**Digital Forensics Essentials**   
Module Notes

Table of Contents

[1 Computer Forensics Fundamentals 3](#_Toc141115390)

[1.1 Fundamentals of Computer Forensics 3](#_Toc141115391)

[1.2 Digital Evidence 4](#_Toc141115392)

[1.3 Forensic Readiness 4](#_Toc141115393)

[1.4 Roles and Responsibilities of a Forensic Investigator 4](#_Toc141115394)

[1.5 Legal Compliance in Computer Forensics 4](#_Toc141115395)

[2 Computer Forensics Investigation Process 5](#_Toc141115396)

[2.1 Forensic Investigation Process and its Importance 5](#_Toc141115397)

[2.2 Forensic Investigation Process - Pre-investigation Phase 5](#_Toc141115398)

[2.3 Forensic Investigation Process - Investigation Phase 5](#_Toc141115399)

[2.4 Forensic Investigation Process - Post-investigation Phase 5](#_Toc141115400)

[3 Understanding Hard Disks and File Systems 6](#_Toc141115401)

[3.1 Different Types of Disk Drives and their Characteristics 6](#_Toc141115402)

[3.2 Logical Structure of a Disk 6](#_Toc141115403)

[3.3 Booting Process of Windows, Linux, and Mac Operating Systems 6](#_Toc141115404)

[3.4 File Systems of Windows, Linux, and Mac Operating Systems 6](#_Toc141115405)

[3.5 File System Examination 6](#_Toc141115406)

[4 Data Acquisition and Duplication 7](#_Toc141115407)

[4.1 Data Acquisition Fundamentals 7](#_Toc141115408)

[4.2 Types of Data Acquisition 7](#_Toc141115409)

[4.3 Data Acquisition Format 7](#_Toc141115410)

[4.4 Data Acquisition Methodology 7](#_Toc141115411)

[5 Defeating Anti-forensics Techniques 8](#_Toc141115412)

[5.1 Anti-forensics and its Techniques 8](#_Toc141115413)

[5.2 Anti-forensics Countermeasures 8](#_Toc141115414)

[6 Windows Forensics 9](#_Toc141115415)

[6.1 Volatile and Non-Volatile Information 9](#_Toc141115416)

[6.2 Windows Memory and Registry Analysis 9](#_Toc141115417)

[6.3 Cache, Cookie, and History Recorded in Web Browsers 9](#_Toc141115418)

[6.4 Windows Files and Metadata 9](#_Toc141115419)

[7 Linux and Mac Forensics 10](#_Toc141115420)

[7.1 Volatile and Non-Volatile Data in Linux 10](#_Toc141115421)

[7.2 Analyse Filesystem Images Using the Sleuth Kit 10](#_Toc141115422)

[7.3 Memory Forensics 402 Mac Forensics 10](#_Toc141115423)

[8 Network Forensics 11](#_Toc141115424)

[8.1 Network Forensics Fundamentals 11](#_Toc141115425)

[8.2 Event Correlation Concepts and Types 11](#_Toc141115426)

[8.3 Identify Indicators of Compromise (IoCs) from Network Logs 11](#_Toc141115427)

[8.4 Investigate Network Traffic 11](#_Toc141115428)

[9 Investigating Web Attacks 12](#_Toc141115429)

[9.1 Web Application Forensics 12](#_Toc141115430)

[9.2 IIS and Apache Web Server Logs 12](#_Toc141115431)

[9.3 Investigating Web Attacks on Windows-based Servers 12](#_Toc141115432)

[9.4 Detect and Investigate Attacks on Web Applications 12](#_Toc141115433)

[10 Dark Web Forensics 13](#_Toc141115434)

[10.1 Dark Web 13](#_Toc141115435)

[10.2 Dark Web Forensics 13](#_Toc141115436)

[10.3 Tor Browser Forensics 13](#_Toc141115437)

[11 Investigating Email Crimes 14](#_Toc141115438)

[11.1 Email Basics 14](#_Toc141115439)

[11.2 Email Crime Investigation and its Steps 14](#_Toc141115440)

[12 Malware Forensics 15](#_Toc141115441)

[12.1 Malware, its Components and Distribution Methods 15](#_Toc141115442)

[12.2 Malware Forensics Fundamentals and Recognize Types of Malware 15](#_Toc141115443)

[12.3 Analysis Static Malware Analysis 15](#_Toc141115444)

[12.4 Analyse Suspicious Word Documents Dynamic Malware Analysis 15](#_Toc141115445)

[12.5 System Behaviour Analysis 15](#_Toc141115446)

[12.6 Network Behaviour Analysis 15](#_Toc141115447)

# Computer Forensics Fundamentals

## Fundamentals of Computer Forensics

Objectives of Computer Forensics

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

Need for Computer Forensics

* 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 organisation’s money and valuable time. Many managers allocate a large portion of their IT budget for computer and network security.
* Cases of complex tracking such as ransomware attacks, email spamming, etc.

When to use Computer Forensics

* Prepare for incidents by securing/strengthening the defence 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.

Types of Cybercrimes

*Cybercrime:* any illegal act involving a computing device, network, its systems, or its applications.

1. *Internal/Insider attacks:* an attack performed on a corporate network or on a single computer by an entrusted person (insider) who has authorised access to the network. Such insiders can be former or current employees, business partners, or contractors.
2. *External attacks:* occurs when an attacker from outside the organisation tries to gain unauthorised access to its computing systems or informational assets. These attackers exploit security loopholes or use social engineering techniques to infiltrate the network.

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:* 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:* 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 a seemingly harmless program with hidden malicious code. It gains control when users perform certain actions, like unwittingly installing malicious software or clicking on malicious links. Once activated, Trojans give attackers complete access to the compromised system, leading to potential severe damage, including harm to the file allocation table on the hard disk.
* *Structured Query Language Attack:* In this technique, the attacker injects malicious SQL queries into a user input form either to gain unauthorised access to a database or to retrieve information directly from the database.
* *Brute-force Attack:* 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:* 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:* 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:* 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:* 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 organisation or individual. Sending defamatory emails or posting defamatory statements on social media can damage the reputation of the target organisation/entity to a great extent.
* *Cyberterrorism:* 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.
* *Cyberwarfare:* the use of information systems against the virtual personas of individuals or groups. It includes information terrorism, semantic attacks (like 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).

Impact of Cybercrimes at the Organisational Level

* Loss of confidentiality, integrity and availability of information stored in organisational systems.
* Theft of sensitive data.
* Sudden disruption of business activities.
* Loss of customer and stakeholder trust.
* Substantial reputational damage.
* Huge financial losses.
* Penalties arising from the failure to comply with regulations.

## Digital Evidence

## Forensic Readiness

## Roles and Responsibilities of a Forensic Investigator

## Legal Compliance in Computer Forensics

# Computer Forensics Investigation Process

## Forensic Investigation Process and its Importance

## Forensic Investigation Process - Pre-investigation Phase

## Forensic Investigation Process - Investigation Phase

## Forensic Investigation Process - Post-investigation Phase

# Understanding Hard Disks and File Systems

## Different Types of Disk Drives and their Characteristics

## Logical Structure of a Disk

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

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

## File System Examination

# Data Acquisition and Duplication

## Data Acquisition Fundamentals

## Types of Data Acquisition

## Data Acquisition Format

## Data Acquisition Methodology

# Defeating Anti-forensics Techniques

## Anti-forensics and its Techniques

## Anti-forensics Countermeasures

# Windows Forensics

## Volatile and Non-Volatile Information

## Windows Memory and Registry Analysis

## Cache, Cookie, and History Recorded in Web Browsers

## Windows Files and Metadata

# Linux and Mac Forensics

## Volatile and Non-Volatile Data in Linux

## Analyse Filesystem Images Using the Sleuth Kit

## Memory Forensics 402 Mac Forensics

# Network Forensics

## Network Forensics Fundamentals

## Event Correlation Concepts and Types

## Identify Indicators of Compromise (IoCs) from Network Logs

## Investigate Network Traffic

# Investigating Web Attacks

## Web Application Forensics

## IIS and Apache Web Server Logs

## Investigating Web Attacks on Windows-based Servers

## Detect and Investigate Attacks on Web Applications

# Dark Web Forensics

## Dark Web

## Dark Web Forensics

## Tor Browser Forensics

# Investigating Email Crimes

## Email Basics

## Email Crime Investigation and its Steps

# Malware Forensics

## Malware, its Components and Distribution Methods

## Malware Forensics Fundamentals and Recognize Types of Malware

## Analysis Static Malware Analysis

## Analyse Suspicious Word Documents Dynamic Malware Analysis

## System Behaviour Analysis

## Network Behaviour Analysis