**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

## 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