UNIT 1: INTRODUCTION TO DIGITAL FORENSICS

1.1 Overview of Digital Forensics

- Definition and Objectives
- Importance in Cybersecurity
- Applications in Real-World Scenarios

1.2 Evolution of Digital Forensics

- History and Milestones
- Development of Forensic Tools and Techniques
- Role of Digital Forensics in Modern Crime Investigation

1.3 Digital Forensics Process

- Identification of Evidence
- Preservation of Data
- Analysis of Digital Evidence
- Documentation and Reporting
- Presentation in Court

1.4 Types of Digital Forensics

- Computer Forensics
- Network Forensics
- Mobile Forensics
- Cloud Forensics
- IoT and Embedded Device Forensics

1.5 Legal and Ethical Aspects

- Digital Evidence and the Law

- Chain of Custody Procedures
- Ethical Responsibilities of a Forensic Investigator

UNIT 2: COMPUTER FORENSICS FUNDAMENTALS

2.1 Computer Forensics Overview

- Definition and Scope
- Types of Computer Crimes
- Role of File Systems in Investigation

2.2 File System Analysis

- FAT, NTFS, and EXT File Systems
- File Metadata and Timestamps
- Deleted File Recovery Principles

2.3 Data Acquisition and Imaging

- Types of Data Acquisition (Static, Live, and Hybrid)
- Bit-by-Bit Copy vs Logical Copy
- Hashing (MD5, SHA1, SHA256) and Data Integrity

2.4 Forensic Tools and Environments

- FTK Imager
- Autopsy
- EnCase (overview)
- Disk Image Creation and Verification

2.5 Practical Forensic Analysis

- Recovering Deleted Files
- Analyzing File System Artifacts

- Creating Chain-of-Custody Documentation

UNIT 3: MOBILE DEVICE FORENSICS

3.1 Introduction to Mobile Forensics

- Mobile Device Architecture (Android and iOS)
- Common Sources of Evidence in Mobile Devices

3.2 Data Acquisition Techniques

- Logical Acquisition
- Physical Acquisition
- SIM and Memory Card Data Extraction

3.3 Common Mobile Artifacts

- Call Logs, Contacts, and SMS Recovery
- Chat Application Data (WhatsApp, Telegram)
- GPS and Location Data

3.4 Mobile Forensic Tools

- MOBILedit Forensic
- Andriller
- Cellebrite UFED (Overview)
- Open-Source Alternatives

3.5 Challenges in Mobile Forensics

- Data Encryption and Security Locks
- Cloud Synchronization
- Anti-Forensic Techniques

UNIT 4: NETWORK FORENSICS

4.1 Basics of Network Forensics

- Definition and Importance
- Network Attacks and Evidence Sources

4.2 Network Architecture and Protocols

- OSI Model Layers
- Common Protocols: TCP, UDP, HTTP, FTP, DNS
- Understanding IP Addressing and Ports

4.3 Capturing and Analyzing Network Data

- Packet Capture Basics
- Identifying Suspicious Network Behavior
- Analyzing Malware Communication Patterns

4.4 Tools for Network Forensics

- Wireshark
- NetworkMiner
- TCPdump
- Packet Analysis using Filters

4.5 Log Analysis and Correlation

- Router and Firewall Logs
- IDS/IPS Log Interpretation
- Event Correlation and Reporting

UNIT 5: MEMORY AND MALWARE FORENSICS

5.1 Introduction to Memory Forensics

- Volatile vs Non-Volatile Data
- Importance of RAM Analysis

5.2 Memory Acquisition

- RAM Dumping Tools
- Memory Image Formats and Preservation

5.3 Analysis of Memory Dumps

- Extracting Running Processes
- Identifying Malicious Activities
- Registry and DLL Analysis

5.4 Malware Forensics

- Malware Behavior Analysis
- Static and Dynamic Analysis Basics
- Detecting Persistence Mechanisms

5.5 Tools for Memory and Malware Analysis

- Volatility Framework
- Redline
- Process Explorer (Sysinternals)

UNIT 6: CLOUD AND EMAIL FORENSICS

6.1 Introduction to Cloud Forensics

- Cloud Computing Models (IaaS, PaaS, SaaS)
- Challenges in Evidence Collection

6.2 Cloud Data Acquisition

- Data Retrieval from Cloud Services
- Forensic Readiness in Cloud Environments
- Service Provider Logs and Metadata

6.3 Email Forensics Fundamentals

- Structure of an Email Message
- Email Header Analysis
- Identifying Spoofing and Phishing Attempts

6.4 Tools for Cloud and Email Forensics

- Email Header Analyzer
- G Suite Admin Tools
- CloudTrail (AWS), Azure Activity Logs

6.5 Case Study

- Investigating a Phishing Email Campaign

UNIT 7: FORENSIC DOCUMENTATION AND REPORTING

7.1 Importance of Documentation

- Maintaining Investigation Records
- Evidence Labeling and Tracking

7.2 Report Writing Standards

- Structure of a Forensic Report
- Key Sections: Summary, Evidence, Findings, Conclusion

7.3 Presentation of Evidence

- Courtroom Procedures

- Expert Witness Role
- Handling Cross-Examination

7.4 Common Mistakes in Forensic Reporting

- Incomplete Documentation
- Lack of Chain of Custody Proof
- Poor Report Formatting

7.5 Practical Exercise

- Prepare a Forensic Report for a Case Study