Unit 1 – Cybercrime and Digital Forensics (Detailed Notes)

---

1. Introduction to Cybercrime

Definition

Cybercrime refers to **criminal activities carried out using computers, digital devices, or the internet**. In cybercrime, the **computer can be the target, tool, or medium of crime**.

Cybercrime involves:

- Unauthorized access to systems
- Data theft
- Financial fraud
- Identity theft
- Cyber terrorism

Key Characteristics of Cybercrime

1. **Global nature** – crimes can occur across countries.
2. **Anonymity** – criminals can hide their identity.
3. **High speed** – attacks can spread quickly.
4. **Low cost** – criminals need only internet access and technical skills.
5. **Difficult to trace** – attackers often use VPN, proxies, or dark web.

Examples

- Hacking bank accounts
- Stealing credit card information
- Ransomware attacks
- Online fraud
- Phishing emails

Impact of Cybercrime

- Financial loss
- Loss of privacy
- National security threats
- Reputation damage
- Data leakage

---

2. Types of Cybercrime

Cybercrimes are categorized based on **target and method**.

1. Crimes Against Individuals

These crimes target **individual persons**.

Examples:

- Identity theft
- Cyber stalking
- Online harassment
- Email spoofing
- Phishing

Example:

A hacker sends a fake bank email and steals login credentials.

---

2. Crimes Against Property

These involve **stealing or damaging digital property**.

Examples:

- Software piracy
- Intellectual property theft
- Data theft
- Virus attacks

Example:

Illegal downloading of paid software.

---

3. Crimes Against Organizations

Target businesses, companies, or institutions.

Examples:

- Database hacking
- Ransomware attacks
- Corporate espionage
- Denial of Service (DoS)

Example:

Hackers encrypt company files and demand money.

---

4. Crimes Against Government

These are **serious cyber threats affecting national security**.

Examples:

- Cyber terrorism
- Attacking government websites
- Military system hacking
- Spreading misinformation

Example:

Hacking government databases.

---

3. The Internet Spawns Crime

Meaning

The **internet has created new opportunities for criminals** because of its open and global nature.

Reasons Why Internet Increases Crime

1. **Anonymity**
   Criminals hide identity using VPN, TOR, proxy servers.
2. **Global connectivity**
   Criminals can attack systems anywhere in the world.
3. **Easy access**
   Anyone with basic technical knowledge can attempt attacks.
4. **Large amount of data**
   Organizations store valuable data online.

5. **Lack of awareness**
   Many users are unaware of cyber threats.

Common Internet Based Crimes

- Online scams
- Phishing attacks
- Malware distribution
- Fake websites
- Cryptocurrency fraud

---

4. Worms vs Viruses

Both are **types of malware**, but they behave differently.

Virus

Definition

A virus is a **malicious program that attaches itself to another file or program and spreads when the infected file is executed**.

Characteristics

- Requires a **host file**
- Spreads when user runs infected program
- Can corrupt or delete data

Example

- Boot sector virus
- Macro virus

Worm

Definition

A worm is a **self-replicating malware that spreads automatically across networks without user interaction**.

Characteristics

- Does **not require host file**
- Spreads through network vulnerabilities
- Consumes system resources

Example

- WannaCry worm
- SQL Slammer worm

Difference Between Virus and Worm

Feature	Virus	Worm
Requires host	Yes	No
User interaction	Required	Not required
Spread method	Infected files	Network
Speed of spread	Slow	Very fast

---

5. Computer's Role in Crimes
Computers can play **three roles in cybercrime**.

---

1. Computer as Target
Here the **computer system itself is attacked**.
Examples:

- Hacking
- Malware attacks
- Data deletion
- Denial of Service attack

Example:
A hacker breaks into a bank server.

---

2. Computer as Tool
Computer is **used to commit crimes**.
Examples:

- Online fraud
- Phishing emails
- Identity theft
- Financial scams

Example:
Sending fake payment links.

---

3. Computer as Evidence
Computers may contain **digital evidence of crime**.
Examples:

- Emails
- Log files
- Chat messages
- Documents

Example:
Police retrieving deleted files during investigation.

---

6. Introduction to Digital Forensics
Definition
Digital Forensics is the **process of identifying, collecting, analyzing, and presenting digital evidence from computers or digital devices**.
It is used in:

- Cybercrime investigations
- Corporate investigations
- Legal proceedings
- Security incidents

Goals of Digital Forensics

1. Recover deleted files
2. Identify attackers
3. Preserve evidence
4. Analyze system activity
5. Present evidence in court

Types of Digital Forensics

1. **Computer Forensics**
   Investigation of computers and hard drives.
2. **Network Forensics**
   Monitoring network traffic to detect attacks.
3. **Mobile Forensics**
   Investigation of smartphones.
4. **Database Forensics**
   Investigating database logs and activities.
5. **Cloud Forensics**
   Investigating cloud systems.

Steps in Digital Forensics

1. Identification
2. Preservation
3. Collection
4. Examination
5. Analysis
6. Presentation

---

7. Introduction to Incident

Definition

An incident is **any event that compromises the confidentiality, integrity, or availability of information systems**.

Examples of Security Incidents

- Malware infection
- Unauthorized access
- Data breach
- System hacking
- Website defacement

Types of Incidents

1. Malware attack
2. Network intrusion
3. Data leakage
4. Insider threat
5. Denial of service attack

---

8. Incident Response Methodology

Incident Response is a **structured approach to handling cyber security incidents**.

It helps organizations:

- Detect attacks
- Reduce damage
- Recover systems
- Prevent future incidents

Standard Incident Response Phases

1. Preparation
2. Detection and Analysis
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

---

9. Steps in Incident Response

1. Preparation

Organization prepares for cyber attacks.

Activities:

- Security policies
- Incident response team
- Monitoring systems
- Security tools

---

2. Detection

Identify whether a security incident has occurred.

Methods:

- IDS/IPS alerts
- Log monitoring
- User reports
- Antivirus alerts

---

3. Containment

Limit the damage caused by the attack.

Examples:

- Disconnect infected system
- Block malicious IP
- Disable compromised accounts

---

4. Eradication

Remove the cause of the attack.

Examples:

- Delete malware

- Patch vulnerabilities
- Remove malicious files

---

5. Recovery
Restore systems to normal operation.
Examples:

- Restore backups
- Monitor systems
- Reconnect network

---

6. Lessons Learned
Analyze incident and improve security.
Activities:

- Document incident
- Improve policies
- Train staff

---

10. Activities in Initial Response
When an incident is detected, the **initial response phase** begins.
Key activities include:

1. **Confirm the incident**
   Verify if the alert is real.
2. **Assess severity**
   Determine how serious the incident is.
3. **Notify response team**
   Inform security team and management.
4. **Secure the system**
   Prevent further damage.
5. **Collect evidence**
   Preserve logs and system data.
6. **Document everything**
   Maintain investigation records.

---

11. Phase After Detection of an Incident
Once the incident is detected, several actions follow.
1. Containment
Stop the attack from spreading.
Example:
Disconnect infected computer.

---

2. Investigation
Analyze logs and evidence.
Example:
Check login history and network traffic.

---

3. Removal of Threat
Remove malware or attacker access.
Example:
Delete malicious programs.

---

4. Recovery
Restore normal operations.
Example:
Reinstall system and restore backups.

---

5. Post-Incident Review
Evaluate response process.
Questions asked:

- What happened?
- How did it happen?
- How can it be prevented?

Short Exam Ready Definitions
Cybercrime:
Criminal activities performed using computers or the internet.
Digital Forensics:
The process of collecting and analyzing digital evidence.
Virus:
Malware that attaches to files and spreads when executed.
Worm:
Self-replicating malware that spreads automatically through networks.
Incident:
Any event that threatens information security.
Incident Response:
Process used to detect, respond, and recover from cyber attacks.

Unit-2: Initial Response & Forensic Duplication (Detailed Notes)

---

1. Initial Response and Forensic Duplication

Initial Response

Definition

Initial Response refers to the **first actions taken when a security incident or cybercrime is discovered**.

The goal is to **secure the system, preserve evidence, and prevent further damage**.

If the response is handled incorrectly, **important digital evidence may be destroyed or modified**.

Objectives of Initial Response

1. Protect digital evidence
2. Identify scope of the incident
3. Prevent further damage
4. Begin investigation process
5. Maintain chain of custody

Key Principles of Initial Response

1. **Do not alter the system unnecessarily**
2. **Document every action**
3. **Preserve volatile data**
4. **Follow forensic procedures**
5. **Ensure legal admissibility**

Steps in Initial Response

1. **Identify the incident**
    - Detect unusual activity.
2. **Secure the scene**
    - Restrict access to affected system.
3. **Document the system**
    - Record system details and screen status.
4. **Collect volatile data**
    - Capture RAM and running processes.
5. **Preserve evidence**
    - Avoid modifying original data.
6. **Prepare for forensic duplication**
    - Create a copy of storage devices.

---

2. Volatile Data Collection

What is Volatile Data?

Volatile data is **temporary data stored in memory (RAM)** that **disappears when the system is powered off**.

Examples:

- Running processes
- Network connections
- Logged-in users
- RAM contents
- System time

Because volatile data **changes rapidly**, it must be collected **immediately**.

---

3. Initial Response & Volatile Data Collection from Windows System

When investigating a **Windows computer**, investigators must collect volatile data before shutting down the system.

Steps for Windows Volatile Data Collection

1. Record System Time

Check current system time.

Command:

time /t

date /t

Purpose:

Helps synchronize logs during investigation.

---

2. Identify Logged-in Users

Command:

query user

Purpose:

Shows active user sessions.

---

3. Identify Running Processes

Command:

tasklist

Purpose:

Lists currently running applications and services.

---

4. Identify Network Connections

Command:

netstat -ano

Purpose:

Displays active network connections and ports.

---

5. Identify Open Files

Command:

openfiles

Purpose:

Shows files currently opened by processes.

---

6. Capture RAM (Memory Dump)
Tools used:

- FTK Imager
- DumpIt
- Belkasoft RAM Capturer

Purpose:
Capture full memory for forensic analysis.

---

7. Collect System Information
Command:
systeminfo
Provides details such as:

- OS version
- Installed patches
- Hardware information

---

4. Initial Response & Volatile Data Collection from Unix / Linux System
Unix systems (Linux, BSD, etc.) require similar forensic procedures.
Volatile data should be collected **before shutting down the system**.

Steps for Unix Volatile Data Collection
1. Record System Time
Command:
date
Purpose:
Record system time for log analysis.

---

2. Identify Logged-in Users
Command:
who
Shows currently logged users.
Another command:
w
Shows user activity.

---

3. Identify Running Processes
Command:
ps -ef
Displays all active processes.

---

4. Check Network Connections
Command:
netstat -an
Displays active connections and listening ports.

---

5. Check Open Files
Command:
lsof
Shows open files and associated processes.

---

6. Check Network Interfaces
Command:
ifconfig
Displays network interface information.

---

7. Capture Memory Dump
Tools:

- LiME (Linux Memory Extractor)
- AVML
- fmem

Purpose:
Capture RAM contents.

---

5. Forensic Duplication
Definition
Forensic Duplication is the **process of creating an exact bit-by-bit copy of digital storage media** such as:

- Hard drives
- USB drives
- Memory cards
- SSDs

The duplicate copy is used for **analysis while preserving the original evidence**.

Why Forensic Duplication is Important

1. Protect original evidence
2. Allow repeated analysis
3. Maintain legal integrity
4. Prevent data modification

Types of Forensic Copies

1. **Bit-stream copy**
2. **Disk image**
3. **Clone**

---

6. Forensic Duplicates as Admissible Evidence
In court, digital evidence must follow **legal standards** to be admissible.
A forensic duplicate can be accepted as evidence if:

1. It is **exactly identical to original data**

2. It is created using **forensic tools**
3. Integrity is verified using **hash values**
4. Chain of custody is maintained

Hash Functions Used

Hash functions verify data integrity.

Common algorithms:

- MD5
- SHA-1
- SHA-256

If the **hash value of original and duplicate match**, the copy is verified.

Example:

Original Hash = Duplicate Hash

Meaning → Data is unchanged.

---

7. Forensic Duplication Tool Requirements

A forensic duplication tool must meet specific requirements.

---

1. Bit-by-Bit Copy Capability

The tool must copy **every bit of data**, including:

- Deleted files
- Hidden data
- Slack space

---

2. Write Blocking

The tool must prevent any **modification of original evidence**.

Devices used:

- Hardware write blockers
- Software write blockers

---

3. Hash Verification

The tool must generate **hash values** to verify integrity.

---

4. Logging Capability

The tool must maintain logs of:

- Date
- Time
- Investigator
- Steps performed

---

5. Compatibility

The tool must support multiple storage formats.

Examples of Forensic Duplication Tools

1. EnCase
2. FTK Imager
3. dd (Linux tool)
4. Guymager
5. Autopsy

---

8. Creating a Forensic Duplicate / Qualified Forensic Duplicate of a Hard Drive
Definition
A Qualified Forensic Duplicate is a **verified copy of digital media created using forensic procedures and tools**.

Steps to Create Forensic Duplicate

Step 1: Prepare Investigation Environment

- Secure forensic workstation
- Use write blocker
- Document system details

Step 2: Connect Evidence Drive
Attach suspect hard drive using:
Hardware write blocker.
Purpose:
Prevent accidental modification.

Step 3: Use Forensic Imaging Tool
Example tools:

- FTK Imager
- EnCase
- dd command

Example using Linux:
dd if=/dev/sda of=/evidence/disk_image.dd
Meaning:

- if → input file
- of → output image

Step 4: Generate Hash Values
Calculate hash of:

- Original drive
- Forensic image

Example:
MD5 Hash = 8f14e45fceea167a5a36dedd4bea2543
If both hashes match → image is verified.

Step 5: Verify the Image

Use forensic software to confirm:

- Image integrity
- File system consistency

Step 6: Store Evidence Securely

Original device should be:

- Sealed
- Labeled
- Stored safely

Analysis is performed on **duplicate image**.

Short Exam Definitions

Initial Response:
First actions taken after detecting a cyber incident to secure evidence and systems.
Volatile Data:
Temporary data stored in memory that disappears when the system shuts down.
Forensic Duplication:
Process of creating an exact bit-by-bit copy of digital storage.
Qualified Forensic Duplicate:
A verified forensic copy that maintains the integrity of original evidence.
Hash Value:
A digital fingerprint used to verify data integrity.

Important Exam Questions (Unit-2)

Short Questions

1. Define forensic duplication.
2. What is volatile data?
3. Explain hash values in digital forensics.
4. Write commands for volatile data collection in Windows.
5. Write commands for volatile data collection in Unix.

Long Questions

1. Explain the initial response process in digital forensics.
2. Describe volatile data collection from Windows systems.
3. Explain forensic duplication and its legal importance.
4. Describe steps to create a forensic duplicate of a hard drive.
5. Explain requirements of forensic duplication tools.

Unit – 3: Forensics Analysis and Validation & Network Forensics

---

1. Forensics Analysis and Validation

Definition

Forensic Analysis is the **process of examining collected digital evidence to discover facts related to a cybercrime**.

Validation means **verifying that the collected forensic data is accurate, authentic, and has not been modified**.

The purpose is to **identify the attacker, determine the attack method, and provide reliable evidence for legal investigation**.

Objectives of Forensic Analysis

1. Identify digital evidence
2. Reconstruct events of the attack
3. Detect malicious activities
4. Maintain data integrity
5. Present valid evidence in court

---

2. Determining What Data to Collect and Analyze

Before starting forensic analysis, investigators must decide **which data sources are relevant to the investigation**.

Collecting unnecessary data can waste time and resources.

Important Sources of Digital Evidence

1. System Logs

Logs contain records of system activities.

Examples:

- Login records
- Error logs
- Application logs

Example log file:

/var/log/syslog

---

2. Network Logs

Network logs record network communication.

Examples:

- Firewall logs
- Router logs
- IDS alerts

Purpose:
Identify suspicious connections.

---

3. File System Data

Includes files stored in the system.

Examples:

- Documents
- Images
- Executable files
- Deleted files

---

4. Memory Data (RAM)

RAM contains important volatile data.

Examples:

- Running processes
- Encryption keys
- Malware traces

---

5. User Activity Data

Includes:

- Browser history
- Email messages
- Chat logs
- Downloads

---

6. External Storage Devices

Examples:

- USB drives
- External hard disks
- Memory cards

These may contain stolen or hidden data.

---

3. Validating Forensic Data

Validation ensures that **digital evidence remains unchanged from its original state**.

If evidence integrity is compromised, it **cannot be used in court**.

Methods for Validation

1. Hash Verification

Hash algorithms generate a **unique digital fingerprint of data**.

Common algorithms:

- MD5
- SHA-1
- SHA-256

Example:

Original Hash = Duplicate Hash

If both values match → evidence is valid.

---

2. Chain of Custody

Chain of custody is a **record showing who handled the evidence and when**.

It includes:

- Evidence ID
- Date and time
- Investigator name
- Description of action

Purpose:
Maintain accountability.

---

3. Documentation

Every step must be documented.

Documentation includes:

- Investigation notes
- System screenshots
- Evidence labels

---

4. Addressing Data-Hiding Techniques

Cybercriminals often hide data to **avoid detection**.

Digital forensic investigators must detect these hidden data techniques.

Common Data Hiding Techniques

1. Steganography

Steganography hides information inside other files.

Example:
Secret message hidden inside an image file.

Example file:

image.jpg

May contain hidden data.

---

2. Encryption

Attackers encrypt files to prevent access.

Examples:

- Encrypted ZIP files
- Password-protected documents

Investigators must attempt:

- Password recovery
- Encryption analysis

---

3. Hidden Files and Folders

Attackers may hide files using operating system features.

Example in Windows:

attrib +h secret.txt

The file becomes hidden.

---

4. File System Manipulation

Criminals may manipulate file systems.

Examples:

- Changing timestamps
- Altering metadata
- Deleting logs

---

5. Rootkits

Rootkits hide malware by modifying operating system functions.

Effects:

- Hidden processes
- Hidden files
- Hidden network connections

---

5. Performing Remote Acquisitions

Definition

Remote Acquisition means **collecting digital evidence from a remote system over a network without physically accessing the device**.

This technique is used when systems are located in **different geographic locations**.

Advantages

1. Saves time
2. No need for physical access
3. Useful in large networks
4. Enables quick evidence collection

Challenges

1. Network bandwidth limitations
2. Security risks
3. Data transmission integrity
4. Legal permissions

Remote Acquisition Tools

Examples:

- EnCase Enterprise
- FTK Enterprise
- SSH tools
- Remote forensic agents

---

6. Network Forensics

Definition

Network Forensics is the **process of capturing, recording, and analyzing network traffic to investigate cyber attacks**.

It helps investigators understand:

- How attackers entered the system
- What data was transmitted
- Which systems were affected

Importance of Network Forensics

1. Detect network attacks
2. Trace hacker activities
3. Analyze malware communication

4. Prevent future attacks

---

7. Network Forensics Overview

Network forensics focuses on **monitoring and analyzing data packets traveling across a network**.

Data packets contain:

- Source IP address
- Destination IP address
- Protocol
- Packet contents

Key Components

1. Packet Capture

Capturing network packets for analysis.

Tools:

- Wireshark
- tcpdump

---

2. Traffic Analysis

Analyzing captured packets to identify malicious activities.

Examples:

- Suspicious connections
- Malware communication
- Data exfiltration

---

3. Log Analysis

Examining logs from:

- Firewalls
- Routers
- Servers

---

8. Performing Live Acquisitions

Definition

Live Acquisition refers to **collecting digital evidence from a running system without shutting it down**.

This is important because shutting down the system may destroy volatile data.

Data Collected During Live Acquisition

Examples:

- RAM data
- Running processes
- Network connections
- Open files
- Active users

Steps in Live Acquisition

1. Document system state
2. Capture memory dump
3. Record running processes
4. Record network connections
5. Collect system logs

---

9. Developing Standard Procedures for Network Forensics

Organizations should establish **standard procedures for investigating network incidents**.

Key Steps

1. Preparation

Prepare tools and policies for forensic investigation.

Examples:

- Monitoring tools
- Incident response team

---

2. Detection

Detect suspicious network activity.

Examples:

- IDS alerts
- Unusual traffic patterns

---

3. Collection

Collect relevant evidence such as:

- Packet captures
- Log files
- System alerts

---

4. Analysis

Analyze collected data to identify attack patterns.

---

5. Documentation

Prepare detailed reports for investigation.

---

10. Using Network Tools

Several tools are used in network forensic investigations.

---

1. Wireshark

Wireshark is a **network protocol analyzer** used to capture and analyze packets.

Features:

- Real-time packet capture
- Detailed packet inspection
- Protocol analysis

---

2. tcpdump

Command-line packet capture tool.

Example command:

tcpdump -i eth0

Captures packets from network interface.

---

3. Snort

Snort is an **Intrusion Detection System (IDS)**.

It detects suspicious network activities.

---

4. Netstat

Displays active network connections.

Example:

netstat -an

---

11. The Honeynet Project

Definition

A Honeynet is a **network of honeypots designed to attract hackers so that their activities can be studied**.

The Honeynet Project is an **international research organization focused on studying cyber attacks**.

Purpose of Honeynet

1. Study hacker techniques
2. Detect new malware
3. Improve security systems
4. Understand attack behavior

What is a Honeypot?

A honeypot is a **decoy computer system designed to attract attackers**.

Attackers think it is a real system, but it is monitored by security experts.

Types of Honeypots

1. Low Interaction Honeypots

Simulate limited services.

Example:
Fake FTP server.

---

2. High Interaction Honeypots

Real systems used to study advanced attacks.

Provides deeper analysis.

Benefits of Honeynet

1. Detect unknown attacks
2. Understand attacker behavior
3. Improve intrusion detection systems
4. Provide research data

Short Exam Definitions

Forensic Analysis:
Process of examining digital evidence to determine facts related to cybercrime.

Validation:
Process of verifying that forensic data has not been altered.

Remote Acquisition:
Collecting digital evidence from a remote computer through a network.

Network Forensics:
Monitoring and analyzing network traffic to investigate cyber attacks.

Honeypot:
A decoy system designed to attract attackers for monitoring.

Important Exam Questions (Unit-3)

Short Questions

1. Define forensic analysis.
2. What is remote acquisition?
3. What is network forensics?
4. What is steganography?
5. What is a honeypot?

Long Questions

1. Explain methods of validating forensic data.
2. Discuss data hiding techniques used by attackers.
3. Explain remote acquisition in digital forensics.
4. Describe network forensic tools and their functions.
5. Explain the honeynet project and its importance.

Unit – 4: Current Forensic Tools, E-Mail Investigations, and Mobile Device Forensics

---

1. Current Forensic Tools

Digital forensic investigations require **specialized tools** to collect, analyze, and preserve digital evidence.

Forensic tools help investigators:

- Recover deleted files
- Analyze disk images
- Examine logs and network data
- Investigate cybercrimes

These tools are classified into **software tools and hardware tools**.

---

2. Evaluating Computer Forensic Tool Needs

Before selecting a forensic tool, investigators must **evaluate the requirements of the investigation**.

Factors to Consider

1. Type of Investigation

The tool should support the investigation type.

Examples:

- Disk forensics
- Network forensics
- Mobile forensics

---

2. Operating System Compatibility

The tool should support multiple operating systems.

Examples:

- Windows

- Linux
- macOS

---

3. File System Support

The tool must support different file systems such as:

- NTFS
- FAT32
- EXT3 / EXT4

---

4. Evidence Integrity

The tool must ensure **data integrity**.

Features required:

- Hash verification
- Write blocking

---

5. Reporting Capability

Forensic tools should generate **investigation reports** for legal use.

---

6. Cost and Performance

Tools should provide **efficient analysis without excessive cost**.

---

3. Computer Forensics Software Tools

These are **software programs used to analyze digital evidence**.

---

1. EnCase

EnCase is one of the **most widely used digital forensic tools**.

Features:

- Disk imaging
- File recovery
- Evidence analysis
- Report generation

Used by:

- Law enforcement agencies
- Cybercrime investigators

---

2. FTK (Forensic Toolkit)

FTK is a **popular forensic investigation software**.

Features:

- Fast file indexing
- Email analysis
- Password recovery
- Registry analysis

---

3. Autopsy

Autopsy is an **open-source digital forensic tool**.

Features:

- File system analysis
- Timeline analysis
- Keyword searching
- Web activity analysis

---

4. Wireshark

Wireshark is a **network packet analyzer**.

Features:

- Capture network traffic
- Analyze protocols
- Detect suspicious activity

---

5. Sleuth Kit

The Sleuth Kit is used for **disk image analysis and file system investigation**.

---

4. Computer Forensics Hardware Tools

Hardware tools are **physical devices used during forensic investigation**.

---

1. Write Blockers

Write blockers prevent **modification of original evidence**.

Example:

If a forensic investigator connects a suspect hard drive to a computer, the write blocker ensures **no data is changed**.

---

2. Forensic Workstations

Special computers designed for **digital forensic analysis**.

Features:

- High storage capacity
- Powerful processors
- Multiple disk interfaces

---

3. Disk Duplicators

Devices used to **create exact copies of storage media**.

Example:

Duplicating a hard drive for forensic analysis.

---

4. Faraday Bags

Faraday bags block **wireless signals from mobile devices**.

Purpose:

Prevent remote wiping or tampering with mobile evidence.

---

5. Validating and Testing Forensics Software

Forensic tools must be **tested and validated before use in investigations**.

Validation ensures:

- Accurate results
- Reliable evidence
- Legal admissibility

Validation Methods

1. Tool Testing

Investigators test tools using **sample data** to verify accuracy.

---

2. Hash Verification

Hash values confirm that evidence remains unchanged.

Common algorithms:

- MD5
- SHA-1
- SHA-256

---

3. Cross Verification

Results from one tool are verified using another tool.

Example:

Checking disk image using two forensic software tools.

---

6. E-Mail Investigations

Email plays an important role in **cybercrime investigations**.

Many cybercrimes involve email communication.

Examples:

- Phishing attacks
- Fraud emails
- Threatening messages
- Malware distribution

---

7. Role of E-Mail in Investigation

Emails provide important evidence such as:

- Sender identity
- Message content
- Attachments
- Date and time

Email evidence can help investigators:

- Identify criminals
- Track communication
- Determine crime motive

---

8. Roles of Client and Server in E-Mail

Email communication involves **two major components**:

1. Email Client

The email client is the **application used by the user to send and receive emails**.

Examples:

- Outlook
- Thunderbird
- Gmail web interface

Functions:

- Compose emails
- Read messages
- Download attachments

---

2. Email Server

Email servers store and transfer emails between users.

Common email protocols:

- SMTP (Simple Mail Transfer Protocol)
- POP3 (Post Office Protocol)
- IMAP (Internet Message Access Protocol)

---

9. Investigating Email Crimes and Violations

Email crimes include:

- Phishing
- Email spoofing
- Spam attacks
- Malware distribution

Investigation Steps

1. Collect Email Evidence

Evidence sources include:

- Email messages
- Email headers
- Attachments
- Server logs

---

2. Analyze Email Headers

Email headers contain routing information.

Example fields:

- From
- To
- Received
- IP address
- Time stamps

Investigators use headers to **trace the sender's origin**.

---

3. Analyze Attachments

Attachments may contain:

- Malware
- Hidden data
- Fraudulent documents

---

4. Check Server Logs

Email servers maintain logs showing:

- Message transfers
- User access records

---

10. Understanding Email Servers

Email servers manage email transmission and storage.

Types of Email Servers

SMTP Server

Responsible for **sending emails**.

Example:

Sending message from Gmail to Yahoo.

POP3 Server

Used for **downloading emails from the server**.

IMAP Server

Allows users to **access email directly from the server without downloading**.

---

11. Specialized Email Forensic Tools

These tools analyze email evidence.

---

1. MailXaminer

Used for:

- Email header analysis
- Email recovery

- Attachment investigation

---

2. Paraben Email Examiner

Features:

- Email evidence extraction
- Keyword searching
- Message reconstruction

---

3. Aid4Mail

Used to:

- Analyze large email archives
- Extract forensic evidence

---

12. Cell Phone and Mobile Device Forensics

Mobile device forensics is the **process of recovering digital evidence from mobile devices**.

Devices include:

- Smartphones
- Tablets
- SIM cards
- Memory cards

Importance of Mobile Forensics

Mobile phones contain valuable evidence such as:

- Call logs
- SMS messages
- Contacts

- Photos and videos
- GPS location data
- App activity

---

13. Understanding Mobile Device Forensics

Mobile forensic investigators analyze mobile devices to:

- Recover deleted data
- Analyze communications
- Track suspect movements
- Identify criminal activity

Challenges in Mobile Forensics

1. Large variety of devices
2. Different operating systems (Android, iOS)
3. Data encryption
4. Rapid technology changes

---

14. Acquisition Procedures for Cell Phones and Mobile Devices

Acquisition means **collecting data from mobile devices for forensic investigation**.

Types of Mobile Data Acquisition

1. Manual Acquisition

Investigator manually examines phone screen and records information.

Example:

- Viewing call logs
- Reading SMS messages

---

2. Logical Acquisition

Extracts data using software through operating system.

Data collected:

- Contacts
- Messages
- Call logs

---

3. Physical Acquisition

Creates **complete copy of device memory**.

Includes:

- Deleted data
- Hidden files

---

4. File System Acquisition

Extracts file system structure of the device.

---

15. Mobile Forensic Tools

Examples of tools used for mobile investigations:

1. Cellebrite UFED

Used by law enforcement agencies.

Features:

- Data extraction from smartphones
- SIM card analysis

---

2. Oxygen Forensic Suite

Features:

- Mobile data extraction
- Social media analysis

---

3. MOBILedit

Used to:

- Extract phone data
- Analyze SMS and contacts

Short Exam Definitions

Computer Forensic Tools:
Software or hardware used to collect and analyze digital evidence.

Email Forensics:
Investigation and analysis of email messages for cybercrime evidence.

Mobile Device Forensics:
Process of recovering and analyzing data from mobile devices.

Write Blocker:
A hardware device that prevents modification of digital evidence.

Email Header:
Metadata of an email containing routing information.

Important Exam Questions (Unit-4)

Short Questions

1. Define computer forensic tools.
2. What is email forensics?
3. What is a write blocker?
4. What is mobile device forensics?
5. What are email headers?

Long Questions

1. Explain computer forensic software and hardware tools.
2. Describe the role of email in cybercrime investigations.
3. Explain the structure of email communication (client and server).
4. Discuss mobile device forensic acquisition methods.

Unit – 5: Working with Windows and DOS Systems

This unit focuses on **Windows operating systems, file systems, disk structures, encryption, registry analysis, and startup processes** used in digital forensic investigations.

---

1. Understanding File Systems

Definition

A **File System** is a method used by operating systems to **store, organize, and manage files on storage devices** such as hard disks, SSDs, and USB drives.

It defines:

- How data is stored
- How files are organized
- How files are accessed and retrieved

Functions of File Systems

1. File storage
2. File organization
3. File access management
4. Data security
5. File retrieval

Common File Systems

FAT (File Allocation Table)

Used in older Windows systems.

Characteristics:

- Simple structure
- Limited security
- Supports small storage devices

Examples:

- FAT12
- FAT16
- FAT32

NTFS (New Technology File System)

Modern Windows systems use NTFS.

Features:

- File permissions
- Encryption
- Compression
- Large disk support
- Journaling

---

exFAT

Used in portable devices like:

- USB drives
- SD cards

Importance in Digital Forensics

Investigators analyze file systems to:

- Recover deleted files
- Examine metadata
- Identify hidden data

---

2. Exploring Microsoft File Structures

Microsoft operating systems store data using **specific file structures**.

These structures organize how files are stored and accessed.

Key Components of File Structure

1. Boot Sector

The boot sector contains **instructions required to start the operating system**.

It is located at the beginning of a disk.

---

2. File Allocation Table (FAT)

The FAT keeps track of **file locations on disk**.

It tells the system where each file is stored.

---

3. Master File Table (MFT)

In NTFS systems, the **Master File Table (MFT)** stores information about every file.

Each file has an entry in the MFT.

Information stored includes:

- File name
- File size
- Time stamps
- File location

---

4. Data Area

The data area stores the **actual contents of files**.

---

3. Examining NTFS Disks

NTFS Overview

NTFS is the **default file system used by modern Windows operating systems**.

Examples:

- Windows 10
- Windows 11
- Windows Server

Features of NTFS

1. Master File Table (MFT)

The MFT stores metadata about files.

Each file has a unique MFT record.

---

2. File Permissions

NTFS allows administrators to control file access.

Example permissions:

- Read
- Write
- Execute

---

3. Journaling

NTFS keeps a **log of file system changes**.

This helps recover data after system crashes.

---

4. File Compression

Files can be compressed to save disk space.

---

5. Encryption

NTFS supports **Encrypting File System (EFS)**.

Importance in Forensics

Investigators analyze NTFS to:

- Recover deleted files
- Examine timestamps
- Detect hidden files

---

4. Understanding Whole Disk Encryption

Definition

Whole Disk Encryption (WDE) protects data by **encrypting the entire storage disk**.

Only authorized users with the correct password or key can access the data.

Purpose of Disk Encryption

1. Protect sensitive data
2. Prevent unauthorized access
3. Secure lost or stolen devices

Examples of Disk Encryption

BitLocker

BitLocker is a disk encryption feature in Windows.

Features:

- Full disk encryption
- TPM security support
- Password protection

VeraCrypt

Open-source encryption tool.

Used for:

- Disk encryption
- Secure containers

Challenges for Forensic Investigators

Encrypted disks are difficult to analyze because:

- Data cannot be accessed without keys
- Encryption hides file content

Investigators may need:

- Password recovery
- Memory analysis

---

5. Windows Registry

Definition

The **Windows Registry** is a database that stores configuration settings for the Windows operating system.

It contains information about:

- Hardware
- Software
- User preferences
- System settings

Registry Structure

The registry contains **keys and values** similar to folders and files.

Main registry sections:

- HKEY_LOCAL_MACHINE
- HKEY_CURRENT_USER
- HKEY_CLASSES_ROOT
- HKEY_USERS
- HKEY_CURRENT_CONFIG

Importance in Digital Forensics

Registry analysis can reveal:

- Installed programs
- User activity
- USB device usage
- Login information

Example evidence:

- Recently opened files
- Connected devices
- Malware persistence

---

6. Microsoft Startup Tasks

Startup tasks are programs that **automatically run when Windows starts**.

These tasks can be configured in several locations.

Common Startup Locations

Startup Folder

Programs placed in the startup folder run automatically.

Example path:

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

Registry Startup Entries

Malware often adds entries in the registry.

Example registry path:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

---

Scheduled Tasks

Programs may run automatically using Windows Task Scheduler.

Importance in Forensics

Investigators check startup entries to detect:

- Malware persistence
- Unauthorized programs

---

7. MS-DOS Startup Tasks

MS-DOS systems use **startup configuration files** to initialize system settings.

Important Startup Files

AUTOEXEC.BAT

Contains commands executed automatically when the system starts.

Example:

PATH C:\DOS

CONFIG.SYS

Configures system settings and device drivers.

Example:

DEVICE=HIMEM.SYS

Role in Forensic Investigation

Investigators examine these files to detect:

- Unauthorized commands
- Malicious scripts
- System configuration changes

---

8. Virtual Machines

Definition

A **Virtual Machine (VM)** is a software-based computer that runs inside another computer.

It behaves like a real computer with its own:

- Operating system
- Applications
- Storage

Examples of Virtualization Software

- VMware
- VirtualBox
- Hyper-V

Uses in Digital Forensics

Virtual machines are used to:

1. Safely analyze malware
2. Test suspicious files
3. Simulate attack environments
4. Examine disk images

Advantages

1. Safe testing environment
2. Easy system recovery

3. Multiple operating systems on one computer

Short Exam Definitions

File System:
A method used by operating systems to organize and store files on storage devices.

NTFS:
A modern Windows file system that supports security, encryption, and large disk storage.

Windows Registry:
A database storing configuration settings of the Windows operating system.

Whole Disk Encryption:
A security technique that encrypts the entire storage disk to protect data.

Virtual Machine:
A software-based computer that runs inside another physical computer.

Important Exam Questions (Unit-5)

Short Questions

1. Define file system.
2. What is NTFS?
3. What is Windows Registry?
4. What is whole disk encryption?
5. What is a virtual machine?

Long Questions

1. Explain Windows file systems and their importance in digital forensics.
2. Describe NTFS disk structure and features.
3. Explain the Windows Registry and its role in forensic investigation.
4. Discuss Microsoft startup tasks and their forensic significance.
5. Explain virtual machines and their role in forensic analysis.

Unit – 6: Laws and Acts in Cyber Forensics

Cybercrime investigations must follow **legal rules and ethical guidelines** to ensure that digital evidence is **valid in court**. This unit focuses on laws, ethics, and evidence handling procedures.

---

1. Laws and Ethics

Laws

Laws are official rules created by governments to regulate behavior in society.
In cybercrime investigations, laws define:

- What activities are illegal
- Punishments for cybercrimes
- Procedures for investigation
- Rules for collecting digital evidence

Examples of cyber laws include:

- Information Technology Act (India)
- Data protection laws
- Cybercrime laws

Ethics

Ethics refers to moral principles that guide professional behavior.

In digital forensics, investigators must follow ethical practices such as:

1. Maintaining integrity
2. Protecting privacy
3. Avoiding unauthorized access
4. Reporting findings honestly
5. Preserving evidence properly

Importance of Ethics in Cyber Forensics

Ethical behavior ensures:

- Fair investigation
- Trust in digital evidence
- Protection of individuals' rights

Forensic investigators must avoid:

- Altering evidence
- Accessing unrelated private data
- Misusing sensitive information

---

2. Digital Evidence Controls

Definition

Digital evidence controls refer to **procedures and measures used to protect digital evidence from tampering or loss**.

Digital evidence includes:

- Emails
- Files
- System logs
- Network traffic
- Images and videos
- Hard disk data

Characteristics of Digital Evidence

Digital evidence is:

1. Fragile
2. Easily modified
3. Easily duplicated

4. Difficult to detect if altered

Control Measures

To maintain evidence integrity, investigators must:

1. Use forensic tools
2. Maintain evidence logs
3. Secure storage systems
4. Create forensic duplicates
5. Use write blockers

Chain of Custody

Chain of custody is a **documented process showing who collected, handled, and analyzed evidence**.

It ensures that evidence has not been altered.

Chain of custody includes:

- Evidence ID
- Date of collection
- Investigator name
- Storage location
- Transfer records

---

3. Evidence Handling Procedures

Digital evidence must be handled carefully to maintain its **legal validity**.

Steps for Handling Digital Evidence

1. Identification

Identify potential digital evidence such as:

- Computers
- Mobile devices
- Storage media
- Network logs

---

2. Collection

Evidence should be collected using **forensic methods** to prevent modification.

Example:

- Creating disk images
- Using write blockers

---

3. Preservation

Evidence must be protected from:

- Damage
- Unauthorized access
- Data alteration

Methods include:

- Secure storage
- Access control

---

4. Documentation

All activities must be documented including:

- Collection method
- Tools used
- Analysis performed

---

5. Analysis

Investigators analyze evidence to find:

- Malware
- Unauthorized access
- Deleted files

---

6. Presentation

Evidence findings must be presented clearly in court using:

- Reports
- Charts
- Screenshots
- Expert testimony

---

4. Basics of Indian Evidence Act

The **Indian Evidence Act (1872)** defines rules for **admissibility of evidence in Indian courts**.

It determines:

- What evidence is acceptable
- How evidence should be presented

Digital Evidence in Indian Courts

Section **65B of the Indian Evidence Act** allows **electronic records to be used as evidence**.

Examples of electronic evidence:

- Emails
- Digital documents
- CCTV recordings
- Hard disk data

Section 65B Certificate

A certificate must be provided to confirm:

- Authenticity of electronic records
- Proper device operation
- Integrity of the data

Without this certificate, electronic evidence may not be accepted in court.

---

5. Indian Penal Code (IPC)

The **Indian Penal Code (IPC)** defines criminal offenses and punishments.

Some IPC sections related to cybercrime include:

- Fraud
- Identity theft
- Cheating
- Defamation
- Harassment

Cybercriminals may be charged under IPC along with cyber laws.

---

6. Criminal Procedure Code (CrPC)

The **Criminal Procedure Code (CrPC)** provides procedures for:

- Investigation
- Arrest
- Search and seizure
- Trial process

Role of CrPC in Cybercrime Investigation

CrPC allows law enforcement to:

- Conduct digital searches
- Seize computers and storage devices
- Collect digital evidence

Search warrants may be required before accessing digital devices.

---

7. Electronic Communications Privacy Act (ECPA)

The **Electronic Communications Privacy Act (1986)** is a U.S. law that protects electronic communications.

It regulates government access to:

- Emails
- Phone calls
- Electronic data

Components of ECPA

1. Wiretap Act

Protects real-time electronic communications.

Example:

Phone calls, voice chats.

---

2. Stored Communications Act

Protects stored electronic communications such as:

- Emails
- Messages stored on servers

---

3. Pen Register Act

Regulates the collection of dialing and routing information.

Importance

ECPA ensures that **privacy rights are protected during investigations**.

---

8. Legal Policies

Legal policies are **organizational rules and procedures designed to ensure compliance with laws**.

Organizations must create policies to regulate:

- Data usage
- Security procedures
- Employee conduct
- Incident reporting

Common Cyber Security Policies

1. Acceptable Use Policy (AUP)

Defines how employees may use computer systems.

---

2. Data Protection Policy

Ensures that sensitive information is protected.

---

3. Incident Response Policy

Provides guidelines for responding to cyber incidents.

---

4. Access Control Policy

Controls who can access systems and data.

Importance of Legal Policies

Legal policies help organizations:

- Prevent cybercrime
- Protect data
- Ensure legal compliance
- Reduce security risks

Short Exam Definitions

Digital Evidence:
Information stored or transmitted in digital form that can be used in legal investigations.

Chain of Custody:
A record showing how evidence has been handled and transferred during investigation.

Indian Evidence Act:
A law that defines rules for admissibility of evidence in Indian courts.

IPC:
The Indian Penal Code defines criminal offenses and punishments.

CrPC:
The Criminal Procedure Code provides procedures for investigation and trial.

Important Exam Questions (Unit-6)

Short Questions

1. Define digital evidence.
2. What is chain of custody?
3. What is Section 65B of the Indian Evidence Act?
4. What is IPC?
5. What is ECPA?

Long Questions

1. Explain laws and ethics in cybercrime investigation.
2. Describe digital evidence controls and handling procedures.
3. Explain the role of the Indian Evidence Act in digital forensics.
4. Discuss IPC and CrPC in cybercrime investigations.
5. Explain legal policies related to cybersecurity.