REFERENCE 📘 *A. Bhardwaj & K. Kaushik (2023) – Practical Digital Forensics*

- ✅ Definitions
- ✅ Goals
- ✅ Cybercrime and sources
- ✅ Digital evidence (types and locations)
- ✅ Forensics categories
- ✅ Data analysis
- ✅ Users
- ✅ Investigation types
- ✅ Forensics readiness
- ✅ Chain of custody
- ✅ Examination process

# 1. Introduction

Digital forensics is an Important part of modern cyber investigations. As technology becomes central to daily life and business, **cybercrime** has increased rapidly. To investigate these crimes, we need **scientific methods** to collect and analyze **digital evidence**.

📈 **Example:**
Every second, emails, transactions, and logs are created. When a crime happens (like data theft or fraud ), this information becomes vital evidence.

# 2. Defining Digital Forensics

🧠 **Definition:**
A branch of forensic science that applies **scientific techniques** to **identify, collect, preserve, analyze, and present** digital evidence in a court of law.

🎯 **Purpose:**
To find out:

- **What happened**
- **When it happened**
- **Who was responsible**

🧩 **Scope:**

- Computers (PCs, laptops)
- Mobile devices
- Internet of Things (IoT)
- Storage media (USBs, SSDs, CDs)

📜 **Principles:**

- Evidence must remain **authentic**
- Process must be **repeatable_ A repeatable process is one that can be done again by another investigator and will give the same findings.**
- Results must be **verifiable** and **legally admissible •**

# 3. Goals of Digital Forensics

1. **Preserve Evidence**
    - Prevent alteration or damage
2. **Follow Legal Procedures**
    - Ensure evidence is acceptable in court
3. **Assign Responsibility**
    - Identify the actor behind an activity
4. **Understand Incidents**
    - Detect data breaches and impacts o
5. **Document Clearly**
    - Create formal, understandable reports
6. **Support Legal Process**
    - Present evidence and testify in court

🧠 **Key Point:**
Integrity and accuracy are more important than speed.

# 4. Defining Cybercrime

⚖️ **Definition:**
Any **illegal activity** carried out **against or using** a computer or network.

💰 **Main Motives:**

- Financial gain
- Spy
- Disruption
- Revenge

💻 **Common Examples:**

- Phishing
- Identity theft
- Ransomware •
- Unauthorized access
- Denial of Service (DoS) • •
- Data theft and sabotage

# 5. Sources of Cybercrime

🔹 **1. Insider Threats**

- Employees, ex-staff, or contractors
- Already have authorized access
- Often harder to detect

🔹 **2. External Attackers**

- Hackers or cybercriminals
- Use phishing, malware, or stolen credentials
- May cooperate with insiders •

🧠 **Example:**
A disgruntled employee leaks data, or an outside hacker breaches the system using stolen passwords.

# 6. Computers in Cybercrimes

🧩 **Three Roles:**

1. **Computer as a Weapon**
    - Used to attack others (e.g., DoS, ransomware)
2. **Computer as a Target**
    - Victim of an attack (e.g., hacking or theft)
3. **Computer as a Tool**
    - Used to plan or assist crime (e.g., communication, storage)

🧠 **Example:**
A hacker uses one system to launch attacks (weapon), steals data from another (target), and hides stolen files on a third (tool).

# 7. Categories of Digital Forensics

🖥️ **1. Computer Forensics**

- Analysis of PCs, laptops, and drives
- Recover deleted files and logs

### 📱 2. Mobile Forensics

- Extract data from smartphones and SIMs
- Recover messages, call logs, GPS data

### 🌐 3. Network Forensics

- Capture and analyze network traffic

  The instruction **"Capture and analyze network traffic"** means you must **collect (capture)** data moving across a network and then **examine (analyze)** it to find useful information — like connections, websites visited, files transferred, or suspicious activity.
- Detect intrusions or data leaks •
- 💾 **4. Database Forensics**
- Investigate SQL logs and transactions
- Detect data manipulation or fraud

### ☁️ 5. Other Subfields

- **Cloud Forensics:** Virtual servers, SaaS
- **IoT Forensics:** Smart sensors and devices
- **Memory Forensics:** RAM and live data

# 8. Forensic Data Analysis

### 🧠 Focus:

Structured corporate data like:

- Databases
- Financial records
- Audit logs •
- 🔍 **Used For:**
- Fraud detection •

- Policy violation tracking •
- Pattern recognition

⚙️ **Techniques:**

- Log correlation=relationship •

  The term **“Log correlation”** means **combining and analyzing logs from different sources** to find **patterns, relationships, or evidence** that a single log alone cannot show.
- Timeline reconstruction •

  The phrase **“Timeline reconstruction”** means **building a chronological sequence of digital events** (what happened, when, and how) during an investigation.

- Behavior analysis

  The phrase **“Behavior analysis”** in **digital forensics** means studying **how a user, system, or attacker behaves** by examining **digital evidence** — to understand **patterns, intentions, and anomalies**.

# 9. Digital Forensic Users

👮 **Law Enforcement:**
Investigate criminal cases and present evidence in court.

🏢 **Corporate / Civil Litigation:**
Investigate fraud, theft, or employee misconduct.

🕵️ **Intelligence Agencies:**
National security, terrorism, and espionage.

⚖️ **Legal Professionals:**
Use digital evidence in lawsuits and trials.

🧠 **Key Idea:**
Digital forensics supports both **criminal** and **civil** justice systems.

# 10. Investigation Types

🔸 **Public Investigations**

- Run by **law enforcement**
- Based on **legal frameworks**
- Example: Police cybercrime unit investigating hacking

🔸 **Private Investigations**

- Done by **organizations**
- For internal issues: data leaks, policy violations •
- May later support court cases

# 11. Forensics Readiness

🧰 **Definition:**
The capability to collect, preserve, and use digital evidence **quickly and legally** when incidents occur.

🎯 **Goals:**

- Reduce investigation cost and time
- Ensure compliance with law
- Support faster response
- Detect threats early •
- ⚙️ **Measures:**
- Logging and monitoring
- Data keep policy •
- Incident response plan
- Secure evidence storage

🧠 **Think:** Preparedness = faster and more accurate investigations.

# 12. Types of Digital Evidence

📄 **User-Created Data:**

- Documents, images, emails, backups, encrypted files

⚙️ **Machine-Created Data:**

- Logs, registry, browser history, metadata, IP/MAC addresses •

📌 **Important:**
Both human and system data are essential to reconstruct events.

# 13. Locations of Digital Evidence

🖥️ **Devices:**

- PCs, laptops, servers
- Smartphones, IoT devices
- USBs, HDDs, SSDs
- Cloud storage

🌐 **Network Components:**

- Routers, switches, modems
- Firewalls, DVRs, GPS devices

🧠 **Explain:**
Evidence is everywhere — investigators must know **where to look**.

# 14. Chain of Custody

📜 **Definition:**
A record that **tracks the evidence** from collection to presentation..

📦 **Includes:**

- Who collected and handled the evidence
- When and how it was stored
- Tools used for analysis

🎯 **Goal:**
To keep integrity and acceptability in court.

Evidence can be **rejected** in legal proceedings

# 15. Examination Process

🧭 **Phases:**

1. **Search & Seizure**
    - Identify and collect devices legally
    - Capture volatile memory if possible
2. **Acquisition**
    - Create **forensic image** (bit-by-bit copy)
    - Use **write-blockers** to avoid tampering
3. **Analysis**
    - Use forensic tools (EnCase, FTK, Autopsy)
    - Recover deleted data, logs, hidden files
4. **Reporting**
    - Write clear, non-technical report
    - Submit evidence copies to court

🧠 **Explain:**
Each phase must be documented to ensure credibility.