💻 Lecture 25 – Digital Forensics

🔹 Introduction to Digital Forensics

Digital Forensics is the **science of collecting, analyzing, preserving, and presenting digital evidence** from computers, mobile devices, storage media, and networks to investigate cybercrimes or digital attacks.

It helps to **trace how an attack happened**, **who was responsible**, and **to recover or analyze the affected data**.

Example:
If a website like *CodingSeekho* gets hacked, the digital forensic investigator's job is to find:

- Who hacked it,
- How they entered,
- What data was accessed or modified, and
- How to prove it with evidence in court.

🔹 Main Objectives of Digital Forensics

1. **Identify** – Detect compromised systems, suspicious files, and attack traces.
2. **Preserve** – Secure evidence so it cannot be tampered with.
3. **Analyze** – Examine the collected data for clues.
4. **Document** – Record every step with timestamps and details.
5. **Present** – Prepare valid legal reports for court or investigation.

🔹 Types of Data in Digital Forensics

Digital forensics deals with **electronic data**, meaning any information stored or transmitted digitally:

- Documents, emails, chats
- Browser history
- Network logs
- System logs
- Photos, videos, or files
- Databases and application data

🔹 Types of Storage in Systems

Type	Meaning	Example	Description
Volatile Memory	Temporary memory (data lost when power off)	**RAM**	Used for active programs and processes.
Non-Volatile Memory	Permanent memory (data retained)	**SSD, HDD, USB Drive**	Used for long-term data storage.

💡 *Volatile = Temporary, Non-Volatile = Permanent*

Forensic experts analyze both types, because **RAM** contains live session data, passwords, network connections, and malware traces.

🔹 Write Blocker – Data Protection Device

A **Write Blocker** is used before copying data from the suspect's device.
It allows **read-only access**, meaning no one can edit, delete, or modify original evidence.

⚙️ Why Write Blocker is Used

- Prevents modification of timestamps or metadata.
- Protects evidence integrity.

- Ensures the data remains legally acceptable in court.

💡 Example:
If you connect a suspect's hard disk directly, your system might alter the file access time.
So, you connect it using a write blocker → then take its copy.

🔹 **Faraday Bag – Evidence Isolation**

After copying or seizing any digital device (like a phone, laptop, or tablet), investigators place it inside a **Faraday Bag**.

Faraday Bag is a shielded, signal-blocking bag that prevents all wireless signals like Wi-Fi, Bluetooth, GPS, or mobile networks.

⚙️ **Purpose:**

- Prevents remote data deletion or modification.
- Stops incoming/outgoing signals.
- Ensures safe preservation of evidence.

🔹 **Memory Analysis in Digital Forensics**

Memory analysis is used to extract live or stored data from RAM or virtual systems.
There are **5 common sources of memory data**:

Method	Description	Typical File / Location
1. Raw Format	Direct dump of system memory captured live.	Created using tools like FTK Imager, dd, DumpIt.
2. Crash Dump	Data captured when system crashes (BSOD).	File path: C:\Windows\MEMORY.DMP
3. Hibernation File	Stores system state during hibernation.	File: C:\hiberfil.sys

Method	Description	Typical File / Location
4. Page File	Virtual memory used when RAM is full.	File: C:\pagefile.sys
5. VMware Snapshot	Snapshot of virtual machine memory and state.	Files: .vmem / .vmsn inside VM folder

⚙️ **Tools for Memory Analysis:**

- **Volatility Framework**
- **Autopsy**
- **FTK Imager**
- **Magnet AXIOM**

These tools help recover passwords, malware traces, and running process details from memory.

🔹 **Steps of Digital Forensics Investigation**

1. **Identification** – Detect attack or compromised system.
2. **Preservation** – Isolate system (disconnect from network).
3. **Collection** – Create a forensic image (bit-by-bit copy).
4. **Examination** – Inspect files, logs, and hidden data.
5. **Analysis** – Reconstruct events and gather proof.
6. **Reporting** – Prepare documentation and timeline of events.

🔹 **Forensic Imaging**

Once the system is isolated, investigators create a **forensic image** of the storage drive.

A **Forensic Image** is a *bit-by-bit copy* of the original storage media.

⚙️ **Why It's Important:**

- The original disk remains untouched.
- All analysis is done on the image copy.
- Legally accepted in court (if chain of custody maintained).

🧰 **Tool Used:**

FTK Imager

Steps:

1. Connect suspect drive using **write blocker**.
2. Open **FTK Imager → Create Disk Image**.
3. Select the target drive and destination folder.
4. Generate image (.E01 or .dd).
5. Verify hash value (MD5/SHA256).

🔹 **Evidence Used to Prove Innocence (In Court)**

If a client claims a cyberattack occurred on their system, the forensic expert gathers the following evidence to prove what actually happened:

1. **Browser History** – Shows what sites were visited.
2. **Installed Software List** – Checks for unknown or malicious programs.
3. **Network Monitoring Logs** – Identifies suspicious IP connections.
4. **Search & Process Records** – Shows running applications or services.
5. **Temporary Files & AppData** – Reveal deleted or recent activities.
6. **System Logs** – Provide event data such as login/logout times.
7. **Network Traffic** – Helps detect data exfiltration or intrusion.

This data shows **whether the attack was user-side or server-side**.

🔹 Disk Architecture Overview

A storage disk is structured into several key areas:

Component	Description
MBR / Boot Sector	Contains partition and boot information.
File System Area	Defines file structure (NTFS, FAT32, etc.).
Data Area	Stores actual files and user data.
Slack Space	Unused or leftover space in file clusters.

🔹 Slack Space (Hidden Data Recovery)

Slack Space is the small leftover area when a file doesn't completely fill a disk cluster.

🧩 Example:
If a file takes 3 KB but the cluster size is 4 KB → 1 KB remains unused (slack space).
Old or deleted data might still exist there.

Forensic experts use **Autopsy** or **FTK Imager** to recover data from slack space.

🔹 Autopsy Tool – Forensic Data Analysis

Autopsy is a graphical tool for forensic analysis, part of *The Sleuth Kit (TSK)*.

⚙️ **Functions:**

- Recover deleted or hidden files.
- Analyze file modification history.
- Detect changes in file extensions or timestamps.
- Examine browser history, email, and logs.
- Generate comprehensive investigation reports.

Autopsy helps determine:

- When a file was created or modified.
- If its extension was changed (e.g., .jpg to .exe).
- Evidence of tampering.

🔹 Chain of Custody (Legal Evidence Handling)

The **Chain of Custody (CoC)** ensures that **digital evidence is properly documented and tracked** from collection to courtroom presentation.

⚙️ Steps Involved:

1. **Preservation** – Secure the original device immediately.
2. **Documentation** – Record date, time, collector's name, and device details.
3. **Tracking** – Maintain record of every transfer.
4. **Acknowledgement** – Each handler signs and dates the log.
5. **Integrity Check** – Verify with hash values to ensure no alteration.

If the CoC is broken, the evidence can be **rejected in court**.

🔹 Additional Areas in Digital Forensics

1. Computer Forensics

Focuses on computers, hard drives, and file systems.
Used to find malware, logs, or deleted files.

2. Network Forensics

Monitors and analyzes network packets.
Tools: *Wireshark, TCPDump, NetworkMiner*

3. Mobile Forensics

Extracts data from phones, SIMs, and apps.
Tools: *Cellebrite, Oxygen Forensics*

4. Cloud Forensics

Analyzes cloud platforms (AWS, Azure, Google Cloud).
Involves API logs, access records, and virtual disk images.

5. Database Forensics

Examines database transactions, queries, and logs.
Used in cases of data theft or record manipulation.

6. Email Forensics

Tracks sender identity, header info, timestamps, and IPs.
Used in phishing, spam, and fraud investigation.

🔹 Popular Tools in Digital Forensics

Tool	Use
FTK Imager	Create forensic images
Autopsy / Sleuth Kit	Analyze and recover data
Volatility	Memory and RAM analysis
Wireshark	Network traffic analysis
EnCase	Professional forensic suite
Cellebrite UFED	Mobile data extraction
Magnet AXIOM	End-to-end digital evidence management

🔹 Why Digital Forensics is Important

- Detects and investigates cybercrimes.
- Helps recover lost or deleted data.
- Proves innocence or guilt in court.
- Protects organizations from insider threats.
- Improves cybersecurity policies.

🧩 Complete Forensic Workflow

Incident Detected

↓

Isolate the System (Preserve Evidence)

↓

Use Write Blocker → Take Forensic Image

↓

Store Device in Faraday Bag

↓

Analyze Image (Autopsy / Volatility)

↓

Recover Hidden or Deleted Files

↓

Prepare Investigation Report

↓

Maintain Chain of Custody

↓

Submit in Court as Digital Evidence

🧠 Extra Key Concepts

🔸 Hashing in Forensics

A hash (MD5/SHA256) is a unique fingerprint of a file.
If the hash value changes → data has been modified.
Used for verifying evidence integrity.

🔸 Timeline Analysis

Reconstructs the sequence of events (creation, modification, access times).
Helps determine when and how an attack occurred.

🔸 **File Carving**

Technique to recover files from unallocated or corrupted disk space.

🔸 **Log Analysis**

System and application logs reveal unauthorized access or suspicious activities.

✅ **Summary**

- **Digital Forensics** = Investigation of digital crimes.
- **Write Blocker & Faraday Bag** = Protect evidence.
- **Memory Analysis** = Retrieve data from volatile memory.
- **FTK Imager** = Create disk image.
- **Autopsy** = Analyze & recover data.
- **Chain of Custody** = Legal tracking of evidence.
- **Slack Space** = Hidden data recovery area.
- **Goal** = To prove truth using digital evidence.