Unit VIII: Introduction to Auditing and Digital Forensic

- Auditing
- Monitoring
- Digital Forensic :Team , methodology and procedure

1. Auditing

Auditing is the systematic, independent examination of a system, process, or product to determine its compliance with specific requirements, policies, or standards. In IT, it's about "checking the homework" of the security system.

- **Purpose:** To provide assurance that security controls are functioning as intended and to identify gaps in compliance (e.g., ISO 27001, GDPR, or SOC2 **GDPR:** General Data Protection Regulation **SOC 2:** System and Organization Controls 2).

  - **Types of Audits:**
    - **Internal Audit:** Conducted by members of the same organization to prepare for external reviews.
    - **External Audit:** Conducted by an independent third party to provide an unbiased opinion.
  - **Key Audit Activities:**
    - Reviewing user access logs and permissions.
    - Evaluating password policies and encryption standards.
    - Testing physical security (server room access).
    - Verifying software patch management cycles.

2. Monitoring

While auditing is a periodic "snapshot," **Monitoring** is an ongoing, real-time process. It involves the continuous observation of systems to detect anomalies, performance issues, or security threats.

- **Key Components:**
  - **Log Management:** Collecting data from firewalls, routers, and servers.
  - **SIEM (Security Information and Event Management):** Tools that aggregate logs and use AI/rules to alert admins of suspicious patterns.
  - **Intrusion Detection Systems (IDS):** Monitoring network traffic for signs of a breach.

3. Digital Forensics

Digital forensics follows a strict, step-by-step process to ensure the evidence isn't tampered with.

Digital Forensics is the practice of collecting, preserving, and analyzing digital evidence in a way that is legally admissible.

A. The Digital Forensic Team

A successful investigation requires a multidisciplinary team:

- **Lead Investigator:** Manages the case and coordinates the team.
- **Evidence Technician:** Responsible for the "Chain of Custody" and secure storage.
- **Forensic Analyst:** The "deep-diver" who recovers deleted files and analyzes metadata.
- **Legal Counsel:** Ensures the investigation follows privacy laws and search warrant requirements.
- **IT Specialist:** Provides technical context for specific infrastructure or proprietary software.

B. Methodology and Procedure

1. **Identification:** You arrive at the scene. Do you take the laptop? The USB drive? The smartwatch? You must identify where the "evidence" lives.
2. **Preservation:** This is the most important step for to remember.
    - You use a **Write Blocker**. This is a hardware device that allows you to read data from a drive but physically prevents your computer from writing even 1 bit of data back to it.
    - You create a **Forensic Image** (a bit-by-bit copy). If the hard drive has 500GB of data, your copy is exactly 500GB, including the "empty" space where deleted files might be hiding.
    - **Hashing:** Using algorithms like MD5 or SHA-256 to create a "digital fingerprint" of the data to prove it hasn't changed.
3. **Analysis:** This is where the detective work happens.
    - **Metadata Analysis:** Looking at the "data about data" (e.g., a photo's GPS coordinates or the date a Word doc was created).
    - **Carving:** Recovering files that were "deleted" but haven't been overwritten yet.
    - Using tools (like EnCase or FTK) to find hidden files, browser history, registry entries, and deleted data.
4. **Documentation/Reporting:** You must be able to explain your technical findings to a judge or jury who may not know what a "hard drive" actually is.

How "Deleted" Files are Recovered (File Carving)

When you "delete" a file on your computer, it isn't actually erased immediately. Instead, the Operating System just deletes the "pointer" to that file and marks that space as "Available."

Think of a book: deleting a file is like tearing out the **Table of Contents** but leaving all the **Chapters** inside. As long as you don't write new "chapters" (new data) over them, they are still there.

The Technique: Header and Footer Analysis

Forensic tools look for specific "Signatures" (Magic Numbers) in the raw data of a hard drive:

- **JPEG files** always start with the hex code FF D8 FF.
- **PDF files** always start with %PDF.

The software scans the entire drive. When it finds FF D8 FF, it knows a photo starts there. It keeps reading until it finds the "Footer" (the end of the file) and "carves" that chunk of data out to recreate the image.

2. Order of Volatility: What to Grab First?

In a crime scene, a forensic investigator has to act fast because some evidence "evaporates." This is known as the **Order of Volatility**. You always collect the most "fragile" data first.

Priority	Data Type	Why?
1. Highest	**CPU Cache & RAM**	If you pull the power plug, this data is gone forever. It contains active passwords and unencrypted messages.
2. High	**Network State**	Shows who the computer was talking to (IP addresses) at the moment of the crime.
3. Medium	**Hard Drive (Disk)**	This is "Non-Volatile." It stays even when the power is off, so it can wait a few minutes.
4. Lowest	**Backups & Printouts**	These are physically stable and won't change.

The Forensic Toolkit

As a student, you might want to know the names of the industry-standard software used to perform these tasks:

- **Autopsy / Sleuth Kit:** A very popular open-source tool used for disk analysis. It's great for students to practice with.
- **FTK Imager:** Used specifically for the "Preservation" stage—it creates the forensic image and calculates the Hash (MD5/SHA) to prove integrity.
- **Wireshark:** The go-to tool for **Network Forensics**. It captures "packets" of data moving across a wire.
- **Volatility:** A specialized tool used only for analyzing **RAM** (Memory forensics).

4. Summary Table: Auditing vs. Monitoring vs. Forensics

This is a great cheat sheet for exams:

Feature	**Auditing**	**Monitoring**	**Digital Forensics**
Main Goal	Compliance & Accuracy	Speed & Security Alerts	Evidence & Investigation
Timeline	Past (Historical)	Present (Real-time)	Post-Incident (After the fact)
Analogy	A Tax Audit	A Security Guard	A Detective
Key Output	Audit Report	Alert/Dashboard	Expert Testimony/Legal

The Case: "Operation Insider Threat"

Phase 1: Monitoring (The Trigger)

It is Tuesday at 2:00 AM. The company's **SIEM (Security Information and Event Management)** tool flags a suspicious event.

- **The Event:** An employee's account (Upadesh) just logged in from an IP address in a different country and is downloading 50GB of sensitive design files.
- **The Action:** The monitoring system sends an automated alert to the Security Operations Center (SOC).

Phase 2: Auditing (The Background Check)

The security team needs to know: *Is this normal?* They perform an immediate **Audit** of Upadesh access logs and HR records.

- **The Discovery:** The audit reveals that Upadesh submitted his resignation letter yesterday. It also shows he was granted "Admin" privileges last month for a project that ended two weeks ago—meaning his access was never revoked (a compliance failure found via auditing).

Phase 3: Digital Forensics (The Investigation)

Now that the company suspects Upadesh is stealing intellectual property (IP), the **Digital Forensic Team** is called in to gather evidence for a potential lawsuit.

1. Identification: The team identifies Upadesh company laptop, his corporate cloud account, and the office security camera footage as key evidence.

2. Preservation:

- They pull the laptop from his desk.
- They use **FTK Imager** to create a bit-for-bit forensic image of the drive.
- They calculate the **Hash Value** (e.g., SHA-256) of the image.
    - *Original Hash:* 5d41402abc4b...
    - *Copy Hash:* 5d41402abc4b... (Matches! Evidence is intact).

3. Analysis: The analyst uses a tool like **Autopsy** to look into the "unallocated space" (deleted areas) of the hard drive.

- **The "Smoking Gun":** They find evidence that Upadesh plugged in a personal USB drive at 1:45 AM.
- **File Carving:** They recover a deleted PDF titled "Secret_Project_Draft" that Upadesh tried to hide by deleting it after copying it to his USB.
- **Metadata:** They find a Chrome browser history entry showing Upadesh searched for "how to delete history permanently" and "competitor job openings."

4. Reporting & Presentation: The team creates a detailed report. Because they followed the **Methodology** (Write blockers, Hashing, and Chain of Custody), the evidence is strong enough to be used in court to sue Upadesh for theft of trade secrets.

****