1) explain the use of forensic science with an appropriate example. Explain forensic science.

1) What is Forensic Science?

(Write these 3 points.)

1. **Forensic Science is the scientific method of collecting, examining, and analyzing evidence** related to a crime.
   DF1_1
2. It helps **establish facts** by using scientific tests and techniques.
3. The evidence collected is **used in the court of law** to solve crimes and identify the criminal.

2) Uses of Forensic Science

(Write any 3 points.)

1. **To prove elements of a crime scene** using scientific evidence. DF1_1
2. **To identify suspects or victims** from the evidence found.
3. **To establish a link** between the suspect, victim, and the crime (e.g., fingerprints, DNA, digital data).
4. **To verify or disprove statements** given by suspects or witnesses.
5. Helps solve cases that **cannot be solved by traditional methods** using advanced scientific techniques.
   DF1_1

(You can write any 3-4 in exam.)

3) Example of Forensic Science

Write one simple example in exam:

Example:

Police find a **mobile phone** at a crime scene.
Digital forensic experts recover **deleted messages, call logs, and location history** from the device.
This evidence helps identify the suspect and proves their involvement in the crime.

(OR you can write:)
Fingerprints found on a weapon are matched in the forensic lab and used to identify the criminal.

2) List and explain in brief about applications of digital forensic.

- Crime Detection- There are various malwares and malicious activities that happen over digital media and networks, such as phishing, spoofing, ransomware, etc.
- Crime Prevention- There are various cyber crimes that happen due to lack of security or existing unknown vulnerabilities, such as zero-day vulnerability. Cyber forensics helps in finding out these vulnerabilities and avoiding such crimes to occur.
- Crime Analysis- This is the main application of digital forensics
- Preservation- This process involves protecting the crime scene and the digital evidence or setup from further manipulation and photographing and videographing the crime scene, for future reference. Also this process involves stopping any ongoing command that may be linked to the crime.

- Financial fraud detection.
- Criminal Prosecution
- Civil Litigation (evidence in court cases and proceedings)
- Corporate Security Policy and Acceptable Use Violations
  - Embezzlement (Misuse, fraud, cheating etc.)
  - Email threats data theft-industrial espionage (spying, intelligence units)

Criminal Prosecution means the **legal process in which the government (police + court) takes action against a person who is accused of committing a crime.**

3) What is digital forensics explain its process, Uses of digital forensics, Challenges of digital forensics, Branches of digital forensics, purpose of digital forensics.

- Digital forensic science is
  - A branch of forensic science that focuses on the recovery and investigation of material found in digital devices related to cybercrime.
  - The process of identifying, preserving, analyzing, and documenting digital evidence. This is done in order to present evidence in a court of law when required.
  - The process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information to reconstruct past events.

Process of Digital forensic

- Digital forensics process involves the following steps:
  - Identification
  - Preservation
  - Analysis
  - Documentation
  - Presentation

- Identification
  - It is the first step in the forensic process.
  - Mainly includes things like what evidence is present, where it is stored and lastly, how it is stored (in which format).
  - Electronic storage media can be personal computers, Mobile phones, PDAs, Laptops, HDD, etc.
- Preservation
  - In this phase, data is isolated, secured, and preserved.
  - It includes preventing people from using the digital device so that digital evidence is not tampered with.

- Analysis
  - In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found.
  - It might take numerous iterations of examination to support a specific crime theory.
- Documentation
  - In this process, a record of all the visible data must be created.
  - It helps in recreating the crime scene and reviewing it.
  - It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

- Presentation
  - In this last step, the process of summarization and explanation of conclusions is done.
  - It should be written in a layperson's terms using abstracted terminologies. All abstracted terminologies should reference the specific details.

Challenges faced by Digital Forensics

Here, are major challenges faced by the Digital Forensic:

- The increase of PC's and extensive use of internet access
- Easy availability of hacking tools
- Lack of physical evidence makes prosecution difficult.
- The large amount of storage space into Terabytes that makes this investigation job difficult.
- Any technological changes require an upgrade or changes to solutions.

- The major challenges are the growing number and size of evidence to be analyzed and the cybercriminals being equally equipped with anti-forensic tools to erase that digital evidence or to produce a delay in the digital evidence generation process.
- Few of the current challenges in the field of digital forensics are listed here.
- Digital Media types
  - There are various digital devices used these days.
  - The technique used for one specific device cannot be used for some other device because of the different characteristics of each device.
  - The digital forensic expert must be equipped with the use of software for analysis and also the device being analyzed.

- Online Disks
  - The large firms store their data on online disks.
  - Generate a huge amount of data on online disks
  - Imaging of such huge data takes a lot of time and also requires the firm to shut their services until the imaging is complete.
- Anonymity of the IP-
  - This is one of the big challenge to cyber forensics.
  - IP address allows network identification and location addressing of a device connected to a network.
  - IP address can easily be spoofed by cybercriminals and hence can become a hindrance in the address location of the device.
  - Similar to IP address spoofing, there is MAC address and email address spoofing as well that becomes a challenge for the digital forensic expert.
- Anti- Digital Forensic-
  - This is used by cybercriminals and also used legitimately by individuals who want to protect their privacy.
  - Anti-digital forensics is a set of techniques and measures used to slow down or incapacitate the process of investigation by manipulating, erasing, or obscuring the data.
  - Most commonly used anti-digital forensic techniques is RootKit that has been used by cybercriminals for years to hide the activities of the malicious code.
- Testing and Validation-
  - With the cybercriminals getting more equipped, there is always a need to update the software to efficiently analyze the evidences and also provide valid results that can be made admissible in the court of law, like the use of Virtual Machines.
  - It is a forensic investigation tool that allows the investigators to clone the image from the target computer, virtually, but when the image is booted on a machine with different hardware, it installs the missing drivers and thus makes the image a modified one, thus renders it inadmissible in the court of low.

Types of Digital Forensics

- Disk Forensics:
  - It deals with extracting data from storage media by searching active, modified, or deleted files.
- Network Forensics:
  - It is a sub-branch of digital forensics related to monitoring and analysis of computer network traffic to collect important information and legal evidence.
- Wireless Forensics:
  - It is a division of network forensics.
  - Offers the tools need to collect and analyze the data from wireless network traffic.

- Database Forensics:
  - It is a branch of digital forensics relating to the study and examination of databases and their related metadata.
- Malware Forensics:
  - This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.
- Email Forensics
  - Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.
- Memory Forensics:
  - It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.
- Mobile Phone Forensics:
  - It deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

⭐ 1) Purpose of Digital Forensics (Easy Points)

(What digital forensics tries to achieve)

1. **To identify digital evidence** from computers, mobiles, networks, etc.
2. **To preserve the evidence** in its original form without tampering.
3. **To analyze data** (deleted files, logs, emails, browser history, etc.) scientifically.
4. **To reconstruct events** and understand "what happened" in the cybercrime.
5. **To find out who committed the crime** using digital clues.
6. **To present the digital evidence in court** in a legally acceptable manner.
7. **To maintain chain of custody**, ensuring evidence is handled properly.

⭐ Uses of Digital Forensics (GTU – 4 Marks)

The **uses** are the *practical applications* of digital forensics in the real world.

1. **Criminal Investigations**
   - Used to detect cybercrimes like hacking, phishing, identity theft, cyberstalking, fraud.
   - Helps recover deleted files, messages, call logs, browser history, etc.
2. **Corporate and Legal Investigations**
   - Used to detect employee misconduct, data leakage, IP theft, policy violations, and financial fraud.
3. **Incident Response & Cybersecurity**
   - Helps organizations find malware, analyze attacks, detect unauthorized access, and prevent future breaches.
4. **Data Recovery**
   - Recovers deleted, formatted, hidden, or encrypted data from computers, mobiles, HDD, SSD, etc.
5. **Court Evidence Support**
   - Provides scientific, verifiable digital evidence to support court cases and legal disputes.
6. **Tracking Terrorists or Criminal Networks**
   - Helps track online activity, emails, social media logs, and communication patterns.

1) Define active data, Latent data and archive data.

1) Active Data

Active Data is the data that is currently visible, usable, and accessible to the user.

Examples: files on desktop, documents, images, videos, folders you can open normally.

✔ This is the data we use daily and can directly see on the screen.

---

2) Latent Data

Latent Data is the hidden or deleted data that is not directly visible to the user but still exists on the storage device.

Examples: deleted files, fragments in unallocated space, data in cache, slack space.

✔ It requires **digital forensic tools** to recover it.

---

3) Archive Data

Archive Data is old data stored for long-term backup or reference and not used in daily operations.

Examples: backup drives, old emails, compressed zip files, cloud backups.

✔ This data is stored safely and only accessed when needed.

2) Explain cloud computing with its different types of services.

⭐ Cloud Computing (Easy Definition – Write in Exam)

Cloud computing is a technology that allows users to store, access, and use data, software, and services over the internet instead of using their own computer's storage or hardware.

In simple words:

✔ You don't need to install software → you use it online.
✔ You don't need your own server → cloud provider gives resources.
✔ You can access your data from anywhere, anytime.

Examples: Google Drive, Gmail, AWS, Microsoft Azure, Dropbox.

⭐ Features of Cloud Computing (short points)

(Write any 3–4 if needed)

- On-demand access (use whenever needed)
- Pay-as-you-go (pay only for what you use)
- Scalability (increase/decrease resources easily)
- Accessible from anywhere
- No need to maintain hardware

⭐ Types of Cloud Services (SERVICE MODELS)

These are the **three main service models** of cloud computing:

⭐ 1) IaaS – Infrastructure as a Service

It provides virtual hardware resources over the internet.

You get:

- Virtual machines
- Storage
- Networks
- Servers

You manage your own software, applications, OS.

✔ **Example:** AWS EC2, Google Compute Engine, Microsoft Azure VM

Easy example:
Instead of buying a physical computer or server, you rent a virtual machine from the cloud.

⭐ 2) PaaS – Platform as a Service

It provides a full platform for developers to build, test, and deploy applications.

You get:

- Development tools
- Runtime environment
- Databases
- Operating System

You only focus on coding; cloud handles everything else.

✔ **Example:** Google App Engine, Microsoft Azure App Service

Easy example:
You just write code, and the cloud handles the environment, OS, and updates.

⭐ 3) SaaS – Software as a Service

It provides ready-to-use software over the internet.

You don't install anything; just login and use.

Examples:

- Gmail
- Google Docs
- Microsoft 365
- Zoom
- Salesforce

Easy example:
Using Gmail without installing any email software — everything works online.

3) What is cache memory? Explain direct mapping of cache memory with an example.

⭐ 1) What is Cache Memory? (Easy + Detailed)

Cache memory is a small, very fast memory located between the CPU and the main memory (RAM).
Its job is to **store frequently used instructions and data** so the CPU can access them quickly.

✔ Why do we need Cache?

CPU is extremely fast → RAM is slower.
So if CPU waits for data from RAM every time → system becomes slow.

Cache solves this by storing the data that CPU needs again and again.

⭐ Features of Cache Memory (Write any 4–5)

1. **Very fast memory** (faster than RAM)
2. **Stores most frequently used data**
3. **Reduces CPU waiting time**
4. **Improves overall system performance**
5. **Smaller in size but costly**
6. **Located close to CPU (on-chip or near processor)**

⭐ 2) Direct Mapping in Cache Memory (Easy Explanation)

Direct Mapping is the **simplest technique** to place data from main memory into the cache.

✔ Simple Idea:

Each memory block is mapped (assigned) to **one fixed cache line only**.

Formula:

Cache Line Number = (Main Memory Block Number) MOD (Number of Cache Lines)

✔ Means:

- Every block has **only one place** in the cache where it can go.
- Even if cache lines are empty, the block must go to *its* assigned line.

⭐ 3) How Direct Mapping Works? (Super Easy Steps)

1. **Main Memory is divided into blocks.**
2. **Cache is divided into lines.**
3. Each block from main memory can go to **only one fixed cache line** using MOD formula.
4. If two blocks map to the same line → **they replace each other** (conflict).

⭐ 5) Simple Real-Life Example (for understanding)

Think of 4 parking slots (cache lines).
Each house number (memory block number) decides its parking slot using:

House number mod 4

So:

- House 4, 8, 12 → always park in slot 0
- House 1, 5, 9 → always slot 1

Even if other slots are empty,
they **must** park in their fixed slot → just like direct mapping.

⭐ 6) Advantages of Direct Mapping

1. Very **simple** to understand and implement
2. **Fast** because position is fixed
3. **Low hardware cost**

⭐ 7) Disadvantages of Direct Mapping

1. High **conflict misses** (many blocks map to same line)
2. Cache line gets replaced frequently
3. Not suitable for large programs that access many blocks

4) Explain functional model of IOT.

⭐ Functional Model of IoT (Easy Explanation + 3 Marks Answer)

The **Functional Model of IoT** explains **how an IoT system works step-by-step.**
It shows the main functions needed for any IoT device to collect data, send it, process it, and perform actions.

IoT = Devices + Network + Cloud + Applications

⭐ Functions in IoT (Explain these 5 steps in exam)

1) Sensing (Data Collection)

IoT devices have sensors like temperature, motion, light, humidity, GPS, etc.
These sensors **collect real-world data.**

✔ Example: Temperature sensor measuring room temperature.

---

2) Communication (Data Transfer)

After sensing, the device sends data using communication technologies like:

- Wi-Fi
- Bluetooth
- RFID
- Zigbee
- 4G/5G

✔ Example: Smartwatch sending heart rate to mobile via Bluetooth.

3) Data Processing (Computation)

The received data is processed in:

- Microcontroller
- Edge device
- Cloud server

Processing includes filtering, analysis, decision making.

✔ Example: Cloud analyzes temperature data to check if AC should be ON or OFF.

---

4) Storage (Saving Data)

IoT systems store data for future use.

Storage can be:

- Cloud database
- Local device memory
- Edge storage

✔ Example: Smart home app stores past electricity usage.

---

5) Application (Action & Output)

The final function is performing action or giving output:

- Sending notifications
- Controlling devices
- Showing real-time data

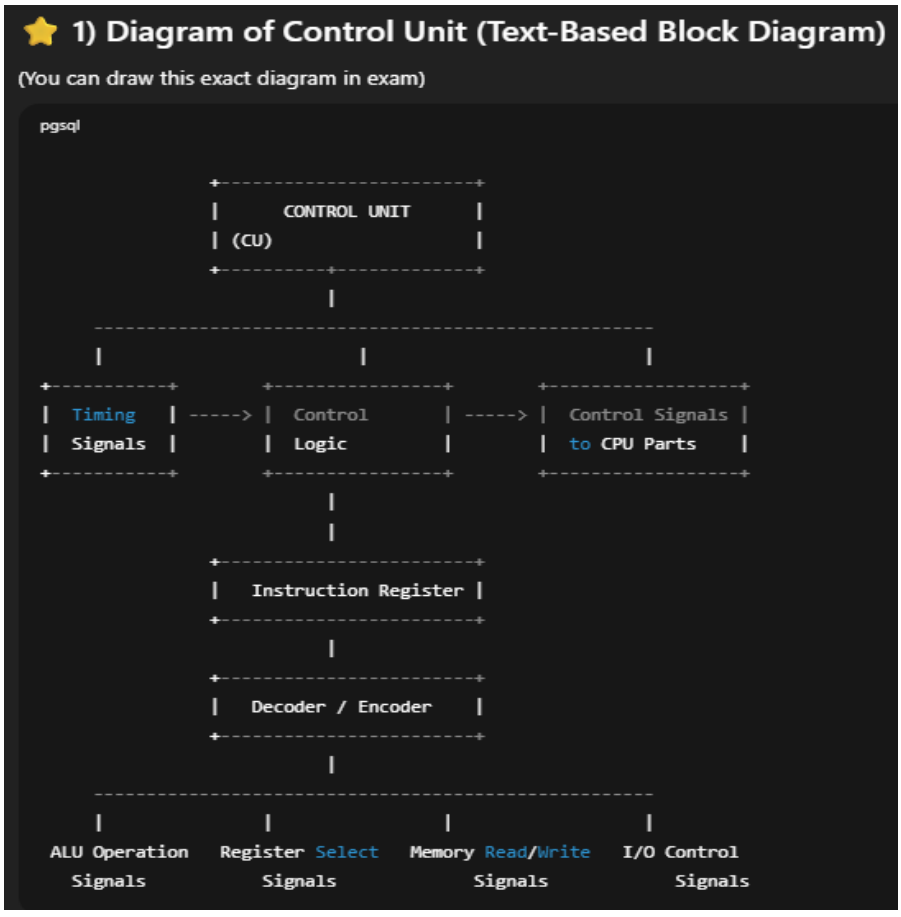
✔ Example: Turning ON fan automatically when room is hot.

5) Draw and explain control unit of basic computer.

⭐ 1) Diagram of Control Unit (Text-Based Block Diagram)

(You can draw this exact diagram in exam)

pgsql



⭐ 2) What is Control Unit? (Easy Explanation)

A Control Unit (CU) is the part of the CPU that controls the entire operation of the computer.
It does **not** perform calculations — but it **tells all parts of the CPU what to do, when to do, and how to do it.**

⭐ In simple words:

"Control Unit is the brain inside the CPU which sends signals to control ALU, registers, memory, and I/O devices."

⭐ 3) Functions of Control Unit

(Write any 5–6 points for marks)

1. **Fetches instructions** from memory.
2. **Decodes instructions** using the instruction decoder.
3. **Generates timing and control signals** for ALU, memory, registers, and I/O.
4. **Controls data flow** inside the CPU.
5. **Coordinates between CPU and memory.**
6. **Executes instructions** by sending necessary control commands.
7. **Maintains sequence of operations** using the clock.

⭐ 4) Explanation of Components (Detailed and Easy)

⭐ (1) Instruction Register (IR)

- Holds the current instruction fetched from memory.
- CU reads this instruction to understand what operation is needed.

Example:
If instruction = ADD R1, R2 → IR stores this.

⭐ (2) Instruction Decoder

- Decodes the instruction stored in IR.
- Converts it into internal bits that tell the system:
  - ✔ which operation?
  - ✔ which register?
  - ✔ which memory address?

Example:
ADD → tells ALU to perform addition
R1 → select register 1
R2 → select register 2

⭐ (3) Timing Signals (Clock)

- Provides timing (T0, T1, T2...) to perform steps in order.
- Ensures one operation happens at the correct time.

Example:
T0 → fetch
T1 → decode
T2 → execute

⭐ (4) Control Logic

- The central part of the CU.
- Uses the decoded instruction + timing signals to generate control signals.

Example:

If instruction is ADD, CU generates:

- ✔ ALU_Add = 1
- ✔ Load_ACC = 1
- ✔ Read_R1 = 1
- ✔ Read_R2 = 1

⭐ (5) Control Signals to CPU Components

CU sends signals to:

✔ **ALU**

- Tells ALU which operation to perform (ADD, SUB, AND, etc.)

✔ **Registers**

- Which register to read/write
- When to load data
- When to increment the PC

✔ **Memory**

- Read or Write signal
- Address select signal

✔ **I/O**

- Input/Output enable signals

⭐ 5) Working of Control Unit (Step-by-Step)

Step 1: Fetch

CU fetches the instruction from memory into the Instruction Register (IR).

Step 2: Decode

CU decodes the instruction using the instruction decoder.

Step 3: Generate Control Signals

CU generates necessary control signals based on the decoded instruction.

Step 4: Execute

CU sends signals to ALU, registers, and memory to perform the operation.

Step 5: Move to Next Instruction

CU increments Program Counter and repeats the cycle.

6) Explain main memory and auxiliary memory with example.

⭐ 1) MAIN MEMORY (Primary Memory)

✔ Definition (Easy)

Main memory is the memory that the CPU can access directly. It stores data and instructions that are currently being used or processed by the computer.

It is also called **Primary Memory** or **Internal Memory.**

⭐ 2) Features of Main Memory

1. **Directly accessed by CPU**
2. **Fast and expensive** compared to auxiliary memory
3. **Volatile** → data is lost when power is off
4. Stores programs that are currently running
5. Limited storage capacity compared to secondary storage

⭐ 3) Types of Main Memory

a) RAM (Random Access Memory)

- Temporary memory
- Stores currently used programs
- Data is lost when power is off

  Example: Opening MS Word → RAM stores it temporarily.

b) ROM (Read Only Memory)

- Permanent memory
- Stores system instructions
- Data is NOT lost when power is off

  Example: BIOS stored in ROM.

⭐ 4) Examples of Main Memory

- RAM (4GB, 8GB, 16GB)
- ROM
- Cache Memory
- Registers

⭐ 2) AUXILIARY MEMORY (Secondary Memory)

✔ Definition (Easy)

Auxiliary memory is long-term storage used to store data permanently. It is not directly accessed by CPU but used for backup and long-term storage.

It is also called:

- **Secondary Memory**
- **External Memory**
- **Backup Memory**

⭐ 2) Features of Auxiliary Memory

1. **Large storage capacity** (GB → TB)
2. **Cheaper** than main memory
3. **Non-volatile** → data stays even after power off
4. Slower compared to main memory
5. Used for long-term storage of files, software, OS

⭐ 3) Types of Auxiliary Memory

a) Magnetic Storage

- Hard Disk Drive (HDD)
- Magnetic Tapes

b) Optical Storage

- CD, DVD, Blu-ray

c) Solid-State Storage

- SSD
- Pen Drive
- Memory Card

⭐ 4) Examples of Auxiliary Memory

- HDD (1TB)
- SSD (256GB)
- Pen Drive (32GB)
- CD/DVD
- Google Drive / Cloud Storage

7) Explain Bits, bytes and number scheme.

⭐ 1) Bit (Binary Digit)

A bit is the smallest unit of data in a computer. It can have only two values: 0 or 1.

- 0 = OFF
- 1 = ON
- Used to represent binary information.
- All computer data (numbers, images, videos) are stored as bits.

Example:

1011 contains 4 bits.

⭐ 2) Byte

A byte is a group of 8 bits.

It is the basic unit used to measure memory/storage.

✔ Byte Conversions

- 1 Byte = 8 bits
- 1 KB = 1024 Bytes
- 1 MB = 1024 KB
- 1 GB = 1024 MB

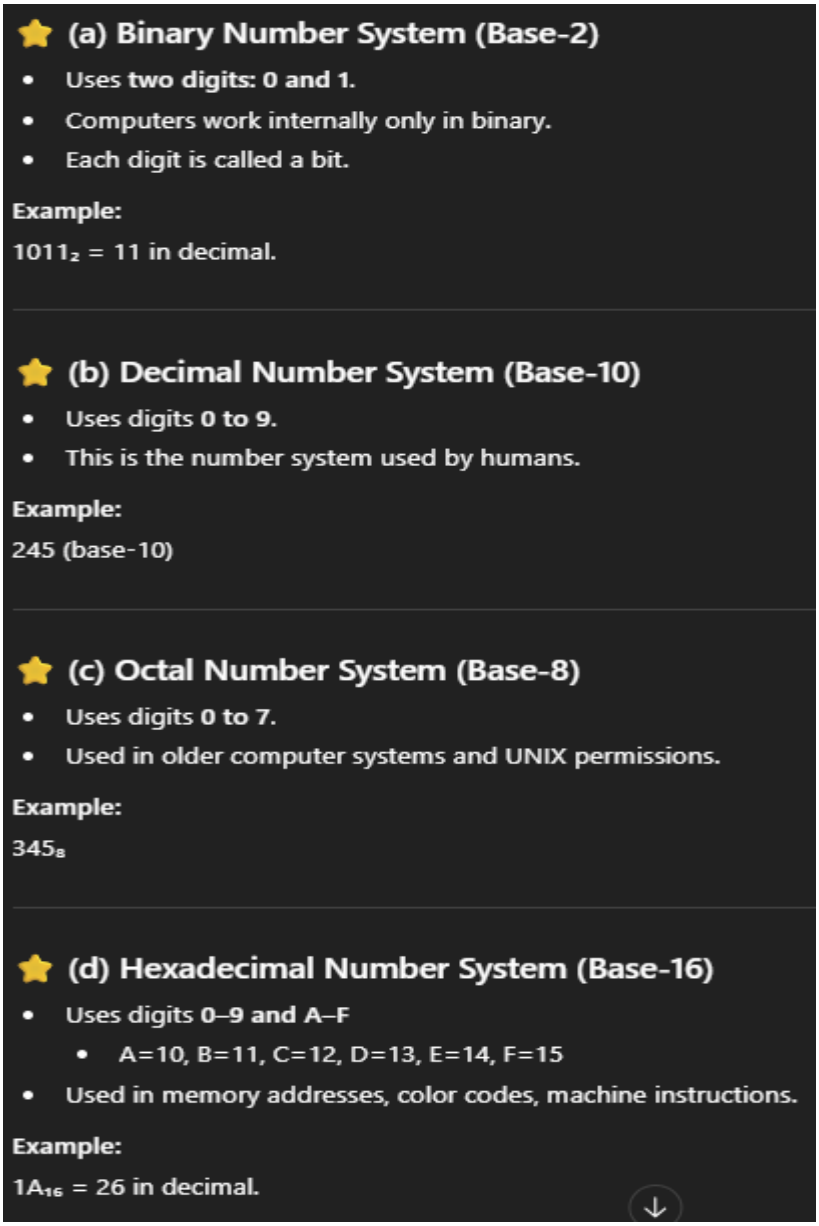
Example:

A = 01000001 (8 bits = 1 byte)

⭐ 3) Number Schemes (Number Systems)

Computers use different number systems to represent data.

Here are the **main number schemes** for GTU:



9) Requirements to set up a workstation in Digital forensics.

⭐ Introduction (Write 1–2 lines)

A **digital forensic workstation** is a specially designed computer system used by forensic investigators to analyze digital evidence safely and efficiently.
It must be powerful, secure, and equipped with proper tools to perform imaging, analysis, and recovery.

⭐ 1) High-Performance Computer / Workstation

A strong and fast computer is required because forensic analysis involves processing large amounts of data.

- ✔ Multi-core processor (Intel i7/i9 or Ryzen 7/9)
- ✔ High-speed RAM (16GB or 32GB or more)
- ✔ Large storage (SSD for OS + HDD for evidence storage)
- ✔ Good cooling system for long-running tasks

⭐ 2) Write Blockers (Hardware)

A **write blocker** prevents any data from being changed on the suspect drive during analysis.
This ensures *evidence integrity*.

Types:

- USB Write Blocker
- SATA/IDE Write Blocker

- ✔ Prevents accidental modification
- ✔ Maintains chain of custody

⭐ 3) Forensic Software Tools

Special software is needed to collect, examine, and analyze digital evidence.

Examples:

- EnCase
- FTK (Forensic Toolkit)
- Autopsy / Sleuth Kit
- X-Ways Forensics

- ✔ Used for imaging, recovery, file carving, keyword search, registry analysis, etc.

⭐ 4) Storage Devices for Evidence

You need large, secure storage to save images (copies) of suspect drives.

- ✔ External hard drives (1TB, 2TB, 4TB)
- ✔ RAID storage system
- ✔ Secure backup devices

Evidence images are often very large, so storage is critical.

⭐ 5) Forensic Duplicator / Imaging Tools

A forensic workstation must have devices or software to make **bit-by-bit copies** of drives.

- ✔ Used to create exact clones of suspect hard disks.
- ✔ Ensures original evidence remains untouched.

Examples:

- Logicube Falcon
- FTK Imager
- EnCase Imager

⭐ 6) Proper Operating Systems and Environment

A forensic workstation may use multiple OS environments for flexibility:

- ✔ Windows OS
- ✔ Linux forensic distributions (Kali Linux, CAINE, DEFT)
- ✔ Secure boot environment
- ✔ No internet connection (or limited, controlled)

Some tools run only on specific OS, so multiple OS support is helpful.

⭐ 7) Additional Hardware Tools & Accessories

To handle different types of devices:

- ✔ Dongles, adapters (SATA, IDE, NVMe, mSATA)
- ✔ Card readers (SD, microSD)
- ✔ Cables and connectors
- ✔ Faraday bags (to block network signals)
- ✔ Write-protected USB ports

Useful for mobile phones, laptops, and storage analysis.

⭐ 8) Secure Laboratory Environment

The forensic workstation must be placed in a controlled environment:

- ✔ Access control (only authorized personnel)
- ✔ CCTV monitoring
- ✔ Anti-static work table
- ✔ Fireproof storage for evidence
- ✔ Log book for chain of custody

This protects evidence and ensures proper documentation.

⭐ 9) Documentation Tools

A workstation must support documentation because **"If it's not written, it didn't happen."**

- ✔ Case management software
- ✔ Report writing tools
- ✔ Screenshots and logging utilities

Helps investigators prepare legally acceptable reports.

10) Different types of storage in the world.

⭐ 1) Primary Storage (Main Memory / Internal Storage)

This is the memory that the CPU can access directly.
It is fast but smaller in size.

✔ **Features:**

- Very fast
- Expensive
- Volatile (data lost when power off)

✔ **Examples:**

- **RAM (Random Access Memory)**
- **ROM (Read Only Memory)**
- **Cache memory**

Use: Stores data currently being processed.

⭐ 2) Secondary Storage (External / Auxiliary Storage)

Used for **long-term storage** of data.
Larger, cheaper, and non-volatile.

✔ **Features:**

- High capacity
- Permanent storage
- Slower than primary memory

✔ **Examples:**

- **Hard Disk Drive (HDD)**
- **Solid State Drive (SSD)**
- **Pen Drive / USB Drive**
- **Memory Card**
- **CD / DVD**

Use: Stores software, videos, documents, OS, backups, etc.

⭐ 3) Cloud Storage (Online Storage)

Data is stored on remote servers and accessed using the internet.

✔ **Features:**

- Access from anywhere
- Very large storage
- Used for backup and sharing

✔ **Examples:**

- **Google Drive**
- **Dropbox**
- **Microsoft OneDrive**
- **iCloud**

Use: Online data storage, sharing, collaboration.

11) Difference between Volatile and non volatile Memory.

Volatile Memory	Non-Volatile Memory
1. Data is lost when power is turned off.	1. Data is NOT lost even after power is off.
2. Used for temporary storage.	2. Used for permanent/long-term storage.
3. Faster in speed.	3. Slower compared to volatile memory.
4. More expensive per GB.	4. Cheaper per GB.
5. Directly accessible by CPU.	5. Usually not directly accessed by CPU.
6. Used while programs are running.	6. Used to store files, software, OS, backups.
7. Examples: RAM, Cache.	7. Examples: HDD, SSD, ROM, Pen Drive.
8. Smaller storage capacity.	8. Larger storage capacity.
9. High performance but temporary.	9. Lower performance but permanent.

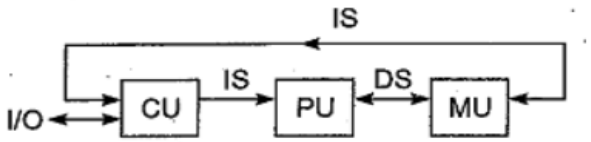
12) Flynn's classifications of computer.

Flynn' s Classification (Taxonomy)

- Classification of various computer architectures based on notions of instruction and data streams
  - **SISD** single instruction stream over a single data stream
  - **SIMD** single instruction stream over multiple data streams
  - **MISD** multiple instruction stream and a single data streams
  - **MIMD** multiple instruction stream over multiple data streams

- SISD
  - Conventional sequential machines

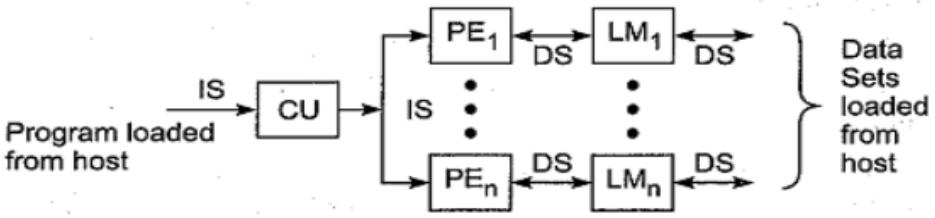
Captions:
CU = Control Unit
PU = Processing Unit
MU = Memory Unit
IS = Instruction Stream
DS = Data Stream
PE = Processing Element
LM = Local Memory



(a) SISD uniprocessor architecture

- SIMD
  - Vector computers are equipped with scalar and vector hardware

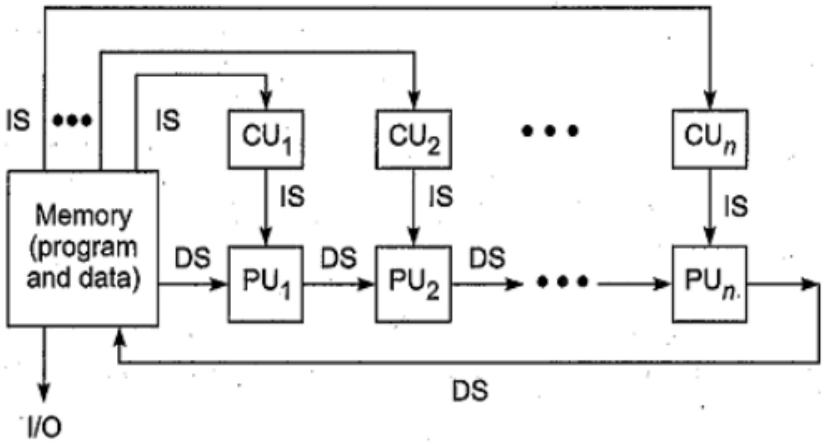
Captions:
CU = Control Unit
PU = Processing Unit
MU = Memory Unit
IS = Instruction Stream
DS = Data Stream
PE = Processing Element
LM = Local Memory



(b) SIMD architecture (with distributed memory)

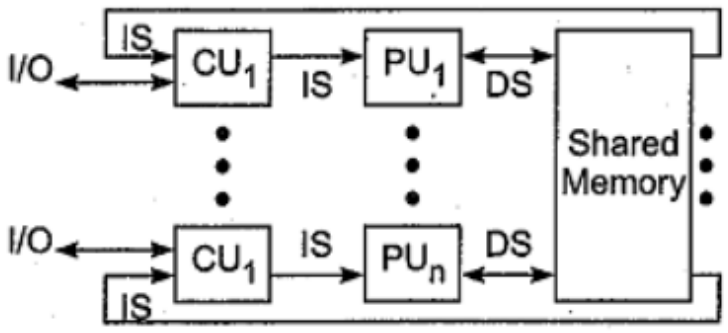
- MISD
  - The same data stream flows through a linear array of processors executing different instruction streams

Captions:
CU = Control Unit
PU = Processing Unit
MU = Memory Unit
IS = Instruction Stream
DS = Data Stream
PE = Processing Element
LM = Local Memory



- MIMD

Captions:
CU = Control Unit
PU = Processing Unit
MU = Memory Unit
IS = Instruction Stream
DS = Data Stream
PE = Processing Element
LM = Local Memory



(c) MIMD architecture (with shared memory)

1) Forensic cloning process of evidence with an appropriate example.

Forensic cloning is the process of creating an exact **bit-by-bit copy** of digital evidence (such as a hard disk, pen drive, mobile storage) without changing the original data.
It is also called **Forensic Imaging**.
This helps investigators work on the cloned copy while the original evidence remains safe and untouched.

⭐ 2) Why Forensic Cloning is Needed? (Short points)

- To preserve original evidence in its pure form
- To avoid accidental modification
- To analyze deleted, hidden, or encrypted data
- To maintain chain of custody for court presentation

⭐ 3) Steps in Forensic Cloning Process (Easy & Detailed)

⭐ Step 1: Preparation of Workstation

- A clean, secure forensic lab environment is prepared.
- Required tools: write blocker, forensic software (FTK Imager, EnCase), cables, storage device.

⭐ Step 2: Connect Original Evidence Device

- The suspect device (HDD, pen drive, SSD, etc.) is connected **through a write blocker**.
- Write blocker ensures **no data is altered** on the original device.

⭐ Step 3: Identify and Select the Source (Suspect Drive)

- Forensic tool detects the suspect drive.
- Investigator verifies details—storage size, partitions, sectors.

⭐ Step 4: Create a Bit-by-Bit Image (Forensic Clone)

- Using forensic tools (FTK Imager, EnCase, Autopsy), a **bit-stream copy** is created.
- Bit-stream = exact replica including:
  - ✔ Deleted files
  - ✔ Hidden files
  - ✔ File slack
  - ✔ Unallocated space

This image is usually saved as:

- **E01** (EnCase format)
- **DD/RAW** image
- **AFF** format

⭐ Step 5: Generate Hash Values (MD5/SHA-1)

- Before cloning → hash is calculated from the original drive
- After cloning → hash is calculated from the cloned image
- If both hashes match → image is verified as **exact copy**

Hash values maintain evidence integrity.

⭐ Step 6: Store and Protect the Original Evidence

- Original device is unplugged, sealed in evidence bag and stored securely.
- Chain of custody form is updated with date, time, and signatures.

⭐ Step 7: Start Analysis on the Clone (Not on Original)

- Investigation is done on the cloned copy only.
- Searching, data carving, keyword search, recovery, timeline analysis, etc., are performed.

⭐ 4) Example (Very Simple & Relevant)

Example: Hard Disk Cloning in a Cyber Fraud Case

Police seized a suspect's **500 GB hard disk** in a cyber fraud investigation.
The forensic expert connects the drive to the computer using a **write blocker** to avoid altering data.
Using **FTK Imager**, the expert creates a **bit-for-bit clone** and saves it as **E01 image** on a 1TB external drive.
MD5 hash value of the original and cloned image is exactly the same, proving the clone is 100% accurate.
The original hard disk is safely stored, and all investigation is done on the cloned image.
During analysis, deleted Excel files are recovered from the clone which reveal fraudulent transactions.

2) How a cell phone obtained from a crime scene can be handled by a digital forensic scientist ?

1) Secure and Isolate the Phone

- The first step is to **prevent the phone from receiving signals** (calls, messages, remote wipe commands).
- The phone is placed in a **Faraday bag/box** to block network signals.
- This protects data from being deleted or modified remotely.

2) Maintain Chain of Custody

- The forensic scientist **records details** like time, date, place, device model, serial number, and who collected it.
- A **chain of custody form** is maintained to ensure the phone is legally admissible in court.

3) Preserve the Device in Original Condition

- The phone is **not powered on**, not unlocked, and not tampered with at the crime scene.
- If the phone is ON, it is kept powered to avoid data loss but still isolated from networks.

4) Create a Forensic Image (Clone) of the Phone

- Using forensic tools like **Cellebrite, UFED, Oxygen Forensics, or MSAB**, an exact **bit-by-bit copy** of phone memory is taken.
- This ensures analysis is done on the **clone**, not the original phone.

5) Analyze the Extracted Data

- The cloned data is examined for:
  - ✔ Call logs
  - ✔ SMS / WhatsApp messages
  - ✔ Images and videos
  - ✔ GPS / location data
  - ✔ Browser history
  - ✔ Deleted files
  - ✔ Social media chats
- Patterns or evidence related to the crime are identified.

6) Document and Report Findings

- All steps, tools used, and evidence found are **properly documented**.
- A detailed forensic report is prepared for presentation in court.

3) Explain chain of custody. Step of maintaining chain of custody of an digital evidence obtained from a crime scene.

What is chain of custody?

- A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

- Example: A computer taken in as evidence makes many stops on its road to court.
- It's collected, logged in at the lab, stored, checked out for analysis, checked back in for storage, and so on.
- Each of these stops must be noted, tracking each and every time the evidence item changes hands or locations. Without this detailed records, the evidence won't be considered as trustworthy.

⭐ 1) Identify and Secure the Digital Evidence

- Locate the device (mobile, laptop, HDD, USB, etc.) at the crime scene.
- Ensure it is **not tampered with**, damaged, or altered.
- If it is a phone or laptop, isolate it from network signals (Faraday bag).

⭐ 2) Label and Document the Evidence

- Give a **unique identification number** to the evidence.
- Record details such as:
  - ✔ Type of device
  - ✔ Model, serial number
  - ✔ Date, time, and location of collection
  - ✔ Name of the person who collected it

This is written in the **Chain of Custody Form**.

⭐ 3) Collect and Package the Evidence Properly

- Use **evidence bags, anti-static covers, or Faraday bags.**
- Seal the evidence to prevent tampering.
- Write the seal number on the form for verification.

⭐ 4) Transfer the Evidence Securely

- Whenever evidence is passed from one person to another, it must be recorded.
- Details entered:
  - ✔ From whom
  - ✔ To whom
  - ✔ Date and time
  - ✔ Reason for the transfer

This keeps the legal trail unbroken.

⭐ 5) Store the Evidence Safely

- Keep it in a **secure evidence locker or forensic lab.**
- Access should be limited only to authorized personnel.
- Environmental safety (temperature, humidity) must be maintained.

⭐ 6) Create a Forensic Image (Clone) Without Altering Original Data

- Use write blockers and forensic software to create a **bit-by-bit copy.**
- Calculate hash values (MD5/SHA-1) before and after imaging.
- The original evidence is stored safely; analysis is done on the clone.

⭐ 7) Record Every Action Taken on the Evidence

- Document all steps: imaging, testing, analysis, storage, transfers.
- This documentation is important for court presentation.

⭐ 8) Present Evidence and Log in Court

- Submit the final report with the chain of custody record.
- The chain must show **unbroken control** from th↓me scene to the courtroom.

4) Document the scene of evidence by maintaining chain of custody.

When digital evidence (like a mobile, laptop, USB drive) is found at a crime scene, it **must be documented properly** and the **chain of custody must be maintained** to prove that the evidence remained authentic and untampered.

Below are the steps written in **simple and exam-ready format.**

⭐ Steps to Document the Scene & Maintain Chain of Custody

1) Photograph and Record the Scene

- Take clear photographs and videos of:
  - ✔ The device exactly as found
  - ✔ Surroundings and position
  - ✔ Cables, accessories, power state (ON/OFF)
- Note the exact time, date, and location.

Purpose: Shows the original condition of evidence.

---

2) Describe the Evidence in Notes

Record detailed information such as:

- Type of device (mobile, HDD, laptop)
- Brand and model
- Serial number
- Visible damage or modifications
- Current status (powered ON/OFF, connected to Wi-Fi, etc.)

This helps create a **formal written record.**

3) Assign a Unique Evidence ID

- Give the device a **unique identification number.**
- This number is written on:
  - ✔ The evidence label
  - ✔ Chain of custody form
  - ✔ Packaging bag

---

4) Packaging and Securing the Evidence

- Use proper forensic containers:
  - ✔ Anti-static bags
  - ✔ Faraday bags (if device has wireless communication)
- Seal the bag and record the seal number.

This prevents tampering.

---

5) Fill the Chain of Custody Form

The form must include:

- Evidence ID
- Description of device
- Date and time of collection
- Name and signature of officer collecting it
- Place where it was found

This establishes *legal ownership trail.*

6) Transfer the Evidence Securely

Whenever evidence is handed over (e.g., from police to forensic lab):

- Document:
  - ✔ From whom
  - ✔ To whom
  - ✔ Date and time
  - ✔ Reason for transfer
- Get signatures from all parties.

This ensures **unbroken chain of custody**.

---

7) Store the Evidence in a Secure Lab

- Keep it in a **locked evidence locker**.
- Only authorized personnel may access it.
- Access is logged each time.

5) **How a PC obtained from a crime scene can be handled by a digital forensic scientist ?**

1) Secure and Isolate the PC

- The PC is **not touched or powered on/off** without proper precautions.
- If the PC is ON → keep it ON (to avoid losing data in RAM).
- If the PC is OFF → keep it OFF (to avoid altering data).
- Disconnect it from the internet/Wi-Fi to prevent **remote deletion**.
- Photograph the PC in its exact position at the crime scene.

---

2) Document and Collect the Evidence

- Note details:
  - ✔ PC brand, model
  - ✔ Serial number
  - ✔ Attached devices (keyboard, mouse, USB, cables)
  - ✔ Current state (ON/OFF)
- Label the system with a **unique evidence ID**.
- Package the PC safely in anti-static or protective bags.

---

3) Maintain Chain of Custody

- Fill the chain of custody form with:
  - ✔ Date, time, place of collection
  - ✔ Who collected the PC
  - ✔ Signatures of officers
- This proves evidence was not altered.

---

4) Use Write Blockers and Create Forensic Image

- Connect the PC's storage (HDD/SSD) using a **write blocker** to ensure no changes to original data.
- Create a **bit-by-bit forensic clone** using tools like FTK Imager or EnCase.
- Calculate **hash values** before and after to verify integrity.

5) Analyze Only the Cloned Image

- All investigation—file recovery, logs, emails, browser history, deleted files—is done on the cloned copy.
- The **original PC is sealed and stored safely** as evidence.

6) how will you document the crime scene.

⭐ 1) Photograph and Video Record the Scene

- Take clear photos of the **entire scene** from all angles.
- Capture close-up photos of evidence (weapons, devices, footprints, bloodstains).
- Record the condition of the room, lighting, door positions, windows, etc.
- Video recording helps show the actual sequence and layout.

✔ Purpose: Creates a **permanent visual record** of the original condition.

⭐ 2) Sketch/Draw the Scene

- Make a rough sketch showing:
  - ✔ Position of evidence
  - ✔ Distances and measurements
  - ✔ Entry/exit points
  - ✔ Orientation (North direction)
- Later, a final neat sketch is prepared.

✔ Purpose: Gives a **clear map** of the crime scene layout.

⭐ 3) Write Detailed Notes

Document everything the investigator observes, such as:

- Date, time, and place of investigation
- Weather and lighting conditions
- Condition of doors, windows, furniture
- Position and description of evidence
- Any smells, sounds, or disturbances
- Names of people present

✔ Purpose: Notes act as a **factual written record** for the court.

⭐ 4) Collect, Label, and Package Evidence

- Each evidence item is given a **unique ID number**.
- Proper packaging is used (paper bags, Faraday bags, boxes).
- Seal the evidence and write seal number.
- Fill the **Chain of Custody Form** with:
  - ✔ Who collected
  - ✔ When collected
  - ✔ Description of item

✔ Purpose: Maintains the **integrity and legal trail** of the evidence.

7) Explain Order of volatility.

Order of Volatility refers to the sequence in which digital evidence should be collected based on how quickly the data may be lost, changed, or overwritten.
The most fragile (short-lived) data must be collected **first**, and the most stable (long-lasting) data is collected **last**.

⭐ 2) Why Order of Volatility is Important?

- Digital data disappears very fast.
- RAM, running processes, and network connections disappear if the device turns OFF.
- To preserve maximum evidence, forensic experts follow a priority order.
- Ensures the investigation is scientifically correct and legally acceptable.

⭐ 3) Order of Volatility (FROM MOST VOLATILE → LEAST VOLATILE)

Below are the levels explained in **simple and detailed** GTU-friendly points:

⭐ (1) CPU Registers and Cache Memory (Most Volatile)

- Data here changes millions of times per second.
- Lost immediately when system is powered off.
- Includes CPU instructions, temporary values, cache lines.

✔ **Collect First** using live response tools.

⭐ (2) RAM (Random Access Memory)

- Stores running programs, passwords in memory, logs, clipboard data, chat fragments, decryption keys, etc.
- Completely lost when the device shuts down.

✔ Tools: FTK Imager Lite, Belkasoft RAM Capture.

⭐ (3) Running Processes & Network Connections

- Active processes, open ports, live network sessions, system state.
- Includes:
  - ✔ IP connections
  - ✔ Open files
  - ✔ Active malware
  - ✔ User logins

✔ Must capture before unplugging or turning off the device.

⭐ (4) System Logs & Temporary Files

- OS logs, browser temp files, cache, recent documents.
- Persist for some time but can be overwritten easily.

✔ Need timely extraction.

⭐ (5) Hard Disk / SSD Data

- Less volatile because data remains after shutdown.
- Includes stored files, documents, emails, images, databases.

✔ Create **forensic image** using write blocker.

⭐ (6) External Storage Devices

- Pen drives, memory cards, CDs.
- More stable than internal memory, but still portable and may be damaged or stolen.

✔ Seize and image securely.

⭐ (7) Backups & Cloud Storage (Least Volatile)

- Cloud data (Google Drive, OneDrive, iCloud)
- Server backups
- Remote logs

This data remains intact for months/years.

✔ Collected last through legal procedures.

8) explain Hasing concepts to maintain integrity of evidence.

Hashing is a process that converts any digital data (file, image, disk, etc.) into a fixed-size unique value called a hash.
This hash looks like a long string of numbers and letters.

Example of a hash (MD5):
`5d41402abc4b2a76b9719d911017c592`

⭐ 2) Why is Hashing Used in Digital Forensics?

Hashing is used to **maintain integrity** of evidence.
This means proving that the digital evidence has *not been changed, altered,* or *tampered with* during investigation.

If even **one bit** changes in the file, the hash value will be completely different.

So, hashing is like a **digital fingerprint** of evidence.

⭐ 3) How Hashing Maintains Integrity? (Easy Explanation)

✔ Step 1: Before imaging

A hash value of the original device (HDD, phone, USB) is calculated.

✔ Step 2: After creating the forensic clone

A hash value of the cloned image is calculated.

✔ Step 3: Compare both hash values

- If both are **same → evidence is original and unchanged**
- If hash values are different → evidence is **altered or corrupted**

This gives proof in court that the evidence is **authentic.**

⭐ 4) Common Hash Algorithms Used in Forensics

✔ MD5 (Message Digest 5)

- Produces a 32-character hash
- Most commonly used in forensics

✔ SHA-1 (Secure Hash Algorithm 1)

- Produces a 40-character hash
- More secure than MD5

✔ SHA-256

- Very strong, used for higher security cases

⭐ 5) Properties of Hashing (Important for GTU)

1. **Unique Value:** Each file has a unique hash.
2. **Deterministic:** Same file → same hash always.
3. **Avalanche Effect:** A small change → completely different hash.
4. **One-way Function:** Cannot reverse a hash to get original data.
5. **Fast Computation:** Hashing is quick even for big files.

⭐ 6) Simple Example (Understand Easily)

An investigator finds a 1TB hard disk at the crime scene.

Step 1: Calculate hash of original drive

MD5: `A1B2C3D4E5F69800AA11CC22DD33EE44`

Step 2: Create forensic clone (bit-by-bit image)

Step 3: Calculate hash of cloned image

MD5: `A1B2C3D4E5F69800AA11CC22DD33EE44`

Both hashes match →

Evidence is 100% identical and not tampered.

9) Define and differ live and dead system forensic.

⭐ 1) Definition of Live System Forensics (Easy + Detailed)

Live System Forensics is the process of collecting and analyzing evidence from a computer or device *while it is running (powered ON).*
The investigator examines **volatile data** such as RAM, running processes, network connections, open ports, temporary files, and active malware.

✔ **Key points:**

- Evidence is collected **before shutting down** the system.
- Used when important data exists only in **volatile memory** (RAM).
- Requires careful handling because actions may change system state.

✔ **Example:**

Capturing RAM to recover passwords, chat messages, encryption keys, or live malware.

⭐ 2) Definition of Dead System Forensics (Easy + Detailed)

Dead System Forensics is the process of analyzing a system *when it is powered OFF.*
The investigator removes the storage device (HDD/SSD/pen drive) and creates a **forensic clone** for analysis.

✔ **Key points:**

- System is off → **no volatile data exists.**
- Safer and easier because data does not change.
- Commonly used in most investigations.

✔ **Example:**

Creating a bit-by-bit image of a hard disk from a powered-off computer.

Live System Forensics	Dead System Forensics
1. Performed on a system **that is ON and running.**	1. Performed on a system **that is powered OFF.**
2. Collects **volatile data** (RAM, network info, active processes).	2. Collects **non-volatile data** (disk files, logs, documents).
3. Risk of altering data is **high** during examination.	3. Risk of altering data is **low** because system is off.
4. Must be done **quickly** before data disappears.	4. Can be done **slowly and safely.**
5. Requires specialized live-response tools.	5. Requires imaging tools (write blockers, forensic duplicators).
6. Useful when RAM contains important evidence.	6. Useful when only stored files are needed.
7. Harder to maintain integrity (system keeps changing).	7. Easier to maintain integrity (data remains static).
8. Used in cases involving **active attacks, malware, intrusions.**	8. Used in **general investigations**, disk analysis, deleted file recovery.
9. Hash values may change during capture.	9. Hash values remain constant and easy to verify.
10. Example: capturing RAM from a live computer.	10. Example: imaging hard disk from a seized PC.

⭐ 4) Simple Examples (For Extra Clarity)

✔ Live Forensics Example

Police find a running laptop used for hacking.
Investigators capture **RAM**, active connections, and malware processes before shutting it down.

✔ Dead Forensics Example

Police seize a turned-off office desktop.
They remove the hard disk, create a clone using a wr[illegible]locker, and analyze recovered files.

10) Advantages of live collection.

⭐ Advantages of Live Collection (4 Marks – Easy & Detailed)

Live collection means collecting evidence from a system **while it is running (powered ON).**
This helps investigators capture data that would disappear if the system is turned off.

⭐ Advantages of Live Collection (Explain These 4–6 Points in Exam)

1) Captures Volatile Data (RAM Data)

- Live collection allows investigators to collect **volatile data** that exists only when the system is ON.
- This includes:
  - ✔ Passwords stored in RAM
  - ✔ Decryption keys
  - ✔ Running programs
  - ✔ Clipboard data
  - ✔ Chats and temporary files
- Once the system is turned off, all this data is **lost forever.**

2) Helps Identify Running Processes & Active Attacks

- Live collection shows **what is happening right now** in the system.
- Investigators can see:
  - ✔ Active malware
  - ✔ Hackers currently connected
  - ✔ Open network ports
  - ✔ Live connections
  - ✔ Background processes
- This is important for cases involving **intrusions, hacking, or ransomware.**

3) Recovers Network Information

- When the system is ON, investigators can capture:
  - ✔ IP addresses
  - ✔ Network logs
  - ✔ Open sessions
  - ✔ Connections to remote servers
- After shutdown, all live network information is lost.

4) Allows Safe Shutdown of System

- In some cases, improper shutdown can trigger:
  - ✔ Data deletion
  - ✔ Self-destruct malware
  - ✔ Encryption activation
- Live collection allows experts to **document and control the shutdown process** safely.

5) Prevents Loss of Critical Evidence

- Some evidence exists only temporarily (RAM, cache, temp files, paging memory).
- Live collection ensures this evidence is saved before it disappears.

6) Useful in Encrypted or Locked Systems

- If a system uses **full disk encryption**, the disk is readable only when the system is ON.
- Live collection helps extract:
  - ✔ Encryption keys
  - ✔ Decrypted files
  - ✔ Open containers
- After shutdown, the entire disk may become unreadable.

11) Write a note on report writing In digital forensics.

⭐ 1) Meaning of Forensic Report Writing

Report writing in digital forensics refers to creating a clear, accurate, and well-documented report of the entire investigation process, methods used, evidence collected, and results found.

It explains *what was done*, *how it was done*, and *what was discovered*.

⭐ 2) Purpose of a Digital Forensics Report

- To explain the investigation results in a clear manner
- To present technical evidence in a **simple, understandable form**
- To maintain legal validity of evidence
- To demonstrate that correct forensic methods were followed
- To assist police, lawyers, and judges in understanding the findings

⭐ 3) Contents of a Digital Forensic Report

These are the common sections included:

✔ a) Case Information

- Case number
- Investigator name
- Date and time
- Authority for investigation

✔ b) Description of Evidence

- Type of device (HDD, mobile, laptop)
- Serial number, model, capacity
- How and when it was collected
- Hash values of original and cloned data

✔ c) Tools and Methods Used

- Forensic tools used (EnCase, FTK, Autopsy, Cellebrite)
- Imaging method
- Analysis procedures

✔ d) Findings / Results

- Recovered files
- Deleted data
- Browser history
- Emails, chats, logs
- Malware activity
- Timeline reconstruction

✔ e) Conclusions

- Summary of evidence
- Relevance to the case
- Final interpretation

✔ f) Attachments

- Screenshots
- Hash reports
- Logs
- Copies of recovered files

⭐ 4) Qualities of a Good Forensic Report

- **Clear and easy to understand**
- **Accurate and factual** (no assumptions)
- **Objective and unbiased**
- **Technically valid**
- **Properly documented**
- **Legally acceptable**

⭐ 5) Importance of Report Writing in Digital Forensics

- Used as **legal evidence in court**
- Shows that proper forensic procedures were followed
- Ensures transparency in investigation
- Helps other investigators understand the case
- Prevents disputes or questions on evidence handling

12) What is data preservation in cyber security.

Data preservation in cybersecurity means protecting and storing data in its original, unchanged form so that it remains safe, intact, and available for future use or investigation.

It ensures that no one can modify, delete, or damage the data.

⭐ Detailed Explanation (Simple Points)

1) Protecting Data from Modification or Deletion

Data preservation ensures that critical data—such as logs, emails, system files, backups, or digital evidence—remains **unchanged.**

This prevents hackers or unauthorized users from tampering with data.

---

2) Maintaining Integrity for Investigation

In cybercrime investigations, digital evidence must stay in its *original condition.*

Preservation keeps data authentic so that it can be used in:

- Court cases
- Forensic analysis
- Incident response

Tools like hashing, write-blockers, and secure backups are used.

---

3) Long-Term Secure Storage

Preserved data is stored safely for future reference.

This includes:

- Secure servers
- Backups
- Cloud storage
- Forensic archives

This prevents loss due to accidental deletion, corruption, or system failures.

13) Rule of cyber forensic investigator.

14) What is important to work on a duplicate image.

In digital forensics, investigators **never work on the original evidence** (like the real hard disk, phone memory, or USB).
Instead, they create a **duplicate image** (an exact bit-by-bit copy) and perform all analysis on that copy.

This protects the original evidence from any damage or modification.

⭐ Why It Is Important to Work on a Duplicate Image? (Detailed Points)

⭐ 1) Prevents Modification of Original Evidence

- Investigating directly on the original device can accidentally **change files**, update timestamps, or alter logs.
- Working on a cloned image ensures the **original evidence remains untouched**.

✔ This keeps the evidence legally valid.

⭐ 2) Maintains Evidence Integrity

- Before and after imaging, investigators calculate **hash values** (MD5/SHA-1).
- If hash values match, the duplicate is an exact copy.
- This confirms the **integrity** of both original and clone.

✔ Courts accept only verified, unmodified evidence.

⭐ 3) Protects Against Data Loss

- The original device may be damaged, encrypted, corrupted, or unstable.
- Working on a duplicate image ensures that even if something goes wrong, **the original evidence remains safe.**

✔ Useful for sensitive or one-time access devices.

⭐ 4) Allows Multiple Examinations and Repeated Testing

- Many forensic operations require repeated scans, recovery, and testing.
- Doing this on the original device may destroy or overwrite data.
- A clone allows unlimited analysis:

  ✔ File carving
  ✔ Malware analysis
  ✔ Keyword search
  ✔ Timeline reconstruction

✔ Without risking the real evidence.

⭐ 5) Legally Required for Court Procedures

- Courts require proof that the **original evidence was preserved** perfectly.
- If the investigator works directly on original storage, the evidence may be rejected.
- Working on a duplicate image ensures:

  ✔ Legality
  ✔ Authenticity
  ✔ Admissibility in court

15) explain Important of photography and note for documenting the scene.

⭐ 1) Introduction (Write 2 lines)

Documenting a crime scene ensures that the original condition of the scene and all evidence is recorded properly.
Photography and note-taking are essential because they provide a **permanent, accurate, and reliable record** for investigation and court.

⭐ 2) Importance of Photography in Documenting the Scene

⭐ 1) Captures the Original Condition of the Scene

- Photos show the exact position of objects, evidence, victims, and surroundings.
- Helps investigators revisit the scene anytime.

⭐ 2) Provides a Permanent Visual Record

- Once the crime scene is cleaned or disturbed, photographs become the only visual proof.
- Useful during investigation and legal proceedings.

⭐ 3) Helps in Analysis and Reconstruction

- Photos help reconstruct the sequence of events—entry, struggle, damage, blood patterns, etc.
- Assists forensic experts in understanding what happened.

⭐ 4) Shows Detail Better Than Human Memory

- Investigators may forget details, but photographs remain 100% accurate.
- Close-up photos reveal small details like fingerprints, tool marks, or digital devices.

⭐ 5) Supports Court Evidence

- Judges and lawyers rely on photographs to understand the situation clearly.
- Helps prove that evidence was found exactly as reported.

⭐ 3) Importance of Notes in Documenting the Scene

⭐ 1) Provides a Written Record of Observations

- Notes include time, date, weather, smells, sounds, condition of the room, and investigator's observations.
- Helps capture information that photos cannot show.

⭐ 2) Records Detailed Description of Evidence

- Notes describe size, color, position, type of evidence, and any visible damage.
- This helps during proper identification later.

⭐ 3) Supports Chain of Custody

- Notes include:
  - ✔ Who collected the evidence
  - ✔ When and where it was found
  - ✔ How it was packaged
- This documentation is required for legal acceptance.

⭐ 4) Helps in Preparing Final Forensic Report

- Notes become the base for the final report submitted to police and court.
- Ensures accuracy, clarity, and continuity in the investigation.

⭐ 5) Useful When Photographs Are Not Enough

- Photographs cannot record investigator thoughts, measurements, or conditions.
- Notes fill these gaps and provide context.

⭐ 4) Combined Importance (Photography + Notes)

- Together, they provide **complete documentation** of the scene.
- Photos = what the scene looked like
- Notes = what the investigator observed
- Both support forensic analysis and make the evidence legally strong.

Q-1.What are the steps to restore deleted data?
ANS

⭐ Expanded Answer: Steps to Restore Deleted Data (Based on PPT Content)

1. **Identify and secure the storage device**
   First, the suspect hard disk, pen drive, or memory card is identified and secured.
   This prevents any new data from being written, because new data can overwrite deleted files.
   (PPT explains that deleted data remains until overwritten.)
2. **Create a forensic image (bit-by-bit copy)**
   As shown in the Data Acquisition part of the PPT, investigators always create a **bitstream disk-to-image** file.
   This is a complete sector-by-sector copy of the original device.
   All recovery work is done on this cloned image, not on the original, to maintain evidence integrity.
3. **Scan unallocated space using forensic tools**
   The PPT explains "File Carving" (Page 13), which is the process used to recover deleted files.
   Tools like FTK, Autopsy, or EnCase scan the **unallocated space** of the clone and
   search for **file headers and footers** (signatures) to reconstruct deleted files.
4. **Recover and verify the data**
   Once the deleted files are found, they are restored and saved separately.
   To ensure they are not altered, hash values (MD5/SHA) are calculated before and after recovery.
   This ensures that the recovered data is accurate and forensically valid.

⭐ Easy Explanation of Steps to Restore Deleted Data

1️⃣ Identify and secure the storage device

Imagine someone deleted files from a pendrive or laptop.

The first thing the forensic expert does is:

- take that device safely
- **stop using it immediately**

Because if you continue using it, **new files overwrite deleted data**, and then recovery becomes impossible.

So step 1 is simply **protect the device**.

2️⃣ Create a forensic image (bit-by-bit copy)

Now, experts **never touch the original disk** directly.

They make a **bitstream image** — meaning:

- every single bit
- every sector
- including deleted space
- including unallocated space

is copied into a separate file.

Why?
Because this protects the original device.
If something goes wrong, the original evidence is st[illegible]afe.

Think of it like taking a Xerox copy of a notebook.

3️⃣ Scan unallocated space using forensic tools (File Carving)

When a file is deleted:

- It does NOT disappear.
- The space is just marked as **free**.

The actual data stays until overwritten.

Forensic tools scan this "free space" (called **unallocated space**) and try to find:

- file headers (start of file)
- file footers (end of file)

These are like **signatures** for files.

Example:

- JPG files start with a known header code
- PDF files start with `%PDF`
- MP4 files have `ftyp` header

The tool uses these signatures to **rebuild the deleted file**.
This technique is called **File Carving** (your PPT).

4️⃣ Recover and verify the files

Once the tool finds the deleted files:

- they are **restored**
- saved to another location

Then, the expert uses **hashing** (MD5/SHA) to check:

- the file recovered
- is the same as the file found in the image
- meaning it is **not modified**

This keeps the evidence genuine.

Q-2.What is Metadata? How can we remove metadata?
ANS

Here is the **perfect GTU-style answer** based *exactly from your PPT* and in very **easy language**.
I'm giving both **explanation** + **exam-ready 4–5 mark answer**.

⭐ **Explanation (Easy Version)**

What is Metadata?

Metadata means **"data about data."**
It is extra information stored inside a file.
Example:
For a photo, metadata can include:

- date and time photo was taken
- camera model
- location (GPS)
- resolution
- file author

For a document, metadata includes:

- author name
- company name
- when the file was created
- when it was last edited
- number of pages/words

Metadata helps computers understand and organize files.
But it can also reveal private information during investigation.
(All these points come from PPT pages 43–53.)

How can we remove metadata?

Windows gives a direct option to remove metadata.
Steps (from PPT pages 50–51):

1. **Right-click the file** → select **Properties**
2. Go to the **Details** tab
3. Click **"Remove Properties and Personal Information"**
4. Two options appear:
    - **Create a copy with all metadata removed**
    - **Choose specific fields to remove** (author, title, comments, etc.)
5. Select what you want to remove → click **OK**

This removes personal data that you don't want to share.

⭐ **GTU Exam-Ready Answer (Full Marks)**

Q. What is Metadata? How can we remove metadata?

Metadata is "data about data."

It is extra information stored inside a file such as author name, creation date, modification date, camera details, location, file size, etc. Metadata helps in identifying, managing, and

searching files. It is very important in digital forensics, as it reveals hidden details about user activity.

Removing Metadata:

In Windows, metadata can be removed using the “Remove Properties and Personal Information” option.

Steps:

1. Right-click the file and open **Properties**.
2. Go to the **Details** tab.
3. Click **Remove Properties and Personal Information**.
4. Select either:
    - Create a copy with all possible metadata removed, or
    - Choose which specific metadata fields to remove.
5. Click **OK** to apply.

If you want, send the next question — I’ll answer in the same simple exam style 📘🔥

Q-3.What relevance does metadata have to the evidence collected?
ANS

Here is a **simple explanation + perfect GTU exam answer**.

⭐ **Easy Explanation (Understand First)**

Metadata is extremely important in digital forensics because it tells the **hidden story behind a file**.

It helps an investigator know:

- **When** a file was created
- **Who** created or edited it
- **What device** created it
- **When it was last opened**
- **If the file was modified or tampered**

So even if someone deletes or hides a file, the metadata can still reveal **what happened with that file**, and **when**.

That's why metadata is powerful evidence.

⭐ **GTU Exam-Ready Answer (3–4 Marks)**

Relevance of Metadata in Evidence Collection

Metadata is important in digital forensic investigations because it provides **additional hidden information** that supports the main evidence. It helps investigators:

1. **Establish timelines**
   Metadata gives accurate created, accessed, and modified (MAC) times.
   This helps in reconstructing when an activity occurred.
2. **Identify user actions**
   It reveals who created or edited a file, which user account was used, and which device was involved.
3. **Prove authenticity of evidence**
   If metadata matches expected values, it shows the file is original.
   If timestamps are changed, it can indicate tampering.
4. **Recover important information even if content is deleted**
   Metadata like thumbnails, authors, camera details (EXIF), or version history may survive even after the main file is removed.
5. **Link a suspect to a file**
   Metadata contains data like username, computer name, or software used, which can directly connect a suspect to a digital artifact.

Thus, metadata increases reliability, authenticity, and context of the digital evidence collected.

If you want, I can also give a **short 2–3 line version** for writing quickly.

Q-4. Define sleep, Hibernation and Hybrid sleep.
ANS:
Here is the **simplest explanation + perfect GTU exam answer** (based exactly on your PPT pages 15–21).

⭐ **Easy Explanation**

Sleep

Sleep means the computer "pauses" everything and stores current work in **RAM**.
It uses a **small amount of power** to keep data alive.
When you turn it back on, it resumes instantly.

Hibernation

Hibernation saves everything from **RAM to Hard Disk**.
Then the computer fully powers off.
When restarted, it loads everything back to the same state.
Used mostly in **laptops** to save battery.

Hybrid Sleep

Hybrid sleep is a mix of **Sleep + Hibernation**.
It keeps data in **RAM** (like Sleep) **and** writes a copy to **Hard Disk** (like Hibernation).
Used mostly on **desktops** to protect data if power goes off.

⭐ **GTU Exam Answer (3–4 Marks)**

Sleep

Sleep mode is a power-saving state where all open applications and data are stored in **RAM**. A small amount of power is supplied to RAM to keep data active. The system resumes very quickly.

Hibernation

Hibernation saves the entire RAM content to the **hard disk** and then shuts down the system. It uses no power and is mainly used in laptops. When the computer starts again, it restores everything from disk.

Hybrid Sleep

Hybrid sleep is a combination of Sleep and Hibernation. Data is kept in RAM and also copied to the hard disk. It is mainly used on desktops to protect data during a power loss while still allowing quick resume.

If you want, I can also make a **short 2–3 line version** for quick writing.

Q-5. How to restore your deleted or modified folders or files from Shadow Copies.
ANS:
Here is the **easiest explanation + full GTU-exam answer** based exactly on your PPT (pages 67–77).

⭐ Easy Explanation (Understand First)

Shadow Copies = automatic snapshots of your files/folders.
If you delete or change a file by mistake, Windows may still have an **older version saved inside Shadow Copies**.
You can open that old version and **restore it**.
Restoring means:

- bring back the old file
- or copy it to a new location
- or restore the whole folder

Very helpful in forensics because it shows older states of data.

⭐ GTU Exam-Ready Answer (4–5 Marks)

How to restore deleted or modified files/folders from Shadow Copies
Windows stores previous versions of files and folders using **Restore Points / Shadow Copies**. These older versions can be used to recover files that were deleted or modified.
Steps:

1. **Go to the location of the file/folder**
   Navigate to the folder where the deleted or modified file originally existed.
2. **Right-click the file or folder**
   Select **Properties** from the context menu.
3. **Open "Previous Versions" tab**
   Windows will show all available older versions saved from Restore Points or Shadow Copies.
4. **Choose the version to recover**
   Select the version you want to restore.
   You will get three options:
   - **Open** → view the contents of the older version
   - **Copy…** → save the older version to another location
   - **Restore…** → replace the current file/folder with the older version
5. **Click Copy or Restore**
   - **Copy** is safer because it keeps the current file and gives you a recovered version.
   - **Restore** directly replaces your current file/folder with the previous one.

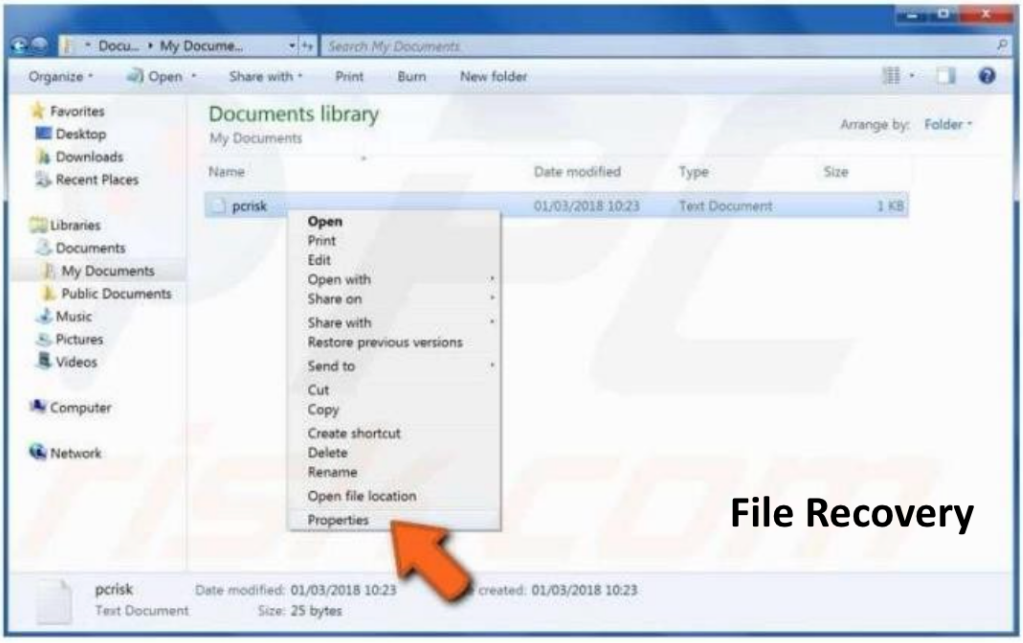
Windows will now recover the file/folder from the Shadow Copy and save it in the selected location.

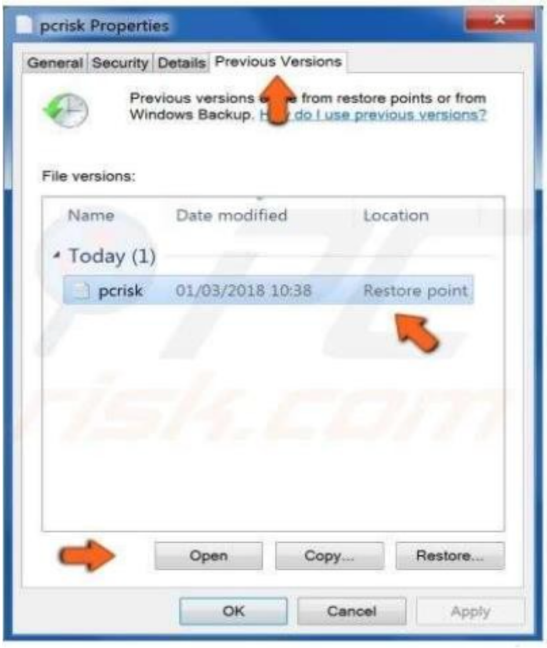
⭐ Short 3-line version (for exam)

Deleted or modified files can be restored using Shadow Copies by right-clicking the file/folder → Properties → Previous Versions. Select the required older version and choose

Open, **Copy**, or **Restore**. This brings back the earlier version saved by Windows automatically.

it and then select "Properties" from the context





File Recovery

Q-6.Discuss techniques of hibernating files

ANS:
Here is a **full 7-mark GTU answer**, written exactly from your PPT (pages 16–21) and explained in a clean, scoring way.
This is the BEST possible answer to write in the exam for:
"Discuss techniques of hibernating file." (7 Marks)

⭐ **7-MARK ANSWER**

Techniques of Hibernating File

A **hibernating file** is a special system file called **hiberfil.sys** created by Windows when the computer enters hibernation mode. This file stores the complete contents of RAM onto the hard disk so that the system can resume from the exact same state later. Digital forensic investigators analyze this file to recover evidence such as open documents, passwords, browser sessions, chats, and temporary data.
The techniques related to hibernating file can be understood through the three power-saving modes of Windows: **Sleep, Hibernation, and Hybrid Sleep**, as explained below.

---

1. Sleep Mode

- In Sleep mode, the system saves the current state (open files, applications, processes) in **RAM**.
- A small amount of power is supplied to RAM to keep data intact.
- This mode is fast to resume from but **does not create a hibernation file**.
- Because RAM is volatile, data is lost if power is removed.
- For forensic purposes, sleep mode is **not very useful**, as RAM content disappears on shutdown.

---

2. Hibernation Mode

- In Hibernation, the contents of RAM are **written to the hard disk** in a special file called **hiberfil.sys**.
- After writing RAM data to disk, the computer completely powers off.
- On restarting, Windows loads all data back from hiberfil.sys and restores the system to the exact previous state.
- Hiberfil.sys may contain:
    - open documents
    - unsaved work
    - temporary files
    - browser tabs
    - chat messages
    - encryption keys
    - passwords and credentials
- From a forensic viewpoint, this is **highly valuable**, because even deleted or unsaved data may appear in this file.

---

3. Hybrid Sleep

- Hybrid Sleep is a combination of **Sleep and Hibernation**.
- The system keeps data in **RAM** (like Sleep) but also writes a copy to the **hard disk** (like Hibernation).
- Mainly used on **desktop computers** to protect against power failures.
- If power is lost, data can be restored from the hibernation file.
- Creates or updates **hiberfil.sys**, making it useful for forensic recovery.

---

4. Forensic Importance of Hibernation File

- The hibernating file stores **RAM snapshots**, which often contain critical evidence.
- Suspects usually forget to delete or disable hibernation, so hiberfil.sys often remains untouched.
- Investigators extract:
  - deleted documents that were open
  - login sessions
  - decrypted data
  - browsing content
  - running programs before hibernation
- Tools like Volatility can analyze the hibernation file.

Conclusion

Hibernating file techniques include understanding Sleep, Hibernation, and Hybrid Sleep modes. Among these, **Hibernation and Hybrid Sleep** produce the hiberfil.sys file, which stores valuable RAM data for forensic analysis. Therefore, the hibernation file becomes an important artifact in computer system investigations.

Short 2–3 line exam summary

Hibernating files (hiberfil.sys) store RAM content when the system enters Hibernation or Hybrid Sleep. Sleep mode stores data only in RAM, while Hibernation and Hybrid Sleep write data to disk. This file contains valuable evidence like open documents, passwords, and unsaved data, making it useful in forensic investigation.

Q-7.Differentiate a restore point and a shadow copy.

ANS:
Here is the **clearest, simplest, GTU-ready difference between Restore Point and Shadow Copy** (perfect for 3–5 marks).

⭐ Easy Explanation (Understand First)

Restore Point

- A restore point is a **system snapshot** of Windows settings, registry, drivers, and configuration.
- Used to **restore the whole system** to an earlier working state.

Shadow Copy

- A shadow copy is the **actual backup copy of files and folders** created by the system.
- Used to **recover older versions of individual files/folders**.

Restore point = snapshot of system
Shadow copy = snapshot of files

⭐ GTU Exam-Ready Answer (Table Form)

Aspect	Restore Point	Shadow Copy
Definition	Snapshot of system settings, registry, drivers, and configuration.	Backup copy (snapshot) of files and folders.
Purpose	To restore the entire system to a previous working state.	To restore previous versions of individual files/folders.
What it captures?	System files, registry, installed programs, drivers.	User documents, folders, and data files.
Created by	System Restore feature.	Volume Shadow Copy Service (VSS).
Creation time	Automatically before major system events (software install, driver update) or manually by user.	Created automatically as part of restore points or backup operations.
Location	Stored as system snapshots.	Stored as hidden volume copies on the disk.
Recovery scope	Broad – full system recovery.	Narrow – recover specific files/folders.
Dependency	Shadow copies use restore points to generate snapshots.	Shadow copies are the underlying file versions that restore points rely on.

⭐ Short 3-line version (Rapid writing)

A **restore point** is a system-level snapshot used to revert Windows to an earlier working state.
A **shadow copy** is a file-level snapshot used to restore previous versions of files and folders.
Restore points protect system configuration, while shadow copies protect user data.

If you want more comparisons, give the next topic.
Q-8. What is Recycle Bin and its operation?
ANS:

Here is the **clearest, simplest, GTU-style answer** based exactly on your PPT (pages 39–42).
Perfect for **3–5 marks**.

⭐ Easy Explanation (Understand First)

The **Recycle Bin** is a temporary storage area in Windows where deleted files are kept.
When you press **Delete**, the file is *not permanently deleted*.
It is moved to the Recycle Bin so you can **restore it later** if needed.
It becomes permanently deleted only when:

- You **empty** the Recycle Bin, or
- You use **Shift + Delete**, or
- System is set to bypass Recycle Bin.

⭐ GTU Exam-Ready Answer

What is Recycle Bin?
The Recycle Bin is a system folder in Windows that stores deleted files temporarily.
When a user deletes a file, it is moved to the Recycle Bin instead of being permanently removed.
This allows the user to **restore the file** later.
Recycle Bin helps prevent accidental loss of data.

Operations of Recycle Bin

1. Deleting Files

- When a file is deleted normally (Delete key or right-click → Delete), Windows **moves it to the Recycle Bin**.
- File is still recoverable until the bin is emptied.

2. Restoring Files

- Users can open the Recycle Bin and choose **Restore**.
- The file is sent back to its **original location**.

3. Emptying the Recycle Bin

- Emptying deletes all items in the bin permanently.
- After this, recovery becomes difficult for normal users.

4. Bypassing the Recycle Bin (Shift + Delete)

- Using **Shift + Delete** sends files directly to **unallocated space**, skipping the Recycle Bin entirely.
- This makes recovery harder but possible using forensic tools.

5. Configuring Recycle Bin

- Right-click on Recycle Bin → Properties.
- The user can choose:
  - Custom size of Recycle Bin
  - "**Don't move files to Recycle Bin, delete them immediately**" option (this bypasses the bin completely)

6. Forensic Relevance

- Recycle Bin is one of the first places investigators check.
- Deleted files, metadata, and file names remain inside until emptied.
- Even emptied files may be recovered using **file carving** techniques.

⭐ **Short 3-line version (Quick Writing)**

The Recycle Bin is a Windows folder that temporarily stores deleted files, allowing recovery.
Normally deleted files go to the Recycle Bin, while Shift + Delete bypasses it.
Files can be restored, permanently deleted, or analyzed for forensic evidence.

Q-1.What are the legal provisions against cybercrime?

ANS: Got it — here is a **better, cleaner 3-mark answer** with **just the necessary points**, exactly what GTU expects.

⭐ **3-Mark Answer: Legal Provisions Against Cybercrime**

Legal provisions against cybercrime in India mainly come from the **Information Technology (IT) Act, 2000** and certain sections of the **Indian Penal Code (IPC)**.

Under the IT Act, 2000:

- **Sec. 66** – Hacking and misuse of computer systems
- **Sec. 66C/66D** – Identity theft and online fraud
- **Sec. 66E** – Violation of privacy
- **Sec. 66F** – Cyber terrorism
- **Sec. 67** – Publishing/transmitting obscene content

Under IPC:

- **Sec. 292** – Obscene material
- **Sec. 354D** – Cyberstalking
- **Sec. 420** – Online cheating/fraud

Indian Evidence Act:

- **Section 65B** – Certificate required for electronic evidence to be admissible.

⭐ **Even Shorter (If you want 2–3 lines):**

The IT Act 2000 provides legal provisions like Sec. 66 (hacking), 66C/66D (identity theft & fraud), 66E (privacy), 66F (cyber terrorism), and 67 (obscenity).
IPC sections like 292, 354D, and 420 also punish online crimes.
Digital evidence must follow Section 65B for court admissibility.

Q-2.Write a note on Electronics discovery.

For 3 marks
Here is the **3-mark answer in clear points**, perfect for GTU.

⭐ **3-Mark Answer (in Points): Electronic Discovery**

1. **Electronic Discovery (E-Discovery)** is the process of identifying, collecting, preserving, and producing **electronically stored information (ESI)** for legal cases and investigations.
2. **ESI includes** emails, documents, presentations, databases, social media data, audio/video files, and website content.
   (PPT page 26)
3. E-Discovery is important because digital evidence is **easily modified or deleted**, so it must be handled carefully using proper legal procedures like interrogatories, depositions, and document production.
   (PPT page 27)

If you want, I can make a **1-mark definition** also.

For 7 marks

Here is a **complete 7-mark answer** on **Electronic Discovery**, written exactly from your PPT (pages 26–27) and expanded into clear points for full marks.

⭐ **Electronic Discovery (E-Discovery) – 7 Marks Answer**

Electronic Discovery, commonly called **E-Discovery**, is the legal process of identifying, collecting, preserving, reviewing, and producing **electronically stored information (ESI)** for use in investigations, lawsuits, or court proceedings.
ESI includes emails, documents, presentations, databases, chats, audio/video files, social media data, and website content.
Below are the **key points for a full 7-mark answer**:

⭐ **1. Definition of Electronic Discovery**

E-Discovery refers to the electronic aspect of discovering, collecting, and presenting digital evidence (ESI) during legal cases.
It ensures that electronic data is obtained legally and preserved in its original form.

⭐ **2. Types of ESI (Electronically Stored Information)**

E-Discovery deals with:

- Emails & attachments
- Office documents (Word, PDF, Excel)
- Databases & logs
- Social media posts
- Audio & video files
- Website content
- Voicemail & chat messages

- Any digital content stored on computers, phones, or servers
  (PPT page 26)

⭐ 3. Purpose of E-Discovery

The goal is to find **relevant electronic evidence** for court cases, investigations, or compliance.
It helps lawyers and investigators understand the truth behind events through digital footprints.

⭐ 4. The E-Discovery Process

It includes:

- Identification of relevant digital evidence
- Collection and imaging of ESI
- Preserving evidence without altering it
- Reviewing the data
- Producing the data in court-acceptable formats
  (PPT page 26)

⭐ 5. Importance in Legal Proceedings

Digital evidence is now widely used in civil and criminal cases.
E-Discovery ensures all relevant electronic data is available for both parties, maintaining transparency and fairness.

⭐ 6. Challenges of ESI

According to the PPT:

- ESI is **volatile**, easily modified, deleted, or duplicated
- Large volume of digital data makes review difficult
- Data can be spread across cloud servers, devices, or networks
  (PPT page 27)
  These challenges make E-Discovery more complex than dealing with paper records.

⭐ 7. Use in Litigation (Court Cases)

Common legal discovery methods:

- **Interrogatories** (written questions)
- **Depositions** (oral questioning)
- **Document Production Requests**
  E-Discovery focuses on producing **digital documents** required during these legal procedures.
  (PPT page 27)

⭐ Conclusion

Electronic Discovery is a critical process in modern digital forensics and legal investigations. It ensures that electronic evidence is properly identified, preserved, analyzed, and presented in court while maintaining integrity and legal validity.

Q-3.What is the most important legal features about digital evidence?(3 TIMES)

ANS

⭐ **4-Mark Answer (6 Points): Important Legal Features About Digital Evidence**

1. **Section 65B Requirement**
   Digital evidence is admissible in court only if accompanied by a valid **Section 65B certificate** from the Indian Evidence Act.
2. **Integrity and Authenticity**
   Digital data can be easily altered, so investigators must prove that the evidence has not been modified by using hashing and proper imaging methods.
3. **Proper Collection Procedure**
   Evidence must be collected using standard forensic practices (bit-by-bit imaging, write blockers). Improper handling makes it legally invalid.
4. **Chain of Custody**
   Every step of evidence handling must be documented. A broken chain of custody can lead to rejection of the evidence in court.
5. **Compliance with Cyber Laws**
   The evidence must relate to relevant sections of the **IT Act (Sec 43, 66, 67)** and IPC sections dealing with cybercrimes to support legal action.
6. **Privacy and Legal Boundaries**
   Investigators must respect privacy laws and avoid unauthorized access; illegally collected evidence may be declared inadmissible.

Q-4.Explain role of the forensic examiner in judicial system.

ANS:

Here is your **full 7-mark expanded answer** for:
⭐ **Role of the Forensic Examiner in the Judicial System (7 Marks)**
A forensic examiner plays an essential role in helping the judicial system handle digital evidence properly, fairly, and scientifically. Their work ensures that cybercrimes are investigated correctly and evidence is legally acceptable in court. The major roles are:

⭐ **1. Identification and Seizure of Digital Evidence**
The examiner identifies all possible digital evidence sources (computers, mobiles, cloud accounts, storage devices, logs).
They lawfully seize devices while ensuring no data is modified. This is the first and most crucial step in any investigation.

⭐ **2. Preservation of Evidence Integrity**
Digital evidence is fragile and easily altered.
Examiners preserve its integrity using:

- Write blockers
- Bit-by-bit imaging
- Hashing (MD5/SHA)
  This ensures the original evidence remains untouched and can stand legal scrutiny.

⭐ **3. Analysis and Reconstruction of Events**
Examiners analyze:

- Deleted files
- Browser history
- Registry, logs
- Metadata
- Network traffic
- Emails, chats, images
  They reconstruct timelines, user actions, and methods used in the cybercrime.
  This technical analysis helps convert raw data into meaningful evidence.

⭐ **4. Maintaining Chain of Custody**
Every movement of evidence is documented — who collected it, when, where it was stored, and who accessed it.
A proper chain of custody prevents accusations of tampering and ensures the evidence is admissible in court.

⭐ **5. Preparing Detailed Forensic Reports**
Examiners prepare clear, accurate, and unbiased reports summarizing:

- Methods used
- Tools applied
- Findings

- Interpretation of results
  These reports act as strong support for judges, lawyers, and investigators who may not understand technical details.

⭐ 6. Assisting Investigators and Prosecutors

They help police, lawyers, and prosecutors understand technical aspects of digital evidence. They guide them on what evidence to focus on, what data is relevant, and how the crime was committed.

⭐ 7. Expert Testimony in Court

The examiner appears as an **expert witness** and explains findings in simple language.
They justify the forensic methods used and defend the integrity of the evidence.
Their testimony can strongly influence the final judgment.

⭐ 8. Ensuring Evidence Meets Legal Requirements

Examiners make sure digital evidence complies with laws such as:

- **Section 65B of the Indian Evidence Act** (admissibility)
- IT Act & IPC sections
  They ensure that evidence is collected and presented legally and ethically.

⭐ Conclusion

A forensic examiner acts as a bridge between technology and the law.
Their work ensures that digital evidence is properly collected, preserved, analyzed, and presented, helping the judicial system deliver justice in cybercrime cases.

If you want, I can also prepare **extra short versions**, **diagram versions**, or **point-only versions** for quick revision.

Q-5.How do you write a digital forensic investigation report?

ANS:

Here is a **perfect 4-mark GTU-style answer** for:
⭐ **"How do you write a Digital Forensic Investigation Report?" (4 Marks)**
Short, clear, and in **point format** exactly suited for 4 marks.

⭐ **4-Mark Answer: Writing a Digital Forensic Investigation Report**

1. **Case Details and Purpose**
   Start with case number, investigator name, dates, and the purpose/scope of the investigation (e.g., hacking, data theft, fraud).
2. **Evidence Description**
   List all devices and media collected (laptop, hard disk, USB drive, phone), including serial numbers, model details, and seizure information to maintain proper chain of custody.
3. **Tools and Methods Used**
   Mention forensic tools (FTK Imager, EnCase, Autopsy), techniques such as bit-by-bit imaging, hashing, file carving, and procedures used during analysis.
4. **Analysis and Findings**
   Provide results such as recovered deleted files, logs, metadata, browser history, timestamps, or traces of unauthorized activity. Present only factual evidence.
5. **Conclusion**
   Summarize what the evidence proves (e.g., user activity, data theft, unauthorized access) based entirely on digital findings.
6. **Appendices/Supporting Data**
   Attach hash values, screenshots, tool logs, and chain-of-custody forms to support the validity of the report.

Q-6.Electronic data discovery: What is it? How it functions.
ANS:

Yes bro, this question is similar to the previous one but shorter.
Here is a **perfect 3-mark GTU-style answer**, simple and in point format.

⭐ **3-Mark Answer: Electronic Data Discovery – What is it? How it Functions?**

1. What is Electronic Data Discovery?

Electronic Data Discovery (E-Discovery) is the process of **identifying, collecting, preserving, reviewing, and producing electronically stored information (ESI)** for legal cases, investigations, or court proceedings.
ESI includes emails, documents, databases, social media posts, audio/video files, and website data.

2. How it Functions (Process)

E-Discovery works through the following steps:

- **Identification:** Finding relevant electronic data sources.
- **Collection & Preservation:** Gathering ESI without altering original content.
- **Review & Analysis:** Examining data to find relevant evidence.
- **Production:** Providing the required digital information to the court or investigation team in a legally acceptable format.

3. Purpose

It helps lawyers and investigators obtain accurate digital evidence, maintain integrity, and present it properly during interrogatories, depositions, or document production.

Q-7.Name four different forms of web attacks. How are these web-based attacks examined?

ANS:

Q-1.What are the legal provisions against cybercrime?

ANS: Got it — here is a **better, cleaner 3-mark answer** with **just the necessary points**, exactly what GTU expects.

⭐ **3-Mark Answer: Legal Provisions Against Cybercrime**

Legal provisions against cybercrime in India mainly come from the **Information Technology (IT) Act, 2000** and certain sections of the **Indian Penal Code (IPC)**.

Under the IT Act, 2000:

- **Sec. 66** – Hacking and misuse of computer systems
- **Sec. 66C/66D** – Identity theft and online fraud
- **Sec. 66E** – Violation of privacy
- **Sec. 66F** – Cyber terrorism
- **Sec. 67** – Publishing/transmitting obscene content

Under IPC:

- **Sec. 292** – Obscene material
- **Sec. 354D** – Cyberstalking
- **Sec. 420** – Online cheating/fraud

Indian Evidence Act:

- **Section 65B** – Certificate required for electronic evidence to be admissible.

⭐ **Even Shorter (If you want 2–3 lines):**

The IT Act 2000 provides legal provisions like Sec. 66 (hacking), 66C/66D (identity theft & fraud), 66E (privacy), 66F (cyber terrorism), and 67 (obscenity).
IPC sections like 292, 354D, and 420 also punish online crimes.
Digital evidence must follow Section 65B for court admissibility.

Q-2.Write a note on Electronics discovery.

For 3 marks
Here is the **3-mark answer in clear points**, perfect for GTU.

⭐ **3-Mark Answer (in Points): Electronic Discovery**

4. **Electronic Discovery (E-Discovery)** is the process of identifying, collecting, preserving, and producing **electronically stored information (ESI)** for legal cases and investigations.
5. **ESI includes** emails, documents, presentations, databases, social media data, audio/video files, and website content.
   (PPT page 26)
6. E-Discovery is important because digital evidence is **easily modified or deleted**, so it must be handled carefully using proper legal procedures like interrogatories, depositions, and document production.
   (PPT page 27)

If you want, I can make a **1-mark definition** also.

For 7 marks

Here is a **complete 7-mark answer** on **Electronic Discovery**, written exactly from your PPT (pages 26–27) and expanded into clear points for full marks.

⭐ **Electronic Discovery (E-Discovery) – 7 Marks Answer**
Electronic Discovery, commonly called **E-Discovery**, is the legal process of identifying, collecting, preserving, reviewing, and producing **electronically stored information (ESI)** for use in investigations, lawsuits, or court proceedings.
ESI includes emails, documents, presentations, databases, chats, audio/video files, social media data, and website content.
Below are the **key points for a full 7-mark answer**:

⭐ **1. Definition of Electronic Discovery**
E-Discovery refers to the electronic aspect of discovering, collecting, and presenting digital evidence (ESI) during legal cases.
It ensures that electronic data is obtained legally and preserved in its original form.

⭐ **2. Types of ESI (Electronically Stored Information)**
E-Discovery deals with:

- Emails & attachments
- Office documents (Word, PDF, Excel)
- Databases & logs
- Social media posts
- Audio & video files
- Website content
- Voicemail & chat messages
- Any digital content stored on computers, phones, or servers
  (PPT page 26)

⭐ 3. Purpose of E-Discovery

The goal is to find **relevant electronic evidence** for court cases, investigations, or compliance.
It helps lawyers and investigators understand the truth behind events through digital footprints.

⭐ 4. The E-Discovery Process

It includes:

- Identification of relevant digital evidence
- Collection and imaging of ESI
- Preserving evidence without altering it
- Reviewing the data
- Producing the data in court-acceptable formats
  (PPT page 26)

⭐ 5. Importance in Legal Proceedings

Digital evidence is now widely used in civil and criminal cases.
E-Discovery ensures all relevant electronic data is available for both parties, maintaining transparency and fairness.

⭐ 6. Challenges of ESI

According to the PPT:

- ESI is **volatile**, easily modified, deleted, or duplicated
- Large volume of digital data makes review difficult
- Data can be spread across cloud servers, devices, or networks
  (PPT page 27)
  These challenges make E-Discovery more complex than dealing with paper records.

⭐ 7. Use in Litigation (Court Cases)

Common legal discovery methods:

- **Interrogatories** (written questions)
- **Depositions** (oral questioning)
- **Document Production Requests**
  E-Discovery focuses on producing **digital documents** required during these legal procedures.
  (PPT page 27)

Conclusion
Electronic Discovery is a critical process in modern digital forensics and legal investigations. It ensures that electronic evidence is properly identified, preserved, analyzed, and presented in court while maintaining integrity and legal validity.

Q-3.What is the most important legal features about digital evidence?(3 TIMES)

ANS

4-Mark Answer (6 Points): Important Legal Features About Digital Evidence

7. **Section 65B Requirement**
   Digital evidence is admissible in court only if accompanied by a valid **Section 65B certificate** from the Indian Evidence Act.
8. **Integrity and Authenticity**
   Digital data can be easily altered, so investigators must prove that the evidence has not been modified by using hashing and proper imaging methods.
9. **Proper Collection Procedure**
   Evidence must be collected using standard forensic practices (bit-by-bit imaging, write blockers). Improper handling makes it legally invalid.
10. **Chain of Custody**
    Every step of evidence handling must be documented. A broken chain of custody can lead to rejection of the evidence in court.
11. **Compliance with Cyber Laws**
    The evidence must relate to relevant sections of the **IT Act (Sec 43, 66, 67)** and IPC sections dealing with cybercrimes to support legal action.
12. **Privacy and Legal Boundaries**
    Investigators must respect privacy laws and avoid unauthorized access; illegally collected evidence may be declared inadmissible.

Q-4.Explain role of the forensic examiner in judicial system.

ANS:

Here is your **full 7-mark expanded answer** for:
⭐ **Role of the Forensic Examiner in the Judicial System (7 Marks)**
A forensic examiner plays an essential role in helping the judicial system handle digital evidence properly, fairly, and scientifically. Their work ensures that cybercrimes are investigated correctly and evidence is legally acceptable in court. The major roles are:

⭐ **1. Identification and Seizure of Digital Evidence**
The examiner identifies all possible digital evidence sources (computers, mobiles, cloud accounts, storage devices, logs).
They lawfully seize devices while ensuring no data is modified. This is the first and most crucial step in any investigation.

⭐ **2. Preservation of Evidence Integrity**
Digital evidence is fragile and easily altered.
Examiners preserve its integrity using:

- Write blockers
- Bit-by-bit imaging
- Hashing (MD5/SHA)
  This ensures the original evidence remains untouched and can stand legal scrutiny.

⭐ **3. Analysis and Reconstruction of Events**
Examiners analyze:

- Deleted files
- Browser history
- Registry, logs
- Metadata
- Network traffic
- Emails, chats, images
  They reconstruct timelines, user actions, and methods used in the cybercrime.
  This technical analysis helps convert raw data into meaningful evidence.

⭐ **4. Maintaining Chain of Custody**
Every movement of evidence is documented — who collected it, when, where it was stored, and who accessed it.

A proper chain of custody prevents accusations of tampering and ensures the evidence is admissible in court.

⭐ 5. Preparing Detailed Forensic Reports

Examiners prepare clear, accurate, and unbiased reports summarizing:

- Methods used
- Tools applied
- Findings
- Interpretation of results
  These reports act as strong support for judges, lawyers, and investigators who may not understand technical details.

⭐ 6. Assisting Investigators and Prosecutors

They help police, lawyers, and prosecutors understand technical aspects of digital evidence.
They guide them on what evidence to focus on, what data is relevant, and how the crime was committed.

⭐ 7. Expert Testimony in Court

The examiner appears as an **expert witness** and explains findings in simple language.
They justify the forensic methods used and defend the integrity of the evidence.
Their testimony can strongly influence the final judgment.

⭐ 8. Ensuring Evidence Meets Legal Requirements

Examiners make sure digital evidence complies with laws such as:

- **Section 65B of the Indian Evidence Act** (admissibility)
- IT Act & IPC sections
  They ensure that evidence is collected and presented legally and ethically.

⭐ Conclusion

A forensic examiner acts as a bridge between technology and the law.
Their work ensures that digital evidence is properly collected, preserved, analyzed, and presented, helping the judicial system deliver justice in cybercrime cases.

If you want, I can also prepare **extra short versions**, **diagram versions**, or **point-only versions** for quick revision.

Q-5.How do you write a digital forensic investigation report?

ANS:

Here is a **perfect 4-mark GTU-style answer** for:
⭐ **"How do you write a Digital Forensic Investigation Report?" (4 Marks)**
Short, clear, and in **point format** exactly suited for 4 marks.

⭐ **4-Mark Answer: Writing a Digital Forensic Investigation Report**

7. **Case Details and Purpose**
   Start with case number, investigator name, dates, and the purpose/scope of the investigation (e.g., hacking, data theft, fraud).
8. **Evidence Description**
   List all devices and media collected (laptop, hard disk, USB drive, phone), including serial numbers, model details, and seizure information to maintain proper chain of custody.
9. **Tools and Methods Used**
   Mention forensic tools (FTK Imager, EnCase, Autopsy), techniques such as bit-by-bit imaging, hashing, file carving, and procedures used during analysis.
10. **Analysis and Findings**
    Provide results such as recovered deleted files, logs, metadata, browser history, timestamps, or traces of unauthorized activity. Present only factual evidence.
11. **Conclusion**
    Summarize what the evidence proves (e.g., user activity, data theft, unauthorized access) based entirely on digital findings.
12. **Appendices/Supporting Data**
    Attach hash values, screenshots, tool logs, and chain-of-custody forms to support the validity of the report.

Q-6.Electronic data discovery: What is it? How it functions.
ANS:

Yes bro, this question is similar to the previous one but shorter.
Here is a **perfect 3-mark GTU-style answer**, simple and in point format.

⭐ **3-Mark Answer: Electronic Data Discovery – What is it? How it Functions?**

1. What is Electronic Data Discovery?

Electronic Data Discovery (E-Discovery) is the process of **identifying, collecting, preserving, reviewing, and producing electronically stored information (ESI)** for legal cases, investigations, or court proceedings.
ESI includes emails, documents, databases, social media posts, audio/video files, and website data.

2. How it Functions (Process)

E-Discovery works through the following steps:

- **Identification:** Finding relevant electronic data sources.
- **Collection & Preservation:** Gathering ESI without altering original content.
- **Review & Analysis:** Examining data to find relevant evidence.
- **Production:** Providing the required digital information to the court or investigation team in a legally acceptable format.

3. Purpose

It helps lawyers and investigators obtain accurate digital evidence, maintain integrity, and present it properly during interrogatories, depositions, or document production.

Q-7.Name four different forms of web attacks. How are these web-based attacks examined?

ANS:

Here is a full 7-mark GTU-style answer for:
⭐ “Name four different forms of web attacks. How are these web-based attacks examined?”
Clear, clean, and in exam-perfect points.

⭐ 7-Mark Answer
I. Four Different Forms of Web Attacks (Any Four)
1. SQL Injection (SQLi)
The attacker inserts malicious SQL code into input fields (like login forms) to access or modify database data.
Example: logging in without a password.

2. Cross-Site Scripting (XSS)
Attackers inject malicious scripts into a trusted website.
This script runs in the victim’s browser and can steal cookies, sessions, or redirect users.

3. Cross-Site Request Forgery (CSRF)
Attacker tricks a logged-in user into performing unwanted actions (like money transfer, password change) without their awareness.

4. Denial of Service (DoS) / Distributed DoS (DDoS)
Attackers flood a web server with massive requests to overload it and make the website unavailable.

5. Phishing Attack *(optional extra)*
Fake websites or forms are created to trick users into giving passwords, credit card details, OTP, etc.
You can write any four above.

⭐ II. How Web-Based Attacks Are Examined?
1. Log Analysis
Investigators examine server logs, access logs, error logs, and firewall logs to detect:

- unusual IP addresses
- repeated requests
- suspicious URLs

- SQL injection patterns
  Logs help recreate what the attacker did.

---

2. Browser and Client-Side Artifact Examination
Cookies, browsing history, cache, and session tokens are analyzed to identify:

- stolen session IDs
- malicious script execution
- phishing URLs visited
  These artifacts show how the user was targeted.

---

3. Network Traffic Analysis
Using tools like Wireshark, investigators inspect network packets to detect:

- suspicious payloads
- encoded scripts
- unexpected traffic patterns
- DoS traffic spikes

---

4. Web Server File System Analysis
Investigators check the server's directories to identify:

- uploaded malicious scripts
- modified web pages
- suspicious PHP/JS files
  This helps locate the attacker's footprint.

---

5. Database Examination
For SQL injection cases, the database logs and tables are checked for:

- unauthorized changes
- dumped tables
- deleted or altered records
  This confirms if data was extracted.

---

6. Malware / Script Reverse Engineering
If the attacker uploaded or injected a script, it is analyzed to understand its purpose, behavior, and payload.

---

7. Timeline Reconstruction
All events (logins, file changes, network activity) are arranged chronologically to understand:

- how the attack started
- what the attacker did
- what damage occurred
  This is essential for reporting.

⭐ Short Summary (last 2 lines for full marks)
Web attacks like SQL injection, XSS, CSRF, and DoS are examined using server log analysis, network traffic study, browser artifacts, database inspection, and script analysis. This helps investigators trace the attack path and understand the impact on the system.

DF CHAP 6 NOTES

1. Explain quality assurance in detail. (4m).

Quality Assurance (QA) in digital forensics refers to all the systematic activities carried out to ensure that the forensic process, tools, and examiners maintain accuracy, reliability, and integrity throughout an investigation. Its main goal is to produce results that are **repeatable, reproducible, and legally acceptable in court**.

Detailed Explanation:

1. Standard Operating Procedures (SOPs)

- QA ensures that every investigator follows **predefined and documented procedures**.
- SOPs include steps for evidence handling, imaging, analysis, and reporting.
- This ensures **uniformity** and reduces errors.

2. Tool Testing and Validation

- All forensic tools must be **tested and validated** before use.
- Testing ensures that tools give **correct, consistent, and repeatable results**.
- Validation helps confirm that tools do not alter the original evidence.

3. Evidence Integrity and Chain of Custody

- QA ensures that every piece of evidence has a **proper chain of custody record**.
- This includes documenting who handled the evidence, when, why, and how.
- Helps maintain **trustworthiness** and prevents tampering.

4. Examiner Competency and Training

- QA promotes regular training for forensic examiners.
- Ensures examiners are capable of using tools correctly and interpreting data.
- Includes certifications, workshops, and knowledge updates.

5. Quality Control (QC) Reviews

- QA includes **peer review** and **double-checking** of reports.
- Every investigation report is reviewed for accuracy before submission.
- This helps identify mistakes early and ensure **high-quality findings**.

6. Documentation and Reporting Standards

- QA requires detailed documentation of each step taken in an investigation.
- Reports must be clear, complete, and understandable for non-technical audiences.
- Proper documentation helps in presenting evidence in court.

2. Types of tools that can be selected for mobile device investigation. (3m)

Types of tools that can be selected for mobile device investigation (3 Marks)

Mobile device investigation requires specialized tools that can extract, analyze, and preserve data from smartphones and tablets. These tools can be broadly classified as follows:

1. Manual Extraction Tools

- These tools allow investigators to view data directly from the mobile device screen.
- Examples: Built-in phone menus, screenshots, screen recording apps.
- **Use:** Useful when device is locked or physical extraction is not possible.
- **Limitation:** Only visible data can be captured; cannot recover deleted files.

2. Logical Extraction Tools

- These tools extract data using the standard APIs provided by the mobile OS.
- **Data collected:** Contacts, SMS, call logs, installed apps, media files.
- **Examples:** *Cellebrite UFED Logical*, *Oxygen Forensic Suite*.
- **Use:** Safe method with minimal risk of data corruption.

3. File System Extraction Tools

- Provide access to the entire device file system.
- **Data collected:** App data, internal storage, configuration files, logs.
- **Examples:** *MSAB XRY*, *Magnet AXIOM*.
- **Use:** Deeper insight into app activities and user behavior.

3. Explain total validation in context of quality assurance. (4m)

Explain Total Validation in context of Quality Assurance. (4 marks)

Total Validation in Digital Forensics – GTU 4-Marks Answer

Total Validation refers to a *complete and end-to-end verification* of all processes, tools, and results used during a digital forensic investigation. The goal is to ensure that the investigation is **accurate, reliable, repeatable, and legally acceptable** in court.

Explanation:

1. **Ensures Tool Accuracy:**
   Total validation checks whether the forensic tools (like EnCase, Cellebrite, FTK) produce correct and consistent results. Tools are tested using known datasets to confirm that they extract data without altering the original evidence.
2. **Checks Entire Investigation Process:**
   It validates every step — evidence collection, preservation, analysis, and reporting. This ensures the process follows standard forensic guidelines such as NIST, ISO, or ACPO principles.
3. **Repeatability and Reproducibility:**
   A key part of total validation is ensuring that different investigators should get the *same results* when using the *same tools* on the *same evidence*. This builds trust in the investigation.
4. **Legal Reliability:**
   Courts require digital evidence to be validated. Total validation proves that the process was scientifically sound and the evidence is admissible. It also reduces the chance of legal challenges questioning tool errors.

4. What are the three types of tools used by DF examiners. (3m)

Digital forensic examiners mainly use the following **three types of tools**:

1. Hardware Tools

- These are physical devices used for acquiring and examining digital evidence.
- Examples: Write-blockers, forensic duplicators, SIM card readers, chip-off devices.
- Purpose: To extract data safely without modifying the original evidence.

2. Software Tools

- These are applications used to analyze, recover, and examine digital data.
- Examples: EnCase, FTK, Autopsy, Cellebrite UFED.
- Purpose: To perform tasks like data recovery, keyword search, file carving, timeline analysis, etc.

3. Open-Source Tools

- Free tools available to examiners for basic to advanced forensic analysis.
- Examples: Autopsy, Volatility, Wireshark, Oxygen Community Toolkit.
- Purpose: Low-cost alternative for analysis, useful for education, research, and initial investigation tasks.

5. What is hashing? Explain hashing concepts to maintain the integrity of evidence? (3m)

What is Hashing?

Hashing is a process of applying a **mathematical algorithm (hash function)** to digital data in order to generate a **fixed-size unique value** known as a **hash value or digital fingerprint**.
Common hash algorithms include **MD5, SHA-1, and SHA-256**.

Hashing Concepts to Maintain Integrity of Evidence

1. **Unique Digital Fingerprint:**
   Every file or evidence piece produces a unique hash value. Even a **1-bit change** in the data produces a completely different hash. This helps ensure that the evidence has not been altered.
2. **Integrity Verification:**
   When digital evidence is seized, its hash value is calculated. Later, during analysis and presentation in court, the same evidence is hashed again.
   - If **both hash values match**, it proves the evidence remained unchanged.
   - If they differ, it indicates tampering.
3. **Chain of Custody Support:**
   Hash values are recorded at every stage of evidence handling (collection, storage, transfer). This maintains a trustworthy **chain of custody**, ensuring investigators, lawyers, and courts that the evidence is authentic.

6. Differntiate Accrediation vs Certification. (4m)

Accreditation vs Certification (Tabular Form – 4 Marks)

Accreditation	Certification
Accreditation is the **formal recognition** that an organization (e.g., laboratory, institute) is competent to perform specific tasks according to standards.	Certification is the **validation of an individual or product** that it meets certain predefined standards or skills.
It is given to **organizations** (e.g., digital forensic labs).	It is given to **individuals or products** (e.g., certified examiner, certified tools).
Focuses on **overall competence, processes, quality system, and reliability**.	Focuses on **skills, knowledge, or capability** of a person or tool.
Granted by **accreditation bodies** (e.g., NABL, ISO/IEC 17025).	Granted by **certifying authorities** or vendors (e.g., EnCE, CHFI).
It ensures the **lab follows international standards** while handling evidence.	It ensures the **examiner or tool is qualified/standardized** to perform forensic tasks.

7. What three categories of tools do digital forensic investigators use? Explain it. (7m)

Digital forensic investigators use different types of tools to collect, analyze, and preserve digital evidence. These tools mainly fall into **three major categories**:

1) Hardware Tools

Hardware tools are **physical devices** used for acquiring and preserving data from computers, mobile phones, storage devices, etc.
They ensure **forensic soundness** by preventing accidental changes to the evidence.

Examples & Explanation:

- **Write Blockers (Tableau, WiebeTech):**
  Allow reading data from hard drives **without modifying** it, thus preserving evidence integrity.
- **Forensic Workstations (FRED, Talon, Forensic PC):**
  High-performance machines designed for imaging and analyzing large volumes of data.
- **Imaging Devices (Logicube Falcon, TD3):**
  Used to create **bit-by-bit copies** (forensic images) of storage media.
- **Cables, Adapters, Faraday Bags:**
  Protect devices like mobile phones from network signals to avoid remote tampering.

Purpose:

To **collect and preserve** evidence safely and reliably.

2) Software Tools

Software tools help investigators to **analyze acquired data**, recover deleted files, examine logs, extract artifacts, and generate reports.

Examples & Explanation:

- **EnCase Forensics:**
  Industry standard tool for in-depth forensic analysis, timeline generation, search, and reporting.
- **FTK (Forensic Toolkit):**
  Fast indexing, email analysis, file recovery, hash matching, etc.
- **Autopsy/Sleuth Kit:**
  Open-source suite for analyzing files, deleted data, browser history, keywords, etc.
- **Cellebrite UFED / Oxygen Forensics:**
  Specialized for **mobile device extraction**, app data, call logs, chats, etc.
- **Volatility / Rekall:**
  Used for **memory forensics** (RAM analysis).

Purpose:

To **examine, recover, search, and interpret** digital evidence.

3) Live (or “On-the-spot”) Analysis Tools

These tools help investigators collect data from a system that is still **powered ON**.
They are used when shutting down the system may destroy important evidence.

Examples & Explanation:

- **Sysinternals Suite (Process Explorer, Autoruns, TCPView):**
  Used to observe running processes, services, network connections.
- **Nmap / Wireshark:**
  Used for live network traffic capture and protocol analysis.
- **RAM Capture Tools (Belkasoft RAM Capture, FTK Imager Lite):**
  Used to capture **volatile data** like keys, passwords, and running processes.
- **Netstat, Command-line Utilities:**
  Collect active sessions, open ports, user activity.

Purpose:

To collect **volatile evidence**, i.e., data that disappears when the system is turned off.

DF CHP 7 NOTES

1. Explain network forensics techniques with examples. (7m)

Network Forensics Techniques (7 Marks Answer)

Network forensics is the branch of digital forensics that deals with **monitoring, capturing, analyzing, and investigating network traffic** to detect security incidents, cybercrimes, and policy violations.
Its main aim is to **trace attackers**, **identify malicious activities**, and **preserve evidence** for legal or organizational actions.

Below are the major **network forensics techniques**, explained in detail with examples.

1. Packet Sniffing / Packet Capture

Meaning:

Capturing all data packets traveling across a network to analyze their contents.

How it works:

Tools like **Wireshark** or **tcpdump** are used to capture packets in real time.

Use case example:

If an attacker is suspected of stealing login credentials, packet sniffing can identify **unencrypted usernames and passwords** in captured traffic.

2. Log Analysis

Meaning:

Examining logs generated by firewalls, routers, IDS/IPS, and servers.

Purpose:

To trace suspicious connections, failed login attempts, or unusual access patterns.

Example:

Firewall logs may show repeated login attempts from the same IP → indicates a **brute-force attack**.

3. Intrusion Detection and Prevention System (IDS/IPS) Analysis

Meaning:

Monitoring alerts generated by IDS/IPS tools.

Tools: Snort, Suricata.

Example:

IDS may detect a **SQL injection attempt** based on known attack signatures.
The forensic investigator analyzes the alert to confirm intrusion.

4. Traffic Analysis (Flow Analysis)

Meaning:

Analyzing network flow records (NetFlow, IPFIX) to understand communication patterns.

What it shows:

- Who communicated with whom
- Duration of the communication
- Amount of data sent

Example:

A sudden increase in outbound traffic from one system may indicate **data exfiltration** by a hacker.

---

5. Network Device Forensics

Meaning:

Investigating network devices like routers, switches, firewalls.

What investigators check:

- Routing tables
- ARP cache
- Configuration files
- Access Control Lists (ACLs)

Example:

Investigating whether a hacker tampered with router settings to **redirect traffic using malicious DNS servers**.

6. Deep Packet Inspection (DPI)

Meaning:

Examining the payload of each packet, not just headers.

Use:

To detect malware signatures or hidden malicious commands.

Example:

DPI can detect **command-and-control (C2) traffic** of a botnet hidden inside HTTP requests.

7. Correlation and Timeline Reconstruction

Meaning:

Combining evidence from different network sources to create a timeline of the attack.

Steps:

1. Collect logs from IDS, firewalls, servers
2. Arrange events chronologically
3. Understand attack flow

Example:

Timeline may reveal:

- 10:05 PM – Port scan from attacker's IP
- 10:07 PM – Exploit delivered
- 10:10 PM – Data exfiltrated

This helps identify how the attack happened.

2. Explain the use of Digital Forensics in social networking sites. (7m)

Use of Digital Forensics in Social Networking Sites

Digital Forensics plays a very important role in investigating crimes and incidents that take place on social networking platforms such as **Facebook, Instagram, Twitter, WhatsApp, Snapchat, LinkedIn**, etc. As these platforms store huge amounts of user-generated content, forensic experts extract, preserve, and analyze this information to identify suspects, victims, evidence, and patterns of criminal activity.

Below is a detailed 7-mark answer:

1. Identifying Fake Profiles and User Identity

Many cybercrimes happen through fake or anonymous accounts.
Digital forensics helps to:

- Track the **IP address**, **login history**, **device information**, and **location data** used to access the fake account.
- Identify the **real person** behind a fake profile.
  Example: Fake Instagram account used for cyberstalking can be traced using IP logs.

2. Recovering Deleted Messages, Posts, and Media

Users often delete posts, chats, comments, and photos after committing cybercrimes.
Forensic tools can recover:

- Deleted chats from WhatsApp/FB Messenger
- Removed posts, stories, videos
- Edited or hidden profile information
  This recovered data becomes key evidence.

3. Tracking Cyberbullying, Harassment, and Threats

Social networks are commonly used for:

- Online harassment
- Cyberbullying
- Threatening messages
- Abusive comments
  DF experts collect screenshots, message history, timestamps, metadata, and user activity to prove the crime.

4. Investigation of Fraud, Scams, and Phishing Attacks

Social platforms are widely used for financial scams and phishing.
Digital forensics can identify:

- The source of fake messages
- Fraudulent links shared
- The chain of communication
- Accounts involved in scam groups
  Example: A phishing link shared through Facebook message can be traced to the attacker's domain or device.

5. Geo-location and Activity Tracking

Many platforms store **location tags**, login locations, and GPS metadata.
Investigators use this to:

- Track suspect movement
- Confirm presence at crime scene
- Identify accomplices
  Example: A photo uploaded on Instagram may contain GPS metadata showing exact coordinates.

6. Evidence Collection for Cyberstalking Cases

Digital forensics helps collect:

- Timeline of stalker's interactions
- Profile visits
- Repeated messaging patterns
- IP logs from multiple devices
  This evidence is used in court.

7. Monitoring Terrorism, Hate Speech, and Illegal Activities

Social media is sometimes used to spread:

- Terrorist propaganda
- Hate content
- Illegal trade
- Human trafficking, drug sale
  DF investigators use keyword monitoring, AI tools, and social media forensics tools (like X1 Social Discovery) to track such activities and identify involved accounts.

3. Discuss e-mail header forensics in brief. (3m)

3. Discuss e-mail header forensics in brief. (3 Marks – GTU Style)

E-mail header forensics refers to the process of examining the hidden metadata present in an e-mail header to trace the **origin**, **path**, and **authenticity** of an e-mail message. Every e-mail contains a header that stores technical information such as sender's IP address, mail server details, timestamps, and routing hops.

Key Points:

1. **Identifying Sender Information:**
   The header includes fields like *From*, *Return-Path*, and *Received* lines. Investigators use these to verify whether the sender's address is spoofed or genuine.
2. **Tracing the E-mail Route:**
   The *Received* fields list all mail servers through which the e-mail passed. By analyzing these in reverse order, investigators can track the e-mail's journey and locate the original sending IP.
3. **Checking for Tampering or Spoofing:**
   Header forensics helps detect common cybercrimes like phishing, spamming, and impersonation. Analysts check inconsistencies between *Received* lines, unusual IPs, or mismatched timestamps.

Example:

If a phishing e-mail claims to be from "support@bank.com" but the header shows the origin IP belongs to another country, investigators conclude the e-mail is fraudulent.

4. Write case study of social networking sites. (4m)

Case Study: Cyberstalking Incident on Instagram

Case Overview

A college student reports repeated harassment and threatening messages from an unknown Instagram account. The suspect uses a fake profile, deletes chats, and frequently changes usernames. The case is handed to a digital forensic investigator.

Forensic Steps Taken

1. Evidence Collection

- The investigator captures **screenshots**, **message logs**, **profile information**, and **timestamps**.
- A legal request is sent to Instagram for:
  - IP login history
  - Device information
  - Linked email and phone
  - Account creation details

2. Metadata Analysis

- Each message and post contains metadata such as:
  - **Time sent**
  - **Device type**
  - **Location/IP address**
- Investigators correlate the IP addresses with the ISP to trace the suspect's physical location.

3. Timeline Reconstruction

- Using message history and login logs, a timeline is created:
  - Frequency of messages
  - Login locations
  - Changes made to the account
- Timeline helps connect events and confirm harassment patterns.

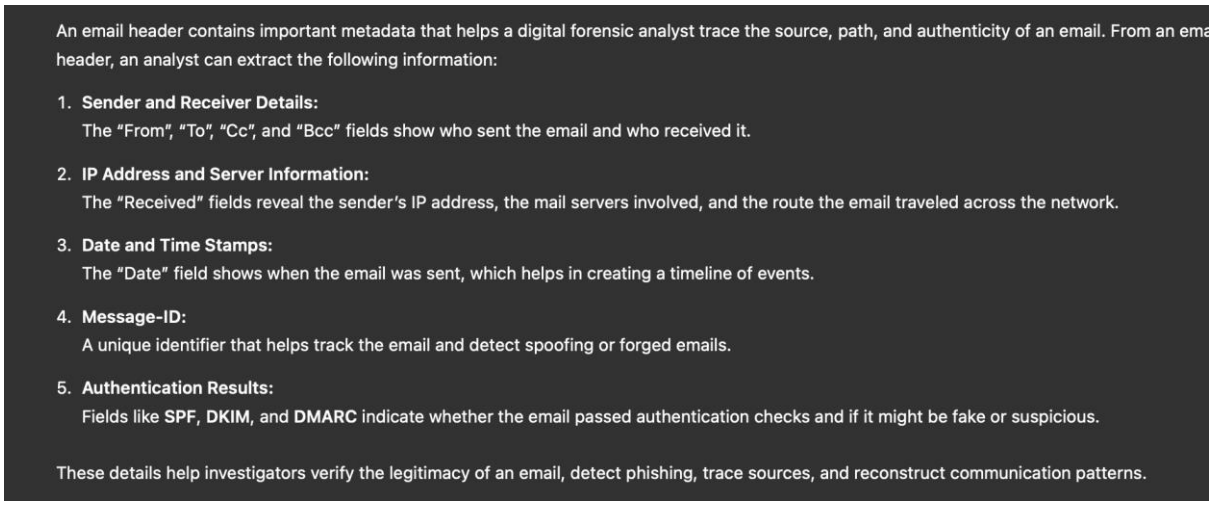
4. Linking Digital Identity

- Email ID used to create the account is traced.
- The same email and device details match another genuine account belonging to the suspect.
- Device fingerprinting shows:
  - Same smartphone model
  - Same OS version
  - Similar login times

5. Reporting

- Investigator prepares a **forensic report** including:
  - Evidence collected
  - Log details from Instagram
  - Device and IP analysis
  - Final conclusion linking suspect to the fake account

5. What information analyst could get from email header? (3m)

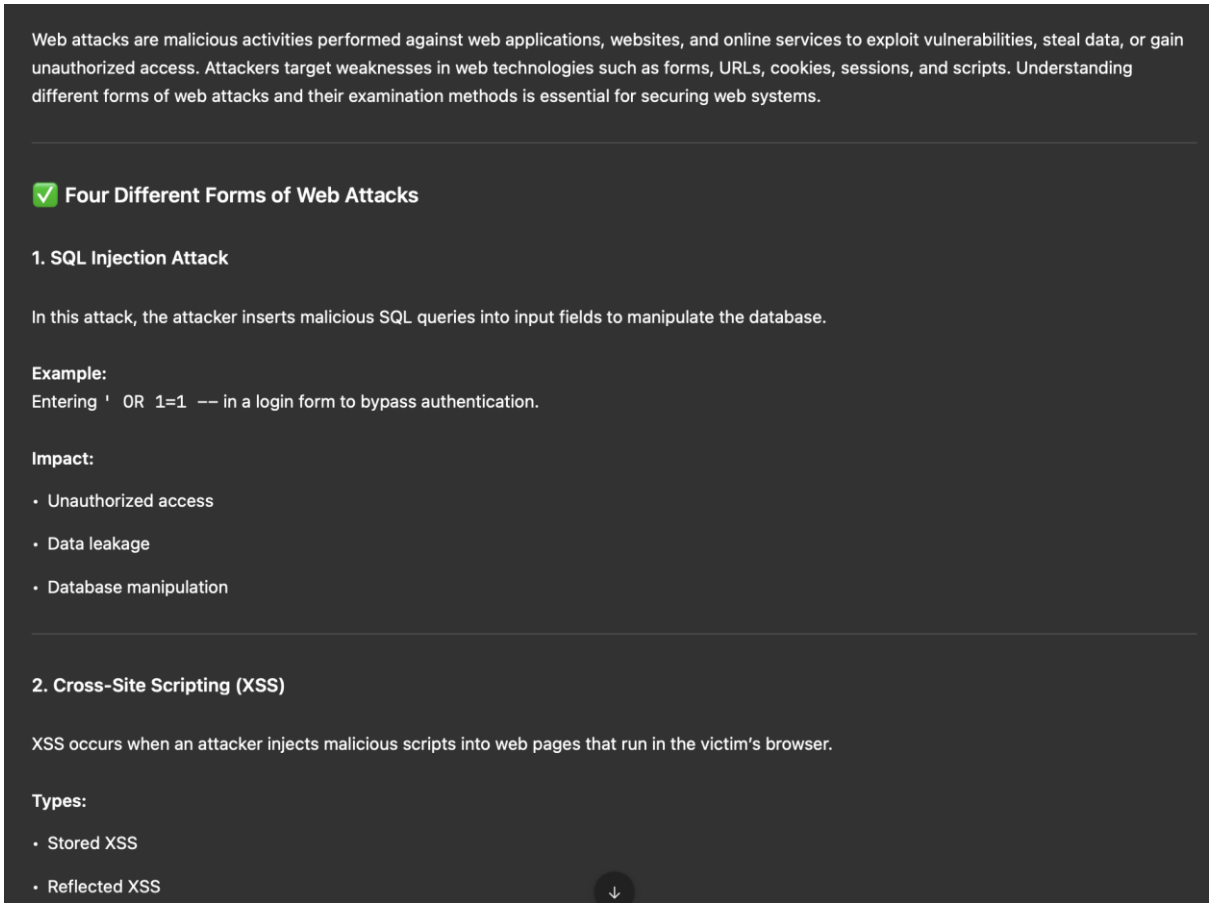


An email header contains important metadata that helps a digital forensic analyst trace the source, path, and authenticity of an email. From an ema header, an analyst can extract the following information:

1. **Sender and Receiver Details:**
   The "From", "To", "Cc", and "Bcc" fields show who sent the email and who received it.
2. **IP Address and Server Information:**
   The "Received" fields reveal the sender's IP address, the mail servers involved, and the route the email traveled across the network.
3. **Date and Time Stamps:**
   The "Date" field shows when the email was sent, which helps in creating a timeline of events.
4. **Message-ID:**
   A unique identifier that helps track the email and detect spoofing or forged emails.
5. **Authentication Results:**
   Fields like **SPF**, **DKIM**, and **DMARC** indicate whether the email passed authentication checks and if it might be fake or suspicious.

These details help investigators verify the legitimacy of an email, detect phishing, trace sources, and reconstruct communication patterns.

6. Name four different forms of web attacks. How are these web-based attacks examined? (7m)



Web attacks are malicious activities performed against web applications, websites, and online services to exploit vulnerabilities, steal data, or gain unauthorized access. Attackers target weaknesses in web technologies such as forms, URLs, cookies, sessions, and scripts. Understanding different forms of web attacks and their examination methods is essential for securing web systems.

✅ **Four Different Forms of Web Attacks**

1. SQL Injection Attack

In this attack, the attacker inserts malicious SQL queries into input fields to manipulate the database.

Example:
Entering `' OR 1=1 --` in a login form to bypass authentication.

Impact:

- Unauthorized access
- Data leakage
- Database manipulation

---

2. Cross-Site Scripting (XSS)

XSS occurs when an attacker injects malicious scripts into web pages that run in the victim's browser.

Types:

- Stored XSS
- Reflected XSS

- DOM-based XSS

Example:
A malicious script embedded in a comment section that steals user cookies.

Impact:

- Session hijacking
- Data theft
- Browser manipulation

---

3. Cross-Site Request Forgery (CSRF)

CSRF tricks a user into performing unintended actions on a website where they are authenticated.

Example:
A fake link causes a logged-in user to unknowingly transfer funds.

Impact:

- Unauthorized transactions
- Account misuse
- Data modification

4. Denial of Service (DoS) Attack

The attacker floods the web server with excessive requests, making it unavailable for legitimate users.

Example:
Sending thousands of requests per second to crash a website.

Impact:

- Server downtime
- Service unavailability
- Performance degradation

✅ Examination of Web-Based Attacks

Web attacks are examined using the following techniques:

1. Web Application Firewall (WAF)

Filters HTTP requests and blocks suspicious patterns such as SQL injection and XSS.

---

2. Vulnerability Scanning

Automated tools scan websites for known weaknesses and misconfigurations.

3. Log File Analysis

Server logs are analyzed to detect unusual requests, repeated failed logins, or abnormal traffic.

---

4. Signature-Based Detection

Identifies known attack patterns using predefined signatures.

---

5. Anomaly Detection

Monitors user behavior for deviations such as:

- Sudden traffic spikes
- Irregular access patterns

---

6. Penetration Testing

Simulated ethical hacking is performed to test system security.