

CSDF UNIT – 5 (Computer Forensics analysis and validation) – END-SEM PYQ Answers**➤ MAY / JUN 2023****Q5) a) Explain different approaches for validating forensic data. [9 Marks]**

Validation in computer forensics ensures that the **data and evidence collected are accurate, reliable, and have not been altered**. It helps confirm that the forensic tools and methods used produce consistent and authentic results. The validation process gives credibility to the evidence in legal proceedings.

1. Approaches for Validating Forensic Data**(i) Hash Function Approach**

- Hashing algorithms such as **MD5, SHA-1, or SHA-256** generate a unique digital fingerprint (hash value) for data.
- Before and after data collection, the hash value of files or disk images is compared.
- If both values match, it proves that **no modification or tampering** occurred.
- Example: Comparing hash values of a seized hard drive and its forensic image.

(ii) Tool Verification and Cross-Validation

- Using multiple forensic tools to analyze the same evidence and comparing results validates consistency.
- If different tools give identical outcomes, the data and findings are confirmed as accurate.
- Example: Verifying results obtained from EnCase with FTK or Autopsy software.

(iii) Repeatability and Reproducibility Testing

- Repeat the forensic process multiple times under the same conditions.
- If repeated tests yield the same results, it confirms the reliability of both the data and process.
- This principle ensures the evidence can withstand legal scrutiny.

(iv) Peer Review and Independent Verification

- Another qualified forensic expert independently reviews the process and findings.
- This ensures objectivity and removes the possibility of investigator bias.
- Peer validation adds **credibility and legal weight** to the forensic report.

(v) Validation Using Known Data Sets

- Known data sets (test images, sample malware, etc.) are used to verify that forensic tools detect and extract data accurately.
- This approach validates tool performance before applying it to real evidence.

2. Importance of Data Validation

- Ensures integrity and authenticity of digital evidence.
- Increases court admissibility of forensic reports.
- Builds confidence in the accuracy of forensic tools and processes.
- Helps maintain **chain of custody** and prevents manipulation claims.

b) Explain the approaches for seizing digital evidence at the crime scene. [8 Marks]

The process of **seizing digital evidence** at a crime scene is one of the most crucial steps in computer forensics. It involves the careful identification, collection, and preservation of electronic devices and storage media to ensure that the **evidence remains untampered** and admissible in court.

1. Preparation before Seizure

- Investigators prepare by carrying **forensic toolkits**, evidence bags, gloves, labeling materials, and write blockers.
- They also ensure **legal authorization**, such as a search warrant, before entering the scene.

2. Securing and Documenting the Scene

- The first step is to **secure the crime scene** to prevent unauthorized access.
- Investigators take **photographs and videos** of the digital devices and their connections before touching anything.
- Documentation includes system status, screen displays, and network connections.

3. Identifying and Labeling Digital Evidence

- Identify all possible sources of digital evidence like **computers, hard drives, USBs, mobile phones, routers, CCTV systems, etc.**
- Label each item clearly to maintain proper chain of custody.
- Record serial numbers, model, and condition of each device.

4. Handling Powered-On Systems

- If the system is **powered on**, investigators must decide whether to **pull the plug** or perform a **live acquisition**.
- **Live acquisition** is preferred when volatile data (like RAM, network connections, or running processes) needs to be captured.
- Pulling the plug is done only when necessary, ensuring the **preservation of evidence integrity**.

5. Using Forensic Tools and Write Blockers

- Storage devices are copied using **write blockers** to prevent accidental modification.
- Forensic imaging tools such as FTK Imager or EnCase are used to create **bit-by-bit copies** of the data for later analysis.

6. Maintaining Chain of Custody

- Every piece of evidence must be logged from the moment of collection.
- Record who collected it, when, and how it was stored and transferred.
- This ensures transparency and **authenticity** in court proceedings.

7. Transport and Storage

- Evidence must be **sealed, labeled, and transported** securely to the forensic lab.
- Devices are stored in **anti-static, temperature-controlled, and tamper-proof environments**.

Q6) a) Explain the process of identifying digital evidence in computer forensics. [9 Marks]

The **identification of digital evidence** is the first and most critical step in any computer forensic investigation. It involves recognizing, locating, and determining which data may be relevant to the investigation. Proper identification ensures that potential evidence is not missed or destroyed.

1. Understanding the Case Requirements

- Investigators begin by understanding the **nature of the crime** — whether it involves hacking, data theft, fraud, or cyber harassment.
- This helps to decide **what types of evidence** may be relevant (emails, logs, files, or network activity).

- Clear objectives guide the entire identification process.

2. Locating Possible Sources of Evidence

- Digital evidence can exist in **many forms and locations**, including:
 - Hard drives, SSDs
 - Mobile phones and tablets
 - Cloud storage and social media accounts
 - Network devices (routers, firewalls, servers)
 - External media like USBs or DVDs
- The investigator must list and locate all possible sources.

3. Classifying Evidence Types

- Digital evidence is divided into **volatile** and **non-volatile**:
 - **Volatile evidence:** Data stored in temporary memory (RAM, cache, running processes).
 - **Non-volatile evidence:** Data stored on permanent storage (hard drives, USBs).
- Volatile data must be captured **first**, as it disappears once power is lost.

4. Examining Live Systems

- If a computer is running, investigators perform a **live analysis** to capture volatile data:
 - Open connections
 - Running processes
 - Network activity
 - System time
- This information can be crucial for tracing current user activity.

5. Identifying Relevant Files and Data

- Once storage devices are accessed, specific files or logs related to the case are identified:
 - Emails, documents, chat logs
 - Browser history, deleted files
 - Metadata, registry entries, or timestamps
- Forensic tools (like EnCase, Autopsy, or FTK) are used to scan and identify these items systematically.

6. Marking and Labeling Evidence

- Every piece of identified evidence is **clearly labeled and documented**.
- Serial numbers, device IDs, and timestamps are recorded.
- This ensures **traceability and authenticity** of evidence in the chain of custody.

7. Preserving Identified Evidence

- Once evidence is identified, steps are taken to **preserve it without alteration**.
- Forensic imaging is performed using write blockers.
- Original data is sealed and stored securely, and analysis is done only on duplicates.

b) Explain Network Forensics and Order of Volatility for Computer System. [8 Marks]

Network forensics is a specialized branch of computer forensics that deals with **monitoring, capturing, analyzing, and investigating network traffic** to identify unauthorized access, data breaches, or other cybercrimes. It helps in tracking attackers, analyzing communication, and collecting admissible network evidence.

1. Network Forensics:

- Network forensics focuses on examining **data packets transmitted across networks** (LAN, WAN, or Internet).
- The main purpose is to **detect security incidents, reconstruct network events, and trace attackers** by studying traffic logs and communication patterns.
- It is useful for investigating **hacking, phishing, DoS attacks, or data leakage**.

2. Key Steps in Network Forensics

(i) Data Capture:

- Tools like Wireshark, tcpdump, or Network Miner are used to capture live traffic.
- Investigators record packets in real time without altering them.

(ii) Preservation:

- The captured data is securely stored to maintain its **integrity and authenticity** for legal use.
- Cryptographic hashing is often applied to verify originality.

(iii) Analysis:

- The recorded packets are analyzed to identify suspicious activities, communication patterns, and IP traces.
- Helps reveal malicious traffic, intrusion attempts, or data exfiltration.

(iv) Reporting:

- A detailed report is prepared describing findings, attack origin, and evidence logs.
- This documentation is crucial for court presentation and incident response.

3. Order of Volatility in Computer Systems

The **order of volatility** defines which data should be collected **first** during forensic investigation because some evidence disappears quickly when power is off.

Order (Highest → Lowest Volatility)	Type of Data	Description
1	CPU Registers, Cache, Running Processes (RAM)	Lost immediately after shutdown

Order (Highest → Lowest Volatility)	Type of Data	Description
2	Network Connections, Logs, Active Sessions	May expire or reset quickly
3	Temporary Files, Swap Space, Page File	May be overwritten soon
4	Hard Drive Data, Disk Files	Relatively stable unless deleted
5	Backups, Cloud Storage, External Drives	Least volatile and long-term evidence

4. Importance of Following Order of Volatility

- Ensures **no critical evidence** (like memory or session data) is lost.
- Maintains **accuracy and completeness** of forensic data.
- Supports reconstruction of events in **chronological order** for court presentation.

➤ MAY / JUN 2024

Q5) a) What are some common data hiding techniques? Explain any one in detail. [8 Marks]

Data hiding is the process of concealing digital information so that it cannot be easily detected, accessed, or modified by unauthorized users. In computer forensics, understanding these techniques is essential for detecting cybercrimes, data theft, and covert communication.

1. Common Data Hiding Techniques

- (i) **Steganography** – Hiding data within images, audio, or video files without altering their visible or audible appearance.
- (ii) **Encryption** – Transforming data into unreadable form using cryptographic keys.
- (iii) **File System Manipulation** – Hiding files in slack space, alternate data streams (ADS), or unallocated disk sectors.
- (iv) **Data Masking** – Replacing original data with fictional or scrambled data for privacy.
- (v) **Metadata Modification** – Altering file attributes (timestamps, author info, etc.) to conceal identity or timeline.

i) Steganography : Steganography is one of the **most common and powerful data hiding techniques** used in cybercrimes.

- **Meaning:** It hides a secret message within another digital medium, such as an image, audio, or text file, without changing its visible or functional appearance.
- **Working Principle:**
 - The secret data (e.g., text or code) is embedded in the **least significant bits (LSB)** of image pixels or sound samples.

- The modified file looks identical to the original file, making detection difficult.
- Specialized tools are used to hide and extract the concealed information.
- **Example:**
An image file (e.g., “photo.jpg”) may look normal but could contain a hidden text file inside it, stored in pixel data using steganographic tools like **Steghide** or **OpenStego**.
- **Applications:**
 - Used by hackers to hide malicious scripts or stolen data.
 - Used by organizations for **digital watermarking** and **copyright protection**.
- **Forensic Relevance:**
 - Investigators use **steganalysis tools** to detect hidden data by comparing original and modified files.
 - Techniques such as **statistical analysis** and **pattern recognition** help uncover concealed content.

b) What is the Honeynet Project, and how does it contribute to network forensics? [9 Marks]

- The **Honeynet Project** is an international research organization that develops and shares security tools to study cyber threats.
- It deploys **honeypots** and **honeynets** — systems intentionally designed to appear vulnerable — to attract hackers and analyze their behavior.
- The main goal is to understand the latest attack techniques, tools, and motives used by attackers.
- A **honeynet** is a network of decoy systems connected to monitor and record all activities of intruders.
- These systems simulate real networks but contain no valuable data, so any access attempt is suspicious and logged for forensic analysis.
- The data collected helps researchers strengthen security defenses and improve intrusion detection systems.

In network forensics, the Honeynet Project contributes by:

1. Capturing real attack traffic and malware in a controlled environment.
2. Providing detailed evidence of intrusion methods, tools, and exploit patterns.
3. Supporting law enforcement and cybersecurity experts with real-world data for investigation.
4. Helping to improve network monitoring and response capabilities against emerging threats.

Thus, the Honeynet Project serves as a critical platform for forensic investigators to study attacker behavior, validate detection systems, and enhance overall cybersecurity awareness through global collaboration.

Q6) a) What precautions should investigators take to prevent data alteration or loss during the seizure process? Explain any one in detail? [8]

During the seizure process, investigators must take several precautions to ensure that digital evidence remains unaltered, authentic, and admissible in court. Proper handling prevents accidental modification, loss, or contamination of evidence that could compromise the investigation.

Precautions include:

1. **Use of Write Blockers:** To prevent any changes to the original storage device when data is accessed or copied.
2. **Document Everything:** Maintain a detailed chain of custody log to record every step and person handling the evidence.
3. **Power Handling:** Avoid shutting down or restarting systems without assessing volatile data in RAM.
4. **Proper Packaging:** Use antistatic bags and tamper-proof seals to protect hardware from damage or tampering.
5. **Use of Forensic Imaging:** Create a verified bit-by-bit copy of data and analyze only the copy.
6. **Environmental Protection:** Ensure devices are kept in controlled temperature and humidity to avoid hardware degradation.

Example – Use of Write Blockers:

A write blocker is a hardware or software tool used to access digital storage devices without allowing any data modification. When investigators connect a suspect's hard drive through a write blocker, it ensures that the operating system cannot write or alter any files, timestamps, or metadata. This preserves the original evidence for court use. Write blockers also help maintain integrity by ensuring that analysis is always performed on a verified forensic copy.

This procedure guarantees **data authenticity, repeatability of analysis, and admissibility in legal proceedings** while protecting against accidental human or system-induced data modification.

b) What are the challenges and best practices associated with performing remote acquisitions? [9]

Remote acquisition is the process of collecting digital evidence from a system over a network rather than physically accessing the device. It is useful when devices are in different locations or when downtime must be minimized. However, it presents unique technical and legal challenges that investigators must handle carefully.

1. Challenges in Remote Acquisition

(i) Network Security Risks

- Data transferred over the internet may be intercepted or tampered with.
- Requires secure channels such as VPNs or encrypted tunnels to ensure confidentiality.

(ii) Bandwidth Limitations

- Large forensic images require significant time and bandwidth to transfer.

- Network congestion can lead to incomplete or corrupted acquisitions.

(iii) **Authentication and Access Issues**

- Gaining authorized remote access without violating privacy laws is difficult.
- Investigators must ensure proper credentials and legal warrants.

(iv) **Data Integrity Verification**

- Remote acquisitions increase the risk of altered or missing data packets.
- Hashing and checksum verification are mandatory to ensure authenticity.

(v) **Volatile Data Loss**

- Network latency may cause delay in capturing live data such as running processes or RAM contents.
- Timing is critical to avoid losing valuable volatile information.

2. Best Practices for Remote Acquisition

(i) **Use of Encrypted Communication Channels:** All data transmission should occur through secure, encrypted protocols (e.g., SSL, VPN, SSH) to prevent eavesdropping.

(ii) **Hash Verification:** Compute cryptographic hash values (MD5, SHA-1) before and after acquisition to confirm data integrity.

(iii) **Use of Specialized Tools:** Use trusted tools like **FTK Imager**, **EnCase Remote Agent**, or **DC3DD** for safe and verifiable acquisitions.

(iv) **Legal Authorization:** Always obtain necessary legal permissions before remotely accessing systems to avoid privacy violations.

(v) **Logging and Documentation:** Maintain a detailed record of timestamps, commands used, and tools applied during the acquisition for evidential transparency.

➤ MAY / JUN 2025

Q5) a) What steps should be taken to secure computer incident or crime scene before beginning the search for digital evidence?[8]

1. Ensure personal & scene safety

First check for any physical hazards (fire, electrical risk, biohazards) and ensure investigators wear appropriate PPE. Do not touch or move items unless required for safety—preserve the scene as found.

2. Isolate and control access to the scene

Establish a secure perimeter and limit entry to authorized personnel only. Use logs or an entry/exit register to record everyone who enters; this reduces risk of evidence tampering and maintains scene integrity.

3. Preserve volatile data and power-state decisions

Identify powered-on devices and decide whether to preserve volatile data (RAM, active network

connections) by performing live-collection if legally permissible. If live collection is not done, document the exact power state and take steps to prevent automatic changes (e.g., disable network to prevent remote access).

4. **Prevent remote tampering / network isolation**

If devices are network-connected, isolate them from external networks (air-gap or unplug network cable, disable Wi-Fi) to prevent remote wiping or intrusion, while avoiding actions that alter system clocks or volatile data unnecessarily.

5. **Document the scene thoroughly**

Take time-stamped photographs and/or video of the overall scene and each device in situ, plus detailed written notes describing locations, visible connections, labels, power states, and the environment. Photograph cable connections and screens exactly as found.

6. **Mark, tag and label evidence; establish initial chain of custody**

Assign unique identifiers to each device/item, tag them, and record who collected them, when, and why. Seal and package items appropriately to avoid contamination; keep all chain-of-custody records accurate and contemporaneous.

7. **Forensic handling and evidence preservation**

Use write-blockers when acquiring storage media, collect forensic images using validated tools, and store originals in secure, tamper-evident packaging. Preserve logs, removable media, and any peripheral devices; maintain environmental controls (temperature, humidity) where relevant.

8. **Legal and procedural compliance**

Ensure actions are authorized (warrant, consent, or lawful exception), document legal authority, and follow organizational policies and accepted forensic standards so that evidence remains admissible in court.

b) What is the honeyenet project, and how does it contribute to network forensics? [9]

→ Done

Q6) a) Why a digital hash is important while storing digital evidence, and how it is generated [9]

A *digital hash* (cryptographic hash) is a fixed-length string produced by a hash function from input data (file, disk image, memory dump). The same input always yields the same hash; any change in the input — even one bit — produces a different hash.

(1) Why a digital hash is important (forensic significance)

1. **Proof of integrity:** A hash proves that evidence has not changed since the hash was taken. If the computed hash at any later time matches the original, the data is unchanged.
2. **Tamper detection:** Any accidental or deliberate modification produces a different hash — making tampering evident.
3. **Chain-of-custody support & admissibility:** Hash values recorded with time/date and collector identity form strong, objective documentation that the evidence presented in court is the same as originally seized.
4. **Reliable comparison & de-duplication:** Hashes allow quick comparison of files/devices (e.g., identify known illicit files by comparing hashes to a database).

5. **Efficiency and reproducibility:** Hashes are small and easy to record; verifiers can independently recompute and confirm integrity without re-checking entire contents manually.

(2) How a digital hash is generated

1. **Prepare and document:** Record device identifiers, power state, serial numbers, time/date, who will compute the hash and why. Photograph the device in situ.
2. **Use forensically sound procedures:** If possible, acquire a forensic image (bit-for-bit copy) of the original storage using a write-blocker. Always compute hashes in a way that does not modify the original evidence.
3. **Compute the hash(s):** Generate hashes of the *original* media (if permitted) and of the *forensic image*. Record algorithm used (e.g., SHA-256) and the full hash string. It is best practice to compute more than one algorithm (e.g., MD5 for legacy compatibility + SHA-256 for robustness), but rely on strong algorithms for integrity.
4. **Record and store results:** Save the hash values in the case notes, on evidence tag, and within the forensic tool logs. Seal evidence and maintain chain-of-custody.

(3) Example commands / workflow (typical Linux forensic commands)

- Compute SHA-256 of a device node (requires privileges):
`sha256sum /dev/sdb`
- More controlled method reading via dd (useful to show imaging step):
`dd if=/dev/sdb bs=4M | tee image.dd | sha256sum`
This shows imaging and computes the hash of the image stream.
- Compute hash of a saved image file:
`sha256sum image.dd`
(Always record timestamps and the exact command/tool and version used.)

(4) Verification & ongoing use

- **Re-hash at each transfer or analysis step.** Whenever evidence is copied, transferred, or opened in a different environment, recompute hashes and record the comparison result.
- **Independent verification:** A prosecutor, defence, or lab peer can independently compute hashes from the provided image to confirm integrity.

b) What are some common network tool used in network forensics, Explain any one detail? [8]

Network forensics involves capturing, recording, and analyzing network traffic to investigate security incidents, intrusions, or policy violations. Specialized tools help investigators monitor, collect, and interpret network data efficiently.

(1) Common Network Forensic Tools

1. **Wireshark** – A widely used open-source packet analyzer for capturing and inspecting network traffic in real-time.

2. **Tcpdump** – A command-line packet capture tool that records network traffic for later analysis.
3. **Network Miner** – A passive network sniffer that extracts files, images, and credentials from captured traffic.
4. **Nmap (Network Mapper)** – Used for network discovery, port scanning, and identifying services running on hosts.
5. **Snort** – An open-source intrusion detection and prevention system (IDS/IPS) that analyzes traffic and detects malicious patterns.
6. **Xplico** – A tool that reconstructs application-layer data such as emails, VoIP calls, and web pages from captured packets.
7. **NetFlow / IPFIX Tools** – Used to analyze network flow data collected from routers and switches to identify unusual traffic behavior.

(2) Detailed Explanation — Wireshark

Overview: Wireshark is the most popular open-source packet analyzer used in network forensics. It allows live capture and offline analysis of network packets across various protocols such as TCP, UDP, HTTP, DNS, and SSL.

Key Features:

- Captures packets in real-time and displays detailed protocol-level information.
- Provides filtering options (e.g., `ip.addr == 192.168.1.5`) to isolate suspicious traffic.
- Supports hundreds of protocols and can decode encrypted or compressed data (if keys are available).
- Allows exporting of captured data in pcap format for later analysis or evidence presentation.
- Enables color coding and graphical statistics (e.g., conversation charts, protocol hierarchy) for easy visualization.

Use in Forensics: Investigators use Wireshark to trace suspicious connections, detect data exfiltration attempts, analyze malware communication, or reconstruct the sequence of events during a cyberattack. The tool's detailed packet view helps identify source and destination IPs, ports, and payloads, which can be correlated with intrusion timelines.

Example Scenario: If a suspected system is communicating with a malicious IP, Wireshark can capture those packets, revealing commands or stolen data being transmitted — providing vital digital evidence in network intrusion investigations.

➤ NOV / DEC 2023

Q5) b) What is the honeynet project, how does it contribute to network forensics? [9]

→ Done

Q5) a) How do investigators determine which data is relevant to collect & analyze in digital forensics investigation? [8]

In digital forensics, determining *relevant data* means identifying which information is most useful in proving or disproving an incident or crime. Investigators must balance thoroughness with focus — collecting all potential evidence while avoiding unnecessary or unrelated data.

(1) Understand the case objective and legal scope

Investigators begin by reviewing the case details, such as the type of incident (e.g., data theft, unauthorized access, cyber fraud) and legal authorization (warrant or consent). The objective defines what kind of data is relevant — for example, in an email fraud case, only communication and transaction logs may matter. Clear understanding prevents collecting irrelevant or inadmissible data.

(2) Identify potential sources of digital evidence

Based on the case, investigators locate systems, devices, or media likely to hold useful evidence. These include computers, mobile phones, servers, cloud storage, USB drives, and network logs. By mapping how data flows through these sources, they can target the most informative ones for acquisition.

(3) Use triage and prioritization techniques

Digital evidence is often huge, so investigators use triage to focus on the most critical data first. For example, they might prioritize volatile data (RAM, active sessions) or files modified around the incident time. Triage tools and timelines help filter unnecessary data and speed up analysis.

(4) Examine metadata and contextual clues

File metadata (timestamps, owners, access history), registry entries, browser logs, and communication patterns help determine if files or actions relate to the event. Investigators check file extensions, keywords, and user accounts to confirm relevance before deeper analysis.

(5) Apply keyword and content-based searches

Specialized forensic tools (e.g., EnCase, FTK, Autopsy) allow searching for keywords, email addresses, file types, or hash matches. These searches isolate data linked to the case — like emails with certain subjects or documents containing sensitive terms.

(6) Consider timeline correlation

Investigators build a timeline of digital activity using log files, file system timestamps, and system events. Events that match or surround the reported incident time are marked as relevant and analyzed further to reconstruct user behavior.

(7) Validate relevance through cross-correlation

Collected evidence is compared across different devices or logs — for example, matching a login time on a server with a file modification on a workstation. Cross-verification strengthens the reliability and reduces false relevance.

(8) Maintain documentation and justification

At each step, investigators record *why* certain data was selected and *how* it relates to the case hypothesis. Proper documentation ensures transparency, reproducibility, and admissibility in court.

Q6) a) Why is data validation crucial in digital forensics & what methods are commonly used for data validation? [8]

Data validation in digital forensics refers to the process of confirming that digital evidence has remained authentic, accurate, and unaltered from the moment it was collected to the time it is presented in court. It ensures that the integrity of evidence is maintained throughout the investigation.

(1) Importance / Need for Data Validation

1. **Ensures Evidence Integrity:**
Validation confirms that the evidence collected has not been tampered with or modified. This guarantees that what investigators analyze is an exact copy of the original data.
2. **Maintains Chain of Custody:**
Every time evidence is transferred, copied, or examined, validation checks (like hash comparison) ensure it remains consistent across all stages — strengthening the credibility of the chain of custody.
3. **Legal Admissibility in Court:**
Courts require proof that evidence presented is authentic. Data validation provides scientific assurance that the digital evidence is genuine, reliable, and can be trusted in legal proceedings.
4. **Prevents Accidental Corruption or Tool Errors:**
Validation helps detect any unintentional errors caused during imaging, storage, or analysis. It confirms that forensic tools or hardware did not alter the evidence.
5. **Supports Reproducibility of Results:**
When other investigators or legal experts re-examine the same evidence and compute the same validation values, they should obtain identical results — proving the process is repeatable and trustworthy.

(2) Common Methods of Data Validation

1. **Hashing Techniques:**
Cryptographic hash functions like **MD5**, **SHA-1**, and **SHA-256** generate a fixed-length digital fingerprint of evidence. The hash of the original and copied data are compared — if they match, integrity is confirmed.
Example: sha256sum image.dd → both original and duplicate must produce the same hash value.
2. **Checksums:**
Simpler than hashes, checksums (like CRC32) provide a basic integrity check to detect accidental data corruption during transfer or storage. However, they are less secure for forensic use due to collision risks.
3. **Bit-by-Bit Comparison:**
In this method, every byte of the original media is compared with its forensic image to ensure a 100% identical copy. It provides strong validation but can be time-consuming for large drives.

4. **Tool Verification and Cross-Validation:**

Evidence is verified using multiple forensic tools to confirm consistent results. For example, computing a SHA-256 hash using both EnCase and FTK should yield the same output — proving reliability of tools.

5. **Digital Signatures (Advanced Method):**

Digital signatures combine cryptographic hashing with encryption to ensure authenticity and non-repudiation of digital evidence. This is often used in high-security forensic workflows.

b) Describe the process of seizing digital evidence at a crime or incident scene?[9]

Seizing digital evidence refers to the lawful and systematic process of identifying, documenting, collecting, and securing electronic devices or storage media that may contain potential digital evidence from a crime or incident scene. The main goal is to preserve data integrity while maintaining legal admissibility.

(1) Ensure Legal Authority and Safety: Before beginning the seizure, investigators must confirm they have valid legal authorization such as a *search warrant* or *consent from the owner*. Scene safety is the first priority — ensuring no electrical, chemical, or physical hazards exist.

(2) Secure and Control the Scene: Establish a clear perimeter and restrict entry to essential forensic staff. Use logs to record every person entering or leaving. This prevents tampering and maintains scene integrity. Investigators should photograph the scene before moving or disconnecting anything to capture the original condition of devices and cables.

(3) Document Everything Thoroughly: Detailed documentation is essential. Investigators must record the *date, time, location, device description, serial numbers, power status, and connection details*. Photographs or videos should be taken from multiple angles, showing how devices are connected to networks or other peripherals. All observations should be entered in official notes.

(4) Identify and Prioritize Digital Devices: Identify all potential sources of digital evidence — such as computers, laptops, mobile phones, USB drives, external hard disks, CCTV DVRs, routers, and cloud access devices. Prioritize devices most likely to contain critical data related to the crime (e.g., suspect's computer or communication device).

(5) Handle Powered-On and Powered-Off Devices Appropriately

- **If powered ON:** Determine whether to perform a *live acquisition* (to capture volatile data such as RAM, network connections, and running processes) or to shut down safely to prevent alteration.
- **If powered OFF:** Do not power it on. Label and collect the device as-is. Connecting it to power may modify evidence.

(6) Prevent Remote Access or Data Destruction: Immediately disconnect devices from networks to stop remote tampering. For Wi-Fi or Bluetooth devices, disable wireless communication. If a system is network-connected, isolate it by unplugging network cables or disabling the interface, avoiding changes to stored data.

(7) Collect, Label, and Package Evidence: Each seized item is assigned a unique evidence number and properly labeled with details such as description, collector's name, date, and time. Devices

should be packed in anti-static and tamper-evident bags. Special precautions (e.g., Faraday bags) are used for wireless devices to block remote access signals.

(8) Maintain Chain of Custody: A *chain of custody form* must accompany every item collected. It records who collected the evidence, when and where it was collected, and who handled it next. This document ensures traceability and authenticity during court proceedings.

➤ NOV / DEC 2024

Q5) a) What are some common network tools, used in network forensics. [9]

→ Done

b) Describe the process of seizing digital evidence at a crime or incident scene? [8]

→ Done

Q6) a) What is the honeynet project, how does it contribute to network forensics? [9]

→ Done

b) Give in detail the different techniques to hide data in digital forensics?[8]

Data hiding (anti-forensic techniques) are methods used to conceal information from discovery, analysis, or attribution. Investigators must know common techniques and their forensic indicators to detect and recover hidden data.

1. Steganography

- **What:** Embedding secret data inside carrier files (images, audio, video, text) so that the carrier looks normal.
- **How:** LSB (least-significant-bit) modification in images/audio, hiding in image palettes, or embedding in metadata fields.
- **Forensic notes:** Look for statistical anomalies, unexpected changes in file size, or use stego-detection tools (steganalysis). Extracting hidden payloads often requires known carrier and method.

2. Encryption and Encrypted Containers

- **What:** Using cryptographic algorithms (AES, etc.) to render data unreadable without keys; creating encrypted containers (VeraCrypt, BitLocker).
- **How:** Full-disk encryption, encrypted files, hidden volumes (plausible deniability).
- **Forensic notes:** Detect presence via headers, entropy (high entropy suggests encryption), and metadata. Access requires keys/passwords — forensic acquisition preserves containers for offline brute-force/credential recovery.

3. Alternate Data Streams (ADS) on NTFS

- **What:** Storing data in NTFS ADS attached to a filename (e.g., file.txt:secret) which is invisible in many directory listings.
- **How:** Tools or commands create/read ADS; they don't increase the visible file size.
- **Forensic notes:** Use specialized tools to enumerate ADS; examine MFT records and file slack to locate ADS entries.

4. Hidden / Unallocated Space (Slack Space & Unused Sectors)

- **What:** Placing data in file slack (space between end of file and end of cluster) or in unallocated disk sectors.
- **How:** Directly write raw data into unallocated clusters or manipulate file sizes to create slack-containing payloads.
- **Forensic notes:** Carve unallocated space and slack for file fragments; raw imaging and carving techniques can recover hidden content.

5. Hidden Partitions and Filesystem Manipulation

- **What:** Creating partitions not visible to the OS (deleted/hidden partition table entries) or using obscure filesystems.
- **How:** Modify partition table (MBR/GPT) or use nested/hidden partitions and stego file systems.
- **Forensic notes:** Analyze disk geometry and partition tables; look for gaps between partitions and use full-disk imaging to reveal hidden partitions.

6. Timestomping and Timestamp Manipulation

- **What:** Altering file timestamps (creation, modification, access) to mislead timelines.
- **How:** Use tools (e.g., touch, forensic timestomp utilities) or rootkits to change metadata.
- **Forensic notes:** Cross-check timestamps with other artifacts (logs, MFT entries, prefetch, browser history) to spot inconsistencies.

➤ Additional question from Nov/Dec 2022:

Q5) a) Explain how to perform remote and live acquisitions with an appropriate example. [9]

1. Remote Acquisition

- Remote acquisition involves acquiring digital evidence from a suspect system over a network without physical access, using specialized tools to connect securely and copy data like drives or RAM while minimizing alterations.
- **Process:**
 - Install or deploy a remote agent (e.g., PDServer in ProDiscover) on the target system if permitted, or use network-based tools.
 - Establish an encrypted connection from the forensic workstation to the target via LAN/WAN.
 - Preview the drive, capture volatile data (RAM, processes), perform bit-stream imaging, and verify with hashes (MD5/SHA).
 - Log all actions for chain of custody, avoiding detection modes if stealth is needed.
- **Example: ProDiscover Investigator:**
 - Connect remotely to a suspect Windows server suspected of data exfiltration.
 - Use encrypted link to preview C: drive, copy RAM contents, acquire full disk image to forensic server.
 - Analyze running processes remotely for malware; benefits include no downtime but risks network interference or agent detection.

2. Live Acquisition

- Live acquisition captures volatile data from a running system (e.g., RAM, network connections, processes) before shutdown, as powering off loses this evidence; used when system cannot be seized immediately.
- **Process (Order of Volatility):**
 - Boot from forensic live CD/USB (e.g., with Magnet RAM Capture or KAPE) or use trusted shell on running OS.
 - Collect volatile data first: network state (arp, netstat), RAM dump, running processes (tasklist), clipboard, then non-volatile like disk images via write-blockers.
 - Hash outputs (MD5), transmit to secure storage via Netcat/Cryptcat, document timestamps and tools used.
 - Minimize footprint: avoid altering system, photograph screen state.
- **Example: Incident Response on Running Laptop:**
 - Suspect laptop shows active malware; insert USB with KAPE triager.
 - Capture RAM (Magnet RAM Capture), network connections, browser artifacts; triage files without full imaging.
 - Export to external drive, verify hashes; preserves ephemeral evidence like encryption keys lost on shutdown.

Note: Please check and verify all answers once before referring.