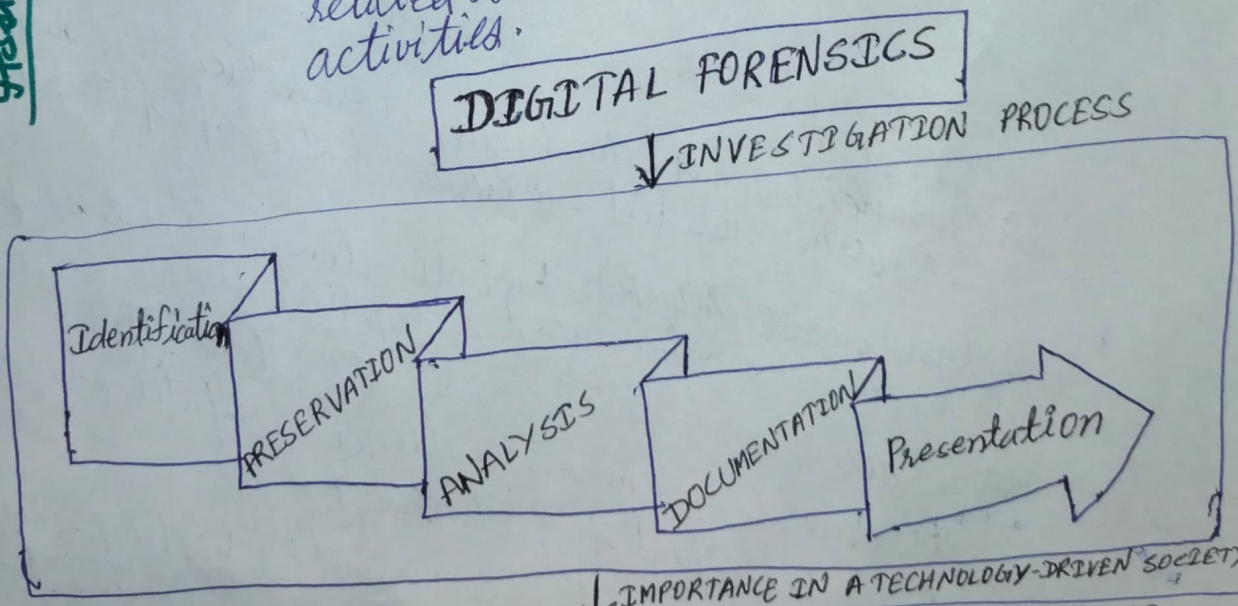
Name - ASHUTOSH KUMAR, CSE(AI&ML-A), (01)
Roll - 2300321530046, Subject - Cyber security
Date - 06/06/2025, Total No of pages - 10

# Assignment - 04 (BCC401)

Q1 Define digital forensics and explain its importance in modern technology-driven society. Provide examples of scenarios where digital forensics is crucial.

Ans. :- **Digital Forensics**

- Digital forensics is a branch of forensic science focused on the identification, preservation, analysis, and presentation of electronic data that can be used as evidence in legal cases.
- It involves the systematic investigation of digital devices (such as computers, smartphones, and storage media) to uncover and interpret information related to criminal or unauthorized activities.




Assignment-04(BCC401), Roll-2300321530046, Ashutosh Kumar, CSE(AI&ML-A), Total No. of Pages-10

Ans. (1) :- (contd--)

## Importance in Modern society

☆ In today's technology-driven world, vast amounts of sensitive information are stored and transmitted electronically. ☆ Digital forensics is crucial for:

→ Investigating cybercrimes such as hacking, data theft, and online fraud.
→ Supporting legal cases by providing admissible digital evidence.
→ Responding to incidents like data breaches, malware, attacks, and insider threats.
→ Tracking cybercriminals by following digital trails and analyzing logs.
→ Preventing future incidents by identifying vulnerabilities and strengthening cybersecurity policies.

## Examples of Scenarios where Digital Forensics is Crucial:

☆ Financial Fraud: Analyzing transaction logs and recovering deleted emails to identify perpetrators.
☆ Ransomware Attacks: Investigating malware samples, tracing the origin, and decrypting files.
☆ Insider Threats: Recovering deleted files or emails from an employee's computer suspected of intellectual property theft.
☆ Cyberbullying and Harassment: Collecting evidence from social media and messaging platforms to support legal action.

Ans. (1) :- (contd-)

☆ Data Breaches: Tracing unauthorized data transfers and identifying compromised accounts.

(Q2) Discuss the tools and technologies commonly used in digital forensics.

Ans. :- Common Tools and Technologies commonly used in digital forensics.

☆ Disk Imaging and Analysis:

→ EnCase: used for imaging, recovering, and analyzing files from storage devices.

→ FTK (Forensic Toolkit): For creating forensic images and analyzing file systems.

→ Autospy: open source platform for analyzing hard drives and file systems.

☆ Memory Forensics:

→ Volatility, Rekall: Tools for analyzing volatile memory (RAM) to detect running processes, malware, and encryption keys.

☆ Mobile Device Forensics:

→ Cellebrite, Oxygen, Forensic Suite: extract data from smartphones and tablets, including messages, call logs, and app data.

☆ Network Forensics:

→ Wireshark: Captures and analyzes network traffic to detect malicious activities.

→ Snort, Zeek (Bro): Intrusion detection and network monitoring tools.

Ans. (2) :- ☆ Email Forensics:
(contd--) → MailXaminer, X1 Social Discovery: Analyze email communications, headers, and attachments.

☆ Cloud Forensics:
→ Magnet AXIOM, FTK: Tools for acquiring and analyzing data from cloud storage services.

☆ Hashing and Integrity Verification:
→ MD5, SHA-256 utilities: Ensure evidence integrity by generating digital fingerprints.

☆ Other Utilities:
→ Write-blockers: Prevent modification of evidence during acquisition.
→ Forensic data recovery tools: Recuva, R-Studio for recovering deleted files.

(Q3) Discuss the phases of the digital forensics lifecycle with a diagram. Explain the activities carried out in each phase.

Ans:- The digital forensics lifecycle is a structured process that ensures the integrity and admissibility of digital evidence.

The key phases are:

☆ Identification:- Recognize potential digital evidence and determine the scope of the case (devices, data types).

☆ Preservation: Secure evidence to prevent tampering or alteration; create forensic images; document chain of custody.

☆ Collection: Systematically gather evidence using forensic tools; ensure legal compliance and documentation.

Ans (3) (contd.) :-

☆ Examination : Use specialized tools to extract, recover, and scrutinize data (e.g., deleted files, metadata). (05)

☆ Analysis : Correlate and interpret evidence, reconstruct timelines, identify patterns or anomalies.

☆ Reporting : Prepare detailed, clear, and legally defensible reports with findings, methods, and conclusions.

☆ Presentation : Present findings to stakeholders (law enforcement, court, management) in an understandable way.

(Q4) What is e-mail forensics? Describe the process of analyzing e-mails for digital evidence.

Ans :- E-mail forensics is a specialized branch of digital forensics focused on investigating and analyzing email communication to uncover evidence of cybercrimes such as phishing, fraud, data breaches, or harassment.

Process of Analyzing E-mails for Digital Evidence

(i) Email Acquisition

☆ Collect suspect emails from sources like email servers, clients, or device backups.

☆ Export data in formats such as .pst, .ost, or .eml.

(ii) Preservation of Evidence

☆ Use hashing (MD5, SHA-256) to ensure data integrity.

☆ Document all actions for chain of custody.

(iii) Email Header Analysis

☆ Examine metadata: sender, recipient, timestamps, IP addresses, and message routing.

☆ Trace the email's journey and identify spoofed or forged headers.

Ans. (4) :- (iv) Content Analysis

(contd--)

☆ Analyze the email body, attachments, and embedded links for malicious content.
☆ Scan attachments for malware and check links using tools like Virus Total.

(v) Attachment and Link Analysis

☆ Extract and scan attachments for malware or exploits.
☆ Analyze URLs for phishing or malicious redirects.

(vi) Metadata Analysis:

☆ Investigate hidden data, such as ~~geological~~ geolocation tags or device information.

(vii) Spam and Phishing Filter Logs.

☆ Review email filter logs to determine if the email bypassed detection systems.

(viii) Social engineering Analysis

☆ Identify attempts to deceive or manipulate the recipient (e.g., urgent requests for sensitive info).

(ix) Legal Documentation and Reporting

☆ Record all analysis steps, tools used, and findings.
☆ Prepare a comprehensive report for legal or organizational use.

Ans. (4) (contd.):- Key Indicators of Malicious Emails: (07)

- ☆ Suspicious sender address or domain.
- ☆ Generic greetings and urgent language.
- ☆ Poor grammar and spelling.
- ☆ Suspicious links or unexpected attachments.
- ☆ Requests for sensitive information.
- ☆ Spoofed domains or mismatched sender details.

(Q5) Define network forensics and explain its role in cyber incident response.

Ans:- Network forensics is a branch of digital forensics that involves monitoring, capturing, analyzing, and investigating network traffic to identify malicious activities, security breaches, and unauthorized access.

Role in Cyber Incident Response.

- ☆ Detecting Cyberattacks: Identifies intrusion attempts, malware communication, or DDoS attacks by analyzing traffic patterns and anomalies.
- ☆ Preventing Data Breaches: Tracks unusual data transfers or unauthorized access to sensitive information.
- ☆ Incident Response: Helps understand the attack vector, reconstruct events, and restore systems.
- ☆ Legal Investigations: Provides admissible evidence for use in court.

Ans. (5) :- Typical steps:

(contd-)

- Capture network data using tools like Wireshark or Netflow.
- Filter relevant logs and traffic.
- Analyze packets for malicious payloads or anomalies.
- Reconstruct events to understand attacker actions.
- Report findings for legal or organizational action.

(8b) Explain the security and privacy threats associated with the use of social networking sites.

Ans :- Social Networking Sites (SNS) pose significant security and privacy risks, including:

- Identity Theft: Cybercriminals steal personal information to impersonate users.
- Phishing Attacks: Fradulent messages or links are used to steal credentials or financial data.
- Malware Distribution: Malicious links or files infect devices with malware or spyware.
- Social Engineering: Attackers manipulate users into revealing confidential information.
- Privacy Breaches: Personal data is misused by third parties or hackers.
- Cyberbullying and Harassment: SNS are often misused for bullying or hate speech.

Ans. (6) (contd-) :- ★ Fake News and Misinformation: False information spreads quickly, causing panic or harm.

★ Data Harvesting: Third-party apps collect excessive personal data without user consent.

## Forensic Cases:

★ Tracing harassment to fake accounts.

★ Investigating phishing campaigns via SNS messages.

★ Identifying data theft through fake profiles.

(Q7) What challenges do forensic investigators face when collecting evidence from social media platforms?

Ans. :- ★ ~~Encryption~~ Challenges: End-to-end encryption on platforms like WhatsApp hinders access to private messages.

★ Data Volatility: Posts and messages can be deleted or are temporary (e.g., Snapchat, Instagram stories).

★ Jurisdictional Issues: Data may be stored in different countries with varying laws.

★ Platform Restrictions: Limited access due to privacy policies or lack of cooperation from SNS providers.

★ Volume of Data: Enormous volume of posts, messages, and interactions complicates evidence collection.

★ Authentication: Proving the authenticity and origin of social media content can be difficult.

# Assignment-04 (BCC401)

(10)

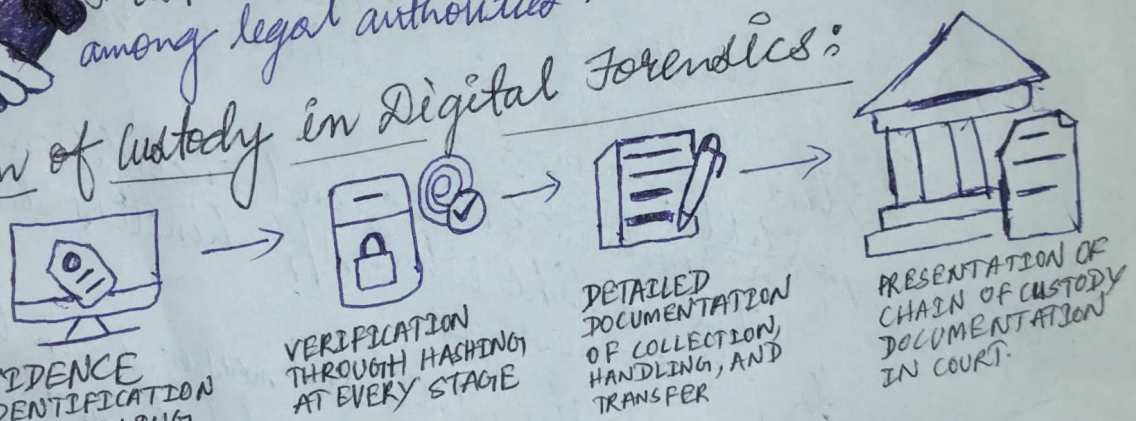
(Q8) What is the chain of custody in digital forensics? Explain its significance in ensuring the admissibility of evidence in court.

Ans:- Chain of custody is a documented process that tracks the handling of digital evidence from collection to presentation in legal proceedings, ensuring evidence remains unaltered and admissible.

## Significance:

- ★ Maintains Integrity: Ensures evidence is not tampered with.
- ★ Legal Admissibility: Provides proof of authenticity for court.
- ★ Accountability: Tracks who handled evidence, when, and why.
- ★ Trustworthiness: Builds confidence in the evidence among legal authorities.

## Chain of Custody in Digital Forensics:




## Key Components:

- ★ Evidence identification and labeling.
- ★ Detailed documentation of collection, handling, and transfer.
- ★ Secure storage and access control.
- ★ Verification through hashing at every stage.
- ★ Presentation of chain of custody documentation in court.

## Consequences of Breaking Chain of Custody:

- ⊗ ★ Evidence may be deemed inadmissible.
- ⚠ ★ Investigation credibility is compromised.

Ashutosh Kumar, CSE(AI&ML-A), Roll-2200321530046
Subject-Cyber Security, Assignment-03 (BCC401),
Date 06/08/2025, Total No. of Pages 10