

# Cyber Security and Digital Forensics (4361601) - Summer 2025 Solution

Milav Dabgar

May 8, 2025

## Question 1(a) [3 marks]

Give comparison between Public key and Private Key cryptography.

### Solution

Table 1. Key Cryptography Comparison

Aspect	Private Key Cryptography	Public Key Cryptography
Key Management	Same key for encryption/decryption	Different keys for encryption/decryption
Key Distribution	Secure channel required	No secure channel needed
Speed	Fast processing	Slower than private key
Security Level	High if key is secret	High mathematical security
Example	DES, AES	RSA, ECC

### Mnemonic

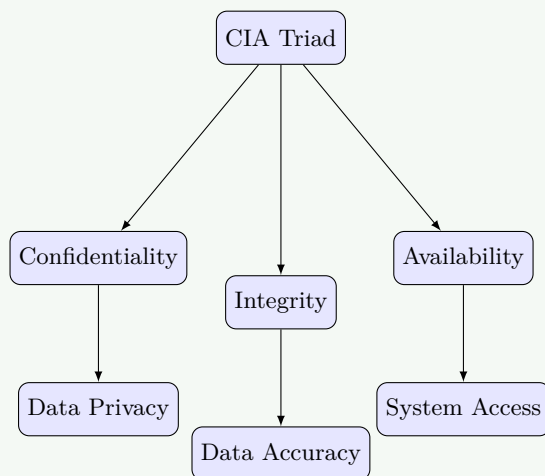
"Private Personal, Public Pair"

## Question 1(b) [4 marks]

Explain CIA Triad in detail.

### Solution

CIA Triad is the foundation of information security with three core principles:



- **Confidentiality:** Ensures data is accessible only to authorized users
- **Integrity:** Maintains accuracy and completeness of data
- **Availability:** Ensures systems are accessible when needed

#### Mnemonic

"Can I Access" (Confidentiality, Integrity, Availability)

## Question 1(c) [7 marks]

Explain Md5 algorithm steps.

### Solution

MD5 (Message Digest 5) is a cryptographic hash function producing 128-bit hash value.

**Table 2.** MD5 Algorithm Steps

Step	Process	Description
1	<b>Padding</b>	Add bits to make message length $\equiv 448 \pmod{512}$
2	<b>Length Addition</b>	Append 64-bit length of original message
3	<b>Initialize Buffers</b>	Set four 32-bit buffers (A, B, C, D)
4	<b>Process Blocks</b>	Process message in 512-bit blocks
5	<b>Round Functions</b>	Apply 4 rounds of 16 operations each

```

1 # MD5 Processing Steps
2 def md5_process():
3     # Step 1: Padding
4     padded_message = original + padding_bits
5     # Step 2: Process in 512-bit chunks
6     for chunk in chunks:
7         # Step 3: Apply round functions
8         result = round_functions(chunk)
9     return final_hash

```

- **Round 1:**  $F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$
- **Round 2:**  $G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$
- **Round 3:**  $H(X,Y,Z) = X \oplus Y \oplus Z$
- **Round 4:**  $I(X,Y,Z) = Y \oplus (X \vee \neg Z)$

#### Mnemonic

"My Data Needs Proper Processing" (Message, Digest, Needs, Proper, Processing)

OR

## Question 1(c) [7 marks]

List inventors of RSA. Write steps of RSA algorithm.

## Solution

## RSA Inventors:

- Ron Rivest (MIT)
- Adi Shamir (MIT)
- Leonard Adleman (MIT)

Table 3. RSA Algorithm Steps

Step	Process	Formula
1	Select Primes	Choose p, q (large primes)
2	Calculate n	$n = p \times q$
3	Calculate $\phi(n)$	$\phi(n) = (p-1) \times (q-1)$
4	Choose e	$\gcd(e, \phi(n)) = 1$
5	Calculate d	$d \times e \equiv 1 \pmod{\phi(n)}$
6	Encryption	$C = M^e \pmod{n}$
7	Decryption	$M = C^d \pmod{n}$

## Key Pairs:

- Public Key: (n, e)
- Private Key: (n, d)

## Mnemonic

"RSA: Rivest Shamir Adleman"

## Question 2(a) [3 marks]

Define: Firewall. List limitations of firewall.

## Solution

**Definition:** Firewall is a network security device that monitors and controls incoming/outgoing network traffic based on predetermined security rules.

Table 4. Limitations of Firewall

Limitation	Description
Internal Threats	Cannot protect against insider attacks
Application Layer	Limited protection against application-specific attacks
Performance	Can slow down network traffic
Configuration	Requires proper setup and maintenance
Encrypted Traffic	Cannot inspect encrypted content effectively

## Mnemonic

"Fire Walls Limit Internal Protection"

## Question 2(b) [4 marks]

Sketch IPsec Tunnel Mode and Transport mode.

**Solution****IPsec Modes Comparison:****Transport Mode:**

Original IP Header	IPsec Header	Original Payload
--------------------	--------------	------------------

**Tunnel Mode:**

New IP Header	IPsec Header	Original IP Header	Original Payload
---------------	--------------	--------------------	------------------

**Table 5.** Key Differences

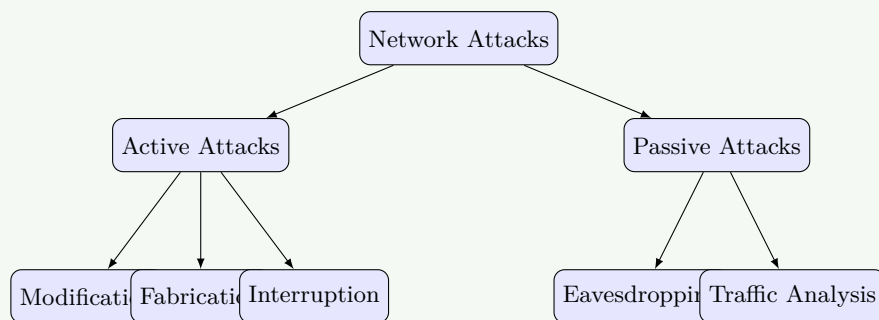
Aspect	Transport Mode	Tunnel Mode
<b>Protection</b>	Payload only	Entire packet
<b>Use Case</b>	End-to-end	Gateway-to-gateway
<b>Overhead</b>	Lower	Higher
<b>IP Header</b>	Original preserved	New header added

**Mnemonic**

"Transport Travels, Tunnel Total"

**Question 2(c) [7 marks]**

Explain various types of Active & Passive attacks in detail.

**Solution****Attack Classification:****Table 6.** Active Attacks

Type	Description	Example
<b>Masquerade</b>	Impersonating another entity	Fake identity
<b>Replay</b>	Retransmitting captured data	Session replay
<b>Modification</b>	Altering message content	Data tampering
<b>DoS</b>	Denying service availability	Server flooding

**Table 7.** Passive Attacks

Type	Description	Impact
<b>Eavesdropping</b>	Listening to communications	Data theft
<b>Traffic Analysis</b>	Analyzing communication patterns	Privacy breach
<b>Monitoring</b>	Observing network activity	Information gathering

- **Active attacks** modify system resources or data
- **Passive attacks** observe and collect information
- **Detection:** Active attacks easier to detect than passive

#### Mnemonic

"Active Acts, Passive Peeks"

OR

### Question 2(a) [3 marks]

**Define: Digital Signature. Also discuss various application areas of Digital Signature.**

#### Solution

**Definition:** Digital Signature is a cryptographic technique that validates authenticity and integrity of digital messages or documents using public key cryptography.

**Table 8.** Application Areas

Area	Use Case
<b>E-commerce</b>	Online transactions, contracts
<b>Banking</b>	Electronic fund transfers, cheques
<b>Government</b>	Digital certificates, official documents
<b>Healthcare</b>	Patient records, prescriptions
<b>Legal</b>	Electronic contracts, court documents

#### Mnemonic

"Digital Documents Demand Authentic Approval"

OR

### Question 2(b) [4 marks]

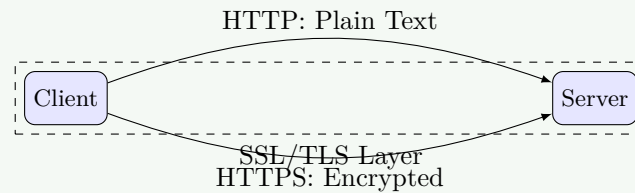
**Differentiate HTTP & HTTPS.**

#### Solution

**Table 9.** HTTP vs HTTPS

Parameter	HTTP	HTTPS
Security	No encryption	SSL/TLS encryption
Port	80	443
Protocol	Hypertext Transfer Protocol	HTTP + SSL/TLS
Data Protection	Plain text	Encrypted
Authentication	No server verification	Server certificate validation
Speed	Faster	Slightly slower
URL Prefix	http://	https://

**Diagram:**



#### Mnemonic

"HTTPS Has Security"

OR

## Question 2(c) [7 marks]

**Define: Malicious software. Explain Virus, Worm, Keylogger, Trojans in detail.**

#### Solution

**Definition:** Malicious software (Malware) is any software designed to harm, exploit, or gain unauthorized access to computer systems.

**Table 10.** Types of Malware

Type	Characteristics	Behavior
<b>Virus</b>	Requires host file	Attaches to programs, spreads when executed
<b>Worm</b>	Self-replicating	Spreads independently through networks
<b>Keylogger</b>	Records keystrokes	Steals passwords and sensitive data
<b>Trojan</b>	Disguised as legitimate	Provides backdoor access to attackers

#### Detailed Explanation:

##### Virus:

- Requires host program to execute
- Spreads through infected files
- Can corrupt or delete data

##### Worm:

- Self-propagating malware
- Exploits network vulnerabilities
- Consumes network bandwidth

##### Keylogger:

- Records user keystrokes
- Captures login credentials
- Can be hardware or software-based

**Trojan:**

- Appears as legitimate software
- Creates backdoor for remote access
- Does not self-replicate

**Mnemonic**

"Viruses Visit, Worms Wander, Keys Captured, Trojans Trick"

**Question 3(a) [3 marks]**

**Define: Cybercrime. Also discuss needs of Cyber Law.**

**Solution**

**Definition:** Cybercrime refers to criminal activities carried out using computers, networks, or digital devices as tools or targets.

**Table 11.** Needs of Cyber Law

Need	Justification
<b>Legal Framework</b>	Establish clear definitions of cyber offenses
<b>Jurisdiction</b>	Define authority across geographical boundaries
<b>Evidence</b>	Guidelines for digital evidence collection
<b>Punishment</b>	Deterrent measures for cybercriminals
<b>Protection</b>	Safeguard individual and organizational rights

**Mnemonic**

"Cyber Laws Create Legal Protection"

**Question 3(b) [4 marks]**

**Explain Cyber spying and Cyber theft.**

**Solution****Cyber Spying:**

- **Definition:** Unauthorized surveillance of digital communications and activities
- **Methods:** Malware, phishing, social engineering
- **Targets:** Government, corporate secrets, personal data
- **Impact:** National security threats, competitive disadvantage

**Cyber Theft:**

- **Definition:** Unauthorized taking of digital assets or information
- **Types:** Identity theft, financial fraud, intellectual property theft
- **Methods:** Hacking, social engineering, insider threats
- **Consequences:** Financial loss, reputation damage

**Table 12.** Comparison Table

Aspect	Cyber Spying	Cyber Theft
<b>Purpose</b>	Information gathering	Asset acquisition
<b>Detection</b>	Often undetected	May be noticed
<b>Duration</b>	Long-term monitoring	One-time or periodic
<b>Motivation</b>	Intelligence/espionage	Financial gain

**Mnemonic**

"Spies Spy, Thieves Take"

**Question 3(c) [7 marks]**

Explain article section 66 of cyber law.

**Solution****Section 66 - Computer Related Offences (IT Act 2008):****Table 13.** Key Provisions

Sub-section	Offense	Punishment
<b>66(1)</b>	Dishonestly/fraudulently computer resource damage	Up to 3 years imprisonment + fine up to 5 lakh
<b>66A</b>	Sending offensive messages	Up to 3 years + fine
<b>66B</b>	Receiving stolen computer resource	Up to 3 years + fine up to 1 lakh
<b>66C</b>	Identity theft	Up to 3 years + fine up to 1 lakh
<b>66D</b>	Cheating by personation using computer	Up to 3 years + fine up to 1 lakh
<b>66E</b>	Violation of privacy	Up to 3 years + fine up to 2 lakh
<b>66F</b>	Cyber terrorism	Life imprisonment

**Detailed Coverage:****Section 66 Main Offenses:**

- **Hacking:** Unauthorized access to computer systems
- **Data Theft:** Stealing or copying data without permission
- **System Damage:** Destroying or altering computer data
- **Virus Introduction:** Introducing malicious code

**Elements Required:**

- **Intent:** Dishonest or fraudulent intention
- **Access:** Without permission of owner
- **Damage:** Causing harm to system or data
- **Knowledge:** Awareness of unauthorized access

**Legal Framework:**

- **Cognizable:** Police can arrest without warrant
- **Non-bailable:** Bail at court's discretion
- **Evidence:** Digital evidence admissible in court

**Mnemonic**

"Section 66 Stops Cyber Sins"

OR



### Question 3(a) [3 marks]

Explain Cyber terrorism.

#### Solution

**Definition:** Cyber terrorism involves the use of digital technologies to create fear, disruption, or harm for political, religious, or ideological purposes.

**Table 14.** Characteristics

Aspect	Description
<b>Target</b>	Critical infrastructure, government systems
<b>Method</b>	DDoS attacks, system infiltration, data destruction
<b>Motivation</b>	Political, religious, ideological goals
<b>Impact</b>	Public fear, economic disruption, national security

#### Examples:

- Power grid attacks
- Transportation system disruption
- Financial system targeting

#### Mnemonic

"Terror Through Technology"

OR

### Question 3(b) [4 marks]

Explain Cyber bullying & Cyber stalking.

#### Solution

##### Cyber Bullying:

- **Definition:** Using digital platforms to harass, intimidate, or harm others
- **Platforms:** Social media, messaging apps, online forums
- **Characteristics:** Repetitive, intentional harm, power imbalance
- **Impact:** Psychological trauma, depression, social isolation

##### Cyber Stalking:

- **Definition:** Persistent online harassment causing fear or emotional distress
- **Methods:** Unwanted messages, tracking, identity theft
- **Duration:** Long-term, continuous behavior
- **Legal:** Criminal offense in many jurisdictions

**Table 15.** Comparison

Aspect	Cyber Bullying	Cyber Stalking
<b>Duration</b>	Episodes	Persistent
<b>Age Group</b>	Mainly minors	All ages
<b>Motivation</b>	Social dominance	Obsession/control
<b>Platform</b>	Public/semi-public	Private/public

**Mnemonic**

"Bullies Bother, Stalkers Stalk"

OR

### Question 3(c) [7 marks]

Explain article section 67 of cyber law.

**Solution**

**Section 67 - Publishing Obscene Information (IT Act 2008):**

**Table 16.** Main Provisions

Section	Content	Punishment
<b>67</b>	Publishing obscene material	First conviction: 3 years + 5 lakh fine
<b>67A</b>	Sexually explicit material	Up to 5 years + 10 lakh fine
<b>67B</b>	Child pornography	First: 5 years + 10 lakh, Subsequent: 7 years + 10 lakh
<b>67C</b>	Intermediate liability	Failure to remove illegal content

**Key Elements:****Section 67 - Obscenity:**

- **Publishing:** Making available in electronic form
- **Content:** Lascivious, sexually explicit material
- **Medium:** Website, email, social media
- **Intent:** Corrupt or deprave viewers

**Section 67A - Sexually Explicit:**

- **Enhanced punishment** for explicit sexual content
- **Broader scope** than general obscenity
- **Commercial purpose** considered aggravating factor

**Section 67B - Child Protection:**

- **Zero tolerance** for child exploitation
- **Strict liability** for possession and distribution
- **Higher penalties** reflecting seriousness
- **Age verification** requirements for platforms

**Defenses Available:**

- **Scientific/educational** purpose
- **Artistic merit** consideration
- **Private viewing** in some cases
- **Lack of knowledge** about content nature

**Digital Evidence Requirements:**

- **Chain of custody** maintenance
- **Technical authenticity** proof
- **Source identification** methods
- **Preservation** of electronic evidence

**Mnemonic**

"Section 67 Stops Shameful Sharing"

## Question 4(a) [3 marks]

Discuss types of Hackers.

### Solution

#### Hacker Classification:

Table 17. Hacker Types

Type	Motivation	Activities
White Hat	Ethical security testing	Authorized penetration testing
Black Hat	Malicious intent	Illegal system breaking
Gray Hat	Mixed motivations	Unauthorized but non-malicious
Script Kiddie	Recognition/fun	Using existing tools
Hacktivist	Political/social causes	Protest through hacking

#### Detailed Types:

- **White Hat:** Ethical hackers, security professionals
- **Black Hat:** Cybercriminals seeking profit or damage
- **Gray Hat:** Between ethical and malicious

#### Mnemonic

"Hats Have Hacker Hierarchy"

## Question 4(b) [4 marks]

Explain RAT.

### Solution

#### RAT (Remote Administration Tool):

**Definition:** Software that allows remote control of a computer system, often used maliciously for unauthorized access.

Table 18. Characteristics

Feature	Description
Remote Control	Complete system access from distance
Stealth Mode	Hidden from user detection
Data Theft	File access and transfer capabilities
Keylogging	Keystroke recording
Screen Capture	Desktop monitoring

#### Common RATs:

- BackOrifice
- NetBus
- DarkComet
- Poison Ivy

#### Detection Methods:

- Antivirus software
- Network monitoring
- Process analysis
- Behavioral detection

**Mnemonic**

"RATs Run Remote Access Tactics"

**Question 4(c) [7 marks]**

**Explain Five Steps of Hacking.**

**Solution****The Five-Phase Hacking Methodology:**

1. Reconnaissance → 2. Scanning → 3. Gaining Access → 4. Maintaining Access → 5. Covering Tracks

**Table 19.** Detailed Steps

Phase	Purpose	Techniques	Tools
<b>1. Reconnaissance</b>	Information Gathering	OSINT, Social Engineering	Google, Shodan, WHOIS
<b>2. Scanning</b>	Identify Vulnerabilities	Port scanning, Network mapping	Nmap, Nessus
<b>3. Gaining Access</b>	Exploit Vulnerabilities	Password attacks, Code injection	Metasploit, Hydra
<b>4. Maintaining Access</b>	Persistent Control	Backdoors, Rootkits	RATs, Trojans
<b>5. Covering Tracks</b>	Hide Evidence	Log deletion, Steganography	CCleaner, File wipers

**Phase 1 - Reconnaissance:**

- **Passive:** Public information gathering
- **Active:** Direct target interaction
- **Goal:** Map target infrastructure

**Phase 2 - Scanning:**

- **Network scanning:** Live system identification
- **Port scanning:** Service discovery
- **Vulnerability scanning:** Weakness identification

**Phase 3 - Gaining Access:**

- **Exploitation:** Vulnerability utilization
- **Authentication attacks:** Password cracking
- **Privilege escalation:** Higher access levels

**Phase 4 - Maintaining Access:**

- **Backdoor installation:** Future access
- **System modification:** Persistence mechanisms
- **Data collection:** Information harvesting

**Phase 5 - Covering Tracks:**

- **Log manipulation:** Evidence removal
- **File deletion:** Trace elimination
- **Timeline modification:** Activity concealment

**Mnemonic**

"Real Smart Guys Make Choices" (Reconnaissance, Scanning, Gaining, Maintaining, Covering)

**OR**

## Question 4(a) [3 marks]

Explain Brute force attack.

### Solution

**Definition:** Brute force attack is a trial-and-error method used to decode encrypted data by systematically trying all possible combinations.

**Table 20.** Characteristics

Aspect	Description
Method	Exhaustive key search
Time	Computationally intensive
Success	Guaranteed but time-consuming
Target	Passwords, encryption keys
Tools	Automated software

**Types:**

- **Simple Brute Force:** All possible combinations
- **Dictionary Attack:** Common passwords
- **Hybrid Attack:** Dictionary + variations

### Mnemonic

"Brute Force Breaks By Trying"

OR

## Question 4(b) [4 marks]

Define: Vulnerability, Threat, Exploit

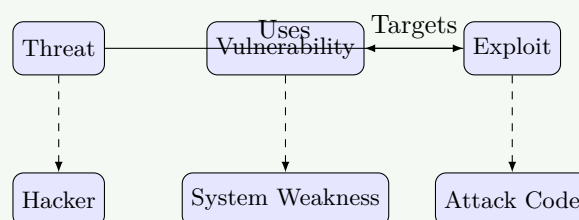
### Solution

**Security Terminology:**

**Table 21.** Term Definitions

Term	Definition	Example
<b>Vulnerability</b>	Weakness in system/software	Unpatched software bug
<b>Threat</b>	Potential danger to asset	Malicious hacker
<b>Exploit</b>	Code taking advantage of vulnerability	Buffer overflow attack

**Relationship:**



**Examples:**

- **Vulnerability:** SQL injection flaw

- **Threat:** Cybercriminal
- **Exploit:** SQL injection payload

**Risk Formula:** Risk = Threat × Vulnerability × Asset Value

#### Mnemonic

"Threats Target Vulnerable Exploits"

OR

## Question 4(c) [7 marks]

Explain any three basic commands of kali Linux with suitable example.

### Solution

#### Essential Kali Linux Commands:

##### 1. NMAP (Network Mapper):

```
1 # Port scanning
2 nmap -sS target_ip
3 nmap -A -T4 192.168.1.1
```

Table 22. Nmap Options

Option	Purpose	Example
-sS	SYN scan	nmap -sS 192.168.1.1
-A	Aggressive scan	nmap -A target.com
-p	Specific ports	nmap -p 80,443 target.com

##### 2. Metasploit:

```
1 # Start Metasploit
2 msfconsole
3 # Search exploits
4 search apache
5 # Use exploit
6 use exploit/windows/smb/ms17_010_eternalblue
```

#### Commands:

- **search:** Find exploits/payloads
- **use:** Select module
- **set:** Configure options
- **exploit:** Launch attack

##### 3. Wireshark:

```
1 # Command line version
2 tshark -i eth0
3 # Filter traffic
4 tshark -i eth0 -f "port 80"
```

#### Features:

- **Packet capture:** Real-time network monitoring
- **Protocol analysis:** Deep packet inspection
- **Filter options:** Targeted traffic analysis
- **GUI interface:** User-friendly analysis

**Additional Commands:****4. Hydra (Password Cracking):**

```
1 hydra -l admin -P passwords.txt ssh://192.168.1.1
```

**5. John the Ripper:**

```
1 john --wordlist=rockyou.txt hashes.txt
```

**6. Aircrack-ng (WiFi Security):**

```
1 airmon-ng start wlan0
2 airodump-ng wlan0mon
```

**Table 23.** Command Categories

Category	Tools	Purpose
Network Scanning	nmap, masscan	Host/port discovery
Vulnerability Assessment	OpenVAS, Nessus	Security scanning
Exploitation	Metasploit, SQLmap	Vulnerability exploitation
Password Attacks	Hydra, John	Credential cracking
Wireless Security	Aircrack-ng	WiFi penetration testing

**Mnemonic**

"Network Maps Make Security"

**Question 5(a) [3 marks]**

List the branches of Digital Forensics.

**Solution****Digital Forensics Branches:****Table 24.** Branches

Branch	Focus Area	Applications
Computer Forensics	Desktop/laptop systems	Hard drive analysis
Network Forensics	Network traffic analysis	Intrusion investigation
Mobile Forensics	Smartphones/tablets	Call logs, messages
Database Forensics	Database systems	Data integrity verification
Malware Forensics	Malicious software	Malware analysis
Email Forensics	Email communications	Email header analysis
Memory Forensics	RAM analysis	Live system investigation

**Specialized Areas:**

- Cloud Forensics
- IoT Forensics
- Blockchain Forensics

**Mnemonic**

"Digital Detectives Discover Many Clues"

**Question 5(b) [4 marks]**

Discuss Locard's Principle of Exchange in Digital Forensics.

**Solution**

**Locard's Exchange Principle:**

**Original Principle:** "Every contact leaves a trace"

**Digital Application:**

**Table 25.** Digital Traces

Digital Activity	Trace Left	Location
File Access	Access timestamps	File metadata
Web Browsing	Browser history, cookies	Browser cache
Email Communication	Headers, logs	Mail servers
Network Activity	Connection logs	Network devices
USB Usage	Device artifacts	Registry/logs

**Digital Evidence Traces:**

**System Level:**

- **Registry entries:** System changes
- **Log files:** Activity records
- **Temporary files:** Process artifacts
- **Metadata:** File information

**Network Level:**

- **Router logs:** Traffic records
- **Firewall logs:** Connection attempts
- **DNS queries:** Website visits
- **Packet captures:** Communication content

**Application Level:**

- **Browser artifacts:** Web activity
- **Application logs:** Software usage
- **Database changes:** Data modifications
- **Cache files:** Temporary storage

**Forensic Implications:**

- **No perfect crime:** Digital traces always exist
- **Evidence location:** Multiple sources available
- **Corroboration:** Multiple trace validation
- **Timeline reconstruction:** Activity sequencing

**Mnemonic**

"Every Exchange Exists Electronically"

**Question 5(c) [7 marks]**

List the critical steps in preserving Digital Evidence.



## Solution

### Digital Evidence Preservation Process:



**Table 26.** Critical Preservation Steps

Step	Process	Purpose	Tools
1. Identification	Locate potential evidence	Determine scope	Visual inspection
2. Documentation	Record scene details	Maintain chain of custody	Photography, notes
3. Isolation	Prevent contamination	Preserve integrity	Network disconnection
4. Imaging	Create bit-by-bit copy	Preserve original	dd, FTK Imager
5. Hashing	Generate integrity checks	Verify authenticity	MD5, SHA-256
6. Storage	Secure evidence storage	Prevent tampering	Write-protected media
7. Chain of Custody	Document handling	Legal admissibility	Forensic forms

### Detailed Preservation Methods:

#### Physical Preservation:

- **Power management:** Proper shutdown procedures
- **Hardware protection:** Anti-static measures
- **Environmental control:** Temperature/humidity
- **Access restriction:** Authorized personnel only

#### Logical Preservation:

- **Bit-stream imaging:** Exact disk copies
- **Hash verification:** Integrity confirmation
- **Write blocking:** Prevent modifications
- **Metadata preservation:** Timestamp protection

#### Legal Preservation:

- **Documentation standards:** Detailed records
- **Chain of custody:** Handling log
- **Authentication:** Evidence verification
- **Admissibility:** Court requirements

#### Best Practices:

##### Do's:

- Create multiple copies of evidence
- Use forensically sound tools
- Document every action
- Maintain chain of custody
- Verify integrity with hashes

##### Don'ts:

- Never work on original evidence
- Avoid contamination of scene
- Don't power on suspect systems
- Never modify evidence
- Don't break chain of custody

#### Quality Assurance:

**Table 27.** Checks

Check	Verification Method	Frequency
Hash Validation	Compare original vs copy	Before/after operations
Tool Calibration	Verify tool accuracy	Regular intervals
Process Review	Audit procedures	Case completion
Documentation Check	Verify completeness	Each step

### Legal Considerations:

- **Admissibility requirements:** Court standards
- **Expert testimony:** Technical explanation
- **Cross-examination:** Process validation
- **Standard compliance:** Industry best practices

#### Mnemonic

"Proper Preservation Prevents Problems" (Plan, Preserve, Protect, Prove)

OR

## Question 5(a) [3 marks]

Explain Malware forensics.

### Solution

**Definition:** Malware forensics involves the analysis of malicious software to understand its behavior, origin, and impact on infected systems.

**Table 28.** Key Components

Component	Description
<b>Static Analysis</b>	Examining malware without execution
<b>Dynamic Analysis</b>	Running malware in controlled environment
<b>Code Analysis</b>	Reverse engineering malware code
<b>Behavioral Analysis</b>	Studying malware actions

#### Process:

- **Sample collection:** Malware acquisition
- **Isolation:** Sandbox environment
- **Analysis:** Behavior observation
- **Reporting:** Findings documentation

#### Mnemonic

"Malware Makes Mysteries"

OR

## Question 5(b) [4 marks]

Explain why CCTV plays an important role as evidence in digital forensics investigations.

### Solution

**CCTV in Digital Forensics:**

**Table 29.** Importance of CCTV

Role	Description	Benefit
<b>Visual Documentation</b>	Records actual events	Objective evidence
<b>Timeline Establishment</b>	Timestamps activities	Chronological sequence
<b>Identity Verification</b>	Captures suspect images	Person identification
<b>Corroboration</b>	Supports other evidence	Strengthens case

#### Digital Evidence Properties:

##### Technical Aspects:

- **Metadata preservation:** Timestamp, camera ID, settings
- **Chain of custody:** Secure handling procedures
- **Format integrity:** Original file structure maintenance
- **Authentication:** Digital signatures, hash values

##### Forensic Value:

- **Real-time documentation:** Live incident recording
- **Unbiased testimony:** Mechanical witness
- **High resolution:** Clear image quality
- **Audio capture:** Additional sensory evidence

##### Analysis Methods:

- **Frame-by-frame examination:** Detailed scrutiny
- **Enhancement techniques:** Image improvement
- **Comparison analysis:** Multiple angle correlation
- **Motion tracking:** Subject movement patterns

##### Legal Admissibility:

- **Authenticity verification:** Chain of custody
- **Technical validation:** Equipment calibration
- **Expert testimony:** Forensic analysis explanation
- **Standard compliance:** Industry best practices

#### Mnemonic

"CCTV Captures Criminal Conduct Clearly"

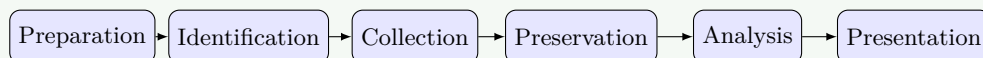
OR

### Question 5(c) [7 marks]

Explain phases of Digital forensic investigation.

#### Solution

##### Digital Forensic Investigation Process:



**Table 30.** Phase Breakdown

Phase	Objective	Activities	Output
<b>1. Preparation</b>	Readiness establishment	Tool setup, training	Forensic kit
<b>2. Identification</b>	Evidence location	Survey, documentation	Evidence list
<b>3. Collection</b>	Evidence acquisition	Imaging, copying	Digital copies
<b>4. Preservation</b>	Integrity maintenance	Hashing, storage	Verified evidence
<b>5. Analysis</b>	Data examination	Investigation, correlation	Findings
<b>6. Presentation</b>	Results communication	Reporting, testimony	Final report

**Detailed Phase Analysis:****Phase 1 - Preparation:**

- **Tool readiness:** Forensic software installation
- **Hardware setup:** Write blockers, imaging devices
- **Documentation templates:** Chain of custody forms
- **Team preparation:** Role assignments, training
- **Legal preparation:** Warrant requirements, permissions

**Phase 2 - Identification:**

- **Scene survey:** Evidence location mapping
- **Device inventory:** System identification
- **Volatile evidence:** Memory, network connections
- **Priority assessment:** Critical evidence first
- **Photography:** Scene documentation

**Phase 3 - Collection:**

- **Live system analysis:** Memory acquisition
- **Disk imaging:** Bit-for-bit copies
- **Network evidence:** Log files, packet captures
- **Mobile devices:** Physical/logical extraction
- **Cloud evidence:** Remote data acquisition

**Phase 4 - Preservation:**

- **Hash generation:** MD5, SHA-256 checksums
- **Write protection:** Hardware/software blocking
- **Storage security:** Tamper-evident containers
- **Chain of custody:** Handling documentation
- **Backup creation:** Multiple evidence copies

**Phase 5 - Analysis:**

- **File system examination:** Directory structure analysis
- **Deleted data recovery:** Unallocated space searching
- **Timeline creation:** Event chronology
- **Keyword searching:** Relevant content identification
- **Pattern recognition:** Behavioral analysis

**Phase 6 - Presentation:**

- **Report writing:** Findings documentation
- **Visual aids:** Charts, diagrams, screenshots
- **Expert testimony:** Court presentation
- **Peer review:** Quality assurance
- **Archive maintenance:** Case file storage

**Best Practices:****Technical Standards:**

- **Tool validation:** Regular calibration
- **Methodology consistency:** Standard procedures
- **Quality control:** Verification checks
- **Documentation completeness:** Detailed records

**Legal Requirements:**

- **Admissibility standards:** Court requirements
- **Chain of custody:** Unbroken documentation
- **Expert qualifications:** Professional certification
- **Cross-examination preparation:** Defense against challenges

**Quality Assurance:****Table 31.** Check Points

Check Point	Verification	Documentation
Evidence integrity	Hash comparison	Verification logs
Tool reliability	Calibration tests	Certification records
Process compliance	Standard adherence	Procedure checklists
Report accuracy	Peer review	Review signatures

**Common Challenges:**

- **Encryption:** Data protection barriers
- **Anti-forensics:** Evidence hiding techniques
- **Volume:** Large data sets
- **Volatility:** Temporary evidence
- **Legal complexity:** Jurisdiction issues

**Success Factors:**

- **Systematic approach:** Methodical investigation
- **Technical expertise:** Skilled personnel
- **Proper tools:** Adequate resources
- **Legal knowledge:** Compliance understanding
- **Documentation discipline:** Thorough records

**Mnemonic**

"Proper Planning Prevents Poor Performance" (Preparation, Preservation, Processing, Presentation, Proof)