

Cyber Forensics Q&A



21IT021.docx.pdf
PDF

give question and answer....

Sure! I will give **clear, direct QUESTION & ANSWER format** for the entire file **21IT021 – CYBER FORENSICS**.

I'll cover **all parts (A1, B1, C2, D2, E2, A3, B3, C3, D3, E3)** with **simple explanations** suitable for **exam or viva.**

A1 – Cyber Attacks

(i) Identify the attack

Q: A customer gets an email saying “offer ends in 5 minutes, click link and enter details.” After entering details, offer disappears.

A: Phishing attack

Justification:

Phishing tricks the user into clicking a fake link and entering personal information using urgency or fear.

(ii) Match protection methods to cyber-attacks

- **Firewall** → blocks DoS, malware, unauthorized access
- **Cryptography** → prevents data theft, Man-in-the-Middle, identity theft
- **Spam Filter** → blocks phishing emails, malicious spam

(iii) Identify scenario and attack

Scenario	Attack
1	Phishing (email from fake domain)
2	DoS attack (sending huge packets)
3	Insider attack (employee misuses credentials)
4	Botnet / Worm (system performs malicious activities automatically)

B1 – Network Configuration & DoS

(i) From which components logs are generated?

Logs come from:

- Cloud service provider
 - Edge node
 - Distributed storage system
 - User systems
 - Router / firewall
-

(ii) Modify ping command for DoS

Original:

```
ping www.amazon.com -n 60000 -l 300
```

Required: Attack Amazon → Flipkart

Packet size = 500 bytes

Count = 16000

Answer:

```
ping www.flipkart.com -n 16000 -l 500
```

(iii) Fill components in Knowledge-Driven Digital Investigation Architecture

Correct order:

1. Digital Evidence
 2. Parsing
 3. Annotation
 4. RDF Data
 5. Ontologies
 6. Reasoning
 7. Querying
-

C2 – Encryption & Hashing

(i) Caesar Cipher with key 4

Plain: B A N N A R I

Shift +4:

- B → F
- A → E
- N → R
- N → R

- A → E
- R → V
- I → M

Cipher text = FERR EVM

(ii) Watermarking and Hashing

- a) **Payload received** → 1101100011
(unless modified)
 - b) **Hash code when NOT modified**
→ **UFE583D** (same as sender)
 - c) **Hash code when modified**
→ **Different value** (hash always changes)
-

(iii) Symmetric vs Asymmetric

Symmetric Key Cryptography

- Uses **one secret key** for encryption & decryption
- Example: AES, DES
- Fast

Asymmetric Key Cryptography

- Uses **Public Key + Private Key**
 - Public key encrypts; private key decrypts
 - Example: RSA
-

✓ D2 – Firewall

(i) Draw network

5 computers → connected to **Switch** → **Router**

(ii) Placement of firewall

Firewall should be placed:

Between Router and Internet

Reason:

It filters all incoming/outgoing traffic before reaching internal network.

(iii) Match Firewall Types

Purpose	Advantage	Firewall Type
Monitors incoming/outgoing packets	Single device for entire network	Packet Filtering Firewall
Determines connection state	Blocks protocol vulnerability attacks	Stateful Inspection Firewall
Inspect OSI layers including Application	Blocks app-layer attacks	Application Layer Firewall
Gateway between two networks for applications	Provides privacy	Proxy Firewall
Works at Session layer allowing two TCP connections	Masks original client	Circuit-Level Firewall

✓ E2 – Malware

(i) Identify malware type

- a) Spreads through pen-drive/CD → **Virus**
- b) Spreads through network automatically → **Worm**
- c) Looks legitimate but malicious → **Trojan**

(ii) Correct statements

- ✓ Statement 1 – True (Spyware observes user)
- ✓ Statement 2 – False (Adware, not Trojan)
- ✓ Statement 3 – True (Ransomware encrypts files)
- ✓ Statement 4 – True (Adware enters via ads)
- ✓ Statement 5 – False (Virus does not silently observe; spyware does)

(iii) Preventive measures and attacks prevented

- **Firewall** → prevents DoS, malware traffic
- **Antivirus** → prevents malware, ransomware
- **Spam filter** → prevents phishing
- **Strong passwords** → prevents identity theft and ransomware

✓ A3 – Identity Theft

(i) Missing Incident Response Steps

- A – **Preparation**
- B – **Detection & Analysis**
- C – **Containment, Eradication, and Recovery**

(ii) Correct order of Investigation phases

1. Identification
2. Collection
3. Preservation
4. Examination
5. Analysis
6. Presentation

(iii) Match case with identity theft method

Case	Method
1	Phishing
2	SQL Injection
3	Malware / Virus infection
4	Unsecured HTTP (MITM possible)

B3 – Windows Files

(i) File functions

File	Function
Software	Installed software info
Default	Default system profile
System	System configuration, drivers
SAM	Username & password hashes
Security	Local security policies

(ii) Map forensic tools

- **Windows** → FTK Imager
- **Linux** → Autopsy, Sleuth Kit
- **Mac** → MacQuisition

(iii) Assertion & Reasoning

 Both assertion & reasoning are **TRUE**

Correct Answer: **A**

C3 – Email Forensics

(i) Protocol for email

- **TCP** is suitable (reliable, no data loss)
 - Secure email uses:
 - **SSL/TLS, HTTPS, SMTPS, PGP, S/MIME**
-

(ii) Parameters showing malicious email

- Unknown sender
 - Suspicious domain
 - Grammar errors
 - Threat/urgency
 - Phishing links
 - Unexpected attachment
-

(iii) Email investigation flow

1. Collect sender information → **Preservation**
2. Collect header → **Preservation**
3. Detect spoofing
4. Use analysis tools

Preservation steps: Step 1 & Step 2

✓ D3 – Firewall Policies

(i) Correct statements

- ✓ 1 – True
 ✗ 2 – False
 ✓ 3 – True
 ✗ 4 – False
 ✓ 5 – True
-

(ii) Create firewall rules

Rule	Description
1	Block all incoming from 192.168.3.9
2	Block incoming to port 80
3	Block incoming to host 192.168.8.3

(iii) Check allowed/blocked

- a) 192.168.5.6 → 192.168.3.9 → **Blocked** (Rule 3)
 - b) 192.168.3.7 → 192.168.3.4 → **Blocked** (Rule 3)
 - c) 192.168.8.3 → 192.168.8.9 → **Allowed**
 - d) FTP request → port 21 → **Blocked**
-

E3 – Security Terms

(i) MITM – Identify Risk, Threat, Vulnerability

- **Vulnerability (A):** Unsecured communication / weak Wi-Fi
 - **Threat (B):** Attacker intercepting messages
 - **Risk (C):** Data theft, password leakage
-

(ii) Stateless firewall analysis

- Stateless firewall does **not track connection states**
 - Can't prevent DoS attack
 - Only checks packet headers
 - Less secure than stateful firewall
-

(iii) DoS Attack: Risk and Threat

- **Threat:** Attacker sending huge ping packets
 - **Risk:** Server crash, service unavailability
-

Done!

If you want, I can also generate:

- A PDF with full questions & answers
- Separate 2-mark / 10-mark answers
- A revision cheat sheet

Just tell me!