

## ASSIGNMENT-2

Q1

Examples:

- Phishing → Malware Distribution
- Email Fraud → Identity theft.
- Harassment

Phishing: Fake emails that look genuine trick users into giving credentials or banking details.

Forensic investigations involve examining headers, IP Addresses & logs to trace attackers.

Q2

Ex: Encase Forensic:

- Industry: standard tool used for disk imaging recovery & analysis.
- Recovers deleted / hidden files, analyses file systems & generates court admissible reports.
- Helps ensure evidence integrity through verified process

Q3

a) Computer Forensics Hardware Tools:

Write blockers, disk duplicators, portable forensic kits

b) Validating & Testing Software:

ensured forensic tools are accurate; cross checked with test data & hashing.

c) Email Investigation: Examine headers, routing, attachments & metadata to detect spoofing, phishing or fraud.

Q4

→ Client (MUA - Mail User Agent) End user apps (Outlook, Thunderbird). Sends / Receives messages using SMTP, IMAP, POP3

→ Server (MTA - Mail Transfer Agent): Handles storing, forwarding & delivering messages (eg. Exchange, Postfix)

→ Forensics Role: understanding client-server interaction helps trace email origins, analyse delivery logs & recover deleted evidence.