

ASSIGNMENT-2Q1

Some common data hiding techniques are:

- Steganography
- Encryption
- Password Protection
- Alternate Data Streams.
- Code Obfuscation.

Steganography:

Information is hidden inside images, audio, video without visible change.

Example: Modifying the least significant bits of image pixels to embed text. Invisible to human eyes, widely used in secure communication but also misused for hiding malware.

Q2

- A research project that uses honeypots to attract attackers
- Helps track real time attack techniques, malware behaviour & intrusion attempts.

Contributions to forensics:

- collect evidence of attacker methods.
- Improved ~~Detection~~ Intrusion Detection Systems (IDS/TPS)

→ provides training data for investigators

Q3

→ Always use write blockers to avoid accidental changes to evidence.

→ Work on forensic images (bit by bit) copies instead of originals.

→ Maintain chain of custody - logs to prove authenticating in court.

→ use validated forensic tools.

→ Apply hashing before & after analysis to ensure no tampering

→ Isolate evidence systems from networks

Q4 Challenges

→ limited bandwidth & network delays.

→ Risk of tampering during data transfer

→ encrypted or password protected files

→ crossborder jurisdiction & legal issues

Best Practices

→ use secure encrypted channels for transfer

→ Perform hash verification before & after acquisition

→ Document every step with detailed logs

→ Prioritize imp. files if bandwidth is slow.