CCF 3456: Computer Crime and Digital Evidence - Exam Answers

# QUESTION ONE (30 MARKS)

a) Five Rules of Digital Evidence:

1. 1. Admissibility: Evidence must comply with legal standards to be accepted in court.
2. 2. Authenticity: Evidence must be proven to be what it purports to be.
3. 3. Integrity: Evidence must be protected against tampering or alteration.
4. 4. Chain of Custody: A documented history of evidence handling must be maintained.
5. 5. Relevance: Evidence must relate directly to the case.

b) Explanation of Terms:

* i. Affidavit: A written sworn statement used in court.
* ii. Plain View Doctrine: Allows officers to seize evidence without a warrant if it is clearly visible.
* iii. Search Warrant: A legal document authorizing a search.
* iv. Chain of Custody: Process of documenting the handling of evidence.
* v. Cyclic Redundancy Check: A method for detecting errors in digital data.

c) Data Hiding Techniques:

1. 1. Steganography
2. 2. Encryption
3. 3. File obfuscation or alternate data streams

d) Distinction Between Computer Crime and Digital Evidence:

Computer Crime refers to illegal acts involving computers (e.g., hacking). Digital Evidence refers to data collected and used to support legal proceedings.

e) Guidelines for Writing Investigation Reports:

1. 1. Use clear and concise language.
2. 2. Maintain objectivity.
3. 3. Document all findings.
4. 4. Include timestamps and data sources.
5. 5. Ensure the report is properly formatted and signed.

f) Initial Response Field Kit Tools:

1. 1. Digital camera
2. 2. Evidence bags and labels
3. 3. Write blockers
4. 4. Portable storage media
5. 5. Documentation forms

g) Intellectual Property and Protection Methods:

* Intellectual Property refers to creations of the mind like software and inventions. Protection methods include:

1. 1. Copyrights
2. 2. Patents
3. 3. Trademarks
4. 4. Non-disclosure agreements (NDAs)