CE1.3-R4: CYBER FORENSIC & LAW

NOTE:

1. **Answer question 1 and any FOUR from questions 2 to 7.**
2. **Parts of the same question should be answered together and in the same sequence.**

Time: 3 Hours **Total Marks: 100**

1.

a) List down the essential tasks that an examiner performs during the analysis of evidentiary digital evidence.
b) Describe the process involved in the digital forensic investigations.
c) Differentiate between Secret Key Cryptography and Public Key Cryptography.
d) What is anti-forensics? Is anti-forensics a set of tools or products a process or a methodology?
e) Explain use of Recycle bin and its use in restoring data?
f) List down the different ways of validating the identity of a suspicious host.
g) What is file allocation table? Compare different types of FAT in operating system.

(7x4)

2.

a) What is Cyber Stalking? What is its significance in cyber forensic? Explain different types of cyber stalking?
b) Define the Digital Forensic Laboratory Accreditation Standards with their grading criteria with their standard operating procedure checklist.

(9+9)

3.

a) Describe the process of material alteration of evidence called spoliation. Describe its three different components in detail.
b) Define the NTFS and elaborate the data hiding techniques on NTFS.
c) Specify the importance of "chain of custody of Digital Evidence" along with specifying steps for designating a form for recording it.

(6+6+6)

4.

a) Explain the legal regulations associated with the seizing and preserving of digital data storage device from a suspected computer system.
b) What does common law say about privacy in cyber forensic?

(10+8)

5. Write Short notes on following:

a) Coroner's Toolkit
b) i2 Analyst's Notebook
c) EnCase Forensic

(6+6+6)

6.

a) Describe Cloaking Techniques: Data Hide and Seek.
b) List and explain the different tools for deleted partition recovery.

(9+9)

7.

a) What are the recommendations for using data from Network Traffic?
b) Describe the Hijacked Session Attack to hide the original source of access.
c) Explain the role of model hardware: Hard drive and PDAs in cyber forensics.

(6+6+6)