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) What is the goal of forensic investigation? Write steps to do forensic investigation examination.
b) Why organizations need to employ Cyber Forensic Analysis?
c) What is Spoliation? Explain three component parts of spoliation.
d) Explain how tools can be useful in acquiring following type non-volatile operating system data from the file system.
Users and Groups, Passwords, Network Shares, Logs
e) What are the additional features supported by Network Forensic Analysis Tool to further facilitate network forensics?
f) What does the common law say about privacy?
g) Explain the use of recycle bin and restoring from recycle bin.

(7x4)

2.

a) What is Auditing? Differentiate Auditing with Cyber Forensic Investigation in concern of following criteria. Definition, Objectives & Scope, Methodology and Impact
b) Cryptographic algorithms will be categorized based on the number of keys that are employed for encryption and decryption. Explain following three categories of cryptographic algorithms.
i) Secret Key Cryptography
ii) Public Key Cryptography
iii) Hash Functions

(9+9)

3.

a) What are different types of volatile operating system data? Explain how forensic tools can be used in collecting each type of data.
b) What is Personal Digital Assistant? Briefly mention the applications of Personal Digital Assistant.
c) What care should be taken by the cyber forensic investigator in the collection and preservation of data stored on hard drive?

(6+6+6)

4.

a) Explain the Digital Forensic Laboratory Accreditation Standards Grading Criteria with the help of an example of Quality Assurance Checklist.
b) Define cyber stalking. What is its significance in Cyber Forensic? Explain types of cyber stalking.

(9+9)

5.

a) What is file carving? Explain Block-Based Carving and Statistical Carving in brief
b) What is Hash function? Mention applications of hash functions related to cyber forensics.
c) How to recover deleted file in Linux? Explain with the help of an example.

(6+6+6)

6.

a) Define the following terms:
   i) Data diddling
   ii) Email bombing
   iii) Denial of Service attack
   iv) Logic bombs

b) What is Session Hijacking? Explain the methods for session hijacking.

c) Define privacy law. Classify types of privacy law. Explain information privacy law.

(4+9+5)

7. Write Short notes on following:

a) i2 Analyst's Notebook

b) Forensic Toolkit

c) Steganography

(6+6+6)