CE1.3-R4: CYBER FORENSIC AND 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) How does computer recover the deleted file from hard disk?
b) What is file carving? Illustrate your answer with an example.
c) How you will prepare a suspected system for making forensic image of its hard disk at the site of crime?
d) List the differences between Caller ID spoofing and email spoofing.
e) Differentiate between Public Key Cryptography and Private Key Cryptography.
f) What are the utilities of Hash Value? Explain with examples.
g) What precautions have to take while solving any cyber crime case?

(7x4)

2.

a) List the standards for accreditation of the digital forensic lab.
b) In Cyber Forensic Analysis, what is the significance of Recycle Bin, Shortcut files, Print spool files, Thumbnails database, Index.dat, Swap and Hybernation files?

(9+9)

3.

a) What is criminal justice in India and implication on cyber crime?
b) Define and classify law of privacy.
c) Discuss the procedure and precautions for creating evidence control checklist.

(8+5+5)

4.

a) Discuss i2 Analyst's Notebook. What are its applications and outcome?
b) What do you understand about constitutional law? Discuss the various law and precautions on constitutional law.

(9+9)

5.

a) What is a MAC address and what is its significance in Cyber forensics? How you will find the MAC address from a forensic image of a hard disk of a system?
b) Define Anti-forensics. How is it different from traditional forensics?
c) Define volatile data. How you will acquire and analyze the volatile data from a live system? List the tools for this purpose.

(6+6+6)

6. Write the syntax/steps to execute the statements:

a) To recover deleted partition
b) To duplicate data in another partition
c) To create the image of hard disk.

(6+6+6)

7. Discuss about the tools for:

a) Network forensics tool
b) Attacker identification tool
c) Hash value identification and generation tool

(6+6+6)