CE1.3-R4: CYBER FORENSICS 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) Define cyber forensics and incident response.

b) List the important cyber forensics tools, which are required during cyber forensics.

c) How does Hash function useful during cyber investigation? Discuss the mechanism of Hash Function.

d) Discuss the data hiding techniques on NTFS.

e) Is there any difference between corporate cyber investigation and Government cyber investigation process?

f) What do you know about bit by bit copying method?

g) What is counter forensics? Explain with an example.

(7x4)

2.

a) In Cyber Forensic Analysis, what is the significance of Recycle Bin, Shortcut files, Print spool files, Thumbnails database, Index.dat, Swap and Hybernation files?

b) Describe the role of Windows Registry in digital forensic investigations.

(9+9)

3. Gaurav had an appointment with Doctor at the XYZ Hospital, Mumbai. While waiting for Doctor, Gaurav remembered that he had to email a document (that he was carrying in a floppy) to his office. As he looked around, he realized that there was a computer at the reception desk, which was switched on. However, the receptionist was nowhere to be seen. Gaurav immediately inserted the floppy disk containing the document into the floppy drive of the computer at the reception desk. Just then, the receptionist entered and saw Gaurav at the computer. She immediately called the security guards and intimated the manager about the incident. The manager wants to take legal action against Gaurav for unauthorized access. Advise the manager.

(18)

4.

a) Discuss the procedure and mechanism for recovering the deleted files and partitions.

b) Why is data acquisition and data duplication required? Discuss the tools for data duplications and acquisition for the purpose of cyber crime investigation.

(9+9)

5. List the command syntax /method for performing the following actions:

a) Remote login to other’s computer

b) To collect network traffic data

c) To access the information about the users currently on line in a particular network.

d) To examine collected data

(4.5x4)

6.

a) Differentiate between Steganography and cryptography. Explain with the help of examples.

b) Discuss the following forensics tools in detail-

  i) Autopsy browser

  ii) NetWitness

(9+[4.5x2])

7. Write short notes on **any two** of the followings:

a) Digital Forensics Lab accreditation standards

b) File carving

c) Rules of computer forensics

(9x2)