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 Incident response? Explain goals of incident response.

   (b) Explain the term Cyber terrorism with examples.

   (c) What is Evidence? Explain the type of Evidence.

   (d) Explain different types of Intrusion Detection Systems?

   (e) What is the need of cyber law in India?

   (f) Explain various anti-forensic techniques used by perpetrators.

   (g) Describe Intellectual property and IPR governance?

(7x4)

2. (a) Briefly explain difference between Block based and Characteristic based carving?

   (b) Analyze briefly about the Forensic Duplication and discuss the failings of standard duplication techniques from a forensic standpoint.

   (c) Explain the term steganography in detail with example and how can steganography files be identified?

(9+4+5)

3. (a) Write a note on Session Hijacking and list down methods to perform Session Hijacking.

   (b) Explain the difference between Cyber and Conventional Crime?

   (c) What are the duties of a subscriber of digital signature certificate? Generating key pair.

(6+4+8)

4. (a) What is a Swap file? Explain working of swap file with the help of a suitable example. What is the importance of a swap file in computer forensics?

(b) Explain the term spoofing attack. State the difference between IP spoofing attack and ARP spoofing attack.

(c) Explain Cloaking techniques in detail.

(5+7+6)

5. (a) Explain Email Header Forensic Analysis.

(b) Discuss the various types of models used for storage of data.

(9+9)

6. (a) Explain cyberstalking. List down its type in details.

(b) Explain the functions of an integrated digital forensic toolkit. Give examples of two such toolkits.

(9+9)

7. (a) How you will trace the crime which has been happened through email using tool.

(b) What are the tools used in Network forensics. Justify any two of them.

(c) Explain how law enforcement is done in computer forensics.

(6+6+6)
