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) Define computer forensics. Explain at least two techniques for computer forensic investigation

b) What is software piracy? What methods should an organization implement to prevent software piracy?

c) What can be inferred from the word "Digital Forensics"?

d) How are deleted files from a computer hard disk be recovered?

e) Explain the difference between copying and imaging of a hard disk.

f) Explain the use of recycle bin and restoring from recycle bin.

g) What is volatile data? How it is useful in computer forensic investigation? Explain the method and tools for capturing volatile data.

(7x4)

2.

a) What is file carving? Explain Block-Based Carving and Statistical Carving in brief

b) Define the following terms:

i) Data diddling

ii) Email bombing

iii) Denial of Service attack

iv) Logic bombs

c) Define data acquisition. Explain methodology of data acquisition in detail.

(6+4+8)

3.

a) Explain the working of BIOS. How can BIOS be updated?

b) What is Personal Digital Assistant? Briefly mention the applications of Personal Digital Assistant

c) Explain the strategies to collect live network traffic data alongwith the criterion for their selection.

(7+4+7)

4.

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

b) What is spoofing? Explain Caller ID spoofing, Email Spoofing, Web Spoofing in brief.

(9+9)

5.

a) Explain the technology advancements in Law Enforcement for Computer Forensics.

b) What are the features of NTFS v 3.0 file systems?

c) Write a short note on steganography.

(6+8+4)

6.

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) Define CyberCrime. Distinguish between Computer Crime and Computer-related Crime.

c) Define Computer Forensic Toolkit. What standard features should be built in a toolkit? How are these useful in computer forensic analysis of digital evidence?

(6+6+6)

7.

a) What is Cloaking? Differentiate between Cloaking and IP delivery.

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

c) Explain Public key cryptography with advantages and disadvantages

(7+6+5)