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) Differentiate between Computer Forensics and Computer Security. Why is Computer Forensics Important?

b) Explain the following terms in brief:
   i) SafeBack
   ii) GetTime
   iii) GetFree
   iv) Swap Files

c) What is volatile data? How can one gather Volatile Evidence from a running computer system?

d) When imaging a hard drive, is it better to clone the drive or create its image file? Justify your answer.

e) Write the syntax/steps for the following:
   i) To duplicate data in another partition.
   ii) To create the ISO of CD-ROM.

f) How to recover deleted file from Linux?

g) What risks are there if an organization does not consult a computer forensics expert after noticing a Cyber Security incident?

(7x4)

2.

a) What do you understand by a 'Protected System' under IT Act? Discuss about the systems, which should be declared as 'Protected System' under IT Act.

b) Explain the tools: Mandiant First Response and NetWitness.

(9+9)

3.

a) What is Session hijacking? Spoofing can take on many forms in the computer world, all of which involve some type fraudulent representation of information. Explain IP Spoofing.

b) Write the applications of Steganography. What types of files are most suited for steganography and why? How does Watermarking differ from Steganography?

(9+9)

4.

a) Define "Network forensics". Explain some strategies to collect live data from network.

b) Describe Slack space. How can data hiding achieved in slack space? When a file with used slack space is copied from one drive to another; then what is the status of data hidden in slack space in the destination drive?

(9+9)

5.

a) What is File Carving? Explain Statistical Carving and Block-based Carving.

b) Write short note on the following:
   i) Data Acquisition and imaging
   ii) Digital Forensics.

c) Describe how to recover deleted partition using FDISK and DISKPART commands.

(6+4+8)

6.

a) List the standards for digital accreditation of the Digital Forensic lab.

b) List the hardware and software which would be required for configuring user computer or laptop as a Cyber Forensic workstation. Explain the functioning of Hardware and Software used for this purpose.

(9+9)

7. Write short notes on the following:

a) Types of Computer Crimes

b) Define terms logic bombs, Trojan horse and denial of service attack

(9+9)