

## 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) List and explain the various kinds of cyber crimes.
- b) What do you know about cyber forensics? How is it different from traditional forensics?
- c) What is the role of 'hash function' in cyber forensics? Explain your answer with an example.
- d) List the differences between deleted file recovery techniques and deleted partition recovery techniques.
- e) What is file carving? List the software tools for file carving. Explain the process of file carving with the help of an example.
- f) List at least four laws covered in IT act 2000.
- g) Define NIST in detail.

(7x4)

2.

- a) List the hardware and software to be required for configuring your computer or laptop as a cyber forensic workstation. Explain the functioning of hardware's and software's used for this purpose.
- b) What precautions should be taken while solving any case of cyber crime and why? Explain your opinion.

(9+9)

3. Discuss the functioning of the following software's used in cyber forensics.

- a) FTK
- b) Helix
- c) Mandiant
- d) Netwitness
- e) Getfree
- f) Safeback

(6x3)

4.

- a) Discuss the differences between Public Key cryptography and Private Key cryptography. Explain your answer with an example.
- b) Discuss the steps of Data hiding and seeking for i) NTFS and ii) ext

(9+9)

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

- a) Collecting network traffic data and IP address and machine address of a machine.
- b) Collecting the information of sender, who has sent a SPAM mail to you?
- c) Collecting the keystrokes information of any computer machine.
- d) Collecting the information about the external storage devices attached in past with your system.

(4.5x4)

**6.**

- a) Discuss the digital forensic laboratory accreditation standards, in detail.
- b) What do you think about the term “Legal Liability for mistakes”? Explain in detail.

**(9+9)**

**7.** Write short notes on any **three** of the following:

- a) Data acquisition and imaging
- b) Applications of Digital Signature
- c) Spoofing Attack
- d) Session Hijacking

**(3x6)**