

## 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) Describe the common elements in act of terrorism and classify the information warfare.
  - b) How can emails be traced for forensic investigation purpose?
  - c) Explain digital forensics life cycle in detail.
  - d) Differentiate between corporate cyber law and civil cyber law.
  - e) Explain briefly the role of interactive communication in cyber forensics.
  - f) What is file carving?
  - g) Define hash function and discuss its role in cyber forensics.

**(7x4)**
  
2.
  - a) Discuss and explain the rules of computer forensics in detail.
  - b) Discuss cyber forensics investigation process in detail.

**(9+9)**
  
3. Explain the functioning and features of following tools:
  - a) Sleuth kit
  - b) Netwitness
  - c) Prodiscover

**(3x6)**
  
4.
  - a) Differentiate between cryptography and Steganography. Explain public key cryptography and private key cryptography.
  - b) How does data hiding carried out in NTFS file system? Explain in detail.

**(12+6)**
  
5. Explain the role of following in cyber forensics-
  - a) BIOS
  - b) RAM
  - c) Network traffic
  - d) Internet
  - e) Hard disk

**(18)**
  
6.
  - a) Discuss the accreditation standards to setup a typical digital forensics Lab.
  - b) Explain the role of following documents in cyber forensics-
    - i) Evidence Control Checklist
    - ii) Quality Assurance Checklist
    - iii) Equipment Checklist
    - iv) Health and Safety Checklist

**(6+12)**
  
7. Write short note on followings:
  - a) Recovery of deleted partition
  - b) Data hide and seek
  - c) Overview of cyber crimes.

**(3x6)**