CE1.3-R4: CYBER FORENSICS 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 steps involve in handling electronic evidence.

b) Spoofing and Hijacked Session Attack are designed to hide the original source of access or identity. Clearly differentiate between Spoofing and Hijacked Session Attack.

c) Write Short note on *Root kits*.

d) What care should be taken by the cyber forensic investigator in the collection and preservation of data stored on hard drive?

e) What are the recommendations for Cyber forensic investigators while extracting Data from Operating Systems?

f) Explain the additional features supported by Network Forensic Analysis Tools to facilitate network forensics.

g) Why Cyber forensic investigators may also need to examine secondary network traffic data sources, such as host-based firewall logs and packet captures, and non-network traffic data sources, such as host operating system audit logs and antivirus software logs.

(7x4)

2.

a) Explain the steps of Cyber Forensic Investigation Process.

b) Cryptographic algorithms are classified or categorized based on the number of keys that are employed for encryption and decryption. Explain following three category of cryptography algorithms with their significance in Cyber Forensic.

i) Secret Key Cryptography (SKC)

ii) Public Key Cryptography (PKC)

iii) Hash Functions

c) List different types of volatile operating system data and explains how forensic tools can be used for collection of each type of data.

(4+6+8)

3.

a) Define cyber stalking. Explain Email stalking and Internet Stalking.

b) What is File Allocation Table (FAT)? List and Explain different versions of FAT. Differentiate between FAT12, FAT16 and FAT32.

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

(6+6+6)

4.

a) Explain the concept of Hiding Data in File system Slack Space with Bmap. What are the advantages and disadvantages?

b) What is Hooking? Explain API Hooking, IAT Hooking and Inline Hooking.

(9+9)

5.

a) Explain in detail the significance of TCP/IP layer in Network Forensics

b) Explain the different ways of validating the identity of a suspicious host.

c) Explain the Digital Forensic Laboratory Accreditation Standards Grading Criteria with the help of an example of Quality Assurance Checklist.

(6+8+4)

6.

a) Explain the Law Relating to Access to Private Information.

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

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

(6+6+6)

7. Write a short note on the following:

a) Forensic Toolkit

b) i2 Analyst's Notebook

c) Steganography

(6+6+6)