No. of Printed Pages : **2**

Sl. No.

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 Cyber Forensics. List the techniques for investigation process and explain any two in detail.

(b) Distinguish between Cyber Crime and Traditional Crime.

(c) Discuss the features and limitations of FAT32, NTFS and exFAT file system in Windows OS.

(d) What is steganography and give its significance in security of data.

(e) What are Logic Bombs and Email Bombs ?

(f) Define Volatile Data and its usefulness in forensic investigation. Explain the methods for capturing Volatile Data.

(g) Write a brief note on i2 Analyst's Notebook. **(7x4)**

2. (a) Explain following three categories of Cryptography Algorithms with their significance in Cyber Forensic.

(i) Secret Key Cryptography (SKC)

(ii) Public Key Cryptography (PKC)

(iii) Hash Functions

(b) Define Computer Forensic Toolkit. What standard features should be built in a Toolkit ? How are these useful in Computer Forensic Analysis of digital evidence ?

(c) Elaborate session hijacking and explain session hijacking as threat. **(6+6+6)**

3. (a) Define Cloaking. Explain Cloaking Techniques in detail.

(b) What is Hooking ? Explain API Hooking, IAT Hooking and Inline Hooking. **(9+9)**

4. (a) What is Network Traffic in terms of Cyber Forensic ? Briefly explain Network Forensic Analysis Tools.

(b) Narrate data acquisition with reference to Cyber Forensics.

(c) What is Privacy Law in terms of Cyber Forensics ? Explain types of Privacy Law. Explain Information Privacy Law. **(5+4+9)**

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

(b) Explain important of Windows Registry in investigation of a windows OS based system. **(9+9)**

6. (a) List the Rootkits of Cyber Forensics and narrate them in few lines.

(b) What is File Carving ? Explain Block-Based Carving and Statistical Carving in brief.

(c) How can we have message authentication using digital signature ? **(6+6+6)**

7. (a) What is Software Encase Forensic ? How does this software work ?

(b) List the offences included in IT Act 2000.

(c) What is Spoofing ? Explain Caller ID spoofing, Email Spoofing, Web Spoofing in brief. **(5+4+9)**

- o O o -