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) What is Computer Forensics? Cite some common applications of computer forensics.

(b) What are the key features of i2 Analyst's Notebook? Explain Flexible Data Acquisition with respect to i2 Analyst's Notebook

(c) Difference between Steganography and Cryptography

(d) How a Laptop does differ from a PDA (Personal Digital Assistant)?

(e) Explain Data Acquisition and Duplication.

(f) What is the Role of Digital Evidence?

(g) What is the role of "Chain of Custody of Digital Evidence" in digital investigations? **(7x4)**

2. (a) Describe the various phases of Cyber Forensics.

(b) What is "EnCase Forensic Toolkit"? Explain its working. In which phase of Cyber Forensics, this tool can be used? **(9+9)**

3. (a) What is a Hash function? How do Cyber Forensic Examiners use Hashes?

(b) What is Email Spoofing? How does it affect a computer system? What are the necessary guidelines that one must follow to prevent the system from Spoofing attacks. **(9+9)**

4. (a) Explain the working of BIOS. What are the main functions of PC BIOS? How can BIOS be updated?

(b) Describe NIST Cyber security Framework in detail. **(9+9)**

5. (a) Discuss the role of "First Responder" in digital forensic investigations?

(b) What is Forensic Hard Drive Imaging? If software is available to create a forensic image of a hard disk or other media, what is the benefit of forensic hardware?

(c) How File Recovery is different from File Carving? Explain block based carving and statistical carving in brief. **(6+6+6)**

6. (a) Explain Data Recovery in Linux.

(b) Why is it important that all the software used by law enforcement officers be licensed and registered? Law enforcement budgets are often tight; why not use freeware as much as possible?

(c) Discuss measures to tackle Cyber Crime. **(6+6+6)**

7. Write short notes on the followings :

(a) Importance of Cyber Laws.

(b) Swap Files and Temporary Files

(c) Digital Forensic Examiner Checklist **(6+6+6)**

- o 0 o -