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) How does digital forensics differ from data recovery ?

(b) Consider a file system with 4KB blocks and 64 bit block indexes, Each inode has 10 direct blocks, 1 indirect block, and 1 double indirect block. What is the largest file possible that can be stored ?

(c) Elaborate and Justify with an example how the developments in technology has invaded personal and corporate securities ?

(d) How cyber attackers are identified ? Elaborate the strategies.

(e) What is the role of PDA ? How cyber criminals can exploit PDA security ?

(f) What is a dead acquisition ?

(g) What are Cloaking techniques ? Explain their role in Cyber forensics ? **(7x4)**

2. (a) Consider the following scenario :

A computer is suspected of having been used to download contraband pictures from the Internet. Formulate higher-level hypothesis and low-level hypothesis for this.

(b) Elaborate the different possible cases of Cyber crimes. Highlight some possible real life cases to justify your answer. **(9+9)**

3. (a) What is Stenography technique ? Discuss the process of reversing the stenography ?

(b) What is Locard's Exchange Principle ? Give three examples of how this principle could apply to digital forensic investigation.

(c) What is the difference between imaging and copying ? **(4+8+6)**

4. (a) RSA key is N = 187, e = 107. You observe a ciphertext c = 2. What is the plaintext ? (Note: 187 = 11 “ 17.)

(b) Is hashing a reversible process ? Most viruses infect your system by implanting themselves into the existing executable files on the disk. Explain how to use a hash algorithm to design a virus detector, which identifies the files that may be infected by viruses.

(c) A file system with 300 GByte disk uses a file descriptor with 8 direct block address, 1 indirect block address and 1 doubly indirect block address. The size of each disk block is 128 bytes and the size of each disk block address is 8 bytes.

What will be the maximum possible file size in the file system ? **(6+6+6)**

5. (a) Why is it important to analyze unallocated storage space for the computer forensic analysis ? Discuss the use of GetFree utility to capture data from unallocated storage space.

(b) What is The Sleuth Kit (TSK), Discuss the use of following TSK command line tools.

(i) tsk_gettimes

(ii) tsk_recover

(iii) fls

(iv) blkcalc

(c) What can network forensics reveal ? **(6+8+4)**

6. (a) What is the difference between static acquisition and live acquisition ?

(b) What are File Signatures and why should you care when recovering ?

(c) What is File carving ? What benefits it has in cyber forensics ? **(6+6+6)**

7. (a) Which one is more ideal Dead analysis or live analysis and why ?

(b) What are the contents of Digital Forensics Examiner checklist ? Elaborate and discuss.

(c) Integrity of evidence is essential in order to make digital evidence to be admissible in court of law. What is CoC (Chain of Custody) and why is it important for evidence integrity ? **(6+6+6)**

- o O o -