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) Enlist tools used for capturing network traffic.

(b) What is the main difference between polymorphic and metamorphic viruses ?

(c) How worms propagate through e-mail ?

(d) What is steganography ? Name its types.

(e) What is volatile data ? What role does it play in forensics ?

(f) Write note on ISO/IEC 17025 standard.

(g) Write short note on Data Acquisition and Duplication. **(7x4)**

2. In order to facilitate the exchange of secret messages, Sally & Harry have developed an image based steganography system. After a considerable investigative effort, you have learned that their system deploys an ASCII letter encoding scheme, shown in the below figure. You have also discovered that they use raw RGB images as their 'cover images', and that they embed their secret bits into these images by deploying the LSB scheme. In particular, they use the last 2 bits of each colour channel (in each pixel) for embedding. This morning, you've seized one of their stego images. The image is of size 20x40 pixels. Compute and show how many secret letters, at most, could be contained in the given image ?

Binary	ASCII	Binary	ASCII	Binary	ASCII
000000	A	001010	K	010100	U
000001	B	001011	L	010101	V
000010	C	001100	M	010110	W
000011	D	001101	N	010111	X
000100	E	001110	O	011000	Y
000101	F	001111	P	011001	Z
000110	G	010000	Q		
000111	H	010001	R		
001000	I	010010	S		
001001	J	010011	T		

18

3. How to use :

(a) Firewalls to verify that a Cyber security incident has occurred.

(b) Antivirus tools to check Cyber security breach. **[9+9]**

4. Explain how following are used for evidence collection and analysis :

(a) Safeback

(b) Scrub and GetSwap **[9+9]**

5. As a network traffic analyst how will you use the following for detecting attacks :

(a) Source IP address, Source port number, Destination IP address, Destination port number

(b) Protocol type and flags

(c) Flow count and data bytes count **[6+6+6]**

6. Write short notes on :

(a) Recovering deleted files on Linux System

(b) File carving

(c) Role of cyber cell in fighting cyber-crimes in India **[6+6+6]**

7. (a) Differentiate between public key cryptography and private key cryptography.

(b) Which parameters of TCP header are used for SYN flooding attack ? Explain SYN flooding attack. **[10+8]**

- o 0 o -