No. of Printed Pages : **2**

Sl. No.

CE1.3-R4 : CYBER FORENSIC AND LAW

NOTE :

1. **Answer question 1 and any FOUR questions from 2 to 7.**
2. **Parts of the same question should be answered together and in the same sequence.**

Total Time : 3 Hours **Total Marks : 100**

1. (a) Define what do you mean by Cyber Forensics.

(b) Briefly explain any 3 technological abuses which affect the securities in the corporate sector.

(c) What is Coroner's Toolkit ? Explain in brief.

(d) Explain Secret Key Cryptography as a concealment technique in Cyber Forensics.

(e) What is the process involved in File Carving ? Explain.

(f) How is data recovery happening in Linux environment ? Explain.

(g) What is NIST ? Explain. **(7x4)**

2. (a) Elaborate some of the latest publicly reported Cyber-crimes in the latest time.

(b) Differentiate giving examples between the Temporary file and Swap file. What is their role in Cyber Forensics ? **(9+9)**

3. (a) What do you understand by the term Steganography ? Briefly explain the process involved in the reversal of the steganographic process.

(b) What is the process involved in recovering deleted files ? Explain any two tools which can help in the file recovery. **(9+9)**

4. (a) How is data acquired from the Network Traffic ? Explain some of the network forensics analysis tools that help a cyber forensics expert.

(b) What are the standards required for Digital Forensic Laboratory accreditation ? Explain in brief. **(9+9)**

5. (a) What is the difference between IP Spoofing and E-mail Spoofing ? How can we defend our systems from Spoofing Attacks ?

(b) What factors are used when making the decision for selecting the right Digital Forensic Investigation Tools for Sys Admins ? **(9+9)**

6. (a) Explain how Firewalls can be used to verify that a Cyber security incident has occurred in an organization.

(b) Explain SYN flooding attack. Which parameters of TCP header are used for SYN flooding attack ? **(9+9)**

7. Write short notes on **any three**.

(a) Mandiant First Response

(b) Hijacked Session Attacks

(c) Role of External Storage and Servers in Cyber Forensics

(d) Constitutional Law in Cyber Forensics context

(e) Forensic Analysis **(3x6)**

- o O o -