(b) What is the purpose of sed and grep command in Unix/Linux. (4)

(c) Explain briefly any three forensic tools used for analysing networks. (6)

[This question paper contains 8 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 9945 **K**

Unique Paper Code : 2343010024

Name of the Paper : Cyber Forensics Discipline Specific Elective

Name of the Course : **B.Sc. (H) Computer Science**

Semester : VII

Duration : 3 Hours Maximum Marks : 90

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. **Section - A** is compulsory.
3. Attempt any **4 (Four)** questions from **Section B.**
4. **All** parts of a question must be answered together.

SECTION - A

1. (a) What is forensic triage and why is it important in cybercrime investigations? (2)

(b) Why is it important to start writing and updating the investigation report from the beginning of a project? (2)

(c) Write any two functions performed by each of VeraCrypt and Encrypted Disk Detector (EDD) tools used in encryption and decryption? (2)

(d) What is Formjacking? (2)

(e) How is timeline analysis helpful in cyber forensic investigations? (2)

(f) Differentiate between substantive cybercrime laws and procedural cybercrime laws. (2)

(c) Discuss Password cracking, Hacking and Software Piracy in reference to cybercrime? (6)

6. (a) What is email forensics? Distinguish between email tracing and email tracking, giving suitable examples. (5)

(b) Briefly explain the five phases of the Forensic Evidence Collection Procedure. (5)

(c) Define Cyber Forensics? Explain any three challenges in Cyber forensics. (5)

7. (a) Discuss the following terms : (3+1)

(i) Dual Key encryption

(ii) Digital Signatures

(c) Describe any three precautionary measures that should be taken before the acquisition of digital evidence. (6)

4. (a) What is Recuva tool? Explain its purpose. (2)

(b) Give five differences between digital evidence and physical evidence. (5)

(c) Describe each step of the forensic investigation process. (8)

5. (a) Describe the purpose of the NTUSER.DAT and SYSTEM hives. (4)

(b) What is Extended Idle System? Briefly describe the key features of ext2 and ext4. (5)

(g) Which IPC section of IT Act, 2000/2008 deals with the following cybercrimes : (3)

(i) Sending offensive messages through communication service.

(ii) Cyber terrorism.

(iii) Publishing or transmitting of material depicting children in sexually explicit actin electronic form.

(h) Give any three advantages of NTFS over FAT 32 file system. (3)

(i) Explain the purpose of following OS files : (4)

(i) Configuration Files

(ii) Application Files

P.T.O.

(iii) Temporary Files

(iv) SWAP Files

(j) Write the purpose of the following tools : (4)

(i) RegRipper

(ii) FINALeMAIL

(iii) FTK Imager

(iv) Ophcrack

(k) Explain the following cyberattacks : (4)

(i) Phishing

(ii) Juice Jacking

SECTION - B

(Attempt Any **Four** Questions)

2. (a) Explain the Byte Back and IsoBuster data recovery tools. (4)

(b) What is the use of Windows event logs? Explain any two categories of logs. (5)

(c) Enlist any six key points that must be included in a Chain of Custody form. (6)

3. (a) Explain the following terms : (4)

(i) Electronic Data Interchange (EDI)

(ii) Volatile Evidence

(b) What is a Registry key? Explain its significance. Write the name of tool that is used to parse the registry hives. (5)