[This question paper contains 4 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 5056 **L**

Unique Paper Code : 2344000034

Name of the Paper : Cyber Forensics

Name of the Course : **Generic Elective**

Semester : VIII

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. The paper has **two** sections. **Section A** is compulsory.
3. Attempt any **four** questions from **Section B**.
4. Parts of a question must be answered together.

SECTION A

1. (a) What is the purpose of the sed command in Linux? Write a sed command to delete all log lines containing the word "DEBUG" from logfile.txt. 2

   (b) Name two cryptographic hash algorithms used in digital forensics. What does it indicate if the hash value of an acquired image differs from that of the original evidence? 2

   (c) Classify the following as Volatile or Non-volatile evidence: 2
   - i. Network Connections
   - ii. Windows Registry
   - iii. RAM contents
   - iv. Swap Files

   (d) Explain the provisions of Section 43 of the Information Technology Act, 2000. Give two specific examples of actions that constitute offences under this section. 3

   (e) Briefly explain any two password recovery tools used in forensic investigation. 4

P.T.O.

(f) State whether each of the following statements is True or False: 5

i. SHA-256 generates a 128-bit hash value.

ii. NTFS supports file-level encryption using the Encrypting File System (EFS).

iii. Files deleted from the Windows Recycle Bin are permanently and irrecoverably removed from the disk.

iv. EnCase is a free and open-source digital forensic tool available for download.

v. The $MFT file in NTFS contains one record for every file and directory on the volume.

(g) Match the following Windows Registry hive files with their forensic content: 6

Hive File		Content	
i.	SAM Hive	a.	Installed software and application settings
ii.	SYSTEM Hive	b.	Current user desktop preferences
iii.	SOFTWARE Hive	c.	Local user account names and password hashes
iv.	NTUSER.DAT	d.	Hardware configuration and active services
v.	SECURITY Hive	e.	Shell folder paths and ShellBag entries
vi.	UsrClass.dat	f.	Local security policy and LSA secrets

(h) A file named "systemevents.log" contains timestamped security event entries. Write grep commands to perform the following tasks: 6

i. Find and display all lines containing the text "FAILED LOGIN".

ii. Display all lines that contain the date "2025-03-15".

iii. Count the total number of lines containing the word "SUCCESS"

iv. Show line numbers for all lines containing "ADMIN", ignoring case sensitivity.

v. Display all lines that do NOT contain the word "INFO".

vi. Find and display lines that begin with the tag "[CRITICAL]". its answer

SECTION B

2. (a) Differentiate between the following: 5

i. Physical Disk and Logical Disk

ii. MBR (Master Boot Record) and GPT (GUID Partition Table) partition schemes

(b) What is a digital forensic report? List any four essential components that must be included in a well-structured digital forensic report. 5

(c) What are the salient features of e-commerce? Explain any four key features of e-commerce and their importance in online business operations. 5

3. (a) What is Electronic Data Interchange (EDI)? List two challenges and two advantages associated with EDI in the context of e-commerce. 5

(b) What is Dual Key Encryption? How does it work in the context of digital signatures to ensure (i) authenticity and (ii) non-repudiation? 5

(c) Explain the six stages of digital evidence documentation in a cyber-forensic investigation. Describe what occurs during each stage. 5

4. (a) What is IP tracking? Briefly explain the steps involved in tracing an IP address during a cyber-forensic investigation. 5

(b) What is the AmCache.hve file in Windows? What forensic artifacts does it store and why is it important in a forensic investigation? 5

(c) Explain the complete process of using the Autopsy forensic tool, beginning with setting up a new case and ending with analyzing the findings. Also mention the important ingest modules you would enable during an investigation. 5

5. (a) What is deleted file recovery? Briefly explain any three tools/techniques used to recover deleted files from a storage device. 5

(b) Define a file system and compare the FAT32 file system with the NTFS file system, highlighting their key differences. 5

(c) What is the Windows Event Log? Name and briefly explain any four types of events recorded in Windows Event Logs during a forensic investigation. 5

6. (a) What is the SYSTEM hive in the Windows Registry? Describe any two key forensic artifacts that can be extracted from the SYSTEM hive and explain their investigative significance. 5

(b) What are malicious software attacks? Explain four key types of malwares in detail. 5

(c) What is the EXT4 file system? State any three improvements that EXT4 offers over EXT3 and one limitation of EXT4. 5

7. (a) Write short notes on any three of the following: 15

i. Forensic Triage

ii. DDoS

iii. Password Cracking Techniques

iv. Search and Seizure of Digital Evidence

v. Juice Jacking