(b) What are the major forms of Intellectual Property Rights? Explain with suitable examples. (10)

7. Write short notes on **(any 3)** : (15)

(i) Role of Hive files

(ii) Password cracking techniques

(iii) Security challenges in e-commerce

(iv) Internet and cyber crime

(v) File systems

[This question paper contains 8 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 5323 **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) Mention any two software tools used to capture and analyse network traffic for forensic purposes. (2)

(b) Give one example of a symmetric encryption algorithm and one example of an asymmetric encryption algorithm. (2)

(c) What is e-mail spoofing? How does it differ from a genuine e-mail? Give one example. (2)

(d) What is a registry hive file? Name any two hive files found in a Windows system. (2)

(e) What is an IP address? How does it help in tracking the origin of an e-mail? (2)

(f) What is the purpose of a grep (Global Regular Expression Print) search in digital forensics? Give one example. (2)

(g) Why is peer review essential in digital forensics reporting? What types of errors can it catch? (3)

(h) Define cryptographic hash function. Why are hash values (e.g., MD5, SHA-1) used in digital forensics? (3)

(c) Explain the concept of Intellectual Property (IP) in cybercrime. How does digital forensics help in investigating and proving cases of software piracy or data theft? Illustrate with examples. (5)

5. (a) Differentiate between **(Any two)** (5)

(i) open-source software and pirated software

(ii) evidence collection and evidence preservation

(iii) password cracking and password guessing

(iv) hashing and encryption

(b) Explain the concept of cyber forensics with a relevant example. Discuss the important legal aspects that must be considered during an investigation. (10)

6. (a) What is software piracy. Explain the role of license keys and activation systems in preventing piracy. (5)

(iv) Recognize all potential evidence: running processes, open files, RAM contents, network connections, attached devices.

(v) Label and seal the computer, use anti-static bags, transport without booting or altering the system.

(b) What is timeline analysis in cyber forensics and explain the role of timestamps in timeline analysis. Also, list any two key features of timeline analysis. (5)

(c) Describe the four primary characteristics of digital evidence, providing a suitable justification for each, and briefly explain the reason why digital evidence is regarded as fragile. (5)

4. (a) What is cybercrime? List and explain any three offences defined under the IT Act 2000. (5)

(b) File systems are crucial for reconstructing digital events." Justify this statement. (5)

(i) Why is maintaining a chain of custody critical in digital forensics? Mention two consequences of a broken chain. (3)

(j) Answer the following two questions briefly: (3)

(i) Can the Internet function without the World Wide Web? Give one example.

(ii) Can the World Wide Web function without the Internet? Why or why not?

(k) What is the difference between a forensic imaging tool and a forensic analysis tool? Give one example of each. (3)

(l) Briefly describe the concept of "search and seizure" in digital forensics and its legal significance. (3)

Section B

2. (a) A forensic investigator arrives at a live crime scene. From the following list, classify each item as volatile or non-volatile with a valid reason. (5)

(i) CPU registers / cache

(ii) Swap file

(iii) Running processes

(iv) Registry Hives

(v) Network connections

(b) A given situation where a company's computer systems have been hacked, customer data stolen, and ransomware deployed. Define cybercrime and identify three distinct types of cybercrimes illustrated in this scenario. (5)

(c) What is meant by Dual Key Encryption? Describe how it ensures confidentiality and authenticity in online communication. (5)

3. (a) A forensic investigator arrives at a crime scene containing a running computer. Arrange the phases of evidence preservation from top to bottom that must be followed to maintain the integrity and admissibility of digital evidence. (5)

(i) Calculate hash values (MD5/SHA-1), document chain of custody, store evidence in tamper-proof containers.

(ii) Capture volatile data first (RAM, network state), then create a forensic image using write-blockers for the hard drive.

(iii) Record every action (time, date, person, tool used), photograph the scene, maintain a detailed log for court admissibility.