H **116B3** Total Pages: **2**

Register No.: .... Name: ....

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

SEVENTH SEMESTER B.TECH DEGREE EXAMINATION (R), DECEMBER 2023
COMPUTER SCIENCE AND ENGINEERING
(2020 SCHEME)

Course Code : **20CST491**

Course Name: **Cyber Forensics**

Max. Marks : **100** **Duration: 3 Hours**

PART A

(Answer all questions. Each question carries 3 marks)

1. Explain the three computer forensics data acquisition formats.
2. Describe Public and Private investigations with suitable example.
3. Explain the difference between NTFS and FAT file system.
4. Explain Metadata-based File Recovery technique.
5. What is Locard's exchange principle? Explain its importance in forensic Investigations.
6. Describe Rootkits in detail.
7. List any four OWASP Top 10 security risks in detail.
8. Describe various ICMP attacks.
9. Explain the role of encryption in forensics.
10. How data wiping done in hard drive?

PART B

(Answer one full question from each module, each question carries 14 marks)

MODULE I

11.	a)	Explain different Forensic Protocol for Evidence Acquisition	(6)
	b)	What is Phishing? Explain different types of Phishing.	(8)

OR

12.	a)	What are the different challenges in Cyber Forensics?	(6)
	b)	Describe different types of Cybercrimes and also list the different skills required to become a Cyber Forensic Expert.	(8)

MODULE II

13.	a)	Explain the different data categories in a File System.	(8)
	b)	Describe FAT32 File Structure.	(6)

OR

14.	a)	Describe the terms file slack, RAM slack and drive slack.	(6)
	b)	Explain the different types of volatile information in a live response system. List any two tools used for obtaining volatile information.	(8)

MODULE III

15. a) Illustrate the importance of log analysis in cyber forensics. (6)

    b) What is reconnaissance? List and explain any five reconnaissance tools. (8)

OR

16. a) Why would you conduct a live response on a running system. (6)

    b) Describe Agile analysis in detail. (8)

MODULE IV

17. a) List any six types of web attacks and how these web attacks are investigated? (6)

    b) Explain Penetration Testing in detail. (8)

OR

18. a) List and explain different Network Forensic Analysis Tools. (6)

    b) Explain OSI Reference Model in detail with the help of suitable diagram. (8)

MODULE V

19. a) Distinguish between Steganography and Cryptography. (8)

    b) Explain the different types of Anti-forensics Detection Techniques. (6)

OR

20. a) What is Data Remanence? List the advantages of Data Remanence. (6)

    b) What is Spoofing? How to prevent spoofing attack? (8)

****