Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech Degree S7 (Hons.) Examination November 2025 (2022 Admn)

Course Code: CST495

Course Name: CYBER FORENSICS

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

PART A

Answer all questions, each carries 3 marks. Marks

1		Define Computer Forensics, Network Forensics and Data Recovery.	(3)
2		How Public Investigations are different from Private Investigations?	(3)
3		Explain FAT Partition Boot Sector.	(3)
4		Discuss any three differences between NTFS and FAT.	(3)
5		Why would you conduct a live response on a running system?	(3)
6		What is a Rootkit? How is it detected?	(3)
7		Explain Drive-by Downloads.	(3)
8		Differentiate between Penetration Testing and Risk Analysis.	(3)
9		Distinguish between a Cryptographer and a Crypter.	(3)
10		What does an Eraser tool do?	(3)

PART B

Answer any one full question from each module, each carries 14 marks.

Module I

11	a)	Explain different steps in Cyber Forensic Investigation.	(8)
	b)	Explain the three computer forensics data acquisitions formats.	(6)

OR

12	a)	Describe the various types of Cybercrimes.	(8)
	b)	Differentiate between Static acquisition and Live acquisition with example.	(6)

Module II

13	a)	Explain the different data categories in a File System.	(8)
	b)	Explain Bit Stream Copy. Name any two tools that can be used to make a bit stream copy.	(6)

OR

14	a)	Describe the FAT File Structure in detail.	(8)
	b)	What is Metadata? Describe the first 16 metadata records you would find in the MFT.	(6)

Module III

15	a)	Explain the different types of volatile information in a live response system. List any two tools used for obtaining volatile information.	(8)
	b)	What is Locard's Exchange Principle? Why is it important in forensic investigations?	(6)

OR

16	a)	What is Physical Memory Dump? Explain how a physical memory dump is analysed.	(8)
	b)	Explain Agile Data analysis.	(6)

Module IV

17	a)	Explain the different layers of OSI model.	(4)
	b)	Briefly describe the OWASP Top 10 web application vulnerabilities for 2021.	(10)

OR

18	a)	What is Penetration testing? Explain different types of Penetration Testing.	(8)
	b)	What is Wireshark? How does it work?	(6)

Module V

19	a)	What is Steganography? How is Steganography done?	(8)
	b)	What is Spoofing? How can we prevent spoofing attack?	(6)

OR

20	a)	Explain the various Anti-forensics Detection Techniques.	(8)
	b)	Distinguish between data wiping and data formatting.	(6)

****