Reg No.:_____ **0520MCA267122202** Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Third Semester MCA (Two Years) Degree (R, S) Examination December/January 2023-24

Course Code: 20MCA267

Course Name: CYBER FORENSICS

Max. Marks: 60 Duration: 3 Hours

PART A

Answer all questions, each carries3 marks. Marks

1	List out any six areas of cyber forensics	(3)
2	What are the different formats used to store the collected evidence in digital forensics?	(3)
3	With help of a diagram, explain Drive Slack, File Slack and RAM Slack	(3)
4	What is Alternate Data Stream in NTFS	(3)
5	Explain the data acquisition tools available in Linux OS	(3)
6	Differentiate Symbolic link and Hard link.	(3)
7	What is Wireshark tool used for? List it's features .	(3)
8	List out any four challenges in Mobile phone investigation	(3)
9	List out any six obvious ethical errors to be avoided in Digital Forensics	(3)
10	What are the different types of Forensics reports?	(3)

PART B

Answer any one question from each module. Each question carries 6 marks.

Module I

11	What is cyber forensics? Explain process involved in cyber forensic investigation	(6)
	OR	
12	What are the different steps involved in investigating a company policy violation? Illustrate with a real-time example	(6)

Module II

13	a) Explain in detail the NTFS.	(4)
	b) How to analyse hidden data in NTFS.	(2)
	OR	
14	What is Windows Registry used for in cyber forensics analysis? Explain	(6)

Module III

15	a) What is the importance of Write Blocker in forensics?	(3)
	b) Explain the use of Sleuth Kit tool.	(3)

OR

16	Discuss the file structure in Mac OS. What are the forensics procedures involved in Mac?	(6)

Module IV

17	Explain mobile forensics extraction methods	(6)

OR

18	What is Network forensics? Explain the standard procedures followed in network forensics.	(6)

Module V

19	Explain the guidelines for writing a report which is admissible in a court of law.	(6)

OR

20	Explain the structure of a forensic report?	(6)

****