Reg No.:_______________ Name:__________________________

0720MCA267112401

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Third Semester MCA (Two Year) Degree (R,S) Examination December 2024

Course Code: 20MCA267

Course Name: CYBER FORENSICS

Max. Marks: 60 Duration: 3 Hours

PART A

Answer all questions, each carries 3 marks. Marks

1 List out any 6 areas of cyber forensics. (3)

2 Differentiate between bit- stream copy and sector copy. (3)

3 Analyse how deleted data in solid state storage devices possess a challenge for investigation. (3)

4 In which version of windows, Microsoft BitLocker is supported? What are the hardware and software requirements of BitLocker? (3)

5 What is a data fork and a resource fork? (3)

6 Differentiate between Symbolic Link and Hard Link. (3)

7 What is Wireshark tool used for? List its features. (3)

8 Define the DiD strategy for protection. (3)

9 Mention the responsibilities of a computer forensic investigator. (3)

10 What are the different types of reports? (3)

PART B

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

Module I

11 Categorize the formats used to store the collected digital evidence. (6)

OR

12 Briefly describe the procedures for the Internet abuse investigations, Email abuse investigations and Industrial Espionage investigations. (6)

Module II

13 Explain in detail the NTFS mentioning the procedures to analyse hidden data in NTFS. (6)

OR

14 Explain the importance of Windows registry in forensics analysis. (6)

Module III

15 Explain the file structures of Linux and Unix operating systems. (6)

OR

16 Explain data acquisition and validation tools / commands available in Linux. (6)

Module IV

17 Describe the importance and steps in the standard operating procedure for network forensics. (6)

OR

18 Explain the smart phone specific hardware options. (6)

Module V

19 Describe the structure of a forensic report. (6)

OR

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

****