0520MCA267122102

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

Third Semester MCA (Two Years) Degree (S, FE) Examination May 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	What are the activities considered as company policy violations?	(3)
2	Is there any difference between Bit-Stream Copy and Sector Copy? Comment on it.	(3)
3	Why Solid-State Drives are a challenge for forensics investigators?	(3)
4	In which version of Windows, Microsoft BitLocker support? What is hardware and software requirements of BitLocker?	(3)
5	How Macintosh reduces file fragmentation?	(3)
6	Which are the data acquisition tools available in Linux that are forensically sound?	(3)
7	Enumerate systems used to collect network data for forensics.	(3)
8	List down the features of Wireshark tool.	(3)
9	Mention the responsibilities of a Computer Forensic Investigator.	(3)
10	How Autopsy tool is used to generate forensics report?	(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	Illustrate the areas of cyber forensics.	(6)

Module II

| 13 | Differentiate between FAT and 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 | (a) | How B* tree is helpful in Mac file? | (2) |
| | (b) | With the help of neat diagrams explain about Mac OS 9 volumes. | (4) |

Module IV

| 17 | Explain about smartphone specific hardware options. | (6) |

OR

| 18 | How the forensics acquisition method in mobile differs from that in computer system? | (6) |

Module V

| 19 | Illustrate layout and presentation of reports. | (6) |

OR

| 20 | Address the difficulties that occurred while preparing an Expert Testimony. | (6) |

****