

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

- | | | | |
|---|---|----|-----|
| 11. List the different types of digital crimes. | 2 | K1 | CO1 |
| 12. Recall the legal and ethical aspects of cyber forensics. | 2 | K1 | CO1 |
| 13. Outline various challenges faced during evidence collection. | 2 | K2 | CO2 |
| 14. Define forensic copy and mention its uses. | 2 | K1 | CO2 |
| 15. Compare live acquisition and static acquisition methods. | 2 | K2 | CO3 |
| 16. Mention two challenges faced during data recovery from damaged devices. | 2 | K1 | CO3 |
| 17. Infer the role of EnCase in digital investigations. | 2 | K2 | CO4 |
| 18. Differentiate between data recovery and forensic analysis. | 2 | K2 | CO4 |
| 19. Show the technical limitations in collecting cloud-based evidence. | 2 | K2 | CO5 |
| 20. Encryption a major issue in mobile and cloud forensics. Justify your answer. | 2 | K2 | CO5 |
| 21. Outline the role of an expert witness in cyber-crime cases. | 2 | K2 | CO6 |
| 22. List the importance of clear and concise reporting during presentation of findings. | 2 | K1 | CO6 |

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

- | | | | |
|---|----|----|-----|
| 23. a) Apply the different steps involved in a cyber-crime investigation to trace the source of a phishing email attack on a bank's customers. | 11 | K3 | CO1 |
| OR | | | |
| b) Identify the Principles of digital evidence handling and justify how each principle maintains the integrity of evidence. | 11 | K3 | CO1 |
| 24. a) Analyze the various evidence collection techniques used and discuss how data is preserved in a corporate network. | 11 | K4 | CO2 |
| OR | | | |
| b) Discover a forensic chain of custody management suitable for cybercrime investigations. | 11 | K4 | CO2 |
| 25. a) Demonstrate how machine learning techniques can be applied to detect anomalies in Cyber forensic. | 11 | K4 | CO3 |
| OR | | | |
| b) Examine the different methods used for data recovery from damaged storage devices and discuss their limitations. | 11 | K4 | CO3 |
| 26. a) Make use of appropriate tool, extract deleted call logs and chat messages using mobile forensic techniques. | 11 | K3 | CO4 |
| OR | | | |
| b) Experiment the various forensic tools that can be applied in forensic data analysis to uncover hidden or encrypted information with an example. | 11 | K3 | CO4 |
| 27. a) Analyze the differences in evidence collection methods between mobile devices and cloud-based environments. | 11 | K4 | CO5 |
| OR | | | |
| b) Discover the forensic procedure for investigating data breaches in a cloud-based enterprise. | 11 | K4 | CO5 |
| 28. a) Examine how ethical considerations influence documentation and expert testimony in cyber forensics. | 11 | K4 | CO6 |
| OR | | | |
| b) Inspect how email metadata and keyword searches helped investigators identify fraudulent communication by analyzing real world cyber forensic cases. | 11 | K4 | CO6 |