1.What are events and incidents?
2.Explain Incident Response Policy in Details
3.Explain Preparation, Identification, Containment in Details.
4.Explain IRM reports with necessary information with any recent case study with root cause.
5.Discuss Goal of Incident Response Team.
6.Explain Terms with Example
    1.Viruses
    2.Spyware
    3.Adware
    4.Ransomware
    5.Keylogger
    6.Botnet
7.Explain Sign of Incident with Classification
8.Elaborate on any 2 computer security incidents. Suggest how to handle such incidents to avoid system failure?
9.What makes you an ideal candidate for a position of incident manager in a network related organization?
10.Consider a situation in a company where Confidentiality is more more important than integrity and availability.
11.Explain the steps involved in incident management. Use suitable Diagram.
12.Define incident prioritization. Give reasons why incident prioritization is important.
13. A technology-based company suggested data replication and virtualization as a disaster recovery solution. Justify your answer.
14.Consider a situation of physical security breach at a retail store. Calculate direct cost, indirect cost and total cost on this incident.
15.What are system internal tools? Discuss any 5 sys-tools in detail. Consider suitable data wherever applicable.
16.What are the roles and responsibilities of the incident response team? Elaborate in detail.
17.What is autopsy? How to install autopsy on windows-based system? How to recover files using this tool, to be produced in the court of Law?
18.What is a botnet? Give any 5 ways to identify botnets? Suggest a tool to identify and mitigate botnets in a given network.
19.What is the use of timeline analysis? How Gantt chart is different from a vertical timeline? Explain using a suitable diagram.
20.How to recognize, avoid and remove malwares? Discuss any malware removal tool.
21.What is quality assurance (QA) ? How QA is different from Quality control? Discuss Functional and Nonfunctional testing Methods.
22.Using suitable diagrams explain steps involved in the digital forensics process.
24.What are the steps required to acquire digital evidence? Explain using a suitable diagram.

25. How FTK Imager can help in producing the right evidence in the court of law? consider suitable data.
26. Draw and explain general architecture of windows 11 operating system.
27. What are the important artifacts related to user activities? How SIEM Tools analyze these artifacts?.
28. what is Digital Forensics and "Branches of Digital Forensics"
29. What is write blocker and its types?
30. Explain cost estimation?.