1905E720

Candidate's Seat No :_____

IMBA CSM Sem.-4 Examination

CSM_BBA_DSE - 1

FDF

Time : 2-30 Hours] May-2025 [Max. Marks : 70

Question 1 Answer the following questions:

i. Explain the evolution of computer forensics. How have the techniques and tools changed over time to address modern cybercrimes? Illustrate your answer with relevant milestones. 7Marks

ii. Discuss the various stages of the computer forensic process. Why is each stage critical to maintaining the integrity and admissibility of digital evidence in court? 7Marks

OR

i. What is forensic readiness? Explain its importance in an organizational context and describe how it enhances the effectiveness of a digital forensic investigation. 7Marks

ii. Describe the key phases in a computer crime investigation process. How does a forensic investigator assess the situation, acquire and analyze data, and prepare a final investigation report? 7Marks

Question 2 Answer the following questions:

i. Define digital evidence. What are the essential characteristics that make digital evidence admissible in court, and what challenges do forensic experts face in preserving its integrity? 7Marks

ii. What is the role of the first responder in a digital forensic investigation? Describe the essential components of a first responder toolkit and the procedures to be followed at a digital crime scene. 7Marks

OR

i. Explain the internal structure of a Hard Disk Drive (HDD). How does understanding the booting process help forensic investigators in analyzing compromised systems? 7Marks

ii. Discuss the concept of a file system. Compare common file systems such as FAT32, NTFS, and ext4, and explain how knowledge of file systems aids in digital forensic investigations. 7Marks

Question 3 Answer the following questions:

i. What is file carving? Describe how it is used to retrieve deleted data from slack space, unallocated space, and swap space in Windows-based systems. 7Marks

ii. Discuss the role of Windows event logs in forensic investigations. What types of information can be retrieved from these logs, and how can they assist in reconstructing a digital incident? 7Marks

OR

i. Explain the need for Windows forensics in modern digital investigations. What are the major forensic areas specific to the Windows operating system? 7Marks

ii. Differentiate between volatile and non-volatile information in Windows forensics. Provide examples of each and describe their significance in an investigation. 7Marks

E720-2

Questions 4 Answer the following questions:

i. Explain the forensic significance of network components such as routers, switches, hubs, and network interface cards (NICs). How do these components contribute to a network forensic investigation? 7Marks

ii. Describe the types of forensic information that can be extracted from various layers of the OSI and TCP/IP models. How does log analysis help in detecting and investigating network-based attacks? 7Marks

OR

i. What are the major challenges faced in mobile forensics? Discuss how mobile communication architecture and encryption impact evidence extraction. 7Marks

ii. Outline the mobile forensic process from evidence identification to report generation. Compare at least two forensic acquisition tools used in mobile device investigations. 7Marks

Questions 5: Attempt any Seven out of Twelve. 14 Marks

1. Computer forensics is the process of collecting, analysing, and preserving _____ evidence in a way that is legally admissible.
   A) historical B) financial C) digital D) biological
2. The main objective of computer forensics is to identify, preserve, recover, analyze, and present _____ evidence.
   A) oral B) tangible C) digital D) documentary
3. The final step in the computer forensics investigation process is to _____ the findings in a legally acceptable format.
4. _____ readiness refers to an organization's ability to maximize its capability to use digital evidence while minimizing the cost of an investigation.
5. _____ evidence is any data that can be used to support or refute a hypothesis in a legal context and is stored or transmitted in binary form.
6. A _____ is the person who first arrives at a digital crime scene and is responsible for securing and collecting potential evidence.
7. The _____ is responsible for loading the operating system into memory during the computer's startup process.
8. A _____ system manages how data is stored and retrieved on a storage device such as a hard drive.
9. _____ information refers to data stored in RAM, active processes, and network connections that are lost when the system is powered off.
10. In Windows systems, _____ logs are records that contain information about system events, application errors, and security-related activities.
    A) firewall B) DNS C) event D) kernel
11. _____ space refers to the unused space in a disk cluster that may still contain residual data from previously deleted files.
12. In mobile forensics, _____ acquisition is the process of extracting a complete bit-by-bit copy of data from a mobile device without modifying the original.