Y/K/TY

Reg. No: 22BCS0189

Final Assessment Test – November 2025

VIT Vellore Institute of Technology

Course: BCSE322L - Digital Forensics

Class NBR(s): 1474/1478

Slot: D1

Time: Three Hours

Max. Marks: 100

- KEEPING MOBILE PHONE/ANY ELECTRONIC GADGETS, EVEN IN 'OFF' POSITION IS TREATED AS EXAM MALPRACTICE
- DON'T WRITE ANYTHING ON THE QUESTION PAPER

COs	CO Statements
CO1	Understand the responsibilities and liabilities of a computer forensic investigator.
CO2	Seize a computer from a crime scene without damage and follow the legal procedures and standards.
CO3	Demonstrate the ability to perform forensic data acquisition and analysis.
CO4	Analyze and retrieve hidden and damaged files from different operating systems.
CO5	Apply forensics to recent technologies such as smart phones, email, cloud and social media.

BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)

Answer ALL Questions

(10 X 10 = 100 Marks)

1. As a digital forensic investigator in a hospital having 1000 beds, you have been assigned to prepare for an internal investigation involving an employee suspected of exfiltrating confidential patient data. Describe in detail the essential preparatory steps you would take before conducting the forensic investigation. Your answer should include procedures for evidence identification, collection, preservation, documentation, and ensuring compliance with legal and organizational policies. Support your answer with the case example where poor preparation led to the collected digital evidence being ruled inadmissible in court, explaining what went wrong and how it could have been avoided. CO1 BL1

2. As a digital forensic investigator, you are expected to uphold the highest standards of ethics and professionalism during all stages of an investigation. Also, Explain the key ethical and professional responsibilities that guide your conduct in digital forensics, including adherence to objectivity, confidentiality, integrity, and impartiality. Support your discussion with your own case study illustrating how the failure to maintain professional conduct such as bias, data leakage, or evidence tampering. CO1 BL2

3. Investigating cybercrimes demands a structured and methodical approach to ensure the credibility, accuracy, and admissibility of digital evidence. Between May and July 2017, American credit bureau Equifax was breached. Hackers exploited a web application vulnerability and compromised sensitive personal and financial data of over 147.9 million Americans along with 15.2 million British citizens and about 19,000 Canadian citizens. Exemplify the key stages of a systematic digital forensic investigation, from incident identification to the final reporting. CO2 BL5

4.	In modern criminal investigations, especially in homicide cases, digital evidence such as data from smartphones, CCTV systems, cloud storage, and digital devices plays a crucial role in uncovering timelines, communications, and motives. Explain the significance of understanding various the digital storage formats during the collection and forensic analysis of such evidence. Support your discussion with your own case study demonstrating how improper handling or misinterpretation of storage formats will compromise the integrity or admissibility of digital evidence in a murder investigation.	CO2	BL4
5.	A large healthcare organization, MedSecure Hospital, suffered a ransomware attack that encrypted several patient record servers and critical diagnostic systems. During the digital forensic investigation, the team realized they lacked a well-defined contingency plan for acquiring forensic images from compromised and encrypted systems. As a digital forensic expert, describe the essential components of an effective contingency plan for forensic image acquisition in such an incident. Also, explain the significance of validation and verification procedures.	CO3	BL2
6.	During a corporate fraud investigation at a multinational accounting firm, forensic investigators discovered that the company's financial databases were stored on a RAID-configured server. However, the system had partially failed, complicating data recovery and evidence acquisition. As a digital forensic examiner, illustrate the different RAID levels (RAID 0, 1, 5, and 10), comparing their approaches to data redundancy and performance enhancement, and discuss the technical challenges investigators face when recovering and analyzing evidence from damaged or complex RAID arrays.	CO3	BL1
7.	During an internal investigation into unauthorized file access at a government research laboratory, forensic analysts suspect that a Windows workstation was used to copy confidential project data onto an external USB drive. Discuss the importance of the Windows Registry in uncovering digital evidence in this scenario. Explain the structure of the Windows Registry, including its main hives and key hierarchies, and describe how investigators can analyze Registry artifacts to trace user activities, connected devices, and system configurations.	CO4	BL3
8.	As a digital forensic expert, discuss the significance of file systems in understanding the data organization within an operating system. Explain the main types of file systems such as NTFS, FAT32, exFAT, and HFS+ that are commonly encountered in the forensic investigations highlighting their structures, features, and limitations. Also, describe how the forensic investigators examine these file systems to recover deleted or hidden data and reconstruct the user activity timelines.	CO4	BL4
9.a)	Illustrate the stages of the Unix/Linux boot process, detailing the role of key components such as the BIOS/UEFI, bootloader, kernel, and the init/systemd process. Also, explain how a thorough understanding of the Linux boot sequence helps investigators detect startup-level compromises, analyze malicious persistence mechanisms, and reconstruct system activity during a security incident.	CO5	BL5

OR

9.b) In 2023, law enforcement agencies investigated a coordinated online harassment and cyberbullying campaign targeting a public official across multiple social media platforms including X (Twitter), Instagram, and Telegram. The attackers used fake profiles, direct messages, and manipulated images to spread false information and threats. As a digital forensic analyst, discuss the importance of social media forensics in uncovering digital evidence during such investigations. Explain the key forensic techniques involved in data collection, preservation, and analysis of posts, chats, and multimedia content. Also, explicate how these techniques help the investigators trace the anonymous accounts, establish timelines of communication, and gather admissible evidence of criminal activities. **CO5 BL5**

10.a) In 2024, a corporate espionage investigation uncovered that an employee was allegedly using a company-issued smartphone to leak confidential design documents and internal communications to a competitor through encrypted messaging apps. As a digital forensic investigator, describe the key steps involved in the acquisition process for mobile devices, emphasizing both logical and physical acquisition methods. Explain the importance of proper handling and preservation techniques to ensure evidence integrity and prevent data loss or tampering. Also, discuss the challenges investigators may face during mobile device acquisition. **CO5 BL6**

OR

10.b) In 2023, a major healthcare technology company experienced a data breach after attackers exploited exposed API keys in a developer's cloud-based storage account. The hackers gained unauthorized access to patient records hosted on Microsoft Azure, compromising sensitive personal and medical data of over 4 million users. This incident raised critical concerns about cloud forensics, data protection, and regulatory compliance in healthcare environments. As a digital forensic investigator, explain the key components and significance of cloud forensics in modern digital investigations. Discuss the major challenges involved in cloud forensic analysis. Also, describe the methodologies and best practices used in cloud forensic investigations. **CO5 BL6**

⇔⇔⇔ Y/K/TY ⇔⇔⇔