REG.NO.: 22BC3019

SLOT: D1

VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - I
FALL SEMESTER 2025-2026

Programme Name & Branch	: B.Tech. CSE
Course Code and Course Name	: BCSE322L and Digital Forensics
Faculty Name(s)	: Dr. Aju D, Dr. Madiajagan M
Class Number(s)	: VL2025260101478, VL2025260101474
Date of Examination	: 20 Aug 2025
Exam Duration	: 90 minutes **Maximum Marks: 50**

General instruction(s):

- Answer All Questions
- M - Max mark; CO – Course Outcome; BL – Blooms Taxonomy Level (1 – Remember, 2 – Understand, 3 – Apply, 4 – Analyse, 5 – Evaluate, 6 – Create)
- Course Outcomes: (Type the CO statements covered in this question paper. Use the CO number as per the syllabus copy)

1. Understand the responsibilities and liabilities of a computer forensic investigator
2. Seize a computer from a crime scene without damage and follow the legal procedures and standards.
3. Demonstrate the ability to perform forensic data acquisition and analysis.

Q. No	Question	M	CO	BL
1.	Twitter is in the spotlight after a controversy erupted involving a fake corporate account. A 19-year-old commerce student named Ravi allegedly created a counterfeit Twitter profile impersonating the customer support handle of a popular online shopping company. Through this fake account, Ravi responded to genuine customer complaints, sharing fraudulent payment links and collecting personal data from unsuspecting users. Several victims reported financial losses and data breaches. After multiple complaints, the company's legal team approached the cybercrime cell. The account was found to have been active for only three weeks but had already engaged with over 200 customers. Following the investigation request, Ravi was traced and detained. As a forensic investigator, describe the standard procedure you would adopt to investigate this case and ensure the findings are admissible in the court to help solve the case.	10	1	2
2.	A well-known city hospital reported to the cybercrime cell that its patient record management system had been encrypted by ransomware. Hackers had infiltrated the network through a phishing email sent to hospital staff. The attackers demanded payment in cryptocurrency in exchange for the decryption key. The hospital's IT team confirmed that several servers and workstations were compromised, and patient data backups were suspected to be tampered with. a) Devise a complete forensic investigation plan for the above ransomware incident. Explain how you would analyze and interpret the digital evidence	5	2	4

VIT
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

REG.NO.:

SLOT: D1

SCHOOL OF COMPUTER SCIENCE AND ENGINEERING
CONTINUOUS ASSESSMENT TEST - I
FALL SEMESTER 2025-2026

	collected in order to identify the attacker and determine whether the accused can be acquitted or convicted.			
	b) By referring to the above mentioned case, compile and consolidate all the digital evidence you would gather during the investigation. Justify the forensic methodology and tools you would use for evidence acquisition, preservation, analysis, and interpretation in this case.	5		
3.	A government healthcare agency has reported that sensitive patient records from its central database were illicitly accessed and copied to unknown external storage devices. The breach is suspected to involve both external hacking attempts and possible insider involvement. a) As the lead forensic examiner assigned to this case, describe the incident and discuss the different file formats for storing collected digital evidence. For each format, explain its characteristics, advantages, and disadvantages in the context of this case. Also, create a formal chain of custody to track every stage of evidence handling.	5	3	4
	b) By referring to the above mentioned case, outline the contingency strategies that you would adopt to ensure evidence acquisition from diverse devices such as database servers, employee workstations, and removable media in situations where systems may be damaged, encrypted, or remotely wiped.	5		
4.	A digital film production studio handles high-resolution 4K and 8K video projects that require real-time playback, fast rendering, and secure storage. To avoid issues like frame drops or playback lag, the studio is exploring redundant storage solutions that can deliver both high throughput and fault tolerance. As a storage systems consultant, explain the architecture, working principle, merits, and demerits of the following RAID levels. a) RAID 5 b) RAID 1+0 c) RAID 6 Also, based on the studio's need for large data throughput, real-time performance, and redundancy, recommend the most suitable RAID configuration. Provide clear technical justification for your choice.	10	3	
5.	Illustrate the comprehensive procedure for collecting digital evidence at a cybercrime scene with a relevant example. As a forensic investigator, explain the methods you would employ to securely preserve the acquired data and the steps you would take to verify its integrity and authenticity throughout the investigation.	10	3	

****