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 - II
FALL SEMESTER 2025-2026

Programme Name & Branch	: B. Tech (IS)
Course Code and Course Name	: BCSE322L Digital Forensic
Faculty Name(s)	: Dr. M. Madiajagan and Dr. Aju
Class Number(s)	: VL2025260101477 & VL2025260101478
Date of Examination	: 08-10-2025
Exam Duration	: 90 minutes

Maximum Marks: 50

General instruction(s):

- Answer All Questions and Materials allowed as per the Dean Academic guidelines.
- Course Outcomes:
  a. CO3- Demonstrate the ability to perform forensic data acquisition and analysis.
  b. CO4-Analyze and retrieve hidden and damaged files from different operating systems.
  c. CO5- Apply forensics to recent technologies such as smart phones, email, cloud and social media.

Q. No	Question	M	CO	BL
1.	A mid-level manager at a financial services company is suspected of leaking confidential client data to a competitor. The company's IT security team discovered suspicious USB activity and unusual login times on the suspect's windows workstation. The case was handed over to the Digital Forensic team for analysis and they started analysing the systems of the manager, network & internet activities, external devices and registry analysis. Demonstrate the digital forensic investigator analysing methodologies applied to investigate the above problem statement and give the detailed report as a solution for the above scenario.	10	3	3
2.	A software company suspects that an insider has modified the Linux server configurations to create a secret backdoor for remote access. The system administrator noticed unusual outbound SSH traffic and suspected unauthorized modifications in system-level configuration files. The problem has been handed over to the company's digital forensic investigating team with the complete supporting privileges, roles and rights to access the Linux server. Illustrate the methodologies adapted by the investigating team and what are the recommendations & findings submitted.	10	3	3

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 - II
FALL SEMESTER 2025-2026

3.	Demonstrate the comprehensive structure of the NTFS file system, why Master File Table is important in digital forensic investigations. A company suspects that an employee hid confidential data in NTFS without creating a visible file. As a computer forensic expert, how would you investigate the employee's suspicious activities and give the steps carried out by the expert?	10	4	4
4.	A senior project manager in a multinational software company reported that her corporate email account was compromised. She received alerts of suspicious login attempts from foreign IP addresses. Later, unauthorized emails were sent to clients requesting confidential project files. Illustrate the detailed email forensic investigation procedure, how the attackers gained users login access, bypassed password protection and your explanation should reveal the techniques used by the hacker to perform the above-mentioned malicious activity without the knowledge of the end-user.	10	5	2
5.	A 16-year-old student reports receiving threatening and abusive messages on Instagram and Twitter from accounts using fake names and profile pictures. The accounts frequently delete posts, use VPNs, and change usernames to avoid detection. The victim's parents file a complaint, and the case is handed over to the Digital Forensics Unit for investigation. Elucidate the social media digital forensic investigation analysis performed by the digital forensic experts?	10	5	3

****