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

SCHOOL OF COMPUTER SCIENCE & ENGINEETING
CONTINUOUS ASSESSMENT TEST - I
WINTER SEMESTER 2024-2025

Programme Name & Branch	: B.Tech & CSE
Course Code and Course Name	: BCSE322L and Digital Forensics
Faculty Name(s)	: Dr. Aju D
Class Number(s)	: VL2024250501658
Date of Examination	: 31 Jan 2025
Exam Duration	: 90 minutes

SLOT: E2

Maximum Marks: 50

Q. No	Question (Answer ALL Questions)	M	CO	BL
1.	As a forensic investigator, exemplify the systematic approach that can be adopted for the below given criminal case. Detail the steps taken to gather, preserve, and analyze evidence, ensuring accuracy and integrity throughout the process. Dennis Rader, a serial killer tortured and killed at least ten people while he was still at loose and undiscovered. He did taunt the police forces by sending them cryptic messages during his killing sprees, baffling them even more. However, it was this very habit that finally led to his arrest. In 2005, Rader sent the police a Microsoft Word document on a floppy disk. Digital forensics experts were able to trace the metadata contained within the disk, helping unveil the serial killer's true identity. Rader was finally arrested and imprisoned shortly after this.	10	1	2
2.	An IT organization recently discovered that their computer systems were compromised, resulting in slow system performance, unexpected pop-ups, and the continuous sending of spam emails from their network. After a detailed internal investigation, it was concluded that the company's systems had been hijacked and incorporated into a botnet controlled by remote hackers. The attackers used the botnet to send spam emails and launch attacks on other systems. The company filed a complaint, seeking a forensic investigation to determine the extent of the compromise and identify the perpetrators. Explain the comprehensive plan for investigating the filed complaint mentioned above. How would you analyze and interpret the digital evidence collected to determine whether the accused should be acquitted or convicted? Also, justify the plan used for analyzing and interpreting this evidence.	10	2	4
3.	Discuss a cyber case you are familiar with and explain the various file formats used for storing the collected data. As a forensic expert, outline the contingency plans you would implement for acquiring the digital data from different devices. Additionally, describe how you would maintain a chain of custody form to ensure the integrity of the evidence.	10	3	4
4.	Discuss the various RAID systems that can be implemented in an CMM-5 organization. For each RAID level, explain its structure, benefits, and limitations. Evaluate the factors that the organization should consider when selecting a RAID configuration, and recommend the most suitable RAID	10	3	1

SCHOOL OF COMPUTER SCIENCE & ENGINEETING
CONTINUOUS ASSESSMENT TEST - I
WINTER SEMESTER 2024-2025

	system for the said enterprise with both high availability and performance requirements.			
5.	Describe in detail the process involved in acquiring data from a crime scene, using a relevant example. Also, explain the measures you would take to safeguard the acquired data and ensure its validation as a forensic investigator.	10	3	5

****