Name:

Enrolment No:

UPES

End Semester Examination, May 2025

Course: Digital Forensics **Semester : 2**
Program: MTech_CSE/MCA **Time : 03 hrs.**
Course Code: CSCS7017 **Max. Marks: 100**

SECTION A (All questions are compulsory)

S.No		Marks	CO
Q 1	Analyze the methods used in mobile device forensics to investigate encrypted messaging apps such as WhatsApp.	4	CO1
Q 2	Demonstrate how the Volatility tool can be applied to extract encryption keys from a memory dump.	4	CO2
Q 3	Describe the significance of maintaining a proper chain of custody in digital forensic investigations.	4	CO3
Q 4	Evaluate the importance of timely memory acquisition and assess how improper procedures can compromise forensic integrity.	4	CO4
Q 5	Justify how digital signatures or hash values uphold the integrity of the chain of custody in forensic investigations.	4	CO5

SECTION B

Q 6	Describe the six phases of the Incident Response Lifecycle. Explain the importance of maintaining documentation during each phase and how it contributes to the overall effectiveness of incident response.	4+3+3	CO4
Q 7	Differentiate between digital evidence and physical evidence in the context of a cybercrime investigation. Analyze each type by providing relevant examples and explaining their significance in legal proceedings.	4+3+3	CO4
Q 8	Explain how investigators apply IP address tracking and log analysis to trace cybercriminals. Analyze the strengths and limitations of using these methods in real-world scenarios.	4+3+3	CO4
Q 9	Compare and contrast containment strategies used during incidents involving ransomware and data exfiltration. Evaluate the effectiveness of each approach in minimizing damage and preserving evidence. OR Evaluate the role of collaboration among law enforcement agencies, ISPs, and cybersecurity professionals in addressing cross-border cybercrime. Propose a collaborative strategy by referring to a real-world example where such efforts led to a successful outcome.	10	CO5

SECTION-C

Q 10	A mobile device and a laptop are seized during a digital forensic investigation. On the laptop, a deleted WhatsApp backup file is recovered. However, the mobile device shows no active traces of WhatsApp being installed or used.	10+10	CO5

	a) Analyze how a forensic analyst could apply cross-device correlation techniques to infer possible user activity related to WhatsApp. b) Evaluate which types of timestamps and metadata would be most critical to support or refute the findings of this correlation.		
Q 11	A suspect is believed to have used anti-forensic tools to cover their tracks. (a) Describe the common types of anti-forensic techniques used to hinder digital investigations. (b) Analyze how a forensic investigator can detect traces of anti-forensic actions (c) Evaluate how detection methods may vary between NTFS and ext4 file systems, using specific examples. OR A forensic examiner suspects that a suspect has used volume hiding techniques, such as hidden partitions or encrypted containers, to conceal data. a) Describe the concept of volume hiding in digital forensics, including common techniques such as hidden partitions and encrypted containers. b) Demonstrate how forensic tools can be used to examine logical volumes for signs of hidden or encrypted data. c) Analyze a given disk image to identify indicators of hidden or encrypted volumes that are not listed in the partition table or mounted. d) Evaluate the effectiveness of different forensic tools and techniques in detecting concealed volumes during a forensic investigation. e) Design a step-by-step forensic methodology for detecting and analyzing potentially hidden or encrypted volumes within a suspect storage device.	8+6+6 OR 4+4+4+4+4	CO5