


Name:			
Enrolment No:			
UPES End Semester Examination, December 2023			
Course: Digital Forensics I Program: B.Tech (CSE-H+NH)-CSF Course Code: CSSF3003		Semester: V Time : 03 hrs. Max. Marks: 100	
Instructions: All questions are COMPULSORY. Internal choice available in Q9 and Q11.			
SECTION A (5Qx4M=20Marks)			
S. No.		Marks	CO
Q 1	What is RAM analysis in digital forensics, and why is it a valuable source of information in investigations? Provide an example of how RAM analysis can assist in a case.	04	CO1
Q 2	You are tasked with a complex case involving a corporate espionage investigation. The suspect is believed to have stolen highly confidential data. Describe the step-by-step process you would follow in a computer forensics investigation to gather evidence against the suspect. Provide detailed actions you would take and explain their significance.	04	CO2
Q 3	You are a computer forensic examiner and want to determine whether a user has opened or double-clicked a file. What folder would you look in for a windows operating system artefact for this user activity? Support your answer with valid explanation.	04	CO2
Q 4	What is Windows Sysinternals? Explain TWO tools with their functionality that is present in Sysinternals.	04	CO3
Q 5	You have received a computer forensics case involving a cyberattack on a financial institution. The suspects are sophisticated hackers who have employed encryption and steganography to hide their activities. Explain the techniques you would use to identify and decode hidden data in this scenario.	04	CO4
SECTION B (4Qx10M= 40 Marks)			
Q 6	In a case involving a cyberattack on a critical infrastructure facility, you have been called to conduct network forensics. Discuss the steps you would take to track the network traffic, identify the attack vectors, and trace the origins of the attack. Include the use of network logs and other relevant tools.	10	CO3
Q 7	a. In a corporate environment, you are tasked with investigating an employee's computer for potential intellectual property theft. Outline the	10	CO5

	<p>steps you would follow to perform a sound forensic examination while maintaining the employee's privacy. [05]</p> <p>b. Discuss the challenges and potential legal issues associated with employee computer investigations, particularly in terms of privacy and consent. [05]</p>		
Q 8	Describe TWO forensic tools which are used for creating forensics image of evidence. Also name three formats in which data is acquired. Explain how validating and analysis of digital evidence is done.	10	CO1
Q 9	<p>Discuss the legal aspects of Online Obscenity & Pornography according to Indian Cyber Laws?</p> <p style="text-align: center;">OR</p> <p>Discuss the legal aspects of Cyber Stalking and Defamation according to Indian Cyber Laws?</p>	10	CO2
<p>SECTION-C (2Qx20M=40 Marks)</p>			
Q 10	<p>Differentiate between the following: [5*4]</p> <p>a) Logical Acquisition v/s Physical Acquisition</p> <p>b) IMAP v/s POP3</p> <p>c) Volatile v/s Non-Volatile evidence</p> <p>d) Static IP v/s Dynamic IP</p> <p>e) Data Integrity v/s Data Authenticity</p>	20	CO3
Q 11	<p>State the term 'Messenger Forensics'? How it is useful in forensics investigations. Explain the working structure of Yahoo Messenger.</p> <p style="text-align: center;">OR</p> <p>State the term 'Web Browser Forensics'? What is the role of index.dat in forensics investigation? Explain about some tools used in Web Browser Forensics.</p>	20	CO4