


Name:			
Enrolment No:			
UPES End Semester Examination, May 2024			
Course: Digital Forensics II Program: BTech LLB(Cyber Law) Course Code: CSSF4004_2		Semester: XII Time : 03 hrs. Max. Marks: 100	
Instructions:			
SECTION A (5Qx2M=10Marks)			
S. No.		Marks	CO
Q 1	Compare cybercrime with traditional crime.	2	CO3
Q2	Explain the role of white hat hackers.	2	CO2
Q3	Define live memory acquisition in memory forensics.	2	CO3
Q4	Describe the challenges faced by digital forensic investigators.	2	CO1
Q5	Identify any two symptoms of rootkit infection.	2	CO4
SECTION B (4Qx5M= 20 Marks)			
Q 6	Describe how rootkits support cyber criminals.	5	CO4
Q7	Construct an appropriate procedure for securing crime scenes and computer incidents.	5	CO3
Q8	Illustrate what justifies the seizure of digital evidence for crime scene analysis.	5	CO3
Q9	Outline the crucial steps involved in memory forensics.	5	CO2
SECTION-C (2Qx10M=20 Marks)			
Q 10	Defend how digital forensics assists in the identification of the criminal and why digital forensics has become essential for present-day crime investigations.	10	CO4
Q11	Analyze the procedure for obtaining volatile data from a Windows computer.	10	CO3

SECTION-D
(2Qx25M=50 Marks)

Q12	Explain the following terms: a) Steganography b) Malware c) Mobile forensics d) Advanced tracker hacker e) Memory Acquisition	25	CO3
Q 13	Case Study: A few months back, there was a situation where a student utilized a campus computer lab to access her Google account. Before leaving the lab, she made sure her Google account was closed in the browser window. She was followed in by someone else who accessed her account again using the same browser. They used it to send emails, which led to all kinds of problems. Point out the necessary actions you must take as if you were a forensic specialist.	25	CO4