


Name: Enrolment No:			
UPES End Semester Examination, May 2025			
Course: Advanced Digital Forensics Program: M. Tech. Course Code: CSCS7015		Semester: 2 Time : 03 hrs. Max. Marks: 100	
Instructions: Attempt all questions. Assume any missing data and take assumptions of relevant scenarios, draw diagrams wherever applicable along with appropriate examples. Answer as per the marking weightage of the questions. Any type of calculating/smart device is not permitted.			
SECTION A (5Q X 4M = 20Marks)			
S. No.		Marks	CO
Q 1	Define Digital Forensics.	4	CO1
Q 2	How can you identify the malicious software?	4	CO2
Q 3	Illustrate Amateurs in cyber forensics	4	CO3
Q 4	Write a short note on FTK.	4	CO4
Q 5	Explain the purpose of collection of RAM Dump at Scene of Crime.	4	CO5
SECTION B (4Q X 10M= 40 Marks)			
Q 6	Discuss the significance of volatile and non-volatile memory for cyber-forensics expert.	10	CO1
Q 7	Illustrate the methodology you may adopt for the <i>Chain of Custody</i> during your forensic investigation.	10	CO2
Q 8	You as a Security Analyst observed some malicious activity in the organization's system. How will you manage the incident response and report for that. Show a template of the compiled report for any of the assumed incident.	10	CO3
Q 9(a)	Evaluate the effectiveness of different cybersecurity measures in preventing cyberattacks, such as firewalls, encryption, multi-factor authentication, and intrusion detection systems. Which of these measures is most critical for protecting sensitive data, and why?	10	CO4

	OR		
Q9(b)	Explain the challenges in Cloud Forensics (TOR and Proxy). Suggest a solution to overcome them.	10	CO4
SECTION-C (2Q X 20M = 40 Marks)			
Q 10	<p>Design and demonstrate your own designed network for an organization like “Virus Research and Diagnostic Laboratories”.</p> <p>Now assume an intruder is trying a DOS attack in that organization’s network.</p> <p>Your motive is to block the intruder who is sending unwarranted requests through a vulnerable device. You first identify the incident and respond accordingly as an emergency response. What Information security life cycle steps will you take.</p> <p>Elaborate and discuss the standard procedures and analysis to make the organization secure from cyber attackers.</p>	20	CO5
Q11(a)	<p>You have been designated as a Cyber Forensics Analyst and Cyber Security Consultant for the Government of Uttarakhand. Your responsibility is to design and propose a robust cybersecurity and information protection strategy for the Uttarakhand State Data Centre.</p> <p>In your proposal, students are expected to:</p> <ul style="list-style-type: none"> • Develop diagrams to demonstrate the architecture and structure of the proposed cybersecurity setup. • Provide relevant examples of tools, technologies, and techniques that will be used during the implementation phase. • Justify how your proposed plan will bolster the security of the State Data Centre. <p>The solution should focus on key aspects but not limited to:</p> <ul style="list-style-type: none"> • Forensic tools, analysis procedures, and methodologies • Security measures for server operating systems, ports, and firewalls • Network architecture, VPNs, and VLANs • Compliance with relevant IT Acts and regulations. <p>Finally, the proposal should conclude with a detailed explanation of how the implementation of your plan will make the Uttarakhand State Data Centre more secure and resilient against cyber threats.</p>	20	CO5

	OR		
Q11(b)	<p>Governments, businesses, and individual users are increasingly becoming the targets of cyberattacks, and experts predict that the frequency of these attacks will likely rise in the future. Cybersecurity education has become a top international priority as high-profile incidents highlight the potential threat that such attacks pose to the global economy. According to the Center for Strategic and International Studies, cybercrime costs the global economy over \$600 billion annually.</p> <p>Some of the most notable cyberattacks include:</p> <ul style="list-style-type: none"> • Colonial Pipeline Ransomware Attack • Code Red Worm • United Nations Data Breach <p>Select any one of the high-profile cyberattacks listed above and provide a detailed analysis of the attack. Your response should address the following questions:</p> <ul style="list-style-type: none"> • Description of the Attack: Provide a comprehensive overview of how the attack occurred, including key details about the timeline and impact. • Methodology and Tools Used: Discuss the techniques, tools, or vulnerabilities exploited during the attack. • Response and Mitigation: Explain how the targeted organization responded to the attack and what measures were taken to mitigate the damage. • Lessons Learned: Highlight the key takeaways from the incident, especially in terms of improving cybersecurity practices. • Future Preventive Measures: Suggest steps that could have been taken, or can be taken in the future, to prevent similar attacks. 	20	CO5