


Name:			
Enrolment No:			
<b>UNIVERSITY OF PETROLEUM AND ENERGY STUDIES</b> <b>End Semester Examination, December 2022</b>			
Course: Cyber Forensic Procedures and Analysis		Semester: 3	
Program: MCA		Time : 03 hrs.	
Course Code: CSCS8001		Max. Marks: 100	
<b>Instructions: Instructions: Attempt all questions. Assume any missing data, draw diagrams wherever applicable, provide appropriate examples</b>			
<b>SECTION A</b> <b>(5Q X 4M = 20Marks)</b>			
S. No.		Marks	CO
Q 1	Write a short note on Autopsy.	4	CO1
Q 2	What do you understand by Watermarking	4	CO1
Q 3	Explain the purpose of memory forensics.	4	CO2
Q 4	Write a short note on Ransomware.	4	CO2
Q 5	What is a primary responsibility of a Cyber Forensics investigator?	4	CO3
<b>SECTION B</b> <b>(4Q X 10M = 40 Marks)</b>			
Q 6	Discuss why the understanding of Watermarking is very important for cyber forensic procedures and analysis.	10	CO1
Q 7	Describe the steps of Digital Forensics: Identification, Preservation, Analysis, Documentation and Presentation, Chain of Custody.	10	CO2
Q 8	Illustrate the significance of network logs in forensics.	10	CO3
Q 9	Elaborate and discuss the standard procedures and analysis to make the organization secure from cyber attackers.	10	CO4
<b>OR</b>			
	Explain the challenges in Network and Cloud Forensics (TOR and Proxy)		
<b>SECTION-C</b> <b>(2Q X 20M = 40 Marks)</b>			
Q 10	The data centre has been attacked by some unidentified ransomware. The servers in data centre are in critical attack. Propose a plan so that we can	20	CO4

	<p>avoid these types of cyberattacks make them secure for future such cyber vulnerabilities.</p> <p>Hint [Antimalware protection, Host-based malware protection, network based malware protection, firewall, network security etc.]</p>		
Q 11	<p>You as a Cyber Forensics and Security Consultant for Uttarakhand Government deputed to propose a cyber-security and information safety plan for Uttarakhand State Data Centre.</p> <p>Students are supposed to draw diagrams, give examples, and provide tools and technologies involved during the setup.</p> <p>The answer should be concluded with the justification that how State Data Centre will become more secure after implementing your proposed plan.</p> <p>[Hint: Forensic tools, procedures and analysis, focus on Servers OS/Ports/Firewalls and then on Network setup/VPN/VLAN, IT Acts etc.]</p>	20	CO5
	<b>OR</b>		
	<p>Governments, businesses, and individual users are increasingly the targets of cyberattacks and experts predict that these attacks are likely to increase in the future. Cybersecurity education is a top international priority as high-profile cyber-security related incidents raise the fear that attacks could threaten the global economy. The Center for Strategic and International Studies estimates that the cost of cybercrime to the global economy is more than \$600 billion annually.</p> <p>Some of the famous attacks are:</p> <ul style="list-style-type: none"> <li>o Colonial Pipeline ransomware attack</li> <li>o The Marriott data breach</li> <li>o United Nations data breach</li> <li>o Microsoft customer support database breach</li> <li>o Stuxnet Virus</li> </ul> <p>Select any two of the high-profile cyberattacks from above and discuss the analysis of the attack and answers to the questions below.</p> <ol style="list-style-type: none"> <li>1. Who were the victims of the attacks?</li> <li>2. What technologies and tools were used in the attack?</li> <li>3. What Systems were targeted?</li> </ol> <p>What was the outcome of the attack? (stolen data, ransom, system damage, etc.)</p>		