


Name: Enrolment No:	
--------------------------------------	--

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2023

Course: Cyber Forensic Procedures and Analysis
Program: MCA
Course Code: CSCS8001

Semester: 3
Time : 03 hrs.
Max. Marks: 100

Instructions: Instructions: Attempt all questions. Assume any missing data, draw diagrams wherever applicable, provide appropriate examples

SECTION A
(5Q X 4M = 20Marks)

S. No.	Question	Marks	CO
Q 1	Write a short note on FTK.	4	CO1
Q 2	What do you understand by incident handling and response?	4	CO1
Q 3	Explain the purpose of collection of RAM Dump at Scene of Crime.	4	CO2
Q 4	Write a short note on Wireshark.	4	CO2
Q 5	Describe social media forensics?	4	CO3

SECTION B
(4Q X 10M = 40 Marks)

Q 6	What is the significance of volatile and non-volatile memory for a cyber-forensics expert? Briefly explain the order of volatility.	10	CO1
Q 7	Explain in details the various steps of Digital Forensics: Identification, Preservation, Analysis, Documentation and Presentation, Chain of Custody.	10	CO2
Q 8	How will you perform steganography on a media file and analyze the file. Write a report for the same.	10	CO3
Q 9	You have been assigned a task to establish the standard hard drive imaging tool and procedure for your organization. What considerations and steps will you take to create those standards?	10	CO4

OR

	Explain the challenges in Network and Cloud Forensics (TOR and Proxy)		
--	---	--	--

SECTION-C
(2Q X 20M = 40 Marks)

Q 10	<p>Design and demonstrate network of your own. Now assume an intruder is trying a DOS attack in that network. Your motive is to block the intruder who is sending unwarranted requests through a vulnerable device. Justify your actions in a report.</p> <p>Elaborate and discuss the standard procedures and analysis to make the organization secure from cyber attackers.</p>	20	CO4
Q 11	<p>You have been deputed as a Cyber Forensics Analyst and cyber security Consultant for Uttarakhand Government to design and 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. The answer should be concluded with the justification that how State Data Centre will become more secure after implementing your proposed plan. [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
OR			
	<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. Some of the famous attacks are:</p> <ul style="list-style-type: none"> o Colonial Pipeline ransomware attack o Code Red Worm o United Nations data breach o Microsoft customer support database breach o Stuxnet Virus <p>Select any one 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">1. Who were the victims of the attacks?2. What technologies and tools were used in the attack?3. What Systems were targeted? <p>What was the outcome of the attack? (stolen data, ransom, system damage, etc.)</p>		
--	--	--	--