UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2022

Course: Forensic Computing   **Semester: II**
Program: M. Tech   **Time : 03 hrs.**
Course Code: CSC7003   **Max. Marks: 100**

Instructions:
- **Section A** has 5 Questions of 4 marks each, select the best fit answer.
- **Section B** has 4 Questions for a total of 10 marks each, write brief notes, examples with diagrams.
- **Section C** has choice of 2 Questions for a total of 20 marks, mention answers, examples with diagrams.
- Use white A4 with black gel-pen; write clearly with diagrams to illustrate your answers.
- If the answer is more than one page long, mention the section & answer number on each page.

SECTION A
(5Qx4M=20Marks)

S. No.		Marks	CO
Q 1	You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case? a. The registry b. The swap file c. The recycle bin d. The metadata	4	CO1
Q 2	Karan is a Forensic Investigator working for Adani Corp. He started investigating a forensic case and has collected some evidence. Now Karan wants to use this evidence for further analysis. What should Karan do? a. He should use the original evidence he has collected and proceed with the analysis process b. He should not use the original evidence he has collected c. He should send the report for further analysis d. He should not use the evidence collected and use some other's evidence report.	4	CO1
Q 3	Which one of the following is the smallest allocation unit of a hard	4	CO1

	disk, which contains a set of tracks and sectors ranging from 2 to 32, or more, depending on the formatting scheme? a. Sector b. Cluster c. Track d. 4Platter		
Q 4	A critical drawback of binary system is …. a. It requires very large strings of 0s and 1s to represent decimal numbers. b. It requires unusually small string of 1s and 0s to represent decimals. c. It requires large strings of 0s, but small strings of 1s to represent decimal numbers. d. It requires small strings of 0s, but large strings of 1s to represent decimal numbers.	**4**	**C02**
Q 5	Digital Forensic Investigators are required to maintain three types of records. Which these is not a record? a. Chain of custody b. Documentation of the crime scene c. Searching the crime scene d. Document your actions	**4**	**C04**
	SECTION B **(4Qx10M= 40 Marks)**		
Q 6	a. Mention different types of hard disks? b. How would you collect Volatile information c. What do you understand by text-based logs and Events?	**10**	**CO1**
Q 7	What do you understand by File Systems? Give examples. OR What do you understand by File Format, describe at least four file formats with examples?	**10**	**CO3**
Q 8	a. Why and when do you use Computer Forensics? b. What are the different types of Computer crimes?	**10**	**CO2**
Q 9	a. Describe the Windows Booting process?	**10**	**CO2**

	b. How will you analyze Windows Thumb-caches? c. What are the essential Windows Systems files?		
	SECTION-C **(2Qx20M=40 Marks)**		
Q 10	a. What are the four categories of Open Source Intelligence? b. Mention at least four advantages and challenges of OSINT. OR a. What do you understand by Digital evidence? b. Mention at least five sources of Digital evidence.	**20**	**CO3**
Q 11	Describe the types of Data acquisition systems? What do you understand by Password types and cracking techniques?	**20**	**CO4**