Name: Enrolment No:	

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

Course: Digital Data Recovery and Analysis   **Semester:** III
Program: MCA (AIML, IoT, CSF, BFSI)   **Time:** 03 hrs.
Course Code: CSCS 8006P   **Max. Marks: 100**

Instructions: Attempt all the questions. Q. No. 11 has internal choice.

<table>
<tr><th colspan="4">SECTION A
(5Qx4M=20Marks)</th></tr>
<tr><th>S. N.</th><th></th><th>Marks</th><th>CO</th></tr>
<tr><td>Q 1</td><td>List two types of digital investigations typically conducted in a business environment.</td><td>4</td><td>CO1</td></tr>
<tr><td>Q 2</td><td>Is it imperative that the evidence media be protected write-protected? Justify your answer.</td><td>4</td><td>CO2</td></tr>
<tr><td>Q 3</td><td>Enumerate the advantages and disadvantages of the raw storage format.</td><td>4</td><td>CO3</td></tr>
<tr><td>Q 4</td><td>Differentiate between static and live data acquisition.</td><td>4</td><td>CO3</td></tr>
<tr><td>Q 5</td><td>Define block-wise hashing and express its utility.</td><td>4</td><td>CO4</td></tr>
<tr><th colspan="4">SECTION B
(4Qx10M= 40 Marks)</th></tr>
<tr><td>Q 6</td><td>(a) Explain different digital storage media and compared them towards their efficacy for digital data recovery.

(b) Discuss 'fdisk' program. Has it been deprecated? Discuss its utility in data acquisition process.</td><td>6, 4</td><td>CO1</td></tr>
<tr><td>Q 7</td><td>(a) Justify the need for preserving the digital crime scene. Enlist various computer evidence processing steps.

(b) Define a 'bit-stream copy'. Give an example of bit-stream copy.</td><td>6, 4</td><td>CO2</td></tr>
<tr><td>Q 8</td><td>(a) Discuss Authenticode and Digital ID. Brief the benefits of using them.

(b) Express the need for digital image verification and authentication protocol.</td><td>6, 4</td><td>CO3</td></tr>
<tr><td>Q 9</td><td>(a) Explain how Autopsy can be used for forensic data validation.

(b) Define honeypots and honeywalls. Discuss their utilities.</td><td>6, 4</td><td>CO4</td></tr>
</table>

	SECTION-C (2Qx20M=40 Marks)		
Q 10	(a) Define RAID. Explain various levels of RAID. (b) Explain any two techniques to hide data.	**10, 10**	**CO3, CO4**
Q 11	(a) Explain various digital data acquisition tools. (b) Express meaning of network forensics. Explain how packet analyzers are used for network forensics.	**10, 10**	**CO3, CO4**
	OR		
	(a) Explain any remote network acquisition tool. (b) Explain the techniques to validate forensic data.	**10, 10**	**CO3, CO4**