Name: **Enrolment No:**	UPES UNIVERSITY OF TOMORROW

UPES

End Semester Examination, December 2023

Course: Forensic Tools **Semester: 3**
Program: MCA CSF **Time : 03 hrs.**
Course Code: CSCS8002P **Max. Marks: 100**

Instructions:

1. Attempt all questions. Be precise and to the point.
2. In all attempted questions, provide the question number.
3. Begin answering each question on a new page of the answer sheet.
4. ***Answering both questions in a single choice question will result in the dismissal of both answers.**

SECTION A (5Qx4M=20Marks)

S. No.		**Marks**	**CO**
Q 1	Illustrate 4 differences between MD5 and SHA256.	**4**	**CO1**
Q 2	What is VirusTotal and how does it work?	**4**	**CO2**
Q 3	Mention the role of File Systems in Cyber Forensics.	**4**	**CO3**
Q 4	State and compare Mobile Forensics and Memory Forensics	**4**	**CO4**
Q 5	Illustrate the different features of the Volatility Workbench.	**4**	**CO5**

SECTION B (4Qx10M= 40 Marks)

Q 6	How Can Volatility Be Used in Memory Forensics and Analysis?	**10**	**CO1**
Q 7	Explain in detail the stages involved in the evidence-collecting process in mobile forensics.	**10**	**CO1/CO2**
Q 8	What specifically is a Central Data Repository? Explain all the different types of Window Registry in detail.	**10**	**CO2**
Q 9	What is the need for Forensic Image in Hard Drive forensics? Describe all the features of FTK. How is FTK different from ProDiscover Basics? OR State and compare features of partition using the EaseUS tool and Mini Tool.	**10**	**CO3**

SECTION-C
(2Qx20M=40 Marks)

Q 10	Explain WinHex. Demonstrate the 10 features of WinHex using suitable applications based on license type comparison.	**20**	**CO4**
Q 11	What is RAM Capture? What information could be stored in RAM for forensic purposes? How do you obtain protected files in RAM capture? OR Explain the significance of OS Forensics. What are the concerns with contamination and event logs in Windows? Provide four examples of in-depth event tracking.	**20**	**CO5**