Name: **Enrolment No:**	

UPES
End Semester Examination, May 2024

Course: Digital Forensics **Semester: VIII**
Program: B Tech (CSE+AI&ML-BD-CCVT-DEV-CSF – H/NH) **Time : 03 hrs.**
Course Code: CSSF4015P **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.
- Mention each answer number clearly, draw 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	Which one of the following is the smallest allocation unit of a hard 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. Platter	**4**	**CO1**
Q 2	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 3	Convert the following Binary numbers into Hexadecimal: a.) 10101011 b.) 11001101 c.) 10011101 d.) 10110101	**4**	**CO1**

Q 4	Digital Forensic Investigators are required to maintain three types of records. Which of 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**	**CO1**
Q 5	Which one of the following is the smallest allocation unit of a hard 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. Platter	**4**	**CO1**
SECTION B (4Qx10M= 40 Marks)			
Q 6	Describe the terms with example: a.) Alerts b.) Events c.) Incidents d.) Problem e.) Issue	**10**	**CO1**
Q 7	a. How will you analyze Windows Thumb caches? b. What are the essential Windows Systems files?	**10**	**CO2**
Q 8	a. Why and when do you use Computer Forensics? b. Describe the different types of Computer crimes?	**10**	**CO2**
Q 9	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**
SECTION-C (2Qx20M=40 Marks)			
Q 10	a. Describe the types of Data acquisition systems? b. What do you understand by Password types and cracking techniques?	**20**	**CO3**
Q 11	a. What are the four categories of Open-Source Intelligence? b. Mention at least four advantages and challenges of OSINT. OR	**20**	**CO4**

	a. What do you understand by Digital evidence? b. Mention at least five sources of Digital evidence.		