UPES

End Semester Examination, May 2025

Course: Digital Forensics
Program: BTech-CS-All
Course Code: CSSF4015P

Semester   : 8
Time   : 03 hrs.
Max. Marks : 100

Instructions: Attempt all questions. Calculators not allowed.

SECTION A
(5Qx4M=20Marks)

S. No.		Marks	CO
Q 1	Discuss different PE sections and their functions.	4	CO1
Q 2	Discuss the importance of examining the (.rsrc).	4	CO2
Q 3	With example note down different types of malwares.	4	CO5
Q 4	Write a short note on PGP protocol.	4	CO4
Q 5	Write a short note on different types of Steganography.	4	CO3

SECTION B
(4Qx10M= 40 Marks)

Q 6	Compare MBR and GPT partition table.	10	CO4
Q 7	Discuss the importance of cookie and cache analysis in web browser analysis.	10	CO3
Q 8	Discuss static malware analysis.	10	C05
Q 9	(a) White a note on LSB-Steganography. (8) (b) Discuss the effect on the cover media if we do use other bits in LSB-Steganography to hide our data. (2) **OR** (a) Discuss legal considerations in digital evidence handling. (5) (b) Discuss how to preserve the chain of custody in Digital Forensics investigation. (5)	10	CO4

	SECTION-C (2Qx20M=40 Marks)		
Q 10	Examine the role of digital forensics in investigating a suspected bank account fraud over call, involving seized mobile phones and laptops. Identify the critical data types to focus on and explain the step-by-step process for extracting, analyzing, and utilizing this information to uncover fraudulent activities.	20	CO5
Q 11	(a) With clear diagrams, discuss how to back up your forensic data using RAID. (10) (b) Discuss file metadata and its importance in digital forensics. (10) **OR** (a) Discuss malware hashing and it's purpose. (5) (b) Draw PE header structure. (10) (c) Steps to analyze the PE header. (5)	20	CO4