Name: Enrolment No:	

UPES
End Semester Examination, May 2025

Course: Digital Forensics II **Semester : 12**
Program: BTech LLB **Time : 03 hrs.**
Course Code: CSSF 4004 **Max. Marks: 100**

Instructions: Attempt all questions. Calculators not allowed.

S. No.		Marks	CO
	SECTION A **(5Qx2M=10Marks)**		
Q 1	In a laboratory setting, determine the sources within a mobile device from which call data can be retrieved.	**2**	**CO1**
Q 2	Discuss the role of master file table managed by the OS.	**2**	**CO1**
Q 3	A JPEG file uses i. WinZip compression ii. Lossy compression iii. Lzip compression iv. Lossless compression	**2**	**CO2**
Q 4	Analyze the implications of utilizing the MSB for steganographic techniques.	**2**	**CO3**
Q 5	List down various steganographic techniques.	**2**	**CO2**
	SECTION B **(4Qx5M= 20 Marks)**		
Q 6	Discuss different types of malwares.	**5**	**CO4**
Q 7	Analyze objectives of cryptography and steganography to determine whether they serve the same purpose.	**5**	**CO2**
Q 8	Assess when we call a cryptographic scheme ‘‘secure’’.	**5**	**CO1**
Q 9	List different ways to do image steganography. (2.5) List different transformation techniques for image steganography. (2.5)	**5**	**CO4**
	SECTION-C **(2Qx10M=20 Marks)**		
Q 10	Deduce the probabilistic definition of CPA security with a clear diagram.	**10**	**CO3**

Q 11	Given the following scenarios, identify the most suitable RAID architecture (with diagram) for each, and justify your choice: 1. A small business needs a solution where data redundancy is crucial, but cost is a primary concern. (2.5) 2. A high-performance computing system requires fast data access with no need for redundancy. (2.5) 3. A large enterprise requires a balance of redundancy and performance with the ability to recover from a single disk failure. (2.5) 4. A high-availability environment needs both redundancy and fault tolerance, with the capability to continue operation even if two disks fail. (2.5) **OR** (a) Discuss the importance of direct memory access. (3) (b) Discuss the control flow of direct memory access controller to CPU control unit.	**10**	**CO4**
SECTION-D (2Qx25M=50 Marks)			
Q 12	(a) **Scenario:** A malware analyst is given a file that is suspected of containing a Trojan. Describe, in detail, the steps they would take to perform static malware analysis on the file. (10) (b) **Scenario:** A team of analysts is preparing to analyze a malware sample in a controlled environment. What security guidelines should they follow to ensure the analysis is safe and prevents contamination or data leakage? (5) (c) **Scenario:** A cybersecurity firm is tasked with analyzing a suspicious file that has been detected in a corporate network. Discuss the different types of malware analysis that could be employed in this case. (5) (d) **Scenario:** A security researcher needs to identify whether a file is an executable, image, or archive. Explain the process of identifying different file types and how it can help in malware analysis. (5)	**25**	**CO4**
Q 13	(a) **Scenario:** A cybersecurity analyst receives an alert about a suspicious file that matches the fingerprint of previously seen malware on multiple endpoints in the company's network.	**25**	**CO3**

	Question: Describe the process of malware hashing and explain why this technique is crucial for identifying, cataloging, and tracking malware samples. (10) (b) **Scenario:** While reversing a newly captured binary in a secure sandbox, an analyst notices that the payload behavior isn't obvious from dynamic execution alone. **Question:** Discuss the step-by-step process of extracting and analyzing strings from the malware sample, and how these findings can reveal insights into the malware's functionality or provenance. (5) (c) **Scenario:** You have obtained a potentially malicious Windows executable that may carry a hidden backdoor. Before running it, you need to inspect its metadata. **Question:** First, draw the layout of a Portable Executable (PE) header. Then, discuss in detail how you would analyze each major header field to uncover anomalies or signs of tampering. (10) **OR** (a) **Scenario:** A covert communications specialist is tasked with hiding sensitive text within innocuous images to evade detection. **Question:** Discuss the principal idea behind LSB steganography and how it enables secret data embedding without visibly altering the carrier image. (8) **Question:** Evaluate whether it is possible to embed an arbitrary amount of data in an image using LSB steganography and explain the limiting factors. (2) (b) **Scenario:** Following a suspected insider data theft, a digital forensics team arrives on-site to preserve and examine all relevant digital artifacts. **Question:** In detail, outline the standard procedures for collecting and analyzing digital evidence—covering chain-of-custody, imaging techniques, and examination methodologies. (10) (c) **Scenario:** After a user accidentally reformats their workstation drive, critical project files appear lost. **Question:** Describe the step-by-step methods for recovering and reconstructing deleted data from formatted or partially overwritten storage media. (5)		