Name: **Enrolment No:**	

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Sem Examination, May 2023

Course: Digital Forensics II **Semester: 6th**

Program: B.Tech-CSE **Max. Marks: 100**

Course Code: CSSF3014 **Time: 03 hrs.**

SECTION A **(5Qx 4M = 20 Marks)**

Note: This section have 5 Questions (short answer type) of 4 marks each.
All the questions shall be compulsory.

S. No.		Marks	CO
Q 1	State the process of creating a memory dump.	**4**	**CO1**
Q2	Explain how steganography can be used for malicious purposes.	**4**	**CO2**
Q3	Differentiate between static and dynamic analysis in malware analysis.	**4**	**CO4**
Q4	Elucidate the role of a SIM card in mobile device forensics. What is the information that reside on the mobile device?	**4**	**CO3**
Q5	Contrast the comparison between logical and physical acquisition in mobile device forensics.	**4**	**CO3**

SECTION B **(4Qx 10M = 40 Marks)**

Note: This section have 4 Questions of 10 marks each.

Q 6	Analyze the difference between Non-invasive and invasive Mobile forensics **OR** Elaborate the mobile forensics with its objectives. Also, discuss the different types of data that can be extracted from mobile devices, and how this data is extracted?	**10**	**CO3**
Q 7	A suspicious file on a computer system has been identified and suspected that it may be a malware. Describe the steps you would take to analyze the file.	**10**	**CO4**
Q8	State the different techniques used for memory acquisition and analysis in digital forensics.	**10**	**CO1**
Q9	Demonstrate how image steganography works with an example of a common technique used to hide (text & image) secret information in an image (cover file).	**10**	**CO2**

SECTION-C **(2Qx 20M= 40 Marks)** **Note: Q11 has internal choice to attempt any one.**			
Q10	a) ***Scenario:*** *Alice works for a large corporation and has been accused of stealing confidential company information. She denies the accusation and claims that her computer was hacked. The company hires a digital forensics team to investigate the incident and recover any relevant evidence from Alice's computer.* **Question:** Summarize the **data hiding methods** which may have been used by Alice, and **recovery techniques** used by forensics team to recover the hidden data. b) How many types of different malwares are there and how those infect the systems. Elucidate the techniques used for analyzing the malware behavior.	**10+10**	**CO4**
Q11	Define Steganography and its four types with examples. Also, list their advantages and disadvantages. **OR** You want to hide a secret message of length 300 bits within a BMP image of size 800 pixels x 600 pixels. You decide to use LSB steganography to hide the message in the least significant bit of each color channel. What is the maximum number of bits you can hide in each color channel, assuming that the image is in 24-bit color (8 bits per color channel) and the LSB of each color channel pixel can be modified?	**20**	**CO2**