Name:

Enrolment No:

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, May 2022

Course: Digital Forensics
Semester: VIII
Program: B.Tech CSE+(CCVT &IFM) **Time : 03 hrs.**
Course Code: CSSF 4011P **Max. Marks: 100**

Instructions: ***Attempt all questions. Section B and Section C have internal choice. Write the answers pointwise as per marking of the question.***

SECTION A

(5Qx4M=20Marks)

S. No.		Marks	CO
Q 1	What is some of the volatile information you would retrieve from a computer system before powering it off/on?	**4**	**CO4**
Q 2	What is an incident? List the goals of incident response.	**4**	**CO1**
Q 3	Answer **TRUE** or **FALSE** with respect to registries in Windows OS: a. When a program is installed, a new sub key containing settings like a program's location, it's version, and how to start the program, are all added to the Windows Registry. b. Registry contains user who is currently logged into Windows and their settings. c. Registry contains list of startup programs. d. Registry records every SSID of every wireless network.	**4**	**CO3**
Q 4	Choose the correct answer(s):- i. …………………..includes the attacks on the images by various image processing techniques to expose the hidden information by attackers A. Steganography B. Steganalysis C. Cryptography D. Cryptanalysis ii. ……………are sometimes visible to human eye and usually become an attribute of the image. A. Hidden data B. Signatures C. Water marks D. Certificates iii. Choose all Mobile Forensics tool(s):- A. XRY	**4**	**CO2**

	B. UFED C. AccessData FTK D. MobilEdit iv. Mobile devices typically contain one or two different types of non-volatile flash memory A. True B. False		
Q 5	What are various types of security policies?	**4**	**CO1**
SECTION B **(4Qx10M= 40 Marks)**			
Q 6	Explain the process of collecting volatile data in Windows System. **OR** Explain in detail, the Standard Operating Procedure of seizing and handling digital evidence.	**10**	**CO4**
Q 7	What do you understand by Memory forensics? Explain the process of memory forensics.	**10**	**CO3**
Q 8	Classify the different categories of cyber-crime with examples of each. Identify the type of cyber-crime for each of the following situations:- 1. Hacking into a web server and defacing legitimate web pages. 2. Introducing virus, worms, and other malicious code into a network or computer. 3. Unauthorized copying of copyrighted software, music, movies, art and books. 4. Internet gambling and trafficking	**6+4**	**CO1**
Q 9	**Scenario:** The suspect uses physical storage media for hiding the information e.g. hard drives, floppies, USB drives, mobile phone memory cards, digital camera memory cards, CD ROMs, DVD ROMs, iPods etc. **As per the above scenario, answer the following questions:-** 1. Which sections of IT Act are applicable? 2. Who do you think is liable? 3. What might be the motive? 4. How would Cyber Crime Cell investigate and solve the case?	**10**	**CO5**
SECTION-C **(2Qx20M=40 Marks)**			
Q	a. Consider a DC signal that is a constant 100 for domain [0, 7]. Calculate F (0) and F (1) for 1D DCT. b. What is D-O-R-A Process? Explain it with the help of a diagram.	**10+10**	**CO5**
	Draw a flowchart to explain Incident Handling and Response Process for UPES Dehradun. **OR** A student was connected to UPESNET wifi. He received a mail from admin team to change his stu password immediately. As soon as he	**20**	**CO1**

	clicked on the link, a message displayed: “Your files have been encrypted. To decrypt pay in Bitcoins.” Explain the process flow of Evidence gathering and Forensic Analysis for above incident.		