Name: **Enrolment No:**	UPES UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, May 2023

Course: Digital Forensics **Semester: VIII**
Program: B. Tech (CSE) **Time: 03 hrs.**
Course Code: CSSF4040P **Max. Marks: 100**

Instructions: All Questions are COMPULSORY. Internal choice is available in Q 9 and Q 11.

SECTION A

S. No.		Marks	CO
Q 1	Describe Cybercrime, how it is different from traditional criminal activity?	**04**	**CO5**
Q 2	You are a computer forensic examiner and want to determine whether a user has opened or double-clicked a file. What folder would you look in for a windows operating system artefact for this user activity? Support your answer with valid explanation.	**04**	**CO2**
Q 3	Which information you will collect before switching off the computer system. Also, explain its role in digital forensic investigation.	**04**	**CO1**
Q 4	Explain the functions of the following registry HKEYs: i. HKEY_CLASS_ROOT ii. HKEY_CURRENT_USER iii. HKEY_LOCAL_MACHINE iv. HKEY_CURRENT_CONFIG	**04**	**CO1**
Q 5	Describe Windows Sysinternals? Explain TWO tools with their functionality that is present in Sysinternals.	**04**	**CO3**

SECTION B

Q 6	a) What do you understand by Order of Volatility? How it is helpful in performing digital investigation. [05] b) Explain TCP/IP 3-way handshake with the help of a proper diagram. [05]	**10**	**CO2**
Q 7	a) How will you trace the crime, which has happened through email using a tool? [05] b) Which information you can draw from the e-mail header given below: [05]	**10**	**CO3**

	Received: from antivirus1.its.rochester.edu (antivirus1.its.rochester.edu [128.151.57.50]) by mail.rochester.edu (8.12.8/8.12.4) with ESMTP id h2OGQs9o002563; Mon, 24 Mar 2003 11:26:54 -0500 (EST) Received: from antivirus1.its.rochester.edu (localhost [127.0.0.1]) by antivirus1.its.rochester.edu (8.12.8/8.12.4) with ESMTP id h2OGQrQx003450; Mon, 24 Mar 2003 11:26:54 -0500 (EST) Received: from galileo.cc.rochester.edu (galileo.cc.rochester.edu [128.151.224.6]) by antivirus1.its.rochester.edu (8.12.8/8.12.4) with SMTP id h2OGQrDC003447; Mon, 24 Mar 2003 11:26:53 -0500 (EST) Received: (from majord@localhost) by galileo.cc.rochester.edu (8.12.8/8.12.4) id h2OGQq91029757; Mon, 24 Mar 2003 11:26:52 -0500 (EST) Date: Mon, 24 Mar 2003 11:26:50 -0500 (EST) From: somesender@mail.rochester.edu Message-Id: <200303241626.h2OGQojt002507@mail.rochester.edu> To: someuser@its.rochester.edu Subject: My mail message is about:		
Q 8	Name three formats in which data is acquired. How Digital Evidence Acquisition is done and how it is authenticated?	**10**	**CO4**
Q 9	What are the legal aspects of Online Obscenity & Pornography according to Indian Cyber Laws? OR What are the legal aspects of Cyber Stalking and Defamation according to Indian Cyber Laws?	**10**	**CO5**
	SECTION-C		
Q 10	Differentiate between the following: [5*4] a) FAT v/s NTFS file system structure b) IMAP v/s POP c) Volatile v/s Non-Volatile evidences d) Static IP v/s Dynamic IP e) TCP v/s UDP	**20**	**CO2**
Q 11	What is Messenger Forensics? How it is useful in forensics investigations. Explain the working structure of Yahoo Messenger. OR What is Web Browser Forensics? What is the role of index.dat in forensics investigation? Explain about some tools used in Web Browser Forensics.	**20**	**CO3**