Name:

Enrolment No:

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2022

Course: Digital Forensics-I **Semester: V**
Program: B.Tech CSE+CSF **Time : 03 hrs.**
Course Code: CSSF3003 **Max. Marks: 100**

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

SECTION A
(5Qx4M=20Marks)

S. No.		Marks	CO
Q 1	Explain about e-mail forensics? Explain the various agents involved in the typical flow an email with the help of a diagram.	**4**	**CO3**
Q 2	Summarize Windows Sysinternals? Explain TWO tools with their functionality that is present in Sysinternals.	**4**	**CO2**
Q 3	Classify the different categories of cyber crime with examples of each. Identify the type of cyber-crime for each of the following situations: a) Hacking into a web server and defacing legitimate Web pages b) Introducing viruses, worms, and other malicious code into a network or computer c) Unauthorized copying of copyrighted software, music, movies, arts, books. d) Internet gambling and trafficking	**4**	**CO3**
Q 4	Briefly explain the role of Windows registry in collecting forensic evidence. Explain the functions of the following registry HKEYs: a) HKEY_CURRENT_USER b) HKEY_LOCAL_MACHINE	**4**	**CO1**
Q 5	Explain the process for the analysis of a digital evidence is performed? Write the list of analysis done in most of the cybercrime cases.	**4**	**CO4**

SECTION B
(4Qx10M= 40 Marks)

S. No.		Marks	CO
Q 6	Explain Disk Imaging and preservation achieved in Digital Forensics? [05] Illustrate the Order of Volatility? How it is helpful in performing digital investigation. [05]	**10**	**CO1**
Q 7	Mention the best practices for seizing a home personal computer or laptop computer. If you (as a forensic investigator) visits the crime scene, what are the general investigative questions that may be asked regarding a crime involving computers and electronic evidence.	**10**	**CO4**

Q 8	Telecaller Private Limited (TPL) is a business process outsourcing (BPO) outfit handling business process outsourcing for various clients in North America and Europe. The employees of TPL become privy to confidential customer information during the course of their work. The nature of this information ranges from medical records of individuals to financial data of companies. The unprocessed data is transmitted from the client's location to TPL offices in Gurgaon, Pune and Hyderabad through the Internet using VPN (Virtual Private Network) connections on broadband. TPL allows clients to transfer information via dedicated FTP servers on the Internet, which can then be accessed and processed by its employees. TPL, through its website, worksource.com allows its clients to log in and view billing and other information specific to them. Access to this information is restricted through the usual user name - password combination found on most websites. Looking at the above scenario, discuss the threats TPL faces to its information and suggest controls which it may put in place to secure its information from such Threats.	**10**	**CO4**
Q 9	Describe the legal aspects of Online Obscenity & Pornography according to Indian Cyber Laws? OR Describe the legal aspects of tampering with computer documents and hacking according to Indian Cyber Laws?	**10**	**CO5**
SECTION-C **(2Qx20M=40 Marks)**			
Q 10	Differentiate between the following: [5*4] a) FAT v/s NTFS file system structure b) IMAP v/s POP3 v/s SMTP c) Switched v/s Unswitched network d) Static IP v/s Dynamic IP e) TCP v/s UDP	**20**	**CO1**
Q 11	Define Messenger Forensics? List the challenges of Messenger Forensic. Explain the architecture of any one messenger of your choice along with its forensic tools. OR Define Web Browser Forensics? Explain the role of index.dat in forensics investigation? Explain about some tools used in Web Browser Forensics.	**20**	**CO3**