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

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
Online End Semester Examination, December 2020

Course: Digital Forensics - II **Semester: V**
Program: B. Tech. CSE + CSF **Time 03 hrs.**
Course Code: CSSF 4004 **Max. Marks: 100**

SECTION A

1. **Each Question will carry 5 Marks**
2. **Instruction: Complete the statement / Select the correct answer(s)**

S. No.	**Question**	**CO**
Q 1	Which of the following is a correct sequence of steps followed in Mobile Forensics? a) Examination of evidences, Preservation, Analysis, Collection, Identification, Presentation b) Collection of evidences, Preservation, Identification, Analysis, Examination, Presentation c) Identification of evidences, Collection, Preservation, Examination, Analysis, Presentation d) Analysis of evidences, Collection, Identification, Preservation, Examination, Presentation	**CO1**
Q2	_____ command lists computers that are/have recently connected to the system. _____ command displays information about network state and the MAC address of the computer.	**CO3**
Q3	Write any 10 plugins (names only) used in Volatility Framework :....., ..., ..., ..., ..., ..., ..., ..., ..., ..., ...	**CO3**
Q4	The file signature for PE files are represented by hexadecimal values of _____ in the first two bytes.	**CO4**
Q5	The ABSENCE of Red, Green and Blue color in RGB color cube yields _____ colour.	**CO2**
Q6	_____ is a 32 bit unique code attached on a chip inside CDMA by the manufacturer in which _____ bits represents manufacturer code and _____ bits represents serial number.	**CO1**

SECTION B

1. **Each question will carry 10 marks**
2. **Instruction: Write short / brief notes**

Q 7	Differentiate between Steganography, Cryptography and Watermarking? Also, describe the classification of steganography with the help of a diagram.	**CO2**

Q 8	Explain with the help of a neat diagram about the Windows Process Genealogy used in Memory Forensics.	**CO3**
Q 9	What is Malware Analysis and what is the need of it? Briefly describe the types of Malware based on their functionality.	**CO4**
Q 10	Write down the steps involved with brief description the steps involved in static analysis of a malware.	**CO4**
Q 11	What type of useful data can be found with the help of memory forensics? Mention any 5 RAM acquisition or analysis tools. OR What is Memory Forensics? Why there is a need of Memory Forensics? Also, mention the benefits of memory analysis.	**CO3**
Section C 1. **Each Question carries 20 Marks.** 2. **Instruction: Write long answer.**		
Q12	Draw and explain SIM card file system. Also, explain the use of IMEI and ICCID. What are the different type of information that can be recovered from a SIM card? OR Draw and explain the mobile device tool classification system that are used in extracting evidences from a mobile device. Also, down the steps involved in handling /seizing of a mobile device (android or iOS).	**CO1**