Name:

Enrolment No:

UPES
UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination QP, December 2021

Course: Digital Forensics II **Semester : V**

Program: B.Tech CSE-CSF **Time : 03 hrs.**

Course Code: CSSF 4013 **Max. Marks: 100**

Instructions: ***All questions are compulsory in Section A. There is an internal choice in Section B and Section C.***

SECTION A (20 Marks)

1. Each Question will carry 4 Marks
2. Instruction: This section contains FB, T/F, multiple choice, and multiple answer questions.

S. No.		**Marks**	**CO**
Q 1	Write the full forms of the following acronyms:- i. GSM ii. IMEI iii. CDMA iv. JTAG	**4**	**CO1**
Q 2	Distinguish between Steganography and Cryptography.	**4**	**CO2**
Q 3	What are packed and obfuscated malwares?	**4**	**CO4**
Q 4	**Choose the correct answer(s):-** i. Which of the following tools are not used for dissecting malware in memory images or running systems? A. Blacklight B. DAMM C. Volatility D. FLOSS ii. If the Internet History file has been deleted, _____________ may still provide information about what Web sites the user has visited. A. Cookies B. Metadata C. user profiles D. Sessions	**4**	**CO3**
Q 5	**Choose the correct answers:-** i. Choose all Mobile Forensics tool(s):- A. XRY B. UFED C. AccessData FTK D. MobilEdit ii. Mobile devices typically contain one or two different types of non-volatile flash memory	**4**	**CO1**

	A. True B. False iii. Android is a truly open platform that separates the hardware from the software that runs on it. A. True B. False iv. WCDMA in GSM decreases the data transmission speed by using the air interface of CDMA A. True B. False		

SECTION B (40 Marks)

1. **Each question will carry 10 marks**
2. **Instruction: Write short / brief notes. There is internal choice in this section.**

Q 6	Given a 15-digit IMEI No. below, answer the following questions: **IMEI: 359040056589206** i. How do we check for IMEI no. of any mobile device? ii. What does an IMEI no. indicate? iii. Identify TAC in above IMEI and explain in brief about it. iv. Identify FAC in above IMEI and explain in brief about it. v. Identify Serial No. in above IMEI and explain in brief about it.	**10**	**CO1**
Q 7	List three main types of steganography. How is steganography used with audio files?	**10**	**CO2**
Q 8	What do you understand by Memory forensics? Explain the process of memory forensics.	**10**	**CO3**
Q 9	Write short note on the following:- i. Hash Dumping ii. Keyloggers **OR** What is dynamic malware analysis? What precautions should be taken while performing dynamic malware analysis? When dynamic analysis can get failed?	**10**	**CO4**

SECTION-C (40 marks)

1. **Each Question carries 20 Marks.**
2. **Instruction: Write long answer. There is an internal choice.**

Q 10	**Case Study:** Jeremy Johnson, 26, was hired by Adams Central School District as a teacher. During his tenure as a teacher, there were rumors around the school campus about an inappropriate relationship between him and a female student. Both denied the rumors. Since school officials had no evidence of the relationship, they could only	**20**	**CO2**

	issue a warning. Several months later, the student told her cousins about the relationship. This triggered an investigation by the Adams County Sheriff's Department. The police searched Johnson's home. Johnson's bedroom matched the description given by the student in an interview with a female police officer. Johnson continued to deny the girl's claims concerning their sexual relationship. During the search, they seized his laptop and desktop computer. The investigators were able to verify that Johnson and the student exchanged e-mails. Johnson had reportedly set up an e-mail account for the girl in his wife's name. Though the e-mails were not explicit, the investigators could prove that Johnson and the student had been having a sexual relationship. Later, the forensic examiner found that Johnson had been trading child pornography over the Internet. He had hundreds of nude pictures of children obviously under the age of 18. He had tried to hide the images by putting them in a folder labeled "music." Jeremy Johnson was arrested and jailed on 19 charges of child seduction, a Class D felony. With respect to above scenario, answer the following questions:- i. What are the methods investigators use to acquire digital evidence? ii. Is there a need of data duplication? Why? iii. Write down the hardware and software tools used for data acquisition. iv. Write down the hardware and software tools used for data duplication. **OR** With respect to Image Forensics, answer the following questions:- i. Name three image file formats and name whether each is vector, raster, or both. ii. When you analyze image file headers, what are you looking for? iii. What does carving mean? iv. Name a steganalysis tool and describe how it works. v. List three different image file forensic tools. Describe why you would use each.		
Q 11	Consider a DC signal that is a constant 100 for domain [0, 7]. Calculate F (0) and F (1) for 1D DCT.	**20**	**CO1**