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

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2019

Course: Digital Forensics II **Semester : VII**

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

Course Code: CSIB 444 **Max. Marks: 100**

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

S. No.		Marks	CO
	SECTION A (20 Marks)		
Q 1	Write the full forms of the following acronyms:- i. GSM ii. IMEI iii. GPRS iv. CDMA	**4**	**CO1**
Q 2	State the principles of mobile forensics.	**4**	**CO1**
Q 3	Define JTAG.	**4**	**CO1**
Q 4	What are packed and obfuscated malwares?	**4**	**CO4**
Q 5	Distinguish between Steganography and Cryptography.	**4**	**CO5**
	SECTION B (40 Marks)		
Q 6	Discuss the memory types in featured mobile handsets.	**10**	**CO1**
Q 7	What do you understand by Memory forensics? Explain the process of memory forensics.	**10**	**CO3**
Q 8	Name three main types of steganography. How is steganography used with audio files?	**10**	**CO2**
	OR		

	Explain Steganalysis with example. Discuss any five attacks on Steganography.		**CO2**
Q 9	Categorize Malwares based on their functionality.	**10**	**CO4**
SECTION-C (40 marks)			
Q 10	What is D-O-R-A Process? Explain it with the help of a diagram. How a mobile device connects to the Internet?	**20**	**CO1**
Q 11	What is the purpose of Windows registry? How do malwares take advantage of registry? How many types of registry root keys are there? List the function of each root key. Also name the tool to view and edit registry.	**20**	**CO4**
	OR		
	How to set up a malware analysis lab for learning purpose? Draw the architecture. Mention the static and dynamic analysis tools that will be used to setup lab. Also, write the functionalities of those tools.	**20**	**CO4**