Name: Enrolment No:	UPES

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2018

Course: B.Tech **Semester:** VII
Programme: CSE + CSF
Time: 03 hrs. **Max. Marks:** 100

SECTION A

S. No.		Marks	CO
Q 1	List out the memory that may be useful in mobile forensics. What are the first byte of each SMS in SIM slot for following cases? • Unused • Read Incoming Message • Unread Incoming Message • Outgoing & Already Sent Message • Outgoing message which has not yet been sent	4	CO1
Q 2	Differentiate between steganography and cryptography functions.	4	CO2
Q 3	What are the different methods for acquiring volatile memory? Explain in detail	4	CO3
Q 4	What is the use of Write Blockers in digital forensics?	4	CO3
Q 5	Categorize Malwares based on their functionality.	4	CO4
	SECTION B		
Q 6	Discuss different mechanisms used for steganography in images.	10	CO2
Q 7	Explain different types of information that may be recovered via volatile memory forensics	10	CO3
Q 8	What is the need of malware analysis when there is antivirus? Define all three-malware analysis in brief. **OR** What is dynamic malware analysis? What precautions should be taken while performing dynamic malware analysis? When dynamic analysis can get failed?	10	CO4
Q 9	Describe different types of analysis that can be performed on DSC images to answer the following questions: a. What digital images exists? b. Where did they originate from? c. When were the images created or transferred? d. How were the images transferred?	10	CO1

SECTION-C			
Q 10	What kind of evidence collection technique is recommended for any mobile device forensics? How to choose evidence collection technique for a mobile device? Demonstrate a data recovery mechanism using mobile memory forensics that can preserve the data within the chain of custody. **OR** Explain SIM card file system. Also explain the meaning of IMSI and LAI. What are the different type of information that can be recovered from a SIM card?	**20**	**CO1**
Q 11	How can steganalysis guarantee robustness? Evaluate at least two mechanism that differentiate image to video steganalysis. Conclude on how data recovery is guaranteed without change of image specification during communication.	**20**	**CO2**

Name:

Enrolment No:

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, December 2018

Course: B.Tech **Semester:** VII
Programme: CSE + CSF
Time: 03 hrs. **Max. Marks:** 100
Instructions:

SECTION A

S. No.		Marks	CO
Q 1	Explain use of PUK in SIM? What is IMSI and LAI, and what are they made up of?	4	CO1
Q 2	Classify the different approaches of steganalysis used by steganalyst.	4	CO2
Q 3	What are the indicators of compromise while performing dynamic malware analysis?	4	CO4
Q 4	Describe data recovery techniques; SPM,MFM, and STM.	4	CO2
Q 5	What is the difference between FAT and NTFS based on MFT?	4	CO3
	SECTION B		
Q 6	Describe different types of analysis that can be performed on DSC images to answer the following questions: a. What digital images exists? b. Where did they originate from? c. When were the images created or transferred? d. How were the images transferred?	10	CO1
Q 7	What do you understand by Memory forensics? Explain the process of memory forensics.	10	CO3
Q 8	Write the necessary steps to set up a malware analysis lab for learning purpose? Draw the architecture.	10	CO4
Q 9	Discuss different types of audio steganography algorithms. **OR** Using string-based extraction, demonstrate how volatile memory is searched and discovered?	10	CO2, CO3
	SECTION-C		
Q 10	Dynamic malware analysis is very critical in practice. Justify which precautionary measure can improve the performance of success by reducing failures. **OR** Evaluate any four tools used by forensic analysts for memory analysis, by keeping a real-time scenario in view	20	CO4, CO3
Q 11	Draw the architecture of SIM card file system. Also explain the meaning of IMSI and LAI. What are the different type of information that can be recovered from a	20	CO1

	SIM card?		