Roll No: ----------

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2017

Program Name	**: B.Tech CSE + CSF**	**Semester**	**: VII**
Course Name	**: Digital Forensics 2**	**Max. Marks**	**: 100**
Course Code	**: CSIB 444**	**Duration**	**: 3 Hrs**
No. of page/s	**: 02**		

Note:

1. Answers to question 1 to 5 of Section A carries 4 marks each.
2. Answers to question 6 to 9 of Section B carries 10 marks each.
3. Answers to question 10 and 11 of Section C carries 20 marks each.

SECTION A

1. What do low and high frequencies means in an image?

2. What is hex dump? When hex dump is used?

3. Write the volatility commands:

(a)To see the information related to the image
(b)To list the processes those were running

4. Write the volatility commands:

(a)To identify the processes which could be rootkit or malware.
(b)To list the dll files

5. What is the use of Write Blockers in digital forensics?

SECTION B

6. What is the need of malware analysis when there is antivirus? Define all three-malware analysis in brief.

7. How to set up a malware analysis lab for learning purpose? Draw the architecture.

8. In continuation to previous question please mention what static and dynamic analysis tools will be used to setup lab. Also, write the functionalities of those tools.

9. What do you understand by Memory forensics? Explain the process of memory forensics.

SECTION C

10. Compare the levels of Mobile Forensics Tool in tabular format based on following:

Level Name	Process	Tools	Pros	Cons

11. Consider a DC signal that is a constant 100 for domain [0, 7]. Calculate F (0) and F (1) for 1D DCT.

Roll No: ----------

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, December 2017

Program Name	**: B.Tech CSE + CSF**	**Semester**	**: VII**
Course Name	**: Digital Forensics 2**	**Max. Marks**	**: 100**
Course Code	**: CSIB 444**	**Duration**	**: 3 Hrs**
No. of page/s	**: 02**		

Note:

1. Answers to question 1 to 5 of Section A carries 4 marks each.
2. Answers to question 6 to 9 of Section B carries 10 marks each.
3. Answers to question 10 and 11 of Section C carries 20 marks each.

SECTION A

1. What do you understand by Fourier Transform?

2. What is JTAG?

3. Write the volatility commands:

(a)To see the information related to the image
(b)To list the connections made on network

4. Write the volatility commands:

(a)To list physical address of registry files
(b)To list virtual address of registry files

5. What is the use of write blockers in digital forensics?

SECTION B

6. Categorize Malwares based on their functionality.

7. What is dynamic malware analysis? What precautions should be taken while performing dynamic malware analysis? When dynamic analysis can get failed?

8. What are the indicators of compromise while performing dynamic malware analysis?

9. What do you understand by Memory forensics? Explain the process of memory forensics.

SECTION C

10. Explain SIM card file system. Also explain the meaning of IMSI and LAI.

11. Consider a DC signal that is a constant 100 for domain [0, 7]. Calculate F (0) and F (1) for 1D DCT.