| | |
|---|---|
| **Name:**<br>**Enrolment No:** | UPES<br>UNIVERSITY WITH A PURPOSE |

**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**

**End Semester Examination QP, December 2020**

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

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

**Course Code: CSSF 4004** **Max. Marks: 100**

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

## SECTION A (30 Marks)

**1. Each Question will carry 5 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:-<br>i. GSM<br>ii. IMEI<br>iii. GPRS<br>iv. CDMA<br>v. LTE | **5** | **CO1** |
| Q 2 | Choose the correct answer(s):-<br>i. …………………..includes the attacks on the images by various image processing techniques to expose the hidden information by attackers<br>A. Steganography<br>B. Steganalysis<br>C. Cryptography<br>D. Cryptanalysis<br>ii. ……………are sometimes visible to human eye and usually become an attribute of the image.<br>A. Hidden data<br>B. Signatures<br>C. Water marks<br>D. Certificates | **5** | **CO2** |
| Q 3 | Choose the correct answer(s):-<br>i. Which of the following tools are not used for malware analysis?<br>A. VirusTotal<br>B. PEView<br>C. BlackWidow<br>D. SysInternals<br>ii. ……………………………..involves examining any given malware sample without actually running or executing the code.<br>A. Reverse Engineering<br>B. Static malware analysis<br>C. Dynamic malware analysis | **5** | **CO4** |

| | | | |
|---|---|---|---|
| | D. All of the above | | |
| Q 4 | Choose the correct answer(s):-<br>i. Which of the following tools are not used for dissecting malware in memory images or running systems?<br>A. Blacklight<br>B. DAMM<br>C. Volatility<br>D. FLOSS<br>ii. If the Internet History file has been deleted, _____________ may still provide information about what Web sites the user has visited.<br>A. Cookies<br>B. Metadata<br>C. user profiles<br>D. Sessions | **5** | **CO3** |
| Q 5 | Choose the correct answers:-<br>i. Choose all Mobile Forensics tool(s):-<br>A. XRY<br>B. UFED<br>C. AccessData FTK<br>D. MobilEdit<br>ii. Mobile devices typically contain one or two different types of non-volatile flash memory<br>A. True<br>B. False<br>iii. Android is a truly open platform that separates the hardware from the software that runs on it.<br>A. True<br>B. False<br>iv. WCDMA in GSM decreases the data transmission speed by using the air interface of CDMA<br>A. True<br>B. False | **5** | **CO1** |
| Q 6 | Write the volatility commands:-<br>i. To see the information related to the image.<br>ii. To list the processes those were running<br>iii. To identify the processes which could be rootkit or malware.<br>iv. To list the dll files<br>v. To list the connections made on network | **5** | **CO3** |
| **SECTION B (50 Marks)**<br>**1. Each question will carry 10 marks**<br>**2. Instruction: Write short / brief notes. There is internal choice in this section.** | | | |
| Q 7 | Discuss the memory types in featured mobile handsets. | **10** | **CO1** |
| Q 8 | What do you understand by Memory forensics? Explain the process of memory forensics. | **10** | **CO3** |
| Q 9 | Name three main types of steganography. How is steganography used with audio files?<br>OR<br>Explain Steganalysis with example. Discuss any five attacks on Steganography. | **10** | **CO2** |
| Q 10 | Categorize Malwares based on their functionality. | **10** | **CO4** |

| | | | |
|---|---|---|---|
| Q 11 | What is D-O-R-A Process? Explain it with the help of a diagram. How a mobile device connects to the Internet? | **10** | **CO1** |
| **SECTION-C (20 marks)**<br>1. **Question carries 20 Marks.**<br>2. **Instruction: Write long answer.** | | | |
| Q 12 | 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.<br>**OR**<br>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** |