


Name: Enrolment No:	
--------------------------------------	--

UPES
End Semester Examination, May 2024

Course: Digital Forensics II Program: B TECH(CSE+CSF-H/NH) Course Code: CSSF3014	Semester: VI Time : 03 hrs. Max. Marks: 100
---	--

Instructions:

1. Attempt all questions.
2. Be precise and to the point.
3. Begin answer to each question on a new page of the answer sheet.
4. Provide the question number.
5. Handwriting should be clear.
6. No calculators, any electronic gadgets or graph sheet allowed.

***Answering both questions in a single choice question will result in the dismissal of both answers.**

SECTION A
(5Qx4M=20Marks)

S. No.	Question	Marks	CO
Q 1	Differentiate between Low-Level Formatting and High-Level Formatting of any storage device.	04	CO1
Q 2	Differentiate between direct memory access (DMA) and Virtual Address Descriptor (VAD) tree.	04	CO2
Q 3	State any 4 (names only) data found in Volatile Memory.	04	CO3
Q 4	Discuss the importance of data recovery in any forensic investigation.	04	CO2
Q 5	Write any 10 plugins (names only) used in the Volatility Framework.	04	CO4

SECTION B
(4Qx10M= 40 Marks)

Q 6	“The Exif Metadata can contain a tremendous amount of information.” Explain in detail all the information obtained. What is this kind of forensics known as?	8+2	CO1
Q 7	Differentiate between Mobile forensics and Digital Camera Forensics.	5+5	CO2
Q 8	Explain Steganalysis. What does data recovery through Imaging involve? List 3 common forms of data loss.	2+5+3	CO4
Q 9	What type of useful data can be found with the help of Mobile forensics? Mention any 2 analysis tools for Mobile Forensics. <p style="text-align: center;">OR</p> What is Malware Forensics? Why there is a need of Malware Forensics? Also, mention the benefits of Malware analysis.	6+4 OR 3+4+3	CO3

SECTION-C
(2Qx20M=40 Marks)

Q 10	You are now engaged in the development of specific software using the Linux operating system. Unexpectedly, you begin to get a duplicate folder nested inside the original folder. Describe the methodology you will use to detect and remove malicious software from Linux operating systems.	20	CO2
Q 11	Illustrate and elucidate the SIM card types. Additionally, please explain the purpose and functionality of IMEI and ICCID. What are the many types of information that may be retrieved from a SIM card? OR Describe a classification of mobile device tools used to obtain evidence from mobile devices. Furthermore, outline the sequential procedures for managing and confiscating a mobile device, whether it is an android or iOS device.	20	CO1