Seat No. [redacted] 18 Enrolment No [redacted]

NATIONAL FORENSIC SCIENCES UNIVERSITY

M.Sc. Digital Forensics and Information Security - Semester I
Semester End Examination- December, 2024

Subject Code: CTMSDFIS SI P1 **Date: 4th December, 2024**
Subject Name: Computer Forensics

Time: 2:30 PM -5:30 PM **Total Marks: 100**

Instructions:

1. **Write down each question on a separate page.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

			Marks
Q.1		**Attempt any three**	
	(a)	Describe various components of a computer system.	**8**
	(b)	Describe the different categories of logs encountered during investigations on a Linux machine.	**8**
	(c)	What is Data Carving? How does it differ from Data Recovery? Explain various carving methods in detail.	**8**
	(d)	Convert **a. $(111110101011)_2$ to Decimal** **b. $(473)_{10}$ to Octal** **c. $(423)_{10}$ to Hexadecimal** **d. $(354)_8$ to Hexadecimal**	**8**
Q.2		**Attempt any three**	
	(a)	Explain various characteristics of HDD along with its internals and Geometry.	**8**
	(b)	Explain in detail the file systems FAT and NTFS.	**8**
	(c)	Explain the steps for digital investigation in detail.	**8**
	(d)	What types of artefacts can be discovered in Mac Forensics?	**8**
Q.3		**Attempt any three**	
	(a)	Explain the role of OS and its various types in detail.	**8**
	(b)	What is a File System? Explain the FS found in Linux machines.	**8**
	(c)	What is a Registry? Describe the different Windows artefacts that can be located within the registry.	**8**
	(d)	What is a Number system? Explain its various types.	**8**
Q.4		**Attempt any two**	

	(a)	Explain the Windows Event and Log Analysis in detail.	7
	(b)	What do you mean by Booting? Explain the process with a diagram.	7
	(c)	Explain in detail about HFS, HFS+ And APFS.	7
Q.5		**Attempt any two**	
	(a)	What is the chain of custody, and why is it important? Please provide a detailed explanation of its significance.	7
	(b)	What is imaging? Discuss its significance and the different types available.	7
	(c)	What are write blockers? Describe their importance and the different types.	7

--- End of Paper---

National Forensics Sciences University, Goa Campus
Mid-semester Examination

Programme – M.Sc. DFIS Sem – 1st Date- 7/10/2024 Subject Name Computer Forensic Subject Code- CTMSDFIS SI P1 Time- 1.5 Hours Max.Marks- 50 Instructions - 1) Answer all questions. 2) Assume suitable data.		
Q.1	Solve any four	20 marks
	a. Convert decimal number 450 into the hexadecimal representation.	5 marks
	b. Explain the functions of the control unit and ALU.	5 marks
	c. Explain Master Boot Record with a neat diagram	5 marks
	d. What is a write blocker? How is it useful in forensic investigation?	5 marks
	e. Write down a short note on Lockard's principle from the digital forensic perspective with an example.	5 marks
Q.2	Attempt all	15 marks
	a. Explain different branches of digital forensics.	5 marks
	b. How do you preserve the data on a live system?	5 marks
	c. What is slack space in memory?	5 marks
Q. 3	Attempt a and b	15 marks
Q.3 a	Attempt any one	
Q.3 a	I. Write down the guidelines for digital evidence collection and archiving.	8 marks
	OR	
	II. Write down the step-by-step procedure for memory imaging (Hard drive) and which tool you prefer to use and why.	8 marks
Q.3 b	Attempt any one	7 marks
Q3 b	I. Write down the design principles of the Windows 10 operating system.	7 marks
	OR	
	II. With a neat diagram briefly explain Windows 10 architecture.	7 marks

National Forensics Sciences University, Goa Campus

TA-1 Examination

Program Name – M.Sc. [redacted] DFIS Sem – I Date- 09/09/2024
Subject Name- Computer Forensics Subject Code- CTMSDFIS SI P1
Time- 45 minutes Max. Marks- 25
Instructions - 1) Answer all questions. 2) Assume suitable data.

Q.1	Answer the following:-	5 marks
	With the help of neat diagram, explain the parts of a HDD.	
Q.2	Answer as per the instruction:-	5 marks
	I. State True/False: In SSD, the file deletion is dependent upon over-writing. F	1 mark
	II. State the path in Windows Registry Editor, to derive the time zone of the given machine.	1 mark
	III. Define resident and non-resident files.	1 mark
	IV. State True/False: In HDD, a file deletion is just indicated at its record MFT, although the file continues to reside still. T	1 mark
	V. Solve the number system conversion : (1101010)2=(?)8	1 mark
Q.2	Answer any 3 questions (3x5 marks each)	15 Marks
	i. Which are the digital evidences in crime? How are they helpful in the verdict?	5 marks
	ii. Why is there a sudden increase in online fraud and how to differentiate between online & offline fraud?	5 marks
	iii. Give a brief description of the incident handling process given by Cichonski and Kral.	5 marks
	iv. Give the details of the partitioning and formatting in HDD.	5 marks