National Forensic Sciences University
School of Cyber Security & Digital Forensics
M.Sc. DFIS (2024-25)

Subject Code: (CTMSDFIS SII P3) **Date: 10/02/2025**

Subject Name: Malware Analysis & Forensics

Exam: TA- I Examination (Feb 2025) **Time: 03:00 PM to 03:45 PM**

Q1. Answer the following questions in brief. (Answer any 3) [15 Marks]

1. Describe the different types of malware and methods of malware analysis, and explain how Clam AV virus signatures are utilized for malware detection.

2. Describe the working algorithm FLOSS tool with one use case.

3. Describe the X86 CPU architecture, including the processing unit (CPU) and memory (register and stack).

4. Translate a simple C code snippet to assembly and explain the underlying constructs.

5. Discuss the YARA signatures, providing an example of rule formation.

Q2. Answer the following questions in word(s). (Attempt all) [10 Marks]

1. _________ type of malware is known for disguising itself as a legitimate program.

2. List two tools primarily used to set up a malware analysis laboratory.

3. Hashing is used in malware analysis to _________.

4. _________ section of a PE file contains the executable code.

5. _________ is the primary function of Clam AV Virus Signature.

6. _________ tool is used for capturing and analyzing network traffic in malware analysis.

7. List two components present in X86 CPU architecture.

8. List any two tools used for debugging and analyzing executable files.

9. List any two tools used for creating virus signatures and give one example showing its use case.

10. List one tool used for live memory analysis and give one example showing its use case.

Enrollment No.:_____

NATIONAL FORENSIC SCIENCES UNIVERSITY

School of Cyber Security & Digital Forensics

End Semester Examination - May-2025

Subject Name: Malware Analysis **Total Marks: 50**

Perform kernel debugging with WinDBG to analyze a rootkit.

Explain how forensic analysis helps in attribution and legal proceedings.

Seat No.: ________ Enrolment No.___________

NATIONAL FORENSIC SCIENCES UNIVERSITY

Semester End Examination (April – 2025)
M.Sc. Digital Forensics & Information Security
Semester – II

Subject Code: CTMSDFIS24 SII P3 **Date:** 28/04/2025
Subject Name: Malware Analysis & Forensic
Time:10:30am To 01:30pm
Total Marks: 100

Instructions:

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

			Marks
Q.1		**Attempt any three.**	
	(a)	Explain the Process Explorer tool in Detail.	**08** 5
	(b)	What Volatility Framework? Explain any 5 command of it.	**08**
	(c)	What is the use of Sand Box in Malware Analysis. Explain one Sand box.	**08** 5
	(d)	Discuss the role of Dynamic Analysis in Malware.	**08** 5
Q.2		**Attempt any three.**	
	(a)	What is Malware?Explain any 4 Malware with example.	**08** 5
	(b)	What is Register?Expalin General Purpose Register in Details.	**08**
	(c)	Explain the structure of PE files with Diagram, focusing on the Importance of headers and sections in malware analysis.	**08** 4
	(d)	What is DLL?Explain it Types and Role in Malware Analysis.	**08** 3
Q.3		**Attempt any three.**	
	(a)	What is Yara rule?How to Write it?Explain it one example.	**08**
	(b)	Explain the purpose and basic usage of the reverse engineering tool IDA Free.	**08** 3
	(c)	Discuss the Lab setup for Malware Analysis in Virtual Machine.	**08** 4
	(d)	Explain various Flags in x86 CPU architecture.	**08** 4
Q.4		**Attempt any two.**	
	(a)	What are the artefact you can cover from Linux System.	**07** 4
	(b)	Explain how Dependency Walker can be used to analyse .dll files.	**07** 3
	(c)	What is DLL Injection?Explain DLL Injection Methods.	**07**
Q.5		**Attempt any two.**	
	(a)	Discuss any Case Study of Malware Attack.	**07** 3
	(b)	What is a Debugger, and Explain its various types?	**07**
	(c)	Explain Hooking Injection in details	**07** 3

--- End of Paper---

Enrolment No.____________________

NATIONAL FORENSIC SCIENCES UNIVERSITY

School of Cyber Security & Digital Forensics

M.Sc. DFIS Sem - II

Mid Semester Examination - March-2025

Subject Code: (CTMSDFIS SII P3) **Date: 18/03/2025**

Subject Name: Malware Analysis & Forensics

Time: 11:00 AM to 12:30 AM **Total Marks: 50**

Instructions:

1. **Make suitable assumptions wherever necessary.**
2. **Figures to the right indicate full marks.**

Q.1 Answer the following / Define the following **10 x 2 (Marks)=20**

i) What is the forensic importance of malware analysis?

ii) Mention one behavior commonly observed in malware.

iii) What is the significance of a virtual machine in a malware analysis lab?

iv) List two reverse engineering tools used for malware analysis.

v) Define the role of PE (Portable Executable) file headers.

vi) What is the purpose of a malware signature?

vii) What is the role of Process Monitor?

viii) Mention one use of Wireshark.

ix) What is IDA Pro used for?

x) Translate a basic C code example into assembly (simplified representation).

Q.2 Answer the following questions in short (any 5 6) **4 x 5 (Marks)=20**

i) Describe the role of Dependency Walker in malware analysis.

ii) What are YARA signatures, and how are they used in malware detection?

iii) Explain the usage of Process Explorer in identifying malware behavior.

iv) Differentiate between kernel mode and user mode debugging.

v) Discuss the significance of packers in malware and the process of unpacking them.

vi) Discuss anti-disassembly techniques employed by malware.

Q.3 Answer the following in detail (any 2) **2 x 5 (Marks)=10**

i) Explain how sandboxes are utilized to safely monitor malware behavior.

ii) Explain debugging features such as breakpoints, exceptions, and program execution modification in detail.

iii) Analyze the differences between anti-debugging and anti-virtual machine techniques.
