Enrolment No./Seat No.:

GUJARAT TECHNOLOGICAL UNIVERSITY

M.SC INTEGRATED - SEMESTER - VIII EXAMINATION - SUMMER 2025

Subject Code: 1380309 **Date: 19-05-2025**

Subject Name: Malware Analysis

Time:10:30 AM TO 01:00 PM **Total Marks: 70**

Instructions

1. Attempt all questions.

2. Make suitable assumptions wherever necessary.

3. Figures to the right indicate full marks.

4. Use of simple calculators and non-programmable scientific calculators are permitted.

			Marks
Q.1	**(a)**	Define malware and list its common types.	**03**
	(b)	Compare worms and trojans with examples.	**04**
	(c)	Evaluate the evolution of malware and discuss how malware threats have adapted over time.	**07**
Q.2	**(a)**	Explain the concept of a logic bomb.	**03**
	(b)	What is the difference between static and dynamic malware analysis?	**04**
	(c)	Justify the importance of understanding OS security concepts for malware analysis.	**07**
		OR	
	(c)	Create a step-by-step guide for performing static analysis on an unknown executable.	**07**
Q.3	**(a)**	Describe any two anti-static analysis techniques.	**03**
	(b)	Explain the structure of a virtual machine used in malware analysis.	**04**
	(c)	What are the common malware threats that exist today? Give a short description of each	**07**
		OR	
	(a)	Define obfuscation and explain its role in malware.	**03**
	(b)	Explain how anti-static analysis techniques like packing and obfuscation hinder analysis.	**04**
	(c)	What are C code constructs commonly found in disassembled malware?	**07**
Q.4	**(a)**	Define breakpoints and their role in OllyDbg.	**03**
	(b)	Describe how Wireshark can be used in analyzing network activity of malware.	**04**
	(c)	Define file-less malware and explain its execution mechanism.	**07**

OR

(a) What are system calls and why are they important in dynamic analysis? **03**

(b) How can debuggers be used to unpack malware from memory? **04**

(c) Explain the use of memory forensics in identifying and analyzing advanced malware **07**

Q.5 (a) Define metamorphic malware. **03**

(b) Compare signature-based and non-signature-based detection methods. **04**

(c) What is app sandboxing and how does it protect Android systems? **07**

OR

(a) What is code injection? **03**

(b) Analyze the behavior of DroidKungFu malware. **04**

(c) Explain smartphone app permissions and how misuse leads to malware infections. **07**

***