

GUJARAT TECHNOLOGICAL UNIVERSITY**BE- SEMESTER-V (NEW) EXAMINATION – WINTER 2024****Subject Code:3154803****Date:02-12-2024****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. Simple and non-programmable scientific calculators are allowed.

		MARKS
Q.1	(a) What is malware? What is malware analysis? Explain in brief.	03
	(b) List out the reasons to perform malware analysis.	04
	(c) Define following terms: (1) Ransomware (2) Backdoor (3) Botnet (4) Rootkit (5) Scareware (6) Launcher	07
Q.2	(a) What is the full form of API? What is the role of API in malware analysis? Explain in brief.	03
	(b) Differentiate between packed and obfuscated malware.	04
	(c) What is the interpretation of term "MZ" in PE File Format? Describe the PE Headers and Sections with suitable figures.	07
	OR	
	(c) Explain any five common DLL files functionalities.	07
Q.3	(a) Explain User mode debugging.	03
	(b) How does WinDbg is applicable to analyze malware? Explain with suitable example.	04
	(c) What hex values "Magic" field in Optional header is set to? How to determine total size of header in Disk? Explain with suitable example.	07
	OR	
Q.3	(a) Explain Kernel mode debugging.	03
	(b) How ransomware works? Explain with suitable example.	04
	(c) How virus works? How to apply prevention mechanism to defend virus attacks?	07
Q.4	(a) Define Windows API with its functionalities.	03
	(b) Sketch the structure of virtual machine and illustrate the risk of using VMware for Malware Analysis.	04
	(c) What is the full form of .DLL file? How Kernal32.DLL is applicable to identify IoC in malware analysis? Explain with suitable example.	07
	OR	
Q.4	(a) Differentiate between Hook Injection and APC Injection.	03
	(b) Why does malware analyst need to perform dynamic analysis?	04

- (c) How does malware establish persistence? Explain it with suitable example of malware with CVE details. **07**
- Q.5** (a) Write down the functionalities of kernel32.dll file. **03**
- (b) Define polymorphic malware and metamorphic malware with suitable example. **04**
- (c) How Wireshark can help to understand the malware behaviour in network communication? How to collect the Indicators of Compromise (IOCs) (such as File Hashes, Host IP Address, Domain Name, Host Name MAC address of Host) for malware using Wireshark? **07**
- OR**
- Q.5** (a) List the functionalities of Process Monitor. **03**
- (b) Explain MITRE ATT&CK Framework with suitable diagram. **04**
- (c) Distinguish Signature-based Vs. Non-signature Based Malware Detection Techniques. **07**
