GYANMANJARI INNOVATIVE UNIVERSITY

GYANMANJARI INSTITUTE OF TECHNOLOGY

M. Tech.-End Semester Examination (ESE)- Summer-2026

Enrollment No.: _____

Subject Code: METCS12510 | **Date: 16-05-2026**

Subject Name: Malware Analysis | **Semester: 02**

Time: 10:30 AM to 01:30 PM | **Total Marks: 100**

Instructions:

1. **Question No. 1 is compulsory.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

			Marks
Q.1	(a)	Define malware and explain different types of malwares with examples.	10
	(b)	Explain x86 architecture including registers, memory, and instruction formats.	10
Q.2	(a)	Explain live malware analysis and dead malware analysis.	10
		OR	
	(a)	Describe credential stealers and their working mechanisms.	10
	(b)	Explain signature-based malware detection techniques.	10
		OR	
	(b)	Discuss types of mobile malware and their distribution procedures.	10
Q.3	(a)	Discuss malware sandboxing and monitoring using Process Monitor.	10
	(b)	Discuss persistence mechanisms and privilege escalation techniques used by malware.	10
		OR	
Q.3	(a)	Discuss invariant inference in malware detection.	10
	(b)	Analyze malware in malicious mobile applications.	10
Q.4	(a)	Compare signature-based and non-signature-based detection techniques.	10
	(b)	Explain covert malware launching techniques such as launchers and process replacement.	10
		OR	
Q.4	(a)	Explain Android security architecture and APK file structure.	10
	(b)	Propose a framework for detecting deepfake content in digital forensics.	10
Q.5	(a)	Evaluate the role of AI and machine learning in digital forensics.	10
	(b)	Explain packet sniffing using Wireshark in malware analysis.	10
		OR	
Q.5	(a)	Explain the Portable Executable (PE) file format with headers and sections.	10
	(b)	Describe the evolution of malware and how attack techniques have changed over time.	10