Gandhi Institute of Engineering and Technology University, Odisha, Gunupur
(GIET University)

B. Tech (Eighth Semester – Regular/Supplementary) Examinations, April – 2026

21BCSPE48001/22BCSPE48011 – Malware Analysis

(CSE)

Time: 3 hrs Maximum: 70 Marks

(The figures in the right hand margin indicate marks)

PART – A **(2 x 5 = 10 Marks)**

	Q.1. Answer ***ALL*** questions	CO #	Blooms Level
a.	What are the primary goals of malware analysis?	CO1	K1
b.	List any four common types of malware and give one characteristic of each.	CO1	K2
c.	What are the risks of using VMware for malware analysis?	CO2	K1
d.	Why is disassembly important in malware analysis?	CO3	K3
e.	What is IDA scripting?	CO4	K1

PART – B **(15 x 4 = 60 Marks)**

	Answer ***ALL*** the questions	Marks	CO #	Blooms Level
2. a.	Describe the different malware analysis techniques, including static analysis, dynamic analysis, and behavioural analysis. Compare their advantages and limitations.	8	CO1	K1
b.	How can a combination of these techniques improve the effectiveness of malware detection?	7	CO1	K3
	(OR)			
c.	How hashing techniques (MD5, SHA-1, SHA-256) are used as fingerprints for malware identification ?	8	CO1	K3
d.	Explain the structure of the Portable Executable (PE) file format.	7	CO1	K1
3.a.	Describe the step-by-step process of creating a secure malware analysis machine.	8	CO2	K2
b.	Discuss the role of the hypervisor, virtual hardware components, and guest operating systems.	7	CO2	K1
	(OR)			
c.	How registry monitoring contributes to malware analysis?	8	CO2	K3
d.	Describe the use of tools like Regshot to compare registry snapshots before and after malware execution.	7	CO2	K1
4.a.	Explain the process of disassembling an executable, including linear sweep and recursive traversal techniques	8	CO3	K2
b.	Compare their advantages and limitations in analysing complex binaries.	7	CO3	K4
	(OR)			
c.	What are the techniques for navigating and manipulating disassembly in IDA?	8	CO3	K1
d.	Explain how to Navigate functions and cross-references, Rename variables and functions, Add comments and annotations and Modify disassembly output.	7	CO3	K2
5.a.	Describe the graphical capabilities of IDA, including graph view and visualization of control flow.	8	CO4	K1
b.	Compare graphical mode with console mode IDA.	7	CO4	K4
	(OR)			
c.	Discuss real-world applications of reverse engineering using IDA in vulnerability analysis and malware research.	8	CO4	K1
d.	Provide an overview of the Android operating system and its security model.	7	CO4	K2

--- End of Paper ---