Reg No.:_____ Name:_____

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech Degree S6 (R,S) Examinations April 2026 (2019 Scheme)

Course Code: CCT352
Course Name: MALWARE FORENSICS

Max. Marks: 100 Duration: 3 Hours

PART A

Answer all questions, each carries 3 marks. Marks

1	What are the types of fingerprinting techniques?	(3)
2	Compare Static and Dynamic analysis.	(3)
3	What are the major steps done in dead malware analysis?	(3)
4	Define the details that can be track from registry during malware analysis	(3)
5	How a signature-based malware detection technique works?	(3)
6	List the steps in the process of packing in packed malware signatures.	(3)
7	List the tools used to identify users logged on the windows system.	(3)
8	What are guidelines to preserve the volatile data for malware analysis?	(3)
9	Define post-mortem forensics.	(3)
10	How we can Inspect Auto-starting Locations, Configuration Files, and Scheduled Jobs in Linux system?	(3)

PART B

Answer one question from each module, each carries 14 marks.

Module I

11	a)	Explain in detail the different types of Malware Analysis Techniques.	(8)
	b)	What is antivirus scanning? define its different types of scanning	(6)

OR

12	a)	Briefly describe the evolution of malware.	(6)
	b)	Explain the dynamic analysis tools used in malware analysis.	(8)

Module II

13	a)	Compare the live and dead malware analysis.	(6)
	b)	Explain the anti-dynamic analysis and its methods.	(8)

OR

14	a)	Compare kernel vs user mode debugging	(6)

	b)	How to perform packetsniffing using wireshark? Explain.	(8)

Module III

15	a)	Differentiate metamorphic and polymorphic malware signatures	(6)
	b)	Describe the working of similarity-based malware detection technique.	(8)

OR

16	a)	Explain the invariant inferences in malware detection techniques.	(6)
	b)	Compare signature-based and non-signature-based malware techniques	(8)

Module IV

17	a)	Explain the process of Forensic Preservation of Select Data on a Live Linux System	(6)
	b)	Describe the process of collecting volatile data from a Linux system.	(8)

OR

18	a)	Explain the process of Non-Volatile Data Collection from a Live Windows System	(8)
	b)	Describe the process of identifying drives and services while collecting volatile data from a live windows system.	(6)

Module V

19	a)	"To provide the necessary focus and ultimately locate key evidence, digital investigators employ a number of techniques". Explain	(8)
	b)	How we can gather data for malware discovery such as examine logs, keyword searching and review user accounts in windows system?	(6)

OR

20	a)	Explain the process of examining file system during malware discovery in a live Linux system.	(6)
	b)	How we can gather data for malware discovery such as Review Installed Programs, Examine Prefetch Files, Inspect Executables and Examine Logs in Linux system?	(8)

****