Reg. No. : | | | | | | | | | | | | |

Question Paper Code: U9873

B.E./B.Tech. DEGREE EXAMINATION, APR/MAY 2025

Open Elective

21UIT973- CYBER FORENSICS AND MALWARE

(Common to ALL Engineering Branches)

(Regulations 2021)

Duration: Three hours | Maximum: 100 Marks

Answer ALL Questions

PART A - (10 x 2 = 20 Marks)

1.	Explain Military Computer Forensics Technology.	CO1- U
2.	What is Forensic Analysis?	CO1- U
3.	List the types of DOS attacks.	CO1- U
4.	Define Network Forensics.	CO1- U
5.	Explain security strategies for web applications.	CO1- U
6.	Investigate Static and Dynamic IP address for any network oriented problems.	CO2-App
7.	Explain about cell phone crimes.	CO1- U
8.	What is android security?	CO1- U
9.	Computer running slower than usual, and some files are missing. Which two malware functionalities are most likely at play in this scenario?	CO2-App
10.	What are Backdoors? Give an example.	CO1- U

PART – B (5 x 16= 80 Marks)

11.	(a)	Discuss about the step by step process of the forensic analysis using scientific method.	CO1- U	(16)
		Or		
	(b)	Briefly explain about information security investigations.	CO1- U	(16)
12.	(a)	Use the techniques to detect and investigate DOS attacks and explain the situations to the organizations.	CO2- App	(16)
		Or		
	(b)	Apply various types of DoS Attacks for different scenarios.	CO2- App	(16)

13.	(a)	Explain about the Static and Dynamic IP addresses in a detailed manner.	CO1- U	(16)
		Or		
	(b)	Give some detailed explanations of web attacks investigations.	CO1- U	(16)
14.	(a)	Given a scenario where an Android device is compromised through a malicious app exploiting excessive permissions, evaluate the effectiveness of Android's security features such as App Sandbox and Runtime Permissions in preventing this. How would you apply best practices for securing sensitive data on such a device while ensuring a balance with user experience?	CO2- App	(16)
		Or		
	(b)	In a forensic investigation of an Android device, analyze the application of different data extraction techniques such as logical, physical, and file system extraction. How would you decide which technique to use based on the device's condition and encryption status, and what challenges might you face during the process?	CO2- App	(16)
15.	(a)	List the different types of malware functionality and explain every type in detail.	CO1- U	(16)
		Or		
	(b)	Explain in detail about the Backdoors and its causes in Cyber Forensics.	CO1- U	(16)