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

Question Paper Code: U9873

B.E./B.Tech. DEGREE EXAMINATION, NOV 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 information security investigations.	CO1- U
2.	Explain the steps of scientific method in forensic.	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.	List the Non-signature based techniques.	CO1- U
10.	Explain about Machine Learning Methods.	CO1- U

PART – B (5 x 16= 80 Marks)

11.	(a)	Apply the principles of risk management frameworks to analyze the potential impact for a hypothetical data breach scenario involving the theft of customer financial data from a large e-commerce platform.	CO1- U	(16)
		Or		
	(b)	You are a cyber security analyst investigating cyber attacks. Outline three internet tracing methods, explain their advantages/disadvantages, apply them to the scenario, and discuss the ethical and legal considerations of using these methods.	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)	Give some detailed explanations for Web Attacks Investigations.	CO1- U	(16)
		Or		
	(b)	Explain about the Static and Dynamic IP addresses in a detailed manner.	CO1- U	(16)
14.	(a)	In a forensic investigation involving a suspect's Android device, describe how you would set up the environment for data acquisition while ensuring the integrity of the evidence. Discuss the tools and methods you would use for preserving data from encrypted devices, and how you would handle potential challenges during the extraction process.	CO2- App	(16)
		Or		
	(b)	In the case of a deleted file recovery from an Android device, evaluate the effectiveness of different data recovery techniques such as file carving and the use of root access. How would you approach the recovery of encrypted or fragmented data, and what are the potential limitations of these techniques in real-world forensic investigations?	CO2- App	(16)
15.	(a)	Explain in detail about the Backdoors and its causes in Cyber Forensics.	CO1- U	(16)
		Or		
	(b)	Briefly explain the steps for preventing systems from Credential Stealers.	CO1- U	(16)