Code No.: CY733PE | R20 | H.T.No. | | | 8 | R | | | | | |

CMR ENGINEERING COLLEGE: : HYDERABAD
UGC AUTONOMOUS
IV–B.TECH–I–Semester End Examinations (Regular) - November- 2024
CYBER FORENSICS
(CSC)

[Time: 3 Hours] **[Max. Marks: 70]**

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 20 marks. Answer all questions in Part A.
Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b, c as sub questions.

PART-A **(20 Marks)**

1.	a)	State one activity performed after detecting an incident.	[2M]
	b)	Identify two major types of cyber crime.	[2M]
	c)	Identify one type of volatile data that should be collected from a Windows system during initial response.	[2M]
	d)	State one tool commonly used to collect volatile data from a Windows system.	[2M]
	e)	State the primary goal of network forensics	[2M]
	f)	Define Honeynet Project, and how does it support cyber security efforts.	[2M]
	g)	List responsibilities of an e-mail server in processing e-mails.	[2M]
	h)	Identify the primary objective of mobile device forensics.	[2M]
	i)	How does NTFS handle file permissions compared to FAT32?	[2M]
	j)	Name tools used for whole disk encryption in Windows systems.	[2M]

PART-B **(50 Marks)**

2.	Compare worms and viruses in terms of their propagation methods, payloads, and impacts. Explain how these malware types can be mitigated effectively.	[10M]
	OR	
3.	Describe the concept of incident response and discuss the primary goals of an effective incident response methodology.	[10M]
4.	Discuss the legal and technical requirements that make a forensic duplicate admissible as evidence in court.	[10M]
	OR	
5.	Explain the significance of initial response in forensic investigations and discuss how forensic duplication ensures the integrity of evidence throughout the investigation.	[10M]
6.	Describe how forensic data is validated to ensure authenticity and analyze the impact of improper validation on the outcome of an investigation.	[10M]
	OR	
7.	Identify key tools used for network forensic analysis and discuss how these tools help capture and interpret network traffic effectively.	[10M]
8.	Discuss the role of e-mail servers in forensic investigations and how they aid in gathering evidence.	[10M]
	OR	
9.	Explain the challenges involved in acquiring data from encrypted mobile devices.	[10M]
10.	Explain the various types of file systems used in Windows environments and analyze their strengths and weaknesses	[10M]
	OR	
11.	Discuss the concept of virtual machines and evaluate their benefits in testing and developing software in a controlled environment.	[10M]

****