K. J. Somaiya Institute of Technology, Sion, Mumbai-22
(Autonomous College Affiliated to University of Mumbai)

May-June 2024
(B.Tech)Program: Computer Engineering Scheme III
Regular Examination: LY Semester: VIII
Course Code: CEDLC8023 and Course Name: Digital Forensic
Date of Exam: 16/5/2024 Duration: 02.5 Hours Max. Marks: 60

Instructions:
(1)All questions are compulsory.
(2)Draw neat diagrams wherever applicable.
(3)Assume suitable data, if necessary.

		Max. Marks	CO	BT level
Q 1	Solve any six questions out of eight	12		
i)	What distinguishes the phase after detection of an incident from the initial response phase in incident response methodology?	2	CO1	U
ii)	What are two key differences in the forensic analysis of FAT and NTFS file systems?	2	CO2	U
iii)	Name two types of evidence commonly encountered in forensic investigations, and briefly describe one challenge in handling each type?	2	CO3	U
iv)	Briefly explain one challenge encountered when investigating live systems in a Windows environment?	2	CO5	U
v)	Explain briefly how email headers are used in the process of tracing emails in internet fraud investigations.	2	CO4	U
vi)	You are tasked with selecting a forensic duplication tool for an investigation. Identify and describe two key requirements you would consider when choosing the tool?	2	CO2	AP
vii)	List two guidelines for writing an effective computer forensics report	2	CO6	U
viii)	Identify and explain two different types of network attacks commonly encountered in cyber security?	2	CO4	U
Q.2	Solve any four questions out of six	16		
i)	Explain the importance of documenting investigative steps immediately and clearly in computer forensic investigations?	4	CO6	U
ii)	Imagine you are a cyber-security analyst. Describe the steps you would take to mitigate the risks posed by malware attacks on a corporate network?	4	CO1	AP
iii)	Explain the importance of preserving and recovering digital evidence in	4	CO3	U

K. J. Somaiya Institute of Technology, Sion, Mumbai-22
(Autonomous College Affiliated to University of Mumbai)

May-June 2024
(B.Tech)Program: Computer Engineering Scheme III
Regular Examination: LY Semester: VIII
Course Code: CEDLC8023 and Course Name: Digital Forensic
Date of Exam: Duration: 02.5 Hours Max. Marks: 60

	the context of cyber security incidents?			
iv)	Explain the role of intrusion detection systems (IDS) in safeguarding networks against different types of attacks?	4	CO4	U
v)	Discuss the significance of forensic duplication in ensuring the admissibility of digital evidence in legal proceedings.	4	CO2	U
vi)	Explain the importance of data analysis techniques in cyber security investigations?	4	CO5	U
Q.3	Solve any two questions out of three.	16		
i)	You are a cybersecurity analyst tasked with investigating a suspected breach in a corporate network. Upon initial analysis, you suspect that the breach may have originated from a compromised router. Describe the steps you would take to investigate the router and analyze network protocols involved in the incident.?	8	CO4	AP
ii)	Discuss and explain the ethical issues surrounding the use of hacker tools in cybersecurity, considering both their potential benefits and risks?	8	CO5	U
iii)	Discuss the proliferation of cybercrime facilitated by the Internet, focusing on the various types of cybercrimes and malware.	8	CO1	U
Q.4	Solve any two questions out of three.	16		
i)	Differentiate between FAT and NTFS file systems in terms of their structure and characteristics. How does forensic analysis of file systems aid in digital investigations?	8	CO2	U
ii)	Explain difference types of Evidence and Challenges in evidence handling	8	CO3	U
iii)	List and explain the basic template for a computer forensic report?	8	CO6	U

****