

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

May-June 2025		
(B. Tech / M. Tech.) Program: Computer Engineering Scheme I/II/IIB/III: III		
Regular/Supplementary Examination: LY Semester: VIII		
Course Code: CEDLC8023 and Course Name: Digital Forensics		
Date of Exam: 21/05/2024	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.				
Q. No.	Question	Max. Marks	CO	BT level
Q 1	Solve any two questions out of three: (05 marks each)	10		
a)	Describe the role of computers in modern criminal activities.		1	U
b)	Explain malware and its types with examples.		1	U
c)	Describe the layers of storage and their relevance in digital forensics.		3	U
Q 2	Solve any two questions out of three: (05 marks each)	10		
a)	A company detects unusual traffic on its server. Describe the steps of the initial response.		4	A
b)	Compare and contrast the commands used in Linux and Windows operating systems for obtaining process and network information.		5	U
c)	Describe forensic Report writing guidelines.		6	U
Q.3	Solve any two questions out of three. (10 marks each)	20		
a)	Explain the importance of forensic duplication in investigations.		2	U
b)	Explain the procedure for handling evidence.		3	U
c)	An e-commerce website is targeted by a DDoS attack. Explain the forensic response methodology.		4	A
Q.4	Solve any two questions out of three. (10 marks each)	20		
a)	Differentiate between complete imaging, partition imaging and logical imaging with example.		2	U

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

May-June 2025		
(B. Tech / M. Tech.) Program: Computer Engineering Scheme I/II/IIB/III: III ✓		
Regular/Supplementary Examination: LY Semester: VIII		
Course Code: CEDLC8023 and Course Name: Digital Forensics		
Date of Exam: 21/05/2025	Duration: 02.5 Hours	Max. Marks: 60

b)	Compare and contrast Volatility, Autopsy, and FTK Imager in terms of their purpose, interface, and usage in digital forensics investigations. Provide suitable examples where each tool is most effectively used.		5	U
c)	Explain expert report and forensic report with template of each in detail.		6	U
