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

May-June 2025
(B. Tech) Program: COMP/AID/EXTC/IT Scheme : I
Regular Examination: TY Semester: VI
Course Code: HCSC601 and Course Name: Digital Forensics (Cybersecurity Honors)
Date of Exam: 31/05/2025 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)	In what way DOS attacks prevent in an organization.		CO1	U
b)	How does the evidence flow model plays an important role in digital investigation.		CO2	U
c)	What do you mean by ram forensic analysis and why it is important.		CO3	U
Q 2	Solve any **two** questions out of three: (05 marks each)	10		
a)	Differentiate between incident handling and incident response.		CO4	U
b)	Explain the typical structure of a forensic investigation report.		CO5	U
c)	Describe the difference between packet flow analysis and statistical flow analysis with respect to traffic analysis.		CO6	U
Q.3	Solve any **two** questions out of three. (10 marks each)	20		
a)	You are a digital forensic investigator called to a corporate office following a suspected insider data breach. The suspect's workstation is powered on and connected to the company network. Apply the steps of performing live forensics on the system and also explain how you would collect volatile data and justify the tools or techniques you would use to preserve the integrity of the evidence.		CO4	Ap
b)	Explain various types of mobile communications and relate this to forensic investigation.		CO6	U
c)	Breakdown the steps involved in mobile acquisition with one use case.		CO6	An
Q.4	Solve any **two** questions out of three. (10 marks each)	20		

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

May-June 2025
(B. Tech) Program: COMP/AID/EXTC/IT Scheme : II
Regular Examination: TY Semester: V
Course Code: HCSC601 and Course Name: Digital Forensics (Cybersecurity Honors)
Date of Exam: 31/05/2025 Duration: 02.5 Hours Max. Marks: 60

a)	You are required to submit a digital forensic investigation report to a legal team. Describe how you would apply professional style and formatting to make your report clear and legally admissible. Discuss the use of headings, fonts, language style, inclusion of visuals (e.g., tables, screenshots), and citation practices.	CO5	Ap
b)	What are the major sources of evidence in mobile device? Explain with example.	CO6	U
c)	State the usage and analyze the importance of PsLoggedon, Netsessions, Logonsessions tools.	CO6	An

****