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

May-June 2023-24
(B.Tech) Program: Computer Engineering/Scheme IIB
Regular/Supplementary Examination: LY Semester: VI
Course Code: HCSC601 and Course Name: Digital Forensics (Honors)
Date of Exam: 29-05-24 Duration: 2.5 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)	Differentiate between computer viruses and worms	2	CO1	U
ii)	What is evidence flow model of digital investigation process	2	CO2	U
iii)	What is windows forensic volatile information?	2	CO3	U
iv)	List the contents of incident response lifecycle.	2	CO4	U
v)	How to preserve digital evidence with cryptography.	2	CO5	U
vi)	Describe in brief about network components and their forensic importance.	2	CO6	U
vii)	State the importance of report style & formatting in forensic investigation & report writing.	2	CO5	U
viii)	State the difference between network flow and statistical flow while analyzing the traffic over network evidence.	2	CO6	U
Q.2	Solve any four questions out of six.	16		
i)	Explain the incident timeline for cyber stalking.	4	CO1	U
ii)	Illustrate about assessment phase of forensic investigation process.	4	CO2	U
iii)	Write an overview on MAC as boot sequence.	4	CO3	U
iv)	How to do a duplication of a hard drive.	4	CO4	U
V)	Describe the term reproducible and stick to the facts w.r.t to reporting standards.	4	CO5	U
Vi)	Explain the mobile forensics with example.	4	CO6	U
Q.3	Solve any two questions out of three.	16		
i)	Illustrate the steps for Trojan attack with suitable example.	8	CO1	U

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

May-June 2023-24
(B.Tech) Program: Computer Engineering Scheme IIB
Regular/Supplementary Examination: LY Semester: VI
Course Code: HCSC601 and Course Name: Digital Forensics (Honors)
Date of Exam: Duration: 2.5 Hours Max. Marks: 60

ii)	Write a short note on 'finding IR talent'	8	CO4	U
iii)	Illustrate the concept of report content & organization with suitable case study.	8	CO5	U
Q.4	Solve any two questions out of three.	16		
i)	Demonstrate the steps for digital evidence investigation process with suitable case study.	8	CO2	U
ii)	Write a short note on a) Event logs b) Anatomy of disk drive	8	CO3	U
iii)	Explain the steps of packet capturing using TCP dump.	8	CO6	U

****