Reg No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

A Constituent Institution of Manipal University

II SEMESTER M.TECH. (COMPUTER SCIENCE AND INFORMATION SECURITY)

END SEMESTER REGULAR EXAMINATIONS, May 2023

SUBJECT: CYBER FORENSICS [CSE 5014]

REVISED CREDIT SYSTEM

(31/05/2023)

TIME : 3 HOURS **MAX.MARKS : 50 M**

Instructions to the Candidate

- Answer all **FIVE** full Questions.
- Missing data can be suitably assumed.

Q. No	Questions	M	CLO	Blooms Taxonomy Level
1.A	"The knowledgeable computer forensics professional should ensure that a subject computer system is carefully handled". Justify your answer.	3M	1	3
1.B	"Computer Forensics professionals should be able to successfully perform complex evidence recovery procedures with the skill and expertise that lends credibility to the case. " Justify your answer	5M	1	3
1.C	At what point should computer security professionals stop handling digital evidence and contact law enforcement?	2M	1	3
2.A	"As devices develop more capabilities, the threats are expected to grow more serious and frequent." Justify your answer.	3M	1	3
2.B.	Write the privacy issues, that has contributed to people's awareness by an internet.	4M	1	3
2.C	"IM management and security systems act as proxies for IM traffic going into the network, which imposes policies before letting traffic through." Justify your answer.	3M	1	3
3.A	Having looked at the biggest cybercrime across the globe, discuss the impact of any sort of cybercrime that persists even today.	2M	2	4
3.B	Having learnt about all sorts of crimes, suggest the measures an individual should adopt to avoid being a victim to any of these crimes.	4M	2	4
3.C	What do you think has been the most important cyber security incident in the recent past? Ascertain the threat and suggest appropriate measures for policy makers.	4M	2	3

4.A	The sales manager, A, of Company X leaves his job and soon after, clients of that company start receiving defamatory messages from A against Company X. How can you prove that mail originated from the sales manager in your capacity as the forensic examiner (FE).	3M	3	4
4.B	The trade secrets and sensitive information from a company were sold to a competing company. Employee X who is working in that company is suspected to have sold the information. Employee x claims that his system does not have any USB ports. Explain how such a suspicion was raised. How can it be proved that employee X was with the cybercrime?	3M	3	4
4.C.	List the mobile forensic tools; which mobile forensic tool is the best? Give the justifications.	4M	3	3
5.A	Assume that a machine has NTFS file system. How can you determine whether there is track fragmentation? Justify your answer.	3M	4	3
5.B	List and explain the crimes and probable location of evidence.	5M	4	3
5.C	With neat sketch, write the Stages in investigation of digital evidence.	2M	4	3

-ALL THE BEST-