HT NO: | 7 R | |

CMR TECHNICAL CAMPUS

UGC AUTONOMOUS

B. Tech. VIII Semester Regular End Examinations, April-2024 Cyber Forensics Department of CSM

Time: 3 Hours

Note

Max. Marks: 70

i. This Question paper contains Part- A and Part- B.

ii. All the Questions in Part A are to be answered compulsorily.

iii. All Questions from Part B are to be answered with internal choice among them.

PART-A

 $10 \times 02 = 20 \text{ Marks}$

				Marks	CO	BL
1.	a	What is the role of computers in a crime?		. 2	CO1	T.1
	b	Briefly Explain the Computer Forensics Services.		2		L1
		· · · · · · · · · · · · · · · · · · ·		2	CO1	L1
	c ·	Write about role of backup in the data recovery.		2	CO2	L1
	d	How does a duplication tool ensure the integrity and authenticity of the copied data?		2	CO2	LI
	e	What is computer forensic validation?		2	CO2	T 1
	f	Define Network forensics.			CO3	L1
			- 11	2	CO3	L1
	g.	What are the needs of computer forensic tools?		2	CO4	L1
	h	List the steps to Recovering data.		2	CO4	
		•		4	CO4	L1
	i	Define FAT and NTFS.		2	CO5	L1
	j	list the steps when the computer is turned on in NTFS		2	CO5	
		computers			CO3	L1

PART-B

 $5 \times 10 = 50 \text{ Marks}$

			Marks	CO	BL
2.	a	Explain Internet security architecture?	5	CO1	L2
	b	Discuss major components of incident response. OR	5	COI	L2
3	a	Write the goals of incident response in forensic science.	5	CO1	L1
	b	Explain in detail about Incident Response Methodology.	5	CO1	L2
4	a	Give the steps to duplicate and preservation of digital evidence.	. 5	CO2	L2
	ь	Explain Duplication Tool Requirements	5	CO2	L2
5	a .	What challenges may arise during the forensic duplication	5	CO2	L2

Subject	Code	: 20CS862PE SET-I	HT NO:	7 F	R	
	b	process, and how can they be mitigated? What is meant by a forensic duplicate (or quaduplicate) of a hard drive, and why is it impoforensics?	ulified forensic rtant in digital	5	CO2	L2
6	a	List and explain forensic data tools.		5	CO3	L2
	b	How are standard procedures developed for network OR	ork forensics?	5 ·	CO3	L2
7	a	Explain how to validate Forensic Data with an Ex	cample?	. 5	CO3	L2
	b	Write short notes on network forensic overview.		5	CO3	L2
8	a	List and Explain the five major categories for data analysis and recovery.	further refining	5	CO4	L2
	b	What do you understand by mobile device for OR	rensics. Explain	5	CO4	L2
9	a	How does email serve as a critical source of edigital investigations?	vidence in	5	CO4	L2
	b	Can you name some popular command-line for and describe their primary functions?	orensics tools	5	CO4	L2
10	a	Write short notes on Windows Registry		5	CO5	L2
	b	Explain the NTFS Encrypting File System		5	CO5	L2
		OR			- 000	LL
11	a	Analyze startup tasks of MS-DOS.		.5	CO5.	L2
	b	What is a virtual machine (VM), and how doe a physical machine?	s it differ from	. 5	CO5	L3
