Register Number:……..

KUMARAGURU
college of technology
character is life

B.E. / B.TECH. DEGREE EXAMINATIONS: APRIL / MAY 2023

(Regulation 2018)

Sixth Semester

COMMON TO ALL BRANCHES

U18CSR6214: Cyber Forensics

COURSE OUTCOMES

CO1: Apply security principles in the application layer

CO2: Explain computer forensics

CO3: Use forensics tools

CO4: Analyze and validate forensics data

Time: Three Hours **Maximum Marks: 100**

Answer all the Questions:-
PART A (10 x 2 = 20 Marks)
(Answer not more than 40 words)

1.	How does identify theft happen?	CO1	[K_1]
2.	Examine the factors to be considered to investigate an incident.	CO1	[K4]
3.	Identify the tools that create a forensic duplicate.	CO2	[K3]
4.	Discover the need to preserve the evidence.	CO2	[K_4]
5.	Determine whether you can seize computers and digital devices in processing crime.	CO2	[K_5]
6.	Compare verification and validation.	CO3	[K_2]
7.	Define Known File Filter.	CO3	[K_1]
8.	Discuss the role of E-mail in Investigations.	CO4	[K2]
9.	What are SIM Card Readers?	CO4	[K1]
10.	List out the addressing Data-hiding Techniques.	CO4	[K1]

Answer any FIVE Questions:-
PART B (5 x 16 = 80 Marks)
(Answer not more than 400 words)

11.		Discuss the traditional problems associated with computer crime.	16	CO1	[K_2]
12.		Analyze the systematic approach, assessments to be done and investigation process for the below case study. The police raided a suspected drug dealer's home and found a desktop computer, several USB drives, a tablet and a mobile in a bedroom. The computer was eventually bagged and tagged. The lead detective on the case wants you to examine the computer and mobile to find and organize data that could be evidence of a crime, namely contacts, text messages and photos. The acquisition officer gives you documentation of items that the investigating officers collected with the computer, including removable disks and flash drives. He also notes that the computer is a Windows 8 system, and the machine was running when it was discovered. Before shutting down the computer, the acquisition officer takes a snapshot of all open windows in the desktop and gives you the photo before shutting down the computer.	16	CO2	[K_4]
13.	a)	Describe the software/ hardware tools in current computer forensics tools.	8	CO3	[K_2]
	b)	Discuss the guidelines for processing law enforcement crime scenes.	8	CO3	[K_2]
14.		Illustrate the concepts of processing crime and incident scenes.	16	CO3	[K_2]
15.	a)	Determine the type of data to analyze in a computer forensics investigation.	8	CO4	[K_4]
	b)	Illustrate the procedure for acquiring data from cell phones and mobile Devices	8	CO4	[K_2]
16.		Explain the basic concepts of mobile device forensics.	16	CO4	[K_2]

****