R18 Regulation *Subject code: 2E7EH*

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

(Autonomous, Accredited by NAAC with 'A' Grade)

B.Tech VII Semester Regular/Supplementary Examinations, November 2022

COMPUTER FORENSICS
(Professional Elective)

(Computer Science and Engineering)

Maximum Marks: 70 Date:05.12.2022 Duration: 3 hours

Note: 1.This question paper contains two parts A and B.
2. Part A is compulsory which carries 20 marks. Answer all questions in Part A.
3. Part B consists of 5 Units. Answer any one full question from each unit which carries 10M.
4. Each question carries 10 marks and may have a, b, c, d as sub questions.

Part-A

All the following questions carry equal marks (10x2M=20 Marks)

1 Define Traditional Computer Crime and What are the motivations for computer intrusion in contemporary society?
2 Point out which CF Techniques are being used for Investigations.
3 Illustrate the Criminal and Civil proceedings which can be used as computer Forensics Evidence.
4 Summarize the general tasks investigators perform while working with Digital Evidence.
5 Illustrate the three items should be on an evidence custody form.
6 Demonstrate the features of Forensic Duplication and Investigation & also outlinethe problems and challenges forensic examiners face when preparing and processing investigations, including the ideas and questions they must consider.
7 List the tools used in validation and discrimination in Forensics.
8 Decide the roles of Client and Servers in E-mail investigations.
9 How will you create "New Technology File System"?
10 Differentiate Master Boot Record (MBR) and Master File Table (MFT).

Part-B

Answer All the following questions. (5X10M=50Marks)

11 Explain about the various types of CF techniques and how to apply the CF techniques in various applications. 10M

OR

12 Describe in detail about the following:-
(i) Understanding Data Recovery Workstations and software 5M
(ii) Preparing for a Computer Investigation. 5M

13 Explain the different types of evidence collection methods using real-time scenario. 10M

OR

14 Experiment with the legal aspects of collecting and preserving computer forensic evidence. 10M

15	Give a brief description of the following data-hiding techniques: (i) Hiding Partitions (ii) Bit-Shifting (iii) Marking Bad Clusters	 3M 3M 4M
	OR	
16	Examine the processes involved in preparing for a search and also the seizing procedure for the Digital Evidence.	10M
17	Analyze how mobile devices play a crucial role in forensics by : (i) Basics of mobile Forensics (ii) Inside Mobile Devices (iii) Inside PDAs	 3M 3M 4M
	OR	
18	Apply validating and testing forensics software with real-time applications.	10M
19	Describe the following mechanisms in detail: (i) NTFS data streams, Encrypting file systems. (ii) NTFS compressed files.	 5M 5M
	OR	
20	A. Discuss the MS-DOS Startup Tasks and other Disk OperatingSystems in detail. B. Express in detail about how the understanding of NTFA, FAT,FAT32 in the system plays a crucial role in Cyber Forensics.	 5M 5M