R18 Regulation *Subject code:2E7EH*

TKR COLLEGE OF ENGINEERING AND TECHNOLOGY

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

B.Tech VII Semester Supplementary Examinations, April 2024

COMPUTER FORENSICS

(Computer Science and Engineering)

Maximum Marks: 70 Date:27.04.2024 **Duration: 3 Hours**

Note: **1.This question paper contains two parts A and B.**
2. Part A is compulsory which carries 10 marks. Answer all questions in Part A.
3. Part B consists of 10 questions. Answer any 5 questions which carries 12M.
4. Each question carries 12marks and may have a, b, c, d as sub questions.

Part-A

All the following questions carry equal marks (10X2M=20 Marks)

1 Why is it necessary to maintain professional conduct during computer investigation?

2 Why should companies appoint an authorized requester for computer investigations?

3 What is Data Recovery?

4 What is the process of Data Seizure?

5 What is preservation of Digital crime scene.

6 Why are most of the companies. Industries are ill equipped to investigate?

7 Define SMTP.

8 Define e-mail violation.

9 What is file sharing.

10 List tools used to validate forensics data.

Part-B

Answer all the questions **(5X10M=50Marks)**

11 Explain Data Collection, Analysis, Presentation and their role in Computer forensic Investigations. [10]

OR

12 Explain the role of Forensics in Computer Forensics. [10]

13 Explain any four challenges faced by a computer forensic professional while data backup. [10]

OR

14 Explain claim of custody duplication and preservation of digital information. *[10]*

15 Develop the standard procedure for network forensics. [10]

OR

16 Discuss storing digital evidence procedure. [10]

17 Explain the role of e-mail in investigation. [10]

OR

18 What are the International Principles Against Damaging of Computer Evidence? [10]

19 Examine the NTFS disks in terms of disk encryption. [10]

OR

20 Write a brief note on disk and data capture tools used in computer forensics along with one example. [10]