M.Sc.(IT)(Sem-IV)   July-2023

Information Technology : Cyber Forensics (R-2021)

(2 Hours)   **[Total Marks: 60]**

N. B.:

(1) **All** questions are **compulsory**.
(2) Make **suitable assumptions** wherever necessary and **state the assumptions** made.
(3) Answers to the **same question** must be **written together**.
(4) Numbers to the **right** indicate **marks**.
(5) Draw **neat labeled diagrams** wherever **necessary**.
(6) Use of **Non-programmable** calculators is **allowed**.

Q1. Attempt the two of the following.   **12 Marks**

• Define computer forensic. Also explain advantages and disadvantages of Computer forensics.

• Briefly explain the five critical steps in computer forensics.

• Explain the examples of electronics evidence in details.

• What procedure will be followed by the first responder for cyber forensics?

Q2. Attempt two of the following   **12 marks**

• Explain Gaseous suppression.

• Explain different Data Acquisition Tools?

• Explain how perform digital forensics on a windows-based machine.

• What is Investigating System State Backups?

Q3. Attempt two of the following.   **12 marks**

• Briefly explain the EnCase? Explain the features of EnCase. What are the Steps to Create a Case in

EnCase?

• What are the step to recovering the deleted files using Recuva?

• Explain using access data FTK and EnCase for investigation?

• Explain steganography and also explain about the type of Steganography?

Q4. Attempt two of the following.   **12 marks**

- Explain Network Information-Gathering Tools

- How to Tracking Security Policy Violations? Explain in details.

- What are the Advantages of a Wireless Network?

- What is Web Attacks?

Q5. Attempt two of the following.   **12 marks**

- What is Email? Explain working of Email system

- Explain in detail "How to investigate the Email Crime."

- Explain Rooting an Android Device. Also explain the advantages and disadvantages of rooting.

- Explain how we perform Image Extraction of an Android Device

****