

M.Sc IT Part II (Sem-IV) 75:25 dt 10/01/2023

(3Hours)

[Total Marks: 75]

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 labelled diagrams wherever necessary.

(6) Use of Non-programmable calculators is allowed.

Q1. Attempt the three of the following.

15 Marks

- Explain evidence assessment in the cyber forensic.
- Explain the forensic process to be followed by the first responder.
- Explain the system administrator and Forensic personnel under the first responder role.
- Describe the documenting and reporting in cyber forensic.
- Write a short note on LAN or WAN planning under electrical and power plant.

Q2. Attempt the three of the following.

15 Marks

- What is duplication platforms? Explain in details.
- How do we will set up a computer lab for computer forensics?
- Explain the laboratory strategic planning for strategic planning for business.
- Explain FTK Imager under data acquisition tools.
- Explain locating and gathering evidence on a windows host for volatile evidence.

Q3. Attempt three of the following.

15 marks

- What is EnCase? Give the steps of investigation using EnCase.
- Explain OSI model with physical layer.
- Explain the process of recovering the deleted partitions.
- What is steganalysis? Explain Methods of detecting the Steganography.
- Explain the methods used for cracking or attacking passwords.

Q4. Attempt three of the following.

15 marks

- Explain the wireless access point in detail.
- Explain the process of capturing logs and correlating to the events.
- Write a short note on network address and NAT.
- What are the basics of wireless? Explain.
- What do you mean by wireless penetration testing? Explain.

Q5. Attempt three of the following.

15 marks

- Why is documentation so essential? Doesn't simply the verification impart?
- Write a short note on Mobile Forensic.
- Explain the working of email system with the help of diagram.
- How to investigate email crime?
- What is the requirement of report? What are the types of Investigation report?
