

Time: 3 hours

Max. Marks: 80

Instructions:

- 1) Only **Four question** need to be solved.
- 2) All question carries equal marks.
- 3) Illustrate your answers with neat sketches wherever necessary.
- 4) Figures to the right indicate full marks.
- 5) Assume suitable additional data, if necessary and clearly state it.
- 6) All sub-questions of the same question should be grouped together.

- Q.1** (a) What is Evidence? Explain the various types of digital evidence. **05**
(b) Discuss the significance of ICCID, IMSI, MSISDN and LAI. **05**
(c) What are the potential challenges or limitations associated with conducting Windows registry analysis? **05**
(d) Define digital forensics and explain its goal in detail. **05**
- Q.2** (a) What constitutes a computer security incident? What objectives are pursued through incident response? Elaborate on the concept of CSIRT. **10**
(b) What are the challenges of acquiring Volatile Memory (Live Acquisition)? Give the tools used for Acquiring Volatile Memory. **10**
- Q.3** (a) What are the potential risks involved in hard drive imaging during digital forensic investigations? Explain. **10**
(b) How does Autopsy utilize advanced file carving techniques to recover deleted or fragmented files? **10**
- Q.4** (a) Explain the process of conducting a static acquisition of digital evidence from a storage device. **10**
(b) Explain in detail the process of reviewing pertinent logs in Unix systems investigation. **10**
- Q.5** (a) How does forensic analysis of Microsoft Edge differ from other Web browsers, such as Google Chrome or Mozilla Firefox? **10**
(b) What is GPS forensic? Explain the structure of the GPS device. Explain GPS Exchange Format (GPX). **10**
- Q.6** (a) What is data carving, and how does it contribute to digital forensic investigations? **10**
(b) Explain what SIM cards Forensics means. Explain the SIM architecture and file structure. Explain evidence extraction in SIM card forensics. **10**