Paper / Subject Code: 52773 / Digital Forensic

BE/VIII/COMP/C-Scheme/DEC-24/04-12-2024

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)** Explain data carving. **05**

(b) What is Domain Key Identified Mail (DKIM). **05**

(c) Write short note on web Forensic. **05**

(d) What is SIM cards Forensic? Explain the SIM architecture and file structure? **05**

Q.2 **(a)** What is digital Forensic? What are the goals of digital forensics? Explain the phase after detection of incident? **10**

(b) Explain volatile data collection for windows system? **10**

Q.3 **(a)** What is malware analysis? What is the importance of Malware analysis? List and explain any four malware analysis tools and techniques **10**

(b) Explain data analysis in mobile forensics? Also explain what type of evidence will be obtain from any social networking application (e.g Facebook, whtasapp, webchat) **10**

Q.4 **(a)** What is digital forensic? Explain the incident response methodology. **10**

(b) What are the challenges of obtaining RAM memory? List tools to capture RAM. **10**

Q.5 **(a)** Explain the steps in the router investigation. **10**

(b) Describe GPS evidentiary data. What are its challenges and limitations? How to extract waypoints and track points from GPX files for displaying the tracks on a Map? **10**

Q.6 Write short note **(any 2)** **20**

1 Event log Analysis
2 Hidden hard drive partition analysis
3 Guidelines for incident report writing
4 Steps involved in Unix system investigation