12/12/2023

BE (COMP) / Sem VIII / R-19 / C-Scheme / SH 2023

QP Code 40852

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 the challenges in evidence handling.	**05**
	(b)	Explain Sender Policy Framework (SPF).	**05**
	(c)	Write short note on Windows registry analysis.	**05**
	(d)	Explain the SIM architecture and file structure?	**05**
Q.2	**(a)**	What is incident? Explain the incident response methodology in detail.	**10**
	(b)	What is digital evidence? Explain the various types of Digital Evidence? Explain the digital forensic examination process.	**10**
Q.3	**(a)**	Explain the steps in the router investigation?	**10**
	(b)	What is USB device forensic? Explain USB device forensics.	**10**
Q.4	**(a)**	Define digital Forensics and state its goals. Explain the phase after detection of incident?	**10**
	(b)	What are the hard drive imaging risk and challenges?	**10**
Q.5	**(a)**	Write down the steps involved in Unix system investigation?	**10**
	(b)	What is Android forensic? Explain the structure of smartphone?	**10**
Q.6	**(a)**	What is GPS forensic? Explain structure of GPS device? Explain GPS Exchange Format (GPX)?	**10**
	(b)	Explain the guidelines for incident report writing.	**10**