May-2023

Paper / Subject Code: 52773 / Digital Forensic (DLOC - V)

B.E. (Comps) (Sem-VIII) (CB (GS) (R-19-20) (C Scheme)

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 acquiring digital evidences?	**05**
	(b)	What is Domain based Message Authentication Reporting and Confirmation (DMARC)?	**05**
	(c)	Explain Pagefile.sys, Hiberfil.sys, and Swapfile.sys system files.	**05**
	(d)	What is GPS forensics? Explain structure of GPS device.	**05**
Q.2	**(a)**	What is incident? Explain the incident response methodology in detail.	**10**
	(b)	Explain importance of forensic duplication and its method and also list some duplication tools.	**10**
Q.3	**(a)**	List and explain the malware analysis tools and techniques.	**10**
	(b)	Explain hidden hard drive partition analysis and windows minidump file forensics.	**10**
Q.4	**(a)**	What is digital forensic? Explain the process of digital forensic.	**10**
	(b)	Explain non- volatile memory/ static acquisition in detail.	**10**
Q.5	**(a)**	Write short note on windows registry analysis.	**10**
	(b)	Explain data analysis in mobile forensics? Explain what type of evidence will be obtain from any social networking application (e.g. Facebook, WhatsApp, webchat).	**10**
Q.6	**(a)**	What is SIM cards Forensic? Explain the SIM architecture and file structure. Explain evidence extraction in SIM card forensics.	**10**
	(b)	Explain the investigative report template in detail.	**10**
