BCSE322L	DIGITAL FORENSICS	L	T	P	C
		2	0	0	2
Pre-requisite	**NIL**	**Syllabus version**			
		1.0			

Course Objectives

1. To present a comprehensive perception of digital forensic principles, collection, preservation, and analysis of digital evidence.
2. To enlighten the importance of forensic procedures, legal considerations, digital evidence controls, and the documentation of forensic analysis.
3. To develop a comprehension of the different tools and methods for conducting digital forensic acquisition and analysis.

Course Outcomes

After completion of this course, the student shall be able to:

1. Understand the responsibilities and liabilities of a computer forensic investigator
2. Seize a computer from a crime scene without damage and follow the legal procedures and standards.
3. Demonstrate the ability to perform forensic data acquisition and analysis.
4. Analyze and retrieve hidden and damaged files from different operating systems.
5. Apply forensics to recent technologies such as smart phones, email, cloud and social media.

Module:1	**Understanding Digital Forensics and Legal Aspects**	**3 hours**

Understanding computer forensics - Preparing for computer investigation – Maintaining professional conduct – understanding computer investigations – Taking a systematic approach – Corporate Hi-Tech investigations – Conducting an investigation.

Module:2	**Acquisition and Storage of Data**	**4 hours**

Understanding Storage Formats for Digital Evidence - Determining the Best Acquisition Method - Contingency Planning for Image Acquisitions - Using Acquisition Tools - Validating Data Acquisitions - Performing RAID Data Acquisitions - Using Remote Network Acquisition Tools - Storing Digital Evidence - Obtaining a Digital Hash - Sample Cases.

Module:3	**Working with Windows**	**5 hours**

Understanding File Systems - Exploring Microsoft File Structures - Examining NTFS Disks - Understanding Whole Disk Encryption - Understanding the Windows Registry - Understanding Microsoft Startup Tasks - Understanding MS-DOS Startup Tasks - Evaluating Computer Forensics Tool Needs - Computer Forensics Software and Hardware Tools.

Module:4	**Working with Linux/Unix Systems**	**4 hours**

UNIX and Linux Overview - Inodes - Boot Process - Drives and Partition Schemes - Examining disk Structures - Understanding Other Disk Structures - Ownership and Permissions, File Attributes, Hidden Files, User Accounts - Case studies - Validating Forensic Data – Addressing Data-Hiding Techniques – Locating and Recovering Graphics File.

Module:5	**Email and Social Media Forensics**	**4 hours**

Investigating E-mail crimes and Violations – Applying Digital Forensics Methods to Social Media Communications - Social Media Forensics on Mobile Devices - Forensics Tools for Social Media Investigations.

Module:6	**Mobile Forensics**	**4 hours**

Mobile phone basics – Acquisition procedures for mobile - Android Device –Android Malware – SIM Forensic Analysis – Case study.

Module:7	**Cloud Forensics**	**4 hours**

Working with the cloud vendor, obtaining evidence, reviewing logs and APIs.			
Module:8	**Contemporary Issues**		**2 hours**
	Total Lecture hours:		**30 hours**
Text Book(s)			
1.	B. Nelson, A. Phillips, F. Enfinger, and C. Steuart, Guide to Computer Forensics and Investigations, 2019, 6th ed. CENGAGE, INDIA (ISBN: 9789353506261)		
Reference Books			
1.	André Årnes, Digital Forensics, 2018, 1st ed., Wiley, USA(ISBN No.: 9781119262411)		
2.	Nihad A Hassan, Digital Forensics Basics: A Practical Guide to Using Windows OS, 2019, 1st ed, APress, USA (ISBN: 9781484238387)		
Mode of Evaluation: CAT, assignment, Quiz and FAT			
Recommended by Board of Studies	04-03-2022		
Approved by Academic Council	No.65	Date	17-03-2022