Cyber Forensics

Course Code	19CS4702B	**Year**	IV	**Semester**	I
Course Category	Program Elective - V	**Branch**	CSE	**Course Type**	Theory
Credits	3	**L-T-P**	3-0-0	**Prerequisites**	-
Continuous Internal Evaluation :	30	**Semester End Evaluation:**	70	**Total Marks:**	100

Course Outcomes		
Upon successful completion of the course, the student will be able to		
CO1	Understand Fundamentals of Cyber Forensics, Tools and Techniques	**L2**
CO2	Apply digital techniques for processing of crime evidence and incident scenes for a given scenario	**L3**
CO3	Apply various Disk management techniques/File Structures for Examining and investigating a given case and make an effective report	**L3**
CO4	Apply various digital forensics tools and methods on various platforms for a given scenario	**L3**

Syllabus		
Unit No.	**Contents**	**Mapped CO**
I	**Understanding the Digital Forensics Profession and Investigations:** An Overview of Digital Forensics, Preparing for Digital Investigations, Maintaining Professional Conduct, Preparing a Digital Forensics Investigation, Conducting an Investigation. **Data Acquisition:** 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, Using Other Forensics Acquisition Tools.	**CO1**
II	**Processing Crime and Incident Scenes**: Identifying Digital Evidence, Collecting Evidence in Private-Sector Incident Scenes, Processing Law Enforcement Crime Scenes, Preparing for a Search, Securing a Digital Incident or Crime Scene, Seizing Digital Evidence at the Scene, Storing Digital Evidence, Obtaining a Digital Hash	**CO1,CO2**

III	**Working with Windows and CLI Systems:** Understanding File Systems, Exploring Microsoft File Structures, Examining NTFS Disks, Understanding Whole Disk Encryption, Understanding the Windows Registry, Understanding Microsoft Startup Tasks, Understanding Virtual Machines	**CO1,CO3**
IV	**Current Digital Forensics Tools:** Evaluating Digital Forensics Tool Needs, Digital Forensics Software Tools, Digital Forensics Hardware Tools, Validating and Testing Forensics Software **Digital Forensics Analysis and Validation:** Determining What Data to Collect and Analyze, Validating Forensic Data, Addressing Data-Hiding Techniques. **Network Forensics:** Network Forensics Overview: The Need for Established Procedures, Securing a Network, Developing Procedures for Network Forensics, Investigating Virtual Networks, Examining the Honeynet Project.	**CO1,CO4**
V	**E-mail and Social Media Investigations**: Exploring the Role of E-mail in Investigations, Exploring the Roles of the Client and Server in E-mail, Investigating E-mail Crimes and Violations, Understanding E-mail Servers, Using Specialized E-mail Forensics Tools, Applying Digital Forensics Methods to Social Media Communications. **Mobile Device Forensics and the Internet of Anything:** Understanding Mobile Device Forensics, Understanding Acquisition Procedures for Mobile Devices, Understanding Forensics in the Internet of Anything. **Cloud Forensics:** Basic Concepts of Cloud Forensics, Conducting a Cloud Investigation, Tools for Cloud Forensics	**CO1,CO4**

Learning Resources
Text Books
1. Guide to Computer Forensics and Investigations, Bill Nelson, Amelia Phillips, Christopher Steuart, Sixth edition, 2020, Cengage Learning India Pvt. Ltd.
References
1 Investigating the Cyber Breach: The Digital Forensics Guide for the Network Engineer, Lakhani Joseph,Muniz,Aamir, First edition, 2018, PearsonEducation. 2 Digital Forensics Basics: A Practical Guide Using Windows OS,Nihad A. Hassan, First edition, 2019, Apress. 3 Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications,JoakimKävrestad,First edition, 2018,Springer International Publishing.
e-Resources & Other Digital Material
1. https://www.udemy.com/topic/computer-forensics/ 2. https://www.coursera.org/professional-certificates/ibm-cybersecurity-analyst