DIGITAL FORENSICS AND INCIDENT RESPONSE

Subject Code: CS34211CS	Subject Type: Core
Evaluation Scheme: MSE(30), TA(20), ESE(50)	L-T-P: 2-0-2

Pre-Requisites: Computer Networks, Operating Systems, Basics of Cyber Security, Programming.

Course Objective: To understand the fundamentals of digital forensics and the techniques used for forensic examination of various digital devices. The course focuses on data acquisition, evidence identification, analysis, and investigation of cyber crimes using forensic tools and methodologies.

Course Outcomes: At the end of the course, the student will be able to:

CO-1	Understand the fundamentals of digital forensics, cyber crimes, and legal considerations.
CO-2	Apply investigation procedures and forensic techniques in real-world scenarios.
CO-3	Perform data acquisition, validation, and evidence handling using forensic tools.
CO-4	Analyze digital evidence and use forensic tools to investigate cyber crimes.

Course Articulation Matrix:

CO/PO	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	3	2	2	2	3	1
CO-2	3	3	3	3	3	2
CO-3	3	3	3	2	3	2
CO-4	3	2	2	1	2	3

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus

Unit 1 Basic of Digital Forensic:

Incident Response, Chain of Custody, Stages of Digital Forensics, Volatile and Non-Volatile Memory Forensics, File System Forensics Analysis: NTFS, Ext 2/3/4, FAT, APFS, etc., Forensic Study of File System Metadata and Other Attributes, Secure Deletion, Slack Space, Data Recovery, Data Carving

Unit 2 Advanced Forensic Analysis and Anti-Forensics:

Windows Forensics Anti and Anti-Anti Forensics, Event Reconstruction Methods and Tools, Time Stomping, Database Forensics, Network Forensics, Approximate Matching, Email Forensics, Mobile Forensics Tools & Techniques, DRONE Forensics, IoT Forensics, Cloud Forensics, Cryptocurrency Forensics, Role of AI in Digital Forensics, AI Forensics, Emerging Technologies in Digital Forensics

Unit-3 Crime Scene Handling and Evidence Management:

Processing Digital Crime Scenes, Securing Computer Systems, Seizing Digital Evidence, Preserving and Storing Evidence, Maintaining Chain of Custody, Generating and Verifying Digital Hash Values, Case Documentation and Review, Evidence Integrity and Handling Procedures.

Unit-4 Forensic Tools, Advanced Techniques, and Applications:

Overview of Current Digital Forensic Tools (Software and Hardware), Testing and Validation of Forensic Tools, Data Hiding Techniques and Detection, Remote Forensic Acquisition, Email Forensics including Investigation of Email Crimes and Violations, Understanding Email Servers, Use of Specialized Email Forensic Tools, Emerging Trends in Digital Forensics.

Learning Resources

Text Books:

1. Computer Forensics: Incident Response Essentials – Warren G. Kruse II and Jay G. Heiser, Addison Wesley, 2002.
2. Guide to Computer Forensics and Investigations – Nelson, Phillips, Enfinger, Stuart, 2nd Edition, Thomson Course Technology, 2006.

Reference Books:

1. Computer Forensics: Computer Crime Scene Investigation – John R. Vacca, 2nd Edition, Charles River Media, 2005.