DIGITAL FORENSICS			
Semester	**III**	CIE Marks	**50**
Course Code	**24MCPE652**	SEE Marks	**50**
Teaching Hrs/Week (L: T:P)	**3:0:0**	Exam Hrs	**03**
Total Hrs	**42**	Credits	**03**

Course Learning Objectives:

This course is designed to

1. Impart knowledge on computer forensics, including its principles, methodologies, and role in modern investigative processes.
2. Familiarize in conducting systematic investigations and executing detailed forensic analysis.
3. Provide the ethical and legal principles required for conducting investigations related to cybercrimes.
4. Instill the ability to critically review and analyze digital evidence, fostering the development of effective investigative strategies.
5. Provide knowledge to apply ethical and legal principles in conducting email investigations, ensuring compliance with privacy regulations and chain of custody requirements.

Module 1: Computer forensics fundamentals	**No. of Hrs: 08**

An Overview of Digital Forensics, Preparing for Digital Investigations, Maintaining Professional Conduct, Preparing a Digital Forensics Investigation, Procedures for Private-Sector High-Tech Investigations, Understanding Data Recovery Workstations and Software, Conducting an Investigation.

Textbook 1: Ch 1

Module 2: Data Acquisition	**No. of Hrs: 08**

Understanding Storage Formats for Digital Evidence, Determining the Best Acquisition Method, Using Acquisition Tools, Validating Data Acquisitions, Performing Raid Data Acquisitions, Using Remote Network Acquisition Tools, Using Other Forensics Acquisition Tools.

Textbook 1: Ch 3

Module 3: Processing Crimes and Incident Scenes	**No. of Hrs: 08**

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, Reviewing a Case.

Textbook 1: Ch 4

Module 4: Current Digital Forensics Tools	**No. of Hrs: 10**

Evaluating Digital Forensics Tool Needs, Digital Forensics Software Tools, Digital Forensics Hardware Tools, Validating and Testing Forensics Software, E-Mail Investigations: Investigating Email Crime and Violations, Understanding E-Mail Servers, Using Specialized E-Mail Forensics Tool, Applying Digital Forensics Methods to Social Media Communications.

Textbook 1: Ch 6, Ch 11

Module 5: Digital Forensics Analysis, Validation and Virtual Machine Forensics	**No. of Hrs: 8**

Determining What Data to Collect and Analyze, Validating Forensic Data, Addressing Data-Hiding Techniques, An Overview of Virtual Machine Forensics, Performing Live Acquisitions, Network Forensics Overview.

Textbook 1: Ch 9, Ch 10

Course Outcomes:

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

CO1: Identify the fundamental concepts in computer forensics and its associated systems.

CO2: Apply systematic approaches to conduct the systematic investigations and executing detailed Forensic analyses.

CO3: Use the different data acquisition methods and choose an appropriate approach for a given case.

CO4: Solve a forensics case with the available digital evidence and using the appropriate strategies.

CO5: Apply ethical and legal principles in conducting email investigations and ensuring compliance with privacy regulations

Textbooks:

1. Bill Nelson, Amelia Phillips, Chris Stuart, "*Guide to Computer Forensics and Investigations"*, Thomson Course Technology, 6th Edition, 2018

Reference Books:

1. John R Vacca, Computer Forensics, "*Computer Crime Scene Investigation",* Charles River Media, 2nd Edition, 2005
2. John Sammons, "*The basics of digital forensics: The primer for getting started in digital forensics",* Elsevier Science, 2014
3. Linda Volonino, Reynaldo Anzaldua, and Jana Godwin, "*Computer Forensics: Principles and Practices"*, Pearson, 2007

Web Links:

1. Computer Forensics Specialization : https://www.coursera.org/specializations/computerforensics
2. Digital Forensics and Electronic Evidence: https://www.udemy.com/course/digital-forensics-and-electronic-evidence
3. Cyber Forensics : https://www.mygreatlearning.com/academy/learn-for-free/courses/cyber-forensics