COURSE CONTENT

DIGITAL FORENSICS								
II Semester: CSE								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
		L	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
BCSE18	**Elective**	3	-	-	3	40	60	100
Contact Classes:48	**Total Tutorials: Nil**	**Total Practical Classes: Nil**				**Total Classes: 45**		
Prerequisite: Computer Networks, Information Security								

I. COURSE OVERVIEW:

Digital forensics course focuses on the investigation and analysis of digital devices, networks, and electronic data to uncover evidence for legal or investigative purposes. It involves the application of specialized techniques and tools to collect, preserve, analyze, and present evidence found in digital devices.

II. COURSE OBJECTIVES:

The students will try to learn:

I. provides an in-depth study of the rapidly changing and fascinating field of computer forensics.
II. combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
III. knowledge of digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, and e-discovery tools.

III. COURSE OUTCOMES:

After successful completion of the course, students will be able to:

CO 1 Apply ethical hacking in the Information Communication Technology (ICT) world.
CO 2 Underline the need for digital forensics and the role of digital evidence
CO 3 Understand incident response and security issues in the ICT world, and identify digital forensic tools for data collection.
CO 4 Apply digital forensic duplication and tools for analysis to achieve adequate perspectives of digital forensic investigation.
CO 5 Apply the knowledge of Intrusion Detection System to protect the network and perform router and network analysis
CO6 List the techniques to generate legal evidence and supporting investigation reports

IV. COURSE CONTENT:

MODULE-I: INTRODUCTION OF CYBERCRIME (10)

Types of cybercrime, categories of cybercrime, Computers' roles in crimes, Prevention from Cybercrime, Hackers, Crackers, Phreakers.

Digital Forensic: Rules for Digital Forensic The Need for Digital Forensics, Types of Digital Forensics, Ethics in Digital Forensics.

Digital Evidence: Types and characteristics and challenges for Evidence Handling

MODULE-II: ETHICAL HACKING (10)
Difference between Hacking and Ethical hacking: Steps of Ethical Hacking, Exploring some tools for ethical hacking: scanning tools.
Introduction to Computer Security Incident: Goals of Incident response, Incident Response Methodology, Formulating Response Strategy.
IR Process – Initial Response, Investigation, Remediation, Tracking of Significant, Investigative Information.

MODULE-III: LIVE DATA COLLECTION (09)
Live Data Collection on Microsoft Windows Systems: Live Data Collection on Unix-Based Systems

Forensic Duplication: Forensic Image Formats, Traditional Duplication, Live System Duplication, Forensic Duplication tools.

MODULE-IV: FILE SYSTEMS (10)
Various Types of File Systems, Introduction to Storage Layers, Forensic Analysis of File Systems
Data Analysis: Analysis Methodology Investigating Windows systems, Investigating UNIX systems, Investigating Applications, Web Browsers, Email, Malware Handling: Static and Dynamic Analysis

MODULE-V: NETWORK FORENSICS (09)
Technical Exploits and Password Cracking, Introduction to Intrusion Detection systems, Types of IDS Understanding Network intrusion and attacks, Analyzing Network Traffic, Collecting Network evidence, Evidence Handling. Investigating Routers, Using Routers as Response Tools.
Report: Goals of Report, Layout of an Investigative Report, Guidelines for Writing a Report.

V. TEXT BOOKS:

1. Nilakshi Jain, Dhananjay Kalbande, "Digital Forensic: The fascinating world of Digital Evidence" Wiley India Pvt Ltd 2017.

VI. REFERENCE BOOKS:

1. Jason Luttgens, Matthew Pepe, Kevin Mandia, "Incident Response and computer forensics", Tata McGraw Hill, 3rd edition 2014.
2. Cory Altheide, Harlan Carvey, "Digital forensics with open source tools", Syngress Publishing, Inc. 2011.
3. Clint P Garrison "Digital Forensics for Network, Internet, and Cloud Computing A forensic evidence guide for moving targets and data", Syngress Publishing, Inc. 2010.

VII. WEB REFERENCES:

1. https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section---references

VIII E-Text Books:

1. https://www.oreilly.com/library/view/digital-forensics/9781119262381/
2. https://uou.ac.in/sites/default/files/slm/MIT(CS)-202.pdf
3. https://ec.europa.eu/programmes/erasmus-plus/project-result-content/2a54509d-b6bb-43d8-8250-eae26782c392/FORC%20Book%201.pdf