DIGITAL FORENSICS

II Semester: CSE								
Course Code	Category	Hours / Week			Credits	Maximum Marks		
BCSC21	Elective	L	T	P	C	CIA	SEE	Total
		3	0	0	3	30	70	100
Contact Classes: 45	Total Tutorials: Nil	Total Practical Classes: Nil				Total Classes: 45		

I. COURSE OVERVIEW:

This course provides a broad overview of computer forensics as an occupation by exploring methodologies used surrounding digital forensics. In addition, the student acquires open-source forensic tools to use throughout this path. This course includes digital forensics science, computer crime, cybercrime scene analysis, evidence management, presentation and legal aspects of digital forensics.

II. COURSE OBJECTIVES:

The students will try to learn:

I. The in-depth study of the rapidly changing and fascinating field of computer forensics.
II. Both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
III. Digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools
IV. E-evidence collection and preservation, investigating operating systems and file systems, network forensics, art of steganography and mobile device forensics

III. COURSE OUTCOMES:

After successful completion of the course, students should be able to

CO 1	**Organize** digital investigations that conform to accepted professional standards and are based on the investigative process: identification, preservation, examination, analysis, and reporting.	Create
CO 2	**Understand** the Computer forensics and digital detective and various processes, policies and procedures.	Apply
CO 3	**Identify** E-discovery, guidelines and standards, E-evidence, tools and environment.	Evaluate
CO 4	**Experiment** Email and web forensics and network forensics**.**	Apply
CO 5	**Relate** work collaboratively with clients, management, and/or law enforcement to advance digital investigations or protect the security of digital resources.	Knowledge

IV. SYLLABUS

MODULE – I: DIGITAL FORENSICS SCIENCE AND COMPUTER CRIME (09)

Digital Forensics Science: Forensics science, computer forensics, and digital forensics.
Computer Crime: Criminalistics as it relates to the investigative process, analysis of cyber-criminalistics area, holistic approach to cyber-forensics.

MODULE-II: CYBER CRIME SCENE ANALYSIS (09)

Cyber Crime Scene Analysis: Discuss the various court orders etc., methods to search and seizure electronic evidence, retrieved and un-retrieved communications, Discuss the importance of understanding what court documents would be required for a criminal investigation.

MODULE-III: EVIDENCE MANAGEMENT & PRESENTATION (09)

Evidence Management & Presentation: Create and manage shared folders using operating system, importance of the forensic mindset, define the workload of law enforcement, Explain what the normal case would look like, Define who should be notified of a crime, parts of gathering evidence, Define and apply probable cause.

MODULE-IV: COMPUTER FORENSICS AND NETWORK FORENSICS (09)

Computer Forensics: Prepare a case, Begin an investigation, Understand computer forensics workstations and software, Conduct an investigation, Complete a case, Critique a case,
Network Forensics: open-source security tools for network forensic analysis, requirements for preservation of network data.

MODULE-V: MOBILE FORENSICS AND LEGAL ASPECTS OF DIGITAL FORENSICS (09)

Mobile Forensics: mobile forensics techniques, mobile forensics tools.
Legal Aspects of Digital Forensics: IT Act 2000, amendment of IT Act 2008, Recent trends in mobile forensic technique and methods to search and seizure electronic evidence.

V. TEXT BOOKS:

1. John Sammons, “The Basics of Digital Forensics”, Elsevier, 2014.
2. John Vacca, “Computer Forensics: Computer Crime Scene Investigation”, Laxmi Publications 2005.

VI. REFERENCE BOOKS

1. Brian Carrier , "File System Forensic Analysis" , Addison Wesley, 2005
2. Dan Farmer &WietseVenema ,"Forensic Discovery", Addison Wesley, 2005

VII. WEB REFERENCES:

1. https://www.researchgate.net/publication/300474145_Digital_Forensics
2. https://ec.europa.eu/programmes/erasmus-plus/project-result-content/2a54509d-b6bb-43d8-8250-eae26782c392/FORC%20Book%201.pdf

VIII. E-Text Books:

1. https://booksite.elsevier.com/samplechapters/9781597496612/Front_Matter.pdf