

DIGITAL FORENSICS

II Semester: CSE

Course Code	Category	Hours / Week			Credits	Maximum Marks		
BCSB18	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 students with comprehensive knowledge on how to combat cybercrime through digital forensics. Students will gain expertise in various areas, including cybercrime scene analysis, evidence management and presentation, computer forensics, network forensics, mobile forensics, and legal aspects of digital forensics.

II. OBJECTIVES:

The students will try to learn:

- I. How to Combines both the technical expertise and the knowledge required to investigate, detect and prevent digital crimes.
- II. The Knowledge on digital forensics legislations, digital crime, forensics processes and procedures, data acquisition and validation, e-discovery tools
- III. The 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.	Understand
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.	Understand

IV. SYLLABUS

UNIT-I	DIGITAL FORENSICS SCIENCE AND COMPUTER CRIME	Classes: 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.		
UNIT-II	CYBER CRIME SCENE ANALYSIS	Classes: 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.		
UNIT-III	EVIDENCE MANAGEMENT & PRESENTATION	Classes: 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.		
UNIT-IV	COMPUTER FORENSICS AND NETWORK FORENSICS	Classes: 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.		
UNIT-V	MOBILE FORENSICS AND LEGAL ASPECTS OF DIGITAL FORENSICS	Classes: 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.		
Text Books:		
<ol style="list-style-type: none"> 1. John Sammons, “The Basics of Digital Forensics”, Elsevier. 2. John Vacca, “Computer Forensics: Computer Crime Scene Investigation”, Laxmi Publications. 		
Reference Books:		
<ol style="list-style-type: none"> 1. John Sammons, “The Basics of Digital Forensics”, Elsevier. 2. John Vacca, “Computer Forensics: Computer Crime Scene Investigation”, Laxmi Publications. 		
Web References:		
<ol style="list-style-type: none"> 1. http://www.sctie.iitkgp.ernet.in/ 2. http://www.rkala.in/softcomputingvideos.php 3. http://www.sharbani.org/home2/soft-computing-1 4. http://www.myreaders.info/html/soft_computing.html 		
E-Text Books:		
<ol style="list-style-type: none"> 1. https://www.books.google.co.in/books?id=bVbj9nhvHd4C 2. https://www.books.google.co.in/books?id=GrZHPgAACAAJ&dq=1.+J.S.R.Jang,+C.T.Sun+and+E.Mizutani,+Neuro,+Fuzzy+and+Soft+Computing,+PHI,+2004,Pearson+Education. 		