CS3213OE: COMPUTER FORENSICS
(Open Elective- I)

III-II:CSE(CS)								
Course Code	**Category**	**Hours/Week**			**Credits**	**Max Marks**		
CS3213OE	**Open Elective- I**	**L**	**T**	**P**	**C**	**CIE**	**SEE**	**Total**
		3	**0**	**0**	**3**	**25**	**75**	**100**
Contact Classes:45	**Tutorial classes:15**	**Practical classes: Nill**				**Total Classes:60**		
Prerequisites								

B.Tech. III Year II SEM

Course Objectives:

- **T**o understand the cyberspace.
- To understand the **forensics** fundamentals.
- To understand the evidence capturing process.
- To understand the preservation of **digital** evidence.

Course Outcomes:

- Students will understand the usage of computers in forensic, and how to use various forensic tools for a wide variety of investigations.
- It gives an opportunity to students to continue their zeal in research in computer forensics.

UNIT-I

Computer Forensics Fundamentals: What is Computer Forensics?

Forensics in Law Enforcement, Computer Forensics Assistance to Human Resources / Employment Proceedings, Computer Forensics Services, Benefits of Professional Forensics Methodology, Steps taken by Computer Forensics Specialists

Types of Computer Forensics Technology: Types of Military Computer Forensic Technology, Types of Law Enforcement — Computer Forensic Technology — Types of Business Computer Forensic Technology

Computer Forensics Evidence and Capture: Data Recovery Defined — Data Back-up and Recovery — The Role of Back-up in Data Recovery — The Data-Recovery Solution.

UNIT-II

Evidence Collection and Data Seizure: Why Collect Evidence? Collection Options —Obstacles — Types of Evidence — The Rules of Evidence — Volatile Evidence — General Procedure — Collection and Archiving — Methods of Collection — Artifacts — Collection Steps — Controlling Contamination: The Chain of Custody

Duplication and Preservation of Digital Evidence: Preserving the Digital Crime Scene —Computer Evidence Processing Steps — Legal Aspects of Collecting and

Preserving Computer Forensic Evidence

Computer Image Verification and Authentication: Special Needs of Evidential Authentication—Practical Consideration—Practical Implementation.

UNIT-III

Computer Forensics analysis and validation: Determining what data to collect and analyze, validating forensic data, addressing data-hiding techniques, performing remote acquisitions

Network Forensics: Network forensics overview, performing live acquisitions ,developing standard procedures for network forensics, using network tools, examining the honey net project.

Processing Crime and Incident Scenes: Identifying digital evidence, collecting evidence in private-sector incident scenes, processing law enforcement crime scenes, preparing for a search, securing a computer incident or crime scene, seizing digital evidence at the scene, storing digital evidence, obtaining a digital hash, reviewing a case

UNIT-IV

Current Computer Forensic tools: evaluating computer forensic tool needs, computer forensics software tools, computer forensics hardware tools, validating and testing forensics software

E-Mail Investigations: Exploring the role of e-mail in investigation, exploring the roles of the client and server in e-mail, investigating e-mail crimes and violations, understanding e-mail servers, using specialized e-mail forensic tools.

Cell phone and mobile device forensics: Understanding mobile device forensics, understanding acquisition procedures for cell phones and mobile devices.

UNIT-V

Working with Windows and DOS Systems: understanding file systems, exploring Microsoft File Structures, Examining NTFS disks, Understanding whole disk encryption, Windows registry, Microsoft startup tasks, MS-DOS startup tasks, virtual machines.

TEXTBOOKS

1. Computer Forensics, Computer Crime Investigation by John R. Vacca ,Firewall Media ,New Delhi.
2. Computer Forensics and Investigations by Nelson, Phillips Enfinger, Steuart, CENGAGE Learning

REFERENCEBOOKS

1. Real Digital Forensics by Keith J.Jones ,Richard Bejtiich, Curtis W.Rose,

Addison-Wesley Pearson Education
2. Forensic Compiling ,A Tractitioner is Guide by Tony Sammes and Brian Jenkin son ,Springer International edition.
3. Computer Evidence Collection & Presentation by Christopher L.T.Brown, Firewall Media.
4. Home l and Security, Techniques & Technologies by Jesus Mena, Firewall Media.
5. Software Forensics Collecting Evidence from the Scene of a Digital Crime by Robert M. Slade, TMH 2005

Windows Forensics by Chad Steel, Wiley India Edition