4/4 B.Tech. SECOND SEMESTER
CYBER FORENSICS

CS8T3C **Credits: 4**

Elective – IV

Lecture: 4 periods/week **Internal assessment: 30 marks**
Tutorial: 1 period /week **Semester end examination: 70 marks**

Course Context and Overview: This course introduces the fundamental concepts of Cyber forensics. With this foundation students can take up engineering career in industry or research.

Prerequisites: C LANGUAGE, I/O ANALOG AND DIGITAL INTERFACING, AND PERIPHERALS

Learning Outcomes:

Ability to:

1. Take systematic approaches for computer investigation & understanding data recovery work stations and tools.
2. Make validation & testing forenciscs software using current computer forensics tools.
3. Make e-mail investigation with cellphone, mobile device forensics.
4. Understand acquisition procedure for cellphone, mobile and e-mail servers.

UNIT – I

Computer Forensics and Investigation: Understanding Computer Forensics, Preparing for Computer Investigations, Taking A Systematic Approach, Procedure for Corporate High – Tech Investigations, Understanding Data Recovery Workstations and Software.

UNIT – II

Investor's Office and Laboratory: Understanding Forensics Lab Certification Requirements, Determining the Physical Requirements for a Computer Forensics Lab, Selecting a Basic Forensic Workstation.

UNIT - III

Data Acquisition: Understanding Storage Formats for Digital Evidence, Determining the Best Acquisition Method, Contingency Planning for Image Acquisitions, Using Acquisition Tools, Validating Data Acquisition, Performing RAID Data Acquisition, Using Remote Network Acquisition Tools, Using Other Forensics Acquisition Tools.

UNIT - IV

Processing Crime and Incident Scenes: Identifying Digital Evidence, Collecting the Evidence in Private – Sector Incident Scenes, Processing Law Enforcement Crime Scenes, Preparing for a Search, Securing a Computer Incident or Crime Scene, Sizing Digital evidence at the Scene.Storing Digital Evidence, Obtaining a Digital Hash.

UNIT – V

Current Computer Forensics Tools: Evaluating Computer Forensics Toll Needs, Computer Forensics Software Tools, Computer Forensics Hardware Tools, Validating and Testing Forensics Software.

UNIT - VI

Computer Forensics Analysis and Validation: Determining What Data to Collect and Analyze, Validating Forensic Data, Addressing Data-Hiding Techniques, And Performing Remote Acquisition.

UNIT – VII

Recovering Graphics and Network Forensics: Recognising a Graphics File, Understanding Data Compression, Locating and Recovering Graphics Files, Understanding Copyright Issues with Graphics, Network Forensics, Developing Standard Procedure for Network Forensics, Using Network Tools, Examining Hiney Project.

UNIT – VIII

E–mail Investigations Cell Phone and Mobile Devices Forensics: Exploring the Role of E-mail in Investigations, Exploring the Role of Client and Server in E-mail. Investigatin E-mail Crimes and violations, Understanding E-mail Servers, Using Specialized E-mail Forensics Tools, Understanding Mobile Device Forensics, Understanding Acquisition Procedure for Cell Phones and Mobile Devices.

Learning Resources

Text Book:

Computer Forensics and Investigations, Nelson, Phillips Enfinger, Steuart,