CS8074 CYBER FORENSICS

DETAILED SYLLABUS

OBJECTIVES:

- To learn computer forensics
- To become familiar with forensics tools
- To learn to analyze and validate forensics data

UNIT I INTRODUCTION TO COMPUTER FORENSICS

Introduction to Traditional Computer Crime, Traditional problems associated with Computer Crime. Introduction to Identity Theft & Identity Fraud. Types of CF techniques - Incident and incident response methodology - Forensic duplication and investigation. Preparation for IR: Creating response tool kit and IR team. - Forensics Technology and Systems - Understanding Computer Investigation – Data Acquisition.

UNIT II EVIDENCE COLLECTION AND FORENSICS TOOLS

Processing Crime and Incident Scenes – Working with Windows and DOS Systems. Current Computer Forensics Tools: Software/ Hardware Tools.

UNIT III ANALYSIS AND VALIDATION

Validating Forensics Data – Data Hiding Techniques – Performing Remote Acquisition – Network Forensics – Email Investigations – Cell Phone and Mobile Devices Forensics

UNIT IV ETHICAL HACKING

Introduction to Ethical Hacking – Foot printing and Reconnaissance - Scanning Networks - Enumeration - System Hacking - Malware Threats - Sniffing

UNIT V ETHICAL HACKING IN WEB

Social Engineering - Denial of Service - Session Hijacking - Hacking Web servers - Hacking Web Applications – SQL Injection - Hacking Wireless Networks - Hacking Mobile Platforms.

TEXT BOOKS:

1. Bill Nelson, Amelia Phillips, Frank Enfinger, Christopher Steuart, ―Computer Forensics and Investigations‖, Cengage Learning, India Edition, 2016.

2. CEH official Certfied Ethical Hacking Review Guide, Wiley India Edition, 2015.

REFERENCES

1. John R. Vacca, ―Computer Forensics‖, Cengage Learning, 2005

2. MarjieT. Britz, ―Computer Forensics and Cyber Crime‖: An Introduction‖, 3rd Edition, Prentice Hall, 2013.

3. AnkitFadia ― Ethical Hacking‖ Second Edition, Macmillan India Ltd, 2006

4. Kenneth C. Brancik ―Insider Computer Fraud‖ Auerbach Publications Taylor &amp; Francis Group–2008.