CS6004   **CYBER FORENSICS**   **L T P C 3 0 0 3**

OBJECTIVES:
The student should be made to:
- Learn the security issues network layer and transport layer
- Be exposed to security issues of the application layer
- Learn computer forensics
- Be familiar with forensics tools
- Learn to analyze and validate forensics data

UNIT I   NETWORK LAYER SECURITY &TRANSPORT LAYER SECURITY   9
IPSec Protocol - IP Authentication Header - IP ESP - Key Management Protocol for IPSec .
Transport layer Security: SSL protocol, Cryptographic Computations – TLS Protocol.

UNIT II   E-MAIL SECURITY & FIREWALLS   9
PGP - S/MIME - Internet Firewalls for Trusted System: Roles of Firewalls – Firewall related terminology- Types of Firewalls - Firewall designs - SET for E-Commerce Transactions.

UNIT III   INTRODUCTION TO COMPUTER FORENSICS   9
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 IV   EVIDENCE COLLECTION AND FORENSICS TOOLS   9
Processing Crime and Incident Scenes – Working with Windows and DOS Systems. **Current Computer Forensics Tools:** Software/ Hardware Tools.

UNIT V   ANALYSIS AND VALIDATION   9
Validating Forensics Data – Data Hiding Techniques – Performing Remote Acquisition – Network Forensics – Email Investigations – Cell Phone and Mobile Devices Forensics

TOTAL: 45 PERIODS

OUTCOMES:
Upon completion of the course, the student should be able to:
- Discuss the security issues network layer and transport layer
- Apply security principles in the application layer
- Explain computer forensics
- Use forensics tools
- Analyze and validate forensics data

TEXT BOOKS:

1. Man Young Rhee, "Internet Security: Cryptographic Principles", "Algorithms and Protocols", Wiley Publications, 2003.
2. Nelson, Phillips, Enfinger, Steuart, "Computer Forensics and Investigations", Cengage Learning, India Edition, 2008.

REFERENCES:

1. John R.Vacca, "Computer Forensics", Cengage Learning, 2005
2. Richard E.Smith, "Internet Cryptography", 3rd Edition Pearson Education, 2008.
3. Marjie T.Britz, "Computer Forensics and Cyber Crime": An Introduction", 3rd Edition, Prentice Hall, 2013.