CYBER LAWS & CYBER FORENSICS

Course Code : CSC 501 **Credit Units: 03**
Total Hours: 45

Course Objectives:

- To provide the fundamentals of digital and cyber space, impact of the activities.
- To cover the fundamentals of cyber-crime and steps involved in collecting the evidence through various tools.
- To provide basics of Cyber-crime incidents and implementing cyber law based on IT Act

Course Contents:

Module I: Introduction to cyber laws & cyber forensics: (9 Hours)

Classifications of Cyber Crimes against individuals, property and nation, Need for Digital forensics and steps in digital forensics (scientific methods), Number System: Binary, Decimal, Hexadecimal, ASCII, and Unicode representation of data, Arenas for digital forensics: disk, network, wireless, database, mobile, e-mail, GPS and memory, Incident handling and response with forensic triage, Ethical Hacking and future of cybercrime.

Module II: Fundamentals for Cyber Forensics: (9 Hours)

Locard's exchange principle and digital forensic investigation models, types: artifacts, identifying raw and proprietary forensic storage formats, identification of potential evidence: slack space, swap space, steganography, recovery of hidden, deleted and corrupt data, standard file formats with their headers and forensic file carving, planning your investigation, order of volatility and forensic triage, overview of file systems.

Module III: Rules for Cyber Security and Digital Forensics: (9 Hours)

Rules of collecting Digital Evidence, Standard collection procedures: seizure, write blockers, bit-stream imaging, hashing, Chain of Custody (COC), evidence bags and SOP for collecting evidence, Source and Location of Digital Evidence, Duplicating and Preserving Digital Evidence, Importance of MAC timings, Types of System logs and Windows Registry.

Module IV: Implementation of Cyber Law and Digital Forensics: (9 Hours)

Forensic laboratory requirements: setting up of lab, evaluating lab staff, selection of appropriate forensic workstations, backup and recovery plans, generating forensically sound reports, IPR and Cyber Laws in India - IT Act 2000 and 2008 Amendment and like-minded IPC sections, Code of Ethics, Expert Witness and analyzing sample forensic reports.

Module V: Practical approaches of Cyber Forensics: (9 Hours)

Validating and gathering evidence using DOS Commands and Unix/Linux Commands, Forensic imaging using DD commands, Software tools - Open Source and proprietary digital forensic frameworks, Hardware tools - write blockers, images and evidence protection containers/bags, NIST tools - CFReDS, CTFF and NSRL and analyzing e-mail headers and network packets.

Course Outcomes:

The student will learn

- Explain the concept of digital forensics and cyber forensics
- Understand and able to perform cyber forensics for the cybercrime incident
- Able to use different forensics tools and standard to report the real-world cyber incidents
- Familiarizing the fundamentals of Anti-forensics and Cyber laws.

Examination Scheme:

Components	A	CT	S/V/Q/HA	EE
Weightage (%)	5	15	10	70

Amity School of Engineering & Technology Gwalior Madhya Pradesh

Director-ASET
Amity University Madhya Pradesh Gwalior

A: Attendance, CT: Class Test, S/V/Q/HA: Seminar/Viva/Quiz/ Home Assignment, EE: End Semester Examination.

Text & References:

- E. Casey, Handbook of Digital Forensics and Investigation, Academic Press; 2010.
- David Cowen, Computer Forensics: A Beginners Guide, McGraw Hill Education.
- Bill Nelson, Amelia Phillips, Christopher Steuart, Guide to Computer Forensics and Investigations.
- Brian Carrier, File System Forensic Analysis, Pearson.
- Marjie T. Britz, Computer Forensics and Cyber Crime, Pearson.