Semester 2
Paper 204: Cyber Law and Forensic Evidence

Marks: 100 **Lectures 60**

Objective: The paper aims to create the basic clarity and understanding of cybercrimes and cyber security laws to the professionals learning the ethical hacking programme. The paper would address and emphasise on the activities leading to infringement of individual or organisational privacy. Further, the paper intends to create highly sensitised professionals who can be responsible for handling the cyber security issues pertaining to varied domains and dealing in forensics diligently.

Unit I: Introduction to Cyberspace, Cybercrime and Cyber Law
The World Wide Web, Web Centric Business, E Business Architecture, Models of E Business, E Commerce, Threats to virtual world. Cyber Crimes& social media, Cyber Squatting, Cyber Espionage, Cyber Warfare, Cyber Terrorism, Cyber Defamation. Online Safety for women and children, Misuse of individual information. Objectives, Applicability, Non applicability and Definitions of the Information Technology Act, 2000.

Unit II: Regulatory Framework of Information and Technology Act 2000
Digital Signature, E Signature, Electronic Records, Electronic Evidence and Electronic Governance. Controller, Certifying Authority and Cyber Appellate Tribunal.(Rules announced under the Act)

Unit III: **Offences and Penalties**
Offences under the Information and Technology Act 2000, Penalty and adjudication. Punishments for contraventions under the Information Technology Act 2000 (Case Laws, Rules and recent judicial pronouncements to be discussed).Limitations of Cyber Law.

Unit IV: Fundamentals of Cyber Forensics
Cyber Forensic Basics- Introduction to Cyber Forensics, Storage Fundamentals, File System Concepts, Data Recovery, Operating System Software and Basic Terminology Data and Evidence Recovery- Introduction to Deleted File Recovery, Formatted Partition Recovery

Unit V: Data Recovery Tools, Data Recovery Procedures and Ethics
Gathering Evidence- Precautions, Preserving and safely handling original media for its admissibility, Document a Chain of Custody and its importance, Complete time line analysis of computer files based on file creation, file modification and file access, Recover Internet Usage Data, Data Protection and Privacy, Recover Swap Files/Temporary Files/Cache Files,

Introduction to Encase Forensic Edition, Forensic Toolkit etc, Use computer forensics software tools to cross validate findings in computer evidence-related cases.

Unit VI: Cyber Forensics Investigation

Introduction to Cyber Forensic Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Encryption and Decryption methods, Search and Seizure of Computers, Recovering deleted evidences, Password Cracking, Cracking with GPU Systems , Hashcat. Work on open Source, Commercial tools and Cyber range.

Suggested readings

1. Craig, B. *Cyber Law: The Law of the Internet and Information Technology.* Pearson Education
2. Paintal, D. *Law of Information Technology*. New Delhi: Taxmann Publications Pvt. Ltd.
3. Lindsay, D. (2007). *International domain name law: ICANN and the UDRP*. Oxford: Hart Publishing.
4. Sharma J. P, & Kanojia S. (2016). *Cyber Laws.* New Delhi: Ane Books Pvt. Ltd.
5. Duggal, P. *Cyber Laws*. (2016) Universal Law Publishing.
6. Kamath, N. (2004). *Law relating to computers, internet and e-commerce: A guide to Cyber Laws and the Information Technology Act, 2000 with rules, regulations and notifications (2nd ed.)*. Delhi: Universal Law Publishing Co.
7. Stephenson, P.R. & Gilbert, K. *Investigating computer- related crime a handbook for corporate investigators*. Boca Raton, FL: Taylor & Francis.
8. Prosise, C. & Mandia, K. (2003). Incident response & computer forensics (2nd ed.). New York, NY: McGraw-Hill Companies.

Latest Editions of the Suggested Readings along with discussion material by the Faculty.