

PIS205 FORENSICS AND CYBER LAW

L	T	P	Cr
3	0	2	4.0

Course Objectives: To maintain an appropriate level of awareness, knowledge and skill required to minimize the occurrence and severity of incidents related to forensics and cyber law.

Introduction to Forensics and Cyber Crime: Fundamentals of computer, Internet Technology, E-Governance & E - Business ,Crime, criminology, origin, source, recent trends.Emergence of information based society, economic, administration, social, dependence of use of information, accession, threats, civil society and global society, Overview of computer forensics and Investigative Techniques, Computer forensic tools, activities of forensic investigations and testing methodology.

Types and Categories of Cyber Crime Categories of Cyber Crime: Personal, Business, Financial, Office Security, Cyber Crime – Complete transparency, hacking/cracking, denial of service, IP piracy, phishing, hetaerism etc. Cyber Attack – cyber attackers.

Role of Computers and Internet in Cyber crime, penetration testing and auditing : Computer as witness, evidence, act, defining evidence, computer forensics, computer storage, media of electric record for use of course of law.Customers and legal agreements, Router penetration testing, Firewalls penetration testing, Intrusion detection system penetration testing, Wireless networks penetration testing, Password cracking penetration testing, Social engineering penetration testing, Application penetration testing, Policies and controls testing. Penetration testing report and documentation writing , Policies and procedures Security Policies-checklist.

Cyber Security: The concept of cyber security , meaning, scope and the frame work, basic structure development and management, Rules, Regulations, Act, Legislation - Meaning, Scope, Difference between Rules.

Need for a Cyber Act: The Indian Context , Need for a Cyber Act , Information Technology Act , Scope and further Development , Information Technology Act (Amendment) , coverage of Cyber Security and Cyber Crime Indian cyber Laws vs. cyber laws of U.S.A , similarities , scope and coverage , Effectiveness.

Laboratory work: consists of gathering information, evidence with tools like WinHex, Metasploit and Social Engineering toolkit.

Recommended Books

1. Cyber Forensics: from Data to Digital Evidence , Albert J. Marcella Jr., Wiley, 1st Edition, 2012
2. Hack I.T. - Security Through Penetration Testing, T. J. Klevinsky, Scott Laliberte and Ajay Gupta, Addison-Wesley, 1st Edition, 2002
3. Computer Forensics: Cybercriminals, Laws, And Evidence , Marie-Helen Maras, Jones & Bartlett Learn , 1st Edition , 2011
4. Computer Forensics: Investigating Network Intrusions and Cyber Crime, EC Council Press Series, Cengage Learning , 2010