RAJIV GANDHI PROUDYOGIKI VISHWAVIDYALAYA, BHOPAL

New Scheme Based On AICTE Flexible Curricula

Computer Science & Information Technology, VIII-Semester

Open Elective CSIT- 803 (C) Cyber Laws and Forensics

Objective

The objective of this course is to emphasize the importance of cyber laws and digital forensics, and to prepare students to conduct a digital investigation in an organized and systematic way.

Course Outcomes: After the completion of this course, the students will be able to:

1. Become aware of various cyber crimes and cyber laws
2. Underline the need of digital forensic and role of digital evidences
3. Understand different types of digital evidences that can be presented to support investigations
4. List the methods to generate legal evidence and supporting investigation reports
5. Use various digital forensic tools

UNIT-I

Introduction to cybercrime, definition, cyber crime and information security, classification of cybercrimes, cybercrime: the legal perspectives, an Indian perspective, cybercrime and the Indian ITA 2000, a global perspective on cybercrime, Cyber offences: How criminals plan them, Tools and methods used in cyber crime, Need of cyber law, The Indian IT act, challenges to Indian law and cybercrime scenario in India, digital signature and Indian IT act,

UNIT-II

Law and framework for information security, law for intellectual property rights (IPR), patent law, copy right law, Indian copyright act, privacy issue and law in Hong Kong, Japan, and Australia, data protection act in Europe, health insurance portability and accountability act of 1996(HIPAA),Gramm-leach-Bliley act of 1999(GLAB),Sarbanes-Oxley(SOX), legal issue in data mining.

UNIT III

Digital forensics Science, The need for computer forensics, Understanding computer forensics, computer forensics versus other related disciplines, A brief History of computer Forensics, Cyber forensics and digital evidence, Digital forensics lifecycle, chain of custody concept, Network forensics, Approaching a computer forensics investigation, setting up a computer forensics laboratory, Forensics and social networking sites, computer forensics from compliance perspective, challenges in computer forensics, forensics auditing, anti forensics.

UNIT IV

Current Computer Forensics Tools, Evaluating Computer Forensics Tool Needs, Types of Computer Forensics Tools, Tasks Performed by Computer Forensics Tools, Tool Comparisons, Other Considerations for Tools, Computer Forensics Software Tools, Command-Line Forensics

Tools, UNIX/Linux Forensics Tools, Other GUI Forensics Tools, Computer Forensics Hardware Tools, Forensic Workstations

UNIT V

Forensics of hand held devices, Investigating Network Intrusions and Cyber Crime, Network Forensics and investigating logs, investigating network Traffic, Investigating Web attacks, Router Forensics. Cyber forensics tools and case studies

Recommended Books

1. The Indian Cyber law with Cyber glossary, Suresh T. Vishwanathan, New Delhi, Bhart Law House, 2000.
2. Law of Cyber Crimes and Information Technology Law, S.V. JogaRao, 2007.
3. Cory Altheide, Harlan Carvey, Digital Forensics with Open Source Tools, Syngress imprint of Elsevier.
4. Bill Nelson, Amelia Phillips, Christopher Steuart, "Guide to Computer Forensics and Investigations", Fourth Edition, Course Technology.
5. Angus M. Marshall, "Digital forensics: Digital evidence in criminal investigation", John –Wiley and Sons, 2008.
6. Nina Godbole and Sunit Belapure–Cyber Security, Wiley India Publication.