राष्ट्रीय प्रौद्योगिकी संस्थान पटना / NATIONAL INSTITUE OF TECHNOLOGY PATNA
संगणक विज्ञान एंव अभियांत्रिकी विभाग / DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
अशोक राजपथ, पटना-८००००५, बिहार / ASHOK RAJPATH, PATNA-800005, BIHAR
Phone No.: 0612-2372715, 2370419, 2370843, 2371929 Ext- 200, 202 Fax-0612-2670631 Website: www.nitp.ac.in

No:- Date:

CS84140: Cyber Forensics

L-T-P-Cr: 2-0-2-3

Prerequisite: Computer and Network Security, Operating Systems

Learning Objectives:

1. Identify the security vulnerability and threats computing systems
2. Describe the security events and their reasons
3. Handle the computers and connected devices with securely.

Syllabus:

Unit I
Introduction: Computer Forensics Fundamentals, Types of Computer Forensics Technology, Types of Computer Forensics Systems, Vendor and Computer Forensics Services.

Forensic Sciences: Basics, Ethics, Rules, Laws, Procedures. Introduction to Computers, Software, Hardware, Computer Ethics and Application Programs.

Unit II
Cyber Forensic Basics- Introduction to Cyber Forensics, Storage Fundamentals, File System Concepts, Data Recovery, Operating System Software and Basic Terminology, Deleted File Recovery, Data Recovery Tools, Preserve and safely handle original media, Document a "Chain of Custody", Recover Internet Usage Data, Recover Swap Files/Temporary Files/Cache Files, Introduction to Encase Forensic Edition, Forensic Tool Kit (FTK) etc., Use computer forensics software tools to cross validate findings in computer evidence-related cases,

Unit–III
Computer forensics evidence and Investigation: Data Recovery, Evidence Collection and Data Seizur E-Duplication and Preservation of Digital Evidence E-Computer Image Verification and Authentication. Cyber Forensic Investigation, Investigation Tools, eDiscovery, mobile device forensics, memory forensics, E-Mail forensics, internet forensics, cloud forensics,

Unit–IV
Introduction to IT laws & Cyber Crimes: Internet, Hacking, Cracking, Viruses, Virus Attacks, Pornography, Software Piracy, Intellectual property, Legal System of Information Technology, Social Engineering, Mail Bombs, Bug Exploits, and Cyber Security etc

Unit–V

Computer forensic cases: Developing Forensic Capabilities, Searching and Seizing Computer Related Evidence, Processing Evidence and Report Preparation, Future Issues.

Textbook:

1. John R. Vacca, “Computer Forensics: Computer Crime Scene Investigation”, Cengage Learning, 2nd Edition, 2005
2. Marjie T Britz, “Computer Forensics and Cyber Crime: An Introduction”, Pearson Education, 2nd Edition, 2008. (CHAPTERS 3 – 13).

REFERENCE BOOKS:

1. Real Digital Forensics by Keith j.Jones, Richard Bejitlich,Curtis W.Rose ,Addison Wesley Pearson Education
2. Forensic Compiling, A Tractitioneris Guide by Tony Sammes and Brain Jenkinson,Springer International edition.
3. Computer Evidence Collection &Presentation by Chrostopher L.T. Brown, Firewall Media.
4. Homeland Security, Techniques& Technologies by Jesus Mena, Firewall Media.
5. Software Forensics Collecting Evidence from the Scene of a Digital Crime by Robert M. Slade ,TMH 2005

Windows Forensics by chad Steel, Wiley India Edition.