राष्ट्रीय प्रौद्योगिकी संस्थान पटना / NATIONAL INSTITUE OF TECHNOLOGY PATNA
संगणक विज्ञान एंव अभियांत्रिकी विभाग / DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
अशोक राजपथ, पटना-८००००५, विहार / 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:

CSXX2015: ***Digital Forensics*** **L-T-P-Cr: 2-0-2-3**

Pre-requisites: Prior knowledge of fundamentals of operating systems and cyber security

Objectives/Overview:

- To identify the security vulnerability and threats in computing systems.
- To comprehend the basic digital forensics and techniques for steering the forensic examination on different digital devices.
- To realize how to examine digital evidences such as the data acquisition, identification analysis.

Course Outcomes:

At the end of the course, a student should:

S. No	Course Outcome (CO)	Mapping to POs
1.	Understand with the underlying principles of forensics	PO1
2.	Identify and formulate the research problems in digital forensics	PO2, PO3
3.	Develop the ability to design and analysis of forensic tools	PO3, PO4
4.	Analyze the forensic evidences using tools	PO5
5.	Create, apply ideas for forensic applications.	PO5, PO6

UNIT I: **Lectures: 6**

Computer forensics fundamentals, Benefits of forensics, computer crimes, computer forensics evidence and courts, legal concerns and private issues. Forensic Sciences: Basics, Ethics, Rules, Laws, Procedures. Introduction to Computers, Software, Hardware, Computer Ethics and Application Programs.

UNIT- II **Lectures: 10**

Computer forensics evidence and Investigation: understanding storage formats and digital evidence, determining the best acquisition method, acquisition tools, validating data acquisitions 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 II: **Lectures: 8**

Current computer forensic tools- software, hardware tools, validating and testing forensic software, addressing data-hiding techniques, performing remote acquisitions, E-mail investigations- investigating email crime and violations, understanding e-mail servers, specialized E-Mail forensics tool, cyber forensics. Introduction to IT laws & Cyber Crimes

UNIT III: **Lectures: 4**

Computer forensic case studies, 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.