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:

CSX4166: File System Forensic

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

Prerequisite: Computer Architecture and Operating Systems

Learning Objectives:

1. Understand the basics of disk capturing and storing
2. Know how to clean a disk, and copy evidence.
3. Know how to recover the deleted files from the disk.

Syllabus:

Unit I

Digital Investigation Foundations: Digital Investigations and Evidence, Digital Crime Scene, Investigation Process, Data Analysis, Overview of Toolkits

Computer Foundations: Data Organization, Booting Process, Hard Disk Technology

Unit II

Hard Disk Data Acquisition: Introduction, Reading the Source Data, Writing the Output Data

Volume Analysis: Introduction, Background, Analysis Basics

PC-based Partitions: DOS Partitions, Analysis Considerations, Apple Partitions, Removable Media

Unit–III

File System Analysis: File System, File System Category, Content Category, Metadata Category, File Name Category, Application Category, Application-level Search Techniques, Specific File Systems

FAT Concepts and Analysis: Introduction, ,File System Category, Content Category, Metadata Category, File Name Category

Unit–IV

FAT Data Structures: Boot Sector, FAT32 FSINFO, FAT, Directory Entries, Long File Name, Directory Entries

NTFS Concepts: Introduction, Everything is a File, MFT Concepts, MFT Entry Attribute, Concepts, Other Attribute Concepts, Indexes

Unit–V

Ext2 and Ext3 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, Application Category

Ext2 and Ext3 Data Structures: Superblock, Group Descriptor Tables, Block Bitmap, Inodes, Extended Attributes, Directory Entry, Symbolic Link, Hash Trees, Journal Data Structures

The Sleuth Kit and Autopsy

Textbook:

1. Brian Carrier, "File System Forensic Analysis", Addison Wesley Professional, 2005

REFERENCE BOOKS:

1. Dan Farmer and Wietse Venema, "Forensic Discovery", Addison Wesley
2. Harlan Carvey, "Windows Forensic Analysis Toolkit", Syngress