Course Instructors

Dr. Rinku Dewri
Associate Professor
University of Denver, USA
Email: rdewri@cs.du.edu

Dr. SamratMondal
Assistant Professor
IIT Patna, India
Email: samrat@iitp.ac.in

Who can Attend

Executives, resaerchers and field officers from regulatory, service and government organization including R&D laboratories, law firms, cyber-crime units, and law enforcement agencies.Students at all levels (BTech/MSc/MTech/PhD) or Faculty from reputed academic institutions and technical institutions.

Accomodation

There is a limited availability of accomodation in IIT Patna hostel for student participants at an affordable rate, which will be offered on a first-come-first served basis. Besides there are several hotels and guest-houses around IIT Patna where the participants may stay during the course.

About CEP

The continuing Education Programme (CEP) activity hasbeen setup to meet the manpower training and knowledgeupgradation needs of the industry, academia, and researchorganizations. The main aim of CEP of IIT Patna is toimpart knowledge related to the frontiers in science, technology, and management to the people, who want toupgrade their knowledge relevant to their field of interest.

About IIT Patna

Indian Institute of Technology Patna, established in Aug 2008, is an autonomous institute of education and research in science, engineering and technology located in Bihta, 35 km from Patna. As of today, IIT Patna has 10 academic departments that offers B.Tech, M.Tech, MSc and PhD programs.
The faculties of this institute come with academic and research training from various institutes of excellence within the country and abroad. The recent publication records of the Faculty with several practical constraints appear to be outstanding. It includes many reputed national and international journals.

About CSE Department

The department has three major programs- B.Tech CS, M.Tech CS and PhD. Additionally, there is a M.Tech in Mathematics and Computing program jointly with Mathematics dept. The CSE department is equipped with several research and teaching labs. The faculty members of the department are engaged with various research, teaching and administrative activities. The department has a liaison with reputed national and international Universities

CEP Short Term Course

Computer Forensics

16th-20th December 2019

Organized by

Department of Computer Science & Engg.
Indian Institute of Technology Patna,
Bihta-801103

Overview

Computer forensics involves the examination of information contained in digital media with the aim of recovering and analyzing latent evidence. The ubiquitous nature of digital devices and their integration into our day-to-day activities makes them one of the richest sources of information in today's criminal and civil investigations. Besides understanding the legal issues surrounding digital evidence analysis, a working knowledge of disk structures, file systems, operating system internals, file formats, and various software artifacts are crucial to correctly extract and process digital data for use in an investigation.

This course aims to introduce various computer forensics related topics through a "learning by doing" approach. The participants will obtain working knowledge of the topics in lecture sessions, and later apply them in practical (lab).

Objective

Upon successful completion, participants will be able to analyze various disk and memory forensic related issues. Participants will obtain an understanding of the basic concepts in preservation, identification, extraction and validation of forensic evidence in a computer system. Specific learning objectives include the ability to manipulate disk partitions, file systems and memory images to recover user files, deleted data and operating system artifacts from memory.
Participants will be exposed to few commercial forensics tools and will also work extensively on raw images of disks, and in the process, build components commonly seen as features of commercial tools.

Schedule

Day1	**Lecture:** Overview, evidence acquisition and disk structures (Binary data manipulation; bit stream copies; validation and filtering with hash functions; disk geometry and block addressing; surplus sector identification; MBR and GPT structures; partition extraction) **Lab:** Warmup and disk structure manipulation
Day2	**Lecture:** Windows/Linux file recovery (Logical addressing in file systems; partition organization in Windows/Linux; FAT root directory, allocation table and file data extraction; NTFS master file table and data run interpretation; NTFS metadata in attributes; Windows file deletion mechanism; ext3/4 indexing table; forensics artifacts generated by operating systems) **Lab** : File extraction in FAT and NTFS
Day3	**Lecture:** Data hiding and carving **(**Data hiding with file segmentation, cluster map manipulation, bitwise operations, rootkits, and steganography; basic data salvaging with header-footer, header-size, and header-length carving; deep carving with structural data; reconstructing fragmented files with gap carving; media triage with bulk extraction; implementation and efficiency) **Lab:** Carving unused space
Day4	**Lecture**: Memory forensics; Machine learning frontier **(**Process and memory management structures; process memory enumeration; networking artifacts; pool-scanning kernel modules; identifying hooks; disk artifacts in memory; use cases of machine learning forensics) **Lab**: Volatility framework
Day5	**Lecture:** Password file vulnerabilities **(**Password file structure, Password cracking strategies, Use of race condition to write to password file, Counter measures) **Lab**: Exploiting password file vulnerabilities

How to Register

Course Name	Computer Forensic
Course Fees:	
Rs 5000	Participants from Industry/Research Organization/ Academic Institution
Rs 3500	Students & Research Scholars

Payment Details: The participation fees for the CEP will be accepted only through DD drawn in favour of Indian Institute of Technology Patna" or e -transfer / RTGS/ NEFT

Account Details: For paying the registration fees, following account details of IIT Patna can be used. Please keep a copy of the transaction.

Account Name	Indian Institute of Technology Patna
Account No.	30957551934
IFSC Code	SBIN0017164
Bank Name	State Bank of India
Branch Name	IIT Patna, Bihta Campus
MICR No.	801002005

To register for the course, participants need to pay the fees as mentioned above. After making required payment, partcipants must send a proof of payment to skpandacs@gmail.com with a cc to samrat@iitp.ac.in along with the details of name, email, designation, organization, address, mobile, highest academic degree by 9th Dec 2019.

Also, to complete registration, participants must fill the following google form
https://forms.gle/tAcKnU2Ls1h1KTdx8

For any general query contact skpandacs@gmail.com with a cc to samrat@iitp.ac.in