Opp. Rewati Range, Gate No. 1, Sanwer Road, Jakhya, Indore (M.P.) Ph.0731-2448602
19b, Vishal Nagar, Near Allahabad Bank – Annapurna Road Indore, Madhya Pradesh, +91-9406841953
www.cybertalkindia.com | www.oui.edu.in

About the course:

Computer forensics (also known as computer forensic science) is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.
Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence.

Forensic techniques and expert knowledge are used to explain the current state of a digital artifact, such as a computer system, storage medium (e.g. hard disk or CD-ROM), or an electronic document (e.g. an email message or JPEG image). The scope of a forensic analysis can vary from simple information retrieval to reconstructing a series of events.

In a 2002 book, Computer Forensics, authors Kruse and Heiser define computer forensics as involving "the preservation, identification, extraction, documentation and interpretation of computer data". They go on to describe the discipline as "more of an art than a science", indicating that forensic methodology is backed by flexibility and extensive domain knowledge.

However, while several methods can be used to extract evidence from a given computer the strategies used by law enforcement are fairly rigid and lack the flexibility found in the civilian world.

The Online Certificate Course offered by Oriental University in Collaborations with CYBERTALKINDIA, intends to spread awareness among the general public about the complete investigation process with illustrations of the computer forensics.

Who can pursue?

Anyone who has access to a computer and the Internet can enroll for the Certification Course.

Duration of Course: 3 Months

About the exam: The exam will consist of 20 questions, 5 marks each. For passing, you need to secure a minimum of 40%. No negative marking.

Mock Examination: There will be a Mock test for the course in question

About the Assignment: You need to submit one assignment on the themes selected by the boards and it will be mailed to you. Where the selected Assignments will be published by us in a book bearing an International Standard Book Number for free of cost. (You will be charged only for Paperback edition of the Book)

Fees for the course: Rs.4500/- (For students only the amount for a hard copy of the publication will be charged extra)

Syllabus

- E-Mail & Web Forensics
  a. Exploring the world of e-mail
  b. Examining e-mail structures
  c. Finding the forensic perspective
  d. Performing e-mail forensics
  e. Looking into Web mail
  f. Checking Hotmail, Yahoo, and Google Mail
  g. Investigating Instant Messages
- Data Forensics
  a. Storage Hardware
  b. File system basics
  c. Data hiding places
  d. Data extractions
  e. Rebuilding data
- Document Forensics
  a. Finding data about data
  b. Finding the CAM
  c. Where documents are found
- Mobile Forensics
  a. Mobile device basics
  b. Becoming familiar with mobile acquisitions
  c. Extracting mobile device data
- Network Forensics
  a. Rooting network data collection
  b. Hunting through networks and traffic
  c. Speaking the language of networks
  d. Picking the right network forensics tool
- Investigating X- Files : eXotic Forensics
  a. Surprising places to look for evidence
  b. Tools for extracting evidence from nonstandard device
  c. The future of data storage