unicri
advancing security, serving justice, building peace

mediaservice.net
CORPORATE SECURITY & IMAGE

FIRST COMPREHENSIVE TRAINING PROGRAMME on CYBER CRIMES

»» Digital Forensics

Summary

In order to address the legal and technical difficulties inherent in the acquisition, preservation and processing of digital evidence, UNICRI offers a comprehensive training course on digital forensics to educate participants on the present realities of IT media involved in both computer and conventional crimes, the proper method of approaching the electronic evidence of a crime scene, data acquisition best practices and analysis methodologies, as well as and the current state of both forensic and anti-forensic tools and techniques.
The training program is structured in a (non-technical) Basic 2-day course, in a 4-day Intermediate level course, and in an intensive 7-day Advanced level course.
At the end of each course, the participant will receive a certification detailing the material covered and his or her acquired skills.

Target Audience

Basic level course

Lawyers, public prosecutors, attorney assistants, criminologists, non-technical law enforcement officers, system or network administrators, students and researchers interested in digital forensics, law court technical advisors, fraud analysts, journalists.

Intermediate and Advanced level courses

Senior-level system or network administrators, intelligence and counter-intelligence experts, fraud researchers, digital forensics experts, technically inclined law enforcement officers, persons licensed to practice law with a solid technical background.

Course Syllabus

Basic course sample topics:

» **Why** digital forensics is important;
» The nature of **computer crimes** today and conventional crimes involving IT media;
» Use of encryption to protect sensitive data, and common **anti-forensic** techniques spotted in the wild;
» **Laws** and standards in place pertaining to digital forensics;
» The **evidence acquisition phase** and the **chain of custody**;
» Open-source vs. closed-source tools and why **open-source** is preferred in the course of investigations;
» Special case studies of **digital and mobile phone forensics. Special guest lecture** is foreseen.

The *Intermediate* and *Advanced* courses address more technical aspects of forensics and include **live lab sessions**, as well as a special guest's lecture. **Sample** topics include:

» Computer crimes today and conventional crimes involving **IT media**;
» Digital Forensics methodology: from incident verification to the final report;
» Proper evidence **acquisition** and **handling**;
» Seizing volatile or **"live"** data;

- Acquiring digital evidence on both Windows and UNIX-based systems;
- Locating and **acquiring evidence on Mac OSX Server** and understanding Mac OSX security policies and File Vault;
- Establishing a **chain of custody**;
- **File system fundamentals:** different file system structures, partition schemes and timestamp analysis, etc;
- How to build an open-source **forensics lab**;
- How to analyse unallocated space and slack space;
- The concept of **"file carving"**;
- UNIX authentication systems: pam, kerberos, etc., as well as logging and accounting systems, **hidden files** and history files;
- Fundamentals and methodologies in mobile forensics: preserving evidence on mobile devices, SIM cloning, and available tools for **mobile forensics**;
- Fundamentals and methodologies in **network forensics**: networking sniffing and monitoring, available tools (Wireshark, Snort), and **analyzing VoIP**;
- How to spot common **anti-forensic techniques** used in the wild.

All trainers are from @Mediaservice.net, a leading vendor-neutral security consulting company.

Prerequisites, Equipment and Material

All participants will be required to have a solid grasp of English.
Basic level course participants are encouraged to bring a laptop or other personal computing devices in order to better enjoy and understand the course material.
Intermediate and Advanced course participants will require a laptop and are suggested to be familiar, at the very least, with basic file system structures, TCP/IP protocols and operating system concepts.
The following course material will be provided for the duration of the course: a hard drive USB mini adapter kit for SATA/IDE hard drives (1.8"/2.5"/3.5"/5.25") for the live lab sessions.

Dates, Language and Fees

Level	Running Dates	Subscription Deadline	Fee
Basic	March 29 – 30, 2010	March 22, 2010	1.000 €
Intermediate	April 12 – 15, 2010	April 5, 2010	1.800 €
Advanced	April 19 – 27, 2010 *	April 12, 2010	3.200 €

**Courses will not run over the weekend of April 24th and 25th.*

All courses will be held in English for 8 hours per day, at the United Nations Campus in Turin (Italy). Lunch and regular coffee breaks will be provided, courtesy of UNICRI. A bus shuttle service will be offered every day, before and after classes.

For further information on how to apply, or questions pertaining to the training course and accommodation please consult **www.unicri.it** or e-mail us at **cybertraining@unicri.it**

United Nations Interregional Crime and Justice Research Institute (UNICRI)

UNICRI provides applied research, training programmes and technical cooperation to assist intergovernmental, governmental and non-governmental organizations in formulating and implementing improved policies in the field of crime prevention and justice. UNICRI's main goals are: to advance understanding of crime related problems; to foster just and efficient criminal justice systems; to support the respect of international instruments; to facilitate international law enforcement cooperation and judicial assistance.

The current priorities include, inter alia, activities related to justice reform, prevention and control of international terrorism, transnational organised crime, illicit trafficking, cyber crimes, and crimes against the environment.

UNICRI
Viale Maestri del Lavoro, 10 - 10127 Turin - Italy
Tel.: (+39) 011 6537 111 - Fax: (+39) 011 6313 368