

# Computer Forensics Workshop

## Nature and Objectives

Computer forensics is an emerging area for I.T. practitioners as well as fraud investigators and legal personnel. As our daily life relies heavily in computer systems including mobile devices, evidence for hacking incidents, internal frauds or staff misconduct might exist in digital format in computer systems / devices instead of the traditional paper forms. This module will discuss the basic concepts of computer forensics, tools and procedures that can help to preserve and discover evidence from digital sources. On completion of the course, participants should:

- know about the basic procedure to preserve digital evidence;
- know how to identify, preserve and analyse evidence in computer systems / devices; and
- know about the challenge / threats to digital evidence.

## Who Should Attend:

Fraud investigators, Legal practitioners, IT Auditors and Managers, Data Security Officers, Information Security Analysts / Managers, Security Consultants, System and Network Administrators / Engineers / Analysts / Managers, and Technical Engineers / Managers. Participants are expected to have basic understanding on computer systems.

**Fee(HK\$):** 4,000 / 3,600 ( *Enrolment on or before Oct.13, 2008* )

## Course Outline:

**Code:**  
40088064

**Date:**  
Oct.13-14, 2008

**Time:**  
9:30 – 17:00

**Venue:** Hong Kong  
Productivity Council

**Medium of Instruction:**  
Cantonese (with  
terminology & handout in  
English)

**Award of Certificate:**  
Certificate of Attendance  
will be awarded to those  
attending all sessions.

## Basic Concepts

- Computer incident response
- Investigation into the computer incidents
- What is computer forensics
- Examples of legal cases involving computer records and digital evidence
- Nature of digital data
- Admissibility of evidence to court

## Digital Evidence on the Network

- Overview of IP address
- Email / Internet news tracing
- Peer-to-peer networking issues
- System logs
- Network traffic sniffing
- Limitations and challenges : impact of new networking technology and onion routing technology

## Evidence in Storage Devices

- Disk structure and common file systems
- Disk cloning and common disk imaging tools
- Slack area and deleted files
- Time/date stamps
- Evidence search
- Common tools for preservation and analysis of evidence for storage devices
- Live forensics
- Limitations and challenges

## Evidence on Mobile Devices

- Information available in common mobile devices
- Extraction of information from mobile phones : preparation and tools

## Miscellaneous Topics

- Hash set
- Volatile information
- Sources of evidence for common activities
- Tools for wiping digital data
- Tools for hiding IP address
- Steganography and digital fingerprinting
- Password cracking and rainbow tables
- Forensic readiness

## Management Considerations

- Preservation of evidence
- Chain of custody
- Best practices and guidelines
- Basic requirements for a computer forensics laboratory

**Tel: 852 2788 6266 or 852 2788 6271 / Fax: 852 2788 6260 / [ait@hkpc.org](mailto:ait@hkpc.org)**

Name: _____	Job Title: _____
Organization: _____	Fee: _____
Address: _____	
Tel: _____	Fax: _____
Email: _____	Signature: _____

- To enroll, please complete the enrolment form and send it together with the appropriate fee to ICT & Logistics Unit, Productivity Training Institute, HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong. All cheques should be crossed and made payable to "Hong Kong Productivity Council".
- Course fee must be accompanied with this form (or its photocopy), otherwise enrolment may be rejected.
- HKPC has adopted a Personal Data (Privacy) Policy. Information about the policy is available at HKPC enrolment counters for collection. You may also contact our Personal Data Controlling Officer for further details.
- Applicants are encouraged to pay by credit cards, EPS or cheques, if possible. Amount received will be imprinted. Cheques are subject to bank clearance.
- Enrolment fee is not refundable unless HKPC is notified in writing of your withdrawal at least 5 working days before the course commences. A handling charge of HK\$200 will also be levied.
- An applicant may, subject to approval from HKPC, nominate a person to attend the course on his/her behalf.
- HKPC reserves the right to change the contents, venue and / or time as necessary.
- Classes in the morning, afternoon or evening will be cancelled if typhoon signal No. 8 or above OR black rainstorm warning is still hoisted after (or is announced by the Hong Kong Observatory to be hoisted at/after) 6:00 a.m., 11:00 a.m. and 4:00 p.m. respectively. Participants will be notified when the class will be made up as soon as possible.

Organized by

