

Course Name:	Computer Forensics Workshop
Duration:	2 Day
Medium of Instruction:	Cantonese (with terminology & handout in English)
Award of Certificate:	Certificate of Attendance

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.

Course Outline:

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