香港大學數碼港學院
The Cyberport Institute of Hong Kong
The University of Hong Kong

HKU SPACE 香港大學專業進修學院
HKU School of Professional and Continuing Education

CI 63-814-00/81 "Postgraduate Diploma in IT Forensics" *(Subject to approval)*

Enquiries: 2587 3218 E-mail: corine.tam@hkuspace.hku.hk

Background

The Postgraduate Diploma in IT Forensics programme to be offered by HKU Cyberport Institute of Hong Kong (HKU Cyber.i) in conjunction with the Information Security and Forensics Society (ISFS) will provide professionals with an excellent opportunity to enhance their IT Forensics knowledge for developing his/her career to be Crime Laboratory Analyst, Forensic Engineer and Crime Scene Examiner. Graduates from IT, Business or Accounting are suitable to enroll this programme.

Aims and Objectives

This programme aims to equip participants with an in-depth knowledge on the following topics:

- Use of Digital Evidence Search Kit (DESK)
- Use forensic tool to preserve digital evidence
- Discriminating between physical and digital evidence
- Applying the Computer Crime Ordinance and Personal Data Privacy Ordinance
- Analysing different types of theft cases
- Applying the Crime Scene management technique to collect and preserve evidence

The Curriculum

This is a one-year programme consisting of 8 core modules and 2 elective modules. Each module includes 21 lecture hours, 3 non-lecture activities hours (tutorial /workshop) and 2 hours of written examination. Total Contact hours for the programme is 240 hours.

Core Module Title	**Contact Hours**
CI 63-814-01 IT Technology in a Business Environment *(Allow exemption to IT graduate)*	24
CI 63-814-02 Digital Forensics, Forensics Science and Crime Scene Management	24
CI 63-814-03 e-Business Related Legislations and Cyber Crime Management	24
CI 63-814-04 e-Business Related Legislations and Digital Banking	24
CI 63-814-05 Collecting Digital Evidence and Presentation in Court	24
CI 63-814-06 Digital Forensics Case Studies (forensics tool to preserve digital evidence)	24
CI 63-814-07 Digital Forensics Case Studies (theft of company's sensitive/proprietary information)	24
CI 63-814-08 Mock Court Exercises for IT and e-Business Related Cases	24
SUBTOTAL:	**192**
Elective Module Title (Select ANY TWO from below)	**Contact Hours**
CI 63-814-09 Digital Forensics Case Studies of Intranet Environment	24
CI 63-814-10 Digital Forensics Case Studies of Internet Environment	24
CI 63-814-11 Digital Forensics Case Studies of Mobile and Wireless Communication	24
CI 63-814-12 Current Research Issues in Digital Forensics	24
SUB-TOTAL:	**48**
GRAND TOTAL:	**240**

Delivery

The programme will be delivered in part-time mode. Different teaching formats like lectures; tutorials, workshop, case discussions and assignments will be employed. The medium of delivery is English, supplemented with Cantonese only when the case material is in Chinese. All handouts and reading materials are written in English. Case material may be in Chinese.

The minimum registration period for this programme is 12 months and the maximum registration period for this programme is three years.

Assessment and Award

To be eligible for the award of the postgraduate diploma, students must satisfy the following criteria:

- Achieve 70% attendance
- Continuous Assessment (weighting 50%) and
- Examination (weighting 50%)

Total passing score is 50%

Application Details

Day(s) Time	Starting from 19 March 2009 (Tentative schedule is listed in "Details of Modules")
Venue	HKU SPACE Learning Centre
Entry Requirements	Applicants shall: (a) (i) Hold a bachelor's degree in any discipline awarded by a recognized university; or (ii) Be practitioners with 5 years or more experience in the related field and hold recognized professional qualifications in the relevant discipline. (Practitioner includes IT/Computer engineer, Accountant/Forensic accountant, Auditor, Lawyer/Judiciary, Forensic scientist/Laboratory specialist, IT security professional, Senior Executive/CIO/IT manager); and (b) Provide evidence of English proficiency, such as (i) HKCEE English Language at Level 2; (ii) HKCEE English Language (Syllabus B) at Grade E (Grade C in the case of English Language (Syllabus A)); (iii) An overall band of 6 with subtest of 5.5 in the IELTS; (iv) A score of 550 in the paper-based TOEFL or a score of 213 in the computer-based TOEFL.
Medium of Instruction	English supplemented with Cantonese only when the case material is in Chinese
Instructors	The programme will be delivered by the following instructors from ISFS: - Dr CHAN Kwok Hung Hilton, Dr CHOW Kam Pui, Dr FUNG Wai Wa, Mr IEONG Sze Chung Ricci, Mr IP Ting Pong Vincent, Mr KWAN Yuk Kwan Michael Mr LEUNG Cheuk Yin David, Mr LI Fu Kay Frankie, Mr LUK Wing Kai Danny Mr TSE Ka Sze Hayson, and other invited speakers
Fee	HK$4,180 per module (10 modules in total)
Application and Payment Methods	- Application form can be downloaded from http://hkuspace.hku.hk/form/SF26.pdf - Application form should be returned to Ms. Corine Tam, HKU SPACE, Units 402-3, Level 4, Cyberport 1, 100 Cyberport Road, H.K. together with the following supporting documents: - i. photocopied evidence of your full name (including any change of name) and date of birth (i.e. Hong Kong identity card, passport, birth certificate, marriage certificate, deed poll or statutory declaration); ii. one set of photocopied academic / professional certificates which support your application. - Payment can be made by cash/EPS/VISA/MasterCard at any HKU SPACE enrolment counters upon receiving an offer letter from our office.
Closing Date	**21 February 2009**

Details of Modules

Core Modules: -

CI 63-814-01 IT Technology in a Business Environment ***(Allow exemption to IT graduate)***

(Tue & Thu 7 – 10 p.m.; Mar 19 – Apr 14)

This module will provide the non-IT participant a fundamental understanding of the key computing concepts and technologies. Topics included computer architecture, electronic storage media, file structure, data storage/retrieval, operating systems, boot up process, IP address, DESK (Digital Evidence Search Kit) and digital signature.

CI 63-814-02 Digital Forensics, Forensics Science and Crime Scene Management

(Sat 2 – 6 p.m.; Apr 18 – May 30)

The module participants will learn about the theories and concepts about digital forensics. Topics included Ethics and professionalism; constituents and categories of digital forensics; fundamental principles in performing computer forensic examination; similarities and differences between physical and digital evidence; challenges and future development of digital evidence; procedures to handle digital evidence during or after an IT security incident, ways to preserve the integrity of digital evidence for future legal proceedings, crime scene analysis with computers.

CI 63-814-03 e-Business Related Legislations and Cyber Crime Management

(Tue & Thu 7 – 10 p.m.; May 26 – Jun 23)

The module participants will learn about the UN model laws on Computer Crime and e-Commerce with reference to the related legislations in Hong Kong. Topics included Computer Crime Ordinance and Personal Data Privacy Ordinance; fundamental skills required to conduct criminal investigations; knowledge to inter-relate the investigative process to the total criminal justice process.

CI 63-814-04 e-Business Related Legislations and Digital Banking

(Wed & Fri 7 – 10 p.m.; Jun 17 – Jul 15)

The module participants will learn about the knowledge on how to start an investigation, collect evidence, and prepare prosecution/defence of an IT crime or e-business incident, Internet security related to Internet banking, e-Commerce, theft of digital assets, copyright infringement, Legislations such as Electronic Transaction Ordinance, Intellectual Property/ Copyright ordinance.

CI 63-814-05 Collecting Digital Evidence and Presentation in Court

(Sat 2 – 6 p.m.; Oct 24 – Nov 28)

The course participants will learn about the knowledge on the trial process, the admissibility of exhibits/documents, difference types of evidence (traditional evidence vs. digital evidence), Evidence Ordinance, Admissibility of computer records, Role of expert witness/testimony in Court, Role of scientists and engineering experts in litigation, Principles of effective expert testimony.

CI 63-814-06 Digital Forensics Case Studies (forensics tool to preserve digital evidence)

(Sat 2 – 6 p.m.; Jun 6 – Jul 11)

This module is a hands-on laboratory teaching, topics included:

- Knowledge on using the computer forensic tool, i.e. DESK (Digital Evidence Search Kit) to preserve digital evidence, conducts forensic analysis and data mining, and reconstructing the cyber crime scene.
- Issues, techniques, and vulnerabilities of digital device forensics;
- Acquisition, preservation, analysis and presentation of digital devices as evidence.
- Collect, examine, and preserve digital evidence in support of criminal investigations, civil investigations, and sensitive business matters.
- Cyber forensics discipline

CI 63-814-07 Digital Forensics Case Studies (theft of company's sensitive/proprietary information)

(Sat 2 – 6 p.m.; Sep 5 – Oct 17)

The module participants will learn how to collect, preserve and analyze the following simulated cases:

- Theft of company's sensitive / proprietary information
- Theft of company's digital properties
- Emails
- Obscene and incidents files,
- Digital signature
- E-banking transactions

CI 63-814-08 Mock Court Exercises for IT and e-Business Related Cases

(Tue & Thu 6:30 – 10:30 p.m.; Dec 1 – Dec 17)

During the Mock Court exercise, the course participants will prepare the digital forensic cases from the lab session, and play the role as an expert witness for either the plaintiff/prosecution or the defence, and giving expert evidence or challenge the digital evidence respectively.

Elective Modules: - (choose 2 modules)

(Schedule to be confirmed)

CI 63-814-09 Digital Forensics Case Studies of Intranet Environment

The module participants will have to prepare the forensic analysis report for giving expert evidence in Court. The simulated cases will be a mixed of the following incidents - Internal hackers, leakage of corporate information/emails, breach of corporate IT security policies, industrial espionage.

CI 63-814-10 Digital Forensics Case Studies of Internet Environment

The module participants will have to prepare the forensic analysis report for giving expert evidence in Court. The simulated cases will be a mixed of the following incidents - DDOS, e-fraud, e-financial transactions, external hacking, copyright infringement, etc.

CI 63-814-11 Digital Forensics Case Studies of Mobile and Wireless Communication

The module participants will learn the followings:

- Wireless Threats: Cracking WEP - Hacking Techniques- Wireless Attacks – Airborne Viruses
- Security Principles: Authentication, Access control and Authorization
- Privacy in Wireless World: Attacks and vulnerabilities
- Secure authentication for mobile users – Mobile Commerce security, Payment methods, Mobile Coalition key evolving Digital Signatures scheme for wireless mobile networks

CI 63-814-12 Current Research Issues in Digital Forensics

The module participant will learn about the followings:

- Protection of intellectual property on electronic networks through trademarks, copyrights and patents.
- Privacy and liability issues will be examined in areas that include the handling of e-mail, the electronic dissemination of data and the regulatory requirements for the safeguarding of confidentiality of information.
- Society's responsibility to provide universal availability of web-based technologies is considered, and an ethical framework for the development and implementation of EC applications is developed.