行政院及所屬各機關出國報告
（出國類別：實習）

參加2009年國際電腦調查專家協會(IACIS)訓練課程心得報告

服務機關　：法務部調查局

出國人姓名：林調查員雅婷(資通安全處)

出國地點　：美國佛羅里達州奧蘭多市

出國日期　：中華民國98年4月27日至5月8日

報告日期　：中華民國98年7月1日

參加2009年國際電腦調查專家協會(IACIS)訓練課程心得報告

目錄

壹、 目的

此行主要目的係參加 2009 年國際電腦調查專家協會(The International Association of Computer Investigative Specialists – IACIS,以下簡稱 IACIS)之基礎訓練課程，學習電腦鑑識相關技術。

貳、 行程記述

一、 行程往返： 2009 年 4 月 25 日自桃園中正機場搭乘國泰航空至香港及紐約轉機後，順利抵達奧蘭多國際機場。參加為期 2 週之鑑識人員基礎訓練課程，課程結束後， 於 5 月 9 日自奧蘭多國際機場先後至洛杉磯、香港轉機後，抵達台灣。

二、 受訓時程：2009 IACIS Basic Conference 之訓練課程自 2009 年 4 月 27 日起至 5 月 8 日止，實際上課天數共計 10 天，假美國佛羅里達州奧蘭多喜來登飯店之國際會議廳舉行。

參、 協會簡介

一、 源起：

國際電腦調查專家協會(IACIS)，創始於 1990 年，該協會當

初係由一群非營利之電腦鑑識領域愛好者所組成，成員多為美國當地執法機構人員或相關領域專家學者。因鑑於電腦犯罪案件日新月異，電腦取證培訓機構相當缺乏，執法單位也相繼遭遇挑戰，因此培養專業鑑識人員乃為迫切需求，亦是該機構核心價值。

二、 目的：

該協會自 1990 年起，於每年 4 月下旬至 5 月上旬，提供電腦鑑識相關訓練課程，並致力培養更多專業電腦鑑識執法人員及提供正規電腦鑑識認證考試，藉此提升打擊電腦犯罪之能量。歷年來已經訓練了數千名來自世界各國執法單位電腦鑑識人員。除提供嚴謹及多樣化的訓練課程外，該協會亦提供 2 種電腦鑑識認證考試平台，包括：

（一） 電腦鑑識人員認證(Certified Forensic Computer Examiner，以下簡稱 CFCE)考試。

（二） 電子證據蒐證專家認證(Certified Electronic Evidence Collection Specialist，以下簡稱 CEECS)考試。

三、 成員：

IACIS 是一個國際性組織，負責培訓來自世界各國之執

法人員，目前會員人數約數千人，遍布全球三十餘國，為國際上重要之電腦鑑識科學組織。由於該協會會員身兼教練，多數為現職美國執法人員亦或退休人員，且已通過專業認證，因此舉辦課程期間均為教練利用自己私人假期前來協助課程進行，故每年只舉辦一次訓練課程，4 月下旬至 5 月上旬於佛羅里達奧蘭多舉辦為期兩周的電腦鑑識訓練課程。

肆、 訓練課程

一、 學員報到

由於學員人數達兩百多人，為避免學員集中湧入，影響早上報到手續之順利進行，因此，學員可於 4 月 26 日（即正式上課前一天)晚上 7 點後，提前至會場報到，除填寫個人基本資料外，並當場拍照，以便製作學員上課證，註冊費用為每人 $1995 美元，已先於網路報名時線上刷卡繳費，報名費用比前年提高 200 美金。

二、 學員組成

本次參與電腦鑑識訓練課程的人員約為兩百多人，學員國家分布相當廣泛，亞洲國家包含有台灣、香港廉政公署、香港

海關、中國大陸、日本、韓國等國家，歐美國家則有美國、加拿大、英國、紐西蘭、德國、西班牙等。

三、 電腦鑑識訓練課程概述

（一） 首日早場為開幕式與訓練課程介紹，及簡要介紹上課講師與教練。

（二） 每天上課時間為早上 8 點至下午 5 點，中午 12 時至下午 1 時為中午用餐休息時間。

（三） 每六位學員指派一名教練(coach)，負責從旁協助學員上機實作練習作業、講義分發作業及問題解答等。

（四） 每晚 6 點至 6 點半安排電腦鑑識軟、硬體廠商做簡報，介紹對電腦鑑識業務有助益之相關軟、硬體產品。

（五） 主辦單位在晚上另行提供個別指導時間，以利進一步將白天所學之各類電腦鑑識理論加以實作及提供問題解答，對於與來自各國之執法人員，在受訓後返回到個人工作崗位時，更能確實在最短時間內將課程上所學之電腦鑑識技術與技巧應用至實際案件上。

四、 第一天課程內容：

電腦鑑識簡介(Intro to Forensics)、電腦犯罪(Computer Crime)、電腦鑑識道德與標準(Ethics and Standards)、硬

體簡介(Intro to Hardware)、犯罪現場(Crime Scene)、搜索扣押現場(Seizure Practice)。

五、 第二天課程內容：

電子證據蒐證專家認證考試(CEECS TEST)、搜索扣押現場(Seizure Practice)、虛擬機器(Virtual Machine)、位元與位元組(Bits &Bytes)、基礎輸入輸出系統與系統開機順序(BIOS & Boot Sequence)、磁碟物理結構簡介(Physical Disk Structures)、磁碟邏輯結構簡介(Logical Disk Structures)。

六、 第三天課程內容

DOS 作業系統簡介(DOS)、磁碟編輯程式(Disk Editor)、鑑識開機磁碟與實作練習(Forensic Boot Disk and Practical Exercises)、媒體清除與確認(Media Sterilization & Validation)、雜湊法及雜湊集(Hashing & Hash Sets)。

七、 第四天課程內容

鑑識備份程序簡介(Forensic Back-Up Theory)、鑑識備份及硬碟映像檔製作練習(Forensic Backup & Hard Drive Imaging Practical Exercises)、鑑識備份與防寫裝置(Forensic Backup & Write Blocking Device)、FAT 檔案系

統結構簡介(FAT File System Structure)

八、 第五天課程內容

FAT 檔案系統結構復原介紹(FAT-FS Recovery)、FAT 檔案系統結構練習(FAT-FS Practical Exercises)。

九、 第六天課程內容

NTFS 檔案系統結構簡介(NTFS File System Overview)、NTFS 檔案系統結構練習(NTFS-FS Practical Exercises)。

十、 第七天課程內容

檔案標頭資訊(File Headers & Compression)、檔案結構與屬性(File Structure & Attributes)、作業系統證據(OS Evidence)、系統登錄檔(Registry)、網路加工(Internet Artifacts)。

十一、 第八天上課內容

鑑識方法論(Forensic Methodologies)、報告撰寫(Report Writing)。

十二、 第九天上課內容

SPADA 鑑識工具軟體基礎介紹(SPADA)、影像備份實作考試(Imaging Practical Test)。

十三、 第十天上課內容

法庭證言介紹(Courtroom Testimony)、移動式儲存媒體(Removable Media)、MAC-OS（麥塔基作業系統)、CFCE考試流程(CFCE Process)。

十四、 本次全部與會學員之訓練證書及CEECS證照也於課程結束時轉交給每位學員。

十五、 學員結訓後可參加CFCE考試，在一年內依序完成5題實機測試題及通過最終筆試測驗，學員必須充分掌握考試時間及克服語言障礙，方能取的最後CFCE證書。

伍、 心得報告

（一） 對於提昇工作經驗與技巧獲益良多:

1. 國際電腦調查專家協會(IACIS)之工作人員及會員皆為世界各國在電腦鑑識領域相當優秀之鑑識人員，此次參與基礎訓練課程對於交換彼此工作經驗及吸取新知上有莫大助益，此次係本局第 3 次派員與會，在與會期間亦通過電子證據蒐證專家(CEECS)證照考試，為本局多增一張證照。

2. 課程中除了理論的講解、專有名詞的說明外，亦加入許多實作課程，硬體的實作與軟體的操作，相輔相

成，對於新進人員而言是非常扎實的訓練。此外，講師教授的課程內容亦相當廣泛，一步步帶領學員深入了解浩瀚之電腦鑑識科學領域。

（二） 與外國鑑識人員資訊交流:

貼心的工作人員特地將來自香港廉政公署與香港海關之學員跟我的座位安排在一起，兩個星期的密集上課課程中，讓我更能深入了解香港的電腦鑑識發展;香港海關在2001 年即成立電腦鑑識部門，而本局於 2005 年才籌劃成立電腦鑑識實驗室，起步已經落後。此外，香港對專業鑑識人員培育也不餘遺力，年年派員赴外國學習更先進技術亦或進行學術交流。再者，香港雖然回歸中國大陸，但仍是以英文為官方語言，因此英文程度比我們優異，語言方面的優勢，大幅降低學習門檻，所以我們更需不斷提升自己的英文能力。香港鑑識人員對自我的要求也很高，上課認真積極，倘若遇到問題，會舉手發問，每個人都擁有數張電腦鑑識專業認證。此次課程，除了電腦專業技術讓我受益良多外，最令我感到震撼的是了解其他國家的公僕是如何替自己國家努力付出，利用最新科技，讓違法亂紀份子於電腦證物證實下百口莫辯。反觀台灣，各執法單位對

電腦證物鑑識之重要性，近幾年來才慢慢正視，我們起步已晚，更應該加倍努力，迎頭趕上才是。

陸、 建議

（一） 鑑識人員認證及人員訓練規範

鑑識實驗室的鑑識人員應訂定鑑識人員資格，相關人員必須受過相關鑑識訓練、至少取得一項電腦鑑識領域相關證照，以確保操作鑑識設備、執行鑑識程序及撰寫鑑識報告之可信度。此外，鑑識工作亦是經驗傳承的工作，必須對鑑識工具有廣泛的涉獵，對各種犯罪態樣能有一定的認知，方能找出最佳利器，一舉蒐得最具證據力之證物，因此學長們彼此間鑑識經驗的交流與薪火相傳亦相當重要。

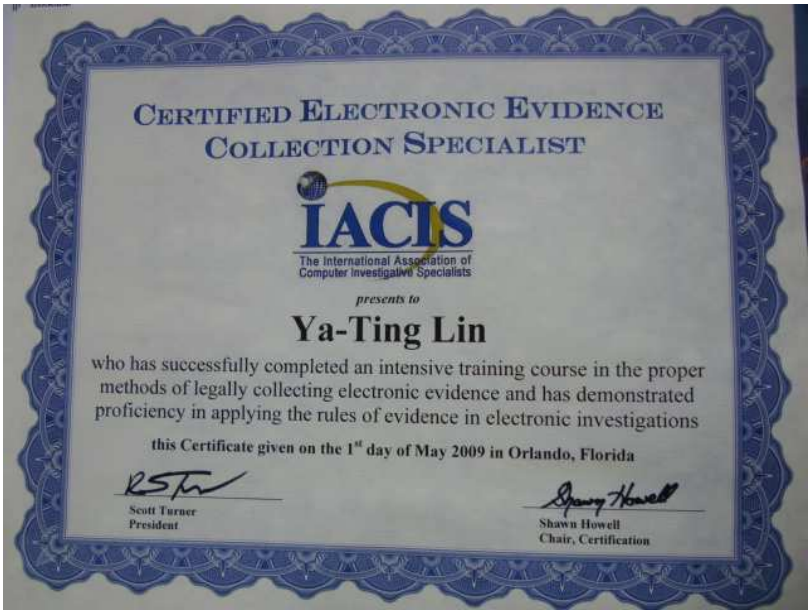
（二） 資安鑑識實驗室之認證

資安鑑識實驗室設立之目的，在於提供具有證據力與證據能力之鑑識報告。然而國內負責實驗室認證單位係為「財團法人全國認證基金會」，尚未具有電腦證物實驗室之認證標準可供依循。本實驗室也尚待制定一套證物實驗室的標準作業流程與文件管理程序，倘若本局資安鑑識實驗室能通過實驗室認證，成為具有認證資格之鑑識實驗室，將

更能提高鑑識結果之說服力及可信度。

上課情形

與來自香港廉政公署與香港海關的學員合影



CERTIFIED ELECTRONIC EVIDENCE COLLECTION SPECIALIST

IACIS
The International Association of Computer Investigative Specialists

presents to

Ya-Ting Lin

who has successfully completed an intensive training course in the proper methods of legally collecting electronic evidence and has demonstrated proficiency in applying the rules of evidence in electronic investigations

this Certificate given on the 1st day of May 2009 in Orlando, Florida

Scott Turner
President

Shawn Howell
Chair, Certification

CEECS 證書

IACIS
The International Association of Computer Investigative Specialists

Presents this

Certificate of Course Completion

To

Ya-Ting Lin

for successful completion of the 80 hour

Forensic Computer Examiner Training Program

Given this 8th day of May 2009 in Orlando, Florida

Scott Turner
President

Heather Strong
Chair, Basic Training

完成 80 個小時之課程認證