行政院所屬各機關出國報告
出國類別：研習）

赴英國警政、學術單位及民間顧問公司數位鑑識實驗室及專業廠商參訪心得報告

服務機關 ： 法務部調查局資通安全處(原資訊室)

出國人姓名 ： 陳調查專員受湛(資通安全處);林調查員怡伶(台北市調查處)

出國地點 ： 英國倫敦

出國期間 ： 中華民國 97 年 12 月 6 日至 12 月 13 日

報告日期 ： 中華民國 98 年 2 月 12 日

赴英國警政、學術單位及民間顧問公司數位鑑識實驗室及專業廠商參訪心得報告

目錄

壹、緣起

為執行本局「資通安全鑑識實驗室」97年度科技計畫中有關「赴英美地區警政單位數位鑑識實驗室及當地專業廠商參訪研習各類儲存媒體數位鑑識新技術」案，經簽准派資通安全處(原資訊室)陳調查專員受湛及台北市調查處林調查員共赴英國參訪研習。

貳、目的

電腦鑑識科學在西方國家是較為深入並成熟的領域，以往本局為提昇電腦鑑識之技術能量，在成立資安鑑識實驗室之初期，多仰仗美國在此領域之專業技術與經驗，而較少接觸歐洲國家執法單位在此領域之現況。

此次前往英國拜會皇家警察在反恐單位之電腦鑑識小組，瞭解其組織及其運作模式，並與民間鑑識公司之合作方式，均有許多參考價值，並且鑑識所使用之工具與作業平台與美國有頗多差異。另接觸英國皇家哈洛威大學資訊安全小組，瞭解英國學術界在電腦鑑識及網路安全之研究方向及教育課程內容，與國內有那些異同之處。並藉此次參訪，建立與歐洲國家在電腦鑑識領域之合作交流管道。

參、參訪行程

本次參訪由資通安全處陳調查專員受湛及臺北市調查處林調查

員怡伶於中華民國 97 年 12 月 5 日星期五上午 09:00 搭乘長榮航空公司 BR-67 班機出發前往英國，抵達倫敦希斯羅國際機場，時間為當地時間 12 月 5 日下午 07:04（以下均為當地時間），開始此次參訪行程。利用一週的時間，從皇家哈洛威大學、英國皇家警察、顧問公司及相關廠商等單位，行程緊湊地一一參訪，最後於 12 月 12 日星期五晚上結束行程返國，參訪行程如下：

12 月 6 日（週六）皇家哈洛威大學宿舍整備資料 Royal Holloway University of London

此參訪團初到英國，先與校方聯繫，並開始準備此週之活動行程。並瞭解倫敦市區之交通工具，及瞭解並品嚐學校的餐飲情形。

12 月 7 日（週日）皇家哈洛威大學校園環境認識 Royal Holloway University of London

利用假日瞭解學校環境，包括所住的宿舍及校園各個教學大樓。英國倫敦大學是非常古老的學校，其建築物均非常雄偉並具歷史意義。

12 月 8 日（週一）皇家哈洛威大學 Royal Holloway University of London

Information Security Group 皇家哈洛威大學數學系資訊安全組。

此行的第一個參訪單位是皇家哈洛威大學資訊安全組，12 月 8 日中

午 10 點抵達 Dr Stephen D Wolthusen 教授的辦公室(Mc Grea Buiding 535)，先簡要與 Stephen 教授確認週一至週五之所有參訪行程，接著 Stephen 教授引導至教職員餐廳用餐。下午先介紹資安鑑識實驗室的建置過程：

一、 資安鑑識實驗室是於 2 年前成立，包括建置證物室，證物備份室，鑑識分析室，案件討論室及展示室，現有人員 7 人。

二、 95 年 4 月本局曾派員參訪美國聯邦調查局總部及 FBI 電腦鑑識實驗室等相關單位並座談，作為建置之參考。

三、 實驗室於 97 年通過 ISMS 認證，並參與多項國際性研討會議，如 IACIS、HTCIA、RCFG 等，另參加相關鑑識工具之教育訓練，

四、 與政府相關單位有密切聯繫並相互合作。

因此電腦鑑識領域亟需要法律面及技術面之支援，實驗室成立兩年至今，主要有兩項任務，一是協助犯罪調查部門取得數位證據，二是分析鑑定所取得之數位證據為呈堂證供。數位證據之蒐集對象，因著電子科技之不斷研發創新，不只來自於電腦設備，亦來自於其它電子儲存媒體如手機、PDA 等各式可攜式電子產品，故須不斷學習新產品之鑑識技術與技巧。此次來訪就是想瞭

解並接觸相關軟、硬體之資訊，並藉由此次的拜訪開啟直接的接觸，以便將來有機會與歐洲地區的聯繫。2005 年本局曾舉辦鑑識科學之國際研討會，其中有一議題即為數位鑑識，希望將來能聯繫英國學者、警方、廠商等，共同主持並參與專業研討會。資訊安全領域非常廣，台灣已有些大學參與研究數位鑑識，但只是在初始階段而已，且包含的領域又太廣泛，未來希望能研發一套簡單操作並標準程序之鑑識軟體，可提供第一線調查人員簡易的鑑識工具，能產生基本之鑑識結果。

Stephen 教授表示該資訊安全組在學校數學系所裡是目前最資深的小組，有 13 年的研究經驗，該部有 20 多位教授，各有不同專長領域。研究如資訊安全及網路犯罪分析相關議題，其中也有鑑識相關研究，在目前其一年的教學研究計畫中，研究生須閱讀 30 多本專業書籍。又學校於兩年前規定，基本的學士學位需 3 至 4 年全職完成，接著碩士學位需 1 年完成，完成此階段即可獲得足以在相關產業工作之認可資格，博士學位則需 4 年完成，3 年內先修完學分，最後 1 年完成論文，故需全力集中學習研究，通常都是全職進修，不會兼職。英國籍生多為單純學生背景，而海外學生，有些已有相關工作經歷。至於畢業後就職那些領域的工作？就目前來看尚未有特定的發展，有些是資訊業廠商，有些是政府機關，有些則是會計公司，只要有資安發

展潛力，學生畢業後都可能投入就職。而台灣並未多此方面就業機會，主因是由於臺灣業界尚未普遍重視資安領域潛在問題。

下午 2 點 Fred Piper 教授前來參與座談，並帶來兩本關於 MSC in Information Security 及 The Information Security Group Brief History 的簡介。

Stephen 教授接著表示，另外學生最好能有基本的法律、電腦基礎背景，才能有辦法接受資訊安全與鑑識之學識，有些領域更可能需要電子學背景。目前該校分為 Full-time 全職生、Part-time 在職生、Block Mode 密集課程訓練、Distance Learning 遠距課程訓練，可利用不同方式取得學分。另外還有面授短期班（如一、二、四天，建議十天較能學習全貌）之訓練基本課程，但最建議仍是當全職生。並期許將來有機會派員來該校學習，於一年內取得碩士學位，只要學生對此領域真有興趣，甚至不用一年，可能於數個月內即可取得碩士學位。這是國際化的教學機構，學生來自於不同國家，利用遠距教學、及利用網路環境即可教學，關鍵在於碩士學位即能取得相關領域工作之資格，但要取得博士學位就有難度，真的是有興趣研究者才有辦法完成。另外學生需要如何獲得可用之資訊安全技能，或從何基礎研究開始，校方均有完善之訓練計畫，且每週均提供學生不同討論主題。根據此教學研究計劃完成後，學生即可取得碩士學位並就業。

下午拜訪 Keith Mayes 博士(Smart Card Centre Director)的 ISG Smart Card Centre。其學生 Dr Konstantinos Markantonakis 一同列席座談。

Keith Mayes 博士表示，其研究部門於 2002 年成立，其學生亦有來自於台灣、中國，並與來自台灣之機構合作，其部門主要研究 Smart Cards、手機 SIM 卡等電子產品之偵查鑑識軟硬體設備，首先展示一套名為 USIM detective 軟體，可用於鑑識分析手機 SIM 卡內含之數位資訊。將 SIM 卡插入 USB 界面之接收器後，只要簡易四個步驟（插入、輸入所需資訊、分析鑑識、儲存），即可產出詳細報告，如 SIM 卡類型、Pin Code、服務廠商、通訊錄名簿、儲存的 MSIDN 資訊、訊息、撥打或接通電話記錄、2G 或 3G 網路相關資訊（最近使用之區域所在地），此套軟體係商業用途，惟中文系統辨識仍有待改進。

為瞭解此軟體是否只能運用於手機之 SIM 卡辨識及讀取其內資料，詢問可否直接連接手機作鑑識分析，是否考量因時間久遠，可能已經沒有電力，可能開機需要密碼或可能早已註銷手機號碼，而這些手機服務廠商又要求需在開機狀況才能連接提供手機內含資訊，只是分析 SIM 卡，可能無法取得儲存於手機內之相關資訊，故鑑識工具與方式之不同，將影響數位證物之取得。唯 Keith Mayes 教授回答目前仍無法突破。又因手機功能日新月異，在數年前只有 2G，現在推

出了 3G，若無與廠商合作，可能無法取得即時有效之協助，以支援該類證物分析鑑識所需之專業技術並研析犯罪模式，故需不斷與國內相關科技廠商聯繫合作，以便解決所遭遇之問題。

接著 Keith Mayes 博士展示 SCC-SHOWCASE LAB，該實驗室研究以下領域，1.Smart Card 分析、2.Finger TIP(infineon) 3.ORGA JAVA Card 4.CHIP ATTACKS(Si Venture) 5.商品雷射貼紙(SPYCARE) 6.雷達 7.手機 SIM 卡或信用卡晶片分析 8.實體電子記憶體。學生並展示其研究成果，如卡片感應器、手機資訊分析等。

Stephen 教授表示，因為該中心是較私密的單位，故無法討論太深入之議題。現行的制度是博士生研發產品相關軟、硬體技術，英國政府會給予其工作機會，使其能有機會繼續研發其研究產品。但廠商不願提供員工全職就讀，怕員工學成後另尋更好的工作機會，故有些公司則是與員工簽約，要一直在單位內任職直到完成學業才可取得更優漏的工作條件。目前該部門應該至少有 60 多名學生畢業後擔任資訊安全相關之工作。

接著常駐皇家哈洛威大學資訊中心，專研 IT Security 之 ABATIS(UK)LTD 公司的 Kerry Davies(Director)及 William Rothwell(Management Director)先生參與座談。首先 Kerry Davies 先生介紹其任職此公司之緣由，鑑於虛擬網路世界所遭受到之各種攻擊，

如 malware、rootkit、駭客入侵等，希望能協助政府及學術單位提供相關資訊安全實務上支援。該公司亦提供學生實習機會，在英國大多公司都有資訊安全部門。但目前在台灣仍為少數，主因是產業界不願負擔太多成本，多傾向委外給專業廠商，亦少有結合學術單位之研發。若能結合學術單位之師生做資安方面研究發展，相對是有利的。

Kerry 先生表示，該公司自 1992 年開始即投入資安系統研發，但資訊安全發展不易，須要耗費時間人力，且又與各產業有密切的關係而面臨到許多難題。本參訪團亦藉此機會介紹國內情形：目前台灣從事資安產業之公司為數不多，但已有了起步；政府亦開始重視，因著駭客竊取機密資訊的案件日益嚴重，有些政府網站已開始委外由專業廠商來代管。又最近 2 到 3 年資訊安全相關議題已日漸受到產業重視，與鑑識有關的議題也受到關注，因為有資安問題，就有數位鑑識工作。因前所述電腦案件犯罪多為公司內部人員所為，公司必須有能力舉證其涉案之數位證據，故相關軟硬體的鑑識是極為重要，惟在鑑識過程中須保持中立，才能使鑑識報告有其可信度。目前每年均安排人員訓練，包括內部人員及協助友軍單位等，並表示很高興能與該公司聯繫，並多保持聯繫，相信有機會建立合作關係。

12 月 9 日（星期二）早上至QCC，下午至Metropolitan Police Counter Terrorism Command, Forensics Division

上午先至 Stephen 教授辦公室，Stephen 教授詳細介紹將自今(98)年 9 月開始，為期一年的教學研究計畫之各個主要教學議題，包含

1.Windows 作業系統

2.Encase 的操作

3.Unix 及麥金塔等作業系統

4.電腦鑑識基本概念

Stephen 教授非常推崇 VERITAS 著名電腦公司所撰寫之 UNIX FileSystem 等幾本著作，包括如何蒐集資料供鑑識、檔案系統原理、基本協定原則、網路 traffic、malware 如何入侵系統、破解隱藏於多媒體資料中的資訊。瞭解特別裝置如光碟、隨身碟、手機、GPS 等儲存異同、儲存於虛擬網路上之資訊。

之後 John Austen 教授加入座談，教授高齡 72 歲，係退休警官，主要偵察電腦犯罪，參訪團向其介紹此行目的，John 教授亦分享幾例其跨國偵察駭客犯罪之案例。

隨後 John Austen 教授陪同前往參訪 QCC 資訊安全公司(QCC Information Security Ltd.)。該公司為英國警方所正式簽約之五家電腦鑑識公司之一，且是最具規模者，專替英國警方處理所移送之電腦鑑識案件。

我們會見了 Neil Hare-Brown(Senior Security Advisor)、Phil

Swinburne(Senior Security Advisor)、Robert Boyes(Director of Forensics)、John Douglas(Forensic Computing Specialist)等先生，為該公司之員工。

首先向該公司成員介紹此行目的，並說明實驗室業務與英國警方業務之異同，與英國一樣都擁有相同的鑑識單位，只是分屬於不同架構之下。並與該公司分享所使用之鑑識軟、硬體設備，如 Guidance 之 Encase、AccessData 之 FTK 的經驗交流，(中文辨識是所面臨之一項問題)。該公司提及 FTK 2.0 所使用資料庫 Oracle 容量相當大，運作起來效能不佳，而版本 1.8 雖然較穩定，但僅於部分電腦系統使用。

下午實地參觀其三間辦公室。第一間辦公室係蒐集電子設備之電磁記錄，在不破壞原始狀態下，將其轉換成映像檔存於硬碟後交實驗室鑑識分析，其擁有各式規格之界面設備，以便讀取不同規格之儲存媒體，轉換成映像檔後的電子設備另外置於房間內之證據室，John 先生特別說明所有扣押之證物將不歸還所有人，起訴後將銷毀或送供警方研究使用。第二間辦公室專門蒐集手機電磁紀錄，潘朵拉的盒子 SHU 係一項非常強的設備，建議使用。JOHN 並展示實例，每個案件都需有警方的授權委託書，內有此案件專責之警方及承辦人資料、嫌犯資料、案件說明及需求、及警方授權章。每個案件都需有該委託書，QCC 分析人員才可開始執行鑑識分析程序，並嚴格依據 ISO9001

標準作業程序，產製標準鑑識報告提交給法院。第三間辦公室 Forensics Computing LAB 專責鑑識第一間辦公室所交來之映像檔及報告，檢查其鑑識結果是否正確。目前該公司有 7 位員工，每位員工基本都會配有 3 部電腦，一部供外網，另外兩部做為鑑識之用。

下午離開 QCC 公司，轉乘地鐵抵達位於 St James’s Park 參訪英國皇家警局，由接待人員(該員為英國皇家警察 New Scotland Yard SO15 CTC 的成員)引導進入參觀英國警方國際炸彈資料中心，由中心主任講解，此中心係 911 後所成立，內含歷年來各國恐怖事件炸彈攻擊案件之研究，室內陳列各種炸彈製作之基本模型，小至煙盒，大至利用鐵筒，而炸彈基本原料僅需電池、打火機、糖即可製作簡易型但具威力之炸彈，並以電腦多媒體展示相關運作原理。

參觀後，轉乘地鐵於下午 3 點 30 分抵達 Frank O’Nill House 大樓，拜會英國反恐任務特勤組電腦鑑識單位，首先參觀其電腦鑑識流程及運送，包括收取所移送至此之電磁記錄的工作室，內有一個很大的工作平台，以便處理各式電子設備及內含之電磁記錄，並視需要處理掃瞄機、影印機等設備資料。接著介紹其辦公處所，共有 15 位鑑識人員，每位人員都從事鑑識相關工作，個人均擁有各式鑑識設備及軟體（如 Encase、FTK 惟視個人習慣使用），3 部麥金塔電腦（較穩定，分割磁區後安裝不同作業系統，鑑識軟體可各安裝在不同作業系

統上)，外接直插式硬碟讀取機， 各種尺寸之 STORM CASE 鑑識工具箱（就近放置於可隨時外出攜帶之位置)、使用之鑑識軟體（推崇比 Helix 更好用的鑑識軟體 Raptor)，L 型辦公桌，桌上都有櫃子，置放相關鑑識工具軟體書籍、各式作業系統。接著由該組某鑑識人員介紹其單位同仁均普遍使用之 smart 鑑識軟體，此軟體僅需其軟體光碟及一 USB 界面裝置，將所需鑑識之硬碟（不論是何作業系統）插入此裝置，即可利用此 smart 軟體進入鑑識作業，其操作界面非常簡易好用。

下午 4 點 50 離開，晚上 8 點 55 分至 waterloo 搭乘火車回 Egham，抵達時間 9 點 25，再搭 John 的車回到旅館時間 9 點 45 分，結束今日參訪行程。

12 月 10 日（星期三）參訪 MMI無線網路偵查手機犯罪

上午 9 點前往該公司，於上午 9 點 45 分抵達位於 Hampshire Hartley Wintney 的 MMI RESEARCH 公司 (Communications and security solutions)。首先由 Neil Craigie 先生(account manager)為我們展視該公司無線網路偵查手機犯罪技術。投影片分四部分介紹：Introductions、company profile、solution 、equipment protfile。

該產品主要研究追蹤目標手機通訊，該公司是由 Cobham Plc 集

團所屬，成立已有 12 年時間，目前已有可追蹤並監視第三代 GSM 手機通訊之軟、硬體解決方案，新加坡及華盛頓各有其分公司。設計基本概念包括：

一、固定截取 Fixed Interception：GSM 手機會尋找網路蜂巢連線，並永遠尋找最強的訊號。利用此原則，GSM_XPZ 會複制鄰近 cell，並提供更強的訊號力。以致手機都會自動導向其機器，再由其連接實際電話網路。

二、目標辨識 Target Identification：撥打任何手機*#06#會顯示獨一無二的 IMEI 資訊。開車行進中的目標手機每經過一建築物（家、旅館、高塔），因為會自動搜尋訊號，自動註冊區域，故利用此特性，即能即時辨識目標手機所在地，並回傳相關資料(MSISDN、Cell ID、Call REC 等)，及所經過路線的繪圖 Pattern of Life、即使更換 SIM 卡亦無所遁形。

三、目標定位 Direction Finding：手機每至一新地點，即會主動註冊取得區域號碼，利用此特性，即可利用網路商提供之通話紀錄取得目標手機之 IMSI 追蹤 GSM cell。並能取得其控制權，用 Blind call，定時播打無聲電話予目標手機，取得連繫。並能持續轉譯目標手機通訊紀錄。而 DF(direction finding) team 目標搜尋小組即可追蹤目標手機所在地，進而利用 GPS 定位系統。

四、語音及簡訊截取 Voice & SMS Intercept：可即時接聽並錄下目標手機通話語音及簡訊記錄，存在其硬體設備內的 SIM 卡中。亦可取得暫時控制權，中斷目標手機通話要求，回應"暫時無法通話，請再播打一次"之訊息，進而取得緩衝應用時間。

五、狀況控制 situation control：提供如 service denial(主機忙錄拒絕接聽)、bubble(鎖住所有電話並模擬網路雍塞)、white and black lists 等模式。3G IMSI 系統會自然地截取，但目前尚無法控制 3G 手機，因其安全性較高，只能做到回絕 3G 通話請求，或利用 PUSH 功能，將其通訊要求轉換至 2G。

六、GSM solution：目前硬體演進過程有

1999-2002 GSM-X—＞2002-2005 GSM-XP－＞2006 迄今 GSM-XPZ(其 M 可攜式系列 HP 高度可攜性系列)，該系統可視其追蹤手機系統需求，為不同產品設定至 2 至 4 個硬體頻道，惟亦可用軟體設定擴充，如 DF(direction finding)硬體設備(NB+MMI_SS+感應器：即可追蹤)。

另外此產品亦可使用於直昇機，高度無影響，也提供教育訓練及軟體更新、硬體維修服務。

下午該公司即開始實機展示，並藉現有設備實際表演其設備功能。

12 月 11 日（星期四）早上至皇家哈洛威大學資訊安全組，下午至Guidance公司參訪

上午 9:15 分抵達 Stephen 教授辦公室，先參觀位於主校園區內之一間電腦教室，它建置了一虛擬教學環境 VM Homework，學生可連線至隔離的虛擬主機，內有不同的作業系統，及不同資訊安全的習題挑戰，因此時正值假期，學生可自由連線進入解題，目前正開放了一個名為聖誕節挑戰，等著同學於年假中破解。接著返回至位於教授辦公室二樓處之機房，此機房即係電腦教室連結對外之網路主機並可作網路上的功能測試，內明訂嚴格之安全政策，確保同學的任何操作都是合法的，以免有觸犯法律之虞。

上午 9:45 分返回 Stephen 教授辦公室，Stephen 教授表示其學生來自不同領域各有不同專長，教學計劃先以統籌的概念教導起，同學再針對自己有興趣的部分自行深入研究。目前實驗室裡有一項研究就是追蹤目標手機，並將有資訊產出，這項議題應該和資安鑑識會有所相關，主要研究 3 項子題：談話中行動定位、更換 SIM 卡辨識、確認交談對象，技術是利用每部手機去定位目標手機的距離，利用如：silent signal、looking info、in call moving 等技術，再加上如藍牙耳機設定配合定位，因為藍芽發送距離限制，更能離認目標手機的有效距

離。

上午 10:25 分 John 教授加入談話，表示日後法院審判、數位證據鑑識面臨更嚴格的檢視，律師會詳細檢驗證據的有效性。

下午離開 Stephen 教授辦公室前往 Guidance 公司。該公司從事專業電腦鑑識軟體開發。

首先向該公司業務經理表示，2004 年開始規劃資安鑑識實驗室，於 2005 年即購入 Encase 5 使用、使用中亦發生許多問題，直至 2007 年因版本升級，終於可以大致解決，此次來訪的目的，即是想取得更多關於新開發產品的資訊及未來公司的發展方向。

接著由 James Buckland 解說介紹產品，包括 Information Assurance、FIM（執法單位使用，具網路連線功能，從運行中的系統擷取資料，可不用中斷電源）、Neutrino（可攜式動置之鑑識與分析，用於串流數位調查），另有供商業用途之產品。

接著由 Bill 先生引導參觀公司內部兩間教室，各可容納 24 位及 18 位學員，每兩位學員皆會有三台螢幕。中間一台是教師用來教學廣播，或 vnc 遠端螢幕操控至同學電腦教學使用。接著拜訪 Simon 程式設計師，該設計師亦是從警界退休，他非常重視使用者的意見回饋，會不斷詢問，以改進 Encase 的產品缺失。接著 Bill 先生展示使用 Neutrino，只要將 SIM 卡裝入，需入密碼，即可產出報告，詳列所

有撥打記錄，及 SMS 記錄。16:30 結束今日參訪行程。

12 月 12 日（星期五）皇家哈洛威大學資訊安全組

因著本週在 Stephen 教授的精心安排下，參訪許多單位，並從中學得許多，故一早先至學校教授辦公室，作本週參訪單位之回顧。Stephen 教授亦分享其所整理之資料，參訪團亦向教授報告此次的參訪心得並感謝他這一週熱忱的接待，會後也利用一點時間到倫敦去逛逛並整理行李，於晚間 9:30 搭乘長榮班機返國，並 12 月 13 日晚間 10 時抵達桃園國際機場。

肆、參訪心得

一、政府執法單位與民間公司在電腦鑑識上的合作：

此次參訪最主要的單位是英國警方，因美國911事件之後，英國十分重視反恐任務，且在其業務下特別著重於電腦鑑識，故其案件中，只要涉及電腦相關設備，就由該組成員負責處理。並未假手外人。但若是一般的案件，則因警方的人力不足，而採取此種方式：案件的搜索扣押由警方負責，警方將所扣押的電腦相關證物經整理造冊以正式公文送交民間簽約的電腦鑑識顧問公司，由其執行後續作業，再將結果送交警方。此可大量減輕執法人員的負擔，是值得參考。

二、電腦鑑識於大學課程與在職訓練的重視

英國大學及警方對於電腦鑑識人員人才培育均十分重視。大學之研究所學生在資訊安全組的必修課程中，有非常重的比例在電腦鑑識方面，教授亦在其校方未來的發展上有完整的規劃，使學生在未來工作上有此技能發揮所長，由其該國許多公司均設有資訊安全部門，是較容易就業的。

英國警方亦重視其在職訓練，且能結合各執法單位之力量相互學習，參加研討會，使其技術能多方交流。亦定期至電腦鑑識軟體顧問公司上課，吸收新知。

三、鑑識工具之多元化

藉此次參訪，到不同的單位看到所使用之各種不同的工具，並且聽取他們使用之心得，發現鑑識工具因人的使用情形不同而有不同的反應，尤其是SO15所使用的麥金塔電腦，是他們主要的工作平台，他們使用FTK很順手，而QCC卻不用FTK，故此說明鑑識工具之好壞取決於個人之使用習慣與熟悉程度。並且使我們對麥金塔電腦有另一種的體認。

伍、建議

一、推動坊間電腦鑑識顧問公司之能量，為將來與政府合作舖路：

為因應電腦犯罪案件日益增多，許多民間公司因考量本身公司之信譽不願向執法單位報案，並轉向坊間電腦鑑識顧問公司尋求協助，故此需考量其鑑識能量，並建立合作管道，有一致的鑑識標準程序並在法律要件成立時能結合偵辦。

二、建請國內知名大學於資訊科學系所，重視資安之養

成教育：

由於接觸英國皇家哈洛威大學之教授，瞭解其校如何於課程中著重資訊安全之人才培育，並有其長遠規劃，大量培養資訊安全人才，國內目前亦有部分學校有此方面之研究所，希望能更加擴大，能藉資訊安全課程，推動資安鑑識領域的專才，帶動國內資安鑑識能量。

三、加強建立國際合作管道：

與英、美國等先進國家之司法機關所屬之電腦鑑識實驗室建立合作管道，促進國際交流合作，除可瞭解國際電腦鑑識技術發展脈動，亦增進實驗室之鑑識能量。