出國報告（出國類別：會議）

赴香港參加「亞太地區國際高科技犯罪調查協會（HTCIA）會議」心得報告

服務機關：法務部調查局
出國人姓名：曾玉堂調查官
出國地點：香港
出國期間：中華民國 101 年 11 月 26 日至 12 月 1 日
報告日期：中華民國 102 年 1 月 7 日

報告大綱

壹、 行程記述

此次出國計畫包含赴香港（Hong Kong）參訪 Data Expert 科技公司（下稱：Data Expert 公司）及參加國際高科技犯罪調查協會（High Technology Crime Investigation Association；HTCIA）會議，本次會議時間自 101 年 11 月 27 日至 29 日，地點爲香港 Icon 飯店二樓會議廳舉行，另有英國、美國、以色列、俄羅斯、印度、香港、及中國大陸等數十家廠商與會參展。參訪行程係由美國著名鑑識軟體廠商 Guidance Software™公司之台灣授權代理廠商鑒真數位科技公司協助安排，於 2012 年 11 月 30 日參訪香港 Data Expert 公司。

Data Expert 公司主要業務爲資料複製、回復、救援及清除、硬碟消磁及破壞、數位鑑識等，另包括手機修復、鑑識、破解及資料擷取（含中國山寨機研究），爲香港地區從事數位鑑識及電腦資料回復之代表廠商之一，亦爲此次 HTCIA 參展及贊助廠商之一。

HTCIA 爲一非營利組織，針對數位鑑識、網路安全、資料回復、電腦犯罪等相關領域，舉行教育訓練及高科技犯罪調查研討會，鼓勵並促進會員進行實務經驗分享及技術交流，參展廠商及與會成員包括各國權威鑑識軟體廠商、世界各國執法單位、民間知名電腦科技公司及大型會計師事務所等。2012 年爲第 6 屆舉辦之亞太地區訓練會議，議題包括網際網路安全、數位鑑識與調查、雲端科技、鑑識工具方法介紹等，並由香港執法單位進行案例介紹；研討內容包括：WiFi Investigation、FTK 最新更新及技術解說、手機分析鑑識實例解說、Encase 更新介紹等，前述技術研討示範以及技術分享，皆有助於提升我國對於數位鑑識水準之提升，並拓展國際視野及能見度。

貳、 Data Expert 公司簡介

Data Expert 公司位於香港地區，爲一民間機構之資料救援及數位鑑識科技公司，該公司因應民間大眾及政府機關，針對各類型電腦、筆記型電腦、伺服器等設備，從事電磁紀錄之數位證據蒐集、回復及驗證，除電腦之儲存裝置外，該公司亦提供智慧型手機（Smart Phone）及平版（Tablet）電腦等消費性電子通訊設備之資料擷取及回復分析。此次 Data Expert 公司亦爲 2012 HTCIA 會議參展廠商之一，展示設備包含可攜式鑑識裝置、可攜式手機擷取裝置、各類介面型號防寫盒、硬碟複製機及實驗室等級之鑑識設備等，該公司並與中國大陸上市公司美亞柏科信息公司合作代理，專研中國山寨手機鑑識技術研發，於硬碟修復及中國山寨機破解擷取頗負盛名，然其硬碟修復代價不斐，於香港地區具相當地位。

參、 HTCIA 組織會議簡介

HTCIA 全名爲國際高科技犯罪調查協會，1988 年夏天 HTCIA 舉行了第 1 次全美高科技犯罪調查培訓研討會，後於 1989 年 3 月 17 日正式向聯合國以非營利、公共利益組織名義申請成立，爲國際數位鑑識領域知名組織，致力於有關高

科技犯罪調查、預防、偵查及起訴的研究，透過會議及訓練研討的方式，將與會會員之實務經驗及技術水平做充分交流，提升調查職能及電腦技術，網路犯罪專家克里斯布朗（Christopher Brown）曾讚評 HTCIA 爲最有水準且最受尊崇的研討組織，會議成員多來自國際高科技犯罪調查單位及大型民間機構，包含各國警察、國安組織、反恐部門、司法單位及各民間顧問公司團體等。今年 HTCIA 爲第 6 屆亞太地區會議，會議時程共 3 天，第 1 天安排 Verisign、Belkasoft、Guidance Software、eWalker 顧問等公司進行技術分享及報告，第 2 天及第 3 天爲訓練研討會，有 AccessData、ThinkSECURE Pte、Guidance Software、XRY 等著名鑑識廠商進行產品更新功能介紹或技術交流等研討。

今年 VIP 演講（VIP Address）請到香港警察資深主管（Senior Superintendent）Lawrence Wong，主講目前香港國際合作之網路犯罪調查及因應現況（International Cooperation in Combating Cyber Crime），Mr. Wong 於 1987 年投身香港警界服務，曾經歷於組織犯罪及三合會調查科（Organized Crime & Triad Bureau）、商業罪案調查科（Commercial Crime Bureau）專責網路詐欺犯罪調查等，於 2008 年 6 月至 2010 年 6 月間，曾於法國里昂（Lyon France）擔任國際刑事警察組織（International Criminal Police Organization；INTERPOL）之副主席，主要負責毒品查緝及組織犯罪調查等業務。

HTCIA 亞太區現任主席爲香港警務處商業罪案調查科之總督察羅越榮（Dr. Frank LAW）博士，羅博士於 2001 年加入網路犯罪調查工作，現主導科技罪案組（Technology Crime Division）之電腦鑑識工作，主要案件類型爲數位調查及數位證據回復等。2009 年他當選國際信息系統安全核准聯盟（International Information Systems Security Certification Consortium；ISC2）所頒發之資訊安全領導人獎（Information Security Leadership Award），且具有資訊系統安全認證專家證照（Certified Information Systems Security Professional；CISSP）。

肆、參訪 Data Expert 公司活動紀要

參訪時間爲 2012 年 11 月 30 日上午 9 點至 12 點，Data Expert 公司負責人陳寶明先生親自接待解說，帶領參觀公司辦公環境及硬碟修復實驗室，介紹硬碟修復實驗室之相關設備及軟硬體，包含硬碟修復、硬碟複製、硬碟消磁及硬碟實體破壞等設備，以及從事案件處理之類型，並針對硬碟相關作業及技巧原理進行解說，分述如次：

一、硬碟修復

負責人陳寶明先生解釋硬碟修復係一門綜合各領域知識的技術，由於硬碟製作過程及原理複雜，在台灣地區尚無廠商可獨立研發製作硬碟技術，因此當硬碟出現毀損或資料無法讀取等問題，需利用多面向的分析來判斷硬碟故障毀損之處，當中需要具備電子、機械、電腦、檔案系統等知識，因此修復硬碟往往比換購全新硬碟要價更高。該公司所承接的硬碟修復案件包括：硬碟不過電、馬達及軸承無法運轉、軸承移位、電路板晶片短路燒鎔、針腳斷裂、插槽接面斷裂短路、

電腦主機無法偵測及無法讀取硬碟等案件類型，當硬碟外觀或晶片毀損或故障，仍有機會存取出硬碟內部資料，但當發生硬碟碟片破裂、刮盤或位移等，要能救出資料的機會則大大降低。另外硬碟韌體（Firmware）部分，往往因其故障而造成硬碟在開機時，與基本輸出輸入系統（Basic Input/Output System；BIOS）間傳遞訊息出現問題，因硬碟需在電腦開機時，提供硬碟內部參數給主機板，內部參數包含硬碟型號、序號、磁軌、容量、硬碟自我監測分析報告程式（Self-Monitoring, Analysis and Reporting Technology，SMART）及永久缺陷表（P-List；指硬碟出廠前所進行低階格式化，自動找出所有壞軌及磁區，紀錄於硬碟中的永久缺陷表，這些紀錄位址將於硬碟存取時自動被跳過，不影響硬碟讀取速度）等資訊，故當硬碟韌體發生問題，會造成 BIOS 無法偵測到硬碟設備或無法正確讀取到硬碟資訊，此種案件類型都以先救援資料爲優先。

二、硬碟複製

硬碟複製通常與硬碟修復相輔相成，當硬碟修復成功，則需要使用硬碟複製工具，將硬碟內可讀取的磁區備份，通常都以製作映像檔或鏡像備份（Mirror Backup）的方式，將資料完整備份。

三、硬碟消磁（Magnetic Degausser）

Data Expert 公司使用 3 款消磁機來清除硬碟、軟碟、磁帶及磁卡等磁性儲存裝置媒介上的數據資料，該公司使用 DEA-MD15X、DEA-MD25X、DEA-MD30X 等機型消磁，皆能產生 10000 高斯，可達到永久性脫磁，達到資料永久銷毀的目的，通常用於政府國防軍事部門、金融、商業及航空業等領域。該消磁機皆符合美國 DOD 5220.22M 標準，該標準係美國國防部在「國家工業安全計畫」（National Industrial Security Program）下的國家工業安全計畫操作手冊所提及到資料清除及銷毀的方法參考矩陣標準。

（銷毀前）　　（銷毀后）

四、硬碟實體破壞

目前固態硬碟（Solid State Drive；SSD）等的儲存媒介，資料儲存已不存在於碟盤或磁區中，通常係以快閃記憶體（FLASH Memory）及同步動態隨機存取記憶體（Synchronous Dynamic Random Access Memory；SDRAM）的方式做爲電腦外部儲存裝置，最常用於筆記型電腦以取代傳統硬碟，因此種固態硬碟的永久性記憶體特性，用消磁機已無法達到資料清除的目的，因此則需利用硬碟實體破壞的方法來達到資料清除及銷毀的目的。硬碟實體破壞實際作法通常有泡水、焚燬融化、敲擊內部使碟片變形粉碎等物理性破壞，該公司使用 DED-HD2 的自動化設備，可直接將硬碟碟片穿刺、打洞或彎折九十度，直接破壞實體硬碟設備。

伍、 2012 HTCIA 國際高科技犯罪調查協會研討會紀要

一、 VIP Address「International Cooperation in Combating Cybercrime」(9：15－9：30)：演講者 Lawrence Wong 表示香港網路犯罪 2012 年 1-10 月以來，共發生 786 件非法入侵或分散式癱瘓系統等攻擊案，較 2011 年一整年上升 36%，可見電腦犯罪偵辦及數位資料保存的重要性，香港警察當局已成立商業罪案調查科網路中心，該網路中心 24 小時收集分析網路上可疑封包及監控網路流量，以因應日益增加的跨國際電腦犯罪、病毒攻擊及駭客入侵。又透過國際刑事警察組織，針對毒品犯罪、線上網路及電話詐欺等組織犯罪，提供合作及交流平台，以共同打擊犯罪，徹底瓦解跨國犯罪組織。HTCIA 亞太區現任主席羅越榮博士補充：前述這些電腦犯罪案件中，有 761 件係入侵電腦案，共造成 1.35 億港幣的損失，因此香港警方已花費 900 萬港幣打造網路中心，以通訊業、運輸業、服務業、金融業及政府部門等 5 個重要領域爲服務對象。

二、 Keynote Address「Cyber Security」(9：30－10：15)：此主題的演講者爲美國 Verisign 公司東亞地區首席研究員 Tom Creedon 先生，他說明 Verisign 的安全服務，使政府單位確保重要服務能不被中斷，並保護機敏的即時通訊及商務活動內容，所有政府部門，均倚賴網路之基本建設服務，如農業、食物、水資源、公共衛生、緊急服務、國防及社會福利等等。Versign 的智慧控制服務（Intelligence Control Service）是利用科技和系統傳輸架構來整合所有政府部門各項資料及各類安全設定。該公司於網路安全的服務特點如次：

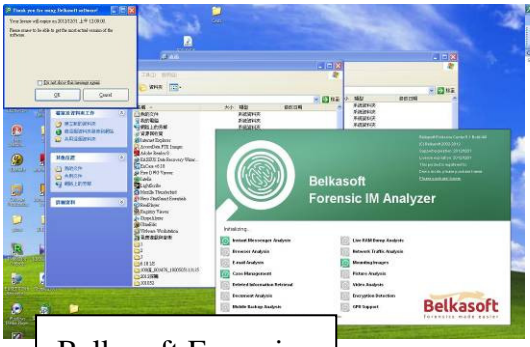
（一）Verisign 公司每日解決超過 14 億筆 DNS 查詢及 40 億筆情報資料庫查詢，處理 2.7 億 Signal System 7（SS7）訊息，保全超過 40 萬個網站，經由 Verisign 公司的付費管理平台，處理北美地區超過 35% 的電子商務轉帳。

（二）Verisign 公司利用驗證的公鑰機制（Public Key Infrastructure ；PKI），政府單位可以對所有使用者及所有設備，達到完整範圍的認證處理，達到交易安全，資料不外洩的目的。Verisign 公司透過雙層授權機制，結合智慧卡(Smart Card)、或具通用序列匯流排裝置（電腦加密裝置、USB token）、或是由 Verisign 公司合作夥伴提供的生物測定技術（如指紋認證），及結合伺服器和設備之認證，以確保 PKI 系統於內部網路及網際網路的各種情況下，使之順利運作維持。

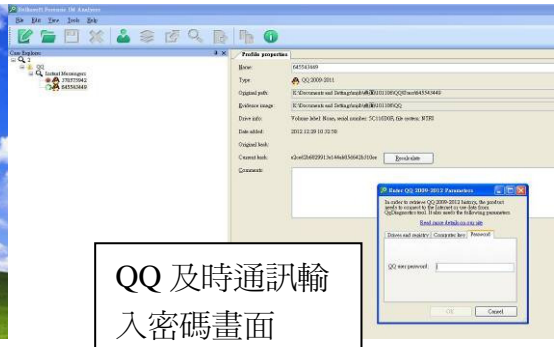
（三）Verisign 公司系統與具領先地位的 IBM Tivoli Access Manager 管控系統整合，提供以使用者爲主的便利管控使用介面。

三、 「How to find an elephant in a haystack: Retrieving Digital Evidence-Methods, Techniques and Issues」(10：45－11：45)：此主題的演講者爲俄

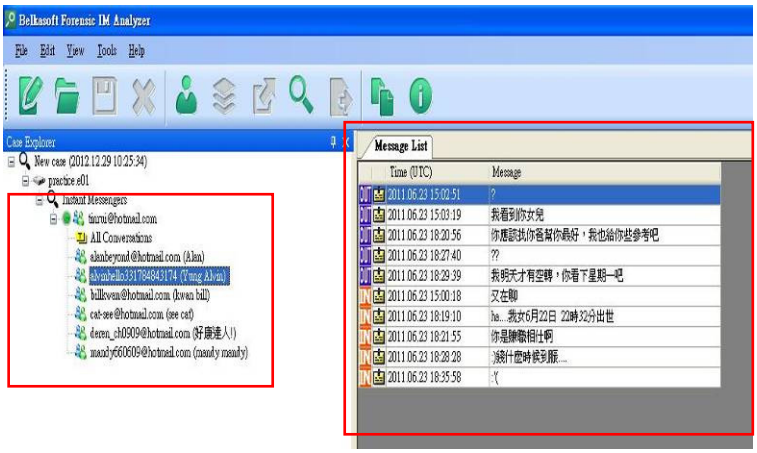
國Belkasoft鑑識公司負責人Yuri Gubanov先生，Belkasoft公司成立於2002年，公司產品主要係電腦鑑識工具及提升 IT 安全的軟體開發，該公司產品發展宗旨爲讓電腦鑑定變爲更加容易，開發更快速、便利、簡易的鑑識軟體，近年將許多單一功能鑑識程式，整合爲鑑識工具（Belkasoft Evidence Center），該公司提供即時通訊分析軟體（Instant Messenger Analyzer）試用版。以平日於陸區廣泛使用的「騰訊 QQ」對話紀錄作測試，經測試後發現該軟體仍須當事人提供密碼，方能取得 QQ 對話紀錄，尚無法繞道（ByPass）QQ 登入密碼，作法與其他鑑識軟體大致相同。



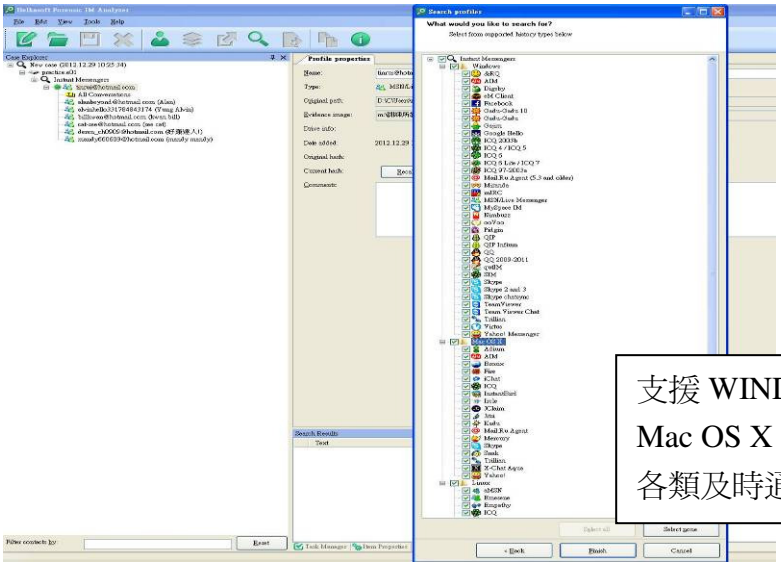
Belkasoft Forensic IM Analyzer 畫面



QQ 及時通訊輸入密碼畫面



MSN 及時通訊紀錄



四、 「Solving Your Digital Investigation Needs」（11：45－12：45）：此主題演講者爲美國鑑識公司 Guidance Software 歐洲、中東和非洲亞太地區（Europe, Middle East and Africa& Asia Pacific；EMEA&APAC）副總裁 Frank Coggrave 先生，Coggrave 先生提到在過去 5 年中，企業發生資料外洩的案例暴增 10 倍以上，許多公司都遭到針對性的資料竊取，企業必須在資料安全的前端及後端做好準備，提高事前避免資料外洩及事後發生資安事件的調查鑑定能力。Coggrave 先生表示 Guidance Software 公司開發電腦鑑識調查軟體，目前發表出最新 Encase Portable V4.0 可攜式版本（Portable Version 4），其特點在於對鑑識所需的資料作分類與收集將更爲方便，該軟體以隨身碟（USB，5GB）的方式設計，最大優點爲可直接使用 USB 介面開機，並整合 Encase Forensic 7.05 版本，提供更多函數功能，同時可執行結構化查詢語言指令（Structured Query Language；SQL），簡化軟體操作並提供強大且人性化的介面，使調查人員更容易快速取得所需資料。

五、 「The Underground Economy: An Overview of the Miscreant Ecosystem and where it's going」（13：45－15：15）：此主題演講者爲美國專業網路安全研究 Team Cymru 公司全球擴展主管 Steve Santorelli 先生，該公司登記爲美國伊利諾州聯邦非營利組織，總部設立於美國佛羅里達州 Orlando，分部散布於全球各地，包含英國、波蘭、紐西蘭、澳洲等地，Cymru 發音爲 kumree，在威爾斯語中爲鯨魚的意思，該公司由創辦人 Rob Thomas 於 1998 年成立，Thomas 博士是威爾斯人後代，當初創設宗旨是使整體網路體系更加安全可靠，該公司目前已擁有 25 類不同的服務軟體、工具、資料及使用技術等服務項目。此論文介紹 Team Cymru 團隊在探討殭屍網路（Botnet）、傀儡網路、安裝次數付費機制（Pay-Per-Install；PPI）、點擊次數付費（Pay-Per-Click；PPC）與地下非法金融犯罪之關聯。網路犯罪者長期以來，不斷地尋找資源來換取獲得最大的收益，廣告視窗或網路聊天

軟體（Internet Relay Chat；IRC）都是駭客的操作手法，透過殭屍網路，將特定程式植入受害者電腦，一個下載程式或點擊廣告的小動作就可讓業者賺取利潤，更嚴重的手法，藉由此種機制遠端控制受害者電腦，進而從事犯罪行爲。2009 年 Team Cymru 公司發現駭客利用僵屍網路的操縱手法，以 PPI 付費機制來賺取利潤，2010 年駭客利用多樣下載程式入侵受害者電腦內，讓受害者電腦會不中斷地以 PPI 及 PPC 付費機制來賺取利潤，亦會使受害者的電腦運作顯著變慢，甚至會危害系統檔案造成使用者電腦當機。2010 年後，Team Cymru 公司發現 PPI 業者或駭客利用蠕蟲程式，執行垃圾程式碼發動阻斷式服務攻擊，Team Cymru 公司介紹說明以 X-Lass 蠕蟲程式來散布惡意程式爲例，說明網路駭客日新月異的犯罪手法。

六、 「WiFi Investigation」（15：45－16：30）：此主題演講者爲新加坡 ThinkSECURE Pte 公司 Julian HO 先生，ThinkSECURE Pte 公司係於亞太地區提供專業電腦技術培訓課程，提高組織資訊安全，減少不必要的資本支出（Capital Expenditure；CAPEX）及營運支出（Operational Expenditure；OPEX），在電腦 IT 安全技術及培訓認證教學方面具領導地位，參與培訓課程的人員包含金融、製造、電信、保險及政府機構等行業。HO 先生是該公司的技術總工程師，他曾負責過 StarHub 公司的網路安全管理，該演講描述無線網路查核工具（Auditing Toolkit），以 WiFi、藍牙及射頻辯識技術（Radio Frequently Identification；RFID），幫助 IT 人員偵測 WiFi 網路的安全性，藉由射頻辯識技術的特性，消耗功率低、辨識能力強且便於攜帶等優點，將 WiFi 無線網路及 RFID 辯識技術整合，可快速追蹤定位 WiFi 系統，此種技術通常使用於室內定位搜尋，利用電子標籤（Tag）、讀取器（Reader）及微型天線（Antenna），以微型天線配合電子標籤及讀取器，無線傳遞射頻訊號，進一步計算出位置距離及角度的定位資訊。

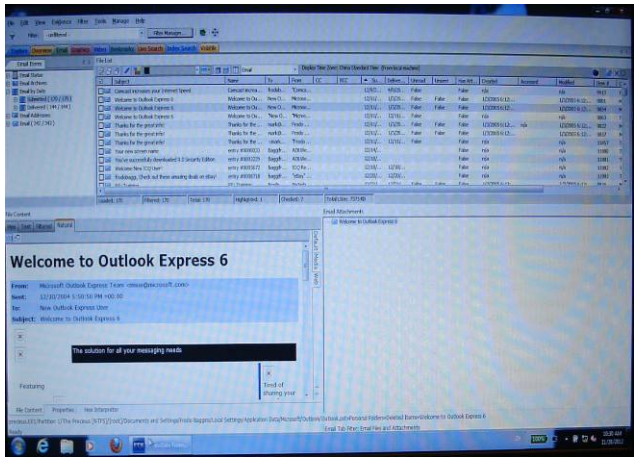
七、 「Data Breach Investigation Report」（15：45－16：30）：此主題演講者爲美國通信資訊服務 Verizon 公司 Mark Goudie 先生，主講機敏資料遭竊調查報告，Verizon 公司總部設在紐約，對全球超過 150 個國家的消費者、業者及政府等單位，提供 4G 長期演進技術（Long Term Evolution；LTE）無線及光纖網絡等服務。該公司自 2008 年起每年均出版機敏資料遭竊調查報告（Data Breach Investigation Report；DBIR），分析全球各商家所遭受的資安威脅、技術及不斷演進的手法及數據統計。這類資安事件，大多圍繞在盜取資料及資料庫所演化的各種方法，以合法掩護非法的手法來偷取敏感資料。2010 年全球有 22 個國家發生資料遭竊的資安事件，2011 年則增加至 36 個國家，且此類資安事件已不是只發生於單獨區域的事件，多爲跨國事件，需要更多國家來參與防範。研究報告亦指出駭客的目標大都是隨機性，專門找尋有資安漏洞的使用者，而非特定目標的攻擊。今年度 Verizon 團隊提供一張檢查單（Check List），供使用 POS（Point-of-Sale）

付費系統的商家進行資安檢查，像是定期更改密碼及裝設防火牆等措施，並針對大型機構提出 10 大資安威脅警訊，如使用鍵盤側錄間諜程式（Key Logger）竊取情資、利用後門程式掩護執行其他惡意程式、利用仿冒之釣魚網站欺騙受害顧客線上消費、SQL 程式碼攻擊（SQL Injection）、密碼暴力破解（Brute Force）、攻擊伺服器隱藏欄位（Tampering）等相關訊息，Verizon 的風險管控（Risk Intelligence Solutions Knowledge；RISK）團隊採用企業風險及事件分攤（Verizon Enterprise Risk and Incident Sharing；VERIS）架構協助客戶檢查並處理資安問題。Verizon 表示 2013 年最有可能發生的資安威脅是驗證碼及錯誤驗證攻擊（Authentication Attacks）、間諜程式、大規模駭客攻擊（Espionage and Hacktivism）、網路應用程式攻擊及社交工程等資安威脅，整個 RISK 團隊將持續對未來發生各類資安議題提出解決之道。

八、 「Latest features and updates to FTK4」（9：30－11：30）：此主題爲介紹 FTK4 更新功能，包含多媒體分析功能、提升輸出品質、增強資料處理程序、快速檢視證據檔案內容、新增支援 Windows EVTX Log（事件紀錄檔）檔案格式、提升解碼功能及資料庫擴增等進階功能，說明如次：

（一）多媒體影像功能：FTK4 新增影像擷取功能，於影片縮圖（Thumbnail）功能中，可從一段影片中擷取所需的畫面，讓調查人員更快速檢視影片中的每段內容，而不用浪費時間看過全部影片檔。另外新版的功能支援其他類型的影片檔，可轉換成 Windows 預設支援之格式（Windows Media Player），在 FTK4 下播放影片還可直接調整改變該段影片的解析度及影片流率。

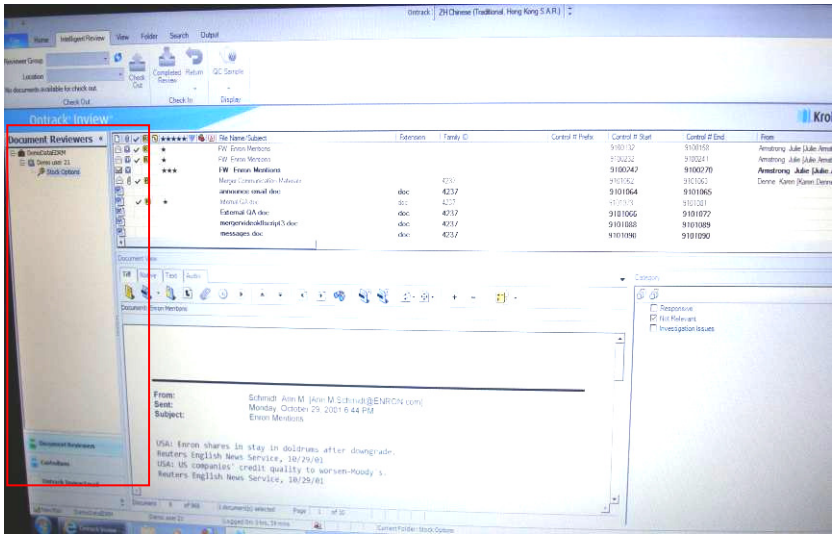
（二）郵件可轉換成 PST 檔（Outlook 格式）功能：調查人員可將郵件訊息資訊輸出成 PST 檔，另外支援 RFC822（定義網路電子郵件位址的格式）、NSF（Lotus Notes 格式）等轉檔格式成 PST 檔，以便於檢視。



以 FTK 檢視電子郵件畫面

九、 「e-Discovery Technique」（13：30－16：00）：此主題演講者爲美國 Kroll

Ontrack 公司，亞太地區香港公司業務總監 Kate Chan 律師，Kroll Ontrack 軟體開發公司 1985 年成立，已有 25 年長遠歷史，公司於 1987 年另發展數位回復及資料救援領域之技術，平均每年多達 5 萬資料救援案件，包含硬碟、筆電、桌上型電腦、網路磁碟、陣列、資料庫、磁帶、信件、手機、記憶卡及快閃記憶體等，所涵蓋及服務層面極廣，該公司連續 8 年被美國法律科技調查機構（Am Law Tech Survey），認定在法律諮詢及科技服務上具有領導地位，主講人 Kate 律師介紹該公司 e-Discovery 技術，除了鑑識軟體所具備之基本功能外，該軟體另具一特別功能，以後端資料庫連接每一鑑識人員主機，可線上連線查詢各鑑識案件結果，提供鑑識主管檢視，便利鑑識調查工作。



電腦鑑識人員編號及鑑識案件

十、「So we got the phone, now what?- Analyzing the data & the challenge of encrypted apps」（9：30－11：30）：此主題演講者爲瑞典 Micro Systemation 公司 Martin Westman 先生，Micro Systemation 公司係全球領先地位的手機鑑識軟體公司，該公司總部設於斯德哥爾摩，已於 1999 年在瑞典證券交易所上市，並於歐洲及美國設有辦事處，從 80 年代開始，該公司即投入手機研發通訊，現主要研發手機鑑識資料回復工具及軟體。Westman 先生介紹，有關針對手機內部已加密的 APP 檔案，如何進行分析或讀取，目前多以物理層擷取手機內容資料，透過 16 進位傾印（Hex-Dumps）及解碼（Decoding）過程，從手機記憶體內轉存資料，可繞過（Bypass）手機的作業系統，通常可回復已刪除或加密保護的手機資料，透過此種傾印（Dumping Raw Data）過程，自動解碼及重建手機資料，更便利調查鑑識工作的取證作業。此外，Westman 先生亦介紹該公司目前推出最新版 XRY 6.4.2 版，增加多達 8108 種各類手機裝置的擷取破解，新增功能如下所示：

（一）支援 Window　7，64 位元的版本。

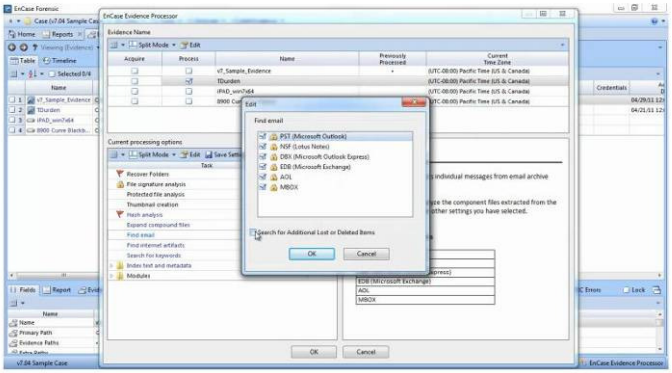
（二）黑莓機（Black Berry）物理層擷取（Physical Support）。

（三）聯發科晶片（MTK Chipset）系列手機的物理層擷取。

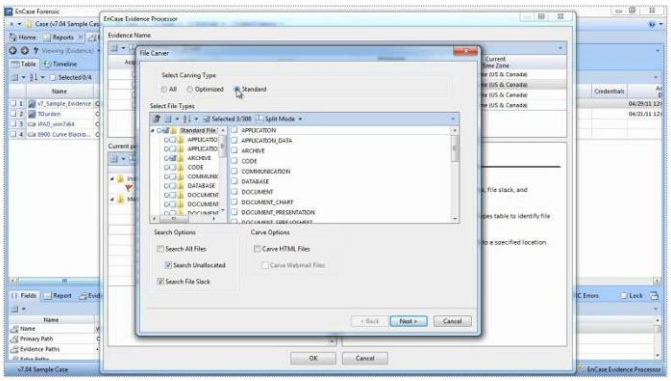
（四）Nokia 第五代（Base Band 5；BB5）手機的物理層擷取。
（五）支援 iPhone 5 及 iOS6 版本。
（六）支援 Window Phone 8 系統。
（七）支援新版 Android 及 iOS Apps 的支援。
（八）改善資料擷取系統介面，更人性化更便利的設計。
（九）增強 Android 4.0 系統備份擷取功能。
（十）增強 Android 檔案系統的支援。
（十一）新增 110 種智慧型手機 APP 應用系統的資料擷取。
（十二）增加葡萄牙語、巴西語及俄語版本。

Forensic Method	XRY6.4 版 新增支援的手機數	全部支援手機數
XRY 邏輯層資料擷取	153	3670
XRY 物理層傾印	167	1594
XRY 物理層解碼	116	1368
密碼回復或解碼	123	647
智慧型手機 APP 資料擷取	17	110
XRY 未實測但可支援	241	719
總計	817	8108

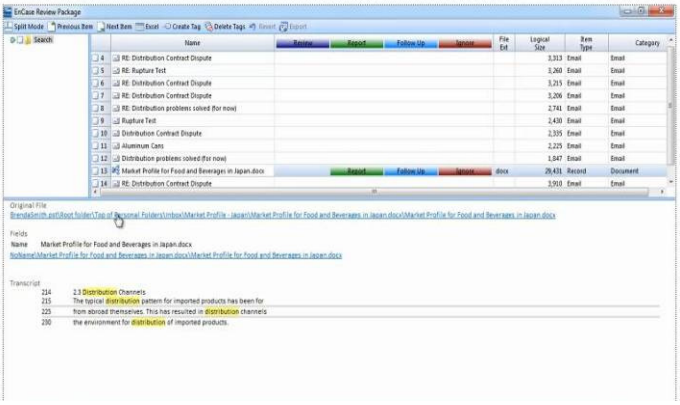
十一、「Encase Update Ⅱ」(13：30－16：00)：此主題演講者爲美國 Guidance Software 鑑識公司 Frank Coggrave 先生，介紹 EnCase V.7 鑑識軟體更新的進階功能，包括教導使用者如何以完善可靠的鑑識方式，從可攜式裝置中（包含手機及平版電腦）取得完整的複製資料，利用處理程序功能（Processing Evidence）檢視證據檔案，新增標籤功能（Tag）可對資料進行註記及分類。EnCase V.7 新增報告樣版（Report Template）索引功能，更有助於使用者以自訂創設的樣版，來產生鑑識報告，分類更新功能如次：
（一）整合智慧型手機及平版電腦資料擷取。
（二）客制化的報告面版設計。
（三）簡化電子郵件的檢視，直接預覽信件、聯絡人及附件檔，可直接分析郵件及各信件通訊人間聯絡關係。
（四）透過自動化處理程序（processing）及索引（indexing）功能，可減少工作時間，更快速檢視案件。



電子郵件搜尋畫面



檔案資料挖掘畫面



信件檢視及標籤記號畫面

陸、 心得與建議

一、心得

（一）此次前往中國香港參訪 Data Expert 公司，瞭解硬碟修復、備份、消磁及實體破壞的作法，經由廠商的介紹及實體展示，對於硬碟的基本原理、結構及實務作法有相當的認識，針對香港地區鑑識技術及硬碟修復的水平有深刻的體認，透過此次機會參訪獲得相當寶貴經驗，對未來調查鑑識工作或資料救援案件具有相當的助益與參考價值。

（二）HTCIA 會議中各家廠商發表或展示其鑑識軟體並提供產品服務等，對

於數位鑑識實務有相當的助益，能即時與各大數位鑑識廠商所發表之產品接軌，深刻體會各家廠商在鑑識領域的努力。許多產品亦逐漸設計具便捷且簡易的介面，整合許多分散軟體程式，降低數位鑑識工作技術門檻，簡化繁瑣操作步驟及程序，進而增強數位鑑識能量，快速完成電腦鑑定調查工作。

（三）以往鑑識軟體及工具大多仰賴美國公司所開發之軟體，如 Guidence Software 與 AccessData，對於其他國家如俄羅斯及新加坡等國的產品相對較爲陌生，此次認識俄羅斯 Belkasoft 公司所開發的即時通訊分析軟體，以及新加坡 ThinkSECURE Pte 公司所開發的 WiFi 應用工具，未來有機會可與前揭廠商合作配合，對於鑑識工作可廣泛擴大面向。

（四）中國山寨手機的發展一向是日進千里，從以往品質低落發展成現行具水準且實用的山寨手機，從以往實務經驗而言，若涉嫌人爲陸區往返工作的臺灣人民，送鑑證物手機中山寨手機佔相當比例，因此有關山寨手機的鑑識研究相當重要，此次參展廠商美亞柏科信息股份有限公司，專門研究中國山寨手機鑑識開發及破解，未來可持續關注瞭解，以增進手機鑑識工作能量。

二、建議事項

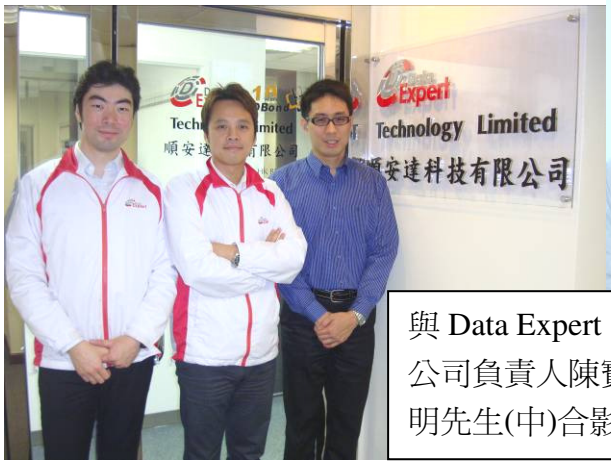
（一）國際鑑識研討會議幾乎每年舉辦一次，地區如香港、美國、歐洲各地皆有，應持續參與此類研討會議，保持與各國專家、軟體廠商友好聯繫關係，提升本局數位鑑識專業技能。

（二）本國鑑識領域不乏優秀人才及廠商，本局亦可比照利用舉辦研討會或訓練課程方式，號召聚集國內外專家學者以交流分享相關數位鑑識經驗。

（三）與陸區山寨手機鑑識軟體廠商合作，配合手機鑑識及 SIM 卡鑑識需求，增強手機鑑識工作能量。

（四）持續加強本局鑑識人員語言能力，能更快速吸收最新鑑識知識與技能，並積極參與國際研討會，以提升本局國際水準及能見度。

柒、 附表 1（Data Expert 公司參訪照片）



與 Data Expert 公司負責人陳寶明先生(中)合影

Data Expert 公司營業項目

實體破壞的硬碟（彎折九十度）

資料救援實驗室

實體破壞的硬碟（經穿刺）

附表 2（HTCIA 會議議程）

Day 1 Management 27th Nov 2012

Time	Topic	
09:00 - 09:15	President's Opening Address	
09:15 - 09:30	VIP Address - Hong Kong Police or Hong Kong Judiciary	
09:30 - 10:15	Keynote Address: Cyber Security - ***Verisign***	
10:15 - 10:45	COFFEE BREAK	
10:45 - 11:45	How to find an elephant in a haystack: Retrieving Digital Evidence - Methods, Techniques and Issues - ***Belkasoft***	
11:45 - 12:45	Solving Your Digital Investigations Needs - ***Guidance Software***	
12:45 - 13:45	LUNCH	
	Technical Track	**Management Track**
13:45 - 14:30	Cloud Computing Incident Response and Forensics Management - ***eWalker Consulting Limited***	The Underground Economy: An Overview of the Miscreant Ecosystem and where it's going - ***Team Cymru***
14:30 - 15:15	Current Challenges and Trend in Cloud Computing Forensics - ***eWalker Consulting Limited***	
15:15 - 15:45	COFFEE BREAK	
15:45 - 16:30	WiFi Investigation- ***ThinkSECURE Pte Ltd***	Data Breach Investigation Report - ***Verizon***
16:30 - 17:15	A Christmas Carol of Forensic Imaging - featuring the ghosts from Forensic Past Present & Future - ***CIA Solutions***	Case Study - Investigation of Cybercrime
17:45 ~	COCKTAILS - Green in Hotel ICON	

Day 2 Technical 28th Nov 2012

Time	DAY ONE		
AM	WiFi Investigation - ***ThinkSECURE Pte Ltd***	Network Attack Investigation - ***VXRL and Nexusguard***	Latest features and updates to FTK4 - ***AccessData***
PM	Identify APT Attack through Memory Forensics - ***VXRL***	e-Discovery/Email Investigation - ***Nuix***	e-Discovery Technique - ***Kroll Ontrack***

Day 3 Technical 29th Nov 2012

Time	DAY TWO		
AM	So we got the phone, now what? - Analyzing the data & the challenge of encrypted apps - ***XRY***	Mac Forensics - ***Ryan Kubasik***	Encase Update I - ***Guidance Software***
PM	BotNet Investigation - ***Team Cymru***	Incident Response - Live Forensics & Digital Forensics Triage - ***Zoran Iliev***	Encase Update II - ***Guidance Software***

附表 3（參與 2012 HTCIA 會議照片）

HTCIA 會場

與 HTCIA 亞太區主席羅越榮博士合影

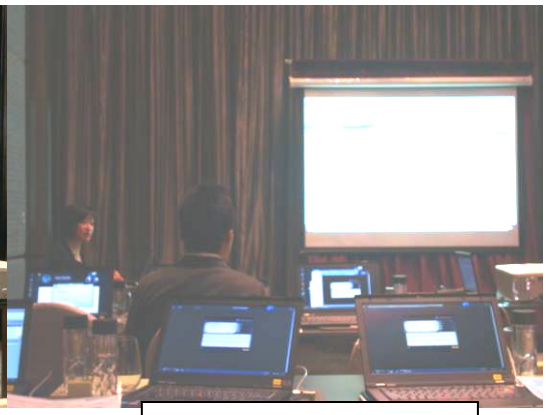
HTCIA 參展廠商

Belkasoft 公司 Gubanov 先生介紹軟體功能

Guidance Software 公司 Coggrave 先生介紹數位調查工作

ThinkSECURE Pte 公司 Ho 先生主講 WiFi 調查應用

AccessData 公司技術人員介紹 FTK4.0 更新升級功能



Kroll Ontrack 公司 Chan 小姐介紹 e-Discovery 軟體功能

與 Data Expert 公司人員合影

與 Belkasoft 公司負責人 Yuri Gubanov 先生合影