出國報告（出國類別：實習）

赴美參加「數位鑑識、安全及法律組織（**ADFSL**）」研討會心得報告

服務機關：法務部調查局
出國人姓名：劉宜發專門委員，曾玉堂調查官
出國地點：美國維吉尼亞州列治文市
出國期間：中華民國 101 年 5 月 27 日至 6 月 2 日
報告日期：中華民國 101 年 8 月 6 日

報告大綱

壹、 行程記述

此次行程由劉宜發專門委員與曾玉堂調查官赴美國維吉尼亞州列治文市（Richmond VA）參訪 AVM 電腦科技公司（下稱：AVM 公司）及參與數位鑑識、安全及法律協會（The Association of Digital Forensics, Security and Law；ADFSL）會議。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及美商數位鑑識公司 H-11（H-11 Digital Forensic）協助安排，於 2012 年 5 月 29 日參訪當地 AVM 公司，該公司對於處理民間糾紛及刑事案件之數位鑑識工作頗負盛名，針對各種網路及電腦使用所造成之民、刑事糾紛，提供完整、安全、公正之電腦鑑識及法律諮詢服務，係當地法院機關、執法單位及一般民眾等信賴之數位鑑識證據科技公司。

ADFSL 會議主題針對網際網路安全、網路法律、數位鑑識、資訊科技、跨國網路相關議題、電磁紀錄隱私權保護等進行學術討論及實務分享。會議時程自 2012 年 5 月 30 日至 5 月 31 日止，為期 2 日，於當地凱悅飯店一樓會議廳舉行，計有美國、英國、德國、埃及、印度、日本、香港、澳洲及中國大陸等共 30 多位學者與會。

貳、 AVM 電腦科技公司簡介

AVM 公司係屬美國民間機構之電腦資訊科技公司，針對各類型

電腦、筆記型電腦、伺服器等設備，進行電磁紀錄之數位證據蒐集、回復及驗證，除電腦相關設備外，該公司亦提供智慧型手機、iPod、iPad 及平版電腦等電子 3C 設備之資料擷取及回復分析，服務對象擴及政府機構、小型企業、律師事務所、私人偵探事務所及一般民眾等，該公司經常爲各類案件提供中立之第三方意見，由於立場公正、依法正當執業，提供之數位證據往往扮演案件中客觀重要角色，處理之案件類型包含民、刑事案件、家庭紛爭、離婚、子女扶養權、電腦犯罪及資料解析回復等。

參、 ADFSL 組織會議簡介

ADFSL 係一非官方及非營利之組織，該協會研究領域不僅僅針對數位證據方面，亦包括網路行爲所涉及之法律議題、社會議題及安全議題等，近年來更將研究領域擴展至犯罪調查、民事案件以及政府國土安全等面向。自 2006 年起每年舉辦國際數位鑑識會議，今年係第 7 屆之國際學術研討會，所邀稿件論文主題計有數位鑑識國際化及個人領域之探討、網際網路安全、相關法律領域、商用軟體於數位鑑識之分析及案例研究。會議特別邀請來自埃及的 Mohamed Chawki 教授演講，Mohamed Chawki 教授是埃及資深法官、法國里昂第三大學法學博士（University of Lyon Ⅲ）、金融市場管理局前主席顧問（former advisor to the Chairman of Capital Market Authority；簡稱

CMA）、財政監督局主席（the Chairman of the Egyptian Financial Supervisory Authority；EFSA），演講主題爲埃及的 IT 發展及政權改變（IT and Regime Change）。ADFSL 大會主席爲美國籍的 Glenn S. Dardick 教授，Dardick 博士畢業於美國維吉尼亞聯邦大學，現於朗伍德大學管理資訊系統學系任教（Management Information System），於數位鑑識領域有著顯著研究及論文發表。

肆、參訪 AVM 公司活動紀要

參訪時間於下午 2 點至 5 點止，AVM 公司負責人 Domingo J. Rivera 先生親自接待解說，帶領我們參觀公司辦公環境及數位證據工作室，介紹證據工作室之相關設備及軟硬體，以及從事案件類型，介紹完畢後與我們進行經驗會談，可分爲數位鑑識領域、案件技術類型、人員培訓等，分述如次：

一、電腦數位鑑識領域趨勢進展迅速

Rivera 先生表示電腦數位鑑識已是司法程序中不可或缺的一環，該公司屬民間企業，電腦鑑識業務強調保持立場公正客觀，不介入案件正方或反方當事人間，只針對所送證物進行數位證據分析，所產出之報告方能令人信服。此外數位鑑識領域進展快速，新產品與新技術日新月異，鑑識人員必須要自我砥礪、時時精進、同業交流、並多方上課參與會議，方能於鑑識領域生存，否則必將落伍淘汰。

二、案件技術類型

Rivera 先生表示 AVM 公司所處理之案件類型繁雜，政府機關及各民間事務所亦時常委託送鑑，型態皆不同，所蒐集之數位證物標的、類型及方法不同，所需鑑識工具及軟體亦有所不同，爲了完成各種數位鑑識工作，往往花費極大心思及人力，瞭解需求透過經驗累積及專家請益交流，才能精準蒐集所需之證據。所有的案件中，「證物監管鏈」（Chain of Custody）則是必須具有完整性及一致性，遵守證物保管及鑑識流程的規定，不可擅自變更違反流程作法，以維持案件證物的可信度。Rivera 先生亦將該公司執行案件時所依循之「鑑識確認流程表」（Forensics Checklist）提供給我方參考。

三、人員培訓

人員培訓方面，Rivera 先生認爲應先認識瞭解各種作業系統，進而研究各類型檔案架構以及研究硬碟等儲存媒體構造、運作原理，最後再學習鑑識軟體應用，如此才能瞭解鑑識軟體所運用之原理，取得何種、何類的資料，以進一步分析研究。除基礎學科養成外，所舉行之研討會議、訓練課程及鑑識廠商軟體介紹等，對於鑑識人員而言，皆是不可或缺且有效的學習機會，從基礎學科原理與實際案件累積增加深度，再與外部接觸及交流增加視野廣度，才能夠培養多元多方的人才。

伍、 2012 ADFSL 數位鑑識、安全及法律組織研討會紀要

一、Session 1（8：50am – 10：10am）:「Update on the State of the Science of Digital Evidence Examination」學術論文，本篇論文是由加州科學研究學院校長 Fred Cohen 和他的研究團隊所提出,這篇文章更新了以往數位證據鑑識在幾個基本條件上所存有之共識，研究成果發現重要的共識只出現在清楚的定義下，許多基礎概念已有科學性的共識,而數位鑑識仍然缺乏普遍性的共通語言，換言之，即便是在已經相對成熟的證據蒐集上，有關取得數位證據的適切性仍舊缺乏某種共識。因此使用清楚詳實的定義成爲數位鑑識領域中,要達到科學性的共識所必要採取的作爲。另外在這篇文章裡還探討了一些研究，像是美國國家標準與技術研究院（The National Institute of Standards and Technology；NIST）曾經利用有局限性的少數工具進行數位鑑識工作，研究發現這些工具會造成重大的限制性，因此應用這些工具的使用者或是檢視人員（Examiner）必須要瞭解所選用的工具和最後產生的結果是否可靠。

二、Session 2（10：30am – 12：30am）:「The Xbox 360 and Steganography：How Criminals and Terrorists Could Be "Going Dark"」,此篇論文主要在探討數位鑑識科技中的影像匿蹤技術

應用（steganography），影像匿蹤技術應用乃係最適合使用於多媒體檔案上，因多媒體檔案容量較大，使用者可利用調整影像畫素（Pixel）對應字母的技術來嵌入隱藏的訊息。在本文中 3 位來自美國賓州 Drexel 大學的研究生 Ashley, Rob 以及 Cindy，以破解 Xbox 360 遊戲機內所藏匿之訊息爲例，說明犯罪者或是恐怖份子亟有可能利用影像匿蹤技術於 Xbox 360 遊戲機來傳達訊息及檔案資料，也說明了鑑識技術在分析傳統電腦和遊戲機之間不同，報告提到使用影像匿蹤技術有兩個主要的方法，首先是有關於嵌入的技術，也就是將要嵌入的另一個檔案資訊（祕密檔案）植入原始的檔案（傳送檔案），一但植入，影像檔案的容量便會出現些微改變。第二種方式被稱爲取代替換，也就是將原始檔案的資料以其他檔案作爲取代，像是在一個 8 bit 的圖像檔裡，用其他的資料取代掉最不重要的位元（Least Significant Digit-LSD）對原來畫素的影響改變最小，影像改變的幅度以人眼亦無法判斷出差異。研究者另外示範拆解 Xbox 360 遊戲機的硬體，尋找需分析的驅動硬體並檢查遊戲機是否被動過手腳。應用影像匿蹤技術這樣一個新的概念雖是從古希臘時代就有的想法，一直至演進至現代，身爲數位鑑識人員，能多瞭解國外已經有的研究，對於未來的鑑識工

作拓展將可產生更多的幫助。

三、Session 3(1：45pm – 3：00pm)：「Nist Cloud Computer Reference Model and its Forensic Implications」，此篇論文由英國都柏林大學網路安全暨網路犯罪調查中心所發表，探討雲端運算和數位鑑識，在 2011 年底美國國家標準與技術研究院（NIST）針對雲端運算最新發布的定義中，缺乏了鑑識概念的應用。雲端運算是一個尋常且便利的模式，藉由網路使用分享所有的電腦資源（包含網路服務儲存 NAS 等）。這樣的雲端提供者可以是個人，也可以是組織，負責對有興趣的團體創造提供雲端服務，雲端廠商管理電腦架構以提供服務，應用雲端軟體來處理顧客的需求，透由網路傳送雲端服務給雲端客戶，雲端所提供的服務可以區分成 5 種角色定位，包含雲端使用者（Cloud Consumer）、雲端提供者（Cloud Provider）、雲端通信公司（Cloud Carrier）、雲端稽核者（Cloud Auditor）及雲端中間人（Cloud Broker），其中雲端提供者又可分爲使用服務（Service Deployment），服務組合（Service Orchestration），雲端服務管理（Cloud Service management），安全（Security）及隱私（Privacy）。在雲端鑑識方面，雲端提供者及雲端使用者之間一直欠缺標準界面及法律程序，造成電腦調查的能力仍處於原

始階段，需要一標準介面及法律規範，以面對多樣的司法程序，爲了保存雲端數位資料，雲端提供者需要有一組人員，提供維護安全問題、輔助外部問題處理及法律諮詢的能力。而雲端中間人需協調各方的雲端提供者，確認所必要的鑑識能力，以符合雲端使用者的需求。這樣的雲端運算概念是近期人類發展裡的一個大變化，也會一直持續改變我們對電腦產業的管理使用。本文學者認爲在面臨越來越多的全球性網路犯罪問題時，應用雲端運算時，也要同時抓住這個發展的黃金時段，建造一套合適的數位鑑識標準架構，研究者未來也將積極參與 NIST 舉辦的研討會及說明會，持續追蹤進化及成熟的雲端運算，將數位鑑識之作爲視爲一個必要性元素，納入雲端標準化的過程中。

四、Session 4（3：20pm – 4：40pm）:「IPad2 Logical Acquisition : Automated or Manual Examination?」，此篇論文係屬實際測試報告，由阿拉伯聯合大公國札耶德大學（Zayed University），4 位進階網路鑑識研究實驗室（Advanced Cyber Forensics Research Laboratory）人員所發表，研究 iPad2 的邏輯層擷取備份資料時，以「自動擷取」的方式與「手動擷取」的方式間，比較所取得數位證據的差異，研究的動機係因 iPad 系列的產

品在全球的使用率不斷地上升，該產品在數位鑑識的犯罪調查活動中，已然是蒐集關鍵證據的資料來源。「自動擷取」的方式是透過安裝花燈軟體（Lantern Software）自動解析資料進而取得證據，「手動擷取」的方式係透過 Apple iTunes 軟體以備份方法逐一取得，結果顯示利用「手動擷取」的方式更能取得較多的數位證據資料。另研究者表示，若使用 iOS 系統以「自動擷取」資料的方式則更能快速地得到數位證據資料，不同的 iOS 系統裝置（以 iOS 3 與 iOS 4 爲例），所取得的「檔案名稱」在備份的資料夾中會有所不同，這樣的研究結果對於 iPad2 的數位鑑識技術而言，是一個很有幫助的參考。

五、Session 5（8：30am – 10：15am）：「Russia：The Analysis of the 2011 Russian Cybercrime Scene」，此篇論文在分析 2011 年俄羅斯的網路犯罪現況，文中表示去年俄羅斯人或說俄羅斯語言的民族，網路犯罪數量超過全球數量比例的三分之一，這數據令當地政府不得不重視這個犯罪問題，該國的網路安全研究集團（IB-Group）估計，去年全球的網路犯罪金額達到 12.5 億美元（約爲 7.74 億俄元），而俄羅斯族群就包含 4.5 億美元，比例最高的網路犯罪樣態就是線上詐欺，傳統黑手黨或黑道組織控制許多俄羅斯的組織團體，以犯罪模式結合 C2C 方式

（Crime-to-Crime），進行網路犯罪詐騙，最著名的案例就是 2008 年蘇格蘭皇家銀行遭到 Yevgeniy Anikin 及 Viktor Pleschuk 等駭客從全球支付 ATM（WorldPay ATM）系統竊取達 1 千萬美元，研究指出會造成網路犯罪原因的攀升，主因是該國電腦工程師及電腦技術人員的薪水少、工作操勞（耗損腦力）、壓力大及時間長，無法足夠應付當地生活水平，再加上俄羅斯不齊備的法律及缺乏嚴格的刑罰等因素所造成。

六、Session 6（10：30am – 12：30am）:「Facilitating Forensics in the Mobile Millennium Through Proactive Enterprise Security」, 接下來這個主題的發表學者 Andrew R. Scholnick 教授，他在電腦安全領域已經有超過 30 多年的經驗，他最近的職位爲美國陸軍科技團隊的一員，過去曾經指導美國國防部通過整合高科技技術，並進一步評估認證像是 Android 系統的安全性，將通過認證的智慧型手機應用於美國軍方，Scholnick 教授在現代多款智慧型手機的安全性維護上多有研究，他並藉由本文討論，目前新型的智慧型手機通訊設備存有安全性顧慮的企業中，造成多種新型態的問題，這些新的溝通工具重新定義了現代工作環境所處的架構。這些變化已經造成科技上許多有力的改變，卻也代表了相當程度上有關行動電話的安全性顧慮，這樣的顧

慮在許多公司機構中是種潛在的安全資訊維護問題，換句話說，智慧型手機的快速發展，在某些程度已超越許多企業集團所架構的安全資訊維護機制，而這些影響也將改變數位鑑識分析的作爲。在未來，會有更多的方法來整合智慧手機的資源，並且提供政府或是軍隊提昇於智慧手機方面的安全維護等級，達到更有效率安全的使用，屆時也會出現更多鑑識作爲被應用之研究。

七、Session 7（1：45pm – 3：00pm）:「A Case Study of the Challenges of Cyber Forensics Analysis of Digital Evidence in a Child Pornography Trial」，此篇論文係由澳洲莫道課大學（Murdoch University）IT 學系 Richard Boddington 先生所提出，Boddington 先生擁有法醫科學榮譽理學士資格（B.Sc（Hons）），目前於莫道課大學攻讀博士學位，因具有警察及網路安全技術相關背景，經常爲法院提供民、刑事案件的數位鑑識分析，目前有任教資訊安全及網路鑑識等課程，本文章引用圖爾明模型（Toulmin’s Model）針對兒童色情犯罪審判進行案例研究，圖爾明模型係論證結構中最具代表性，他認爲一個明確的論證可以經由資料推論而產生最後主張，該模型的論證架構圖中，以 6 個參數（因子）組成，其因子代表意義如下：

（一）資料（Data）：可支持主張的事實。

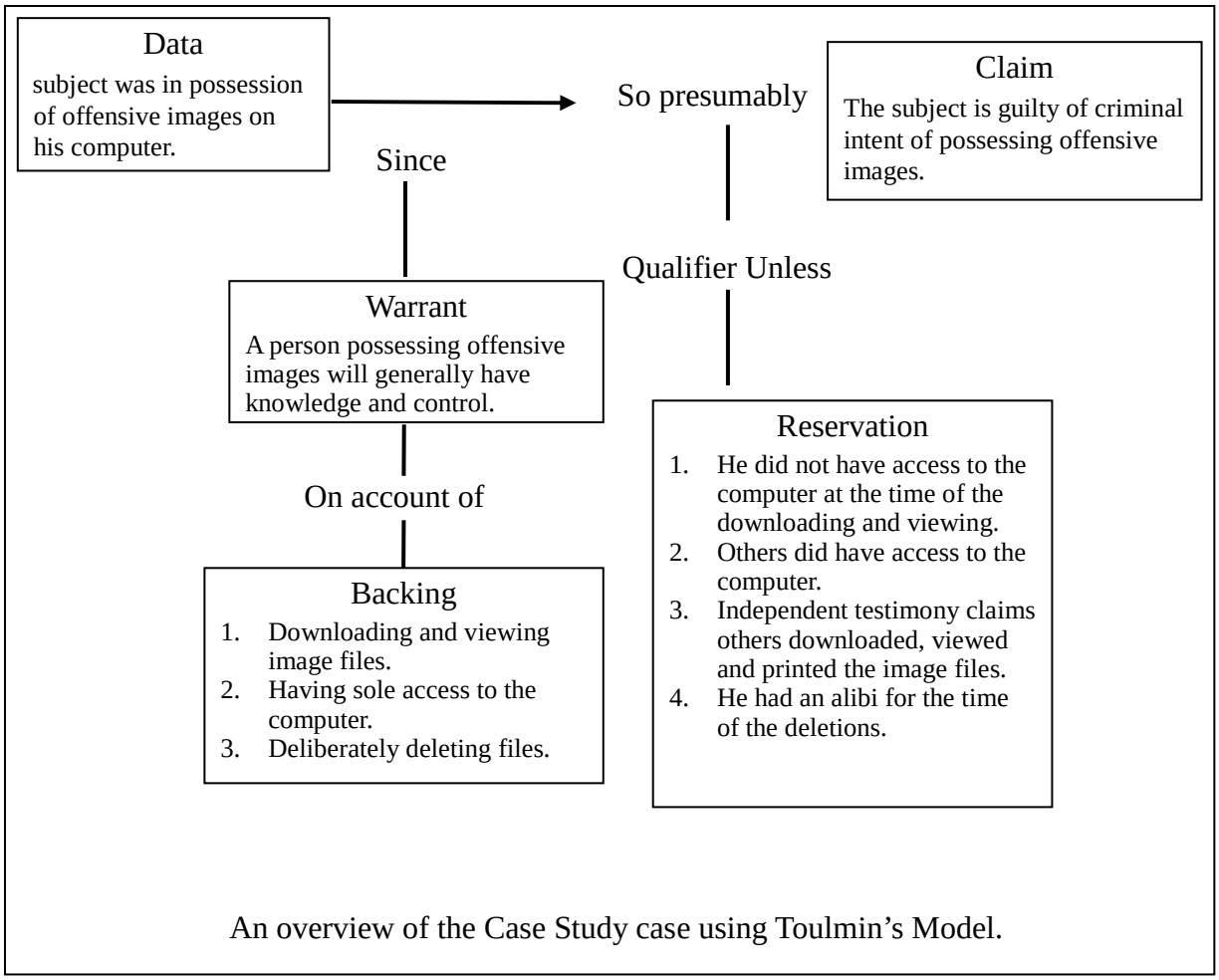
（二）主張（Claim）：論證過程中形成的結論，以合理資料建立合乎邏輯概念，以說服他人。

（三）理由（Warrant）：資料之推論過程至主張成立，提供所需的規則及證據。

（四）支持（Backing）：一般人可認同之邏輯觀念，用來證明理由（Warrant）。

（五）條件限制（Qualifier）： 在特定限制下，主張論證方可成立。

（六）反駁（Rebuttal 或 Reservation）：說明論證過程中例外情形。



An overview of the Case Study case using Toulmin's Model.

圖形模式如上所示，「資料」顯示犯罪嫌疑人在他自己電腦中存有不法圖片。「理由」：表示擁有不法圖片的人應有所認知並有控制能力，「理由」的「支持」是：犯罪嫌疑人自行下載或檢視這些不法圖片、擁有電腦唯一的存取權利、刻意刪除檔案。「條件限制」：若他在該時段無下載或檢視存取電腦、其他人有存取他的電腦、另有獨立公正的證詞表示其他人有下載存取及列印這些圖檔、檔案刪除的時段中犯罪嫌疑人有不在場證明。若前述「條件限制」出現，則「主張」犯罪嫌疑人有犯罪意圖來存取不法圖片則不成立，即當事人無罪；反之，若「條

件限制」未出現，則可邏輯推論「主張」犯罪嫌疑人有犯罪意圖來存取不法圖片，亦當事人有罪。藉由流程分析、正反舉證、背景檢查及驗證等方式，來推測評判案件當事人之涉案程度與否，透過此種模型分析實際案件，提升案件證據之可接受度（admissibility）、可信賴度（plausibility）及可確認度（corroboration）。

八、Session 8（3：20pm – 4：40pm）：「Pathway into a Security Professional：A New Cyber Security and Forensic Computing Curriculum」，本文是由南澳大學 Elena Sitnikova 及 Jill Slay 教授所提出，他提出一套新的網路安全及數位鑑識課程的連結學習計畫，讓大學生逐步進修學習至研究所及博士班的等級，課程分 2 部分，一是數位證據鑑識課程類，有數位鑑識（Forensic Computing）、網路鑑識（Network Froensics Course）、鑑識結果分析及報告（Electronic Evidence Analysis and Presentation）、E-Crime 及 E-Discovery，另一是網路安全課程類，有入侵分析及回應（Intrusion Analysis and Response）、重要基礎及控制系統安全（Critical Infrastructure and Control Systems Security）、軟體安全週期（Software Security Lifecycle）、資訊確保與安全（Information Assurance and

Security），爲使課程更彈性便利，設計成面對面課程及遠距課程 2 種，爲期 13 週，此計畫已經完成 2 年週期循環，目前仍運作實施，且不定時依據最新技術發表更新課程內容，已有 3 個學生通過了這 8 門課程，且繼續深造研究所及進階課程。

陸、 心得與建議

一、心得

（一）此次前往美國維吉尼亞州列治文市參訪 AVM 公司及參與 ADFSL 會議，瞭解美國民間鑑識公司業者於數位電磁證物相關作法，及 ADFSL 會議各國發表鑑識研究論文，對於本局從事數位鑑識工作有著相當的助益，對於 AVM 公司負責人所提供的「鑑識確認流程表」（Forensics Checklist），從送件人、收件證明、證物型態、外觀、序號資訊、製作映象檔（Image）過程、防寫裝置使用、紀錄 Hash 值、檢驗過程紀錄、電腦系統紀錄、紀錄刪除及回復檔案及路徑、分析電腦及網路活動、檢視殘缺片段空間、報告撰寫格式等，有助於檢視本數位鑑識實驗室認證流程所不足或欠缺之處，亦可強化完備「證物監管鏈」（Chain of Custody）的流程。

（二）數位鑑識工作面臨各式電腦設備及 3C 資訊產品推陳出新，各種資料擷取方式與保存皆不相同，每次新設備的發表，就

產生一次新的數位證據保存擷取技術，在此鑑識領域必須保持學習的熱誠，增加案件實務經驗累積，謹守法律規範要件，以公平、公正及同理心面對，方能順利完成數位鑑識工作。

（三）iPad2 的數位鑑識技術，多利用 Apple iTune 軟體及 XRY 鑑識分析工具，這次會議論文發表使用花燈軟體（Lantern Software）來比對所擷取證據資料，可作爲將來鑑識 iPad2 時的參考。

（四）俄羅斯 2011 年度居高不下的網路犯罪數字，引起各國之注意，係因當地電腦從業人員薪資低廉，工作負荷重且法規不完整等因素造成，從事電腦鑑識工作亦屬相關工作內容，時時轉換心境，適時充電，面對各類案件挑戰，以永保鑑識工作能量及熱誠。

二、建議事項

（一）持續參與國際數位鑑識研討會議，維持與各國專家教授友好關係，強化數位鑑識專業聯繫及交流。

（二）強化各類型電子消費產品之數位鑑識技術發展，提升數位鑑識工作成效。

（三）與國內手機製造商及各類電信公司合作，配合手機鑑識及 SIM 卡鑑識工作，減少手機鑑識工作斷層。

（四）增進學術單位交流，參考學術模型架構及原理，強化犯罪調查及數位鑑識等實務工作。

（五）持續加強本局調查人員語言能力，培養國際觀及視野，增加國際合作及交流，提升本局調查工作能見度。

柒、附表 1（AVM 公司提供之 Forensics Checklist）

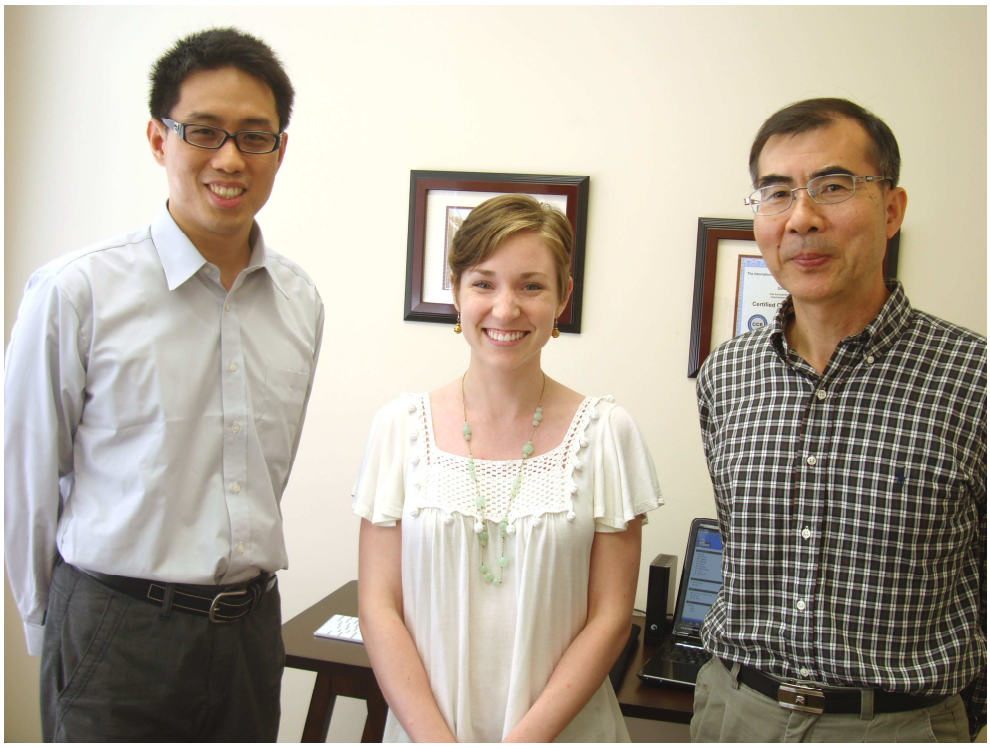
Computer Forensics and Forensic Report Checklist

- **Describe any media and include a picture of that media**
- **The color, size, label, serial number, or any other descriptive found on the media**
- **Chain of Custody was Established**
- **Who gave it to you?**
- **Receipt was given for the media**
- **That it was securely stored**
- **How did you obtain it （removed from computer, image was sent, etc.）**
- **Shipping Receipts or Other Delivery records**
- **That the media was protected by: Anti-static policy, Storage and shipping controls**
- **Write Blocking and Validation of Write Blocking**
- **Original Media Hashes**
- **Use of Sterile Target Media**
- **Hashes of Image Media**
- **That Examinations were performed on images**
- **Note all volume attributes （date, name, etc.）**
- **List all partitions found**
- **Examine all partitions and all files**
- **Note all active and deleted files on the media**
- **Note path and location of files on specific media**
- **Indicate if the file was deleted or not viewable for some reason**
- **Recover All Documents and Note Content**
- **Recover and Note All Passwords**
- **Analyze all Document Metadata**
- **Analyze Internet Activity and History**
- **Note any unusual or special purpose software**
- **Analyze any network connections on record**
- **Analyze any websites or domains found**
- **Note any attempts to obfuscate data or destructive methods**
- **Examine Slack and Unallocated Space**
- **Use Data Carving on Slack and Unallocated Space**
- **Document all procedures and steps**
- **Draw Conclusions about any relevant files**
- **Draw Conclusions about any related files**

附表 2（AVM 公司參訪照片）

我方人員與 AVM 公司負責人 Domingo J. Rivera 先生於該公司合影

我方人員與 AVM 公司同仁合影



我方人員與 AVM 公司同仁合影

附表 3（參與 2012ADFSL 研討會照片）

ADFSL 研討會報到會場

ADFSL 研討會發表會場

與 ADFSL 組織大會主席 Glenn S. Dardick 教授合影（中間者）

與 ADFSL 組織大會主席 Glenn S. Dardick 教授合影（中間者）

及香港大學姚兆明教授合影（左 1）