行政院及所屬各機關出國報告

（出國類別：其他）

參加美國國家白領犯罪中心(National White Collar Crime Center)舉辦之「數位資料回復及鑑識課程」研討會報告

服務機關：內政部警政署刑事警察局
姓名職稱：周伯翰偵查員
派赴國家：美國
出國期間：100 年 08 月 12 日 至 08 月 21 日
報告日期：100 年 11 月 9 日

摘要

本文說明此次出國參加美國國家白領犯罪中心 NW3C (National White Collar Crime Center)舉辦之「數位資料回復及鑑識課程研討會」的研討會的教學內容及參加心得。

研討會參加的成員來自美國司法第一線執法人員。包括西雅圖市警察、聯邦調查局調查員、及大學教授等等。課程的內容是針對電腦證物的(1)保存、(2)蒐集、(3)分析、(4)報告，教導警察執行鑑識軟體工具及製作符合刑事法律證據能力的司法報告。

研討會教學包括(1)計算機概論、(2)硬碟的組態及組成、(3)作業系統檔案系統架構實務操作、(4)犯罪現場模擬檔案還原及(5)Forensic Toolkit(FTK)軟體使用。

本文也綜整研討會在犯罪情資分析方面的實際實務操作訓練授課講義及現場上課流程環境，提出研習心得及建議。

此行上課內容是「數位資料回復及鑑識」重要觀念及正在使用的 FTK 工具，利用分析數位證物，有效應用犯罪情資分析實務及幫助犯罪偵查。期望讀者在閱讀本文後，能對認識美國數位資料犯罪情資分析及犯罪現場數位證物鑑識實務。也能引發未來我國公務人員出國參加類似 NW3C 或美國警察常訓課程，節省行程花費及增加學習效益。

途中順道參訪 Kent 市政府警察局訓練中心(Kent Police Training Center)，這個中心是美國華盛頓州用來訓練美國司法人員電腦專業課程和反擊恐怖份子攻擊的專業訓練單位。這個訓練中心在美國 911 事件發生後，也成爲一個警察訓練反恐的訓練中心。因爲本計畫的內容是希望能見習反恐情資分析，因此安排見習這個中心。學習反恐情資分析平時訓練警察及相關單位如合聯合演習作業。警察局訓練中心業務包括: 訓練警察的消防救生、警察街頭巡邏訓練、反恐突擊訓練、網路犯罪訓練。尤其是該中心長期和民間公司或財團法人合作，引進有系統且專業的課程，幫助警察學習專業知識。此行希望由完整見習，引進類似的制度。也希望讀者在讀完本文後能對美國警察電腦鑑識標準程序有基礎概念，且會引發讀者服務單位派員出國到美國實習相關課程，政府人員應學習美國警察熱心服務及值得讚賞的團隊精神。

目次

壹、前言及目的

隨著網際網路的迅速發展和廣泛普及，網路犯罪手法及科技工具進步，政府迫切需要電腦犯罪證物的專業鑑識人員，幫助犯罪案件的追查及製作鑑識報告。根據各國的司法調查報告均指出:現代犯罪通常會在過程使用電腦或電話，所以數位證物有可能是破獲刑案的重要證據或重要線索。而專業電腦犯罪案件也日漸增加，專業電腦犯罪案件也帶來巨大的經濟損失。隨著電腦犯罪數量的增長。在短短幾年的時間裏，電腦鑑識在政府司法部門訴訟案件佔的角色日漸增加，電腦案件類型也從傳統的電腦病毒破壞，轉爲竊取有價值的數位資訊。台灣的各大電信公司近年均發現詐騙集團滲透，派遣或買通工程技術人員，以檔案複製方式，有計劃地竊取客戶的個人資料。

犯罪的案件除了傳統的案件，在犯案時會使用電腦爲通信或通聯工具(簡訊、網路即時通、網路電話)之外，司法人員偵查專業犯罪的詐欺集團過程中，更須一套能有效及標準化的電子數位證據的分析技巧及培養訓練專用軟體工具，並且這個電腦鑑識分析流程要能符合未來在法庭的呈現要求，及犯罪現場即時分析證物及情報，幫助警察偵訊及製作刑事報告。

最近的刑事案件中，需要電腦鑑識協助偵辦的案件包括證券業及銀行業，案件犯罪人更是在電腦領域專業從業人員，使用的電腦工具及犯罪手法，必須有電腦鑑識人員參與犯罪的偵查。在過去個人資料保護法未實施前，部份商業公司，未重視或有效管理客戶個人資料，台灣地區詐騙集團專職蒐集商業公司擁有的一般民眾個人隱私資料，用以爲詐騙劇本。間接造成台灣地區詐騙犯罪盛行，損失巨大。

由於偵辦案件的電腦鑑識需求日漸增加，此行將美國現在最新的電腦鑑識軟體及管理方法、警察在犯罪現場電腦的鑑識制度，學習回國。更重要的學習是:此行透過 NW3C 的電腦教育課程制度，將種子教師的概念及教學制度引回台灣，希望未來台灣也能有類似的教育制度。

上課地點選定美國華盛頓州的肯特市警察訓練中心，報名參加美國國家白領犯罪中心 National White Collar Crime Center (NW3C)的電腦鑑識課程。NW3C 現在是美國司法單位指導電腦犯罪及經濟犯罪的專業訓練及支援單位，教師包括司法單位退休轉職及大學教授。本次上課的學生包括西雅圖市警察局警察及華盛頓州分局警察，本局自獲得 NW3C 同意本局學員不須繳交學費，讓本局學員以美國友好國家的國際警察學員身份參加上課後，即積極規劃考察主題、議題，並努力準備課程講義內容，以利進行有效交流及學習。學員到美國上課後，美國承辦人員及上課認識的警察同學的真誠與熱情，非常值得肯定與讚賞。

人員遴選方面，由本局指派 1 員偵查員周伯翰參加上課。本次考察行程計 10 天，主要上課 4 天，參訪肯特市警察局訓練中心 1 天，自 100 年 8 月 12 日至 21 日。

National White Collar Crime Center(NW3C)的 BDRA 課程，教學內容包括:學習先進的數位鑑識技術、國際上該領域最新動態、應用實踐，並有經典案例分析及軟體教學、技術指導。課程講義內容包括:美國司法單位的電子證物在現場的調查手冊、Norton 公司的硬碟架構說明手冊、還原 Compact Flash 電子媒體手冊、Windows 及 DOS 的軟體開機手冊、犯罪現場的採證手冊、Windows 格式化命令解析。經由訪談參與上課的同學，得知美國的警察平常須自費參加電腦課程或警察專業課程，美國政府給予公假，但上課報名費用由同學自費。

現在的刑事案件，越來越常見犯罪者利用電腦及高科技通訊工具應用，在犯罪現場使用的電腦中有通聯通訊紀錄、犯罪筆記本、Email 通聯複本、犯罪所得檔案紀錄，刑事人員在犯罪現場要能有效讀取數位通訊紀錄、電腦中的帳冊檔案、電腦網路附加的通聯紀錄(email、Instant messages、facebook social networking software、……)。這套課程是要讓司法人員在接觸科技犯罪現場及電子證物時，能採行有效的四個程序: 1.證物蒐集(Collect)、2.檢查(Examine)、3.分析(Analysis)、4.司法報告(Report)。

這次訓練的講義中有美國司法部電子證物調查組撰寫的手冊，供警察人員參考爲現場標準手冊。另外，訓練課程實作是利用美國司法部發展的標準 FTK，針對常見的檔案(文字檔及影像檔案)證據，能還原及保存，能進行有效的司法起訴及調查。課程內容即是針對電腦硬碟的格式、原理、讀取及備份的操作，作有效演練及實作教學。讓警察在現場能有效保存證據、紀錄環境及使用各種硬碟軟體工具及讀取資料，並未來在司法法庭上能爲有效的數位證據及證人資格。

研討會前兩天是電腦計算機概論，後兩天是用 FTK 實作電腦鑑識。電腦鑑識讀取電腦資料過程，在犯罪嫌疑犯願意配合搜索或訊問的有效時間，以能取得密碼及該電腦遠端連線(連線出去及連進入)的紀錄爲優先。在取得電腦的帳號及密碼後，要開始用標準的 FTK 工具進行影像檔的讀取及製作 image 影像(如 ISO 檔案)，並檢查硬碟的分割磁區(partitions)，如果有隱藏磁區(hidden partition)，要將它設爲啓動模式(active mode) ，針對隱藏磁區作映像檔案(image file)。類似的軟體工具可被應用在手機的 SIM 卡資料及手機 Flash Card 的數位鑑識。

電腦鑑識的核心是利用作可完整對映硬碟映像檔案後，要用 MD5 工具檢查映像檔案磁區和檔案的完整性，並且詳細紀錄各映像檔案的內容及檔案 MD5 亂數值、時間。要注意映像檔案的時間是否符合時間次序及辦理案件的採證時間。映像檔案要用格式化過的乾淨硬碟備份。未來在司法程序的漫長起訴過程中(目前部份刑事案件的訴訟時間，長達數 10 年未結案。司法程序訴訟過程中，警察及檢察官必須思考完整保存數位證據，在未來保有公信力。如果不同審級的審判需調用證據，仍然可以獲得明確且一致的證據)。

在此行程中，學員到肯特市警察訓練中心附近安置好後，就開始準備 NW3C 的上課講義及教材。在學習的教室裡，每位學員都以一台筆記電腦爲上課模擬，完整實習認識數位鑑識案件的分析。

貳、考察行程

一、行程紀要如下:

8 月 12 日 第 1 日	啟程，由桃園機場往美國華盛頓州。
8 月 13 日至 14 日 第 2 日、第 3 日	預備研習資料。
8 月 15 日至 18 日 第 4 日~第 7 日	參加美國國家白領犯罪中心(NW3C)「數位資料回復及鑑識課程」。
8 月 19 日 第 8 日	參訪華盛頓州肯特市警察局訓練中心。
8 月 20 日至 21 日 第 9 日、第 10 日	啟程返國。
參加人員	警政署刑事警察局資訊室周伯翰偵查員(共 1 員)

二、行程內容:

此次行程是參加 NW3C 主辦的[數位資料回復及鑑識課程研討會]，主辦地點是華盛頓州肯特市警察局訓練中心。課程內容配合美國司法單位的課程學分認證，本局派員參加美國警察研討會課程，課程目的是培養美國司法人員的電腦鑑識專業能力。課程內容在第參節說明。研習會場的軟體、硬體建設及上課情形如下圖。

圖 1 及圖 2:上課地點及設備環境。地點: 華盛頓州肯特市警察局訓練中心(24523 116th avenue South East Kent, WA).建築大樓是美國 Kent Police Training Center.

參、數位資料回復及鑑識課程研討會過程介紹

一、 NW3C 介紹

NW3C(National White Collar Crime Center)是一個成立三十年以上的非盈利性會員組織。通過結合訓練和支援訓練服務支援，協助美國各州和聯邦執法機構的司法偵辦經濟犯罪及電腦犯罪、分享司法警察專業經驗及技能，並有效傳承司法訓練資源。幫助司法警察單位解決新出現的經濟和網絡犯罪問題。此次上課地點是: 肯特市警察局訓練中心 Kent Police Training Center (24523 116th Avenue South East, Kent, WA 98031)。本地點是位在美國東岸華盛頓州，是警察和其他反恐單位合作的訓練中心，中心主要提供警察、消防、電腦訓練。挑選本中心爲上課地點的主要原因是此行透過這個中心和美國反恐警察及消防單位均有長期合作，能由此獲得打擊犯罪現場的數位鑑識實務。此外，這個中心的位置是位在美國西岸，交通時間比美國東岸來回台北，旅程可節省約 9 個小時。從西雅圖機場出來後，轉公車及火車，約需 2 小時的公車交通時間可到訓練中心。目前此中心除了電腦訓練，還包括員警在巡邏時的技巧訓練、犯罪現場調查、員警駕駛訓練、消防訓練、警察及消防單位的整合、電腦教室、情報訓練，這個訓練中心的課程可以和其它華盛頓州的警察資源互補及共享，例如 Kent Police College.

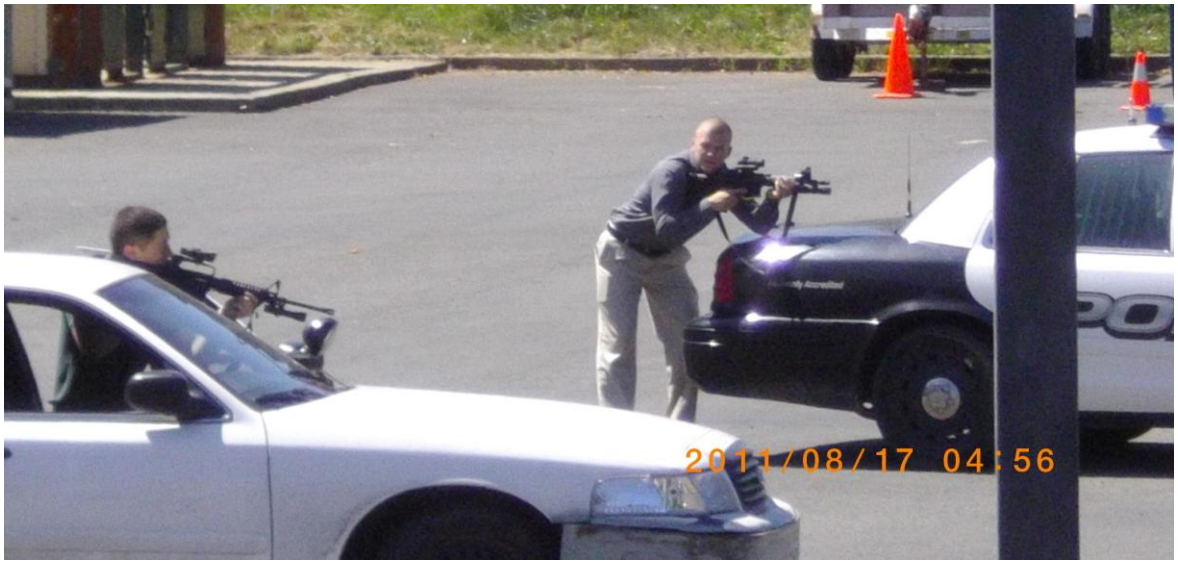


圖 3 及圖 4: 中心除了電腦訓練，還包括員警在巡邏時的技巧訓練、犯罪現場調查、電腦教室、情報訓練、員警駕駛訓練、警察及消防單位的整合、消防訓練，這個訓練中心的課程可以和其它華盛頓州的警察資源互補及共享，例如 Kent Police College

以 NW3C 電腦課程爲例，說明 NW3C 課程廣度和深度。這些專業課程請參考 NW3C 開課的電腦課程明細表: http://www.nw3c.org/ocr/courses_desc.cfm. 超過 30 門專業的電腦課程，均是和電腦犯罪或資訊案全有關的課程，如下表:

Cyber Investigation 100 - Identifying and Seizing Electronic Evidence (ISEE)
Cyber Investigation 101 - Secure Techniques for Onsite Preview (STOP)
Cyber Investigation 105 - Basic Cell Phone Investigations (BCPI)
Cyber Investigation 201 - Basic On-Line Technical Skills (BOTS)
Cyber-Investigation 205 - Cell Phone Interrogation (CPI)
Cyber-Investigation 210 GPS Interrogation (GPSI)
Cyber-Investigation 220 - Wireless Network Investigation (WNI)

研討會過程會有考試和階段測驗。美國警察能有 NW3C 支持完整的電腦訓練，台灣警察人員前往美國，可學習電腦課程業務，回國後，可推動類似電腦課程業務，促進刑事司法進步。

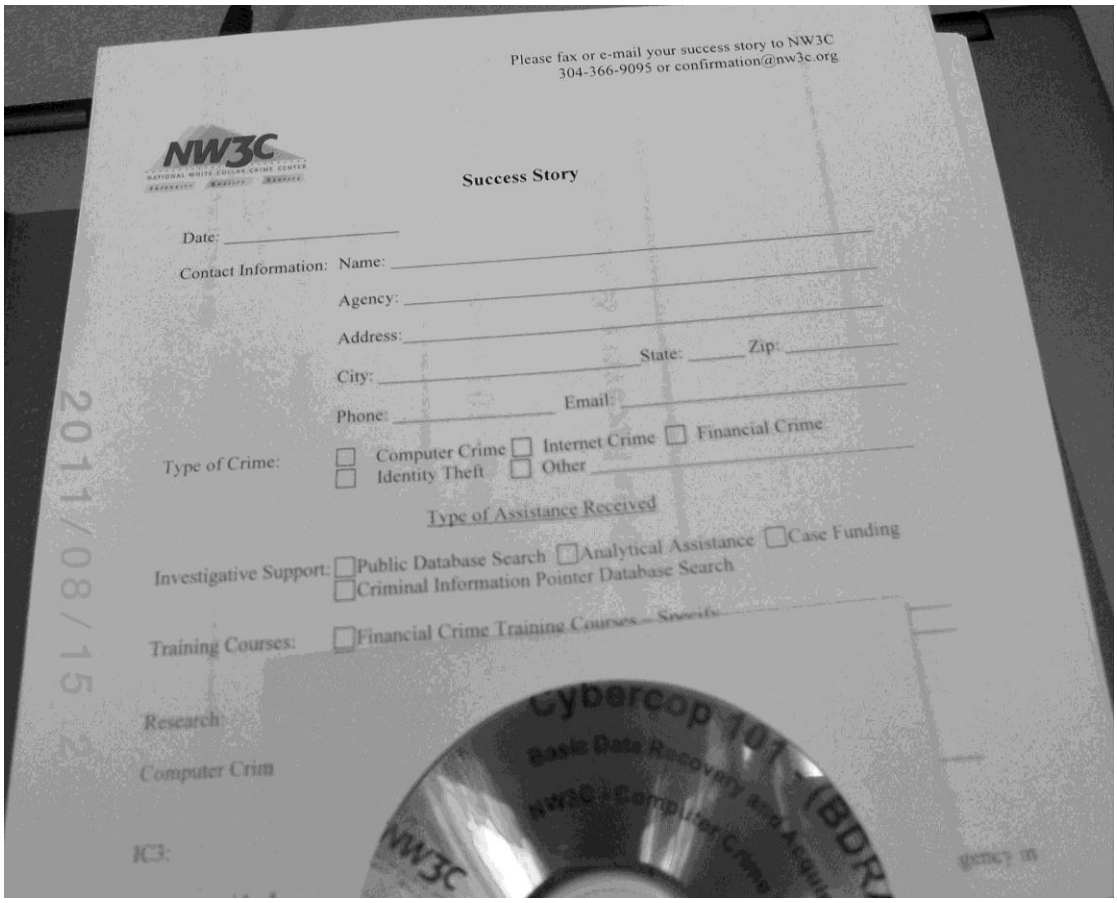


圖 5: NW3C 支持美國警察完整的電腦訓練。我政府應派公務員前往美國，學習及推動類似電腦教育專業課程業務，長期且有系統地促進刑事司法進步。

二、 「數位資料回復及鑑識課程」研討會內容介紹

（一）研討會的報名、時間、地點、參與人員:

電腦鑑識課程(**Basic Data Recovery and Acquisition)**的開課目的是增強司法人員在調查電腦犯罪的調查能力，提供基本的軟體及硬體知識。所以參加課程的必要條件是從事司法調查的司法人員或警察人員。我國警察部門在考慮公務出國見習或訪問時，應該優先詢問能否參加業務相關且類似 NW3C 的課程或美國警察的研習討論。參加類似 NW3C 的課程優點有(1)學費便宜:一般美國上課，通常學費爲 4 萬元新臺幣，但 NW3C 的課程通常在 1 萬元新臺幣以內。(2)參加課程的同學大都是美國警察，我們可以學習美國警察第一線的經驗及工作態度。在公務及私誼建立的合作關係，也可參考及改進政府運作效能，也間接幫助未來對台灣對美國國家的外交關係。(3)課程在上課教材中會同時包括警察法律、犯罪現場實務及問題文換及討論。(4)課程安排有很大比例是外聘專家，課程有系統及有效果。這類課程的教學模式也值得台灣政府學習及實踐。

本課程在報名時，台灣司法人員需要透過 FBI 駐香港聯絡官，協助確認警察人員的身分及報名資格。NW3C 報名初審後，受訓人員要先通過網路線上的電腦常識基礎

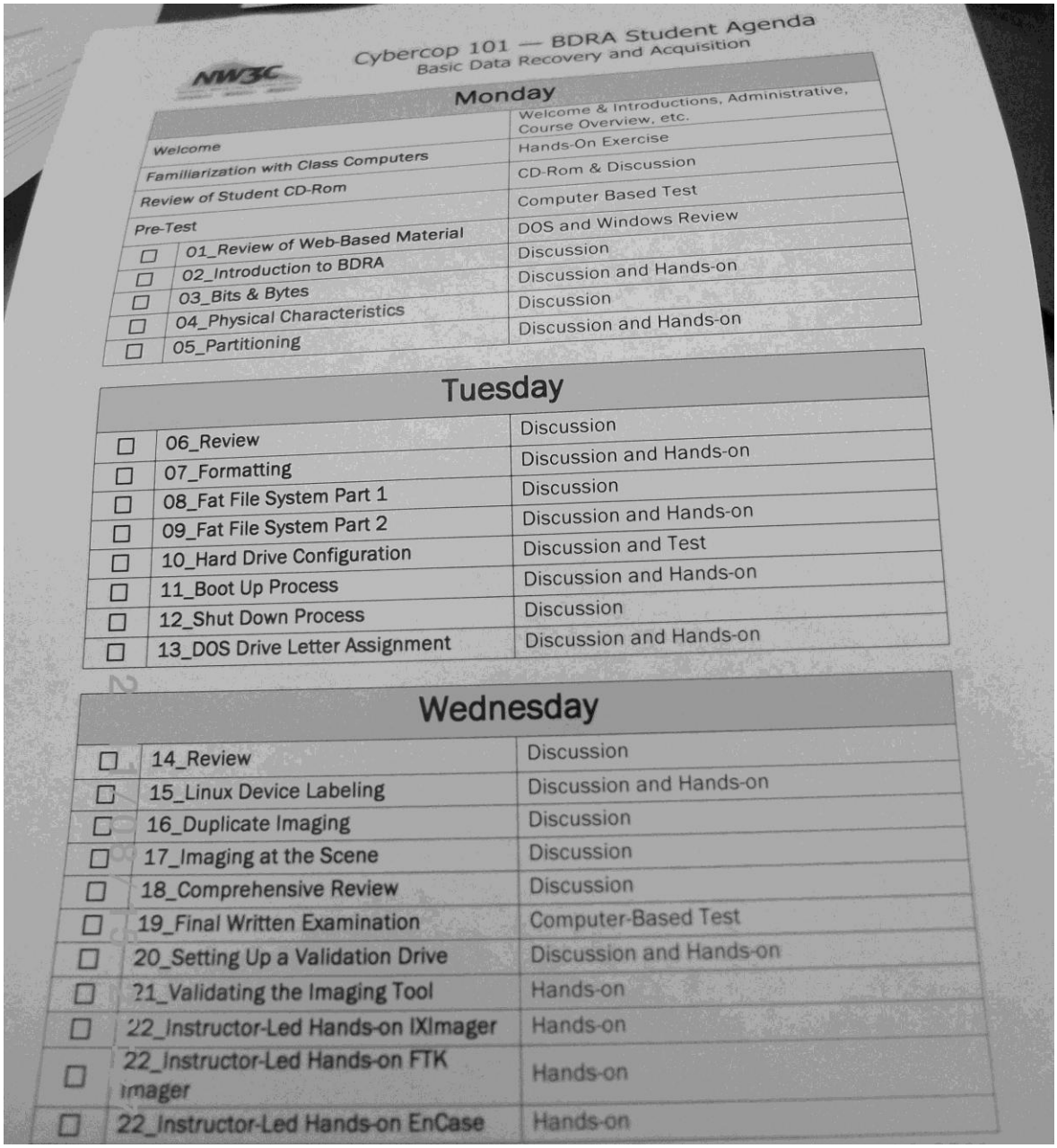
訓練,測驗題數 50 題,測驗分數在 85 分以上方可報名。上課地點在(Kent Police/Fire Training Center,24523 116th Avenue South East,Kent, WA 98031)。此次授課教師:Mel Joiner，場地接待人員爲警察局訓練中心的值班員警。上課同學大部份是西雅圖市警察局警察，包括當地的 Community Corrections Officer:Philip Ahn、Seattle Police Department Investigator:Christopher Young 等等同學，在上課期間，同學及講師都不吝嗇給予指導及協助。

（二）研討會的技術專題討論內容:

美國是一個重視司法程序的國家，警察在現場的調查及出庭作證，都需要證明採證的標準是符合司法程序。美國各行各業比台灣更早應用個人電腦在各商業領域及家庭家電，所以一般的刑事犯罪(謀殺案、洗錢、交通案件、國際販毒或違法運輸、詐欺案件等等)的偵辦過程，數位證據的分析起步比台灣早發展，美國數位證物需求不停地增加。因此，美國司法部集合司法第一線專家，撰寫手冊，發展軟體工具，增加電腦鑑識課程及訓練。

研討會在開始時，要求學員仔細注意教材手冊中，和犯罪現場紀錄有關的教材。在犯罪現場最重要做的工作是:詳實記錄電腦的使用情形、儲存媒體、其它電子證物及傳統證物。文件的記錄格式、項目、欄位、時間、人員、地點、照相都要遵守聯邦及各州的刑事司法標準程序。紀錄的程序要照司法電子證物手冊詳細地填寫。

研討會的技術專題討論: 但本課程是初階課程，進階的檔案系統分析要留在其它進階的課程，在本篇出國報告中，略爲摘要研討會課程內容各階段重點及節錄課程內容，但是詳細細節則需要參考 BDRA 課程中的手冊及講義。美國課程嚴謹，上課過程嚴格要求參課同學要完成這系列的課程，在課堂有測驗要完成外，也有專題作業要同學在接續的研討會討論及繳交。這次的作業是:模擬在犯罪現場獲得硬碟一顆，SD 記憶卡一張且 SD 卡中有一些相片檔。如果 SD 卡中有部份圖檔遺失，遺失部份的的數位相片檔要嘗試還原，同學要如何還原圖檔?這份作業是上課同學在下一堂課要完成，且同學要嘗試完成或提出解決方法的指定作業。



Cybercop 101 — BDRA Student Agenda
Basic Data Recovery and Acquisition

Monday	
Welcome	Welcome & Introductions, Administrative, Course Overview, etc.
Familiarization with Class Computers	Hands-On Exercise
Review of Student CD-Rom	CD-Rom & Discussion
Pre-Test	Computer Based Test
☐ 01_Review of Web-Based Material	DOS and Windows Review
☐ 02_Introduction to BDRA	Discussion
☐ 03_Bits & Bytes	Discussion and Hands-on
☐ 04_Physical Characteristics	Discussion
☐ 05_Partitioning	Discussion and Hands-on

Tuesday	
☐ 06_Review	Discussion
☐ 07_Formatting	Discussion and Hands-on
☐ 08_Fat File System Part 1	Discussion
☐ 09_Fat File System Part 2	Discussion and Hands-on
☐ 10_Hard Drive Configuration	Discussion and Test
☐ 11_Boot Up Process	Discussion and Hands-on
☐ 12_Shut Down Process	Discussion
☐ 13_DOS Drive Letter Assignment	Discussion and Hands-on

Wednesday	
☐ 14_Review	Discussion
☐ 15_Linux Device Labeling	Discussion and Hands-on
☐ 16_Duplicate Imaging	Discussion
☐ 17_Imaging at the Scene	Discussion
☐ 18_Comprehensive Review	Discussion
☐ 19_Final Written Examination	Computer-Based Test
☐ 20_Setting Up a Validation Drive	Discussion and Hands-on
☐ 21_Validating the Imaging Tool	Hands-on
☐ 22_Instructor-Led Hands-on IXImager	Hands-on
☐ 22_Instructor-Led Hands-on FTK Imager	Hands-on
☐ 22_Instructor-Led Hands-on EnCase	Hands-on

圖 6: 研討會在開始時，說明上課內容，要求學員注意教材手冊及有關的教材。並明考試範圍及作業題目。

1 <u>電腦鑑識課程的基本計算機軟體及硬體介紹</u>

這個階段的講義內容主要分介紹基本的計算機軟體及硬體概念,從基本的電腦計算機概論，說明電腦最基本的輸出及輸入軟體及硬體，到完整硬碟取證及分析檔案，皆有示範及演習。

認識電腦的硬體(CPU、memory、Hard disk、Input devices、Output devices、主機面板、主機背後、主機背後接線圖、主機內部、磁碟、硬碟、光碟、磁碟比較、鍵盤、滑鼠、喇叭、螢幕按鈕)。現場教師準備過去 20 年到現在的常見軟碟及硬碟、

各種數位裝置零件。課程最必要認識的是儲存數位資料的媒體，因爲這些媒體是現場蒐證最重要的關鍵證物。媒體或硬體最重要及最常見的是硬式磁碟機（Hard Disk Drive）。硬式磁碟機就是我們常聽到的硬碟，是目前使用最普遍的儲存設備，它是一種容量大、傳輸速度快的儲存裝置。第一台硬碟出現於 1956 年，是 IBM 生產，容量只有 5MB。隨著科技進步，20、40GB 早已不敷需求。目前，Hitachi、Seagate 等硬碟廠商還推出高達 2TB 的硬碟。現場實作及分析硬碟的工具是 Acronis 的 DiskEditor.

認識電腦的軟體:這個部份教授電腦軟體的概念。從電腦是二進位系統開始教導二進位系統。再來是認識最常見的軟體名詞，例如:BIOS、作業系統、及常見的應用程式，如 email 軟體、文字檔案、圖片檔案。

BIOS(Basic Input Output System):從主機機殼上的電源開始接通,到進入作業系統的期間，儲存於主機板上那顆 EEPROM（電氣可抹除暨可程式化唯讀記憶體）裡的 BIOS 程式會執行以下的工作：

Step 1. 初始化：當電腦打開，CPU 會自行重置爲初始狀態，準備運作。BIOS boot block（基本輸出輸入系統開機區塊）初始化階段啓動，因爲此時系統記憶體中是空的，沒有程式碼可以執行， CPU 去尋找系統 BIOS ROM 中的 reset vector（重置向量實體位址）：用一個固定的位置來啓動所謂的 BIOS boot program 開機程式。

Step 2. POST（Power On Self Test；開機自我檢測）：然後 BIOS 開始施行 Power-On Self Test（POST；開機自我檢測），在過程中檢查電腦各項組件及其設定，像是：CPU、主記憶體、鍵盤、滑鼠等等狀態。接著便尋找被內建在 BIOS 內部的顯示卡程序並執行。

Step 3. 記錄電腦系統的設定值：BIOS 會根據「系統資源表」，來對系統進行確認電腦系統資源或設備。電腦會逐步顯示這些被偵測到的設備。例如 BIOS 支援隨插即用，那 BIOS 會偵測和配置隨插即用裝置，並顯示偵測到的隨插即用設備。

檢測結束後，BIOS 會打出一個偵測總結表於畫面上。

Step 4.提供常駐程式：提供作業系統或應用程式呼叫的中斷向量，如 INT 10h（VGA 圖形及文字輸出中斷）等。

Step 5. 載入作業系統：到這裡是系統檢測的部分，接下來 BIOS 便開始尋找開機裝置，使用者可以透過在 BIOS 的設定來決定搜尋順序，目前常見的開機設備至少包含 FDD、HDD 以及光碟機和 USB 開機裝置等多項。找到開機裝置後，BIOS 將會搜尋開機訊息以進行作業系統的開機過程。如果是找到了一個硬碟，它將會尋找位在硬碟第 0 面，第 0 軌，第 1 磁區裡的 Master Boot Record（主要開機磁區）。如果它找到的是 FDD，也會讀取軟碟的第 1 磁區。再把讀取到的資料放在記憶體 0x7C00h 的位置，跳到那裡並且執行它。自此才開始進入 OS 啓動階段。

Step 6:關閉程序(Shutdown Process): 教師說明關閉程序對儲存資料可能產生的影響。在正常的採證，我們會不關機，先將電腦的資料作檢查，因此時有可能可以直接獲得儲存在電腦上的暫存密碼。但是，如果警察在現場，感覺有刪除重要資料的程式正在進行，則以抽出電源線爲優先。在下列幾種控制狀況下，警察現場蒐證過程，應拍攝 Screen 相片、PC 系統佈線接頭及現場環境後，關閉電腦系統。而教師也說明，

在現場如果剛好犯罪嫌疑人正在刪除檔案，則現場人員應強制將電腦電源中斷。這可保全未被刪除的檔案，也有可能可以留下部份的帳號及密碼在虛擬記憶體(virtual memory)上。

例:(1).安裝新軟體或變更現有軟體的配置之後。(2).存在硬體問題時。(3).系統死當時。(4).系統效能降低時。(5).檔案系統可能毀損時。

Formatting 及實作硬碟切割磁區(partition): 這個章節目的是讓學員熟悉(1)FDISK 及 FORMAT 指令。(2)比較不同的 fat(file system) 。(3)解釋 clusters。(4)比較 FAT16 FAT32。 在這個章節，教師指導 FAT 檔案系統的觀念及如何讀取檔案。DOS、Windows 95 都使用 FAT16 檔案系統，Windows 98/NT/2000/XP 等系統均支援 FAT16 檔案系統。它最大只能管理 2GB 的分割磁區，每個分割磁區，最多只能有 65,525 個叢集(Cluster，是磁碟空間的配置單位)。隨著硬碟或分割容量的增大，每個叢集所占的空間將越來越大，從而導致硬碟空間的浪費。隨著大容量硬碟的出現，從 Windows 98 開始，FAT32 開始流行，它是 FAT16 的增強版本，可用在容量爲 512MB 到 2TB（2,048GB）的硬碟上。FAT32 使用的叢集比 FAT16 小，從而有效節約硬碟空間。基於 FAT32 的 Win 2000 可以支援分割最大爲 32GB，而基於 FAT16 的 Win 2000 支援的分割最大爲 4GB。 這個章節，教師示範用硬碟工具去讀取 FAT 檔案系統的重要 entries 及檔案系統和 cluster 上的資料或檔案配置。

2 學習作業系統和檔案系統，分析犯罪者(部份的)硬碟資料

要學習作業系統和檔案系統的原因是，分析犯罪者(部份的)硬碟資料。警察可能只能找到現場已經被刪除檔案的硬碟，部份殘留的資訊。例如下圖，說明檔案即使被刪除，因爲只有刪除根目錄的 block/cluster 紀錄，但 block/cluster 檔案資料內容仍留在磁碟上，可以還原局部資料。

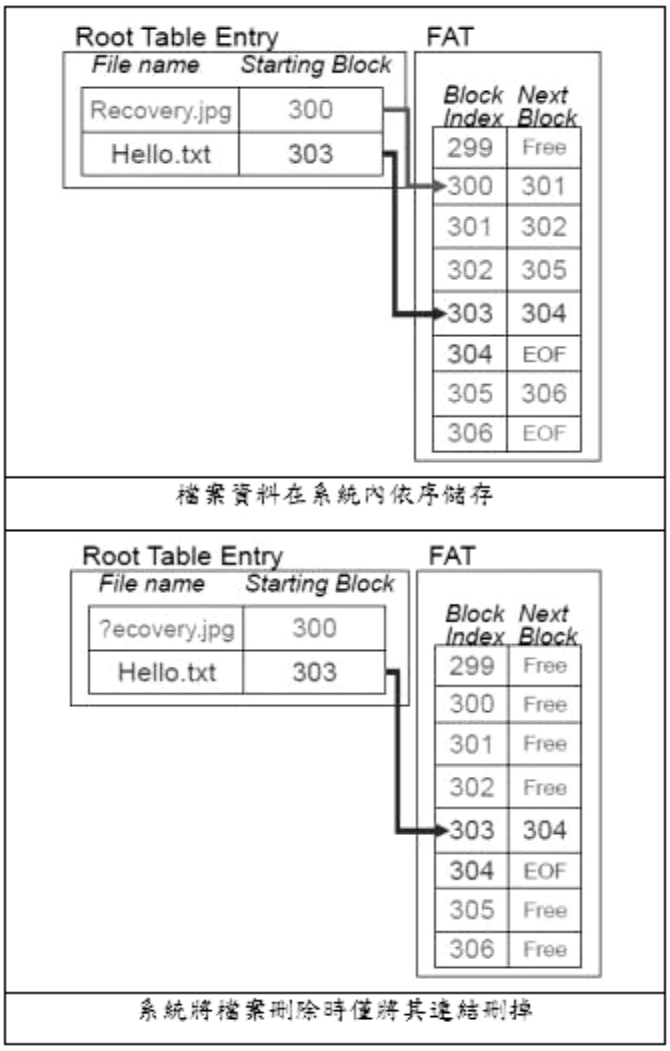


圖 7:警察可能利用作業系統和檔案系統的原理，找到部份的犯罪者留下的硬碟資料。即使檔案已經被刪除的，部份殘留的資訊仍可能被發現。

3 電腦鑑識的司法人員標準程序

電腦鑑識的課程在警察偵辦犯罪的過程，除了是必要的技能外，更重要的是，在講求證據的法庭中，警察在司法取證及法庭證據過程，可以列舉曾經受過的專業課程，證明警察是符合司法要求資格及重視證據的司法警察人員。電腦鑑識的基本觀念及操作方式:警察人員在現場，需從電源線及電腦裝置佈線、伺服器設置、現場是否有犯罪共犯可能從遠端控製本機設備，電腦是否有裝置類似自動重開機後，自動清除硬碟資料的安全軟體(部份犯罪者有習慣設置此種軟體，讓)、RAID 設備要注意磁碟機的安裝次序，在現場就依裝置位置次序貼標籤。這些都要列清單逐一檢查。如果在現場發現犯罪人正在清除檔案，可以直接去除電腦線，並停止現場 UBS 不中斷供電系統。指導教師在上課的講義，開宗明義指出，電腦鑑識必須完整包括: (1) 蒐集程序 (Collection). (2) 分析程序(Analysis). (3) 鑑定程序(Forensics) (4) 報告階段(Report)。說明如下:

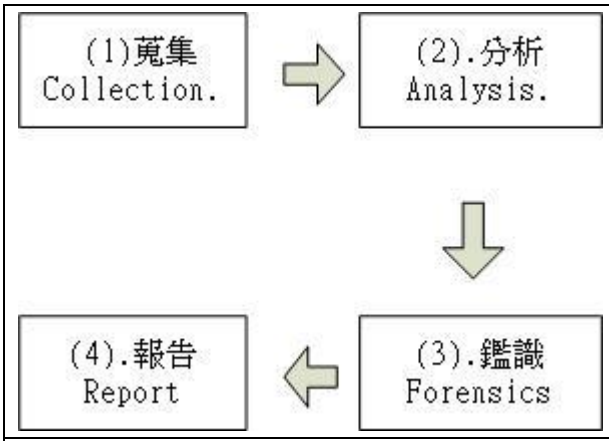


圖 8:電腦鑑識必須完整包括:(1) 蒐集程序 (Collection). (2) 分析程序 (Analysis). (3) 鑑定程序(Forensics) (4) 報告階段(Report)

(1)蒐集程序(Collection): 判斷數位資料的類型(硬體及軟體環境)，並選擇適當的工具來加以蒐集。美國司法部有針對電腦鑑識的需求，特別採購及開發標準 Liunx 作業系統環境的蒐集工具，以 Linux 作業系統高相容各種檔案系統的特性，蒐集數位檔案。警察人員在這個階段也必須準備必要的司法文書，諸如:搜索令、自願搜索書、同意書。

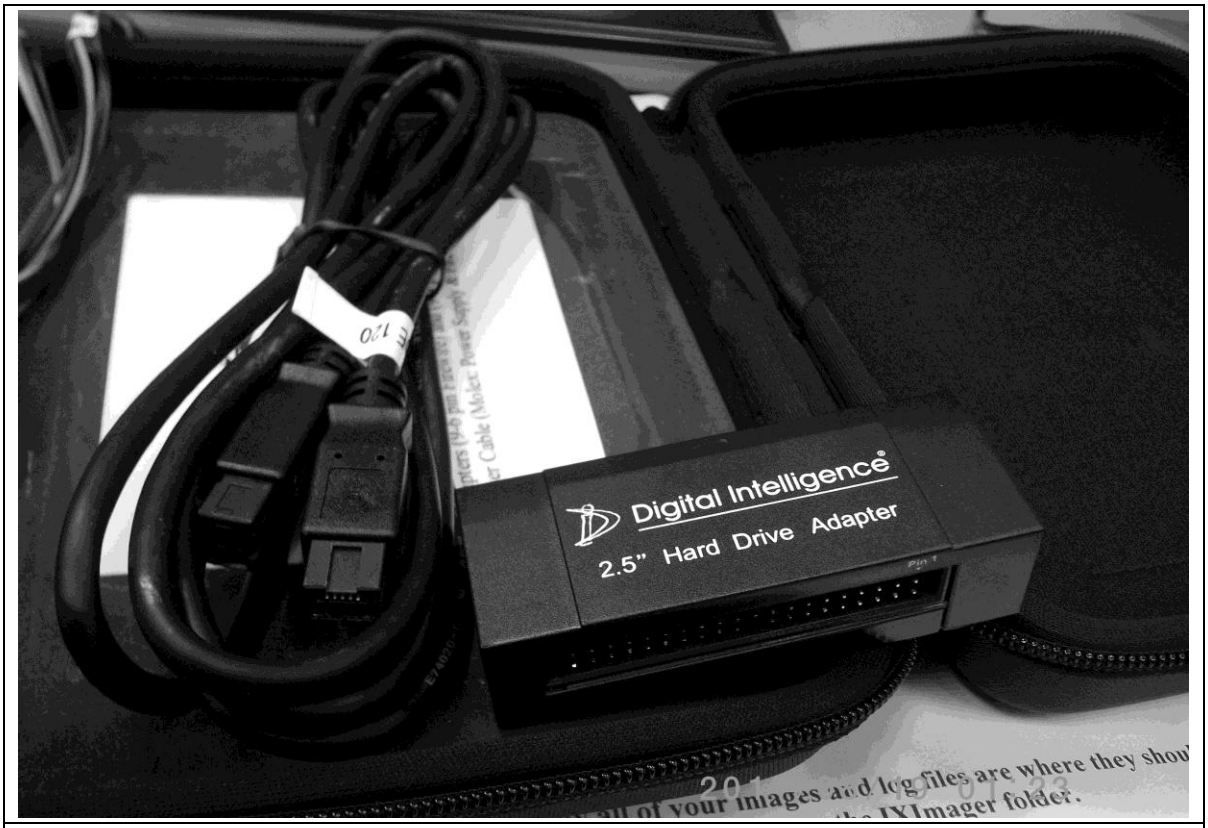


圖 9 及圖 10:學員在平時，應注意及判斷數位資料（硬體及軟體環境）的可能需要處理的情境，平時熟悉適當的工具來完成數位資料蒐集需求。

(2)分析程序(Analysis): 需要分析的資料類型可分爲一般檔案、(系統)記錄/稽核檔、各種日誌(系統日誌、事件日誌和安全日誌)、惡意程式碼……等等。透過警察人員對案情的分析和了解，找和案情相關係的關鍵字，以這個關鍵字爲過濾檔案的條件，將相關案件的檔案找出來。其它重點包括:準備復原或還原資料(部份犯罪人的電腦資料可能被刪除或損毀)，現場人員也要觀看犯罪人的電子郵件和電腦網路使用紀錄，並文字記錄看到的螢幕畫面。獲取電腦硬碟上儲存的資料，諸如:電腦控制設定、準備照相紀錄過程、準備 MD5 hashing tools. 因爲在這個程序的過程需要各種數位鑑識軟體及硬體，警員應平時就有研究或學習準備，警察單位平時應準備好這些數位鑑識軟體及硬體，在第一案發現場的警察才能有條理進行四道鑑識步驟，執行有效反應及偵查。

(3) 鑑定程序(Forensics):資料萃取、比對及個化、重建犯罪現場。數位證據的定義通常包括:1.email.2.文字檔，如 word 檔。3.影像檔及影片檔。4.excel 試算表。 數位證據通常儲存在任何可以儲存數位資料的裝置，所以警察人員應在到現場前先準備必要的常用工具，包括各種接頭介面及線材，如 CD/DVD、USB 隨身碟、硬碟、遠端硬碟。這次課程的重點集中數位資料的讀取(acquisition)。課程的目的是讓學生習慣用 FTK 的操作，快速有效蒐集必要的資訊，並完成一份標準的紀錄文件，文件紀錄一顆硬碟有那些分割磁區，用何種工具，製作 image

映像檔案，完成 MD5 hashing 值，重要的案件相關搜索關鍵字及有那些可疑檔案等等。

4 天的課程結束前，會有測驗，通過測驗後，員警會獲得 NW3C 給予上課證明，未來警察在司法程序中可以證明採證是由有足夠訓練的員警，用符合司法標準採證的方式去做採證及證物分析。

圖 11：員警完成研討會及通過測驗後，NW3C 給予警察上課證明。警察在司法程序中可以證明案件採證是用符合司法標準採證的方式去執行採證及證物分析。

在採證的過程，了解電腦計算機概論是很重要的，包括:電腦檔案的組成原理、檔案系統的格式及原理、硬碟的實體定址及邏輯定址原理等等。硬碟的實體定址是由 CHS(Cylinder、Header、Sector)所定位，資料也是儲存在其中。而因爲硬碟的實體架構關係，犯罪者也可能利用這個空間計算和電腦檔案系統的配置，作爲隱藏檔案資料的配置。也因爲電腦硬碟的原理，是最基本及可被套用分析流程到其它的數位硬體裝置。課程內容包括硬碟磁碟分割。使用 FDISK 分割工具，實作的硬碟分割。教師示範如何隱藏磁碟作業區及設立 active 主要啓動分割區。在分割的過程，教師示範硬碟的容量要如何計算(CHS 單位的計算)。硬碟在啓動的過程，會讀取 master partition table(MPT)，判斷開機程式碼及開機磁區。教師示範 MPT 上的各欄位意義及計算方式。利用 MPT 欄位，犯罪者可以有效有技巧地隱藏磁碟作業區。爲了完整找出電腦上的檔案或某個字串，教師示範如何用最基本的 Disk Editor 去讀取指定 CHS 或 cluster 實體位址的檔案內容。

數位資料分爲變動性數位資料(記憶體)、固定性數位資料(硬碟)及檔案系統數位資料。針對現場正在執行的變動性數位資料，通常正在執行，表示最近電腦使用者的登入軟體帳號及密碼可能剛鍵入電腦記憶體中，犯罪嫌疑人正在編輯台完成編輯或瀏覽的檔案資料。如果這些資料是重要的資訊線索或證據，則在現場應嘗試將資料 dump 到警方的硬碟中。

(4) 報告階段(Report)：提供法院審判需要的相關。警察準備必要的紀錄報告，報告敍明如何執行電腦鑑識。列印發現的犯罪資訊。將必要的電腦檔案妥善保存及備份。這個步驟很重要。因爲目前台灣對數位證物的重視程度不高，部份證物在上訴時，法庭發現證物可能已經因未妥善保失而滅失。

4 美國現在正在使用的 FTK

這次電腦課程實習過程，作業系統的模擬以 DOS、Windows 98、windows 2000、Windows XP 爲模擬環境。嘗試讀取 FAT16 及 FAT32 檔案系統的檔案。使用的軟體工具有美國聯邦調查局開發的 Linux 可開機光碟標準工具及 Encase 等二種 FTK。Encase 相當於結合了磁碟檢視、編輯、字串搜尋工具與檔案檢視工具。目前台灣警察開始導入 Encase 工具，這個工具目前台灣和美國的作業是同步，但是美國重視司法報告的標準流程及教育訓練，或者說警察人員行政流程的標準化作業，符合司法規範及現場作業時效。這個部份台灣政府應學習及加強。在犯罪現場執行蒐證及偵查案件線索的警察人員如果是在有時效限制的環境下，則必須要將整顆硬碟都作影像檔。在需要進階檔案回復或分析電腦作業系統刪除的檔案，但要還原留存的局部數位資料時，則要立即找尋專業單位支援。

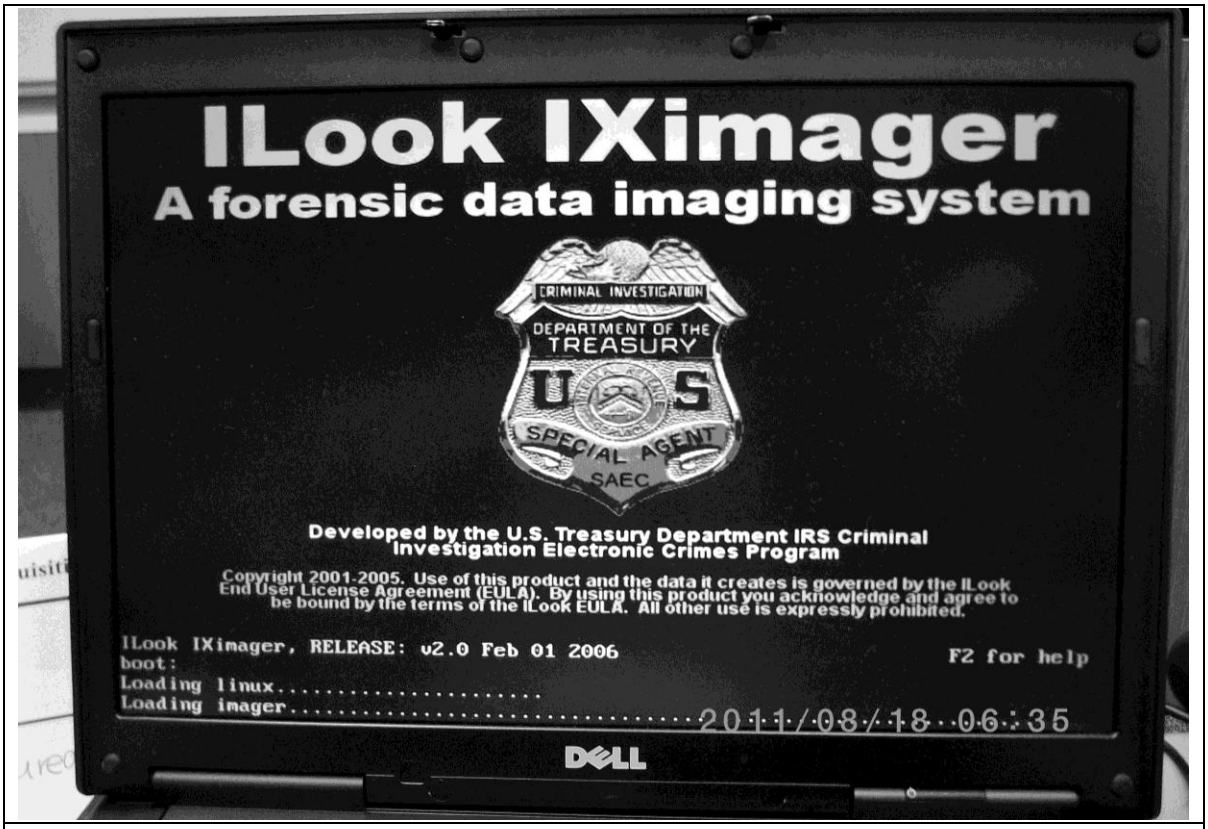


圖 12: 美國司法單位使用的電腦鑑識軟體。可用為製作標準刑事司法報告及列印發現的犯罪資訊。在妥善保存數位證物及電腦檔案備份，以為未來法庭呈現。

此行看到美國警察的敬業和團隊合作精神，是最讓我印象深刻。因爲美國警察即使下班時間，例如休假，如果有重要支援或現場作業，需要人手支援，被請求支援的人員，仍會熱心給予幫助。這在人民犯罪過程可能因法律允許合法保管及使用槍械，犯罪現場會有槍戰的國家，警察人員要冒生命危險才能完成任務。公務人員能如此敬業，真是值得學習。

圖 13:參訪的美國警察訓練中心，正在演習臨檢支援，前來支援的員警是便衣警察，模擬團隊合作、心戰喊話及攔截拒停車輛。

另外課程有介紹 Microsoft Computer Online Forensic Evidence Extractor 微軟電腦線上法務證據提取器 簡稱 COFFEE. 微軟於 2008 開發的司法取證工具,免費給與國際警察相關刑警組織及 National White Collar Crime Center (NW3C) 使用

http://www.megaleecher.net/taxonomy/term/8322 (其它相關參考 http://www.microsoft.com/industry/government/solutions/cofee/default.aspx).美國政府知道資訊證據的分析及資訊科技進步是不會停下腳步，只會越來越快。所以此類課程不停強調，要求學員主動學習及準備各種軟體工具，熟悉電子證物的取證。美國政府能運用專業授課的單位，協調軟體廠商給予司法第一線警察價格便宜或不需費用的軟體，值得我國政府學習，用公部門協調軟體大廠，請軟體廠商給予支援或優惠價格的軟體工具。

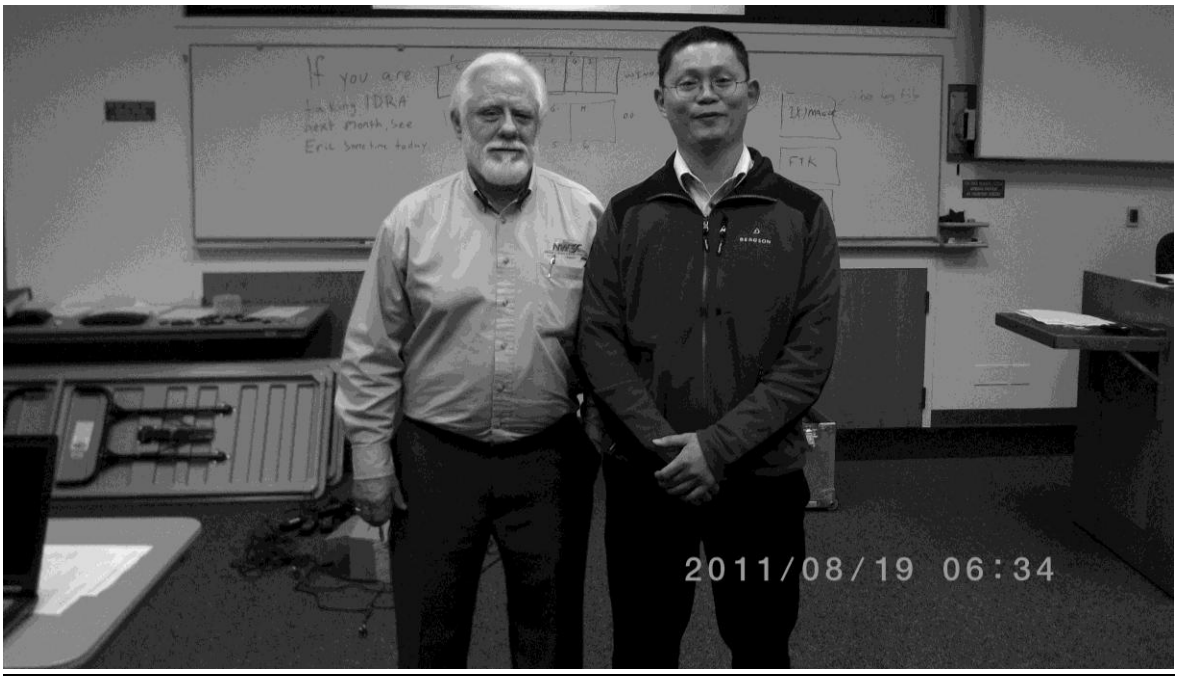


圖 14:NW3C 的專業教師提供第一線的實務經驗及電腦鑑識軟體工具。

5 其它重要參考資料

(1)電腦鑑識實務操作及訓練講義內容:

這一次的上課課程是以實務操作及訓練爲主,此章節詳細敍明所見所聞的軟體及工作操作重點。電腦鑑識除了必要的軟體工具外，重要的是員警平常有 重視電子證物處理的決心，員警能接受數位科技的進步會越來越快，如筆記電腦及手機不停進步，包括軟體的功能也日新又新、平時準備及熟悉相關電子媒體的操作方法、儲存硬體規格、檔案系統的操作。電腦鑑識軟體工具可以粗分爲(1)數位證據搜尋方法及工具。(2) 數位證據採集工具。(3)數位證據分析工具。

(2)電腦鑑識軟體工具:

I. 數位證據搜尋方法及工具

A. 電腦軟硬體規格參考手冊:採集數位證物必須平時有準備及研讀相關電子儲存媒體的手冊和規格書，如硬碟規格手冊、檔案系統手冊、加密軟體手冊及操作。平時員警應利用公餘閒暇時間熟悉這些不停進步更新及修正的規格手冊內容，準備現場連接電腦硬體的連接電源線材、資料匯流排線材、USB轉接頭、光碟片格式及支援機器等等。電腦伺服器的網路線連接及無線網路的連接中斷及LOG備份。

B. 犯罪工具程式參考手冊:部份軟體是被利用爲犯罪的常用軟體工具。警察在佈線偵查及現場蒐證時，必須要記錄軟體的組態及連線，分析程式的LOG，

列表可能的使用者(犯罪的幫助犯)，被遠端連線的裝置或伺服器(重要犯罪工具或證據)。

C. 破解電腦密碼工具:在現場第一時間訊問犯罪嫌犯可能的帳號及密碼是最應該優先做的事情。如果犯罪嫌犯不願意透露密碼，再採用其它可能破解密碼的方法。在此次訓練中，針對訊問犯罪人的密碼，手冊有如下建議:在現場要確認電腦的帳號。確認犯罪人電腦網路的使用習慣和網路信箱或網路軟體的帳號。犯罪人的電腦密碼、全部電腦中安裝的軟體及電腦安全軟體加密及解密的帳號、最近的即時通訊帳號及帳號登入後的朋友名單。MySpace、Facebook等通訊服務的帳號。最常見的關鍵檔案是:聊天室、最近編輯的文字檔、遠端硬碟(雲端硬碟)、兒童色情圖檔、匯款電子檔、加密的檔案、可能的人頭帳戶、境外匯款、親屬帳戶、支票、禮券、償還債務、(無存單)定存、銀樓、地下匯款公司、買賣高價值商品(包括珠寶、古董、名畫等)相關紙本或數位檔案或交易檔案紀錄。

D. 磁碟資料檢視工具:部份檔案可能被刻意加密及修改切割磁區.所以全部的磁碟切割磁區,要在用fdisk磁碟工具,去檢查是否有作業系統讀取不到的切割磁區。如果作業系統讀取不到分割磁區，則有可能未發覺的重要犯罪相關電子檔案。

E. 掃描追蹤工具:觀察電腦server 提供那些遠端連線服務。

II. 數位證據採集工具

A. 回復被刪除資料之工具:有時侯，檔案雖被刪除，仍然可以嘗試還原。如Recuva。

B. 資料檢視及媒體讀取工具:Acronis的DiskEditor(支援 IDE、SCSI、USB、IEEE 1394 介面的硬碟，並可以以十六進位文字模式簡式硬碟分割區內容.)這種工具的特點是可以用sector/byte 爲單位，去讀取硬碟(MBR、開機磁區 volume boot records, 檔案系統及目錄檔案) 。

C. 備份儲存工具:有效的備份及切割磁區完整映像檔案。 爲了要能保證完全未改變證物，並以原犯罪人所用的媒體情況下進行分析，在進行數位鑑識時，就要考量是否能就磁碟資料進行備份再進行分析。警察在平時應準備空白的儲存媒體，在現場時能有效備份犯罪現場的電腦硬碟或相關數位儲存媒體。一個軟體要成爲可靠的案例複本製作工具至少要符合美國國家科技標準局（NIST)的要求:(A)這工具要能建立字元串流複本(Bit-Stream Duplicate）或者在原始固定或可移動的磁碟、磁區上建立映象檔案（Image)。而所謂映象檔案，係指用將磁碟實體分割磁區內容(CHS)及相關資訊存成一個檔案，即映像檔。(B）不能修改到原始磁碟。即該程式不可對原始證據媒體做出任何改變。(C)這工具應能檢驗資料映像檔的完整性。(D)這工具應能記錄I/O錯誤。也就是說，該程式對於讀取錯誤必須要有一套解決方法，假如行程不斷地對某一個受損的磁區發出讀取錯誤,那麼此時就該注意此磁區將被忽略以及必須在輸出流需要放置一個同等大小的預備磁區。(E）工具的記錄文件

應正確。

D. 證明檔案的採集及分析是有效MD5工具:主要是具有md5 checksum的計算能力。 用以證明檔案的採集及分析是有效，具未異動原始數位檔案。這個工具的功能必須和司法報告文書的紀錄欄位一致。爲了符合刑事程序法要求的證物標準，要能證明偵查並未改變數位檔案證據，故需要使用證明工具軟體，例如MD5、SHA-1。(md5的詳細說明請參考 http://en.wikipedia.org/wiki/Md5sum)。進行數位鑑識時，如何配合現場環境，實施拍照(有效還原及模擬第一現場設備運作情形)，快速與有效的進行檢驗也是很重要的一個條件，尤其在第一線場的警察，在第一時間偵訊犯人時間的限制，如而刑事訴訟法第93條第二項規定24小時內聲請羈押(*檢警共用24小時*)。因此，警察在現場的分析及採證需考量時間的限制，使用MD5運算的速度卻比SHA-1運算來得快及有效，因此，還是以利用MD5爲檔案**證明工具軟體能幫助節省警察作業時間**。另外利用數位鑑識還原的電腦檔案，在第一時間確定參與犯罪的人犯、各人犯犯罪的程度、犯罪所得、犯罪是否爲常業犯罪、犯罪手段是否重大罪惡、犯罪證據用以爲24小時內的偵查證據、防止串證、滅證、僞證等等。在科技進步的同時，警察司法人員也必須學習及交流數位鑑識的技巧。採證過程才能有效提高證據可信度。警察面對不停進步的軟硬體設備更新，才能有效及省時地辦案。

III. 數位證據分析工具:警察部門專業單位負責這些工具的採購及例行教育訓練。因爲這些軟體工具可能每年都有更新的版本。而市面作業系統，例如 winXP、Vista、Win7 可以說是每年都會有更新，檔案系統的改進也不停止。

A. 修復硬碟毀損或檔案實體磁區部份遺失或殘留資料之工具。

B. 破解加密檔案工具。

C. 檢驗磁區資料之工具。

肆、參觀Kent Police Station Training Center

一、 Kent Police Station Training Center

本次參訪行程包括參觀Kent Police Training Center。這個訓練中心在美國911事件發生後，也成爲一個警察訓練反恐的訓練中心，業務包括:指導警察的消防救生、警察反恐突擊訓練、警察網路犯罪及電腦訓練、警察街頭巡邏訓練。訓練中心是附屬在Kent 市警察局，硬體建築有區分爲(1)消防大樓、(2)電腦訓練及視聽室、(3)模擬消防現場及警員演習訓練的大樓、(4)供警車模擬臨檢盤查的平面廣場。在參觀這個訓練中心的硬體設備過程，可以發現部份美國警察使用的設備較台灣先進，例如警械及警槍及警用電腦系統。警員可以購買方便個人使用的警槍，通常在開車巡邏時，車後有配備行動電腦及長步槍。

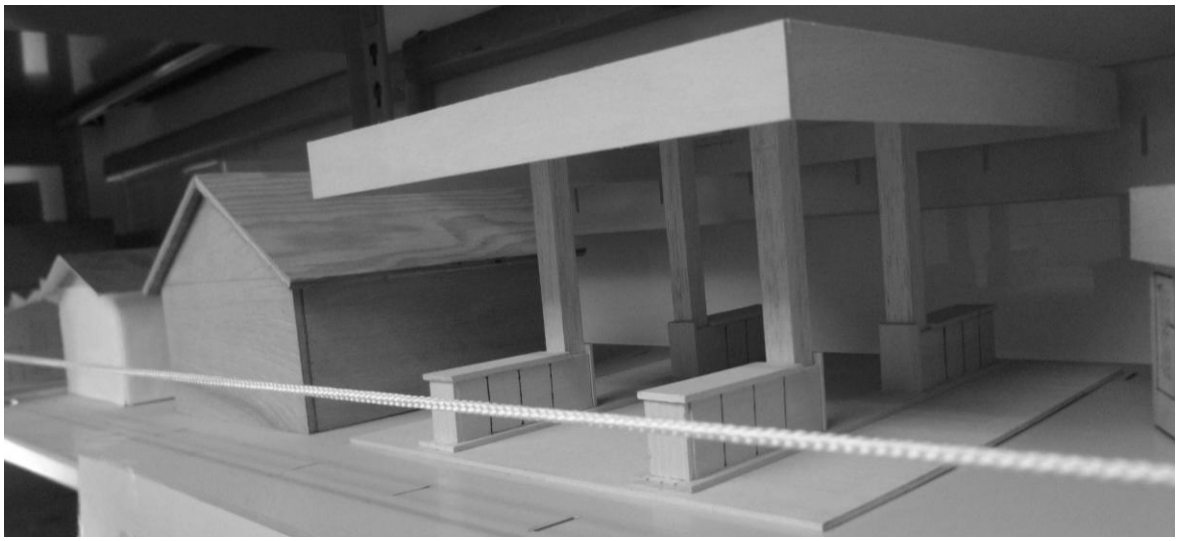


圖 15:參訪的美國警察訓練中心,平時準備各種建築及交通工具模型,準備沙盤推演。
圖 16:美國警察汽車中備有數位電腦及攝影器材。

在台灣,警察的業務大概可以區分爲行政協助及司法犯罪偵查。美國警察除了行政協助及司法犯罪偵查之外,在政府刑事司法體系扮演重要的角色(協助犯罪矯正,包括緩刑及假釋)。例如當任社區的 Probation officer,可協助裁定重案但服完部份刑責的犯罪者,在申請假釋後,Probation officer 會限制居住自由及行動自由。例如:定期到 Probation officer 警局報到,報告現在的職業及居住所。Probation officer 警察如果覺得重案假釋者的平時行爲可疑,可以要求假釋者居住的窗戶平時要打開,不得加裝窗簾。Probation officer 警察可有有不需搜索令狀,即時搜索的權力。

另外 Kent 警察的訓練制度及警民合作也值得台灣參考。美國因爲國家廣大,所以重視地方自治。警察的重點工作之一是協助及結合社區自我經營及管理。例如:每年的警察常訓課程,均外聘專家及專業機構來講習,講習過程約爲三天,通常是由員警和自身業務相關,上課的員警需配合上課時間約爲 1 天到 4 天。另外,美國警察在招募人員時,也仔細挑選警察從業人員的背景和素質。以 Kent 市爲例,它推擴對警察業務有興趣或未來想從警的民眾,符合年紀在 14 到 21 歲及未曾犯過刑事罪及符合身家調查條件後,可以接受警察訓練。受訓後,可以支援(及體驗)警察的例行業務(無危險性質的例行業務),例如:消防、家庭暴力、交通法規相關公文書、交通指揮、警用無限電設備訓練、警察司法文書撰寫及其它例行性警察業務。此外,美國警察招募社區人員,協助 part-time 的社區巡守。巡守的範圍除了社區的安全巡護外,也包括清除塗鴉。

美國是一個移民友善及開放的國家,包括開放部份課程給國際參訪學生或人員,如此行的學費是由美國當地機構贊助,未收學費。美國司法及警察的行政協助業務的

部份，最明顯的是針對大量的移民，警察在提供服務給民眾時，會給予各種語言的服務小冊子，市政府也用公費聘請律師給予司法協助，方便新移民。例如移民過程中，最常發現的例子是家庭暴力。如果家庭暴力的程度嚴重，則政府提供受暴力的婦女一個庇護居住安置地方。

肯特市警察局也透過各種治安宣導的聚會加強和社區民眾的溝通及協調。例如慈善活動或社區居民夜晚志願巡邏活動。

圖 17: 美國警察和社區民眾交流意見及參與各種社區活動。

伍、研習心得及建議

一、 數位證據的相關法律：

目前數位證據的保存及選任鑑定人製作鑑定報告日漸專業。數位證據通常可以區爲爲(1)電腦原儲存紀錄，例如電子郵件、word 文件等等。這種檔案是將人類思想轉爲電磁紀錄。其它類似性質且常見的數位證據包括:數位文書檔案、數位聲音檔案、數位影像檔案。(2)電腦產生的紀錄:這是電腦作業系統或作業程式執行過程留下的歷史軌跡檔紀錄。常見有電腦稽核紀錄、ISP 業者連線 LOG、電腦電話通聯紀錄、電腦檔案建立時間、提款機存取紀錄。應用程式日誌等等都是。(3)電腦儲存及產生性質兼具的紀錄: 同時有兩種性質的數位證據。(4)電腦程式產生的紀錄:例如 ICQ、MSN、Facebook 等在執行過程留下的對話檔案及執行紀錄。

警察人員在處理數位證據時，應注意上列四種數位證據的證據能力及未來在法庭做證時，應註記的司法報告欄位。尤其證明:(1) 數位證據未遭修改。(2) 數位證據的製作者。(3)資料的驗證及驗真。(4)數位證據的保管。要做到這四點，警察人員平時須要利用時間，把握進修及累積並傳承實務經驗。

台灣刑法的電腦犯罪部份條文(第二百二十條、第三百十五條到第三百五十二條等等) 是和電腦或其相關設備有關的電腦犯罪條文。但是更常發生的犯罪是利用電腦爲犯罪工具。對於常業使用電腦犯罪(例如:專業架設電腦設備或通信網路，幫助詐欺集團的常業犯罪者)，台灣的刑事法律有跟隨時代改進的需要，將以此爲常業犯罪者，加重其刑責。

二、 專業的鑑識能力的電腦鑑識單位

數位證據作爲物證調查時，是指利用電腦軟硬體設備播放，能聽聞或閱讀看見內容之證物。數位證據證物保管適用一般證物，在刑法出庭出示爲證據，台灣現在是由檢察官或法官，依數位證物內容特性及疑慮可疑特點，移請有公信力的政府機關或民間數位證物來源相關公司(例如:電子郵件的日期或註冊公司爲 Yahoo,法庭請 Yahoo 說明真僞或佐證證物出處真實性。)

數位證據有多種態樣，因此適當分類數位證據的態樣後，警察在現場的證物蒐集及證物分析、鑑識、報告均應符合未來法庭的呈現重點及標準。現在政府機關主要的數位鑑識有**調查局**成立的數位鑑識實驗室及**刑事警察局**的數位鑑識實驗室。目前提供的鑑定項目包括復原儲存媒體中被損毀的數位資料，例如數位檔案資料，即便資料被刪除，也可以透過各種工具進行資料復原。

現在警察機關有建立如刑事警察局數位鑑識小組的單位，主要業務除警察犯罪現場數位鑑識支援外，也支援司法機關，如法院的請求協助。此行見習心得，建議台灣政府應結合民間教育單位，試將刑案現場或民事訴訟過程的各種可能需求或標準，製成類似美國司法部所發給的標準現場電腦數位證物處理手冊。爲因應實務的需要，台

灣政府應思考，訂定那些標準及規範後，民間可以成位刑事及民事數位鑑識證物的驗證公司，結合民間的人力資源及活力，使數位證據在依一定的標準程序保存及鑑識後，能被法庭承認，加速法庭案件的透明度、公信力及審理時間。節省政府人力成本。

三、 數位鑑識及軟體

目前台灣和美國所使用或購買的軟體，廠商及功能大概相同。但美國司法部有專責部門，找相關的專家，培養類似智庫，並發展 Linux/Unix 下，相容各作業系統的鑑識軟體，並依司法部的作業手冊，製作標準的司法文書報告。

行政部門必要的教育進修，外包給專業的教育機構(如 NW3C)，有系列地教導專業課程，值得台灣推廣及學習。

陸、結語

一、政府應重視電腦鑑識的專業性及實際作業需求

政府在改進刑事訴訟程序法的過程，應參考民間電腦鑑識或資訊安全顧問公司的業務實際經驗，並建立合作管道，有標準的鑑識標準程序。如此，警察在現場的電腦鑑識作業能更有效率，未來在法庭的證據證明時，也可以節省大量人力及司法資源。

二、警察常訓過程，應外包民間專業單位，學習更專業及更系統課程

主要原因包括電腦鑑識的專業性及案件需求增加趨勢。過去是科技十倍速成長的時代，現在更是百倍速成長。分工的專業需求及符合刑事訴訟要求，政府更應投資資源在專業警察或專業政府人員的人才培育。

四、 加強建立國際合作管道，學習數位鑑識科技

與美、日、香港、大陸、新加坡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，瞭解國際電腦鑑識技術發展脈動。尤其香港、日本和新加坡應爲台灣優先選項。