出國報告（出國類別:軍售訓練）

美國防部網路犯罪中心(DC3)
網路犯罪鑑識班返國報告
International Cyber Forensics Course

服務機關：憲兵指揮部刑事鑑識中心

姓名職稱：王登翰（上尉憲兵刑事官）

派赴國家：美國/馬里蘭州

出國期間：108年7月5日至8月12日

報告日期：108年10月31日

摘要

本次受訓係奉國防部民國 108 年 6 月 26 日國人培育字第 1080010034 號令核定，赴美國國防部網路犯罪中心(Department of Defense Cyber Crime Center, DC3)所屬網路防護調查訓練學院(The Defense Cyber Investigations Training Academy, DCITA)受訓，課程名稱為網路鑑識班(International Cyber Forensics Course)，訓期民國 108 年 7 月 8 日起至 108 年 8 月 9 日止，共計 5 週；係美國國防部網路犯罪中心為國際學生首創之班隊，課程內容主要為了解電腦硬體及網路基礎概念、數位證物採集工具及採證流程、熟悉操作數位鑑識軟體(EnCase)並了解其主要功能，結合上述所學，在模擬情境中進行網路案件調查。

目次

壹、受訓目的

本次受訓班隊為國際學生網路鑑識課程，藉此次機會了解美方數位鑑識所用工具，及擁有相關技術之專業人才如何培養，培養本軍符合國際軍事規格之數位鑑識種子能量。未來將參考美方所用教材融入本中心數位鑑識組新進人員教育訓練，採納美方教材之優點使新進人員更容易吸收相關知識，並由職擔任數位鑑識種子教官，提升本中心數位鑑識品質。

貳、受訓過程

一、單位介紹

（一）美國國防部網路犯罪中心：
(Department of Defense Cyber Crime Center, DC3)

美國國防部網路犯罪中心(Department of Defense Cyber Crime Center, DC3)創立於 1998 年，總部設立於馬里蘭州林西克姆，其主要任務為提供先進的數位鑑識服務、網路技術訓練、漏洞分享以及針對美國國防部管轄任務範圍（網路安全、重要基礎建設及公家機關防護、反恐行動）實施網路分析。

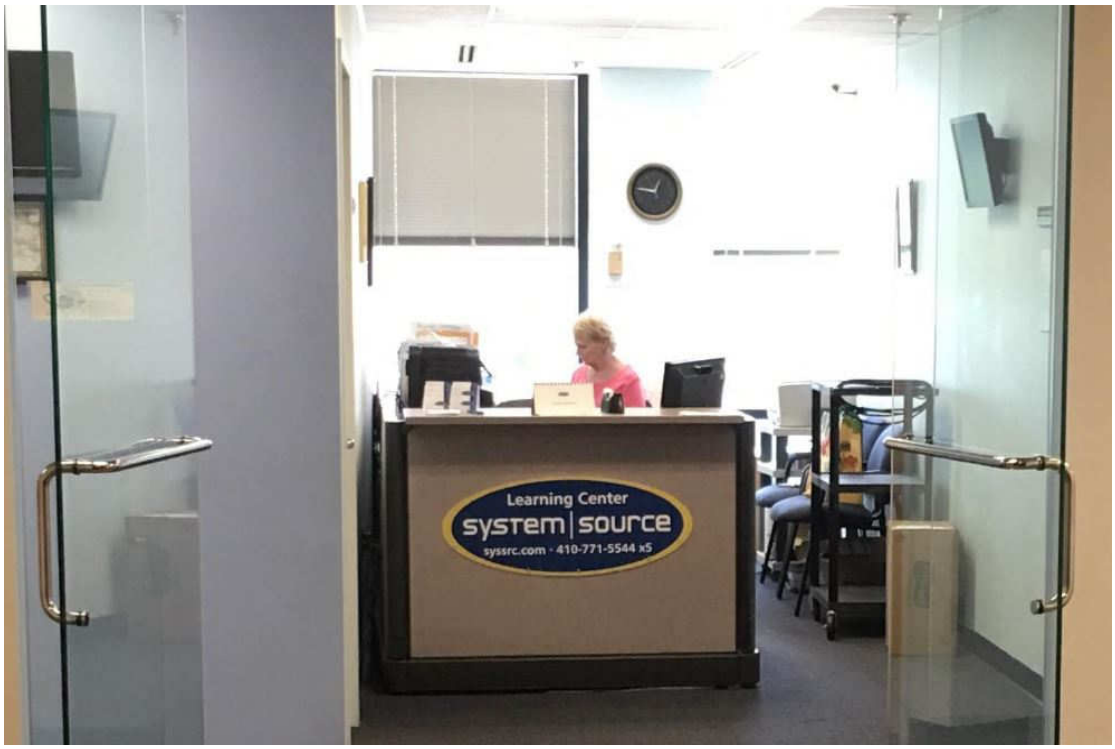
（二）網路防護調查訓練學院：
(The Defense Cyber Investigations Training Academy, DCITA)

網路防護調查訓練學院(The Defense Cyber Investigations Training Academy, DCITA)為 DC3 專門負責培育網路技術人才的教育機構，教學目的主要為保護國防資訊系統不受犯罪、詐欺、國外情蒐等未經授權行動之侵擾。學院針對不同領域皆有專門的課程，1998 年至今已有超過 35,000 名學生接受訓練。

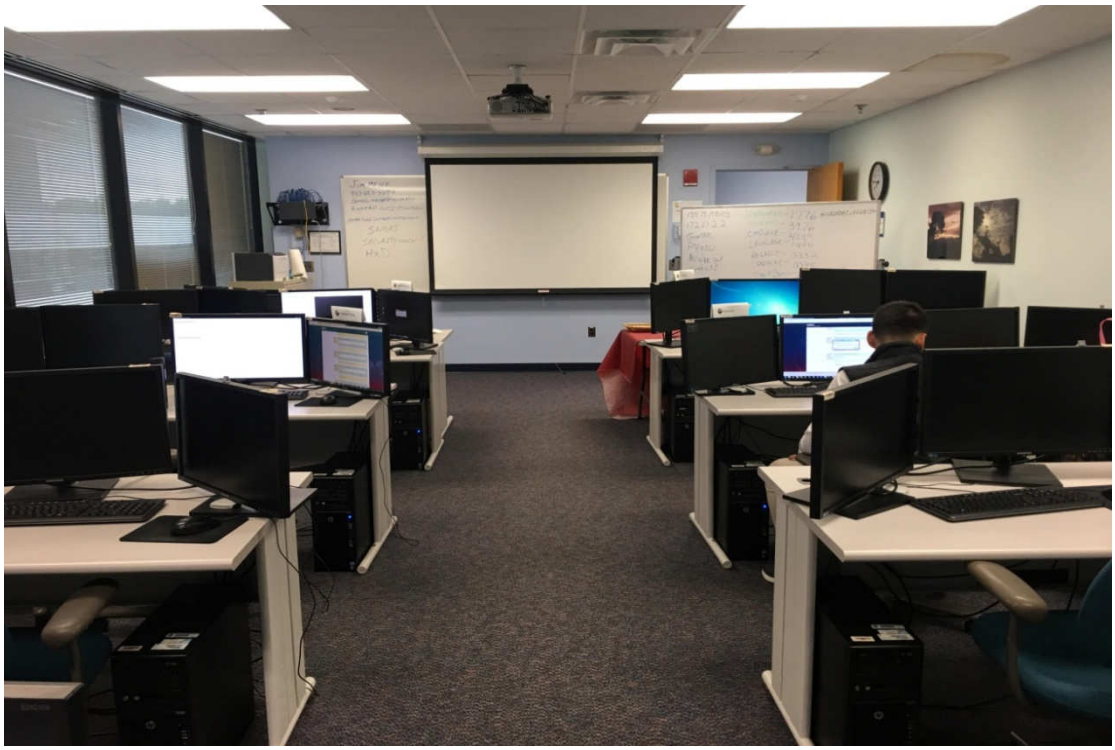
DCITA 提供美國各軍種及聯邦政府機關教育訓練。訓練課程分級實施，從最基礎的介紹網路及電腦硬體到進階的實務網路案件調查皆有相關課程。DCITA 提供 20 種以上不同的現場課程，其中部分課程以直播方式供外地的學生一同參與。DCITA 也提供線上課程，可以讓學生遠端進入虛擬的鑑識工作站，在安全的沙箱環境中對各種鑑識方法實施練習。由 DCITA 的教官研究及設計相關課程，他們也會在各種網路安全會議中（包含美國國防部網路犯罪會議）正式發表研究結果。

本次受訓地點位於馬里蘭州哥倫比亞距離 DC3 總部約 20 公里與外包廠商合作名為 System Source 的教學點，原教學點位於 DC3 總部，近期因內部空間使用調整而將教學點外移，教學點位

置未來規畫尚未確定，在美國德州也有設立教學點。約有 5-6 個不同班隊在此教學點授課，各班隊訓期長度不盡相同，人數均為 10 員以下的小班制。

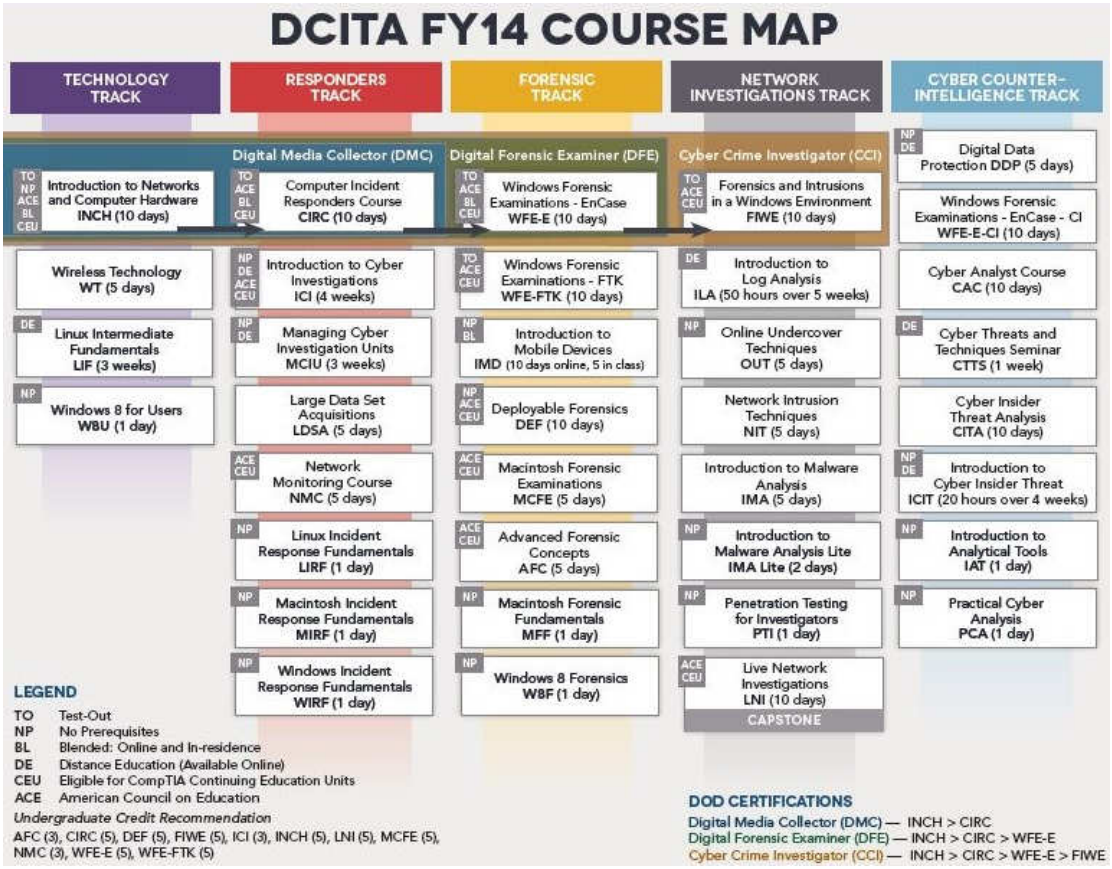


教學點 System Source 櫃台



上課教室（每人兩台電腦分別為 Win7、Win10 作業系統，每台電腦配 2 個螢幕）

二、課程介紹



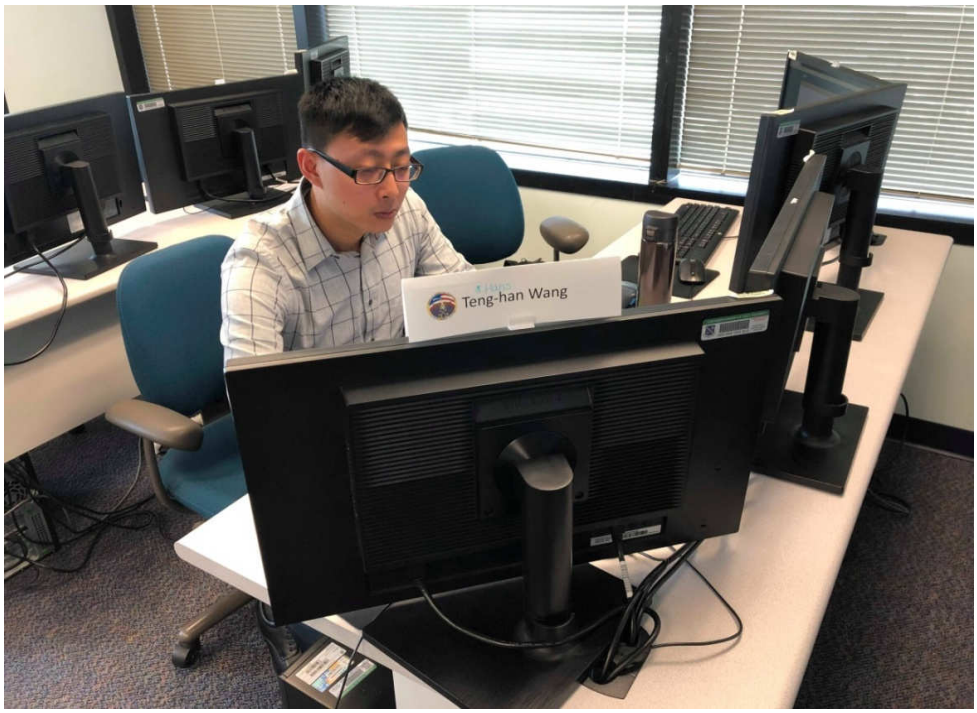
上圖為 DCITA 沿用 2014 年的課程表，概略分為五大領域，分別為科技知識、電腦事件應處、數位鑑識、網路事件調查、網路反情蒐。

（一）網路與電腦硬體介紹：

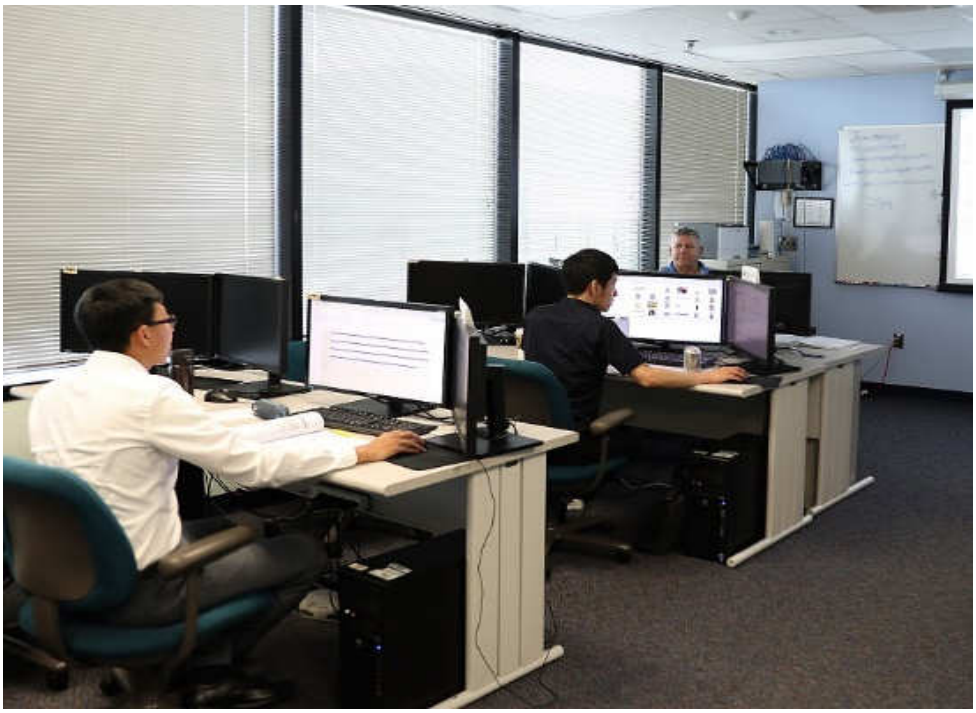
(Introduction to Network and Computer Hardware, INCH)

網路與電腦硬體介紹課程為期一週，教官藉由此課程了解學員對於電腦及網路的熟悉程度，透過此基礎課程為後續的課程紮根。課程內容主要分為四部份：

1. 電腦硬體：安全規定介紹、電腦基本系統、主機板組成元件、中央處理器及記憶體功能、匯流排種類、輸出輸入裝置、電腦故障排除。
2. 資料儲存元件：傳統硬碟元件、硬碟運作原理、固態硬碟、硬碟抹除、硬碟控制器、磁碟陣列。
3. 微軟作業系統：介紹微軟作業系統、指令介面、基本指令、檔案系統、電腦工作管理員、網路和共用中心、微軟伺服器。
4. 網路基本概論：網路模型、傳輸媒體、網路拓撲、乙太網路、網路層協定、傳輸層協定、應用層協定、網路種類、網路安全。



上課實況 1



上課實況 2

DCITA 主任至教學點了解學員學習狀況-1

DCITA 主任至教學點了解學員學習狀況-2

（二）網路事件應處課程：

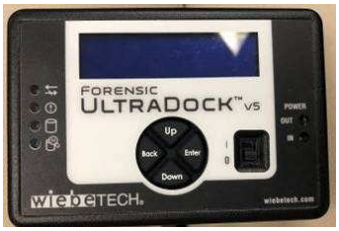
(Cyber Incident Response Course, CIRC)

網路事件應處課程為期一週，主要介紹犯罪事件發生後應處的準備工作，從接獲案件、評估案件所應攜帶的相關工具、案發現場調查應注意事項、蒐集證物流程、調查結束後應注意事項。課程使用工具及鑑識軟體有 Cellebrite UFED(手機鑑識軟體)、FTK 及 EnCase(電腦鑑識軟體)，主要著重於蒐集證物以及記錄流程。教材部分教官準備相當充足，每位學員都有一個工具箱，其中包含證物硬碟、防螢幕保護程式鎖定裝置(Mouse Jiggler)、硬碟轉接器(Drive Adapter)、防寫盒、證物手機（Android 系統、iOS 系統）。課程內容主要分為六部份：

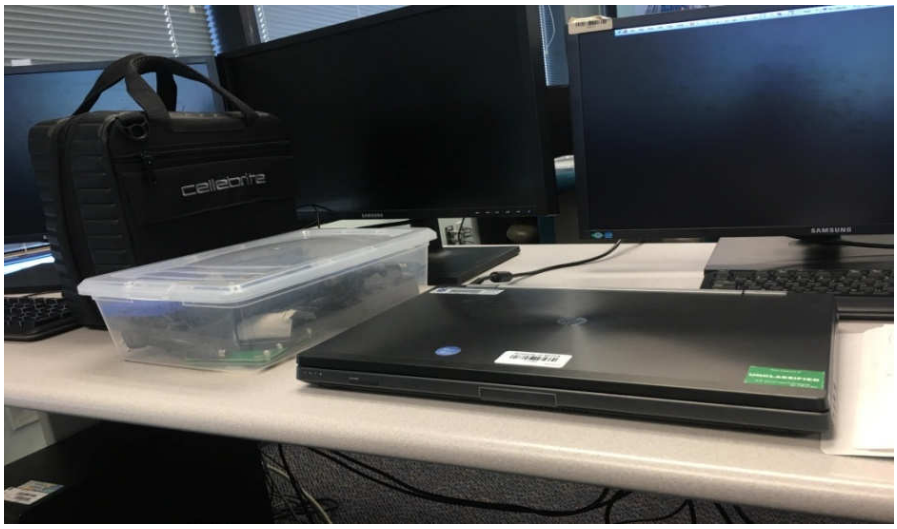
1. 事件應處：綜觀事件及準備工作、識別數位證據、蒐集資料工具。
2. 電腦評估：現場電腦評估、紀錄搜索及採證流程、作業系統加密、揮發性資料、關機程序、檢測硬體。
3. 製作數位媒體映像檔：製作映像檔原則、實作及計算雜湊值。
4. 手機及證據：處理證物手機、手機狀態評估、紀錄手機資料、取得手機密碼。
5. 取得手機資料：內建硬體及移動式儲存媒體、擷取手機資料。
6. 處理證物：證物標籤、證物保管鏈追蹤、證物包裝及運送、證物儲存。

防螢幕保護程式鎖定裝置(Mouse Jiggler)

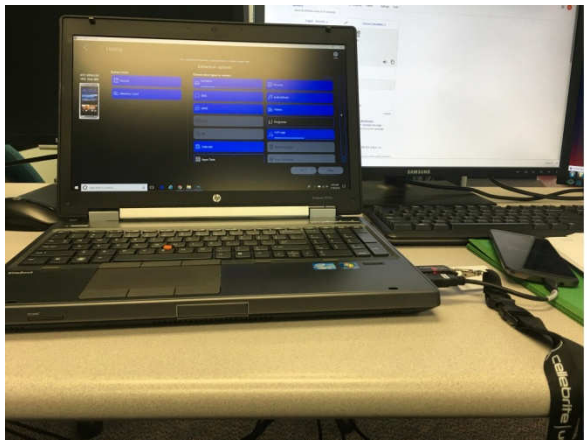
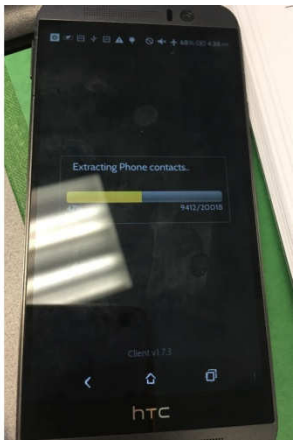
硬碟轉接器(Drive Adapter)



防寫盒



課程配備筆記型電腦、工具箱、Cellebrie UFED 線材組

使用 Cellebrite UFED 擷取手機資料

（三）EnCase 微軟作業系統數位鑑識：
(Windows Forensics Examinations-EnCase, WFE-E)

EnCase 微軟作業系統數位鑑識課程為期一週，此課程主要目標為使學員熟悉 EnCase（第 7 版）鑑識軟體操作，在微軟作業系統環境中了解其各項功能，後續課程中 EnCase 所能蒐集到的調查資料比重佔 5 成以上。由於 EnCase 功能繁多，教官僅概略傳授常用功能及重點，課程內容主要分為六部份:

1. 開始操作：設定鑑識工作站、驗證系統無病毒、鑑識工具設定。
2. 開始新案件：圖形化介面、開啟新案件、數位媒體驗證、書籤功能、使用條件及篩選功能搜尋、惡意程式掃描。
3. 證物處理：關於證物處理程序、證物處理選單物件。
4. 鑑識分析基礎：基本檔案系統、微軟作業系統、微軟紀錄檔。
5. 鑑識分析：文件簽名檔分析、雜湊值分析、關鍵字搜尋、日期搜尋、資料還原。
6. 檔案式分析：電子郵件、網頁瀏覽器、即時訊息、壓縮檔案、微軟工具、密碼還原。

（四）微軟作業系統環境入侵手法與鑑識：
(Forensics and Intrusions in a Windows Environment, FIWE)

微軟作業系統環境入侵手法與鑑識課程為期二週，此課程主要透過模擬情境使學員了解調查案件著手的方向，以及如何紀錄調查過程。教官透過假想情境公司遭可疑 IP 入侵，使用 netflow、wireshark 以及 snort 搜集網路資訊，分析駭客入侵手法，課程情境為被害電腦點擊釣魚郵件後觸發的漏洞攻擊。Volatility 為可分析記憶體映像檔之軟體，透過命令提示字元輸入指令即可產出相關資訊，包含記憶體中運行程式的 PID（程序代碼）、PPID（父程序代碼）及程式啟動時間，了解各應用程式間的相互關係。藉由 PID 又可查出所對應應用程式之網路連線狀態，並可查詢程式使用者權限。

使用 EnCase 搜尋被害電腦硬碟映像檔，設定篩選器搜尋 ADS(替代資料串流 Alternate Data Streams)內的隱藏檔案，ADS 在正常情況下可以看到的檔案中，額外附上一個以上檔案在裡面，而這些被附加的檔案不僅無法用正常的方式被看到，甚至也不會改變原始檔案的大小，因此一般的使用者是很難察覺的，容易遭有心人士利用。在 EnCase 中透過相關網站所提供惡意程式的雜

湊值來搜尋是否有變更檔案名稱來掩人耳目的惡意程式，並查詢駭客入侵時段是否有可疑的檔案建立或修改。還原微軟事件檢視紀錄檔，加以分析事件狀態，並透過特定事件編號查詢可疑檔案。將映像檔中疑似惡意程式的檔案還原至指定資料夾，並運用 Strings 指令將惡意軟體內容轉換為文字檔，以 notepad++開啟文字檔，並藉由 icyberchef 網站所提供之代碼搜尋 IP 相關資訊，透過雜湊值解析該軟體為何種惡意程式。分析過程中每個可疑的行徑都需加以記錄時間、分析結果，拼湊出事件完整的時間軸了解來龍去脈，在製作調查大綱時需提出如何防止此類事件發生的建議作為，課程內容主要分為三部份：

1. 介紹：綜觀入侵痕跡調查、如何著手案件報告。
2. 調查：搜集潛在威脅資訊、網路封包分析、記憶體鑑識、微軟系統及應用程式分析、識別惡意程式。
3. 結論：報告調查大綱、改善建議。

三、參訪行程

參訪行程於訓期第五週星期一實施，旨在結訓前接受 DC3 中心主任訪談並參觀 DC3 內部設施，了解大家學習狀況及對課程的意見。主任也對未來國際學生相關的課程提出說明，他表示本次是 DC3 第一次接待國際學生，算是一個實驗階段的課程，仍在摸索未來針對國際學生授課的方向。對於美國國內學生而言一段訓期只能接受一種課程，而國際學生遠從他國而來，須將多種課程整合在同一訓期內教授以節省學員往返次數，而該將哪幾種課程整合尚有研討的空間。

DC3 實驗室內具有 X 光機可分析證物毀損狀況，直接在屏幕上顯示異常的零件，視損壞狀況購買新硬體拆卸零件替換。科技進步日新月異，為了能處理各種案件，實驗室人員需要掌握科技的脈動，在新的科技產品上市後將其採購回實驗室進行分析，不僅針對手機、平板，讓我感到驚訝的是連電動玩具(PS4、XBOX)也成為他們鑽研的一部分，透過反覆的進行遊戲了解其記憶體在各種情況下的變化，掌握所有記憶體正常的狀態，才能查覺用於犯罪時的異常，也讓我們了解只要有心任何儲存媒體都可能成為犯罪的工具。實驗室中有少部份人員擁有將唯讀記憶體取下(Chip-Off)進行解析的技術，可用顯微鏡或 LED 液晶螢幕放大觀看實施操作。

DC3 中有 6 成以上為聘雇人員，其餘為政府人員（含軍人），平時會向民間徵才，並送到教學點受訓評量其所具備的能力是否足以勝任。各軍種的採證單位會將證物送至 DC3 實驗室分析，而 DC3 幾乎每天都會受理案件，每個案件工作天約 40-50 天，以美國國防部委任案件為主，僅受理數位鑑識相關案件，有機會收到其他政府機關委託國防部的案件

（例如 FBI）。

DC3 中心主任訪談

DC3 實驗室參觀-1

DC3 實驗室參觀-2

DC3 主任頒發紀念幣

DCITA 主任頒發結訓證書

全員合影

參、受訓心得

出國前就對美國教育文化與我國差異甚大時有耳聞，此次受訓學員僅有我國及日本各兩名學員，美方教官在了解我們資訊知識相關背景後，以適合我們的方式來教授課程內容。教官時常提醒我們若有不懂的地方請不客氣的打斷，也會放慢說話的速度好讓我們理解，更常要求我們提出問題，甚至鼓勵在下課後如果有問題也可以傳 email 給教官，並在隔天上課時間講解說明。然而教官們似乎也意識到文化的差異一時半刻很難調整，助教在教官講課時，也會適時針對當地用語提出說明。由課程安排也可看出教育著重循序漸進、由淺入深以及互動式教學，相較我國及日本的單向教學更容易了解學員學習狀況。教官也善於使用生動活潑的例子來講解較難以理解的資訊知識，專業的課程中也不乏學員們的歡笑聲。

美方教育系統相當完善，硬體方面每人配有兩台主機分別為 Win7 及 Win10 作業系統，每台主機各搭配雙螢幕，在操作繁複的調查作業同時需要操作軟體並記錄時，可發揮相當大的助益；軟體方面更令我感到印象深刻，DCITA 為課程設計專門的教學系統，由教官權限帳號來控制學生所能在網頁上看到的內容，依課程進度實施開放，其中提供學生下載課程相關電子檔、隨堂練習、每週課後測驗……等等。與隨堂練習及每週課後測驗相結合的虛擬系統讓我們熟悉如何操作課程內所提到的功能，將題目的答案藏在虛擬系統中，透過上一題答案的線索再尋找下一題的答案，環環相扣的問題與答案不僅能讓我們複習所學，更產生了尋寶遊戲般的趣味，就如同調查案件般搜集散落的證據拼湊出完整的真相。

有鑑於本軍同時具語言專長及資訊背景人員並不在多數，職規劃將美方教材翻譯成中文，並納入本中心數位鑑識組新進人員教育訓練之教案，培育未來數位鑑識種子能量，甚至將相關知識推展至基層憲兵隊，有效利用受訓資源。

肆、其他建議事項

職為本中心數位鑑識組新進人員，而此課程正好適用於鑑識基礎入門，但未來希望能提供更深入的課程，例如本軍欠缺戰場鑑識、前線蒐證、反鑑識等相關知識及實務經驗。科技是柄兩面刃，由於手機的普及化以及不斷推陳出新，手機安全性越來越高的情況下將成為爾後鑑識的一大挑戰，若在手機鑑識方面能參與更深入的課程必定有很大的助益。

經過此次訓練也深刻體認培育專業人才十分不容易，應留在相關技術單位發揮最大效用，在美國也看到實驗室的人員長年鑽研數位鑑識技術，且廣招人才，建議減少專業技術人員調動以累積鑑識能量。