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：憲兵第 205 指揮部
姓名職稱：石家翰（中尉通信官）
派赴國家：美國/馬里蘭州
出國期間：109 年 2 月 21 日至 3 月 29 日
報告日期：109 年 4 月 28 日

摘要

本次受訓係奉國防部民國 109 年 2 月 13 日國人培育字第 1090028483 號令核定，赴美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，課程名稱為國際網路鑑識班(International Cyber Forensics Course)，訓期自民國 109 年 2 月 24 日起至 3 月 27 日止，共計 5 週；係美國防部網路犯罪中心為國際學生創立之班隊，課程內容從基礎的電腦硬體及網路基礎概念介紹開始，接著說明刑案現場數位證物之採集工具及採證流程，並熟悉操作數位鑑識軟體(EnCase)及網路封包分析軟體(Wireshark)，最終結合上述所學，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，藉由此次受訓機會，瞭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，培養本部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部鑑識人員及通資作業人員教育訓練，採納美方教材之優點使新進人員更容易吸收相關知識，並由職協助撰擬數位鑑識相關教材，提升本部數位鑑識品質。

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，其主要任務為提供優質的數位鑑識服務、網路技術訓練、網路漏洞分享、技術解決方案開發，並針對美國國防部任務範圍之網路安全(cybersecurity)、關鍵基礎建設防護(critical infrastructure protection)、執法及反情報(law enforcement and counterintelligence)及反恐行動(counterterrorism)實施網路分析。

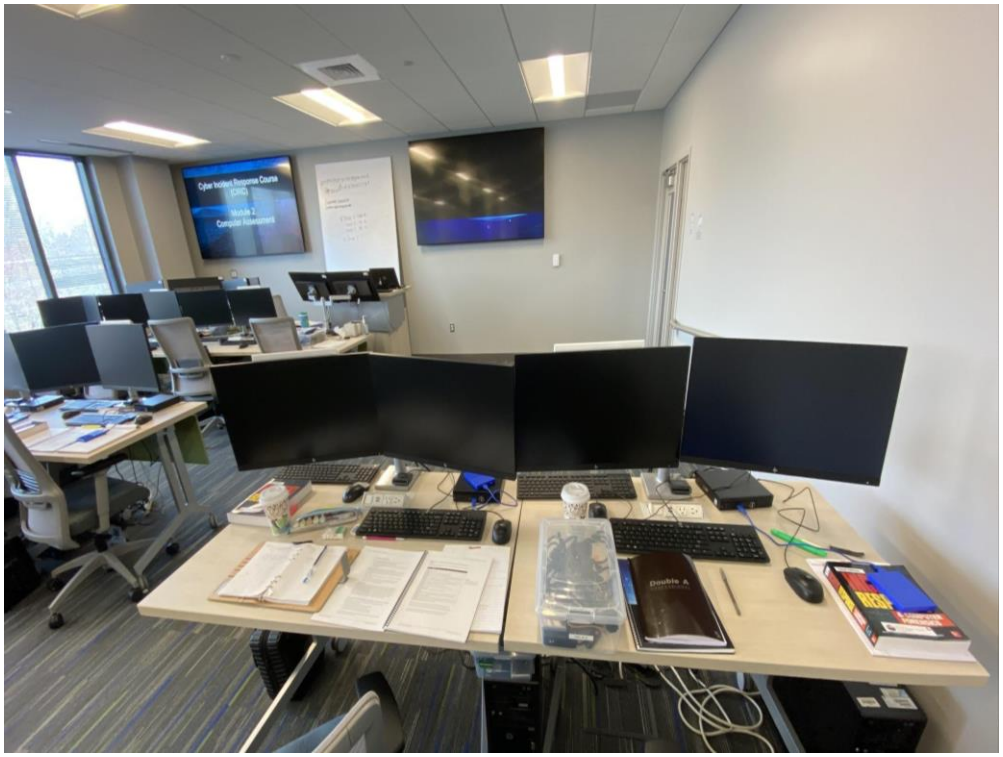
（二）網路防護調查訓練學院：
(The Defense Cyber Investigations Training Academy, DCITA)

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，致力於為美國國防部各軍種人員開發及提供網路方面的培訓及教育，並提供有關科技、網路工具、鑑識和情報類別等 15 種以上專業課程。DCITA 的使命是為個人和國防部提供網路鑑識調查培訓，並確保國防資訊系統不會受到未經授權的情報蒐集，以及犯罪和欺詐活動的侵害。

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。

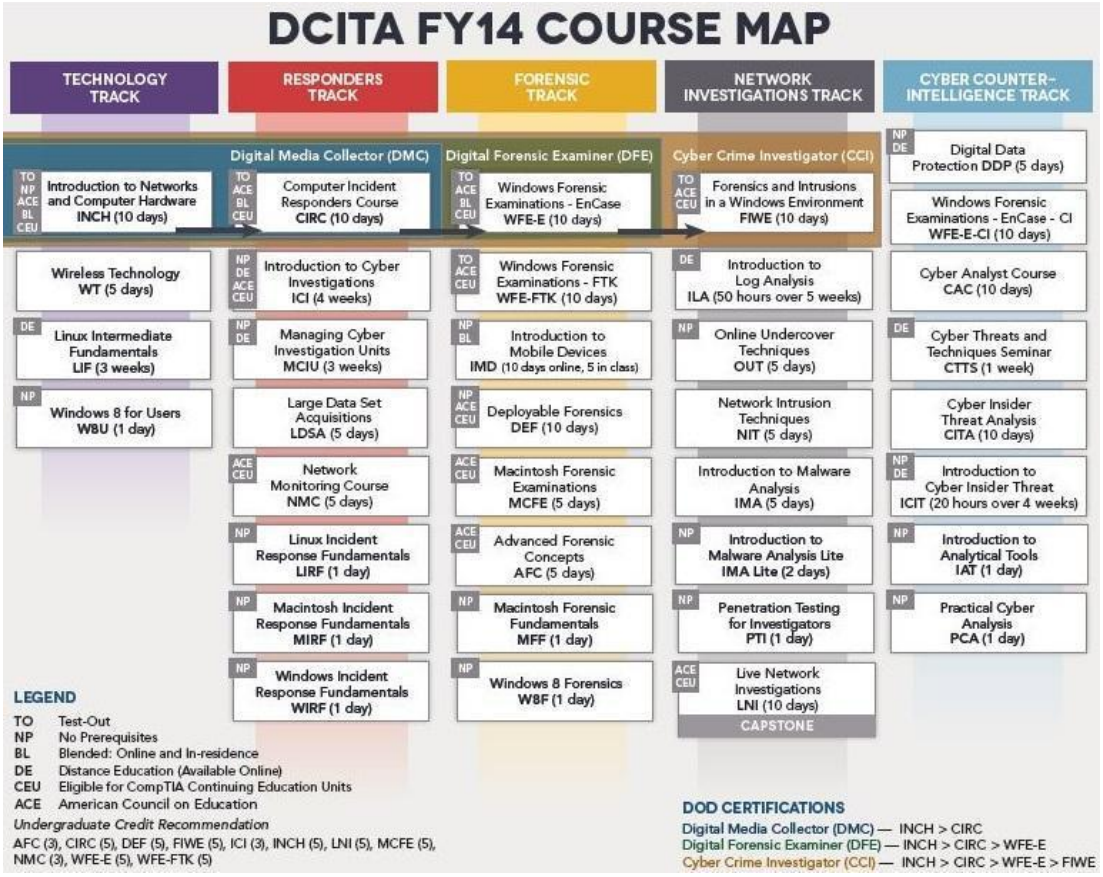
本次受訓地點位於馬里蘭州漢諾威，在巴爾的摩市西南方 15 英里左右，位於 KeyW 建築物內。同時最多有 3-4 個不同班隊在此授課，各班隊訓期長度不盡相同，人數均為 10 員以下的小班制，最後三週因應疫情關係，僅剩國際班隊現地授課，其餘班隊均取消或改為線上授課。

KeyW 建築物外觀



教室環境

二、課程介紹



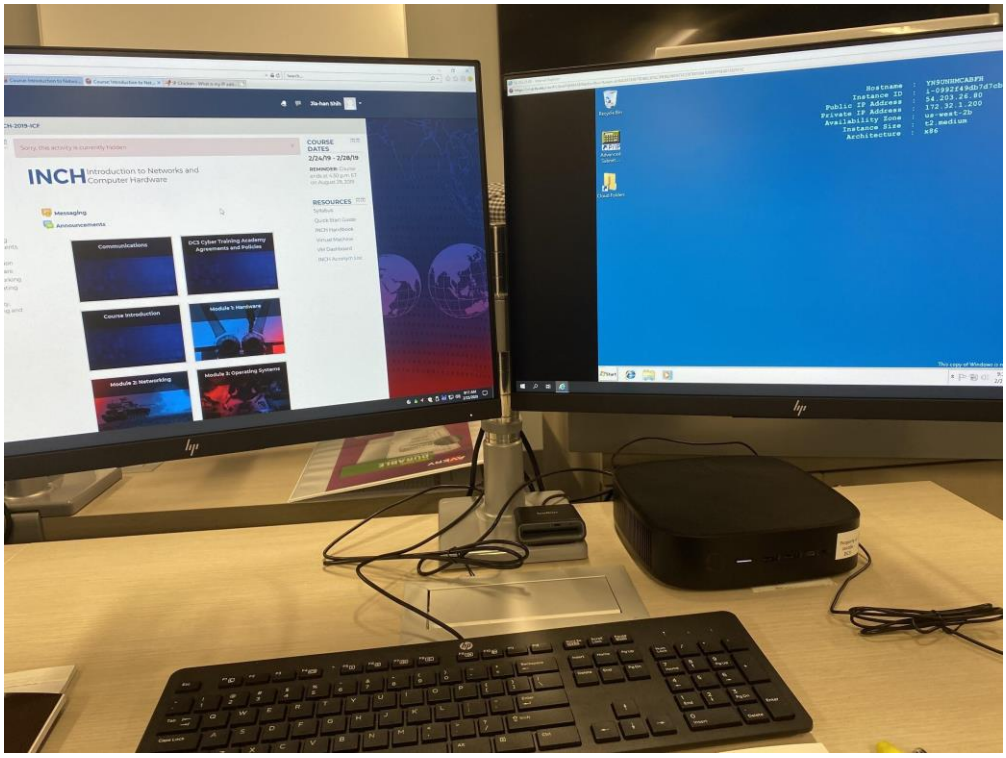
上圖為 DCITA 沿用 2014 年的課程表，概略分為五大領域，分別為科技知識、電腦事件應處、數位鑑識、網路事件調查、網路反情蒐。

（一）網路與電腦硬體介紹：

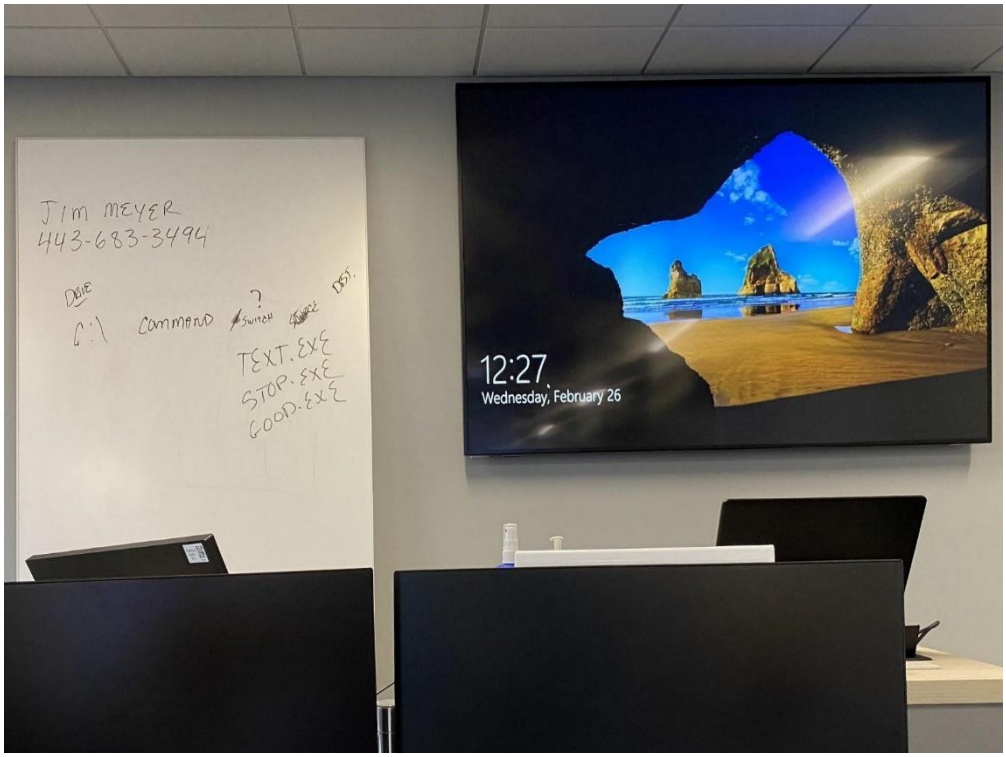
(Introduction to Network and Computer Hardware, INCH)

網路與電腦硬體介紹課程為期一週，教官藉由此課程瞭解學員對於電腦及網路的基本架構熟悉程度，透過此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、主機板組成元件及功能、中央處理器、基本輸入輸出系統、記憶體、匯流排種類、輸出輸入裝置、開關機設定。
2. 網際網路概論：網路基本模型、傳輸協定、網路拓墣、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、防火牆。
3. 微軟作業系統：介紹微軟作業系統、磁碟分割、硬碟運作原理、基本指令、檔案系統、資料結構、硬碟抹除、硬碟控制器、磁碟陣列。
4. 安全與故障排除：常見故障排除（主機板、記憶體、中央處理器、電源供應）、安全模式、安全性設定、加密模式、檔案及資料夾共用。



學員所使用的教學系統（左）及虛擬機器（右）

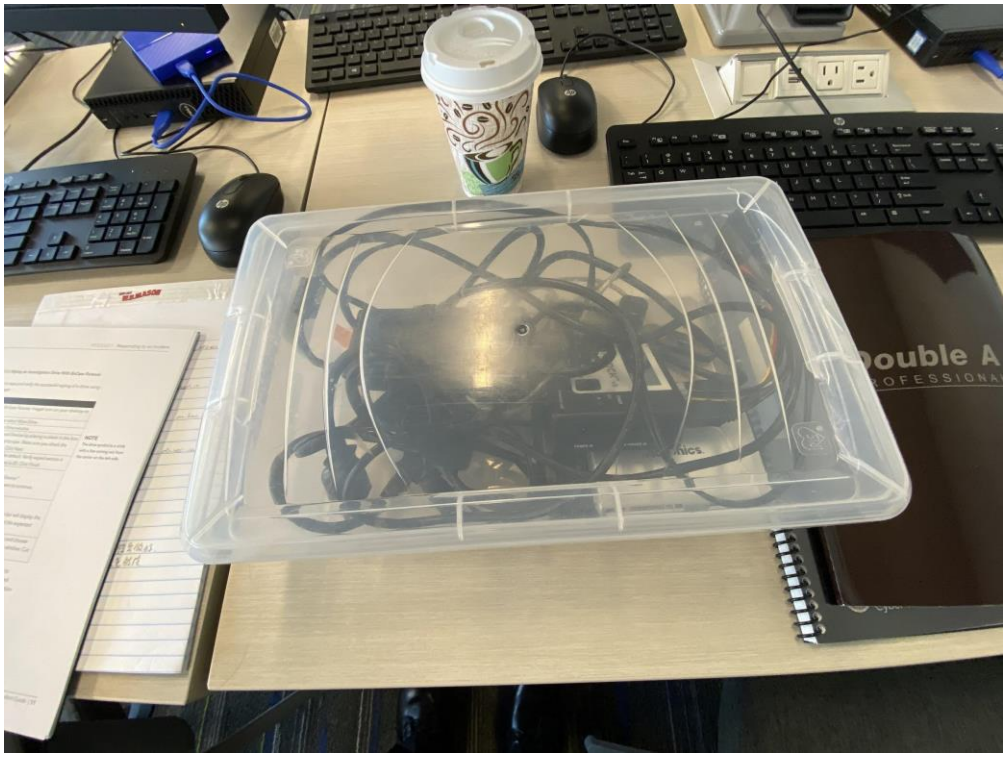


教官所使用的大型電腦螢幕及白板

（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，主要介紹刑案事件發生前的準備工作及應處作為，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)、防寫裝置、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：事件分析、事前準備工作、蒐證工具準備、證物鏈及紀錄、識別數位證據。
2. 電腦評估：現場電腦評估、資料刪除及格式化、電腦執行程序、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。



課程配備工具箱

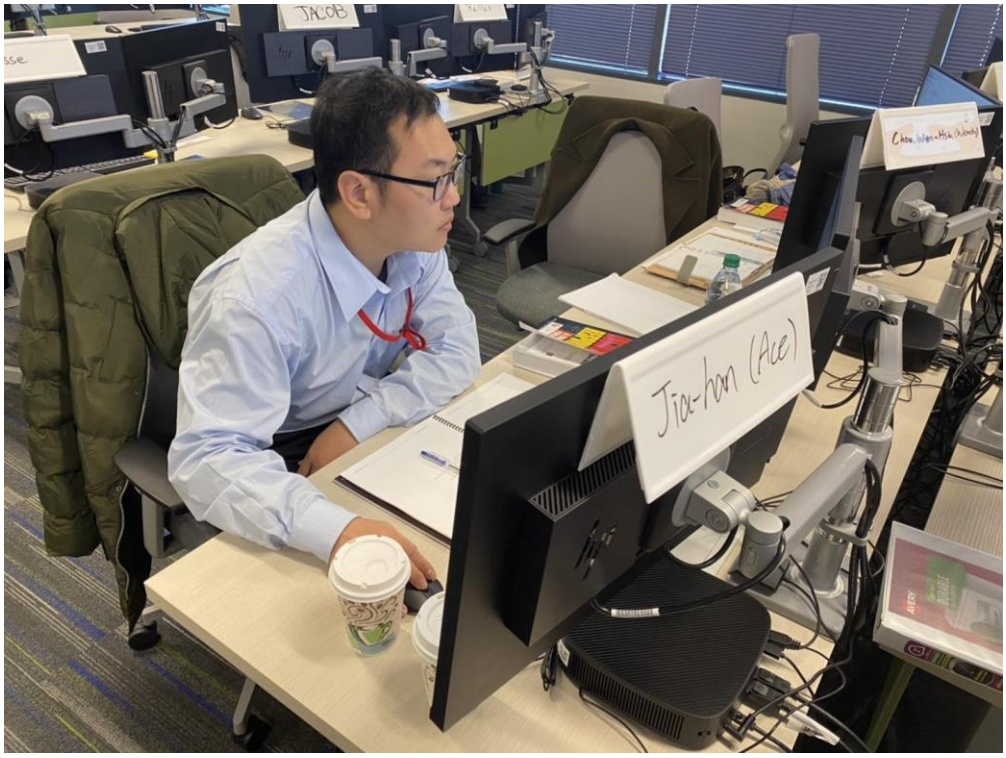
防螢幕保護程式鎖定裝置(Mouse Jiggler)

硬碟防寫盒

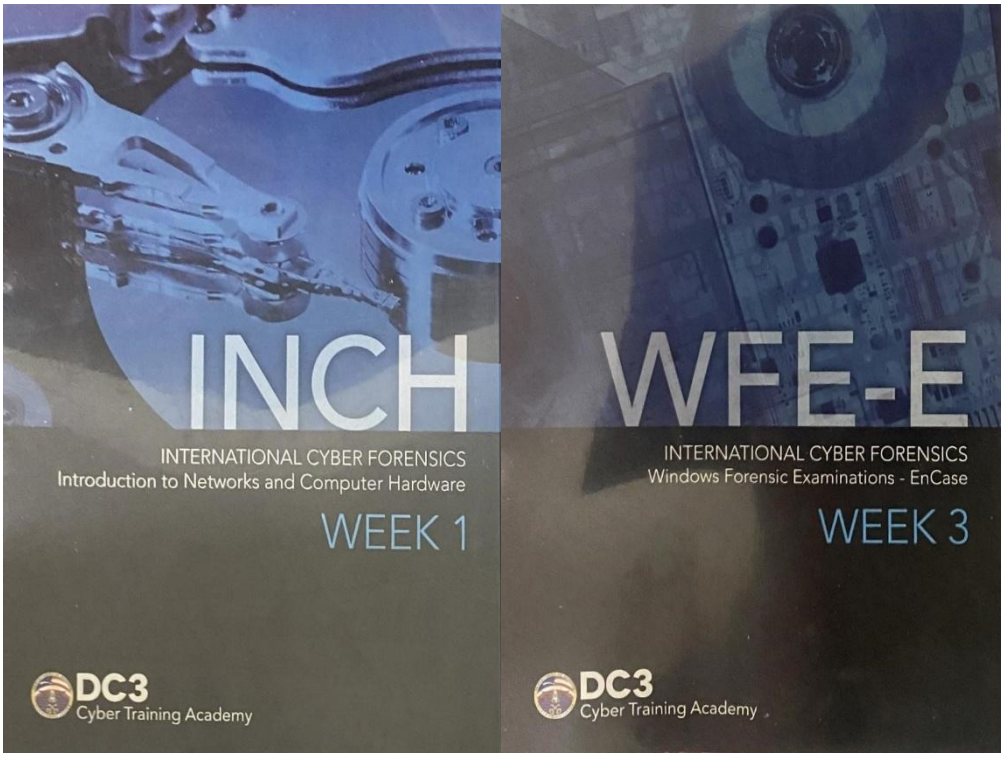
（三）EnCase 微軟作業系統數位鑑識：
(Windows Forensics Examinations-EnCase, WFE-E)

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 鑑識軟體操作，在微軟作業系統環境中瞭解其各項功能，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、驗證系統無毒環境、鑑識工具設定（雜湊值、時區設定、磁區命名、EFS 加解密分析）。
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。


JACOB
Jia-hon (Ace)

上課實況


INCH
INTERNATIONAL CYBER FORENSICS
Introduction to Networks and Computer Hardware
WEEK 1
DC3
Cyber Training Academy
WFE-E
INTERNATIONAL CYBER FORENSICS
Windows Forensic Examinations - EnCase
WEEK 3
DC3
Cyber Training Academy

上課教材

（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瞭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，使用案件提供的 netflow 檔案了解公司整體網路狀況即可疑 IP 位址、使用 wireshark 軟體分析可疑的網路封包以及 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，瞭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 cyberchef 網站所提供之代碼搜尋 IP 相關資訊，透過雜湊值解析至 Virustotal 網站搜尋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瞭解來龍去脈，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。


DC3
Cyber Training Academy
教官合影


DEPARTMENT OF DEFENSE
CYBER CRIME CENTER
DOD CYBER CRIME CENTER
DC3
CHALLENGE
DIGITAL FORENSICS CHALLENGE
結訓紀念獎牌

DC3 CYBER TRAINING ACADEMY

CERTIFICATE OF COMPLETION

This is to certify that

Lieutenant Jia-han Shih

has successfully completed

International-Cyber Forensics Course
(I-CFC)

INCH, CIRC, WFE-E, and FIWE
24 February 2020 – 27 March 2020 | Duration 200 Hours

Mr. Casimer F. Szyper, GS-14
Director, DC3 Cyber Training Academy

CompTIA
Eligible for CEUs

ACCREDITED IACET PROVIDER

ACE American Council on Education
Recommended for College Credit Hours

結訓證書

參、受訓心得

一、國際交流

首先很榮幸有這個機會能夠出國受訓，感謝各位長官的栽培，這也是我第一次到美國，在印象中西方教育的許多做法與我國有很大的差異，與上一梯次不同的是，因為疫情的影響，本次國際學員只有我國的兩位（另一位為資通電指揮部的同仁），教官一開始也提醒我們，亞洲學生比較不喜歡問問題，希望我們有任何問題要提出不要客氣，畢竟有些內容因為語言的關係可能會有認知上的差異。

第一週是比較基礎的內容，且學員僅有我們二位，不論是授課內容還是教官上課速度都可以吸收，頓時放心不少；殊不知第二週加入美國籍學員，教官說話速度明顯有加快，美籍同學跟教官間的談話內容及速度也有顯著差異，這是我有待加強的部分，畢竟在國內比較少遇到這樣的環境，不過整體來說教官幾乎都會配合我們放慢講課速度，真的有不懂下課後詢問教官也都會很詳細的幫我們講解。

本次受訓期間因國際學員人數僅有兩員，DC3 特別安排美國籍學員與我們一同上課，學員因單位需求受訓長度不一，因此遇到的同學每週都有變化，也藉此機會認識來自不同單位的美國籍同學，包含有海岸防衛隊、空軍及海軍的同學。其中我比較感興趣的是在海軍犯罪調查局(NCIS)服務的同學，經過在閒暇時間聊天得知，他們大多有不少出國辦案的經驗，美方各軍種均有類似的單位，各軍種案件各自分開偵辦，這是與我國較為不同的地方；他們隸屬美國海軍，絕大部分為聘雇人員，在許多國家都設有相關辦事處，包含在部份軍艦上也有設置，服務範圍以偵辦海軍案件為主，偶爾也會和美國其他執法機構合作執行國內的司法調查。

共同上課之美國籍學員

二、硬體設施

在硬體設施方面，每位學員配有雙螢幕，在同時操作多軟體時很有幫助，所有資訊皆能一目了然。大多數實作都是在虛擬主機操作，確保所有學員每次操作都是在相同的環境跟條件，不會有操作或設定錯誤所造成的問題。在虛擬機器上的資料都是一整套案件，從上課練習到最後測驗的內容都是有所相關連，感覺這套教材經過相當嚴謹的設計及無數次的除錯，對學員的學習及實際操作幫助頗大。

上課教材除了發放的課本外，在 DCITA 的教學網站上也放有教官的上課講義，第一天上課會給每位學員一組專屬自己的帳號密碼，由教官依照進度開啟權限，學員方能實施課後練習，每週測驗也是相同作法，考試前教官才會開啟權限，所有人的進度都會一致。且測驗及考試的安排常常是環環相扣，由上一題的答案當作下一題的題目，且每個練習都是一個完整的案子，有種抽絲剝繭破案的感覺。

三、師資能量

本次美方教官多為由 DCITA 聘請民間專業師資，舉例來說本次課程主要教官 James Meyer 先生即是在警界從事鑑識領域相關工作二三十年，相關實務經驗豐富，親自辦過的案例也是不勝枚舉，因此後期鑑識課程均由 James Meyer 先生實施授課；前面屬於基本硬體課程的教官也是在資訊業界服務並且有多年教學經驗的人士擔任，不論在教學品質或臨場提出的問題都能立即解決。即便如此，如課程中軟硬體有任何問題，教官不會因為自己是這方面專業自己解決，而是由專業的維修人員前來協助，教官負責授課而維護人員負責設備維護，分工相當明確。

肆、其他建議事項

一、專業領域

這次受訓遇到很多教官都是專研在專業領域好幾十年的專業人士，如這次從第一天陪我們到最後一天的 James Meyer 先生，在警界服務了二三十年，實務經驗相當豐富，在課程中常有實際案例可以搭配說明，在授課過程中能夠更好吸收並理解，故職建議本部應將過去偵辦案例彙集成冊，未來如遇類似案況，可供後輩們參考運用；另專業人材栽培不易，建議應考量單位需求及個人意願，跳脫傳統經管限制，減少人員調動機會。

二、教材編撰

本次受訓期間對教材方面印象深刻，但要充分理解教材內容，除了要有語文專長更要有資訊背景，考量本部同時有此專長者不在多數，職建議以美方教材為參考，翻譯並編撰適合本部的教材內容，並針對不同需求規劃課程難易度。現代人生活已離不開科技，未來數位證物比例的增加已是趨勢，因此職希望能將此課程內容推廣至基層憲兵隊，讓前線偵辦人員也能對數位鑑識有基本的了解，對案件偵辦及數位證物採集能更有幫助，提升本部專業素養；另課程內容提及資訊安全部分也建議納入本部各階層資安人員教育訓練，以培養本部所屬官兵資安違規事件查處之基本學養與能量。

三、持續精進

本此受訓課程適用於鑑識基礎入門，也讓我對數位鑑識有了更深的認識與了解，本次受訓單位 DCITA 提供的課程至少還有 2、30 種，因為疫情的關係其他的課程幾乎都沒開課，也沒機會參觀 DC3 的實驗室設備，讓職更加好奇其他的課程的相關內容。未來希望能有機會參加更深入的課程，例如本部欠缺戰場鑑識、前線蒐證、反鑑識等相關知識及實務經驗，提升本部鑑識能量，另 DCITA 除鑑識外尚有提供專業網路戰等課程，現今大規模網路侵害行動比比皆是，建議本部能積極爭取受訓員額，厚植相關師資能量。