出國報告（出國類別：短期進修）

美國國防部網路犯罪中心
網路犯罪調查班心得報告

服務機關：憲兵指揮部刑事鑑識中心
姓名職稱：董乃寧（上尉憲兵刑事官）
派赴國家：美國/馬里蘭州
出國期間：110 年 5 月 29 日至 7 月 5 日
報告日期：110 年 10 月 08 日

摘要

本次受訓係奉國防部民國 110 年 4 月 1 日國人培育字第 1100059595 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)受訓，訓期：110 年 6 月 1 日起至 110 年 7 月 2 日止，共計 5 週；該班隊係美國國防部網路犯罪中心為國際學生首創之班隊，課程內容區分網路與電腦硬體介紹、網路事件應處課程、微軟作業系統數位鑑識及微軟作業系統環境入侵手法與鑑識等 4 項，結合上述所學，帶回相關學習內容、心得及建議，供憲兵調查專業體系人員指導與參用。

目次

壹、目的

本次奉派美國網路犯罪調查班，藉實體參訓方式，瞭解美方網路及數位鑑識工作技術和其所採用之軟、硬體設備，並掌握可用於未來鑑識及教育訓練之研改方向。本文將受訓內容及美方鑑識設備等分析其優點，運用於未來裝備效能提升和人員專業培訓等面向，以提升案件偵查及鑑識工作能量。

貳、受訓過程與內容

一、單位介紹

(一）美國國防部網路犯罪中心：

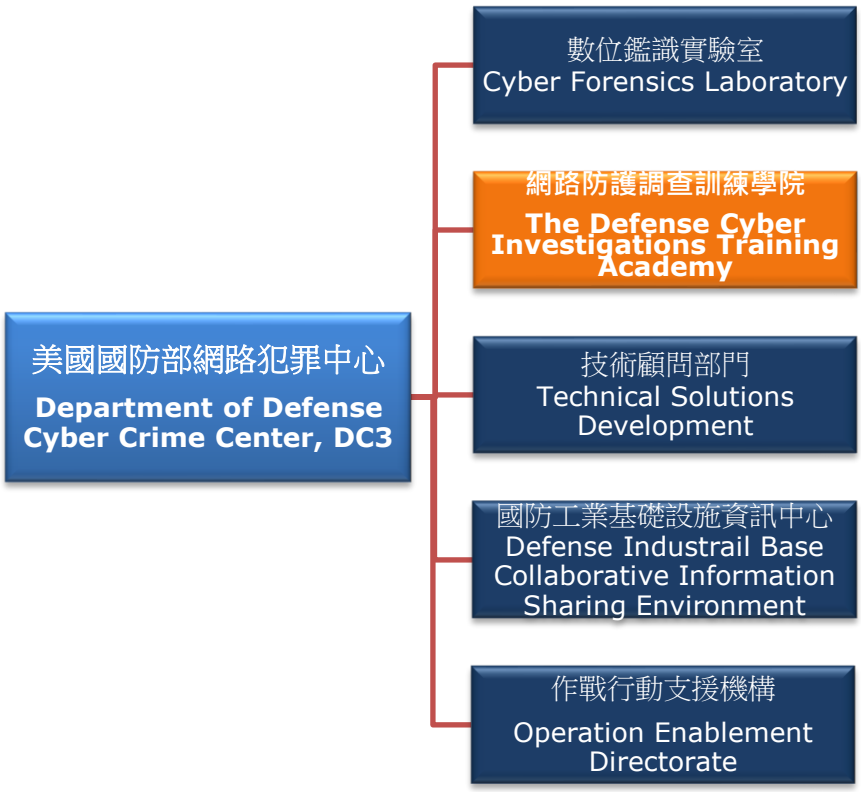
(Department of Defense Cyber Crime Center, DC3)

美國國防部網路犯罪中心，提供數位證物取證、網路技術人員培訓、網路漏洞研究、大數據提取及專業的顧問服務；本次參訓之美國網路防護調查訓練學院(The Defense Cyber Investigations Training Academy, DCITA)則為其下屬的鑑識人員培訓機構。

（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負責美方執行網路犯罪調查人員的合格訓練單位，該單位除訓練現役軍人外，亦同時接受民間人員參訓，本次包含美方軍事偵察機關專業幹員，如：美國國防犯罪調查局(Defense Criminal Investigation Services)及海軍犯罪調查局(United States Naval Criminal Investigation Service, USNCIS)等單位。



網路犯罪中心組織架構圖

1.軟體設施介紹：

每週授課採循序漸進方式進行，並依課程進度更換上課教室，使用之軟體則由簡入深指導學員運用，如：入侵檢測系統、網路封包分析軟體及手機鑑識系統；另外每個學員皆於主機中配置一個虛擬機器以進行各項模擬情境測驗。

2.硬體設施介紹：

訓練學院各間教室除基本設備外，亦因應課程的不同而有相應的教學電腦及儀器;最大納訓量可同時有 10 間教室同步授課，學員達百人之多。

3.師資介紹：

約翰,梅爾(John Mayer)為本次 5 週訓期的主任教官，過去曾在費城警察局服務 30 餘年，並以美國警察高階警司身份退休，後至網路防護調查訓練學院服務。

教官 John Mayer 下課時間與職說明課程內容不理解之處

4.學員組成：

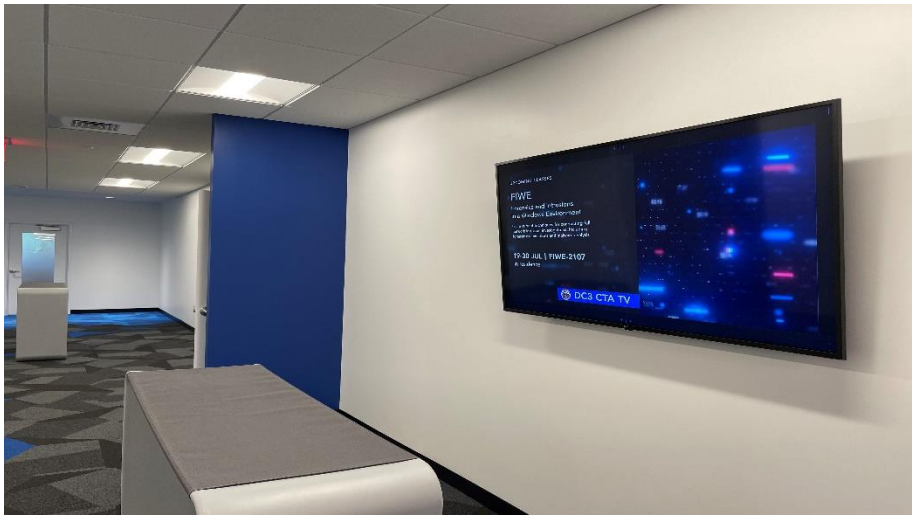
本次參訓班隊為 5 員小班制教學，教官也因此較能掌握學員受訓狀況；除職為國際學生外，也納訓國防犯罪調查局及海軍犯罪調查局等幹員共同訓練。

美國國防犯罪調查局　　美國海軍犯罪調查局

5.其他：

因 COVID-19 疫情，學院為落實防疫要求，自疫情起均改為視訊教學，此次為該中心自疫情後第 1 個現地授課的班隊，包含授課教官及全體行政工作人員等，均必須完成疫苗施打方能進入教學辦公場所。

受訓地點：Jacob’s Building、位於美國馬里蘭州漢諾威鎮



學院室內設施與環境

二、課程內容

此次受訓的內容，課程安排上均由淺入深，從第 1 週基礎的網路及硬體介紹到第 5 週實際使用軟體執行案件偵查及目標手機及硬碟鑑識的安排上，使學員可逐步的了解一整套案件偵查之始末，並使學員在期末測驗週有獨立產製出鑑識報告的能力，其課程內容介紹詳如下表。

美國網路犯罪調查班課程表	
時間	內容
第一週	網路與電腦硬體介紹 (Introduction to Network and Computer Hardware, INCH)
第二週	網路事件應處課程 (Cyber Incident Response Course, CIRC)

第三週	EnCase 微軟作業系統數位鑑識 (Windows Forensics Examinations-EnCase, WFE-E)
第四、五週	微軟作業系統環境入侵手法與鑑識 (Forensics and Intrusions in a WindowsEnvironment, FIWE)

（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(6 月 1 日－4 日)，學員可藉此第一週的課程內容當作對未來課程的暖身訓練，後續課程都依此週基本知識作為基石。課程內容主要分為四部份：

課程	第一週
網路與電腦硬體介紹	◆電腦硬體 電腦組成元件、主機板組成元件、存儲及媒體鏈結裝置
	◆網路運作 網路連結之特色、傳輸控制協定
	◆微軟作業系統 作業系統需求及特色、命令列操作、系統管理員操作、預防性維護程序、虛擬化客戶端及雲端硬碟概念
	◆電腦故障排除及系統作業安全 問題排除、作業系統安全設定、系統安全作業程序
小結	使學員複習電腦構造、網路知識及網路基礎常識與概念。

（二）網路事件應處課程：

(Cyber Incident Response Course, CIRC)

網路事件應處課程(6 月 7 日－11 日)，說明在目標案件處理前的準備工作，學員必須有評估及瞭解案件處理上等各需求所可能需要的各相關鑑識工具，並清楚知道抵達現場時之應注意事項，同時完備案件證物取得合法流程等相關技巧。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。每位學員在課程中需運用學院提供之工具箱(內含證物硬碟、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)等。課程內容主

要分為四部份：

課程	第二週
網路事件應處課程	◆事件應處 評估案件及準備工作、識別數位證據類型
	◆電腦評估 現場電腦評估、搜索及採證流程、作業系統加密、揮發性資料、關機程序、硬體檢測
	◆製作手機類完整媒體檔案 製作原則、實作及計算雜湊值、處理證物手機、手機狀態評估、紀錄手機資料、取得手機密碼
	◆證物處理 證物標籤、證物監管鏈追蹤、證物包裝及運送、證物儲存
小結	包含較多實務上技術執行技巧，主軸在於確保現場完整性與適法性。

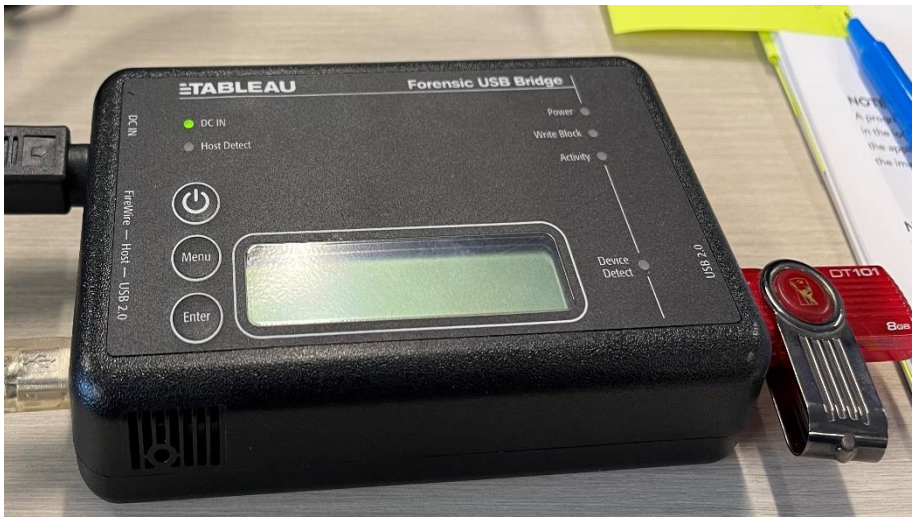


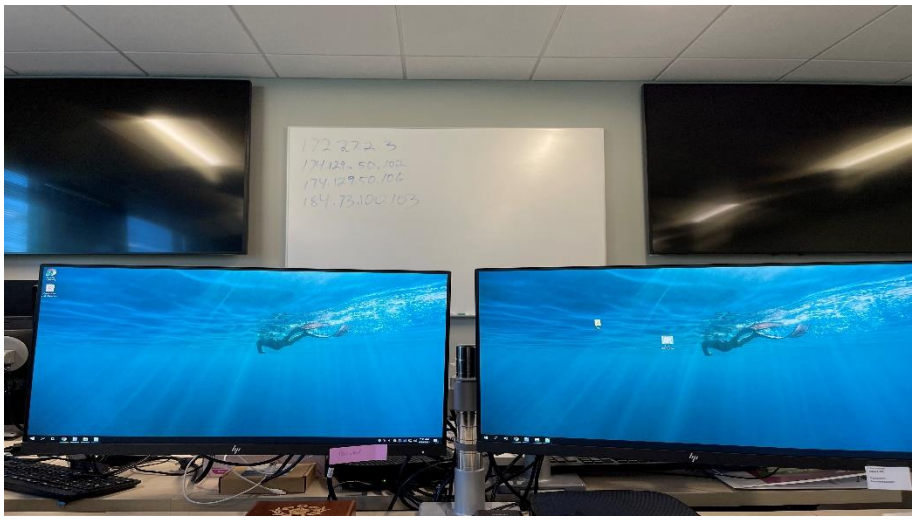
Tableau 防寫盒與需鑑識的拇指碟(右側紅色 8GB 硬碟)

（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(6 月 14 日-18 日)，本週課程係指導學員在遇目標案件時的應變作為，並在鑑驗階段時執行完善的資料獲取工作，學員將藉由鑑識軟體(EnCase-7)來製作模擬案件的鑑識報告，此週的課程著重於 EnCase 鑑識軟體將會被大量運用在期末測驗中，學員需對該軟體有完整的操作技術。本週課程內容分為六部份:

課程	第三週
EnCase 微軟系統數位鑑識	◆工具設定 圖形化介面、開啟新案件、數位媒體驗證、書籤功能、條件及篩選功能搜尋、惡意程式掃描
	◆基礎鑑識分析 基礎檔案系統、微軟作業系統、微軟登入紀錄檔
	◆鑑識分析 文件特徵碼、雜湊值、關鍵字、日期搜尋、資料還原
	◆檔案分析 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
小結	所授之報告調查大綱及提供改善建議等，因其為調查人員專業執行領域，故網安碩士班在課程中著墨較少。



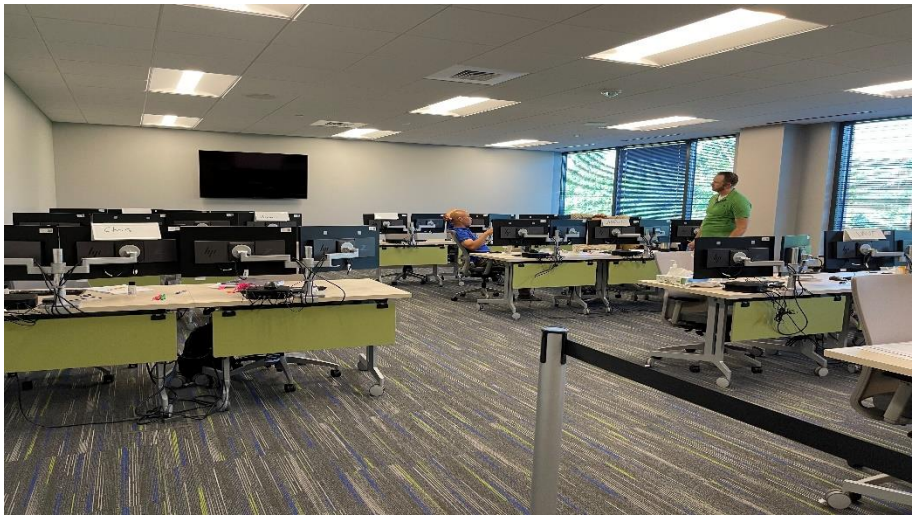
上課教室使用之雙螢幕電腦設備

（四）微軟作業系統入侵手法與鑑識：

(Forensics and Intrusions in a Windows Environment, FIWE)

微軟作業系統入侵手法與鑑識課程(6 月 21 日－7 月 2 日)，在此兩週的課程當中，主要運用 EnCase 以及 Wireshark 等兩項鑑識軟體作為主軸，同時配合 Netflow、Cyberchef、Volatility 以及 Snort 等輔助軟體來完成模擬案件鑑識工作。

課程	第四、五週
EnCase 微軟系統 數位鑑識	◆微軟作業系統環境入侵手法： 入侵痕跡調查、著手案件報告
	◆微軟作業系統環境入侵鑑識： 搜集潛在威脅資訊、網路封包分析、記憶體鑑識、系統及應用程式分析、識別惡意程式
	◆報告調查大綱、改善建議
小結	本週課程中，強調關鍵調查手法，著重鑑識軟體，諸如：（EnCase,Cellebrite)使用、關鍵字、日期搜尋等。



上課教室環境(每位學員皆配有 Windows10 版本電腦)

三、測驗規劃

（一）簡介：

區分為每週五小考及最後一週的期末測驗，最後一週的期末測驗共 2 日，合計 12 小時；期末測驗成績比重：時間序報告 50%、選擇題測驗 25%、總結報告 25%)。

（二）期末測驗（計 2 日）

1.第 1 日：

教官將在虛擬電腦中建立測驗情境，受害電腦使用者因點擊惡意釣魚郵件而啟動一連串的指令攻擊受害電腦，學員需運用所學知識及鑑識軟體完整分析並紀錄時間序報告。

2.第 2 日：

根據時間序報告加以分析，進而製作出此惡意攻擊程式的總結報告與改善建議，最後完成選擇題測驗。

（三）合格標準：每週成績均須達 70 分(均與美方學員相同)。

結訓前與教官 John Mayer 和助教 David Brooker 合影留念

網路防護調查訓練學院結訓證書

參、心得

一、專長職能與經驗提升

此次共同參訓學員均為美國網路犯罪調查領域的專業幹員，受訓期間藉由課程議題與網路攻擊案件研討，使職在網路駭侵及鑑識領域應用技巧皆獲得提昇，如：網駭緊急應變課程中，可知惡意程式於電腦所執行之最新入侵手法及指令，同步將所見情況紀錄於時間序報告中，對紀錄駭侵及鑑識作業程序上有實質收穫；另訓練學院在課程中指導學員操作美方常運用軟、硬體設備，使職進一步瞭解我國與美方採用設備上之差異性與操作技巧，並瞭解美方網路鑑識及資安領域中經常面臨的問題。以上所學在返國後執行偵查、鑑識工作及裝備性能提昇時，皆有極大助益。

二、測驗模式參考價值

此次參訓，在美方所提供的測驗模式，尤其令人印象深刻。在共計 2 日 12 小時的測驗中，美方提供 1 臺虛擬機器、1 臺實體電腦以及所需運用之鑑識裝備，例如：手機鑑識軟體 Cellebrite、Tableau 防寫盒等必要工具。學員必須在極大的時間壓力下運用鑑識軟體搜尋並分析惡意軟體在電腦中所執行的指令，並將所發現的指令詳細記錄在報告當中，產出的報告使偵查人員瞭解是所下載或是破壞的資料狀況。在實際偵查網路攻擊案件中，時間壓力是偵查人員經常面臨的挑戰，因為在惡意程式執行後，會在短時間內執行隱藏或刪除自身程式的指令，使得偵查人員僅能發現進出、入的時間日期，而無從得知更加詳細的細節。

肆、建議

一、綿密培養合適人選持恆派訓：

職比較過去擔任憲兵隊調查官及鑑識人員的經驗，此次赴美受訓吸收美方在案件偵查及鑑驗工作等理論，更能將國內、外知識與技術融會貫通，進而內化為專業知識，同時也因過去的經驗，使得在課堂上與教官及美方學員的交流能有更深的討論與互動，並獲得許多的回饋與建議。在未來納訓人員遴選上，職建議以曾經擔任調查官或鑑識專業人員等背景人員赴美，可使學員在學習上有事半功倍的效果，也更能將所見所學回饋從事偵查及鑑識專業人員。

二、鼓勵所屬至國防大學網路安全碩士在職班就讀並輔導考取相關證照：

近期犯罪手法及犯罪工具日趨新穎，建議具調查官或鑑識背景人才報名網路安全碩士在職班就讀，並輔導考取相關證照，如：資安鑑識調查專家及資安危機處理員等證照，在網路犯罪，網路攻擊等領域，強化調查人員偵查手段，進而提升偵查及鑑識專業能量。

出國報告審核表

出國報告名稱：美國網路犯罪調查班		
出國人姓名 (2人以上，以1人為代表)	職稱	服務單位
董乃寧	上尉鑑識官	憲兵指揮部刑事鑑識中心
出國類別	☐考察 ■進修 ☐研究 ☐實習 ☐視察 ☐訪問 ☐開會 ☐談判 ☐其他_____ (出國類別請依預算書之計畫預算類別填列)	
出國期間：110 年 5 月 30 日 至 110 年 7 月 2 日		報告繳交日期：110 年 9 月 30 日

出國人員自我檢核	計畫主辦機關審核	審核項目
☑	☐	1.依限繳交返國報告
☑	☐	2.格式完整(本文必須具備「目的」、「過程」、「心得及建議事項」)
☑	☐	3.無抄襲相關資料
☑	☐	4.內容充實完備
☑	☐	5.建議具參考價值
☑	☐	6.送本機關參考或研辦
☑	☐	7.送上級機關參考
☐	☐	8.退回補正，原因：
☐	☐	(1) 不符原核定出國際化
☐	☐	(2) 以外文撰寫或僅以所蒐集外文資料為內容
☐	☐	(3) 內容空洞簡略或未涵蓋規定要項
☐	☐	(4) 抄襲相關資料之全部或部分內容
☐	☐	(5) 引用相關資料未註明資料來源
☐	☐	(6) 電子檔案未依格式辦理
☑	☐	9.本報告除上傳至公務出國報告資訊網外，將採行之公開發表：
☑	☐	(1) 辦理本機關返國報告座談會(說明會)，與同仁進行知識分享。
☐	☐	(2) 於本機關業務會報提出報告
☐	☐	(3) 其他_____
☐	☐	10.其他處理意見及方式：

出國人簽章(2人以上，得以1人為代表)	計畫主辦機關審核人	一級單位主管簽章	機關首長或其授權人員簽章
董乃寧		憲兵指揮部計畫處處長 許協榮	憲兵指揮部參謀長 陳致航

說明：

一、各機關可依需要自行增列審核項目內容，出國報告審核完畢本表請自行保存。

二、審核作業應盡速完成，不以影響出國人員上傳出國報告至「公務出國報告資訊網」為原則。