行政院各機關因公出國人員報告書
(出國類別：研究)

107 年度「研習網站滲透測試與攻防技術」出國研習報告

服務機關: 內政部警政署刑事警察局
出國人員: 偵查員 張文欣、偵查員 余厚萱
出國地區: 美國
出國期間: 107 年 5 月 9 日至 5 月 21 日
報告日期：107 年 8 月 6 日

目錄

壹、摘要

本科為拓展資訊安全專業領域，培訓資安鑑識專業人員，於本年度派員赴美國參加 SANS(System Administration, Networking and Security)相關課程，SANS 為合作研究及學術教育組織，提供超過 165,000 名以上的資訊安全專家、稽核員、網管系統管理人員及首席資訊長等相關人士，分享其資訊安全教育課程，同時能為其所遭遇的問題提供解決方案。

貳、目的

本次行程為參加美國 SANS 資訊安全相關課程，內容包含電腦蒐證與進階現場數位證物處理、事件日誌檔鑑識與分析、殼層物件(Shell Item)分析、電子郵件鑑識等資安事件調查技術、關鍵安全控制與稽核機制等主機鑑識課程，及網路封包鑑識、威脅追蹤、研析及事件處理等資安事件調查技術，提升網路犯罪調查人員、資安鑑識分析人員及網路安全管理人員對於最新犯罪偵查技術的認知，並促進各國執法人員、資安專家與高科技犯罪調查產業間的互動、交流與知識分享。

參、行程摘要

一、 偵查員 張文欣

107 年		預定行程	任務	備註
日 期	星期			
5 月 9 日	三	臺灣前往美國聖地牙哥	飛往美國	搭乘長榮航空 10 時 15 分班機，於舊金山國際機場轉機
5 月 10 日	四	美國聖地亞哥	抵達美國聖地亞哥	當地時間 5 月 9 日 10 時 35 分抵達美國聖地亞哥國際機場(臺灣時間 5 月 10 日 01 時 35 分)，並前往飯店。

5 月 11 日	五	美國聖地亞哥	至 SNAS 上課地點報到，並領取 SANS 上課證、上課教材及上課需知。	
5 月 12 日	六	美國聖地亞哥	FOR572 首日課程	●網路代理伺服器檢驗 ●基礎網路鑑識工具 ●取得網路證物 ●網路架構所帶來的挑戰與機會
5 月 13 日	日	美國聖地亞哥	FOR572 課程第二日	●HTTP 協定與日誌檔 ●DNS 協定與日誌檔 ●防火牆、IDS 日誌檔 ●日誌檔格式及獲取
5 月 14 日	一	美國聖地亞哥	FOR572 課程第三日	●網路流量蒐集與分析 ●開源網路流量分析工具 ●FTP 協定 ●微軟協定
5 月 15 日	二	美國聖地亞哥	FOR572 課程第四日	●SMTP ●商用網路鑑識工具 ●無線網路鑑識 ●自動化工具
5 月 16 日	三	美國聖地亞哥	FOR572 課程第五日	●加密、壓縮及 SSL 封包 ●中間人攻擊 ●網路協定逆向工程 ●營運安全及威脅情資
5 月 17 日	四	美國聖地亞哥	FOR572 課程第六日	●網路件事實作
5 月 18 日	五	美國聖地亞哥	搭機返臺	搭乘當地時間 5 月 17 日 20 時 40 分班機(臺灣時間 5 月 18 日 11 時 40 分)自美國聖地亞哥起飛，於洛杉磯國際機場轉機。

5 月 19 日	六	美國返回臺灣		5 月 19 日 5 時 10 分抵達桃園國際機場。
合計	11 日			

二、 偵查員 余厚萱

107 年		預定行程	任務	備註
日期	星期			
5 月 9 日	三	臺灣前往美國聖地牙哥	飛往美國	搭乘長榮航空 10 時 15 分班機，於舊金山國際機場轉機
5 月 10 日	四	美國聖地亞哥	抵達美國聖地亞哥	當地時間 5 月 9 日 10 時 35 分抵達美國聖地亞哥國際機場(臺灣時間 5 月 10 日 01 時 35 分)，並前往飯店。
5 月 11 日	五	美國聖地亞哥	至 SNAS 上課地點報到，並領取 SANS 上課證、上課教材及上課需知。	
5 月 12 日	六	美國聖地亞哥	FOR500 首日課程	●Windows 作業系統各版本運作原理與差異 ●核心數位鑑識準則 ●現場數位蒐證技術 ●NTFS 作業系統介紹 ●檔案雕刻(File Carving) ●記憶體分析
5 月 13 日	日	美國聖地亞哥	FOR500 課程第二日	●註冊檔鑑識與核心介紹： ➢ 使用者與群組使用資訊 ➢ 系統資訊 ➢ 使用者活動紀錄

5 月 14 日	一	美國聖地亞哥	FOR500 課程第三日	●殼層項目(Shell Item)鑑識 ●USB 鑑識
5 月 15 日	二	美國聖地亞哥	FOR500 課程第四日	●電子郵件鑑識 ●Windows 跡證介紹 ●事件日誌檔分析
5 月 16 日	三	美國聖地亞哥	FOR500 課程第五日	●網頁瀏覽器鑑識技術： ➢ Internet Explorer ➢ Firefox ➢ Chrome ➢ 網頁瀏覽器相關跡證介紹
5 月 17 日	四	美國聖地亞哥	FOR500 課程第六日	●Windows 數位鑑識實例挑戰
5 月 18 日	五	美國聖地亞哥	SEC440 課程第一日	●建立授權和未授權設備的清單 ●建立授權和未授權軟件清單 ●筆記型電腦、工作站與伺服器之軟、硬體安全設定 ●持續漏洞評估和修復 ●管理者權限控管 ●日誌檔之維護、監控與分析 ●電子郵件與網頁瀏覽器保護 ●惡意程式防護 ●網路埠、協定及服務之限制與控制
5 月 19 日	六	美國聖地亞哥	SEC440 課程第二日	●資料救援能力 ●網路設備(如防火牆、路由器與交換器)之安全設定

				●邊界防禦措施(Boundary Defense) ●資料保護 ●最小權限原則 ●無線設備控制 ●帳戶監控與控制 ●安全技術評估與訓練 ●應用程式安全 ●資安事件處理與管理 ●滲透測試與分析
5 月 20 日	日	美國聖地亞哥	搭機返臺	搭乘當地時間 5 月 19 日 20 時 40 分班機(臺灣時間 5 月 20 日 11 時 40 分)自美國聖地亞哥起飛,於洛杉磯國際機場轉機。
5 月 21 日	一	美國返回臺灣		5 月 21 日 5 時 10 分抵達桃園國際機場。

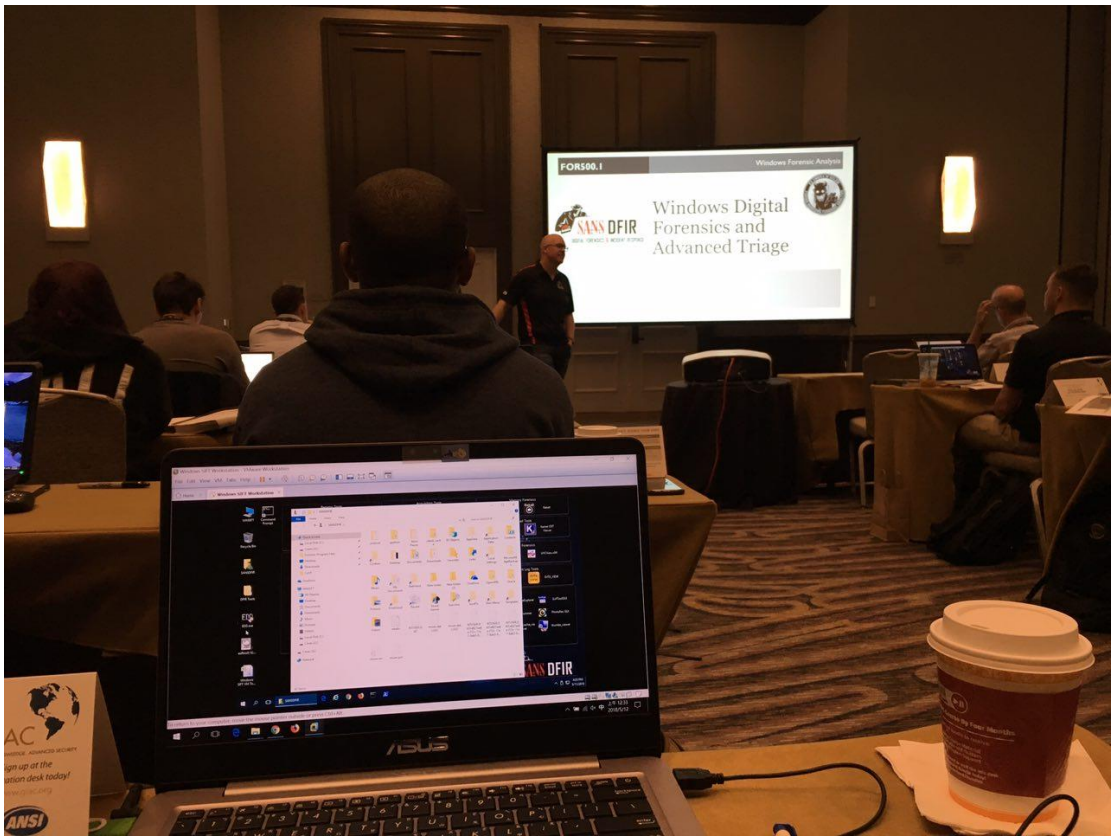
肆、課程內容重點

一、 課程摘要：

(一) FOR500 Windows 數位鑑識分析課程(Windows Forensic Analysis)：講師為資安專家 Rob Lee，具備資訊安全、資安事件處理與威脅狩獵、數位鑑識之專業，曾為美國空軍專責資訊作戰的軍事單位--第 609 資訊戰爭中隊(the 609th Information Warfare Squadron)創始成員，具備與美國國防部、情報機構、執法機關合作漏洞發現、漏洞開發、數位採證之技術負責人，具備豐富技術知識與實務經驗。

課程大綱：

1. Windows 作業系統數位蒐證與鑑識技術。
2. 註冊檔鑑識與核心介紹。
3. 殼層項目(Shell Item)與 USB 鑑識。
4. 電子郵件鑑識、Windows 跡證介紹與事件日誌檔分析。
5. 網頁瀏覽器鑑識技術。
6. Windows 數位鑑識實例挑戰。

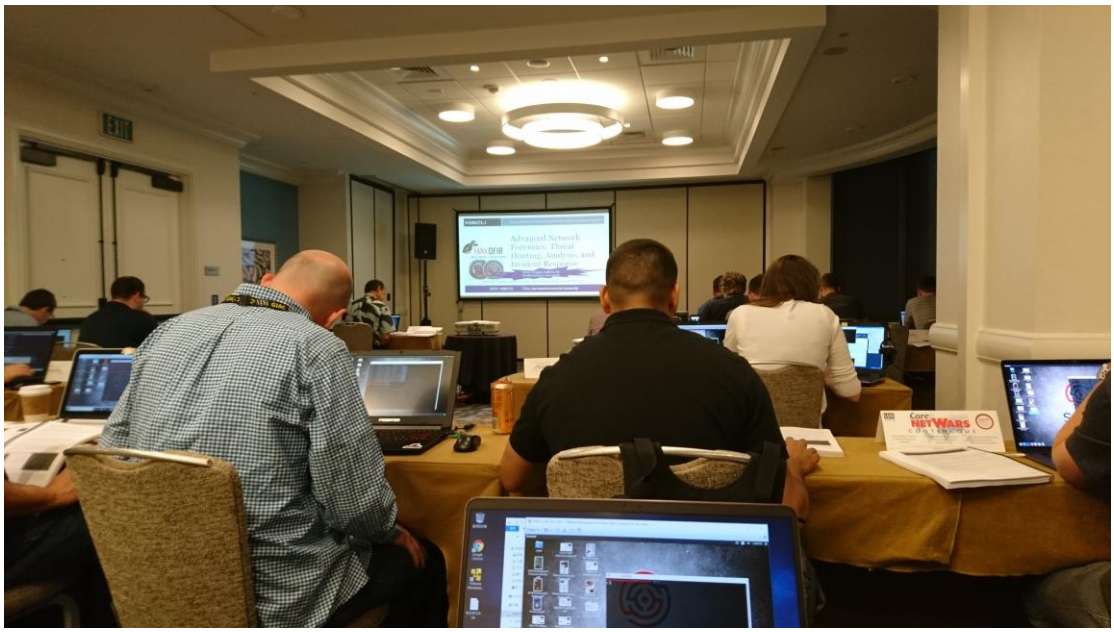


圖片說明：FOR500 Windows 數位鑑識分析課程上課情形

(二) FOR572(網路鑑識、威脅追蹤、分析及事件處理)：講師為　Philip Hagen，在資訊安全領域擁有超過 18 年的經驗，且為 FOR572 課程的負責人和共同作者，並自行開發了開源的網路鑑識環境「SOF-ELK」。

課程大綱：

1. 離開磁碟進入網路領域。
2. 核心的網路協定、日誌檔的獲取及分析。
3. 網路流量、檔案存取協定。
4. 商業工具、無線網路及封包分析。
5. 加密封包、逆向工程、營運安全及威脅情資。
6. 網路鑑識實例挑戰。

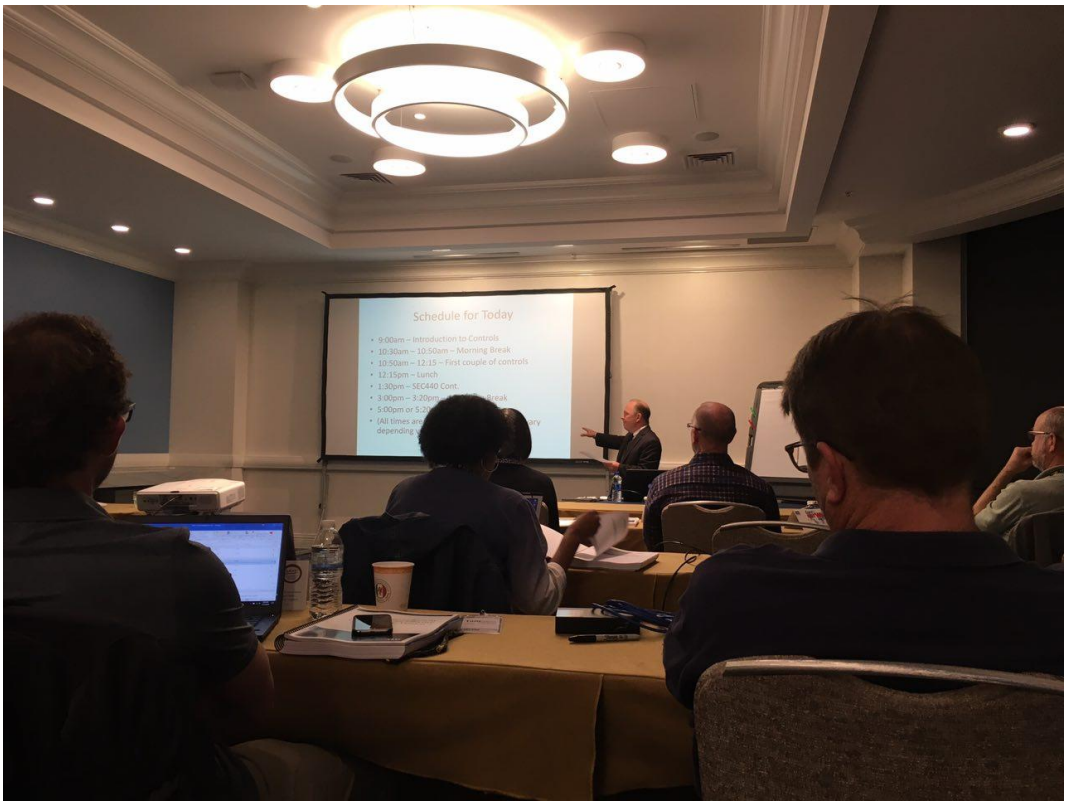


圖片說明：FOR572 網路鑑識、威脅追蹤、分析及事件處理上課情形

(三) SEC440 關鍵資訊安全控制：規劃、實踐與稽核(Critical Security Controls: Planning, Implementing, and Auditing)：講師為 Chris Christianson，具備 20 年以上的資訊安全工作經驗及相關證照，包含 GSEC, GCIH, GCIA, GREM, GPEN, GWAPT, GCCC, GISF, GCED, CISSP, CCSE, CCDP, CCNP, IAM, CEH 及 IEM。

課程大綱：

1. 介紹關鍵控制措施之重要性。
2. 詳細介紹 20 種關鍵控制措施與實踐方式。



圖片說明：SEC440 關鍵資訊安全控制：規劃、實踐與稽核上課情形

二、 主機鑑識

(一) Windows 作業系統數位蒐證與鑑識技術：

1. 課程從簡介當今網路環境中的數位鑑識開始，並與學員討論行動設備、平板電腦、雲端空間和現代 Windows 作業系統帶來的挑戰，亦討論固態硬碟（SSD）等現代硬碟運作原理如何影響數位鑑識過程以及分析人員該如何因應這些新技術。目前科技發展使得硬碟儲存空間不斷擴增，增加數位鑑識處理與採證的困難，以往的數位鑑識流程為保持證據之完整性須製作映像檔，但日與遽增的儲存空間使得傳統數位鑑識流程變得不可行，如何在證據完整性與取證效率之間取得平衡是現今數位鑑識分析人員必須面臨的課題。
2. 本次課程先介紹數位鑑識核心觀念，再帶入適合現今狀況的現場採證流程，提升採證程序之速度與效率。現場可先採集相關電子跡證，包含記憶體、NTFS 檔案系統之 MFT 表、Windows 日誌檔、註冊表與可能存有重要跡證之檔案等，快速找出關鍵證據，並介紹如何使用商業工具與開源免費工具處理所蒐集之證物。
3. 數位映像檔掛載與檢視，在不變更證物之前提下進行分析，以維持證物之完整性，並進行文件與檔案的元資料(Metadata)分析，利用檔案時間判斷檔案複製、建立之時間等。
4. 檔案雕刻(File Carving)介紹與原則，當檔案元資料(Metadata)遺失時，如何透過檔案特徵進行檔案雕刻(File Carving)找回資料片段，並介紹

相關工具使用方式。

5. 記憶體、分頁檔與未配置空間分析，用於協助跡證還原，例如從記憶體中找出 Facebook Live, MSN Messenger, Yahoo, AIM, GoogleTalk 等即時通訊訊息、網頁電子信箱內容等。

(二) 註冊檔鑑識與介紹

1. 註冊檔介紹：註冊檔之資料結構包含巢(Hive)、鍵(Keys)與值(Value)，註冊檔僅保存最後寫入時間，該時間對於鑑識人員具有重要分析價值，例如可藉此分析最後網站瀏覽時間、USB 最後插入與退出時間等等。此外，MRU(Most Recently Used)列表可協助分析使用者活動、開啟之文件等。
2. 使用者與群組使用資訊：對應使用者名稱與其 SID，配合註冊檔紀錄判斷最後登入時間、最後登入失敗時間、登入次數及密碼政策等。
3. 系統資訊：學習如何識別工作站之目前控制設定(Current Control Set)、電腦名稱與系統版本、時區、IP 位置資訊、連接無線網路、有線網路與 3G 網路之歷史紀錄、判斷網路地理位置之歷史資訊、網路芳鄰資訊、最後關機時間等重要跡證。
4. 使用者活動紀錄：利用電腦跡證證明程式執行、檔案下載、檔案或資料夾存取、Office 及 Office 365 檔案歷史紀錄、搜尋紀錄、最近開啟文件等相關活動紀錄。

(三) 殼層項目(Shell Item)與 USB 鑑識

1. 透過檢視 LNK 捷徑檔、Jump List 及 Shellbag 資料庫以判斷檔案或資料夾的初次、最後一次開啟時間，該技巧可以運用於追蹤駭客或機密資料竊盜案件之相關使用者在關鍵電腦上的活動軌跡。
2. 可卸除式儲存媒體之鑑識與調查為數位鑑識重要的一個環節，經過講師深入淺出的分析，理解到 USB 設備使用後可能在 Windows 7-10 殘留之跡證，藉此可判斷設備第一次與最後一次接上電腦之日期時間、廠牌、型號及單一識別序號等重要資訊。

(四) 電子郵件鑑識、Windows 跡證介紹與事件日誌檔分析

1. 面對各種不同的調查案類，電子郵件有時能提供分析人員非常有用的資訊，藉由學習復原遭刪除之電子郵件協助找出可用於定罪的證據。基於電子郵件發送與接收原理，同一封電子郵件可能會有多個副本存在於使用者本機、企業的郵件伺服器、私有雲端空間或多個網頁電子郵件帳戶中，這些特性大大增加調查人員找回遭刪除的電子郵件證據。
2. 其他 Windows 跡證例如 Prefetch 檔、appcompatcache 資訊等都可以作為程式執行、存在過的重要證據。此外，就算嫌犯使用反鑑識處理相關證物，可以透過最近新發現的 System Resource Usage Monitor (SRUM)跡證協助判斷使用者行為。

3. 最後再由講師介紹 Windows 的事件日誌檔，大多數案件都可以從事件日誌檔獲得有用資訊，瞭解其存放地點與內容意義可提供調查人員更加全面的事件分析角度。例如可追縱使用遠端桌面登入、暴力破解密碼的行為與帳戶權限濫用等。

(五) 網頁瀏覽器鑑識技術

1. 隨著網頁使用者數目不斷增加、許多應用程式開始漸漸轉移至網頁上、雲端運算技術成熟化，網頁瀏覽器分析成為不可或缺的數位鑑識技術。不同的網頁瀏覽器皆具備不同的運作模式，保存之紀錄也不盡相同，講師除了介紹目前最常見的 Internet Explorer、Firefox 與 Google Chrome 瀏覽器分析，亦一步步解析其 SQLite 與 ESE 資料庫，給予分析人員完整的底層運作知識，該技術可運用到其他大部分的瀏覽器。
2. 學習透過分析網頁 cookies、瀏覽與下載紀錄、網頁快取資料、瀏覽器插件，講師亦特別叮嚀一般分析人員可能誤判的資訊(例如有些造訪紀錄可能是網頁廣告造成，並非使用者真實瀏覽紀錄)，並教導每項跡證之限制與如何正確解讀其內含之訊息。

(六) Windows 數位鑑識實例挑戰

透過小組合作，以講師提供實際調查情境演練方式，分工合作完成完整之事件調查，其過程必須運用課程所學以分析相關電子跡證，例如網頁瀏覽紀錄、USB 使用紀錄、使用者活動軌跡及電子郵件等，釐清事件發生之過程，其最快完成調查之優勝隊伍可獲得 SANS 講師頒發之 DIFR 徽章。

三、 網路鑑識

(一) 網路鑑識基礎入門知識

1. 儘管網路採證的許多概念與任何其他數位採證調查的概念類似，但網路採證仍呈現出許多需要特別注意的細微差別。
2. 網路資料只有在直接從線路側錄時可被以保留，故網路封包側錄是重要的基礎，其中 tcpdump、Wireshark 分別為用於側錄和分析網路封包的最常用工具。
3. 由於長期完整側錄網路封包在大多數環境中並不常見，因此可以透過管理網路功能的設備(如防火牆)來了解過去在網路上發生的事情。

(二) 了解網路協定及日誌檔

1. 通過學習這些各種網路協定的典型態樣，以更容易地識別出濫用協定用於惡意目的之異常態樣，另外也可以透過流量分析以及相關系統所創建的日誌檔來分析這些協定狀態和異常行為。
2. 鑒於完整的網路封包側錄因快速累積大量資料導致難以儲存，且造成後續分析的困難，日誌檔資料是網路採證領域的重點之一；了解

不同網路傳輸設備中的日誌檔數據及其採證、分析過程是一項重要的網路採證技能，檢查以網路為中心的日誌當資料可以填補不完整或不存在的網路封包側錄所留下的空白。

(三) 網路流量分析

網路連線日誌檔記錄通常稱為 NetFlow(網路流量分析)，因其儲存要求極低，故可能是網路調查中最有價值的證據來源；由於 NetFlow 不側錄任何傳輸內容，因此可以減輕許多長期保留的法律問題，且即使沒有傳輸內容，NetFlow 也提供了一種極好的方法來呈現攻擊者的活動態樣。

(四) 商用工具的應用

1. 隨著無線網路的廣泛應用，調查人員為了能準備好應對這項技術帶來的獨特挑戰，無論正在研析的協定或用於執行分析的預算，建置大規模執行側錄封包及研析之工具格外重要。
2. 在預算考量之下，可評估分別利用不同專為小規模使用而設計的開源工具特性，組合用於大規模部署來滿足調查需求。

(五) 針對加密封包之應對

1. 技術的進步使駭客得以更容易地隱匿自己的行蹤。儘管如此，即使在最先進的方法中仍存在弱點，在學習駭客隱匿行蹤技術的同時，偵查人員應謹慎操作以避免逾越偵查至害親攻擊之底線。
2. 加密經常被認為是有效網路取證的最重要障礙，但針對加密網路流量的正確分析仍然可以從中獲得與內容相關的有價資訊。

(六) 網路鑑識實例挑戰

結合您在本週之前和本週學到的所有知識來分析實際案例的網路證據，透過分組挑戰的方式，嘗試數據分析、形成假設並提出結論來還原駭侵事件的發生始末，另可嘗試針對所發生的事件提供具體的資安機制或流程之改善建議。

四、 20 項關鍵資訊安全控制措施：

本課程在於協助學員如何實施與審核Center for Internet Security (CIS)所規範之關鍵安全控制措施，及其所需之具體技術與工具。課程列出的重要安全控制措施近年來幾乎成為敏感情資機關首要任務，這些措施是由美國軍方、政府機構及許多情資機構(如美國國安局、國土安全部、法院)等共同選訂，用於阻止已知攻擊的最佳實踐方式，並協助機關、企業減輕受攻擊所遭受的損害。本課程歸納之 20 項關鍵資訊安全控制措施簡要羅列如下：

(一) 建立授權和未授權設備的清單

(二) 建立授權和未授權軟件清單

(三) 筆記型電腦、工作站與伺服器之軟、硬體安全設定

(四) 持續漏洞評估和修復

(五) 管理者權限控管

(六) 日誌檔之維護、監控與分析

(七) 電子郵件與網頁瀏覽器保護

(八) 惡意程式防護

(九) 網路埠、協定及服務之限制與控制

(十) 資料救援能力

(十一) 網路設備(如防火牆、路由器與交換器)之安全設定

(十二) 邊界防禦措施(Boundary Defense)

(十三) 資料保護

(十四) 最小權限原則

(十五) 無線設備控制

(十六) 帳戶監控與控制

(十七) 安全技術評估與訓練

(十八) 應用程式安全

(十九) 資安事件處理與管理

(二十) 滲透測試與分析

伍、心得與建議事項

一、 與學員交流鑑識工作經驗：

本次課程之參訓學員來自各大廠商的資安人員與美國政府官員，並取得過多張資訊安全相關證照。不少學員經驗豐富，本次課程認識到一位現任微軟員工、前執法人員之同學 Steve，因具備相同執法背景，藉此機會瞭解美國執法單位與本國警察機關運作流程之異同；另亦認識一位現任美國政府官員 Amy，其專責調查詐領醫療保險金之數位鑑識工作，對於本國警察機關面對各種案類數位鑑識經驗非常有興趣，也希望雙方未來有機會可進行交流與參訪。

二、 提供最新資安相關資訊、理論與實務結合之案例：

講師每日會提供大量近期資訊安全最新之攻擊手法、威脅趨勢、鑑識與分析技術等情資，並搭配曾辦理過之時事案例，例如美國總統參選人希拉蕊電郵門案件，介紹如何運用課程所學知識進行分析鑑識，提供學員理論與實務結合的最佳範例。

三、 將所得經驗及技術內化為本局科偵能量

透過方法技術及經驗的學習，運用於未來資安事件偵查、數位跡證蒐集與分析技術之實務運用，並強化專業人才培育，推廣相關偵查技巧至各警察機關科技偵查人員，透過有效專業分工並以團隊合作方式，強化科技犯罪預防及偵查能量，有效提升執法效能。

陸、結語

本次代表本局參加 SANS 數位鑑識與資訊安全課程，獲益良多，隨著 Windows 作業系統、網頁瀏覽器不斷更新，講師提供許多詳盡各版本鑑識重點解析，並建議學員不應過度依賴工具，因此課程著重在許多跡證之運作原理等底層分析知識，未來就算面臨版本更新、鑑識工具還無法支援的時候，便能運用相關知識進行分析；或為避免鑑識工具誤判，亦能以相關知識進行確認，確保證據的正確性。本次課程認識許多學員大方交流調查技術與過往經驗，藉此機會建立兩國聯繫窗口，可有助於未來案件之國際合作。講師於課程中提供之工具與技術之知識，我國警察機關可運用於未來資安事件偵查、數位跡證蒐集與分析技術之實務運用，期望未來能推廣相關偵查技巧至各警察機關科技偵查人員，強化科技犯罪預防及偵查能量，有效提升執法效能。