

出國報告（出國類別：研究）

赴美國參加 2018 年 HTCIA 研討會

服務機關：內政部警政署刑事警察局

姓名職稱：黃禎慶 股長

吳佳祐 警務正

洪振耀 警務正

胡正憲 偵查員

王靖欽 偵查員

派赴國家：美國

出國期間：107 年 8 月 14 日至 107 年 8 月 25 日

報告日期：107 年 11 月 12 日

摘要

隨著資通訊科技與社群網路快速發展，近年許多犯罪分子與駭客均利用新興資通訊技術或科技產品從事犯罪活動，更使用科技手法將數位證物內部關鍵證據加以掩飾，造成電腦、智慧型手機、社群網路甚或是 IoT 裝置等數位證物，皆淪為犯罪者進行犯罪之媒介，此類科技犯罪活動已是層出不窮且越趨嚴重，值得執法人員高度重視此類科技犯罪議題。

故此，世界各國均積極蒐集相關技術資訊、培育相關技術人才，尋求最佳解決方案或因應策略。本次參加的 HTCIA 高科技犯罪調查研討會即是國際間有關高科技犯罪及偵查技術探討與交流之重要年會，循例開設許多數位鑑識、資訊安全及網路犯罪偵查技術相關課程。

目次

壹、 目的.....	4
貳、 過程.....	4
一、 HTCIA 高科技犯罪調查研討會	5
(一) 暗網偵查 Darknet / Darkweb Investigation	5
(二) 追蹤行動裝置-從社交網站及智慧手機 APPs 抓取數位證據	7
(三) 晶片摘取 (Chip-Off) 數位鑑識	8
(四) 假照片的數位鑑定	10
(五) 快速擷取數位證據	11
(六) 心理學武器化-社會學及最佳化釣魚之警方詢問策略	12
(七) HTCIA 課程中之國際交流	12
二、 參訪行程	13
(一) 參訪美國蒙哥馬利郡警察局數位鑑識實驗室	13
(二) 馬里蘭州蒙哥馬里縣蓋瑟斯堡市警察局	14
(三) 參訪 FAIRFAX 郡警察局	16
(四) 拜會駐美國臺北經濟文化代表處	17
(五) 參訪 NUIX 數位鑑識軟體公司	18
參、 心得及建議	18

壹、目的

HTCIA 高科技犯罪調查研討會為全球最大科技犯罪調查討會且有多國相關執法人員參加，並有相關科技偵查、數位鑑識設備展示，採短天數、密集與多項研習主題同時進行方式辦理，為持續提升本局科技犯罪偵查能力，乃指派本局股長黃禎慶率警務正吳佳祐、警務正洪振耀、偵查員胡正憲及偵查員王靖欽等 5 人，參與會議，於同時間不同課堂內學習國際最新數位鑑識及科技偵查知識，並和與會各國執法機關相互研討問題、建立跨境打擊犯罪、資訊交換等國際合作管道，並參訪美國司法機構及數位鑑識設備廠商。

藉由參加研討會及參訪等機會，瞭解新型態犯罪手法之最新數位鑑識與科技犯罪偵查方法，以作為國內科技偵查、數位鑑識技術發展與制度機制規劃之參考。

貳、過程

本次派員參加 HTCIA 高科技犯罪調查研討會暨參訪行程，規劃自 107 年 8 月 14 日起至 107 年 8 月 25 日止，共計 12 日。於臺灣時間 107 年 8 月 14 日於桃園國際機場出發，搭乘長榮航空前往美國舊金山，復轉乘美國聯合航空抵達美國華盛頓特區；另於美國時間 107 年 8 月 23 日自美國華盛頓特區搭乘美國聯合航空前往美國舊金山轉機，轉乘長榮航空於臺灣時間 107 年 8 月 25 日返抵臺灣桃園國際機場。

日期	預訂行程	內容	日數
107 年 8 月 14 日	啟程	啟程經美國舊金山轉機，赴美國華盛頓與會	1
107 年 8 月 15 日至	參訪	參訪美國司法機構及數位鑑識設備廠商	4
107 年 8 月 19 日至	研討會	參加 2018 年 HTCIA 高科技犯罪調查研討會	4

日期	預訂行程	內容	日數
107 年 8 月 23 日 至	返程	參訪美國司法機構後返臺	3

一、HTCIA 高科技犯罪調查研討會

(一) 暗網偵查 Darknet / Darkweb Investigation

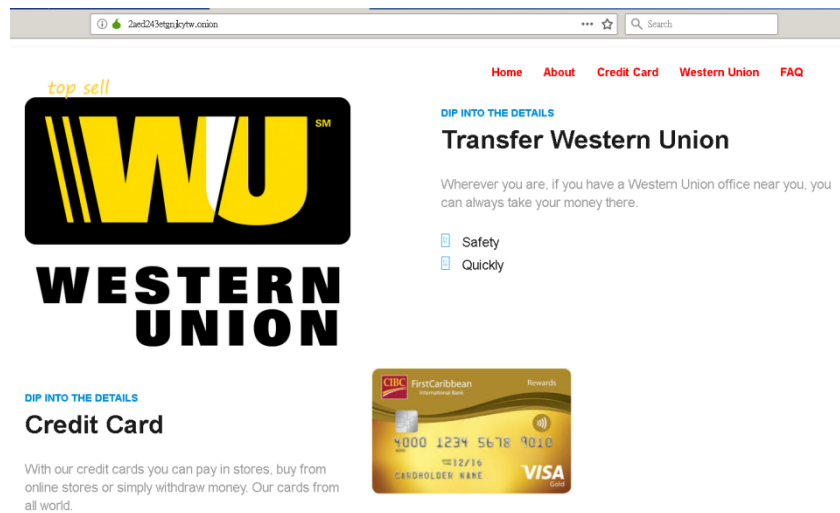
Darknet (暗網) 是相對於明網而言，明網是指一般網際網路公開的網路服務 (網站或是電子郵件)，大多數都能透過搜尋引擎搜尋到相關的網址，而暗網就是一些網站或是網路服務被隱藏，無法被搜尋引擎搜尋到，通常必須透過特殊的軟體才能進入。

TOR (The Onion Router)，進入暗網的工具之一，1995 年美國海軍研究實驗室啟動了 TOR 開發計畫，目的是為了保護通訊網路安全，避免被跟蹤信號等等，2004 年後，美國政府因實驗室陷入財政危機，將 TOR 改為對外募資，並開始與自由主義網路組織：電子前哨基金會合作推廣 TOR 的易用性、普及性及隱匿性。

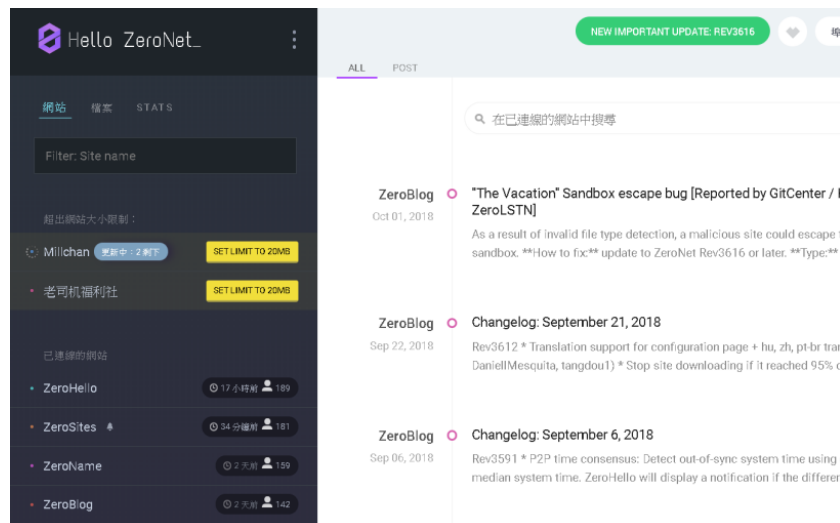
不同於明網的網路運作，暗網的網站不願意公開網址、IP 位址，因此暗網的連線中間需透過 TOR 伺服器建立封包傳遞的路由，而伺服器之間的傳遞都是採加密的方式進行。但加密只在傳遞過程中，送到 TOR 伺服器後，因為要知道送往何處，所以會將封包解密，再將封包加密後往下個伺服器傳送，這過程會經過 6 個伺服器傳遞。

由於這樣的網路模式是傾向保護伺服器端，因此衍生出很多非法交易的網站，例如有名的毒品網站絲路 (Silk Road) >。除此外，暗網內容亦包含其他如：色情、槍枝販賣、駭客等等。

這類網站的特性可大致區分成實體物品交易，以及數位內容交易兩大區塊，實體物品交易類包含毒品、槍枝、屍體、色情應召等等，這樣的交易需要突破的是國境的邊界檢查，這類交易的特性是可跨國交易（比特幣付款），並且透過用過即焚的通訊軟體來隱蔽。而數位交易種類包含盜版影音、線上色情、委託駭客攻擊、檔案加密勒索、個資販買等，這類內容均需數位化，而且無國際邊境問題，付款同樣可以透過比特幣，即可在網路上完成交易，幾乎完全隱蔽。



而另一種暗網的名稱叫 Zero Net（零網），會議中提到這個零網是透過 P2P 的方式連結，目前中國大陸的用戶最多，但上面的兒少色情也十分嚴重氾濫。



News	Politics	Porn
Torrent Freak News 180 ☆ 125	Pirate Party Forum Politics discussions 19 ☆ 92	老司机福利社 76 ☆ 新奇的猎枪老司机乐器 我是老司机 我为自己开车 68
Zero News News 33 ☆ 132	Wikileaks Torrents All torrent files from Wikileaks 16 ☆ 28	撈大师 52 ☆ 瀏覽器鎖的色情网站，域名：ledashi.tk 256
ZeroLeakz The Snowden Surveillance Archive & Wikileaks Torrents on Zer... 23 ☆ 108	Kill ISIS消灭伊斯兰教 10 ☆ 清真寺是恐怖分子培训基地，地球文明的毒瘤 9	Ochan Porn 47 ☆ A Freedom Porn Chan 342
Vault7: CIA Hacking Tools Revealed Vault7: CIA Hacking Tools Revealed 11 ☆ 30	The Daily Stormer 7 ☆ Daily Stormer Mirror 21	怡红院 43 ☆ 中文警告论坛 (已链接到: MiKChan) 220
Linux.RU Новости российского анкистирования 9 ☆ 27	郭老七 6 ☆ 群发英文资讯链接模板 20	凡号 29 ☆ 平生阅片无数，心中自然开窍。 118
朝花夕拾 收集中国正规互联网媒体发表又被删除的文章 9 ☆ 26	Values on Zeronet 4 ☆ Find out what political values you hold important. 23	PornPad 23 ☆ The Porn Pad 1661
River of News Link collator from NYT, BBC and Al Jazeera. Must leave ZN to read. 7 ☆ 39	Right Politics Without Censorship 3 ☆ Free right politics discussion, blog, links. In English. 24	Dog123站点目录 23 ☆ 中文成人网站目录、博客目录 152

(二) 追蹤行動裝置-從社交網站及智慧手機 APPs 抓取數位證據

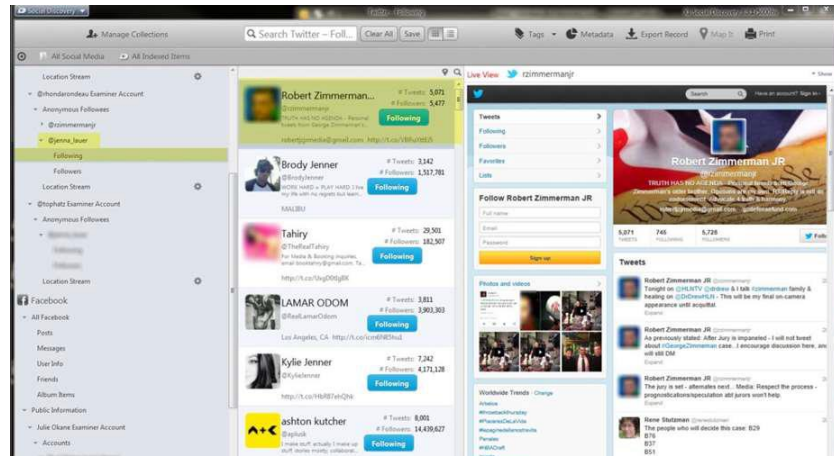
Digital Mountain 公司係於 2003 年創立，總部位於加州 Santa Clara，提供電腦鑑識、發掘電子跡證及網路安全服務、雲端軟體及社交網路監視等服務，有多種產品提供執法機關使用需要。

常見各類軟體介紹：

1. 社交軟體：分為公開頁面及私人頁面，公開頁面係針為任何人皆可觀看之畫面，私人頁面為僅供私密團體或其他已被用戶允許的帳號。
2. 雲端帳號：透過認證取得用戶帳號資訊，但非駭入（依據美國制定之電腦詐欺及濫用法）。
3. 螢幕截圖軟體：Snagit、Ashampoo Snap、FastStone Capture、FullShot Pro、ScreenHunter Pro
4. 畫面爬蟲軟體：FMiner、Helium Scraper、Mozenda、Visual Web Ripper、WebSundew

上述軟體均不可自動蒐集社交媒體資訊，且須人工辨識各

類資訊，而該公司的一對多社交軟體管理應用程式：X1 social discovery 可排程蒐集臉書、推特、Youtube、IG、Tumblr 及其他網站，並下載所有本機資料，依據貼文內容、好友及其他資訊依時間排序產出報告，輸出格式為 PDF、HTML、CSV 及其他格式。



▲軟體執行畫面

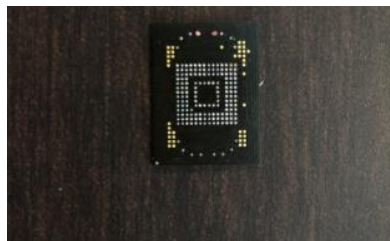
	Public Social Media										Enterprise Social Network		
	Facebook	Twitter	Instagram	YouTube	LinkedIn	Tumblr	Pinterest	Google+	Vimeo	WebSite	WebSite	Jive	Yammer
ArchiveSocial	✓	✓	✓	✓	✓	✓	✓	✓					
X1	✓	✓	✓	✓	✓	✓	✓	✓					
globalRELAY	✓	✓	✓	✓	✓	✓	✓	✓					
gremlin	✓	✓			✓								
MICRO FOCUS	✓	✓			✓								✓
Hanzo	✓	✓	✓	✓	✓	✓	✓	✓		✓			
NEXTPOINT	✓	✓		✓	✓	✓							
PageFreezer	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			
proofpoint	✓	✓	✓	✓	✓	✓	✓	✓			✓	✓	✓
smarsh	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓
Socialite	✓	✓	✓	✓	✓		✓						
SocialSafeGuard	✓	✓	✓	✓	✓		✓				✓	✓	✓
SOCIALWARE	✓	✓			✓								

▲相容網站一覽表

(三) 晶片摘取 (Chip-Off) 數位鑑識

隨著智慧型行動裝置的作業系統版本的不斷更新，安全性也更加提升及強化，不論是 Android 或 iOS 皆然。這的確會對

手機或平板等智慧型行動裝置的數位鑑識取證上造成問題。在取證的層次來說，採取物理提取（Physical Extraction）比邏輯提取（Logical Extraction）能獲取更完整的跡證，然而若當現有的鑑識工具力有未逮時，確有必要考慮採用更底層的取證方式，如 JTAG、ISP 等等。JTAG 一般較廣為人知，除了是做為功能測試機制之外，亦可用於讀取儲存於手機晶片的資料而產生出證物映像檔。至於 ISP 的全名是 In System Programming（線上燒錄），可以此方式直接讀取 eMMC 晶片本身，達成獲取完整證物映像檔的目的。JTAG 或 ISP 此二者皆為非破壞性的取證方式，與之相對的破壞性取證方式則是 Chip-off 晶片摘取，一般而言非到沒有辦法時不會輕易使用，因為採用此方式時須將手機晶片解焊卸下以進行讀取。現今半導體製程技術進步，拆開手機內部通常就只有一顆晶片，內有控制器和儲存晶片，故晶片本身就像一個 USB 隨身碟，使用者使用手機時的一切，包含郵件、好友、個資、GPS 軌跡通通存在這顆晶片上。本團成員在此課程中親自練習操作晶片摘取鑑識流程，拆下課程所提供報廢手機之晶片後直接讀取檔案系統，發現幾乎所有被手機刪除的資料都仍可以還原（據聞 apple 手機除外，因採晶片層級加密）。



▲拆下晶片並進行讀取



▲晶片解焊設備

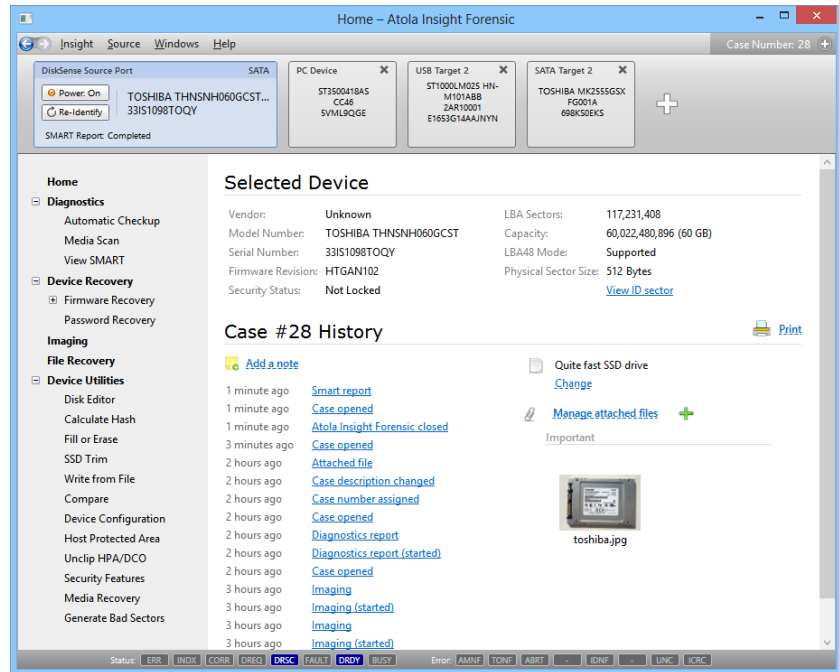
(四) 假照片的數位鑑定

2017年6月4日英國倫敦橋發生恐攻事件，造成多人傷亡。案發後網路上流傳許多宣稱是嫌犯以及嫌犯車輛的假照片，讓英國警方疲於奔命，事後證實許多照片都是偽造或是其他案件的照片。為了釐清圖片是否遭篡改，數位鑑識人員會在圖片的隱藏圖層尋找線索。當編輯圖片時，會留下數位痕跡，例如圖像感測器隨機產生的顏色和亮度變化的不一致。目前已有廠商投入研究利用 AI 人工智慧來辨別假照片，將大量變造過圖片的資料用來測試人工智慧，讓人工智慧從中發現、學習變造圖片的常見模式。經由反覆訓練人工智慧，有可能發現人工難以辨別的偽造影像；惟目前人工智慧仍無法分辨陰影或反射幾

何形狀不一致的高階偽造手法。假照片現今已成為治安、國安隱憂，隨著 AI 人工智慧技術的發展，雖能幫助數位鑑識人員辨識出假照片，但諷刺的是，AI 人工智慧技術的發展亦製造出大量假影像。

（五）快速擷取數位證據

科技日新月異，生活中充斥各種科技產品，滿足人類各種需求。過去觀念認為數位證據隱藏在案件相關人的電腦、手機上，早已不合時宜，智慧家電、智慧手錶、雲端儲存空間都可能發現案情相關證據。需要執行數位鑑識的證物不斷增加，加上儲存技術的進步，數位產品能儲存的空間越來越大，如何在有限時間內快速擷取數位證據成為數位鑑識人員的重大課題。因此，選擇數位鑑識工具，確保證物資料成功擷取固然是第一要務，但若兼顧擷取的速度，完善的資料分類管理，將能大大提升數位鑑識的效率。講師 Yulia Samoteykina 任職於數位鑑識設備廠商 Atola 公司，針對上述需求，介紹產品 Atola Insight Forensic 相關功能，並於會場實機操作，該產品強項在於針對硬碟資料複製、修復，支援支援一對多複製，大幅縮短作業時間，取得完整鑑識映像檔案。未來本局如有相關採購需求，Atola 系列產品或可提供解決方案。



▲ Atola Insight Forensic 操作畫面

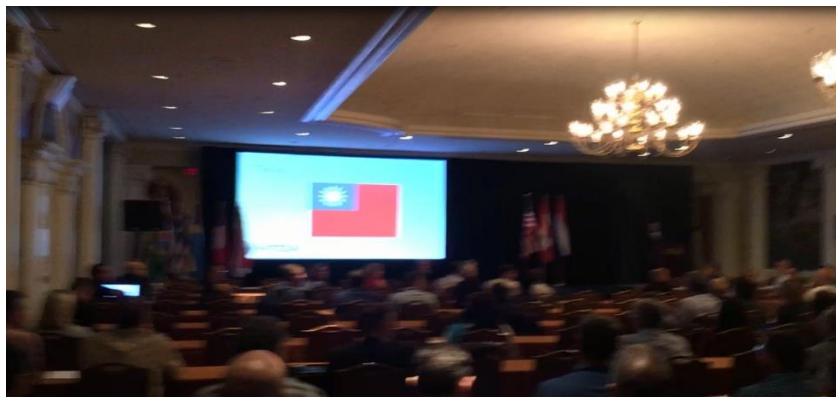
(六) 心理學武器化-社會學及最佳化釣魚之警方詢問策略

DFDR 係顧問公司，透過公開來源情報（如爬梳社交媒體（Crawling social media）並利用心理學及各項技巧探測商業間諜，協助執法機關針對可疑對象進行分析或進行試探攻擊（社交工程），針對典型的幾種人進行了解並辨識弱點（Identifying the vulnerabilities），如年輕人症候群（Youngest child syndrome）；另可利用打斷睡眠循環（Sleep cycle）等技巧使可疑對象陷入易露出破綻的生理情況，該公司呈現出針對嫌疑犯或待調查對象之可能調查方式。

(七) HTCIA 課程中之國際交流

HTCIA 課程一年一度舉行，除了可吸收最新高科技執法知識與技術外，各國執法機關代表齊聚一堂，也是國際執法機關間交流的好機會。最讓團員們難以忘懷的，HTCIA 課程開幕當日開幕典禮主辦單位特地介紹我國代表團，並播放我國國

旗於舞臺前方投影幕上，令團員們感到相當興奮。此外課程之間主辦單位亦精心安排相當多 coffee break，讓各國與會代表們可充份把握機會交流。本次出國團員們也都努力把握機會，與各國執法機關代表交流彼此的經驗與知識，其中包含 HTCIA 主席 Anthony Reyes。Reyes 主席先前任職美國紐約市警局 (NYPD)，擁有相當多國際執法機關人脈。Reyes 主席對於我國團員之積極參與感到印象深刻，特於某日課程結束後邀請我國團員們參加他所特別舉辦 HTCIA member 聚會，加深 HTCIA member 對我國的印象。另挪威警察局、加拿大皇家騎警 (RCMP)、荷蘭政府代表與各課程授課講師們，團員們也都積極交流或交換名片，加深各國對於我國的印象。



▲HTCIA 開幕典禮，大會投影我國國旗並介紹我國代表團

二、參訪行程

(一) 參訪美國蒙哥馬利郡警察局數位鑑識實驗室

該實驗室正式成員共 4 名，另有 4 名其他單位人員機動支援實驗室，故實際從事數位鑑識工作人員共 8 人。鑑識能量部分，該實驗室每年完成數位鑑識之證物數量約一千多件。與本局數位鑑識實驗室相較，雙方人數及鑑識能量均在伯仲之間。本局人員現場詢問對於經圖形鎖保護之手機，該實驗室是否能

夠破解並擷取內部資料，而渠等表示只能針對實驗室現有數位鑑識工具可支援的手機版本進行解鎖、採證；對於無法解鎖之手機，該實驗室僅能紀錄其型號並反應給廠商，建議於下次改版時將該型號手機列入支援範圍。該實驗室不論是正式人員或支援人員，均配有個人使用的數位鑑識工具；本局數位鑑識實驗室囿於經費，必須 2 至 5 人輪流使用數位鑑識工具。因此，若能採購足量數位鑑識設備，威信能有效提升本局數位鑑識能量。

（二）馬里蘭州蒙哥馬里縣蓋瑟斯堡市警察局

蓋瑟斯堡市面積約 26.78 平方公里，大小約等同連江縣（28.8 平方公里），人口數約 7 萬人，約等同雲林縣虎尾鎮，人口密度約大於苗栗縣苗栗市，小於屏東縣屏東市。由於地方自治制度的不同，在美國地方自制並非如我國採階層制，相對於警察機關編制而言，便無所謂的層級差別，所以聯邦警察、洲警、市警、縣警均是平權，沒有隸屬或指揮、督導關係。也因為如此蓋瑟斯堡市的警察招募是由該市直接招募，經宣誓後成為 **Sworn Officer**，而我們在很多英文新聞中，常見的“**Deputy**”其實就是職位在警長局長以下的所有制服警員，蓋瑟斯堡市警察局的 **sworn officer** 約有 57 人，**unsworn officer** 約有 9 人，其中設置警察局長（**Chief of Police**）1 人。

參訪時獲得局長（**Mark P. Sroka**）的接待，並同時進行一個小型的座談及意見交流，美方詢問我方對於密錄器的配置與使用方式，我方則詢問有關數位證物如何解析，以及如何反應治安狀況做出相關作為。美方於近兩年才開始配置值勤員警使用的密錄器，因為美國強調隱私，因此對於密錄器的錄影一直

有爭議，因此連路口監視器的建制也非常謹慎，全市只在重要路口有監視器，數量不到 10 支，而當密錄器成為警察標準配備時，渠等在操作規範，系統上做了很多的設計。以密錄器啟動時機為例，渠設計成自動、手動兩種方案，其中自動部分與配發之槍套以及電擊槍連動，當有拔槍舉動時便啟動密錄器，渠稱因為街頭狀況瞬息萬變，當需要動用武器時，其實已無餘力去開啟密錄器，因此設計為武器觸發的模式，密錄器在回到警局後放到專屬座臺上，便將影像資料上載至伺服器內，該局另有一套系統類似員警工作記錄簿的系統，記錄今日派遣的任務，由處理員警進行記錄，同時結合密錄器影像，因此日後查詢事件時，除有人事時地外，還有當時處理案件的報告、影像。經詢問渠等巡邏勤務出勤後，即在街道上巡邏、待命、機動處理報案，因此勤務時間多數在車上，所以車上配有一台筆記型電腦，當成員警的行動辦公室，相關的報告及文書作業均能在外完成，包含上述填寫工作記錄等工作。

而我方則詢問渠等查扣之數位證物如何解析處理，他們解釋一些重大刑案的數位證物均送至蒙哥馬里縣的數位證物實驗室解析，由於先前提到各警局是平權互不隸屬，因此他們通常會由周邊較小的市集合一些預算到較大的縣，共同出錢購買設備，日後有數位鑑識需求時，便由縣警局協助處理。另外，如何衡量警察局的績效指標時，渠等提到，他們並沒有這樣的指標，地方治安的政策是取決於統計的趨勢，例如上個月某個街區的住宅竊盜件數上升，渠等就會依照熱點時區安排警力加強巡邏，因此相關勤務作為是依照統計數據及報告來擬定，擬定之後於警員出勤時，進行勤前教育提示相關具體作為。

該局的巡邏勤務均是一人出勤，因此巡邏車上的後座，靠近駕駛的後方設置成裝備放置區，遠離駕駛的座位間隔出一個一人獨立空間，類似簡單的拘留室，並有車載攝影機對準該空間進行錄影，由於單警出勤是常態，因此巡邏車的設計非常注意值勤人員的安全。

警察局長與我方相談甚歡，除互相交換警察工作的經驗外並合影留念，該局亦將我方之參訪狀況登載於該局官方臉書粉絲專頁。

(三) 參訪 FAIRFAX 郡警察局

FAIRFAX 郡警察局係目前全美國第 37 大地方警察局，該局位於維吉尼亞州北部，北隔波托馬克河與馬里蘭州相望，人口約有 114.2 萬人，為維州最大的郡，同時也是華盛頓都會區最大的行政區。本次參訪 FAIRFAX 郡警察局，由局長 Chief Roessler 親自接見本局參訪同仁，並由該局 Muhammad 及 Peter Liu 警官導引及協助翻譯，其中 Peter Liu 警官為臺灣人，此舉更顯親切，並與該局電子設備鑑識人員 (Inspector) 及刑事人員 (Detective) 交流執法技巧及偵辦方式，主題如下：

1. 有關監視器影像調閱處理部分，目前監視器影像是該局積極處理之問題，由於美國人注重個人隱私，一般車輛並不裝備行車紀錄器，以免遭路人抗議，各商家也常因私人理由拒絕提供監視錄影，另各監視錄影影片格式不一，難以過濾處理需要的資訊；該局表示不易與各地警察機關合作，如嫌犯使用高速公路逃亡，只有州警才能接收嫌犯過收費站訊息，聯邦調查局之各項資源僅在涉及聯邦罪名之刑事調查下才可能取得，各州使用不同手紋、駕照系統等問題；

另外錄影影片尚有因天氣及時間因素導致車輛外觀顏色變化等諸多問題。我們回應因臺灣監視器密度甚高，一般車輛常為免遭遇車禍難以釐清肇責，故常配置行車紀錄器，且各家銀行及超商配合度佳，故較無監視器影像數量過少的問題，且本局係中央機關，可順利調閱各地警察機關相關影像資料，各商家通常與警方合作，我國問題是影像資料量過多且格式不一，不容易使用資訊系統進行有效率地分析過濾。

2. 美國需由法官簽發搜索令才能執行裝置 GPS 追蹤嫌犯，此處與臺灣相同。
3. 搜索及保存資料：搜索令期限可長達 15 天，保存資料可到 100 年。
4. 詐欺犯罪型態：美國罪犯常使用卡片側錄器於加油站或提款機盜刷信用卡或盜領現金；或是利用暗網（Deep Web）購買駭客取得之被害人個人資料，相對臺灣常見之詐欺樣態（如網拍詐欺）有所不同，但仍有針對退休老人假裝政府官員之詐欺手法。
5. 會後該局致贈本次參訪同仁紀念品及該局簡介。

（四）拜會駐美國臺北經濟文化代表處

本次出國行程非常感謝本局駐美聯絡官的大力協助，參訪部分不僅全程陪同，亦親自接、送機，大幅提升便利性與移動之效率，以利本次出國團員能在有限時程內完成任務，在此特向聯絡官表達感謝。在本局聯絡官安排下，本次行程中亦抽空拜會我國位於華盛頓特區之駐美國代表處。能在異國看到我國國徽，全體團員們有種莫名的感動！團員由我國駐美國台北經

濟文化代表處領務組組長周道元接見，陪同者除本局駐美聯絡官外，還有行政組法務秘書藍家瑞（來自法務部調查局）與領務組秘書陳清福（來自移民署）。過程中談到有關治安議題上，代表處領務組周組長提到，最近美國地區華人常遭遇詐騙集團利用電話，冒充假公安、假大陸領事館人員等技倆，佯稱被害人重要文件未領取，進一步騙得個資，然後偽造北京公安局、檢察院的公文，假冒檢警誣稱被害人涉及洗錢，必須監管其帳戶，否則將強制遣返回大陸，然後要求被害人匯款。據代表處了已有不少案例發生，並有多人受騙，周組長亦曾接到上述詐騙電話。團員們則提到，有關在美華人遭遇電話詐騙一事，今年 7 月由國安局召開之臺、美會議中，本局偵四大隊有針對查獲詐騙在美華人電信詐欺機房案件提出說明，引起美方高度重視。後會偵四大隊並與美國 FBI 駐我國人員取得共識，美方表示將全力協助取得被害人筆錄，共同打擊不法。

（五）參訪 NUIX 數位鑑識軟體公司

該公司介紹數位鑑識軟體，可結合地理及照片等資訊進行資料分析，進一步取得聊天紀錄、電子郵件及檔案等資訊，且可使用關鍵字篩檢，縮小搜尋範圍，目前正在積極研究支援 LINE 資料庫；惟在資料檢視、篩檢速度，則取決於檔案數量及硬體規格。

另該公司的分析及智慧工作臺（Analytics and Intelligence Workflow）類似 I2，可依時間顯示結果，並可透過腳本（Script）找出交集、最短路徑。

參、心得及建議

網際網路與科技產品的發展趨勢，一直以來均提供使用者各式各樣便利的服務，讓使用者能夠在生活的大小事上，得以大幅度地減少空間、時間的限制，兼之個人隱私權意識的抬頭，使原本即具有高度隱匿、易竄改、難以個化等特性的數位資料，更加地無法獲知其原有樣貌；在正常的使用規劃下，為全球性的合作，帶來長足的幫助，惟從另一個角度反向思考，也為非法活動，帶來十分友善的環境。

這些因科技成長後所衍生的犯罪行為，多年來已遍布全球，影響各國的社會、經濟安定甚鉅，早已受各國政府的高度關注，紛紛投入大量人力、物力，嘗試研究、瞭解各類不同態樣的新型犯罪，如何與現實生活結合、蠶食鯨吞人類社會的和諧。

國內對新興科技犯罪的變化，亦有不少的接觸及研討，在便利及安全之間，各領域不時地上演拉鋸戰，試著要在其中取得完美的平衡點；然而，科技無論在深度及廣度，均仍不斷以倍數成長，社會的未來將面臨更加嚴峻的考驗，為了有效地維持民眾的生活環境，更須將現有資源作出妥適的分配，以因應未來更加強大的挑戰。

臺灣雖然在國際間承受不小的壓力，然而並未完全阻止我們對外的發展，與世界各先進國家，均保有密切的聯繫、互助合作；而也正因如此，全球因犯罪行為所產生的動蕩，影響臺灣亦不可謂不重大。故此，建議持續編列相關出國預算，派員參與是類全球性組織所舉辦的各式研討會，即時掌握國際犯罪型態的發展及防制策略，更積極擴展、延續與國際司法機關的合作模式，結合全球性資源，保障國民生命、財產的安全及對政府的信心。