行政院及所屬各機關因公出國人員報告

（出國類別：會議）

國際數位鑑識會議
美國田納西州納什維爾

姓名職稱暨服務機關：
李維哲檢察事務官（臺灣高等檢察署）
周慶鴻檢察事務官（臺灣高等檢察署）

服務機關：法務部
姓名職稱：李維哲　臺灣高等檢察署檢察事務官
　　周慶鴻　臺灣高等檢察署檢察事務官
派赴國家：美國
出國期間：112 年 4 月 17 日至 4 月 23 日
報告日期：112 年 5 月 9 日

摘要

關鍵字

數位鑑識

內容摘要

數位證據在偵查中之比例日趨增加，本署及所屬檢察機關自民國106 年起陸續購置數位採證設備，期提升檢察機關科及偵查之能量。惟國內培訓課程有限，鑑識人員技術能力之培育尚難完全與國際有效接軌。是以，本署為強化「科技偵查中心」之建置與運作，培育檢察機關數位鑑識人才，編列預算選派優秀檢察機關人員至國外參加研討會研習。

本次參與之國際研討會為 Magnet User Summit 2023，於 112 年 4 月 17 日至 19 日，地點在美國納什維爾，田納西州(Nashville, Tennessee, USA)，內容探討數位鑑識最新技術、趨勢，並得與當地執法人員相互交流。

本署預計於今年底通過國際 ISO/IEC 實驗室認證，持續關注國際最新技術知識，故本次選派本署實驗室品質主管、技術主管共計 2 名檢察事務官，參與國際數位鑑識會議，另於 112 年 4 月 20 日參訪當地執法單位之數位鑑識實驗室，進行廣泛交流，收穫豐富。

本文除針對會議內容概述外，另就所學新知提供國內數位鑑識發展及未來受訓相關建議，期提升數位鑑識品質並增進相關人員之專業能力。

目錄

壹、會議內容

一、 全球數位鑑識挑戰與雲端的助力(Global Digital Forensic Challenges And How The Cloud Can Help)

在該會議中探討了全球數字鑑識實驗室所面臨的挑戰，以及雲端服務如何滿足需求，包括可擴展的雲架構、數字鑑識即服務和信息等方面。為了說明這些概念，來自新加坡講者以內政團隊科技局 HTX (Home Team Science & Technology Agency)實際案例探討，並討論一些創新的想法，以獲得支持並讓解決方案更接近現實。

二、 拆解生物群落(Breaking Down the Biomes)

該會議著重在 iOS 系統的生物辨識議題，儘管多個 iOS 版本中都存在 biome 文件夾和相關的 "SEGB" 文件，但最新版本大幅擴展了這些文件的使用。該會議探討最新 iOS 16 的文件系統中幾個不同的生物群落及其用途。會議中展示了檢查數據以幫助鑑識工具的使用（從 KnowledgeC.db 移動），可以揭示留下的已刪除記錄，並探索 iOS 鑑識中一個尚未充分挖掘的新領域。

三、 提升 LevelDB 技能(Level up Your LevelDB skills)

LevelDB 是當今最受歡迎的數據結構之一。這種結構在各種應用程序中變得越來越普遍，實務上極有可能會遇到不受支持的應用程序。在該會議中，講者 Jessica Hyde 為具有數位鑑識經驗的大學教授，深入研究 Google 的開源級數據庫格式，探索其解析方法及有助於調查這些數據庫的開源工具。

四、 TAILS 的取證分析(Does Slicing Onions Make You Cry - Forensics Analysis Of TAILS)

隱私在每個人的日常詞彙中變得越來越普遍。講者分享在過去的五年中，看到暗網市場供應商領域的非法活動激增，由於過量服用芬太尼導致的死亡人數上升，其中許多交易對我們的社區造成了毀滅性影響。許多這些非法交易和活動都是在 TAILS 操作系統內進行的。本次演講說明數位鑑識人員如何在現場收集物理內存和文件系統工件，以及我們可以用來分析收集到的數據以找到與案件相關的工件的方法。

五、 使用 Magnet Forensics DFIR 解決方案更快地調查安全事件(Investigate Security Incidents Faster With Magnet Forensics DFIR Solutions)

當安全事件發生時，數位鑑識和事件響應工作必須迅速而全面，同時能夠隨時隨地收集、分類、處理和分析數據。講者 Trey Amick 介紹涉及多個目標端點的事件響應場景，以了解如何使用 Magnet Forensics 解決方案盡快發現關鍵見解。從構建和執行自動

化工作流程到對端點進行分類，再到分析證據和報告。

六、 顯示未識別 AirDrop 文件的發送電話號碼(Where Did This Come From? Revealing the Sending Phone Number of an Unidentified AirDrop File)

Apple 的 AirDrop 功能雖然是一種方便高效的文件傳輸方法，但最近已被用於分享不受歡迎的裸體圖像以及對公眾的普遍威脅。由於 AirDrop 不依賴網絡提供商、電話號碼或電子郵件地址來傳輸到附近的設備，因此識別未知發件人是有問題的。接收設備可能只能看到用戶定義的發射器的友好名稱，並且沒有任何提供商的傳輸記錄。該會議中演示文稿將討論一種使用在接收設備上找到的日誌來識別 AirDrop 發送設備電話號碼的新技術方法。

七、 將 DFIR 錯誤轉化為機會(Turning DFIR Mistakes Into Opportunities)

數位鑑識這項工作往往伴隨風險，對其中一些錯誤的反應可能會結束職業生涯，也可能會轉化為機會。無論是該領域的新手還是經過數十年經驗的專家，都不可避免地會犯錯誤。然而，數位鑑識人員不僅很少有關於減少錯誤的指導，而且還會因決策不當而在更多錯誤之上加重錯誤。未能保護證據到誤解數據，都可能對案件和聲譽造成不利影響！ 講者 Brett 分享他 20 年來犯下的一些錯誤，以及減輕錯誤和失誤並從中受益的技巧。

八、 Android 提取和分析(Android Extractions and Analysis)

並非所有 Android 提取都是一模一樣的做法。移動設備安全、用戶設置和加密都可以在可用採集類型和證據工件中發揮作用。本次會議僅限執法人員，透過實際案例操作，深入探討 Android 安全和獲取方法。

九、 數位鑑識（DF IRL）現場經驗分享(Lunch & Digital Forensics In Real Life (DF IRL) Live Recording)

已退休的國土安全調查局（HSI）Jim 分享一個關於丹尼爾哈里斯的案例，他是一名頂尖的海軍 F-18 飛行員，在全球範圍內對至少 70 名兒童受害者實施性騷擾。 由於眾多機構所做的出色數字取證和調查工作，哈里斯因其可怕的罪行而被起訴。

十、 使用者自定義腳本 (Custom Artifacts: Supporting the Unsupported)

隨著第三方應用越來越多，沒有任何取證工具可以支持一切。但是，由於自定義工件，Magnet AXIOM 可以提供支持不受支持的構建塊。 本次會議透實際案例實作，了解關於快速有效地定位文件以使用 AXIOM、Dynamic App Finder 和 Magnet Custom Artifact Generator 構建自定義工件的資訊。

十一、 Magnet2Go.支援離線收集(Magnet2Go. Building A 'Windows To Go' Drive To Support Offline Collections)

了解如何使用 Magnet OUTRIDER 和 Magnet ACQUIRE 建立自己

的 Windows To Go 裝置以支援離線資料收集。Magnet OUTRIDER 提供快速搜尋如 CSAM 等非法內容、快速識別系統上可操作證據並收集即時系統資訊，而 Magnet ACQUIRE 提供製作硬碟、隨身碟、ios 及 Android 等裝置映像檔之功能。並可在建立之同一個磁碟上加入其他實時響應工具(如 Magnet RESPONSE)以完善收集現場證據所需的工具。

十二、 Windows 中之遠端訪問跡象(Establishing Connections: Illuminating Remote Access Artifacts In Windows)

在調查過程中，可能會發現有利用現有的遠程訪問工具進行初始訪問和橫向移動之情形。這種趨勢持續上升，由於缺乏可用日誌記錄或不了解可用日誌提供的內容，這種情形往往被忽視不見。本場講者試著提出幾種常用遠程連線工具的日誌紀錄，透過其日誌紀錄及幾種系統事件紀錄，可用以判斷此類遠端登入情形，講者並分享自定義工具，有助於對一些事件進行分析，更好地識別惡意行為。

十三、 將 OSINT 和 DFIR 調查融合在一起(The Tangled Web: Fusing OSINT & DFIR Investigations Together)

會議介紹 Cobwebs 和 Magnet AXIOM 如何探索公開來源情資數據。公開來源情資數據可能存在於外部資料來源中，例如雲和社交媒體平台以及使用 AXIOM 獲取的跡證等。通過將開源情報與取證資料相結合，調查員可以補充他們的調查並獲得比以往更多的數據。Cobwebs 可利用公開來源情資數據查看特定個人的活動，以幫助回

答調查性問題。

十四、 利用 Magnet AUTOMATE 強化數位鑑識(Supercharging Your Digital Investigations With Magnet AUTOMATE)

隨著越來越多的數位資料湧入數位鑑識實驗室，從聊天記錄到地理定位數據、照片、視頻以及其他，獲取證據的時間至關重要。自動化和編排技術可以幫助實驗室加快調查速度，同時讓鑑識人員能夠專注於證據分析。Metro Nashville 警察局探員 Chad Gish 和 Magnet Forensics 顧問 Greg Ward，在會議中展示 Magnet AUTOMATE 如何強化實驗室運作，以提高效率並縮短取證時間。

十五、 透過 DVR Examiner 來提取影像資料(Enhancing Your Video Results By Incorporating DVR Examiner In Your Video Toolkit)

Magnet DVR Examiner 可以幫助從 CCTV 系統中提取和組織數位影像資料，有助於解決從這些系統中識別數位影像檔案和檔案系統的常見問題。本場會議透過實機操作，在講者的引導下，探索 DVR Examiner 並了解如何利用 Magnet DVR Examiner 的掃描、導出和報告功能提取影像檔案並生成報告，有助參加者了解 Magnet DVR Examiner 功能。

貳、參訪內容

一、 參訪納什維爾大都會警察局數位鑑識實驗室(Metro Nashville Police Department)

本次由研討會主辦單位協助聯繫，安排前往納什維爾大都會警察局的數位鑑識實驗室參訪，該實驗室主要協助納什維爾地區的數位鑑識案件。

當日由警探 Chad Gish 說明實驗室現況並帶領參訪人員進行實驗室導覽。該實驗室設施完善，空間包括收件區、證物室、工具間、數位鑑識人員工作區等，實驗室配置高性能伺服器、網路儲存裝置、常用數位鑑識軟硬體、各式維修線材及工具，並有 3D 列印機以製作所需的客製化工具、零件等物，此外並備有車床等重機具以對待銷毀之儲存裝置進行物理破壞，以避免其中所存資料外洩。另外一項令本次參訪人員皆感興趣的實驗室工具是手機充電箱，該實驗室為維持採證手機電源狀態，證物室及鑑識人員工作區皆備有操作便利的手機充電箱，可同時為多隻手機進行充電。

此外，在該實驗室中有 2 項配置是在本國實驗室中較少見的，一是解毒劑，一是排風機，經實驗室人員分享其親身經歷，會有此配置是因曾經發生某手機中藏有芬太尼毒品，鑑識人員獨自 1 人在實驗室中拆開該手機時，芬太尼毒品飛散，致其吸入後中毒，經緊急通報送醫急救後才倖免，所以實驗室在該事件之後即必備解毒劑，並購入排風機，要求鑑識人員有拆除手機需求時，一定要在排

風機中操作，以保障鑑識人員生命安全。

此次參訪中，經警探 Chad Gish 說明，得知該實驗室鑑識人員為專責人員，每年需處理之數位鑑識案件達上千件，近年在利用可自動排程的鑑識軟體協助下，才得以有限的實驗室專責人員，有效率的完成相關數位鑑識工作。在使用自動排程工具前，鑑識人員將待採證裝置連上鑑識軟體並開始採證後，需不定時以人工確認是否已完成採證，待採證完成後，再以人工方式將所採得檔案以鑑識軟體開啟進行判讀並產製報告，透過自動排程軟體之協助，鑑識人員可以將時間集中在報告的分析上，減少鑑識過程無謂人力的耗損。由此可知運用專責人力及選擇合適鑑識軟體，對於日益繁重鑑識工作的重要性。

二、　參訪行動之光基金會(Operation Light Shine)

本次除前往納什維爾大都會警察局參訪其數位鑑識實驗室外，亦前往位於納什維爾地區的行動之光基金會(Operation Light Shine)參訪。行動之光基金會成立的主要目的是支持打擊人口販運和兒童剝削，其下創建特別工作組（INTERCEPT Task Force)，由基金會負責提供特別工作組所需的各式資源，特別工作組下設有數位鑑識實驗室，負責協助調查兒童性剝削和販賣兒童犯罪，以取得關鍵證據，不僅可以起訴罪犯，還可以用確鑿的證據拯救兒童。

當日由基金會人員說明基金會現況並帶領參訪人員進行導覽。參觀其相關辦公空間及下設之數位鑑識實驗室，得知基金會中有專屬律師協助，並規劃有執法人員辦公空間，以供與基金會合作之地方執法部門人員進駐辦公使用。基金會之所以需要設置自有之數位鑑識實驗室，係因其特別工作組除調查工作外，並兼計畫與執行識別、救援被害人之工作，而執法機關所屬的數位鑑識實驗室案件量過多，透過基金會自設數位鑑識實驗室可加快調查速度。

基金會下設之數位鑑識實驗室規模雖不及警察局所屬鑑識實驗室，然該有的高性能伺服器、網路儲存裝置、數位鑑識工具等各式軟硬體一樣不缺，並配置有專屬數位鑑識人員。其與納什維爾大都會警察局一樣透過自動排程軟體之協助，以在有限的人力資源下完成任務。

行動之光基金會為非政府組織，其與司法機關這種密切合作的

方式，在司法機關資源有限的情況下，對於特定案件，確實能有效的達成一定成果，其作法或有值得借鏡之處。

參、建議

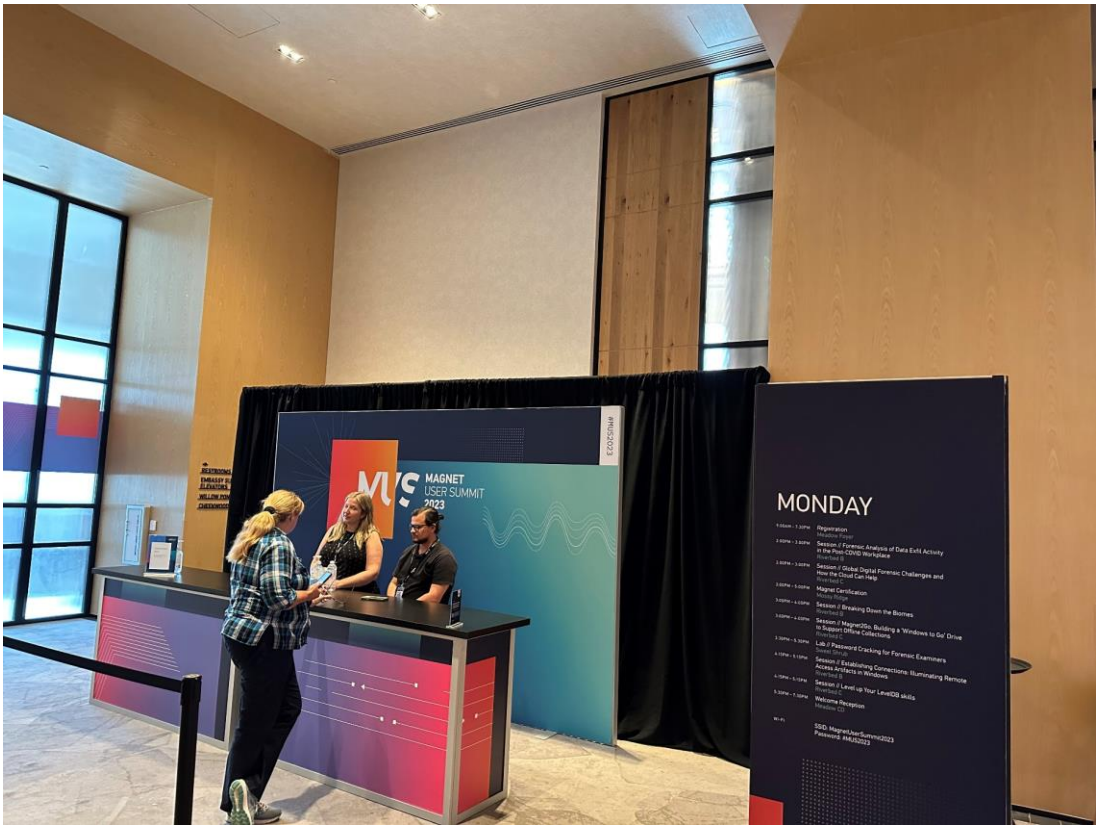
一、　有鑑於我國近年極力推動科技偵查業務，其中數位鑑識業務相關預算大幅增長，各單位積極投入大量資源。為使效益最大化，建議各單位可定期舉辦數位鑑識交流會議，以提升我國整體鑑識能量，並達到資源有效整合運用、避免重工浪費之目標。

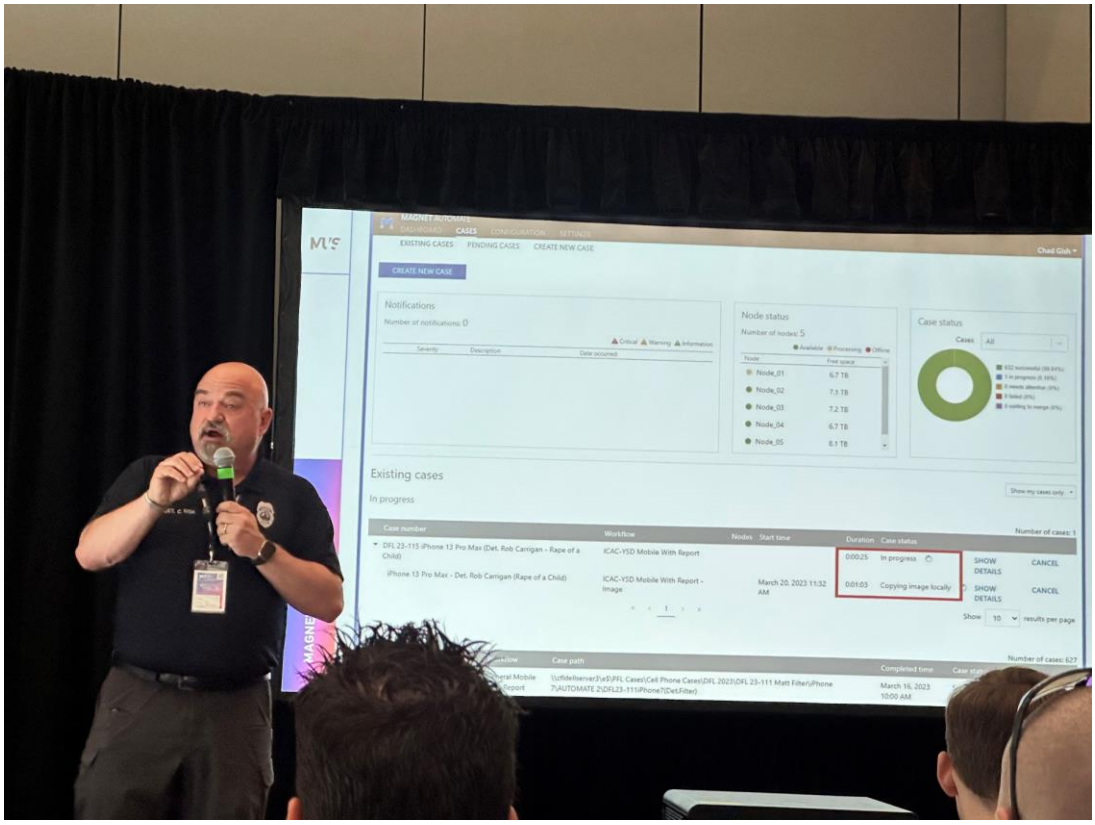
二、　新型態的犯罪手法隨著新興科技日新月異，往往增加辦案之困難度，為了強化專業科技化辦案人員之能力，建議應定期出國參加研討會或參訪國外相關單位，透過國際交流，除可增加我國能見度外，亦可提升人員之視野及專業能力，避免閉門造車。又透過國際交流深入瞭解鑑識工具技術及發展趨勢，亦為直接回饋意見及需求予國外廠商，使鑑識工具發展更符合我國實務上之使用需求。

三、　本次研討會，新加坡內政團隊科技局 HTX(Home Team Science and Technology Agency)亦有參與並分享科技偵查心得，交流後得知該局有從事數位鑑識工作，與本署及我國其他執法單位業務相近。建議未來可派員參訪該局，相互交流、學習優良經驗，借鏡失敗案例，進而提升本署科技偵查之能量。

肆、照片


MAGNET
USER SUMMIT
2023
WELCOME TO
MAGNET USER SUMMIT
2023!


MAGNET
USER SUMMIT
2023
MONDAY


MAGNET AUTOMATE
DASHBOARD
CASES
CONFIGURATION
SETTINGS
EXISTING CASES
PENDING CASES
CREATE NEW CASE
Chad Gish
CREATE NEW CASE
Notifications
Number of notifications: 0
Node status
Number of nodes: 5
Available
Processing
Offline
Node
Free space
Node_01
6.7 TB
Node_02
7.1 TB
Node_03
7.2 TB
Node_04
6.7 TB
Node_05
6.1 TB
Case status
Cases
All
Existing cases
In progress
Show my cases only
Case number
Workflow
Nodes
Start time
Duration
Case status
Number of cases: 1
DFL 23-115 iPhone 13 Pro Max (Det. Rob Carrigan - Rape of a Child)
ICAC-YSD Mobile With Report
0:00:25
In progress
SHOW DETAILS
CANCEL
iPhone 13 Pro Max - Det. Rob Carrigan (Rape of a Child)
ICAC-YSD Mobile With Report - Image
March 20, 2023 11:32 AM
0:01:03
Copying image locally
SHOW DETAILS
CANCEL
Show 10 results per page
Case path
Completed time
Number of cases: 627
March 16, 2023 10:00 AM


Scaling to Cloud
Access via Internet
OSINT / Cloud Forensics
* Credit to Netherlands Forensic Institute (NFI) for their work on DFaaS and Hansken/Xiraf
Cloud Data from multiple sources
DF as a Service
Secure Gov Cloud
Police
Access via Gov Network
Border
Narcotics
Gov Network
Prosecutors
Other LEAs
Physical Device Data from Kiosks/Clients
MAGNET USER SUMMIT 2023
NASHVILLE
MAGNETUSERSUMMIT.COM
#MUS2023