出國報告（出國類別：開會）

Magnet User Summit Magnet 用戶會議

服務機關：法務部調查局
姓名職稱：詹調查官右任、廖調查官昱筌
派赴國家：美國
出國期間：113 年 4 月 14 至 4 月 21 日
報告日期：113 年 6 月 12 日

摘要

為深入瞭解各類數位鑑識議題及新興鑑識技術，以利精進本局鑑識能量，於 113 年 4 月 15 日至 17 日赴美國參加 Magnet Forensics 公司舉辦之 2024 年「Magnet User Summit Magnet 用戶會議」，會議主題包含該公司軟體功能介紹、「Magnet One」等新產品發佈、執法單位數位鑑識心得、技術分享、科技犯罪偵查案例分享及互動實驗室實作等。

4 月 18 日由 Magnet Forensics 公司安排參訪「Metropolitan Nashville Police Department」警察機構行程，透過此本次會議及參訪當地執法機關，能進一步瞭解國際數位鑑識發展趨勢，並透過藉此機會與各國數位鑑識產業專業人士及執法單位進行資訊安全、科技犯罪及數位鑑識技術交流，有助於推動本局數位鑑識領域的深度及廣度。

目次

一、會議簡介及目的

Magnet Forensics 公司於 2011 年成立，總部位於加拿大安大略省滑鐵盧市，專門提供數位鑑識的產品和服務。其主要產品包括數位鑑識軟體「Magnet AXIOM」和手機鑑識與解密工具「GrayKey」等為各國執法機構在數位鑑識方面的重要工具。該公司與執法單位、資安團隊和數位鑑識專家合作，開發數位證據的處理與分析方法，並提供培訓課程和諮詢服務，幫助執法機關充分運用其工具和技術來獲取關鍵證據，以提高調查效率，確保公平和正義的實現。

本次會議旨在提供數位鑑識相關專業人員交流並分享經驗之平臺，議程包含演講、互動實驗室實作、鑑識實驗室參訪和交流會等多種形式，邀請資訊安全、科技偵查及數位鑑識領域等專家擔任主講者，與會者包含鑑識人員、政府執法人員、研究機構及民間企業等，於會議中相互分享國際間新興之技術與發展趨勢，並針對各國曾面臨之案例進行探討。此外，亦於會場展示 Magnet Forensics 公司最新產品並由軟體開發團隊及資深鑑識人員現場回應用戶問題，協助與會者提升專業技能及知識，以期發揮軟體最大效能。

二、參與會議過程紀要

（一） 113 年 4 月 15 日

1. 12:00 報到

上午於美國納許維爾 Embassy Suites by Hilton Nashville Downtown 飯店會議廳櫃臺辦理報到手續，領取參加證及紀念衣，會議廳展場外設有 Magnet Forensics 公司鑑識軟體展示攤位，與會者可直接與軟體開發團隊進行即時詢問及現場操作，並回饋使用情形，同時 Magnet Forensics 公司創辦人 Jab Saliba 亦於現場歡迎與會者的到來。

2. 參加 Magnet Forensics CIO Jab Saliba 及 CFO Bradon Epstein 講授之「Prove it! The Future of Synthetic Media Detection in DFIR」，演講首先指出近年美國公眾人物遭 AI 深偽之事件層出不窮，各大網路社群媒體不斷散播各種偽造影片，造成社會恐慌與民眾對政府不信任，而我國近年亦深受深偽技術危害，並以近期選舉期間最為盛行，而 Magnet Forensics 公司技術團隊開發出能識別人工合成多媒體檔案之演算法以識別影片真偽，在示範案例中指出多媒體檔案中必定會記錄特定資訊，例如：多媒體編碼方式、光圈大小、解析度、感光度(ISO)、時間戳記、使用拍攝程式之版本、鏡頭類型及拍攝裝置類型等軟硬體訊息，並記錄在檔案檔頭中，需透過特殊軟體開啟才能檢視該些訊息，而經深度偽造產生之多媒體檔案必有其特徵，如透過特定深偽軟體製作多媒體檔時，使用軟體名稱、版本或其他資訊會留存在該檔案 metadata 紀錄中，或會竄改參數以偽裝成正常檔案，而 Magnet Forensics 聲稱透過其開發之演算法能鑑別出多數經深度偽造之多媒體檔案，並可指出異常或遭竄改之欄位資訊，俾利鑑識人員判別檔案真偽。

3. 參加 Nardello & Co.公司數位安全部門主任 Joe Pochron 講授之「Investigating a Turncloak:：A Case Study on When AXIOM Cyber and VERAKEY Intersect With a Malicious Insider」，本次主題提到近年美國私人企業面臨商業機密遭竊取外流、個資外洩及勒索軟體等威脅所造成之損失大幅提升，故如何在勒索軟體威脅中，

透過數位鑑識將事件發生經過還原為本次主題重點，講師以案例討論並以 Magnet Forensics 公司開發之軟體 AXIOM Cyber 及 VERAKEY 演示該軟體之在案件中扮演之角色，首先由 AXIOM Cyber 以遠端連線方式蒐集及擷取目標數位證物，縱使目標硬碟被加密 AXIOM Cyber 亦支援外掛插件，可安裝字典檔對加密硬碟進行暴力破解以提取檔案，解決當代取證痛點，另 VERAKEY 主要針對 iOS 行動裝置進行資料擷取（Full Filesystem 模式），若同時有多台 iOS 手機須擷取時，該系統支援自動化擷取作業，大幅節省人工作業及等待時間，且亦支援擷取部分 Android 機種，在取得全部目標證物後能以管線化方式開始分析證物，同時結合電腦端及手機端跡證，大幅提升鑑識分析效率，並在分析結束後產生視覺化關鍵證據及證據來源之關聯分析等功能，俾便察知檔案來源、時間戳記及操作歷程（如檔案開啟、修改或刪除等操作），縱非專業鑑識人員，亦能快速理解該軟體產生之資訊，快速探查可疑事件並協助將跡證彙整，確證犯行歷程。

4. 參加新加坡內政科技局（Home Team Science and Technology Agency, 簡稱 HTX）數位資訊鑑識中心主管 LIM Tuan Liang 及 Magnet Forensics 公司區域經理 Harry KOH 講授之「How HTX Singapore Uses Magnet GRAYKEY and the Magnet Digital Investigation Suite to Prepare for Next Forensic Challenges in Singapore」，本次主題首先介紹提到 HTX 為整合新加坡原先隸屬於不同部門之科技及科研人員，以資源及人員集中管理方式，提高新加坡政府科技科研開發及創新研究，其中數位資訊鑑識中心即為整合原先隸屬於不同司法警察之鑑識人員共同成立之部門。此外，LIM Tuan Liang 介紹 HTX 如何使用 Magnet Forensics 產品，例如 Magnet AXIOM 及 Graykey 進行數位鑑識工作，並提到隨著數位證據容量及數量日趨增加，且不同鑑識工具之介面且適用之證物類型及強項不同，為減少單位購置儲存媒體數量及成本，已開發並佈署「Kiosk」設備於新加坡各地用以連接證物，透過網路連線至集中化雲端系統進行鑑識作業，並且近年致力於推動國際上各家鑑識工具與 Kiosk 設備進行整合，以達到透過 Kiosk 單一介面即可透過後端雲端系統使用不同公司之鑑識工具進行取證。

5. 參加 Magnet Forensics 公司資深資安鑑識專家 Doug Metz 所講授之「Honey, I ransomwared the Kids: Building a Home Lab for DFIR and malware analysis」，本次主題分享如何正確建置安全的惡意程式分析環境，及分析惡意程式時應注意事項，講師提及目前熱門且具有公信力之兩套軟體分別為 SANS（SysAdmin, Audit, Network and Security，系統網路安全協會）之 REMnux 虛擬機器及 Google 公司之 FLARE 虛擬機器，可免費從上述官方網站取得，易於安裝使用並支援多種作業系統，若以本局現有之軟硬體設備，即可迅速搭建惡意程式分析環境，且上述軟體可依單位需求進行個人化更動，故能將該虛擬機器檔案佈署於其他主機以擴大分析能量。本局曾於偵辦電腦犯罪案件時需分析勒索軟體，從遭駭公司取得勒索軟體樣本後帶回分析時，發現該勒索軟體執行時會先偵測目前所在之系統環境，若為虛擬環境或發現網路連線封閉狀況下，該程式不會正常執行，而本次主題提到如何正確設置虛擬網路卡之參數，再透過具備網路分享能力之智慧裝置，以熱點模式分享網路連線於惡意程式所在之虛擬主機，模擬真實網路環境令惡意程式成功執行，且該惡意程式之行為亦不會影響到系統，該方法安全性十足，有利後續分析惡意程式行為。

6. 參加由美國秘勤局 Jason Kan 及 Matt Stephenson 講授之「Building the Next Generation Forensic Lab」，秘勤局隸屬美國國土安全部，除了負責美國正副總統重要官員及外賓特勤安全外，也會辦理金融犯罪及協助其他聯邦政府犯罪調查。本次演講主題著重在美國秘勤局隨著數位證物及金融犯罪猖獗，現行實驗室已經面臨運算能力、儲存空間等限制。Jason Kan 藉由調查時效、預算成本及技術能力等三個面向切入，分享秘勤局將於美國 42 個網路詐欺調查部門規劃建置新世代實驗室方向。

（二） 113 年 4 月 16 日

1. 參加由 Magnet Forensics 公司總裁 David Miles 及 CIO Jad Saliba 講授之「Magnet User Summit 2024 Keynote: The Road Ahead」，本次演講重點為 Magnet Forensics 公司新興技術展示及重要產品發布。Magnet One 為該公司本年度重要發布產

品，主要透過 Web 服務整合公司旗下包含 AXIOM、Graykey、Automate 及 Review 等鑑識軟體。David Miles 提到已往旗下產品著重在單一軟體的功能性，為提升用戶體驗，近幾年開始整合各產品開發團隊，用戶建立雲端儲存空間並透過網路將旗下軟體串聯，透過 Magnet One 一站式服務即可操作 Magnet 旗下軟體，從設定證物鑑識流程、證物分析狀態至分析完成後產製報告，並透過電子郵件寄送連結給指定人員，即可於遠端連線檢視鑑識軟體分析結果。整個過程可完全自動化，縮短鑑識人員作業程序及外勤調查人員取得分析結果之移動時間及硬體資源成本。

2. 參加 Walmart 公司數位安全部門 Aaron Sparling 與 Ashely Bolding 講授之「Windows Subsystem for Linux; Finding the Hidden Penguin」，本次演講重點在如何識別、擷取並分析 WSL（WSL，Windows 子系統 Linux 版，是 Windows 10 版本後內建的功能，讓使用者在 Windows 電腦上無需透過虛擬機或雙開機，即可執行 Linux 環境）內之數位跡證，講師以自身過往經驗，分享有部分案例是發現重要關鍵檔案存放在 WSL 內，因此鑑識 Windows 系統時須特別注意是否有使用 WSL，首先講師指出如何以電腦內之系統檔案、註冊表資訊或路徑等特徵，識別電腦上是否啟用 WSL 功能，接續以各種鑑識工具講授如何擷取 WSL 內之檔案，如 WSL 儲存體使用 vhdx 格式，須利用轉換工具轉為其他儲存格式便能繼續鑑識，及記憶體傾印工具（如 Belkasoft RAM Capture）可匯出當時 WSL 執行中程序之情形，接續講者提到鑑識 WSL 時需特別注意檔案位於儲存體之時間戳記異於外部 Windows 系統本身，故鑑識人員辨識跡證時須特別留意，最後強調鑑識工具僅只是輔助識別跡證，鑑識人員仍須善用多種鑑識工具，並細心、嚴謹地交叉比對每筆跡證之屬性及資訊，切勿僅依據單一跡證便推斷結果。

3. 參加由美國聯邦局調查局 Special Agent Tom Thompson 講授之「Key Artifacts in Child Abduction & Enticement Cases」，本次演講分享聯邦調查局偵辦誘拐兒童案例，透過播放執行逮捕錄音並解說現場狀況，講師強調在現場進行逮捕時，當進入場所時，必須及時控制現場，以避免嫌疑人破壞數位證據。接著，講師介紹 3 種行動裝置鑑識軟體擷取資料技術類型：邏輯提取（Logical Extraction）、

檔案系統提取（File System Extraction）及物理提取（Physical Extraction）及其資料差異，並且提到蘋果 iPhone 手機若無法取得解鎖密碼，請務必保持開機狀態，盡快透過鑑識軟體進行 AFU 模式擷取，以取得更多案關資料。此外講師針對兒童誘拐犯罪實際案例，說明此類案件多半透過交友軟體及通訊軟體進行犯罪，隨著通訊軟體安全及隱私政策日趨嚴格，相關對話紀錄可能已無法還原，鑑識人員可以透過雙方手機其他擷取資料，例如 GPS、手機基地台等資訊抽絲剝繭進行勾稽，也能成為法庭上強而有力的證據。

4. 參加由美國秘勤局 Jason Kane、美國聯邦調查局 Stacy Diaz、加拿大皇家騎警 Jim Stewart 及美國網路安全暨基礎設施安全及（CISA）Artie Crawford 聯合講授之「Enhancing Your Incident Response Playbook With Public-Private Partnerships」，本次演講主題著重在政府部門合作之重要性，因美國及加拿大國土幅員遼闊，各執法單位因地理限制導致聯繫上有難度，起初各單位取得情資後無共享管道、能力有限，導致無法有效打擊犯罪，但在兩國政府密切合作後便建立情資共享機制，傳遞重要情資，並依據單位特性在犯罪偵查中發揮其職能，美加兩國近年便成功共同破獲多起駭客犯罪集團，因此美國及加拿大執法單位在犯罪偵查上合作更為密切，由此演講得到之啟發，未來本局能多與國內各級政府機關密切接觸，加強縱橫溝通管道，並多與重要單位簽署資安合作備忘錄，交換駭侵情資，並將本局偵結之 IOC 分享於簽署單位，作為預警情資，增加其防護能量，亦可多接觸及聯繫有量能之私人機構，如各級 I-SAC（Information Sharing and Analysis Center，資訊與情資分享中心），取得潛在駭客犯罪情資，以預防我國政府遭駭客攻擊，強化本局資安偵查能量。

5. 參加由洛杉磯州警局 Danielle Ponce de Leon 及 Romy Haas 講授之「Google Geofences: Understanding the Fundamentals and Updates」，本場次限定為執法單位參加講座，主題著重在 Google 帳號紀錄地理位置技術介紹，講者提到以往使用者在使用 Google 相關雲端服務時，Google 會在使用者同意下蒐集並記錄使用者手機及連網裝置之 GPS 地理位置，美國執法機關可以透過「Geofence Warrants」向 Google 調閱取得特定帳號的 GPS 定位或是指定時間及地點之相關

裝置及帳號使用者，勾稽相關時間地點以發掘潛在犯罪嫌疑人。然而，隨著用戶安全及隱私意識提升，Google 雖依然會配合執法機關提供特定帳號相關註冊資訊，但將不再提供執法單位調閱特定帳號及特定時間區域 GPS 位置及時間軸資訊，並宣稱 Google 不再於雲端儲存使用者 GPS 紀錄，用戶地理位置相關紀錄將會儲存於用戶裝置內，意味著行動裝置之地理位置資料擷取及分析作業將成為數位鑑識中更重要的議題。

6. 參加 Mandiant Google 公司 Technical Manager, Fernando Tomlinson 所講授之「Ransomware Playbook: Illustrating Artifacts for Enriched Analysis」，演講中提到近年美國備受勒索軟體威脅，受害者及財務損失皆大幅增加，最知名案例為 Colonial Pipeline（為美國東岸最大燃油輸油管線業者）遭 Dark Side 集團勒索數億美金，故防範勒索軟體威脅最佳方式為掌握勒索軟體之特性及攻擊軌跡，講者以實際發生案例及個人鑑識經驗，指出勒索軟體鑑識難點在於多數紀錄皆被加密，須搭配多種鑑識工具交互使用，方能拼湊出事件原貌，講者再以個人累積經驗講解勒索軟體之著手點，解釋如何藉由鑑識軟體還原勒索軟體攻擊軌跡，而從勒索軟體之侵入點、潛伏方式到最後執行加密等不同攻擊時期，可藉此發現單位資安防禦盲點及薄弱之處，反思缺失後，不但能強化遭勒索軟體攻擊時的應變處置能力，更能縮短未來再次遭遇勒索軟體的反應時間，以減輕勒索軟體造成的損失，最後講者指出雖然勒索軟體加密檔案使用之演算法日趨複雜，但攻擊途徑及方法並沒有太大變化，最大破口仍在於人為疏失，如社交郵件攻擊等，故資安的防護重點仍在人的資安意識，提升資安知識便能提高整體資安防護能力。

7. 參加由 Magnet Forensic 公司 CIO Jad Saliba 講授之「Unmasking the Future: Detecting Deepfakes and Revolutionizing Digital Investigations With AI」，本次演講首先介紹近年許多金融詐騙及電腦犯罪使用 Deepfake 深度偽造影音，誘使受害者誤信錯誤資訊導致財務損失，為使鑑識或調查人員能夠快速針對證物進行 Deepfake 影音檢測，講者於現場介紹並展示 Magnet AXIOM 鑑識軟體與微軟進行整合，在該軟體中即可將證物中儲存之圖片及影片上傳至微軟 Copilot AI 工具提供之

三種開源檢測工具進行檢測，並提供低中高等 Deepfake 深度偽造的可能性檢測結果供鑑識人員參考。此外，鑑識人員可以透過提問方式，利用生成式 AI 工具於大量檔案中進行分析，縮短人工檢視案關資料時間成本及提高發現潛在犯罪線索可能性。

（三） 113 年 4 月 17 日

1. 參加 Magnet Forensic 公司資深資安鑑識技術專家 Christopher Vance 講授之「Mobile Unpacked Ep. 16 // Exploring the Possibilities of iOS Shortcuts in Mobile Investigations」，iOS 在 17 版時推出「捷徑」功能，該功能可自動化各種作業，例如取得行事曆中下一個行程的路線、將文字從某應用程式複製到另一個應用程式內或產生特定報告等，相當於巨集之能力，講者指出該捷徑功能十分豐富，若有不肖使用者精心設計一連串捷徑功能，鑑識軟體於分析手機時可能誤判或錯過潛在資訊，因此講者以實際操作手機（iPhone 15 Pro）由簡入繁之方式先設定捷徑功能，並解釋每一種捷徑功能在當時執行情境下，可能影響之系統設定及紀錄，及呼叫應用程式執行之順序及 iOS 系統本身存在之紀錄，便可依此畫出時間軸前後拼湊出完整捷徑功能及其過去執行歷程，便能揭開捷徑功能的神秘面紗，最後講者特別提醒鑑識人員須留意捷徑功能可能驅使的任何程式或行為，及這些操作行為所留下的任何軌跡，皆為鑑識的重點。
2. 參加美國陸軍 NERD（Networking Engineering Research Development）Dave Shaver 講授之「Malware and CSAM－How Do You Prove Malware Did Not Run?」主要講授勒索軟體之重要觀念及鑑識技巧，並輔以鑑識軟體來重現勒索軟體的駭侵歷程，本次主題著重在個案討論。首先講者提出真實案例，展示一部已遭勒索軟體加密的電腦，由此開始展開鑑識調查，首先從 Windows 排程工作發現該勒索軟體建置之一次性工作（該工作目的為加密整台電腦），檢視工作記載之資訊便能追到加密惡意程式之所在位置，再以該程式最後執行時間，比對到 Windows ETL（追蹤記錄檔），發現並鎖定惡意程式之 PID（Process ID）及名稱，便能鎖定所在目錄位置，找到勒索軟體程式本身後即能開始鑑識其攻擊軌跡，

並分享鑑識勒索軟體時須特別注意的檔案及資訊，例如可從 Windows 註冊表、Jumplist、Prefetch 及 shimcache 等獲取勒索軟體的攻擊時序，再將上述調查資訊整合 Windows 本身之 Event Log，即可還原該勒索軟體之入侵途徑及執行情形，再藉其行為軌跡，以修正系統弱點之處，演講最後指出勒索軟體日新月異，鑑識人員須不斷累積個人技術及經驗，才能應處勒索軟體帶來的危害。

3. 參加由 Magnet Forensic 公司 Solutions Consultant Jay Varda 講授之「Magnet for Mobile－Interactive Lab」，本次主題為實作課程，講者首先介紹 Magnet AXIOM 8.0 在分析擷取資料時可顯示為手機模擬介面，提供鑑識及檢視人員更具人性化之介面，並提供數道情境題供參加人員進行實機操作模擬案件調查，其中包含操作手機擷取資料使用微軟 Copilot AI 服務進行調查、通訊軟體關鍵字搜尋技巧以及透過軟體整合手機 GPS、Wifi 資訊及 Google Map 圖資判斷犯罪嫌疑人移動路徑等技巧。

4. 參加由 Magnet Forensic 公司 Consultant, Steve Gemperle 及 Verizon, Associate Director, Tony Balzanto 所講授之「Digital Forensics After the Badge」，講者們在踏入業界前皆任職於政府執法單位，主要業務為犯罪調查及數位鑑識，在職期間接受多種專業數位鑑識課程、取得認證執照，並偵查數以百件以上的刑事案件鑑識，具有相當豐富的鑑識歷練，講者道出專業數位鑑識人員培養不易，且人員流動率大，難以做到經驗傳承，兩位講者目前皆在私人企業從事數位鑑識教育指導及顧問工作，並以技術指導方式協助公家單位進行鑑識，從本次演講，思考個人在本局之工作角色及定位，目前已經歷過各種態樣之數位犯罪，其中不乏特殊案例，就此演講獲得之啟發，個人應將所見所學之鑑識經驗，撰寫繪製成電子文件，便於後期同仁們參考利用，並定期舉辦技術分享等小型讀書聚會，將大家聚集起來討論目前所學之最新技術、分享目前案件鑑識遇到的瓶頸，彼此互相激發討論，利於傳承。

5. 參加 County Cyber Crime Unit, St. Joseph 所講授「Leveraging Digital Evidence: A Comprehensive Approach to Digital Traffic Crash Reconstruction」，本次主題探討如何透過鑑識軟體還原車禍現場及肇事人之當下行為，並從多個車輛事故案例，

逐步帶領大家掌握鑑識重點及技巧，首先必須取得肇事人之手機，以鑑識軟體進行資料萃取後，即可檢視手機內 GPS 定位資訊，如時間戳記、經緯度及使用 GPS 之應用程式等訊息，再由一段時間之經緯度變化可描繪出移動路徑，再經計算後即可得到當時車輛之行駛速度，有上述訊息後便能判斷是否是車速過快導致車禍的發生，另手機也會記錄應用程式使用情形、螢幕鎖定紀錄等其他軟硬體資訊，藉由該些紀錄可判斷肇事人在行為當下是否係因使用手機未注意周遭環境導致車禍發生，整合上述資訊便可還原肇事人之行為，以釐清事故發生原因，還原事實經過。

（四） 113 年 4 月 18 日

參訪田納西州首府納什維爾警察局（址設:600 Murfreesboro Pike, Nashville, TN 37210）之數位鑑識實驗室，由警察官 Chad 帶領本局學長參訪，Chad 在大廳簡單介紹後便引導大家進入數位鑑識實驗室，進入實驗室瞬間即感受到該實驗室案件量之繁重，隨處可見等待鑑識之行動裝置、電腦及 USB 儲存媒體，實驗室中間螢幕可顯示追蹤全部案件鑑識進度，同時也顯示正在擷取中之手機的狀況。整間實驗室配置數臺硬體及運算能力強大鑑識主機，每臺主機可同時擷取 8 支手機資料，證物複本及手機擷取資料則透過網路連線存放在實驗室機房。Chad 表示目前實驗室使用 Magnet Forensic 公司最新產品 Magnet One，該產品整合所有 Magnet 鑑識軟體，其中包含手機破密專用的 Graykey，從收案、資料擷取、跡證分析至報告產出，每一操作皆自動化作業，並透過雲端伺服器儲存鑑識軟體產出之報告，並於完成時同步以 Email 通知送鑑單位，並提供連結供其直接於遠端查看分析結果，以往鑑識人員多數時間是在等待證物擷取及分析時所產生的重複性的替換作業，現在透過軟體整合全部鑑識流程，滿足各階段鑑識需求，使實驗室鑑識能量大幅提升。

三、心得與建議

Magnet User Summit Magnet 用戶會議廣邀全球專業鑑識人員、政府執法人員及業界權威人士於講座經驗分享及案例講述，其中不乏曾經任職於執法單位

並從事數位鑑識工作者，講座內容十分多元，包含資訊安全議題、犯罪調查、勒索軟體之鑑識分析、深偽技術鑑識探討等，於大會前可透過官方網站上取得各項議程之主題、講者介紹及大綱供與會者檢視，並提供線上預約功能，與會者能自由選擇並安排有興趣之議題參與。

透過會議及參訪當地執法單位觀察到一站式服務及數位鑑識流程自動化已為國際近年發展方向。透過整合國際各廠牌鑑識工具，搭配數位鑑識流程使其流程自動化，不僅使鑑識人員更快速地處理大量數據，簡化重複性工作，縮短製作證物映像檔、行動裝置資料擷取、資料分析及匯出等各階段等待時間，也能減少人工操作錯誤機率及頻率，並自動產製相關操作設定及執行紀錄，提升數位鑑識效率，為目前數位鑑識軟體發展主流趨勢。本局於研擬佈署自動化流程前，需經過嚴謹的鑑識工具相容性驗證及良好的網路、運算伺服器及儲存系統等基礎設施，才能確保流程確實執行並且達到預期目的。

隨著 AI 技術發展日益成熟，透過本次會議也了解到生成式 AI 技術於數位鑑識領域應用案例，藉由 AI 技術能夠快速針對數位證物中不同種類資料，例如：對話內容、圖片、電子郵件等大量數據，進行快速處理分析，從中提取關鍵資訊，並透過語言模型生成可能的證據說明或犯罪情節，以幫助鑑識及案件偵辦人員理解案件。然而生成式 AI 也可能因訓練模型及訓練數據及方法不同，而導致分析的數據與真實數據有所不同，因而導致結果不準確，因此在投入實際案例使用時需要進行評估和驗證。此外，使用公開之 AI 雲端服務，可能會有個資及案情等機敏資料洩漏的風險。對此，本局可研擬透過爭取商用雲端服務落地本局機房或自行開發訓練 AI 模型，不僅能夠掌握證物資料流降低洩漏風險，也能夠掌握 AI 模型訓練之方法及過程，以確保結果準確性和可靠性。

本次會議令人印象深刻之內容為美國秘勤局退休之官員，退休後仍不斷研究精進鑑識技術，在私人企業二次就職繼續從事數位鑑識工作，並將所見所學傳授於其他鑑識人員，退而不休的精神令人敬佩，給予現職調查人員職涯發展作為一個最好的借鏡。於會議休息時段，也與各個國家的執法人員交流，討論

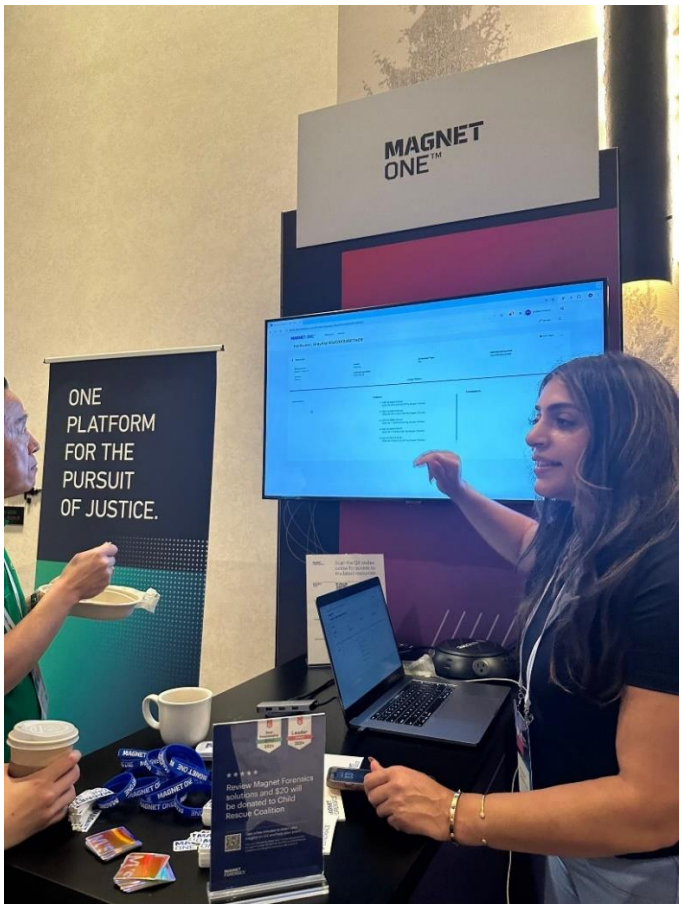
鑑識技術並交換工作心得，也從對談中瞭解各國面對資安領域或鑑識範疇的規範及做法，以利提升各方知能與時俱進。

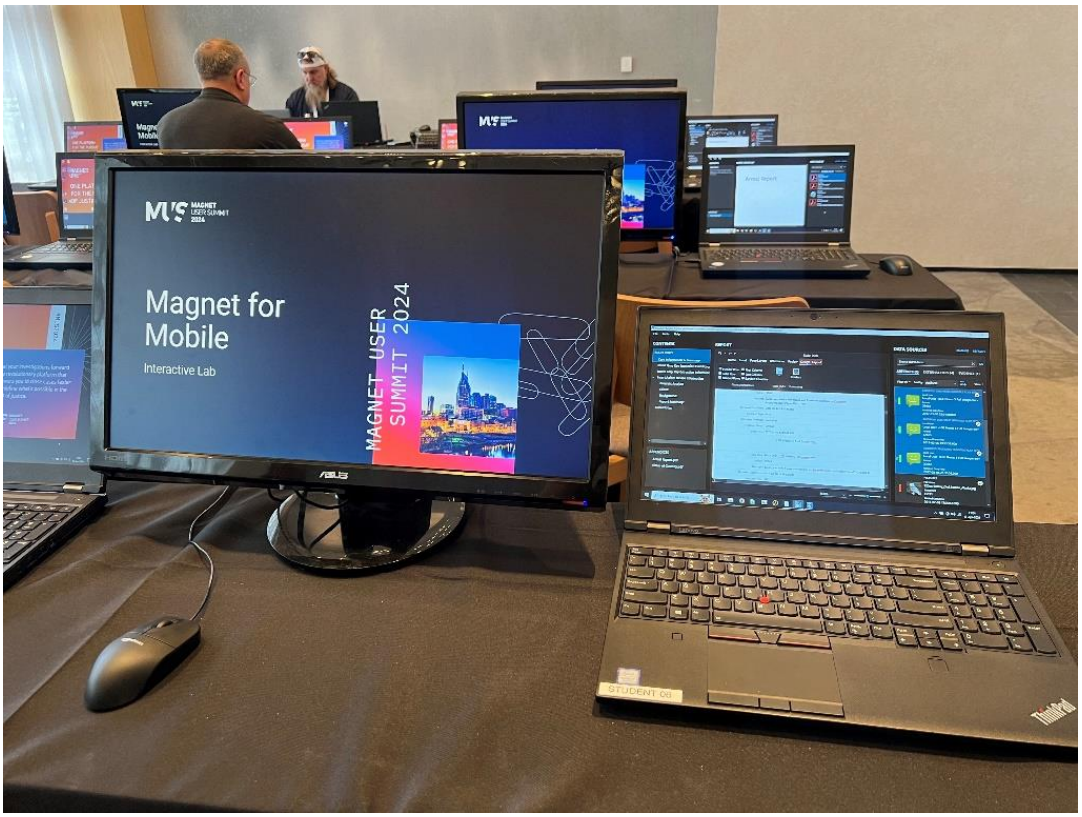
本次行程認識到各國面臨的新形態威脅及挑戰，更學習到各種案件類型的數位鑑識技巧，體認鑑識工作不可太過依賴鑑識軟體，軟體僅是輔助鑑識人員提升流程上的便利性及效率，主要仍要透過自身經驗及技術，從鑑識軟體之分析結果中挑出可用之跡證，拼湊使用軌跡還原事實，故累積個人經驗及技術能力是鑑識人員首要追求的目標。

四、附錄：會場照片暨議程總表

（一） 報到服務及 Keynote 講座

（二） 軟體開發團隊訪談及現場實作講座



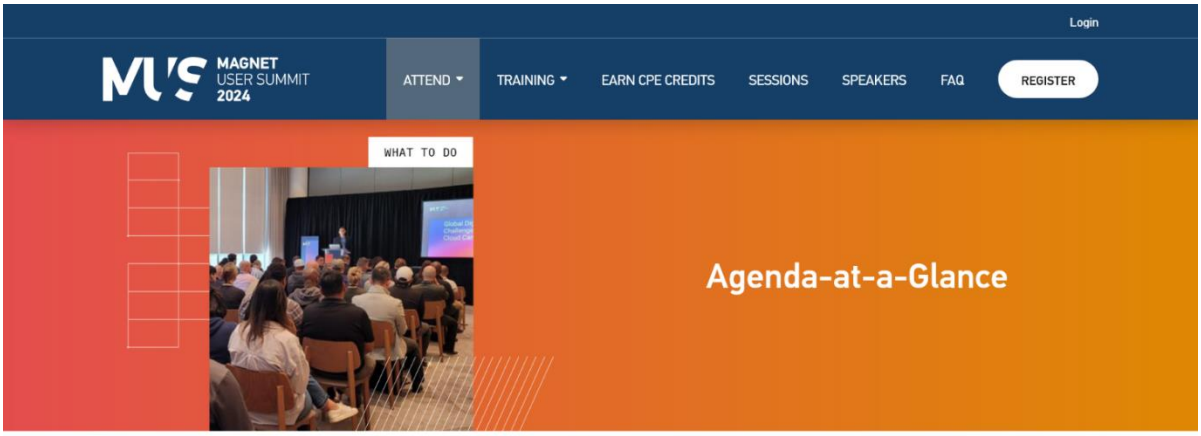


（三） 會議及參訪


MAGNET
ONE™
MAGNET FORENSICS


METRO NASHVILLE
POLICE HEADQUARTER
METRO
POLICE

（四） 會議議程表



Agenda-at-a-Glance

Mon April 15	Registration	10:30 AM - 7:30 PM
	Sessions & Labs	2:00 PM - 5:30 PM
	Welcome Reception	5:30 PM - 7:30 PM
Tue April 16	Breakfast & Registration	7:30 AM - 8:30 AM
	Sessions & Labs	8:30 AM - 12:30 PM
	Lunch	12:30 PM - 1:30 PM
	Sessions & Labs	1:30 PM - 5:15 PM
	Customer Appreciation Event	7:00 PM - 10:00 PM
Wed April 17	Breakfast	9:00 AM - 10:00 AM
	Sessions & Labs	10:00 AM - 12:15 PM
	Lunch	12:15 PM - 1:30 PM
	Sessions & Labs	1:30 PM - 5:00 PM

Prove It! The Future of Synthetic Media Detection in DFIR

Jad Saliba, Chief Innovation Officer, Magnet Forensics
Brandon Epstein, Chief Forensic Officer, Medex Forensics

Monday, Apr 15 | **2:00 PM - 3:00 PM CDT** | Meadow AB

How HTX Singapore Uses Magnet GRAYKEY and the Magnet Digital Investigation Suite to Prepare for Next Forensic Challenges in Singapore

Tuan Liang Lim, Director Digital & Information Forensics, Home Team Science & Technology Agency (HTX)

Monday, Apr 15 | **3:15 PM - 4:15 PM CDT** | Riverbed C

Investigating a Turncloak: A Case Study on When AXIOM Cyber and VERAKEY Intersect With a Malicious Insider

Joe Pochron, Executive Director, Ernst & Young LLP
Jeremy Horowitz, Senior Consultant, EY

Monday, Apr 15 | **3:15 PM - 4:15 PM CDT** | Riverbed AB

iO+S

Jessica Hyde, Owner and Founder, Hexordia
Nick Dubois, Digital Forensics Specialist and Developer, Hexordia

Monday, Apr 15 | **3:15 PM - 5:15 PM CDT** | Sweet Shrub

MCCE - Magnet Certified Cloud Examiner

Monday, Apr 15 | **3:15 PM - 5:15 PM CDT** | Mossy Ridge (Exam Room)

MCFE: Magnet Certified Forensics Examiner

Monday, Apr 15 | **3:15 PM - 5:15 PM CDT** | Mossy Ridge (Exam Room)

MCGE – Magnet Certified GRAYKEY Examiner

Monday, Apr 15 | **3:15 PM - 5:15 PM CDT** | Mossy Ridge (Exam Room)

MCME - Magnet Certified MAC Examiner

Monday, Apr 15 | **3:15 PM - 5:15 PM CDT** | Mossy Ridge (Exam Room)

MCVE - Magnet Certified Video Examiner

Monday, Apr 15 | **3:15 PM - 5:15 PM CDT** | Mossy Ridge (Exam Room)

Building the Next Generation Forensic Lab

Jason Kane, Special Agent in Charge, Secret Service
Matt Stephenson, Technical Special Agent, US Secret Service

Monday, Apr 15 | **4:30 PM - 5:30 PM CDT** | Riverbed C

Honey, I Ransomwared the Kids: Building a Home Lab For DFIR and Malware Analysis

Doug Metz, Senior Security Forensics Specialist, Magnet Forensics

Monday, Apr 15 | **4:30 PM - 5:30 PM CDT** | Riverbed AB

Welcome Reception

Monday, Apr 15 | **5:30 PM - 7:30 PM CDT** | Meadow CD

Magnet User Summit 2024 Keynote: The Road Ahead

David Miles, President, Magnet Forensics
Jad Saliba, Chief Innovation Officer, Magnet Forensics

Tuesday, Apr 16 | **8:30 AM - 9:45 AM CDT** | Meadow AB

Crazy Eight: Exploring Magnet AXIOM 8.0

Preston McNair, Forensics Trainer, Magnet Forensics

Tuesday, Apr 16 | **10:15 AM - 11:15 AM CDT** | Sweet Shrub

What's New in Magnet AXIOM Cyber 8.0

Justin Almanza, Forensics Trainer, Magnet Forensics

Tuesday, Apr 16 | **10:15 AM - 11:15 AM CDT** | Mossy Ridge

Windows Subsystem for Linux; Finding the Hidden Penguin

Aaron Sparling, SR Technical Expert Incident Response, Walmart
Ashley Boldig, Forensics Lead Examiner, Walmart

Tuesday, Apr 16 | **10:15 AM - 11:15 AM CDT** | Riverbed AB

Key Artifacts in Child Abduction & Enticement Cases

Tom Thompson, Special Agent, Federal Bureau of Investigation

Tuesday, Apr 16 | **11:30 AM - 12:30 PM CDT** | Riverbed C

New Kid on the Block: Magnet WITNESS

Thad Winkelman, Forensics Trainer, Magnet Forensics

Tuesday, Apr 16 | **11:30 AM - 12:30 PM CDT** | Sweet Shrub

Optimizing Remote Acquisition by Threat Type

Jean-Francois Brouillette, Practice Lead - IR, National Bank of Canada

Tuesday, Apr 16 | **11:30 AM - 12:30 PM CDT** | Mossy Ridge

Transforming Digital Investigations With Magnet Forensics Solutions

Trey Amick, Director, Technical Marketing & Forensic Consultants, Magnet Forensics
Drew Roberts, Director, Product Management, Magnet Forensics

Tuesday, Apr 16 | **11:30 AM - 12:30 PM CDT** | Riverbed AB

AUTOMATE'ing Your Lab

Trey Amick, Director, Technical Marketing & Forensic Consultants, Magnet Forensics
Greg Ward, Professional Services Consultant, Magnet Forensics

Tuesday, Apr 16 | **1:30 PM - 2:30 PM CDT** | Mossy Ridge

Enhancing Your Incident Response Playbook With Public-Private Partnerships

Stephen Boyce, Director, Magnet Digital Investigations, Magnet Forensics

Tuesday, Apr 16 | **1:30 PM - 2:30 PM CDT** | Riverbed AB

Next Level Investigations with Analyze DI Pro

Lawrence McClain, Training Manager, Magnet Forensics

Tuesday, Apr 16 | **1:30 PM - 2:30 PM CDT** | Sweet Shrub

Advanced Mobile Forensics with VERAKEY & AXIOM Cyber

Matt Fullerton, Solutions Consultant, Magnet Forensics

Tuesday, Apr 16 | **3:00 PM - 4:00 PM CDT** | Mossy Ridge

Magnet Forensics for Public Safety: Integrating Tools and Teams for Smarter Digital Investigations

Trey Amick, Director, Technical Marketing & Forensic Consultants, Magnet Forensics
Curtis Mutter, Director, Product Management, Magnet Forensics

Tuesday, Apr 16 | **3:00 PM - 4:00 PM CDT** | Riverbed C

Ransomware Playbook: Illuminating Artifacts for Enriched Analysis

Fernando Tomlinson, Technical Manager, Incident Response, Mandiant/ Google

Tuesday, Apr 16 | **3:00 PM - 4:00 PM CDT** | Riverbed AB

Unmasking the Future: Detecting Deepfakes and Revolutionizing Digital Investigations With AI

Jad Saliba, Chief Innovation Officer, Magnet Forensics

Tuesday, Apr 16 | **4:15 PM - 5:15 PM CDT** | Riverbed C

Customer Appreciation Event

Tuesday, Apr 16 | **7:00 PM - 10:00 PM CDT** | Off-Site Venue

Magnet User Summit Wrap-Up: Drinks With Product Experts

Drew Roberts, Director, Product Management, Magnet Forensics
Curtis Mutter, Director, Product Management, Magnet Forensics
Joanna Doute, Director, Product Management, Magnet Forensics
Cody Bryant, Director, Product Management, Magnet Forensics

Wednesday, Apr 17 | **4:15 AM - 4:45 AM CDT** | Meadow AB

Mobile Unpacked Ep. 16 // Exploring the Possibilities of iOS Shortcuts in Mobile Investigations

Christopher Vance, Senior Technical Forensics Specialist, Magnet Forensics

Wednesday, Apr 17 | **10:00 AM - 11:00 AM CDT** | Meadow AB

Artificial Intelligence's Impact on Cybersecurity

Ervin Daniels, Senior Security Architect, IBM

Wednesday, Apr 17 | **11:15 AM - 12:15 PM CDT** | Riverbed AB

Case Study: Magnet Exhibit Builder

Steve Gemperle, Forensic Consultant, Magnet Forensics
Chad Gish, Detective, Metro Nashville Police Department

Wednesday, Apr 17 | **11:15 AM - 12:15 PM CDT** | Sweet Shrub

Malware and CSAM - How Do You Prove Malware Did Not Run?

Dave Shaver, Nerd, US Army

Wednesday, Apr 17 | **11:15 AM - 12:15 PM CDT** | Riverbed C

Understanding and Mitigating Advanced Ransomware Attacks: Lessons From the HSE Ireland Incident

Jack Nicholls, PhD Candidate, University College Dublin
Sarah Bibbs, Investigator, St. Joseph County Cyber Crimes Unit

Wednesday, Apr 17 | **11:15 AM - 12:15 PM CDT** | Mossy Ridge

Digital Forensics After the Badge

Anthony Balzanto, Senior Manager, Digital Forensics, Verizon
Steve Gemperle, Forensic Consultant, Magnet Forensics
Lynita Hinsch, Manager, Solutions Consultants, West, Magnet Forensics

Wednesday, Apr 17 | **1:30 PM - 2:30 PM CDT** | Riverbed C

Eyes in the Sky

Christopher Vance, Senior Technical Forensics Specialist, Magnet Forensics

Wednesday, Apr 17 | **1:30 PM - 2:30 PM CDT** | Mossy Ridge

Introducing our Latest Solution for Company-wide Remote Endpoint Investigations

Drew Roberts, Director, Product Management, Magnet Forensics
Tayfun Uzun, Product Director, Magnet Forensics

Wednesday, Apr 17 | **1:30 PM - 2:30 PM CDT** | Riverbed AB

Crazy Eight: Exploring Magnet AXIOM 8.0

Preston McNair, Forensics Trainer, Magnet Forensics

Wednesday, Apr 17 | **3:00 PM - 4:00 PM CDT** | Sweet Shrub

Dive Into Supporting eDiscovery with Magnet Forensics Solutions

Maja Kokotovic, Senior Product Manager, Magnet Forensics
Jeff Bickford, Solutions Consultant, Magnet Forensics

Wednesday, Apr 17 | **3:00 PM - 4:00 PM CDT** | Riverbed AB

Leveraging Digital Evidence: A Comprehensive Approach to Digital Traffic Crash Reconstruction

Mitch Kajzer, Executive Director, St. Joseph County Cyber Crimes Unit
Brianna Drummond, AV/EV Cybersecurity Engineer, Ford
Bianca Burnett, Forensic Research Scientist, University of Notre Dame

Wednesday, Apr 17 | **3:00 PM - 4:00 PM CDT** | Riverbed C