出國報告（出國類別：開會）

赴美參加 Techno Security & Digital Forensics Conference 數位鑑識會議心得報告書

服務機關：法務部調查局

姓名職稱：林科長家舜、陳調查專員兼組長昱龍、廖調查官昱筌

派赴國家：美國

出國期間：112 年 9 月 10 至 9 月 16 日

報告日期：112 年 11 月 27 日

摘要

為了解各類數位鑑識議題及鑑識軟體技術發展趨勢，以利持續精進本局數位鑑識技術，故於 112 年 9 月 11 日至 13 日赴美國參加 COMEXPOSIUM 公司舉辦之 2023 年「Techno Security & Digital Forensics Conference」技術安全與數位鑑識會議，本會議主題包含目前國際各大鑑識軟體公司最新技術展示與產品發布，並針對資訊安全及數位鑑識相關議題舉辦各類講座，9 月 14 日則由鑒真數位有限公司安排參訪本局數位鑑識重要供應商 Logicube 公司，了解設備生產流程並針對本局實際使用情境進行交流。透過本次會議與參訪，能進一步了解國際數位鑑識趨勢，並與各國資安鑑識產業及執法單位進行交流、分享新知及經驗，有助於了解各國執法單位實務運作情形，可供本局數位鑑識發展方向決策參考。

目次

壹、會議簡介及目的

「Techno Security & Digital Forensics Conference 數位鑑識會議」自 1999 年開始舉行，每年分別於美國東西岸各舉辦一場，該會議為專業鑑識人員、政府執法人員及犯罪偵查人員所舉辦，其中包括展示新興數位鑑識技術及現場講座，邀請數位偵查及雲端蒐證等各領域之業界權威或政府執法人員，就電腦、行動裝置等之數位證物進階鑑識相關議題進行研討、交流，並展示介紹最新研發之鑑識工具功能及未來數位鑑識之發展趨勢。

本局規劃「資安威脅獵蒐執法行動計畫」之「資安鑑識新象子計畫」安排專業人員至國外參加新興鑑識技術研討等會議，加深及擴大數位證據及數位資產搜扣範圍，同時為鞏固現場數位蒐證之證據能力，發展符合執法機關偵查及搜扣需求之蒐證工具及程序，協助網路犯罪案件或電信詐欺案件之調查、鑑識作業，本次會議目的為瞭解目前最新數位鑑識技術及其他單位於數位證據及網路犯罪之偵辦方法，以此獲取知識及增加技術深度及廣度，故新增參加旨揭會議符合原訂計畫目標。

貳、參與會議過程紀要

一、112 年 9 月 11 日

（一）於美國加州帕薩迪納 Pasadena Convention Center 會議櫃台辦理報到手續，領取參加證及贈品。會議包含不同主題 Session 及展覽會場。展覽會場有資安調查及數位鑑識等各家廠商攤位展示及介紹產

品，並且安排「Networking Break」及「Happy Hour」供與會者交流。

（二）參加由英國 BlackRainbow 公司首席策略官 Larry Depew 講授之「Case Management & Integrated Quality Management: Why Is this Important for the Future of Digital Forensics？（個案管理與綜合品質管理：為什麼這對數位鑑識的未來很重要）」，講座首先探討為何適用於主流法醫學的傳統認證標準被認為不適用於數位鑑識學的從業人員？根據美國國家科學技術研究院（The National Institute for Science and Technology）的一份研究報告指出，人們對如何實施 ISO 17025 作為數位取證和電子取證組織的品質基礎普遍缺乏了解。透過 Larry 的講授，提供了與會者對於認證模式、流程和標準以及它們如何應用於數位鑑識的一般了解，以及強調實現和維持認證的價值，並確定標準可能不適用的地方。此一課程對於今年 10 月底即將接受全國認證基金會（TAF）現地評鑑，以期取得 ISO 17025 實驗室管理制度認證的本局高雄資安鑑識實驗室團隊成員而言，獲得許多的啓發與幫助。

（三）參加由美國 Sumuri 公司軟體分析師 Andrew Pomerleau 講授之「Everything You Need to Know About Mac Timestamps: Understanding POSIX and Apple Extended Attribute Timestamps」，該講座提及時間戳記為數位證物中重要的證據內容，透過梳理時間順

序可以還原出使用者於該裝置新增、存取、複製及刪除檔案等行為。講者提到在 Apple 電腦作業系統 macOS 為 Linux 為基礎，在其系統中會同時存在 POSIX/UNIX（Linux Base）及 Apple Extended Attribute 兩種時間戳記紀錄方式。Apple Extended Attribute 是專屬蘋果產品 macOS 及 iOS 作業系統的時間戳記，不同 POSIX 時間最小單位只能記錄到整秒（seconds），Apple Extended Attribute 因儲存格式不同最小單位可以記錄到奈秒（nanoseconds），能夠更精確紀錄系統行為的先後順序，在時區方面，POSIX 儲存的格式為 UTC 時間，而 Apple Extended Attribute 則會記錄裝置所在地的時間，故在數位鑑識時務必注意裝置設定的時區對時間的影響，也可以透過兩者比對確認所在地點。此外，Apple Extended Attribute 比 POSIX 提供更多且更細部的時間戳記資訊，例如檔案及資料夾的上次開啟時間及開啟次數，並且將系統的開啟行為與使用者開啟行為紀錄分別紀錄避免造成誤判，可為追溯使用者行為及還原檔案時間軸提供重要依據。

（四）參加「Recovering and Carving Data from SQLCipher Encrypted Databases」，該講座主要說明目前行動裝置 APP 主流使用的資料庫加密方法「SQLCipher」之特徵、架構與解密方法，其解密金鑰可分微生物特徵、PIN 碼或沒加密，常見 APP 如「Wechat」、「snapchat」

之資料庫均使用「SQLCipher」加密。實務上，各國司法警察大多透過執法人員專用手機擷取軟體取得手機內部跡證，如 Cellebrite UFED，但該等軟體支援度有限，特定地理區域使用度較高之 APP 恐無法支援，此時便需要透過此類解密、拆解 Sqlite 資料庫方式提取資料，惟此種方法耗費時間成本較高，並不適合本局投入人力嘗試，或可透過與研究人員或商務合作方式進行。

（五）參加「Cell site analysis -what is that & why you should do it」，該演講係由波蘭 vespereye 公司提出針對基地台位址分析之執行方式、必要性與使用情境。基地台資訊的取得與揭露在各國有不同法律規範，在美國或歐盟，執法人員可透過「Cellhawk」、「ABM INTEL」等軟體來取得基地台資訊，亦可透過「NDCAC」(美國國家家庭通訊協助中心)來協助，可以不需透過電信公司快速掌握涉嫌人之基地台，藉此推斷移動方向或目的地，在執行時有所幫助。在我國亦有相同的機制，但限制較多，目前執行階段多透過警方「即時定位」(民營）與本局「中華電信最終基地台」來輔助，其中警方之定位係採歷史資料加三角定位綜合研判，較易縮小範圍，惟若對象移動範圍小或持有多支手機，仍可能有誤判情形，本局則僅有最終基地台，仍須進一步研判或依賴通訊監察。在實務上，目前偵辦電信詐欺案件中，詐團之工作機均以國外 SIM 卡上網，以國內門號進行通訊監

察實難以發現通聯情形，此時如可執行類似 M 化車之功能，但不需要如此龐大的硬體，如有「Cellhawk」、「ABM INTEL」等產品，單純以軟體方式執行掃描，則可機動掃描與受監察手機相同移動路徑之設備的 IMEI，藉此取得工作機資訊，有效廓清偵查迷霧，我相關機關或可嘗試訪商或找尋類似產品。

（六）參加由美國 Amped Software Inc.訓練師和技術支援專家 Melissa Kimbrell 講授之「Overcoming the Fake News of Deepfakes - Techniques for Video Authentication（克服 Deepfakes 的假新聞-視訊認證技術）」，探討當不知文件來源為何時，我們如何能信任文件？透過本課程講座展示我們該如何開始檢查從公眾或受害者收到的視訊證據，以證明內容未被更改並找到文件的來源。講座首先介紹影像認證（Image Authentication）乃是評估影像檔案是否準確表示聲稱內容的過程，而深度造假（Deepfake） 一詞，即是取自深度學習（Deep learning）和造假（Fake）二字，Deep 係指影像/影片包含由深度神經網路生成的畫素，Fake 則係指影像/影片不再是原始資料或場景的準確表示，實務上是指利用 AI 人工智慧（Artificial Intelligence）結合電腦製作虛假影音。Deepfake 原植根於 GANs 生成對抗網路及自動編碼器兩種型別架構，神經網路原本已是舊技術，但透過近 5 年來 GPU 成為 AI 生成模型主力後，亦即 ChatGPT 引

爆生成式 AI 以來，不論是影片、文字、圖像、聲音類的 AI 技術都隨著加速進步，其所造成的擬真危害使得這世界的一切事物都不再真實(比真實更真實)，人們是否還能相信親眼所見的影像和影片？技術的準備乃是關鍵。對此，講座提出四大可能的解決方法：

1.完整性分析（Integrity analysis）

主動方法：相機在內容中嵌入可信任資訊以保護完整性，使之容易驗證，而使用者必須使用並信任特殊的媒體創建應用程式。

被動方法：分析儲存媒體以檢查與可接受的（acceptable）錄製設備的兼容性，如此可以靈敏且快速的驗證，並依賴龐大且快速發展的資料庫的可用性。

2.傳統的多媒體取證法（Conventional multimedia forensics approaches）

圖像生命週期中的每個處理步驟都會在圖像本身中留下一些獨特的痕跡，故可深入研究所有圖像元資料（metadata）和編碼屬性。此類別包括用於簡單和輔助位元流（bitstream）檢查的過濾器、Exif 和其他元資料提取、JPEG 量化表分析以及與 Amped Authenticate 的內部資料庫的比較，以識別其中所存異常，例如：編輯工具、重新壓縮和自定義標籤（customized tags）等情況。並可檢查出圖片是否源自 Facebook、Flickr、Instagram、Whatsapp、Twitter 等社群媒體平台下載。

3.以深度學習對抗深度學習（Deep learning to fight deep learning）

直接從資料中學習特徵，而不是提取手工製作（hand-crafted）的特徵，二種可能的方法：（1）使用深度學習，但致力於「建議」的分析領域（混合方法/hybrid approach）；（2）讓電腦完成全部工作（完全資料驅動方法/ full data-driven approach）。

4.生理和行為方法（Physiological and behavioral methods）

Deepfake 圖像越來越好，但有時會包含明顯的不一致之處，不過這些問題很快就會解決，因此，高階的一致性分析在未來是必要的，這些人眼幾乎無法察覺的不一致檢測方法包括：眨眼分析（Eye-blinking analysis）、頭部姿勢估計（Head pose estimation）、音位-視位一致性(Phonemes-visemes consistency)及耳朵與口腔動力學(Ear-vs-oral dynamics）等。

（七）參加「Could and network-based Evidence Sources for Malicious insider investigations」，此課程主要說明針對內部惡意竊密、破壞者之調查應注意事項與準備內容，在本局業務中的對應情境為「營業秘密案件中有關數位證據的採證」，講座提到內部惡意人員在整個犯罪流程中可分為準備階段（Search and stage）、數據外洩階段（data Exfiltration）與滅證階段（clean up），在涉嫌人之行動裝置、個人電腦均會產生對應跡證，最大的困難在於滅證或企業並未保存足夠的

資料（或資料遭覆蓋、裝置重置），對此，企業內部可導入 UEBA（User and Entity Behavior Analytics，使用者與實體行為分析），並搭配各類端點管理工具，如 NDR、EDR，同時將日誌導出至 SIEM 或使用權限控管系統，以 AI 自動化方式加強偵測與防禦；另一方面，講座亦建議如企業無法投入太多監控資源，亦可使用 Google Workspace Business 解決方案或其他雲端公司服務方案，該等公司可提供異常詳盡的資料操作歷程監控。對本局案件偵辦而言，在偵辦初期採證時應向公司瞭解有無前揭 UEBA 相關資訊，並注意端點管理工具產出之資料或雲端資料；另一方面，則必須搭配專業資訊人員，採合作方式，由資訊人員解讀專業日誌並與偵辦人員討論日誌能否凸顯竊密竊資行為的動機與犯意，以達到一槍斃命之效果。

二、112 年 9 月 12 日

（一）參加本次大會的主題演講「The DFIR Investigative Mindset: Hack your Mind to rack the Crime（DFIR 調查心態：破解你的思維來打擊犯罪）」議程，主講者 Brett Shavers 將其數十年的精采案例提煉成主題演講內容，生動地以圖例演示如何破解我們的固有思維，進而做到掌握 Digital Forensics and Incident Response（DFIR）的調查思維，同時避免可能破壞我們調查和聲譽的常見陷阱和偏見。無論是初學者還是經驗豐富的調查專業人士，Brett 都提供其實用且相關的提

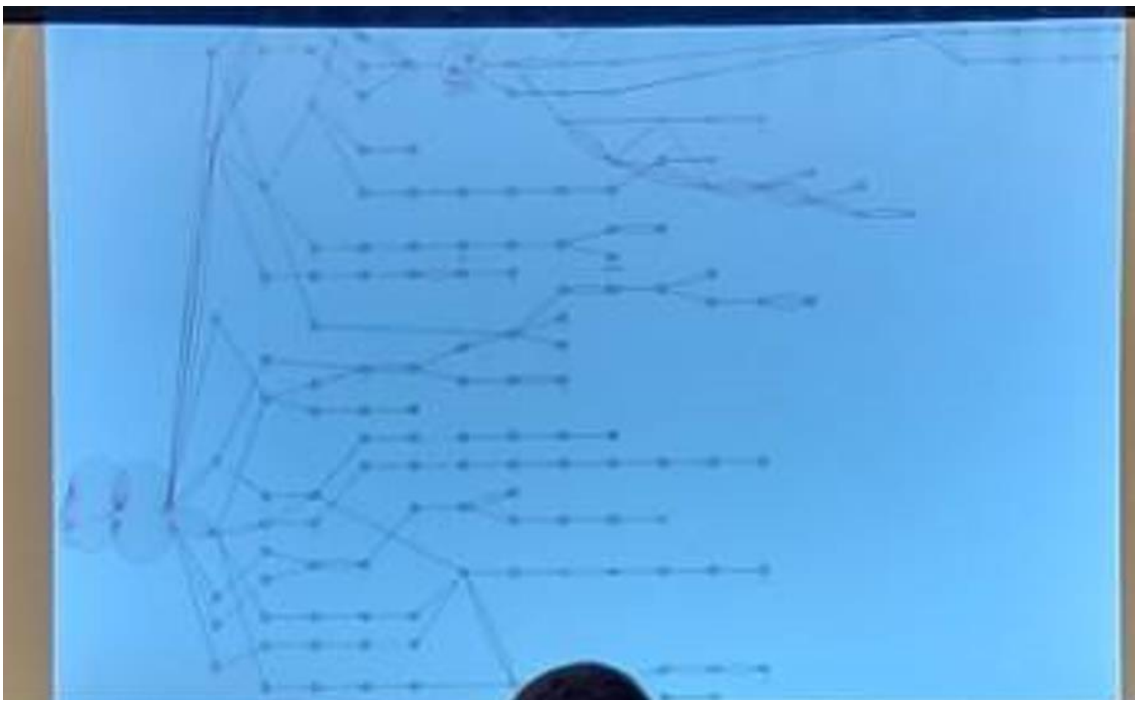
示，促使與會者得以將其提示應用於實際的 DFIR 案例，期能深化而成為個人職涯中的有效指引。

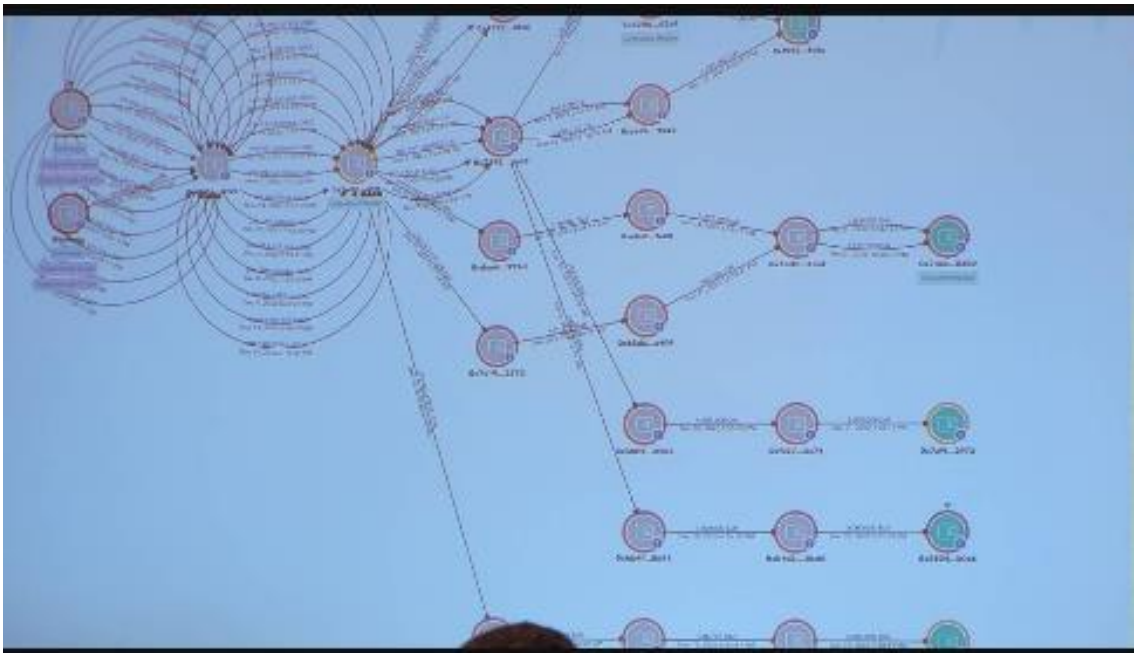
（二）參加「How to indetify and Mitigate hacker Obfusaction Techiques、Forensic Threat Hunting with Digital Evidence」，講述駭客入侵之混淆手法，以及 Threat Hunting（威脅狩獵）之作法、資料來源、內部、外部觀察指標等，講座建議公司應從「劃定邊界」開始，即將竊密惡意行為與數位跡證做出對應，定義出「竊密行為」的觸發條件，當內部人員涉有「超過邊界」之行為時，企業即可展開內部調查與注偵，避免營業秘密遭竊。此演講內容對從事中繼站調查或駭侵事件調查者執行駭侵調查時提供相關基礎知識概念。

（三）參加由 Cisco 公司業務營運主管 Mubashir Hussain 講授之「Solving the Puzzle: How Ediscovery and Investigations Fit Together」（解決困惑：電子取證如何適切與調查工作結合），講座首先指出電子取證和調查是法律程序的兩個關鍵組成部分，但它們通常被視為獨立且不同的做法。事實上，這兩個領域緊密相連，了解它們如何結合在一起對於有效管理法律事務至關重要。Mubashir 並進一步解釋電子鑑識和調查在實務上可以如何相輔相成，以創建更有效率、更有效的法律流程。透過和與會者共同深入探討實際的案例，突顯結合電子取證和調查整體方法的好處，並藉由學習如何解決電子取證和調

查的難題以提升法律實務。

（四）參加「Pig Butchering：An Interactive Case Study」，該課程係限定 LE（Law Enforcement/Police）執法人員之專場，由美國秘勤局洛杉磯分局特別幹員 Derek Wang 分享之「殺豬盤」實案，該案件偵查耗時兩年，犯罪集團一開始切入點是愛情簡訊詐騙，當受害人上鉤後就逐漸轉換為投資詐騙，該案件遇到最大的困難在於金流追查，犯罪集團使用大量加密貨幣地址進行交易，中間並將 USDT 轉換為 DAI 幣規避凍結與調查，層層節點轉換。講座最後以「Outreach!」為題，提出四點建議：增加自我能力（參加 Chainalysis、TRM、CipherTrace 之訓練課程）、教育第一線人員、發展扣押與儲存加密貨幣之程序、與其他地方機關、洲政府、聯邦政府合作，尋求資源。該等建議事件本局多已在軌道上，惟仍可觀察到各類犯罪加上加密貨幣金流後，其調查確有其難度，已非單一機關閉門造車可為，我政府應可在金管會整合之下，擴大包容產、官、學等各界資源，逐步完善各類系統與教學。





圖一、二：加密貨幣地址節點及交易流向

三、112 年 9 月 13 日

（一）參加由美國 V2 Forensics 公司負責人 Jansen Cohoon 講授之「Who's Up There? RemoteID and Drone Forensics」。講座中提及美國聯邦航

空總署（FAA）於 2020 年底發表針對無人機新法規，規範 2023 年開始 250 公克以上之無人機出廠即必須具備 Remote ID 來辨識身份。Remote ID 功能為廣播無人機裝置與遙控裝置或操控者身分及位置資訊，可供其他無人機及飛航管制單位於公開平臺查詢，目前 Remote ID 可採 Wifi 或藍芽通訊技術進行廣播，一般大眾皆可都過手機 APP 查詢附近有哪些無人機，講座中展示目前市面上已出現干擾器可以偽造或是干擾 Remote ID，並提供可供判斷的方式。

針對無人機鑑識取證方面，講者提到大多數無人機只要開啟電源即自動啟動紀錄裝置位置相關訊息，甚至錄製畫面，然而裝置儲存空間有限，若儲存空間已滿則會自動覆寫，可能會造成關鍵資訊遺失，故建議只在必要時開啟電源，並且在需求結束後立即關閉電源以避免資料因覆寫遺失。此外，講座也提到除了無人機本體擷取資料外，因控制器操控需求，可能也會儲存單一或多台無人機設備相關資訊，也可從其中嘗試搜尋飛行相關資訊。

（二）參加由 Magnet Forensics 公司首席鑑識工程師 Matthieu Regnery 講授之「Pressing Snapchat to Extract Juicy Data」，Snapchat 為目前常見行動裝置通訊軟體之一，除了可以傳遞文字訊息外，透過拍攝照片或影片並可快速編輯傳送給好友是此款通訊軟體的特色。講座提到，隨著雲端技術日益成熟，用戶隱私意識提高，許多通訊軟體資

料庫內容皆改以雲端儲存，用戶裝置資料清除頻率提高，並且可能會以加密或雜湊方式增加直接讀取難度。講座分別針對 Andriod 及 IOS 系統剖析該通訊軟體位於手機內資料庫存放位置及解析欄位資訊，部分欄位資訊會被加密或利用函式庫轉換（例如：Andriod 系統之 cache_controller.db 及 IOS 系統之 ClientEncryptionService.plist 檔案等）無法將其直接對應到其他欄位庫進行關聯，因此必須深度分析應用程式與資料庫儲存方式及結構始能反向推出對應欄位，連結出更多資訊．此外，講座也提到依照 Snapchat 的機制大部分的 SNAPS 圖片及聊天文字會在對方讀取之後的 24 小時後自動被刪除，不過應用程式並沒有規範記憶體及快取資料清除機制，可以嘗試取得更多資訊。若手機無法取得資訊，據其他美國執法單位與會者分享，該機關有正式行文 Snapchat 所屬公司取得用戶資料成功案例。

（三）參加「Google Geofence understanding the fundamentals & Dealing with rejection」，該演講亦為執法人員專場，講座透過兩個案件[1]說明「Geofence」（地理圍欄）相關資訊在司法調查上的重要性、分析方法與適法性。Google 公司在 2021 年的營收達到 USD 257.63 BN，其中 80％以上為廣告，而該等廣告均透過「Geofence」搭配

[1] 參考 https://www.eff.org/deeplinks/2023/01/eff-files-amicus-briefs-two-important-geofence-search-warrant-cases

「Advertising IDS」進行推播[2]，這些資訊包含時間、地理位置、裝置名稱，便成為重要的犯罪調查資源。實務上，地理圍欄在調查中仍需要多重證據進行稽核與判斷，亦有誤判情形，但由於廣告推播與地理圍欄無所不在的特性（地理圍欄會參考 GPS、RFID、WIFI、行動網路之訊號），該跡證實已成為重要線索來源，在 2021 年，地理圍欄搜查令占 Google 在美國收到政府命令總數的四分之一，惟我國各司法機關似未與 Google 建立調取管道，此外，地理圍欄資訊係向 google 公司調取特定時間、特定地理範圍之可能連線 RLOI（reverse location obfuscated ID），其法律概念與我刑事訴訟法搜索票聲請或通訊保障及監察法並不相容，恐仍有適法性問題。

四、112 年 9 月 14 日

於上午 10 時參訪位於加州洛杉磯市 Logicube 公司，該公司主要研發數位鑑識證物映像檔製作設備。隨著儲存媒體技術日益成熟，大空間儲存媒體不再僅限於伺服器等級設備，在大眾消費型相關產品也逐漸成為標準配備。硬碟儲存空間的增加也相對增加製作數位證物映像檔所耗費之時間，增加後續證物分析及報告產製時程。對此，公司執行長 Farid Emrani 提到該公司新開發產品 Falcon Neo2 相較於舊款提供更快的硬碟

[2] 用戶在有位置感知服務的設備上開啟了基於位置的服務後進入或離開地理圍欄內的區域時，用戶的設備會觸發警報，並向劃定地理圍欄的服務方發送消息。該信息可能包含用戶設備的位置，而且該信息也會發送到用戶的行動電話或電子郵件帳戶中

讀取速度，以及 USB3.2 及 SAS 3 協定，可縮短映像檔製作時間。此外，為提高實驗室效率及減少手動操作失誤，參訪中與該公司技術長 Gabi Abraham 針對本局資安鑑識實驗室未來規劃數位證物取證及分析程序透過乙太網路及 API 方式結合相關鑑識軟體達到流程自動化，以及本局現行使用狀況進行討論與反饋。最後，由營運長 Chris Hernandez 帶領參訪設備研發、生產及測試包裝流程，了解該公司品保流程及資安規定。

參、心得與建議

一、林科長家舜

每年 6 月、9 月在美東及美西舉行的「技術安全與數位鑑識會議（Techno Security & Digital Forensics Conference）」[3]，舉辦迄今已有 24 年歷史，一直是致力於數位取證和電腦安全產業的私營部門和政府單位與會者極為重要的會議資源。主辦單位用心規劃提供與會者在行前即可註冊登入會議官網，且有專屬的 Mobile APP 可供下載，方便行程管理並掌握即時資訊，讓與會者得以事前瞭解為期三天的會議期程安排、課程內容及講師簡介，得以在同時段進行的多個不同類型課程中，選擇與自身能力、興趣相符或與業務、專長相關的課程，並對選定的課程主題內容預作準備，以利上課時能更加進入狀況。課堂中也感受到外國與會者踴躍

[3] The Techno Security & Digital Forensics Conference 包涵 Cybersecurity、eDiscovery、Forensics、Investigations 及 Sponsor Demos 五個面向的課程，課程並按目標級別（初級、中級、高級或全部）和目標受眾（公司/私營部門、政府、調查人員、執法/警察、檢察官/律師/法律）進行分類。目的是提高國際社會對 IT 安全和數位鑑識領域的發展、教學、培訓、責任和道德的認識。

提問發言，敢於表達個人意見的氛圍，進而能與講座更深入地探討議題內容或表達不同看法，這些都是在華人社會中較為少見的；而擔任課程的講座中，其中不乏多有從執法單位退休的資深探員，例如講授「鑑識個案管理與綜合品質管理」的 BlackRainbow 公司首席策略官 Larry Depew，即在美國聯邦調查局（FBI）擔任探員和數位鑑識實驗室主任長達 31 年（任職期間 Larry 曾帶頭進行長期刑事調查，利用本土技術將數據轉化為可採取行動的情報，另曾擔任數位鑑識檢查員及聯邦調查局地區電腦鑑識實驗室主任），自 FBI 退休後，他建立了一家成功的顧問公司，為國際執法機構和財富 500 強公司提供發展網路安全和數位取證能力、開發風險管理流程以及實施符合 ISO 17025 中定義的認證品質標準的業務工作流程的指導。這種退而不休持續傳承專業及工作經驗的精神，足可作為本局科技偵查專業人才職涯及生涯發展的借鏡；另外，在此次的國際會議課程中，與會者亦得以瞭解工作上所面對的各項問題或挑戰，其在國際上的發展趨勢及解決技術，都是非常寶貴的新知，例如「克服 Deepfakes 的假新聞-視訊認證技術」這門課程中所提到的先進視訊認證技術，即涵括在課程贊助商美國 Amped Software 公司所出品的「Amped Authenticate」圖像驗證軟體，係用於鑑識影像認證和篡改偵測的照片分析軟體，使用單一工具，即可執行多項測試來確定影像是否已遭操縱

（manipulated），並驗證照片是否係從特定裝置拍攝[4]。

二、陳調查專員兼組長昱龍

本次會議安排多場執法人員專場（LE Only）演講，內容包含加密貨幣調查、先進數位跡證、無人機數位鑑識等，透過實案經驗分享、會後交流，可收穫各種寶貴的觀點與案件切入點，實為重要的體驗。建議可以六都（或北中南）為中心，依照業務性質舉辦「案件瓶頸突破討論會」、「偵查技巧分享會」等非正式會議，首先由各業務處選擇各領域案件之專精學長，負責分享偵辦歷程並解答疑難，後由承辦人之間面對面討論案件癥結，透過腦力激盪方式推動案件前進或凝聚問題共識，再借重局本部的力量排除問題，由下而上反向刺激進步成長。

觀察美國秘勤局或警察局的案件調查情形，並非由單一承辦人負責所有案件內容，而是將案件分為程序部分與專業調查部分，以秘勤局為例，本次分享經驗之特別幹員 Derek Wang，在案件中僅負責線索、司法程序、現場執行等，偏向「專案管理」之角色，至於加密貨幣金流分析、扣押物研析、行動裝置 APP 分析等均由其他專案同仁負責，係採專業分工之團隊作戰，此種分工方法可讓專業者更加精進，亦不需耗費時間在彼此均不擅長之事務上，缺點在於需要足夠的專業人力。現今犯罪業已

[4] Amped Authenticate 是一款可進行數位圖像驗證、變造偵測與識別相機彈道（camera ballistics）之工具。它是市面上唯一一個能進行圖像驗證的工具，它提供了許多強力功能的完整套裝來利用數位圖像背後隱含的資料，並提供在證據被用於作為情資或證物前進行影像真實性確認，原始資料驗證、來源及歷史和變造偵測。透過這套工具，可執行許多測試來確保圖樣是否經過竄改以及是否是透過特定裝置被拍攝下來。目前國內係授權鑒真數位有限公司代理。

高度分散化，以電信詐欺案件為例，車手、人頭、一線二線三線機手、水房、外務、幹部、桶主均專業化分工，除少數機房仍有集中外，其餘人員多已分散在不同區域甚至國家之中，其間牽涉的犯罪手法相當專業，特別是在水房部分，非財經或資訊專業人員長時間分析，恐無法有效追查，故建議在偵辦電信詐欺、營業秘密等較專業案件時，應可以改以主承辦加上技術承辦方式推動案件進行。

三、廖調查官昱筌

本次會議不僅包含儲存媒體及行動裝置等數位取證技術，也提及無人機 IoT 物聯網設備取證與 DeepFake 等新興犯罪手法可能觸及的設備技術。除了安排國際數位鑑識廠商展覽產品，並同時舉辦技術講座，提供多元內容並給予與會者自主選擇參加有興趣的議題，與各行業專業鑑識人員相互探討鑑識方法及困境，探討各國間法律及制度的差異，不僅有機會瞭解國際脈動，也進而增加知識廣度及提升技術深度，獲益良多。此外，於會議後參訪設備供應商了解設備生產流程，直接與開發團隊針對產品使用進行回饋，能使鑑識人員更了解設備特性發揮最大效能，並提出本局需求供廠商開發參考，對提高鑑識效率有所幫助。

透過會議與廠商及其他國家執法單位進行交流，可掌握各國執法機關在科技偵查上法律及制度的差異，以及國際數位鑑識技術發展方向及最新應用方式。例如美國因地方自治空間較大，雖然聯邦及各州執法單

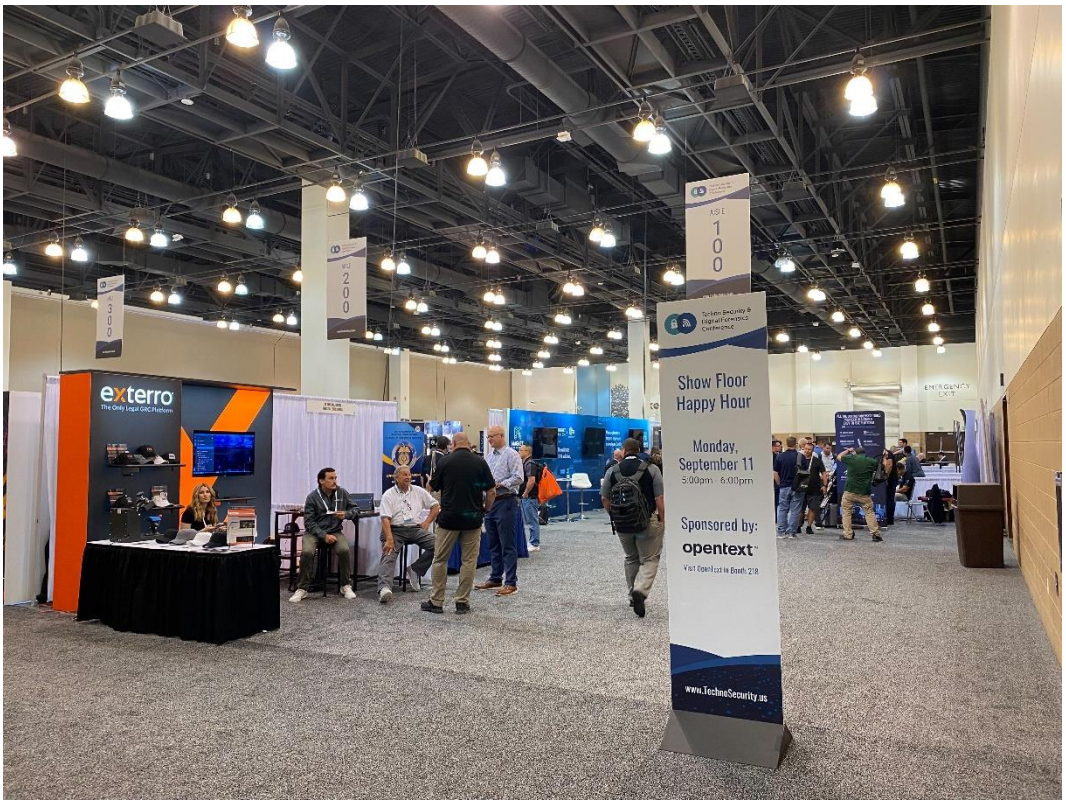
位編制不盡相同，不過在案件調查上人員專業分工及編制較為細緻，技術人員可以全力投入專業領域。此外，觀察到美國納許維爾（Nashville）警察局等不少執法單位在偵查手段及數據利用等規範相較我國法規有較大的空間，已開始利用雲端技術儲存數位證據及基地台資訊等資料作為潛在犯罪調查使用，在數據蒐集應用上有更大的彈性。

數位鑑識流程自動化為近年發展方向，透過整合各家鑑識工具，搭配數位鑑識流程使其流程自動化，不僅可減少製作證物映像檔、行動裝置資料擷取、資料分析及匯出等各階段工作鑑識人員等待時間，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，值得本局研擬參考。

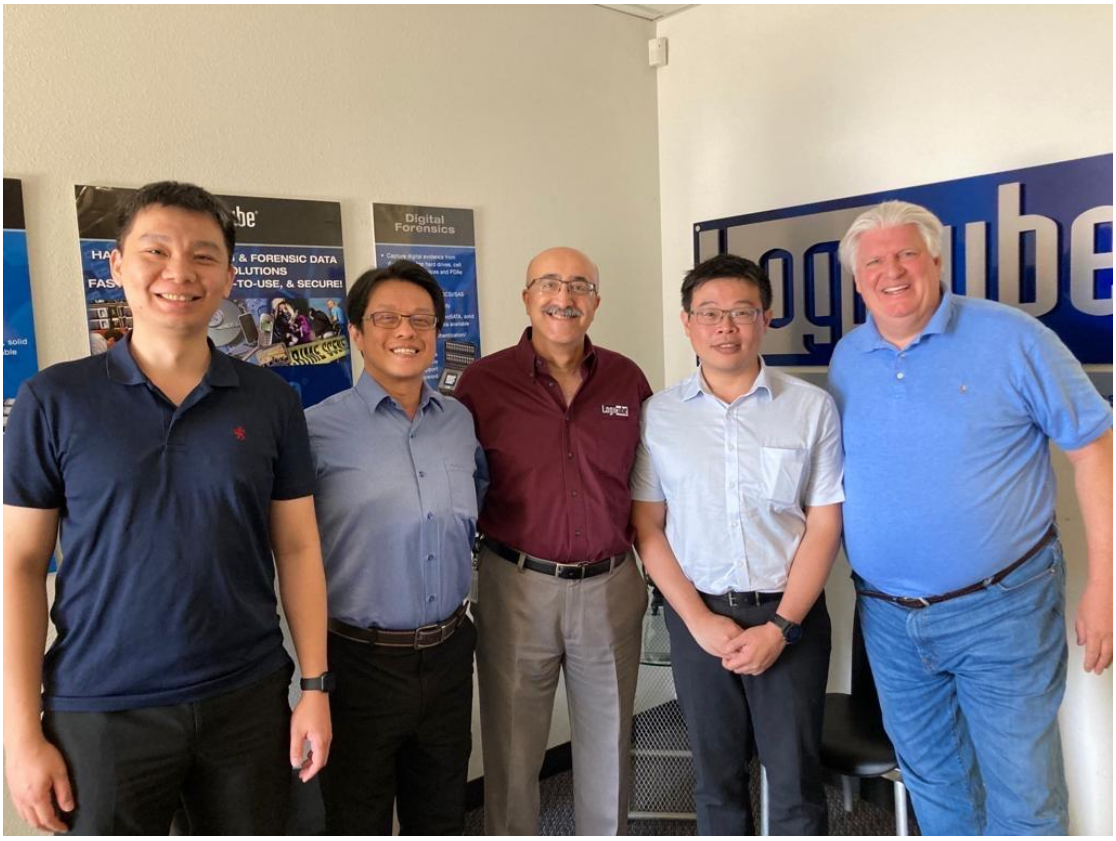
除了技術新知外，會議邀請國際數位鑑識權威 Brett Shavers 分享取證調查時調查人員可能面臨到的思路困境。講者透過常見圖例及邏輯測驗，展示人員的成見及偏見會影響偵查方向的判斷。專業技術及調查經驗固然重要，但每個案件都是獨立的個體，隨著技術發展犯罪手法也日益創新，調查人員務必時常提醒自己避免抱持成見思考導致限縮思路，錯失偵辦方向與時機。

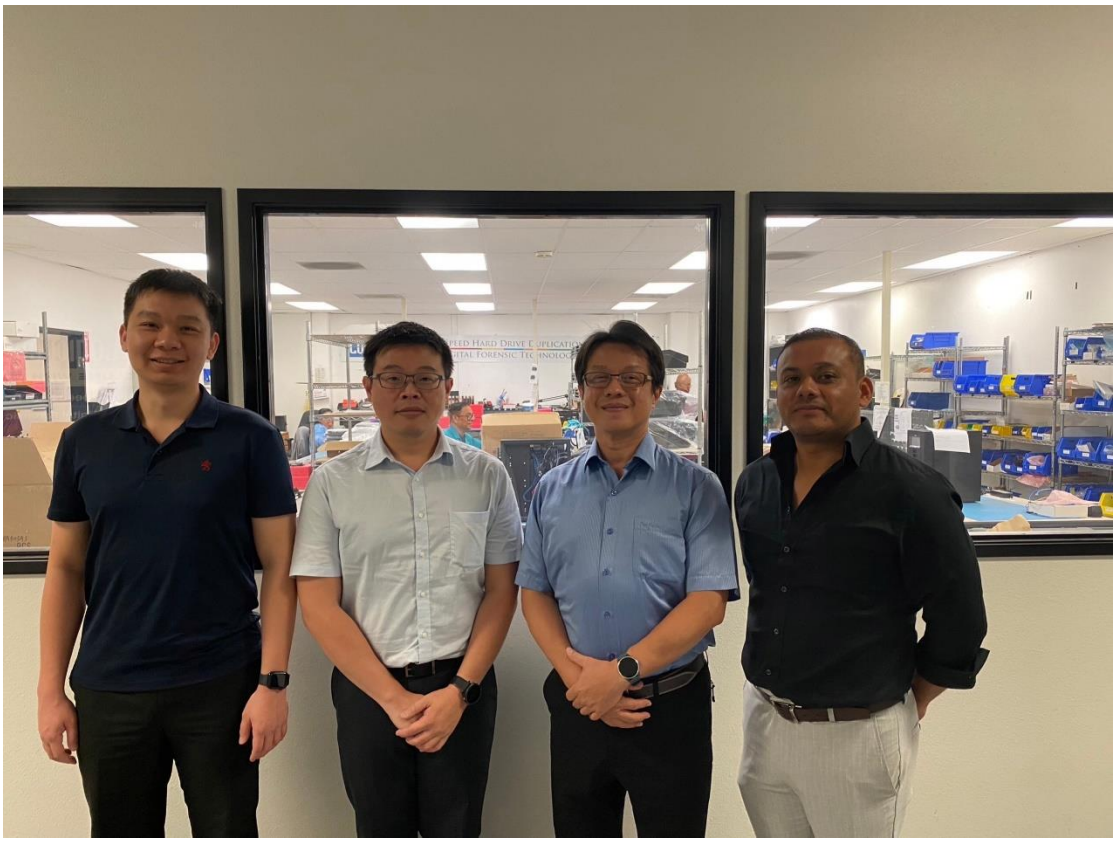
肆、附錄：會場照片暨議程總表

一、展覽會場及議程專題演講



二、參訪





Techno Security & Digital Forensics Conference

Onsite Snapshot Guide

September 11-13, 2023 | Pasadena, CA

Monday, September 11

Time	Function	Speaker(s)	Room
7:30am - 6:00pm	Registration Open		Registration Lobby
12:00pm - 1:00pm	Common Repairable iPhone Logic Board Problems: Fix the Board, Recover the Data	Jessa Jones, iPad Rehab Microsoldering	Ballroom A
12:00pm - 1:00pm	Wireless Visibility: The MUST for Zero Trust	Brett Walkenhorst, Bastille	Ballroom B
12:00pm - 1:00pm	Future Forward – Examining Technology Changes to Plan for the New Realities of Digital Evidence	Ali Kamdar, Oxygen Forensics	Ballroom C
12:00pm - 1:00pm	Case Management & Integrated Quality Management: Why Is this Important for the Future of Digital Forensics?	Larry Depew, BlackRainbow	Ballroom F
12:00pm - 1:00pm	Radio Forensics – What It Is and How It Can Help With Investigations	Dominik Gieralt, Vespereye Eugene Kim, Beverly Hills Police Department	Ballroom G
12:00pm - 1:00pm	Path of a Defense Case	Brandon Reim, Legal Aid Society	Ballroom H
1:15pm - 2:15pm	SPONSOR DEMO: Shaping the Future of Forensics: Your Voice Matters in the Physical Analyzer Ultra Interactive Feedback Session	Matt Goeckel, Cellebrite Mark Tacconelli, Cellebrite	Ballroom A
1:15pm - 2:15pm	OSINT Tools and More	Cynthia Navarro, OSMOSIS	Ballroom B
1:15pm - 2:15pm	Everything You Need to Know About Mac Timestamps: Understanding POSIX and Apple Extended Attribute Timestamps	Andrew Pomerleau, SUMURI	Ballroom C
1:15pm - 2:15pm	Recovering and Carving Data from SQLCipher Encrypted Databases	Matthieu Regnery, Magnet Forensics/ University of Lausanne	Ballroom F
1:15pm - 2:15pm	Trusted Authentication with Unique ID Token	Don Malloy, Initiative for Open Authentication	Ballroom G
1:15pm - 2:15pm	eDiscovery...What's In It For Me?	Laura Anne Day, Epiq Bree Murphy, Exterro Patti Zerwas, Haynes and Boone, LLP	Ballroom H
2:00pm - 6:00pm	Exhibit Hall Open		Exhibit Hall
2:15pm - 2:45pm	Networking Break in Exhibit Hall		Exhibit Hall
2:45pm - 3:45pm	SPONSOR DEMO: Digital Forensic Automation: How Nashville Metro Police demolished their mobile device backlog and accelerated justice with Magnet AUTOMATE	Trey Amick, Magnet Forensics Chad Gish, Metro Nashville Police Department	Ballroom A
2:45pm - 3:45pm	Courtroom Strategies for Mobile Forensics	Matt Goeckel, Cellebrite	Ballroom B
2:45pm - 3:45pm	Accelerating DFIR Investigations & Workflow with Hardware	Manny Kressel, BitMindz	Ballroom C
2:45pm - 3:45pm	iOS Forensics – The Good, The Bad, and The Ugly	Maria Khripun, Belkasoft	Ballroom F
2:45pm - 3:45pm	Actively Engaging the Business in Security Initiatives	John Wallace, RGP	Ballroom G
2:45pm - 3:45pm	Using AI to Improve Your Life - Techniques & Concerns	Richard Greenberg, ISSA Los Angeles	Ballroom H
4:00pm - 5:00pm	SPONSOR DEMO: Filling the Gaps in your Investigations with XRY Pro	Jaime Hauseman, MSAB Kevin Kyono, MSAB	Ballroom A
4:00pm - 5:00pm	SOAR goes SOLAR: How To Utilize (Machine) Learning	Jason Robbins, Amgen	Ballroom B
4:00pm - 5:00pm	Overcoming the Fake News of Deepfakes - Techniques for Video Authentication	Melissa Kimbrell, Amped Software USA Inc.	Ballroom C
4:00pm - 5:00pm	What to Expect When You Are Expecting (to testify)	Don Vilfer, Digital Evidence Ventures	Ballroom F
4:00pm - 5:00pm	Advancing Digital Forensics: Efficient Approaches for On-Scene Investigations	Mike Bates, Detego Global	Ballroom G
4:00pm - 5:00pm	Cloud and Network-based Evidence Sources for Malicious Insider Investigations	Rick Baca, Digital Mountain	Ballroom H
5:00pm - 6:00pm	Happy Hour in Exhibit Hall		Exhibit Hall

Tuesday, September 12

Time	Function	Speaker(s)	Room
7:30am - 5:30pm	Registration Open		Registration Lobby
8:00am - 8:30pm	Morning Coffee		Registration Lobby
8:30am - 9:30am	KEYNOTE: The DFIR Investigative Mindset: Hack Your Mind to Crack the Crime	Brett Shavers	Ballroom B/C
9:45am - 10:45am	SPONSOR DEMO: Taking Your Investigations to the Next Level: Boosting Your DFIR Skills with Belkasoft X	Maria Khripun, Belkasoft	Ballroom A
9:45am - 10:45am	Tackling Collaboration Software, Social Media & Text Messages With a ChatGPT Twist	Addison Bradley, Digital Mountain, Inc. Julie Lewis, Digital Mountain, Inc.	Ballroom G
9:45am - 10:45am	Ask Me Anything: Securing Active Directory from Attacks	Derek Melber, QOMPLX	Ballroom H
9:45am - 12:00pm	The Kidnapping of Alani C. - Dangers of Online Gaming	Colleen Stanich, National City Police Department	Ballroom F
11:00am - 12:00pm	SPONSOR DEMO: Collecting and Analyzing Mobile Evidence in the Workplace	Trey Amick, Magnet Forensics Matt Fullerton, Magnet Forensics	Ballroom A
11:00am - 12:00pm	I've Been Called to Testify! What Should I Expect?	Raul Mejias, Microsoft	Ballroom B
11:00am - 12:00pm	Evidence on Trial: Identifying Digital Evidence Management Best Practices for Compliant and Accelerated Investigations	Ryan Parthemore, Cellebrite	Ballroom C
11:00am - 12:00pm	How to Identify and Mitigate Hacker Obfuscation Techniques	Tony Lauro, Akamai	Ballroom G
11:00am - 12:00pm	E-Discovery and Mass Disasters: How to Respond to Investigations and Litigation	Ronald Hedges, Ronald J. Hedges LLC	Ballroom H
11:00am - 3:30pm	Exhibit Hall Open		Exhibit Hall
1:30pm - 2:30pm	Forensic Threat Hunting with Digital Evidence	Dan Sumpter, Exterro	Ballroom B
1:30pm - 2:30pm	Geolocating Vehicles Using Open Source Data	Stephen Lewington, Berla	Ballroom C
1:30pm - 2:30pm	Data Blackouts – Examining the Causes and Challenges for Law Enforcement When Collecting Digital Evidence and Cloud Stored Evidence Data	Ali Kamdar, Oxygen Forensics	Ballroom F
1:30pm - 2:30pm	AI's Impact to Security	Dr Keith Clement, California State University - Fresno Ervin Daniels, IBM Security	Ballroom G
1:30pm - 2:30pm	Web 3: Embracing Possibilities & Mitigating Risks	Melissa Heidrick, Norton Rose Fulbright/ Women in eDiscovery	Ballroom H
2:30pm - 3:15pm	Networking Break in Exhibit Hall		Exhibit Hall
3:15pm - 4:15pm	SPONSOR DEMO: Mobile Device Faraday Shielding and Charging from Field to Lab	Ryan Judy, MOS Equipment	Ballroom A
3:15pm - 4:15pm	Security Is As Security Does. Law Enforcement's Great Migration To Operating Securely In The Cloud	Trey Amick, Magnet Forensics Kevin Davis, CloudFit Software Joshua Dobyns, Bedford County Sheriff's Office, SOVA-ICAC Chad Gish, Metro Nashville Police Department Scott Montgomery, Amazon Web Services (AWS)	Ballroom C
3:15pm - 4:15pm	Pig Butchering: An Interactive Case Study (LE ONLY)	Andrew Frey, U.S. Secret Service Derek Wang, Los Angeles Field Office, Cyber Fraud Task Force	Ballroom F
3:15pm - 4:15pm	Hacking Demos, Dirty Secrets, Dangerous Lies, and Asset Intelligence	Ken Liao, Sevco Security	Ballroom G
3:15pm - 4:15pm	Solving the Puzzle: How Ediscovery and Investigations Fit Together	Mubashir Hussain, Cisco	Ballroom H
3:15pm - 5:15pm	Using Open Source Tools for Memory Acquisition and Triage	Greg Tassone, Nevada County (CA) District Attorney's Office, Bureau of Investigations	Ballroom B
4:30pm - 5:30pm	In-House Mobile Device Repair in a Forensic Setting ... Do I Need It?	William Aycock, VeriFi Laboratory, LLC	Ballroom C
4:30pm - 5:30pm	Finding a Diamond in the Dumpster: Decoding RAM in Mobile Forensics	Adam Firman, MSAB	Ballroom F
4:30pm - 5:30pm	Vision of a Compromise: Using Data Analytics to Visualize Business Email Compromise Investigations	Joe Pochron, EY	Ballroom G
4:30pm - 5:30pm	Avoiding the Traps and Perils of Engaging in High-Profile/ Public Figure Cases Successfully	Rene Novoa, HaystackID John Wilson, HaystackID	Ballroom H

Wednesday, September 13

Time	Function	Speaker(s)	Room
8:30am - 2:00pm	Registration Open		Registration Lobby
8:45am - 9:15am	Morning Coffee		Registration Lobby
9:15am - 10:15am	Working Smarter - Critical Workflows in Analysis of CSAM	Sherry Torres, Griffeye	Ballroom C
9:15am - 10:15am	Pressing Snapchat to Extract Juicy Data	Matthieu Regnery, Magnet Forensics/ University of Lausanne	Ballroom F
9:15am - 10:15am	The Future of Python and Forensics	Chester Hosmer, Python Forensics	Ballroom G
9:15am - 10:15am	Public/Private Sector Cybersecurity Collaboration – The Key to Risk Management & Cybercriminal Defeat	David Chow, Trend Micro	Ballroom H
9:15am - 11:15am	LE ONLY: Google Geofences: Understanding the Fundamentals & Dealing with Rejection	Romy Haas, Los Angeles County Sheriff's Department Danielle Ponce de Leon, Los Angeles County Sheriff's Department	Ballroom B
10:30am - 11:30am	Transitioning from Public Sector to Private Sector	William Aycock, VeriFi Laboratory, LLC	Ballroom C
10:30am - 11:30am	Who's Up There? RemoteID and Drone Forensics	Jansen Cohoon, V2 Forensics	Ballroom F
10:30am - 11:30am	Sad Face, Happy Face, or Shoulder Shrug? How to Navigate Emojis in E-Discovery	Brett Burney, Nextpoint	Ballroom G
10:30am - 11:30am	The Dark Web and Why It's Important to Your Investigation	Todd Shipley, Dark Intel, LLC	Ballroom H
11:00am - 1:30pm	Exhibit Hall Open		Exhibit Hall
1:15pm - 2:15pm	Hansken – Big Data Forensics	Luc Koevoets, The Netherlands	Ballroom B
1:15pm - 2:15pm	What's in Your Data? You Can't Govern What You Don't See	Sarai Schubert, IPRO	Ballroom C
1:15pm - 2:15pm	Firearms in Digital Multimedia Evidence	Motti Gabler, National Center for Audio and Video Forensics	Ballroom F
1:15pm - 2:15pm	Proactive Threat Hunting: Getting Left of Boom	Matt Lembright, Censys	Ballroom G
1:15pm - 2:15pm	Enhancing Your Case With Digital Communications Exploitation	Darryl Valinchus, PenLink	Ballroom H
2:30pm - 3:30pm	Windows Memory Forensics: Unveiling Digital Artifacts and Collecting Volatile Data	Steven Bolt, Bechtel	Ballroom B
2:30pm - 3:30pm	Introductory Linux Digital Forensics/Incident Response for IT Security and Enterprise Defenders	Thomas Millar, TrustedSec	Ballroom C
2:30pm - 3:30pm	Processing, Reviewing, & Producing Emerging Data Sources (EDS)	Haydn Forrest, Morrison & Foerster LLP Andrew Freiheit, FTI Consulting Collin Miller, FTI Consulting Deedra Smith, FTI Consulting	Ballroom F
2:30pm - 3:30pm	After the Crash: The Application of Digital Forensics in Motor Vehicle Collisions	Jake Green, Envista Forensics Spencer Mcinvaille, Envista Forensics	Ballroom G
2:30pm - 3:30pm	Forensic Investigation of Email Client Tool Marks	Arman Gungor, Metaspike	Ballroom H

Download the Techno Security Mobile App!

Search for **"Techno Security"** in your App Store or Scan the QR Code and download the 2023 Mobile App to stay connected throughout the entire event.

- Get Up-To-Date Show Details
- Download Presentations
- Connect With Other Attendees
- Find Exhibiting Sponsors and More!

Enter Event Code: TSW23

For complete details on downloading and using the app, visit: **www.TechnoSecurity.us/West/AppInfo**

*Please note, due to a recent update, it is necessary to remove any older versions of the Techno Security mobile app from your device and reinstall the app to ensure the best functionality while onsite.

Share photos of your experience with us using the **#TechnoSecurity** tag! Like us on Facebook and Follow us on Twitter and LinkedIn for updates and to stay connected with fellow attendees.

www.twitter.com/technosecurity **www.facebook.com/TechSecNA** **www.linkedin.com/company/techno-security-digital-forensics-conference**