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：潘科長季翔、陳調查官品芳、蔡調查官宇勝
派赴國家：美國
出國期間：113 年 9 月 15 日至 9 月 22 日
報告日期：113 年 12 月 15 日

# 摘要

為了解各類數位鑑識最新議題及鑑識軟體技術發展趨勢，俾利持續精進本局數位鑑識技術，於 113 年 9 月 16 日至 18 日赴美國參加 COMEXPOSIUM 公司舉辦之 2024 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及產品發布，並針對數位鑑識領域新興議題及實務經驗分享舉辦各類講座，9 月 19 日則由鑒真數位有限公司安排參訪鑑識軟體 EnCase 供應商 Opentext 公司，了解業界鑑識軟體發展狀況並針對本局使用情境進行交流。9 月 20 日透過國際事務處協助安排參訪加州橘郡(Orange County)區域電腦鑑識實驗室(RCFL)，借鏡其鑑定技術、報告流程及證物保管等，並針對加密貨幣、人工智慧及數位證物同一性等議題進行討論。透過本次會議與參訪，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及經驗分享，可供本局數位鑑識發展決策參考。

# 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、儲存媒體及行動裝置等數位證物相關議題進行研討、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鑑識技術研討會議，加深及擴大數位證據及數位資產應處能力，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，並持續針對 AI 及虛擬貨幣等新型態資安領域投入研究，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、 113 年 9 月 16 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) 趨勢科技威脅情報部門副總裁 Jon Clay 主講之「公與私部門合作最佳實踐-LockBit 集團打擊行動案例」(Best Practices in Public/Private Sector Collaboration – LockBit Takedown) 分享與 FBI(美國聯邦調查局)及 NCA(英國國家犯罪局)的合作，成功打擊了在 2023 年佔全球約 25%勒

索病毒事件的 LockBit 駭客集團。該集團的運作方式是透過網絡攻擊和漏洞滲透進入機構內部系統，利用自動化工具來加密受害者數據，然後以公布或揭露敏感資料為要脅，迫使受害者支付比特幣等加密貨幣來解鎖數據。在偵辦行動中，私部門提供威脅情報的資安公司發揮了重要作用，協助識別和封鎖 LockBit 勒索病毒行為，並與執法機構持續協作與資訊共享，經過持續數月的調查行動，LockBit 集團多個重要成員被逮捕，並成功取得勒索軟體金鑰，為我國未來跨部門交流合作提供寶貴經驗和最佳實踐。

(三) Detego Global 經理 Javis Olson 主講之「Enhancing Digital Forensics Efficiency: Triage, Selective Extraction, and AI Methodologies」提到，鑑識人員目前須面對諸多困境，例如電子設備日益增加的儲存容量，動輒達數 TB 以上，面對如此龐大的資料數據，該如何選擇重要的資料進行擷取；必須注意擷取資料過程中侵犯到證物主人的隱私；資料可能被加密、混淆及多因子認證，擷取難度增加。為增加鑑識人員效率，講者建議制定準則是必要的，例如取證流程、不同類型證物的取證方法、簽章及稽核日誌需確保為可供審查的狀態等等，另外，AI 及 ML(機器學習)能夠幫忙處理龐大數據及分類，惟任何 AI 給出的建議或產物皆有可能存在偏差，因此調查人員須參與所有 AI 活動，準備不同資料環境訓練ＡＩ，並適時驗證其合理性及準確性。

(四) 參加「Unmasking Deception in AI-Generated Images」專題演講，由拉斯维加斯警察局偵查佐及數位鑑識專家 Jeff Lomas 分享，課程中講述生成對抗網路(GANs)、深度學習(Deep Learning)及卷積神經網路(CNNs)之概念，說明圖像辨識、物體檢測及影像分類等多媒體檔案之分析原理。特別探討類神經網路仿人類視覺處理圖像處理過程，包含自圖像中分析不同層次特徵，用於對圖像進一步分類或其他操作等。課程中提供執法人員識辨是否為 AI 生成圖像之方法，如檢查 Metadata 資訊是否完整、是否有浮水印、研究相機像素值偏差方式輔助識別及圖像合

理性識別等，提供執法人員未來針對生成式 AI 圖像之檢測方向。

(五) MSAB 漏洞研究經理 Martin Westman 主講之「I Swear, I Have Never Seen That Image Before! That Statement Can, in Fact, Be True in Devices with Reused Memory Chip」提到，二手市場中流通著大量 TSOP NANDs 記憶體，多數被利用為廉價或盜版 USB 設備，該記憶體無法儲存原有紀錄，因其需額外搭配 Contoller 並進行一連串計算才能儲存資料，若 TSOP NANDs 記憶體沒有搭配到適合的 Controller，相當於資料無法救援了；新一代記憶體 eMMC 將 Controller 與晶片設計在一起，大幅增加資料救援機率，就算使用者輸入格式化指令，大部分「0」與「1」電磁紀錄仍保存在記憶體中，就算換了個 USB 載體仍可能存留個人機敏資訊，故講者建議，若須丟棄隨身碟，最好使用專業工具抹除資料，或是使勁地存入大量影音檔案來覆蓋原有資料。

二、 113 年 9 月 17 日

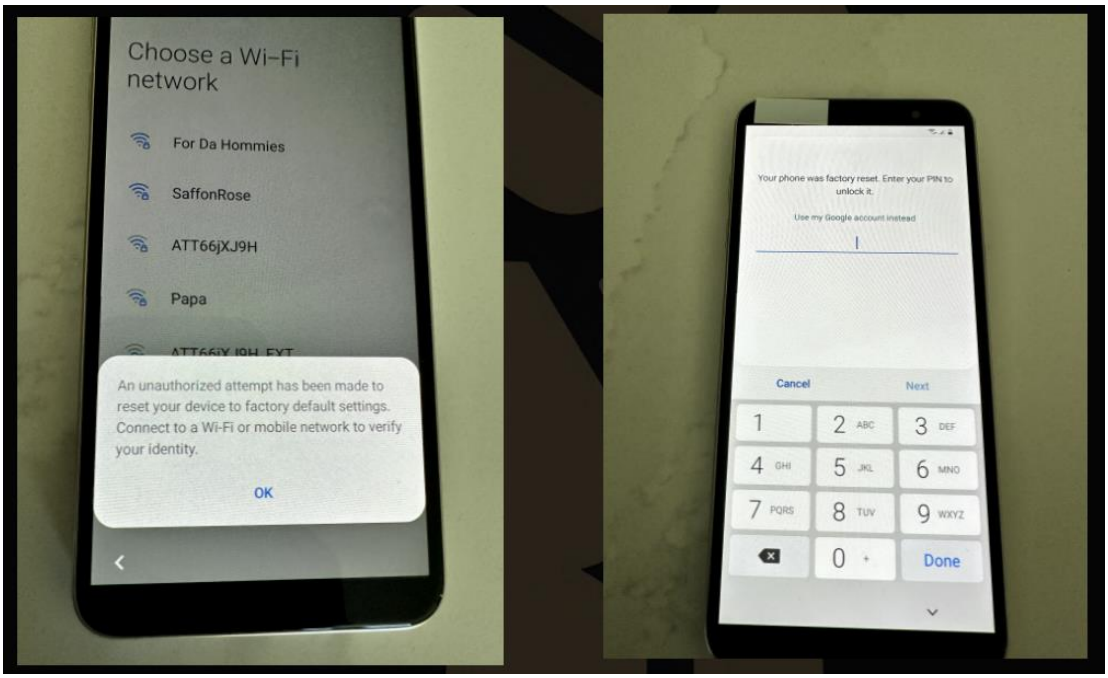
(一) MSAB 漏洞研究經理 Martin Westman 主講之「恢復原廠設定之手機，遊戲結束了還是可以挽回？」(Factory Reset'ed Phone, Game Over - Or Is It?)說明當手機經過原廠重設後，雖然通常會刪除用戶資料、應用程式和相關設定，並將設備恢復至出廠狀態，但並不一定意味著所有數據都會被完全消除，仍然是有可能進行數位鑑識取得證據，包括加密區塊中未遭覆蓋的數據及檔案碎片，SIM 卡中的通話紀錄、簡訊、聯絡人等資料，microSD 卡等外部儲存裝置的文件、圖片等資料，過往曾同步至雲端的資料，保持開機手機的隨機存取記憶體(RAM)內未被清除的資料，以及某些網路活動留下的 IP 位址等紀錄。因此，利用專業工具和技術，仍可能檢索到原廠重設後殘留的數據，而這些數據可能成為案件的關鍵證據。

(二) 聯邦調查局幹員 Peter Phurchpean 主講之「Don’t Get WASTED: A Look Into the Wasted App」說明當一隻 Android 手機裝上 wasted 應用程式後，手機將暴露在隨時遭遠端控制回復原廠設定的風險中，將帶給鑑

識人員很大的麻煩。該 APP 可於 Google Play 中下載安裝，並透過「Device Administration API」取得手機最高權限，再遇到以下狀況時將可能回復原廠設定：

1. 當手機在未解鎖的情況下偵測到 USB 連接。
2. 當有人按下偽裝成某知名社交軟體的假 APP。
3. 當有人按下偽裝成飛航模式的假圖示。
4. 若手機一定時間後仍未成功解鎖。

若鑑識人員不巧遇到這種回復原廠設定的手機，仍可試著找尋開機密碼或 Google 帳號密碼，因 Android 手機內建的機制「FRP(Factory Reset Protection)」，當手機受到非正常回復原廠設定時，需輸入重置前的 Google 帳號密碼，輸入後才能再次使用手機，此時就回到前一個主題，手機重置後仍有部分資訊能擷取出來。




(三) 由亞馬遜公司安全工程經理 Krishna Chirumamilla 主講之「Taming the Tide: Building a Scalable Vulnerability Management Program」，分享到企業如何進行弱點管理，共有以下階段：Discovery、Vulnerability Assessment、Prioritization、Reporting、Remediation、Continuous Monitoring，從發現弱點開始，經過弱點評估、優先層級判

斷、告知及通報、弱點修復到持續監控，將系統風險降至最低。對於日益複雜的資訊系統，任何組織都需面對系統可能出現漏洞的風險，這時可引入講者分享之弱點管理方案，審慎評估各階段的優先層級及優缺點，並確保組織內部的資訊及弱點管理觀念達到一致。

(四) 由 Detego Global 公司北美培訓總監 Rob Maddox 主講之「Expediting Investigations with the Advanced Analytics and Automation in Detego Analyse AI+」介紹該公司旗下一款功能強大之鑑識工具 Analyse AI+，有其獨特的專利分類系統，能將檔案標示為紅色、黃色及綠色，分別代表 Hash 匹配、關鍵字匹配及兩者皆無命中，幫助鑑識人員快速掌握證物狀況。亦融合 AI 技術，利用 AI 驅動的人臉辨識系統篩選大量圖像和影片，在幾秒鐘內識別嫌疑人、證人和其他相關人員（Analyse AI+每秒檢測 10 多張人臉，比行業平均水準快 2 倍）。AI 語義搜索能最大限度地減少手動數據篩選並快速識別更廣泛的概念及上下文，例如「痛苦的兒童」、「晚上在倫敦戴著面具拿著武器的男人」、「客戶帳戶詳細信息截圖」等，能大幅縮短案件偵辦時間。雖無實際使用經驗，無法確認其 AI 精準度是否如其敘述一致，仍殊值本局學長持續關注該工具發展狀況。

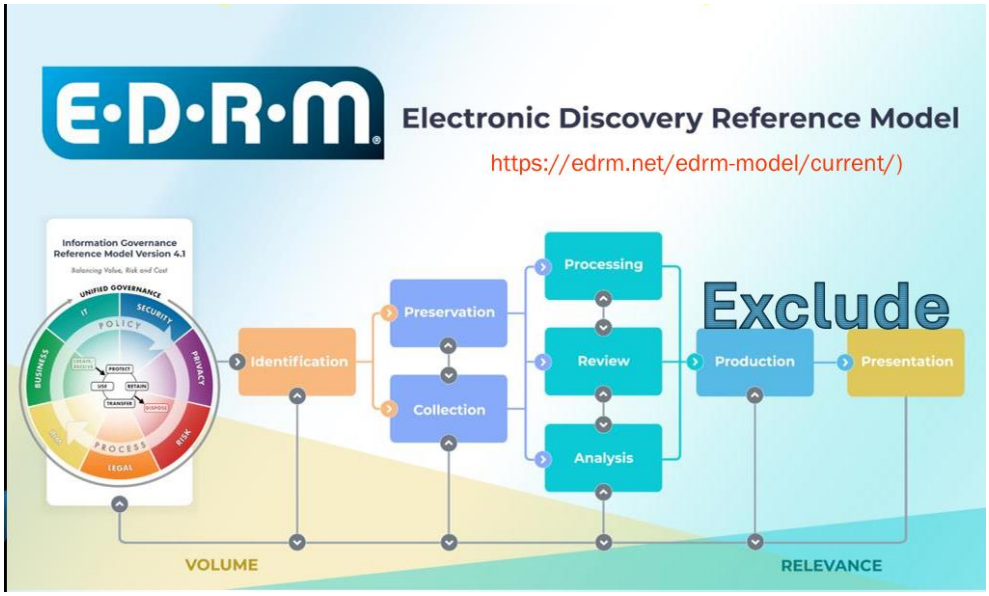
三、 113 年 9 月 18 日

(一) PKF O'Connor Davies 網絡安全與隱私顧問總監 Robert Gaines 主講之「商業電子郵件詐騙攻擊簡介」(An Overview of Business Email Compromise Attacks)介紹標準的商業電子郵件詐騙調查方法，結合了技術工具、數據分析及調查經驗。調查商業電子郵件詐騙案件之步驟，首先要確認攻擊情形，瞭解是否冒充公司內部人員或合作客戶的電子郵件，誘使受害者進行財務轉帳或洩漏敏感資訊；接著蒐集可疑電子郵件範本，確認表頭(header)資訊，分析郵件中使用的相關詐術內容，並檢查郵件伺服器日誌，追蹤可疑的登入活動與發送之電子郵件；再對受害者的電腦設備進行取證分析，尋找有無被安裝惡意軟體或有敏

感行為；同時，應檢查攻擊者使用的電子郵件域名及 IP 位址，確認是否與已知詐騙域名或黑名單 IP 相符，如發現攻擊者使用社交工程(如冒充高層或合作客戶)，便需進一步調查其資訊來源或漏洞，甚至可能為郵件寄件人被駭；調查結束後，公司應檢討採行郵件過濾措施、雙因子認證及進行員工培訓等手段，俾防止未來再遭受商業電子郵件詐騙攻擊。

(二) 參加「Using Open Source and Free Tools to Locate Hidden Web Artifacts」專題演講，由美國內華達郡檢察官辦公室調查員 Greg Tassone 分享。由於行動裝置應用程式的功能及複雜性均不斷提升，本課程以實案作為分享內容，使用開源工具和技術，展示如何尋找隱藏或可能遭現今商用工具忽略之資料，並分享案件分析結果。透過講者講述，深入瞭解網際網路資料可能留存之位置及其內容，並學習使用開源工具搜尋解譯該資料之有效方法。

(三) 由企業電子取證審查員 Grace Parker 講授之「E-Discovery, EDiscovery, eDiscovery ... eDiscovery Basics 101」中提到，美國的訴訟要求當事人在開庭前召開會議，發現證據的過程被稱為「discovery」，特別是電子數據被稱為「e-discovery」，在當今資訊技術發達的時代，電子證據佔有非常大的比例。電子取證的工作流程是「EDRM(Electronic Discovery Reference Model)」，是一個全球標準工作流程，共分為 Information Governance、Identification、Preservation、Processing、Production、Presentation 等階段，EDRM 是長時間、資料量巨大、高度專業的流程，執行者或供應商具備專業能力及相關法學知識是必須的。




(四) 由 WitFoo 聯合創始人兼首席技術官 Charles Herring 主講之「Birthing Perjury-free AI」，透過一個資料外洩案件分享數位資料取證過程中，能如何提取資料、如何整理成易於閱讀的圖表且確認資料無偽證可能，具體步驟為：Understand the Signals、Maintain State、Create Analytic Unit、Analysis 及 Commentary，過程中使用 Artificial Narrow Intelligence (ANI)概念，為特定事件撰寫專屬 AI 程式碼，將有更快、更便宜及更能預測等優點，且可由專家在法庭上進行辯護。

## 四、 113 年 9 月 19 日

於上午 9 時參訪位於加州洛杉磯市 OpenText 公司，該公司係加拿大第四大軟體公司，產品服務範圍包含資訊安全、數位資產管理、雲端服務及資料重現技術等等。在這個資訊爆炸的時代，搜索現場往往存放多台電腦設備，而主管 Chuck Dodson 介紹到，其公司產品 Tableau Forensic Imager 可於搜扣現場連接嫌疑人電子設備後，篩選需要的檔案資料匯出，省去複製整台設備的冗長時間；Tableau Forensic Duplicater 提供現場快速的備份服務，主要用於記憶卡、隨身硬碟等容量較小的設備；Tableau Forensic Bridge 則是提供防寫功能。考慮到 Tableau Forensic Imager 的便攜性與高效率，有利於本局學長於辦案過程中更精準掌握關鍵跡證，值得本局研擬其需求性。接著由顧問 Victor De La Pena 實作各鑑識工具，並帶領本局學長參訪辦公區域及實驗室。

五、 113 年 9 月 20 日

於上午 10 時參訪位於加州橘郡的聯邦調查局(FBI)區域電腦鑑識實驗室（RCFL），RCFL 計劃創建於 2000 年，是 FBI 與其他聯邦、州及地方執法機構聯合鑑識中心，彼此共享設備、技術、經驗及訓練等資源，並使用各自單位的網路專線傳輸資料，有效整合有限資源並將鑑識量能最大化，至今年全美已創建 17 所實驗室，每年協助破獲許多重大刑案。由來自 FBI 的負責人 Glenford Gillett 帶領參訪 RCFL，能注意到 RCFL 規劃許多功能專一的辦公室，例如影片剪輯室，透過剪輯各監視器、行車紀錄器及 GPS 定位等影像，為特定案件訂製出能迅速理解案情的影片；亦有電子設備修復區，能看到掛滿儀器的工作檯、電焊槍及各種外觀毀損程度不一的手機或硬碟；還有取證區，供外單位人員備份及下載鑑識報告相關檔案；另外，RCFL 相當鼓勵職員布置其個人辦公空間。參訪結束後，本局學長及 RCFL 幹員於會議室中交流分享工作中遇到的問題與困境，譬如臺灣在選舉時須面對各種 DeepFake 虛假影音充斥網路，而美國亦有可能遭到外國勢力惡意攻擊，只是對社會影響程度相對較低；虛擬貨幣發展日漸蓬勃，交易越加便利的同時也不免淪為犯罪集團洗錢工具，RCFL 實驗室有專人負責這塊，這也是他們亟欲解決的問題。接著也針對證物保存及鑑定報告內容格式等相關問題進行交流。

## 參、心得與建議

### 一、 潘科長季翔

這次參加的科技安全與數位鑑識會議(Techno Security & Digital Forensics Conference)，已有超過 25 年歷史，一直是數位鑑識與電腦安全產業中，讓來自世界各地之公、私部門參與者聚集在一起學習、交流與分享的重要平台，所獲得之經驗不僅對數位取證的最新技術和挑戰產生更深刻地理解，也拓展了在此領域未來發展方向的視野。

研討會中許多講者均提及，隨著物聯網設備、智慧型手機及社交媒體的普及，案件需要處理的數位證據數量呈爆炸性增長，對於調查人員而言，如

何能快速且有效地篩選出與案件密切相關的數據，已成為重要且關鍵的能力，除了資訊與技術的交流外，使用人工智慧與相關設備的輔助已不可或缺。因為現代設備的加密技術與安全機制，使得取證工作變得更加困難，經由相關專題所展示的解密與取證工具新進展，例如破解受密碼保護的設備，或自受損或原廠重設之設備中回復取得數據，將直接有助於調查實務工作。

藉由至橘郡(Orange County)區域電腦鑑識實驗室(RCFL)參訪的行程，可充分瞭解美國數位鑑識單位運作的實際現況，其中部分讓人印象深刻，包括該實驗室係美國聯邦調查局(FBI)、橘郡地區檢察署及警察單位聯合組成，由來自 FBI 之 Glenford Gillett 擔任負責人，總成員約 40 人亦分為混編的 6 個小組輪流接案，共享設備、技術、經驗及訓練等資源，並且使用各自單位的網路專線傳輸資料，兼顧案件保密性及便利性。反思我國檢察、調查及警察系統在數位鑑識領域幾乎各自為政，分別編列預算購置相同的鑑識設備、軟體及訓練鑑識人員，如各單位能摒除本位主義，並有效統合資源、人力，應可發揮降低成本支出與擴大整體能量之綜效。

此外，RCFL 在案件受理上，有限制每案每次 8 件之規定，對此實深表認同，蓋因近年來數位證物(以智慧型手機及電腦最為常見)之容量逐年遽增，鑑識耗時亦倍增，然而人力時間卻有限，且過往案件經驗中部分案件承辦人有著不論證據重要性，均以送過鑑識作為完成取證象徵之傾向，造成鑑識設備與人力無謂耗損，實際對案件亦無多大助益，故除了重要敏感案件外，對一般案件的鑑識件數加以限制的作法，似有評估推行的可能，以減少不必要的非核心工作，將設備及人力用在真正急要刀口上。

## 二、 陳調查官品芳

(一) 本次會議探討議題相當廣泛，除針對數位鑑識相關之儲存媒體及行動裝置等提供新興鑑識及檢測方法外，更包含多場虛擬貨幣追蹤、駭侵偵查、人工智慧發展與犯罪防治及 IoT 物聯網設備取證方式等，供與會者依興趣或專業領域選擇參與，議題內容專業且豐富多元，廣泛觸及數位鑑識領域的各個面向。會場中安排專業數位鑑識廠商實際展示產品，

由技術人員即時回應與會者提問，有助於深入瞭解產品功能評估導入應用之可行性。主辦單位邀請各國執法機關、相關領域之研究調查人員及開發商參與，於課程中場休息安排了交流時段，供各行業具豐富實務經驗之專業鑑定人員，於會議期間與各國與會者分享透過數位鑑識輔助案件偵辦之相關經驗，並深入探討偵查方法精進之可能性，透過交流激盪收穫許多寶貴經驗與技術，瞭解新興犯罪趨勢、執法情形及因應作為，亦衍生新的案件偵辦思維。

(二) 藉由參與研討會之機會，亦安排參訪位於橘郡(Orange County)之美國聯邦調查局區域電腦鑑識實驗室(RCFL)及數位鑑識領域之軟硬體設備供應商-Opentext。經 RCFL 實驗室主管詳盡介紹，瞭解該實驗室作業流程及使用設備，包含門口管制措施、受理櫃檯、送鑑表單、辦公室區域規劃安排、鑑定人員分工、證物庫管制方式、教育訓練及使用之專業數位鑑識軟硬體設備等。於實驗室介紹結束後亦安排交流討論時間，與 FBI 執法及數位鑑識專業人員探討如虛擬貨幣追蹤、資安事件分析及 Deepfake 等新興犯罪，於美方之權責分工、法律規範及因應作法等議題；另於 Opentext 公司參訪期間，該公司專業技術人員透過簡報與實機方式，展示多項可供協助資安防護、數位鑑識及現場蒐證等軟硬體產品，其中亦包含尚處於雛型階段即將於來年推出之設備，可作為規劃未來推動數位證物分析及現場蒐證方向參考。

(三) 隨著資訊科技持續發展演譯，電腦犯罪結合新興科技，使其犯罪樣態及技巧更趨多元且複雜，因此數位犯罪執法人員廣博學習各方新知更顯重要。透過積極參與國際研討會議或資安研習活動，藉此補足無法從各式媒體、期刊論文等方式獲得之新穎知識及技術，亦不失為培訓人才的方式之一。藉由國際研討會及各式交流機制，與來自世界各國之執法機關人員及業者針對數位犯罪議題共同探討，除提升本局資安人員之國際見聞與知識廣度，更期待結合自身業務並接軌國際資安領域，達成即時掌握數位犯罪發展趨勢之目標。

## 三、 蔡調查官宇勝

本次會議主題多元，內容包含人工智慧及資訊安全等理論探討、加密貨幣及 IoT 物聯網設備調查實務經驗分享，亦有數位證據保存專用之法拉第袋及 Oxygen Forensic 鑑識軟體介紹等鑑識工具應用情境解講，與會者可自行選擇感興趣的主題聆聽，比較國內外數位鑑識法規及流程上的差別，吸收最新的鑑識技術與時俱進。大會另安排業界頂尖資安及鑑識軟體供應商於「Networking Break」及「Happy Hour」時段展示產品，現場看到許多本實驗室已具備的鑑識軟體，能針對使用上的問題直接與原廠討論；亦有許多不熟悉的鑑識設備，各設備間著重的功能不盡相同，未來能針對各式鑑識需求更換鑑識設備，以提升鑑識人員鑑定效率。另外，透過參與本次大會發現 AI 人工智慧技術為國際上重要趨勢，AI 相關議題課程達 11 堂以上，例如「Brave New (Forensic) World: Unraveling the Impact of Artificial Intelligence on Digital Forensics」這門課提到 AI 能幫忙篩選犯罪熱點，透過大數據分析得知哪片地區有著較高的犯罪型態或趨勢；AI 亦有強大的圖像識別和行為分析能力，能從影音及文本中分類出可疑活動，相比傳統鑑識工具能提供更多關鍵線索並提升鑑識工作效率。

參訪美國聯邦調查局電腦鑑識實驗室(RCFL)了解到兩地鑑識流程差異，例如 RCFL 鑑定案一次最多只收 8 件，並於 2 周內回覆鑑定結果，如此能更專注於重要證物修復及取證能力且避免案件延宕，國內亦能借鑑此做法，外勤案件承辦人先初步篩選送鑑證物，能提升本實驗室鑑定效率並專注於部分重要而棘手的證物。另 RCFL 證物室有放置數台大型法拉第箱(Faraday cage)用來保存行動裝置及電子設備，能阻絕網路信號避免證物遭有心人士遠端連線操控並破壞，足見 RCFL 對證物保存之嚴謹態度。最後，鑑識軟體價格非常昂貴，人員培訓亦須大量時間及資源，RCFL 為整合多個單位的鑑識中心，相當於國內檢警調相關單位擰為一繩，比此共享技術、設備及經驗，這也體現美國高度分工的專業性，雖然案件管理上須顧慮洩密問題，但仍值得本局參考借鑒。

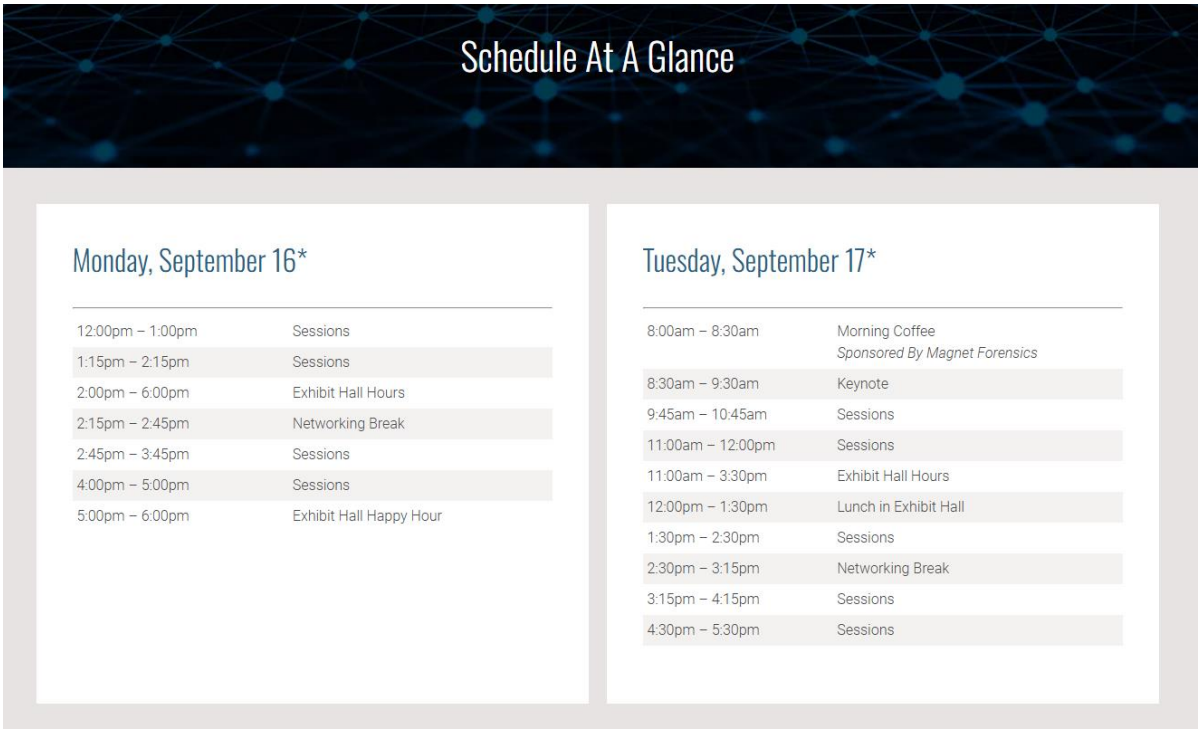
# 肆、附錄：會場照片暨議程總表

## 一、 展覽會場及議程專題演講


## 二、 參訪


NOTICE:
ORANGE COUNTY
REGIONAL COMPUTER
FORENSICS LABORATORY
SUITE 800
RCFL

## 三、 鑑識會議議程



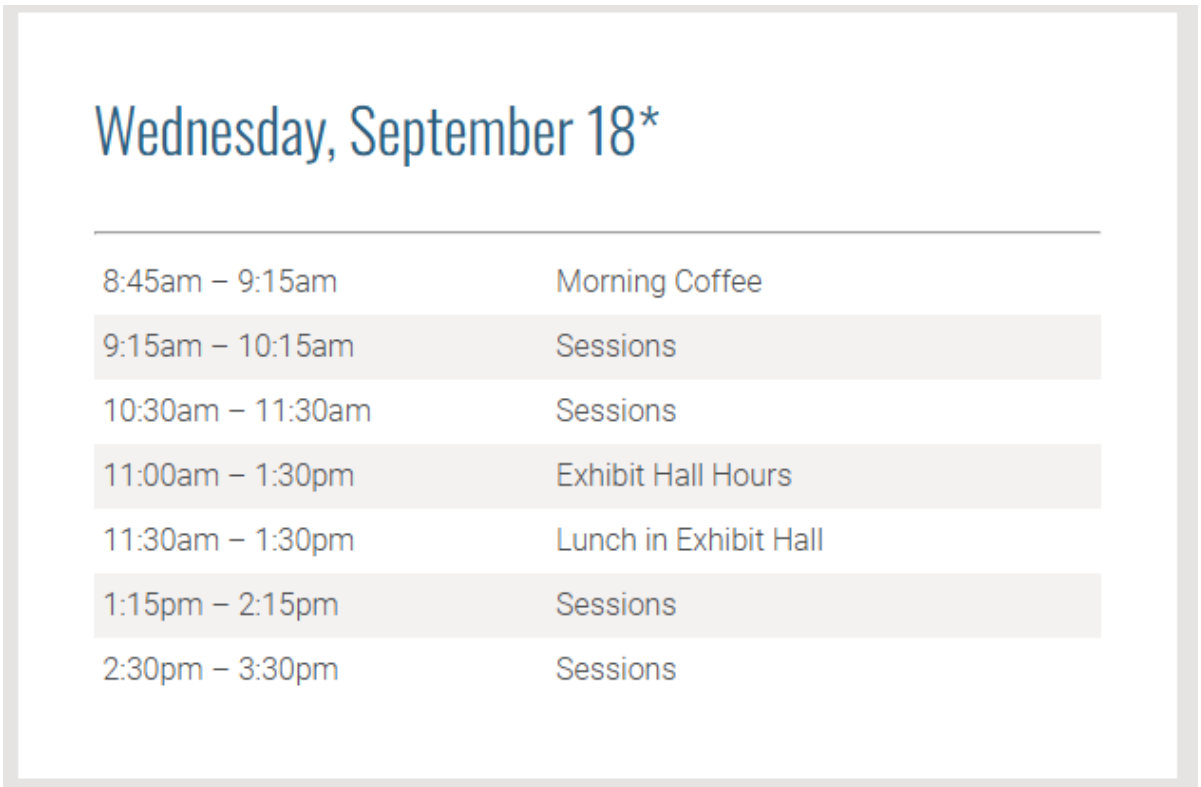
### Schedule At A Glance

#### Monday, September 16*

| | |
|---|---|
| 12:00pm – 1:00pm | Sessions |
| 1:15pm – 2:15pm | Sessions |
| 2:00pm – 6:00pm | Exhibit Hall Hours |
| 2:15pm – 2:45pm | Networking Break |
| 2:45pm – 3:45pm | Sessions |
| 4:00pm – 5:00pm | Sessions |
| 5:00pm – 6:00pm | Exhibit Hall Happy Hour |

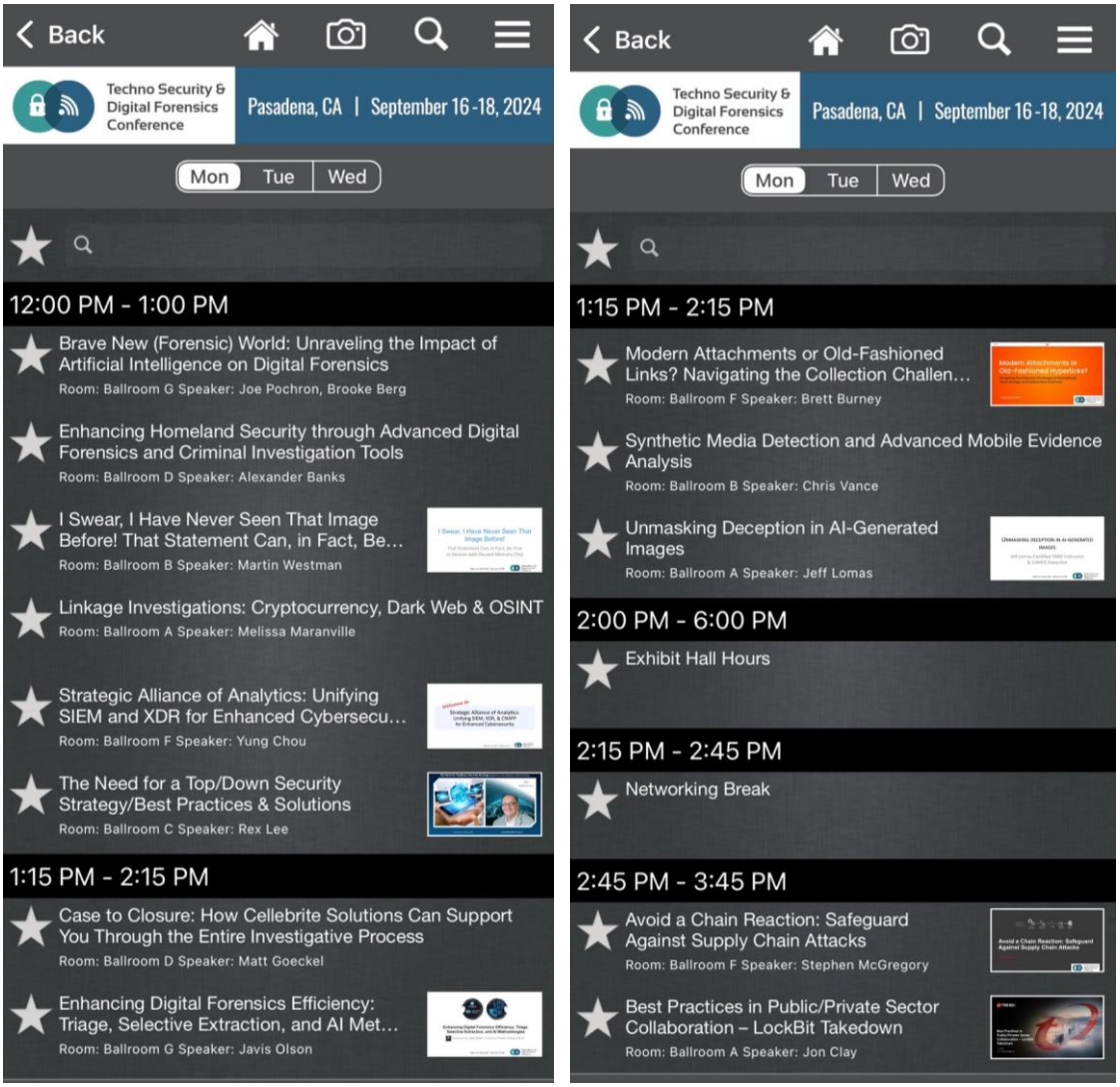
#### Tuesday, September 17*

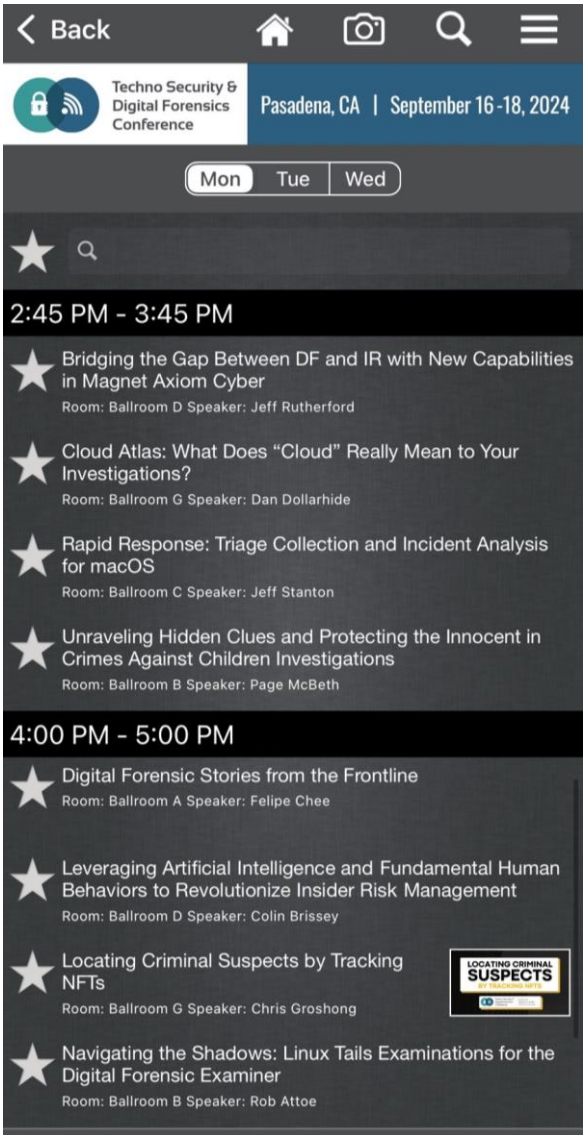
| | |
|---|---|
| 8:00am – 8:30am | Morning Coffee<br>*Sponsored By Magnet Forensics* |
| 8:30am – 9:30am | Keynote |
| 9:45am – 10:45am | Sessions |
| 11:00am – 12:00pm | Sessions |
| 11:00am – 3:30pm | Exhibit Hall Hours |
| 12:00pm – 1:30pm | Lunch in Exhibit Hall |
| 1:30pm – 2:30pm | Sessions |
| 2:30pm – 3:15pm | Networking Break |
| 3:15pm – 4:15pm | Sessions |
| 4:30pm – 5:30pm | Sessions |

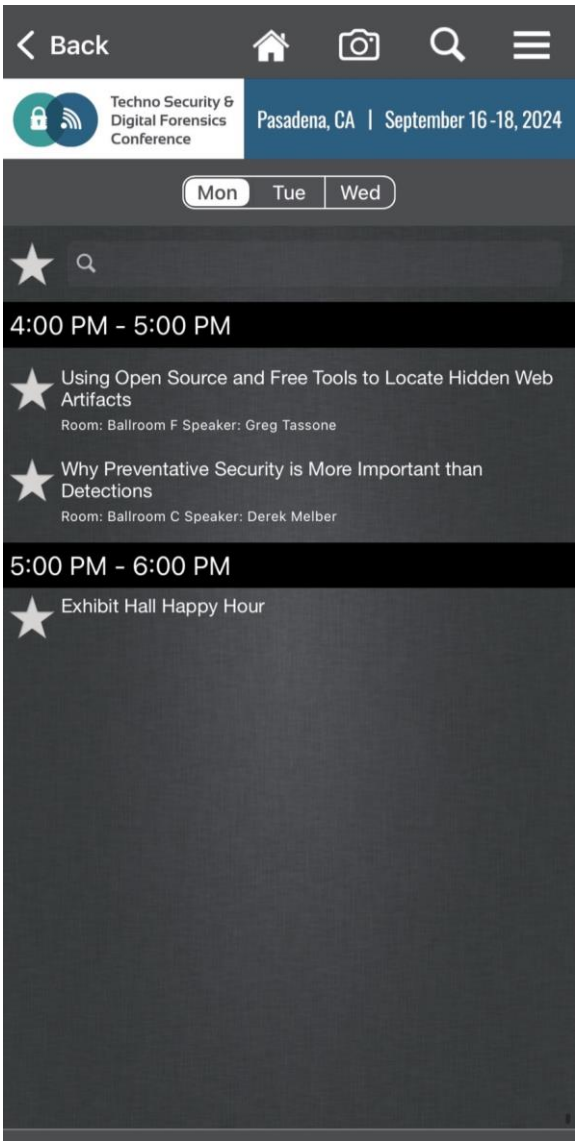


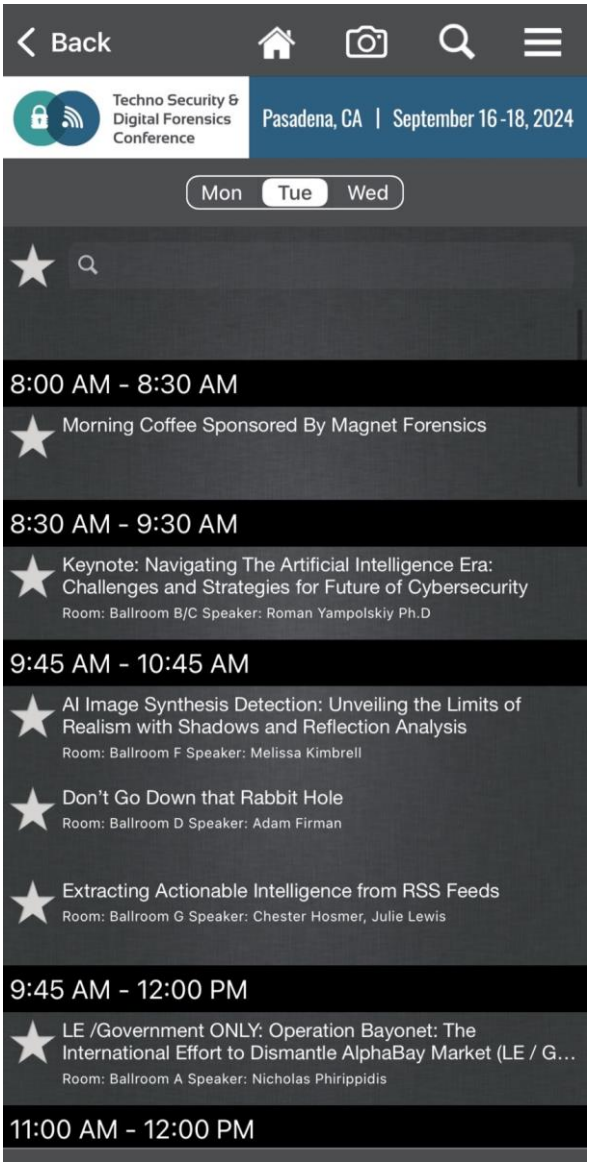
#### Wednesday, September 18*

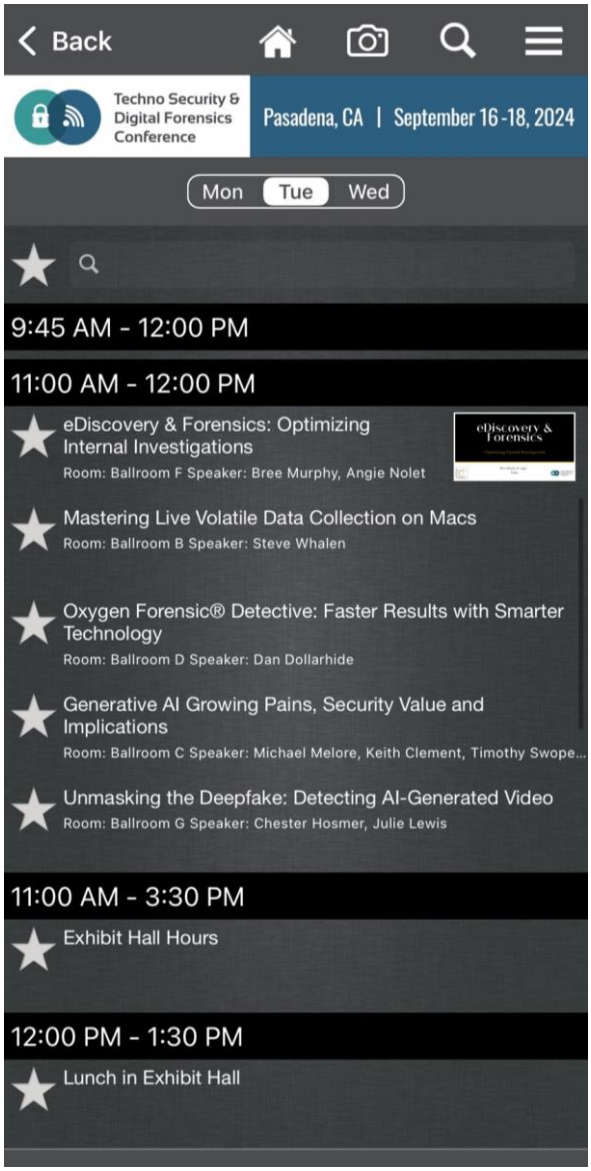
| | |
|---|---|
| 8:45am – 9:15am | Morning Coffee |
| 9:15am – 10:15am | Sessions |
| 10:30am – 11:30am | Sessions |
| 11:00am – 1:30pm | Exhibit Hall Hours |
| 11:30am – 1:30pm | Lunch in Exhibit Hall |
| 1:15pm – 2:15pm | Sessions |
| 2:30pm – 3:30pm | Sessions |

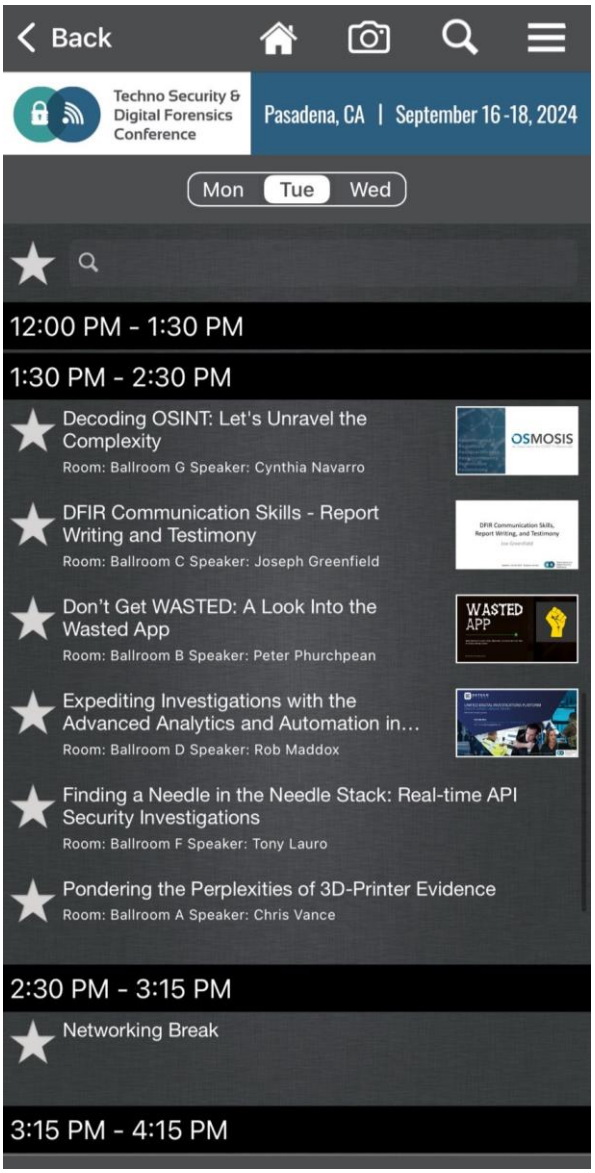

Back
Techno Security & Digital Forensics Conference
Pasadena, CA | September 16 -18, 2024
Mon
Tue
Wed
12:00 PM - 1:00 PM
Brave New (Forensic) World: Unraveling the Impact of Artificial Intelligence on Digital Forensics
Room: Ballroom G Speaker: Joe Pochron, Brooke Berg
Enhancing Homeland Security through Advanced Digital Forensics and Criminal Investigation Tools
Room: Ballroom D Speaker: Alexander Banks
I Swear, I Have Never Seen That Image Before! That Statement Can, in Fact, Be…
Room: Ballroom B Speaker: Martin Westman
Linkage Investigations: Cryptocurrency, Dark Web & OSINT
Room: Ballroom A Speaker: Melissa Maranville
Strategic Alliance of Analytics: Unifying SIEM and XDR for Enhanced Cybersecu…
Room: Ballroom F Speaker: Yung Chou
The Need for a Top/Down Security Strategy/Best Practices & Solutions
Room: Ballroom C Speaker: Rex Lee
1:15 PM - 2:15 PM
Case to Closure: How Cellebrite Solutions Can Support You Through the Entire Investigative Process
Room: Ballroom D Speaker: Matt Goeckel
Enhancing Digital Forensics Efficiency: Triage, Selective Extraction, and AI Met…
Room: Ballroom G Speaker: Javis Olson
Back
Techno Security & Digital Forensics Conference
Pasadena, CA | September 16 -18, 2024
Mon
Tue
Wed
1:15 PM - 2:15 PM
Modern Attachments or Old-Fashioned Links? Navigating the Collection Challen…
Room: Ballroom F Speaker: Brett Burney
Synthetic Media Detection and Advanced Mobile Evidence Analysis
Room: Ballroom B Speaker: Chris Vance
Unmasking Deception in AI-Generated Images
Room: Ballroom A Speaker: Jeff Lomas
2:00 PM - 6:00 PM
Exhibit Hall Hours
2:15 PM - 2:45 PM
Networking Break
2:45 PM - 3:45 PM
Avoid a Chain Reaction: Safeguard Against Supply Chain Attacks
Room: Ballroom F Speaker: Stephen McGregory
Best Practices in Public/Private Sector Collaboration – LockBit Takedown
Room: Ballroom A Speaker: Jon Clay

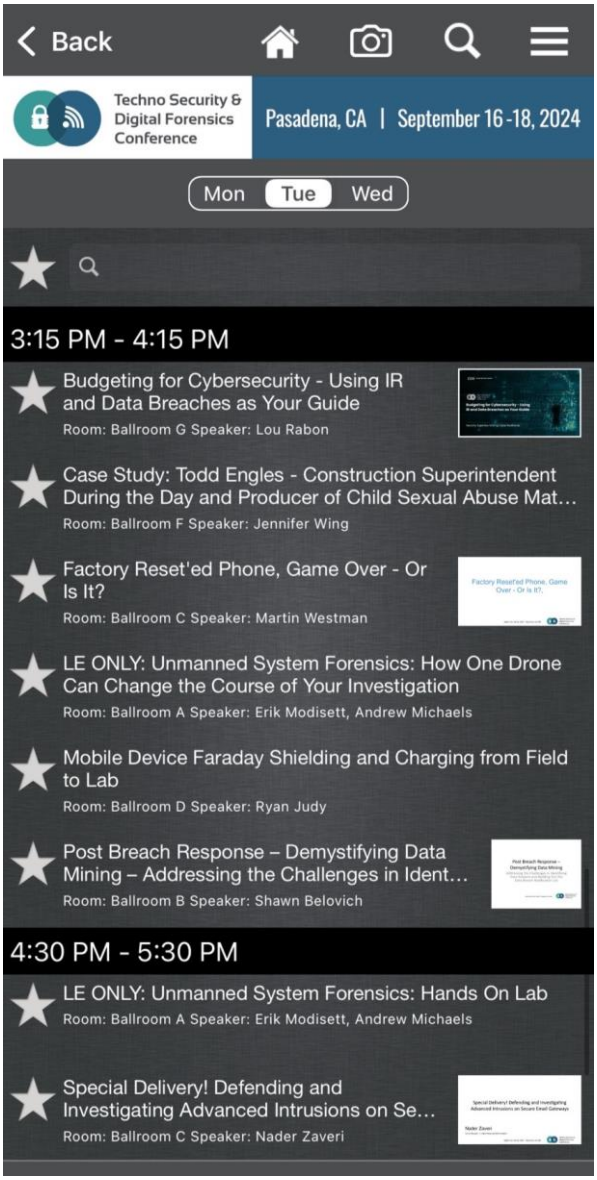

Back
Techno Security & Digital Forensics Conference
Pasadena, CA | September 16-18, 2024
Mon
Tue
Wed
2:45 PM - 3:45 PM
Bridging the Gap Between DF and IR with New Capabilities in Magnet Axiom Cyber
Room: Ballroom D Speaker: Jeff Rutherford
Cloud Atlas: What Does "Cloud" Really Mean to Your Investigations?
Room: Ballroom G Speaker: Dan Dollarhide
Rapid Response: Triage Collection and Incident Analysis for macOS
Room: Ballroom C Speaker: Jeff Stanton
Unraveling Hidden Clues and Protecting the Innocent in Crimes Against Children Investigations
Room: Ballroom B Speaker: Page McBeth
4:00 PM - 5:00 PM
Digital Forensic Stories from the Frontline
Room: Ballroom A Speaker: Felipe Chee
Leveraging Artificial Intelligence and Fundamental Human Behaviors to Revolutionize Insider Risk Management
Room: Ballroom D Speaker: Colin Brissey
Locating Criminal Suspects by Tracking NFTs
Room: Ballroom G Speaker: Chris Groshong
LOCATING CRIMINAL SUSPECTS
Navigating the Shadows: Linux Tails Examinations for the Digital Forensic Examiner
Room: Ballroom B Speaker: Rob Attoe

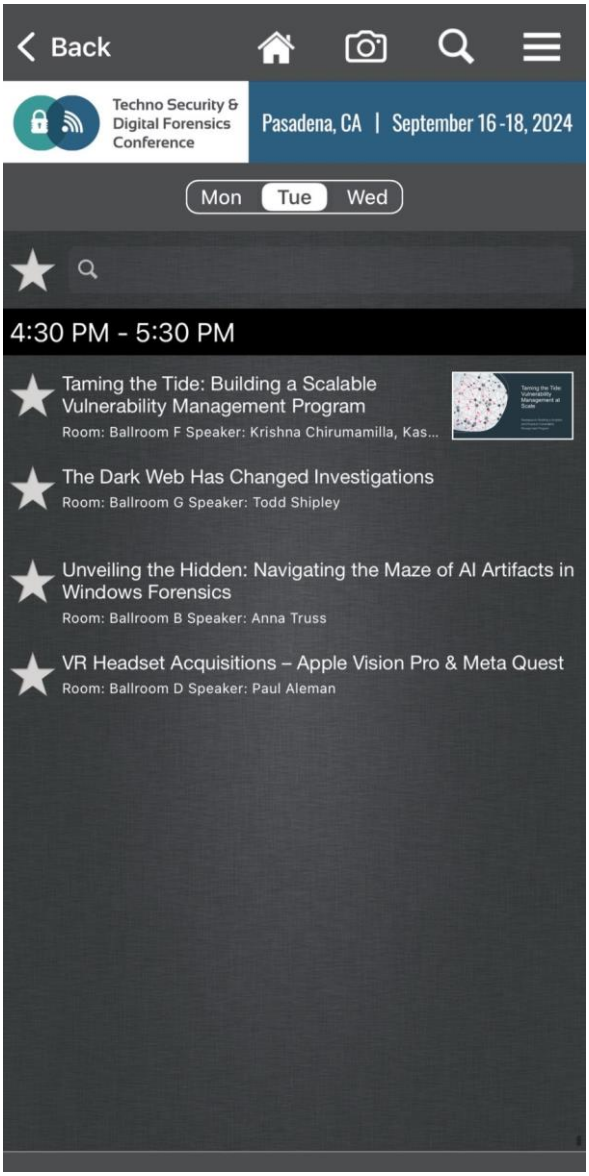

Back
Techno Security & Digital Forensics Conference
Pasadena, CA | September 16-18, 2024
Mon
Tue
Wed
4:00 PM - 5:00 PM
Using Open Source and Free Tools to Locate Hidden Web Artifacts
Room: Ballroom F Speaker: Greg Tassone
Why Preventative Security is More Important than Detections
Room: Ballroom C Speaker: Derek Melber
5:00 PM - 6:00 PM
Exhibit Hall Happy Hour

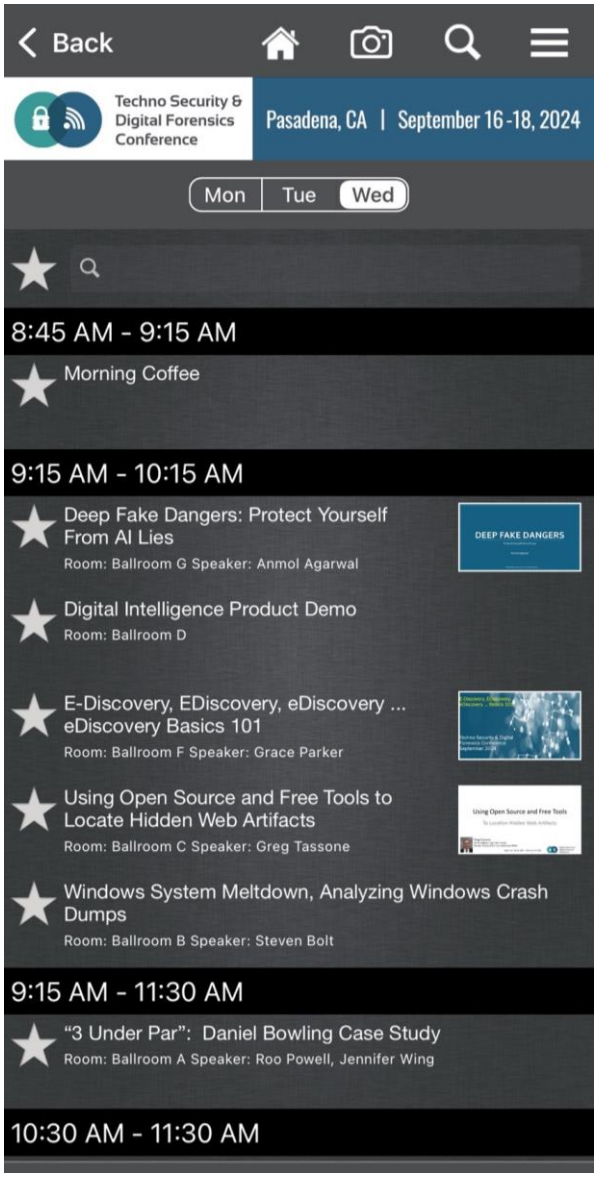

Back
Techno Security & Digital Forensics Conference
Pasadena, CA | September 16-18, 2024
Mon Tue Wed
8:00 AM - 8:30 AM
Morning Coffee Sponsored By Magnet Forensics
8:30 AM - 9:30 AM
Keynote: Navigating The Artificial Intelligence Era: Challenges and Strategies for Future of Cybersecurity
Room: Ballroom B/C Speaker: Roman Yampolskiy Ph.D
9:45 AM - 10:45 AM
AI Image Synthesis Detection: Unveiling the Limits of Realism with Shadows and Reflection Analysis
Room: Ballroom F Speaker: Melissa Kimbrell
Don't Go Down that Rabbit Hole
Room: Ballroom D Speaker: Adam Firman
Extracting Actionable Intelligence from RSS Feeds
Room: Ballroom G Speaker: Chester Hosmer, Julie Lewis
9:45 AM - 12:00 PM
LE /Government ONLY: Operation Bayonet: The International Effort to Dismantle AlphaBay Market (LE / G...
Room: Ballroom A Speaker: Nicholas Phirippidis
11:00 AM - 12:00 PM

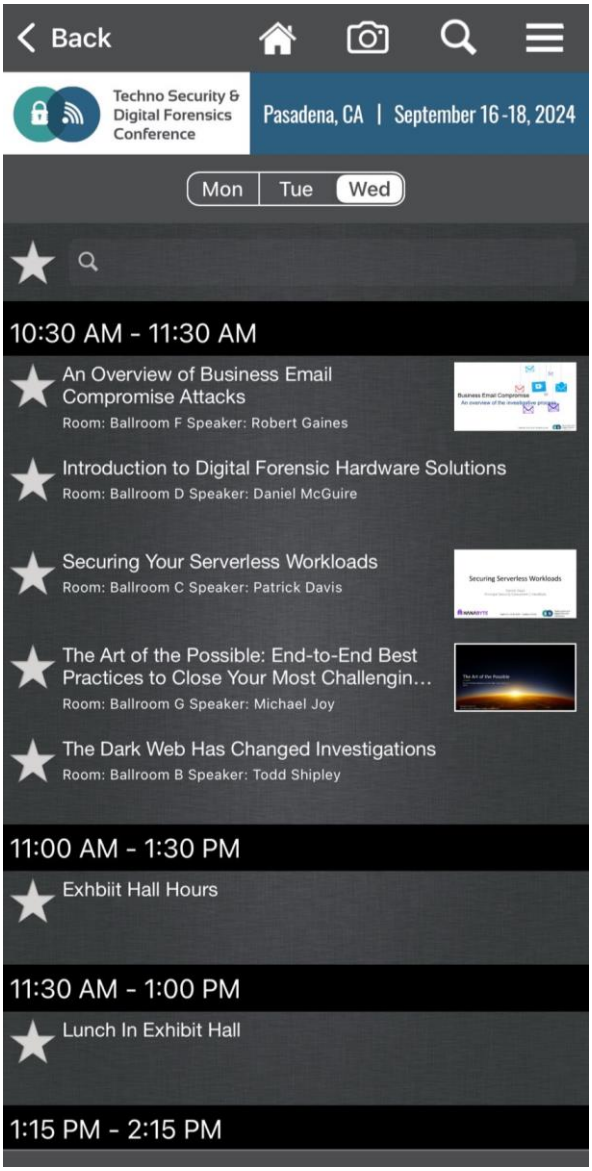

Back
Techno Security & Digital Forensics Conference
Pasadena, CA | September 16-18, 2024
Mon Tue Wed
9:45 AM - 12:00 PM
11:00 AM - 12:00 PM
eDiscovery & Forensics: Optimizing Internal Investigations
Room: Ballroom F Speaker: Bree Murphy, Angie Nolet
Mastering Live Volatile Data Collection on Macs
Room: Ballroom B Speaker: Steve Whalen
Oxygen Forensic® Detective: Faster Results with Smarter Technology
Room: Ballroom D Speaker: Dan Dollarhide
Generative AI Growing Pains, Security Value and Implications
Room: Ballroom C Speaker: Michael Melore, Keith Clement, Timothy Swope...
Unmasking the Deepfake: Detecting AI-Generated Video
Room: Ballroom G Speaker: Chester Hosmer, Julie Lewis
11:00 AM - 3:30 PM
Exhibit Hall Hours
12:00 PM - 1:30 PM
Lunch in Exhibit Hall

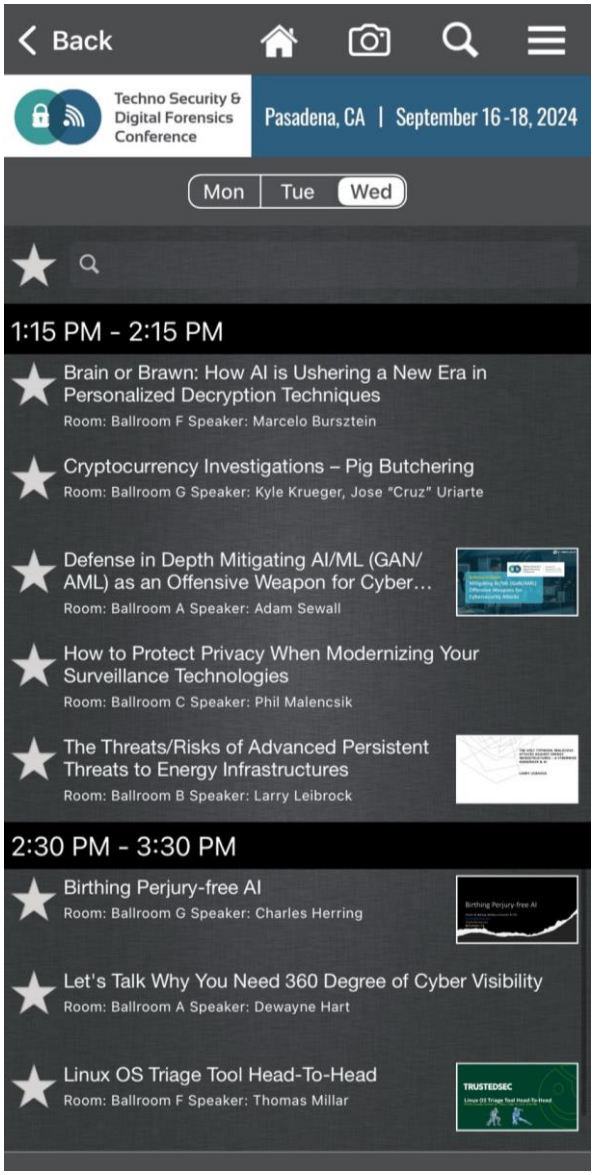

Back
Techno Security & Digital Forensics Conference
Pasadena, CA | September 16-18, 2024
Mon Tue Wed
12:00 PM - 1:30 PM
1:30 PM - 2:30 PM
Decoding OSINT: Let's Unravel the Complexity
Room: Ballroom G Speaker: Cynthia Navarro
DFIR Communication Skills - Report Writing and Testimony
Room: Ballroom C Speaker: Joseph Greenfield
Don't Get WASTED: A Look Into the Wasted App
Room: Ballroom B Speaker: Peter Phurchpean
Expediting Investigations with the Advanced Analytics and Automation in…
Room: Ballroom D Speaker: Rob Maddox
Finding a Needle in the Needle Stack: Real-time API Security Investigations
Room: Ballroom F Speaker: Tony Lauro
Pondering the Perplexities of 3D-Printer Evidence
Room: Ballroom A Speaker: Chris Vance
2:30 PM - 3:15 PM
Networking Break
3:15 PM - 4:15 PM

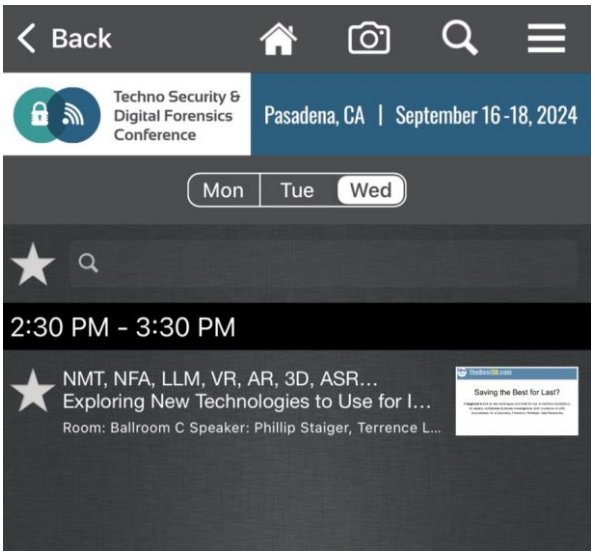

Back
Techno Security & Digital Forensics Conference
Pasadena, CA | September 16-18, 2024
Mon Tue Wed
3:15 PM - 4:15 PM
Budgeting for Cybersecurity - Using IR and Data Breaches as Your Guide
Room: Ballroom G Speaker: Lou Rabon
Case Study: Todd Engles - Construction Superintendent During the Day and Producer of Child Sexual Abuse Mat…
Room: Ballroom F Speaker: Jennifer Wing
Factory Reset'ed Phone, Game Over - Or Is It?
Room: Ballroom C Speaker: Martin Westman
LE ONLY: Unmanned System Forensics: How One Drone Can Change the Course of Your Investigation
Room: Ballroom A Speaker: Erik Modisett, Andrew Michaels
Mobile Device Faraday Shielding and Charging from Field to Lab
Room: Ballroom D Speaker: Ryan Judy
Post Breach Response – Demystifying Data Mining – Addressing the Challenges in Ident…
Room: Ballroom B Speaker: Shawn Belovich
4:30 PM - 5:30 PM
LE ONLY: Unmanned System Forensics: Hands On Lab
Room: Ballroom A Speaker: Erik Modisett, Andrew Michaels
Special Delivery! Defending and Investigating Advanced Intrusions on Se…
Room: Ballroom C Speaker: Nader Zaveri


Back
Techno Security & Digital Forensics Conference
Pasadena, CA | September 16-18, 2024
Mon Tue Wed
4:30 PM - 5:30 PM
Taming the Tide: Building a Scalable Vulnerability Management Program
Room: Ballroom F Speaker: Krishna Chirumamilla, Kas...
The Dark Web Has Changed Investigations
Room: Ballroom G Speaker: Todd Shipley
Unveiling the Hidden: Navigating the Maze of AI Artifacts in Windows Forensics
Room: Ballroom B Speaker: Anna Truss
VR Headset Acquisitions – Apple Vision Pro & Meta Quest
Room: Ballroom D Speaker: Paul Aleman


Back
Techno Security & Digital Forensics Conference
Pasadena, CA | September 16-18, 2024
Mon Tue Wed
8:45 AM - 9:15 AM
Morning Coffee
9:15 AM - 10:15 AM
Deep Fake Dangers: Protect Yourself From AI Lies
Room: Ballroom G Speaker: Anmol Agarwal
DEEP FAKE DANGERS
Digital Intelligence Product Demo
Room: Ballroom D
E-Discovery, EDiscovery, eDiscovery ... eDiscovery Basics 101
Room: Ballroom F Speaker: Grace Parker
Using Open Source and Free Tools to Locate Hidden Web Artifacts
Room: Ballroom C Speaker: Greg Tassone
Windows System Meltdown, Analyzing Windows Crash Dumps
Room: Ballroom B Speaker: Steven Bolt
9:15 AM - 11:30 AM
"3 Under Par": Daniel Bowling Case Study
Room: Ballroom A Speaker: Roo Powell, Jennifer Wing
10:30 AM - 11:30 AM


Back
Techno Security & Digital Forensics Conference
Pasadena, CA | September 16-18, 2024
Mon Tue Wed
10:30 AM - 11:30 AM
An Overview of Business Email Compromise Attacks
Room: Ballroom F Speaker: Robert Gaines
Introduction to Digital Forensic Hardware Solutions
Room: Ballroom D Speaker: Daniel McGuire
Securing Your Serverless Workloads
Room: Ballroom C Speaker: Patrick Davis
The Art of the Possible: End-to-End Best Practices to Close Your Most Challengin…
Room: Ballroom G Speaker: Michael Joy
The Dark Web Has Changed Investigations
Room: Ballroom B Speaker: Todd Shipley
11:00 AM - 1:30 PM
Exhbiit Hall Hours
11:30 AM - 1:00 PM
Lunch In Exhibit Hall
1:15 PM - 2:15 PM


Back
Techno Security & Digital Forensics Conference
Pasadena, CA | September 16-18, 2024
Mon Tue Wed
1:15 PM - 2:15 PM
Brain or Brawn: How AI is Ushering a New Era in Personalized Decryption Techniques
Room: Ballroom F Speaker: Marcelo Bursztein
Cryptocurrency Investigations – Pig Butchering
Room: Ballroom G Speaker: Kyle Krueger, Jose "Cruz" Uriarte
Defense in Depth Mitigating AI/ML (GAN/ AML) as an Offensive Weapon for Cyber…
Room: Ballroom A Speaker: Adam Sewall
How to Protect Privacy When Modernizing Your Surveillance Technologies
Room: Ballroom C Speaker: Phil Malencsik
The Threats/Risks of Advanced Persistent Threats to Energy Infrastructures
Room: Ballroom B Speaker: Larry Leibrock
2:30 PM - 3:30 PM
Birthing Perjury-free AI
Room: Ballroom G Speaker: Charles Herring
Let's Talk Why You Need 360 Degree of Cyber Visibility
Room: Ballroom A Speaker: Dewayne Hart
Linux OS Triage Tool Head-To-Head
Room: Ballroom F Speaker: Thomas Millar


Back
Techno Security & Digital Forensics Conference
Pasadena, CA | September 16-18, 2024
Mon Tue Wed
2:30 PM - 3:30 PM
NMT, NFA, LLM, VR, AR, 3D, ASR… Exploring New Technologies to Use for I…
Room: Ballroom C Speaker: Phillip Staiger, Terrence L…