出國報告（出國類別：研究）

赴美國參加「Techno Security & Digital Forensics Conference 科技安全與數位鑑識研討會」

服務機關：內政部警政署刑事警察局
出國人員：警務正　潘佩琪
偵查員　林映榕
出國地區：美國洛杉磯、帕薩迪納
出國期間：113 年 9 月 11 日至 9 月 20 日
報告日期：113 年 12 月 6 日

摘要

本局今年派員赴美國帕薩迪納參加了 2024 年的「Techno Security & Digital Forensics Conference」科技安全與數位鑑識研討會，該會針對各類議題的深入研討，以及與來自世界各地的執法專業人士彼此之間互動交流，使本局在提升科技犯罪偵查與數位鑑識能力方面獲得了寶貴的經驗與啟發。研討會有來自世界各地的政府機關、有關數位鑑識的企業及民間組織，共同分享及討論數位鑑識、網路安全、科技偵查以及數位證據蒐證等領域之問題、技術、辦案技巧與合作經驗。

此外，通過參訪美國聯邦調查局（FBI）區域電腦鑑識實驗室及國土安全調查署（HSI）數位鑑識部門，本局參訪人員有幸了解美國從事數位鑑識之公家單位，他們各自在整體未來規劃、人員教育訓練、數位鑑識設備、以及鑑識工作流程等方面的實務運作情形。此次參訪不僅加深了我們對數位鑑識技術應用的理解，也促進了與數位鑑識專業人員之間的實務經驗交流，為本局未來數位鑑識實驗室的建設與發展提供了寶貴的借鏡，並使本局在全球數位鑑識領域中學習成長。

目次

壹、目的

本次行程是參加美國 Techno Security & Digital Forensics Conference（科技安全與數位鑑識研討會），該研討會至今已成功舉辦超過 20 年，成為全球領先的科技安全與數位鑑識領域的重要平台。每年，會場內都會設有多家國際數位鑑識廠商的展覽，展示最新的技術成果外，世界各地政府機構、企業界以及民間組織的專業人士齊聚一堂，討論分享在各個有關數位鑑識、網路安全、科技偵查以及數位證據蒐證等各領域的最新技術與合作經驗。

除了會議之外，行程中還安排了前往聯邦調查局（FBI）區域電腦鑑識實驗室和國土安全調查署（HSI）數位鑑識部門的參訪。在這些機構，我們有機會與數位鑑識專業人員進行實務交流，深入了解他們在實際操作中的經驗與挑戰。這些寶貴的交流經驗，不僅擴展了我們的視野，也為本局未來在科技犯罪偵查方面的工作提供了重要的參考與啟示。

這次行程無疑是一次提升專業能力、拓展國際合作的寶貴機會，也為未來的數位鑑識工作打下了堅實的基礎。

貳、過程

行程表

113 年		預定行程	任務	備註
日期	星期			
9 月 11 日	三	啟程	啟程赴洛杉磯（飛航時間估約 11 小時 55 分）	臺灣前往美國洛杉磯
9 月 12 日	四	參訪	參訪國土安全調查署（HSI）數位鑑識部門	美國洛杉磯
9 月 13 日	五	參訪	參訪美國聯邦調查局（FBI）區域電腦鑑識實驗室	美國洛杉磯
9 月 14 日	六	參訪	參訪洛杉磯警察局(LAPD)博物館	美國洛杉磯
9 月 15 日	日	前往帕薩迪納	搭車前往帕薩迪納	美國帕薩迪納
9 月 16 日	一	會議	參加 Techno Security & Digital Forensics Conference 科技安全與數位鑑識研討會	美國帕薩迪納
9 月 17 日	二	會議	參加 Techno Security & Digital Forensics Conference 科技安全與數位鑑識研討會	美國帕薩迪納
9 月 18 日	三	會議	參加 Techno Security & Digital Forensics Conference 科技安全與數位鑑識研討會	美國帕薩迪納
9 月 19 日	四	返程	由美國洛杉磯搭機返回台灣（飛航時間計 13 小時 45 分）(當晚於機上過夜)	美國洛杉磯返回臺灣
9 月 20 日	五	返程	預計當(20)日下午 4 點 55 分飛機抵達台灣	臺灣

一、參訪國土安全調查署（HSI）數位鑑識部門

美國國土安全調查署（Homeland Security Investigations, HSI）隸屬於國土安全部（DHS），專責跨國犯罪及安全威脅調查，特別是涉及海關與移民相關的犯罪組織。我們此次參訪位於洛杉磯長灘的數位鑑識部門，該部門負責洛杉磯地區的數位鑑識工作並協助地方警察單位建置鑑識實驗室。

參訪過程了解了他們的鑑識工作區域與設備參觀及經驗交流，由該部門人員說明並引導我們參觀，瞭解該部門的負責業務、收案及數位鑑識流程，並參觀了鑑識人員辦公室、證物室及法拉第室，與本局數位鑑識實驗室相較，該部門鑑識人員的個人配備較多，參訪內容概述如下：

（一） 數位鑑識設備:

該部門配備與本局相似，包括 Falcon 副本製作機、Graykey 手機破密工具及 Magnet AXIOM 鑑識軟體。特別的是，由於地域廣闊，現場支援需攜帶大型工具箱，內含各式鑑識工具與線材。

（二） 鑑識人員辦公室:

每位鑑識人員擁有完整配備，包含 Encase、X-Ways 及硬碟複製機等工具。針對敏感案件（如兒少性剝削），部門設有獨立數位鑑識空間，確保證據的隱私與安全。

（三） 證物室:

電腦、手機等證物集中存放，其中手機採用專用**充電置物櫃**，便於存放與充電檢視，設計實用且整潔，值得參考。

（四） 法拉第室（Faraday room）:

有全美首間**法拉第室**，所有需訊號遮蔽的工作將在該室內進行，以確保數位證據的完整性與公信力。但現場有向對方提出小建議，因該法拉第室內有證物充電區，卻無消防設備(如滅火器)。

（五） 教育訓練室:

新進人員需要跟著師父學習直到培訓成績達到 A+才可以正式獨當一面。該訓練室也不定期規劃課程培訓 HSI 的執法人員。

（六） 第二數位鑑識實驗室:

他們除了駐地的人員使用的數位鑑識實驗室以外，在其他樓層有設立第二數位鑑識實驗室提供其他地區的 HSI 部門人員剛好來到他們駐地需要數位鑑識時，可以在不打亂駐地的鑑識進度情況下，進行數位鑑識比較突發或是跨區聯合的案件。

（七） 報告室:

提供給執法人員(像是律師、檢察官等)調閱證據的小房間，只能看案件證據但不能下載或編輯，但可以產出報告，現場主管確認可以才會讓執法人員帶走。

（八） 大量資料儲存設備:

資料儲存很久因為怕幾十年後有人翻案需要調閱證據，所以要很大儲存空間，儲存很多案件相關證據。

（九） 未來規劃建置鑑識車:

他們規劃未來建置鑑識車，在車上裝設各鑑識設備，未來在較急迫之案子時，可以更完善且全面的現場做初步的數位鑑識釐清案況。

參觀結束後，雙方互相分享於鑑識實務工作所遭遇之困難與挑戰。本次參訪 HSI 數位鑑識部門收穫良多，認識了該部門的數位鑑識業務、收案及數位鑑識流程等，皆值得納入本局未來數位鑑識實驗室規畫之參考。

二、參訪聯邦調查局（FBI）區域電腦鑑識實驗室（RCFL）

美國區域電腦鑑識實驗室（RCFL）由 FBI 與各級執法機構合作成立，是專注於數位鑑識的專業平台。參訪議程分為參觀實驗室各工作區域及交流討論等 2 階段進行，由該實驗室的主管及二位實驗室人員引導我們參觀。其高效的運作模式、完善的設備及流程、跨部門協作的機制值得深入探討與學習。實驗室主要設施與運作區域包含:

（一）證物管理流程

證物清點與編號：

每件證物在登入系統後，給予證物專屬編號並進行標準化封裝，確保可追溯性。

證物室管理：

嚴格規範證物的拆封與密封，並採用磁帶儲存鑑識檔案，保障證據完整與安全。

（二）數位鑑識工作區

配備高端設備，包括法拉第箱、手機破密設備及智慧型手機充電架。

提供鑑識人員專用的工作站，支持案件取證與技術分析。

（三）自助採證與影像分析

自助採證區：

為送件單位提供數位鑑識軟體，允許送件單位自行操作並獲得技術協助。

監視影像處理：

整合多角度影片素材，製作案件回顧影片，加入時間、地點及重點標示，支援法庭審理。

（四）鑑識人員專屬空間

每人配多台電腦：鑑識用、報告撰寫用及內部系統使用。

配備專業工具如防寫器、晶片焊接設備，用於數據恢復及設備維修。

（五）教育訓練與技術支持

教育訓練室：

提供完整的訓練環境，培養專業鑑識人才（約需兩年培訓期）。

系統機房：

各部門間的系統協作保障資訊流通，尤其 FBI 擁有專屬系統線路。

此外，並於參觀過程中學習到：

（一）資源整合與彈性運作

RCFL 採用開放式人員招募，吸引各執法機關的數位鑑識專才。

彈性的人員組成模式有助於降低流動性並提升穩定性。

（二）高效設備與標準流程

配備先進設備、標準化的證物處理程序，顯著提升作業效率。

建議本地實驗室加強設備升級與流程優化，應對案件數量不斷增加的挑戰。

（三）專業人才培養的重要性

長期專業培訓為 RCFL 的核心競爭力。

應建立國際交流計劃，導入高水準訓練機制，強化本地鑑識能力。

（四）數位證據管理的嚴謹性

嚴格的證物保存與檔案歸檔機制，確保司法公正與透明。

可參考其證據完整性保障措施，提升數據存取安全性。

（五）面對挑戰的技術突破

案件數量增長使得效率與品質的平衡成為挑戰。

可考慮引入人工智慧輔助分析技術，加速取證過程並提升精確度。

RCFL 在數位鑑識領域展現了先進技術與完善的運作模式，為全球數位鑑識實驗室提供了卓越範例。未來若能結合當地需求與資源，推動類似的跨部門合作平台，將有效提升數位犯罪取證與調查的能力。

三、參訪洛杉磯警察博物館

（一）博物館背景與展覽特色

洛杉磯警察博物館是紀錄執法歷史與文化的重要場所，展示了洛杉磯警察局（LAPD）的發展歷程、重大案件的調查過程，以及執法人員面對的挑戰與成就。博物館位於洛杉磯市歷史悠久的地區，其本身亦是一座具有歷史價值的建築，令人感受到執法工作與城市變遷之間的聯繫。

（二）展覽主題

警察歷史演變：包括早期執法設備、制服與巡邏車的展示，讓人見證執法科技的進步。

重大案件回顧：重現洛杉磯著名案件的調查經過，如銀行搶劫案。

警民關係發展：特別探討了洛杉磯警察局如何處理社會問題，例如種族關係與社會衝突。

（三）互動與教育意義

設有模擬犯罪場景，讓參觀者體驗調查取證的過程。

透過影像、紀錄片與導覽解說，加深對警察工作挑戰的理解。

（四） 心得與感受

１、 了解執法歷史與文化的價值：透過展品與案例，深刻認識到執法人員不僅是法律的執行者，更是社會穩定的重要支柱。從早期裝備的簡陋到現代高科技裝置的應用，展現了執法技術的進步以及與犯罪對抗的持續努力。

２、 對警察職責與挑戰的深層理解：展覽強調了警察在日常工作中面對的風險與壓力，例如面對高風險逮捕行動或應對突發事件。

３、 對警民關係的反思：透過博物館展出的案例，了解到警察工作的透明化對改善警民信任的重要性。也讓人反思警察制度如何與多元文化共存並服務於不同社群的需求。

４、 科技對執法工作的影響：博物館展示的各類執法裝備，讓人看到科技如何輔助案件調查，例如早期的指紋分析與現代的數位鑑識技術。

洛杉磯警察博物館的參訪，不僅讓人回顧了執法歷史，更反思了警察工作在社會中的角色與價值。這樣的經驗不僅增進了對警察工作的理解，也啟發我們思考如何平衡執法效率、科技應用與人性化服務。

四、Techno Security & Digital Forensics Conference 科技安全與數位鑑識研討會

（一） 研討會議程及展場安排說明

這次研討會從 113 年 9 月 16 至 113 年 9 月 18 日，在美國加州帕薩迪納的帕薩迪納會議中心（Pasadena Convention Center）舉行。會場主要分為展區及研討會議。展區為一個完整空間，每個廠商以分配之攤位編號展示相關硬體及軟體工具，而研討會議總計有 8 間會議室，從編號 A 至編號 H，並依會議室外的議程表，舉行不同主題之演講。以下分別為本次研討會議程及參展的廠商列表：

1、研討會議程表

12:00-13:00	I Swear, I Have Never Seen That Image Before! That Statement Can, in Fact, Be True in Devices with Reused Memory Chip 地點：Ballroom B 講師：Martin Westman, Exploit Research Manager - MSAB

	Brave New (Forensic) World: Unraveling the Impact of Artificial Intelligence on Digital Forensics 地點：Ballroom G 講師：Joe Pochron, Managing Director, Digital Investigations & Cyber Defense - Nardello & Co. Brooke Berg, Director - Nardello & Co.
	Strategic Alliance of Analytics: Unifying SIEM and XDR for Enhanced Cybersecurity 地點：Ballroom F 講師：Yung Chou, Cloud Solution Architect - Microsoft
	The Need for a Top/Down Security Strategy/Best Practices & Solutions 地點：Ballroom C 講師：Rex Lee, Security Advisor/Tech Journalist - My Smart Privacy
	Linkage Investigations: Cryptocurrency, Dark Web & OSINT 地點：Ballroom A 講師：Melissa Maranville, Founder/CEO - DeVille and Associates, LLC
	Enhancing Homeland Security through Advanced Digital Forensics and Criminal Investigation Tools 地點：Ballroom D 講師：Alexander Banks, Program Manager - DHS S&T
13:15-14:15	Unmasking Deception in AI-Generated Images 地點：Ballroom A 講師：Jeff Lomas, Detective - Las Vegas Metropolitan Police
	Enhancing Digital Forensics Efficiency: Triage, Selective Extraction, and AI Methodologies 地點：Ballroom G 講師：Javis Olson, North American Sales Manager - Detego Global
	Synthetic Media Detection and Advanced Mobile Evidence Analysis 地點：Ballroom B 講師：Chris Vance - Magnet Forensics
	Modern Attachments or Old-Fashioned Links? Navigating the Collection Challenges of Hosted Email, Cloud Storage, and Collaboration Platforms

	地點：Ballroom F 講師：Brett Burney, eLaw Evangelist - Nextpoint
	Case to Closure: How Cellebrite Solutions Can Support You Through the Entire Investigative Process 地點：Ballroom D 講師：Matt Goeckel, Senior Technical Manager - Cellebrite
14:45-15:45	Best Practices in Public/Private Sector Collaboration – LockBit Takedown 地點：Ballroom A 講師：Jon Clay, VP, Threat Intelligence - Trend Micro
	Cloud Atlas: What Does “Cloud” Really Mean to Your Investigations? 地點：Ballroom G 講師：Dan Dollarhide - Oxygen Forensics, Inc.
	Avoid a Chain Reaction: Safeguard Against Supply Chain Attacks 地點：Ballroom F 講師：Stephen McGregory,- Keysight Technologies
	Rapid Response: Triage Collection and Incident Analysis for macOS 地點：Ballroom C 講師：Jeff Stanton, Sr Incident Response Commander - Adobe
	Unraveling Hidden Clues and Protecting the Innocent in Crimes Against Children Investigations 地點：Ballroom B 講師：Page McBeth, Customer Success Manager - Cellebrite
	Bridging the Gap Between DF and IR with New Capabilities in Magnet Axiom Cyber 地點：Ballroom D 講師：Jeff Rutherford, Forensic Consultant - Magnet Forensics
16:00-17:00	Navigating the Shadows: Linux Tails Examinations for the Digital Forensic Examiner 地點：Ballroom B 講師：Rob Attoe, CEO - Spyder Forensics
	Why Preventative Security is More Important than Detections 地點：Ballroom C 講師：Derek Melber, Chief Strategist - Nanitor

	Locating Criminal Suspects by Tracking NFTs 地點：Ballroom G 講師：Chris Groshong, President - CoinStructive Inc.
	Digital Forensic Stories from the Frontline 地點：Ballroom A 講師：Felipe Chee, District Attorney Investigator - San Diego County District Attorney's Office
	Leveraging Artificial Intelligence and Fundamental Human Behaviors to Revolutionize Insider Risk Management 地點：Ballroom D 講師：Colin Brissey, Sales Lead - EchoMark
	Using Open Source and Free Tools to Locate Hidden Web Artifacts 地點：Ballroom F 講師：Greg Tassone, DA Investigator - High Tech Crimes - Nevada County (CA) District Attorney's Office, Bureau of Investigations
113 年 9 月 17 日星期二	
8:30-9:30	Keynote: Navigating The Artificial Intelligence Era: Challenges and Strategies for Future of Cybersecurity 地點：Ballroom B/C 講師：Roman Yampolskiy, Futurist,- University of Louisville
9:45-10:45	AI Image Synthesis Detection: Unveiling the Limits of Realism with Shadows and Reflection Analysis 地點：Ballroom F 講師：Melissa Kimbrell,- Amped Software USA Inc.
	Don't Go Down that Rabbit Hole 地點：Ballroom D 講師：Adam Firman, Tech Evangelist - MSAB
	Extracting Actionable Intelligence from RSS Feeds 地點：Ballroom G 講師：Chester Hosmer, CEO - Python Forensics
9:45-12:00	LE /Government ONLY:Operation Bayonet: The International Effort to Dismantle AlphaBay Market (LE / Government Only) 地點：Ballroom A 講師：Nicholas Phirippidis, Special Agent - FBI
11:00-12:00	Mastering Live Volatile Data Collection on Macs

	地點：Ballroom B 講師：Steve Whalen, Co-Founder - SUMURI LLC
	Generative AI Growing Pains, Security Value and Implications 地點：Ballroom C 講師：Michael Melore, Senior Cybersecurity Advisor, CISSP - IBM Keith Clement, State of CA Workforce and Development Cyber Task Force - State of CA Timothy Swope, Interim CISO - University of Chicago Medicine Veronica Mitchell, Supervisor Cybersecurity Advisor - Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), Region 9
	Unmasking the Deepfake: Detecting AI-Generated Video 地點：Ballroom G 講師：Chester Hosmer, CEO - Python Forensics Julie Lewis, CEO - Digital Mountain, Inc.
	eDiscovery & Forensics: Optimizing Internal Investigations 地點：Ballroom F 講師：Bree Murphy, Sr. Solutions Consultant - Women in eDiscovery/ Exterro Angie Nolet, Co-Founder & Podcast Co-Host - eDiscovery Chicks
	Oxygen Forensic® Detective: Faster Results with Smarter Technology 地點：Ballroom D 講師：Dan Dollarhide - Oxygen Forensics, Inc.
13:30-14:30	DFIR Communication Skills - Report Writing and Testimony 地點：Ballroom C 講師：Joseph Greenfield, Vice President; Associate Professor of Practice - Maryman; University of Southern California
	Finding a Needle in the Needle Stack: Real-time API Security Investigations 地點：Ballroom F 講師：Tony Lauro, Director of Security Technology & Strategy - Akamai
	Decoding OSINT: Let's Unravel the Complexity 地點：Ballroom G

	講師：Cynthia Navarro, President - OSMOSIS
	Pondering the Perplexities of 3D-Printer Evidence 地點：Ballroom A 講師：Chris Vance, Senior Technical Forensics Specialist - Magnet Forensics
	Don’t Get WASTED: A Look Into the Wasted App 地點：Ballroom B 講師：Peter Phurchpean, Digital Forensic Examiner - Federal Bureau of Investigation
	Expediting Investigations with the Advanced Analytics and Automation in Detego Analyse AI+ 地點：Ballroom D 講師：Rob Maddox, Director of North American Training - Detego Global
15:15-16:15	Factory Reset'ed Phone, Game Over - Or Is It? 地點：Ballroom C 講師：Martin Westman, Exploit Research Manager - MSAB
	Post Breach Response – Demystifying Data Mining – Addressing the Challenges in Identifying Data Subjects and Building Out the Data Breach Notification List 地點：Ballroom B 講師：Shawn Belovich, Senior Vice President - Digital Forensics & Cyber Incident Response - HaystackID
	LE ONLY: Unmanned System Forensics: How One Drone Can Change the Course of Your Investigation 地點：Ballroom A 講師：Andrew Michaels, CAMDEx Lab Manager - U.S. Customs and Border Protection
	Mobile Device Faraday Shielding and Charging from Field to Lab 地點：Ballroom D 講師：Ryan Judy, President - Mission Darkness
	Case Study: Todd Engles - Construction Superintendent During the Day and Producer of Child Sexual Abuse Material (CSAM) at Night 地點：Ballroom F 講師：Jennifer Wing, Detective/Task Force Officer - Orlando Police Department/FBI Violent Crimes Against Children and

	Human Trafficking Task Force, Tampa Division
16:30-17:30	Special Delivery! Defending and Investigating Advanced Intrusions on Secure Email Gateways 地點：Ballroom C 講師：Nader Zaveri, Senior Manager - Incident Response & Remediation - Mandiant Inc.
	Unveiling the Hidden: Navigating the Maze of AI Artifacts in Windows Forensics 地點：Ballroom B 講師：Anna Truss, Founder / CEO - DefSec LLC
	The Dark Web Has Changed Investigations 地點：Ballroom G 講師：Todd Shipley, President - Dark Intel
	Taming the Tide: Building a Scalable Vulnerability Management Program 地點：Ballroom F 講師：Krishna Chirumamilla - Amazon Inc. Kashif Memon - Amazon Inc.
	LE ONLY: Unmanned System Forensics: Hands On Lab 地點：Ballroom A 講師：Erik Modisett, Supervisory Agent - U.S. Customs and Border Protection Andrew Michaels, CAMDEx Lab Manager - U.S. Customs and Border Protection
	VR Headset Acquisitions – Apple Vision Pro & Meta Quest 地點：Ballroom D 講師：Paul Aleman, Director - DATAPILOT Inc
113 年 9 月 18 日星期三	
9:15-10:15	Using Open Source and Free Tools to Locate Hidden Web Artifacts 地點：Ballroom C 講師：Greg Tassone, DA Investigator - High Tech Crimes - Nevada County (CA) District Attorney's Office, Bureau of Investigations
	E-Discovery, EDiscovery, eDiscovery ... eDiscovery Basics 101 地點：Ballroom F 講師：Grace Parker, Principal IT Specialist - EDiscovery & BCMP - CEDS, EnCE - Parsons Corp

	Deep Fake Dangers: Protect Yourself From AI Lies 地點：Ballroom G 講師：Anmol Agarwal, Senior Security Researcher - Alora Tech, LLC.
	Windows System Meltdown, Analyzing Windows Crash Dumps 地點：Ballroom B 講師：Steven Bolt, Acting Chief Information Security Officer - Bechtel
9:15-11:15	“3 Under Par”: Daniel Bowling Case Study 地點：Ballroom A 講師：Roo Powell, CEO and Founder - SOSA (Safe from Online Sex Abuse) Jennifer Wing, Detective/Task Force Officer - Orlando Police Department/FBI Violent Crimes Against Children and Human Trafficking Task Force, Tampa Division
10:30-11:30	The Art of the Possible: End-to-End Best Practices to Close Your Most Challenging Cases 地點：Ballroom G 講師：Michael Joy, Captain (Ret.) - New York City Police Department
	An Overview of Business Email Compromise Attacks 地點：Ballroom F 講師：Robert Gaines, Director, Cybersecurity and Privacy Advisory - PKF O'Connor Davies
	Securing Your Serverless Workloads 地點：Ballroom C 講師：Patrick Davis, Principal Security Consultant. - Hanabyte Cybersecurity
	Introduction to Digital Forensic Hardware Solutions 地點：Ballroom D 講師：Daniel McGuire, Digital Forensics Technology Specialist - Ace Forensics
	The Dark Web Has Changed Investigations 地點：Ballroom B 講師：Todd Shipley, President - Dark Intel
13:15-14:15	Brain or Brawn: How AI is Ushering a New Era in Personalized Decryption Techniques 地點：Ballroom F

	講師：Marcelo Bursztein, CEO - Novacene AI Corp.
	How to Protect Privacy When Modernizing Your Surveillance Technologies 地點：Ballroom C 講師：Phil Malencsik, Strategic Account Executive - Public Sector - Genetec
	Defense in Depth Mitigating AI/ML (GAN/AML) as an Offensive Weapon for Cybersecurity Attacks 地點：Ballroom A 講師：Adam Sewall, CEO - WATERLEAF INTERNATIONAL LLC
	Cryptocurrency Investigations – Pig Butchering 地點：Ballroom G 講師：Kyle Krueger, Network Intrusion Forensic Analyst - United States Secret Service Jose “Cruz” Uriarte, Investigative Analyst - U.S.. Secret Service
	The Threats/Risks of Advanced Persistent Threats to Energy Infrastructures 地點：Ballroom B 講師：Larry Leibrock, Researcher – USG
14:30-15:30	Birthing Perjury-free AI 地點：Ballroom G 講師：Charles Herring, Co-founder & Chief Technology Officer - WitFoo
	Let's Talk Why You Need 360 Degree of Cyber Visibility 地點：Ballroom A 講師：Dewayne Hart, CEO - SEMAIS
	Linux OS Triage Tool Head-To-Head 地點：Ballroom F 講師：Thomas Millar, Senior Security Consultant - TrustedSec
	NMT, NFA, LLM, VR, AR, 3D, ASR… Exploring New Technologies to Use for Investigations 地點：Ballroom C 講師：Phillip Staiger, Consultant in machine translation and multimedia - TheBest3D.com Terrence Lewis, Translator and Software Developer Steve Braich, Computational Linguist, Localization Consultant - Robotic Polyglot

	Gilberto Segura, VP of Technology - PGLS

2、展場出席廠商

1	Ace Forensics	14	LeadsOnline
2	Amped Software USA, Inc.	15	Logicube, Inc.
3	Apricorn	16	Magnet Forensics
4	Atola Technology	17	Mission Darkness
5	Cellebrite	18	Monolith Forensics
6	DATAPILOT	19	MSAB
7	Detego Digital Forensics	20	Open Text
8	Digital Intelligence	21	Oxygen Forensics
9	EchoMark	22	SEARCH Group, Inc.
10	Exterro	23	Silicion Forensics
11	G3 Technologies	24	SUMURI
12	GetData Forensics	25	VESPEREYE
13	IACIS		

（一）演講：Linkage Investigations: Cryptocurrency, Dark Web & OSINT

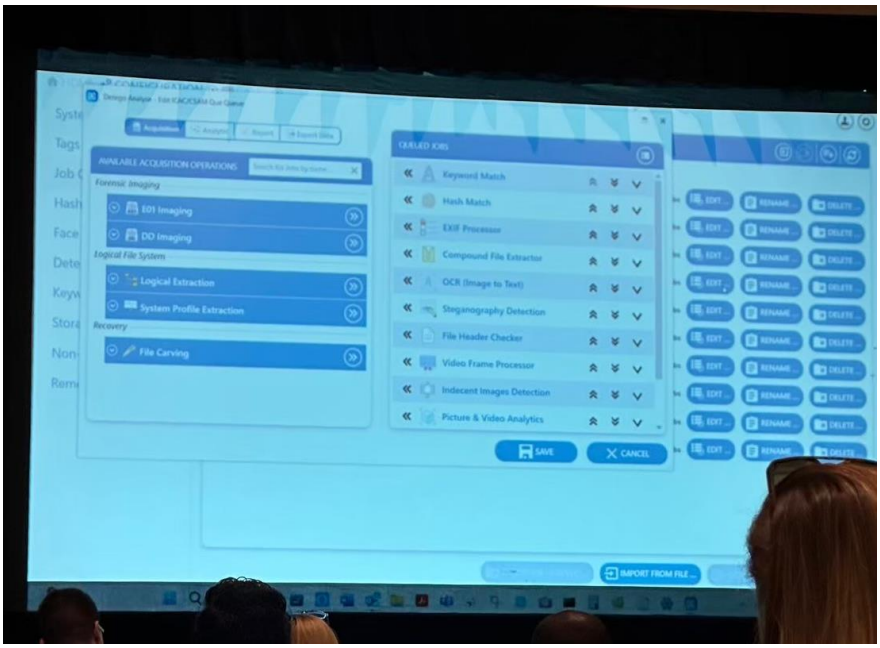
本場主講人 Melissa Maranville 為 DeVille and Associates 的創辦人兼 CEO，首先介紹基本的網路世界構造，不僅止於我們常見的網際網路使用，還包括深網及暗網的部分，在說明現行罪犯多使用暗網搭配虛擬貨幣，以期達成匿名犯罪的目的。

講者進一步於會議中講解如何突破因為暗網或洋蔥路由等隱藏來源或身分情資的困境，可利用公開來源情資，及暗網中與現實世界的連結，形成突破防線的缺口。例如其發布的照片、影片、文章等蒐集相關資訊，特別是虛擬貨幣的交易，雖然有許多手法可以混淆幣流的追蹤，介紹了「QLUE」的軟體可以解析判讀經由混幣器的的交易流向，另外有些交易過程可能留下 IP 位址，從而連結到到實體位址，或是 Email 的各種排列組合，取得於其餘網站註冊的資料，相當推薦「Meltego」及「Darkblue」可協助我們進行公開情資的蒐集。

（二）演講：Enhancing Digital Forensics Efficiency: Triage, Selective Extraction, and AI Methodologies

本場演講為 Detego Global 公司的銷售經理 Javis Olson，介紹其數

位鑑識產品：Triage、Selective Extration 及 AI Methodologies，主要功能與我們現行使用的 Cellebrite 大同小異，較特別的部分有相片的臉部辨識功能，可以圖搜尋相似的結果；影片或影音檔的語言辨識及翻譯，可以直接產出文字檔；另外也有與 Greykey 介接，可以直接以該軟體實施破密功能，對科技犯罪偵查人員有相當大的助益。



（三） 演講：Operation Bayonet: The International Effort to Dismantle AlphaBay Market

本場演講限定執法人員參加，故禁止拍照攝影，由 FBI 的特別探員 Nicholas Phirippidis 講述犯嫌如何利用 Tor 網路隱匿 IP 位址，並於暗網明目張膽的的銷售各種違法物品，包含槍枝、毒品、假鈔、假證件、偷盜得手的信用卡，而且已發展成甚具規模的組織，有領導者、主管及銷售人員，分層負責各自的工作。

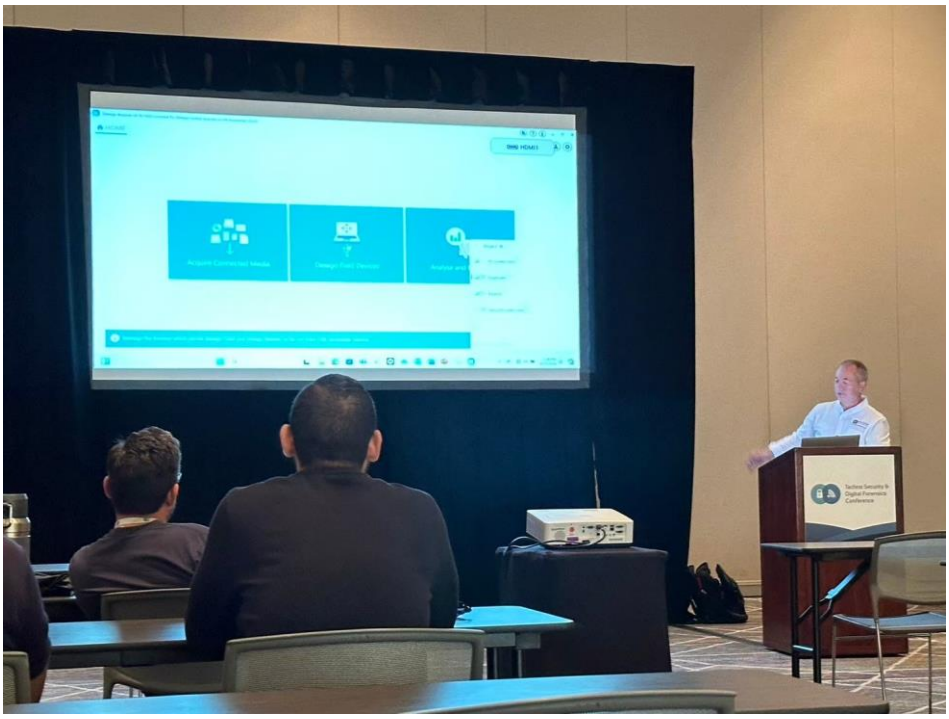
經過偵查人員鉅細靡遺地檢視各項線索，挖掘出一封幕後首腦不慎使用個人 Email 寄出之信件，從而展開一連串的追查行動，自 IP 位址、Email 地址、伺服器名稱，連結至 Linkedin 的個人頁面、Paypal 的付款資料，得知其聲稱任職於加拿大魁北克省的軟體設計師，雖然證明其為空殼公司，但循線追查金流至泰國某豪宅，及其購買的 Porsche 車輛，最後透過於其宅第門口製造的假車禍將此首腦吸引現身，並趁其不及將手機電腦上鎖的狀態下執行逮捕、扣押。

（四） 演講：Expediting Investigations with the Advanced Analytics and Automation in Detego Analyse AI+

本場演講是延續前一日 Detego Global 公司的產品進階功能介紹，主講人 Rob Maddox 介紹了 Triage 於犯罪現場針對特定情資或標

的進行採證，節省處理時間，另外關鍵字搜尋及預先建立蒐證模型等功能，也可以加速證物處理的速度。

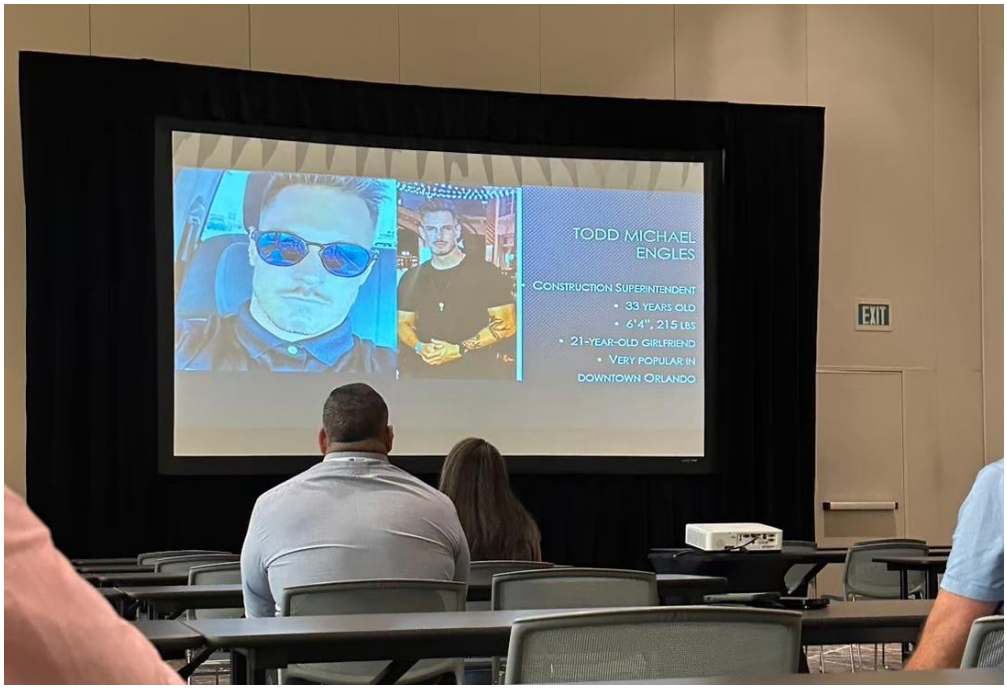
另外，在 AI 技術的發展下，亦可以文字指令執行特定物件的搜索，例如執行「holding a weapon」搜尋，便可於各資料庫、郵件或相簿中找出持槍恐嚇的照片。



（五） 演講：Case Study: Todd Engles - Construction Superintendent During the Day and Producer of Child Sexual Abuse Material (CSAM) at Night

本場演講為奧蘭多警察局警探 Jennifer Wing，主責偵辦兒少性剝削及人口販運，此案例講述一名相當具有人氣的營建監造，涉嫌在「KIK」App 上誘姦未成年，經調閱使用者帳號取得身分確認將其逮捕，其聲稱遭駭客盜取帳號非本人使用。然而經由數位鑑識其所持有之設備，不僅於 App 聊天室偽裝未成年女孩，與小男孩聊天取得其裸露影像後，冒名為該男孩與其餘女孩聊天誘騙見面後下藥性侵。

手機中有大量未滿 12 歲孩童的影像，及迫使他們稱他為「Daddy」的病態威權感，本案受害者一共有 9 名未成年孩童。



（六） 演講：LE ONLY: Unmanned System Forensics: How One Drone Can Change the Course of Your Investigation

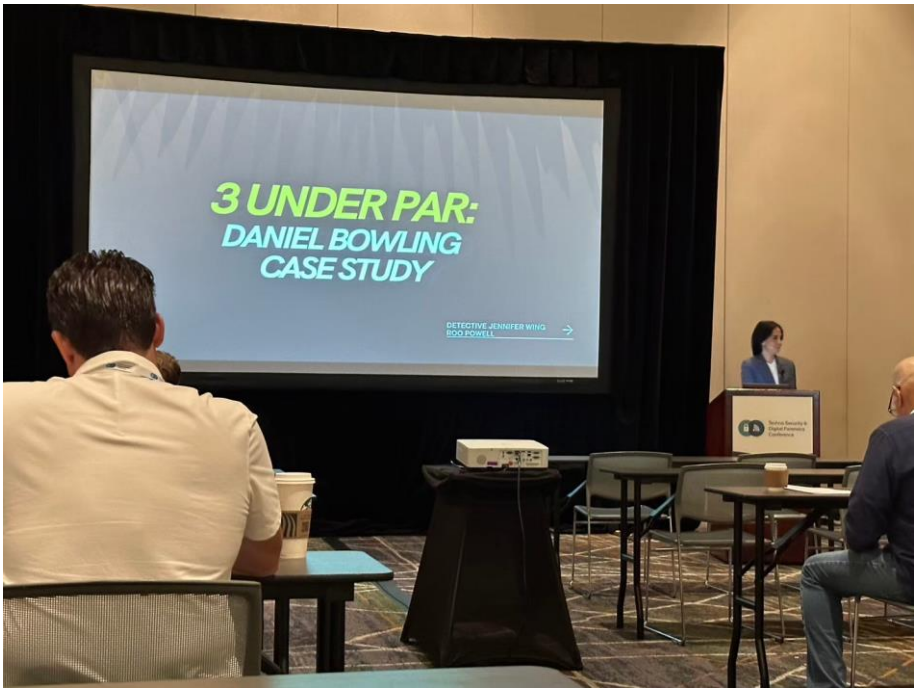
本場演講由美國海關及邊境保衛局實驗室主管 Andrew Michaels 展示如何進行無人機的鑑識，包括提取解密的數據，甚至已刪除覆寫的歷史紀錄，可與案件建立關聯的歷史地點資訊，約可萃取得

（七） 演講：“3 Under Par”: Daniel Bowling Case Study

本場演講的講者為 SOSA (Safe from Online Sex Abuse)的創辦人 Roo Powell，該組織會主動發掘網路上的性虐待案件並與執法機關合作，在執法部門的監督指導下，與犯嫌接觸聯繫，取得最新即時的犯罪證據。

講者親自扮演未成年女孩與犯嫌對話，過程中不斷透漏自己為 14 歲，確保犯嫌知道對象為未成年女童，例如：還不能飲酒、要再 4 年才能開車，而且要深入了解該年紀的女孩會有怎樣的行為、用語，包括會使用的 emoji 圖示，因為犯嫌會不斷要求傳送自拍照，因而布置了一個兒童房間，作為專屬拍照環境。

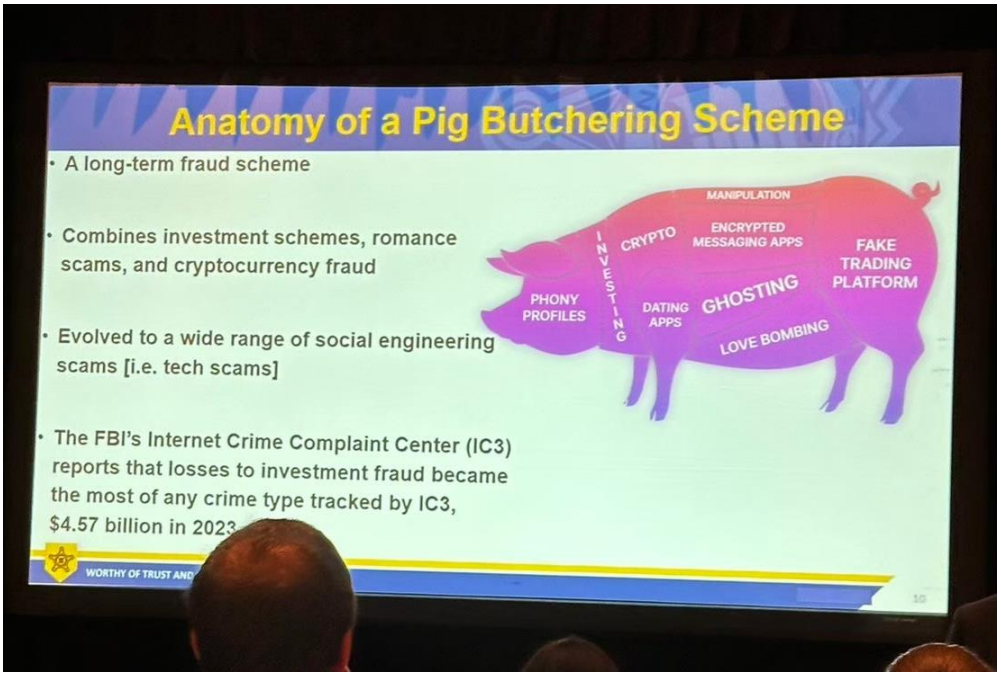
過程中也不斷索取犯嫌的生活背景，進而縮小實際出沒地點，最終鎖定位置而成功逮捕。



（八） 演講：Cryptocurrency Investigations – Pig Butchering

本場演講由鑑識分析師 Kyle Krueger 及調查分析師 Jose “Cruz” Uriarte 分享加密貨幣犯罪的調查案例- Pig Butchering，介紹了當前盛行的詐騙手法及常見流程，其中 IC3(FBI Internet Crime Complaint Center)統計 2023 年投資詐欺以 45.7 億美金位居詐騙金額的第一名。犯嫌多以通訊軟體尋找被害人，分享自身奢華的生活誘使被害人渴望一同投資獲利；亦或設下愛情陷阱，以情感拉攏被害人參與投資等，後先回饋小額獲利，被害人嘗到甜頭後通常便會投注更大筆資金，然於欲提領回饋時，便開始虧損或是要求支付手

續費或稅金。此類詐騙通常具有相當規模的分工及跨國運作，包括人口販運廉價勞工、於中國或新加坡架設網路伺服器、於東南亞開立銀行帳戶等，並利用加密貨幣進行洗錢，會運用混幣器或跨鏈換幣的方式，增加追查金流的難度。



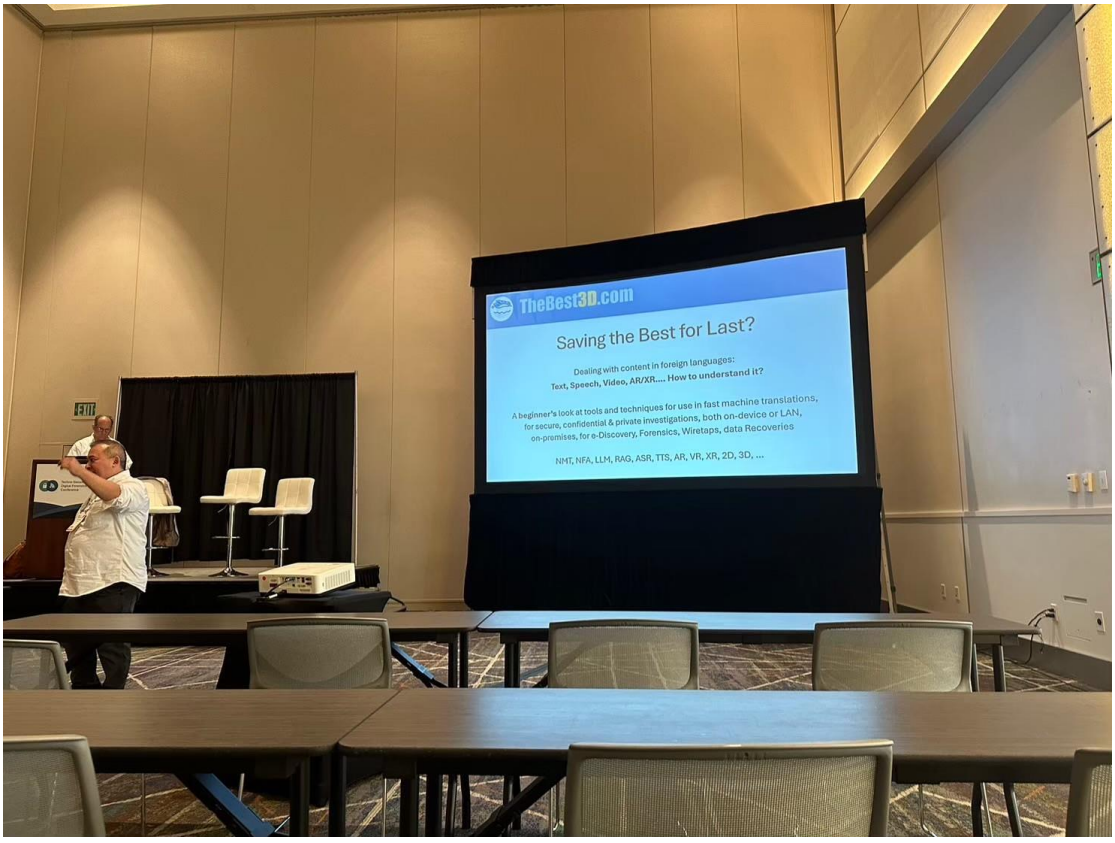
（九） 演講：Gilberto Segura, VP of Technology - PGLSNMT, NFA, LLM, VR, AR, 3D, ASR… Exploring New Technologies to Use for Investigations

Ballroom C

Phillip Staiger, Consultant in machine translation and multimedia - TheBest3D.com

Terrence Lewis, Translator and Software Developer

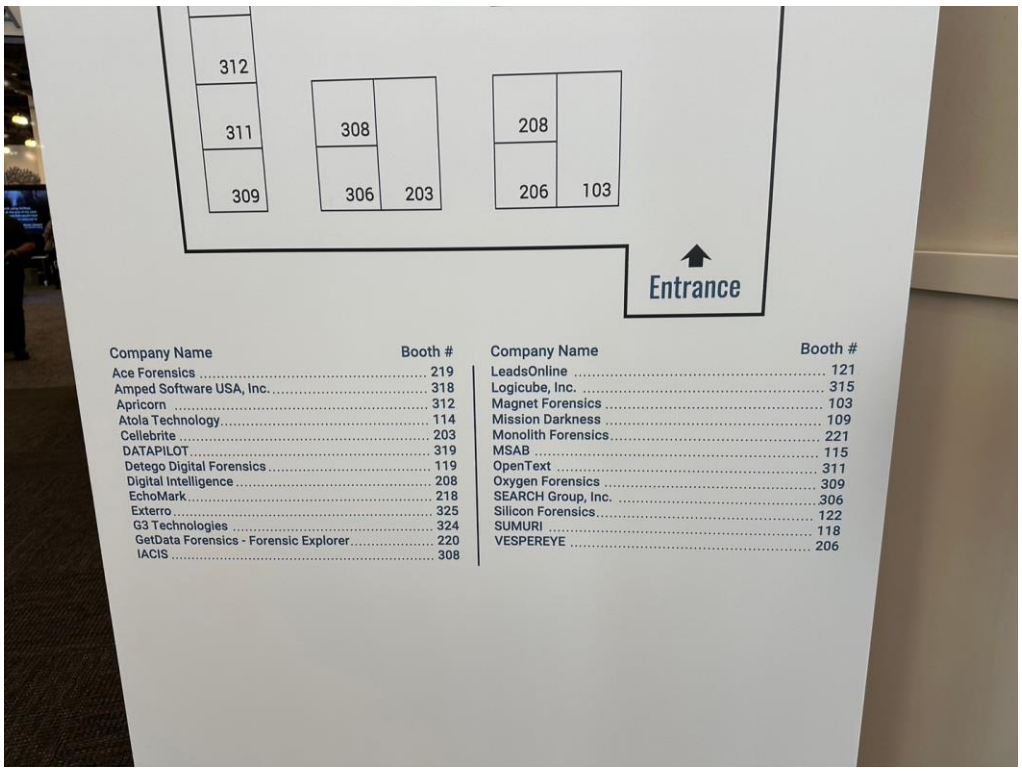
Steve Braich, Computational Linguist, Localization Consultant - Robotic Polyglot

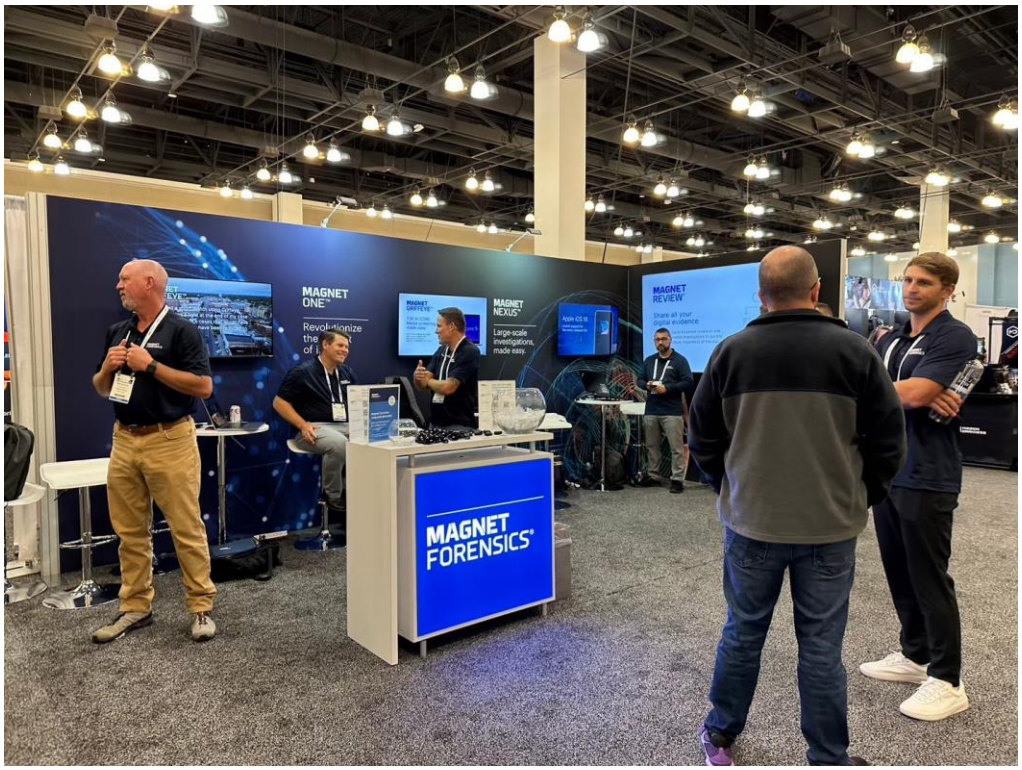


本場演講為 TheBest3D 公司介紹

（十） EXPO 會場展覽

該會議分為兩種型式，包括會議廳的專題演講及展場的廠商商品展示。本次參展的軟硬體廠商眾多，領域涵蓋數位鑑識、虛擬貨幣追蹤、DFIR 及 E-Discovery；各廠商在展場以設攤的方式，供與會人員參觀。可以瞭解目前數位鑑識的最新發展，並可實機觀看設備或直接操作軟體，尤其若先於專題演講獲取相關背景知識職操作介紹，再至現場操作，會更能了解該產品的特性和功能，像是 Detego 及 TheBest3D 都強調他們軟體的語言辨識及翻譯功能，恰能測試其中文的辨識及翻譯能力，這些產品未來或有機會用於數位件事上；此外，亦可直接接觸產品的廠商，瞭解最新產品資訊及未來數位鑑識發展方向，此亦為赴國外參加研討會的重要性，與國際接軌並交流。


312
311
309
308
306
203
208
206
103
Entrance
Company Name Booth #
Ace Forensics 219
Amped Software USA, Inc. 318
Apricorn 312
Atola Technology 114
Cellebrite 203
DATAPILOT 319
Detego Digital Forensics 119
Digital Intelligence 208
EchoMark 218
Exterro 325
G3 Technologies 324
GetData Forensics - Forensic Explorer 220
IACIS 308
Company Name Booth #
LeadsOnline 121
Logicube, Inc. 315
Magnet Forensics 103
Mission Darkness 109
Monolith Forensics 221
MSAB 115
OpenText 311
Oxygen Forensics 309
SEARCH Group, Inc. 306
Silicon Forensics 122
SUMURI 118
VESPEREYE 206


MAGNET ONE
MAGNET NEXUS
Large-scale investigations, made easy.
MAGNET REVIEW
MAGNET FORENSICS

參、心得及建議

一、 心得感想:

本次研討會的演講內容涵蓋了數位鑑識、區塊鏈與虛擬貨幣的安全性、暗網及公開來源情報（OSINT）的應用等多個領域，對數位證據的收集、分析與應用有了更深入的了解。

AI 技術正在改變數位鑑識的工作方式，尤其是在處理大數據、圖片、視頻等非結構化數據方面。Triage 和 Selective Extraction 等工具的介紹，對如何提高證據處理的效率和準確性有了更具體的了解。

許多案例都強調了公開來源資料（OSINT）的重要性。現今的數位犯罪往往隱匿於暗網或使用匿名化技術，而結合公開資料和暗網行為的分析，能夠為案件的破獲提供新的視角。Meltego 等工具的介紹，顯示了如何有效整合公開資料來輔助追蹤。

隨著數位犯罪日益增多，數位鑑識工作者需要不斷提升自己的專業能力，特別是在區塊鏈、暗網及 AI 領域的知識。參加這類研討會能夠為執法部門提供新的技能和方法，促進學術界與實務界的交流。

這些資訊對未來的數位鑑識工作至關重要，無論是在追蹤虛擬貨幣犯罪還是應對網路犯罪，都是值得深入研究和應用的領域。

二、 建議:

(一)提升調查人員調查虛擬貨幣案件之能力:

區塊鏈的匿名性使得虛擬貨幣成為洗錢和詐騙活動的工具，這要求執法機關不僅要掌握數位鑑識的技能，還需了解區塊鏈技術及其各種交易手法，在調查虛擬貨幣案件時，必須有更強的數據分析能力來應對複雜的幣流隱匿技術。

(二)現有的鑑識工具和技術需要與時俱進

未來發展應加強跨領域合作與技能融合，數位鑑識不僅僅是技術層面的挑戰，還涉及到對犯罪行為的理解。隨著數位犯罪手段的日益複雜，現有的鑑識工具和技術需要不斷更新。