行政院各機關因公出國人員報告書
（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：股　長　林芳如
警務正　郭彥伶
偵查正　徐綵薇
偵查員　王婷琪

出國地區：美國洛杉磯、帕薩迪納
出國期間：112 年 9 月 6 日至 9 月 15 日
報告日期：112 年 12 月 5 日

目次

壹、摘要

本局於本年度派員赴美國參加 Techno Security & Digital Forensics Conference 科技安全與數位鑑識研討會，該研討會廣邀政府、企業及民間組織，分享在網路安全、數位鑑識、科技偵查及電子蒐證之技術與合作經驗，透過各類議題之研討，及與各國執法人員之交流，對本局持續提升科技犯罪偵查與數位鑑識能力有相當助益。

另藉由參訪聯邦調查局區域電腦鑑識實驗室、國土安全調查署數位鑑識部門之機會，瞭解美國數位鑑識單位之空間規劃、設備配置、教育訓練、鑑識工作流程等實務運作情形，並與數位鑑識人員進行實務經驗交流。此次參訪收穫許多可作為本局借鏡之處，對於本局未來數位鑑識實驗室的發展有很大的幫助。

貳、目的

本次行程為參加美國 Techno Security & Digital Forensics Conference 科技安全與數位鑑識研討會，該研討會舉辦迄今已逾 20 年，議程廣邀政府、企業及民間組織，分享在網路安全、數位鑑識、科技偵查及電子蒐證之技術與合作經驗，並有多家國際數位鑑識廠商前往參展。本局為因應犯罪者利用科技進行犯罪、隱匿或消滅犯罪跡證等挑戰，需汲取國際間經驗並學習新興科技偵查工具與技術，爰指派筆者參與會議，以持續提升本局科技犯罪偵查與數位鑑識能力，並促進與各國執法人員、科技犯罪調查企業、學界專家交流、互動；會前並參訪聯邦調查局區域電腦鑑識實驗室、國土安全調查署數位鑑識部門，與數位鑑識人員進行實務交流。

參、過程

行程表

112 年		行　　程	任　　務	備　　註
日　　期	星 期			
9 月 6 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 7 日	四	參訪	參訪洛杉磯地區聯邦調查局（FBI）區域電腦鑑識實驗室（RCFL）	美國洛杉磯
9 月 8 日	五	參訪	參訪洛杉磯執法機關	美國洛杉磯
9 月 9 日	六	參訪	參訪洛杉磯警察局（LAPD）博物館	美國洛杉磯
9 月 10 日	日	前往帕薩迪納	搭車前往帕薩迪納	美國帕薩迪納
9 月 11 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 12 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 13 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 14 日	四	返程	由美國洛杉磯搭機返回臺灣（飛航時間計 13 小時 50 分）（當晚於機上過夜）	美國洛杉磯 返回臺灣
9 月 15 日	五	返程	預計當（15）日下午 5 點 5 分飛機抵達臺灣	臺灣

一、參訪聯邦調查局（FBI）區域電腦鑑識實驗室（RCFL）

美國的區域電腦鑑識實驗室（Regional Computer Forensic Laborator，簡稱RCFL）是聯邦調查局（FBI）與其他聯邦、州和地方執法機構之間合作，組成的數位鑑識工作小組，負責該區域內的電腦、智慧型手機和其他連網工具等設備之數位鑑識。RCFL 計劃創建於 2000 年，至今全美已有 16 間實驗室。我們所參訪的實驗室位於橘郡（Orange County），從門口即有管制措施，入門後即是受理櫃檯，櫃檯旁亦設有電腦設備，供送件員警處理相關送件表單。由於實驗室屬於管制區域，因此內部禁止拍照，僅能於入口大廳處合影紀錄此次參訪。

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，瞭解該實驗室的證物立案及收案流程、證據監管鍊、副本製作及證據檔案存放，並參觀了供執法人員或律師操作或檢視數位鑑識案件的分析室、鑑識人員的工作區、監視器影像分析室及教育訓練室，與本局數位鑑識實驗室相比，該實驗室的工作區域更大且人員更多，鑑識人員均配備多台個人工作站，在硬體規格上比本局更優，主要工作區域介紹概述如下：

（一）自助採證區

簡要說明送鑑單位可以在這個區域自行操作數位鑑識軟體，進行簡易的數位採證，現場也會有人員協助。

（二）證物清點編號

演示送鑑的證物會登入系統後，給予證物編號，並逐一進行封裝，有制式的證物標籤及證物袋。

（三）數位鑑識工作區

簡要說明工作區有的鑑識設備，包括法拉第箱、智慧型手機充電架、手機破密設備等。

（四）鑑識人員辦公室

展示每個鑑識人員的基本設備，包含複製機、防寫器及線材工具包等，電腦也區分鑑識用、撰寫報告使用及內部系統使用等 3 臺，最後帶至實驗室唯一會進行設備維修的鑑識人員位置，介紹其工作還包含晶片焊接等回復工作。

（五）監視影像整合處理

展示說明該工作為整合案件所有監視錄影畫面，以供法庭上進行檢視，瞭解案件發生的過程。影片來源包含員警身上的密錄器、行車

紀錄器及涉案場所之監視器,經影片編輯軟體將多角度畫面整合為一支影片，並加入時間、地點及重點標示（例如：畫圈）等解說資訊。

（六）教育訓練室

簡要說明教育訓練之環境，主要為電腦教室，而一個專業的鑑識人員訓練，一般需要耗費 2 年的時間。

（七）證物室

展示數位證物存放之空間，簡要說明證物袋在每一次拆開，都需將在剪開之塑膠條上簽名放入證物袋中，鑑識完成後再將證物袋密封，以記錄證物的鑑識經手的歷程，鑑識檔案的歸檔機制，最後會以磁帶之方式儲存。

（八）系統機房

說明由於該實驗室是 FBI 與其他聯邦、州和地方執法機構之間合作組成，各單位使用不同系統，尤其 FBI 有專門的系統線路。

此外，並於參觀過程中得知，由於該實驗室人員匯集除 FBI 以外的司法或執法機關，故其成員組成面相齊全，且其成員雖非屬 FBI，但對於數位鑑識領域有興趣，故可於該實驗室服務，除可降低人員流動率，有助於該實驗室的穩定運作外，我們認為由於數位鑑識領域的專業培訓不易，且相關培訓課程亦十分昂貴，數位鑑識人員實為數位鑑識實驗室最大的資產與投資，然如因機關所屬編制而限縮實驗室成員的組成來源，著實有點缺乏彈性，FBI 的做法值得本局作為借鏡。

參觀結束後，於會議室進行經驗交流，討論到數位鑑識案件的證物數量與日俱增，如何有效辦理作業並迅速提供鑑識結果，實為實驗室面臨之挑戰。我們現行常遇到一案送多件電子設備，導致鑑識量能不足的問題，美國 RCFL 則有規定一案件最多收 8 件電子設備，變相要求送件單位必須經過篩選，以解決鑑識量能損耗的問題。另外，詢問關於深偽影音之數位鑑識，目前該領域非 RCFL 實驗室所負責，由於偽造的影音對於選舉可能產生不確定性的影響，導致社會動盪，目前 FBI 也有專責的單位負責處理。最後提到有關數位鑑識後擷取的資料，未來是否有規劃將資料進行關聯式分析處理，美國的 RCFL 回應尚無規劃，但是個不錯的想法。透過這次參訪，瞭解美國的 RCFL 運作及工作場域規劃，給了我們很多啟發，對於未來實驗室的發展有很大的幫助。會後，我方並送上本局的紀念徽章予該實驗室，代表我方對於其提供雙方交流的機會之感謝，希能未來有更多交流合作之機會。

筆者在先前 108 年參訪舊金山的 RCFL 後，即將該實驗室設置供執法人員操作或檢視數位鑑識案件的分析室的做法帶回本局，供外勤大隊人員可至數位鑑識實驗室使用手機鑑識軟體取證，以使偵查人員更即時取得數位鑑識的檔案；本次參訪認為其證物袋封緘及存放，亦可引為本局實驗室的參考，尤其證物送抵實驗室後，可能有許多配件、裝袋或紙條，若證物自副本室領出後，未妥善識別，易發生如紙條被遺落後，難以追查屬於哪個證物所有，為使證物保存流程更嚴謹完備，落實證物監管鍊，本局實驗室的證物保存確實有可精進之處。

二、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，簡稱 HSI）是隸屬於美國國土安全部（United States Department of Homeland Security，簡稱 DHS）的主要調查機關，屬於美國聯邦政府的一個執行機關，負責處理涉及跨國犯罪和安全威脅的調查，尤其是與美國海關和移民法的相關犯罪組織，HSI 在美國有 10 個負責數位鑑識的單位，我們係參訪位於洛杉磯長灘的數位鑑識部門。

參訪議程分為組織工作介紹、參觀數位鑑識工作區域與設備及交流討論等 3 階段進行，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、證物室及規畫中的法拉第室，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）組織工作介紹

此 HSI 數位鑑識部門主要負責洛杉磯全區的數位鑑識，辦理警察

初階、高階教育訓練，並協助地方警察機關建置數位鑑識實驗室。這部門有 8 位偵查員（investigator）及 2 位支援技術人員，數位鑑識流程說明如下：

1、數位證據取得（Digital evidence obtained）：在數位鑑識進行前，偵查人員須依規定事先取得令狀（搜索票）與證據搜索票，並於網路填表錄案。

2、鑑識請求（Forensic request）：偵查人員提出數位鑑識需求。

3、資料取得（Data acquisition）：運用設備擷取手機、電腦、儲存媒體、雲端等數位證物資料。

4、鑑識處理（Forensic processing）：將擷取之數位鑑識資料進行分析、刪除還原等鑑識處理。

5、調查人員對證據的審查（Review by investigator）：請調查人員前來確認鑑識結果是否符合需求，並同步確認是否需要修正、修正之鑑識方向為何。

6、從鑑識工具產生報告（Reporting from forensic tool）：將數位鑑識之結果匯出報告檔案。

7、鑑識人員撰寫報告（Examiner authors forensic report）。

8、提供報告予調查人員（Reports provided to investigator）。

（二）參觀數位鑑識工作區域與設備

1、數位鑑識設備

HSI 使用之副本製作機 Falcon、手機破密取證工具 Graykey、電腦鑑識軟體 Magnet AXIOM 皆與本局相同，較為特別的是，由於地域遼闊，他們出勤支援現場鑑識時會攜帶體積非常大的工具箱，工具箱內包含電腦副本製作工具、手機鑑識工具及各類基本線材等。

2、鑑識人員辦公室

每位鑑識人員均有 Encase、X-Ways、Magnet AXIOM 等數位鑑識分析軟體，以及硬碟複製機、防寫器及線材工具包，Graykey 則由專門負責手機鑑識的人員進行操作。另外，若為兒少性剝削類型之案件，由於案件特殊、證據需要保密並僅能由負責偵查人員、數位鑑識人員檢視，故設有獨立的數位鑑識空間及工作站，用於檢視、分析、處理此類案件之數位證據。

3、證物室

電腦、手機等證物皆存放於證物室，其中手機有獨立的充電置物櫃，手機可以整齊放置且充電非常方便，並易於檢視充電情形，令我們印象深刻，可作為本局參考。

圖片說明：手機充電置物櫃

4、法拉第室（Faraday room）

由於美國 eSIM 的使用非常普遍，手機、平板等證物容易透過 eSIM 的網路竄改、抹除數位證據資料，因此他們訊號遮蔽器、法拉第袋、法拉第箱的使用需求相當重要。HSI 為建立更加健全之 eSIM 手機處理流程，他們已在規畫建立全美數位鑑識實驗室第一間法拉第室（Faraday room），所有須訊號遮蔽之工作將來皆可在法拉第室處理，確保數位證據之完整性與證據能力。

參觀結束後，於會議室進行經驗交流，互相分享於鑑識實務工作所遭遇之困難與挑戰，亦藉此機會詢問關於深度偽造影音之數位鑑識作法，該部門表示此議題係由中央相關單位進行研處。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工作流程、工作區域規劃及設備等。其中，手機充電置物櫃、法拉第箱及法拉第室的概念，以及就兒少性剝削等敏感案件建立獨立數位鑑識空間等，皆值得納入本局未來數位鑑識實驗室規畫之參

考。我方於會後致贈本局紀念徽章，表達我方對於此次交流機會之感謝，並期盼未來有更多機會進行交流與合作。

三、參訪洛杉磯警察博物館

洛杉磯警察局（Los Angeles Police Department，簡稱 LAPD）是位於美國加州洛杉磯的警察機關，並為美國第三大的執法機關；洛杉磯警察博物館（Los Angeles Police Museum）透過引人入勝的展覽和稀有文物來展示 LAPD 豐富歷史，並且係以之為使命而創建之博物館。博物館建築物本身亦歷史悠久，前身為高地公園警察局（Highland Park Police Station），現已被註冊為國家歷史地標。

博物館展示了洛杉磯警察局近 100 多年來的發展歷史，從早期的警用裝備到現代先進科技裝備，以及各個時期的警用歷史文物，如古老的電話、手銬、警棍、各個年代的警車、制服、警帽、徽章、照片檔案等，甚至還有防爆車及警用直升機，讓身為警察的筆者也目不暇給。其中筆者認為館內最特別的部分是保留著 20 世紀初的監獄，床鋪、馬桶、洗手臺、鐵欄杆等一應俱全，讓人有著身歷其境的感覺。

館內並以展覽的方式陳列了許多該城市歷史上知名的重大治安事件，包括曼森家族（Manson Family）案、北好萊塢搶劫案等，這座博物館除了展示該城市的警察歷史，其用心的陳列方式，亦使民眾得以深入瞭解過去警務

工作所面臨的艱辛和挑戰，以及警察機關對當地治安的貢獻。

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 112 年 9 月 11 至 112 年 9 月 13 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

112 年 9 月 11 日（星期一）	
12:00-13:00	Radio Forensics – What It Is and How It Can Help With Investigations（偵查類） 地點：Ballroom G 講師：Dominik Gieralt, Eugene Kim
	Case Management & Integrated Quality Management: Why Is this Important for the Future of Digital Forensics? （鑑識類） 地點：Ballroom F 講師：Larry Depew
	Future Forward – Examining Technology Changes to Plan for the New Realities of Digital Evidence（偵查類） 地點：Ballroom C 講師：Ali Kamdar
	Wireless Visibility: The MUST for Zero Trust（資安類） 地點：Ballroom B 講師：Brett Walkenhorst
	Path of a Defense Case （鑑識類） 地點：Ballroom H 講師：Brandon Reim
13:15-14:15	Recovering and Carving Data from SQLCipher Encrypted Databases（鑑識類） 地點：Ballroom F 講師：Matthieu Regnery
	eDiscovery...What's In It For Me?（電子蒐證類） 地點：Ballroom H 講師：Bree Murphy, Patti Zerwas, Laura Anne Day
	Everything You Need to Know About Mac Timestamps: Understanding POSIX and Apple Extended Attribute Timestamps （鑑識類） 地點：Ballroom C 講師：Andrew Pomerleau
	OSINT Tools and More（偵查類） 地點：Ballroom B 講師：Cynthia Navarro
	Trusted Authentication with Unique ID Token（資安類） 地點：Ballroom G 講師：Don Malloy
	SPONSOR DEMO: Shaping the Future of Forensics: Your Voice

	Matters in the Physical Analyzer Ultra Interactive Feedback Session（贊助展示） 地點：Ballroom A 講師：Matt Goeckel, Mark Tacconelli
14:45-15:45	Accelerating DFIR Investigations & Workflow with Hardware（鑑識類） 地點：Ballroom C 講師：Manny Kressel
	iOS Forensics – The Good, The Bad, and The Ugly（偵查類） 地點：Ballroom F 講師：Maria Khripun
	Courtroom Strategies for Mobile Forensics（鑑識類） 地點：Ballroom B 講師：Matt Goeckel
	Using AI to Improve Your Life- Techniques & Concerns（資安類） 地點：Ballroom H 講師：Richard Greenberg
	SPONSOR DEMO: Digital Forensic Automation: How Nashville Metro Police demolished their mobile device backlog and accelerated justice with Magnet AUTOMATE（贊助展示） 地點：Ballroom A 講師：Trey Amick, Chad Gish
16:00-17:00	Overcoming the Fake News of Deepfakes - Techniques for Video Authentication（鑑識類） 地點：Ballroom C 講師：Melissa Kimbrell
	Cloud and Network-based Evidence Sources for Malicious Insider Investigations（偵查類） 地點：Ballroom H 講師：Rick Baca
	Advancing Digital Forensics: Efficient Approaches for On-Scene Investigations（偵查類） 地點：Ballroom G 講師：Mike Bates
	What to Expect When You Are Expecting （to testify）（鑑識類） 地點：Ballroom F 講師：Don Vilfer
	SPONSOR DEMO: Filling the Gaps in your Investigations with

	XRY Pro（贊助展示） 地點：Ballroom A 講師：Jaime Hauseman, Adam Dale
	Common Repairable iPhone Logic Board Problems: Fix the Board, Recover the Data（鑑識類） 地點：Ballroom B 講師：Jessa Jones
112 年 9 月 12 日星期二	
8:30-9:30	KEYNOTE: The DFIR Investigative Mindset: Hack your Mind to Crack the Crime 地點：Ballroom B/C 講師：Brett Shavers
9:45-10:45	Ask Me Anything: Securing Active Directory from Attacks（資安類） 地點：Ballroom H 講師：Derek Melber
	Tackling Collaboration Software, Social Media & Text Messages With a ChatGPT Twist（鑑識類） 地點：Ballroom G 講師：Julie Lewis, Addison Bradley
	SPONSOR DEMO: Taking Your Investigations to the Next Level: Boosting Your DFIR Skills with Belkasoft X（贊助展示） 地點：Ballroom A 講師：Maria Khripun
9:45-12:00	The Kidnapping of Alani C. – Dangers of Online Gaming（偵查類） 地點：Ballroom F 講師：Colleen Stanich
11:00-12:00	How to Identify and Mitigate Hacker Obfuscation Techniques（鑑識類） 地點：Ballroom G 講師：Tony Lauro
	E-Discovery and Mass Disasters: How to Respond to Investigations and Litigation（電子蒐證類） 地點：Ballroom H 講師：Ronald Hedges
	I've Been Called to Testify! What Should I Expect?（鑑識類） 地點：Ballroom B

	講師：Raul Mejias
	Evidence on Trial: Identifying Digital Evidence Management Best Practices for Compliant and Accelerated Investigations（鑑識類） 地點：Ballroom C 講師：Ryan Parthemore
	SPONSOR DEMO: Collecting and Analyzing Mobile Evidence in the Workplace（贊助展示） 地點：Ballroom A 講師：Trey Amick, Matt Fullerton
13:30-14:30	AI's Impact to Security（資安類） 地點：Ballroom G 講師：Dr Keith Clement, Ervin Daniels
	Web 3: Embracing Possibilities & Mitigating Risks（資安類） 地點：Ballroom H 講師：Melissa Heidrick
	Geolocating Vehicles Using Open Source Data（鑑識類） 地點：Ballroom C 講師：Stephen Lewington
	Data Blackouts – Examining the Causes and Challenges for Law Enforcement When Collecting Digital Evidence and Cloud Stored Evidence Data（偵查類） 地點：Ballroom F 講師：Ali Kamdar
	Forensic Threat Hunting with Digital Evidence（鑑識類） 地點：Ballroom B 講師：Dan Sumpter
15:15-16:15	Security Is As Security Does. Law Enforcement's Great Migration To Operating Securely In The Cloud（鑑識類） 地點：Ballroom C 講師：Kevin Davis, Scott Montgomery, Chad Gish, Joshua Dobyns
	Solving the Puzzle: How Ediscovery and Investigations Fit Together（電子蒐證類） 地點：Ballroom H 講師：Mubashir Hussain
	Hacking Demos, Dirty Secrets, Dangerous Lies, and Asset Intelligence（資安類） 地點：Ballroom G 講師：Ken Liao

	Pig Butchering: An Interactive Case Study（偵查類） 地點：Ballroom F 講師：Andrew Frey, Derek Wang
	SPONSOR DEMO: Mobile Device Faraday Shielding and Charging from Field to Lab（贊助展示） 地點：Ballroom A 講師：Ryan Judy
15:15-17:15	Using Open Source Tools for Memory Acquisition and Triage（鑑識類） 地點：Ballroom B 講師：Greg Tassone
16:30-17:30	Finding a Diamond in the Dumpster: Decoding RAM in Mobile Forensics（鑑識類） 地點：Ballroom F 講師：Adam Firman
	In-House Mobile Device Repair in a Forensic Setting ... Do I need It?（鑑識類） 地點：Ballroom C 講師：William Aycock
	Actively Engaging the Business in Security Initiatives（資安類） 地點：Ballroom G 講師：John Wallace
	Avoiding the Traps and Perils of Engaging in High-Profile /Public Figure Cases Successfully（電子蒐證類） 地點：Ballroom H 講師：John Wilson, Rene Novoa
	SPONSOR DEMO: A Crypto Tracing Showcase by Ciphertrace, a Mastercard company and Cellebrite（贊助展示） 地點：Ballroom A 講師：Nick Steegmans, Matt Goeckel
112 年 9 月 13 日星期三	
9:15-10:15	Public/Private Sector Cybersecurity Collaboration – The Key to Risk Management & Cybercriminal Defeat（資安類） 地點：Ballroom H 講師：David Chow
	Working Smarter - Critical Workflows in Analysis of CSAM（鑑識類） 地點：Ballroom C

	講師：Sherry Torres
	The Future of Python and Forensics（鑑識類） 地點：Ballroom G 講師：Chester Hosmer
	Pressing Snapchat to Extract Juicy Data（鑑識類） 地點：Ballroom F 講師：Matthieu Regnery
9:15-11:15	LE ONLY: Google Geofences: Understanding the Fundamentals & Dealing with Rejection（偵查類） 地點：Ballroom B 講師：Romy Haas, Danielle Ponce de Leon
10:30-11:30	LE ONLY: Who’ s Up There? RemoteID and Drone Forensics（鑑識類） 地點：Ballroom F 講師：Jansen Cohoon
	Transitioning from Public Sector to Private Sector（鑑識類） 地點：Ballroom C 講師：William Aycock
	Sad Face, Happy Face, or Shoulder Shrug? How to Navigate Emojis in E-Discovery（電子蒐證類） 地點：Ballroom G 講師：Brett Burney
	The Dark Web and Why It's Important to Your Investigation（偵查類） 地點：Ballroom H 講師：Todd Shipley
13:15-14:15	Enhancing Your Case With Digital Communications Exploitation（偵查類） 地點：Ballroom H 講師：Darryl Valinchus
	What’ s in Your Data? You Can’ t Govern What You Don’ t See（資安類） 地點：Ballroom C 講師：Sarai Schubert
	Firearms in Digital Multimedia Evidence（鑑識類） 地點：Ballroom F 講師：Motti Gabler
	Proactive Threat Hunting: Getting Left of Boom（偵查類）

	地點：Ballroom G 講師：Matt Lembright
	Hansken – Big Data Forensics（鑑識類） 地點：Ballroom B 講師：Luc Koevoets
14:30-15:30	**After the Crash: The Application of Digital Forensics in Motor Vehicle Collisions（鑑識類）** 地點：Ballroom G 講師：Jake Green, Spencer Mcinvaille
	Processing, Reviewing, & Producing Emerging Data Sources （EDS） （電子蒐證類） 地點：Ballroom F 講師：Deedra Smith, Andrew Freiheit, Collin Miller, Haydn Forrest
	Windows Memory Forensics: Unveiling Digital Artifacts and Collecting Volatile Data（鑑識類） 地點：Ballroom B 講師：Steven Bolt
	Introductory Linux Digital Forensics/Incident Response for IT Security and Enterprise Defenders（鑑識類） 地點：Ballroom C 講師：Thomas Millar
	Forensic Investigation of Email Client Tool Marks（鑑識類） 地點：Ballroom H 講師：Arman Gungor

2、展場出席廠商

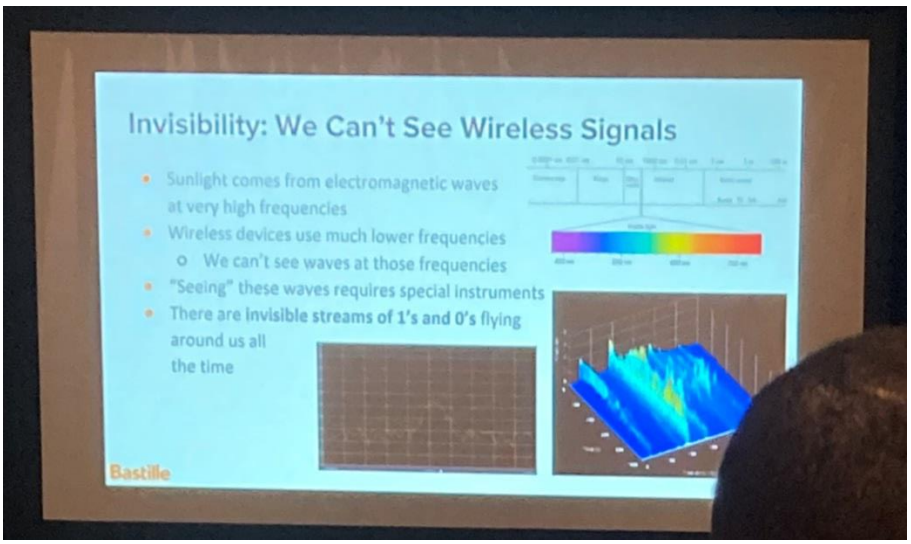
1	Magnet Forensics	17	Oxygen Forensics, Inc.	33	DekkoSecure
2	Belkasoft	18	ScanWriter	34	Digital Intelligence
3	Cellebrite	19	Teel Technologies	35	Evolver
4	CipherTrace	20	US DHHS-OIG, Digital Investigations Branch	36	Forensic Drone
5	MOS Equipment	21	Vespereye	37	G3 Technologies
6	MSAB	22	Vound Software	38	GreyCastle Security
7	ADF Solutions	23	Akerman LLP	39	Griffeye
8	Amped Software USA	24	Atola Technology	40	iPadRehab Microsoldering & Data Recovery

9	BlackRainbow	25	AVAIL Forensics	41	LeadsOnline
10	Ciphertex Data Security	26	Berla	42	MediaClone, Inc.
11	DATAPILOT	27	BitMindz	43	Silicon Forensics
12	Detego Digital Forensics	28	BlockChain Security	44	SkySafe
13	Exterro	29	Censys	45	SUMURI
14	Logicube	30	Chainalysis	46	Systools Mailxaminer
15	Monolith Forensics	31	Cyacomb Forensics	47	www.CTFDATA.pro
16	OpenText	32	Defense Forensic		

（二）演講：Wireless Visibility：The MUST for Zero Trust

本場主講人 Brett Walkenhorst 為 Bastille 公司的技術長，首先講者說明了成功的零信任方法始於持續監控，以瞭解不斷變化的網路設備、資源和連線，並識別惡意的活動。由於我們無法防禦看不到的東西，因此可見性是非常重要的。

然而，無線訊號無所不在、不可見且易被利用，講者進一步於會議中介紹 Bastille 公司的無線威脅偵測產品，用於偵測、定位和回應未經授權的蜂巢、藍牙、Wi-Fi 和物聯網設備，能夠監控無線基礎設施，及其設施內的每個無線設備，使其變得可見，有助於確保無線環境的安全。



（三）演講：OSINT Tools and More

公開來源情報（Open Source Intelligence，簡稱 OSINT）是現今科技犯罪偵查的重要工具之一，本場演講主要在增強聽者對於 OSINT 的理解，講者 Cynthia Navarro 從基礎認知講起，就調查時需注意的基本觀念進行重點整理，如：清楚瞭解正在搜尋的內容、保持客觀，不得考慮預設結果的偏見或個人想法、使用 2 至 3 個來源交互驗證所

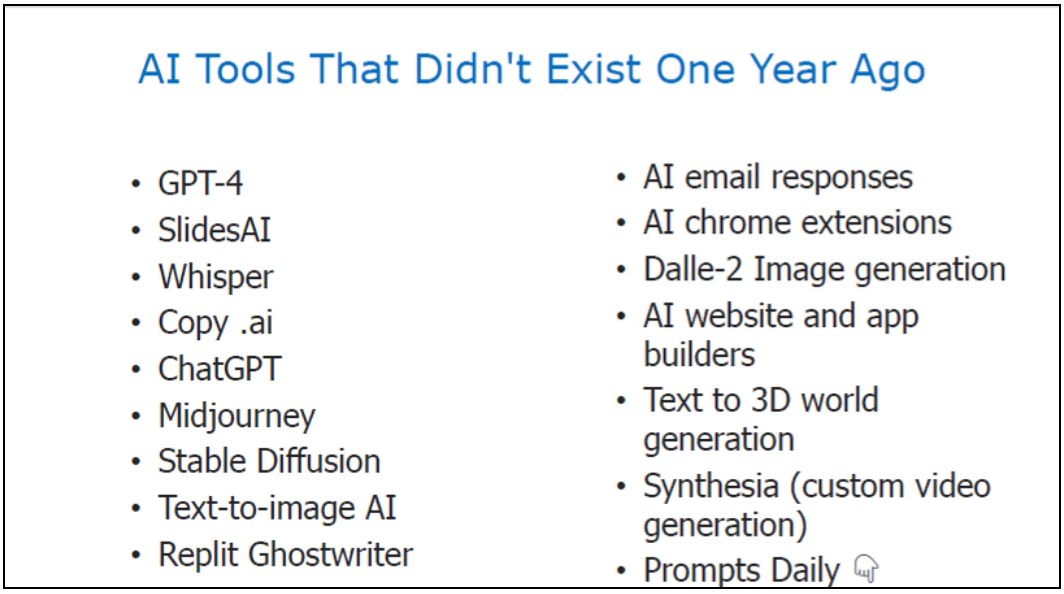
得資訊及記錄工作和流程等。

講者另整理並介紹許多有用的工具和資源，如：OSINT Framework、社群媒體網站清單、搜尋引擎清單、進階搜尋技巧、與 OSINT 相關的 Podcasts 和 YouTube 等，本議程系統性的整理與說明，對科技犯罪偵查人員欲快速瞭解 OSINT 重要觀念與工具而言，有相當大的助益。

（四）演講：Using AI to Improve Your Life- Techniques & Concerns

講者 Richard Greenberg 主要在講述如何充分利用人工智慧（AI）來改善我們的生活及其需要注意之處，講者分享了許多工具和運用在撰寫社群媒體文案、產品行銷文案等實際案例，其中令筆者最為印象深刻的是，現在許多人們耳熟能詳的 AI 工具，如 ChatGPT、Midjourney、Stable Diffusion 等在一年前都還尚未存在，顯見 AI 技術發展之快速。

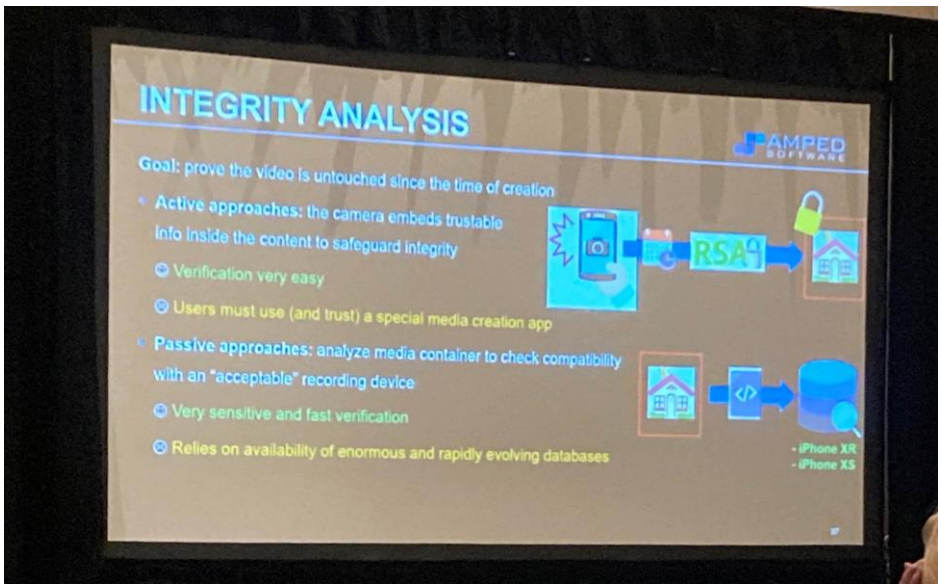
在 AI 改善生活的同時，亦需注意其存在著網路安全問題，由於 AI 系統可能會被欺騙而做出錯誤的決定或產生有害內容，易受到網路攻擊。另外，AI 技術將降低網路犯罪的門檻、製作令人信服的網路釣魚電子郵件將變得更加容易等，也是科技犯罪偵查人員需要持續關注的問題。



（五）演講：Overcoming the Fake News of Deepfakes - Techniques for Video Authentication

在這場議程中，主講人 Melissa Kimbrell 介紹深度偽造（Deepfake）的基本知識，如生成式對抗網路（Generative adversarial Networks，簡稱 GANs）、卷積神經網絡（Convolutional Neural Networks，簡稱 CNN）等，並以 Can we trust anything we see?為題進行後續討論。

在這個眼見不為憑的年代，講者提出了 4 個可能有助於辨別真偽的方法，分別為完整性分析（Integrity analysis）、傳統的多媒體鑑識法（Conventional multimedia forensics approaches）、以深度學習對抗深度學習（Deep learning to fight deep learning）及生理和行為法（Physiological and behavioral methods），供數位鑑識人員在使用檢測軟體之餘，亦可作為辨別的參考。



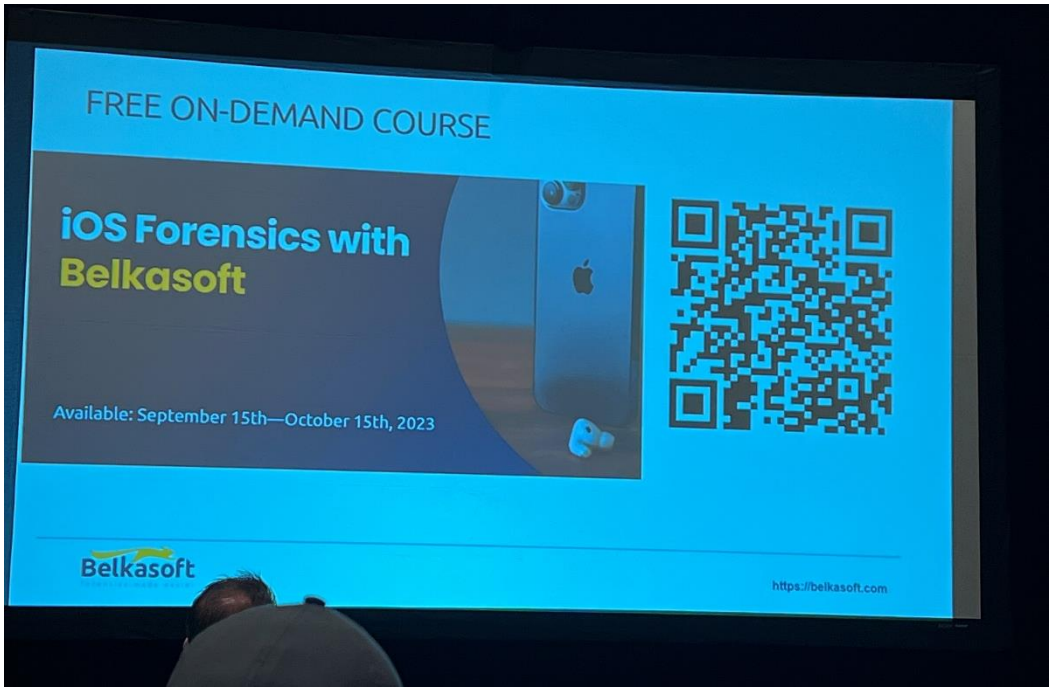
（六）演講：KEYNOTE：The DFIR Investigative Mindset：Hack your Mind to Crack the Crime

本場主題演講主要在講述進行 DFIR（為 Digital Forensics and Incident Response 的縮寫，中文為數位鑑識與事件應處）調查時，應秉持的原則及該避免的陷阱。主講者 Brett Shaver 從幾十年的案例工作，彙整成演講內容，首先從「DFIR 算是偵查嗎?」切入，提出進行 DFIR 不僅需要熟練鑑識軟體及硬體工具，更需要以一個偵查人員的立場進行思考，而在建構案件的過程中很容易受到既定成見、外在干擾及看待事物的角度影響，因而產生誤判甚至破壞調查。

講者 Brett 提出要避免既定成見，就必須從零開始，而不能確信該案與之前的某案或某人相同，對於外在干擾則必須識別干擾源並加以排除，才能真正地看到證據，此外看待事物的角度，則必須認知到存在相異、變動及可能對可能錯的情況。更建議聽者在思考的時候，要避免慣性思考、腦力激盪及情緒性思考，取代之的是，透過學習、認知、理解、應用及清楚表達，進而對於經由觀察、聆聽及接觸所收到的訊息，進行整理、過濾、分析、思考、選擇並開始行動。最後以「I might be wrong」勉勵聽者，透過驗證錯誤的過程，取得正確的結果。

（七）演講：SPONSOR DEMO：Taking Your Investigations to the Next Level：Boosting Your DFIR Skills with Belkasoft X

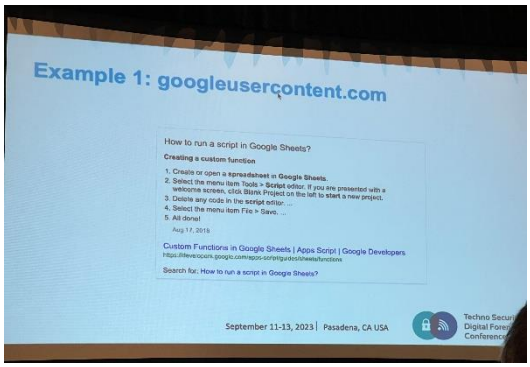
本場演講主要展示最新的 Belkasoft X 產品功能，該產品為 Belkasoft 公司推出的鑑識軟體，支援行動裝置、電腦、記憶體、無人機及雲端。講者 Maria Khripu 先從產品功能展示開始，首先為開箱即用（即 out-of-the -box）的提取功能及自動化工具，能簡化工作流程並增強調查過程，並強調雲端部分的執行能力及編排工作流程的方式，包含 Belkasoft X 及第三方工具。簡介產品功能後，以多類型裝置案例（在同一案例中擁有電腦、手機、無人機及雲端）實機展示前述功能。最後提供免費的線上工具課程供聽者於會後能多瞭解該產品。

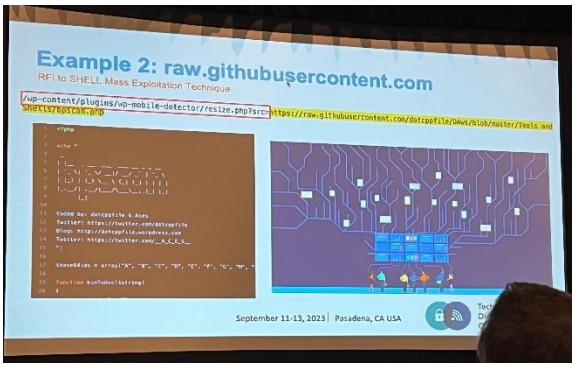


（八）演講：How to Identify and Mitigate Hacker Obfuscation Techniques

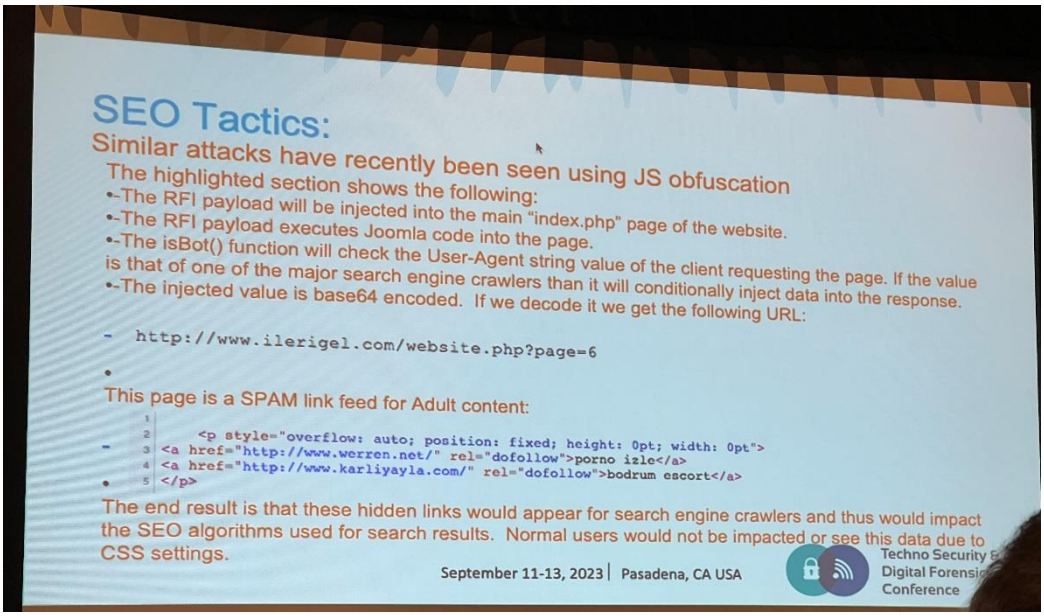
本場演講主要在講述如何識別攻擊手法中混淆（Obfuscation）技術，講者 Tony Lauro 現職為阿卡邁（Akami）科技公司的安全技術及策略主管。講者提出 5 種常見的混淆技術分類，前 3 種為一般為人熟知的模仿（impersonate）、受信任網站（Trusted site）及人類智慧結晶（Human Ingenuity）技術，後面 2 種為講者自行分類，稱之為「Shot in the dork」及「Final Battle」。

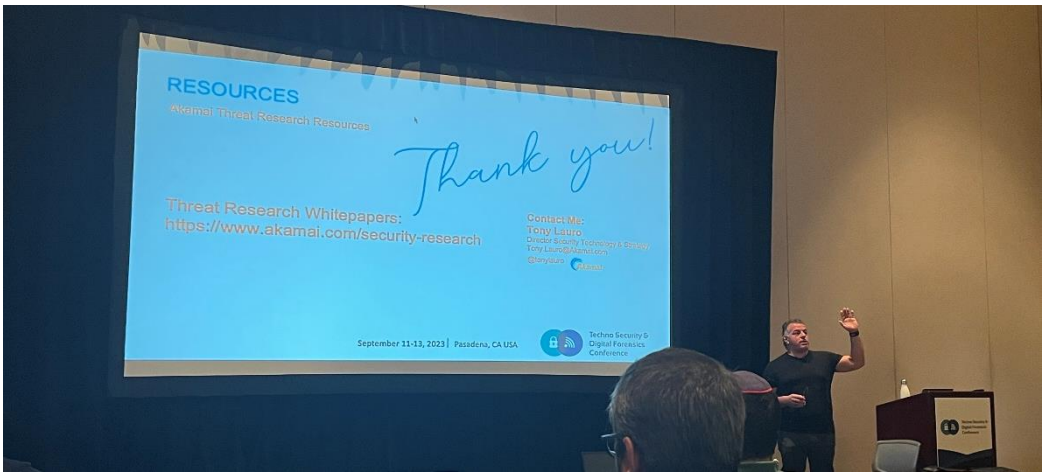
模仿（impersonate）技術部分，講者談到了 Good Bots，相關服務包含：正面 SEO（Search Engine Optimization 即搜尋引擎優化）、Google 表單及 Google Bots，駭客會透過 bad Bots（即模仿 Good Bots）進行攻擊，因此可以透過驗證（verify）Good Bots 及管理（manage）Bad Bots 的方式辨識。受信任網站（Trusted site）部分提到「googleusercontent.com」及「raw.githubusercontent.com」為例子，駭客利用受信任網站騙取信任，用以植入惡意程式碼進行攻擊。





人類智慧結晶（Human Ingenuity）部分，提到「Cybersole 5.0」、「Shopify.io」及「Dashe.io」等網路平台大量倚賴 API 及 Bot 進行運作，導致遭惡意濫用。接著是「搜尋引擎優化的手法」，類似的攻擊近期較常見的是使用 JavaScript 混淆技術，將 RFI Payload 放在網站的主要索引頁面（index.php page），並透過 payload 執行 Bot（）功能讀取相關數值，將隱藏連結提供給搜尋引擎，進而影響搜尋結果。此外講者提到，他們觀察到近期線上免費 PHP 混淆器服務的使用率上升，而 PHP 混淆器服務可以規避 WAF 的安全性偵測。整場演講透過實際案例進行解說，對於聽者而言，不僅易懂更印象深刻。



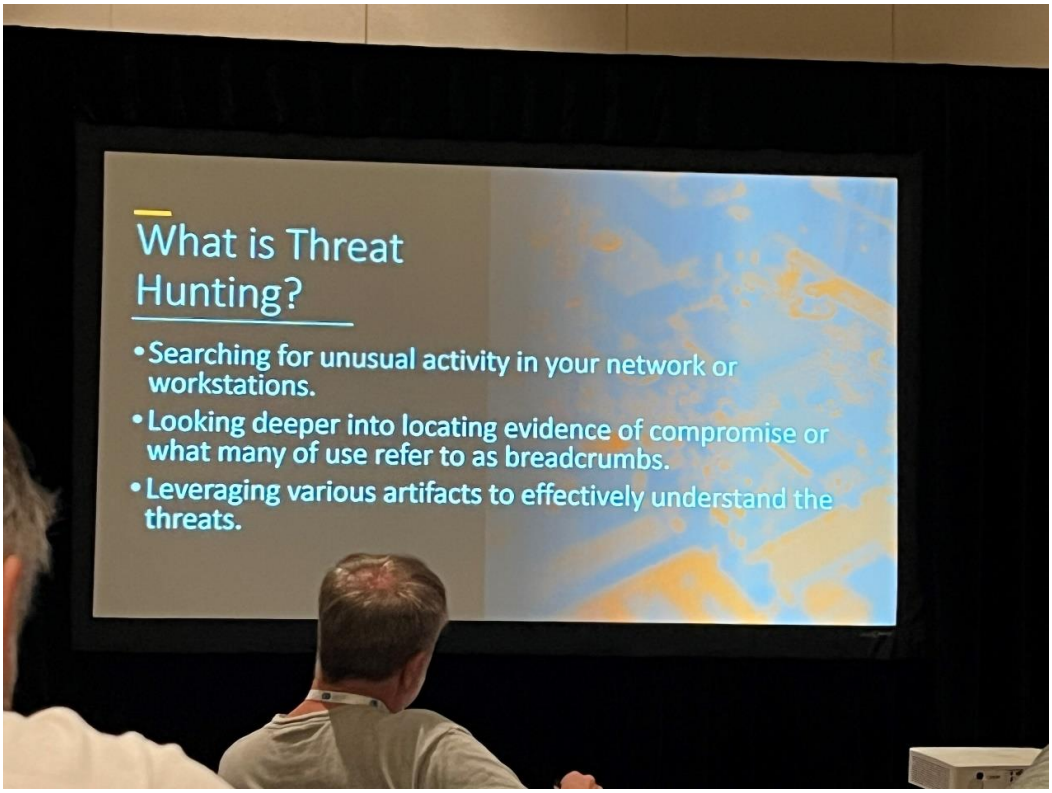


（九）演講：Forensic Threat Hunting with Digital Evidence

本場主題主講人 Dan Sumpter 深入探討「使用數位證據進行鑑識威脅獵捕」的重要性，特別是針對內部威脅與外部侵入。數位跡證不僅限於入侵防護系統（IPS）、入侵檢測系統（IDS）與防火牆系統，本地端伺服器的紀錄，包括日誌、文件和使用者活動紀錄等，亦可以提供調查人員有價值的關鍵證據。

威脅獵捕包含主動式和被動式，主動式方法包括在網路或工作站中尋找異常活動，而被動式方法則是深入本地端受威脅的證據，有效地進行風險控管並保全記憶體等相關數位證據。威脅防護機制包括 SIEM、SOAR、EDR、XDR、IDS 和 IPS 等資安防護，均有助於紀錄資安或駭侵事件的經過，達到防護與保全的目的。

本場演講強調了數位證據在威脅獵捕中的關鍵作用，以及如何利用這些證據來有效地追蹤和應對威脅。最後介紹 Windows event viewer、FTK-system summery tab 兩項工具在處理相關數位證據之應用，對於提升駭侵案件或資安事件的數位鑑識技術具有相當的參考價值。



（十）演講：Security is as Security Does. Law Enforcement’ s Great Migration to Operating Security in the Cloud

本場主題探討「執法部門資料遷移到雲端運營安全」的挑戰和優勢。許多行業利用雲服務已經十分普遍，然而對於執法部門，特別是在數位鑑識領域，須特別謹慎並考慮資訊安全的風險。

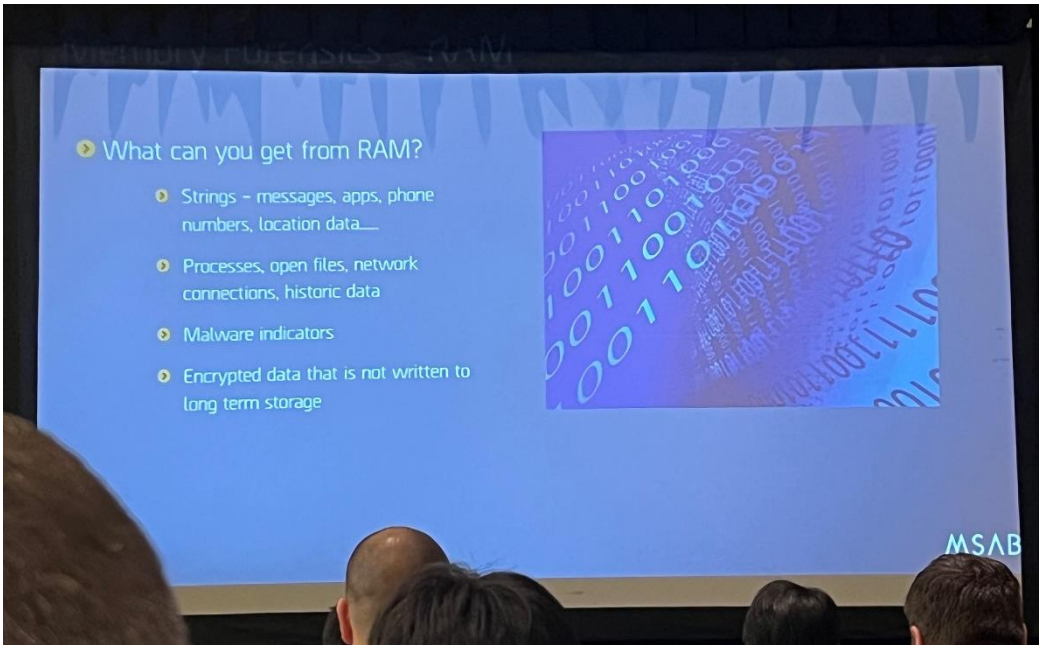
講者們 Kevin Davis, Scott Montgomery, Chad Gish, Joshua Dobyns 分享了遷移、利用和維持雲端環境安全性的最佳狀況，最大程度發揮科技犯罪調查中利用雲端技術的可用數位鑑識資源。隨著資料量的不斷增加，傳統儲存空間可能不足，使用雲端服務不僅價格更低、更可靠，而且還提供了便利的，亦不受制於硬體空間有限、可能故障毀損的問題，提高了整體操作的穩定性。雲端空間管理方面的選擇，可由執法部門自行建置管理或委外維護，各有優缺。

本議程呈現了執法部門在雲端安全方面的運用與面臨的挑戰，講者也介紹了西弗吉尼亞警方在 AWS 上建立犯罪資料庫的案例。回顧國內，本局於 107 年建置「雲端鑑識平台」也是將數位鑑識資料轉移到雲端，更方便備份、資料分享及傳輸。

（十一）演講：Finding a Diamond in the Dumpster：Decoding RAM in Mobile Forensics

這場演講由主講人 Adam Firman 介紹 RAM 解碼在行動裝置取證中的重要性，以及它對發現潛在重要資料的優勢。以下是研討會的重點：

多年來，電腦取證專家一直依賴 RAM 分析來發現有價值的證據，而在行動裝置取證中應用 RAM 解碼的技術，可能為數位鑑識帶來革命性影響。講者分享了一些 RAM 解碼工具，如 FORMOBILE 和 XRY，這些工具具備擷取及解碼 RAM 的功能，透過 RAM 解碼可以找到密碼、查看登入行為、獲取 Wi-Fi 密碼等資訊。同時講座中討論 RAM 解碼工具的操作，包括如何選擇任務、顯示字串、進行清除背景噪音等操作。這項技術將成為數位鑑識領域中一個引人注目的領域，可作為未來行動裝置取證的啟發。



（十二）演講：LE ONLY：Who’ s UP There? Remote ID and Drone Forensics

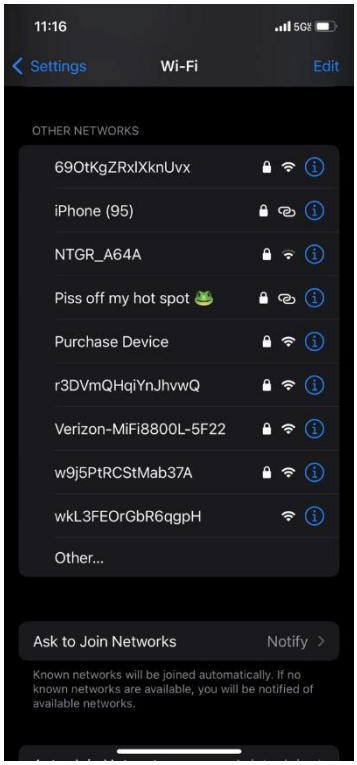
該次簡報由 V2 Forensics 主講，主題內容為如何利用無人機的 Remote ID 做偵查，並提供執法單位未來做無人機數位鑑識時的參考。關於無人機（Drone）引發的飛安議題，美國十分重視。自 2021 年 4 月 21 日起，所有無人機都要具備廣播自身 ID、位置、經緯度及起飛地的功能，但許多玩家對此廣播功能表示憂心，因為任何人只要有手機就能知道無人機的位置。

Remote ID 規定適用於向美國聯邦航空管理局（FAA）註冊的無人機，該無人機應內建有 Remote ID 系統或附加 Remote ID 模組，以供識別，Remote ID 主要依賴 3 種技術進行廣播：WiFi（802.11）、藍芽 5.0 及 4.0；未來非美國聯邦航空管理局 FAA 網站認可具 Remote ID 之無人機，只能在指定的區域飛行。

對於執法者而言，無人機可被應用在墜機現場的繪測、現場監控及 DFR（Drone First Responders），但無人機也將帶來一些隱憂，如可能被竊取的 GPS、鏡頭等訊息，其儲存的資料未做加密，可輕易的解析；此外，其日誌檔（Log）可能因為重新開機而被抹除（erase），也可能因為儲存空間不足而被刪除；無人機的儲存資訊過於分散，可能儲存於無人機本身、用於連線的手機 app 及 remote controller；很多無人機的操控器為 Android-based，可以利用 ADB 指令方式輕易與機器連線操作等。

偽造的 Remote ID（Remote ID Spoofing）是目前可預見的犯罪型態，執法者要如何從突然出現的大量的 Remote ID 中，判斷真偽，會是很大的挑戰，現場也示範 SSID Spoofing，突然產生大量的 SSID 供連線，以情境模擬方式體會 Remote ID Spoofing 的樣態（如下圖），短

時間內產生大量的 Wi-Fi SSID，待釐清的 SSID 會影響執法人員的偵辦速度，造成無法在最短時間內掌握關鍵資訊；此外，犯罪者亦可利用廣播的方式，讓所有被操控的無人機執行起降，將是大規模且分散的犯罪現場，對於執法者如何在短時間內緝凶，將是十分困難之挑戰。



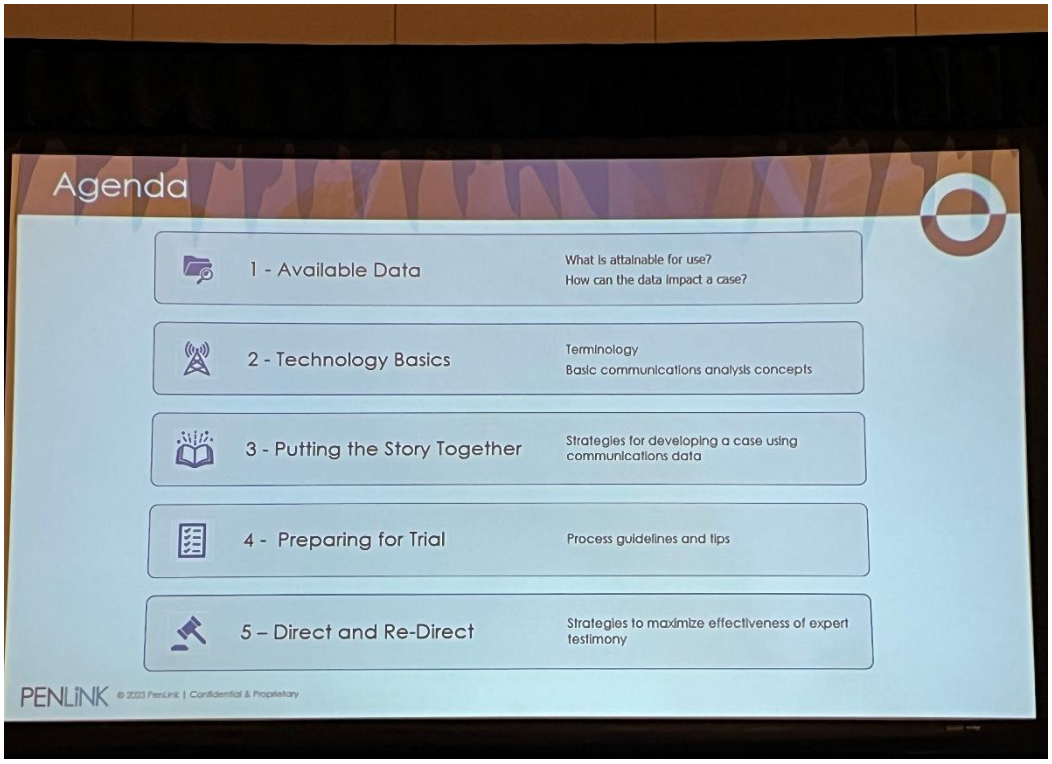
圖片說明：Spoofing（手機截圖畫面）

（十三）演講：Enhancing Your Case With Digital Communications Exploitation

在這場演講中，主講人 Darryl Valinchus 介紹如何運用手機、電子郵件、社交媒體和 Google 等數位通訊工具提升案件調查的效力。

在法庭上呈現數位證據時，需要確保數位證據的合法獲取與真實性。非法獲取的證據可能會被排除。因此保全數位證據的證據能力對數位鑑識人員來說一直是十分重要的。當數位證據十分複雜或需要釐清鑑識過程時，法庭會傳鑑識人員作為證人出庭進行技術方面的解釋，以確保法庭理解證據的技術細節。

數位鑑識人員出庭時，須說明數位證據與案件的相關性，可以使用時間軸、圖表等視覺輔助工具，使法庭更容易理解案件的發展經過。數位證據可能包含手機、電子郵件、社交媒體、Google 等不同資料類型， 在交互詰問中，證人須熟悉數位鑑識的資料種類，也要瞭解有關案件與數位鑑識程序的科技、通訊、電磁設備的相關法律內容，避免使用可能誤導法庭的資訊或有選擇性地解釋法律資訊。 透過聆聽這場演講，可以更加有效利用數位證據來強化案件調查和法庭表現，獲益良多。

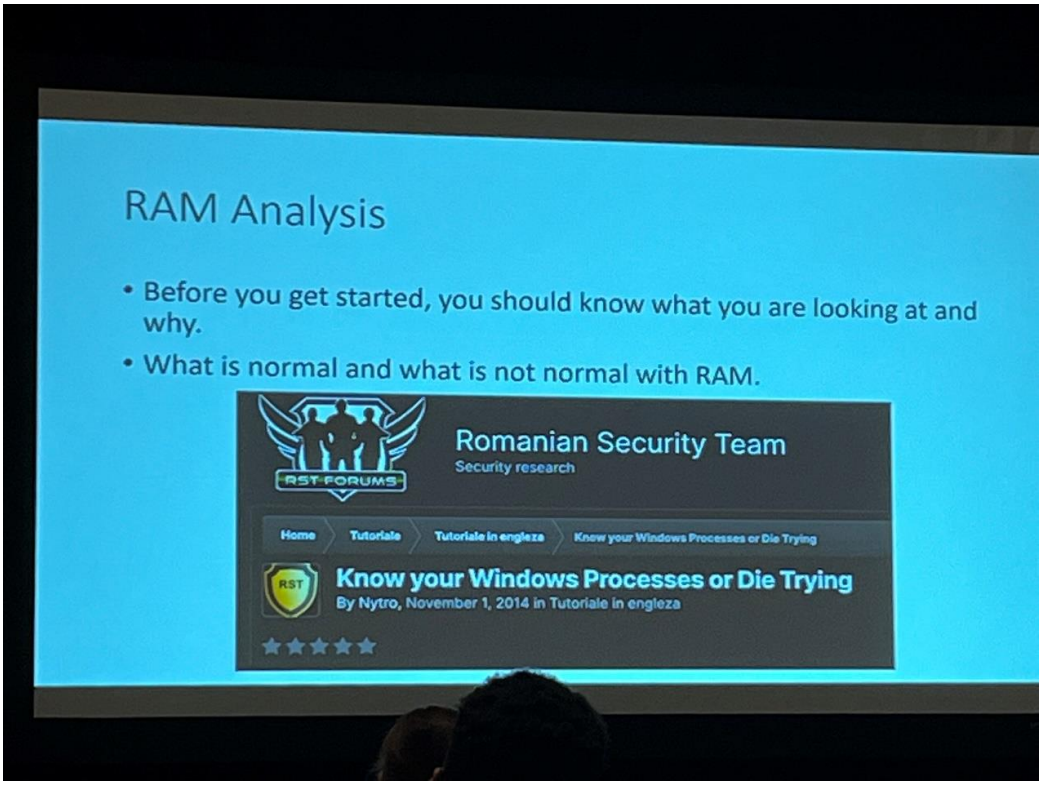


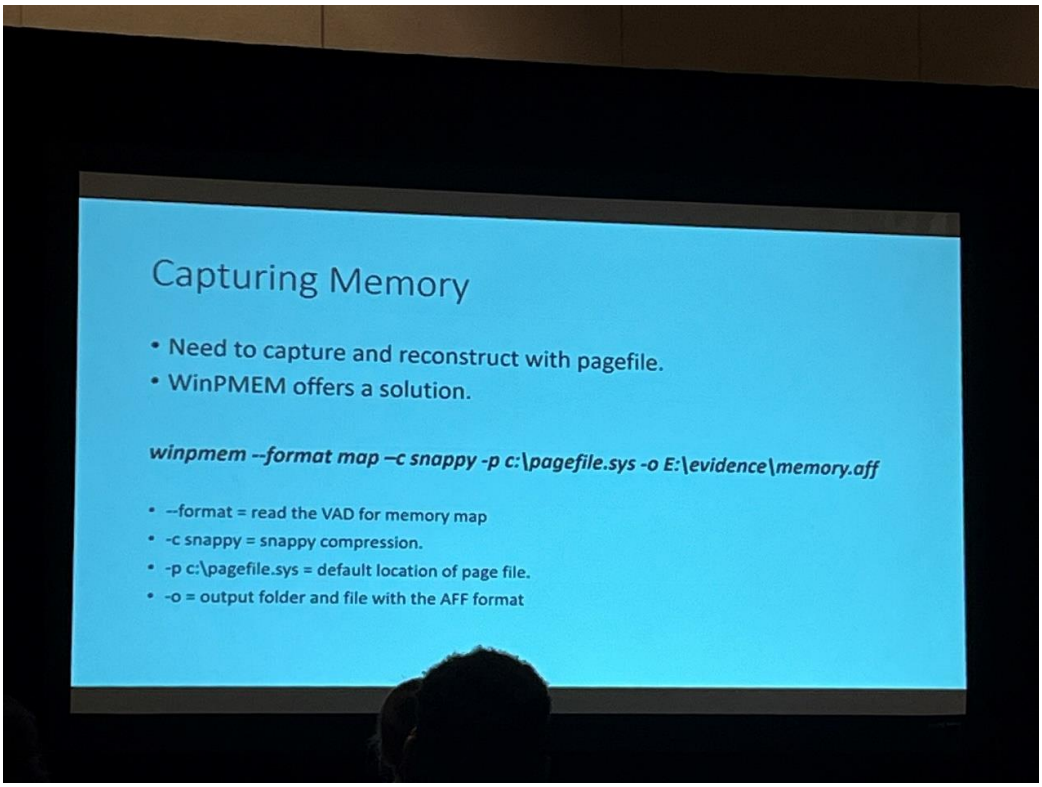
（十四）演講：Windows Memory Forensics：Unveiling Digital Artifacts and Collecting Volatile Data

在這場議程中，主講人 Steven Bolt 討論 Windows 記憶體取證的基本知識、揮發性資料擷取及相關分析工具（Bulk Extractor、FTK、Winpmem）的應用，並強調揮發性數位證據在事件中的重要性以及從揮發性記憶體中可取得 WER 文件、分頁文件、帳號密碼資料、程式

資訊、網路連接、已加載的 DLL 等。

本議程讓身為數位鑑識人員的我們瞭解如何有效面對 Windows 記憶體取證挑戰、取證揮發性資料的方法並於法庭上成功呈現。

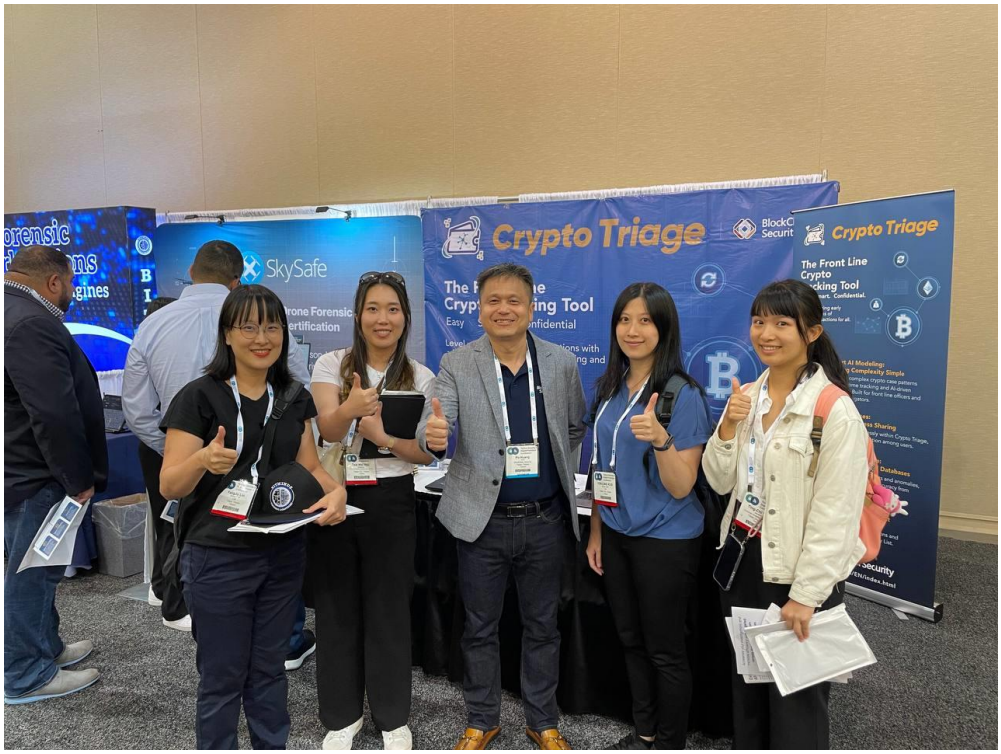




（十五）EXPO 會場展覽

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。該會議的場地安排得宜，展場與會議廳相鄰，筆者在各演講的空檔，即可步行至展場參觀，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。本次到多家廠商的攤位包括 Atola、Amped、Oxygen Forensics 及 Mission Darkness 等瞭解產品，利用本次研討會之 app，我已預先登錄個人之相關基本資訊，在與這些廠商討論後，對方直接掃描我的識別證，即可取得我的電子郵件等資訊，可會後寄送相關資料至我的電子信箱，十分便利；在 Atola 攤位看到 Atola TaskForce 2 的產品（如下圖），該產品升級後可連接 26 個 ports、支援 NVMe 硬碟、且設計 Device Rack，更適合做硬碟副本，讓筆者思考升級實驗室 Atola 產品的必要性，另外在 Mission Darkness 看到 Forensic Crack Cabinet，非常適合存放破密中手機的充電及管理；倘非參加這次的會議，由於目前我國使用之數位鑑識軟硬體均為歐美產品，國內僅有代理商代理，較難有機會可以看到或直接操作這些產品的實物；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。我國區塊科技廠商亦有赴該會議參展，亦是全場唯一亞洲參展廠商，筆者亦赴區塊科技的攤位進行交流（如下圖）。

圖片說明：Atola TaskForce 2



圖片說明：區塊科技攤位

肆、心得及建議

本屆 Techno Security & Digital Forensics Conference 科技安全與數位鑑識研討會議題種類豐富，分享者更是橫跨政府、企業及民間組織，顯見科技安全與數位鑑識在各國、各領域都已受到高度的重視。參加會議期間除既定之議題研討外，與各國執法人員、企業、學界專家之技術交流與經驗分享，亦是難能可貴的機會，本次會議收穫良多，於短時間內即獲得許多數位鑑識等相關新知，有助本局精進科技犯罪偵查與數位鑑識能力。

本次研討會有多家數位鑑識、虛擬貨幣追蹤、DFIR 及 E-Discovery 等領域之國際廠商參展，相較於國內較難有機會可接觸產品實物，於現場則可直接與產品廠商對談，瞭解最新產品資訊及未來發展方向，且多有實物展示甚或可操作最新設備，有助於筆者思考實驗室設備之精進及其必要性，以提升效能並與國際接軌，此部分亦為赴國外參加研討會的重要之處。

此次有機會能參訪聯邦調查局區域電腦鑑識實驗室、國土安全調查署數位鑑識部門，瞭解美國數位鑑識單位之實務運作情形，其中發現許多可作為本局借鏡之處，如：實驗室成員的組成來源、證物袋封緘及存放方式、設置手機充電置物櫃、法拉第箱、法拉第室、就敏感案件設立獨立數位鑑識空間等，經由實務經驗交流亦給予筆者很多啟發，有助本局實驗室的未來發展。

上述這次出國學習的收穫，於國內均較難取得相關資源或資訊，為即時掌握國際間數位鑑識重要議題與最新技術，建議未來持續安排數位鑑識人員參加國外相關研討會汲取新知，並藉由與各國執法人員進行交流，共同商討所遭遇困境之解決方法。

近年隨著科技設備的迅速發展與普及，科技犯罪手法不斷翻新，科技犯罪偵查與數位鑑識能力的重要性無庸置疑。本次研討會與參訪所接觸之相關領域從業及研究人員，多係在該領域深耕多年，具有豐富的經、資歷。優秀數位鑑識人才養成不易，除相關培訓課程昂貴外，亦需對該領域有興趣之人員長期投入、累積經驗，建議更加重視數位鑑識人員之長期培育。本次出國筆者獲益良多，學習到許多新的數位鑑識與科技犯罪偵查知識、工具和資源，對於未來工作相信將有相當的助益。