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「MAGNET USER SUMMIT 2023 數位鑑識研究會議」

服務機關：內政部警政署刑事警察局
出國人員：股長　洪振耀
　　巡官　林映榕

出國地區：美國納許維爾
出國期間：2023 年 4 月 15 日至 4 月 24 日
報告日期：2023 年 7 月 14 日

目錄

壹、摘要

近年來許多犯罪案件利用新興資通訊技術或科技產品做為犯罪工具，數位證物類型亦愈來愈多元，目前各國致力於探討及研發數位鑑識工具以輔助蒐證及分析，經由參加各式會議與各國經驗交流及技術分享，可藉此提升國內數位鑑識的能力及研究能量，以因應未來可能面臨的犯罪偵查挑戰。

目前本局數位鑑識皆實作於本科數位鑑識實驗室，透過跟進國際數位鑑識技術的發展、學習使用實用的數位鑑識工具等方式，增加國內數位鑑識人員的數位鑑識能力或數位證據分析能力是非常重要的課題，藉由參與國際的研討會來多接觸國外的實際做法，促進我們的數位鑑識能力、數位證據分析能力接軌國際，且能與時俱進。故此，本科為強化專業領域，培訓數位鑑識專業人員，於本年度派員赴美國參加「MAGNET USER SUMMIT 2023 數位鑑識研究會議」，透過各類數位鑑識議題之研討，精進各類數位鑑識之議題與技術。

透過與各國執法機關、學術單位之數位鑑識人員交流，期望能學習國際間最新的數位鑑識規範與技術，未來將可運用於數位證據蒐集與分析技術之實務情形上，學以致用，並配合內政部警政署辦理「精進警察科技偵察設備及人才培訓計畫」，將相關數位鑑識技巧推廣至全國各警察機關科技偵查人員，促進科技偵查人才培育，提升我國數位鑑識能量。

貳、目的

本次行程為參加美國 MAGNET USER SUMMIT 2023 數位鑑識研究會議，Magnet Forensics 為全球知名的數位鑑識公司，該公司舉辦 MAGNET USER SUMMIT 2023 數位鑑識研究會議，討論數位鑑識工具使用的程序、方法、技術及各類數位證據分析等議題研討，為持續提升本局數位鑑識與科技犯罪偵查能力，指派本局股長洪振耀與巡官林映榕等 2 人參與會議，於同時段分別參與不同演講，從中學習國際最新科技知識，提升數位鑑識人員對於最新犯罪偵查技術的認知，並與各國執法人員、學界專家互動、交流。

此行藉由參加研討會及參訪納許維爾警局(Metropolitan Nashville Police Department)、協助執法機關的非營利技術組織(Operation Lightshine)等機會，瞭解國外數位鑑識實驗室的建置、規劃、運作等，以作為國內各警察機關科技偵查、數位鑑識技術發展之借鏡，學習相關數位鑑識技術與趨勢。

參、行程

一、 行程表

112 年		預定行程	任務	備註
日期	星期			
4 月 15 日	六	啟程	啟程赴舊金山（飛航時間估約 11 小時 20 分）	臺灣前往 美國舊金山
4 月 16 日	日	啟程	美國舊金山搭機至美國納許維爾(飛航時間 4 小時 25 分)	美國納許維爾
4 月 17 日	一	會議	參加 MAGNET USER SUMMIT 2023 會議	美國納許維爾
4 月 18 日	二	會議	參加 MAGNET USER SUMMIT 2023 會議	美國納許維爾
4 月 19 日	三	會議	參加 MAGNET USER SUMMIT 2023 會議	美國納許維爾
4 月 20 日	四	參訪	參訪 納許維爾警局 (Metropolitan Nashville Police Department)	美國納許維爾
4 月 21 日	五	參訪	參訪 協助執法機關的非營利技術組織 (Operation Lightshine)	美國納許維爾
4 月 22 日	六	返程	美國納許維爾搭機至舊金山轉機(飛航時間 4 小時 53 分)	美國納許維爾
4 月 23 日	日	返程	由美國舊金山搭機返回台灣（飛航時間計 13 小時 30 分） (當晚於機上過夜)	美國舊金山 返回臺灣
4 月 24 日	一	返程	預計當(24)日上午 5 點 15 分飛機抵達台灣	臺灣

二、 數位鑑識研究會議日程表

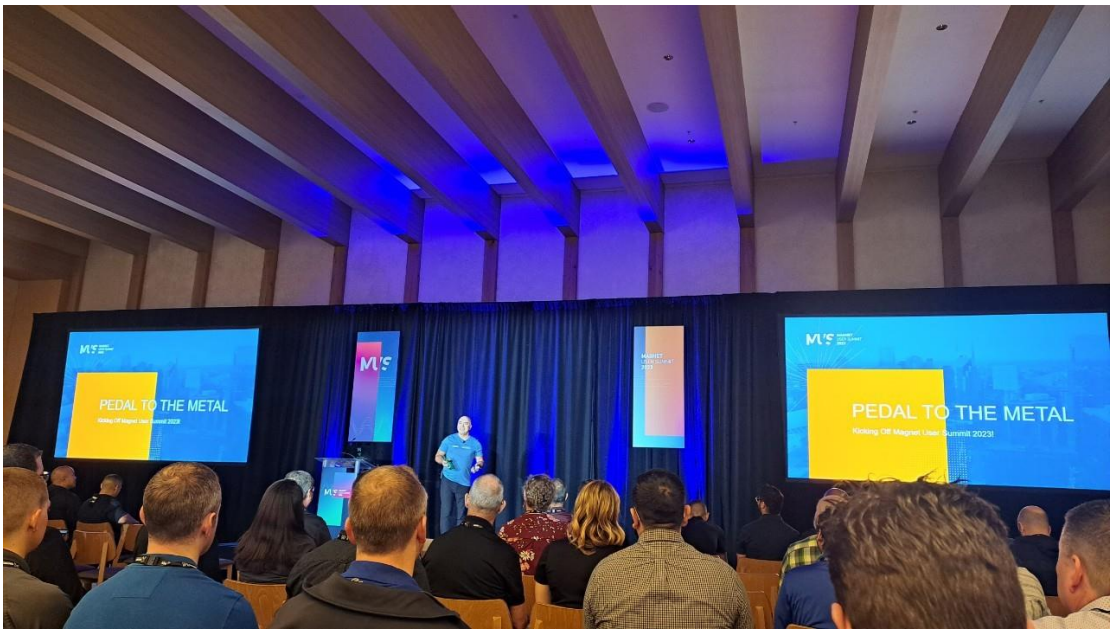
場次	時間	議程內容	說明及備註
第 1 天 4 月 17 日 (一)	14:00-14:45	議程一	在發生 COVID 後，工作場所發生資料外洩如何進行鑑識分析
	15:00-16:00	議程二	Magnet2Go.建立一個‘Windows to Go’推動支持離線蒐集 (下列講座同時進行) 1. 瓦解這個生物群系(Biomes) 2. 鑑識人員如何密碼破解(上)
	16:15-17:15	議程三	建立連線：闡明在 Windows 中遠端存取所留下的人為跡證 (下列講座同時進行) 1. 提升你的 LevelDB 技能 2. 鑑識人員如何密碼破解(下)
第 2 天 4 月 18 日 (二)	09:00-10:00	開幕：歡迎致詞	
	10:15-11:15	議程一	通往7的階梯:深入Magnet AXIOM 7.0 (下列講座同時進行) 1. 切洋蔥會讓你哭嗎 - TAILS 的鑑識分析 2. 說明 Magnet AXIOM Cyber 7.0 的新功能 3. 使用 AWS Config 補充 IR 調查
	11:30-12:30	議程二	使用 Magnet Forensics DFIR 解決方案更快地調查安全事件 (下列講座同時進行) 1. 調查事件回應的無文件威脅 2. 透過在您的影片工具包中加入 DVR Examiner 來增強您的影片結

			果 3. Oculus Quest“Meta”取證—可以完成嗎？
	13:30-14:30	議程三	搶旗工作坊：通過動手實踐參加 Magnet Summit CTF 比賽的技巧 (下列講座同時進行) 1. 智慧型手機中的活動追踪：回答是誰、在哪裡、何時以及如何！ 2. 在公共安全層面的 Magnet 鑑識解決方案：在每一步都擴大您的數位調查 3. DFIR 的執業者：eDiscovery 的瑞士軍刀
	14:30-15:00	中場休息	
	15:00-16:00	議程四	這個是從哪裡來的？ 顯示未識別 AirDrop 文件的發送電話號碼 (下列講座同時進行) 1. 企業雲端資料和 Magnet AXIOM Cyber 2. 位置，位置，位置。每項調查的一部分 3. 糾纏的網路：將 OSINT 和 DFIR 調查融合在一起
	16:00-16:30	中場休息	
	16:30-19:00	課程活動	搶旗 (CTF) 挑戰賽
4 月 19 日 (三)	10:00-11:00	議程一	將 DFIR 錯誤轉化為機會
	11:15-12:15	議程二	使用 Berla 在 Magnet AXIOM 中進行車輛取證 (下列講座同時進行)

			1. 使用 Magnet AUTOMATE 增強您的數位調查 2. 使用 Magnet AUTOMATE Enterprise 提高 DFIR 調查的生產力和效率
	13:30-14:30	議程三	為數位證據挑戰尋找合適的解決方案 (下列講座同時進行) 1. 自定義人為跡證：支持那些不受支持的 2. 知道記憶喪失時，該何時尋求幫助 3. 智慧型手機中的活動追踪：回答是誰、在哪裡、何時以及如何！
	14:30-15:00	中場休息	
	15:00-16:00	議程四	神探 Gadget：網路安全、事件回應和法律 (下列講座同時進行) 1. 雲端安全就跟安全一樣。執法部門大遷移到在雲端中安全的運行 2. 通往7的階梯:深入Magnet AXIOM 7.0 3. 說明 Magnet AXIOM Cyber 7.0 的新功能
	16:15-17:00	會議總結	

肆、MAGNET USER SUMMIT 2023 數位鑑識研究會議

本次數位鑑識研究會議聚集了各國數位鑑識專家、學者、執法人員等共同研究、討論使用數位鑑識工具取證、鑑識、分析等議題，本次參訪人員參加 2023 年 4 月 17 日至 4 月 19 日於美國納許維爾舉辦的場次。



圖片說明：MAGNET USER SUMMIT 2023 數位鑑識研究會議會場照片

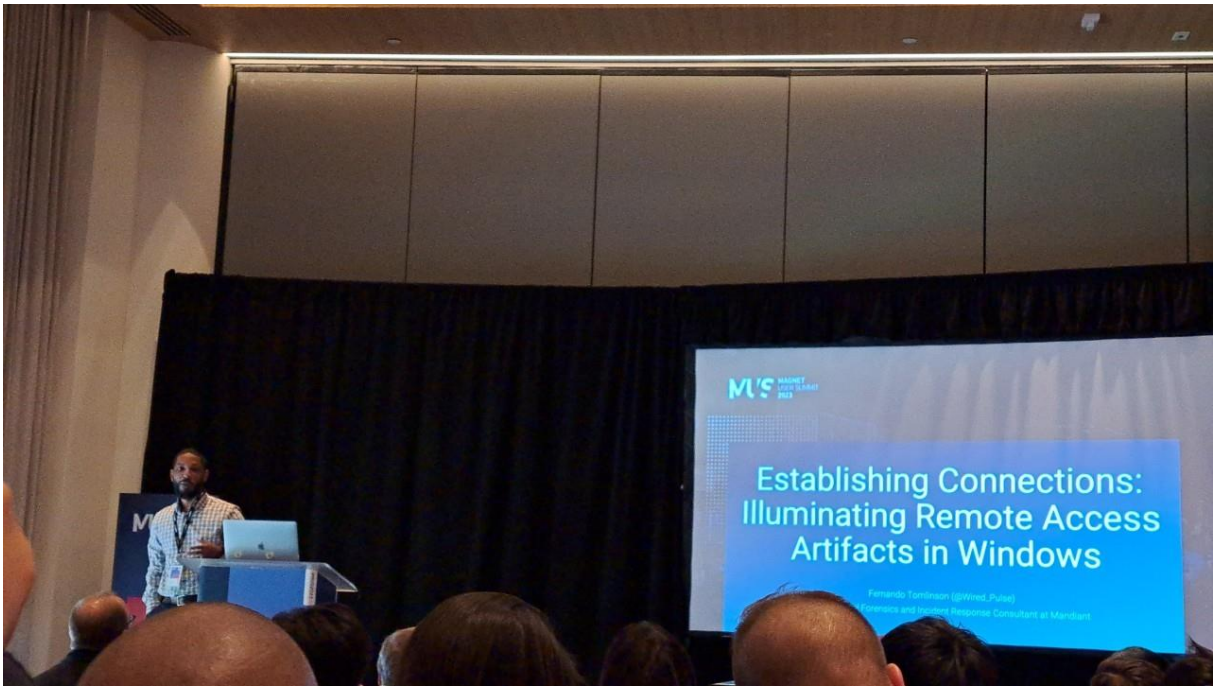
一、 建立連線：闡明在 Windows 中遠端存取所留下的人為跡證：

本議程講師為美國麥迪安網路安全公司(Mandiant)的數位鑑識與事件反應顧問 Ferando Tomlinson，說明 Windows 中遠端存取所留下的人為跡證。

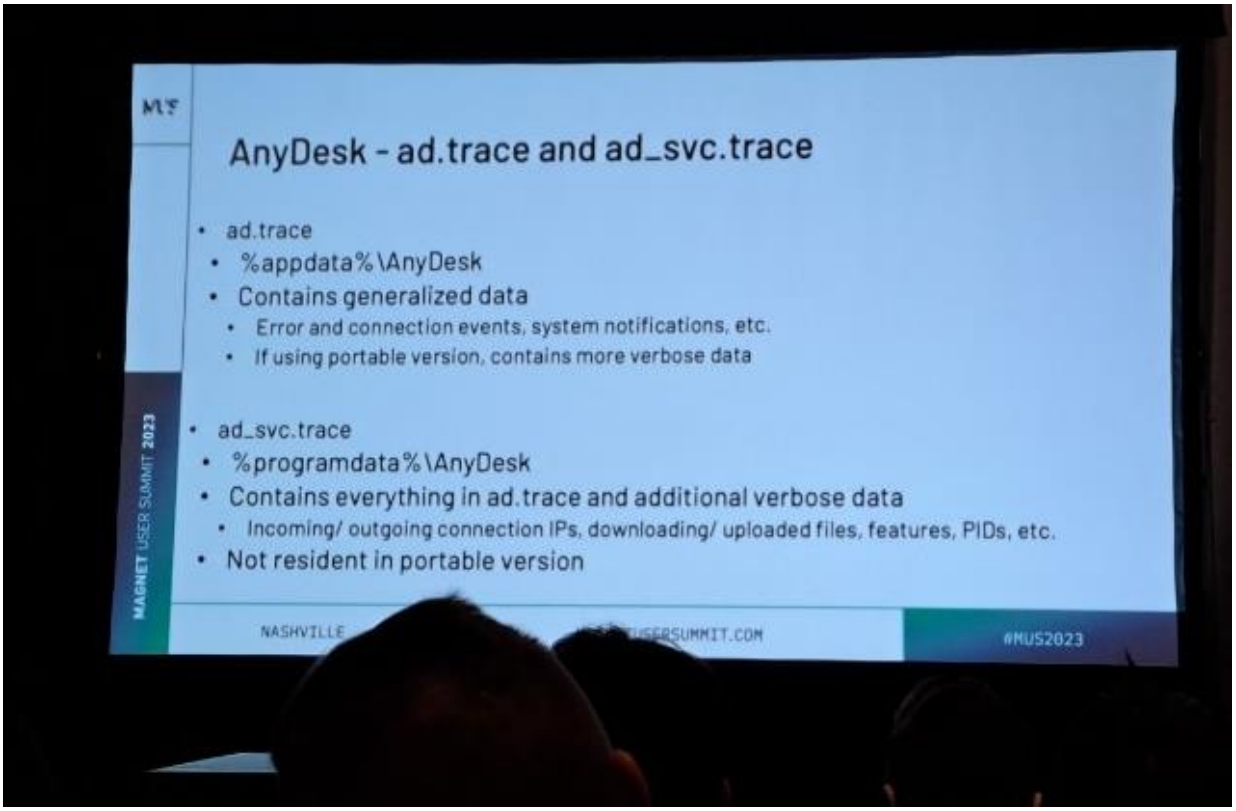
平常會使用到遠端連線的原因有：可以提升工作效率、在不同硬體裝置間能合作使用、能遠端提供技術上的支援。

以常使用到的遠端連線程式：AnyDesk 為例，在 connenction_trace.txt 的檔案裡面會存有一些連線的紀錄：時間戳記(timestamps)、連接的狀態(User、Reject、Passwd、Token)、提出遠端連線要求的起始點(Request origin)等人為跡證。

未來期許遠端存取所留下的人為跡證，能拓展至其他更多的遠端存取工具了解不同的遠端存取工具會留下哪些人為跡證、加入一些註冊資料來連結到 IP 位址、去發掘更多可靠的可能性連結還有地理座標等。



圖片說明：講師開始分享「建立連線：闡明在 Windows 中遠端存取所留下的人為跡證」



圖片說明：講師分享在 AnyDesk 裡找到的人為跡證

二、 通往 7 的階梯：深入 MAGNET AXIOM 7.0：

本議程講師為 Magnet Forensics Inc. 的創辦人兼首席技術長 Jad Saliba，原於加拿大擔任警官和數位鑑識調查員打擊網路犯罪幾年之後，Jad 決定於 2011 年創立 Magnet Forensics。他希望解決現代網路犯罪中技術不斷進步所帶來的挑戰。作為 Magnet Forensics 的首席技術長，Jad 和所有 Magnet 員工努力不斷研究數位證據取證、分析等工作，並提供數位鑑識軟體使世界各地數千個機構能夠在更短的時間內解決更多網路犯罪案件。

此次研討會 Jad 向大家說明 MAGNET AXIOM 更新出 7.0 的版本，還有其他子軟體也有更新，如：MAGNET AXIOM Cyber 7.0、MAGNET AUTOMATE、MAGNET REVIEW、MAGNET AUTOMATE ENTERPRISE 等，提供了新的功能來使世界各國執法單位能有更有效率的分析數位證據，提升解決犯罪案件的成功率。

而 MAGNET AXIOM 7.0 強化了 CSAM 技術與 AI 模組的整合、可以預先安排想處理數位證據的工作流程、可將數位證據標籤和評論並上傳到 REVIEW 區供不同使用者能交流、了解案情、查詢快速等功能。

圖片說明：簡報說明 MAGNET AXIOM 7.0 的新功能

三、 為數位證據挑戰尋找合適的解決方案

此講座係由三位講師以聊天的方式來討論現在面臨數位證據鑑識的挑戰以及該如何面對、尋找合適的解決方案。

講師提出了兩大現階段主要面臨的挑戰：

(一)現在 AI 技術越來越進步，Deep Fake 偽造影片的問題仍待解決，chatgpt 免費的開源軟體真的能安心使用嗎?是否會有假消息甚至演變成訊息戰等問題。

(二)雲端也是越來越多公司、企業甚至是政府正在使用的資料儲存方式，但也進一步衍生出雲端上資料共享的安全性問題。

講師亦說明未來如何尋者合適的解決方案：

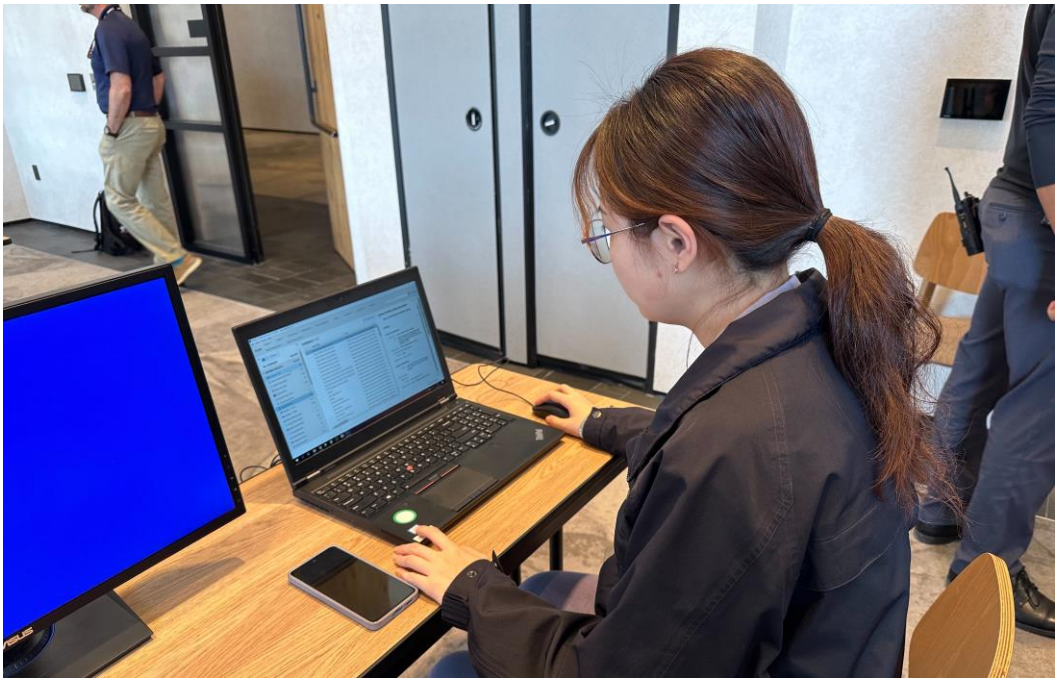
(一)因科技日新月異，更新變化的速度太快，數位鑑識人員唯有不斷的學習，跟上變化，成為數位鑑識專家，才能使自身具有可信度，亦才能使數位證據能具有證據能力。

(二)透過多方的嘗試、交流，科技與執法做結合，才能強強聯手，不斷精進。

四、 神探 Gadget：網路安全、事件回應和法律

此次研討會 Magnet 也有舉辦幾場實作的課程，打造實驗室的環境，僅提供執法單位人員學習，會由講師提供案例，教執法單位的人員去操作、使用他們公司的軟體。此次實驗課程係由 Magnet Forensics Inc.講師 Kim Bradley 及 COBWEBS Technologies 公司的 John Michael O’ Hare 講師上課，透過實作來更深入的了解該公司的軟體可以如何運作，幫助執法人員能將軟體之使用成效提升。

圖片說明：實驗室課程照片



圖片說明：巡官林映榕於實驗室課程實作照片

陸、與當地執法機關、協助執法機關的非營利技術組織交流

我們有幸參訪納許維爾警局(Metropolitan Nashville Police Department)數位鑑識實驗室，與其交流數位鑑識技術、流程、經驗與方法，了解當地警察組織編制與執法狀況，透過我國與美國警察的技術交流，有利於使我國數位鑑識實驗室的水準與技術與國際接軌，可能有機會建立未來良好的合作與聯繫。

另外亦有參訪協助執法機關的非營利技術組織(Operation Lightshine)，了解他們非營利組織的運作方式，他們也有數位鑑識的人才，盡全力協助警方及民眾尋找失蹤兒童，解救許多家庭回歸原本的生活。

圖片說明：股長洪振耀與美國納許維爾警察局數位鑑識警官合影

圖片說明：刑事局、調查局、高檢署參訪人員與美國納許維爾警察局合影

圖片說明：刑事局、調查局、高檢署參訪人員與 Operation Lightshine 組織人員合影

柒、心得與建議事項

一、 心得：

(一) 獲得最新數位鑑識相關資訊分享：

本屆 DFRWS APAC 2022 數位鑑識會議期間除議題發表、技術經驗交流與分享外，並與各國執法機關、學術單位的專家學者交流討論，會議成果豐碩，有助增進本局數位鑑識技術更新與人才培育。

(二) 增廣見聞、拓展國際視野：

透過本次參加 DFRWS APAC 2022 數位鑑識會議與澳洲警局之參訪，開拓我的國際視野並實際瞭解世界各國的執法機關對於電腦犯罪偵查、數位鑑識執法之實際運作，收穫良多，期許能夠將所吸收的經驗帶回我國運用。

二、 建議事項：

數位鑑識專業分工與人才養成：

數位鑑識人才養成不易，經過本次參加 DFRWS APAC 2022 數位鑑識研究會議，可以發現在這個領域的從業人員或研究人員都具有相當豐富的

資歷與經驗，我國應更加重視數位鑑識的人才培育與養成。

捌、結語

近年隨著資通訊設備普及與發達趨勢，科技犯罪持續興盛，數位鑑識技術與數位證物的取證與分析顯得更加重要。本次代表本局參加 DFRWS APAC 2022 數位鑑識研究會議，獲益良多，各個議程均提供許多詳盡、最新的數位鑑識相關訊息，且在與國際數位鑑識領域人士討論過程中，也能大方交流數位鑑識技術與過往經驗。

本次數位鑑識研究會議中的工具與技術之知識，我國警察機關可運用於未來數位跡證蒐集與分析技術之實務運用，期望未來能推廣相關數位取證技巧至各警察機關科技偵查人員，強化科技犯罪偵防能量，有效提升我國執法效率與效能。