出國報告（出國類別：研究）

赴美參加 DFRWS 2019 USA 研討會之數位鑑識課程出國報告

服務機關：內政部警政署刑事警察局

職稱姓名：警務正黃翰文、林芳如

派赴國家：美國・舊金山、波特蘭

出國期間：108 年 7 月 10 日至 7 月 20 日

報告日期：108 年 10 月 15 日

摘要：

筆者係參加 2019 年於美國波特蘭(Portland)舉辦為期 4 天的數位鑑識研究會議 DFRWS(Digital Forensic Research Workshop)，時間為 7 月 14 日至 7 月 17 日，並於會前拜訪舊金山地區科技偵查實驗室、英特爾博物館及網路巨擘 Google 總部，除了解有關數位鑑識的新知外，並與他國從事數位鑑識的人員交流有關數位鑑識的經驗，包含人員訓練、討論數位鑑識軟硬體的使用及數位鑑識流程等議題。DFRWS USA 2019 的研究討論及議題發表主題主要包含 Chip-off 技術、IoT 物聯網裝置、記憶體鑑識、檔案系統的數位鑑識、資訊裝置的存取及可存取性、資訊裝置的 artifact 及基於 artifact 的數位鑑識、數位鑑識的搜尋(Search)等議題；議程的第三天晚上舉辦的數位鑑識解題競賽，需要使用的知識包括 nmap 的網路掃描、資料隱碼、檔案系統 Signature 的認識及密碼學等，並由與會人員自行組成參賽小組進行參賽，藉由參與競賽讓筆者在時間壓力下進行解題，極具挑戰性。

本次的交流使筆者了解到隨著資訊科技進步，數位鑑識目前仍存有許多待研究的議題，現有的數位鑑識技術亦存在瓶頸亟需突破，尤其應用於保護個人資料的技術(如加密等)將大為提升數位鑑識的困難度。這是一個仍在進步的領域，目前各國仍致力於探討有效且有效率地從數位鑑識中發現相關的數位證據，研發數位鑑識工具以輔助蒐集分析等。筆者認為國內的警察機關亦需跟上當前國際向前行的步伐，提升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，由於案件發生後，掌握時間快速採證到關鍵證據至為重要，本局應持續投注人力及心力於數位鑑識技術的研究，並充實數位鑑識軟硬體設備；尤其數位鑑識需具備經驗及大量的背景知識，專業人員的培養誠屬不易，需有長期且

完善的教育訓練及人員培育制度，始能建立專業的警政數位鑑識團隊。

目錄

壹、前言

一、會議介紹

數位鑑識研究會議 DFRWS(Digital Forensic Research Workshop)由一群非營利的志願者共同投入數位鑑識的研究，以處理數位鑑識的挑戰。自 2001 年於美國首度舉辦後，迄今已舉辦 18 年，每年舉辦 2 場次，分別於美洲及歐洲舉行，2020 年將首度增加亞太場次於澳洲舉行，主要邀請研究學者、廠商、學術界及執法人員共同與會。DFRWS 的願景為強化運用跨領域(transdisciplinary)的方式以處理新興的數位鑑識挑戰，並鼓勵創新的研究議題及提出可運用於解決實務問題的方法，該方法需經過科學系統化過程並可信賴。DFRWS 的任務包括經營數位鑑識的討論社群，成員涵蓋實務及學術界人員，對於數位鑑識議題進行學術性的討論，以期望能激勵出新一代創新的數位鑑識知識或技術。

DFRWS 的每日的議程主要分為 Presentation 及研究論文的發表，Presentation 邀集數位鑑識領域的各國研究人員或相關廠商發表數位鑑識的研究成果，研究論文的發表係接受學生的投稿並遴選優越的文章。此外，會議亦有工作坊（workshop）的實機操作課程、海報展示(POSTERS and Demos)及數位鑑識搶旗賽(Forensics Rodeo)，議程內容豐富。目前許多新興的數位研究技術都是首先於 DFRWS 會議被提出，因此本會議所提出的相關議題，可視為數位鑑識領域的新方向，也是對未來數位鑑識研究引領的指標。

圖 1 筆者參加 DFRWS 2019 USA

二、出席目的

刑事警察局數位鑑識實驗室自 95 年成立以來，職司全國各警察機關、地方檢察署及各級法院送鑑之數位證物，辦理數位鑑識的證物數量逐年增加，近年來除積極擴增軟硬體數位鑑識設備外，亦加強人員培訓；為期能與國際接軌，了解國際間數位鑑識的趨勢及技術，有鑑於 DFRWS 為數位鑑識領域重要的會議之一，故由筆者赴美參加 DFRWS 2019 USA 會議；會前並參訪舊金山地區科技偵查實驗室，與數位鑑識人員進行實務的交流，另參訪英特爾博物館及網路巨擘 Google 總部，了解晶片技術及 Android 系統的發展。

貳、活動過程

一、參訪舊金山地區科技偵查實驗室

本次洽請外交部協助，由我國舊金山代表處移民署陳組長協助聯繫，安排 7 月 13 日前往位於舊金山地區的科技偵查實驗室參觀，該實驗室於全美共有 16 座，協助美國各地數

位鑑識案件。

如同本局數位鑑識實驗室，該實驗室已取得 ISO/IEC 17025 認證，當日由實驗室人員進行簡報及實驗室導覽。該實驗室成員由聯邦、州警以及地區警察所組成，並不限定加入前需有資訊科技相關的從業背景或學位，但需具備對於投入數位鑑識工作的熱情。加入實驗室後，需先簽訂合約，於訓練期滿後需服務 6 年以上。並且將接受非常紮時的教育訓練課程，訓練時數長達 500 小時，包括基礎的檔案系統(FileSystem Basic)、微軟作業系統權限機制(Windows Authorications)及模擬法庭(Moot Court)等，並設有專門的訓練教室，有監視系統、CCTV 等實際教材，讓人員可以操作學習；授課師資包括實驗室人員及民間訓練課程如 SANS 課程等。此外安排有 1 至 2 年的實務工作訓練，訓練合格後，始能成為具備進行數位鑑識作業能力人員並開始進行數位鑑識作業。

經人員導覽該實驗室空間規劃主要分為收案室、證物室、副本室、線材室、數位鑑識人員工作區、J-Tag 區及 Kiosk 區，空間占地寬廣，平均一個數位鑑識人員的作業區目視約有 5 坪，並配有多臺工作站及手機訊號屏蔽箱，以供進行手機數位鑑識時遮蔽訊號使用。

較為特別的是線材室及 Kiosk 區，線材室係收集各種數位設備的線材，以避免在收到較為舊式的設備時，遇到欠缺線材無法操作的窘境，線材以整理箱收納，並在外箱標示內容物，一目了然。Kiosk 區域設置一台自助式採證工作機（Kiosk）及手機採證電腦(使用 Cellebrite 手機採證軟體)，目前實驗室負責較需要數位鑑識技術分析的困難數位鑑識案件，一般的手機數位採證或多媒體採證需求的案件，會引導送鑑的偵查人員使用 Kiosk 區的鑑識設備自行操作，並可將

數位鑑識成果燒錄成光碟或使用外接式讀取硬碟攜回，Kiosk區並錄製有教學操作影片，送鑑人員可觀看影片後學習操作，如遇有操作困難，再由實驗室人員從旁提供協助；此可做為我國之借鏡參考。

由於目前多數刑案需求為手機通訊錄及通訊軟體對話紀錄等一般的採證，或需要找電腦裡兒少色情的圖片等，然送到本局數位鑑識實驗室後，由於人員有限且實驗室案件處理量較為龐大，需等待一段時間始能取得數位鑑識結果，若本局能學習，設置類似工作站由送鑑人員自行操作，將可減少偵查人員等待鑑識結果的時間，並可立刻進行後續的偵辦；本局數位鑑識實驗室亦可關注於較為困難或需技術研究的案件，才能有效提升實驗室的數位鑑識能量。

實驗室人員非常熱烈地分享經驗，該實驗室具有 J-Tag 平台，在取得送鑑人員的授權後才進行 J-Tag，其成功率可達 9 成，其經驗值得我方學習。另討論到數位鑑識人才短缺的問題，該實驗室表示解決之道建議可持續招募有意願的人員，並讓相關人員接受足夠的教育訓練，專心在處理數位鑑識案件。由於科技進步十分快速，該實驗室亦持續在研究數位鑑識的技術並為未來做準備，包括無人機等未來可能用於犯罪的工具，該實驗室雖未接獲相關案件但都已在研究相關的鑑識採證，已做好準備等待應用，亦為本局應引以為鑑之處。

該實驗室配備的工作站及數位鑑識軟硬體種類齊全，亦為實驗室最基礎的需求，內部嚴格禁止參訪人員攜入任何電子設備，包含筆者的手機、電腦，其控管非常嚴格。同樣臺灣身為科技大國，數位鑑識技術亦應能跟上國際的腳步，尤其科技及犯罪並無國界，愈早做好萬全的準備，才有足夠的能力因應各種可能發生的情況。

圖 2 實驗室所在的大樓

二、參訪英特爾博物館及網路巨擘 Google 總部

筆者至 Intel 博物館參訪，Intel 博物館位於聖荷西中，裡面有介紹 intel 晶片的製程以及未來發展方向與趨勢。博物館中保留了第 1 代 8086 的晶片，並與現行的 i7 晶片做一個比較，讓人感受到晶片技術的進步神速。晶圓的尺吋越來越大，但是單位面積內所容納的電晶體卻越來越多，平均每 18 個月就可以增加 1 倍（摩爾定律）。現場備有電子顯微鏡，讓我們可以了解到現代晶片內部的製程是多麼微小，目前我國台灣積體電路開發的最新製程是 7 奈米，並預計於 2022 年投入 3 奈米製程，電晶體數量將再一次依摩爾定律而實現。

參訪網路巨擘 Google 總部，Google 並成立開放手機聯盟(Open Handset Alliance，OHA)，持續領導與開發現今的 Android 系統。目前許多行動裝置採用 Android 系統，從 2008 年發行第一版 1.0 至 2019 年 9 月已更新至 Android 10，先前的版本都以甜點作為開發代號，自第 10 版起不再以甜點作為代號，直接命名為 Android Q。總部不時可見 Android 各版本的代號甜點的裝置藝術，科技大廠洋溢俏皮的氛圍；漫步

在總部，也見識傳聞中 Google 對於員工工作環境的重視，佔地廣大的總部園區設有排球及網球等相關設施，有幸能來 Google 總部參觀，對於常使用 Google 功能的筆者來說，十分有意義。

圖 3 警務正黃翰文在 Intel 博物館前的留影

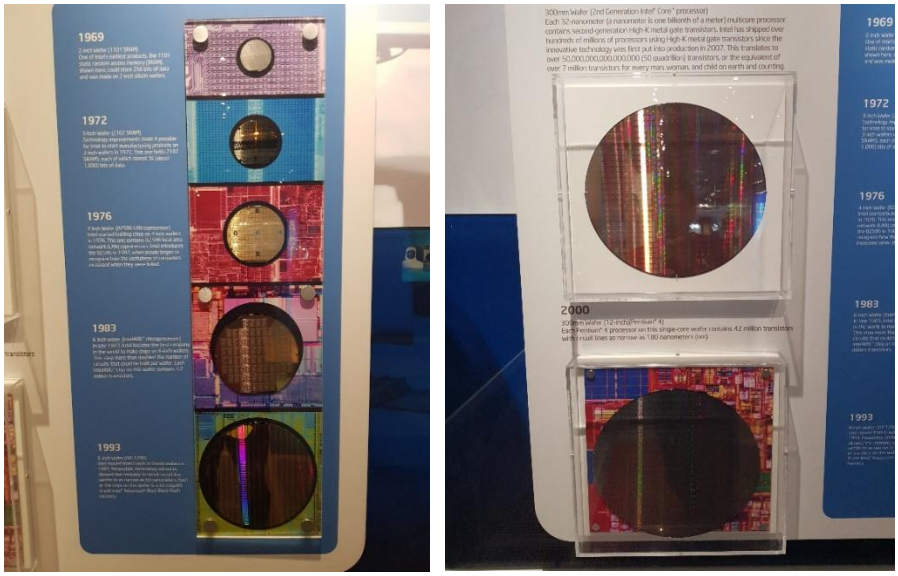

圖 4 Intel 博物館解釋晶片的演進及製作技術

圖 5 警務正林芳如在 Google 總部前的留影

三、DFRWS USA 2019 會議

（一）第一天：工作坊（Workshop）：

7 月 14 日進行進行第一天的議程，主要為 2 個講廳分別同時進行 2 場的工作坊，議程包括 Chip-off 技術、鑑識工具 KAPE 介紹及分析，說明如下：

1.Chip-off 技術：

對比於一般的熱風槍解焊方式，講者展示了他們自行開發的解焊機器，採用彈力夾的方式，先將夾子與要拆取的晶片黏住如圖 6，再放入他們自行設計開發的「烤箱」進行加溫等到加熱的溫度與時間到達設定值之後，晶片上的焊錫就會融化，並且因為原有彈簧的關係，晶片就會被連根拔起。

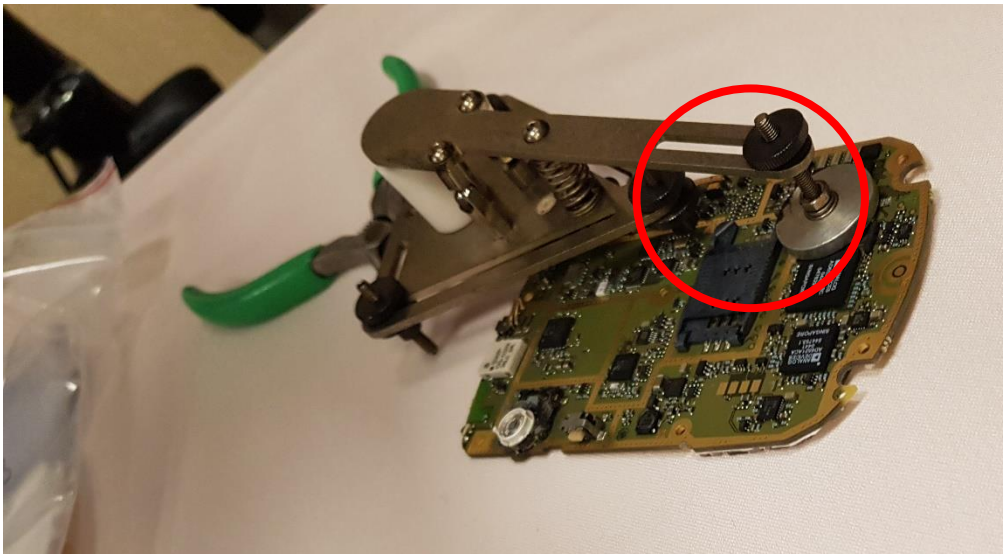

圖 6 先以彈力夾子夾住機板，並黏貼欲取出的晶片

圖 7 置於加溫箱中加溫

當然講者宣稱，這是一項完美的 chip-off 工具，但對照本局現有的 chip-off 工具就可以知道，其實晶片於拆取的時候，最理想的狀態應該要依機板、焊接方式、晶片腳位等等不同的特性，設定不同的加溫時間以及曲線，而這項工具則顯著地無法達成這一點。另外在以物理彈簧的方式拔取晶片，

則會因為有角度的關係，容易造成晶片的接腳彎曲，這些對於晶片可能都會造成損傷，故這一項技術其實並非如其宣稱的那麼完美，仍有許多改進的空間。

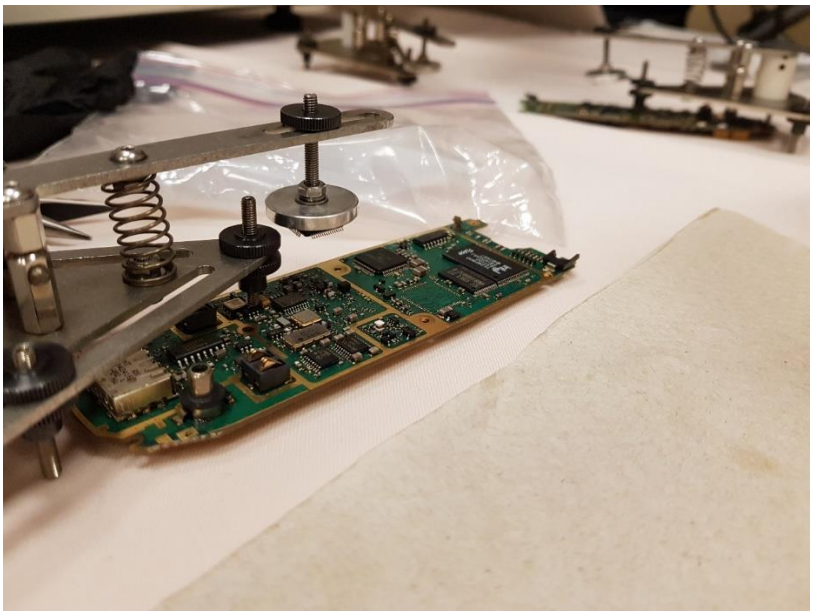

圖 8 使用該工具成功取下晶片

2.KAPE 工具：

KAPE 是 Kroll Artifact Parser and Extractor 的縮寫，由知名的數位鑑識專家 Eric Zimmerman 所提出。KAPE 是一個全方位的免費數位鑑識及 DFIR 的 triage 工具，有 GUI 介面版本，目前仍在增加內建的處理模組(Module)，使用者可自行定義要蒐集的檔案，數位鑑識資料可快速被蒐集並進行分析(parse)，主要目標(tkape)及模組(mkape)兩項目進行。

（二）第二天：與記憶體分析相關的學術論文分享及資訊裝置的存取及可存取性。

1.議題發表

（1）介紹對於極度被破壞的硬碟裝置要如何修復並能夠成功進行數位鑑識，由講者示範其所屬實驗室處理的案例向與會者說明即便硬碟極度被損壞，仍有修復的可

能性。

（2）Cyber Sleuth Science Lab (CSSL)利用虛擬的數位學習環境進行數位鑑識的教學，提出全新的數位鑑識學習方式。

2.投稿論文-Windows memory forensics：Detecting(Un) Intentionally Hidden Injected Code by Examining Page Table Entries

本篇文章的主題是針對記憶體的數位鑑識，主要是設計了一個流程，來判定記憶體內是不是有被載入惡意的程序，比如偵測一些正常的記憶體位址是不是有合於相關入侵行為（如修改 tdl）。另外講者也提到可以將正常的記憶體 page 做出一個資料庫，並且將欲偵測惡意程序的記憶體 page 與正常 page 做一個比對，其他比如以權限來比對，原本只應該有 rw（讀取、寫入）權限的程序，出現了 rwx（讀取、寫入、執行）的狀況，則可能就是被植入惡意程序。

講者並於最後有在 github 提供該程式：https://github.com/f-block/DFRWS-USA-2019

3.投稿論文：Virtual Space in Memory Space in Real Space - Memory Forensics of Immersive Virtual Reality with the HTC Vive

這篇研究主要的目的是，如何從使用過 HTC Vive 虛擬實境系統中，擷取資料，並重建所使用的場所，首先講者提到，HTC Vive 虛擬實境系統的鑑識分為兩個部分，首先是先將數據擷取出來後，透過逆向工程的方式還原出原始的數據。也因為 HTC Vive 所使用的 OpenVR 軟體，並不是一個 OPEN SOURCE 的軟體，再加上 HTC Vive 的更新速度很快，所以如何有效而且避免錯誤地去擷取且解析 HTC Vive 中記憶體的資料，是很重要的課題，也因此講者提供了一個叫做 YARA

的程式，可以有效地去解析數據而解析之後，便是將該數據還原重建出虛擬實境的位置與狀況，如圖 9 便是講者還原出來的 HTC Vive 的虛擬實境的資料。

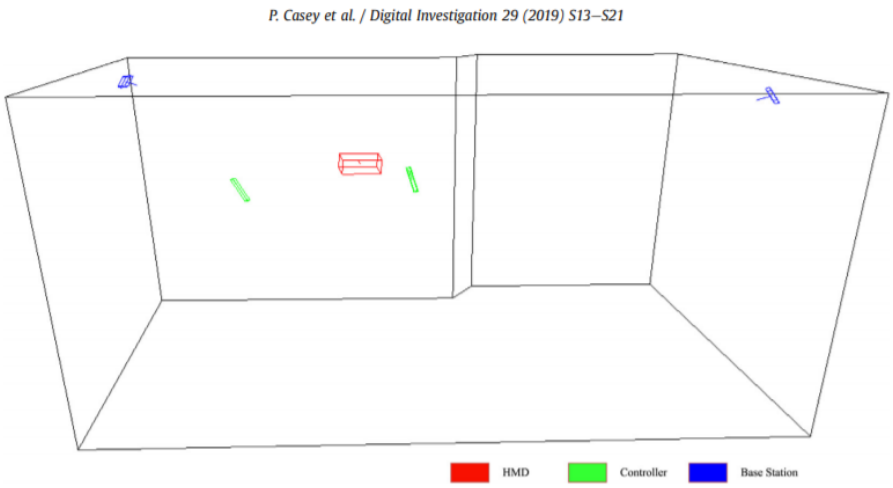

Fig. 3. Sample output of the visualization provided by Vivedump.

圖 9 作者還原 HTC Vive 內虛擬實境環境

4.投稿論文：Syntactical Carving of PNGs and Automated Generation of Reproducible Datasets

文件回復是一種無需依賴文件系統或文件系統即可從儲存介質恢復文件的技術，也因為文件的儲存是屬於連續的狀態，因此一般的文件是很容易被回復的。但是一但文件被碎片化分割，即使分割情況相對簡單且大多數情況下，回復過程也變得非常複雜。講者應用文件格式的語法來最大程度地轉換為 PNG 文件格式，並且能夠完全正確地還原 98%的測試文件，其餘則達到至少部分還原。PNG 檔案是由 chunk 所組成的，而 chunk 包含 IHDR、IDAT 以及 IEND 等元素如圖 10。第一個是 IHDR、chunk 然後是 IDAT，再來 chunk，最後以 IEND 做為結尾。

圖 10 作者指出 PNG 檔中，chunk 的組成

因此，我們只要先找到 IHDR，再來找 IDAT，最後再找出 IEND，則中間的就是 PNG 檔案。但如果找到 IDAT 的話，就可以用 length 欄位來找出下一個 IDAT 在哪邊，因此在沒有分割的 PNG 檔案的狀態下，可以用 IHDR、IDAT 以及 IEND 等字串，來找出 PNG 檔案的位置。而在分割的狀態下，中間會有一些資料存在，如何去辨識出 IDAT 是從哪邊開始的呢？事實上在 IDAT 中，有一個 last chunk length，經由使用 mod block size 計算，可以算出中間的 block 的大小，以及有一個 intra block offset 來描述下一個 PNG 分割檔案所在的位置。

最後該文作者比較了自己的方式與其他 foremost 等三種方式，他的成功率較高達 98%。

5.投稿論文：bring2lite: a structural Concept and Tool for Forensic Data Analysis and Recovery of Deleted SQLite Records

目前來說如 WhatsApp 或 Skype 之類的移動應用程序已使用 SQLite 資料庫格式來存儲其數據。因此從數位鑑識的角度出發，必須提取所有與之相關的信息到 SQLite 資料庫。在本文中，作者建議使用一種結構化的方法來分析在不同的數據庫進行刪除行為，參數的不同。根據相關的分析結果，開發概念來進行解析和處理。在實驗中，講者設計了五個情境

情境 1：插入 1 筆紀錄，並刪除之。

情境 2：插入 3 筆紀錄，並刪除 1 筆紀錄。

情境 3：插入 3 筆紀錄，並全數刪除之。

情境 4：插入多筆紀錄直到產生新的頁面，並刪除第 2 頁的紀錄。

情境 5：插入多筆紀錄直到產生新的頁面，並刪除第 1 頁的紀錄。

情境 6：插入多筆紀錄直到產生新的頁面，並刪除全部的紀錄。

根據作者實驗的結果，在不同的 SQLite 資料庫設定之下可以得到不同的結果，「+」表示所有的紀錄都被完整的擷取出來、「0」表示有一些紀錄可以還原及「-」表示沒有辦法追蹤還原紀錄如圖 11。

Table 1
Sample pragma combinations under which it is possible to restore deleted records.

Scenarios	secure_delete = 0/ auto_vacuum = 0/ journal_mode = OFF	secure_delete = FAST/ auto_vacuum = 0/ journal_mode = OFF	secure_delete = 1/ auto_vacuum = 0/ journal_mode = WAL	secure_delete = 1/ auto_vacuum = 0/ journal_mode = PERSIST
S1	+	−	+	+
S2	+	−	+	+
S3	+	−	+	+
S4	+	−	+	+
S5	+	0	+	+
S6	+	0	+	+

圖 11 作者於所設定 6 種情境下，分析資料庫刪除還原的情形

因此，經由本研究，我們可以知道哪些資料庫的設定是可以去還原遭刪除的資料，並由作者提供了「bring2lite」這一個 parser 程式去還原，該程式連結如下：https://github.com/bring2lite/bring2lite。

6.投稿論文：DB3F & DF-Toolkit: The Database Forensic File Format and the Database Forensic Toolkit

大多數敏感和個人用戶數據存儲在不同的數據庫管理系統中（DBMS）。例如，Oracle 通常用於存儲公司數據，MySQL 則通常作為後端大多數網絡商店的存儲空間，SQLite 將個人數據（例如 SMS 消息、APP 通話紀錄）存儲在電話

中。也因此資料庫的取證工具是相當重要的，在本文中作者提出了一種標準存儲格式，即資料庫取證文件格式(DB3F)，用於資料庫取證工具輸出遵循其他（文件系統）取證所建立的準則工具，以及資料庫取證工具包（DF-Toolkit)，可用於分析。

在簡報中作者提到，相較於傳統的作法，在 DBCarver 之後，使用者直接去分析相關數據比起來，他們的 DB3F 以及 DF-Toolkit，可用於資料庫還原後的協助進行資料解析，並且將所解析的資料採用圖形化的介面來輸出。雖然理論上作者聲稱他們提供了圖形化的操作介面可以讓使用者更容易使用以及分析資料，但是就現場看起來，他們的介面相當陽春，而且與本局現在正在使用的 Cellebrite UFED Analytic Desktop 等相似的產品，似乎並沒有辦法有很顯著的進步以及分析功能。

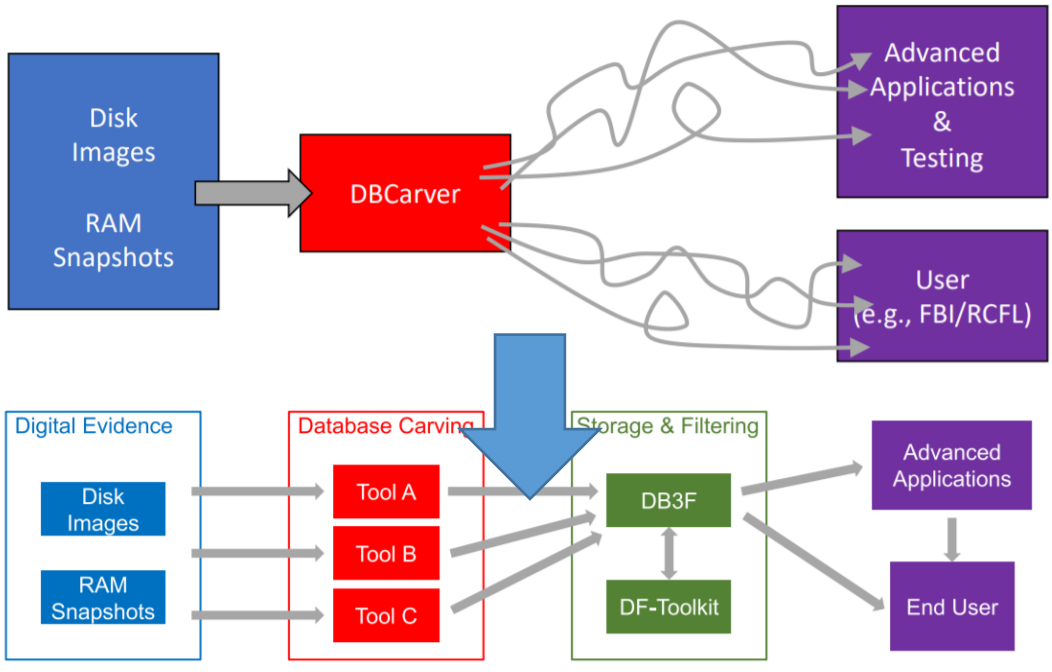

Fig. 1. The role of DB3F and DF-Toolkit in database forensics.

圖 12 作者於論文中使用 DB3F 以及 DF-Toolkit 協助使用者分析

7.投稿論文：Using NTFS Cluster Allocation Behavior to Find the Location of User Data

隨著電腦硬體技術的進步，需處理資料正在大量不斷增加，數位鑑識工作也因此受到強烈的影響，因此如何有效地過濾我們不感興趣的文件來減少需要處理的工作量，是蠻重要的課題。作者在本篇研究中，以集群分配算法（cluster allocation algorithm）在 NTFS 檔案系統中，查看新存入的資料實際在磁盤上的位置。作者實驗了在 32 個新安裝的 Windows 7、8、8.1 或是 10 中隨機寫入，增加，減少和刪除文件，結果顯示，儲存的資料經常分配到更靠近磁碟中間的特定的位置。也因此，在對 NTFS 格式的硬碟進行數位鑑識的時候，該可更加針對該區域來進行取證，將可以獲得比傳統更好的效果。作者採用了 64GiB（GiB：1024 進制，GB：10 進制，稍有不同，但可約略看為 64GB）的硬碟，作者將整個硬碟的磁區位置分成了 64 個族群，並且統計出，不論是使用 Win7、8、8.1 或是 10，資料的存取位置其實都約略會在特定的區塊，因此我們未來在做鑑識的時候，可以更加針對這些特定的區塊去嘗試資料採證，可有效增加數位鑑識的效率。

對我們執法人員來說，數位鑑識並不能以機率統計的概念來採證，不論作業系統將檔案存放於何處位置，我們的責任便是將該檔案找出來，本篇文章作者的方法或許可以增加部分數位鑑識工作的效率，亦可以讓數位鑑識工具在設計時候的參考。

（三）第三天：與物聯網相關的學術論文分享及對於電腦的 artifact 研究及數位鑑識技術研究。

1.議題發表：

（1）APFS 的檔案特色及數位鑑識方法：由在該領域知名的研究人員 Jonathan Levin 擔任 Keynote Speaker，並提及到 Apple 推出的 T2 Security Chip 所帶來的影響，由解析 APFS 的檔案系統結構，並釋出相關的研究資源於 http://NewOSXBook.com/QiLin。

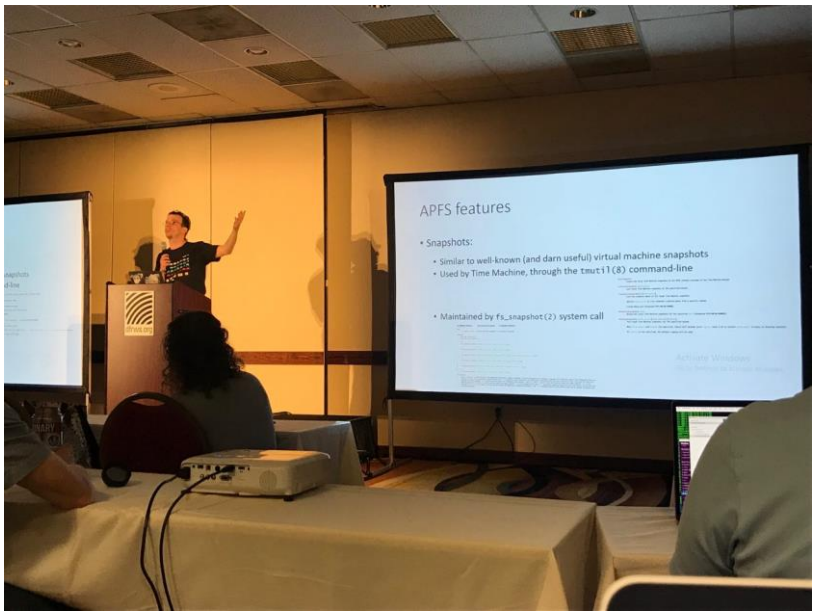

圖 13 講解 APFS 系統的特色

（2）Android Auto 及 Google 助手：講解 Android Auto 的運作模式，以了解該如何對其做數位鑑識，並說明 Android Auto 是如何和 Google 助手互動；了解 Google 助手會產生的 artifact，包含使用者的音檔、時間戳及使用 Android Auto 產生的使用位置、最後執行時間及裝置資訊等。

（3）Windows 10 version 1803 的時間軸分析，該版作業系統紀錄許多資訊，包含網站的存取、文件的開啟和編輯、應用程式的執行及和許多使用者活動有關的紀錄。

（4）將記憶體分析用於 Triage 分析：講者為現職的波特蘭警察，有豐富的數位鑑識經驗，有鑑於記憶體分析為有效且快速的分析方式，在講者的案例中，可快速的

追蹤使用者使用紀錄、識別外接裝置、建立使用者活動的時間軸及識別曾被存取的檔案等。

（5）數位鑑識軟體執行蒐尋(Search)的比較：本篇主要由 NIST 提出，NIST 為美國國家標準暨技術研究院 National Institute of Standards and Technology 的縮寫，講者介紹 CFTT 計畫，為 NIST 提出用來測試數位鑑識軟體工具的功能，包含映像檔製作、防寫、刪除檔案還原、File Carving、行動裝置及字串蒐尋等；其中字串蒐尋已完成測試的軟體包括 Autopsy 4.6、X-Ways19.6 R4、FTK 7.0.0.163 及 BlackLight 2018R4。經實驗證實，不同的鑑識軟體可能產生不同的數位鑑識結果，故也驗證尚未有一個能夠涵蓋全部數位鑑識能力的數位鑑識軟體。因此，國內警察機關不可只備有單一鑑識軟體，應在經費許可之下，具備多套廣泛被國際間採用的數位鑑識軟體。

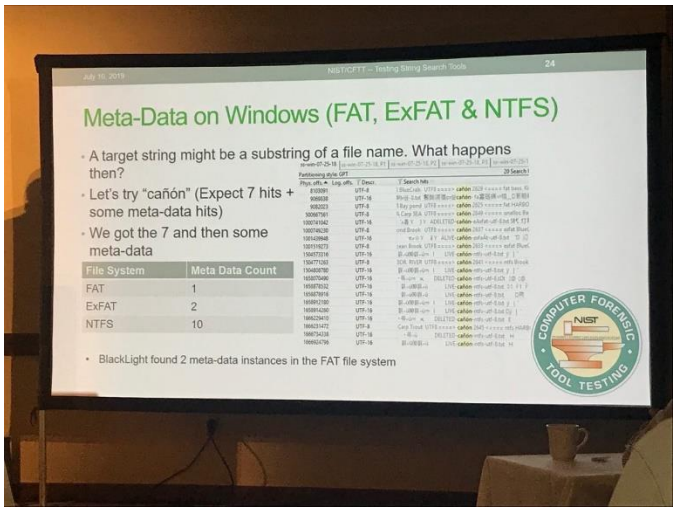

圖 14 講者說明不同檔案系統的關鍵字搜尋結果

2.投稿論文：Forensic analysis of the Nientendo 3DS NAND

講者探討如何對任天堂的 3DS 產品做數位鑑識，以取出和使用者相關的朋友清單及 wifi 連線的密碼，使用

microSD/SD 卡對內建的 NAND 做映像檔(image)是顯著的創新，使得鑑識人員取得 3DS 的 image 後，可對 3DS 進行 live forensic；本篇也是首篇使用駭客工具取得鑑識資料的研究。

任天堂 3DS 在全球銷售量達 7,353 萬銷售量，可見其廣受歡迎的程度，在美國也引起討論對於 3DS 的數位鑑識，包括資料的擷取(extraction)及分析。本篇利用對 NAND 晶片做成的 image 做鑑識，將 image 解密以進行解析。作者提出的工具，可能是目前最有效率的分析，可規避產品為保護著作權而使用的保護措施。作者使用 R4 卡(R4i+3DS/DS)，並將卡片上面的 switch 調整到 N 模式就可以做 NAND 記憶體的 Image 並取得解密的金鑰。準備一張可存放 image 用的 flashcart，該 flashcart 已事先 pre-flash ntrboot 檔案，將原始的 microSD/SD 卡製作 image 後取出，並將新的 micro SD/SD 卡置入卡槽，新的 micro SD/SD 卡有 boot9strap 及 decrypt9WIP 等 2 個工具，該 2 個工具為駭客社群所釋出，，即可進入將 NAND 記憶體做傾印(dump)的步驟。

講者使用 AccessData FTK 7.0 進行數位鑑識，與使用者資料相關多存在 data 資料夾每個 app 料夾都有 2 個基本的檔案，00000001 及 00000002，儲存與系統相關資訊，00000000 則儲存實際的內容，可還原被刪除的錄音檔案及 camera app 儲存的刪除圖片，並可解析連線網路的 SSID 資訊及該 3DS 在網路中的名稱及登入的帳號等；若對 3DS 做格式化，則先前提到的 camera app 存的照片會不見，但可使用 FTK 從 unallocated space 還原。

講者認為他並不贊成因為這些駭客工具可進行數位鑑識分析，就忽略其對產品著作權的侵害，但使用這些工具，的確可以發現重要的資訊；由於本篇所提到的擷取方式均為手動操作，講者希望未來能開發自動化的操作工具。

3.投稿論文：Forensic analysis of water damaged mobile devices

本篇投稿單位為日本警政署(National Police Agency of Japan)，講者為 Aya Fukami 警官。本篇文章探討由於有些送到數位鑑識實驗室的手機已被刻意或因意外而泡水損壞，chip-off 技術因面臨全磁碟加密(full-disk encryption)的挑戰而逐漸無法使用，故對泡水損壞的手機，實驗室必須儘量修復手機後，再使用數位鑑識軟體進行解析。本篇文章主要探討利用電化的角度，觀察泡水手機隨時間的變化，若操作得宜，可能可在實驗室找出使泡水手機回復到可進行鑑識的狀態。

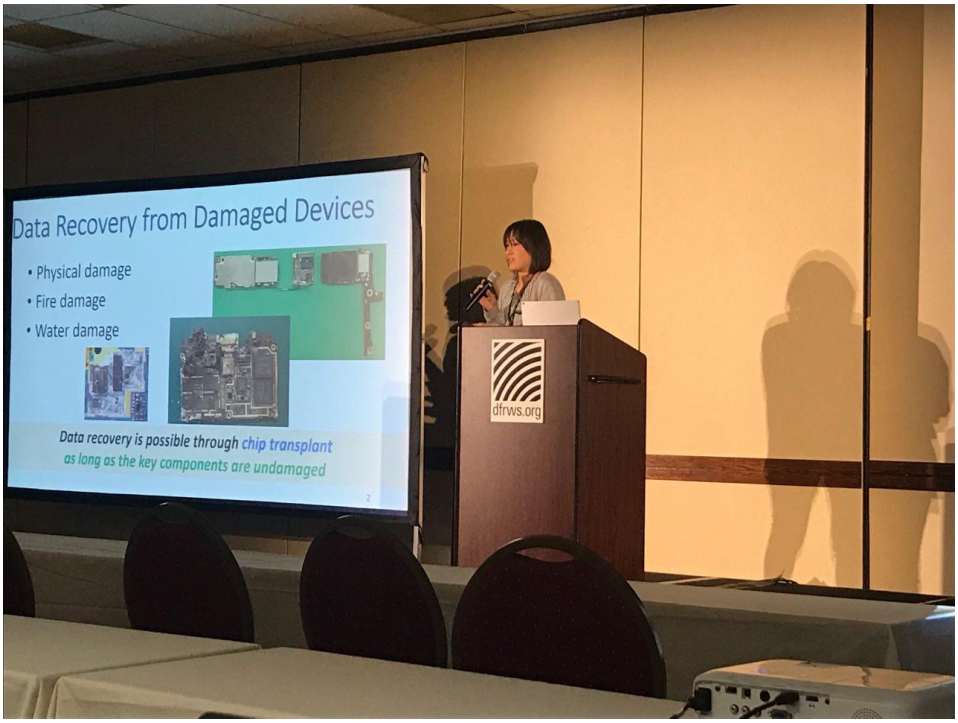

圖 15 Aya Fukami 警官講解實驗結果

手機的資料對於犯罪偵查日益重要，但嫌犯可能故意將手機浸水破壞手機，導致手機損壞後無法進行數位鑑識。過去提出各種方法處理泡水的手機，最常被使用的是拆解手機並把電路板清潔及用乾，若處理後仍無法開機，則會進一步做 chip-off 或 chip transplantation。在高濕度的環境下，金屬腐蝕(metal corrosion)是常發生的情形，其中浸泡在液體中是

最極端的例子，尤其手機愈做愈小但又提升效能，內部零組件排列緊密，金屬腐蝕會更嚴重。該署探討手機內部泡到水裡後的金屬腐蝕情形。

為了研究泡水對手機的損壞，實驗室 2 個不同廠牌的手機泡在水龍頭流出來的水，手機廠牌分別為 Samsung Galaxy S6 Edge(SM-G925，以下簡稱 SM)及 LG Nexus 5X(H790，以下簡稱 LG)，分別泡在深度 20 公分的水面下達 72 小時(72 小時為該實驗室統計平均浸泡時間達 72 小時會對手機造成損壞)。共分兩組進行(實驗組為 SM-1、LG-1 及對照組 SM-2、LG-2)，一組浸泡時手機為關機，對照組浸泡時開機且螢幕為顯示的狀態，水的氯濃度為 0.4mg/L，溫度為室溫，浸泡結束後，將手機拆解並乾燥至相對濕度為 0%，再用顯微鏡及電腦斷層 X-ray 系統(micro-focus X-ray system)檢查，另手機的 PCB 版的元件汙染情形，則再用 X 射線光譜(X-ray spectrometry, EDX)檢查。

經實驗後發現，LG-1 手機可成功被開機；SM-1、SM-2 及 LG-2 手機損壞後，對該 3 款手機做修復；先使用熱槍移除 3 款手機的 PMIC 晶片，發現 SM-1 手機的一個 PMIC 晶片發生內層短路(internal short circuit)，故置換同一型號手機的同款 PMIC 晶片後，重新焊回 PCB 板上，可成功開機；SM-2 在重新植球後，可成功開機；LG-2 手機的 PCB 板在 chip-off 後，發現 PCB 板上的接腳亦被腐蝕，因開路電壓(open circuit)導致螢幕顯示功能無法被正常供電，且導電金屬遺失，即使重新植球也無法正常使用；因此，實驗室研究 PCB 板的電路寫法並使用銅線重新產生 PCB 板和顯示螢幕的導電路徑，並成功使 LG-2 重新開機。

經實驗顯示，泡水對 LG 手機的影響小於 Samsung 手機，SM 手機比較會因泡水發生焊料的異常，但 LG 手機較不易

發生。LG 和 Samsung 手機兩者最大的差異在於 LG 手機在 PCB 板和晶片之間及焊球都有使用底部填充劑(underfill)，所以可以避免水氣帶來的損壞。泡水手機在未用乾前接電，對手機的損壞遠大於泡水的因素；在相同的條件下，開機狀態下泡水的損壞，比關機狀態下泡水損壞嚴重。此外，泡水手機送到實驗室的運輸期間，手機內的水氣也持續對 PCB 板造成金屬腐蝕，可能導致持續更大的損壞。另將 SM-1 的 PCB 泡在海水中 14 天，可能導致 PCB 的電子零件都脫落，大大降低可修復的機率。

此外，為了要研究泡水多久才會導致開路電壓(open circuit)，使用有 0.4mm 接腳的手機連接簡單的螢幕進行模擬。理論上要達到 15V 電壓螢幕才會亮起來，但泡水手機在 15V 的通電，螢幕就會亮，同時並產生大量的氣泡並產生黑色的汙染物，1466 秒(24.43 分)後，螢幕就關掉了；泡水時會加速金屬腐蝕速度，並導致螢幕加速被關掉。故收到泡水手機時，金屬腐蝕程度及電子零件是否遺失為檢視重點，重新建立 PCB 迴路仍比 chip-off 容易，因此，收到手機後，先評估螢幕顯示的狀況應為處理的第一步驟。若 IC 晶片發生內層微短路的損壞(CAF)的損壞，則幾乎不可能被修復，需要進一步 chip-off 或 chip-transplantation。

實驗室歸納出當手機泡水後，移除電池或電力的供應是第一時間處理的首要步驟，以免泡水愈久導致更嚴重的金屬腐蝕；在實驗室處理時，要移除汙染物，以便免造成短路，另查看 PCB 板的零組件，以檢查是否有缺陷或造成開路電壓，若以遺失重要電子零組件或遺失 PCB 板上多處的導電金屬，則只能進行 chip-off 或 transplantation。了解泡水對手機的損壞有助於第一線人員正確處理應變，提升成功擷取泡水手機資料的可能性。

4. 投稿論文：Digital Forensic Practices and Methodologies for AI Speaker Ecosystems

本篇文章為南韓檢察署與南韓亞洲大學共同研究提出，主要研究智能音箱(AI Speaker Ecosystems)，屬基於雲端系統的 IoT 研究。本文主要提出對於南韓販售的智能音箱的 5 個鑑識方法，並研發一鑑識工具可蒐集使用者於 NAVER Clova 的指令紀錄。

智能音箱和其他 IoT 產品最大的不同是使用者(AI Speaker)扮演系統的重要角色，可控制多個 IoT 設備。依據 Gartner 統計，在 2020 年前將達 20%的已開發國家市民會使用智能音箱，所以對智能音箱的數位鑑識也日益重要，在美墨都有智能音箱提供破案證據的案例，如美國 2015 年的一起謀殺案中，智能音箱就扮演重要的破案關鍵，Amazon 也配合本案辦理。本文主要研究智能音箱包含 Clova of NAVER(來自 NAVER 公司)、Kakao I(來自 KAKAO 公司)、NUGU(來自 SMT 公司)及 GiGA Genie of KT(來自 KT)公司。

經研究發現，使用者在智慧音箱及 app 上使用的指令，都會存到雲端，也就是說雲端存有使用者的資料，包含識別的資訊及裝置資訊等，業者是否有做到去識別化，顯得重要；此外，手機和智慧音箱也會儲存使用者的個資如姓名、住址及帳戶資訊，部分個資在使用者於手機登出後，仍會被保留；在智慧音箱上，可以還原出使用者已刪除的音檔，甚至在 Kakao I 的智慧音箱上，發現回應音檔都會被完整保存。研究團隊並開發一數位鑑識工具，取得的資訊分為 Program and Token Information、Voice Command History 及 Export to Excel，包含使用者 ID、裝置名稱、時間戳記、問的問題及回答等，並可做關鍵字搜尋，若 conversation 的檔案提到犯罪的資訊，如 kill 時(已將韓文翻譯為英文)，則會將該筆資訊紅字標示

呈現。要即時存取智慧音箱的資料很困難，因為部分智慧音箱會在每次更新後重新安裝所有的 app，瞭解其所使用的檔案系統結構十分重要；此外，研究發現 NAVER Clova 2.xx 的反編譯複雜性比先前的版本更高，故先對剛推出的版本做反編譯，可能可以得到較多的有用資訊。

未來，將進一步研究如何提出適用於所有智慧音箱的鑑識框架，並克服在 tunneled session 下如何取得金鑰及了解 Android 封包的加密機制，以進行反編譯的程序。

5.海報展示

中午稍做休息後，在會場提供講者擺放經錄取的海報展示，包括會議的論文投稿海報展示及數位鑑識廠商如 Magnet AXIOM 及 Nuix 等廠商均有參展，並提供產品說明，供與會者可了解產品的功能及運用方式。

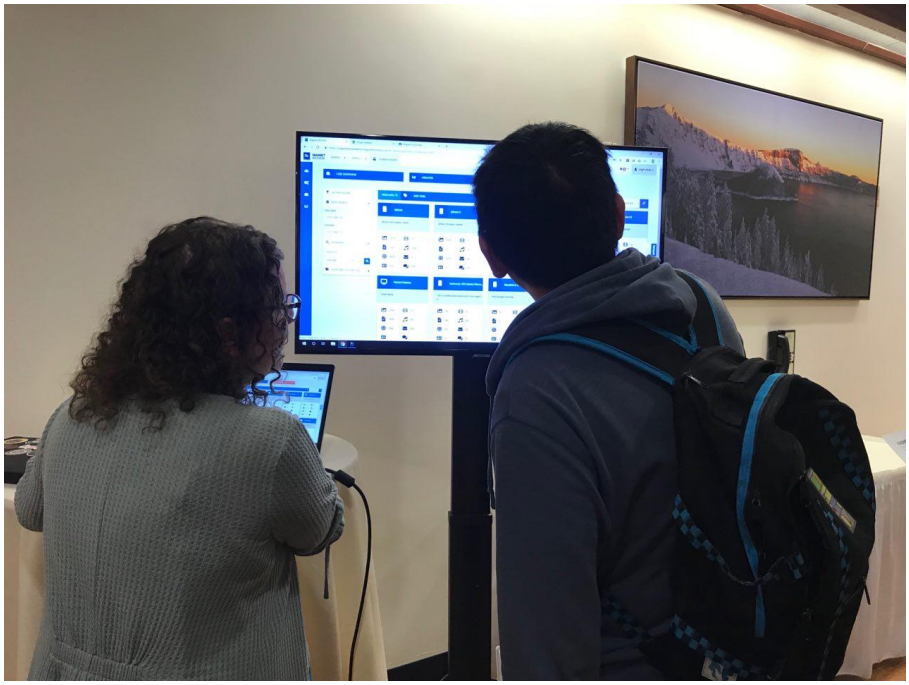

圖 16 和數位鑑識廠商討論數位鑑識產品的應用

6. 數位鑑識搶旗賽（Forensics Rodeo）

晚餐過後稍做休息，於 19 時 30 分開始的數位鑑識搶旗

賽（Forensics Radeo）競賽是活動的另一個高潮，該遊戲係由DFRWS 制定各式不同的與數位鑑識相關的解謎遊戲，以搶旗的方式進行，與會者可自行組隊參加，每隊最多 5 人，本參訪團也組了臺灣代表隊一起共襄盛舉。

圖 17 筆者參加比賽合影

活動在會場的交誼廳舉行，最前方架設一大螢幕，可即時顯示各隊解謎成績現況，過程相當刺激，題目設計亦非常有趣，出題者會將旗標（flag）隱藏在題目的資訊中，但需經由解碼、數位鑑識、封包側錄或是解謎等各種方式獲得。參賽的隊伍拿到答案後，要立刻上傳檔案，越快完成題目得到旗標的隊伍分數越高，反之越低。

活動原預定於 22 時前結束，由於未能有參賽隊伍完成所有答題，最後延至 23 時 30 分結束，並於結束後進行解題，經講解後所需的解題知識包含需要使用的知識包括 nmap 的網路掃描、資料隱碼、檔案系統 Signature 的認識及密碼學等，大會並邀請第一時間答對題目的人員分享解題方式。筆者發現，多數位鑑識人員均係依賴過去的數位鑑識經驗，才能夠在短時間內使用正確的方式解題並搶旗成功，足見經驗對於數位鑑識人員的重要性；此外，鑑識團隊亦為重要的成功關

鍵，藉由團隊成員間的討論及努力，才能在最短的時間搶到最多的分數，藉由討論的過程中，亦可以突破瓶頸或盲點，找到解決問題的關鍵。

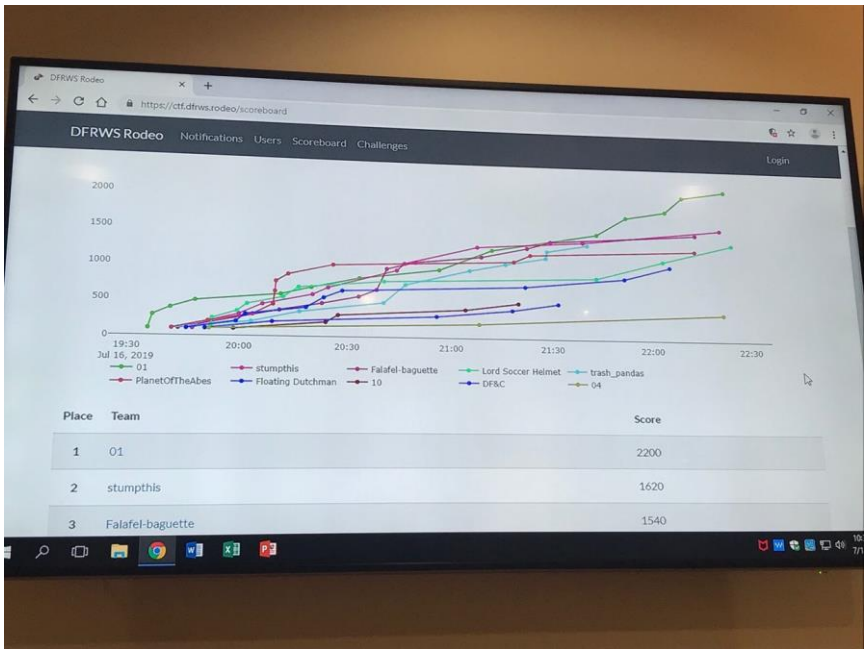

圖 18 隨時公布比賽的成績

筆者深思警察機關在犯罪偵查的過程中，由於第一時間可能有許多需要採證的跡證，其時間壓力遠大於搶旗的時間限制，係有必要由足夠的專業數位鑑識團隊進行採證。本次活動亦充分展現各國人士對於數位鑑識的熱情，在結束一日長達約 8 小時的課程後，大家在夜間仍不覺疲累投入競賽，甚至主動要求大會延長比賽時間，筆者在比賽過程中，亦藉此機會檢視自己數位鑑識的能力，惟許多答題需要的知識可能與美國民眾的生活議題相關，如某一知名美劇的劇情做為題目，使筆者較為困惑，但發現所學的相關知識被實際應用在題目上時，仍十分振奮。本次筆者組成的臺灣代表隊雖然只有 2 名，但仍然成功解出 3 題，獲得第 10 名。

有關搶旗賽可參考的相關題目連結如：https://www.dfrws.rodeo/

圖 19 競賽人員全神貫注投入搶旗競賽

（四）第四天：特殊的數位鑑識研究學術論文分享

1.投稿論文：HookTracer: A System for Automated and Accessible API Hooks Analysis

講者專注於分析 API hooks 的分析，所謂的 API hooks 是屬於修改 API 時，可以使用的工具，我們可以通過 API hook，改變一個 API 的原有功能。基本的方法就是通過 hook「接觸」到需要修改的 API 函數入口點，改變它的地址指向新的自定義的函數。而 API hook 也常常讓惡意軟體利用以劫持合法功能的執行流程。這些掛鉤可讓惡意軟體在關鍵時刻獲得控制權，並對功能進行完全控制，因此作者提出了「hooktracer」，可用於快速調查大量機器是否存在惡意軟體感染的跡象。API hook 在 Windows 系統中的數量越來越多，據統計到了 Windows 10，API hook 的數量有了爆炸性的成長。因此作者提供了一個模擬記憶體鑑識的程式，hooktracer，主要是可以判定 API hook 的來源以及去向，並依此來判斷是

否為惡意程式。

2. 投稿論文：FbHash: A New Similarity Hashing Scheme for Digital Forensics

講者提出一個模糊 hash 值的改善作法，所謂的模糊 hash 值，通常用來比較 2 個文件之間的相似程度，其主要原理如下：

（1）使用的一個弱 hash 值來計算文件的部分內容，並進行分割。

（2）計算文件每一個分割部分的強 hash 值。

（3)將每一個分割部分的強 hash 值轉換為一個更短的值。

（4）計算 2 個檔案模糊 hash 值之相似程度。

模糊 hash 主要是用於比較兩個檔案之間的相似程度，這部分較為具體的作法可以參考 ssdeep, sdhash, mvHash 等方式。而作者提出了 FbHash 的方法，作為改進現有的模糊 hash 值的方式，並證明了他的方式不論是在效率或是正確性方面，都優於其他方法。並且作者強調，以 FbHash 方法進行模糊 hash 值的比對，可以檢測出 2 個檔案之間小至 1%的共同點，且準確度達 98%以上。

3.投稿論文：A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM)

講者研究在兒少色情檢測（Child Sexual Abuse Material，CSAM）的使用上，為了減少檢測人員的負擔，一般會使用人工智慧來進行檢測，以自動化的方式先行篩選出可能為兒少色情圖片的方式來減輕篩選人員的負擔，使用的需求主要有「裸露檢測（nudity detection）」、「年紀估計（age estimation）」以及「膚色檢測（skin tone detection）」；講者提到了其他的方法，比如加入姿勢、性別、年齡等等的作為圖片以及影片的

估計項目：另外除了上述的元素以外，也可以如不同的影片中，找出同一個兒少受害者，並且估計其年紀。

兒少的照片以及影片，在我們數位鑑識的工作上，常常是重要的標的。嫌犯電腦的硬碟內，可能會有成千上萬的照片以及影片，如何有效地借由不同的方式過濾出兒少影片以及照片，是重要的課題。目前本局的數位鑑識軟體，可以針對膚色的裸露、相同人員以及地點進行辨識自動過濾，但過濾後仍然須要鑑識人員人工進行檢視以及比對。另外不同國家的青少年，通常也較難以辨識是否未成年，比如歐美小孩通常較為早熟，臺灣的執法人員較難以判斷其年紀，挌這一部分未來也可借重於此技術來更為精進。

4.投稿論文：AFF4-L: A Scalable Open Logical Evidence Container

本研究提供了一種開放式的製作映像檔的方式，稱為邏輯映像檔（logical imaging），該種映像檔製作方式，可以針對一些特別的資料來進行採證，比如加密的磁碟（如 Apple Mac 電腦的使用 T2 晶片加密），雲端硬碟以及串流影音的採證，在無法針對實體硬碟製作映像檔的情況下，就只能進行 AFF4 邏輯映像檔的製作。採用邏輯映像檔的製作，會以檔名來作為原始檔案儲存位置之表示。而本篇研究最主要是針對重複數據在使用邏輯映像檔採證時，可以只須製作 1 次即可，從而減少時間以及儲存的空間。具體實現的方式是先將 Logical Files 做一個 Block 的 hash，並經由 Metadata 去判斷他是不是重複的檔案，如果有則歸類為同一個檔案，整後就將其儲存 1 個檔案，如此即可有效減省空間。。

目前本局數位鑑識的標的，Mac 筆電已慢慢佔據一定之比例，我們也發現在 Mac 筆電於取證時，確實因為 T2 晶片加密的關係，需使用數位鑑識工具將 image 檔案儲存成 AFF4

格式再進一步進行解析。

參、本次心得及建議

數位鑑識在各國都是正在發展的領域，由於犯罪證據已逐漸多出現在數位裝置上，故數位鑑識亦受到高度的重視。國際大廠如 Google、微軟、Apple 等乃至網路上各式的免費工具及服務，推出的速度及數量相較於各國實際從事數位鑑識人員的數量，都更多且更快，故執法機關亦可能遭遇數位鑑識瓶頸的挑戰。另反鑑識技術的發展，致使數位鑑識人員需花費更多研究心力，以找出可能的關鍵證據，筆者認為出國研習是汲取新知最快的途徑與機會，吸收國際間的研究成果及了解未來趨勢，為提升國內數位鑑識能量應善用的方法。

本次有機會能參觀美國的科技偵查實驗室，了解對於數位鑑識及人員教育訓練的安排，數位鑑識需有一批有熱情的人員長期投入，培育一個優秀的數位鑑識人員需要長時間及多方的經驗，誠屬不易；參加 DFRWS 2019 研討會，遇見各國的數位鑑識研究學者、執法人員乃至國際大廠 Magnet AXIOM 及 BlackLight 等，了解包括 NIST 機構對於數位鑑識工具可信度的鑑驗、多種數位鑑識的研究主題，如 IoT、手機鑑識、惡意程式等，議題包羅廣泛，使筆者能了解數位鑑識的應用方式，他山之石，可以攻錯，假以時日可能為國內進一步研究的基礎。本次研討會並與南韓警方進行交流，了解南韓警方對於數位鑑識領域的人力投入是比我國還多，南韓學術界對於數位鑑識領域的研究亦相當盛行；另外與美國蘋果公司總部的數位鑑識人員交流，了解美國蘋果公司對於數位鑑識技術的重視；此外參加研討會的數位鑑識搶旗賽，也讓筆者了解精進技術及相關知識的必要性。這些出國取經的經驗，係為在國內較難取得的資源，筆者建議能夠持續安排鑑識人員能持續參加國外的數位鑑識相關的研討會，讓數

位鑑識人員能了解國際間重視的數位鑑識議題，並能與各國人員進行交流及尋找數位鑑識瓶頸的解決之道。

本研討會有包含日本警政署自行投稿及南韓司法機關與大學共同投稿，顯現與學術界共同研究亦是可提升執法單位數位鑑識技術的方式，可作為國內的參考；另目前各家數位鑑識工具的數位鑑識能力不一，故很難單一依賴一種數位鑑識工具就完整取得證物的證據，故準備多種數位鑑識工具是有必要的，而此項需求須持續投入經費。數位鑑識需有相關專業知識的人員操作數位鑑識工具並進行資料的解讀，尤其在各系統廠商持續不斷更新系統，如 Android、MAC OSX 及 Windows 等，鑑識人員需負有鑑識經驗，且必須在更版後能即使了解可能證據的存在位置，故建議數位鑑識人員能有長期培育的計畫。本次出國的經驗讓筆者獲益良多，也認識到一些新的鑑識工具和鑑識資源，相信對於未來工作的運用，有正面的效益和提升。