網路名偵探

凡走過必留下痕跡，利用數位鑑識找出網路犯罪足跡

網路科技的發展帶動雲端時代的來臨，人們可以隨時隨地存取雲端資料，並同步更新於所持有的行動裝置，其方便性雖然為人們生活帶來便利，卻也讓網路犯罪者開始伺機而動。由於網路犯罪不受地理限制、數位證據的獲取不易，使得數位鑑識工作較以往更為複雜，傳統的數位鑑識作法已不再符合需求，亟需建立一些可用於雲端的數位鑑識技術。

為解決雲端發展可能面臨的數位鑑識困境，中央警察大學資訊管理系王旭正教授研究團隊將其分為虛擬機器與雲端儲存兩個部份分別探討。在虛擬機器的部分，由於虛擬資料的完整性會影響虛擬機器的正常運作，為了避免虛擬機器的資料遭受損害，鑑識人員應盡量採用「現場蒐證鑑識法」，就是在主機仍在運行的狀態下，進行資料的取證與分析。研究團隊提出三種不同情境可採用的鑑識方法，供鑑識人員參考使用。第一，複製虛擬機器資料：在主機運行的狀態下採取資料，此時除可以複製硬碟資料外，還可以採取揮發性記憶體的資料，並將虛擬機器輸出成一個映像檔以利鑑識環境的建置。第二，虛擬機器映像檔損壞的鑑識方法：虛擬機器的映像檔可能會在採集的過程中或是人為的操作下損壞，導致資料不完整、無法啟動虛擬機器。為找尋虛擬機器中的證據，鑑識人員必須修復損壞的映像檔。若映像檔的檔案格式是 SPARSE 資料型別，在一定的損壞程度下，可以利用 SPARSE 資料表頭的復原與 SPARSE 資料描述的復原兩個步驟進行修復。第三，無法復原及其他鑑識手法：若採用前述的方法，映像檔仍然無法恢復，鑑識人員還是必須對於映像檔進行 metadata 的採取及分析。而鑑識人員除了對映像檔做分析外，也必須對於 Vmem 檔進行分析。在分析 Vmem 檔時可以利用「Compare VMware snapshots 工具」或是「Memparser 工具」，從記憶體中取得有用的資料。

在雲端儲存技術的部份，透過分析 Google Drive、OneDrive 和 MEGA 等目前市面上熱門的雲端硬碟 APP，期望能對雲端空間的資料記錄格式有所了解。團隊發現不論是哪一個雲端硬碟，皆能夠從手機中找到帳戶名稱，而在 Google Drive 和 OneDrive 中則可以找到檔案名稱與檔案創建、修改時間等，其中最為特別的是 MEGA，因為其將資料庫內的大部分資料加密，團隊在 MEGA 裡只找到了帳號名稱和使用者名稱的資料而已，其他資料因為加密所以無法得知。隨著數位證據的保存，將能夠提供調查人員更多實質上的鑑識分析與現場重建。

數位證據雖然不如實體犯罪事證那樣容易掌握，但凡走過必留下痕跡，所有網路行為都將成為犯罪調查的重要線索，因此研究團隊除了介紹雲端資料的儲存與虛擬機器的數位鑑識外，也分享復原影像檔的方法與相關工具，以協助

執法機關準確迅速地因應網路犯罪事件。

團隊 1. 中央警察大學資訊管理系王旭正教授研究團隊
計畫 1-1. 資訊安全之虛擬機器鑑識技術研究與證據分析(104 年)
AT https://www.grb.gov.tw/search/planDetail?id=11573474

計畫 1-2. 數位鑑識於雲端環境之犯罪者證據揭露研究(106 年)
AT https://www.grb.gov.tw/search/planDetail?id=12488377

新聞 1. 化身 CSI 鑑識偵探！「數位鑑識」專家如何從小小記憶體找出犯罪證據？
AT https://buzzorange.com/techorange/2020/08/11/digital-forensics/

新聞 2. 破解資訊隱藏伎倆 力阻數位影像藏密外流
AT https://www.netadmin.com.tw/netadmin/zh-tw/technology/C97145B13825464CB1F293223D009A7B