數位證物鑑識

「電腦虛擬世界遊戲Second Life中的明星突然身亡，詭異的是與這位明星談戀愛的男子也被謀殺。鑑識小組運用高科技數位技術抽絲剝繭調查，與罪犯鬥智後，竟牽扯出一連串的雇傭殺人事件。」這是目前最夯的刑事鑑識影片中的一個代表性劇情。

21世紀是數位科技登峰造極的時代，數位化除了正面的應用改善人類生活外，負面的也被使用在各式各樣的犯案中，從毒品、勒索到經濟犯罪等等，都利用電腦及網路作為犯罪工具，電子郵件、MSN或線上遊戲聊天功能常被用來進行犯罪行為的溝通聯繫，可以說幾乎每一個案件都無可避免地會有數位證據產生。

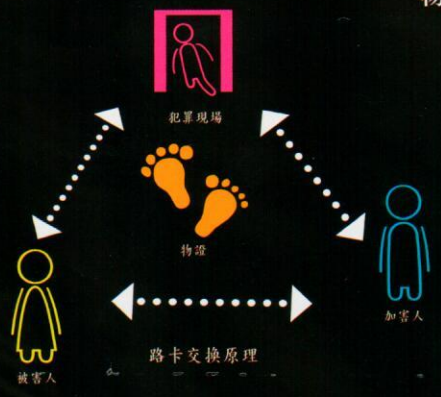
王朝煊／中央警察大學資訊管理系教授兼主任

0與1的魔法

數位資料乃以0與1符號編碼，儲存於電磁儲存媒體中，用以記載人類活動的資料或資訊。在電腦與網路廣為應用之後，人類活動資訊直接或間接記載於電磁儲存媒體的比率與日俱增。因此，蒐集與運用電磁儲存媒體中的資料或資訊，以還原或重建人類的犯罪活動，便成為資訊時代犯罪偵查不可或缺的一環。

數位證物乃足以證明犯罪構成要件的數位資料，或可以證明犯罪與被害者間或犯罪與犯罪者間關聯的數位資料。數位證物的型態包括：文字資料、數據資料、電腦圖像、數位影音資料等等。例如電話通聯紀錄、交易紀錄、電子郵件備份、網路連線紀錄、BBS 備份、部落格、色情圖像、監控影像、及最近流行的臉書，…等等。

數位證據主要基於路卡交換原理（Locard's Exchange Principle）：任何曾進入犯罪現場的物件必定留下跡證，且離開時也必定帶走現場的物證。偵查人員可據以重建犯罪現場、加害人、及被害人間的關係。類似地，任何進入計算機系統的存取行為，也會在計算機及網路系統的電磁儲存媒體留下電子跡證，甚至帶走系統中的電磁記錄。數位鑑識人員可採集被遺留的電子跡證或被帶走的電磁記錄，據以重建存取行為。



數位證據的取證與鑑識程序的步驟

數位證物雖為物證的一種特殊型式，但由於其具有備份與原件完全相同，軟體證據易於修改及不易銷毀等特性，因此數位證物的處理及鑑識與一般的物證略有所別。一般而言，數位證物鑑識（Digital Forensics）的工作主要包含證物的識別、蒐集、保存、記載、萃取、及分析與解讀儲存於電磁儲存媒體的證據。

證物識別乃從犯罪現場發現及分辨具有證據價值的物品。數位證物主要儲存於電腦及其週邊設備（如電腦主機、硬碟機、及掃瞄器等）或電磁儲存媒體（如光碟、磁碟、外接硬碟、及隨身碟等）。但其他的設備或物品只要具證據價值，亦應加以蒐集，例如運轉中的電腦螢幕如正顯示案件相關訊息，也是數位證物的一種形式；又如電腦報表紙的內容、螢幕或鍵盤上的小貼紙或文字符號，如與案情相關，皆應列為證物加以蒐集。

在明辨具數位證據價值的物品後，應即有系統地加以蒐集。證物應一一加以編號並攝影存證，如蒐集時必須拆解連接線，連結點的兩端應先貼好編號標籤，以便在鑑識實驗室依犯罪現場的組態重新組裝。

蒐集的數位證物或設備應妥為包裝與保存：以防靜電的袋子包裝，並避免置於高溫的環境或接近磁場，儲存環境的溫度與溼度，均應控制於適當的範圍，如溫度介於攝氏 10~32 度間，及相對溼度介於 20%~80% 間，以避免電磁儲存媒體受到損壞。

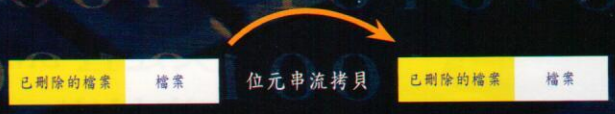
數位證物搜集及分析的過程均應詳加記載，例如證物被發現的位置與狀態，電腦組裝及網路連接的情形，發現及採集證物的人員等，皆應詳加記載，必要時並錄影或攝影存證。此外，為證明軟體證據未遭受到竄改或破壞，在犯罪現場宜計算及列印軟體證據的數位訊息摘要或簽章（如 MD5 或 SHA-1，SHA-2 等），並請當事人捺印指紋加以留存。另外，犯罪現場電腦系統顯示的時間及其與實際時間的差異情形亦應加以記載。

從電磁儲存媒體萃取軟體證據之前，宜先以適當的位元串流拷貝（Bit Stream Copy）工具[1]，將電磁儲存媒體的內容複製兩份，並計算其數位訊息摘要。其中一份作為萃取或分析的標的，避免直接於原始證物萃取或分析。在採集與案件相關的證據時，並應一併記載證據在電磁儲存媒體的位置。在分析與解讀電磁儲存媒體的軟體據證，特別需注意證據是否可以說明或提供物件與物件或犯罪者之關聯、物件之功用或如何被使用、及事件發生之時序關係等。

數位鑑識專業人才確保完整數位證物

由於電磁儲存媒體的軟體證據易於被修改的特性，且電腦在存取檔案資料時，往往會自動將存取活動記載於檔案的詮釋資料；且由於數位鑑識工作必須盡可能在不改變或破壞證物的情況下取得原始證物、能夠證明所抽取的證物來自扣押的證物、以及在不改變證物的情況下進行分析。數位鑑識人員不但必須具備證物鑑識的專業知識，而且必須精通電腦系統運作的原理與技術，以確保數位證據的證據能力與證據力。此外數位鑑識人員也須了解行為證據分析相關的基本知識，以進一步協助偵查人員重建犯罪的行為與動機，期能在勿枉勿縱的情形下，還原犯罪事件真相，順利破案。

1. 一般檔案拷貝並不會複製已被刪除的檔案。但位元串流拷貝將電磁儲存媒體的內容視為一系列的位元串流，並完整的複製每一個位元，已被刪除的檔案，甚至未被使用空間的內容，會一同複製到拷備的電磁儲存媒體上。



隨著微處理機及電磁儲存媒體技術的發展，電子設備的應用範圍已深入人類生活的每一個層面。例如電話手機、數位相機、各種資訊家電設備、衛星導航系統及定位系統、行車記錄器、悠遊卡及其讀卡機、錄影監控設備…等等，都將記載人們活動的詮釋資訊或內容。必要時各種電子設備的跡證，都可作為佐證或重建犯罪事件的輔助資訊，因此數位鑑識工作的範圍，也將隨著電子設備的廣為應用而日益擴展。鑑識人員必須與時俱進，隨時汲取科技新知，善用資訊環境的跡證，以釐清事實真相，協助破案。 FACT