談「數位鑑識」－從國內外實際案例看數位鑑識之重要性

張紹斌 / 合盛法律事務所律師
陳威棋 / 勤業眾信聯合會計師事務所經理

一、前言

隨著電腦科技及網際網路日新月異，日常生活與辦公事務均發生巨大改變，原本以手寫筆記記錄生活瑣事，轉變為以電腦或行動裝置記錄日常作息，從書寫信件改為透過電子郵件傳遞訊息。網際網路及電腦取代過去的人工處理程序，許多資訊轉變為數位化資料，並以電磁紀錄的方式保存在電腦設備、行動裝置或虛擬網路空間裡。日常生活如此，犯罪活動亦然。

電腦設備或行動裝置已變成一種犯罪工具，網際網路也成為新興的犯罪場所或媒介，因此，面臨訴訟爭議時，常會涉及數位證據[註1]的運用。由於數位證據有易遭竄改及刪除的特性，為確保於法院呈現之數位證據與原始證據相符，亦即訴訟法上常探討的「證據能力」及「證據同一性」，合乎標準程序的數位鑑識就十分重要。本文提供兩件國內外刑事案例，並介紹鑑識標準程序及訴訟常見策略，讓讀者對「證據能力」及「證據同一性」有更深入的瞭解，同時對數位鑑識在訴訟過程中的重要性有更深刻的感受。

二、數位鑑識定義

鑑識 (Forensics) 的拉丁語 Judiciale，原本的涵義就是「在法庭上的」。鑑識是為了支援訴訟事項，而不僅是針對事件本身的剖析。數位鑑識若與訴訟無關，充其量只是電腦科學上的數位環境重現。因此，數位鑑識可定義為：利用科學驗證的方式調查數位證據，經由數位證據的還原、擷取、分析等過程，還原事件原貌，以利事件調查，並提供法庭訟訴之依據。

數位鑑識源於國際電腦調查專家協會 (International Association of Computer Investigative Specialists，IACIS) 之研究，首次以電腦鑑識科學協助司法人員偵辦網路犯罪案件，提供網路犯罪證據蒐集與鑑識原則。在歐美等海洋法系國家，因應司法訴訟攻防強烈需要，數位鑑識領域廣受重視且蓬勃發展。採用數位鑑識技術所產出之數位證據是為了在法庭

中輔助判決，若執行人員展現的知識或能力不足以勝任數位鑑識技術之要求，勢必受到質疑與反駁，法官也可能不予採信（參考文獻 1）。

三、淺談證據能力與證據同一性

（一）何謂證據能力

在目前改良式當事人進行主義之下，「無證據能力、未經合法調查之證據，不得作為判斷之依據。」[註 2] 因此，具備證據能力並經合法調查，而得為法院評價之對象，乃嚴格證明法則之要件。[註 3]

證據能力，亦可稱為證據資格，係指得成為證明犯罪事實存在與否之證據資格。基本上，是否具備證據資格須由法院證據調查程序加以判斷。對於已提出接受檢驗的事實資料，進行事實關聯性 (證據能力) 及取得正當性 (證據合法取得) 之檢視，具備證據能力並通過合法性審查者，即為具備證據資格。

（二）何謂證據同一性

證據同一性，指在法院所呈現的證據即原始得用以證明待證事實的證據，亦即呈現於法院的證據必須未經竄改或刪除。換言之，必須是純淨且無污染，確實用以證明待證事實的原始證據，才符合訴訟法對於證據同一性的要求。如果無法通過證據資格檢驗，當然無法成為認事用法的依據。

由於數位證據本身之特性，數位證據同一性往往成為訴訟雙方攻防的重點。目前判斷有無證據能力仍依循刑事訴訟法相關規定，僅就證據取得程序進行審查，並未就證據內容做實質審酌。

四、實際國內外案例彙總與分析

談到數位證據，第一個聯想到的可能是電子郵件。其實除電子郵件外，生活中常見的文書檔案或線上即時對話紀錄，例如：Line message、Skype message、甚或幾年前十分盛行的 MSN 對話紀錄等，都可能成為案件的關鍵證據。以下分別列舉國內外實際案例進行分析：

（一）國內實際案例彙總與分析

去年國內有一起以 MSN 對話紀錄作為關鍵證據的性侵案件。一名 18 歲女子控告 20 歲前男友涉嫌性侵，兩人交往過程中，常透過 MSN 聊天。警方在調查過程中，查扣了男方筆記型電腦，並調閱兩人 MSN 對話紀錄，檢察官並以某則對話紀錄作為起訴男方的主要憑據之一。但男方反駁，當時兩人正在討論某齣偶像劇劇情，聊天過程中還談了其他很多事情，在警方所出示的對話紀錄中都不見了。

之後，男方將曾遭警方查扣的筆記型電腦送交法務部調查局資安鑑識實驗室進行鑑定，鑑定結果顯示此「關鍵 MSN 對話紀錄」有遭竄改的現象。雖然鑑識人員盡全力想還原 MSN 對話紀錄，不過由於當時檢察官的無心之過，直接開啓被查扣的筆記型電腦，並在讀取 MSN 對話紀錄時，以另存新檔的方式儲存成 Excel 格式，暫存於電腦桌面，導致原始 MSN 對話紀錄所在磁區已遭此 Excel 檔案寫入，部分資料遭覆蓋難以回復，因此無法還原原始的對話紀錄檔。男方進一步回推檔案遭竄改時間，發現是他在警局製作筆錄、電腦遭查扣期間發生，因而懷疑有員警涉嫌篡改或湮滅證據。

依「刑事訴訟法」第 155 條第 2 項之規定，該筆記型電腦內的電磁紀錄檔案均有可疑之處，亦即遭到污染而應無證據能力。因此，MSN 電磁紀錄以及所列印的文書資料均喪失其證據能力，當然不能據以作為認定被告犯罪事實的基礎。

最後，法院認定檢察官呈庭證據不足以得出男方有罪之結論，而判決男方無罪，並要求檢察官應就扣案電腦內資料遭刪除及覆蓋一事，進行偵查並加以釐清，如有不法情事，則應依法究辦。本案遭媒體揭露後，臺北市政府警察局發表新聞稿澄清表示，承辦員警僅「還原」嫌犯電腦資源回收筒內的檔案，檢視相關證據，並將案件相關檔案燒錄成光碟，附於調查卷宗後，再刪除檔案，移至資源回收筒，並未竄改或湮滅任何證據。然而為期勿枉勿縱，仍將承辦此案的員警移送地檢署偵辦。

(二) 國外實際案例彙總與分析

另一個案子發生在日本，西元 2009 年 10 月間，大阪發生一起轟動全國的案件，部分團體假冒身心障礙團體，享受郵資優惠，大量郵寄廣告傳單推銷商品。寄一封廣告信原需 140 日圓郵資，若持有厚生勞動省核發的「殘疾人團體專用郵費優惠證明」，則僅需 8 日圓，這些團體幾年內少繳的郵資逾 8 億日圓。大阪地方檢察署特別搜查部 (類似我國的特偵組，我國特偵組最初係參考日本特別搜查部制度所設立) 偵查終結後，以違反郵政法為由，將這些團體、廣告主及廣告代理商全部起訴。不過，偵辦此案的主任檢事 (相當於我國之主任檢察官) 前田恒彥因涉嫌篡改證據，於 2010 年 9 月遭逮捕，特搜部正、副部長稍後亦因涉嫌包庇前田恒彥而被逮捕，震撼日本法界。

前述團體要假冒身心障礙團體，必須取得身心障礙團體的假證明。偵辦厚生勞動省偽造文書案件的主要負責人前田恒彥主任檢事，懷疑承辦本案的村木厚子局長在國會議員關說下，指示屬下協助偽造身心障礙團體證書。前田主任檢事認為，實際製作假證明書的上村科長是在 2004 年 6 月上旬接到村木局長指示。然而，在上村科長家中查扣的電腦軟碟資料卻顯示：假冒證明書的電子檔案最後修改時間為「2004 年 6 月 1 日凌晨 1 時 20 分」。如此一來，故事發展顯然和前田主任檢事設想及起訴書所載「局長於 6 月上旬為指示」的內容不一致。為了使故事發展和設想劇本一致，前田主任檢事竟然於 2009 年 7 月 13 日，用自己的手提電腦將扣押的磁碟資料內容改為「2004 年 6 月 8 日午後 9 時 10 分」，如圖 1 所示。

圖 1　前田主任檢事篡改電子檔案最終更新日之紀錄（參考文獻 2）

案件進入法院審理後，發現關鍵證據日期與起訴事實不符，最後判決村木局長無罪，同時對檢察官所提大部分證據的真實性存疑，不予採用。前田主任檢事涉嫌變造證據一事，經媒體踢爆後，最高檢察廳被迫介入詳細調查，2010 年 9 月 21 日以「篡改、湮滅證據」的罪名，逮捕瀆職的前田恒彥；稍後又以明知前田變造證據，卻故意掩蓋其犯行，有隱蔽犯人之嫌，逮捕前特搜部部長大坪弘道與副部長佐賀元明，兩人皆遭到起訴免職。

(三) 案例綜觀

由上述兩案例可知，刑事案件若涉及數位證據之運用，針對證據是否曾遭汙染？是否能於法院提出作為裁判之基礎？是否具備證據能力？這些議題往往成為法庭攻防的重點。越是關鍵的證據，處理越應小心，以免好不容易找到可以證明待證事實的珍貴資料，最後卻因為忽略證據同一性而無法使用。

五、數位證據同一性重要性之說明及常見訴訟策略分享

由於數位證據具有增刪修改不著痕跡的特性，在法院呈現的數位證據都無法排除遭破壞或修改的可能性。因此，數位證據所面臨的挑戰不外乎當事人質疑數位資料遭到篡改或破壞。在訴訟攻防時，雙方當事人的爭執焦點往往在於「於法院呈現的數位證據內容是否曾遭增刪修改？」

針對此問題，實務上常見的攻擊或防禦方法包括：(1) 利用數位證據鑑識技術，證明數位證據內容曾或未曾遭增刪修改；(2) 說明數位證據自蒐集到呈送法院的流程，包括數位證據蒐集、保存、運送及分析等環節的細節。

回頭看上述國內實際案例，該案於數位證據蒐集與處理時，有三個可議之處：

(一) 關鍵 MSN 對話紀錄檔遭修改，前面已多所著墨，不再細談。

(二) 檢察官於蒐集及分析 MSN 對話紀錄檔時，未恪遵「避免對證據造成不必要變動」之原則，直接開啓被告的電腦，而非以適當的鑑識專用軟硬體擷取目標檔案至鑑識分析主機，或者銜接防寫設備後再進行後續作業。此做法讓被告有機會質疑檢察官進行勘驗時，其做為起訴基礎的 MSN 對話紀錄檔於蒐集及分析過程有遭修改之疑慮。

(三) 檢察官開啓被告電腦進行作業時，以另存新檔的方式將 MSN 對話紀錄檔 (已遭修改，但檢察官並不知情) 存成 Excel 格式，暫時存放在該電腦的桌面上，而 Excel 檔在儲存 (寫入) 磁碟機時，剛好重複寫入原本儲存原始 MSN 對話紀錄檔的磁區，導致原始 MSN 對話紀錄檔部分內容遭覆蓋而無法還原，因此無從得知原始 MSN 對話紀錄內容。

針對上述三點可議之處，整理各種可能情境及其對證據同一性之影響，如表 1 所示。

表 1　不同情境對證據同一性之影響

項次	可能情境	取得證據是否具備證據能力？
1	檔案遭修改，第一線人員取證方式又有瑕疵。	很可能被認定為無證據能力
2	第一線人員取證方式無瑕疵，但取得的是被竄改過的證據 (無論取證人員在取證過程中知情與否)。	
3	檔案未遭竄改，但第一線人員取證方式有瑕疵。	
4	檔案未遭竄改，第一線人員取證方式亦無瑕疵。	基本上會被認定具有證據能力

六、國外數位證據標準程序最佳實務說明

國際標準組織暨國際電工委員會 (International Organization for Standardization / International Electrotechnical Commission，ISO/IEC)、英國警察協會 (Association of Chief Police Officers，ACPO) 與美國國家司法研究院 (National Institute of Justice，NIJ) 等組織均曾發布數位鑑識相關作業程序，以符合證據同一性之原則。由這些作業程序可以歸納出以下共通性原則與個別特色要點：

(一) 共同基本原則

1. 確保數位證據未受外力影響

數位證據有易被時間影響、易遭改變、毀損或破壞等特性，在處理上必須特別強調證據的完整性，以保全其證據能力。

2. 執行人員須有專業能力

數位證據的蒐集、分析過程皆有可能導致原始資料的改變，在存取原始資料時，必須確保人員具備實作能力，並且可以說明即將進行的行為與證據的關聯性。

3. 完整記錄證據監管鏈 (chain of custody)

數位證據處理過程的每一道程序皆應被完整記錄 (即證據監管鏈)，以備第三方得以依據留存的紀錄重現程序，並得到相同的結果，以驗證數位證據之正確性。

4. 遵守標準作業程序

針對證據監管鏈原則，從現場採證至呈庭供證為止，監管物證之所有人員均須出庭確認，以建立完整之監管鏈，證明物證未遭掉包、干擾或破壞。為確保各種物證的證據能力，偵查人員與鑑識人員必須遵守嚴謹的標準作業程序。

(二) ISO/IEC 27037:2012

ISO/IEC 27037（參考文獻 3）是 ISO 國際組織針對數位證據相關作業程序所訂定之指引 (Guidelines)，其中訂有第一線證據保全原則，包含：證據鏈監管原則、現場處理注意事項、角色與職責、人員能力建議、謹慎處理原則、文件化要求、勤前會議簡述、證據蒐集及擷取優先順序、數位證據保存等。除前述共同基本原則外，該指引的特點分述如下：

1. **現場處理注意事項**

為保持現場完整，該指引要求設置現場管制負責人，以管制現場進出與證據存取，除隔離嫌疑人員接觸現場外，並記錄現場環境與設備狀態，管制設備現況與相關資訊等。

2. **角色與職責**

該指引將涉及數位鑑識證據保全作業程序的人員分為兩種角色：一是數位證據一線處理人員，主要職責為數位證據的辨識、蒐集、擷取與保存，包含數位證據蒐集及擷取報告的編撰、數位證據的保存及處理；二是具備專業鑑識職能之數位證據鑑識專家，在一線人員無法處理時 (如複雜的伺服器架構或磁碟陣列儲存裝置等)，提供技術性協助。

3. **文件化要求**

應詳細記錄操作動作與所存取的資料名稱、螢幕顯示畫面、目標設備的廠牌、型號、規格等資訊，並建議可用攝影方式記錄。

4. **勤前會議**

由於進行證據保全的現場環境情況可能無法預料，必須先經由勤前會議討論案情方向、處理證據類型、人員職責分工、異常狀況處理對策等。

5. **證據蒐集及擷取優先順序**

若電腦主機是開機狀態，則非必要時不要關閉，以避免揮發性資料 (如 RAM、Cache RAM、執行中程序、網路連線與應用程式開啓通訊埠等) 可能因關閉主機而消逝無法回復。

6. **證據封存、運送及儲存**

取得證據後，證據的封存應有明確標示紀錄與阻隔防護性包裝，運送過程中應確保環境受到監管與保護，證據的儲存地點應確保實體環境與防護機制的安全性。

(三) NIJ 電子犯罪現場調查

NIJ 的「電子犯罪現場調查：第一線應變人員指引」（參考文獻 4）所闡述的作業要點與前述文獻要點相似，在證據擷取部分有細部說明為其特色，簡述如下：

1. 應確認檢查人員的鑑識用儲存裝置已事先完成鑑識性抹除作業。
2. 存取證據資料時，皆應使用具防寫功能的方法存取。
3. 應取得所調查的儲存媒體實體與邏輯大小，以確認所有配置空間 (包含主機保護資料區域) 、硬碟序號、是否有刪除分割等資訊。
4. 應使用適當的鑑識專用軟硬體將目標證據擷取至檢查人員的儲存裝置。
5. 應比較原始證據與複本的 Hash 驗證值，以確認是否成功擷取。

(四) ACPO 數位證據良好實務指引

ACPO 的「數位證據良好實務指引」（參考文獻 5）主要分為四大部分：數位證據處理原則、犯罪現場注意事項、網路鑑識與揮發性資料、向內部調查人員進行簡述。除共同基本原則外，其餘重點分述如下：

1. 現場處理注意事項

在現場處理時，該指引特別關注電腦在關機與開機狀態下的不同處置，以及運送時的狀態保護與儲存時的防護環境狀態。

2. 網路鑑識與揮發性資料

於某些情況下，目標主機雖處於運作狀態，仍須對設備擷取相關揮發性數位證據，如記憶體內存放的資料，此時須謹慎處理，以避免對證據造成不必要之變動。

七、結語

綜言之，數位證據的取證過程對於證據能力有極大的影響力，若缺乏鑑識人員專業知識、技術與設備，一般人自行任意操作數位設備都可能導致關鍵證據遭覆蓋或刪除。由於數位證據具有不著痕跡增刪修改的特性，從產生到呈庭供審，其內容的真實性會不斷遭受質疑，任何略懂電腦的人都能改變數位資料，縱使數位證據遭司法機關扣押，仍不能保證內容不會遭人更動。

因此，舉凡數位證據的蒐證、保全、分析與監管，每一環節都應由專業機構及人員執行，並依據嚴謹的作業程序，全程留下文字與影像紀錄，才能於訴訟攻防時，提出具體有利之佐證。

企業組織可能面臨員工背信、營業秘密或個資外洩等訴訟困境，更應重視數位鑑識對業務營運的重要性，思考如何適切導入數位鑑識，並結合現行資訊安全、稽核內控、遵法規範等措施，以建構有效的防禦基石，除於事故發生第一時間保存有效證據外，並可進一步於平日建立符合鑑識原則之整體證據環境，自我培養數位鑑識能量，或委託外部專業數位鑑識機構協助，使企業管理階層能從容因應可能的訴訟挑戰。

※ 註：

1. 我國刑法與刑事訴訟法並沒有數位證據用語之規範，但數位證據本質上即是電磁紀錄所形成的電子資料。而與電磁紀錄有關之法律用語，在刑法中首次出現於第 10 條第 6 項，刑事訴訟法則於第 122 條。
2. 刑事訴訟法第 155 條第 2 項參照。
3. 大法官會議釋字第 582 號解釋。

※ 參考文獻 / 資料來源：

1. Dr. Frederick B. Cohen, Ph.D. Fred Cohen & Associates and California Sciences Institute, “Fundamentals of Digital Forensic Evidence”, 2008。
2. http://blog.goo.ne.jp/narmuqym/e/3b0575daa1dd4b71c54ede86a5f46dd4。
3. ISO/IEC 27037 Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence, 2012。
4. National Institute of Justice, “Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition”, April 2008。
5. Association of Chief Police Officers, “Good Practice Guide for Digital Evidence”, March 2012。