專 題 企 劃

數位鑑識「原件不可變動原則」之適用—由行動裝置鑑識與電腦鑑識差異探討

內政部警政署刑事警察局科技研發數位證據股股長 陳詰昌

◆ 目次 ◆

壹、前言

數位鑑識（Digital Forensics）發展已經有數十年時間，於1984年美國聯邦調查局（Federal Bureau of Investigation，FBI）因應電腦犯罪成立電腦分析與犯罪應對小組（Computer Analysis and Response Team）後，往後數十年間全球其他國家亦相繼成立電腦犯罪偵查單位。經過十幾年時間的摸索後，各國政府機關或相關單位與學術界在2000年前後，相繼推出各種數位鑑識標準程序或原則，提供執法機關或相關單位作為參考或範本，這些程序與原則不僅對實務界之數位鑑識程序標準化、證據鍊（Chain of Custody）及證據完整性有相當程度提昇，也讓院、檢、辯三方對數位證據之證據能力及證據同一性有所依循並產生信賴，但是數位證物愈來愈多元，尤其行動裝置（Mobile Device，平板電腦、智慧型手機等）類數位證物呈級數成長，過去針對電腦類證物所制定數位鑑識程序與原則，是否仍然可套用於行動裝置取證上，值得去討論，而其中「原件不可變動」就是其中一項深植鑑識人員及司法人員的重要原則。

在2010年前，犯罪案件相關數位證物主要還是以電腦、伺服器及儲存裝置等為主，當時諾基亞（Nokia）還是手機業龍頭，手機僅有簡單撥打電話、接收簡訊等簡易功能；當Android、iPhone等智慧型手機陸續上市，外加國內3G、4G行動網路普及化，智慧型手機與平板電腦等證物數量每年以倍數成長，過去幾年以刑事警察局每年收案數量統計，行動裝置證物已超過整體證物數量七成以上，當初訂定數位鑑識原則之時空背景與現在實際狀況已迥然不同，但是許多數位鑑識程序或原則仍未適時修訂，並將之套用到行動裝置鑑識領域。

智慧型手機等行動裝置普及原因主要為渠兼具通訊、小額支付（MicroPayment）、衛星定位（Global Positioning System，GPS）、攝影錄音等功能，作業系統與硬體架構本來就與電腦主機不同，且系統開發商或手機製造商均不斷提升行動裝置安全性，相對造成司法機關或偵查機關在數位鑑識工作上諸多瓶頸。以今（2016）年2月間新聞，蘋果（Apple）公司拒絕美國法院請求，不肯為涉嫌加州恐怖攻擊案狙擊手所持用的iPhone手機進行解鎖[1]，就可以窺知數位鑑識在行動裝置取證上遇到極大挑戰，雖然後來美國聯邦調查局支付數約50萬台幣酬勞請鑑識公司Cellebrite協助成功解鎖，但並不是每案件都能如此幸運。

1 中時電子報2016年2月18日，拒絕解鎖 蘋果公然槓上法院，
http://www.chinatimes.com/realtimenews/20160218000012-260408

同樣在國內數位鑑識工作中，在行動裝置鑑識方面也遇到開機密碼鎖、安全鎖、全磁碟加密及應用程式（APP）安全機制提昇等挑戰，而過去數位鑑識原則-「原件不可變動」又如孫悟空的緊箍咒般緊緊綁住數位鑑識人員手腳，因此筆者認為實有必要在衡量法律上證據能力及證據同一性等原則及數位鑑識技術可行性後，適度修正數位鑑識程序與原則以符合現況改變。

貳、文獻探討

一、數位鑑識意義與範疇

數位鑑識早期稱為電腦鑑識（Computer Forensics），最早是在1991年於波特蘭舉辦的國際電腦專家協會（International Association of Computer Investigation Specialists, IACIS）所提出，就字義來看，就可以知道當時主要是針對電腦設備上數位證據以科學及經驗證方法對數位證據進行保存、擷取、驗證、識別、分析、解讀、紀錄及呈現，還原事件原貌並協助法院重建犯罪過程作為審判之參考[2]。而所謂數位證據（Digital Evidence）依照電腦證據國際組織（International Organization on Computer Evidence，IOCE）於2002年提出之定義，任何以數位型態儲存或傳送，可用於證明某項事實都稱為數位證據。因此數位證物不再僅限於過去電腦主機，而是擴展至各式生活用品，如MP3撥放器、汽車導航設備、行車紀錄器、平板電腦、智慧型手機、數位相機、隨身碟、網路分享器、網路磁碟機、網路攝影機、智慧穿戴裝置等，甚至未來可能問市的智慧汽車、智慧冰箱、智慧冷氣等物聯網（Internet of Thing，IoT）設備；當網路犯罪或科技犯罪證物不在僅僅限於電腦主機，當然數位鑑識標的也不再局限於電腦主機，因此數位鑑識一詞漸漸取代電腦鑑識成為通用名詞；電腦犯罪也漸漸被網路犯罪或科技犯罪所取代。

除了數位產品種類繁多外，法庭上因案情需要所提出之鑑識需求也愈來愈五花八門，因此數位鑑識也衍生出不同子領域:電腦鑑識、行動裝置鑑識（Mobile Device Forensics）、網路鑑識（Network Forensics）、資料分析鑑識（Forensic Data Analysis，FDA）、資料庫鑑識（Database Forensics）等；其中電腦鑑識主要包含電腦、嵌入式系統及隨身碟等數位證物鑑識，主要進行還原、解讀及分析儲存裝置（Storage Device）內殘存檔案，重建及還原事件過程或與取得案情相關證據；行動裝置鑑識主要在還

2 Digital Forensics Research Workshop. “A Road Map for Digital Forensics Rsearch”, 2001. Technical Report. https://www.dfrws.org/2001/dfrws-rm-final.pdf

原行動裝置內遭刪除資料或證據，與前項差異在於行動裝置儲存裝置通常燒焊於主機板，且型號、種類因裝置廠牌型號等均不盡相同，因此行動裝置上資料擷取與保存之難度較電腦主機高；網路鑑識主要監錄網路設備透過網路路由傳送封包內容及網路設備紀錄檔，透過分析擷取封包、網路設備及電腦主機系統日誌檔（Log File）等方式，追查及還原駭客入侵事件；資料分析鑑識主要分析結構化資料找出可疑犯罪事證；資料庫鑑識主要針對資料庫及其元資料（metadata）進行鑑識分析，運用資料庫內容、日誌檔及記憶體資料等進行案發重建。

數位證物經由數位鑑識方法擷取分析後，呈現與案情相關之數位證據，而美國司法實務上將數位證據分為三大類：一類為使用者非主觀意識下，由電腦系統自動生成之紀錄（Computer-generated Records）、第二類為使用者主觀意識下運用設備產生或儲存之資料或檔案（Computer-Stored Records）及第三類為兩者混合型。第一類主要為系統自動產生之紀錄，用於記錄系統狀態及稽核使用，例如Windows系統中事件檢視器記錄應用程式、安全性及系統日誌、瀏覽器記錄上網歷程、伺服器日誌檔等；第二類者為使用者所輸入或人為產生檔案或紀錄，例如Microsoft Word、Excel、Power Point文書檔案、聲音檔、影片檔、圖片檔、電子郵件等；第三類混合型資料含有系統產生及使用者輸入資料，舉例來說如試算表中，有部分為使用者輸入，部分為依據使用者輸入值後，經數學運算後所得資料。

二、數位證據之證據能力與同一性

數位鑑識之最終目的就是將案情相關之數位證據[3]真實呈現於法庭，並為法庭所採用，還原及釐清系爭事實。因此數位證據是否具有證據能力及證據同一性就是法庭是否採用之關鍵。

㈠ 證據能力

刑事訴訟法第155條第2項規定「無證據能力，未經合法調查之證據，不得作為判斷之依據」。證據能力[4]即是證據得提出於法庭調查，以供作認定犯罪事實之用，所應具備之資格；此項資格必須證據與待證事實具有自然關聯性，符合法定程式，且未受法律之禁止或排除[5]，始能具備。因此證據能力主要規範證據取得是否合法取得及與待證事實有相當關聯性。

3 Inikpi O. Ademu, “A New Approach of Digital Forensic Model for Digital Forensic Investigation”, International Journal of Advanced Computer Science and Application,Vol 2, No.12, 2011

4 司法院大法官釋字582號解釋

5 最高法院94年台上字第716號判決

㈡ 證據同一性

證據同一性[6]即指於呈現於法庭用來證明待證事實之證據與原始證據兩者必須一致，亦即證據是否有可採用價值之程序，在提出該項數位證據前，提出者必須要證明數位證據符合真實性要求。在美國聯邦證據法第901條已明訂證明證據真實性相關規定，並且可適用於數位證據。要證明證據的同一性，就在於證據鍊的控管，在數位鑑識要分為兩個層面來談，一為實體證物，另一為數位證物內含的數位資料；由於數位證據具有抽象、易破壞、消逝等[7]特性，因此數位證據同一性往往成為訴訟攻防的重點，數位鑑識人員為避免不必要爭議，加上數位證據具有可無損複製等特性，因此通常會以重製原件方式產生證物副本，並以證物副本進行鑑識工作，避免更動原件並將原件封存供第三方複驗；因此「原件不可變動」成為數位鑑識人員及司法人員最高原則及鑑識程序鐵律。

三、數位鑑識原則

為達到法庭對證據能力及證據真實性之要求，過去十幾年來已有相關數位鑑識流程及原則，以下例舉近年來具代表性之數位鑑識原則。

㈠ 美國國家司法研究院（National Institute of Justice，NIJ）

2008年美國國家司法研究院發布電子犯罪現場調查導引第二版[8]（Electronic Crime Scene Investigation: A Guide for First Responders, 2nd Edition），這份指導文件主要原則:

1. 在證物蒐集、保全及運送過程中不可變更證據。
2. 數位證據只能由受過訓練之專業人員進行檢驗。
3. 數位證據在擷取、運送過程之處理細節及步驟、裝置狀態等必須詳細記錄及保存，供作日後重新檢視時使用。

㈡ 歐洲鑑識科學協會（European Network of Forensic Science Institutes，ENFSI）

2009年歐洲鑑識科學協會發表數位證據司法鑑定最佳實踐指南（Guidelines for Best Practice in Forensic Examination of Digital Technology），提出以下5項原則:

1. 一般證據處理規定適用於所有數位證物。
2. 擷取數位證據時，所有操作不能改變證據本身。
3. 當有需要對證物原件進行存取時，處理人員必須經過適當訓練並取得資格。

---

6 劉秋伶，數位證據之刑事證據調查程序，政治大學法律學研究所，99年1月
7 同註3
8 NIJ Special Report, Electronic Crime Scene Investigation: A Guide for First Responders, 2nd Edition, https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

4. 所有對證物進行擷取、存取、儲存或轉移之動作都需要被詳細記錄、保存，供作重新檢視時之用。
5. 當處理人員處理證據時，必須對所有處置數位證據之操作負責。

㈢ 英國警察協會（Association of Chief Police Officers，ACPO）

2012年英國警察協會提出數位證據最佳實踐指南第5版（Good Practice Guide for Digital Evidence）[9]，這份指南主要提供檢驗各類電腦設備的指引，使處理人員能及時並適當方式來處置高科技產品。這項指引中列出處理數位證據的4大原則：

1. 執法部門及其所屬人員不能對將提交於法庭之數位證據採取改變資料內容之動作。
2. 如有必要對證據原件進行直接存取時，操作人員必須具有相當訓練資格，而且有足夠理由說明並解釋進行該操作與取證之關聯性及可能造成之影響。
3. 所有處理數位證物之動作必須記錄及保存，使第三方單位可由前述紀錄在同樣程序或操作得到相同結果。
4. 承辦人員必須確保遵守相關法律及原則。

㈣ 進階資料擷取模型（The Advanced Data Acquisition Model，ADAM）

於2013年理查亞當斯等人所提出，在這篇論文中提及數位鑑識人員必須遵守以下原則：

1. 數位鑑識人員不可以改變原件資料。如果必須對原件進行更動，鑑識人員之操作必須明確知道造成之影響並合理解釋所造成之變動。
2. 擷取及處理原件資料的操作及任何原件資料的複製必須清楚記錄及包存。這包括規範證據處理的規則，譬如證物監管鍊紀錄及檢核步驟的雜湊值[10]（Hash Value）等。
3. 數位鑑識人員不可從事任何超出自己知識或技術範圍之操作。
4. 數位鑑識人員進行鑑識工作時，必須全面考量人員、設備安全等因素。
5. 任何時刻必須考量鑑識過程之操作是否可能造成他人法律權益影響。
6. 數位鑑識人員必須明瞭機關對數位鑑識的政策與程序。
7. 客戶端、司法人員、管理者及團隊成員間必須要有適當溝通。

由以上數位鑑識原則，為確保證據同一性，其實都含禁止對外力對數位證據原件變動，除非有合理之理由及確認操作結果不會造成證據資料更動下，才能有經驗並且

9 ACPO Good Practice Guide for Digital Evidence V.5, http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

10 雜湊：雜湊運算，可將不特定資料經函數運算得到一值，數位鑑識領域通常用MD5或SHA1雜湊運算來比對檔案是否一致，若兩值不一致時，表示兩檔案有出入。

訓練合格人員進行取證；因此，為避免引起爭議，在訂定數位鑑識程序時，即依循此原則訂下禁止更動原件並使用副本作為鑑驗操作分析使用；但此原則套用於行動裝置鑑識或雲端鑑識時，使鑑識人員操作分析造成限制，讓法院、檢察署及律師產生混淆之情形，甚至有律師質疑行動裝置鑑識過程為何未使用副本進行分析、為何變動原件等情形。

參、行動裝置鑑識之困難

一、行動裝置與電腦鑑識之差異

電腦鑑識與行動裝置鑑識在操作上有些許差異，而造成差異的主要原因就是兩者在作業系統（Operation System）、檔案儲存位置系統、功能及特性等，造成數位鑑識原則適用於行動裝置時之困擾，以下例舉電腦系統與行動裝置之差異：

㈠ 電腦的作業系統存在次要記憶體（Secondary Memory，常見的有硬碟、軟碟、光碟、USB隨身碟等），但行動裝置的作業系統存放在唯讀記憶體（Read Only Memory, ROM）；電腦的檔案存放在次要記憶體，然而行動裝置的檔案存放於隨機存取記憶體（Random Access Memory， RAM）。由此可見，電腦系統之作業系統與檔案系統是存放在同一位置，而行動裝置卻不是如此。

㈡ 電腦鑑識要對硬碟行全磁碟複製（bit-by-bit copy或稱副本製作）取證，可以將電腦開機後，直接取出硬碟進行映像檔複製；然而行動裝置鑑識時，由於各家晶片廠牌規格不一，將唯讀記憶體取下（Chip Off）進行分析解讀所需技術、花費及時間等門檻過高，因此幾乎行動裝置常見取證方式，均於開機狀態下透過連接線連接取證設備或電腦設備進行。

㈢ 另外行動裝置內部通常嵌入快閃記憶體（Flash Memory），用於內部儲存使用，這是一種非揮發性記憶體，具有可寫可讀之特性；而快閃記憶體依照晶片物理數位邏輯特性分為NOR及NAND兩種，NOR快閃記憶體速度比較快，因為這類記憶體可以映射到處理器記憶體，而且處理器可以由NOR快閃記憶體上直接執行，但是在售價上比較高且刪除、寫入資料速度較慢；另一種NAND快閃記憶體就比較像電腦硬碟，價格上比較平價，但是無法像前者可以直接映射到處理器記憶體，所以儲存在上面的程式碼無法直接執行，必須要先載入到記憶體後才能由處理器執行。因此多數行動裝置會將NOR快閃記憶體使用於儲存作業系統的啟動程序或系統程式，使用NAND快閃記憶體作為儲存資料或外插的記憶卡使用。

㈣ 行動裝置在硬體、嵌入式系統多元化、產品週期短、汰換速度快、網路與通訊混合、執行緒具有啟動後背景運作關機暫停運作等特性；以鑑識角度檢視，行動裝置較電腦鑑識困難度與複雜提高許多。以電腦系統中的儲存磁碟而言，當系統沒有連接電源時就是關機狀態，且可在關機狀態下取出硬碟進行取證，然而對行動裝置而言，大致上區分為以下5種狀態，若沒有搞懂極可能改變裝置狀態並破壞證據完整性。

1. 關機狀態：裝置關機、電池移除。
2. 初始狀態：回復出廠狀態，使用者資料清除。
3. 待機狀態：雖然系統已開機，但裝置處於被動狀態，只維持系統正常運作，如系統時間及網路連結等。
4. 半啟動狀態：系統等待特定時間去執行某件工作，譬如鬧鐘在特定時間要響鈴，應用程式在特定時間要執行特定功能。
5. 啟動狀態：裝置為開機狀態並且該應用程式執行，例如接到來電。

二、證據同一性之適用

行動裝置有專屬的作業系統、資料儲存、電源系統及其他電子元件等，且行動裝置因為無法像電腦系統有統一儲存裝置規格、檔案系統及易取出的儲存裝置等條件，因此行動裝置必須在開機狀態下進行取證，如前所述，行動裝置的狀態是變動的，當鑑識人員開機後連接至取證設備時，其狀態可能已經改變，甚至於部分資料可能已更動，重點還不是鑑識人員可以掌握，因此證據的完整性或同一性就可能遭受質疑。

過去鑑識人員為驗證證據同一性，在製作完映像檔時，通常會對製作出來的映像檔進行雜湊值（Hash Value）計算，用來證明證據一致性；但是在手機取證上，當下擷取之映像檔與下一秒所擷取之映像檔計算出之雜湊值可能不同，因為擷取手機資料時，手機狀態是在開機狀態下，磁區上資料可能前後有所差異。

除此之外，由於行動裝置是在開機狀態下取證，作業系統密碼破解的問題、系統安全控管的問題、映像檔製作權限問題等都需要對原件，也就是必須要對行動裝置進行適度更動才取出關鍵性證據；而每一種取證方式都是對證據同一性的破壞，下一節中將例舉常見必須更動原件之取證狀況。

三、行動裝置「不變動原件」之困境

㈠ 無法破開機密碼鎖及圖形鎖

行動裝置與電信門號相結合已成為個人身分之代表符號，因此許多金融、購票、社群服務均利用行動裝置進行認證，為保護使用者隱私及提高行動裝置安全性，行動

裝置可設定密碼鎖或圖形鎖等第一道安全機制，避免因遺失或其他因素遭人冒用。相反地，在鑑識取證時，第一道難關就是密碼鎖與圖形鎖，由於行動裝置無法像電腦一樣可以輕易取出儲存裝置進行取證，而且現在行動裝置已開始支援全磁碟加密等機制，在無密碼鎖或圖形鎖之前提下，行動裝置無法進行下一步鑑識取證。

因此為能繼續手機取證之目的，第一步就是要破解密碼鎖或圖形鎖，電腦系統可以藉由取出磁碟或以外接裝置啟動方式進行勘查取證，然而行動裝置系統基於安全性及避免使用者設定錯誤等因素考量，最高權限帳號已遭鎖定，行動裝置使用者只能使用特定權限範圍，再加上行動裝置無法接受以內建作業系統以外之其他系統啟動前提下，要能破解密碼必須要進行提權操作。

所為提權就是讓行動裝置取得最高控制權，如同Windows系統的Administrator帳號，在行動裝置中藥取得最高權限稱為Root[11]（Android系統取得最高權限帳號）或iOS JailBreaking（iOS取得最高權限）；以Android手機為例，要破解開機密碼必須要取得gesture.key這個檔案[12]，但由於這個檔案存放在系統目錄下，若無Root權限是無法存取，所以必須要對Android系統進行提權動作，常見方式就是透過刷機方式進行，簡單來說就是置換作業系統，藉以取得最高權限。

以上取證方式對律師、檢察官、法官或者過去的鑑識原則似乎有違背之情形，然對於關鍵證據本身並無改變，因為以Android手機所分配磁區而言，有發生改變的是在系統區（System）與還原區（Recovery），對於雙方所爭論的使用者資料區（Data）是不發生影響或改變的。

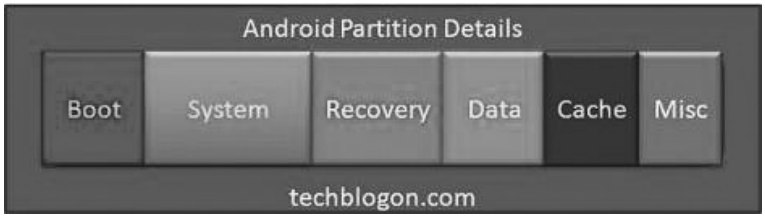

圖1　Android磁區分配圖

㈡ 無法取證行動APP內容

通訊及社群軟體已取代電話簡訊及語音服務，過去各司法機關或相關人員把取

11 維基百科，root(Android)，https://zh.wikipedia.org/wiki/Root_(Android)
12 圖型鎖密碼儲存位置http://forum.xda-developers.com/showthread.php?t=1800799

出通訊軟體對話紀錄及刪除還原視為理所當然，但是在系統不斷提升安全性同時，Android系統也對APP開發商進行要求，不管在APP權限控管或APP安全設定等，對數位鑑識人員而言，又是另一項新的挑戰。

過去對於行動裝置取證大多透過邏輯取證（Logical Extraction）或備份取證，也就是相當於Windows系統的檔案複製功能；即便如此簡單的功能，在某些行動裝置APP都是禁止的。舉例來說，國人最喜歡使用的通訊軟體LINE，在5.3.1版之後就加入安全性機制「allowbackup=false」，禁止透過邏輯取證方式對LINE進行取證，因此只能由Root方式或更動LINE應用程式進行取證，兩者擇一進行。

而以上兩種取證方式都是更動到行動裝置部分原件，前者如前項所述破壞系統及還原區，後者更動應用程式本身，對法院、檢察官、律師或偵辦單位來說，必須要在更動部分與案情無關證據為前提，取出關鍵證據，亦或「不更動原件」，但完全無法取出所要證據之情形做一選擇。

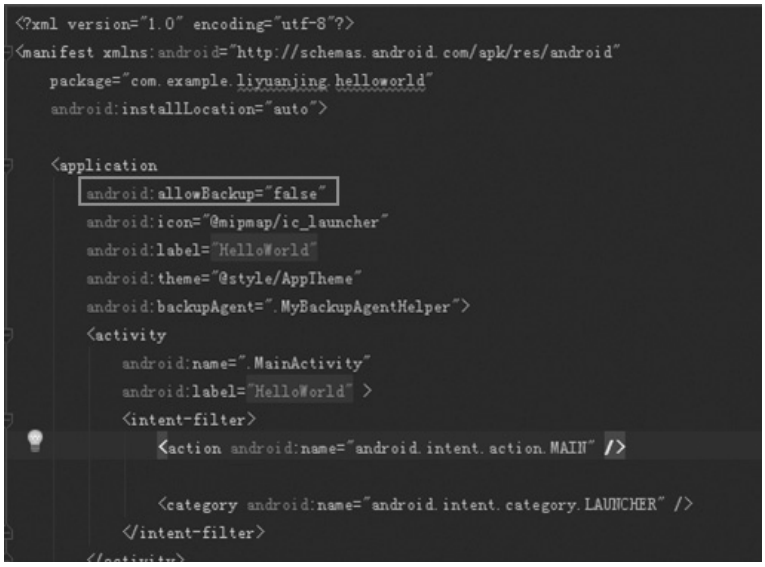

圖2　APP中allowBackup安全選項

㈢ 無法製作映像檔（Image File）進行檔案刪除還原

嫌犯在犯案後通常會進行滅證動作，這是人之本性；如果嫌犯不滅證，證物就沒必要以數位鑑識方法來進行刪除還原。在進行檔案刪除還原工作時，作法為先對儲存裝置進行完全複製產生副本，然後再以副本進行刪除還原等分析工作。對於電腦磁碟

來說，取映像檔是簡單的，而對於行動裝置而言，取出儲存裝置製作副本難度是非常高，尤其以目前平均4天上市一款智慧型手機的速度，每款手機介面、作業系統版本、特性及功能差異大，鑑識設備更新速度根本趕不上新機上市速度。因此行動裝置儲存裝置映像檔取證必須藉由電腦設備遠端連入操作，通常會先將行動裝置進行Root後，在行動裝置開機狀態下，以傳輸線連接電腦與行動裝置，然後再由電腦端下達指令進行映像檔取證；但此方法必須取得行動裝置最高權限前提下進行，否則是無法存取行動裝置磁區。

在許多性侵害案件中，嫌犯會在犯案過程中以行動裝置拍照、錄影，留下案件直接證據；但是當被害人報案後，嫌犯隨即將影片或照片刪除，這時候法院或地檢署即會將嫌犯所用智慧型手機或平板電腦送請鑑驗，這時如果以邏輯取證是達不到刪除還原效果，只有物理取證（Physical Extraction）才能進行檔案刪除還原。

要進行物理取證就必須對行動裝置系統進行更動，透過更動系統方式取得最高權限後，接下來才有辦法對取證重點磁區-使用者資料區進行映像檔製作，製作出來的映像檔在使用於刪除還原。

肆、因應行動裝置取證之修正與調整

一、數位鑑識原則之修正

㈠ 美國國家標準技術研究院（NIST）

美國國家標準技術研究院在2014年公布行動裝置鑑識準則[13]（Guidelines of Mobile Device Forensics，NIST-SP-800-101 Revision 1），這準則中介紹行動裝置特性、處理流程及方式等，其中在檢驗與分析一節中，提到行動裝置所擷取出來是遠較電腦鑑識為少，其中一因素就是受限於鑑識工具所能提供的擷取方式，因此在這準則中，建議使用連接線進行取證，但如果在不可行狀況下，可以選擇無線或其他破壞性方式進行，但是在方法提出時，應該評估其風險與影響；所以在不同案類有不同的取證重點，譬如說性侵害案件也許重點在有無涉案相關照片或影片，網路詐欺案件的重點也許在於網頁瀏覽歷史紀錄；在不影響取證關鍵證據之前提下，可適度修改取證方式，但是取證人員應將取證過程詳細紀錄並負有舉證責任，用來說明為何以該方式進行取證是最佳處理方式。

13 NIST SP-800-101，http://csrc.nist.gov/publications/PubsSPs.html#800-101

另外美國國家標準技術研究院也針對行動裝置取證設備訂定測試方法、參考資料、驗證標準等，針對各類數位鑑識設備或軟體進行試驗，依據數位鑑識工具及設備之功能、效能及正確性等進行測試審查，通過認證後，會將名單公布於網路上，其中包括Cellebrite UFED系列產品、XRY、EnCase Smartphone Examiner等著名行動裝置取證設備；這些通過名單中，各執法機關最普及之產品應是Cellebrite及XRY之取證設備，Cellebrite公司更於今（2016）年協助美國聯邦調查局破解iPhone手機而名噪一時[14]，但其方法係使用系統漏洞（類似駭客手法），這種方式亦可能改變原件造成證據一致性疑慮，是否能為國內院、檢、辯三方所接受仍待觀察。

㈡ 英國警察協會提出數位證據最佳實踐指南第5版

在原則1中，要求執法人員對於要呈上法庭之證物不可採取任何動作去改變證物，避免證物遭到汙染；於是常使用的方法是將智慧型手機置入隔離袋，但是放入隔離袋後，由於手機會不斷搜尋訊號，因此電量會不斷耗損，因而導致電量不足關機，為避免電量不足關機，有時會外接行動電源避免電量不足，但卻發現外接行動電源後，可能成為智慧型手機輔助天線或隔離袋無法完全隔離訊號之情形發生。另外如選擇將手機關機，有時又會遇到證物電源鍵損壞，有時可能因為關機或電池移除導致揮發性資料遺失情形；如果將手機維持開機狀態，手機內資料又可能由無線網路方式遠端進行刪除。

另外現在手機鑑識工具無法全面支援所有型號智慧型手機，因此常由鑑識人員以人工方式進行手動擷取，而此時原則2之適用與否又產生質疑，質疑鑑識人員手動方式擷取是否影響證據完整性。例如取整人員對相片進行擷取時，相片檔案的存取時間就改變，抑或對未讀簡訊進行讀取，讀取狀態也發生改變。又或有時為取得關鍵證據檔案必須在智慧型手機內部安裝第三方軟體，這樣做法嚴格說來也是破壞證物完整性，但卻是國外目前的使用方法，例如NewSecure（原名viaForensic）公司所出鑑識軟體viaExtract。

因此原則2著重在鑑識人員是否具有資格對證物進行分析，是否對所操作步驟能夠有足夠理由解釋與取證之關聯性，取證動作必定會對證物產生影響，就如同鑑識人員到現場勘查取證時，在採證同時也在破壞現場，但從沒有人去質疑現場勘查人員。

14 FBI支付巨額金解鎖iPhone手機,http://technews.tw/2016/03/24/israeli-forensic-firm-cellebrite-is-helping-fbi-to-unlock-iphone/

二、鑑識設備取證方法之調整

㈠ 行動裝置鑑識設備廠商Cellebrite

在Cellebrite官方部落格中，Cellebrite已於2016年4月20日[15]公開說明，Cellebrite設備UFED 5.0已具有暫時性Root行動裝置及將行動裝置內安裝的APP降版（downgrade）等取證方式，由此可見，全世界廠商對行動裝置取證已經採用別無選擇的選項，為取出關鍵性證據且不更動關鍵證據內容為前提下，已經允許有限度更動行動裝置證物原件；因此國內院、檢、辯三方如不接受合理範圍更動證物原件之概念，未來將無任何數位取證設備能夠在不變更元件前提下，對行動裝置進行關鍵性取證。

㈡ 行動裝置鑑識設備廠商XRY

XRY在過去針對iPhone手機密碼破解，在幾年前就已經採取切換至iPhone手機DFU（Device Firmware Update）模式下，利用手機漏洞進行密碼破解，而其原理有點類似越獄方式，來破解iPhone 4以下手機開機密碼。

由以上兩家行動裝置取證設備大廠之取證方式，不難看出資訊技術及鑑識設備在行動裝置取證方面，已經不得不採取適度更動原件之方式進行取證，為能在取證與不破壞關鍵證據間取得平衡，適度更動證物原件乃必要之作為。

三、法律見解之修正

國內目前對於數位證物仍處於過去電腦取證之觀念，禁止鑑識人員對行動裝置進行更動與改變，在國內沒有電子證據相關配套法令前提下，目前鑑識人員只能採最安全之取證方式，也就是盡量不引起爭議的取證方法-「不更動原件」，由鑑識設備進行標準取證，但這些國外生產之取證設備還是依循國內法律見解「不更動原件」舊式鑑識人員無法掌握。

世界各國於行動裝置之取證趨勢均朝向適度開放及調整，國內司法界或許可以思考如何在取證與證物完整性間取得平衡，最佳方式應當賦予責任給鑑識人員進行自主判斷，採用何種方式進行取證是最佳方式，並將詳細操作過程與步驟留下紀錄，供作第三方公正機關複驗。對於目前辯方一再於法庭提出的「不更動原件」取證方式，要適用於行動裝置取證實在有其困難，且世界各國對於行動裝置取證方式與標準程序已相繼修訂時，實不該再拿過去電腦取證原則套用於行動裝置取證上。

15 Cellebrite官方部落格宣布以降版及Root方式取證, http://blog.cellebrite.com/blog/2016/04/20/version-5-0-drastically-decreases-your-time-to-evidence-by-drilling-into-the-data-thats-most-crucial/

伍、結論與建議

行動裝置已成為現在各類犯罪最常見之證物，然而行動裝置與電腦類證物在硬體架構不同，在系統及運作方式迥異之前提下，法庭仍就將過去電腦取證之標準套用於行動裝置取證上，對實務運作上確有難處，對鑑識人員實有不公。

建議國內專家、學者、法界人士能夠針對數位鑑識之程序建立原則性規範，讓國內數位鑑識實驗室能有在此概念性原則下訂定標準作業程序，並將操作程序過程詳實記錄。這樣不僅讓取證人員不在受限於「不更動原件」之箍咒，讓鑑識人員可以在不影響證據完整性之合理範圍進行變動，也可滿足法院對取證之要求，依照不同案類取出關鍵性證據，作為法庭訴訟之用。

參考文獻

1. Paul Owen, Paula Thomas,2011, “An analysis of digital forensic examinations: Mobile devices verus hard disk drive utilizing ACPO & NIST guidelines”, Digital Investigation Vol 8
2. DCA. Murphy, 2009, “Developing Process for Mobile Device Forensics”, SANS Digital Forensics and Incident Response.
3. Anahita Farjamfar, Mohd Taufik Abdullah, Ramlan Mahmod and Izura Udzir,2014, “A Review on Mobile Device’s Digital Forensic Process Models.”, Research Journal of Applied Science, Engineering and Technology Vol8
4. Yunus Yusoff, Roslan Ismail and Zainuddun Hassan,2011, “Common Phase of Computer Forensics Investigation Models”, International Journal of Computer Science and Information Technology,Vol3
5. Fakeeha Jafari and Rabail Shafique Satti,2015, “Comparative Analysis of Digital Forensic Models”, Journal of Advances in Computer Networks, Vol 3
6. Bill Nelson,Amelia Philips, Christopher Steuart, “Guide to Computer Forensics and Investigation”, Cengage Learning,2009 Sep., 4 edition.