建構數位證據鑑識標準作業程序與有效性之研究 -以智慧型手機為例

吳穩男
華梵大學資訊管理學系
Email:winwu@ms1.hinet.net

林宜隆
中央警察大學資訊管理學系
Email:Paul@mail.cpu.edu.tw

張志宗
華梵大學資訊管理學系
chang.pie@gmail.com

隨著資訊科技進步，社會大眾愈來愈依賴資訊技術從事社會行為，但伴隨著的是資通安全及倫理、素養等問題卻層出不窮。研究指出 2009 年全球智慧型手機出貨達 1.83 億支，年增 28.2%。其強大的軟硬體功能帶動各層面的廣泛運用，進使智慧型手機犯罪活動激增。然手機屬於私人物品，並受隱私權保護，故此類的犯罪偵辦與傳統犯罪型態存在著極大的差異。鑑於此，本研究探討英國國家專家執法中心之手機調查指導方針與國內學者林宜隆提出之數位證據鑑識標準作業流程，並優化此程序對智慧型手機之數位證據蒐證方式與探討其法庭上的數位証據之有效性與合法性，使鑑識人員能夠運用此鑑識程序即可完成鑑識工作，提高數位證據在法庭上之證明力及公信力，作為日後法官審判之依據。

關鍵詞—資訊技術、資通安全、電腦鑑識、數位證據、智慧型手機

一、前言

(一) 研究的動機

隨著科技不斷的進步，電腦、通訊網路帶給人類工作、生活的巨大的改變及衝擊，然而隨著資訊的便捷而來令人擔憂的資通安全與犯罪問題快速成長，同時，伴隨電腦、電信及網路為犯罪標的及工具的各類犯罪活動也如雨後春筍般的滿地遍生，各類入侵、攻擊手法層出不窮，故如何打擊和防治資訊犯罪及資安事件，儼然已成為司法界亟待解決的新難題。

近來國內智慧型手機蓬勃發展，據拓墣產業研究所預估，2009 年全球智慧型手機出貨量可達 1.83 億支，年成長率 28.2%[19]。並就 Gartner 統計，2009 年第二季，全球手機銷售量為 2.861 億支，較去年同期衰退 6.1%；但其中智慧手機銷售量為 4,000 萬支，較去年同期成長了 27%，是行動通訊市場的增長最快的產品線[20]。其強大的軟硬體功能帶動各層面的廣泛運用，例如即時高品質的影像傳輸，以及更強的網路功能[30]。

智慧型手機存有豐富的個人資訊，具備高度機動性且強大的軟硬體功能帶動各層面的廣泛運用，進使智慧型手機犯罪活動激增[15]。然手機屬於私人物品，其儲存內容並受隱私權保護[13]，故此類的犯罪與傳統犯罪型態存在著極大的差異。由於智慧型手機犯罪的證據不若傳統犯罪來得明確，且數位證據具有高度隱匿、易消失及蒐證不易的特性，因此，必需制定一套標準合宜之電腦鑑識及數位證據蒐證方式，明確告知智慧型手機犯罪偵查及鑑識人員，蒐證時該依循的標準為何？並提升網路犯罪偵查及電腦鑑識的品質，將是刻不容緩的工作。

(二) 研究的目的

電腦鑑識(Computer Forensics)這個名詞是一九九一年波特蘭的國際電腦專家協會（International Association of Computer Specialists，IACIS）首次提出[18]，電腦鑑識主要是在處理電腦有關的數位證據之保留、識別、萃取、記錄及解讀，以確保案件現場電腦物證及數位證據之原貌，使鑑定過程合法，鑑識結果具備完整性[27]，並作為法院審理犯罪案件的重要參考依據，最重要的目的就是能從「數位證據」

中認定嫌犯是否有罪。以目前我國的司法環境來觀察，由於尚未建立一套標準的智慧型手機之蒐證程序，使得數位證據的證據能力及證明力不足，以致於讓法官無法由蒐證的數位證據中直接判斷，可能導致法庭上之爭議。本文探討英國國家專家執法中心（National Specialist Law Enforcement Centre, NSLEC）之手機調查指導方針（Mobile Phone Examination Guidelines）[15]與國內學者林宜隆提出之數位證據鑑識標準作業流程[2]，並優化此程序對智慧型手機之數位證據蒐證方式與合法性，讓鑑識人員能夠運用此鑑識程序即可完成鑑識工作，並於法庭上，可補強數位證據能力及證明力，輔助法庭上證據的佐證能力，最終目的在協助執法單位對於數位證據鑑識、擷取及分析時之遵循依據。

二、文獻探討及理論基礎

(一) 智慧型手機功能探討

手機是現代人隨身必備的數位產品，而且也是最具親密性與私密性的個人通訊裝置。隨著相關技術的成熟，消費者對手機功能的要求越來越高，現在彩色螢幕加上相機鏡頭也只算基本規格，除了更輕、更小，人們還希望手機有更多、更好用的功能[29]。因此，結合手機、PDA、MP3player 與 GPS 設備功能的智慧型手機，便成了新一波高階手機產品的熱門發展趨勢[12]。

表一 資策會對於智慧型手機之定義

項目	定義
外觀	輕、薄、短、小，易於攜帶。
基本功能	具備數據與語言之無線通訊功能，且皆為內坎式而非外加之模組。
數據通訊	1、 具備 PIM 功能，其中包含 data book(行程表)、contact(通訊錄)、to do list(工作表)、memo(記事本)、hotSync(與電腦同步)等功能。 2、 可連接 Internet、收發 E-mail。
語音通訊	需具備內崁式語音通訊功能。
輸入方式	任何營形式，不限於觸控式、按鍵式或語音輸入等。
處理器與作業系統	擁有多工的崁入式微處理器與作業系統。

就資策會對智慧型手機（Smart Phone）的定義，廣泛地來說，是指在開放性的作業系統環境下，整合了個人資訊管理功能（PIM）和行動通訊功能的一種手持式裝置。目前各界對於智慧型手機並未有明確且統一的定義，但有一個共通的準則，即必須具備語音通訊與數據通訊之功能，且其中應以語音功能為主（表一）[9]。近年來智慧型手機更結合家庭無線區域網路（Wireless Local Area Network, WLAN）設備，包括 WLANAP、WLANCard、Wi-FiVoIPPhone、WebStation、E-mailStation 等[12]，享受網際網路（Internet）所提供便利之商務應用。

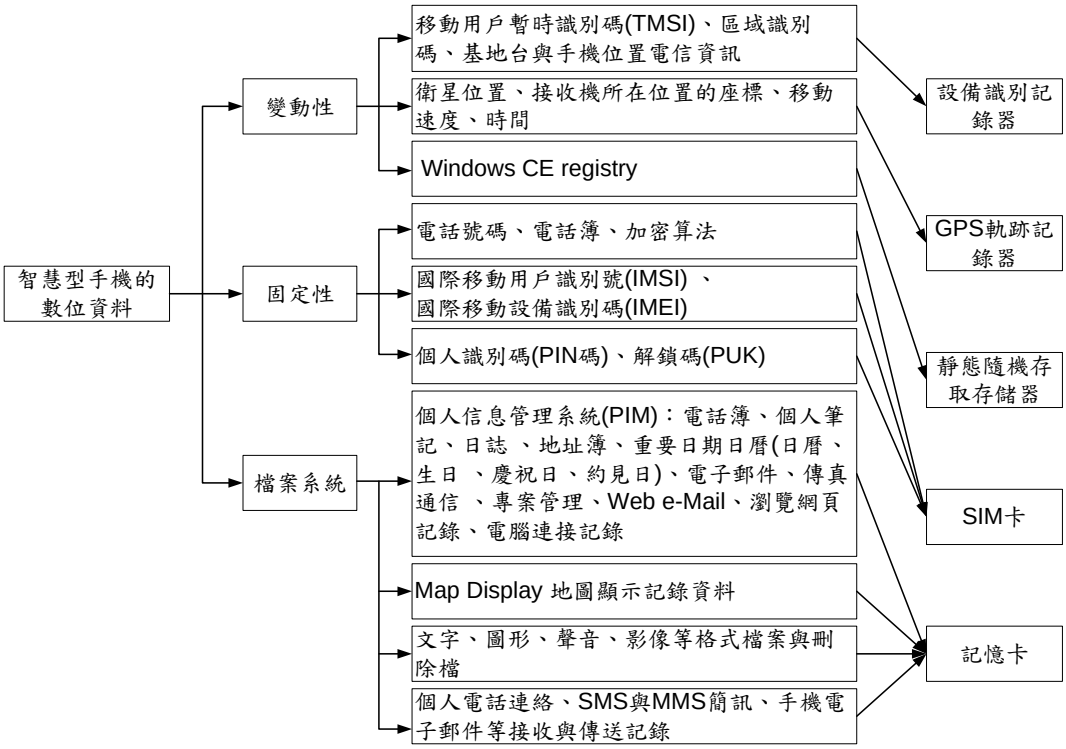
綜合上述，智慧型手機外觀類似平板電腦，可以讓不會電腦的使用者輕易瀏覽網頁，減少接觸網際網路的障礙與負擔，再加上強大的作業系統，智慧型手機就等於擁有一台筆記型電腦（圖一），那其運用空間就可以變得無限寬廣了[11]。

圖一 智慧型手機組成元件及功能組合圖

(二) 智慧型手機之數位資料探討

就上小節所論，智慧型手機的強大功能可完成各項私人資料處理，例如利用瀏覽器（Browser），可以連接網頁，取得相當豐富的生活資訊，例如停車場、餐廳、火車時刻等生活情報；而未來電信業者將整合 GPS 的定位功能可以提供安全性服務，諸如掌握子女安全、汽車導航；更進一步 GPS 搭配 Internet，可以隨時得到使用者所在位置週邊的加油站、停車場、百貨公司等資訊。如此一來，智慧型手機將不再只是單純的通話工具，而是智慧行動生活裡重要的資訊中心 [11]，其過程中保留很多數位資料於智慧型手機儲存元件內，例如 SIM 卡(Subscriber Identity Module)、設備識別記錄器（Equipment Identity Register，EIR）、GPS 軌跡記錄器（GARMIN）、靜態隨機存取存儲器（Static Random AccessMemory，SRAM）、記憶卡（如 Secure Digital-SD/SDHC；CompactFlash-CF；Memory Stick-MS；microSD-TransFlash；miniSD；MultiMedia-MMC；SmartMedia-SM/SMC）等。

就學者林宜隆提出數位資料分為三個部分，分別為變動性數位資料、固定性數位資料及檔案系統之數位資料[2]。本研究參照圖一之智慧型手機組成元件及功能組合圖，由兩者可推展出智慧型手機之數位資料分類（如圖二）[16,10,1]。



圖二 智慧型手機的數位資料分類

(三) 智慧型手機之資訊隱私探討

隱私權被視爲一種人格權並受到法律保護，是現代法律制度的產物。隨著資訊時代的來臨，人們越來越需要在紛亂蕪雜的環境中保留自己內心世界的安寧，隱私權也就逐步成爲人們的一種基本需求。今天，隱私權已經成爲公民保持人格尊嚴和從事社會活動所不可缺少的條件之一。泄漏並宣揚他人隱私，給他人聲譽造成不良影響的，加害人要承擔名譽侵權的法律責任。情節惡劣、後果嚴重的，還有可能構成犯罪受到刑罰制裁 [6]。

然智慧型手機屬於私人物品，其儲存內容並受隱私權保護，所以智慧型手機的犯罪偵查與傳統犯罪偵查存在著極大的差異。就智慧型手機擁有者於未被確認有犯罪行為或可逮捕之嚴重罪行嫌犯，及沒有擁有者審查電話書面同意等，智慧型手機仍屬私人物品[15]，偵查、數位與刑事鑑識人員對執行手機調查時，其搜查證據行為之合法性將十分重要。

如案例一（2008 年 9 月），某中部某私立高中以防偷拍等理由，要求學生簽切結書，讓校方得搜查學生手機內容，已侵害學生受憲法第廿一條保障的「隱私權」[21]；案例二（2006 年 9 月），年美國弗吉尼亞州的一家公司對 10 部廢棄的手機進行安全測試，結果顯示，包括愛人間的交流、公司的營利計畫，甚至一些銀行賬目和密碼等資訊，幾乎都能準確恢復。這意味著，已經清空的手機簡訊、通話記錄以及通訊錄都有可能被他人知曉，機主則毫不知情地洩露了自己的隱私或商業機密。據美國法律要求如沒有擁有者書面同意，私自恢復他人已刪除資料將涉嫌侵犯隱私權。恢復他人手機資訊大都存在目的性，若資訊被有意或無意散佈造成機主損失，資料恢復者和要求恢復者（非擁有者）有可能承擔共同責任。應慎重使用數據恢復手段，恢復後資料提供和使用都應遵循法律規定[22]。

綜合上述，以目前我國的司法環境來觀察，由於尚未建立一套標準的智慧型手機之蒐證程序，使得數位證據的證據能力及證明力不足，以致於讓法官無法由蒐證的數位證據中直接判

斷，可能導致法庭上之爭議。

(四) 智慧型手機之犯罪行為與偵辦合法性探討

近年來，我國智慧型手機發展日益普及，其手機功能之運用已成為國民日常生活不可或缺的一部分，但智慧型手機運用的偏差行為亦層出不窮。例如利用手機散播簡訊公然誹謗他人名譽、散播自殺方法、散佈猥褻圖片、定位追蹤位置、濫發商業電子郵件、從事電信援交與電信販毒等犯罪行為。於刑案上則利用手機進行簡訊詐欺或恐嚇取財與綁票勒索之聯絡等犯罪工具[8]。

綜合上述犯罪行為，可以得到以下幾項結論（1）犯罪者都是以手機連繫方式要求被害人支付錢財或進行誹謗攻擊。（2）手機的通聯紀錄是這幾件犯罪案例偵查與破案的重要關鍵（3）講求時效與品質的犯罪偵查資料蒐集方式是另一個破案的重要因素[14]。

手機的犯罪偵查作業中，有些通聯紀錄的資料對於檢察官的犯罪證據蒐集及法官的犯罪行為認定，可以提供具體的舉證成效，我們將這些資料視為「具體性的舉證資料項目」。犯罪者透過手機進行犯罪行為時，通聯紀錄所記載發話手機的發話日期、發話時間、通話秒數、IMEI 及發話基地台識別碼等項資料，具有高度的犯罪舉證效果。其中發話日期、發話時間及通話秒數在通聯紀錄中是記載實際的資料，而 IMEI 及發話基地台則是以代碼的方式記錄，從嫌犯發話手機的IMEI 代碼可以查出嫌犯使用手機的廠牌及型號，從接收嫌犯發話手機的基地台可以查出嫌犯發話的區域範圍；犯罪者透過手機進行犯罪行為時，交換機也精確的記錄了此通犯罪手機的發話日期、發話時間、通話秒數、發話手機的廠牌與型號及發話時所處的區域範圍等資料，這些犯罪的具體資料，日後都將成為檢察官進行犯罪行為認定與判刑的過程中，非常重要且具體的舉證項目[14]。

綜合上述，搜索（Search）及扣押（Seizure）是刑事訴訟法中證據保全之重要手段及程序之一，且扣押是搜索之接續行為但未必是必要行為。我國刑事訴訟法於民國九十年對搜索程序作了大幅度之修正，除認搜索程序需依法官保留原則（令狀主義－刑事訴訟法第一百二十八條第三項、第一百二十八條之一）外，亦對其例外（刑事訴訟法第一百三十條至第一百三十一條之一）之相關規定。惟刑事訴訟法之搜索對人身及隱私權均有相當之侵害，我國刑事訴訟法第一百三十二條即規定搜索不得逾越比例原則[23]。

就美國為了確保刑法上被告（嫌疑犯）各種人身保護，對於政府行使政府權力的權限，予以重重之限制與束縛。此乃導因有兩個很重要的理念來維護個人權益，一為「正當法律程序」（Due Process）；另一為隱私權（Right of Privacy）[28]。「正當法律程序」使美國警察、檢察官及法院的行為皆能依法行事，而非全憑個人之喜惡為斷。而隱私權是犯罪嫌疑犯所得享有各種重要權利中的第一種權利[23]，在偵查犯罪的過程中，警察的權力受到極嚴格的限制，不可以單依其權限而任意搜索，換言之，任何人的隱私權皆為法律所保護，而不容公權力專段的侵入。

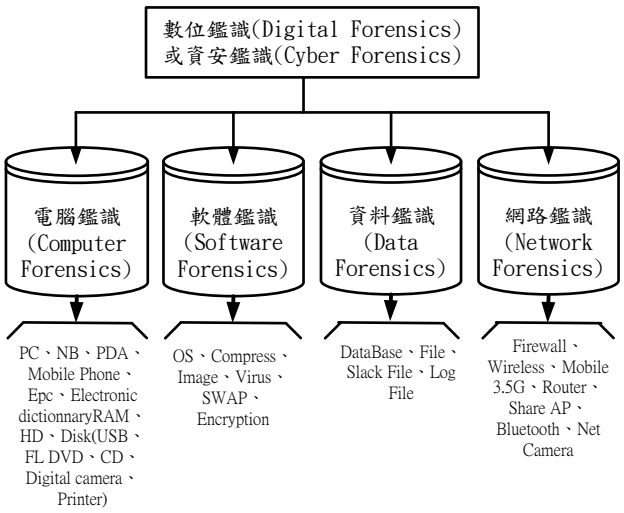
綜合上述，「正當法律程序」對智慧型手機之犯罪偵查與資料蒐集方式有其重要性，故建立一套具備合法性之數位證據蒐證程序是有其必要。其可讓鑑識人員能夠運用此鑑識程序即可完成鑑識工作，並於法庭上，可補強數位證據能力及證明力，輔助法庭上證據的佐證能力，最終目的在協助執法單位對於數位證據鑑識、擷取及分析時之遵循依據。

(五) 數位鑑識

電腦鑑識的觀念源自於刑事鑑識，可謂鑑識科學的分支，只是鑑識的標的物不同，電腦鑑識需要大量資通科技來加以輔助，用以分析我們無法實際觸摸到的電子記錄[24]。正因如此，電腦鑑識需要更為完善及可驗證的證物保護方式，來保護鑑識前後的證據不被竄改，使得經鑑識分析後的證據更可信及具有法律地位，以利在法院審理時可以作為判決之依據[4]。電腦鑑識分兩部分，一為現場的電腦鑑識，一為實驗室的鑑識工作。現場鑑識是保留當時的案發情況並找出可能的蛛絲馬跡，以利犯罪偵查，然後證物送證物室保管或送專業鑑識實驗室進行鑑識分析，最後將

結果送交負責偵辦的司法單位，以提供相關的偵查協助 [25]。

就上述所論，學者林宜隆提出數位鑑識所涵蓋的範圍不單單僅僅限於電腦鑑識、網路鑑識，凡是以數位方式儲存的相關設備都包含在數位鑑識的領域中，包括：電腦、網路設備、個人數位助理、行動電話、數位相機、記憶卡等數位設備，故亦稱資安鑑識（Cyber Forensics），其應包含電腦鑑識（Computer Forensics）、硬體鑑識（Hardware Forensics）、軟體鑑識（Software Forensics）及網路鑑識（Network Forensics）等(如圖三)，故舉凡與數位資料有關之鑑識皆屬之，故提出數位鑑識之觀念。數位鑑識必須以周延的方法及程序保存、識別、抽取、記載及解讀數位媒體證據與分析其成因之科學[5]。其目的是保留數位證據的完整性和正確性，及建構資訊安全事件發生的過程，以作為資訊安全事件及司法單位調查判決電腦網路犯罪之依據 [3]。



圖三 數位鑑識(Digital Forensics)

(六) 數位證據

傳統證據依我國刑事訴訟程序中，係根據證據來證明被告是否犯罪，而所謂證據，係指：在刑事訴訟程序中用來認定事實之資料。證據的分類方式甚多，其中較重要者為將其分為：（1）人證（2）物證（3）書證等三類證據[2]。

學者 Casey 定義數位證據為電子儲存媒介中所存放的資料若足以構成犯罪要件或者具有相關的之電子資料[16]，如：聲音、文字、影像及圖片等等，即可稱之為電腦證據或電子證據。國內林一德與黃景彰教授觀點則認為，犯罪者從事犯罪活動，利用電腦或網路所產生或者傳送 0 與 1 等數位符號、然後所組成的特定意義，而且這些特定意義具備可做為法律上犯罪事實之認定，即稱為數位證據[11]。所以數位證據與傳統證據之性質截然不同、不若傳統證據般有形體、可觸摸的到的，它本身可能屬於電磁紀錄，以電波或電磁方式儲存在電子媒體上；由於這些證據內容是我們肉眼直視看不見的，必須由電子設備加以讀取、分析顯示，轉換成人類能讀、了解的內容如：文字、聲音及影像。

我國刑法對於「電磁紀錄」的定義，電子簽章法對於電子文件之相關定義為：「電子文件：指文字、聲音、圖片、影像、符號或其他資料，以電子或其他以人之知覺無法直接認識之方式，所製成足以表示其用意之記錄，而供電子處理者。」，另依據刑法第二百二十條第三項規定：「以電子、磁性、光學或其他相類似之方式所製成，而供電腦處理之紀錄，稱之為電磁紀錄。」，目前在世界各國及我國法律目前都尚未對數位證據有正式的定義，只有對電子紀錄、電磁紀錄及電子文件加以定義，使得數位證據的定義非常模糊，本研究中，根據我國法律之定義及學者的定義，將其定義為藉由電腦或網路設備儲存或傳送可供證據用，稱之為數位證據，即包括電子文件、電子紀錄及電磁紀錄。

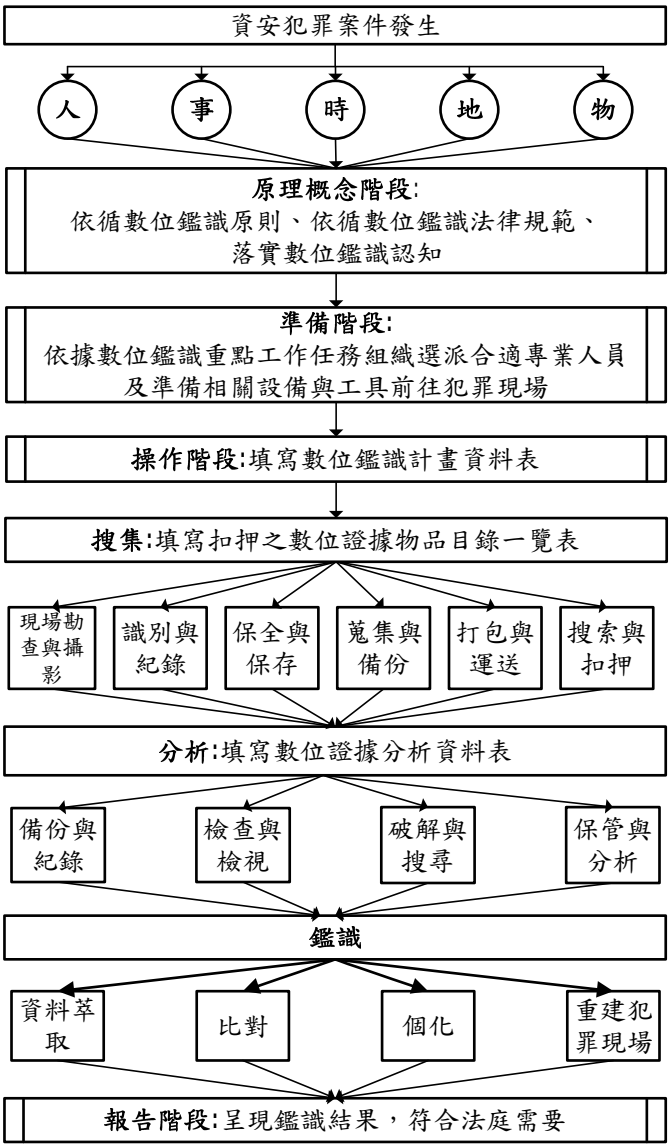
三、智慧型手機數位證據鑑識標準作業程序之建構

本研究將探討英國國家專家執法中心手機調查指導方針整理分析與歸納，以及參考國內學者林宜隆所提出數位證據鑑識標準作業程序，並優化此程序對智慧型手機之數位證據蒐證方式、安全性與合法性，建構智慧型手機之數位證據鑑識標準作業程序。

(一) 數位證據鑑識標準作業流程

數位證據鑑識標準作業流程，可分為原理概念階段、準備階段、操作階段及報告階段。其中以操作階段最為重要，操作階段又分為蒐集、分

析、鑑識（如圖四）。



圖四 數位證據鑑識標準作業流程（林宜隆）

（1）原理概念階段

1.1 法規

數位證據的取得要遵循合法、真實的原則，當事人不得以非法侵入他人電腦資訊系統的方法獲取證據；證據取得的途徑必須以立法的形式規定取得數位證據的程序及許可權。

1.2 原則

主要原則有以下七點：

1.2.1 儘早蒐集證據，並保證其沒有受到任何破壞，即在處理時，必須確保智慧型手機或其它儲存媒體上的資料保持在原始的狀態，內容不得修改。

1.2.2 必須保證「證據的連續性」，即在證據被正式提交給法庭時，必須能夠說明在證據從最初的獲取狀態到法庭上出現狀態之間的任何變化，當然最好是沒有任何變化。

1.2.3 對於數位證據的任何稽核資料、紀錄或分析的處理過程，應建立處理方法、紀錄與保留結果，就算委由公正第三方進行相同的處理程序，其所得結果應相同。

1.2.4 在特殊情況下，如果需存取原始數位證據的資料，則必需由有能力處理的專家，進行存取的動作，並對其處理的動作予以說明及適當解釋。

1.2.5 應當全程紀錄及拍攝蒐集、分析及鑑識等過程。

1.2.6 存放和使用存有拷貝證據的軟碟、光碟、磁帶、硬碟、隨身碟、儲存卡等時應當注意安全，並遠離強磁場、水、火等，使用時應注意病毒的檢測。

1.2.7 使用證據複製品進行分析、調查及鑑識的工作。

（2）準備階段

本階段的主要工作是做一些鑑識前的準備工作，並蒐集相關資料，是為操作階段各程序執行的預作準備，以下為其步驟：

2.1 蒐集犯罪對象基本資料

根據犯罪的類型，並利用已掌握的情況分析可能作案的人員，若案情需要也可訪談相關人員，並規劃鑑識執行的策略。

2.2 決定搜索地點、對象與時間

根據犯罪的類型，決定搜索地點、對象與時間，依據蒐集嫌犯資料後，決定搜索地點和時間。

2.3 工具的準備

必需準備電腦軟硬體規格的參考手冊、犯罪工具程式的參考手冊及破解電腦。

2.4 人員的專業性

對於一些鑑識工具的使用，鑑識人員必須具備專業性，也就鑑識人員應該考取相關鑑識證照或認可，才不致於在鑑識過程中遺漏寶貴的數位證據，甚至是破壞掉數位證據。

2.5 技術勤前教育

在每次出任務前，必須針對鑑識人員進行進一步的說明，說明搜索任務、項目，並檢查軟硬體及工具是否準備齊全，以避免一些意外狀況發生。

（3）操作階段

3.1 蒐集程序

依據圖二智慧型手機的數位資料分類瞭解，在蒐集資料這個階段將數位資料分為三個部分，分別為變動性數位資料、固定性數位資料及檔案系統數位資料，在各個部分整理出何種數位資料該用何種工具來蒐集。

3.2 分析程序

依據圖二智慧型手機的數位資料分類瞭解，在分析資料這個階段將分析資料分為六個部分，分別為設備識別記錄器、GPS 軌跡記錄器、靜態隨機存取存儲器、SIM 卡、記憶卡及其他，在各個部分整理出何種數位資料該用何種工具來進行分析。

（4）鑑定程序

在鑑定這個階段將鑑定分為五個部分，分別為資料萃取、比對及個化、重建犯罪現場、報告撰寫及法庭參考證物，在比對及個化整理出數位資料該用何種工具來進行鑑識。

(二) 數位証據於法庭上之有效性分析

本小節將探討美國司法上之提供數位證據敗訴案例，以分析數位証據於法庭上之有效性需具備那些要求。

案例 1（美國訴 Turner 案，1999 年），執法警官獲得了被告的同意對其家進行搜查，以便尋找與被告鄰居遭受性攻擊相關的証據。在搜查期間，一名調查員察看了 Turner 的電腦，發現了兒童色情製品。於是 Turner 又被起訴擁有兒童色情製品，但是 Turner 並未同意對他的電腦進行搜查，因此他說以此為由提出查禁証據的聽証會，以排除這些數位文件作為証據，並認為探員把標有“ young ”或“ young with the breasts”字樣的檔案總結為性侵犯（授權搜查的特定對象）的証據是顯然不合理的[16]。由本案例中瞭解調查員在搜查、提取數位證據時，於事前準備工作時應提高其”適法性”之概念。

案例 2（密歇根川訴 Miller 案，2002 年），2000 年電子郵件和美國線上即時訊息(AOL Instant Messages)提供了強有力的證據指控 Sharee Miller 陰謀殺害了她的丈夫，並唆使已經認罪的凶手(Jerry Cassaday)自殺，她曾經借助 Internet 勾引過他。米勒通過偽裝成她的丈夫向凶手發送無禮的信息，小心謹慎地控制了殺手對她丈夫的感覺。在這種情況下，儘管能夠進行這樣的線上交談，但是於美國線上即時訊息所蒐證之數位證據其”可用性”受到了質疑[16]。

案例 3（美國訴 TANK 案，2002 年），美國訴 TANK 是與 Orchid/Wonderland 俱樂部相關的調查中案件，被告爭辯 Internet 聊天記錄的真實性和相關性不足以成立。被告爭辯的觀點之一是聊天記錄能被輕易地修改。控方使用了大量證據來證實記錄是真實的。但法庭堅持認為打印出來的聊天室討論記錄可能是依照證據製造出來的，這些證據能夠顯示這些討論是如何準備的、表示會談的精確性以及它們與被告的聯繫關係[16]。此案例有重大的意義，因為它是第一個涉及在線聊天記錄真實性的案件之一。但是，關於 Internet 聊天記錄的真實性、完整性和可用性仍有一些尚未解決的問題[16]。例如在 IRC（Internet Relay Chat）上，除了聊天頻道視窗外，在某個 IRC 客戶端的其他區域內，如狀態視窗，以及在私人聊天或硬碟檔案存取的交流（mIRC's File Server, fserve）視窗中，可能有非常重要的資訊。既然對一個調查員而言，不可能同時瀏覽每一個視窗，因此必須依靠更多客戶端的記錄，來證實所提交的證據是真實、完整與可靠，並能夠彌補文件上的不足。

由案例 2 與案例 3 瞭解調查員應提交具有“真實性”之數位証據，並於搜尋、保存證據時

應使具其”可用性”，於分析、檢查証據過程時使其具有”完整性”。綜合上述論點，有效之數位證據應包括以下四點（如表二）：

（1）機密性（Confidentiality）

數位證據處理時，應需妥善正確處理數位證據於程序中，並只讓合法使用者取得數位證據與應具備安全保護亦可防禦存取式攻擊，所有的數位證據都皆為涵蓋之範圍。

（2）適法性（Compliance）

數位證據處理過程與鑑識工具的使用為電腦鑑識領域中是相當重要的一環，並非所有的數位證據處理過程與鑑識工具都可以使用，要考慮到的是該數位證據處理過程與工具軟體於法庭上的適法性問題。避免違反任何法律、法令、法規或契約義務，以及任何安全要求[17]，導致數位證據之無法使用。此處也對應學者林宜隆提出之完整性(其方法與原則為在不改變或破壞證據的情況下取得原始證據) 觀念是相同的。

表二 數位証據法於庭上之有效性分析

數位証據之鑑識項目	各國學者鑑識程序觀點	數位証據之有效性
證據處理步驟	證據鑑識程序	機密性
事前準備	法規、原則、準備工作	適法性
蒐集資料	搜尋、保存、復原	可用性
分析資料	分析、檢查	完整性
鑑識報告	鑑定、呈現結果	

（3）完整性（Integrity）

數位證據處理程序中之保存、分析、鑑識時要能確保數位證據的正確性，讓數位證據可使執法相關者可信任其數位證據是正確的，且沒遭人修改與污染。此處也對應學者林宜隆提出之一致性(在不改變證據的情況下進行分析)與完整性(其方法與原則為在不改變或破壞證據的情況下取得原始證據)觀念是相同的。

（4）可用性（Availability）

數位證據處理程序中之準備工作、文件紀錄、收集之工具與方法需維持在可用與合法的狀態，無論處於正常或非常之情境下，皆應保證其蒐證之數位證據為有效與可進行鑑識。

綜合上述，數位証據於法庭上之有效性應具備適法性、可用性與完整性等要求，並以機密性於數位證據處理之事前準備、蒐集資料、分析資料與鑑識報告各個階段保護數位証據安全與不受污染。如此將可提高數位證據在法庭上之證明力及公信力，作為日後法官審判之依據。

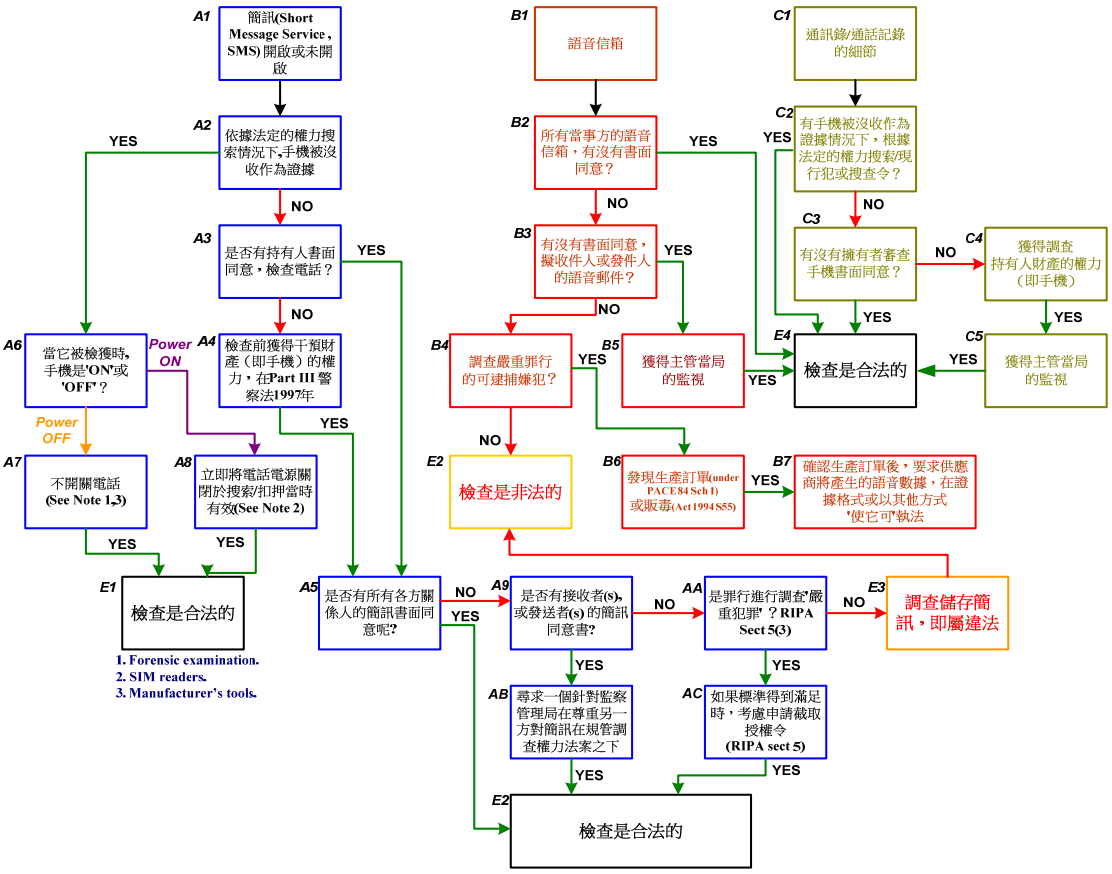
(三) 手機的數位証據之合法性

英國國家專家執法中心（National Specialist Law Enforcement Centre，NSLEC）主要執行監測培訓、機密人力情報來源處理、高科技犯罪技能分析、法律方面的監控、跨機構的研究和開發、跨機構的研討會和會議等任務。見於手機屬於私人物品，其儲存內容並受隱私權保護。故於 2004 年發表手機調查指導方針（NSLEC Mobile Phone Examination Guidelines），提供偵查、數位與刑事鑑識人員對執行手機調查時，數位證據蒐集、分析、鑑識之合法性的依據[15]，此手機調查指導方針本研究整理如圖五所示。

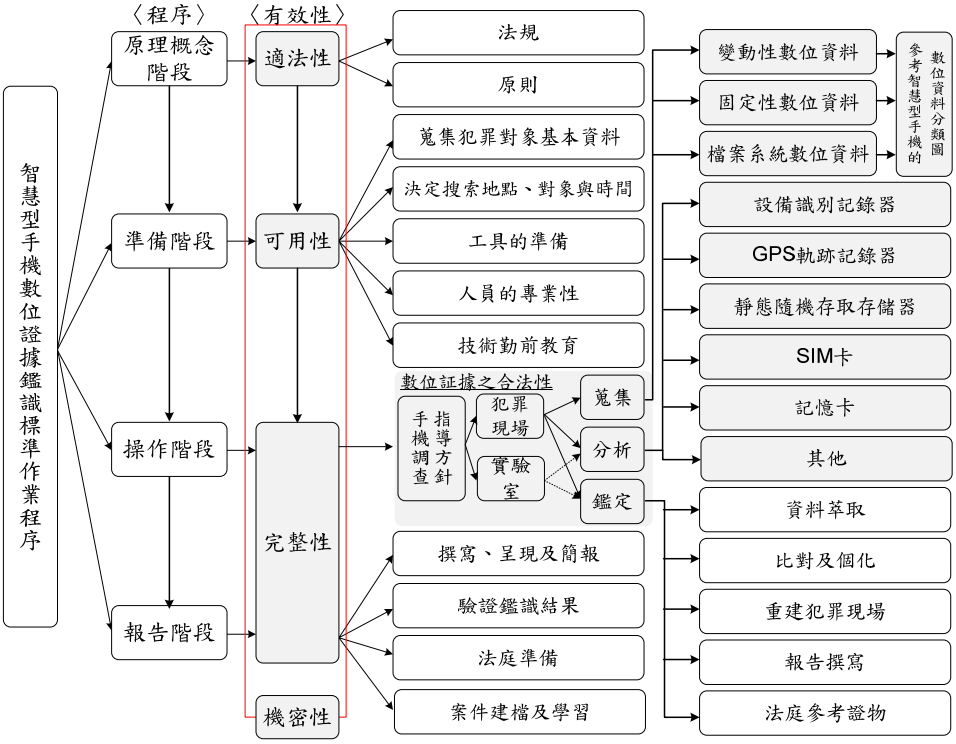
如圖五發現手機偵查與數位證據蒐集、分析與鑑識過程內藏有許多注意事項，考驗手機分析與鑑識人員舉證的能力與責任，例如標號”B2 所有當事方的語音信箱，有沒有書面同意？”等皆是。根據國內法律，偵查與鑑識單位仍須履行刑法 306 條、刑法 133 條、刑法 315 條、刑法 315-1 條、民法第 195 條，與未來將通過之個人資料保護法之法律要求，確保所有鑑識進行的合法性。並建議有適當的機關進行稽核，以充分理解於此期間之鑑識有沒有違反現行法例與手機偵查與數位證據蒐集、分析與鑑識過程之合法性。

(四) 智慧型手機數位證據鑑識標準作業程序

本研究綜合各節所述，整理提出智慧型手機數位證據鑑識標準作業程序（如圖六所示），清楚說明數位證據處理之事前準備、蒐集資料、分析資料、鑑識報告各個階段應做何工作項目與兩相對映機密性、適法性、可用性與完整性等數位證據有效性之要求。並依此鑑識標準作業程序建議偵查、數位與刑事鑑識人員對執行手機數位證據調查時，該於何處搜尋、保存與復原等，提供一個依循的標準。



圖五 手機的數位證據蒐集、分析、鑑識之合法性



圖六 智慧型手機數位證據鑑識標準作業程序

四、建議與結論

本研究中整理電腦鑑識科學領域專家對於電腦數位鑑識的定義，瞭解智慧型手機數位鑑識領之概念及意義，並發現手機偵查與數位證據蒐集、分析與鑑識過程內藏有許多許多注意事項，考驗手機分析與鑑識人員舉證的能力與責任，例如圖五標號"B2 所有當事方的語音信箱，有沒有書面同意？"或"A3 是否有持有人書面同意，檢查電話？"等皆是。

綜合學者林宜隆的意見與相關手機調查指引之探討，提出智慧型手機數位證據鑑識標準作業程序。並說明進行每項鑑識步驟之目的、執行那項程序與手機偵查與數位證據蒐集、分析與鑑識過程之合法性，提供給偵查、數位與刑事鑑識人員一個依循的標準。並進一步分析司法案件，瞭解數位証據於法庭上之有效性應具備適法性、可用性與完整性等要求，並以機密性於數位證據處理之事前準備、蒐集資料、分析資料與鑑識報告各個階段保護數位証據安全與不受污染。但就此智慧型手機數位證據鑑識標準作業程序仍須加強以下幾點，(1) 專業的數位鑑識實驗室建置；(2) 加強警察機關智慧型手機偵辦技巧；(3) 建立國內智慧型手機偵辦標準指引。如此才能真正達到提高數位證據在法庭上之證明力及公信力，作為日後法官審判之依據。

五、參考文獻

[1] 林一平，"行動電話及數據網路管理"， 維科出版社，1999.

[2] 林宜隆，"網路犯罪理論與實務-網際網路與犯罪問題第三版"，中央警察大學出版社，2009.

[3] 林宜隆、朱惠中、張志汞，"數位證據鑑識標準作業程序與案例驗證之建構—以 Windows XP 系統為例"，2008 數位科技與創新管理研討會，華梵大學資訊管理學系，2008.

[4] 吳豐乾，"基值於 Windows 系統的電腦鑑識工具之研究"，樹德科技大學資訊管理研究所碩士論文，2004.

[5] 吳穩男、林宜隆、朱惠中、張志汞，"數位證據鑑識標準作業程序與案例驗證之建構—以 Linux/Unix 系統為例"，2008 聯合國際研討會－第十屆「網際空間：資安、犯罪與法律社會」學術暨實務研討會，華梵大學資訊管理學系，2008.

[6] 周健，"資訊時代隱私權的法律保護"，重慶圖情通訊，第 4 期，2001.

[7] 陳志誠、蔡旻峰，"數位鑑識實驗室建構標準之芻議"， 2004 第六屆「網際空間:資訊、法律與社會」研討會，大同大學資訊經營學系，2004.

[8] 陳順和，"行動電話簡訊詐欺犯罪問題之成因與對策探討"，透視犯罪問題，第 2 期，2003.

[9] 陳連福、李孟軒，"智慧型手機結合彩色條碼辨識技術應用於互動式多媒體行動商務商品展示介面設計之探討"，2007 電子商務與數位生活研討會論文集，崑山科技大學空間設計系，2007.

[10] 陳韋哲，"POCKET PC STYLE：POCKET PC 2002 徹底活用"，金禾出版社，2003.

[11] 陳明秀，"智慧型手機對電腦媒介溝通之影響初探"，台灣圖書館管理季刊，第 3 卷，第 2 期，2007.

[12] 曾建榮，"不單純的手機智慧行動生活裡的資訊中心"，技術尖兵，第 113 期，2004.

[13] 楊智傑，"資訊法(增訂二版)"，五南出版社，2008 年 03 月 31 日.

[14] 賴森堂、林宜隆，"行動電話犯罪偵查資料探勘與量測模式"，中央警察大學『資訊、科技與. 社會』學報，第 1 卷，第 1 期，pp. 59-74，2001.

[15] Barrie Mellars, "Forensic examination of mobile phones", Digital Investigation, Vol. 1, pp.266-272, 2004.

[16] Eoghan Casey, "Handbook of Computer Crime Investigation: Forensic Tools and Technology", ACADEMIC PRESS, 2001.

[17] Eoghan Casey, "Digital Evidence and Computer Crime", second Edition, Elsevier

Inc., 2004.

[18] National Institute of Justice, “Forensic Examiniation of Digital Evidence ：A Guide for Law Enforcement”, Digital Investigation, Office of Justice Programs National Institute of Justice , 1999.

[19] 鉅亨網，“拓墣：智慧型手機今年全球出貨量達 1.83 億支 業者毛利恐下滑”，http://news.cts.com.tw/cnyes/money/200908/200908190304817.html，2009.

[20] 電子工程專輯網站，“行動電話市場衰退 智慧手機成救命仙丹”，http://www.eettaiwan.com/ARTP_8800581476_617723.HTM，2009.

[21] 中時電子報，“咱的教育—搜查手機侵犯隱私權？”，http://www.coolloud.org.tw/node/26472，2008.

[22] 都市快報，“手機裡的已刪信息可恢復，律師提醒：私自恢復他人信息也算違法”，http://www.hangzhou.com.cn/pdf/2006/09/07/dskb/KB35907C(ps).pdf，2006.

[23] 台灣法律網，“美國刑事訴訟法中搜索與隱私權間的關係”，http://www.lawtw.com/article.php?template=article_content&area=free_browse&parent_path=,1,660,&job_id=146146&article_category_id=1532&article_id=76355，2009.

[24] 臺灣電腦網路危機處理暨協調中心，“電腦鑑識科學的現在與未來(一)”，http://www.cert.org.tw/document/cloumn/show.php?key=68，2006.

[25] 臺灣電腦網路危機處理暨協調中心，“電腦鑑識科學的現在與未來(二)”，http://www.cert.org.tw/document/cloumn/show.php?key=69，2006.

[26] HTC 宏達電手機論壇，“隱藏在 SIM 卡中的秘密”，http://bbs.mpbus.com/thread-4544-1-1.html，2008.

[27] Information Security 資安人科技網，“數位鑑識的挑戰與展望”，http://www.isecutech.com.tw/article/article_detail.aspx?aid=478，2005.

[28] Warren and Brandeis, “The Right to Privacy”, Harvard Law Review, Vol. 5, 1890.

[29] ZDNET，“智慧手機大會戰”，http://taiwan.cnet.com/digilife/0,2000089053,20102428,00.htm，2005.

[30] ZDNET，“Fortinet 提供「09 年 9 大網路安全趨勢預測」”，http://www.zdnet.com.tw/news/comm/0,2000085675,20135596,00.htm，2009.

Constructing the Standard Operation Procedure of Digital Evidence Forensics and Verification – Taking Smartphones as an example

Win Nan Wu (吳穩男)
Dept.of Information Management, Huafan University
Email:winwu@ms1.hinet.net

I-Long Lin (林宜隆)
Dept.of Information Management, Central Police University
Email: Paul@mail.cpu.edu.tw

ChihPai Chang (張志岩)
Dept.of Information Management, Huafan University
Email: chang.pie@gmail.com

As information technology advances, more and more dependent on information technology, the community engaged in social behavior, but accompanied by the information and communication security, and ethics, literacy and other problems are endless. Study indicated that in 2009 the global smart phone shipments reached 183 million, rose 28.2%. Its powerful hardware and software capabilities at all levels promote extensive application into making smart phones surge in criminal activity. Ran phones are personal items, and are subject to privacy protection, so this kind of criminal investigation by the existence of traditional forms of crime are significant differences. In view of this, the study of law enforcement experts explore Britain's National Center phone survey guidelines and domestic scholars Lin Long Ti out of the digital forensic evidence, standard operating procedures, and optimizing this process right smart phone forensic examination of digital evidence in court to explore the way the digital evidence of effectiveness and legitimacy, so that forensics personnel to use this process to complete forensic forensic work to improve the digital evidence in court to prove the strength and credibility as a judge of the basis for the future.

Keyword: Information Technology, Information and Communication Security, Computer Forensic and Digital Evidence, Smartphones.