智慧型手機作業系統之比較分析與數位證據鑑識標準作業程序初探

林宜隆
元培科技大學資訊管理系
cyberpaul747@mail.ypu.edu.tw
伍台國
國防大學管理學院資訊管理學系
w13464@yahoo.com.tw
呂宗霖
國防大學管理學院資訊管理系
alinna56@gmail.com

摘要

近年來智慧型手機已成為趨勢，其邏輯運算能力、多媒體能力就像是一台輕便型電腦裝置，多半智慧型手機都能連上網路瀏覽網頁等資訊，透過網路下載平台所提供大量之應用軟體運用至各個領域中，因此使得犯罪者利用智慧型行動裝置之便利特性，行犯罪事實，造成許多安全上的問題。

科技犯罪偵查上常強調個人電腦或伺服器上之數位證據偵查鑑識，對行動通訊裝置部分則相對較少提及，本研究主要是將智慧型手機之類型、硬體架構及作業系統分析比較，以及建立行智慧型手機之數位鑑識標準作業程序。

關鍵字：數位鑑識、鑑識工具、智慧型手機、標準作業程序。

一、前言

(一) 研究背景與動機

根據市場研究機構所示，2011 年整年度全球智慧型手機設備銷售量達 1 億 7745 萬支，比起去年同期銷售量成長率達 11.1%。人們對行動電話的依賴性可見一斑，對於這些體積小、重量輕、功能多元、便於攜帶、普及率高的裝置，加上無線上網等功能後，行動電話在未來將等同一部迷你個人電腦。很多的犯罪者將其高科技運用於犯罪上，因此從行動電話裡萃取出重要的證據，證明此內容為犯罪者所有，或是藉由其他證據之證明、以電腦相關軟硬體設備輔助，達到數位證據的可靠信。

由於數位證據可儲存在不同的軟、硬體設備之中，如個人電腦、網路伺服器、智慧型手機等各種存放數位資料之設備，且根據數位資訊的特性及存放的軟、硬體與應用程式的不同，必須使用不同的鑑識工具與技術進行數位鑑識的取證工作，才能萃取出關鍵性的數位證據，使其能在法庭上提出有效且可被法官採納的數位證據，成為法庭上的呈堂證供，故如何打擊和防治數位犯罪，成爲司法界亟待解決的一大難題。加上數位資料是易消滅、易修改及不易個化等特性，蒐集及保存數位證據時，必須顧及不影響網路正常運作，網路中同一段時間內有多個位置發生，證據可能在不同地方或設備發現，網路連接的改變路等等的問題，一一都在挑戰數位證據鑑識（Digital Evidence Forensics）的困難性。

(二) 研究目的

鑑於智慧型手機數位犯罪案件層出不窮的發生，因不同類型手機作業系統而異，其在搜證上將有所區別，而國內目前沒有一套智慧型手機數位證據鑑識標準作業程序，對於智慧型手機數位證據採集方法、鑑識程序、鑑識效率、工具軟體及所需技術亦嚴重欠缺，有必要對此議題進行深入的研討。

本研究主要目的為將目前市面上的智慧型手機之類型、硬體架構及作業系統，建置行動通訊裝置數位鑑識標準作業程序，以利數位證據偵查鑑識。

二、文獻探討

本章節將探討數位鑑識與電腦鑑識的內容，並將智慧型手機的作業系統中 Android、Windows Phone、iOS 系統分析比較，以建置構智慧型手機數位證據鑑識標準作業程序架構，提升科技犯罪偵查能力，以及偵查人員偵辦案件之能量，增強證據之證據能力及證明力。

(一) 數位鑑識與數位證據

1. 數位鑑識

數位鑑識必須以周延的方法及程序保存、識別、抽取、記載、解讀及分析儲存於數位媒體裡的證據。學者林宜隆提出數位鑑識所涵蓋的範圍為：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，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裡，應包含電腦鑑識（Computer Forensics）、資料鑑識（Data Forensics）、軟體鑑識（Software Forensics）、網路鑑識（Network Forensics）及行動裝置鑑識(Mobile Device Forensics)等。

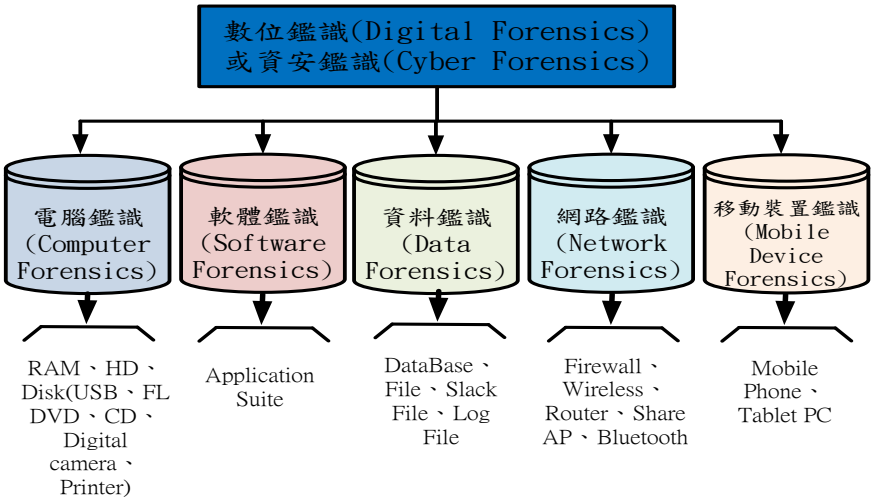

圖 1 數位鑑識(Digital Forensics)

這是一門能夠幫助解決資通安全事件或網路犯罪中有關數位證據的科學。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。

數位證據的特性有：(1) 容易複製 (2) 容易修改 (3) 不易證實其來源及製作人難以確定 (4) 人類無法直接感知、理解其內容。須遵守數位證物鑑識的標準作業程序，以克服數位證據這些特性，使證據能為法官所採用。

2. 數位證據

國外學者 Casey 在其著述「Digital Evidence and Computer Crime」中談論到數位證據的定義，認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，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。學者林宜隆教授及蔡宜縉，將數位證據定義為，任何使用電腦或相關電子設備儲存、傳輸的電磁紀錄，包含：文字、聲音、影像、圖片、符號或其他資料，凡是可以透過適當設備讀取出來的電磁紀錄，可用於支持或反證犯罪，或可以用來表達犯罪動機、犯罪現場等關鍵要素都可稱為數位證據。數位證據不像傳統證據般有實體、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，是一種抽象的存在；由於這些證據內容不能由肉眼直接看見，必須經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。

(二) Smart Phone 作業系統

智慧型手機鑑識上的難度來自於手機接口種類繁多、作業系統不同及國內法律沒有制定統一鑑識標準程序；而非智慧型手機則是只能使用手機裡內建之功能，不

能藉由其他第三方應用程式獲得額外功能，有些能運行少數 JAVA 程式。智慧型手機作業系統，本研究分別針對三個熱門作業系統 Android、iOS 及 Windows Phone 作介紹。

1. 智慧型手機作業系統市佔率比較

根據國際數據中心 (International Data Center；IDC) 數據顯示，2011 年智慧型手機出貨量已從 2010 年的 3.04 億支成長至逾 4.91 億支，2011 年全球智慧型手機預期將會成長 61.3%。其中 Android 手機市占率將有 39.5%，成為作業系統之冠。此外，也預計 Windows Phone 7(WP7)的 2015 年市占率將達 20.9%，居第二名。與 Android 相比較，2011 年 Apple iOS 占有率達到 15.7%的高峰後，仍能維持一定基本盤，讓 Apple iOS 在 2014 年前，都能穩坐全球智慧型手機第 2 大作業系統的地位；預估 2015 年則將被另一支後起之秀-微軟大軍超前，維持在智慧型手機全球市占第三名位置，形成 Android、Apple iOS、Windows Phone 的三分局面，全球智慧型手機預測如表 1 所示：

表1 全球智慧型手機2011~2015預測

Operation System	**2011 Market Share(%)**	**2015 Market Share(%)**
Android	39.5	45.4
Black Berry	14.9	13.7
Apple iOS	15.7	15.3
Symbian	20.9	0.2
Windows Phone 7	5.5	20.9
Others	3.5	4.6
Total	100	100

由於智慧型手機及數位證據所涵蓋之議題甚廣，面對不同的資訊犯罪場景，所進行的鑑識及蒐證作法亦有不同，無法對所有手機作業系統作完整的說明，接下來將挑選谷歌(Android)、蘋果(Apple iOS)和微軟(Windows Phone)等目前市場知名度較高的產品，針對其核心特色、開發環境與應用場合等內容做介紹，在有限的時間與人力下為了集中討論焦點。

2. Smart Phone 作業系統比較

本研究進行 Android、iOS 及 Windows Phone 三種常見智慧型手機作業系統功能比較，如表 2 各作業系統之比較；認為各家智慧型手機所搭配的作業系統不盡相同，功能也有所不同，有手機廠商自行研發的作業系統，也有其他廠商開發的作業系統，在這些系統的選擇與運用上，各有優缺點，依照消費者選取所需的系統及手機。

表 2 各作業系統之比較表(本研究整理)

分類	**Android**	**iOS**	**Windows Phone**

主要開發公司	Google	Apple	Microsoft
發源歷史	以 Linux 為核心發展而成	以 Mac os 為核心發展而成	以 Windows CE 為核心發展而成
最新公佈版本	Android 4.0 版本 (Ice Cream Sandwish)	iOS 5 版本	Windows Phone 7.5 版本 (Mango)
主要支援程式語言	Java、C/C++	Xcode(含 C/C++、、Objective-C 等)	Java、C++、VB
系統開發	開放原始碼	封閉源	封閉源
系統授權方式	免費	無授權	高授權金
軟體市集	專門的交換平台 Android Marke	專門的交換平台 App Store	專門的交換平台 Market Place
軟體副檔	.IPA	.APK	.XAP
應用程式數量	第三方應用程式較 iOS 少(約 30 萬)，快速增加。	第三方應用程式最多(50 萬)，遊戲方面軟體大幅領先其它系統。	第三方應用程式最少(5 萬)，持續增加。
OS 業者提供資源	低	高	高
硬體規格需求	低	中等	高
資訊安全性	中等	高	高
支援手機廠牌	HTC、SONY、SAMSUNG、MOTO 等	IPhone 系列	NOKIA、HTC
優勢 Advantage	開發廠商多，手機選擇性多。自家設計的 UI，操作起來會有比較不一樣的感受。	手機介面簡單易用，觸控性佳、硬體規格統一，軟體開發相容性高。	Windows 自家相關功能產品成熟並可整合電腦使用。
弱點 Weakness	版本可能會參差不一，舊產品升級機率較低、軟體相容性會有些問題。	軟體開發限制較多、必須透過 iTune 存取檔案系統。瀏覽器不支援 Flash、Java。蘋果商品限定，價格高昂	硬體規格需求高，相對提高手機價格、第三方應用程式數量少，收費較高。
機會 Opportuity	與既有 Google 服務的緊密結合、易於推出中價與入門級智慧型手機	支援的軟體眾多，市占率高。	軟體高度整合搶攻市場，連結 windows 相關運用、新系統可算最晚出現，可以充

			分了解各家平台的優缺點。

Android 系統由於有許多廠商投入生產，為了要有所區別性也加入許多自家 UI 設計，所以操作起來會有比較不一樣的感受，iOS 系統跟 Android 系統都以有強大的的軟體市集為傲，兩者內容量上主要以 App Store 的軟體種類較多，但在帳號申請或是操作介面以英文為主，使用者在剛入手時可能會有點麻煩，Windows Phone 在應用軟體則是最少數量但仍持續增加。由於 Android 的產品遍佈各家廠商，每家的規格都不近相同，所以也往往發生軟體不支援硬體的問題。儘管如此，各家無不提升軟、硬體規格、提高運算速度，但這又衍生出另一個問題：提高運算速度導致了手機耗能加大、結果就是縮短了待機時間，電池續航力成了智慧型手機一個
共同須解決的問題。

三、智慧型手機數位證據鑑識標準作業程序

(一)、數位證據鑑識標準作業程序架構

參考國內學者林宜隆教授所提出數位證據鑑識標準作業程序，認為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，其中又以操作階段最為重要，如圖 2 圖說明：

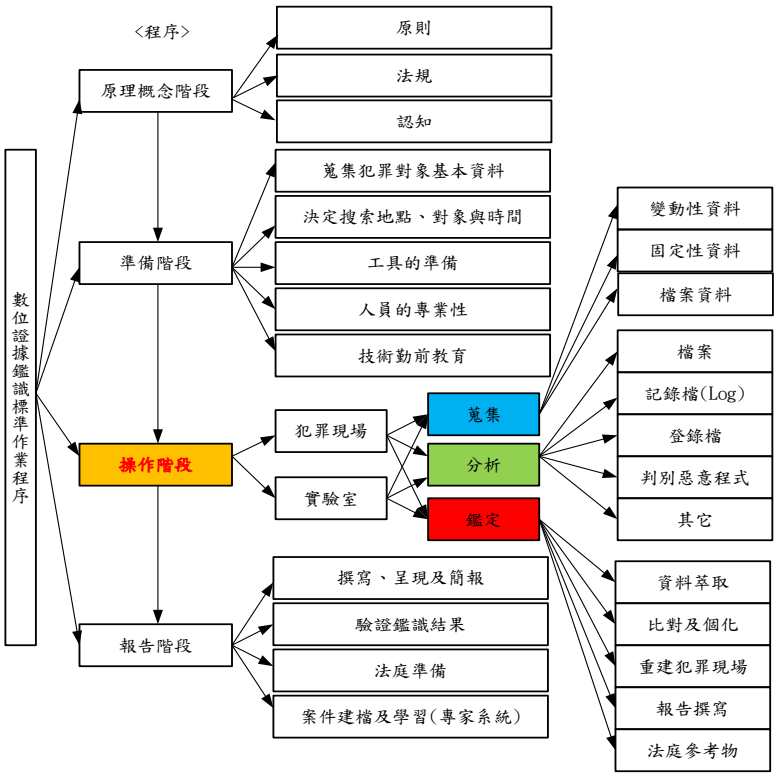

圖 2 數位證據鑑識標準作業程序（DEFSOP）

(1) 原理概念階段：分為「法規」、「原則」、「認知」三個部份，說明如下

a. 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。

b. 原則：

(a)完整性（Integrity）：在不改變或破壞證物的情況下取得原始證物。

(b)正確性（Proper）：證明所擷取的數位證據來自扣押的證物。

(c)一致性（Consistency）：在不改變證物的情況下進行分析。

(d)符合性（Compliance）：符合當地的法律規範。

(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，是為了操作階段各程序執行的預作準備，以下為其步驟(吳穩男、張志宗、林宜隆、朱惠中，2008)：

a. 準備工具及勤前教育：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；在每次出任務前，必須計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。

b. 確定人事時地及理由：根據犯罪的類型，並利用已掌握的情況分析可能作案人員，若案情需要也可訪談相關人員，另外再決定搜索地點、對象與時間，依據蒐集嫌犯資料後，決定搜索地點和時間。

c. 蒐集對象基本資料：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。

(3) 操作階段

a. 蒐集程序：蒐集及採樣數位證據，將數位資料分為「變動性」、「固定性」、「檔案資料」等三個部分。

b. 分析程序：在分析資料這個程序，將分析資料分為五個部分，分別為「檔案」、「記錄檔（Log）」、「作業系統登入檔」、「判別惡意程式碼」、「其它（遠端主機通訊埠）」。

c. 鑑定程序：在鑑定這個程序，將鑑定分為四個部分，分別為「資料萃取」、「比對」、「個化」、「重建犯罪現場」。

(4) 報告階段：在報告這個階段，分為四個程序，分別為「撰寫、呈現及簡報」、「驗證鑑識結果」、「法庭準備」、「案件建檔及學習（專家系統）」。

(二)、 NIST 智慧型手機數位鑑識標準作業程序比較分析

歸納美國國家標準與技術研究院所提出的作業程序分成四個階段，分別為保存階段(Preservation)、萃取階段(Acquisition) 、檢驗與分析階段(Examination and Analysis)及報告階段(Reporting)[12]，如圖 3 所示：

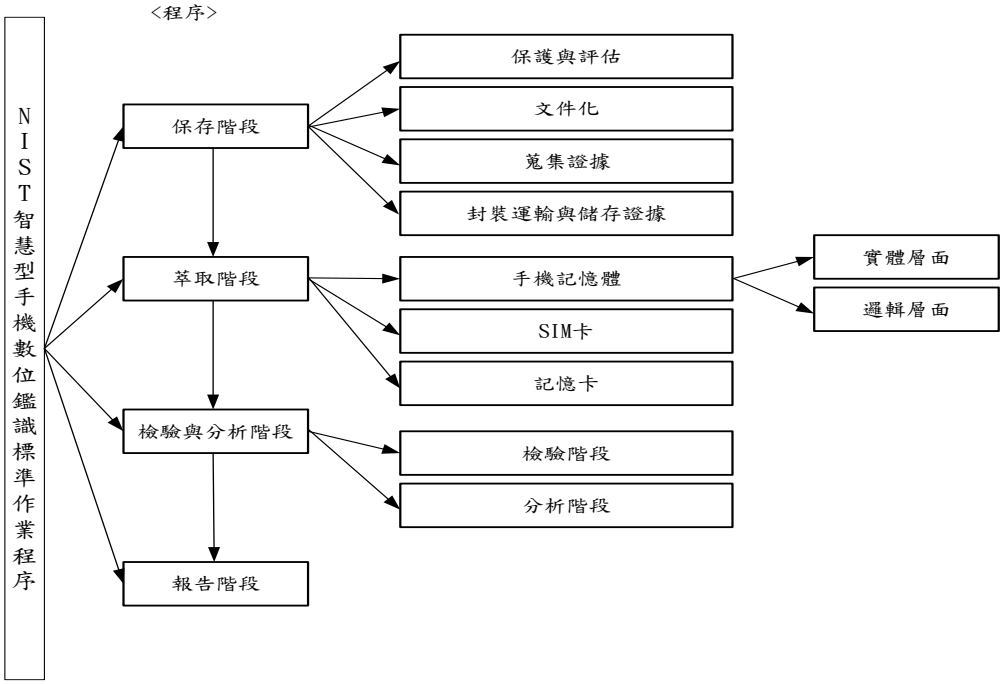

圖 3 NIST 手機鑑識作業程序

經由整理 NIST 標準作業程序發現與學者林宜隆教授所提出的數位證據標準作業程序(DEFSO)有許多異同之處，其比較分析如表 3 所示：NIST 所提出的作業程序並沒有提出以法律為基礎的概念階段來輔助其它階段，使其數位鑑識作業程序具合法性；NIST 標準作業程序並未將人員的訓練，鑑識前的準備歸納入標準作業程序內，而是透過文件來闡述，在 DEFSOP 中分別將這兩項列為重要標準之一(原理概念階段、準備階段)，故學者林宜隆教授提出的 DEFSOP 流程中較 NIST 標準較周全(17)。

表3 智慧型手機數位鑑識標準作業程序差異比較

比較	**DEFSOP by Paul Lin**	**NIST Smart-Phone DEFSOP**
相同	「操作階段」主要分成蒐集、分析及鑑定三細項。	「保存階段」為蒐集證據，「萃取階段」為萃取數位證據，「檢驗與分析階段」分別為鑑定與分析。
	「報告階段」將數位證據呈現給法官。	「報告階段」將數位證據呈現給法官。
差異	「概念階段」提出藉由法律程序取得數位證據，加強證據力。	NIST並無詳細提到透過法律或政府來取得數位證據。
	「準備階段」提出人員的訓練、工具的準備。	NIST並無詳細提供人員訓練及事前工具準備事宜。

本研究歸納 NIST 的保存階段、萃取階段和檢驗與分析階段，認為此三階段因都偏屬較技術實務方面，故應以一個階段完成，學者林宜隆教授所提出與 NIST 不同架構的標準作業程序，因將各階段明確地分類，有助於各類不同專業領域的鑑識人員能有效分工進行鑑識。參考國內學者林宜隆教授所提出 DEFSOP 的操作階段、報告階段互相對映遵循說明如圖 4 所示：

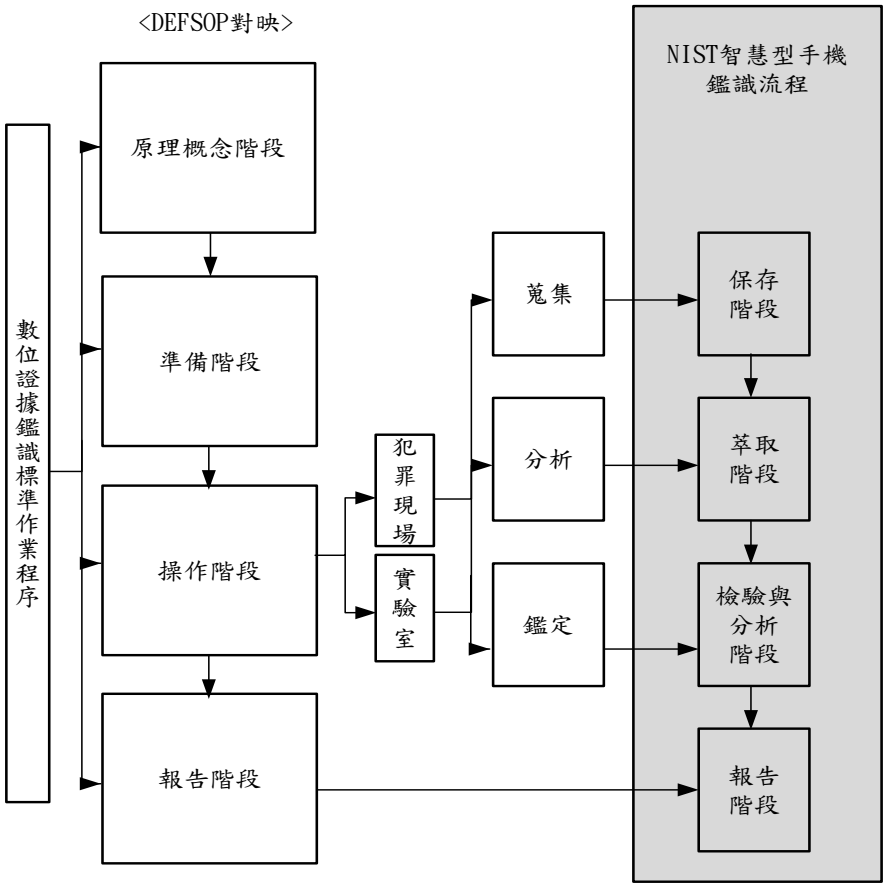

圖 4 DEFSOP 與 NIST 手機鑑識流程對映圖

四、智慧型手機案例分析

(一)、鑑識工具模擬－以 XRY Forensic Tool 為工具

1. XRY 簡介

本研究以 XRY 為 Micro Systemation 公司開發之鑑識軟體工具箱進行案例分析，能供調查人員取證、以各種格式瀏覽資料、書籤標記，XRY 甚至可能查看某些隱藏信息，例如歷史訪問的網站，安全代碼、IMSI 和國際刑事法院的代碼等。有了這個系統，可以快速收回大量信息。

重要資訊、匯出資料和多種報表格式，在瀏覽資料時會依照資料格式自動選擇最佳瀏覽方式。該軟體能從手機裡取出以下資料：簡訊記錄、文字記錄、電話簿(含

手機記憶體及 SIM 卡)、通話紀錄(含已接、未接來電、撥打號碼及日期和持續時間)、記事本、行程表、日曆、代辦事項列表、檔案系統、系統文件、圖片、音訊、視訊、JAVA 檔案、已刪除資料、E-mail、登錄檔等。

2. 案例實作

本研究使用之智慧型手機為 iPhone 4，其作業系統為 OS X v5.01，操作環境 Windows 7，以下為操作過程之一部分。

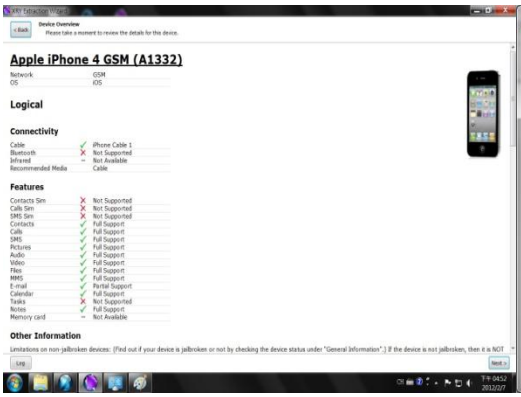

圖 5 連結並辨識手機

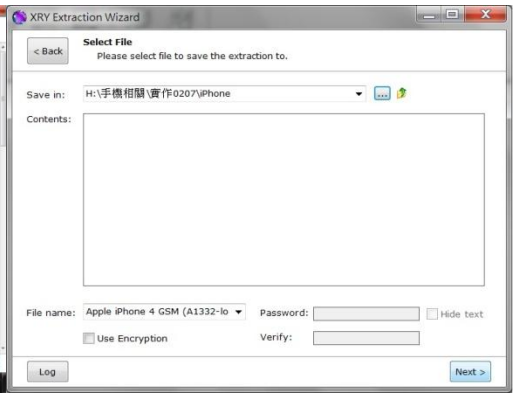

圖 6 建立新專案並輸入各項基本資料

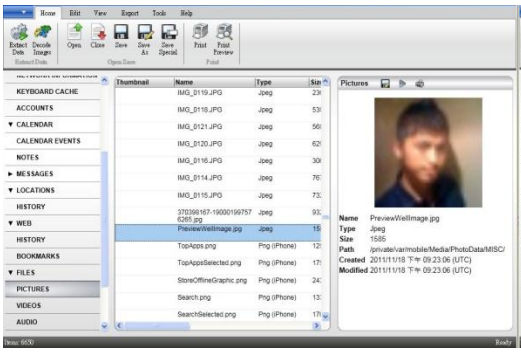

圖 7 檔案預覽-照片

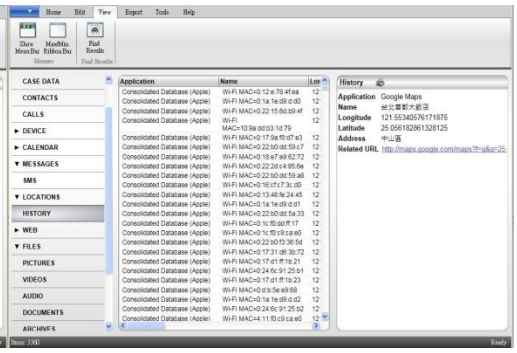

圖 8 檔案預覽-GPS 位置

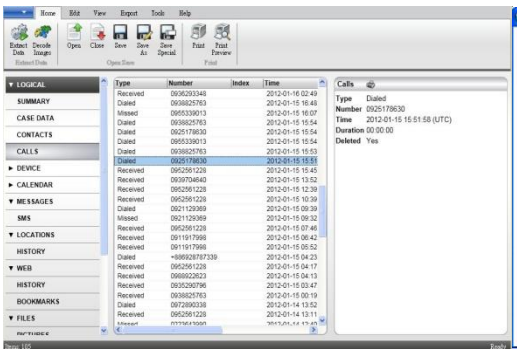

圖 9 檔案預覽-通話紀錄

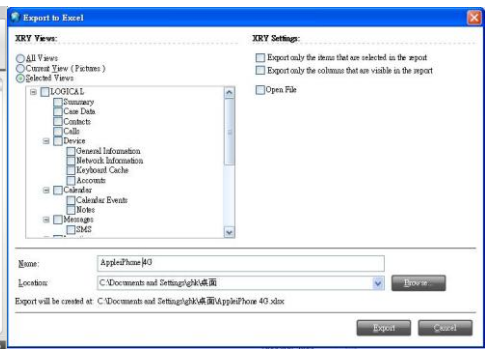

圖 10 製成報告，可選擇輸出類型

智慧型手機有一個對鑑識非常不利的條件，不斷更新的系統及硬體，這些因素都會造成鑑識上無法避免的阻礙。加上近年來由於山寨機的盛行，一些國際大廠的手機鑑識產品也開始支援對山寨機的取證，支援型號數量對鑑識人員是否能快速正確解讀出手機內的相關資訊有非常大的影響。與手機硬體不同，電腦的硬體大多都是遵循標準生產製造，因此不管使用者使用的作業系統為何，鑑識人員都能快速從電腦主機中擷取出相關資料進行分析。而手機設備的情況卻十分不一樣，廠商在生產手機時通常使用自己公司專有的技術和規格，甚至同樣廠商不同型號的產品都可能使用不同的技術，由於手機設計均被各家手機製造商視為機密，因此如何廣泛支援各家的手機成了手機鑑識產品的努力的目標。就實務而言，鑑識人員在進行手機取証時會搭配使用不同的手機鑑識產品，以應付不同的手機設備。

四、結論

本研究整理電腦鑑識科學領域專家對於數位鑑識的定義，了解智慧型手機數位鑑識之概念及意義，說明進行每項鑑識步驟之目的、執行程序與手機偵查及數位證據蒐集、分析之有效性與鑑識過程之合法性，並與美國國家標準與技術研究院所提出的智慧型手機數位鑑識標準作業程序比較，再次驗證學者林宜隆教授所提出的鑑識程序考慮了數位證據的合法性，補強數位證據能力與證明力。最後以 XRY 手機鑑識軟體針對智慧型手機(本研究以 iPhone 為例)數位證據進行案例模擬分析。

參考文獻

1. 林宜隆、藍添興 (2004)。資訊犯罪與安全管理之探討。中央警察大學。
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. 台灣電腦網路危機處理暨協調中心技術專欄，電腦鑑識科學的現在與未來(一)，http://www.cert.org.tw/document/column/
4. 周瑞國、林宜隆、伍台國，2011，植基於雲端安全之數位證據鑑識標準作業程序之研究，碩士論文，國防大學管理學院。
5. 林宜隆、歐啟銘，手持式行動通訊裝置數位鑑識工具比之較與案例分析，第十屆「網際空間：資安、犯罪與法律社會」學術研究暨實務研討會，2008。
6. 歐啟銘，建構我國科技犯罪偵防能量之研究-以行動設備數位犯罪鑑識能量為例，碩士論文，2009。
7. 林宜隆、吳政祥，數位鑑識標準作業程序案例驗證之分析，第 9 屆網際空間：資安犯罪與法律社會學術研究暨實務研討會，2007。
8. Android developers , Android Architecture http://developer.android.com/guide/basics/what-is-android.html)
9. Apple developers ,iOS

Features(http://developer.apple.com/technologies/ios/features.html)
10. Eoghan Casey , 2002, “Digital Evidence and Computer Crime”,ACADEMIC PRESS.
11. Gartner, Gartner Says Sales of Mobile Devices in Second Quarter of 2011 Grew 16.5 Percent Year-on-Year; Smartphone Sales Grew 74 Percent, (http://www.gartner.com/it/page.jsp?id=1764714)
12. http://www.3cx.com.tw/voip-sip/voip-definition.php
13. IDC, “Worldwide Smartphone 2011-2015 Forecast Update：2011 September”, (http://www.idc.com/getdoc.jsp?containerId=230173)
14. Lin IL, Yen YS, Wu BL. Analysis of VoIP security threat vulnerability and prevention policy, CISC 2009 Conference,Taipei, June 2009a.
15. Lin IL, Yen YS, Wu PL. Primary research on VoIP security threatvulnerability and attack prevention. In: ISMAD 2009, Taoyuan,March; 2009b.
16. Lin IL, Yen YS, Wu BL, Yu CC. VoIP security problem and digital forensics. In: Information management, practical application and talent nurturing conference, Taipei, May; 2009c.
17. Lin I-Long, Chao Han-Chieh, Peng Shih-Hao, "Research of Digital Evidence Forensics Standard Operating Procedure with Comparison and Analysis Based on Smart Phone," 2011 International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), pp.386-391, 26-28 Oct. 2011.
18. NIST, “Smart Phone Tool Specification” , Public Draft 2 of Version 1.1 , 2009 July 7(http://www.cftt.nist.gov/documents/Smart_Phone_Tool_Specification.pdf)
19. NIST, Special Publications (800 Series),2007(http://csrc.nist.gov/publications/PubsSPs.html)
20. Wiki, Android ,2011(http://zh.wikipedia.org/wiki/Android)
21. Wiki, iOS ,2011(http://zh.wikipedia.org/wiki/IOS)
22. Windows Phone, Windows Phone 7 智慧型手機應用程式開發總覽, http://msdn.microsoft.com/zh-tw/windowsphone/ff955778
23. Yun-Sheng Yen, I-Long Lin, Bo-Lin Wu.A study on the forensic mechanisms of VoI P attacks: Analysis and digital evidence;2011

The Analysis of Smartphone Operating Systems and Digital Evidence Forensics Standard Operating Procedures Investigation

I-Lung Lin
Department of Information Management, Yuanpei University
cyberpaul747@mail.ypu.edu.tw

Tai-Kuo Wu
Department of Information Management, Management College of National Defense University
w13464@yahoo.com.tw

Tsung-Lin Lu
Department of Information Management, Management College of National Defense University
alinna56@gmail.com

Abstract

Smart phones in recent years has become a trend, its logic of computing power, mult-imedia capabilities as a portable computer device, the majority of smart phones can even access the Internet to browse the wab and other information downloaded through the Internet platform to provide a large number of applications software to use to all fields, thus making the offender to the use of smart mobile devices convenience features, the line the facts of the crime, resulting in many security problems.

PC or server on the digital evidence investigation forensics, a relatively small part of the mobile communications device mentioned, this study is the type of smart phone, the hardware architecture and operating system analysis is often highlighted in the technology crime investigation, and the establishment of the line smart phone, digital forensics standard operating procedures.

Keywords: Digital Forensics, Digital Evidence Forensic Standard Operating Procedures, Smart Phone