智慧型手機犯罪 DEFSOP 與案例驗證之研究

林宜隆
元培科技大學資訊管理學系 教授
E-mail:cyberpaul747@mail.ypu.edu.tw,cyberpaul727@gmail.com
宋元傑
中央警察大學資訊管理系 學生

摘要

在這個數位科技發展一日千里的年代,行動通訊裝置已然成為現代人生活不可缺少的工具，其往往擁有照像、錄音、錄影、藍芽傳輸、紅外線傳輸、無線網路傳輸、行事曆、電話簿、文字簡訊、多媒體影音簡訊傳遞及無線上網等功能，已不再像傳統單純用於通訊，而更進步的智慧型手機更擁有專屬的作業系統，可以 3.5G 行動上網、安裝許多客製化的應用程式，所以可能存在著大量的私密個人資料，在具有高度機動性且幾乎成為一台迷你個人電腦的要件下，行動通訊裝置成為許多違法亂紀的人使用的工具,任何藏匿於這些輕巧裝置裡的蛛絲馬跡，均可能成為刑事司法人員破案關鍵之所在。

關鍵詞：數位鑑識、標準作業程序

一、緒論

行動通訊裝置之作業系統市場相較於一般電腦來得複雜，因為行動通訊裝置之廠商不僅有各種陣營之分，如:Google 的 Andorid、Apple 的 IOS、微軟的 Windows Mobile、Nokia 的 Symbian…等。各廠商也會因為系統軟體版本、套件或是廠商另行開發而衍伸出更多差異，且其作業系統更新速度相當快速，因應這些差異必須用相對應的更新之後的鑑識工具軟體，才能達成鑑識工作。

科技犯罪偵查上常注重個人電腦或伺服器上之數位證據，對智慧型手機裝置部分則相對較少提及，本研究主要是希望能夠介紹智慧型手機之類型、硬體架構及作業系統，以及建立智慧型手機裝置之數位證據鑑識標準作業程序(DEFSOP for Smart Phone Devices)與案例分析及驗證。

二、智慧型手機犯罪與犯罪偵查

2.1 智慧型手機犯罪

現今智慧型手機的快速崛起，改變現代人使用行動設備的想法與模式，不需透過個人電腦，經由無線網路上網收發信件、瀏覽網站中最新消息、連上 facebook、google+、twitter、微博…等等社群網站來分享最新的個人資訊，成為主流青少年、學生、上班族的每天必做的一件事，在面對現今持續方便與發達的網際網路，手持行動裝置的便利，很多使用者易於忽略其安全性，可能造成個人資料外洩、信用卡資訊被竊取，或手機被植入惡意程式，偷偷撥打付費電話或傳送垃圾一般的簡訊，為犯罪者帶來大量報酬與心理上的滿足，讓受害者承擔鉅額的帳單。智慧型手機上網功能強大，透過 Skype、Jumblo 等視訊音訊程式能進行線上通話，若受話方也在線上接聽，是通訊監控的死角地帶，不僅已有歹徒用於犯罪聯繫，情報機關人士擔心國防規範、政府情資上會產生漏洞。單純由智慧型手機上所造成的犯罪，實屬少數，由絕大部分的犯罪內容分析顯示，智慧型手機在犯罪過程之中處於輔助的角色，然而卻是現今犯罪手法多元化之不可或缺的要件之一。本次研究主要注重在智慧型手機可能使用的犯罪手法，構想一套智慧型手機犯罪偵查模式，將智慧型手機犯罪偵查分為三個部分，依序並進，並整合專業人員與現今常使用的工具。

2.2 智慧型手機犯罪偵查

第一階段:偵查分析智慧型手機犯罪行為

需確定智慧型手機犯罪模式，藉由報案人的案情描述與犯罪偵查人員對於案情的情資掌握，透過與過往常見的一般犯罪手法進行比較分析，始能判斷為可能是利用智慧型手機為工具所犯下的案件，才能採取更進一步行動。使用工具偵測嫌犯手機的上網紀錄、GPS 定位資訊、或是透過電信單位取得該人通話時的基地台定點位置…等，進而發現犯罪集團的大本營。

第二階段:確定犯罪來源與行為

藉由各種辦法描繪出案情的輪廓，由案件五何(何人、何事、何時、何地、如何)，我們可透過清查與該犯罪現場有地緣關係的前科犯、系統使用者資料、個人的銀行帳戶、連線登入來源清查、電子郵件來源追查、瀏覽過網站的痕跡追蹤。每隻智慧型手機都擁有一組獨一無二的 IMEI(International Mobile Equipment Identity)國際移動設備辨識碼，指的就是每隻手機序號，主要用於手機中遍別出每一隻獨立的手機，為國際上公認的手機標記序號，等同於行動電話的身份證明。序號共有 15 位號碼，前 6 位(TAC)是型號核准號碼，代表手機類型。接著 2 位(FAC)是最後裝配號碼，代表產地。[24]

而每張 sim 卡也擁有一組 IMSI(International Mobile Subscriber Identity)國際移動用戶識別碼，對應著每個獨立的門號。綜合上述種種手法強化科技犯罪偵防能量。

第三階段:逮捕犯罪人員

該部分透過搜索、證物保全、相關嫌犯移送與偵訊與智慧型手機證據鑑識標準作業程序的採用，適用一般犯罪偵查程序。

2.3 智慧型手機犯罪與 DEFSOP

其犯罪偵查流程如圖 1

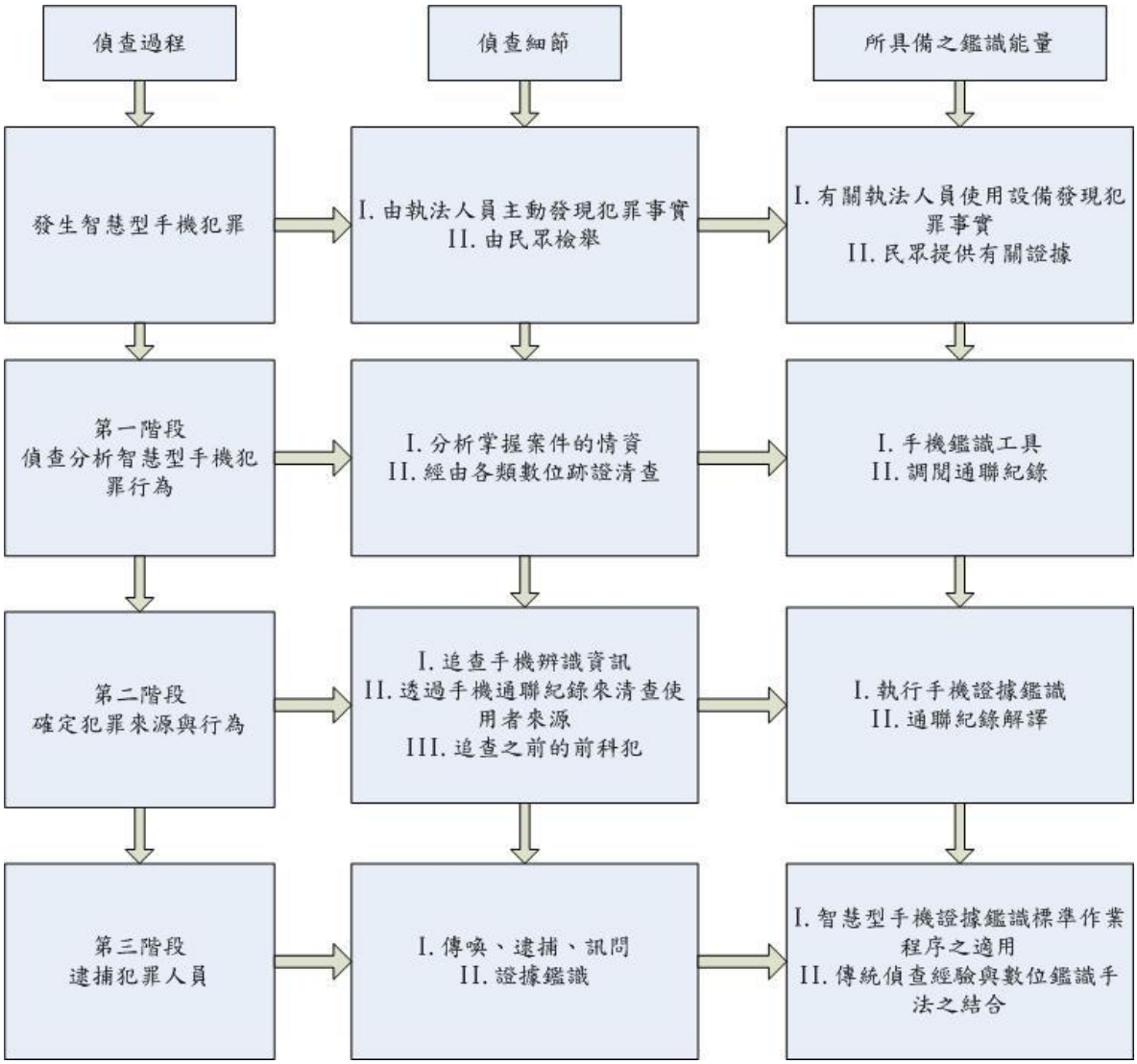

圖 1、智慧型手機犯罪偵查流程

大多智慧型手機之犯罪包括:以手機作為輔助工具之犯罪與手機本身為犯罪主體，如圖 2 所述。

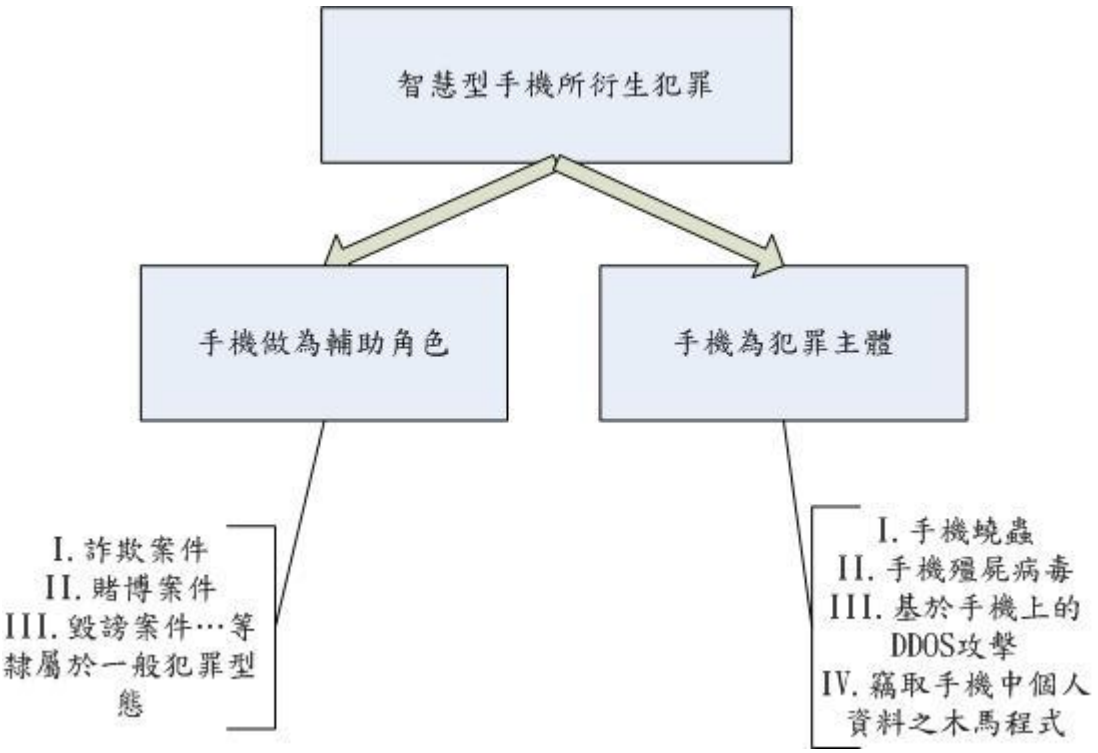

圖 2 智慧型手機所衍生之犯罪類型

由實際智慧型手機相關的案例分析，再透過犯罪模式與偵查程序的統整，經由本研究所整理的偵查方式，所得到的犯罪偵查模式如圖 22。由當事人報案做筆錄、提出告訴開始，檢察官與警方針對案情主動介入調查之後，由於智慧型手機所產生的犯罪特徵，收集那些特別的數位跡證，如:該手機之上網紀錄、通話時與基地台之定位，期望掌握所有與犯罪最為相關的證據，經由偵辦人員分析比較之後，找出犯罪人員的藏身之處或在下次犯案之前攔截、逮捕。

三、鑑識工具軟體實作與鑑識模擬

3.1 使用鑑識工具軟體實作

本次使用之智慧型手機為 HTC，其作業系統為 Android，工作環境作業系統為 Microsoft Windows XP，以下為操作過程。

3.2 鑑識模擬－以 MOBILedit! 5.5.0 為工具

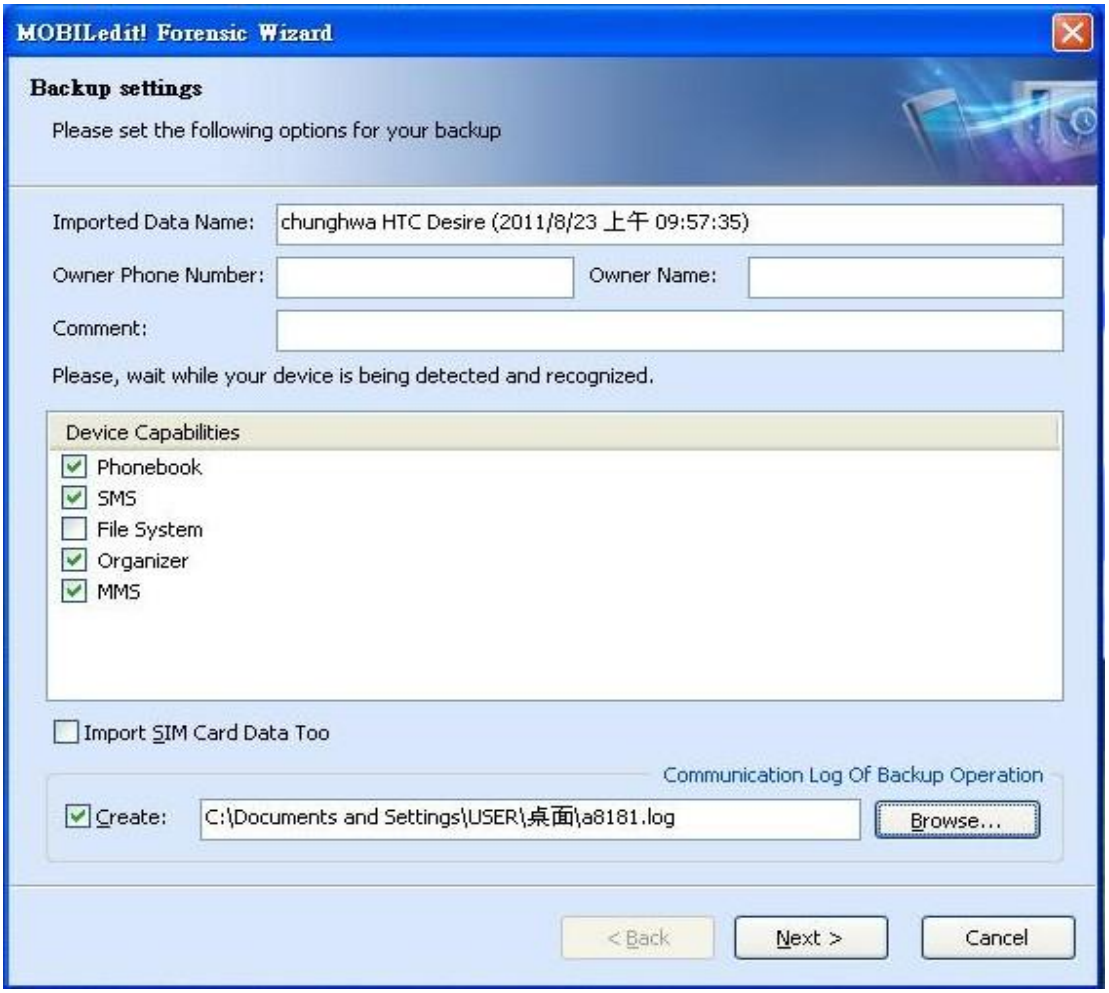

圖3、開新專案，輸入各項案件資料、選取欲鑑識項目。

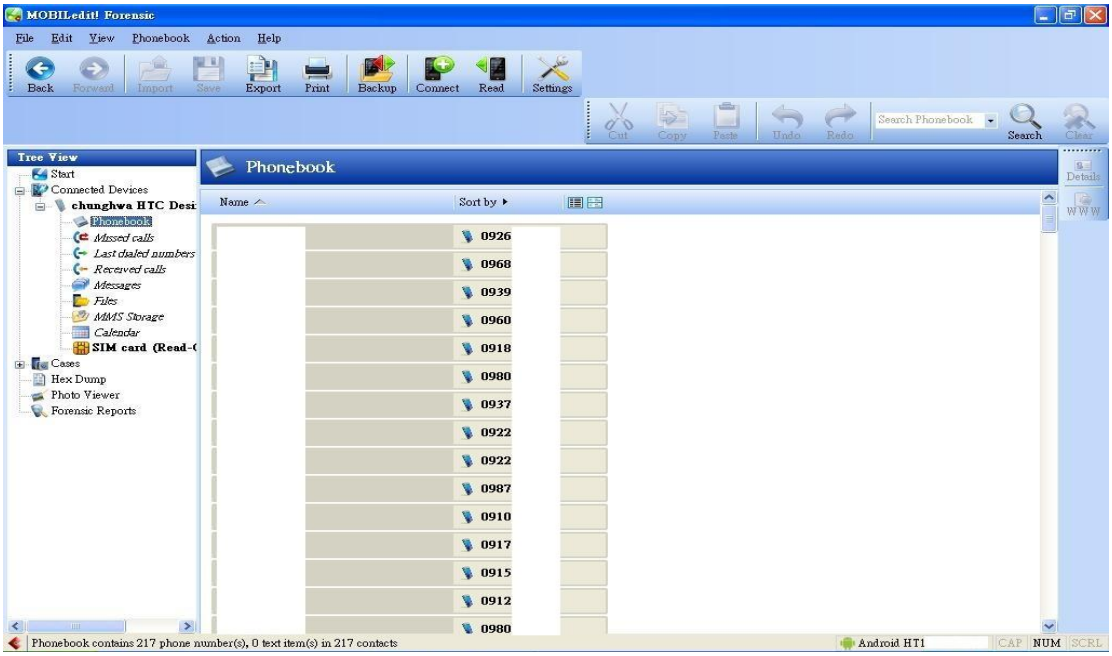

圖4、擷取出來的電話簿。

圖 5、瀏覽各類項目，選取左邊的項目

輸出之 xls 檔，內容包含所有項目之清單，並依類別分開存放於不同分頁，下圖為全部檔案所儲存之路徑、格式。

	A	B	C	D	E	F	G	H	I	J
1	Manufacturer:	chunghwa								
2	Product:	HTC Desire								
3	IMEI:	355 50								
4	Returned IMEI:	355 50								
5	MOBILedit! Version:	5.5.0.1148								
6	Forensic Version:	5.5.0.1148								
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										

圖 6、輸出之 xls 截圖，圖為手機之概要資訊。

四、智慧型手機鑑識工具指引平台建置

透過相關鑑識文獻探討，整理出相關鑑識流程、鑑識工具，本研究使用了這些鑑識工具，系統首頁使用後對於這些工具的特性，本研究認為，這幾套鑑識工具可以交互使用，因為這幾套鑑識工具特性的不同，本研究認為不同類型使用者，可以使用者不同類型工具。

在本研究的智慧型手機鑑識工具指引平台，為了要推薦使用者找到適合使用者的鑑識工具，在智慧型手機鑑識工具指引平台，一開始會先對使用者的基本資料作調查，並且做為數位鑑識能力的一個評斷，以利本系統推薦使用者其適合的數位鑑識工具。

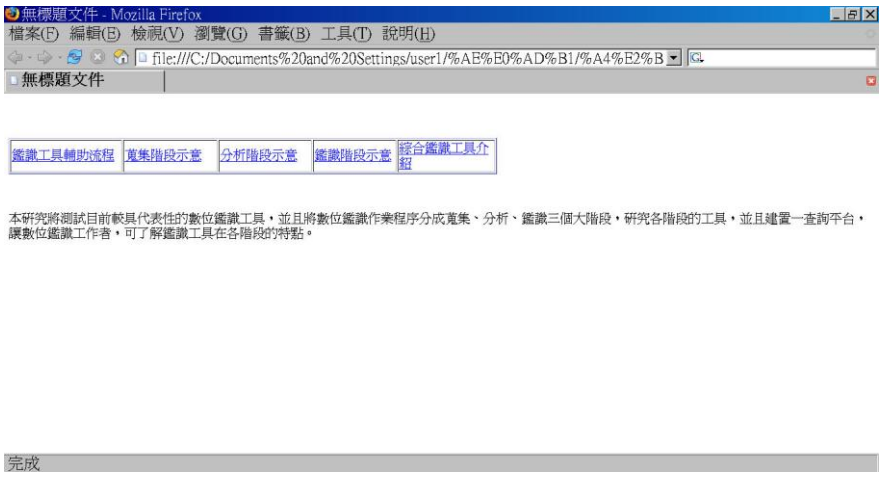

圖 7 本系統首頁

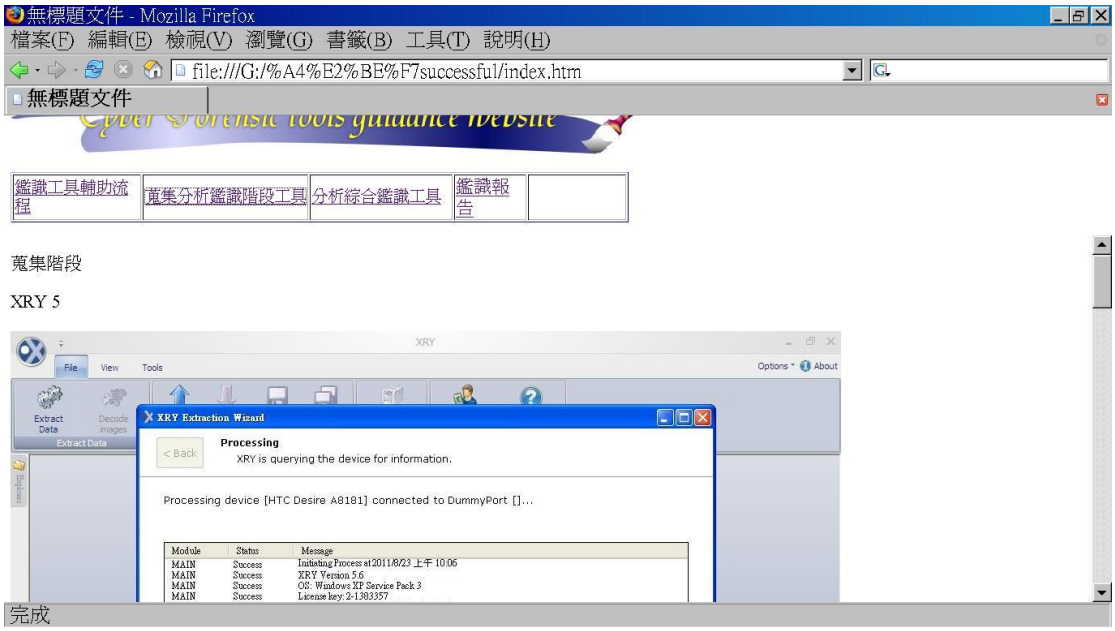

圖 8 鑑識蒐集階段流程

五、結論

大部分具有公信力之工具軟體，其授權費用往往所費不貲，而數位產品推陳出新頻繁，行動裝置不像一般個人電腦，就算硬體介面相同，但是往往會因型號、功能而特別作不同設計，甚至相同作業系統版本不同，可能就有不小的差別，各種鑑識軟體對於不同行動裝置很有可能遇到無法完整支援之情形，在研擬針對不同作業系統與硬體裝置之鑑識標準作業流程外，也應配合鑑識工具之更新與增購，以完善鑑識工作之環境。

六、參考文獻

[1]林宜隆、朱惠中、張志宋、吳穩男，Unix 與 Windows 數位證據鑑識標準作業程序與案例驗證之比較，2008 聯合國際研討會，第十屆「網際空間：資安、犯罪與法律社會」，2008。

[2]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。

[3] android developers ：http://developer.android.com/

[4]微軟公司網站：http://www.microsoft.com/windowsembedded/en-us/default.mspx

[5]Apple Developer Connection：http://developer.apple.com/

[6] Paraben Device Seizure：http://www.paraben-forensics.com/

[7]國家通訊傳播委員會統計資料：http://www.ncc.gov.tw/chinese/index.aspx

[8]維基百科：http://zh.wikipedia.org/zh-tw/

[9]http://techcrunch.com/2010/11/10/gartner-android-share-jumps-to-25-5-percent-now-second-most-popular-os-worldwide/

[10] iPhone：http://www.apple.com/tw/iphone/

Case Study of Smart Phones Crimes and its Digital Evidence Forensics Standard Operating Procedure (DEFSOP)

I-Long Lin
Professor of Department of Information Management, Yuanpei University
Email : cyberpaul747@mail.ypu.edu.tw,cyberpaul727@gmail.com
Jack Sung
Student of Department of Information Management, Central Police University

Abstract

In this digital era of technological development by leaps and bounds, the mobile communication device has become an indispensable tool of modern life.

They often have a camera,sound recording, video recording, Bluetooth, infrared, wireless networks,calendar, phone book, text messaging, multimedia text messaging and wireless internet access is no longer like the traditional purely for communication, while more advanced smart phones also has a proprietary operating system, can be 3.5G mobile Internet to install customized applications program.

There may be a large number of private personal information in a highly mobile and almost become the tools of the elements of a mini-PC, the mobile communication device as many irregularities, any hiding in these lightweight devices clues are likely to become the key to solve the case.

Keywords: digital forensics, standard operating procedure