Android平台智慧型手機鑑識軟體設計與實現

楊景翔
國立高雄師範大學
資訊教育研究所 研究生
ginshone@hotmail.com

楊中皇
國立高雄師範大學
資訊教育研究所 教授
chyang@nknucc.edu.tw

摘要

Android 作業系統自 2007 年 11 月 5 日由 Google 與 Open Handset Alliance 公佈以來，已快速發展成為全球第二大的智慧型手機作業系統，隨著日趨普及與日益廣泛的使用，伴隨而來的安全與犯罪媒介等問題，產生了 Android 平台智慧型手機鑑識的需求。

本研究使用 Android SDK 設計與實作 Android 平台智慧型手機鑑識軟體，透過軟體與邏輯採集的方式，排除特殊硬體需求上的限制，協助鑑識人員進行資料採集，取得手機硬體、SIM 卡內容、通話記錄、簡訊、通訊錄、最後定位記錄、網頁瀏覽與網路搜尋記錄等資訊，並確保取得資料的完整性，完成鑑識工作。

關鍵詞：Android、智慧型手機、數位證據、手機鑑識

1. 前言

隨著行動科技的發展，智慧型手機的功能越來越強大，智慧型手機不再僅是單純的語音通訊工具，它提供了網際網路、全球衛星定位、攝相與影音多媒體等功能、高容量的儲存空間以及多樣化的應用軟體，不僅擴展了手機的應用領域，同時也伴隨而來安全與犯罪媒介的問題。

根據國際研究暨顧問機構 Gartner 在 2010 年 8 月的統計與調查結果，Android 平台智慧型手機以 17.7%的市場占有率，成為全球第二大的智慧型手機作業系統，Gartner 並預測於 2014 年底時，Android 的市場占有率將會與目前第一名的智慧型手機作業系統 Symbian 非常接近 [7]，這說明 Android 平台智慧型手機的使用普及率正快速的增長。

本研究以 Android SDK 做為開發工具，參考美國國家標準技術局(National Institute of Standards and Technology, NIST)智慧型手機工具規範 [10]，設計與實作 Android 平台智慧型手機鑑識軟體，並且採用軟體不受特殊硬體工具限制的邏輯採集方法 [8]，協助鑑識人員透過簡單、方便的安裝與操作程序，快速的取得手機內部的各項重要鑑識資訊，達到協助案件調查證據採集與分析的目的。

2. 文獻探討

本研究著重於 Android 平台智慧型手機鑑識與鑑識軟體的開發與設計，依據研究所需之相關名詞與定義進行文獻研究。

2.1 智慧型手機

手機是現代人不可或缺的通訊工具，依據國家傳播通訊委員會的資料顯示，我國行動通訊用戶的普及率早在民國 91 年時就已超過 108% [3]，並且隨著科技的不斷進步，手機的功能也早已不在侷限於語音通訊，網際網路、電子郵件與全球衛星定位等功能都相繼整合到手機裡，並且正逐漸的與個人資訊助理(Personal Digital Assistant, PDA)走向整合 [11]，依據資策會產業情報研究所對智慧型手機的定義，如表 1 所示，智慧型手機在外觀上具有輕、薄、短、小的外型，在功能上，具備語音通訊、個人資訊管理(Personal information manager, PIM)、上網與電子郵件收發等功能，並且具有能與其他資訊產品進行資料交換或同步的能力 [2]。

表 1 智慧型手機定義 [2]

項目	定義
外觀	輕、薄、短、小，易於攜帶。
基本功能	具備數據與語音之無線通訊功能，且皆為內嵌式功能而非外加模組。
數據通訊	具備個人資訊管理功能、能連接網際網路、能收發電子郵件、並且能與其他資訊產品進行資料交換或同步。
語音通訊	需具備內嵌式語音通訊功能。
輸入方式	任何形式，不限於觸控式、按鍵式或語音輸入等。
處理器與作業系統	具備多工的嵌入式微處理器與作業系統。

2.2 Android 作業系統

Android 是一套基於 Linux 為核心的開放原始碼手機作業系統，最初是由 Google 於 2005 年時併購自手機作業系統開發公司 Android，之後由 Google 接續開發，一直到 2007 年 11 月 5 日由 Google 與另外 33 家手機設備製造商所組成的 Open Handset Alliance 共同公佈，目前 Android 的最新版本為 2.3 版，依據 Android Market 於 2010 年 7 月 1 日止的統計，Android 的版本市場占有比例分別為 1.5 版 21.3%、1.6 版 23.5%、2.1 版 53.1%與 2.2 版 1.8% [5]，Android 應用程式具有開發平台版本向上相容的特性，因此本研究採用 Android 1.5 版平台(API Level 3)進行開發，以確保所開發的鑑識軟體達到最大的版本相容性。

Android 系統架構共分為四層，如圖 1 所示，最底層是 Linux 核心與硬體驅動程式，它的上一層是提供底層軟體功能的原生 C\C++函式庫，與原生函式庫位於同一層的還有 Android 的執行環境，包含了核心函式庫與 Dalvik 虛擬機器，目的是提供 Android 應用程式一個執行的環境，再往上一層是應用程式框架，提供 Android 應用程式開發時所需的應用程式介面 (Application programming interface, API)，最上層是 Android 的應用程式 [6]，本研究使用 Android SDK，運用應用程式框架提供的應用程式介面，設計與實作 Android 平台智慧型手機鑑識軟體，提供手機內部鑑識相關資訊採集功能。

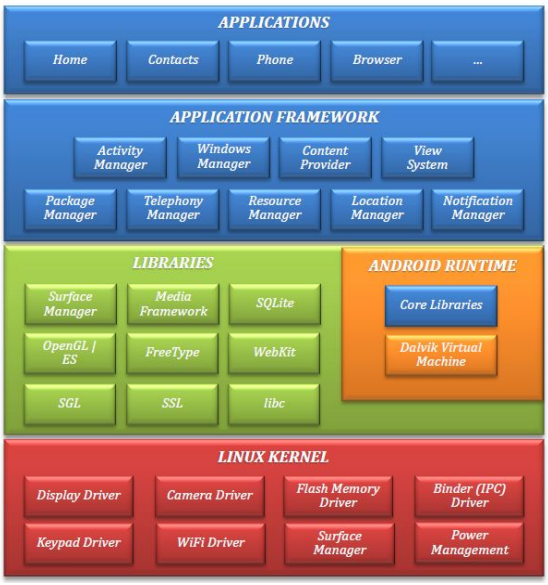

圖 1 Android 系統架構圖 [6]

2.3 數位證據

數位證據是以數位的形式儲存或傳送具有證據力的資訊 [12]。數位證據具有案件偵查上的價值，必須將它從實體設備當中擷取出來以證明發生過的事實。因此數位證據又被稱為電子證據 (Electronic evidence) [1]。

數位證據不同於一般物理性質的證據，它是以二進位的資料形態儲存於電子媒體中，因此數位證據具有易遭修改、複製、不易證明資料來源與資料完整性、無法直接感知或理解內容、不易採集擷取以及不易建立連結關係等特性 [1]。

在執行數位證據鑑識時，應確保所採用的方法能符合在不改變與破壞證物的情況下取得原始證物，並且可以證明所採集的證據來自扣押的證物，以及能在不造成證物改變的情況下進行資料分析的原則 [1]。

2.4 手機鑑識

手機鑑識是指在良好的鑑識條件下，

使用可接受的方法獲得手機內部的電子證據 [14]，隨著現代人越來越倚賴手機，手機內部的儲存資訊，如聯絡人、通話記錄、簡訊等，成為犯罪案件中非常重要的線索依據，並且隨著手機提供的功能越廣泛與多樣化，如全球衛星定位、網際網路、電子郵件、攝相等，使手機能提供的證據更加豐富，同時也增加了手機鑑識的重要性。

依據美國國家標準技術局手機鑑識指引，手機的鑑識流程可分為保存(Preservation)、採集(Acquisition)、檢驗及分析(Examination and Analysis)和報告呈現(Reporting)等四個階段 [14]。

- 保存(Preservation)：在不造成裝置本身與可卸除式儲存媒體內容改變的情況下，扣押犯罪嫌疑人所持有儲存著數位證據的裝置。
- 採集(Acquisition)：以製作映像檔或其它的方式，取得儲存於數位裝置本身與週邊裝置內的數位資料。
- 檢驗及分析(Examination and Analysis)：揭示採集到的數位證據，包含隱藏或刪除的內容，並且尋找證據中對於案件具有直接或潛在價值的資訊。
- 報告呈現(Reporting)：產生一份詳細的總結記錄，包含案件調查中所有採用的步驟與最後得到的結論。

2.5 手機鑑識工具

手機鑑識工具依其對鑑識目標手機資料採集的方式，可分為實體採集(Physical acquisition)與邏輯採集(Logical acquisition)兩種 [15]，實體採集的方式使用硬體連結線連接鑑識目標手機與電腦或鑑識專用硬體，透過專屬的通訊協定，驅動手機內部的系統服務，以位元為單位進行手機內部記憶體內容複製，邏輯採集的方式則可使用連結線連接鑑識目標手機與電腦或鑑識專用硬體，或是透過手機支援的外接式儲存媒體，如 SD 卡，做為鑑識軟體與採集資料存放的裝置，並且透過軟體對檔案系統存放的邏輯性資料進行讀取或複製的方式，取得手機內部儲存的資訊，表 2 為實體採集與邏輯採集兩種不同方式的比較。

表 2 實體採集與邏輯採集比較 (自行整理)

項目	實體採集	邏輯採集
硬體連結線	需要	可有可無
專屬通訊協定	需要	可有可無
在鑑識目標手機中安裝軟體	不需要	需要
資料採集方式	記憶體位元複製	透過作業系統 API 讀取資料或檔案
優點	取得完整記憶體內容，可進一步分析或恢復使用者已刪除資料 [9]。	不受硬體連結線規格與鑑識目標手機須實作專屬通訊協定的限制 [8]。
缺點	受硬體連結線規格與鑑識目標手機須實作專屬通訊協定的限制。	無法進一步分析或恢復使用者已刪除資料。

本研究進行同時，市場上的手機鑑識工具也開始逐漸支援 Android 平台智慧型手機，但無論是商業軟體如 Oxygen Forensic Suite、Paraben's Device Seizure 或 MOBILedit! Forensic [11]還是開放原始碼的 Open Source Android Forensics Application，皆與本研究相同採用邏輯採集的方式，進行 Android 平台智慧型手機鑑識，截至目前為止尚無任何 Android 平台智慧型手機鑑識工具採用實體採集的方式。

3. 系統架構

本研究設計與實作 Android 平台智慧型手機鑑識軟體，透過軟體的方式，採用邏輯採集的方法對手機內部儲存之資訊，如手機硬體、SIM 卡內容、通話記錄、簡訊、通訊錄、最後定位記錄、網頁瀏覽與網路搜尋記錄等資料進行採集，並且對採集所得之資料進行 SHA-256 單向雜湊函數運算與記錄，以確保採集資料的完整性。

完整的鑑識程序可分為前置作業與鑑識操作兩部份。

- 前置作業的目地是為鑑識工作準備所需的軟體與硬體工具，首先是將用來存放鑑識軟體與採集資料的 SD 卡，進行 FAT32 檔案系統格式化，讓它能夠被 Android 平台智慧型手機正確掛載與讀寫，接著再將本研究所開發的鑑識軟體複製到 SD 卡中。
- 鑑識操作是對 Android 平台智慧型手機執行鑑識工作的流程，如圖 2 所示，首先是卸載鑑識目標手機中原有的 SD 卡，然後置入前置作業所準備的 SD 卡，接著於鑑識目標手機中安裝儲存在 SD 卡中的鑑識軟體並執行，當鑑識軟體完成資料採集後，會將結果儲存於 SD 卡中，此時鑑識人員可選擇直在手機上觀看鑑識結果報表，或是卸除 SD 卡，取得鑑識結果報表以進行後續的資料分析。

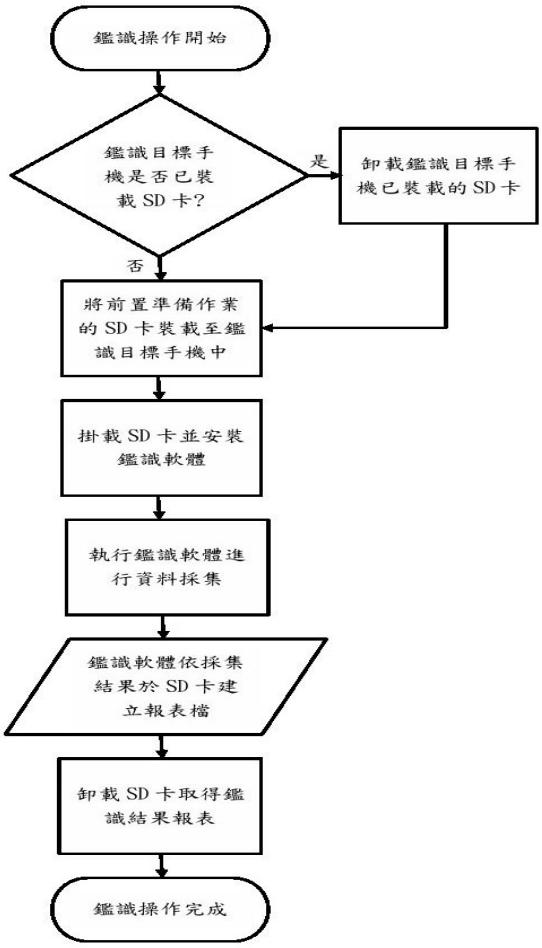

圖 2 鑑識操作流程圖

4. 系統實作

4.1 開發工具與環境

本研究使用 Android SDK 支援的 Java 程式語言，搭配 Eclipse 整合式開發環境 (Integrated development environment, IDE) 與提供完整 Android 應用程式開發、編譯、測試與除錯的 Android Development Tool (ADT) plugin，透過 Android SDK [4] (Android Platform 1.5, API level 3)提供的鑑識相關資訊提取功能 API，進行鑑識軟體設計與實作，表 3 為系統開發所使用的環境與工具。

表 3 系統開發環境與工具

作業系統	Windows XP
開發工具	■Java SE Development Kit (JDK) 6 ■Eclipse + Android Development Tool (ADT) plugin ■Android SDK (Android Platform, API Level 3)
程式語言	Java
測試手機	HTC Legend

4.2 系統功能

本研究使用簡潔、直覺的 GUI 設計概念進行軟體設計與開發，排除繁複的操作程序，協助鑑識人員以方便且快速的方式取得完整的 Android 平台智慧型手機鑑識資訊。

鑑識軟體執行起始時，鑑識人員需先輸入案件編號，之後按下「開始採集」按鈕進行鑑識資料採集，軟體畫面如圖 3 所示，鑑識人員輸入的案件編號將做為鑑識結果報表檔的檔名，並且儲存於 SD 卡中。

圖 3 鑑識軟體起始畫面

圖 4 為鑑識資料採集畫面，鑑識資料採集速度視鑑識目標手機的硬體規格與儲存的資料量而定，依實際測試的結果，以 HTC Legend (CPU: Qualcomm MSM7227, RAM: 384MB)手機採集硬體 13 項資訊並將採集結果進行 SHA-256 雜湊運算，僅耗時 0.014 秒(數據資料請參考圖 7)。

圖 4 鑑識資料採集畫面

完成鑑識資料採集後，鑑識人員可選擇直接在手機上進行鑑識結果報表檢視，或是結束程式,卸載 SD 卡取得鑑識結果報表，也可以回到鑑識軟體起始畫面，重新執行鑑識資料採集，功能選擇畫面如圖 5 所示。

圖 5 鑑識資料採集完成畫面

鑑識軟體提供鑑識結果報表檢視功能，如圖 6 所示。

圖 6 檢視鑑識結果報表功能畫面

鑑識結果報表，如圖 7 所示，以跨平台的 HTML (Hyper Text Markup Language) 檔案格式儲存，依鑑識人員輸入之案件編號命名，內容提供案件編號、鑑識日期以及各項分類採集資訊，如手機硬體、SIM 卡內容、通話記錄、簡訊、通訊錄、最後

定位記錄、網頁瀏覽與網路搜尋記錄等，能清楚且便捷的提供鑑識人員於各種不同作業系統平台使用網頁瀏覽器進行採集資料分析。

20110305AB

Sat Mar 05 21:01:03 GMT+08:00 2011

Build

Item	Value
BOARD	legend
BRAND	htc_asia_tw
DEVICE	legend
DISPLAY	FRF91
FINGERPRINT	htc_asia_tw/htc_legend/legend/legend:2.2/FRF91/
HOST	
ID	FRF91
MODEL	HTC Legend
PRODUCT	htc_legend
TAGS	release-keys
TIME	GMT+08:00 2010
TYPE	user
USER	unknown
HASH	62BAB124E516290200613CA4C390BC12CA9F412453C20E2838CD93CFF43F4B0
Time Consumption (sec.)	0.014

TelephonyManager

Item	Value
Device ID	
Deice Software Version	01
Line 1 Phone Number	null
Network Country Iso	tw
Network Operator	46692
Network Operator Name	中華電信
Network Type	NETWORK_TYPE_UMTS
Phone Type	PHONE_TYPE_GSM
SIM Country Code	tw

圖 7 鑑識結果報表畫面

5. 結論

Android 是一個發展快速、普及率遽增的智慧型手機作業系統，它具有彈性可擴充的軟體功能，同時也能提供比傳統手機更豐富多樣的鑑識資訊，本研究在 Android 平台智慧型手機普及率成長之初，即投入鑑識軟體的研究與實作，透過 Android 應用程式標準開發平台，採用邏輯採集的方式，實作跨廠牌與機種的 Android 平台智慧型手機鑑識軟體，並且提供能跨平台檢視的鑑識結果報表，協助鑑識人員能快速並且方便的取得鑑識資訊。

本研究未來將朝向豐富採集資訊與系統即時資訊採集 [13]的方向進行，並且克服某些機型進行 SD 卡卸除或裝載時，必須要關閉電源造成系統即時資訊遺失的問題，此外，本研究也計劃與市場上支援 Android 平台智慧型手機的商業鑑識軟體進行詳細測試比較，藉以提升本研究開發之鑑識軟體的證據力。

參考文獻

[1]王旭正、柯永瀚、ICCL 資訊密碼暨建構實驗室，***電腦鑑識與數位證據：資安技術、科技犯罪的預防、鑑定與現場重建***，博碩文化股份有限公司，2007。

[2]吳穩男、林宜隆、張志欉，*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*，台北大學 2009 年全國計算機研討會，2009。

[3]國家通訊傳播委員會新聞稿，*我國行動通信用戶普及率持續攀升至 116.6%，行動上網服務總用戶數達 1,820 萬戶，占行動通信總用戶比例提升至 67.5%，行動上網可望流行*，http://www.ncc.gov.tw/chinese/news_detail.aspx?site_content_sn=8&is_history=1&pages=5&sn_f=14091，February 2010。

[4]蓋索林，***Google! Android 2 手機應用程式設計入門第二版***，松崗資訊股份有限公司，2009。

[5]Android.com, *Platform Version*, http://developer.android.com/intl/zh-TW/resources/dashboard/platform-versions.html, August 2010.

[6]Android.com, *What is Android?*, http://developer.android.com/guide/basics/what-is-android.html, December 2009.

[7]Gartner, *Gartner Says Android to Become No.2 Worldwide Mobile Operating System in 2010 and Challenge Symbian for No.1 Position by 2014*, http://www.gartner.com/it/page.jsp?id=1434613, September 2010.

[8]G. Me, and M. Rossi, "*Internal forensic acquisition for mobile equipments,"* IEEE International Parallel & Distributed Processing Symposium 2008, 2008, pp. 1-7.

[9]M. Breeuwsma, M. DeJongh, C. Klaver, R. VanDerKnijff, and M. Roeloffs, "*Forensic Data Recovery from Flash Memory,"* Small Scale Digital Device Forensics Journal, Vol. 1, No. 1, June 2007.

[10] NIST, "*Smart Phone Tool Specification Version 1.1,"*

http://www.cftt.nist.gov/documents/Smart_Phone_Tool_Specification.pdf, April 2010.

[11] R. Ayers, W. Jansen, L. Moenner, and A. Delaitre, "*Cell Phone Forensic Tools: An Overview and Analysis Update,"* National Institute of Standards and Technology, March 2007.

[12] SWGDE and IOCE, "*Digital Evidence: Standards and Principles,"* Forensic Science Communications, Vol. 2, No. 2, April 2000.

[13] V. L. L. Thing, K. Y. Ng, and E. C. Chang, "*Live memory forensics of mobile phones,"* Digital Investigation, Volume 7, Supplement 1, August 2010, pp. S74-S82.

[14] W. Jansen, and R. Ayers, "*Guidelines on Cell Phone Forensics,"* National Institute of Standards and Technology, May 2007.

[15] W. Jansen, and R. Ayers, "*An overview and analysis of PDA forensic tools*," Digital Investigation, Volume 2, Issue 2, June 2005, pp. 120-132.