Android Live SD資料還原系統設計與實作

Design and Implementation of Android Live SD Data Recovery System

陳聖文
國立高雄師範大學資訊教育研究所
和平一路116號
高雄市802苓雅區
c.s.w.wendy@gmail.com

楊中皇
國立高雄師範大學資訊教育研究所
和平一路116號
高雄市802苓雅區
chyang@nknucc.nknu.edu.tw

陳世仁
資訊工業策進會資安科技研究所
和平東路二段106號11樓
台北市大安區
sjchen@iii.org.tw

摘要

手機鑑識是利用符合法律規範的方式對手機進行資料的採集、儲存、分析、還原手機被上鎖、隱閉、刪除的通話記錄、簡訊、通訊錄、電子郵件、照片、聲音檔等。做爲法律上證明或反駁的證據。依據美國國家標準技術局(National Institute of Standards and Technology, NIST)手機鑑識指引，手機鑑識流程可分爲保存(Preservation)、採集(Acquisition)、檢驗及分析(Examination and Analysis)和報告呈現(Reporting)等四個階段[12]。手機鑑識的過程中資料採集是一個重要的環節，在合理的鑑識條件下，使用可接受的方法獲得手機內部的電子證據[12]，手機資料採集的方式，可分爲實體採集(Physical acquisition)與邏輯採集(Logical acquisition)兩種[11]，目前大多數手機鑑識軟體採邏輯採集的方法，這樣的方法採集出來的資料可直接識別，但都面臨著相同的問題，已刪除的資料無法還原且內部採集工具必需安裝至手機內部，利用呼叫內建函數的方式進行採集動作，這樣的採集方式，令人遲疑，是否違背了鑑識科學中保留現場的觀念。

本研究提出一種Live SD的概念，相當於電腦鑑識中的Live CD/DVD/USB的概念，並利用Recovery原理實踐於Android智慧型手機中製作實體採證與資料還原，這樣的採證方式有別於目前大多數手機鑑識軟體所使用的採證方法，進而分析與還原刪除資料。

關鍵詞: Android、Recovery、Live SD、手機鑑識、採集方法。

Abstract

Mobile Forensics is defined as to legally collect, store, analyze, recover the call records, SMS, contact list, e-mails, photos and audios which are locked, hidden, or deleted in the mobile phones. With mobile forensics, data can become the evidence for legal proof or objection. According to National Institute of Standards and Technology(NIST), the mobile forensic process consists of four parts, including Preservation, Acquisition, Examination & Analysis, and Reporting. Data acquisition is the key part which can acquire internal electronic evidences in mobile devices under reasonable forensic conditions. There are two main mobile data acquisition methods, including Physical Acquisition and Logical Acquisition. Presently, most of the mobile forensics tools are implemented with logical acquisition. However, the method will result in the problem where the forensics tools are required to firstly install in the mobile devices and the acquisition can in turn be performed. This often raises the concern if it is against the concept of scene reservation.

Our research proposes the concept of Live SD in mobile phones, which can be treated similar with the Live CD/DVD/USB in computer forensics. Moreover, Recovery theory is implemented to realize the physical acquisition and data recovery in Android smart phones. This method is different from most of the ones embedded in present mobile forensic software and can improve the ability for data recovery.

Keywords: Android, Recovery, Live SD, Mobile Forensics, Acquisition

一、前言

智慧型手機已經成爲現代人不可或缺的隨身數位載具，已超過以往我們對手機功能的認知，智慧型手機提供了穩定的平臺、人性化的功能，配合今日無線網路與3.5G行動網路便利的環境，造就了智慧型手機的快速成長，高度的機動性，令人愛不釋人，根據國際研究暨顧問機構Gartner公佈，2011年8月智慧型手機市調報告，2011年第二季銷售量達4億2,870萬支，較2010年同季成長16.5%，其智慧型手機作業系統市佔率，Android平臺市率佔已達43.4%，位居智慧型手機市佔率冠軍[10]，Android平臺打著開放式系統的口號，從2007年11月5日 [6] 出來後市佔率不斷攀升，一直都是智慧型手機市場上最大的勁敵，Android智慧型手機功能建全且強大，手機內部的儲存資訊，如聯絡人、通話記錄、簡訊等，成爲犯罪案件中非常重要的線索依據，並且隨著智慧型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、攝影等，使手機能提供的證據更加豐富，同時也增加了手機鑑識的必要性。

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爲保存(Preservation)、採集(Acquisition)、檢驗及分析(Examination and Analysis)和報告呈現(Reporting)等四個階段 [12]。手機鑑識的過程中資料採集是一個重要的環節，在合理的鑑識條件下，使用可接受的方法獲得手機內部的電子證據 [12]，手機資料採集的方式，可分爲實體採集(Physical acquisition)與邏輯採集(Logical acquisition)兩種 [11]；實體採集

的方式，以硬體連結線與鑑識目標手機作專屬通訊協定，進行記憶體位元複製，取得完整記憶體內容，進一步分析或恢復使用者已刪除資料 [7]；邏輯採集的方式，透過作業系統API讀取資料或檔案，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 [14]，但無法進一步分析或恢復使用者已刪除資料。目前大多數手機鑑識軟體採邏輯採集的方法，且都面臨著相同的問題，軟體必需安裝至手機內部，才可進行資料採集動作，這樣的採集方式，令人遲疑，是否違背了鑑識科學中保留現場的觀念。

本研究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 [16]，提出一種Live SD的概念，利用Recovery的原理實踐於Android智慧型手機中製作實體資料採證，這樣的採證方式有別於目前大多數手機鑑識軟體所使用的採證方法。本研究將於電腦端針對實體資料庫進行分析與已刪除資料的還原。

二、文獻探討

本研究著重於Android平臺智慧型手機實踐Live SD手機鑑識實體採證並進行實體資料庫進行分析爲研究重點，依據研究所需之相關名詞與定義進行文獻研究。

1. 手機鑑識

手機中的資料都是電磁記錄，凡指針對手機內數位資料所進行的鑑識，皆稱爲數位鑑識。一般而言，數位鑑識的目的是鑑定調查的數位證據，擷取手機內的各項重要資訊，包含通聯紀錄、通訊錄、簡訊、手機多媒體資料等實體電腦的犯罪。手機鑑識的程序一般分爲四個階段 [12]：保存(Preservation)、採集(Acquisition)、檢驗及分析(Examination and Analysis)、報告呈現(Reporting)。

(1)保存(Preservation)：主要目的確定搜索及識別可能存放有數位證據之設備，數位證據因其無形的特性，造成鑑識過程中容易遭破壞，或採集證據時因處理不當受損，無妥善保存數位證據原始狀態，將可能危及到數位證據的佐證能力。

(2)採集(Acquisition)：將從犯案現場中取得的數位設備，以擷取映像檔方式或其它方法，取得儲存於數位裝置中的數位資料。

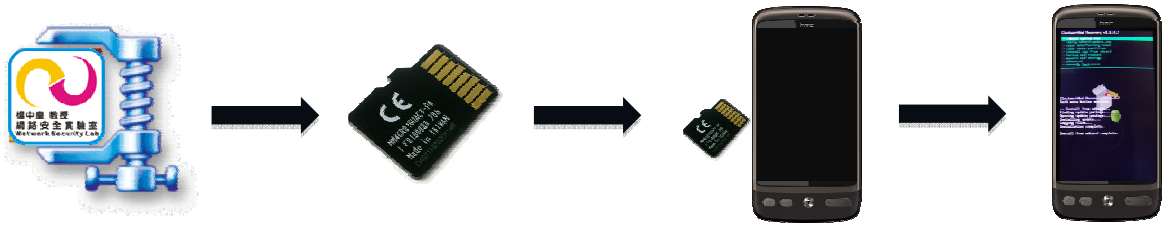
(3)檢驗及分析(Examination and Analysis)：檢驗是將蒐集到的數位證據揭示，包含隱藏檔案或遭刪除的檔案，分析則是將採集到的數位證據，透過現有資料將證據中與案情高度相關的證據數據化或結合，以利協助釐清案情。

(4)報告呈現(Reporting)：將數位證據分析結果，以清晰明瞭方式呈現，如報表文件，以提升法庭審理作業效率。

2. Live SD

Live CD/DVD[17]預先配置軟體的可開機的儲存媒體中，讓使用者可以在不需要使用硬碟的情況下，執行儲存媒體中的軟體，經由可開機媒體開機使用，而不會更動到現有系統。Live SD爲Live CD/DVD的延伸觀念，可滿足使用者儲存資料的需求，並解決先前CD/DVD唯讀不可更動的限制，提供更快的存取速度，配合依照使用者需求建置的系

統與軟體建置與Live媒體中，使Live媒體的應用更加多元化，成爲可移動之系統、平台、軟體與工具。其基本原理如圖一。



圖一: Live SD運作原理

3. 數位證據

數位證據又稱爲電子證據。數位證據與傳統證據不同之處，在於數位證據是以數位的型態儲存或傳輸、它是可以在法庭成爲證據用的數位電子資訊。數位證據 [5] 並非可以直接察覺的具體存在事物，通常以電磁或電波的方式儲存於電子媒體上。因爲這個特性，它必須藉助電子設備加以讀取、分析或顯示，呈現爲視覺可判讀的資訊型態，因此在法律上不易如實體證據般[9]。

由於數位資料非實體的物質，其具以下幾個特性 [2]：難以蒐集萃取與保存、無法直接感知與理解、易於複製竄改與刪除、難以證實來源與完整性、難以建立連結關係等性質。鑑識人員在採證的過程中，應注意幾個基本原則：在取證的過程中，應在不會對原始證物有任何變更的情況下進行、必須要有辨法證明所採集之證物源自扣押的證物、進行鑑識分析時亦不能對證物造成更動或破壞[1]。

根據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[16] 所定義的智慧型手機數位證據，如表一所示。

4. Android啓動流程

Android作業系統是由Linux衍生而來，在開機的過程當中與Linux是類似的，Bootloader(一般常見的bootloader有許多種，包含fastboot、blob、U-Boot…等) [8][19]是在執行Linux Kernel前的段程式，系統開機由bootloader對CPU、記憶體、RS232、網路卡…等相關硬體作初始化的設定，接著複製Flash ROM中的Kernel image至記憶體，然後設置Linux kernel的啓動參數並開始執行記憶體中的Linux kernel，將CPU控制權交給Linux kernel。Linux kernel在執行完系統初始化設定之後，會將控制權轉移給User space的程式：init(init一般爲busybox [8])，然後busybox會產生Shell讓使用者可以透過特定指令與作業系統互動。Dalvik是Google開發一個支援Java語法的Virtual Machine，其特色是Register-based Virtual Machine，而非Stack-based Virtual Machine(Java Virtual Machine)，因此Dalvik可以針對其支援的平臺作最佳化處理，這也是針對嵌入式系統所作的設計[4][15] ，Android開機流程如圖二所示。

OS Level，電源啓動後，由Bootloader載入Linux kernel後，初始化kernel，載入相關驅動程式。kernel完成後，載入init process，切換至user-space，結束kernel的循序過程，進入排程模式。

Android Level，由init process開始，讀取init.rc並啓動重要的外部程式，例如：Service Manager、Zygote與System Server。

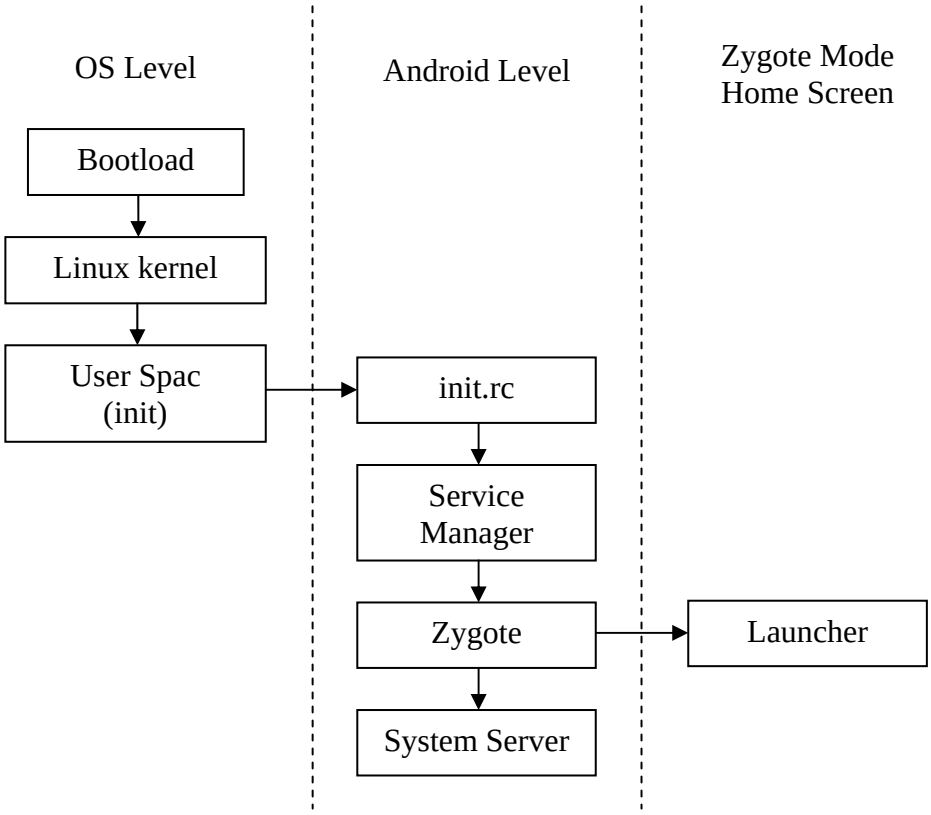
Zygote Mode，Zygote觸發System Server啓動後，進入Zygote Mode，於Socket等候命令。桌面環境實作完成。

表一: 智慧型手機數位證據

手機數位證據	儲存位置
國際移動設備識別碼(MEI)	GSM設備內存
移動設備識別碼(EID)、電子序列號(ESN)	CDMA設備內存
縮位撥號號碼(ADNS)	SIM卡儲存器
地理位置資料、定位點、GPRS LOCI數據	SIM卡儲存器
服務提供商名稱(SPN)	SIM卡儲存器
集成電路卡識別碼(ICCID)	SIM卡儲存器
最後號碼重撥(LND)	SIM卡儲存器
國際移動用戶識別(IMSI)	SIM卡儲存器
移動用戶國際ISDN號碼(MSISDN)	SIM卡儲存器
短信(SMS、EMS)	SIM卡儲存器
個人訊息管理(PIM)資料 (如通訊錄、行事曆、待辦事項清單、任務、記事)	設備內部記憶體
應用程式檔案(例如：Word檔、Excel檔…等)	設備內部記憶體
瀏覽記錄(例如：我的最愛、存取過的網站、暫存檔…等)	設備內部記憶體
通話記錄(來電和撥出電話)	設備內部記憶體
多媒體訊息(MMS)/電子郵件(E-Mail)和相關的資料(例如：聲音、圖片、視訊…等)	設備內部記憶體
文件存儲、獨立的文件(例如：聲音、圖片、視訊…等)	設備內部記憶體
GPS相關資料(經度和緯度坐標)	設備內部記憶體

5. Android Recovery

Android利用Recovery模式，還原出廠設定、更新patch及更新firmware。Recovery一般是使用官方所提供的套件(update.zip) 達到更新與還原的動作，將該套件置入SD卡，於開機時使用組合鍵開機進入Recovery模式，Recovery模式隨著手機廠牌與型號不同而各有所不同的組合鍵[20]如表二所示。



圖二: Android作業系統開機流程圖

Recovery模式啓動後，請模式會參考套件中的一個觸發指令腳本(META-INF/com/google/update-script)，該指令腳本可操控Recovery的過程，例如format BOOT…等。該指令腳本執行完畢後，方可完成Recovery動作。Android Recovery流程如圖三所示。

6. 資料刪除與還原

儲存媒體在儲存檔案資料的時候，必須記錄檔案的相關資訊，如名稱、大小和儲存相關叢集位置等，這些資訊都會記錄在檔案配置表中。當裝置存取檔案的時候，會在檔案配置表中找到檔案所在的叢集位置，才能存取該檔案。

作業系統在刪除檔案時，只會將磁碟或記憶卡中的目錄紀錄及資料所在的儲存區域標示爲可利用空間，並未將所儲存的資料作消磁歸零的動作。例如在Windows作業系統中，執行刪除檔案的動作時，其相對應目錄紀錄的第一個字元會被更改爲十六進制值E5，並且將配置給該檔案的檔案配置表記錄重置爲零，以表示其對應的儲存空間是可利用的，Windows作業系統在存取這樣的代碼時，就會知道它所對應的是已經刪除的檔案，但實際上作業系統並不會去改變這些儲存空間內的資料內容，除非這些儲存空間被後來的檔案覆蓋利用[13]。

在行動裝置內的資料復原是指將內部記憶體所儲存的檔案資料，包括ROM、分段FAT檔案系統、二進位檔案、已刪除檔案及記憶卡內的資料、資料庫記錄，還原儲存媒

體中原有的證據資料，並找出所有刪除或僞裝在內部記憶體及外部記憶卡中的檔案資料與記錄。

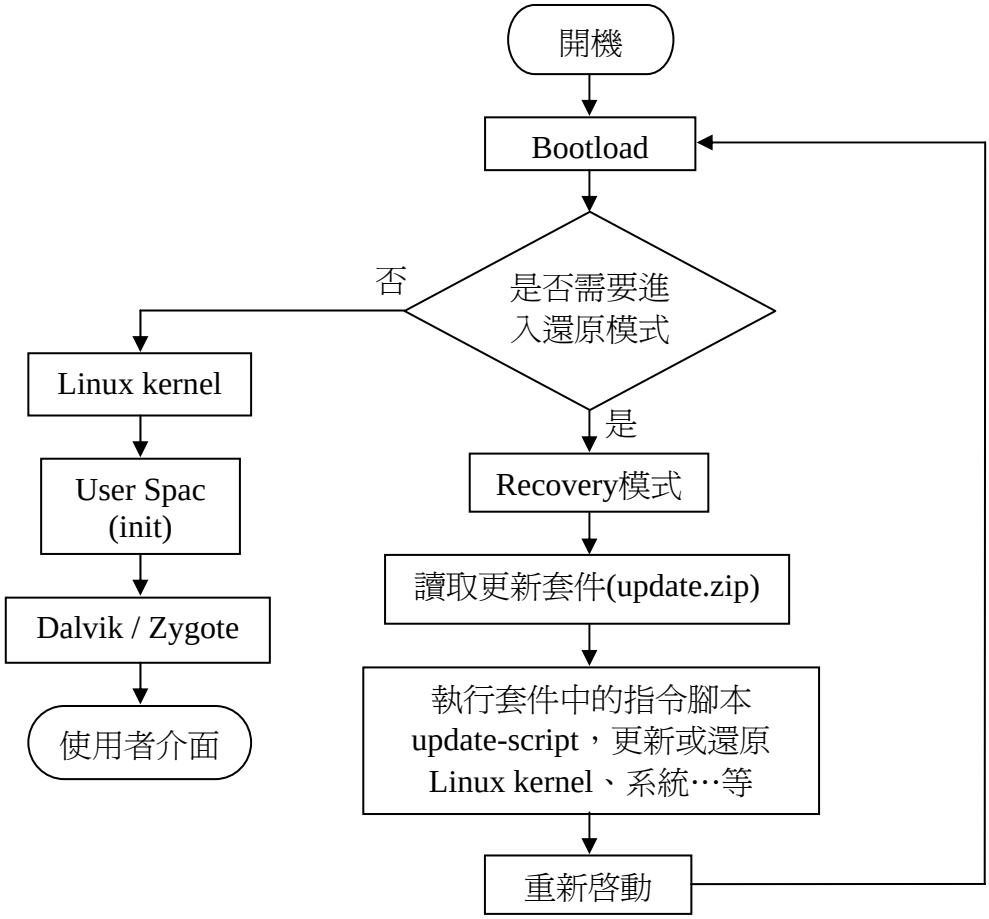
表二: 進入Android Recovery模式的組合鍵

廠牌	型號	組合鍵
Motorola	Droid	Power + x
Motorola	Milestone、Defy	Power + Vol Up
HTC	G1	Power + Camera
HTC	T-Mobile	Power + Home
HTC	Hero	Power + Home
HTC	Tattoo	Power + Home
HTC	Nexus One	Power + Vol Down
HTC	Legend	Power + Vol Down
HTC	Desire	Power + Vol Down
HTC	Desire Z	Power + Vol Down
HTC	Wildfire	Power + Vol Down
HTC	Aria	Power + Vol Down
HTC	Desire HD	Power + Vol Down
HTC	Incredible S	Power + Vol Down
HTC	Wildfire S	Power + Vol Down
HTC	Sensation	Power + Vol Down
Samsung	Captivate	Power + Vol Up + Vol Down
Samsung	Galaxy Tab	Power + Vol Up
Samsung	Nexus S	Power + Vol Up
Samsung	I9000	Power + Home + Vol Up

進行數位鑑識時，在行動裝置上所採集的檔案資料包含實體萃取（Physical Extraction）和邏輯萃取（Logical Extraction）兩種[17][21]，表三爲實體萃取與邏輯萃取兩種不同方式的比較[3]。詳細說明如下：

6.1 實體萃取

資料儲存於該硬體的儲存設備、元件及各類電子媒體當中，進行數位鑑識時，必須使用該媒體或該硬體儲存設備的存取方法將資料萃取出來。意指不使用作業系統的命令提示字元來溝通或交換資料。實體萃取的方式一般使用硬體連結線連接鑑識目標裝置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，以位元爲單位進行手機內部實體記憶體內容做複製，取得完整記憶體內容，進一步分析或恢復使用者已刪除資料 [7]。



圖三: Android Recovery流程圖

表三: 實體採集與邏輯採集比較

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
揮發性資料	低	高
採集資料所需權限	高	低
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 [7]。	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 [14]。
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。

6.2 邏輯萃取

資料必須經由相關原始資訊資源中萃取出來，這些資源包含了日誌檔及資料庫等，例如使用作業系統的命令提示字元，可以透過通訊協定提供若干命令，允許應用程式或電腦與行動裝置系統溝通並交換資料。邏輯萃取的方式一般也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，做爲鑑識軟體與採集資料存放的裝置，並且軟體透過作業系統的API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，但這樣的採集方法無法分析或恢復使用者已刪除資料。

三、Android Live SD資料還原系統架構與設計

本研究設計與實作Android平臺智慧型手機以Live SD方式進行實體資料採集，Live SD利用Recovery模式觸發啓動，啓動後以實體採集的方式進行對目標手機內部底層資料庫進行實體檔案採集，完整的Android Live SD資料還原系統可分爲實體資料採集與資料鑑識分析工作兩部份。

1. 實體資料採集工作

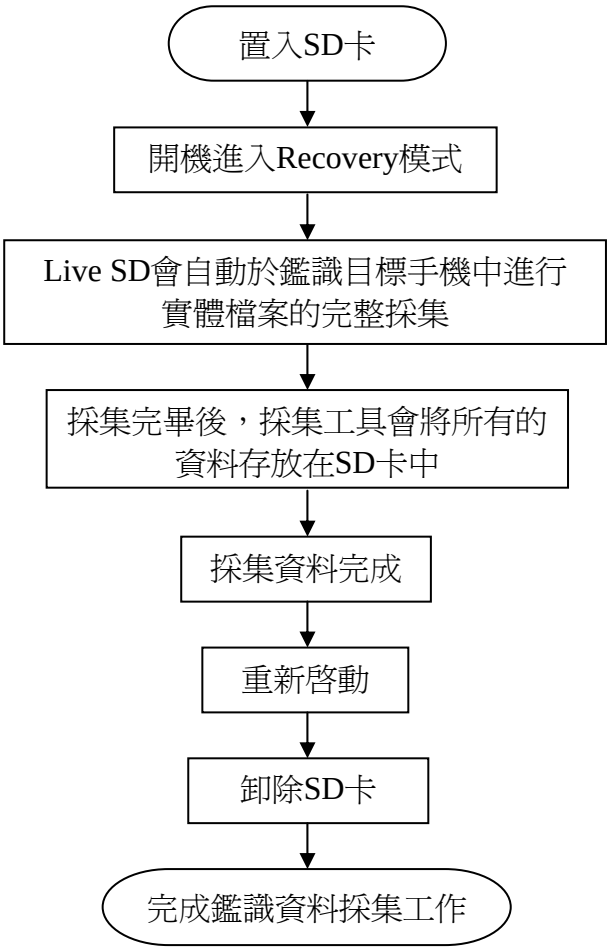
將用來存放鑑識軟體與採集資料的SD卡，進行FAT32檔案系統格式化，讓它能夠被Android平臺智慧型手機正確掛載與讀寫，接著再將本研究自行設計與開發的鑑識工具包(update.zip)複製到SD卡中。於目標手機中置入鑑識SD卡，接著於開機的過程中進入Recovery模式，Live SD會自動於鑑識目標手機中進行實體檔案的完整採集，資料採集完成後，採集工具會將所有的資料存放在SD卡中，重新啓動系統，卸除SD卡，取得相關內部資料以進行後續的資料鑑識分析。實體採集工作流程如下圖四所示：

2. 資料鑑識分析

取得目標手機中的實體資料庫後，將資料庫匯入本研究Live SD Android智慧型手機鑑識系統進行鑑識分析工作，採集資料如下表四所示：

表四:實體採集資料

實體位置	採集檔案	相關資訊
/data/data/com.android.providers.contacts/databases /contacts2.db	contacts2.db	通訊錄與通聯記錄
/data/data/com.android.providers.media/databases /internal.db	internal.db	多媒體資料庫
/data/data/com.android.providers.telephony/databases/ mmssms.db	mmssms.db	簡訊
/data/data/com.android.providers.calendar/databases /calendar.db	calendar.db	行事曆



圖四: 實體採集工作流程圖

四、系統開發與實現

本研究利用Android平臺智慧型手機容許使用者自行由Recovery模式的操作功能，做到從開機就可以合法的干預開機流程與開機程序，並設計與實作一個符合鑑識資料採證的觸發套件，讓該鑑識套件自動化的完成完整的內部資料採集的動作，採集完畢後並於Live SD Android智慧型手機鑑識系統進行資料庫鑑識分析。表五爲Android Live SD資料還原系統開發所使用的環境與工具。

將Live SD置入鑑識目標手機中，開機進入Fastboot(也稱HBoot)。該模式一定會存在，但會因各廠牌手機的設計不盡相同，而有所差異。本研究以HTC Desire爲測試手機，於開機時按住降低音量鍵，方可進入Fastboot模式。如圖五所示。

於Fastboot模式選擇Recovery，切換至Recovery模式。如圖六所示。

於Recovery模式下選擇apply sdcard:update.zip的選項，執行鑑識採證工具，開始將手機低層實體資料庫採集至SD Card。系統執行過程如圖七所示。

將Live SD採集完畢後的低層資料庫，匯入本研究Android智慧型手機鑑識系統進行資料鑑識分析。下列範例爲，以通訊錄爲主要示範，利用該平臺進行資料鑑識分析與還原。圖八爲上傳採集出來的實體資料庫，通訊錄(contacts2.db)資料庫上傳。

上傳完成後，系統會自動於畫面中秀出使用者所上傳的資料庫分析結果。如圖九所示。

系統右側選單會自動顯示，該資料庫是否還有其他相關的資訊可以進行資料可視化。並提示可將該資料庫裡面已經被刪除的資料記錄做還原分析。如圖十所示。

整個資料還原的原理，事實上，在應用程式(通訊錄)對資料庫進行刪除資料的動作時，只是在刪除資料的某個特定欄位，如deleted、status或data_type等，加上註解已刪除；但事實上資料並真正的被執行刪除動作，而是在應用程式讀取該筆資料時，因爲特定欄位被註解已刪除，所以應用程式判定該筆資料已刪除。本研究資料還原的動作，也是利用相同刪除的原理反相推理，將特定欄位已經被註解已刪除的欄位值，恢復正常值，進行資料的分析動作。

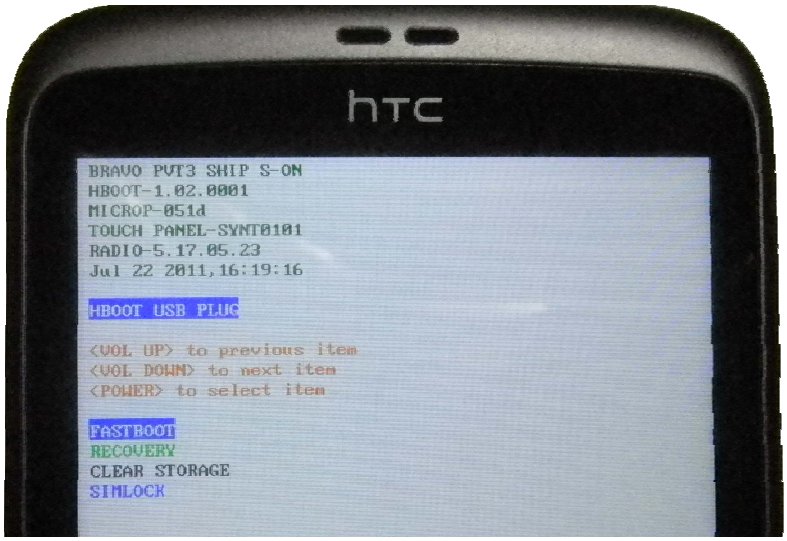
表五: Android Live SD資料還原系統開發環境與工具

作業系統	Windows 7
開發工具	Java SE Development Kit (JDK) 6 Apache Tomcat 7.0.12 Eclipse 3.6.2 SQLite 3
程式語言	Shell-Script Update-Script Java Server Pages
測試環境	HTC Desire T-Mobile

五、結論

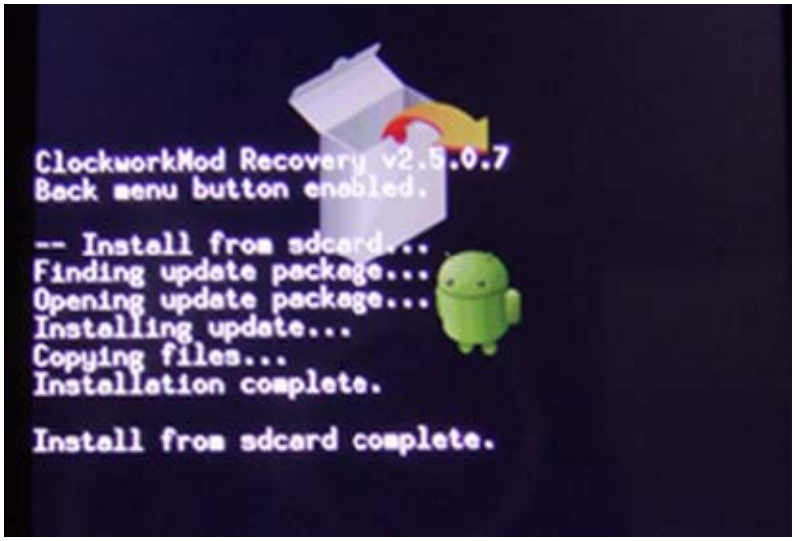
Android是一個發展快速、普及率遽增的智慧型手機作業系統，它具有彈性可擴充軟體的功能，同時也比傳統手機更令人依賴，內有豐富的個人資訊。近年來資訊犯罪案件層出不窮，個資外洩，殭屍網路等等名詞已不再是新聞。因此，除了使用者的日常防範外，鑑識人員如何在事件發生後，從受害手機上蒐集任何蛛絲馬跡，成爲當前必須面臨的重要課題。目前使用的商業版數位鑑識軟體成本過高，另外都是採內部邏輯採集的方式，這樣的採集方式，常令人遲疑內部軟體安裝後是否已經違背了鑑識科學中的改變現場的大忌加上邏輯採集的方式是利用API做數據的提取，這樣的方式可能無法將已遭受到破壞的資料還原。

本研究利用Android平臺容許使用者自行合法更新套件的特性，並參考電腦鑑識中的Live CD/DVD/USB鑑識之原理[22]，設計與實作Live SD實體採證工具，並以Web Based的系統做資料庫的鑑識分析，Live SD實體採證方式於開機進入Recovery模式後執行鑑識套件系統底層實體資料庫進行採集動作，鑑識軟體即不用安裝且在採集的過程中使用實體檔案的匯出，並針對資料庫進行資料刪除之探討，並將這樣的概念設計與實作，加入友善的操作介面，發展成爲Live SD Android智慧型手機鑑識系統。本研究未來將朝向受損之實體檔案採集還原與系統即時資訊鑑識[18]的方向進行研究。



圖五: Fastboot模式

圖六: Recovery模式



圖七: 系統執行過程

圖八: 上傳通訊錄(contacts2.db)資料庫

圖九: 通訊錄鑑識資料分析

[謝啓]

本研究依經濟部補助財團法人資訊工業策進會「101年度資通安全與資料防護技術發展計畫」辦理，本研究部分成果承蒙國科會計畫經費補助（NSC 98-2221-E-017-010-MY3），特此致謝。

圖十: 通訊錄資料還原分析

參考文獻

[1] 王旭正、林祝興、ICCL-資訊密碼暨建構實驗室，數位科技安全與鑑識：高科技犯罪預防與數位證據偵蒐，臺北：博碩文化出版公司，2009。

[2] 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，臺北：博碩文化出版公司，2007。

[3] 楊景翔、楊中皇，“Android平台智慧型手機鑑識軟體設計與實現”，*第22屆國際資訊管理學術研討會(ICIM 2011)*，2011。

[4] 鐘文昌，“Android作業系統移植之研究與實現”，*國立臺北科技大學碩士論文*，2009。

[5] Ahmed, R. and Dharaskar, R. V., “Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective,” *6th International Conference on e-Government (ICEG 2010)* , Cape Town, South Africa, September 2010.

[6] Android.com, http://www.android.com/about/timeline.html, September 2011.

[7] Breeuwsma, M., De Jongh, M., Klaver, C., Der Knijff, R. V. and Roeloffs, M., “Forensic Data Recovery from Flash Memory,” *Small Scale Digital Device Forensics Journal*, 2007: Volume 1, No. 1, pp. 1-17.

[8] BusyBox, http://www.busybox.net, September 2011.

[9] Distefano, A. and Me, G., “An Overall Assessment of Mobile Internal Acquisition Tool,” *Digital Investigation*, 2008: Volume 5, Supplement 1, pp. S121-S127.

[10] 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, August 11, 2011.

[11] Jansen, W. and Ayers, R., "An Overview and Analysis of PDA Forensic Tools," *Digital Investigation*, 2005: Volume 2, Issue 2, pp. 120-132.

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

[13] Kruse II, W. G. and Heiser, J. G., "Computer Forensics: Incident Response Essentials," *Lucent Technologies*, 2004: pp.17-18, pp.77-78.

[14] Me, G. and Rossi, M., "Internal Forensic Acquisition for Mobile Equipments," *IEEE International Parallel & Distributed Processing Symposium 2008*, 2008: pp. 1-7.

[15] Moko365, http://www.moko365.com, October 2011.

[16] National Institute of Standards and Technology, *Smart Phone Tool Specification*, Version 1.1, April 12, 2010.

[17] Pillay, H., *The Magic of Live CDs*, Free Software Magazine, February 2005.

[18] Thing, V.L.L., Ng, K.Y. and Chang, E.C., "Live Memory Forensics of Mobile Phones," *Digital Investigation*, 2010: Volume 7, Supplement 1, pp. S74-S82.

[19] U-Boot Bootloader at SourceForge.net, http://sourceforge.net/projects/u-boot, September 2011.

[20] Vidas, T., Zhang, C., and Christin, N., "Towards a General Collection Methodology for Android Devices," *11th Digital Forensics Research Workshop (DFRWS 2011)*, New Orleans, LA. August 1-3, 2011.

[21] Wright, T., *The Field Guide for Investigation Computer Crime: search and seizure basic part three*, Security Focus Incident Handling focus, 2000.

[22] Yang, C.H. and Yen, P.H., "Fast Deployment of Computer Forensics with USBs," *The First International Workshop on Cloud, Wireless and e-Commerce Security (CWECS 2010)*, Fukuoka, Japan, November 2010.