Symbian 智慧型手機內部採集工具設計與實作

陳聖文[1]　　楊中皇[2]
[1]國立高雄師範大學 資訊教育研究所 c.s.w.wendy@gmail.com
[2]國立高雄師範大學 資訊教育研究所 chyang@nknucc.edu.tw

摘要

隨著資訊科技的進步及數位時代的來臨，智慧型手機(Smart Phone)功能越來越強大也越來越普及，根據拓墣產業研究所預估(EETimes，2009)，2010 年全球智慧型手機出貨量持續成長達 2.35 億，年成長率 29%。並就 Gartner 2010 年全球智慧型手機平台市場佔有率統計顯示，Symbian 市場佔有率 41.2%、Research In Motion 市場佔有率 18.2%、Android 市場佔有率 17.2%、iOS 市場佔有率 14.2%、Microsoft Windows Mobile 市場佔有率 5%、Linux 市場佔有率 2.4%、Other 市場佔有率 1.8%，強大的軟硬體功能帶動各層面的廣泛運用，例如：全球定位系統應用，以及更強的網路功能。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增加。然而手機內的所有檔案均為電磁紀錄，故此類的犯罪與傳統犯罪型態存在著極大的差異。

本研究提出了一種內部採集證據的方法，並使用 Symbian C++(Coultion, P., Edwards, R. and Clemson, H.，2007)進行系統之設計與實作。目前採集手機證據的方法，必需透過特定的硬體裝置或使用電腦經由手機傳輸線與手機連線後，做證據採集的動作。一旦沒有該手機傳輸線，將無法採集證據。本研究所提出的方法只需要將軟體安裝至一塊記憶卡上，經由內部採集工具(Distefano, A. and Me, G.，2008)，採集手機內部通聯記錄、通訊錄、簡訊等資料，有效解決設備經由傳輸線採證的問題。

關鍵詞：智慧型手機、手機鑑識、數位鑑識、Nokia、Symbian

Symbian 智慧型手機內部採集工具設計與實作

1. 前言

隨著資訊科技的進步及數位時代的來臨，智慧型手機(Smart Phone)功能越來越強大也越來越普及，手機的功能不再是只有打電話接電話的功能，還結合了行動通訊、數位相機、無線上網、文書編輯、藍芽傳輸、全球定位系統等功能。因其便利性高及儲存容量大，智慧型手機(Smart Phone)所儲存及處理常會涉及到個人或組織的機密資訊，包括通聯記錄、行事曆、上網紀錄、電子郵件、簡訊、組織機密檔案等，這些資料均以數位方式記錄、儲存，並透過網路或可移除式裝置與電腦進行資料同步傳輸、更新。

諾基亞為全球行動通訊的領導品牌，根 Gartner 統計，2010 年全球手機市場佔有率統計顯示，諾基亞手機的全球市場佔有率有高達 34.2%，坐擁手機龍頭；在通訊技術方面，諾基亞 3G 手機的全球市場佔有率超過 30%，並針對多媒體影音、遊戲、音樂和企業解決方案等領域，透過提供手機、解決方案、系統設備和應用服務等創新產品，打造通訊產業中的超級品牌。智慧型手機(Smart Phone)提供我們便利的生活，也成為心懷不軌人士犯罪的利器，進行不法之行為，而我們如何找出這些違法的行為軌跡，則有賴於數位鑑識的技術。依據美國國家標準局(National Institute of Standards and Technology)手機鑑識的程序一般分為四個階段：保存(Preservation)、蒐集(Acquisition)、檢驗及分析(Examination and Analysis)、報告呈現(Reporting)。這些資訊在犯罪偵查的過程當中均扮演著關鍵性的數位證據，往往成為破案的關鍵。在採證手機犯罪的現場，已不再適用傳統的蒐證方法，鑑識人員需依賴鑑識工具取得數位證據。

2. 文獻探討

本研究著重於 Symbian 智慧型手機系統的內部資料蒐證，依據研究所需之相關名詞進行文獻探討。

2.1 智慧型手機

根據國際數據資訊(IDC)針對智慧型手機之定義，乃指結合手機與個人數位助理之整合型行動裝置(Converged Mobile Device)，除了基本的語音通訊功能之外，尚可進行無線上網、收發電子郵件、個人資料處理(Personal Information Management；PIM)，以及遊戲、多媒體等應用軟體的擴充。國內方面資策會亦對其定義(吳穩男、林宜隆、張志泉，2009)(陳盈嘉，2007)。

表一: 智慧型行動電話之定義(資料來源：尤克熙，資策會 MIC 研究報告)

	項目	定義
1	外觀	輕、薄、短、小，易於攜帶。
2	基本功能	具備數據與語音之無線通訊功能，且皆為內嵌式而非外加之模組。

3	數據通訊	1.具備 PIM 功能，其中包含行程表、通訊錄、工作表、記事本、與電腦同步等功能。 2.可連接 internet、收發 e-mail。
4	語音通訊	須具備內嵌式語音通訊功能。
5	輸入方式	任何形式，不拘於觸控式、按鍵式或語音輸入等。
6	處理器與作業系統	擁有多工的嵌入式微處裡器與作業系統。

2.2 數位證據

數位證據又稱為電子證據。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、它是可以在法庭成為證據用的數位電子資訊。數位證據(Ahmed, R. and Dharaskar, R.V.，2008)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。因為這個特性，它必須藉助電子設備加以讀取、分析或顯示，呈現為視覺可判讀的資訊型態，因此在法律上不易如實體證據般(Distefano, A. and Me, G.，2008)。

由於數位資料非實體的物質，其具以下幾個特性(王旭正、柯永瀚、ICCL-資訊密碼暨建構實驗室，2007)：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(王旭正、林祝興、ICCL 資訊密碼暨建構實驗室，2009)。

2.3 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，皆稱為數位鑑識。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為四個階段(Raghav, S. and Saxena, A.K.，2009)(Jansen, W. and Ayers, R.，2007)：保存(Preservation)、蒐集(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) 蒐集(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。

2.4 手機鑑識工具

2.4.1 Oxygen Forensic Suite

Oxygen Forensic Suite 為美國 Oxygen 這家公司所設計，專為鑑識 Smart Phones 和 PDA 的軟體，特別是對 Smart Phones，超過 500 種各大廠牌手機支援，客戶包括司法單位、警察單位、軍方、海關與其他政府當局，自 2002 年已經成功在世界超過 50 個國家。

其主要功能有可鑑識的資料包括 SIM 卡的資料、電話簿(包括名字、電話、傳真、電子信箱，大頭照和其他聯繫訊息)、未接/已撥/撥入來電、記事本資料、日曆事件(會議，備忘錄，提醒，紀念日和生日)、文字簡訊資料(簡訊，log，資料夾，被刪除的簡訊資料)、多媒體訊息、電子郵件、GPRS， EDGE， CSD， HSCSD， Wi-Fi session log 與網路流量、照片、影片、聲音檔案、錄音、記憶卡裡的全部檔案，包括安裝的應用程式、廣播電台數據庫等(Jansen, W. and Ayers, R.，2007)。

2.4.2 Device Seizure

Device Seizure 為 Paraben.co 所研發，專為鑑識手持數位裝置的產品，整合了 Cell Seizure 與 PDA Seizure 功能，支援大部份手機、PDA、GSM 手機的 SIM 卡、特定的 GPS 裝置的鑑識。與其他由資料管理軟體轉變成的數位鑑識工具不同，Device Seizure 擁有專屬自己的功能。

主要功能及特性為針對手機內的文字、多媒體訊息、電話簿、聲音檔、影像檔、通聯紀錄、行程等進行實體或邏輯萃取資料(鄧少華、邱俊霖，2008)。還原已刪除的資料、利用 MD5 及 SHA-1 兩種雜湊值，驗證檔案正確性。檢視內部檔案的屬性、瀏覽紀錄及書籤功能。還可針對檔案資料以文字模式或十六進制模式進行檢視、檢視 Windows Mobile 登錄檔、系統檔案資料。最後以 HTML 格式或純文字格式產生鑑識報告等，可鑑識目前各系統的智慧型手機(Gilbert, K.，2009)。

2.5 Symbian

Symbian OS 是專門為手機裝置而設計的操作系統，包含相關函式庫、UI 架構、共用工具等，由 Symbian Ltd. 開發維護。以 Symbian 作業系統為基礎的手機用戶介面有 UIQ、諾基亞的 S60、S80、S90、NTT DoCoMo 的 FOMA 等。Symbian 是以 EPOC 為基礎，架構與許多桌上型作業系統相似。支援先佔式多工 (pre-emptive multitasking)、多執行緒 (thread)、記憶體保護 (memory protection)等技術(Symbian Foundation，2010)。其架構如圖 1 所示。

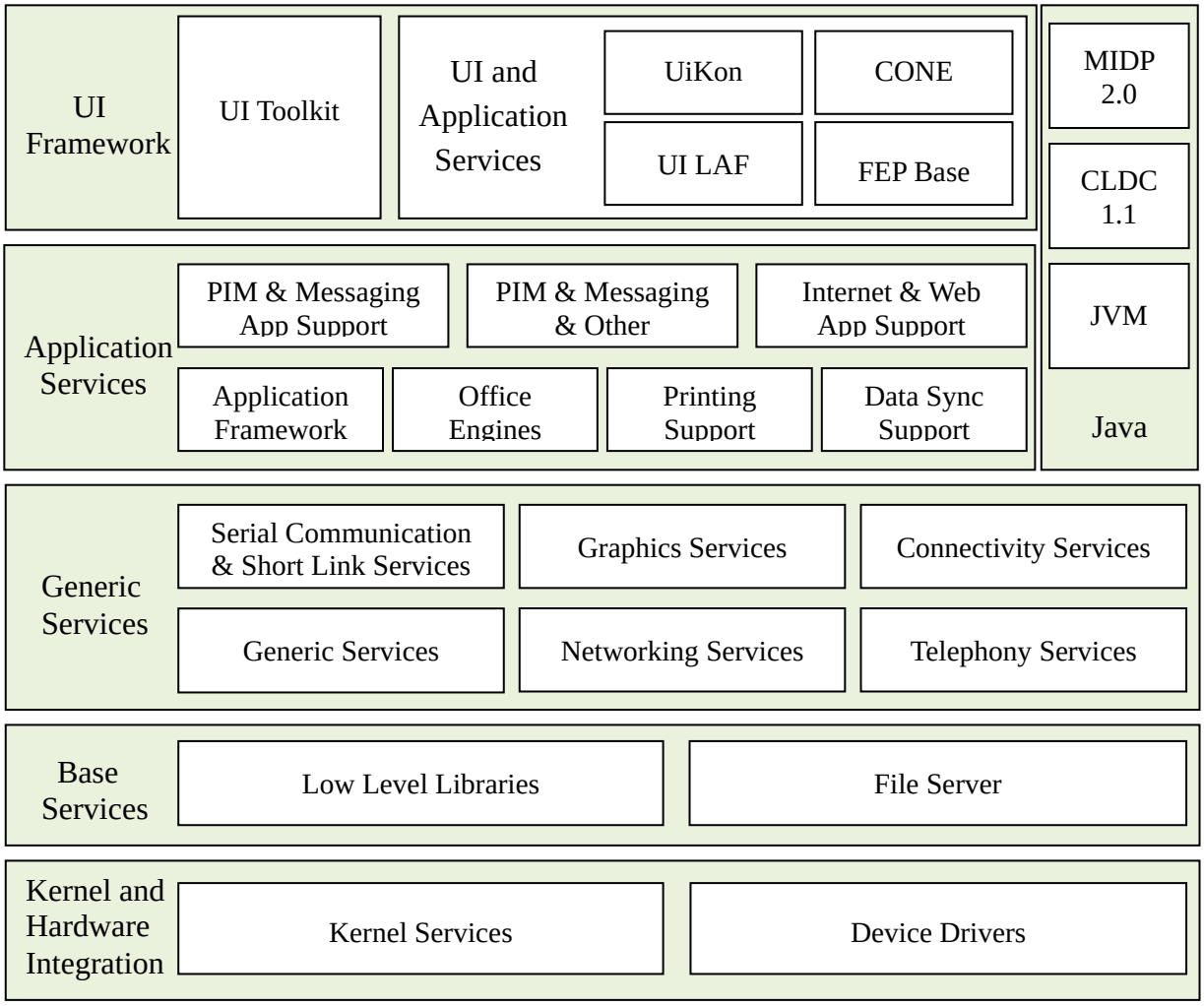

圖 1 Symbian 平臺架構(資料來源：Symbian Foundation)

UI Framework：UI Framework 是 Symbian 作業系統最頂層服務，為建構使用者介面提供的框架和資源。(Mokhonoana, P.M. and Olivier, M.S.，2007)

Application Services：該層為 Symbian 作業系統的應用程式，提供獨立於使用者介面的支援。這些服務大致上被分成三個主要的部份：

- 系統服務，如基本的應用程式架構，可以被所有應用程式使用。
- 提供基本功能服務，如簡訊和多媒體權限，可以被應用程式的多個類使用。
- 支援單個應用程式的服務，如個人資訊管理(PIM)和應用程式。

Java：Symbian 的 Java 基於 Java ME MIDP 2.0 和 CLDC 1.1。Symbian 作業系統從開始發展就支持 Java，早期的 Java 系統是基於 Personal Java 和 Java Phone。

Generic Services：Generic Services 層提供了 Symbian 作業系統的服務器、框架和資源庫，從而將基本的系統擴充成一個較完整的作業系統(Sales, J.，2005)(Harrison, R. and Shackman, M.，2007)。

Base Services：Symbian 作業系統的 Base Services 提供了使用者底層的服務。這些服務只針對作業系統核心相關資源。Base Services 將作業系統的核心擴充成為一個可用的最小平臺。

Kernel and Hardware Integration：Symbian 操作系統的最底層包含了作業系統核心本身和硬體連接介面，包括物理設備的驅動和各種支援。

3. 系統架構

本研究實作一個手機內部採集工具，將工具放在記憶卡中，將記憶卡插入手機，再將工具安裝至手機記憶卡上，執行內部採集工具，採集手機內部通聯記錄、通訊錄、簡訊等相關資料。為了確保採集完整資料，本研究所實作的方式是直接將底層的相關資訊資料庫直接複製至記憶卡。系統鑑識流程如圖 2

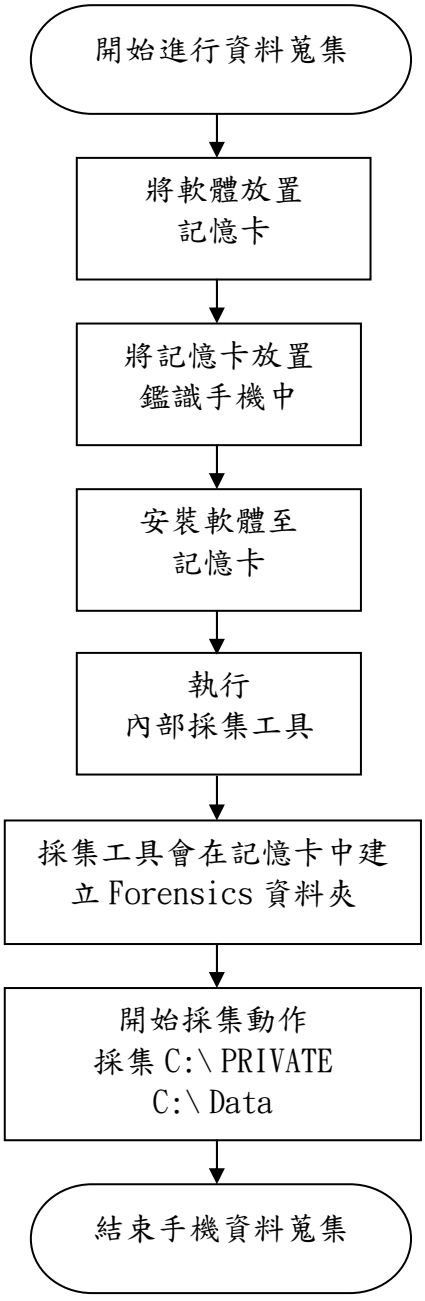

圖 2 系統流程圖

4. 系統實作

4.1 開發工具與環境

程式開發部份,本研究使用 Symbian C++作為開發語言,Symbian C++是 Symbian OS 基本的程式語言，Symbian C++是從 C++改進而來。為了在適於手機這種資源較少的環境下執行，改進 C++讓 Symbian C++開發更是快速便利。表二為本研究所測試使用的環境。

表二: 開發工具與環境

開發平臺	Windows XP
開發工具	1. Active Perl 2. J2SE Development Kit 3. Carbide C++
程式語言	Symbian C++
測試手機	Nokia E90 S60v3

4.2 系統功能

本研究利用 Symbian C++設計與實作一個內部採集系統，直接在手機上執行，將帶有內部採集工具之記憶卡插入手機中，將工具安裝至手機記憶卡中進行內部採集工作，由於系統是安裝至記憶卡上，故不會破壞目前手機的狀態，系統開啟後會自動將畫面導向至 Console 模式，並在 Console 下執行系統功能。系統開啟畫面如圖 3

圖 3 系統畫面圖

按下手機上 Options 按鍵，系統將會出現工作選單畫面如圖 4 所示。

圖 4 系統執行畫面圖

選擇 Acquisition 後，按下 Select，系統將會自動切換至 Console 模式，畫面如圖 5 所示。

圖 5 系統執行畫面圖

按下任一鍵，系統將開始執行手機內部資料採集工作，系統在執行的過程中會將正在複製的資料出現在畫面上如圖 6

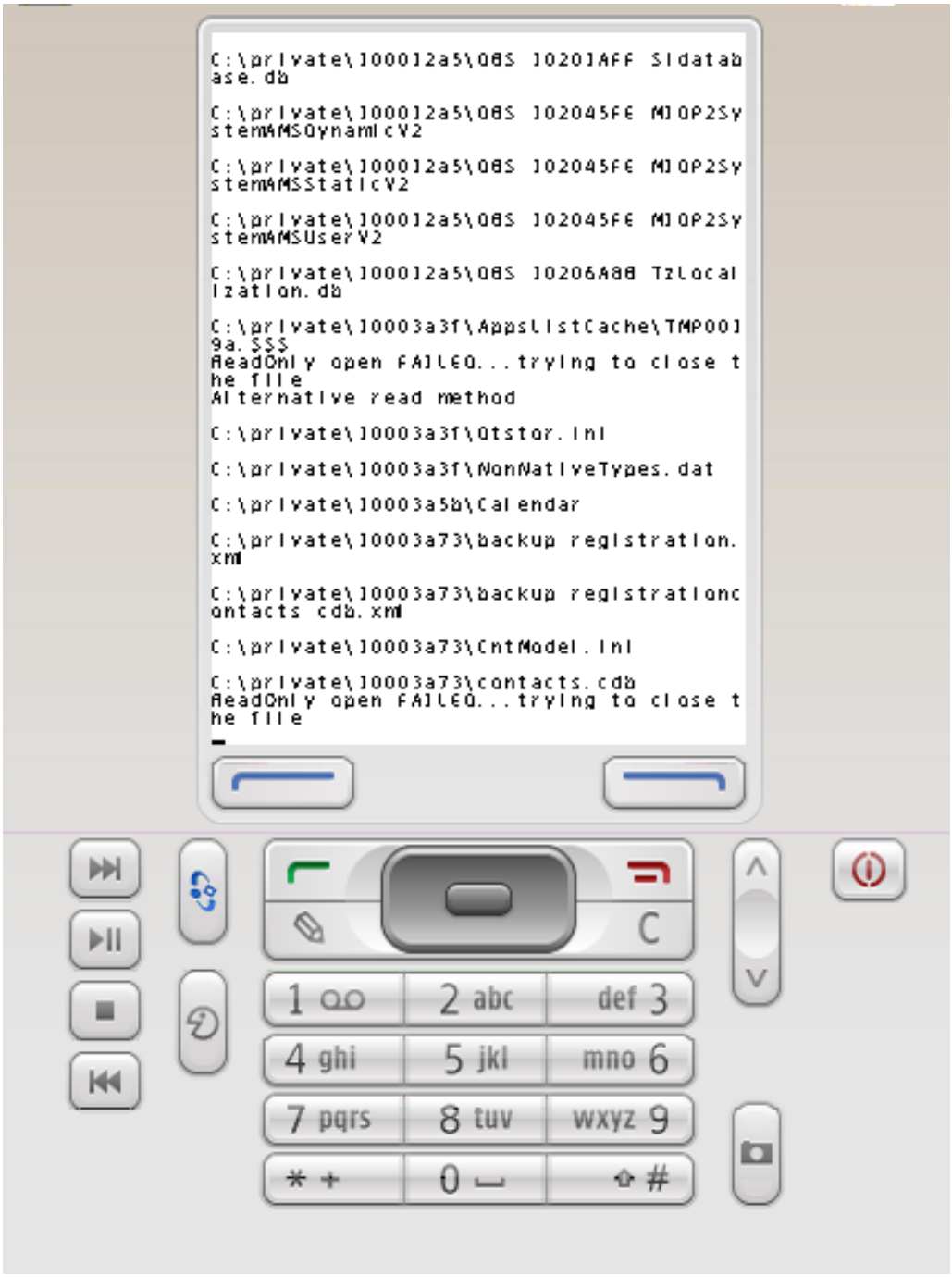

圖 6 系統執行畫面圖

資料採集完成後系統會在記憶卡上建立一個資料夾(Forensics)，在這個 Forensics 的資料夾中包含 Symbian 底層的數據庫與使用者資料夾，相關資料夾整理如表三所示：

表三: Forensics 目錄列表

目錄	存放檔案相關功能
SD Card\Forensics\PRIVATE\100012a5\	通訊錄、藍牙連線設備清單
SD Card\Forensics\PRIVATE\10003a3f\	手機應用程式捷徑
SD Card\Forensics\PRIVATE\10003a5b\	行事曆
SD Card\Forensics\PRIVATE\10003a73\	快速撥號設定
SD Card\Forensics\PRIVATE\1000484b\	簡訊
SD Card\Forensics\PRIVATE\10005399\	備份日誌
SD Card\Forensics\PRIVATE\10005903\	時間設定
SD Card\Forensics\PRIVATE\100059c9\	語言和地理位置設定相關
SD Card\Forensics\PRIVATE\10005a3e\	內建播放器播放歷史記錄
SD Card\Forensics\PRIVATE\10008d38\	內建瀏覽器保存的書籤
SD Card\Forensics\PRIVATE\10008d39\	書籤、網站 Logo 圖示
SD Card\Forensics\PRIVATE\101f401d\	通訊記錄
SD Card\Forensics\PRIVATE\101f413c\	SIP(Session Initiation Protocol)設置
SD Card\Forensics\PRIVATE\101f4cd2\	程式 UID 和圖示路徑數據記錄(應用程式安裝數據記錄文件)
SD Card\Forensics\PRIVATE\101f5027\	鬧鐘設定
SD Card\Forensics\PRIVATE\101f72a6\	安裝軟體的證書
SD Card\Forensics\PRIVATE\101f7989\	WAP 設定
SD Card\Forensics\PRIVATE\101f8530\	COOKIESC
SD Card\Forensics\PRIVATE\101f875a\	開機自啟動程式
SD Card\Forensics\PRIVATE\101f8857\	副檔名關聯程式訊息
SD Card\Forensics\PRIVATE\101f9a06\	聊天室
SD Card\Forensics\PRIVATE\101f9cfe\	內建詞典
SD Card\Forensics\PRIVATE\10202be9\	系統檔案
SD Card\Forensics\Data\Games\	遊戲
SD Card\Forensics\Data\Images\	圖片
SD Card\Forensics\Data\Installs\	已安裝文件
SD Card\Forensics\Data\Others\	其他
SD Card\Forensics\Data\Sounds\	鈴聲
SD Card\Forensics\Data\Videos\	影片

5.結論與未來發展

現代社會幾乎人手一支的手機，同時也是犯罪集團的最愛。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(者)手機中蒐集任何蛛絲馬跡，成為當前必須面臨的重要課題。目前大多數採集手機資料的方法都是透過鑑識箱或經由電腦連線取出資料，這樣的做法傳輸線的更新速度成了一個問題。

本研究提出了一種不同於目前採集手機資料的方法並加以實作，系統直接將最原始的資料來源也就是資料庫，直接複製出來。這樣的方法可以有效的幫助傳統手機鑑識，使用手機鑑識箱採集手機內部資料時，所面臨的傳輸介面不足的情況。這樣的方法可以不使用任何設備，將手機內部資料傳輸出來，也可以避免資料在傳輸的過程中發生意外，未來的研究將針對採集到的資料進行分析、線上鑑識與還原刪除資料。

參考文獻

1. 王旭正、林祝興、ICCL 資訊密碼暨建構實驗室，2009，數位科技安全與鑑識：高科技犯罪預防與數位證據偵蒐，博碩文化出版公司。
2. 王旭正、柯永瀚、ICCL-資訊密碼暨建構實驗室，2007，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，博碩文化出版公司。
3. 吳穩男、林宜隆、張志欶，民 98，探討智慧型手機之數位證據鑑識作業程序與工具之研究，2009 第十五屆資訊管理暨實務研討會，中華民國資訊管理學會。
4. 陳盈嘉，民 96，影響智慧型行動電話第三方應用軟體廠商網絡連結對象決策之因素研究，國立中央大學企業管理學系研究所碩士論文。
5. 鄧少華、邱俊霖，2008，行動裝置 PDA 資料復原鑑識之研究，2008 第三屆數位教學暨資訊實務研討會，台南 南台科技大學。
6. Ahmed, R. and Dharaskar, R.V. "Mobile Forensics: an Overview, Tools, Future trends and Challenges from Law Enforcement perspective", 2008.
7. Coultion, P., Edwards, R. and Clemson, H. "S60 Programming A Tutorial Guide", John Wiley & Sons, Ltd., 2007.
8. Distefano, A. and Me, G. "An overall assessment of Mobile Internal Acquisition Tool", 2008.
9. EETimes, http://www.eettaiwan.com/ART_8800590111_617723_NT_6f45f34a.HTM
10. Gartner, http://www.gartner.com/it/page.jsp?id=1421013
11. Gilbert, K. "GROUP TEST Digital forensics", SC Magazine, 2009. http://www.scmagazineuk.com/digital-forensics-2009/grouptest/176/
12. Harrison, R. and Shackman, M. "Symbian OS C++ For Mobile Phones Volume 3, Application Development for Symbian OS v9", John Wiley & Sons, Ltd., 2007.
13. Jansen, W. and Ayers, R. "Guidelines on Cell Phone Forensics", NIST SP 800-101,2007. http://csrc.nist.gov/publications/nistpubs/800-101/SP800-101.pdf
14. Mokhonoana, P.M. and Olivier, M.S. "Acquisition of a Symbian Smart phone's Content

with an On-Phone Forensic Tool", 2007.
15. Raghav, S. and Saxena, A.K. "Mobile Forensics: Guidelines and Challenges in Data Preservation and Acquisition", 2009.
16. Sales, J. "Symbian OS Internals, Real-time Kernel Programming", John Wiley & Sons, Ltd., 2005.
17. Symbian Foundation, http://www.symbian.org/

Design and Implementation of Internal Acquisition Tool in Symbian Smart Phone

Sheng-Wen Chen[1] Chung-Huang Yang[2]

[1] Graduate Institute of Information & Computer Education, National Kaohsiung Normal University Kaohsiung, Taiwan, c.s.w.wendy@gmail.com

[2] Graduate Institute of Information & Computer Education National Kaohsiung Normal University Kaohsiung, Taiwan, chyang@nknucc.edu.tw

Abstract

With the fast IT progress and the coming of digital times, the functions which Smart Phone offers are even more powerful and popular. According to the estimation of Topology Research Institute (EETimes，2009), the global quantity of Smart Phone in 2010 will continue to grow up to 0.235 billion, with 29% annual growth rate. From the global market share statistics of Gartner (Gartner，2010), Symbian occupies 41.2.4%, Research In Motion 18.2%, Android 17.2%, iOS 14.2%, Microsoft Windows Mobile 5%, Linux 2.4% and the others 1.8%. Powerful software and hardware bring various applications, including GPS and better internet connection. Smart Phones embed rich personal information with high mobility, and may further induce the increase of Smart Phone commitment. However, the files in the phone are recorded in electromagnetic manner, so it is very different from the traditional crime commitment.

A solution of Internal Acquisition Evidences is proposed in this paper, and implemented the system with Symbian C++ (Coultion, P., Edwards, R. and Clemson, H.，2007). The present evidence collection in mobile phones must be performed with specific hardware or connection between PCs and phones via transmission lines. Once the transmission lines are not available, it is impossible to perform the task of evidence collection. The solution proposed in this paper only suggests to setup the software in the SD cards, and perform the internal communication records, personal directories, and messages with Internal Acquisition Tool (Distefano, A. and Me, G.，2008), which may effectively solve the problem of lack of transmission lines.

Keywords: Smart Phones, Mobile Forensics, Digital Forensics, Nokia, Symbian.