PC 及 PDA 操作平台之即時通訊之證據關聯分析研究

高大宇
海岸巡防署海洋巡防總局海務組

劉心玫
中央警察大學資訊管理系

王旭正
中央警察大學資訊管理系
sjwang@mail.cpu.edu.tw

摘要

個人電腦或個人數位助理經常出現在現代社會的各方面，它可能被用來作為犯罪工具，並保存證據。當個人數位助理功能運用範圍日漸擴大且重要時，發展技術連結個人電腦及個人數位助理的重要性便日漸增加。不幸的是，這樣的關連技術仍存在科學上的限制。本文探究即時通訊軟體在對話記錄、顯示圖片、傳送檔案及共享資料夾等方面的證據性關連。對話記錄能夠識別特定對象，其他則能用來作為剖繪之用，以縮小嫌犯範圍，降低調查範圍。6W1H（何人 Who、何時 When、何地 Where、何事 What、何物 Which、為何 Why 及如何 How）問題策略作為發現事實的起始點，三 E 方法則從教育、執法與工程等三個面向進行證據分析，並從犯罪學、事件調查與鑑識科學角度輔助剖繪工作的進行，以導入高科技犯罪的有利切入方向。

關鍵詞：數位鑑識、行動鑑識、6W1H 問題、3E 方法、智慧型手機

1. 前言

移動辦公的通訊需求將加速手機與個人電腦的整合趨勢。行動電話（即手機）是使用於較廣範圍內的無線攜帶型電話設備。90 年代前價格昂貴，之後大幅降價，成為日常生活不可或缺用品。第二代手機(2G)以數位型態傳送的 GSM 和 CdmaOne 為主，可語音通信、收發簡訊(短消息、SMS)及 MMS(多媒體簡訊)。過去的電腦犯罪著重現場犯罪偵查及數位鑑識，較少提及行動設備，目前產業正邁向第三代手機（3G）發展。然行動設備科技攜帶性方便且操作容易，日漸成為犯罪行為不可或缺的一部分。

手機外觀包括液晶螢幕和按鍵（觸摸螢幕無實體按鍵），除典型電話功能外，包含個人數位助理(Personal Digital Assistant; PDA)、遊戲機、MP3、 照相機、錄音、GPS 等多項功能。純 PDA 雖已式微，選購結合手機功能的智慧型手機已成趨勢。未來，智慧型手機將更智能化、微型化、安全化與多功能化。比一般打電話、傳簡訊、玩遊戲、照相的手機具備更多特殊功能，最簡單的定義就是「PDA」加上「手機」，將個人數位助理功能加入手機內。偏重安全和數據通訊、加強數位資料研發、邏輯運算能力及個人隱私保護。

1.1 個人數位助理

個人數位助理(PDA)分狹義及廣義兩種，狹義 PDA 指僅作為記事本的相關電子產品，功能著重固定結構化之單一管理個人資訊，無法因應使用者需求進行修改、新增或客製化；廣義 PDA 則泛指掌上型電腦，與電子記事本最大差別在於掌上型電腦不只針對單一記事功能，更結合強效硬體性能、多樣應用軟體和開放式作業系統等，不僅可使用網際網路瀏覽網頁、收發電子郵件，更能

視個人需求進行修改、新增、刪除相關應用軟體，讓 PDA 使用更趨多元化[2, 4]。PDA 具可攜性及特殊軟硬體架構等許多不同於個人電腦的特性，需特殊作業系統及檔案管理系統，達到自動壓縮檔案、執行程序或管理資料等功能。為便利攜帶、節省記憶體，採揮發性記憶體儲存資料，執行運作端看電力作用有無。ROM 存放作業系統的內部資訊和所需資料，RAM 存放使用者個人管理資料，這些資料均會因蓄電不足或電力耗盡導致資料的遺失。目前大部份 PDA 手機廠都搭配微軟的 WIN CE 軟體，如同一般簡易型 PC 類之小行動秘書，只安裝 WINDOWS 系統，其他軟體均未安裝，僅能使用 IE 瀏覽器上網、使用 Media Player 看影片聽音樂、使用 Outlook Explorer 收電子郵件、設定連絡人、提醒該辦事項(行事曆)等等。內建 WIFI(無線上網功能)，BlueTooth(藍牙功能)，GPS 導航(衛星定位功能)、3.5G 視訊電話或上網功能。

1.2 智慧型手機

智慧型手機（Smart Phone)，泛指整合各種運算、多媒體功能，採用類 PC 嵌入式作業系統手機，採用允許安裝第三方應用程式之開放式作業系統的行動設備，隨時撥打電話功能。主要供應商包括 Nokia、Samsung、HTC、Research in Motion (RIM)及 Apple 等，常見作業系統包括 Symbain、Windows Mobile 及 Android 平台等，有行事曆、聯絡人等 PDA 常用個人資訊管理(Personal Information Manager; PIM)功能。智慧型手機得提供便捷多樣的多媒體裝置及行動電話服務，讓使用者享受有效率、富彈性的工作生活。透過簡單操作，不受地點限制，使用應用軟體及人性化介面，透過全球移動通訊系統(UMTS)、3.5G 行動上網（HSDPA)、無線網路（W-LAN）及藍芽技術等標準傳輸工具，進行檔案傳輸等多樣行動服務。

智慧型手機如同隨身小電腦，因須執行使用者自行安裝軟體，所需效能和記憶體容量較高，但也因開放軟體安裝，穩定性（存在當機可能）不如一般手機。智慧型手機作業系統的不斷推陳出新，如觸控介面（HTC Touch 系列產品)、捲軸捲動技巧(微軟 WM 內建 IE)、多點觸控技術（Apple iPhone）或點擊區塊放大功能(Opera 公司的 Opera Mini 瀏覽器）等不同操作方式，均不斷刺激市場的創新發展。取源於使用者觀點的應用系統改善機制，各有優缺，如何適合使用者需求，乃須持續探究。

數位證據以電磁紀錄方式儲存於電腦等資訊科技設備儲存媒體上，具易竄改、來源不易確定、資料完整性需驗證等特性。本文從數位證據角度探討微軟生活通訊（Windows Live Messenger; WLM）運用於個人電腦(Personal Computer; PC)與個人數位助理(PDA)之即時通訊軟體應用關連分析（分以 WLM 及 Pocket MSN 為例)，期提供開發廠商、犯罪學者、執法者、系統管理者、電腦安全專家、法律專家和電腦犯罪偵查學習人員等，未來處理數位證據議題時，能採行合宜政策與策略。

第 2 節討論即時通訊的數位證據存留，檢視相關數位證據的保存結果，模擬嫌犯使用電腦與行動裝置登入 WLM 對話後，透過鑑識工具檢視比較微軟生活通訊(WLM)在兩者間的數位稽證、使用差別與問題限制。第 3 節將 6W1H 問題融入 PDA 鑑識實作分析過程，根據分析結果，釐清事件的關連，作為提供解決方法的參考。第 4 節為綜合應用。第 5 節歸納本文的結論。

2. 即時通訊的數位證據存留

MSN、Yahoo 即時通、Skype 等工具，屬青少年族群較廣泛使用的即時通訊軟體。即時通訊提供網際網路即時傳遞訊息的通訊系統，具紀錄保存、實用方便、成本低廉及廣泛流行等特性。功能包含個人對個人/多人文字訊息交流、多媒體影音交流、語音視訊會議、共享與傳送檔案及企業內部使用等。舉凡販賣毒品、走私槍枝、詐欺、傳播色情、網路援交及散佈電腦病毒等問題，均可能成為使用即時通訊進行犯罪的新興管道。本文針對PC與PDA裝置之微軟即時通訊軟體，採集數位證據，進行關連分析。研究軟體，說明如下：

(1)PC：WLM

微軟生活通訊(WLM)是微軟公司開發的即時訊息客戶端軟體，包含一系列線上應用服務的套裝軟體，透過網路瀏覽器介面提供服務。

(2)PDA：Pocket MSN

Pocket MSN 搭配 PDA 裝置使用，可直接使用 Windows Live ID 帳號(hotmail.com、msn.com、yahoo.com等)登入。

2.1 WLM 的數位證據

即時通訊軟體傳送文字訊息、語音及影像，WLM 包含下列資料：

(1)對話紀錄

個人對個人或多人會客室之對話內容，以 XML 檔案形式存於 C:\Documents and Settings\User\My Documents\我已接收的檔案\使用者帳號\記錄資料夾。

(2)圖片檔案

利用圖片檔案分辨使用者身份，存於 C:\Documents and Settings\User\Local Settings\Application Data\Microsoft\Messenger\使用者帳號@hotmail.com\ObjectStore\UserTile 內。

(3)傳送檔案

除對話訊息外，傳送或接收檔案存於 C:\Documents and settings\user\My Documents\我已接收的檔案。

(4) 共享檔案

共享檔案存於 C:\Documents and Settings\User\My Documents\我的共用資料夾。帳號設定常與姓名、生日等個人資訊相關，所屬群組(如家人、同學等)、雙方使用的自訂圖片（存在使用者外貌、居住地、興趣或時間戳記等訊息)，可據以分析案件的時間關聯，提供後續追查情資。

2.2 數位鑑識工具

為維持訴訟公正性，數位證據的鑑識分析作為，須符合法律規範。一般數位鑑識工具須提供映像備份環境，有簡明的操作介面、強大的功能運用及自動化的證據分析等三項特色[5,6]：

(1) 簡明的操作介面

具圖形化操作介面，方便檢視、分類不同檔案格式，能清楚呈現檔案屬性、細緻內容及分析結果。

(2) 強大的功能運用

具檢視資料內容、檔案格式轉換、數位記錄備份、快速搜尋數據、回復刪除資料、分析及回復登錄檔資訊、破解密碼及製作鑑識結果報告等功能。

(3) 自動化的證據分析

具有效減少處理時間及去除多餘資料成效。

解析數位證據前之製作證據副本方法有二：一般複製與映像備份。一般複製利用位元流備份儲存目標硬碟，再直接於電腦作業系統檢視副本硬碟，避免變動原始證據。映像備份是使用鑑識工具對目標硬碟進行映像檔製作，達成證據保全完整性，確保證據未更動。另 PDA 證據可能因意外、人為蓄意或電力耗盡等原因導致毀損，若是因電力耗盡而導致的資料遺失，則回復的機率幾乎微乎其微。因此，PDA 鑑識的最大不同點在於製作映像備份的時機要越早越好，後續鑑識處理也必須選擇適用行動裝置的工具或程序。

2.2.1 PC 鑑識工具

PC 鑑識工具（如 Encase、FTK、TCT、Live CD 等）或非鑑識軟體（如 Final Data）均可達到檢視被刪除資料等功能，本次使用的 EnCase 鑑識工具，雖可針對 PC 之 Windows 系統的 NTFS、FAT32、UNIX 系統的 EXT2/EXT3 等多種不同格式的檔案系統，進行鑑識分析，但針對 PDA 裝置僅適用 Palm 作業系統，其他如 Windows Mobile 6 等作業系統無法相容。

2.2.2 PDA 鑑識工具

不同作業系統的 PDA 裝置，須使用不同鑑識工具，如表一之 PDA 作業系統與鑑識工具表[1,4]，具備圖檔列表、搜尋、標記書籤、產生報告及製作數位簽章等功能。但 PDA 鑑識軟體功能發展較 PC 鑑識工具狹窄，尚無一套可適用所有廠牌或作業系統的 PDA 鑑識工具。鑑識人員可採取多種工具，比較相關裝置的共用性，過濾不同態樣案件。

表一：PDA 作業系統與鑑識工具

PDA 種類 / 鑑識工具	Palm OS	Pocket PC	Linux
PDD	擷取裝置	X	X
Pilot-link	擷取裝置	X	X
POSE	檢驗分析 產生報告	X	X
PDA Seizure	擷取裝置 檢驗分析 產生報告	蒐集資料 檢驗分析 產生報告	X
EnCase	擷取裝置 檢驗分析 產生報告	X	檢驗分析 產生報告
DD	X	X	擷取裝置

3. 討論與分析

晶片、位元與頻寬技術陸續精進，智慧型手機成為社群聯繫工具與身分象徵。智慧型手機豐富的使用者介面、便利的觸控功能及複雜的作業系統，短期價格仍居高不下。但行動通訊的即時性與便利性，是一種消費升級的需求。即使現今智慧型手機的

市場佔有率仍低,在蘋果、諾基亞 、 微軟等大廠全力推陳出新下，持續獲社會大眾支持，形成全新使用習慣，銷售成績的攀升，實可預期。隨著科技進步、開放原始碼的流行，智慧型手機可提供的服務越來越豐富。未來，普遍透過手機取代電腦上網指日可待，相關證據保留要求，亦需列入考量。本節從相關人員分別使用 PC 及 PDA 等不同硬體，執行 WLM 軟體作為觀察起點,將 6W1H 問題融入數位證據的鑑識分析，根據分析結果，釐清事件關連，作為提供解決方法的參考。

3.1 6W1H 問題

為發現犯罪事實,從 6W1H 問題分析案件的人、事、時、地、物；何人(Who)、何時(When)、何地(Where)、何事(What)、何物 (Which)、為何(Why)及如何(How)。從對話記錄、圖片檔案、傳送檔案及共享資料夾等證據種類，釐清使用者間的聯繫情形與案件相關資訊,如表二之 6W1H 結合即時通訊數位證據的應用表[3]。除自訂圖片檔案本身具特殊性外，其他三者所在之預設資料夾位置皆依使用者帳號資訊依序建立，故可據以作為對方帳號資訊的識別機制。「對話紀錄」提供雙方互動紀錄，分析案件之人、事、時、地、物。「圖片檔案」檢視雙方顯示圖片檔案之建立時間可以得知雙方最早開始使用即時通訊進行聯繫的時間。「傳送檔案」及「共享資料夾」知悉雙方互相傳送/接收，如文字、圖片、聲音、影像等檔案。可能揭露出事件所需資訊，其關聯程度視檔案的重要性強度不一，相關檔案之詳細資料亦可分析時間框架、推敲案發時間。

表二：6W1H 結合即時通訊數位證據

證據種類	Who	When	Where	What	Which	Why	How
對話記錄	✓	✓	✓	✓	✓	✓	✓
圖片檔案	✓	視案件情形不同表現關連程度					
傳送檔案	✓						
共享資料夾	✓						

3.2 實作分析

本文實作比較 PC 與 PDA 執行 WLM 軟體之數位證據關連分析，其設備資訊、鑑識工具與鑑識目的如表三之實作介紹表。分別利用鑑識軟體進行映像檔備份、分析檢視，探討 PDA 即時通訊軟體在電腦犯罪偵查及數位鑑識方面，可達成的分析應用及遭遇的困難問題。

表三：實作比較

項目	PC	PDA
設備資訊	HP/Microsoft Windows XP / Home Edition/ Version 2002/Service Pack3	HP/iPAQ 112 Class Handheld/Windows Mobile 6.0
鑑識工具	Encase 6.2	Paraben's Device Seizure
通訊軟體	Windows Live Messenger	
鑑識目的	1.證明聯繫關係	

	2.證明紀錄特殊性 3.蒐集相關證據 4.提出待證事實證明

3.2.1 實作情境

收送雙方分別於 PC 及 PDA 使用 WLM，開啟對話視窗進行文字溝通，皆使用具有獨特性且能夠代表個人本身的自訂顯示圖片檔案（具獨特性）。

3.2.2 檢視證據

利用鑑識備份方法，分別對 PC 與 PDA 進行完整硬碟複製與映像檔複製後，檢視證據。

(1)鑑識工具檢視

- PC：EnCase6.2。
- PDA：Paraben's Device Seizure。

(2)目標內容檢視：

- 特定目錄蒐尋：尋找 C:\Documents and Settings\User\Local Settings\Application Data\Microsoft\Messenger\使用者帳號@hotmail.com\ObjectStore\UserTile 存放顯示圖片的檔案夾。
- 還原圖檔：將 dt2 檔案更改副檔名為 jpg。
- 特定目錄蒐尋：檢視行動裝置路徑為 C:\Documents and Settings\使用者帳號\Local Settings\Temp\MessengerCache 資料夾。

4.綜合應用

即時通訊為智慧型手機一項基本的網路通訊功能，本節嘗試從此議題審視利用 6W1H 問題及 3E 方法之運用可能性，降低無數位證據可取或可得之窘境。

4.1 利用 6W1H 問題

隨著行動科技發展，PDA 或智慧型手機不斷推陳出新，功能趨近個人電腦效能。為處理日新月異之科技犯罪型態，未來電腦鑑識仍須進一步注重 PDA 等行動裝置的鑑識探討。為便利攜帶，PDA 使用簡化記憶體架構與應用軟體，達到類似 PC 之操作功能，在不造成系統負荷前提下，僅具軟體精簡功能，作業系統亦無法保存完整使用記錄。本實作過程發現，WLM 軟體在 PC 與 PDA 裝置均可找出雙方的自訂圖片檔案，但 PDA 裝置為避免系統負荷過重，精簡應用軟體功能，致使用者活動無法完全記錄，此為即時通訊 PDA 鑑識的障礙，如表四個人電腦與 PDA 之即時通訊證據表。

表四：個人電腦與 PDA 之即時通訊證據

檢視證據	對話記錄	顯示圖片	傳送檔案	共享資料夾
個人電腦	✓	✓	✓	✓
行動裝置	X	✓	✓	✓

可從 PC 對話記錄檔案，檢視嫌疑人與被害人間述及人、事、時、地、物之對話內容。以下，謹從圖片紀錄、傳輸紀錄及帳號紀錄等紀錄類別做一探討，如表五之實作鑑識分析表：

(1) 圖片紀錄：釐清關連特性
鑑識 PC 和 PDA 後，若找到雙方使用的顯示圖片檔案，可證明雙方曾經使用即時通訊軟體互相聯繫，延伸追查各項紀錄的特殊性，如聯絡人清單顯示暱稱、名稱可能透露相關資料或所在位置等訊息，證明案件人(Who)的關係。

(2) 傳輸紀錄：蒐集相關證據
雙方傳輸檔案，在未改變既有路徑情況下，會存於預設資料夾。檢視資料夾之留存檔案，除審視內容外，尚須注意檔案的建立日期、修改日期、存取日期及作者等詳細資料，以進行時間框架分析。另 PC 與 PDA 之 WLM 可藉聯絡人清單上顯示之名稱，進行使用者交友關聯分析，縮小追查對象範圍，對照使用者檔案傳輸之時間與內容，可進一步分析案件的犯罪事實（What）、犯罪手法（Which）、如何達成犯罪（How）及犯罪動機（Why）等。再依 PC 對話紀錄及檔案傳輸內容，進行犯罪時間（When）分析，釐清事件的前後時序關係。

(3) 帳號紀錄：提出待證事實證明
掌握雙方帳號資訊，追查犯罪地點（Where），確認該帳號使用者的真實身分，釐清所有 6W1H 關係。

表五：鑑識分析

紀錄類別	6W1H 應用目的	PC	PDA
圖片紀錄	Who：使用者確實建立聯繫	自訂圖片檔案	自訂圖片檔案
傳輸紀錄	What：犯罪事實 Which：犯罪手法 When：犯罪時間 How：如何達成犯罪 Why：犯罪動機	1. 雙方帳號資訊 2. 聯絡人清單顯示名稱 3. 對話紀錄、傳輸檔案時間框架 4. 對話記錄、傳輸檔案	1. 聯絡人清單顯示名稱 2. 檔案收發時間框架 3. 傳輸檔案
帳號紀錄	Where：犯罪地點	帳號身份確認	1. 雙方使用者帳號 2. 清單聯絡人涉案分析 3. 帳號身份確認

4.2 利用 3E 方法

3E 方法(Triple-E Approach)從教育面(Education)、執法面(Enforcement)和工程面(Engineering)等三種議題討論電腦犯罪，每種議題皆可進一步的應用到犯罪學、偵查和鑑識三個領域，每個領域著重不同面向。本文應用此方法，透過實作結果，解析行動鑑識的面臨挑戰，提供可行政策與策略，如圖一所示。

(1)教育面

教育面著重犯罪學領域，瞄準各

種犯罪行為進行不同的偵查，除強化資訊安全之公共意識外，透過分析即時通訊之數位證據，進行 6W1H 策略剖繪案例的相關資訊。教育對象為使用者、偵查人員與應用軟體開發廠商。

- 使用者教育

開啟對話記錄功能、聯絡人清單分類、網路通訊安全基本常識。

- 資訊調查人員教育

正確保存 PDA 裝置、有效擷取裝置資料與認識數位鑑識的處理原則。

- 廠商教育

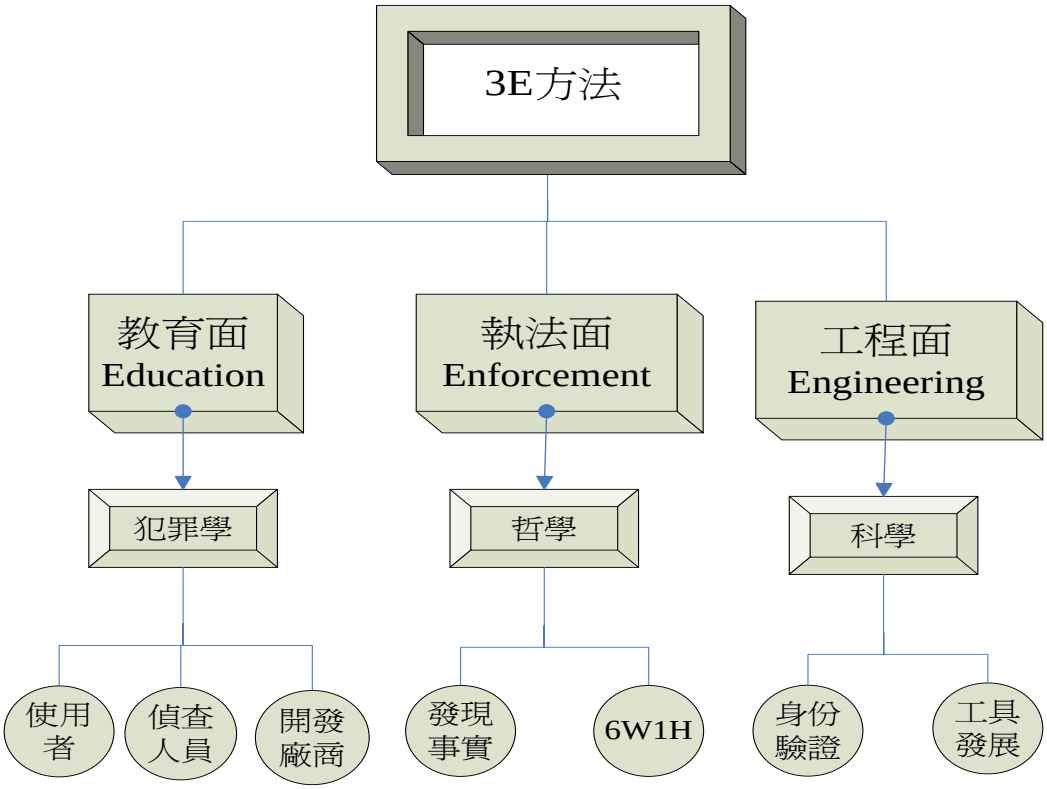
PDA 即時通訊軟體之使用者帳號記錄、簡易對話記錄功能開發。

(2)執法面

執法面著重偵查領域的哲學角色，期從不同觀點發現與重建事實。藉資訊調查人員檢驗數位證據所得結果，幫助執法人員釐清案件，依照法律程序做出正確判斷、制裁犯罪。PDA 鑑識整體成熟度較電腦鑑識不足，應加強偵查人員對 PDA 等行動裝置架構與特性之認識，由各方面檢驗犯罪事實，探索其犯罪行為應用，並分析案件之 6W1H 資訊。

(3)工程面

工程面著重鑑識科學角色，期進行數位證據目標驗證逮捕罪犯，資訊調查人員取得 PDA 即時通訊內容後，根據聯繫關係證明、紀錄特殊性、相關證據等方向進行時間框架、隱藏資料、應用程式、所有權與支配權分析，藉由合法程序建立即時通訊證據稽核檢驗或交叉比對，證明使用者身份等資訊。未來，PDA 軟體應配合上述偵查方向發展必要記錄功能，藉由適當鑑識工具配合行動裝置作業系統，突破行動鑑識之限制。



圖一：3E 方法架構

5. 結論

目前智慧型手機功能朝衛星定位（GPS）及無線通訊（Wi-Fi）等功能研發，開發尚無一定標準，作業系統及相關軟體的使用功能、流暢運作、簡單性和介面親和性，已獲各廠商重視，但後續應用程式相關紀錄保存亦應一併考慮，如何提供使用者必要數位紀錄自清或釐清法律訴訟爭議，在可預見的未來，其重要性可見一斑。經實作分析，PDA 因可隨身攜帶，依使用習慣進行各項數位活動，須縮小記憶體容量，致即時通訊沒有 WLM 對話紀錄功能。現今記憶體技術日趨成熟，PDA 記憶體容量大幅增加，未來 PDA 裝置的應用軟體，建議能建立簡易記錄檔，提供重要事件證明的參考資訊，避免事證不足，難以回復事件真相。

Acknowledgments

This research was partially supported by the National Science Council of the Republic of China under the Grant NSC 98-2221-E-015-001-MY3-

參考文獻

[1] Ayers, R. and Jansen, W., “PDA Forensic Tools: An Overview and Analysis,” National Institute of Standards and Technology, NISTIR 7100, pp. 10–19, August 2004.

[2] Jansen, W. and Scarfone, K., “Guidelines on Cell Phone and PDA Security,” Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-124, October 2008.

[3] Kao, D. Y., “The Retest of the Reintegrative Shaming Theory and Its Implications on Taiwanese Juvenile Hackers,” Ph. Dissertation, Department of Crime Prevention and Corrections, Central Police University, Taiwan, pp.18-28, January 2009.

[4] McNemar, C. M., “Forensic Analysis of Digital Evidence from Palm Personal Digital Assistants,” College of Engineering and Mineral Resources at West Virginia University, pp. 11–34, 2004.

[5] Mellars, B., “Forensic Examination of Mobile Phones,” Digital Investigation, Vol. 1, pp. 266-272, 2004.

[6] Radack, S., “Security of Cell Phones and PDAs,” Information Technology Laboratory National Institute of Standards and Technology, pp.30-36, October 2008.