道路交通事故之行動裝置 OSINT 工具鑑識研究

何昌岳[1]、黃正達[2] 、王旭正[3]
[1]中央警察大學資訊管理學系
[2]亞東技術學院資訊管理學系
[3]中央警察大學資訊管理學系
[1]im1033095@mail.cpu.edu.tw、[2]cthuang@mail.oit.edu.tw、[3]sjwang@mail.cpu.edu.tw

摘要

智慧型行動裝置的普及，及無線網路技術的成熟，透過行動裝置可達成的服務愈來愈多，但也因其即時性與方便性，使駕駛人在駕駛車輛時，常使用行動裝置上網，此行為易造成駕駛人分心，進而導致道路交通事故的發生。當事故發生時，在行動裝置發現關鍵或相關之數位證據的情形，也會隨著行動裝置使用的增長，可能性同樣增加。然而，現今行動裝置鑑識調查面臨最大窘境，便是商業型鑑識工具對於行動裝置的支援程度，追不上行動裝置硬體型號及軟體版本的更新速度，這時便迫切需要建立可支援第一線調查人員和研究者去鑑識調查的工具及方法。本文將先利用行動裝置的日誌檔內容，判別使用者的使用行為，再藉由行動裝置的備份檔，進一步找出通訊紀錄、傳送之多媒體檔案等數位證據，證明其與交通事件或犯罪行為之關連性，並透過交通事故個案研究進行觀察分析跟探討。

關鍵詞：行動裝置鑑識、iTunes 備份、ADB 工具、buffer logs、道路交通事故調查

Traffic Forensics in Mobiles on OSINT Tools Operations Ushering Evidence Revelations

Chang-Yueh Ho[1], Cheng-Ta Huang[2], Shiuh-Jeng WANG[3]
[1]Department of information Management, Central Police University, [2]Department of information Management, Oriental Institute of Technology, [3] Department of information Management, Central Police University
[1]im1033095@mail.cpu.edu.tw, [2]cthuang@mail.oit.edu.tw, [3]sjwang@mail.cpu.edu.tw

ABSTRACT

Following up the popularity of smart mobile devices and the maturity of wireless networking technologies, the services are able to be achieved through the operations of the mobile devices. By means of the functionalities of immediacy and convenience, the mobiles are always associated with the drivers when operating the cars on the driving ways. The behaviors are likely to distract the drivers from the driving procedures, and leading to the occurrence of road traffic accidents. When an accident occurs, finding critical or relevant digital evidence on the mobile devices associated with the drivers are necessary at the first moment. However, the biggest concern of mobile device forensic investigation now is that the support of commercial forensic tools can not catch up the upgrading rate of the hardware and software versions in the mobile operations. By the way, it is required to build the tools and methods of forensic investigations to cope with the forensics investigators to guarantee the completeness of probing evidence. In this paper, we use the log file of mobile device to analyze the user behaviors. And then fix the key evidence in terms of communication records and multimedia files to make the connections, either in the case of the traffic accidents or criminal events.

Keywords: Mobile forensics、iTunes backup、ADB tools、Buffer logs、Traffic event investigations

壹、前言

根據行動數據分析平台 Yahoo Flury 在 2016 年度關鍵報告，社交通訊 APP 的使用時間相較 2015 年，飆升近 4 倍，另台灣網路資訊中心（TWNIC）於 2016 年調查，全國 12 歲以上民眾的行動上網率為 68.8%，人數約為 1,448 萬人，另有 86.3%的受訪者在上網時，使用即時通訊軟體，顯示即時通訊軟體的使用已相當普遍。但也因即時通訊軟體的即時性與方便性，造成使用者經常拿起行動裝置滑一下，導致發生危險駕車之情形。且依內政部警政署統計，因汽、機車駕駛人過失而導致道路交通事故發生的比率，佔全部肇事原因的 9 成以上，因此，交通部於 2012 年針對「道路交通管理處罰條例」修法，增訂汽、機車駕駛人於行駛道路時，不得以手持方式使用手機進行數據通訊功能，並於 2013 年 1 月 1 日起開始實施。

然而，要如何調查駕駛人是否有使用行動裝置，或進而導致道路交通事件發生的需求，日益增加，因此為了提供第一線調查人員先行快速確認使用者使用手機的行為，並有效解決行動裝置之鑑識限制及瓶頸，本文嘗試針對智慧型行動裝置，透過備份檔進行相關鑑識研究調查，找出相關應用程式的使用行為及可能留存之數位跡證，並以實際測試分析相關檔案之內容，驗證所使用的鑑識調查方法。本文各節安排如下：第貳節探討智慧型行動裝置及其即時通訊軟體等鑑識的相關研究文獻探討。第參節針對 iOS 及 Andrid 行動裝置進行鑑識調查分析研究，並透過行動裝置之日誌檔及備份檔，對即時通訊軟體進行鑑識分析。第肆節討論與分析行動裝置日誌檔、備份檔及即時通訊軟體鑑識研究，並進行相關比較。第伍節為本文之結論。

貳、文獻探討

於 2015 年時，He 等學者研究頭戴式顯示器 Google Glass 會影響駕駛人對於車輛的控制，並以與智慧型手機手持互動、以語音與智慧型手機手持互動、及以語音與 Google Glass 互動等三種情況進行統計分析，發現就算以語音方式與 Google Glass 互動，仍會影響駕駛人之駕駛行為[12]。可見於交通事故中，智慧型行動裝置之使用，有其影響性存在，以下將針對智慧型行動裝置及其即時通訊軟體之鑑識方法進行介紹。

2.1 智慧型行動裝置數位鑑識

Android 是一套以 Linux 為核心的開放原始碼手機作業系統，Google 於 2005 年 7 月時收購手機作業系統開發公司 Android，並於 2007 年 11 月時，由 Google 與多家手機硬體製造商、軟體開發商及電信營運商所組成的 Open Handset Alliance（OHA）共同公佈

最早版本 Android 1.0 beta 版，其後便由 OHA 共同研發改良。而於 2009 年 5 月起，Android 作業系統改用甜點作為版本代號，並按照大寫字母的順序來進行命名，目前 Android 的最新版本為 Nougat 版（版號 7.1.2）[8]。

相較於 Android 系統，可供各家手機製造商自由搭載，由 Apple 公司推出的行動裝置，如 iPhone、iPad 等，都屬於較特殊且封閉之硬體規格及作業系統，僅有該公司所推出之相關產品有支援，如透過 iTunes 管理安裝與執行 Apple 公司授權之應用程式。

目前針對行動裝置進行相關鑑識的方法，可依鑑識標的區分為 2 種方式，第 1 種是「行動裝置鑑識」，意即直接萃取行動裝置上的資料，此種資料萃取的方式，又可分為邏輯萃取與實體萃取；第 2 種則是「備份檔鑑識」，鑑識人員無須拿到行動裝置本體，只需要找到使用官方所提供同步備份軟體的電腦，對電腦內的備份檔進行鑑識即可[4][10]。

2.1.1 行動裝置鑑識

根據美國國家標準技術局（National Institute of Standards and Technology，NIST）手機鑑識指引，手機鑑識流程可分為保存（Preservation）、萃取（Acquisition）、鑑識及分析（Examination and Analysis）和報告呈現（Reporting）等四個階段[17]。在這四階段中，以資料萃取階段最為重要，其萃取方式可分為實體萃取（Physical Acquisition）與邏輯萃取（Logical Acquisition）兩種，兩者最大的差異在於前者是以位元複製取得完整記憶體內容，可找出、分析或恢復使用者已刪除的資料，而邏輯萃取則無法取得已刪除之檔案，導致可能遺漏手機儲存空間內的殘存空間（Slack Space）。

此外，若執行實體萃取，因須對行動裝置安裝鑑識軟體，故必須先將 iOS 裝置進行「越獄」（JailBreak,簡稱 JB）或 Android 裝置進行「取得最高權限」（ROOT）的程序。由於行動裝置製造商為維護行動裝置作業系統裝置之安全及穩定性，鎖定使用者對行動裝置進行修改、檢視作業系統的檔案系統之權限、非經允許的操作存取動作等，而「越獄」或「取得最高權限」就是針對 iOS 或 Android 作業系統進行破解的技術程序，當行動裝置經過越獄後，便能順利安裝並執行鑑識工具軟體。

2.1.2 備份檔鑑識

由於行動裝置製造商對於行動裝置具有較嚴格的保護及管理機制，無法任意由其他軟體工具進行存取及修改，但又為了讓使用者可輕易管理自身行動裝置的資料內容，所以推出了讓使用者可將行動裝置與個人電腦連結並管理其資料內容的工具平臺，iTunes 或 ADB 工具。

iTunes 是由 Apple 公司發行，可依據自身的 iOS 作業系統的版本，由官方網站免費下載安裝，功能包含同步、備份 iOS 行動裝置資料、影音播放器、共享與瀏覽 App Store 與 iTunes Store 資料等。iTunes 對 iDevice 進行的同步及備份之資料內容，有 App、音樂、影片、電視節目、鈴聲、照片、通訊錄、行事曆、語音備忘錄等，如圖一。另透過 iTunes

執行的備份，其備份檔會因為連結之電腦作業系統不同，而有不同儲存的路徑，表一即列出在 Mac 及 Windows 作業系統所儲存之路徑位置。

圖一：iTunes 管理工具畫面

表一：iTunes 備份路徑

作業系統	路徑
Mac	/使用者/資源庫/Application Support/MobileSync/Backup
Windows Vista、7、8、10	Users\使用者名稱\AppData\Roaming\Apple Computer\MobileSync\Backup

另 ADB（Android Debug Bridge）工具，是讓使用者可對 Android 使用命令列的開發工具，屬於 Android SDK（Software Development Kit）工具的一種，方便檢測程式有無執行錯誤並進行除錯。如同 CMD（命令提示字元）於 Windows 作業系統中功能，輸入一些 Dos 指令，檢查硬體設備與系統的執行狀況。相同地，Android 程式開發者，為了解 Android 系統與手機硬體間運行狀況，或對 Android 進行存取的動作，透過 API（Application Programming Interface）介面執行 ADB 指令，操作或管理 Android 系統，以判斷系統執行情形，如刪除 Android 內部的檔案、將某個檔案放到 Android 檔案目錄下、或者取得目前系統的資訊等[6]。

若要以 ADB 工具的指令操作或管理 Android 系統之行動裝置，首先需在電腦端安裝行動裝置同步資料的連線驅動程式，其次是在行動裝置端開啟“USB 除錯”模式，這 2 個前置作業說明如下：

(1) 電腦端安裝手機同步驅動程式

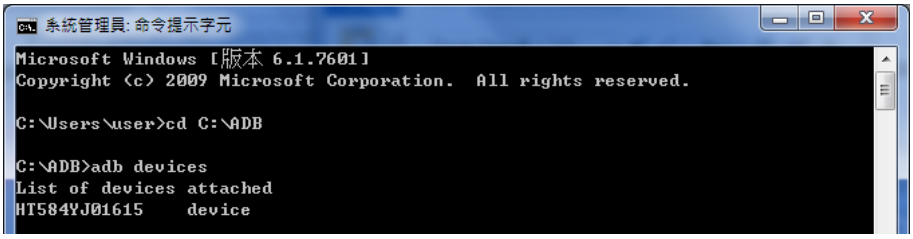
電腦端需安裝手機同步資料的連線程式，安裝後可透過該程式檔案總管存取手機裡的相片、影片、檔案、音樂等資料，如 HTC 手機需安裝 HTC Sync，Samsung

手機需安裝 Kies 等。

(2) 手機端開啟 USB 除錯模式

該模式開啟的方式，會因行動裝置製造商的不同，而有不同的開啟方式，如以本文 HTC M9u 為例，要進入手機設定頁面，點選“應用程式”，再點選“開發”，找到“USB 除錯”並勾選後，即開啟“USB 除錯”模式。

此外，在行動裝置端開啟“USB 除錯”模式後，電腦端須先在 CMD 上執行“adb devices”指令，檢測是否連接上行動裝置，若有成功連接，則 CMD 上會顯示連接手機的序號，如圖二。



圖二：利用 ADB 工具連接上手機

2.2 行動裝置即時通訊軟體鑑識

2.2.1 iOS 通訊軟體鑑識

2010 年時，Husain 及 Sridhar 針對沒有越獄過 iPhone，以 iTunes 邏輯備份的方式，進行 AIM、Yahoo!及 Google Talk 等即時通訊軟體之調查[15]，而 Bader 及 Baggili 更進一步利用命令列工具，如 grep、find 等，手動尋找 iTunes 備份檔內容，並將其內容與 iPhone 上的原始文件進行匹配[2]；另在 2011 年，Hoog 及 Strzempka 則針對即時通訊軟體 Kik，研究其資料庫內容，並發現使用者的密碼以未加密的方式儲存在行動裝置上[13]。

而在 2012 年，Tso 等學者就著重在針對當時較流行的通訊軟體，解析 iTunes 備份檔案內的 SQLite 資料庫及 plist 檔案，而這也被當作從 iOS 設備邏輯萃取鑑識的主要方法[24]。但也因邏輯萃取而得的備份檔，無法找到被刪除的資料，因此 2016 年時，Ovens 及 Morison 利用越獄過後的行動裝置，針對即時通訊軟體 Kik 的資料庫進行分析，進而發現被刪除的資料，除可在行動裝置上被發現，亦可從 Kik 的伺服器上下載[21]。

2.2.2 Android 通訊軟體鑑識

除了 iOS 行動裝置以外，也有些研究人員在相關 Android 行動手機進行鑑識分析研究，如在 2013 年，Al Barghouthy 等學者針對行動裝置上的瀏覽軟體 Orweb，探討數位跡證的發現與行動裝置本身有無 root 之關聯性，後來發現要經過 root 後，才可找到其跡證[1]。在 2014 年時，Faheem 等學者展示即使商業型鑑識工具是試用版的，也可針對映像檔進行鑑識分析[11]，同時，Karlsson 及 Glisson 則利用 CyanogenMod 的反鑑識技術，

阻擋商業型鑑識工具的資料萃取、agent 的安裝、及呈現假資料等，且不會影響設備正常運作[18]。此外，在 2015 年，Horsman 及 Conniss 等學者利用 Android 開發人員所使用的開發工具 ADB，找出存於日誌資料夾下的日誌檔，藉以探討手機使用情形的跡證[14]。

參、iOS 及 Android 行動裝置鑑識調查方法研究

本文將挑選讓使用者對所發送內容較有完整的主控權的 U 通訊，及無須使用者註冊驗證的 Kik 等 2 種即時通訊軟體作為研究對象，並透過 Apple 公司所提供的 iTunes 官方軟體及 Android 開發工具 ADB，針對行動裝置執行備份之實驗與測試。本文所需設備及軟體彙整如下：

1.個人筆記型電腦一台，作業系統 Windows 7 Professional 64-bit。
2.Apple iPad Air 2 一台，iOS 版本 9.3.2。
3.HTC M9u 一台，Andriod 版本 5.1。
4.同步備份軟體：Apple iTunes 12.5.1.21、ADB 工具 24.4.1。
5.檔案檢視軟體：Plist Editor Pro for Windows（version 3.0）、SQLite Database Browser（version 3.8.0）、iTools 3、Cygwin（version 2.5.2）。

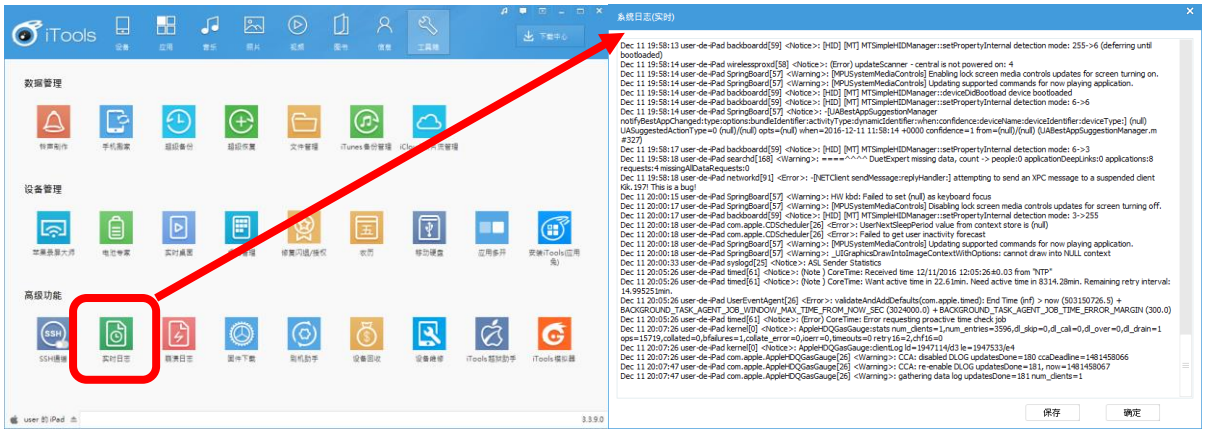
3.1 iOS 行動裝置鑑識方法探討

相較於 Android 系統，iOS 系統屬於較封閉式的系統，且其行動裝置並未支援任何外部擴充的記憶卡，所有系統及使用者資料皆儲存在裝置內之記憶體，所以造成對 iOS 行動裝置有其困難度在。有關 iOS 行動裝置鑑識流程圖如下圖三。

圖三：iOS 行動裝置鑑識流程圖

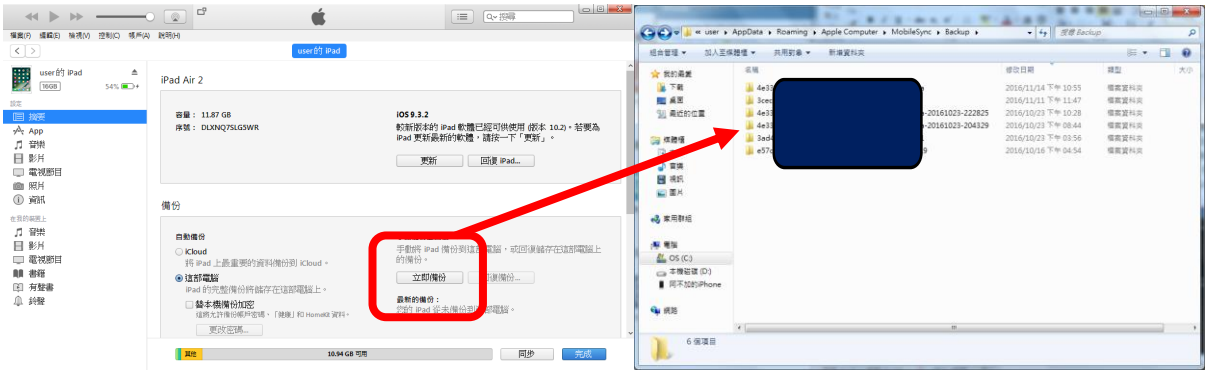
本文利用 iTools 內建的「實時日誌」的功能，顯示目前 iOS 裝置的系統日誌內容（如圖四），而這些內容也可以儲存至指定的路徑。iTools 是一款可管理 iOS 系統及 Android 系統等雙平臺行動裝置的工具，且對 iDevice 的基本管理功能，一應俱全，另相較於

iTunes，該工具有較直覺化的操作介面。此外， iTools 亦可支援已越獄過 iDevice 的管理功能。



圖四：iTools 的工具箱頁面及實時日誌的畫面

另當電腦連接上 iOS 行動裝置，iTunes 會顯示這臺 iDevice 的基本資訊，如裝置名稱、型號、iOS 版本、電話號碼、序號等。點選「立即備份」功能的按鈕即可進行備份，而備份完成後之備份檔，會儲存在本文參考文獻所提到之路徑，如圖五。



圖五：iTunes 備份操作畫面

接著利用 iTools 工具針對備份檔進行檢視，iOS 系統的檔案格式，主要分為 2 種，第 1 種是 Property List(.plist)檔案，主要儲存使用者對行動裝置的設定，第 2 種是 SOLite (.sqlite)檔案，主要儲存使用者於行動裝置上使用之資料庫。前者可利用 Plist Editor Pro for Windows 工具軟體，提供一個較直觀的使用者介面，讓使用者可輕鬆存取各種標準屬性清單檔案；而後者則使用 SQLite Database Browser 工具軟體(含.sqlite3 檔、.db 檔、.db3 檔等)，讓使用者在不使用 SQL 程式語法的情況下，用來建立、設計、編輯 SQLite 資料庫檔案的視覺化工具。

3.2 Android 行動裝置鑑識方法探討

3.2.1 匯出日誌檔

行動裝置製造商為了應用程式的開發與除錯（debug）目的，都會想辦法記錄系統訊息的記錄，如在 Android 系統中，「buffer logs」就是扮演這樣角色，其內所保存日誌檔的內容，是由使用者與行動裝置間的互動所產生，而且只要是開機的狀態，就會持續記錄所產生的記錄。

「buffer logs」並非單一的日誌檔，它有許多種類，每種日誌檔都有其主要記錄的內容，如表二所示，包含使用者使用手機來開啟或關掉某個 App 等動作事件，而如同電腦執行序一樣，在 Android 手機裡，每個事件都可以用特定 PID（Process ID）來區分[14]。然而，「buffer logs」也有容量限制，不同款行動裝置的容量不一定相同，而一旦達到了該限制，系統則會開始覆寫之前的日誌內容，且如同電腦的 RAM，若行動裝置關機的話，「buffer logs」也會隨之消失。

表二：buffer logs 種類

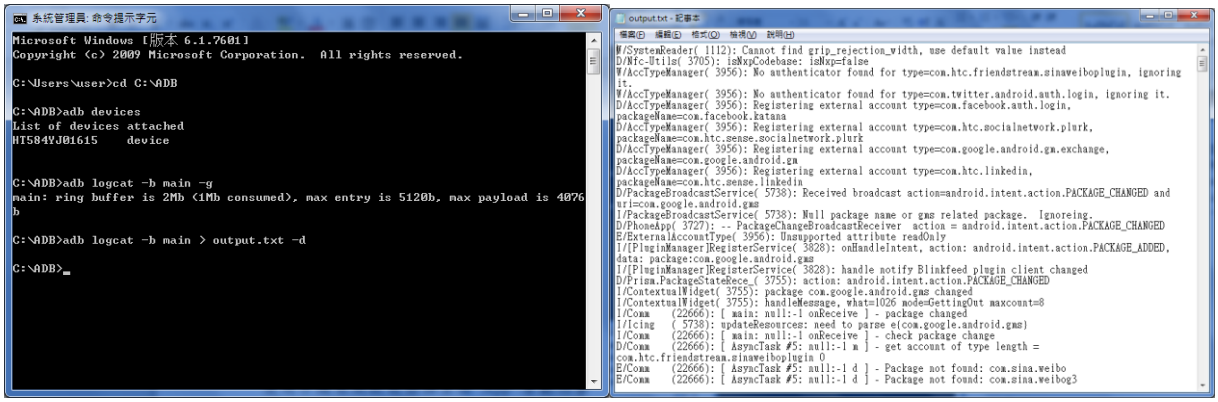
種類	主要內容
System	系統除錯的記錄
Main	預設的主要系統記錄
Events	與系統事件相關的記錄
Radio	廣播或是通話相關的記錄

為了查看日誌檔的內容，ADB 工具提供“logcat”的指令，針對 Android 日誌系統所蒐集日誌訊息進行查看及過濾。表三列出一些執行“logcat”指令時，搭配的參數項目。

表三：logcat 指令參數說明

參數	說明
-b 〈buffer〉	選擇查看何種「buffer logs」，預設是 main。
-c	清除或刷新日誌。
-d	將日誌顯示在螢幕上後自動結束。
-g	找出特定「buffer logs」的大小。
-v 〈format〉	將日誌檔匯出成指定格式，如是 process 表示以 PID 排序。

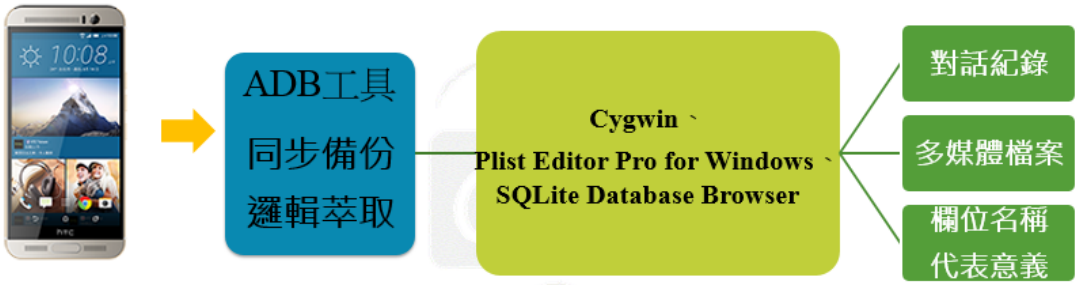
此外，也可以利用“logcat > filename”的指令，將日誌檔內容匯出，以方便分析及後續檔案保存作業，另若只單純輸入“logcat > filename”的指令，則 Android 系統會持續匯出最新的日誌檔，需按“ctrl + C”方才停止，所以，需要加上“-d”，將目前日誌檔內容印完後即停止，如圖六。



圖六：匯出 buffer log 至 output.txt 及其內容

3.2.2 行動裝置備份

為了備份行動裝置的內容，ADB 工具提供“backup”的指令，針對 Android 的系統及 APP 內容等，不用 ROOT 也可進行備份，而 Android 行動裝置鑑識流程圖如下圖七。本文用到的指令為“adb backup [-system/-nosystem] [-all/-<APP 檔名>] [-apk/-noapk] [-shared/-noshared] -f <檔案路徑及名稱>”，表四將針對各個參數進行解說。



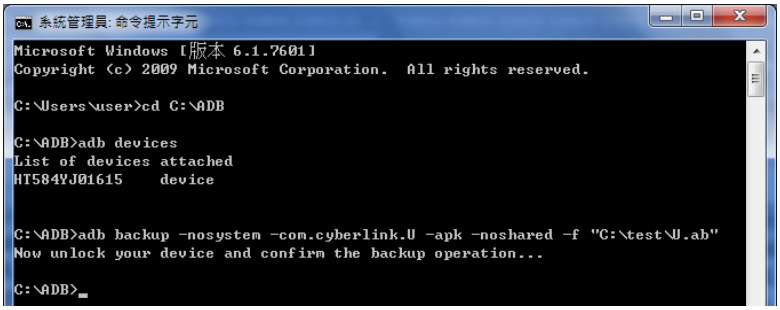
圖七：Android 行動裝置鑑識流程圖

表四：“backup”指令參數說明

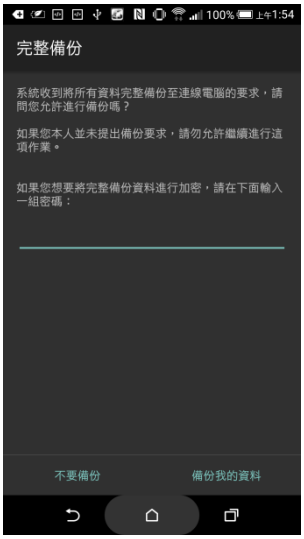
參數	說明
-system/-nosystem	決定系統是否備份，預設是-system，表示會連系統備份。
-all/-<APP 檔名>	決定備份哪些 APP，可輸入 APP 檔名。
[-apk/-noapk]	決定是否備份 APP 的 APK 安裝檔。
[-shared/-noshared]	決定 SD 卡內檔案是否備份。
-f <檔案路徑及名稱>	備份檔用什麼檔名存在哪個路徑，但副檔名一定為「.ab」。

在輸入完指令後，會出現如圖八的訊息，並在手機上出現如圖九的「完整備份」畫面，要求輸入備份檔的密碼，但也可選擇不輸入而直接進行備份。當備份完後，手機會

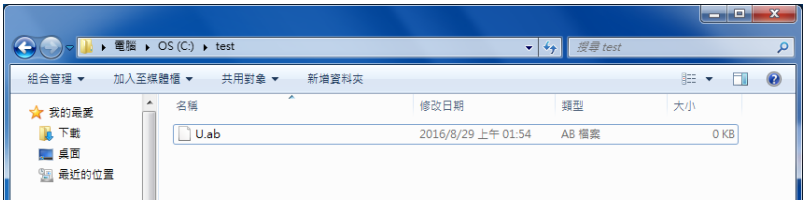
自動跳出畫面「完整備份」，並到指定的路徑下，即會看到備份檔，如圖十。



圖八：輸入指令後之訊息

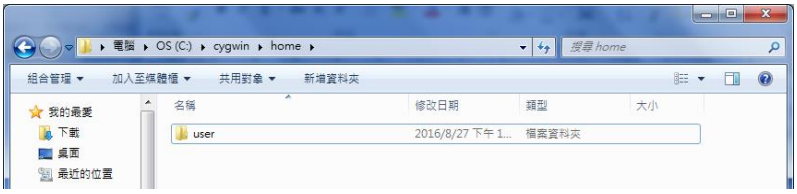


圖九：手機上出現「完整備份」之畫面



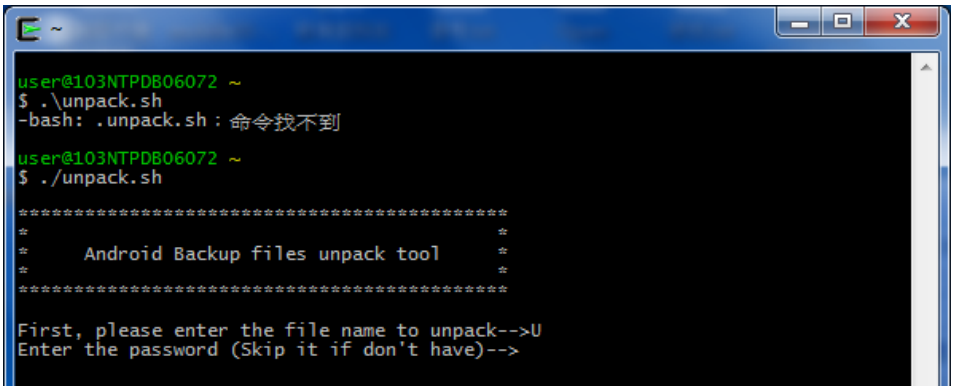
圖十：備份檔出現之畫面

接著把備份檔及解壓縮的腳本複製到 Cygwin 資料夾裡的 home\（使用者名稱）\底下。Cygwin 是一群符合 GNU 通用公眾授權條款（GNU General Public License）的開放原始碼工具之組合，其可在 Windows 上，執行類 UNIX 系統的操作方式。從官網下載 Cygwin 安裝完成並在執行過一次後，會在 Cygwin 資料夾裡的 home 底下，自動建立一個以現在正在使用的使用者名稱為名的資料夾，如圖十一。



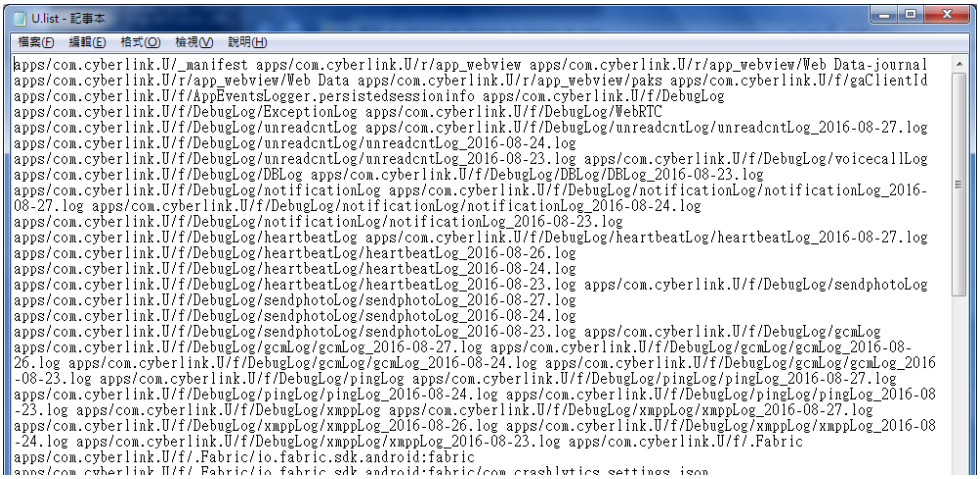
圖十一：出現以使用者名稱為名的資料夾

開啟 Cygwin 程式，輸入指令"./unpack.sh"，便會開始執行解壓縮腳本。該腳本一開始會先要求輸入備份檔的檔名（不用輸入副檔名），接著會問備份密碼，若當初備分時有設定，則輸入該組密碼，若無，則留空即可，如圖十二。



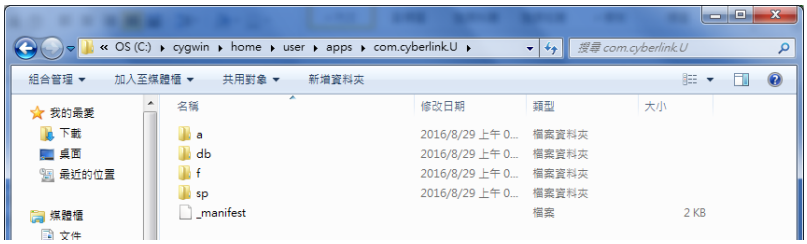
圖十二：Cygwin 解壓縮腳本執行畫面

輸入完密碼後，開始執行解壓縮，結束後到 Cygwin 資料夾裡的 home\（使用者名稱）\底下，會看到一個和備份檔同名的「.list」檔及一個名為 apps 的資料夾，前者紀錄本次解壓縮過程中，各種 APP 資料檔解出來的檔案內容，如圖十三。



圖十三：「.list」檔案內容

另點進 apps 的資料夾後，會發現以各個 APP 檔名命名的資料夾，而每個資料夾裡會有一些資料夾及檔案存在，如圖十四，下表五將對各資料夾及檔案資訊說明。



圖十四：APP 檔名資料夾內的資料夾及檔案

表五：資料夾及檔案說明

資料夾或檔案名稱	說明
a	存放 APK 的資料夾。
db	存放該 APP 相關資料庫檔案。
f	存放該 APP 資訊，如 debug 紀錄等。
sp	存放該 APP 執行時的相關資訊，這些檔案以 xml 檔儲存。
_manifest	紀錄該 APP 屬性。

3.3 行動裝置於即時通訊軟體之鑑識研究

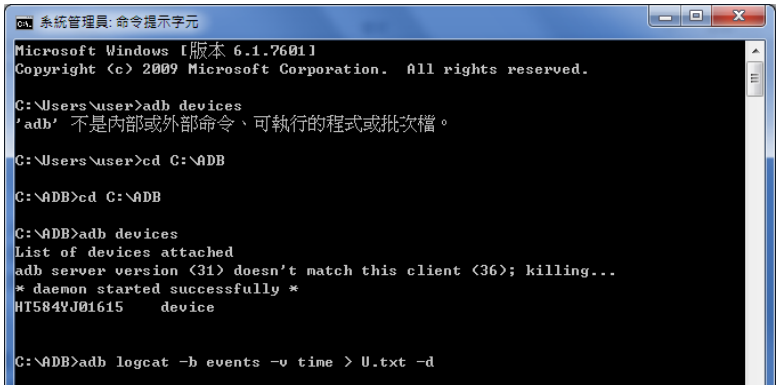
現行行動裝置上的即時通訊軟體種類眾多，本文中，選擇讓使用者對所發送內容較有完整主控權的 U 通訊，及無須使用者註冊驗證的 Kik 等 2 種即時通訊軟體作為對象。

3.3.1 U 通訊即時通訊軟體

「U 通訊」是由臺灣訊連科技股份有限公司（CyberLink）在 2014 年底推出的即時通訊軟體，其獨特的功能如圖文聊天、訊息延遲傳送、訊息回收、自行刪除訊息等，讓使用者對所發送內容較有完整的主控權。在本文中，嘗試就 HTC M9u 針對 U 通訊即時通訊軟體所傳送之聊天紀錄進行相關鑑識分析，相關鑑識實驗的 U 通訊軟體版本為 3.6。

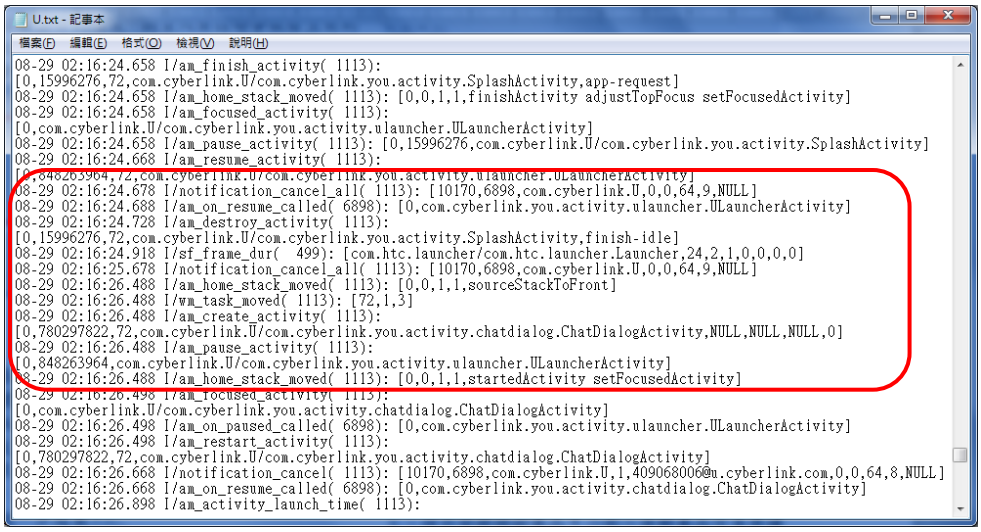
(1) 匯出行動裝置的日誌檔：

首先將 HTC 手機連接上電腦，並透過 ADB 工具進行連接，為了確認使用者是否有使用手機，以“logcat”加上“－v time”指令（如圖十五），指定匯出的日誌檔內容，僅含日期、時間、PID 及事件內容等訊息。



圖十五：以“logcat”加上“－v time”指令匯出日誌檔

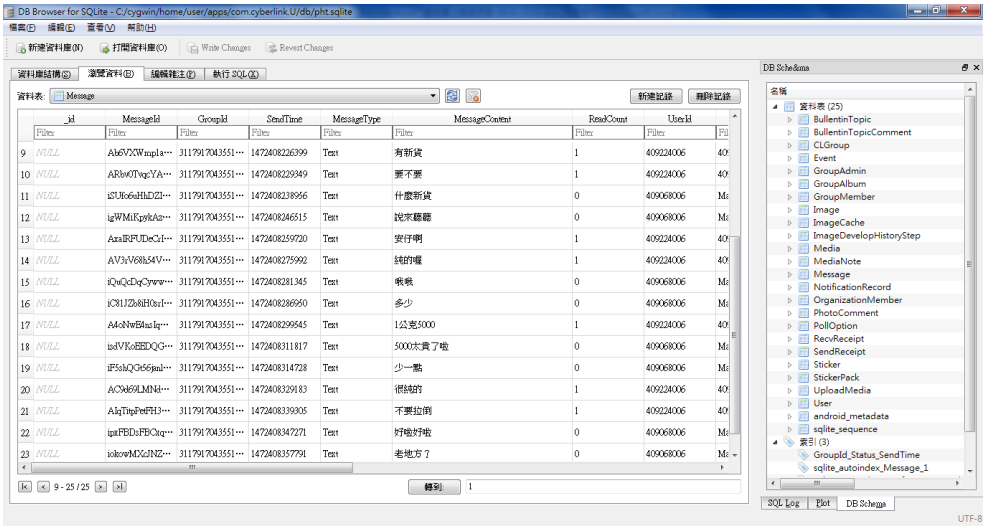
在匯出日誌檔後，搜尋日誌檔的相關紀錄，可發現通訊軟體 U 通訊的使用紀錄（如圖十六），如出現“notification_cancel_all:[…com.cyberlink.U…]”的訊息，表示使用者將訊息通知解除，出現“am_on_resume_called：[0,com.cyberlink.you.activity...]”的訊息，表示在行動裝置背景執行的應用程式被叫到前臺執行，出現“am_＜Scribe＞_activity”的訊息，表示使用者在查看 U 通訊的內容。



圖十六：U 通訊使用的記錄

(2) 行動裝置內 U 通訊之備份

利用 ADB 備份工具針對 U 通訊軟體進行備份，將備份完後之備份檔放入 Cygwin 資料夾裡的 home\user\底下，並利用解壓縮腳本進行解壓縮，完成後再利用 SQLite Database Browser 工具（如圖十七），檢視聊天紀錄。



圖十七：利用 SQLite Database Browser 檢視聊天紀錄

可發現在其資料庫內有一張名叫 Message 的資料表，其內紀錄著聊天紀錄傳送的時間（類似 UNIX 的時間格式）、內容、訊息傳送者的名稱等資訊，訊息傳送者名稱的命名方式為「“一組數字”@u.cyberlink.com」，而這名稱可從另一張資料表 User，找出對應的聯絡人，進而可得知，使用者與特定聯絡人對話之內容。

3.3.2 Kik 即時通訊軟體

軟體開發商 Kik Interative 在 2010 年時，推出第 1 版的「Kik」App，其較獨特的功能為趣味 GIF 動圖和手繪塗鴉功能。然因 Kik 在註冊新使用者時，無須輸入電話號碼（如圖十八），對於新使用者的審核機制較為薄弱，易導致有心人士創造假帳號進行非法行事。在本文中，嘗試就 iPad Air 2 針對 Kik 即時通訊軟體所傳送之聊天紀錄、多媒體檔案等進行相關鑑識分析，相關鑑識實驗的 Kik 通訊軟體版本為 10.17。

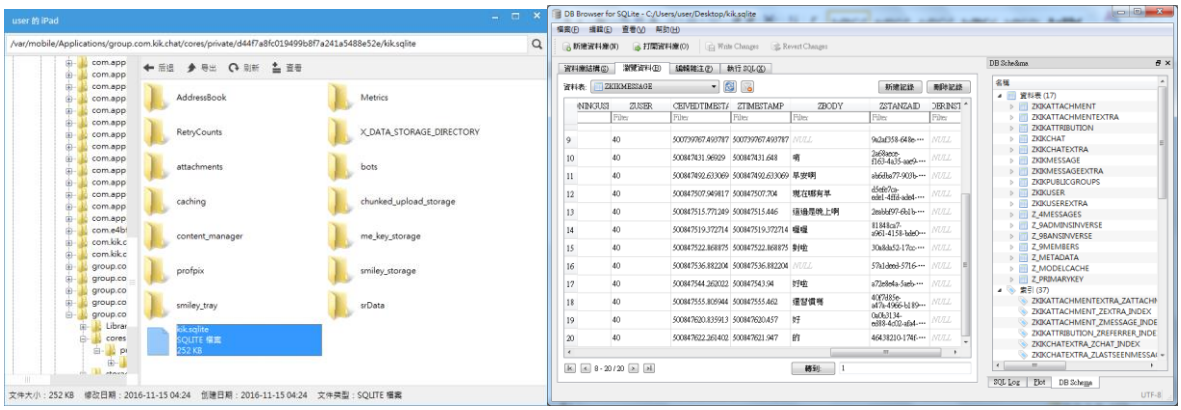
圖十八：Kik 即時通訊軟體註冊畫面

(1) 檢視行動裝置的日誌檔：

將 iPad 裝置連接上電腦，利用 iTools 工具提供之「實時日誌」的功能，查看使用者行動裝置之使用行為。在日誌檔內，如出現“SpringBoard[57] <Warning>: [MPUSystemMediaControls] Enabling lock screen media controls updates for screen turning on”的訊息，表示使用者將螢幕解鎖，而出現“SpringBoard[57] <Warning>: [MPUSystemMediaControls] Disabling lock screen media controls updates for screen turning off”的訊息，則表示使用者將螢幕關閉。

(2) 行動裝置內 Kik 通訊軟體之備份

將 iPad 透過 iTunes 進行同步備份資料後，利用 iTools 工具查看備份檔之資料，在“/var/mobile/Applications/group.com. kik.chat”路徑下（如圖十九），可發現與 Kik 通訊軟體相關之檔案，如聊天紀錄的資料檔、聊天所傳送之相片、影片及其 plist 檔、使用者註冊資訊等，相關檔案整理如表六，其中 UUID 是指 Universally Unique Identifier，是 Apple 公司自 iOS 8 版後，取代應用程式以自身為名的命名方式。



圖十九：利用 iTools 找 SQLite 檔案及 SQLite Database Browser 檢視聊天紀錄

表六：與 Kik 相關檔案說明

內容說明	路徑	檔案名稱
儲存聊天紀錄之資料檔	~/cores/private/fbd041558d884548bf3aebd0c26be09b	kik.sqlite
聊天所傳送的附件之 plist 檔	~/cores/private/fbd041558d884548bf3aebd0c26be09b/attachments	以附檔之 UUID 為檔名，可對應至 kik.sqlite
聊天所傳送之圖片及影音檔	~/cores/private/fbd041558d884548bf3aebd0c26be09b/content_manager/data_cache	以附檔之 UUID 為檔名，可對應至 kik.sqlite
聊天所傳送的圖片及影音檔之 plist 檔，內含 URL 連結	~/cores/private/fbd041558d884548bf3aebd0c26be09b/content_manager/metadata_cache	以附檔之 UUID 為檔名，可對應至 kik.sqlite
使用者資訊，如註冊名稱、使用者名稱、電子郵件等	~/Library/Preferences	group.com.kik.chat.plist

「kik.sqlite」內含有許多資料表資料，其中資料表「ZKIKUSER」有使用者的聯絡人相關資訊，資料表「ZKIKCHAT」含有使用者與聯絡人聊天紀錄的細節，資料表「ZKIKMESSAGE」包含使用者及所有聯絡人之聊天紀錄內容及聊天時間等，資料表「ZKIKATTACHMENT」則是聊天所傳送之附件資訊。表七到表十將針對上述資料表的部分欄位資料做一介紹。

表七：ZKIKUSER 欄位說明

欄位名稱	內容描述
ZFLAGS	使用者是否與聯絡人聊天
ZEXTRA	當群組或聯絡人第一次出現在使用者的清單裡時，皆會產生一個數值。當數值愈大，代表這群組或聯絡人愈近才加入使用者的清單中。
ZDISPLAYNAME	使用者呈現的名字
ZJID	根據「ZUSERNAME」創造的 ID

ZPPTIMESTAMP	使用者照片的更新時間
ZPPURL	使用者照片的 URL 網址
ZUSERNAME	註冊新用戶時的使用者名稱，此名稱為不可改的

表八：ZKIKCHAT 欄位說明

欄位名稱	內容描述
Z_OPT	儲存使用者與其他聯絡人間，互動的量，如數值愈大，表示互動愈密切
ZEXTRA	互動紀錄的數值
ZUSER	與資料表「ZKIKUSER」的欄位「ZEXTRA」對應

表九：ZKIKMESSAGE 欄位說明

欄位名稱	內容描述
Z_PK	與資料表「Z_4MESSAGES」的欄位「Z_6MESSAGES」對應
ZFLAGS	數值 4 表示有傳送檔案
ZSTATE	表示訊息傳送接收的狀態
ZTYPE	數值 1 表示接收訊息，數值 2 表示傳遞訊息
ZUSER	與資料表「ZKIKUSER」的欄位「ZEXTRA」對應
ZBODY	聊天訊息內容

表十：ZKIKATTACHMENT 欄位說明

欄位名稱	內容描述
Z_OPT	顯示附檔是否存在，數值 1 表示存在，數值 2 表示已被刪除
ZFLAGS	數值 4 表示有傳送檔案
ZMESSAGE	與資料表「ZKIKMESSAGE」的欄位「Z_PK」對應，找出檔案傳送的順序
ZCONTENT	傳送附檔之 UUID

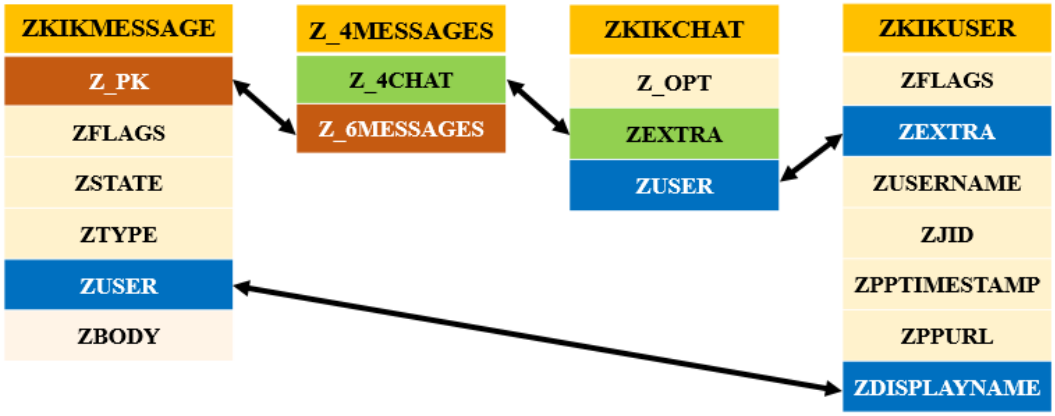
當需要分析聊天內容時，便須利用上述資料表間互向對應，找出聊天紀錄傳遞之順序，如圖二十：

第 1 步：在資料表「ZKIKUSER」的欄位「ZDISPLAYNAME」，找到聊天雙方的使用者名稱，再由欄位「ZDISPLAYNAME」對應到同資料表的欄位「ZEXTRA」，並提供數值；

第 2 步：由第 1 步所提供之數值，對應到資料表「ZKIKCHAT」的欄位「ZUSER」，再對應到同資料表的欄位「ZEXTRA」，找出互動紀錄的數值；

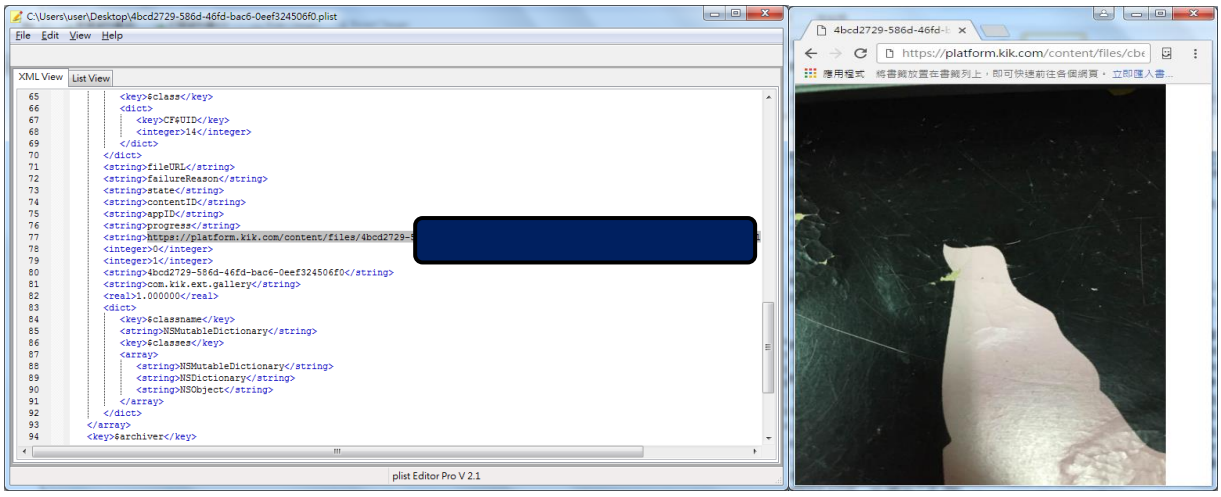
第 3 步：由第 2 步提供之互動紀錄數值，對應到資料表「Z_4MESSAGES」的欄位「Z_4CHAT」，再對應到同資料表的欄位「Z_6MESSAGES」，提供訊息內容的數值；

第 4 步：由第 3 步提供之訊息內容數值，對應到資料表「ZKIKMESSAGE」的欄位「Z_PK」，再對應到同資料表的欄位「ZBODY」，即可找出聊天訊息之內容。



圖二十：Kik 各資料表間互相串聯之關係

若聊天紀錄內有傳送附檔資料，如圖片、影片、塗鴉等，可由資料表「ZKIKMESSAGE」的欄位「Z_PK」，對應到資料表「ZKIKATTACHMENT」的欄位「ZMESSAGE」，再對應到同資料表的欄位「ZCONTENT」，如此可得知所傳送附檔之 UUID，並至“/var/mobile/Applications/group.com.kik.chat/cores/private/fbd041558d884548bf3aebd0c26be09b/content_manager/data_cache”路徑下，找尋相同 UUID 的檔名，即可得知所傳送之附檔為何。此外，在“/var/mobile/Applications/group.com.kik.chat/cores/private/fbd041558d884548bf3aebd0c26be09b/content_manager/metadata_cache”路徑下，存有傳送附檔之 plist 檔，以 Plist editor 開啟，可發現有一 URL 網址，此為這檔案在 kik 伺服器上之位置，將此 URL 以瀏覽器開啟，亦可看到所傳送之附檔檔案，並可供下載，如圖二十一。

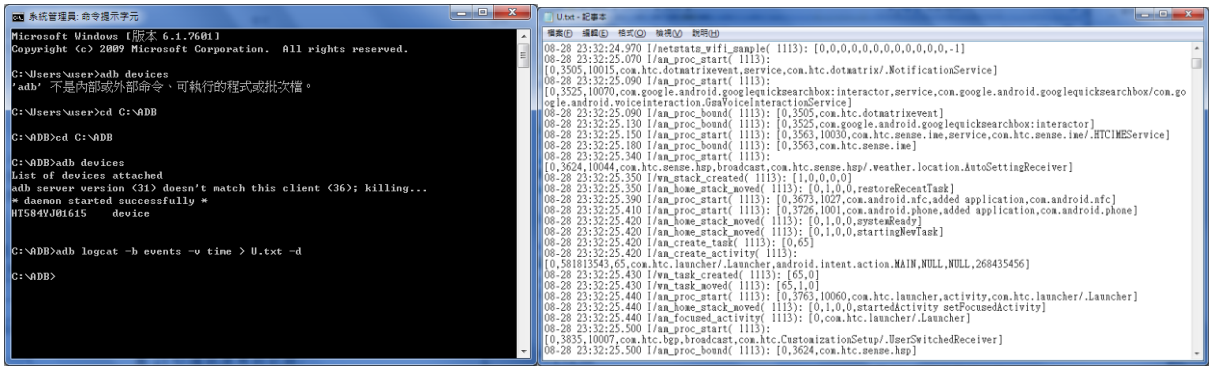


圖二十一：Plist editor 開啟附檔之 plist 檔及以瀏覽器開啟附檔之 URL 網址

3.4 交通事故鑑識案例探討-以 U 通訊即時通訊軟體為例

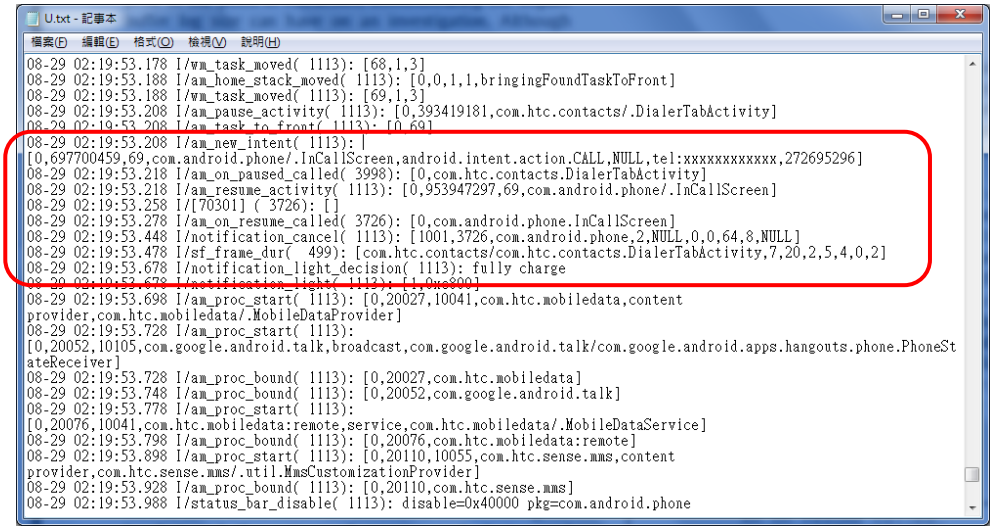
T 城市市區道路上發生一起轎車與機車相撞事故，當調查人員到場欲進行調查時，轎車駕駛 A 君竟駕車逃逸，所幸調查人員隨即通報線上人力，在幾個路口後即將轎車攔下。A 君表示，轎車原預訂在上一個路段靠右邊停，在要臨停時，有減慢車速且打右轉方向燈，但這時騎乘機車的 B 君忽然竄出執行，因煞車不及而導致兩車相撞。但 B 君卻說，他一直都騎在轎車的右側，是因為 A 君在要靠邊停時，有疑似在使用手機，所以才會沒注意到右車機車，造成事故發生。因現場路口剛好沒有架設監視器，雙方也未裝設行車記錄器，亦無目擊者，所以調查人員只能從 A 君的手機上找尋跡證。

倘如 B 君所言，A 君極有可能是在打電話，但查看 A 君手機內通話紀錄，發現通話記錄都是空白的，疑似遭人刪除，雖本件事故雖有牽涉肇事逃逸，但就現行「通訊保障及監察法」規定，仍無法調閱通聯，造成難以判斷 A 君於事故發生前是否有使用手機。於是為了確認 A 君於事故發生前是否有使用手機，調查人員首先將 HTC 手機連接上電腦，並透過 ADB 工具進行連接，以“－v time”指令，匯出指定的日誌檔內容，如圖二十二。

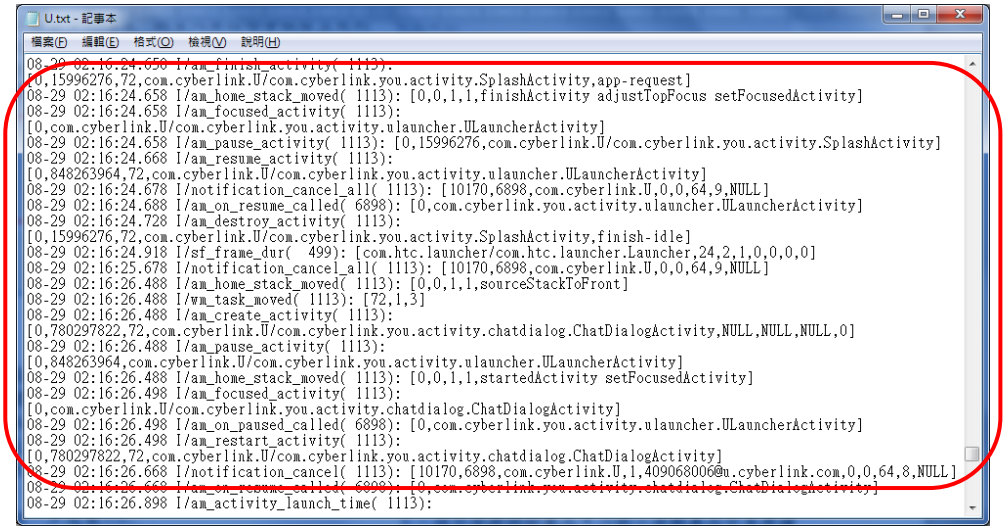


圖二十二：以“－v time”匯出日誌檔及其內容

在匯出日誌檔後，調查人員搜尋事故發生前的相關紀錄，找到 A 君撥打電話的紀錄（如圖二十三），另也發現通訊軟體 U 通訊的使用紀錄（如圖二十四）。



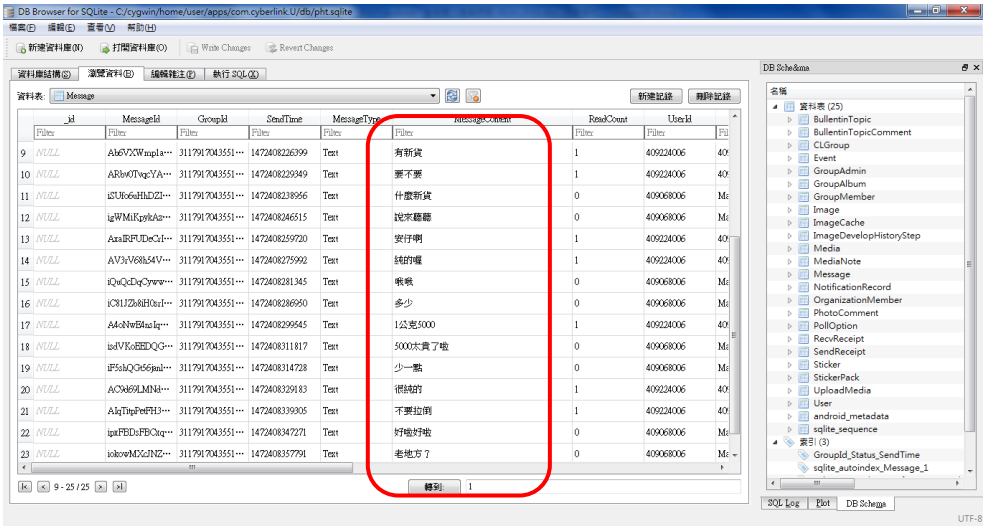
圖二十三：電話使用的記錄



圖二十四：U 通訊使用的記錄

在確認從 A 君手機匯出的日誌檔後，調查人員對 A 君在一次進行詢問，並將相關日誌檔事件內容告知 A 君，而 A 君也承認確實在事故發生前，因有與朋友通話而分心，但對使用通訊軟體的過程，卻支吾其詞，令調查人員起了疑心，且當初在現場調查時，為何 A 君會忽然駕車逃逸，這使得調查人員決定進一步追查。

調查人員首先將手機內的 U 通訊軟體，利用 ADB 備份工具進行備份，備份完後，將備份檔放入 Cygwin 資料夾裡的 home\user\底下，並利用解壓縮腳本進行解壓縮，完成後，最後再利用 SQLite Database Browser 工具，檢視聊天紀錄。當調查人員檢視 U 通訊裡的聊天紀錄時，發現 A 君與一個名稱叫 Mark 的人，在事故發生前亦有聊天紀錄，且紀錄內容談及「安仔」(安非他命的暱稱) 的交易事情，如圖二十五。



圖二十五：A 君與 Mark 的聊天紀錄

有了這線索後，再次向 A 君詢問有關發生事故前，使用通訊軟體的情形，並將相關聊天紀錄告知 A 君，終於，A 君坦承今日的確要跟 Mark 進行交易，因此看到調查人員進行調查時，才會因一時緊張而駕車逃逸，而隨後調查人員便在 A 君的轎車上，搜出安非他命毒品 5 小包，並朝毒品交易罪嫌偵辦。

肆、討論與分析

由第參節可得知，本文所提利用行動裝置的日誌檔及備份檔，進行數位鑑識之技術與方法，確實可在 iOS 及 Android 等行動裝置上，找到相關數位跡證，而這些跡證也都與交通事故相關聯。以下再分別針對行動裝置日誌檔、備份檔及即時通訊軟體鑑識研究發現進行討論與分析。

4.1 行動裝置日誌檔、備份檔

本文針對不同行動裝置的作業系統 iOS 及 Android，利用開發人員的開發工具，或行動裝置製造商所發行的同步程式執行同步備份，再將其備份檔進行數位跡證分析調查，找出即時通訊軟體會留下哪些數位痕跡。2 種行動裝置平臺的相關日誌檔及備份檔比較如表十一所示。

此外，在實驗過程中發現，在利用 ADB 工具進行備份時，雖然不設定備份檔的密碼，但若手機有設定密碼來鎖定螢幕，則備份出來的備份檔在解壓縮時，也是需要輸入該鎖定螢幕的密碼，才可完成解壓縮。

表十一：行動裝置匯出日誌檔及備份檔之比較

行動裝置平臺	iOS	Android
須「越獄」或「取得最高權限」	X	X
日誌檔匯出功能	V（透過 iTools 工具）	V（透過 ADB 工具）
日誌檔之內容	可顯示螢幕有解鎖的紀錄，但無法找出使用何種應用程式	可清楚顯示行動裝置之使用紀錄
備份檔密碼設定	V	V
備份檔路徑設定	V	V
備份檔分析方式	由 iTools 工具找出備份檔所在路徑，再將其.plist 或.sqlite 檔案以相關工具開啟檢視	須先經過解壓縮的程序，再以相關工具開啟檢視.plist 或.sqlite 檔案

4.2 即時通訊軟體鑑識分析

本文所使用的 U 通訊及 Kik 即時通訊軟體，若以 iPad Air 2 及 HTC M9u 等行動裝置，均可利用 iTunes 及 ADB 工具對其進行備份功能，再透過相關工具鑑識分析其備份檔，進一步獲取聊天紀錄等相關資訊。相關重要跡證路徑如表十二所示。

表十二：即時通訊軟體鑑識分析比較

類別	iOS		Android	
	重要跡證儲存路徑	有重要跡證之檔案	重要跡證儲存路徑	有重要跡證之檔案
U 通訊	/var/mobile/Applications/com.cyberlink.U	UData.sqlite com.cyberlink.U.plist	~\apps\com.cyberlink.U	pht.sqlite
Kik	/var/mobile/Applications/group.com.kik.chat	kik.sqlite group.com.kik.chat.plist 相關多媒體檔案	~\apps\kik.android	kikDatabase.db

此外，在實驗過程中發現，若使用者於 Kik 應用程式中刪除單一聊天紀錄，就無法找到其訊息，僅能利用訊息之編號排序得知，有訊息遭使用者刪除，然而，對於聊天中所傳送之附檔，如圖片、手繪塗鴉等，若使用者將其刪除，仍可利用備份檔中，描述附檔的 plist 檔，找到其上傳至 Kik 伺服器之 URL 位置，透過瀏覽器即可下載。

伍、結論

智慧型行動裝置是近年來最具顛覆性的創新產品，其幾乎影響了民眾日常生活中的每個領域，然而，也因智慧型行動裝置的普及，其所產生的治安及交通問題，日益漸增。在以往交通事故的調查，監視器影像扮演相當重要的角色，幾乎所有案件皆以監視器影像為判斷肇事原因之依據，然並非所有案件皆有監視器影像佐證，而調查人員在處理此類案件時，除向現場目擊者詢問，或找尋前、後車之行車記錄器，難以有其他調查方式，且要證明因用路人分心而導致事故發生，更是難上加難，就算有監視器影像，也會因拍攝角度、光線等因素，無法直接證明用路人分心之情事。

此外，當使用商業型行動裝置鑑識軟體工具對用路人的行動裝置進行鑑識時，也會因最新款或最新版本作業系統問題，導致調查人員無法利用該工具進行鑑識分析，又智慧型行動裝置的鑑識，對於一般人員來說，技術門檻較高，不易自行完成分析工作。也因為如此，本文主要以 iTools 及 ADB 工具匯出行動裝置的日誌檔及所產生的備份檔進行研究，利用行動裝置之日誌檔判別使用的行為，再針對備份檔內的即時通訊軟體進行鑑識分析，提供找出行動裝置的使用行為，及可能相關聯資訊的一種鑑識調查方式。本文以於 iOS 及 Android 行動裝置上，使用 U 通訊、Kik 等即時通訊軟體為標的，探討以日誌檔及備份檔解決交通事故發生原因調查之方法，並以案例實驗測試確認本文所提出的鑑識調查方法確實可行，而所提出的方法除可解決目前 iOS 及 Android 行動裝置商業型數位鑑識軟體工具之支援度不足，更能提供在 iOS 及 Android 行動裝置上的各類應用程式進行數位鑑識調查之方向參考。

日新月異的科技發展時代，行動裝置數位鑑識人員可能因行動裝置的硬體或作業系統的更新速度，面臨難以突破之瓶頸與嚴峻的挑戰，因此數位鑑識人員除了熟悉現行的行動裝置商業型數位鑑識工具，更必須即時瞭解各行動裝置設備，並嘗試找尋既有的資源，透過現有的工具軟體，找出對應的鑑識分析方式，以進行有效及準確的調查。本文提出的方法主要貢獻為提供第一線調查人員可透過判別和檢視 iOS 及 Android 行動裝置的相關日誌檔及備份檔，快速找出使用者對於行動裝置的使用行為，藉以判斷其與交通事件或犯罪行為之關連性，並作為交通事件原因分析或案件後續追查之參考依據。

參考文獻

[1] N. Al Barghouthy, A. Marrington and I. Baggili, “The Forensic Investigation of Android Private Browsing Sessions Using Orweb,” *International Conference on IEEE*, 2013, pp. 33-37.

[2] M. Bader and I. Baggili, “iPhone 3GS Forensics: Logical Analysis Using Apple iTunes

Backup Utility," *Small Scale Digital Device Forensics Journal*, VOL. 4, NO.1, 2010.

[3] D. Bennett, "The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations," *Information Security Journal: A Global Perspective*, Vol. 21 , Issue3, pp. 159 -168, 2012.

[4] S. Bommisetty, R. Tamma and H. Mahalik, *Practical Mobile Forensics*, 1st ed., Packt Publishing Ltd., 2014.

[5] Cygwin authors, Cygwin, Retrieved from https://www.cygwin.com/ (2016/8/28).

[6] Developers, Android Debug Bridge, Retrieved from http://developer.android.com/tools/help/adb.html (2016/8/28).

[7] Developers, Configuring Auto Backup for Apps, Retrieved from https://developer.android.com/training/backup/autosyncapi.html (2016/8/28).

[8] Developers, Dashboards , Retrieved from http://developer.android.com/intl/zh-tw/about/dashboards/index.html (2016/8/28).

[9] Developers, Reading and Writing Logs , Retrieved from http://developer.android.com/tools/debugging/debugging-log.html (2016/8/28).

[10] M. Epifani and P. Stirparo, *Learning iOS Forensics*, 1st ed., Packt Publishing Ltd., 2015.

[11] M. Faheem, N. A. Le-Khac and T. Kechadi, "Smartphone Forensic Analysis: A Case Study for Obtaining Root Access of an Android Samsung S3 Device and Analyse the Image without an Expensive Commercial Tool," *Journal of Information Security*, 2014, pp. 83-90.

[12] J. He, W. Choi, J. S. McCarley, B. S. Chaparro and C. Wang, "Texting While Driving Using Google Glass™: Promising but Not Distraction-free," *Accident Analysis & Prevention*, 2015, pp. 218-229.

[13] A. Hoog and K. Strzempka, "iPhone and iOS Forensics: Investigation, Analysis and Mobile Security for Apple iPhone, iPad and iOS Devices," *Elsevier*, 2011.

[14] G. Horsman and L. R. Conniss, "Investigating Evidence of Mobile Phone Usage by Drivers in Road Traffic Accidents," *Digital Investigation*, 2015, S30-S37.

[15] M. I. Husain and R. Sridhar, "iForensics : Forensic Analysis of Instant Messaging on Smart Phones," *International Conference on Digital Forensics and Cyber Crime*, 2009, pp. 9-18.

[16] J. Ige, A. Banstola and P. Pilkington, "Mobile Phone Use While Driving: Underestimation of a Global Threat," *Journal of Transport & Health*, 2015.

[17] W. Jansen and R. Ayers, *Guidelines on Cell Phone Forensics*, NIST Special Publication, 2007.

[18] K. J. Karlsson and W. B. Glisson, "Android Anti-Forensics: Modifying Cyanogenmod,"

International Conference on System Sciences, 2014, pp. 4828-4837.

[19] J. Lessard and G. Kessler, "Android Forensics: Simplifying Cell Phone Examinations," *Small Scale Digital Device Forensic Journal (SSDDFJ)*, vol. 4, no. 1, 2010.

[20] A. Oulasvirta, T. Rattenbury, L. Ma and E. Raita, "Habits Make SmartPhone Use More Pervasive," *Personal and Ubiquitous Computing*, Volume 16, Issue 1, 2012, pp. 105-114.

[21] K. M. Ovens and G. Morison, "Forensic Analysis of Kik Messenger on iOS Devices," *Digital Investigation*, 17, 2016, pp. 40-52.

[22] C. Sgaras, M. T. Kechadi and N. A. Le-Khac, "Forensics Acquisition and Analysis of Instant Messaging and VoIP Applications," *Computational Forensics*, 2015, pp. 188-199.

[23] Sqlitebrowser, DB Browser for SQLite, Retrieved from http://sqlitebrowser.org/ (2016/8/28).

[24] Y. C. Tso, S. J. Wang, C. T. Huang and W. J. Wang, "iPhone Social Networking for Evidence Investigations Using iTunes Forensics," *the 6th International Conference on Ubiquitous Information Management and Communication*, no 62, 2012.

[25] WHO, Mobile Phone Use: a Growing Problem of Driver Distraction, Retrieved from http://www.who.int/violence_injury_prevention/publications/road_traffic/distracted_driving_en.pdf, 2011.

[26] Cyberlink, U 通訊 App , Retrieved from http://tw.cyberlink.com/stat/product/CyberLink_app/U/cht/U.jsp (2016/8/28).