智慧型手機 資料刪除之救援技術

陳受湛 / 法務部調查局科長
林育峰 / 鑒真數位有限公司鑑識顧問
黃敬博 / 鑒真數位有限公司執行長
洪啟恒 / 鑒真數位有限公司技術長

一、前言

隨著智慧型行動裝置愈來愈普及，人們對智慧型手機的依賴日深，它具備了通訊錄、記事、行事曆、地圖、導航，以及聊天軟體App等等功能。一台智慧型手機便能滿足人們生活中的大小需求，因此儲存在手機上的資料，其重要性不言可喻。尤其是社群與聊天軟體App，取代了傳統的電話與簡訊等通訊方式，舉凡文字訊息、影音訊息或檔案的傳送接收等功能均十分便利快速，成為聯繫溝通的主要平台。手機當中所呈現的即是一個人的生活縮影，因此在鑑識分析上，手機資料刪除之救援回復亦成為一個十分重要的議題。

二、手機資料的儲存

（一）儲存媒體

依手機資料儲存媒介的不同，手機的資料儲存主要有三區塊，分別為SIM卡、外接式記憶卡及手機內建儲存記憶體。分別說明如下：

1. SIM卡

SIM 卡內的資料主要可分為 2G/3G/4G，其資料格式均為公開之規範，一般可用普通的讀卡機讀取未遭刪除的資訊，主要是記錄SIM卡ID 及手機號碼對應之ID統稱為ICCID(GSM)及IMSI，另外可貯存通訊錄、簡訊及通話紀錄。若搭配專用的鑑識軟體XRY或Cellebrite均可恢復此部份刪除的資訊。但由於智慧型手機的資訊大多已儲存在手機記憶卡及內建的儲存記憶體，因此對於SIM卡的資料回復已較無重要性，但對於嫌犯是否使用此SIM卡撥號的IMSI對應則仍有其關鍵鑑識之需求。

2. 外接記憶卡

手機外接記憶卡，最常見的記憶卡為Micro SD 卡 ，由於iPhone本身並無支援外接式記憶卡的裝置，因此此類型的儲存裝置只見於非iOS平台之智慧型手機。目前隨著手機設計的應用趨勢，新款的中高階手機也多傾向於使用內建儲存記憶體，因此外接式記憶卡的資料儲存也漸漸式微。在處理外接式記憶卡時，一般儲存的資料較多為照片、影音或個人下載多媒體音樂等，因此對於此類的資料救援困難度並不高。在救援時可採用防寫式的讀卡設備，搭配專業的資料救援軟體即可適當的進行刪除檔案的救援回復。主要需克服的問題，在於軟體必需能支援BlackBerry/NTFS/FAT/Linux/iOS…等不同的檔案系統，救援的方式主要有三類型：第一，檔案剛遭刪除則系統的索引表只作標記，但實體資料及索引表均未刪除的狀態，第二，檔案刪除並有新檔案存入，部份主關連的索引表被覆寫，此時仍可保留檔名，但無法正確解析全路徑，且可能部份內容遭覆寫的狀態，第三，檔案刪除並有新檔案存入，且原有檔案索引表徹底遭覆寫的狀態，以上第一及第二種狀況均可用一般的鑑識軟體EnCase或FTK或X-Ways來進行救援。而第三種狀態，則必需利用檔案內容Hex特徵的定義來挖取及還原(一般稱為Carving的救援方式),利用此一方式的資料救援則可能產生救援結果的差異，因此好的救援軟體可以很精準的定義出內容Hex特徵並予以拼湊還原，國際上NIST每隔一段時間即會針對各鑑識軟體進行驗證評比[1]。

3. 手機內建儲存記憶體

多媒體卡協會（MultiMediaCard Association，簡稱MMCA）針對手機與平板電腦等消費性電子產品，製定了內嵌式記憶體的標準規格——eMMC（embedded Multi Media Card），簡化記憶體的設計，採用多晶片封裝將NAND Flash晶片和控制晶片整合在一起，可以省去零組件佔用

電路板的面積。eMMC具備高容量的彈性，支援有效讀寫、開機、睡眠模式、雙通道資料傳輸率、多重磁區支援，以及系統安全強化等優勢。但eMMC的資料貯存物理特性將完全不同於傳統硬碟利用磁性的資料貯存方法，資料貯存的實際位置將主要取決於控制晶片的演算法，因此不同品牌的NAND Flash記憶體晶片均會有不一樣的資料貯存管理模式，對於資料刪除後的保留也有不同的對應方式，傳統硬碟中的資料遭刪除後，資料仍會保存於硬碟中的不同碟片的磁軌上，直到新資料寫入原有磁軌位置後，舊資料才會真正遭抹除，但手機內建儲存記憶體對於刪除的資料，控制晶片有可能會進行資料清除的實際動作，且部份晶片內建加密模組，預設資料寫入時即為加密狀態，因此若無取得正確的解密金鑰，資料亦無法救援，此部份為資料救援中手機與一般電腦可能面臨的不同地方。

手機內部儲存空間當中包含了作業系統、所安裝的App及使用者資料，是進行資料回復時的重點所在。但由於它並非如同電腦中的硬碟一般易於拆卸，加上手機廠商會加入Bootloader鎖定等安全措施，因此在進行手機映像檔獲取(Acquire)時往往會面臨比硬碟獲取更多的障礙。

（二）儲存系統

檔案系統是一種儲存和組織資料的方法，它使得對其存取和尋找變得容易，檔案系統使用檔案和樹狀目錄的抽象邏輯概念代替了儲存裝置使用資料區塊的概念。使用者使用檔案系統來儲存資料不必關注資料實際儲存在儲存裝置的物理位址，只需要記住這個檔案的所屬目錄和檔案名。 在寫入新資料之前，使用者不必考慮儲存裝置上的那個區塊位址沒有被使用，儲存裝置上的儲存空間管理功能由檔案系統自動完成，使用者只需要知道資料被寫入到了哪個檔案名稱之中即可。

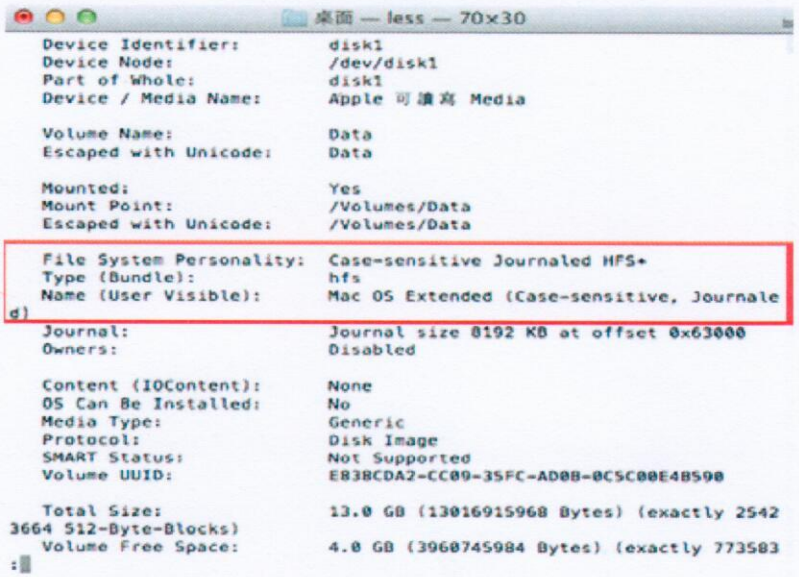

圖1

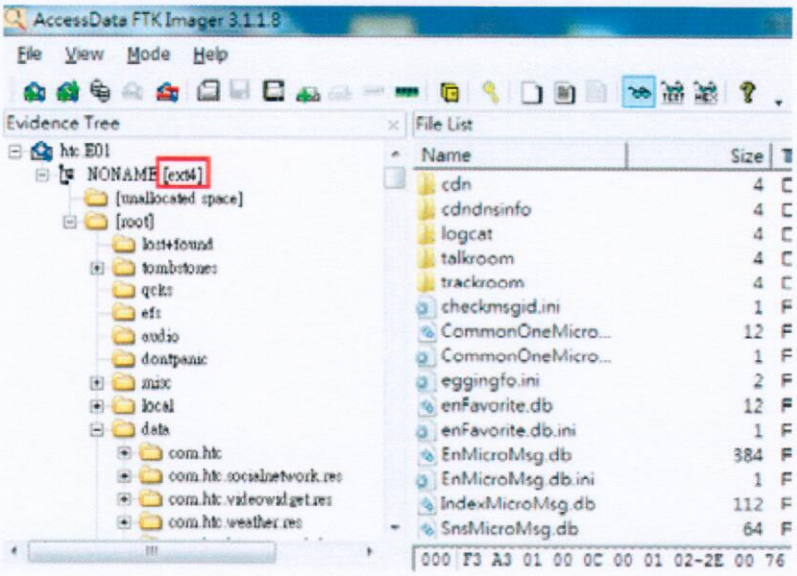

圖2

iOS平台的檔案系統為HFS+ Journaled，而Android平台主要則為Ext2/3/4。在對iPhone進行JB及對Android手機進行Root之後，透過物理獲取(Physical Acquisition)的方式產生證物映像檔（如圖1~圖2所示）後，便可進行掛載。再以鑑識工具或資料救援工具進行資料回復，很大的可能是可以回復被刪除的資料。

三、手機資料的刪除

手機資料的”刪除”的意涵可以分為檔案系統層面的刪除及資料庫層面的刪除，分別說明如下：

（一）檔案系統層面的刪除

在檔案系統層面的刪除，例如刪除了一個文件、一張照片或一段影片，不論是iOS或是Android平台，皆會把刪除的資料放至所謂的Unallocate Space，在這個Unallocate Space的資料是否能順利回復，基本上在尚未被新寫入進的資料覆蓋之前，還是有機會可進行回復，但仍需視不同平台版本、貯存晶片及加密與否而定，新版的作業系統往往具有更高的安全性，此也導致刪除資料回復的難度更高。

（二）資料庫層面的刪除

在資料庫層面的刪除，例如在聊天軟體LINE或WeChat的聊天介面中，進行聊天訊息的刪除等動作，其實並未被”真正”刪除。因為這些App是基於使用SQLite資料庫的機制，雖然在聊天App介面中已看不到那些被刪除的對話紀錄，但它們仍躺在資料庫檔案中的某處，一個稱

為”free block”及Database本身的”Unallocate”區塊。基本上在尚未被新寫入資料庫進的資料覆蓋之前，還是有機會可進行回復，但仍需視該App不同版本而定，新版的App往往具有更高的安全性，此也易導致刪除資料回復的難度更高。

（三）針對刪除仍未被抹除訊息的資料庫之Hex 特徵研究

主流通訊軟體例如”Line”、”Wechat”、”Skype”或”WhatsApp”等均為使用SQLite Database[2]來儲存訊息之手機通訊軟體。以硬碟為例，資料刪除後會移動到Unallocated Space，SQLite適用同樣的觀念但是多了一個freeblock區塊。故在SQLite內，刪除的訊息資料會存在Unallocated Space以及freeblock[3]兩個位置，必須將這兩個位置都檢視過才是回復所有刪除的資料。如下圖3所示為”Leaf Table Page”[4]的結構，其中只有看到Unallocated Space，而freeblock實際上是位於Cell content area中。

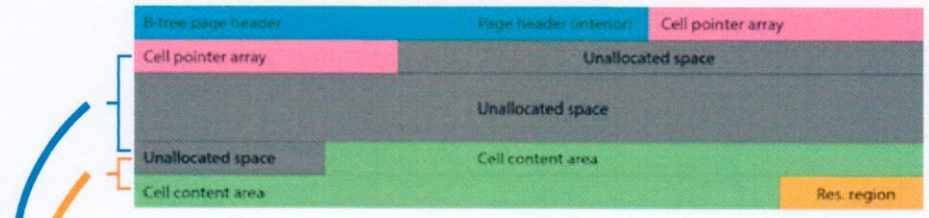

圖3

詳細說明如下圖4所示，第2個freeblock的意思為將此位置之content area的訊息刪除，而此位置前後的訊息都還存在的時候，此時就會變成freeblock區域。

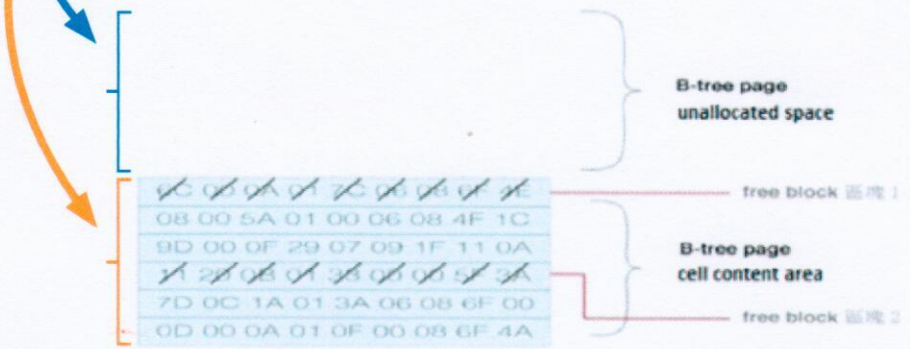

圖4

各種Page都有其header來代表，如下圖5所示，第0個byte “\x0D”代表此Page為Leaf Table Page。第1-2 byte代表第一個freeblock位置，此位置就是儲存刪除訊息的位置之一。第3-4 byte代表此Page內現有訊息之數量，不包含刪除的訊息。第5-6 byte代表Cell Content Area起始的位置，配合圖3可以發現Cell Content Area上方即為Unallocated Space，所以從此位置往上即可找到另一個儲存刪除訊息的位置。

Hex	Decimal	Description
0D	13	Page type - Leaf table b-tree
05 05	1285	Two byte integer - start of first freeblock
02 10	528	Two byte integer - number of cells
05 14	1300	Two byte integer - start of cell content area

圖5

因此如果要找到所有的freeblock的位置，除了第一個freeblock起始位置外還需要兩個資訊; freeblock的大小及下一個freeblock的起始位置。這兩個資訊都可以從第一個freeblock位置的前4個byte找到。第0-1 byte代表下一個freeblock的位置，若為\x00\x00則代表沒有下一個freeblock。第2-3 byte代表此freeblock之大小，也代表freeblock的區塊。每一個區塊中記錄著Table裡面所建立的欄位資訊內容，其中一個欄位就是儲存訊息的內容，故必須了解此區塊中每個byte所代表的意義才能找到刪除的訊息，因此只要將所有freeblock以及UnallocatedSpace依上述相同方式進行分析，即可將此SQLite檔案內之刪除訊息全數還原。

四、手機資料的回復

（一）iOS平台

iOS是蘋果公司所生產的iDevcice如iPhone、iPad等所使用作業系統，而iPhone在4s及之後的機型，均具備了硬體加密的晶片，資料安全性備增。一旦照片、檔案等資料刪除會被放至所謂的Unallocated space，便再無回復的可能。但iOS8之後新增了一個功能叫”最近刪除”，亦即照片的資源回收筒，裡頭存放已刪除的照片，除非再進行”全部刪除”或是過了刪除照片上面所顯示的剩餘天數，刪除的照片才會徹底被刪除(如圖6所示)。

圖6

以鑑識軟體UFED Physical Analyzer採用Advanced Logical Method模式擷取iPhone 6內的資

料，iPhone 6的作業系統版本為9.2且未越獄(Jail Break)，(如圖7~圖8所示)，未能擷取已刪除的檔案。但是可擷取出手機資料庫檔案中的遭刪除之聯絡人資料，(如圖9所示)。這是由於聯絡人資料是存放在SQLite資料庫中之故，因此只要能順利擷取出該資料庫檔案，便有機會自資料庫檔案中將被刪除的聯絡人資料加以回復。

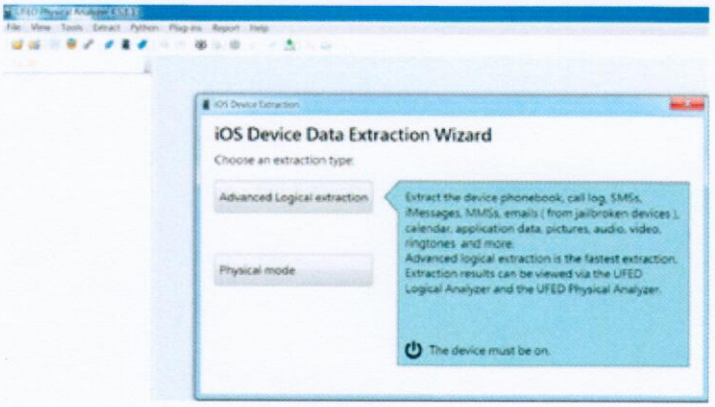

圖7

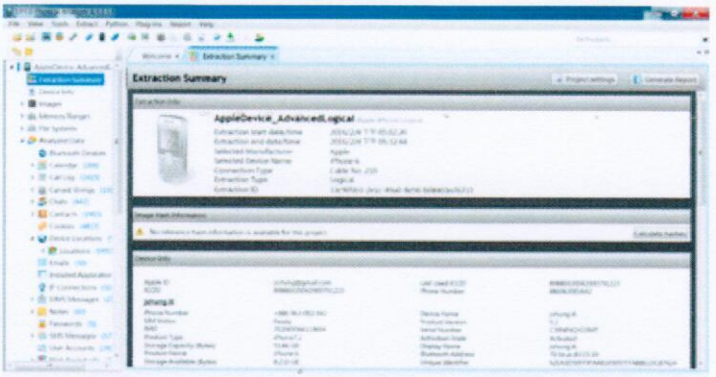

圖8

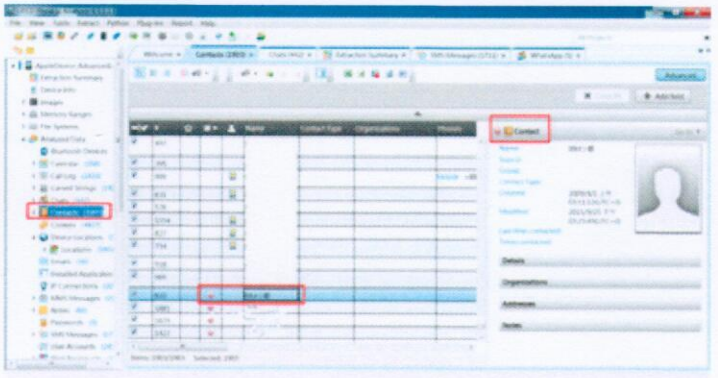

圖9

在iOS平台欲回復更多遭刪除的資料，必須是在已越獄(Jail Break)的狀態下才有可能。我們以iPhone 5s搭配iOS 9.0.2(如圖10所示)，在越獄之後，以資料救援軟體WonderShareDr.Fone(如圖11所示)進行測試，可順利回復遭刪除的項目包括簡訊、網頁瀏覽紀錄、行事曆、通訊紀錄、聯絡人(如圖12~圖13所示)。由此可得知在iPhone已JB越獄的情況下便能較大程度將iOS被刪除資料回復，但以上這些資訊主要仍是存在於資料庫內而非檔案形式才能進行回復，若是檔案型態則仍無法回復。

圖10

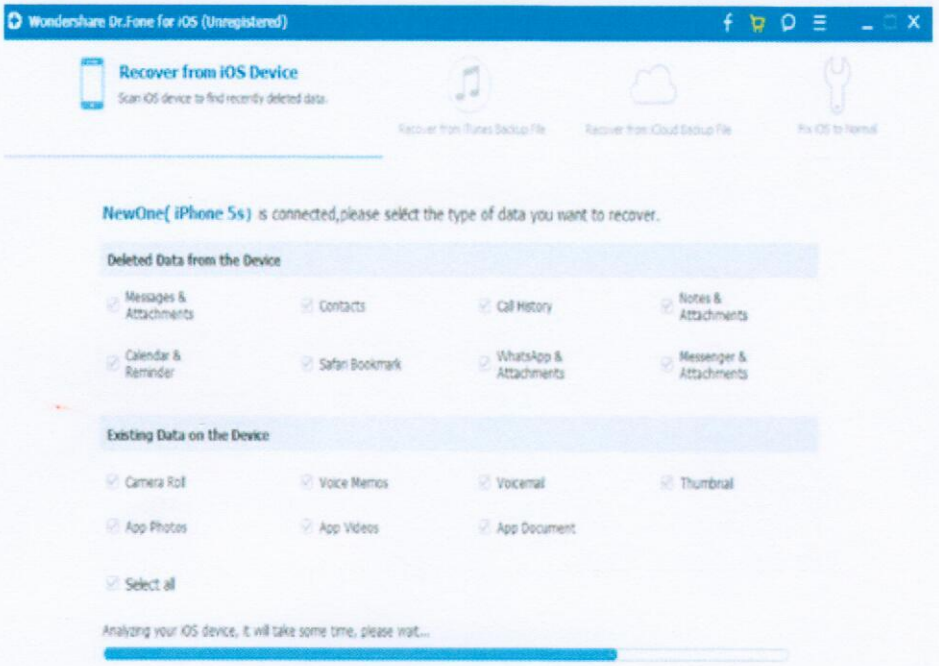

圖11

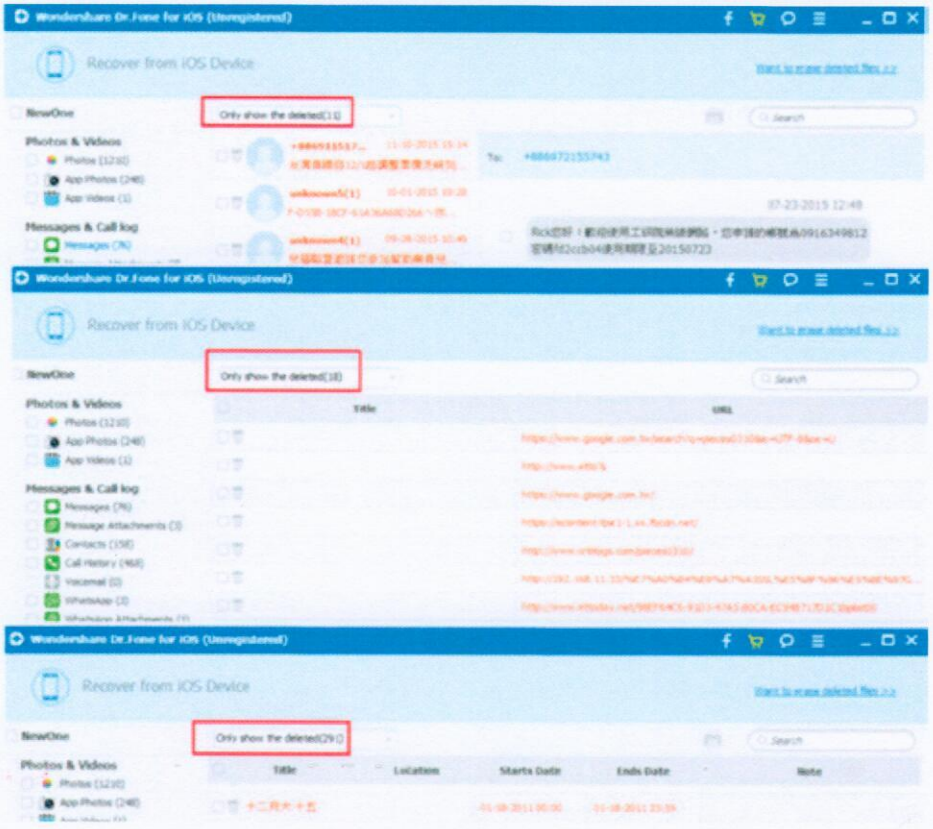
Wondershare Dr.Fone for iOS (Unregistered)
Recover from iOS Device
Only show the deleted(11)
Only show the deleted(18)
Only show the deleted(29)
Photos & Videos
Messages & Call log

圖12

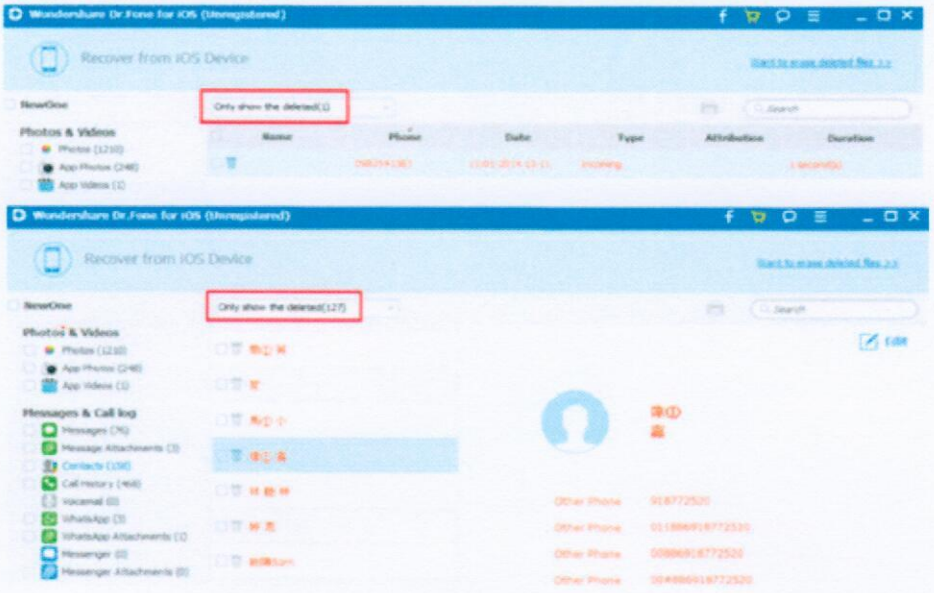
Wondershare Dr.Fone for iOS (Unregistered)
Recover from iOS Device
Only show the deleted(1)
Only show the deleted(127)
Photos & Videos
Messages & Call log

圖13

（二）Android平台

Android為Goolge公司所研發的作業系統，以Linux為核心，屬於開源系統，盛行於各種嵌入式設備。在Android平台之下，若要最大可能地回復被刪除的資料，則需要進行Root提權。以hTC J預設搭配Android 4.0.4，進行Root之後(如圖14所示)，以WonderShareDr.Fone進行資料回復，可回復項目如照片、通話紀錄、聯絡人、刪除的檔案、簡訊。針對較新版的Android4.4或Android5.x其救援狀況亦類似，由此得知在Root提權的狀況下較能順利回復遭刪除的檔案(如圖15~圖16所示)。

圖14

圖15

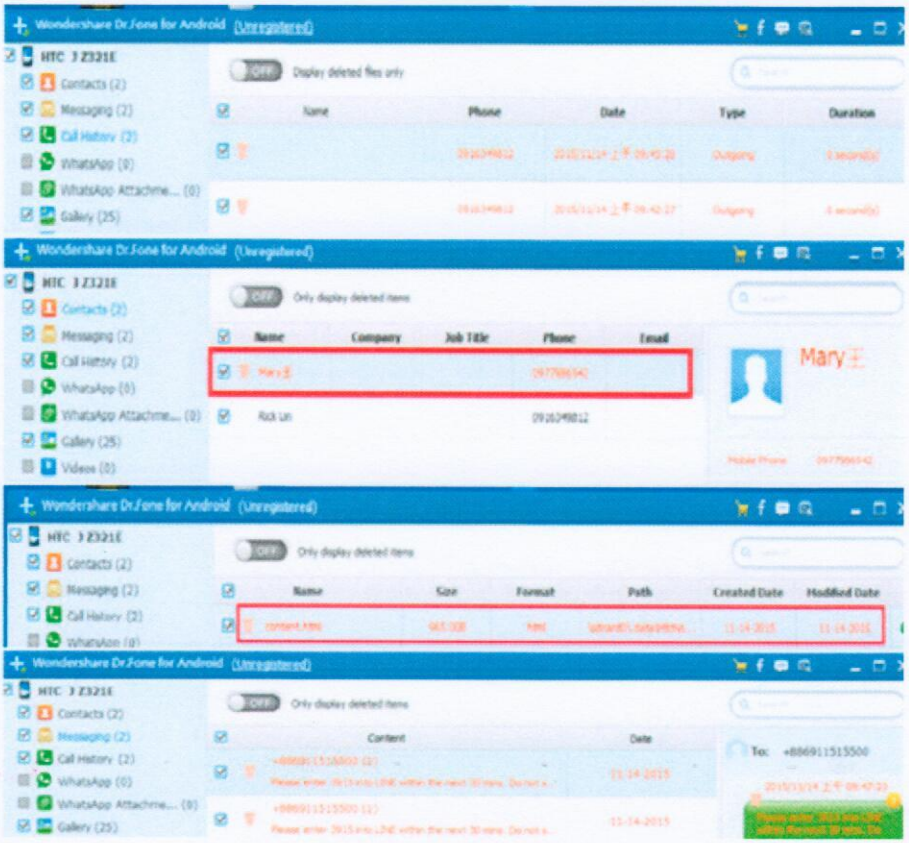

圖16

在資料庫檔案內的遭到刪除之聊天訊息，之所以能夠加以回復，是基於資料庫的特性，所謂的刪除並非真正徹底刪除，因此只要在尚未被新寫入進的資料覆蓋之前，仍有機會回復。但目前有些App如LINE的5.3版之後及WeChat 6.2版之後，已具備了徹底刪除，亦即抹除(Wipe)的特性。以Oxygen Forensic SQLite Viewer對LINE 5.5.1版進行測試，開啟LINE資料庫檔案naver_line，檢視資料表chat_history，在”Blocks containing deleted data”的頁籤中未看到任何遭到刪除的聊天訊息，而是全部遭到填零 除了(如圖17所示)。再以WeChat 6.3版進行測試，因為WeChat在Android平台的資料庫檔案EnMicroMsg.db是加密保護的檔案，無法直接以SQLite Browser等軟體進行檢視，若以WinHex進行檢視亦只能看到加密的內容(如圖18所示)。因此需先設法解出加密用的key值，再以SQLCipher進行處理。將處理過後的資料庫檔案wechat6.db以Oxygen Forensic SQLite Viewer開啟，檢視資料表messages，在”Blocks containing deleted data”的頁籤中未看到任何遭到刪除的聊天訊息，如同LINE新版的資料庫情況，亦已全部遭到填零 除了(如圖19所示)。未來若更多App跟進此一特性，將使得聊天訊息回復所面臨的挑戰更加艱鉅嚴峻，但若一般無抹除功能的資料庫， 對於刪除的資訊則可在未覆寫前進行回復。

五、結語

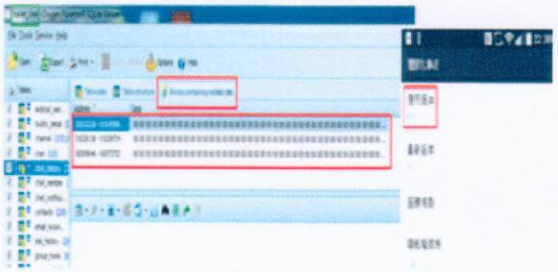

圖17

目前智慧型手機除特有的通訊功能及APP應用外，其複雜度已超過傳統電腦上的大部份功能，在資料救援領域也大不同於以往處理電腦硬碟資料之方式，對應於各種新式手機更嚴謹的加密及保護機制，使得資料救援的困難度也相對提高，因此手機鑑識領域一直是目前最多問題有待突破的重點之一，本次僅就實務上提出相關的資料刪除回復心得，由於要能救回較多刪除的資訊往往需要Root或JB手機，此部份仍有改善空間，也希望國內有更多的先進能一同投入此方面研究。FACT

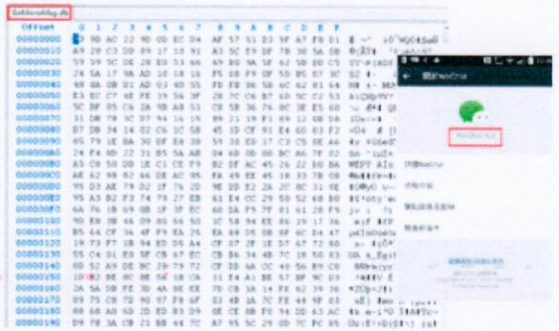

圖18

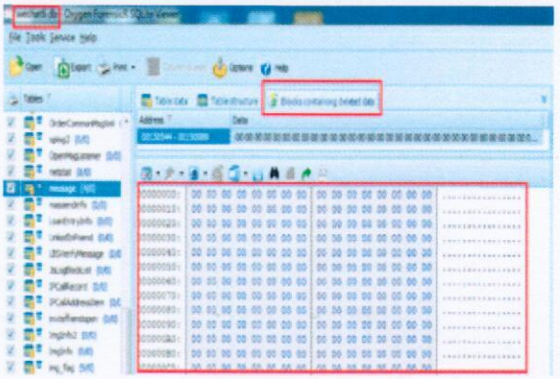

圖19

誌謝

本篇文章關於SQLite部分研究承蒙103年行政院國家科學技術發展技術管理會補助計畫(計畫編號 MOST103-3114-Y-138-003)之經費補助，謹此致謝。

參考文獻

1.http://www.cftt.nist.gov/DeletedFileRecovery.htm

2.SQLite website， “SQLite file format” https://www.sqlite.org/fileformat2.html

3.Martin Westman，"Analysing free pages in SQLite databases"， Micro Systemation，2014.

4.Douglas Comer ，"The Ubiquitous B-Tree", Computer Science Department,Purdue University，1979.