行動裝置數位證據鑑識標準作業程序與案例驗證之探討-以行動鑑識工具 UFED 萃取數位證據為例

林宜隆[1]、方彥霏[2]
[1]元培醫事科技大學資訊管理系教授
[2]國立宜蘭大學多媒體網路通訊數位學習碩士
[1] cyberpaul747@gmail.com

摘要

隨著網際網路技術的提升，手機不再是傳統的通話功能，透過智慧型手機，可以使用通訊軟體互相聯絡、上網瀏覽網頁與交易、儲存個人相關資訊(如照片、記事等)，如同行動電腦。手機帶來的便利性，成為有心人士的犯罪工具，智慧型手機如同行動電腦存在大量的電磁記錄，這些記錄是具備鑑識價值的數位證據。有鑑於此，傳統的鑑識設備與方法，將不足以蒐集手機裡的數位證據。對於數位證據的認知、鑑識工具的選擇與使用，將是鑑識人員必需具備的主要專業與基本認知。

數位證據的蒐集、分析、萃取過程，必須使用標準的數位鑑識流程，本研究參考ISO 27037: 2012、ISO 27041: 2015等國際數位證據處理標準與國內學者林宜隆教授所提出的數位證據鑑識標準作業程序(DEFSOP) 逐步整理建構行動裝置數位證據鑑識標準作業程序（DEFSOP for Mobile Device），並以實際案例模擬，驗證 DEFSOP for Mobile Device的程序無缺漏，以提高其公信力及有效性。手機鑑識作業中，資料的萃取已有一些工具軟體可以使用，萃取所需的證據並不是問題，比較困難的問題是如何妥善運用這些數位證據，發揮其最大效能。本文研究所選擇的鑑識工具為 Cellebrite UFED，透過鑑識軟體萃取相關數位證據，分類並識別資料的可用性及有效性，交叉分析、個化比對，還原犯罪事實。

關鍵詞：UFED、ISO 27037/27041、數位鑑識、行動鑑識、數位證據鑑識標準作業程序

壹、前言

當資訊犯罪發生時，需要依據數位證據的鑑識能力識別及還原真相，使得數位證據鑑識的重要性不容忽視，因此，鑑識人員如果能保全相關數位證據並經由蒐集、分析、鑑定等程序，讓數位證據更能在法庭上被採信，將犯罪人繩之以法。所以，使用的鑑識工具就非常重要。在手機鑑識作業中，資料的萃取已有一些工具軟體可以提供使用，在工具的運用下，萃取所需的證據並不是問題，比較困難的問題是如何妥善運用這些數位證據，搭配各種驗證、整理方法，使其發揮最大效能。參考 ISO 27037: 2012、ISO 27041: 2015 等國際數位證據處理標準及學者林宜隆教授所提出的數位證據鑑識標準作業程序((**Digital Evidence Forensic Standard Operation Procedure ,DEFSOP)**) 逐步整理建構行動裝置數位證據鑑識標準作業程序（DEFSOP for Mobile Device），透過手機鑑識軟體 UFED，進行實例案件分析，驗證(DEFSOP For Mobile Device)，找到犯罪證據，提供專業鑑識執法人員參考依據。

貳、文獻探討

本研究希望設計出基於開放源碼雲端運算架構之高彈性駭客攻防教學平台，來幫助學生進行學習，培育更多的資訊安全人才，替未來全國資訊安全環境打造出可用之兵。

2.1 數位證據

凡是以電腦或相關電子裝置所處理、儲存、傳輸的電子記錄，包含，文字、聲音、影像、照片、符號或其他資料等，透過適當的設備將之讀取出來，用以支持或反證犯罪的證據者都可稱為數位證據。數位證據就是以計算機為基礎或是和計算機及行動裝置有關的證據，儲存於電腦及行動裝置媒體或藉由各類型電腦及行動裝置媒體傳送之資料。任何可以證明犯罪構成要件、犯罪意圖或不在場證明等有關聯的數位資料，為物理證據之一種。目前世界各國及我國法律都尚未對數位證據有正式的定義，只有對電子紀錄、電磁紀錄及電子文件加以定義，使得數位證據的定義非常模糊，根據我國法律及學者的定義，將其定義為藉由電腦或網路設備儲存或傳送可供證據使用，稱之為數位證據，即包括電子文件、電子紀錄及電磁紀錄。因此，唯有專業的鑑識人員，嚴謹的鑑識流程，以及專業的鑑識工具，才能確保蒐集到的數位證據具有法律效力及避免同樣的證據產生不同的解讀。

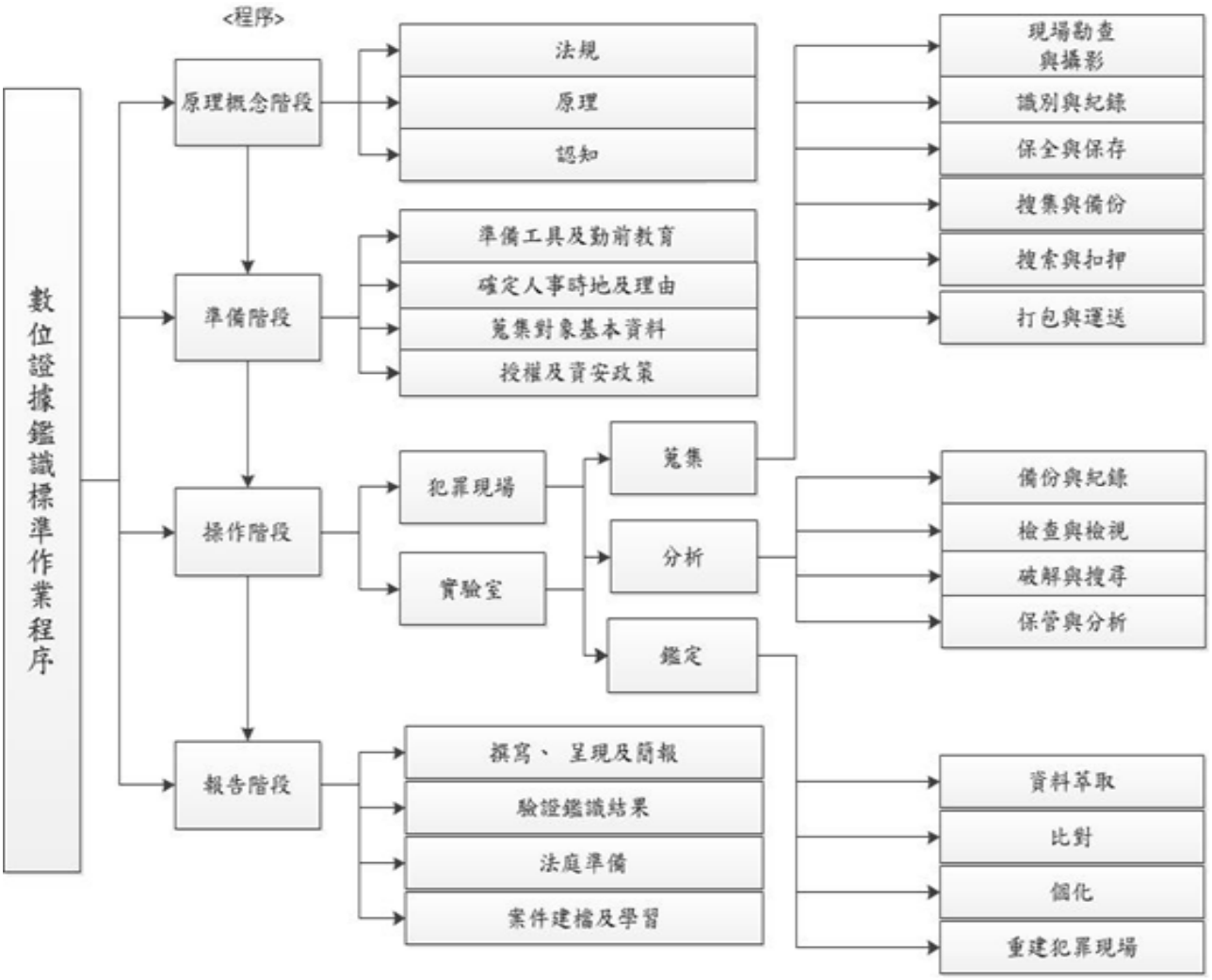
2.2 數位鑑識與行動鑑識

數位鑑識(Digital Forensics)又稱電腦鑑識(Computer Forensics)或資安鑑識(CyberForensics)屬於鑑識科學的分支，用以取得數位資料中存在的數位化法律證據。數位鑑識可以定義為：利用科學驗證的方式調查數位證據，經由數位證據的擷取、分析、還原等過程，還原事件原貌，以利事件調查，並提供法庭訴訟之完整依據。行動鑑識屬於數位鑑識的其中一部份，指所有對行動裝置上的數位資料進行保存、識別、萃取、分析及鑑定的行為。手機中儲存的資料，以電磁紀錄存在，此即所謂的數位證據，手機上的證據，屬於數位證據在行動鑑識的延伸。

2.3 數位證據鑑識標準作業程序（DEFSOP）

國內學者林宜隆教授提出數位證據鑑識標準作業程序(DEFSOP)，其程序包含原理概念、準備、操作及報告四階段，如圖 1 所示[8]。

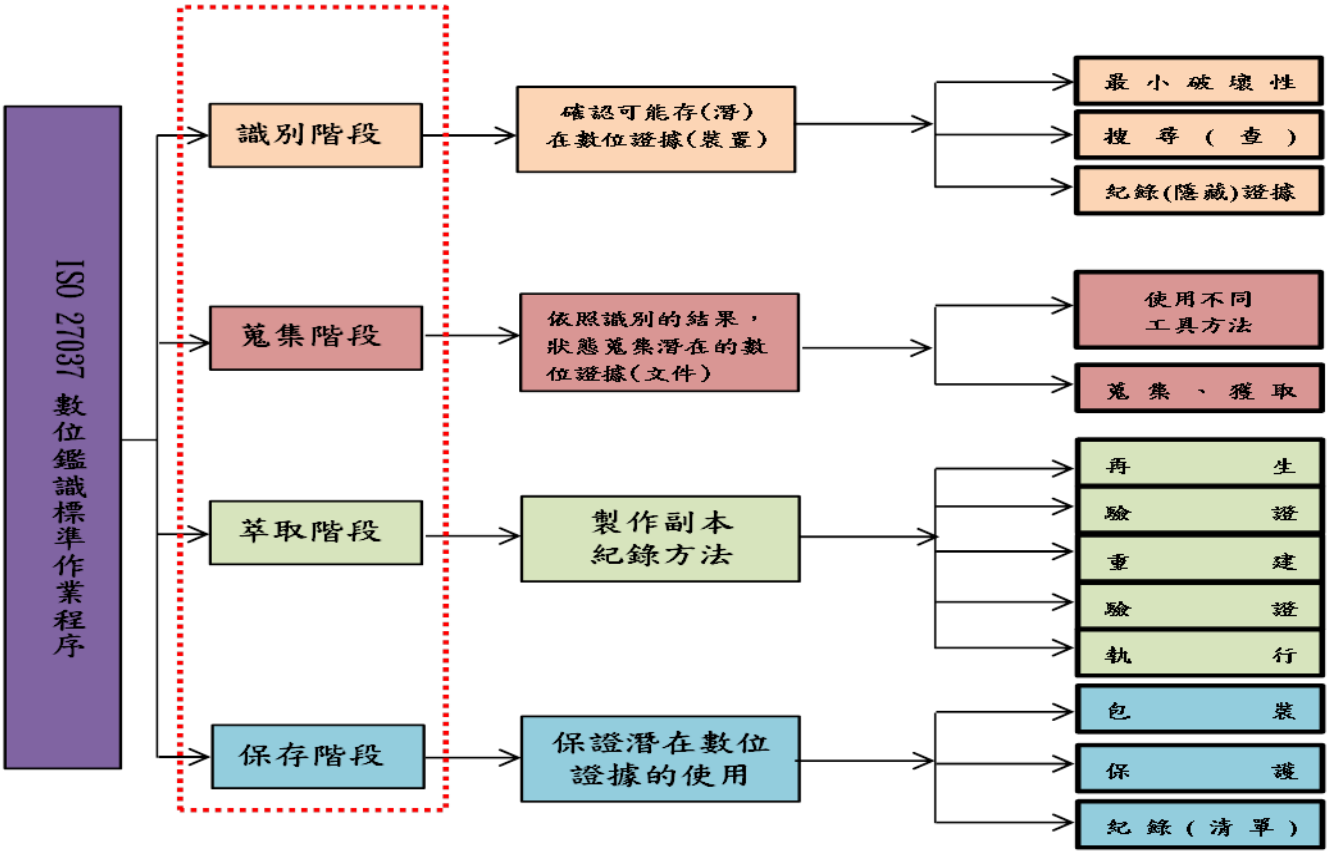
1. 原理概念階段：數位證據的取得要遵循合法與真實的原則。
2. 準備階段：主要是鑑識前的準備工作。
3. 操作階段:
   (1) 蒐集程序：蒐集及備份數位證據，分為識別與記錄、保全與保存、收集與備份、搜索與扣押、打包與運送等五項工作。
   (2) 分析程序：搜尋及分析關鍵資料，在這個程序中可分為備份與紀錄、檢查與檢視、破解與搜尋、保管與分析四項。
   (3) 鑑定程序：擷取、比對及利用數位證據還原犯罪現場，在這個程序中將鑑定分為四個部分，分別為資料萃取、比對、個化、重建犯罪現場。
4. 報告階段：
   (1) 撰寫、呈現及簡報: 撰寫鑑識作業流程，註明使用工具及分類法，報告撰寫需詳實，簡報說明需用易讀圖呈現。
   (2) 驗證鑑識結果:證據檢驗及證據呈現需正確。
   (3) 法庭準備:出庭前人員及物證的準備。
   (4) 案件建檔及學習:案件資料庫建檔及案例教學教育。



圖一: 數位證據鑑識標準作業程序[8]

2.4 ISO 27037:2012 國際標準數位證據處理程序

是國際標準組織(International Organization for Standardization，ISO)針對數位證物識別、收集、獲得與保存所訂定的指南，提供資訊安全事件調查過程中，對事件分析進行數位證據處理時，可依循的標準與指南，所提出的數位證據處理程序分成四個階段，分別為識別階段(Identification)、蒐集階段(Collection)、萃取階段(Acquisition)及保存階段(Preservation)，如圖二所示。



圖二：ISO27037 圖型(參考 ISO 27037：2012 [1]及本研究自行整理)

1. 識別階段(Identification):

   到搜索犯罪現場時必須辨識任何可能含有潛在數位證據的儲存裝置、文件、紙張、電腦、網路設備等等，同時也必須對證據最小程度破壞。

2. 蒐集階段(Collection):

   數位證據處理程序的流程，也許從被刪除的資料之中搜尋，裝置的狀態可能是正在運作或是關閉的。

3. 萃取階段(Acquisition):

   處理人員必須依據不同的情況、損失、時間、文件以判斷採取合適的萃取方式。

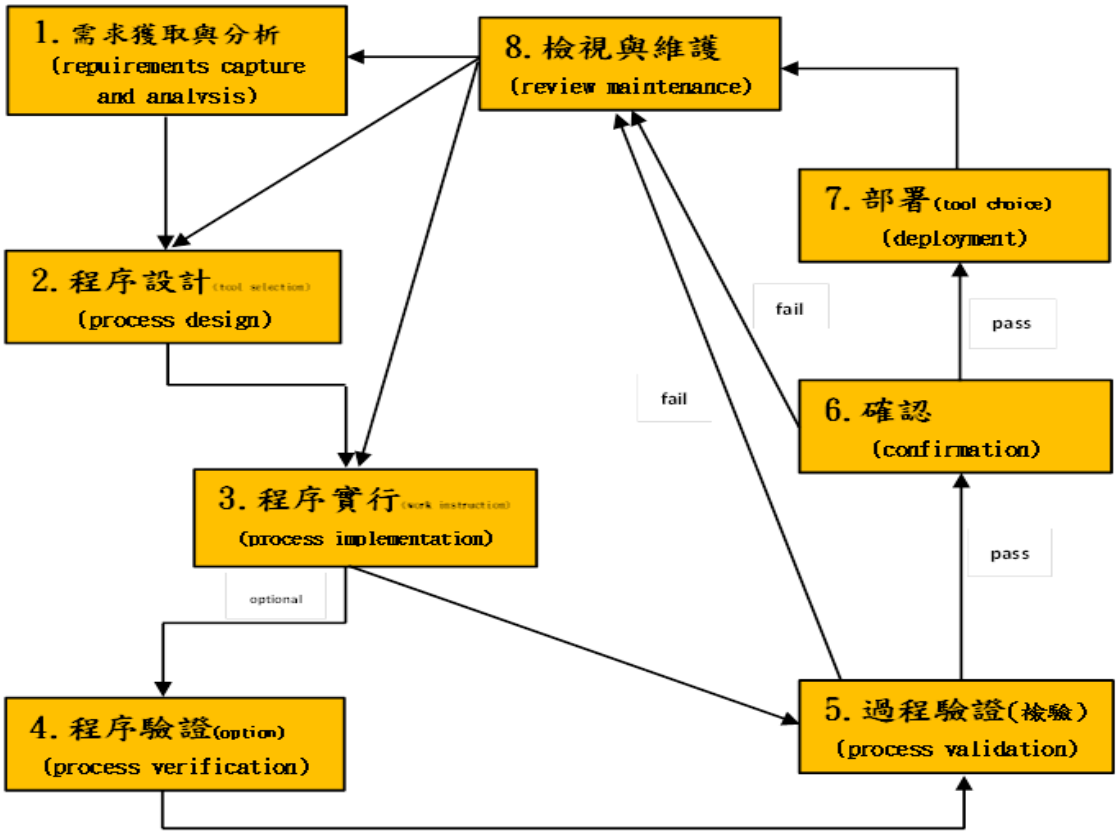
4. 保存階段(Preservation):

保存程序必須保護會被破壞或竄改的潛在的數位證據和數位裝置。保存程序應該從一開始到整個數位證據處理程序。

2.5 ISO27041:2015 資安事件調查與確保適當性之指引

國際標準組織為確保資訊安全調查事件所使用的方法及程序的適當性，並且結果符合預期，其定義需求，說明方法，提供證據，透過第三方輔助確保處理程序。

1. 目的提供以下指引：
   (1) 獲得及分析資訊安全相關事件調查之功能性與非功能性需求。
   (2) 驗證調查流程是適當的。
   (3) 評估驗證等級及產生證據。
   (4) 驗證過程中，外部測試與文件如何整合。
2. 為提供事件調查使用，其開發和部署程序步驟，如圖三。



圖三: ISO27041 (參考 ISO27041：2015 [2]及本研究自行整理)

各階段說明如下：

(1) 需求獲取及分析(Requirements capture and analysis):
可以從已經完成的調查事件中，取得明確定義的需求，這些需求完整而且也可以驗證程序設計的結果。依據需求的目的或特性分類，

以輔助分析，需求類別可分為:

i. 功能性:描述功能或執行任務並將這些考慮因素作為預期的輸入和輸出。例如，處理指定的檔案，它是直接從調查結果產生的。
ii. 效能：定義程度，結果狀態，執行任務的條件限制。
iii. 介面：定義與外部系統交互的解決方案，什麼因素會互相影響(包含人為因素)。
iv. 過程：包含遵守當地的法律和程序或行政要求。
v. 非功能性：定義一個解決方案，包括：品質要求，如可攜性、可維護性和安全性；或人為因素的要求，如安全、效率、健康和福利。

(2) 處理程序設計(Process design):

提供實作方法的詳細資料，選擇合適的工具。設計需清楚定義執行的流程及獲得證據的步驟。建議使用調查員熟悉的工具及程序，可以降低錯誤的發生。

(3) 處理程序實作(Process implementation):

提供正確的工作清單，操作步驟的詳細說明。

(4) 驗證程序或工具符合規範(Process verification):

程序與工具符合其規範保證的等級，選擇性選項，不保證滿足預期用途的需求，如果驗證結果符合需求清單，也可以當作正式證據。使用白箱測試，允許與設計程序內容比對。

(5) 處理程序驗證(Process validation):

i. 驗證工作清單的處理程序完全符合預期的需求,處理程序在設定好的輸入值中產生正確的結果，屬於黑箱測試。
ii. 當程序驗證失敗，回到「檢視和維護(Review and maintenance)」階段再實施驗證。

(6) 確認(Confirmation):

i. 正式的評估處理程序是否符合需求並且提供正式的證據。
ii. 當確認失敗，回到「檢視和維護(Review and maintenance)」階段再實施驗證。

(7) 部署(Deployment):

處理程序被驗證後即可部署，提供調查事件使用。

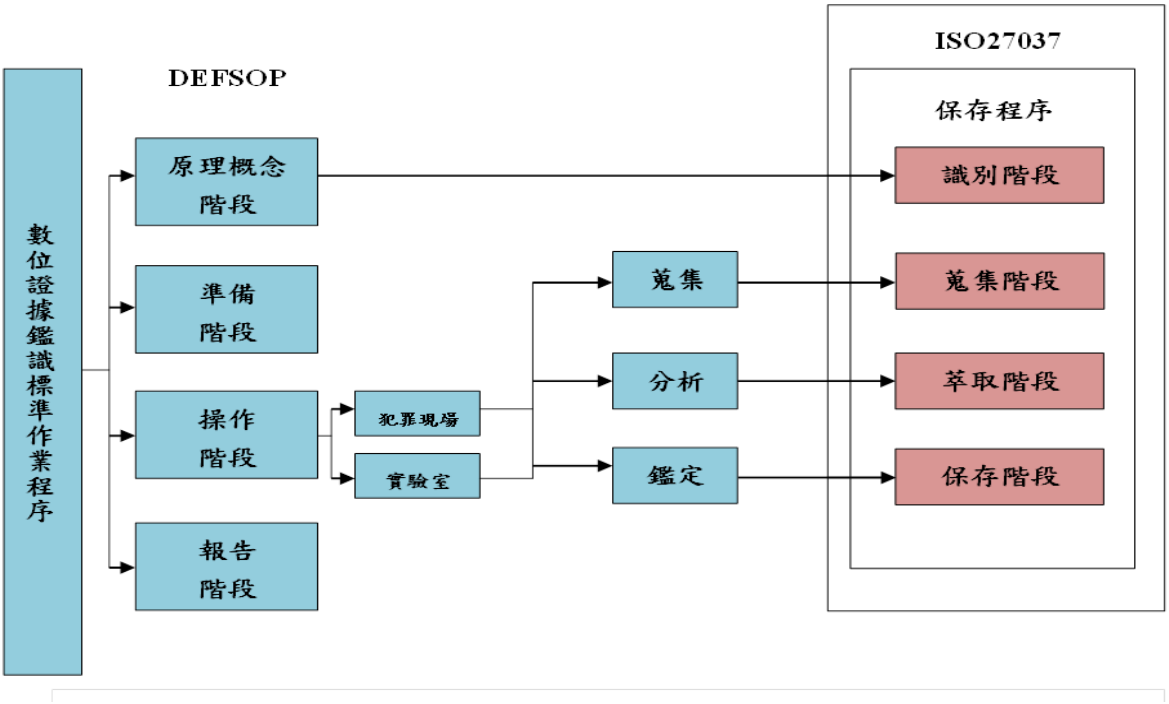
(8) 檢視和維護(Review and maintenance):

i. 檢視，當需求有變更或不符預期，會回到 「需求獲取及分析(Requirements capture and analysis)」、「處理程序設計(Process design)」、「處理程序實作 (Process implementation)」階段。

ii. 維護，確保驗證處理程序是成功的。

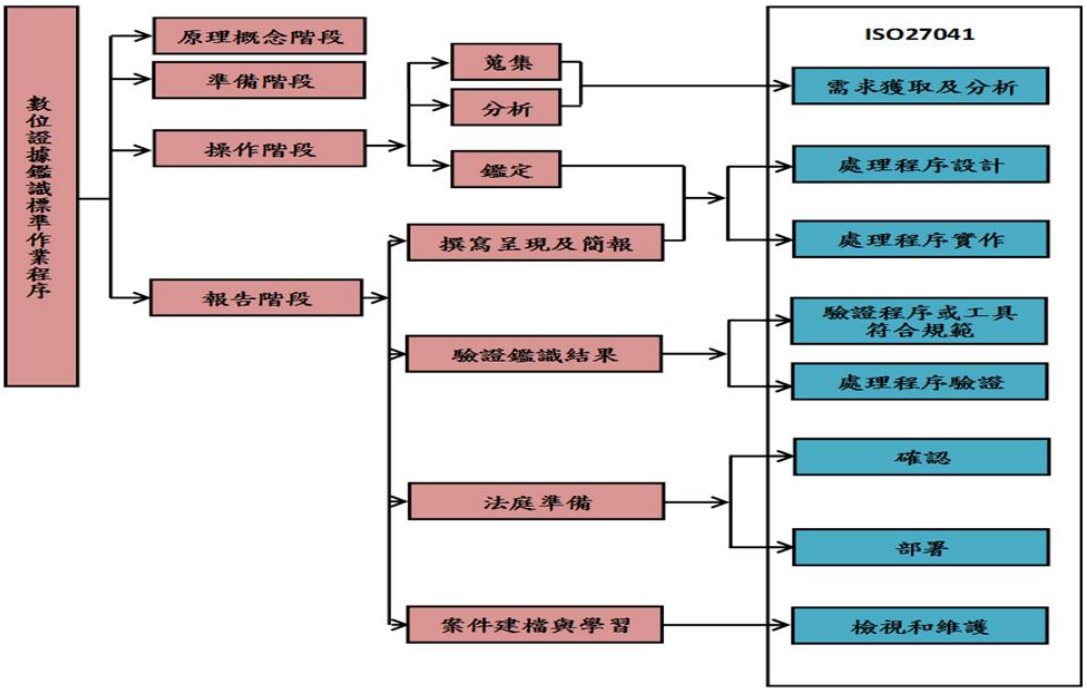
參、行動裝置數位鑑識標準作業程序

1. 數位證據鑑識標準作業程序（DEFSOP）與 ISO 27037:2012 比較，如圖四[9]。



圖四: DEFSOP 與 ISO 27037 對應圖

2. 數位證據鑑識標準作業程序（DEFSOP）與 ISO 27041:2015 比較，如圖五。
3. 比較分析:
   (1) ISO 27037:2012 定義數位證據的識別、蒐集、萃取、保存，主要是定義數位證據處理的過程，與 DEFSOP 比較，主要作業流程在 DEFSOP 的原理概念階段及操作階段。
   (2) ISO 27041:2015 確保資訊安全調查事件的調查方式，與 DEFSOP 比較，主要作業流程在 DEFSOP 的操作階段及報告階段。
   (3) 經過上述比對(如圖四、圖五)，DEFSOP 的四階段程序，完全符合 ISO 27037:2012 及 ISO 27041:2015，並且提供更完整的數位證據鑑識標準作業程序。



圖五: DEFSOP 與 ISO 27041 對應圖

肆、案例驗證分析與實例驗證

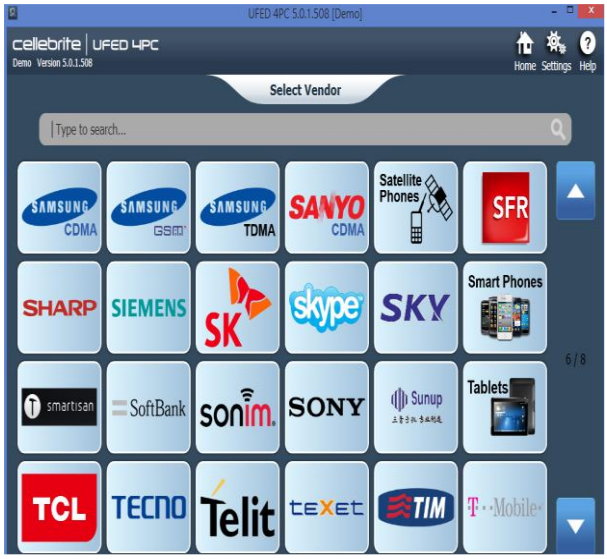
透過框架理論分析，將此案例以結構化方式呈現[5]，參考網路犯罪框架將此案例的重要資訊分析，如表一。

表一: 犯罪分析內容表

犯罪時間	105 年 3 月
犯罪地點	新北市新店區
犯罪事實	利用網路銀行**APP**「假轉帳，真詐騙」案 詹姓男子，自104 年底起持續於各大網路購物、拍賣平台上尋找3C 賣家（販售手機、筆電等），以私訊方式聯絡賣方面交商品後，持網路銀行APP 轉帳畫面、個人身分證件等取信被害人，得手後即將贓物轉賣變現，不法獲利近新臺幣60 萬元。105 年1 月初曾遭警方查獲，交保後仍不知悔改，於3 月起因缺錢花用，重施故技，已連續犯案 15 起。
犯罪損害	民眾財產損失
查獲贓證物	筆記型電腦、手機等
鑑識程序及驗證流程	如表十

依據行動裝置數位證據鑑識標準作業程序(Mobile Device DEFSOP)，執行以下處理程序：

1. 原理概念階段：
   (1) 取得數位證據鑑識許可權。
   (2) 初步研判為網路詐騙案。
2. 準備階段：
   (1) 偵查機關向 ISP 追查 IP 註冊相關資料、鎖定嫌疑犯。
   (2) 透過「資安事件調查系統」，參考過去已完成之調查事件案例，立即召開專案會議，分析案情，選派合適專業人員及相關設備前往犯罪現場。
   (3) 填寫事件調查資料表。
3. 操作階段:
   (1) 蒐集：手機、 SIM 卡、記憶卡、連接線配件等。瀏覽內容及拍照、檔案數位證物保全並備份、搜索與扣押運送至實驗室做細部分析。
   (2) 分析:依據案例資訊,分析鑑識重點,如遭刪除的簡訊 (SMS Messages)、通聯紀錄(Call Log)、多媒體資訊含照片、影像及聲音）(Images、Videos、Audio)、網站瀏覽記錄(Web History)、通訊軟體記錄 (Chats)、GPS 地圖定位 (Devices Locations)、其他置於手機內的文件 (Calendar、Notes、Application Usage)等。
   (3) 鑑定：
      i. 資料萃取:
         a. 環境與使用工具:
            手機裝置：Samsung Note2
            作業系統：Android 4.1.2
            鑑識工具：自動擷取工具 UFED(版本:5.0.1.508)
         b. UFED(UFED 4PC)工具介紹:
            Cellebrite 於 2007 年成立其手機鑑識部門，可透過先進的擷取方法和分析技術， 能夠從手機、智慧手機和 GPS 設備等數千種行動裝置中擷取和分析資料。是美國 FBI 唯一認證之數位鑑識工具，他們的專長就是「數位鑑識」技術。
         c. 執行步驟:
            選定鑑識工具 UFED(UFED 4PC)，選擇手機廠牌及型號，選擇萃取方式為 File System(可還原已刪除的資料)，備份數位證據(圖七-九)。
      ii. 萃取出來的數位證據如 Chats、WebHistory、Images、Device Locations 等，透過 UFED 分析工具(UFED Physical Analyzer 5) 分類分析，如圖十。



圖七: 手機廠牌選擇

圖八: 手機型號選擇

圖九: 萃取方式選擇(Samsung)

iii. 依據本案例，分析鑑識內容：

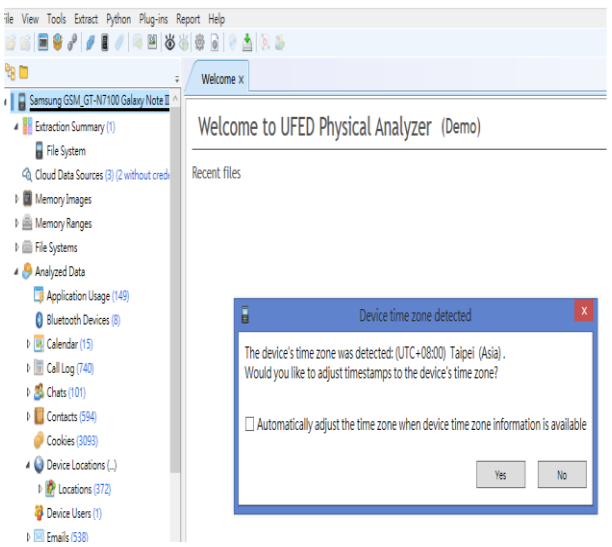
a. 根據上網的紀錄網頁分析，找出瀏覽或訂購的購物網站相關資料，如圖十一。

b. Password 內容分析，找出帳密並登入網頁找出商品購物及付款內容，如圖十二。

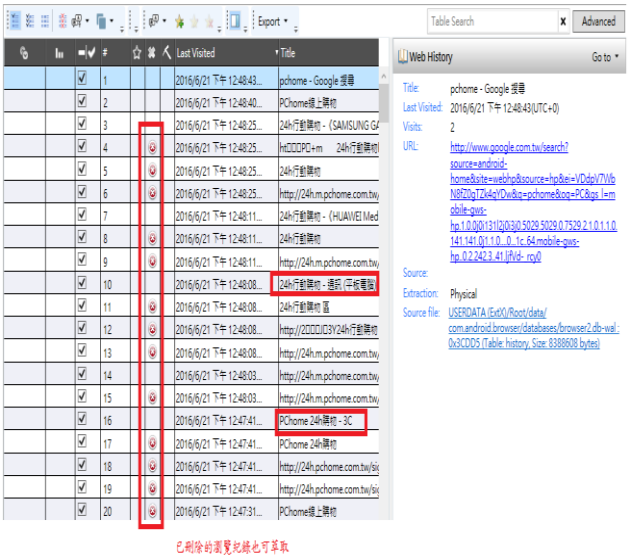
c. 以通訊軟體(chats)聯絡內容分析，找出關於商品購物及付款內容，如圖十三。

d. 依據通聯記錄分析，找出與受害者通話記錄，如圖十四。

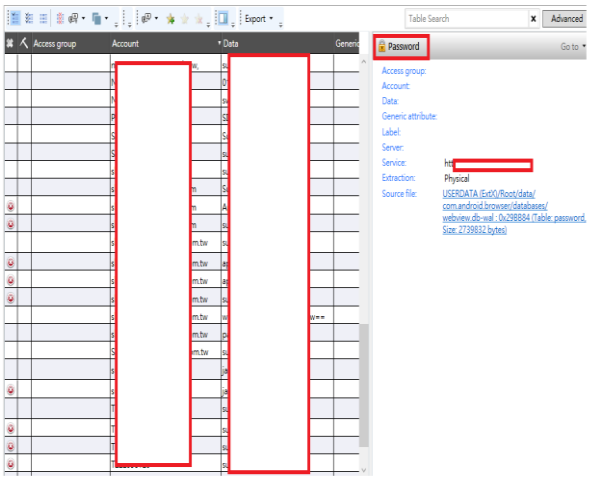
根據上述交叉驗證和關聯分析，找出嫌犯犯罪證據，還原犯罪事實。



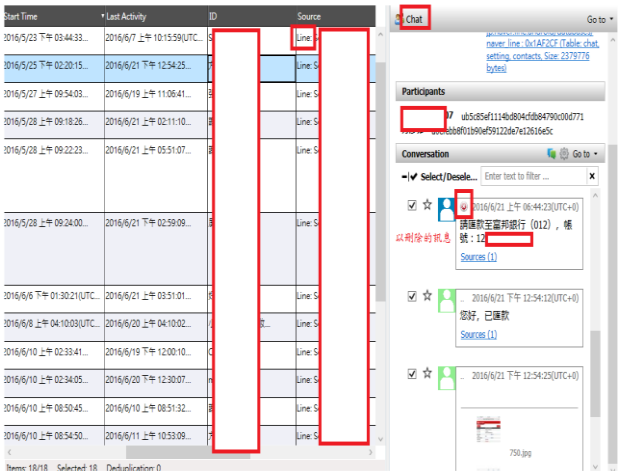
圖十: UFED 分析工具(Samsung)



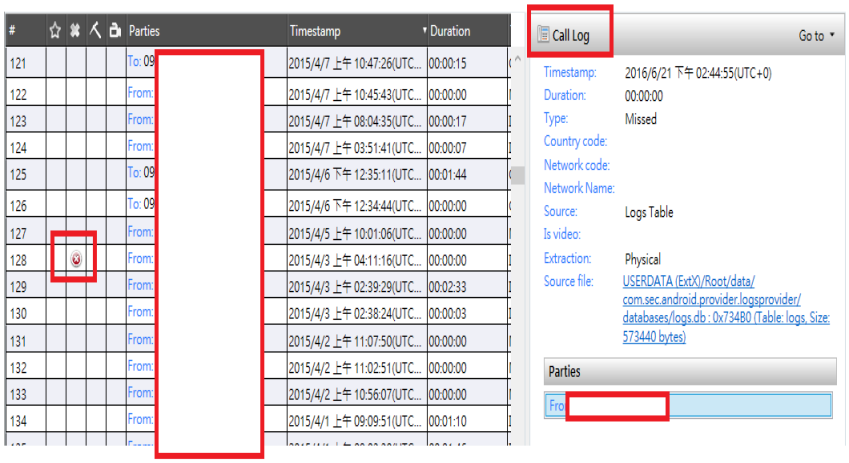
圖十一: Web History 模擬(Samsung)



圖十二: Password 模擬(Samsung)



圖十三: Chat (LINE)模擬(Samsung)



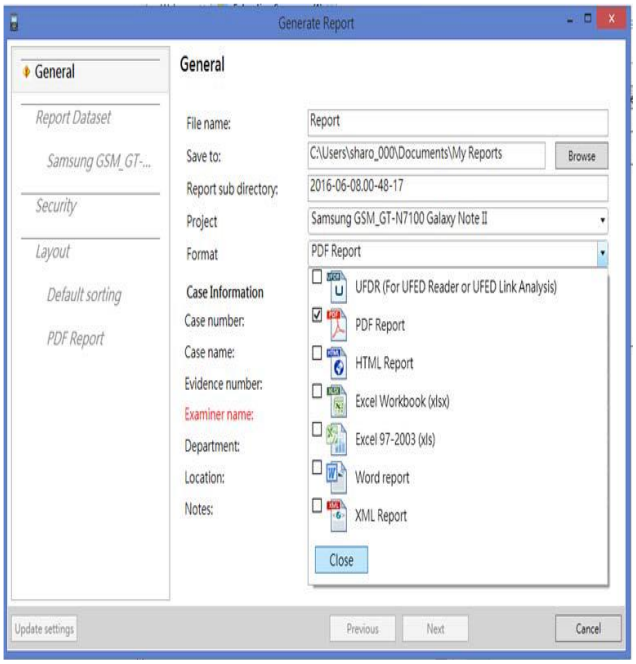
圖十四: Call Log 模擬(Samsung)

4. 報告階段

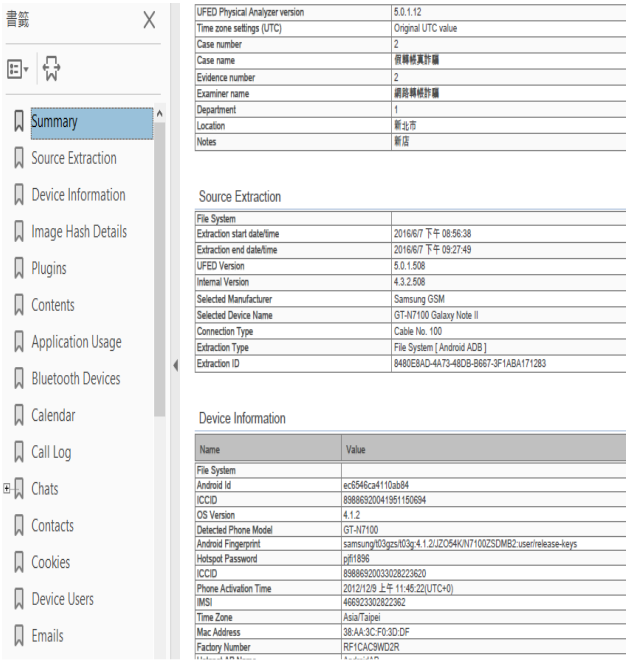
(1) UFED 提供產生報表工具，選擇產生 PDF 檔，其報表資料分類並且內容完整，簡明易懂，如圖十五、圖十六。

(2) 由第三機關或人複驗。

(3) 鑑識經驗及技術分享，透過刑事知識庫建檔學習，「資安事件調查系統」。



圖十五: 產生 UFED 報表(Samsung)



圖十六: UFED 結果報表(Samsung)

伍、結論

數位證據的取證鑑識過程對於證據能力有極大的影響，所以對於數位證據的蒐集、分析、保全與監管，每一環節都應由專業機構與人員執行。在操作階段透過先進 Cellebrite 的 UFED 的擷取方法和分析技術，破解罪犯手機，對行動裝置的物理萃取、解碼、分析和報告，嚴格執行「數位證據保全」之安全控管及驗證機制，以確保各鑑證物不會遭到污染或破壞，以確實達到數位證據之公正性、合法性、完整性與正確性(IACC)。本文以市場上占有率最高 Android 智慧型手機當作實驗，使用鑑識工具 UFED 萃取相關的數位證據，透過交叉分析數位證據及完整結果的呈現，還原犯罪事實，提供事件調查鑑識人員可依循的工具選擇參考。

參考文獻

[1] ISO/IEC 27037 Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence, 2012.

[2] ISO/IEC 27041 Information technology -- Security techniques -- Guidance on assuring suitability and adequacy of incident investigative method, 2015.

[3] "Mobile Forensics Products – Decoding & Review, " http://www.cellebrite.com/Mobile-Forensics/Applications.

[4] 王宗隆，"數位證據分析與鑑識雲端平台 DEFSOP 之研究-以 LINE DESOP 為例"，碩士論文，國立宜蘭大學多媒體網路通訊數位學習碩士在職專班，2015。

[5] 林宜隆，"網際網路與犯罪問題之研究"，2001。

[6] 林宜隆，"網路犯罪:理論與實務"，台北，中央警察大學出版社，2009。

[7] 林宜隆，"司法新聲，第 101 期_第 4 篇"，2012。

[8] 林宜隆、藍添興，"資訊犯罪與安全管理之探討"，中央警察大學，2004。

[9] 林宜隆、李政謙、陳靜玉、張志欶，"數位證據鑑識標準作業程序與 ISO27037 數位證據處理程序之比較分析"，*第十九屆資訊管理暨實務研討會*，2013。

[10] 陳威棋，"談數位鑑識—從國內外實際案例看數位鑑識之重要性"，*財金資訊季刊*，勤業眾信聯合會計師事務，2014 年 7 月。

[11] 藍添興，"數位證據標準作業程序之研究"，碩士論文，中央警察大學，2004 年 6 月。