電腦鑑識之手持行動通訊鑑識程序研究

高大宇
海岸巡防署海洋巡防總局海務組
camel@mail.cpu.edu.tw

吳憲政
中央警察大學資訊管理系
im751203@mail.cpu.edu.tw

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

摘要

對電腦鑑識人員而言，數位鑑識科學領域的處理手機數位證據科技需求已漸受重視。本文剖析技術挑戰議題及數位鑑識工具，審慎因應涉及手機鑑識調查之大量證據資料，有效處理利用鑑識或非鑑識工具處理證據所衍生的難題：遵行可信賴、可解釋、可驗證及可適法等四原則。藉此，本文提出手機鑑識的 PDCA 模型及 MDFA 策略分析，可有效改善處理數位證據的一致性並具實質效益。

關鍵字：手機鑑識，數位證據，非鑑識工具，鑑識程序

1. 前言

電腦網路興起普及，對人們生活產生諾大影響。E 化(Electronic)使企業組織的作業流程電腦化，減少人工作業需求。隨著行動通訊逐漸成型，無線網路的快速發展，M 化(Mobile)趨勢，行動通訊技術讓資訊服務可在任何地點、任何時間，使用各種移動的終端設備與後端 E 化資訊系統同步，即時交換資料。未來，將邁向 U 化(Ubiquitous)標準，無所不在的通訊網路，以「人」為中心提供各種服務，獲取各種資訊。隨著手機普遍使用，各行各業陸續使用手機連絡，便於攜帶，操作容易，功能邁向 M 化標準。然潛在問題相應而生，如犯罪者利用手機通訊，對話紀錄或簡訊透露出犯罪訊息；這些數位紀錄儲存於手機記憶體、SIM 卡記憶體或電話通信業者的相關主機中，如何擷取、採集，保證完整性，是手機鑑識工作的努力方向。手機鑑識目的為從目標手機，擷取及保存手機中有用數位證據，作為有用的法庭證據。透過操作適當的鑑識設備，達預期效果。數位證據的要求包含可信賴、可解釋、可驗證及可適法等四原則[1,2]：

(1)可信賴(Reliable)原則：調查人員採取的任何動作，不應該改變數位裝置或儲存媒體內的資料。若在鑑識過程中改變數位證據，則最後的結果將不被法官或審判團採用。

(2)可解釋(Explainable)原則：任何存取原始資料的人必須具備適當資格，且有能力解釋每一步動作，減少改變證據的可能。

(3)可驗證(Repeatable)原則：一個稽核或程序紀錄、經第三人認可結果，詳細記錄調查步驟並儲存。隨後檢視這些結果，可清楚了解調查步驟，驗證過程是否適當。

(4)可適法(Compliable)原則：負責調查的人已全面負責，確保遵守上述程序與政府法律。採證工作必須合法，鑑識取證工作才能獲認可。

本文比較手機鑑識設備及非鑑識設備的結

果，提出一套標準的鑑識流程，使用相關策略，討論及分析。第 2 節討論手機證據、手機與電腦鑑識的差別與 MDFA 策略的四面向。第 3 節模擬與比較手機鑑識工具及非鑑識工具的使用。第 4 節討論分析。第 5 節為本文之結論。

2. 文獻探討

2.1. 手機證據

行動電話同時使用揮發性手機記憶體及非揮發性手機記憶體和非揮發性 SIM 卡記憶體，作為數位儲存媒介。揮發性手機記憶體僅暫時儲存在使用者的數位資料，但電腦均使用非揮發性硬碟作為儲存媒介，搭配使用 RAM 等暫存記憶體。手機如斷電及內部電池耗盡，則揮發性手機記憶體之使用者數位資料將可能遺失。相反地，電腦非揮發性硬碟，即使電力失去，數位資料仍存硬碟。因 SIM 卡記憶體儲存容量有限，超額的電話簿及簡訊資訊可儲存於手機記憶體，但 SIM 卡特徵可變化、可選擇性，致不同款式呈現局部不同。

2.1.1 SIM 卡記憶體

SIM 卡檔案系統存放於非揮發性記憶體，由階層樹結構組成，包含三種元素：檔案系統的根目錄(MF)、次層的檔案目錄(DF)與基本資料的檔案(EF)。整個檔案系統不同型態的數位證據可從 SIM 卡中回復，有些存於 SIM 卡資訊也可存放手機。SIM 卡包含使用者建立的非標準檔案，內含一組認證金鑰 Ki，讓使用者向網路證明身分，取得使用者服務的，它同時也提供個人資訊的儲存及相關的訊息，儲存在 SIM 卡上的非揮發性檔案資訊有[1, 5]：

- 國際移動用戶識別碼(International Mobile Subscriber Identity; IMSI)
- 個人識別碼 (Personal Identification Number; PIN)
- 電話簿
- SMS 簡訊
- 簡速撥號 (Abbreviated Dialing Number; ADN)
- 收發電話資訊
- 所在地資訊(Location Information;LOCI)

2.1.2 手機記憶體

手機記憶體資訊，主要包含下列幾種：

- 國際移動設備識別碼(International Mobile Equipment Identity; IMEI)：輸入手機”＊＃06＃”取得該值，有 15 位數字，表明製造商，型號類型及國家批准的 GSM 設備。IMEI 最初的 8 位數稱為類型分配碼 (Type Allocation Code; TAC)，標示模組和原產地。其餘部份是特定製造商編碼及最後檢查碼。
- 電子序號(Electronic Serial Number; ESN)：手機製造商在安全芯片記錄的獨特的 32 位識別碼。
- FCC ID：前 3 位字母是公司代碼，接下來的 14 位是產品代碼。美國聯邦通信委員會提供資料庫查詢服務，確定設備製造商和檢索話機本身的訊息，包括照片，用戶手冊，和無線電頻率的測試結果。
- 電話簿
- SMS 簡訊
- 鈴聲

- 圖片
- 影片
- 文字訊息
- 已瀏覽網頁
- 行事曆
- 可執行的應用程式

2.1.3 可移除式裝置

可移除式裝置規格多由製造商自行決定，種類繁多，主要功能為擴充手機的儲存容量，目前最大的記憶體容量可達到 16G，未來仍會繼續發展，甚至提出更快的傳輸規格。常見記憶卡種類包含多媒體記憶卡(Multi-Media Cards; MMC)、安全數位記憶卡(Secure Digital Card; SD Card)、記憶條(Memory Sticks; MS)、TransFlash 卡等等，可儲存的資訊依據每隻手機的不同而有不同的儲存規格及種類[2]。

2.2 手機與電腦鑑識的差別

手機製造商個別客製化的規格不一，可利用紅外線、藍芽等無線通訊方式連接，致手機鑑識設備需搭配多種附屬設備使用。復因手機製造商的更新周期快速，相關鑑識設備軟硬體的更新速度始終落後，輔以手機蓄電量不足、無適當連接設備、手機鑑識困難及難適時保存證據等犯罪現場問題，使得手機鑑識的工具較電腦鑑識複雜、多樣且困難。個人電腦及手機外觀的不同，在於攜帶及運算能力之差異。我們以表一說明手機鑑識與電腦鑑識的差別[3, 5]:

表一：手機鑑識和電腦鑑識的差別

類別	手機	電腦
複雜的連接方式	不同規格的各種有線及無線裝置，如紅外線、藍芽、WiFi 等連接。	類似規格的共通性滑鼠、鍵盤、喇叭及可攜式儲存媒體介面
多變的軟體應用	客製化的作業系統	Windows、Linux、MAC 作業系統
特殊性的硬體變更	客製化、多樣性	較無差異
電池壽命的長短	較短	較長
Hash 值的差異性	關機狀態 Hash 值會隨時間變化而變化，無法比對 Hash 值，故無法證明電腦內資料是否遭修改。	關機狀態 Hash 值不會隨時間變化而變化，可比對 Hash 值，證明電腦內資料無修改。
非揮發的證據保存	須注意電源供應充足，避免揮發性數據遺失。	關機後揮發性數據遺失。

(1)複雜的連接方式

電腦規格較統一，鑑識設備的連接選擇較少，無法連接問題較少；然手機規格多樣性，各型紅外線、藍芽、WiFi 等有線或無線輔助周

邊裝置，需適當中介軟硬體設備與手機連結，鑑識設備更需注意連接方式的可行性。

(2)多變的軟體應用

隨製造商不同，作業系統亦不同，除 Nokia、Motorola 及 SonyEricsson 等手機大廠較統一外，其他地區性手機品牌之作業系統種類更是五花八門。復因手機製造商為本身的商業機密，不會釋出作業系統的原始碼，造成各家產品相關系統各不相同，致鑑識工作及測試，更難達成。電腦的作業系統目前則以 Windows、MAC 及 Linux 為三大類，目前手機作業系統及文件鑑識發展所面臨缺點是「極短的作業系統版本」。如開發手機作業系統的 Symbian 公司，每個作業系統的釋出壽命週期很短，平均不到 1 年就有新的版本釋出，鑑識工作需注意系統版本更新的速度。

(3) 非揮發的證據保存

從鑑識角度觀察，如電源沒持續開啟，部分手機裝置證據可能會遺失(僅剩非揮發性 SIM 卡記憶體內容)，這表示調查人員須確保移動設備有足夠的電源供應，並在有限的時限內採集相關數位證據，確保數位資料的維護與保存。

(4) 特殊性的硬體變更

手機設計考量便利性，與電腦考量應用性不同。手機硬體結構著重機動性、簡單功能及電池壽命的延長性。除手機軟體的作業系統及應用系統多樣化外，不同手機供應商的蓄意增加硬體的差異性、軟體的功能性與客製化的優異性，意味著手機鑑識相關軟硬體的差異性，促使後續鑑識分析工作，份外辛苦。很難有共通的手機鑑識工具提供完善的檢查效果，也因此，如何善用非鑑識工具及證據保存的方法，便顯得更加重要。

2.3 MDFA 策略的四面向

大部分事件的現場所獲事證常受限，事後也未必妥適保存。個別事件數位鑑識的結果分析，不應只考慮證據本身，還需加入其他因素，解讀證據透露出的訊息，本文使用多面向的數位鑑識分析(Multi-Faceted Digital Forensics Analysis; MDFA)，提供一個全面、完整性的鑑識分析策略，考慮可能出現的犯罪跡證。MDFA 策略考慮證據、場景、受害者及嫌疑人等四個面向，期運用此分析策略，有效解析事件內涵，如圖一之 MDFA 模型的四個面向[4]。

圖一：MDFA 模型的四個面向

(1) 證據(Evidence)：注意證據的保存方式，避免在運送或採集過程中遭受汙染或毀損。

(2) 場景(Scene)：第一犯罪現場往往存在破案的關鍵證據。

(3) 受害者(Victim)：受害者受侵害所做的陳述是犯罪紀錄的重點，可由受侵害的行為，分析犯罪者的犯罪動機、行為，從中

過濾可疑嫌疑人。

(4) 嫌疑人(Suspect)：對於可能參與犯罪的嫌疑人，執行個別訊問調查，交叉比對分析訊問結果，供法庭參考。

3. 鑑識模擬

本節描述使用手機鑑識工具及非鑑識工具得到的鑑識結果，必須注意在鑑識過程中，避免修改數位證據的內容，確保其完整性。3.1 節描述使用 CellBrite 及 CellDEK 手機鑑識工具的過程，3.2 節操作手機製造商提供的 PC Suite 軟體，從備份資料檢視手機內容，3.3 節列出報告得到的結果。

3.1 手機鑑識工具的使用

目標手機為 Sony Ericsson K800i，分別使用 CellBrite 及 CellDEK 手機鑑識工具，針對記憶體進行鑑識分析工作：

(1)CellBrite 對手機本身及外接記憶體做鑑識。

(2)CellBrite 對手機中 SIM 卡記憶體做鑑識。

(3)CellDEK 對手機中 SIM 卡記憶體做鑑識。

實作過程，概述如下：

(1) 選擇適合的連接電纜線，連接手機與 CellBrite 鑑識工具，於手機中選擇手機模式連接，並插入 USB 隨身碟，儲存映象備份資料。

(2) 在 CellBrite 中勾選全部可備份內容，進行鑑識備份，避免任何有用的資料遺失。

(3) 資料備份完成，CellBrite 產生報告。

(4) 經由檢視報告的結果，得到手機儲存資訊，詳細項目整理於表格中，並產生的 MD5 Hash 函數，避免數位資料遭修改。

(5) 另使用 CellDEK 鑑識工具，對目標手機進行鑑識分析，但因機型不支援（大部分的手機鑑識工具僅支援特定軟硬體），只作 SIM 卡記憶體部分，復因 CellDEK 內建 Windows XP 作業系統視窗介面，可即時檢視鑑識結果。

3.2 非鑑識工具的使用

相對於鑑識工具，非鑑識工具的使用主要是讓使用者便於操作，利用電腦對手機內容進行同步操作，是一個雙向的資訊流動，可對其內容進行修改，以下流程，我們使用 Sony Ericsson PC Suite 5.0 軟體，透過手機內附的連接電纜，選擇”備份”的功能，對整個手機內容進行資料備份，保存備份當時的狀態。手機資料遭刪除時，可使用”還原”功能，還原至備份當時的狀態。程序如下：

(1)安裝 Sony Ericsson PC Suite 5.0 後，啟動軟體，並選擇手機的連接方式(使用手機模式，有線電纜連接)。

(2)選擇備份模式，將手機裡的所有資訊，備份至電腦，產生一個副檔名”.dbk”檔案。

(3)移除手機後，使用 PC Suite 軟體，開啟該”.dbk”檔，檢視備份內容。

3.3 鑑識結果

表二：各種工具所得手機資訊表

工具名稱	CellBrite	CellBrite	CellDEK	PC Suite
工具類別	手機鑑識工具	手機鑑識工具	手機鑑識工具	非鑑識工具
鑑識標的	手機	SIM	SIM	手機
建檔時間	✓	✓	✓	✓
IMSI	✓	✓	✓	
IMEI	✓			
MCC	✓	✓	✓	
ICCID	✓	✓	✓	
PIN				
手機資訊	✓	✓	✓	✓
電話簿	✓	✓	✓	✓
已撥電話	✓	✓	✓	
未接來電	✓			
SMS 簡訊	✓	✓	✓	
日期	✓	✓	✓	✓
便條	✓			✓
行事曆	✓			✓
已瀏覽網頁	✓			✓
圖片	✓			✓
鈴聲	✓			✓
音樂	✓			✓
影片	✓			✓
主題	✓			✓
可執行的應用程式	✓			✓
檢視已刪除訊息	✓	✓		
MD5 Hash	✓	✓	✓	

表二整理各種工具所得手機資訊表。鑑識及非鑑識工具主要差別是鑑識工具可產生 Hash 函數，避免鑑識報告遭到修改，得到資料備份內容是相同的。過程中，本文發現部分鑑識工具適用範圍有限、還原已刪除的資訊檔案的功能亦待加強。有時依然需要手機製造商提供的軟體替代，解決鑑識工具無法適用問題，但是，必須要有一套標準的作業程序，確保取證過程中不當改變手機內容。本文結合 6W1H 問題模式及 P-D-C-A 流程[4],提出手機鑑識的標準流程。

4. 討論及分析

本節使用手機鑑識工具及非鑑識工具，對同一台手機內容進行資料備份，為避免人為操作修改內容，先使用 CellBrite 及 CellDEK 對其進行擷取，接著再由電腦操作 Sony Ericsson PC Suite 5.0 軟體，對手機內容做備份。

4.1 使用非鑑識軟體可能遭遇的問題

鑑識工具(Forensic Tool)和非鑑識工具(Non-Forensic Tools)常用相同的通訊連接與手機設備連接，然而，非鑑識工具允許雙向的資訊流動，增強或客製化自己的手機(例如，添加自己的電話鈴聲，桌布，主題等)，而鑑識工具必須在不改變設備內容下，從設備中獲取資料數位資料並產生完整的 Hash 函數值。廠商提供的軟體工具，商業軟體，甚至是駭客工具等等，都屬於非鑑識軟體的類型，因此，在使用非鑑識軟體時，可能遭遇的問題有：

(1)可信賴(Reliable)原則：調查人員採取的任何動作，不應該改變數位裝置或儲存媒體內的資料。當使用非鑑識工具時，會被質疑的問題就是證據是否可被信賴、可使用。

(2)使用的價值：當鑑識工具的存在時，使用非鑑識工具不易被接受。為什麼要使用非鑑識工具來做鑑識分析？有哪些優點是鑑識工具無法取代的？

(3)法律的保障：沒有法律的保障，使用非鑑識工具分析結果，不容易被法官或審判團採用。因此，是否有相關法律條文的支持，也是使用非鑑識工具必須面對的問題。然台灣的訴訟法律，對此部分尚無明確規定。

4.2 非鑑識工具的優點

本文中使用非鑑識工具，探討手機鑑識流程的建立，和一般手機鑑識工具比較起來，手機的非鑑識工具，有以下優點：

(1)價格便宜：一套完善的手機鑑識工具，需要花費好幾百萬的經費建置，而非鑑識工具往

往是免費的，手機製造商所提供的軟體、網路上免費的工具軟體，都可用來檢視手機中的內容。

(2)取得容易：常無法直接將鑑識設備帶到現場進行鑑識，若使用非鑑識工具，取得管道較為容易。犯罪現場發現的手機軟硬體連接設備，可直接將手機內容進行備份，避免嫌疑人在第一時間將資料刪除。

(3)適用方便：手機更新的速率週期很短，鑑識設備需要經常更新軟硬體內容，以適用新型手機。手機設備接口多樣，若採用非鑑識工具，適用較為方便，減少因設備不支援造成鑑識人員的困擾。

4.3 手機鑑識的 PDCA 程序模型

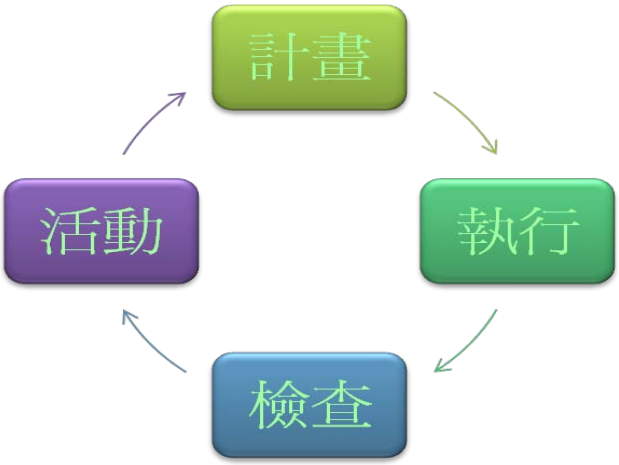
處理數位鑑識工作，加入「戴明循環」(Deming Cycle)的 P-D-C-A 流程，由計畫(Plan)、執行(Do)、檢查(Check)及行動(Action)四項步驟，尋求一連串追求改善的行動，以建立一套鑑識工作的標準作業流程，透過管理循環，檢視問題及結果，達成呈現事件原由的預期目標[4]。如圖二 P-D-C-A 模型所示的不斷循環、檢視問題並重新實作，改善運作的方式，能研析四階段間交互影響的行為研究，據以設計一套較佳的鑑識流程。

(1) 計畫：計畫階段是鑑識目標的建立，必須注意需要採行的策略，選擇一些適當的控制，避免不當操作使證據無效。

(2) 執行：在執行階段，實施操作過程及控制。

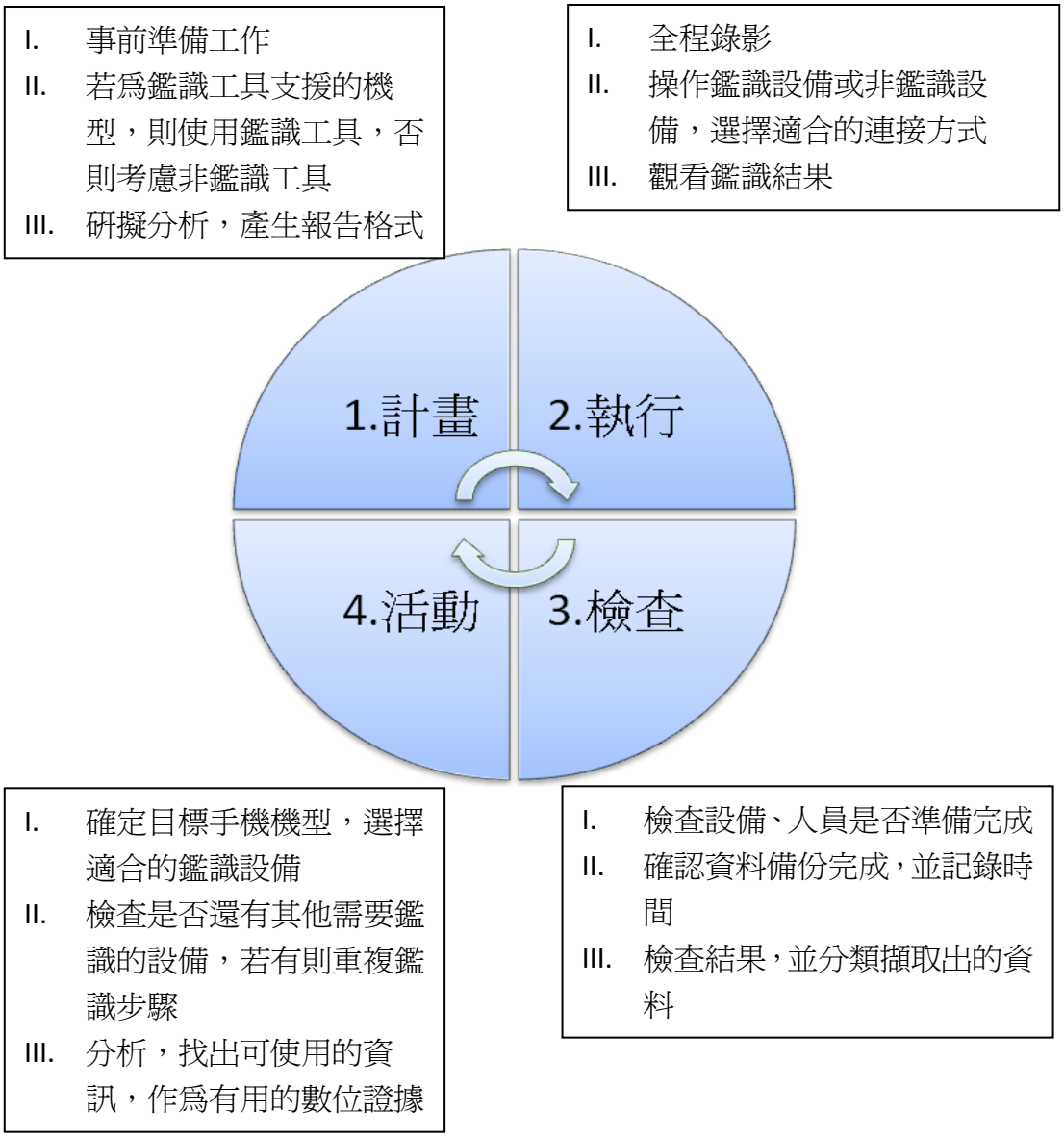
(3) 檢查：檢查階段審視實施的效能及效果，及評估鑑識結果的有效性。

(4) 行動：履行行動階段時，改變需要的過程，以符合鑑識流程的標準。



圖二：PDCA 模型

使用非鑑識工具容易因為違背「可信賴」原則導致鑑識結果未具證據資格。為確保非鑑識工具的檢查結果，本文提出手機鑑識的 PDCA 程序模型（如圖三之手機鑑識的 PDCA 程序模型）及 MDFA 策略分析（如表三之手機鑑識的 MDFA 策略分析），期降低非鑑識工具被質疑「可信賴」後，喪失證據資格，鑑識過程應由全程錄影（可驗證-重複檢視原處理程序是否允當），解釋動作（可解釋-採取必要的檢視程序，可信賴-非鑑識工具存取過程未修改所獲資訊），委由法院認可之政府機關或獲授權人員進行檢查（可適法-確保遵守鑑識程序與政府法律），提升法官或審判團接受度，：



圖三：手機鑑識的 PDCA 程序模型

以 PDCA 程序操作手機的鑑識過程，必須全程錄影，透明化流程，避免鑑識過程遭到不當的修改，相關人員設備的準備，在操作過程中逐一檢視下一步應該進行的步驟，產出的鑑識結果應妥善保存，給鑑識分析人員做合理的分析，提供法庭上有用的證據。

4.4 手機鑑識的 MDFA 鑑識分析

數位鑑識過程須注意多個面向，避免證物

遭汙染及不當的操作。本文使用 6W1H 問題，檢視數位鑑識的調查分析工作，配合 MDFA 策略，製作一份完善的鑑識結果分析。探討下列問題，期還原事件的真相：

- Who?

  誰來做？參與的人員有哪些？

- What?

  做什麼？必須要做什麼才能達到預期的目標？

- Which?

  哪一個？選擇哪一個方向做為執行的策略？

- Where?

  在哪裡？犯罪現場在哪裡？證據可能會在哪裡出現？

- When?

  在何時？犯罪發生的時間及證據被發現的時間，是否可由時間檢測數位證據有無更改？

- Why？

  為什麼？犯罪者為什麼要做這個行為？數位證據為什麼會出現在這裡，是否有什麼犯罪關聯？

- How?

  怎麼樣？如何來完成整個數位證據的擷取、採集，並避免數位證據不會遭受汙染？

除證據的採集保存外，面對犯罪，須考慮場景、受害者、嫌疑人等其他三個因素，使用 6W1H 問題進行分析，可對案件做完整的描述，從中檢討可改進的事項。表三提出手機鑑識的 MDFA 策略分析，檢視整個案件概況，使檢警人員檢視鑑識報告時，能了解數位證據透露出訊息，期順利逮捕嫌疑人歸案。

表三：手機鑑識的 MDFA 策略分析

面向	6W1H 問題	分析
證據	誰來採集?	數位證據的採集應由受過訓練的專業人員擔任，時間與地點是記錄重點，依據不同的數位證據，應考慮不同的採集方式。
	做什麼工作?	
	哪一個東西需要採證?	
	證據會出現的地方?	
	何時做採證動作?	
	證據為什麼會出現在這地方?	
	如何完成採證工作?	
場景	誰在事發現場?	案發現場應妥適保存，現場疑點應再次確認。可詢問案發當時在場的人員，回復案發現場當時的情形，有利於案情分析。
	現場有何疑點?	
	在哪一種情況下發生?	
	現場在哪裡?	
	事件發生的時間?	
	為什麼為在這場景發生?	
	犯罪如何在這場景下完成?	
受害者	受害者是誰?	依據受害者的描述，確認損失情形及犯罪者的關聯。
	他做了什麼?	
	受了哪一種傷害或損失?	

	在哪裡受害?	
	何時發生?	
	為什麼發生?和犯罪者有關聯嗎?	
	受害的經過?	
嫌疑人	可能的嫌疑人?	訊問嫌疑人的犯罪時間、動機及實施方式。
	嫌疑人可能做了什麼?	
	嫌疑人犯了何種罪?	
	可能的犯罪地點?	
	犯罪時間?	
	犯罪動機?	
	執行方式?	

5. 結論

手機鑑識程序須克服可信賴、可解釋、可驗證及可適法等難題。本文使用非鑑識工具，減少因專業鑑識設備不支援產生的執行困難，並透過 PDCA 模型程序，全程錄影，降低未符可信賴性之質疑結果，讓採證結果得做為法庭證據。進一步地，本文利用 MDFA 策略分析，由不同面向分析證據的證明力，使得手機鑑識研究亦可有完善的發展，因應日益多變的手機犯罪行為。

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] Jansen W. and Ayers, R., “Guidelines on Cell Phone Forensics,” National Institute of Standards and Technology, 2007.

[2] Ayers, R. et al., “Cell Phone Forensic Tools: An Overview and Analysis,” National Institute of Standards and Technology Interagency Report, 2005.

[3] AlZarouni, M., “Mobile Handset Forensic Evidence: a challenge for Law Enforcement,” School of Computer and Information Science Edith Cowan University, 2006.

[4] Kao, D. Y., The Retest of the Reintegrative Shaming Theory and Its Implications on Taiwanese Juvenile Hackers, Ph. D. Dissertation, Central Police University, Taiwan, January 2009.

[5] Wolleschensky, L., “Cell Phone Forensics,” IT-Sicherheit Seminar, 2007.