數位鑑識操作作業程序之原理及規範之探討

黃志龍　　陳建勳　　林宜隆

刑事警察局資訊室　中央警察大學資訊管理系

cyberlong@email.cib.gov.tw　im933095@mail.cpu.edu.tw

摘要

電腦與網路成爲犯罪場所、工具及標的等各類犯罪活動已是社會中的常態，如何打擊、防制及有效控制這類的資通犯罪，成爲司法界亟待解決的一大難題。且數位資料是易消滅、易修改及不易個化等特性，加上蒐集及保存數位證據時，必須顧及不影響網路正常運作又要完整性，數位鑑識的認知的不足及挑戰，例如網路中同一段時間內有多個位置發生，證據可能在不同地方或設備發現，網路連接的改變，及從連接區域網路到所謂網格(Grid)網路等等的問題，一一都在挑戰數位鑑識（Digital Forensics）的困難性。

成立「數位鑑識實驗室」是有效解決上述問題之對策之一，其中重要工作就是數位鑑識操作作業程序之原理及規範，【3】【4】才能在偵查面有效打擊及防制資通犯罪問題，故希望藉由本研究有關數位鑑識操作作業程序之原理及規範的研究，分別以蒐集、分析、鑑定及報告等四個步驟作業程序之原理及規範，來探討操作程序、重點工作及規範事項，使政府、專家學者及民間業者對此一議題之重視及參考。

關鍵詞：資通犯罪、數位鑑識。

1. 前言

電腦與網路成爲犯罪場所、工具及標的等各類犯罪活動層出不窮的發生，如何打擊和防制資通犯罪，成爲司法界亟待解決的一大難題。加上數位資料是易消滅、易修改及不易個化等特性，蒐集及保存數位證據時，必須顧及不影響網路正常運作，網路中同一段時間內有多個位置發生，證據可能在不同地方或設備發現，網路連接的改變，及從連接區域網路到所謂網格(Grid)網路等等的問題，一一都在挑戰數位鑑識（Digital Forensics）的困難性。

2. 文獻理論探討

2.1 國際知名鑑識專家李昌鈺博士所探討之刑案現場鑑識蒐證方法，研擬一套數位證據之科學的鑑識蒐證程序及注意事項，詳述如下：【1】【2】

一、數位鑑識程序

（一）辨識：辨識數位證據有二個處理方式，第一，辨識有數位資訊的硬體如個人電腦、儲存媒體等硬體設備；第二，必須分辨那些數位資訊才是犯罪行為所運用或犯罪結果產生，所以在犯罪現場以下列方式辨識數位資料：

（二）保存、採集與記錄：

1. 保存：數位證據必須保持原始狀態且不能遭受損壞，例如保存電腦硬體設備必須給予適當的溫度與溼度保護，且在運送過程中小心輕放，至於軟體或電腦檔案則必須複製備份存放，以應不時之需。
2. 採集：採集數位證據有兩種方式：完整複製，或針對需要的資訊或檔案複製，但兩種方式皆必須檢查複製是否成功及在其他電腦是否可讀取。其中完整複製方式，必須採用一個位元對一個位元的複製（bit stream）方法，將所有硬碟資料或未使用之空間複製，而未使用空間硬碟的複製，是為了日後將被刪除的重要資料救回。
3. 記錄：記錄數位證據的原始狀態，或物證的位置，甚至可利用攝影機獲照相機拍照記錄犯罪現場，以利日後犯罪現場重建，在數位證據蒐證時，必須記錄真實時間與電腦顯示之時間、由誰來複製資料或檔案、作業系統名稱、利用什麼軟體工具或指令複製檔案，檔案有什麼重要訊息等皆必須詳細記錄。

（三）分類、比較與個化：

1. 分類：分類是將數位證據歸類於一般項目或是某一數位特質樣本的方法。例如圖片檔可以分類為 JPG、GIF、TIFF 等格式，或是同一個帳號的電子郵件檔可以分成同一類，如經過分析後，有大量的數位資料指向某一個人，則此人與該案件有很大的關聯。
2. 比較：比較方法是檢驗數位證據的一個重要方法，除可以比較出數位證據分類的特質外，還可以從數位證據的樣本中比較出唯一性（個化），如某一人習慣運用特定的電子郵件格式寄送郵件，此時可利用電子郵件的格式分類，比較出某一人的習性，此為達到個化前的一個重要方法。
3. 個化：個化的數位證據就如同指紋或血跡的 DNA 等可以辨識個體，就是在犯罪現場可以證明此嫌疑者犯罪的直接證據，例如在網際網路的網址（IP address）或網路卡網址（MAC address）是一台上網電腦個化的數位資料，因網際網路通訊僅允許一個網址與網路卡網址存在。運用下列幾種方法來達到數位證據分類、比較與個化分述如下：

（四）現場重建

1. 刑案現場重建分二個方面一方面將被毀損或刪除的數位證據重建，另一方面重建刑案現場。前者，必須知道數位證據的型態、電腦之等級、執行的作業系統及電腦軟、硬體的設定，如此才可將數位證據重建，其中最重要的是如何利用

特殊的軟體工具復原被刪除或毀損的檔案；至於後者，除了實體物證外，必須利用修復的數位資料重建犯罪行為，以釐清犯罪的手法與動機，故現場重建最終的目的在於利用假設推論的原理，以瞭解犯罪案件發生的原因、什麼時候犯罪、犯罪手法如何、犯罪的地方、何人犯罪等。

二、犯罪現場注意事項

（一）電腦系統的搜索與扣押之注意事項

1. 透過偵查、監視或情報資料研判電腦系統的種類(Windows 系統、Li*nux 系統*、Unix 系統、蘋果電腦系統、DOS 系統等)，是否為單機型系統或連接網路系統，如果可能應確定電腦位置是否在需要搜索票的保管場所（如住家）或不一定需要搜索票的地點（私人公司的職員位置）。
2. 檢查是否有無線網路系統裝置。
3. 若需要扣押，則需要確定是否為搜索票所列範圍。
4. 管制現場，對電腦與電源附近的人員進行清場疏導，若可能應將可能的被告帶離電腦，詢問有關保護裝置、密碼程式或電腦系統或個人檔案需要的任何特殊程式。
5. 檢查在現場有人控制的紅外線遙控或音控起動裝置。
6. 不要讓未經核准或未受過訓練的人員碰電腦或其週邊設備(FBI 認為只有刑事電腦鑑定專家才能碰電腦)。
7. 攝影：
   （1） 電腦擺放的房間。
   （2） 螢幕上的影像。
   （3） 電腦、週邊設備、連接線、可攜式裝置等數位設備。
   （4） DIP 的開關設定
   （5） 電腦週邊區域、紙張、手冊、進行入密碼、個人密碼等。
8. 如果電腦是開著的，拔掉插座；如果電腦是開著的且似乎在執行自我毀滅程式，應立即拔掉插座，而非觸碰電腦上的電源開關；若有不斷電系統（UPS），應拔掉電腦後面的電源線。
9. 尋找現場有無會破壞電子產品的大磁鐵。
10. 在磁碟機槽插入扣押磁片或空白磁片，並貼上證物膠帶封好。
11. 若電腦有連上數據機線，則應拔掉牆壁端的連線，測電話是否可通，記錄在搜索時電話線是否在使用。
12. 打開蓋子對內部組件及設定拍照，拔掉所有電源連線。
13. 扣押與記錄：
   （1） 電腦與週邊設備。
   （2） 軟、硬體手冊。
   （3） 與電腦或週邊設備相關的筆記或記錄簿。
   （4） 所有的資料儲存媒介（如磁碟片、光碟片、ZIP 磁片、隨身碟等）。
14. 標示所有週邊設備的連接線，貼上或標示所有未使用的插槽 或連接埠，在拆開電腦系統連線前，先照相顯示其連接情形。
15. 以電腦扣押物專用的證物清單目錄表及專用袋，詳列所有扣押物，注意證物監管鏈的完整。
16. 確保所有組件與資料儲存媒介在運送或儲存在證物室時，不受雙向無線電的干擾。
17. 可以在鍵盤或特定開關採指紋，以協助瞭解是誰曾使用過這部電腦。

2.2 常見的潛在的證據之探討

人們所使用的數位設備都可從中找到數位證據。本節是針對通常在犯罪現場所接觸到的各種數位設備，提供一般的偵查作為。許多數位設備須供應電源才能運作，例如電池或AC電源。如果拔掉電源或電池沒電就會造成資料遺失，參考美國司法部所訂定「犯罪現場電子證據—第一時間反應員警的指引」資料探討如下。【6】【7】

一、電腦系統（Computer Systems）

（一）名稱說明：電腦系統包括主機（中央處理單元）、資料儲存裝置、螢幕、鍵盤和滑鼠。它可以是一台獨立式的電腦或是連上網路的電腦。電腦系統有很多種類型，例如筆記型電腦、桌上型電腦、伺服器電腦、大型電腦、甚至超級電腦。其它的電腦元件有數據機、印表機、掃描器、轉接埠和外接資料儲存裝置，例如一台桌上型電腦包括有外殼、主機板、中央處理單元、資料儲存裝置、輸出入單元、鍵盤和滑鼠。

（二）主要功能：計算和儲存資訊，包括文書處理、程式設計、計算、通訊和繪圖等。

（三）潛在數位證據：一般從儲存在硬碟、儲存裝置的檔案都可找到證據。舉例說明如下：

1. 使用者自建檔案（User-Created Files）

使用者自建檔案可能含有很多犯罪證據，例如通訊錄、資料庫檔案、電子郵件或信件都可能和犯罪有關聯，另外，從試算表也可能找到毒品交易清單。

（1） 通訊錄。
（2） E-mail 檔案。
（3） 網路日誌／我的最愛。
（4） 聲音檔。
（5） 影像／圖片檔。
（6） 日曆/行事曆。

（7） 資料庫檔案。
（8） 試算表檔。
（9） 文件或文字檔。

2.使用者保護檔案（User-Protected Files）

使用者可能會以各種型式隱藏證據，例如將資料加密或設密碼保護，也可能將檔案隱藏在硬碟或其它檔案內。

（1） 壓縮檔。
（2） 故意誤名檔案。
（3） 加密檔。
（4） 密碼保護檔案。
（5） 隱藏檔。
（6） 隱匿法（Steganography）之資訊隱藏檔。

從電腦系統檔案或其它資料區亦可發現證據，因為使用者並不會察覺到某些資料會寫到這些區域，例如通常從密碼檔、網路活動日誌和暫時備份檔都可取得證據。

3.電腦系統檔案（Computer-Created Files）

（1） 系統檔。
（2） 日誌檔。
（3） 暫存檔。
（4） 備份檔。
（5） 檔案結構檔。
（6） cookies。
（7） 交換檔。
（8） 隱藏檔。
（9） 歷史檔。

4.其它資料區（Other Data Areas）

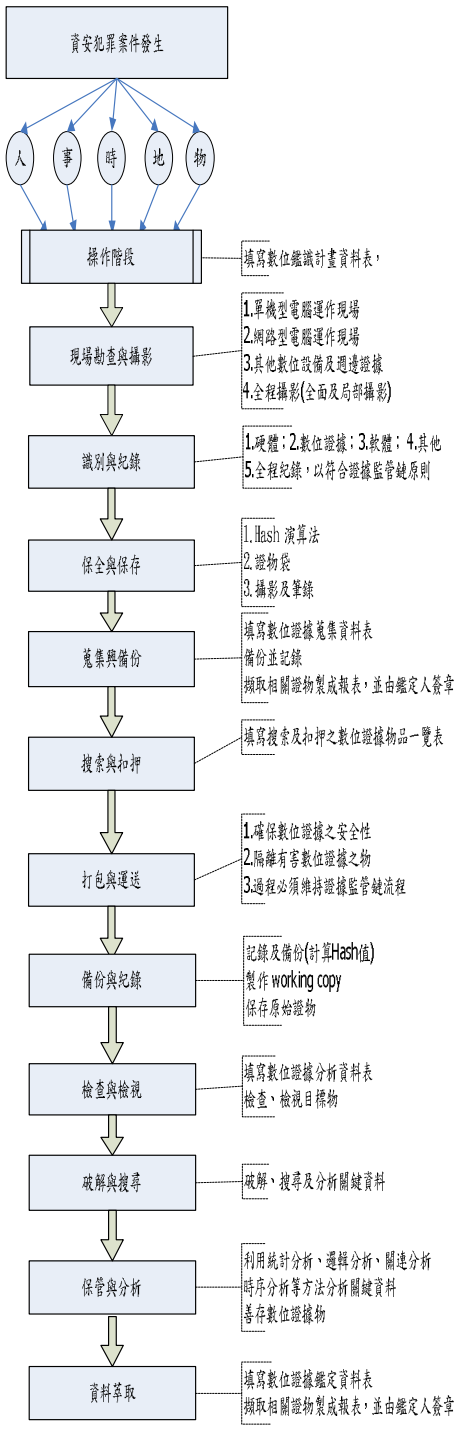
（1） 損壞磁區。
（2） 其它分割區。
（3） 電腦日期、時間和密碼。
（4） 保留區。
（5） 刪除檔。
（6） 檔案剩餘空間。
（7） 可用空間。
（8） 隱藏分割區。
（9） 系統區。
（10）遺失磁區。
（11）檔案未配置空間。
（12）資料。

3. 數位鑑識操作作業程序之原理及規範之探討

本研究提出（一）犯罪現場數位鑑識操作作業程序之原理及規範流程圖及（二）數位鑑識實驗室數位鑑識操作作業程序之原理及規範流程圖，分別如圖3.1及圖3.2所示及所設計流程分述如下。【5】

一、犯罪現場數位鑑識操作作業程序之原理及規範流程

犯罪現場數位鑑識操作作業程序之原理及規範流程，就是建立犯罪現場蒐證及鑑識作業之操作作業程序，其中包含操作階段的蒐集、分析、鑑定等項目規範事宜，其中犯罪現場的分析及鑑定步驟，係屬初步的處理，圖分為二部份，分別為左半部為程序流程，右半部為作業或規範內容來說明詳如圖3.1，本程序流程是大方向的程序，並不是嚴謹一定因果順序的關係，甚至相關的作為可以並行處理，也非要執行每個程序不可，可依個案的重要性及複雜性，選擇重要程序來執行，但其各規範內容原則及要求是不變的。



（接下頁）

(承上頁)

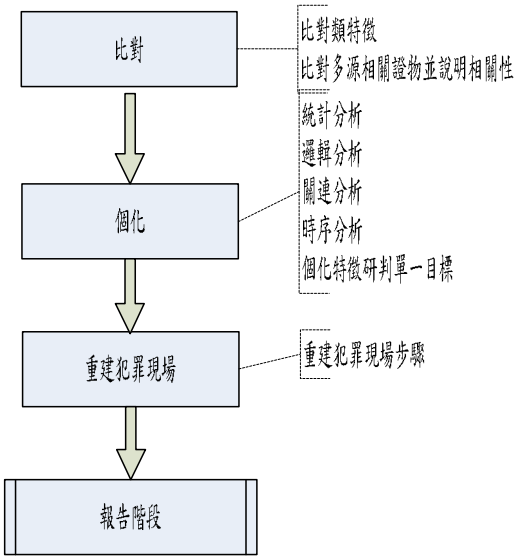
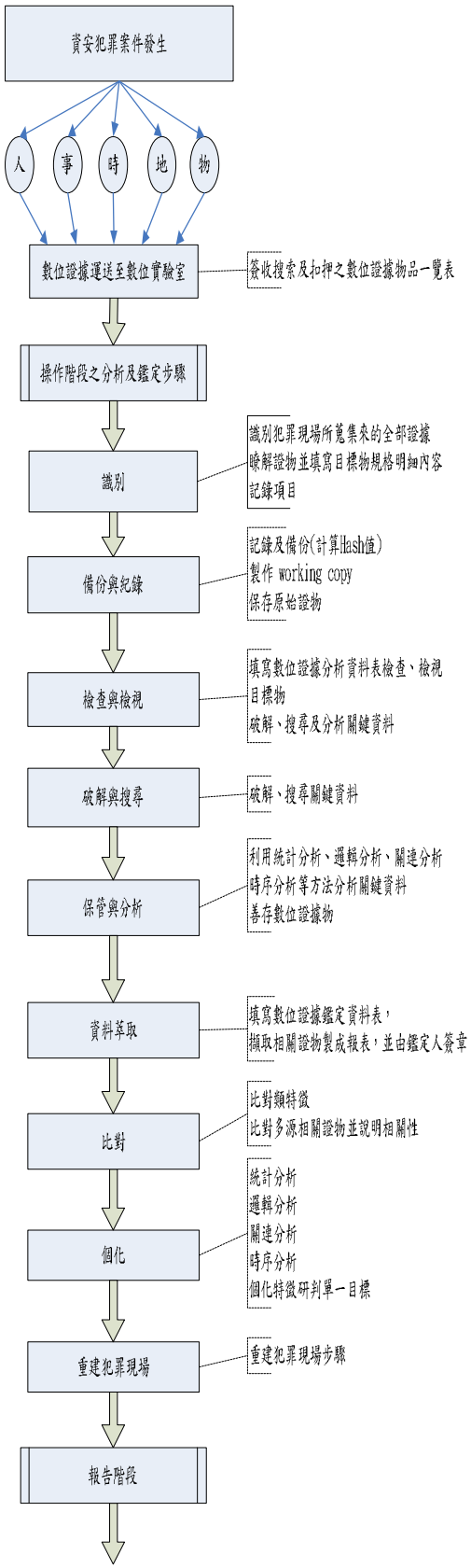


圖 3.1 犯罪現場數位鑑識操作作業程序之原理及規範流程圖

二、數位鑑識實驗室數位鑑識操作作業程序之原理及規範流程

數位鑑識實驗室數位鑑識操作作業程序之原理及規範流程，即是建立受各司法單位或政府機關委託數位鑑識之操作作業程序，其中包含操作階段的分析、鑑定項目及報告階段規範事宜，其中實驗室的分析及鑑定步驟，係較犯罪現場更一步的仔細及深度的處理，圖分為二部份，分別為流程及作業或內容規範來說明詳如圖 3.2，本程序之流程並不是嚴謹因果順序的關係，甚至相關的作為可以並執行，若考量時間及成本等相關因素，並非要執行每個程序不可，且可依案件的重要性及複雜性，可選擇重要程序來執行。



(接下頁)

(承上頁)

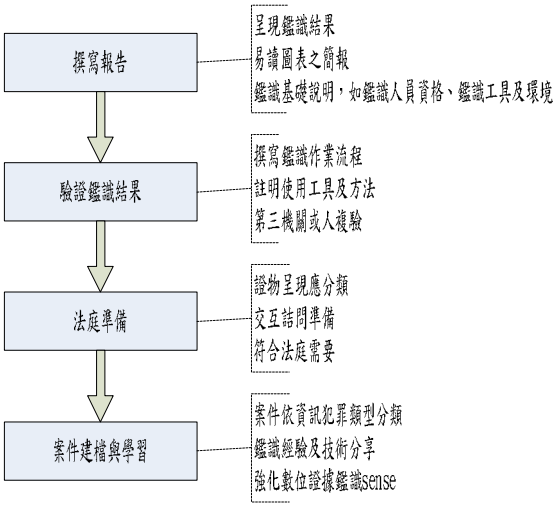


圖 3.2 數位鑑識實驗室數位鑑識操作作業程序之原理及規範流程圖

操作階段係屬實際針對目標物作鑑識的工作，即技術性的工作內容，本研究針對本階段之技術性的探討，設計操作性階段程序規範流程圖，詳如圖 3.3，列出相關的重點規範內容。其重要工作內容規範詳如如表 3.1。

表 3.1 操作階段重要工作內容規範

操作階段項目	重要工作內容規範
蒐集	● 完全現場回應（live response）資料蒐集。 ● 獲得網路及網路設備上的資料。例如：Intrusion detection systems、Routers、firewall 、switches、log servers 等。 ● 獲得主機上資料。例如：易揮發資料、系統時間、硬碟等資料。 ● 獲得可攜式上的資料，例如：備份磁帶、磁片、光碟片及隨身碟等。 ● 安裝活動監視工具。例如：sniffer 、network monitor，監視攝影等工具。 ● 確保完整及正確的蒐集，利用防寫保護及 Hash 計算等工具。 ● 蒐集後的包裝、運送及保存資料。
分析	● 減化大量的資料，使之能分析的量及形式。 ● 實施原始資料的調查，分析較明顯的數位證據。並評估犯罪嫌疑人的資訊技能。 ● 利用資料回復、破解、搜尋等功能的工具，去找到相關的證據。
鑑定	● 從大量資料中，萃取出與案情相關之資料。 ● 利用類特徵比對相關資料。 ● 利用多源類特徵及個特徵，以確定嫌疑犯，並能回答與案情相關之訊息，例如鑑定出是誰？是什麼?在何處?在何時？為什麼?及如何作到? ● 根據上述的資料，模擬犯罪現場重建的步驟。

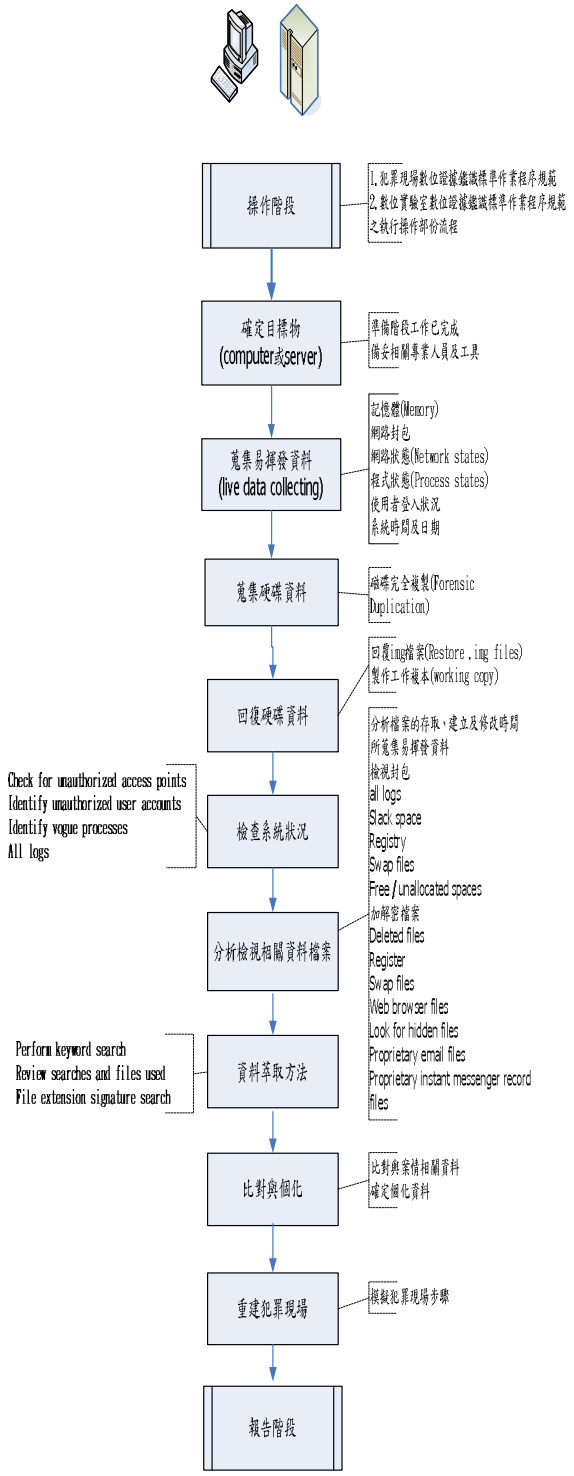


圖 3.3 操作階段程序規範流程圖

4. 結論與建議

4.1 結論

本研究最後提出數位鑑識操作作業程序之原

理及規範，共分為蒐集、分析、鑑定及報告步驟等程序之原理及規範，其中其中(一)蒐集：分為1.現場勘查與攝影，2.識別與記錄，3.保存與保全，4.蒐集與備份，5.搜索與扣押，6.打包與運送，等六項程序之原理及規範；（二）分析：分為1.備份及記錄，2.檢查與檢視，3.破解與搜尋，4.保管與分析，等四項程序之原理及規範，（三）鑑定：分為1.資料萃取，2.比對，3.個化，4.重建犯罪現場等四項程序之原理及規範，(四)報告:分為1.鑑識報告、呈現及簡報，2.驗證鑑識結果，3.法庭準備，4.案件建檔及學習等程序之原理及規範等。

4.2 建議

我國執法機關目前尚未建立數位鑑識標準作業程序之原理及規範，且數位鑑識的挑戰及困難存在並不少，例如：一、針對資料的挑戰，例如資料量不斷的增加、隱藏或加密資料的技術不斷創新；二、針對工具的挑戰，例如鑑識工具與惡意程式的開發時差、欺騙鑑識工具的方法等；三、針對鑑識者的挑戰，例如：鑑識往往由一人負責，駭客是遍及全球，造成一對無數人的窘境；四、針對科技的不斷創新的挑戰等等，都代表數位鑑識還有成長的空間及加強的部份，故希望相關機關應儘速製訂其標準作業規範外，最後本研究提出幾點之建議：

（一）國家應重視數位鑑識相關之人才之培養。

（二）建立數位鑑識相關證照及認證制度，例如本研究數位鑑識標準作業程序之原理及規範，能由第三專業的機關來認證。

（三）建立數位鑑識相關程序與工具設備之標準化及認證機制。

（四）應修正刑事訴訟法有關數位證據（電磁紀錄）搜索及相關法律之規定，以利偵查的需要

（五）加強司法人員對數位證據及數位鑑識重要性的認知，並提昇其數位證據之證據能力及證明力。

參考文獻

[1] 李昌鈺，1997年，犯罪偵查與刑案現場重建，內政部警政署，台北。

[2] 李俊憶譯，2005年，犯罪現場，李昌鈺刑事鑑定指導手冊，Henry Lee’s Crime Scene Handbook ，初版八刷，頁274-282。

[3] 林宜隆、閻瑣琳、陳受湛，2005年，中央警察大學資訊管理學系研討會，我國資安事件實驗室建構與規劃之探討以法務部調查局為例，桃園。

[4] 林宜隆，2001年，網際網路與犯罪問題之研究，桃園，中央警察大學，第二版。

[5] 黃志龍、林宜隆，2006年，「數位鑑識作業規範及流程」，第十屆資訊管理學術暨警政資訊實務研討會，中央警察大學，桃園縣。

[6] U.S.Department of Justice ，2001，Electronic Crime Scene Investigation，A Guide for First responders，http://www.ojp.usdoj.gov/nij Visited on 2005.10.03。

[7] U.S.Department of Justice，2004，Forensic Examiniation of Digital Evidence:A Guide for Law Enforcement，http://www.ojp.usdoj.gov/nij Visited on 2005.09.03 。