專題企劃

建構數位證據鑑識標準作業程序（DEFSOP）與案例實證之研究

元培科技大學資訊管理系（數位創新管理研究所）教授 林宜隆*

目　次

壹、前言

資通訊科技（ICT）日新月異發達的今日，電腦、網路及科技帶給人們工作、生活的巨大進步和便捷，各行各業幾乎都以數位方式來輸入、蒐集、處理、儲存、保管及利用資料，使數位資料無所不在，而電腦與網路亦成為犯罪標的及工具，各類與電腦網路有關之犯罪活動也層出不窮，故如何打擊和防治電腦網路犯罪，便成為司法界亟待解決的一大難題。當資安事件或資訊犯罪發生時，因需靠數位證據的鑑識能力以識別或還原真相，使得數位證據鑑識（Digital Evidence Forensics）的重要性不容忽視，故培養數位證據鑑識專業人才，成立「數位鑑識實驗室」建構數位證據鑑識標準作業程序（Digital Evidence Forensic Standard Operation Procedure，DEFSOP），乃是現今刻不容緩的問題，且應透過標準作業流程（SOP）及規範、工具的標準化及認證，以強化鑑識單位之數位鑑識能力及法庭上公信力，再者也應瞭解數位證據的特性及其在證據法上的規範，讓其標準作業流程及規範能更契合證據法的需要，才能增強其證據能力及證據證明力。

以出身於台灣刑事鑑識專家李昌鈺博士為例，其因鑑識各種刑案，讓許多證據能說話且建立鑑識科學的公信力及重要性而成為國際知名的鑑識專家[1]；那數位證據鑑識呢？由於資通訊技術的複雜性，在數位鑑識領域內要培養像李昌鈺這樣人物，並不容易，本研究乃參考、

* 中央警察大學資訊管理系所兼任教授；雲林科技大學科技法律研究所兼任教授；東吳大學法律研究所科技法律組兼任教授；cyberpaul747@mail.ypu.edu.tw；paul@mail.cpu.edu.tw。

1 請參閱參考文獻3、13、14。

蒐集國內外相關專家學者的數位證據鑑識作業流程及規範與數位證據相關文獻的探討，來建構數位證據鑑識標準作業程序（DEFSOP），並就四大階段：原理概念階段、準備階段、操作階段及報告階段，分別探討其重點工作、規範及流程，供檢、警及調偵查人員在處理數位證據鑑識時的重要參考依據及標準化，讓其標準作業流程及規範能更契合證據法的需要，以強化鑑識單位之數位鑑識能量及法庭上公信力，並以案例實證檢驗本研究團隊多年研究提出DEFSOP之可行性及有效性，使政府、司法機關、專家學者及民間業者對此一議題之重視。

貳、文獻探討與理論基礎

一、數位證據鑑識之意義與範圍

電腦鑑識（Computer Forensics）這個名詞是1991年波特蘭的國際電腦專家協會（International Association of Computer Investigative Specialists，IACIS）首次提出[2]，主要是在處理電腦有關的數位證據之保留、識別、萃取、記錄及解讀，以確保事件現場電腦物證及數位證據的原貌，使鑑定過程合法，鑑識結果具備完整性[3]，並能作為法院審理犯罪案件的重要參考依據。本文數位證據鑑識所涵蓋的範圍不單單僅限於電腦鑑識、網路鑑識，凡是以數位方式儲存的相關設備都包含在數位鑑識的領域中，包括：電腦、網路設備、PDA、手機、數位相機、記憶卡等數位設備，故亦稱資安鑑識（Cyber Forensics），其應包含電腦鑑識（Computer Forensics）、網路鑑識（Network Forensics）、軟體鑑識（Software Forensics）、資料鑑識（Data Forensics）及行動裝置鑑識（Mobile Devices Forensics）等五大分類，故凡舉與數位資料有關之鑑識皆屬之。是一門能夠幫忙解決資通安全事件或網路犯罪中數位證據難題的科學。故「數位鑑識科學」（Forensic Computing）其定義為：以周延的方法及程序保存、識別、抽取、記載及解讀數位媒體證據與分析其成因之科學[4]。

二、國內學者架構之數位證據之科學鑑識的蒐證程序及注意事項

國內有學者依據國際知名鑑識專家李昌鈺博士所架構之刑案現場鑑識蒐證方法，研擬一套數位證據之科學鑑識的蒐證程序及注意事項，詳述如下[5]：

㈠數位證據鑑識程序

1. 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：

⑴ 尋找硬體設備：找出儲存與犯罪有關資訊的硬體，如桌上型電腦，筆記型電腦及掌上型電腦等。

⑵ 尋找軟體：將犯罪現場特殊的軟體扣押，以協助日後偵查人員解析電腦檔案資料。

⑶ 尋找其他儲存媒體：例如軟碟或光碟片等。

⑷ 尋找與硬體、軟體及其他儲存媒體的文件。

⑸ 尋找電腦附近是否有密碼（password）或電話號碼等資訊。

⑹ 尋找與證物相關聯的電腦報表。

2. 保存、採集與記錄：

⑴ 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

2　請參閱參考文獻7、15、22。
3　請參閱參考文獻1、5、6、10。
4　請參閱參考文獻7、22、31、32、33、34。
5　請參閱參考文獻6、7、10、13、14、15。

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。

⑵ 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 Copy）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。

⑶ 記錄：記錄數位證據的原始狀態，或物證的位置，甚至可利用攝影機或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，必須記錄現在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。

3. 分類、比較與個化：

⑴ 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。

⑵ 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。

⑶ 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：

A. 內容：如電子郵件標題的內容，可以得到這封電子郵件來自那一台電子郵件伺服器或發信者的名稱等資訊。

B. 功能：以檢驗軟體功能分類與個化數位證據，例如檢驗某一軟體，具有木馬程式的特性時，同時進一步瞭解那一台電腦利用此木馬程式作為通訊的橋樑。

C. 特質：檔案名字、訊息摘要、建立的日期等有助於分類或個化數位證據。

4. 現場重建

⑴ 刑案現場重建分兩方面，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。

⑵ 現場重建應注意下列事項：

A. 記錄每一個現場重建的處理步驟。

B. 利用資料復原的軟體回復被毀損的數位證據。

C. 利用軟體工具尋找電腦硬體的空間是否有被刪除或覆蓋的殘餘資料。

D. 重建關聯性數位證據，係指物證與被害人或涉嫌人等之關係，如伺服器的紀錄檔，記錄那一台電腦主機或使用者使用過伺服器資源，即可利用以瞭解此數位證據與一般證物或犯罪有何關聯。

E. 重建功能性數位證據，某些證物發現及檢驗的結果，具有瞭解數位證據之功能及如何運作的功能，如入侵者入侵系統後，植入木馬

程式，以便再度入侵系統，當我們檢驗出入木馬程式功能，就可了解這台電腦已遭入侵。

F. 重建暫時性數位證據係指證據只是暫時性存在，例如兩台電腦正在連線時，可以利用指令查看連線動作，若斷線就無法得知連線狀態，以瞭解當時犯罪的情形。

㈡犯罪現場注意事項

1. 電腦系統的搜索與扣押之注意事項

⑴ 透過偵查、監視或情報資料研判電腦系統的種類（Windows系統、Linux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系統實際位置是否在搜索票的保管場所（如住家）。

⑵ 檢查是否有無線網路系統裝置。

⑶ 若需要扣押，則需要確定是否為搜索票所列範圍。

⑷ 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。

⑸ 檢查在現場有人控制的紅外線遙控或音控起動裝置。

⑹ 不要讓未經核准或未受過訓練的人員碰觸電腦或其週邊設備（FBI認為只有刑事電腦鑑定專家才能碰電腦）。

⑺ 攝影與錄影。

⑻ 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。

⑼ 尋找現場有無會破壞電子產品的大磁鐵。

⑽ 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。

⑾ 若電腦有連上數據機線，則應拔掉牆壁端的連線，測試電話是否可通，記錄在搜索時電話線是否在使用。

⑿ 打開電腦外殼蓋子對內部組件及設定拍照，拔掉所有電源連線。

⒀ 扣押與記錄。

⒁ 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。

⒂ 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。

⒃ 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。

⒄ 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. 證物處理注意事項

⑴ 切勿檢驗原始證物，應製作一份Bit Stream複製版本，讓證物保存原來的狀態，並讓所有人簽署證明與原版無誤。

⑵ 開啟檔案前應先用防毒軟體掃描。

三、美國學者Eoghan Casey的數位鑑識探討

Eoghan Casey在其「Digital Evidence and Computer Crime」第二版的書中，提出有關「數位證據及資訊犯罪偵查鑑識的作業技術及方法」，經本研究整理說明如下[6]：

㈠準備與授權：準備工作及取得授權書。

㈡識別（recognition）

1. 尋找硬體：除了桌上型電腦之外，尋找手提式電腦、掌上型電腦、外接式硬碟、軟碟，數位相機或其他儲存設備，及其他週邊設備如印表機、掃描器、數據機等等。

2. 尋找軟體：如果產生數位證物之軟體工具為特殊軟體，搜尋原版安裝磁片或光碟以利檢視證物。

6　請參閱參考文獻2、35。

3. 尋找可拆解式儲存設備：例如軟碟、ZIP / JAZZ磁碟、備份磁帶、光碟片、隨身硬體。犯罪者通常會以這類儲存媒體隱藏與犯行有關之資訊。

4. 尋找與硬體、軟體及可拆解式儲存設備有關的說明文件。這些文件有助了解軟、硬體及備份程序之細節，有助於偵查程序之進行。

5. 尋找密碼（password）或電腦及其週邊之電話號碼。電腦駭客通常會保有許多連線服務提供者之電話號碼、帳號及其密碼。

6. 從垃圾桶中尋找電腦報表或相關證據。這些報表常含有寶貴的資料，並可用來比較其與電腦系統資料之差異程度。

7. 尋找連結至網路系統之跡證。

㈢數位證據之保存（preservation）、蒐集（collection）與記載：

1. 錄影，特別注意線路連接情形：與一般之現場攝影情形一樣，有助於保全現場及增加證據力。

2. 對重要之螢幕畫面記載、攝影或錄影：如果發現有磁碟格式化程式或檔案刪除程式正在執行，應儘速將電腦主機後端之電源拔除。

3. 盡量列印相關證據，並令嫌犯當場捺印指紋或簽名，以資鑑別。

4. 繪製現場簡圖，並作筆記，記錄蒐證過程，以利現場重建。

5. 對每一項證物，均加註編號，註明日期、時間及蒐集人員，切實做好證物鏈之管理。

6. 如需查扣整部電腦需注意下列事項：

⑴ 接線及連接埠均加標籤，未用之連接埠亦以「未用」標示之。

⑵ 以空白之磁片，插入軟碟機，以資保護。

⑶ 以證物膠帶封閉電腦機盒及磁碟機，以避免不必要之碰觸。

⑷ 審慎裝箱，避免塵土、流體、潮濕、撞擊、過熱或過冷、磁場、靜電。

7. 如不需查扣整部電腦，但需查扣所有數位證物時，需注意下列事項：

⑴ 以另一開機片重新開機。

⑵ 記錄電腦系統之日期與時間，以及實際之日期與時間。

⑶ 拷貝二份（必要時以完整拷貝Bit Stream Copy為之），並確認之。

⑷ 對證物標號、加註日期、時間、蒐集人員，並載明電腦型式及其作業系統種類版本，以及拷貝用之軟體名稱。

⑸ 記載磁碟檔案系統之情形，如檔案之創設時間、修改時間等等，計算所有檔案及磁碟之雜湊值（Hash code）或稱訊息摘要（Message Digest），並載明證物之所以被蒐集之理由。

8. 只需查扣部份數位證物時：

⑴ 記錄電腦系統之日期與時間，以及當時之日期及時間。

⑵ 拷貝二份（必要時以完整拷貝Bit Stream Copy為之），並確認之。

⑶ 對證物標號、加註日期、時間、蒐集人員，並載明電腦型式及其作業系統種類版本，以及用於拷貝之軟體名稱。

⑷ 記載磁碟檔案系統之情形，如檔案之創設時間、修改時間等等，計算所有檔案及磁碟之雜湊值或訊息摘要，並載明證物之重要性及其之所以蒐集之理由。

㈣過濾和數據簡化

由於數位資料容量非常龐大，則需要進一步過濾和數據簡化，以求時效。

㈤證據之分類（classification）、比對（comparison）與個化（individualization）：

1. 分類：詳細檢查特徵並加以分類，例如證物存在之作業系統為Windows、Unix或 Linux，其應用軟體之種類及名稱，是否為特殊之軟體環境所產生等。

2. 比對與個化：將證物與已知之樣本比對與確定其來源，並檢查有無特殊可作為鑑別之特徵。

㈥證據恢復與犯罪現場重建：

1. 記錄重建時所作之每一動作。

2. 可能的話，重複證物之產生過程，以釐清案情。

3. 以資料回復工具，找回遭刪除、或破壞之數位證物。

4. 以特殊之軟體搜尋slack space或swap files之內容。

5. 重建物件與物件或犯罪者之關聯。

6. 重建物件之功用或如何被使用。

7. 重建物件發生之時間關係。

㈦報告結果

1. 報告內容不宜太複雜須簡化。

2. 須以易懂易讀方式呈現技術性的問題。

3. 針對不同的作業系統須編寫不同的報告。

四、我國警察偵查犯罪規範、刑事鑑識規範

1995年我國刑事警察局為新興電腦犯罪的需要，制定警察偵查犯罪規範，係依據刑事訴訟法等規定，綜合有關偵辦刑事案件規定訂定之，作為辦案程序之準據。該規範列出了有關執行電腦犯罪案件搜索前置作業、執行電腦搜索、電腦犯罪案件證物處理、電腦犯罪案件電腦鑑識等應注意事項，詳列如下說明：

㈠警察偵查犯罪規範[7]

1. 執行電腦犯罪案件搜索前置作業應注意事項：

⑴ 依據民眾檢舉或主動上網發現非法網站，蒐集相關資料。

⑵ 調閱搜索對象基本資料：運用警察資訊系統、刑事資訊系統或其他資訊系統調閱搜索對象基本資料。

⑶ 決定搜索地點、對象與時間：依據搜索對象上網時間及地區，決定搜索地點。

⑷ 勘查搜索環境：

A. 確定搜索地點是否正確。

B. 確定搜索地點電腦設備及其數量。

⑸ 擬訂搜索計畫：

A. 勘查現場、畫現場圖：確定有那幾種型式的電腦及其數量、使用的系統、媒體、週邊設備等以決定搜索警力。

B. 擬定搜索成員及其任務：依據現場勘查結果，估計搜索所需警力，並分配每位人員任務。

C. 訂定搜索計畫：搜索計畫應含下列的項目：

(a) 現場狀況：現場人數、電腦數量及其系統。

(b) 任務：搜索何種犯罪型態網站，如色情、盜賣非法光碟網站等。

(c) 搜索項目：依據搜索對象係何種型態網站擬訂搜索項目。

(d) 交通：前進與離開路線。

(e) 通信：回報搜索結果或請求支援。

⑹ 技術勤前講習：說明搜索任務、項目，模擬現場搜索狀況，講解人員示範如何操作電腦，自電腦內部取出犯罪證據，並由搜索人員親自實際操作演練。

2. 執行電腦搜索應注意事項：

⑴ 執行扣押時以扣押整套電腦設備為宜，包含電腦主機、銀幕、鍵盤、電源線等周邊設備。

⑵ 扣押電腦應符合比例原則，尤其網路公司應特別注意其影響層面。

⑶ 扣押物品時最好使用原扣押物的包裝或紙箱以免扣押證物受損影響其證據力，尤其是電腦主機內含所有重要證據，更需小心拆裝搬運。

⑷ 磁碟片、光碟片等電腦輔助記憶體之數量應確實清點，並詳載於搜索扣押證明筆錄中。

7　請參閱參考文獻12。

3. 電腦犯罪案件證物處理應注意事項：

(1) 電腦：使用原設備包裝或紙箱避免受損影響其證據力，並小心拆裝搬運。

(2) 磁碟片、光碟片：避免置於強光、高溫、磁場附近及灰塵場所。

4. 電腦犯罪案件電腦鑑識應注意事項：

(1) 重大特殊案件之電腦證物遭毀損、刪除、格式化或經加密無法解讀，得將證物送刑事警察局資訊室電腦犯罪小組鑑識解析。

(2)鑑識前應先將重要資料備份以完整保存證據，必要時可全部備份。

(3)鑑識時應於備份資料執行非破壞性鑑識，必要時得於原始資料鑑識解析。

(4)如電腦資料、檔案或證據已遭刪除或格式化，應還原被刪除或格式化的資料、檔案或證據。

(5)如電腦資料、檔案或證據被隱藏，應還原隱藏電腦資料、檔案或證據。

(6)如電腦資料、檔案或證據被設定密碼，應將所設定之密碼解密。運用搜尋工具，輸入檔案名稱或檔案內容可能出現之數字、姓名或文字串，搜尋電腦內部重要檔案或證據。

㈡刑事鑑識規範[8]

內政部警政署為提升刑事鑑識水準，確保刑案現場勘察採證品質，並完備相關法律程序，特訂定本規範。其鑑識範圍包含下列1.物理鑑識，2.化學鑑識，3.電氣鑑識，4.印文鑑識，5.痕跡鑑識，6.影像鑑識，7.測謊鑑識，8.毒物鑑識，9.聲紋鑑識，10.指紋鑑識，11.法醫鑑識，12.刑案現場處理等十二項鑑識，並無所謂數位鑑識的規範，本研究參考其內容，整理出下列與數位鑑識相關的規範。

1. 現場勘察

(1) 現場勘察人員主要任務如下：

A. 運用科學技術與方法勘察現場、蒐集證物，作為犯罪偵查及法庭審判之證據。

B. 採集各類跡證，依其特性分類並妥善保管，送相關單位鑑驗。

(2) 現場勘察應視實際需要攜帶下列器材：

A. 照相、錄影及照明器材。

B. 測繪器材。

C. 採證器材、工具。

D. 包裝、封緘、保存器材。

E. 其他必要器材。

(3)現場記錄方法及要領：

A. 為記錄現場跡證原始位置與狀況，蒐證前之方法：(a)照相，(b)錄影，(c)筆記，(d)測繪、(e)錄音。

B. 現場照相要領：

(a) 現場照片應求真、求實並表明現場相關位置、現場全貌及現場內重要跡證。

(b) 照相前，勿觸碰或移動現場跡證。

(c) 重要跡證為顯示其大小，應於其旁放置比例尺。

(d) 重要跡證在採取前宜先照相。

2. 刑案證物包裝、封緘、保管與送驗

(1) 刑案證物應依其特性，使用適當之工具或方法採取，分開包裝、封緘，包裝外應註明案由、證物名稱、採證位置、數量及採證人姓名等資料。

(2) 刑案現場證物採取後，應即製作證物清單，如所有人、保管人、持有人在場者，應付與其證物清單，並請其簽名確認。

(3) 刑案證物自發現、採取、保管、送驗至移送檢察機關或法院，每一階段交接流程（如交件人、收件人、交接日期時間、保管處所、負責保管人等）應記錄明確，完備證物交接管制程序。

(4) 各級警察局鑑識或刑事單位，應設置貯存刑案證物之專櫃，並指派專人負責保管。

8 請參閱參考文獻4。

參、建構數位證據鑑識標準作業程序（DEFSOP）

本研究在探究相關文獻及本研究團隊的多年的研究後[9]，認為建構數位證據鑑識標準作業程序（DEFSOP），可分為原理概念階段、準備階段、操作階段及報告階段等四大階段，如圖1數位證據鑑識標準作業程序架構圖，分述如下：

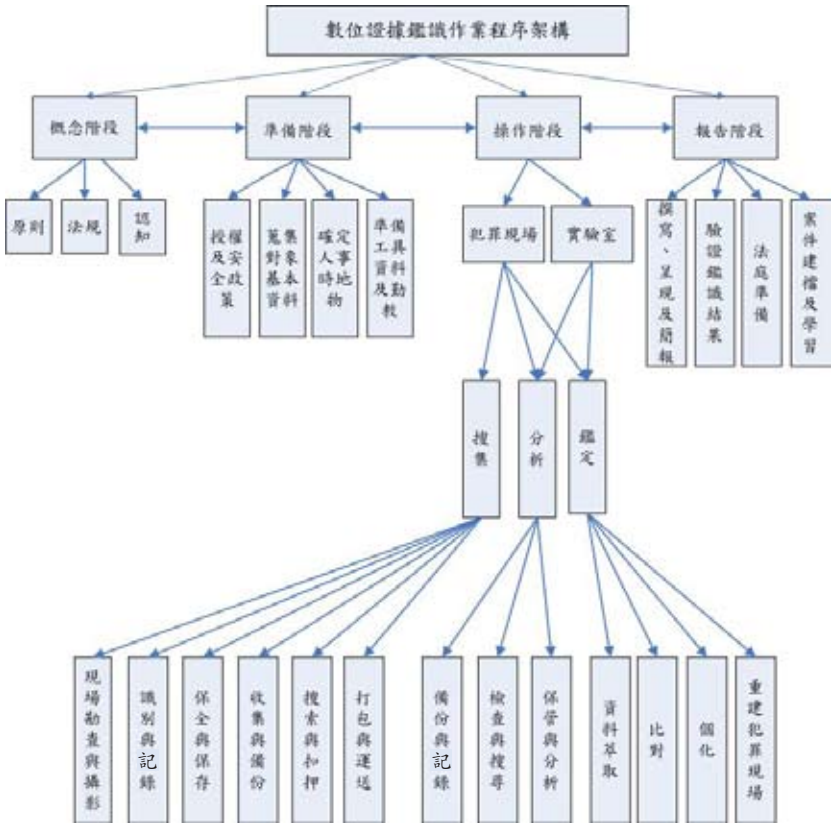


圖1　數位證據鑑識標準作業程序架構圖

一、概念階段

本階段分為原則、法規及認知三項規範分述如下[10]：

㈠原則

數位證據鑑識工作（Digital Evidence Forensic）的指導原則如下：

1. 應制定大原則，並不宜訂太細原則。
2. 不變更數位證據原則。
3. 電腦鑑識程序完整記錄原則。
4. 人員專業性原則。
5. 電腦鑑識工具應獲得國際專業機構認可。
6. 最佳證據原則。
7. 最小侵害性原則。
8. 運送與保存應符合安全性原則。
9. 確保原始證據的完整性。專人操作及負責。

㈡法規

1. 法規規範是重要的且程序合法始有證據能力。

9　請參閱參考文獻1、4、6、7、8、9、10、11、19、20、21、22、31、32、33、34、35。
10　請參閱參考文獻5、10、19、20、21、22、31、32、33、34。

2. 符合證據法中對於真實性、可靠性之要求。

3. 應規範人員資格、設備及鑑定環境之要件。

4. 視個案情形，以刑事訴訟法、行政訴訟法及民事訴訟法關於證據之規範為最低要求。

㈢認知

數位證據鑑識不應限於資訊犯罪發生後，才來作數位證據鑑識，應該是把數位證據鑑識當作是資訊犯罪預防的一項重要的工作，且分為1.事前鑑識：安全防護機制及應變計畫，2.事中鑑識：處置及保留證據，3.事後鑑識：鑑定及資料復原等三階段的鑑識認知，因數位證據易消失、修改及刪除等特性，故其走過未必留下痕跡，故數位證據鑑識的認知，就是讓其走過必留痕跡且強迫留下痕跡，才能供事後鑑識的需要。

二、準備階段

㈠授權及資訊安全政策

1. 授權

執法人員或系統管理人員在執行數位證據鑑識工作前，除應具備上述的條件及能力外，最好必須先獲得授權書（搜索票）或資訊安全政策規範的支持，尤其是執法人員，避免涉入訴訟及確保證據的證據能力，依程序取得搜索票且遵守上述法規的注意事項後，才執行數位證據鑑識。

2. 資訊安全政策

能在合法之下合理的蒐集數位證據而不影響商業的運作，且當蒐集證據是為了潛在的犯罪及爭議，且可能會衝擊組織，故容許調查的進行是有一定比例的風險，調查應儘量減少防礙商業的運作，且任何行動結果應確保證據是對組織是正面幫助的，故企業或政府機關都必須要有資訊安全政策。

3. 蒐集對象基本資料

當資訊犯罪事件發生進入偵查階段時，根據資訊犯罪偵查流程圖，掌握重點資訊，以人、事、時、地、物及理由的角度，從各種管道，蒐集與案情相關的資訊，以發現嫌疑犯。

4. 確定人、事、時、地、物及理由

當能發現可能之嫌疑犯，訪談與案情相關的人員，再深入瞭解案情，綜合所蒐集的資訊，以掌握蒐搜的人、事、時、地、物及理由之資訊。

5. 準備工具、資料及勤教

根據案情的類型及特性，準備不同之軟硬體工具設備及資料，含犯罪現場鑑識工作必填之相關表單及搜索票。任務出發前，依各人之專長，作好任務編組，建立指揮系統及讓能彼此能相互溝通的管道，並做好勤前教育及演練，說明案情、搜索之任務、範圍、重點，且宣達每人的任務，檢查相關之工具是否準備齊全，以期發揮最大的工作效能。

任務編組必須要有下列之重點工作人員，依本研究整理出數位證據鑑識人員重點工作編組圖2，重點工作分述如圖內容說明，現場必須要有指揮者，連繫各項工作及做最後的決定，及主持搜索調查最後的討論事項的確認[11]。

11 請參閱參考文獻1、13、14、21、22、23。

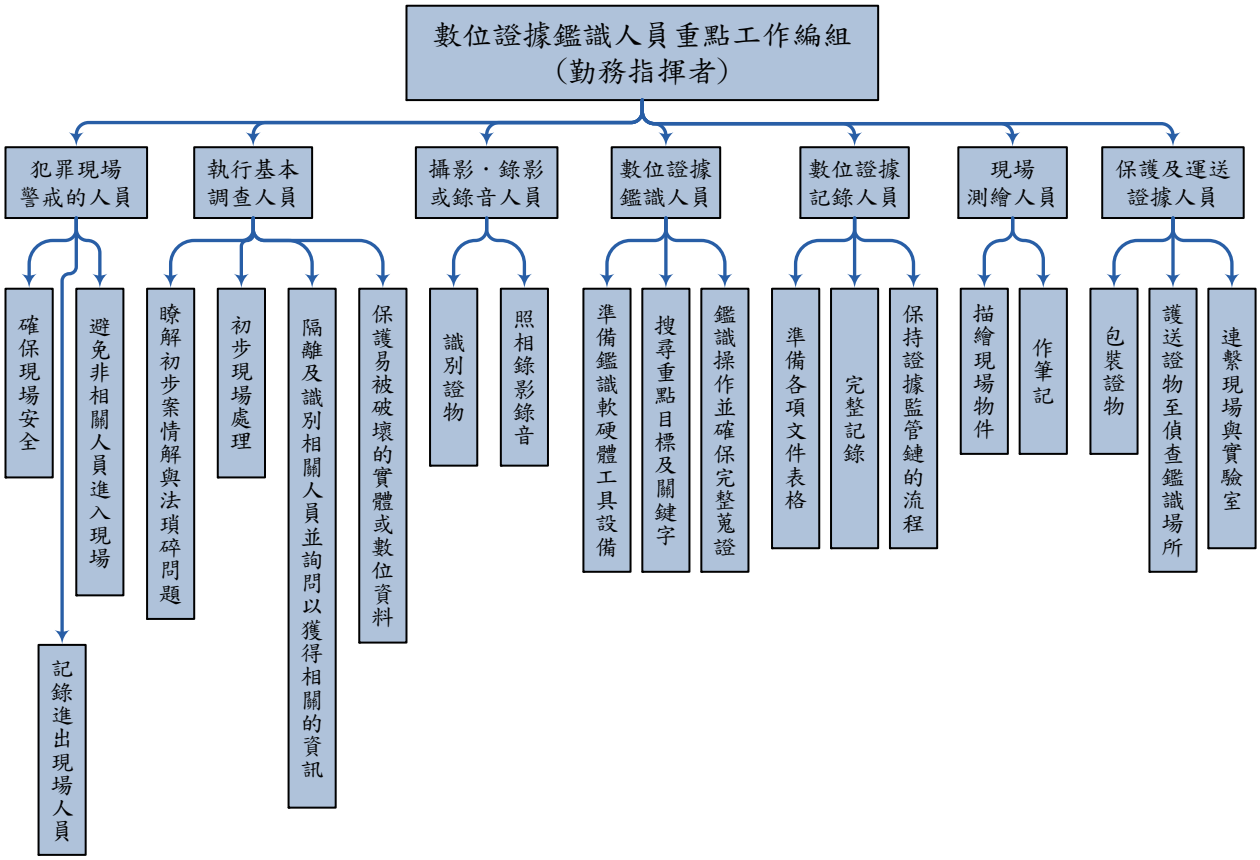


圖2　數位證據鑑識人員重點工作編組

除上述重點工作外，搜索調查到最後，必須要與所有執行搜索人員討論，以確保已完整及正確記錄所有的文件，攝影最後的狀況場景，確保所有證據物都被扣押了，及已對所有設備作蒐證及鑑識資料，沒有忽略易隱藏及困難處理的區域。

三、操作階段

人員到達現場依其任務展開蒐集、分析及鑑定的工作，本階段是展開鑑識的操作階段，現場蒐證最重要的即是要發現犯罪證據，但為求慎慎，本研究提出數位證據鑑識計畫資料表（詳如附錄），供鑑識作業時檢查，並將其鑑識作業分犯罪現場數位證據鑑識標準作業程序流程及數位鑑識實驗室數位證據鑑識標準作業程序流程，分述如圖3及圖4，及各項規範探討如下[12]：

12 請參閱參考文獻1、4、8、9、21、22、23、31、32、33、34。

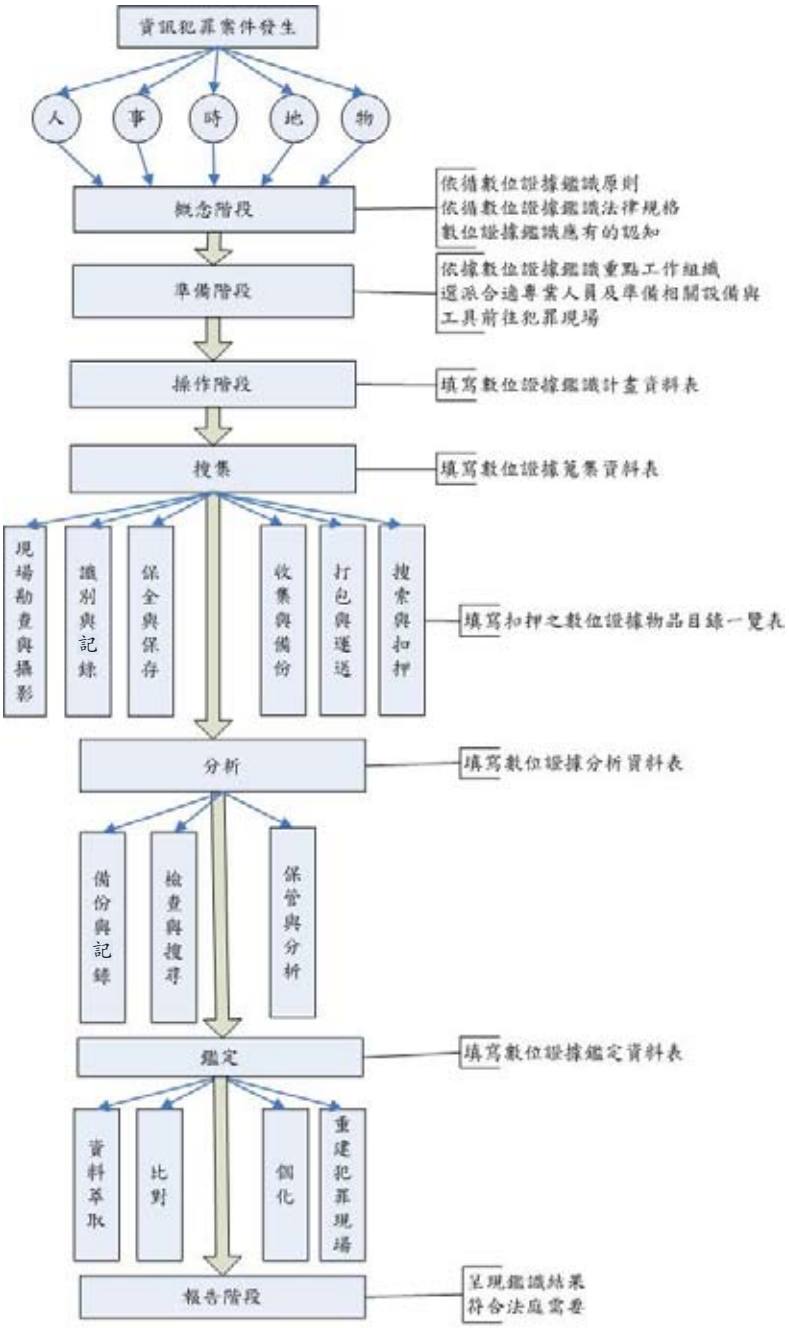


圖3　犯罪現場數位證據鑑識作業程序流程圖

㈡數位鑑識實驗室數位證據鑑識標準作業流程

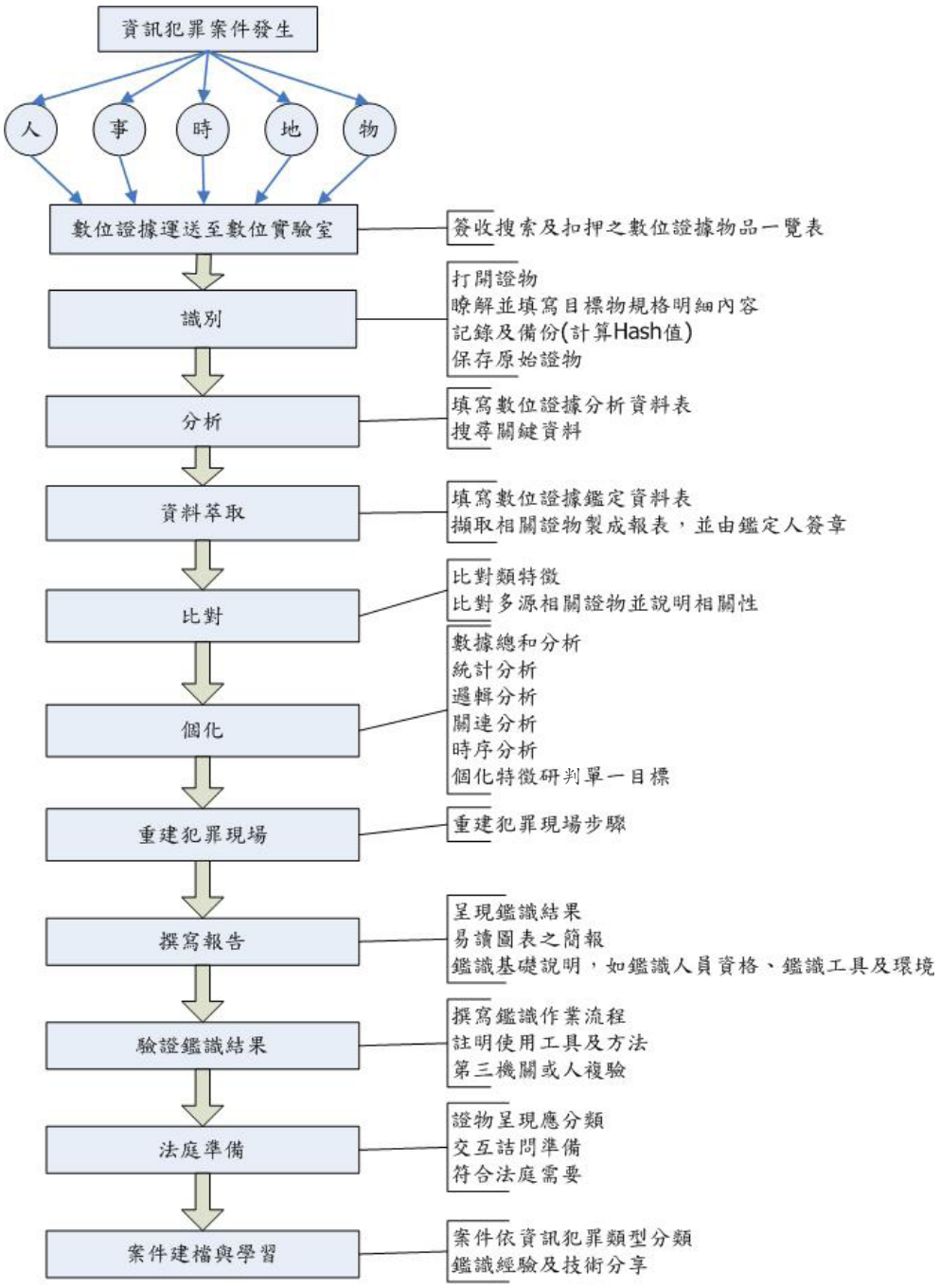


圖4　數位鑑識實驗室數位證據鑑識作業程序流程圖

1. 搜集

數位證據之搜集，係執法人員到達現達的首要工作，其工作項目，依本研究可分為(1)現場勘查與攝影，(2)識別與記錄，(3)保全與保存，(4)收集與備份，(5)搜索與扣押，(6)打包與運送等六項工作，分述如下：

(1) 現場勘查與攝影

A. 現場勘查

在刑事案件中，現場是指罪犯犯罪的地點，往往遺留下來的證據也最多，但網路的特性使得犯罪所遺留數位證據的地方，不僅包括犯罪者的電腦及場所、受害者的電腦及場所，其所經過的網站主機，現場勘查就是對這個現場進行有效且全面性的勘查。

B. 攝影

在刑事案件中，現場是指罪犯犯罪的地點，往往遺留下來的證據也最多，但網路的特性使得犯罪所遺留數位證據的地方，不僅包括犯罪者的電腦及場所、受害者的電腦及場所，其所經過的網站主機，現場攝影就是對這個現場進行有效且全面性的攝影。

(2) 識別與記錄

A. 識別

當初步勘查現場後，決定扣押物範圍，除攝影存證外，應製作標籤，並妥善封緘所有要扣押證物均應依序編列流水號，分類依序識別。若證物移轉保管應遵守扣押證物監管鏈流程原則，交付人、收受人需要簽名，以示負責。

B. 記錄

於犯罪現場拆解電腦各項設備前，應先從各種角度拍攝各種硬體設備銜接的情形，做各項設備之連接的紀錄，並貼上標籤記號。如受鑑證物為電腦主機，首先記錄系統時間。記得將主機的外殼拿掉，檢視主機裡面有那些東西，並記錄下來。記錄檔案名稱、建立與修改之日期、時間。記錄實施電腦鑑識之處理過程或使用之鑑識軟體工具，及其產生之結果，並由鑑定人簽名。記錄電腦系統及真實之日期與時間，故記錄工作是瑣碎的，必須記錄每一件事及搜證的程序應包括是誰？在那裡？如何？什麼時候？為什麼收集證物？等等，以符合證據監管鏈流程及完整性原則。

(3) 保存與保全

證據保存與保全即證據的固定和保護，是指用一定的形式將證據固定下來，加以妥善保護，以便於法官及檢調人員分析、認定案件事實時使用。證據保全是蒐證制度的重要環節，證據蒐集工作的延續。數位證據相對於傳統證據而言，往往更易於被刪除、修改，因此加強數位證據的保存與保全工作具有更特殊的意義。例如常用方法或工具如現場製作筆錄、錄影、證物袋與MD5。

(4) 收集與備份

若是網路主機系統，因硬碟容量非常大，若非特殊案件，非必要否則建議不現場備份，因備份所需花費的時間成本相較的較久，也可僅收集重要資料。

備份的原因是因為無法攜走原始證物，為了要能確保完整性，備份應採Bit Stream Copy，完後仍需再針對現場製作的該硬碟Image檔進行MD5運算，將其記錄其Hash code，一切證據當場請嫌犯簽名捺印。

(5) 搜索與扣押

搜索是偵查人員為了收集犯罪證據，對可能隱藏犯罪證據的人的身體、物品、住處和其他相關場所進行的專門調查活動。只要在搜索中發現了可以證明犯罪嫌疑人有罪或犯罪案情相關的物品和文件，則應當扣押，根據案件不同類型，有其不同的搜索重點目標，搜索現場之蒐證並不全然僅是電腦及相關儲存裝置的勘驗，應該還得視案情本身，搜索於犯罪現場所有相關的事證。例如販賣盜版光碟的案件就應特別注意盜版工具、盜版成品、金融存簿等資料。在搜索和扣押數位證據前，偵查人員有必要作縝密的準備工作，例如在蒐搜票上是否已

完全註明清楚。

(6) 打包與運送

將原始證物封緘保存，並注意安全性及隱密性，依照安全物證管制措施，將電腦設備運送至安全及鑑識之處。這些行為應確保不增加、修改或破壞儲存在電腦或其它儲存媒體內的資料，電腦是易碎的裝置且對溫度、濕度、震動、靜電和電磁敏感的，所以，當打包、運送和儲存數位證據時特別預防是必須的，為了維護數位證據的證物鏈，應記錄打包、運送和儲存過程。確保打包、運送和儲存數位證據時有適當的程序可遵循，以避免資料被修改、遺失、損失或破壞。

2. 分析

在數位證據搜集打包後，需要進一步鑑識的證據，應該先送回相關警察機關保管，或逕送數位證據鑑識實驗室，作進一步的分析，或因案情需要，須在其犯罪現場作初步的分析，其工作項目，依本研究可分為：(1)備份及記錄，(2)檢查與搜尋，(3)分析與保管等三項工作，以確保分析資料的完整性及正確性。

(1) 備份及記錄

A. 備份

若扣押原證據，在鑑定數位證據前，必須將所有電腦儲存設備之空間利用位元拷背方式，進行資料的完整備份，再以備份的資料作為實施分析與鑑定之對象。針對證據檔案或備份資料進行分析。

B. 記錄

為遵守鑑據監管鏈流程原則，在做任何備分或分析動作時，都做好紀錄或錄影存證，且每項證據都要讓相關之人員簽名捺印，以示負責。

(2) 檢查與搜尋

A. 檢查

檢視於受鑑證物上之所有檔案，包含正常檔案、已刪除但實際上仍存在的檔案、隱藏檔、壓縮檔及有進行過加密的檔案。此部份的工作包含顯示隱藏檔、救回已被刪除的檔案、顯示暫存檔、交換檔、殘餘檔案及存於閒置空間之內容，以及解開遭壓縮、加密及隱藏之檔案。

B. 搜尋

由於資料龐大，先必須利用關鍵字去搜尋關鍵性的資料，例如：在檔案、殘餘檔案、尚未配置空間及已刪除檔案搜尋，利用與犯罪有關的關鍵字，進行檔案、殘餘檔案、未使用硬碟空間的搜尋，找出與犯罪有關聯的證據資料。

(3) 分析與保管

A. 分析

分析證據時，必須要能初步判斷不同的案情，會有不同的類型的重要資料，例如在兒童色情案例中，第一位反應或蒐證者合理期待發現下述證據，故可重點式分析，分述如下：

(a) 聊天紀錄；

(b) 日期與時間Stamps；

(c) 數位相機軟體；

(d) 電子郵件、備忘錄、相關文件；

(e) 遊戲軟體；

(f) 繪圖及影像編輯及觀看軟體；

(g) 影像檔；

(h) 上網活動記錄；

(i) 電影檔；

(j) 移動刪除的檔案；

(k) 自建一些影像的目錄及檔案名稱。

B. 保管

扣押之原始數位證據要妥善的保管存放，由於備份容易及價格越來越便宜，在實驗室作任何分析動作時，千萬不要動到「原本」數位證據，只對複本作分析，必要時可備份二份，其保管過程或注意事項如下：

(a) 在保管過程中，儲存證據在安全區域遠離極大的溫濕度，保護它遠離磁性、濕氣和灰塵和其它有害的顆粒或污染物，並避免證據被人為破壞，建議最好能存放在如金庫的地方。

(b) 最好只有少數人且經過授權的人才能取得保管證據場所的門鎖之專責場所，且存放的地方必須有24小時的監控錄影。

3. 鑑定

其數位證據資料還是很龐大時，就需要進一步鑑定證據，作進一步的分析，其工作項目，依本研究可分為(1)資料萃取，(2)比對，(3)個化，(4)重建犯罪現場等四項工作，為確保分析資料的完整性及正確性。

(1) 資料萃取

在分析數位證據時，由於資料龐大且時間的限制，必須要過濾數位證據，除原始數位證據不要作任何動作外，針對複本把精力集中於最有可能之資料，萃取出與案件相關之資料。

(2) 比對

數位證據的來源是多方面的，要先瞭解需要什麼類型的證據和證據來源，先識別相似特徵的證據，即所謂類特徵，例如：.doc的檔案是否是Microsoft Word的文件或WordPerfect的文件，必須先比對清楚；電子郵件的標頭訊息，就可得知是由那裡的主機伺服器所傳送及IP的位址。

(3) 個化

由於數位證據易遭到修改或隱藏，若只靠一個個化證據，有時會欠說服力，故當找到類特徵證據時，除要個化其特徵證據至個化特徵，必須多鑑定出有多源證據的個化特徵，例如：撥接上網的訊息，最好能利用身份證明伺服器及Call-ID系統分別找出電話號碼、帳號、住址、IP及MAC adrress等個化特徵皆指同一人或同地方。

(4) 重建犯罪現場

犯罪現場重建是依據犯罪現場的痕跡、證據的位置與實驗室鑑識的結果，以研判當時犯罪發生時的所有活動，不管是刑事案件或資訊犯罪皆可適用，其所涉及到現場科學、資訊、統計及邏輯分析，尤其數位證據易消失的特性，若沒有作好事前鑑識的工作，紀錄所有資訊流的活動，其資訊犯罪的重建工作，將是一大難題，證明鑑識的工作，不像是一般的刑事案件，是事後才作鑑識工作，而是應具備有事前、事中、事後鑑識的概念，機關或公司網路系統若事前能同步記錄進出之資訊流的資料，待資訊犯罪發生時，也能同時記錄其所有活動情形，待鑑識時，就能蒐證及分析其犯罪之數位證據，利用暫時性重建、相關性重建及功能性重建，重建其犯罪現場。因少有機關有事前鑑識的準備，故重建犯罪現場之困難性高，故應利用多重證據源的重建，以提高其正確性。例如：結合router,firewall,ids及其他系統中的日誌文件，有時才能揭示出重要的信息。

4. 報告階段

本研究提出報告階段可分為(1)撰寫報告、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。分述如下：

(1) 撰寫報告、呈現及簡報

A. 撰寫報告

鑑識報告，是必須要給法官、被告及偵辦人員等相關人員閱讀的，故內容不宜太深奧，且又必須呈現真實的內容，其包含內容如下：

(a) 註明報告的單位；

(b) 案件的識別編號；

(c) 註明案件調查員姓名；

(d) 收到數位證據的時間日期；

(e) 鑑識報告的時間日期；

(f) 描述一連串檢測的項目，包括序號、作法與程序；

(g) 註明檢驗人員並簽名負責；

(h) 簡述鑑識的問題及證據監管鏈的流程說明；

(i) 結果呈現；

(j) 備註：鑑識人員的資格、鑑識工具及環境說明。

B. 呈現及簡報

原則上可供證據的物品皆應作為呈堂證供，即具有證據能力及證明力之證物都要呈現

及報告於法庭上，由於數位證據資料龐大，若要一一列印出，可能其報表比人都還要高，故在簡報時，可以整理出圖表說明，但證據表現的形式必須符合法律規定，即下列原則來呈現：

(a) 用圖表提供整個事件的綜覽。

(b) 用可視覺化的工具。

(c) 用簡單易懂方式描述技術性及複雜的問題。

(d) 針對不同作業系統類型編寫不同的報告。

(2) 驗證鑑識結果

鑑識結果的正確性，除遵守相關之原則外，其操作手冊及相關表格建立，鑑識工具的使用說明在電腦鑑識領域中是相當重要的一環。鑑識人員必須撰寫鑑識流程及使用工具，以便日後第三人或機關檢驗或複驗以求其正確性及公信力。

(3) 法庭準備

數位證據鑑識應分類，說明符合證據監管鏈的流程，作好法庭交互結問的準備工作，以最專業及最真實的呈現給法官裁判。

(4) 案件建檔及學習

由於數位證據鑑識是不斷進步的科技及技術，每件案件應依案件類型分類，建立每件案件的卷宗及經驗、技術分享，最好建立專家知識庫，供下次他人偵辦案件參考。

肆、案例實證檢驗本DEFSOP

資訊犯罪類型，常見的類型依網際網路在犯罪中所扮演的角色，可將資訊犯罪分為以下三類：一、以網路空間作為犯罪場所；二、以網路為犯罪工具；三、以網路為犯罪客體，如表1所示[13]。

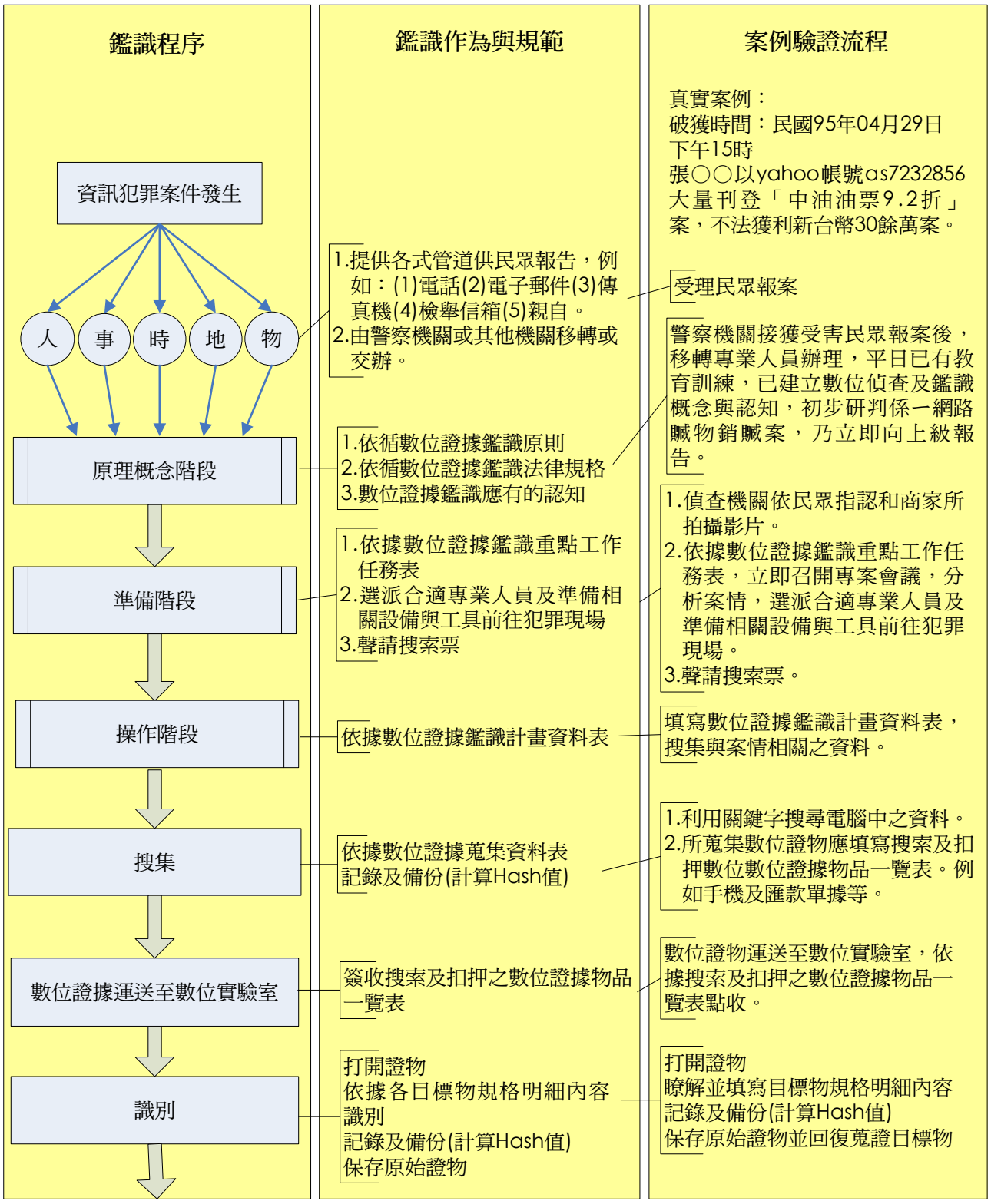
表1　資訊犯罪之分類及其常見型態分類標準

	特點	常見型態	知悉程度	偵查難度	鑑識難度
以網路空間為犯罪場所（被動）（類型一）	被動性質，引誘吸引一般人進入	1. 網路色情。 2. 網路援交。 3. 販賣盜拷。 4. 網路賭博。 5. 網路遊戲。 6. 販賣槍械。 7. 教授仿製炸彈。	高	低	低
以網路為犯罪工具（利用、方法）（類型二）	針對特定目標予以侵害性質，藉由網路作為犯罪工具	1　網路恐嚇。 2　網路誹謗。 3　網路詐財。 4　網路釣魚	中	中	中
以網路為犯罪客體（為攻擊目標）（類型三）	對網路或電腦系統的攻擊性或破壞性	1　網路入侵或干擾。 2　散播電腦病毒。 3　網路竄改。 4　SQL Injection。	低	高	高

13 請參閱參考文獻1、10、31、32-34。

一、案例一

經由案例分析驗證本DEFSOP，可以更清楚的了解，網路犯罪多數符合數位證據鑑識標準作業程序（DEFSOP）流程圖，首先介紹以類型一網路空間為犯罪場所，以雅虎帳號拍賣92折中油油票涉嫌詐騙為例，如下圖4.1所示：



（接下頁）

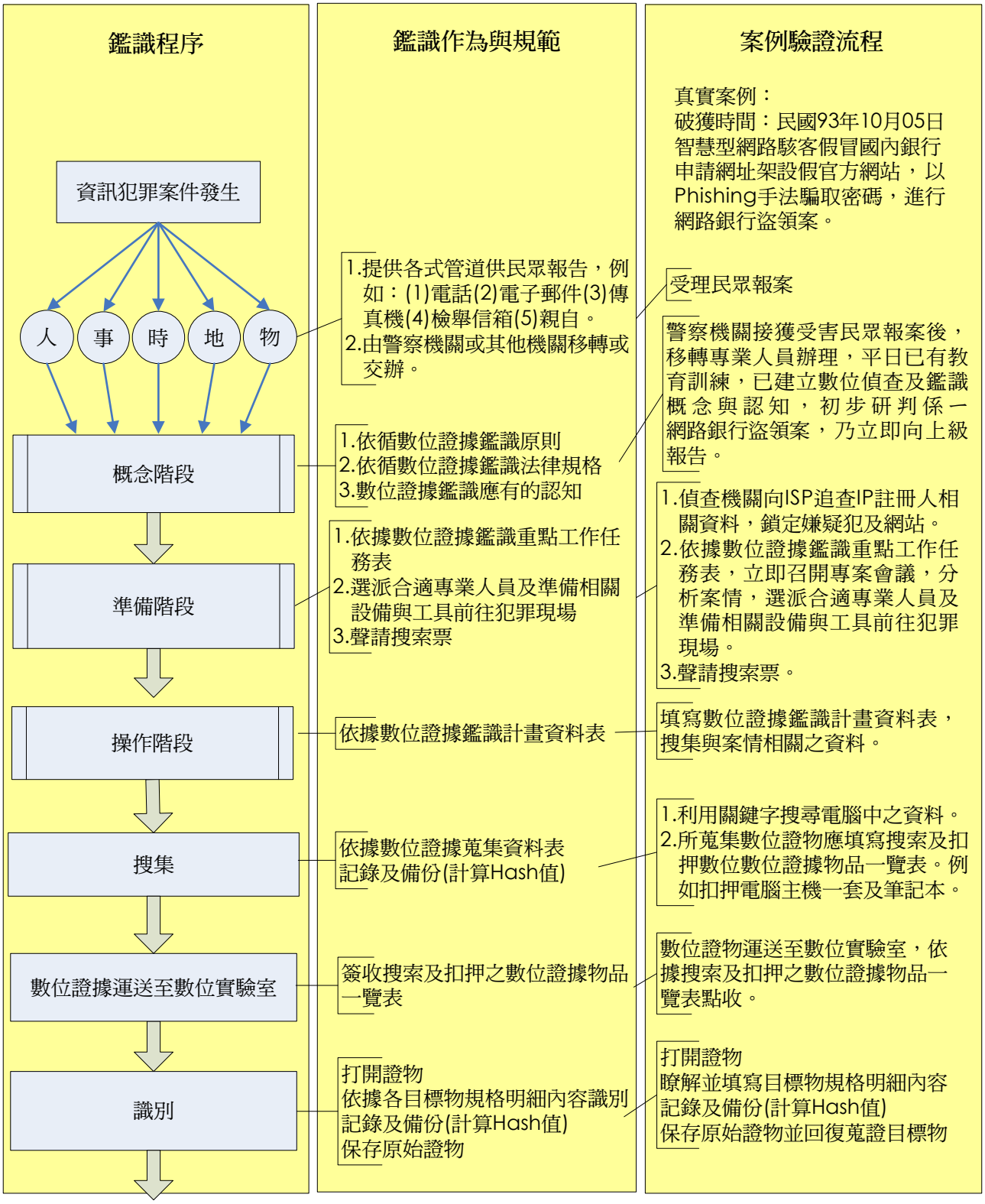
（承上頁）

圖4.1　類型一以網路空間為犯罪場所：以雅虎帳號拍賣92折中油油票涉嫌詐騙為例

二、案例二

再者介紹類型二以網路為犯罪工具，以　　例，如下圖4.2所示：

Phishing手法騙取密碼，進行網路銀行盜領案為



（接下頁）

（承上頁）

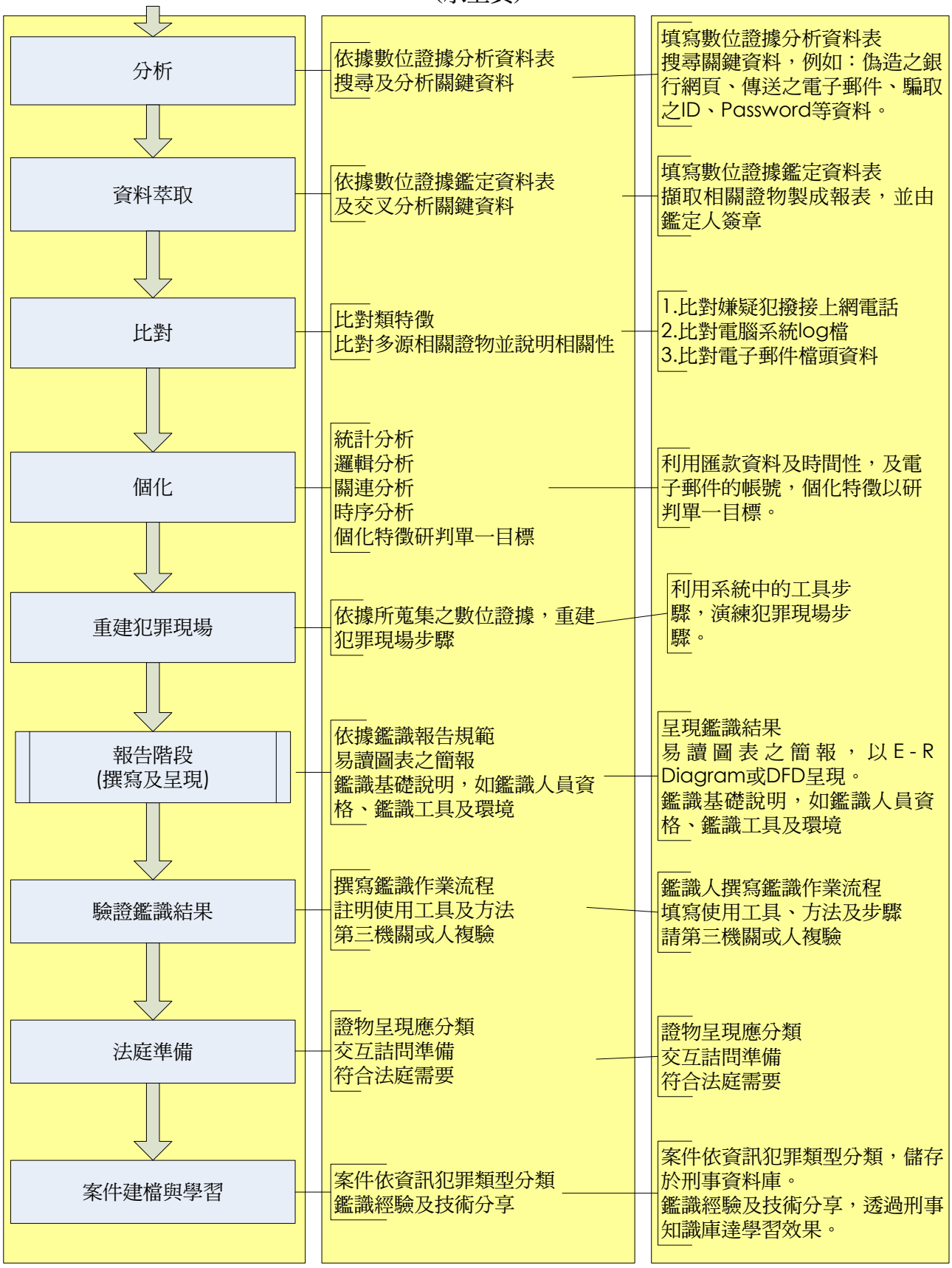
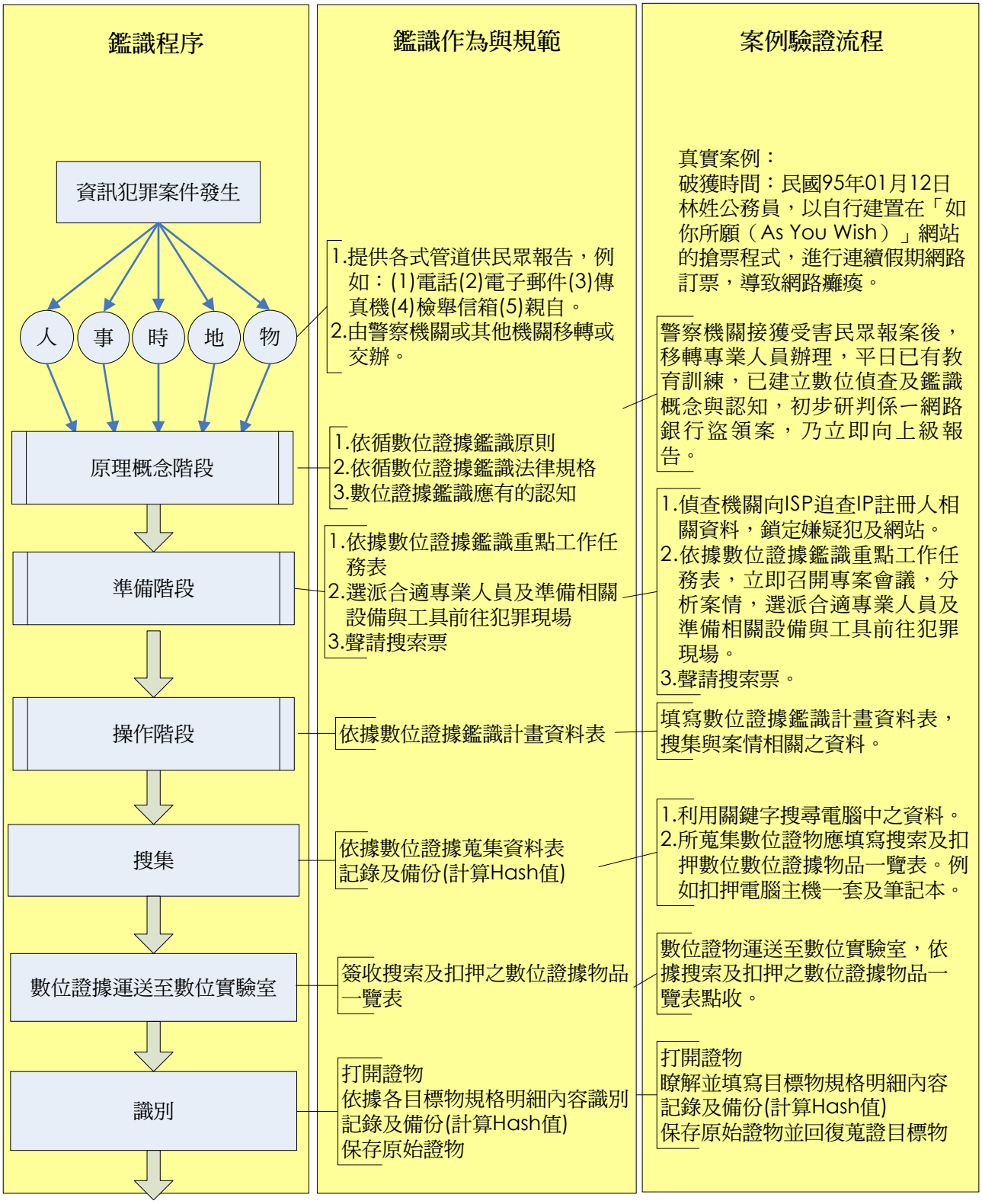


圖4.2　類型二以網路為犯罪工具：以Phishing手法騙取密碼進行網路銀行盜領案為例

三、案例三

最後介紹類型三以網路為犯罪客體，以網路入侵攻擊伺服器，使台鐵車票遭到網路搶光　　案為例，如下圖4.3所示：



（接下頁）

（承上頁）

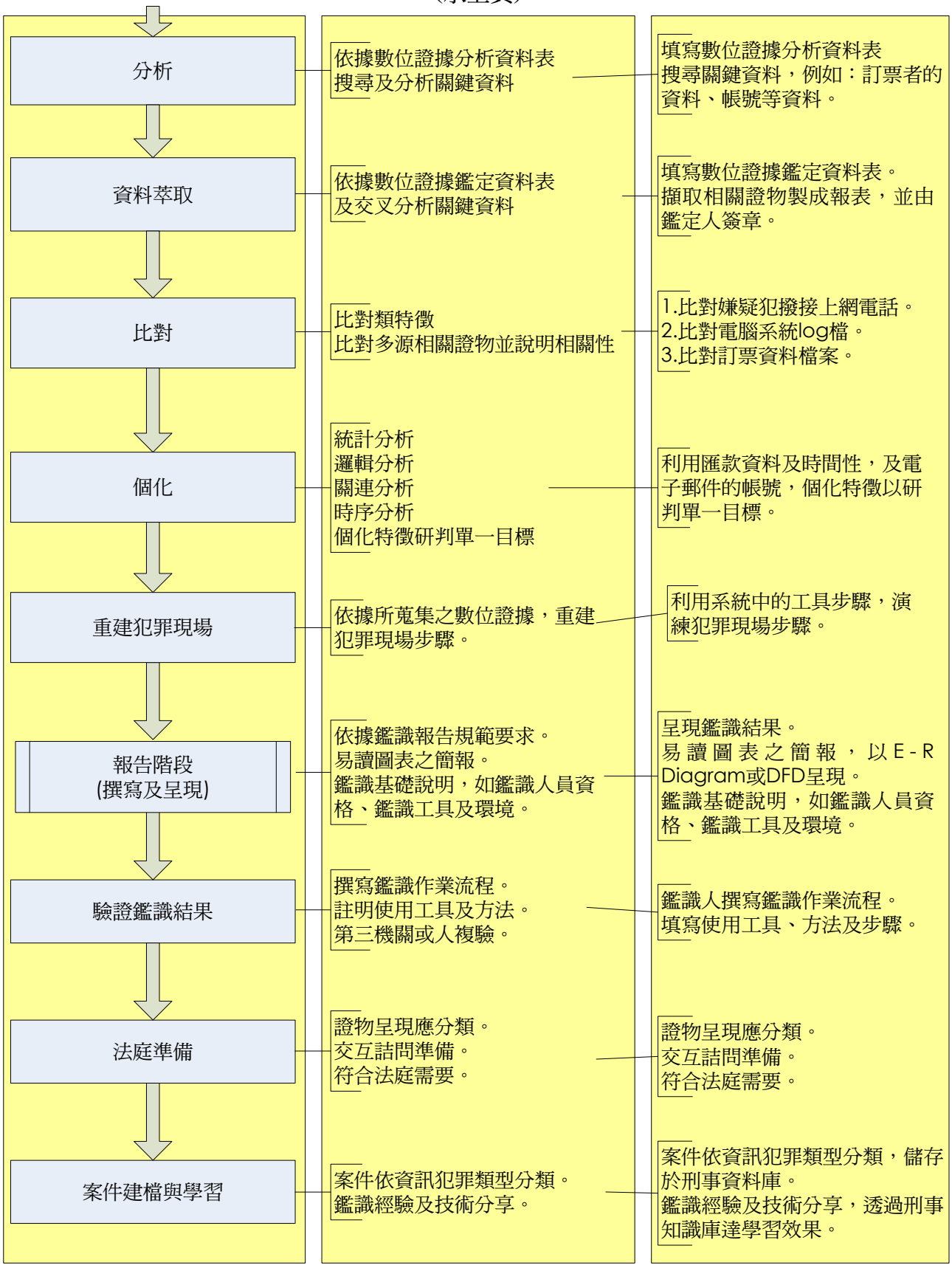


圖4.3　類型三以網路為犯罪客體：以網路入侵攻擊伺服器使臺鐵車票遭網路搶光案

伍、結論與建議

由於資訊犯罪問題日益嚴重，可預知數位證據鑑識機制在未來將影響甚大且重要，因此培養數位證據鑑識專業人才、建立數位鑑識作業規範及流程標準化（如DEFSOP），是現今刻不容緩的問題，應透過作業規範、流程及認證來加強鑑識結果及公信力，以強化司法鑑識單位之能力及法庭上公信力，再者也應瞭解數位證據的特性及其在證據法上的地位，讓其作業規範及流程能更契合證據法的需要，才能使數位證據增強其證據能力及證據證明力，也就是讓證據說話，並以案例實證檢驗本研究團隊多年研究提出數位證據鑑識標準作業程序之可行性及公信力。希望上述的探討能使政府、司法機關、專家學者及民間業者對此一議題之重視及相關單位作業時的重要參考依據及標準化。

最後本研究提出幾點之建議，一、國家應速建置數位鑑識實驗室（如調查局資安鑑識實驗室），二、數位鑑識相關之專業人才之培養，三、建立數位鑑識相關證照制度。四、建立數位鑑識相關程序（DEFSOP）與鑑識工具之標準化[14]。

參考文獻

1. 林宜隆，2007年，「數位證據標準作業程序（DEFSOP）之建構」，電腦稽核期刊，中華民國電腦稽核協會，第16期。

2. 蔡宜縉、林宜隆，2009年，「數位鑑識工具之比較研究——以Encase, FTK及Helix進行案例分析」，中央警察大學警學叢刊，第40卷第1期，頁231～250。

3. 李俊憶譯，2005年，李昌鈺刑事鑑定指導手冊（Henry Lee's Crime Scene Handbook），初版八刷。

4. 刑事鑑識規範，2002年，內政部警政署，台北市。

5. 余俊賢，2005年，數位鑑識的挑戰與發展，http://www.isecutech.com.tw/feature/view.asp?fid=540，最後瀏覽日：2006.02.03。

6. 林宜隆、閻瑣琳、陳受湛，2006，「我國資安鑑識實驗室建構與規劃之探討——以法務部調查局為例」，電腦稽核期刊，中華民國電腦稽核協會，第14期。

7. 楊鴻正，2002年，我國資通安全鑑識科技能量規劃之研究，中央警察大學資訊管理所論文，桃園縣。

8. 鄭進興、林敬皇、沈志昌，2003年，電腦鑑識方法與程序之研究，台灣網際網路研討會。

9. 蔡旻峰，2002年，電腦犯罪案件偵查中數位證據蒐證、鑑識之建議作業規範及流程，中央警察大學資訊管理學所研究碩士論文，桃園縣。

10.藍添興、林宜隆，2003年，數位證據蒐證程序之初探，第七屆資訊管理暨警政資訊實務研討會，中央警察大學，桃園。

11.蘇清偉，2001年，電腦犯罪之數位證據鑑識，刑事科學，內政部警政署刑事警察局，第51期，頁83。

12.警察犯罪偵查規範，1999年，內政部警政署，台北市。

13.李昌鈺，1997年，犯罪偵查與刑案現場重建，內政部警政署，台北。

14.李俊憶譯，2005年，李昌鈺刑事鑑定指導手冊（Henry Lee's Crime Scene Handbook），初版八刷，頁274-282。

15.U.S.Department of Justice, 1999, Forensic Examiniation of Digital Evidence: A Guide for Law Enforcement.

14 請參閱參考文獻2、6、10、16-20、30-34。

16.林宜隆、薛明杰，2010年，「我國資安鑑識人才規劃與驗證之研究」，電腦稽核期刊，中華民國電腦稽核協會，第21期。

17.林宜隆，楊鴻正，2005年，「各國資通安全鑑識技術能量之研究」，電腦稽核期刊，中華民國電腦稽核協會，第13期。

18.林宜隆、藍添興，2004年，「建構我國資通安全鑑識實驗室芻議之探討」，電腦稽核期刊，中華民國電腦稽核協會，第11期。

19.邱獻民、林宜隆，2007年，「數位證據在法庭上之攻防對策」，中央警察大學『資訊、科技與社會』學報，Vol.7 No.1 第12期。

20.林宜隆、邱獻民、呂芳懌，2010年，「數位證據同一性在法庭上之攻擊與防禦——以在網際網路蒐集之數位證據為中心」，中央警察大學學報，中央警察大學警察政策研究所，第47期，頁363～377。

21.林宜隆、顏雲生、吳柏霖、蕭勝方，2011年，VoIP攻擊分析與數位證據鑑識機制之研究，資訊管理學報，中華民國資訊管理學會。

22.Abe C. Lin, **I-Long Lin**,T. H. Lan ,Tzong-chen Wu, 2005, "Establishment of the Standard Operating Procedure (SOP) for Gathering Digital Evidence," Proceedings of the First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05).

23.**I-Long Lin**, Jack, 2005, "The Study on Constructing Digital Evidence Standard of Procedure," 2005 International Forensic Science Symposium ,Taipei,Taiwan.

24.**I-Long Lin**, Jack, 2005, "A Study on Planning Cybersecurity Professionals in Taiwan : Based on the Case of Cyber Forensic Professionals," 2005 International Forensic Science Symposium ,Taipei,Taiwan.

25.Yi-Chi Lin ,Jill Slay and **I-Long Lin**, 2008, "Computer forensics and Culture," Pacific Asia Workshop on Cybercrime and Computer Forensics at ISI 2008, Taipei-IEEE International Conference of Intelligence and Security Informatics, Taiwan.

26.**I-Long Lin**, Yen YS, Wu BL., 2009, "Analysis of VoIP security threat vulnerability and prevention policy," CISC 2009 Conference, Taipei,.

27.**I-Long Lin**, Yen YS, Wu PL., 2009,"Primary research on VoIP security threat vulnerability and attack prevention," ISMAD 2009, Taoyuan.

28.**I-Long Lin**, Yen YS, Wu BL, Yu CC., 2009, "VoIP security problem and digital forensics," Information management, practical application and talent nurturing conference, Taipei,.

29.**I-Long Lin**; 2009, "A Research of Cyber Security Forensic Mechanism in Taiwan," e-CASE 2009, in Singapore.

30.**I-Long Lin**, Yun-Sheng Yen, Bo-Lin Wu, and Hsiang-Yu Wang, 2010, "VoIP Network Forensic Analysis with Digital Evidence Procedure," NCM2010(IEEE) Proceeding, Seoul, Korea, August 16-18.

31.**I-Long Lin**, Yun-Sheng Yen, Bo-Lin Wu and Hsiang-Yu Wang, 2010,"VoIP Digital Evidence Forensics Standard Operating Procedure (DEFSOP)," The First International Workshop on Cloud, Wireless and e-Commerce Security (CWECS 2010), Fukuoka, Japan, November 4 - 6.

32.**I-Long Lin**, Chao Han-Chieh, Peng Shih-Hao, 2011, "Research of Digital Evidence Forensics Standard Operating Procedure with Comparison and Analysis Based on Smart Phone," 2011 International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA), pp.386-391.

33.**I-Long Lin** and Yun-Sheng Yen, 2011, "VoIP Digital Evidence Forensics Standard Operating Procedure", International Journal of

Research and Reviews in Computer Science (IJRRCS), Vol. 2, No. 1.

34.Yun-Sheng Yen, **I-Long Lin**, Bo-Lin Wua, 2011, "A study on the forensic mechanisms of VoIP attacks: Analysis and digital evidence", The Journal of Digital Investigation.

35.Eoghan Casey, 2004, Digital Evidence and Computer Crime ,Second Edition, forensic science, computer and the internet.