Procedure-oriented Laboratory of Digital Forensics in a Case Study

左瑞麟
政治大學資訊科學系
raylin@cs.nccu.edu.tw

許晉銘
政治大學資訊科學系
winterthink@gmail.com

高大宇*
中央警察大學資訊管理學系
* Correspondence: camel@mail.cpu.edu.tw

摘要

隨著通資訊設備普及，電腦犯罪及衍生的數位證據呈現爆炸式增長，網路使用者越來越關心資料保護及數位鑑識議題。數位鑑識作業包含多個階段程序，期從數位人為殘留跡證，判斷出適合解釋該犯罪事件的人、事、時、地、物之結論。本文針對數位鑑識實驗室的數位鑑識標準作業流程問題，描繪適合數位鑑識實驗室環境的架構，提高鑑識分析結果之可靠度。該有效的鑑識環境架構，提供數位鑑識分析人員值得信任的鑑識分析作業過程，構建合適、友善的基礎鑑識環境，提昇分析網路犯罪活動的效率。

關鍵詞: 數位鑑識、鑑識實驗室、數位鑑識標準流程

Abstract

The pervasion of ICT devices has led to an explosion of computer crime and digital evidence. Internet users are becoming increasing concerned with data protection and digital forensics. Digital forensics involves several steps, and determines the who, what, when, where, how and why of digital artifact activity. This paper presents a solution to the problem of standard operation procedure at digital forensic lab, outlines a framework for digital forensic investigation environment, and increases the reliability of the forensic attribution process. The effective of the framework environment will provide trusted digital forensics support to digital forensic investigators, enable them to establish their own forensics-friendly infrastructures, and help reduce the time and effort in analyzing criminal activities on the Internet.

Keywords: Digital Forensics, Digital Forensic Laboratory, Standard Operation Procedure

一、 前言

1991 年波特蘭的國際電腦專家協會(International Association of Computer Specialists，IACIS) 首次出現電腦鑑識這個名詞，隨著資訊時代的快速演進，電腦鑑識不單侷限在個人電腦。任何對案件有幫助的檔案甚至隻字片語，都有可能影響數位鑑識專案之分析結果，這些線索、證據常存在於龐大容量硬碟中的某一檔案、剩餘空間(File Slack)或未分配空間(Unallocated area)之中[24]，數位鑑識人員須透過適當的處理程序，妥善操作技術工具，才能完成數位鑑識的時間性、功能性或關聯性等分析作業。若技術工具功能不足或流程錯誤，將錯失重要證據並影響鑑識分析結果，甚或導致該案件證據不足，而無法釐清責任歸屬[12]。數位鑑識人員面對各式各樣鑑識工具及實驗室設備，須遵循符合規範的鑑識分析流程，完成鑑識作業。回顧國內外探討數位鑑識程序或模型文獻[7][8][14][19][20]，多僅摘述數位鑑識程序，未詳細說明各程序之實際操作細節。實際執行數位鑑識作業地點可劃分為鑑識實驗室及蒐證現場，數位鑑識人員需瞭解不同地點所應執行之作業內容及注意要點。本文以實務經驗為基礎，重新構建數位鑑識作業程序及鑑識實驗室應有組成元件，並提出初步鑑識分析應有標的，供數位鑑識人員作為分析依據。

本文將於第二節探討數位鑑識相關文獻，如數位證據及數位鑑識國際標準等。第三節提出程序處理導向數位鑑識實驗室的組成元件，界定實驗室人員組織架構與職掌。第四節為數位鑑識作業處理流程，第五節透過模擬案例說明各項處理作業之實際應用。第六節為本文結論。

二、 文獻探討

本節將探討數位證據、數位鑑識及國際標準等相關文獻，包含數位鑑識標準作業程序及數位鑑識實驗室國際規範，藉以說明數位鑑識現況，作為本文基礎。

1. 數位證據

隨著資訊電子產品大量普及，電子犯罪事件日益頻繁，學者Casey[12]定義數位證據係指能夠證明犯罪或提供案件相關線索之任何數位資料。國際規範中，SWGDE(Scientific Working Group on Digital Evidence)定義數位證據為任何具證明犯罪案件價值之儲存或傳送數位資料[27]；ISO/IEC 27043: 2015[19]定義為以二進制儲存或傳輸且可被認可為證據之資訊或檔案。簡言之，數位證據為數位資訊媒體中所存在之電磁紀錄，該電磁紀錄可提供案件相關證明。我國刑法第十條第六項，定義電磁紀錄為：「以電子、磁性、光學或其他相類似方式所製成，而供電腦處理之紀錄，稱為電磁紀錄」。Casey亦提出數位證據四種特性[12]：

(1) 數位證據蒐集和處理相當困難，只有少部份可成為證據。
(2) 無法直接以人的知覺瞭解內容。
(3) 易於複製與修改，不易保留原始狀態。
(4) 不易證實來源及完整性。

由於上述數位證據特性，數位證據的取得和保存為數位鑑識的重要一部分，數位鑑識人員需有專業數位證據認知，能善用軟硬體資源，提供完整的、正確的數位證據。數位鑑識實驗室檢查人員於蒐集數位證物時，須遵守下列基本原則 [21]：

(1) 不異動數位證據之情況下取得數位證據內容。

(2) 鑑識分析後須證明所擷取之數據來源始於該數位證據。

(3) 不異動數位證據內容情況下，進行鑑識分析作業。

第一項原則亦即數位鑑識人員取得數位證據過程中不能破壞證據能力，否則將導致該證據無法被法院採信。台灣高等法院台南分院刑事判決100年度上訴字第228號案例為例，該案告訴人將數位證據自行儲存於光碟後，交予數位鑑識人員進行鑑識分析，但儲存方式已異動該數位證據之最後修改時間，致數位鑑識人員不願意鑑定該證據內容。第二項原則亦即數位證據第二種特性：不易證實其來源及完整性。數位證據易於複製與修改，數位鑑識人員須於呈現鑑識分析成果前，佐證相關數位證據與原始證物相同。第三項原則常發生於不適用數位鑑識工具或錯誤數位鑑識作業程序。

2. 數位鑑識

傳統刑事案件涉及刑事鑑識學，涵蓋彈道學、血液學等，發展較早且可供參考，隨著資訊科技發達，數位鑑識為取得、妥善保存及分析數位證據而衍生之專門領域。學者Solms及Lourens[25]定義數位鑑識為「為分析及調查技巧，用以保存、識別、擷取、文件化及分析儲存媒體中之證據或根因分析」，此類型調查作業將協助法院處理電腦及網路犯罪案件或企業內部調查[18]。學者Kuchta[22]則對數位鑑識定義為「數位鑑識是電腦應用的法律議題，使用電腦技術針對電子儲存媒體之數位證據，進行擷取及分析說明，進而取得法律上的效力」。由此可知，數位鑑識作業因案件需進入司法訴訟程序，或數位鑑識作業結果將用於釐清責任、究責等，成為關鍵重點。

有別於鑑識傳統刑事案件，數位鑑識可分為電腦鑑識、行動裝置鑑識、網路鑑識、資料庫鑑識、多媒體鑑識、屬於新興科技之雲端鑑識[15]及物聯網(Internet of Thing, IOT)鑑識等領域。若以分析標的劃分，分為如惡意程式鑑識、即時通訊鑑識、檔案系統鑑識及電子郵件鑑識等項目。為因應各種不同數位鑑識作業，鑑識分析人員需在可信賴且完善數位鑑識設備環境，透過標準作業程序，產出可被信任的數位鑑識結果分析報告。

3.國際標準

執行資安事件的數位鑑識作業時包含擷取、封存及分析等步驟，需符合正當的法律程序及相關規範，確保鑑識人員取得的數位證據，具備證據能力[11]，鑑識人員應清楚認知完整鑑識程序及各階段作業注意要點。電腦鑑識基本程序[4]，自鑑識人員抵達犯罪現場開始，包含現場保全與評估、現場文件紀錄、證據蒐集、證據封存及數位證據檢驗，共五個步驟，如圖1：

圖1：電腦鑑識之基本程序圖

根據NIST(The National Institute of Standards and Technology)定義數位鑑識程序，包含收集(Collection)、檢驗(Examination)、分析(Analysis)及報告(Reporting)，說明如下[20]：

(1) 收集：針對所有數位證據進行識別、標示、紀錄及擷取。
(2) 檢驗：結合特定數位鑑識工具或手動方式，針對大量數位證據進行數位鑑識相關檢驗。
(3) 分析：使用合法合理的方法與技術，分析自收集及檢驗步驟取得之數位證據，產出可用訊息。
(4) 報告：最後階段將報告分析結果，並說明分析操作流程、工具及程序等內容。

國際標準化組織(International Organization for Standardization, ISO) 與國際電氣技術委員會(International Electrotechnical Commission, IEC)共同提出ISO/IEC 27043: 2015[19]，說明數位鑑識作業應包括準備(Readiness)、起始(Initialization)、擷取(Acquisitive)及調查(Investigative)等階段，作為資訊安全事件調查過程，進行數位鑑識作業依循的標準與建議，確保取得數位證據具備證據能力。該組織亦針對所有測試與校正實驗室能力之共同要求制定ISO/IEC 17025:2005[3]，用於提高實驗室品質、技術及一般行政作業水準，藉由標準流程規範等方式，確保實驗室產出報告，符合國際規範及法律訴訟要求。美國司法部(National Institute of Justice, NIJ)為了協助高科技犯罪案件偵查作業並建立數位鑑識能量，以利於法庭上提出數位證據，制定「Forensic Examination of Digital Evidence A Guide for Law Enforcement」[9]，作為美國司法或警政單位電腦鑑識指導原則，說明數位鑑識作業程序應包括資料蒐集 (Data Collection)、檢核(Examination)、分析(Analysis)及報告(Reporting)。

4. 文獻比較

鑑識作業流程可分為「準備(Readiness)」、「起始(Initialization) 」、「現場保全(Securing the Scene) 」、「文件紀錄(Documentation) 」、「識別(Identification) 」、「收集(Collection)、「擷取(Acquisitive) 」、「保存(Preservation) 」、「檢核(Examination) 」、「分析(Analysis) 」及「報告(Reporting)」等11種鑑識作業項目，歸納比較後如表1[4][7][9][19][20][25][29]。針對鑑識分析標的，各文獻所提出鑑識人員應著重分析標的資料亦有不同，歸納比較後如表2[7][9][10][11][17][28]。

表1：鑑識作業項目比較表

鑑識作業項目	Agarwal et al. [7]	Ashcroft et al. [9]	ISO/IEC 27043 [19]	Kent et al. [20]	Smutny [25]	Yusoff et al. [29]	黃嘉宏等人 [4]	我們的方法
準備	V	N/A	V	N/A	N/A	N/A	N/A	V
起始	V	N/A	V	N/A	N/A	N/A	N/A	V
現場保全	V	N/A	N/A	N/A	N/A	N/A	V	V
文件紀錄	V	N/A	N/A	N/A	N/A	N/A	V	V
識別	N/A	N/A	N/A	N/A	V	N/A	N/A	V
收集	V	N/A	N/A	N/A	V	N/A	V	V
擷取	V	V	V	V	V	V	V	V
保存	N/A	N/A	N/A	N/A	V	N/A	N/A	V
檢核	V	V	N/A	V	N/A	V	V	V
分析	V	V	N/A	V	N/A	V	N/A	V
報告	V	V	V	V	N/A	V	N/A	V

註：符號 “ V”表示保有該項功能/特質

表2：鑑識分析標的比較表

鑑識分析標的	Agarwal et al. [7]	Ashcroft et al. [9]	Blackwell et al. [10]	Carvey, H. [11]	Fenu and Solinas [17]	Yang and Yang [28]	我們的方法
回復硬碟磁區及資料夾	N/A	N/A	N/A	N/A	V	N/A	V
雜湊值比對	N/A	V	V	V	V	V	V
關鍵字搜尋	N/A	N/A	N/A	N/A	N/A	N/A	V
特徵值分析	V	N/A	N/A	N/A	N/A	N/A	V
日誌檔案	N/A	N/A	V	N/A	V	N/A	V
電子郵件	V	N/A	N/A	V	V	N/A	V
檢查系統帳號	N/A	N/A	N/A	N/A	N/A	N/A	V
在未分配區域搜尋檔案	N/A	N/A	N/A	N/A	V	N/A	V
案件時間軸	V	N/A	N/A	N/A	N/A	N/A	V

註：符號 “ V”表示保有該項功能/特質

三、程序處理導向的數位鑑識實驗室

鑑於數位證據特性及數位鑑識標準作業重要性，作為主要鑑識分析場所的數位鑑識實驗室，需結合相關國際規範並明確定義其構成要素、人員架構職掌、各分區環境設備需求及作業注意要點等重要項目，保障數位證據之證據能力、提高案件處理效率，減少發生錯誤可能性。

1.構成要素

歸納數位鑑識實驗室主要構成內涵，如圖2[8][26][29]：

(1) 軟硬體設備：包含實驗室內軟硬體含網路等設備，處理或分析數位證據過程，應使用含有防寫功能(Write Block)及通過NIST之電腦鑑識工具測試(Computer Forensic Tool Testing, CFTT)[23]計畫檢驗之鑑識工具[16]。

(2) 實驗室認證及規範：規範鑑識實驗室之設備使用、人員進出、保固維護等相關文件，明定應遵循標準及管理制度。

(3) 組織架構與職掌：記錄實驗室成員及其職掌，規定每個角色應具備技術能力與固定應接受教育訓練及合格標準。

(4) 標準作業流程：根據該實驗室主要鑑定項目制定標準作業流程，包含各項軟硬體設備標準操作手冊。

(5) 環境規劃：除特定區域供鑑識分析人員便於操作工具外，證物保管區設定特殊存取權限，確保實驗室各項安全性需求合於規範[16]。

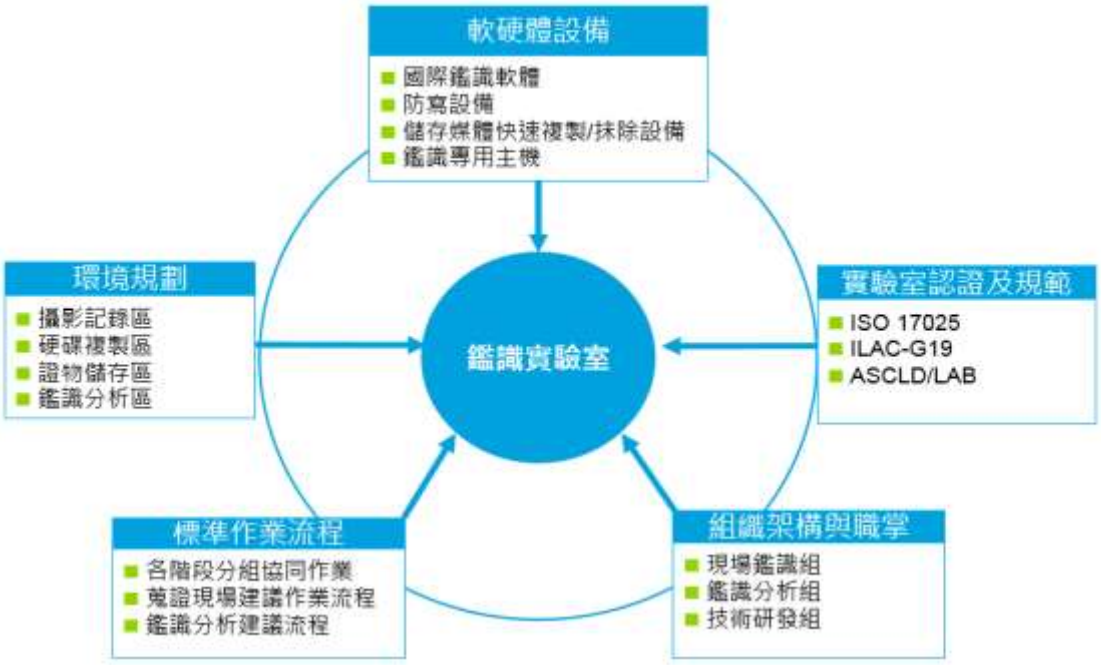


圖2：鑑識實驗室構成要素

2.人員架構及職掌

國內外數位鑑識實驗室多僅區分外勤及鑑識分析人員，應細分為學術研究組、電腦鑑識組及技術研發組 [1]，或分為技術研發小組、網路鑑識組、電腦鑑識組及手機鑑識組[2]。本文建議，分為現場鑑識組、鑑識分析組及技術研發組，如圖3，職掌說明如下：

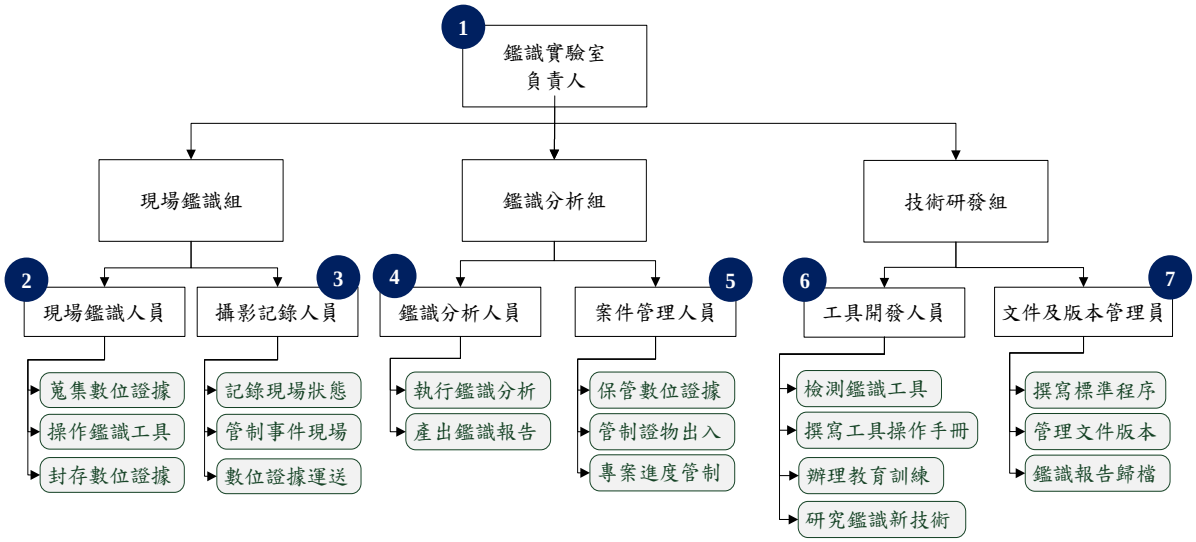


圖3：鑑識實驗室人員架構及職掌建議

(1) 現場鑑識組

A. 鑑識實驗室負責人：確認案件鑑識方向及各項資源調度事宜，案件偵結時，簽署鑑識報告並召開結案會議。

B. 現場鑑識人員：須熟悉相關現場鑑識工具及相關作業程序要求，負責數位證據蒐集及封存作業。

C. 攝影記錄人員：負責管制事件現場，確保現場除現場鑑識人員外，沒有未經授權人員進出現場。將現場所有狀態透過錄影、拍照或紙本等方式予以記錄，包含現場中相關標的設備與數位證據所在位置，電腦設備、週邊設備、可攜式儲存媒體及網路等連接方式。

(2) 鑑識分析組

A. 鑑識分析人員：負責執行鑑識分析作業負責製作鑑識分析報告。

B. 案件管理人員：保管數位證據，確保數位證據收件管制、入庫保存、調閱歸還及出庫流程皆有詳細、正確紀錄。

(3) 技術研發組

A. 工具開發人員：依據鑑識分析需求開發相關工具，撰寫或更新數位鑑識工具操作手冊。辦理教育訓練，講解鑑識工具功能及操作方式，使現場鑑識人員及鑑識分析人員能熟練並運用於鑑識作業。

B. 文件及版本管理員：管理數位鑑識作業所需文件及表單，若需修改文件或表單內容，由版本管理員統一更新並交付技術研發主管發布。於專案結束後將鑑識報告歸檔並保妥善保存。

3.環境需求

當實驗室取得數位證物後，鑑識分析人員須按照實驗室規範製作數位證物複本，供後續鑑識分析使用。基於數位證物易於被破壞特性，鑑識分析人員需以數位鑑識專用硬碟複製機應將來源數位證物(Source)複製至已完全抹除(Wipe)之另一空白證物硬碟中，最後將複製完成的數位證據複本(Clone)再製作出供後續鑑識分析作業之證據映像檔(Image)。待複製完成並確認複製工具無錯誤訊息後，將來源數位證據及數位證據複本妥善封存至證物儲存區。因證據映像檔皆有雜湊值及循環冗餘校驗(Cyclic redundancy check, CRC)，可確保鑑識分析作業不會影響到數位證據資料，鑑識分析人員須以證據映像檔(Image)為主要分析標的。圖4為鑑識實驗室各區域作業內容及說明[2][3][6][13]：

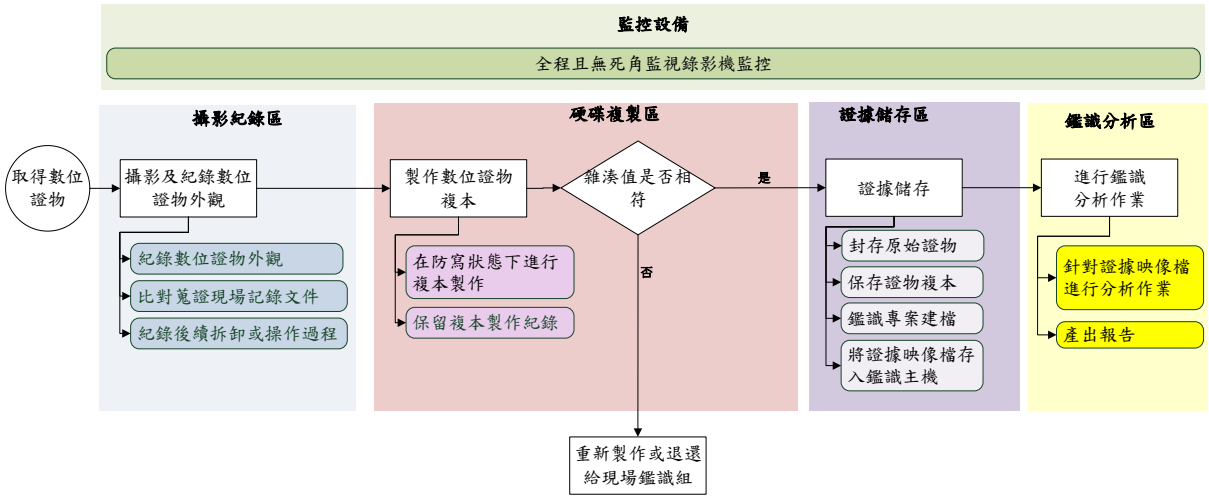


圖4：鑑識實驗室各區域作業內容

(1) 攝影紀錄區：腳架和攝影機為主要記錄工具，數位相機及訪談紀錄為輔，充分記錄證物狀態，記錄後續拆卸或操作過程。當現場鑑識組將數位證物送抵實驗室時，鑑識分析人員須當面確認數位證物封存狀況，若封口或包裝有破損或破壞痕跡，應立即記錄並與現場鑑識組確認該情況是否異常。

(2) 硬碟複製區：位元串流複製方式(Bit-Stream Duplicate)，透過防寫設備或快速複製設備製作映像檔或複製證物，製作完成後比對雜湊值是否相同及是否有錯誤訊息，記錄於表單。若現場鑑識人員於蒐證現場完成複本或證據映像檔製作，鑑識分析人員須於本區進行重複核對雜湊值。

(3) 證物封存區：完成證物複本或映像檔製作後，須進行文件建檔及封存來源數位證物及數位證據複本。

(4) 證物儲存區：本區應與上述各區做實體區隔，妥善執行管制人員進出及存取權限等保護措施。

(5) 鑑識分析區：應有專門鑑識分析電腦主機，安裝通過國際檢測機構之鑑識分析工具。本區設備須使用獨立內部鑑識網路或停用網路，隔絕外部網路連結。

四、數位鑑識作業處理

數位鑑識處理作業可分為蒐證現場作業流程和鑑識分析流程。現場鑑識人員若於蒐證現場遭遇無法處理情況時，應詢問現場鑑識主管因應策略，避免毀損數位證物。以下討論現場蒐證的前置準備、作業流程和實驗室的分析流程。

1.現場蒐證的前置準備

鑑識實驗室接獲出勤需求，進入準備階段[7]，召開勤前會議，說明案件相關資訊、確定案件管理人等職務，本文提出於現場作業前置準備階段應檢查及準備項目，如圖5：

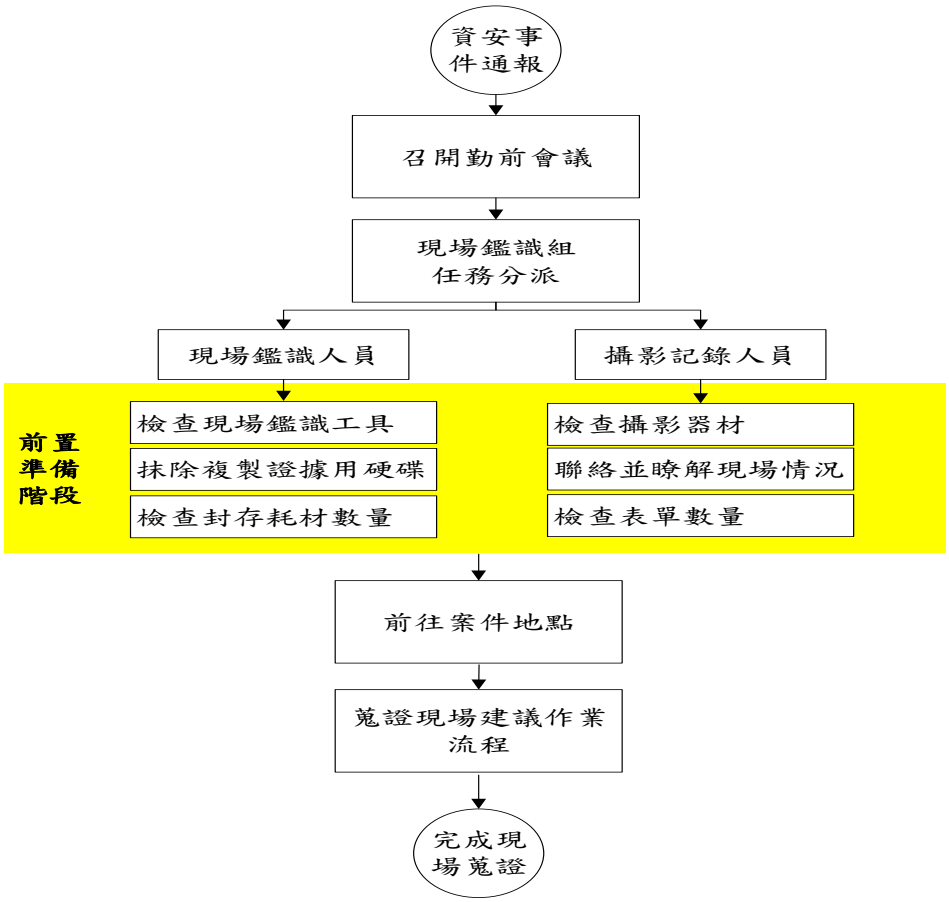


圖5：現場蒐證作業前置準備階段任務內容

(1) 現場鑑識人員：

A. 檢查現場鑑識工具：重新操作與現場蒐證作業相關功能，記錄結果於表單中。

B. 抹除複製證據用硬碟：現場鑑識人員須確認目標主機硬碟容量，準備合適容量硬碟，完整抹除該硬碟資料。

C. 檢查封存耗材數量：現場鑑識人員須根據已知案件資訊，領取所需耗材並確認數量足夠。

(2) 攝影記錄人員：

A. 檢查攝影器材：檢查攝影器材電池電力及儲存空間是否足夠。

B. 聯絡並瞭解現場情況：攝影記錄人員應聯絡案件聯絡窗口，瞭解現場情況並將該訪談資訊記錄於表單中。

C. 檢查表單數量：前往案件現場前，攝影記錄人員應確認所攜帶表單數量足夠使用。

2.蒐證現場的作業流程

蒐證現場建議作業流程如圖6，現場鑑識人員可考量現場環境及鑑識設備，採取適當方法完成蒐證作業[7][13][22][28][25]。

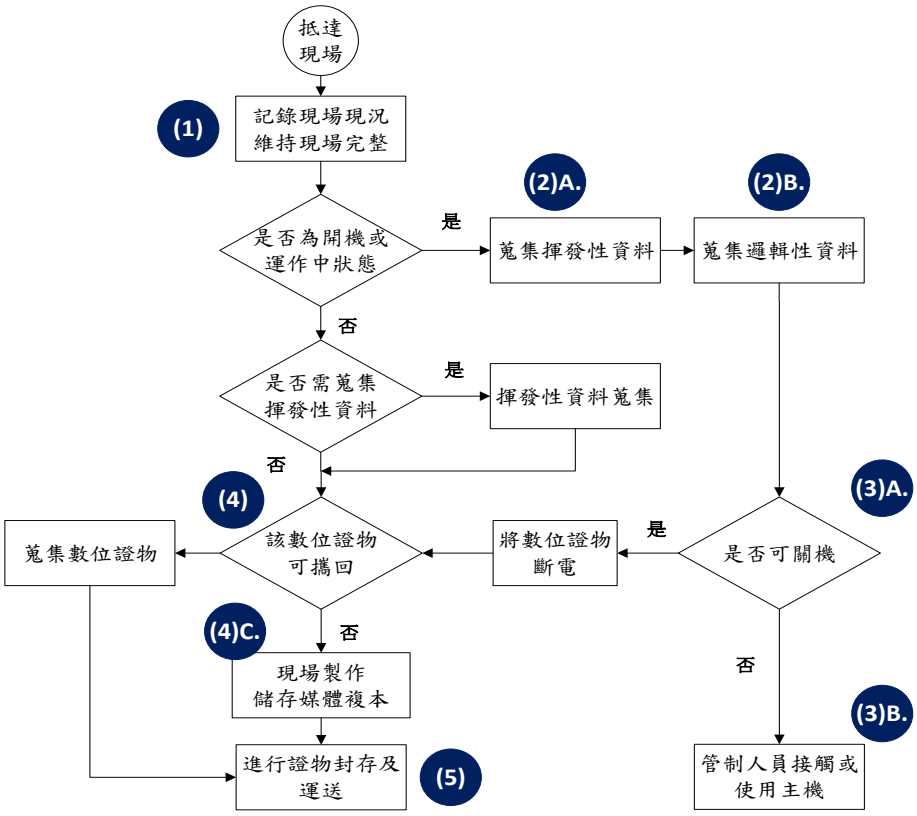


圖6：蒐證現場建議作業流程圖

(1) 現場保全

A. 記錄現場現況：攝影記錄人員應透過錄影記錄，藉此說明動作前後關係；可輔以使用拍照方式，記錄設備序號或外觀等靜態畫面[7]。

B. 維護現場完整

(A) 攝影記錄人員應要求案件現場相關人員，維持數位證物原始狀態。

(B) 攝影記錄人員應協助管制事件現場，針對數位證物週遭人員進行清場，描述管制現場之人員進出緣由。

(2) 現場資料蒐集

A. 揮發性資料蒐集

(A) 如數位證物處於開機狀態，現場鑑識人員應識別揮發性資料種類，使用現場數位證據蒐集工具盡可能取得揮發性資料[7][28]，舉例如表3[11]

表3：揮發性資料種類

	揮發性資料種類	揮發性資料內容
1	作業系統	目前登入之使用者
2		執行中程式資訊
3		已啟動服務
4		已開啟之檔案
5	網路	已開啟之網路連線埠
6		程式所建立網路連線資訊
7	記憶體	記憶體資料及分頁檔

(B) 進行揮發性資料蒐集時，現場鑑識人員應透過工具自動執行蒐證作業，避免人為操作錯誤，導致證據能力遭到質疑。

(C) 揮發性資料蒐集完畢後，現場鑑識人員應取得其對應之雜湊運算值，作為後續比對檔案完整性依據。

(D) 進行揮發性資料蒐集作業時，應對於所採取的每一個動作都必須能解釋其動機、目的與關聯性並紀錄操作步驟。

(E) 攝影記錄人員應以錄影方式記錄現場蒐證方法及步驟。

B. 非揮發性資料蒐集：若標的主機開機運作中，為避免關機或重新開機後，造成證據檔案因各種反鑑識 (Anti-Forensics)手法而毀損，應於揮發性資料蒐集結束後，進行非揮發性資料蒐集[7]，惟蒐集範圍將因案件不同而異，現場鑑識人員需依照案件需求進行識別及擷取。

(3) 開機狀態下是否攜回數位證物

A. 若該數位證物處於開機狀態，現場鑑識人員須詢問該設備負責人，判斷是否可以關閉電源並攜回。作業系統正常關機程序可能會導致部份證據被異動[19]。

B. 待所有蒐證程序完成且無法關機攜回數位證物時，應避免未經授權人員再操作或使用該主機。

(4) 關機狀態下數位證據是否可攜回

A. 現場鑑識人員應詢問相關人員，判斷是否可攜回儲存媒體或完整資訊設備。

B. 攝影記錄人員應錄影記錄儲存媒體取出步驟，拍照記錄型號序號等資訊。

C. 現場製作儲存媒體複本

(A) 如不能將其儲存媒體攜出數位證物時，現場鑑識人員應直接於現場透過儲存媒體，複製設備製作儲存媒體複本[17][25]。

(B) 攝影記錄人員應以錄影方式記錄儲存媒體複本製作步驟

(C) 複本製作完畢後，應產出其雜湊運算值，作為後續比對檔案完整性依據。

(5) 證據封存及運送

A. 現場鑑識人員應確實清點數位證物項目及數量，並提供證據監管鏈表單，請相關單位或證物所有人簽章。

B. 封存方式應考量運送過程，避免影響或異動該數位證物內容[7][25][29]，確保外觀標示清楚。

C. 攝影記錄人員應將要封存之數位證據及封存步驟進行錄影拍攝作業。

D. 攝影記錄人員應確保運送過程中，不會對數位證據造成損害，另應注意證據監管鏈之完整性[14]，若有必要可記錄全部運送過程。

3.實驗室的分析流程

鑑識分析作業因各專案不同，無法定義完整之標準作業流程，本文提出鑑識分析流程，如圖7[7][9][17]：

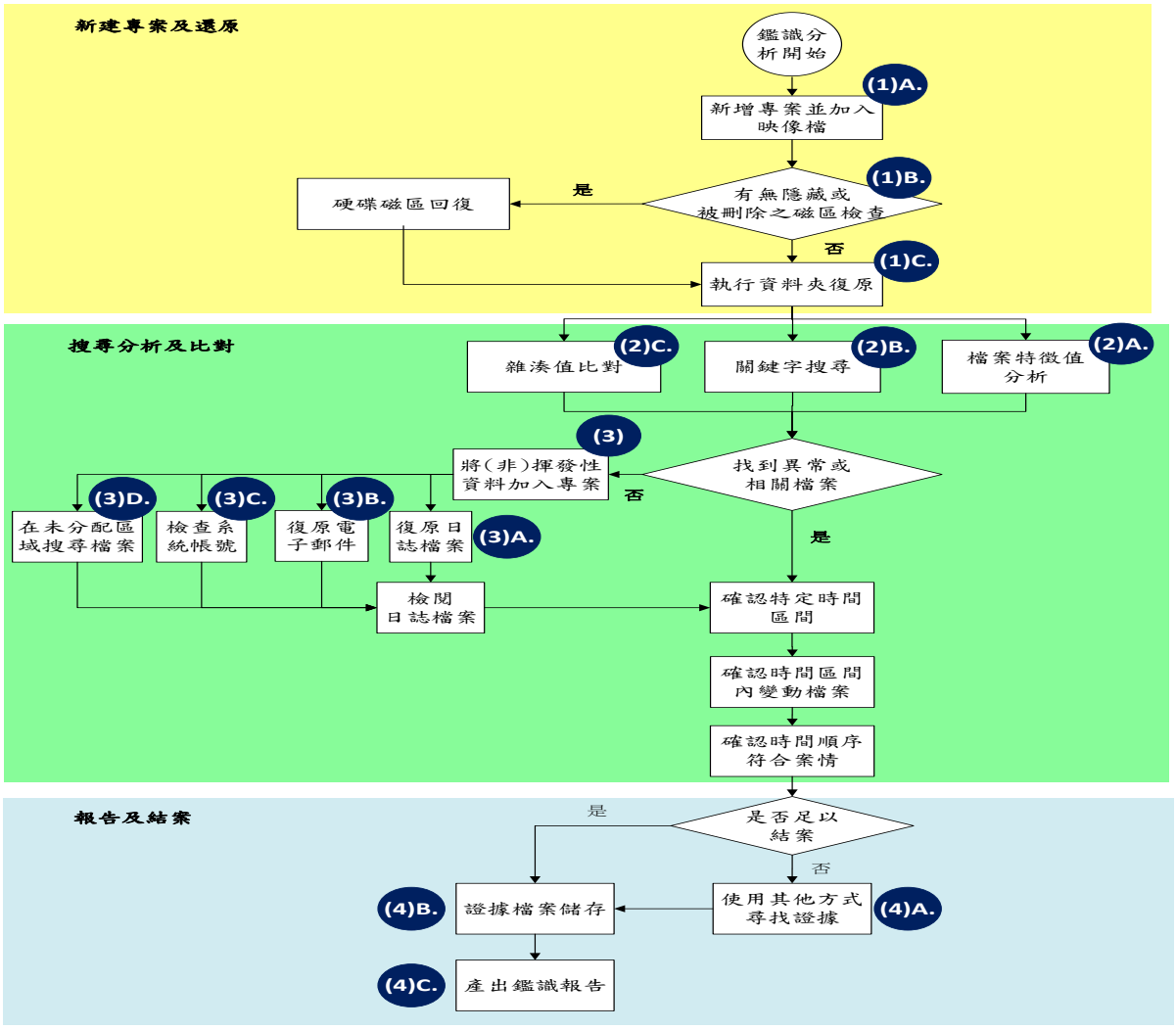


圖7：鑑識分析作業流程

(1) 新建專案及還原

A. 新增專案並加入映像檔：鑑識分析人員應根據專案不同建立新專案，專案名稱須與案件相關連，加註日期及證據編號，避免使用流水號等無意義名稱。

B. 檢查隱藏或刪除磁區：鑑識分析人員應透過鑑識分析軟體，還原任何被隱藏或被刪除之邏輯硬碟磁區[17]，如發現有大量空間未被分配，可進一步確認是否有主要硬碟磁區被隱藏或被刪除。若有則應立即復原，避免遺漏任何相關資料。

C. 執行資料夾復原：為防止資料夾於鑑識分析軟體預覽模式下被隱藏或被覆蓋，鑑識分析人員應於確認硬碟是否有隱藏或刪除磁區後執行此作業，以利後續比對分析作業進行。

(2) 搜尋分析及比對

A. 檔案特徵值分析：鑑識分析人員應判斷主機是否有任何意圖隱藏而變更副檔名之檔案。

B. 關鍵字搜尋：如分析作業執行尚未確定關鍵字，鑑識分析人員可依據案件屬性及現場訪談資料，進行特定類別之關鍵字搜尋。

C. 雜湊值比對：鑑識分析人員如能取得部份證據檔案並算出雜湊值，可透過雜湊值比對，過濾檔案[9][10][17][28]，縮短鑑識流程。

(3) 如未能發現異常或相關檔案，應將現場取得之(非)揮發性資料加入專案，執行進階分析。透過重建現場數位證物之狀態，將有助於案件分析。

A. 復原日誌檔案：若日誌檔案有遭異動跡象，須復原日誌檔案[10]後檢閱是否有異常行為。

B. 復原所有電子郵件：電子郵件為資安事件中常見分析標的[11][17]，鑑識分析人員可檢閱電子郵件附件是否有可疑資料。

C. 檢查系統帳號:鑑識分析人員須檢查系統內是否有非法建立帳號及其時間點。

D. 在未分配區域搜尋檔案[17]：若無法藉由前述步驟找到異常或與該案件相關檔案，鑑識分析人員須執行未分配區域檔案搜尋，找出被刪除之資料。

(4) 報告及結案

A. 使用其他方式尋找證據：鑑識案件經過上述步驟若仍未能取得足以結案之數位證據，鑑識分析人員可依特定案件類型採用其他進階鑑識分析功能。

B. 證據檔案儲存：鑑識分析人員應將證據檔案及鑑識分析結果，使用光碟機燒錄或其他不可修改存檔方式進行保存，並將其雜湊運算值一併存放。

C. 產出數位鑑識報告：鑑識分析人員應附加鑑識過程所相關紀錄作為鑑識報告附件，佐證數位鑑識報告所述資訊[12]。

五、 模擬案例分析

將透過模擬資料外洩案例，應用本文提出之標準作業流程進行鑑識分析，說明各步驟作法及發現之數位證據。

1.模擬案例說明

員工A是某公司的資訊人員，因不滿同一部門的員工B因裙帶關係迅速升遷，憤而竊取員工B電腦中之機房機敏資料，造成資料外洩事件，企圖使員工B遭到懲處。公司收到客戶投訴後發現已有部份機房檔案被公開於網路上，該檔案屬於員工B之業務範圍，懷疑有機敏資料自員工B電腦外洩，請鑑識人員進行蒐證及調查。由現場鑑識人員及攝影記錄人員組成之現場鑑識組，在員工B的主管陪同下，抵達員工B電腦所在位置時，依照現場蒐證程序，首先記錄員工B電腦及其位置週邊狀態，管制人員進出維持現場完整。現場鑑識人員當場製作儲存媒體複本，進行後續鑑識分析作業。

2.數位鑑識作業處理流程

鑑識分析人員取得員工B硬碟之證據映像檔後，依照鑑識分析作業流程針對資料外洩案件中需分析之竊取來源、使用工具、洩漏途徑及內容，進行下列作業：

(1) 【步驟 1】：檢查並復原磁區及資料夾

檢視員工B電腦硬碟中之MBR(Master Boot Recode)位置後發現於未分配空間中有VBR(Volume Boot Recode)之關鍵字「NTFS」，鑑識人員研判其為手動刪除磁區之現象 (如圖8)。原先員工C電腦中僅有「C」、「D」兩個磁碟分區(如圖9-1)，針對被刪除磁區進行還原後可得另一磁區，該磁區位於原先磁區「D」之前，鑑識軟體重新排序及標示該遭刪除磁區為「D」，自動將原先為「D」之磁區改為「E」(如圖9-2)，該遭刪除之磁區「D」中含有大量被刪除資料。針對所有磁區執行資料夾復原作業後可得共有72,579個資料夾被還原，鑑識人員後續即可針對所有邏輯檔案進行特徵值比對(如圖10)。

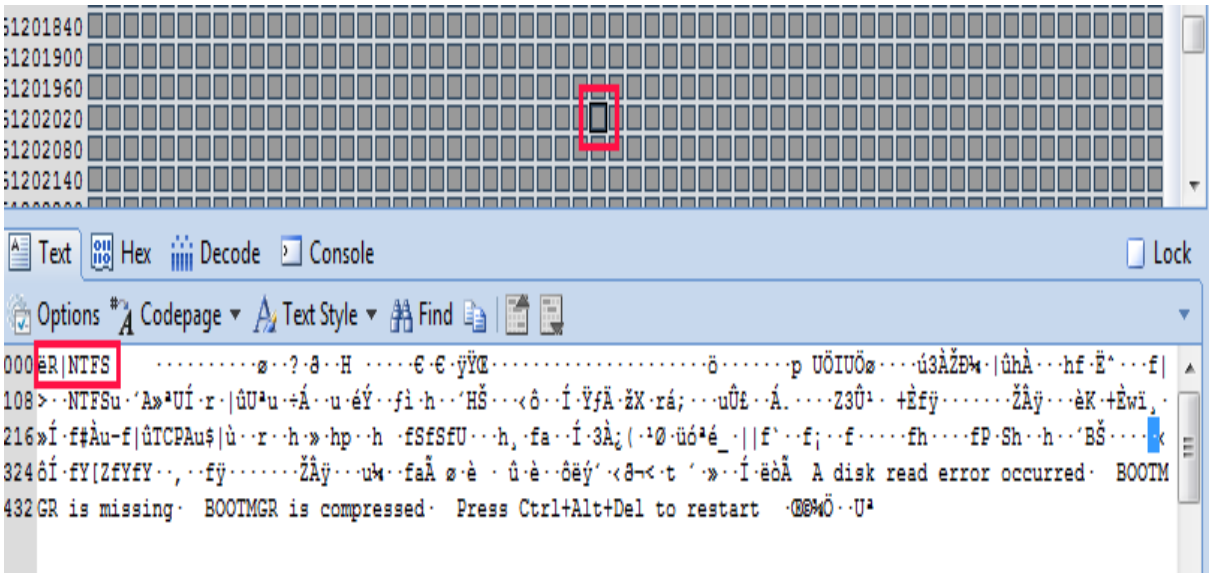
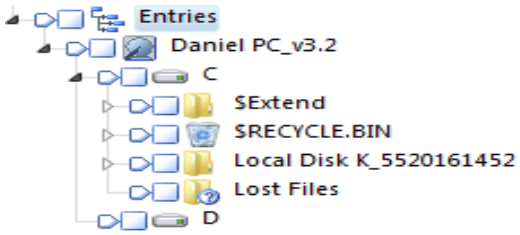


圖8：員工C電腦中有被刪除磁區



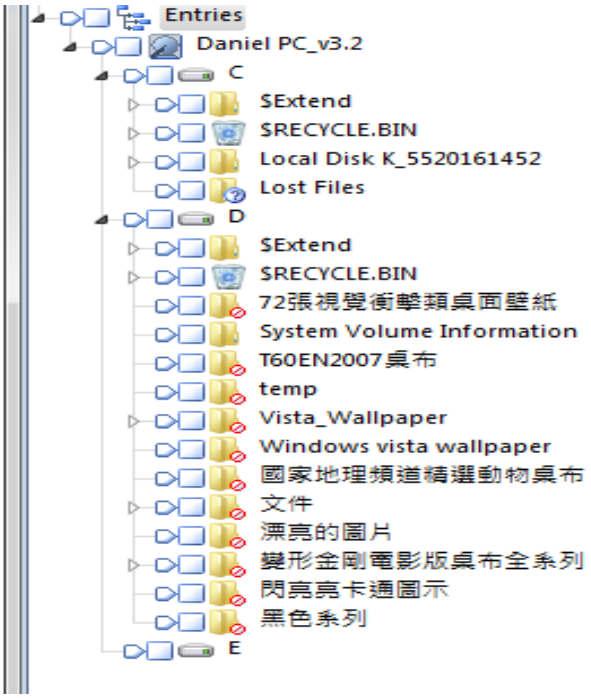


圖9-1：原始磁區狀態　　圖9-2：還原後磁區狀態

圖9：員工B硬碟磁區狀態

圖10：資料夾還原作業執行結果

(2) 【步驟 2】：執行檔案特徵值比對

比對檔案副檔名(Extension)及標頭特徵值(Head Signature)，可確認檔案副檔名是否遭到異動，鑑識人員檢查特徵值比對執行結果時發現員工B電腦中有部份機房相關圖片的副檔名與正確檔案類型不符，以圖11為例，該圖片之副檔名被變更為DLL且該類型圖片皆位於被刪除之磁區中，顯示意圖隱藏攻擊者之惡意行為。

(3) 【步驟 3】：根據案情執行關鍵字搜尋

在Encase鑑識工具，以「169\.254\.7\.0|([3-9]#?)|(1#{0,2})|(2([0-4]#?)|(5[0-5]?)|[6-9])」字串做為關鍵字，搜尋員工B電腦中之內部網路IP位址相關檔案後，雖未能直接找到異

常檔案或數位證據，卻發現該主機曾有遠端連線紀錄，如圖12，鑑識人員針對系統日誌檔案進行分析。

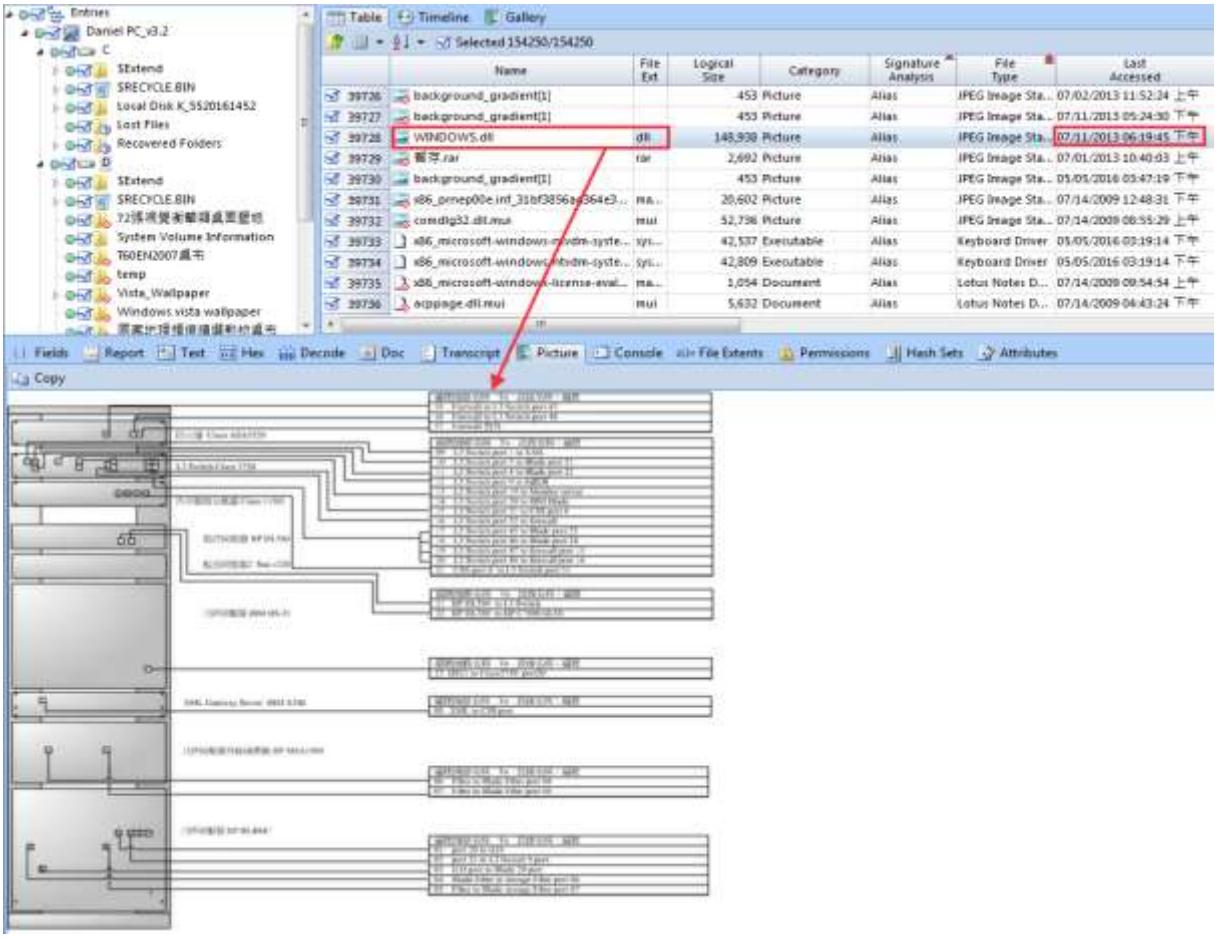


圖11：檔案特徵值比對執行結果

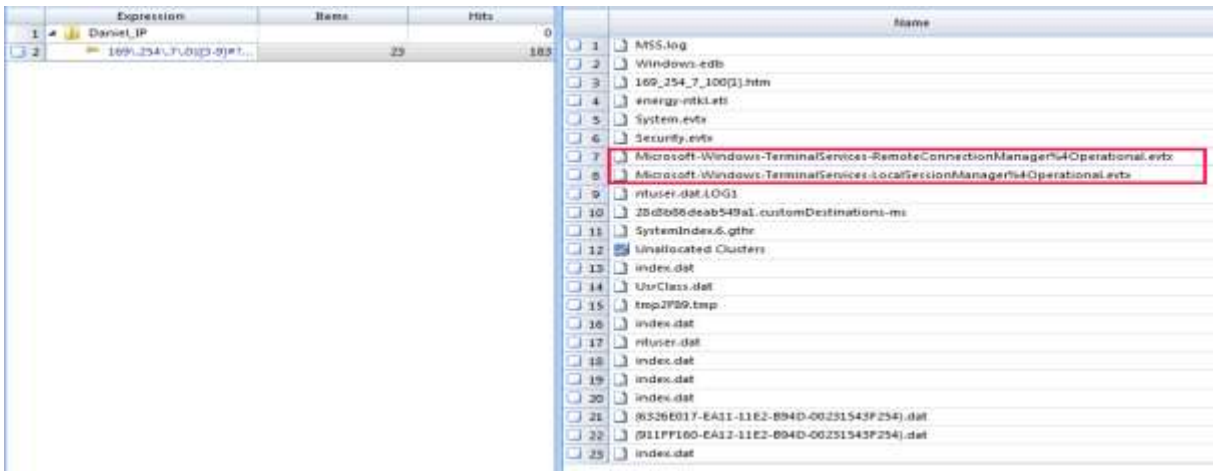


圖12：以內部網路IP位址作為關鍵字之搜尋結果

(4) 【步驟 4】：復原並檢查系統日誌檔案及電子郵件

鑑識人員除檢閱上述與關鍵字相符之遠端連線系統日誌外，針對「Security.evtx」及「System.evtx」進行，發現169.254.7.92此網路IP位址曾透過遠端連線進入員工B的電腦中，如圖13。鑑識人員檢查員工B電腦中之電子郵件後發現有一廣告信件中含有指向惡意網址「http:/169.254.7.92:8080/Zch9a0PWE3i4」之超連結，該網址與前述之遠端桌面連線來源「169.254.7.92」相關，如圖14，研判應為攻擊者發送之釣魚信件，使員工B點擊該超連結後，攻擊者便可遠端連線該電腦。

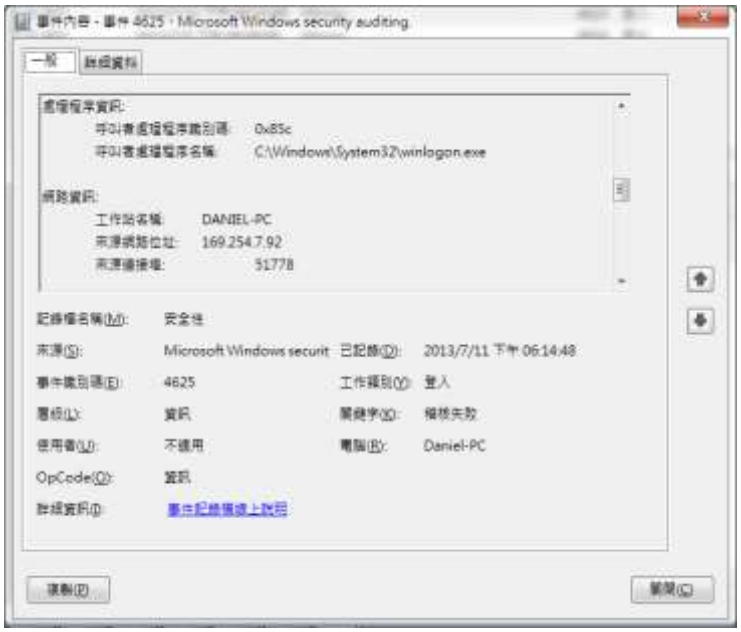


圖13：遠端連線紀錄

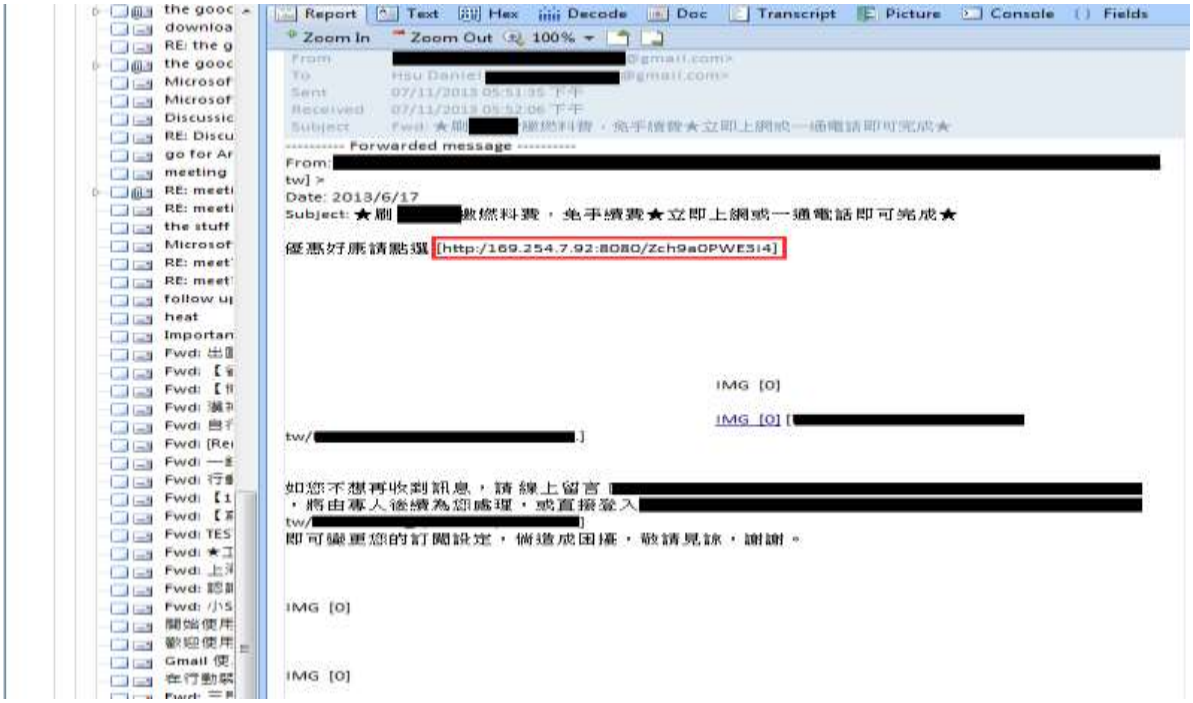


圖14：含異常超連結之廣告信件

(5) 【步驟 5】：確認時間順序符合案情並製作報告

鑑識人員根據所取得之數位證據時間屬性，彙整案件時間軸如圖15，網路IP位址「169.254.7.92」發送釣魚信件後，以遠端連線方式進入員工B電腦中，進行變更圖片副檔名及刪除磁區等作業，經研判應與該資料外洩案件有關。隨後，鑑識人員將所有於分析階段發現數位證據詳實紀錄，製作鑑識報告。鑑識人員分析標的檔案，透過關鍵字及特徵值分析找到線索後，輔以流程化之鑑識分析步驟，循序漸進完成複雜鑑識作業，避免遺漏重要證據。

圖15：時間軸分析

上述模擬案例為透過內部網路發送釣魚信件後，取得遠端存取權限，進而竊取資料。考量員工A為避免直接傳送機敏資料，可能進行變更副檔名等反鑑識手法，可透過檔案特徵值分析先找出是否有可疑檔案。員工B電腦僅能由內部網路進行存取，作業系統日誌中將可能留存內部網路IP位址遠端存取軌跡。以上述兩者為起始，即可找到更多有助於後續分析作業之相關檔案或隻字片語。該案件分析過程及結果可完整對應本文所提出之標準作業流程，透過循序漸進分析方法，可結構化鑑識分析作業，提昇鑑識分析作業效率。

六、結論

本文以國際鑑識標準或建議為基礎，輔以實際鑑識作業需求，定義數位鑑識實驗室人員架構及其職掌，提出數位鑑識現場蒐證及鑑識分析階段應有之標準作業流程及相關標的，設計實驗室各分區及其作業範圍要點，作為建構數位鑑識實驗室之依據，使實驗室主管得以妥善安排人力，鑑識人員可對照實際作業範圍或項目，完備數位鑑識處理流程及分析結果，提升鑑識分析作業的實作效率。未來研究，將評析數位設備處於開機情況的現場取證方式與技術，期擷取揮發性資訊或網路狀態之同時，亦能找到或恢復有價值的即時資訊，並提出識別、收集、獲取及保存的調查工具、方法，滿足數位證據相關性、可靠性及足夠性要求，符合數位鑑識實務應用需要。

謝啟

本研究課題得到科技部研究計畫(MOST 105-2221-E-015-001-)資助，特此致謝。

參考文獻

[1] 王旭正、林祝興、ICCL資訊密碼暨建構實驗室, "數位科技安全與鑑識", 博碩文化出版社, 2009.
[2] 余山亮, "數位鑑識實驗室建置之芻議",碩士論文,高雄師範大學資訊教育研究所, 2011.

[3] 財團法人全國認證基金會, "ISO/IEC 17025：2005 測試與校正實驗室能力一般要求", 2011.
[4] 黃嘉宏、詹前隆、王旭正, "電腦鑑識工具應用於犯罪偵查之研究", 警察通識與專業學術研討會論文集, 2008.
[5] 廖惠雯、劉文港, "電腦鑑識程序之研究", 資訊科技國際研討會論文集, 2008.
[6] 蔡旻峰、陳志誠, "數位鑑識實驗室建構標準之芻議", 第六屆「網際空間：資訊、法律與社會」學術研究暨實務研討會, 2004.
[7] Agarwal, A., Gupta, M., Gupta, S., and Gupta, S.C., "The Systematic Digital Forensic Investigation Model", *International Journal of Computer Science and Security (IJCSS)*, Vol. 5, No.1, 2011.
[8] Al-Fedaghi, S. and Al-Babtain, B., "Modeling the Forensics Process", *International Journal of Security and Its Applications*, Vol. 6, No. 4, October 2012.
[9] Ashcroft, J., Daniels, D.J. and Hart, S.V., "Forensic Examination of Digital Evidence: A Guide for Law Enforcement", NIJ (National Institute of Justice) Special Report, 2004.
[10] Blackwell, C., Islam, S. and Aziz, B., "Implementation of Digital Forensics Investigations Using a Goal-Driven Approach for a Questioned Contract", *Ninth Annual IFIP WG 11.9 International Conference on Digital Forensics*, 2013.
[11] Carvey, H., *Windows Forensic Analysis Toolkit 3rd Edition*, Syngress, 2012.
[12] Casey, E., *Digital Evidence and Computer Crime: Forensic Science, Computer and the Internet, 3rd Edition*, Academic Press, pp. 11-27, 2011.
[13] Casey, E., *Handbook of Computer Crime Investigation: Forensic Tools and Technology*, Academic Press, 2004.
[14] Cosic, J. and Cosic, Z., "Chain of Custody and Life Cycle of Digital Evidence", *Computer Technology and Application*, Vol. 3, pp. 126-129, 2012.
[15] Dezfoli, F.N., Dehghantanha, A., Mahmoud, R., Binti, N.F., Sani, M. and Daryabar, F., "Digital Forensic Trends and Future", *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, Vol. 2, No. 2, 2013.
[16] Falayleh, M.A., "Building a Digital Forensic Laboratory for an Education Institute", The International Conference on Computing, Networking and Digital Technologies (ICCNDT), pp. 285-293, 2012
[17] Fenu, G. and Solinas, F., "Computer Forensics an Approach to Evidence in Cyberspace", *Society of Digital Information and Wireless Communications (SDIWC)*, 2013.
[18] ISO/IEC Information Technology, "Security Techniques: Codes of Practice for Information Security Management", International Organisation for Standardization and the International Electrotechnical Commission, ISO/IEC 17799, 2005.
[19] ISO/IEC Information Technology, "Information Technology — Security Techniques — Incident Investigation Principles and Processes", International Organisation for Standardization and the International Electrotechnical Commission, ISO/IEC 27043, 2015.
[20] Kent, K., Chevalier, S., Grance, T. and Dang, H., "Guide to Integrating Forensics into Incident Response", Special Publication 800-86, Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, 2006.
[21] Kruse, G.W. and Heiser, J.G., *Computer Forensic: Incident Response Essentials*, Addison Wesley, pp 2-8,163-174, 2002.
[22] Kuchta, K.J., "Computer Forensics Today", *Information Systems Security*, Vol. 9, No. 2, pp. 29-33, 2002.
[23] NIST, Computer Forensic Tool Testing (CFTT) project, http://www.cftt.nist.gov/
[24] Pladna, B., "Computer Forensics Procedures, Tools, and Digital Evidence Bags: What They Are and Who Should Use Them", *The Hitchhiker's World*, Vol. 8, 2008.

[25] Smutny, Z., "Standard ISO 27037:2012 and Collection of Digital Evidence Experience in the Czech Republic", *14th European Conference on Cyber Warfare & Security*, Hatfield, pp. 2-3, July 2015

[26] Solms, S.V., Louwrens, C., and Grobler, T., "A Control Framework for Digital Forensics", *International Federation for Information Processing (IFIP)*, 11.9, 2006.

[27] Scientific Working Group on Digital Evidence (SWGDE), "Digital Evidence: Standards and Principles", *Forensic Science Communications*, 2000.

[28] Yang, C.H. and Yang, B., "Design and Implementation of Digital Forensic Systems", The Institute of Electronics Information and Communication Engineers, 2012.

[29] Yusoff, Y., Ismail, R. and Hassan, Z., "Common Phases of Computer Forensics Investigation Models ", *International Journal of Computer Science & Information Technology (IJCSIT)*, Vol. 3, No. 3, June 2011.