可否變動數位證據：現場存取原始證物的省思

高大宇*

目　次

摘　要

執法機關經常處於快速變動的工作環境，在調查案件中需要分析數位資料，提供關鍵證據。數位鑑識科學利用科學方法識別、收集、獲取及保存數位證據，2001年數位鑑識研究研討會律定「不可存取原始證物，只可檢查備份」原則，對整體執法環境而言是危險的。該原則忽略執法機關現場第一線調查人員需要獲取快速、立即、可用情資的實際需要。本文回顧數位鑑識調查「存取原始證物之變動數位證據」的相關文獻，討論犯罪現場取證的相關活動意涵，再就由區別現場調查及實驗室鑑識的差異，提出一個新的數位證據的證物治理策略，改善整體執法調查程序。

關鍵字：數位證據、證據分類、犯罪現場、鑑識實驗室、網路犯罪

*高大宇，中央警察大學資訊管理系副教授，中央警察大學犯罪防治所（刑事司法組）博士，
Email: camel@mail.cpu.edu.tw。

Can we work from the original data and change the digital evidence at crime scene?

Da-Yu Kao*

Abstract

Law enforcement agencies work in an area of constant change, need to analyze digital data, and supply vital evidence in all investigations. Digital forensic science provides scientifically proven methods that can be used to identify, collect, acquire and preserve digital evidence. Setting an absolute standard that dictates "work from an exact copy of the original data" is dangerous from the 2001 first Digital Forensic Research Workshop in a legal context. It has ignored the urgent need for first responders to find actionable intelligence immediately at crime scene. This study reviews some former arguments on this evidence dynamics of accessing the original data for digital forensic investigation, and aims at the relevant activities at crime scene. The results illustrate the difference between scene investigation and lab forensics, and propose a new digital evidence governance strategy to improve the whole investigation process.

Key Words: **Digital Evidence, Evidence Triage, Crime Scene, Forensics Lab, Cybercrime**

* Da-Yu Kao, Associate Professor, Central Police University, E-mail: camel@mail.cpu.edu.tw

壹、前言

網路犯罪案件無遠弗屆、無特定地域性、與日俱增，跨國犯罪的警察追捕程序與偵查技術，需要藉助各國家的配合，並遵循大家認同的數位證據蒐集程序。2001年數位鑑識研究研討會（DFRWS, Digital Forensic Research Workshop）律定「不可存取原始證物，只可檢查備份」原則，避免變動數位證據（Palmer, 2001）。2004 年美國國家司法研究院（NIJ, National Institute of Justice）和司法部（DoJ, Department of Justice）也相繼律定：「蒐集或處理數位證據時，不該影響證據的完整性（integrity）」（NIJ, 2004）。調查人員也被要求，採用建議的調查程序是對開機電腦「拔插頭」、「不得存取原始證物」，蒐集相關配備後送實驗室檢查。隨著網路犯罪變得越來越普遍，犯罪調查現場充斥著電腦顯示器，鍵盤和滑鼠等，這樣的調查程序非但沒有提供實質幫助，卻反而阻礙訴訟調查的進行，費時程序伴隨大量積案，凸顯「拔插頭」、「不得存取原始證物」的規定不切實際（Casey, 2011）。

各國執法實務工作上，日漸傾向認為，數位鑑識調查或分析人員應該於犯罪現場電腦關閉設備前，運用科技方法對軟體和網路進行快速證據分類或預覽（evidence triage/preview），避免系統崩潰或數位證據遺失（ISO/IEC, 2012; SWGDE, 2014）。分類（triage），原意為當醫療資源不足以處理所有傷患時，施以分類、排序或選擇，決定緊急治療的優先處理順序，使傷患能得到有效率的處理，並根據病人受傷情形，決定治療處理的優先程序，又稱分類診斷或檢傷分類。該檢傷分類主要目的就是「適當時間內，能讓受傷的人，在適當地方，使用適當資源」。反思證據分類（evidence triage），亦有尋求「適當時間內，讓犯罪證據，能在適當地方（犯罪現場或實驗室），採用適當工具資源蒐集證據」之意（Pearson and Watson, 2010）。亦即不同時機或處所，採集證據的工具或方法，得因地制宜；而非，僅貿然律定「不得存取原始證物」。執法人員因為犯罪現場（crime scene）或鑑識實驗室（forensics lab）的蒐證地點、目的、工具不同，所採行的蒐證程序、優先順序也應該有所不同，實有必要進一步釐清，供各現場第一線調查人員（first responder）或實驗室分析人員（lab analyzer）參考。因為電子形式儲存資料的檢查（examination）、蒐集（collection）或保存（preservation），往往須在調查者到達現場，於有限時間內，以最小干擾（侵入）方式完成。有時，部分資料的變更是不可避免的，亦須奉行「最少量變更資料」、「最小化干擾原始證物」之原則（ISOC, 2002; SWGDE, 2014）。如電腦網路等機器設備在開機執行期間的活體證據獲取（live acquisition）。部分屬性資料本質的改變原因，必須交待清楚、可被解釋、也可被法院所接受的，這樣的觀念與想法，日漸獲得執

法機關與承審法院的認同（ACPO, 2012）。

本文相關章節安排如下：第貳節討論傳統數位鑑識之靜態證物的處理缺陷及數位證據的動態性，解析犯罪偵查與鑑識科學的相關概念與運作原理。第參節為釐清存取原始證物之變動數位證據爭論疑慮，蒐集「得」與「不得」存取原始證物之各項主張，並比較異同。第肆節依據學術文獻及實務運作觀察結果，先分析存取原始證物的優勢、劣勢、機會與威脅，再探討「不得存取原始證物非傳統鑑識科學要求」及「數位分類鑑識快速立即獲取可用情資證據」兩觀點，剖析存取原始證物的爭議問題。第伍節從人力分工、處理程序及分析技術三面向，研提數位證據的證物治理策略，以現場利用多樣工具調查，存取原始證物，快速蒐證獲取及時情資，為執法機關的優先考量方向。第陸節歸納結論。

貳、文獻探討

一、傳統數位鑑識

數位鑑識是個快速發展的領域，須妥適訓練數位鑑識實作人員確認數位證據在執行調查時，沒有被毀壞、破壞或不當存取（Brooks, 2015; Kleiman et al, 2007）。考慮數位證據的可信度時，亦需驗證這些數位證據是否值得信賴（trustworthiness of digital evidence），降低現場或實驗室發現的問題或錯誤。

（一）數位證據的動態變化

數位資料分析會因電腦時間、開啟程式、執行程序或電腦狀態的不一致，產生不同的紀錄結果，此乃證據動態性所致。「存取原始證物」的動態鑑識，雖然可能變更原始證物、對系統造成變動，常常卻是需要的（Zeng, 2014）。例如，雲端環境的數位證據是動態的，包含本地主機及網路環境證據兩種，本地主機證據包含記憶體資訊、暫存資訊、檔案讀寫狀態，這些均屬重要的證物屬性。網路環境證據包含網路協定、數位封包大小、電腦的 IP 位址、開啟通訊埠、連線時間，這些在傳統數位鑑識中均無法察覺（Zang and Mai, 2011）。大部分的數位鑑識分析也會呈現不盡相同的結果（Most analysis in digital forensic science cannot make similar claims），該證據分析需要闡述解釋，方能了解實情（Palmer, 2001）。

（二）靜態證物的處理缺陷

傳統的數位鑑識，主張「不得存取原始證物」，處理靜態證物都是事後處理，避免原始證物上執行，以映像檔執行分析（image analysis）為主軸，降低不當的證據

變更疑慮（Akhgar, Staniforth, and Bosco, 2014）。調查者會先產生映像檔，再透過 Encase 或 FTK 等鑑識工具分析證據，嘗試還原原始狀態，卻會遺失正在執行程式（running program）、開啟通訊埠（open port）、網路連線狀況（netstat）等揮發性證據。數位證據具動態變化特質，蒐證現場考量搜索時間壓力，往往難以執行映像拷貝動作，又無法取得上述揮發性證據，之後，實驗室也會累積過多案件，顯見傳統數位鑑識之避免原始證物上執行蒐證動作主張，呈現窒礙難行處。

二、犯罪偵查與鑑識科學

（一）犯罪偵查

犯罪偵查（criminal investigation）包含應用現代科學技術的鑑識科學（forensic science），如表 1，犯罪偵查與鑑識科學屬兩種不同概念。當查無識別身分的指紋、DNA 等事證時，尚需進一步分析作案手法或特殊技術，尋求查獲嫌犯。犯罪偵查目的在釐清人、事、時、地、物，透過發現、分析問題，尋找解答。犯罪偵查尋求確認犯罪者的方法、動機及對象，著重被害者的識別，證人的會晤與查訪，致力於探索事件的真實原貌。

表 1　犯罪偵查與鑑識科學比較表

區別	犯罪偵查	鑑識科學
定義	研究事實的應用科學，可識別、鎖定、驗證被控罪犯的罪責。	法律訴訟的應用科學，於調查程序中，客觀蒐集、保存、分析科學性證據。
主要概念	運用搜尋、訪談、訊問、證據蒐集及保存等調查方法，以發現事實。	利用科學方法現場蒐集證據後，實驗室執行分析，以形成結論、見解或意見。
目的	釐清人、事、時、地、物	釐清證物類別及個化
相互關係	包含鑑識科學	包含於犯罪偵查

資料來源：作者整理

（二）鑑識科學

在法律案件上，鑑識科學使用可被接受的識別、蒐集、保存、分析、報告證據等客觀調查程序。重點在於利用科學方法蒐集證據，使用可重複且可被驗證的方法。鑑識科學目的在釐清法院訴訟案件證物的類化（classification）及個化（individualization），並形成結論（conclusion）、見解或意見（opinion）。類化乃嘗試決定一個證物的原本狀態或種類。個化乃使用一連串的特質識別該項目。結論，是

指針對事實所推導出來的結果，是客觀描述。例如在被害電腦中找到遭刪除的木馬程式，則可做出被害電腦曾安裝木馬程式的結論。見解或意見，是指依照科學知識、測試結果、或自己的經驗所作出的結論，相較於結論，見解或意見較主觀。例如依照蒐集到的證物來推論被害電腦於何時安裝木馬程式（Stephenson, 2014）。

參、存取原始證物之變動數位證據爭論

數位證物狀態屬一種持續變動的數位運作環境。要從待檢驗的數位儲存設備中，獲取相關線索資料，原始狀態的確認是個難解疑題。尤其當原始狀態是不斷變動時，獲取數位證物的技術，屬藝術或科學（art or science），或屬調查或鑑識（investigation or science），存在爭議討論的空間。也因為產官學界的角色不同，主張論調的解決方式各有不同，致存在可否存取原始證物的爭點（如表 2）。

表 2　存取原始證物的重點主張一覽表

存取原始證物論點	年度	組織	強調重點	主張
得與不得併行	1999-2014	數位證據科學工作群組(SWGDE)	鑑識處理能力	獲取數位證物時，原則上不得變更原始證物。但若有人需存取原始證物時，那個人必須要有鑑識處理能力。
得	2000	美國聯邦調查局的標準原則	鑑識科學的方法	任何可能變更、損壞或毀壞數位證據的任何行為，應該被合格專業人員，以符合鑑識科學的方法執行之。
不得	2001	數位鑑識研究研討會(DFRWS)	數位證據的信賴性	不得存取原始證物，只可檢查備份，確保數位證據的信賴性。
得	2002	徵求意見書(RFC)3227	揮發性的順序	調查人員須儘量減少自己留下的痕跡，應該按揮發性的從高到低順序，依序處理待檢證物。
不得	2004-2008	美國國家司法研究院(NIJ)和司法部(DoJ)	數位證據的完整性	蒐集或處理數位證據時，不該影響證據的完整性。

得與不得併行	2007-2012	英國高級警官協會(ACPO)	處理動作的適當解釋	為了取得法院對於電腦證據或數位證據的認可，警察處理人員或其委託人員必須確保電腦或其它電子媒體上的資料保持為犯罪現場原始的狀態，不得修改其任何內容。在特殊情況下，如果需存取原始電腦證據的資料，則必須由有能力的人員進行存取動作，並對其處理的動作予以說明或適當解釋。
得	2012	ISO/IEC 27037:2012	數位證據的相關性、可靠性及充分性	極小化處理原始證物數位證物。說明數位證物變更原因。

資料來源：作者整理

一、不得存取原始證物

「不得存取原始證物」主張，應優先適用實驗室鑑識，不適用現場調查。但雲端或智慧手機等鑑識，因鑑識工具功能限制，於實驗室鑑識時，仍有「得存取原始證物」之潛在需求。

（一）2001 年，數位鑑識研究研討會，強調數位證據的信賴性

2001 年 8 月 7 至 8 日，第一屆數位鑑識研究研討會（DFRWS, Digital Forensic Research Workshop），在紐約州的由提卡（Utica）舉行，會中聚集超過 50 位的大學研究學者、電腦鑑識檢查及分析人員，討論四個議題（Palmer, 2001）：

1.定義數位鑑識科學架構（a framework for digital forensic science）

2.數位證據的信賴性（trustworthiness of digital evidence）

3.隱藏資料的偵測與復原（detection and recovery of hidden data）

4.網路鑑識（network forensics）。

為獲取信賴的數位證據（Trustworthiness of Digital Evidence），與會專家研討如何於第一次獲取資料時，便能達到原始資料架構不變動的狀態（Has the structure of the data remained unchanged since it was first obtained?），以確保資料完整性，並能精確、真實地呈現事件事實。得出：「不得存取原始證物，只可檢查備份（Work from an

exact copy of the original data)」的結論建議(Palmer, 2001)。但該問題本身存在瑕疵，未考慮證據揮發性、動態性及急迫性，應考慮執法機關在現場的即時分析需求，可藉由嫌犯(或在場人)會同勘查、錄影存證及適當說明解釋等補強合理性、適法性，而非一味以事後鑑識實驗室的觀點，考量資料完整性或信賴度，額外建立傳統鑑識科學沒有的數位鑑識原則：「不得存取原始證物」。看似解決信賴性的學理性爭議，卻又引發執法機關實務上不可行的爭議問題。

(二) 2004-2008 年，美國國家司法研究院和司法部，強調數位證據的完整性

2004 年，美國國家司法研究院(NIJ, National Institute of Justice)和司法部(DoJ, Department of Justice)發行執法機關之數位證據的鑑識檢查指引(Forensic Examination of Digital Evidence: A Guide for Law Enforcement)內容，提及：執行數位證據檢查人員應該接受適當訓練。蒐集或處理數位證據時，不該影響證據的完整性。蒐集、檢查、儲存或轉換數位證據的過程，應該要文件化保存，供專家後續審視(NIJ, 2004)。2008 年美國國家司法研究院和司法部再度合作發行電子犯罪現場調查之第一線調查人員指引(Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition)亦延續類似主張(NIJ, 2008)。

二、得存取原始證物

「得存取原始證物」主張，應優先適用現場調查。執法機關亦需參考相關標準，律定現場存取原始證物的標準作業程序，降低變動數位證據的衝擊影響。

(一) 2000 年，美國聯邦調查局的標準原則，強調鑑識科學的方法

2000 年，美國聯邦調查局的標準原則(FBI's standards principle)之一為：任何可能變更、損壞或毀壞數位證據的任何行為，應該被合格專業人員，以符合鑑識科學的方法執行之(Any action that has the potential to alter, damage, or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner)(SWGDE and ICOE, 2000)。執法機關執行數位證物的動態調查，勢必得存取原始證物，也可能會導致局部變更、損壞或毀壞數位證據的行為，故需合格專業人員執行，降低損害程度。

(二) 2002 年，徵求意見書(RFC)3227，強調揮發性的順序

1.按揮發性順序蒐集資料

2002 年，網際網路社會組織(ISOC，Internet SOCiety)提供的徵求意見書(RFC, Request for Comments)，編號 3227 的證據蒐集及歸檔指引(Guidelines for Evidence

Collection and Archiving），為提供適合資安政策、事件處理、執法人員及系統管理者作為資安事件證據蒐集與備份的指引（ISOC, 2002），調查人員收集資料行為會因接觸而留下痕跡，破壞犯罪現場，須儘量減少自己留下的痕跡，且能區分蒐集者或攻擊者留下的人為痕跡。調查人員的每一次收集證據過程，應該按揮發性從高到低的順序（order of volatility），依序處理待檢證物，蒐集資料。電腦系統揮發性從高到低的順序（ISOC, 2002），如下：

(1) CPU 的暫存器檔案結構（register files）、快取記憶內容（cache）
(2) 路由表（routing table）、位址解析協定（ARP; Address Resolution Protocol）的 IP 位址及對應 MAC 位址之記憶內容（ARP cache）、處理程序表（process table）、核心統計（kernel statistics）、記憶體內容（memory dump）
(3) 暫存檔案系統（temporary file systems）
(4) 磁碟（disk）
(5) 遠端登入和監控資料（remote logging and monitoring data）
(6) 組態設定（physical configuration）、網路拓撲架構（network topology）
(7) 檔案儲存媒體（archival media）

2.存取原始證物時，應避免或減少變更資料

考量數位證據的揮發性順序，為有效依序蒐集資料，建議（ISOC, 2002）：

(1) 未完成證據蒐集前，不要關機。蒐集資料時，要減少對資料內容、目錄或檔案存取時間的變更，避免採用會變更資料的方法。
(2) 盡可能擷取正確的系統資訊畫面，保持包含日期時間等隨同詳細註解。
(3) 盡可能使用批次處理的工具組，避免寫入待扣證據的儲存媒體。
(4) 隨同註解或列印文件均須附上簽名及日期。

3.資料先收集，再分析

面對收集或分析的抉擇時，要先收集，之後再分析。當受檢電腦系統少且時間足夠時，可以逐步慢慢檢查，但待檢電腦太多時，便須透過套裝工具組，快速檢查大量電腦檔案，期於有限時間內，能達成調查目的。但如果分析會變更檔案存取時間時，應該在完整拷貝的映像檔上執行。

（三）2012 年，ISO/IEC 27037:2012，強調數位證據的相關性、可靠性及充分性

ISO/IEC 27037: 2012 之資訊技術-保密技術-數位證據識別、收集、獲取和保存指引，為個人涉及電腦、行動電話、數位相機和錄影機、導航定位系統或其他儲存設備之潛在數位證據的識別（identify）、收集（collect）、獲取（acquire）和保存

（preserve），提供數位證據現場第一線調查人員（Digital Evidence First Responders）、數位證據專家（Digital Evidence Specialists）、事件回應專家（Incident Response Specialists）、鑑識實驗室管理人（Forensic Laboratory Managers）收集資料指導原則。執法機關可依靠該標準分析、提交數位證據、確保數位證據的完整性。但該標準雖為數位證據的調查實務指引，尚不能取代任何地區的法律法規。ISO/IEC 27037:2012國際標準描述通過參與調查的早期階段，包括最初的反應，期獲取充分的潛在數位證據，適當地繼續進行偵查作為。

1. 數位證據的處理原則：相關性、可靠性及充分性

大部分的司法管轄或組織，要考慮數位證據的相關性（relevance）、可靠性（reliability）及充分性（sufficiency）等三項處理原則，不是僅考慮法院是否接受問題（ISO/IEC, 2012），而非一味貿然地認定原始證物一律不得存取之信賴性。

(1) 相關性，指證明或否定個案的某個關鍵。數位證據是否相關，要根據個案調查過程，該證據是否能證明或否定個案的關鍵事項；

(2) 可靠性，指確保具體展現數位證據的真實意義。現場鑑識人員未必需要蒐集所有資料，或製作完整的原始證物拷貝，雖然可靠性在不同的司法管轄權內的定義各不相同，一般的可靠性定義為確保具體展現數位證據的真實意義獲認可；

(3) 充分性，指蒐集充分的潛在數位證據，讓待釐清事件確實被檢查或調查。當時間或花費（經費金額）是影響關鍵或疑難重點時，現場處理人員才會知道哪些事項是重點，知悉該現場調查或實驗室鑑識應如何處理方為恰當。

2. 數位證據的處理程序

就數位證據的處理程序（digital evidence handling processes）而言，要遵循文件化的處理程序，確保維持潛在數位證物之可靠性，並該遵循的下列原則：

(1) 極小化處理原始數位證物。

(2) 說明數位證物變更原因，及文件化處理步驟，讓專家能對該程序的可靠性表示意見。

(3) 遵循本地的證據處理原則。

(4) 不要做超出能力的行為。

三、得與不得存取原始證物併行

本「得與不得存取原始證物併行」主張，兼顧現場調查及實驗室鑑識需求，同時適用現場調查及實驗室鑑識，應列為現今主流論點，並由實際已獲適當訓練的執

行人員，自行判斷是否須「存取原始證物」且負全責。

（一）1999-2014 年，數位證據科學工作群組，強調鑑識處理能力

鑑識人員要與調查人員詳談，攜帶必要的工具設備至現場，避免於蒐集事實（Fact）過程浪費時間、精力，要能整併相關線索、資料及資訊，廣泛獲得各方證據資料。

1.原則上不得存取原始證物，例外得存取原始證物，維護數位證據的信賴性

1998 年 2 月，成立數位證據科學工作群組（SWGDE, Scientific Working Group on Digital Evidence），與美國致力發展標準程序的電腦證據國際組織（IOCE, International Organization on Computer Evidence），共同發展跨領域的數位證據之復原、保存與檢查工作。於 1999 年 10 月 4 至 7 日，在英國倫敦舉行的國際高科技犯罪與鑑識研討會（IHCFC, International Hi-Tech Crime and Forensics Conference），首先提出數位證據的交換標準草案，後被美國執法機關採用。該草案指出：「獲取數位證物時，原則上不得變更原始證物。但若有人需存取原始證物時，那個人必須要有鑑識處理能力（Upon seizing digital evidence, actions taken should not change that evidence. When it is necessary for a person to access original digital evidence, that person must be forensically competent.）」（SWGDE and ICOE, 2000）。

2.證據分類與預覽（Evidence Triage/Preview），維護數位證據的相關性、可靠性及充分性

2014 年 9 月 5 日，SWGDE 的電腦鑑識最佳實作（Best Practices for Computer Forensics），承認證據分類及預覽的必要，均屬延續 2010 年，美國專家 Stephen Pearson 及 Richard Watson 主張數位分類鑑識（Digital Triage Forensics）概念一樣，得存取原始證物，快速取得需求資料（Pearson and Watson, 2010），並補充下列幾點（SWGDE, 2014）：

(1) 數位鑑識的前置動作

證據分類是數位鑑識的前置動作，如同病患檢傷分類處理機制，尋求快速地蒐集情資，期在最短時間內獲致最佳效果。傳統數位證據程序著重數位證據開始檢查之前的映像拷貝及雜湊函數驗證，證據分類也被視為傳統數位證據的預覽程序（Cantrell, 2012）。伺服器可能不宜拔插頭（或關機），避免損壞系統、影響合法商業運作、或對該伺服器所屬組織不利。原則上，現場電腦關機，就不要開機。只有受訓者才能重新開機，執行證據分類或預覽程序（SWGDE, 2014）。

(2) 視個案需要判斷是否存取原始證物

在執行系統中執行證據分類或預覽程序，會影響檔案的時間戳記紀錄。證據分類可能不適所有狀況，預覽證據可能會錯失一些證據價值。因為每種蒐證方法均有不同得失利弊，不同角色鑑識人員或執行者應該要能自行依據不同情境判斷，因地因時制宜，決定蒐證程序步驟及方法，並負擔全部責任 （SWGDE, 2014）。

(3) 彼此互補，無法取代

許多組織沒有專業人員可以執行數位證據的蒐集。證據分類和預覽，只可被妥適訓練的專業人員執行。當證據分類無法達到鑑識目的、無專業人員或時間時，仍可透過映像拷貝處理。證據分類或預覽程序，無法取代映像拷貝技術完整檢查的信賴性。同樣地，映像拷貝技術的完整檢查亦無法取代證據分類或預覽方法的相關性、可靠性及充分性。

（二）2007-2012 年，英國高級警官協會（ACPO），強調處理動作的適當解釋

英國高級警官協會（ACPO, Association of Chief Police Officers）是英國警方和政府部門重要智庫，於 2007 年間提出電腦上的數位證據實作指引（Good Practice Guide for Computer Based Electronic Evidence），建議下列處理數位證據的四項原則，逐年檢討修正（ACPO, 2012），分析說明如下：

1.原則一：為了取得法院對於電腦證據或數位證據的認可，警察處理人員或其委託人員必須確保電腦或其它電子媒體上的資料保持為犯罪現場原始的狀態，不得修改其任何內容。

所有數位證據應該適用相同的法律規範，並應用於衍生的文件化證據。該文件化證據應該被解釋為：起訴、告發或檢舉那一方的職責，在執法機關首次接觸、或持有該證據的當下狀況，不可增刪減，應原封不動地呈現法院。

2.原則二：在特殊情況下，如果需存取原始電腦證據的資料，則必須由有能力的人員進行存取動作，並對其處理的動作予以說明或適當解釋。

作業系統和其他程式常會變更、增加和刪除電子儲存內容，在使用者未必知情下，自動變更資料狀態。如果調查者要針對完整電子設備的實體/邏輯萃取、或分類分批處理的部分/選擇性的資料萃取，製作映像檔，應該利用專業判斷，致力於擷取相關、關鍵的證據。如果處理的資料，不存在本地端，可能存在遠地端，會面臨無法獲取映像檔的困境，直接存取原始資料成為必要程序。有這樣的前提認知與務實考量，有能力擷取資料且能向法院提供解釋的人便可直接存取原始資料。假如待擷

取資料置於另一個管轄權內，需要審慎考慮是否適用執法權問題。

3.原則三：對於電腦證據的任何稽核資料或其他紀錄、分析的處理過程，應建立處理方法、記錄與保留結果，就算委由公正的第三者進行相同的處理程序，其所得的結果應相同。

為展現法院訴訟程序的客觀性，證據的一致性與完整性是很關鍵的。如何復原證據，以及證據獲得程序之呈現已是必要的。保存證據應達一定程度，該程度必須：當證據呈現給法院時，獨立的第三方能夠重複相同程序重新檢查，也能達成相同的結果。但若無法重複現場的相同程序，亦可藉由現場的錄影等文件化紀錄，審視資料的可靠度。數位證據調查中，主要挑戰為證據是動態事件的靜態結果；尤其當證據的動態性發生時，確定的數位證據可能無法被取得或者不完整。任何的證物變更皆應記錄，可記錄蒐集過程的流失證據，並因應個案需要判斷取證方法。

4.原則四：案件承辦的負責人，必須確實遵守法律的規範與以上的原則，並且應用於所有對於案件電腦設備的存取，不管任何人存取電腦資料或拷貝資料都必須遵守法律規範與以上原則。

值得注意的是：這些原則不會排除按比例的數位證據方法（搜索、扣押應符合比例原則，對大企業組織亦同）。數位證據的調查，應該要判斷調查的重點與範圍，考慮可用的情資（如線索、資料、資訊、證據）與調查資源（如團隊人力、時間限制、待理積案）。這包含技術或非技術因素的風險評估，例如，特定型態設備特有的潛在證據（如 Unix-like 系統有 inode 屬性，可查刪除檔案時間），或嫌犯的歷史犯罪前科紀錄。

肆、存取原始證物的省思

本節依據學術文獻及實務運作觀察結果，先分析存取原始證物的優勢、劣勢、機會與威脅，再探討「不得存取原始證物非傳統鑑識科學要求」及「數位分類鑑識快速立即獲取可用情資證據」兩觀點，剖析存取原始證物的爭議問題。

一、存取原始證物的 SWOT 分析

存取原始證物會變更原始證物部分狀態，現場調查（scene investigation）之 SWOT 分析，如表 3（Aljaedi, Lindskog, Zavarsky, Ruhl, and Almari, 2011; Hay, Nance, and Bishop, 2009; Gianni, and Solinas, 2013; Mrdovic, Huseinovic, and Zajko, 2009; Rahman and Khan, 2015; Zhang, Zhang, and Wang, 2010），分述如下。

表 3　現場調查的存取原始證物 SWOT 分析

因　　素（Factors）	好的（Helpful）	差的（Harmful）
內部能力	優勢（Strengths）：事件相關 使用多樣工具，關注重點資訊，得快速蒐集智慧情資。	劣勢（Weaknesses）：缺完整性 變動數位證據，未完整檢查證物，缺完整性、無法重作。
外部環境	機會（Opportunities）：可靠充足 獲取揮發性證據、帳號密碼等快速情資，有效鑑識分析。	威脅（Threats）：失信賴性 使用多樣工具，蒐證品質不一，喪失信賴性。

資料來源：作者整理

（一）內部因素（Internal Capability）

1.優勢（Strengths）：使用多樣工具，關注事件相關資訊，得快速蒐集智慧情資。

(1)使用多樣工具：得利用容易使用、免費或開放原始碼等多樣工具，檢查待驗電腦證物，擴充資料蒐證工具管道。

(2)關注重點資訊：著重事件相關內容，關注於內部檔案資料的獲取，提供調查者更多過去與現在的狀態資料。調查者可蒐集執行中的原始資料及程序資訊，獲取已完成或暫存的執行程序。不需要獲取全部記憶體的映像檔，可降低獲取映像檔（image）的檔案大小。

2.劣勢（Weaknesses）：變動數位證據，未完整檢查證物，缺完整性、無法重作。

(1)變動數位證據：Encase Portable、FTK Imager 或解密等鑑識工具，仍需安裝部分程式或檔案於待驗證物中，始能運作，會變動數位證據。例如：EnCase Portable 需使用 USB 接上目標主機，使用內建應用程式進行採證，可藉由 USB 裝置讓調查者可快速、簡易地分類文件、信件、圖片及網路紀錄，蒐集相關資料。實務運作環境中，許多資料會因而產生變動，也可能影響部分證據內容。系統變更可能會遺失某些證物，無法確保證物的完整性，對待驗證物的損害影響應納入考慮。

(2)未完整檢查證物：未完整檢查證物，可能還有待驗檔案。例如：找尋隱藏資料對調查者而言，是惱人且費時的工作，需進一步檢查，才能獲取較完整的證據資訊。

（二）外部環境（External Environment）

1.機會（Opportunities）：獲取可靠充足揮發性證據、帳號密碼等快速情資，有效鑑識分析。

(1)有效鑑識分析：犯罪現場的動、靜態分析，可獲取或復原使用者的帳號及密碼，讓調查者更容易且更有效率地從事數位鑑識分析工作。

(2)獲取快速情資：快速獲取揮發性及非揮發性資料，觀察現場的電腦環境、網路狀況之原始狀態，快速提供證據情資，降低調查者的時間需求與精力。

2.威脅（Threats）：使用多樣工具，蒐證品質不一，喪失信賴性。

(1)使用多樣工具：商用鑑識工具常未及更新，未取得證物資料，須使用非鑑識工具、商用軟體開發工具、資安管理工具或其他適用工具，蒐證品質不一。例如：不同智慧手機使用 Android、Apple、Blackberry、Window Mobile、Symbian 等不同作業系統，商用鑑識工具常無法提供最新版本的破密、分析或鑑定功能。

(2)喪失信賴性：電腦系統會自動偵測外接式 CD 或 USB 等連接設備，新增蒐證者的接觸（或汙染）事證。獲取證據的信賴性，會因執行人員的身分、方法而遭受質疑。

二、存取原始證物的爭議釐清

存取原始證物有助釐清網路狀態及通訊流量，例如：網路上可能存在的跡證，處理雲端證據的時候，資料儲存的位置可能不確定。網路通訊及流量都是短暫的，必須在其傳輸時才能擷取到。當下抓取網路封包的擷取皆為副本備份資訊，無從比較其與原始資料的異同。收集數位證據不能僅關注靜態資料，網路動態資料亦須一併注意，避免漏失重要事證。

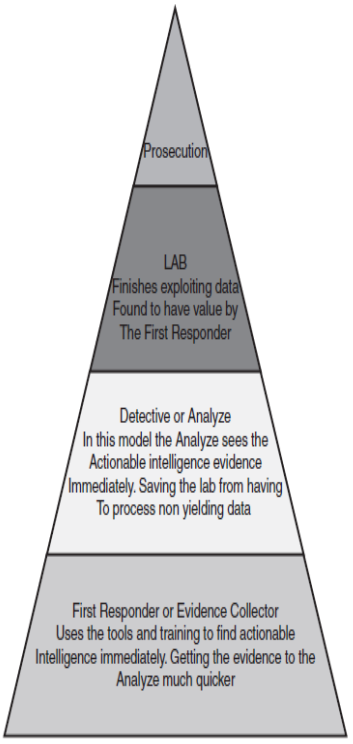
（一）不得存取原始證物：「保存但不變更任何證物」，非傳統鑑識科學要求

2004 至 2011 年，美國學者 Eoghan Casey 主張：不得存取原始證物不切實際。並在其數位證據和電腦犯罪（Digital Evidence and Computer Crime）一書中提及：「一些從事鑑識的人員認為數位證據不能被改變才符合鑑識的要求，這是錯的」（Casey, 2011）。傳統鑑識科學的 DNA 檢驗，沒有要求不得變更原始證物，鑑識分析 DNA 證據樣本時，本身檢驗屬破壞性的檢驗，會變更 DNA 樣本，仍符合鑑識要求且一向被法院接受（Casey, 2011）。指紋鑑定也是一樣，檢驗原始證物。只要對證物的改變做出合理解釋，則證物的改變不影響證物在鑑識上的本質。但都以一個標準來陳

述：「保存但不變更任何證物」，跟原本傳統的鑑識科學要求不同。也就是說，保存任何東西而不變更原始證物的準則，跟傳統鑑識科學的要求呈現不一致現象。這樣的論述，在法院訴訟過程中是相當危險且沒道理的。因為，鑑識實驗分析工作，往往由另一批未至現場的專業人員擔任。從了解案情、映像檔備份、資料復原、關鍵字蒐尋及現場重建等一系統分析證物下來，曠日廢時，未能快速、有效率的處理證物，往往導致待驗證物的快速累積，不利訴訟進行。

（二）數位分類鑑識可快速立即獲取可用情資證據

2010 年，美國專家 Stephen Pearson 及 Richard Watson 提出數位分類鑑識（Digital Triage Forensics）之預防實驗室積案未及處理的金字塔概念（Pearson and Watson, 2010），如圖 1 為數位分類鑑識處理金字塔（processing pyramid）。圖 1-1 之數位分類鑑識處理程序，要求現場處理人員或證據蒐集人員將發現的數位證物送至實驗室前，得適用工具或訓練嘗試檢查，以快速立即獲取可用情資證據，供偵查或分析人員參考，並可於犯罪現場直接洽詢或偵詢嫌犯該情資內容，作為釐清案情、扣押證物或解送人犯的判斷依據。降低後續遞送實驗室的件數比例，減輕實驗室的鑑定負擔，提升實驗室的鑑定品質。圖 1-2 之傳統數位鑑識處理程序，要求現場處理人員或證據蒐集人員要將發現的數位證物直接送至實驗室，不得嘗試作任何檢查，避免變動數位證物的狀態，問題是：該狀態本來就是持續變動的，就算是直接拔電源，部分揮發性證據依然會消失不見。有鑑於傳統的數位鑑識處理程序，讓數位鑑識實驗鑑識室累積過多的待處理案件，難以有效解決大量、巨量儲存數位媒體的待檢需求。偵查或分析人員也僅能默默等待檢查結果，曠日廢時，不切實際，不合實用。分析如下（Pearson and Watson, 2010）：



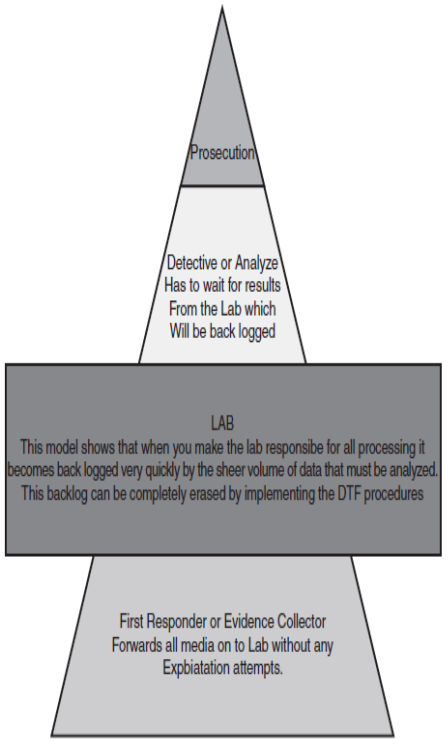


圖 1-1　數位分類鑑識處理程序　圖 1-2　傳統數位鑑識處理程序

圖 1　數位分類鑑識處理金字塔

資料來源：Pearson and Watson, 2010

1.數位分類鑑識工具的興起

數位分類鑑識工具（Digital Triage Tool），又被稱作田野調查蒐尋軟體（Field Search Software），常被應用在敲門談話（knock and talk）之同意搜索（consent search）的執法程序中，再透過診斷（diagnose）、論述處理（treat）、監測（monitor）和管理（manage）等方式，收集鎖定對象的電腦使用資訊。因員警進行前要取得同意進入的前提要件，又稱為「敲門談話式搜索」。同意搜索乃經當事人同意而進行搜索之無搜索票搜索。無搜索票搜索也廣泛存在於偵查程序。調查人員在事先獲得當事人的自願同意後，無搜索票即可對其住所、人身或相關物品實施搜索、檢查行為。

2.田野調查（Field Search）的實際需要

要運用田野調查蒐尋軟體，讓無專業技術人員可以在刑案現場，簡單且有效的檢查電腦。例如，helix 蒐證工具執行時，也會變動一些。要能從錯誤中學習經驗，數位證物的處理，需要依照一定的操作程序，維持檢查的一致性。最好先使用數位防寫設備，蒐集數位資料，再獲取數位證物的映像檔，並使用數位分類鑑識工具，於防寫的環境下處理資料。

(1)到犯罪現場處理數位證據時，須將證據連接並妥善保護後，使用數位分類鑑識工具，快速分析已經蒐集到的數位媒體。所需方法，因應個案需要的不同，需要不同的知識、訓練、工具與經驗。

(2)遠端鑑識（remote forensics），需先植入對應的伺服器代理程式（agent），於待驗主機中，方能遠端存取該主機。

3.現場蒐證時間限制

從受理報案、偵查案件到移送法院，案件偵查時程因案而異，但調查人員進入搜索現場蒐證，原則上不會超過 2~3 小時，從進入現場後的盤查人員、蒐集事證、釐清案情、安全戒護、扣押證物等多項任務時，尚需確認電腦設備是否有扣案必要時，當場預覽檢驗係屬必要，如何利用妥適工具，配合適當訓練，期現場蒐證人員能快速協助取證，釐清案情。

伍、數位證據的證物治理策略

數位證據為傳統物理證據的一種，數位證據易於竄改與傳送的特性，加深調查網路犯罪案件的困難度。謹從人力分工、處理程序及分析技術三面向，研提數位證據的證物治理策略，如圖 2，並以現場利用多樣工具調查，存取原始證物，快速蒐證獲取及時情資，為執法機關的優先考量方向，分析如下。

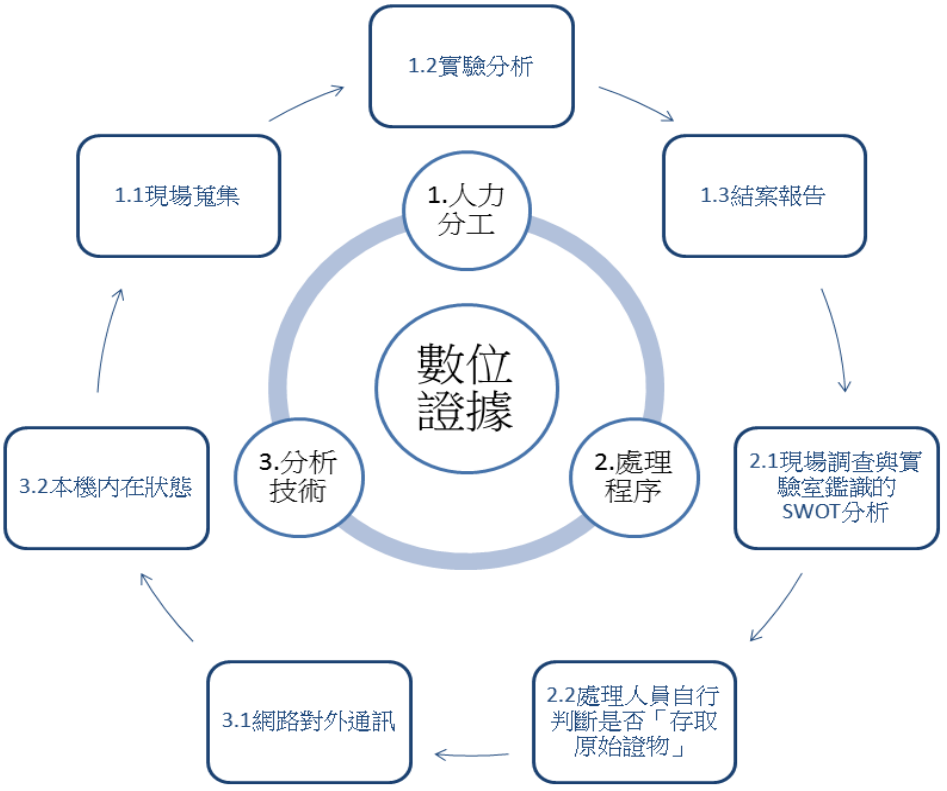


圖 2　數位證據的證物治理策略圖
資料來源：作者整理

一、人力分工

一般刑案電腦會儲存一些數位證據，電腦網路亦為數位證據來源。數位證據的證物治理任務，需要有經費支援，建置實驗鑑識設備（含電腦及手機），補足專業認證訓練，善用現場套裝工具（含防寫設備）蒐集揮發證據。檢查現場電腦取得關鍵證據是必要的，不可能未做證據分類或預覽，便直接送實驗室，這樣的流程不切實際，也無從遵守。再大的實驗室，或再多的人，也無法處理各地送來的大量數位證物，更何況在個案情節、蒐證重點不明狀況下，逐一檢查、蒐尋數位證據，曠日廢時，浪費時間與精力，不具經濟效益。存取證物的人力分工，可從證據蒐集、實驗分析及結案報告等三方面，分工處理，各司其職，妥適因應。

（一）證據蒐集

保存證據為進入現場後的首要工作，對於網路犯罪案件中脆弱的數位證據（digital evidence）尤其重要，數位證據隨時可能因鍵盤或滑鼠的執行動作而改變。這些證據如果處理不當可能使得證物毀損，資料無法讀取，致無法證明罪犯犯罪的事實，面臨無證據能力的命運。所以，到現場的第一步，就要控制現場，開始記錄時間與進行偵查及鑑識人員對證據的操作，管理證物鏈（chain of custody）。

1.適當人力

面對單一網路犯罪案件，應當針對案件的大小分配適當的人力，避免於小案件中投入過多人力，遭成人力浪費，反而增加調查的複雜度；亦應避免於大案件中投入不足人力，造成偵辦困難的情形。

2.專業分工

透過培訓專業、專業分工、協同互助及外援輔助機制，善用人多勢眾（strength in numbers）優勢，進行證據蒐集、實驗分析、結案報告等不同工作任務。例如：「封裝與標籤」程序的執行人員，可由訓練有素且最具經驗的一名調查人員進行，避免重要證據於蒐集、保存、傳遞的程序中出現由不同人員執行而產生疑義、矛盾或衝突。

3.快速蒐證

證據蒐集，須事先了解個案，於規劃時地內，快速蒐證，根據搜索內容，判斷是否扣押證物，移送嫌犯。如果數位證物沒有當下分類（triage）或預覽（preview），將無從判斷下一個偵查作為。由於證據動態性問題，不同時間點的數位證據不盡相同，蒐證者需釐清當下釐清基於何種因素，採用何種蒐證方法，並描述那些數位資料，蒐證結果呈現變動現象，乃蒐證過程的必然結果。

（二）實驗分析

1.工具多樣

數位鑑識工具，並非全能、有解。資通訊科技的不斷進步，工具、技術不斷演進，開發廠商不願意公開加密技術、設計邏輯與軟體內涵，數位鑑識工具往往不能處理新版本的證物內容，尤其是智慧手機鑑識，更是如此，僅能處理舊版本的數位資料。在鑑識工具未能足以蒐證或及時更新之際，善用商用軟體、開放原始碼、免費工具或資安滲透工具等多樣化工具解析證物，以交叉比對證物內容，已日漸被執

法機關及法院所接受。但因有變動部分數位證據的後遺症，這也使得文件化變動證物的描述與說明，更顯重要。

2.證據保全

如果司法機關未能提供足夠的數位鑑識人員，或執法人員的電腦資訊知識不足，則可委由專門從事數位鑑識的公司或機構，指派數位鑑識人員參與證據保全工作，但一般電腦資訊專家未必具備鑑識程序的證據觀念。

3.證據處理

人員的核心認知、知識及技巧需要包含數位證據的識別、收集、獲取及保存。數位鑑識處理人員針對各種不同的作業系統、檔案系統、套裝軟體、通訊協定與網路環境進行解讀時，可運用蒐尋工具，蒐尋電腦內部重要檔案或證據，對於電腦物證的任何稽核資料或其它紀錄之處理方法、過程與分析結果，不得因執行人員之不同，產生不同的分析處理結果。

（三）結案報告

1.淺顯易懂

調查任務中，數位證據產物成為主要輸出資訊，為避免遺漏重要資訊，要將相關數位證據列於報告內。報告須用清楚文字、簡明撰寫、淺顯易懂，讓不懂事件調查技術的法庭人員、原告、被告、律師、或員工等聽眾，均能理解、明白。報告須注意錯誤結果的可能產生後果，須詳細闡明收集哪些潛在證據，使用哪些分析技術，考量哪些情況，產出哪些結果。結果須排除掉可能的替代解釋，能清楚陳述、探究證據的來源、成因與嫌犯關係。

2.專業可信

專家所作的證言要基於客觀、事（真）實，且是經完整的分析過程，不帶有任何直覺、猜測。當發現所作的證言有誤時，要即時向法庭更正，不要因面子問題而不更正。證人的專業、可信度在第一時間就會在法庭上的所有人心中烙下印記，第一印象會影響該證人往後的證言在法官審理過程中形成心證。當面臨激烈的交互詰問時，要保持冷靜，情緒勝過理性時，證人其專業度就會遭疑，故必須忠於專業，不受對方言詞影響（Stephenson, 2014）。

3.出庭說明

數位鑑識為法院訴訟程序上證據之有效力、證明力的重要參考。數位鑑識人員在採證程序上，除須確認合法、公正與完備外，亦須經常出庭為其所發現的電腦數

位證據做說明，提供電腦資訊技術專家證言，作為法院訴訟行為的重要佐證。

4.鑑定證言

鑑定證人具有專業的知識、技巧、經驗，提供的證言來自相關資料、可靠原則及充分事實，產生的結果，採用的原則或方法能應用於該案件事實，可協助法官或審判團辨識證據或判斷事實。新科技所運用的證據調查方法，須普遍可接受(general acceptance)，始能作為法官審理時的參考。法官於採納專家證人之證言可考量下列事項（Stephenson, 2014）：

(1) 科技調查方法背後的科學原理。
(2) 有無標準規範調查之執行方法。
(3) 該方法是否經該領域同儕或公眾檢視。
(4) 已知或可能出錯之機率。
(5) 是否普遍接受。
(6) 結果之解釋是否合理。

二、處理程序

（一）現場調查與實驗室鑑識的 SWOT 分析

數位鑑識分析（digital forensic analysis）可區分現場調查（scene investigation）及實驗室鑑識（lab forensics）兩類，法庭上均有實務需要，但彼此考慮重點不同（Rahman and Khan, 2015），如表 4 之現場調查及實驗室鑑識之數位鑑識分析表。

表 4　現場調查及實驗室鑑識之數位鑑識分析表

考慮重點	現場調查	實驗室鑑識
主要功效	偵查探索答案	鑑識確認結果
主機狀態	開機（power on）	關機（power off）
標的內容	主記憶體內容 （primary memory）	數位儲存媒體 （digital storage media）
所在地	犯罪現場 （crime scene）	鑑識實驗室或辦公室 （at lab or office）

資料來源：作者整理

1.現場調查（scene investigation）

現場調查，針對開機狀態的動態證據，著重偵查探索答案，乃在犯罪現場(crime scene)，於開機（power on）狀態下，可透過不同操作與技術，針對主記憶體內容

（primary memory），作開機動態調查（live investigation），快速蒐集揮發性證據之智慧情資，但會變更原始證物、缺完整性、無法重作。在正式處理資料之前，必先對現場進行拍照或錄影。關掉電腦電源並非是在現場所要做的第一件事，因為立即關掉電腦電源將無可避免的會使得正在記憶體中運行的程式與資料流失，這有時就會破壞到證據。例如當我們在調查嫌犯是否進行阻絕服務攻擊（DoS, Denial of Service）時，遽然關掉電腦電源，就會使得程式與網路連線中斷，之後就算在嫌犯的硬碟中發現相關的程式，也會使得證據的證明力減低，使得嫌犯有機會加以否認。

2.實驗室鑑識（lab forensics）

實驗室鑑識（lab forensics），針對關機狀態的靜態證據，著重鑑識確認結果，在鑑識實驗室或辦公室（at lab or office），於關機（power off）狀態下，透過數位鑑識工具，針對數位儲存媒體（digital storage media），作關機靜態鑑識（dead forensics）分析，可重複檢驗證物，具資料完整性，法庭接受度高，但費時處理，會因待驗證物過多形成積案如山（backlog），難以負荷。

（二）處理人員自行判斷是否「存取原始證物」

鑑識實驗分析工作，往往由另一批未至現場的專業人員擔任。從了解案情、映像檔備份、資料復原、關鍵字蒐尋及現場重建等一系統分析證物下來，曠日廢時，未能快速、有效率的處理證物，往往導致待驗證物的快速累積，不利訴訟進行。現場調查及實驗室鑑識的存取原始證物比較表，分析如表 5。

三、分析技術

數位調查任務須分析大量具差異性或複雜性資料，數位證據的檢驗和分析，尋求數位證據的結果呈現與現場重建，現場重建乃將被損毀或刪除的數位證據回復，以釐清犯罪的手法與動機。面對資安事件的第一時間反應者，可將 NirSoft 或 Sysinternals 等套裝工具組，自行籌組成實際需求的批次檢查檔，並區分「網路對外通訊（network-based communication）」及「本機內在狀態（host-based status）」2 部分（Brooks, 2015），以檢查系統狀況，並匯出報告資料備查。現場調查（scene investigation）的動態分析，以網路對外通訊為蒐證重點，具偵查功效，卻破壞證據完整性，且無法重複檢驗。實驗室鑑識（lab forensics）的靜態分析，本機內在狀態重點，亦屬傳統數位鑑識的發展重點，但動態分析可減輕其弱點。調查者同時存在兩種需求，這兩類可按實際需要互補不足（Rahman and Khan, 2015），如表 6 之 SWOT 分析。

表 5　現場調查及實驗室鑑識的存取原始證物比較表

數位證據處理	現場調查（scene investigation）	實驗室鑑識（lab forensics）
目的	證據分類（triage）或預覽（preview），快速獲取有用情資	時間（temporal）、功能（functional）及關係（relational）分析，重建犯罪現場
適用人員	第一線調查人員（first responder）	實驗室分析人員（lab analyzer）
原則	可存取原始證物	不可存取原始證物
系統狀態	開機（power-on）、網路（network）、活體（live）或運行（dynamic）狀態	關機（power-off）、本機（host）、死體（dead）或靜態（static）狀態
主要蒐證標的	主記憶體內容（RAM）、揮發性資料（volatile）	數位儲存媒體（ROM/Disk）、非揮發性資料（non-volatile）
所在地	犯罪現場（crime scene）	鑑識實驗室（forensic lab）
可能問題	變更原始證物、無法信賴（trustworthiness）	積案如山、待驗證物過多（backlog）
各界學說支持	(1)2000 年美國聯邦調查局的標準原則（FBI's standards principle） (2)2002 年徵求意見書（RFC）3227 (3)2012 年 ISO/IEC 27037:2012	(1)2001 年數位鑑識研究研討會（DFRWS） (2)2004-2008 年美國國家司法研究院（NIJ）和司法部（DoJ）
綜合意見	(1)1999-2014 年數位證據科學工作群組（SWGDE） (2)2007-2012 年英國警察學會（ACPO）	

資料來源：作者整理

表 6　現場調查與實驗室鑑識的 SWOT 分析

分析重點		現場調查	實驗室鑑識
內部因素	優點	快速蒐集智慧情資	完整性、可重複檢驗
	缺點	缺完整性、無法重作	費時處理、蒐證效率不彰
外部環境	機會	揮發性證據	法庭接受度高
	威脅	蒐證品質不一，喪失信賴性	積案如山（Backlog 待驗證物過多）

資料來源：作者整理

陸、結論

建立明確的「保存但不變更任何證物」數位鑑識標準，不僅和其他傳統鑑識原則相悖，在法律的層面上也十分危險。遵守這樣的標準，在犯罪現場、智慧手機或雲端環境等情況下，根本不可能把這樣的標準當成最好的做法，只會使調查程序招受批評。綜合各組織資安管理（尋求快速回復的正常運作）或鑑識執法（尋求蒐集證據的事件還原）的需求觀點觀察，各有不同需求，主張自然相異。值此網路犯罪國際化時代，以合理、合法、效率方式蒐集事證，運用受認證、肯定、有效的鑑識工具、方法，同時滿足系統管理、鑑識執法目標，抑或現場調查、實驗室鑑識的不同場域之需求是困難的。為降低意見衝突，尋求獲致共識，授權有能力的執行檢查者自行因時因地制宜的檢查方法，是否存取原始證物，得按實際需要自行判斷，記錄處理過程，適當說明解釋。要達到此目的，檢查人員的處理程序須光明正大，判斷決定須坦率正當，處理程序的根本原因或邏輯依據，要合理且有紀錄可循，讓公正第三方專家亦得事後審視驗證，使受害者與受審判者雙方皆能夠心服口服。。

以執法機關而言，每天均要處理大量案件，應於接觸嫌犯的當下，檢查關鍵標的數位證物，使第一時間到場的員警，可以洽詢嫌犯或被害人，進一步快速、立即深入蒐集相關數位事證。透過現場調查可以解決約百分之九十的案件，用現場檢驗技術，找出關鍵證物，取得揮發性證據，期於現場快速處理，降低實驗室的大量積案負擔，據以究辦、起訴被告，盡快結束調查。若能快速找尋部份證物，讓嫌犯當場承認，以利後續移送程序，故應於現場處理積極取證。儘管直接存取原始證物會面臨變更部分數位資料，影響某些證物的完整性、重複檢驗性。但為能取得揮發性記憶體資料、快速取得關鍵證據、縮短案件偵查時間、獲取有效人供證言、降低實驗室積案、回歸傳統鑑識科學規範等因素考量，專業蒐證人員可於嫌犯在場、現場錄影蒐證、保存蒐證過程，並由鑑定證人於蒞庭時陳明經費、技術或現實考量下的存取原始證物，乃依據符合執法機關之證據分類或預覽的最新妥適調查作法。這樣的解套作法，符合美國數位證據科學工作群組（SWGDE）及英國高級警官協會（ACPO）的數位證據實作原則，亦可完成處理數位證物的萃取證據任務。

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

ACPO (2012), "ACPO Good Practice Guide for Digital Evidence," UK: Association of Chief Police Officers,pp. 6-12, <http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf >

Aljaedi, A., Lindskog, D., Zavarsky, P., Ruhl, R., and Almari, F. (2011), "Comparative Analysis of Volatile Memory Forensics: Live Response vs. Memory Imaging," 2011 IEEE Third International Conference on Social Computing (Socialcom), pp. 1253-1258.

Brooks, C. L. (2015), CHFI computer hacking forensic investigator, New York : McGraw-Hill Education, pp. 1-50.

Cantrell, G (2012), "Implementing the Automated Phases of the Partially-Automated Digital Triage Process Model," Digital Forensics, Security and Law, 7(4), pp. 99-116

Casey, E. (2011), Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition, MA: Elsevier Academic Press, pp. 19-21.

Gianni, F., and Solinas, F. (2013),"Live Digital Forensics: Windows XP vs Windows 7," 2013 IEEE Second International Conference on Informatics and Applications (ICIA), pp. 1-6.

Hay, B., Nance, K., and Bishop, M. (2009), "Live Analysis: Progress and Challenges," IEEE Security and Privacy, 7(2), pp. 30–37.

ISO/IEC (2012), "ISO/IEC 27037:2012 - Information Technology: Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence," Switzerland: ISO Office, pp. 6-27.

ISOC (2002). "Network Working Group-Request for Comments 3227-Best Current Practice- Guidelines for Evidence Collection and Archiving," Switzerland: The Internet Society, pp. 1-5, <https://tools.ietf.org/pdf/rfc3227.pdf>

Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., and Wright, C. (Eds.) (2007), The Official CHFI Study Guide (Exam 312-49): For Computer Hacking Forensics Investigators, MA: Syngress Publishing, pp. 1-14.

Mrdovic, S., Huseinovic, A., and Zajko, E. (2009), "Combining Static and Live Digital Forensic Analysis in Virtual Environment," 2009 IEEE ICAT XXII International Symposium on Information, Communication and Automation Technologies, pp. 1-6.

NIJ (2004), Forensic Examination of Digital Evidence: A Guide for Law Enforcement, DC: National Institute of Justice, pp.1-2.

NIJ (2008), "Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition," DC: National Institute of Justice, pp. 15-18, <https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>

Palmer, G. (2001), "DFRWS Technical Report: A Road Map for Digital Forensic Research," First Digital Forensic Research Workshop (DFRWS), New York: Air Force Research Laboratory, pp. 14-31. <http://www.dfrws.org/2001/dfrws-rm-final.pdf>

Pearson, S. and Watson, R. (2010), Digital Triage Forensics: Processing the Digital Scene, MA: Elsevier Inc., 2010, pp.13-24.

Stephenson, P. (2014), Official (ISC)2® Guide to the CCFP CBK, FL: Auerbach Publications, pp. 293-404.

SWGDE (2014), "SWGDE Best Practices for Computer Forensics, Version: 3.1," Virginia: Scientific Working Group on Digital Evidence, pp. 5-7, <https://www.swgde.org/documents/Current Documents/2014-09-05 SWGDE Best Practices for Computer Forensics V3-1>

SWGDE and ICOE (2000), "Digital Evidence: Standards and Principles," Forensic Science Communications, 2(2), Virginia: Scientific Working Group on Digital Evidence, pp. 1-3, <https://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm/>

Rahman, S. and Khan, M. N. A. (2015), "Review of Live Forensic Analysis Techniques," International Journal of Hybrid Information Technology, 8(2), pp.379-388.

Zang, J. and Mai, Y. H. (2011), "Cloud Computing Environment Simulation Computer Forensics," Netinfo Security, 10, pp.7-12.

Zeng, G. (2014), "Research on Digital Forensics Based on Private Cloud Computing," International Journal of Information Technology (IIJIT), 2(9), pp. 24-29.

Zhang, L., Zhang, D., and Wang, L. (2010), "Live Digital Forensics in a Virtual Machine," IEEE Computer Application and System Modeling Conference (ICCASM), 4, pp. 328-332.