數位鑑識工具的分類與運用：核心程序與

高大宇 / 中央警察大學資訊管理學系助理教授

壹、前言

網路人口日漸攀升，以電腦、網路、行動或雲端等通資科技設備為基礎的不法活動，更加氾濫與難以應付，通資科技相繼成為各種電腦犯罪事件的工具（Tool）、場所（Place）或標的（Target）。面對日益嚴重的通資科技犯罪，數位證據在法律訴訟案件中的運用日趨頻繁，促使數位鑑識工作成為執法機關的努力目標。數位鑑識屬於鑑識科學領域中較新興的跨領域整合性科學，需同時審慎面對鑑識科學、電腦科學、法律程序、犯罪剖繪等不同議題[4]。各式各樣的數位鑑識工具，雖可輔助執法機關調查犯罪事件，但在蒐證的核心程序中，有效地妥適分類、動態運用數位鑑識工具，將可進一步協助處理科技犯罪案件的數位證據，降低數位鑑識實驗室的大量積案問題。

貳、文獻探討

數位證據屬於動態屬性資料的短暫靜態資料，不易保存，處理原則易引發不同立場的爭論意見。本文採用日漸被接受的「第一現場之數位鑑識人員可酌情存取原件」數位證據處理原則，但須遵循「極小化變動修改」、「適當解釋說明必要性」及「存取動作文件化」等規範[1,2,6]。該種主張可概分為「ACPO數位證據的實作指南」及「ISO/IEC 27037:2012標準」兩種。遵循這些指南原則，將更能確保數位證據的可靠性和可信性，提升數位證據在適用法律、執行規範和鑑識要求的完整性。

動態能力研究

一、英國高級警官協會數位證據的實作指南

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南（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[1,2]。

（一）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。

（二）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。

（三）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。

（四）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使用拷貝設備拷貝資料都必須遵守法律規範與以上原則。

二、數位證據識別、蒐集、擷取和保存指南（ISO/IEC 27037:2012）

由於每個人對於處理數位資訊的理解與想法不同，使得鑑識作業流程一直無法形成統一見

解，鑑識程序分歧、種類繁多，包含識別、蒐集、保存、檢驗、分析、呈現及結論等程序。國際標準化組織（ISO，International Organization for Standardization）及國際電工委員會（IEC，International Electrotechnical Commission）於2012年共同發布的ISO/IEC 27037:2012資訊安全標準，提供數位鑑識人員一個核心的、可靠的數位證據採證流程，如圖1[6]。

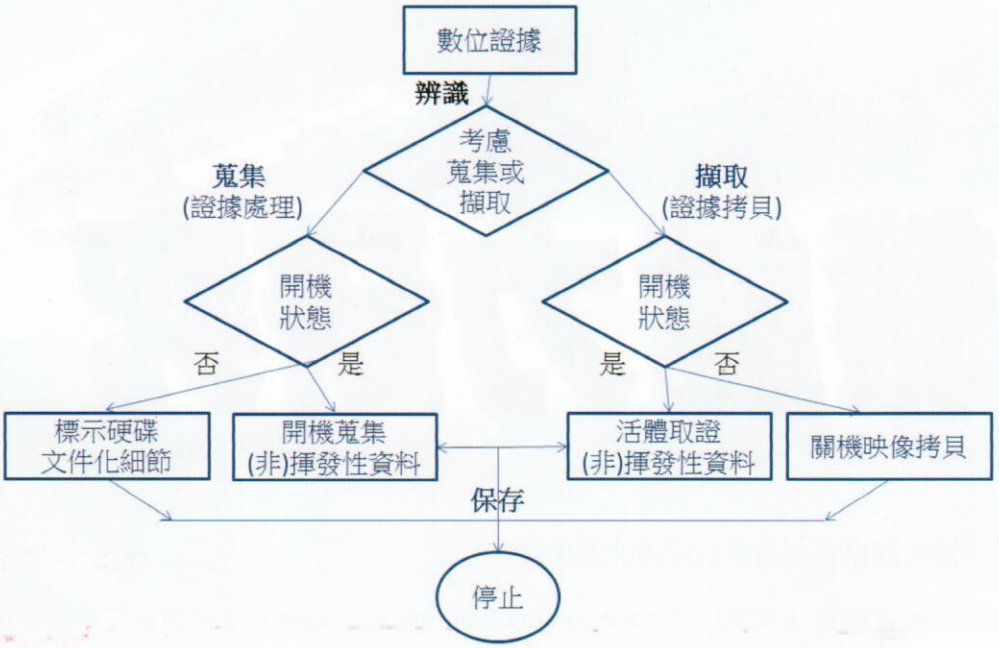

圖1、數位鑑識人員一個核心的、可靠的數位證據採證流程

參、數位證據的核心程序與動態能力

目前在數位鑑識領域的討論，著重在工具、方法、定義、標準、道德以及其他在此發展領域中的基礎觀念[3,4]。從一個數位設備或裝置內取證時，應透過適當科技擷取數位證據，引用與解釋相關電腦及鑑識科學的基本原理。例如，活體取證（Live Acquisition）之最小變動原始證據（Original Evidence）原則，如同指紋與DNA鑑定一樣，具不可重複性且會變動原始資料。

一、數位證據的核心程序

2012年發布的ISO/IEC 27037:2012標準，被歸類為屬於《資訊科技 – 安全技術 - 數位證據識別、蒐集、擷取和保存指南》的國際標準，涉及數位證據的識別（Identification）、蒐集（Collection）、擷取（Acquisition）和保存（Preservation）等四項核心程序議題[6]，提供具體指導的指導原則，如表1。

（一）識別關鍵的稽核紀錄

識別的作用在於瀏覽現場，找尋可為證物之數位（Digital）和非數位證物，識別過程包括進行辨識（Recognize）、尋找（Find）、或搜尋（Search）數位證據。識別數位證據的過程中務必注意稽核記錄的網路位址（IP Address）、時間戳記（Date-Time Stamp）、數位動作（Digital Action）、回應訊息（Response Message）等四項要件，鎖定涉案嫌犯，如表2。

表1：數位證據核心程序的內容與重點

編號	核心程序	程序內容	程序重點
1	識別	識別關鍵的稽核紀錄	數位和非數位證物
2	蒐集	速度準確的證據蒐集	揮發性和非揮發性資料
3	擷取	即時反應的擷取資料	實體和邏輯擷取
4	保存	法律訴訟的證據保存	完整性和真實性

表2：追查嫌犯的稽核紀錄四要件

編號	要件	理由	目標
1	來源網址	追查來源電腦帳號或電話號碼	鎖定涉案嫌犯的犯罪行為
2	時間戳記		
3	數位動作	檢查犯罪構成要件的該當或合致	
4	系統訊息		

（二）速度準確的證據蒐集

蒐集程序，首重證據蒐集的先後次序，識別數位設備之開機（系統電源開啟）或關機（系統電源關閉）狀態後，根據情境、成本和時間等實際情況決定採用最合適的蒐集或擷取方法。數位證據依其消逝速度，可分為揮發性資料（Volatile Data）和非揮發性資料（Non-volatile Data）。揮發性資料為開機狀態的即時資訊，如網路連線狀態、記憶體資料等，在電源拔除後，這些資料會消逝而無法蒐集。非揮發性資料乃儲存於媒體的資料，如安全稽核記錄、系統相關組態設定，在移除電源後，資料仍可從媒體中蒐集。由於拆卸數位設備電源或關機，儲存媒體內的非揮發性資料會被保留，但部分揮發性資料會消失，因此如果調查案件需要揮發性資料時，就要適用「揮發性優先」原則。揮發性資料包括隨機存取記憶體（RAM，Random Access Memory）、虛擬交換空間（Swap Space）和正在執行程序（Running Processes）等。為保存證據，數位鑑識第一線處理人員，必須能分辨、及時蒐集揮發性資料，同時應詳細記錄蒐證過程，確保所蒐集之資料具有證據能力。

（三）即時反應的擷取資料

擷取程序，將數位證據資料製作成完全相同的位元映像檔副本（bit stream copy），同時記錄所使用的方法和動作，維持證物鏈完整性。擷取程序分為實體擷取（Physical Acquisition）和邏輯擷取（Logical Acquisition）二類。實體擷取能完整複製儲存媒體，會複製已刪除資料和未配置空間資料。邏輯擷取只擷取檔案系統的已配置空間和標示為檔案的資料。

（四）法律訴訟的證據保存

證據保存，保存過程始於蒐集階段終於案件偵結。證據保存過程，要保持證物鏈（Chain of Custody）的完整性（Integrity）和真實性（Authenticity），應保護已蒐集數位設備和數位證據，免於從漏失、竄改或損毀。保存程序，應注意下列事項[4,6]：

1、應根據情境、成本和時間等狀況，採納合適的證據保存方法。

2、應明確詳細記錄，決定使用某種數位鑑識工具方法和執行活動的原因及理由。

3、應以最少變動方式來獲得資料，避免造成變更。若處理方式會改變部分數位資料的話，應記錄執行活動過程，說明資料被變更的緣由。

這四個核心程序構成一有系統的證據採集流程，同時確保證物鏈的完整。遵循該指南將更能確保數位證據的可靠性和可信性，提升數位證據在適用法律、執行規範和鑑識要求的完整性，來處理各種技術議題，具體電腦犯罪調查實作的實務指南、指導原則。可見ACPO數位證據實作指南四項原則的基本概念與內涵，亦被ISO/IEC 27037:2012標準接受與採用。

二、數位鑑識的動態能力

「工欲善其事，必先利其器」，現有數位鑑識工具的多樣化，常使執法人員困擾於何種情境該使用那些工具，作為蒐集數位證據的利器。本文依據ISO/IEC 27037:2012標準的論點，將數位鑑識工具區分「開機鑑識」及「關機鑑識」兩種探討，透過數位鑑識工具的利用與研究，審酌網路鑑識、行動鑑識及電腦鑑識等不同個案情境，輔以事前蒐證（蒐集事證）、事中取證（網路鑑識）及事後驗證（電腦鑑識）的階段性工作，提出適合我國警察執法環境的可行程序[5]，如表3，說明如下：

（一）事前蒐證階段（蒐集事證）

1、網路管理者，平時就應利用適當工具監控電腦的活動狀態，蒐集、紀錄各個動作的執行，發生異常事件時可交付給稽核（或執法）人員，進行後續行動，適合一般民眾於私人企業組織使用的數位鑑識工具。

2、探討蒐證前必要的準備工作，包含警覺（Awareness）、授權（Authorization）、計畫（Planning）、通知（Notification）、搜尋和辨識證據（Search for and identify evidence）。

3、事前擬定可疑犯罪事件調查計畫，當一個事件正在進行，應依據當時情勢，執行蒐證作為，利用照相、錄影或文件化等方式，保存事件資料或稽核紀錄。

表3：數位鑑識工具的分類運用表

階段	事前蒐證階段	事中取證階段	事後驗證階段
重點能力	蒐集事證	網路鑑識	電腦鑑識
鑑識方式	開機鑑識	開機鑑識	關機鑑識
適用對象	網路管理者（使用者）	現場鑑識人員	實驗室管理人員
數位鑑識工具	1.網路鑑識監控系統 2.電子郵件分析調查 3.無線/有線網路鑑識分析 4.網路即時通訊分析 5.網路行為鑑識分析 6.作業系統的記憶體擷取分析	1.網路封包鑑識工具 2.電腦主機校驗系統 3.情資萃取工具組 4.動態擷取工具組	1.電腦鑑識工具，如EnCase、FTK） 2.手機鑑識工具，如Cellebrite、XRY 3.資料救援工具，如硬碟救援、檔案救援、破密工具

（二）事中取證階段（網路鑑識）

1、現場處理人員，應利用即時活動檢查工具採證，蒐集網路狀態、瀏覽器暫存紀錄、郵件暫存訊息等網路活動資料。適合一般警察人員於犯罪現場使用的數位鑑識工具。

2、探討取證過程，包含蒐集證據（Collection of evidence）、運送證據（Transport of evidence）、儲存證據（Storage of evidence）及檢查證據（Examination of evidence）。

3、數位設備處於開機情況下，執行必要的活體取證（Live Acquisition），從開機狀態下進行現場資料取證，擷取揮發性資訊（Volatile Information）或網路狀態（Network Status），找到或恢復有價值的即時資訊。

（三）事後驗證階段（電腦鑑識）

1、實驗室管理人員，應進行專業的鑑識，如檔案系統的檔案分析、還原等，適合專業警察鑑識人員於實驗室使用的數位鑑識工具。

2、取證後在法院的審判流程，包含提出假設（presentation of hypothesis）、驗證或反駁假設（proof/defense of hypothesis）及分送資訊（dissemination of information）。

3、數位設備處於關機情況下，使用經過驗證的映像工具執行映像拷貝過程，執行關鍵字搜尋及資料復原等工作程序。

肆、數位鑑識工具的分類與運用

數位鑑識議題日漸受到重視，各資訊公司無不卯足全力設計數位鑑識工具軟體。Encase、FTK等主流的鑑識軟體，頗受各國司法單位信任。面對日新月異的科技，商業軟體可能會無法支援新的硬體、作業系統等，且由於工具軟體所費不貲，在預算有限的情況下，執法單位可能無法即時購置，缺乏彈性。因此本節依表3的分類提出適合事前蒐集事證、事中網路鑑識及事後電腦鑑識的數位鑑識工具，探討適合（或訓練）警察人員數位鑑識工具。

一、事前蒐集事證：適合網路管理者

適合網路管理者（使用者）之蒐集事證工具如下:

（一）網路鑑識監控系統

提供側錄網路封包內容，包含網路服務協定：郵件、網頁郵件、檔案傳輸、即時通訊、網頁、社群網站等。將Email封包（POP3、SMTP、IMAP、Webmail）、FTP封包、Instant Message封包（ICQ、Yahoo Message等）、Website封包、Telnet封包等進行解譯還原。

（二）電子郵件分析調查

能迅速對電子郵件建立索引以搜索引擎和獨特的視覺方式呈現，讓調查人員能夠快速搜索和審查電子郵件和電子儲存訊息，找到關鍵數據，可視覺化的相關關係，擷取最相關之證據。

（三）無線/有線網路鑑識分析

能支援無線網路、支援無線加密協議（WEP，Wireless Encryption Protocol）解密資料。

（四）網路即時通訊分析

可產出易於閱讀理解之即時通訊軟體報告。可簡便迅速搜索和分析即時通訊，網路瀏覽器和各種郵件、即時通訊之歷史紀錄、聯絡人資料。

（五）網路行為鑑識分析

可選擇聯絡人檢視對話記錄，分析即時通訊、網路瀏覽器之歷史紀錄、聯絡人資料。

（六）作業系統的記憶體擷取分析

表4：可擷取之記憶體

1、處理程序、驅動程式、模組	4、已開啟的檔案
2、已建立的網路連線	5、每個處理程序所開啟的登錄編輯器鍵值
3、等待連線的通訊埠	6、還原金鑰鍵值、密碼及網路歷史活動

二、事中網路鑑識：適合現場鑑識人員

為使現場處理人員，依據不同狀況，選擇不同的模式，擷取、分析行動裝置、瀏覽器、電腦硬碟等資料，進行證據蒐集，須有簡便易攜的工具包，提供經常使用的數位鑑識工具。適合現場鑑識人員之事中網路鑑識工具與功能。

表5：網路鑑識工具與功能

工具名稱	功能
（一）Diamond A-PacketMan網路封包鑑識工具	可動態即時顯示封包內容、偵測未知（異常）通訊程式。
（二）S-Check電腦主機校驗系統	可校驗電腦系統檔案，是否已經被遭到攻擊，而留下惡意程式，或異常通訊等。
（三）ADF Solutions-Triage-G2情資萃取工具組	可掃描Windows、 Macintosh 及 Linux等電腦，快速取得單一設備重要資訊。
（四）Helix3 Pro動態擷取工具組	可搜尋圖形、文字等檔案擷取及分析Window及UNIX系統的即時資料。

三、事後電腦鑑識：適合實驗室管理人員

表6：電腦鑑識工具與功能

工具種類	主要功能	
（一）電腦鑑識工具	EnCase Forensic數位鑑識軟體、FTK專業電腦鑑識軟體。	
（二）手機鑑識工具	Cellebrite UFED Touch Ultimate Ruggedized Kit手機內部實體資料手機物理取證器、Cellebrite中國山寨手機內部實體資料擷取硬體設備、XRY 智慧型手機裝置鑑識設備。	
（三）資料救援工具	1、硬碟救援	專業硬碟壞軌暨Firmware損毀資料救援工作平台、專業硬碟開盤工具平台（硬碟開盤暨磁頭及碟片更換工具平台）
	2、檔案救援	GetData Recover My Files、Eraser或Diskinternals 檔案復原套件、Adroit Photo Forensics圖片救援工具
	3、破密工具	PasswareKit Forensics Version電腦密碼鑑識工具、Elcomsoft iOS Forensic Toolkit密碼鑑識工具組
	4、管理環境	（1）證物管理系統：數位證物的收案、編碼、控管、追蹤、稽核、結案之證物管理系統，進行案件證物鏈控管，並具備帳號管理、新增、更新、刪除、查詢、列印等基本功能。 （2）鑑識分析主機：輔助電腦（手機）鑑識工具的分析處理。 （3）虛擬化軟體：VMWare Workstation 11.x虛擬化軟體減少處理過程的Metadata資料變動。 （4）複製設備：硬碟映像檔複製機設備、VFC3映像檔開機設備。

伍、結論

本文嘗試以實務工作面臨的困難與挑戰，提出具有彈性和節省機關成本等優點的數位鑑識分類，希望對第一線執法人員有所幫助。任何數位鑑識策略的擬定，在不同環境下，都應有不同的作法，亦即數位鑑識策略與所處環境必須要能相互配合，才能產生效果，再好的策略放在不適合的環境下都無法產生功效。現場直接進行證據蒐集及簡單的分析不只可以加快偵辦案件的速度，也可以蒐集到更多的犯罪資訊。為使整個數位鑑識的效率提升，本文除遵循「ACPO數位證據的實作指南」及「ISO/IEC 27037：2012標準」外，也適當改變數位鑑識的分類、分工角色。在時間、工具及資源有限的情境下，受適當教育訓練的第一現場的數位鑑識處理人員，

可以選擇恰當的軟體工具蒐集證據、製作蒐證紀錄、及到庭解釋採證過程。必要時，再交由後續專業的數位鑑識實驗室分析。警察執法機關採用此分類分工作法，將可處理大量通資科技犯罪案件，並具有下列優勢：

1、第一時間檢查關鍵通資科技設備證物，取得嫌犯或被害人的（無修飾）證詞。

2、約百分之九十案件，可於現場檢驗揮發性及非揮發性證據，找到關鍵資訊。

3、於現場處理，找到部份重要證物資料，讓嫌犯承認犯行，以利後續移送程序，盡快結束調查，起訴被告。

4、現場快速處理，減低數位鑑識實驗室的大量案件負擔，降低壓力，使堆積的待驗鑑識案件減少，讓實驗室專注處理一些較棘手的案件。

誌謝

本研究蒙103年李昌鈺博士物證科學教育基金會補助研究經費，特此誌謝。FACT

參考文獻

1.ACPO, "2007 Good Practice Guide for Computer-Based Electronic Evidence," Retrieved December 29, 2014, from http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf。

2.ACPO, "2012 ACPO Good Practice Guide for Digital Evidence," Retrieved December 29, 2014, from http://www.acpo.police.uk/documents/crime/2011/201110-cba-digital-evidence-v5.pdf

3.Casey, E., Handbook of Digital Forensics and Investigation, NY: Elsevier Academic Press, 2010, pp. 215-356.

4.Casey, E., Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed, Elsevier Academic Press, 2011.

5.Ciardhuáin, S. Ó., "An extended model of cybercrime investigations. International Journal of Digital Evidence," Vol. 1, Issue 4, 2004, pp.1-22.

6.ISO/IEC 27037:2012, "Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence," Retrieved December 29, 2014, from http://www.iso.org/iso/catalogue_detail?csnumber=44381。