

政府機關電子檔案管理與 電腦鑑識

Electronic Records Management and Computer Forensics in Government Agencies

許芳銘 Hsu, Fang-Ming
國立東華大學資訊管理學系教授
Professor, Department of Information Management,
National Dong Hwa University
E-mail: fmhsu@mail.ndhu.edu.tw

范秋足 Fan, Chiu-Tsu
東南科技大學企業管理學系助理教授
Assistant Professor, Department of Business Administration,
Tungnan University
E-mail: jofan@mail.tnu.edu.tw



摘要

資訊時代中，社會各角落已逐漸擁有大量以數位型式存在的資料。這些資料記載著各式活動的紀錄，普遍儲存於政府機關與人民生活中。鑑於數位證據的脆弱，檔案管理局已大力推動各式電子檔案的保存規範。然而在法庭的證據力要求下，當電子檔案被破壞或發生資訊安全事件時，如何重建數位證據以恢復原始的活動事實，就成為很重要的課題。電腦鑑識的興起，正是要彌補這部分的管理需求。本文探討電子檔案管理與電腦鑑識兩者之間的雷同之處，並說明電腦鑑識之內容，以供我國政府機關檔案管理人員在推動電子檔案管理相關業務時之參考。

Abstract

There is huge amount of digital data with various formats in the information era. The data recording various activities is stored in the public and government agencies. Owing to the fragility of digital evidence, National Archives Administration has promulgated a number of regulations related to electronic records management for better preservation. However, for satisfying the requirement of judicial evidence to courts, how to restore destroyed data becomes a big issue for information security. Computer forensics can amend the gap of management between the two perspectives. Thus, this study discusses the similarity between electronic records management and computer forensics. Meanwhile, the content of computer forensics is introduced to government records managers and archivists for promoting electronic records management.

關鍵字：電子檔案管理、電腦鑑識、資訊安全

Keywords: Electronic Records Management, Computer Forensics, Information Security



緒論

在高度資訊化的時代，使用電腦來完成文書檔案管理作業以及聯絡溝通，已成為現代人日常活動之一。因著電腦與網路成為人類生活中的重要工具，因此它們也可能成為詐欺、偽造與經濟犯罪的幫兇。在資訊時代中，「凡走過必留下痕跡（footprint）」，故此，電腦與網路等電子設備，極仍可能儲存著犯罪上的重要歷程紀錄。這些證據資料都是儲存於電腦及其週邊設備中，而且經常以數位型式存在，因此就稱之為「數位證據（digital evidence）」。然因過去大眾較不注意數位證據的保存與維護，所以在面對數位資訊相關法律與證據問題時，常常無法還原原始的真相。

在現今時代，因為檔案管理中的數位資訊是寶貴且有價值的，所以經常成為有心人士覬覦的對象，這就使得檔案管理專業人員也必須試著去瞭解主要用於保護與重建電子檔案的「電腦鑑識（computer forensics）」知識。在ISO 15489國際檔案管理標準中，揭示電子檔案管理作業之目標在於確保其資料之真實性（authenticity）、完整性（integrity）、可靠性（reliability）、可用性（usability）與可及性（accessibility），以使得檔案不僅成為組織之重要紀錄，也可成為事務活動的證據。然而電子檔案必須依附於儲存媒體與相關的資訊系統，方可被保存與閱讀。因此在電子檔案的保存過程中，使得電子檔案管理作業強烈地與資訊系統息息相關。這個依附關係（dependency）益然增加電子檔案的揮發性（vulnerability）以及脆弱性（fragility）。

隨著科技的進步，電腦帶來的諸多便利，卻也造成許多高科技犯罪的可能，數位證據就成了在資訊時代中用以指證犯罪行為的重要證據。數位證據包含任何存在於數位媒體中與犯罪有關的資訊。數位證據可發現於電腦本身、數位科技產品、儲存媒體與其他相關電腦設備。這些儲存體包含各式電腦、電腦硬碟、外接式硬碟、隨身碟、快閃記憶體（flash memory）、磁碟片、CD光碟片、DVD光碟片、隨機存取記憶體（random access memory，簡稱RAM）、快取記憶體（cache）、電子郵件、語音郵件、簡訊、網頁瀏覽紀錄、數位相片、數位攝影機、個人數位助理（personal digital assistant，簡稱PDA）、iPod、錄音筆、MP3播放器、呼叫器（pager）、手機、智慧型手機、印表機、傳真機、硬體防火牆、全球定位系統（global positioning system，簡稱GPS）之追蹤、網際網路服務業者（Internet service provider，簡稱ISP）之客戶連線紀錄以及信用卡刷卡機之刷卡紀錄等。因為數位證據具有不易取得、易被消滅與易被竄改的特性，因此在資訊安全事件發生後，如何保存相關的數位證據，就成為一個重要的課題，電腦鑑識因而應運而生。

電腦鑑識又稱為數位鑑識（digital forensics），它藉由一套完整的識別證據、擷取證據、保存證據、分析證據以及呈現證據的方法，以協助機關進行相關犯罪行為鑑識及採證，因此常見於保存證據之資訊安全領域。資訊安全的重點在於避免非法與惡意的入侵與破壞，而電腦鑑識則是探討有關電腦應用與法律的議題，運用電腦技術分析、擷取並解釋從電子媒體上所採集的數位證據，以取得法律上的效力。電腦鑑識的概念源自電腦網路保安與及刑事偵查，主要是在發生資訊安全事件之後，作為調查電腦犯罪，尋找相關證據之行為。電腦鑑識的範疇主要在於當公司或個人遇到資訊相關緊急事故時，應用嚴謹的程序及科技的方法去處理數位資訊設備相關鑑識工作，還原當時事情發生的過程。大部分的資訊犯罪案例中，都會留下數位足跡，因此透過電腦鑑識，以科技的方法，正確蒐集及分析所有的數位資訊證據，透過「一分證據，說一分話（data talk）」的作法，找出跟事件有關聯的資訊證據，還原事情的真相。



數位證據與電腦鑑識

虛擬世界裡的電子紀錄很容易遭到竄改，因此電腦鑑識也必須保護電子證據，確保在鑑識的前後，電子證據並沒有被破壞，這樣鑑識分析之後的證據資料，才能具有可信之法律地位。相較於傳統犯罪之指紋、刀、槍、去氧核糖核酸（deoxyribonucleic acid，簡稱 DNA）等證據，電腦犯罪的偵辦更具難度。數位證據具有以下特性：一、蒐證範圍大：數位資料散布在網路上，範圍浩瀚，或經特殊手法，使得關鍵性資料隱藏在電腦中，故取證不易。二、無法被人類直接閱讀與理解：因為電子設備記錄數位符號，需經由電腦設備與閱讀軟體才能存取這些二進位資料並解讀其符號所代表的意義，因此提高數位證據存取的困難度。三、易於複製及竄改：數位資料的狀態容易被改變，為了能確保數位證據的完整性，以取得數位證據在法庭上的證據力，因此證明所擷取的證據與原始資料相同一致是很重要的。四、不易定位於個人：數位資料並不具備生物指紋及DNA等可作為判斷獨立個體唯一性的證據特質。分析數位資料僅能知道嫌犯在某台電腦犯案，卻難以得知或證明嫌犯是誰。由於數位證據的性質特殊，使得電腦犯罪案件在證據的採集、分析、保存，以及往後法庭上的呈現都比一般刑事案件困難許多。因此，資訊時代發生資安事件時，正確的資料採證程序是保障正當資訊媒介使用者權益的重要證據，或追蹤與起訴犯罪嫌疑者的重要判定佐證來源。

美國司法部所提出之數位證據蒐集流程，如下頁圖1（註1）。

電腦鑑識是一門有效解決電腦犯罪難題的科學，一般將電腦鑑識定義為：「以周延的方法及程序保存、識別、萃取、記載與解讀電腦媒體證據並分析其成因之科學」（註2）。西元1991年，國際電腦調查專家協會（International Association of Computer Investigative Specialists，簡稱 IACIS）提出電腦鑑識做為電腦犯罪證據蒐證與鑑識的方法，其主要目的在於協助司法人員蒐證網路犯罪案件與犯罪之證據（註3）。當發生資安或犯罪事件時，便可利用電腦鑑識來還原事件的發生過程或擷取已儲存在電腦中的資料，以進一步提供相關證據。首先判斷數位證據可能存在地方，接著在不破壞數位證據的前提下進行蒐集與萃取，其所蒐集與萃取的原始證據或映像檔必須符合嚴謹的保存程序，然後開始進行一連串的研究分析，最後再將分析的結果以完整的鑑識報告方式呈現。

學術上，學者對於電腦鑑識程序有不同的看法。其中，Rude認為電腦鑑識的程序應包括現場鑑識準備工作、快照（snapshot）、移轉（transport）、鑑識準備、調查等步驟（註4）；Kuchta認為電腦鑑識程序應該包含：準備工作、記錄與文件化、收集、驗證（authentication）、分析（analyze）、保存（preserve）、產出結果、報告文件等步驟（註5）；Sinangin則認為電腦鑑識程序包含識別（identify）、取得、保護、分析、呈現（present）等步驟（註6）。基本上電腦鑑識過程應包含識別、保存、萃取（extract）、記錄、分析、解釋（interpret）及呈現電腦媒體資料等步驟。

在蒐集數位證據時，應於犯罪現場找出所有可能成為證據的資訊設備或儲存媒體，例如：外接式硬碟、光碟片、隨身碟等。在檢驗時，因為涉及存取並截取與案情相關的資訊，時常會面臨需要繞過作業系統（operating systems）及應用程式的安全保護程序、存取控制、密碼加密以及資料壓縮等。在輸出相關資料之後，對這些資料進行分析、交叉檢驗及推論，以得到一個資安事件發生的過程及結論。然後，將分析結果及結論製成報告，以便清楚完整地提供給組織管理者、法官或律師做為參考。最後，呈現數位證據

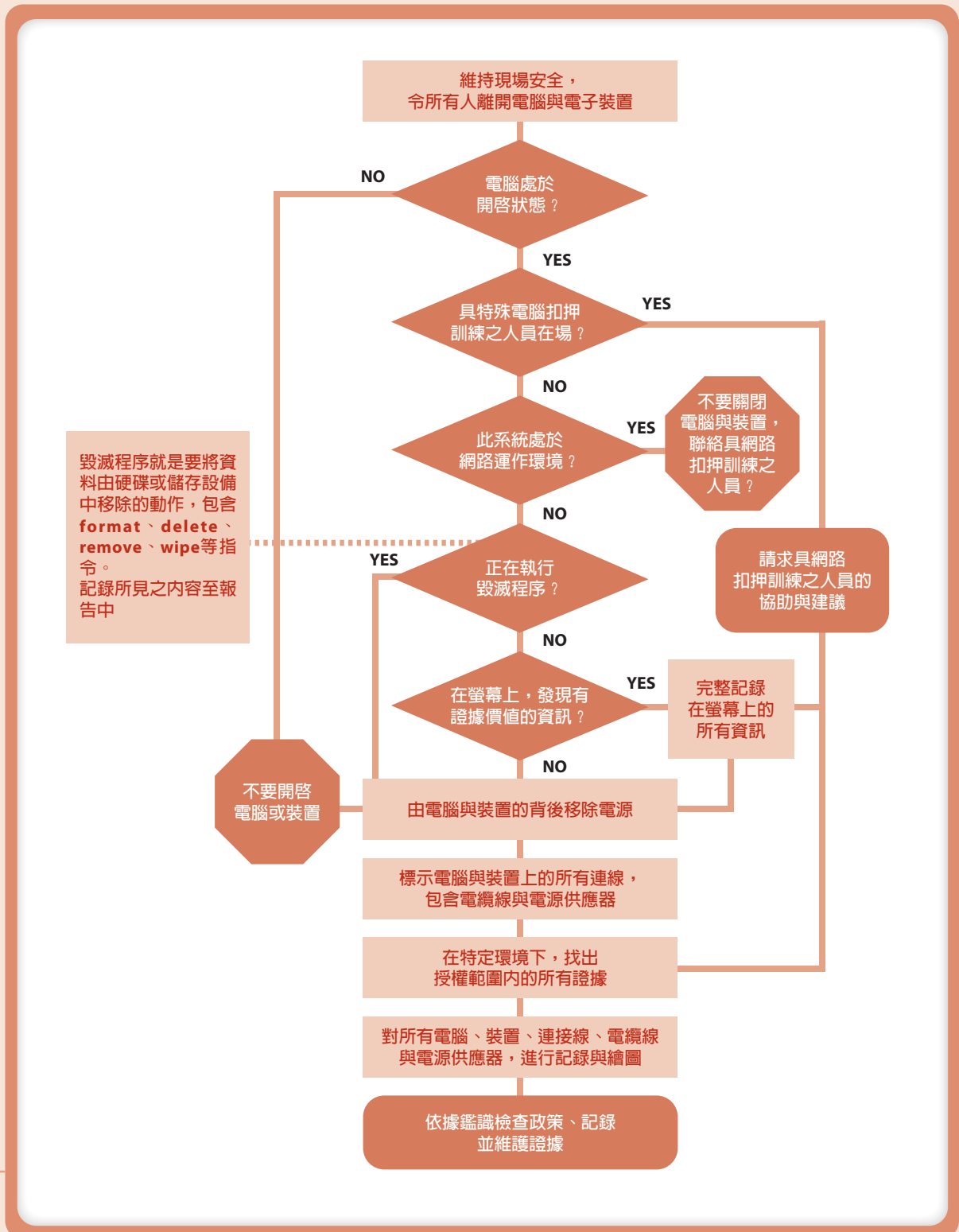


圖 1——美國之數位證據蒐集流程

資料來源：National Institute of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*, Office of Justice Programs, U.S. Department of Justice, (2008).

與報告於法庭中，成為認定事實之基礎，鑑識人員得視案情需要，出庭作證成為專業證人。

電腦鑑識工作所需的工具如下：一、磁碟備份軟體：需具備位元串流（bit-Stream）拷貝的功能，因為一般的複製功能僅能複製檔案總管可以顯示的資料項，而位元串流拷貝卻能完整複製硬碟的使用狀態，把曾經刪除資料的狀態也複製下來。二、檔案還原軟體：可以將已刪除的資料從磁碟中還原。嫌犯為煙滅證據，經常會把重要資料或犯罪工具從電腦中刪去，適當利用還原軟體便能將這些檔案復原，從中找尋犯罪證據。三、密碼破解工具：用來破解基本輸出入控制系統（basic input output system）、作業系統管理員的密碼及以密碼保護之檔案的密碼等。為防止電腦過多的保護措施阻礙了鑑識人員的重要資料蒐集，尤其當嫌犯將犯罪資料以密碼保護的時候，利用密碼破解工具可使得鑑識工作的過程更順利。四、整合性工具：為使鑑識工作更有效率，有些軟體整合了多種數位鑑識需要使用的功能，例如：磁碟備份及還原刪除資料等，以確保資料完整性為考量，具備自動處理鑑定資料產出鑑定文書的功能。常見的整合性工具如Encase等。Encase乃Guidance Software公司所研發的軟體，使得鑑識人員得以協助找出被刻意隱藏、刪除或是遭到覆蓋的電腦檔案，針對電腦、手機、記憶體做特定的鑑識分析，並以簡單快速的方式產出鑑識報告（註7）。除了這些專業工具之外，數位相機、攝影機、筆記型電腦、隨身碟等都是現場採證的重要協助工具的，可用以檢視及儲存數位資料。



電子檔案管理與電腦鑑識之關係

在資訊時代中，凡走過必留下痕跡，這些痕跡可能存在於原始電子設備本身，也可能被其他設備所記載。例如：某人藉由電腦去存取一筆紀錄，則其交易細節包括何時、何地、何筆紀錄、做了何事等都將被記錄下來。這些紀錄即使被刻意或無意地刪除，未來仍有被還原的可能，因此電腦鑑識已成為現今資訊科技時代的重要工作。電腦鑑識利用科學的方法針對記錄一連串交易活動的「日誌（log）」進行蒐證，以提供線索來幫助偵察或法庭審理。此日誌檔可以被後續的鑑識活動所分析以確保檔案資料的真實性。整體而言，數位證據存在於4類電腦相關系統中：一、特定式電腦系統，例如：公文線上簽核系統等；二、開放式電腦系統，例如：網際網路等；三、通訊系統，例如：手機等；四、嵌入式電腦系統，例如：洗衣機的晶片等。大部分的檔案管理案例都落在第1類與第2類電腦相關系統設備中。

在電子檔案管理中，另一個與電腦鑑識相關的領域就是刪除檔案的復原（recovery）。某些電子檔案可能被有意或無意地破壞，這時可以採用一些電腦鑑識軟體將它復原，例如：Encase等，使得原始檔案可以被復原，擴充檔案可以被改變，隱藏的影像可以被發現。電腦鑑識的第一步就是小心的保護原始檔案與裝置，所有電腦鑑識人員都必須學習確保沒有破壞所保有的證據，亦即證據之完整性（evidential integrity）。為了確保證據之完整性，所有的電腦鑑識調查首先必須在不更動檔案或裝置的狀況下，產生一份與檔案或裝置一模一樣的影像檔，才進行後續的分析，其進行步驟必須明確詳實地記錄下來。

電子檔案儲存於電腦系統與電子儲存媒體上，政府機關利用檔案管理系統來管理電子檔案。這些環境經常處於網際網路中，所以對外還有網際網路防火牆以進行過濾存取與阻隔攻擊。然而對網際網路防火牆、檔案管理系統與電子儲存媒體而言，都可能存在電腦犯罪行為，因此，各機關乃遵守行政院所頒布之「行政院及所屬各機關資訊安全管理規範」與「行政院及所屬各機關資訊安全管理要點」辦理資訊

安全相關事項，以善盡保存電子檔案的責任。然而在電子檔案受到損害的情形下，電腦鑑識人員就需要逐步進行識別數位證據、分析數位證據、修護數位證據、呈現數位證據等電腦鑑識工作，以修護電子檔案，檔案管理人員再會同資訊人員將修護後的電子檔案匯回檔案管理系統或電子儲存媒體中。在電子檔案管理情境中，可採用資訊安全與電腦鑑識原則，並利用資訊安全與電腦鑑識相關工具，以確保電子檔案的完整性、真實性、可靠性、可及性與可用性，如圖2。

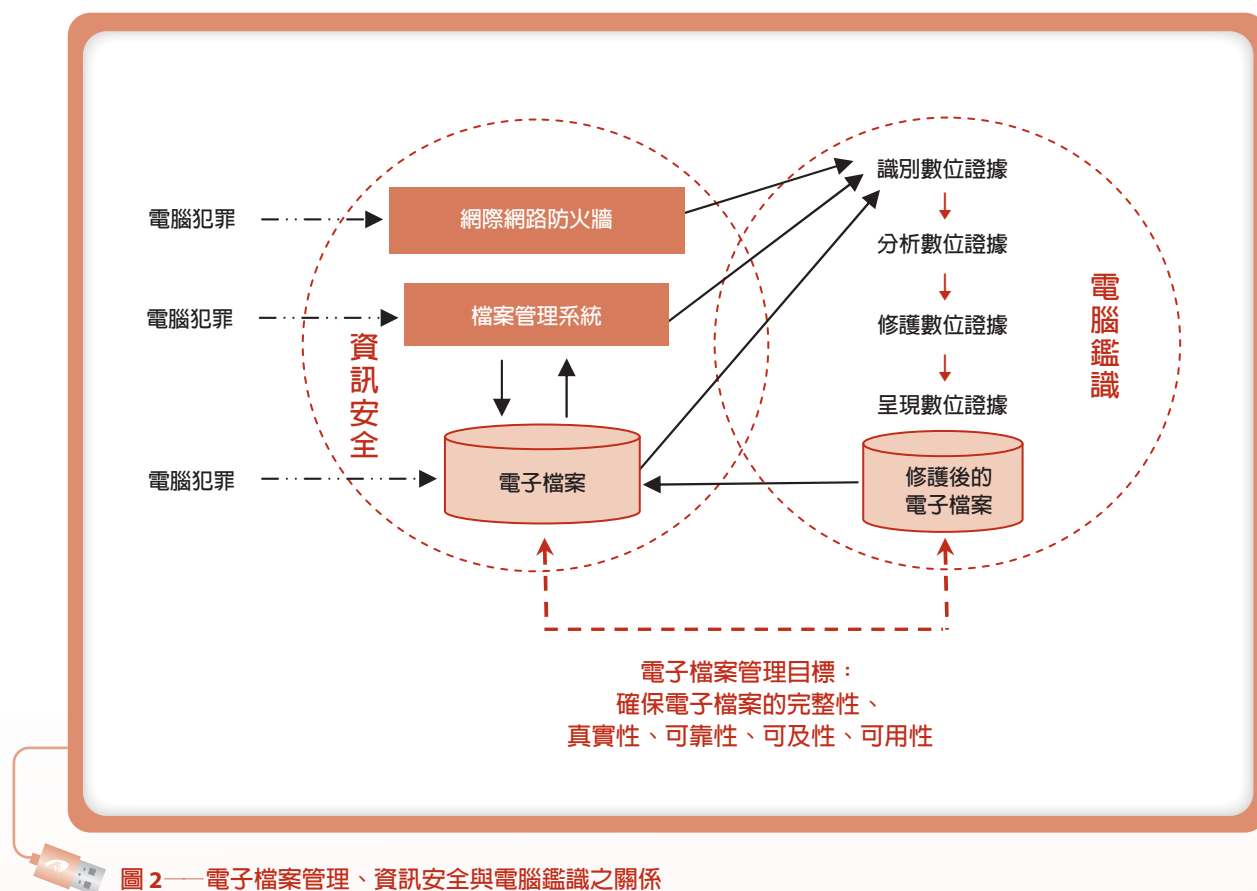


圖2——電子檔案管理、資訊安全與電腦鑑識之關係

資料來源：作者繪製。

電腦鑑識中，必須確保所檢查的電子材料都沒有被任何型式的修改，以確保其完整性。任何違反此原則的作法都會使此電子檔案喪失其證據力，這也是電子檔案管理在使用電腦鑑識時，最先要確立的原則。在ISO 15489中，說明一個檔案完整性代表檔案是完整且未經修改的。因此必須建立防護措施，以避免電子檔案被非經授權地修改。對電子檔案進行任何被授權的詮釋、新增或删除都必須是被敘明且可追蹤的。電腦鑑識工具與技術亦可以識別與追蹤電子檔案上的合法增加、修改、删除等，哪一位使用者在何時使用哪部機器進行哪些修改等，因而確保電子檔案的完整性。

在ISO 15489中，說明一個具真實性的檔案須被證實如下：一、如其所宣稱的目的；二、如其所宣稱的由所建立或送出的人來建立或送出；三、如其所宣稱在某時間建立或送出。應保護電子檔案以避免未經

授權的增加、刪除、修改、使用與隱藏。電腦鑑識工具與技術可協助找出原始產生者、產生時間，因此有助於維持電子檔案的真實性。

在ISO 15489中，說明一個具可靠性的檔案意謂著其內容可被信任是活動與事實的完整及正確記載，得做為後續活動所參考的證據。電腦鑑識工具與技術透過電子日誌資料可協助追蹤電子檔案的修改歷程，找出其活動的完整記載，因此有助於維持電子檔案的可靠性。

在ISO 15489中，說明檔案的可用性代表其可被置放、取出、呈現及解釋。其可被其後的營運活動所呈現。檔案的情境連結必須具備瞭解形成與使用此檔案異動所需的資訊。電腦鑑識工具與技術可協助找出隱藏或刪除的檔案及其連結，因此有助於維持電子檔案的可用性與完整性。



各國之電腦鑑識工作

各國已逐步建立高科技電腦鑑識組織，以專業知識提供服務，並藉由教育訓練提升電腦鑑識相關人員的技能。以下介紹美國、英國、新加坡以及我國政府在電腦鑑識方面之工作。美國國防部成立電腦鑑識實驗室部門（Department of Defense Computer Forensic Laboratory），在各州成立電腦鑑識實驗室，並組成區域電腦鑑識實驗室（Regional Computer Forensic Laboratory，簡稱RCFL），RCFL和其他執法機構合作運作，專司電腦鑑識的服務以及協助重大涉及電腦犯罪案件偵辦並提供專業建言。美國司法體系

也已經將數位證據視為有效的法庭證據，因此認證通過的各個數位鑑識實驗室或機構，由其所發表的報告皆具有證明力，亦為司法官所接受。在電腦鑑識領域有關的實驗室，較著名的包括：加州聖地牙哥的區域電腦鑑識實驗室（網址：<http://www.rcfl.org/index.cfm?fuseAction=Public.display>）、佛羅里達州的國家鑑識科學中心（National Center for Forensic Science，網址：<http://ncfs.ucf.edu/>）。美國康乃迪克州刑事實驗室是全美優良的刑事實驗室之一，負責該州執法案件之指紋、文書鑑定、痕跡、槍彈、攝影、微物、縱火物、DNA、影像處理等鑑定工作，並參與重要刑案現場勘查與重建工作等^(註8)。美國司法部於1994年提出「數位證據的鑑識檢驗：法律強化指引（Forensic Examination of Digital Evidence: A Guide for Law Enforcement）」，2008年出版「電子犯罪現場調查：第一現場人員指引（Electronic Crime Scene Investigation: A Guide for First Responders）」第二版，目前已經建立多項鑑識檢驗的標準指引（Standard Guide for Forensic Examinations）等。

英國數位鑑識實驗室（Forensic Science Service）協助英國刑事司法體系、警察單位、私人公司、甚至整個英國的鑑識工作，提供電腦犯罪偵查、電子相關犯罪等技術的支援，而其取得的證據也被英國刑事司法體系所採信^(註9)。英國警察協會（Association of Chief Police Officers，簡稱 ACPO）於1999年提出「電腦證據優良實務指引（The Good Practices Guide for Computer-Based Evidence）」，依此指引來引導電腦鑑識人員進行數位證據的處理，以做為法庭上認可的證據。英國ACPO提出的4個電腦證據處理準則如下：

原則1：為了取信於法院，必須確保警察或其他人員沒有修改電腦或儲存媒體上的任何資料。

原則2：在某情況之下，如果必須存取電腦或儲存媒體上的資料，該人員必須由有能力做這些動作，並且有能力對其動作予以適當說明及解釋。

原則3：必須產生與保存電腦數位證據的稽核過程或其它所有流程紀錄，獨立的第三者可檢驗其程序，並若進行相同處理程序，亦應得相同結果。

原則4：案件調查的承辦人必須確實遵守法律的規範與以上原則，並且負擔所有責任。

新加坡法證科學中心，隸屬於衛生科學局，提供新加坡執法單位、政府部門、醫院、私人團體、個人以及其他國家尋求協助鑑驗時，刑事科學調查之技術支援與服務。相關鑑定類別有微物跡證、物理型態鑑定、生物DNA跡證鑑定、文書鑑定、一般毒品鑑驗、尿液毒品鑑驗、毒物藥性鑑驗等。鑑識部門專責刑案現場之勘察採證，包括生物跡證、指紋、工具痕跡等。另外，新加坡警察局共有6個分區，鑑識部門專責刑案現場之勘察採證，包括生物跡證、指紋、工具痕跡等，因其指紋檔案之建檔及比對是由警察局負責，故刑案現場所採之檢體指紋送警察局鑑定，其他證物則送法證科學中心進行鑑定。新加坡警察局鑑識部門除了現場勘查外，並負責基層員警刑案現場採證及法庭交互詰問之訓練，邀請在職檢察官至模擬法庭擔任教官，進行訓練^(註10)。

我國行政院國家資通安全會報在「建立我國通資訊基礎建設安全機制計畫（民國94至97年）」中，特別揭示由內政部警政署負責建置資通安全網路犯罪資料庫，建立有關單位之資料庫分享機制，並成立國家資通安全鑑識實驗室。法務部調查局已於2006年底正式成立國內首座資安鑑識實驗室，可提供具備嚴謹程序的電腦鑑識服務，作為協助處理電腦犯罪、鑑識數位證據等，該實驗室的主要服務對象是調查局外

勤人員及檢察官，但亦可協助法院、資通安全會報以及其他政府部門在發生資訊安全事件時的數位鑑識工作。目前提供的鑑識項目包括搶救、復原儲存媒體中被損毀的機密資料等，例如：行賄資料、公司名冊等，即使資料被刪除，也可以透過各種工具進行復原（註11）。此外，鑑識實驗室也能追查網路入侵的來源，以及使用何種工具入侵，並保障數位鑑識證據的可靠度，不但可以分辨數位證據的真偽，還可以找出隱藏在數位證據內的細微內容。

另外，檔案管理局已經建置「電子檔案長期保存實驗室」，其業務內容包括：一、研發轉置、模擬等電子檔案長期保存相關技術與工具，並進行實作與驗測，訂定標準作業程序及驗測方式，俾提供機關執行作業之參考。二、提供電子檔案相關技術諮詢服務之管道，協助機關解決電子檔案所面臨之保存、應用及安全等問題。三、提供電子檔案模擬、轉置、修復及各項驗證作業程序諮詢服務，俾利協助機關執行相關作業。其作業區域包括系統保存、轉置、模擬、驗證、修復等。另成立「電子檔案技術服務中心」，電子檔案長期保存實驗室係著重於電子檔案長期保存技術研究及提供服務支援，電子檔案技術服務中心則提供機關服務及諮詢，同時蒐集機關電子檔案相關需求，以便使電子檔案長期保存實驗室的技術研究能滿足機關實務運作需求（註12）。



結語

機關愈重視電子檔案管理，就愈必須面對外在科技與內部有意或無意的不適當傷害，這樣方能積極達成電子檔案管理的目標，確保電子檔案的完整性、真實性、可靠性、可及性與可用性。電子檔案管理與電腦鑑識都以保存數位證據作為目標，其主要差異在於電子檔案管理利用前端收集、保存、清理與應用為主要流程，重點在於整理與應用，避免使電子檔案產生任何的傷害，修護僅是其中產生損害時的非常作法。電腦鑑識則是在電子檔案發生資訊安全事件之後，積極取得數位證據的手段。

因為電腦鑑識是一項複雜且不容易熟練的專業工作。所以目前在電腦鑑識上，仍有一些瓶頸與挑戰，最主要就是如何提升電腦鑑識人員的系統分析能力以及對各項工具與電子設備的掌握能力。電腦鑑識人員使用資訊科技平台，蒐集各項細微的證據，因此必須瞭解各項新興的高科技、其運作原理、所形成的電子設備以及分析這些設備的最新穎工具。累積各項的破解知識以及吸收新知，就成為其必須不斷學習的推力，例如：現在常見的行動裝置所使用的iOS與Android作業系統平台就需要採用不同的蒐證方法與技巧。同樣地，電子郵件與網頁的蒐證方式亦有所不同。

常用於電腦鑑識的原則、技術或工具亦可適用於檔案管理領域，尤其在電子檔案被破壞之後，可協助機關進行適當的電子檔案保護與數位修護。在資訊時代，檔案管理人員必須具備風險管理、協同治理、法律等相關議題的知識，至少應該意識到電腦鑑識的功能與工作。檔案管理領域中的電腦鑑識工作並非是單向的，它必須包含許多的檔案管理知識與技巧，例如：詮釋資料專業、管理、數位典藏的知識、資料分析的技能、數位資產相關法規的瞭解、長期數位保存的概念等。事實上，這些事項都必須與資訊人員互相聯繫，請求資訊人員的協助，方能有效地推展。機關檔案管理人員亦可尋求檔案管理局電子檔案技術服務中心的協助。未來，藉著檔案管理局電子檔案長期保存實驗室以及相關電腦鑑識實驗室的專業能力，相信必能對我國政府機關之電子檔案管理工作做出極大的貢獻。



註 釋

- 註1： “Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition, Office of Justice Programs, U.S. Department of Justice (2008),” *National Institute of Justice Website*, <<https://www.ncjrs.gov/pdffiles1/nij/219941.pdf>> (2 Aug. 2012) .
- 註2： Pollitt, Mark M., *Principles, Practices, and Procedures: An Approach to Standards in Computer Forensics*,” The Second International Conference on Computer Evidence, Baltimore, MD (1995): 10-15.
- 註3： Marcella, A. Jr. and Greenfield, R. S., *Cyber Forensics: A field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, Auerbach Publications, (2002).
- 註4： Rude, Thomas. “Evidence Seizure Methodology for Computer Forensics” , (2000), <<http://www.crazytrain.com/seizure.html>> (1 Aug. 2012) .
- 註5： Kuchta, Kelly J. “Forensic Fieldwork: Experience Is the Best Teacher,” *Information Systems Security*, 11(1) (2002): 36-43.
- 註6： Sinagin, Deniz. “Computer Forensics Investigations in a Corporate Environment,” *Computer Fraud & Security*, 6(1) (Jun. 2002): 11-14.
- 註7： 王旭正、高大宇、吳忠哲、江安展，〈資訊時代資安事件：數位媒介證據的來源、依據、判斷與說服力〉，國家實驗研究院科技政策研究與資訊中心資通安全分析專論，（2005），<<http://web.thu.edu.tw/s944946/www/paper/3.pdf>> (15 Sep. 2008) .
- 註8： 彭莉娟，刑事實驗室之標準學習，*刑事雙月刊*，（2007年1-2月），23-26。
- 註9： 王旭正、張躍瀚、黃嘉宏、高大宇，〈電腦鑑識環境建置的規劃 / 訓練時代需求〉，國家實驗研究院科技政策研究與資訊中心資通安全分析專論，（2006），<http://web.thu.edu.tw/s944946/www/paper/0409_2.pdf> (15 Sep. 2008) .
- 註10： 同註8。
- 註11： 黃彥榮，〈調查局成立第一座國家級資安鑑識實驗室〉，iThome online, 2006-12-20, <<http://www.ithome.com.tw/itadm/article.php?c=41099>> (15 Sep. 2008) .
- 註12： 電子檔案技術服務中心，<<http://erlp.archives.gov.tw/>> (5 Aug. 2012) .