數位證據在法庭上之攻防對策

邱獻民
臺灣士林地方法院檢察署檢察事務官
witness7@mail.moj.gov.tw

林宜隆
中央警察大學資訊管理學系教授
paul@mail.cpu.edu.tw

摘要

吾從事刑事偵查工作已有數年，很明顯發現到法院實務工作者大多僅有法律背景[1]，不論是處理電腦、網路犯罪或財經案件，若要在承辦案件過程中切中問題核心，往往需要花許多時間在基礎觀念的建立上，始得分析移送機關或案件當事人所提供之證據資料。有鑑於此，正因在案件偵辦過程無可避免會接觸數位證據，吾將試圖分別以辯護人之角度，攻擊及挑戰偵查機關在訴訟過程中所提出之數位證據，以及就偵查機關之立場，防禦及鞏固偵查中所獲得數位證據之證據能力(Admissibility)與證據力(Weight of the Evidence)，希望能提供司法實務工作者及各領域之先進關於此議題之思考方向。

關鍵字:數位證據(Digital Evidence)

一、前言

由於網路及電腦設備的普及，已形成一種族群混雜且不限時空的社會，傳統犯罪（指刑法所列之犯罪類型）因而出現新犯罪手法，更產生新型態電腦、網路犯罪（指刑法增訂罪章或刑法以外法律所列之犯罪行爲），常見在報章媒體的網路性交易、妨害風化、詐欺、駭客入侵等犯罪行爲，網路成爲新興犯罪場所及媒介，電腦及相關設備成爲犯罪工具之一。

有別於傳統犯罪行爲，電腦、網路犯罪者其行爲不容易被發現，甚至有些情況如駭客入侵盜取電腦存放之資料、窺視資料夾、植入木馬程式、病毒等，被害者常已遭侵害仍不自知，此因網路做爲犯罪工具具有不限時、地、匿名等特性，又使用電腦及相關設備所產生之數位資料因其特性，不若傳統文書般具有高度屬人性，故確定犯罪者身份及蒐證對象爲偵查此等犯罪首先面對的問題。然而發現犯罪者並蒐集相關證據資料後，因數位資料可以輕易的不著痕跡進行更改，且數位資料之原本不易確定，若提出之數位證據(Digital Evidence)之同一性(Identity)及真實性(Authenticity)遭被告或辯護人質疑，偵查機關與司法審判機關對此等數位資料應有如何之認知，如何以數位資料證明犯罪事實，將爲以下所要討論之議題。

二、數位證據

(一)數位證據概述

[1] 我國檢察署目前設有檢察事務官，分成四組，爲偵查實務組、財經實務組、電子資訊組、營繕工程組，其中財經實務組、電子資訊組、營繕工程組各招考相關領域之專業人才，爲檢察署中跨領域案件之偵查主力。

隨著科技與時代進步，法院與檢察署所使用的文書資料也邁向數位資料化，政府更推動行政 E 化，早期的法院與檢察署書類是以毛筆撰寫，經過以打字機繕打階段，現在則以電腦製作，而法院之裁判書與檢察署書類也已經以數位資料方式儲存於電腦之中，法院裁判書並可以供民眾上網瀏覽。司法院及法務部與民間業者合作，開發出司法人員辦案系統，使得法院及檢察署案件進行處理得以全面電腦化、數位化，案件管考不再完全靠人工，且現在開庭業已使用電腦設備錄音、錄影、製作筆錄，並可利用電腦網路設備進行遠距視訊訊問[2]，還可以電子郵件方式向法院傳送書狀[3]。而警察機關現在也不僅以電腦製作偵查筆錄，更以數位相機拍攝現場圖，並運用數位資料儲存指紋與嫌犯照片以供比對，以及偵訊時之錄音、錄影設備由傳統的卡帶，轉換成數位錄音、錄影。因此，資訊數位化不僅已存在於生活之中，司法機關也必得跟上此一潮流。

然而，因數位資料之特性(詳後述)，除得以經由電腦設備與軟體輔助，作任意修改或編輯外，在儲存過程中，因爲多以檔案壓縮方式儲存，在解壓縮還原後，理論上會有資料流失的情形，不管是人爲所在成的失真，或者是檔案處理過程中所無法避免的情形，但皆足以影響資料原貌，遂有司法機關所蒐集、製作的數位資料得否於訴訟程序中提出作爲證據，或者有無證據能力之疑問。惟現今辦案人員使用數位蒐證器材蒐集證據已成爲執行職務的方式之一，且因應市場及科技化之需求，不可能要求辦案人員持傳統的器材製作傳統紙本文書、照片、影音，在此前提下，警察機關所提出的數位證據應與傳統的證據形式等視，不應以數位資料得以在電腦上修改、編輯，而不採用數位證據。因此，不論是案件當事人所提出之數位資料，或者是司法機關自行蒐集之數位證據，都必須承認數位證據係得以證明待證事實之證據種類之一。

在承認數位證據得作爲證明待證事實之證據資料後，必先瞭解何謂數位證據。首先，就數位證據之型態，在文獻上有廣義與狹義之差別，廣義的數位證據包含我們常見之電腦、顯示器、印表機、掃描機、光碟、隨身碟等，可作爲數位資料存取、輸出之工具均包含在數位證據之概念中，然而廣義之見解似乎較不符合數位證據在文意上之定義，而應以電腦證據定義之。因此，本文對數位證據之定義採狹義見解，不包括硬體設備，而係指電腦儲存媒體中任何足以證明犯罪構成要件或關聯之數位資料，爲物理證據之一種，包括有文字、圖片、聲音、影像等型態，具有可無限無差異複製、原始作者不易確定、資料完整性不易驗證等性質，其以數位方式儲存於電腦儲存媒體上，換言之，就是在電腦儲存媒體上以數位方式儲存而可供佐證犯罪之資料[4]。

我國刑法及刑事訴訟法並無數位證據或數位資料之用詞，而係以電磁紀錄[5]稱之，惟依照刑法對電磁紀錄之定義，包含以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄，似乎較強調資料讀取方式之物理特性，而忽略資料本身之組成方式，

---

[2] 參刑事訴訟遠距訊問作業辦法。

[3] 參民事訴訟文書傳真及電子傳送作業辦法

[4] Digital Evidence and Computer Crime，Casey， 2000

[5] 刑法第十條第六項
稱電磁紀錄者，謂以電子、磁性、光學或其他相類之方式所製成，而供電腦處理之紀錄。
第二百二十條第三項(已刪除)
稱電磁紀錄，指以電子、磁性或其他無法以人之知覺直接認識之方式所製成之紀錄，而供電腦處理之用者。

尤其電磁紀錄在字義上僅能包含以電子和磁性方式存取之資料，若包含以光學或其他方式則較爲勉強，因此，本文將以資料之組成係以 0 跟 1 二進位演算出來而始得以供人閱覽之數位化特性，將所有相類之資料均稱之爲數位資料，可作爲證明待證事實之證據資料者，稱之爲數位證據。

(二)數位證據在證據法上之分類

1.傳統分類方式

證據依照證據的物理性質及既存狀態，依我國刑事訴訟法可分爲人證、物證、書證等型態，數位證據究係屬於哪一種證據類型，有以下數種說法。

(1)書證說

傳統書證係將某一內容以文字符號等方式紀錄在紙張上，數位證據則只是以不同的方式將同樣的內容記載在非紙張之儲存媒介上，兩者之儲存方式與媒介雖然不同，但是卻有相同的功能，即均能紀錄完全相同的內容。再者，數位證據通常以其代表的內容來說明某一問題，且必須輸出、列印到紙上形成書面材料後，始得被人們閱覽、利用，因而具有書證的特點。故只要對書證做廣義解釋，數位證據即可與書證概念一致。因此，數位資料之產生有完全得自於程式執行之結果者；數位資料有屬於單純之數據；數位資料有屬於本身並未顯示具體之意思表示而必須列印爲報表，配合報表上之文字、表格之後，始能表現出文書之意思性，這些數位資料均具有書證之功能。然而，此一說法非盡然能完全反應解讀數位資料之技術問題，係因數位資料非全然需經列印成紙本後始得閱覽其內容，透過電腦螢幕及其他電子媒體播放，同樣可以瞭解數位資料之內容，而用此一方式解讀數位資料內容是否符合傳統書證之概念，仍有待進一步釐清。

(2)物證說

此說認爲數位證據係以載有數位資料之電子儲存媒介物之存在、狀態、性質作爲證據，例如:在行動電話簡訊詐騙中，被害人提供行動電話所儲存之簡訊證明遭詐騙集團施用詐術，此時，詐騙簡訊儲存於行動電話之中，以行動電話作爲數位資料儲存媒介。但是，以本文定義之數位證據，係指儲存媒介所儲存之資料，而儲存媒介係屬硬體設備，兩者組成方式、概念完全不同，尤其數位資料只是 0 跟 1 二進位演算出來的結果，是否可視爲傳統物之概念，實有待商榷。

(3)多種類型說

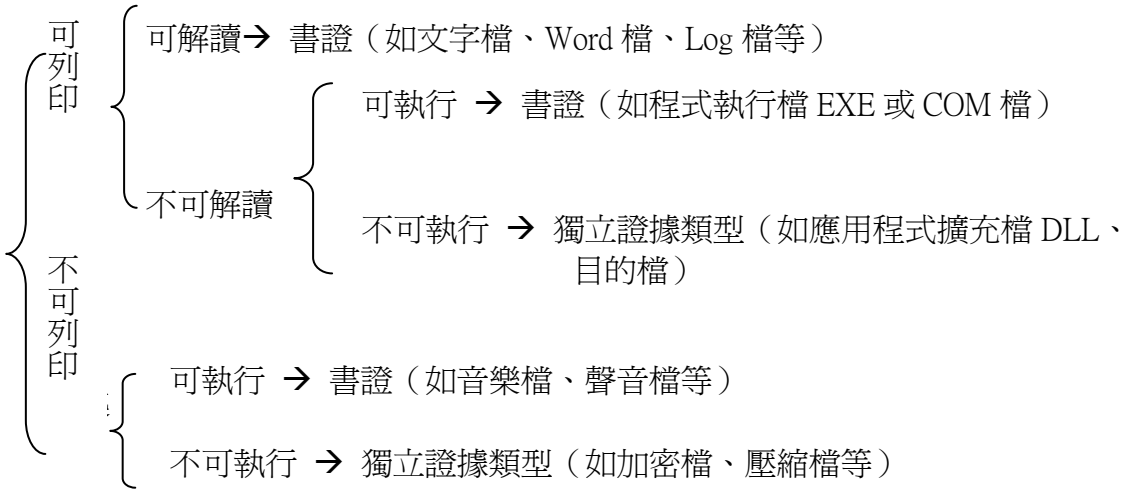
數位證據不能僅以單一證據種類做區分，而應區別不同情形來確定其證據類型。儲存數位資料的儲存設備，如電腦硬碟、光碟、隨身碟等，應屬物證的性質，如果輸出列印到紙張上即爲書證。

(4)獨立證據說

此說以數位證據無法明確區分究係屬傳統證據類型中的物證或書證爲論據，認應將數位證據作爲一種新的證據類型，因爲數位證據具有兩個主要特點，第一，數位證據係以所儲存的訊息內容來證明待證事實，第二，數位證據係以二進位數碼形式儲存在儲存媒介中。前者使數位證據具有書證的某些特質，但後者使得數位證據區別於所有的證據類型，一旦資料數位化，就可以利用電腦任意編輯、修改，而不具有其他證據相對穩定可靠的特點。因此，爲了避免對數位證據性質歸屬繼續爭論，以及對數位證據之證據能力有無之認定有統一見解，實有必要在刑事訴訟法上增訂新種類之證據。

2.數位證據依其特性之分類

本文依據數位證據的定義與特性，做如下之分類[6]:



圖示之分類方式，係先以提出之數位證據得否經電腦輸出列印進行分類，若數位證據得以紙本呈現其內容，再就其內容是得以經一般人所解讀進行區分，若屬列印後難以解讀其內容之情形，可再區分該數位證據可否經執行顯示其內容；此外，若數位證據無法列印，可再區分爲該數位證據得否經執行顯示其內容。綜上分類方式，詳述其內容如下:

(1)**可列印:**本文將數位證據可列印與否作爲分類之基準，理由在於目前法院實務對於數位證據之調查方式，仍以紙本之提出爲主，透過提示紙本解讀數位證據之內容，當數位證據可透過電腦輸出列印其內容後，再以該列印出來之內容能否爲一般人所解讀，區分爲可解讀與不可解讀。

A.**可解讀:**數位證據大都儲存在電腦及其周邊設備內，很難從外表明瞭其意義，一般仍靠電腦及其周邊設備才能將其內容顯示或列印，使用者才能了解其真正意義，若其列印出來的資料，使用者可閱讀並了解其意義，例如文字檔、Word 檔、Excel 檔等，這與傳統的書證意義相符。

B.**不可解讀:**當數位證據內容列印出來爲一堆亂碼、符號、數字，或許透過具專業電腦知識背景之人得以加以解讀其意義，但對於一般人而言，只是一堆無意義之亂碼、符號、數字。然而，這些不可解讀之數位證據，或許能透過電腦之執行，展現出原先設計者所要表達之意念，故就該數位證據可否爲電腦執行，可再區分爲:

a.**可執行:**若數位證據經列印出來之內容，一般人無法了解其意義，但若能經由電腦執行，可以展現出檔案或程式設計者所要表達之意念，例如執行遊戲程式執行檔（exe、com 檔等）後，即可顯示遊戲之內容，或者執行硬體驅動程式之控制介面等，這與傳統書證之概念相同。

b.**不可執行:**若數位證據不可閱讀，亦無法透過電腦執行方式表現出得以讓一般人了解其用意者，例如應用程式擴充檔（dll 檔）等，此種數位證據因爲不足以爲表示

[6] 參林宜隆，數位證據標準作業程序(DESOP)之建構

其用意，故非屬文書之概念，而無法歸類爲書證，又非爲傳統物之概念，亦無法歸類爲物證，因此應將之歸類爲獨立之證據類型。

(2) **不可列印:**其實所有之數位資料均爲程式運作下之結果，均爲電腦程式語言組成，不論是何種檔案類型，都是一連串之符號數字演算出來，嚴格說來，這些符號數字經轉換成文字檔後，都可列印出來。不過本項著重在數位證據在一般閱覽時之展現方式，而區別出此種一般非以列印方式展現其內容之分類，而此種分類之項下，可再依是否得以電腦執行展現其內容分爲如下兩種類型:

A.**可執行:**數位證據雖非以利用電腦及其周邊設備列印解讀其內容，但可利用其來執行，執行後就能了解其意義與功能，例如音樂檔、聲音檔等，此種數位證據足以展現其用意，而得爲一般人所能了解其內容，故屬於書證之範疇。

B.**不可執行:**若數位證據非得以列印展現其內容，又不能執行者，例如加密檔、壓縮檔等，當檔案加密或其壓縮技術高超而無法解開時，實難以得知其內容，故無法將之歸類爲書證，又非爲傳統物之概念，亦無法歸類爲物證，因此該種數位證據應屬獨立之證據類型。

綜上述，本文提出此種分類方式，係因傳統證據法就書證及物證方面仍以有形物爲論述之主軸，然而就數位證據而言，已然無法就傳統證據法之分類方式進行清楚之分類，尤其電腦科技之進步，數位資料展現之態樣日新月異，分析數位證據不應陷於傳統證據概念之窠臼，而應理解數位證據之諸項特性後重新定義及分類，以解決數位證據在證據分類上之紛爭。

(二)數位證據之特性

瞭解上述數位證據之分類後，本節將進一步說明數位證據異於紙張書面證據之處，亦即基於數位資料的本質而具有之特性，先瞭解數位證據之特性後，始能發現數位證據何以在證據法上引起眾多討論，並可從中知道如何在案件中對數位證據進行攻防。以下列出數位證據之諸項特性[7]:

1.無限複製及無差異複製

電子數位資料透過電腦複製之指令，可以無限次地進行複製，只要在電腦正常運作下，每一次進行複製動作所增加之電子數位資料，與原本製作之電子數位資料不會有任何差異，甚至透過儲存設備、傳輸設備，可以任意散佈複製之電子數位資料。此一特性而顯與紙張書面之情形不同，紙張形式的文書固然可以無限制的影印，但是影本會因使用紙張之不同、墨色濃淡之選擇、及影印機本身之功能等因素而與原本有差別，尤其當原本上留有簽章或簽名的情形時最爲顯然，但是數位資料無論電腦之廠牌、年份、系統爲何，均不會產生複製物與原本有差異之結果。

2.不著痕跡增刪修改

所有數位資料只是 0 跟 1 二進位演算出來的結果，因此可以不著痕跡進行增刪改，不若紙本資料修改，一望即知修改知部位爲何，故要確知電子數位資料是否曾遭修改著實不易，需透過歷史儲存資料、登入資料查得有否遭修改。因此，數位證據之同一性雖然較不容易確定，但不應以此遽然否定其得以作爲證據之可能性，蓋困難並不等於絕對無法做到，且電腦科技仍在不斷進步中，將來必會發展出值得信賴之鑑識技術鑑定數位

[7] 參林一德，電子數位資料於證據法上之研究，碩士論文，國立臺灣大學，民國八十九年，第 124-129 頁。

證據之真僞。

3.復原可能性

傳統書證若遭損毀，如文件遭燒毀，或被放入碎紙機，要回復成原狀幾乎是不可能，即使得以拼湊出片段訊息，然而已破壞原先該書證所欲證明之完整內容。但數位證據若遭到刪除或毀損，如資料被移到資源回收筒後又被清除，或檔案中毒等情況，仍然可以藉由特別的軟硬體設備，將檔案內容加以完整復原。

4.製作人不易確定

我們可以很容易指出這台電腦曾經做過什麼事，但是卻無法確定是誰以這台電腦執行這個動作。由於數位資料不若手寫文書可以字跡辨別，即便具名製作數位資料，仍易遭質疑其真實性，故要以數位資料內容本身確認製作人爲誰，實屬不易，仍需要透過其他相關事實或電腦相關科技之輔助，始得加以確定。

5.無法以人之知覺直接認識、理解其內容

簡單舉出以平日瀏覽網頁爲例，網頁顯示出之畫面爲經過瀏覽器程式執行後之結果，然檢視網頁之原始檔，多爲一長串之指令及數碼，一般人無法直接以原始碼辨識出原始碼所代表之意義爲何，即使熟知電腦指令之人可辨別其中指令之目的，然而如圖像等編碼，仍無法直接判讀出該符碼所顯示出之圖像爲何。換言之，此情形類似錄音帶、錄影帶需經機器設備之播放始能顯示內容，而紙張或其他形式之文書，係得以人類之知覺直接認識，不需經過任何轉換之過程。

6.對環境具有依賴性

所有數位資料是 0 跟 1 二進位演算出來的結果，因此數位資料的輸入、儲存、輸出都必須依賴電腦設備及軟體程式來完成，如果產生、儲存數位資料的硬體設備性能及運轉狀況不可靠，或電腦所依賴的軟體程式不可靠，那麼將使數位資料的真實性受到質疑。再者，隨著技術不斷進步，軟、硬體設備不斷更新，若出現新舊系統之間相容性不好，造成數位資料無法無法存取，如此將無法利用數位資料的內容來證明待證事實，或者因爲電腦存取格式改變，數位資料要經過一定格式轉換才能被讀取，在格式轉換過程中，很可能會造成數位資料原始數據變動或破壞，進而使數位資料喪失證據能力。

三、數位證據在法庭上之攻防對策

(一)在法庭上常見之數位證據

在犯罪偵查過程中，不論是傳統犯罪或電腦網路犯罪常見用來證明待證事實之數位證據有:

1.電腦設備產生之紀錄:指的是作業系統本身所留存之數位證據，因爲任何電腦都是靠作業系統來運作的，基本上，作業系統可定義爲管理電腦硬體的管理程式，各種作業系統均有一些歷史軌跡檔的紀錄，這些紀錄檔紀錄著這台電腦曾經做過的各種行爲，故對於數位證據蒐證者而言，此處爲不可忽略的部分。

2.數位文書:目前常見的數位文件編輯款體有 Microsoft Word、Excel、Power Point、WordPad、漢書(法務部書類製作軟體)、文采(法院書類製作軟體)等，常見數位文件檔名型態爲*.txt、*.doc、*.xls、*.ppt、*.pdf 等。

3.數位聲音:目前常見數位聲音撥放軟體有 Windows Media Player、Real Player、Quick Time

等，常見的聲音格式有*.wma、*.mp3、*.rm、*.midi 等。

4 數位影像:目前常見的影像播放軟體有 Windows Media Player、Real Player、Quick Time、Power DVD 等，常見的影像編輯軟體有 ACDSEE、PhotoShop、PhotoImpact、Windows Movie Maker 等，常見的影像格式有*.jpg、*.tiff、*.bmp、*.avi、*.wmv、*.asf、*.mpg 等。

5.經轉檔、解碼、復原後之數位證據資料。

6.用程式顯示之數位跡證:如 ENCASE 軟體、車牌辨識軟體等。

7.網際網路數位證據:如電子郵件、網路即時通訊、網頁等。

8.電腦以外設備儲存之數位證據:如 PDA、數位錄音筆、數位相機、行動電話等。

(二)數位證據之檢視

上述數位證據會面臨的挑戰不外乎，其一爲當事人質疑數位資料遭到竄改、破壞，由於數位證據具有不著痕跡增刪修改之特性，庭呈到法院之數位證據都無法排除遭破壞、修改之可能性。其二是質疑產生數位資料的電腦程式之可靠性，電腦使用者都知道，電腦軟體程式常會出現 BUG，需要不斷更新軟體、除錯，而且電腦程式爲人所撰寫，運算結果可爲程式設計者所控制，無法排除電腦演算之結果爲使用者刻意控制下之結果。其三是質疑作者之身分，此因數位證據具有製作者身分不易確定之特性，即使數位證據可據以證明待證事實，然而在無法個化(Individualization)數位證據之情形下，面對此不利證據之當事人必會辯稱任何人均有可能製作出完全相同之數位證據。故在對數位證據進行攻防之前，必先瞭解數位證據本身之諸項特性，始得切中攻防之爭點，因此，在總結數位證據在法庭上之攻防對策之前，本文針對數位證據之特性，提出當事人及法院當面對庭呈之數位證據時，有哪些係擬定數位證據攻防策略前所應檢視之重點，其相關重點及理由表列如下:

數位證據檢視表

數位證據檢視之重點	檢視之理由
數位證據來源	由於數位證據可以在任何時間，以任何一台電腦製作，因此需檢視數位證據之來源爲何，以釐清該數位證據之出處與案件相關人等之關係。
數位證據蒐集方式	合法蒐集證據係證據取得證據能力之前提要件，因此需檢視庭呈之數位證據係以何種方式取得。
數位證據作者	數位證據不論是匿名或者具名製作，因數位證據無法如同一般紙本文書以筆跡個化作者爲誰，因此需檢視數位證據之作者與案件相關人等之關係。
數位證據格式	由於數位證據格式多樣，顯示其內容之方法也不同，因此需檢視原始之數位證據之格式爲何，確定數位證據原始格式始得忠實呈現其內容爲何。
數位證據內容	由於數位證據具有可以不著痕跡增刪修改之特性，因此需檢視原始數位證據內容與庭呈到法院之內容是否相符。
數位證據建立時間	數位證據之建立時間、修改時間、存取時間均得以檢視庭呈之數位證據是否遭變動。

數位證據提出於法庭之方式	由於目前法院實務數位證據內容之證據調查方法多以紙本爲之，然而紙本內容爲數位證據經輸出後之結果，因此需檢視數位證據提出於法院之方式是否爲得以忠實呈現數位證據原始內容之方式。

本表爲作者自行整理

(三)攻防對策

依本人數年偵查實務之經驗，粗淺提出上述數位證據可能在法庭上所會面臨攻擊及防禦之方法，然而，對數位證據進行攻防，不論是何種類型之數位證據，均會因其具有相同之特性而有相同之攻防爭點。因此，承上述提出對數位證據應檢視之重點後，以下將針對數位證據之特性，提出當事人對數位證據進行攻擊與防禦之爭點及對策:

數位證據攻防策略對應表

攻防爭點	待證事項	攻擊對策	防禦對策
數位證據來源	提出數位證據之一方欲以該數位證據證明與案件相關人等之關聯性，如該數位證據出自於某人之電腦、儲存設備等	庭呈之數位證據非出自於與案件相關之當事人	1.依該數位證據蒐集者之證述證明出處。 2.依其他證據資料證明該數位證據來源與案件相關之當事人有關。
數位證據蒐集方式	庭呈之數位證據有出自於網際網路、電子郵件、儲存設備等	所蒐集之數位證據非公開在網路上之資料	1.若進行網路通信監察，提出檢察官核發之通信監察書。 2.公開蒐集數位證據之方法及步驟。
數位證據作者	數位證據依期內容所載之作者證明與某人相關，如電子郵件恐嚇信由某人所寄發、數位文書內容曾提及案件相關人、或作者爲案件相關人等	庭呈之數位證據非某人所製作	蒐集其他數位證據及數位證據以外之證據資料個化數位證據之作者。
數位證據格式	呈交數位證據爲可得閱覽其內容	庭呈之數位證據格式非原始儲存格式	利用專家證人、鑑定、勘驗證明數位證據格式之變更不會更動數位證據之內容。
數位證據內容	提出之數位正據內容可以直接證明待證事實，如:車禍現場之數位影像檔、當	庭呈之數位證據內容遭增刪修改	1.利用數位證據鑑識技術證明該數位證據之內容未曾遭增刪修改。 2.說明數位證據自蒐集到

	事人間對話之數位錄音檔等		庭呈至法院之過程。
數位證據建立時間	數位證據建立時間與案件事實重要之時間點有交集，如:數位監視錄影畫面建立時間某當事人出現在拍攝地點附近。	與案件相關之當事人在數位證據建立時間、存取時間、修改時間有不在場證明	1.以其他證據資料證明該數位證據係與案件相關當事人所製作。 2.以其他證據資料證明數位證據建立時，當事人與該時空有交集。
數位證據提出於法庭之方式	數位證據表現方式多樣,以最方便閱覽方式檢視數位證據,如檢視複製後之數位影音檔、或列印出之紙本等	1.數位證據內容以紙本提出與原始內容有異。 2.憑以列印出紙本之原始數位證據不存在。	1.當庭勘驗比對以電腦讀取之數位證據內容與紙本內容是否相符。 2.若原始數位證據已不存在，則以其他證據資料證明該紙本內容爲真實。

本表爲作者自行整理

四、結論

數位資料於偵查實務中作爲證據之案例，已隨著電腦與網路之普及顯著增加，由於數位證據有不同於以往物證與書證之諸項特性，以之採用爲認定犯罪事實的證據之前，即必須針對其浮動性加以克服，亦即不論藉由其他證據之證明，或以電腦相關科技之輔助，最後必須能達到增加數位資料信憑性之效果，或者是證明其屬真實、正確且未經更動之資料，併證明行爲人誰屬。以上所陳，是在各種類型之案件中，均應加以注意並解決之問題。

而案件當事人提出數位資料作爲證據時，鑑於其複製版本及輸出物均具有完全相同於原本之品質，故應允許以複製資料或輸出物作爲證據，惟爲確保與原本之同一性，仍應以其他證據證明之。外國立法例即訂有相關規範，規定符合某些條件之數位資料複製版本或輸出物具有證據能力，而不再拘泥於最佳證據法則之適用，然而，我國刑事訴訟法並未針對數位證據之浮動性，以及其舉證之對象作出因應之修正。因此，將來修法應明訂以數位資料作爲證據時，所應提出之版本爲何，例如是否將原始數位資料與其輸出物一併提出，並且亦明訂解決數位資料信憑性之方向，例如採取舉證責任之轉換，將符合某些要件之數位資料推定爲真正，以避免法官無所適從，偏離個案正義之情形。

至於在具體案例中，數位資料所扮演之證明角色已有不同，此則直接影響其證據方法之屬性及證據調查之方式。由於數位資料經電腦轉換後所呈現之型態不勝枚舉，其在訴訟法所處之地位又係包羅萬象，故法院對之加以調查時，往往發生模糊證據調查方法之情形，此反映出有對於數位資料重新定位其證據方法屬性之必要。因此，有必要修法將數位資料視爲獨立的新種證據方法，並在刑事訴訟法證據章中另訂數位證據專節。最後，在關於數位證據處理及鑑識方面，亦應制定標準作業程序及成立專責單位，以利偵

查機關所蒐集之數位證據得以爲法院所採納，並提高其證據力。

參考文獻

專書部份:

1.Arthur Best著 蔡秋明、蔡兆誠、郭乃嘉譯，*證據法入門 美國證據法評釋及實例解說*，元照，2002。
2.錢世傑、錢世豐、劉嘉明、張紹斌著，*電腦鑑識與企業安全*，文魁資訊，2004。
3.樊崇義著，*證據法學*，法律出版社，2004年10月三版。
4.江偉主編，*中國證據法草案(建議稿)及立法理由書*，中國人民大學出版社，2004。
5.林鈺雄著，*刑事訴訟法*，林鈺雄出版，2003。
6.陳樸生著，*刑事訴訟法實務*，海宇文化事業有限公司，1999。
7.齊樹潔主編，*英國證據法*，廈門大學出版社，2001。
8.Allen C.Snyder、Anthony J.Bocchino、David A.Sonenshein著，蔡秋明、魏玉英譯，*加州證據法與異議實務*，商周出版社，2005。
9.王兆鵬著，*美國刑事訴訟法*，元照出版有限公司，2004。
10.黃朝義著，*刑事訴訟法:證據篇*，元照出版有限公司，2002。
11.黃朝義著，*刑事訴訟法*，一品文化出版社，2006。
12.石井一正著，鄭善印譯，*日本實用刑事訴訟法*，五南圖書出版有限公司，2000。
13.吳巡龍著，*新刑事訴訟法制度與證據法則*，學林文化事業有限公司，2003。
14.陳祐治著，*佛羅里達證據法逐條釋義*，翰蘆圖書出版有限公司，2006。

論文部分:

1. 林一德，”電子數位資料於證據法上之研究”，碩士論文，國立臺灣大學，2000。
2. 丁秋玉，”網路犯罪證據之搜索扣押研究”，碩士論文，中央警察大學，2002。
3. 謝昆峰，”網際網路與刑事偵查”，碩士論文，國立臺灣大學，2001。
4. 蘇清偉，”網路犯罪入侵案件之數位證據蒐證研究”，碩士論文，國立交通大學，2001。
5. 邱獻民、林宜隆，”數位證據同一性之攻擊與防禦-以網際網路蒐集之數位證據爲中心”，*第四屆資訊科技與人文管理教育論壇暨數位內容、數位教育與管理政策研討會:資訊倫理與資訊教育論文集*，2007。
6. 邱獻民、林宜隆，”數位證據同一性之攻擊與防禦”，*二00六年網際空間:資訊、法律與社會學術研討會暨實務研討會論文集*，2006。
7. 林朝榮，”刑事證據法則之新發展-*黃東熊教授七秩祝壽論文集*:證據能力與證明力”，學林文化事業有限公司，2003。

期刊部分:

1.蔡震榮、張維平，”電腦犯罪證據之研究”，刑事法雜誌，第四十四卷第二期，2000。
2.張弘昌，”應用數位影像證據問題之探討”，刑事科學，2004。
3.蔡震榮、黃玥婷，”數位證據之證據力”，*刑事法雜誌*第，四十九卷第二期，2005。
4.黃朝義，”證據能力與證據力之概念區分”，*本土法學雜誌*，第二十期。
5.陳佳瑤、吳佳育，”數位證據於現行法律之相關議題”，*二00二年網際空間:資訊、法律與社會學術研討會暨實務研討會論文集*，2002。

網路文獻部分:

1. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations，Computer Crime and Intellectual Property Section Criminal Division United States Department of Justice July 2002，http://www.cybercrime.gov/s&smanual2002.htm#_V_
2. Orin S. Kerr，Computer Records and the Federal Rules of Evidence，March2001

http://www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm
3. Orin S. Kerr,Computer Records and the Federal Rules of Evidence
www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm

國外文獻部分:

1. E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, Academic Press, 2000.
2. K. Mandia and C. Prosise, Incident Response: Investigating Computer Crime, McGraw-Hill, 2002.