電腦鑑識工具應用於犯罪偵查之研究

黃嘉宏[1]　詹前隆[1]　王旭正[*]

[1]元智大學資訊管理學系　[*]中央警察大學資訊管理學系

摘要：由於資訊科技的發達，現階段刑事案件現場已不再單純只是傳統犯罪現場，在高科技資訊化的環境中，雖然是相同的犯罪案件，但與以往最不同的地方是犯罪現場多了許多軟硬體及數位電子設備，如：監視器、電腦、PDA 及隨身碟等。面對這些涉及電腦的傳統犯罪或是電腦犯罪案件，鑑識人員已無法利用傳統的犯罪偵查模式來完成採證工作，此時需要電腦鑑識技術的輔助來完成證據採集。因此，爲了將所蒐集的證據在法庭上受到法官的採信，所以我們將使用電腦鑑識工具來幫助鑑識工作的進行，並透過標準的電腦鑑識流程以及使用國際公認之電腦鑑識工具蒐集證據，可增加數位證據的完整性及可驗證性。在本討論中，我們將電腦鑑識流程各階段所需使用之電腦鑑識工具做深入的整理，提供給從事電腦鑑識工作之人員作爲參考。依本研究整理可節省尋找適當鑑識工具的時間得以加速電腦鑑識工作速度，以提高鑑識工作的效率。

關鍵詞：電腦鑑識、數位證據、電腦鑑識流程

目次：

1.前言

二十一世紀電腦科技的發達，資訊透過網際網路快速地流通，不僅爲組織帶來無限的商機外，亦帶給人類在工作上或生活上許多的便利，而這股資訊科技無形中帶來的力量讓地球村的世界得以實現，然而資訊科技的發達雖然帶給人類便利的生活，但也使得負面的問題更加地嚴重、複雜，如：透過電腦所從事的各種犯罪行爲、網路色情等。

電腦網路快速及高普及化的程度帶來相當多的益處，卻也同時帶來不少問題，如電腦犯罪或是利用電腦作爲輔助工具之傳統犯罪。而現在的電腦或網路犯罪已不單純只是利用電腦爲工具之犯罪，其中亦牽涉法律層面及道德層面的問題，透過網際網路推波助瀾下，各種網路毀謗、恐嚇、妨害名譽、侵害著作權及隱私權等等的犯罪型態有增加的趨勢。雖然，政府針對電腦與網路犯罪已制定相關法律條文，但是徒有法律條文亦無法解決所有的犯罪問題，而在許多的電腦或網路犯罪案件中，所有相關的證據及資訊都被存放在電腦內部裝置，如：各種儲存裝置、網路設備、IDS、IPS、或防火牆系統日誌中[8]。在犯罪偵查工作上或在法庭上時，非常需要相關的證據來證明其犯罪行爲，而這些相關的證據大多存放於電腦裝置或網路設備內，所以我們需要一套有系統的方法來取得

及分析這些存在於裝置或設備內的資訊，經由電腦鑑識工作所蒐集及分析的相關證據，期望在未來能作爲法庭上判決及起訴依據之參考。

「犯罪偵查」或「鑑識」對一般人來說，很直觀的都會認爲這是屬於司法機關或警察單位的工作，其實不然，在犯罪現場，第一線到達現場人員如果無法保持現場情況，往往會造成重要證據被汙染，而讓證據無法作爲判定犯罪人之重要依據。相對於「電腦鑑識」而言，第一線鑑識人員如果能保全相關數位證據，則數位證據更能在法庭上被採信，將犯罪人繩之以法。在本研究中我們必須依循著定義良好且清楚、兼具靈活與彈性的方法、程序，分析電腦鑑識流程[1,2]各階段所需使用之電腦鑑識工具，進而進行數位證據資料之蒐集、分析及重建現場，並將本研究所提出之電腦鑑識工具介紹，讓鑑識人員從事犯罪偵察時有所依據，並可幫助電腦鑑識工作順利的進行，並提高工作效率。其最終的目的是讓數位證據在經過司法程序審理時作爲判決的依據。

本篇研究結構說明如下：第二節文獻探討。第三節提出電腦鑑識工具應用於犯罪偵查之介紹。最後第四節中爲本研究之結論。

2.文獻探討

爲了能有效地利用電腦鑑識工具完成電腦鑑識的工作，使用者必須擁有基本檔案系統之概念，了解可能存有數位證據的設備，方能找尋具有效性及可靠性之數位證據。爲了使數位證據能具備有效性及可靠性，故需先了解檔案系統、電腦鑑識與數位證據，進而了解電腦鑑識的前置作業流程及鑑識標準作業流程，方知鑑識工具的固定操作流程之原由。相關觀念說明如下:

2.1 檔案系統[4]

數位證據通常是存放於硬碟或其他儲存設備中的記錄檔、文字檔、聲音檔、影片檔、圖像檔，但只要有任何資料有了修改，即使是中繼資料(Metadata，資料中的資料)，如：檔案建立時間、修改時間、存取時間、使用者名稱、檔案屬性等，也有可能是具證據價值的資料。故需先了解檔案系統，方知如何尋找數位證據，以下就無法操作但可能存有數位證據之設備提出說明：

檔案剩餘空間(File Slack)

由於每個磁區的大小是固定的(512 bytes)，若此時有一個 900 bytes 的檔案欲存放至磁區上，則存放此檔案時必使用到二個磁區（1024 bytes），但並未完全使用到二個磁區，故多出來的 124 bytes 的空間，即爲檔案剩餘空間，檔案剩餘空間有可能曾存放過可作爲證據之資料。

未配置空間(Unallocated Space)

未配置到任何磁區的可用磁碟空間。由於尚未有檔案系統，故無法存取資料。雖然目前未使用，但也可能曾經被使用過，故其上可能存在一些遭刪除之資料，未配置空間也有可能曾存放過可作爲證據之資料。

交換檔(Swap File)

交換檔是在虛擬記憶體中使用的隱藏系統檔。作業系統於硬碟切割一部份空間作爲虛擬記憶體，當可用實體記憶體不足時，便將實體記憶體中較無急迫性或放置過久之資

料，挪移至交換檔，這些存於至交換檔的資料稱之爲環繞資料(Ambient Data)，系統並不分配磁碟空間。由於交換檔有緩衝資料的作用，等同於擴充實體記憶體之容量，但交換檔位於硬碟，故其存取速度遠不如實體記憶體，雖可虛擬出記憶體容量，卻不能將其用來替代實體記憶體。由於許多資料片斷被儲存於交換檔裡，分析交換檔內容可收集到許多具證據價值的資料，甚至可能有使用者登入系統時所使用的帳號、密碼之記錄，故爲蒐集數位證據的來源之一。

2.2 電腦鑑識與數位證據[1,2]

電腦鑑識是利用科學的方法對電腦等資訊科技設備進行犯罪蒐證，處理各種數位記錄之保存（Preservation）、識別（Identification）、擷取（Extraction）、文件化（Documentation）及解釋（Interpretation）電腦資料，並依據其方法與基本原則：

(1)在不改變或破壞證物的情況下取得原始證物。

(2)證明所抽取的證物來自扣押的證物。

(3)在不改變證物的情況下進行分析。

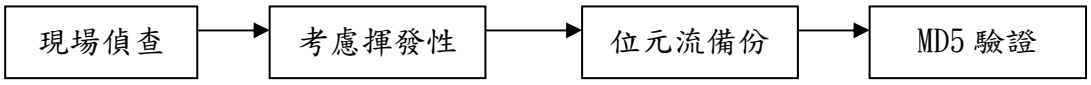
以確保數位證據的可靠性和有效性，使所蒐集之數位證據具證據能力與證明力(證據能力乃指證據能力之適格能力；證據之證明力乃指證據用以證明待證事實之強弱)。隨著網際網路的發展，高科技犯罪事件增加、案件複雜性也日趨提昇，爲了有助於案情的釐清，各式各樣的證據都是十分重要的，雖然數位記錄比起一般的人證、事證、物證，更容易去竄改、僞造，但數位記錄任何新增、存取與修改動作，都會儲存在電腦設備中，「凡走過必留下痕跡」，無論是做出了什麼樣的舉動，還是會留下蹤跡可尋的，此乃電磁記錄之天性，即使是被有人心士蓄意刪除，還是可透過鑑識工具還原，數位證據的蒐集已經變成一個眾所皆知且具有價值的調查方法。

數位證據

數位證據是電腦等資訊科技設備內部的一些記錄檔、文字檔、聲音檔、影片檔、圖像檔，以電磁紀錄方式儲存於電腦等資訊科技設備儲存媒體上。如何蒐集數位證據並妥善保存，確保數位證據的可靠性和有效性，便有賴於各種高科技鑑識工具。

2.3 電腦鑑識前置作業流程[7]

由於數位證據具有容易受外力修改之特性，故現場電腦犯罪偵查需遵守標準作業程序，如圖一所示，而鑑識工具之操作也需按照圖一之步驟進行，方能保障數位證據之完整性與可靠性，才能有效地偵查電腦犯罪，進而維護整體資訊安全。



圖一 電腦鑑識前置作業流程

揮發性（Volatile）與非揮發性（Non-Volatile）[6]：由於電子設備需持續供應電源以保留內部資料，故電子設備在電源供應中斷後對內部資料之保存能力不同而有所區別。當電源供應中斷，所儲存之資料會消失者，稱之「揮發性」，如：動態隨機存取記憶體(Dynamic Random Access Memory，DRAM)、靜態隨機存取記憶體(Static Random

Access Memory，SRAM)，兩者均屬於隨機存取記憶體；當電源供應中斷，所儲存之資料會消失，但重新供電後，可再次讀存取資料者，稱之「非揮發性」，如：唯讀記憶體(Read-Only Memory，ROM)、可程式之唯讀記憶體(Programmable Read-Only Memory，PROM)、可擦拭及程式之唯讀記憶體(Erasable Programmable Read-Only Memory，EPROM)、可電子擦拭及程式之唯讀記憶體(Electrically Erasable Programmable Read-Only Memory，EEPROM)、快閃記憶體(Flash memory)。由於需考慮揮發性之問題，故搜索犯罪現場時需評估可否立即關掉使用中的電腦。在圖一中，電腦鑑識前置作業流程內容分述如下：

位元流備份(Bit Stream Backup)

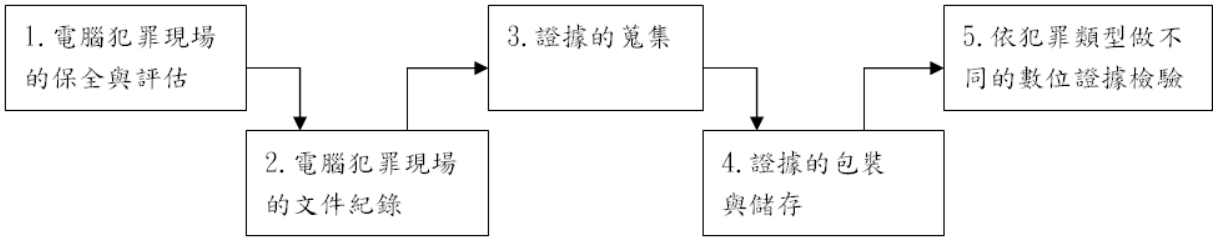
由於一般的備份方式是無法達到完整拷貝之效果，可能會間接造成一部份資料流失。故數位證據的備份需使用位元流備份之方式，將原始資料進行完整之拷貝，以創建出完全符合原始資料之精確複本，方能從複本上進行分析數位證據。

MD5(Message-Digest Algorithm 5)

爲一廣泛使用的 Hash 演算法，可用來確保資料完整性，無論輸入是任何資料或字串，將固定輸出較短的位元串以表示之。由於二個不同內容的檔案算出來的 MD5 值會一樣的機率爲 2^{128}，不太可能產生相同的 Digest，故可用於驗證原始檔案與複製檔案的完整性，且在原始檔案中作微小改變其 MD5 值也會發生巨大的變化，故常用於判斷一個檔案的內容是否遭修改。

2.4 鑑識標準作業流程[5,6]

非法入侵事件發生時，在證據的取得上亦需符合正當的法律程序。在證據的取得過程，我們必需依照電腦鑑識的標準作業程序，確保經由鑑識人員取得的資料能提供其證據力及證明力。而一般的電腦鑑識程序及證據的取得是以入侵者的電腦爲第一現場，以現場所存在的數位設備作爲蒐集的對象。證物鏈的掌握包括現場的電腦主機、螢幕、印表機以及數位儲存媒體(如記憶卡、隨身碟等)，並要求文件的紀錄、物證的包裝運送，最後才到實驗室的鑑定。電腦鑑識程序主要的工作項目如圖二所示：



圖二 電腦鑑識的基本程序

一般的電腦鑑識程序，主要強調在於事件第一現場設備扣押時至檢驗期間的完整證物鏈(Chain of Custody)。要求文件的紀錄、物證的包裝運送，最後才到實驗室的鑑定。所有的過程都需要專業且懂得電腦鑑識標準作業程序的鑑識人員，才有辦法應付各種事件現場所遺留的設備及數位證據。

3. 電腦鑑識工具應用於犯罪偵查

3.1 電腦鑑識工具於鑑識流程之應用

自 2000 年以來資訊犯罪手法日新月異，電腦鑑識與網路鑑識愈來愈受到重視。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有個統一見解。而 2001 DFRWS(Digital Forensic Research Workshop)裡提出一鑑識作業流程(see dfrws.org/about/history.shtml)，使得鑑識作業流程有較明確的規範。DFRWS 所提供的鑑識作業流程規範以下七個步驟：

1. 識別(Identification)：事件/犯罪偵查。
2. 獲取(Preservation)：案件管理、證據鏈、映像技術。
3. 蒐集(Collection)：經認可的方法、硬體、軟體、還原技術。
4. 檢驗(Examination)：驗證技術、過濾技術、比對技術。
5. 分析(Analysis)：資料探勘、時間軸順序。
6. 呈現(Presentation)：專業證明、建議對策。
7. 結論(Decision) 。

2004 年亦有學者 Ciardhuain [3] 提出鑑識作業流程不單只是爲執法單位或鑑識取證人員設計，而是必須將範圍再擴大到資通犯罪的領域。因爲愈來愈多的資安工作者、資訊稽核單位、公司資安部門也需要藉由鑑識作業流程來規劃相關的技術策略和未來的發展目標。藉此，Ciardhuain 提出新的資通犯罪調查模型，該模型重點架構如下：

1.蒐證前必要的準備工作
- 警覺(Awareness)
- 授權(Authorization)
- 計畫(Planning)
- 通知(Notification)

2.蒐證過程
- 搜尋和辨識證據(Search for and identify evidence)
- 蒐集證據(Collection of evidence)
- 運送證據(Transport of evidence)
- 儲存證據(Storage of evidence)
- 檢查證據(Examination of evidence)

3.取證後在法院的審判流程
- 假設(Hypothesis)
- 授予假設(Presentation of hypothesis)
- 抗辯假設(Proof/Defense of hypothesis)
- 散播資訊(Dissemination of information)

整體而言，資通犯罪調查模型將整個鑑識工作應有之程序從頭到尾詳盡描述，其適合用來解釋處理資通犯罪之流程。由於過於強調其次序性，設計太過嚴謹而刻板，若能從多個觀點來構想將更有彈性。

藉此，爲能搭配鑑識作業流程，電腦鑑識工具的選用於犯罪偵查上，即以數位證據的關鍵萃取爲最重要考量之一。以下以三種整合性鑑識工具, Encase, TCT and FTK之整理說明如下：

(1)Encase：Guidance Software (http://www.guidancesoftware.com/)所研發的產品。EnCase 是目前使用最爲廣泛的鑑識工具，爲 Guidance Software 所研發的產品，能支持各種作業系統，包括：FAT16、FAT32、NTFS、Macintosh HFS、HSF+、Sun Solaris UFS、Linux EXT2/3、Reiser、BSD FFS、Palm、TiVo Series One and Two，AIX JFS、CDFS、Joliet、DVD、UDF 和 ISO 9660 等。EnCase 之使用相當人性化且功能完整，能循序引導電腦鑑識人員完成映像複本，具備位元流備份、Hash-MD5 驗證、CRC 校對碼等，得以驗證數位證據之完整性，並能深入作業系統底層查看所有數據，包括：檔案剩餘空間、未配置空間、交換檔之數據等，得以重新組織檔案結構，其採用 Windows 圖形介面顯示文件內容，除了基本的查看檔案建立時間、修改時間、存取時間、使用者名稱、檔案屬性外，尚有方便的圖檔顯示器，能支持 ATR，BMP，GIF，JPG，PNG 和 TIFF 等多種格式。在分析檔案方面，EnCase 能比較已知的特徵簽名，以避免爲隱藏證據檔案而變更副檔名之情況，並能支持多種郵件格式，如 Outlook、Outlook Express、Yahoo、Hotmail、Netscape Mail、MBOX、AOL 6.0、7.0、8.0、9.0、PFCs 等，且可支持多種瀏覽器格式，如 IE、Mozilla Firefox、Opera、Apple Safari 等，爲了能讓電腦鑑識人員使用方便，還可以撰寫巨集，以設定一些自動完成之鑑識步驟，最後，可以自動生成詳細的鑑識結果報告，能以 RTF(Rich Text Format)文本方式或 HTML(HyperText Markup Language)形式顯示之。

(2)The Coroner's Toolkit（TCT）: The Coroner's Toolkit（TCT）是一套由 C 和 perl 語言寫成的鑑識工具集。它可以用來搜尋或分析 Unix（Unix-like）系統上的資料。TCT 工具可以免費從 http://www.porcupine.org/forensics/tct.html（TCT 官方網站）下載。網站上除了有 TCT 可以下載外，也有相關的介紹和說明，對於初學者來說，是一個方便學習操作的網站。TCT 主要分爲三個部分，分別爲 Grave-robber, MACtime, 與 Unrm & Llazarus，說明如下：

（a）Grave-robber

Grave-robber 是 TCT 的核心工具，主要是下達指令來擷取檔案系統中的資料，或是儲存一些需要分析的檔案。在正常的情況下，Grave-robber 會掃瞄整個系統，並盡可能地擷取所有資料。例如暫時（ephemeral）資料（如網路狀態）、系統硬體 configuration（特別是磁碟或磁碟分割）、檔案系統的 critical files（configuratio -n files, log files）。但如果你不是以 root 的身份執行，它會阻止你擷取 root 權限的檔案。執行完畢後，它會建立所有輸出資訊的 MD5 簽章（儲存在 data/ hostnam -e/MD5_all 裡）。如果無法帶走 Grave-robber 所有輸出結果，至

少可以帶著 MD5_ -all，會給予你莫大的幫助。在資料蒐集前，它會檢查對系統而言是很重要的檔案或工具，如/etc,/bin 等。

（b）MACtime

這是一個收集 Mtime, Atime, Ctime 的鑑識工具。Mtime（Modified time）是檔案最後被修改的時間。Atime（Access time）是檔案最後讀取的時間。Ctime（Changed time）是檔案屬性最後被改變的時間。這些時間很容易被竄改，必須要小心處理，以免造成證據的更動。

（c）Unrm＆Lazarus

一般人以爲損壞或遺失的檔案無法復原，其實它還在硬碟的某一個地方，只是我們需要工具把它重新找回來。而這兩個工具，正是擁有救回原來檔案的能力。Unrm 是一個以 C 語言寫成的工具。它可以找出未配置的資料，挖掘潛在的檔案。例如，有 20G 的硬碟空間已使用 12G，它可以把剩下 8G 的未配置資料復原。接著，Lazarus 可以從 Unrm 的成果或其他資料來源找到需要的資料。Lazarus 適用在 UFS, EXT2, NTFS, FAT32 檔案系統上。最後的成果也會隨著不同檔案系統而有所變化。

(3)Access Data's Forensic Toolkit (FTK)： Access Data 公司的 UTK(Ultimate Toolkit)是一套經由美國政府及法院認可的數位鑑識軟體，能夠簡單使用並快速分析，其主要的工具有：

(a) Forensic Toolkit(FTK)：數位鑑識分析工具。
(b) Password Recovery Toolkit(PRTK)：密碼分析、破解與回復工具。
(c) Registry Viewer：登錄檔分析及解密工具。
(d) FTK Imager：數位證據預覽及獲取映像工具。
(e) Wipe Drive：硬碟資訊及資料完全清除工具。

其中 FTK 則是 UTK 中最主要的分析工具，可以分析、獲取、組織並保存數位證據。FTK 透過索引化的概念將所有文字內容建立索引，強大的過濾及搜索功能爲其特色。其支援的檔案系統如 FAT12/16/32、NTFS、EXT2/3，支援的映像格式如 Encase、Ghost(Forensic Image only)、Linux DD、SMART 及 CD 和 DVD 映像格式如 CDFS、Alcohol(*.mds)、ISO、Nero(*.nrg)、CloneCD(*.ccd) 。

表一 整合性鑑識工具

綜合鑑識軟體	開發團隊	功能
EnCase	Guidance Inc.	Windows/Linux/Unix 泛功能電腦鑑識軟體
Forensic toolkit	Accessdata	Windows 鑑識工具，具登入檔、email、zip檔案分析功能
TCT	The Coroner's Toolkit	Linux/Unix系統上使用

3.2 鑑識軟體功能之比較

發生資安事件於蒐集各種數位證據時，在每個不同的蒐證階段應該使用何類型工具;表二列出了電腦鑑識領域中，較具有公信力之電腦鑑識工具並加以分析比較。而這三大鑑識工具各有其特色，從事電腦鑑識工作人員可利用這三種鑑識工具之優點，交叉使用以利電腦鑑識工作之進行。透過本研究所整理出之電腦鑑識工具應用於犯罪偵查，可加速電腦犯罪偵查調查的速度，藉此提高了犯罪偵查的效率。

表二 EnCase、FTK and TCT 三大鑑識軟體功能之比較

	Encase	FTK	TCT
Free for charge（免費）	N/A	N/A	◎
Wipe Disk（清理磁碟）	◎	◎	N/A
Duplicate（建立映像副本）	◎	◎	◎
Validate Image （映像副本驗證）	◎	◎	◎
File Recovery（檔案復原）	◎	◎	◎
EXT2/3 support（支援EXT2/3格式）	◎	N/A	◎
FAT 16/32 support （支援 FAT16/32格式）	◎	◎	◎
NTFS support（支援NTFS格式）	◎	◎	N/A
E-mail search（電子郵件搜尋）	◎	◎	N/A
Keyword search（關鍵字搜尋）	◎	◎	◎
Password recovery（密碼破解）	◎	◎	◎
CDFS support（支援CDFS格式）	◎	N/A	◎
View Registry（檢視登錄檔）	◎	◎	N/A
Image gallery（影像瀏覽）	◎	◎	N/A
Generate report（產生報告）	◎	◎	◎

4.結論

本整理研究，在處理電腦犯罪時可作爲參考之依據，並可支援不同類型的電腦犯罪案件。透過鑑識軟體之比較，可得知 EnCase、FTK and TCT 這三大鑑識軟體各有其優缺點，例如：EnCase 可支援各種不同系統及環境所使用之鑑識軟體，但是 EnCase 在搜尋檔案及回復檔案的效率上不如 FTK 來的快，而 FTK 只支援 Windows 環境下之鑑識工作，在 Linux 系統環境中只有 EnCase 及 TCT 可以完成其工作。所以各種不同的鑑識軟體各有其優缺點，鑑識人員可依不同的環境及犯罪現場來適時使用不同的電腦鑑識工具。經由本文所整理之結果，期許能讓電腦鑑識人員節省思考可使用的電腦鑑識工具的時間，得以在第一時間掌握重要數位證據的內容以爲鑑識報告之依據。

Acknowledgements: We are indebted to the source offer from ICCL (http://hera.im.cpu.edu.tw) research papers/reports and the information summaries made by H.Y. Chang who is the ICCL-member.

參考文獻

[1] E. Casey, “Digital Evidence and Computer Crime: Forensic Science,” Computers and the Internet, Academic Press, pp. 41-46, 2000.

[2] E. Casey, “Investigating Sophisticated Security Breaches,” Comm. ACM, pp. 48-55, Feb. 2006.

[3] S.O. Ciardhuain, “An Extended Model of Cybercrime Investigations,” International Journal of Digital Evidence, Vol. 3, Issue 1, Summer, 2004.

[4] A. Silberschatz, P.B. Galvin, and G. Gagne, “Operating System Concepts 6th Edition,”2007.

[5] H.B. Wolfe, “Computer Forensics,” Computers and Security, Vol. 22, No. 2, pp. 26-28, Jan. 2003.

[6] H.B. Wolfe, “The Circumstances of Seizure,” Computers and Security, Vol. 22, No. 2, pp. 96-88, Feb. 2003.

[7] 王旭正 and 柯永瀚，電腦鑑識與數位證據，博碩文化，2007 年 6 月。

[8] 王旭正、姚深淵、黃嘉宏 and 詹前隆, “Firewall-based 遠端網路的數位證據蒐集,”Journal of e-Business,2008 年 3 月,pp.235-254.