數位證據鑑識標準作業程序 For Windows

林宜隆 、 黃志龍 、 林佳慶
中央警察大學資訊管理系所 、刑事警察局-資訊室 、 銘傳大學資訊管理系所
paul@mail.cpul.edu.tw 、Im933094@mail.cpul.edu.tw 、Smalldog000@msn.com

摘要

資訊科技發達的今日，資料大都是以數位方式來處理、儲存、保管，使數位資料無所不在，當數位資料發生爭議或問題時，就顯示出數位證據的重要，則需要靠數位證據的鑑識能力才能識別或還原真相，因此培養數位證據鑑識人才、建立數位證據鑑識作業程序的標準與認識，是現今刻不容緩的問題，且應透過標準及認證來加強鑑識結果及公信力，以強化數位鑑識單位之能力及法庭上公信力。

因此本研究係參考國內外相關學者的數位證據鑑識作業程序及數位證據相關的文獻探討，建構一套數位證據鑑識標準作業程序，同時將標準作業程序應用於 Windows 平台進行鑑識，以輔助國內司法調查人員或鑑識人員調查資訊犯罪的參考依據。

關鍵詞：數位證據、數位證據鑑識、標準作業程序

1 前言

現在的資訊科技發達，電腦與網路以及科技帶給人們在工作上、生活上的便捷，隨著資訊科技日新月異，使得一些入侵和攻擊手法層出不窮，而伴隨而來的將是網路上種種入侵、竊取帳號等等的資訊犯罪事件，故如何打擊和防治資訊犯罪變成司法界亟待解決的一大難題。

如果在「電腦資訊犯罪事件」發生後，經由「電腦鑑識」蒐集相關的數位證據，將所有電腦資訊犯罪事件完整的紀錄，以利往後偵查並且做為法庭上的依據，由此可知維護整個資訊安全是非常重要的。然而「數位證據」具有易竄改、易流失以及難以蒐集的特性，想要在發生電腦資訊犯罪事件後取得數位證據，則必須要有一套完善的標準作業程序。

1.1 研究動機與目的

在歐美先進國家，電腦鑑識已實施許久，從早期政府單位、軍警單位甚至民間都具備這些技術、人才、專門工具及完備的程序，尤由甚者，經過合法程序調查及撰寫正確文件後，即視為合法證據。反觀國內，對電腦鑑識領域之採證方面，較少相關研究或定義及標準程序，本文蒐集國內外相關學者的數位證據鑑識作業規範及流程和數位證據相關的文獻探討，並加以分析、嘗試建構數位證據鑑識作業規範及流程，其共分為三大階段：概念階段、準備階段、操作階段，探討其重點工作、規範及流程，供檢、警、調偵查人員在處理數位證據鑑識時的參考，同時在本文中介紹相關的工具及技術提供國內警政鑑識單位參考使用，最終目的是協助國內執法單位對於「電腦資訊安全事件」之數位證據擷取分析時有遵循的依據。

1.2 研究範圍及限制

目前個人電腦盛行，再加上使用者可能因為工作需求而使用不同的作業系統，作業系統的種類上也趨於多樣化，在有限的時間內不可以一一針對不同平台去作研究測試工具，因此本文研究主題主要是在探討有關 Windows 作業系統的電腦鑑識。

Windows 作業系統在目前個人電腦上有將近百分之八、九十機率是使用微軟 Windows 作業系統，由於系統漏洞及弱點多，也易於撰寫病毒程式及容易入侵，因而成為攻擊者與駭客們下手的目標之一，因此研究主題針對 Windows 作業系統下執行鑑識的鑑識工具當作研究標的，並提出一套完善的 Windows 作業系統的標準作業程序。

2 文獻探討

2.1 鑑識

2.1.1 鑑識之基本概念

執法人員根據法律，追訴犯罪，往往發現許多認定犯罪事實所憑藉之論據，必須借重具有特殊科學之人與工具的協助，始能達到追求事實真相的目的。故在許多缺乏人證、偵查困難的案例中，都因科學鑑識顯現出物證、犯罪嫌疑人、被害人、現場之間的因果性及相關性，進而達到證明犯罪或澄清冤情之目的，刑事鑑識學便是此種背景而生，一般鑑識就是指刑事鑑識。

2.1.2 鑑識之意義

「鑑識科學」一詞屬國內慣用之名詞，究其意

函，應與「forensic science」一詞相當，亦即包含民事鑑識與刑事鑑識二大部份，另外「鑑識科學」名稱之由來，似與刑事學界慣將刑事偵查與刑事鑑識相提並論，卻常將刑事兩字省略，故現今「鑑識科學」之中性名稱反而較能契合現代民主法治之精神，至少頗為強調物證或證據之科學鑑識。

2.2 數位鑑識

2.2.1 數位鑑識之基本概念

數位鑑識（Digital Forensics）由於資訊化的社會及電子商務的普及，造成資訊犯罪大幅的升高，而發展出較新興的鑑識科學，且因數位資訊的特性及系統、硬體與應用程式的不同等，而需要不同數位鑑識的工具及技術，使得數位鑑識變成很複雜性的科學。數位鑑識科學（Digital Forensics Science）的目的為協助司法人員偵辦電腦網路資訊犯罪案件與犯罪證據之蒐證，而其目標就是能在法庭上提出有效且可被採納的證據，因而成為法官判案的佐證及依據。

2.2.2 數位鑑識之意義

電腦鑑識（Computer Forensics）這個名詞是一九九一年波特蘭的國際電腦專家協會（International Association of Computer Specialists，IACIS）首次提出[8]，主要是在處理電腦有關的數位證據之保留、識別、萃取、記錄及解讀，以確保事件現場電腦物證及數位證據的原貌，使鑑定過程合法，鑑識結果具備完整性[9]，並能作為法院審理犯罪案件的重要參考依據。

2.3 數位證據

2.3.1 數位證據之基本概念

以傳統的法律觀念來看，在所有糾紛當中的證據講求的是“白紙黑字”和有原訴人親筆簽名的原件，但使用電腦的作者只有電子文文件、使用網路的商人只有商業往來的電子郵件、遭人詆毀的被害者只能找到 BBS（Bulletin Board System）上的電子文章，而這些電子文件，不僅沒有“白紙黑字”的“原件”爲憑，而且連存放在電腦系統內的電子文件內容和署名本身，都能夠被任何人輕易修改。這些新型的電子記錄以及電子郵件、多媒體軟體、網頁等，在法律上如何準確定位他們的地位和證明效力，將是清晰解決各種電腦及網路糾紛的前提，這些嶄新的法律問題，值得我們認真深入探討。

2.3.2 數位證據之意義

「數位證據」一詞在學者 Casey 所著「Digital Evidence and Computer Crime」一書中係指電腦儲存媒體中任何足以證明犯罪構成要件或關聯的電子數位資料，為物理證據的一種，包括有文字、圖片、聲音、影像等型態，具有可無限無差異性複製、原始作者不易確定、資料完整性驗證等性質，亦稱電腦證據，其以電磁紀錄方式儲存於電腦儲存媒體上，換言之，就是在電腦儲存媒體或網路上以電磁紀錄方式儲存而可供佐證犯罪之資料。[11]

世界各國及我國法律目前都尚未對數位證據有正式的定義，有的是定義電子紀錄、電磁紀錄，有的是電子文字，不過本研究在此統稱為數位證據，經彙整以上各國法律之定義，加上學者定義，本研究將其定義為：藉由電腦或網路設備儲存或傳送可供證據用。

2.3.3 數位證據之特性

與傳統的證據相比，數位證據有以下突出的特性：[1][4][5][6]

（一）高科技性

電腦是現代化的計算工具和資訊處理工具，其證據的產生、儲存和傳輸，都必須借助於電腦技術、儲存技術、網路技術及相關高科技設備等，離開了高科技含量的技術設備，數位證據無法保存和傳輸。

（二）多樣性

數位證據超越了以往所有的證據形式，不僅可以用文字、圖像、動畫和聲音等多種方式儲存於電腦硬碟、軟碟、光碟、磁帶等設備及介質中，其生成和還原卻離不開相關的電腦等設備，而且還有將上述多種形式綜合形成的“多媒體”形式。

（三）易變性

數位證據使用電磁介質，儲存的資料修改簡單而且不易留下痕跡，這導致了當有人利用非法手段入侵系統、盜用密碼時，還有操作人員的差錯或供電系統和網路的故障等情況發生時，數位證據均有可能被輕易地盜取、修改甚至全盤毀滅而不留下任何證據。

（四）無形性

在電腦內部，所有資訊都被數位化了。透過電腦把二進位編碼轉換爲一系列的電脈衝，來實現某種功能。在進行電子商務交易的過程中，一切資訊都由這些不可見的無形的編碼來傳遞。因此數位證據也具有這樣的無形性。

（五）易破壞性

電腦登錄、處理、傳輸的資料均以電磁濃縮的形式儲存，體積極小，攜帶方便，而行爲人往往具有各種便利條件，極易變更軟體資料，隨時可以毀滅證據。

2.3.4 數位證據處理程序

由於數位證據具有易於竄改、易於流失、難以蒐集等特性，且其內容易於被破壞，加上電腦設備

的儲存空間越來越大等因素，偵查人員容易因處理不當導致重要線索不易蒐集造成破案先機盡失，下列為學者們及電腦鑑識公司所提出之處理程序：[12][14][10][13]

表 1 數位證據處理程序比較分析表

New Technologies Inc	美國	1999	1.將電腦關機 2.記錄系統的硬體結構 3.傳送電腦系統至安全的場所 4.對硬體和軟碟片做完整一對一備份 5.對儲存設備的資料用數學方式來鑑定 6.記錄電腦系統日期和時間 7.對關鍵搜尋字列出清單 8.找出作業系統裏交換檔的資料 9.找出殘餘檔案的資料 10.找出尚未配置空間（包括已刪除檔案）的資料 11.用關鍵字搜尋檔案、殘餘檔案和尚未配置空間 12.記錄檔案名稱及檔案異動日期及時間 13.識別檔案、程式和儲存體異常情形 14.評估程式的功能 15.記錄調查結果 16.將使用過的軟體備份並保留
Thamos Rude	美國	2002	1.刑案現場準備工作 2.拍照 3.傳送 4.實驗室鑑識準備 5.檢查
Deniz Sinangin	美國	2002	1.識別 2.復原 3.保存 4.分析 5.呈現
Timothy Wright	美國	2000	1.搜索與扣押：程序規劃、著手處理犯罪事件、記錄犯罪等級、搜索證據、擷取證據、處理證據。 2.資訊探索：程序規劃、搜索證據、處理證據。

綜合以上專家學者對電腦鑑識程序的觀點，歸納出鑑識流程不外乎有下列幾點：準備工作、搜尋、保存、復原、分析、檢查、鑑定及呈現結果。
將這幾點歸納到 windows 鑑識流程上，如下：
事前準備：準備工作
蒐集資料：搜尋、保存、復原
分析資料：分析、檢查
鑑識報告：鑑定、呈現結果
程序之重要性，在於其能夠幫助蒐證及鑑識工作的進行有一定的依循標準，使得數位證據更有可信度，就因為它的客觀性，即使透過公平的第三者進行驗證，仍會得到相同的結果。

2.4 標準作業程序

2.4.1 程序

所謂「程序」(procedure)，乃指為達到一定之目的，所為多數法律行為或事實的動作方法、手續之連續而言。任何政府決策機關為了要運作，都必須有一套程序規則。因為一般程序規則具有穩定性與可預測性、決策的合法化、權責的區分、衝突的減少及權力的保障等功能。[3][7]

2.4.2 標準作業程序

標準作業程序（Standard Operating Procedures，簡稱 SOP)，一般字典將標準作業程序定義為：「一定的程序或過程可作為依據者」，標準作業程序係指某作業程序其前後因果關係具有強列的規則性，可被用來作為操作之依據而不致產生管理上的失誤、缺漏等事件，並可降底作業產出不良率。國外學者對標準作業程序解釋如下：「有些場合，標準作業程序被描述為某特定任務或工作必須完成連續性步驟或技術」。另一種說法為：對於經常性或重覆性工作，例如各種檢驗、操作、作業等，為期程序一致化，將其執行過程予以詳細描寫之一種書面文件稱之。

2.4.3 訂定標準作業程序的好處

為什麼要訂定標準作業程序（Standard Operating Procedures，簡稱 SOP）？標準作業的意義在於以統一的書面作業流程，將企業所有的作業架構、作業環境、設備的操作、工作的內容與步驟，以圖形、規格、文字等方式，使負責人員於工作時，有所依循與規範，並且透過標準化的過程，將工作流程與事務流程合理化，使作業上的錯誤降低，藉以提升工作效率及效能。因此數位證據若能制定標準作業程序將可使檢警蒐證人員在蒐證時能有依循的標準，所得的證據將更具公信力，並提高其證據能力及證據力。

因此透過標準化作業，可以得到的好處包括：[2]

（一）得以建立一套健全的制度，使新進人員快速上手。
（二）減少不必要的工作流程，增加行政效率。
（三）制度的合理化，減少勞資爭議發生。
（四）減少冗員增加，以及不必要的資源浪費。
（五）避免認知差距，使要求與時機發生落差。
（六）新人上手容易，用語統一。

數位證據若能訂定標準作業程序，無論對於檢警偵查人員甚至於企業單位它們面對違法事件時，有關蒐證、分析及鑑識等程序都能有個依循的標準，及作為參考，所得的數位證據更具說明力及公信力，並達到完整性、一致性及正確性的要求。

3 Windows 系統鑑識標準作業程序的建構

目前的刑事訴訟法是針對 86 年修正過的傳統證據，並沒有適用 92 年修正過的，且只有將電磁紀錄列入，對於相關的程序也沒有隨著修改，所以刑事

訴訟法的相關程序已不合現在需求，92 年 6 月份通過的電腦網路犯罪專章對於數位證據部分並不是很完整且也沒有完全適用，基於以上原因，我們認為整個標準作業程序，應遵守及注意法規及原則相關概念，如此方能使數位證據更能符合完整性、合法性及真實性。綜合上述理論探討、資料搜集、各國所制定的相關程序和專家學者及實務辦案人員寶貴意見與案例驗證、分析後，本研究再修正、整理與歸納後，提出了概念、準備及操作三個階段之數位證據標準作業程序，最後將數位證據標準作業程序套用在 Windows 作業系統上。(如下圖)

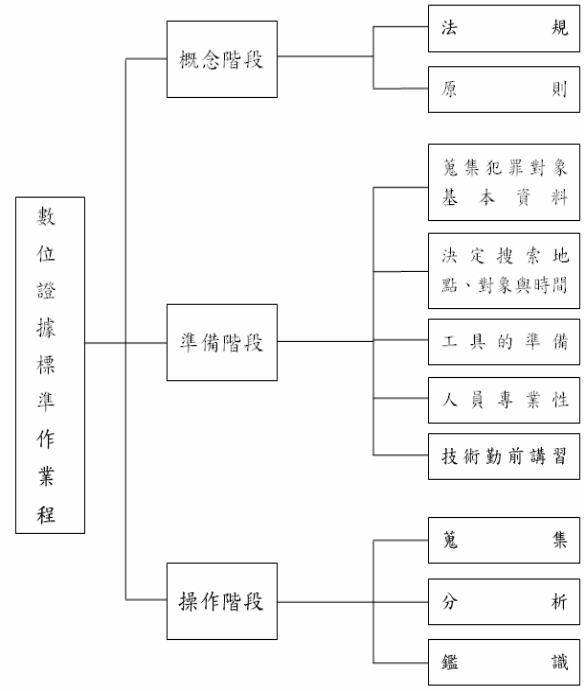

圖 3-1 建構數位證據標準作業程序

3.1 概念階段

此階段分為法規及原則兩部分，在操作階段所執行的各程序及步驟，應該符合及遵守此概念階段之法規及原則，方可使獲得之數位證據符合公正性、合法性及真實性，並提高其證據能力與證明力，以做為法官審判之依據。

3.1.1 法規

數位證據的取得要遵循合法、真實的原則，當事人不得以非法侵入他人電腦資訊系統的方法獲取證據；證據取得的途徑必須以立法的形式規定取得數位證據的程序及許可權。

在數位證據的蒐集過程中，要注意數位證據的蒐集和相關人的隱私權之間的衝突問題的解決，在一般情形下，數位證據的蒐集和取證主要是對在電腦的資料處理系統中已經儲存或者處理的資料，但是許多情形下，電子資料並不是現成的,而這種時候往往會採取監聽和竊聽的方式來取得證據，這種方式如果運用不當就會侵犯人民的隱私權。隨著近年來電腦網路犯罪的增加以及數位證據的取證上的難度，應對在蒐集證據中侵犯隱私的行為加以明確的規定。

3.1.2 原則

主要原則有以下幾點：

(1) 儘早蒐集證據，並保證其沒有受到任何破壞，即在處理時，必須確保電腦或其它儲存媒體上的資料保持在原始的狀態，內容不得修改。

(2) 必須保證「證據連續性」，即在證據被正式提交給法庭時，必須能夠說明在證據從最初的獲取狀態到在法庭上出現狀態之間的任何變化，當然最好是沒有任何變化。

(3) 對於數位證據的任何稽核資料、紀錄或分析的處理過程，應建立處理方法、紀錄與保留結果，就算委由公正的第三者進行相同的處理程序，其所得結果應相同。

(4) 在特殊情況下，如果需存取原始數位證據的資料，則必需由有能力處理的專家，進行存取的動作，並對其處理的動作予以說明及適當解釋。

(5)應當全程紀錄及拍攝蒐集、分析及鑑識等過程。

(6) 存放和使用存有拷貝證據的軟碟、光碟、磁帶和硬碟時應當注意安全，並遠離強磁場，使用時應注意病毒的檢測。

(7)使用證據複製品進行分析、調查及鑑識的工作。

3.2 準備階段

此階段的主要工作是做一些鑑識前的準備工作，並蒐集相關資料，為了操作階段各程序執行的預作準備，以下為其步驟：

(一)蒐集犯罪對象基本資料

根據犯罪的類型，並利用已掌握的情況分析可能作案的人員，若案情需要也可訪談相關人員，並規劃鑑識執行的策略。

(二)決定搜索地點、對象與時間

當發現可能之嫌疑犯，約談與案情相關的人員，例如系統管理人員、相關廠商及被害人等，再深入瞭解案情，綜合所蒐集的資訊，以決定蒐索的人、事、時、地、物、理由、範圍等之資訊。

(三)工具的準備：

(1) 電腦軟硬體規格的參考手冊：彙整各種電腦軟硬體設備規格資料、一般及特殊的電腦或網路系統基本資料描述等，以作為搜索前或現場搜索時對於搜索標的有深入的了解而不盲目搜索，進而決定後續採證技術方法及工具的選擇。另外避免因不適宜的採證技術方法、工具或動作，導致重要證物資料的毀損、遺漏。

(2) 犯罪工具程式的參考手冊：

彙整目前可能作為網路入侵或攻擊之工具程

式，作為犯罪現場搜索重要標的，並提供證據與入侵者關聯之重要參考。

（3）破解電腦密碼工具：

對於搜索現場之電腦設備設定有開機或啟動密碼等，運用破解工具程式或社交工程等方式取得進入密碼，以利數位證物採證。

(四)人員的專業性：

對於一些鑑識工具的使用，鑑識人員必須有具備專業性，也就是鑑識人員應該考取相關鑑識證照或認可，才不致於在鑑識過程中遺漏寶貴的數位證據，甚至是破壞掉數位證據。

(五)技術勤前之講習：

在每次要出任務時，都必須要對鑑識人員進行進一步的說明，說明搜索任務、項目，並檢查軟體及工具是否準備齊全，以避免一些意外狀況發生。

3.3 操作階段

3.3.1 蒐集

（一）變動性數位資料：

A、隨機存取記憶體、快取記憶體與暫存器

B、主機正在執行中的程序

C、網路連線與應用程式開啟通訊埠

（二）固定性數位資料：

A、應用程式的記錄檔(事件檢視器)

B、作業系統的記錄檔(事件檢視器)

C、安全事件記錄檔(事件檢視器)

D、系統登錄檔(regdump)

（三）檔案系統數位資料

A、交換檔/暫存檔-轉存記憶體

B、殘存檔案-bit by bit copy

C、未分配空間-debugfs、賽門鐵克反刪除軟體

3.3.2 分析

一、檔案：

A、檔案分析：

(a). 關鍵字搜尋

(b). 加密與壓縮檔軟體

(c). 找出隱藏檔案及資訊

(1). 搜尋隱藏 Stream

(2). 搜尋多媒體檔案

B、檔案系統：

(a). 殘存空間

(b). 未分配空間

(c). 交換檔

二、記錄檔（log）

三、Windows 登錄檔（registry）

四、判別惡意程式碼

五、其他：掃描遠端主機與 port 號

3.3.3 鑑識階段

一、報告撰寫

鑑識完成後，確定出犯罪嫌犯，最後還是要將所有證據及鑑識的結果，在法庭上當呈堂證據，故製作報告時必須遵守下列的原則：

（1）鑑識的每一個程序，均應準確、清楚、不混淆及客觀地記載，並記載於鑑識報告中，對於鑑識過程所使用到的方法、工具、軟體、硬體，亦要有詳實的記錄於鑑識報告中，故報告必須要完整及正確的記錄。

（2）鑑識報告要有鑑識單位之名稱和鑑識人員以及審查人員之親筆簽名。

（3）每份鑑識報告均應有唯一之識別編號。

（4）鑑識報告中不應含有鑑識人員對案件本身的主觀判斷。

（5）鑑識報告最好以表格的方式呈現，以降低鑑識報告的錯誤率。

二、法庭參考證物

鑑識報告是必須要給法官、被告及偵辦人員等相關人員閱讀的，故內容不宜太深奧，且又必須呈現真實的內容。原則上可供證據的物品皆應作為呈堂證供，即具有證據能力及證明力之證物都要呈現及報告於法庭上，由於證據資料龐大，若要一一列印出，可能其報表比人都還要高，故在簡報時，可以整理出圖表說明，但證據表現的形式必須符合法律規定，並作好法庭交互詰問的準備工作，以最專業及最真實的呈現給法官裁判。

4 結論

在本研究中整理電腦鑑識科學領域專家對於電腦鑑識的定義，瞭解電腦鑑識領域之概念及意義。而調查犯罪事件，講求調查程序及步驟，因此在電腦鑑識領域上，專家針對電腦鑑識執行程序提出各自觀點，認為電腦鑑識該如何執行、執行過程需注意哪些事項。本研究綜合一些專家與學者的意見，並提出的電腦鑑識的標準作業程序，這個標準作業程序包含了數位證據的來源、蒐集數位證據、分析數位證據及產生鑑識結果報告，同時介紹 Windows 作業系統相關的電腦鑑識工具。利用資訊科技進行攻擊或入侵，在法律上是已屬於觸法的行為，但是我國法規對於電腦犯罪所遺留下來的數位證據部份可以加以援用的條文卻極為有限。即使是有關電腦犯罪相關條文，也是寥寥無幾，這也顯示了當前我國法律條文必須因應時勢作適度增刪，以因應未來資訊安全犯罪事件。

本論文是朝向 Windows 作業平台的電腦鑑識研究，因此整個過程是以這個作業平台為主，並且提出一套完整的數位證據鑑識標準作業程序。另外利用一些相關的工具進行鑑識，每一項工具都有其特定的目的，因此搭配在論文中所提出的電腦鑑識標準作業程序，進行每一項工具的測試，而且依照測試結果再分門別類歸納到每個相對應程序步驟。

參考文獻

[1] 王進，電子證據的認定，2001 年。

[2] 行政院勞工委員會職業訓練局企業訓練聯絡網，2004 年，http://www.b-training.org.tw/btraining/etn_faq_Aq.asp。

[3] 吳文誠，「論我國之程序基本權及其所形成之程序保障體系」，國防管理學院法律研究所碩士。

[4] 於朝，檢察機關電子證據的收集與固定，2004 年，http://www.law-lib.com。

[5] 張媛媛，電子證據的法律挑戰，北大法律周刊第 5、6、7、8、9 期。

[6] 劉志超，論電子證據在刑事訴訟中的運用，盱眙縣人民法院，2004 年。

[7] 羅傳賢，行政程序法基礎理論，台灣五南圖書出版公司，1993 年。

[8] Albert J. Marcella, Ph.D. Robert S. Greenfield editors , 2002, Cyber forendics-A field manual for collecting, examining, and preserving evidence of computer crimes. Chapter 8.

[9] Albert J. Marcella, Robert S. Greenfield, 2002 Cyber Forensics: a field manunal for collecting, examining, and preserving evidence of computer crimes, Auerbach Publications.

[10] Deniz Sinangin, Computer Forensics Investigation in a Corporate Enviroment, IEEE Computer Fraud & Secutity, 2002.

[11] Eoghan Casey, “Digital Evidence and Computer Crime: Forensic Science, Computer and The Internet”, Academic Press, 2000

[12] New Technologies Inc., Computer Evidence Processing Steps, Retrieved May 7 1999, http:/www.forensics-intl.com/evidguid.html

[13] Timothy Wright, The Field guide for investigation Computer Crime:search and seizure basic part three, security focus, 2000.

[14] Tohmas Rude,Evidence Seizure Methodology for computer forensics, crazytrain, 2002.