電腦鑑識程序之研究

A Survey of the Procedure for Computer Forensics

廖惠雯 助理教授
嶺東科技大學
資訊科技應用研究所
hwliao@mail.ltu.edu.tw

劉文港 碩士生
嶺東科技大學
資訊科技應用研究所
djkong123@yahoo.com.tw

摘要

隨著資訊科技的興起與電腦時代的來臨，利用電腦以及網路犯罪的問題，讓執法單位面臨了更大的挑戰與困難，如何利用在電腦上的鑑識相關工具來取得有效的數位證據，是當前迫切所需要的課題，一般鑑識單位針對無法開機鑑識的電腦主機，大多使用 Linux Live CD 整合鑑識工具研究，但以目前電腦作業系統來看，以 XP 作業系統佔有率最高，文本研究提出電腦鑑識程序，利用 XP Live CD 整合電腦鑑識相關工具，建置實驗環境，針對電腦犯罪情事，採集相關證據，經由搜尋、分析、驗證階段，探討解決方法。通常單一鑑識工具所提出的證據不足，但以測試多套鑑識工具使用，過程中產生的相關癥結，最後彙整鑑識報告，相信能讓調查鑑識人員於數位證據擷取上趨於完善，在法庭呈現上的證據多一分效力。

關鍵詞：電腦鑑識、數位證據、Live CD。

Abstract

With the emergence of information technology and the advent of the computer age, the use of computers, as well as the issue of Internet crime, including fraud, is one of the most significant challenges that the law enforcement agencies have ever faced; the difficulties in detecting some criminal behavior, significant under-reporting (particularly by big business) and the lack of any meaningful statistics on the nature and incidence of electronic crime leads to the urgent need for the computer forensic tools to collect effective digital evidence; At present time, forensic divisions often use the Linux Live CD forensic integrated tools to handle the cases where they are unable to boot up the computer to gather forensic evidences; however, current computer operating system is mostly Window XP; thus, this paper will use XP Live CD integrated computer forensic tools to study computer forensic procedures; The process will build an experimental environment, then use computer crime cases to collect relevant evidences, perform research, analysis, validation, and explore solutions. Usually a single forensic tool presents insufficient evidence, but when more forensic tools are used, the relevant crux can obtained during in the processes and presented in the forensic final report; I believe it will allow officers, who are investigating digital crimes/frauds, capture more complete evidences, and thus improve the chance at the court.

Keywords: Computer forensics, Digital evidence, Live CD.

1. 緒論

1.1 研究背景

隨著資訊科技的興起與電腦時代的來臨，網路大量且迅速發展，高深的學問與知識也能讓一般大眾輕鬆的取得和學習，相對的也浮現了電腦犯罪的問題，在真實生活上所發生的刑案封鎖現場，檢調單位會同鑑識小組，在現場採集犯罪者所遺留下來的重要的證據，經過分析比對犯罪者相關證據後，再經偵辦檢察官起訴並逮捕犯罪者，誠如刑事鑑定專家李昌鈺博士所說，凡走過必留下痕跡，利用電腦鑑識來擷取電腦犯罪所遺留的數位證據亦是相同，刑事鑑定所鑑識的物品為實體物證，而電腦鑑識的證據，大部分是以數位科技設備所產生的電子紀錄，以數位證據稱之，因此電腦鑑識的工作，必須依賴特定的工具加以蒐集分析，才能當作檢調單位在法庭上有力的間接證據。

1.2 研究動機

近年來電腦犯罪案例層出不窮，讓司法機關與執法單位面臨了更大的挑戰與困難，因為此時的刑案現場，已經由一般的真實生活拓展到資訊電腦的平台上，無遠弗屆的網際網路上也成為一個犯罪的場所，在國外政府單位、企業機關甚至個人都具備電腦鑑識技術，法律針對電腦犯罪所頒佈的明文規定也相當完整，反觀國內，目前電腦鑑識仍屬於起步階段，缺乏相關學者研究，所以本文提出電腦鑑識程序，盼能提供國內鑑識單位參考。

1.3 研究目的

如何讓經過電腦鑑識分析後的數位證據可以具有公信力及法律地位，分析電腦犯罪的型態及電腦作業平台上所能利用的電腦鑑識相關工具，是調查鑑識人員需要清楚了解的問題。當有心人士利用電腦犯罪，進而有損他人利益等非法行為發生時，如何找出犯罪者在電腦留存的相關紀錄檔案以為事實證據，讓檢調單位作為佐證，電腦鑑識工作嚴然已成為資訊安全領域裡，不可或缺的重要技術之一，一般鑑識單位針對無法開機鑑識的電腦主機，大多使用 Linux Live CD 整合鑑識工具研究，但以目前電腦作業系統來看，以 XP 作業系統佔有率最高，文本研究提出 XP Live CD 整合電腦鑑識工具，建置實驗環境，針對電腦犯罪情事，採集相關證據，經由搜尋、分析、驗證階段，探討解決方法。通常單一鑑識工具所提出的證據不足，但以測試多套鑑識工具使用，過程中產生的相關癥結，最後彙整鑑識報告，相信能讓調查鑑識人員，數位證據擷取上趨於完善，能在法庭呈現上的證據多一分效力。

1.4 研究範圍及限制

目前已知約有 20 餘種的電腦作業系統，根據 Market Share 對全球作業系統佔有率的報告顯示，到 2007 年 11 月為止，XP 為 78%，作業系統佔有率還是以 MS Windows 系列獨大，見圖 1，相對的成為電腦犯罪上常見的作業平台，因此，實驗環境建置的軟體工具，主要針對可在 XP 作業系統下執行。

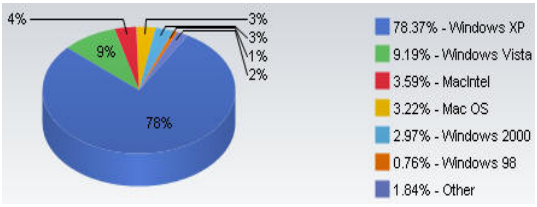

圖 1. 作業系統佔有率[25]

1.5 研究架構及方法

本研究之架構，由緒論開始說明研究的背景、動機、目的，並為了讓研究結果能更加完善，文獻探討首先對電腦犯罪與科技法律做初步的瞭解，再配合電腦鑑識蒐集數位證據，建置實驗環境，最後提出結論與建議。

2. 文獻探討

2.1 詮釋電腦犯罪

現今生活使用電腦的普遍性，達至家庭個人，使用者可以快速而有效的處理大量工作以及資料，使得重要資料皆儲存其中，一旦被有心人士所利用，其所造成的損害，對受害者肯定不小，加上近年來發展蓬勃的電腦網路，可將資訊傳達到世界的每一個角落，網際網路上變成盜版、色情犯罪者利用的場所，因此學者指出網路必須開闢警察巡邏區域[1,26]，學者 Morris 指出應設立網路警察[27]，以解決有心人士以網路當作犯罪場所的問題。利用電腦資訊科技的技術，進行有損他人利益之情事，我們稱之為電腦犯罪，有人戲稱電腦已成為槍枝發明以來，威力最強大的犯罪工具，故有探討的重要性與迫切性[2-4]，電腦佔了我們生活密不可分的關係，學者 Bawden[28]大膽的預測，未來除了性侵害案件外，幾乎所有犯罪均可能利用電腦科技來完成，此時電腦在犯罪中所扮演的角色，主要可以分成以下三類[5,29]：

一.以電腦作為犯罪工具

甲利用 BBS 或論壇發佈對乙不實的訊息、使乙的名譽受損。駭客利用電腦軟體程式入侵受害者電腦，竊取受害者電腦上資料。

二.以電腦作為犯罪場所

透過電腦網路傳遞病毒或木馬程式至全球電腦使用者的主機上。

三.以他人電腦作為犯罪目標

駭客利用電腦作業系統漏洞來控制他人電腦主機，進行電腦犯罪活動。

2.2 電腦犯罪動機

學者 Philippsohn[30]提出截然不同的電腦犯罪動機，以政治動機：國際上處於對立的國家，人民與人民之間的國情不同、政治或民族意識型態的鼓舞而導致互相攻擊入侵對方的網站。國內黃景彰教授[6]分析電腦犯罪的動機包括了：好奇、破壞、報復、金錢利益與競爭利益及蒐集情報。廖有祿教授[7]提出電腦犯罪的動機事實上以圖利為主、其次是好玩、報

復、詐財、侵佔、及破壞等。

2.3 電腦犯罪趨勢及威脅統計

根據 2006 CSI/FBI Computer Crime and Security[31]調查研究報告，圖 2 我們可以瞭解: 近七年來(1999-2006)電腦犯罪攻擊統計，資訊安全最大的威脅依然是病毒，其次是筆記型電腦或可移動設備遭竊，再其次是企業內部網路濫用，值得注意的是：在 2003 年剛成長的資訊科技中，無線網路濫用威脅直到 2006 年均為最高。近年來，在政府、企業及學校宣導資訊安全的重要性，讓每個人都有資訊安全的認知，不少重大的電腦攻擊事件已漸漸下降，可從圖 2 看出電腦犯罪攻擊趨勢。

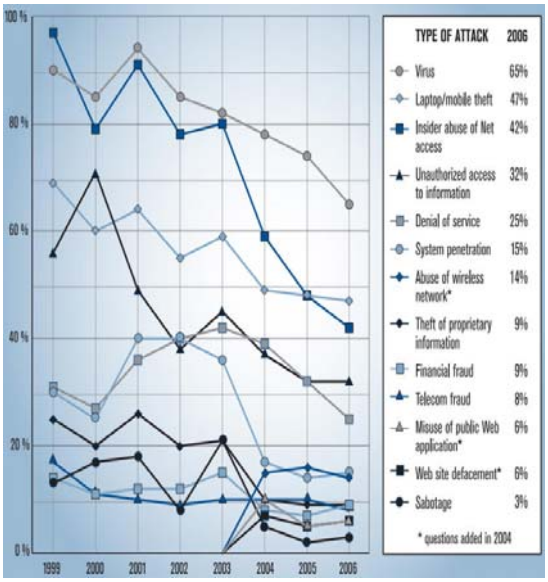

圖 2. 近七年來電腦犯罪趨勢及威脅統計[31]

根據美國 CERT 觀察利用電腦網路技術犯罪分析的趨勢[8]，大致分為以下：

一.自動化攻擊程式：

網路上入侵攻擊的第一步，通常是搜尋目標受害者，因此駭客都會先使用偵測掃描漏洞程式。隨著電腦科技的發展進步，中央處理器 CPU 處理資料速度加快，以至於掃描速度大增。掃描的用意在於找出電腦作業系統的弱點以及漏洞，藉此可以找出入侵電腦作業系統的入口。

二.入侵工具漸趨複雜：

編寫程式的語言軟體，在軟體的開發時間上縮小，技術也越來越成熟，駭客開發入侵工具的特徵會比以前更難以分析發現，導致防毒軟體或防木馬後門植入軟體常常發生誤報情形，造成使用者的困擾。

三.作業系統漏洞曾出不窮：

當紅兩大作業系統 Windows 及 Linux 都含有未知系統漏洞，每個月幾乎都會發佈系統漏洞修補程式，例如系統組件更新，服務升級包(Service Packs)，安全修補程序(Security fixes)。

四.防火牆穿透能力提升：

防火牆是公司企業依照需求制訂規則，允許或是限制存取網路資料流量，防火牆大致可分為硬體式或軟體式兩種架構，穿透防火牆的協定 IPP(Internet Printing Protocol)，駭客利用此協定設計一些可以產生 Buffer Over Flow 的程式碼，藉此取得主機上的權限[9]。著名 SoftEther[10]軟體便是可以穿透防火牆的工具之一，由日本大學生－登游大所開發的網路連線軟體，在使用者的電腦中模擬出一塊虛擬的網路卡，並且利用這塊網路卡來與遠端的服務器進行連接，讓所有連接到這個服務器中的電腦就像在同一個區域網路進行資料交換一樣，SoftEther 設計架構是以 OSI Level 2(資料連結層)上軟體模擬網路通訊，將實體層的通訊內容封包軟體模擬 Ethernet 到 TCP Package 裡去，把自己的通訊包變成 SSL Session，用 HTTPS 傳輸協定穿越 Internet，能穿透 Firewall 128 bit RC4，SoftEther 傳輸封包所走的是類似 VPN 的協定，因此可以跳脫防火牆的限制，處於防火牆後方的使用者能夠很容易的穿透防火牆而存取到被網路管理人員所禁止的網路連線，讓網路管理人員所設定的嚴密網路規則形同虛設，日本資訊處理事業協會 IPA[10]便要求這位築波大學學生停止公開此程序，在許多公司為了安全因素，也禁用此款軟體。

五.非對稱式攻擊：

駭客藉由入侵多台受害者主機，並植入木馬後門程式。選定一台真正的攻擊目標(victim host)，部署代理機器來控制多台受害者主機對攻擊目標發動非對稱性攻擊。

國內經濟部智慧財產局發佈電腦犯罪的形式[11]分析如下：

一.誹謗

透過網路電子布告欄（BBS）散播他人不實之事，使他人名譽嚴重受損。

二.詐欺與不實廣告

設立網路，提供與事實不符之物品，販售他人；或未提供物品，詐取他人金錢。

三.色情

利用網路傳送男女性愛圖畫，於網頁上標示猥褻圖文，對外紹募會員，以每月二百元的代價供其會員下載觀看。 設立色情網站，以招募會員的方式，透過電子信箱與顧客進行交易，販售以男女交媾為主題之色情光碟。

四.毀損罪
網路上散播足以毀損他人電磁資料之電腦病毒，造成企業及個人無法正常使用電腦。
五.賭博
利用網路架設網站提供他人下注或聚賭。
六.煽惑犯罪
意圖煽惑他人非法持有槍彈，公然販賣槍枝，介紹有關槍枝之規格、性能、配件以及販賣價格、訂購方武與交槍方法等資訊，或設立網站教人製造炸彈。
七.侵害著作權
利用光碟燒錄機，重製他人著作之電腦軟體，並利用網路陳列目錄進行銷售。
八.竊盜
駭客闖入他人網路系統竊取機密文件之行為。
九.侵占
公司職員利用修改電腦程式，對於客戶之存款予以侵占。
十.其他
尚有侵犯他人商標、威脅刺殺生命、恐嚇炸毀住所，販賣違禁物品、網路上傳播足以破壞他人經濟信用的消息、侵入國防機密系統、未經授權侵入他人的系統檔案或窺看電子郵件、假冒他人名義，發送涉及權利義務的電子郵件或偽造金融卡。

2.4 電腦犯罪損失統計

在2006年電腦犯罪損失統計由大到小依序為病毒、未授權登陸、筆記型電腦或可移動設備硬體被竊、業界公司重要資產信息被竊等，筆記型電腦或可移動設備硬體被竊迅速竄升，可從圖3看出：前四名就佔了將近所有安全損失的四分之三。

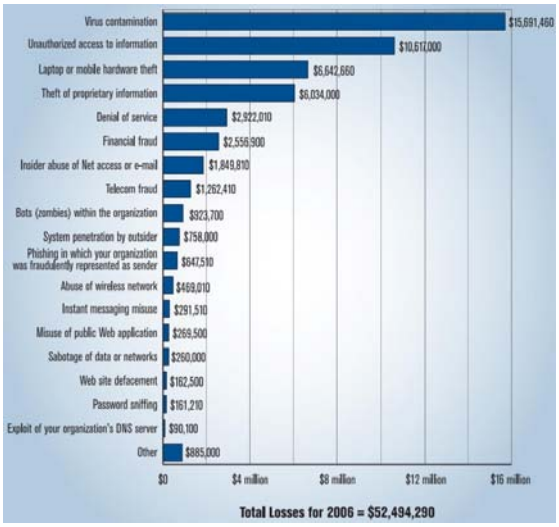

圖 3. 電腦犯罪損失統計 Dollar Amount Losses by Type 2006 年[31]

對比 2005 年的統計資料我們可從圖 4 看出：病毒的破壞損失依然是最高的，佔據著損失的第 1 名。

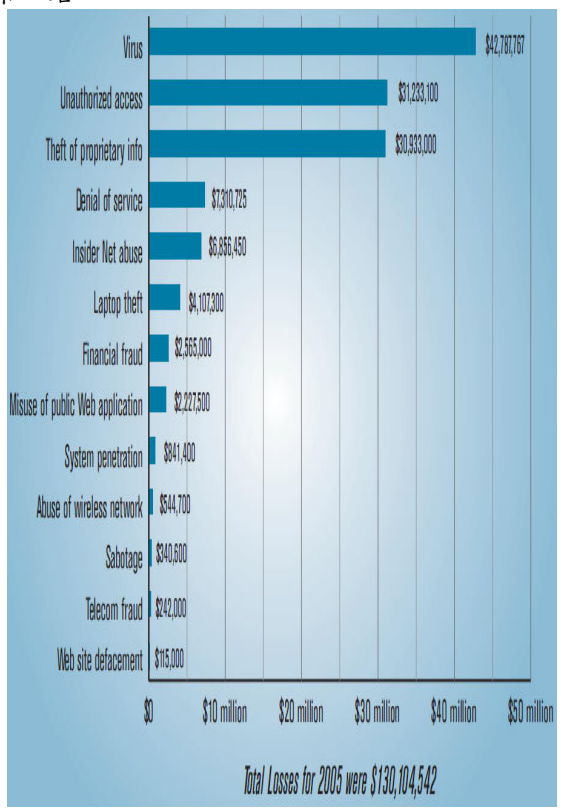

圖 4. 電腦犯罪損失統計 Dollar Amount Losses by Type 2005 年[32]

對比 2004 年，可從圖 5 看出：阻斷服務攻擊(DoS)在 2005-2006 年沒有大規模的發生過。

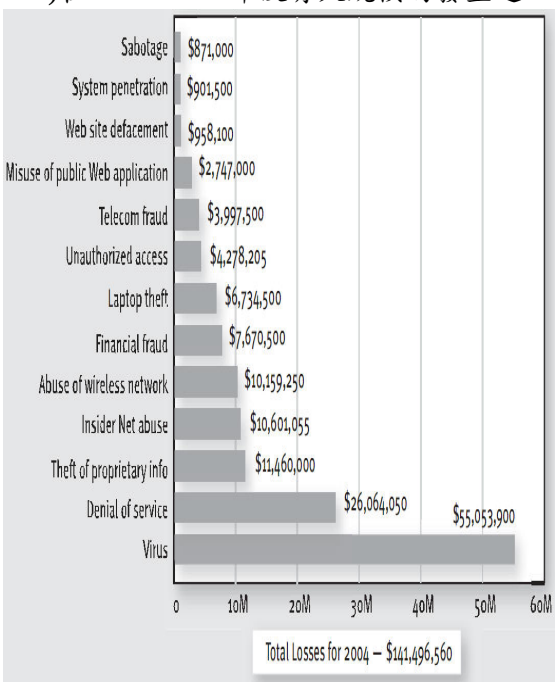

圖 5. 電腦犯罪損失統計 Dollar Amount Losses by Type 2004 年[33]

2.5 電腦犯罪安全技術應用統計

CSI/FBI 在 2006 年把鑑識工具、防木馬後門植入軟體獨立出來，長期以來入侵偵測系統(IDS)佔據第 3 名的位置也被取代，防木馬後門植入軟體並非新出現的技術，之前在資安領域都是歸類在防毒軟體類別下，近年來由於入侵偵測系統(IDS)越來越不能滿足企業用戶的需求，預警的功能有限，部署及應用已逐年下降，另外電腦資料數據在傳輸存取中的加密也越來越受到企業用戶及一般個人的重視，可從圖 6 看出。

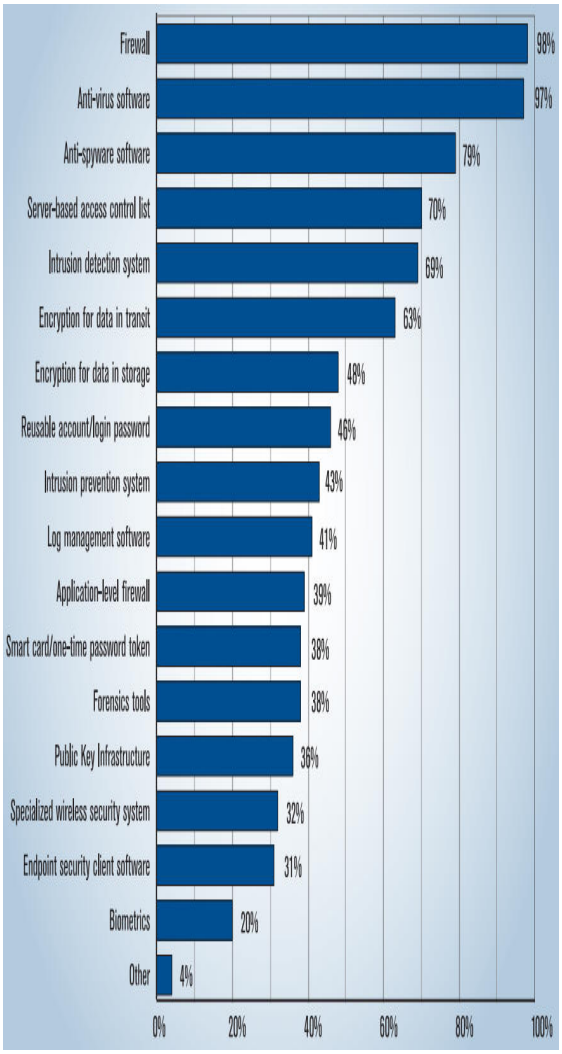

圖 6. 電腦犯罪安全技術應用統計 Security Technologies Used 2006 年[31]

2.6 科技法律

資訊科技日新月異之下，例如電腦網路的快速發展，背後所衍生出的電腦犯罪行為相對的也不斷推陳出新，目前在每個國家的立法條文上，對於未經授權而不法接近、截取與入侵電腦之行為都設有刑法之規定。面對電腦犯罪的行為在各國家定義各有差異，當然法律規定上也不同。美國對於電腦犯罪行為的規範上，最早訂立出現在「防止電腦詐欺與濫用法」(The Computer Fraud and Abuse Statute，1984 年所立)，即美國聯邦法規 18USC、第 47 章、第 1030 條，明文規定禁止未經許可或意圖詐欺的使用政府電腦，同時也對這些使用的行為訂定刑罰與相關處置，例如可以將犯罪者的連線工具沒收。CIA 和 FBI 根據電腦詐欺和濫用條款，清楚的被賦予管轄權，來調查條款中所訂定的六項電腦犯罪行為[12]。規範上僅限於政府或金融機構，電腦系統未經授權進入使其有影響的之行為[13]。之後，美國聯邦在 1986 年公佈了「電子通訊隱私權法 ECPA（Electronic Communications Privacy Act）[35]，並於 1994 年作了大幅度的修正，增修了禁止攔截無限電及電子通訊行為之規定[36]。該法對於取得、變更或防止授權進入電子儲存（electronic storage）資料之行為，特別訂定處罰之明文條款。且於 1996 美國聯邦法規制定「國家資訊基礎建設保護法」NIIPA[14]（National Information Infrastructure Protection Act），用來修正前述之「防止電腦詐欺與濫用法」(The Computer Fraud and Abuse Statute）的不足。此次修正在於為了使適用範圍能夠涵括到所有在州際商業或通訊中的電腦，乃將其所規定範圍由原先的「聯邦利益電腦」(federal interest computers）擴大到「受保護之電腦」(protected computers）的概念，使法規不再僅限於政府或金融機構的電腦系統。即便是涉案的多部電腦僅位於同一州境內，但只要該等電腦與網際網路係處於連線之狀態，便足以成為「國家資訊基礎建設保護法」NIIPA 所規範的對象。

學者 Anne W. Branscomb[20]解讀關於美國電腦犯罪刑法上的見解如下：

一.未經電腦所有人授權意圖侵入或使用。

二.將傳統上財產權之概念，擴及到可以包含有電子資料和電腦科技在內。

三.未經授權侵入電腦系統之行為視同不法侵入、將惡意銷毀或變更資料行為視同暴力行為、將非法複製程式或資料行為視同竊盜。

四.利用電腦作為犯罪工具從事犯罪行為者。

五.非法變更、損害、 刪除、電腦檔案的行為。

六.美國聯邦著作權法中，關於侵害著作權的行為，列入等同於侵害州政府主權之違法行為。

七.任何人的行為，若損及授權使用者，並獲取該部電腦系統設備所能提供的資料者。

八.未經授權之人，假裝其已經獲得合法的授權，進而達成控管電腦的行為，來從事其不法

之犯罪目的者。
九.針對電腦病毒或具有破壞性程式訂定條文。

國內目前用來規範電腦犯罪行為之相關法律依據有：普通刑法、著作權法、電腦處理個人資料保護法、電信法、通訊保障及監察法、電信法等。了解我國法律對電腦犯罪的認定，並且配合調查人員實地採取調查、收集證據，在合法規定範圍調查犯罪。刑事警察局自 95 年 4 月成立科技犯罪防制中心[15]，針對新興科技(資、通訊)犯罪手法不斷研究偵查與防制之道，如非法電信機房查緝與掃蕩、電腦鑑識與事件調查、網路詐騙監控與分析等，皆與民眾生活息息相關，影響社會治安甚鉅。司法單位才起步之電腦鑑識而言，數位證據對於犯罪偵查之重要性，已在中心成立電腦鑑識實驗室，研發最新電腦鑑識技術，培育電腦鑑識專才，以解析數位資訊特徵，協助全國警察機關偵辦各類刑事案件，並接受各地法院、檢察署等司法機關等送鑑相關數位證物。

電腦犯罪相關法律條文，刑法及刑事訴訟法均有明文規定，引述最重要的刑法第十五章第 220 條第三項：在紙上或物品上之文字、符號、圖畫、照像，依習慣或特約，足以為表示其用意之證明者，關於本章及本章以外各罪，以文書論。錄音、錄影或電磁紀錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以為表示其用意之證明者，亦用。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。

2.7 電腦鑑識

資訊科技的電腦技術進步，導致電腦犯罪日漸遽增，以一般刑事案件舉例，傳統鑑識調查主要以刑案現場還原為主，在過程中取得佐證，並在法庭上呈現證據，鑑識調查人員必須瞭解電腦鑑識，相對於一般傳統鑑識上不同。1991 年在波特蘭的國際電腦專家協會 IACIS (International Association of Computer Specialists) 中，首次提出電腦鑑識科學 (Forensics Computer Science)[40]，主要目的在於定義電腦鑑識程序，數位證據之保存（Preservation）、鑑定（Identification）、淬取（Extraction）與文件化（Documentation），協助調查人員偵辦電腦犯罪，作為數位證據之蒐證與鑑識方法，以確保證據的完整性，作為法庭審理電腦犯罪案件的參考證據。電腦鑑識就像傳統刑事鑑識一樣，主要的共同點有犯罪現場採集證據，確認犯罪時間、地點、使用之工具關聯性，進而重建還原犯罪現場。誠如刑事鑑定專家李昌鈺博士所說，凡走過必留下痕跡，亦即犯罪者在犯罪過程中，必會在現場遺留部分的痕跡，傳統刑事鑑識的指紋、毛髮及血液，好比電腦鑑識的使用者登入 Log 訊息、網路位址等。證據可能因為存在的時間短暫，或者分散各處難以採證，實驗室中分析及擷取的技術都關係著鑑識的正確性。學者 Kuchta [38] 認為電腦鑑識程序如下：準備工作(Preparation)、紀錄與文件化（Documentation）、收集（Collection）、驗證（Authentication）、分析 （Analysis）、保護（Preservation）、產出結果 （Production）、報告文件（Reporting）八種程序。學者 Thomas Rude[39] 認為電腦鑑識程序如下：電腦鑑識準備工作(Preparation)，快照（Snapshot），移轉（Transport），實驗室鑑識準備工作(Preparation)，調查（Examination）。

王旭正學者等人提出電腦鑑識程序[16]：
1.保存證據：
調查人員必須確保犯罪現場證據的原始性，重點在於確定證據完整性，不能被竄改及刪除造成變動，偵辦人員必須製作原始證據的鏡映像檔，利用加密驗證方法加以保存以保障證據。
2.檢驗證據：
調查人員利用鑑識工具，將被刪除的重要證據資料，還原並加以檢視。若是遇上需要輸入密碼才能觀看的檔案，必須利用破解密碼工具加以破解再進行檢視動作。
3.分析證據：
調查人員取得證據之後，檢驗分析結果是否可以連結到嫌犯關係，藉以推斷犯罪行為及證明罪行。
4.結果呈現：
釐清相關疑點，鑑識證據結果確定犯罪行為。

為了提升辦案品質、建立專業分工制度、培育辦案特長，並且適時支援地區警察機關偵辦重大、特殊刑案，以有效遏制犯罪，民國八十五年內政部警政署刑事警察局下設偵查第九隊[17]，該隊前身為電腦犯罪偵防小組，是國內電腦犯罪的主要偵防單位，專責資訊、網路、科技相關犯罪偵查。民國九十二年二月二十二日成立「刑事鑑識中心」，鑑識科負責各犯罪鑑識工作專司，其工作內容分為毒物、聲紋、電氣、痕跡、測謊、影像、綜合、印文、化學、物理十個鑑識組別，見圖 7。

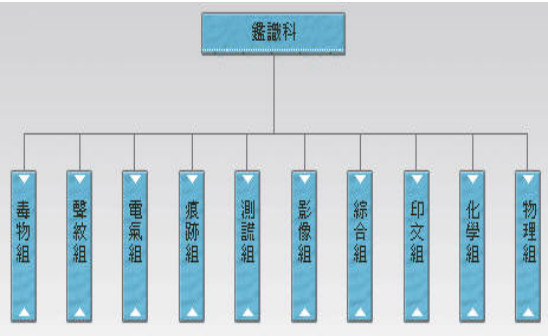

圖 7. 刑事鑑識科[18]

刑事鑑識中心解釋刑事科學或刑事鑑識為將科學應用於法律上的一門學問，舉凡可解答在法庭上被質疑問題的任何科學領域均屬之。例如：刑事化學、刑事工程學、刑事攝影學、法醫學、刑事牙醫學、指紋學、刑事血清學、文書鑑定、筆跡鑑定、槍彈鑑識、工具痕跡鑑定、刑事昆蟲學、刑事骨骼學、影像處理技術…等均屬之。

電腦犯罪主要以調查局的電腦犯罪防制科專司，主要以維護國內網路安全，防止犯罪集團進行攻擊行為，目前以偵辦刑法第 36 章妨害電腦使用罪章為主，此章犯罪型態有四種，列舉如下：
一.無故入侵電腦系統罪。
二.違反保護電磁紀錄罪。
三.干擾電腦系統罪。
四.設計違反電腦犯罪之程式罪。

法務部調查局於 2006 年底正式建置國內首座「資安鑑識實驗室」[19]，成立目的有以下：
一.建立電腦鑑識制度。
二.培養電腦鑑識人才。
三.電腦犯罪案件採證。
四.幫助企業建立資安防護。
五.檢察官或法院審理案件，鑑定相關事證。

TAF 財團法人全國認證基金會其下之中華民國實驗室認證體系 CNLA[20](Chinese National Laboratory Accreditation)，CNLA 致力於推動國內實驗室(Laboratory)及檢驗機構(Inspection Body)各領域之國際認證，建立國內實驗室/檢驗機構品質與技術能力之評鑑標準，依據國際標準 ISO/IEC 17025、ISO 15189 及 ISO/IEC 17020，結合專業人力進行實驗室/檢驗機構評鑑及認證，提昇實驗室/檢驗機構品質與技術能力，並輔以能力試驗(Proficiency Testing)活動來確保實驗室之技術能力保持在一定水準之上，CNLA 提出實驗室認證共通規範有：
一.組織：
實驗室或其所屬組織，應是負法律責任之實體，且應遵守 CNLA 所訂之規範，並選任一人為負責人，以及數位鑑識報告簽署人。
二.品質系統：
應建立、實施及維持一套適用其活動範圍之品質系統，並將政策、系統、方案、程序及工作說明予以文件化至需要的程度，並製訂相關品管手冊，以確保鑑識結果之正確性及品質。
三.文件管制：
需建立與維持各種程序，以管制構成品質系統之所有文件。例如工具操作冊、鑑定程序方法、依循法規等，並能夠適時的調整以維持常新。此外，所有實驗室所產生的文件需要有唯一的識別。
四.鑑識工作外包：
實驗室無論因任何非預期的原因（如需更進一步深入的專業技術）將工作外包時，此工作仍需交給有能力者（同樣經過認證之實驗室）。
五.保密條款：
鑑識結果，不得洩漏予第三人。
六.鑑識程序修正措施：
實驗室應建立矯正措施之政策與相關程序，當品質系統或鑑識程序出現偏差時，應能及時修正。同時，實驗室要有隨時監控鑑定結果的機制，以確保所採取程序之有效性。
七.紀錄管制：
實驗室應建立程序，以鑑別、蒐集、索引、取閱、建檔、儲存、維護及銷毀品質與技術紀錄。這些紀錄至少要保存三年。
八.實驗室稽核：
實驗室應定期地對所有程序進行稽核，以查證作業程序是否持續符合品質系統之要求。稽核項目至少應涵蓋 ISO 17025 要求之項目，且要定期（至少一年一次）對實驗室的品質系統與鑑識程序進行審查，以確保其持續地合適性與有效性。

2.8 數位證據

數位證據具備了易消失、易更動、不易取得等特性，證據表示上，以各種鑑識工具的性質不同，會有不同的分析結果呈現，各國法律所定義的數位證據標準也不同，一般法律專門人士在電腦資訊上的技術無法瞭解，而電腦鑑識人員對法律知識的瞭解也不夠，此時可能造成數位證據在法庭上的效力有所遞減，嚴重者，造成不被採信的結果，鑑識人員必須瞭解

所採集到的數位證據，是否可以在法庭上被採納，在國外有專門測試鑑識相關工具，證實證據的有效性，由政府機構在法庭上通過認證的辯護電子犯罪研究所[41]，可以幫助電腦鑑識單位所研發的軟體，在法庭上具有公正性。林宜隆教授[21]認為調查人員，不單單只是針對電腦本身所儲存的資料作分析，必須與其他證據相互配合，才可以表現出證據的公信力。在所有的犯罪調查行動，最後都會匯出整理的報告，成為在法庭上實際的書面證據，電腦鑑識產生的數位證據也不例外，要在法庭上發揮證據的效力，必須實施嚴謹的調查程序、符合法定標準，最主要調查人員要注意以下二點：

一.工具之合法性[42]：

電腦鑑識的工具必須取得合法使用權。調查人員必須從軟體製造商處獲取許可使用的授權。

二.收集過程之合法性：

我國刑事訴訟法第 154 條規定：「犯罪事實應依證據認定之，無證據不得推定其犯罪事實」。而且「證據是指在刑事訴訟法上具證據能力，並依本法所規定之方法為調查，而能做為認定犯罪事實之基礎者」。

英國警察協會(Association of Chief Police Officer, ACPO)參考國際電腦證據組織(International Organization of Computer Evidence)數位證據採集原則，在 1999 年提出「The Good Practices Guide for Computer Based Evidence」四項電腦證據處理指導原則[40]，依此原則處理的數位證據，才可具備法院上所認可的證據能力，此四項原則分述如下：

一.為了取得法院對於數位證據的信任，處理刑事案件的警察人員或委託人員，必須確保數位證據為犯罪現場原始的狀態，內容不得修改。

二.在例外情況下，如果需要存取原始電腦物證的資料，必須由有能力處理的人員，進行存取的動作，且對其處理的動作應予說明，並適當解釋證據的意義。

三.對於電腦物證的任何稽核資料或其它紀錄的處理過程，應建立處理方法與保留結果，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。

四.案件承辦的負責人，不管任何人存取電腦資料或使用拷背設備存取資料，都必須確保遵守法律的規範與以上處理原則。

學者 Eoghan Casey 認為電子儲存裝置中所存放的資料[40]，如：聲音、文字、影像、圖片等，若足以構成犯罪要件資訊，即可稱之數位證據。黃景彰教授[6]認為，犯罪者利用電腦或網路從事犯罪活動，在電子儲存裝置產生 0 與 1 等數位符號、所組成的資訊表現為法律上犯罪事實之認定，即稱為數位證據。不同於傳統證據有形體、可觸摸的到，數位證據本身以電波或電磁方式紀錄在電子儲存裝置上；數位證據是我們肉眼看不見的，必須經由電腦鑑識加以讀取、分析，轉換成人類能了解的資訊。

林一德教授以法律觀點來看數位證據可以分為以下幾類[22]：

一.書證：

原始證據資料以書面文字記載，後來輸入電腦中儲存。由書面文字轉成電磁記錄、以二進位資料型態存放在磁性媒體上，不具備人類可直接讀取的特性。因此若將其原始資料印製在電腦螢幕上並且列印輸出，即能還原始書面文字資料，具備可直接讀取能力，即可視同是書證。

二.物證：

此類證據必須實地的去實驗及操作，如此才能得知其證據內容，無法以外表或語言陳述該證據內容，必須透過電腦讀取才能得知內容。例如利用光碟機讀取光碟片，才能瞭解光碟片的內容；盜版的程式光碟片、唱片或者是色情光碟，此類光碟在外觀上形狀相同。

三.其他證據：

可輸出至文字檔或影像檔，直接成為一般證據。例如病毒程式或者色情圖片。

以刑案現場蒐證技術觀點來看[23]，在進行電腦鑑識所採集的數位證據，主要包含實體（physical）與邏輯（logical）兩種。

一.實體：

數位證據是存在於電子儲存設備的資料，進行蒐證時，使用存取資料方法，將資料分析出來的證據即為數位證據。

二.邏輯：

數位證據必須經由相關資源中粹取出來，資源包含 logfile、資料庫等等。

CERT 網路與系統安全實務一書所提出數位證據之收集與保存[8]，分析為以下四點：

一.進行電腦犯罪調查，所採集到的證據都必須以文件檔案紀錄留存。

二.針對電腦系統，製作案例複本以唯讀狀態進行分析，避免破壞證據原始性。

三.調查系統事件記錄檔尋覓線索。

四.將所有採集的證據作好分類，保存在一個安全無疑慮且未接受連線的儲存媒體裝置上。

3. 實驗環境建置

本研究提出調查人員在面對電腦犯罪問題時，電腦鑑識程序之作業流程，如圖 8 所示。

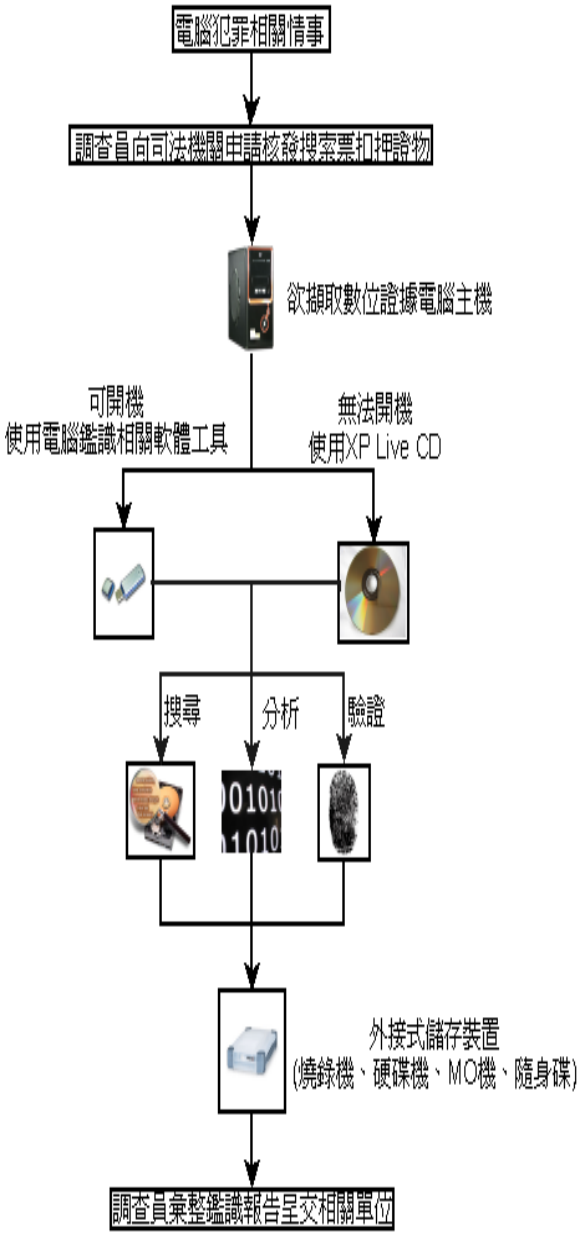

圖 8. 電腦鑑識程序

實驗電腦設備如下：
作業系統：XP Professional Service Pack 2
CPU：DualCore Intel Core 2 Duo E6300
系統記憶體：3.6GB
顯示卡：NVIDIA GeForce 7600 GT
虛擬系統軟體：VirtualBox 1.5.4

步驟一.
調查員偵察電腦犯罪相關情事，發現利用電腦網路當作犯罪工具、犯罪場所的違法者，調查員必須向司法機關申請核發搜索票，扣押違法者電腦主機等相關電子儲存裝置，因為所在網路上看到的相關犯罪事項，罪證並不是調查員所看到的網頁內容，原始內容可能在犯罪者自行架設網站的電腦主機、或委託外包公司架設網站的電腦主機。

本文研究以實際探訪利用電腦網路當作犯罪空間的違法者。
案例一.
網路聊天室中充斥著色情的陷阱，有心人士喬裝成援交妹，要求匯款轉帳，色欲薰心者自然容易上當受騙，造成金錢以及名譽損失，見圖 9、圖 10：

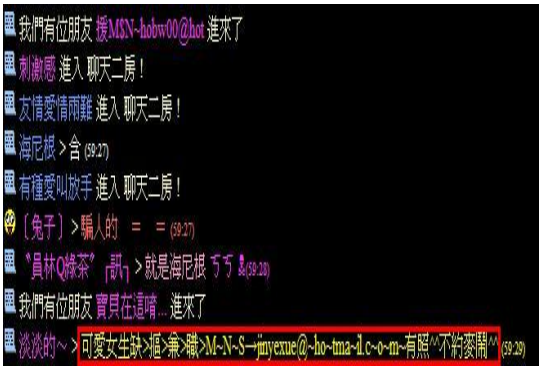

圖 9. 網路聊天室中充斥著色情的陷阱

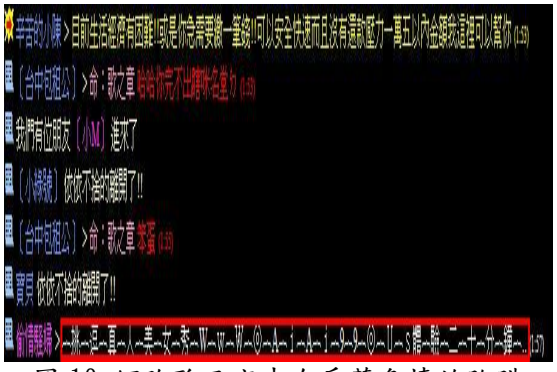

圖 10. 網路聊天室中充斥著色情的陷阱

案例二.
賣淫集團從以前的報紙刊登廣告，現以多元化的電腦入口網站介紹應召站女郎，見圖 11：

圖 11. 應召站女郎網站

案例三.

非法地下賭場也以電腦資訊化的方式經營，在網際網路上招收會員，見圖 12：

圖 12.賭博網站

案例四.

盜版商以商業化的經營理念架設網站，分門別類的目錄，詳細介紹盜版的新貨，見圖 13、圖 14：

圖 13.盜版網站

圖 14.盜版價目表

針對案例四，調查員使用 nslookup 工具，正解 xyz66.com 網站，查出其網站 IP 為 74.86.178.68，見圖 15：

圖 15. 正解 xyz66.com 網站

調查員使用 FastResolver 工具，正解 xyz66.com 網站，查出網站 IP 為 74.86.178.68，見圖 16：

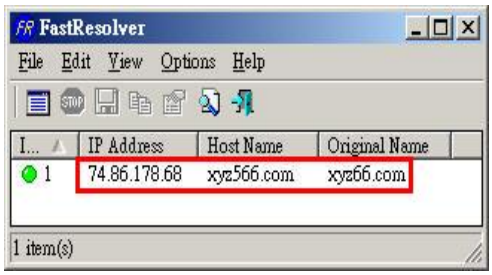

圖 16. 正解 xyz66.com 網站

調查員使用 DNS 查詢程式，探查 xyz66.com 相關主機資訊，見圖 17：

圖 17. DNS 查詢程式

調查員使用 IPNetInfo 工具，探查網站位置 IP 74.86.178.68 登記資訊，見圖 18。

調查員使用 WhoisThisDomain 工具，查詢 xyz66.com 登記網域名稱資訊，見圖 19。

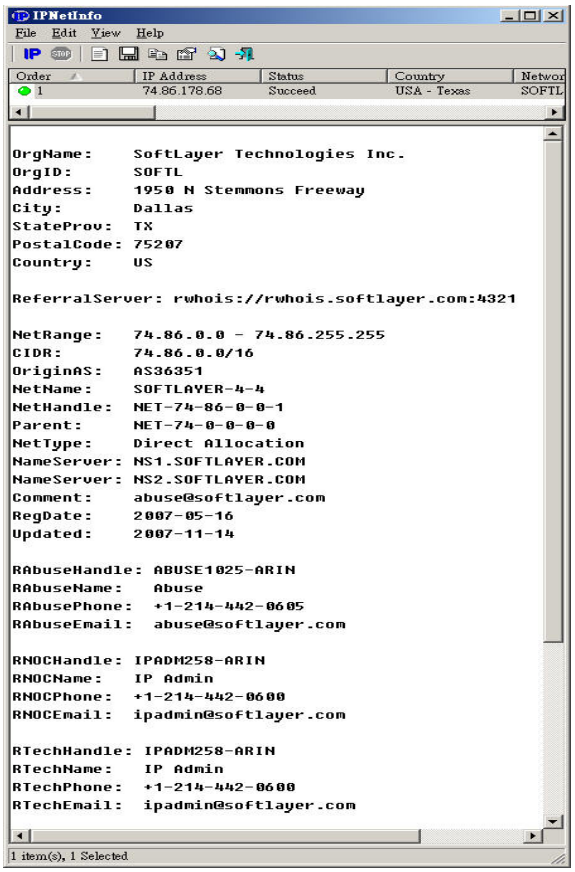

圖 18. IPNetInfo

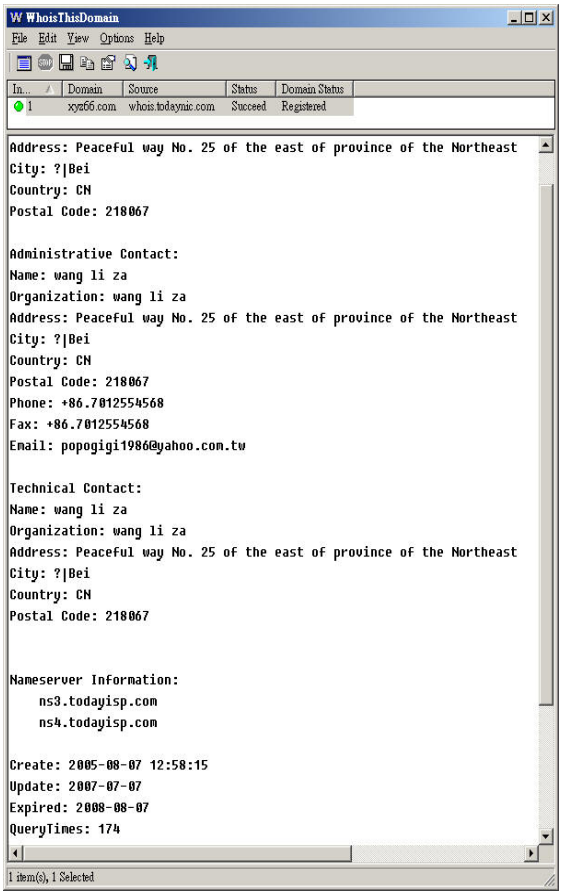

圖 19. WhoisThisDomain

步驟二.

調查員在扣押了證物之後，針對違法者的電腦主機如遇開機不了，無法順利進入作業系統調查證據，調查員以 XP Live CD 整合電腦鑑識相關工具順利開機成功，本研究以 VirtualBox[47] 虛擬系統軟體實驗，見圖 20、圖 21：

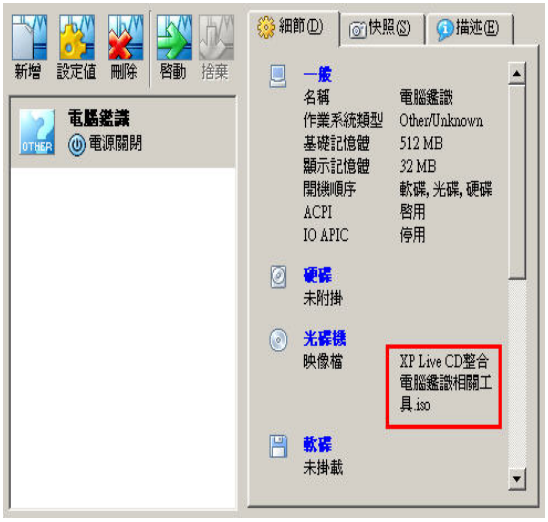

圖 20.VirtualBox 啟動畫面

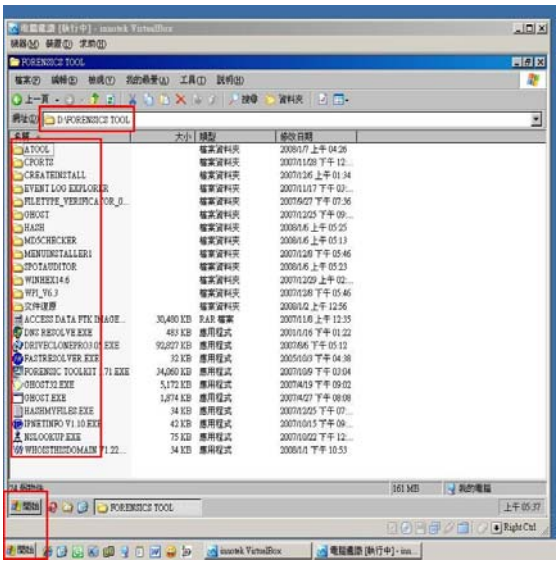

圖 21.XP Live CD 整合電腦鑑識相關工具

在使用光碟開機建立獨立性的作業系統下，讓調查員可以在不更動電腦系統硬體狀態下，進行電腦鑑識工作，間接隔絕電腦主硬碟開機所帶來的電腦病毒侵害，避免破壞鑑識檔案所收集數位證據的完整性。學者王俊城分析[24]：一般使用者，要在電腦上使用作業系統，硬碟必須要劃分主開機區，經過格式化後，在安裝作業系統步驟到硬碟上，作業系統才可以使用，Live CD 主要取出作業系統的開機核心檔案，修改電腦硬體驅動程式設定，使作業系統不需要安裝到硬碟，透過 CD、DVD、USB

隨身碟開機，便成為一個獨立的作業系統，除了有作業系統本身的功能，還可以另外執行其它應用程式，適合用於展示(demo)，緊急救援(rescue)，測試(testing)等應用。

步驟三.

調查員順利開機進入作業系統後，先以 Ghost 工具將鑑識主機相關儲存設備加以複製，製作映像檔保存，包括作業系統、驅動程式、使用者權限設定、資料檔案等，見圖 22、圖 23、圖 24，確保日後資料如果發生毀壞得以還原。

圖 22. 製作映像檔

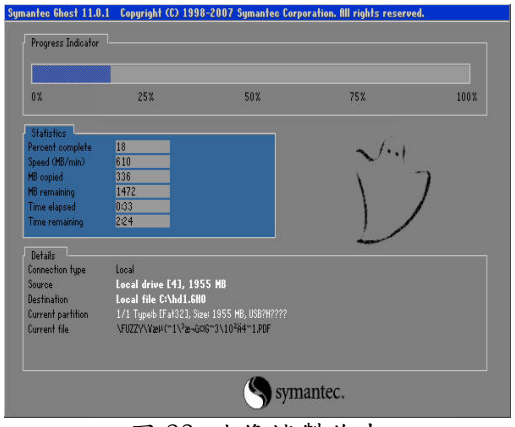

圖 23. 映像檔製作中

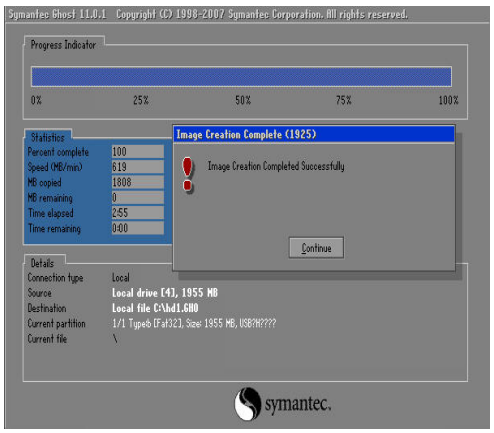

圖 24. 製作映像檔完成

在國外有公眾服務標準和技術學會 NIST[43](National Institute of Standards and Technology) 執行一項計畫，名為 CFTT[44](Computer Forensic Tool Testing Program)，專責測試電腦鑑識工具的安全驗證，能提供調查人員在調查電腦犯罪時，所使用鑑識工具的特性與合法性分析。工欲善其事，必先利其器，更加說明了鑑識工具的重要性，因此，本研究提出電腦犯罪的搜尋、分析、驗證三階段。根據此三階段分析相關鑑識工具，提供調查方向。但以電腦犯罪類型繁多，此次針對犯罪者以網路為電腦犯罪事件，調查員並不能一一使用鑑識相關工具。

搜尋階段：

1.針對檔案的不同資訊來搜尋。
2.連線的 Log 檔對不尋常的區域或行為查看。
3.檢測檔案類型。
4.資源回收筒還原刪除的檔案。
5.還原遭到病毒刪除、電力中斷遺失、磁區重新格式化、壞軌損毀的檔案。
6.找出即時通訊軟體登入的密碼。
7.查看使用者曾經開啟的程式。
8.系統紀錄中曾經出現的密碼。
9.監聽本機及區域網路 Web、FTP、Email 所傳送的密碼。
10.破解 MS Word Excel Outlook Access 密碼。
11.破解 PDF 密碼。
12.隱藏檔資訊。
13.登記的網域的資訊。
14.IP 位址的擁有者、電話、電子郵件等資訊。

在 XP 作業系統內建搜尋功能中發現了案例四中調查員偵察盜版網站，提供盜版資訊給消費者的網頁檔，見圖 25：

圖 25. 提供盜版資訊給消費者的網頁檔

分析階段：

1.系統登錄檔(Registry)中的註冊鍵值。
2.傾印 Dump Process Memory 的資料。
3.磁碟資料夾的大小、數量、建立日期等資訊。
4.執行中進程的資訊。
5.作業系統服務 Service。

6.本機登入、遠端網路登入、使用伺服器用戶。
7.安全標識符(SID) 。
8.目錄、檔案及登錄機碼的存取對象和方式。
9.硬碟存取活動紀錄。
10.追蹤系統或應用程式檔案組態。
11.檔案開啟、讀取、寫入或刪除發生的時間。
12.系統登入時的自動啟動程式。
13.監控程式，顯示讀取和寫入的登錄資料。
14.擷取 TCP/IP 封包。
15.電腦上各個通訊埠連接情況。
16.最近開啟的檔案目錄。
17.Cookies 檔案的資料。
18.IE 緩衝的臨時網頁文件。
19.網頁瀏覽歷史紀錄。
20.瀏覽器搜索記錄。
21.解析、反解析 IP 地址。

驗證階段：

1992 年 8 月 Ronald L. Rivest 在 IETF 提交了一份 RFC1321[45]，描述了 MD5 (Message-Digest algorithm 5)雜湊演算法的原理，MD5 由 MD4、MD3、MD2 演進而來，主要增強演算法複雜度和不可逆性，在 90 年代被廣泛使用在各種程序語言電腦中，用以確保資料傳遞無誤，使用者可將任意長度的資料，以 MD5 雜湊演算法運算，得到一組固定長度為 128 位元(16 個字元)的結果，其優點有以下：
一.雖然不同的資料經由 MD5 雜湊演算法計算所得到的結果有可能相同，但是根據統計顯示，重覆的機率低於百萬分之一。
二.MD5 為一個單向雜湊演算法，亦即不易以逆向運算得到原始資料。

SHA 安全雜湊標準 (Secure Hash Standard)，1993 年由美國安全局(NSA)所設計，並由國家標準與技術研究院（NIST）發佈[46]。1995 年發佈修訂版本 SHA-1，SHA-1 在許多安全協定中廣為使用，包括 TLS、SSL、PGP、SSH、S/MIME、IPsec，SHA-1 可將一個 2^{64} 次方位元的訊息，轉換成一串 160 位元訊息摘要，其設計原理相似於 MIT 教授 Ronald L. Rivest 所設計的密碼學雜湊演算法 MD4 和 MD5。

驗證算是鑑識工具裡面最重要的階段，調查員針對工具、檔案、硬碟映像檔使用 MD5、SHA1 及 CRC32 演算法，以 HashMyFiles 工具製作 Hash 驗證碼保存見圖 26，可以保障工具安全性或證明資料原始完整性，表示資料沒有經過任何的修改或破壞，增加法庭上的證據效力。

Filename	MD5	SHA1	CRC32	File Size
圖10.網路聊天室中充斥著色情的陷阱.JPG	a172f59fd9f3e5bb299f170d9b78b067	d959a35197e47f8f0d8750c149a45a3534b5abea	79c950b2	27,699
圖11.網路聊天室中充斥著色情的陷阱.JPG	b4d2fe39a825c51a1681db7551d896d0	8a3d1d4965947becaba84ca605b2644e41d68fa7	9350727d	33,467
圖12. 應召站女郎網站.JPG	54750f8d116e79119524ba44ffb909ef	b3eb6c40ae9490c7b1b206b29fc4bfe64fd933c5	6c9580fe	107,292
圖13.賭博網站.JPG	35a2cc0352bdef6832b6d221ca1dbb37	027768757c12c42befd93b5a75b6a31099457b74	4ab0fee1	54,184
圖14.盜版網站.JPG	9080eb685c363531c710ac6c92f020fc	95ffab1a4dd8024d0c38a0c756c9790181f60beb	a080fb64	117,564
圖15.盜版價目表.jpg	4b758f0e7b22dc9594d7681d8ad87658	46db5a5a4a7581eb4d215107ae7aaafffdb5a37e	1d5ddeb1	63,758
圖16.反解譯xyz66.com網站.JPG	ffa46aee56d3fff0a788a068bc1bda97	db5f43dcf6636e49a8e7d7a6a39e42315770705 3	b09b61e8	10,241
圖17.反解譯xyz66.com網站.JPG	e1170f4a9419c625db76cfc5f64d3466	dcf7a1dc1123bb3c14605fa09627ac4b5c8676b1	ada078fc	15,244
圖18.DNS查詢程式.JPG	fe005f9023317ec72f3eb842008fe4c3	8b268ecdf354d56a2c00ba8c1038cf8c51f40e5f	b9ca75b4	52,203
圖19.IPNetInfo.JPG	f7c4278d4cc6c989cdbf068e45e15a02	2429c031a0f5d27d32163a1e729a3c85958eeb00	8f3a1245	89,155
圖20. WhoisThisDomain.jpg	b37a663f367f63e3823dac0f935a5cfb	5c1e9b1af9e8f4fee06df7d5fe75b97f18ee7ff2	8065e828	80,668
鑑識主機Ghost映像檔.GHO	398d23d3f5101def20c97fa31c3201e0	d29157ba11ff8abdf312c2a6b01127cf6a55a55b	dedb9a95	1,888,259,100
xyz盜版網站目錄.mht	89db7e4b8807dd2053393576a629c4cf	b3e39a7b586e4fe00e87b4c600251e3846275ac8	fe4baece	19,300
xyz盜版網站訂購單1.htm	4c7063374625afd4a087ef290f7a7a6c	413e32a9ad27a3d016506a7e2e64ef8836bf219b	58803067	39,515
xyz盜版網站訂購單2.htm	ef6335cc7c231bf2ba26df2d274f3e87	5bc442b0ab4ca12645f96dccf9c08e5c2a7c8010	4a92da48	39,513
xyz盜版網站首頁.mht	ca8fc6aa78986891c4cab3e348b761a4	6c3d70c61fc5134febae39db22433b7bf176b93f	889f3bcd	216,750
xyz盜版網站價格表.mht	b9544c87b8b340ca3cd493f72c9529bf	7a9b0ffbfefcc08c6ce215adfb33f9197e173752	1657c215	196,619
工具-DNS Resolve.exe	b30113ac48376b851435617e632156...	543d1f0c33f75856b1e8f50fa521a99161f81a4b	c459bdc4	494,080
工具-FastResolver.exe	8b497d41125e6c758fd99af442dc5786	e30668a848646ad5effd42bc390b2a7725369b0f	f8d11210	32,256
工具-ghost.exe	0f269ef23bbbe9aca916dd7e114dddc2	75f223cc91ee4e066c2df52a25a9d3125fdc891f	115586f9	1,918,788
工具-ghost32.exe	aa220708c439ddba9f65495a9481a4c8	17c8ff644151c1db393f91a9ccfe32305cbd9cbf	5d416dda	5,295,752
工具-HashMyFiles.exe	a5632ec67d163b8623fb7cd898014f03	b8c6ae5697fb935d948b976920b3cc137740d5d1	47197402	34,816
工具-IPNetInfo v1.10.exe	f1ec0d64eb888433394f85a598b30c90	60946fcc70ac7e4919b03ee24d865b3e30946dd2	91db5987	43,008
工具-nslookup.exe	88919d2206da070fb39a53c7694c6337	4428aa3bce7a42474535 2f2c9b6ee834df10b867	a82c324c	76,800
工具-WhoisThisDomain v1.22.exe	3c4396b4a9b8c279a9298fbdb2d3d8a2	b8804d5c5fa0d66429ab52801fcdae4b04ece885	74150c30	34,816

圖 26. 製作 Hash 驗證碼

步驟四.
調查員將鑑識程序的相關檔案，另外儲存到外接式儲存裝置，放到安全的地方保管。

步驟五.
調查員彙整鑑識報告，陳述鑑識過程使用的工具以及事件描述，呈交相關單位，見圖 27。

<table>
<tr><td>調查員</td><td colspan="2">XXX XXX XXX XXX XXX</td><td>日期</td><td>XX 年 XX 月 XX 日</td></tr>
<tr><td>案件</td><td colspan="4">以網站架設方式，成立盜版光碟網站，販賣圖利之電腦犯罪情事。</td></tr>
<tr><td>扣押證物</td><td colspan="4">(證物 1)電腦主機 10 台 (證物 2)1TB 容量硬碟一顆
(證物 3)對拷光碟燒錄器 20 台 (證物 4)印表機 6 台
(證物 5)傳真機 3 台</td></tr>
<tr><td colspan="2">鑑識工具</td><td colspan="3">描述</td></tr>
<tr><td colspan="2">網路瀏覽器 Internet Explorer</td><td colspan="3">圖 13、14:上網偵察搜索發現可疑盜版光碟網站</td></tr>
<tr><td colspan="2">Nslookup
FastResolver</td><td colspan="3">圖 15、16:正解 xyz66.com 網站，查出其網站位置 IP 為 74.86.178.68</td></tr>
<tr><td colspan="2">DNS 查詢程式</td><td colspan="3">圖 17:xyz66.com 相關主機資訊</td></tr>
<tr><td colspan="2">IPNetInfo</td><td colspan="3">圖 18:網站位置 IP 74.86.178.68 登記資訊</td></tr>
<tr><td colspan="2">WhoisThisDomain</td><td colspan="3">圖 19:xyz66.com 登記網域名稱資訊</td></tr>
<tr><td colspan="2">XP 作業系統內建搜尋功能</td><td colspan="3">圖 25：從電腦主機以及硬碟儲存裝置都發現有提供盜版資訊給消費者的網頁檔</td></tr>
<tr><td colspan="2">HashMyFiles</td><td colspan="3">圖 26: Hash 驗證碼</td></tr>
</table>

圖 27. 鑑識報告

4.結論與建議

目前電腦鑑識研究在國內尚處於萌芽階段，在本文實驗環境架構經過，提出電腦鑑識程序之研究，讓司法機關、執法單位、調查人員瞭解電腦鑑識相關的癥結，在鑑識中如何去產生有效的數位證據，希望能在打擊電腦犯罪上有所幫助，奠定電腦鑑識的重要性，企業個人在面對資安問題時，都可以藉助電腦鑑識來解決許多的問題，最後提出建議如下：

一.在電腦鑑識工具上，無論是國內還是國外，所採集的相關數位證據，必須還要依靠法律上的支持，才能讓執法單位得以在法庭上打擊不法，隨著科技的日新月異，當然電腦犯罪手法與種類也會陸續增加，法律明文訂定也必須要隨時掌握最新的資訊，面對電腦犯罪才能得以伸張，打擊不法。

二.國家應培養開發電腦鑑識工具人才，因應未來犯罪者利用高科技電腦犯罪之情事。

三.近年來不法者利用網路當作犯罪場合以及工具遽增，網際網路服務提供者 ISP(Internet Service Provider)應有效配合執法單位在不法者網路位置上的蒐證。

四.政府加強國際合作，共同打擊電腦犯罪，進行電腦鑑識技術交流。

參考文獻

[1]林宜隆，”網路使用的犯罪問題與防範對策之研究”，中央警察大學學報 34 期，1999 年 3 月，頁 353-381。

[2]黃榮堅，電腦犯罪的刑法問題，台大法學論叢，第二五卷第 4 期，八五年七月，197 頁至 228 頁。

[3]周宜寬，以科爾曼理論探討美國電腦犯罪，淡江大學美國研究所碩士論文,1994 年 5 月。

[4]李柏宏、廖有祿，”電腦犯罪之問題與對策”，警學叢刊 26 卷 6 期，1996 年 5 月，頁 141-154。

[5]廖有祿，電腦犯罪者特徵剖析之探討，2000，二○○○年網際空間：資訊、法律與社會研討會論文集（一）。

[6]黃景彰，資訊安全-電子商務之基礎，2001，華泰文化事業公司。

[7]廖有祿，2001，電腦犯罪特性分析之研究，第六屆亞太安全會議論文集。

[8]孫宇安譯，Julia H. Allen 原著，2002，CERT 網路與系統安全實務，培生教育出版社集團。

[9]台灣電腦網路危機處理暨協調中心，目前網路攻擊趨勢之概述，2002-07。

[10]日本資訊處理事業協會 IPA http://www.ipa.go.jp/

[11]經濟部智慧財產局 http://www.tipo.gov.tw

[12]陳永旺，David Icove, Karl Sege, & William VonStorch 原著，電腦犯罪（Computer Crime）一書，1999 年 2 月，第 84-87 頁。

[13]蔡美智，電腦駭客的罪與罰-談網路入侵的法律問題，資訊法務透析，1998 年 7 月，第 20 與 21 頁。

[14]蔡懷卿，電腦犯罪問題-美國刑事立法之參考，收錄於刑事政策與犯罪研究論文集(二)，民國八十八年五月，法務部犯罪研究中心編印，頁 175-203。Michael Hatcher, Jay McDonnell & Stacy Ostfeld, Computer Crimes, 36 Am. Crim. L. Rev.,at 399-402 (summer, 1999).

[15]內政部警政署警政治安全球資訊網-年終記者會參考資料刑事警察局的回顧與展望 http://www.npa.gov.tw/NPAGip/wSite/ct?xItem=34790&ctNode=11436

[16]王旭正、柯宏叡、楊誠育，2002，網站入侵安全的證據存留鑑識探討，Communications of the CCISA ，2002， Vol. 8 No. 4 。

[17]認識刑事警察局 偵查一至九隊 http://www.cib.gov.tw/kids/tcon01_06.aspx

[18]刑事警察局-刑事鑑識科學

[19]I Security-資安鑑識實驗室

[20]CNLA Internet 實驗室檢驗機構服務網 http://www.cnla.org.tw/CNLA/la_index.aspx

[21]林宜隆、邱士娟，2002，我國網路犯罪案例現況分析第四屆，2002 年「網際空間：資訊、法律與社會」 學術研究暨實務研討會。

[22]林一德，2000，電子數位資料於證據法上之研究，國立台灣大學法律研究所。

[23]林茂雄翻譯，李昌鈺原著，1999，刑案場蒐證，中央警察大學。

[24]王俊城 Live CD 2005/07/21

[25]Market share http://marketshare.hitslink.com/report.aspx?qprid=10&qpmr=15&qpdt=1&qpct=3&qptimeframe=M&qpsp=106

[26]Sterling, B.,“Good Cop, Bad Hacker”,Wired, 3, 1995：pp.122,124-129.

[27]Morris, J. H., “Our Global City”,Communications of the ACM, 32(6), 1989：pp.661- 662.

[28]Bawden, B., “International Symposium on

the Prevention and Prosecution of Computer Crime”, Computer Law and Security Report, May-June, 1992：pp.7-11.
[29]Mark J. Biros & Thomas F. Urban II，Crime Online - Knowledge, Prevention and Detection (chapter 10)，Business & Legal Guide to Online Internet Law, Glasser Legal Works, N.J. USA,1997.
[30]Philippsohn，2001，Trends in Cybercrime An Overview of Current Financial Crimes on The Internet，Computer &Security 20.
[31]CSI/FBI ，COMPUTER CRIME AND SECURITY SURVEY，2006
[32]CSI/FBI ，COMPUTER CRIME AND SECURITY SURVEY，2005
[33]CSI/FBI ，COMPUTER CRIME AND SECURITY SURVEY，2004
[34]SoftEther http://www.softether.com/jp/
[35]Pub. L. No.99-508, Title I, §101(a), (c) (1) (A), (4), 100 Stat. 1848, 1851 (1986)
[36]18U.S.C. §2511(1) (e) (1994); 18 U.S.C. §2510-2521, 2701-2710.
[37]18U.S.C. §2511(1) (e) (1994); 18 U.S.C. §2510-2521, 2701-2710.
[38]Kuchta, Kelly J.，2002，Forensic Fieldwork：Experience Is the Best Teacher.，Information Systems Security ，Vol. 3 Issue 1, p29-33.
[39]Tohmas Rude ，2002 ，Evidence Seizure Methodology for computer forensics crazytrain com.
[40]Eoghan Casey, 2002, Handbook of Computer, Crime Investigation, ACADEMIC PRESS。
[41]Defense Cyber Crime Institute (DCCI) http://www.dc3.mil/dc3/home.htm
[42]Sammes、Jenkinson，2000， Forensic Computing- A Practitioner’s Guide.
[43]National Institute of Standards and Technology http://www.nist.gov/
[44]NIST Computer Forensic Tool Testing Program http://www.cftt.nist.gov/
[45]Rivest 1992 MD5 Message-Digest Algorithm RFC 1321 http://www.ietf.org/rfc/rfc1321.txt
[46]D. Eastlake, 3rd Motorola P. Jones US Secure Hash Algorithm 1 (SHA1) September 2001 http://www.ietf.org/rfc/rfc3174.txt
[47]VirtualBox http://www.virtualbox.org/