開放原始碼電腦鑑識系統的設計與實現

許文隆
高雄師範大學資訊教育研究所
allen66@ks.edu.tw

楊中皇
高雄師範大學資訊教育研究所
crypto@computer.org

摘要

資訊科技應用層面的擴大，正向的提昇工作效能，增加生產力，也相對的讓非法入侵與破壞行為如洪水猛獸般的襲向電腦使用者。因此，當破壞入侵等非法行為發生時，如何找出入侵者的犯罪證據，或是將被破壞的資料還原，『電腦鑑識』工作，已成為電腦安全領域裡，不可或缺的重要技術。

本研究主要是將開放原始碼的電腦鑑識程式—Sleuthkit 與 Autopsy 進行功能的加強與中文化整合，並加入時戳服務來證明採證時間。目前台灣尚未有中文版本的電腦鑑識程式，並且大都依賴價格昂貴的外國軟體進行電腦鑑識。故研究希望依照本地之需求，並減少使用者進入本領域的障礙，將電腦鑑識程式製作成中文版本的 LiveCD，讓使用者在不更動電腦系統下，進行電腦鑑識工作，並救援被破壞的系統檔案，甚至找出犯罪證據，供執法單位作為事證，進行司法審判。

關鍵字：電腦鑑識、電腦安全、時戳、Autopsy、LiveCD

一.緒論

隨著科技的進展，電腦已經完全融入人們的生活中，不管食衣住行育樂，樣樣都必須依賴這方便的工具。但相反的，因為使用者眾多，也造成入侵與破壞行為日炙，不管中毒、非法入侵、擷取私人重要資料等非法行為日益增加，甚至破壞作業系統，癱瘓電腦運作等，讓企業或政府單位蒙受嚴重損失。因此，當入侵或破壞行為發生時，找出入侵者，復原被破壞的系統與資料，甚至找出犯罪的證據提交檢調單位，在這不安全的資訊時代，已經成為不可或缺的電腦工程。

目前在大家的觀念裡面，『電腦鑑識』這件事，一般人都認為是警方或是檢調單位的工作。殊不知其實在我們生活週遭，尤其是資訊設備，因為目前其安全性不足，所以隨時都可能有遭受入侵或破壞。這時候，嚴重造成傷害的入侵行為，或是產生無法彌補的損失時，我們會報警請求電腦鑑識，找出原因或兇手。但有時對於入侵未造成破壞的小問題，或是內部控管不周造成的小傷害，就必須由自己的人員進行『電腦鑑識』，來救援系統或是清查到底是哪一環節出了差錯。尤其當發生事件的第一時間，若有相關專業人員瞭解鑑識流程，更能保護證據，以免不當關機或更新系統，而造成證據嚴重流失。因此，我們要瞭解，電腦鑑識並非只是檢警單位獨立應用的領域，一般單位也要對其有基本的概念與因應措施。

另外，對於證據的採樣部分，目前我國司法單位對於電腦鑑識證據的採用，並沒有非常多的判例供為參考，所以法官對於採用電腦鑑識證據都會比較謹慎。因此，一個有公信力的電腦鑑識軟體非常重要，而應用電腦鑑識，有分為 Live-analy

sis 與 Dead-analysis 兩大類，也就是電腦系統能否開機進入系統進行電腦鑑識。目前許多鑑識軟體都必須安裝於作業系統內，然後再進行鑑識，但這過程可能造成證據因安裝程式而流失或拔除硬碟過程造成硬體的損壞。因此，如何在電腦硬體安全無虞狀況下，且不更動系統的情況中，進行電腦鑑識，確保資料與證據的完整與安全性，這也是本研究想要著墨的地方。所以採用 LiveCD 的方式,在完全不更動系統與拔除硬體的過程中，將鑑識軟體執行，進行電腦鑑識。

最後，對於鑑識結果的資料呈現，除了進行鑑識者知道結果外，另外對於想知道結果的相關人員，如檢調單位或法官，因為該員未有本領域相關知識，如何將結果用最簡易的方式呈現，也是本研究的另一個重點。因為證據的呈現，關係到鑑識結果的成功與否。因此，本研究希望開發一套鑑識結果的呈現系統，讓證據的呈現更具說服力，更能讓司法單位對證據採信與納用。

二. 文獻探討

本研究著重的領域在於電腦系統的安全性探討與系統遭受損害的的偵測與回復，茲依據研究所需之相關名詞進行文獻分析：

(一)電腦鑑識

『電腦鑑識』領域可視為鑑識科學的一個新旁支，其不僅需要對資訊科技領域有一定的瞭解，也必須對傳統的刑事鑑識科學有所涉略，才能在本領域有所發揮。最早提出『電腦鑑識』名詞，是在一九九一年的『國際電腦專家協會』(IACIS)所提出的『電腦鑑識科學』(Computer Forensic Science),目的為希望研究出網路犯罪證據的蒐證與方法。自此美國政府與相關研究機構開始進行電腦鑑識處理原則的研究與相關工具的開發，來因應數位犯罪的日益增加，強化數位證據的採集與系統安全[7]。

而對於電腦鑑識，我們可以定義如下：電腦鑑識在處裡有關電腦證據的『保留』(Preservation)、『鑑定』(Identification)、『淬取』(Extraction)與『文件化』(Documention)等過程，目的是為了保留犯罪現場電腦物證的原貌與鑑定結果的完整性，來提供檢調單位與法院審理案件時的參考依據[1]。

依據中央警察大學林宜隆、王旭正博士等的研究，認為『在電腦鑑識作業上，有些人會試圖自行撰寫程式來進行電腦鑑識，然而這並不是很好的方式，原因在於自行撰寫的程式難有公信力，不僅容易被質疑，連帶地也會影響證據的證明力。因此許多時候都要使用到較具穩定性的電腦鑑識相關工具軟體來進行鑑識工作』[2][4]。所以本研究採用在外國使用多年的開放原始碼鑑識軟體作為研究的基礎，在相同的架構下，進行本地端化與功能的加強，讓本軟體更適合國人進行電腦鑑識。

(二)The Coroners Toolkit

The Coroners Toolkit[11]也就是我們所說的 TCT,是一個 unix 下的指令式文件系統工具集，支持 FFS 及 ext2fs，可從 live system 來對數據進行分析與恢復。它能夠針對文件的最後修改、訪問或者改變(MAC)的時間來進行分析,並且根據數據節點的值提取出文件列表以進行恢復。

在西元 2000 年,Farmer 與 Venema 釋出了第一版的 TCT,其指令工具名為『grave-robber』與『pcat』,其功能為可以從運作中的系統(live system)複製重要的

資料。而分析指令工具為『ils』與『icat』，允許使用者來分析 UNIX 系統 inode 架構的檔案系統。『mactime』工具建立檔案使用的時間軸。『unrm』工具可以從檔案系統裡面解析出為使用的資料區塊。『lazarus』工具分析資料的(chunks)與復原其被刪除內容與格式[10]。

所以當時就有七個 unix 的指令工具包含在 TCT 套件裡面。但 TCT 有一個缺點，就是無法讀取除了附掛系統的檔案格式，也就是假如你將 TCT 安裝於 Linux 系統上，就無法讀取其他系統程式，如 Solaris，這將嚴重阻礙電腦鑑識的進度與發展。所以 Brian Carrier 才會改良 TCT 而建立 Sleuthkit，sleuthkit 全名為『The @stake Sleuth Kit (TASK)』，簡稱『TASK』[12]。

對一般鑑識工具來說，檔案系統是被動的透過作業系統讀取其他檔案格式，但較先進的鑑識工具，會由工具本身自行運作來讀取其他作業系統的檔案格式，並不需要依靠作業系統。因此，即使 Solaris 作業系統核心不支援 NTFS 格式，較進步的鑑識工具依然可以讀取該格式進行鑑識。

(三)SleuthKit

Sleuth Kit[12]是開放原始碼軟體，可以偵測 Unix 或是微軟作業系統的檔案與磁區，並允許使用者在執行中的系統復原並且製成映像檔來進行鑑識。本軟體的來源是從 The Coroner's Toolkit (TCT) 改寫而來，可以讀取除了 Unix 系統檔案外，對於NTFS與FAT皆可以順利進行鑑識。

為了提供支援相關的檔案格式，TASK 使用階層式模式來設計，總共分成四個階層：

- 資料單元(Data Unit)層存放檔案與資料夾內容的地方。一般來說，當作業系統需要時，磁碟空間是從這兒分配出去。資料單元的檔案大小在一般系統大概都是 2 bytes、1024 或 4096 bytes。資料單元在不同檔愛系統模式其名稱也不同，有些稱為 fragments 或是 clusters，但是內容都是一樣的。
- 資料元(meta data)層是檔案與資料夾的描述性資料存放的地方。本階層包含 Unix 系統下的 inode 架構，NTFS 下的 MFT 架構，與整個 FAT 的目錄架構。本階層包含最後存取時間、檔案屬性或是資料單元的檔案與資料夾配置。本層完整的描述一個檔案相關資料，但它給予的資料都是以數字位址方式顯示，一般人很難了解與記住。
- 檔案名稱層是檔案與資料夾名稱實際儲存的地方，一般來說，這與 meta data 架構不同，但 FAT 檔案系統除外。傳統的檔案名稱是儲存於上一層目錄分配下的資料單元，檔案名稱架構包含與 meta data 架構符合的名稱與位址。
- 檔案系統層是其他特定的檔案系統儲存的地方，舉例來說：每個資料單位的大小與有多少 inode 的架構。這個階層包含有在同樣格式下與其他檔案系統不同的鑑定值，當然管理架構的不同此處也有相關資訊。

整個系統程式架構是以指令模式在 UNIX 系統下執行，如此對於一般使用者會有嚴重的使用阻礙。因此，Carrier 又開發了一套瀏覽器架構的圖形化介面偵測程式名為『Autopsy』，透過瀏覽器，連結到 Sleuth Kit，即可進行電腦鑑識工作。

(四)Autopsy

Autopsy[13]剛開始並非為了 sleuth

kit 而開發，在 sleuthkit 還未出現前，Autopsy 已經出現並與 TCT 做結合，是 TCT 的圖形化介面程式。其程式介面使用的是網頁介面，主要用途是作為 Computer Forensics,可為遭到入侵破壞的電腦系統進行「驗屍」(Autopsy 英文涵義即為驗屍)。

無論具備特定目的或僅是挑戰自己能力，網路上每日都有大量的網路漏洞測試與攻擊行動。但所有的入侵行為都有跡可尋，無論是全自動化攻擊蠕蟲、或單一的滲透攻擊。入侵者的手法與使用的工具都可作為證據，甚至可用於區分出執行攻擊的組織或個人。有些組織在網路上佈署了數台 honeypot 系統，就是用來收集各式攻擊手法、工具以及蠕蟲。

Autopsy 中的每個案件可依照受害主機建立檔案分析，每個案件可包含數件主機資料(host)，主機資料中再區分為磁碟映像。每個案件可設定由好幾位的調查員進行調查，以建立歸檔機制。autopsy 目前支援的檔案系統如下表所示：

表一：Autopsy 支援之檔案系統列表

fat16	fat32
bsdi	Fat
freebsd	linux-ext2
linux-ext3	Ntfs
openbsd	solaris

除了基本的檔案與磁碟映像資料外，autospy 也提供「時間軸」(TimeLine)功能，可依照時間列出特定時間內遭到存取或建立的檔案列表，輕易的分析出檔案的建立順序。

此外便是『Hash Database』功能，所謂的 hash 是對檔案進行 SHA-1 或 MD5 驗算。因為不同的入侵者使用的工具不同，即使使用的原始碼相同，但是依照編譯器、慣用的編譯最佳化的不同，產生出來的二元程式必定不同。因此藉由『Hash Database』，可以逐漸歸納出攻擊來源。

(五)時戳服務

時戳(TSA)[14]可以為任何電子文件或網上交易提供準確的時間證明，並可以檢驗文件或交易的內容自蓋上時戳後是否曾被人修改過。電子時戳就如一個值得信賴的第三者或公證人，提供可靠的時間確認和核實服務。所有電子數據或資料，不論是什麼樣的格式或內容，都可以蓋上電子時戳。這個可靠的時間核證服務可應用於網上商務交易、電郵、加密訊息、保障知識產權和其他需要準確時間證明的事務。

時戳服務最主要的目的，是以公正第三者的角色提供『某一份資料在某一時間點就已經存在』的證明，是建立不可否認性的重要機制。由時戳服務中心(Time Stamp Authority; TSA)提供數位時戳(Digital Time Stamp)服務,扮演電子世界簽發『時戳』的角色。本研究在鑑識過程中的相關證據檔案，皆加入時戳函數，來提供證據具有不可否認性的地位。

(六)Live CD

大多數的使用者都習於使用微軟的作業系統，不過近年來 X-windows 介面的設計已非常的完善，也漸漸帶動 Linux 的平台的興盛。伴隨著使用者不斷的增加，問題也隨之而來，雖然 Linux 為開放原始碼及免費使用，但其安裝設定卻不如微軟的方便。因此在自由的前提下，開始有人將 Linux 平台改寫成速成光碟版，讓使用者只需要將一片光碟置入，免安裝、而且無須硬碟就可以馬上直接在光碟上執行完整的 Linux 作業系統。這樣的 Live CD 既可

以用來當桌上工作站用，也可以用來當網路伺服主機，十分方便。目前已有許多的 Live CD 釋出，較有名的如 KNOPPIX 、Mandrake Move、Fedora Live CD…等等，而微軟也推出 Windows PE ，更有進階版支援微軟系統掃毒的 avast! BART CD 出現。

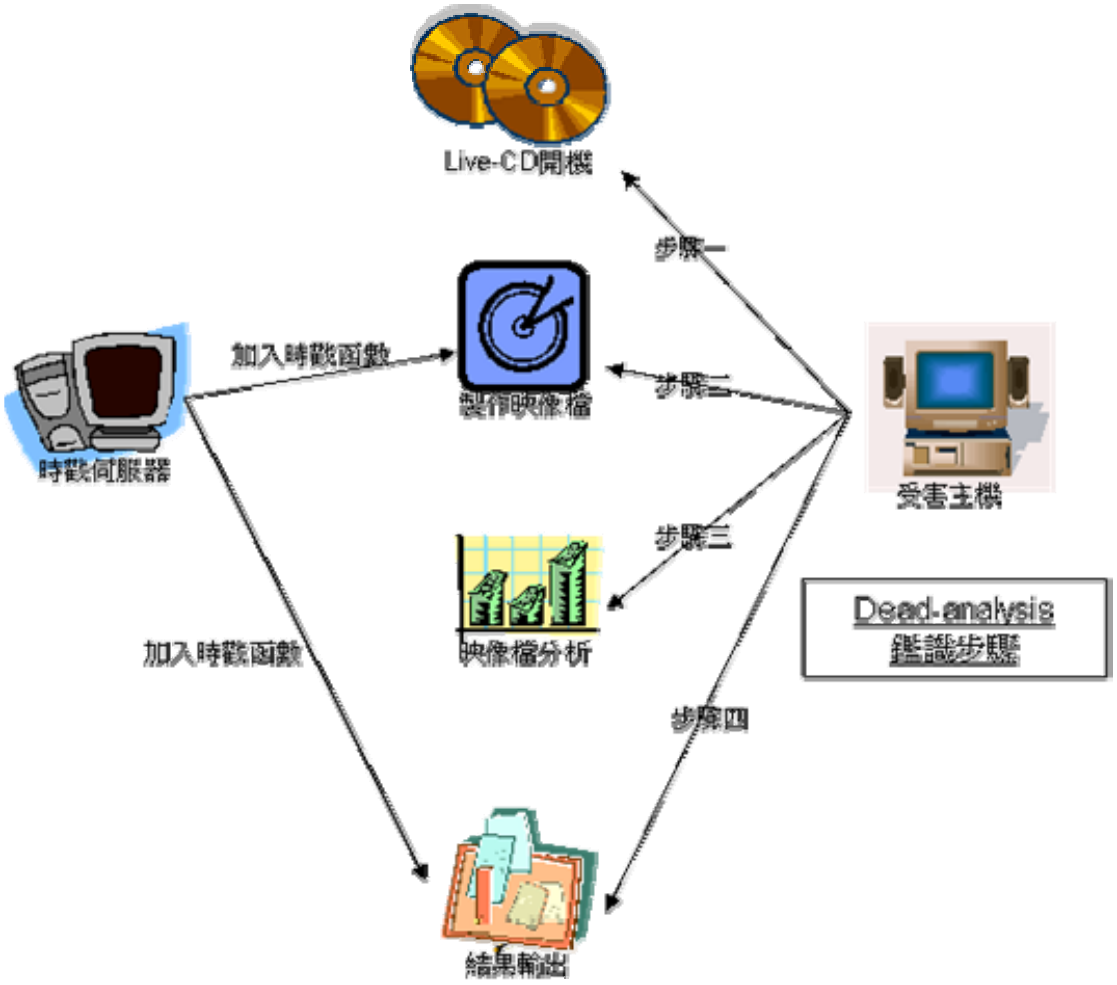
本研究將以『KNOPPIX』Linux 進行 LiveCD 的製作[6]，在電腦鑑識領域裡面，欲做鑑識的系統，其更動越少，將可以獲得更多的證據。因此，將鑑識軟體安裝於 LiveCD 中，由光碟片開機不更動電腦硬碟，將可以完整的鑑識硬碟中的所有資料，找到犯罪證據或復原相關資料。

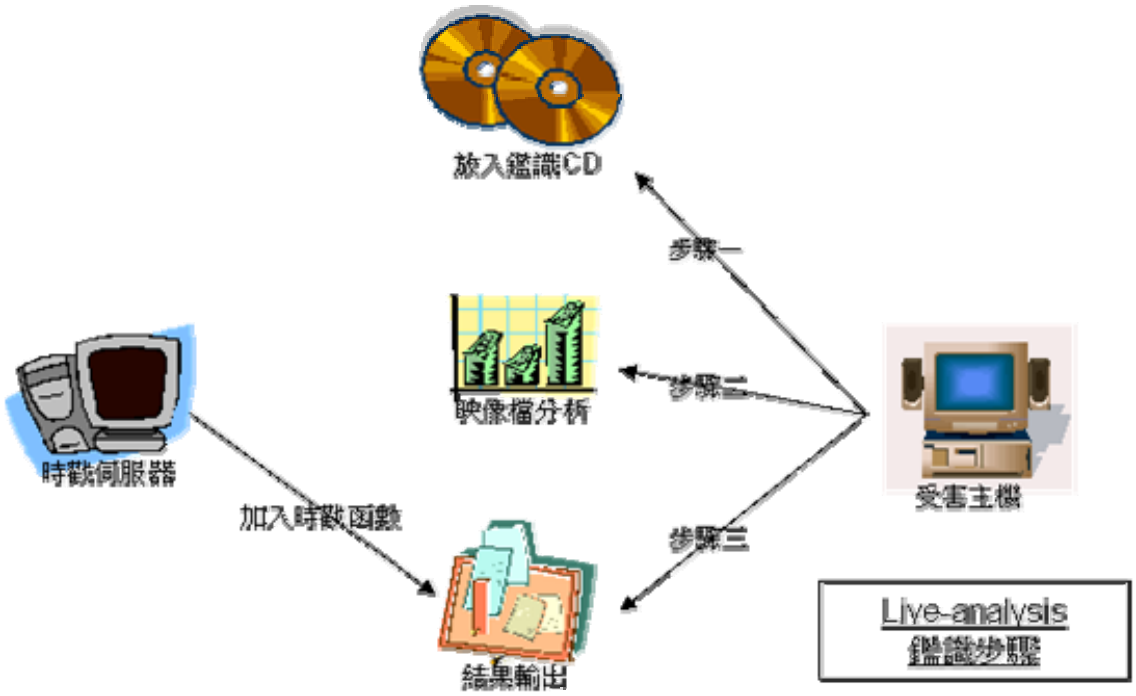
三. 電腦鑑識系統實作

(一)系統架構

本研究以製作兩種鑑識光碟為主要研究方向，一為 Live-CD，來進行 Dead-analysis,也就是電腦系統遭受破壞而導致無法開機，或是已經關機的電腦，當要進行電腦鑑識時，其動作就稱為『Dead-analysis』。另一片光碟為可直接執行的應用程式，無須安裝於作業系統下來進行 Live-analysis，也就是電腦尚在運作中，但已經發現系統有所異常，在不破壞其運作狀況下，進行的鑑識動作，但受鑑識系統需有支援 Perl 程式的服務,若沒有該程式則必須安裝 Perl 相關程式。而 Dead-analysis 採證過程中的製作磁碟映像檔，除了以雜湊函數計算其編碼值輸出外，並加入時戳值進行編碼，以確保採證時間不遭受質疑，具有『不可否認性』,其系統架構如圖一、圖二：

圖一：受害電腦進行 Dead-analysis 步驟架構圖





圖二：執行中的受害電腦進行 Live-analysis 步驟架構圖

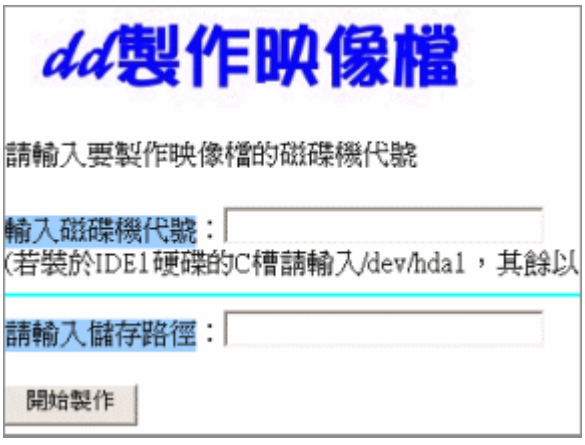
(二)Dead-analysis 系統開發

當電腦系統遭受破壞而無法開機時，使用 Live-CD 來進行救援與偵測是最好的方式之一。本研究使用 Knoppix 系統製作 Live-CD，將開發與中文化的相關鑑識軟體安裝於 CD 中，其內容包含製作映像檔程式 dd、電腦鑑識程式 TASK、圖形化介面 Autopsy 等，並整合時戳伺服器，以瀏覽器方式進行相關程式運作，最後使用 C++Bulider 開發鑑識結果呈現軟體，茲以下列各子項進行說明。

(1)製作映像檔，加入時戳證明

當系統要進行電腦鑑識時，將欲鑑識的磁碟製作成映像檔，並使用雜湊函數驗算其編碼值，讓證據得到完整的保留，是鑑識步驟裡面最重要的一環。因為若磁碟在鑑識的過程中遭到修改或損壞，會導致無以回復的機會，也會因此錯失相關證據的取得或讓犯罪者逍遙法外。因此如何保存受害電腦原始狀況，並進行相關電腦鑑識與系統還原，將受害主機磁碟製作成映像檔並將映像檔移出主機進行鑑識，是保護原始證據免受損壞的重要步驟。

在開放原始碼作業系統裡，最廣泛使用的映像檔製作軟體當屬『dd』指令，幾乎所有開放原始碼作業系統皆會將該指令加入系統運作中。但 dd 指令需要在文字模式下運行，對於剛入門或指令語法不熟悉之使用者，會產生阻礙。故本研究使用 perl 開發圖形化介面的 dd 映像檔製作介面，使用者只需輸入欲至作映像檔的磁碟路徑，與存放的路徑，按下『開始製作』按鈕，即可建立一個映像檔檔案(如圖三)。

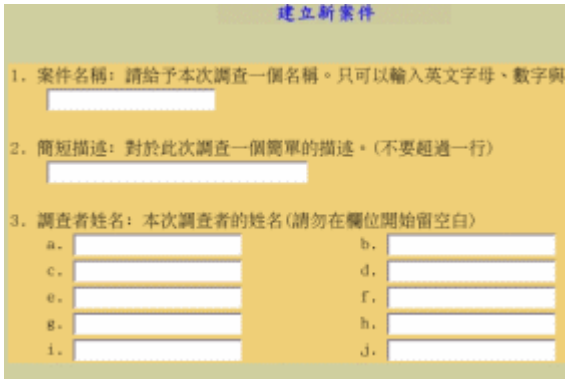


圖三：圖形化介面的 dd 製作映像檔工具

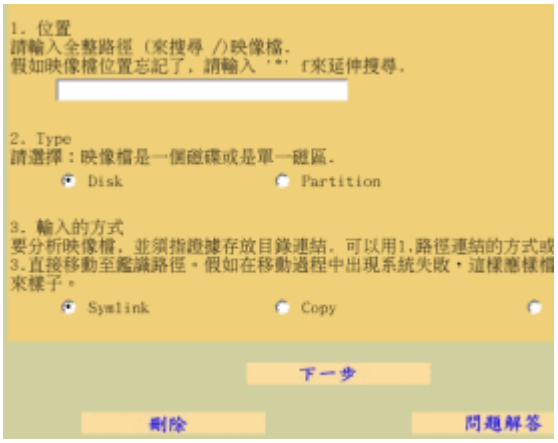
製作完映像檔之後，必須證明其映像檔在移出受害主機之後不會遭受修改，甚至主機可能因某些因素必須歸還使用者使用，其證據將無法再次獲得。為確保該映像檔有其公信力，我們將此映像檔加入時戳編碼服務，也就是將映像檔加上時戳之 tsr 之後重新編碼，並使用 MD5 雜湊函數計算出該映像檔的編碼值，並在移出主機時附帶其加入時戳數值的映像檔 MD5 編碼值，來確保該映像檔的唯一性與公正性[8]。如此，進入司法程序之後，要將電子證據納入審判結果，才有其不可否認性的立場。

(2)進行映像檔磁碟分析

要進行分析映像檔，首先必須設定一個新案件來做分類，接著將映像檔載入分析程式中(如圖四)。而一個案件裡面可以分為多個主機(host)，目的為若一個案件有多部電腦或多個磁碟需要分析，則可在細分成不同主機來進行鑑識。而載入映像檔可以選擇以連結、複製或是移動整個映像檔來進行分析(如圖五)，因為我們是使用開機光碟進行電腦鑑識，所以一般建議使用連結的方式來進行載入映像檔，避免因複製或移動而造成映像檔損壞或複製不完整之遺憾。



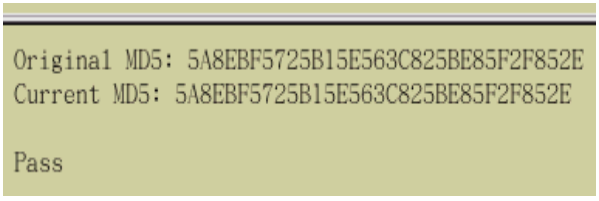
圖四：建立新案件畫面



圖五：新增映像檔畫面

當載入映像檔之後，首先我們必須先確定該映像是否完整，是否與先前製作好的映像檔之時戳與 MD5 編碼值一樣。此動作必須在分析之前做確認，因為若該映像檔遭更動或不完整，則鑑識結果將有誤差。因此載入映像檔之後，必須使用『映像檔確認』功能，來計算與驗證是否映像檔為當初所壓製的映像檔，程式計算過後會列出其編碼值，可以用來比對是否有問題(如圖六、圖七)。

圖六：系統映像檔編碼值



圖七：計算映像檔來源與載入的 MD5 編碼

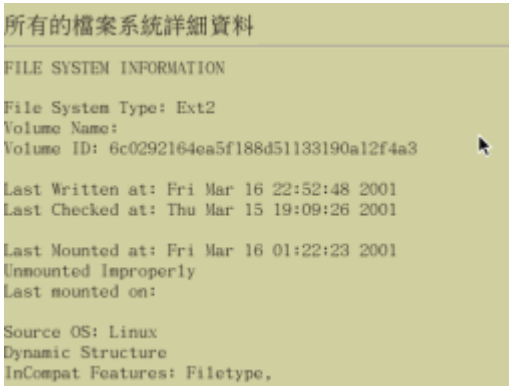
接著為重頭戲『系統分析』，載入之映像檔會包含所有該系統原先留存的所有狀況，可以依照需求進行相關的分析鑑識動

作。一般我們常用的功能有下列幾點：

■檔案回復：受害的電腦常常會有檔案遭受破壞的問題，因此將遭受刪除的檔案救援回復，是鑑識過程中最常做的事(如圖八)。

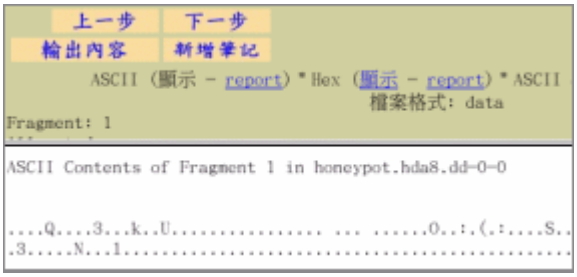
圖八：可還原的刪除檔案列表

■檔案格式分析：此功能為分析該映像檔系統所有的檔案格式資料，包含使用多少配置磁區、未配置磁區數，有多少子目錄與有多少格式的檔案，結果都會一一列表(如圖九)。



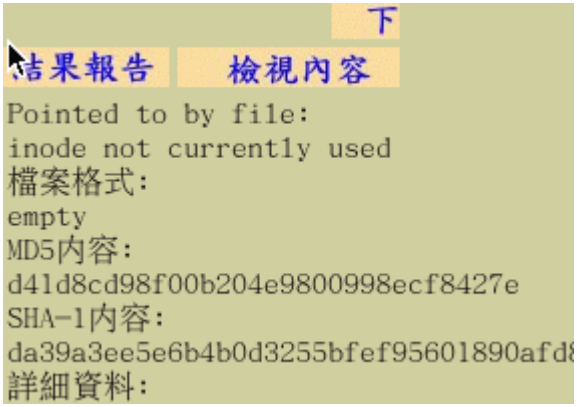
圖九：分析映像檔裡面所有檔案的相關資料

■單一磁區分析：本功能可以依照磁區的最小的單位一一進行分析，以一個『fragment』為單位，分析其內容。在分析過程中並可將該檔案備份至其它地方，也可以列出該單位磁區的 ASCII 值，進行比對工作(如圖十)。



圖十：單一磁區分析圖示，下為 ASCII 值

■MetaData 分析:metadata 分析是依照『單獨的儲存區』(如 Linux 系統格式就是 inode)來進行分析，其分析內容包含整個儲存區的檔案格式、雜湊函數編碼值與該區的 MACtime,也就是檔案與時間相關的各種資料，而上述的相關資料也是電腦鑑識過程中要提取的重要部份(如圖十一)。



圖十一：metadata 提取 inode 的相關資訊

(3)結果輸出

當整個鑑識過程完成，接著就是結果的呈現。對於呈現結果，系統鑑識程式預設會有一個資料夾，裡面包含所有相關鑑識結果的輸出(如圖十二)。但其檔案卻是隨時可以修改的狀態，因此若有心人將鑑識結果做更動，則辛苦鑑識過程將徒勞無功。因此本研究設計一套結果鑑識輸出系統，將鑑識的相關文字與網頁檔案進行雜湊函數驗證與時戳編碼服務，將結果進行

打包，以防鑑識結果遭受竄改。另外本研究使用 C++ Builder 開發一套視窗版的電腦鑑識結果輸出系統，讓輸出結果以更簡潔的方式呈現，並且要輸出結果時，需先行比對時戳與雜湊函數編碼值，確認其與先前編碼值符合，才可以進行證據列印或輸出的動作。

圖十二：結果資料夾詳細內容

(三)Live-analysis

若電腦腦是在運行中，為避免因關機而造成記憶體資料流失，我們必須進行 Live-analysis。其實 Live-analysis 步驟與 Dead-analysis 非常類似，差別只在於是否製作映像檔，另一不同為鑑識結果可直接用遠端聯結的方式進行結果的存放。但 Live-analysis 有較多不可靠的因素在裡面，因為需要鑑識的系統，往往已經遭受入侵或篡改，在入侵或篡改的過程中，有可能其控制權已經在非法入侵者的手中，如此進行電腦鑑識，其結果將會與事實有所差距，因此非不得已，一般不建議進行 Live-analysis，茲以下列步驟進行解說：

(1)檢查系統是否安裝 Perl 程式

本程式所製作的 Live-analysis 分析光碟，程式需依靠 Perl 程式來執行，故系統必須安裝有 Perl 相關程式，若無 Perl 程式則必須進行安裝，安裝之後即可執行本光碟，來進行鑑識。一般 Unix-like 系統幾乎都已經安裝有 Perl 應用程式，而 Windows 系統則都未安裝，需要進行加裝 Perl 應用程式。

(2)執行程式並設定儲存路徑

執行程式步驟與 Dead-analysis 一樣，差別在於指令後面的參數。一般狀況執行 Autopsy 直接輸入『./autopsy』即可，但因為 Live-analysis 其電腦尚在運作，若將鑑識結果直接存在該硬碟，可能會遭受篡改，因此當執行程式時，若網路是連線狀態，可以在執行程式後面加入參數『-d 遠端電腦路徑 連線電腦的 IP』，如此可以將鑑識結果直接存於遠端電腦，以防鑑識結果遭到修改。

(3)進行電腦鑑識分析與結果呈現

在電腦鑑識分析過程，皆與上述 Dead-analysis 相同，故在此不在重複贅述。而鑑識結果存放於遠端電腦，結束鑑識前必須進行時戳與 MD5 編碼，幫檔案進行認證動作，接著也可以使用本研究所開發之鑑識結果呈現系統來進行結果的呈現與列印，進行結果的分析或司法的的審查。

四. 結論

隨著電腦犯罪與日俱增，如何防範未然，減少電腦網路犯罪，是一件刻不容緩的工作。尤以網路普及之後，各行各業為增加工作效率，幾乎都以電子化與網路化為其工作依歸，但也因此造成各式各樣的入侵與破壞行為。當電腦犯罪發生後，其事後的救援或是找出犯罪者來繩之以法，都是發生電子犯罪後很重要工作。目前電腦鑑識研究在本國尚處於萌芽階段，如何開發一套更具權威性，更人性化與適合本

土使用的鑑識軟體，是本研究主要的目的。尤以使用開放原始碼軟體，不但不用擔心其核心有問題或遭人竄改，也沒有版權的問題，更可讓後人依據前人的足跡，開發出更進步的電腦鑑識系統，強化本領域系統的效能與動能。

致謝

本研究部分成果承蒙國科會計畫經費補助（NSC 93-2213-E-017-001），特此致謝。

五、參考文獻

[1] 鄭進興、林敬皇、沈志昌、林宜隆，”電腦鑑識方法與程序之研究”，2003年台灣網際網路研討會，ID.9961。

[2] 林宜隆、楊鴻正、辜國隆、林勤經，”我國資通安全鑑識技術能量初探”，TANET 2002研討會，pp.759-764。

[3] 吳豐乾，”基值於Windows系統的電腦鑑識工具之研究”，樹德科技大學資訊管理研究所碩士論文，2004。

[4] 王旭正、柯宏叡、楊誠育，”網站入侵安全的證據留存鑑識探討”，Communations of the CCSI，2002 年 9 月，Vol.8 No.4。

[5] 林一德，”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碩士論文，2003。

[6] KNOPPIX 中文交流網,http:// knoppix.tnc.edu.tw ,取得時間 2005/8/13。

[7] B.Carrier, “*File System Forensic Analysis*” ,Addison Wesley, 2005

[8] R. Rivest, “The MD5 Message-Digest lgorithm”, IETF RFC 1321, April,http://www.ietf.org/rfc/rfc1321,1992.

[9] B.Carrier,”Open Source Digital Forensic Tools:The Legal Argument” ,http://www.digital-evidence.org, Fall. 2003

[10] R.Clifford ,”Cybercrime:The Investigation ,Prosecution ,and Defense of a Computer-Related Crime” ,Durham,2001

[11] The Coroner's Toolkit (TCT), http://www.porcupine.org/forensics/tct.html,取得時間 2005/7/26

[12] The Sleuth Kit (TSK), http://www.sleuthkit.org/sleuthkit/index.php ,取得時間 2005/8/6

[13] The Autopsy Forensic Browser, http://www.sleuthkit.org/autopsy/desc.php ,取得時間 2005/8/10

[14] OpenTSA , http://www.opentsa.org/ ,取得時間 2005/8/15