電腦鑑識平台系統之設計與實現
Design and Implementation of a Computer Forensics System

嚴珮華
國立高雄師範大學 研究生
E-mail:amber8520@gmail.com
楊中皇
國立高雄師範大學 教授
E-mail: chyang@computer.org

摘 要

資訊化的時代，無論是傳統的刑事案件或是駭客藉由病毒、木馬入侵主機系統，電腦已成為犯罪的工具、場所或是攻擊的目標，幾乎每分每秒電腦系統都遭受惡意的攻擊，因此鑑識調查人員如何處理高科技的犯罪案件，已成為重要的課題。

本研究以 Linux 為開發平台，使用開放原始碼的工具進行系統之開發與設計，將開放原始碼之數位鑑識工具整合至 Live DVD，進行 Dead-analysis 鑑識分析，可以交叉使用各種工具，以補足單一工具鑑識功能的不足，並針對關閉電源或拔除插頭可能造成的資料流失，以自行撰寫之 Live-analysis 程式，收集開機時的系統資訊，以補強數位證據採集的完整性

本研究所有的數位證據皆以 SHA-256 計算並驗證其雜湊值，以確保數位證據的同一性。

關鍵詞：數位鑑識、數位證據、Live DVD。

一、前言

全世界 Web AP 安全公認組織 OWASP 預計在 2010 年第一季度發佈新版 OWASP Top 10，目前僅釋出 RC 版，但其公告屢次被美國聯邦貿易委員會、美國國防部等機構列為 Web 應用程式安全規範的指標，因此其權威性無庸置疑。

而新版 OWASP Top 10 2010 評比標準又比 OWASP Top 10 2007 嚴謹許多，其移除 A3-惡意檔案執行及 A6-不當資訊揭露與錯誤訊息處理，新增 A6-不當安全配置與 A8-驗證的轉址與轉送，此外，資料隱碼攻擊 (Injection) 把「跨網站攻擊程式」(XSS, Cross Site Scripting) 擠下，從第 2 名躍升至首位[9]，但不變的是駭客持續不斷對程式、系統的漏洞發動攻擊，可見電腦/網路犯罪案件的日益嚴重，而如何於犯罪事實發生後，快速蒐集受害電腦上留存證據，及鑑定入侵軌跡則有賴數位鑑識技術。

二、文獻探討

本研究著重在於電腦系統的安全性探討與系統遭受入侵、資料毀損等損害之系統的鑑識為研究標的，以分析相關數位證據之關連性，茲依據研究所需之相關名詞進行文獻分析。

（一）電腦鑑識程序與原則

由於數位證據容易被增修改、不易取得、不易保留等特性，因此想要在資訊安全事件發生後，取得犯罪的證據，則必須有一套完善的收集、分析、保存數位證據的程序及方法，而過去已有許多電腦鑑識程序之探討，本文採用美國司法機構於 2001 年的犯罪現場調查指南中提出了四個階段的鑑識流程[11]（NIJ 四階段數位鑑識程序如圖 1），程序依序簡單敘述如下：

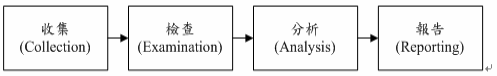

圖 1 NIJ 數位鑑識程序

1.採集(Collection)：此階段包含數位證據的搜尋、辨識、收集及文件化。
2.檢查(Examination)：檢查階段則是將證據可視化並說明證據的來源與重要性。
3.分析(Analysis)：與檢查階段不同，此階段著重於確定證據是有意義的及有價值的。
4.報告(Reporting)：產生調查的報告，其必須敘述檢驗的過程和相關的資料復原的記錄。

而電腦/網路犯罪的現場，已不再只是傳統的犯罪跡證，鑑識人員需依賴鑑識工具取得數位證據。

數位鑑識所得之數位證據是無實體非物質的，並具有以下三個特性[3]：(1)可以輕易的複製與修改、(2)不易證實其來源及完整性、(3)無法以人之知覺直接感知、理解其內容。在數位鑑識的過程，為了使數位證據具有法律效力，須參考 ACPO 國際電腦證據組織(International Organization of Computer Evidence)於 1999 年提出「The Good Practice Guide for Computer-Based Evidence」的電腦證據指導原則，才能使數位證據具有法律效力[1]。

(二) 電腦鑑識的盲點

目前鑑識模式多在事件發生後，將電腦主機關

＊ 本研究接受國科會編號：NSC 98-2221-E-017-010-MY3 研究計畫經費補助

機後，再以鑑識軟體啟動受害電腦，但此方法會造成揮發性資訊的流失(Volatile Information)[2]，而導致無法追查攻擊者的來源、所使用的工具及入侵方式。而蒐集揮發性資訊包含[10]：目前系統時間、作業系統類型與版本、系統安裝日期、使用者登錄系統的歷史資料、目前網路連線狀態、開啟的 UDP 及 TCP 等等。於 UNIX/Linux 作業系統下，我們可透過表 1 這些揮發性資訊收集工具，進行犯罪現場的 Live-analysis：

表 1 揮發性資訊收集工具

資料類別	Unix/Linux 指令工具
系統時間	Date, w
目前登入的使用者	w, who
目前開啟的網路連線與埠號	netstat
目前正在執行的程序	ps
目前開啟的檔案	losf
執行過的指令	history
建立映像檔	dd

(三) 電腦鑑識Live CD

目前美國 FBI 鑑識實驗室採用由 Guidance software 所推出的 Encase[5]、AccessData 的 Forensic Tool Kit (FTK) [6]、e-fense 公司以 Knoppix 套件所開發整合的 Helix[7]。

其中，Helix 是使用 Live CD 的格式，Live CD 具可攜性之特色，因此發展出針對不同目的之 Live CD，例如：Security Live CD 此類的 Live CD 包含：弱點掃描、網路探測、滲透測試、誘捕攻擊等網路安全工具，以協助資訊安全人員進行各項測試與資訊收集，於 2006 年 Darknet 資訊安全社群公布「十大 Linux 資安 Live CD」[4]，其第一名為 BackTrack，其包含超過 300 種的網路安全工具，另外排名第七的 Helix 及第八 F.I.R.E 則是著重於電腦鑑識之 Live CD。而本論文利用 Live CD 的技術整合開放原始碼之鑑識工具。

(四) Live DVD

Live CD 的技術是即將整個作業系統壓縮在一張可開機的 CD/DVD 或是 USB 中，電腦可不需安裝，即可自動啟動作業系統，完全不會影響到原有安裝的作業系統[8]，適合用於教學、展示和作業系統的初學者學習與使用，目前已有許多 Live CD 釋出，較有名的如 KNOPPIX 或是某些 Linux 發行廠商提供屬於自己的製作工具（例如：FedoraLiveCD）、Tux2live 等等，本系統以 Tux2live 製作 Live DVD。

而數位鑑識採證以不破壞受害系統原始態為基本原則，因此本系統利用 Live DVD 不須安裝於硬碟及使用便利的特性，進行整個數位鑑識流程。

三、系統架構

本研究以 Python 為主要開發語言，將受害主機區分為兩類，一為尚在運作的電腦，另一種則為已關機或無法正常開機的電腦。本系統自行撰寫 Shell Script 程式，並裝載至 USB 內，若系統尚在運行，則執行該 Shell Script 程式進行 Live-analysis，收集目前系統的記錄並自動將所收集的檔案存入 USB 中，再於鑑識主機將資料存入資料庫。

若電腦已是關機狀態，我們使用 Live DVD 開機進行 Dead-analysis 製作映像檔及資料還原，本系統將常見的映像檔製作軟體與數位鑑識工具整合至我們所製作的 Live DVD 中，以便鑑識人員依其需求使用，圖 2 為電腦鑑識系統架構。

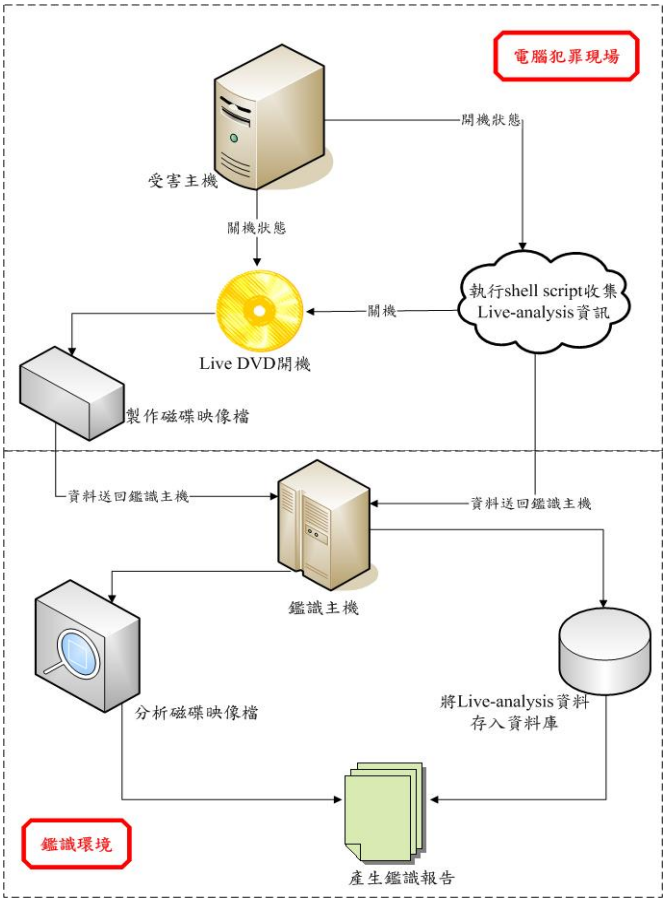

圖 2 系統架構

四、系統實作

(一) Live-analysis 系統開發

所謂 Live-analysis 是指在電腦犯罪現場進行的鑑識工作，其目標可能是電腦主機或網路系統等，而鑑識人員必須於第一時間收集「揮發性資訊(Volatile Information)」，以避免電腦系統關機或移除電源後，揮發性資訊也隨之消失殆盡，而造成日後重建案件原貌的困難。

本研究將系統揮發性資訊工具整合至 Shell

Script (log.sh)中並儲存於 USB 裝置上，當鑑識人員到達電腦犯罪現場時，若該主機是開機狀態，則執行 USB 裝置中的 Shell Script，以收集揮發性資訊，並將所收集的「結果」存回 USB 裝置，以避免破壞受害系統的狀態。

為了驗證所收集的數位證據來自原始證據，而驗證數位證據之同一性就交由雜湊函數(hash function)來處理，證明證據沒有任何改變，由於 2004 年，山東大學王小雲教授在國際密碼學會議中提出破解 MD5 相關研究[12]，因考慮安全性問題，所以本研究數位證據之雜湊值計算全採用 SHA-256，圖 3 為揮發性證據之 SHA-256 值。

```
**********SHA-256**********
f169b3cc93f8a5bd46743817e012082dcaf6d53a5d78923ce3695a2850739d78    basel.txt
852064ce0562d29c4ef1d711fa8e78e5d70b3befad90f7e0870a62eb83c2e40a    base.txt
1cc5f92000decd47c2b6d65a70714a366363282dbadc27be73651e38ad36a0cd    cronl.txt
3c82307386a997d5af172a9ebd92ada66493662b967da3f9cfcdbcf3d270d52f    cron.txt
b6af82b9516e763934baac799e34832dc5fdbed566f8a638284eb227ce2c273d    Failerlog
```

圖 3 揮發性證據之 SHA-256 值(部份)

另外，為使鑑識人員可方便瀏覽數位證據，不受限於單一平台，因此本研究除妥善保管原始證據，並利用 Python 所撰寫的正規表示式過濾簡化資料，最後以 PHP 網頁呈現「揮發性資訊」，圖 4 系統基本資訊畫面、圖 5 為目前開啟的網路連線與埠號畫面、圖 6 為可能對受害主機進行暴力密碼破解之 IP 來源，我們透過 SQL 語法統計其登入失敗次數。

鑑識資訊			
鑑識人員名稱	鑑識日期	鑑識編號	
陳在天	2009/July/09 16:03:50 (Thursday)	1001	
系統資訊			
核心版本	CPU資訊	主機名稱	目前系統時間
Linux version 2.6.24-24-generic	Intel(R) Core(TM)2 Duo	pei-forensic	2009/July/21 13:54:35 (Tuesday)

圖 4 系統基本資訊畫面

圖 7 顯示的是受損系統之基本資訊（核心版本、CPU 資訊、主機名稱、目前系統日期與時間）與鑑識資訊(鑑識人員名稱、鑑識日期、鑑識編號)。

Protocol	本地IP	外來IP	開啓狀態
tcp	127.0.0.1:3306	0.0.0.0:*	LISTEN
tcp	0.0.0.0:80	0.0.0.0:*	LISTEN
tcp	127.0.0.1:631	0.0.0.0:*	LISTEN
tcp	127.0.0.1:25	0.0.0.0:*	LISTEN

圖 5 網路連線與埠號

上圖顯示目前系統開啟的 UDP 及 TCP 埠號，其包含協定名稱、本地端與遠端位置、埠號狀態，由此資訊可分析是否有開啟可能被攻擊的埠號。

IP	次數
200.157.65.194	657
66.64.128.234	331
219.94.194.246	274
74.220.16.25	43

圖 6 可疑 IP 來源統計

上圖顯示的是登入失敗 IP 列表及嘗試登入失敗次數之統計列表，圖中顯示 IP:200.157.65.194 嘗試登入次數 657 次，IP:66.64.120.234 嘗試登入次數 331 次等。

(二) Dead-analysis 系統開發

當系統遭破壞而無法開機時，使用本系統製作之 Live DVD 重新啟動受損電腦，由於完全是在 Live DVD 上運作，故不會破壞目前電腦的狀態。

本研究 Dead-analysis 之開發平台為 xUbuntu 8.04，整合開放原始碼之鑑識工具及安全工具於 Live DVD，接下來將依序說明本研究如何整合數位鑑識工具與如何中文化、圖形化鑑識工具軟體。

(1) 中文化鑑識工具

自行開發鑑識工具不但需具備深厚的程式撰寫能力，還須要經過一連串的測試與審核，國內學者林宜隆、王旭正博士等研究亦認為自行開發一套新的鑑識工具，並不是很好的方式。

因此，本研究採用外國使用多年的開放原始碼鑑識工具 Autopsy 作為研究開發的基礎，在其相同的架構下將其中文化，使該軟體更適合國人進行電腦鑑識調查。

(2) 圖形化鑑識工具軟體

目前在 Linux 系統下可使用的工具大部份皆是用終端機安裝執行工具軟體，使用該工具前，必須詳讀 man page 的說明，且須輸入的指令冗長複雜，使用門檻太高，使得大幅降低使用者的使用意願。

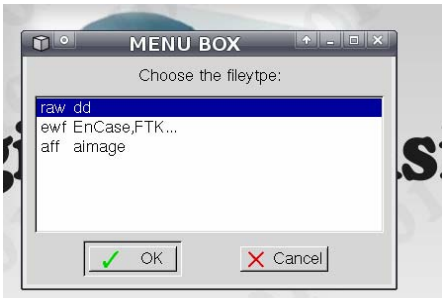

圖 7 Scalpel 圖形化畫面

本研究利用 Linux 平台中使用最廣泛的 bash shell 與 Xdialog 應用程式作為圖形化開發語言，提供使用者文字引導與圖形化的方式，協助使用者一步一步完成映像檔的分析、還原，達到更親善的人機介面，如圖 7 為 Scalpel 圖形化畫面。

(3) 鑑識報告

使用開放原始碼之鑑識相關工具優勢為成本低，但各工具間缺乏整合性，不如商業軟體從映像檔製作、分析至最後的鑑識報告呈現都已包含於套裝軟體中。因此本研究除利用成本低之優勢外，將鑑識過程中所須的工具都整合於 Live DVD 中，最後將各工具的分析結果彙整至鑑識報告，如圖 8。

圖 8 鑑識報告

五、資料分析

為了測試能否收集到駭客入侵的證據，本研究架設一台實體的受害主機，收集駭客入侵的軌跡。測試環境及事件描述，如表 2。

表 2 測試環境及事件描述

架設日期	99 年 1 月 6 日
系統硬體	Intel Core2Duo E6550 2.33GHz 150GB
作業系統	xUbuntu 8.10
系統使用者	pei、test、vivi、kevie、ftp
設置描述	系統上包含 pei、test、vivi、kevie、ftp 等五位使用者，其中 test 使用者密碼設至為 IMPERVA 公司所統計最容易被入侵之密碼「123456」，用以收集入侵行為。
犯罪發現時間	99 年 2 月 1 日 系統管理者於 99/2/1 觀看「最後登入系統之使用者」資訊，發現 test 帳號有不知明 IP 登入，隨即對該系統進行資料的收集。

在管理者發現電腦系統異狀後，即隨進行鑑識調查，由於該系統為開機狀態，因此先收集受害主機的「揮發性資訊」，再將資料送回鑑識主機，進行資料的分析。

管理者利用「lastlog」觀看使用者登入的最後時間，發現「test」帳號由非正常的 IP 登入，我們鎖定「test」帳號進行資料分析，由使用者輸入的歷史指令中發現，駭客利用暴力密碼破解使用者密碼後，他利用「sudo su」切換成 super user，並利用「uname」、「uptime」等指令觀察受害的系統狀態。

駭客為避免其建立的資料夾被管理者察覺，他試圖利用「mkdir " "」建立以空白命名的資料夾，以隱藏該資料夾，接下來，在資料夾內安裝來路不名的檔案「czech.tgz」並於「bot」目錄下執行，因此，由檔名我們可判定，該駭客以殭屍病毒來感染受害系統，這是初步由「揮發性資訊」所進行的分析，我們會透過 Dead-analysis 作進一步的追蹤，以瞭解其感染行為。

六、相關數位鑑識系統比較

表 3 本研究與美國 FBI 所採用的鑑識軟體之比較表

	本研究	EnCase	FTK	Helix
中文化介面	有，且為繁體中文	有，且是繁體中文，但翻譯的不是非常好	沒有	沒有
操作介面	容易操作	複雜	容易操作	容易操作
免費	是	沒有	沒有	沒有，但提供試用軟體
揮發性資訊收集	有，針對 Linux	沒有	沒有	沒有
證物保存，做映像檔	有，且有兩套工具，鑑識人員可依其需求選用	有	有	有
支援 EXT2/3	有	有	沒有	有
支援 FAT16/32	有	有	有	有
支援 NTFS	沒有	有	有	沒有
E-mail 尋	沒有	有	有	有
證物比	Sha-256	MD5	MD5	MD5

	本研究	EnCase	FTK	Helix
對，產生 hash				
關鍵字搜尋	有	有	有	有
密碼破解	有	有	沒有	有
相關安全工具	67 種	沒有	沒有	10 種
鑑識報告	中文	英文	英文	英文

本研究與 Helix 皆是 Live CD 的格式，透過光碟機開機，不須掛載任何硬碟上面的分割區，且利用唯讀模式開啟硬碟上的資訊，不會更動到置換空間(swap space)，因此能確保不會改變證據的狀態。

七、結論

近年來電腦犯罪案件層出不窮，犯罪手法日新月異，但凡走過必留下痕跡，鑑識人員如何在事件發生後，從受害電腦上蒐集任何的數位證據，成為當前面臨的重要課題。目前使用的商業版數位鑑識軟體成本過高，且多為英文版本，對於國人的使用上是一大障礙。

本系統整合開放原始碼之電腦鑑識相關工具於 Live DVD，使用 Live DVD 優點是重新開啟受害電腦時，因為不必安裝於硬碟，故不會更動受害電腦現有的狀態，而我們整合數位鑑識工具之目的為降低鑑識人員工具安裝時間及可利用不同工具的功能，補足單一工具鑑識能力的不足，另外，我們將部分工具中文化，降低國人使用上的門檻。

此外，我們對尚在運作的電腦進行 Live-analysis 鑑識，以預防在關閉電源後重要資訊的消失，而無法真實呈現結果，並將結果存入資料庫，方便鑑識人員分類及管理。

參考文獻

[1] 王旭正、張躍瀚、黃嘉宏、高大宇，“電腦鑑識環境建置的規劃／訓練時代需求”，國家實驗研究院科技政策研究與資訊中心資通安全分析專論，T95017，http://ics.stpi.org.tw/Treatise/，2006年。

[2] 王旭正、姚深淵、黃嘉宏、詹前隆，“Firewall-based遠端網路的數位證據蒐集，”電子商務學報，10卷1期，235頁-253頁，2008年。

[3] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computer and the Inter, Academic Press, pp.41-46, 2000.

[4] Darnet, http://www.darknet.org.uk/2006/03/10-best-security-live-cd-distros-pen-test-forensics-recovery/, February 2010.

[5] EnCase, http://www.guidancesoftware.com/, February 2010.

[6] FTK, http://www.accessdata.com/Products.html, February 2010.

[7] Hilex, http://www.e-fense.com/products.php, February 2010.

[8] C. Negus, Live Linux: Building And Customizing Bootables, Prentice Hall, 2006.

[9] OWASP，http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project，February 2010.

[10] C. Pogue, C. Altheide and T. Haverkos, UNIX and Linux Forensic Analysis DVD Toolkit, Syngress Publishing, 2008.

[11] United States National Institute of Justice, Technical Working Group for Electronic Crime Scene Investigation, 2001.

[12] X. Wang, D Feng, X. Lai and H. Yu, Collisions for Hash functions MD4, MD5, HAVAL-128 and RIPEMD, Cryptology ePrint Archive: Report 2004/199, August 2004.