Forensics Study in Exact Evidence Investigation Based upon Fixing Registry File

林曾祥
中央警察大學 資訊管理系

劉權漢
中央警察大學 資訊管理系

王旭正
中央警察大學 資訊管理系
sjwang@mail.cpu.edu.tw
*whom correspondence

摘要

根據犯罪調查人員所查獲的數位媒體裝置，Microsoft Windows 是最常見的電腦系統平台，由於硬體儲存容量的不斷增長，使得數位犯罪證據的復原成為曠日廢時的過程。甚且，分析儲存媒體所有的空間位置，對數位調查人員來說是一件困難而複雜的任務，當這兩個要素相結合時，將導致案件提交至法院的時間延遲。為了解決上述的困境，我們可以採用如下的基礎概念:針對最可能蘊藏數位證據的位置-Windows 設定檔(Registry)，進行儲存媒體的初始化分析，如此一來，鑑識分析流程以及數位證據的復原會需要更少的時間來完成，因此設定檔的相關研究顯得更加重要。本文於 Windows10 電腦裝置模擬具備價值性的檔案，針對這些檔案進行一系列的行為操作:開啟、竄改、存取，而後分別利用 Regshot 以及 Process monitor 兩種工具進行分析研究，將研究所得彙整、比較為設定檔的特徵值，並以此些特徵值為基礎調整既有的鑑識流程，提供資安健檢的附加價值。

Keywords: Digital forensics 、 Windows registry、 Regshot、 Process monitor

1、前言

電腦鑑識是數位鑑識科學的一條分支，目標是在電腦及數位儲存媒體找尋合法的數位證據[14]，數位證據則包含所有可以用來達成犯罪，或者提供「犯罪、被害者、嫌疑人」三者鍊結關係的數位資料[15]。欲從電腦系統發現數位證據須使用一些技術，而且隨著電子裝置儲存容量的上升又產生許多複雜難題:有價資訊參雜於許多資料垃圾中，數以百計的電腦及裝置等待著分析、挖掘，為了要解決既有資源(時間、儲存設備、分析裝置)的浪費問題，我們可以在證據識別階段進行分析、調整，聚焦在電腦系統上最有可能發現數位證據的區域，萃取與保存階段有別於以往，選取系統的部分空間進行映像檔的製作，分析階段則著墨於電腦系統中有機會達成犯罪、發生攻擊的區塊[8]，而這一切的數位鑑識流程調整有賴於 Windows 設定檔的研究、發揮。

Windows 作業系統是全世界最常使用的作業系統，Windows 設定檔是一個富含組態資訊的完整元件，記錄在人類使用下，硬體、軟體以及相關元件的細節，有助於後續的鑑識調查[7]。隨著 Windows 作業系統的版本不同，

Windows 設定檔會有細微的差異，在 Windows10 正式發行過後，不難想見 Windows10 將成為各家電腦大廠預設的作業系統，許多個人使用者也將選擇將其系統升級至 Windows10，因此了解資料如何在新版本的 Windows 中運行是必要的[12]。

隨著電子裝置越發貼近我們的生活，其內所儲存的訊息越是與我們息息相關，檔案的價值可能引起旁人的覬覦，不論其起心動念為何，我們都很好奇自身裝置是否始終獨立的存放，在離開期間若遭旁人使用是否會留下線索、痕跡。隨著資安議題的沸沸揚揚，檔案的開啟、存取甚至是竄改依然是眾人關注的焦點，是以本研究利用設定檔的監控工具：Regshot 以及 Process monitor，觀察一系列行為下的設定檔變異，提供個別使用者資安健檢的參考指引，並作為鑑識檢查人員日後流程調整的指標。

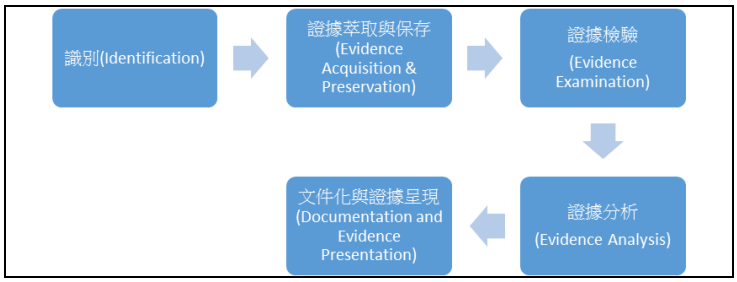
本篇文章的章節編排如下：第二節為背景知識，說明鑑識流程，並介紹 Windows 設定檔的相關概念。第三節為本文研究 Regshot 及 Process monitor 兩種工具的實驗。第四節是工具比較與數位鑑識效能。第五節範例與證據分析。第六節為結論。

2、背景知識

本研究將從數位鑑識的流程談起，接著探討媒體儲存裝置發展下的鑑識流程困境，最後說明 Windows 作業系統下的設定檔(Registry)，包括其相關定義、命名法、及其於硬體中的位置。

2.1 數位鑑識的流程

數位鑑識是個多步驟的流程(如圖一)[10]，



圖一、數位鑑識流程

2.1.1 識別：

從犯罪場景內的數位媒體識別潛在性的證據，最後由專家證人在法院上呈現之，此步驟涉及一個或者多個數位儲存媒體的識別，數位媒體所儲存的數位資訊將於後續步驟著手調查。

2.1.2 證據萃取與保存：

此步驟主要是針對識別後的數位媒體，將其所包含的所有內容以二進位的方式進行拷貝、複製，而後透過標準化的雜湊簽章(例如：MD5 或者 SHA1)將其保存下來，如此便可確保數位證據的完整性。

2.1.3 證據檢驗：

一旦數位證據經過萃取、保存過後，就必須在這些唯讀的複製檔進行鑑識性的測試，避免任何行為竄改了儲存自原始來源的資料[4, 5]。Casey 對於證據檢驗的定義如下：〝從數位證據中萃取資訊並使其得以用於後續的分析〞[3]。

2.1.4 證據分析:

Casey 將證據分析定義為〝科學方法以及關鍵思維的應用，以解決調查中基本的問題〞[3]。

2.1.5 文件化與證據呈現:

這些個別步驟的過程將因此記錄在案，而且此紀錄檔案亦將呈現於法庭，有時，法庭上的數位證據呈現可能伴隨著專家證人的作證。

2.2 電子裝置發展下的鑑識困境

電子裝置的日漸流行，引起儲存媒體容量上的巨幅成長，伴隨電子裝置的價格下降，導致一項重大議題:司法程序的即時性。擷取資料正不斷成長且等待著後續的分析、呈現，數以兆計的資料組成正等待著每位調查人員，此現象主要由下列原因所導致[9]:

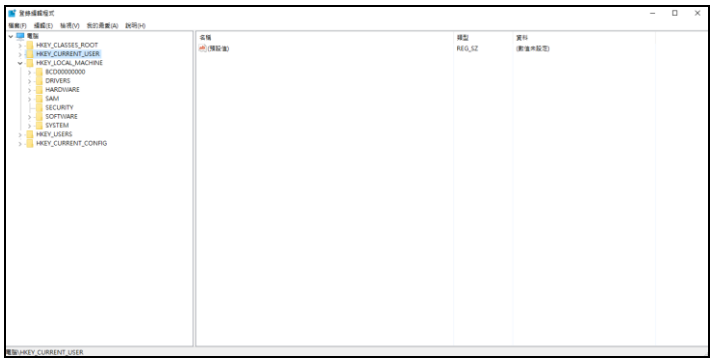
1. 每件案子所牽涉的裝置數量增加。
2. 和數位證據有關的案件日增。
3. 每項裝置所蘊藏的資料量逐漸上升。

案件及裝置數量的增加，複合裝置儲存容量的上升[6]，現行的鑑識軟體解決方案從最初的工具產生，演化至今日的可擴展性議題，然而，量大而歧異性高的資料集分析仍存在著缺口，每一年的資料量增加都快過處理器的能力以及鑑識工具所能負荷[11]，處理次數隨著所需分析的資料量相對應的增加，近十年來，有許多呼聲要求研究聚焦在大型資料集的分析上[6]，包括資料探勘技術的應用，以及數位鑑識領域正努力解決的資訊量成長議題[1]。

和資料量積壓有關的嚴重影響包括:有罪被告的刑期減免，因等待鑑識分析結果的時間長短而有所不同;嫌疑人在等待鑑識分析的過程自殺或者拒絕接觸原生家庭及兒童[13]。此外，長期被調查的嫌疑人可能在就業上受到影響，當電腦和其他設備遭到扣押時，嫌疑人或者無辜者可能因而遭遇困境，嫌疑人的筆電裡可能存有孩子的學校作業或者另一半的稅務資料和商業訊息。

2.3 設定檔(Registry)的定義

Windows 設定檔是一個二元資料結構，意圖用來取代 Windows 早期版本(Windows 3.1)的組態檔案或者初始檔案，這對一般的 Windows 使用者以及管理人員來說，減輕了使用上的負擔且清楚容易瞭解。設定檔內的登錄檔以及組態資訊在電腦鑑識調查中顯得相當重要，因為它們可以幫助我們識別裝置上所發生的活動，設定檔不僅以專有的形式儲存而且只有專屬的工具能夠有效的從中存取資訊，多數的使用者以及管理人員並不直接和設定檔進行接觸、互動，而是透過某種圖形化使用者介面，例如:登錄編輯程式(如圖二)，登錄編輯程式通常和 Windows 一同安裝發行[2]。



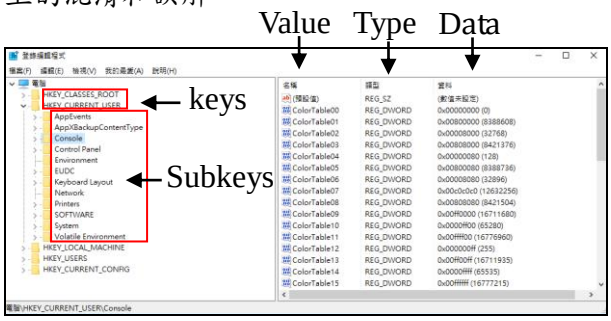
圖二、登錄編輯程式

2.4 設定檔的命名法(Nomenclature)

當我們談論到設定檔的時候，能有一致的理

Value

解和認識是相當重要的，彼此都清楚所指的是設定檔的哪一個區塊(如圖三)，方可避免溝通上的混淆和誤解。

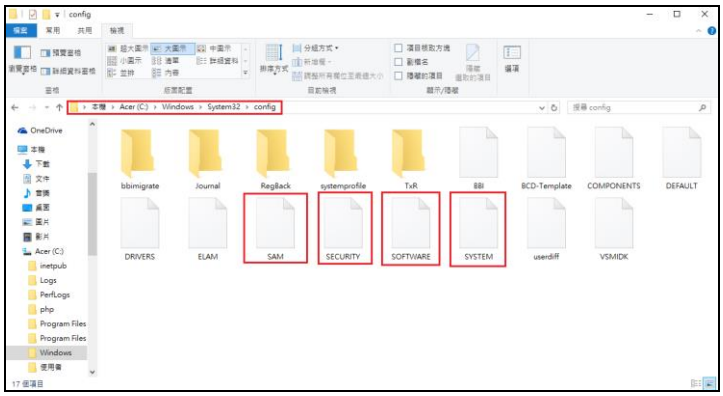


圖三、設定檔的命名法(Windows10)

Keys 與 Subkeys 是顯示於編輯器左側儀表板的資料夾，這是一個恰當的比喻，因為鍵可以包含或者指向其他的鍵(例如:子鍵)或者數值，由鑑識角度觀之，二進制的鍵值架構也包含非常有價值的資訊(例如:最後寫入的時間)，右側儀表板的數值(Value)包含了資料(Data)及其所屬型態(Type)，可能為字串值、多重字串值、二進位數值、或者 32 位元的二進位數值 DWORD。

2.5 設定檔於硬體中的位置

由鑑識角度觀之，分析人員通常並非透過登錄編輯程式和設定檔互動，大多透過商業鑑識分析軟體和蜂巢狀的設定檔接觸，或者從檔案系統及映像檔萃取之，對分析人員來說，瞭解此些檔案於硬碟上的所在位置是很重要的，如此方能將其取回進行後續分析，大抵而言，核心系統的設定檔可於下列路徑找到：「C:\Windows\system32\config folder」(如圖四)所示:

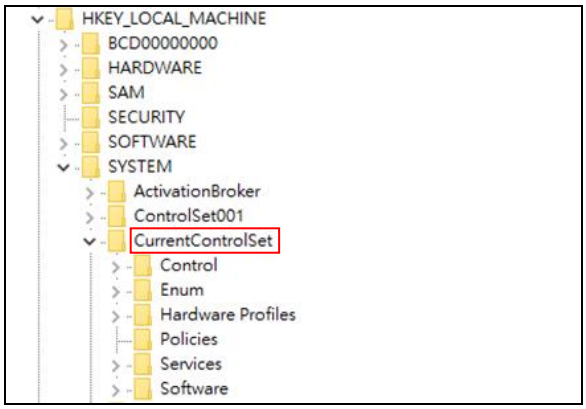


圖四、核心系統的設定檔(Windows 10)

透過登錄編輯程式所能看見的 Windows 設定檔，某部份具有“揮發性”，這也意謂著:當系統啟動或者使用者登錄時，檔案內容隨之充填，當系統關閉時則不存在於硬碟中，此部分的瞭解對於事件最先回應者及鑑識分析人員來說是相當重要的，因為某些有價資料並不存在於萃取而得的映像檔中，而必須在系統運行時進行蒐集。揮發性資料的其中一個案例:〝HKEY_CURRENT_USER〞，透過登錄編輯程式可以清楚的看見這個蜂巢狀檔案，而且在些的許探勘後，將發現此部分的設定檔資訊專屬於某位登錄使用者，然而，當關閉系統並且分析萃取而得的映像檔，你將不會發現 HKEY_CURRENT_USER 或者名稱相同的檔案，那是因為此檔案的充填是透過使用者登錄系統，並且針對近期登錄的使用者而言。

另一個揮發性鍵值案例是:〝HKEY_LOCAL_MACHINE\Hardware〞，此鍵值儲存了和系統相連接的設備資訊(中央處理器、鍵盤、硬碟等)及其所指定的資源，系統啟動時打開登錄編輯程式，搜尋〝HKEY_LOCAL_MACHINE\System〞，你將會看到一個名為〝CurrentControlSet〞(如圖五)的鍵，還有另外兩個很相似以 ControlSet0 開頭且以數字作結尾，系統關閉時 CurrentControlSet

即不存在。



圖五、CurrentControlSet(Windows 10)

尚有另一個設定檔的揮發性案例:〝HKEY_CLASSES_ROOT〞,當系統啟動時此鍵將以〝HKEY_LOCAL_MACHINE\Software\Classes〞的內容充填;當某位使用者登錄時,〝HKEY_CURRENT_USER\Software\Classes〞的內容將因此增加。說明至此,須銘記於心的重要事項為:某部分的 Windows 設定檔只存在於記憶體中,這些資訊可以透過必要工具進行存取、取回、而後分析。

3. 研究實驗

在實際進行進行設定檔的研究之前,必須先了解哪些工具可以協助我們觀察設定檔的變動,每項工具皆有其優劣,最好的方式是在時間允許下使用多種工具,如此方能解釋更廣泛的人為結果、令實驗結果得以再次檢驗,並且維持各種鑑識軟體的熟練度,主要目的是用有效的方法萃取所關注的精確資料集[12]。

3.1 RegShot

Regshot 是一個開源實用程式,用於紀錄並且彙整 Windows 設定檔所受到的異動,此程式的運作是透過用戶指定目錄的初始快照,經過某些變動過後(例如:應用程式的安裝、或者外接式數位媒體裝置的使用)進行第二次的快照,而後根據用戶的喜好將差異以純文字或者 HTML 檔產出,此工具有一個簡單的圖形化使用者介面,受到資訊科技專家、家庭使用者、以及鑑識檢查人員的廣泛使用,使用 Regshot 監控設定檔是故障排除的便捷方法,特別是在安裝新的應用軟體後,不慎對作業系統產生負面的影響。

3.2 RegRipper

另一個用於設定檔鑑識分析的開源工具是 RegRipper,由 Harlan Carvey 所設計,這並不是一個全方位的設定檔分析工具,而是以 Perl 實作而成的插件(plugin)平台,利用各式插件從設定檔萃取資訊,目前有 Linux 和 Windows 作業系統的軟體版本,以及 324 個事先建好的擴充插件,這些插件亦可由使用者進行客製化的撰寫,除了必須熟悉 Perl 腳本之外,還須瞭解插件所解析的細節類型。相較於 Regshot 其好處在於運行時會產生一份日誌文件,這在鑑識上頗有助益,因為可將運行於特定證據項目的行程檔案化。

3.3 SysInternals Suite

SysInternals Suite 是一款 Microsoft 的免費工具,就像 ProcMon 所提供的行程監控,允許使用者在 Windows 工作平台上識別即時的運作,結果的呈現可透過多種方式過濾,以磨練出特定的資料集。主畫面上的圖標讓使用者聚

焦在僅和設定檔有關的變化上，這些結果更可藉由過濾器的選擇及參數的指定進一步的過濾，例如:使用 ProcMon 視察外部媒體裝置所帶來的設定檔變化時，可利用過濾器僅顯示和設定檔寫入有關的操作(如圖九)。當過濾器設定完畢並且引入一個掛載裝置後，即可捕捉變動的結果，使用者可以用“CTRL E” 開始或者暫停記錄功能，此功能對限縮觀察事件的範圍很有幫助。

3.4 EnCase Enterprise

EnCase 平台亦提供將設定檔異動檔案化的功能，EnCase 能夠分析已配置空間及未配置空間的紀錄，還可進行資料的分類及雜湊演算，Windows 設定檔的未配置空間可能包含刪掉的紀錄及檔案片段，EnCase 的功能特色在於將各種設定檔掛載為項目實體，包括未配置空間的數值與紀錄，這些項目實體可以被雜湊演算並且分析製檔，作為控制測試的結果。雜湊分析結果可能是大量的，幸運的是，結果範圍可以透過事件發生的時間日期進一步分類聚焦，這項技術確保設定檔紀錄了事件及相對應的時間軸。

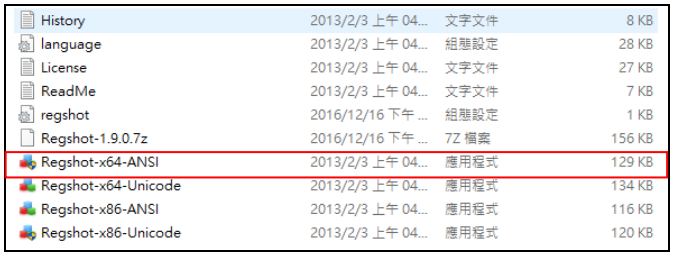
諸如 Carvey 等設定檔研究人員[2]，於 Windows7 及 Windows8 的設定檔中，使用上述討論的工具將掛載裝置上的行為痕跡檔案化，當我們慮及機器上的活動紀錄，這些行為痕跡有很高的鑑識價值，鑑識檢驗人員及事件即時回應人員，致力於獲得工作站的日誌完整記錄，利用上述工具紀錄觀察結果，可以提供一組共通的資料集，有效將行為操作和變動區域相互對應[12]。

3.5 實驗流程

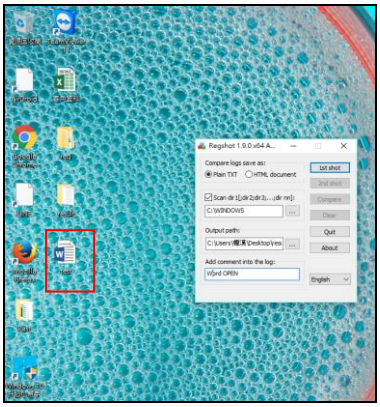
本次研究主要是以 HP Probook 440 為硬體平台，並且搭配 Windows10 的作業系統環境，模擬鑑識檢驗人員未來最有可能遇見的操作場景，針對所欲探求的標的-(Registry)選用 Regshot 及 Process monitor 軟體工具，先後進行一系列的分析實驗:1. 文件開啟 2. 內容竄改 3. 檔案存取，實驗步驟如下:

3.5.1 Regshot:

解壓縮後的 Regshot 有四個選項可供選擇(如圖六)，使用者可以依自身之硬體條件選用，筆者在 Windows 10 環境下的測試成果，發現 Unicode 不如 ANSI 來得穩定，時常發生無法開啟或者比對檔無法產生之狀況，所以後續實驗皆以 ANSI 為主。並且自行假設實驗用之 Word 文檔:test.doc(如圖七、八)，實驗步驟大致如下: 1. 初始環境掃描、建檔 2. 目標行為操作、環境掃描 3. 掃描成果比對、關機 4. 開機、環境掃描、差異比對



圖六、Regshot 之選用



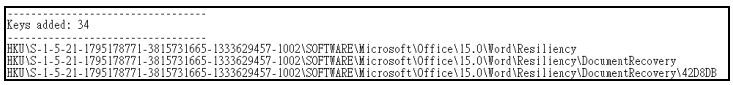
圖七、實驗用之 test 文檔

圖八、test 文檔之內容

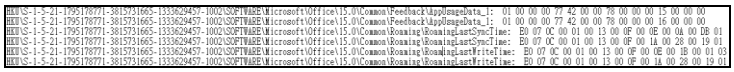
之所以加入關機和開機的動作，一來是讓模擬情境更加逼真，因為關機將導致揮發性資料的遺失，有助於掩藏犯罪手法，二來是在掃描檔的相互比對之下，觀察關機行為將對設定檔產生什麼樣的影響。

3.5.1.1 Word 檔開啟:

對於 Word 檔的開啟，我們可更細分為「檔案開啟中」以及「檔案開啟而後關閉」，兩者在 Keys deleted 有著同樣的結果，但是在 Keys Added 則有些微的差異，估計是在檔案開啟的狀態，系統預留 Keys 以待未來復原所需(如圖九)。而後我們以「office」作為搜尋之關鍵字，皆可於兩者的 values modified 發現相似的時間記錄構造，即便是重新開機後的比對結果亦是如此(如圖十)。



圖九、檔案開啟較檔案關閉多出三個 Keys



圖十、相似的時間紀錄構造

3.5.1.2 Word 檔內容竄改:

針對內容竄改我們做同樣的細分，並且在對比檔發現相同的邏輯規律:Keys deleted 相同、Keys Added 保持些微的差異，只是重新開機後的結果比對，反而更明確的指示使用者 X 曾在某時間進行資料竄改（如圖十一）。

圖十一、重新開機後的對比結果反而更加明確

3.5.1.3 用 USB 進行 Word 檔存取:

在尚未關機之前，我們試著同樣以「office」進行搜尋卻無功而返，反倒是重新開機後可於 Values added 得到一行相關提示，此外，若我們以「usb」作為關鍵字進行搜尋，不論是重新開機前後系統都詳實記錄著 USB 的相關訊息(如圖十二)

圖十二、USB 存取所遺留下的相關訊息

3.5.1.4 利用 hotmail 夾帶檔案:

檔案的夾帶及傳送完成後便進行瀏覽紀錄的清空，以此提高做案手法以及對比檔的研究價值，結果顯示:不論是重新開機前、後，以關鍵字「office」、「browser」、「docx」3 等，

皆無法找到有效的相關訊息，唯獨在兩者之 file modified 可以發現關鍵字「chrome」的蹤影(如圖十三)。

```
C:\WINDOWS\Prefetch\CHROME.EXE-CCF9F3F5.pf
C:\WINDOWS\Prefetch\CHROME.EXE-CCF9F3F6.pf
C:\WINDOWS\Prefetch\CHROME.EXE-CCF9F3FA.pf
C:\WINDOWS\Prefetch\CHROME.EXE-CCF9F3FB.pf
C:\WINDOWS\Prefetch\CHROME.EXE-CCF9F3FC.pf
```

圖十三、僅存的 chrome 痕跡

3.5.1.5 將檔案上傳至雲端空間:

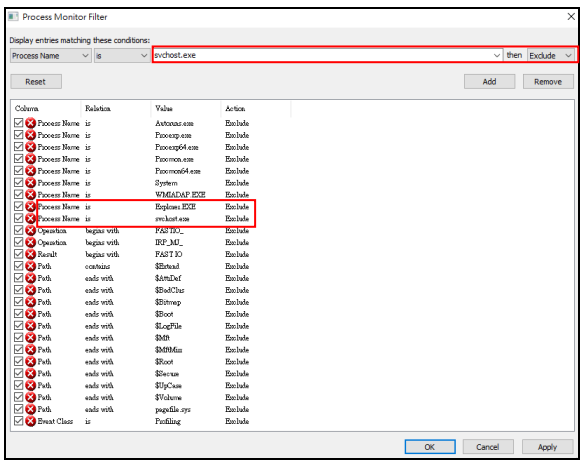
雲端的操作和 hotmail 檔案夾帶相去不遠，唯獨以「browser」作為關鍵字時，重新開機前後皆於 Values deleted 產生相似的證據痕跡，最後，兩者同樣可於 file modified 發現關鍵字「chrome」的蹤影，只是數量痕跡較少(如圖十四)。

```
C:\WINDOWS\Prefetch\CHROME.EXE-CCF9F3F4.pf
```

圖十四、於對比檔尾聲所發現的 chrome 痕跡

3.5.2 Process Monitor:

打開 Process Monitor 可以發現系統狀態不斷的更新，其中許多並非是我們感興趣的技術操作，因此我們可以利用過濾器針對系統常駐程式(例如:svchost.exe、Explore.exe 等)進行第一層級的過濾(如圖十五)。

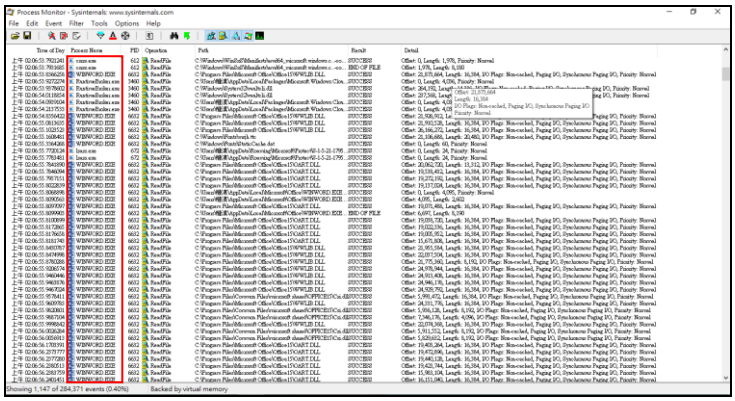


圖十五、過濾器設定

實驗步驟大致如下:1. 打開程式進行錄製 2. 目標行為操作 3. 停止錄製、調整過濾器 4. 搜尋標的、分析比較成果

3.5.2.1 Word 檔開啟:

慮及此為讀檔行為，於是在過濾器新增「Operation is Readfile then include」的設定，接著發現此行為之操作多半跟 word 檔之檢視相關(如圖十六)，便能在接下來的過濾結果發現目標檔的確經過開啟。



圖十六、Word 檔開啟之相關追蹤

3.5.2.2 Word 檔內容竄改:

由於此為寫入檔案的行為，於是在過濾器新增「Operation is Writefile then include」的設定，接著便於過濾結果輕鬆發現目標檔案。

3.5.2.3 用 USB 進行 Word 檔存取:

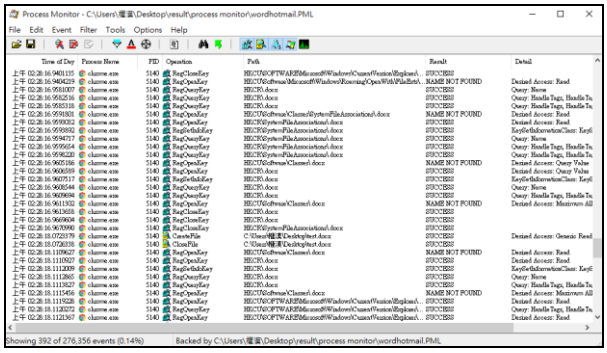
面對 USB 的存取行為，以及隨之而來的軟體紀錄結果，一時半刻可能不知該從何下手，筆者建議利用檔案類型進一步的限縮結果，我們雖然無法確切知道哪些檔案遭到存取，卻可以推敲感興趣的標的檔是什麼類型，例

如:docx、pdf、xlsx 等，接著我們在過濾器新增「path ends with .docx then include」的設定，便能意外的探知隨身碟的存取結果(如圖十七)。

圖十七、發現硬碟 H 曾有 test.docx 的存取

3.5.2.4 利用 hotmail 夾帶檔案:

快覽紀錄結果之後，我們發現這段期間的操作和 Chrome 息息相關，於是我們在過濾器新增「Process Name is chrome.exe then include」的設定，然此過濾結果仍充斥許多不感興趣的資訊、影響判讀，讀者仍可套用檔案類型之限縮方法，達成目的檔之搜尋效果(如圖十八)。



圖十八、利用過濾器篩出 hotmail 之檔案夾帶

3.5.2.5 將檔案上傳至雲端空間:

基本上雲端的上傳和 hotmail 的檔案夾帶都是通過瀏覽器進行，是以兩者的搜尋狀況及結果大同小異，於此不再贅述。

4. 比較與數位鑑識效能

為了維持系統的正常運作，電腦系統會維護一組組態資訊，連同使用者的操作行為一併紀錄、管理，Windows 作業系統主要是透過設定檔達成上述功能，因此我們可以透過 Regshot 及 Process monitor 兩種工具，觀察設定檔在檔案存取前後所發生的變化，為避免設定檔之揮發性影響判讀，使用 Regshot 觀察設定檔在電腦重啟前、後之不同變異，針對感興趣之檔案操作行為，將第三節之實驗結果歸納如下(如表一):

表一、以 Regshot 觀察設定檔變化

	word 檔案開啟	word 檔案竄改	以 USB 夾帶 word 檔案	Hotmail 夾帶 word 檔案	將 word 檔上傳雲端
關機前	✔	✔	✘	✘	✘
關機後	✔	✔	✔	✘	✘

符號 ✔:可找到標的檔;
符號✘:無法找到標的檔

對於檔案開啟的行為，不論其現行為開啟的狀態，或歷經開了又關，我們都可以在關機前、後發現「Microsoft\Office\15.0」的蹤跡，以及相似的寫入時間架構。檔案竄改行為可比照檔案開啟作同樣的細分:竄改中、竄改結束，同樣可以發現「Microsoft\Office\15.0」的痕跡，只是關機又重啟的行為讓寫入時間的指示更加明確，甚至可以和寫入的使用者相互對應。

若以隨身碟進行檔案的存取，關機前我們無法得到標的檔任何相關資訊，反倒是在重新啟動後得到了一行線索，但是不論關機與否，隨

身碟的詳細資料皆會記錄在案。最後是對於網路存取行為的探討，雖可分為 hotmail 夾帶檔案以及雲端空間上傳兩種，但此兩者的對比紀錄皆無標的檔的蹤跡，頂多只有使用 browser 及 chrome 的零星紀錄。

由於 Process monitor 主要提供即時監控的功能，所以就不做關機前後的區分，而且只要過濾條件設定的當，就能在各式存取行為下發現標的檔的紀錄，雖然在隨身碟存取 word 檔的實驗項目中，其所記錄之隨身碟資訊不如 Regshot 來的詳細，可是卻彌補了 Regshot 在網路存取的不足，因此我們可以根據兩者之特性列出比較表(如表二)。

表二、Regshot 及 Process Monitor 之比較

	Regshot	Process monitor
優	1. 即便是關機狀態，仍可於重啟後進行紀錄比對。 2. 詳細記錄外接式儲存媒體的相關資訊。	1. 使用者不需事先持有一份紀錄檔。 2. 可以針對網路存取行為，進行詳實而有效的紀錄。
缺	1. 使用者須先持有一份紀錄檔，方得進行操作後的行為比對。 2. 對於網路存取檔案的行為，無法有效偵測標的檔參與其中。	1. 使用時，須持續保持開機狀態。 2. 使用外接式儲存媒體所遺留下之媒體資訊略顯粗糙。

認識設定檔特徵有助於數位鑑識流程的調整(如圖十九)，從背景環境搜索出感興趣的電子裝置後，於識別階段可先進行一次初始化分析，尋找證據最有可能的所在位置，而後在萃取與保存階段，只需針對部分空間進行映像檔的製作，相較於全域空間的複製拷貝，資料量將大幅的減少，而這也意謂著後續檢驗、分析所需時間下降，以滿足司法即時性的要求。鑑識調查人員可以根據使用者所使用軟體:Regshot 或者 Process monitor，搭配設定檔特徵值之背景知識，判斷標的檔的名稱、解讀存取時間及存取方式，藉此分析其於硬碟上之所在位置，在初始分析後針對部分硬體空間進行證據萃取與保存，以此降低後續證據檢驗、證據分析之所需時間。

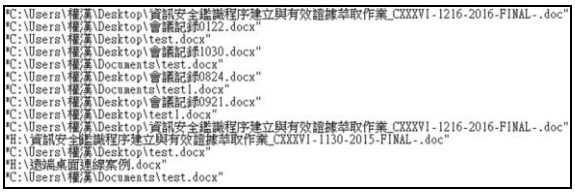
圖十九、數位鑑識流程之調整

5. 範例與證據分析

A 君是董事長身旁的機要秘書，常常列席公司高層的主管會議，亦兼處理重要會議記錄與機密檔案登載管理。有天 A 君發現前天下班忘記隨手關機，辦公室疑似遭不明人士潛入，並竊取了電腦內重要機密性檔案資料，正當 A 君為此感到焦慮時，靈機一動想起前天因朋友推薦而測試使用的軟體-Regshot，他趕緊打開軟體、載入之前錄製好的系統環境作為 shot1，接著掃描現行的環境狀態為 shot2，等一切準備就緒後進行兩者的快照比對，並於對比檔進行一系列的特徵值搜尋。

【步驟一】搜尋標的檔之操作痕跡

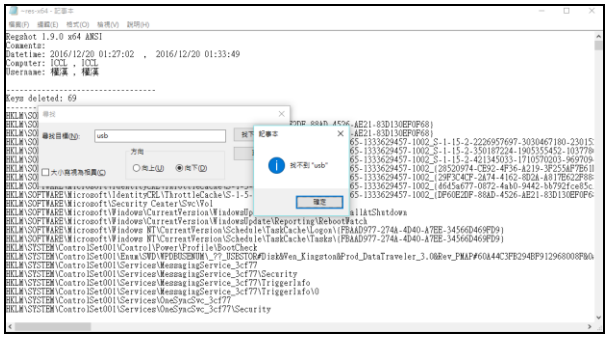
首先，A 君根據較具機密性的重要檔案標的-會議記錄，針對其共通性-「office」檔，以此為關鍵字進行搜索，藉此確認檔案是否有經過開啟或是竄改(如圖二十)，果然可以發現許多會議記錄有開啟的跡象，應可推測入侵者曾於 A 君的電腦進行檔案翻找的動作。



圖二十、office 檔紀錄搜尋

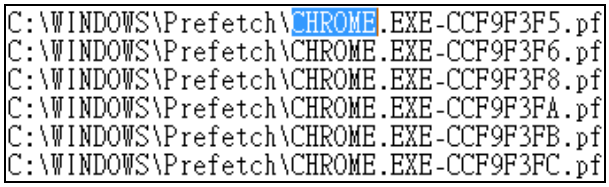
【步驟二】確認檔案散布途徑

A 君接著以「usb」為關鍵字搜索(如圖二十一)，發現並無相關紀錄因此可以將 usb 存取檔案的操作可能性刪去。



圖二十一、搜尋利用 USB 存取檔案的可能性

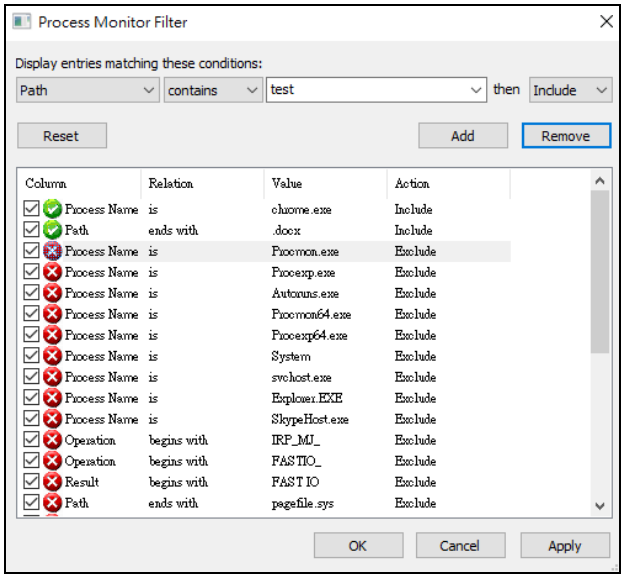
A 君仍想知道，入侵者若非透過外接式儲存媒體(usb)，是否仍有可能透過網路的方式(E-mail 或雲端硬碟)將檔案夾帶出去，於是 A 君接著使用「chrome」為關鍵字進行搜索(如圖二十二)，果然於對比檔的尾端發現 file modified 有 chrome Prefetch 的痕跡，因此不排除有文件從網路的途徑攜出。



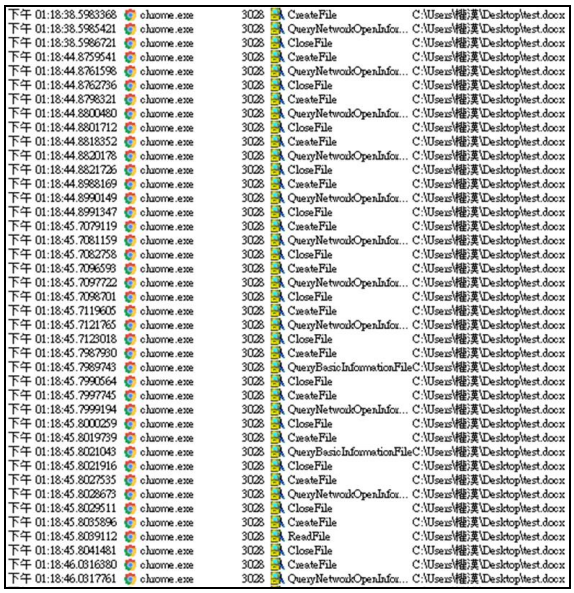
圖二十二、探究文件從網路攜出的可能

【步驟三】入侵行為之後續追蹤

A 君掌握大致情況後，決定不動聲色的在電腦上安裝 Process monitor，因為嫌疑犯很可能重回犯罪現場再次犯案，而且機密外洩的事情也不好向外界聲揚，他必須靠自己將嫌疑犯繩之以法，於是 A 君養成每天檢查系統狀況的習慣，以固定的過濾篩選條件監控檔案的存取情況(如圖二十三)，終於在某一天的過濾結果發現不合理的資料內容(如圖二十四)，下午 1:18 仍是 A 君固定的午休時間，怎麼會有利用 chrome 瀏覽器夾帶 Word 檔的情況呢?於是 A 君按照此時間點調閱監視錄影器，這才發現兇手是新進員工 B 君，他在瞭解 A 君之回家午休習慣過後，伺機摸入 A 君之辦公室，試圖將公司之機密文件攜帶而出，A 君將監視畫面及電腦上之比對結果提供給調查人員，B 君亦因己身不法行為遭受逮捕。



圖二十三、以固定條件監控感興趣的目標檔案



下午 01:18:38.5983368	chuome.exe	3028	CreateFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:38.5985421	chuome.exe	3028	QuesyNetwoukOpenInfou...	C:\Users\權漢\Desktop\test.docx
下午 01:18:38.5986721	chuome.exe	3028	CloseFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:44.8759541	chuome.exe	3028	CreateFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:44.8761598	chuome.exe	3028	QuesyNetwoukOpenInfou...	C:\Users\權漢\Desktop\test.docx
下午 01:18:44.8762736	chuome.exe	3028	CloseFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:44.8798321	chuome.exe	3028	CreateFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:44.8800480	chuome.exe	3028	QuesyNetwoukOpenInfou...	C:\Users\權漢\Desktop\test.docx
下午 01:18:44.8801712	chuome.exe	3028	CloseFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:44.8818352	chuome.exe	3028	CreateFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:44.8820178	chuome.exe	3028	QuesyNetwoukOpenInfou...	C:\Users\權漢\Desktop\test.docx
下午 01:18:44.8821726	chuome.exe	3028	CloseFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:44.8988169	chuome.exe	3028	CreateFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:44.8990149	chuome.exe	3028	QuesyNetwoukOpenInfou...	C:\Users\權漢\Desktop\test.docx
下午 01:18:44.8991347	chuome.exe	3028	CloseFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.7079119	chuome.exe	3028	CreateFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.7081159	chuome.exe	3028	QuesyNetwoukOpenInfou...	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.7082758	chuome.exe	3028	CloseFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.7096593	chuome.exe	3028	CreateFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.7097722	chuome.exe	3028	QuesyNetwoukOpenInfou...	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.7098701	chuome.exe	3028	CloseFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.7119605	chuome.exe	3028	CreateFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.7121765	chuome.exe	3028	QuesyNetwoukOpenInfou...	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.7123018	chuome.exe	3028	CloseFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.7987990	chuome.exe	3028	CreateFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.7989743	chuome.exe	3028	QuesyBasicInformationFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.7990564	chuome.exe	3028	CloseFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.7997745	chuome.exe	3028	CreateFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.7999194	chuome.exe	3028	QuesyNetwoukOpenInfou...	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.8000259	chuome.exe	3028	CloseFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.8019739	chuome.exe	3028	CreateFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.8021043	chuome.exe	3028	QuesyBasicInformationFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.8021916	chuome.exe	3028	CloseFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.8027535	chuome.exe	3028	CreateFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.8028673	chuome.exe	3028	QuesyNetwoukOpenInfou...	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.8029511	chuome.exe	3028	CloseFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.8035896	chuome.exe	3028	CreateFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.8039112	chuome.exe	3028	ReadFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:45.8041481	chuome.exe	3028	CloseFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:46.0816380	chuome.exe	3028	CreateFile	C:\Users\權漢\Desktop\test.docx
下午 01:18:46.0817761	chuome.exe	3028	QuesyNetwoukOpenInfou...	C:\Users\權漢\Desktop\test.docx

圖二十四、在不正常的時間點發現檔案上傳

綜上所述，本案例首先於工具軟體 Regshot 的協助下，以標的檔之共通性搜尋其異動之痕跡，而後以特徵值「usb」、瀏覽器「chrome」確認檔案之散布途徑，為便於此非法行為之後續追蹤，接著利用軟體 Process monitor 監控電腦之日常運作，最後在過濾器的篩選下發現關鍵時間點以及異常操作，根據此關鍵時點及監視器畫面可以鎖定檔案攜出之可能人選，最後以電腦上之證據偵查結果解釋其非法進入之原因，此三者之有效串連可協助偵破一起商業間諜之入侵案件。

6. 結論

電子裝置的容量上升衝擊了既有的鑑識流程，鑑識人員須於有限時間內識別感興趣的裝置，進而從龐雜的資料垃圾中萃取數位跡證，以待後續之證據分析、呈現。本研究專注於檔案操作後的系統紀錄痕跡，除了透過 Process monitor 即時監控檔案操作所帶來的影響，更在 Regshot 的快照比對下，觀察設定檔的前後差異，接著針對此些紀錄變化以關鍵字進行搜尋，不難發現標的檔遭受開啟、竄改而留下的數位痕跡，唯獨在檔案存取方面較難發現直接相關的證據指標。甚且，關機前後的結果比對也和我們的認知相異，反倒是在電腦重啟後可於系統設定檔發現更多的使用紀錄。透過實驗結果的分析、比對，可將設定檔的變動彙整為特徵值，幫助我們更加精確的識別標的檔，而得以鎖定感興趣的硬體部分空間，使得分析所需時間大幅下降，此外，設定檔的特徵值研究可以附帶出資安健檢的功能，當電腦裝置上的檔案文件越是機密，使用者越有理由自行發現電腦裝置的使用痕跡。

參考文獻

[1] N. Beebe and J. Clark, "Dealing with terabyte data sets in digital investigations," *IFIP International Conference on Digital Forensics*, Springer US, 2005.

[2] H. Carvey, Windows registry forensics: Advanced digital forensic analysis of the windows registry, Elsevier, 2011.

[3] E. Casey, *Digital evidence and computer crime: Forensic science, computers, and the internet, Academy Press Publications*, London, 2011.

[4] Common Digital Evidence Storage Format Working Group (CDESF-WG), "Standardizing digital evidence storage," Commun ACM, 49(2), pp.67–68, 2006.

[5] Common Digital Evidence Storage Format Working Group (CDESF-WG), "Survey of disk image storage formats.", 6th annual

digital forensic research workshop (DFRWS'05), pp 1–1, New Orleans, 2006.

[6] S. Garfinkel, P. Farrell, V. Roussev, and G. Dinolt, "Bringing science to digital forensics with standardized forensic corpora," Digital Investigation 6, S2–S11, 2009.

[7] J. Luttgens, M. Pepe, and K. Mandia, *Incident response & computer forensics*, McGraw Hill Professional, 2014.

[8] E.P. Panchal, "Extraction of Persistence and Volatile Forensics Evidences from Computer System," International Journal of Computer Trends and Technology (IJCTT)-volume4 Issue5, pp.964-968, 2013.

[9] D. Quick, and K. K. R. Choo, "Impacts of increasing volume of digital forensic data: A survey and future research challenges," Digital Investigation, 11(4), pp.273-294, 2014.

[10] S. Raghavan, "Digital forensic research: current state of the art," *CSI Transactions on ICT* 1.1, pp.91-114, 2013.

[11] V. Roussev, C. Quates, and R. Martell, "Real-time digital forensics and triage," Digital Investigation, 10(2), pp.158-167, 2013.

[12] J. S. Shaver, " *Exposing vital forensic artifacts of USB devices in the Windows 10 registry",* Diss. Monterey, California: Naval Postgraduate School, 2015.

[13] A. Shaw and A. Browne, "A practical and robust approach to coping with large volumes of data submitted for digital forensic examination," *Digital Investigation, 10*(2), pp.116-128, 2013.

[14] Computer forensics, Retrived from http://en.wikipedia.org/wiki/Computer_forensics, 2016.

[15] Digital Evidence, Retrieved from http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Presentations/DigitalEvidence.pdf, 2016.