主記憶體鑑識方法之研究

朱惠中
華梵大學資訊管理學系
hcchu@cc.hfu.edu.tw

鍾文魁
國巨管理顧問(股)有限公司
mark.chung@msa.hinet.net

葉廣傑
華梵大學資訊管理學系在職專班研究生
jay5338@gmail.com

摘要

隨者資訊科技的進步與資訊教育的普及，電腦犯罪案件亦不斷增加，而在網際網路蓬勃發展之下，數位證據除儲存於非揮發性儲存媒體外，亦會儲存於揮發性儲存媒體，如何從揮發性儲存媒體(特別是電腦的主記憶體)中擷取相關的數位證據，已成為鑑識人員主要的課題之一。

本研究將在 Windows 作業系統架構下，對主記憶體中數位證據之採證及分析方法進行深入探討，並整合相關數位鑑識工具，開發針對主記憶體中之數位證據自動採證及分析工具，再以案例來驗證該工具的可行性與有效性，期能幫助鑑識人員減少採證程序產生之錯誤，以及強化數位證據分析深度。

關鍵詞：數位鑑識、主記憶體鑑識

壹、緒論

隨著資訊科技的進步及資訊教育的普及，電腦犯罪的案例，亦逐年呈巨幅的增加，面對這些涉及電腦的傳統不法或是電腦犯罪案件，傳統的證據及其採證方法已無法有效的在法庭上起訴嫌疑犯，而必須用數位鑑識工具來幫助鑑識數位證據，以為呈堂證據；而由於網際網路的使用率增高，相關數位證據除儲存於非揮發性儲存媒體外，亦會儲存於揮發性儲存媒體，故如何從揮發性儲存媒體(特別是電腦的主記憶體)中擷取相關的數位證據，已成為鑑識人員主要的課題之一。

由於電腦作業系統及程式在執行時皆會利用電腦之主記憶體進行運算，所以鑑識人員使用鑑識工具進行主記憶體採證動作時，鑑識工具亦會載入至主記憶體中執行，造成主記憶體內資料的改變，因此鑑識人員除了須依據適當的採證程序進行之外，也應該採用自動化的鑑識工具來協助主記憶體之採證行為，避免因為人為的操作錯誤，造成暫存在主記憶體中數位證據的破壞，另外，新興的電腦犯罪會利用網際網路隱匿之特性進行，例如使用網頁加密通道(Secure Sockets Layer, SSL)技術來進行犯罪訊息傳遞，或是採用網頁瀏覽器私密瀏覽(Private Browsing)功能進行網頁資料存取(Stefan & Felix 2011)，此類技術造成數位證據不會留存於非揮發性儲存媒體當中，鑑識人員必須深入分析主記憶體等揮發性儲存媒體，才能獲得有效之數位證據。

本研究在 Windows 作業系統架構下，先對主記憶體中數位證據之採證及分析方法進行深入探討，並整合相關數位鑑識工具，開發針對主記憶體中之數位證據自動採證及分析工具，再以案例來驗證該工具的可行性與有效性，期能幫助鑑識人員在進行主記憶體鑑識時，能減少採證程序產生之錯誤並強化主記憶體分析深度。

貳、文獻探討

近年來電腦犯罪案件日趨嚴重，且犯罪手法更呈現了多樣性的變化，為了維護資訊安全並對於電腦犯罪之行為加以遏止，必須從各類儲存媒體中擷取關鍵之數位證據，進而將犯罪者繩之以法。

本研究蒐集國內外相關文獻，探討數位鑑識相關理論與執行方法，藉以對研究之問題有一架構性的瞭解，以作為本研究參考之依據。

一、數位鑑識

數位鑑識是指以科學及嚴謹的程序，在儲存媒體中查找與犯罪行為相關之數位證據(Wikipedia 2011)，國外學者 Endicott 認為：「數位鑑識主要在保存及發掘數位證據，以證明犯罪行為並且能起訴其犯罪活動。」(Endicott-Popovsky & Frincke 2006)，而國內學者林宜隆則認為：「數位鑑識之目的是在於如何於蒐證過程中，確保數位證據之不可否認性與完整性，使數位證據具有絕對證據能力，而能成為呈堂證據」(林宜隆 2010)。

數位鑑識應包含資訊科技技術、鑑識程序管理與法律相關議題三個構面(鄭進興 2003)，分述如下：

(一)資訊科技技術：

數位鑑識所分析之標的物，均以儲存媒體中的電子數位資料為主，而該類電子數位資料均以 0 或 1 的型式存在，要將這些數位資訊解析成可理解、感知的訊息，必須藉由相關的資訊科技技術輔助。

(二)鑑識程序管理：

正確的鑑識程序管理，可確保採證、分析及鑑定的數位證據具有法律效力，由於數位證據具有產製者難以確定等特性，數位鑑識過程中要如何採證、分析及呈現都應依循訂定之程序進行，如此即可避免數位鑑識作業時，因鑑識人員的疏忽而造成數位證據遭受破壞。

(三)法律相關議題：

數位鑑識所獲得之數位證據，將來有可能成為司法審理的重要證據，因此所有的鑑識行為必須符合法令規定，否則所獲得之數位證據將失去其證據力。

數位鑑識是一門能夠幫助解決電腦犯罪案件的科學，因此必須以周延的方法及程序保存、識別、抽取、記載及解讀數位媒體證據與分析其成因(楊鴻正 2003)，其最終目的是保留數位證據的完整性和正確性，以作為司法審理單位之判決依據。

二、數位證據

「數位證據」一詞出自於「Digital Evidence and Computer Crime」一書，是指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，也就是在儲存媒體上以電磁紀錄方式儲存可供佐證犯罪之資料，包括有文字、圖片、聲音、影像等型態(Casey 2000)。數位證據在蒐證上為確保其證據之有效性，需應用並結合電腦科學與鑑識科學兩個領域的專業技術，其中電腦科學提供了電腦基本常識及技術來處理數位證據，而鑑識科學則提供了處理傳統證據的方法與步驟，結合這兩項專業知識後，鑑識人員才具備有數位證據蒐證及分析之能力。

數位證據是由電子數位資料所組成，其無法以人的知覺直接認知，必須經由特定的裝置加以解讀其內容，具有如下之特性：

(一)無法以感官知覺直接理解：

數位證據是無法經由人的感官知覺直接理解訊息，以電子郵件為例，信件內容所顯示之畫面是經過轉碼編譯後所呈現之結果，若檢視信件原始檔則多為一長串指令及編碼，因此數位證據除了須利用顯示裝置輸出顯示之外，也須透過適當的編譯程式解譯後始得從感官知覺直接理解(劉秋伶 2010)。

(二)無限複製及無差異複製：

數位證據與一般證據不同，具有無限複製及無差異複製等特性，數位證據可以透過作業系統指令，或者軟體工具無限制產生與正本一致的複本，而產生之複本與正本在內容不會有任何的差異，此特性跟傳統證據有著截然不同的特性，如傳統紙本證據雖然也具有可複製特性，但是複製後無論紙張、墨水等條件必然與正本有所不同，難以達到數位證據正、複本無差異的特性(邱獻民 2007)。

(三)復原之可能性：

由於檔案系統之特性，使得數位證據具有可復原性，當使用者刪除數位證據檔案時，檔案系統往往並未將檔案完全從儲存媒體中刪除，而只是將該筆檔案標註為已刪除，由於實際上檔案還存在於儲存媒體中，尚未被其他檔案覆蓋，所以透過軟、硬體設備的運用，即能將該數位證據檔案復原(馬林 2009)。

(四)產製者不確定性：

由於數位證據具有無限複製及無差異複製的特性，所以在數位鑑識中，要以數位證據內容來確認產製者實屬不易，仍需要透過其他相關事實或電腦系統相關資訊之輔助，始得加以確定產製者，故鑑識人員在鑑識時須做最完善之考量，收集最完整之資料，以避免造成證據力不足之結果(王旭正 2006)。

三、揮發性數位證據

在傳統的數位鑑識調查中，如調查物件為電腦，鑑識人員通常將欲鑑識之電腦關閉電源，然後再開始進行非揮發性儲存媒體(如硬碟)的採證動作，此種方式所採集到的資料為靜態非揮發性質的數位證據，然而，一個執行中的作業系統，事實上還存有其他揮發性的動態資料，例如主記憶體執行中的程序資訊、網路資訊及暫存的應用程式紀錄等，此種資料即稱之為揮發性數位證據(Carvey 2009)。揮發性數位證據的特性可以區分為以下幾點：

(一)易變性：

揮發性數位證據隨時均在變動，如何有效採集揮發性數位證據以避免揮發性數位證據的變動，這是鑑識人員最大的挑戰之一(Carvey 2009)，學者 Brezinski 與 Killalea 所撰寫的 RFC3227 文件指出，鑑識人員在採集數位證據前應就各類數位證據的揮發性等級加以了解，並訂定針對揮發性數位證據的鑑識程序(Brezinski & Killalea 2002)。

(二)不易採集：

儲存於主記憶體當中之揮發性數位證據，需要透過專業的採證設備或軟體才能完整保存(Maclean 2006)，由於每次案件的屬性可能有所不同，鑑識人員在面對不同案件時所需採集的揮發性數位證據也可能有所差異，往往鑑識人員的一個錯誤採證動作，即可能造成揮發性數位證據的消失或導致無證據能力(Farmer & Venema 2006)，有鑑於此，鑑識人員應使用自動化之採證工具，以減少採證時的錯誤發生(Beebe 2009)。

(三)不易分析：

在分析儲存於主記憶體中的揮發性數位證據時，必須先解析其檔案結構，主記憶體檔案結構皆因 Windows 作業系統版本不同而有所差異(Naja 2008)，此外，如何擷取主記憶體中的各類運行資訊，也因應用程式的不同而有所變化(Stefan & Felix 2011)，這些問題使得鑑識人員在分析上，需要更多的時間和技術能量，才能有效擷取所需之揮發性數位證據。

(四)易消逝：

由於揮發性儲存媒體必須仰賴電源進行運作，所以當關閉電源時，揮發性儲存媒體中之揮發性數位證據會隨即快速的消逝(Kleiman et. al. 2007；錢世傑 2004)，鑑識人員必須了解，揮發性數位證據消逝後即無法再回復，所以在處理相關案件時，鑑識人員應該視案件情況盡可能的採集揮發性數位證據，以免遺失重要之關鍵資訊。

四、主記憶體鑑識方法介紹

主記憶體鑑識方法於 2005 年 DFRWS(Digital Forensic Research Workshop)研討會開始被探討，迄今各種主記憶體採證、分析方法也越趨成熟，本節彙整目前主記憶體之採證、分析方法，以下分別介紹：

(一)主記憶體採證方法之介紹

在實務上已有很多方法可針對主記憶進行採證動作，鑑識人員應該了解各種採證方法之優缺點，進而在採證時選擇最合適的方法作業，有關主記憶體採證之方法如下所述：

1.使用作業系統內建工具採證：

在開機的作業系統中，使用該系統內建之命令列工具，直接針對主記憶體中資料進行截取作業，例如使用「tasklist」指令，即可針對目前作業系統執行之程序進行查看，此方法可以快速地進行採證作業，但鑑識人員必須衡量作業系統內工具之正確及有效性(Cameron 2009)。

2.使用作業系統運作機制採證：

利用微軟作業系統 BSoD Crash Dump 機制來進行主記憶體轉存(Microsoft 2011)，此方法可以瞬間暫停作業系統運作，進而完整採集主記憶體內資料，但採用此方式轉存前必須先行設定登錄檔參數，且轉存會在電腦硬碟內寫入與主記憶體相同大小之 Crash 映像檔，所以此方式並不能減少採證調查時的採證足跡留存。

3.使用鑑識工具採證：

鑑識人員使用相關鑑識工具進行主記憶體之採證，比如國內鑒真數位公司所開發的 LiveDector 工具(iForensic 2011)，該工具為自動化主記憶體採證工具，使用此類工具可快速進行主記憶體採證作業，但須注意的是，此類圖形化介面之採證工具有可能會留下較多之採證足跡於主記憶體中。

4.利用 IEEE1394 設備採證：

利用 IEEE1394 設備 DMA(Direct Memory Access)機制直接存取主記憶體(Freddie 2010)，此方式可不透過 CPU 而直接存取系統主記憶體，使得鑑識人員可以快速不留足跡的執行主記憶體採證動作，但並非所有主機均配備 IEEE1394 設備，故此方法會形成採證上的限制。

5.虛擬系統特有之採證：

如果欲採證之的系統為 VMWare 軟體之虛擬作業系統，則可利用 VMWare 軟體的操作選項「suspend」(VMWare 2010)來暫停該作業系統的執行，此時 VMWare 會將虛擬系統中的主記憶體轉存為.vmem 檔案，此檔案為 DD(Data dumper)格式之主記憶體映像檔，鑑識人員可從此檔案中取得相關揮發性數位證據(Cal et. al. 2008)，利用此種方式可以非常便捷快速的取得主記憶體映像檔，唯僅限於虛擬系統上作業，亦形成採證上的限制。

(二)主記憶體分析方法介紹

在作業系統運行時，鑑識人員可以使用系統內建工具，或其他鑑識工具來查看運行中主記憶體之內容，例如使用 Windows 作業系統中 ipconfig 指令，即可從主記憶體當中取得網路 IP 資訊，該類資訊鑑識人員可直接分析解讀，但如果是分析採證後所取得之

主記憶體映像檔，則相對困難許多，目前分析的方法主要為透過尋找主記憶體中的特定字串來擷取各種可辨識資訊，例如透過分析主記憶體中的 EProcess 標頭資訊(DISPATCHER_HEADER)，將程序(Process)資訊解譯出來(Schuster 2006)，利用此類方法，鑑識人員可以尋找存在於主記憶體中的證據資訊，但如何快速有效地進行主記憶體中關鍵證據之擷取，則是目前鑑識人員還需研究的方向之一(Beebe 2009)。

參、研究方法與工具架構

由於揮發性數位證據具有不易採集、不易分析之特性，鑑識人員在採證時必須清楚每一個步驟對於主記憶體的影響，例如鑑識人員所使用的鑑識工具會被作業系統讀取至主記憶體中，進而改變主記憶體的內容，因此在針對主記憶體採證時，應該先針對主記憶體進行完整的複製，並且詳細記錄每一個採證行為，才能在將來解釋這些採證足跡對主記憶體所造成之變化。另外，主記憶體內資料結構隨者 Windows 作業系統版本及執行程式的不同而有所差異，鑑識人員必須運用各種鑑識手法及工具來分析主記憶體，方能快速有效的擷取主記憶體中之數位證據。

一、研究工具所採用之主記憶體採證方法

擷取主記憶體內之揮發性證據必須透過專業的鑑識工具來達成，但這些鑑識工具的使用，必然會造成主記憶體內的資料改變，例如鑑識人員執行鑑識工具時，作業系統就會移動某些主記憶體空間，供鑑識工具所使用。因此本研究以命令列鑑識工具(Command line Interface)為主要參考工具，命令列的鑑識工具相較圖形介面(Graphical User Interface)之鑑識工具佔用較少的主記憶體空間，可以對主記憶體內容的影響降到最低，另外，命令列鑑識工具通常不需運用作業系統中之動態連結檔(DLL)，亦減少了採證時對於作業系統的足跡留存。

使用命令列鑑識工具除了對主記憶體影響較少之外，也較容易配合批次檔或 Script 來進行自動化的處理，如果使用圖形化介面的工具，則很難將各種工具進行統合性的自動化作業，故本研究採用 MoonSols Windows Memory Toolkit 中 Windd32(MoonSols 2011)搭配 Microsoft Sysinternals pslist(Microsoft 2010)等工具做為主記憶體之採證工具。

二、研究工具採用之主記憶體分析方法

採證後之主記憶體檔案結構複雜，需要另外加以分析，才能成為可判讀且有效之數位證據，本研究使用之主記憶體分析方法包含以下幾種方式：

(一)利用特殊字串重組訊息

由於主記憶體中存放的部份數據為明文類型，因此，可利用 Microsoft Sysinternals 所開發的 strings(Microsoft 2011)工具來對主記憶體證映像檔進行 ASCII 或 Unicode 字串的匯出，匯出之後的資訊如圖 1，接下來鑑識人員可以利用 Gnuwin32 sed(Gnuwin32 2010)配合相關參數進行特殊字串重組動作，此分析方法可以幫助鑑識人員快速的分析出關鍵證據，唯須把找到的特殊字串重組起來成為有意義之訊息，具有一定之困難度，故本研究目前只針對 Google Talk(SSL 網頁版)即時通訊程式(Wikipedia 2012)、TrueCrypt 加密程式(TrueCrypt 2012)進行特殊字串重組動作。

```
85739552:Norton AntiVirus
85739586:SPLATITUDE
85739616:Symantec AntiVirus Realtime Protection Loaded.
85739772:Norton AntiVirus
85739806:SPLATITUDE
85739836:Symantec AntiVirus services startup was successful.
85740004:EAPOL
85740016:SPLATITUDE
```

圖 1 主記憶體中字串

(二)彙整可識別字串

通常鑑識人員在面對各類案件進行鑑識時，均會有相關的鑑識目標或方向，如果鑑識目標為尋找關鍵文字或字串，可利用 X-Ways Forensics(X-Way 2012)等鑑識工具來搜尋既定的關鍵字串或是關鍵檔案名稱，例如搜尋已知網卡卡號(MAC)後檢視前後字串，可能會發現該系統使用之 IP、DNS 等訊息，如圖 2，本研究使用 Microsoft Sysinternals strings 工具彙整主記憶體中可識別之字串，方便鑑識人員進行關鍵字串之搜尋作業。

```
6947546A  20 00 20 00 20 00 20 00  20 00 20 00 20 00 50 00  68                 P h
6947547B  00 79 00 73 00 69 00 63  00 61 00 6C 00 20 00 41  00  .y.s.i.c.a.l. .A.
6947548C  64 00 64 00 72 00 65 00  73 00 73 00 2E 00 20 00  2E  d.d.r.e.s.s... ..
6947549D  00 20 00 2E 00 20 00 2E  00 20 00 2E 00 20 00 2E  00  . ... ... ... ...
694754AE  20 00 2E 00 20 00 2E 00  20 00 2E 00 20 00 3A 00  20   ... ... ... .:.
694754BF  00 30 00 30 00 2D 00 35  00 30 00 2D 00 35 00 36  00  .0.0.-.5.0.-.5.6.
694754D0  2D 00 43 00 30 00 2D 00  30 00 30 00 2D 00 30 00  31  -.C.0.-.0.0.-.0.1
694754E1  00 20 00 20 00 20 00 20  00 20 00 20 00 20 00 20  00  . . . . . . . .
694754F2  20 00 20 00 20 00 20 00  20 00 20 00 20 00 20 00  20   . . . . . . . .
69475503  00 20 00 20 00 20 00 20  00 20 00 20 00 20 00 20  00  . . . . . . . .
69475514  20 00 20 00 44 00 68 00  63 00 70 00 20 00 45 00  6E   . .D.h.c.p. .E.n
69475525  00 61 00 62 00 6C 00 65  00 64 00 2E 00 20 00 2E  00  .a.b.l.e.d... ...
69475536  20 00 2E 00 20 00 2E 00  20 00 2E 00 20 00 2E 00  20   ... ... ... ...
69475547  00 2E 00 20 00 2E 00 20  00 2E 00 20 00 2E 00 20  00  ... ... ... ... .
69475558  2E 00 20 00 3A 00 20 00  4E 00 6F 00 20 00 20 00  20  .. .:. .N.o. . .
69475569  00 20 00 20 00 20 00 20  00 20 00 20 00 20 00 20  00  . . . . . . . .
6947557A  20 00 20 00 20 00 20 00  20 00 20 00 20 00 20 00  20   . . . . . . . .
6947558B  00 20 00 20 00 20 00 20  00 20 00 20 00 20 00 20  00  . . . . . . . .
6947559C  20 00 20 00 20 00 20 00  20 00 20 00 20 00 20 00  20   . . . . . . . .
694755AD  00 20 00 20 00 20 00 20  00 20 00 49 00 50 00 20  00  . . . . . I.P. .
694755BE  41 00 64 00 64 00 72 00  65 00 73 00 73 00 2E 00  20  A.d.d.r.e.s.s...
694755CF  00 2E 00 20 00 2E 00 20  00 2E 00 20 00 2E 00 20  00  ... ... ... ... .
694755E0  2E 00 20 00 2E 00 20 00  2E 00 20 00 2E 00 20 00  2E  .. ... ... ... ..
694755F1  00 20 00 2E 00 20 00 2E  00 20 00 3A 00 20 00 31  00  . ... ... .:. .1.
69475602  39 00 32 00 2E 00 31 00  36 00 38 00 2E 00 33 00  30  9.2...1.6.8...3.0
69475613  00 2E 00 31 00 20 00 20  00 20 00 20 00 20 00 20  00  ...1. . . . . .
```

圖 2 關鍵字搜尋結果

(三)比對資料結構並還原檔案

從主記憶體中比對常見的檔案資料結構(標頭標尾)，並利用還原軟體將主記憶體中可識別之檔案擷取出來，此方法可以檢視作業系統或使用者所存取之相關檔案，本研究使用 Cygwin Foremost(Cygwin 2009)針對主記憶體進行檔案還原作業，下圖 3 為 Cygwin Foremost 從主記憶體中還原出一筆圖示檔案。

圖 3 比對資料結構後還原之檔案

(四)解析主記憶體中檔案結構

透過主記憶體中之頁目錄、頁表項以及特定字串，可擷取作業系統執行之程序、網路連結狀態、系統資訊等訊息，此種方法解析出的資訊非常詳盡且易於識別，本研究採用 Volatility framework(Volatility 2012)鑑識工具將主記憶體中程序、網路通訊等資訊列出，如圖 4。

PPID	Time created	Time exited	Offset	PDB	Remarks
0			0x00558e80	0x00039000	Idle
3352	Mon Jul 04 18:24:00 2005		0x013383b0	0x19d19000	PluckTray.exe
2392	Mon Jul 04 18:21:11 2005		0x0133d810	0x1ebc8000	firefox.exe
2392	Mon Jul 04 18:18:06 2005		0x01462be0	0x185c5000	VPTray.exe
2300	Mon Jul 04 18:18:03 2005		0x0146e860	0x17b7f000	explorer.exe
800	Mon Jul 04 18:19:11 2005		0x01474510	0x1c1b5000	wuauclt.exe
3352	Mon Jul 04 18:24:30 2005	Mon Jul 04 18:26:44 2005	0x01488350	0x1bb44000	PluckUpdater.ex
2392	Mon Jul 04 18:18:15 2005		0x014b8a58	0x1972e000	WZQKPICK.EXE
400	Mon Jul 04 18:17:29 2005		0x014dc020	0x0dec3000	winlogon.exe
2392	Mon Jul 04 18:18:07 2005		0x014ecc00	0x18962000	jusched.exe
524	Mon Jul 04 18:17:31 2005		0x014f0020	0x0e7b3000	svchost.exe
524	Mon Jul 04 18:17:40 2005		0x01521da0	0x12701000	DefWatch.exe
480	Mon Jul 04 18:17:30 2005		0x015221c8	0x0e0de000	services.exe
524	Mon Jul 04 18:17:39 2005		0x0152f9a0	0x1230c000	ati2evxx.exe
524	Mon Jul 04 18:17:33 2005		0x01530228	0x102d8000	svchost.exe
524	Mon Jul 04 18:17:34 2005		0x01534c10	0x1046f000	svchost.exe
2392	Mon Jul 04 18:20:58 2005		0x0153f480	0x1e8a0000	cmd.exe
2392	Mon Jul 04 18:18:05 2005		0x01540da0	0x184c5000	TaskSwitch.exe
3256	Mon Jul 04 18:30:32 2005		0x01543870	0x18a36000	dd.exe

圖 4 解析主記憶體後之程序列表

三、自動化主記憶體鑑識工具開發

本研究結合上述採證、分析方法後開發出自動化主記憶體鑑識工具 Windows Memory Tools(以下簡稱 WMTS)，本工具整合相關之 Command line 鑑識工具，可針對 Windows 作業系統架構下之主記憶體，進行自動化的採證及分析作業，最後再產出可供鑑識人員快速瀏覽之報表，採證及分析項目如表 1。

表 1 WMTS 採證分析項目一覽表

採證項目	
1	主記憶體
2	作業系統日期時間
3	登錄作業系統之使用者訊息
4	使用者開啟之文件及檔案
5	網路連接訊息
6	作業系統程序執行訊息
7	作業系統服務執行訊息
8	作業系統驅動程式執行訊息
9	作業系統暫存訊息(剪貼簿等)
分析項目	
1	作業系統曾經執行之程序訊息
2	作業系統曾經執行之網路訊息
3	作業系統曾經執行之服務訊息
4	通訊軟體(IM)帳號密碼
5	通訊軟體(IM)通聯紀錄
6	加密軟體使用之密碼
7	檔案文件還原

鑑識人員可以將 WMTS 放入隨身碟或 CD-ROM 之中進行採證作業，而採證完畢後，WMTS 的分析作業及報表製作是由後端鑑識分析主機來產出，而非直接於案件電腦上進行分析作業，此方法可以有效降低鑑識流程中案件電腦上的鑑識痕跡，WMTS 運作流程如圖 5。

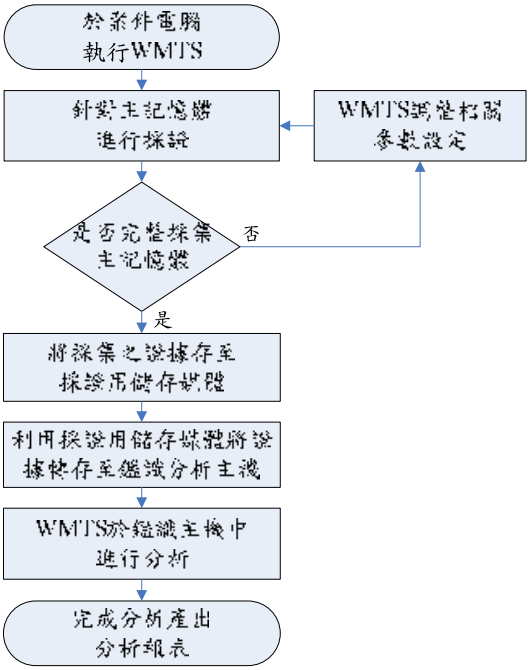

圖 5 WMTS 運作流程圖

首先將存有 WMTS 之 USB 或 CD-ROM 放入欲採證之案件電腦中，執行後 WMTS 會依據預先設計之採證程序，自動採集案件電腦主記憶體及主記憶體內之數位證據，採證完畢後，鑑識人員將採集之數位證據轉存至鑑識分析主機，WMTS 於鑑識分析主機上繼續執行後續鑑識分析作業，分析完成後將會產出分析結果報表，以幫助鑑識人員判讀主記憶體內證據資訊，WMTS 分析後之報表如圖 6。

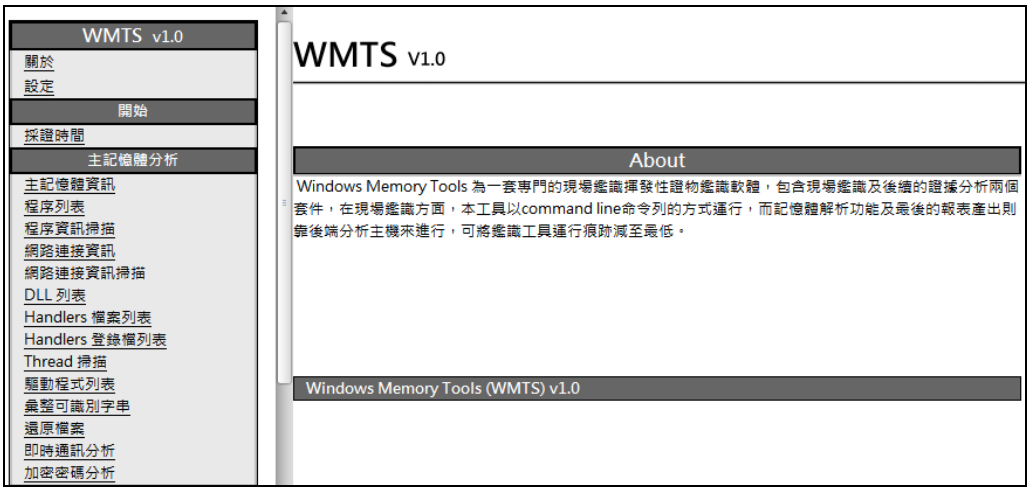

圖 6 WMTS 分析工具產出之報表

肆、模擬案件實作

本研究在第三章中，已分別探討主記憶體之採證及分析方法，並開發 WMTS 自動化主記憶體鑑識工具，本章節將以模擬案件方式實作，以驗證 WMTS 對於主記憶體鑑識之幫助。

一、個案說明

警方經線報通知查獲了某販毒集團，在搜查中發現桌上型電腦乙台(以下簡稱案件電腦)，由於該案件電腦為開機運行中，鑑識人員立即使用 WMTS 來針對案件電腦進行採證動作，採證動作完畢後隨即將案件電腦扣押，該案件電腦的硬體清單如表 2。

表 2 案件電腦硬體一覽表

1	主機板	MSI 770-C45
2	處理器	AMD Phenom II X2 550
3	主記憶體	創建 DDR3 2GB*2
4	顯示卡	Radeon HD 6450
5	硬碟	WD 640GB
6	網路卡	Intel 10/100 MB

在此案例中，由於查察時案件電腦為開機運行中，故警方採用 WMTS 來針對案件電腦進行主記憶體採證動作，採證完畢後，再交由實驗室中的鑑識分析主機進行進一步的分析，各種鑑識案件中都有主要的鑑識目的，在該案例中，警方需要找尋販毒集團與

其餘同夥之通聯記錄，以及其販毒帳冊，在確認鑑識目的後，警方開始執行後續分析動作。

二、主記憶體鑑識實作

在一般數位鑑識中，鑑識人員通常可以從非揮發性的儲存媒體(如硬碟)內找尋到關鍵證據，例如快速辨識出安裝之作業系統、應用程式，再進而過濾出可能的證據訊息，在該案例中，鑑識人員利用非揮發性儲存媒體分析出之作業系統及應用程式資訊如下表3。

表 3 案件電腦軟體一覽表

1	作業系統	Microsoft Windows 7 x86
2	瀏覽器 1	Internet Explorer 9
3	瀏覽器 2	Firefox 10
4	文書軟體	Microsoft Office 2010
5	加密軟體	TrueCrypt 7.1a
6	防毒軟體	Avast! 2012
7	壓縮軟體	WinRAR 3.60

有了初步的作業系統及應用程式資訊後，鑑識人員在非揮發性儲存媒體中卻沒有分析出販毒集團之通聯記錄、販毒紀錄等關鍵性證據，鑑識人員研判犯罪者可能使用隱匿性即時通訊軟體，或針對相關檔案進行加密處理，為了尋找更多有效證據，鑑識人員進而朝向主記憶體鑑識的查察方向前進。

(一)使用軟體之確認

首先開啟 WMTS 分析後產出之報表，在報表「主記憶體分析」>「程序列表」項中可呈現該案件電腦於關機前所執行之程式清單，如圖 7，其中並無發現使用即時通訊應用軟體程序，較值得注意的是網頁瀏覽器 firefox.exe 正執行中，由於網頁瀏覽器可執行多種網頁版即時通訊程式，故鑑識人員針對此程序特別留意，另外也看到加密程式 TrueCrypt.exe 執行於系統中，顯見犯罪者很有可能將重要檔案進行加密處理。

0x8e331030	spoolsv.exe	1288	476	12	270	2012-03-13 08:06:11
0x8e34e7a0	svchost.exe	1320	476	19	297	2012-03-13 08:06:11
0x8e3a0030	svchost.exe	1432	476	15	246	2012-03-13 08:06:12
0x8e480d40	SearchIndexer.	1908	476	11	666	2012-03-13 08:06:20
0x8e5034c0	sppsvc.exe	1152	476	4	149	2012-03-13 08:06:31
0x8d3c3b38	LogonUI.exe	468	380	6	171	2012-03-13 08:06:46
0x8c7398f8	svchost.exe	1780	476	13	360	2012-03-13 08:08:17
0x8e34b8f0	taskhost.exe	1028	476	11	321	2012-03-13 08:09:11
0x8d2fa748	taskhost.exe	3304	476	8	201	2012-03-13 08:34:03
0x8d2eb518	dwm.exe	3420	812	3	66	2012-03-13 08:34:04
0x8d2c5d40	explorer.exe	3396	3360	27	915	2012-03-13 08:34:05
0x8ce47220	wuauclt.exe	3968	868	3	89	2012-03-13 08:34:18
0x8de37030	wmpnetwk.exe	4084	476	10	221	2012-03-13 08:34:21
0x8d2a2030	firefox.exe	1608	3396	26	370	2012-03-13 08:35:19
0x8c7e1328	TrueCrypt.exe	1880	3396	1	62	2012-03-13 09:51:02
0x8d449198	audiodg.exe	2432	720	4	113	2012-03-13 09:51:21

圖 7 案件電腦執行程式清單

(二)通訊軟體之分析

在懷疑犯罪者可能使用網頁版即時通訊軟體後，即可開啟 WMTS 報表中「主記憶體分析」>「即時通訊分析」項來查看是否有其相關通聯紀錄，點選後可看到案件電腦曾經執行過網頁 SSL 版 Google Talk 軟體通聯紀錄，以及使用之帳號密碼，如圖 8。

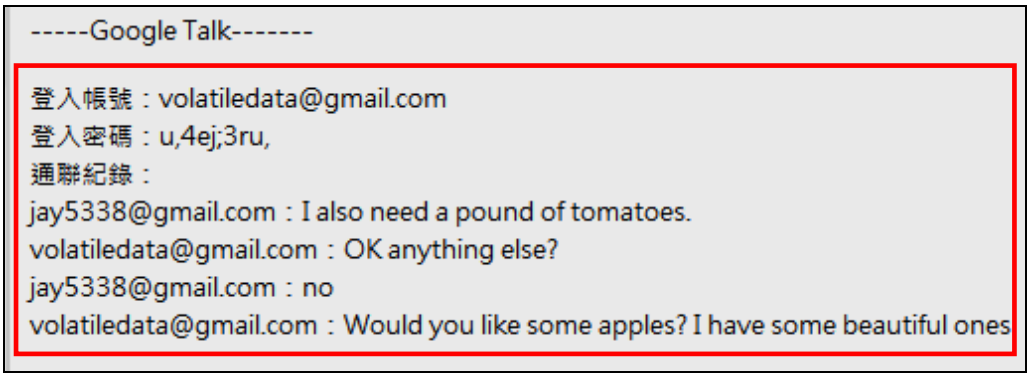

圖 8 Google Talk 通聯紀錄及其使用帳號密碼

(三)加密軟體分析

在確定犯罪者有執行加密程式 TrueCrypt.exe 後，可開啟 WMTS 工具報表中「主記憶體分析」>「加密密碼分析」項來查看是否有其相關加密資訊，點選報表後可看到 TrueCrypt.exe 加密程式之加密密碼，如圖 9，尋獲密碼後即可解密其加密檔案或磁區，如圖 10 解密出關鍵之販毒帳冊。

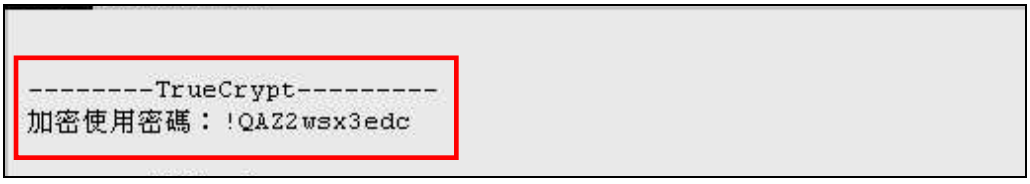

圖 9 TrueCrypt.exe 加密程式使用之加密密碼

項次	日期	種類	購買重量	客戶	google talk帳號	電話	金額	備考
1	20120105	鴉片	500K	D哥	David110110@gmail.com	0910110110	50000	
2	20120105	嗎啡	1000K	C哥	Criss110110@gmail.com	0911110110	2000	
3	20120105	海洛英	800K	X哥	Xenos110110@gmail.com	0913110110	60000	
4	20120105	古柯鹼	1000K	A哥	Abdiel110110@gmail.com	0914110110	100000	欠1000
5	20120110	鴉片	500K	D哥	David110110@gmail.com	0910110110	50000	
6	20120118	嗎啡	1000K	C哥	Criss110110@gmail.com	0911110110	2000	
7	20120119	海洛英	800K	X哥	Xenos110110@gmail.com	0913110110	60000	
8	20120119	古柯鹼	1000K	A哥	Abdiel110110@gmail.com	0914110110	100000	
9	20120119	鴉片	500K	D哥	David110110@gmail.com	0910110110	50000	
10	20120119	嗎啡	1000K	C哥	Criss110110@gmail.com	0911110110	2000	
11	20120124	海洛英	800K	X哥	Xenos110110@gmail.com	0913110110	60000	
12	20120124	古柯鹼	1000K	A哥	Abdiel110110@gmail.com	0914110110	100000	
13	20120124	鴉片	500K	D哥	David110110@gmail.com	0910110110	50000	
14	20120125	嗎啡	1000K	C哥	Criss110110@gmail.com	0911110110	2000	

圖 10 解密後之販毒帳冊

三、分析與討論

經由模擬案件實作結果可以發現，WMTS 可以有效的針對主記憶體進行自動化採證及分析，並且可產出便於鑑識人員快速瀏覽之分析報表，有效的減少鑑識人員於採證時所產生的錯誤以及強化其分析深度，另外，在網際網路應用越來越廣泛的情況下，有越來越多應用程式在執行時，不會留存相關執行足跡於非揮發性儲存媒體之中，如何從揮發性儲存媒體當中尋找所需之數位證據，是鑑識人員後續研究的課題之一。

伍、結論

電腦犯罪手法層出不窮，除了加強各種資安防護措施之外，在案件發生後如何有效的進行採證、分析及呈現數位證據，亦是當前鑑識人員的主要目標之一，經由本研究可了解在 Windows 作業系統架構下，主記憶體中之數位證據採證及分析方法，並證明所使用的方法可協助鑑識人員處理相關之電腦犯罪案件。

鑑識人員在執行採證任務時，常因對鑑識工具操作的不熟悉，導致採證過程中可能遺失重要的數位證據，甚至因錯誤動作造成證明能力與證據力之問題，本研究整合之自動化 WMTS 主記憶體鑑識工具，可簡化採證流程及降低鑑識人員在採證過程中可能發生之錯誤，另外也加強了鑑識分析之深度，在犯罪案件發生的第一時間幫助鑑識人員取得所需的關鍵數位證據。

參考文獻

1. 王旭正、柯宏叡，2006，資訊與網路安全　秘密通訊與數位鑑識新技法，台北：博碩文化出版社。
2. 林宜隆，2010，『網路釣魚之 iPhone 數位證據鑑識標準作業程序』，台灣電腦網路為機處理暨協調中心，電子報第 6 期。
3. 邱獻民，2007，刑事數位證據同一性之攻擊與防禦，東吳大學法律學系碩士論文。
4. 馬林，2009，資料重現-檔案系統原理精解與資料恢復最佳實踐，台北：佳魁資訊。
5. 楊鴻正，2003，我國資通安全鑑識科技能量規劃之研究，中央警察大學資訊管理所碩士論文。
6. 劉秋伶，2010，數位證據之刑事證據調查程序，政治大學法律研究所碩士論文。
7. 鄭進興、林敬皇、沈志昌、吳豐乾，2003，『電腦鑑識工具之研究』，行政院國家科學委員會專題研究計畫，樹德科技大學資訊管理學系。
8. 錢世傑、錢世豐、劉嘉明、張紹斌，2004，電腦鑑識與企業安全，台北：文魁資訊。
9. Beebe, N., ”Digital Forensic Research: The Good the Bad and the Unaddressed” *IFIP Advances in Information and Communication Technology*, 2009, pp. 17-36.
10. Brezinski, D., Killalea, T., “Guidelines for Evidence Collection and Archiving”, RFC3227, 2002.
11. Cal, W., Joseph, A., Richard, N., and Larry, R., “Computer Forensics: Results of LiveResponse Inquiry vs. Memory Image Analysis”, August 2008.
12. Cameron, H., Eoghan, C., and James, M. Malware Forensics Investigating and Analyzing Malicious Code, Syngress, Burlington, 2009.
13. Carvey, H. Windows Forensic Analysis DVD Toolkit, Second Edition, Syngress, Burlington, 2009.
14. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computer and The Internet, Academic Press, Waltham, 2000.
15. Cygwin Foremost, August 2009 (available online at http://www.dcheeseman.com/blog/post/foremost-windows), Retrieved 2012/04/06.

16. Endicott Popovsky, B. , and Frincke, D. “Embedding Forensic Capabilities into Networks: Addressing Inefficiencies in Digital Forensics Investigations.”, *Information Assurance Workshop 2006 IEEE*, June 2006, pp. 133-139.
17. Farmer, D. , and Vanema, W. Forensic Discovery, Addison Wesley, Boston, 2006.
18. Freddie, W., ”Memory Forensics over the IEEE 1394 Interface” *Freddie Witherden*, September 2010(available online at https://freddie.witherden.org), Retrieved 2012/04/05.
19. Gunwin32 sed , December 2010 (available online at http://gnuwin32.sourceforge.net/packages/sed.htm), Retrieved 2012/04/04.
20. iForensic LiveDector, April 2012 (available online at http://www.iforensics.com.tw/Products), Retrieved 2012/04/05.
21. Kleiman, D., Cardwell, K., Clinton, T., Cross, M., Gregg, M., Varsalone, J., and Wright, C. The Official CHFI Study Guide (Exam 312-49): for Computer Hacking Forensic Investigator, syngress, Burlington, 2007.
22. Maclean, N.“Acquisition and analysis of windows memory” *Forensic Informatics 2006*, April 2006.
23. Microsoft Crash Dump, May 2011 (available online at http://support.microsoft.com/kb/244139), Retrieved 2012/04/06.
24. Microsoft Sysinternals pslist, April 2010 (available online at http://technet.microsoft.com/en-us/sysinternals/bb896682), Retrieved 2012/04/05.
25. Microsoft Sysinternals strings, December 2011 (available online at http://technet.microsoft.com/en-us/sysinternals/bb897439), Retrieved 2012/04/04.
26. MoonSols Windows memory Toolkit Windd32 , February 2011 (available online at http://www.moonsols.com/windows-memory-toolkit), Retrieved 2012/04/03.
27. Naja, D., “Live Memory Acquisition for Windows Operating Systems”, Eastern Michigan University, 2008.
28. Schuster, A., ”Searching for processes and threads in Microsoft Windows memory dumps” *Digital Forensic Research Workshop 2006*, August 2006.
29. Stefan, Vo., and Felix, C,F., “A survey of main memory acquisition and analysis techniques for the windows operating system” *Digital Investigation, Volume 8*, July 2011.
30. TrueCrypt, February 2012 (available online at http://www.truecrypt.org), Retrieved 2012/04/06.
31. VMware, April 2012 (available online at http://www.vmware.com/support/ws55/doc/ws_learning_files_in_a_vm. html), Retrieved 2012/04/05.
32. Volatility Framework, April 2012 (available online at https://www.volatilesystems.com/default/volatility), Retrieved 2012/04/06.
33. Wikipedia, April 2012 (available online at http://en.wikipedia.org/wiki/Digital_forensics), Retrieved 2012/04/04.
34. Wikipedia, March 2012 (available online at http://en.wikipedia.org/wiki/Google_Talk), Retrieved 2012/04/05.
35. X-Way Forensics, April 2012 (available online at http://www.x-ways.net/forensics/index-m.html), Retrieved 2012/04/04.

Study on the Forensic Methods of Main Memory

Huei-Chung Chu
Department of Information Management
Huafan University
hcchu@cc.hfu.edu.tw

Chung Wen Kuei
Guo Ju Consultants Co
mark.chung@msa.hinet.net

Kuang-Chieh Yeh
Graduate Student, EMBA program
Huafan University
jay5338@gmail.com

Abstract

Along with the improvement of information technology and the popularization of IT education, the cybercrime cases are also on the increase. As the Internet enjoys a booming development, the digital evidences are not only stored in the non-volatile storage but also in the volatile storage ones. Consequently, it becomes an important subject for the forensic personnel to collect the digital evidences from the volatile storage medium especially in the main memory of computers.

This study deeply investigates the methods of collection and analysis for digital evidences in the main memory based on the structure of the Windows operating system. It also develops the automate tools for digital evidences collection and analysis in the main memory by integrating all related digital forensic tools. Finally, the feasibility and effectiveness of the proposed tool are testified by case study. It is hoped to help the forensic personnel reduce the errors caused by evidence collection programs and to intensify the analysis depth of digital evidences.

Keywords: Digital Forensic, Main Memory Forensic