Communications of the CCISA
Vol. 24 No. 3 Jul. 2018

暗網入口的軌跡：Security and Tor Forensics

邱黃明蓉[1]、王旭正[2*]
[1, 2] 中央警察大學 資訊管理學系
[1]im841225@mail.cpu.edu.tw、[2*]sjwang@mail.cpu.edu.tw

摘要

本文說明洋蔥路由的組成及運作，並利用案例實作，使用鑑識工具來進行相關實驗，了解藉由記憶體萃取分析，可以從中還原企圖者曾使用 Tor browser 所瀏覽的網頁，查看其是否有利用 Tor browser 進入非法網站，並藉此在未來藉由分析網路流量，以及 Registry 變化，可以更加確切得知企圖者的動機目的。

關鍵詞：洋蔥路由、記憶體萃取、Tor browser、網路流量、Registry

Key-windows of Evidence Investigations: Security and Tor Forensics

Ming Jung Chiu Huang[1], Shiuh Jeng WANG[2*]
[1, 2] Department of Information Management, Central Police University
[1] im841225@mail.cpu.edu.tw, [2*] sjwang@mail.cpu.edu.tw

Abstract

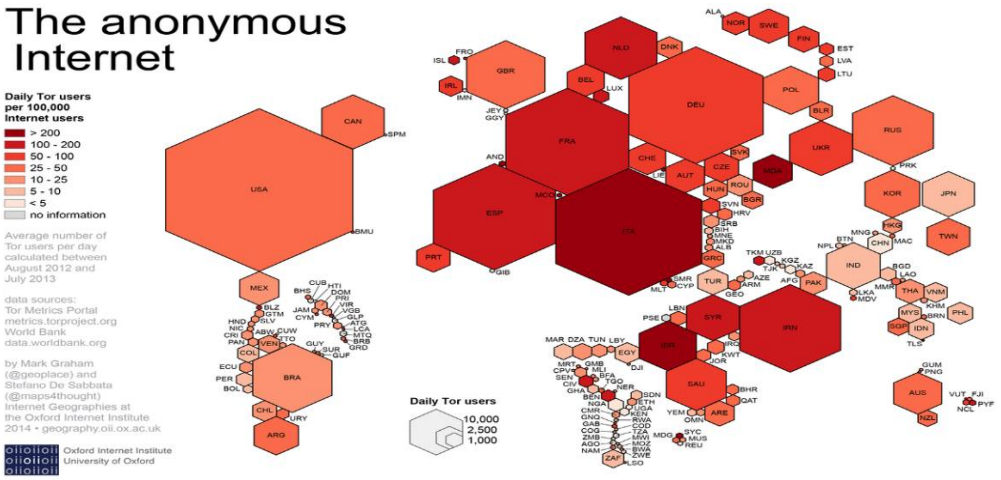
In this paper, we give the introductions of compositions and operations as to the onion router (Tor), firstly. Then there are several forensic tools conducted in forensic experiments, so as to realize the evidence investigations in the memory for extraction and analysis. In this way, we could reveal pages browsed by Tor browsers. According to our proposed method observed in the empirical experiments, we could perceive the criminals if accessing to illegal pages to commit the criminal facts. In our further plans, the analyses of network traffic and the changes of registry are going to be exploited to watch out the motivations of the criminal offense.

Keywords: the onion router, Tor browser, network traffic, registry

* 通訊作者 (Corresponding author.)

壹、前言

科技的急遽發展促使資安事件頻傳，諸如:銀行遭駭客盜領巨額款項等事件，使人心惶惶，深怕自己成為下一個受害者。然而，企圖者為避免遭受到追緝，會運用各種手法，讓自己在犯罪現場，盡可能地不留下行為跡證，以增加調查人員尋找跡證的難度，諸如：透過洋蔥路由器(The onion router, Tor)所提供的瀏覽器，簡稱洋蔥瀏覽器—Tor browser，即為企圖者用來隱藏身分及蹤跡的手法之一。由於 Tor 下載使用相當便利，故使用者範圍相當廣泛，小至一般民眾基於個人隱私需求的使用，大至國家的軍事用途使用，根據 Oxford Internet Institute 研究指出，全球 Tor 使用者分布如圖一所示。



圖一：全球 Tor 使用者分布圖

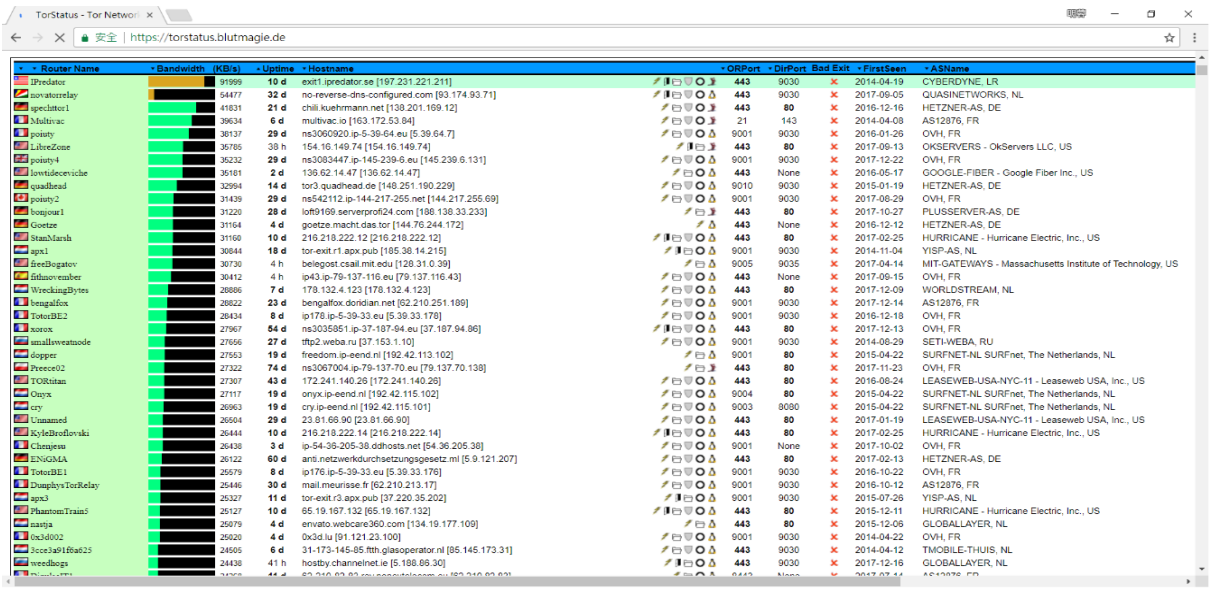
(資料來源: https://commons.wikimedia.org/wiki/File%3AGeographies_of_Tor.png)

由圖一可知，歐美地區的 Tor 使用者較多，且橫跨國際，更可由 TorStatus[9]得知目前的節點分布狀況，如圖二所示。因此 Tor 如此高度的使用率、廣大的分布，再加上回溯源頭困難的特性，無疑成為跨國網路犯罪的一大溫床。

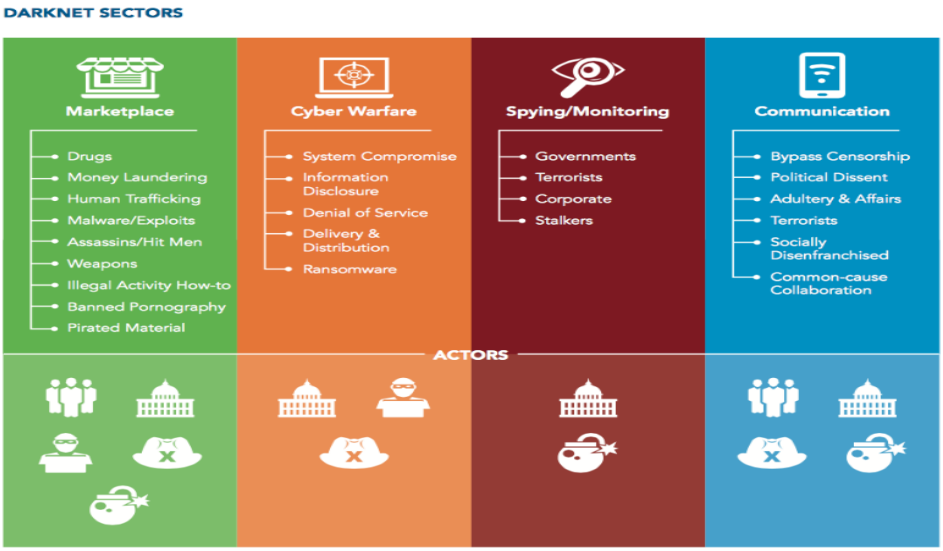
一般使用者可以透過使用 Tor，將自己的隱私資訊隱藏，想當然爾，駭客亦會運用此種特性，來隱匿自己的行蹤，增加數位鑑識人員調查的難度，各類型的網路犯罪也應運而生，最常見的莫過於暗網市場的非法交易，如毒品、槍械的黑市交易(暗網之非法行為詳見圖三)，著名的「絲綢之路」，即是以 Tor 網路作為非法交易市場。除此之外，殭屍網路(Botnet)利用 Tor 作為最有效的網路攻擊平台，以及勒索軟體(Wannacry)利用 Tor 作為支付贖金之方式等，眾多的犯罪應用，使 Tor 成為網路犯罪調查的一大重點。然而，根據路卡交換原理(Locard exchange principle)[10]，凡走過必留下痕跡，因此，越來越多的研究著重於 Tor 殘留跡證之分析，進而達到去匿名化的調查目的。

根據[4]所提出的暗網鑑識架構，將其分為兩大種類:Tor 鑑識與比特幣鑑識，會有如

此地區分，主要是因為企圖者可以利用 Tor browser 來進入暗網，再以比特幣作為金錢流，進行非法交易，本文我們將著重於 Tor 鑑識，利用數位鑑識工具，來對比出使用完 Tor browser 後，對於客戶端所造成的影響，進一步來取得證實企圖者有使用 Tor browser 進行非法行為的證據。



圖二：目前節點分布狀況



圖三：暗網藏有的非法行為(資料來源: Bat Blue, Special Report, 2015)

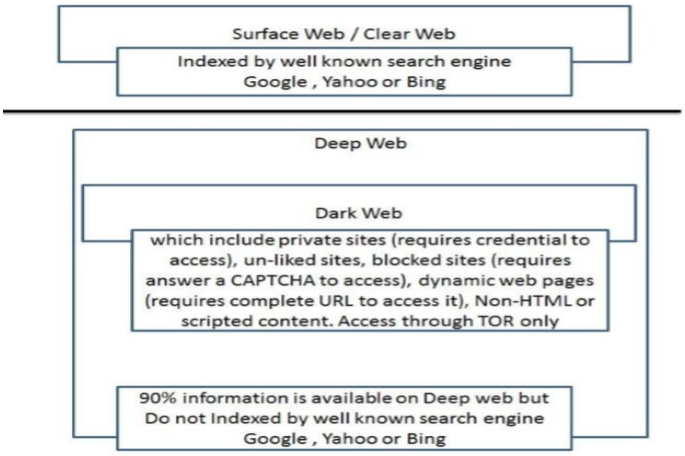
本文將於第二節說明相關之背景，第三節說明實驗之詳細步驟，第四節進行案例之實際運用，第五節為結論，第六節則為未來可研究之方向。

貳、背景知識

2.1 表層網、深網、暗網[4]

網際網路主要可以分為表層網，深網及暗網，根據[4]所介紹如下(見圖四)：

1. 表層網 (surface web)：即為日常生活中我們所能自由使用的網路，不須經過特別的軟體或組態設定，即可進入者，如:一般透過 Google 或 Yahoo 所瀏覽的網頁。
2. 深網 (deep web)：在深網中的內容，是無法被一般的瀏覽器所搜尋的。
3. 暗網 (dark web)：被包含在深網中，大多是一些需要憑證或授權的私人網站、動態網頁等並非自由開放給使用者使用的網站，僅能使用 Tor 才能進入。



圖四：網路分層類型

2.2 洋蔥路由的組成及運作：

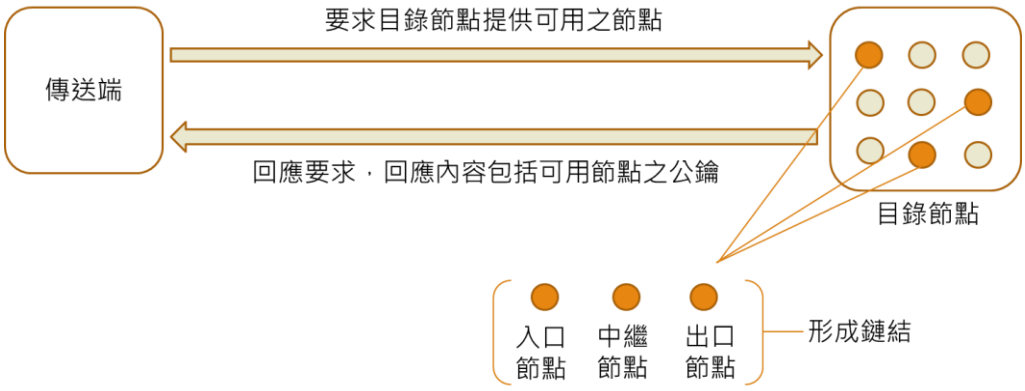
2.2.1 洋蔥路由的組成

1. 傳送端—originator 或 initiator
2. 接收端—responder
3. 目的端—destination
4. 目錄節點--directory node(s)

5. 鏈/線路—circuit / chain
6. 入口節點--entry node
7. 出口節點--exit node
8. 中繼節點--relay node(s)

2.2.2 洋蔥路由的運作

1. 命名緣由：在於訊息會經一層一層的非對稱式加密包裝後，形成類似洋蔥形狀的資料結構，其層數取決於到目的端中間會經過的節點數。
2. 每經過一個節點，會將封包加/解密，因此任一個節點都無法確切知道傳送端與目的端的位置，使發送者達到匿名的效果，根據[1]其過程可分為四大主要步驟，詳述如下：
   (1) 網路拓樸建立階段:確認網路拓樸已建立，相鄰的網路拓樸有提供長期且穩定的連線的環境。
   (2) 連結建立：
      A. 傳送端會由目錄節點所提供的節點目錄中選取一些節點(如：入口/中繼/出口節點)。
      B. 目錄節點同時也會傳送給傳送端，各個選取節點的公開金鑰，以利後續進行非對稱式加密使用，如圖五所示。



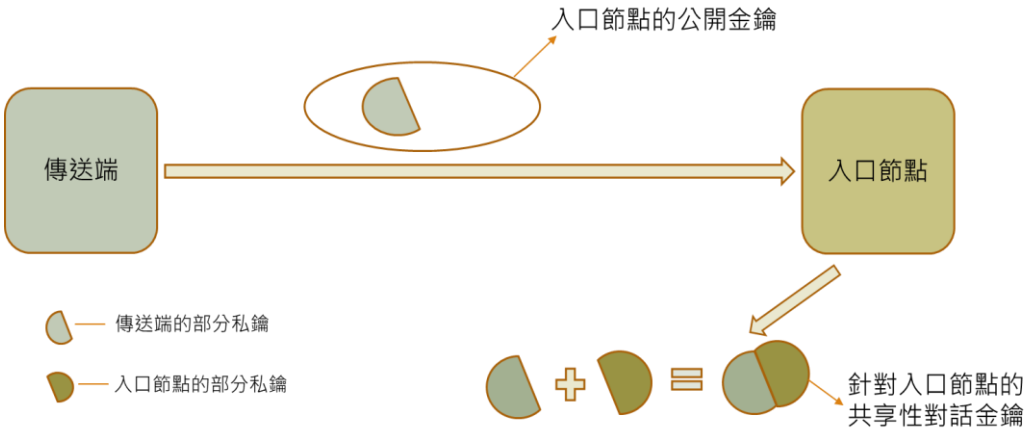
圖五：目錄節點選取經過

      C. 傳送端亦會傳送對話金鑰(Session key)給選取節點，以利後續傳送端與各節點傳送訊息時，所使用的對稱式加密使用。
      D. 傳送端將本身的私鑰以入口節點的公開金鑰加密後，傳送至入口節點，入口節點接收後進行解密，並將本身的私鑰結合傳送端的私鑰，形成共享性對話金鑰(Shared session key)，如圖六所示。

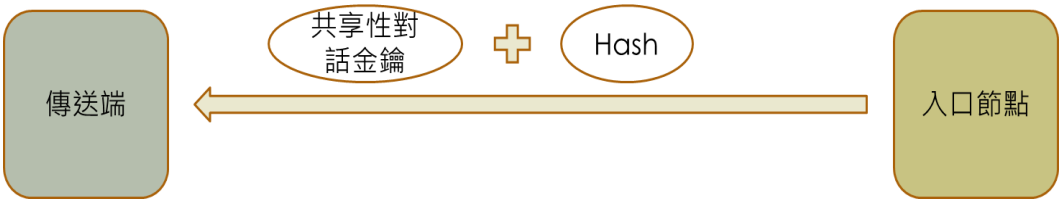
E. 入口節點將所得的共享性對話金鑰進行 hash 後，再將其 hash 值連同共享性對話金鑰一併回傳回傳送端，如圖七所示。

F. 回傳共享性對話金鑰後，傳送端與入口節點即建立連結。

G. 建立連線後，傳送端可透過此連線傳送加密過的訊息至鏈上的第二個節點，該訊息將只有第二個節點可以解密。



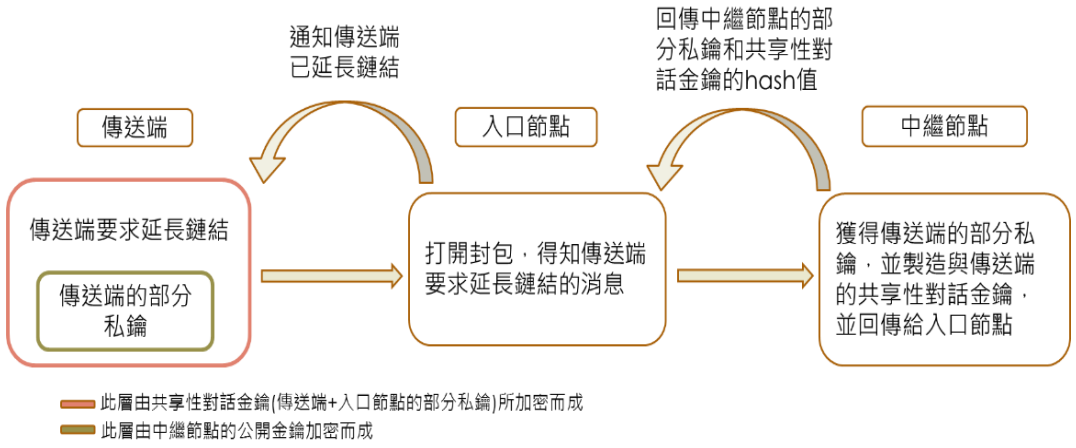
圖六：共享性對話金鑰形成經過



圖七：回傳共享性對話金鑰

H. 當第二個節點收到此訊息後，便會與前一個節點也就是入口節點建立同樣的連線，使發送者的加密連線延伸到第二個節點，然而第二個節點並不曉得前一個節點在鏈中的身分，如圖八所示。

I. 當鏈上節點之連線接建立完畢後，即形成和洋蔥一樣一層層的加密結構。



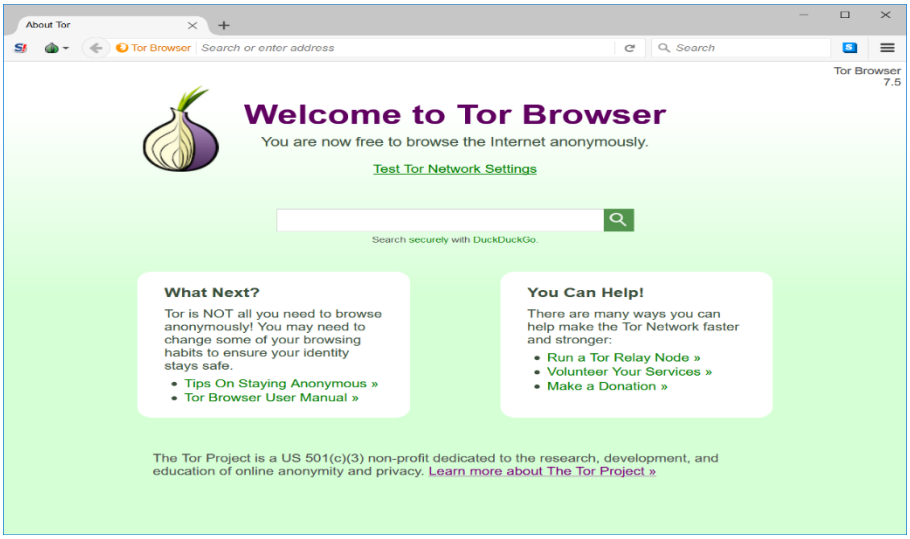
圖八：延長鏈結過程

(3) 訊息傳遞：洋蔥路由形成後，發送者可透過其傳送資料並保持匿名性，為確保發送者的匿名性，任一節點都無法知道在鏈中自己的前一個節點是傳送端還是鏈上的另一節點；同理，任一節點也無法知道在鏈中的下一節點是目的端還是鏈上另一節點。只有鏈上的最後一個節點知道本身是鏈上最終節點，即出口節點。

(4) 訊息解密：訊息封包經洋蔥路由層層加密後，傳送至目的端，目的端再層層解密，而其目的端回傳的訊息亦須經此傳遞鍊。

2.3 洋蔥瀏覽器(Tor browser)：

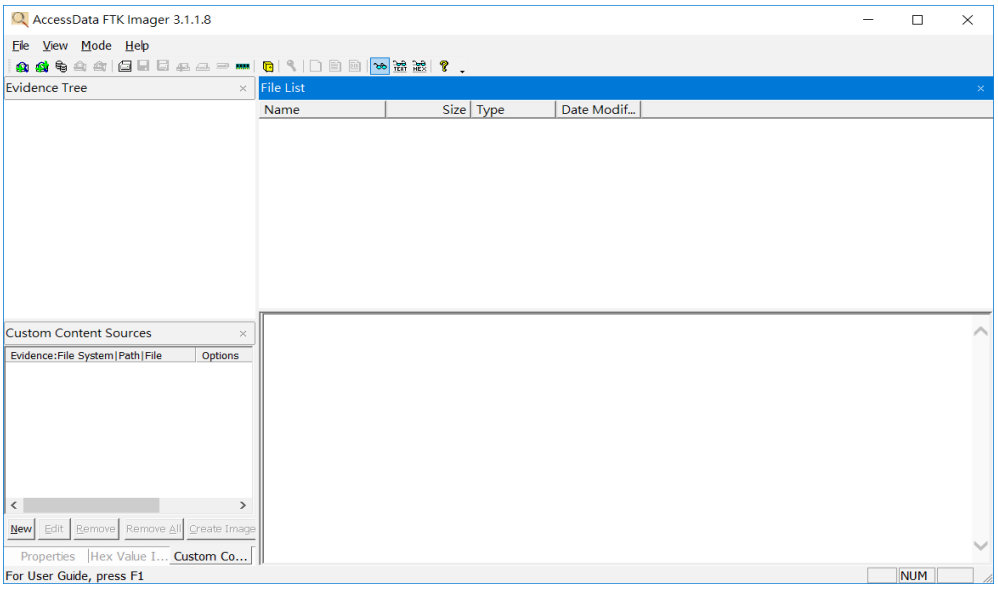
即為洋蔥路由的應用，是由 Mozilla Firefox ESR 瀏覽器修改而成，並由 Tor Project 的開發人員做了許多安全性和隱私保護的設定調整，為開源軟體，可在多種作業系統上運行，如 Windows、Mac OS X、Linux、Unix、BSD、以及 Android 手機。現今亦能於 IOS 使用，只要下載 Tor browser 即可使用。其 Tor browser 會在後台啟動 Tor 並透過其連線網路，一旦程式斷開連接，Tor browser 便會自動刪除屬隱私保護的資料，如 cookie 和瀏覽歷史記錄，亦提供 SOCKS 代理服務，使部分應用程式可藉此使用 Tor 網路，圖九為其開啟畫面。



圖九：Tor browser 開啟畫面

2.4 FTK Imager

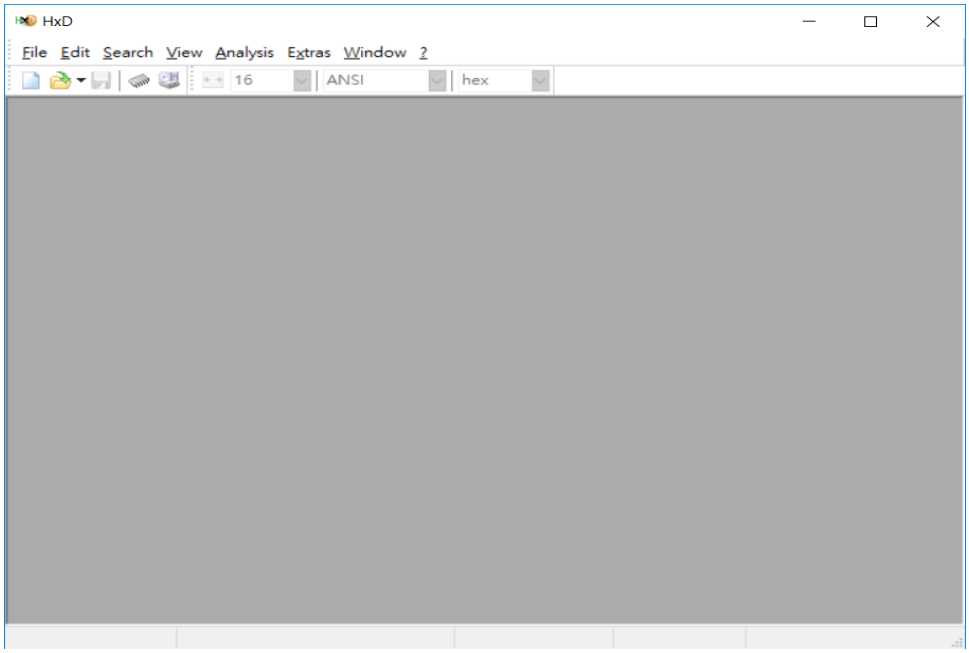
FTK (Forensic Toolkit)是由 Access Data 公司所生產的一套數位鑑識工具，其採用直覺化的操作介面，非常適合接觸電腦鑑識的人員使用。其中 FTK Imager 即為一種專用於製作磁碟及記憶體映像檔之工具，再加上其支援各種作業系統及檔案系統，並採取全文檢索式的資料搜尋技術，使鑑識人員可以快速地找到所需的數位證據。此軟體可免費下載於 Access Data 的官網中，故我們使用此軟體來進行記憶體萃取，以取得所需的犯罪跡證，圖十為其開啟畫面。



圖十：FTK Imager 開啟畫面

2.5 HxD

HxD 為一個可以檢視檔案十六進位碼的軟體，除此之外，也可以利用此軟體直接進行檔案或記憶體的修改，並具有資料匯出的功能，可以直接將修改好的檔案匯出成 VB、C++等語言的專案檔，使用十分便利。此軟體亦為免費軟體，故我們使用此軟體之基本功能—檢視檔案十六進位碼，來檢視由 FTK Imager 所萃取的記憶體中，是否有相關的犯罪跡證，圖十一為其開啟畫面。



圖十一：HxD 開啟畫面

參、實驗分析

本文實驗主要分為兩大部分，第一部分為針對「Tor 具隱匿蹤跡」之特性，實際操作實驗一，以佐證其特性。第二部分著重於 Tor browser 之鑑識，運用數位鑑識工具，還原使用者曾利用 Tor browser 所瀏覽過的網頁。第一部分為在在 Windows10 系統下，使用 Tor browser 瀏覽頁面，並利用 “whois” 查詢其 IP Address，以佐證「Tor 具隱匿蹤跡」之特性，實驗步驟如下：

Step1：使用 Tor browser，並瀏覽 facebook 頁面，如圖十二所示。
Step2：複製網址至 whois 查詢其 ip 位置，如圖十三所示。
Step3：whois 顯示為無效之網域，如圖十四所示。

圖十二：onion 型態的 Facebook 頁面

圖十三：whois 查詢 ip 位置(網址: https://www.facebookcorewwwi.onion/)

圖十四：whois 顯示為無效之網域

第二部分為在 Windows10 系統下，使用 Tor browser 瀏覽頁面，並透過 FTK Imager、HxD 等數位鑑識工具，來還原使用者曾瀏覽過的頁面，其實驗步驟如下：

Step1： 使用 Tor browser，並瀏覽 facebook 頁面，如圖十五所示。

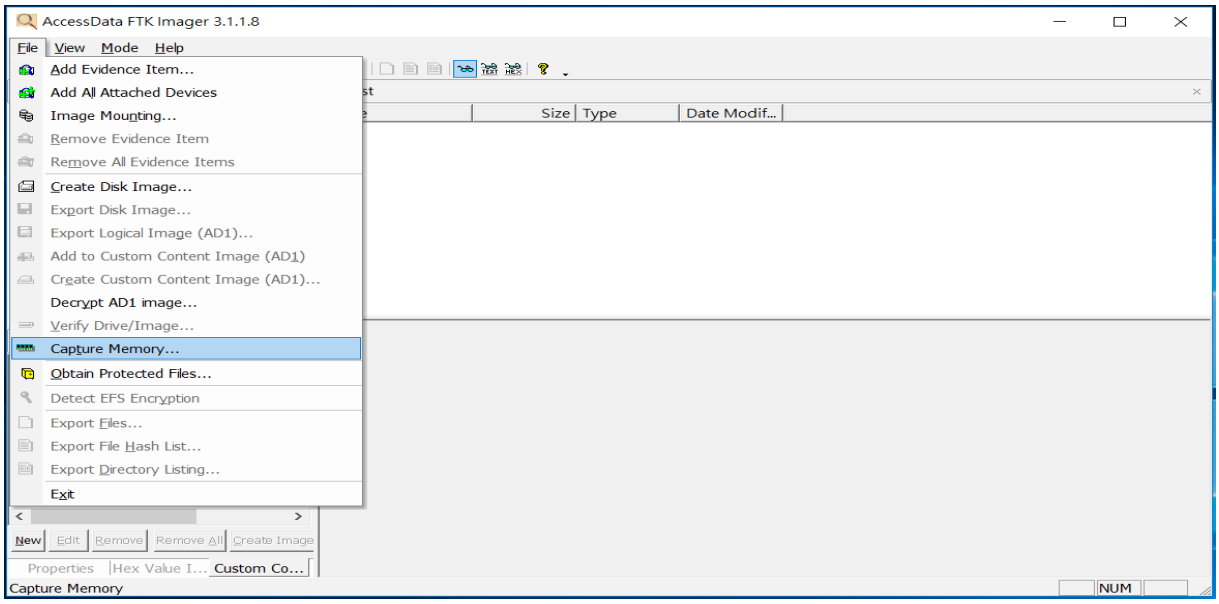
Step2： 利用 FTK Imager 進行記憶體萃取工作，得到 memdump.mem 檔，如圖十六、圖十七、圖十八。

Step3： 將所得的 memdump.mem 檔匯入 HxD，得到此檔的十六進位碼，如圖十九所示。

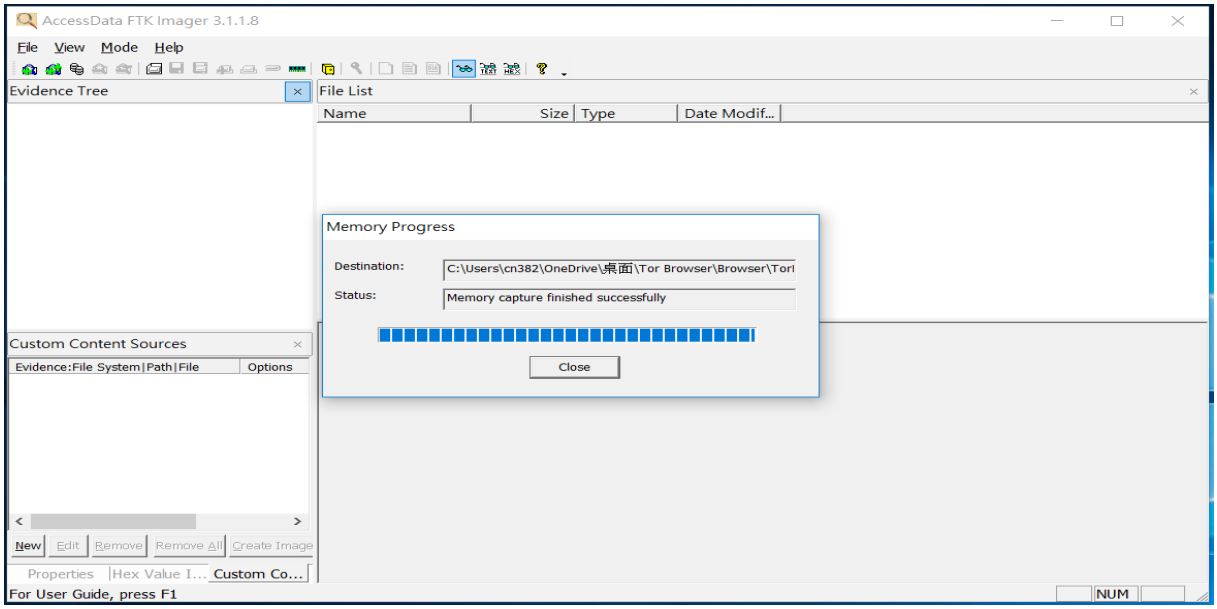
Step4： 輸入字串搜尋 onion，獲得瀏覽網址，如圖二十、圖二十一。

Step5： 還原使用者所瀏覽的頁面，如圖二十二所示。

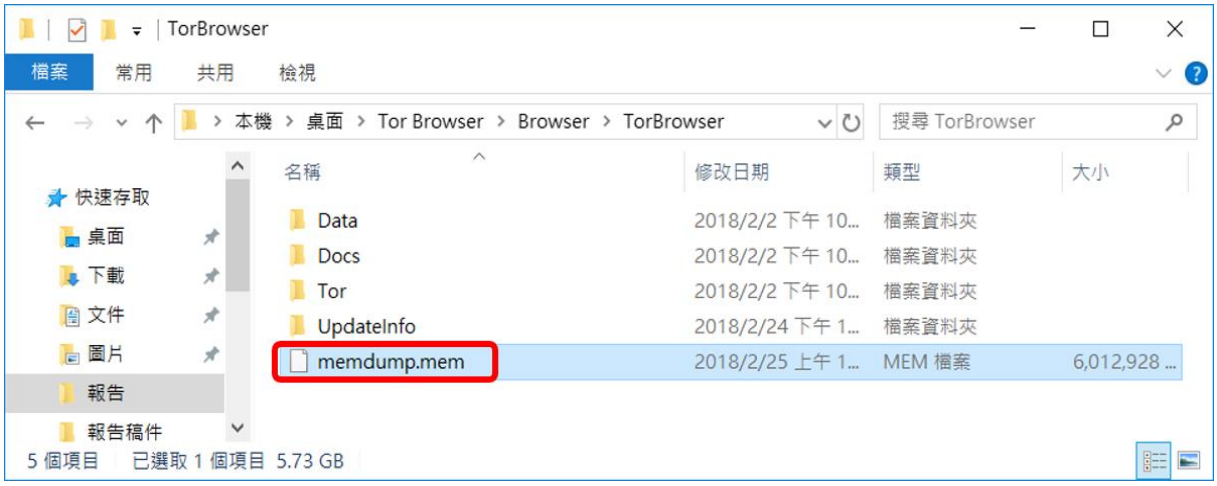
圖十五：onion 型態的 Facebook 頁面



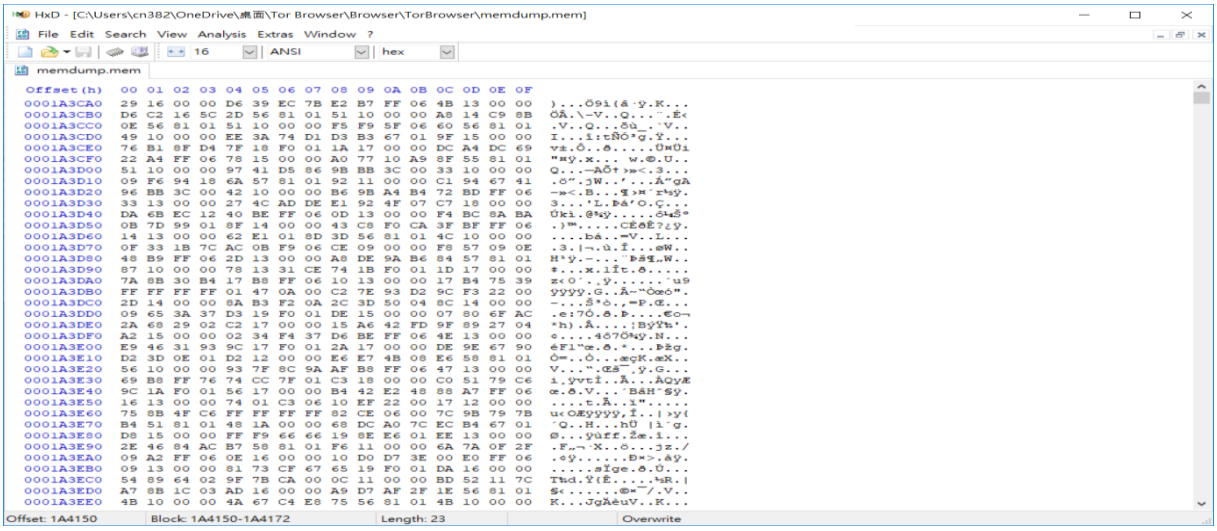
圖十六：FTK Imager 進行記憶體萃取



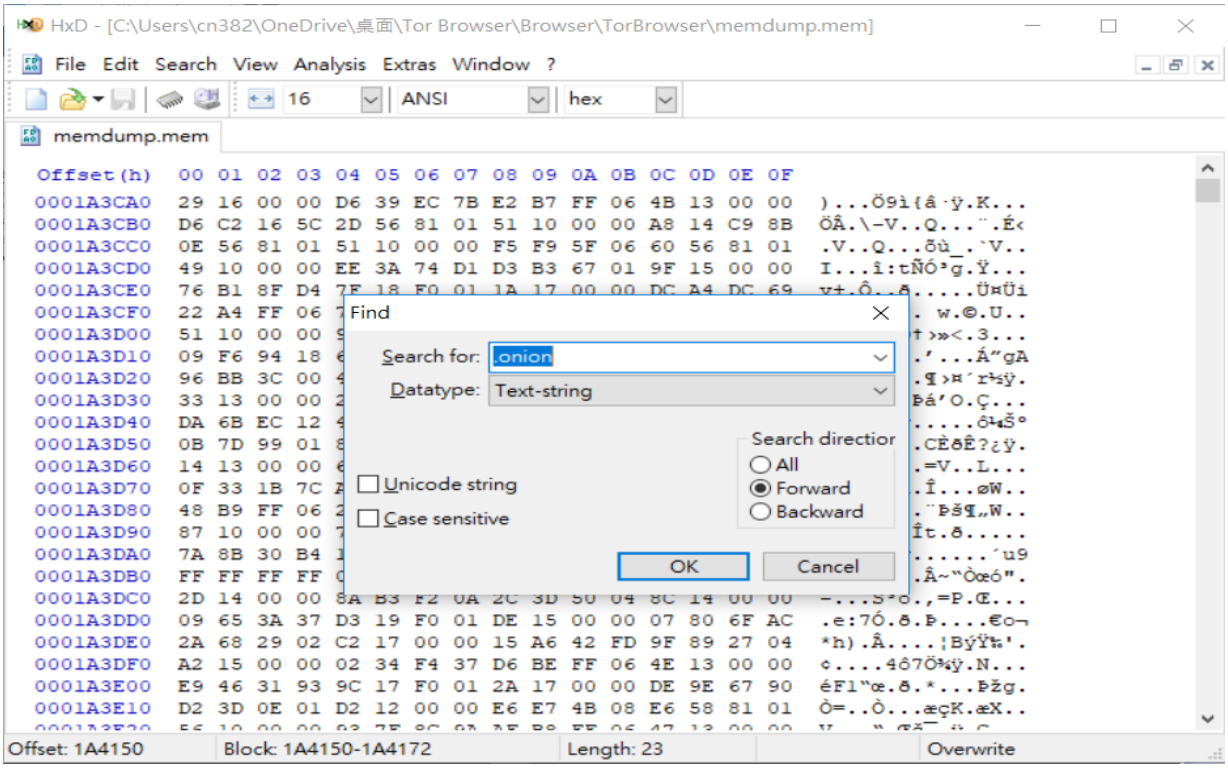
圖十七：記憶體萃取過程



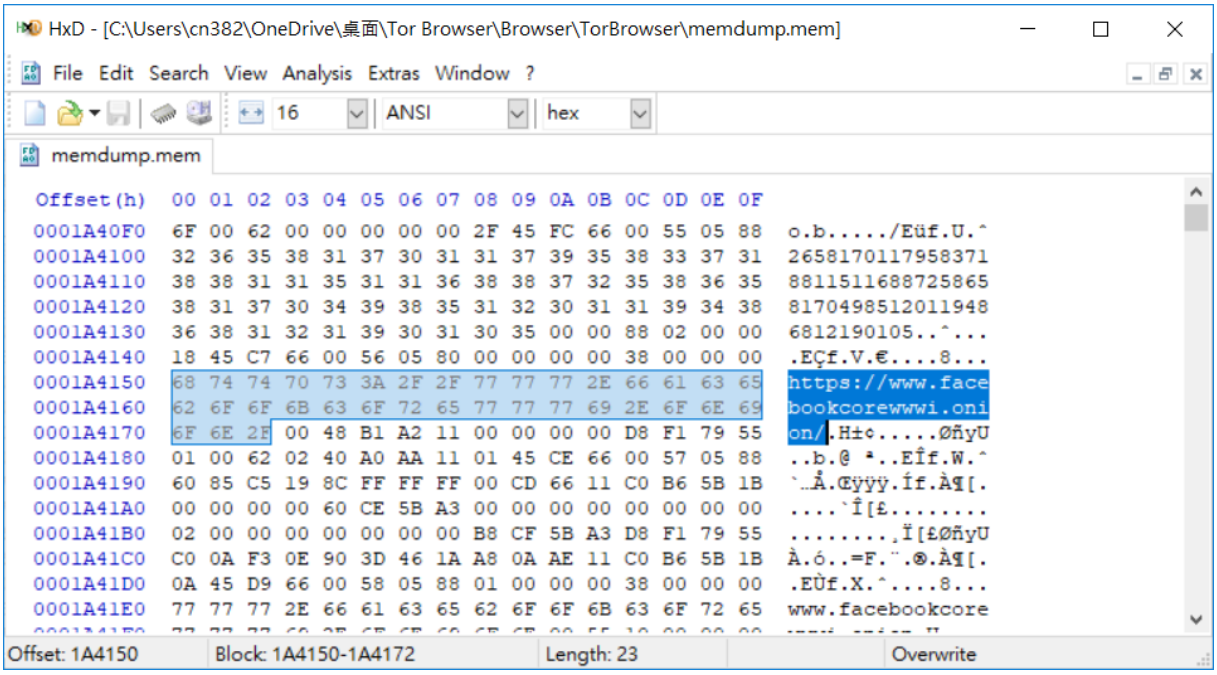
圖十八：獲得 memdump.mem



圖十九：memdump.mem 檔的十六進位碼



圖二十：字串搜尋 onion



圖二十一：獲得瀏覽網址

圖二十二：還原頁面

而下圖圖二十三，則為實驗的整體流程圖。

圖二十三：實驗流程圖

肆、案例

隨著網際網路時代的到來，越來越多人可以透過網路來獲得各類資訊，習得各種知識。然而，水可載舟，亦可覆舟，有些人透過網路，增廣自己的視野，立足國際，有些人卻透過網路，隱藏在螢幕背後，進行各種不法行為，且自以為神不知鬼不覺，而暗自竊喜，殊不知法網恢恢，疏而不漏，透過數位鑑識工具，依舊能夠還原真相，使之獲得應有的法律制裁。

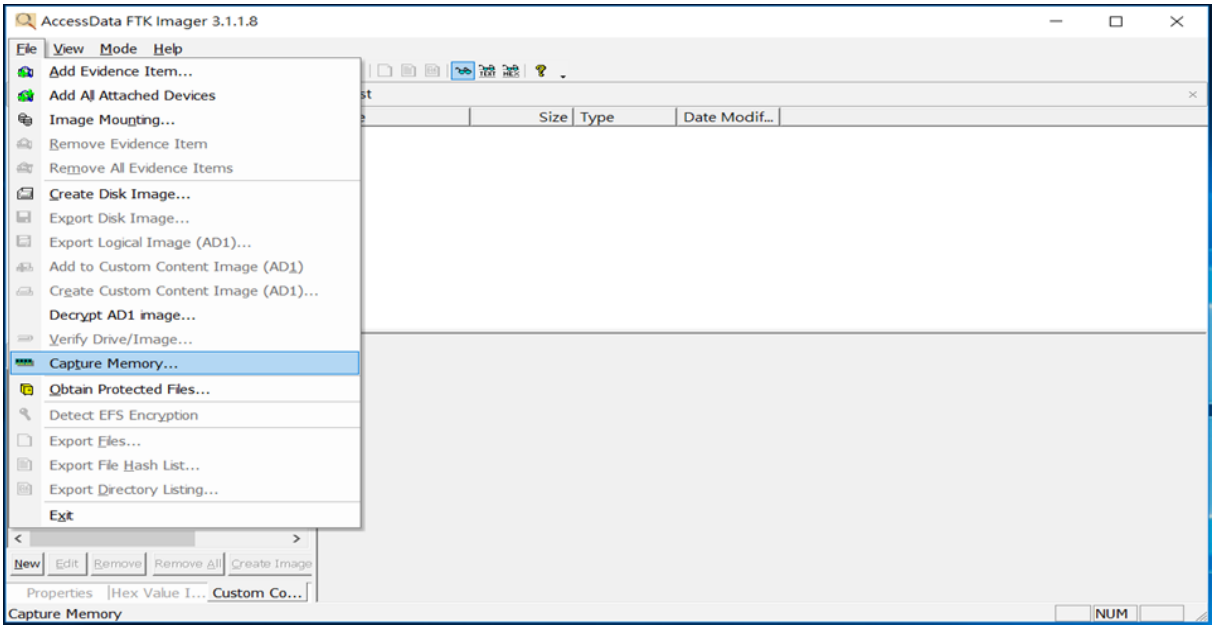
身為暗網交易大老的甲君即是一例，甲君為一位以比特幣在網路上進行不法交易之大老，並將所得的比特幣兌換成現金，來供自身日常所需使用。為使自己透過虛擬貨幣，進行交易的行蹤不被暴露，因此特別喜歡使用 Tor，以躲開調查人員追查金錢流向，而暴露行蹤。儘管交易規模龐大，甲君仍保持其低調之作風，相關交易物品之運送均交由其合夥乙君處理。今於一宗毒品買賣交易中，甲君、乙君因為利益分配而起衝突，乙君欲揭發罪狀，玉石俱焚，因此匿名向調查人員舉報，甲君使用 Tor browser，並以比特幣之方式，來進行毒品買賣。故調查人員開始追查甲君的行蹤及財務狀況，發現甲君並無固定工作，但家中卻有數輛保時捷跑車，且具有多個帳戶，每個帳戶均不定時會有大筆數額的金錢流轉，藉此疑點，及乙君的匿名舉報內容，故調查人員尋求司法單位之合作，傳喚甲君到場說明。然而，甲君到案後卻矢口否認自己有使用過 Tor browser，來瀏覽販賣毒品之網頁，以及毒品交易的犯罪行為，故調查人員透過數位鑑識工具(FTK Imager、HxD)，針對甲君在於 Windows 10 底下的殘留資料進行數位鑑識及資料還原，以獲得其使用過洋蔥瀏覽器之犯罪跡證，其鑑識手法如下所述：

鑑識方法：

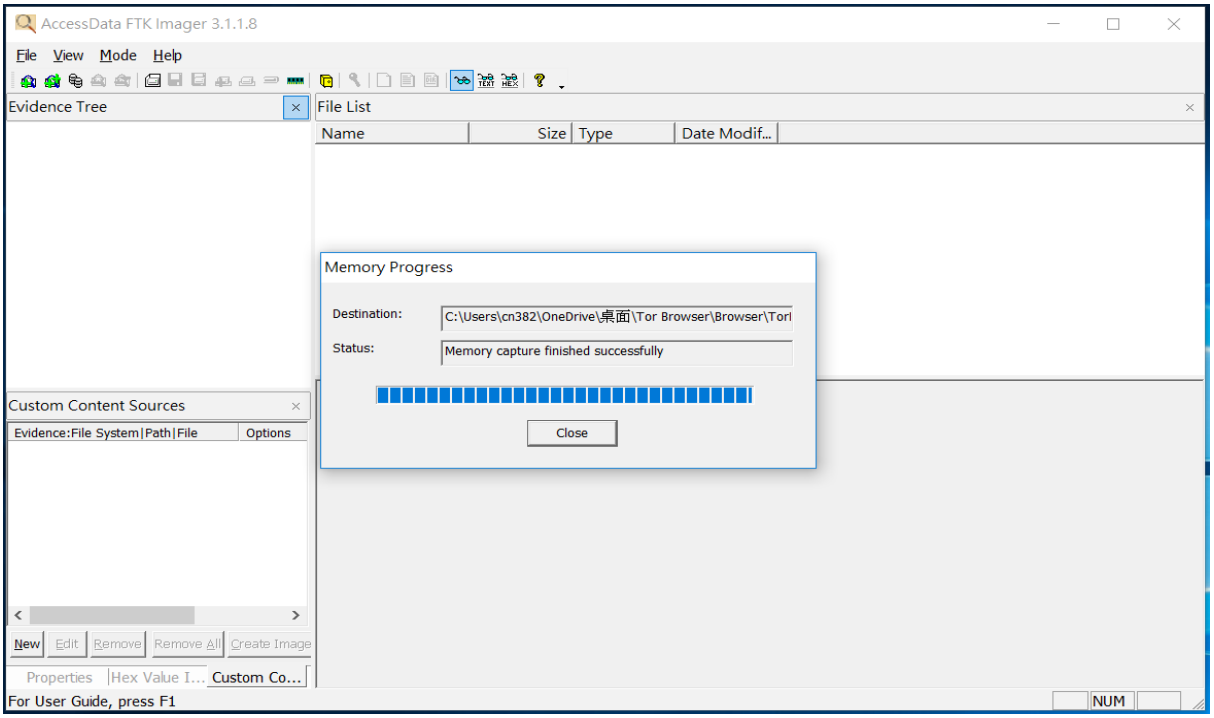
- 場景環境:在 Windows10 下使用 Tor browser
- 鑑識工具:FTK Imager、HxD
- 鑑識目的:證實甲君有在自己電腦使用 Tor browser 瀏覽販賣毒品之網頁，並有毒品交易的犯罪行為產生。
- 鑑識方法:其手法如下：
  1. 為避免甲君於蒐證過程中，有竄改電腦紀錄之疑慮，同時也為了減少鑑識人員於蒐證過程中，因人為疏失，而污染原始證物，影響證物的證據能力的風險，

因此先利用 FTK Imager 對電腦記憶體進行萃取。

→啟動 FTK Imager，並在 file 中選取 Capture Memory 即可進行記憶體萃取，如圖二十四、圖二十五所示。

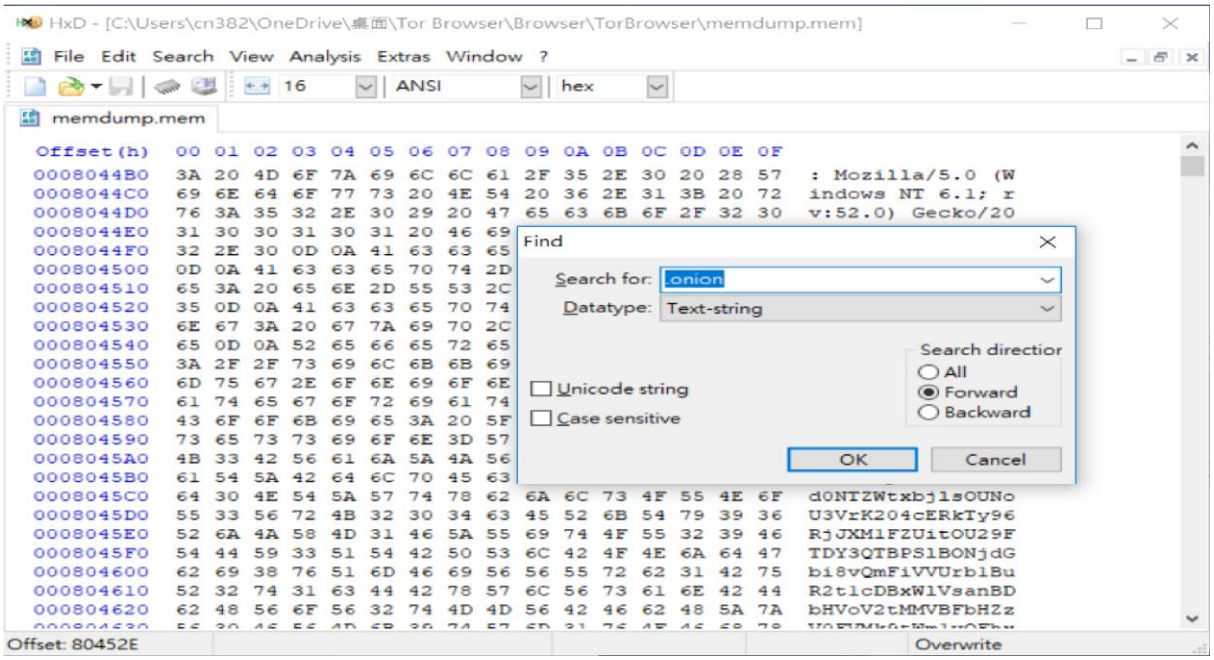


圖二十四：利用 FTK Imager，進行記憶體萃取

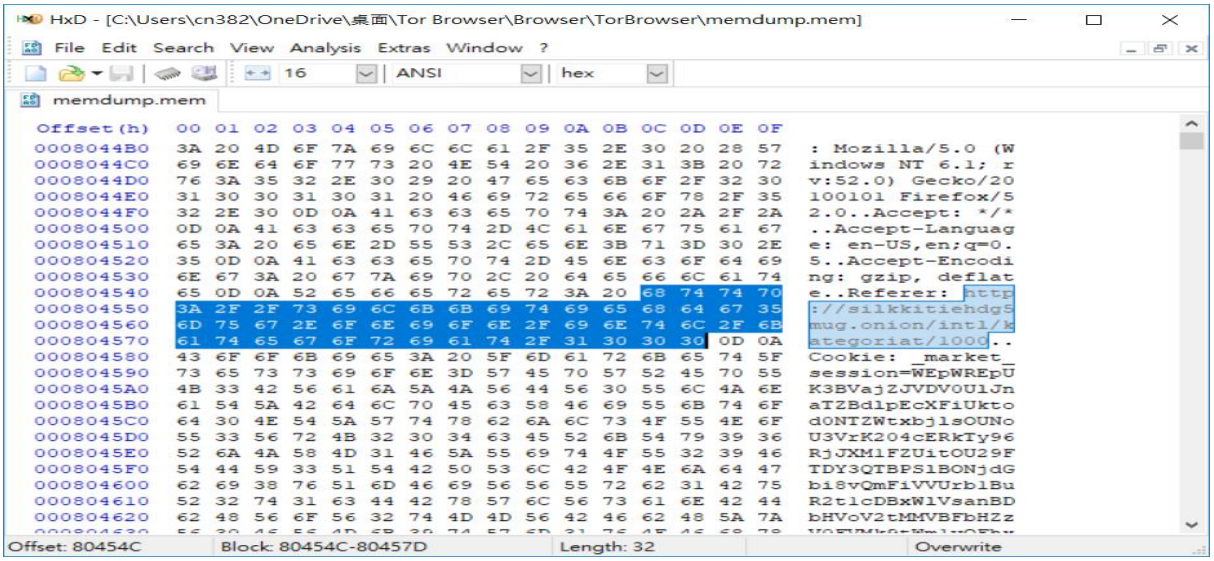


圖二十五：記憶體萃取過程

2. 使用 HxD 檢視由 FTK Imager 所萃取的記憶體中，是否存在甲君曾使用 Tor browser，瀏覽其買賣毒品的網頁。
→啟動 HxD，匯入 FTK Imager 所萃取的記憶體，並使用字串搜尋洋蔥專用 URL，發現在記憶體中清楚看到確實有使用 Tor browser，且瀏覽一個販售毒品的網站如圖二十六、圖二十七所示。

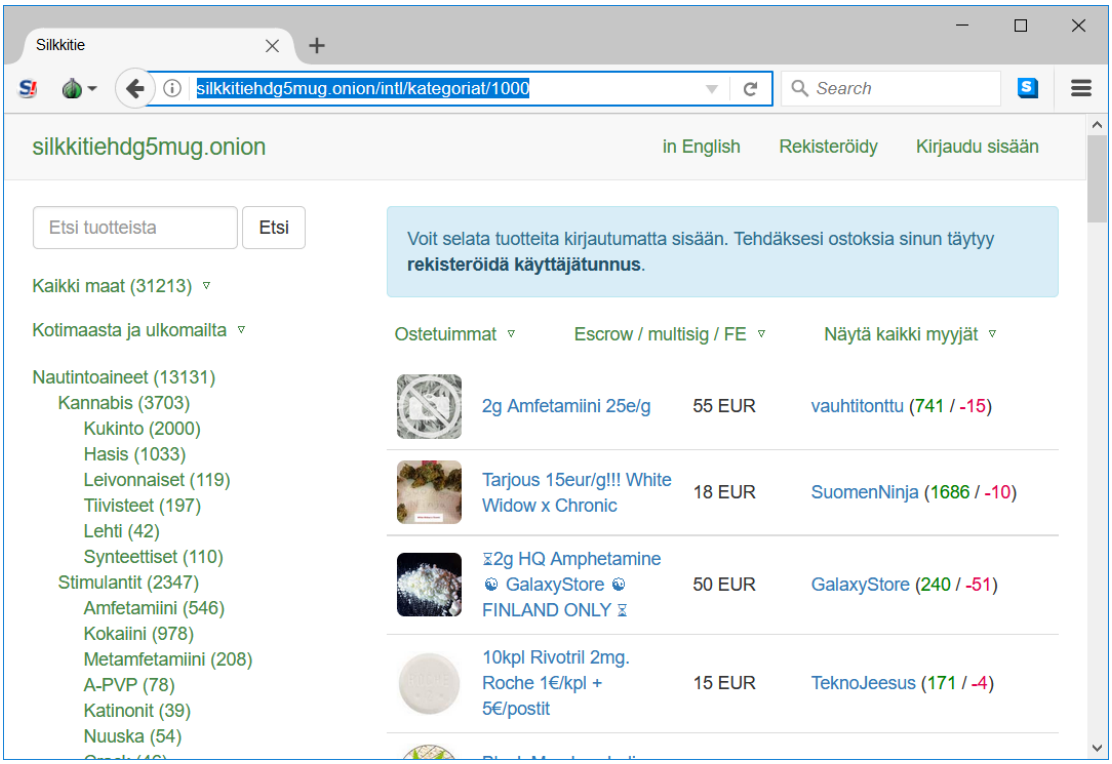


圖二十六：使用字串搜尋洋蔥專用 URL



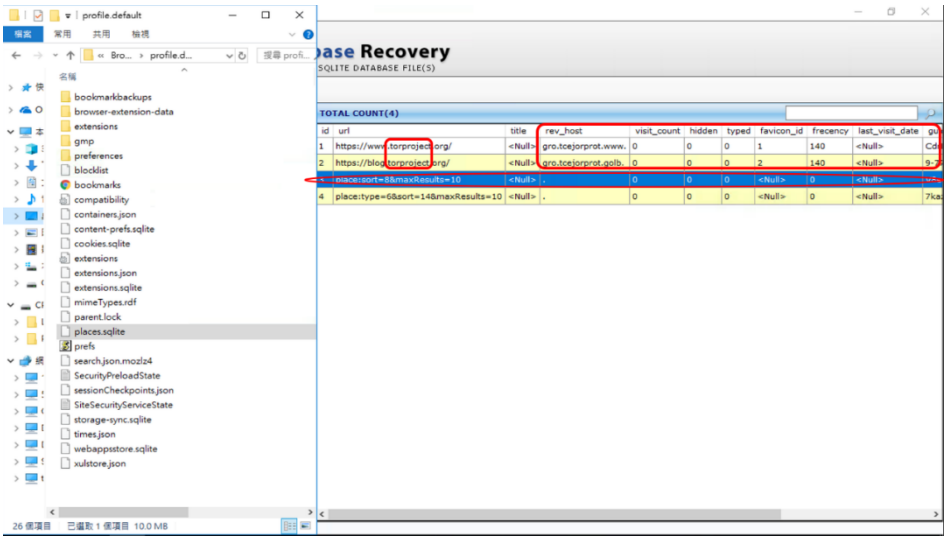
圖二十七：確實有使用 Tor browser 瀏覽毒品販售網站

3. 還原甲君所瀏覽之毒品販賣網站，如圖二十八所示。



圖二十八：還原甲君所瀏覽之毒品販賣網站

4. 欲還原 Tor browser 的瀏覽器資料庫內容，但發現 Tor 基於 Firefox 的瀏覽器資料庫中並無存在相關內容，僅找尋到訪問 Torproject 的紀錄，如圖二十九所示。



圖二十九：僅找尋到 Torproject 的紀錄

故經由調查人員使用鑑識工具進行蒐證後,可以發現甲君確實有使用 Tor browser 來瀏覽販賣毒品之網頁，推翻甲君先前之說詞，因此認定甲君有瀏覽販賣毒品網頁，進而從事不法交易的嫌疑，故交由司法機關做進一步裁定。

伍、結論

隨著資安意識的抬頭，愈來越多人傾向使用具有隱私保護的瀏覽器，例如:Tor browser 等，來避免自己遭到有心人士的不法侵害。然而，這些隱匿行蹤、匿名化的特性，卻成為企圖者最有力的後盾，憑仗著這些特性，不法行為在此橫行，無論是勒索病毒的支付贖金，抑或是暗網的黑市交易，都可以在此猖狂地進行。然而，法網恢恢，疏而不漏，企圖者都終將獲得應有的懲罰，越來越多人著手於 Tor 的去匿名化的研究，也發現 Tor 並非想像中的天衣無縫，凡走過必留下痕跡，要完全抹煞掉曾留下的紀錄，確實有一定的難度。因此，我們透過案例，並利用數位鑑識工具，FTK imager 以及 HxD，來進行 Tor browser 的使用偵測，獲得使用過 Tor browser 的證據並還原其瀏覽頁面，以戳破罪嫌的謊言。透過本文，我們了解洋蔥路由的組成及運作，並進一步鑑識洋蔥瀏覽器的使用，讓匿跡不再是一大資安危機。

陸、未來展望

本文透過記憶體萃取以及部分資料庫還原，來獲得企圖者曾經使用 Tor Browser 進行非法行為的跡證，而在未來，我們將利用 Wireshark 等封包側錄工具，來側錄其使用 Tor Browser 時的封包狀況，以及網路流量分析。除此之外，亦利用 Regshot 查看其安裝 Tor browser 後與安裝前的 Registry 變化。透過記憶體萃取、資料庫還原、封包狀況分析，以及 Registry 比較，來更加了解使用 Tor Browser 後，所產生的變化，並從中取得犯罪的蛛絲馬跡，以還原真相。

參考文獻

[1] A. A. AlQahtani and E. S. M. El-Alfy, “Anonymous connections based on onion routing: A review and a visualization tool,” *Procedia Computer Science*, vol. 52, pp. 121-128, 2015.

[2] C. Díaz, S. Seys, J. Claessens and B. Preneel, “Towards measuring anonymity,” *International Workshop on Privacy Enhancing Technologies*, pp. 54-68, Springer, Berlin, Heidelberg, Apr. 2002.

[3] R. Dingledine, N. Mathewson and P. Syverson, "Tor: The second-generation onion router," *Usenix Security*, Aug. 2004.
[4] D. Rathod, "Darknet forensics," *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 6, issue 4, Jul. - Aug. 2017.
[5] D. Rathod, "Web browser forensics: google chrome," *International Journal of Advanced Research in Computer Science*, vol. 8, No. 7, Jul. - Aug. 2017.
[6] M. G. Reed, P. F. Sylverson and D. M. Goldschlag, "Anonymous connections and onion routing," *IEEE Journal on Selected Areas in Communications*, vol. 16(4), pp. 482-494, IEEE, May, 1998.
[7] R. Ruiz, S. Ruiz, F. P. Amatte, J. Kil and P. D. S. Brandini, "Opening the private browsing data – acquiring evidence of browsing activities," *Proceedings of the International Conference on Information Security and Cyber Forensics*, Kuala Terengganu, Malaysia, Aug. 2014.
[8] Tor, "What is Tor Browser," https://www.torproject.org/projects/torbrowser.html.en, Mar. 2018.
[9] Tor Network Status, https://torstatus.blutmagie.de/
[10] B. Turvey and W.J. Chisum, "Evidence dynamics: Locard's exchange principle & crime reconstruction," *Journal of Behavioral Profiling*, vol.1, no.1, Jan. 2000.