FORENSIC SCIENCE JOURNAL SINCE 2002

Forensic Science Journal
2018;17(1):1-8
fsjournal.cpu.edu.tw
DOI:10.6593/FSJ.2018.1701.01

A Forensic Examination of Anonymous Browsing Activities

Szu-Yuan Teng [1*], M.S. ; Che-Yen Wen [2], Ph.D.

[1] Taipei City Field Office, Investigation Bureau, Ministry of Justice
[2] Department of Forensic Science, Central Police University

Received: May 31, 2018; Accepted: August 15, 2018.

Abstract

Internet crime has become a serious problem. Cybercriminals use the Darknet to sell some software tools in the black market, such as DDOS attack software, ransomware, Crimeware-as-a-service (CaaS), and other cybercrime tools. Users can use the Tor browser with incognito functions to connect to the Darknet and conduct transactions in the black market. Besides, there are some anonymous browsers with the functions of hiding the webpage activities of users. Although these browsers cannot be used to connect to the Darknet directly, they can let a criminal connect to the Internet anonymously and hide all criminal activities. Therefore, the investigation of digital evidence from the used records of anonymous browsers is full of critical challenges. In this paper, we demonstrate how tools and programs can be used in forensic analysis of anonymous browsers. There are six types of anonymous browsers in our experiments: Epic Privacy Browser, Secure Browser, Comodo Dragon, SRWare Iron, Dooble, and Maxthon. The experimental results show the capability of those tools and programs in the investigation of digital evidence.

Keywords: anonymous browser forensics, anti-forensics, digital evidence, digital forensics, webpage activity forensics

Introduction

With the growth in the awareness of personal Internet privacy protection, the concept of the secure browsers attracts people's attention. Commercial web browsers (such as Chrome, IE, and Firefox) have developed a series of security functions (such as incognito mode, URL filtering, download protection, and non-tracking) to comply with personal privacy protection requirements. To an extent, these browsers can be termed as "secure" browsers [1]. From users' point of view, if we use more browser anonymity functions, we can obtain more privacy protection. However, it will cause more difficulties for criminal investigation if criminals use highly anonymous and security function browsers to commit crimes.

Internet crime has become a serious problem. Criminals use the Darknet and underground black market to provide Crimeware-as-a-Service (CaaS). Users can also use the Tor browser with incognito functions to connect to the Darknet and conduct transactions in the underground black market. There are other browsers with incognito functions such as Epic Privacy Browser, Secure Browser, Comodo Dragon, SRWare Iron, Dooble, and Maxthon. Although these browsers are not available for the connection to the Darknet, they can let

[*] Corresponding author: Szu-Yuan Teng, Taipei City Field Office, Investigation Bureau, Ministry of Justice.
E-mail: mjib.teng@gmail.com

users connect to the Internet anonymously and hide all criminal activities. Bursztein et al. conducted automatic security measurement on the private browsing modes of four popular browsers (such as Chrome, Firefox, IE, and Safari), and found that the extensions and plugins of these browsers might damage private browsing security [2]. Mahendrakar et al. analyzed the activity records of browsers. They found some data available for tracing even under the privacy mode [3]. Said et al. investigated the effectiveness of private browsing mode features in three widely used browsers, and outlines their investigation method for criminal activities. They proposed a three-phase analysis method. The first phase is to use a special forensic tool to check common places where browsers history and cached records are stored. The second phase is to check the other location of disk storage space on local machine. The last phase is to capture physical memory (RAM) and analyze artifacts of browsers [4]. Ohana and Shashidhar found residual artifacts of several popular browsers from portable and private browsing sessions. They argued that it is possible to find traces in physical memory (RAM), slack/free space and certain areas of the file system through the specific forensic tool [5]. Ghafarian and Seno showed how to use forensics methodologies and tools to examine the artifacts left in volatile memory after a private browsing session [6]. They recovered browsing evidence related to IE browser from the file system. Flowers et al. partially reconstruct the private browsing session evidence from the physical memory (RAM), hibernate and page files where are the key areas [7]. Shafqat used various forensic tools and techniques to reconstruct the private browsing activity of the Google Chrome browser in Windows 8 [8]. Warren et al. conducted forensic acquisition analysis of the Browzar browser which is an emphasis privacy preserving internet browser. They compared it with other popular anonymous browsers [9].

From previous work, we can see that the current research works on the popular anonymous browsers are very comprehensive and complete. However, research on less-popular anonymous browsers attracted less attention. In this paper, we focus our study on 6 less-popular anonymous browsers (with incognito functions): Epic Privacy Browser Version 40.0.2214.91, Secure Browser Version 57.0.441.112, Comodo Dragon Version 55.0.2883.59, SRWare Iron Version 57.0.3000.0, Dooble Version 1.56c, and Maxthon V 5.0.2.2000. Our experiments are based on the digital forensic procedure of evidence identification, evidence extraction and collection, evidence analysis, and reporting and presentation. Our analysis tools (e.g. file system monitor and network packet monitor) are installed on Microsoft Windows 10 based on VMware Workstation. For each browser, the normal and private browsing session are observed and analyzed in four aspects: file and folder, system registry file, network packet and physical memory.

Methods

Anonymous Browsers

In this paper, we focus on six anonymous browsers which are common in practical cases: Epic Privacy Browser, Secure Browser, Comodo Dragon, SRWare Iron, Maxthon, and Dooble. Each of them emphasizes the unique anonymity and privacy protection features to allow users to hide the webpage activities. The first five browsers are based on the chromium technology that can eliminate usage tracking and other privacy-compromising functions which are included in the Google Chrome browser. These anonymous browsers have their own specific features which are different from Google Chrome. The last browsers, Dooble, utilizes the Qt technology which has stronger anonymity than Chromium-based browsers.

Epic Privacy Browser is based on Chromium. It blocks every conceivable place that can cause privacy leaks, and maximizes privacy. Session data, such as the cookies and tracking data, are deleted at the end of each session. All search processes are conducted through its own server, which attempts to prioritize SSL connections to the maximum extent [10]. Secure Browser provides secure browsing, private browsing, non-tracking, privacy removal, HTTPS encryption, and a series of safety and incognito functions [11]. Comodo Dragon is a free browser based on Chromium. Its browser interface is similar to Google Chrome but without functions that may potentially threaten privacy [12]. SRWare Iron is another free browser based on the Chromium framework. This browser provides similar functions as Chrome [13]. Dooble is a streamlined Chromium-based cross-platform (Windows, Linux, OS X) browser that can disable non-secure interfaces such as Flash and Javascript in its default state. It blocks third-party cookies in iFrames and provides an innovative function that can use various ciphers and passphrases to encrypt all contents (bookmarks, browsing preferences, and history) [14]. Maxthon is an all-new HTML5 compatible browser. Its unique incognito mode can provide secure browsing without leaving any traces [15].

Our goal is to provide an analysis reference for criminal investigators. When they want to find the criminal activities (such as online drug trafficking, cryptocurrency purchasing for money laundering) in anonymous browsers, the reference can help them choose proper forensic tools. In our experiments, we use some well known forensic tools (in the next subsection) to identify traces of anonymous browsing activities after using the unique anonymous features provided by these browsers. We also analyze and compare the difference of the stored digital evidence between non-incognito mode operations (can remove the browsing history) and incognito mode operations of the six anonymous browsers.

Digital Forensic Methods

We use the X-Ways Forensics software to conduct the integration analysis and record the virtual machine file systems. Data from four sources (files and folders, system registry, network packages, and memory) were used for observation and differential analysis to identify possible file paths in residual forensic information or forensic feature items that can be useful for forensic examination. We used the following tools to collect data: SysTracer Version 2.1.0 for the comparison of relevant records (registry keys and registry location), Disk Pulse Version 8.2.16 for observing and recording changes in the folders and files, Wireshark Version 2.4.6 for capturing and analyzing the network packets, Process Hacker Version 2.39 for capturing browser memory, and the Capture Memory function in FTK Imager Version 3.1.0 was used to capture virtual machine memory. Fig. 1 shows the digital forensic process for anonymous browsers.

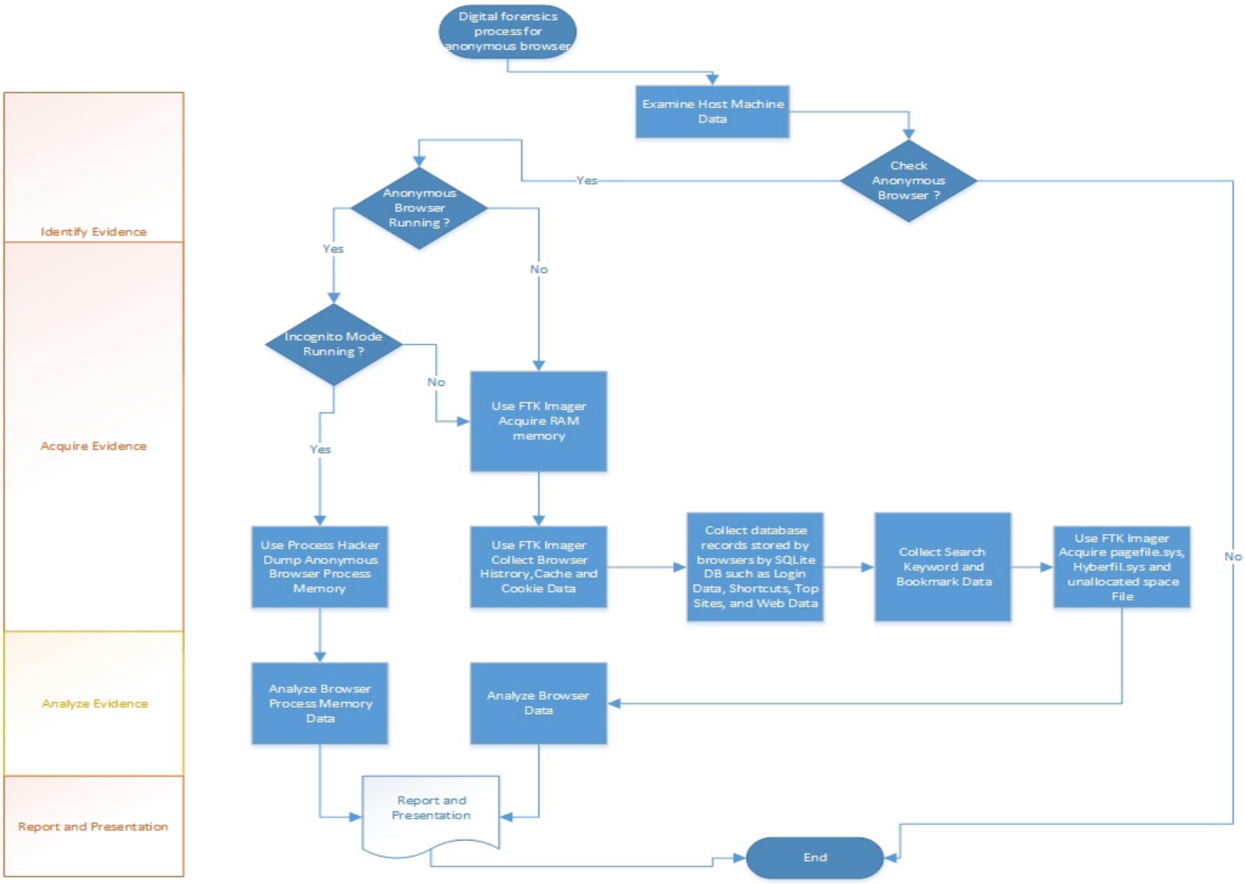
Digital forensics process for anonymous browser
Examine Host Machine Data
Check Anonymous Browser ?
Yes
No
Anonymous Browser Running ?
Yes
No
Incognito Mode Running ?
No
Yes
Use FTK Imager Acquire RAM memory
Use Process Hacker Dump Anonymous Browser Process Memory
Use FTK Imager Collect Browser History,Cache and Cookie Data
Collect database records stored by browsers by SQLite DB such as Login Data, Shortcuts, Top Sites, and Web Data
Collect Search Keyword and Bookmark Data
Use FTK Imager Acquire pagefile.sys, Hyberfil.sys and unallocated space File
Analyze Browser Process Memory Data
Analyze Browser Data
Report and Presentation
End
Identify Evidence
Acquire Evidence
Analyze Evidence
Report and Presentation

Fig. 1 The digital forensic process for anonymous browsers.

Results and Discussions

From the experimental results, we can find residual digital evidence in several regions: the files and folders in the file system, system registry key, browser execution programs and network port used for connection, random access memory, and browser execution memory. Although these six browsers use different incognito functions and frameworks, they still store the browsing information and records in the browser memory. Before we terminate the browser program, it is possible for us to identify and recover some browsing records and data in the incognito mode. We show some important forensic items for the six browsers with incognito functions in Table 1.

Table 1 Important forensic items for the six browsers with incognito functions.

Data analysis of browser files			
Name of browser	Name of important file or folder	Important storage path	Forensic value
Epic Privacy Browser	Files: Cookies, Login Data, Preferences, Secure Preferences, Bookmarks; Folder: Local Storage	1. \Users\User Account\AppData\Local\Epic Privacy Browser\User Data\Default	Identification of whether the user had installed and used this anonymous browser
Secure Browser	1. Files: Cookies, Web Data, Favicons, Login Data, Preferences, Shortcuts, Top Sites, Network Action Predictor, Bookmarks, previews_opt_out.db; Folders: Local Storage, databases, Cache 2. Files: Safe Browsing Cookies, Safe Browsing Download; Folder: CertificateTransparency	1. \Users\User Account\AppData\Local\Safer Technologies\Secure Browser\User Data\Default\ 2. \Users\User Account\AppData\Local\Safer Technologies\Secure Browser\User Data\	
Comodo Dragon Browser	1. Files: Cookies, Web Data, Favicons, Login Data, Preferences, Shortcuts, Top Sites, Network Action Predictor; Folders: Local Storage, Session Storage, Databases, Cache 2. Files: Safe Browsing Cookies, Safe Browsing Download; Folder: CertificateTransparency	1. \Users\User Account\AppData\Local\Comodo\Dragon\User Data\Default\ 2. \Users\User Account\AppData\Local\Comodo\Dragon\User Data\	
SRWare Iron Browser	1. Files: Cookies, Web Data, Favicons, Login Data, Preferences, Shortcuts, Top Sites, Network Action Predictor; Folders: Local Storage, databases, Cache, Session Storage, Media Cache 2. Files: Safe Browsing Cookies; Folder: Certificate Transparency	1. \Users\User Account\AppData\Local\Chromium\User Data\Default\ 2. \Users\User Account\AppData\Local\Chromium\User Data\	

Data analysis of browser files			
Name of browser	Name of important file or folder	Important storage path	Forensic value
Dooble Browser	Files: applications.db, cacheexceptions.db, cookies.db, downloads.db, favicons.db, history.db, preferences.db; Folder: Cache, Dooble	\Dooble\User Account\.dooble	
Maxthon Browser	1. Files: Cookies, Web Data, *.dat; Folders: Local Storage, databases, Application Cache, History, Favorite 2. Files: Cookies, Web Data; Folders: Local Storage, databases, Application Cache 3. Files: *.dat; Folder: NewTab 4. All files	1. \Users\User Account\AppData\Roaming\Maxthon5\Users\guest\ 2. Users\User Account\AppData\Roaming\Maxthon5\Users\guest\Session\ 3. \Users\User Account\AppData\Roaming\Maxthon5\Temp\ 4. \Users\kan\AppData\Local\Temp\Maxthon3Cache\Temp\Webkit\Cache\	

Analysis of registry keys associated with browser			
Name of browser	Important keys	Registry location	Forensic value
Epic Privacy Browser	DisplayName DisplayVersion InstallDate InstallLocation	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Epic\	Confirmation of whether Epic Privacy Browser is installed
Secure Browser	AppId LastAccessedTime LaunchCount	HKEY_USERS\S-1-5-21-3260109858-125348108-769363293-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps\{BBB8055F-9110-4435-8621-8D9062283332}\	Confirmation of whether Secure Browser is installed
Comodo Dragon Browser	InstallDate Version	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\ComodoGroup\Dragon\	Confirmation of whether Comodo Dragon Browser is installed
SRWare Iron Browser	DisplayName DisplayVersion Inno Setup: App Path InstallDate InstallLocation	HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\{C59CF2CE-B302-4833-AA35-E0E07D8EBC52}_is1\	Confirmation of whether SRWare Iron Browser is installed

Analysis of registry keys associated with browser

Name of browser	Important keys	Registry location	Forensic value
Dooble Browser	AppId LastAccessedTime LaunchCount	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps\{765FD9D6-CC3D-4183-8CA7-7CC8B03AA9E0}\	Confirmation of whether Dooble Browser is installed
Maxthon Browser	DisplayName DisplayVersion InstallDate InstallLocation	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\Maxthon5\	Confirmation of whether Maxthon Browser is installed

Network packet analysis

Name of browser	Name of program	Specific website	Specific network ports opened	Forensic value
Epic Privacy Browser	Epic.exe	epicbrowser.net www.epicsearch.in	Port:4430	Confirmation of whether this browser is used in the operating system and as a benchmark for retrieving specific keywords in the memory
Secure Browser	Secure.exe	client.securebrowser.com	Port:80 Port:443	
Comodo Dragon Browser	Dragon.exe	download.comodo.com	Port:80 Port:443	
SRWare Iron Browser	chrome.exe	iron.start.me	Port:80 Port:443	
Dooble Browser	Dooble.exe	metager.de; alt1-safebrowsing.google.com	Port:80 Port:443	
Maxthon Browser	Maxthon.exe	pc-newtab.maxthon.com. l.maxthon.com	Port:80 Port:443	

Analysis of random access memory and browser memory

Browser is in normal or incognito (private) status	Whether specific websites are logged into and service account and password information can be found	Forensic value
The browser is logged into specific websites, showing that its status is not logged out.	Login account number and passwords can be found in the browser execution program memory, and the password exists in a cp 950 or utf-16 encoding format	The account and clear text password information that the user uses to login to websites can be obtained. Data stored in specific websites can be obtained through the account and passwords
The browser displays that it has logged out of specific website services and the browser is not closed	Login account number and passwords can be found in the browser execution program memory, and the password exists in a cp 950 or utf-16 encoding format	
The browser is closed	From the random access memory data, we can find the login account for specific websites, but are unable to obtain clear text password information	

Except the Epic Privacy Browser (with default settings), we can set the incognito functions on or off in the other five browsers. Table 2 presents the analysis results of the browser incognito functions, non-incognito modes (can remove browsing history), and forensic methods for the incognito modes in the browsers.

Table 2 Digital evidence data of the browsers with incognito functions.

Name of browser with incognito functions	Epic Privacy Browser	Secure Browser	Comodo Dragon Browser	SRWare Iron Browser	Dooble Browser	Maxthon Browser
Browser version and technology used for engine	Version: Based on Chromium technology Engine: WebKit	Version: Based on Chromium technology Engine: WebKit	Version: Based on Chromium technology Engine: WebKit	Version: Based on Chromium technology Engine: WebKit	Version: Based on Qt technology Engine: WebKit	Version: Based on Chromium and IE technology Engine: WebKit and Trident
Analysis of incognito functions in browser	Default incognito mode, no normal mode	1. Normal mode 2. Private Browsing mode	1. Normal mode 2. incognito mode	1. Normal mode 2. incognito mode	1. Normal mode 2. Private mode	1. Normal mode 2. Private mode 3. Session mode
Percentage of evidence that can be collected from memory	1. Website content (contains images) of websites browsed 2. History, Cookie, Download, Search, and other information 3. Account and password for logging into website (does not exist when browser is closed, but the passwords for some cloud services can still be found in the memory and are not erased after the Maxthon browser is opened) 4. Percentage of evidence retained differs according to the browser usage					
Forensic methods for browser non-incognito mode operations (can remove browsing history)	1. Collect browser History, Cache, and Cookie 2. Collect database records stored by browsers by SQLite DB such as Login Data, Shortcuts, Top Sites, and Web Data. 3. Collect search keyword and bookmark information 4. Browser temporary storage 5. Registry key 6. Memory data 7. Unallocated space data					
Forensic methods for browser incognito mode operations	1. When the browser is not opened, capture the browser memory for analysis. Epic Privacy Browser, Secure Browser, Comodo Dragon, SRWare Iron, and Maxthon anonymous browsers have a main program during browser execution, whereas Dooble has only one program. All programs should be fully captured to avoid omissions. 2. When the browser is opened, capture random access memory, pagefile.sys, Hyberfil.sys, and unallocated space for analysis					

In summary, we can find digital evidence in several regions, such as SQLite database files (History, Cache, Cookie, Login Data, Shortcuts, Top Sites, Web Data), Search Keyword and bookmark information, browser temporary storage files, system registry key, random access memory, server execution memory, pagefile.sys, Hyberfil.sys, and unallocated space. The browsers with incognito functions possess the anti-forensic ability and present a significant challenge for forensic analysis. However, if the browser memory content can be extracted by forensic tools expeditiously, we still have a chance to obtain and extract the Internet information and records that a user has previously browsed.

Conclusions

In this paper, we use some experiments to investigate digital evidence items in six anonymous browsers with incognito functions. We demonstrate how we can use tools and programs to analyze them and collect digital evidence. The experimental results show the capability of those tools and programs in the inspection of crimes that employ these anonymous browsers.

References

1. The best secure browsers 2018. from http://www.techworld.com/security/best-8-secure-browsers-3246550/.
2. Gaurav A, Bursztein E, Jackson C, Boneh D. An analysis of private browsing modes in modern browsers. USENIX Security'10 Proceedings of the 19th USENIX conference on Security, Washington, DC, 11-13 August 2010.
3. Mahendrakar A, Irving J, Patel S. Forensic analysis of private browsing mode in popular browsers. in Proceedings of the USENIX security symposium 2010.
4. Said H, Mutawa NAI , Awadhi IAI, Guimaraes M. Forensic analysis of private browsing artifacts. Published in International Conference on Innovations in Information Technology, 197-202, Abu Dhabi, United Arab Emirates, 25-27 April 2011 .
5. Ohana D-J, Shashidhar N. Do private and portable web browsers leave incriminating evidence? a forensic analysis of residual artifacts from private and portable web browsing sessions. EURASIP Journal on Information Security 2013; 6.
6. Ghafarian A, Seno S-A-H. Analysis of privacy of private browsing mode through memory forensics. International Journal of Computer Applications, 2015; 132.
7. Flowers C, Mansour A, Khateeb H-M-AI. Web browser artefacts in private and portable modes: a forensic investigation. International Journal of Electronic Security and Digital Forensics, 2016; 8:99-117.
8. Shafqat N. Forensic Investigation of User's Web Activity on Google Chrome using various Forensic Tools. IJCSNS, 2016; 16:123.
9. Warren C, Sheikh E-EI, Khac N-A-Le. Privacy Preserving Internet Browsers: Forensic Analysis of Browzar. in Computer and Network Security Essentials, ed: Springer, 2018:369-88.
10. Epic Privacy Browser Home (2017). Epic Privacy Browser, a secure chromium-based web browser that protects your privacy and browsing history _ a free VPN privacy browser Retrieved 1 June 2017, from https://www.epicbrowser.com/.
11. Seucre Browser Home (2017). Secure Browser Fast, Secure, Private Web Browser Retrieved 15 June 2017, from https://www.securebrowser.com/.
12. Comodo Dragon Browser (2017). Secure Web Browser Fastest Free Dragon Browser from Comodo Retrieved 15 June 2017, from https://www.comodo.com/home/browsers-toolbars/browser.php.
13. SRWare Iron Browser Home (2017). SRWare Iron The Browser of the Future Retrieved 15 June 2017, from https://www.srware.net/en/software_srware_iron.php.
14. Dooble Home (2017). Dooble Web Browser Retrieved 15 June 2017, from http://dooble.sourceforge.net/.
15. Maxthon Browser Home (2017). Maxthon 5 all-new release, supported free entire platform download Retrieved 15 May 2017, from http://www.maxthon.cn/.