FORENSIC SCIENCE JOURNAL SINCE 2002

Forensic Science Journal
2017;16(1):43-50
fsjournal.cpu.edu.tw
DOI:10.6593/FSJ.2017.1601.04

Applying Memory Forensic Technique in Popular Browsers to Assist Criminal Investigation in the Cloud

Wen-Chao Yang [1*], Ph.D. ; Te-Chi Lo [2], M.S. ; Chung-Hao Chen [3], Ph.D.

[1] Department of Forensic Science, National Central Police University, Taoyuan City, Taiwan
[2] National Central Police University, Taoyuan City, Taiwan
[3] Electrical and Computer Engineering Department, Old Dominion University, Norfolk, VA, U.S.A.

Received: October 16, 2017; Accepted: November 19, 2017.

Abstract

A web browser is a widely used application to access data or use cloud applications on the Internet. In crime scenes, forensic artifacts left by a web browser after a session include, but are not limited to, browsing cache and history, cookies, login information and lists of file download. In particular, the login information is a very useful tool for investigators to trace criminal relative evidence in urgent need, because the memory forensic technique can catch the login information in physical memory used for a web browser.

Due to the privacy necessary for web browser users, web browsers add "Private Browsing" which prevented the browser from leaving traces of browsing history, temporary files, usernames, and passwords on a system. In recent crime cases, in order to prevent the browser from leaving trace of the criminal relative information, many suspects use "Private Browsing" to access criminal data, or use cloud applications on the Internet.

In this paper, we focus on applying the memory forensic technique to the investigation of memory artifacts of "Private Browsing" in popular web browsers. According to the experimental results, we not only determine that the login information can be caught from physical memory when suspect uses "Private Browsing" in four popular browsers, but find out necessary information to retrieve login information without usernames.

Keywords: memory forensic, web browser, criminal investigation, cloud investigation

Introduction

Memory forensics is the most fruitful, interesting, and provocative realm of digital forensics [1]. Traditional storage forensics provide a set of techniques to preserve, recover, search, and analyze digital evidence. Storage forensic tools mainly focus on non-volatile storage device and typically use bit-to-bit copied storage media [2]. In recent years, a new technique, memory forensics, has raised for analyzing volatile memory in a system for forensic artifacts. It can reveal a substantial amount of violate evidence which includes lists of running processes, network connections, chat message, etc.

A web browser is a widely used application by users to access data or use cloud applications on the Internet. Malicious clients over the web have always been attempting to steal web browsing related information like Social Security number, account password, client email address, client address book, client browser history, and so forth. Due to the privacy necessary for web browser

*Corresponding author: Wen-Chao Yang, Department of Forensic Science, National Central Police University, Taoyuan City, Taiwan.
E-mail: una135@mail.cpu.edu.tw

users, Apple safari browser adds "Private Browsing," the private browsing mode, which can prevent the browser from leaving traces of browsing history, temporary files, username, and password on a system in 2005 [3]. To date, many popular web browsers, such as Google Chrome, Mozilla Firefox, Microsoft Edge and Microsoft Internet Explorer (IE), include this feature. In Mozilla Firefox the feature is well known as Private Browsing [4]. In Google Chrome, it is called as incognito mode [5]. In Microsoft Edge and Internet Explorer, it is called as In-Private mode[6,7]. Therefore, many suspects use the private browsing mode or the incognito mode of popular web browsers to access criminal data or use cloud applications on the Internet to prevent the browser from leaving trace of criminal relative information.

Several studies have examined the browser trace left by Private Browsing. In 2014, Chivers [8] examined the use of IE 10's In Private Browsing feature to discover what the browser' trace could be recovered. Chivers found that IE 10 maintains its history records and cache in the WebCacheV01.dat file and claimed that over 80% of evidence on browsing history was recoverable from non-database areas. Satvat *et al.* [3] examined the remains left by Firefox 19.0, Safari 5.1.7, Chrome 25.0.1364.97 and IE 10.0.9200.16521. Although they found that evidence from private browsing sessions could not be recovered in its database when Firefox was cleanly closed, cache artifacts was contained in physical memory in Domain Name Server (DNS). Ohana and Shashidhar [9] investigated the artifacts left by private mode and portable browsers like Microsoft IE, Google Chrome, Mozilla Firefox and Apple Safari. From these experiments, they discovered that IE left the most artifacts in untypical locations and Chrome Portable proved to leave the most artifacts on the host machine. For other browsers, physical memory appeared to be the best place to obtain evidence. Alam *et al.* [7] investigated the artifacts left by InPrivate browsing feature in a Microsoft Edge browser and found that physical memory appeared to be the best place to obtain evidence.

Proposed Method

This section describes our proposed testing and forensic framework. The purpose is to analyze whether or not login information is left and which keywords are near login information in physical memory used for "Private Browsing" in popular web browsers.

Instruments

To investigate the artifacts that browsers leave in physical memory, the following list of tools and devices are used.

1. Computer: Intel Pentium 3558U 1.7GHz CPU with 4GB RAM.
2. Virtual machine (VM): VMware Workstation Player (version 12) is used to simulate the suspect's computer.
3. Operating system of suspect's computer: Microsoft Windows 10
4. Physical memory of suspect's computer: 2GB
5. Browsers of suspect's computer:
   5.1. Google Chrome: version 53.0.2785.14m
   5.2. Mozilla Firefox: version 48.0.1
   5.3. Microsoft Internet Explorer: version 11.0.14393.0
   5.4. Microsoft Edge: version 38.14393.0.0
6. Mails or social communities
   6.1. Google Gmail
   6.2. Microsoft Hotmail
   6.3. Facebook
7. Forensic tools
   7.1. AccessData Forensic Toolkit (FTK) Imager: version 3.4.2.6 (in a 256GB M.2 Solid State Disk, SSD)
   7.2. X-ways WinHex: version 18.3

Experiments

The VM is cloned after installing operating system and four kinds of browsers so as a clean system each time. Then, we conduct following tests for the experiment. During each test, we imitate the behavior of suspects, and then an investigator installs the forensic SSD and runs AccessData FTK Imager tool to do memory dump for physical memory and the page file. After memory dump is finished, we use X-ways WinHex to analyze the dump and the page files.

In order to investigate the left memory artifacts, we design three experimental conditions that show different statuses of web browsers, browsing modes, and mails or social communities. In the first experimental condition, we investigate the login information to determine

whether or not the suspect uses only one tab page. In tests 1 and 3, we dump memory when the suspect uses only one tab page. The contrast tests are tests 2 and 4. Then, tests 1, 3, 5, and 6 will use login information in different browsing modes.

The memory analysis is a well-known time consuming work, especially without the assistant keywords. We want to not only determine if the login information exists in different browsing modes to log in different mails or social communities, but find out the assistant keywords to gather login information in the last experimental condition. Tests 7 and 8 are designed to log in different mails or social communities. The following table shows the description of tests. Table 1 summarizes those eight tests.

Table 1 The list of tests.

Test No.	Description
1	Use only one tab page with different browsing modes on a Google Chrome browser to log in Google Gmail
2	Use the second tab page with different browsing modes on a Google Chrome browser to log in Google Gmail
3	Use only one tab page with different browsing modes on a Mozilla Firefox browser to log in Google Gmail
4	Use the second tab page with different browsing modes on a Mozilla Firefox browser to log in Google Gmail
5	Use only one tab page with different browsing modes on a Microsoft IE browser to log in Google Gmail
6	Use only one tab page with different browsing modes on a Microsoft Edge browser to log in Google Gmail
7	Use different browsing modes of on a Google Chrome browser to log in Google Gmail, Microsoft Hotmail, and Facebook
8	Use different browsing modes on a Mozilla Firefox browser to log in Google Gmail, Microsoft Hotmail, and Facebook

Result and Analysis

In this section, we delineate the finding and results from each test with various conditions.

Experimental Results

1. Use only one tab page with different browsing modes on a Google Chrome browser to log in Google Gmail.

We imitate what a suspect does by logging out the connection or not and closing the web browser or not to analyze whether login information is left in physical memory. The result is shown in Table 2.

Table 2 The experimental result of test 1.

No.	Mode	Logout	Close browser	Password in Memory (ASCII)
1	normal	Yes	No	Yes
2	normal	Yes	Yes	No
3	normal	No	Yes	No
4	normal	No	No	Yes
5	incognito	Yes	No	Yes
6	incognito	Yes	Yes	No
7	incognito	No	Yes	No
8	incognito	No	No	Yes

In Table 2, we can see the password can be found if the suspect does not close the browser in both browsing modes.

2. Use the second tab page with different browsing modes on a Google Chrome browser to log in Google Gmail.

We imitate what a suspect does by logging out the connection or not and closing the web browser or not to analyze whether the login information is left in physical memory. The result is shown in Table 3.

Table 3 The experimental result of test 2.

No.	Mode	Logout	Close the browsing page	Password in Memory (ASCII)
1	normal	Yes	No	Yes
2	normal	Yes	Yes	No
3	normal	No	Yes	No
4	normal	No	No	Yes
5	incognito	Yes	No	Yes
6	incognito	Yes	Yes	No
7	incognito	No	Yes	Yes
8	incognito	No	No	Yes

In Table 3, we can see the password can be found if a suspect does not close the browsing page in normal mode. In incognito mode, the password cannot be found just in logout and close the browsing page condition.

3. Use only one tab page with different browsing modes on a Mozilla Firefox browser to log in Google Gmail.

We imitate what a suspect does by logging out the connection or not and closing the web browser or not to analyze whether the login information is left in physical memory. The result is shown in Table 4.

Table 4 The experimental result of test 3.

No.	Mode	Logout	Close browser	Password in Memory (ASCII)
1	normal	Yes	No	Yes
2	normal	Yes	Yes	No
3	normal	No	Yes	No
4	normal	No	No	Yes
5	InPrivate	Yes	No	No
6	InPrivate	Yes	Yes	No
7	InPrivate	No	Yes	No
8	InPrivate	No	No	No

In Table 4, we can see the password can be found if the suspect does not close the browser in normal mode, but cannot be found in InPrivate mode.

4. Use the second tab page with different browsing modes on a Mozilla Firefox browser to log in Google Gmail.

   We imitate what a suspect does by logging out the connection or not and closing the web browser or not to analyze whether the login information is left in physical memory. The result is shown in Table 5.

Table 5 The experimental result of test 4.

No.	Mode	Logout	Close the browsing page	Password in Memory (ASCII)
1	normal	Yes	No	Yes
2	normal	Yes	Yes	Yes
3	normal	No	Yes	Yes
4	normal	No	No	Yes
5	InPrivate	Yes	No	No
6	InPrivate	Yes	Yes	No
7	InPrivate	No	Yes	No
8	InPrivate	No	No	No

From Table 5, we can see the password can be found just in normal mode.

5. Use only one tab page with different browsing modes on a Microsoft IE browser to log in Google Gmail.

   We imitate what a suspect does by logging out the connection or not and closing the web browser or not to analyze whether the login information is left in physical memory. The result is shown in Table 6.

Table 6 The experimental result of test 5.

No.	Mode	Logout	Close browser	Password in Memory (ASCII)
1	normal	Yes	No	Yes
2	normal	Yes	Yes	No
3	normal	No	Yes	No
4	normal	No	No	Yes
5	InPrivate	Yes	No	Yes
6	InPrivate	Yes	Yes	No
7	InPrivate	No	Yes	No
8	InPrivate	No	No	Yes

In Table 6, we can see the password can be found if a suspect does not close the browser in both browsing modes.

6. Use only one tab page with different browsing modes on a Microsoft Edge browser to log in Google Gmail.

   We imitate what a suspect does by logging out the connection or not and closing the web browser or not to analyze whether the login information is left in physical memory. The result is shown in Table 7.

Table 7 The experimental result of test 6.

No.	Mode	Logout	Close browser	Password in Memory (ASCII)
1	normal	Yes	No	Yes
2	normal	Yes	Yes	No
3	normal	No	Yes	No
4	normal	No	No	Yes
5	InPrivate	Yes	No	Yes
6	InPrivate	Yes	Yes	No
7	InPrivate	No	Yes	No
8	InPrivate	No	No	Yes

In Table 7, we can see the password can be found if a suspect does not close the browser in both browsing modes.

7. Use different browsing modes on a Google Chrome browser to log in Google Gmail, Microsoft Hotmail, and Facebook.

We imitate what a suspect does by logging out the connection or not and closing the web browser or not to analyze whether the login information is left in physical memory. The result is shown in Table 8.

Table 8 The experimental result of test 7.

No.	Mode	Mails or social communities	Password in Memory (ASCII)	Account near the password (ASCII)	Assistant information
1	Normal	Gmail	Yes	Yes	Passwd=
2	incognito	Gmail	Yes	Yes	Passwd=
3	Normal	Hotmail	Yes	Yes	Passwd=
4	incognito	Hotmail	No		
5	Normal	Facebook	Yes	Yes	Pass=
6	incognito	Facebook	No		

In Table 8, we can see the password can be found with user account in normal mode when a suspect logs in Gmail, Hotmail, or Facebook. In incognito mode, the password can only be found in user account when a suspect logs in Gmail. In addition, we also discover the assistant keyword “passwd=” can be used to search login information in the rightest column of Table 8.

8. Use different browsing modes on a Mozilla Firefox browser to log in Google Gmail, Microsoft Hotmail, and Facebook.

We imitate what a suspect does by logging out the connection or not and closing the web browser or not to analyze whether the login information is left in physical memory. The result is shown in Table 9.

Table 9 The experimental result of test 8.

No.	Mode	Mails or social communities	Password in Memory (ASCII)	Account near the password (ASCII)	Assistant information
1	Normal	Gmail	Yes	Yes	PasswordField
2	InPrivate	Gmail	No		
3	Normal	Hotmail	Yes	No	password-notification
4	InPrivate	Hotmail	No		
5	Normal	Facebook	Yes	No	passwordfield password-notification
6	InPrivate	Facebook	No		

In Table 9, we can see the password can be found only in normal mode when a suspect logs in Gmail, Hotmail, or Facebook. In addition, we also discover the assistant keywords can be used to search login information in the rightest column of Table 9.

Analysis

According to the test results, we analyze the experimental results in three conditions in the following subsection. In the first experimental condition (different statuses of web browsers), see table 2, 3, 4 and 5, we find out that the login information is left in physical memory before closing a Google Chrome browser regardless of which tab page is used. In contrast, the login information is left in physical memory before closing a Mozilla Firefox browser when a suspect uses only one tab page to log in Gmail with normal browsing mode. In addition, when a suspect uses the second tab page to log in Gmail with normal browsing mode, the login information is left in physical memory regardless of the Mozilla Firefox browser being closed or not (please see table 5).

In the second experimental condition (different browsing modes), see table 2, 4, 6, and 7, we find out that the login information is left in physical memory in both browsing modes before Google Chrome, Microsoft edge and Microsoft Internet Explorer browsers have been closed. When a suspect uses normal browsing mode in a Mozilla Firefox browser, the login information is left in physical memory before the browser has been closed. In contrast, we cannot find out the login information in physical memory using InPrivate browsing mode in a Mozilla Firefox browser (see table 4).

In the last experimental condition (log in different mails or social communities), we find out some assistant keywords which is helpful for the investigator to gather the login account and password. In table 8, we can see the keyword “passwd=” or “pass=” nearby the login account and password in physical memory in a Google Chrome browser. Furthermore, in table 9, the keyword “passwordfield” or “password-notification” is nearby the login account and password in physical memory in a Mozilla Firefox browser. These keywords are helpful information for investigators to reduce the searching time to gather the login information in practice.

Conclusion and Discussion

Web browser forensic is an important work for digital forensic. We applied the memory forensic technique to the investigation of left memory artifacts of “Private Browsing” in popular web browsers. In many major crime cases, login information is very helpful for investigators in urgent need. However, the memory analysis without assistant keywords is a heavy time consuming work. Therefore, we not only investigate

whether login information can be found in the physical memory, but find out the assistant keywords to gather login information in this paper.

According to experimental results, login information in the physical memory of testing systems can be retrieved in some conditions. In contrast to the foregoing researches, we not only determine that login information can be retrieved in physical memory when a suspect uses Private Browsing of most of popular browsers in some cases, but find out useful information for an investigator to gather login information.

Acknowledgements

The authors would like to thank anonymous reviewers for their insight comments and valuable suggestions. This work was supported by National Science Council, Taiwan (MOST 106-2218-E-015-001-).

Reference

1. Ligh MH, Case A, Levy J, Walters A. The art of memory forensics: Detecting malware and threats in windows, Linux, and Mac Memory. John Wiley & Sons, Inc, July 2014.
2. Case A, Richard III G-G. Memory forensics: The path forward. Digital Investigation 2017;20:23-33.
3. Satvat K, Forshaw M, Hao F, Toreini E. On the privacy of private browsing - a forensic approach. Journal of Information Security and Applications February 2014;19(1):88-100.
4. Mozilla Foundation, Private Browsing - Browse the web without saving information about the sites you visit. 2014. Available at: https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history. Accessed time: 14 October 2017.
5. Google, Browse in private, 2015. Available at: https://support.google.com/chrome/answer/95464?co=GENIE.Platform%3DDesktop&hl=en. Accessed time: 14 October 2017.
6. Microsoft, Windows browse InPrivate in Microsoft edge. 2014. https://support.microsoft.com/zh-tw/help/4026200/windows-browse-InPrivate-in-microsoft-edge. Accessed time: 14 October 2017.
7. Alam S, Aziz M-A, Iqbal W. Forensic analysis of edge browser in-private mode. International Journal of Computer Science and Information Security 2016;14(9):256-63.
8. Chivers H. Private browsing: A window of forensic opportunity. Digital Investigation 2014;11(1):20-9.
9. Ohana D, Shashidhar N. Do private and portable web browsers leave incriminating evidence? A forensic analysis of residual artefacts from private and portable web browsing sessions. Proc IEEE Security and Privacy Workshops:135-42, May 2013.