Portable Web Browser Forensics

A forensic examination of the privacy benefits of portable web browsers

Andrew Marrington, Ibrahim Baggili, Talal Al Ismail, Ali Al Kaf
Advanced Cyber Forensics Research Laboratory
Zayed University, College of Information Technology
United Arab Emirates
{andrew.marrington, ibrahim.baggili, m80001181, m80001182}@zu.ac.ae

Abstract—**Portable web browsers are installed on removable storage devices which can be taken by a user from computer to computer. One of the claimed benefits of portable web browsers is enhanced privacy, through minimization of the traces of browsing activity left on the host's hard disk. On the basis of this claim, it would appear that portable web browsers pose a challenge to forensic examiners trying to reconstruct past web browsing activity in the context of a digital investigation. The research examines one popular portable web browser, Google Chrome in both normal and private browsing mode, and compares the forensic traces of its use to forensic traces of the installed version of the same browser. The results show that Google Chrome Portable leaves traces of web browsing activity on the host computer's hard disk, and demonstrate a need for forensic testing of the privacy claims made for the use of portable web browsers.**

Keywords-digital forensics; privacy; portable web browser

I. INTRODUCTION

Web browser forensics is of major importance in the field of digital forensics. The web browser is one of the most ubiquitous ways of connecting to the Internet, enabling users to commit electronic crimes, or assisting in the execution of traditional crimes. Web browser forensics is a part of a larger field of study, known as computer forensics. The goal of computer forensics is to identify, collect, preserve, and analyze evidential data in a manner that preserves the integrity of the evidence collected so it can be used in a legal case. Web browser forensics is concerned with analyzing and extracting evidence related to a user's Internet browsing activities.

In recent years, a new form of web browsers has emerged, and is becoming more popular, due to its ease of use, fast execution, and more anonymous web surfing capabilities, requiring no installation. These new web browsers are known as portable web browsers. These web browsers can be carried on a Universal Serial Bus (USB) stick and used anywhere on any computer requiring no software installation. Additionally, portable browser users prefer them because they can carry with them their favorite bookmarks anywhere they go. Furthermore, corporate computer users who do not have a web browser installed (or whose web browser has been limited by administrators) can now use their portable web browser at the work place, allowing employees to browse the Internet without restrictions in violation of corporate policies and security practices in place.

This experimental research study aimed at investigating the forensic remnants of both installed and portable web browsers. The research questions this research aimed to answer are: Do portable web browsers leave forensic artifacts? What type of artifacts are left by portable web browsers compared to installed browsers? Would the extracted data from an installed browser be identical to the data extracted from a portable one?

This research used an experimental methodology to forensically examine the types of web browsers (installed and portable). The experiment tested the privacy benefits of Google Chrome Portable through forensic analysis of the forensic artifacts left by the portable web browser on the local hard disk, compared to the artifacts left by a normal, installed-version of Google Chrome.

II. RELATED WORK

The web browser is a program that allows users to access web applications and web pages on the Internet. Web browser usage continues to grow as more and more online applications are migrated to the World Wide Web in the form of web applications. A decade ago, email, instant messaging, online chat and file sharing were all primarily performed with custom built applications. Today, the web browser is increasingly the platform employed by users to perform online tasks beyond simply browsing web pages – email is checked in webmail, instant messaging is performed through web applications like Facebook, VoIP and video chats can be conducted through Google's online web application, video is streamed through web applications like YouTube rather than dedicated media players, and so on. Forensic artifacts left by web browsers are therefore relevant to the investigation of all sorts of online activity.

Web browser forensics of a suspect's computer has become an essential component of many computer forensic investigations. It is a common activity in computer forensic investigations because information generated from web browsers can be useful in reconstructing the suspect's online browsing behavior in cases such as possession and distribution of child/illicit pornography, infringement of intellectual property, and improper use of the corporate Internet connection in contravention of the Acceptable Use Policy (AUP).

978-1-4673-5157-7/13/$31.00 ©2013 IEEE.

Web browser forensics is not new in digital forensics research. Due to the fast development in web technologies, web browsers have been adaptive with continuous version releases. This poses a challenge to the digital forensics community in ensuring that they continuously experiment with new web browsers to learn how to forensically analyze their artifacts.

In general, web browsers installed on a Windows computer record the user's web browsing history to the hard disk in some fashion. Research conducted by Jones and Belani described the reconstruction of Internet browsing history with a variety of forensic tools [1]. The techniques described by Jones and Belani identify and extract digital evidence from forensic artifacts left behind on a computer hard drive by installed browsers.

In terms of reconstructing activities with respect to browsing the World Wide Web, the evidentiary areas that have been identified include web browser history, cache, cookies, preferences and the registry. Therefore, investigators need to retrieve data from a combination of locations in order to be confident that they have identified all of the digital evidence relevant to a suspect's web browser usage [2].

Much of the research into the forensic reconstruction of web browser history has been focused on the identification and extraction of forensic artifacts of individual browsers. Pereira's research into the forensic analysis of Firefox 3 described how SQLite databases are employed to store history, bookmarks, cookies and other data in version 3 of Firefox. The research described an algorithm for the recovery of SQLite records which would assist in an investigation of web browser usage of Firefox 3 [3]. Other research has described, for instance, the analysis of forensic artifacts left on a hard disk by Microsoft Internet Explorer [4], and by Apple's Safari (as part of a broader study of Mac OS X forensics) [5]. Unfortunately, as every browser's implementation varies in a number of respects, so will the nature and storage location of their forensic artifacts.

The forensic artifacts of web browser activity may provide digital evidence for a variety of cases. Roussas describes three basic scenarios in which a forensic investigator may be particularly interested in web browsing history [6]:

- User as victim
- User as insider threat
- User as malicious perpetrator

Most cases in which an investigator might be interested in web browsing history can be categorized as a specific instance of one of these three scenarios. As noted earlier, web browsers are used for so much more than simply browsing static web content. Many, if not most, online applications are now available in the form of a web application. Therefore, in addition to specialized tools and techniques being required for an investigation of each individual browser, a forensic examiner may also have to employ specialized tools or techniques to investigate particular types of activities. The different webmail applications each leave different forensic artifacts on different browsers. For example, in experiments conducted by Eleutério and Eleutério, attachment files from an email received using Microsoft Hotmail were recovered on the hard disk when the user received the email through Hotmail using Internet Explorer and Google Chrome [7]. Their experiments suggest that an investigator's ability to retrieve a given forensic artifact depends on the browser, the type of evidence and the webmail service used. Another example is the popular Facebook social networking application, whose instant messaging functionality leaves forensic artifacts in different locations between different browsers, and in different formats depending on the character encoding of messages [8]. The combination of the variety of web browsers and the variety of web applications creates an enormous complexity in the proper forensic analysis of web browser activity, before taking into account any measures undertaken by a user to hide that activity.

The desire for web browsing privacy has led, in recent years, to the creation of private browsing functionality. The motivation for a criminal to use a private browsing feature is to conceal evidence of illicit browsing activity. In related work studying the forensic artifacts of the private browsing modes of installed browsers, Said et al. found that the private browsing modes of the Google Chrome, Mozilla Firefox and Microsoft Internet Explorer browsers all left artifacts in memory. Forensic artifacts of the private browsing session, in the form of deleted files, were also left on the hard disk by Microsoft Internet Explorer. In some experiments, Mozilla Firefox left artifacts on the hard disk in the pagefile.sys file [9]. It seems likely that artifacts in the pagefile.sys file would be left as a result of swaps to virtual memory. We believe that such artifacts might also be left by other browsers (such as Google Chrome), although Said et al. did not find such artifacts in their experiments.

The desire for web browsing privacy has also led to the development of private, portable web browsers. Such browsers are intended for situations where an installed web browser is inappropriate, even with private browsing mode functionality. An installed web browser running on an operating system compromised by malware, for instance, is likely to be compromised by malware itself. For use in such environments, Griffiths and James developed the concept of a web browser designed to run within a secure portable execution and storage environment [10]. This concept was implemented in a modified version of Mozilla Firefox called "Fireguard", which was intended to reduce data leakage from browser data remnants, and the risk of software attacks from malicious code exploiting vulnerabilities in browser plug-ins. Most significantly from a digital forensics perspective, Fireguard was also intended to minimize the forensic footprint of web browser use. There are now several portable web browsers easily available for download on the Internet, including portable versions of Mozilla Firefox, Google Chrome, and Opera, and new browsers designed as portable browsers from the ground-up. This research focuses on the portable versions of the Google Chrome browser.

Past research has shown that web browsers leave data remnants (forensic artifacts) on a hard disk drive, often unbeknown to a user, in the form of cookies, history, saved passwords, cached web pages and downloaded objects. These have been important evidentiary sources for digital forensic investigations. With the release of the portable web browser, which does not require installation, an important question arises: Do portable web browsers leave similar forensic artifacts to those left by installed web browsers? This work attempts to answer that question.

III. METHODOLOGY

To answer the question "Do portable web browsers leave similar forensic artifacts to those left by installed web browsers?", we designed a simple experiment. We regarded that an experimental methodology was required because not all of the source code for either the browsers nor the portable application framework for those browsers is available publicly. Google Chrome, for instance, is based on the open source Chromium project, but contains additional code which is not available publicly. Further, an experimental methodology is easy to generalize from the specific cases of the browsers examined in this paper to other browsers altogether. This facilitates forensic examiners confronted with a digital investigation potentially involving another portable browser from those discussed here to replicate our experiment in order to obtain comparable results, rather than have to analyze voluminous source code or run binary code through debuggers.

Three similar simple web browsing sessions were carried out with the Google Chrome browser, using the portable and installed versions. The objective of this experiment was twofold: first, to determine the privacy benefits of using a portable browser (Google Chrome) over an installed browser, and second, to determine the additional privacy benefits of using the private browsing mode of a portable browser (Google Chrome's "Incognito" mode). In other words, the experiment tested whether the forensic footprint of the Google Chrome web browser is reduced in the portable version from the installed version, and whether that footprint is further reduced by private browsing mode. The instruments and the methodology are outlined in the section that follows.

A. Instruments

The web browsing sessions were carried out on IBM Thinkpad T42 laptops freshly imaged with an institutional standard operating environment based on the Windows XP SP 3 32-bit operating system. The laptops each had one physical hard drive with a maximum capacity of 40GB.

The web browsing sessions were carried out with Google Chrome version 16.0.912.63. For the portable browsing session, Google Chrome Portable was installed on a brand new, blank 4GB Lexar USB thumb drive.

The forensic acquisition was carried out with AccessData FTK Imager version 3.1.0. The analysis was performed with AccessData Forensic Tool Kit (FTK) 3.0. As we intend for our experiment to be easily replicated by digital forensic scientists in the field who need to define the behavior of other portable browsers, we decided to employ software which will already be present in many digital forensics laboratories.

To ensure the integrity of the source drives through-out the imaging process, we employed hardware write blockers which ensured that no data were written to the source disks during acquisition. We used two write blocker devices, one Tableau eSATA Forensic Bridge (for the laptop hard disk) and the other Tableau USB Forensic Bridge (for the USB thumb drive). A Tableau 2.5" Hard Drive Adapter (Model TDA5-25) was also used to plug laptop hard drive into the write blocker.

B. Experiment

1) Portable Google Chrome Session (normal)

a) Setup

The laptop was freshly imaged with the institutional standard operating environment. After booting, the USB drive containing the Google Chrome Portable installation was inserted into the laptop. The browser was started by clicking on "My Computer", then selecting the USB drive, navigating to the "Google Chrome" folder, and launching the application.

b) Web Browsing Session

A short web browsing session was performed, following the steps and performing the activities described in the scenario design, below. After the browsing session, the computer was shut down and disconnected from the power.

c) Acquisition

The laptop's hard disk and the USB drive were both removed from the powered down computer. Both the hard disk and the USB drive were plugged into the appropriate write blocker device. An image of each disk was created using FTK Imager in Advanced Forensic Format (AFF) [11], with maximum compression enabled (to better facilitate distribution). The images were subsequently converted (again using FTK Imager) to raw dd format for analysis.

2) Portable Google Chrome Session (incognito)

a) Setup

A new laptop (of identical make, model and specification) was freshly imaged with the institutional standard operating environment. After booting, the USB drive containing the Google Chrome Portable installation was inserted into the laptop. The browser was started by clicking on "My Computer", then selecting the USB drive, navigating to the "Google Chrome" folder, and launching the application.

b) Web Browsing Session

After Google Chrome was launched, a private browsing window was opened by clicking on the options button, then on "New incognito window". The original window was closed. A short web browsing session was then performed in the incognito window, following the steps and performing the activities described in the scenario design, below. After the browsing session, the computer was shut down and disconnected from the power.

c) Acquisition

The laptop's hard disk and the USB drive were both removed from the powered down computer. Both the hard disk and the USB drive were plugged into the appropriate write blocker device. An image of each disk was created using FTK Imager in Advanced Forensic Format (AFF) [11], with maximum compression enabled (to better facilitate distribution). The images were subsequently converted (again using FTK Imager) to raw dd format for analysis.

3) *Installed Google Chrome Session*

a) *Setup*

The laptop's hard disk was forensically wiped (by overwriting all sectors several times) and re-imaged. This ensured that no artifacts from the first web browser session (the portable web browser session) remained when the second session was performed. After booting, Google Chrome was downloaded (using Internet Explorer), and installed. The application was then launched from the Start Menu.

b) *Web Browsing Session*

A short web browsing session was performed, following the same steps and performing the same activities as in the previous session. The scenario is described below. After the browsing session, the computer was shut down and disconnected from the power.

c) *Acquisition*

The laptop's hard disk was removed from the powered down computer. The hard disk was plugged into the write blocker, and an image was created just as for the previous session.

4) *Usage Scenario*

The same scenario was created for both the installed and portable web browsing sessions. The scenario consisted of:

- Watching videos on Youtube.
- Searching for images on Google Image Search.
- Browsing items on eBay.

Table 1 shows the websites visited, a description of the activities performed on each website, and keywords used in subsequent forensic analysis to search for artifacts of that activity.

TABLE I. WEB BROWSER USAGE SCENARIOS

User scenarios performed		
Website	***Activities***	***Evidence keywords (Chat, Files, Words)***
www.youtube.com	-Searching for "Trikke" -Searching for "Parkour" -Viewing several of the search results	"Trikke" "Parkour"
images.google.com	-Searching for "Dodge Viper" -Searching for "Mini Cooper" -Viewing several of the search results	"Dodge Viper" "Mini Cooper"
www.ebay.com	-Searching for "BlackBerry Playbook" - Searching for "Galaxy i9100" -Browsing through lists of items	"Playbook" "Galaxy"

5) *Analysis*

The analysis was performed using FTK. Each image file (in raw format) was added to an FTK case. A keyword search was then performed using FTK's "Live Search" function, for the keywords in Table 1. The results of this search are outlined in the section that follows.

IV. RESULTS

In this part of the experiment, Google Chrome was tested in its two forms, portable and installed. Keywords were found on all three images acquired. Table 2 is a summary of results for the three images.

TABLE II. KEYWORD SEARCH RESULTS

Keyword	**Keyword hits found on image?**				
	Installed Session HDD Image	***Portable Session HDD Image***	***Portable Session USB Image***	***Portable Incognito Session HDD Image***	***Portable Incognito Session USB Image***
Trikke	Yes	Yes	Yes	Yes	Yes
Parkour	Yes	Yes	Yes	Yes	Yes
Dodge Viper	No	No	Yes	Yes	Yes
Mini Cooper	Yes	Yes	Yes	Yes	Yes
Playbook	Yes	Yes	Yes	Yes	Yes
Galaxy	Yes	Yes	Yes	Yes	Yes

Although keywords were found on all images, it should be noted that the quantity and location of keyword search hits differed (although not significantly) between images. In the case of the portable session hard disk images, many hits were found in unallocated space (i.e. the files had been deleted) or in the *pagefile.sys* virtual memory swap file, but were not overwritten prior to the forensic acquisition of the disk.

Overall, the installed session hard disk image yielded more keyword hits than the portable session hard disk images, but both portable session hard disk images included traces of the suspect web browser usage, including the "Incognito" session.

The files in which keyword hits were found were stored under the same directory for each image. In most cases, the files containing the keyword hits were stored within further subdirectories. Table 3 lists the "parent" directory of the files containing the keywords for each of the three images. Of most interest, from a privacy perspective, is the use of the "Local Settings\Temp" directory under the user's home directory by Chrome Portable (normal browsing session). This indicates that Google Chrome Portable is writing to the temporary directory on the hard disk rather than use a temporary directory on the USB drive. Users might reasonably expect that Chrome Portable would store its temporary files on the removable storage device rather than the local hard disk.

Said et al. report that Google Chrome's "Incognito" private browsing function has a very small forensic footprint [9], and we expected that to also be true of Chrome Portable in "Incognito" mode. Table 3 shows that all evidence of the "Incognito" browsing session was found on the hard disk image's *pagefile.sys* virtual memory swap file. For the sake of completeness, we should add that some of the keyword hits also appeared in unallocated space on the “Incognito” browsing session’s hard disk image, but further examination showed that these hits were generated by unrelated dictionary files, and should therefore be discounted.

TABLE III. FORENSIC ARTIFACT LOCATIONS

Image	Location
Portable Session HDD	`\Documents and Settings\Administrator\Local Settings\Temp\GoogleChromePortable`
Portable Session USB	`\GoogleChromePortable\Data\profile\Default` and drive free space
Portable Incognito Session HDD	`pagefile.sys`
Portable Incognito Session USB	Drive free space only
Installed Session HDD	`\Documents and Settings\Administrator\Local Settings\Application Data\Google\Chrome\User Data`

V. DISCUSSION

The results show that forensic traces were still recoverable for both installed and portable versions of the Google Chrome web browser, and even for the portable version browsing in “Incognito” mode. Consequently, the assumption that using a portable web browser is a guarantee of privacy is not true because our results show that, at least for Chrome Portable, forensic artifacts in the form of cookies, history, saved passwords, and cached web pages can be found on the hard disk even after USB drive containing the portable browser has been removed. Users may believe that surfing the Internet with a portable web browser would leave no forensic footprint on the local hard drive, but our experiments show otherwise.

For practical purposes, there is no significant difference between using the installed or portable version of Google Chrome in normal browsing mode. Both versions leave plenty of evidence on the hard disk of the host machine which can easily be recovered using conventional digital forensic practices. Although our results showed a small decrease in the number of keyword hits on the hard disk images for the Chrome Portable normal browsing session as compared to the installed version’s session, the evidence remaining would be more than enough for an investigator to reconstruct the browser session.

The “Incognito” browsing mode of Chrome Portable leaves no traces on the host hard disk image except in the virtual memory swap file. The accurate hits in the *pagefile.sys* may appear to be of privacy concern to the portable web browser user, but in reality, the risk that evidence would be recovered from this swap file would decrease dramatically the more time elapsed between forensic acquisition and the initial web browser session. The virtual memory swap file is overwritten frequently, and once overwritten the evidence is difficult if not impossible to retrieve. Further, whether or not the host computer would even write such searches to the *pagefile.sys* file depends largely on the amount of physical RAM installed on the computer, the size of the swap file, and the number of active processes. Even under similar circumstances on identical computer systems, the behavior of Windows XP’s virtual memory management is relatively difficult for a user to anticipate. This is illustrated by our own experiment, where no occurrences of the “Dodge Viper” keyword were found on images taken from the normal browsing mode sessions (installed and portable alike), but the keyword was found in the *pagefile.sys* in the Incognito session’s image. With these qualifications then, our results show that if a forensic acquisition is performed soon after the web browser session being investigated, then evidence can be retrieved even from Google Chrome Portable in Incognito mode, but perhaps not consistently.

VI. CONCLUSION AND FUTURE WORK

If the intention of using portable web browsers is to hide traces of browsing, or simply to have a greater sense of privacy, then it is an intention at best only partially realized in the version of Google Chrome Portable we tested. Users who use Chrome Portable with the intention of obscuring their browsing activity from forensic examination should be aware that traces of their browsing activity will be left behind on the hard disk of the computer, despite their browser being on a removable storage device.

Although our experiment was confined to Chrome Portable, users of other portable browsers should not make the mistake that their privacy is assured. The key conclusion we draw from our results is that the privacy claims of portable web browsers should be forensically tested before being accepted. Uncritical acceptance of similar privacy claims made on behalf of other portable web browsers would be foolhardy.

Further forensic testing of portable web browser privacy is required. Our future research into portable web browser privacy will involve forensic testing of other leading portable web browsers, including Firefox and Opera. Our objective is to establish, for all freely available portable web browsers, whether digital forensic investigators can find traces of web browser activity left behind on a computer’s hard disk after the use of each portable web browser in private browsing mode.

ACKNOWLEDGMENT

We would like to acknowledge the invaluable laboratory assistance of our colleague N. Chandrashekaran.

REFERENCES

[1] K.J. Jones, and R. Belan (2010), “Web Browser Forensics,” *Security Focus* [Web Document]. Retrieved 26 May 2011 from http://www.securityfocus.com/infocus/1827.

[2] Junghoon O., Seungbong L., Sangjin L. (2011, Aug.), “Advanced evidence collection and analysis of web browser activity,” *Digital Investigation.* 8, pp. S62-S70. Available: doi:10.1016/j.diin.2011.05.008.

[3] M.T. Pereira (2009, Mar.), “Forensic analysis of the Firefox 3 Internet history and recovery of deleted SQLite records”, *Digital Investigation*, vol. 5, no. 3-4, pp. 93-103. Available: 10.1016/j.diin.2009.01.003.

[4] K.J. Jones (2003), “Forensic Analysis of Internet Explorer Activity Files”, [Web Document]. Retrieved 22 December 2011 from http://nys.fd.org/cja/forensics/ieactivity.pdf.

[5] P. Craiger and P. Burke (2006), “Mac OS X Forensics,” *Advances in Digital Forensics II*, M. Olivier and S. Shenoi, Eds. Springer, pp. 159-170.

[6] G. Roussas, “Visualization Of Client-Side Web Browsing And Email Activity,” M.S. thesis, Naval Postgraduate School, Monterey, CA., 2009.

[7] P.M.S. Eleutério, J.D.A.S. Eleutério, “Webmail evidence recovery: a comparison among the most used Web browsers and webmail services,” *Proc. 6th Int. Conf. Forensic Computer Science,* Florianópolis, 5-7 October 2011, pp. 182-189.

[8] N. Al Mutawa, I. Al Awadhi, I. Baggili, and A. Marington, “Forensic artifacts of Facebook’s instant messaging service,” *Proc. 6th Int. Conf. Internet Technology and Secured Transactions,* 11-14 December 2011, pp. 771-776.

[9] H. Said, N. Al Mutawa, I. Al Awadhi, and M. Guimaraes, “Forensic analysis of private browsing artifacts,” *Proc. 2011 Int. Conf. on Innovations in Information Technology (IIT),* Abu Dhabi, 25-27 April 2011, pp. 197-202.

[10] D. Griffiths, and P. James, “Fireguard - A Secure Browser with Reduced Forensic Footprint”, *Proc. 8th Australian Digital Forensics Conference*, Perth, 30 November 2010, pp. 75-91.

[11] S. Garfinkel, “AFF: A New Format for Storing Hard Drive Images”, *Commun. ACM*, vol. 49, no. 2, pp. 85-87, February 2006.