The Privacy of Private Browsing

Ashley Hedberg[1]
ashley.hedberg@tufts.edu

[1] *Mentor:* Ming Chow, Tufts University

Abstract

Most modern web browsers have a “private browsing” mode that supposedly allows a user to surf the internet without leaving any traces of his or her activity on his or her machine. However, the notion of “private browsing” offers users a false sense of security, as browsing information is often left behind when a private browsing session terminates. Several researchers have already demonstrated methods of detecting this information. These include the analysis of virtual and browser memory and the pagefile on Windows machines. The existence of private browsing artifacts on a users machine raises many questions: how much privacy do web browser developers actually aim to provide with “private browsing” modes? Are these goals accurately conveyed to the end user? And, if the users browsing session can be reconstructed from these artifacts, how might this be exploited by digital forensics professionals? This paper seeks to answer these questions and to prove that such artifacts can be used to determine, at least in part, what a user was doing during his or her “private browsing” session—thereby rendering it not very private at all.

1 Introduction

1.1 Browser Overview

Currently, the most popular browsers for the Windows family of operating systems are Mozilla Firefox, Google Chrome, and Microsoft Internet Explorer. All three of these browsers have built-in private browsing modes. The features and protections provided by each of these private browsing modes are summarized below.[1][2][3]

	Firefox Private Browsing	Chrome Incognito Mode	Internet Explorer InPrivate Browsng
Browser history	X	X	X
Form data	X		X
Search bar data	X		X
Passwords	X		X
Downloads	X	X	
Cookies	X	X	X
Cached files	X		X
Simulataneous sessions with different privacy settings	X	X	X

1.2 What Private Browsing Is Not

The private browsing modes of Firefox, Chrome, and Internet Explorer are designed with the intent of preventing users of the same computer from determining what someone was doing on that computer. They do not attempt to keep a user's internet activities hidden from that user's internet service provider (ISP), and they do not prevent websites from identifying that user.[1][2][3]

2 To the Community

There are many misconceptions about private browsing. Some believe that it prevents an internet service provider, network administrator, or attackers engaged in packet sniffing from linking a user's internet activities to his or her identity. It does not. Any and all network packets leaving the user's machine contain information such as the user's IP address, which can be used to determine his or her location and/or identity. Others think that private browsing sessions leave absolutely no trace of their activities on their local machines. As the next section of this paper will describe, this is also false. Still others think that private browsing will prevent the National Security Agency from tracking them on social media. It certainly does not. This paper will shed some light on what private browsing sessions can and cannot do, allowing internet users to think twice before exploring the web.

3 Applications: Forensics

One of the biggest problems with private browsing sessions is that artifacts remain on a machine after the user exits his or her internet browser. These artifacts can include logon information for websites, browsing history, and digital media such as images and videos—all items that you would expect a private browsing session to keep private.[5]

This section will first summarize locations on a Windows machine where private browsing artifacts might be found. An overview of what specific artifacts were found for each browser using different forensic techniques will follow. The use of SQLite to investigate specific browser artifacts will then be discussed.

3.1 Where To Look

Focused analysis of the hard drive itself can reveal the most artifacts. One private browsing experiment in which logon information, browser history, and cached images were recovered obtained most of the artifacts from portions of the hard disk known as *free space* and *slack space.*[5] Free space refers to a group of hard drive sectors (called a *cluster*) that is not allocated to any particular file. Slack space,on the other hand, refers to the space between the end of a file and the end of the cluster in which it is stored. Hard drive clusters are of a fixed size determined by the operating system. Most of the time, when a user saves a file to his or her hard drive, the file is not exactly the same size as the cluster in which the operating system puts it. Furthermore, when a user “deletes” a file from his or her hard drive, the file is not really deleted—it is simply marked as available to be overwritten if necessary. If a file is eventually stored on the hard drive in a cluster that used to be home to a larger (now “deleted”) file, leftover data from the old file will still exist at the end of that cluster.

Artifacts can also be recovered from the computer’s memory itself. Cached web documents can often be found here.[5] Browsing history, logon information, and cookies have been detected after private browsing sessions by analyzing a computer’s memory. The SQLite databases used by Chrome and Firefox during browsing sessions are generally only stored in memory when private browsing is in use, and their residual data could be detected, as well.[6]

The Windows pagefile can also reveal private browsing artifacts. This file is where the least recently used pages of memory are stored when too many applications are competing for the computer’s physical memory. Browsing history and keywords used in internet search engines have been discovered here.[7]

3.2 Firefox

3.3 Google Chrome

3.4 Internet Explorer

Internet Explorer leaves the most artifacts behind when its InPrivate Browsing mode terminates.[5]

3.5 Forensic Software

4 Conclusion

With all the ways in which private browsing modes can leak information, it may seem as though they are completely useless. This is not entirely true. While private browsing sessions won't help anyone evade law enforcement, a forensic investigation, or the United States government, they are still good enough to fool most computer users. Nosy roommates, family members, or patrons at the public library are unlikely to go to the lengths discussed in this paper to determine what someone else was doing on the internet.

That said, private browsing modes don't do much to keep a user's identity private to the outside world. Users seeking this kind of anonymity should consider using the Tor browser, which employs onion routing to connect them to their destination server. In this type of routing, a random path from the user to the destination is constructed, and content is encrypted at each point in the path. Furthermore, each point (known as a relay or node) only knows from which relay any given piece of network traffic immediately came and the next relay to which it is going. It does not know the original source of the network traffic or its final destination. This is what allows users to keep themselves and their activities anonymous using Tor in a way that the traditional web browsers cannot.[4] Of course, this type of browsing can be (ab)used for a whole host of illicit activities, but those are beyond the scope of this paper.

Until Mozilla, Google, and Microsoft reduce the artifacts leaker by their respective browsers' private modes, users who are concerned about "local attackers"—those of the nosy roommate or family member variety who have physical access to their machine—can do their part to keep their private information secure. Random access memory, where private browsing artifacts have been found, is cleared when a computer is powered down. Shutting down the computer after a private browsing session can reduce or eliminate these artifacts. Hard drive artifacts, however, are nearly impossible to eradicate. The moral of the story is that private browsing is nothing more than a nice illusion useful for fooling the computer-illiterate. At the end of the day, private browsing really isn't that private at all.

References

[1] Verdi, Michael et al. "Private Browsing." *Mozilla Support.* Mozilla Foundation, 29 Mar. 2013. Web. 10 Dec. 2013. <`http://support.mozilla.org/en-US/kb/`

private-browsing-browse-web-without-saving-info>.

[2] "Chrome Browser." *Chrome*. Google, 18 Nov. 2013. Web. 10 Dec. 2013. <http://www.google.com/intl/en/chrome/browser/features.html#privacy>.

[3] "InPrivate Browsing." *Microsoft Windows*. Microsoft, 10 Dec. 2013. Web. 10 Dec. 2013. <http://windows.microsoft.com/en-us/internet-explorer/products/ie-9/features/in-private>.

[4] "Tor Project: Overview." *Tor*. Tor, 7 Dec. 2013. Web. 10 Dec. 2013. <http://www.torproject.org/about/overview.html.en>.

[5] Ohana, Donny, and Narasimha Shashidhar. "Do Private and Portable Web Browsers Leave Incriminating Evidence? A Forensic Analysis of Residual Artifacts from Private and Portable Web Browsing Sessions." IEEE CS Security and Privacy Workshops (SPW), The Westin St. Francis, San Francisco, CA. 23-24 May 2013. Web. 9 Dec. 2013. <http://www.ieee-security.org/TC/SPW2013/papers/data/5017a135.pdf>

[6] Satvat, Kiavash, Matthew Forshaw, Feng Hao, and Ehsan Toreini. "On The Privacy of Private Browsing - A Forensic Approach." Proceedings of the 8th International Workshop on Data Privacy Management (DPM '13), Royal Holloway, University of London, Egham, UK. 12-13 Sept. 2013. Web. 9 Dec. 2013. <http://homepages.cs.ncl.ac.uk/feng.hao/files/DPM13.pdf>

[7] Said, Huwida, Noora Al Mutawa, Ibtesam Al Awadhi, and Mario Guimaraes. "Forensic Analysis of Private Browsing Artifacts." 7th International Conference on Innovations in Information Technology, Abu Dhabi, United Arab Emirates. 25-27 Apr. 2011. Web. 10 Dec. 2013. <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=5893816>