ZULFAQAR Journal of Defence Science, Engineering & Technology
e-ISSN: 2773-5281
Vol. 3, Issue 1 (2020)
DOI: https://doi.org/10.58247/jdset-2020-0301-03
Journal homepage: https://zulfaqarjdset.upnm.edu.my

A STUDY ON PRIVATE BROWSING IN WINDOWS ENVIRONMENT

Yamunah Kathiravan[a,*], Mohd Fahmi Mohamad Amran[a], Noor Afiza Mat Razali[a], Mohd Afizi Mohd Shukran[a], Norshahriah Abdul Wahab[a], Mohammad Adib Khairuddin[a], Mohd Nazri Ismail[a], Zuraidy Adnan[a], Muhammad Fairuz Abd Rauf[a]

[a] Department of Computer Science, Faculty of Science and Defence Technology, National Defence University of Malaysia, Sungai Besi Camp, 57000 Kuala Lumpur, Malaysia

ARTICLE INFO

ARTICLE HISTORY
Received: 01-02-2020
Revised: 30-03-2020
Accepted: 15-05-2020
Published: 30-06-2020

KEYWORDS
Private browsing
Browser artefacts
Privacy
Computer privacy

ABSTRACT

Privacy has always been a constant concern for many people. Internet users are often worried about the browsing information that is left on their storage media. Web browsers were later introduced with a new feature called private browsing to overcome this issue. The private browsing mode is expected to behave as normal browsing session but without storing any data such as browser cookies, history, cache and passwords on the local machine. Unfortunately, previous researchers concluded web browser often failed to provide the intended privacy protection to their user. Along the way of this reviewing process, the weakness and downside of previous web browser vendors have been identified.

1.0 INTRODUCTION

The web browser has been a common task to run on personal computers regardless of whether for work, study, or leisure. Users use a web browser to perform a variety of functions such as checking e-mail, online banking, social network sites, information searching, and many more. Web browser tends to record every bit of data related to the user's activity on the local machine. According to [1], this data focuses on traces regarding visited URLs, cached Web pages, and keywords used in search engines or forums, cookies, username, password, or more commonly known as browsing artefacts. So, the longer the user uses a browser, the more browsing artefacts are generated and stored locally in the machine. These files can easily be obtained by anyone who has access to the same machine. Even if the user uses some third-party PC cleaning tools to wipe out the browser data, the files can still be accessed from computer forensic tools [2]. Current browsers have focused more on encrypted network traffic rather than protecting the data produced by the browser on the local machine. Most of the browser artefacts are recoverable in RAM, slack space, and Orphaned directories. This data is enough to provide useful information about a user [1]. Browser artefacts such as username, electronic browsing history, images, and videos, may contain significant evidence to a computer investigator as well as a hacker. A recent statistic by SC Magazine since 2006 shows that nearly 14% of data breaches due to employees' accidental disclosure and around 25% due to lost or stolen devices [3].

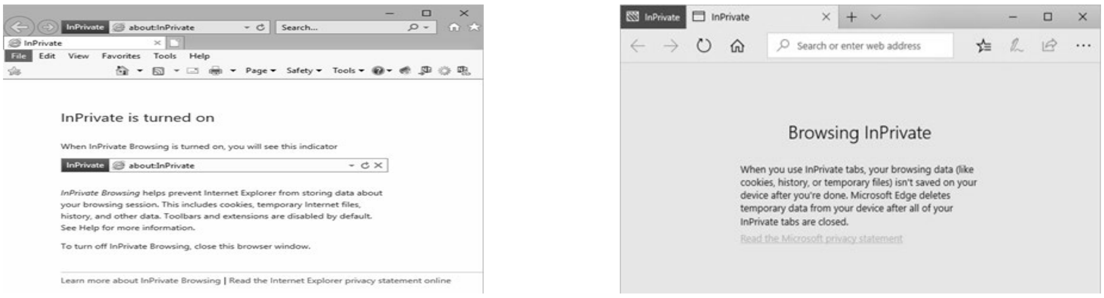
Privacy browsing has been a notable protection feature since 2005, which is included in almost all browsers. These browsers claim this mode is to surf the web without leaving any trace on the user's computer [4, 5]. Apple's Safari was the first browser with private browsing that allows a user to surf the Internet without leaving any data on the hard disk drive [6]. As of late, forensic investigators play an essential role to recover these data by using forensic tools and techniques [7]. Furthermore, researcher [8] said that private browsing had been proven not to deliver the security as they ensure they would, therefore, encouraging researchers to analyse the browser artefacts of Private Browsing mode in different forms, either using local machines or virtual machines to examine the feature [9]. Like every other web browser cryptography project out there, the focus has always been securing the browser's

*Corresponding Author | Khatiravan, Y. | yamunah@icloud.com network traffic. Encryption secures the data that is stored on and between physical assets, computers, databases, servers, etc. The real problems as to why there still has not been a cryptography-based web browser are because current browsers are lacking the basic cryptographic primitives. The most well-known problem is the lack of cryptographic secured random number generator and efficient implementation of key stretching algorithms. Encryption includes generating a random symmetric key and running encryption with a keyword in access policy string [10]. Access control and encryption secure the data on disk drives [2]. Available encryption modes include cipher block chaining, various counter modes with location-dependent IV, location-tweaked electronic codebook or wide-block encryption. Advanced Encryption Standard-128 or AES-256 are probably the best choices for the underlying cipher.

2.0 PROPOSED METHOD

As the concern of privacy is rising, browser vendors have built private browsing mode to prevent tracking and accessing user's information. This feature can avoid websites or prevent offenders from tracking individuals while surfing the web or even storing the browser cache and history list on the individual's computer hard disk [11]. An ordinary user usually sees private mode as a feature that could enhance their privacy protection on the user's browsing activities compared to public browsing mode [10, 12]. However, it is up to the web browser companies to characterize what these extra privacy protections are, and some of them may not fulfil a user's expectation of privacy needs [13]. Unfortunately, implementations of private browsing mode still allow sensitive information to leak into persistent storage [14]. In 2005, Apple introduced the private mode feature in Safari 2.0. Private mode is casually known as "porn mode," as some users to some adult browsing without worrying about potential embarrassing pornographic links appearing on the user's suggestion tabs [15, 16]. A few years later, Google Chrome 1.0 implemented its own private mode version, which is known as "Incognito." The following year, Internet Explorer 8 and Mozilla Firefox 3.5 both added this feature to their browser, known as InPrivate and Private Browsing, respectively [17]. Private browsing mode has been included under various names in every standard browser, to remove all data that prompt offenders to gain information on the user's private browsing activity [18]. Once the private session is closed, the browser deletes all cache, browsing history, cookies, usernames, passwords, and other data from the hard disk [19].

One of the most popular research projects on private browsing [14] has stated that most web browsers failed in some way or another concerning private browser policies, because of browser extensions and plugins. Their work completed on private browsing in three most mainstream browsers (Firefox, Chrome, Internet Explorer) utilizing open-source tools, which proved IE of violating the privacy of In-Private mode. The researcher examined the allocated space, unallocated space, and physical. IE was successful in recovering all traces, whereas Mozilla Firefox and Google Chrome were not able to reveal any data from the hard disk. However, quite a few artefacts were recovered in Google Chrome from RAM after the browsing session [18]. Not only IE, but the Microsoft Edge browser [20] has also been reported of leaving an excessive amount of readable evidence on the local machine while in In-Private mode. This mode is often characterized as the element that does not write any information about a user's current session. The objective of this mode is to preclude any information being stored to the disk [21]. Although web browser vendors claim that private browsing is secure and information during a browsing session will not be saved on the local machine, this researcher has proved that artefacts can be recovered. Fig. 1 illustrates the user interfaces of private browsing modes of four popular browsers used in the Windows operating system; Internet Explorer, Microsoft Edge, Firefox, and Google Chrome.



InPrivate is turned on

When InPrivate Browsing is turned on, you will see this indicator

InPrivate Browsing helps prevent Internet Explorer from storing data about your browsing session. This includes cookies, temporary Internet files, history, and other data. Toolbars and extensions are disabled by default. See Help for more information.

To turn off InPrivate Browsing, close this browser window.

Learn more about InPrivate Browsing | Read the Internet Explorer privacy statement online

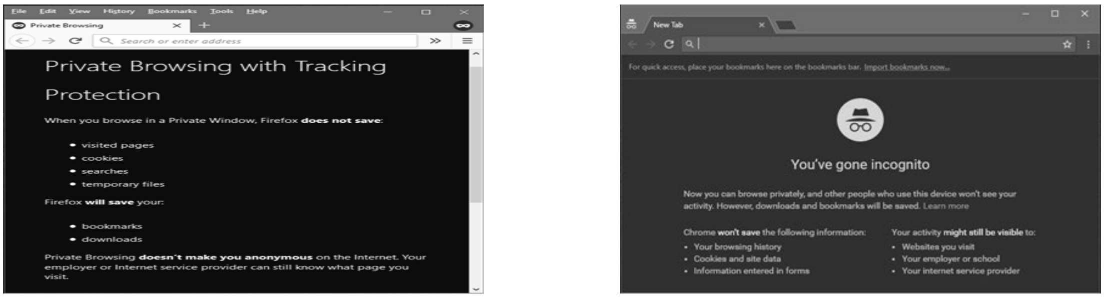
(a) Internet Explorer 11

Browsing InPrivate

When you use InPrivate tabs, your browsing data (like cookies, history, or temporary files) isn't saved on your device after you're done. Microsoft Edge deletes temporary data from your device after all of your InPrivate tabs are closed.

Read the Microsoft privacy statement

(b) Microsoft Edge



Private Browsing with Tracking Protection

When you browse in a Private Window, Firefox **does not save**:

- visited pages
- cookies
- searches
- temporary files

Firefox **will save** your:

- bookmarks
- downloads

Private Browsing **doesn't make you anonymous** on the Internet. Your employer or Internet service provider can still know what page you visit.

For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...

You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome **won't save** the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity **might still be visible** to:

- Websites you visit
- Your employer or school
- Your internet service provider

(c) Firefox (d) Google Chrome

Figure 1. Indications of private browsing mode

3.0 RELATED STUDIES

This section reviews similar approaches by other researchers. Six related types of research were studied and analysed in order to understand the current problem of private browsing and to propose a better methodology for this research.

Table 1. Summary of studied research

Tested Machine	Operating System	Targeted Web Browser	Imaging	Computer Forensic Tools	Ref
Local Machine	Windows XP	Internet Explorer, Firefox, Chrome	Hard Disk RAM	FTK Imager, WinHex, Cache & History viewer, EnCase	[17]
Local Machine	Windows 7	Internet Explorer, Firefox, Chrome, Safari	Hard Disk (Specific files) RAM	Tableau USB Write Blocker, Daemon FS, Nirsoft Internet Tools, AccessData FTK	[22]
Virtual Machine	Windows XP	Internet Explorer, Firefox, Chrome, Safari	RAM	Memory Parser	[23]
Virtual Machine	Windows 7	Internet Explorer	Hard Disk (Specific files)	ShadowCopy, WinHex	[24]
Not Mentioned	Windows XP, Windows 7, Windows 8, Linux	Internet Explorer, Firefox, Chrome, Safari	Hard Disk RAM	Belkasoft, RAM Capturer, Magnet Internet Evidence Finder	[25]
Virtual Machine	Windows 7	Internet Explorer, Firefox, Chrome, Safari	Hard Disk (Specific files) RAM	WinHex, Index.dat analyser, SQLite Browser, SQLite Manager	[4]

One of the prominent studies done on private browsing is by Said et al. [17] who conducted their research on three local machines with three different web browser vendors: Mozilla Firefox, Google Chrome and Internet Explorer, during its Private Mode session in the search for any traces of residual data. As for the result, the researcher reported that the artefacts from each private browsing session were recoverable in the main memory. The researcher was able to retrieve several entries for each string search in Mozilla Firefox. Google Chrome and Internet Explorer both had almost similar results. There were several traces of private data, including password, cookies and history. Another research by Ohana et al. [22] tested their method on both private and portable web browsers. They performed a forensic investigation on RAM with three web browsers: Internet Explorer, Mozilla Firefox, Google Chrome, Safari, and Opera. They decided for portable browsers, recovering evidence from RAM would be the best option. Their experiment revealed that Chrome and Firefox did not write any data to the file system, while data about the private session in Internet Explorer was recovered majority from RAM, slack space, and FTK (Orphan) directories. In this research by Mahendrakar et al. [23], four web browsers were chosen; Mozilla Firefox, Google Chrome, Internet Explorer, and Safari. They created a dummy website that requested various types of data and used their memory parser tool to extract. Their result shows that all four browsers saved information of the private browsing session. However, Safari had successfully detained more information than other browsers. Malmström et al. [24] focused on Internet Explorer 10 and found that InPrivate browsing sessions are recoverable, as the Extensible Storage Engine (ESE) database deletes the private session records after the session is ended by the user which exists on the local hard disk until it is overwritten with other data which proved IE of violating the privacy of InPrivate mode.

Satvat et al. [4]'s justification for using Virtual Machines (VM) was to prevent any cross-examination experiments conducted on other web browsers. Their experiment also includes inspecting the content of RAM after browsing in private mode and closing the session. Both locations were successful in discovering traces of private browsing and pointed out that vendors failed to achieve this goal. The experiment in Noorulla [25] showed the data that could be left by using private browsing mode in Internet Explorer, Mozilla Firefox, Google Chrome, and Safari. The researcher's finding was no different than [17]. Internet Explorer had stored data on the local machine and was recoverable using recovery tools even after the database deletes it. Safari, however, writes and stores visited URLs in its' database and does not delete them. The only way is for the user to manually delete the Webpageicon.db file to get rid of the entire browsing history. The six studies have been reviewed and analysed has proved that there is a lack of capable private web browsers in hiding the browsing artefacts as claimed. Table 1 shows a summary of the six related studies. Almost all research that has been conducted in private browsing has almost similar results. Researchers have implied to conduct more experiments in this area as browsing activities could be potential evidence in a digital forensic investigation.

4.0 IMPLICATION

The private browsing mode is a valuable feature for users who wish to browse without leaving any traces of data. Now, private browsing functionality of common browsers has successfully achieved one of the objectives, which are to browse without being detected [9], [26]. However, researchers [4] and [7] both mentioned in their research that there might be some loopholes about this feature. The browser could leave some information behind regarding the user's private browsing session. Through thorough examination, researcher [22] has concluded that every browser has the intention to record its browser artefact in the operating system but later wipes them after the session has ended.

Table 2: Web browser artefacts storage

Browsers	Artefacts storage location
Internet Explorer	Cookies (Index.dat), History (Index.dat), Registry (typed URLs, search queries, autocomplete, protected storage), NTUSER.dat, Temporary Internet Files and Index.dat Entries, Downloads
Firefox	Sqlite database structure, Prefs.js, Signons.txt, Formhistory.sqlite, Cookies.sqlite, Firefox.cache, Places.sqlite, Downloads.sqlite
Chrome	JSON, Downloads, Bookmarks, Web data, Keyword search terms, Keywords, URL database, History index, Current and last session, Top sites database

These browsers commonly store the following browsing data on the local hard disk:

- Browsing History: Contains mainly typed URLs, redirects and also the number of visited sites.
- Bookmarks: Contains shortcuts or bookmarks created to specific websites.
- Cookies: Created by web sites that are stored on user's computer hard drive when the user visits a site. Vital information like username, passwords and web session can be found here.
- Cache: Temporary location on the disk which is used to store most recently visited web sites.
- Favourite folder: Contains URL's sites.

Table 2 shows the type of browser artefacts stored reviewed from the six research articles based on Windows operating system. The locations of the web browser artefacts stored in the Windows operating system are shown in Table 3. This is essential for investigators as it decides to locate and examine the browser artefacts produced during the normal and private browsing mode.

Table 3. Directory of web browser artefacts in Windows OS

Internet Explorer	
Location within *%userprofile%\AppData\Local\Microsoft\*	
History	…\Windows\History\
Cache	…\Windows\WebCache\
	…\Windows\Temporary Files\Content.IE5\
	…\Windows\ Temporary Files\Low\Content.IE5\
Location within *%userprofile%\AppData\*	
Cookies	…\Roaming\Microsoft\Windows\Cookies\
	…\LocalLow\Microsoft\Internet Explorer\DOMStore\

Firefox	
Location within *%userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles*	
History	…\<random text>.default\places.sqlite
Cookies	…\<random text>.default\cookies.sqlite
Location within *%userprofile%\AppData\Local\Mozilla\Firefox\Profiles*	
Cache	…\<random text>.default\Cache
	…\<random text>.default\jumpListCache

Chrome	
Location within *%userprofile%\AppData\Local\Google\Chrome\UserData\Default*	
History	…\History
	…\History-journal
Cookies	…\Cookies
	…\Cookies-journal
Location within *%userprofile%\AppData\Local\Mozilla\Firefox\Profiles*	
Cache	…\Cache\; …\Favicons; …\Favicons-journal

5.0 CONCLUSION

All browser vendors claim that their private mode does not leave any traces or evidence such as browsing history, temporary internet files, form data, cookies, usernames and passwords, of a browsing session. This paper has inspected numerous literatures ranging from the viewpoint with people who value their privacy while browsing and private browsing has made an impact on digital forensics investigations. The paper began by defining the web browser vendors concern over its' user's privacy and how the private browsing mode feature was introduced. Six similar types of research have been studied and analysed stating the various limitations with each major web browsing vendors. The six researchers have all been successful at recovering browser artefacts from local machine regardless of the browsers or the type of machine they used, pointing out the flaws of current private browsing. Therefore, this paper aims to achieve an improved method for private browsing. The main objective of this research is to propose a more secure and flexible method for private browsing mode. The second objective is to prevent any form of browser fingerprinting being written on the hard disk. This technique is expected to encrypt browsing data after browsing session has ended. It is also to provide a safer environment for the user who often clears their cache files from being a victim data theft.

6.0 ACKNOWLEDGEMENTS

The authors fully acknowledged Ministry of Higher Education (MOHE) and National Defence University of Malaysia (NDUM) for the approved fund which makes this important research viable and effective.

List of Reference

[1] Alam, S., Aziz, M. A., & Iqbal, W. (2016). Forensic analysis of edge browser in-private mode. *International Journal of Computer Science and Information Security (IJCSIS)*, *14*(9).

[2] Anuradha, P., Kumar, T. R., & Sobhana, N. V. (2016, March). Recovering deleted browsing artifacts from web browser log files in Linux environment. In *2016 Symposium on Colossal Data Analysis and Networking (CDAN)* (pp. 1-4). IEEE.

[3] Doug Olenick, Lost devices leading cause of data breaches, report, *SC Media*, (2016). [Online]. Available: https://www.scmagazine.com/home/security-news/lost-devices-leading-cause-of-data-breaches-report/

[4] Satvat, K., Forshaw, M., Hao, F., & Toreini, E. (2014). On the privacy of private browsing–a forensic approach. *Journal of Information Security and Applications*, *19*(1), 88-100.

[5] Krishnamurthy, B., Malandrino, D., & Wills, C. E. (2007, July). Measuring privacy loss and the impact of privacy protection in web browsing. In *Proceedings of the 3rd Symposium on Usable Privacy and Security* (pp. 52-63).

[6] Soghoian, C. (2011). Why private browsing modes do not deliver real privacy. *Center for Applied Cyber security Research, Bloomington*.

[7] Tsalis, N., Mylonas, A., Nisioti, A., Gritzalis, D., & Katos, V. (2017). Exploring the protection of private browsing in desktop browsers. *Computers & Security*, *67*, 181-197.

[8] Ghafarian, A., & Seno, S. A. H. (2015). Analysis of privacy of private browsing mode through memory forensics. *International Journal of Computer Applications*, *132*(16).

[9] Meera, V., Isaac, M. M., & Balan, C. (2013, March). Forensic acquisition and analysis of VMware virtual machine artifacts. In *2013 International Mutli-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s)* (pp. 255-259). IEEE.

[10] Ghafarian, A., & Seno, S. A. H. (2016). Forensics evaluation of privacy of portable web browsers. *International Journal of Computer Applications*, *147*(8).

[11] Bunting, S., & Wei, W. (2006). *EnCase Computer Forensics: The Official EnCE: EnCase? Certified Examiner Study Guide*. John Wiley & Sons.

[12] Liou, J. C., Logapriyan, M., Lai, T. W., Pareja, D., & Sewell, S. (2016, August). A study of the internet privacy in private browsing mode. In *Proceedings of the The 3rd Multidisciplinary International Social Networks Conference on SocialInformatics 2016, Data Science 2016* (pp. 1-7).

[13] Acquisti, A., Gritzalis, S., Lambrinoudakis, C., & di Vimercati, S. (Eds.). (2007). *Digital privacy: theory, technologies, and practices*. CRC Press.

[14] Aggarwal, G., Bursztein, E., Jackson, C., & Boneh, D. (2010). An analysis of private browsing modes in modern browsers. In *19th USENIX Security Symposium (USENIX Security 10)*.

[15] Cherry, D. (2013). *The basics of digital privacy: simple tools to protect your personal information and your identity online*. Syngress.

[16] Zalewski, M. (2011). *The tangled Web: A guide to securing modern web applications*. No Starch Press.

[17] Said, H., Al Mutawa, N., Al Awadhi, I., & Guimaraes, M. (2011, April). Forensic analysis of private browsing artifacts. In *2011 International Conference on Innovations in Information Technology* (pp. 197-202). IEEE.

[18] Nalawade, A., Bharne, S., & Mane, V. (2016, September). Forensic analysis and evidence collection for web browser activity. In 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT) (pp. 518-522). IEEE.

[19] Parsons, J. (2015). Introductory computer concepts 2016, Intro. *Cengage Learning*.

[20] Horsman, G. (2017, April). A process-level analysis of private browsing behavior: A focus on Google Chromes Incognito mode. In *2017 5th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 1-6). IEEE.

[21] Lerner, B. S., Elberty, L., Poole, N., & Krishnamurthi, S. (2013). Verifying web browser extensions' compliance with private-browsing mode. In *Computer Security–ESORICS 2013: 18th European Symposium on Research in Computer Security, Egham, UK, September 9-13, 2013. Proceedings 18* (pp. 57-74). Springer Berlin Heidelberg.

[22] Ohana, D. J., & Shashidhar, N. (2013, May). Do private and portable web browsers leave incriminating evidence? a forensic analysis of residual artifacts from private and portable web browsing sessions. In *2013 IEEE Security and Privacy Workshops* (pp. 135-142). IEEE.

[23] Mahendrakar, A., Irving, J., & Patel, S. (2012). Forensic analysis of private browsing mode in popular browsers.

[24] Malmström, B., & Teveldal, P. (2013). Forensic analysis of the ESE database in Internet Explorer 10.

[25] Noorulla, E. S. (2014). *Web browser private mode forensics analysis*. Rochester Institute of Technology.

[26] Jadhav, M., & Joshi, K. K. (2016, December). Forensic investigation procedure for data acquisition and analysis of Firefox OS based mobile devices. In *2016 International Conference on Computing, Analytics and Security Trends (CAST)* (pp. 456-461). IEEE.