HSPC The Open Access Publisher

J F S R JOURNAL OF FORENSIC SCIENCE AND RESEARCH
ISSN 2575-0186

Research Article

Forensic analysis of private browsing mechanisms: Tracing internet activities

Hasan Fayyad-Kazan[1]*, Sondos Kassem-Moussa[2], Hussin J Hejase[3] and Ale J Hejase[4]

[1]Information Technology, Al Maaref University, Beirut, Lebanon
[2]Department of Forensic Sciences, Lebanese University, Beirut, Lebanon
[3]Senior Member IEEE, Researcher and Professor, Beirut, Lebanon
[4]AKSOB, Lebanese American University, Beirut, Lebanon

More Information

***Address for Correspondence:**
Hasan Fayyad-Kazan, Information Technology, Al Maaref University, Beirut, Lebanon,
Email: hasanfkazan@gmail.com

Submitted: February 19, 2021
Approved: March 06, 2021
Published: March 08, 2021

How to cite this article: Fayyad-Kazan H, Kassem-Moussa S, Hejase HJ, Hejase AJ. Forensic analysis of private browsing mechanisms: Tracing internet activities. J Forensic Sci Res. 2021; 5: 012-019.

DOI: 10.29328/journal.jfsr.1001022

Keywords: Web browsers; Regular mode; Private browsing; Artefacts

Abstract

Forensic analysts are more than ever facing challenges upon conducting their deep investigative analysis on digital devices due to the technological progression. Of these are the difficulties present upon analyzing web browser artefacts as this became more complicated when web browser companies introduced private browsing mode, a feature aiming to protect users' data upon opening a private browsing session, by leaving no traces of data on the local device used. Aiming to investigate whether the claims of web browser companies are true concerning the protection private browsing provides to the users and whether it really doesn't leave any browsing data behind, the most popular desktop browsers in Windows were analyzed after surfing them regularly and privately. The results shown in this paper suggest that the privacy provided varies among different companies since evidence might be recovered from some of the browsers but not from others.

Introduction

There are many turning points for humanity, but there's no doubt that the most important of them is the invention of "Internet". Devices that are connected via internet have greatly changed the way humans communicate and interact. In this context, browsing the internet refers to using the World Wide Web (WWW) using a web browser which is a piece of software installed on the operating system of a digital device serving as a user's window and access point to the different websites meaning that it is an essential application program for accessing the Internet [1].

These browsers record the browsing activity of the user such as the URLs visited, search terms, cookies, saved passwords, cache, recent tabs opened, etc…, therefore various digital forensic techniques used by digital forensic examiners can help obtaining these data and can supply ample amount of information for investigations [2] and this is very important especially that, with browsers use on rise, there's more room for "Cyber Crimes".

In 2005, users' concern about the internet security increased because their work can be compromised by different threats especially tracking their browsing activity. Consequently the "Safari" browser was improved with a new feature in order to satisfy the users' need for a safer browsing experience without leaving traces and information about what they have been up to while surfing the internet. Later on, different web browser companies began adding the aforementioned feature which is known now as "Private Browsing". This feature enhances users' privacy as they claim that no history is stored on the device's hard disk thus people using the same device won't be able to snoop on browsing activities done by previous users because either it is not stored from the first place or deleted and cleared when the browser is closed [3], however, this doesn't mean that the website accessed will not be able to see what the users are doing. As the Private Browsing feature is being more known, the chance of misusing it is increasing as perpetrators tend to use it for the illegal activities they do. This creates an obstacle for forensic analysts that are supposed to find efficient information that can stand as potential evidence out of the data that are saved when browsing regularly, but not, as claimed, in Private Browsing.

This paper shows some experimental work with the aim to test the privacy that web browsers provide, in their private mode, in order to establish a clear path to be followed in case a forensic analyst was to extract crime related data from a computer suspected to be surfed upon using such mode.

Literature review

Forensic analysts need to be given ideas about what to expect and whether it is worth wasting time on finding data if a private mode was found to be used on the computer or to immediately seek getting a warrant in order to get the web activity of the suspect directly from the internet service provider; for this reason and others, many studies have been carried out on Private Browsing modes of different web browsers in order to test the claim of privacy:

Aggarwal, et al. [4] worked on four different browsers to analyze threat models and what constitutes Private Browsing. They found several weaknesses in existing implementations but didn't report the possibility of data retention in Internet Explorer 8. They tested a subset of the artefacts in earlier versions of Chrome, Firefox, Internet Explorer and Safari then expanded their analysis in both extensions and plugins in order to identify any security weaknesses. They concluded to the inadequate implementation of private mode in those browsers, which exposed users' activities as they believe that such privacy can be defeated by determined attackers.

Said, et al. [5] analyzed artefacts from different browsers running in private mode and examined if they were available in the system's memory and they were able to show evidence on disk and in physical memory for the "InPrivate" browsing mode in Internet Explorer 8. They also showed how Google Chrome is relatively more secure although evidence can still be recoverable from memory.

Also, Ohana and Shashidhar [6] investigated the artefacts left by private browsers. Working with different browsers, they spotted recoverable evidence in unallocated and slack space. The number of artefacts left depends on the browser used. For example, Internet Explorer left the most artefacts but not in usual locations, while for other browsers, RAM was the best place to find evidence.

Chivers [7], investigated Internet Explorer 10's "InPrivate" browsing feature to find what evidence could be extracted. He indicated that InPrivate Browsing records can be reliably identified' on a local machine especially if the machine has been powered down during an InPrivate session. He found that Internet Explorer 10 maintains a database of history records and cache in the WebCacheV01.dat file. InPrivate Browsing records were stored in the same tables as normal browsing records and then removed when the browser was closed. He also found evidence in log files that were not removed until Internet Explorer10 was re-opened. InPrivate Browsing records were identified in pagefile.sys and the system volume information directory. He claimed that over 80% of evidence on browsing history was recoverable from non-database areas.

Satvat, et al. [8] expanded the work in Aggarwal, et al. [4], by performing RAM, file system and network analysis, which revealed a notable amount of inconsistencies in the Private Browsing implementation. They observed that when Firefox was cleanly closed, evidence from Private Browsing sessions could not be found in its database, however, if the browser was not cleanly terminated, evidence could be recovered until the browser was re-opened. The authors highlighted that evidence was leaked due to extensions being used in private mode and developed their own extensions to prove that vulnerabilities exist. Thus, they concluded that program crashes might cause privacy leaks.

Ruiz, et al. [9] focused on recovery techniques for page related data created during Private Browsing. The authors performed their tests within 4 individual phases: shutdown, freeze, kill process (browser interruption) and power down, while each phase indicated the way the browser was terminated. Their results showed that all phases included weaknesses regarding user's privacy.

In addition, Montasari and Peltola, [10] analyzed both system's locations and RAM. Their results showed that Chrome is the most secure browser, since there are no artefacts available after Private Browsing, while Firefox only included low risk artefacts.

Tsalis, et al. [11] made some experimentations and their results revealed that private mode has room for improvement since the evaluation of the protection offered by each browser revealed that privacy violations exist contrary to what is documented by the browser. As a result, all browsers have a considerable set of artefacts exposed to local attackers.

According to Gabet, et al. [12], who examined two groups of web browsers, they investigated and identified recoverable web browser artefacts to determine whether enhanced privacy web browsers provide better privacy. Defined by the number of recoverable artefacts as well as content, compared to common web browsers used in private browsing mode, the researchers reached the result that all browsers ultimately produced recoverable browser artefacts but the number varies among them.

After that, Horsman, et al. [13] research results have assessed and clearly demonstrated the effectiveness of the Private Browsing function itself within each browser.

Most recently, Nelson, et al. [14] identified the digital artefacts and their locations that could be recovered from various web browsers and web browsing modes. They were able to recover significantly less artefacts in private sessions than the public browsing sessions, thus validating several of the claims made by the producers of these programs. This shows that different web browsers companies are always improving the private feature they provide and they tend to fix loopholes they encounter.

Tools and methods

To house the different web browsers, a virtual machine was created using VirtualBox Graphical User Interface from oracle “version 5.2.8 r121009 (Qt5.6.2)” [15] since it is available for free, then it was cloned in order to run the different web browsers on different machines to ensure that the experiments would be conducted on a clean system to avoid polluting the research by mixing browsing artefacts. The installers were transferred by drag and drop without using another browser (the default one that comes with the operating system) to download them. This ensured that no browsing artefacts were left behind when experimenting on other browsers. The operating system running within these machines is windows 10 as it is currently the operating system with the largest user base in desktops, therefore, ensuring the representativeness of this work. Artefacts were locally searched for on the storage of the computer meaning that RAM and dump files were not considered in these tests.

The three web browsers tested are the latest, most used, windows compatible browsers [16]. These are:

- Google Chrome version 80.0.3987.149
- Mozilla FireFox version 75.0
- Microsoft Edge version 44.18362.449.0

Late versions of these web browsers were installed for checking the privacy of their private modes in order to test the web browser companies’ claims and to check for any violation of privacy and to ensure that proper privacy is maintained and no traces of browsing activity are stored on the local computer.

Browsers were surfed in both regular and private modes in order to be able to compare the way each browser behaves in different modes.

To access the private mode on:

Google Chrome:

Its Private Browsing mode is called “Incognito Mode”:

Step 1: Start Chrome.

Step 2: Click the special menu in the top-right corner of the browser window (Figure 1).

Step 3: Choose “New incognito window”.

The incognito window is unmistakable, it is dark and there is an icon at the top indicating that the user is browsing in incognito mode.

Mozilla Firefox:

Its Private Browsing mode is called “Private Browsing”:

Step 1: Start Firefox.

Step 2: Click the special menu in the top-right corner of the browser window (Figure 2).

Step 3: Choose “New Private Window”.

The private window is purple in color, it has an icon of a white mask inside a purple circle at the top indicating that the user is browsing privately.

Microsoft Edge:

Its Private Browsing mode is called “InPrivate Browsing”:

Step 1: Start Microsoft Edge.

Step 2: Click the special menu in the top-right corner of the browser window (Figure 3).

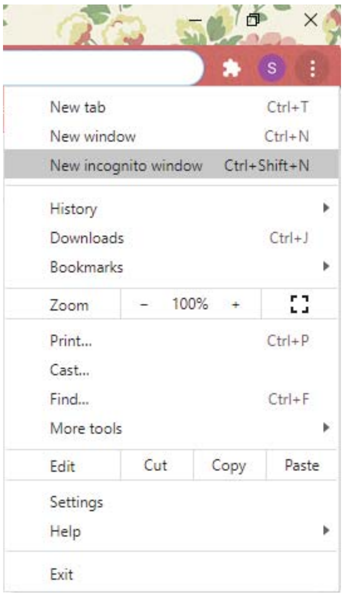


Figure 1: Google Chrome’s settings tab.

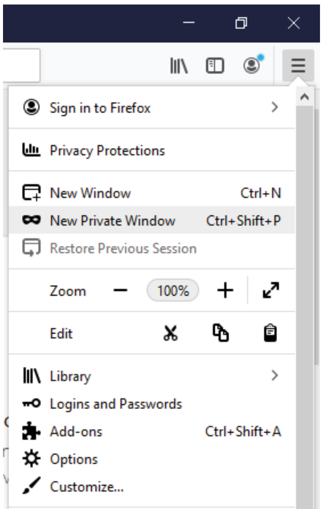


Figure 2: Mozilla Firefox’s settings tab.

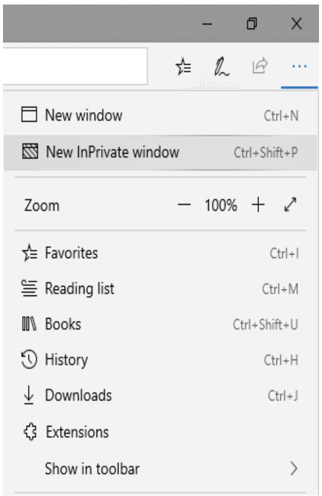


Figure 3: Microsoft Edge's settings tab.

Step 3: Choose "New InPrivate window".

When in InPrivate mode, the window will become grey and each tab along with a blue box on the top left will bear the label "InPrivate".

The browsers were opened and 4 websites were surfed on each in the different modes (regular and private):

www.youtube.com: a random video was chosen and watched.

www.sciencedirect.com: a search was made for articles about browsers forensics.

www.covidvisualizer.com: COVID-19 patients' numbers were looked at for different countries.

www.google.com: images of COVID-19 virus were searched for and two images were opened.

Different programs were used to view the artefacts (history, cache, cookies, ...) that are usually saved to different folders (Tables 1-3), "MiniTool Power Data Recovery v6.8" [17] was used to recover deleted browsing data, and "Process Monitor"[18] was used to track the formation of files while browsing privately.

Results

Examining the artefacts in regular mode

Many programs and tools were used to try viewing the different artefacts produced during the regular mode of browsing, one of which is browser history examiner (Figure 4) [19], which showed the different artefacts along with the time and date of creation.

Clearing browsing data in the different web browsers in regular mode

Table 1: Google Chrome's artefacts storage places.

Artefacts	Storage place
Profile path	C:\Users\X\AppData\Local\Google\Chrome\User Data\Default
History	C:\Users\X\AppData\Local\Google\Chrome\UserData\Default\History
Cookies	C:\Users\X\AppData\Local\Google\Chrome\UserData\Default\Cookies
Cache	C:\Users\X\AppData\Local\Google\Chrome\UserData\Default\Cache

Table 2: Mozilla Firefox's artefacts storage places.

Artefacts	Storage place
Profile path	C:\Users\X\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default\
Navigation history	C:\Users\X\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default\places.sqlite
cookies	C:\Users\X\AppData\Roaming\Mozilla\Firefox\Profiles\[profileID].default\cookies.sqlite
Cache	C:\Users\X\AppData\Local\Mozilla\Firefox\Profiles\[profileID].default\cache2\entries C:\Users\X\AppData\Local\Mozilla\Firefox\Profiles\[profileID].default\startupCache

Table 3: Microsoft Edge's artefacts storage places.

Artefacts	Storage place
Profile path	C:\Users\X\AppData\Local\Packages\Microsoft.MicrosoftEdge_X\AC
History + Cookies	C:\Users\X\AppData\Local\Microsoft\Windows\WebCache\WebCacheV01.dat
cache	C:\Users\X\AppData\Local\Packages\Microsoft.MicrosoftEdge_X\AC\#!001\MicrosoftEdge\Cache

The browsing data were cleared from the browsers, and to check if this step is enough to get rid of browser activity traces, the folders housing these artefacts were checked but they were now emptied. Again, artefacts were examined by the previously used programs, little or no data was shown meaning that those programs are only used to make search easier for forensic analysts since they are not meant to retrieve any deleted data.

Retrieving browsing data in regular mode

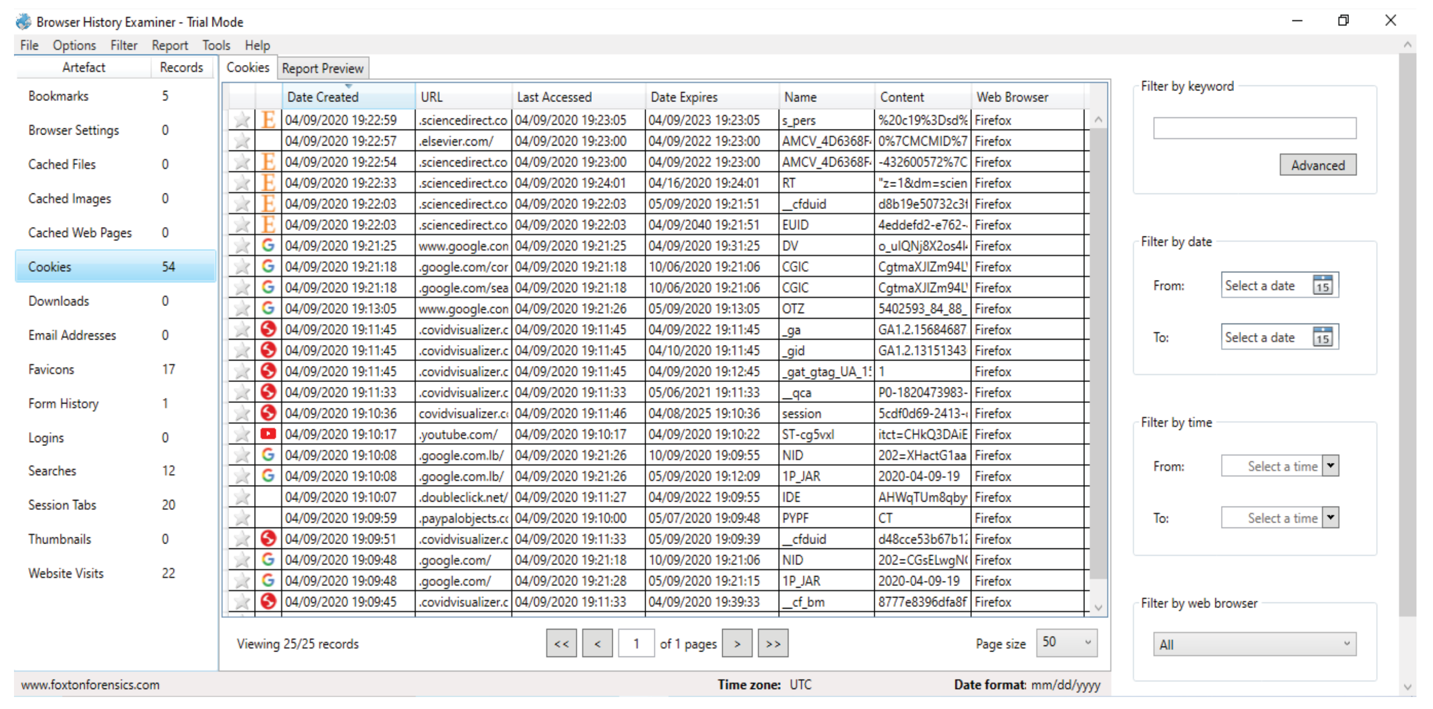
Now, to see if artefacts can be recovered for regular mode to be used as evidence, Minitool Power Data recovery was used in an attempt to retrieve the deleted browsing data, and the attempt was successful for the three browsers meaning that these data were not permanently deleted. Hence, manual deletion of browser data only makes them invisible, and the use of a software can get them back.

Examining the artefacts in private mode

Upon browsing in private mode, Process Monitor was used to track the files that are formed during the private sessions. Files were created in the profile path folders in the case of Chrome and Firefox. However, in the case of Microsoft Edge, and rather being saved in the profile path folder, many files were created at different locations such as in the temporary files folder, the recovery folder, the cache folder (Figures 5,6), and moreover, the webcache.dat file's size increased meaning that some data were added to this database file.

Retrieving browsing data in private mode

After the private sessions were closed, the browsing data saved temporarily for chrome and Firefox were automatically



Browser History Examiner - Trial Mode

File Options Filter Report Tools Help

Artefact	Records
Bookmarks	5
Browser Settings	0
Cached Files	0
Cached Images	0
Cached Web Pages	0
Cookies	54
Downloads	0
Email Addresses	0
Favicons	17
Form History	1
Logins	0
Searches	12
Session Tabs	20
Thumbnails	0
Website Visits	22

Cookies | Report Preview

		Date Created	URL	Last Accessed	Date Expires	Name	Content	Web Browser
☆	E	04/09/2020 19:22:59	.sciencedirect.co	04/09/2020 19:23:05	04/09/2023 19:23:05	s_pers	%20c19%3Dsd%	Firefox
☆		04/09/2020 19:22:57	.elsevier.com/	04/09/2020 19:23:00	04/09/2022 19:23:00	AMCV_4D6368F	0%7CMCMID%7	Firefox
☆	E	04/09/2020 19:22:54	.sciencedirect.co	04/09/2020 19:23:00	04/09/2022 19:23:00	AMCV_4D6368F	-432600572%7C	Firefox
☆	E	04/09/2020 19:22:33	.sciencedirect.co	04/09/2020 19:24:01	04/16/2020 19:24:01	RT	"z=1&dm=scien	Firefox
☆	E	04/09/2020 19:22:03	.sciencedirect.co	04/09/2020 19:22:03	05/09/2020 19:21:51	__cfduid	d8b19e50732c3	Firefox
☆	E	04/09/2020 19:22:03	.sciencedirect.co	04/09/2020 19:22:03	04/09/2040 19:21:51	EUID	4eddefd2-e762-	Firefox
☆	G	04/09/2020 19:21:25	www.google.con	04/09/2020 19:21:25	04/09/2020 19:31:25	DV	o_uIQNj8X2os4l	Firefox
☆	G	04/09/2020 19:21:18	.google.com/cor	04/09/2020 19:21:18	10/06/2020 19:21:06	CGIC	CgtmaXJIZm94L	Firefox
☆	G	04/09/2020 19:21:18	.google.com/sea	04/09/2020 19:21:18	10/06/2020 19:21:06	CGIC	CgtmaXJIZm94L	Firefox
☆	G	04/09/2020 19:13:05	www.google.con	04/09/2020 19:21:26	05/09/2020 19:13:05	OTZ	5402593_84_88_	Firefox
☆	●	04/09/2020 19:11:45	.covidvisualizer.c	04/09/2020 19:11:45	04/09/2022 19:11:45	_ga	GA1.2.15684687	Firefox
☆	●	04/09/2020 19:11:45	.covidvisualizer.c	04/09/2020 19:11:45	04/10/2020 19:11:45	_gid	GA1.2.13151343	Firefox
☆	●	04/09/2020 19:11:45	.covidvisualizer.c	04/09/2020 19:11:45	04/09/2020 19:12:45	_gat_gtag_UA_1	1	Firefox
☆	●	04/09/2020 19:11:33	.covidvisualizer.c	04/09/2020 19:11:33	05/06/2021 19:11:33	__qca	P0-1820473983-	Firefox
☆	●	04/09/2020 19:10:36	covidvisualizer.c	04/09/2020 19:11:46	04/08/2025 19:10:36	session	5cdf0d69-2413-	Firefox
☆	▶	04/09/2020 19:10:17	.youtube.com/	04/09/2020 19:10:17	04/09/2020 19:10:22	ST-cg5vxl	itct=CHkQ3DAiE	Firefox
☆	G	04/09/2020 19:10:08	.google.com.lb/	04/09/2020 19:21:26	10/09/2020 19:09:55	NID	202=XHactG1aa	Firefox
☆	G	04/09/2020 19:10:08	.google.com.lb/	04/09/2020 19:21:26	05/09/2020 19:12:09	1P_JAR	2020-04-09-19	Firefox
☆		04/09/2020 19:10:07	.doubleclick.net/	04/09/2020 19:11:27	04/09/2022 19:09:55	IDE	AHWqTUm8qby	Firefox
☆		04/09/2020 19:09:59	.paypalobjects.c	04/09/2020 19:10:00	05/07/2020 19:09:48	PYPF	CT	Firefox
☆	●	04/09/2020 19:09:51	.covidvisualizer.c	04/09/2020 19:11:33	05/09/2020 19:09:39	__cfduid	d48cce53b67b1	Firefox
☆	G	04/09/2020 19:09:48	.google.com/	04/09/2020 19:21:18	10/09/2020 19:21:06	NID	202=CGsELwgN	Firefox
☆	G	04/09/2020 19:09:48	.google.com/	04/09/2020 19:21:28	05/09/2020 19:21:15	1P_JAR	2020-04-09-19	Firefox
☆	●	04/09/2020 19:09:45	.covidvisualizer.c	04/09/2020 19:11:33	04/09/2020 19:39:33	__cf_bm	8777e8396dfa8f	Firefox

Viewing 25/25 records << < 1 of 1 pages > >> Page size 50

Filter by keyword

Advanced

Filter by date

From: Select a date

To: Select a date

Filter by time

From: Select a time

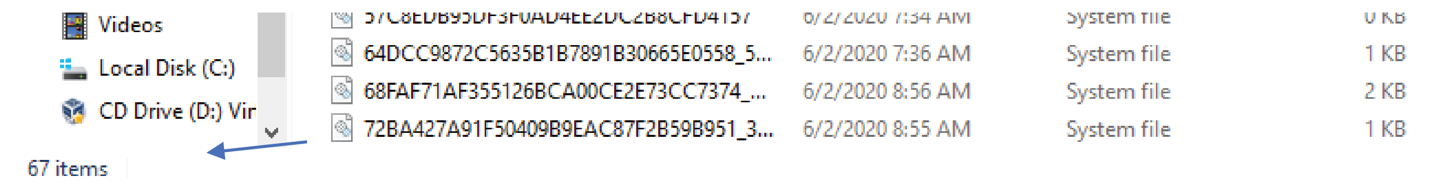
To: Select a time

Filter by web browser

All

www.foxtonforensics.com Time zone: UTC Date format: mm/dd/yyyy

Figure 4: Firefox's artefacts viewed by Browser History Examiner after regular browsing.



Videos

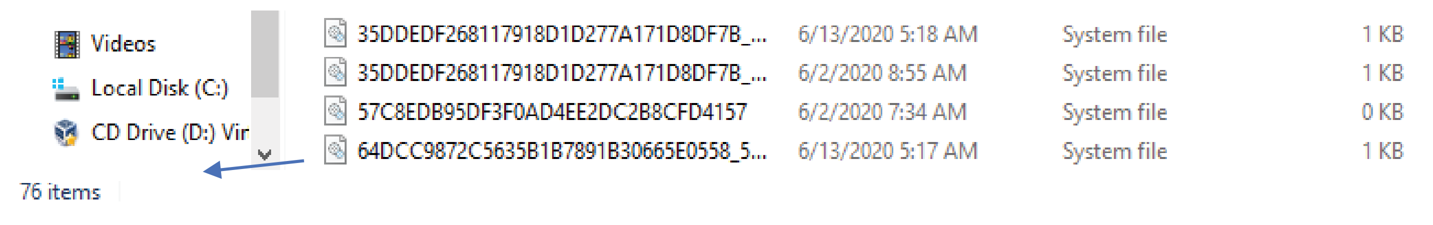
Local Disk (C:)

CD Drive (D:) Vir

67 items

57C8EDB95DF3F0AD4EE2DC2B8CFD4157	6/2/2020 7:34 AM	System file	0 KB
64DCC9872C5635B1B7891B30665E0558_5...	6/2/2020 7:36 AM	System file	1 KB
68FAF71AF355126BCA00CE2E73CC7374_...	6/2/2020 8:56 AM	System file	2 KB
72BA427A91F50409B9EAC87F2B59B951_3...	6/2/2020 8:55 AM	System file	1 KB

Figure 5: Edge's cache folder before opening the private session.



Videos

Local Disk (C:)

CD Drive (D:) Vir

76 items

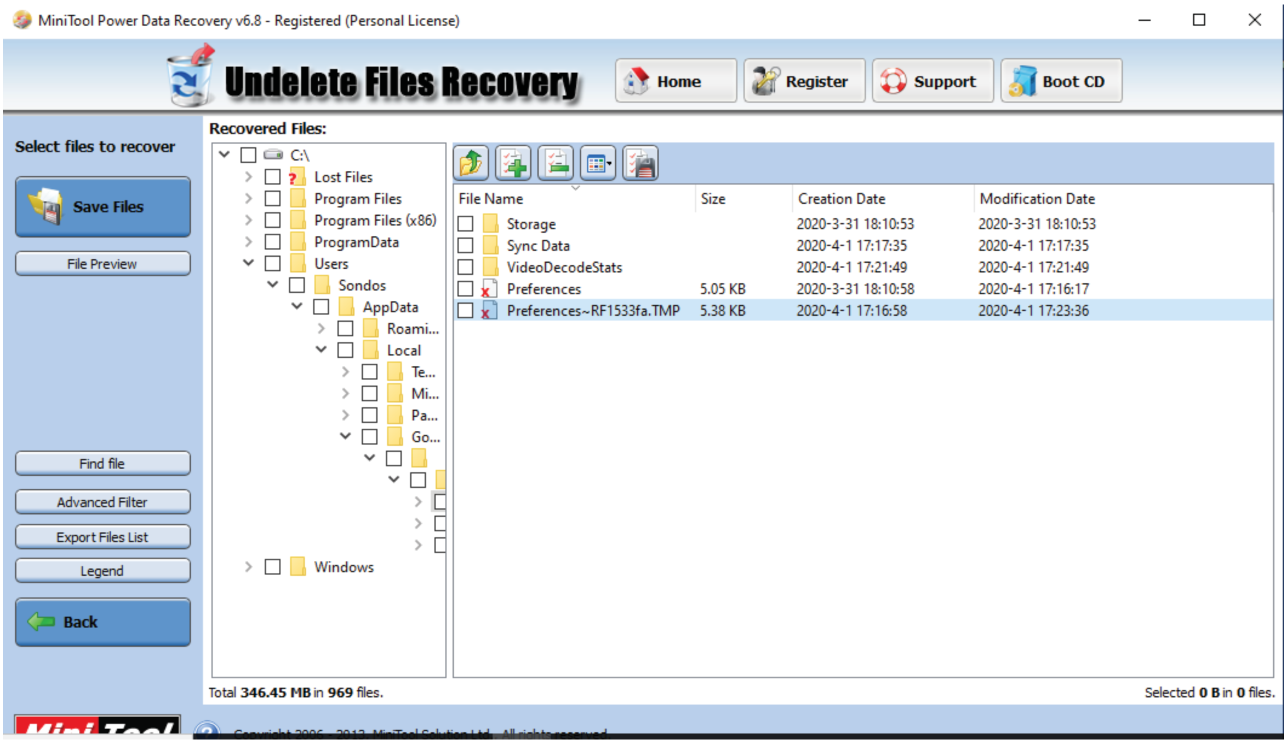
35DDEDF268117918D1D277A171D8DF7B_...	6/13/2020 5:18 AM	System file	1 KB
35DDEDF268117918D1D277A171D8DF7B_...	6/2/2020 8:55 AM	System file	1 KB
57C8EDB95DF3F0AD4EE2DC2B8CFD4157	6/2/2020 7:34 AM	System file	0 KB
64DCC9872C5635B1B7891B30665E0558_5...	6/13/2020 5:17 AM	System file	1 KB

Figure 6: Edge's cache folder after opening the private session.

deleted from the folders, so the next step was to try retrieving them by the recovery tool. For Google Chrome, only two temporary files (Figure 7) were recovered but it was a dead end as no information was deduced from them (Figure 8). And for Mozilla Firefox, 7 database files were recovered (Figure 9). As for Edge, the files created upon browsing privately remained even after closing the private window. Thus, there was no need for using a recovery tool.

Discussion

According to the results, it can be inferred that the privacy provided by web browsers varies among different companies. Some are up to expectations while others are not. When browsing regularly, the three browsers saved their artefacts to the local device. Chrome and Firefox saved them in multiple folders contained in their profile path folders, while Edge saved them to folders located at different locations all over the device as tracked by process monitor. When these artefacts were manually cleared, it was possible to retrieve them by a recovery tool meaning that they weren't permanently deleted. It is worth noting that when a user formats a hard drive or deletes a partition or any file present on the hard drive, he/she is actually deleting the file system only, making the data invisible, or no longer actively indexed, but not gone; it is still there. A file recovery program or special hardware often recovers such information. So, to make sure that the private

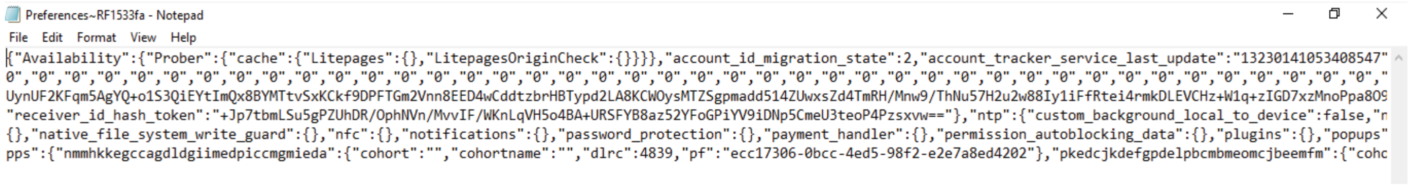


File Name	Size	Creation Date	Modification Date
Storage		2020-3-31 18:10:53	2020-3-31 18:10:53
Sync Data		2020-4-1 17:17:35	2020-4-1 17:17:35
VideoDecodeStats		2020-4-1 17:21:49	2020-4-1 17:21:49
Preferences	5.05 KB	2020-3-31 18:10:58	2020-4-1 17:16:17
Preferences~RF1533fa.TMP	5.38 KB	2020-4-1 17:16:58	2020-4-1 17:23:36

Total **346.45 MB** in **969** files.

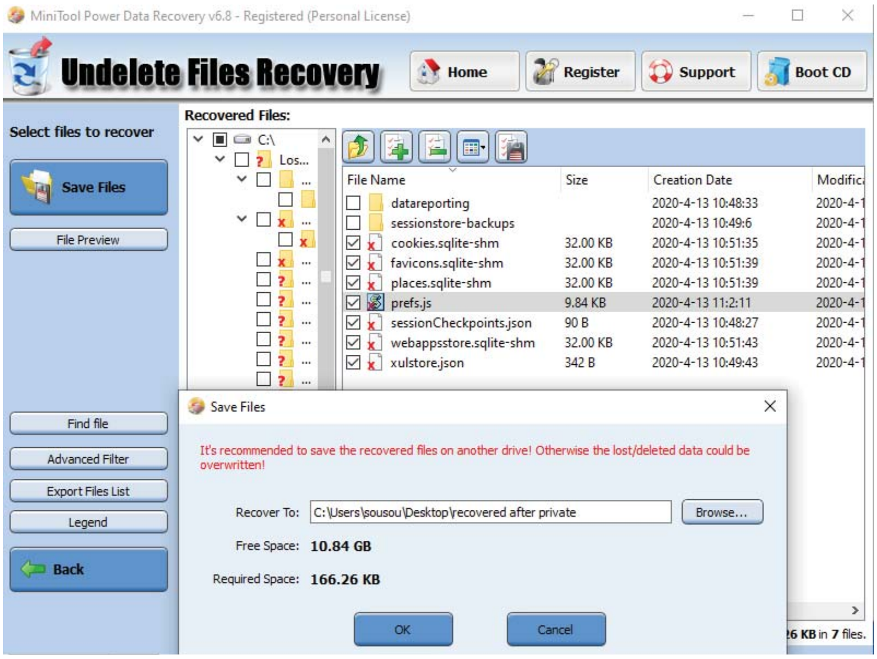
Selected **0 B** in **0** files.

Figure 7: Chrome's automatically deleted temporary files recovered by Minitool Power Data Recovery.



```
{"Availability":{"Prober":{"cache":{"Litepages":{},"LitepagesOriginCheck":{}}}},"account_id_migration_state":2,"account_tracker_service_last_update":"13230141053408547"
0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","0","
UynUF2KFqm5AgYQ+o1S3QiEYtImQx8BYMTtvSxKCkf9DPFTGm2Vnn8EED4wCddtzbrHBTypd2LA8KCWOysMTZSgpmadd514ZUwxsZd4TmRH/Mnw9/ThNu57H2u2w88Iy1iFfRtei4rmkDLEVCHz+W1q+zIGD7xzMnoPpa809
"receiver_id_hash_token":"+Jp7tbmLSu5gPZUhDR/OphNVn/MvvIF/WKnLqVH5o4BA+URSFYB8az52YFoGPiYV9iDNp5CmeU3teoP4Pzsxvw=="},"ntp":{"custom_background_local_to_device":false,"n
{},"native_file_system_write_guard":{},"nfc":{},"notifications":{},"password_protection":{},"payment_handler":{},"permission_autoblocking_data":{},"plugins":{},"popups"
pps":{"nmmhkkegccagdldgiimedpiccmgmieda":{"cohort":"","cohortname":"","dlrc":4839,"pf":"ecc17306-0bcc-4ed5-98f2-e2e7a8ed4202"},"pkedcjkdefgpdelpbcmbmeomcjbeemfm":{"cohc
```

Figure 8: The content of Chrome's temporary file.



File Name	Size	Creation Date	Modific
□ datareporting		2020-4-13 10:48:33	2020-4-1
□ sessionstore-backups		2020-4-13 10:49:6	2020-4-1
☑ cookies.sqlite-shm	32.00 KB	2020-4-13 10:51:35	2020-4-1
☑ favicons.sqlite-shm	32.00 KB	2020-4-13 10:51:39	2020-4-1
☑ places.sqlite-shm	32.00 KB	2020-4-13 10:51:39	2020-4-1
☑ prefs.js	9.84 KB	2020-4-13 11:2:11	2020-4-1
☑ sessionCheckpoints.json	90 B	2020-4-13 10:48:27	2020-4-1
☑ webappsstore.sqlite-shm	32.00 KB	2020-4-13 10:51:43	2020-4-1
☑ xulstore.json	342 B	2020-4-13 10:49:43	2020-4-1

It's recommended to save the recovered files on another drive! Otherwise the lost/deleted data could be overwritten!

Recover To: C:\Users\sousou\Desktop\recovered after private

Free Space: **10.84 GB**

Required Space: **166.26 KB**

6 KB in 7 files.

Figure 9: Firefox's automatically deleted files recovered by Minitool Power Data Recovery.

information is gone forever, the user needs to wipe the hard drive using special software. Such software will decrease the chance of getting any data back by running a low-level format that overwrites all the deleted files with zeros and other incomprehensible data. In fact, this is important for forensic experts because if they were investigating a case where the digital drive is wiped then they would not waste time on getting data out of something that they know there's no chance to retrieve data from. As for the private mode, Google Chrome proved to be more secure at the level of local security since only two temporary files were created during the private session in the profile path folder then automatically deleted by the browser itself. These temporary files, even though recovered, didn't show any informative data so nothing can be inferred from them other than the suggestion that a private mode might have been used; they do not contain browsing data nor are beneficial for investigations. For Mozilla Firefox, up to seven database files were created during the private session in the profile path folder, then these were automatically deleted by the browser itself. Their recovery was quite easy by the recovery tool. Of course, these files require further investigation by database file experts in order to check what information can be extracted from them and to see whether they hold browsing data and artefacts that can be used as evidence in cases of investigations especially that it's known that many browsing data are saved to database files. As for Microsoft Edge, it is proved that their claim of privacy is false. Surprisingly, in private mode the situation was different than that of Chrome and Firefox as the files created while in the private session were not automatically deleted when this session was terminated; they were left on the local device used. Therefore, analysts might be able to extract information, browsing data, and artefacts in order to find evidence that might stand helpful for their investigations. All in all, it can be said that the web browser that provides the best local anonymity is Chrome, then comes Firefox, while Edge is not recommended for such desired privacy.

Conclusion

In the past two decades, information and communication technology has turned into a reality that touches all aspects of our daily life, and it has become a major milestone of development. This enormous scientific development was accompanied with groups of criminals with the intentions to use different available resources for doing many crimes [20]. Computers can be considered as the most available developed tool for committing such activities, and thus they can be a source of evidence because web browser's artefacts allow investigators to reconstruct the timeline of the user's web activity. Unfortunately, it became harder for investigators to gather the aforementioned evidence due to Private Browsing. Whether data can be retrieved or not, this step undoubtedly raised significant challenges for investigators.

In this paper, some experimental work was carried out to investigate the private feature. Internet was surfed in both regular and private modes, then artefacts were traced and looked for to see the difference in the work mode of these browsers, and to check whether any traces might be left behind on the local computer used in case of private browsing. The results of the tests performed showed that Chrome, as Google claims, proves to be safe against local attackers as it leaves no informative traces behind. As for Mozilla Firefox, it left some database files thus requiring further investigation by experts specializing in such types of files. In case of Microsoft Edge, some files were proven to be stored on the used computer thus Microsoft's claim of privacy fails. Therefore, the protection private mode provided differs according to the web browser used.

For browsers with high privacy such as the case of Chrome, further studies must be done in order to facilitate the work done by investigators upon investigating any crime. Forensic Investigators need to concentrate on live memory capturing as it provides many information when compared to dead analysis, keeping in mind that the collected evidences are only an insight to the particular case or incident, so more work must be done to get the bigger picture of the incident. Unfortunately, capturing live memory is not always possible when evidence is being recovered from a scene. It is also possible that doing so could alter original data and affect the forensic value of artefacts.

As so, alternatives must be searched for to avoid wasting time. Hence, in such circumstances where it is thought that private browsing is the case, and the used browsers are proved to be properly protected, the investigators must resort to other solutions. Such alternative solutions might be seeking to obtain a court memorandum authorizing the competent forensic investigators to obtain the necessary information needed from the internet service providers. Furthermore, routers might be checked and analyzed as they save information that pass through them. Also, precautions might be taken for people who are already under supervision such as live monitoring and activity capture which may provide the only viable solution with regards to the effective regulation of Internet usage [21].

Due to the continuous update web browser companies do and the additional features they offer, future research demands excessive work by web browser forensics in order to be able to overcome all the obstacles that might face any investigation enabling them to reach and get whatever information related to web browsers they might need.

References

1. Oh J, Lee S, Lee S. Advanced evidence collection and analysis of web browser activity. Digit Investig. 2011; 8: S62–S70, 2011.
2. Rathod D. Web Browser Forensics: Google Chrome. Int J Adv Res Comput Sci. 2017; 8.
3. Abdulrahman N. Forensics Analysis of Residual Artefacts Acquired During Normal and Private Web Browsing Sessions. 2016.

4. Aggarwal G, Bursztein E, Jackson C, Boneh D. ScoopyNG. 2010. http://www.trapkit.de/research/vmm/scoopyng/index.html

5. Said H, AlMutawa N, AlAwadhi I, Guimaraes M. Forensic analysis of private browsing artifacts. in Innovations in information technology (IIT). 2011; 197–202.

6. Ohana DJ, Shashidhar N. Do private and portable web browsers leave incriminating evidence? A forensic analysis of residual artifacts from private and portable web browsing sessions. in IEEE CS Security and Privacy Workshops. 2013; 135–142.

7. Chivers H. Private Browsing: A Window of Forensic Opportunity. 2014.

8. Satvat K, Forshaw M, Hao F, Toreini E. On the privacy of private browsing - A forensic approach. in Lecture Notes in Computer Science. 2013; 8247: 380–389.

9. Ruiz RDS, Amatte FP, Jin K, Park B, M. Analysis, and N. Nucam, “Acquiring Evidence of Browsing Activities. 2015.

10. Montasari R, Peltola P. Computer forensic analysis of private browsing modes. Commun Comput Inf Sci. 2015; 534: 96–109.

11. Tsalis N, Mylonas A, Nisioti A, Gritzalis D, Katos V. Exploring the protection of private browsing in desktop browsers. Comput Secur. 2017; 67: 181–197.

12. Gabet RM, Seigfried-Spellar KC, Rogers MK. A comparative forensic analysis of privacy enhanced web browsers and private browsing modes of common web browsers. Int J Electron Secur Digit Forensics. 2018. 10: 356–371.

13. Horsman G. A forensic examination of web browser privacy-modes. Forensic Sci Int. Rep. 2019; 1: 100036.

14. Nelson R, Shukla A, Smith C. Web Browser Forensics in Google Chrome, Mozilla Firefox, and the Tor Browser Bundle. 2020.

15. ORACLE. Download VirtualBox. https://www.virtualbox.org/wiki/Downloads

16. NetMarketShare. Market share for mobile, browsers, operating systems and search engines. NetMarketShare. 2020. http://marketshare.hitslink.com

17. MiniTool. MiniTool Power Data Recovery. https://www.minitool.com/download-center/data-recovery-download.html

18. Sysinternals. Process Monitor. https://www.softpedia.com/get/System/System-Info/Microsoft-Process-Monitor.shtml

19. Foxton Forensics. Browser History Examiner. https://www.foxtonforensics.com/browser-history-examiner/download

20. Hejase HJ, Kazan H, Moukadem I. Advanced persistent threats (apt): an awareness review. J Econ Educ Res. 2020; 21: 1–8.

21. Horsman G. The challenge of identifying historic ‘private browsing’ sessions on suspect devices. Forensic Sci Int Digit Investig. 2020; 34: 300980.