|| Volume 5 || Issue 6 || June 2020 || ISSN (Online) 2456-0774

INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH

AND ENGINEERING TRENDS

FORENSIC STUDY AND ANALYSIS OF DIFFERENT ARTIFACTS OF WEB BROWSERS IN PRIVATE BROWSING MODE

Rinchon Sanghkroo[1], Dr. Deepak Raj Rao G.[2] and Kumarshankar Raychaudhuri[3]

M.Sc. (Forensic Science) Final Semester Student, *Cyber Forensic Division, LNJN National Institute of Criminology and Forensic Science (MHA), Delhi, India* [1]

Assistant Professor, *Cyber Forensic Division, LNJN National Institute of Criminology and Forensic Science (MHA), Delhi, India*[2]

Junior Research Fellow, *Cyber Forensic Division, LNJN National Institute of Criminology and Forensic Science (MHA), Delhi, India*[3]

rinchonsanghkroo@gmail.com[1], *gdeepakrajrao@gmail.com*[2], *ksrc089@gmail.com*[3]

-- ***--

***Abstract*: - Web browsers today have become one of the most commonly used applications in digital devices, storing and maintaining huge information on user activities. The privacy mode has been introduced to combat the privacy issues related with browsers. This feature keeps the browsing activities of a user private by not storing or removing the traces of artifacts related to the browsing session on the system. In this study, we test the effectiveness of this claim and to ensure ways in which a forensic investigation may be done in such cases. The private modes of different browsers have been tested in Windows and MAC OS by performing pre-defined browsing activities in each of the browsers in both the operating systems. Moreover, the default locations of normal web browser artifacts are also examined to find whether artifacts of private browsing activities are stored in such locations or not.**

***Keywords:* -** *Private Browsing, Windows, MAC, Safari, Microsoft Edge, Brave Browser*

-- ***--

I INTRODUCTON

In a matter of a few years, the internet has grown to be one of the most powerful platforms; becoming not only the universal source of information, but also an essential means to carry out day-to-day tasks. The access to this ocean of information is done with the help of web browsers. Web browsers allow the users to browse the internet and navigate through websites and web pages, by communicating with the web servers over the internet [1]. At present, its utilization encompasses far more than just browsing and downloading information; it is also used to perform numerous other functions such as social media, e-banking, online blogs, e-business or e-commerce, etc [2]. As a result, web browsers store and maintain logs of an enormous amount of information on user activities on the system. This has resulted in the users using the same device, to be informed of each other's activities, thereby, raising concerns over privacy while browsing the internet.

This issue with privacy of browsing sessions thus, further brought about the development of a new feature known as the 'private browsing' mode. It has been defined as a "web browser mode in which information about visited websites is not saved" [3]. It aims at keeping the user activities carried out during a browsing session "private", by not leaving traces or storing any artifacts related to it on the end device. In this mode, the search history and the sites visited, form data, cookies and cache files would either not be recorded or will be deleted from memory once the browser is closed [4]. However, this feature is limited to the end device and does not prevent internet service providers or employers from viewing the online activities of the users. While the majority of users may prefer private browsing mode for a number of good reasons, it can also be exploited by criminals for committing numerous internet related crimes, who are also seeking ways to hide any traces of their activities. Thus, while private browsing modes tend to be an immense way of addressing privacy concerns, it has also become a painstaking task for Law enforcement agencies and forensic investigators.

The objective of our study is to examine and verify the assured level of privacy stated by the different browser vendors as well as to find the extent to which a forensic investigation can uncover artifacts of evidentiary importance. For these purposes, a set of experiments is done on the private browsing mode of five selected web browsers, on two operating systems, namely, MacOS and Windows OS. These pre-defined browsing activities would remain specific to image viewing and downloading, video streaming, search terms, logging into an e-mail account and viewing flight tickets from a travel website. With RAM being a big repository for such activities, an attempt is made to recover these artifacts from the physical memory. Moreover, the default locations where artifacts of the normal browsing sessions are stored would also be analyzed for the presence of any traces of the activities carried out in the private mode of web browsers.

II REVIEW OF LITERATURE AND BACKROUND STUDY

Private browsing mode was introduced by Safari, the default browser for Apple devices, for the first time in 2005. One of the first studies on private mode of browsers [5] proposed the two main goals of private browsing as privacy against the web attacker and privacy against the local attacker. They examined the private browsing modes of four popular modern browsers and found that while Mozilla Firefox and Google Chrome both take steps during private browsing session to remain private against website, Apple Safari, on the other hand, focused mainly on attacks against local machines.

Previous research has been performed on four of the most widely used web browsers, namely, Google Chrome, Mozilla Firefox, Internet Explorer and Apple Safari on different versions of Windows Operating system. It has been reported that although the private browsing mode left evidence of browsing activities behind in all the four major browsers, yet, the type and the amount of data recovered varied among the browsers [5,6,7]. Most studies have concluded that Firefox [7,8] and Chrome [8,9] supports private browsing better than the other browsers. In the meanwhile, some studies have also pointed out that Internet Explorer provided the most residual artifacts [6,9]. However, it has been asserted that private browsing mode offered a level of privacy which can be considered to be ‘sufficient for the average user’ [8]. A more comprehensive study [4] on the privacy claims of Internet Explorer, Firefox, Chrome and Safari was conducted on different operating systems, namely, Windows, Mac OS X and Linux by monitoring the file system changes and examining the memory dump of the system. The results showed that, when looking at the changes made to the file system, only Chrome and Firefox did not write any changes to the file system. However, Safari wrote data to a single database file called WebpageIcons.db and Internet Explorer wrote data to the file system but then deleted it when the browser was closed.

Over the years, researchers have explored why private browsing mode of browsers is unable to deliver real privacy and found various factors contributing to the cause. Few studies have found that the lack of understanding on the part of the consumers regarding the limitations of such feature [10,11], which may also be caused by the in-browser explanations of private browsing mode [12], played a big role; others held the complications introduced by browser plug-ins and extensions accountable for it [5,13,14]. A more recent study [15] also focused on enhanced privacy web browsers (Epic, Comodo Dragon and Dooble) and compared it with the private browsing modes of common browsers (Chrome, Edge and Firefox). They concluded that the enhanced privacy browsers performed about the same as the common browsers in anonymous browsing mode.

Nevertheless, prior research has been carried out on older versions of the web browsers. Therefore, it was found to be necessary to conduct new experiments to verify their findings on the latest versions of the browsers. Moreover, most of the studies have been carried out on Windows systems with very little to no room for other operating systems. This study will, therefore, further look into whether the recovered artifacts, if any, are consistent with another operating system, namely, MacOS.

III EXPERIMENTAL DESIGN

This section elucidates the experimental set-up required to conduct the study, including the browsers, forensic tools and the methodology followed by the research.

A. *Browsers Used*

The study was carried out on the following versions of the five browsers:

i. Incognito - Google Chrome Version 80.0.3987.87
ii. Private Browsing - Apple Safari Version 13.0.4
iii. In Private Browsing - Microsoft Edge Version 80.0.361.109
iv. Private Browsing - Mozilla Firefox Version 72.0.2
v. Private browsing - Brave Browser Version 1.2.4.3

Apple no longer develops Safari for Windows operating system, with the latest Safari version for Windows being 5.1.7 from 2011 which has become obsolete. Hence, for this study, Safari has been considered specifically for Mac operating system only.

B. *Tools Used*

The following tools have been used for carrying out the experiments for the purpose of research:

Oracle Virtual Box 6.0.16 - For the purpose of virtualization, VirtualBox [16] was used to replicate a (i) Windows 10 and (ii) MacOS Sierra environments. Prior to the testing, no browser was used in the virtual machine. A snapshot of the virtual machine was then taken in this state which acted as the base machine. From this base state, one of the browsers was installed through its installer and the pre-defined activities were carried out in the private browsing mode. For the next browser, the machine was thereafter restored back to the base machine.

AccessData FTK Imager Lite 3.1.1.8 - FTK Imager Lite contains the minimum files necessary to run FTK Imager without installing it on the system. It is used for acquiring the live image of memory on a Windows system [17].

OSXPmem - Mac OS X Physical Memory acquisition tool is an open source tool to acquire physical memory on Mac systems [18].

WinHex 19.9 - WinHex is a universal hexadecimal editor which can be used to inspect and edit all kinds of files, recover deleted files, etc [19]. It was used to analyze the physical memory images of both the operating systems.

DB Browser for Sqlite **-** DB Browser for SQLite (DB4S) is a database tool which can be used to create, view and edit database files compatible with SQLite [20]. It was used to view the database files in which the browsers store their artefacts, mainly for MacOS systems.

Nirsoft Web Browser Tools Package **-** This package is a collection of various tools that extracts history, cache, cookies, downloads, etc., from the default locations of the different browsers, including Chrome, Firefox, Edge, etc. [21]. It was used to extract the browsing artifacts of various browsers on Windows Operating System.

C. Preparation of Dataset

For the purpose of this study, each of the browsers was populated with a set of pre-defined browsing activities carried out in the private browsing modes in both the operating systems (refer Table 1), to mimic the activities of a criminal or a crime suspect:

Table 1: Pre-defined Browser activities

Websites	***Browsing Activities***
Thoughtcatalog.com	1.Enter “best ways to get away with murder” in the search bar. 2.Open the article titled “16 Steps to Kill Someone and Not Get Caught”. 3.The URL is https://thoughtcatalog.com/ juliet-escoria/2013/12/16-steps-to-kill-someone-and-not-get-caught/
Parasite (Image Download)	1.Enter “Parasite” in the search bar. 2.Select the ‘Images’ tab and open the image from Imdb.com 3.Download the image to the Download folder.
Goibibo.com	1.Enter the URL www.goibibo.com in the browser. 2.View flight tickets for Delhi to Dubai on 30th April, 2020, without booking.
Gmail.com	1.Enter the URL www.gmail.com in the browser 2.Enter email address of the user: ‘dissertationtest20@gmail.com’. 3.Enter user’s email password: ‘TEST2020@g’ 4.View some emails from the inbox and sign out
YouTube.com	1.Enter the URL www.youtube.com in the browser. 2.Search keyword “how to spy on a mobile phone” in YouTube search. 3.Play and watch the video titled “How to Spy on a Cell Phone with IMEI Number”.

D. Methodology

1. The browser was firstly launched in its respective private browsing mode and populated with the pre-defined browsing activities given in Table 1.
2. The physical memory was then captured without closing the browser window using memory tools for further analysis. For Windows OS, FTK Imager Lite was used whereas for MacOS, OSXPmem was used.
3. The browser window was then closed and a second dump of the memory was further taken.
4. After capturing the memory in both the scenarios, the default locations where each browser store their browsing artifacts in cases of normal web browsing [4], were analyzed.
5. The previously captured memory was then analyzed in WinHex for the presence of any private browsing artifacts. Various keywords related to the predefined activities such as the URLs and the search terms were used in the string search to find related artifacts on the physical memory.

IV RESULTS AND ANALYSIS

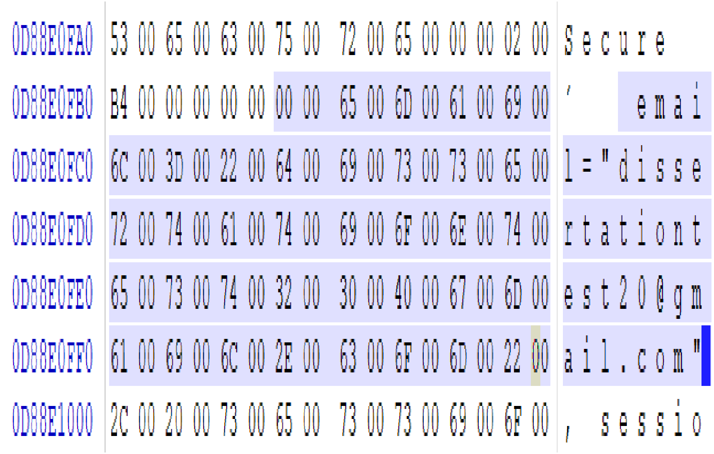
This section describes the findings from the experiments conducted on each web browser on both the operating systems.

A. Analysis of Default Locations of browsing artifacts

After identical browsing activities were carried out on all the browsers and the physical memory was imaged before and after closing the browser; the common locations where artifacts of normal browsing session are stored by default were analyzed to determine whether it records artifacts of private browsing session as well. However, no traces of any of the browsing activities were found on both the operating systems. The only exception was Microsoft Edge on Windows, where the file path of the downloaded image was found along with the time stamp when analyzed in BrowsingHistoryViewer.

B. Analysis of Physical Memory for evidence from browser Microsoft Edge

Windows OS: On analysis of the memory dump taken before closing the browser, various browser related entries were found in both the cases. The URLs of websites visited, email Id, search query and downloaded image file were found to exist in memory. The author, date and time of publishing and even the comment section could be retrieved in case of “thoughtcatalog.com” and as for the travelling website “goibibo.com”, details of the flight search including the origin, destination and date of departure were also found. However, when the browser was closed, the available artifacts were found to be lesser and became limited to the visited URLs and search query while there was no information on email communication, details of the flight search or the video watched on YouTube, as shown in Fig. 1.



```
0D88E0FA0  53 00 65 00 63 00 75 00  72 00 65 00 00 00 02 00  Secure
0D88E0FB0  B4 00 00 00 00 00 00 00  65 00 6D 00 61 00 69 00  '   emai
0D88E0FC0  6C 00 3D 00 22 00 64 00  69 00 73 00 73 00 65 00  l="disse
0D88E0FD0  72 00 74 00 61 00 74 00  69 00 6F 00 6E 00 74 00  rtationt
0D88E0FE0  65 00 73 00 74 00 32 00  30 00 40 00 67 00 6D 00  est20@gm
0D88E0FF0  61 00 69 00 6C 00 2E 00  63 00 6F 00 6D 00 22 00  ail.com"
0D88E1000  2C 00 20 00 73 00 65 00  73 00 73 00 69 00 6F 00  , sessio
```

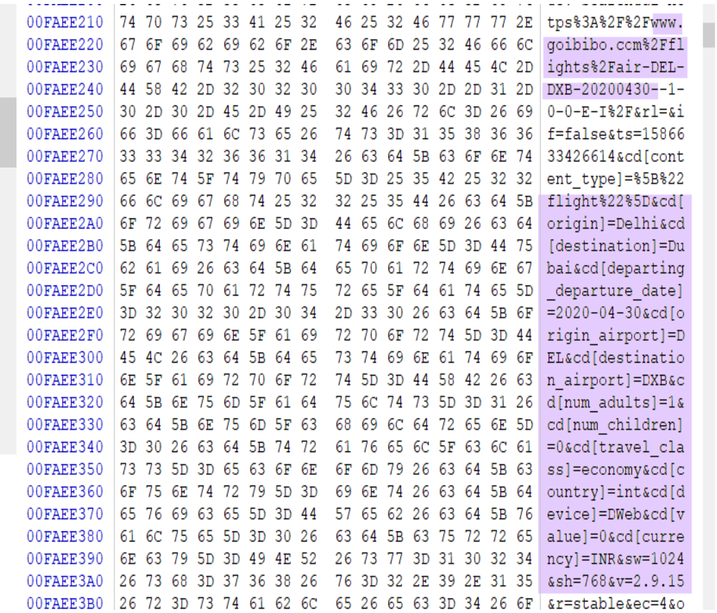
Figure 1: Screenshot of the Gmail Id "dissertationtest@gmail .com" found on analysis of Microsoft Edge with WinHex

MacOS: Analyzing the memory dumps taken after the browser window was closed, yielded similar results as to when it was opened. The keyword search hits that were returned in the two cases included the URLs of the websites visited, downloaded image, email ID and details of the flight search and the video watched on YouTube.

C. Analysis of Physical Memory for evidence from browser Google Chrome

Windows OS: On analyzing the memory dump taken after the browsing session, without closing the browser window, a string search on WinHex returned several hits such as the URLs of websites, downloaded image, and email communication details including the Gmail id as well as some content of the inbox email which was opened during the browsing session. As with the previous browser, details of the flight search including the origin, destination and date of departure were found. In addition to this, the number of travelers, travel class and currency were also found. With the YouTube video, the title and description of the video were found to exist in memory. On closing the browser window, no information of the website "thoughtcatalog.com" or the email communication were found. However, there were still traces of the downloaded image file, URLs of the travel website and the video watched on YouTube.

MacOS: On analysing the memory dumps taken after performing various predefined browsing activities, a number of entries for each of the websites visited during the browsing session were found. Similar to the ones found on Windows, they were the URLs of the websites visited during the session, search queries, downloaded image, email Id and details of the flight search. The details of the YouTube video were limited to the URL and the video title and no description of the video was found. However, it was also found that these entries persisted and were found even after closing the private window. A snapshot of the analysis is shown in Fig. 2.



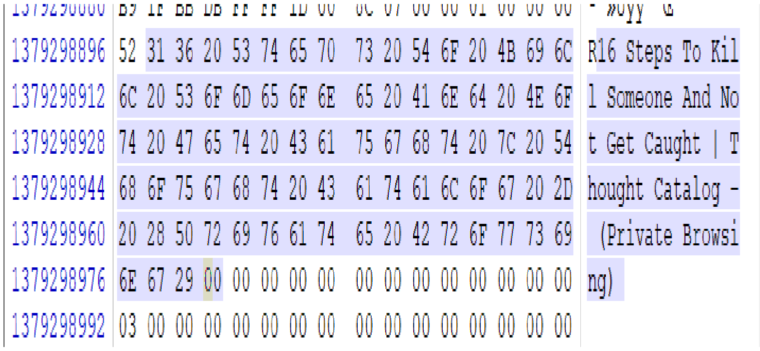
```
00FAEE210  74 70 73 25 33 41 25 32  46 25 32 46 77 77 77 2E  tps%3A%2F%2Fwww.
00FAEE220  67 6F 69 62 69 62 6F 2E  63 6F 6D 25 32 46 66 6C  goibibo.ccm%2Ffl
00FAEE230  69 67 68 74 73 25 32 46  61 69 72 2D 44 45 4C 2D  ights%2Fair-DEL-
00FAEE240  44 58 42 2D 32 30 32 30  30 34 33 30 2D 2D 31 2D  DXB-20200430--1-
00FAEE250  30 2D 30 2D 45 2D 49 25  32 46 26 72 6C 3D 26 69  0-0-E-I%2F&rl=&i
00FAEE260  66 3D 66 61 6C 73 65 26  74 73 3D 31 35 38 36 36  f=false&ts=15866
00FAEE270  33 33 34 32 36 36 31 34  26 63 64 5B 63 6F 6E 74  33426614&cd[cont
00FAEE280  65 6E 74 5F 74 79 70 65  5D 3D 25 35 42 25 32 32  ent_type]=%5B%22
00FAEE290  66 6C 69 67 68 74 25 32  32 25 35 44 26 63 64 5B  flight%22%5D&cd[
00FAEE2A0  6F 72 69 67 69 6E 5D 3D  44 65 6C 68 69 26 63 64  origin]=Delhi&cd
00FAEE2B0  5B 64 65 73 74 69 6E 61  74 69 6F 6E 5D 3D 44 75  [destination]=Du
00FAEE2C0  62 61 69 26 63 64 5B 64  65 70 61 72 74 69 6E 67  bai&cd[departing
00FAEE2D0  5F 64 65 70 61 72 74 75  72 65 5F 64 61 74 65 5D  _departure_date]
00FAEE2E0  3D 32 30 32 30 2D 30 34  2D 33 30 26 63 64 5B 6F  =2020-04-30&cd[o
00FAEE2F0  72 69 67 69 6E 5F 61 69  72 70 6F 72 74 5D 3D 44  rigin_airport]=D
00FAEE300  45 4C 26 63 64 5B 64 65  73 74 69 6E 61 74 69 6F  EL&cd[destinatio
00FAEE310  6E 5F 61 69 72 70 6F 72  74 5D 3D 44 58 42 26 63  n_airport]=DXB&c
00FAEE320  64 5B 6E 75 6D 5F 61 64  75 6C 74 73 5D 3D 31 26  d[num_adults]=1&
00FAEE330  63 64 5B 6E 75 6D 5F 63  68 69 6C 64 72 65 6E 5D  cd[num_children]
00FAEE340  3D 30 26 63 64 5B 74 72  61 76 65 6C 5F 63 6C 61  =0&cd[travel_cla
00FAEE350  73 73 5D 3D 65 63 6F 6E  6F 6D 79 26 63 64 5B 63  ss]=economy&cd[c
00FAEE360  6F 75 6E 74 72 79 5D 3D  69 6E 74 26 63 64 5B 64  ountry]=int&cd[d
00FAEE370  65 76 69 63 65 5D 3D 44  57 65 62 26 63 64 5B 76  evice]=DWeb&cd[v
00FAEE380  61 6C 75 65 5D 3D 30 26  63 64 5B 63 75 72 72 65  alue]=0&cd[curre
00FAEE390  6E 63 79 5D 3D 49 4E 52  26 73 77 3D 31 30 32 34  ncy]=INR&sw=1024
00FAEE3A0  26 73 68 3D 37 36 38 26  76 3D 32 2E 39 2E 31 35  &sh=768&v=2.9.15
00FAEE3B0  26 72 3D 73 74 61 62 6C  65 26 65 63 3D 34 26 6F  &r=stable&ec=4&o
```

Figure 2: Screenshot of the flight details from Mac OS Google Chrome on analysis with WinHex

D. Analysis of Physical Memory for evidence from browser Mozilla Firefox

Windows OS: Browsing related entries such as the URLs visited, email ID, image download, details of flight search and video watched on YouTube were found in both the cases. However, the number of entries greatly decreased when the browser was closed.

MacOS: On analyzing the captured memory that were taken before as well as after closing the private window, browsing related entries similar to those found in windows OS were found. One exception is the password of the email id which was found when the browser was open. Another detail of interest that was found was the term "Private Browsing" which was found next to the search queries and the page title (thoughtcatalog.com) as well as the video title, indicating the use of private browsing instead of regular browsing.

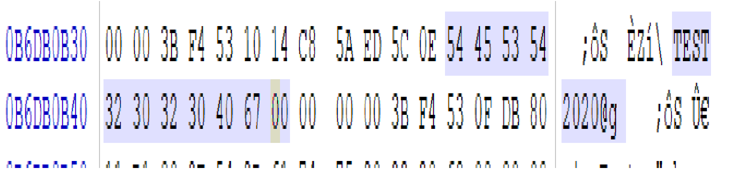


```
1379298896  52 31 36 20 53 74 65 70  73 20 54 6F 20 4B 69 6C  R16 Steps To Kil
1379298912  6C 20 53 6F 6D 65 6F 6E  65 20 41 6E 64 20 4E 6F  l Someone And No
1379298928  74 20 47 65 74 20 43 61  75 67 68 74 20 7C 20 54  t Get Caught | T
1379298944  68 6F 75 67 68 74 20 43  61 74 61 6C 6F 67 20 2D  hought Catalog -
1379298960  20 28 50 72 69 76 61 74  65 20 42 72 6F 77 73 69   (Private Browsi
1379298976  6E 67 29 00 00 00 00 00  00 00 00 00 00 00 00 00  ng)
1379298992  03 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Figure 3: Screenshot of the article viewed on Firefox on MacOS along with private browsing indicator found on analysis with WinHex

E. Analysis of Physical Memory for evidence from Brave Browser

Windows OS: Similar to the other browsers, various browsing related entries were found in both the memory dumps captured before and after closing the Private window. The URLs visited, email Id, image download, details of flight search and video watched on YouTube were found to exist in memory, which became lesser after closing the Private browser window. Brave was the only browser among the four that gave a positive hit for the password of the email id, that is, "TEST2020@g" in Windows 10. However, it was no longer found on analyzing the memory dump taken after the browser was closed. A snapshot of the analysis is shown in Fig. 4.



```
0B6DB0B30  00 00 3B F4 53 10 14 C8  5A ED 5C 0E 54 45 53 54    ;ôS ÈZí\ TEST
0B6DB0B40  32 30 32 30 40 67 00 00  00 00 3B F4 53 0F DB 80  2020@g    ;ôS Û€
```

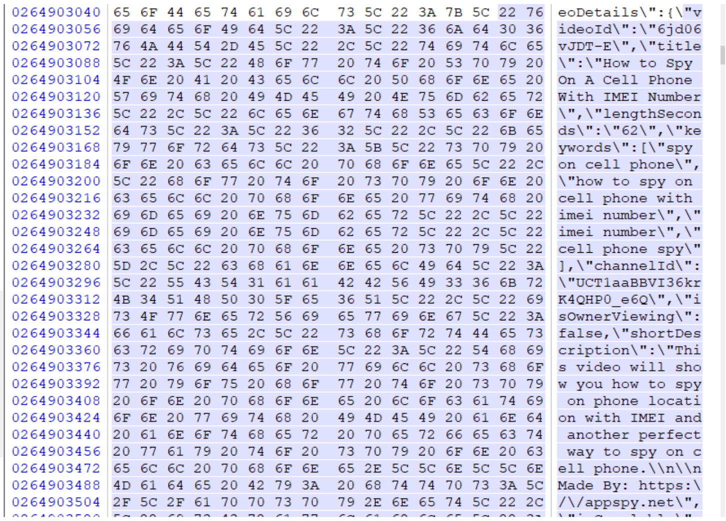
Figure 4: Screenshot of the email password on Brave in Windows 10 found on analysis with WinHex

MacOS: On analysing the captured memory with the help of string search on WinHex, the following browser related entries were found: URLs of the visited websites, search queries, downloaded image, and email Id with some content of the inbox mail that was opened, details of flight search and YouTube Video.

F. Analysis of Physical Memory for evidence from Apple Safari browser

MacOS: The analysis of the memory dump taken after closing the private window gave the same results as that of the memory dump that was taken while the browser was kept opened. Not only were the URLs of the websites and the email Id found, but also the password of the email Id, that is, "TEST2020@g" was found to exist in memory even after the browser was closed. Other entries such as the downloaded image, details of the flight search including the origin, destination and the date of departure as well as the details of the YouTube video including the video title and description also surfaced when analyzed with WinHex, as shown in Fig. 5.

Between the two operating systems opted for this study, Windows 10 was clearly found to store a lesser number of artifacts than MacOS Sierra. Although each browser in both the operating systems exhibited notable amount of entries for each of the predefined browsing activities, there was a clear-cut difference in the number of entries stored by each of the browsers in the two different operating systems. Moreover, on analyzing the memory dumps taken after closing the browser windows, there were significantly lesser entries in Windows 10 (listed in Table 2). However, the closure of the browser windows seemed to have little effect in case of MacOS that resulted in somewhat similar amount of entries (given in Table 3) on analyzing dumps taken before and after terminating the browsing sessions.



```
0264903040  65 6F 44 65 74 61 69 6C  73 5C 22 3A 7B 5C 22 76  eoDetails\":{\"v
0264903056  69 64 65 6F 49 64 5C 22  3A 5C 22 36 6A 64 30 36  ideoId\":\"6jd06
0264903072  76 4A 44 54 2D 45 5C 22  2C 5C 22 74 69 74 6C 65  vJDT-E\",\"title
0264903088  5C 22 3A 5C 22 48 6F 77  20 74 6F 20 53 70 79 20  \":\"How to Spy 
0264903104  4F 6E 20 41 20 43 65 6C  6C 20 50 68 6F 6E 65 20  On A Cell Phone 
0264903120  57 69 74 68 20 49 4D 45  49 20 4E 75 6D 62 65 72  With IMEI Number
0264903136  5C 22 2C 5C 22 6C 65 6E  67 74 68 53 65 63 6F 6E  \",\"lengthSecon
0264903152  64 73 5C 22 3A 5C 22 36  32 5C 22 2C 5C 22 6B 65  ds\":\"62\",\"ke
0264903168  79 77 6F 72 64 73 5C 22  3A 5B 5C 22 73 70 79 20  ywords\":[\"spy 
0264903184  6F 6E 20 63 65 6C 6C 20  70 68 6F 6E 65 5C 22 2C  on cell phone\",
0264903200  5C 22 68 6F 77 20 74 6F  20 73 70 79 20 6F 6E 20  \"how to spy on 
0264903216  63 65 6C 6C 20 70 68 6F  6E 65 20 77 69 74 68 20  cell phone with 
0264903232  69 6D 65 69 20 6E 75 6D  62 65 72 5C 22 2C 5C 22  imei number\",\"
0264903248  69 6D 65 69 20 6E 75 6D  62 65 72 5C 22 2C 5C 22  imei number\",\"
0264903264  63 65 6C 6C 20 70 68 6F  6E 65 20 73 70 79 5C 22  cell phone spy\"
0264903280  5D 2C 5C 22 63 68 61 6E  6E 65 6C 49 64 5C 22 3A  ],\"channelId\":
0264903296  5C 22 55 43 54 31 61 61  42 42 56 49 33 36 6B 72  \"UCT1aaBBVI36kr
0264903312  4B 34 51 48 50 30 5F 65  36 51 5C 22 2C 5C 22 69  K4QHP0_e6Q\",\"i
0264903328  73 4F 77 6E 65 72 56 69  65 77 69 6E 67 5C 22 3A  sOwnerViewing\":
0264903344  66 61 6C 73 65 2C 5C 22  73 68 6F 72 74 44 65 73  false,\"shortDes
0264903360  63 72 69 70 74 69 6F 6E  5C 22 3A 5C 22 54 68 69  cription\":\"Thi
0264903376  73 20 76 69 64 65 6F 20  77 69 6C 6C 20 73 68 6F  s video will sho
0264903392  77 20 79 6F 75 20 68 6F  77 20 74 6F 20 73 70 79  w you how to spy
0264903408  20 6F 6E 20 70 68 6F 6E  65 20 6C 6F 63 61 74 69   on phone locati
0264903424  6F 6E 20 77 69 74 68 20  49 4D 45 49 20 61 6E 64  on with IMEI and
0264903440  20 61 6E 6F 74 68 65 72  20 70 65 72 66 65 63 74   another perfect
0264903456  20 77 61 79 20 74 6F 20  73 70 79 20 6F 6E 20 63   way to spy on c
0264903472  65 6C 6C 20 70 68 6F 6E  65 2E 5C 5C 6E 5C 5C 6E  ell phone.\\n\\n
0264903488  4D 61 64 65 20 42 79 3A  20 68 74 74 70 73 3A 5C  Made By: https:\
0264903504  2F 5C 2F 61 70 70 73 70  79 2E 6E 65 74 5C 22 2C  /\/appspy.net\",
```

Figure 5: Screenshot of the details of the YouTube video watched on Safari in MacOS Sierra found on analysis with WinHex

While all the browsers in both the operating systems returned hits for the email address "dissertationtest20@gmail.com", Brave was the only browser that displayed the password for the email Id in Windows 10. Nevertheless, it did not store the password in memory after the browser was closed. In case of MacOS, two browsers, namely Safari and Firefox, returned hits for the password of the email address "TEST2020@g. In case of Safari, the password was found to exist in memory even after the closure of the private browsing window. As for Firefox, it was found in memory only when the private browsing window was open. Moreover, memory dumps of Firefox taken before and after closing the browser in MacOS had browser related entries that clearly indicated the use of private browsing mode.

V CONCLUSIONS

All the browsers deployed for the study claimed that the usual browser related information such as search history, cookies, temporary cache files, etc., would either not be recorded or deleted from memory once the browser was closed. This study was undertaken to test the effectiveness of this claim and to ensure the ways in which a forensic investigation may go about in such cases.

Although, no traces of the pre defined activities carried out in the private mode were found in the default locations in all the browsers of both the operating systems, except for Microsoft Edge, yet, the artifacts of private browsing were plentiful in the physical memory. The results of this study have shown that it is very much possible to find remnants of the browsing activities in memory in cases where a live system is encountered, even after closing the browser window. It has also shown that if such an opportunity arises, then the traces of browsing artifacts can be recovered through RAM forensics using various available open source tools. Nevertheless, although the amount of artifacts varied among the browsers as well as the operating systems, yet since all of them did leave behind a significant amount of evidences of private browsing, it would not be practical to pinpoint a single browser as the most private, based on the number and type of entries alone. In conclusion, it is clear that the private modes of the browsers have not been very effective in maintaining the privacy of the browsing sessions. Therefore, from the user's point of view, it is reasonable to state that the private modes of browsers in reality are not really that private. However, these traces of private browsing artifacts present in RAM could thus, prove to be potential evidence, in cases where live systems are encountered. Therefore, although the artifacts found in memory undermined the privacy claim of the browser vendors, on the other hand, it has also proven its significance as forensically valuable information in cases of questionable web activities for investigators.

Table 2: Number of entries of each predefined browsing activity found on Windows 10 on analyzing the dumps taken before and after closing the browsing session on WinHex

Keywords	**Edge (open)**	**Chrome (open)**	**Firefox (open)**	**Brave (open)**	**Edge (closed)**	**Chrome (closed)**	**Firefox (closed)**	**Brave (closed)**
thoughtcatalog.com	323	1103	166	244	6	11	7	6
Search term “best way to get away with murder”	0	0	0	6	0	0	0	0
Page title “16 steps to kill someone and not get caught”	7	3	0	9	0	0	0	0
Search term “Parasite"	165	1	0	11	18	18	37	31
Downloaded image file	7	30	20	30	1	12	1	17
www.goibibo.com	109	553	172	322	50	3	10	2
dissertationtest20@gmail.com	1	49	3	70	0	0	1	0
Email password “TEST2020@g”	0	0	0	1	0	0	0	0
Search term “How to spy on a mobile phone”	0	44	61	58	0	0	0	4
Video title “How to spy on a cell phone with IMEI number”	0	25	42	46	0	0	1	3

Table 3: Number of entries of each predefined browsing activity found on MacOS Sierra on analyzing the dumps taken before closing (O) and after closing (C) the browser window on WinHex

Keywords	Safari (O)	Edge (O)	Chrome (O)	Firefox (O)	Brave (O)	Safari (C)	Edge (C)	Chrome (C)	Firefox (C)	Brave (C)
thoughtcatalog.com	597	823	87	275	440	582	892	67	253	494
Search term “best way to get away with murder”	21	0	0	1	5	10	0	0	1	0
Page title “16 steps to kill someone and not get caught”	12	3	0	1	5	9	2	0	1	3
Search term “Parasite"	290	224	150	56	462	336	228	136	39	149
Downloaded image file	70	69	45	32	80	41	113	31	20	81
www.goibibo.com	1157	1010	791	403	1380	977	1000	711	374	1080
dissertationtest20@gmail.com	40	17	5	13	967	31	14	5	6	56
Email password “TEST2020@g”	3	0	0	1	0	4	0	0	0	0
Search term “How to spy on a mobile phone”	105	0	49	56	84	48	0	0	27	6
Video title “How to spy on a cell phone with IMEI number”	47	125	60	35	56	0	0	0	0	0

REFERENCES

[1] P. Gralla and M. Troller, “How the Internet Works”, (8th Edition). London, United Kingdom: Que Pub, 2006.

[2] H. Said, N. Al Mutawa, I. Al Awadhi and M. Guimaraes, “Forensic analysis of private browsing artifacts”, In 2011 International Conference on Innovations in Information Technology, IEEE pp. 197-202, 2011.

[3] M. Vermaat, S. Sebok, M. Frydenberg, S. Freund and J. Campbell, “Discovering Computers, Essentials”, Nelson Education, 2015.

[4] E. Noorulla. Web browser private mode forensics analysis, 2011.

[5] G. Aggarwal, E. Bursztein, C. Jackson and D. Boneh, “An Analysis of Private Browsing Modes in Modern Browsers.” In USENIX security symposium, pp. 79-94, 2010.

[6] D. Ohana and N. Shashidhar, “Do Private and Portable Web Browsers Leave Incriminating Evidence?” In Proceedings of the International Workshop on Cyber Crime, San Francisco, CA 2013

[7] A. Ghafarian and S. Seno, “Analysis of privacy of private browsing mode through memory forensics.” International Journal of Computer Applications, 132(16), 2015.

[8] Montasari R and Peltola P, “Computer forensic analysis of private browsing modes.” In International Conference on Global Security, Safety, and Sustainability, pp. 96-109, Springer, Cham, 2015.

[9] Soghoian C, “Why private browsing modes do not deliver real privacy.” Center for Applied Cyber security Research, Bloomington. 2011.

[10] Gao X, Yang Y, Fu H, Lindqvist J and Wang Y, “Private browsing: An inquiry on usability and privacy protection.” In Proceedings of the 13th Workshop on Privacy in the Electronic Society pp. 97-106, 2014.

[11] Wu Y, Gupta P, Wei M, Acar Y, Fahl S and Ur B, “Your secrets are safe: How browsers' explanations impact misconceptions about private browsing mode.” In Proceedings of the 2018 World Wide Web Conference, pp. 217-226, 2018.

[12] Lerner BS, Elberty L, Poole N and Krishnamurthi S. “Verifying web browser extensions’ compliance with private-browsing mode.” In European Symposium on Research in Computer Security, Springer, Berlin, Heidelberg, pp. 57-74, 2013.

[13] B. Zhao and P. Liu, “Private browsing mode not really that private: Dealing with privacy breach caused by browser extensions.” In 45th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, IEEE, (pp. 184-195), 2015.

[14] R. Gabet, K. Seigfried-Spellar and M. Rogers, “A comparative forensic analysis of privacy enhanced web browsers and private browsing modes of common web browsers.” International Journal of Electronic Security and Digital Forensics, 10 (4), pp. 356-371, 2018.

[15] VirtualBox - Download VirtualBox, Oracle. Available from: https://www.virtualbox.org/wiki/Downloads [Accessed on 21st February 2020].

[16] AccessData - Product Downloads. Available from: https://accessdata.com/product-download [Accessed on 24th February 2020].

[17] Pmem - OSXPMem - Mac OS X Physical Memory acquisition tool. Available from: https://code.google.com/archive/p/pmem/wikis/OSXPmem.wiki [Accessed on 23rd February 2020].

[18] X-ways - WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor. Available from: https://www.x-ways.net/winhex [Accessed on 25th February 2020].

[19] DB Browser for SQLite, 2020, Downloads, Available from: https://sqlitebrowser.org/dl/ [Accessed on 25th February 2020].

[20] Nirsoft - Web Browser Tools Package. Available from: https://www.nirsoft.net/web_browser_tools.html [Accessed on 25th February 2020].