Received: July 17, 2020. Revised: August 25, 2020.

*International Journal of*
Intelligent Engineering & Systems

http://www.inass.org/

# Private Browsing Forensic Analysis: A Case Study of Privacy Preservation in the Brave Browser

**Ahmed Redha Mahlous[1]*** **Houssam Mahlous[2]**

[1]*Prince Sultan University, Kingdom of Saudi Arabia*
[2]*King's College London University, United Kingdom*
* Corresponding author's Email: armahlous@psu.edu.sa

**Abstract:** The Internet and its users are in continual growth. With it grows the number of organized crimes on the Internet and the potential for individuals to carry out illegal activities. These criminals have gained more awareness of private browsing facilities, and many have found a haven in privacy designed browsers that cover up their tracks and shield their nefarious actions. The development of these privacy features has proven to be a challenge for digital forensic investigators. They strive to perform a thorough analysis of web browsers to collect artefacts relating to illegal activity to be presented as evidence to the court of law and used to convict criminals. "Brave" browser is one of the most recent and fastest-growing private browsers that, up to this point, has not been studied in-depth, and its privacy preservation functionality remains unclear. In this paper, we studied Brave's private browsing mode, examined its privacy-preserving and forensic data acquisition, and outlined the location and type of evidence available through live and post-mortem state analysis. The unique approach taken included a set of experiments that unveiled how the browser functions and showed the appropriate tools that could be utilized to extract leftover artefacts. Analysis of our results showed that despite Brave leaving no traces of browsing activity on the Hard Disk, visited URLs, images, keyword searches, and even cached videos were retrievable from the RAM, which shows that Brave is not entirely private.

**Keywords:** Private browsing, Web browser forensics, Forensic acquisition and analysis, Live data forensics, Post-mortem forensics, Brave browser, Private browsing forensics.

## 1 Introduction

Accessing the Internet nowadays has become nearly inevitable, and web browsers remain the most popular tool to do so. The increased amount of web browser users and their aspiration to achieve paramount personal privacy has pushed developers to devise different ways to fulfil the users' need for anonymity and seclusion. One of the outcomes of this campaign was the development of private browsing modes whose main aim is to keep user's browsing sessions private from other users of the same device [1] by not retaining temporary session data. Despite this feature proving useful for people working from shared computers at work, school, and libraries, they are not the only ones enjoying the fruits of it. Cybercriminals have taken advantage of private browsing modes to clear any digital traces leftover on the machine used and leave computer forensic examiners empty-handed. The UK Office for National Statistics (ONS) estimates that around 4.5 million cybercrimes were committed in England and Wales during the year of 2018 only [2]. This further shows the vital importance of capturing and analysing digital evidence for any computer forensic investigation as it can pinpoint the source of compromise which could be the silver bullet that connects criminals and brings them to justice. We've taken it upon our shoulders to investigate Brave Browser and its private mode to try and examine the artefacts left behind, if any, from private browsing sessions and what tools can be used to extract them as well as their locations. Similar studies usually use digital forensic tools to scan the whole memory in general and search only for keywords relating to browsing session activity after using the browser, and this is not always accurate as sometimes browsers store session data in hex code for example rather than plain English and this will not be picked up by general keyword searches like these. For our approach, however, we decided to take it two steps further in order to search for artefacts in the right places and leave a smaller margin for error. First, we took a snapshot of the memory before installing the browser and one right after. This allowed us to pinpoint the files and folders created by Brave, which focuses our search later on as they are the most probable storage locations for Brave's browsing session data. After that, we used Brave in its normal browsing mode (not the private mode) and snapshots of the memory were taken and consequently compared with snapshots of the memory after using the browser in its private mode. This has many advantages as it allowed us to identify the behaviour of the browser in both modes and observe the differences in the types of files stored, the amount of data, the data content, and check whether Brave's private mode just simply deletes the files that would normally be left in the normal browsing mode, or whether it doesn't store them in the first place. Furthermore, we performed a live memory analysis to recover any artefacts from the RAM as well as a post-mortem analysis to retrieve them from the Hard Disk.

The remainder of the paper is organized as follows: Section 1 presents the introduction. Section 2 presents browser forensic background; then, analysis environment preparation is presented in Section 3. The forensic analysis methodology is discussed in detail in Section 4. Section 5 describes results and analysis, while section 6 presents a discussion for the results. Finally, we conclude and discuss future work in Section 7.

## 2 Browser forensics background

Web browser forensics is a branch of digital forensics that aims to identify and collect evidence and essential information related to a crime from recovered traces of browsing sessions to be used for forensic investigation purposes. Browsers store a notable proportion of user data and their browsing activities that range from cached files and visited URLs to usernames and passwords used during browsing sessions. This has led to the development of private browsing modes and consequently private browsers that claim to erase all data related to a browsing session and prevent it from persisting on the device as a way to honour the privacy of its users. Since the introduction of private modes in 2005 by Apple Safari, many researchers went forward to test the extent of truth in these claims and whether private browsing modes actually behave as advertised and provide users with the protection they rely on and believe they have. The study [3] in 2014 defined a threat model and then conducted experiments by applying common local and remote attacks to assess the security of private browsing in the four most popular browsers: Chrome, Safari, Firefox and IE. Analysis of the results obtained brought to light a range of vulnerabilities applicable to private browsing implementations due to a couple of reasons, such as lack of control of extensions running in private mode and negligence of edge case testing. Furthermore, bookmarks and program crashes were proved to cause privacy leaks.

These four browsers were put to the test again in [4]. The experimental results made after the machine was turned off showed that private modes in Firefox, IE and Safari left traces of browsing data that are easily recoverable by using the right tools, while Chrome's Incognito did not leave any browsing artefacts behind.

In 2018, the study [5] further showed that private browsing data created by browsers such as Chrome, Firefox, IE, Safari and Opera could be retrieved from the RAM using RAM imaging or from the hard disk.

Knowing that browsers leak private browsing data is something, but the location of these artefacts is of utter importance. Researchers in [6] investigated web browser's log files which usually store cache, history and cookie files in a Windows environment. It brought to notice the limitations of methodologies in digital forensics and existing tools at that time, then proposed advanced methodology to tackle them. The study conducted also introduced a new tool, WEFA, which parses these log files and provides various functionality such as timeline analysis, user activity classification, report generation as well as recovering deleted log files. Another study [7] also observed web browser log files for Opera, Chrome, Firefox, and IE and suggested an evidence collection methodology that would help to analyse and extract information from these log files using tools like Autopsy, NetAnalysis, and Internet Evidence Finder.

So far, log files have proven to be a gold mine for private investigators, but it is not the only location where browsers leave evidence trails. Researchers in [8] examined the recoverable artefacts leftover by browsers using private browsing modes and portable browsers. The four major browsers tested were IE, Firefox, Chrome and Safari, and the results showed that most leftover artefacts were found in RAM and Orphan directories. Nihad A. Hassan in his book "Digital Forensics Basics" [9] conveys how to

Received: July 17, 2020. Revised: August 25, 2020.

investigate web browsers and e-mail messages for forensics artefacts. It includes valuable information as to where each browser stores its cookies, history, typed URLs and cache as well as step by step analysis to extract valuable information from email headers such as the sender's geographic location.

A somewhat more general study [10] in 2019 examined the "privateness" of 30 web browsers on a Windows 10 OS. The experimental results showed that some browsers leaked browsing session data and almost all of them had keyword hits using a triage-style keyword search. The keyword hits were mainly found in log files, free space, $MFT and .dat files.

There are various tools that could be used to extract the information left behind by browsing sessions. Researchers in [11] observe major web browser analysis tools in a Windows environment and highlights the advantages and limitations of some over the others. The study also shows that using a carving tool such as ESECarve, Internet explorer's InPrivate browsing records can be retrieved from various areas on the disk such as the database file, WebCacheV01.dat and log files. Work by Chivers [12] on InPrivate browsing mode, which claims that it prevents local storage on a computer, also revealed that recovery of browsing records is possible either from database log files or by carving records of the disk even after a machine is powered down.

Similar investigations have been made on other browsers. The research paper [13] studied three privacy-enhanced web browsers, Epic, Commodo and Dooble, and compared their private browsing modes with those of three commonly used browsers, Edge, Firefox, and Chrome, based on the number of recoverable artefacts produced and their contents. The study used FTK and Autopsy as tools to find the number of residual artefacts on Windows operated machines, and only used ten websites to generate web traffic. However, the results were inconclusive as to whether any of the two groups provided better privacy than the other.

Similarly, [14] examined Browzar, a privacy-preserving Internet browser, and compared its results with Chrome and Firefox. The study was based on change monitoring, live data forensics and post-mortem analysis, carried out using a set of tools primarily composed of Procmon, IEF, FTK and X-Ways. Based on the evidence found and analysis conducted, it was shown that out of the three browsers, Browzar left the most information behind, including files, folders, keyword searches, URLs, and pictures.

Another study [15] conducted live and post-mortem analysis of the Epic Privacy Browser on Windows 7 & and Windows 10 machines; the study found out that despite temporary files and folders being cleared at the end of a browsing session, there were still remnant traces that could be recovered using standard tools such as IEF and Regshot.

Despite all the research conducted on different web browsers and their private modes, we noticed a lack of attention given to Brave, a browser which prides itself in the security and privacy it provides and has over 13.5 million active users per month [16] who rely on it for their personal use. This paper aims to bridge this gap and present details that might be of use to both users and private investigators alike.

## 3 Analysis environment preparations

In this paper we studied the behaviour of Brave browser in private mode on a Windows 10 machine. The choice of Windows 10 is justified by the fact that it holds 87.82% share of the market, as shown in Fig. 1.

To do our forensic analysis, a clean environment that avoids mixing browsing artefacts was mandatory. With many options at hand to achieve this, we settled on using a virtualized environment using VMWare Fusion. Other than providing a clean environment out of the box, this choice is further justified for the following reasons:

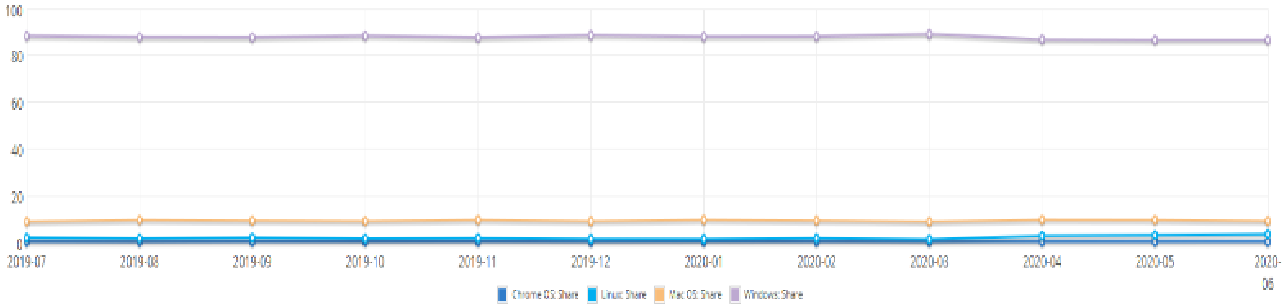


Figure. 1 Operating system share by version [17]

1. Using virtualization will allow us to set only one base virtual machine with necessary configuration, then multiple snapshots could be taken and used later
2. Saving Experiment time, knowing that taking a snapshot would require only a few seconds.
3. Possibility to revert the machine to its initial state easily and quickly.

A Windows 10 virtual machine based on a .iso image acquired from our academic software license portal [18] was used. A pre-configured 1 TB hard disk drive that was wiped according to the NIST 800-88 Standard for Media Sanitization [19] and contained separate tools and evidence part was connected to a MacBook Pro computer. Its primary purpose was to run the tools and store the vmdk image and RAM (dump) for post-mortem forensic examination.

A fresh Windows 10 operating system was installed on the virtual machine. The Brave browser was then installed on the system using an installer that was transferred via a USB. Doing so ensured that the environment was kept as clean as possible, eliminating the chance of mixing the artefacts left by the default browser with the ones left by the Brave browser later on.

The following tools were installed for conducting the analysis:

- FTK Imager [20]
- Autopsy 4.15.0 [21].
- Regshot [22]
- Internet Evidence Finder V6.4 [23]
- WinHex [24].

To make the experiment as realistic as possible, the tasks listed below (based on the most visited websites in the UK as of July 2020 [25] were performed with the Brave browser. A keyword search (using Autopsy) was conducted before performing the tasks to rule out any possible cause of contamination. No results were found for any of the keywords from the tasks (e.g. "basic rat python", or the words from Table 1), ensuring that any results found later are not false positives.

Tasks:

1. Visit www.youtube.com, search for "basic rat python" and watch the first video.
2. Visit www.google.com, search for the keywords in Table 1 and click on one of the search results.
3. Visit www.gmail.com and sign in with an account.
4. Visit www.skysports co.uk.

Table 1. Keywords searched and visited URLs

| Keyword | Visited URL |
|---|---|
| Basic rat python | https://www.youtube.com/watch?v=tczUv_RK-fk |
| Cars | https://www.daimler.com/products/passenger-cars/ |
| Malware | https://searchsecurity.techtarget.com/definition/malware |
| Forensic tools | https://techtalk.gfi.com/top-20-free-digital-forensic-investigation-tools-for-sysadmins/ |
| beach | https://www.agoda.com/coco-palm-beach-resort-spa/hotel/phu-quoc-island-vn.html?cid=1844104 |

5. Visit www.amazon.co.uk, search for "MacBook" and view the results.
6. Visit www.bbc.co.uk.

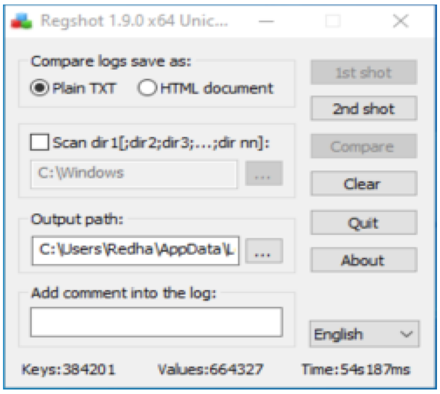
After running these tasks for 48 hours on Brave browser's private mode, a copy of the Random-Access Memory (RAM) was captured using FTK Imager (version 3.1.1.8), prior to shutting down the machine. The VMWare machine was then shut down, and an image of it was acquired using Autopsy [for the post-mortem analysis].

## 4. Forensic analysis methodology

### 4.1 System changes after installing brave browser

To track changes to the system registry as a result of installing the browser, Regshot was used to take a snapshot of the registry before installation (Fig. 2.).

A second snapshot was taken after installing the browser and compared with the first one. Regshot generates a report of the results, showing the new files and folders that were added to the registry key. Searching for "brave" in the report reveals some of the changes that are definitely related to the



Compare logs save as:
● Plain TXT ○ HTML document

□ Scan dir1[;dir2;dir3;...;dir nn]:
C:\Windows

Output path:
C:\Users\Redha\AppData\L

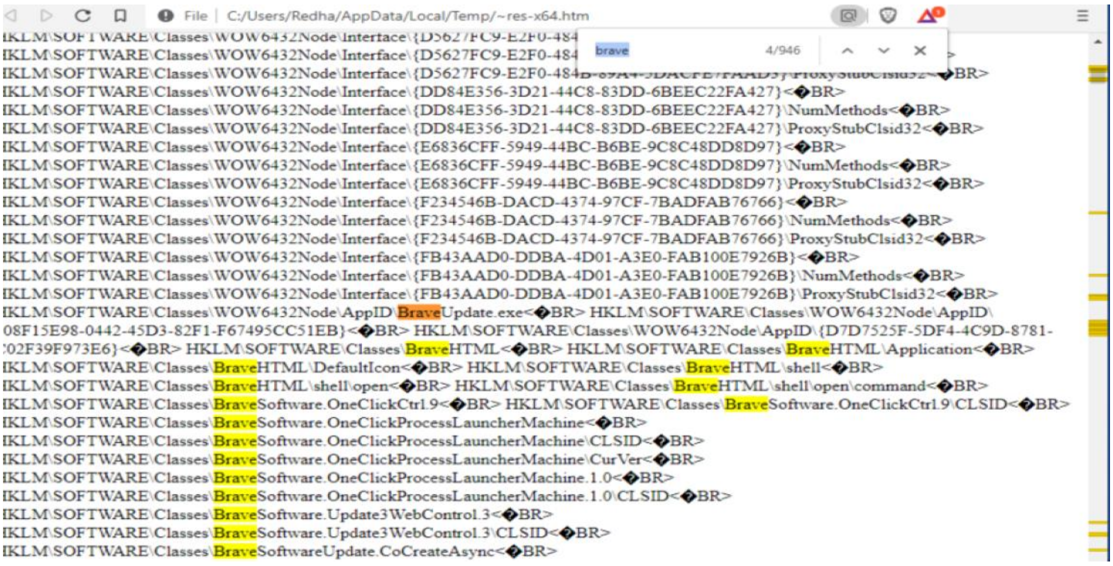
Add comment into the log:

English

Keys:384201 Values:664327 Time:54s187ms

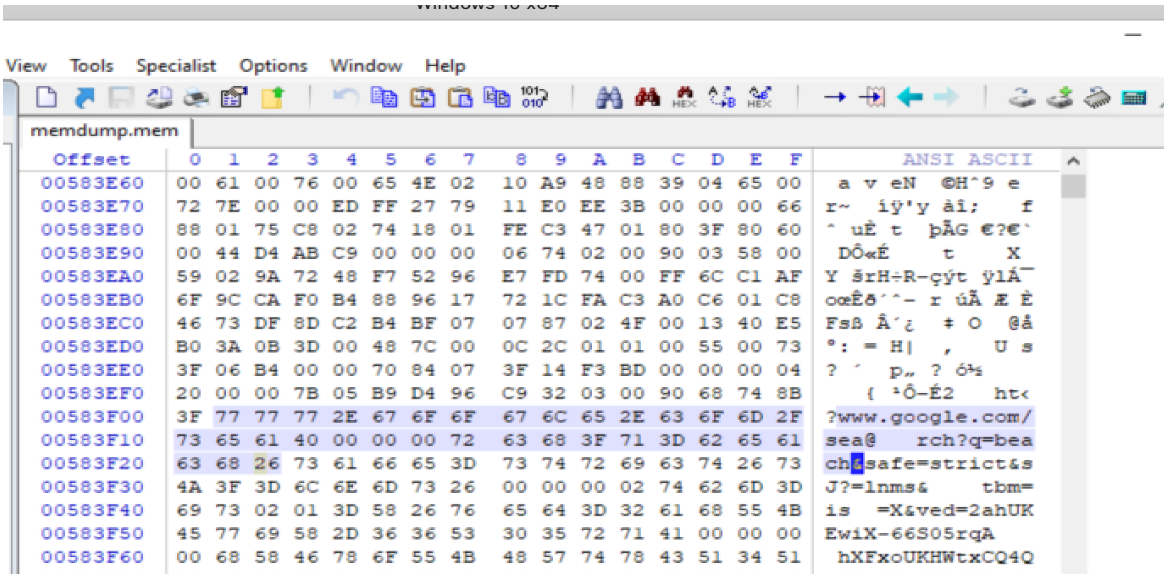
Figure. 2 Regshot 1st shot registry capture (before brave installation)

Received: July 17, 2020. Revised: August 25, 2020.



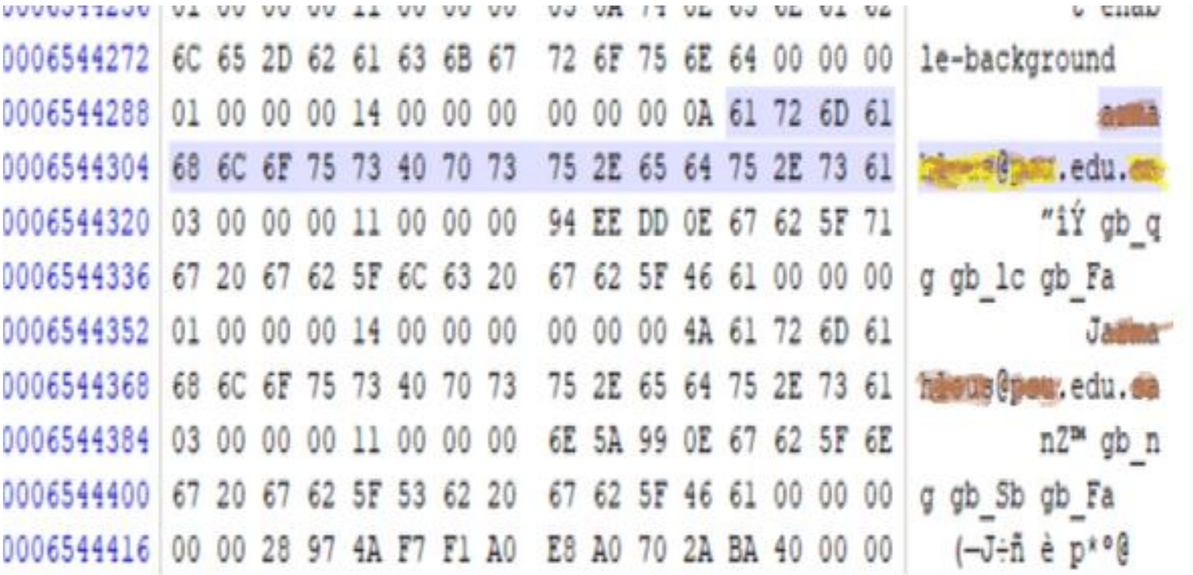
```
IKLM\SOFTWARE\Classes\WOW6432Node\Interface\{D5627FC9-E2F0-484
IKLM\SOFTWARE\Classes\WOW6432Node\Interface\{D5627FC9-E2F0-484
IKLM\SOFTWARE\Classes\WOW6432Node\Interface\{D5627FC9-E2F0-484B-89A4-5DACFE7FAAD5}\ProxyStubClsid32<�BR>
IKLM\SOFTWARE\Classes\WOW6432Node\Interface\{DD84E356-3D21-44C8-83DD-6BEEC22FA427}<�BR>
IKLM\SOFTWARE\Classes\WOW6432Node\Interface\{DD84E356-3D21-44C8-83DD-6BEEC22FA427}\NumMethods<�BR>
IKLM\SOFTWARE\Classes\WOW6432Node\Interface\{DD84E356-3D21-44C8-83DD-6BEEC22FA427}\ProxyStubClsid32<�BR>
IKLM\SOFTWARE\Classes\WOW6432Node\Interface\{E6836CFF-5949-44BC-B6BE-9C8C48DD8D97}<�BR>
IKLM\SOFTWARE\Classes\WOW6432Node\Interface\{E6836CFF-5949-44BC-B6BE-9C8C48DD8D97}\NumMethods<�BR>
IKLM\SOFTWARE\Classes\WOW6432Node\Interface\{E6836CFF-5949-44BC-B6BE-9C8C48DD8D97}\ProxyStubClsid32<�BR>
IKLM\SOFTWARE\Classes\WOW6432Node\Interface\{F234546B-DACD-4374-97CF-7BADFAB76766}<�BR>
IKLM\SOFTWARE\Classes\WOW6432Node\Interface\{F234546B-DACD-4374-97CF-7BADFAB76766}\NumMethods<�BR>
IKLM\SOFTWARE\Classes\WOW6432Node\Interface\{F234546B-DACD-4374-97CF-7BADFAB76766}\ProxyStubClsid32<�BR>
IKLM\SOFTWARE\Classes\WOW6432Node\Interface\{FB43AAD0-DDBA-4D01-A3E0-FAB100E7926B}<�BR>
IKLM\SOFTWARE\Classes\WOW6432Node\Interface\{FB43AAD0-DDBA-4D01-A3E0-FAB100E7926B}\NumMethods<�BR>
IKLM\SOFTWARE\Classes\WOW6432Node\Interface\{FB43AAD0-DDBA-4D01-A3E0-FAB100E7926B}\ProxyStubClsid32<�BR>
IKLM\SOFTWARE\Classes\WOW6432Node\AppID\BraveUpdate.exe<�BR> HKLM\SOFTWARE\Classes\WOW6432Node\AppID\
08F15E98-0442-45D3-82F1-F67495CC51EB}<�BR> HKLM\SOFTWARE\Classes\WOW6432Node\AppID\{D7D7525F-5DF4-4C9D-8781-
:02F39F973E6}<�BR> HKLM\SOFTWARE\Classes\BraveHTML<�BR> HKLM\SOFTWARE\Classes\BraveHTML\Application<�BR>
IKLM\SOFTWARE\Classes\BraveHTML\DefaultIcon<�BR> HKLM\SOFTWARE\Classes\BraveHTML\shell<�BR>
IKLM\SOFTWARE\Classes\BraveHTML\shell\open<�BR> HKLM\SOFTWARE\Classes\BraveHTML\shell\open\command<�BR>
IKLM\SOFTWARE\Classes\BraveSoftware.OneClickCtrl.9<�BR> HKLM\SOFTWARE\Classes\BraveSoftware.OneClickCtrl.9\CLSID<�BR>
IKLM\SOFTWARE\Classes\BraveSoftware.OneClickProcessLauncherMachine<�BR>
IKLM\SOFTWARE\Classes\BraveSoftware.OneClickProcessLauncherMachine\CLSID<�BR>
IKLM\SOFTWARE\Classes\BraveSoftware.OneClickProcessLauncherMachine\CurVer<�BR>
IKLM\SOFTWARE\Classes\BraveSoftware.OneClickProcessLauncherMachine.1.0<�BR>
IKLM\SOFTWARE\Classes\BraveSoftware.OneClickProcessLauncherMachine.1.0\CLSID<�BR>
IKLM\SOFTWARE\Classes\BraveSoftware.Update3WebControl.3<�BR>
IKLM\SOFTWARE\Classes\BraveSoftware.Update3WebControl.3\CLSID<�BR>
IKLM\SOFTWARE\Classes\BraveSoftwareUpdate.CoCreateAsync<�BR>
```

Figure. 3 Windows registry comparison results for brave browser



```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00583E60  00 61 00 76 00 65 4E 02  10 A9 48 88 39 04 65 00   a v eN  ©Hˆ9 e
00583E70  72 7E 00 00 ED FF 27 79  11 E0 EE 3B 00 00 00 66  r~  íÿ'y àî;   f
00583E80  88 01 75 C8 02 74 18 01  FE C3 47 01 80 3F 80 60  ˆ uÈ t  þÃG €?€`
00583E90  00 44 D4 AB C9 00 00 00  06 74 02 00 90 03 58 00   DÔ«É    t    X
00583EA0  59 02 9A 72 48 F7 52 96  E7 FD 74 00 FF 6C C1 AF  Y šrH÷R–çýt ÿlÁ¯
00583EB0  6F 9C CA F0 B4 88 96 17  72 1C FA C3 A0 C6 01 C8  oœÊð´ˆ– r úÃ Æ È
00583EC0  46 73 DF 8D C2 B4 BF 07  07 87 02 4F 00 13 40 E5  Fsß Â´¿  ‡ O  @å
00583ED0  B0 3A 0B 3D 00 48 7C 00  0C 2C 01 01 00 55 00 73  °: = H|  ,   U s
00583EE0  3F 06 B4 00 00 70 84 07  3F 14 F3 BD 00 00 00 04  ? ´  p„ ? ó½
00583EF0  20 00 00 7B 05 B9 D4 96  C9 32 03 00 90 68 74 8B     { ¹Ô–É2   ht‹
00583F00  3F 77 77 77 2E 67 6F 6F  67 6C 65 2E 63 6F 6D 2F  ?www.google.com/
00583F10  73 65 61 40 00 00 00 72  63 68 3F 71 3D 62 65 61  sea@   rch?q=bea
00583F20  63 68 26 73 61 66 65 3D  73 74 72 69 63 74 26 73  ch&safe=strict&s
00583F30  4A 3F 3D 6C 6E 6D 73 26  00 00 00 02 74 62 6D 3D  J?=lnms&    tbm=
00583F40  69 73 02 01 3D 58 26 76  65 64 3D 32 61 68 55 4B  is  =X&ved=2ahUK
00583F50  45 77 69 58 2D 36 36 53  30 35 72 71 41 00 00 00  EwiX-66S05rqA
00583F60  00 68 58 46 78 6F 55 4B  48 57 74 78 43 51 34 51   hXFxoUKHWtxCQ4Q
```

Figure. 4 WinHex memory analysis results (keyword "beach" revealed)



```
0006544272 6C 65 2D 62 61 63 6B 67 72 6F 75 6E 64 00 00 00 le-background
0006544288 01 00 00 00 14 00 00 00 00 00 00 0A 61 72 6D 61     [redacted]
0006544304 68 6C 6F 75 73 40 70 73 75 2E 65 64 75 2E 73 61 [redacted].edu.[redacted]
0006544320 03 00 00 00 11 00 00 00 94 EE DD 0E 67 62 5F 71      "îÝ gb_q
0006544336 67 20 67 62 5F 6C 63 20 67 62 5F 46 61 00 00 00 g gb_lc gb_Fa
0006544352 01 00 00 00 14 00 00 00 00 00 00 4A 61 72 6D 61            J[redacted]
0006544368 68 6C 6F 75 73 40 70 73 75 2E 65 64 75 2E 73 61 [redacted].edu.[redacted]
0006544384 03 00 00 00 11 00 00 00 6E 5A 99 0E 67 62 5F 6E        nZ™ gb_n
0006544400 67 20 67 62 5F 53 62 20 67 62 5F 46 61 00 00 00 g gb_Sb gb_Fa
0006544416 00 00 28 97 4A F7 F1 A0 E8 A0 70 2A BA 40 00 00   (—J÷ñ è p*º@
```

Figure. 5 WinHex memory analysis results (email revealed)

installation, as shown in Fig. 3.

## 4.2 Live acquisition and analysis

### 4.2.1. Memory acquisition

Where live acquisition is possible, memory analysis can reveal valuable information such as decrypted programs, usernames and passwords, chat window contents, and form field entries. For this experiment, FTK Imager was used to obtain a dump of the memory contents after completing all the Internet activities and before closing the browser. The dump files were stored in an external 1TB hard disk drive for analysis.

### 4.2.2. Memory analysis

The following forensic tools were used to search for artefacts within the memory dump:

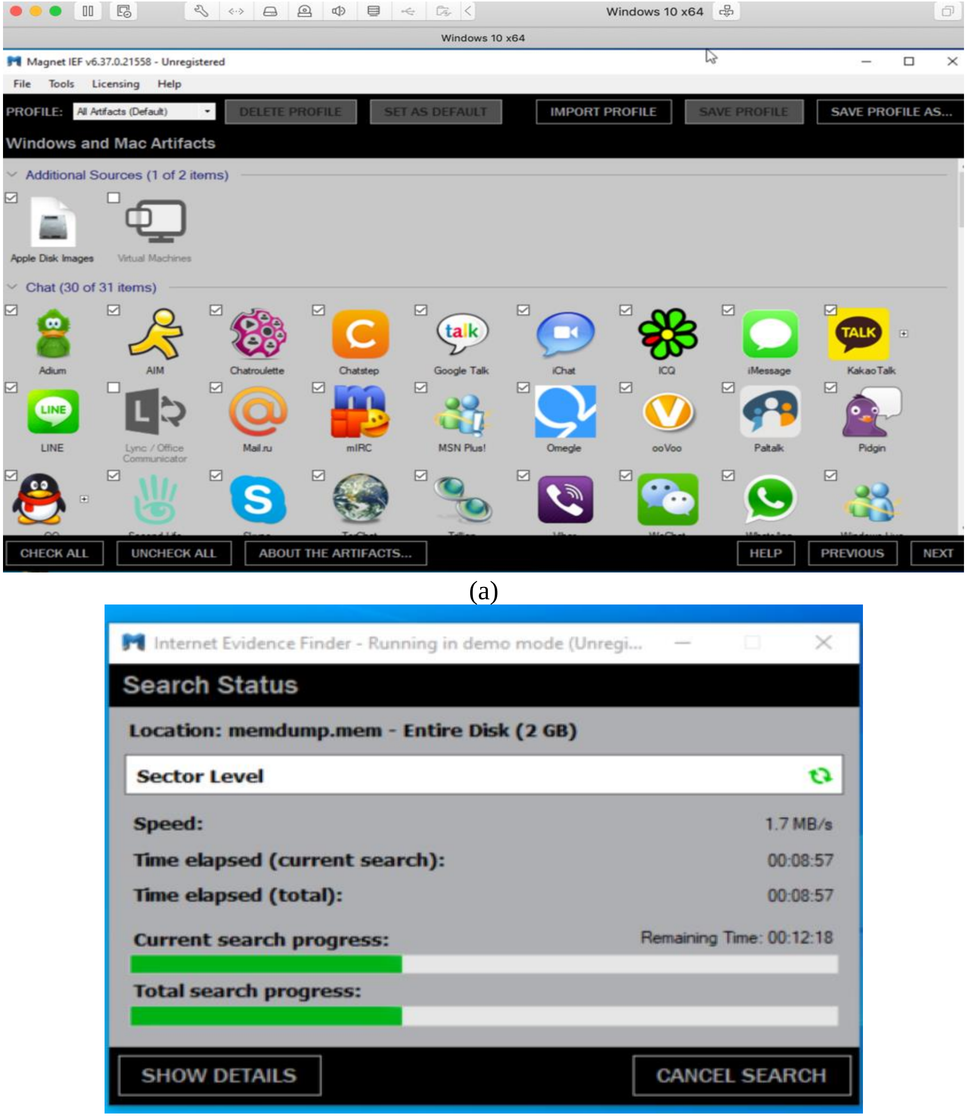
**a) WinHex:**

RAM analysis with WinHex revealed that some residual traces remain of email addresses, keyword searches, and many more, as shown in Fig. 4 and Fig. 5

**b) Internet evidence finder:**

Internet Evidence Finder (IEF) was used to search for evidence relating to the browser-specific search keywords from Table 1. IEF allows us to refine the search by choosing the type of artefacts under investigation as shown in Fig. 6 (a). Fig. 6 (b). shows IEF running the search process.

IEF's RAM analysis revealed further evidence, as shown in Fig. 7 and Fig. 8.



(a)

Internet Evidence Finder - Running in demo mode (Unregi...

Search Status

Location: memdump.mem - Entire Disk (2 GB)

Sector Level

Speed: 1.7 MB/s

Time elapsed (current search): 00:08:57

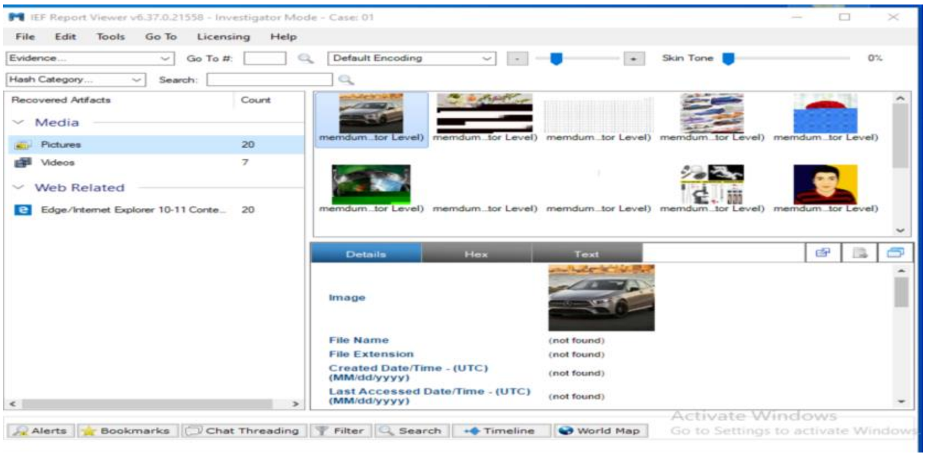
Time elapsed (total): 00:08:57

Current search progress: Remaining Time: 00:12:18

Total search progress:

(b)

Figure. 6: (a) The search category artifacts selection in IEF and (b) RAM search process in IEF

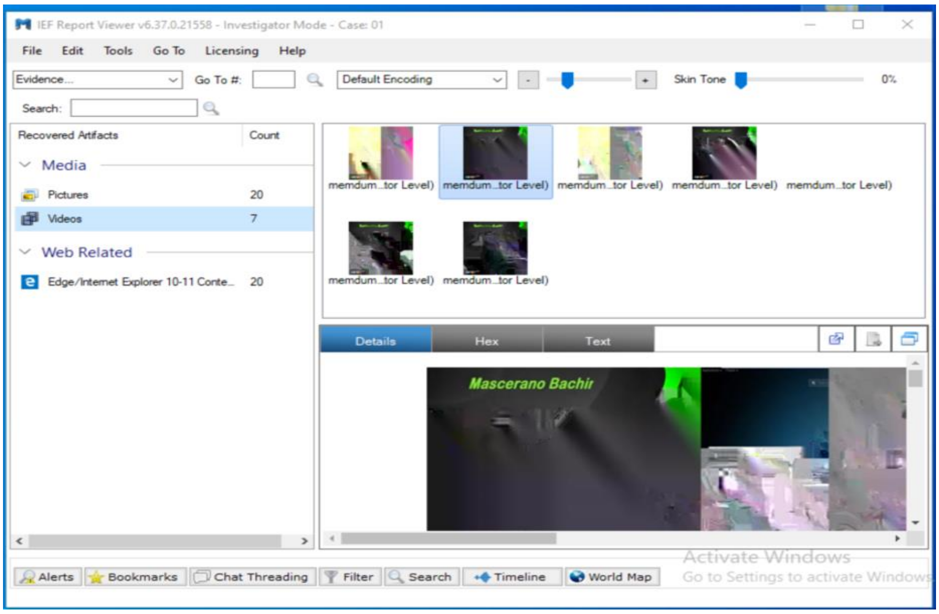

IEF Report Viewer v6.37.0.21558 - Investigator Mode - Case: 01
File Edit Tools Go To Licensing Help
Evidence... Go To #: Default Encoding Skin Tone 0%
Hash Category... Search:
Alerts Bookmarks Chat Threading Filter Search Timeline World Map
Details Hex Text
Activate Windows
Go to Settings to activate Windows

| Recovered Artifacts | Count |
|---|---|
| Media | |
| Pictures | 20 |
| Videos | 7 |
| Web Related | |
| Edge/Internet Explorer 10-11 Conte... | 20 |

memdum...tor Level) memdum...tor Level) memdum...tor Level) memdum...tor Level) memdum...tor Level)
memdum...tor Level) memdum...tor Level) memdum...tor Level) memdum...tor Level) memdum...tor Level)

| | |
|---|---|
| Image | |
| File Name | (not found) |
| File Extension | (not found) |
| Created Date/Time - (UTC) (MM/dd/yyyy) | (not found) |
| Last Accessed Date/Time - (UTC) (MM/dd/yyyy) | (not found) |

Figure.7 IEF discovery of picture of car related to the searched keyword "cars"


IEF Report Viewer v6.37.0.21558 - Investigator Mode - Case: 01
File Edit Tools Go To Licensing Help
Evidence... Go To #: Default Encoding Skin Tone 0%
Search:
Details Hex Text
Mascerano Bachir
Alerts Bookmarks Chat Threading Filter Search Timeline World Map
Activate Windows
Go to Settings to activate Windows

| Recovered Artifacts | Count |
|---|---|
| Media | |
| Pictures | 20 |
| Videos | 7 |
| Web Related | |
| Edge/Internet Explorer 10-11 Conte... | 20 |

memdum...tor Level) memdum...tor Level) memdum...tor Level) memdum...tor Level) memdum...tor Level)
memdum...tor Level) memdum...tor Level)

Figure. 8 IEF discovery of traces of the watched video related to the searched keyword "basic rat python"

### c) Autopsy software:

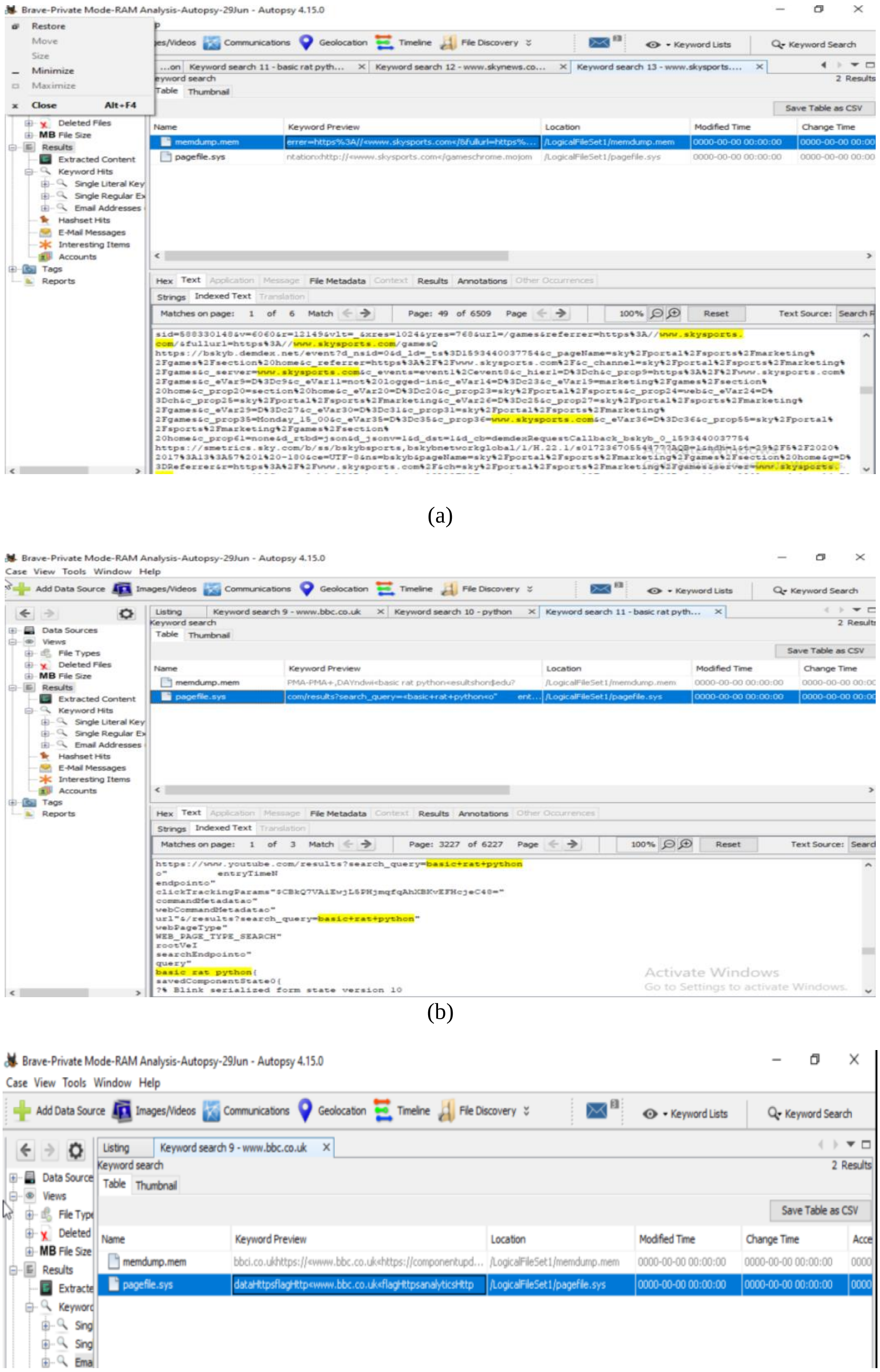
Similar results were retrieved with Autopsy. Searching for websites and some of the keywords mentioned in section 3 (www.bbc.com, www.skysports.com, "basic rat python") allowed us to extract residual artefacts left by our browser in a hidden file called "pagefile.sys", which is used by the operating system to reduce the workload on the physical memory (RAM) and allow it to perform smoothly [26]; the results are shown in Figs. 9 (a), 9 (b), and 9 (c). This highlights the importance of using multiple forensic tools, since one tool may reveal more information than another. Using multiple tools also allows for the cross-validation of detected artefacts.

### 4.2.3. Post-mortem data acquisition and analysis

Forensic investigators frequently conduct post-mortem analyses on disk images of devices that have been powered off. In many cases, this is the only option, since it is not always possible to have a forensic examiner at hand to perform a live acquisition. Moreover, a seized device may not be immediately examined due to delays in processing, or because of a shortage of forensic examiners compared to the number of devices waiting to be examined. It is thus unrealistic and impractical to keep seized devices powered on. Powering off a device also reduces the risk of the data being modified (either accidentally or deliberately) and isolates it from the network to prevent any attempts to wipe it remotely, among other benefits.

Two post-mortem experiments were conducted, one on a disk image obtained after a normal browsing session and the other after a private browsing session.

Received: July 17, 2020. Revised: August 25, 2020.



| Name | Keyword Preview | Location | Modified Time | Change Time |
|---|---|---|---|---|
| memdump.mem | errer=https%3A//«www.skysports.com«/&fullurl=https%... | /LogicalFileSet1/memdump.mem | 0000-00-00 00:00:00 | 0000-00-00 00:00 |
| pagefile.sys | ntation«http://«www.skysports.com«/gameschrome.mojom | /LogicalFileSet1/pagefile.sys | 0000-00-00 00:00:00 | 0000-00-00 00:00 |

```
sid=588330148&v=6060&r=12149&vlt=_&xres=1024&yres=768&url=/games&referrer=https%3A//www.skysports.
com/&fullurl=https%3A//www.skysports.com/gamesQ
https://bskyb.demdex.net/event?d_nsid=0&d_ld=_ts%3D1593440037754&c_pageName=sky%2Fportal%2Fsports%2Fmarketing%
2Fgames%2Fsection%20home&c_referrer=https%3A%2F%2Fwww.skysports.com%2F&c_channel=sky%2Fportal%2Fsports%2Fmarketing%
2Fgames&c_server=www.skysports.com&c_events=event1%2Cevent8&c_hier1=D%3Dch&c_prop9=https%3A%2F%2Fwww.skysports.com%
2Fgames&c_eVar9=D%3Dc9&c_eVar11=not%20logged-in&c_eVar14=D%3Dc23&c_eVar19=marketing%2Fgames%2Fsection%
20home&c_prop20=section%20home&c_eVar20=D%3Dc20&c_prop23=sky%2Fportal%2Fsports&c_prop24=web&c_eVar24=D%
3Dch&c_prop25=sky%2Fportal%2Fsports%2Fmarketing&c_eVar26=D%3Dc25&c_prop27=sky%2Fportal%2Fsports%2Fmarketing%
2Fgames&c_eVar29=D%3Dc27&c_eVar30=D%3Dc31&c_prop31=sky%2Fportal%2Fsports%2Fmarketing%
2Fgames&c_prop35=Monday_15_00&c_eVar35=D%3Dc35&c_prop36=www.skysports.com&c_eVar36=D%3Dc36&c_prop55=sky%2Fportal%
2Fsports%2Fmarketing%2Fgames%2Fsection%
20home&c_prop61=none&d_rtbd=json&d_jsonv=1&d_dst=1&d_cb=demdexRequestCallback_bskyb_0_1593440037754
https://smetrics.sky.com/b/ss/bskybsports,bskybnetworkglobal/1/H.22.1/s01723670554477?AQB=1&ndh=1&t=29%2F5%2F2020%
2017%3A13%3A57%201%20-180&ce=UTF-8&ns=bskyb&pageName=sky%2Fportal%2Fsports%2Fmarketing%2Fgames%2Fsection%20home&g=D%
3DReferrer&r=https%3A%2F%2Fwww.skysports.com%2F&ch=sky%2Fportal%2Fsports%2Fmarketing%2Fgames&server=www.skysports.
```

(a)

| Name | Keyword Preview | Location | Modified Time | Change Time |
|---|---|---|---|---|
| memdump.mem | PMA-PMA+,DAYndwi«basic rat python«esultshon$edu? | /LogicalFileSet1/memdump.mem | 0000-00-00 00:00:00 | 0000-00-00 00:00 |
| pagefile.sys | com/results?search_query=«basic+rat+python«o" ent... | /LogicalFileSet1/pagefile.sys | 0000-00-00 00:00:00 | 0000-00-00 00:00 |

```
https://www.youtube.com/results?search_query=basic+rat+python
o"          entryTimeN
endpointo"
clickTrackingParams"$CBkQ7VAiEwjL5PHjmqfqAhXBKvEFHcjeC48="
commandMetadatao"
webCommandMetadatao"
url"&/results?search_query=basic+rat+python"
webPageType"
WEB_PAGE_TYPE_SEARCH"
rootVeI
searchEndpointo"
query"
basic rat python(
savedComponentState0(
?% Blink serialized form state version 10
```

(b)

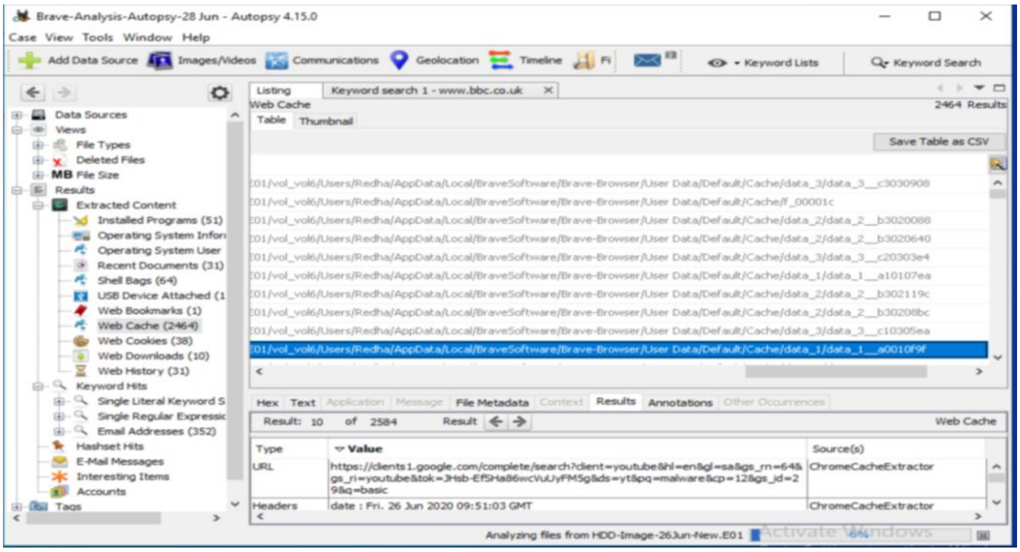
| Name | Keyword Preview | Location | Modified Time | Change Time | Acce |
|---|---|---|---|---|---|
| memdump.mem | bbci.co.uk«https://«www.bbc.co.uk«https://componentupd... | /LogicalFileSet1/memdump.mem | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000 |
| pagefile.sys | dataHttpsflagHttp«www.bbc.co.uk«flagHttpsanalyticsHttp | /LogicalFileSet1/pagefile.sys | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 0000 |

(c)

Figure. 9: (a) Autopsy keyword search result for "www.skysports.com", (b) autopsy keyword search result for "basic rat python", and (c) autopsy keyword search result for "www.bbc.co.uk"

The virtual machine was shut down after each session following the standard method, mimicking normal user behaviour. Two disk images of the virtual machine (for normal browsing mode and private browsing mode) with Expert Witness Format extension (E01) were acquired using FTK imager. The aim of the first experiment (normal browsing mode) was to identify where the browser normally

Received: July 17, 2020. Revised: August 25, 2020.



Web Cache 2464 Results

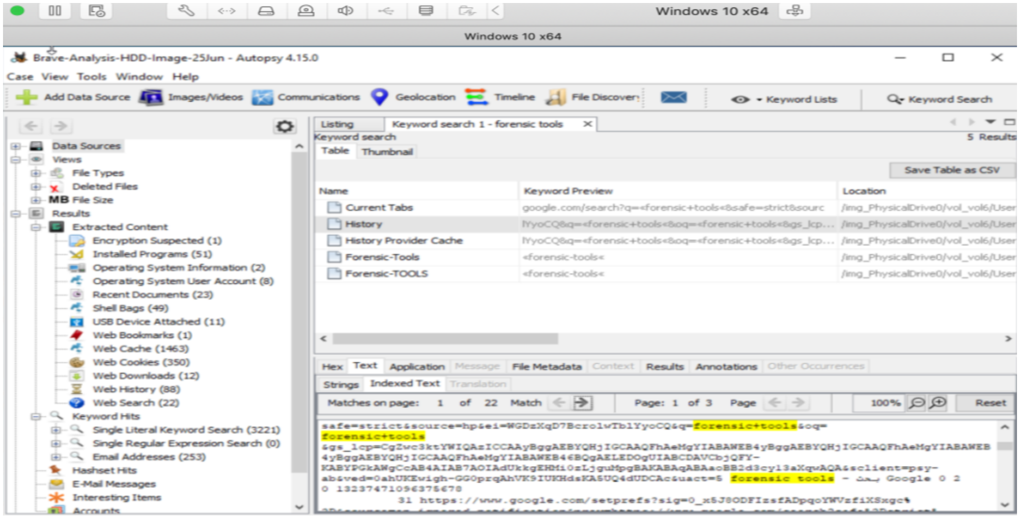
```
E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/data_3/data_3__c3030908
E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/f_00001c
E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/data_2/data_2__b3020088
E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/data_2/data_2__b3020640
E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/data_3/data_3__c20303e4
E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/data_1/data_1__a10107ea
E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/data_2/data_2__b302119c
E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/data_2/data_2__b30208bc
E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/data_3/data_3__c10305ea
E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Cache/data_1/data_1__a0010f9f
```

Result: 10 of 2584 Result — Web Cache

| Type | Value | Source(s) |
|---|---|---|
| URL | https://clients1.google.com/complete/search?client=youtube&hl=en&gl=sa&gs_rn=64&gs_ri=youtube&tok=JHsb-EfSHa86wcVuUyFM5g&ds=yt&pq=malware&cp=12&gs_id=298&q=basic | ChromeCacheExtractor |
| Headers | date : Fri. 26 Jun 2020 09:51:03 GMT | ChromeCacheExtractor |

Analyzing files from HDD-Image-26Jun-New.E01

Figure. 10 Keyword search results for “basic rat python”



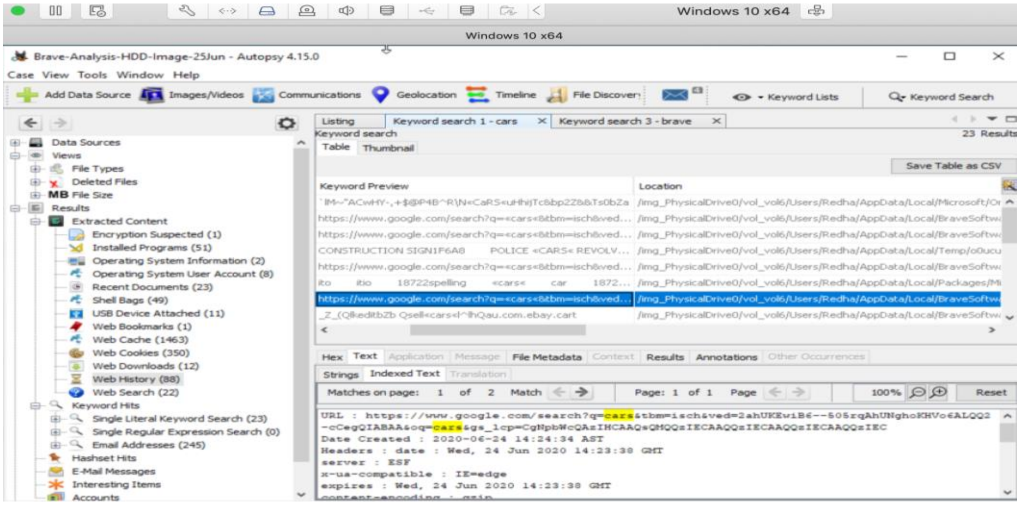
Keyword search 5 Results

| Name | Keyword Preview | Location |
|---|---|---|
| Current Tabs | google.com/search?q=«forensic+tools«&safe=strict&sourc | /img_PhysicalDrive0/vol_vol6/User |
| History | lYyoCQ&q=«forensic+tools«&oq=«forensic+tools«&gs_lcp... | /img_PhysicalDrive0/vol_vol6/User |
| History Provider Cache | lYyoCQ&q=«forensic+tools«&oq=«forensic+tools«&gs_lcp... | /img_PhysicalDrive0/vol_vol6/User |
| Forensic-Tools | «forensic-tools« | /img_PhysicalDrive0/vol_vol6/User |
| Forensic-TOOLS | «forensic-tools« | /img_PhysicalDrive0/vol_vol6/User |

Matches on page: 1 of 22 Match Page: 1 of 3 Page

```
safe=strict&source=hp&ei=WGDzXqD7BcrolwTblYyoCQ&q=forensic+tools&oq=
forensic+tools
&gs_lcp=CgZwc3ktYWIQAzICCAAyBggAEBYQHjIGCAAQFhAeMgYIABAWEB4yBggAEBYQHjIGCAAQFhAeMgYIABAWEB
4yBggAEBYQHjIGCAAQFhAeMgYIABAWEB46BQgAELEDOgUIABCDAVCbjQFY-
KABYPGkAWgCcAB4AIAB7AOIAdUkkgEHMi0zLjguMpgBAKABAqABAaoBB2d3cy13aXqwAQA&sclient=psy-
ab&ved=0ahUKEwigh-GG0prqAhVK9IUKHdsKA5UQ4dUDCAc&uact=5 forensic tools - بحث Google 0 2
0 13237471096375678
            31 https://www.google.com/setprefs?sig=0_x5J8ODFIzsfADpqoYWVzfiXSxgc%
```

Figure. 11 Keyword search results for “forensic tools”



Keyword search 23 Results

| Keyword Preview | Location |
|---|---|
| `IM~"ACwHY-,+$@P4B^R\N«CaRS«uHhiJTc&bp2Z8&Ts0bZa | /img_PhysicalDrive0/vol_vol6/Users/Redha/AppData/Local/Microsoft/Or |
| https://www.google.com/search?q=«cars«&tbm=isch&ved... | /img_PhysicalDrive0/vol_vol6/Users/Redha/AppData/Local/BraveSoftw |
| https://www.google.com/search?q=«cars«&tbm=isch&ved... | /img_PhysicalDrive0/vol_vol6/Users/Redha/AppData/Local/BraveSoftw |
| CONSTRUCTION SIGN1F6A8 POLICE «CARS« REVOLV... | /img_PhysicalDrive0/vol_vol6/Users/Redha/AppData/Local/Temp/o0ucu |
| https://www.google.com/search?q=«cars«&tbm=isch&ved... | /img_PhysicalDrive0/vol_vol6/Users/Redha/AppData/Local/BraveSoftw |
| ito itio 18722spelling «cars« car 1872... | /img_PhysicalDrive0/vol_vol6/Users/Redha/AppData/Local/Packages/Mi |
| https://www.google.com/search?q=«cars«&tbm=isch&ved... | /img_PhysicalDrive0/vol_vol6/Users/Redha/AppData/Local/BraveSoftw |
| _Z_(QlkeditbZb Qsell«cars«l^lhQau.com.ebay.cart | /img_PhysicalDrive0/vol_vol6/Users/Redha/AppData/Local/BraveSoftw |

Matches on page: 1 of 2 Match Page: 1 of 1 Page

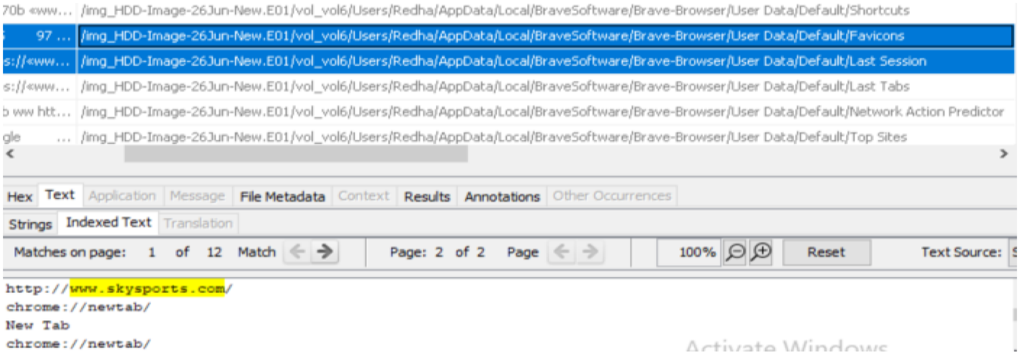
```
URL : https://www.google.com/search?q=cars&tbm=isch&ved=2ahUKEwiB6--505rqAhUNghoKHVo6ALQQ2
-cCegQIABAA&oq=cars&gs_lcp=CgNpbWcQAzIHCAAQsQMQQzIECAAQQzIECAAQQzIECAAQQzIEC
Date Created : 2020-06-24 14:24:34 AST
Headers : date : Wed, 24 Jun 2020 14:23:38 GMT
server : ESF
x-ua-compatible : IE=edge
expires : Wed, 24 Jun 2020 14:23:38 GMT
```

Figure. 12 Keyword search results for “cars”

stores its files, and the aim of the second experiment (private browsing mode) was to see what files were left behind if any.

In the first experiment, Autopsy was used to conduct a keyword search for the URLs visited. The result contained many hits, and it was evident that the

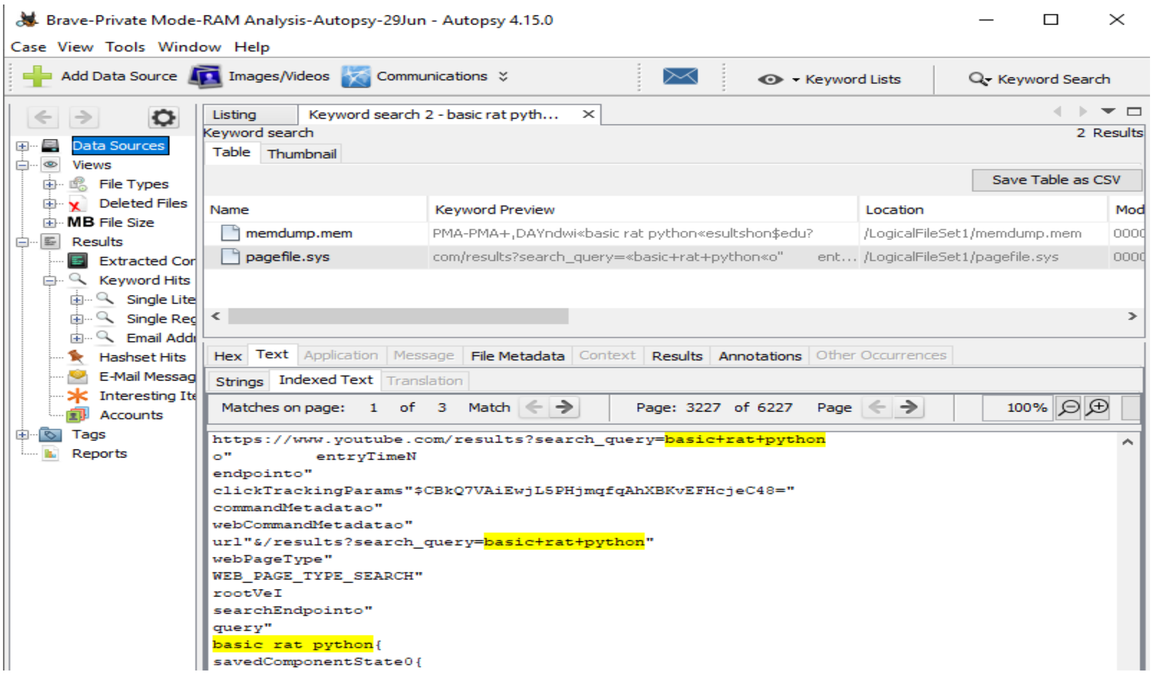
Received: July 17, 2020. Revised: August 25, 2020.



```
70b «ww…  /img_HDD-Image-26Jun-New.E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Shortcuts
   97 …  /img_HDD-Image-26Jun-New.E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Favicons
s://«ww…  /img_HDD-Image-26Jun-New.E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Last Session
s://«ww…  /img_HDD-Image-26Jun-New.E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Last Tabs
b ww htt…  /img_HDD-Image-26Jun-New.E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Network Action Predictor
gle     …  /img_HDD-Image-26Jun-New.E01/vol_vol6/Users/Redha/AppData/Local/BraveSoftware/Brave-Browser/User Data/Default/Top Sites
```

```
http://www.skysports.com/
chrome://newtab/
New Tab
chrome://newtab/
```

Figure. 13 Keyword search results for “www.skysports.com”



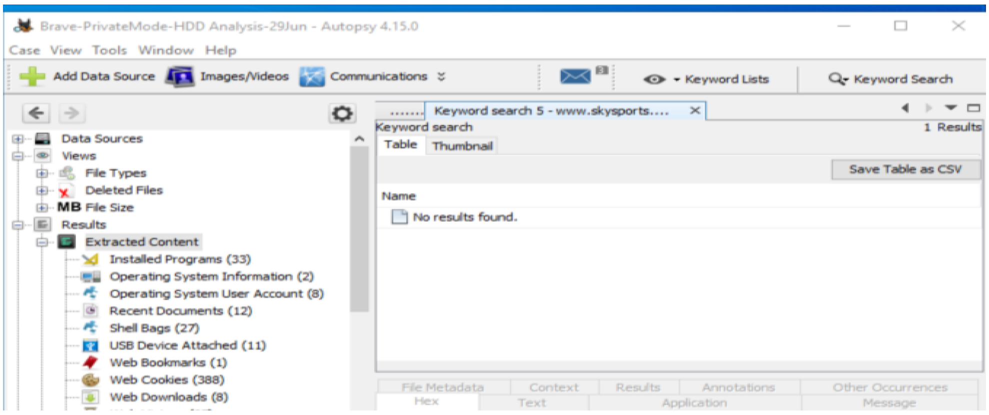
| Name | Keyword Preview | Location | Mod |
|---|---|---|---|
| memdump.mem | PMA-PMA+,DAYndwi«basic rat python«esultshon$edu? | /LogicalFileSet1/memdump.mem | 000( |
| pagefile.sys | com/results?search_query=«basic+rat+python«o" ent… | /LogicalFileSet1/pagefile.sys | 000( |

```
https://www.youtube.com/results?search_query=basic+rat+python
o"        entryTimeN
endpointo"
clickTrackingParams"$CBkQ7VAiEwjL5PHjmqfqAhXBKvEFHcjeC48="
commandMetadatao"
webCommandMetadatao"
url"&/results?search_query=basic+rat+python"
webPageType"
WEB_PAGE_TYPE_SEARCH"
rootVeI
searchEndpointo"
query"
basic rat python{
savedComponentState0{
```

Figure. 14 Keyword search results for “basic rat python”

browser stores browsing history in the “/users/username/AppData/BraveSoftware/Brave-Browser/User Data/Default/Cache” folder as shown in Figs. 10-14.

In the second experiment the same keyword search was conducted on the image obtained after the private browsing session. No results were found, as shown in Figs. 15-17.



| Name |
|---|
| No results found. |

Figure. 15 Keyword search results for www.skysports.com

Received: July 17, 2020. Revised: August 25, 2020.

Table 2. Task related artefacts found on RAM and hard disk

| Task | Hits | | Artefacts found | Tools used |
|---|---|---|---|---|
| | RAM | Hard Disk | | |
| Watch a YouTube video | ✓ | ✗ | video, URLs | IEF |
| Google search: “beach”, “cars”, “malware” , “forensic tools” | ✓ | ✗ | images, keywords, URLs, | WinHex, Autopsy |
| Visit www.skysports.co.uk | ✓ | ✗ | URLs | Autopsy |
| Visit www.gmail.com and sign in | ✓ | ✗ | emails | WinHex |
| Search for “macbook” in www.amazon.co.uk | ✓ | ✗ | URLs, images | Autopsy |
| Visit www.bbc.co.uk | ✓ | ✗ | keywords, URLs | Autopsy |

## 5 Results and analysis

Table 2 summarizes the results of our experiments obtained through a set of tasks done using Brave’s private mode. As it can be seen, a live memory analysis of the RAM can be really rewarding as different types of artefacts, including URLs, emails, images, and even videos, could be recovered. On the contrary, a post-mortem analysis would lead to a dead end for forensic investigators as Brave manages to clear all data and information related to its private browsing sessions from the hard disk.

## 6 Discussion

In this paper we found that after installing Brave browser on Windows 10, a number of files are created in “/users/username/AppData/BraveSoftware/Brave-Browser/User Data/Default/ Privacy Browser directory. Brave browser also creates a default folder which contains temporary files and folders used when the browser is launched and is deleted on closure.

However, this is not enough to hide all traces of browser activities. Some information related to the browser’s activities is left behind on the RAM, and they can be retrieved when doing memory acquisition and analysis using some standard tools. Those artefacts are left in both the memory dump and “pagefile.sys” file, which are both great places for forensic investigators to search for evidence. Many artefacts have been recovered in our experiments such as typed URLs, pictures and keyword searches. These artefacts are similar to the artefacts left using Browzar [12] and Epic [13], which are both privacy-enhanced browsers. The files and folders created temporarily by these browsers got deleted at the end of each browsing session, but the data was still readily available and retrievable using digital forensic tools. Incognito, Chrome’s private mode, as well the Comodo Dragon browser also produced similar results in [11], and their artefacts were found in locations nearly identical to the location of Brave’s artefacts. The most probable reason for the similarity of results between the five browsers, Epic, Browzar, Commodo Dragon, Chrome, and Brave, is that they are all built on the open-source Chromium browser platform, and this explains why they all store data in similar places and in a similar way even though their functionality differs. This might show that there is a weakness in the structure of Chromium-based browsers and there is a need for improvement in the amount and content of data related to browsing sessions stored in the RAM by these browsers in their normal and private modes. Despite the similarities, Brave is the only browser whose private mode managed to leave no traces on the Hard Disk. The post-mortem analysis we conducted proved this and could be deemed accurate as two experiments were carried out; the first was using the normal browsing mode to locate the files and folders Brave normally stores its browsing session data in, and the second was using Brave’s private mode and then searching the previously identified files and folders as well as scanning the whole memory using the most commonly used and standard digital forensic tools in a search for any leftover browsing session data. The acquisition and analysis of the drive image have shown no traces of the user’s browsing activities, and no hits were made in the second experiment.

Indeed, seizing a suspect’s running computer, with Brave browser open or minimized will be a great source of artefacts if a live memory dump is done before shutting down the system or closing the browsing session as demonstrated in our experiments, but unfortunately, that is not always the case.

## 7 Conclusion and future work

Brave browser claims to provide protection to user’s privacy when online and guarantees to clear all traces of browsing history on closure. In this paper, we presented the forensic acquisition and analysis of Brave browser and looked into how its private mode preserves and protects the user's privacy to test the extent of truth for these claims. The series of experiments we performed have shown that some artefacts related to browser activities are still available on the RAM even after ending a browsing session and can be retrieved by forensic investigators using the right tools, but none remain on the hard disk. The approach taken in identifying the files and folders before performing the search has left a minimal margin for error in our results. The artefacts retrieved from the RAM were more than what would have been found if a standard plain English keyword search approach was used, and despite the focused search, there were still no hits on the Hard Disk. This new method would be recommended in future researches in this area as it is more accurate and would also help locate the storage locations of other poorly documented or newly created browsers.

Our study concluded that Brave browser does deliver on local privacy with turning off the machine after a private browsing session being the only caveat. The storage locations for browsing session data in both normal and private browsing modes were identified, and the type and content of leftover artefacts were outlined. These results are useful to forensic investigators seeking to recover web browser's activities of suspected users and could act as a basis for future research done on Brave and other browsers alike. The observations and the proposed approach could also be instrumental for future computer forensic investigations and to developers seeking improvement to the degree of privacy offered by their browsers.

Despite the thorough examination conducted, some research windows relating to the privacy provided by Brave Browser remain open for further investigation. For instance, running these experiments using physical devices rather than virtual machines would give more insight into the behaviour of Brave browser on a real testbed. Another area of interest would be studying and comparing Brave Browser with TOR browser, the number one Dark web browser [27], in an attempt to ascertain which of the two provides their users with better online and local privacy.

## Conflicts of Interest

The authors declare no conflict of interest.

## Author Contributions

Both authors, A. Mahlous and H. Mahlous contributed to the conceptualization, methodology, validation, data curation and writing—review.

Formal analysis, investigation, resources, writing—original draft preparation, supervision, and project administration were handled by A. Mahlous.

H. Mahlous took care of editing and visualization.

## References

[1] https://us.norton.com/internetsecurity-privacy-what-is-private browsing.html

[2] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018

[3] K. Satvat, M. Forshaw, F. Hao, ansd E. Toreini, "On the privacy of private browsing – a forensic approach", *Data Privacy Management and Autonomous Spontaneous Security*, Springer, Berlin, Heidelberg, 2014.

[4] R. Montasari and P. Peltola, "Computer Forensic Analysis of Private Browsing Modes", *In: Jahankhani H., Carlile A., Akhgar B., Taal A., Hessami A., Hosseinian-Far A. (eds) Global Security, Safety and Sustainability: Tomorrow's Challenges of Cyber Security. ICGS3 2015. Communications in Computer and Information Science*, Vol. 534. Springer, Cham. https://doi.org/10.1007/978-3-319-23276-8_9, 2015.

[5] R. Md. Saidi, F. F. Saleh Udin, A. F. Zolkeplay, M. A. Arshad, F. Sappar "Analysis of Private Browsing Activities", In: *Proc. of Yacob N., Mohd Noor N., Mohd Yunus N., Lob Yussof R., Zakaria S. (eds) Regional Conf. on Science, Technology and Social Sciences* (RCSTSS 2016). Springer, Singapore, 2019.

[6] J. Oh, S. Lee, and S. Lee, "Advanced evidence collection and analysis of web browser activity", *Digital Investigation*, S62 - S70, 2011.

[7] D. N. Patil, B. B. Meshram "Web Browser Analysis for Detecting User Activities", *In: Sa P., Bakshi S., Hatzilygeroudis I., Sahoo M. (eds) Recent Findings in Intelligent Computing Techniques. Advances in Intelligent Systems and Computing*, Vol. 707. Springer, Singapore. 2019.

[8] D. J. Ohana and N. Shashidhar, "Do Private and Portable Web Browsers Leave Incriminating Evidence? A Forensic Analysis of Residual Artifacts from Private and Portable Web Browsing Sessions", In: *Proc. of IEEE Security and Privacy Workshops*, San Francisco, CA, pp. 135-142, 2013, doi: 10.1109/SPW.2013.18, 2013

[9] N. A. Hassan "Web Browser and E-mail Forensics", *In: Digital Forensics Basics. Apress, Berkeley,* CA, 2019.

[10] G. Horsman, B. Findlay, J. Edwick, A. Asquith, K. Swannell, D. Fisher, A. Grieves, J. Guthrie, D. Stobbs, and P. McKain, "A forensic examination of web browser privacy-modes", *In: Forensic Science International: Report,* 2019.

[11] A. Nalawade, S. Bharne, and V. Mane, "Forensic analysis and evidence collection for web browser activity", In: *Proc. of International Conf. on Automatic Control and Dynamic Optimization Techniques* (ICACDOT), Pune, pp. 518-522, 2016, doi: 10.1109/ICACDOT.2016.7877639.

[12] H. Chivers, "Private browsing: a window of forensic opportunity", *Digit. Investig*. Vol. 11, No. 1, 2014.

[13] R. M. Gabet, K. C. Seigfried-Spellar, M. K. Rogers, "A comparative forensic analysis of privacy enhanced web browsers and private browsing modes of common web browsers", *Int. J. Electron. Secur. Digit. Forensics,* Vol. 10, No. 4, 356–371, 2018.

[14] C. Warren, E. El-Sheikh, NA. Le-Khac, "Privacy Preserving Internet Browsers: Forensic Analysis of Browzar", *In: Daimi K. (eds) Computer and Network Security Essentials*, Springer, Cham, 2018.

[15] A. Reed, M. Scanlon, N. A. Le-Khac, "Private Web Browser Forensics: A Case Study of the Epic Privacy Browser", 2018.

[16] https://www.forbes.com/sites/billybambrough/2020/04/09/billions-of-google-chrome-users-now-have-another-surprising-option

[17] https://netmarketshare.com/operating-system-market-share

[18] https://psu-sa.onthehub.com/WebStore/Welcome.aspx

[19] https://static1.squarespace.com/static/53cff120e4b095a8ca26053d/t/53ff7b93e4b0e1f6ca3c99bd/1409252243947/nist-sp-800-88-rev1.pdf

[20] https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager

[21] [https://www.autopsy.com

[22] [https://sourceforge.net/projects/regshot/

[23] https://www.magnetforensics.com/news/magnet-forensics-releases-internet-evidence-finder-v6-4/

[24] https://www.x-ways.net/winhex/

[25] https://www.similarweb.com/top-websites/united-kingdom/

[26] https://www.tomshardware.com/news/how-to-manage-virtual-memory-pagefile-windows-10,36929.html

[27] https://drfone.wondershare.com/dark-web/dark-web-browser.html