computers

MDPI

Article

Browsers' Private Mode: Is It What We Were Promised?

Kris Hughes, Pavlos Papadopoulos *, Nikolaos Pitropakis *, Adrian Smales, Jawad Ahmad and William J. Buchanan

Blockpass ID Lab, School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, UK; 40412482@live.napier.ac.uk (K.H.); a.smales@napier.ac.uk (A.S.); j.ahmad@napier.ac.uk (J.A.); b.buchanan@napier.ac.uk (W.J.B.)

* Correspondence: pavlos.papadopoulos@napier.ac.uk (P.P.); n.pitropakis@napier.ac.uk (N.P.)

Abstract: Web browsers are one of the most used applications on every computational device in our days. Hence, they play a pivotal role in any forensic investigation and help determine if nefarious or suspicious activity has occurred on that device. Our study investigates the usage of private mode and browsing artefacts within four prevalent web browsers and is focused on analyzing both hard disk and random access memory. Forensic analysis on the target device showed that using private mode matched each of the web browser vendors' claims, such as that browsing activity, search history, cookies and temporary files that are not saved in the device's hard disks. However, in volatile memory analysis, a majority of artefacts within the test cases were retrieved. Hence, a malicious actor performing a similar approach could potentially retrieve sensitive information left behind on the device without the user's consent.

Keywords: digital forensic investigation; web browsers; private mode; artefacts

Citation: Hughes, K.; Papadopoulos, P.; Pitropakis, N.; Smales, A.; Ahmad, J.; Buchanan, W.J. Browsers' Private Mode: Is It What We Were Promised? *Computers* **2021**, *10*, 165. https://doi.org/10.3390/computers10120165

Academic Editor: Wenbing Zhao

Received: 15 October 2021
Accepted: 26 November 2021
Published: 2 December 2021

1. Introduction

As technology becomes more embedded within our society, there has been an exponential increase in the number of web transactions that take place online on a daily basis. This coverage can include activities that are carried out in the home, work or industry verticals such as education. It is increasingly apparent that people are becoming more reliant on having access to the internet and applications and that they have become dependent, if not complacent, on expectations. Önday et al. [1] described that the computer has had an impact that it has changed the way individuals live, work and play. They also portray internet browsers as being pivotal in the success of electronic business and electronic trade.

Most everyday scenarios involve using an internet browser, such as Google Chrome. This specialist application facilitates communication between the user's device and the remote web server in which the web page's content resides and is then transmitted back to be rendered on the end user's browser. Since the inception of the World Wide Web in 1991 by Tim Berners Lee, the uptake in accessing the internet and user adoption has been significant. Research by [2] focused on the topic of private browsing, specifically on the Brave browser. Their area of research is around browser privacy and the increased number of users who expect privacy whilst browsing online. Private mode browsing first appeared within the Safari web browser in 2005 [3]. Since then, the majority of web browsers have integrated this functionality and have made it available to all who choose to take advantage of it.

Whilst access to the internet provides a wealth of information and allows the freedom and opportunity to learn and conduct legitimate business, there is also the side where individuals can misuse it. Digital forensics forms part of the overall banner of forensic science and involves a technical specialist with the necessary skillset to conduct forensics on a computer device or similar. The authors of [4] describe forensic science as being an investigatory tool that allows for the analysis of evidence by applying expert scientific knowledge and methodology to criminal investigations.

Digital forensics can be extremely challenging in the modern computing environment. One such example would be the increasing uptake and advancement of encryption technology, such as Bitlocker. Using whole disk encryption can help an individuals keep the data they store on their hard drive private, but at the same time it can also render a digital forensics investigators' life challenging. Moreover, whilst there are many tools available for assisting a security professional with their investigation, there is also an increasing amount of anti-forensic tools appearing online by the hacking community that help a malicious actor cover their tracks. As with most of the job roles in the security profession, it appears to be a game of cat and mouse between the legitimate user and the bad actor. Within forensic science, there is a well-known principle called the Locard's exchange principle, "it is impossible for the criminal to act, especially considering the intensity of a crime, without leaving traces of his presence", as discussed in [5].

Even if web browsers are a key component of the internet, their privacy is often neglected. Additionally, there are situations where adversaries try to exploit the private mode of the web browsers to cover their tracks. Some studies investigated the security of their transmitted information [6], and there are studies that focused on the private mode of particular web browsers [7] or investigated a web browser vendor's claims [8]. As observed in Section 2.2, four prevalent web browsers were chosen for this investigation and analysis. These browsers are derived to the following: Google Chrome with the Incognito mode, Microsoft Edge with the InPrivate mode, Mozilla Firefox with the Private Browsing mode and Brave with the Private Window mode.

The main contributions of this paper can be observed in Figure 1, and are summarized as follows:

- We thoroughly and forensically investigate the private mode functionality provided by four of the most prevalent web browsers, namely Google Chrome, Microsoft Edge, Mozilla Firefox and Brave.
- We critically compare our findings across four different web browsers.
- We evaluate the performance of the web browsers' private browsing against the promised claims of the relevant vendors.

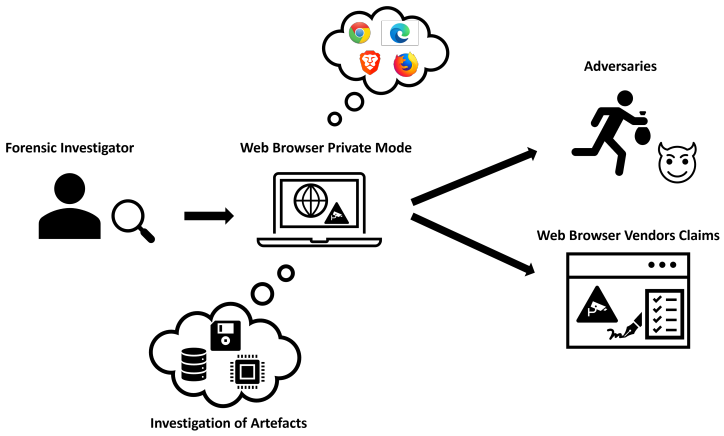

Figure 1. Investigation approach overview. The utilised forensic toolkit involves the FTK imager, Autopsy, Bulk Extractor and Strings Volatility. Our investigation approach aims to identify artefacts left behind from private mode web browsing using Google Chrome, Mozilla Firefox, Microsoft Edge and Brave web browsers in order to identify malicious behaviour and verify the web browser vendor's claims.

The remaining hierarchy of this paper is organised into the following sections: The *Literature Review and Background Knowledge* section provides a review of the related literature as well as background information related to web browser forensics and private web browsing. The *Methodology and Architecture* section discusses and outlines the approach taken to analyze each web browser to identify associated artefacts left behind from a

terminated web session and the tools and methods used to investigate the functionality of each browser while comparing the results. The *Analysis and Results* section is focused on the conducted experimental analysis, which presents and discusses the results that were obtained from our tests along with their respective key findings. The *Discussion* section briefly explains and reviews our investigation goals in order identify if the findings of our work are conclusive and if they warrant further research and investigation into this particular topic of browser forensics. Finally, the *Conclusions* section summarizes our findings regarding the private browsing mode while providing some pointers for future work within this particular area of research.

2. Literature Review and Background Knowledge

2.1. Data Privacy

The topic of data privacy has received significant attention in recent years and has been enforced in various geographies by regulations and acts such as the General Data Protection Regulation (GDPR) [9] and the California Consumer Privacy Act (CCPA) [10]. Data privacy in the context of this paper is concerned with personal information that may be sensitive, financial documents, or other confidential material. These data should be handled with the utmost importance as "GDPR defines personal data as anything that can be used to identify an individual person. This includes personally identifiable details such as names, email addresses, social security number, IP addresses, telephone numbers, location data, birth dates, as well as other information related to genetic, economic, cultural or social identity" [11,12]. The aspect of privacy has been extensively investigated in both centralized and decentralized systems [12]. Especially in decentralized infrastructures, mutual trust is required between the participating entities [13]. Hence, by providing a method for users to take more control over their web browsing activity, the private mode can potentially help reduce the amount of personal and sensitive information saved onto a user's device. Alternative uses, as explained by [14], suggest that cybercriminals can leverage this privacy feature in hope it will reduce or even eliminate traces to their criminal/nefarious behaviour.

Many forensic investigations demonstrated that little attention was given to privacy information based on user behaviours [15]. This could suggest a potential risk for many companies who do not have a security system deployed in their environment capable of detecting such activities. If solely relying only on traditional security mechanisms, it could mean businesses are unaware of nefarious user activities. Whilst clearing a web browser's cache does not necessarily mean anything untoward, it can potentially be a cause for concern, especially in a workplace environment where company policies dictate that non-work-related internet browsing is forbidden during company hours. In [16], the topic of spyware and the possibility of having it as a legitimate use case by a parent or employer is discussed. This would involve installing recording software such as a keylogger, which would record and monitor a user's internet activity along with any other activity carried out on their device. The possibility of individuals intending to cover their tracks by using an anti-forensic tool such as CCleaner is discussed in [17] in which the authors describe CCleaner as a tool that aims to remove residual artefacts left behind after a browser session, such as web browsing history.

2.2. Web Browsers and Private Browsing Mode

The first web browser was introduced in 1991 by Tim Berners Lee. This application facilitates the retrieval of web page content from a web server that a remote provider hosts. The protocols used for this are Hyper Text Markup Language (HTTP) and HTTP Secure (HTTPS). Web browsers are one of the most used applications in existence, running on diverse types of hardware from mobile phones to desktop computers [18], and are constantly evolving.

Private browsing, as described by [19], is incorporated into most modern browsers and aims to promote privacy alongside related security-focused functionality. It can facilitate

a web session that infers a state of anonymity that does not retain information about the users' browsing activities. Examples of what is provided by leveraging this feature in a private browser session are that it does not record web search history, it disables data caching across web sessions, and purges cookies upon session termination. Private browsing comes at no financial cost to the end-user and, instead, can instill a sense of confidence that whilst using this feature, the user's privacy is ensured and protected from prying eyes. However, one may misread this into thinking that they will have complete anonymity, leaving no traces of browsing activity behind on their device whilst surfing the internet or even after the web session has ended. Users have misconceptions and a lack of understanding in how the private browsing feature functions [20,21], and they are also likely to overestimate the protections private browsers allude to provide, such as blocking ads and online tracking, and potentially putting themselves at risk and engaging in risky online behaviour or similar.

This area is discussed by [22] who mentions that private browsing mode can protect one from potentially sensitive and confidential information, such as health, sexual and related sensitive topics saved to their device. This is one of the reasons private browsing is becoming ever more popular amongst all age groups. As with most things that enable legitimate usage and protection from malicious elements, there is also the side where bad actors aim to misuse it. Within a company workplace, it is possible for private mode browsing to be disabled through Microsoft Group policy for browsers such as Internet Explorer and Microsoft Edge. Deploying a security control such as this may seem unnecessary and maybe even somewhat draconian. However, from an Information Technology (IT) security point of view, it can help prevent an insider threat from carrying out malicious activities or trying to cover their browser habits if they were conducting non-work-related activity online. IT security policies are the foundation of a good security culture within a workplace. A good and robust security culture should be spearheaded by the organization from the top down and is augmented by corporate policies and procedures [23].

Furthermore, private browsing can also be proved troublesome for digital forensic investigation of an alleged crime on a computing device. This particular area of concern is discussed in the research by [24] and describes the challenges that law enforcement face with investigations of the internet search history of a suspect only to be left with a gap in time as the user had taken advantage of the private browsing mode and even displaying no records of history at all.

Private Browsers Overview and Scope

Google Chrome Incognito: Google chrome browser was first released in 2008 and developed by Google. The source code used for this browser is part of Chromium, a free and open-source project by Google. According to the statistics provided by stat counter, Chrome has a global market share of 64.47 percent in April 2021. Incognito mode was made available in December 2008. As explained by [25], this allows users to browse the internet without worrying about any of their browsing activity being stored on their computers.

Microsoft Edge InPrivate: Microsoft Edge, also known as "Project Spartan", [26], is a cross-platform web browser developed and released by Microsoft in 2015. The InPrivate feature was designed to help protect a user's privacy by not recording web browsing activities such as web searching history and cookies. In the work of [27], the authors mention that browser artefacts were not completely private when using the InPrivate feature, as remnants of a browser session were still visible in Random Access Memory (RAM).

Mozilla Firefox Private Browsing: Mozilla Firefox is a popular web browser and well-respected in the security field. This privacy-focused browser aims to provide an intuitive and aesthetically pleasing user interface. In the research by [25], Firefox is used as one of the main components of the TOR browser. The private browsing feature within Firefox first became available in 2009 and purports to be one of the best browsers in helping to protect

a user's privacy as well as preventing websites and ads from harvesting web browsing information [28].

Brave Private Window: Brave browser is one of the latest additions to the web browser market, with its first stable release in November 2019. This browser purports to be privacy-focused and claims to have greater privacy by default than alternative browsers, such as Mozilla Firefox. It also has an interesting feature by rewarding the user with cryptocurrency and the Basic Attention Token (BAT), for agreeing to receive targeted adverts as part of the browser's session. This cryptocurrency is designed with privacy at its core along with the aim of reducing the amount of advertising online users are presented with [29]. In the study of [6], the authors found that Brave was the best privacy-focused browser. Brave is similar in its description for the functionality of their private browsing function and purports to prevent cookies, site data, form information and browsing history from residing on the device once the web session has been terminated.

2.3. Digital Forensics and Web Browser Forensics

Digital forensics, as described by [30], is a vast subject that involves input from individuals in various professions. The main areas concerned cover network, database, mobile, cloud, memory, and disk forensics. Digital forensics can be observed as a branch of forensic science, with similarities including identifying, searching, seizure, preserving and investigating digital data in crime scenarios. Digital forensics is characterised as the product of the intersection of the practices of law and computer science [31]. Activity conducted online using a web browser, or similar will leave forensic artefacts and potentially include sensitive information that the user will not be aware of.

Web browser forensics can be one of the most crucial phases deployed as part of a cyber-crime investigation, whether for an investigation in the workplace or part of a criminal investigation. The majority of web browsers available today include the private browsing feature that first appeared in 2005 within the Safari web browser [3]. Private browsing and allows an individual to keep most of their browsing session secret, providing the user with greater control over their privacy, but many can be misled into believing that all browsing activity is completely anonymous [32].

It is worth noting that this private browsing feature does not prevent an individual from downloading malware onto their device nor protects them from visiting a web page serving malicious code. Whilst most use cases are legitimate for using private browsing, an adversary with malicious intent can take advantage of this feature, primarily for covering their tracks and remaining anonymous. A risk of using the standard browsing mode is that if a local attack was successful on a device, then the attacker could potentially gain access to browsing data and other related session artefacts residing in that local machine [33]. Hence, a compromise of this kind could reveal many sensitive and financial information items, such as passwords, credit card numbers and health information. As there is no monetary cost to installing or using a web browser, one has to ask what the actual price of using such a tool is? Since "If something is free, you're not the customer; you're the product" [34].

2.4. Related Work

Experiments such as the one carried out by [7] concentrate on examining the protection capability proposed by private mode functionality in popular web browsers, such as Google Chrome, Mozilla Firefox, Internet Explorer and Opera. Their work comprises using a virtual filesystem as a countermeasure to eradicate the chance of leaving behind remnants of browsing artefacts once the web session has been terminated. Their analysis environment consisted of using virtualisation as their platform, which hosted a Windows 7 guest operating system (OS). Their work aimed to prove that private browsing fails to protect the privacy of the web session and that artefacts can still be retrieved. A piece of software called RAMDisk was used as a countermeasure to protect browsing session activity from being recovered.

In the work of [8], the authors investigated the claims made by web browser companies about the protection that private browsing provides to end users and verifying if residual data remain behind, which contains private data. The researchers used VirtualBox as their virtualisation platform to perform their experimental tests capable of creating snapshots of the machine's clean state. Additionally, the utilization of virtualised platforms such as VirtualBox provides surpassing flexibility and reduces the need to have multiple physical machines to conduct their testing for all the different web browsers. The primary tool they used to search for remnants of browser artefacts left behind was MiniTool Power Data Recovery v6.8. Similarly, in the work of [35], the authors utilized their platform for testing Google Chrome, Mozilla Firefox and Internet Explorer 11. The authors utilized VirtualBox in a Windows 10 host OS and performed a forensic investigation to search for artefacts on the hard disk and live RAM bt using tools such as MagnetRAMCapture. This tool allows an investigator to take a snapshot of live RAM, which can then be analyzed by using another tool, such as WinHex.

A work that focused on volatile memory forensics is [36], which states that files such as *Hiberfil.sys* and *PageFile.sys* are considered to be sources that can potentially contain artefacts such as private browsing history. The authors mention that the activity will still reside in volatile memory by using private mode web browsing, such as IP address, Proxy List, Network commands and Tor-related activities. Ref. [37] describes memory forensics as being a critical method in digital forensic investigations. Valuable information such as files, processes, registry keys, passwords, encryption keys and network data can be retrieved for volatile memory, all of which can provide vital information to a forensic investigator. Their research method also used virtualisation software VirtualBox as their testing platform, enabling them to capture bit by bit copies of the virtual machine easily. Ref. [38] describes a tool written in Python called Volatility as an open-source command-line tool that is developed specifically for memory analysis that is free, extremely versatile and flexible. A GUI version of Volatility called Volatility Workbench also carries out most of the same tasks as the command-line tool. Research carried out by [39] concentrated their focus on the forensic analysis of the Tor browser but used Volatility as one of the main tools to search for interesting artefacts in RAM. They also used virtualisation as their primary platform, VMware Workstation 12 Pro. Virtual machine Memory images from Windows 8.1 guest OS (.vmem files) were analyzed for browsing artefacts.

The research carried out by [2] investigates artefacts left behind by using Brave browser. Their approach involved using VMware as their virtualised environment and a Windows 10 OS as the guest virtual machine. Their methodology involved taking a snapshot of the machine's memory before installing the browser and one immediately after installation. This enabled the researchers to pinpoint the files and folders created by the Brave browser. Furthermore, the authors took snapshots of memory for both normal and private mode browsing and compared the two. This allowed them to identify the behaviours associated with the two different browser modes and observe any differences in the types of files stored, amount of data, data content, and whether private mode deletes the artefacts associated with browsing activity that would typically be left behind if using normal mode or if files are not stored in the first place. Memory analysis of RAM was also used to augment their research.

As observed in Table 1, our study aims to ascertain residual artefacts left behind from private web browsing session and compare the results to that of an ordinary browsing session across the browsers within our scope. There has been increased research covering the main web browsers in this area over the last number of years but not extensively focusing on comparing these with the most recent Brave browser. Additionally, most works in the literature included conventional forensic methodology and tools, but little attention is given to live forensics using Volatility for investigating RAM. Our work intends to evaluate and compare the strengths and weaknesses of using such approaches in combination with traditional forensic investigation. Additionally, our work aims to form the basis of further research regarding forensic investigations in mobile devices.

Table 1. Investigation comparison of our work against other related works.

Web Browsers and Artefacts	Our Work	[7]	[8]	[36]	[35]	[37]	[38]	[2]
Brave	✓	✗	✗	✗	✗	✗	✗	✓
Google Chrome	✓	✓	✓	✗	✓	✗	✗	✗
Mozilla Firefox	✓	✓	✓	✗	✓	✗	✓	✗
Microsoft Edge	✓	✗	✓	✗	✗	✗	✗	✗
Bookmarks	✓	✓	✗	✗	✓	✗	✓	✓
Browser History	✓	✓	✓	✓	✓	✗	✓	✓
Cookies	✓	✓	✓	✓	✓	✗	✗	✓
Downloads	✓	✓	✗	✓	✓	✗	✗	✓
Passwords	✓	✓	✓	✓	✓	✓	✓	✓
Web Search Queries	✓	✓	✓	✓	✓	✗	✓	✓
RAM	✓	✓	✗	✓	✓	✓	✓	✓

3. Methodology and Architecture

Our work investigates the usage of the private mode within the chosen web browser scope, compares the findings with those of normal web browsing mode and identifies which web browser offers the most privacy and if the results correlate with what is promoted by its web browser vendor. In the following sections, we explain extensively all the tools, methodologies and approaches we followed for our investigation approach; additionally, the visualization of it can be seen in Figure 1. The presented investigation approach analyzes each web browser to identify all the artefacts left behind from a terminated web session using private mode. This is compared to the results from a typical web session, which enables us to compare the two modes and each browser directly. Many tools and methodologies are easily accessible online to assist in digital forensics, and one may be easily overwhelmed by the wealth of information covering this specialist topic. Most of these forensic tools allow a trained specialist to investigate cases suspected that a device has been compromised or involved in a criminal act. Examination of areas such as memory or hard drive forensics is where this specialism comes into play.

In order to carry out the experimental part of our work in a controlled environment, VMware Workstation was used, which is a type two hypervisor [40], as this allows for the creation of virtual machines, straightforward configuration and the capability to use system snapshots. The benefits of using snapshots include maintaining the original image's integrity and enabling the virtual machine to be rolled back to a clean state after each test. This approach leverages the capabilities contained within modern CPU's that allow for the creation of virtual machines that are isolated as well as the applications that are installed on them. This is an alternative compared to a Type 1 hypervisor, also known as a bare-metal hypervisor and installed directly on physical hardware. Instead, using a type two hypervisor is shown to be a practical approach [28] in order to maintain a consistent and clean testing environment. Similarly to VMware, VirtualBox can also be leveraged to investigate each web browser by taking snapshots of the virtual machine under investigation before any testing is commenced in order to roll it back to a clean state when required [7].

The technical architecture of our work derives to an X64-based PC with an 11th generation Intel Core i7 CPU at 2.80 GHz, 16 GB RAM and 220 GB SSD. The used virtualisation software is the VMware Workstation 16 Pro to create a Windows 10 Pro virtual machine with 2 GB RAM and 20 GB Hard Disk space. As mentioned above, a clean snapshot of the virtual machine is taken before testing, which we reverted after each experimental test to ensure unbiased results and findings.

For the data acquisition, we followed a *Live acquisition* approach such as the following:

1. **Acquiring the VM's hard disk image**: We used FTK imager to take a forensically sound system image. This image was analyzed in Autopsy. An MD5 hash of each image for each browser test had been recorded.
2. **Acquiring VM's volatile memory image**: A copy of the VM's (*.vmem) volatile memory was taken whilst the web browser session terminated, and the VM was in a suspended state.

The forensic tools we utilized to conduct extensive web browser analysis are the following:

1. **FTK Imager 4.5** is a forensic tool that allows capturing a forensically sound image of a hard drive without making any modification to the original.
2. **Autopsy**: An open-source digital forensic application to conduct hard drive analysis. Examples of web artefacts this application reveals include bookmarks, cookies, web history, downloads, search queries and keywords.
3. **BrowsingHistoryView**: A tool by Nirsoft, which provides the ability to retrieve and display browsing history for several web browsers in a single table.
4. **Volatility Framework**: This tool is used to analyze the RAM images and allows us to view the live running state of the device.
5. **Bulk Extractor**: A tool that can analyze a memory image and extract interesting information such as browsing artefacts.
6. **Strings**: This is a commonly used utility tool to aid a digital forensic investigation that is included in most Unix systems. The tool searches every byte of digital evidence to locate strings of interest.

Common challenges during the digital forensic investigation include the possibility of powering off or restarting the device under investigation, incorrect assumptions that the target device is fully operational, insufficient information about the incident before commencing the investigation and, finally, incorrect investigation techniques that do not follow the order of volatility.

3.1. Normal and Private Mode Baselines

Before testing can commence, there must be a baseline of a known clean state of the file system contained within the virtual machine. This adds consistency and helps us identify any modifications to the Windows OS. Prior to testing the private mode for each web browser, the normal mode is inspected first. This aims to demonstrate the number of artefacts on the file system after each session for the two modes. As seen in Table 2, the following experimental testing steps were carried out in the following order for both normal and private browsing mode for each web browser included within our scope:

- Power on the virtual machine from a clean virtual machine snapshot;
- Invoke a new web browser session;
- Visit specific URLs contained within the test cases table into the address bar of the browser;
- Save the bookmark of the visited URL;
- Download an application to each web browser's default download location;
- Create an email account. Type the search query "gmail" in each web browser's search bar. Select the result for Gmail, and on the "Sign in" page choose "Create account". Continue with account creation.

Table 2. Test case approaches that we followed during the investigation activities.

Test Approach	Actions
1	Visit the *https://us-cert.cisa.gov/ (accessed on 30 November 2021)* URL and create a bookmark. Close the web browser's tab.
2	Visit the *https://eff.org (accessed on 30 November 2021)* and *https://basistech.com (accessed on 30 November 2021)* URLs, each accessed in new web browser tabs. Close both tabs.
3	Download the *Bleachbit* application from *https://bleachbit.org (accessed on 30 November 2021)*.
4	Conduct the following search engine queries in each web browser's address bar: *Bleeping Computer* and *Exploit db*.
5	Create a disposable Gmail account and login. Logout of Gmail account and close the web browser's tab.
6	Suspend the virtual machine.

3.2. Browser Private Mode—Vendor Statements

Each browser vendor provides a notification statement to the user by explaining their private mode functionality within an active web session. The verbiage used in each statement appears similar in content, with all statements alluding to help protect and enhance one's privacy.

The Google Chrome web browser's Incognito mode notice states the following: *"When you browse privately, other people who use the device won't see your history. Chrome doesn't save your browsing history or information entered in forms. Cookies and site data are remembered while you're browsing, but deleted when you exit Incognito mode. You can choose to block third-party cookies when you open a new incognito window"* [41].

Mozilla Firefox web browser's Private Browsing mode notice states the following: *"Private Browsing does not save your browsing information, such as history and cookies, and leaves no trace after you end the session. Firefox also has Enhanced Tracking Protection, which prevents hidden trackers from collecting your data across multiple sites and slowing down your browsing"* [42].

Microsoft Edge web browser's InPrivate mode notice states the following: *"The new Microsoft Edge will delete your browsing history, cookies, and site data, as well as passwords, addresses, and form data when you close all InPrivate windows"* [43]. As an additional note on this notice, Microsoft states the following concerning browser addons/extensions "Microsoft Edge can't prevent extensions from saving your browsing history while browsing InPrivate" [43].

Brave web browser's Private Windows mode notice states the following: *"A private window in Brave prevents Internet browsing history, form data, cookies and site data from being saved once you close the window. However, bookmarks saved from private windows are saved for regular windows too. Private browsing stops Brave from saving browsing activity beyond the current session. Note that some cookies and site data may be saved for the session, but will not be remembered when the browser is closed. Downloads and bookmarks are still saved even after closing a private window"* [44].

The approach used within this paper maintains a fair and consistent test across all web browsers. There are no adjustments made to the web browser settings; instead, the default values are provided as standard.

4. Analysis and Results

The test cases and methodology outlined in the previous Section 3 were performed for each browser in scope. This involved using the normal browsing mode first to establish a baseline for the private browsing mode test. As it can be observed in Table 1, our work tested several web browsers to investigate various artefacts left behind to both the hard disk and the RAM opposed to other works published in the literature. In our work, FTK imager was used to acquire the system images of the virtual machines used for each web browser test. The VM was then rolled back to a clean snapshot before testing commenced

on a different browser. Autopsy is the first tool used to perform hard disk forensics on the test cases. Ref. [45] mentions that whilst it is entirely possible to perform a digital forensic analysis by using the command line, it is not realistic due to the length of time and effort this would take. Autopsy was developed to automate this manual process by leveraging tools from "The Sleuth Kit" that can parse the output from the results into an intuitive graphical user interface. *Dead and live analysis* can be performed using Autopsy, which makes this tool versatile for a digital forensic investigation.

Table 3, depicts each web browser artefacts discovered in private browsing mode using Autopsy and *BrowsingHistoryView* forensic tools. It should be noted that these tools managed to retrieve the presented artefacts in all web browsers in the normal web browsing mode; hence, the normal browsing mode results were not included in the table. As it can be observed from the table, the web browser that has the least remnants of web browsing artefacts on the OS is Google Chrome using the Incognito mode.

Table 3. Artefacts of private browsing for the web browsers within our scope. Ticks present the found artefacts.

Artefacts	Brave	Google Chrome	Microsoft Edge	Mozilla Firefox
Bookmarks	✓	✗	✓	✓
Cookies	✗	✗	✗	✗
Downloaded files	✓	✗	✓	✓
Email	✗	✗	✗	✗
History	✗	✗	✗	✗
Web search queries	✗	✗	✗	✗

Contained within the Windows OS, there is a file named *"pagefile.sys"*. The purpose of this file is to store information from running applications whenever there is no space left in RAM. This file is also known as the swap file or virtual memory. Autopsy provides the necessary functionality to perform keyword searches for any strings chosen by the investigator. The keywords pertaining to the test cases were used, and the results returned several web artefacts contained within this hidden *pagefile.sys*. Similar research was performed by [2].

The results of the *pagefile.sys* can be seen for the normal browsing mode in Table 4 and for the private browsing mode in Table 5. As it can be observed, there were remnants of artefacts discovered in *pagefile.sys* for all web browsers except one: Google Chrome Incognito mode. This is an interesting discovery in the fact that other browsers based on Chromium architecture (Brave and Edge) returned positive results. Further experimentation into this file would be worth pursuing in future work.

4.1. Memory (RAM) Analysis

Analysis of the volatile memory (RAM) is a vital digital forensics technique that is becoming increasingly popular amongst investigators for identifying artefacts that could be vital in an investigation. For all digital forensic investigations, the order of volatility must be followed. The order of volatility deals with the lifetime of data, and data that are the most volatile must be collected first, as this is the most susceptible to being changed or destroyed first [46].

Table 4. Normal web browsing mode findings by inspecting the *pagefile.sys* file. Ticks present the found artefacts.

Artefacts		Brave	Google Chrome	Microsoft Edge	Mozilla Firefox
URLs	us-cert.cica.gov (accessed on 30 November 2021)	✓	✓	✓	✓
	basistech.com (accessed on 30 November 2021)	✓	✓	✓	✓
	eff.org (accessed on 30 November 2021)	✓	✓	✓	✓
	bleachbit.org (accessed on 30 November 2021)	✓	✓	✓	✓
Email Address	test@gmail.com	✗	✓	✓	✓
Web Searching	Bleeping computer	✓	✓	✓	✗
	Exploit db	✗	✓	✓	✗

Table 5. Private web browsing mode findings by inspecting the *pagefile.sys* file. Ticks present the found artefacts.

Artefacts		Brave	Google Chrome	Microsoft Edge	Mozilla Firefox
URLs	us-cert.cica.gov (accessed on 30 November 2021)	✓	✗	✓	✗
	basistech.com (accessed on 30 November 2021)	✓	✗	✓	✓
	eff.org (accessed on 30 November 2021)	✓	✗	✓	✓
	bleachbit.org (accessed on 30 November 2021)	✓	✗	✓	✓
Email Address	test@gmail.com	✗	✗	✓	✓
Web Searching	Bleeping computer	✗	✗	✓	✗
	Exploit db	✗	✗	✓	✗

A user's browsing history is optionally saved to a file on the hard disk, and in order for the browser to access and read that data, it must read the file's content into RAM [47]. This increases the possibility for a forensic investigator to retrieve browsing information from volatile memory. The next stage in this experiment was to capture a memory image of the virtual machine for each browser. This aims to identify whether any browsing-related artefacts reside in volatile memory during the private web browsing session had been terminated and compare that with the results on the hard disk. For this experiment, the following memory analysis forensic tools were used: Volatility, Bulk Extracto and Strings. Using multiple tools on a memory image allows for dual tool verification as not all tools present the same results. Memory analysis was performed utilizing the SANS Sift workstation [48], a forensic toolset containing free and open source utilities to assist a forensic expert in analysing digital evidence collected as part of an investigation. Starting in order for each web browser within our scope, a memory image was acquired and analyzed for both normal and private modes.

Brave Analysis

The Bulk Extractor tool was executed on the memory image that involved normal web browsing mode for Brave web browser specifically. All test cases for this experiment were run, and then the results were analyzed for related artefacts. After analysing all the results from running this tool, it was confirmed that all browsing artefacts in relation to our test cases resided in memory after the browser session had ended and the Brave web browser was closed (Appendix A). To continue the analysis, Strings was used to look for keywords in

relation to our test cases. Comparing this to Bulk Extractor, the results were similar in that almost all related artefacts were discovered by using this method (Appendix B). The final tool used on this memory image was Volatility. Volatility provides numerous plugins that can be used to extract specific information from a memory image. The focus for this test was to use a plugin called "Yarascan."This plugin can search an image for Yara signatures, looks for patterns found in malware or be used to perform searches on the fly, such as looking for strings containing "https:" [48]. All the related artefacts were found by using this plugin in Volatility (Appendix C).

An area-specific to Windows 10 OS is that of Memory Compression. This was introduced to increase the performance of the OS by compressing parts of process memory and then being swapped out to a specific memory store [49]. Their focus was exploring the memory compression issue and developing a method to de-obfuscate compressed pages as there could be the potential to uncover interesting digital artefacts. Within Volatility, a plugin called *pstree* exists whereby it can process and present a list of all running system processes depicted in a tree form. This output will display parent and child processes, which are indicated by indention and periods (.). In order to examine the memory space of the *MemCompression* process, an association of its identifier would need to be confirmed in order to dump the process to a file, which could then be analyzed using the Strings tool. Following the process of capturing, it could be analyzed using the Strings command and searching for keywords in relation to artefacts from the test cases (the investigation and results related to that can be seen in Appendix D).

Similarly to normal browsing mode, Brave's private mode is examined in the same manner. The output of each tool can be seen in Table 6. The Bulk Extractor was the first tool used and had similar results compared to normal browsing mode in Brave. Running this memory image through the next tool, Strings, returned slightly different artefacts than the Bulk Extractor, whereas in the third method for memory analysis through Volatility and using the plugin Yarascan to look for entries that include *"https"*, the results increased more than the previous two tools. In our test related to the web search of *Bleeping computer*, we retrieved *Partially* (the result for Bleeping Computer found was from the following web page: https://www.google.com/search?q=bleepi (accessed on 30 November 2021)), which is a web search query.

Table 6. Memory analysis results using the Bulk Extractor, Strings and Volatility in Brave's private web browsing mode. Ticks present the found artefacts.

Artefacts		Bulk Extractor	Strings	Volatility
URLs	us-cert.cica.gov (accessed on 30 November 2021)	✗	✓	✓
	basistech.com (accessed on 30 November 2021)	✓	✓	✓
	eff.org (accessed on 30 November 2021)	✓	✗	✓
	bleachbit.org (accessed on 30 November 2021)	✓	✓	✓
Email Address	test@gmail.com	✓	✓	✓
Web Searching	Bleeping computer	Partially (The result for Bleeping Computer found was: https://www.google.com/search?q=bleepi (accessed on 30 November 2021))	✓	✓
	Exploit db	✗	✓	✓

From analysing the results so far for private mode, it is clear that running multiple forensic tools is a must, as vital evidence could be potentially missed by a single tool. These results also demonstrate similar findings to browsing in normal mode with Brave and comparing directly with the results from hard disk analysis where it aligned with the web browser vendor statement; this was certainly not the case by analysing the volatile memory.

4.2. Web Browser Results

Table 7 depicts the results using all the tests tools, Bulk Extractor, Strings and Volatility, for all the web browsers within our scope, including the Brave browser already discussed previously. As seen in Brave's analysis in the previous subsection, in the test related to the web search of *Bleeping computer*, we retrieved partially the result (The result for Bleeping Computer found was: https://www.google.com/search?q=bleepi (accessed on 30 November 2021)) from the web search query. The normal web browsing analysis results were as expected, retrieving most of the artefacts in our tests. Hence, they have not been included in the table, and we focused our comparison on the private browsing modes of all the web browsers within our scope. This memory analysis technique provided interesting results, with Firefox private mode reporting the least artefacts found.

Table 7. Results of each tested tool for all the web browsers regarding the private browsing modes. Ticks present the found artefacts.

Tool	Artefacts		Brave	Google Chrome	Microsoft Edge	Mozilla Firefox
Bulk Extractor	URLs	us-cert.cica.gov (accessed on 30 November 2021)	✗	✓	✓	✓
		basistech.com (accessed on 30 November 2021)	✓	✓	✓	✓
		eff.org (accessed on 30 November 2021)	✓	✓	✗	✓
		bleachbit.org (accessed on 30 November 2021)	✓	✓	✓	✓
	Email Address	test@gmail.com	✓	✗	✓	✓
	Web Searching	Bleeping computer	Partially	✗	✓	✗
		Exploit db	✗	✓	✓	✓
Strings	URLs	us-cert.cica.gov (accessed on 30 November 2021)	✓	✓	✓	✓
		basistech.com (accessed on 30 November 2021)	✓	✓	✓	✓
		eff.org (accessed on 30 November 2021)	✗	✓	✓	✓
		bleachbit.org (accessed on 30 November 2021)	✓	✓	✓	✓
	Email Address	test@gmail.com	✓	✗	✓	✗
	Web Searching	Bleeping computer	✓	✓	✓	✗
		Exploit db	✓	✓	✓	✓
Volatility	URLs	us-cert.cica.gov (accessed on 30 November 2021)	✓	✓	✓	✓
		basistech.com (accessed on 30 November 2021)	✓	✓	✓	✓
		eff.org (accessed on 30 November 2021)	✓	✓	✓	✓
		bleachbit.org (accessed on 30 November 2021)	✓	✓	✓	✓
	Email Address	test@gmail.com	✓	✗	✗	✗
	Web Searching	Bleeping computer	✓	✗	✗	✗
		Exploit db	✓	✗	✓	✗

5. Discussion

Most users tend to opt for convenience and usability over security and do not use the private browsing mode offered by many browser vendors or perhaps do not even know that this functionality is available to them. On the other side to this, malicious users may purposely use this functionality in an attempt to cover their tracks. An example of this could be a scenario in the workplace, whereby an employee is wasting time by browsing non-work related websites instead of performing tasks related to their role. This use case may be more common than what is thought, and whilst private browsing can make digital forensics slightly more challenging to retrieve artefacts, it will not prevent technologies such as web filtering and firewalls from recording this activity. There are, in fact, security solutions specific to detecting insider threats, such as time wasting and alert on when a user that browses the web when using private mode. This in itself demonstrates that this is an everyday use case that can be misused and will continue to be misued for the foreseeable future.

Brave is one of the newest browsers that purports to focus on privacy as claimed by the vendor. The experiments in our work expected that Brave would be the browser to have the least amount of recoverable browsing artefacts, either on disk or in RAM. Surprisingly this was not the case, and similarly to others within the browser scope, the results have shown that many were identified primarily through volatile memory analysis. It can be easy for an inexperienced user to be misled by claims from the browser vendors who advertise their private browsing functionality, thinking that by using this particular mode, their web transactions and activity will be completely private with no chance of recovery. It could also induce an individual to engage in riskier online behaviour, both in the workplace or at home.

The results of our experiments have shown that although browser vendors provide privacy-based features, such as private browsing, it does not guarantee complete anonymity. Security awareness training in the workplace is one such tool that helps educate the userbase through means of video content and similar but needs to be engaging enough for the material to resonate with the individual. The decision to choose the browsers included in this scope was taken after reviewing the current web browser market share and comparing it with other works in the literature. The Brave browser is a relative newcomer within this area and was chosen due to its privacy boasting features. As more research has been conducted within this space over the last decade, it presents an opportunity to compare browsers over time and investigates if they have different behaviours regarding private web browsing modes. Additionally, the focus of this paper aims to perform an extensive investigation according to the following investigation goals, seeking to understand better how modern-day browsers using private mode by comparing one to the other and their vendor counterparts.

Which Artefacts Are Left Behind in Windows OS Whilst Using Private Mode within the Web Browsers of Our Scope.

The results obtained through this experiment revealed that all the web browsers within this testing scope had retained remnants of most browsing artefacts included in the test cases, both on the hard disk and in volatile memory. The importance of using different forensic tools has been evident throughout this experiment, as some have identified artefacts that another has not. This would provide an investigator with more data to analyze to attain forensically sound data that can be admissible in a court of law. Table 7 indicates that more browsing artefacts within private browsing mode were uncovered by using memory analysis techniques rather than analysis of the hard disk image using Autopsy. The *pagefile.sys*, which was not the focus of this experiment, returned positive hits within Autopsy.

Evaluating the Results Using Different Forensic Toolsets for Both Normal and Private Web Browsing Modes across Each Web within Our Scope.

Throughout this experiment, using multiple open-source forensic toolsets has been invaluable in uncovering positive results, especially using the straightforward *Strings* command on the volatile memory images. This tool uncovered several browsing artefacts within this investigation and would be one of the easiest and quickest to execute for an examiner. Time is of the essence in any forensic investigation, and having a reliable and effective tool is fundamental to collate forensically sound data. Using *Bulk Extractor* also proved fruitful and achieved similar results to Strings. Finally, *Volatility* was used to perform scans of the volatile memory image using the Yarascan plugin, and the results returned from this technique uncovered the most artefacts of the other memory analysis methods.

Which Browser Leaves the Least Artefacts behind on the OS.

This experiment's results clearly indicate that the browser that leaves the least browsing artefacts behind, both on the hard disk and in volatile memory, was the Google Chrome browser using the Incognito mode. This discovery was unexpected in the fact that the Brave browser was the one expected to be the most privacy-focused out of all in the testing scope, which is also based on the same Chromium engine. Future work could include testing the same web browsers under the same conditions in portable modes, such as mobile devices, and using the same forensic methodology utilized in this experiment.

How Does the Privacy-Focused Brave Browser Compare to the Other Mainstream Browsers.

Both normal and private modes within the Brave browser did not meet the expectations of this experiment compared to the other web browsers, in terms of recovery of URLs of sites, as part of our testing plan. Disk analysis for private mode using Autopsy matched the Vendors declaration of "Downloads and bookmarks are still saved even after closing a private window" [44]. However, during memory analysis, including the results for *pagefile.sys*, it returned most signs of browsing activity, as depicted in Table 7. Memory analysis has shown to be a valuable asset in an examiners toolkit, especially when it comes to web browsers that purport to focus on privacy.

6. Conclusions

The aim of our work was to investigate the usage of the private browsing mode within the chosen web browser scope, compare the findings with that of normal web browsing mode and identify from the findings which one of the browsers offers the most privacy and if the results correlate with what is promoted by each web browser vendor. Our testing methodology and architecture remained consistent across each web browser, along with specific browsing related tests. At the end of each test, the testing VM was rolled back to a clean snapshot so that the environment remained consistent and fresh for each browser.

The conducted analysis related to hard disk forensics met the expectations of what was declared by each web browser vendor, with the exception of artefacts discovered in the *pagefile.sys*. However, viewing the volatile memory's analysis results for all the web browsers in both normal and private web browsing modes has shown that mainly traces of artefacts can be found on the hard disk, and volatile memory can be an essential asset in a forensic investigation. This is particularly accurate for the order of volatility, as if a machine is restarted or powered off, and all traces would be lost, making recovery of evidence difficult for the forensic analyst and overall investigation.

For the vast majority of people, web browsing remains one of the main activities performed on computer systems as more and more technologies transition their services into the cloud and make it easier for people to connect, collaborate and conduct business. Whilst a lot of this will be legitimate behaviour, there will also be an element that allows using technology for nefarious reasons. For this reason, IT specialists with the necessary skills are required to try and keep up with the latest topics in this area and be able to

think similarly to a malicious actor. Digital forensics remain a vital element in any digital investigation and is needed now more than ever as the number of devices increases to for performing cyber-attacks and criminal investigations. This work highlights that private browsing does not mean absolute anonymity, and someone with the appropriate skills and tools can recover artefacts related to the activity carried out through the web browser.

Recommendations for future work would be to consider using a similar methodology and architecture in order to compare the findings with the Tor web browser and the Brave browser with Tor connectivity since these topics have not been extensively investigated in the literature. Additionally, further anti-forensic technologies can be tested, such as CCleaner and Bleachbit. Finally, since the world shifts towards a mobile era, portable web browsing could be analyzed by following a similar investigation approach with our work and especially privacy-focused mobile browsers such as DuckDuckGo.

Author Contributions: All authors contributed in the conceptualization and methodology of the manuscript; K.H. performed data preparation and the practical experiments; K.H., P.P. and N.P. contributed in writing; A.S., J.A. and W.J.B. reviewed and edited the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data is contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A

The Figures A1–A3 present the output of the Bulk Extractor tool regarding Brave's normal web browsing mode.

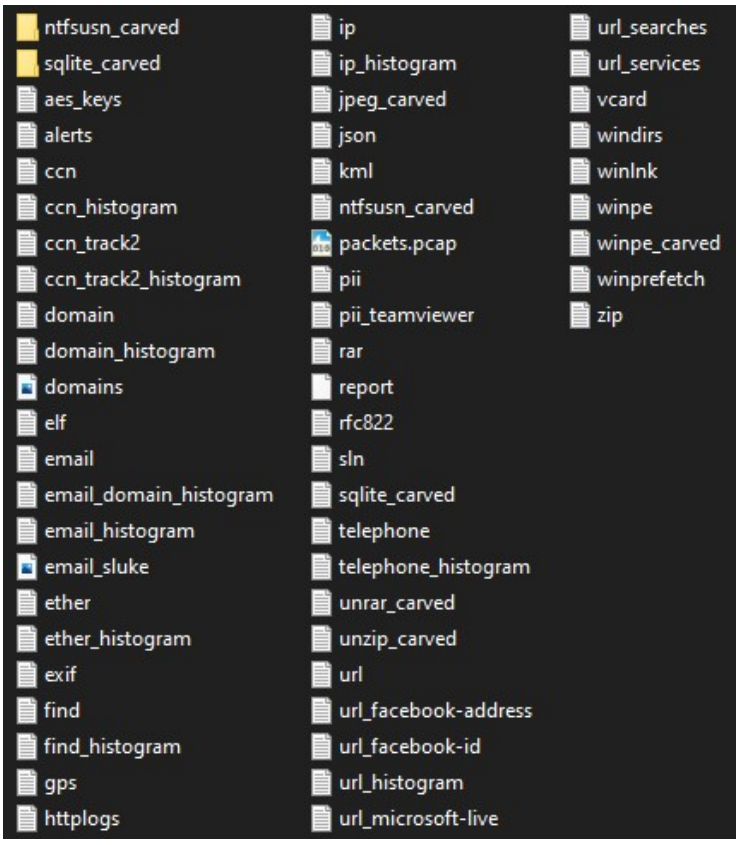

Figure A1. Bulk Extractor results structure.

Figure A2. Example of domain artefacts found in domains.txt file using the Bulk Extractor tool.

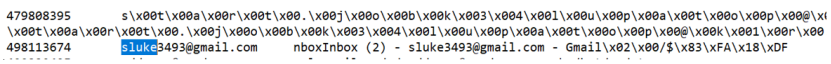

Figure A3. Email address found in email.txt file using the Bulk Extractor tool.

Appendix B

Figure A4 presents the output of the Strings tool regarding Brave's normal web browsing mode.

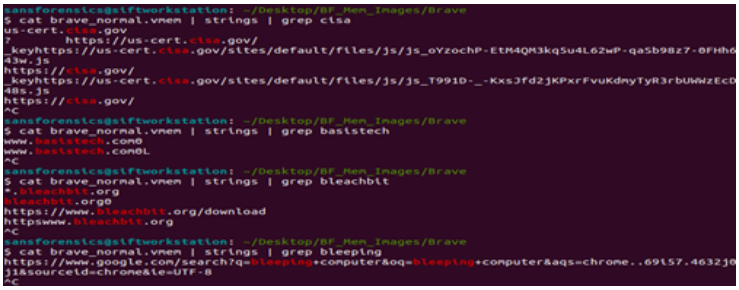

Figure A4. Strings investigation for specific keywords.

Appendix C

The syntax of Figure A5 used to perform a volatility search using the Yarascan plugin in Brave's normal web browsing mode. The results of this command can be seen in Figure A6.

```
vol.py -f brave_normal.vmem --profile=Win10x64_19041 yarascan -U "https:" >
yarascan.txt
```

Figure A5. Volatility Yarascan looking for the keyword "https:".

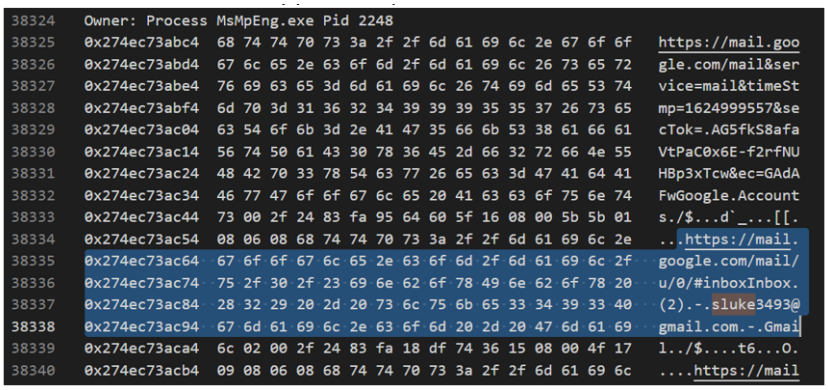

Figure A6. Yarascan Output displaying email artefact running in MsMpEng.exe (Windows Defender Antimalware Application).

Appendix D

In Figure A7, the process of dumping a process to a file can be seen in order to conduct further analysis. Additionally, in Figure A8, this file analyzed using the *Strings* tool in combination with *grep*.

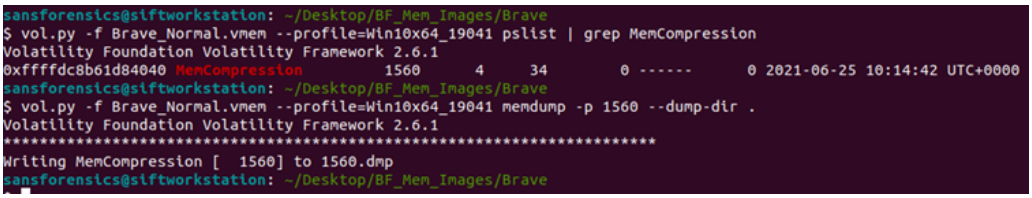

Figure A7. Identifying and dumping MemCompression process for further analysis.

Figure A8. Strings tool in combination with *grep*.

References

1. Önday, Ö. Battle of Desktop Web Browsers: The Case of Internet Explorer and Mozilla Firefox. *J. Sci. Rep.* **2020**, *2*, 53–57.
2. Mahlous, A.R.; Mahlous, H. Private Browsing Forensic Analysis: A Case Study of Privacy Preservation in the Brave Browser. Available online: http://www.inass.org/2020/2020123126.pdf (accessed on 30 November 2021).
3. Satvat, K.; Forshaw, M.; Hao, F.; Toreini, E. On the privacy of private browsing—A forensic approach. In *Data Privacy Management and Autonomous Spontaneous Security*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 380–389.
4. Afridi, N. The Current Status of Forensic Science and its Impact on Administration of Criminal Justice System in Pakistan: An Analytical Study. Available at SSRN 3781586. 2021. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3781586 (accessed on 30 November 2021).
5. Santhosh, B.; Dsouza, N.; Kumbhar, A.D. Digital Forensics in Cloud Computing Environment. Available online: http://www.ijsrcsams.com/images/stories/Past_Issue_Docs/ijsrcsamsv7i6p123.pdf (accessed on 30 November 2021).
6. Leith, D.J. Web Browser Privacy: What Do Browsers Say When They Phone Home? *IEEE Access* **2021**, *9*, 41615–41627. [CrossRef]
7. 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. [CrossRef]
8. Fayyad-Kazan, H.; Kassem-Moussa, S.; Hejase, H.J.; Hejase, A.J. *Forensic Analysis of Private Browsing Mechanisms: Tracing Internet Activities*; 2021. Available online: https://www.researchgate.net/profile/Hussin-Hejase/publication/350555715_Forensic_analysis_of_private_browsing_mechanisms_Tracing_internet_activities/links/607e99512fb9097c0cf7639c/Forensic-analysis-of-private-browsing-mechanisms-Tracing-internet-activities.pdf (accessed on 30 November 2021).
9. Voigt, P.; Von dem Bussche, A. The eu general data protection regulation (gdpr). In *A Practical Guide*, 1st ed.; Springer International Publishing: Cham, Switzerland, 2017.
10. Pardau, S.L. The California consumer privacy act: Towards a European-style privacy regime in the United States. *J. Tech. L. Pol'y* **2018**, *23*, 68.
11. Li, H.; Yu, L.; He, W. *The Impact of GDPR on Global Technology Development*; 2019. Available online: https://www.researchgate.net/publication/339629705_Battle_of_Desktop_Web_Browsers_The_Case_of_Internet_Explorer_and_Mozilla_Firefox (accessed on 30 November 2021).
12. Papadopoulos, P.; Pitropakis, N.; Buchanan, W.J. Decentralised Privacy: A Distributed Ledger Approach. In *Handbook of Smart Materials, Technologies, and Devices*; Hussain, C.M., Di Sia, P. Eds.; Springer: Cham, Switzerland, 2021.
13. Papadopoulos, P.; Abramson, W.; Hall, A.J.; Pitropakis, N.; Buchanan, W.J. Privacy and Trust Redefined in Federated Machine Learning. *Mach. Learn. Knowl. Extr.* **2021**, *3*, 333–356. [CrossRef]
14. Said, H.; Al Mutawa, N.; Al Awadhi, I.; Guimaraes, M. Forensic analysis of private browsing artifacts. In Proceedings of the 2011 International Conference on Innovations in Information Technology, Abu Dhabi, United Arab Emirates, 25–27 April 2011; pp. 197–202.
15. Liou, J.C.; Logapriyan, M.; Lai, T.W.; Pareja, D.; Sewell, S. A study of the internet privacy in private browsing mode. In Proceedings of the 3rd Multidisciplinary International Social Networks Conference on SocialInformatics 2016, Data Science 2016, Union, NJ, USA, 15–17 August 2016; pp. 1–7.
16. Stafford, T.F.; Urbaczewski, A. Spyware: The ghost in the machine. *Commun. Assoc. Inf. Syst.* **2004**, *14*, 49. [CrossRef]
17. De Beer, R.; Stander, A.; Van Belle, J.P. Anti-forensics: A practitioner perspective. *Int. J.-Cyber-Secur. Digit. Forensics* **2015**, *4*, 390–403.
18. Grosskurth, A.; Godfrey, M.W. A reference architecture for web browsers. In Proceedings of the 21st IEEE International Conference on Software Maintenance (ICSM'05), Budapest, Hungary, 26–29 September 2005; pp. 661–664.
19. Fehlhaber, A.L.; Acar, Y.; Fahl, S.; Gutfleisch, M.; Theis, D.; Wallkötter, F. Poster: When Brave Hurts Privacy: Why Too Many Choices Do More Harm than Good. Available online: https://www.ieee-security.org/TC/SP2020/poster-abstracts/hotcrp_sp20posters-final19.pdf (accessed on 30 November 2021).

20. Habib, H.; Colnago, J.; Gopalakrishnan, V.; Pearman, S.; Thomas, J.; Acquisti, A.; Christin, N.; Cranor, L.F. Away from prying eyes: Analyzing usage and understanding of private browsing. In Proceedings of the Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018), Baltimore, MD, USA, 12–14 August 2018; pp. 159–175.
21. Soghoian, C. *Why Private Browsing Modes Do Not Deliver Real Privacy*; Center for Applied Cyber Security Research: Bloomington, IN, USA, 2011. Available online: https://www.consumerwatchdog.org/sites/default/files/resources/soghoian2.pdf (accessed on 30 November 2021).
22. Korniotakis, J.; Papadopoulos, P.; Markatos, E.P. Beyond Black and White: Combining the Benefits of Regular and Incognito Browsing Modes. In Proceedings of the 17th International Joint Conference on e-Business and Telecommunications (ICETE 2020)—SECRYPT, Lieusant, Paris, 8–10 July 2020; pp. 192–200.
23. Fennelly, L.J.; Perry, M.A. Building a Sustainable Culture of Security. In *The Professional Protection Officer*; Elsevier: Amsterdam, The Netherlands, 2020; pp. 397–401.
24. Horsman, G. The challenge of identifying historic 'private browsing'sessions on suspect devices. *Forensic Sci. Int. Digit. Investig.* **2020**, *34*, 300980. [CrossRef]
25. Nelson, R.; Shukla, A.; Smith, C. Web Browser Forensics in Google Chrome, Mozilla Firefox, and the Tor Browser Bundle. In *Digital Forensic Education*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 219–241.
26. Gratchoff, J.; Kroon, G. *Project Spartan Forensics*; Amsterdam University: Amsterdam, The Netherlands, 2015.
27. Yang, W.C.; Lo, T.C.; Chen, C.H. Applying Memory Forensic Technique in Popular Browsers to Assist Criminal Investigation in the Cloud. *Forensic Sci. J.* **2017**, *16*, 43–50.
28. Montasari, R.; Peltola, P. Computer forensic analysis of private browsing modes. In *International Conference on Global Security, Safety, and Sustainability*; Springer: Berlin/Heidelberg, Germany, 2015; pp. 96–109.
29. Garewal, K.S. The Cryptocurrency Ecosystem. In *Practical Blockchains and Cryptocurrencies*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 19–27.
30. Joseph, D.P.; Norman, J. An analysis of digital forensics in cyber security. In Proceedings of the First International Conference on Artificial Intelligence and Cognitive Computing, Beijing, China, 13–15 October 2019; pp. 701–708.
31. Belshaw, S.H. Next generation of evidence collecting: The need for digital forensics in criminal justice education. *J. Cybersecur. Educ. Res. Pract.* **2019**, *2019*, 3.
32. Wu, Y.; Gupta, P.; Wei, M.; Acar, Y.; Fahl, S.; Ur, B. Your secrets are safe: How browsers' explanations impact misconceptions about private browsing mode. In Proceedings of the 2018 World Wide Web Conference, Lyon, France, 23–27 April 2018; pp. 217–226.
33. Brunner, H. *Detecting Privacy Leaks in the Private Browsing Mode of Modern Web Browsers through Process Monitoring*; 2014. Available online: https://resolver.obvsg.at/urn:nbn:at:at-ubtuw:1-76431http://hdl.handle.net/20.500.12708/8355 (accessed on 30 November 2021).
34. Schneier, B. The Hidden Battles to Collect Your Data and Control Your World. Data Goliath, Lond. 2015. Available online: https://www.schneier.com/books/data-and-goliath/ (accessed on 30 November 2021).
35. Mugisha, D.; Rughani, P. WEB BROWSER FORENSICS: Evidence Collection and Analysis for Most Popular Web Browsers Usage in Windows 10. 2018. Available online: https://www.researchgate.net/profile/David-Mugisha/publication/332093270_WEB_BROWSER_FORENSICS_Evidence_collection_And_Analysis_for_Most_Popular_Web_Browsers_usage_in_Windows_10/links/5c9f88cc92851cf0aea2af22/WEB-BROWSER-FORENSICS-Evidence-collection-And-Analysis-for-Most-Popular-Web-Browsers-usage-in-Windows-10.pdf (accessed on 30 November 2021).
36. Mistry, N.R.; Dahiya, M. Signature based volatile memory forensics: A detection based approach for analyzing sophisticated cyber attacks. *Int. J. Inf. Technol.* **2019**, *11*, 583–589. [CrossRef]
37. Qawasmeh, E.; Al-Saleh, M.I.; Al-Sharif, Z.A. Towards a generic approach for memory forensics. In Proceedings of the 2019 Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, 20–21 November 2019; pp. 94–98.
38. Kävrestad, J. *Fundamentals of Digital Forensics*; Springer: Berlin/Heidelberg, Germany, 2020.
39. Jadoon, A.K.; Iqbal, W.; Amjad, M.F.; Afzal, H.; Bangash, Y.A. Forensic analysis of Tor browser: A case study for privacy and anonymity on the web. *Forensic Sci. Int.* **2019**, *299*, 59–73. [CrossRef] [PubMed]
40. Pandey, R. Comparing VMware Fusion, Oracle VirtualBox, Parallels Desktop Implemented as Type-2 Hypervisors. 2020. Available online: https://www.researchgate.net/profile/Rachit-Pandey-3/publication/344046461_Comparing_VMware_Fusion_Oracle_VirtualBox_Parallels_Desktop_implemented_as_Type-2_hypervisors/links/5f4fbf75a6fdcc9879c18621/Comparing-VMware-Fusion-Oracle-VirtualBox-Parallels-Desktop-implemented-as-Type-2-hypervisors.pdf (accessed on 30 November 2021).
41. Chrome. Chrome Notice. 2021. Available online: https://support.google.com/chrome/answer/7440301?hl=en&ref_topic=9845306 (accessed on 30 November 2021).
42. Firefox. Firefox Notice. 2021. Available online: https://support.mozilla.org/en-US/kb/private-browsing-use-firefox-without-history (accessed on 30 November 2021).
43. Edge. Edge Notice. 2021. Available online: https://support.microsoft.com/en-us/microsoft-edge/browse-inprivate-in-microsoft-edge-cd2c9a48-0bc4-b98e-5e46-ac40c84e27e2 (accessed on 30 November 2021).
44. Brave. Brave Notice. 2021. Available online: https://support.brave.com/hc/en-us/articles/360017840332 (accessed on 30 November 2021).
45. Carrier, B. *File System Forensic Analysis*; Addison-Wesley Professional: Boston, MA, USA, 2005.

46. Årnes, A. *Digital Forensics*; John Wiley & Sons: Hoboken, NJ, USA, 2017.
47. Ligh, M.H.; Case, A.; Levy, J.; Walters, A. *The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory*; John Wiley & Sons: Hoboken, NJ, USA, 2014.
48. SANS. Sans SIFT. 2021. Available online: https://www.sans.org/tools/sift-workstation/ (accessed on 30 November 2021).
49. Østerud, A. Windows 10 Memory Compression in Digital Forensics-Uncovering Digital Evidence in Compressed Swap. Master's Thesis, NTNU, Trondheim, Norway, 2018.