Applied Information Technology And Computer Science Vol. 3 No. 2 (2022) 068-083

AITCS

Homepage: http://publisher.uthm.edu.my/periodicals/index.php/aitcs
e-ISSN :2773-5141

A Comparative Analysis of Residual Data Between Private Browsing and Normal Browsing using Live Memory Acquisition

Aina Izzati Afende[1], Nurul Hidayah Ab Rahman [1]*

[1]Faculty of Computer Science and Information Technology,
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA

DOI: https://doi.org/10.30880/aitcs.2022.03.02.005
Received 04 August 2022; Accepted 06 October 2022; Available online 30 November 2022

Abstract: Nowadays, web browsers are an important tool that allows people to perform common online activities such as internet banking, buying online and accessing social networking sites. All user activities and data from browsing can be tracked and stored in normal mode browsing such as cookies, caches, downloads, history, other sensitive data, and temporary files, which helps digital forensic investigators trace any evidence left. Hence, this research analyses and compare which browsers mode among Google Chrome and Firefox can extract the entire residual data from the laptop's volatile storage testing on a forensic tool. The research is conducted using live memory acquisition to acquire disk images from Random Access Memory (RAM). The tool used for acquisition is Belkasoft RAM Capturer while Autopsy is used for analysis. There are four stages involved in methodology: preparation stage, forensic acquisition and analysis stage, analysis stage and validation stage. Findings from this study show that live memory acquisition on private and normal browsing modes is able to acquire key residual data such as email Id, password, downloaded files, web visits and keyword terms. This study shows that RAM forensics can be significantly utilised to acquire the evidence for browsing activities in physical memory such as email Id, password, downloaded files, keyword terms and downloaded files.

Keywords: Live memory acquisition, RAM, Artefacts, Digital forensic, Web Browsers

1. Introduction

Nowadays, web browsers are an important tool that allows people to perform common online activities such as internet banking, buying online and accessing social networking sites. All users' data from browsing activities can be tracked and stored in normal mode browsing such as cookies, caches, downloads, history, other sensitive data, and temporary files. In a case of cybercrime, the data would help digital forensic investigators to trace any evidence left. Meanwhile, private mode enables users to preserve their surfing sessions hidden from others who share a device with them [2]. However, this statement is contrary to [30] that claimed Google is still invading privacy by collecting user's IP addresses, user IDs, cookies and other data while in private mode.

*Corresponding author: hidayahar@uthm.edu.my

Hence, in this research, the residual data is analysed between Google Chrome and Mozilla Firefox web browsers mode, normal browsing and private browsing mode using a forensic tool to compare the difference of number of data extraction. The project is undertaken using a live memory acquisition tool that gathers data in actual time as RAM temporarily stores computer storage due to its dynamic nature.

The objectives of this study are in three-fold: (1) To study the type of residual data that can be extracted, (2) to compare the data extraction between private and normal browsers from Google Chrome and Firefox web browsers and (3) to analyse which browser presents more complete residual data.

The rest of the paper is organised as follows: Section 2 discusses the literature review, such as digital forensics and its conceptual background, digital forensics phases, memory investigations technique, and related work from previous research studies in memory forensics and browser forensics. Next, Section 3 explains the research methodology using the diagram to show all the steps and processes involved in priority during the experiment. The software and hardware specifications and the expected results are also mentioned in this section. Subsequently, Section 4 describes the experimental setup using BelkaSoft RAM Capturer and Autopsy tools on Google Chrome and Mozilla Firefox. All the processes and findings from the experiment were also discussed. Lastly, Section 5 concluded the study and the future work.

2. Background of Study

This section discusses literature review and includes topics like the conceptual background of digital forensics, the stages of digital forensics, memory investigation techniques and related previous works in memory forensics and browser forensics.

2.1 Digital Forensics

Digital forensics concentrated on memory recoverable from devices to acquire digital evidence for cybercrime investigations. However, the obtained evidence should be admissible throughout some processes in the court of law. Therefore, digital forensics investigators must preserve the data in its original state [3].

Furthermore, the process of acquiring, examining, analysing and reporting digital evidence must be conducted in a forensically sound manner. Therefore, investigator teams must comply with the digital forensics phases that are based on widely recognised standards.

2.2 Digital Forensics Phases

The main goal of digital forensics is to collect admissible evidence from computer crime through a proper and strict procedure to assure the integrity and reliability of data. It can be done through a chain of custody that focuses on the documentation before presenting a formal forensic report in a court of law [4]. Many digital forensic models have proposed that each model has different phases from other models depending on its methodology [5].

Five highlighted phases in digital forensics are: (1) identifying and collecting, (2) preservation, (3) acquisition, (4) analysis and examination and lastly, (5) documentation [6], [7]. During the identifying and collecting phase, all the information that has potential evidence for criminal doings and the source location are identified, labelled and collected to be used in the next stage, acquisition. The information that could be evidence for criminal acts is the traces of users left, such as log files, temporary files, network connections, browsing history and cache [8]. Therefore, the forensic tool could mostly find the data in the RAM storage depending on the operating system used [9].

2.3 Digital Forensics Memory Investigation Techniques

Digital forensics memory is applied to investigate the validity of the evidence used at trial. The next phase in most computer forensic examinations is to create an exact copy of data stored on the evidence solid-state drive or any other digital storage device. The purpose is to produce a replica as a backup for evidence not altered [10]. There are two types of forensic techniques to acquire memory images: Dead Forensics and Live Forensics.

2.3.1 Dead Forensics

All the data such as data files, hidden files, exchanged files, web activity, artefacts, and log files will be lost once the computer is shut down and is categorised as dead forensics [11]. The data will be duplicated from non-volatile memory such as hard drives or USB flashcards before proceeding to the investigation process to maintain the evidence originality of well-preserved disk evidence. Data analysis will be stopped once the computer is shut down during dead acquisition analysis [12].

2.3.2 Live Forensics

Live forensics, as it is called live system acquisition, works in a volatile RAM that contains potential artefacts that could be used as evidence for the crime when the system is running in the background [7]. Most of the traces left from computer usage sessions and artefacts are retrievable from volatile memory analysis, which might not be accessible in the external memory [9].

However, the data cannot be collected for acquisition since data is lost once the computer stops running or reboot. Therefore, it would present challenges to handle RAM data without proper procedures during analysis [13]. Live forensics suits for handling any occurrence and efficiently storing data in the volatile RAM [7].

2.4 Web Browser Forensics

Web browser is a software that becomes a medium for people to access the internet by using the access service provided. The most common web browsers are Google Chrome, Mozilla Firefox, Microsoft Edge and Brave. As reported in [13], there were almost 4.5 billion Internet surfers in 2019. It involves everyday browsing activities such as watching videos online, browsing web pages, posting pictures or videos on social media, and downloading and uploading files. There are two different browser modes: normal browsing and private browsing mode.

2.4.1 Normal Browsing Mode

Normal browsing records all the browsing activities such as caches, cookies, search keywords, login credentials and URL history on the computer. The cookies from your browsing activities remember most of the user's details, such as browsing patterns that can tell the frequent website user visit or the video user regularly watch. Therefore, it will provide the content related to your findings [14].

Digital forensics investigators rely on the artefacts left from those browser records in the device, using forensic techniques on how to seize the artefacts to support the findings of evidence [1]. The artefacts are stored in the computer memory after all the browsing histories, caches and cookies are cleared from web browsers, making it easy for digital forensic examiners to extract the data.

2.4.2 Private Browsing Mode

According to [15], internet users pose privacy concerns when surfing the internet as the internet browsing activities can still be viewed even after the histories, caches, and cookies are deleted in the browser. Hence, the developers started developing a private browser mode to improve privacy and anonymity by not leaving traces and information from browsing activities. In addition, all new caches stored during the browsing will be removed once the browser is closed [16].

Each web browser provides a private browser mode with different terms. For example, both Internet Explorer and Microsoft Edge use "InPrivate Browsing," "Incognito Mode" for Google Chrome and "Private Browsing" for Mozilla Firefox. In addition, for Brave browsers, there are two types of private browsing modes, "Private Window" and "Private Window with Tor" [16].

Table 1 shows the result from the type of artefacts and data remnants that can be extracted using digital forensic techniques and tools. Each internet browser displays a different result from an internet browsing session. Some downloaded files in the private browsing mode can be seen, and the tracking protection is not applied on web browsers.

Table 1: An overview of private windows from big internet browsers [16]

Browser	Browsing History Not Stored	Cookies Not Stored	Login Info Not Stored	Form Data Not Stored	Tracking Protection Enabled	Download Files Hidden
Safari 11.03	✓	✓	✓	✓	Do not track	✓
Internet Explorer 11	✓	✓	✓	✓	Do not track	✓
Firefox 58.02	✓	✓	✓	✓	Disconnect	✗
Edge 41.16299.15	✓	✓	✓	✓	✗	✓
Chrome 63.0.3239	✓	✓	✓	✓	✗	✗
Opera 51	✓	✓	✓	✓	✗	✗

2.4.3 Web Browser Forensics

As defined by Jadhav and Meshram [17], web browser forensics is a program that enables the user to access the internet and is primarily used by digital forensic investigators to analyse information from browsing sessions, such as to collect any potential fraud for digital evidence. The potential information extracted from browser forensics are browsing history, cache, cookies, bookmarks, and download list. The digital forensic procedures for browser forensic must be appropriately followed to assist the investigator in performing the investigation; the first step is collection, examination, and analysis, and lastly, documentation of evidence. The procedures differ depending on how they want to handle the inspection. Some popular browser forensics tools such as NetAnalysis, Browsing History Examiner (BHE) and Internet Evidence Provider (IEF) investigate browser features [18].

As study by [15] pointed out, these artefacts left from browsing activities by a criminal can be extracted using forensic tools to assist the investigator's investigation. Moreover, the increase of cybercrimes such as hacking, fraudulent transactions and theft of intellectual property raises the appearance of digital forensics to respond to the cybercrimes using a digital device. This study conducted the experiment using Google Chrome and Mozilla Firefox for browsing activities.

2.4.4 Residual Data

Residual data, called remnants data, is a collection of data that has been removed from storage in a local device. However, the data remanence can still be viewed using a specific tool to identify the location, usually in the file slack place or local folders. According to Khairallah [19], the common types of residual data left from the installed application are link files, log files, registry files, prefetch files and the account registered through a web browser. Digital forensics can gather solid electronic evidence from remnants and artefacts to be used in trials.

The obtained evidence must be admissible in the court of law, especially the digital evidence, as it could easily be tampered with without proper procedures [20]. Hence, there are certain characteristics of digital evidence that the courts accept according to the following criteria:

1. Search warrants – Evidence obtained without permission may not be acknowledged in court.
2. Reports – All the processes, tools, methods, techniques, specific time and date and chain of custody are documented formally to demonstrate and support the authenticity of the digital evidence in the court of law.
3. Evidence authentication – The original obtained evidence should match the copy evidence by comparing the hash values. The acquired evidence must remain unchanged to convince the courts with accurate information. The courts accept copies of evidence if the original evidence has been lost or destroyed.

2.5 Comparison with Existing Works

Table 2 represents the comparative analysis of existing works on different browsers mode by observing the techniques used in the literatures [7], [21], [22]. It was identified that the most common web browsers used for datasets collection are Google Chrome and Mozilla Firefox [1], [21], [22]. The experiment was conducted using normal and private browsing modes [1].

Therefore, this study attempts to extend the previous study by [1] where the technique used was dead forensic on normal browsing and private browsing mode in web browsers using MiniTool Power Data and Process Monitor. Furthermore, a previous study from [22] conducted live data forensics using Process Monitor, FTK and IEF in web browsers Chrome and Firefox. Meanwhile, a study by [7] used live data forensics to acquire artefacts from portable browsers. Hence, this motivates this study to investigate the artefacts from browsing activities using live memory forensics, especially in private browsing mode is likely to be exploited by criminals to conduct crimes. This work considers using Autopsy to compare the study results with the other forensic tools as it can perform in all Windows versions, either 32-bits and 64-bits.

Table 2: Comparative analysis based on existing research

Work	Technique	Tools used	Browser	Browsing Mode	Artefacts found
Fayyad (2021)	Dead Forensic	MiniTool Power Data, Process Monitor	Chrome, Firefox, Edge	Normal browsing mode, private browsing mode	URLs, bookmarks, cache, temporary files
Warren et al. (2018)	Live data forensics, forensic acquisition, and analysis, change monitoring	Process Monitor, FTK, IEF, X-Ways, Procmon	Browzar, Chrome, Firefox	Private browsing mode, normal browsing mode	Temporary internet files, cookies, websites, search keywords, downloaded images
Redha Mahlous and Mahlous (2020)	Live data forensics, forensic acquisition and analysis,	FTK, Autopsy, Regshot, IEF, WinHex	Brave	Private browsing mode	Images, videos, search keywords, emails, URLs
Prayudi and Rochmadi (2017)	Live data forensics	DumpIt, Votality Memory Forensics, WinHex	Internet Explorer Portable, Mozilla Firefox Portable, Google Chrome Portable, Browzar Black	Portable	Cookies, history URLs, timestamp, password

2.6 Significance of Research

Live memory technique was used from previous studies in [22], [21] and [7] to acquire more information from the volatile memory in the device. Two common web browser forensics for digital forensic investigation were used, Google Chrome and Mozilla Firefox to perform the browsing activities for the acquisition. The browsers used were consistent with previous studies, [1], [21] and

[22]. Hence, it is easy to do comparative analysis of the evidence left such as artefacts after browsing activities. Furthermore, the significance of this research is it focuses on two browsing modes, normal browsing mode and private browsing mode. The forensic tools used for acquisition and analysis were BelkaSoft RAM Capturer and Autopsy, respectively. FTK Imager was used for analysis, however due to lack of compatibility and forensic analysis tools, the Autopsy was replaced as it is more convenient and compatible than FTK Imager.

This research may benefit the digital forensic investigators to trace the artefacts from the devices using live memory acquisition as it can produce more valuable information than dead memory forensic. Moreover, all the artefacts found such as email, password, search terms, and website visited from this study are consistent with the previous study [21]. Hence, this study is reliable to be referred by digital forensic investigators to trace and identify the criminal activities from their browsing activities.

3. Methodology/Framework

The research process is a sequence of specific steps that should be followed to ensure the overall operation of the research matches the main objectives. Each step is related to other steps. The overall research process is shown in Figure 1.

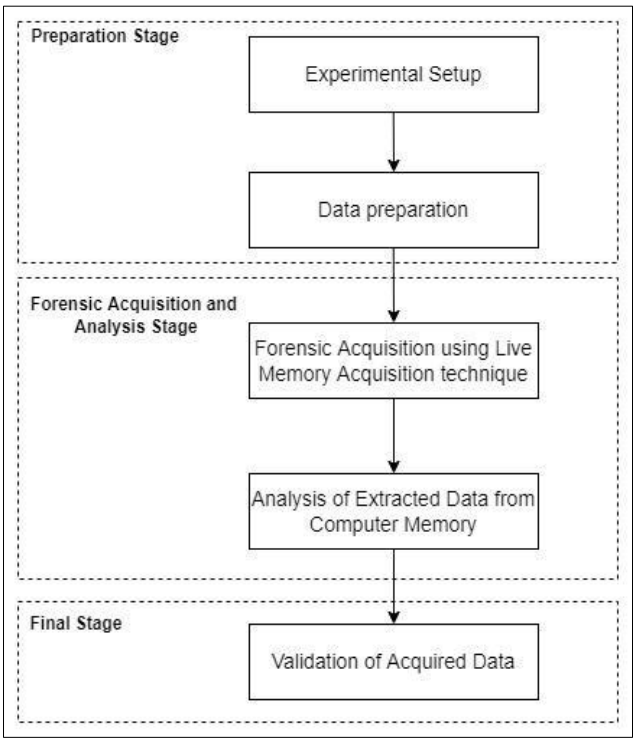

Figure 1: The research methodology

Figure 1 shows the three stages of methodology in this work, namely: (1) preparation stage, (2) forensic acquisition and analysis stage and (3) final stage. Each stage conducts different activities and must be followed in an orderly manner to acquire accurate data.

3.1 Preparation Stage

During the preparation stage, the experimental setup is carried out carefully as it could affect the validity of the results. Therefore, the experiment is conducted in a controlled experiment environment, as consistent with the previous study by [24]. It includes downloading and installing the related software and configuring the required hardware. Subsequently, the hardware and software are being examined to ensure they are working properly during the experimental setup [25].

All information that could be the potential sources of evidence for criminal activity, the source location is identified, labelled and collected before proceeding to the next stage, acquisition.

3.2 Forensic Acquisition and Analysis Stage

The primary purpose of the acquisition stage is to create a copy of the original evidence as a forensic backup from hard disk, CD ROM, and other devices to be presented in the court of law [26]. The advantage of the acquisition stage is that the potential evidence integrity and authenticity are assured if something happens to the copies. The forensic tool is used to perform acquisition on web browsers to acquire a real-time image from the disk to preserve the evidence from being tampered with as the data stored might change due to the live memory technique.

3.3 Analysis Stage

After acquiring forensic images of volatile memory, a forensic tool is used to retrieve and analyse the current and erased information that could be evidence from the operating system [27]. The analysis stage provides the information of activities performed during the running system and the artefacts left on the local drive after the browser installation. In addition, the tool examines the artefacts from internal storage to observe if there are artefacts left and the source of location.

Table 3 presents the forensic analysis plan once the actual experiment is conducted in the final analysis. The results are expected to be similar with Table 3. The browsing activities were adopted from a previous study [31], where it conducted an experiment of web browser abuse for drug stores. The experiment was related to email account username and password of Facebook, keywords and websites visited [31]. Furthermore, this study conducted a browsing activity based on keywords from a dataset from DFIR Training. The selected search term lists such as ‘asparagus’, ‘baby1001’, ‘shinsengumi’ and ‘shotacon’ from the dataset could reveal illicit results during the browsing activities. From the analysis, it is observed that the search term ‘shotacon’ revealed the explicit results from searching during media files downloaded activity.

Table 3: A forensic analysis plan

Type	Expected Findings
URL	www.youtube.com
Social Media	www.youtube.com
Search Engine	google.com
Search Terms (Chrome)	Baby1001, asparagus, shotacon mp3 download, shotacon mp4 download
Search Terms (Firefox)	Baby1001, asparagus, shotacon mp3 download, shotacon mp4 download
Account credentials	password, email

The results from the analysis stage are saved with the .mem extension [28]. Each artefact is stored in different folders depending on the type of browser.

3.4 Validation Stage

The residual data is validated by measuring its completeness by examining the artefacts coverage from the volatile memory in this stage. According to [29], which refers to the National Institute for Standards and Technology (2004), the completeness of artefacts is measured if all the data was acquired, and the accuracy is measured if the data was properly obtained. Hence, this study measured the completeness of residual data depending on the number of artefacts present during the analysis.

The findings of artefacts such as search terms, email and password from browsing activities are documented to record the artefacts found from analysis [17]. The documentation must also consider the hardware and software specifications, and all information that is relevant to the digital investigative process.

3.5 Hardware and Software Specifications

The specification of hardware and software used are stated in Table 4.

Table 4: Lists of hardware and software used

Hardware	Software
Aspire A315-55G Laptop with Processor Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz, 2112 MHz, 4 Core(s), 8 Logical Processor(s)	BelkaSoft RAM Capturer (for forensic acquisition) Autopsy Version 4.19.3 (for forensic analysis) Google Chrome Version 96.0.4664.45 Mozilla Firefox Version 72.0.2

4. Results and Discussion

The results and comparison obtained from the analysis of Google Chrome and Mozilla Firefox are presented in this section.

4.1 Experimental Setup

A series of controlled experiments on private and normal browsing modes using Google Chrome and Mozilla Firefox was designed to demonstrate the research objectives.

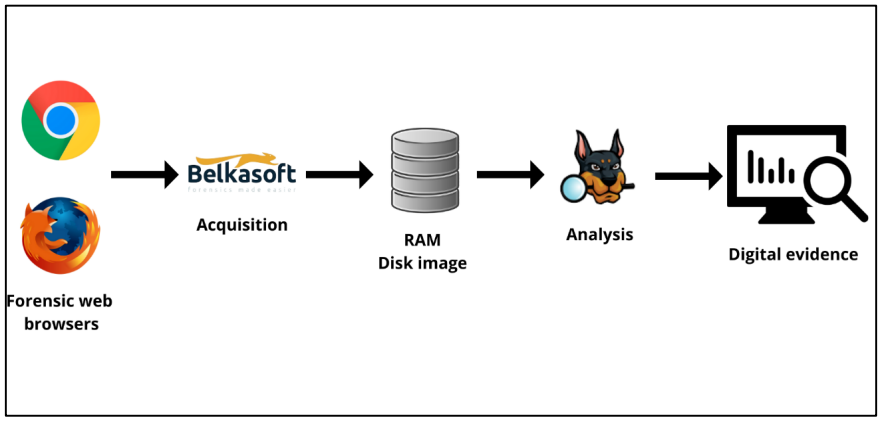

Figure 2: A summary diagram of simulation activities

Based on Figure 2, the simulation activities were conducted on web browsers in normal browsing and private browsing mode of Google Chrome and Mozilla Firefox. After the disk image was acquired, it was analysed using the Autopsy tool to find the artefacts that can be found from the artefacts for digital evidence such as passwords, email and websites visited.

Table 5 presents the details of the simulation activities conducted in the Chrome and Firefox browsers in normal and private browsing modes. There are six tasks performed in the study. Each task was performed in a different browser's tab. The first task was logging into a Google account using a student email and password. Then, the 'Baby1001' keyword was entered on the Google search bar, and the first website that appeared at the top of the search was clicked. Next, the 'asparagus' search term was entered on the new tab in Google Images. The chosen image was downloaded after choosing the location to save the file. Then, the 'shotacon mp3 download' keyword was entered to download the file that related to the keyword. The exact process was repeated for the keyword 'shotacon mp4 download'. Lastly, the first video that appeared at the top in the YouTube's search result for 'shinsengumi' keyword was viewed.

Table 5: Simulation activities

Simulation activities	
Task	Steps
Log in email	1. Go to https://accounts.google.com/ 2. Enter email and password using **ai190079@siswa.uthm.edu.my** as email and **_aina0406** as password.
Search keywords	1. Open a new browser tab 2. Search 'Baby1001' keyword on Google and click Images below the Search bar 3. Click the first link and roaming around the website
Download file (image)	1. Open a new tab 2. Search 'asparagus' then click Enter 3. Click Images, then choose one image of asparagus 4. Right-click mouse and choose 'Save Image as…' 5. Choose directory to download image
Download file (audio)	1. Open a new browser tab 2. Search 'shotacon mp3 download' then click Enter 3. Click the first link and download the file
Download file (video)	1. Open a new browser tab 2. Search 'shotacon mp4 download' then click Enter 3. Click the first link and download the file
Watch video	1. Open a new browser tab 2. Search youtube.com and press Enter 3. Insert 'shinsengumi' keyword in the search bar 4. Play the first video

4.2 Default Location of Web Browsers Artefacts

The browser's artefacts are stored inside of specific folders in the operating system. The location of each directory varies by browser, but the file formats remain the same. It is important to know where the files are stored to investigate them during normal browsing mode and private browsing mode. Table 6 shows the locations of the web browser artefacts such as history, caches and cookies in Google Chrome.

Table 6: Default locations of Chrome artefacts

Artefact	*Location within* C:\Users\User\AppData\Local\Google\Chrome\UserData\Default
History	…\History …\History-journal
Cookies	…\Cookies-journal …\Network\Cookies
Cache	…\Cache\Cache_Data

Table 7: Default locations of Firefox artefacts

Artefact	*Location within* C:\Users\User\AppData\Local\Mozilla\Firefox\Profiles\
Cookies	…\AppData\Roaming\Mozilla\Firefox\Profiles\1p8zafoy.default-release-1652627607782\cookies.sqlite
Cache	…\AppData\Local\Mozilla\Firefox\Profiles\1p8zafoy.default-release-1652627607782\cache2
History & Bookmarks	…\AppData\Roaming\Mozilla\Firefox\Profiles\1p8zafoy.default-release-1652627607782\places.sqlite

Table 7 presents the common location of the Firefox artefacts that can be found and located, such as cookies, cache, history, and bookmarks. All the changes in Firefox, such as bookmarks, extensions installed and saved passwords, are stored in the Profiles folder. As shown in the table, the path shows that the cookies are saved in the cookies.sqlite meanwhile, the cache files are located in the cache2 folder. All the bookmarks downloaded files and browsing history are stored in places.sqlite.

4.3 Analysis of the artefacts in Google Chrome Browsing Modes

The artefacts from browsing activities such as email Id, password, search terms and website visits discovered in the memory from both normal browsing and private browsing mode from Google Chrome on Autopsy tool.

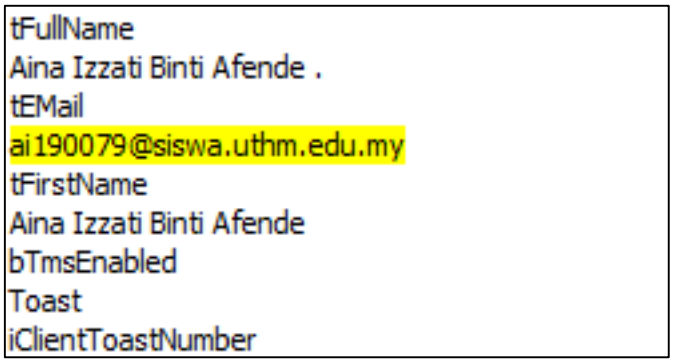

Figure 3: Artefact found for email used

Figure 3 shows the artefact found for email used for browsing activities to access the Google services. It also reveals the full name of the email user.

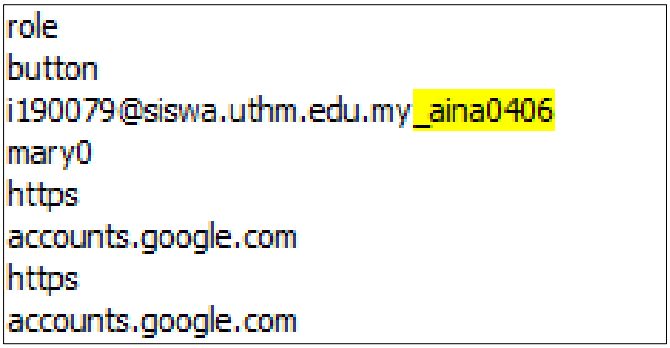

Figure 4: Artefact found for email password

Based on Figure 4, it is observed that the email password entered during the login is revealed in Autopsy. Furthermore, the website visited to login, “accounts.google.com” was also revealed.

4.4 Comparison of Google Chrome in Two Browsing Modes

Table 8 summarizes the results of evidence of interest from Google Chrome. From the analysis, history of URLs, email Id, and keyword search terms can be found in both clear and unclear history. The passwords used to log into Google email, on the other hand, can only be found before history is cleared. The account used for accessing Google email is “ai190079@siswa.uthm.edu.my", and the password is “_aina0406”. The following browser-related entries were found with the help of a keyword string search function on Autopsy: (1) email Id, (2) downloaded files, (3) keyword search terms, (4) websites, and (5) password with some content of the YouTube and details of ‘asparagus’ keyword search.

Table 8: Number of entries of simulation activities found on Google Chrome between normal browsing and private browsing mode

Keywords/ Simulation Activities	Normal mode		Private mode
	Chrome (Unclear)	Chrome (Cleared)	
ai190079@siswa.uthm.edu.my	70	75	106
Email password "_aina0406"	1	0	1
Search term "Baby1001"	318	109	235
Search term "asparagus"	>500	>500	>500
Downloaded image File (path)	9	6	17
Downloaded audio File (path)	75	44	8
Downloaded video File (path)	94	77	60
Search term "shotacon mp3 download"	103	26	29
Search term "shotacon mp4 download"	216	27	25
www.youtube.com	>500	>500	>500
Total artefacts	1886	1338	1481

4.5 Analysis of the Artefacts in Mozilla Firefox Browsing Modes

A number of browser artefacts were found in the RAM from Mozilla Firefox. This indicates that it is likely to find artefacts left in RAM in both normal browsing and private browsing mode even though the browsing activities were conducted in private browsing mode. Figure 5 presents the results from Firefox browsing modes that are found during the analysis.

Figure 5: Artefact found for email used

The analysis revealed the full name of the email user, and new tab indicator where the new tab was opened during the experiment.

Figure 6: Artefact found for password email

It is observed that the Firefox returned hits for the email password "_aina0406" in both normal browsing and private browsing mode in Figure 6. The email used is shown which is denoted as identifier.

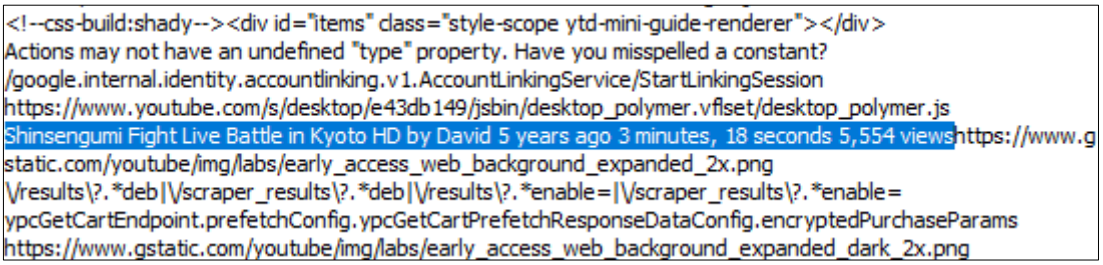

Figure 7: Artefact found for the video watched in YouTube

Figure 7 shows the details of the watched video YouTube in Firefox. The key details are the video title, video duration and the total views are revealed during the analysis.

4.6 Comparison of Mozilla Firefox in Two Browsing Modes

The results obtained from the Mozilla Firefox analysis are summarised in Table 9. It can be observed from the table that the data compare the artefacts found before and after the history cleared in normal browsing and private browsing mode.

Table 9: Number of entries of simulation activities found on Mozilla Firefox between normal browsing and private browsing mode

Keywords/ Simulation Activities	Normal mode		Private mode
	Firefox (U)	Firefox (C)	
ai190079@siswa.uthm.edu.my	82	62	88
Email password "_aina0406"	8	1	8
Search term "Baby1001"	76	30	51
Search term "asparagus"	>500	>500	>500
Downloaded image file	78	109	12
Downloaded audio file	81	139	9
Downloaded video file	26	13	18
Search term "shotacon mp3 download"	8	8	13
Search term "shotacon mp4 download"	22	4	15
www.youtube.com	>500	>500	>500
Total artefacts	1381	1366	1214

Table 9 presents an overview of artefacts found in normal browsing and private browsing mode during live memory acquisition. First, the email Id artefact found in the memory dump of private mood has more entries than normal browsing mode, before and after history cleared. This result is counterintuitive as the private browser was not closed during the live memory acquisition. This may result in the more significant artefacts of email Id found in memory. Nevertheless, it did store the password in the memory as the number of entries in private mode is the same as unclear history in normal browsing but lesser after clearing the history. Next, the search term "Baby1001" in private mode hits less than history uncleared but more than history cleared. It could be seen that the word search "Baby1001" found in Firefox is the same as Google Chrome analysis, which is more than 500. It is shown that the artefacts are remain inside the RAM after the browsing activities in private mode and the history cleared in normal browsing mode.

4.7 Comparison of Google Chrome and Mozilla Firefox in Two Modes

The analysis results in this study on user browsing activities details can be seen in Table 10 after some simulations and analysis conducted.

Table 10: Summary of the overall findings

Residual data	Google Chrome				Mozilla Firefox			
	Normal		Private		Normal		Private	
	(U)	(C)	(U)	(C)	(U)	(C)	(U)	(C)
Email Id	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Password	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
Search terms	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Downloaded file (jpg, mp3, mp4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
URLs	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 10 summarises the artefacts that can be found in RAM after the history was cleared in normal browsing mode and private browsing mode. The type of residual data from private and normal browsing modes are discovered, which are: (1) email Id, (2) password, (3) search terms, (4) download file and (4) URL of the web visited. These findings are consistent with a previous study [21]. According to the study, the different types of artefacts such as email IDs, photos and videos, including websites visited, can be retrieved from the RAM from private browsing mode. The digital forensic investigator is able to trace the illegal activities of the suspect from their browsing activities.

In addition, it can be observed that Chrome and Firefox are able to retrieve different data artefacts from the analysis performed. As shown in Table 8 and Table 9, private browsing mode (Chrome browser) retrieves more data from the browsing activities than private browsing mode (Firefox browser), such as emails, password, and websites visited. These findings are nearly similar with a previous study [32] where the browsing activities were acquired before and after closing the browsing session in Windows 10 and MacOS. The artefacts found are the web visited, search term, downloaded files, email Id and password. It would benefit the digital forensic investigator as these findings conclude that the Chrome browser leaves more artefacts such as user browsing history than Firefox from memory while in private browsing mode. Other than that, for normal browsing mode, the data from RAM before the history cleared in Chrome presents more than Firefox when the history cleared. However, after the history cleared, Chrome presented less than Firefox. The results show that Chrome presents consistent data extraction, which shows that Chrome leaves more artefacts than Firefox during the browsing sessions.

It is observed that each browser has different artefacts stored on the device's RAM. The normal browsing mode stores the user browsing history details before and after history are cleared in memory. Surprisingly, the private browser on Chrome and Firefox consists of little residual data that are able to provide evidence of interests such as search keywords, email Id and password. Nevertheless, the Firefox browser presents more residual data than the Chrome browser. In the context of completeness, Firefox presents more residual data than Chrome.

The residual data found in Chrome private browsing mode had less information than in Firefox private browsing mode. The results are different from a previous study [1]. The results are slightly different; it might be due to different techniques used in which dead forensics was used in Fayyad's paper, but live memory acquisition was used in this study. The results from the previous paper showed that Chrome is more private than Firefox in private browsing mode as the browsing activities were conducted on a virtual machine.

It is revealed that normal browsing mode (clear history) for Chrome presents fewer residual data than normal browsing mode (clear history) for Firefox. The results show that it is possible to retrieve artefacts from browsing activities such email Id, password, search terms, and website visited even after the browser is cleared history. This study results are consistent with the results from previous paper

[31], where the artefacts were discovered on private browsing mode and normal browsing mode (after history is cleared) using live forensics method with DumpIt tool. These results conclude that normal browsing mode of Chrome after history is cleared presents less residual data than normal browsing mode in Firefox (after history is cleared).

Lastly, for unclear history mode, the normal browsing mode in Chrome presents more artefacts than the normal browsing mode in Firefox. Therefore, it can be concluded that the metadata in Chrome such as the search term "shotacon mp4 download" and download file (mp4), was present more than in Firefox during the experiment. It also observed that the different number of metadata presents because Chrome stored artefacts in relation to media more than Firefox in volatile memory. These findings seem to be consistent with that study [32] whose findings for Chrome artefacts presents more than Chrome in Windows 10. Hence, it is concluded that Chrome presents more artefacts than Firefox in normal browsing mode (unclear history).

5. Conclusion

In conclusion, a study for comparative analysis of residual data between private browsing and normal browsing mode using live memory acquisition has achieved its objectives for research development.

Firstly, the type of residual data that were able to be extracted from this study are (1) email Id, (2) password, (3) search terms, (4) downloaded files and (5) links of web visits using Autopsy. Secondly, the comparison of data extraction between private and normal browsers from Chrome and Firefox is analysed using the Autopsy tool. The results are divided into three categories, (1) Private browsing mode, (2) Normal browsing (Unclear history) and (3) normal browsing (Clear history). For private browsing mode, Chrome extracted more residual data such as email Id, password, keyword searches and other artefacts than Firefox.

Meanwhile, for normal browsing mode (unclear history), Chrome extracted fewer residual data compared to Firefox. Then, Chrome extracted less residual data than Firefox in browsing mode after the history cleared. Lastly, the Firefox browser presents complete residual data compared to Chrome. Overall, it can be concluded that this research may help other researchers to utilize the significance of RAM forensics for digital forensic investigation and can be very useful, especially to find the potential evidence for browsing activities in physical memory.

Acknowledgment

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia for its support and encouragement throughout the process of conducting this research.

References

[1] F.-K. Hasan, K.-M. Sondos, H. Hussin J, and H. Ale J, "Forensic analysis of private browsing mechanisms: Tracing internet activities," J. Forensic Sci. Res., vol. 5, no. 1, pp. 012–019, 2021, doi: 10.29328/journal.jfsr.1001022.

[2] Y. Wu, P. Gupta, M. Wei, Y. Acar, S. Fahl, and B. Ur, "Your secrets are safe: How browsers' explanations impact misconceptions about private browsing mode," *Web Conf. 2018 - Proc. World Wide Web Conf. WWW 2018*, pp. 217–226, Apr. 2018, doi: 10.1145/3178876.3186088.

[3] EC-Council, "What is Digital Forensics | Phases of Digital Forensics | EC-Council," 2021. https://www.eccouncil.org/what-is-digital-forensics/ (accessed Nov. 09, 2021).

[4] A. A. Khan, M. Uddin, A. A. Shaikh, A. A. Laghari, and A. E. Rajput, "MF-ledger: blockchain hyperledger sawtooth-enabled novel and secure multimedia chain of custody forensic investigation architecture," *IEEE Access*, vol. 9, pp. 103637–103650, 2021.

[5] A. Dimitriadis, N. Ivezic, B. Kulvatunyou, and I. Mavridis, "D4I-Digital forensics framework for reviewing and investigating cyber attacks," *Array*, vol. 5, p. 100015, 2020.

[6] N. Sridhar, D. D. L. Bhaskari, and D. P. S. Avadhani, "18: Plethora of Cyber Forensics," *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 11, 2011, doi: 10.14569/ijacsa.2011.021118.

[7] Y. Prayudi and T. Rochmadi, "Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser," 2017. [Online]. Available: https://www.researchgate.net/publication/316172830.

[8] R. Umar, I. Riadi, and R. S. Kusuma, "Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method," *IJID (International J. Informatics Dev.*, vol. 10, no. 1, pp. 53–61, 2021, doi: 10.14421/ijid.2021.2423.

[9] N. Mistry and M. S. Dahiya, "VolNet: a framework for analysing network-based artefacts from volatile memory," *Int. J. Electron. Secur. Digit. Forensics*, vol. 9, no. 2, p. 101, 2017, doi: 10.1504/ijesdf.2017.10004409.

[10] M. Kolhe and P. Ahirao, "Live Vs Dead Computer Forensic Image Acquisition," Int. J. Comput. Sci. Inf. Technol., vol. 8, no. 3, pp. 455–457, 2017.

[11] R. Chopade and V. K. Pachghare, "Ten years of critical review on database forensics research," *Digit. Investig.*, vol. 29, pp. 180–197, 2019, doi: https://doi.org/10.1016/j.diin.2019.04.001.

[12] M. P. Gupta, "Capturing Ephemeral Evidence Using Live Forensics," IOSR J. Electron. Commun. Eng., pp. 109–113, Nov. 2013, [Online]. Available: www.iosrjournals.org.

[13] K. Simon, "Digital 2019: Global Internet Use Accelerates," We Are Social Singapore, 2019. https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates (accessed Nov. 09, 2021).

[14] Mozilla, "What is a Web Script?," 2014. https://www.mozilla.org/en-US/firefox/browsers/what-is-a-browser/ (accessed Nov. 09, 2021).

[15] A. Rasool and Z. Jalil, "A Review of Web Browser Forensic Analysis Tools and Techniques," *Res. J. Comput.*, vol. 1, no. 1, pp. 15–21, 2020, doi: 10.1111/RpJC.2020.DOI.

[16] H. Habib et al., "Away From Prying Eyes: Analyzing Usage and Understanding of Private Browsing," pp. 159–175, Aug. 2018, [Online]. Available: https://www.mturk.com/.

[17] M. R. Jadhav and B. B. Meshram, "Web Browser Forensics for Detecting User Activities," *Int. Res. J. Eng. Technol.*, vol. 5, no. 7, pp. 273–279, 2018.

[18] H. Adamu, A. Ahmad Adamu, A. Adamu Ahmad, A. Hassan, and A. Barau Gambasha, "Web Browser Forensic Tools: Autopsy, BHE and NetAnalysis," *Int. J. Res. Sci. Innov.*, 2021, Accessed: Nov. 10, 2021. [Online]. Available: www.rsisinternational.org.

[19] T. Z. Khairallah and J. Amman, "Cloud drives forensic artifacts," A Google Drive Case, vol. 1, no. January, pp. 2–5, Jan. 2019, doi: 10.20944/preprints201812.0345.v1.

[20] Lexology, "Admissibility of digital evidence in court - Commentary - Lexology," 2019. https://www.lexology.com/commentary/litigation/cyprus/elias-neocleous-co-llc/admissibility-of-digital-evidence-in-court#Admissibility of evidence (accessed Dec. 13, 2021).

[21] A. Redha Mahlous and H. Mahlous, "Private Browsing Forensic Analysis: A Case Study of Privacy Preservation in the Brave Browser," *Int. J. Intell. Eng. Syst.*, vol. 13, no. 6, 2020, doi: 10.22266/ijies2020.1231.26.

[22] C. Warren, E. El-Sheikh, and N. A. Le-Khac, "Privacy Preserving Internet browsers: Forensic analysis of Browzar," Comput. Netw. Secur. Essentials, Oct. 2017, doi: 10.1007/978-3-319-58424-9_21.

[23] A. V. Hussein Al-Saadawi, "Volatile Memory Analysis Tools for Voip Forensic Applications: a Classification Study," 2017, [Online]. Available:

https://www.academia.edu/38033121/VOLATILE_MEMORY_ANALYSIS_TOOLS_FOR_VOIP_FORENSIC_APPLICATIONS_A_CLASSIFICATION_STUDY.

[24] N. D. W. Cahyani, N. H. A. Rahman, W. B. Glisson, and K. K. R. Choo, "The Role of Mobile Forensics in Terrorism Investigations Involving the Use of Cloud Storage Service and Communication Apps," *Mob. Networks Appl.*, vol. 22, no. 2, pp. 240–254, Apr. 2017, doi: 10.1007/s11036-016-0791-8.

[25] O. L. Carroll and S. K. Brannon, "Computer Forensics: Digital Forensic Analysis Methodology," January 2008 United States Atty. Bull., vol. 1, no. 1, pp. 1–9, 2017, Accessed: Nov. 28, 2021. [Online]. Available: https://www.crime-scene-investigator.net/computer-forensics-digital-forensic-analysis-methodology.html.

[26] E. Akbal and S. Dogan, "Forensics Image Acquisition Process of Digital Evidence," *Int. J. Comput. Netw. Inf. Secur.*, vol. 10, no. 5, pp. 1–8, May 2018, doi: 10.5815/ijcnis.2018.05.01.

[27] B. Popović, K. Kuk, and A. Kovačević, "Comprehensive forensic examination with Belkasoft evidence center," *Int. Sci. Conf. "Archibald Reiss Days", Belgrade, 2-3 Oct. 2018. Vol. 2*, pp. 419–433, 2018, Accessed: Nov. 28, 2021. [Online]. Available: http://jakov.kpu.edu.rs/handle/123456789/921.

[28] T. Pandela and I. Riadi, "Browser Forensics on Web-based Tiktok Applications," Int. J. Comput. Appl., vol. 175, no. 34, pp. 47–52, 2020, doi: 10.5120/ijca2020920897.

[29] J. Dykstra and A. T. Sherman, "Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform," *Proc. Digit. Forensic Res. Conf. DFRWS 2013 USA*, vol. 10, pp. S87–S95, 2013, doi: 10.1016/j.diin.2013.06.010.

[30] Johan Moreno. (2021), *Alphabet CEO Ordered To Testify About Private Browsing Confusion On Google Chrome*. Forbes. . [Online]. Available: https://www.forbes.com/sites/johanmoreno/2021/12/31/alphabet-ceo-ordered-to-testify-about-private-browsing-confusion-on-google-chrome/?sh=2c7e594d5373

[31] R. Umar, A. Yudhana, and M. N. Faiz, "Experimental analysis of web browser sessions using live forensics method," Int. J. Electr. Comput. Eng., vol. 8, no. 5, pp. 2951–2958, 2018, doi: 10.11591/ijece.v8i5.pp.2951-2958.

[32] R. Sanghkroo, R. Deepak, G. Rao, and K. Raychaudhuri, "Forensic Study and Analysis of Different Artifacts of Web Browsers in Private Browsing Mode," 2020, Accessed: Dec. 18, 2021. [Online]. Available: http://ijasret.com/VolumeArticles/FullTextPDF/461_7FORENSIC_STUDY_AND_ANALYSIS_OF_DIFFERENT_ARTIFACTS_OF_WEB_BROWSERS_IN_PRIVATE.pdf.