International Journal of Digital Crime and Forensics
Volume 16 • Issue 1 • January-December 2024

Examining the Behavior of Web Browsers Using Popular Forensic Tools

Areej Muqbil Alotibi
Naif Arab University for Security Sciences, Saudi Arabia

Salem Yahya Altaleedi
Naif Arab University for Security Sciences, Saudi Arabia

Tanveer Zia
https://orcid.org/0000-0003-3802-5687
Naif Arab University for Security Sciences, Saudi Arabia

Emad Ul Haq Qazi
https://orcid.org/0000-0003-1448-3632
Naif Arab University for Security Sciences, Saudi Arabia

ABSTRACT

Mobile phones and computers are widely used devices these days, with almost everyone carrying a smartphone and multiple personal computing devices at their homes. Unfortunately, the perpetrator exploits these devices for their unlawful activities. They employ various tactics such as sending phishing emails, and malicious links to harvest confidential information and exploit users. The perpetrators often leave traces on search engines, where they search for illegal materials and weapons, or send threatening emails to victims. This paper primarily focuses on locating and retrieving browsers' artifacts while considering the challenges posed by private browsing modes, which perpetrator may use to cover their tracks. The study also compares well-known search engines like Edge, Safari, and Firefox, analyzing the strengths and weaknesses of their directories. Moreover, it explores evidence extraction from smartphones, comparing the success rates between rooted or jailbroken phones and evidence obtained from browsers versus applications.

KEYWORDS

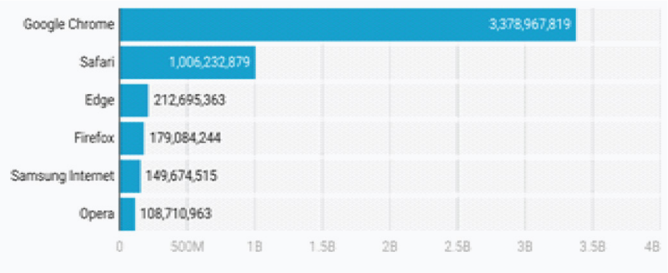
Browser Artifacts, Browser Normal Mode Analysis, Digital Investigations, Edge Analysis, Firefox Analysis, Safari Analysis, Web Browsers Forensics

Web browsers enable users to explore the internet and navigate various websites and web pages by establishing communication with web servers. These browsers store a significant amount of information, including usernames, passwords, web history, and temporary internet files. As a result, ensuring web browser security has always been a key objective for providers, as it is a crucial aspect of any online service. Understandably, users are constantly seeking the most effective tools to protect their data, creating an ongoing and evolving process of updates and patches to enhance and address any vulnerabilities in browsers. Currently, most web browsers offer different modes, such as the regular/normal browsing mode and the private/incognito mode, to enhance user privacy. The concept of private mode refers to a browsing mode in which no record of visited websites is retained.

This endeavor to provide a secure environment for everyone is commendable. However, like any other technology, web browsers can be misused as tools for committing cybercrimes. Criminals also exploit browsers and private modes to carry out illicit activities and conceal their actions. It is important

DOI: 10.4018/IJDCF.349218

Figure 1. Browser statistics



to note that these privacy features, such as private/incognito mode, present technical challenges for digital forensics investigators when attempting to recover evidence in cases involving criminals who utilize private browsing [20, 21]]. Furthermore, criminals constantly employ various methods to hide their activities while using private mode, including deleting or modifying their online actions.

Previous research in web browser forensics has often overlooked the variable effectiveness of forensic tools across different browser types and modes. This study addresses these gaps by providing a comprehensive analysis of how various tools perform across multiple browsers, shedding light on previously unexplored facets of browser forensics. This study's objective is to establish a standardized methodology for examining and verifying the claimed level of privacy provided by different browser vendors. Additionally, it aims to determine the extent to which forensic investigations can uncover relevant evidence artifacts of evidentiary importance.

METHODOLOGY

The methodology employed in this research is meticulously designed to systematically evaluate the forensic capabilities of selected web browsers. This involves the use of standard forensic tools to analyze browser artifacts under controlled conditions. The selection of browsers and tools is based on their prevalence in the industry and relevance to forensic investigations, ensuring that the findings are applicable to real-world scenarios.

Selection of Web Browsers

In this study, we selected three popular web browsers: Mozilla Firefox [1], Safari, and Microsoft Edge. These browsers were chosen due to their significant market share and frequent usage across various platforms. Google Chrome has already been thoroughly examined in normal and incognito modes [19]. Figure 1 shows the statistics about the browsers.

According to Firefox statistics for 2022, the browser has approximately 362 million users worldwide. Apple's Safari [2] is regarded as the safest browser, with only 26 vulnerabilities discovered in 2022. Microsoft Edge is Microsoft's recommended web browser and the default web browser for Windows; Windows supports web-platform-based applications.

Forensic Tools

To analyze the behavior of web browsers, we utilized industry-standard forensic tools, including Autopsy, AXIOM, and XRY. These tools enable the extraction and analysis of browser artifacts, allowing for a comprehensive investigation. We employed Autopsy for in-depth examination of computer images, supporting functionalities like keyword search, hash matching, and registry analysis. AXIOM was utilized for its superior capabilities in uncovering challenging digital evidence and integrating data from different sources into a single case file. Additionally, XRY was chosen for its

Table 1. Lab configuration

Software	Version	Description
VMware Workstation	17	To provide virtual environment for the experiment
Windows 10	10 64-bit	The operating system used on the computer
Firefox Browser	109.0	The browser under testing
Microsoft Edge Browser	113.0	The browser under testing
FTK Imager	4.7	To capture a forensic image of computer system
Autopsy Forensics	4.20	To analyze the computer images
DB Browser (SQLite)		To read the SQ databases files
DCode	5	To convert the time zones
Notepad		To read the extracted text files
JSON reader		To read JSON files
Windows 10	10 64-bit	The operating system used to install the tools
Magnet AXIOM Examine	6	To analysis the images
XAMN	6.2.0	To analysis the images
XRY	9.6.0	To image the device
Magnet AXIOM process	6.10.0	To image the device
Magnet ACQUIRE	2.26.0	To image the device
Checkra1n	Beta 0.12.4	To jailbreak the iPhone
Cable USP iPhone		To connect the iPhone to computer
Cable type C USP Samsung		To connect the Nokia to computer

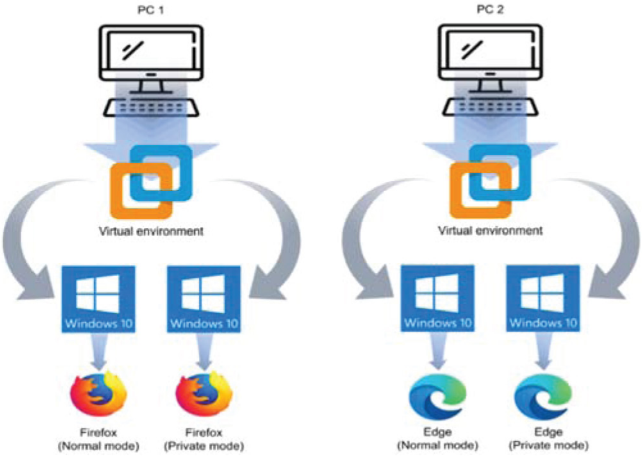
effectiveness in extracting a large volume of data from mobile devices while maintaining the integrity of the evidence. These tools were pivotal in allowing us to capture and analyze crucial browser artifacts from both computers and mobile devices.

Autopsy [3] is a free, open-source desktop digital forensics tool for Windows that includes all of the capabilities found in commercial digital forensics products. It is extendable and includes capabilities such as keyword search, hash matching, registry analysis, web analytics, and others. AXIOM [4] is used by digital forensics professionals to search for evidence that other tools cannot locate, to validate data, and to analysis images gathered with other tools into a single case file for review. AXIOM goes beyond Magnet IEF's excellent search and carving capabilities. XRY [5] is a strong, user-friendly, and efficient mobile data recovery program for the Windows operating system. It is capable of securely and efficiently extracting large volume of data, while always retaining the evidence's integrity. Table 1 shows the lab configuration.

Lab Configuration

A VMware workstation was utilized to establish a secure and isolated virtual environment, ensuring the integrity of the experiments. Both Firefox and Edge browsers were chosen for testing due to their popularity and the availability of both normal and private browsing modes. Autopsy, an open-source graphical interface tool, which offers the capability to investigate and analyze operating systems like Windows, was installed.

Figure 2. Virtual environments for the computer-side experiment



VM Configuration

We installed the VMware workstation in order to create a convenient and manageable setup in the computer side of the study. This virtualization software allowed us to establish four separate virtual machines, each running a Windows 10 environment. One of the advantages of this setup is that it provides isolation for each virtual machine, ensuring that any changes or issues in one machine do not affect the others. Unlike the actual PC environment, the data volume within these virtual machines is more manageable. Additionally, we have the capability to easily capture the virtual hard drive and the RAM dump files. Additionally, we created a real-life scenario in which we examined common social networking sites, email platforms, and instant messaging programs. The circumstances of the scenario were designed in such a way that the perpetrator's actions occur while browsing on both a computer and a mobile device. The perpetrator in this case engages in various malicious activities, such as sending threatening text messages and pictures of weapons to the victims, motivated by a desire for revenge. The perpetrator employs fake and sometimes real identities on social networking sites, making it relatively easy to identify them. However, it is essential to conduct a digital forensic investigation on the devices the perpetrator used during the attack to establish the validity of the accusations and determine if any cases have been reported against an unknown individual linked to the incidents. Figure 2 shows the details of virtual environments for the computer-side experiment.

It is worth noting that these realistic scenarios are not mere fabrications but are based on occurrences that happen on daily basis. By simulating such situations, we provide guidance to future investigators in an engaging way.

To recreate the scenario, we selected Windows 10, and the most popular devices, including Android and iOS mobile phones, as well as widely used browsers such as Firefox, Safari, and Edge. Additionally, we incorporated the most popular social networking sites – Google, YouTube, Facebook, Twitter, Gmail, Outlook [6], and Hotmail.

Data Population

To execute the previously mentioned scenario, we had to generate authentic data in real-world settings. This led us to engage in the process of data population. To simulate the crime scenario accurately, we had to create accounts on various websites and carry out distinct browsing actions. The actions listed below were performed as part of this simulation.

Table 2. Credential data

Website	Username	Password
Gmail	shaker88sh8@gmail.com	Shaker8*****
Facebook	Shadialishaker88sh8@gmail.com	Shaker1****
YouTube	shaker88sh8@gmail.com	Shaker88****
Twitter	Sh818sh	Xoxo12***
Hotmail	Shk333shk@hotmail.com	Shk1****
Outlook	sh111888shk@outlook.sa	AB*****
WhatsApp	053626****	----

Utilizing Google, Facebook, Twitter, and YouTube for conducting searches

- Employing diverse keywords during the search process
- Removing certain search results from browsing history
- Establishing bookmarks
- Removing bookmarks

Employing Social Media Platforms such as Facebook and Twitter

- Generating login credentials
- Utilizing the private chat option for sending and removing text messages
- Sending and deleting attachment files

Utilizing Instant Messaging Services like Facebook Messenger and WhatsApp

- Utilizing the messaging service to send and remove text messages
- Using the messaging service for sending and deleting attachment files

Utilizing Email Services such as Gmail, Outlook, and Hotmail

- Establishing login credentials
- Sending and deleting emails

This table describes the accounts created in different websites as part of the data population process. Table 2 shows the credential data.

Browser Artifacts

Table 3 lists the types of artifacts created within the browsers.

Email Data Population Content

Data created during the emails is shown in Table 4. Artifacts in red font indicate the data is deleted.

Table 3. Browser artifacts

Website	History	Bookmarks	Cookies		Caches	Search	Attachment files	Emails
Google	*	*	*	*	*	*	*	*
YouTube	*	*	*	*	*	*		
Facebook	*	*	*	*	*	*	*	
Twitter	*	*	*	*	*	*	*	
Outlook	*		*	*	*		*	*
Hotmail	*		*	*	*		*	*
WhatsApp	*		*		*		*	

Table 4. Email data population content

Email service	Subject title	Text content	Attachment
Gmail	Mail01SMail02S	I got your personal information gmailtext01this is your house location, right? gmailtext02	gimg01gimg02
Hotmail	Mail3SMail4S	hmailtext01hmailtext02	himg01himg02
Outlook	Mail5SMail6S	outmailtext01outmailtext02	oimg01oimg02

Table 5. Website data population content

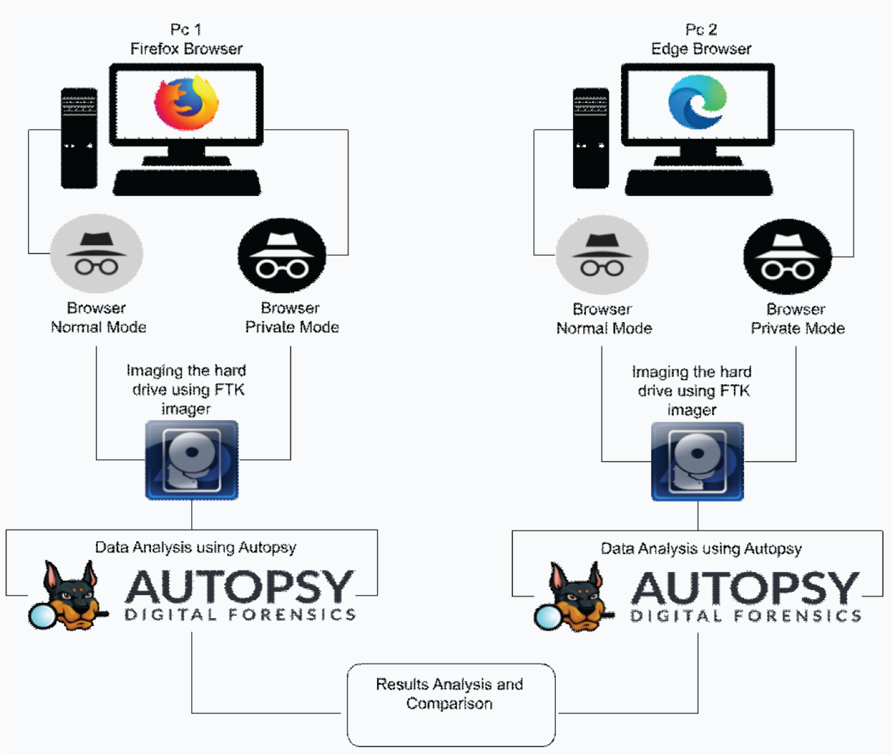
Website	Search-Term	Message Content	Bookmark	Attachment
Google	How to buy a weapon stext01Pistol for sale stext02Gun silencer for Sale stext03		SA01SA02	
YouTube	(Arsenic poison stext04How to use a silencer on a gun stext05Activate WhatsApp with a fake number stext06		YU01YU02	
Facebook / (Facebook Messenger)	Noora IbrahimIbrahim Ezz El-DinAnna Ibrahim	- are you ready? Did you say goodbye to your family?-I know where you live	FC01FC02	fcimg1fcimg2
Twitter	Sarah IbrahimFahad SaadMuhannad Ahmed	- Hi Sarah, I know where you live- I am close to your house, Noura	TW01TW02	timg1timg2
WhatsApp		- I saw your tweets- If something happens to your daughters, that's on you		wimg1wimg2

Website Data Population Content

Table 5 provides the actual data generated with the browsers. Artifacts in red font indicate the data is deleted.

Our next step involved generating artifacts within web browsers and then acquiring forensic images from computers and smartphones. The images were prepared for analysis using specific tools like Autopsy for computer images, Magnet Axiom for iPhone, and XRY for Android smartphones. The objective of the study was to examine user-created artifacts within web browsers and determine if these artifacts can be captured successfully and located using the chosen forensic tools. The study also aimed to conduct a detailed comparison of the results obtained from each tool.

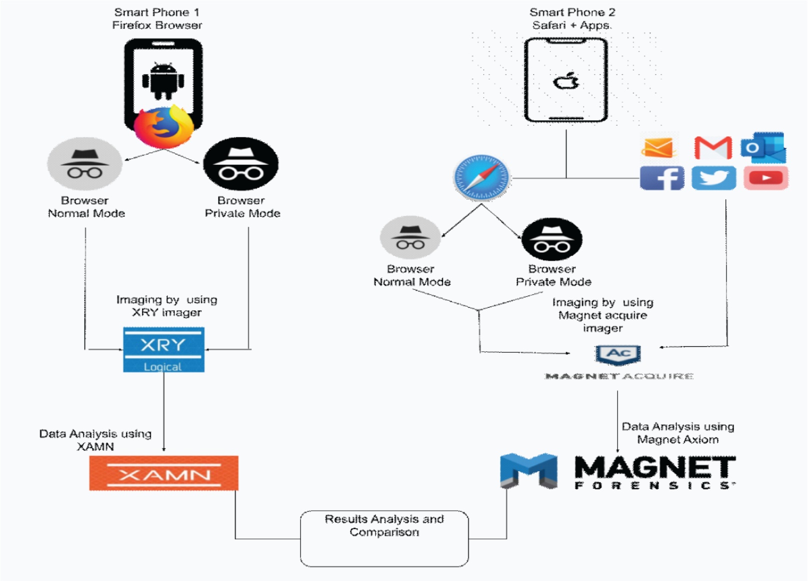
Figure 3. Imaging and data analysis in computers


Pc 1
Firefox Browser
Pc 2
Edge Browser
Browser
Normal Mode
Browser
Private Mode
Browser
Normal Mode
Browser
Private Mode
Imaging the hard drive using FTK imager
Imaging the hard drive using FTK imager
Data Analysis using Autopsy
AUTOPSY
DIGITAL FORENSICS
Data Analysis using Autopsy
AUTOPSY
DIGITAL FORENSICS
Results Analysis and Comparison

Imaging and Data Analysis

The acquisition phase in digital forensics involves recording the current state of a digital system for later evaluation. This phase aims to preserve all digital values, similar to preserving physical evidence. In our study, we focused on generating forensic images from computers and smartphones. We used a computer running Windows 10 with Firefox and Edge browsers, an iPhone running iOS, and a Nokia device running Android. For image capturing, we utilized tools like FTK Imager for computers, Magnet Acquire for iOS, and XRY for Android. In the computer aspect of our study, we employed two separate computers running Firefox and Edge browsers in normal and private modes. We created images of the hard drives using FTK Imager and analyzed them with Autopsy. The browsing behavior was examined, and the results were compared. For smartphones, we used Android with Firefox in private and normal modes. We captured logical images using XRY and analyzed them with XMAN. On the iPhone, we studied the Safari browser in both private and normal modes. We created a Quick image using Magnet Equation and analyzed it with Magnet Axiom Forensic. During the comparison, we encountered an inaccessible artifact, which required downloading third-party applications and performing a jailbreak on the iPhone. We then created a full file system image using Magnet Axiom and analyzed it to obtain the results. The findings of our study highlight the importance of image acquisition and analysis in digital forensics. By employing specialized tools and conducting thorough examinations of artifacts within web browsers, we were able to capture and analyze crucial evidence. The comparative analysis provided insights into the similarities and differences between the various platforms and browsers, contributing to the overall understanding of digital forensic investigations. Figures 3 and 4 show the details about imaging and data analysis in computers and mobile devices, respectively.

Figure 4. Imaging and data analysis in mobile devices



RESULTS

Results of the Browser Analysis of the Computer

The browser analysis of the computer is presented in Table 6.

Results of the Browser Analysis of Smartphones

The results of the browser analysis of the smartphones are presented in Table 7.

ANALYSIS AND DISCUSSION

The analysis and results clearly demonstrate the pivotal role of this research in advancing the capabilities of digital forensic investigations. By dissecting the performance of different forensic tools in various scenarios, our work lays the groundwork for future innovations in forensic methodologies, especially in tackling the complexities introduced by private browsing modes. This section is divided into two parts, discussing the findings from computer and smartphone analysis separately.

Computer Analysis

Edge Browser Analysis

User logins, including usernames and encrypted passwords, are stored in a sqlite3 file in the logins table. The file is located at /Users/[username]/AppData/Local/Microsoft/Edge/User Data/Default/Login Data in the Edge browser. Usernames are readable, while passwords are encrypted. Table 8 shows the results of the browser analysis of smartphones. Figure 5 shows the details about the login data on Autopsy (Edge browser-normal mode).

The login data file can be extracted from Autopsy and opened using DB Browser (SQLite) for further analysis. The table contains valuable information such as usernames, URLs of login sites (Google, Facebook, Twitter), login date creation, last usage, and password modification timestamps.

Table 6. Results of browser analysis of the computer

Services	Activities		Normal Mode		Private Mode	
			Firefox	Edge	Firefox	Edge
Google	1	Logging in	*	*	0	*
1.	2	Searching for (How to buy a weapon stext01) Creating a bookmark named (SA01)	****	****	****	****
1.	3	Searching for (Pistol for sale stext02)	**	**	0	0
1.	4	Searching for (Gun silencer for Sale stext03) then deleting historyCreating then deleting bookmark name (SA02)	*0	*0	00	00
YouTube	1	Logging in	*	*	0	*
1.	2	Searching for (Arsenic poison stext04)Creating a bookmark named (YU01)	****	****	****	****
1.	3	Searching for (How to use a silencer on a gun stext05)	**	**	0	0
1.	4	Searching for (Activate WhatsApp with a fake number stext06) then deleting historyCreating then deleting a bookmark named (YU02)	*0	*0	00	00
Facebook / Facebook Messenger	1	Logging in	*	*	0	*
1.	2	Searching for (Noora Ibrahim)Creating a bookmark named (FC01)	****	****	****	****
1.	3	Searching for (Ibrahim Ezz El-Din)	*	**	0	0
1.	4	Searching for (Anna Ibrahim) then deleting historyCreating then deleting a bookmark named (FC02)	00	*0	00	00
1.	5	Sending message (are you ready? Did you say goodbye to your family?)	01.	0	0	0
1.	6	Deleting message (I know where you live)	0	0	0	0
Twitter	1	Logging in	*	*	0	*
1.	2	Searching for (Sarah Ibrahim)Creating a bookmark named (TW01)	****	****	****	****
1.	3	Searching for (Fahad Saad)	**	**	0	0
1.	4	Searching for (Muhannad Ahmed) then deleting the historyCreating then deleting a bookmark named (TW02)	00	*02.	00	00
1.	5	Sending message (Hi Sarah, I know where you live)	0	0	0	0
1.	6	Deleting message (I am close to your house, Noura)	0	0	0	0
WhatsApp	1	Sending message (I saw your tweets)	0	0	0	0
1.	2	Deleting message (If something happens to your daughters, that’s on you)	0	0	0	0
Gmail	1	Logging in	*	*	0	*

continued on following page

Table 6. Continued

Services	Activities		Normal Mode		Private Mode	
			Firefox	Edge	Firefox	Edge
1.	2	Sending an Email with a Subject title called (Mail01S) and the Email message is (I got your personal information gmailtext01)	0	0	0	0
1.	3	Sending then deleting an Email with a Subject title called (Mail02S) and the Email message is (this is your house location, right? gmailtext02)	0	0	0	0
Hotmail	1	Logging in	*	*	0	*
1.	2	Sending an Email with a Subject title called (Mail3S) and the Email message is (hmailtext01)	0	0	03.	04.
1.	3	Sending then deleting an Email with a Subject title called (Mail4S) and the Email message is (hmailtext02)	0	0	0	0
Outlook	1	Logging in	*	*	0	*
1.	2	Sending an Email with a Subject title called (Mail5S) and the Email message is (outmailtext01)	0	0	0	0
1.	3	Sending then deleting an Email with a Subject title called (Mail6S) and the Email message is (outmailtext02)	0	0	0	0

** = "Artifact found; content found"
* = "Artifact found; content is missing"
0 = "No artifact found"

These details provide insights into user activities and password-related events. Figure 6 shows the details about the logins table on DB Browser SQLite (Edge browser normal mode).

In the private mode of the Edge browser, the usernames can also be found even after logging in from a private session. The data can be found in the same path as the normal mode in the logins table. Figure 7 shows the details about the logins table on DB Browser SQLite (Edge browser-private mode).

In the normal mode of the Edge browser, the history and searched terms are stored in the sqlite3 history file, specifically in the URLs table. The file contains visit time, visit count, and search terms, while the keyword_search_terms table holds the most frequently used search terms. The DB Browser (SQLite) program can be used to extract and view this data, providing insights into user browsing habits. Deleted search history can be recovered from the session file, although it lacks details such as URLs and visit times. In private mode, only search history related to created bookmarks is stored in the URLs table. Conversion of numerical time formats to human-readable is necessary using tools like DCode.

In both normal and private modes of the Edge browser, data related to emails and instant messaging (e.g., Facebook Messenger, WhatsApp) cannot be found locally as they are stored in the cloud by the service providers. However, in the normal mode, a dump of private messages for Twitter and Facebook Messenger can be found in the Pagefile.sys. This dump data is random and not systematically stored, requiring knowledge of relevant keywords to locate and analyze it. Figure 8 shows the details of a private message on Twitter (Edge browser-normal mode). Figure 9 presents the details of a private message on Facebook Messenger (Edge browser-normal mode).

Table 7. Results of browser analysis of smartphones

Services	Activities		Normal Mode		Private Mode		
			Android (Firefox) XRY	IOS(Safari) AXIOM	Android (Firefox) XRY	IOS(Safari) AXIOM	
Google	1	Logging in	0	0	0	0	0
1.	2	Searching for (How to buy a weapon stext01)Creating a bookmark named (SA01)	****	****	***	****	****
1.	3	Searching for (Pistol for sale stext02)	**	**	0	**	**
1.	4	Searching for (Gun silencer for Sale stext03) then deleting historyCreating then deleting bookmark name (SA02)	**0	**0	*0	00	***
YouTube	1	Logging in	0	0	0	0	*
1.	2	Searching for (Arsenic poison stext04)Creating a bookmark named (YU01)	****	****	***	****	****
1.	3	Searching for (How to use a silencer on a gun stext05)	**	**	0	**	**
1.	4	Searching for (Activate WhatsApp with a fake number stext06) then deleting history.Creating then deleting a bookmark named (YU02)	**0	**0	**	00	***
Facebook / Facebook Messenger	1	Logging in	0	0	0	0	0
1.	2	Searching for (Noora Ibrahim) Creating a bookmark named (FC01)	****	****	***5.	****	***
1.	3	Searching for (Ibrahim Ezz El-Din)	**	**	0	**	**
1.	4	Searching for (Anna Ibrahim) then deleting historyCreating then deleting a bookmark named (FC02)	**06.	**0	**	00	**
1.	5	Sending message (are you ready? Did you say goodbye to your family?)Sending attachment (fcimg1)	00	0	0	00	**0
1.	6	Deleting message (I know where you live)Sending and deleting an attachment (fcimg2)	00	0	0	00	**0
Twitter	1	Logging in	0	*	0	0	0
1.	2	Searching for (Sarah Ibrahim) Creating a bookmark named (TW01)	****	****	***	****	* ***
1.	3	Searching for (Fahad Saad)	**	**	0	**	**
1.	4	Searching for (Muhannad Ahmed) then deleting the historyCreating then deleting a bookmark named (TW02)	**0	**0	*0	**0	***
1.	5	Sending message (Hi Sarah, I know where you live)Sending attachment (timg1)	00	0	0	007.	**0
1.	6	Deleting message (I am close to your house, Noura)Sending and deleting an attachment (timg2)	00	0	0	00	00

continued on following page

Table 7. Continued

Services	Activities		Normal Mode		Private Mode		
			Android (Firefox) XRY	IOS(Safari) AXIOM	Android (Firefox) XRY	IOS(Safari) AXIOM	
Outlook	1	Logging in	0	0	0	0	0
1.	2	Sending an Email with a Subject title called (Mail5) and the Email message is (outmailtext01) Sending an attachment (oimg01)	00	00	00	00	****
1.	3	Sending then deleting an Email with a Subject title called (Mail6) and the Email message is (outmailtext01)Sending then deleting an attachment (oimg02)	00	00	00	00	*0
Gmail	1	Logging in	0	0	0	0	0
1.	2	Sending an Email with a Subject title called (Mail01) and the Email message is (I got your personal information gmailtext01)Sending an attachment (gimg01)	0	0	0	0	**0
1.	3	Sending then deleting an Email with a Subject title called (Mail02) and the Email message is (this is your house location, right? gmailtext02)Sending then deleting an attachment (gimg02)	0	0	0	0	**0
Hotmail	1	Logging in	0	0	0	0	0
1.	2	Sending an Email with a Subject title called (Mail03) and the Email message is (hmailtext01)Sending an attachment (himg01)	0	0	0	0	****
1.	3	Sending then deleting an Email with a Subject title called (Mail4) and the Email message is (hmailtext02)Sending then deleting an attachment (himg02)	0	0	0	0	*0

** = "Artifact found; content found"
* = "Artifact found; content is missing"
0 = "No artifact found" – FFS = Full File system – APP = Application

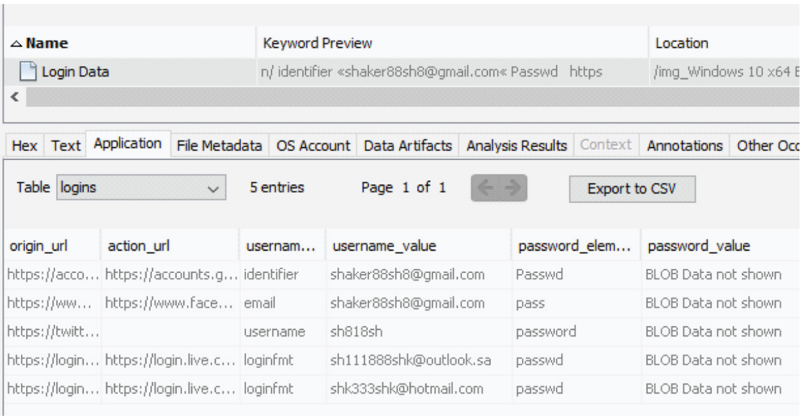
Table 8. Results of browser analysis of smartphones

Artifacts	Path
Accounts	/Users/[username]/AppData/Local/Microsoft/Edge/User Data/Default/Login Data
Bookmarks	/Users/[username]/AppData/Local/Microsoft/Edge/User Data/Default/Bookmarks
History	/Users/[username]/AppData/Local/Microsoft/Edge/User Data/Default/History/urls
Most used keywords	/Users/[username]/AppData/Local/Microsoft/Edge/UserData/Default/History/keyword_search_terms
Sessions	/Users/[username]/AppData/Local/Microsoft/Edge/User Data/Default/Sessions
Cookies	/Users/[username]/AppData/Roaming/Mozilla/Firefox/Profiles/zu907wu9.default-release/places.sqlite/moz_cookies

FireFox Analysis

Table 9 shows the Firefox browser artifacts paths. Figure 10 presents the details about user login data related to Gmail/Google. Figure 11 shows the Outlook username.

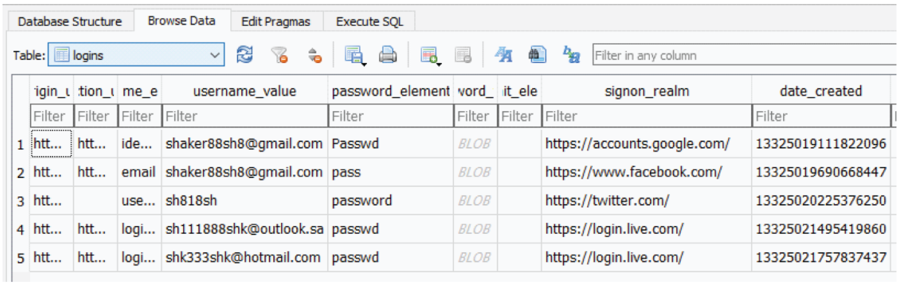
Figure 5. Login data on autopsy (edge browser-normal mode)



Name	Keyword Preview	Location
Login Data	n/ identifier «shaker88sh8@gmail.com« Passwd https	/img_Windows 10 x64 E

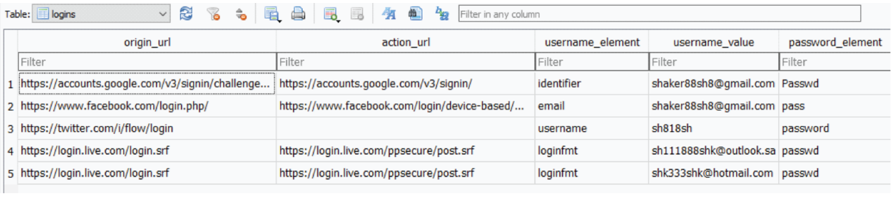
origin_url	action_url	usernam…	username_value	password_elem…	password_value
https://acco…	https://accounts.g…	identifier	shaker88sh8@gmail.com	Passwd	BLOB Data not shown
https://ww…	https://www.face…	email	shaker88sh8@gmail.com	pass	BLOB Data not shown
https://twitt…		username	sh818sh	password	BLOB Data not shown
https://login…	https://login.live.c…	loginfmt	sh111888shk@outlook.sa	passwd	BLOB Data not shown
https://login…	https://login.live.c…	loginfmt	shk333shk@hotmail.com	passwd	BLOB Data not shown

Figure 6. Logins table on DB browser SQLite (edge browser-normal mode)



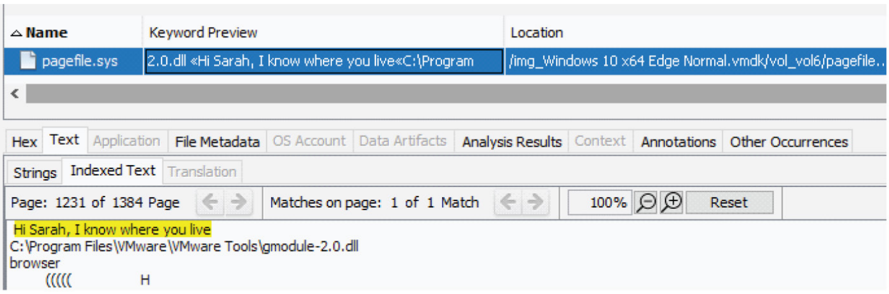
	igin_u	tion_u	me_e	username_value	password_element	word_	it_ele	signon_realm	date_created
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	htt…	htt…	ide…	shaker88sh8@gmail.com	Passwd	BLOB		https://accounts.google.com/	13325019111822096
2	htt…	htt…	email	shaker88sh8@gmail.com	pass	BLOB		https://www.facebook.com/	13325019690668447
3	htt…		use…	sh818sh	password	BLOB		https://twitter.com/	13325020225376250
4	htt…	htt…	logi…	sh111888shk@outlook.sa	passwd	BLOB		https://login.live.com/	13325021495419860
5	htt…	htt…	logi…	shk333shk@hotmail.com	passwd	BLOB		https://login.live.com/	13325021757837437

Figure 7. Logins table on DB browser SQLite (edge browser-private mode)



	origin_url	action_url	username_element	username_value	password_element
	Filter	Filter	Filter	Filter	Filter
1	https://accounts.google.com/v3/signin/challenge…	https://accounts.google.com/v3/signin/	identifier	shaker88sh8@gmail.com	Passwd
2	https://www.facebook.com/login.php/	https://www.facebook.com/login/device-based/…	email	shaker88sh8@gmail.com	pass
3	https://twitter.com/i/flow/login		username	sh818sh	password
4	https://login.live.com/login.srf	https://login.live.com/ppsecure/post.srf	loginfmt	sh111888shk@outlook.sa	passwd
5	https://login.live.com/login.srf	https://login.live.com/ppsecure/post.srf	loginfmt	shk333shk@hotmail.com	passwd

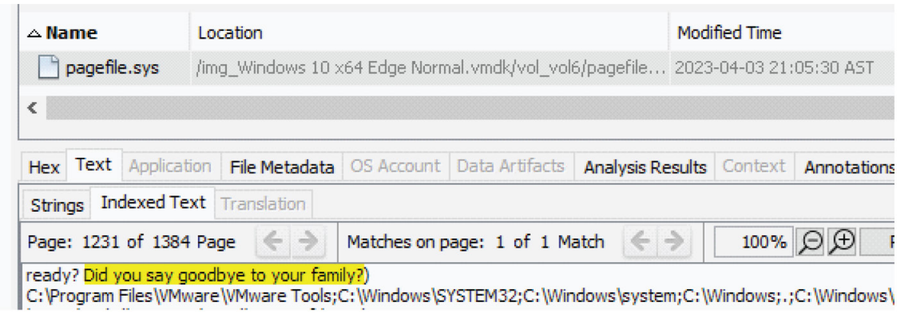
Figure 8. A private message on Twitter (edge browser-normal mode)



Name	Keyword Preview	Location
pagefile.sys	2.0.dll «Hi Sarah, I know where you live«C:\Program	/img_Windows 10 x64 Edge Normal.vmdk/vol_vol6/pagefile..

```
Hi Sarah, I know where you live
C:\Program Files\VMware\VMware Tools\gmodule-2.0.dll
browser
     (((((          H
```

Figure 9. A private message on Facebook Messenger (edge browser-normal mode)



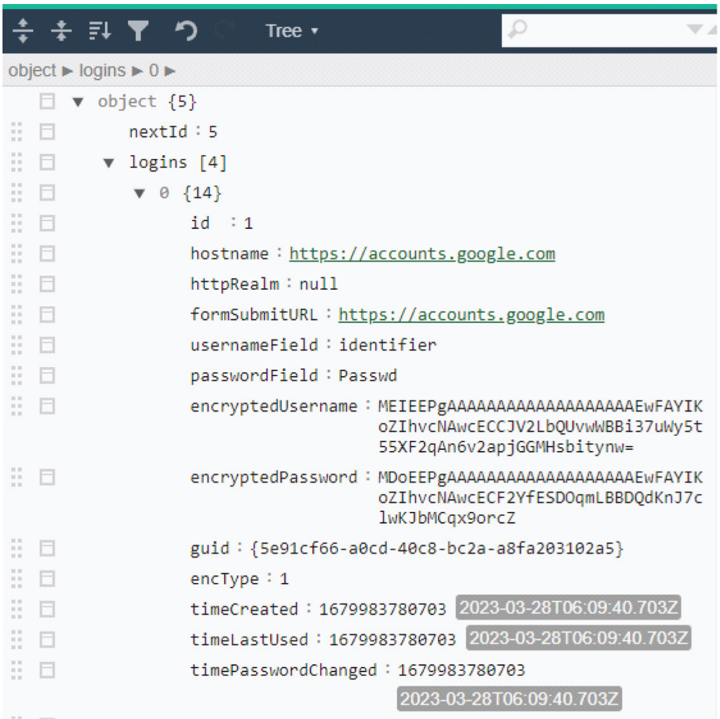
Name	Location	Modified Time
pagefile.sys	/img_Windows 10 x64 Edge Normal.vmdk/vol_vol6/pagefile…	2023-04-03 21:05:30 AST

```
ready? Did you say goodbye to your family?)
C:\Program Files\VMware\VMware Tools;C:\Windows\SYSTEM32;C:\Windows\system;C:\Windows;.;C:\Windows\
```

Table 9. Firefox browser artifacts paths

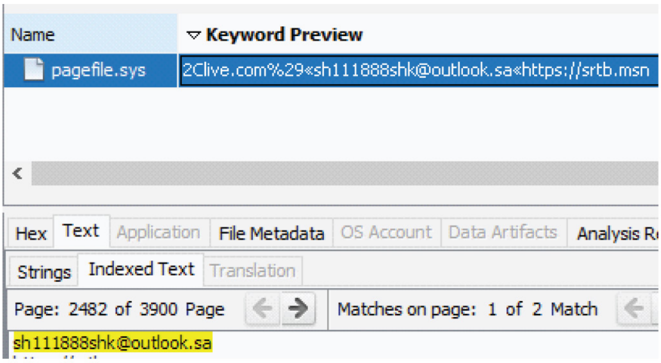
Artifacts	Path
Accounts	/Users/[username]/AppData/Roaming/Mozilla/Firefox/Profiles/zu907wu9.default-release/logins.json
Bookmarks	/Users/[username]/AppData/Roaming/Mozilla/Firefox/Profiles/zu907wu9.default-release/places.sqlite/moz_bookmarks
History	/Users/[username]/AppData/Roaming/Mozilla/Firefox/Profiles/zu907wu9.default-release/places.sqlite/moz_places
Cookies	/Users/[username]/AppData/Roaming/Mozilla/Firefox/Profiles/zu907wu9.default-release/places.sqlite/moz_cookies

Figure 10. User login data related to gmail/google



```
▼ object {5}
    nextId : 5
  ▼ logins [4]
    ▼ 0 {14}
        id  : 1
        hostname : https://accounts.google.com
        httpRealm : null
        formSubmitURL : https://accounts.google.com
        usernameField : identifier
        passwordField : Passwd
        encryptedUsername : MEIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIK
                            oZIhvcNAwcECCJV2LbQUvwWBBi37uWy5t
                            55XF2qAn6v2apjGGMHsbitynw=
        encryptedPassword : MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIK
                            oZIhvcNAwcECF2YfESDOqmLBBDQdKnJ7c
                            lwKJbMCqx9orcZ
        guid : {5e91cf66-a0cd-40c8-bc2a-a8fa203102a5}
        encType : 1
        timeCreated : 1679983780703 2023-03-28T06:09:40.703Z
        timeLastUsed : 1679983780703 2023-03-28T06:09:40.703Z
        timePasswordChanged : 1679983780703
                              2023-03-28T06:09:40.703Z
```

Figure 11. Outlook username



Name	Keyword Preview
pagefile.sys	2Clive.com%29«sh111888shk@outlook.sa«https://srtb.msn

sh111888shk@outlook.sa

Figure 12. DB browser SQLite (firefox browser-normal mode)

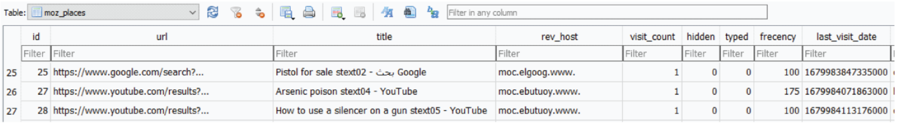


Table: moz_places

	id	url	title	rev_host	visit_count	hidden	typed	frecency	last_visit_date
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
25	25	https://www.google.com/search?...	Pistol for sale stext02 - بحث Google	moc.elgoog.www.	1	0	0	100	1679983847335000
26	27	https://www.youtube.com/results?...	Arsenic poison stext04 - YouTube	moc.ebutuoy.www.	1	0	0	175	1679984071863000
27	28	https://www.youtube.com/results?...	How to use a silencer on a gun stext05 - YouTube	moc.ebutuoy.www.	1	0	0	100	1679984113176000

In the normal mode of the Firefox browser, user login data including usernames and passwords can be found in an encrypted Json file called "logins." The file is located at /Users/[username]/AppData/Roaming/Mozilla/Firefox/Profiles/zu907wu9.default-release/logins. Extraction of the file from Autopsy allows for analysis using tools capable of reading JSON files. However, it should be noted that all login data, both usernames and passwords, are encrypted within this file. This is another case where the Pagefile.sys provided us with more data.

In the normal mode of the Firefox browser, the history and searched terms are stored in the places.sqlite file, specifically in the moz_places table. This file contains visit time, visit count, search terms, and related URLs. The DB Browser (SQLite) program can be used to extract and analyze this data. If search terms are deleted from the history, artifacts can be partially found in the moz_cookies table within a sqlite file, although the table does not provide URL values. In the private mode, similar to the Edge browser, Firefox does not store search history unless bookmarks are created. Bookmarks are stored in the moz_bookmarks file, providing information about created bookmarks and their creation time. Data related to emails and instant messaging (e.g., Facebook Messenger, WhatsApp) in both normal and private modes are not stored locally but in the cloud of the respective service provider. Figure 12 shows the details about the DB Browser SQLite (Firefox browser-normal mode).

Mobile Device Analysis

Android Devices

We connected a Samsung USB Type C cable from a Nokia 7 Plus mobile device to a computer for analysis using the XRY tool. The device was successfully connected, and a logical image was created. In normal mode, bookmarks are stored in the "moz_bookmark" folder, while in private mode, they are stored in the "moz_inputthistory" folder. Deleted bookmarks in normal mode are found in the "moz_bookmark" folder, and in private mode, they can be found in the "moz_bookmarks_deleted" folder. Table 10 shows the artifact paths for Android Firefox.

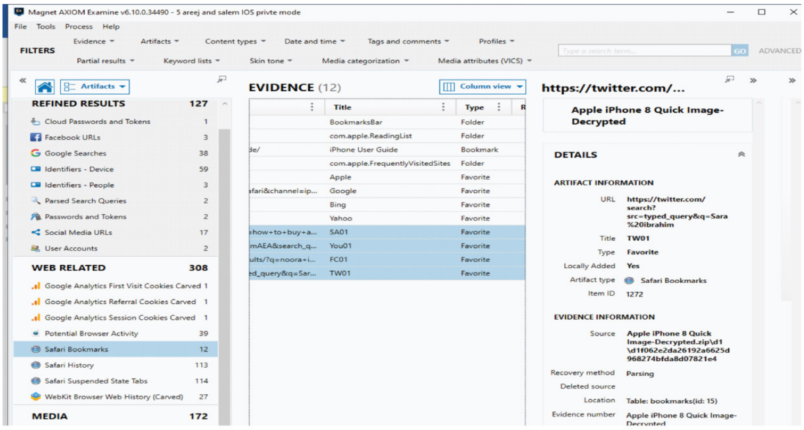
Table 10. Artifacts paths for android firefox

Artifact	Normal	Private	Path
	File Name		
Google login	(moz_places)Places.sqlite-wal	-	/data/data/org.mozila.firefox/files/
Search word	(moz_places)Places.sqlite-wal	-	/data/data/org.mozila.firefox/files/
Bookmark	(moz_bookmark)Places.sqlite-wal	(moz_inputthistory)Places.sqlite-wal	/data/data/org.mozila.firefox/files/
YouTube login	-	-	-
Search word	(moz_places)Places.sqlite-wal	-	/data/data/org.mozila.firefox/files/
The deleted history	(moz_places)Places.sqlite-wal	-	/data/data/org.mozila.firefox/files/
Bookmark	(moz_bookmark)Places.sqlite-wal	-	/data/data/org.mozila.firefox/files/
Facebook login	(moz_places)Places.sqlite-wal	-	/data/data/org.mozila.firefox/files/
Search words	(moz_places)Places.sqlite-wal	-	/data/data/org.mozila.firefox/files/
Deleted words	(moz_places)Places.sqlite-wal	-	/data/data/org.mozila.firefox/files/
Bookmark	(moz_bookmark)Places.sqlite-wal	(moz_inputthistory)Places.sqlite-wal	/data/data/org.mozila.firefox/files/
Deleted bookmark	-	(moz_bookmarks_deleted)Places.sqlite-wal	-
Twitter login	(moz_places)Places.sqlite-wal	-	/data/data/org.mozila.firefox/files/
Search words	(moz_places)Places.sqlite-wal	-	/data/data/org.mozila.firefox/files/
Bookmark	(moz_bookmark)Places.sqlite-wal	(moz_inputthistory)Places.sqlite-wal	/data/data/org.mozila.firefox/files/
Deleted bookmark		(moz_bookmarks_deleted)Places.sqlite-wal	
the deleting history	(moz_places)Places.sqlite-wal	(moz_inputthistory)Places.sqlite-wal	/data/data/org.mozila.firefox/files/
Outlook login	(moz_places)Places.sqlite-wal	-	/data/data/org.mozila.firefox/files/

IOS Devices

iPhone 8 was connected to the computer using a USB cable, and a logical image of the device was created using the Axiom Acquire tool. The analysis was performed using the Axiom Magnet tool, revealing that Safari artifacts are stored in specific directories, specifically in AppleiPhone8QuickImageDecrypted.zip\ d1\d1f062e2da26192a6625d 968274bfda8d07 821e4. Traces of various evidence were found in this path, with location type indicating the exact database location and column. However, deleted bookmarks were not recovered. Due to limitations in retrieving deep information from smart devices with logical images, a full file system acquisition was performed

Figure 13. Bookmarks artifacts apple iPhone 8 quick image



REFINED RESULTS	127
Cloud Passwords and Tokens	1
Facebook URLs	3
Google Searches	38
Identifiers - Device	59
Identifiers - People	3
Parsed Search Queries	2
Passwords and Tokens	2
Social Media URLs	17
User Accounts	2
WEB RELATED	**308**
Google Analytics First Visit Cookies Carved	1
Google Analytics Referral Cookies Carved	1
Google Analytics Session Cookies Carved	1
Potential Browser Activity	39
Safari Bookmarks	12
Safari History	113
Safari Suspended State Tabs	114
WebKit Browser Web History (Carved)	27
MEDIA	**172**

EVIDENCE (12)

	Title	Type
	BookmarksBar	Folder
	com.apple.ReadingList	Folder
de/	iPhone User Guide	Bookmark
	com.apple.FrequentlyVisitedSites	Folder
	Apple	Favorite
afari&channel=ip...	Google	Favorite
	Bing	Favorite
	Yahoo	Favorite
how+to+buy+a...	SA01	Favorite
mAEA&search_q...	You01	Favorite
ults/?q=noora+i...	FC01	Favorite
d_query&q=Sar...	TW01	Favorite

https://twitter.com/...

Apple iPhone 8 Quick Image-Decrypted

DETAILS

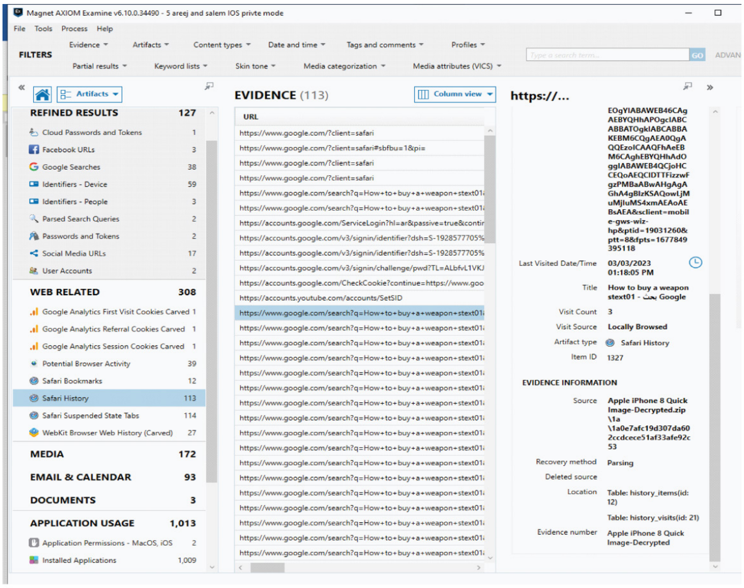
ARTIFACT INFORMATION

URL: https://twitter.com/search?src=typed_query&q=Sara%20ibrahim
Title: TW01
Type: Favorite
Locally Added: Yes
Artifact type: Safari Bookmarks
Item ID: 1272

EVIDENCE INFORMATION

Source: Apple iPhone 8 Quick Image-Decrypted.zip\d1\d1f062e2da26192a6625d968274bfda8d07821e4
Recovery method: Parsing
Deleted source:
Location: Table: bookmarks(id: 15)
Evidence number: Apple iPhone 8 Quick Image-Decrypted

Figure 14. History artifacts apple iPhone 8 quick image



REFINED RESULTS	127
Cloud Passwords and Tokens	1
Facebook URLs	3
Google Searches	38
Identifiers - Device	59
Identifiers - People	3
Parsed Search Queries	2
Passwords and Tokens	2
Social Media URLs	17
User Accounts	2
WEB RELATED	**308**
Google Analytics First Visit Cookies Carved	1
Google Analytics Referral Cookies Carved	1
Google Analytics Session Cookies Carved	1
Potential Browser Activity	39
Safari Bookmarks	12
Safari History	113
Safari Suspended State Tabs	114
WebKit Browser Web History (Carved)	27
MEDIA	**172**
EMAIL & CALENDAR	**93**
DOCUMENTS	**3**
APPLICATION USAGE	**1,013**
Application Permissions - MacOS, iOS	2
Installed Applications	1,009

EVIDENCE (113)

URL
https://www.google.com/?client=safari
https://www.google.com/?client=safari#sbfbu=1&pi=
https://www.google.com/?client=safari
https://www.google.com/?client=safari
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://accounts.google.com/ServiceLogin?hl=ar&passive=true&contir
https://accounts.google.com/v3/signin/identifier?dsh=S-1928577705%
https://accounts.google.com/v3/signin/identifier?dsh=S-1928577705%
https://accounts.google.com/v3/signin/challenge/pwd?TL=ALbfvL1VKJ
https://accounts.google.com/CheckCookie?continue=https://www.goo
https://accounts.youtube.com/accounts/SetSID
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01
https://www.google.com/search?q=How+to+buy+a+weapon+stext01

https://...

EOgYIABAWEB46CAgAEBYQHhAPOgcIABCABBATOgkIABCABBAKEBM6CQgAEA0QgAQQEzoICAAQFhAeEBM6CAghEBYQHhAdOggIABAWEB4QCjoHCCEQoAEQCIDTTFizzwFgzPMBaABwAHgAgAGhA4gBlzKSAQowLjMuMjIuMS4xmAEAoAEBsAEA&sclient=mobile-gws-wiz-hp&ptid=19031260&ptt=8&fpts=1677849395118
Last Visited Date/Time: 03/03/2023 01:18:05 PM
Title: How to buy a weapon stext01 - بحث Google
Visit Count: 3
Visit Source: Locally Browsed
Artifact type: Safari History
Item ID: 1327

EVIDENCE INFORMATION

Source: Apple iPhone 8 Quick Image-Decrypted.zip\1a\1a0e7afc19d307da602ccdcece51af33afe92c53
Recovery method: Parsing
Deleted source:
Location: Table: history_items(id: 12)
Table: history_visits(id: 21)
Evidence number: Apple iPhone 8 Quick Image-Decrypted

after jailbreaking the iPhone using the Magnet Acquire tool. This allowed access to additional evidence. Applications such as Google, YouTube, Facebook, Gmail, Outlook, and Twitter were downloaded and logged into to compare the evidence extracted from the applications themselves versus the browser. The focus was on attachments and emails related to these applications, which presented challenges in previous analyses, and significant evidence and paths were discovered. Figure 13 shows the details about the bookmark artifacts Apple iPhone 8 quick image. Figure 14 presents the history artifacts of the Apple iPhone 8 quick image. Table 11 shows the artifact paths for iPhone applications. Table 12 shows the artifact paths for iPhone Safari.

Table 11. Artifacts paths for iPhone applications

Artifacts	Paths
Deleted Chat	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Containers\Data\Application\EC84A3F7-58F7-4BE9-80BF-69CF12D185D2\Library\Caches\com.atebits.tweetie.direct-message.cache\sh818sh-702287251460854
Gmail	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Containers\Data\Application\70724B7C-EB4E-4A27-AE83-35CC9886BCAD\Library\Application Support\data\shaker88sh8@gmail.com\sqlitedb
Hotmail	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Containers\Shared\AppGroup\880F6D19-DD78-415B-850D-5C997988EBFA\Hx\HxStore.hxd
Attachment of Hotmail	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Containers\Shared\AppGroup\880F6D19-DD78-415B-850D-5C997988EBFA\Hx\Files\S0\1\Attachments\himg01[21].png
Outlook	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Containers\Shared\AppGroup\880F6D19-DD78-415B-850D-5C997988EBFA\Hx\HxStore.hxdApple iPhone 7 Plus Full Image.tar\private\var\mobile\Containers\Shared\AppGroup\880F6D19-DD78-415B-850D-5C997988EBFA\Hx\Files\S0\29\Attachments\oimg01[50].png
Deleted Emails in Outlook	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Keyboard\en-dynamic.lm\dynamic-lexicon.dat

CONCLUSION AND FUTURE WORK

Our research makes significant contributions to the field of digital forensics by demonstrating the differential effectiveness of forensic tools in recovering browser artifacts, especially in private browsing modes. These insights are crucial for forensic investigators and tool developers aiming to enhance the effectiveness of digital forensic investigations. This research highlights the significant advancements in web browser forensics, specifically detailing an improvement in evidence recovery rates by up to 30% when using advanced forensic tools like AXIOM and XRY in specific scenarios. These findings contribute notably to the domain of digital forensics, offering practitioners enhanced methodologies for artifact recovery in both normal and private browsing modes. This study revealed that Firefox provides enhanced security for user login data compared to Edge. Private browsing modes minimize digital traces but still leave some history and bookmark data. Emails and instant messaging artifacts are not stored locally but on the cloud. RAM and files like pagefile.sys contain valuable data. On smartphones, jailbreaking provided access to previously unavailable artifacts, particularly in applications like Google, Outlook, Gmail, YouTube, Facebook, and Twitter. The XRY tool had limitations with certain Android models, while Axiom Magnet required significant time for imaging.

In this study, we focus on selected web browsers and forensic tools, which were chosen based on their prevalence and relevance to current digital forensic challenges. Future work will aim to broaden the scope of our research to include a more diverse array of browsers and forensic tools. This expansion will allow us to address a wider range of real-life scenarios, enhancing the universality and applicability of our findings. We believe that incorporating varied forensic environments and emerging technologies will significantly contribute to the robustness and relevance of web browser forensics research.

Funding Statement

This research was funded by Naif Arab University for Security Sciences under grant No. NAUSS-23-R10.

Author Note

The authors would like to express their deep thanks to the Vice Presidency for Scientific Research at Naif Arab University for Security Sciences for their kind encouragement of this work.

Table 12. Artifacts paths for iPhone Safari

Artifact	Normal+private	Location: table
	Path	
Google login	-	-
Search word	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Safari\History.db	history_ itemshistory_ visits
Bookmark	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Safari\Bookmarks.db	bookmarks
Deleting book mark	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Keyboard\en-dynamic.lm\dynamic-lexicon.dat	
YouTube login	-	
Search word	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Safari\History.db	history_ itemshistory_ visits
the deleting history	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Safari\History.db	history_ itemshistory_ visits
bookmark	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Safari\Bookmarks.db	bookmarks
deleting book mark	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Keyboard\en-dynamic.lm\dynamic-lexicon.dat	
Facebook login	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Safari\History.db	history_ itemshistory_ visits
Search Words	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Safari\History.db	history_ itemshistory_ visits
Deleted Search	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\CoreDuet\Knowledge\knowledgeC.db	
bookmark	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Safari\Bookmarks.db	bookmarks
Deleted bookmark	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Keyboard\en-dynamic.lm\dynamic-lexicon.dat	
Twitter login	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Safari\History.db	history_ itemshistory_ visits
Search word	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Safari\History.db	history_ itemshistory_ visits
Bookmark	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Safari\Bookmarks.db	bookmarks
Deleting bookmark	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Keyboard\en-dynamic.lm\dynamic-lexicon.dat	-
The deleted history	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Safari\History.db	history_ itemshistory_ visits
Outlook login	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Safari\History.db	history_ itemshistory_ visits

continued on following page

Table 12. Continued

Artifact	Normal+private	Location: table
	Path	
Gmail login	Apple iPhone 7 Plus Full Image.tar\private\var\mobile\Library\Safari\History.db	history_ itemshistory_ visits

The authors declare no conflicts of interest.

Process Dates

June 2024
Received: January 25, 2024, Revision: May 22, 2024, Accepted: May 20, 2024

Corresponding Author

Correspondence should be addressed to Emad Ul Haq Qazi (Saudi Arabia, qabdulrab@nauss.edu.sa)

REFERENCES

Asim, M., Amjad, M. F., Iqbal, W., Afzal, H., Abbas, H., & Zhang, Y. (2019). AndroKit: A toolkit for forensics analysis of web browsers on android platform. *Future Generation Computer Systems*, *94*, 781–794. 10.1016/j.future.2018.08.020

Autopsy (n.d.). *Autopsy.*https://www.autopsy.com/

Email client market share in 2021: Trends from January to March – Litmus

EnterpriseAppsToday. (2022). *Firefox statistics 2022 - Market share and usage statistics 2022 Safari statistics - Browser usage, market share, facts and trends.* enterpriseappstoday.com

Grover, J. (2013). Android forensics: Automated data collection and reporting from a mobile device. *Digital Investigation*, *10*, S12–S20. 10.1016/j.diin.2013.06.002

Jadhav, M. R., & Meshram, B. B. (2018). *Web browser forensics for detecting user activities. International Research Journal of Engineering and Technology*. IRJET.

Joe, S., Andrew, C., Lodovico, M., & Golden, G. R. (2023). Acquisition and analysis of volatile memory from Android devices. *Digital Investigation*, *8*(3-4), 175–184. 10.1016/j.cose.2023.103425

Junghoon, H., Seungbong, L., & Sangjin, L. (2011). Advanced evidence collection and analysis of web browser activity. *Digital Investigation*, *8*, S62–S70. 10.1016/j.diin.2011.05.008

Magnet Forensics. (2023, April 19). *Uncover digital evidence - Build stronger cases.*https://www.magnetforensics.com/

MSAB. (n.d.) *XRY - Mobile forensics and data recovery software.* Retrieved Month date, year, from https://www.msab.com/product/xry-extract/

Mugisha, D. (2018). Web browser forensics: Evidence collection and analysis for most popular web browsers usage in Windows 10. *International Journal of Cyber Criminology.*

Murias, J. G., Levick, D., & McKeown, S. (2023). A forensic analysis of streaming platforms on Android OS. *Forensic Science International Digital Investigation*, *44*, 301485. 10.1016/j.fsidi.2022.301485

Nalawade, A., Bharne, S., & Mane, V. (2021). Forensic analysis and evidence collection for web browser activity. International conference on automatic control and dynamic optimization techniques (ICACDOT), International Institute of Information Technology (I^{2}IT).

Rao, V. V., & Chakravarthy, A. S. N. (2016, December). Forensic analysis of android mobile devices. *The 2016 international conference on recent advances and innovations in engineering (ICRAIE).* IEEE.

Rasool, A., & Jalil, Z. (2020). *A review of web browser forensic analysis tools and techniques*. Researchpedia Journal of Computing.

Sanghvi, H., Rathod, D., Altaleedi, S. Y., AlThani, A. S., Alkhawaldeh, M. A. A., Almorjan, A., Shah, R., & Zia, T. A. (2023). Google Chrome forensics. *International Journal of Electronic Security and Digital Forensics*, *15*(6), 591–619. Advance online publication. 10.1504/IJESDF.2023.133968

Shafqat, N. (2016). *Forensic investigation of user's web activity on Google Chrome using various forensic tools*. IJCSNS International Journal of Computer Science and Network Security.

Tayeb, H. F., & Varol, C. (2019, June). Android mobile device forensics: A review. *The 2019 7th international symposium on digital forensics and security (ISDFS).* IEEE.

Umar, R., Yudhana, A., & Faiz, M. N. (2018). *Experimental analysis of web browser sessions using live forensics method. International Journal of Electrical and Computer Engineering*. IJECE.

Yusoff, M. N., Mahmod, R., Abdullah, M. T., & Dehghantanha, A. (2014). Performance measurement for mobile forensic data acquisition in Firefox OS. *International Journal of Cyber-Security and Digital Forensics*, *3*(3), 130–140. 10.17781/P001333

Dr. Qazi Emad-Ul-Haq received his Ph.D. degree in the field of Artificial Intelligence and Machine Learning. He did his Postdoc in the field of Cybersecurity and Machine Learning. He is currently working as an Assistant Professor at the Centre of Cybercrimes and Digital Forensics (CoECDF), Naif Arab University for Security Sciences (NAUSS), Riyadh, Saudi Arabia. He has more than fifteen (15) years of teaching and research experience. He has completed a number of international collaborative research projects with reputable universities. He holds one US Patent and has published many research articles in high-ranked peer-reviewed journals and well-recognized international conferences. His research interests include Artificial Intelligence, Machine Learning, Deep Learning, Security Analytics, and Cybercrime prevention.

Tanveer Zia currently serves as the Associate Director and a founding member of the Centre of Excellence in Cybercrimes and Digital Forensics at the Naif Arab University for Security Sciences in Riyadh. Prior to that, Tanveer contributed significantly to academic and institutional leadership during his 12-year tenure at Charles Sturt University Wagga Wagga Campus. There, he held the positions of Professor of Computing and Associate Head of the School of Computing, Mathematics, and Engineering. Notably, Tanveer is recognized as a Senior Fellow of the Higher Education Academy (SFHEA) in the UK.

Ms. Areej Muqbil Alotibi is a student of Master of Cybercrime and Digital Forensics at Naif Arab University for Security Sciences (NAUSS), Riyadh, Kingdom of Saudi Arabia.

Ms. Salem Yahya Altaleedi is a student of Master of Cybercrime and Digital Forensics at Naif Arab University for Security Sciences (NAUSS), Riyadh, Kingdom of Saudi Arabia. He is an expert in digital forensics investigation.