Applied Information Technology And Computer Science Vol. 3 No. 2 (2022) 084-100
© Universiti Tun Hussein Onn Malaysia Publisher's Office

AITCS

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

A Comparative Analysis of Potential Digital Evidence in WhatsApp Web-Based and Mobile-Based Application

Anis Safi Mohd Idris[1], Nurul Hidayah Ab Rahman[1]*

[1]Fakulti Sains Komputer dan Teknologi Maklumat,
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA

DOI: https://doi.org/10.30880/aitcs.2022.03.02.006
Received 08 August 2022; Accepted 06 October 2022; Available online 30 November 2022

Abstract: WhatsApp has become the most popular instant messaging (IM) application for users to send and receive messages through a web browser and smartphone. As it becomes more popular among users, the chance of digital crimes might happen. There is a lack of investigation to compare the digital artifacts acquired from WhatsApp web-based and WhatsApp mobile-based identified in the previous study. This study attempts to forensically analyze and compare the artifacts that can be recovered in browser and mobile devices using a timeline approach. The research methodology consists of preparation, acquisition, analysis and validation phases. The investigation was done through simulation activities, acquiring images, analyzing artifacts and documenting using forensic examination guidance. The findings were analyzed manually using DB Browser SQLite and WordPad. The main artifact acquired in the Chrome browser was WhatsApp Web log files, which included cache, timestamps, and logs. Meanwhile, WhatsApp mobile acquired additional data from the WhatsApp database file, including login history, timestamps, logs, text messages, images, videos, and call logs. Furthermore, this study will benefit digital forensic investigators and inspire future work using various WhatsApp forensics approaches to obtain valuable data from the WhatsApp application.

Keywords: WhatsApp, Digital Evidence, Timeline Approach, Artifacts

1. Introduction

With the increasing popularity of WhatsApp, the chance of cybercrimes will also increase, such as online fraud and scammers[1]. In the context of digital forensics, WhatsApp conversations, chats and images can be potential evidence of a crime incident. However, capturing forensics evidence is different for browsers and mobile devices. This study aims to analyze the difference in the digital forensic process to acquire digital evidence from WhatsApp web-based and mobile-based applications. Investigators analyzed artifacts in hard disk memory and Android storage files.

For the WhatsApp initiative, the proposed study would raise knowledge of numerous digital forensics topics, such as the browser and mobile forensics. The evidence was discovered due to the discovery of evidence in certain areas. Furthermore, comparing what can be retrieved from the exact

*Corresponding author: hidayahar@uthm.edu.my result or outcome from both sources of WhatsApp forensics to benefit forensic investigators. Three objectives have been set as follows:

1. To study WhatsApp Web-based and WhatsApp mobile-based in acquiring valuable data for digital forensics.
2. To compare the potential acquired artifacts from WhatsApp browser and WhatsApp mobile app platforms.
3. To analyze the acquired artifacts from both platforms using timeline approach.

The rest of the paper is organized as follows: Section 2 discusses the related work of WhatsApp forensics in browser and mobile analysis. Section 3 explains the methodology for acquiring WhatsApp artifacts in browsers and mobile devices. Section 4 presents the research design and implementation and finally, Section 5 describes the importance of this study for future use.

2. Background of Study

This section explains definitions, theoretical background, digital forensic approach and related previous works conducted about the research to understand the literature's landscape and the appropriate methodology.

2.1 Digital Forensics

Zatyko [2] defined digital forensics involves analyzing digital evidence after proper search authority, the chain of custody, validation with mathematics, validated tools, repeatability, reporting and expert presentation. Effective methodologies and developing efficient tools are needed for attack detection efficiency [3]. The digital forensics process involves acquiring digital evidence, identification, preservation, analysis, documentation and presentation, which can be admissible evidence by the court law [4].

2.1.1 Timeline approach

One digital forensic approach for this study was the timeline approach. This research conducted a timeline analysis, compiling a list of events connected to time chronicles [5]. Timeline analysis in computer forensics related to the event's date and time. Qawasmeh and Al-Saleh [6] conducted a memory forensic using a created timeline event, which outlines the events that occurred before, during, and after a given incident in chronological order. Creating a timeline gave investigators a more specific overview of crime-related events, enabling them to identify patterns and gaps that could lead to other sources of evidence [7].

2.2 Instant Messaging (IM) Application Forensics

Instant messaging is crucial for digital investigators when online crimes occur. Many researchers conducted in-depth study on instant messaging forensics through digital forensic analysis on a few IM applications. A study by Rathi et al. [8] explored data storage location in different IM applications using several forensic tools. Similarly, Riadi [1] also conducted an artifacts forensics extraction between WhatsApp, Blackberry Messenger and LINE on the success of retrieving processes with certain tools.

2.2.1 WhatsApp Forensics

The increasing number of WhatsApp application users led to bad actors who took advantage of this existing app to harm innocent people [9]. Mirza et al. [10] studied threatening messages on WhatsApp to illustrate possible cybercrime might occur using technical anti-forensics approaches. WhatsApp Messenger produced artifacts on an Android smartphone which were often saved in a series of files, the names, locations, and contents [11]. Utami et al. [12] proposed a live forensic and scenario-based method that focused on the WhatsApp web application of a fraud case web. Anwar & Riadi [13] also analyzed WhatsApp Messenger's forensics on a web-based website.

2.3 Mobile Forensics

Smartphones could play a crucial role in future crime scene investigations related to digital evidence [14]. Smartphones store a lot of information and possible things, making them a perfect target for mobile forensics investigators. Mobile device forensics has two ways of acquiring digital evidence: physical and logical. There is also manual acquisition of content visual display as buttons, keyboard, or touchscreen [15]. Then, similar to the digital forensic process flow, the technique for mobile forensics was carried out [16].

2.3.1 Mobile Androids Artifacts

To recover potential evidence, investigators used methods and techniques from various digital forensics domains. Some forensics tools are required to acquire evidence from smartphones. Magnet ACQUIRE, Magnet AXIOM, Android Data Extractor Lite, Oxygen Forensics Suite and other forensics tools were mostly used by investigators. Android artifacts with Android Package (APK) samples after being analyzed in an Android analysis environment. An APK file is used to install an app. For example, APK Defined Activity, APK Embedded Libraries, APK Internal File, APK Suspicious Action and APK Suspicious Behavior can contain information stored in the device [17].

2.4 Browser Forensics

Data extracted from the browser includes bookmark, cookies, download, login, most visited sites, and history of web pages [13]. These data collected would be helpful to investigators in recovering the artifacts in a victim's browser related to cybercrime [18]. Users can access social media, read email, use internet banking, and shop through the web browser [19]. Browser forensics aims to collect artifacts connected to internet usage, especially from sources in Google's Chrome browser.

2.4.1 Google Chrome Browser Artifacts

Chrome browser saves these artifacts in the operating system's specified directories. Google Chrome stores all the data inside SQLite format [20][24]. Common artifacts possibly stored in Chrome are history, bookmarks, add-ons, extension and plugins, cache, logins, form data, favicons, session data, thumbnails, favorites and sensitive data [21]. Table 1 and Table 2 describe the structure of various artifacts and their location, and the relevant artifacts information required in the Google Chrome browser for better understanding.

Table 1: Chrome Browser Files[25]

No.	Artifacts	Location
1	History	History.sqlite
2	Cookies	Cookies.sqlite
3	Login data	Login Data.sqlite
4	Network action predictor	NetworkActionPredictor.sqlite
5	Top Sites	TopSites. sqlite
6	Bookmarks	Bookmarks. Json
7	Search Keywords	History.sqlite
8	Downloads	History.sqlite
9	Cache	Cache\

Table 2: Important Forensic Artifacts in Chrome [25]

No.	Artifacts Name	Forensically Relevant Information
1	History	URL, Title, Visit Count, Last Visit Time
2	Cookies	Host key, Name, Path, Time Stamp Information
3	Login data	Name, Type, URL, Time Stamp Information
4	Network action predictor	Id, URL, User Text, Number of Hits, Number of Misses
5	Top Sites	URL, Title, Redirect URL, Last Updated
6	Logins	URL, User Name, Sign on Realm, Date Synced
7	Downloads	Current Path, Target Path, Time Stamp Information, Referrer, MIME Type
8	Search Keywords	Searched Term, URL

2.5 Related Work

Vukadinovic [22] demonstrates the number of WhatsApp artifacts that can be recovered using web browsers and multiple forensics tools. There are 16 data types and ten data types of partially recovered artifacts were found. WhatsApp forensics conducted by Anwar and Riadi [13] shows the locations to find potential evidence from mobile and web browsers in internal and external storage and network packets. Shidek et al. [5] demonstrated visualization of WhatsApp artifacts on an Android mobile device. Researchers focused on experimenting with the timeline approach in Android smartphones.

Actoriano & Riadi [23] presented a WhatsApp forensics analysis that focused only on mobile artifacts for the study because accessing WhatsApp is synchronous in mobile and browser. Mirza et al. [10] examine the WhatsApp application in Android mobile devices by conducting a scenario-based approach. The scenario is used to analyze artifacts of chat conversation by assuming someone is cyber-harassed. Utami et al.[12] conducted a live forensic analysis on WhatsApp Web using RAM imaging technique retrieving log files, timestamps, text messages and more from the browser. The proposed study aim to forensically analyzes potential evidence from WhatsApp Web and mobile application.

The comparison of existing research about WhatsApp forensics analysis between WhatsApp web-based and WhatsApp mobile-based was shown in Table 3. Table 3 describes the overview of related works on locating artifact types retrieved from the experiment conducted and forensic tools used to extract specific artifacts. The comparative analysis presents that there are differences between both WhatsApp platforms in the context of the acquired digital evidence types. Therefore, the observation motivates this study to forensically analyze the potential evidence that can be recovered in browser and mobile devices of the WhatsApp application.

Table 3: Forensics analysis of WhatsApp artifacts

Year	Author	Forensic Analysis Technique	WhatsApp Artifacts		Forensic Tools Used
			Web-Based	Mobile-Based	
2017	[13]	Analysis of capturing artifacts	Bookmark, cookies, download, login	-	Oxygen Forensic Suite, FTK Imager, Network Mapper, SQLite Database, Wireshark Analys.
2018	[23]	Analysis of file storage location using IDFI Framework	History, cache	text messages, contact information, pictures, chat conversation, sent and received messages	DB Browser, SQLite Database, FTK Imager.

Table 4: (cont.)

Year	Author	Forensic Analysis Technique	WhatsApp Artifacts		Forensic Tools Used
			Web-Based	Mobile-Based	
2019	[22]	Analysis of locating artifacts using timestamps	text messages, delete messages, pictures, videos, voice messages, PDF file, sent contact information, log files	-	FTK Imager, MagnetAXIOM, Autopsy.
2020	[10]	Technical Anti-Forensic using scenario-based	-	text message, delete message	Belkasoft, WhatsApp DB Extractor, UFED, Oxygen Forensic Suite
2020	[5]	Visualization of WhatsApp artifacts using a timeline	-	text message, time and date conversation	FTK Imager, SQLite Database
2021	[12]	RAM forensic imaging	log files, cache, history, timestamp, text messages	-	FTK Imager, Browser History Viewer

3. Methodology

Adopting guidelines of the basic digital forensic process framework provided by the National Institute of Standards and Technology (NIST), this research presents four phases that relate to the current study. Each phase shows more details about the flow of this research in the next section.

3.1 Research Flowchart

The research methodology is divided into four phases: preparation, acquisition, analysis, and validation. The study of evidence collection and analysis methodology for WhatsApp application forensics is illustrated in Figure 1.

3.1.1 Preparation Phase

Tools related to the WhatsApp Messenger application were installed for the experiment, such as Chrome browser, WhatsApp mobile application on Android, and several forensic tools such as Magnet ACQUIRE DB Browser (SQLite) and Windows WordPad. The next phase is to create a set of experiments to simulate a user's actions. Based on WhatsApp Messenger's features, the following sets of experiments were defined by adopting the previous study by Anglano et al.[24] on the design experiments methodology. The set of the investigation is as follows:

1. The experiment involving the contacts aimed to recreate the user's contact list and the activities performed on it by the user.
2. Exchange messages experiments were targeted to create the sequence and topic of each dialog's textual and non-textual messages.
3. Test of phone calls performed to recreate the timeline of the user's phone calls made and received.

4. The experiment in conducting a group chat or call involves the user's dialogues in the group chat in which the user took part, the user's role and the group's creation date.

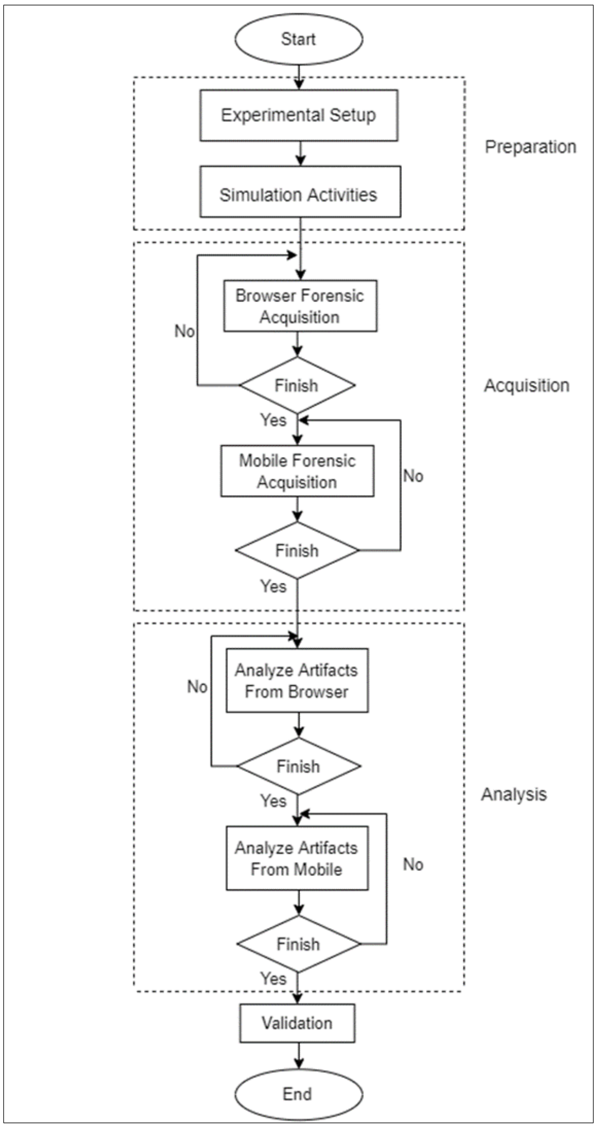


Figure 1: Research Flowchart

3.1.2 Acquisition Phase

The acquisition process for mobile forensics was divided into two categories that are logical and physical. Logical acquisition is performed to copy the data from the device and recover the logical objects stored in the mobile devices file system[14]. The physical acquisition can recover all stored data in the file system, including the deleted files.

Figure 2 and Figure 3 represent the acquisition phase flows adopted from the previous study by Cahyani et al. [25] on the data acquisition procedure.

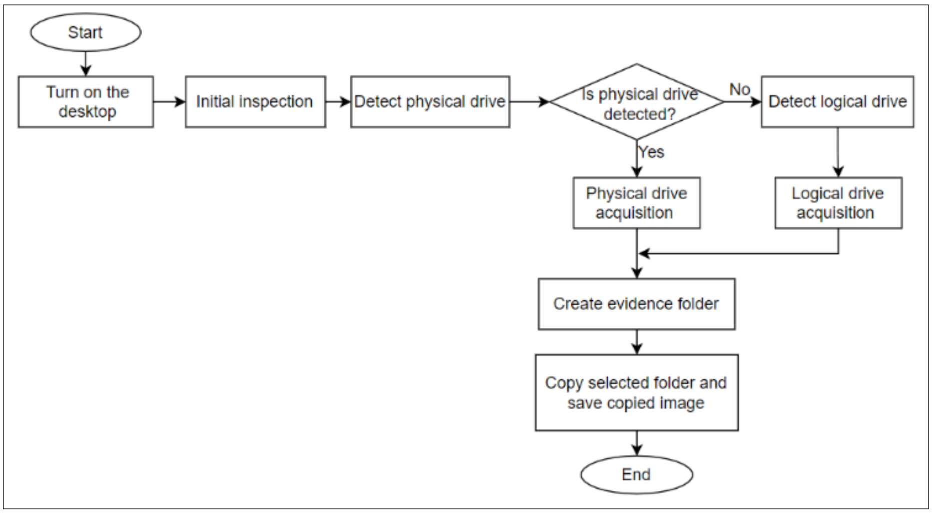

Start
Turn on the desktop
Initial inspection
Detect physical drive
Is physical drive detected?
No
Detect logical drive
Yes
Physical drive acquisition
Logical drive acquisition
Create evidence folder
Copy selected folder and save copied image
End

Figure 2: Acquisition Process in Chrome Browser

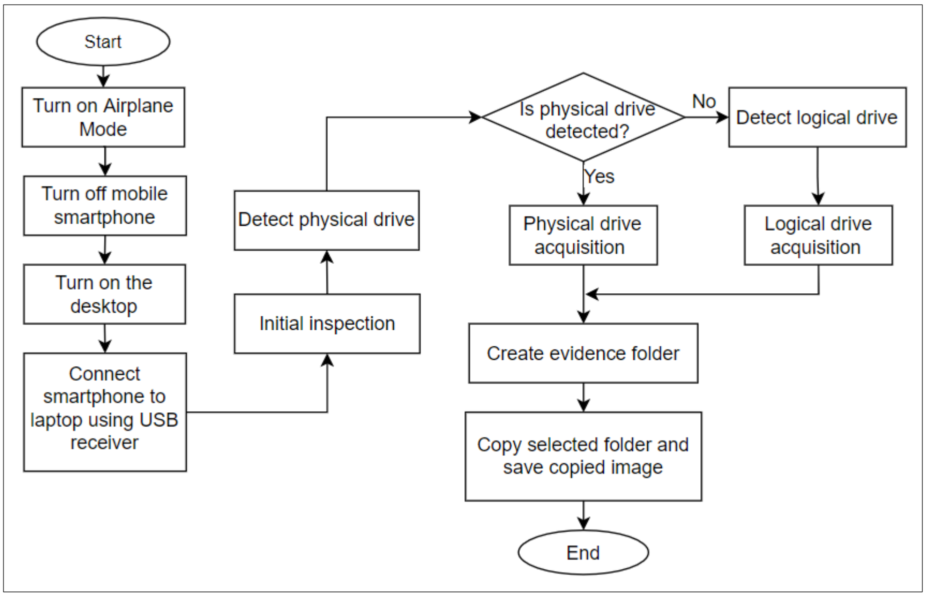

Start
Turn on Airplane Mode
Turn off mobile smartphone
Turn on the desktop
Connect smartphone to laptop using USB receiver
Initial inspection
Detect physical drive
Is physical drive detected?
No
Detect logical drive
Yes
Physical drive acquisition
Logical drive acquisition
Create evidence folder
Copy selected folder and save copied image
End

Figure 3: Acquisition Process in Mobile Device

Figure 2 presents the flows of the acquisition process for the Chrome browser forensic experiment. The initial inspection is done by checking the software and hardware used, device models, or any suspicious entries before the investigation. Meanwhile, in Figure 3, the acquisition process is conducted on Android mobile devices. The device should be switched to Airplane mode and then turned off. Check the model of the device used, model name and the IMEI number for the initial inspection.

3.1.3 Analysis Phase

Analysis of evidence includes the system storage and databases from internal devices. System storage is the main potential artifact that can be found in a browser or mobile. The analysis process on the Chrome browser and the mobile device is shown in Figure 4 and Figure 5.

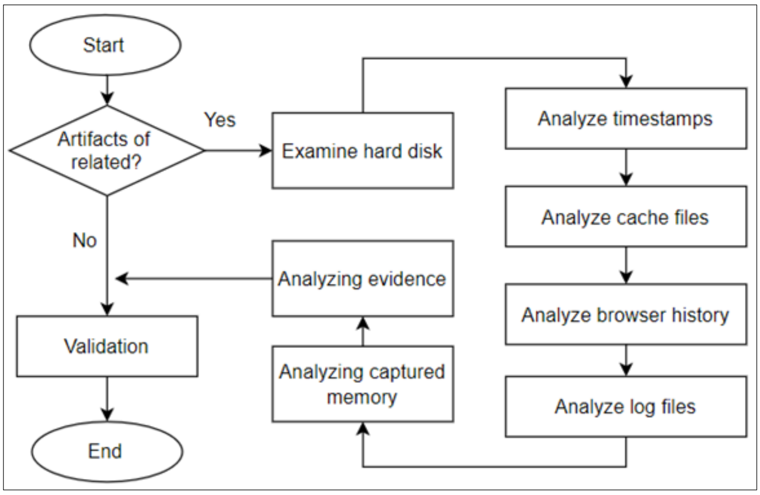


Figure 4: Analysis Process in Chrome Browser

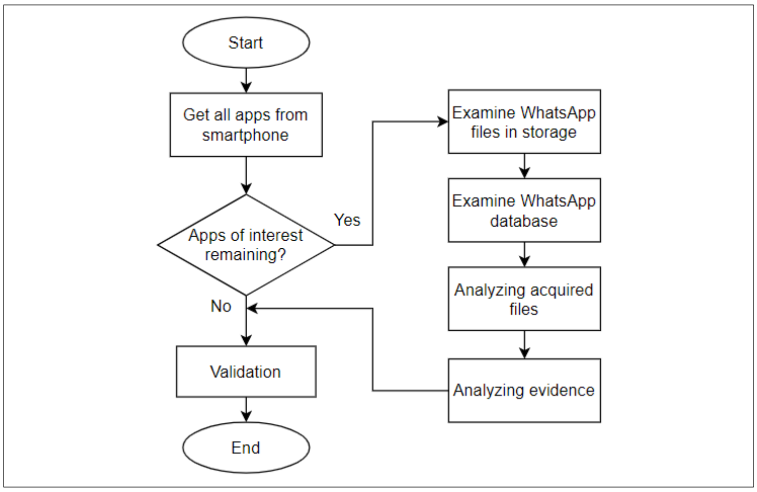

Start
Get all apps from smartphone
Apps of interest remaining?
Yes
No
Examine WhatsApp files in storage
Examine WhatsApp database
Analyzing acquired files
Analyzing evidence
Validation
End

Figure 5: Analysis Process in Mobile Device

From Figure 4, investigate the Random Access Memory (RAM) of the desktop to see if artifacts are related to the experiment. Next, analyze the potential component of the digital evidence for a browser: caches files, browser history, timestamps and log files. As shown in Figure 5, various applications were captured using several forensic tools and techniques during initial investigations. The process continues with analyzing the acquired files and evidence from the device. Lastly, it will undergo the validation process of digital proof.

3.1.4 Validation Phase

The validation step of the research technique refers to validating the results by measuring the analyzed data using a timeline approach. The findings of digital evidence, such as timestamps, must be documented since it is critical to note the continuous process throughout the examination. This is in line with a previous stud by Shidek et al.[5] that investigate WhatsApp artifacts using the timeline approach

According to the National Institute of Justice guidance[26], identify the origin of data extracted from any source, including the file system, application and user. Then, evidence should be protected from outside parties or intruders when it can be easily modified. In this study, airplane mode was turned on during acquisition. The hash values of the forensic image were checked to ensure integrity. Finally, the image file is stored in an external hard disk that was solely used for this experiment. Investigators must also detect modifications that will or may not occur during this phase. Avoid the evidence from any deletions as it must ensure it is safe to any entries without losses and must be recoverable. Next, validation data was made after all the requirements were proven valid. The steps support Daniels and Hart [26] that indicate the digital evidence must be correct and admissible to present in the court of law.

3.2 Hardware and Software

Table 4 shows details of, hardware and software specifications.

Table 5: Hardware and software specification

Device	Type	Specification
Hardware	Laptop : Illegear Onyx V	- OS: Windows 11 - CPU: Intel Core i7 @ 120Hz or 165Hz - RAM: 8GB with two slots up to 64GB - Hard Drive: 500GB NVMe SSD two M.2 slots up to 4TB - GPU: GeForce GTX 16 or RTX 30 Series Graphics
	Mobile smartphone : Samsung Galaxy S III	- OS: Android version 4.1.2 - Model: GT-I9300 - CPU: Quad-core 1.4 GHz Cortex-A9 - GPU: Mali-400MP4 - Card Slot: microSDXC - Internal Memory: 32GB 1GB RAM
Software	WhatsApp application	- WhatsApp Web version 2.2146.9 - WhatsApp mobile app version 2.22.10.73
	Google Chrome	Version 101.0.4951.67
	Magnet ACQUIRE	Version 2.0.1.6843
	DB Browser (SQLite)	Version 3.12.2
	Windows WordPad	Version 21H2

4. Result and Discussion

This section discusses the experimental setup and the simulation process of the investigation, forensic analysis of the WhatsApp application, including functionalities, location and format of WhatsApp artifacts and the result of WhatsApp metadata from mobile and browser. Lastly, the comparison of WhatsApp metadata discusses in this section.

4.1 Experimental Setup

This device undergoes a test to identify data types and artifacts that can be recovered. Device memory from Windows desktop and mobile environment will be taken using selected forensic tools shown in Figure 6, Magnet ACQUIRE for the acquisition, DB Browser (SQLite) and Windows WordPad for the forensic analysis.

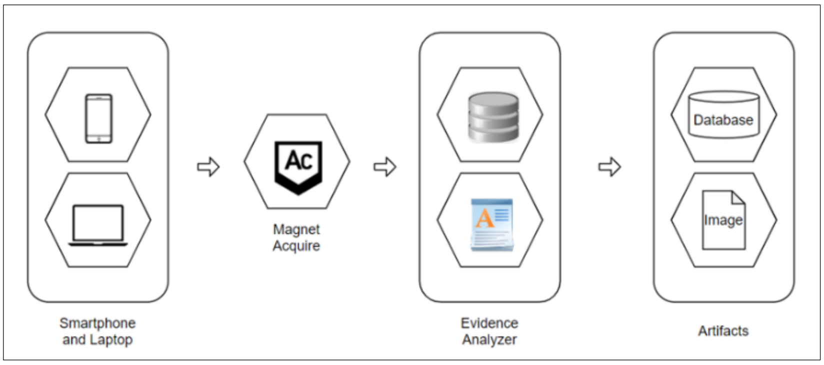


Figure 6: Forensic tools used in the simulation process

4.2 Forensic Analysis of WhatsApp

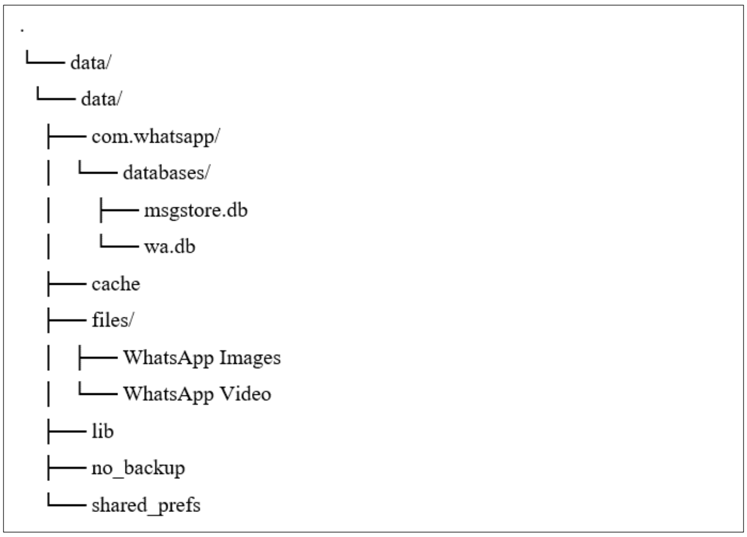
The technique used for the forensic analysis experiment is the timeline approach. Several activities were carried out to illustrate the methods used in WhatsApp before collecting evidence. Plan a scenario of scammer acts using the WhatsApp application. The planned scenario was a situation of a victim who was tricked into buying stuff online from advertisements. Next, forensic tools for the acquisition process should be implemented to handle the experiment correctly. This step directed the acquisition of the devices used during the simulation activities: smartphones and laptops. After the investigation, all the evidence related was collected from the victims and examined the case using the evidence analyzer such as DB Browser (SQLite) and Windows WordPad through the WhatsApp application.

4.2.1 Analysis of WhatsApp Functionalities

The WhatsApp application supports the exchange of textual and non-textual messages. It also works best on voice and video calls as long as there is an Internet connection. Some of the functionalities or features of WhatsApp are creating a contacts list and it can sync with contacts from a smartphone. The similar functions and special functions on WhatsApp used in smartphones and web browsers are exchange messages and group exchange chats. The unique function of the WhatsApp application used on a smartphone is adding contacts and making voice or video calls.

4.2.2 Location and Format of WhatsApp Artifacts

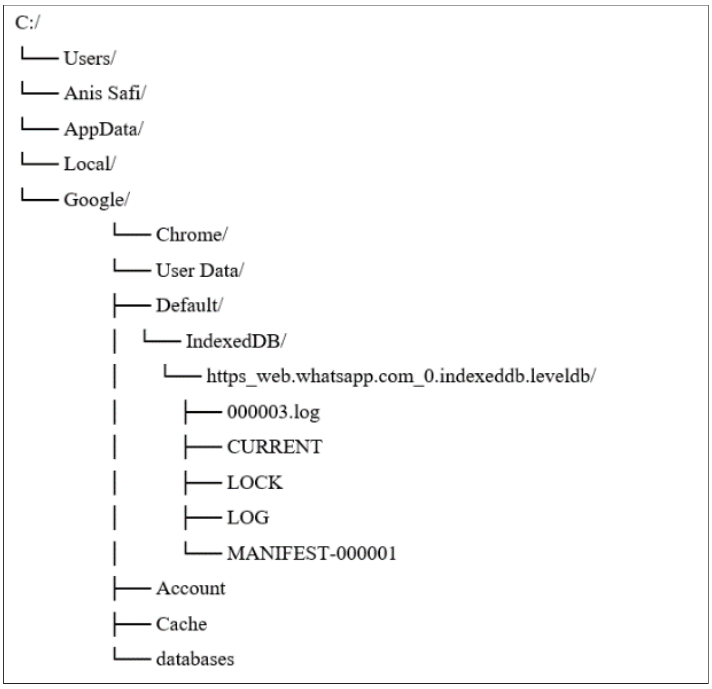
The results of experiments on the location and format of WhatsApp Messenger artifacts were predicted. Android and Windows devices have different paths when acquiring the possible location of evidence. The path would be the crucial part of an investigation where it can be the target of analyzing possible WhatsApp artifacts. Figure 7 and Figure 8 show the folders structure that was adopted from a previous study by Anglano et al.[24], where the WhatsApp application on Android and web browsers stores its artifacts.



```
.
└── data/
  └── data/
    ├── com.whatsapp/
    │   └── databases/
    │     ├── msgstore.db
    │     └── wa.db
    ├── cache
    ├── files/
    │   ├── WhatsApp Images
    │   └── WhatsApp Video
    ├── lib
    ├── no_backup
    └── shared_prefs
```

Figure 7: Structure of the folders where WhatsApp Android stores its artifacts

From Figure 7, WhatsApp android databases were located at msgstore.db and wa.db. The msgstore.db file consists of the messages table containing chat conversations of users who sent and received messages. The wa.db file contains the wa_contacts table which includes all WhatsApp contact lists of users.



```
C:/
└── Users/
└── Anis Safi/
└── AppData/
└── Local/
└── Google/
            └── Chrome/
            └── User Data/
            ├── Default/
            |   └── IndexedDB/
            |     └── https_web.whatsapp.com_0.indexeddb.leveldb/
            |        ├── 000003.log
            |        ├── CURRENT
            |        ├── LOCK
            |        ├── LOG
            |        └── MANIFEST-000001
            ├── Account
            ├── Cache
            └── databases
```

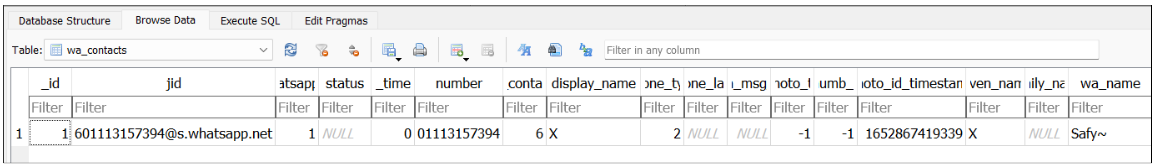
Figure 8: Structure of the folders where WhatsApp web stores its artifacts

WhatsApp Web's possible path was located in IndexedDB storage, as shown in Figure 8. From the observation, the .log file was created from .leveldb during the simulation activities. The files inside .leveldb were recorded based on when WhatsApp Web logged into the Google Chrome browser.

4.3 Analysis Results

4.3.1 WhatsApp Metadata from Android Mobile

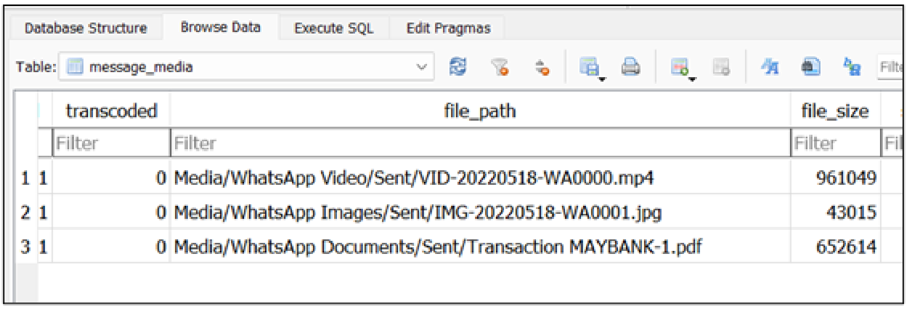
This section presents the acquired evidence findings after conducting forensic analysis with DB Browser (SQLite) and Windows WordPad. DB Browser (SQLite) analyzes the database file, msgstore.db and wa.db from Android memory. Figure 9 presents WhatsApp contact details found in wa_contacts table. Figure 10 shows the file path of WhatsApp media exchange with the file types. Finally, the chat conversation was presented in the message table of msgstore.db databases. The chat conversation in the message table can be referred to in Appendix A



	_id	jid	atsap	status	_time	number	conta	display_name	one_t	one_la	_msg	oto_	umb_	oto_id_timestan	ven_nan	ily_na	wa_name
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	601113157394@s.whatsapp.net	1	NULL	0	01113157394	6	X	2	NULL	NULL	-1	-1	1652867419339	X	NULL	Safy~

Figure 9: The wa_contacts table of wa.db database

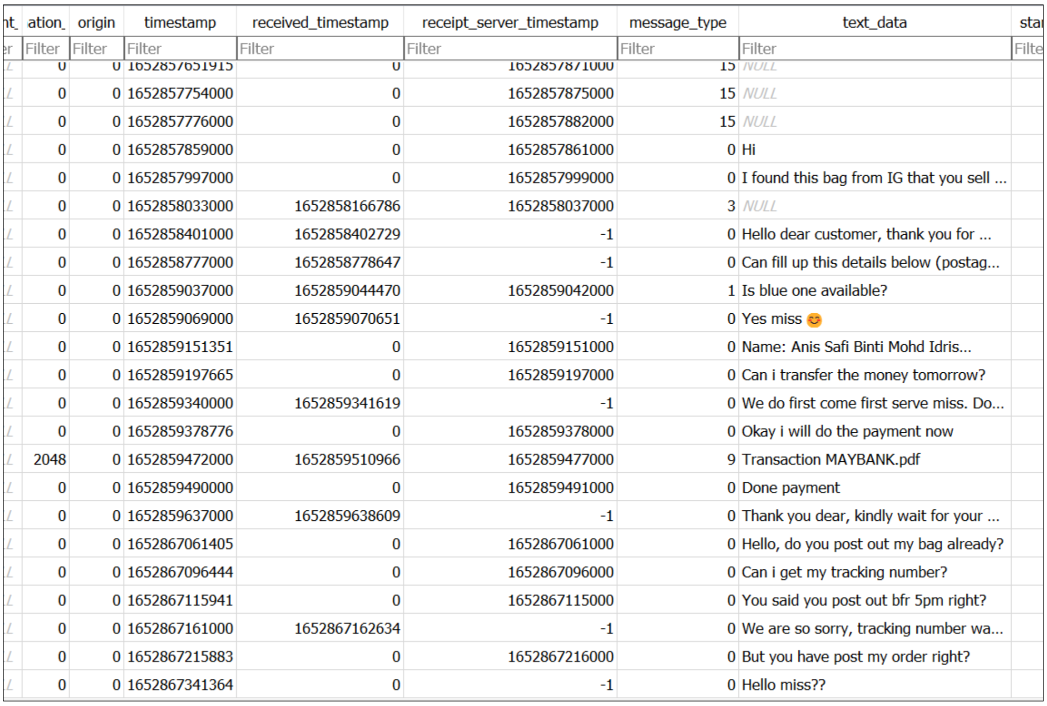
The table structure of wa_contacts describes as follows: (1) *jid*: WhatsApp ID of the contact, (2) *number*: the contact's associated phone number, (3) *display_name*: the contact's display name was saved as 'X' by the user and (4) *wa_name*: WhatsApp name that has been set in their user's profile.



		transcoded	file_path	file_size
		Filter	Filter	Filter
1	1	0	Media/WhatsApp Video/Sent/VID-20220518-WA0000.mp4	961049
2	1	0	Media/WhatsApp Images/Sent/IMG-20220518-WA0001.jpg	43015
3	1	0	Media/WhatsApp Documents/Sent/Transaction MAYBANK-1.pdf	652614

Figure 10: The message_media table of msgstore.db database

Figure 10 shows the message_media table in the Android device, which consists of the media file path. In addition, the list displays all of the attached files that were sent, along with the file's size.



nt_	ation_	origin	timestamp	received_timestamp	receipt_server_timestamp	message_type	text_data	sta
er	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filte
	0	0	1652857651915	0	1652857871000	15	NULL	
	0	0	1652857754000	0	1652857875000	15	NULL	
	0	0	1652857776000	0	1652857882000	15	NULL	
	0	0	1652857859000	0	1652857861000	0	Hi	
	0	0	1652857997000	0	1652857999000	0	I found this bag from IG that you sell ...	
	0	0	1652858033000	1652858166786	1652858037000	3	NULL	
	0	0	1652858401000	1652858402729	-1	0	Hello dear customer, thank you for ...	
	0	0	1652858777000	1652858778647	-1	0	Can fill up this details below (postag...	
	0	0	1652859037000	1652859044470	1652859042000	1	Is blue one available?	
	0	0	1652859069000	1652859070651	-1	0	Yes miss 😊	
	0	0	1652859151351	0	1652859151000	0	Name: Anis Safi Binti Mohd Idris...	
	0	0	1652859197665	0	1652859197000	0	Can i transfer the money tomorrow?	
	0	0	1652859340000	1652859341619	-1	0	We do first come first serve miss. Do...	
	0	0	1652859378776	0	1652859378000	0	Okay i will do the payment now	
	2048	0	1652859472000	1652859510966	1652859477000	9	Transaction MAYBANK.pdf	
	0	0	1652859490000	0	1652859491000	0	Done payment	
	0	0	1652859637000	1652859638609	-1	0	Thank you dear, kindly wait for your ...	
	0	0	1652867061405	0	1652867061000	0	Hello, do you post out my bag already?	
	0	0	1652867096444	0	1652867096000	0	Can i get my tracking number?	
	0	0	1652867115941	0	1652867115000	0	You said you post out bfr 5pm right?	
	0	0	1652867161000	1652867162634	-1	0	We are so sorry, tracking number wa...	
	0	0	1652867215883	0	1652867216000	0	But you have post my order right?	
	0	0	1652867341364	0	-1	0	Hello miss??	

Figure 11: The message table of msgstore.db database

As shown in Figure 11, the message table contains information such as text messages, the status of received timestamps and the files attached as described in the table structure, which (1) *key_id*: For unique message identifier, (2) *status*: Message status which, '0'=received, '4'=waiting on the server, '6'=control message and '13'=message open and read by the recipient, (3) *timestamp*: A timestamp in Unix Epoch Time (ms) format is presented, (4) *received_timestamp*: Time of the recipient's recognition and (5) *text_data*: Users' conversation lists were held on WhatsApp. Table 5 presents the findings of digital evidence of WhatsApp mobile artifacts that stored in SQLite database which shows all the chat conversations between WhatsApp users.

From Table 5, there were conversations related to scam activities around 3:10 PM to 5.49 PM. All the results of WhatsApp chats conversation that happened were analyzed using the DB browser SQLite. The exchange of messages between victim and scammer was done on May 18, 2022. Some shared files are also recorded in the list, which can be analyzed with the types of file formats displayed. The PDF file format was shown in the message table, while the other file format was displayed in the media table. This analysis result may be an important part of WhatsApp artifacts for forensics investigators and support for evidence admitted to court.

Table 6: The findings of digital evidence stored in SQLite database

No.	Evidence	Timestamp
1.	Hi	1652857859000 May 18, 2022 3:10:59 PM
2.	I found this bag from IG that you sell import bags, is it right? I'm interested with C&K product from your latest post. Is it still available?	1652857997000 May 18, 2022 3:13:17 PM
3.	Hello dear customer, thank you for asking. All our product are 100% original from the official store. The item is available. It's our hot selling product collections and comes with free accessories.	1652858401000 May 18, 2022 3:20:01 PM
4.	Can fill up this details below (postage SM=RM8, SS=10): Name: Address: Phone No: Product: Colour: Quantity: Total(inc postage): Instant transfer (only) to: MAYBANK 551584055455 Sahira Thaqif We do first come first serve to secure your order😉 Screenshot payment Thank you.	1652858777000 May 18, 2022 3:26:17 PM
5.	Is blue one available?	1652859037000 May 18, 2022 3:30:37 PM
6.	Yes miss😊	1652859069000 May 18, 2022 3:31:09 PM
7.	Name: Anis Safi Binti Mohd Idris Address: 095 Parit 11,Pasir Panjang 45400 Sekinchan, Selangor. Phone no: 01113157394 Product: C&K Colour: Blue Quantity: 1 Total(inc postage): RM200	1652859151351 May 18, 2022 3:32:31 PM
8.	Can i transfer the money tomorrow?	1652859197665 May 18, 2022 3:33:17 PM
9.	We do first come first serve miss. Do your payment ASAP to secure your order. Plus, we can post out your order before 5 PM	1652859340000 May 18, 2022 3:35:40 PM
10.	Okay i will do the payment now	1652859378776 May 18, 2022 3:36:18 PM
11.	Transaction MAYBANK.pdf	1652859472000 May 18, 2022 3:37:52 PM
12.	Done payment	1652859490000 May 18, 2022 3:38:10 PM
13.	Thank you dear, kindly wait for your order being process today. Any details we will be update later.	1652859637000 May 18, 2022 3:40:37 PM
14.	Hello, do you post out my bag already?	1652867061405 May 18, 2022 5:44:21 PM

Table 7: (cont)

No.	Evidence	Timestamp
15.	Can i get my tracking number?	1652867096444 May 18, 2022 5:44:56 PM
16.	You said you post out bfr 5 PM right?	1652867115941 May 18, 2022 5:45:15 PM
17.	We are so sorry, tracking number was not yet received	1652867161000 May 18, 2022 5:46:01 PM
18	But you have post my order right?	1652867215883 May 18, 2022 5:46:55 PM
19.	Hello miss??	1652867341364 May 18, 2022 5:49:01 PM

4.3.2 WhatsApp Metadata from Chrome Browser

The .log and LOG file can be potential evidence for WhatsApp Web artifacts. These files contain valuable information that can help during the investigation. The LOG file has been observed to be possible evidence for WhatsApp Web artifacts because it records the date and time at which the user was active.

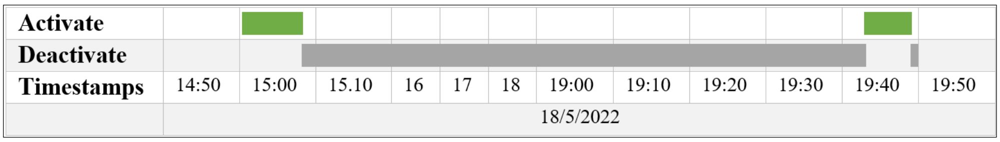


Figure 12: Timeline graph of WhatsApp Web logs activities

As shown in Figure 12, the timestamps of WhatsApp Web log activities were illustrated in a timeline graph where the time of WhatsApp activation and deactivation were used.

Table 8: User's activation in WhatsApp Web browser

No.	Timestamp	Evidence Source	Description
1.	2022/05/18 15:00:59.450	43a0 Creating DB C:\Users\Anis Safi\AppData\Local \Google\Chrome\User Data\Default\IndexedDB \https_web.whatsapp.com_0.indexeddb.leveldb since it was missing.	WhatsApp Web has been successfully logged into the browser.
2.	2022/05/18 15:00:59.454	43a0 Reusing MANIFEST C:\Users\Anis Safi\AppData \Local\Google\Chrome\User Data\Default\IndexedDB \https_web.whatsapp.com_0.indexeddb.leveldb/MANIFEST-000001	IndexedDB stores active WhatsApp Web connections.
3.	2022/05/18 15:01:32.362	da0 Manual compaction at level-0 from '\x00\x02\x00\x00\x00' @ 72057594037927935 : 1 .. '\x00\x03\x00\x00\x00' @ 0 : 0; will stop at (end)	The end of the activation in the browser that records the inactive connection.
4.	2022/05/18 19:49:32.998	1de0 Reusing MANIFEST C:\Users\Anis Safi\AppData \Local\Google\Chrome\User Data\Default\IndexedDB \https_web.whatsapp.com_0.indexeddb.leveldb/MANIFEST-000001	WhatsApp Web was reactivated, and the user opened it in a browser.

Table 9: (cont.)

No.	Timestamp	Evidence Source	Description
5.	2022/05/18 19:49:32.998	1de0 Recovering log #3	WhatsApp Web was deactivated in the browser.
6.	2022/05/18 19:49:33.046	1de0 Reusing old log C:\Users\Anis Safi\AppData \Local\Google\Chrome\User Data\Default\IndexedDB \https_web.whatsapp.com_0.indexeddb.leveldb/000003.log	The end of the activation period, during which log activities are recorded in 000003.log.

As shown in Table 6, the LOG file has been observed to be potential evidence for WhatsApp Web artifacts because it records the date and time at which the user was active. Both .log and MANIFEST files are stored in the same file. When the database is opened, the information in the .log file is converted to data points and the MANIFEST file is updated with information about the known data points. From 3:00 PM to 9:49 PM, the status of WhatsApp Web was active. The potential evidence discovered was only temporary because the Google Chrome browser analysis was done manually. The other files contain database sets, but they are unreadable and do not meet the digital evidence criteria required by the court.

4.4 Comparison of the Metadata

The possible digital evidence discussed in the acquisition phase were focused and constructed in Table 7. The artifacts in WhatsApp mobile presents more data than those in WhatsApp on the web. This study shows that the hard disk forensics technique did not acquire data remnants as much as RAM forensics. Previous research collected more data over the WhatsApp web using RAM forensics. It further indicates that WhatsApp Web does not store chat data on the hard disk. Furthermore, it can be proposed to use RAM forensics in order to collect artifacts in relation to the WhatsApp browser. Meaningful events were successfully reconstructed from both WhatsApp web-based and mobile-based applications using the timeline approach.

Table 10: Comparison of WhatsApp metadata

No.	Metadata	WhatsApp Web	WhatsApp Mobile
1.	Cache	Yes	No
2.	Login history	No	Yes
3.	Timestamps	Yes	Yes
4.	Logs	Yes	Yes
5.	Text messages	No	Yes
6.	Photos	No	Yes
7.	Video	No	Yes
8.	Call logs	No	Yes

5. Conclusion

The current study compared the forensic processes to obtain potential digital evidence from WhatsApp web-based and mobile-based applications. This study discovered and analyzed WhatsApp artifacts such as timestamps, media, and logs. The acquired evidence on each WhatsApp environment was recorded as different in the analysis result during the investigation. The acquired artifacts from the two WhatsApp application environments were retrieved in different paths and locations where the evidence could be found. The final objectives indicated the timeline approach used and were successfully observed and compared with two WhatsApp apps. This technique records proof of date and periods for both WhatsApp apps.

Evidence from WhatsApp Web-based applications can be valuable to use in court cases. There are several ways to conduct further research through different environments such as WhatsApp desktop clients. Further research should address discovering more data and information using the WhatsApp desktop application, which saves the WhatsApp folder rather than the browser. Future works should consider producing more WhatsApp artifacts such as cache, media, call logs, and images such as conducting RAM analysis. WhatsApp web can be accessed on any browser that mirrors chat conversations and messages from mobile devices. Microsoft Edge, Safari, Mozilla Firefox, and Opera have supported browsers using WhatsApp Web on a computer. Future work should also consider using iOS, Windows Phone OS, or Symbian.

Acknowledgement

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

References

[1] A. F. Imam Riadi, “Forensic Analysis of Android-based Instant Messaging Application,” *12th Int. Conf. Telecommun. Syst. Serv. Appl.*, 2018, doi: 10.1109/TSSA.2018.8708798.

[2] Dr K Rama Subramaniam, “Digital Forensics – As we know it today …,” *Valiant Technol. Pvt Ltd*, vol. 13, no. 4, pp. 89–92, 2018.

[3] M. Kaur, N. Kaur, and S. Khurana, “A Literature review on Cyber Forensic and its Analysis tools,” *Ijarcce*, vol. 5, no. 1, pp. 23–28, 2016, doi: 10.17148/ijarcce.2016.5106.

[4] K. Nadeem, N. Saeed, and N. Ahmed, “A Comparative Study of Digital Forensics and Cybercrime Investigation,” *Comput. Appl. Sci. www.erjsciences.info*, vol. 2, pp. 161–171, 2020, [Online]. Available: www.erjsciences.info.

[5] H. Shidek, N. Cahyani, and A. A. Wardana, “WhatsApp Chat Visualizer: A Visualization of WhatsApp Messenger’s Artifact Using the Timeline Method,” *Int. J. Inf. Commun. Technol.*, vol. 6, no. 1, p. 1, 2020, doi: 10.21108/ijoict.2020.61.489.

[6] E. Qawasmeh and M. I. Al-Saleh, “On Producing Events Timeline for Memory Forensics: An Experimental Study,” *2020 7th Int. Conf. Inf. Technol. Trends, ITT 2020*, vol. 2020-Janua, 2020, doi: 10.1109/ITT51279.2020.9396748.

[7] Eoghan Casey, *Handbook of Digital Forensics and Investigation*, Elsevier A. Burlington, USA: Elsevier Inc., 2010.

[8] K. Rathi, U. Karabiyik, T. Aderibigbe, and H. Chi, “Forensic analysis of encrypted instant messaging applications on Android,” *6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding*, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/ISDFS.2018.8355344.

[9] F. E. Salamh, U. Karabiyik, and M. K. Rogers, “Asynchronous forensic investigative approach to recover deleted data from instant messaging applications,” *2020 Int. Symp. Networks, Comput. Commun. ISNCC 2020*, 2020, doi: 10.1109/ISNCC49221.2020.9297227.

[10] M. Mirza, F. E. Salamh, and U. Karabiyik, “An Android Case Study on Technical Anti-Forensic Challenges of WhatsApp Application,” *8th Int. Symp. Digit. Forensics Secur. ISDFS 2020*, 2020, doi: 10.1109/ISDFS49300.2020.9116192.

[11] S. Adwan and F. Salamah, “A Manual Mobile phone forensic approach towards the analysis of WhatsApp Seven-Minute Delete Feature,” *21st Saudi Comput. Soc. Natl. Comput. Conf. NCC 2018*, no. January, pp. 1–5, 2018, doi: 10.1109/NCG.2018.8593153.

[12] S. D. Utami, C. Carudin, and A. A. Ridha, "Analisis Live Forensic Pada Whatsapp Web Untuk Pembuktian Kasus Penipuan Transaksi Elektronik," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 24–32, 2021, doi: 10.14421/csecurity.2021.4.1.2416.

[13] N. Anwar and I. Riadi, "Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web," *J. Ilm. Tek. Elektro Komput. dan Inform.*, vol. 3, no. 1, p. 1, 2017, doi: 10.26555/jiteki.v3i1.6643.

[14] G. Grispos, T. Storer, and W. B. Glisson, "A comparison of forensic evidence recovery techniques for a windows mobile smart phone," *Digit. Investig.*, vol. 8, no. 1, pp. 23–36, 2011, doi: 10.1016/j.diin.2011.05.016.

[15] John Sammons, "Mobile device forensics," *The Basics of Digital Forensics The Primer for Getting Started in Digital Forensics*, 2015. https://www.sciencedirect.com/topics/computer-science/logical-acquisition (accessed Nov. 09, 2021).

[16] S. C. Sathe and N. M. Dongre, "Data acquisition techniques in mobile forensics," *Proc. 2nd Int. Conf. Inven. Syst. Control. ICISC 2018*, no. Icisc, pp. 280–286, 2018, doi: 10.1109/ICISC.2018.8399079.

[17] P. N. Alto, "Android Artifacts," *Aug 02, 2021*, 2021. https://docs.paloaltonetworks.com/autofocus/autofocus-admin/autofocus-search/artifact-types/android-artifacts.html (accessed Nov. 09, 2021).

[18] D. Rathod, "Web Browser Forensics: Google Chrome Available Online at www.ijarcs.info," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. December, pp. 5–9, 2017, doi: 10.26483/ijarcs.v8i7.4433.

[19] 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.

[20] H. Said, N. Al Mutawa, I. Al Awadhi, and M. Guimaraes, "Forensic analysis of private browsing artifacts," in *2011 International Conference on Innovations in Information Technology*, 2011, pp. 197–202, doi: 10.1109/INNOVATIONS.2011.5893816.

[21] N. Malviya, "Browser forensics: Google chrome," *Sept 16, 2020*, 2020. https://resources.infosecinstitute.com/topic/browser-forensics-google-chrome/ (accessed Nov. 08, 2021).

[22] N. V. Vukadinovic, "WhatsApp Forensics: Locating Artifacts in Web and Desktop Clients," *Master's Thesis, Purdue Univ. Grad. Sch.*, no. May, 2019.

[23] B. Actoriano and I. Riadi, "Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation Framework Version 2," *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 4, pp. 410–419, 2018, [Online]. Available: http://sdiwc.net/digital-library/forensic-investigation-on-whatsapp-web-using-framework-integrated-digital-forensic-investigation-framework-version-2.

[24] C. Anglano, M. Canonico, and M. Guazzone, "Forensic analysis of Telegram Messenger on Android smartphones," *Digit. Investig.*, vol. 23, no. December, pp. 31–49, 2017, doi: 10.1016/j.diin.2017.09.002.

[25] N. D. W. Cahyani, N. H. Ab Rahman, Z. Xu, W. B. Glisson, and K.-K. R. Choo, "The role of mobile forensics in terrorism investigations involving the use of cloud apps," 2016, doi: 10.4108/eai.18-6-2016.2264416.

[26] D. J. Daniels and S. V Hart, "Forensic Examination of Digital Evidence: A Guide for Law Enforcement," 2004, [Online]. Available: https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=199408.