Browser Forensic of Extortion Case on WhatsApp Web using National Institute of Justice Method

Cindy Amelia
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
UniversitasAhmad Dahlan
Yogyakarta of Indonesia

ABSTRACT

Whatsapp is a messaging application for smartphones that can be used across platforms including Apple iOS, Android, Windows Phone, etc. popularity Whatsapp's among the public can be misused for negative purposes for the development of society itself. One example of a case that often occurs in the community is extortion through the application Whatsapp. This study will carry out a scenario of a crime of extortion that occurs using Whatsapp Web, Whatsapp runs on the Chrome Browser, this research uses the NIJ stage. The stages of the forensics National Institute of Justice (NIJ)are preparation, collection, examination, analysis, and reporting. This research uses a laptop with a condition that is connected to the internet and accesses Whatsapp via the Chrome browser. The process of collecting digital evidence through forensic tools, namely Belkasoft RAM Capturer, FTK Imager, Browser History Capturer, and Browser History Examiner. This research produces digital evidence, namely information on profile photos of perpetrators and victims, when accessing WhatsApp Web, WhatsApp Weblinks accessed via Chrome, as well as evidence of extortion chats that have been deleted by the perpetrators. The percentage of results obtained from the results of imaging data analysis using the FTK Imager tool is 50% in the form of a WhatsApp Web link and chat from the perpetrator to the victim, while the results from the Browser History Examiner are 50% in the form of a cache of the photo perpetrator, as well as the access time WhatsApp.This research uses the stages of the National Institute of Justice (NIJ), it is hoped that future research can use other stages. This research uses OS Windows 10, so it is hoped that for further research it can use OS Linux or macOS.

Keywords

Forensics, Chrome, WhatsApp Web, Extortion, NIJ

1. INTRODUCTION

The rapid development of instant messaging and social media application technology has facilitated people in living their daily lives, current instant messaging applications such as Whatsapp, Line, SMS, messenger, is not only used to share the news with family or friends but can be a place to earn a living. The growth of social media and instant messaging applications has facilitated many serious crimes.[1] These irresponsible individuals continue to change their strategy to utilize social media services and instant messaging applications to fulfill their own interests without thinking about the impact on others.Whatsapp is a messaging application for smartphones that can be used across platform.[2]Whatsapp uses internet data packages to send instant messages, by using Whatsapp one can have chatted online, share files, videos, and photos as well as other interesting features.[3]popularityWhatsapp's among the public can be misused for negative purposes for the development of society itself. One example of a case that often occurs in the community is extortion through the application Whatsapp.

1.1 Study Literature

1.1.1 Previous Study

The first previous research was entitled "Analysis of Forensic Investigations Whatsapp Messenger Smartphone AgainstWhatsapp Based Web-". This research shows that one can get complete access to all information on Whatsapp, be it Whatsapp Smartphone or Whatsapp Web[4]. Most chat applications follow the same pattern of synchronizing messages, contacts, and user data when syncing and updating conversation data periodically.[5] The approach taken gives a general outline for all similar applications that run on platforms Android and Windows such as Telegram and the like. This research can be useful for Mobile Forensic Analysis and Investigation on Android smartphones and multiple applications web-based browsers.[6]

A previous research both entitled "Analysis of Digital Evidence Whatsapp on Android Smartphone UsingMethods". Live ForensicFrom the results of the identification carried out by analyzing the evidence on the Android Smartphone, it can be concluded that the acquisition, processes imaging and analysis run smoothly using the mobile edit application version 9.0.[7]

The third previous research entitled "Identification of Whatsapp Digital Evidence on Proprietary Operating Systems Using Live Forensic". This research states that live forensic techniques can be applied to the process of retrieving digital evidence from the desktop-based Whatsapp IM application on the Windows 8 operating system using the forensic tools FTK Imager. Digital evidence is obtained in the form of texts of Whatsapp conversations that occurred between the suspect and the victim which can be used as digital evidence related to cases of online shop fraud that occurred.[8]

The fourth previous research entitled "Live Forensic Analysis for Comparison of Instant Messenger Applications on the Windows 10 Operating System".[9] This research analyzes IM applications, namely Line Messenger, Facebook Messenger, and Telegram Messenger and obtains the results that the application of live forensic techniques to obtain digital evidence of activities using IM applications requires different tools and techniques, techniques and tools for live forensics itself also cannot be used on a long time, because if the RAM dies, dumping and analysis of evidence cannot be carried out.[10]

The fifth previous research entitled "Acquisition of Digital

Evidence on Android-Based Instagram Messenger Using the National Institute of Justice (NIJ) Method". The research was conducted to obtain digital evidence from the two smartphones used in cyberbullying cases. The data acquisition process uses the NIJ method which recommends several stages such as preparation, collection, examination, analysis, and reporting.[11] The acquisition process was carried out using the Oxygen Forensic application so as to get the desired results, namely digital evidence in the form of images/photos and conversations from social media Instagram installed on the smartphone. The process of acquiring digital evidence that was successfully obtained on Instagram on a smartphone in Root condition obtained the expected data in the form of photos and conversations while for smartphones that were not in Root condition the expected digital evidence was not obtained.[12]

1.1.2 Digital Forensics

Forensics is one of the branches of science used for the investigation and discovery of digital device content, the term digital forensics was originally synonymous with computer forensics, but has now been expanded to investigate all devices that can store digital data. Digital forensics is a discipline derived from computer security that deals with the finding of digital evidence after an event have occurred. Digital forensics activity itself is a process of identifying, maintaining, analyzing, and using digital evidence according to applicable law.[13]

1.1.3 Live Forensics

Basically live forensics has similarities with traditional forensic techniques in terms of the methods used, namely identification, storage, analysis, and presentation, only live forensics is a response to the shortcomings of traditional forensic techniques which cannot get information from data and information that only exists. when the system is running, for example, activities memory, network processes, swap files, running system processes, and information from files system.[14]

1.1.4 Computer Forensics

Forensics is the process of obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases. Computer forensics is also often referred to as digital forensics, information technology forensics, or data forensics which is an investigative process in which researchers identify, maintain, analyze digital evidence consisting of various types.[15]

1.1.5 Digital Evidence

Evidence is information stored or transmitted inform a *binary* that can be used in court. Digital evidence is generally related to digital crimes such as crimes that use social media as a place to commit crimes so that digital evidence can be used to help prosecute all types of digital crimes.[16] Digital evidence is so susceptible to alteration that it can affect its authenticity if not handled properly. Any kind of alteration that contains digital evidence will lead to wrong conclusions, or the evidence will be unusable.[17]

1.1.6 WhatsApp Web

WhatsApp Web in principle functions to open an account WhatsApp via a computer device. This feature in the early period is easier to use over the web. The developer provides the barcode that needs to be scanned through the application WhatsApp mobile.[18] Scanning will directly open the application WhatsApp according to the working account on the smartphone used for scanning. Conversations contained in the application WhatsApp on smartphones will also be displayed on the version web. Synchronization will be done automatically if there is a change in one of the active applications.[19]

1.1.7 Cybercrime

In conducting investigations and analysis of a criminal case, both cybercrimeand conventional, an investigator must be able to position himself as a criminal (criminologist) in order to help facilitate investigation and case solving.[20] Because a criminologist of course already understands all kinds of crimes that are often committed by criminals which include social phenomena and actions that violate the law and the norms of society that apply.[21]

1.1.8 Chrome Browser

Google Chrome is a browser released by Google, the world's largest and leading search engine company. Google Chrome is also designed to run as fast as possible.[22] Chrome was first released by Google on September 2, 2008 when it was only for Microsoft Windows because it was still in beta status. Then on December 11, 2008, Google Chrome was released for all types of operating systems because it already has a stable version. And as of January 2012, Google Chrome is estimated to have reached 25-28% of all global browser users.[23]

1.1.9 National Institute of Justice (NIJ)

National Institute of Justice (NIJ) is the research, development, and evaluation agency of the United States Department of Justice. [24]

PREPARATION
COLECTION
EXAMINATION
ANALYSIS
REPORTING

Figure 1.Stages of NIJ Method

Figure 1 shows the standard steps of the NIJ, the explanation of these steps is as follows[25] :

a. *Preparation,*this stage is carried out by preparing the tools and materials needed to complete tasks during the investigation.
b. *Collection,* at this stage, activities are carried out to find data and information that can support the investigation process, as well as collect them and make copies of data obtained.
c. *Examination,* this stage is carried out searching for information data from data that has been collected in the previous stage which can be used as evidence. At this stage, the process of making digital evidence and document contents from the data obtained is seen as.
d. *Analysis,* this stage the activity of analyzing digital evidence from data that has been filtered in the previous stage to determine the significance and proof of.
e. *Reporting,* this stage is information presentationobtained from the stage Analysis.

2. METHODOLOGY

2.1 Research Scenario

Several steps were taken to find data that could potentially become evidence, namely preparation, collection, and examination. Volatile data was obtained from the live forensic method in the form of conversational texts and delivery times, as well as usernames and passwords as additional data. The chrome browser will get information in the form of a history of web visits, access times, and cache images of images sent by perpetrators. In the analysis of this research, it aims to create case scenarios for research regarding the search for evidence of crimes cyber that occurred on WhatsApp. Web running on browser Google Chrome. Figure 2 describes the perpetrator accessing WhatsApp Web through the Chrome browser that has been installed on the laptop. The perpetrator sent a message to the victim through his WhatsApp account.

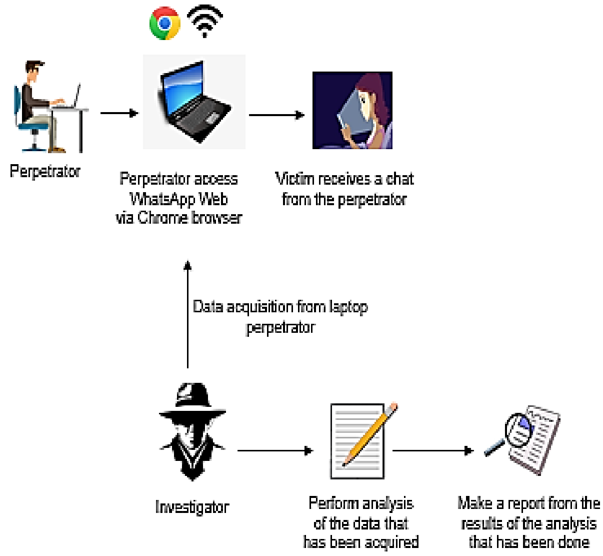

Perpetrator
Perpetrator access WhatsApp Web via Chrome browser
Victim receives a chat from the perpetrator
Data acquisition from laptop perpetrator
Investigator
Perform analysis of the data that has been acquired
Make a report from the results of the analysis that has been done

Figure 2.Flow of the Case Scenario on WhatsApp Web

Figure 2 shows the perpetrator accessing WhatsApp Web using the Chrome web browser that has been installed on the perpetrator's laptop. The perpetrator sent a message to the victim through his account WhatsApp. The victim felt aggrieved, finally, the victim reported it to the police by bringing a screenshot of the conversation between the victim and the perpetrator so that the police formed a team to resolve the case and arrest the culprit. When the arrest was made, the police secured the crime scene along with the evidence found.

2.2 Research Stages

The stages of this research as stated in the case research simulation process can be carried out by trying to find and obtain evidence of a crime on the application WhatsApp Web. The stages of this research refer to the standard stages of National Institute of Justice(NIJ), namely Preparation, Collection, Examination, Analysis, and Reporting.

2.2.1 Preparation

At the preparation stage, what needs to be done is to prepare the equipment and materials that will be used in the investigation stage carried out by the investigator.

Table 1. Tools and Materials

No	Tools and Materials	Description
1	Laptop	Acer Travelmate P645-S
2	Google Chrome ver 89.0.4389.114	Browser
3	RAM Capturer 64-bit version	RAM acquisition tools
4	FTK Imager ver. 4.2.1.4	Imaging tools
5	Browser History Capturer ver. 1.2.7	Browser data capture tools
6	Browser History Examiner ver. 1.14.1	Browser data analysis tools

In Table 1 are the tools and materials that will be used in analyzing and acquiring data from the evidence that has been found.

2.2.2 Collection

At this stage, the evidence is secured with the aim of protecting the authenticity of the evidence.

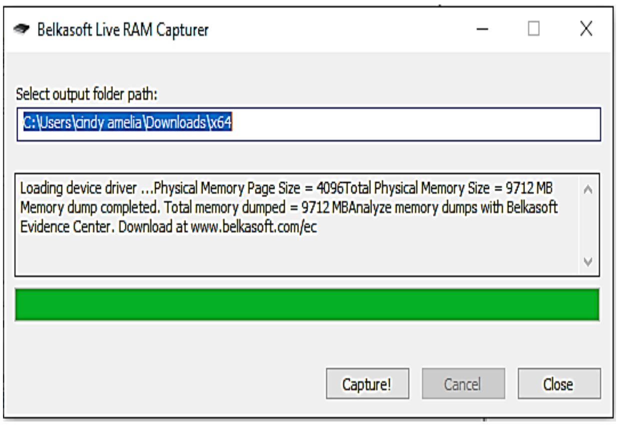
Table 2. Physical Evidence Found

No	Name of Evidence	Figure	Description
1	Laptop		Perpetrator's laptop was found to be turned on and connected to the Internet
2	Charger		Charging cable used by the perpetrator

In Table 2 there are photos of evidence that have been collected by the police and then submitted to investigators.The evidence obtained is electronic evidence in the form of a laptop using the Windows operating system and in it there is a Google Chrome browser which is a communication tool used by perpetrators to commit cybercrime.

2.2.3 Examination

At the RAM data acquisition stage using forensic tools Belkasoft Live RAM Capturer, these tools are used for the acquisition of data stored in RAM electronic evidence found. The acquisition takes time, this time depends on the amount of RAM memory on the perpetrator's laptop.

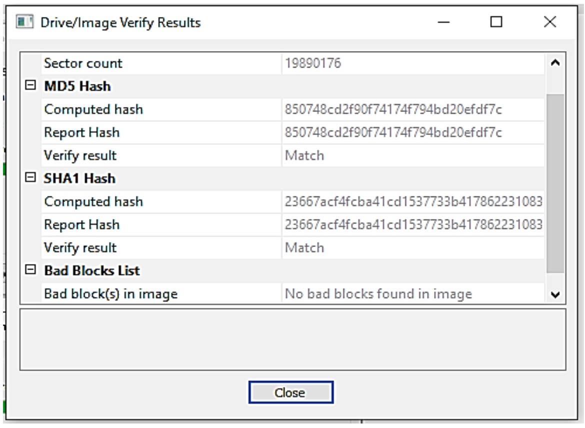


C:\Users\cindy amelia\Downloads\x64

```
Loading device driver ...Physical Memory Page Size = 4096Total Physical Memory Size = 9712 MB
Memory dump completed. Total memory dumped = 9712 MBAnalyze memory dumps with Belkasoft
Evidence Center. Download at www.belkasoft.com/ec
```

Figure 3. RAM Capturer Acquired Successfully

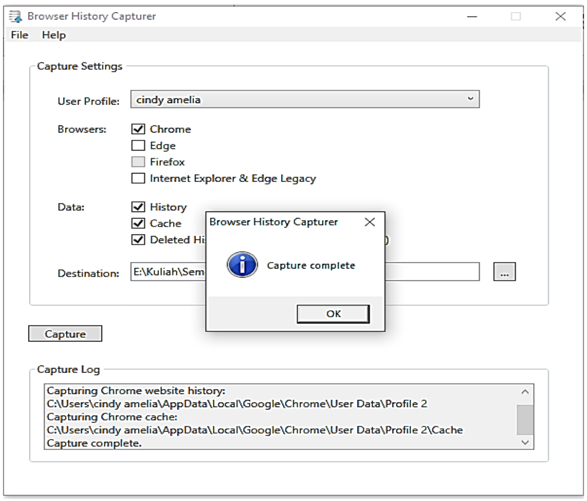
Figure 3 is the display of Belkasoft Live RAM Capturer on the initial screen. The column 'Select output folder path' is a column to write down the folder used to store the acquisition file. The RAM capture results are stored on the C:\Users\cindy amelia\Downloads\x64 drive with a file size of 9712 MB.After the volatile data in RAM has been successfully acquired, imaging is carried out to maintain data integrity and stored in other media storage and inspections are carried out.


Drive/Image Verify Results

Sector count	19890176
⊟ **MD5 Hash**	
Computed hash	850748cd2f90f74174f794bd20efdf7c
Report Hash	850748cd2f90f74174f794bd20efdf7c
Verify result	Match
⊟ **SHA1 Hash**	
Computed hash	23667acf4fcba41cd1537733b417862231083
Report Hash	23667acf4fcba41cd1537733b417862231083
Verify result	Match
⊟ **Bad Blocks List**	
Bad block(s) in image	No bad blocks found in image

Figure 4. theHashing Results of RAM

Figure 4 shows the hash value of the data imaging results that have been carried out, it can be seen that the hash value on MD5 and SHA1 of the verified imaging file matches or is the same as the hash value on MD5 and SHA1 of the original file. This means if the hash value of the imaging file and the original file shows the same, then the imaging process is perfect and there are no changes to the file.


Browser History Capturer

Capture Settings

User Profile: cindy amelia

Browsers:
☑ Chrome
☐ Edge
☐ Firefox
☐ Internet Explorer & Edge Legacy

Data:
☑ History
☑ Cache
☑ Deleted Hi

Destination: E:\Kuliah\Sem

Browser History Capturer

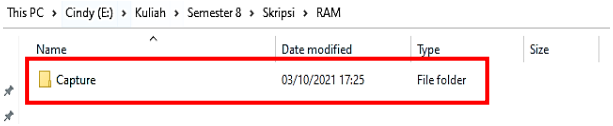
Capture complete

Capture Log

```
Capturing Chrome website history:
C:\Users\cindy amelia\AppData\Local\Google\Chrome\User Data\Profile 2
Capturing Chrome cache:
C:\Users\cindy amelia\AppData\Local\Google\Chrome\User Data\Profile 2\Cache
Capture complete.
```

Figure 5. Display of Browser History Capturer

In figure 5 shows the browser history capturer when successfully capturing data from the chrome browser, the data captured by the capturer is stored on drive E:\Lectures\Semester 8\Thesis\RAM.


This PC › Cindy (E:) › Kuliah › Semester 8 › Skripsi › RAM

Name	Date modified	Type	Size
Capture	03/10/2021 17:25	File folder	

Figure 6.Capture Results File of Browser Chrome

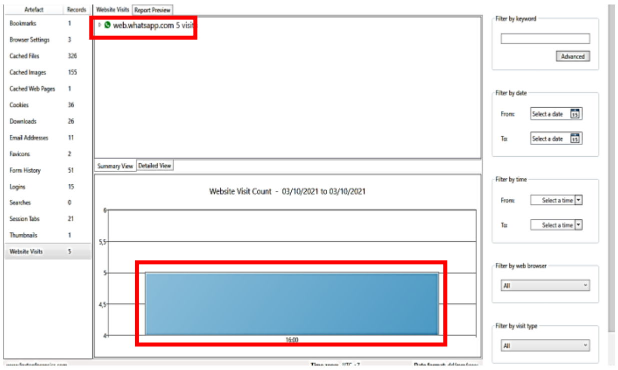
Figure 6 shows the capturer files from the Browser History Capturer tools have been saved in a folder called Capture.

2.2.4 *Analysis*

The analysis stage is the process of searching for information in the form of digital evidence that has been data acquisition from RAM. The information sought is evidence of the perpetrator's chat threatening the victim which has been deleted by the perpetrator. This analysis uses forensic tools, namely Belkasoft RAM Capturer, FTK Imager, Browser History Capturer, and Browser History Examiner.

2.2.4.1 *Browser History Examiner*

Tools Browser History Examiner serves to check the capture results that have been done previously using the Browser History Capturer tool. At this stage, the data to be used is the data contained in the Capturer folder.At this stage will obtain information on the Chrome browser in the form of Browser Settings, Cache, Cookies, Bookmarks, History Website Visited, and others.



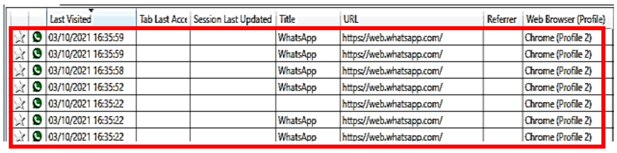
Artefact	Records
Bookmarks	1
Browser Settings	3
Cached Files	326
Cached Images	155
Cached Web Pages	1
Cookies	36
Downloads	26
Email Addresses	11
Favicons	2
Form History	51
Logins	15
Searches	0
Session Tabs	21
Thumbnails	1
Website Visits	5

web.whatsapp.com 5 visit

Website Visit Count - 03/10/2021 to 03/10/2021

Figure 7.ResultData History Chrome

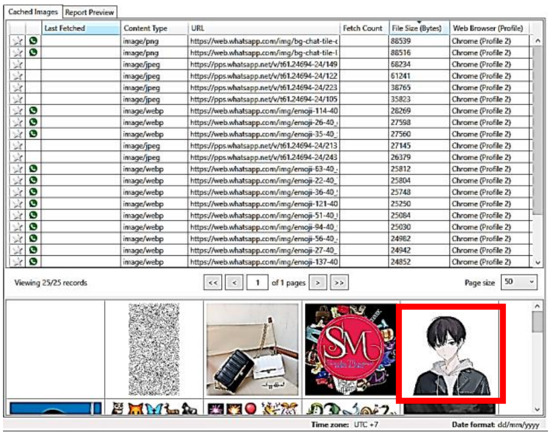
Figure 7 shows the historical data contained in the Capture folder, based on the history data that was successfully obtained, it can be seen that Whatsapp Web was accessed on October 3, 2021, at 16:00.



		Last Visited	Tab Last Acce	Session Last Updated	Title	URL	Referrer	Web Browser (Profile)
☆	●	03/10/2021 16:35:59			WhatsApp	https://web.whatsapp.com/		Chrome (Profile 2)
☆	●	03/10/2021 16:35:59			WhatsApp	https://web.whatsapp.com/		Chrome (Profile 2)
☆	●	03/10/2021 16:35:58			WhatsApp	https://web.whatsapp.com/		Chrome (Profile 2)
☆	●	03/10/2021 16:35:52			WhatsApp	https://web.whatsapp.com/		Chrome (Profile 2)
☆	●	03/10/2021 16:35:22				https://web.whatsapp.com/		Chrome (Profile 2)
☆	●	03/10/2021 16:35:22			WhatsApp	https://web.whatsapp.com/		Chrome (Profile 2)
☆	●	03/10/2021 16:35:22			WhatsApp	https://web.whatsapp.com/		Chrome (Profile 2)

Figure 8. Activity Browser Access WhatsApp Web

In Figure 8 it can be seen that https://web.whatsapp.com/ was accessed on October 3, 2021, at 16:35:22 using the Chrome browser.



Cached Images | Report Preview

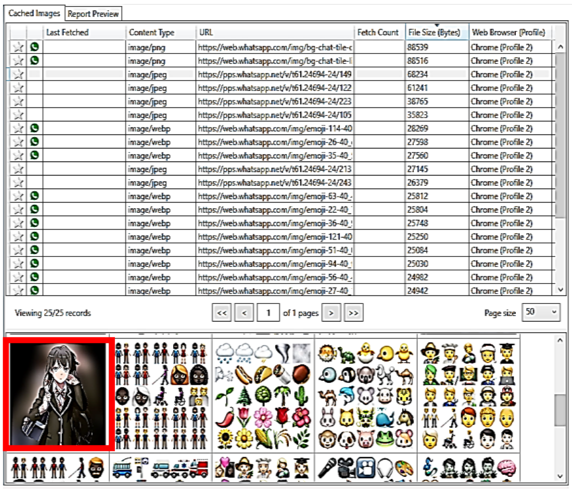
		Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser (Profile)
☆	●		image/png	https://web.whatsapp.com/img/bg-chat-tile-c		88539	Chrome (Profile 2)
☆	●		image/png	https://web.whatsapp.com/img/bg-chat-tile-l		88516	Chrome (Profile 2)
☆			image/jpeg	https://pps.whatsapp.net/v/t61.24694-24/149		68234	Chrome (Profile 2)
☆			image/jpeg	https://pps.whatsapp.net/v/t61.24694-24/122		61241	Chrome (Profile 2)
☆			image/jpeg	https://pps.whatsapp.net/v/t61.24694-24/223		38765	Chrome (Profile 2)
☆			image/jpeg	https://pps.whatsapp.net/v/t61.24694-24/105		35823	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-114-40		28269	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-26-40_		27598	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-35-40_		27560	Chrome (Profile 2)
☆			image/jpeg	https://pps.whatsapp.net/v/t61.24694-24/213		27145	Chrome (Profile 2)
☆			image/jpeg	https://pps.whatsapp.net/v/t61.24694-24/243		26379	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-63-40_		25812	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-22-40_		25804	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-36-40_		25748	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-121-40		25250	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-51-40_		25084	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-94-40_		25030	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-56-40_		24982	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-27-40_		24942	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-137-40		24852	Chrome (Profile 2)

Viewing 25/25 records

Time zone: UTC +7 Date format: dd/mm/yyyy

Figure 9.Image Cached of perpetrator's profile photo

Figure 9 shows the cache of the perpetrator profile photo circled by a red box.



Cached Images | Report Preview

		Last Fetched	Content Type	URL	Fetch Count	File Size (Bytes)	Web Browser (Profile)
☆	●		image/png	https://web.whatsapp.com/img/bg-chat-tile-c		88539	Chrome (Profile 2)
☆	●		image/png	https://web.whatsapp.com/img/bg-chat-tile-l		88516	Chrome (Profile 2)
☆			image/jpeg	https://pps.whatsapp.net/v/t61.24694-24/149		68234	Chrome (Profile 2)
☆			image/jpeg	https://pps.whatsapp.net/v/t61.24694-24/122		61241	Chrome (Profile 2)
☆			image/jpeg	https://pps.whatsapp.net/v/t61.24694-24/223		38765	Chrome (Profile 2)
☆			image/jpeg	https://pps.whatsapp.net/v/t61.24694-24/105		35823	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-114-40		28269	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-26-40_		27598	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-35-40_		27560	Chrome (Profile 2)
☆			image/jpeg	https://pps.whatsapp.net/v/t61.24694-24/213		27145	Chrome (Profile 2)
☆			image/jpeg	https://pps.whatsapp.net/v/t61.24694-24/243		26379	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-63-40_		25812	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-22-40_		25804	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-36-40_		25748	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-121-40		25250	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-51-40_		25084	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-94-40_		25030	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-56-40_		24982	Chrome (Profile 2)
☆	●		image/webp	https://web.whatsapp.com/img/emoji-27-40_		24942	Chrome (Profile 2)

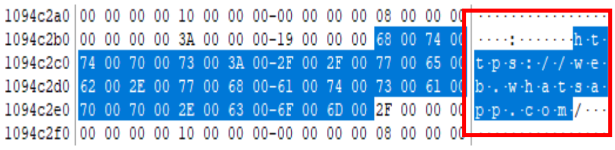
Viewing 25/25 records

Figure 10.Image Cached of victim's profile photo

Figure 10 shows the cache of the victim profile photo circled by a red box.

2.2.4.2 Analysis With FTK Imager

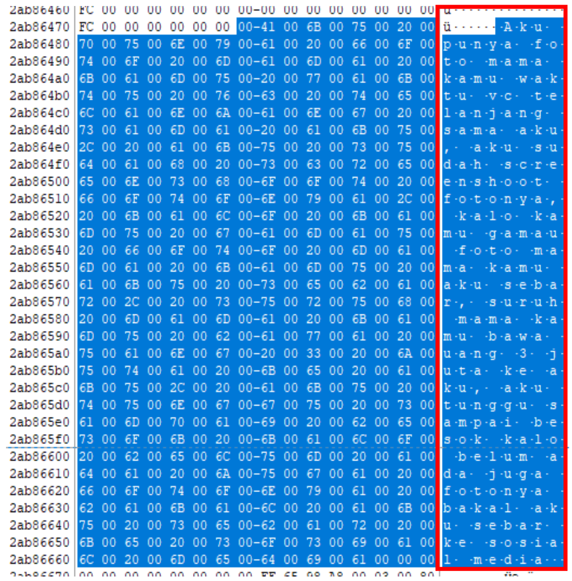
FTK Imager is an Access Data Forensic ToolKit Imageris one of the tools used in the world of digital forensics to perform data acquisition systems developed by AccessData companies. Where the acquisition system itself is a system that functions to retrieve, collect and prepare data, to process it to produce the desired data.



```
1094c2a0 00 00 00 00 10 00 00 00-00 00 00 00 08 00 00 00 ················
1094c2b0 00 00 00 00 3A 00 00 00-19 00 00 00 68 00 74 00 ····:·······h·t·
1094c2c0 74 00 70 00 73 00 3A 00-2F 00 2F 00 77 00 65 00 t·p·s·:·/·/·w·e·
1094c2d0 62 00 2E 00 77 00 68 00-61 00 74 00 73 00 61 00 b·.·w·h·a·t·s·a·
1094c2e0 70 00 70 00 2E 00 63 00-6F 00 6D 00 2F 00 00 00 p·p·.·c·o·m·/···
1094c2f0 00 00 00 00 10 00 00 00-00 00 00 00 08 00 00 00 ················
```

Figure 11. First Results for FTK Imager

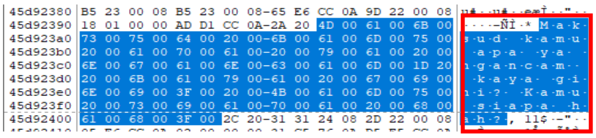
In Figure 11 showing the findings with the keyword Whatsapp, it is seen that the Whatsapp site is accessed via https://web.whatsapp.com/.



```
2ab86460 FC 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ü···············
2ab86470 FC 00 00 00 00 00 00 00-41 00 6B 00 75 00 20 00 ü·······A·k·u· ·
2ab86480 70 00 75 00 6E 00 79 00-61 00 20 00 66 00 6F 00 p·u·n·y·a· ·f·o·
2ab86490 74 00 6F 00 20 00 6D 00-61 00 6D 00 61 00 20 00 t·o· ·m·a·m·a· ·
2ab864a0 6B 00 61 00 6D 00 75 00-20 00 77 00 61 00 6B 00 k·a·m·u· ·w·a·k·
2ab864b0 74 00 75 00 20 00 76 00-63 00 20 00 74 00 65 00 t·u· ·v·c· ·t·e·
2ab864c0 6C 00 61 00 6E 00 6A 00-61 00 6E 00 67 00 20 00 l·a·n·j·a·n·g· ·
2ab864d0 73 00 61 00 6D 00 61 00-20 00 61 00 6B 00 75 00 s·a·m·a· ·a·k·u·
2ab864e0 2C 00 20 00 61 00 6B 00-75 00 20 00 73 00 75 00 ,· ·a·k·u· ·s·u·
2ab864f0 64 00 61 00 68 00 20 00-73 00 63 00 72 00 65 00 d·a·h· ·s·c·r·e·
2ab86500 65 00 6E 00 73 00 68 00-6F 00 6F 00 74 00 20 00 e·n·s·h·o·o·t· ·
2ab86510 66 00 6F 00 74 00 6F 00-6E 00 79 00 61 00 2C 00 f·o·t·o·n·y·a·,·
2ab86520 20 00 6B 00 61 00 6C 00-6F 00 20 00 6B 00 61 00  ·k·a·l·o· ·k·a·
2ab86530 6D 00 75 00 20 00 67 00-61 00 6D 00 61 00 75 00 m·u· ·g·a·m·a·u·
2ab86540 20 00 66 00 6F 00 74 00-6F 00 20 00 6D 00 61 00  ·f·o·t·o· ·m·a·
2ab86550 6D 00 61 00 20 00 6B 00-61 00 6D 00 75 00 20 00 m·a· ·k·a·m·u· ·
2ab86560 61 00 6B 00 75 00 20 00-73 00 65 00 62 00 61 00 a·k·u· ·s·e·b·a·
2ab86570 72 00 2C 00 20 00 73 00-75 00 72 00 75 00 68 00 r·,· ·s·u·r·u·h·
2ab86580 20 00 6D 00 61 00 6D 00-61 00 20 00 6B 00 61 00  ·m·a·m·a· ·k·a·
2ab86590 6D 00 75 00 20 00 62 00-61 00 77 00 61 00 20 00 m·u· ·b·a·w·a· ·
2ab865a0 75 00 61 00 6E 00 67 00-20 00 33 00 20 00 6A 00 u·a·n·g· ·3· ·j·
2ab865b0 75 00 74 00 61 00 20 00-6B 00 65 00 20 00 61 00 u·t·a· ·k·e· ·a·
2ab865c0 6B 00 75 00 2C 00 20 00-61 00 6B 00 75 00 20 00 k·u·,· ·a·k·u· ·
2ab865d0 74 00 75 00 6E 00 67 00-67 00 75 00 20 00 73 00 t·u·n·g·g·u· ·s·
2ab865e0 61 00 6D 00 70 00 61 00-69 00 20 00 62 00 65 00 a·m·p·a·i· ·b·e·
2ab865f0 73 00 6F 00 6B 00 20 00-6B 00 61 00 6C 00 6F 00 s·o·k· ·k·a·l·o·
2ab86600 20 00 62 00 65 00 6C 00-75 00 6D 00 20 00 61 00  ·b·e·l·u·m· ·a·
2ab86610 64 00 61 00 20 00 6A 00-75 00 67 00 61 00 20 00 d·a· ·j·u·g·a· ·
2ab86620 66 00 6F 00 74 00 6F 00-6E 00 79 00 61 00 20 00 f·o·t·o·n·y·a· ·
2ab86630 62 00 61 00 6B 00 61 00-6C 00 20 00 61 00 6B 00 b·a·k·a·l· ·a·k·
2ab86640 75 00 20 00 73 00 65 00-62 00 61 00 72 00 20 00 u· ·s·e·b·a·r· ·
2ab86650 6B 00 65 00 20 00 73 00-6F 00 73 00 69 00 61 00 k·e· ·s·o·s·i·a·
2ab86660 6C 00 20 00 6D 00 65 00-64 00 69 00 61 00 00 00 l· ·m·e·d·i·a···
```

Figure 12. Second Results for FTK Imager

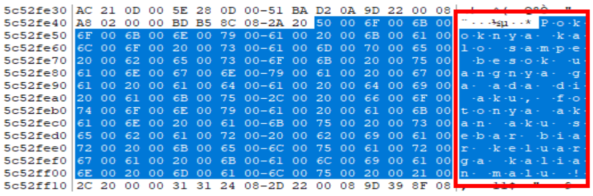
In Figure 12 it can be seen that in the first chat sent by the perpetrator to the victim, the perpetrator sent a blackmail message to the victim.



```
45d92380 B5 23 00 08 B5 23 00 08-65 E6 CC 0A 9D 22 00 08 µ#··µ#··eæÌ··"··
45d92390 18 01 00 00 AD D1 CC 0A-2A 20 4D 00 61 00 6B 00 ····ÑÌ·* M·a·k·
45d923a0 73 00 75 00 64 00 20 00-6B 00 61 00 6D 00 75 00 s·u·d· ·k·a·m·u·
45d923b0 20 00 61 00 70 00 61 00-20 00 79 00 61 00 20 00  ·a·p·a· ·y·a· ·
45d923c0 6E 00 67 00 61 00 6E 00-63 00 61 00 6D 00 1D 20 n·g·a·n·c·a·m··
45d923d0 20 00 6B 00 61 00 79 00-61 00 20 00 67 00 69 00  ·k·a·y·a· ·g·i·
45d923e0 6E 00 69 00 3F 00 20 00-4B 00 61 00 6D 00 75 00 n·i·?· ·K·a·m·u·
45d923f0 20 00 73 00 69 00 61 00-70 00 61 00 20 00 68 00  ·s·i·a·p·a· ·h·
45d92400 61 00 68 00 3F 00 2C 20-31 31 24 08 2D 22 00 08 a·h·?·, 11$·-"··
```

Figure 13.Third Results for FTK Imager

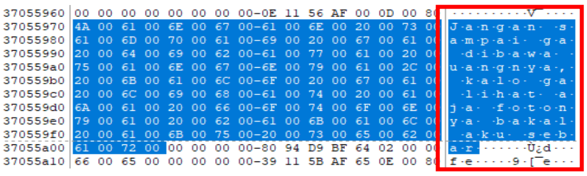
In Figure 13 you can see evidence of the second chat sent by the victim to the perpetrator, the victim asks the perpetrator's intention to threaten the victim.



```
5c52fe30 AC 21 0D 00 5E 28 0D 00-51 BA D2 0A 9D 22 00 08 ¬!··^(··QºÒ··"··
5c52fe40 A8 02 00 00 BD B5 8C 08-2A 20 50 00 6F 00 6B 00 ¨···½µ··* P·o·k·
5c52fe50 6F 00 6B 00 6E 00 79 00-61 00 20 00 6B 00 61 00 o·k·n·y·a· ·k·a·
5c52fe60 6C 00 6F 00 20 00 73 00-61 00 6D 00 70 00 65 00 l·o· ·s·a·m·p·e·
5c52fe70 20 00 62 00 65 00 73 00-6F 00 6B 00 20 00 75 00  ·b·e·s·o·k· ·u·
5c52fe80 61 00 6E 00 67 00 6E 00-79 00 61 00 20 00 67 00 a·n·g·n·y·a· ·g·
5c52fe90 61 00 20 00 61 00 64 00-61 00 20 00 64 00 69 00 a· ·a·d·a· ·d·i·
5c52fea0 20 00 61 00 6B 00 75 00-2C 00 20 00 66 00 6F 00  ·a·k·u·,· ·f·o·
5c52feb0 74 00 6F 00 6E 00 79 00-61 00 20 00 61 00 6B 00 t·o·n·y·a· ·a·k·
5c52fec0 61 00 6E 00 20 00 61 00-6B 00 75 00 20 00 73 00 a·n· ·a·k·u· ·s·
5c52fed0 65 00 62 00 61 00 72 00-20 00 62 00 69 00 61 00 e·b·a·r· ·b·i·a·
5c52fee0 72 00 20 00 6B 00 65 00-6C 00 75 00 61 00 72 00 r· ·k·e·l·u·a·r·
5c52fef0 67 00 61 00 20 00 6B 00-61 00 6C 00 69 00 61 00 g·a· ·k·a·l·i·a·
5c52ff00 6E 00 20 00 6D 00 61 00-6C 00 75 00 20 00 21 00 n· ·m·a·l·u· ·!·
5c52ff10 2C 20 00 00 31 31 24 08-2D 22 00 08 9D 39 8F 08 , ··11$·-"···9··
```

Figure 14.Fourth Results for FTK Imager

In Figure 14 there is evidence of the chat of the three perpetrators to the victim, the perpetrator still threatens to spread photos of the victim's parents if the money he asks for is not given by the victim.



```
37055960 00 00 00 00 00 00 00 00-0E 11 56 AF 00 0D 00 80 ··········V¯····
37055970 4A 00 61 00 6E 00 67 00-61 00 6E 00 20 00 73 00 J·a·n·g·a·n· ·s·
37055980 61 00 6D 00 70 00 61 00-69 00 20 00 67 00 61 00 a·m·p·a·i· ·g·a·
37055990 20 00 64 00 69 00 62 00-61 00 77 00 61 00 20 00  ·d·i·b·a·w·a· ·
370559a0 75 00 61 00 6E 00 67 00-6E 00 79 00 61 00 2C 00 u·a·n·g·n·y·a·,·
370559b0 20 00 6B 00 61 00 6C 00-6F 00 20 00 67 00 61 00  ·k·a·l·o· ·g·a·
370559c0 20 00 6C 00 69 00 68 00-61 00 74 00 20 00 61 00  ·l·i·h·a·t· ·a·
370559d0 6A 00 61 00 20 00 66 00-6F 00 74 00 6F 00 6E 00 j·a· ·f·o·t·o·n·
370559e0 79 00 61 00 20 00 62 00-61 00 6B 00 61 00 6C 00 y·a· ·b·a·k·a·l·
370559f0 20 00 61 00 6B 00 75 00-20 00 73 00 65 00 62 00  ·a·k·u· ·s·e·b·
37055a00 61 00 72 00 00 00 00 00-80 94 D9 BF 64 02 00 00 a·r·······Ù¿d···
37055a10 66 00 65 00 00 00 00 00-39 11 5B AF 65 0E 00 80 f·e·····9·[¯e···
```

Figure 15. **Fifth Results for FTK Imager**

Figure 15 shows evidence of the chat of the four perpetrators to the victim.

2.2.5 Reporting

The reporting stage is the last stage of the stage National Institute of Justice (NIJ). At this stage, the investigator will make a document or record of the results of the analysis of the evidence that has been carried out in detail..

2.2.6 Results

Results will discuss the findings of the RAM data that has been acquired using several forensic tools, namely Belkasoft RAM Capturer, FTK Imager, Browser History Capture, and Browser History Examiner.

Table 3. Results Analysis On WhatsApp Web

No	Information Data	Forensic Tools	
		FTK Imager	Browser History Examiner
1	WhatsApp Weblink	√	-
2	The perpetrator's chat with the victim	√	-
3	Cache Photo Perpetrator	-	√
4	Access time	-	√

Table 3 displays the results found in analyzing WhatsApp Web used on the browser Chrome using tools forensic. As seen in the results from the FTK Imager, evidence was found in the form of a WhatsApp Weblink accessed by the perpetrator, as well as the perpetrator's chat with the victim. The Browser History Examiner tool displays the WhatsApp Weblink accessed via Chrome, the cache perpetrator's photo, and the time of the web access.

Table 4. The Findings of Evidence

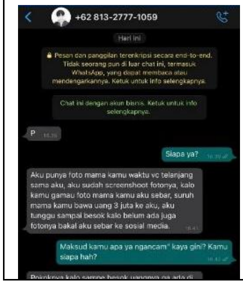
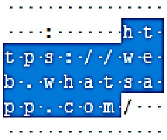
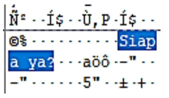
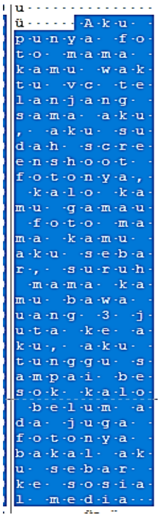
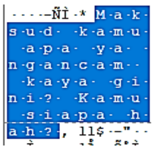
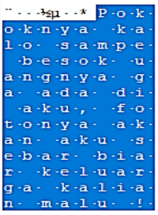
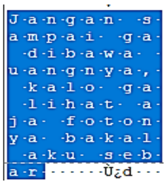
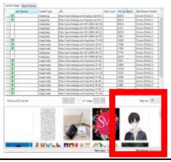
Evidence From Victims	Findings	Text
 +62 813-2777-1059 Hari ini 🔒 Pesan dan panggilan terenkripsi secara end-to-end. Tidak seorang pun di luar chat ini, termasuk WhatsApp, yang dapat membaca atau mendengarkannya. Ketuk untuk info selengkapnya. Chat ini dengan akun bisnis. Ketuk untuk info selengkapnya. P Siapa ya? Aku punya foto mama kamu waktu vc telanjang sama aku, aku sudah screenshoot fotonya, kalo kamu gamau foto mama kamu aku sebar, suruh mama kamu bawa uang 3 juta ke aku, aku tunggu sampai besok kalo belum ada juga fotonya bakal aku sebar ke sosial media. Maksud kamu apa ya ngancam" kaya gini? Kamu siapa hah? Pokoknya kalo sampe besok uangnya ga ada di	 ················ ····:·······h·t· t·p·s·:·/·/·w·e· b·.·w·h·a·t·s·a· p·p·.·c·o·m·/··· ················	WhatsApp Web access link
	 Ṅ²··Í$··Ù,P·Í$·· ©$··········Siap a ya?···aöô·–"·· –"······5"··±·+·	“Siapaya?”
	 u················ ü······ ·A·k·u· · p·u·n·y·a· ·f·o· t·o· ·m·a·m·a· · k·a·m·u· ·w·a·k· t·u· ·v·c· ·t·e· l·a·n·j·a·n·g· · s·a·m·a· ·a·k·u· ,· ·a·k·u· ·s·u· d·a·h· ·s·c·r·e· e·n·s·h·o·o·t· · f·o·t·o·n·y·a·,· ·k·a·l·o· ·k·a· m·u· ·g·a·m·a·u· ·f·o·t·o· ·m·a· m·a· ·k·a·m·u· · a·k·u· ·s·e·b·a· r·,· ·s·u·r·u·h· ·m·a·m·a· ·k·a· m·u· ·b·a·w·a· · u·a·n·g· ·3· ·j· u·t·a· ·k·e· ·a· k·u·,· ·a·k·u· · t·u·n·g·g·u· ·s· a·m·p·a·i· ·b·e· s·o·k· ·k·a·l·o· ·b·e·l·u·m· ·a· d·a· ·j·u·g·a· · f·o·t·o·n·y·a· · b·a·k·a·l· ·a·k· u· ·s·e·b·a·r· · k·e· ·s·o·s·i·a· l· ·m·e·d·i·a···	"Akupunyafoto mama kamuwaktuvctelanjangsamaaku, akusudahscreenshootfotonya, kalokamugamaufoto mama kamuakusebar, suruh mama kamubawauang 3 jutakeaku, akutunggusampaibesokkalobelumada juga fotonyabakalakusebarkesosial media”
	 ·····–ÑÌ·* M·a·k· s·u·d· ·k·a·m·u· ·a·p·a· ·y·a· · n·g·a·n·c·a·m·· ·k·a·y·a· ·g·i· n·i·?· ·K·a·m·u· ·s·i·a·p·a· ·h· a·h·?·, 11$·–"··	“Maksudkamuapayangancam kaya gitu? Kamusiapa hah?"
	 ¨···³⁄₂µ··* P·o·k· o·k·n·y·a· ·k·a· l·o· ·s·a·m·p·e· ·b·e·s·o·k· ·u· a·n·g·n·y·a· ·g· a· ·a·d·a· ·d·i· ·a·k·u·,· ·f·o· t·o·n·y·a· ·a·k· a·n· ·a·k·u· ·s· e·b·a·r· ·b·i·a· r· ·k·e·l·u·a·r· g·a· ·k·a·l·i·a· n· ·m·a·l·u· ·!·	"Pokoknyakalosampebesokuangnyagaada di aku, fotonyaakanakusebarbiarkeluargakalian malu!!"
	 J·a·n·g·a·n· ·s· a·m·p·a·i· ·g·a· ·d·i·b·a·w·a· · u·a·n·g·n·y·a·,· ·k·a·l·o· ·g·a· ·l·i·h·a·t· ·a· j·a· ·f·o·t·o·n· y·a· ·b·a·k·a·l· ·a·k·u· ·s·e·b· a·r·······Ù¿d···	"Jangansampaigadibawauangnya, kalogalihatajafotonyabakalakusebar."
		

Table 4 shows that the evidence found during the forensic process has similarities with the evidence brought by the victim as report evidence. The evidence found in RAM is the contents of the conversation between the perpetrator and the victim as well as the cached image from the browser. The evidence found from the Chrome browser is the history of visits to the Chrome browser, the time spent accessing Whatsapp Web on the Chrome browser, cached images of the perpetrator and victim, and evidence of conversations between the perpetrator and the victim.

3. CONCLUSION

In this research, the main focus is to find and collect evidence from the laptop used by the perpetrator in committing a crime to the victim. Chat that has been deleted by the perpetrator on Whatsapp which is accessed using a browser Chrome can be restored by retrieving volatile data on laptop RAM using tools Belkasoft RAM Capturer, then the data is Imaging using FTK Imager. As well as WhatsApp access history data on the Chrome browser, cached profile photos of perpetrators, and cached profile photos of victims using the Browser History Capturertools and Browser History Examiner. The percentage of results obtained from the results of imaging data analysis using the FTK Imager tool is 50% in the form of a WhatsApp Web link and chat from the perpetrator to the victim, while the results from the Browser History Examiner are 50% in the form of a cache of the photo perpetrator, as well as the access time WhatsApp. This research uses the stages of the National Institute of Justice (NIJ), it is hoped that future research can use other stages. This research uses OS Windows 10, so it is hoped that for further research it can use OS Linux or macOS.

4. REFERENCES

[1] N. Budhisantosa, "Analisis forensik komputer pada timestamps sistem berkas ntfs," *Forum Ilm. Fak. Ilmu Komput. Univ. Esa Unggul*, vol. 13, 2016.

[2] I. Riadi, S. Sunardi, and S. Sahiruddin, "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)," *J. Rekayasa Teknol. Inf.*, vol. 3, no. 1, p. 87, 2019.

[3] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (Nij)," *Elinvo (Electronics, Informatics, Vocat. Educ.*, vol. 3, no. 1, pp. 70–82, 2018.

[4] I. Riadi, S. Sunardi, and M. E. Rauli, "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics," *J. Tek. Elektro*, vol. 10, no. 1, pp. 18–22, 2018.

[5] D. S. Yudhistira, "Metode Live Forensics Untuk Analisis Random Access Memory Pada Perangkat Laptop," 2018.

[6] B. Sugiantoro *et al.*, "Penerapan Framework Harmonised Digital Forensic Investigation Process (Hdfip) Untuk Mendapatkan Artifak the Implementation of Framework Harmonised Digital Forensic Investigation Process (Hdfip) To Get Artifacts Digital Evidence," *CyberSecurity dan Forensik Digit.*, vol. 1, no. 2, pp. 67–74, 2018.

[7] R. Umar, A. Yudhana, and M. Nur Faiz, "Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary," *Pros. Konf. Nas. Ke- 4 Asos. Progr. Pascasarj. Perguru. Tinggi Muhammadiyah*, pp. 207–211, 2016.

[8] T. Rochmadi, "Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browzar," *Indones. J. Bus. Intell.*, vol. 1, no. 1, p. 32, 2019.

[9] D. S. I. Krisnadi, "Citra Forensik Dari Barang Bukti Elektronik Dengan Metode Physical Menggunakan Acquisition Tools Tableau Imager Dan Ftk Imager," p. 16, 2020.

[10] T. Rochmadi, "Deteksi Bukti Digital Pada Adrive Cloud Storage Menggunakan Digital Evidence Detection in Adrive Cloud Storage Using Live," *CyberSecurity dan Forensik Digit.*, vol. 2, no. 2, pp. 21–24, 2019.

[11] E. C. Zatnika, N. Widiyasono, and A. I. Gufroni, "Teknik Live Forensics Dalam Investigasi Malware Pada Memori Komputer Dengan Volatility Framework Versi Windows," *Academia.Edu*.

[12] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Perancangan Digital Forensik pada Aplikasi Twitter Menggunakan Metode Live Forensics," *Semin. Nas. Inform. 2008 (semnasIF 2008)*, vol. 2018, no. November, pp. 86–91, 2018.

[13] A.- Ahmadi, "Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ)," *J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf.*, vol. 4, no. 1, p. 8, 2018.

[14] 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.

[15] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "1490-Article Text-2859-1-10-20190413," *Akuisisi Bukti Digit. Pada Instagram Messenger Berbas. Android Menggunakan Metod. Natl. Inst. Justice*, vol. 4, pp. 219–227, 2018.

[16] 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.

[17] V. R. G. Leri and I. Riadi, "Data Search for Pornographic Content on Twitter Services using National Institute of Standard and Technology (NIST) Method," *Int. J. Comput. Appl.*, vol. 183, no. 24, pp. 25–31, 2021.

[18] E. Wahyudi, M. Zulpahmi, K. Gunawan, and B. Imran, "ANALISIS BUKTI DIGITAL WHATSAPP PADA ANDROID SMARTPHONE," vol. 10, no. 2, pp. 20–26, 2020.

[19] M. N. Faiz, R. Umar, and A. Yudhana, "Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary," *Ilk. J. Ilm.*, vol. 8, no. 3, pp. 242–247, 2016.

[20] J. Moedjahedy, "Forensik komputer Studi Kasus: Universitas Klabat," *J. Sist. Inf. dan Teknol. Inf.*, vol. 5, no. 2, pp. 95–106, 2016.

[21] I. Saputra and M. N. Azhar, "Analisis dan Investigasi Forensik Digital Live Memory untuk Deteksi Tingkah Laku Agresi Pada Aplikasi Whatsapp," *Semin. Nas. dan Disk. Panel Multidisiplin Has. Penelit. Pengabdi. Kpd. Masy.*, pp. 119–125, 2018.

[22] S. A. Mandowen, "Analisis forensik komputer pada lalu lintas jaringan," *J. Sains*, vol. 16, no. 1, pp. 14–20, 2016.

[23] M. Fazarahma, "Forensik Browser pada Aplikasi Facebook Messenger Studi Kasus Ujaran Kebencian Forensik Browser pada Aplikasi Facebook Messenger Studi Kasus Ujaran Kebencian," 2020.

[24] T. D. Larasati and B. C. Hidayanto, "Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10," *Sesindo*, vol. 6, no. November, pp. 456–256, 2017.

[25] D. A. Putri, "Forensic Mobile against Threat WhatsApp Services using National Institute of Standards Technology Method," vol. 183, no. 30, pp. 1–8, 2021.