Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation Framework Version 2

Bery Actoriano[1], Imam Riadi[2]
[1]Departement of Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2]Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
(*bery1400018147@webmail.uad.ac.id*, *imam.riadi@is.uad.ac.id*)

ABSTRACT

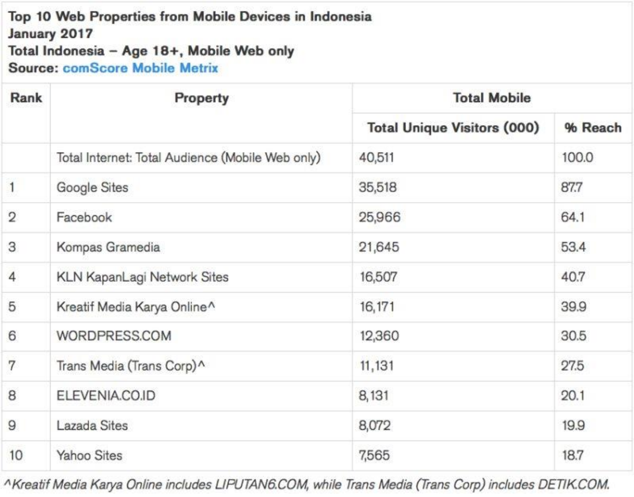
WhatsApp Web is a computer-based extension connected to WhatsApp on smartphones. The handling of crime cases on computers or smartphones has four main stages, namely preparation, Case Place Event, examination of evidence in the digital forensics laboratory and the report of digital evidence as the application of Integrated Digital Forensic Investigation Framework Version 2 which is a model for the investigation process of digital evidence and claimed to have complete stages and can accommodate all stages in the process of cybercrime investigation. In this study using procedures that can be used as a reference to conducting a WhatsApp Web forensic investigation to obtain and process evidence proof and analysis of digital evidence in the form of WhatsApp databases contained in the laptop and Smartphone directories, in order to obtain information to strengthen evidence of crime cases of can be presented in court in the form of analytical results of digital evidence so that it can be understood.

KEYWORDS: Forensic, WhatsApp, IDFIF Version 2, Scene.

1 INTRODUCTION

The Internet as a technology close to the life of modern society has changed human behavior in communicating wherever the user is [1]. If in ancient times people know the communication media through postal mail and telegraph, then now has available many alternative media communication via the internet or better known by name WhatsApp[2].

WhatsApp Messenger is a cross-platform messaging app that allows us to exchange messages at no cost SMS, ComScore claims that the WhatsApp chat app is the most popular Smartphone app with most users in Indonesia, of course after the mandatory Android user app, Google Play. According to comScore, WhatsApp now has about 35.7 million users in Indonesia, WhatsApp the user stats can be seen in Figure 1.



Top 10 Web Properties from Mobile Devices in Indonesia
January 2017
Total Indonesia – Age 18+, Mobile Web only
Source: comScore Mobile Metrix

Rank	Property	Total Mobile	
		Total Unique Visitors (000)	% Reach
	Total Internet: Total Audience (Mobile Web only)	40,511	100.0
1	Google Sites	35,518	87.7
2	Facebook	25,966	64.1
3	Kompas Gramedia	21,645	53.4
4	KLN KapanLagi Network Sites	16,507	40.7
5	Kreatif Media Karya Online^	16,171	39.9
6	WORDPRESS.COM	12,360	30.5
7	Trans Media (Trans Corp)^	11,131	27.5
8	ELEVENIA.CO.ID	8,131	20.1
9	Lazada Sites	8,072	19.9
10	Yahoo Sites	7,565	18.7

^Kreatif Media Karya Online includes LIPUTAN6.COM, while Trans Media (Trans Corp) includes DETIK.COM.

Figure 1. WhatsApp Messenger Usage Statistics

However, the broad user base also makes this app a serious threat with all the convenience provided by the Mesh Mesa WhatsApp app by leveraging the existing features of WhatsApp messenger application as a medium for committing crimes in the cyber world such as spreading malicious code, obtaining and disseminate confidential information [3].

In this paper, the IDFIF V2 method will be presented for reference by other researchers. From various studies on WhatsApp forensic analysis that have been done with methods such as live forensics, forensic smartphones [3] and the National Institute of Standards and Technology (NIST)[4]. Only limited to identifying, collecting, examining, analyzing and reporting but in its implementation the stages of the investigation process against digital evidence at the scene of crime, computer or smartphone forensics has four main stages, namely preparation (pre-process), process of TKP (proactive process), examination of evidence in digital forensic laboratories (reactive process) and examination reports on digital evidence items such as the application of Integrated Digital Forensic Investigation Framework Version 2 (IDFIF V2)[5]. In research using the application of the Integrated Digital Forensic Investigation Framework V2 (IDFIF V2) conducted by Ruuhwan, it was only applied to the SMS (Short Message Service) service[5]. No research has yet applied the IDFIF V2 framework to a web-based WhatsApp application.

2 LITERATURE REVIEW

2.1 Computer forensic

Computer Forensics is one of the forensic sciences that deals with legal evidence found in computers and digital storage media. This forensic computer is known as Digital Forensics[6]. Many areas of science are used and involved in a crime or criminal case for a legal and justice interest, where such science is known as forensic science [7].

2.2 Mobile forensic

Mobile forensics is a branch of digital forensics conducted to obtain and analyze digital evidence from mobile devices for investigation purposes [8]. Currently, most Indonesian people have more than one gadget. One person allows smartphone, tablet and laptop computer simultaneously [9]. The ability of a gadget to do data processing is also higher, so all activities can be done through gadget [3].

2.3 WhatsApp

WhatsApp is a messaging app for smartphones with basic BlackBerry Messenger-like [10]. WhatsApp Messenger is a messaging messenger application medium that allows us to exchange messages with no SMS charges because WhatsApp Messenger uses the same internet network for email, web search, and more. The WhatsApp Messenger app uses a 3G or WiFi connection for data communications [11].

2.4 WhatsApp Web

WhatsApp Web is a computer-based extension of WhatsApp account on user phone. Messages sent and received are fully synchronized between the user phone and the user computer, and the user can view them all on both devices. All actions user take on user phone will be applied also on WhatsApp Web, and vice versa. At the moment, WhatsApp Web is only available for Android phones, iPhone 8.1+, Windows Phone 8.0 and 8.1, Nokia S60, Nokia S40 EVO, BlackBerry and BlackBerry10 only [4].

2.5 Cache

Caches in computer science are defined as components that store newly executed computing data or other useful data duplication to run the command in the future more quickly. But its capacity is limited. When viewed from its function, the cache is intended to help speed up the device when running applications that have previously been used [12].

2.6 FTK Imager

FTK Imager is a digital forensic acquisition tool created by AccessData. FTK Imager is free, but make no mistake, facilities and capabilities are not inferior to the software acquisition paid[13].

2.7 WhatsApp Viewer

WhatsApp Viewer is used to seeing WhatsApp smartphones chat is extracted on user PC device. WhatsApp Viewer has the ability to display chats from an extracted Android msgstore.db file. WhatsApp This viewer supports crypt5, crypt7, crypt8, and crypt12 versions of the database to be displayed. Copying extracted messages to user PC and make it easier for the user to read old message information, without pressing "show old messages". The User can export the message information data that can be as HTML, TXT, and JSON files [13].

2.8 Autopsy

An autopsy is a tool created using Perl language that uses to do digital forensics, an autopsy can analyze the Disk Figure and Partition. The purpose of using Autopsy is to be able to analyze the File System which can be Evidence or evidence [14].

2.9 Framework IDFIF Version 2

This study uses the application of IDFIF (Integrated Digital Forensic Investigation Framework) Version 2 which is a model for the process of investigating the digital evidence and claimed to have complete stages and can accommodate all stages of the cybercrime investigation process. After analyzing the investigation process, IDFIF V2 has several stages that have been modified so that it has been in accordance with the investigation procedure and the process of confiscation of evidence found at the crime scene. Thus, currently, the IDFIF V2 model can be used as a standard for the investigation process[5].

3 METHODOLOGY

The research stages are the stages of doing case simulations to try to implement the IDFIF Version 2 framework for Forensic investigation process WhatsApp Messenger. The case simulation aims to test the process of the IDFIF Version 2 framework in the web-based WhatsApp Messenger app used to search conversations or messages that have been deleted for use as evidence or crime. The stages of this study were conducted to determine the extent of abuse in the application WhatsApp [5]. Here are the methods and stages of research. The method consists of several stages which the authors describe as in Figure 2.

Research Problem
Literature Review
Case Study
Conclution

Figure 2. Research methods

Figure 2 is the method there are several stages of research are:

1. The research problem is the first step taken to obtain and determine research topics to be studied further. At this stage, it begins by looking at various phenomena, events, and information obtained in various ways.
2. The literature review is expected to explore all the information related to the issues to be studied and the object of the research objectives and provide the basis for the direction of research that will be conducted and become the beginning of thinking for each researcher so that research can be used as the reference again in the future.
3. Case Study is the process of applying IDFIF Version 2 to Web-based WhastaApp Messenger investigation process. as shown in Figure 3.

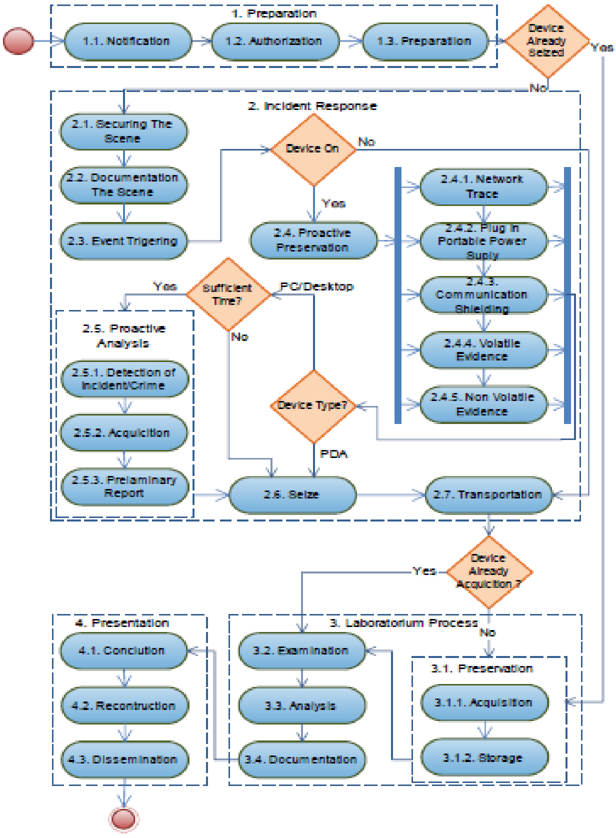


Figure 3. Model IDFIF Version 2

Figure 3 [5], is the result of research that has several stages in handling digital evidence, that is:

a. Preparation

It is a preparation that must be done to conduct the investigation process in handling digital evidence starting from the event of the case to the making of the final report.

1) Notification: Notification of investigation or report of a crime to law enforcers.
2) Authorization: Stages to gain access to evidence and legal status of the inquiry process.
3) Preparation: Preparation that includes the availability of tools, personnel and various needs of the investigation.

b. Incident Response

It is an activity carried out at the scene of the case with the aim of securing the existing digital evidence so as not to be contaminated by other matters.

1) Securing The Scene: Conduct a mechanism to secure crime scenes and protect the integrity of evidence.
2) Documentation The Scene: The main objective of this stage is to process the

crime scene, search for trigger sources of events, search for communication or network connections and document the scene by taking pictures of every detail of the scene.

3) Event Triggering: Perform a preliminary analysis of an event process that occurred.
4) Proactive Preservation: Has 5 sub-stages of network trace perform trace search through the network used by digital evidence.
   a) Plug in a portable power supply is a process of securing digital evidence with the condition "on" so that the power contained in digital evidence can be maintained during the trip up to the forensic laboratory.
   b) Communication shielding is a phase of data communication deactivation in digital evidence so as to prevent changes in data from outside.
   c) Volatile and Non-Volatile Evidence is a process of securing digital evidence. At the end of the proactive Preservation stage, there is a decision process. This stage is not called directly into stages, but the output of this decision is also important for the continuity of the investigation process. From this stage, it was decided that digital evidence should be immediately confiscated and further examination in the forensic laboratory or conducted on-site inspection to obtain an initial report of the incident.
5) Proactive Analysis: the live analysis stage of the inventory and build the initial hypothesis of an event. Detection of Incident / Crime, at this stage, is the stage, to ensure that there has been a violation of the law. The acquisition is the process of data acquisition of inventory items so as to lighten the workload of digital forensic analysis in the laboratory. Preliminary Report is a preliminary report on the proactive investigation that has been done.
6) Seize: Perform the confiscation of digital evidence that has been found for further analysis.
7) Transportation: Is the process of moving digital evidence from the scene to the forensic digital laboratory.

c. Laboratorium Process

After the handling of digital evidence at the scene of the case, then at this stage is to process the data analysis of evidence that has been obtained previously so that can be found the type of crime that has occurred.

1) Preservation: Maintains the integrity of the findings by using a chain of custody and hashing functions.
2) Examination: Processing evidence to find its relevance to events.
3) Analysis: Is a technical study and assembles the linkages between the findings.
4) Documentation: Documentation of all activities that have been done from the beginning of the investigation process to the end of the analysis process in the forensic laboratory.

d. Presentation

This is the final stage in the process of digital investigation. At this stage is the process of making reports related to the results of the analysis performed in the previous stage and ensure that each process is done in accordance with applicable law rules.

1) Conclusion: Summing up the results of the investigation that has been done.
2) Reconstruction: The process of analysis and an overall evaluation of the results of the investigation.
3) Dissemination: The recording of the investigation process and the records may be disseminated to other investigators who are conducting similar cases.

4. The conclusion is the process of all the stages that have been done in the process of this research from the process of handling physical evidence and get digital but goods in the form of variables related to the conversation time, the content of the message conversation, the profile of the perpetrator and the victim on WhatsApp messenger, and the data can be analyzed whether in accordance with the reporting of victims and there is a crime, to the final stage of making a final report to be presented in court to strengthen evidence in a crime.

4 RESULTS AND DISCUSSION

Stages used in the investigation of laptops and smartphones can be seen in Figure 4 to find out the different handling of investigations done on laptops and smartphones to get evidence WhatsApp web on laptops and WhatsApp smartphone form of database to be in extraction and will be in the analysis so that the results can be compared between WhatsApp Web and WhatsApp Smartphones to get information related to crime perpetrated by the perpetrator using WhatsApp web on the perpetrator's laptop who synced with WhatsApp smartphone.

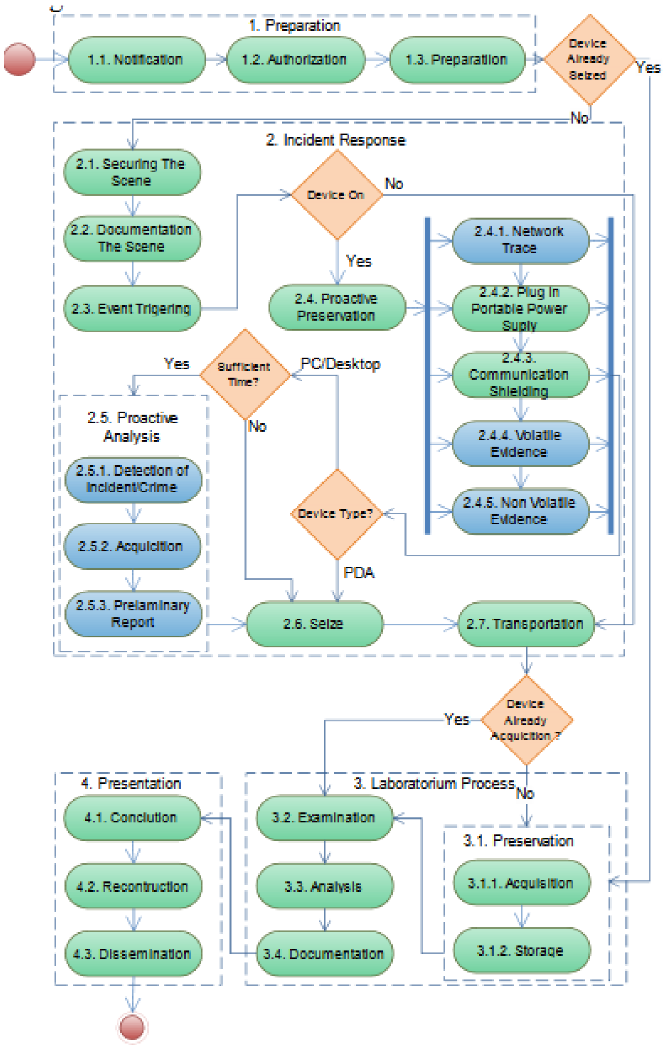


Figure 4. Step IDFIF Version 2 on the investigation.

Figure 4 [5], step IDFIF Version 2 on the investigation, there are 4 main stages of Preparation, Incident response, Laboratory process and presentation that will be implemented in this research.

4.1 Preparation: is the initial stage of the investigation process of digital evidence, especially in laptop investigations and smartphones. This stage is divided into 3 sub-stages:

a. Notification: Victim Reports a crime which is a case of fundraising fraud that occurs with the authorities namely law enforcement to follow up on the investigation process.
b. Authorization: Law enforcement authorities work together and process licensing to mobile operators in order to access rights in the process of tracking fraud perpetrators.
c. Preparation: The law enforcement authorities prepare the need in the investigation process from personnel to search and obtain evidence of offenders, investigative equipment to support investigation activities, hardware and software.

4.2 Incident response: is the initial stage of the inquiry process. The incident response stage is as follows:

a. The investigator undertakes the process of securing the location of the crime in the actual circumstances by the officer taking the first action at the scene of the crime so that the evidence is not lost, damaged and unchanged such as reductions or additions and location and existence proven.
b. Documentation the Scene: The investigator performed documentation at the scene by photographing the crime scene and the evidence found at the scene. Without directly touching the evidence so that the investigator's fingerprints are not scratched on the evidence, and undermine the authenticity of the evidence.
c. Event Triggering: The next process of preliminary analysis on the fraud case occurred at the scene and look for the cause of crime at the scene to be concluded while the type of crime to be processed in the digital forensics laboratory.
d. Proactive Preservation: Investigators secure evidence of Laptops and Smartphones found at the scene.
   1) Plug in portable power supply: Investigators maintain digital evidence on smartphones with portable charging

as smartphone battery power conditions that can be located at the scene are not always fully charged.

2) Communication shielding: At this stage, Investigators keep evidence of smartphones and laptops found on the premises by disconnecting networks against smartphones and laptops from data changes on evidence.

e. Seize: The investigator performs the seizure of evidence found at the scene.

f. Transportation: The investigator performs the procedure of transferring evidence from the scene to the digital forensics lab for further investigation.

4.3 Process Laboratory: is the core stage of the investigation process. This stage is divided into several stages:

a. Preservation: The investigator conducted the process of securing the evidence. Conditions of evidence when in the acquisition process must be disconnected from existing data communications.

1) Acquisition: The investigator takes digital evidence from the Laptop and Smartphone devices found at the scene[15].

a) Acquisition Smartphone is an internal memory imaging for FTK Imager acquisition process which is to upload data in internal memory to find WhatsApp conversation to know the message information and conversation time and to know that the performer smartphone is connected with WhatsApp web.

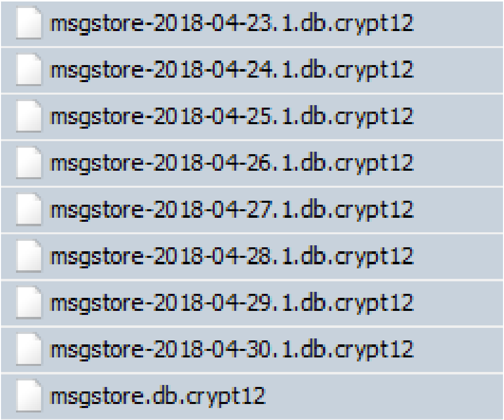
b) Acquisition laptops performed internal imaging memory for the acquisition process using FTK Imager is to upload data on local disk to find SQLite browser database file to find out information that the perpetrators use Google Chrome browser to commit a crime.

c) Storage: The investigator prepares the storage in the laptop investigator directory that has been determined to store backups of digital evidence of laptops and smartphones that have been backed up. In this study, the investigator has prepared a special directory on the Laptop investigator. The contents and forms of digital evidence will be stored in a safe and sterile place.

b. Examination: Investigators conduct checks to find evidence related to the case being handled by the laptop and smartphone offender. Exploring digital evidence to find evidence of WhatsApp databases on laptop devices and smartphone offenders. For the next stage of exploration on the device are:

1) Exploration of digital evidence on smartphones

At the exploration stage of digital evidence that finds the WhatsApp database on the smartphone is in the internal memory of the smartphone Storage / Sdcard0 / WhatsApp / Database, in the database folder there is a file Encrypted WhatsApp database like in Figure 5.



msgstore-2018-04-23.1.db.crypt12
msgstore-2018-04-24.1.db.crypt12
msgstore-2018-04-25.1.db.crypt12
msgstore-2018-04-26.1.db.crypt12
msgstore-2018-04-27.1.db.crypt12
msgstore-2018-04-28.1.db.crypt12
msgstore-2018-04-29.1.db.crypt12
msgstore-2018-04-30.1.db.crypt12
msgstore.db.crypt12

Figure 5. Database encryption WhatsApp smartphone

Figure 5 WhatsApp smartphone encryption database, CRYPT12 file is an encrypted database, to open CRYPT12 must find the encryption key, encryption key is on the smartphone device, to find the key file we have to enter the smartphone device memory, to enter the smartphone device must be in the root to give more access to smartphone device memory and to find the key file on the investigator's memory tool using the File Explorer ES tool to access more settings tools into root explorer to gain more access to the smartphone's internal memory and key files [15]. file folder com.WhatsApp smartphone there are several folders

such as databases and files, in the files folder found the key file on the device memory is \data\data\com.WhatsApp \ files file key as in Figure 6.

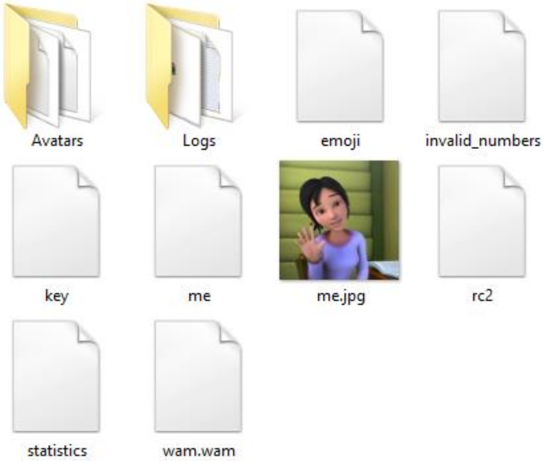


Figure 6. File key on the smartphone

Figure 6 is a key file on smartphones file, there is a file key used to generate encryption files to be open, in addition to the key file in the database file com.WhatsApp smartphone there are several database files on the device memory that is \data\data\com.WhatsApp\databases can in export to obtain information about the crime, file storage location can be seen in Table 1.

Table 1 Smartphone File Storage Location

File Type	Storage Location	File Name
Db WhatsApp	WhatsApp\Database	Mgstore.db.crypt12
Key WhatsApp	\data\data\com.WhatsApp\files	Key
Db WhatsApp	\data\data\com.WhatsApp\databases	Web_sessions.db

2) Exploration of digital evidence on laptops

At the exploration stage of digital evidence that is finding the SQLite WhatsApp database in the Google Chrome browser on the laptop directory, the Google Chrome SQLite database file is located on local disk C that is C:\Users\Adm\AppData\Local \Google \Chrome\User\Data\Default, in the default folder there is Google Chrome database about Google Chrome's acting activities. There are files and folders of Google Chrome doer activity such as cache folders where storage and to speed up Google Chrome access. File history is a file related to the activities of the performer such as downloads, URLs, and visits. Login file is an SQLite database to store login data on Google Chrome doer activity. The location of file storage can be viewed in Table 2.

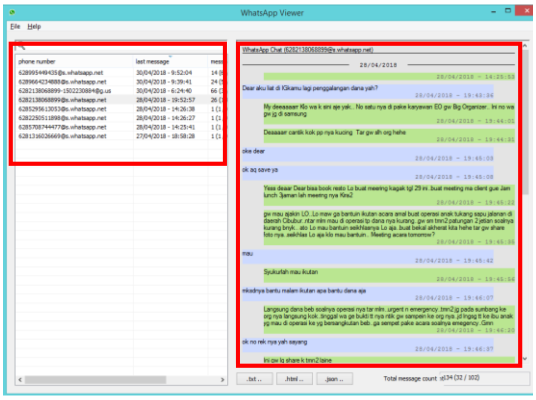
Table 2. Location of Laptop File Storage

File Type	Storage Location	File Name
Db SQLite	C:\Users\Adm\App Data\Local \Google\Chrome\User\Data\Default	History
Db SQLite	C:\Users\Adm\App Data\Local \Google\Chrome\User\Data\Default	Login
Cache	C:\Users\Adm\App Data\Local \Google\Chrome\User\Data\Default\cache	Cache

c. Analysis: at this stage the investigator conducts studies related to fraud cases and digital evidence in the can, then the next investigator to extract the database contained in the laptop and smartphone devices to be able to detail information on the evidence in the can, the first stage of the process of extraction against the WhatsApp database on smartphone devices.

1) Extraction of WhatsApp databases on smartphone devices

In the WhatsApp database extract stage of this smartphone device the database can be on the encrypted smartphone with crypt12, the investigator decrypts the encrypted database using the WhatsApp viewer, the msgstore.db.crypt12 file, and the key file are the key files found on the smartphone set in the folder \data\data\com.WhatsApp\files, then extract the database files with WhatsApp viewer so that the information residing on the file messages.deripted.db can be known whether there is an element of the crime or not, the data evidence in the form of conversation information that is extracted using WhatsApp viewer can be seen in Figure 7.



phone number	last message	mes
628995449435@s.whatsapp.net	30/04/2018 - 9:52:04	14 (
6289664234888@s.whatsapp.net	30/04/2018 - 9:39:41	24 (
6282138068899-1502230884@g.us	30/04/2018 - 6:24:40	66 (
6282138068899@s.whatsapp.net	28/04/2018 - 19:52:57	26 (
6285295613053@s.whatsapp.net	28/04/2018 - 14:26:38	1 (1
6282250511898@s.whatsapp.net	28/04/2018 - 14:26:27	1 (1
6285708744477@s.whatsapp.net	28/04/2018 - 14:25:41	1 (1
6281316026669@s.whatsapp.net	27/04/2018 - 18:58:28	1 (1

WhatsApp Chat (6282138068899@s.whatsapp.net)

28/04/2018

28/04/2018 - 14:25:53

Dear aku liat di IGkamu lagi penggalangan dana yah?
28/04/2018 - 19:43:36

My deeaaaarr Klo wa k sini aje yak.. No satu nya di pake karyawan EO gw Big Organizer.. Ini no wa gw jg di samsung
28/04/2018 - 19:44:01

Deaaaar cantik kok pp nya kucing Tar gw alh org hehe
28/04/2018 - 19:44:31

oke dear
28/04/2018 - 19:45:03

ok aq save ya
28/04/2018 - 19:45:08

Yess deaar Dear bisa book resto Lo buat meeting kagak tgl 29 ini..buat meeting ma client gue Jam lunch 3jaman lah meeting nya Kira2
28/04/2018 - 19:45:22

gw mau ajakin LO..Lo maw ga bantuin ikutan acara amal buat operasi anak tukang sapu jalanan di daerah Cibubur..ntar mlm mau di operasi tp dana nya kurang..gw sm tmn2 patungan 2 jetian soalnya kurang bnyk... ato Lo mau bantuin seikhlasnya Lo aja..buat bekal akherat kita hehe tar gw share foto nya..seikhlas Lo aja klo mau bantuin.. Meeting acara tomorrow?
28/04/2018 - 19:45:35

mau
28/04/2018 - 19:45:42

Syukurlah mau ikutan
28/04/2018 - 19:45:56

mksdnya bantu malam ikutan apa bantu dana aja
28/04/2018 - 19:46:07

Langsung dana beb soalnya operasi nya tar mlm..urgent n emergency..tmn2 jg pada sumbang ke org nya langsung kok..tinggal wa ge bukti tt nya ntik gw sampein ke org nya..jd lngsg tt ke ibu anak yg mau di operasi ke yg bersangkutan beb..ga sempet pake acara soalnya emegency..Gmn
28/04/2018 - 19:46:20

ok no rek nya yah sayang
28/04/2018 - 19:46:37

Ini gw lg share k tmn2 laine

Total message count: 134 (32 / 102)

Figure 7. WhatsApp content information

Figure 7 WhatsApp content information contains the recipient's number information, recent messages, sent and received messages and text and picture content of the conversation between the offender and the victim. In the smartphone device memory, there is a com.WhatsApp database file to obtain information related to the crime, for the database to be extraction database web_sessions.db using the DB Browser tool for SQLite as in Figure 8.

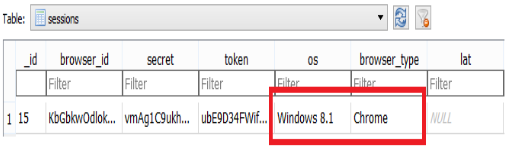


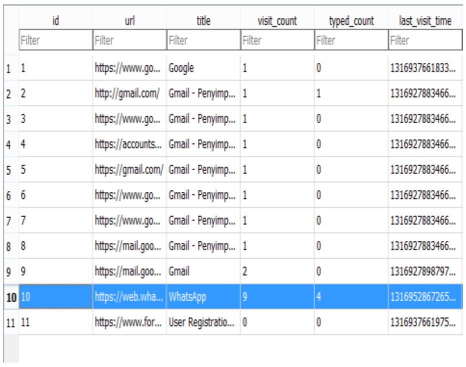
Table: sessions

	_id	browser_id	secret	token	os	browser_type	lat
		Filter	Filter	Filter	Filter	Filter	Filter
1	15	KbGbkwOdlok...	vmAg1C9ukh...	ubE9D34FWif...	Windows 8.1	Chrome	NULL

Figure 8. Usage of WhatsApp web

Figure 8 is the use of WhatsApp web on a smartphone can be viewed using the WhatsApp web contained in the device's smartphone memory, the database is extracted using the DB Browser for SQLite and generates WhatsApp web usage information using Windows OS 8.1 and uses the Chrome web browser as shown in Figure 8.

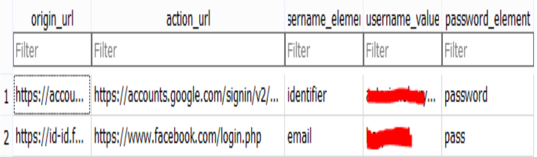
Extract the Google Chrome SQLite database on the laptop boot in the extract stage of the Google Chrome SQLite database on this laptop device can be extracted with tools DB Browser for SQLite SQLite database file is the first in the extract of the history file to know the activities of actors in using Google Chrome to get information about the activities of actors in using Google Chrome to do criminal activity. Extracting the SQLite history database file can be viewed in Figure 9.



	id	url	title	visit_count	typed_count	last_visit_time
	Filter	Filter	Filter	Filter	Filter	Filter
1	1	https://www.go...	Google	1	0	1316937661833...
2	2	http://gmail.com/	Gmail - Penyimp...	1	1	1316927883466...
3	3	https://www.go...	Gmail - Penyimp...	1	0	1316927883466...
4	4	https://accounts...	Gmail - Penyimp...	1	0	1316927883466...
5	5	https://gmail.com/	Gmail - Penyimp...	1	0	1316927883466...
6	6	https://www.go...	Gmail - Penyimp...	1	0	1316927883466...
7	7	https://www.go...	Gmail - Penyimp...	1	0	1316927883466...
8	8	https://mail.goo...	Gmail - Penyimp...	1	0	1316927883466...
9	9	https://mail.goo...	Gmail	2	0	1316927898797...
10	10	https://web.wha...	WhatsApp	9	4	1316952867265...
11	11	https://www.for...	User Registratio...	0	0	1316937661975...

Figure 9. Database SQLite history on Google Chrome

Figure 9 is an SQLite history database Google Chrome can be seen that the offender visits or uses the WhatsApp web with up to 9 visits. And then the SQLite database file that will extract the login data to find the login data of the perpetrator on Google Chrome in Figure 10.

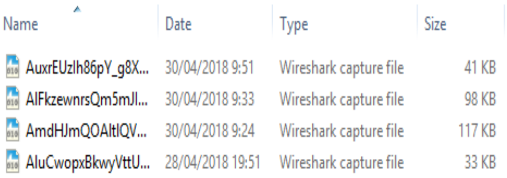


	origin_url	action_url	sername_elemei	username_value	password_element
	Filter	Filter	Filter	Filter	Filter
1	https://accou...	https://accounts.google.com/signin/v2/...	identifier	[redacted]	password
2	https://id-id.f...	https://www.facebook.com/login.php	email	[redacted]	pass

Figure 10. Login data Google Chrome

Figure 10 is Google Chrome login data there is only login activity on google and facebook account, login WhatsApp does not exist because WhatsApp web using QR code and connect with the second party that is

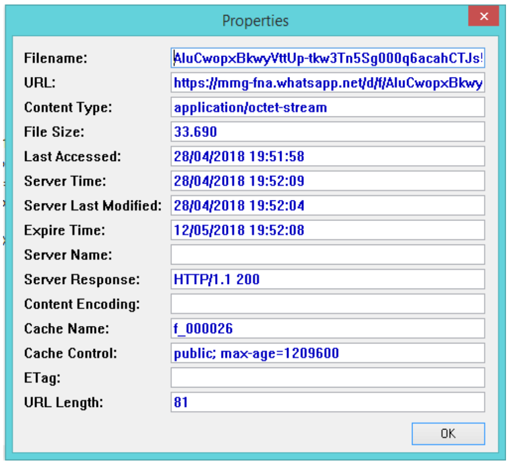
WhatsApp smartphone. Cache file there are some file of actors activity when using Google Chrome there are file name, URL, content type, file size, last accessed, last modified server, expire time and so on, on the URL seen the actor accessing WhatsApp web using Google Chrome, and file name indicated crime there is a network file capture which usually extends the file ". pcapng" but in this cache file there is file capture network extension ".ENC" that is an encrypted file, file extension ".ENC" can be like in Figure 11.



Name	Date	Type	Size
AuxrEUzlh86pY_g8X...	30/04/2018 9:51	Wireshark capture file	41 KB
AlFkzewnrsQm5mJl...	30/04/2018 9:33	Wireshark capture file	98 KB
AmdHJmQOAltIQV...	30/04/2018 9:24	Wireshark capture file	117 KB
AluCwopxBkwyVttU...	28/04/2018 19:51	Wireshark capture file	33 KB

Figure 11. File capture network format ".ENC"

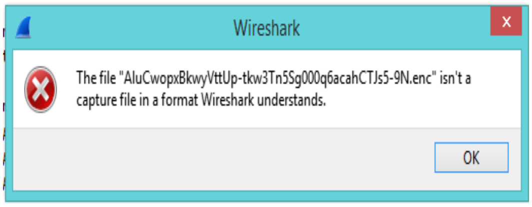
Figure 11 file capture network format ".ENC" which is in the cache is type Wireshark capture file which is indicated as network capture file WhatsApp web that the perpetrators use in Google Chrome. Files indicated as digital evidence WhatsApp web conversations can be viewed at access time as shown in Figure 12.



Filename:	AluCwopxBkwyVttUp-tkw3Tn5Sg000q6acahCTJs!
URL:	https://mmg-fna.whatsapp.net/d/f/AluCwopxBkwy
Content Type:	application/octet-stream
File Size:	33.690
Last Accessed:	28/04/2018 19:51:58
Server Time:	28/04/2018 19:52:09
Server Last Modified:	28/04/2018 19:52:04
Expire Time:	12/05/2018 19:52:08
Server Name:	
Server Response:	HTTP/1.1 200
Content Encoding:	
Cache Name:	f_000026
Cache Control:	public; max-age=1209600
ETag:	
URL Length:	81

Figure 12. Access file extension ".ENC"

Figure 12 is access file extension ".ENC" can be viewed in the date and time access, file size and chace name indicated a crime. Unlike the case of the WhatsApp smartphone database file decryption using the existing key in the device memory, the ".ENC" file is encrypted with another method and there is no key in the perpetrator's laptop directory because of them ".ENC" file extension is a Uuencoded file of the binary encoding method to test if a file with the extension ".ENC" is extracted with Wireshark then ".ENC" extension is not recognized as in Figure 13.



The file "AluCwopxBkwyVttUp-tkw3Tn5Sg000q6acahCTJs5-9N.enc" isn't a capture file in a format Wireshark understands.

Figure 13. Wireshark extension ".ENC"

Figure 13 is a Wireshark extension ".ENC" looks informed that the extension ".ENC" is not recognized and cannot be extracted by Wireshark.

d. Documentation: After the analysis phase of the digital evidence a found at the scene. Data and information are presented in the form of information that can be understood and supported by evidence in accordance with an appropriate and acceptable crime.

4.4 The presentation: is the final stage of the investigation process. Securing the evidence in a safe place and review stage on the investigation of evidence of a crime that has been done for improvement in the process of further investigation.

a. Conclusion: Evidence and information in the investigation process by the investigator is sufficient for the investigation team to demand the perpetrators of fraudulent through the WhatsApp media.

b. Reconstruction: At this stage, the investigator reconstructs based on the findings of the investigative analysis carried out so that the actors' activities can be known in fraudulent using the WhatsApp media.

c. Dissemination: Furthermore, at this final stage is the process of recording at the investigation stage so that if investigators or investigators get a similar case, this investigative process can be a reference in the process of investigation analysis WhatsApp forensic smartphones and laptops.

5 CONCLUSION

WhatsApp is a popular application for social networks where people can exchange personal information between users, this study uses the Integrated Digital Forensic Investigation Framework Version 2 which shows that access to WhatsApp Web synchronized with WhatsApp Smartphones has different access. WhatsApp Web produces information related to access times, browser usage and the operating system used to access WhatsApp Web, and information related to messages on the WhatsApp web is secured by ".ENC" file encryption in cache files that can be opened with ChromeChaceView, on a laptop device. Whatsapp Smartpphone Produces Information related to message content, message time, number of perpetrator and victim, in an encrypted "crypt12" database that can be solved using Whatsapp Viewer.

REFERENCES

1. A. Kurniawan, I. Riadi, and A. Luthfi, “Forensic analysis and prevention of cross-site scripting in single victim attack using open web application security project (OWASP) framework,” *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 6, pp. 1363–1371, 2017.
2. G. M. Zamroni, R. Umar, and I. Riadi, “Forensic Analysis Instant Messaging Application Based on Android,” *Annu. Res. Semin.*, vol. 2, no. 1, pp. 102–105, 2016.
3. Z. Akbar, B. Nugraha, and M. Alaydrus, “Whatsapp Forensics on Android Smartphones: a Survey,” *Sinergi*, vol. 20, no. 3, p. 207, 2016.
4. N. Anwar and I. Riadi, “WhatsApp Messenger Smartphone Forensic Investigation Analysis on Web-based WhatsApp,” vol. 3, no. 1, pp. 1–10, 2017.
5. Ruuhwan, I. Riadi, and Y. Prayudi, “Application of Integrated Digital Forensic Investigation Framework v2 (IDFIF) in the Smartphone Investigation Process,” *J. Edukasi and Penelit. Inform.*, vol. 2, no. 1, pp. 1–8, 2016.
6. M. P. Aji, I. Riadi, and A. Lutfhi, “The digital forensic analysis of snapchat application using XML records,” *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 19, pp. 4992–5002, 2017.
7. Y. Prayudi and D. S. Afrianto, “Anticipating Cybercrime Using Forensic Computer Engineering,” *Snati*, vol. 2007, no. Snati, pp. 1–4, 2007.
8. I. Riadi, Sunardi, and A. Firdonsyah, “Forensic Investigation Technique on Android’s Blackberry Messenger using NIST Framework,” *Int. J. Cyber-Security Digit. Forensics*, vol. 16, no. 4, pp. 198–205, 2017.
9. Y. P. Ruuhwan, Imam Riadi, “Feasibility Analysis of Integrated Digital Forensics Investigation Framework for Smartphone Investigation,” *J. Buana Inform.*, vol. 7, no. 4, pp. 265–274, 2016.
10. S. Sahu, “An Analysis of WhatsApp Forensics in Android Smartphones,” *Int. J. Eng. Res.*, vol. 5013, no. 3, pp. 349–350, 2014.
11. S. Ikhsani and C. Hidayanto, “Forensic Analysis Whatsapp and LINE Messenger Provide Strong and Valid Evidence in Indonesia,” *J. Tek. ITS*, vol. 5, no. 2, 2016.
12. T. Erlina and R. E. Putri, “Evaluate the effect of mapping function on cache memory performance and power consumption,” *J. Ilm. Teknol. Inf. Terap.*, vol. IV, no. 1, 2017.
13. Y. N. Kunang and A. Khristian, “Implementation of forensic procedures for analysis of Whatsapp artifacts on android phones,” in *Annual Research Seminar*, 2016, vol. 2, no. 1, pp. 59–68.
14. Soni, Y. Prayudi, and B. Sugiantoro, “Server Virtualization Acquisition Technique Using Live Forensic Method,” *Teknomatika*, vol. 9, no. 2, 2017.
15. Mansur Zakariyya Shuaibu and A. Bala, “Global Journal of Advanced Engineering Technologies and Sciences,” *Glob. J. Adv. Eng. Technol. Sci.*, vol. 2, no. 8, pp. 33–38, 2015.