Jurnal Elektronik Ilmu Komputer Udayana
Volume 9 No. 4, May 2021

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Cyberbullying Analysis On WhatsApp Messenger Using The National Institute Of Justice (NIJ) Method

I Putu Denny Indra Putra[a1], I Ketut Gede Suhartana[a2]

[a]Informatics Department, Faculty of Math and Science, Udayana University
Bali, Indonesia
[1]dennyindra99z@gmail.com
[2]ikg.suhartana@unud.ac.id

Abstract

Social media is no stranger to today's digital era. Many people prefer to use social media because of its simplicity and safety, This is what makes social media more popular than other services. However, because of its convenience and security, social media, especially WhatsApp Messenger, are vulnerable to crime, one of the most common is cyberbullying. For this reason, a mobile forensic investigation is required to find evidence related to cyberbullying. In this study, the National Institute of Justice (NIJ) method was used to investigate the WhatsApp Messenger platform used for cyberbullying. The NIJ method has 5 (five) stages to carry out the forensic process, namely Preparing, Collection, Examination, Analysis, and Reporting. This study also uses 3 assistance from software, namely MOBILedit Forensic, DB Browser for SQLite, and Odin3. This research is expected to be able to help solve the problem of cyberbullying and other crimes found on social media, especially WhatsApp Messenger.

Keywords: *Media Sosial, WhatsApp, Mobile Forensic, Cyberbullying,* NIJ

1. Introduction

In today's digital era, most people are familiar with social media. Social media is a medium on the internet that allows users to represent themselves and interact, cooperate, share, communicate with other users to form virtual social bonds [1]. It cannot be denied that many people in Indonesia use social media, This can be seen from the research data conducted by We Are Social in 2020, 160 million or 59% of active social media users in Indonesia out of 272.1 million total population in Indonesia.

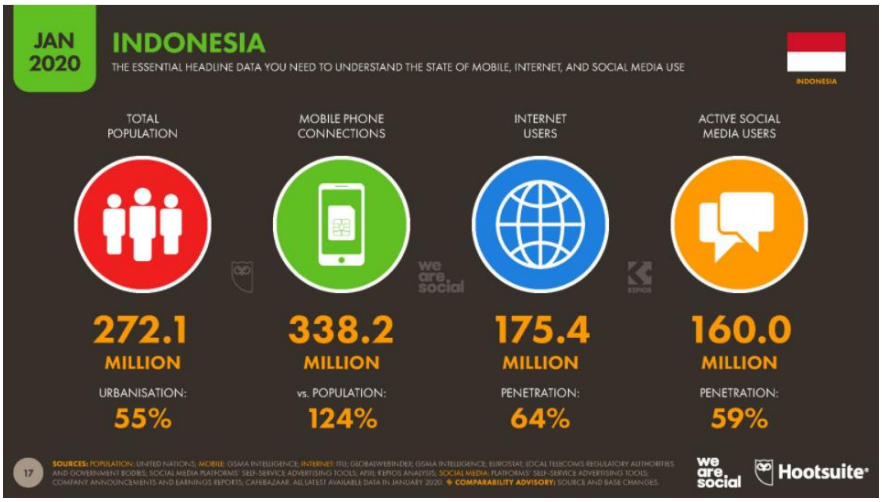


Figure 1. Data on Internet and Social Media Trends in Indonesia January 2020

There are various kinds of social media platforms in Indonesia, one of which is WhatsApp Messenger. WhatsApp Messenger is a mobile application that allows the exchange of messages, video, audio, and pictures via mobile [2] for free. This platform requires the help of the internet so that users can communicate with each other.

However, with this convenience, some people take advantage of social media, especially WhatsApp Messenger, to commit crimes in cyberspace. Crimes committed in cyberspace are often referred to as cybercrime, the crimes vary, such as cyberbullying, data theft, hacking, and so on. To solve a similar problem, forensic action on WhatsApp Messenger is needed, so that the problem can be solved.

It is hoped that the research carried out can help solve problems, especially on cyberbullying problems on WhatsApp Messenger social media. This study uses the National Institute of Justice (NIJ) method and uses MOBILedit Forensic software and DB Browser for SQLite. MOBILedit Forensic Is a forensic software that allows investigators to logically obtain, search and examine cell phone devices [3], while DB Browser for SQLite is software used to perform analysis and search for forensic evidence stored in a database [4].

2. Research Methods

This research uses the National Institute of Justice (NIJ) method. This method is used to explain the stages of research that will be used as a guide in solving a problem [5]. The following is an illustration of the stages of this research.

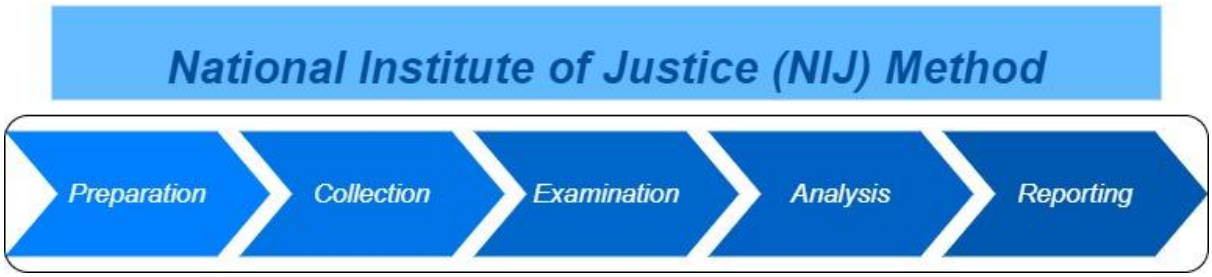


Figure 2. The National Institute of Justice (NIJ) Method stages

There are 5 (five) stages in this research that are used to carry out the forensic process, namely:

a. The preparation stage is the stage where the researcher prepares equipment to support the research process, such as laptops, MOBILedit Forensic software, DB Browser for SQLite software, and Odin3 software.
b. The Collection stage is the activity of collecting and documenting evidence, wherein this study, the evidence is obtained in the form of the perpetrator's smartphone.
c. The Examination stage in this study is to check the data contained on the perpetrator's smartphone, but before that, we have to check whether the smartphone is rooted or not. If not, then you can use the Odin3 software to root your smartphone. After that, data checking can be done with the help of MOBILedit Forensic software.
d. The Analysis stage is the stage where the researcher analyzes the data that has been previously obtained during the examination stage. The data obtained is in the form of a database with SQLite format, so you need help from the DB Browser for SQLite software to read the contents of the database. After that, the data will be analyzed technically and legally to be able to prove the data.
e. The Reporting stage is the activity of making a report that will be carried out after digital evidence is obtained from previous processes, this report will include the results of the analysis in detail, including the actions taken during the investigation, the tools and methods used.

3. Result and Discussion

This study uses case examples related to cyberbullying crimes. In this simulated case, there are 2 (two) users who use WhatsApp Messenger social media, namely user A (victim) uses a

p-ISSN: 2301-5373
e-ISSN: 2654-5101

smartphone with the brand IPHONE 7+ with the A1661 model and user B (the perpetrator) uses a smartphone with the SAMSUNG brand GALAXY GRAND PRIME model. User A has an account name "Denny Indra" while user B has an account name "Isthu Canistya". With the WhatsApp Messenger social media, the two users carry out chat activities both in the form of text messages and picture messages. However, user A feels annoyed with the contents of the message sent by user B, it turns out that the message received by user A is bullying. Furthermore, user A reports the incident to the authorities and after being traced, the incident becomes a cyberbullying case. After that, the authorities confiscated the SAMSUNG brand smartphone with the GALAXY GRAND PRIME model owned by user B, this confiscated item will be investigated further. In this investigation, the authorities used the National Institute of Justice (NIJ) method which has 5 stages for the forensic process.

3.1. Preparation

At this stage, the authorities prepare all the equipment that will be used during the investigation process. The equipment used can be seen in the table below.

Table 1. Equipment used

No	Equipment	Specification	Information
1	Laptop	ASUS VivoBook 8550U Intel Core i7, Windows 10 64bit	Hardware
2	MOBILedit Forensic	Program version 9.0.0.21797	Software
3	DB Browser for SQLite	Program version 3.12.0	Software
4	Odin3	Program version 3.07	Software

3.2. Collection

In this second stage, the authorities are required to collect evidence, both physical items and data contained in the physical goods and their documentation.

Figure 3. Perpetrator's Smartphone

The image above is a documentation of the physical evidence of the smartphone used by the perpetrator to carry out cyberbullying. *The smartphone used by the perpetrator uses the Android*

Operating System version 5.0.2 in a state that has not been rooted. After that, the authorities will take the data in the smartphone by duplicating it, this is so that the original data does not change or is damaged because the original data will later be used as digital evidence.

3.3. Examination

In this third stage what must be done is to check the data contained on the perpetrator's smartphone but before doing that, the authorities must first check whether the smartphone is in root condition or not, if not then the smartphone must be rooted first. Root functions so that users can control or have full access to their smartphone.

Here the authorities use the help of the Odin3 software already installed on the laptop to root the smartphone. If the smartphone is connected to a laptop, the rooting process can be done.

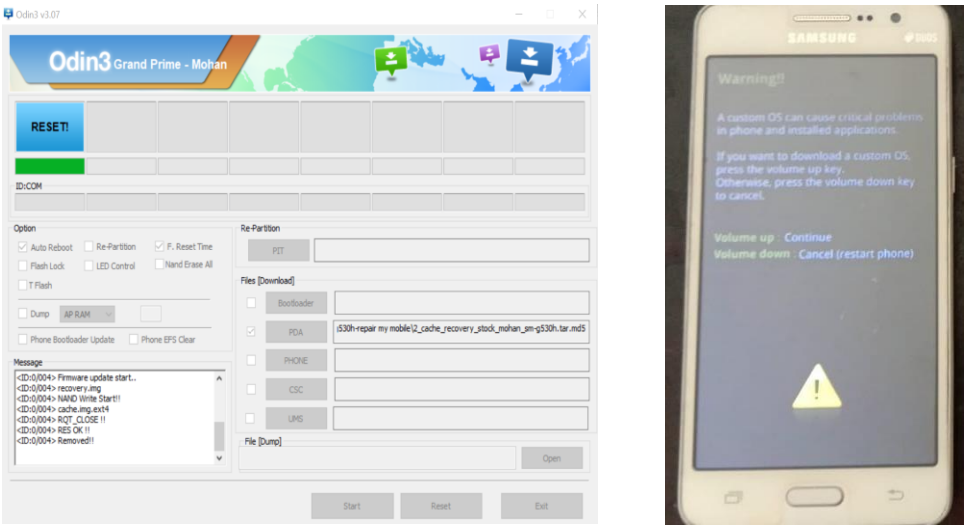


Figure 4. Root Process on The Perpetrator's Smartphone with Odin3 Software

If the smartphone is in root condition, then the inspection process can be done. The examination here uses the help of the MOBILedit Forensic software which is already installed on the laptop, the authorities only need to connect the perpetrator's smartphone with the laptop, if so, the image will appear as below.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

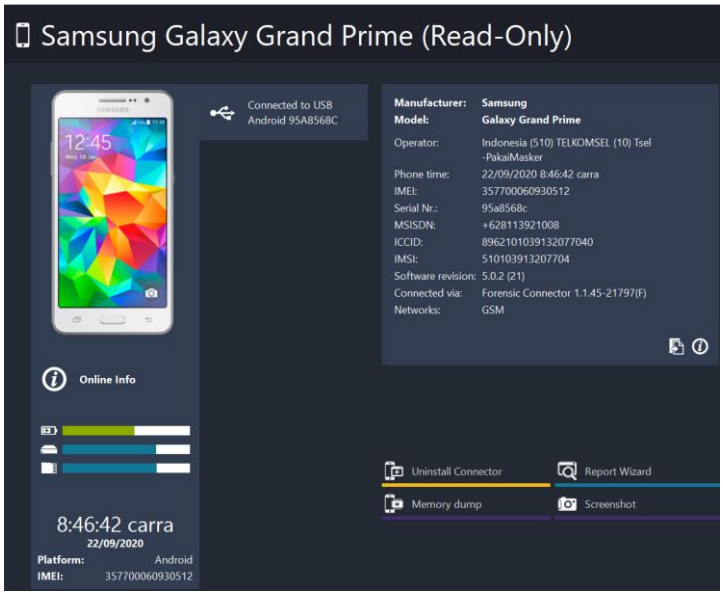


Figure 5. Information About the Perpetrator's Smartphone

In the examination process, apart from obtaining information about the perpetrator's smartphone, the authorities also obtained various types of data contained on the perpetrator's smartphone such as contacts, galleries, applications, and so on. For more details, see the image below.

Figure 6. Results of The Perpetrator's Smartphone Check

In the picture above, there is a WhatsApp Messenger application that was used by the perpetrator to do cyberbullying, so the authorities will immediately carry out further checks on files from the WhatsApp Messenger application which are already in the form of a folder with the name "com.whatsapp", this folder can be found in the directory as follows:

data→data→com.whatsapp

When viewed from the MOBILedit software, this is the contents of the WhatsApp Messenger folder (com.whatsapp).

File Name	Size	Created	Modified	Accessed
app_minidumps	<folder>	19/09/20...	19/09/20...	
app_textures	<folder>	21/09/20...	21/09/20...	
app_webview	<folder>	22/09/20...	21/09/20...	
cache	<folder>	22/09/20...	19/09/20...	
databases	<folder>	22/09/20...	19/09/20...	
files	<folder>	22/09/20...	19/09/20...	
lib-main	<folder>	19/09/20...	19/09/20...	
no_backup	<folder>	19/09/20...	19/09/20...	
shared_prefs	<folder>	22/09/20...	19/09/20...	
lib	<unknow...	<unknow...	22/09/20...	

Figure 7. WhatsApp Messenger Application Folder (com.whatsapp)

In the picture above, there are 9 sub-folders and 1 file with the name “lib”, the number of folders depends on the use of the WhatsApp Messenger application. Next, the authorities will check every sub-folder contained in the “com.whatsapp” folder. From the results of the examination, several files were obtained in the form of a database with SQLite format. To find out the contents of the file, the authorities will open it with the help of DB Browser for SQLite software for further analysis.

3.4. Analysis

In this fourth stage, the authorities will analyze the database with the SQLite format that has been obtained with the name "msgstore.db". From the analysis using DB Browser for SQLite software, there are 112 tables in the database "msgstore.db", which can be seen in the image below for more details.

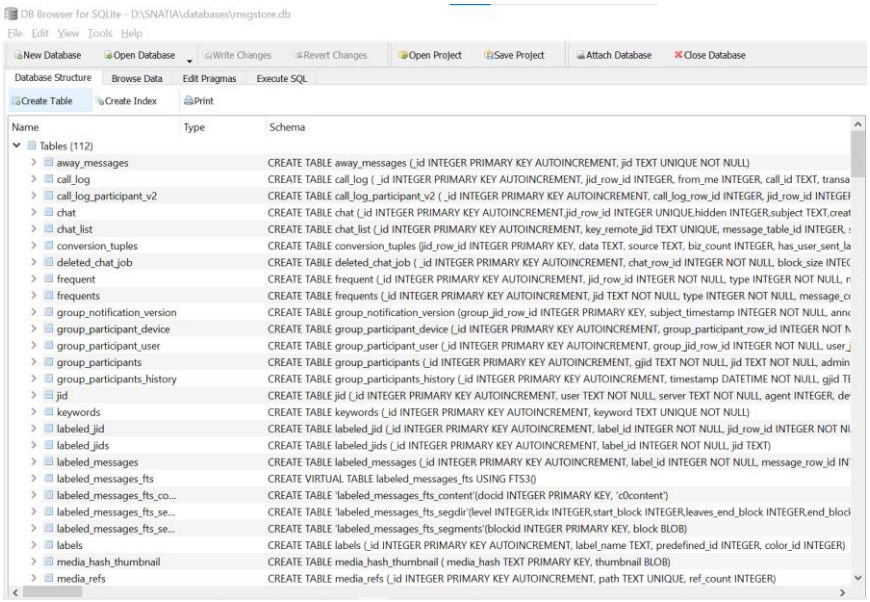
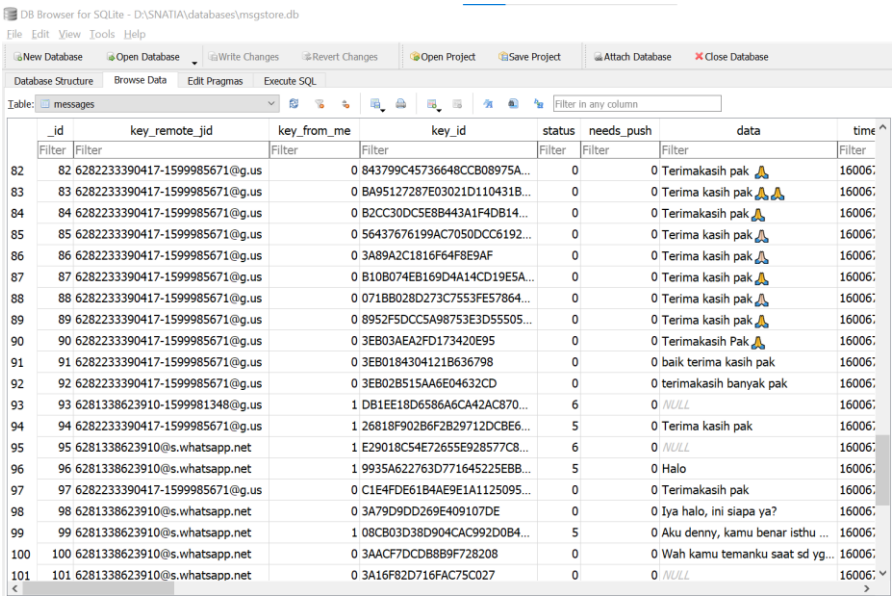


Figure 8. Table Structure in Database "msgstore.db"

First of all, the authorities want to know the messages from anyone on the perpetrator's account. So that the authorities will open the messages table in the DB Browser for SQLite software, and get the following results.

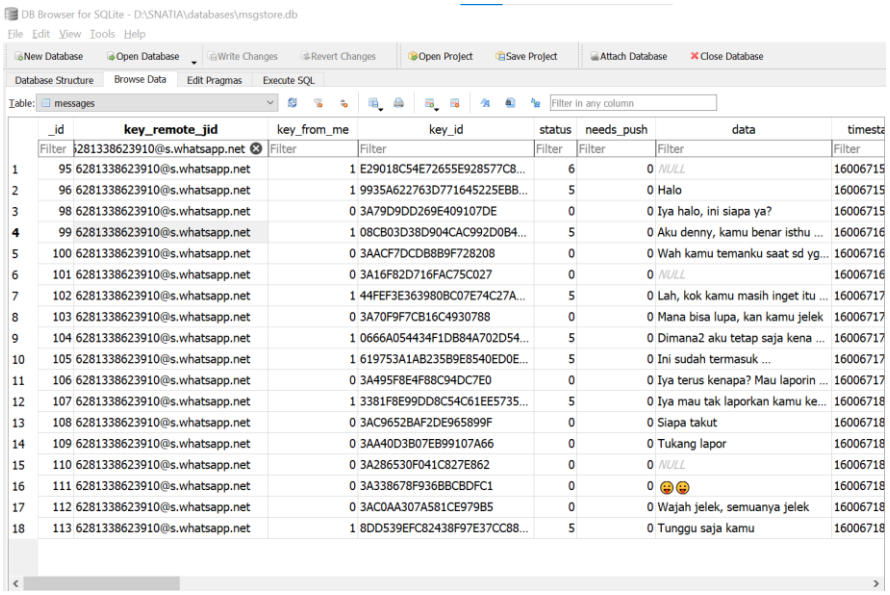
p-ISSN: 2301-5373
e-ISSN: 2654-5101



	_id	key_remote_jid	key_from_me	key_id	status	needs_push	data	time
82	82	6282233390417-1599985671@g.us	0	843799C45736648CCB08975A...	0	0	Terimakasih pak 🙏	16006
83	83	6282233390417-1599985671@g.us	0	BA95127287E03021D110431B...	0	0	Terima kasih pak 🙏🙏	16006
84	84	6282233390417-1599985671@g.us	0	B2CC30DC5E8B443A1F4DB14...	0	0	Terimakasih pak 🙏	16006
85	85	6282233390417-1599985671@g.us	0	56437676199AC7050DCC6192...	0	0	Terima kasih pak 🙏	16006
86	86	6282233390417-1599985671@g.us	0	3A89A2C1816F64F8E9AF	0	0	Terima kasih pak 🙏	16006
87	87	6282233390417-1599985671@g.us	0	B10B074EB169D4A14CD19E5A...	0	0	Terima kasih pak 🙏	16006
88	88	6282233390417-1599985671@g.us	0	071BB028D273C7553FE57864...	0	0	Terima kasih pak 🙏	16006
89	89	6282233390417-1599985671@g.us	0	8952F5DCC5A98753E3D55505...	0	0	Terima kasih pak 🙏	16006
90	90	6282233390417-1599985671@g.us	0	3EB03AEA2FD173420E95	0	0	Terimakasih Pak 🙏	16006
91	91	6282233390417-1599985671@g.us	0	3EB0184304121B636798	0	0	baik terima kasih pak	16006
92	92	6282233390417-1599985671@g.us	0	3EB02B515AA6E04632CD	0	0	terimakasih banyak pak	16006
93	93	6281338623910-1599981348@g.us	1	DB1EE18D6586A6CA42AC870...	6	0	NULL	16006
94	94	6282233390417-1599985671@g.us	1	26818F902B6F2B29712DCBE6...	5	0	Terima kasih pak	16006
95	95	6281338623910@s.whatsapp.net	1	E29018C54E72655E928577C8...	6	0	NULL	16006
96	96	6281338623910@s.whatsapp.net	1	9935A622763D771645225EBB...	5	0	Halo	16006
97	97	6282233390417-1599985671@g.us	0	C1E4FDE61B4AE9E1A1125095...	0	0	Terimakasih pak	16006
98	98	6281338623910@s.whatsapp.net	0	3A79D9DD269E409107DE	0	0	Iya halo, ini siapa ya?	16006
99	99	6281338623910@s.whatsapp.net	1	08CB03D38D904CAC992D0B4...	5	0	Aku denny, kamu benar isthu ...	16006
100	100	6281338623910@s.whatsapp.net	0	3AACF7DCDB8B9F728208	0	0	Wah kamu temanku saat sd yg...	16006
101	101	6281338623910@s.whatsapp.net	0	3A16F82D716FAC75C027	0	0	NULL	16006

Figure 9. The Contents of The messages Table

From the picture above, we can get several conversations from the perpetrator with other accounts. But what is most needed is a conversation between the perpetrator and the victim. From some of these conversations, we get a message that says “Aku denny……”. For that, a filter is needed so that you can find out the entire message of the conversation.



	_id	key_remote_jid	key_from_me	key_id	status	needs_push	data	timesta
	Filter	6281338623910@s.whatsapp.net	Filter	Filter	Filter	Filter	Filter	Filter
1	95	6281338623910@s.whatsapp.net	1	E29018C54E72655E928577C8...	6	0	NULL	16006715
2	96	6281338623910@s.whatsapp.net	1	9935A622763D771645225EBB...	5	0	Halo	16006715
3	98	6281338623910@s.whatsapp.net	0	3A79D9DD269E409107DE	0	0	Iya halo, ini siapa ya?	16006715
4	99	6281338623910@s.whatsapp.net	1	08CB03D38D904CAC992D0B4...	5	0	Aku denny, kamu benar isthu ...	16006716
5	100	6281338623910@s.whatsapp.net	0	3AACF7DCDB8B9F728208	0	0	Wah kamu temanku saat sd yg...	16006716
6	101	6281338623910@s.whatsapp.net	0	3A16F82D716FAC75C027	0	0	NULL	16006716
7	102	6281338623910@s.whatsapp.net	1	44FEF3E363980BC07E74C27A...	5	0	Lah, kok kamu masih inget itu ...	16006717
8	103	6281338623910@s.whatsapp.net	0	3A70F9F7CB16C4930788	0	0	Mana bisa lupa, kan kamu jelek	16006717
9	104	6281338623910@s.whatsapp.net	1	0666A054434F1DB84A702D54...	5	0	Dimana2 aku tetap saja kena ...	16006717
10	105	6281338623910@s.whatsapp.net	1	619753A1AB235B9E8540ED0E...	5	0	Ini sudah termasuk ...	16006717
11	106	6281338623910@s.whatsapp.net	0	3A495F8E4F88C94DC7E0	0	0	Iya terus kenapa? Mau laporin ...	16006717
12	107	6281338623910@s.whatsapp.net	1	3381F8E99DD8C54C61EE5735...	5	0	Iya mau tak laporkan kamu ke...	16006718
13	108	6281338623910@s.whatsapp.net	0	3AC9652BAF2DE965899F	0	0	Siapa takut	16006718
14	109	6281338623910@s.whatsapp.net	0	3AA40D3B07EB99107A66	0	0	Tukang lapor	16006718
15	110	6281338623910@s.whatsapp.net	0	3A286530F041C827E862	0	0	NULL	16006718
16	111	6281338623910@s.whatsapp.net	0	3A338678F936BBCBDFC1	0	0	😀😀	16006718
17	112	6281338623910@s.whatsapp.net	0	3AC0AA307A581CE979B5	0	0	Wajah jelek, semuanya jelek	16006718
18	113	6281338623910@s.whatsapp.net	1	8DD539EFC82438F97E37CC88...	5	0	Tunggu saja kamu	16006718

Figure 10. The Contents of The messages Table after Filtering

In the picture above, there is a conversation between the perpetrator and the victim who has the attribute "6281338623910@s.whatsapp.net" in the column "key_remote_jid". In the conversation between the perpetrator and the victim, there are messages that are bullying that the perpetrator throws at the victim and there are several messages that the DB Browser for SQLite software cannot get, this can be seen in the data column which only displays NULL.

From the results of this analysis, the conversation between the perpetrator and the victim can be used as digital evidence for cyberbullying cases by using the WhatsApp Messenger social media as the platform.

3.5. Reporting

In this study using the National Institute of Justice (NIJ) method, this method has 5 (five) stages in the forensic process. The first stage is Preparing, at this stage, the authorities will prepare digital equipment in the form of laptops, smartphones, MOBILedit Forensic software, DB Browser for SQLite software, and Odin3 software. Continue at the second stage, namely Collection, the authorities will collect evidence both physical goods and data contained in physical goods, after obtaining the evidence, it will be duplicated so that the original evidence is not changed or damaged. Entering the third stage, namely Examination, before carrying out further checks, the authorities must confirm whether the smartphone is in a root condition or not, if not then the smartphone will be rooted with the Odin3 software. If you are already in the root condition, you can also check the data contained on your smartphone, the authorities use 2 (two) pieces of software, namely MOBILedit Forensic and DB Browser for SQLite. *MOBILedit Forensic functions to process smartphones, both extracting and acquiring data contained in the smartphone, the authorities also find folders and files contained on WhatsApp Messenger (com.whatsapp)*. From the results of the folder inspection, there were 9 sub-folders and 1 file with the name "lib". After further examination, important data is obtained with the name "msgstore.db", "msgstore.db". This is a data storage place in the form of a database in SQLite format. The authorities use the second software, namely DB Browser for SQLite to open the database. After opening, there are 112 tables in the database. Kemudian pihak berwajib langsung memeriksa tabel *messages*, dari analisis ini didapatkan beberapa percakapan dari pelaku. After further investigation, a bullying message was obtained between the perpetrator and the victim, and this message will later be used as digital evidence for further processing.

4. Conclusion

The goal of this research is to help solve cyberbullying problems on social media, especially WhatsApp Messenger, by means of mobile forensics using the National Institute of Justice (NIJ) method and using the help of MOBILedit Forensic software, DB Browser for SQLite, and Odin3. The method used in this study has 5 stages to carry out the forensic process, namely Preparing, Collection, Examination, Analysis, and Reporting. In the first stage, the authorities prepare equipment such as laptops and various software. In the second and third stages, the authorities used MOBILedit Forensic software, while the DB Browser for SQLite software was used in the fourth stage. From the use of MOBILedit Forensic software, important data is obtained in the form of a database with the name com.whatsapp. Furthermore, this database is analyzed using DB Browser for SQLite software. From this analysis, the bullying message is obtained in the conversation between the perpetrator and the victim. These results can then be used as digital evidence for cyberbullying cases.

References

[1] Mukti, W. A., Masruroh, S. U. & Khairani, D., 2017. ANALISA DAN PERBANDINGAN BUKTI FORENSIK APLIKASI MEDIA SOSIAL FACEBOOK DAN TWITTER PADA SMARTPHONE ANDROID. *JURNAL TEKNIK INFORMATIKA,* p. 73.

[2] Nasrullah, R., 2015. *Media Sosial Perspektif Komunikasi, Budaya Dan Sosioteknologi.* Bandung: Simbiosa Rekatama Media.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

[3] Riadi, I., Umar, R. & Nasrulloh, I. M., 2018. ANALISIS FORENSIK DIGITAL PADA FROZEN SOLID STATE DRIVE DENGAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ). *ELINVO(Electronics, Informatics, and Vocational Education),* Volume 3, pp. 70-82.

[4] Sahu, M. S., 2014. An Analysis of WhatsApp Forensics in Android Smartphones. *International Journal of Engineering Research,* 3(5), pp. 349-350.

[5] Yadi, I. Z. & Kunang, Y. N., 2014. ANALISIS FORENSIK PADA PLATFORM ANDROID. *Konferensi Nasional Ilmu Komputer (KONIK).*

This page is intentionally left blank