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

I Putu Denny Indra Putra^{a1}, I Ketut Gede Suhartana^{a2}

^aInformatics Department, Faculty of Math and Science, Udayana University Bali, Indonesia ¹dennyindra99z@gmail.com ²ikg.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.

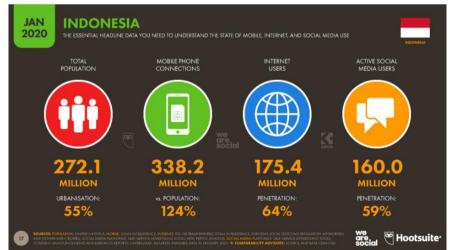


Figure 1. Data on Internet and Social Media Trends in Indonesia January 2020

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

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.

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

Table 1.	Equipment used
----------	----------------

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.

Odin3 v3.07		- • ×	•				
Odin3 Grand Prime - Mohan	R. File		RAMSUNG #1005				
RESETI			A custom OS can cause critical problems in phone and installed applications.				
ID:COM			If you want to download a custom OS. press the volume up key. Otherwise, press the volume down key to cancel.				
Option	Re-Partition						
Auto Reboot Re-Partition F. Reset Time	PIT Volume up Continue Volume down Cancel (restart phone)						
Flash Lock LED Control Nand Erase All	Files [Download]						
	Bootloader						
Dump AP RAM ~	PDA 1530h-repair my mobile\2_cache_reco	very_stock_mohan_sm-g530h.tar.md5					
Phone Bootloader Update Phone EFS Clear			the strength of the State of the state				
Message <1D:0.004> Firmware update start	PHONE						
<id:0 004=""> recovery.img <id:0 004=""> naND Write Start!!</id:0></id:0>	CSC		!				
<id:0 004=""> cache.img.ext4 <id:0 004=""> RQT_CLOSE !!</id:0></id:0>	UMS		the second s				
<id:0 004=""> RES OK !! <id:0 004=""> Removed!!</id:0></id:0>	File [Dump]		Contraction of the second s				
×		Open					
			0 0 5				
	Start Reset	Exit					

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.

🛿 Samsung Gala	xy Grand Pri	me (Rea	d-Onl	y)	
	Connected to USB Android 95A8568C	Manufacturer: Model:	Samsung Galaxy Grand	Prime	
12:45		Operator:) TELKOMSEL (10) Tsel	
		Phone time:	-PakaiMasker 22/09/2020 8:	46:42 carra	
		IMEI:	357700060930		
		Serial Nr.:	95a8568c		
		MSISDN: ICCID:	+62811392100		
		IMSI:	510103913207		
		Software revision:			
		Connected via: Networks:	Forensic Conne GSM	ector 1.1.45-21797(F)	
· · · ·		Networks.	CSM		
					D
(i) Online Info					
		Uninstall Conr	nector	Q Report Wizard	
		Demory dum		O' Screenshot	
8:46:42 carra					
Platform: Android					
IMEI: 357700060930512					

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></folder>	19/09/20	19/09/20	
app_textures	<folder></folder>	21/09/20	21/09/20	
app_webview	<folder></folder>	22/09/20	21/09/20	
🖻 cache	<folder></folder>	22/09/20	19/09/20	
🖿 databases	<folder></folder>	22/09/20	19/09/20	
🖿 files	<folder></folder>	22/09/20	19/09/20	
🖿 lib-main	<folder></folder>	19/09/20	19/09/20	
🖿 no_backup	<folder></folder>	19/09/20	19/09/20	
shared_prefs	<folder></folder>	22/09/20	19/09/20	
lib	<unknow< td=""><td><unknow< td=""><td>22/09/20</td><td></td></unknow<></td></unknow<>	<unknow< td=""><td>22/09/20</td><td></td></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.

New Database	Open Database	→ Write Ch	anges 🔅 Revert Changes	Open Project	Save Project	Attach Database	× Close Database
Database Structure	Browse Data	Edit Pragmas	Execute SQL				
Create Table	Create Index	@Print					
Name		Туре	Schema				
 Tables (112) 							
> 🔳 away_m	issages		CREATE TABLE away_mest	sages (_id INTEGER PR	IMARY KEY AUTO	INCREMENT, jid TEXT	UNIQUE NOT NULL)
> 🔤 call_log			CREATE TABLE call_log (id INTEGER PRIMARY	KEY AUTOINCREM	IENT, jid_row_id INTEG	ER, from_me INTEGER, call_id TEXT, transa
> 🔟 call_log_	participant_v2		CREATE TABLE call_log_pa	articipant_v2 (_id INTE	GER PRIMARY KEY	AUTOINCREMENT, ca	Il_log_row_id INTEGER, jid_row_id INTEGE
> 📃 chat			CREATE TABLE chat (_id IN	NTEGER PRIMARY KEY	AUTOINCREMENT	f.jid_row_id INTEGER U	NIQUE, hidden INTEGER, subject TEXT, crea
> 💷 chat_list			CREATE TABLE chat_list (_i	INTEGER PRIMARY	KEY AUTOINCREM	IENT, key_remote_jid T	EXT UNIQUE, message_table_id INTEGER,
> 🔲 conversi	on_tuples		CREATE TABLE conversion	_tuples (jid_row_id IN	TEGER PRIMARY K	EY, data TEXT, source	TEXT, biz_count INTEGER, has_user_sent_la
> 🔤 deleted_	chat_job		CREATE TABLE deleted_ch	at_job (_id INTEGER P	RIMARY KEY AUT	OINCREMENT, chat_ro	w_id INTEGER NOT NULL, block_size INTE
> 📃 frequent			CREATE TABLE frequent (id INTEGER PRIMARY	KEY AUTOINCREM	MENT, jid_row_id INTEC	ER NOT NULL, type INTEGER NOT NULL, I
> 🔟 frequent	s		CREATE TABLE frequents	(id INTEGER PRIMAR)	Y KEY AUTOINCRE	MENT, jid TEXT NOT N	ULL, type INTEGER NOT NULL, message_c
> 🔤 group_n	otification_version		CREATE TABLE group_not	tification_version (grou	p_jid_row_id INTE	GER PRIMARY KEY, su	bject_timestamp INTEGER NOT NULL, ann
> 🔲 group_p	articipant_device		CREATE TABLE group_par	ticipant_device (_id IN	TEGER PRIMARY K	EY AUTOINCREMENT,	group_participant_row_id INTEGER NOT N
> 🔟 group_p	articipant_user		CREATE TABLE group_par	ticipant_user (_id INTE	GER PRIMARY KEY	AUTOINCREMENT, gr	roup_jid_row_id INTEGER NOT NULL, user_
> group_p	articipants		CREATE TABLE group_par	ticipants (_id INTEGER	PRIMARY KEY AU	TOINCREMENT, gjid T	EXT NOT NULL, jid TEXT NOT NULL, admir
> 🗾 group_p	articipants_history		CREATE TABLE group_par	ticipants_history (_id II	NTEGER PRIMARY	KEY AUTOINCREMEN	T, timestamp DATETIME NOT NULL, gjid T
> 🗐 jid			CREATE TABLE jid (_id INT	EGER PRIMARY KEY A	UTOINCREMENT,	user TEXT NOT NULL, s	server TEXT NOT NULL, agent INTEGER, de
> 💷 keyword	s		CREATE TABLE keywords	(id INTEGER PRIMARY	Y KEY AUTOINCRE	MENT, keyword TEXT	UNIQUE NOT NULL)
> 🔟 labeled_j	id		CREATE TABLE labeled_jid	(id INTEGER PRIMAP	RY KEY AUTOINCR	EMENT, label_id INTEG	ER NOT NULL, jid_row_id INTEGER NOT N
> 🔤 labeled_j	ids		CREATE TABLE labeled_jid	s (_id INTEGER PRIMA	RY KEY AUTOINCE	REMENT, label_id INTE	GER NOT NULL, jid TEXT)
> 🔤 labeled_	messages		CREATE TABLE labeled_m	essages (_id INTEGER I	PRIMARY KEY AUT	OINCREMENT, label_id	d INTEGER NOT NULL, message_row_id IN
> 🔤 labeled_	messages_fts		CREATE VIRTUAL TABLE la	abeled_messages_fts L	JSING FTS3()		
> 🔤 labeled_i	messages_fts_co		CREATE TABLE 'labeled_m	essages_fts_content'(c	docid INTEGER PR	IMARY KEY, 'c0content	:')
> 📃 labeled_	nessages_fts_se		CREATE TABLE 'labeled_m	essages_fts_segdir'(lev	vel INTEGER, idx IN	TEGER, start_block INT	EGER,leaves_end_block INTEGER,end_bloc
	messages_fts_se		CREATE TABLE 'labeled_m		Contraction of the second of t		
> 🔤 labels							redefined_id INTEGER, color_id INTEGER)
> 📃 media_h			CREATE TABLE media_has				
> 🗐 media re	fs		CREATE TABLE media refs	/ id INTEGER PRIMAR	V KEV ALITOINCE	EMENT	OUE and anoth INTECED

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.

Ne	w Databa	se 🛛 🖗 Open Database 🖕 🗟 Write Chan	ges 🛛 🗟 Revert Cha	nges 🚱 Open Project 🕼 Save	Project	Attach Datab	ase XClose Database	
Data	base Strue	cture Browse Data Edit Pragmas H	Execute SQL					
[able:	🔲 mess	sages	× 🕄 % 🔹	5,8 5,8 A 6	Pilter	in any column		
	_id	key_remote_jid	key_from_me	key_id	status	needs_push	data	time
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
82	82	6282233390417-1599985671@g.us	0	843799C45736648CCB08975A	0	C	Terimakasih pak 🙏	16006;
83	83	6282233390417-1599985671@g.us	0	BA95127287E03021D110431B	0	C	Terima kasih pak 🙏 🙏	160067
84	84	6282233390417-1599985671@g.us	0	B2CC30DC5E8B443A1F4DB14	0	C	Terimakasih pak 🙏	16006;
85	85	6282233390417-1599985671@g.us	0	56437676199AC7050DCC6192	0	C	Terima kasih pak 🙏	16006;
86	86	6282233390417-1599985671@g.us	0	3A89A2C1816F64F8E9AF	0	C	Terima kasih pak 🙏	16006;
87	87	6282233390417-1599985671@g.us	0	B10B074EB169D4A14CD19E5A	. 0	C	Terima kasih pak 🙏	16006;
88	88	6282233390417-1599985671@g.us	0	071BB028D273C7553FE57864	0	C	Terima kasih pak 🙏	16006;
89	89	6282233390417-1599985671@g.us	0	8952F5DCC5A98753E3D55505	0	C	Terima kasih pak 🙏	16006;
90	90	6282233390417-1599985671@g.us	0	3EB03AEA2FD173420E95	0	C	Terimakasih Pak 🙏	16006;
91	91	6282233390417-1599985671@g.us	0	3EB0184304121B636798	0	C	baik terima kasih pak	16006;
92	92	6282233390417-1599985671@g.us	0	3EB02B515AA6E04632CD	0	C	terimakasih banyak pak	16006;
93	93	6281338623910-1599981348@g.us	1	DB1EE18D6586A6CA42AC870	6	C	NULL	16006;
94	94	6282233390417-1599985671@g.us	1	26818F902B6F2B29712DCBE6	5	C	Terima kasih pak	16006;
95	95	6281338623910@s.whatsapp.net	1	E29018C54E72655E928577C8	6	C	NULL	16006;
96	96	6281338623910@s.whatsapp.net	1	9935A622763D771645225EBB	5	C	Halo	16006;
97	97	6282233390417-1599985671@g.us	0	C1E4FDE61B4AE9E1A1125095	0	C	Terimakasih pak	16006;
98	98	6281338623910@s.whatsapp.net	0	3A79D9DD269E409107DE	0	C	Iya halo, ini siapa ya?	16006;
99	99	6281338623910@s.whatsapp.net	1	08CB03D38D904CAC992D0B4	5	C	Aku denny, kamu benar isthu	16006;
100	100	6281338623910@s.whatsapp.net	0	3AACF7DCDB8B9F728208	0	C	Wah kamu temanku saat sd yg	16006;
101		6281338623910@s.whatsapp.net	0	3A16F82D716FAC75C027	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.

Data	base Stru	ase Open Database GWrite Chan cture Browse Data Edit Pragmas I	Execute SOL					
	🔲 mes		V S S	6.8.5.4.6	4 Filter	in any column		
Labie.	id	kev remote jid	key from me	key_id	status	needs push	data	time
	_		Filter	Filter	Filter	Filter	Filter	Filter
1		6281338623910@s.whatsapp.net		E29018C54E72655E928577C8	6		NULL	160067
2		6281338623910@s.whatsapp.net		9935A622763D771645225EBB	5		Halo	160067
3		6281338623910@s.whatsapp.net		3A79D9DD269E409107DE	0		Iya halo, ini siapa ya?	160067
4		6281338623910@s.whatsapp.net		08CB03D38D904CAC992D0B4	5		Aku denny, kamu benar isthu	160067
5		6281338623910@s.whatsapp.net		3AACF7DCDB8B9F728208	0		Wah kamu temanku saat sd yg	
6		6281338623910@s.whatsapp.net	-	3A16F82D716FAC75C027	0		NULL	160067
7		6281338623910@s.whatsapp.net		44FEF3E363980BC07E74C27A	5		Lah, kok kamu masih inget itu	
8		6281338623910@s.whatsapp.net	-	3A70F9F7CB16C4930788	0	-		160067
9		6281338623910@s.whatsapp.net		0666A054434F1DB84A702D54			Dimana2 aku tetap saja kena	160067
10		6281338623910@s.whatsapp.net		619753A1AB235B9E8540ED0E			Ini sudah termasuk	160067
10		6281338623910@s.whatsapp.net		3A495F8E4F88C94DC7E0	0		Iya terus kenapa? Mau laporin	
12		6281338623910@s.whatsapp.net		3381F8E99DD8C54C61EE5735	5		Iya mau tak laporkan kamu ke	
12		6281338623910@s.whatsapp.net	-	3AC9652BAF2DE965899F	0		Siapa takut	160067
13		6281338623910@s.whatsapp.net	-	3AA40D3B07EB99107A66	0	-	Tukang lapor	160067
14		6281338623910@s.whatsapp.net		3A286530F041C827E862	0		NULL	160067
15		6281338623910@s.whatsapp.net	-	3A338678F936BBCBDFC1	0	-		160067
17		6281338623910@s.whatsapp.net		3AC0AA307A581CE979B5	0		😝 😜 Wajah jelek, semuanya jelek	160067
17		6281338623910@s.whatsapp.net		8DD539EFC82438F97E37CC88			Tunggu saja kamu	160067

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.

- [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