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

Acquisition of *LINE* Digital Social Media Evidence Using the *National Institute of Justice* (NIJ) Method

Gede Pawitradi[a1], I Ketut Gede Suhartana[a2]

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

Abstract

Nowadays the use of social media has developed very rapidly over time. With very easy to use and also higher security than ordinary messaging services, making one of the factors of social media is very often used in today's world. But behind it all, social media such as LINE is very vulnerable to become one of the crime facilities, one of which is cyberbullying. To follow up on the cyberbullying activity, a forensic cellphone needs to be carried out to find evidence which is then useful to send to court. This study uses the LINE application as cyberbullying crime media, as well as using the National Institute of Justice (NIJ) method. The National Institute of Justice (NIJ) method has five basic stages namely, preparation, collection, examination, analysis, and reporting. In this study using the MOBILedit Forensic tool, and DB Browser for SQLite.

Keywords: *Social media, LINE, cyberbullying, mobile forensics, NIJ*

1. Introduction

The use of social media has grown very rapidly over time. Social media is a tertiary need whose needs must be met like a primary need, and can be enjoyed anywhere and by anyone without exception. Based on research conducted by the organization We Are Social and Hootsuite, entitled "Essential Insights into How People Around the World social networks around the world are 3,534 billion people or 46% of the world's total population, around 3,463 billion people access social media through smartphones or 45% of the world's population [1].

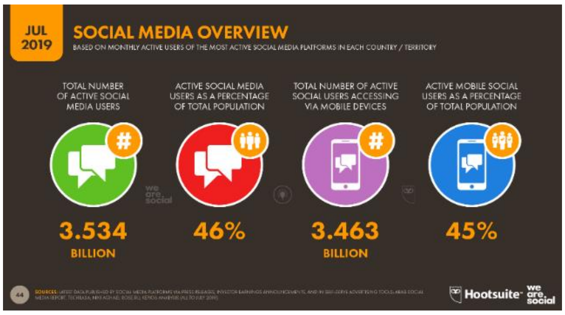


Figure 1. Number of Active Users of Social Media Worldwide in July 2019

One of the most used social media right now is LINE. LINE is a free instant messaging application that has been around since June 2011 [2]. With the help of the internet, users can already communicate with fellow users, such as sending messages, phone calls and video calls, and so forth. However, at this time social media such as LINE is often used as a tool to commit cyber crimes by irresponsible parties, such as cyberbullying, fraud, hoaxes spread, hate speech and other related crimes. One of the crimes of cyberbullying is that it happened to Brandy Vela, an 18-year-old teenager from Texas who continues to receive abusive texts on social media by her harasser, as a result this teenager is trying to improve by shoot her own chest. To overcome these crimes, forensic action is urgently needed, so that the criminal problems in LINE social media applications can be solved.

Figure 2. LINE Social Media Logo

For this reason, it is hoped that the research carried out can help solve cyberbullying problems on LINE social media in mobile forensics using the National Institute of Justice (NIJ) method and with the help of MOBILedit Forensic software and DB Browser for SQLite. MOBILedit Forensic is a forensic device used by investigators to carry out investigations of logical mobile devices. Usually this tool is used by investigators to obtain telephone system information and other information such as contact lists and messages (SMS) [3]. Whereas DB Browser for SQLite is an open source software that is used to create, design, and edit database files that are compatible with SQLite [4].

As for previous studies related to this study include:

- Research entitled “Akuisisi Bukti Digital Pada Instagram *Messenger* Berbasis Android Menggunakan Metode *National Institute Of Justice* (NIJ)” conducted by Imam Riadi, Anton Yudhana, Muhammad Caesar Febriyansah Putra from Ahmad Dahlan University, in 2018. They analyzed the data on smartphones the perpetrators and victims used the National Institute of Justice (NIJ) method and with the help of OXYGEN forensic software [5].
- Research entitled “Ananlisa Forensik Whatsapp dan LINE *Messenger* pada *Smartphone* Android sebagai Rujukan dalam Menyediakan Barang Bukti yang Kuat dan valid di Indonesia” by Syukur Ikhsani and Bekti Cahyo Hidayanto from the Ten November Institute of Technology (ITS), 2016. They did a comparison starting from the folder structure from each application, to comparing the results of experimental data obtained from the study. In this study using the help of FTK Imager and SQLite Browser software [6].
- The study, entitled “Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ)” by Anton Yudhana, Rusydi Umar, Ahwan Ahamadi from Ahmad Dahlan University. They made a comparison of the results of digital evidence analysis from two different tools using the Oxygen Forensics and Mobile Edit Forensics tools, from the study it was found that the Oxygen Forensics tool was superior to the Mobile Edit Forensics tool [7].

2. Research Methods

In this study using the National Institute of Justice (NIJ) method which serves to explain the stages or flow of research conducted so that it can be used as a reference for solving problems. The stages of the National Institute of Justice (NIJ) method are described as follows:

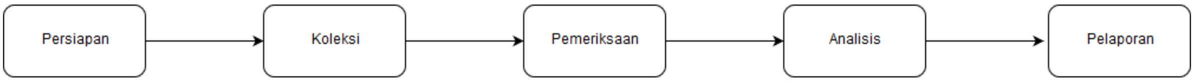


Figure 3. National Institute of Justice (NIJ) Method Stage

In the flow chart above, it is explained that the National Institute of Justice (NIJ) method has 5 (five) basic stages in the forensic process, namely preparation, collection, examination, analysis, and reporting. Preparation is the process of preparing equipment that will be used to conduct an investigation. Collection is a process of collecting or making copies of data obtained during an investigation in order to support the investigation process in the search for digital evidence, at this stage the investigator is required to maintain the integrity of evidence from changes. Inspection is the process by which content and system are documented, data reduction is carried out to identify evidence. Analysis is the process of analyzing evidence that has been obtained from the results of the examination and to find out everything that has been done by the user, later the results of this analysis can be used as digital evidence and can be justified scientifically and legally. And the last stage is reporting, i.e. reporting or explaining the results of an analysis consisting of actions taken during an investigation, an explanation of the tools used when conducting an investigation, as well as the method used [8] [9].

3. Result and Discussions

In this study using a case example indicated the crime of cyberbullying. In the example case that will be simulated, there will be two users of LINE application, namely user a (perpetrator) and user b (victim). Both users have different smartphones, namely user a (the perpetrator) uses a smartphone with the SAMSUNG GALAXY GRAND PRIME brand with the SM-G531H series, while user b uses a smartphone with the SAMSUNG GALAXY S8 + brand with the SM-G9550 series, both users have accounts social media LINE with a different account name. User a (the perpetrator) has the account name "BLANKon" while user b (victim) has the account name "Witra". With an account that is owned, both do chat activities, namely by sending text messages and picture messages using their respective smartphones. After communicating with each other, user B is annoyed by the message sent by user A, apparently the message sent by user A during the chat activity is bullying. Then, user b reports the cyberbullying incident to the authorities. For the follow-up, the authorities seized the Samsung GALAXY GRAND PRIME smartphone with the SM-G531H series from the perpetrators for further investigation. In the investigation, the investigator uses the National Institute of Justice (NIJ) method which has five basic stages in the forensic stage, namely preparation, collection, examination, analysis, and reporting.

A. Preparation

In this preparation process, the duty is to prepare all the tools or tools that will be used during the investigation process. Tools or tools used can be seen in the table below.

Table 1. Tools and materials

No	Alat dan Bahan	Spesifikasi	Keterangan
1	Laptop	ASUS VivoBook A442U Intel Core i7, Windows 10 64-bit	Hardware
2	*Smartphone*	SAMSUNG GALAXY GRAND PRIME SM-G531H, already in the root condition	Hardware
4	MOBILedit Forensic	Program version 10.1.0.25985	Software
5	DB Browser for SQLite	Program version 3.11.2	Software

B. Collection

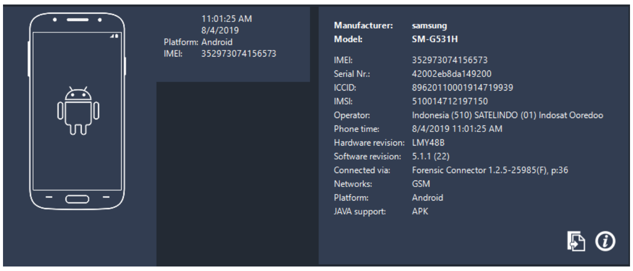
In this process, the investigator collects physical evidence along with the documentation, and also collects data on the suspect's smartphone.

Figure 3. Suspect smartphone

The picture above is the documentation of physical evidence from a communication device in the form of a smartphone that is used by the suspect to carry out acts indicating cyberbullying crime. The smartphone uses the Android Operating System version 5.1.1 or can also be called the Android Lollipop, which also has social media installed in LINE, and is in a root condition. Furthermore, the investigator will retrieve data on the smartphone by cloning, this aims to avoid data changes or data deletion which will later become digital evidence.

C. Examination

What is done in this inspection process is to take an inspection of the data on the smartphone. With the help of the MOBILedit Forensic tool that is already installed on the laptop, the investigator checks the data on the perpetrator's smartphone. If it is connected, the MOBILedit software will display information from the smartphone, as shown below.



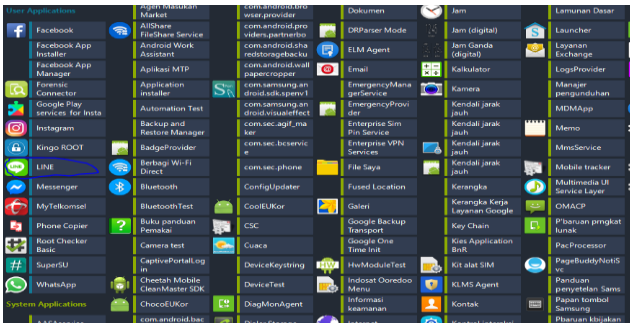
```
11:01:25 AM
8/4/2019
Platform: Android
IMEI:     352973074156573

Manufacturer:       samsung
Model:              SM-G531H

IMEI:               352973074156573
Serial Nr.:         42002eb8da149200
ICCID:              89620110001914719939
IMSI:               510014712197150
Operator:           Indonesia (510) SATELINDO (01) Indosat Ooredoo
Phone time:         8/4/2019 11:01:25 AM
Hardware revision:  LMY48B
Software revision:  5.1.1 (22)
Connected via:      Forensic Connector 1.2.5-25985(F), p:36
Networks:           GSM
Platform:           Android
JAVA support:       APK
```

Figure 4. Information from the perpetrator's smartphone

In the inspection process, various types of data are obtained from the perpetrator's smartphone, ranging from email, contacts, galleries, Bluetooth and so on. And of course LINE social media is also readable, can be seen in **Figure 5**.



User Applications
Facebook
Facebook App Installer
Facebook App Manager
Forensic Connector
Google Play services for Insta
Instagram
Kingo ROOT
LINE
Messenger
MyTelkomsel
Phone Copier
Root Checker Basic
SuperSU
WhatsApp
System Applications

Agen Masukan Market
AllShare FileShare Service
Android Work Assistant
Aplikasi MTP
Application installer
Automation Test
Backup and Restore Manager
BadgeProvider
Berbagi Wi-Fi Direct
Bluetooth
BluetoothTest
Buku panduan Pemakai
Camera test
CaptivePortalLog in
Cheetah Mobile CleanMaster SDK
ChocoEUKor
com.android.bac

com.android.bro wser.provider
com.android.pro viders.partnerbo
com.android.sha redstoragebacku
com.android.wall papercropper
com.samsung.an droid.sdk.spenv1
com.samsung.an droid.visualeffect
com.sec.agif_ma ker
com.sec.bcservic e
com.sec.phone
ConfigUpdater
CoolEUKor
CSC
Cuaca
DeviceKeystring
DeviceTest
DiagMonAgent

Dokumen
DRParser Mode
ELM Agent
Email
EmergencyMana gerService
EmergencyProvi der
Enterprise Sim Pin Service
Enterprise VPN Services
File Saya
Fused Location
Galeri
Google Backup Transport
Google One Time Init
HwModuleTest
Indosat Ooredoo Menu
Informasi keamanan

Jam
Jam (digital)
Jam Ganda (digital)
Kalkulator
Kamera
Kendali jarak jauh
Kendali jarak jauh
Kendali jarak jauh
Kendali jarak jauh
Kerangka
Kerangka Kerja Layanan Google
Key Chain
Kies Application BnR
Kit alat SIM
KLMS Agent
Kontak

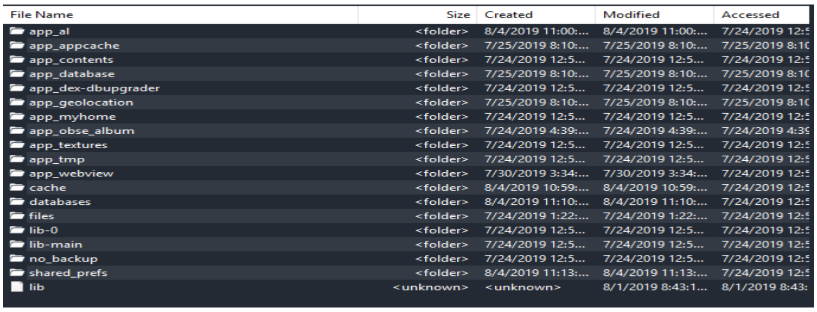
Lamunan Dasar
Launcher
Layanan Exchange
LogsProvider
Manajer pengunduhan
MDMApp
Memo
MmsService
Mobile tracker
Multimedia UI Service Layer
OMACP
P'baruan prngkat lunak
PacProcessor
PageBuddyNotiS vc
Panduan penyetelan Sams
Papan tombol Samsung
Pbaruan kbijakan

Figure 5. The results of retrieving data on the suspect's smartphone using MOBILedit Forensic

Because the perpetrator is using LINE social media, then further checks are carried out on the file from the LINE social media which is in the form of a folder with the name "jp.naver.line.android", the folder is located in the folder location with the following directory:

data→data→*jp.naver.line.android*

When viewed from the MOBILedit software, this is what the folder structure looks like for each folder from the LINE application (jp.naver.line.android).



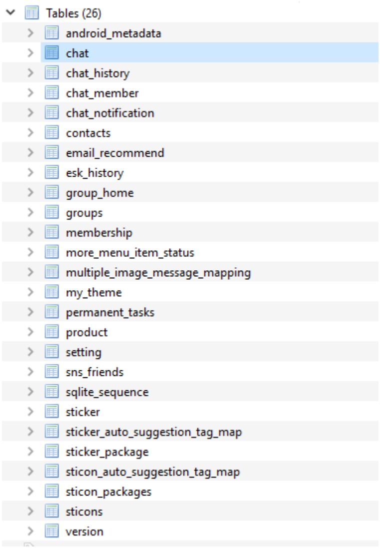
File Name	Size	Created	Modified	Accessed
app_al	<folder>	8/4/2019 11:00:...	8/4/2019 11:00:...	7/24/2019 12:5
app_appcache	<folder>	7/25/2019 8:10:...	7/25/2019 8:10:...	7/25/2019 8:10
app_contents	<folder>	7/24/2019 12:5...	7/24/2019 12:5...	7/24/2019 12:5
app_database	<folder>	7/25/2019 8:10:...	7/25/2019 8:10:...	7/25/2019 8:10
app_dex-dbupgrader	<folder>	7/24/2019 12:5...	7/24/2019 12:5...	7/24/2019 12:5
app_geolocation	<folder>	7/25/2019 8:10:...	7/25/2019 8:10:...	7/25/2019 8:10
app_myhome	<folder>	7/24/2019 12:5...	7/24/2019 12:5...	7/24/2019 12:5
app_obse_album	<folder>	7/24/2019 4:39:...	7/24/2019 4:39:...	7/24/2019 4:39
app_textures	<folder>	7/24/2019 12:5...	7/24/2019 12:5...	7/24/2019 12:5
app_tmp	<folder>	7/24/2019 12:5...	7/24/2019 12:5...	7/24/2019 12:5
app_webview	<folder>	7/30/2019 3:34:...	7/30/2019 3:34:...	7/24/2019 12:5
cache	<folder>	8/4/2019 10:59:...	8/4/2019 10:59:...	7/24/2019 12:5
databases	<folder>	8/4/2019 11:10:...	8/4/2019 11:10:...	7/24/2019 12:5
files	<folder>	7/24/2019 1:22:...	7/24/2019 1:22:...	7/24/2019 12:5
lib-0	<folder>	7/24/2019 12:5...	7/24/2019 12:5...	7/24/2019 12:5
lib-main	<folder>	7/24/2019 12:5...	7/24/2019 12:5...	7/24/2019 12:5
no_backup	<folder>	7/24/2019 12:5...	7/24/2019 12:5...	7/24/2019 12:5
shared_prefs	<folder>	8/4/2019 11:13:...	8/4/2019 11:13:...	7/24/2019 12:5
lib	<unknown>	<unknown>	8/1/2019 8:43:1...	8/1/2019 8:43:

Figure 6. LINE folder structure (jp.naver.line.android)

In the picture above, the LINE folder (jp.naver.line.android) consists of 18 sub-folders and 1 file named lib, the number of these folders also depends on the condition of the device and application usage. Then the folder in the LINE folder (jp.naver.line.android) is analyzed. From the results of the analysis, found several files in the form of a database with SQLite format. To find out the contents of the file, it must be opened with the help of DB Browser for SQLite software for further analysis.

D. Analysis

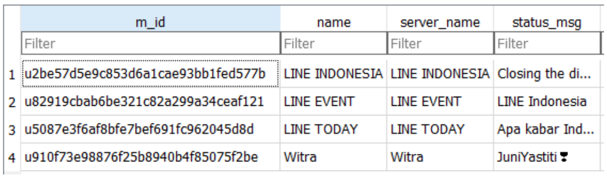
Based on an analysis of the contents of the sub-folder as well as the database from the LINE folder (jp.naver.line.android), it is found important data that can be used to support the investigation, namely a database called "naver_line". From the results of the investigation using DB Browser for SQLite software, the naver_line database has 26 tables, and can be seen in **Figure 7**.



Tables (26)
- android_metadata
- chat
- chat_history
- chat_member
- chat_notification
- contacts
- email_recommend
- esk_history
- group_home
- groups
- membership
- more_menu_item_status
- multiple_image_message_mapping
- my_theme
- permanent_tasks
- product
- setting
- sns_friends
- sqlite_sequence
- sticker
- sticker_auto_suggestion_tag_map
- sticker_package
- sticon_auto_suggestion_tag_map
- sticon_packages
- sticons
- version

Figure 7. Table structure in the naver_line database

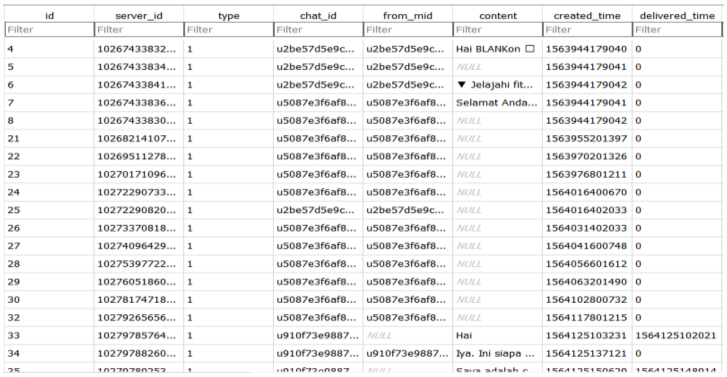
First, the investigator wants to find out who the contacts are stored on the perpetrator's account. So in the DB Browser for SQLite software the investigator opens the contacts table, and the following results are obtained.



	m_id	name	server_name	status_msg
	Filter	Filter	Filter	Filter
1	u2be57d5e9c853d6a1cae93bb1fed577b	LINE INDONESIA	LINE INDONESIA	Closing the di...
2	u82919cbab6be321c82a299a34ceaf121	LINE EVENT	LINE EVENT	LINE Indonesia
3	u5087e3f6af8bfe7bef691fc962045d8d	LINE TODAY	LINE TODAY	Apa kabar Ind...
4	u910f73e98876f25b8940b4f85075f2be	Witra	Witra	JuniYastiti ❣

Figure 8. The contents of the contacts table

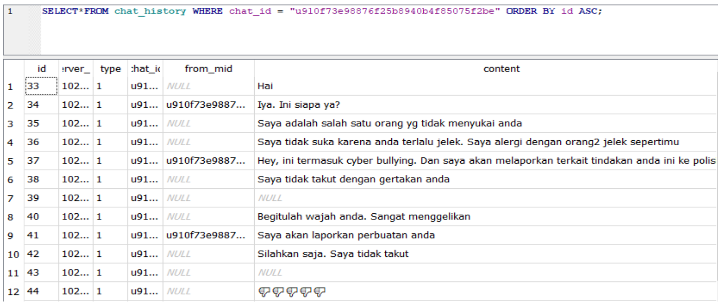
From **Figure 8**, information was obtained that the perpetrator only had 4 contacts, namely LINE INDONESIA, LINE EVENT, LINE TODAY, and Witra, and each contact had a different id. From the beginning it was discovered that the victim had the account name "Witra". In **Figure 8** it is also known that the account with the name "Witra" has the id u910f73e98876f25b8940b4f85075f2be. Then the investigator further investigates by opening the chat_history table to find out the trace of the conversation or chat perpetrator.



id	server_id	type	chat_id	from_mid	content	created_time	delivered_time
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
4	10267433832...	1	u2be57d5e9c...	u2be57d5e9c...	Hai BLANKon □	1563944179040	0
5	10267433834...	1	u2be57d5e9c...	u2be57d5e9c...	NULL	1563944179041	0
6	10267433841...	1	u2be57d5e9c...	u2be57d5e9c...	▼ Jelajahi fit...	1563944179042	0
7	10267433836...	1	u5087e3f6af8...	u5087e3f6af8...	Selamat Anda...	1563944179041	0
8	10267433830...	1	u5087e3f6af8...	u5087e3f6af8...	NULL	1563944179042	0
21	10268214107...	1	u5087e3f6af8...	u5087e3f6af8...	NULL	1563955201397	0
22	10269511278...	1	u5087e3f6af8...	u5087e3f6af8...	NULL	1563970201326	0
23	10270171096...	1	u5087e3f6af8...	u5087e3f6af8...	NULL	1563976801211	0
24	10272290733...	1	u5087e3f6af8...	u5087e3f6af8...	NULL	1564016400670	0
25	10272290820...	1	u2be57d5e9c...	u2be57d5e9c...	NULL	1564016402033	0
26	10273370818...	1	u5087e3f6af8...	u5087e3f6af8...	NULL	1564031402033	0
27	10274096429...	1	u5087e3f6af8...	u5087e3f6af8...	NULL	1564041600748	0
28	10275397722...	1	u5087e3f6af8...	u5087e3f6af8...	NULL	1564056601612	0
29	10276051860...	1	u5087e3f6af8...	u5087e3f6af8...	NULL	1564063201490	0
30	10278174718...	1	u5087e3f6af8...	u5087e3f6af8...	NULL	1564102800732	0
32	10279265656...	1	u5087e3f6af8...	u5087e3f6af8...	NULL	1564117801215	0
33	10279785764...	1	u910f73e9887...	NULL	Hai	1564125103231	1564125102021
34	10279788260...	1	u910f73e9887...	u910f73e9887...	Iya. Ini siapa ...	1564125137121	0
35	10279789253	1	u910f73e9887	NULL	Saya adalah s	1564125150620	1564125148014

Figure 9. The contents of the chat_history table

The picture above is the contents of the chat_history table. Traces of conversation or chat between the perpetrators and other accounts are obtained. But what is most needed is a trace of conversation between the perpetrator and the victim under the name "Witra" account. For this reason, a filter is needed by adding the query code to the available text editor, the results can be seen in **Figure 10**.



```
1    SELECT*FROM chat_history WHERE chat_id = "u910f73e98876f25b8940b4f85075f2be" ORDER BY id ASC;
```

	id	:rver_	type	:hat_i(	from_mid	content
1	33	102...	1	u91...	NULL	Hai
2	34	102...	1	u91...	u910f73e9887...	Iya. Ini siapa ya?
3	35	102...	1	u91...	NULL	Saya adalah salah satu orang yg tidak menyukai anda
4	36	102...	1	u91...	NULL	Saya tidak suka karena anda terlalu jelek. Saya alergi dengan orang2 jelek sepertimu
5	37	102...	1	u91...	u910f73e9887...	Hey, ini termasuk cyber bullying. Dan saya akan melaporkan terkait tindakan anda ini ke polis
6	38	102...	1	u91...	NULL	Saya tidak takut dengan gertakan anda
7	39	102...	1	u91...	NULL	NULL
8	40	102...	1	u91...	NULL	Begitulah wajah anda. Sangat menggelikan
9	41	102...	1	u91...	u910f73e9887...	Saya akan laporkan perbuatan anda
10	42	102...	1	u91...	NULL	Silahkan saja. Saya tidak takut
11	43	102...	1	u91...	NULL	NULL
12	44	102...	1	u91...	NULL	👎👎👎👎👎

Figure 10. The contents of the chat_history table after filtering it

In the picture above, there is a conversation between the perpetrator who has the id "NULL" with the victim who has the id u910f73e9887 ... It can be seen that the perpetrator threw an unpleasant message to the victim and this indicated cyberbulling activities. However, there are some messages that cannot be obtained by DB Browser for SQLite software. This can be seen in the content column which only displays NULL. Furthermore, the results of the analysis can be used as digital evidence for cases that indicate cyberbullying crime by utilizing social media LINE as a container.

E. Reporting

The method used in this investigation is the National Institute of Justice (NIJ) method which has 5 basic stages in the forensic process, namely preparation, collection, examination, analysis, and reporting. The first thing the investigator did was to prepare the tools or tools used during the investigation, namely: Laptops, smartphones, MOBILedit Forensic software, and DB Browser for SQLite software. Next to the collection stage, at this stage the investigator carries out the collection of physical evidence that is the suspect's smartphone and the data on the suspect's smartphone is cloned so that data integrity is maintained, as well as carrying out documentation on the collection of data. The third stage is the examination, the investigator conducts an examination of the data that is on the perpetrator's smartphone and will further conduct a deeper analysis. In this investigation, the investigator uses two different softwares, namely MOBILedit Forensic and DB Browser for SQLite. MOBILedit Forensic is used when extracting and acquiring data on the perpetrator's smartphone, besides this software is also used to analyze the structure of folders and files in the LINE folder (jp.naver.line.android). From the analysis results obtained LINE folder (jp.naver.line.android) has 18 sub-folders and 1 file named lib. After a deeper analysis found important data that can support the investigation, namely naver_line, which is data in the form of a database with the SQLite format. To open the database file, the DB Browser for SQLite software is used. From the results of the investigation using DB Browser for SQLite software, the naver_line database has 26 tables. First the investigator checks the contacts table to ascertain the id of the victim, after finding the investigator checks the chat_histoy table in order to check the trace of the suspect's conversation with the victim. From the chat examination, digital evidence was obtained that the perpetrators did indicate the crime of cyberbullying, and later the digital evidence could be presented at the trial.

4. Conclusion

The aim of this research is to help solve the cyberbullying problem on LINE social media in mobile forensics by using the National Institute of Justice (NIJ) method and the help of MOBILedit Forensic software and DB Browser for SQLite. The National Institute of Justice (NIJ) method itself, has 5 basic stages in the forensic process, namely preparation, collection, examination, analysis, and reporting. The collection and checking process in this study uses the help of MOBILedit Forensic software, while the analysis process uses the help of the DB Browser for SQLite software. From the inspection process, important data obtained that can support the investigation, namely naver_line. Then the data is further analyzed. From the results of the analysis we found traces of chat between the perpetrators and victims, but there were also messages that could not be read. From the chat trail, it was seen that the perpetrator sent an unpleasant message to the victim and this indicated cyberbulling activities. Furthermore, the results of the analysis can be used as digital evidence for cases that indicate cyberbullying crimes.

References

[1] S. Kemp, "Global social media users pass 3.5 billion - We Are Social", *We Are Social*, 2019. [Online]. Available: https://wearesocial.com/blog/2019/07/global-social-media-users-pass-3-5-billion. [Accessed: 20- Jul- 2019].

[2] L. Corporation, "LINE Corporation | Home", *LINE Corporation*, 2016. [Online]. Available: http://linecorp.com/. [Accessed: 20- Jul- 2019].

[3] Ilman, Z. Y., MM, M., & Yesi, N. K. (2014). ANALISIS FORENSIK PADA PLATFORM ANDROID.

[4]"DB Browser for SQLite", *Sqlitebrowser.org*, 2019. [Online]. Available: https://sqlitebrowser.org/. [Accessed: 21- Jul- 2019].

[5] Riadi, I., Yudhana, A., Caesar, M., & Putra, F. (2018). Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ). *Jurnal Teknik Informatika dan Sistem Informasi p-ISSN*, *2443*, 2210.

[6] Ikhsani, S., & Hidayanto, B. C. (2016). Analisa Forensik Whatsapp dan LINE Messenger Pada Smartphone Android Sebagai Rujukan Dalam Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia. *Jurnal Teknik ITS*, *5*(2), A728-A736.

[7] Yudhana, A., Umar, R., & Ahmadi, A. Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ). *vol. X, no. X*, 8-13.

[8] Faiz, M. N., Umar, R., & Yudhana, A. (2016). Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary. *ILKOM Jurnal Ilmiah*, *8*(3), 242-247.

[9] 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)*, *3*(1), 70-82.