

Mobile Forensic on WhatsApp Services using National Institute of Standards and Technology Method

Rizal Adjisman
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT

WhatsApp is a free chat application that allows users to exchange text messages, photos, videos, documents and can share the latest location available on Android and iOS versions built by Brian Acton and Jan Koum. One of the shortcomings of WhatsApp is that it can be used as a medium for committing crimes, such as hate speech. This study uses the National Institute of Standards and Technology (NIST) method, with the stages of collection, examination, analysis, and reporting with several applications that serve as tools to find digital evidence such as MOBILedit Forensic, WhatsApp Viewer, and DB Browser For SQLite. This study uses two smartphones that are evident with different conditions, namely a smartphone that has been in a root condition and a smartphone that is not in a root condition. Test results or looking for evidence using MOBILedit Forensic, WhatsApp Viewer, and DB Browser for SQLite on a smartphone in a root condition managed to find the data you were looking for. The data is in the form of conversational texts containing hate speech content. While the process of searching for evidence using MOBILedit Forensic on smartphones that are not in a data root condition, only images, videos, and audio were found, meaning that they did not find hate speech content in the form of conversational texts. Meanwhile, the process of searching for digital evidence using WhatsApp Viewer and DB Browser for SQLite on a smartphone that is not rooted does not find any data.

Keywords

Digital Forensics, Mobile, Hate Speech, WhatsApp, NIST

1. INTRODUCTION

The development of information and communication technology in the world is growing rapidly and social media users are now increasingly familiar among the public. Now smartphones have developed with features that are adapted to the development of time and the needs of their users[1]. Users who actively use social media in Indonesia are 160 million or 59%, and an average Indonesian spends 3 hours 26 minutes accessing social media a day[2]. Social media is a medium that is used to interact online in unlimited space and time. One of the bad effects of social media is that there are criminal acts. Social media that is very popular today is instant messenger. The popularity of IM applications has led to the emergence of various applications in the instant messaging category that offer different features and qualities[3]. Some instant messenger applications that are widely used include WhatsApp, WeChat, Line, Telegram, FB Messenger, Skype and so on.

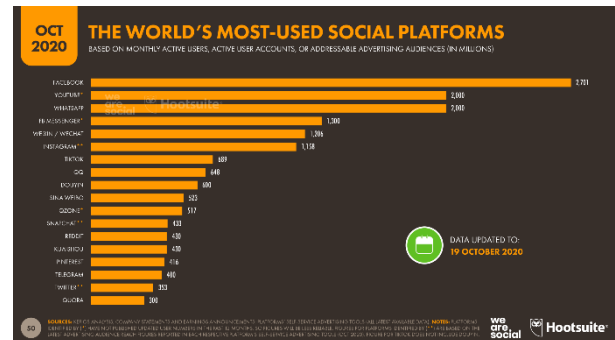


Figure 1. The most popular social media in the world

Figure 1 explains that WhatsApp has 2 billion monthly active users, this makes WhatsApp in the third position as the favorite social media, while the first position is Facebook with 2.701 billion monthly active users[4]. By having many users, WhatsApp can be used as a medium for committing crimes, such as hate speech[5].

In general, hate speech contains matters relating to the point of view of skin color, ethnicity, disability, race, sexual orientation, religion, gender, citizenship, and others[6]. From March to April 2020, Polda Metro Jaya received at least 443 reports related to hate speech[7]. Whatsapp Group is used as a means of communication and exchanging information. Sharing is caring (sharing is a form of attention) becomes a strong influence for users in disseminating information on Whatsapp Group. The main reason for disseminating information depends on the usefulness of the information and the perception of interest, then at any time without realizing it, users spread hoaxes and hate speech[8].

1.1. Study Literature

1.1.1. Previous Study

The first previous study refers to research conducted by Anton Yudhana, Rusydi Umar, and Ahwan Ahmadi (2018) with the title "Google Drive Forensic Data Acquisition on Android Using the National Institute of Justice (NIJ) Method". This research uses Oxygen Forensic and MOBILedit Forensic as software to get the data you want to find. The results obtained using Oxygen Forensic are accounts, file extensions, images, and zip folders. Meanwhile, the results of the analysis using MOBILedit Forensic did not find file extensions, images, zip folders, but only read accounts [1].

The second study was conducted by Anton Yudhana, Imam Riadi, and Ikhwan Anshori (2018) entitled "Analysis of Digital Evidence for Facebook Messenger Using the NIST Method". In this study, the tools used were Oxygen Forensic.

Then, the results obtained in this study were finding text messages, images, audio messages, when the conversation was sent, then from the research that was not found, namely data in the form of video[9].

Previous studies were then carried out by RauhullohAyatulloh Khomeini Noor Bintang, Rusydi Umar, and Anton Yudhana (2020). This research is entitled "Facebook Lite Social Media Analysis with Forensic tools using the NIST Method". This study aims to find digital evidence related to criminal cases such as online buying and selling fraud, drug trafficking, cyberbullying, buying and selling prostitutes online, and other cases that occurred on Facebook Lite. In this study, 5 parameters are sought, namely account id, video, audio, image, and URL. Of the 5 parameters searched, only 4 parameters can be found using MOBILedit Forensic namely account id, video, audio, and image. As for the URL is not found[10].

The fourth previous study refers to research conducted by Imam Riadi, Anton Yudhana, and Muhamad Caesar Febriansyah Putra (2018). This research is entitled "Acquisition of Digital Evidence on Android-Based Instagram Messenger Using the National Institute Of Justice (NIJ) Method". This study aims to assist the process of mobile forensics to overcome cases of cyberbullying crimes that arise on Instagram social media using a smartphone. The results obtained from this study are digital evidence that has been found on Instagram which is installed on a smartphone when the root condition is found, the expected data is in the form of pictures/photos and conversations/chats, while for smartphones that are not in root condition, no digital evidence is obtained[11].

Based on the fifth study conducted by Wisnu Ari Mukti, SitiUmmiMasrurroh, and DewiKhairani (2018) entitled "Analysis and Comparison of Forensic Evidence for Facebook and Twitter Social Media Applications on Android Smartphones". The method used is the simulation method. The results obtained from this research are on the Facebook social media application, the digital evidence that has been obtained are account names, cover photos, private messages in the form of images, profile photos, date of birth, postings in the form of images, phone numbers, location data, posts in the form of text, and private messages in the form of text. While on the Twitter social media application, digital evidence that cannot be found is in the form of direct messages in the form of pictures, date of birth, direct messages in the form of text, and telephone numbers[12].

1.1.2. Digital Forensics

Digital forensics is the analysis of data, such as audio, video, and others obtained after examining electronic devices to assist legal processes[13]. Digital forensics has several aspects, including Mobile Forensics. Digital forensics can get digital evidence that can be stored on permanent computer storage, temporary storage, network traffic, CD, USB, and others[11].

1.1.3. Mobile Forensics

Mobile Forensics is a science that carries out the process of returning digital evidence using techniques suitable for forensic conditions from mobile devices [11]. Digital evidence on mobile devices is easily overwritten by new data or even deleted[14]. Mobile forensics is a component or part of digital forensics, mobile forensics has the goal of carrying out digital data recovery on mobile devices[15].

1.1.4. WhatsApp

Instant messaging (IM) is one of the most popular mobile applications. WhatsApp is one example of IM[16]. WhatsApp is a free chat application that allows users to exchange text messages, photos, videos, documents and can share the latest location available on Android and iOS versions built by Brian Acton and Jan Koum. WhatsApp itself stores all its conversations in a database on every WhatsApp user's device[17].

1.1.5. Hate Speech

Hate speech is an act of communication carried out by individuals or groups in the form of provocation, incitement, or insult to other individuals or groups. In general, hate speech contains matters relating to aspects of race, skin color, ethnicity, gender, disability, sexual orientation, citizenship, religion, and others[6].

2. METHODOLOGY

2.1. Research Scenario

A scenario is designed to obtain digital evidence[18]. The purpose of this scenario is to facilitate the investigation process in cases of hate speech. The simulation is carried out using both smartphones that have the WhatsApp application installed. On WhatsApp there is a group consisting of several people, the group is used to communicate and exchange information as it should. Then in the group, there is one member (suspect) sending a message or information in the form of hate speech. Then to leave a digital footprint, the suspect who sent the message deleted the chat or message in the form of hate speech. Other members of the group reported the incident to the police. From the scenario that has been described, it can be seen in Figure 2.

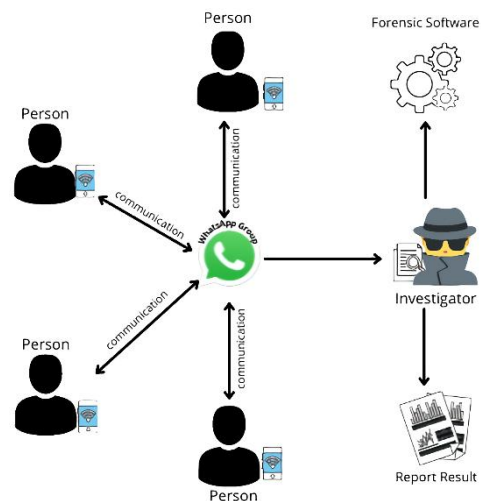


Figure 2. Hate speech case scenario

Figure 2. shows the case of hate speech occurring in the WhatsApp application. The analysis process will use two smartphones with the Mi 4W brand in root condition and Realme 5 Pro, not in root condition. Conversations in the WhatsApp Group will be examined by investigators from the suspect's device and the device of one of the other group members using the MOBILedit Forensic tools, WhatsApp Viewer, and DB Browser for SQLite. After carrying out the examination process using forensic tools, the investigator then made a report from the results of the examination in the case of hate speech that occurred on the WhatsApp application.

2.2. Investigation Flowchart

This stage or process explains the flow of how investigators obtain evidence [19]. The evidence obtained by the investigator comes from the authorities, namely the police who have secured the evidence first.

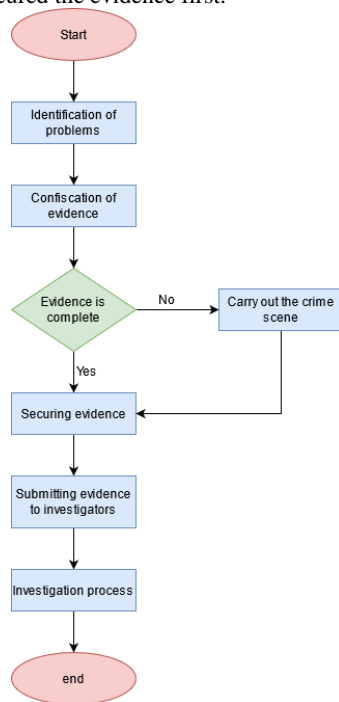


Figure 3. Stages of obtaining evidence

The following is an explanation of the investigation flow to uncover evidence, as shown in Figure 3.

1. Identification of the problem, this is done by the authorities to know in detail the problems that occur to the victims and perpetrators.
2. The confiscation of this evidence is carried out by the police, this is done to secure the evidence and keep it intact in its original state.
3. After the confiscation, the next process is to complete the evidence. What is meant by complete here, is in the confiscation process whether all the evidence has been collected when processing the crime scene.
4. Securing this evidence is carried out by the authorities, namely the police, this is done to maintain the authenticity of the evidence.
5. Further investigations were handed over to the investigators to examine the smartphones that had become evident.
6. The investigation process, is carried out when the authorized party submits evidence to the investigator for investigation to obtain evidence in the case of hate speech crimes.

2.3. Research Plan Scenario

Figure 4. is a communication process carried out by four members in a group. One member sent a message in the form of hate speech. Then the investigator conducts an investigation of the evidence and data collected. In the process of collecting evidence, investigators need several applications such as MOBILEdit Forensic, WhatsApp Viewer, and DB Browser for SQLite.

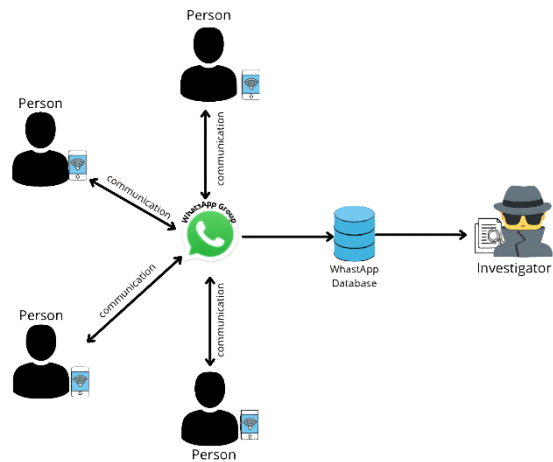


Figure 4. Evidence search scenario

Communication is carried out using a smartphone, the two smartphones will later be secured as evidence to raise hate speech crimes. Investigators conducted an examination of the secured smartphone.

2.4. Research Stages

The stages of the research were carried out to obtain digital evidence of hate speech cases that occurred on WhatsApp Messenger using the National Institute of Standards and Technology (NIST) method [20]. NIST stages consist of Collection, Examination, Analysis, Report can be seen in Figure 5.







Figure 5. Stages of the NIST method

2.4.1. Collection

This step is the first step of the NIST method which searches and collects data. At this stage, there is a process of returning data from relevant data sources and maintaining the integrity of the evidence from changes [21]. In the case scenario it is explained that the smartphone is a tool used to communicate, the smartphone becomes evidence of a crime. The two smartphones that have become evidence have the WhatsApp application installed. The evidence that has been collected can be seen in Table 1.

Table 1. Evidence

No.	Name of evidence	Image	Description
1.	Smartphone 1		Xiaomi brand, already in root condition

2.	Smartphone data cable1		Micro-USB is used to connect a smartphone to a laptop
3	Smartphone 2		Realme brand, notrooted
4	Smartphone data cable2		USB Type-C is used to connect a smartphone to a laptop

The evidence obtained is 1 cellphone with the Xiaomi brand, 1 cellphone with the Realme 5 Pro brand. In addition, other evidence was found, namely 1 data cable used to charge Xiaomi brand cellphones and 1 data cable used to charge Realme 5 Pro brand cellphones.

2.4.2. Examination

This stage is the stage of examining electronic evidence/digital evidence[22].The results of the extraction that have been carried out using MOBILedit Forensic will appear in the form of a full report [23].In this research, the selected full report is in PDF format. The full report results from the Xiaomi brand smartphone can be seen in Figure 6.

Device Properties	
Manufacturer	Xiaomi
Product	MI 4W
HW Revision	MMB29M
Platform	Android
SW Revision	6.0.1 (23)
Android ID	6cfddec3aea9ea75
Serial Number	9c9dd2a2
Device Time	2021-06-09 15:01:42 (UTC+7)
Manual Time	No
Time Zone	Asia/Jakarta
Manual Time Zone	No
Device Storage Encrypted	No
IMEI	867079023087832
Rooted	Yes
SIM Card	Yes
IMSI	510103362618163
SIM Card Country	Indonesia
ICCID	8962100533626181632f
Total Storage	12.5 GB
Used Storage	10.9 GB

Figure 6. Smartphone xiaomi full report

The examination process on Realme brand smartphones is done by connecting the smartphone to a laptop using a data

cable. The full report results from the Realme brand smartphone can be seen in Figure 7.

Device Properties	
Manufacturer	realme
Product	RMX1971
HW Revision	QKQ1.190918.001
Platform	Android
SW Revision	10 (29)
Serial Number	unknown
Device Time	2021-04-27 14:49:54 (UTC+7)
Manual Time	No
Time Zone	Asia/Jakarta
Manual Time Zone	No
Device Storage Encrypted	Yes
Rooted	No
SIM Card	No
SIM Card Country	Indonesia
Operator	XL Axiata, MCC: 510, MNC: 11
Total Storage	109.1 GB
Used Storage	81.7 GB
Total SD Card Storage	108.9 GB
Used SD Card Storage	81.7 GB

Figure 7. Smartphone realme full report

2.4.3. Analysis

The analysis stage is analyzing and looking for evidence in processing the data that has been obtained[24].The purpose of the analysis stage is to find and raise evidence of hate speech committed by the perpetrator from the evidence that has gone through the examination process.

- a. Evidence Search using MOBILedit Forensic on Xiaomi Smartphones

The results of the WhatsApp application analysis found the account used by the perpetrator, the report file shows the WhatsApp Id or phone number used is 62818027116xx as shown in Figure 8.

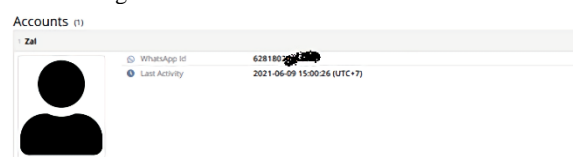


Figure 8. WhatsApp account information

In addition, investigators managed to find evidence of conversation data containing hate speech that had been deleted by the perpetrator on the Xiaomi smartphone. The perpetrator sent the thing at 2:59 pm on the date 2021-06-09. The picture of proof of the conversation that has been deleted can be seen in Figure 9.



Figure 9. Text messages containing hate speech

In the results of the Report file, the author also found 71 contacts on the perpetrator's smartphone. In the contact, data found information containing the name of the contact, phone

number, and also the status. The contact information that was not deleted can be seen in Figure 10.



Figure 10. Contact list

During the inspection and analysis process, it was also found that text messages were not deleted. Text messages that are not deleted can be seen in Figure 11.

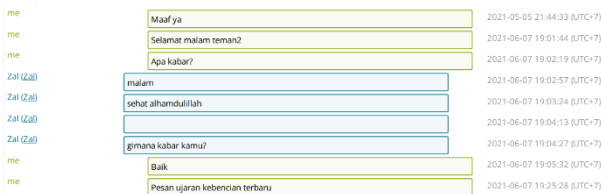


Figure 11. Group conversation content

Of the 73 contacts on the Xiaomi brand smartphone that have become evident, 2 contacts have been deleted. The deleted WhatsApp contacts can be seen in Figure 12.

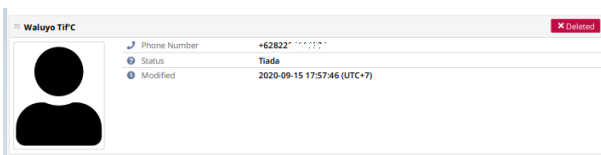


Figure 12. Deleted contact list

The results of the analysis also found media files in the form of images, videos, and audio from Xiaomi smartphones. From the media files found 1273 images, 2644 audio, and 38 videos as shown in Figure 13.



Figure 13. Media files stored on xiaomi smartphones

b. Evidence Search using WhatsApp Viewer on Xiaomi Smartphones

Searching for evidence using WhatsApp Viewer requires an additional application, namely Explorer Ice. The application is used to search for WhatsApp messages that have been decrypted. Using Ice Explorer, the decryption is found in the data/data/com.WhatsApp/databases folder. If you have received a decryption message, the process of copying the data from the smartphone to the laptop is carried out to find evidence of cases of hate speech. The process of copying the data requires a data cable to connect the smartphone to the laptop. After the data copying process is successful, it is then checked using WhatsApp Viewer as shown in Figure 14.

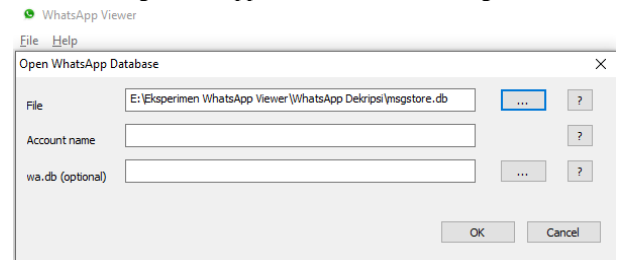


Figure 14. Open WhatsApp database using WhatsApp Viewer

The results of checking using WhatsApp Viewer found messages containing hate speech content. The content of the message is "This is a message of hate speech at 14:59 that was deleted", this can be evidence that the perpetrator committed an act of hate speech. The text message was sent at 2:59 p.m. as shown in Figure 15.

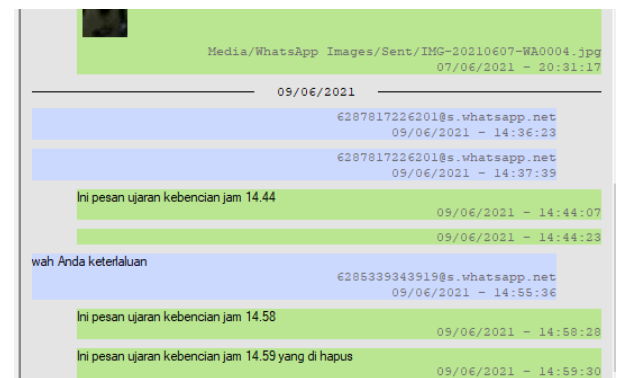


Figure 15. Fill in the conversation in the WhatsApp Group

c. Evidence Search using DB Browser for SQLite on Xiaomi Smartphones

Similar to using WhatsApp Viewer, to find evidence using DB Browser for SQLite requires WhatsApp decryption. The text messages found can be seen in Figure 16.

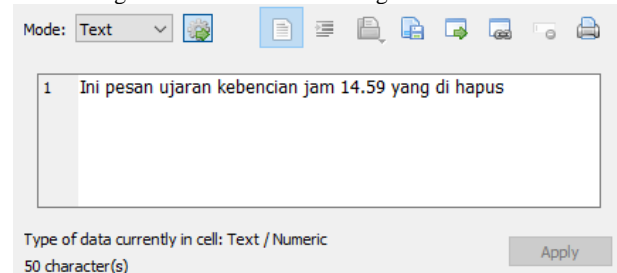


Figure 16. Evidence that the perpetrator sent hate speech

The results of checking using the SQLite DB Browser found messages containing hate speech content. This can be evidence that the perpetrator committed hate speech.

d. Evidence Search using MOBILedit Forensic on Realme Smartphones

The results of the analysis of the Realme smartphone found media files in the form of images, videos, and audio. The media file found 660 images, 1216 audio, and 80 videos according to Figure 17.



Figure 17. Media files stored on realme smartphones

e. Evidence Search using WhatsApp Viewer on Realme Smartphones

Did not find evidence in the form of text messages on Realme smartphones. This happens because the smartphone is not rooted, so the decryption search process on the WhatsApp database cannot be carried out. Investigators only found the crypt14 file from the realme smartphone as shown in Figure 18, but no further investigation process could be carried out because there was no support file, namely the key from the database.

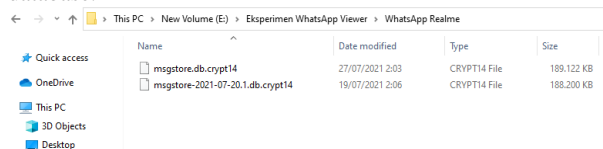


Figure 18. Realme smartphone msgstore

f. Evidence Search using DB Browser for SQLite on Realme Smartphones

The same thing happened with WhatsApp Viewer, looking for evidence in the form of text conversations using the SQLite DB Browser cannot be done because the smartphone used is not rooted.

2.4.4. Reporting

The reporting stage is reporting the results of the analysis which includes a description of the actions taken[25]. The purpose of the reporting stage is to make a report in the form of any data found in the analysis stage. Table 2 is information on 2 android smartphones or evidence used.

Table 2. Checked device information

Description	Smartphone 1	Smartphone 2
Device name	Mi Phone	Realme 5 Pro
Operating System	Android	Android
Model	Mi 4 W	RMX 1971
RAM	3,00 GB	4,00 GB
Android version	6.0.1 MMB29M	10

Based on table 2, the two smartphones were used to look for evidence of crimes, namely, hate speech cases. In addition to hardware, there is software used to uncover cases of hate speech that occurred in the WhatsApp application. MOBILedit Forensic, WhatsApp Viewer, DB Browser SQLite is a software that is a forensic tool used. The comparison of the results after carrying out the process of searching for evidence using MOBILedit Forensic, WhatsApp Viewer, and DB Browser for SQLite can be seen in Table 3.

Table 3. Digital evidence found

Tools	Information found	Mi Phone	Realme 5 Pro
MOBILEdit Forensic	Message	68	0
	Retract message	1	0
	Image	1273	660
	Audio	2644	1216
	Video	38	80
	Phone contact	52	0
WhatsApp Viewer	Call history	5	0
	Message	68	0
	Retract message	1	0
	Image	7	0
	Audio	0	0
	Video	1	0
DB Browser for SQLite	Phone contact	0	0
	Call history	0	0
	Message	35	0
	Retract message	1	0
	Image	0	0
	Audio	0	0
DB Browser for SQLite	Video	0	0
	Phone contact	0	0
DB Browser for SQLite	Call history	0	0

Based on the digital evidence found, using the MOBILedit Forensic tool as a tool on a rooted smartphone managed to find the contents of the deleted conversation and found other data that was not related to the case of hate speech that

occurred on WhatsApp such as images, audio videos, phone contacts, and also calls. Meanwhile, using the MOBILedit Forensic tool as a tool on an unrooted smartphone only finds images, audio, video, and does not find messages, phone contacts, calls. Search results using WhatsApp Viewer on a rooted smartphone managed to find images, videos, and conversation content, whether deleted or not. Meanwhile, the search for digital evidence of hate speech cases on smartphones that are not rooted using WhatsApp Viewer did not find any data. The results obtained using the SQLite DB Browser are slightly different from the MOBILedit Forensic and WhatsApp Viewer applications. For smartphones that are in root condition, evidence of messages containing hate speech sent by the perpetrators was found but did not find images, audio, videos, and others. Smartphones that are not rooted don't find the evidence they want.

3. CONCLUSION

Obtaining digital evidence for hate speech cases on WhatsApp using the National Institute of Standards and Technology (NIST) method is carried out in four stages, namely collection, examination, analysis, and reporting. Test results or looking for evidence using MOBILedit Forensic, WhatsApp Viewer, and DB Browser for SQLite on a smartphone in a root condition managed to find the data you were looking for. The data is in the form of conversational texts containing hate speech content. However, other data have been found, namely audio, video, images, and phone contacts. However, these data are not related to the case. The case occurred in the WhatsApp Messenger application. While the process of searching for evidence using MOBILedit Forensic on smartphones that are not in a data root condition, only images, videos, and audio were found, meaning that they did not find hate speech content in the form of conversational texts. Meanwhile, the process of searching for digital evidence using WhatsApp Viewer and DB Browser for SQLite on a smartphone that is not rooted does not find any data. This research is expected to be a reference for future researchers. It is recommended to use other forensic applications, both paid and unpaid, as well as using a different model or type of cellphone, and can use other forensic methods.

4. REFERENCES

- [1] A.- Ahmadi, "Google Drive Forensic Data Acquisition on Android Using the National Institute of Justice (NIJ) Method," *J. CoreIT J. Has. Researcher. Computer Science. dan Technol. Inf.*, vol. 4, no. 1, p. 8, 2018, doi: 10.24014/coreit.v4i1.5803.
- [2] We Are Social & Hootsuite, "Indonesia Digital report 2020," *Glob. Digit. Insights*, p. 247, 2020, [Online]. Available: <https://datareportal.com/reports/digital-2020-global-digital-overview>.
- [3] M. S. Asyaky, "Analysis and Comparison of Digital Evidence of Instant Messenger Applications on Android," *J. Researcher. Tech. Inform.*, vol. Vol. 3 No. no. 1, pp. 220–231, 2019.
- [4] Hootsuite & We Are Social, "Social Media Users Pass 4 Billion: Digital 2020 October Statshot Report," *www.hootsuite.com*, 2020. <https://blog.hootsuite.com/social-media-users-pass-4-billion/> (accessed Dec. 02, 2020).
- [5] I. Riadi, S. Sunardi, and M. E. Rauli, "Identification of WhatsApp Digital Evidence on Proprietary Operating System Using Live Forensics," *J. Tech. Electrical*, vol. 10, no. 1, pp. 18–22, 2018, doi: 10.15294/jte.v10i1.14070.
- [6] A. Sutantohafi, "Packaged," *Danger News. Hoax and Hate Speech on Social Media. Against Tolerance. Society*, vol. 1, no. 1, pp. 1–5, 2017, [Online]. Available: <http://journal.pnm.ac.id/index.php/dikemas/article/view/153>.
- [7] M. Mansyur, "Digital Literacy Model to Counter Hate Speech on Social Media Digital Literacy Model to Counter Hate Speech on Social Media," vol. 22, no. 2, pp. 125–142, 2020.
- [8] I. P. Cahyani, "Digital Literacy of Lecturers As Whatsapp Group Users in Spreading Hoax Informations and Hate Speech," *Expo. J. CommunicationsStudies.*, vol. 2, no. 2, p. 147, 2019, doi: 10.33021/exp.v2i2.562.
- [9] A. Yudhana, I. Riadi, and I. Anshori, "Analysis of Facebook Messenger Digital Evidence Using the Nist Method," *It J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.
- [10] R. A. Bintang, R. Umar, and A. Yudhana, "Analysis of Facebook Lite Social Media with Forensics tools Using the NIST Method," *Techno (Jurnal Fac. Tech. Univ. Muhammadiyah Purwokerto)*, vol. 21, no. 2, p. 125, 2020, doi: 10.30595/techno.v21i2.8494.
- [11] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "1490-Article Text-2859-1-10-20190413," *Digit Evidence Acquisition. On Instagram Messenger Based. Android Using Method. Natl. Inst. Justice*, vol. 4, pp. 219–227, 2018.
- [12] W. A. Mukti, S. U. Masruroh, and D. Khairani, "Analysis and Comparison of Forensic Evidence for Facebook and Twitter Social Media Applications on Android Smartphones," *J. Tech. Inform.*, vol. 10, no. 1, pp. 73–84, 2018, doi: 10.15408/jti.v10i1.6820.
- [13] S. Dogan and E. Akbal, "Analysis of mobile phones in digital forensics," *2017 40th Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2017 - Proc.*, pp. 1241–1244, 2017, doi: 10.23919/MIPRO.2017.7973613.
- [14] N. Anwar and I. Riadi, "Analysis of WhatsApp Messenger Smartphone Forensic Investigations Against Web-Based WhatsApp," *J. Ilm. Tech. Electrical Computing. and Inform.*, vol. 3, no. 1, p. 1, 2017, doi: 10.26555/jiteki.v3i1.6643.
- [15] M. Fitriana, K. A. AR, and J. M. Marsya, "Application of National Institute of Standards and Technology (Nist) Method in Digital Forensic Analysis for Handling Cyber Crime," *Cybersp. J. Educator. Technol. Inf.*, vol. 4, no. 1, p. 29, 2020, doi: 10.22373/cj.v4i1.7241.
- [16] I. Riadi, A. Yudhana, and I. Anshori, "Forensic Analysis of Instant Messenger on Android-Based Smartphones," *J. Insa. Comtech*, vol. 2, no. 2, pp. 25–32, 2017.
- [17] A. Wirara, B. Hardiawan, and M. Salman, "Identification of Digital Evidence in the Acquisition of Mobile Devices from the Instant Messaging Application 'WhatsApp,'" *Teknoin*, vol. 26, no. 1, pp. 66–74, 2020, doi: 10.20885/teknoin.vol26.iss1.art7.
- [18] A. Fauzan, I. Riadi, and A. Fadlil, "Digital Forensic Analysis on Line Messenger for Cybercrime Handling,"

- Annu. Res. Semin.*, vol. 2, no. 1, pp. 159–163, 2017, [Online]. Available: <http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/832/752>.
- [19] V. A. H. Firdaus, D. Suprianto, and R. Agustina, “Digital Forensic Analysis of Volatile Memory to Obtain Dm-Crypt Application Encryption Keys,” *J. Sist. Computer. and Inform.*, vol. 2, no. 3, p. 283, 2021, doi: 10.30865/json.v2i3.2998.
- [20] P. Widiandana, I. Riadi, and Sunardi, “Analysis of Cyberbullying Forensic Investigations on WhatsApp Messenger Using the NIST Method,” *Semin. Nas. Technol. Fac. Engineering Univ. Krisnadwipayana*, pp. 488–493, 2019, [Online]. Available: <https://jurnal.teknikunkris.ac.id/index.php/semnastek2019/article/view/308>.
- [21] I. Riadi, R. Umar, and I. M. Nasrulloh, “Experimental Investigation of Frozen Solid State Drive on Digital Evidence with Static Forensic Methods,” vol. 9, no. 3, pp. 169–181, 2018.
- [22] I. Zuhriyanto, A. Yudhana, and I. Riadi, “Designing Digital Forensics on Twitter Applications Using Live Forensics Methods,” *Semin. Nas. Inform. 2008 (semnasIF 2008)*, vol. 2018, no. November, pp. 86–91, 2018.
- [23] Imam Riadi, Rusydi Umar, and M. I. Syahib, “Acquisition of Digital Evidence for Android Viber Messenger Using the National Institute of Standards and Technology (NIST) Method,” *J. RESTI (System Engineering and Information Technology)*, vol. 5, no. 1, pp. 45–54, 2021, doi: 10.29207/resti.v5i1.2626.
- [24] Imam Riadi, Sunardi, and P. Widiandana, “Investigating Cyberbullying on WhatsApp Using Digital Forensics Research Workshop,” *J. RESTI (System Engineering and Information Technology)*, vol. 4, no. 4, pp. 730–735, 2020, doi: 10.29207/resti.v4i4.2161.
- [25] Mustafa, I. Riadi, and R. Umar, “E-mail Forensic Investigation Design with the National Institute of Standards and Technology (NIST) Method,” *9th Snst*, vol. 9, pp. 121–124, 2018, [Online]. Available: https://publikasiilmiah.unwahas.ac.id/index.php/PROSIDING_SNST_FT/article/download/2385/2371.