Investigation Cyberbullying on Kik Messenger using National Institute of Standards Technology Method

Bagas Yoga Prasetyo
Departement of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
Almost everyone uses social media. In 2019 there were 130 million social media users on mobile devices in Indonesia. As a result, cybercrime crimes that occur on one of the social media platforms, namely Kik Messenger, have increased, one of which is cyberbullying. This study analyzed the data obtained from a smartphone using the MOBILEdit and FTK Imager tools according to the scenario that the researcher has created. The research stage begins by creating a scenario in which cyberbullying occurs on the Kik Messenger application, the next stage is to investigate the evidence of smartphones with the root process first followed by data retrieval, the last stage is to analyze the data found to obtain an analysis result as supporting evidence. The results of the research conducted contained two pieces of evidence, namely, the first smartphone used by the perpetrator. The smartphone is then investigated to retrieve the required data. The second is evidence of conversation between the perpetrator and the victim on the found smartphone. The data is then analyzed to calculate the presentation of the word "buluk" as the word cyberbullying used in the study. The results of the data analysis found 26 sentences containing the word "buluk", and obtained a percentage of 5.92% of the sentences in the a conversation containing the word "buluk". These results can be concluded that there has been cyberbullying in a group conversation by calculating the percentage of the sentence "buluk" as a bullying sentence contained in conversations using the Kik Messenger application.

Keywords
Digital Forensics, Kik Messenger, National Institute Of Standards Technology (NIST), MOBILEdit, Cybercrime

1. INTRODUCTION
Nowadays, almost all activities are connected to the internet, such as communication, work, playing games, searching for information, studying, and so on. Human life cannot be separated from communication with fellow humans. As technology develops, it makes it easier for humans to communicate with each other. Many social media can support as a means of communication, one of which is Kik Messenger.

Based on digital reports issued by We Are Social and Hootsuite, it is recorded that the total number of internet users in Indonesia has reached 150 million people. Social media users on mobile devices in 2019 were recorded at 130 million users. The following are statistics on digital and internet users in Indonesia released by We Are Social. Figure 1 shows the We Are Social data regarding digital users and internet users.

Figure 1. Data on Digital and Internet Users in Indonesia

Kik Messenger is an application used to exchange messages, pictures, videos, etc. with fellow users. Kik application users can search and share videos from the YouTube platform. The Kik application can be used by IOS, Android, Windows 7, Blackberry, and Symbian users.

According to the Organization of European Community Development (OECD), Cybercrime or cyber crime is all illegal access to a data transmission. In other words, all unauthorized activities in a computer system are criminal acts. Cybercrime can physically impact other people, namely, Violent / Potentially Violent. In addition, cyber crime can also have an indirect impact on other people, namely, Non-Violent.

According to research conducted by Imam Riadi and his colleagues, it is formulated that cybercrime is any act of violating the law in which the action is carried out using an electronic device or device as an object, whether it is aimed at getting profit or not, and has a detrimental impact on other parties. One of the digital crimes that often occur on social media Facebook is Cyberbullying. According to research conducted by Imam Riadi and his colleagues, Cyberbullying is an action that aims to cause fear in a person by degrading the honor of others. Indonesia ranks third in the world for cases of Cyberbullying itself, and there are 91% of reports of Cyberbullying experienced by children. (Aziz, Riadi, & Umar, 2018)

In a study conducted on 150,000 young people in 30 countries, led by Professor Ann John from Swansea University Medical School and in collaboration with researchers from Oxford University and Birmingham University who examined the dangers of cyberbullying, both perpetrators and victims, which usually occurs in children under 25 years of age. The results of the study stated that victims of violence on social media were dominated by young people and they were more prone to commit violence against themselves to commit suicide. (Every princess Ariani, 2018)

Based on previous studies that have stated the dangers resulting from cyberbullying, it is imperative that cyberbullying be prevented. One way is by reporting every cyberbullying to the authorities, so that the authorities can process the case and get evidence so that the perpetrator can be punished according to his violation. As the party in charge of handling this case, it is also demanded to further improve their expertise in their field because in this increasingly advanced era, almost all people in the world use social media, thereby increasing the possibility of cyberbullying.

In this study, the researcher created a cyberbullying case scenario with Kik Messenger on a mobile device. The purpose of this study is to analyze the process of investigation or digital forensics in cybercrime cases and to bring up digital evidence using a method, namely the National Institute of Standards Technology (NIST). Researchers hope that this research can contribute to knowledge for academics and law enforcers to help solve problems in the field of mobile forensics.

2. LITERATURE REVIEW

2.1.1 Previous Studies

Research conducted in 2018 by Muhammad Abdul Aziz, Imam Riadi, and Rusydi Umar, has conducted research on digital forensics entitled "Web-Based Forensic Line Messenger Analysis Using the National Institute of Justice Framework", which is the investigation stage of Cybercrime cases that occur on Line Messenger. Web-based. The research used the National Institute of Justice (NIJ) method with a flow of the preparation stage, the collection stage, the examination stage, the analysis stage, and the reporting stage. The first stage is preparation, which is at this stage preparing all the tools needed to carry out the investigation process. Furthermore, the second stage is collection, which is the collection of digital evidence data from relevant sources to maintain the originality of digital evidence data from possible changes that occur. The third stage is examination, which is at this stage examining digital evidence through a forensic process to ensure that the evidence obtained is the same as that obtained at the scene. Next is the analysis stage, at this stage an analysis of digital evidence found in the previous stage is carried out to determine the significance value of the digital evidence. The final stage is reporting, namely after going through the analysis process, the results of the analysis will be obtained which consists of a description of the activities that have been carried out in the investigation process, the tools used in the investigation process, the methods used to simplify the investigation process, actions that can support the investigation, and provide some recommendations as material for evaluating the supporting elements contained in digital forensic investigations. This study uses a simulation of the conversation tapping process on the victim's Line messenger application. This study describes the testing scheme for the web-based Line messenger application as a medium in the search for digital evidence after the tapping process of the victim's smartphone, so that the evidence obtained from the web-based Line application can be found. In the process of this research, the location of log files, cache, and digital evidence image files was found in the Line messenger application conversation[1].

Research conducted in 2017 by Alfian Futuhul Hadi, Dimas Bagus C. W., Moh. Hasan has conducted research on text mining entitled "Text Mining on Twitter Social Media. Case Study: Quiet Period for the 2017 DKI Pilkada Round 2" which aims to extract information from Twitter social media that can be used about what happened during the election process. This research uses methods in text mining such as sentiment analysis, data grouping and visualization. The Naïve Bayes method is used in this study in the classification stage. Naïve Bayes is generally used to predict sentiments that appear on data that still lacks sentiment. The author has 5 scenarios used for Naïve Bayes. The first scenario is to learn and predict processing data. The second scenario is that learning is carried out on 33% of the data then making predictions on the other 33% of the data. The third scenario is that learning is carried out on 33% of the total data on the previous day and is used to estimate sentiment on 33% of the data on the day after. The fourth scenario is that learning is carried out on a combination of 2500 data on April 15-18 2017, to estimate data on April 19, 2017. The fifth scenario is that learning is carried out every day to predict the sentiment that appears on April 19, 2017[2].

Research conducted in 2018 by Imam Riadi, Anton Yudhana, and Muhammad Caesar Febriansyah Putra has conducted research on digital forensics entitled "Acquisition of Digital Evidence on Android-Based Instagram Messenger Using the National Institute of Justice (NIJ) Method" which examines the steps - step of acquiring digital evidence on android based Instagram messenger. The method used in this study is the National Institute of Justice (NIJ). The method consists of several stages, namely, preparation, collection, inspection, analysis, and reporting. The first stage is preparation, which is the process of preparing the equipment needed to carry out the investigation process. The second is collection, which is the process of finding and collecting documents or making copies of physical objects containing electronic evidence. The third stage is examination, where at this stage is the process of making electronic evidence visible and documenting documents and systems, data reduction is carried out to identify evidence. Next is the analysis stage, which is the process of analyzing evidence for the examination stage which is used to determine the significance and probability value. The last one is the reporting stage, which is the process of making examination records of all cases. Research conducted to obtain digital evidence from both smartphones which becomes electronic evidence of crimes with indications of cyberbullying. The acquisition process is carried out using the OXYGEN forensic application so that it gets the desired results, namely digital evidence in the form of images / photos and conversations / chats from Instagram social media installed on the smartphone. The process of acquiring digital evidence that has been successfully obtained on Instagram on a smartphone in a rooted condition, the expected data is obtained, namely in the form of images / photos and conversations / chats, while for smartphones not in root conditions, digital evidence is not obtained[7].

Research conducted in 2017 by Hafid Wijaya, Imam Riadi, and Sunardi conducted research on digital forensics entitled "Digital Forensic Analysis of Telegram Applications on Android-Based Smartphones" which examines the process of lifting and analyzing digital evidence on the Android-based Telegram application. The method used in this study is the National Institute of Standards and Technology (NIST). This method has several stages, namely, collection, examination, analysis, reporting. The first stage is collection, namely the process of identifying, labeling, recording, and retrieving data from relevant data sources by following data integrity maintenance procedures. The second stage is examination, which is the stage of processing data collected digitally

forensics using a combination of various scenarios, both automatic and manual, as well as assessing and releasing data as needed while maintaining data integrity. Next is the analysis (analysis), namely carrying out the analysis process on the results of previous examinations using methods that are technically and legally justified to obtain useful information to assist the investigation process. The third stage is reporting, which is reporting the results of the analysis in the form of a description of the actions taken, an explanation of the tools and procedures used to determine other actions that need to be taken, and providing recommendations for improving policies, procedures, tools, and other aspects of the digital forensic process. . The tools used to carry out the forensic process in this study were MOBILedit Forensic Tool 7.0[10].

Research conducted in 2017 by Luluk Isman, Yudi Prayudi, and Imam Riadi, has conducted research on digital forensics entitled "Ransomware Analysis Based On The Surface, Runtime And Static Code Method". Ransomware is one of the latest malware in recent years that can infect computers and smartphones. The malware is able to encrypt the files inside the computer or smartphone, thus prevents the users (victims) from accessing their system. In addition, the victims will be asked to pay the ransom through certain online payment methods to get a decrypt key. Due to the latest development of ransomware variants, a solution is required to prevent the malware attack. This study analyzes the cryptolockers ransomware which utilize three method such as surface, runtime and static code method. The result provided the detail characteristics of ransomware through three aforementioned methods as well as the solution to prevent the attack[11].

Research conducted in 2018 by Anton Yudhana, Imam Riadi, and Ikhwan Anshori, has conducted research on digital forensics entitled "Facebook Messenger Digital Evidence Analysis Using the NIST Method" which examines the process of removing as much digital evidence as possible from Facebook Messenger on an android smartphone. . This study uses the National Institute of Standards Technology (NIST) method which has several stages, namely, Collection, Examination, Analysis, and Reporting. The first stage is Collection, namely labeling, identifying, recording, and retrieving data from sources relevant to the processor to maintain data integrity. The next stage is Examination, which is the processing of data collected in the use of forensic combinations of various scenarios, both automatic and manual, as well as assessing and releasing the data needed while maintaining data integrity. The third stage is Analysis, namely the process of analyzing the results of the examination using justified technical methods. The last stage is Reporting, which is the process of reporting the results of the analysis which includes a description of the actions taken. The scenario to get digital evidence is to use the Galaxy V + SMG31HZ Smartphone, carry out the rooting process, install the Facebook Messenger application, create messages, carry out investigations using a forensic tool called Oxigen forensic, then analyze the three forensic software tools, the results of the analysis will be reported as evidence. The results that have been obtained are conversational text, images and audio[12].

Research conducted in 2017 by Ade Kurniawan, Imam Riadi, and Ahmad Luthfi conducted research on digital forensics entitled "Forensic Analysis And Prevent Of Cross Site Scripting In Single Victim Attack Using Open Web Application Security Project (OWASP) Framework. Reported eight of the top ten websites in the world are at a critical point of vulnerability from attacks by injection methods such as Cross Site Scripting and SQL Injection that can be used by certain parties to steal information or for a particular purpose. In this paper the research conducted by three key stages: first Attacking (Single Victim Attack: Information Gathering, Live Webcams Screenshot, Keyloggers and Download Spoofer), second stage Analysis (Digital Forensic: Live Forensic and Analysis Evidence) and third stage to Prevent (Patching). Contribution of this study offers a method of protection solutions to users in the browser application to be filtered, disable the plugin, notifying, blocking, and reducing Cross Site Scripting attacks[14].

Research conducted in 2018 by Rusydi Umar, Imam Riadi, and Guntur Maulana Zamron has conducted research on digital forensics entitled "Mobile Forensic Tools Evaluation for Digital Crime Investigation". This research will experiment using available forensic tools with NIST forensic method for extracting latest WhatsApp's. Based on the results of testing conducted on WhatsApp 2.17.147 with .crypt12 encryption, Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor meet validation test of repeatability and reproducibility. WhatsApp Key/DB Extractor dominates in the extraction ability of text message artifacts. Belkasoft Evidence (trial ver) has advantages in extraction abilities for images, videos, and documents. Further research on WhatsApp artifact extraction abilities in non-Android platforms needs to be done considering the WhatsApp application is available for many platforms. artifacts. Forensics tools capabilities will be evaluated and compared to find its strengths and weaknesses[15].

Research conducted in 2017 by Ruuhwan, Imam Riadi, and Yudi Prayudi, has conducted research on digital forensics entitled "Evaluation of Integrated Digital Forensics Investigation Framework for the Investigation of Smartphones Using Soft System Methodology". The handling of digital evidence can become an evidence of a determination that crimes have been committed ora may give links between crime and its victims or crime and the culprit. Soft System Methodology (SSM) is a method of evaluation to compare the conceptual model can be revealed thus it can perform corrective action against the conceptual method, thus there is no difference between the conceptual model and real activity. Evaluation on the IDFF stage is only done on a reactive and proactive process stages in the process so that the IDFF model can be more flexible and can be applied on the investigation process of a smartphone[16].

Research conducted in 2018 by Sunardi, Imam Riadi, and Andi Sugandi, has conducted research on digital forensics entitled "Forensic Analysis of Docker Swarm Cluster using Grr Rapid Response Framework". An attack on Internet network does not only happened in the web applications that are running natively by a web server under operating system, but also web applications that are running inside container. The currently popular container machines such as Docker is not always secure from Internet attacks which result in disabling servers that are attacked using DoS/DDoS. Therefore, to improve server performance running this web application and provides the application log, DevOps engineer builds advance method by transforming the system into a cluster computers. Currently this method can be easily implemented using Docker Swarm. This research has successfully investigated digital evidence on the log file of containerized web application running on cluster system built by Docker Swarm. This investigation was carried out by using the Grr Rapid Response (GRR) framework[17].

Research conducted in 2016 by Sunardi, Imam Riadi, and Andi Sugandi, has conducted research on digital forensics entitled "Investigation on the Services of Private Cloud Computing by Using ADAM Method". Cloud services are offered by many cloud service providers, but most companies generally build a private cloud computing. Cloud systems abuse can be done by internal users or due to misconfiguration or may also refer to the weaknesses in the system. This study evaluated ADAM (Advanced DataAcquisition Model) method. Referring to the results of the investigation process by using ADAM Method, it can be verified that there are several parameters of the success investigation; therefore the investigation by using ADAM can be succesed properly and correctly. Another contribution of this study was to identify the weaknesses of the service system that used owncloud in users list of the same group can change another's user's password[18].

Research conducted in 2016 by Luluk Usman, Yudi Prayudi, Imam Riadi, and Andi Sugandi, has conducted research on digital forensics entitled "Ransomware Analysis Based On The Surface, Runtime And Static Code Method". Ransomware is one of the latest malware in recent years that can infect computers and smartphones. The malware is able to encrypt the files inside the computer or smartphone, thus prevents the users (victims) from accessing their system. In addition, the victims will be asked to pay the ransom through certain online payment methods to get a decrypt key. Due to the latest development of ransomware variants, a solution is required to prevent the malware attack. This study analyzes the cryptolockers ransomware which utilize three method such as surface, runtime and static code method. The result provided the detail characteristics of ransomware through three aforementioned methods as well as the solution to prevent the attack[19].

Distributed Denial of Service (DDoS) is a network security problem that continues to grow dynamically and has increased significantly to date. DDoS is a type of attack that is carried out by draining the available resources in the network by flooding the package with a significant intensity so that the system becomes overloaded and stops. This attack resulted in enormous losses for institutions and companies engaged in online services. Prolonged deductions and substantial recovery costs are additional losses for the company due to loss of integrity. The activities of damaging, disrupting, stealing data, and everythingthat is detrimental to the system owner on a computer network is an illegal act and can be imposed legally in court. Criminals can be punished based on the evidence found with the Forensics network mechanism. DDoS attack classification is based on network traffic activity using the neural network and naïve Bayes methods. Based on the experiments conducted, it was found that the results of accuracy in artificial neural networks were 95.23% and naïve Bayes were 99.9%. The experimental results show that the naïve Bayes method is better than the neural network. The results of the experiment and analysis can be used as evidence in the trial process[20].

2.1.2 Digital Forensic

Forensics is an investigative process to establish a fact relating to a related legal issue. Digital forensics is a part of forensic science which includes the discovery and investigation of material obtained from the investigation process found on digital devices. The field of digital forensics is growing rapidly which is developing following advances in information technology.[6]

2.1.3 Digital Evidenve

Digital evidence is evidence that is extracted or recovered from electronic evidence. Forensic analysts must look for digital evidence, who can then investigate the connection between criminal cases.

2.1.4 Kik Messenger

Kik messenger is a social media that is used to exchange messages, pictures, videos, etc. The application was founded in 2009 and released in April 2010 by students from the University of Waterloo in Canada. Kik claims that the Kik application users have reached 40 million users from all over the world in April 2013, 3 years away from its release in April 2010.

2.1.5 Cybercrime

Cybercrime is an act against the law that is carried out using a network of electronic devices as a medium or as an object of crime, whether it is profitable or not, and can harm other parties.

3. METHODOLOGY

3.1 Research Scenario

The research subject that will be discussed is the analysis of evidence from Cybercrime that occurs on Kik Messenger social media. The level used in this study is the meso level because it includes a group of companies. This research is expected to contribute knowledge and insights in the field of digital forensics.

Figure 2. Research Scenarios

This research scenario aims to explain the stages of uncovering evidence of cybercrime cases that occurred on Kik Messenger, as shown in Figure 2. The scenario will be investigated into evidence until the final report. In this study, researchers used an account created as the account of the criminal in this scenario. In the scenario the perpetrator commits a crime in the form of cyberbullying on the Kik Messenger application. The conversation is carried out in a chat group that has five group members. There is one account that is the target of bullying by all other group members. Bullying that is emphasized in this scenario is physical bullying. In this scenario the perpetrators mentioned the word "buluk" as a call to the victim. The investigation process will be carried out on one of the perpetrator's smartphones. The next step is to determine the tools to retrieve chat data from the Kik Messenger account. The data retrieval process uses MOBILEedit tools to manage the data to be analyzed. Based on the data that has been collected, then data analysis is carried out using the National Institute of Standards Technology method. The last stage after the analysis stage is the report, namely the stage of making a report on the results of the analysis that has been carried out previously and ensuring that each process is in accordance with applicable procedures.

3.2 Analysis Research

This process is a stage for proof to see the conversation between perpetrators and victims in a chat group. The next stage is to carry out a scenario that has been prepared by the researcher. The case that is being screened is a case of cyberbullying that occurs between several perpetrators and 1 victim. In this case, the perpetrator is screened for a conversation in a chat group that leads to cyberbullying to the victim through a conversation on the Kik Messenger application. This scenario uses the Samsung Galaxy Core 2 smartphone as the victim's smartphone. The condition of the scenario is that the victim and the perpetrator are friends. At first the perpetrator asked about the victim as an old friend. After some time the conversation continued, the perpetrator began to turn to cyber bully by talking about the victim's physical disrepair. The victim felt offended by the perpetrator's words in the conversation, and the victim reported the case to the authorities. After the victim reports the crime they experienced, an investigation process will be carried out through several stages. The first stage will be imaging first. Furthermore, the imaging results will be investigated using the FTK Imager tool. after finding evidence using the FTK Imager tools, then the evidence will be compared with the evidence found on the MOBILEdit tools. Evidence that has been investigated will be calculated for analysis of the word "buluk" found using Excel, which will then be reported as the final stage.

Figure 3. Conversation Investigation Scenarios

Figure 3 shows the scenario of a conversation between the perpetrator and the victim via a smartphone. The conversation takes place in a chat group that has five members. Then the investigation is carried out on the victim's smartphone who is a member of the chat group. After the scenario of the conversation between the perpetrator and the victim is carried out, an investigation is carried out by the investigator, namely the author himself. The initial stage of the investigator is to secure evidence in the form of the victim's smartphone and ensure that all data resulting from the conversation. The investigator analyzes the conversation that has been found on the perpetrator's smartphone.

3.3 Research Stages

In this study using the Mobile Forensic method developed by the National Institute of Standards Technology (NIST). There are several stages in the National Institute of Standards Technology method, including: Collection, Examination, Analysis, Reporting, which can be seen in the following figure 4:

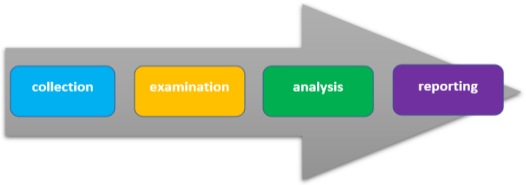

Figure 4. Stages of the National Institute of Standards Technology Method

1. Collection

At this stage, the process of identification, labeling, recording, and data collection will be carried out from relevant data sources according to the procedure.

2. Testing

At this stage, the data collected digitally forensic will be processed using scenarios, as well as assessing and releasing data according to the needs of the forensic process.

3. Analysis

The analysis stage is carried out on the results of the examination by methods that are in accordance with law to obtain information to assist the examination process.

4. Reports

The final stage is a report from the results of the analysis carried out previously which includes the actions taken, an explanation of the tools used, the procedures chosen, and other actions taken and providing recommendations for further research.

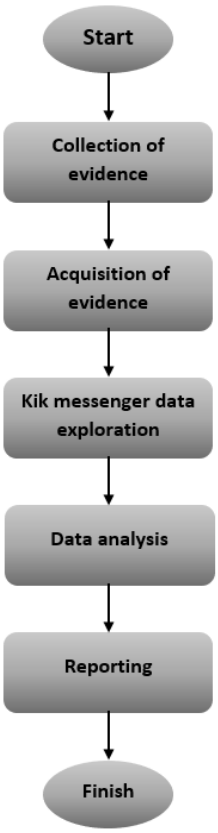

Figure 5. Kik Messenger Investigation Flowchart

Figure 5. is a flowchart of the perpetrator's conversation investigation flowchart from the perpetrator's smartphone on Kik Messenger carried out by the investigator. The stages of the investigation process on Kik Messenger include:

a. Investigators secure evidence in the form of the perpetrator's smartphone and carry out investigations according to the stages in the National Institute of Standards (NIST) method.
b. Investigators obtain evidence obtained for processing imaging data obtained from Kik Messenger.
c. Investigators confirm that the smartphone is rooted for more control.
d. Investigators explore data on the Kik Messenger application.
e. Investigators perform data extraction to obtain evidence of conversations in the Kik Messenger application.
f. The investigator the contents of the perpetrator's message obtained from the perpetrator's smartphone.

3. RESULTS AND DISCUSSION

The research that has been done has found results. The process of collecting evidence on a smartphone using the MOBILEdit and FTK Imager tools. The following in table 1. is a requirement for the tools used in research.

Table 1. Tools and Materials

Number	Name	Spesification	Information
1.	Laptop	Asus GL503VD, Windows 10	Hardware
2.	Smartphone	Android Kitkat, Root	Hardware
3.	Kik Messenger	Android Application	Software
4.	MOBILEdit	Application	Software, Forensic Tools
5.	FTK Imager	Application	Software, Forensic Tools

3.1 Collection

In the collection process using an android smartphone. The smartphone used in this study uses the Samsung SM-G355H which uses the Android Kitkat.

Figure 6. Smartphone used

Figure 6. shows the smartphone used in this study. The smartphone used is the Samsung SM-G355H using the Android operating system and is already in a rooted state. Rooting on a smartphone is used to make it easier to access all the data on the smartphone.

3.2 Testing and analysis

In the testing process, the first Kik Messenger application was tested using the MOBILEdit tool. The investigation process using MOBILEdit tools has several stages.

Figure 7. Physical image process

Figure 7. is a physical image process. The physical imaging process takes a long time depending on the size of the device's storage on the smartphone.

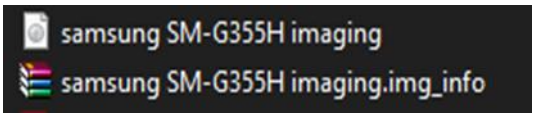

Figure 8. Imaging file

Figure 8. shows the imaging results using MOBILEdit. The physical image process will produce a file with the format "img".

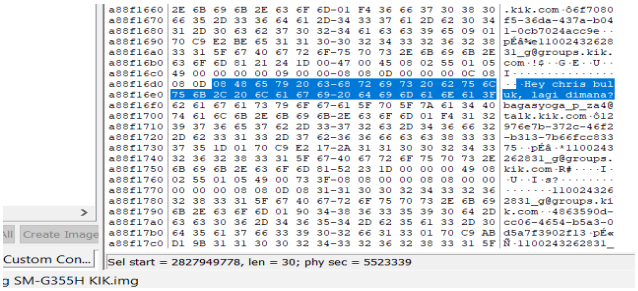

Figure 9. The conversation found

Figure 9. shows the results of testing using the FTK Imager on the Kik Messenger application. The test finds the appropriate conversation in the research scenario. The text found was "Hey chris buluk, lagi kemana?".

Figure 10. Smartphone information

Figure 10. shows the information that can be found on a smartphone using the MOBILEdit tools. Information that can be found includes smartphone series, information on rooting, SIM card not installed, and much more.

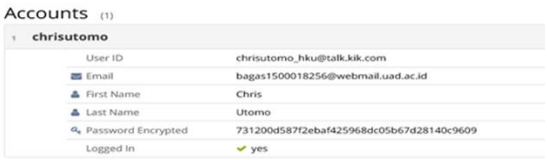

Figure 11. Account information found

Figure 11. shows the account information found on a smartphone using the MOBILEdit tool. Information found, namely, user ID, user email, user name, and account password are still encrypted.

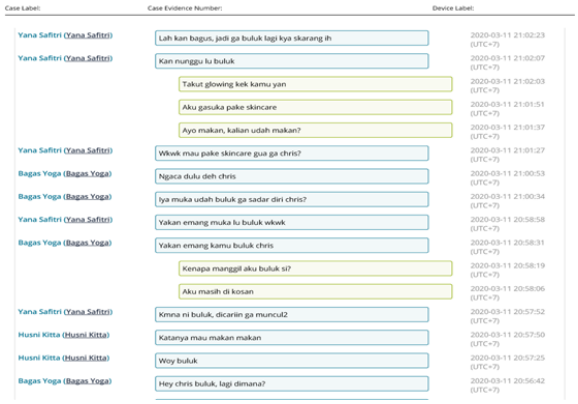

Figure 12. Evidence of conversation between perpetrator and victim

Figure 12. shows evidence of a conversation between the perpetrator and the victim found on a smartphone using the MOBILEdit tool.

3.3 Reporting

Reporting is the final stage of research that discusses the results of the analysis that has been carried out on evidence.

Table 2. Conversation evidence table

Proof of Conversation	Number of Words
Ngaca dulu deh chris	4
Wkwk mau pake skincare gua ga chris?	7
Ayo makan, kalian udah makan?	5
Aku gasuka pake skincare	4
Hei buluk, lu udah ngerjain tugas dari bu risma?	9
Total Number of Words	439
Number of Sentences Containing the Word "Buluk"	26
% Sentences Containing the Word "Buluk"	5,92%

Table 2. shows the conversation. The calculations in the table use Microsoft Excel. The table shows the number of words for each chat. Total words from all conversations totaled 439 words. Furthermore, after getting the total number of words from the conversation conducted, it is necessary to count the number of sentences containing the word "buluk". Found 26 words containing the word "Buluk" in all conversations as the word bullying in the research scenario. So it can be determined that the percentage of words that contain the word "Buluk" is 5.92% of the total number of words in the conversation found on the KIK Messenger application.

4. CONCLUSION

Based on the research that has been done, research has been carried out using a scenario that has been created. This research uses a Samsung SM-G355H smartphone that has been rooted, and uses forensic tools such as FTK Imager and MOBILEdit. FTK Imager is used to identify physical results files using the MOBILEdit tool. The results found were based on extraction using the FTK Imager tool in the form of evidence of the same conversation as the findings on the perpetrator's smartphone. The results of this test and research use the Microsoft Excel application to calculate the total number of words found in the conversation. In this study, 439 total words of group conversations were found for the scenario. Furthermore, we can count the number of words containing the word "buluk" as the word bullying in this study. There were 26 words that contained the word "buluk" in conversation, so it could be determined that the percentage of the word "buluk" that appeared was 5.92%. This research does not discuss conversations that have been deleted and for the recovery of deleted conversations, the hope is that it can be developed regarding conversations that have been deleted and the recovery process of message history in the database. So the focused results are some things related to suspects and Instagram, for more details see Table 3.

Table 3. Results of All Tools

Number	Digital Evidance	MOBILEdit	FTK Imager
1.	Text Chat	✓	✓
2.	User Name	✓	✓
3.	Email	✓	✓
4.	Time	✓	✓

From table 3 it can be seen that the results of the MOBILEdit and FTK Imager tools have the same results.

5. REFERENCES

[1] Aziz, M. A., Riadi, I., & Umar, R. (2018). Analisis Forensik Digital Pada Line Messenger Untuk Penanganan Cybercrime. Annual Research Seminar (ARS) ISBN : 979-587-626-0, 2(1), 159–163.

[2] Hadi, A. F., W, D. B. C., Hasan, M., & Penelitian, A. D. (2017). Text Mining Pada Media Sosial Twitter Studi Kasus : Masa Tenang Pilkada Dki.

[3] Kunang, Y. N. A. K. (2016). Implementasi Prosedur Forensik untuk Analisis Artefak Whatsapp pada Ponsel Android. 2(1), 59–68.

[4] Actoriano, Bery (2018). Investigasi Forensik Pada Whatsapp Web Dengan Penerapan Framework Integrated Digital Forensik Investigation Framework V2 (IDFIF V2)

[5] Marfianto, Anang (2018). Analisis Forensik Whats App Mesengger Berbasis Android Menggunakan Metode Text Mining

[6] Raharjo, B. (2013). Sekilas Mengenai Forensik Digital. Jurnal Sosioteknologi, 12(29), 384–387. https://doi.org/10.5614/sostek.itbj.2013.12.29.3

[7] Riadi, I., Yudhana, A., Caesar, M., & Putra, F. (2018). Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ). 4, 219–227.

[8] Ruuhwan, R., Riadi, I., & Prayudi, Y. (2016). Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone. Jurnal Edukasi Dan Penelitian Informatika (JEPIN), 2(1). https://doi.org/10.26418/jp.v2i1.14369

[9] Hermaduanti, N, & Riadi, I. (2017). Automation Framework For Rogue Access Point Mitigation In Ieee 802.1x-Based Wlan.

[10] Wijaya, H., Riadi, I., & Sunardi. (2017). Analisis Forensik Digital Aplikasi Telegram Pada Smartphone Berbasis Android. Semantikom, 95–98.

[11] Isman, L, Prayudi, Y, & Riadi, I. (2017). Ransomware Analysis Based On The Surface, Runtime And Static Code Method.

[12] Yudhana, A., Riadi, I., & Anshori, I. (2018). Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. It Journal Research and Development, 3(1),13.https://doi.org/10.25299/itjrd.2018.vol3(1).1658

[13] Trisnasenjaya, Helmy (2018). Rancang Bangun Forensik Whatsapp Messenger Terhadap Kejahatan Penipuan Berbasis Android Menggunakan Metode National Institute of Standard and Techno

[14] Kurniawan, A, Riadi, I. & Luthfi A. (2017). Forensic Analysis And Prevent Of Cross Site Scripting In Single Victim Attack Using Open Web Application Security Project (Owasp) Framework

[15] Umar, R, Riadi, I, & Zamroni, G. (2018). Mobile Forensic Tools Evaluation for Digital Crime Investigation

[16] Ruuhwan, Riadi, I, Prayudi, Y. (2017). Evaluation of Integrated Digital Forensics Investigation Framework for the Investigation of Smartphones Using Soft System Methodology.

[17] Sunardi, Riadi, I, Sugandi, A. (2019). Forensic Analysis of Docker Swarm Cluster using Grr Rapid Response Framework.

[18] Widiyasono, Nur, Riadi, I, & Luthfi, A. (2016). Investigation on the Services of Private Cloud Computing by Using ADAM Method.

[19] Usman, L, Prayudi, Y, & Riadi, I. (2017). Ransomware Analysis Based On The Surface, Runtime And Static Code Method.

[20] Yudhana, A, Riadi, I, & Ridho, F. (2018). DDoS Classification Using Neural Network and Naïve Bayes Methods for Network Forensics.