

Mobile Forensic on WhatsApp Services for Cybercrime Case using National Institute of Standards and Technology

Syaharul Khori Abrianto
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

The development of information technology (IT) and science every year is growing very rapidly, especially smartphone devices. The development of this smartphone has also given rise to many social media applications, one of which is WhatsApp. The WhatsApp application has a variety of features that can facilitate user chat interactions. However, the use of WhatsApp also has a negative impact, one of which is a crime committed by creating conversation scenarios containing Online Prostitution or also called Cyber Prostitution through a WhatsApp-based application. This research aims to restore evidence from conversations containing online prostitution activities that have been deleted by perpetrators, by implementing the National Institute of Standards and Technology (NIST) stages which have four stages, namely collection, examination, analysis, and reporting. This research uses a smartphone that has WhatsApp installed and is already rooted. The process of searching for digital evidence uses three forensic tools, namely MOBILedit Forensic Express, SQLite Studio, and Beekeeper Studio. The search for evidence in this research is based on the goals and desired scenarios. Based on the percentage index measurement the number of each tool in the process of finding evidence, the conversation data gets 100% percentage, detail time and date messages were sent and received by 33%, smartphone contacts by 100%, and pictures by 33%. The digital evidence will be used as supporting evidence in the court process by adding other evidence findings.

Keywords

Forensic, Mobile, WhatsApp, NIST, Cyber Prostitution

1. INTRODUCTION

This era has entered the digital era, so that most human activities are carried out through various electronic media, especially internet-based ones, including social media [1]. One of the social media that is currently popularly used by many people in the WhatsApp application. WhatsApp is an application like an instant message sender using the internet network that can be used on smartphones, tablets, and computers [2]. WhatsApp also has many features such as telephone, group chat, messaging, video calling, file sending, and voice messaging [3]. During the COVID-19 pandemic, one form of crime that occurred in the WhatsApp application was online prostitution, which was not only an intermediary for transactions but also led to a meeting and direct prostitution activities [4]. WhatsApp itself stores all its conversations in a database on each WhatsApp user's device [5]. To find the digital evidence, in this research the method

that will be used is National Institute Of Justice (NIST), namely collection, examination, analysis, and reporting [6].

1.1 Research Literature

1.1.1 Previous Research

The first research has conducted a research entitled "Digital Forensic Analysis of WhatsApp Applications on Android-Based Smartphones" this analysis process uses the NIST method. Starting from taking evidence on a smartphone, then the rooting process using the KingRoot application, then lifting evidence using MOBILedit Forensic, and the last one is making a report [7].

The second research has conducted a digital forensics research entitled "Facebook Messenger Digital Evidence Analysis Using the NIST Method". This research aims to carry out the removal of digital crime evidence from Facebook Messenger on an Android smartphone. The stages are through a forensic investigation using a forensic tool called Oxygen forensics, then an analysis is carried out on the forensic software tool, the results of the analysis will be reported as evidence. The results obtained are conversational text, images, and audio as evidence [8].

The third research has conducted digital forensic research entitled "Forensic Analysis of KakaoTalk Applications Using National Institute Standard Technology Methods". The purpose of this research is to assist the process of investigating a digital crime contained in the KakaoTalk Application with the NIST method. The process stages are taking evidence in the form of an Android smartphone to be analyzed, then rooting with the KingRoot application on an Android smartphone to be analyzed, then the process of removing digital evidence from the KakaoTalk application using the MOBILedit Forensic Tool software. After that, make a report on the results of the appointment and an analysis of the digital evidence that has been obtained. The expected result of this research is the analysis process can run well and get digital evidence from KakaoTalk on Android smartphones [9].

The fourth research has conducted digital forensic research entitled "Investigative Analysis of Android Forensic Short Message Service (SMS) on Smartphones". This research aims to find digital evidence of deleted chat messages on the smartphone SMS application through the DRFWS method. Starting from the collection of digital evidence in the form of a smartphone device needed to carry out the research process, then the stage of checking and retrieving data from a smartphone to obtain data that has been deleted on the

evidence, then an analysis of the results of the examination process is carried out. After that, make a report on the results of the appointment and an analysis of the digital evidence that has been obtained. The result of this research is that the recovery of digital evidence in the form of a search to recover deleted SMS messages has been successfully carried out, with the FTK Imager tool, which is highly recommended as a tool in proving criminal cases in court [10].

The last research has also conducted digital forensic research entitled "Application of the National Institute Of Standard Technology (NIST) Method in Digital Forensics for Cybercrime Handling". The purpose of this research is to find forensic digital evidence to handle Cybercrime cases by utilizing the WhatsApp Messenger application using the NIST method and several tools to find forensic digital evidence. The results obtained in this research are the contents of WhatsApp conversations that have been deleted which can be digital evidence in revealing pornographic crimes that occurred [11].

1.1.2 Digital Forensics

Digital Forensics is a forensic method in the field of computer science and technology in terms of legal evidence, which in this case is to prove cybercrime scientifically so that they can get valid digital evidence [12]. Digital forensics can also be referred to as the art of recovering and analyzing content found on digital devices such as desktops, notebooks, tablets, and smartphones [13]. The main purpose of digital forensics is to find and search for evidential data or information from a case that is stored and transmitted in digital form, which can ultimately be used in court [14].

1.1.3 Mobile Forensics

Mobile device forensics is one of the branches of digital forensics that deals with the recovery of digital evidence or data from mobile devices with accountable methods or stages [13]. Mobile forensics is a constantly evolving science and presents a real challenge to the forensic law enforcement community and law due to the rapid and unstoppable changes in technology [15]. In mobile forensics, researchers will analyze mobile devices from any OS platform to retrieve evidence. Among all platforms, Android is the most frequently used forensic platform [13]. Mobile Forensics, will use different tools and are specifically for mobile or smartphone forensics such as MOBILedit Forensics and Oxygen Forensics [16].

1.1.4 Digital Evidence

Digital Evidence or electronic evidence is evidentiary information stored or sent in digital form that can be used by one of the parties in a case in court [13]. Digital evidence relating to mobile devices can be found in browser history, phone book, SMS and MMS, Photos, Audio, and Video [17]. To be accepted in court, digital evidence must have its characteristics, namely Admissible (acceptable), Authentic (original), Believable (trusted), Reliable (trustworthy), and Complete (complete) [18].

1.1.5 WhatsApp Application

WhatsApp is an internet-based application that allows each user to share various kinds of content according to the features in the WhatsApp application [19]. The features contained in WhatsApp are a gallery for inserting pictures or photos, adding contacts, a camera for taking pictures, audio for sending voice messages, and maps for sending various coordinates of map locations according to GPS, as well as

documents for inserting files in the form of documents. All these files can be sent in an instant through the WhatsApp Application [20].

1.1.6 Cybercrime

Cybercrime is a crime committed by using a computer as a tool for the occurrence of crimes in the digital era, such as child pornography, bullying, online fraud, and data theft [21]. Cybercrime is mostly done to generate profit for cybercriminals. Some of these crimes are committed against computers or devices directly to damage or disable them, while others use computers or networks to spread illegal information, malware, images, or other materials [22].

1.1.7 Cyber Prostitution

Cyber Prostitution is wronga crime that is very troubling and get attention in society. The general understanding of prostitution is an activity that is interpreted as a transaction between money and sex [23]. In line with current technological advances, the practice of prostitution has penetrated into the cyber world, so the notion of cyber prostitution is the activity of offering sexual services through cyberspace and is part of cybercrime which is the dark side of activities in cyberspace [24].

1.1.8 National Institute of Standard Technology

NIST provides a standardized framework that can be used in solving problems, as well as analyzing digital evidence or stages to obtain information from digital evidence [25]. The National Institute of Standards and Technology (NIST) mobile forensics stages have the following stages:



Figure 1. NIST Method Stages

In Figure 1, NIST has several methods, namely collection, examination, analysis, and reporting [26]. The method can be described in stages as follows:

1. Collection
The Collection is recording labels, identification, retrieval of data, and records from original or relevant data sources by procedures to maintain data integrity.
2. Examination
The Examination is data processing integrated into forensic use with a combination of various scenarios, either automatically or manually, as well as assessing and releasing data as needed while maintaining integrity or completeness of the data
3. Analysis
The Analysis is the analysis of the results of the examination using technically justified methods and according to the law.
4. Reporting
The Reporting stage is the stage of reporting the results of the analysis which includes the description of the actions taken.

2. METHODOLOGY

2.1 Research Scenario

The scenario in this research was made to explain the steps in mobile application forensics that will be carried out to obtain

digital evidence sought on the WhatsApp application. This research scenario using a smartphone that has been rooted and has been connected to the WhatsApp application has been used as a medium for interaction and as evidence in uncovering cases of Cyber Prostitution crimes committed by perpetrators and their customers. The flow of this scenario can be seen in Figure 2.

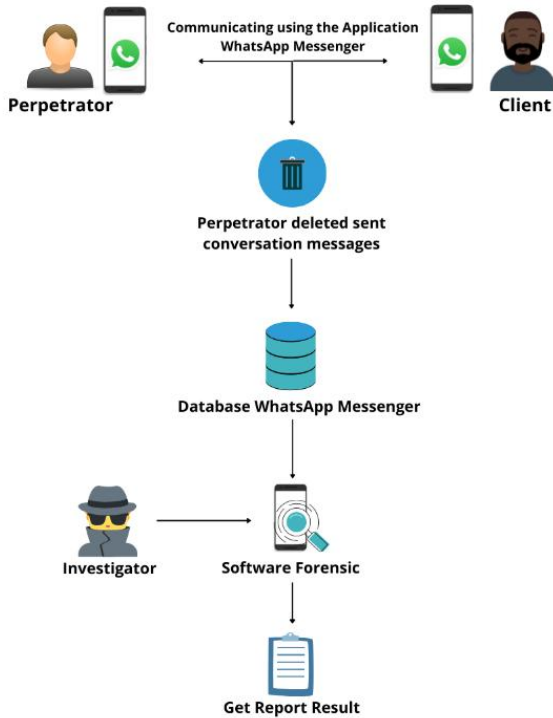


Figure 2. Research Case Scenario

In Figure 2, the flow of the mobile forensic scenario starts from the perpetrator who communicates with prostitution customers, namely smartphones through the WhatsApp application. The customer asks the perpetrator to find a woman who can be invited to commit adultery at the hotel. The results of the two conversations will be stored in the perpetrator's smartphone database. The communication made by the perpetrator was then deleted by the perpetrator to eliminate traces of the actions of the Cyber Prostitution case. Investigators will then confiscate the perpetrator's smartphone for examination and forensic data in the form of communication messages that have been deleted by the perpetrator. After the forensic process is complete, the results of the report will be published.

2.2 Research Stages

The stages in this research use a series of procedures that use the stages from the National Institute of Standards and Technology (NIST) which consists of four stages carried out in the settlement and investigation of cases, namely collection, examination, analysis, and reporting. The following is an explanation of the NIST stages.

2.2.1 Collection

Collection is a stage related to data collection, the stage where an investigator searches for and collects evidence at the location of the case, either in the form of hardware or software. Investigators then collected evidence in the form of an Android-based smartphone that had the WhatsApp application installed, which the perpetrator used to exchange

messages with customers in committing crimes against online prostitution cases. In addition to evidence in the form of a smartphone, a data cable was also found which is usually used to charge by the perpetrators. The data cable that became evidence can be used by Investigators to connect smartphones with PCs, with the aim of obtaining data in the form of imaging files or WhatsApp databases on the perpetrator's smartphone. The following evidence collected by the Investigator can be seen in Table 1.

Table 1. Evidence seized by police




No	Name Of Evidence	Picture	Description
1	The perpetrator's smartphone is seen from the front side		The Samsung Galaxy J1 Ace brand is on, connected to the network, and rooted
2	The perpetrator's smartphone seen from the back		
3	USB Cable		The data cable is not connected to the smartphone

Table 1 is a table that displays documentation of evidence physical evidence found at the scene of the incident which was later collected by the police and will be forensically examined by investigator.

2.2.2 Examination

Examination is a process to prove the integrity of data. An examination is a stage to protect evidence from damage and changes by irresponsible parties so that data integrity can be known that digital evidence has not been modified. To protect digital evidence, this can be done by hashing the electronic data that has been successfully backed up. The initial results and the final results of the hashing will be matched to determine the authenticity of the data from the digital evidence that has been obtained. The hashing process in this research uses CSV file and DB file from the MOBILedit software using the Hash tool.

2.2.2.1 Examination CSV File

The hashing process in this research was carried out on the results of CSV file that had been successfully backed up on a rooted smartphone, using MOBILedit Forensic Express.

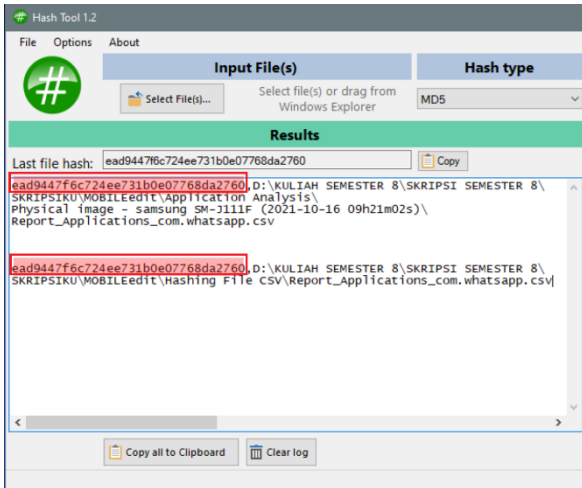


Figure 3. The Result of Hashing the CSVfile Data Backup

In Figure 3, Report_Applications_com.WhatsApp file data in CSV format between the original file and the copy file shows the hashed result by generating the same hash (code from the encryption) in both folders with different storage locations, which means no data changes.

2.2.2.2 Examination DB File

The hashing process in this research was carried out on the results of the DB file that had been successfully backed up on a rooted smartphone, using MOBILedit Forensic Express.

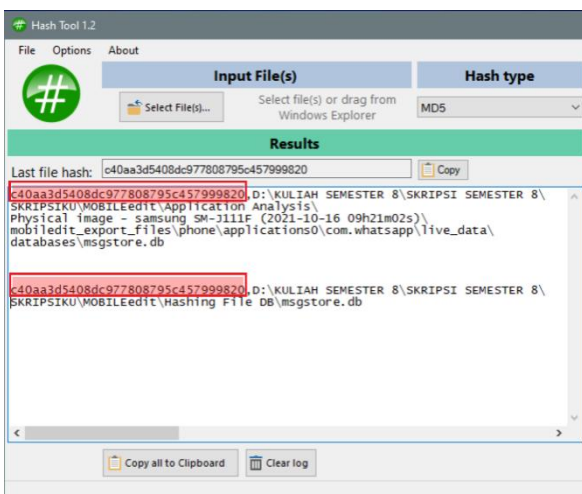


Figure 4. The Result of Hashing the DB file Data Backup

In Figure 4, the DB formatted msgstore.db file data between the original file and the copy file shows hashing results by generating the same hash (code from the encryption) in both folders with different storage locations, which means no data changes.

2.2.3 Analysis

Analysis is collecting and finding evidence from the evidence that has been obtained in a case. The analysis of this crime case is carried out by analyzing the results of the Hash Tool examination, using the forensic tools MOBILedit forensic express, SQLite Studio, and Beekeeper Studio. The purpose of the analysis using these forensic tools is to collect and search for conversation data that indicates a crime in the mobile-based WhatsApp application. The results of the data analysis will be concluded to be included in the Reporting

stage.

2.2.3.1 MOBILedit Forensic Express

The analysis process will start by opening the MOBILedit Forensic Express tool, then the investigator will select the WhatsApp application from which the data will be extracted, the WhatsApp application is stored in the com.WhatsApp directory is shown in Figure 5.

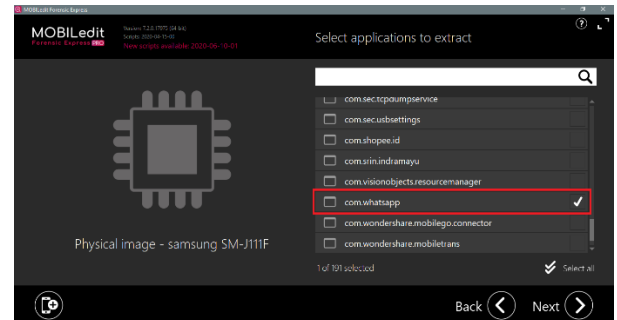


Figure 5. Data Extract Options Display

In Figure 5, after selecting the WhatsApp application to extract the data, the extraction process will appear as shown in Figure 6. The extraction process takes several minutes, depending on the size of the perpetrator's smartphone storage.

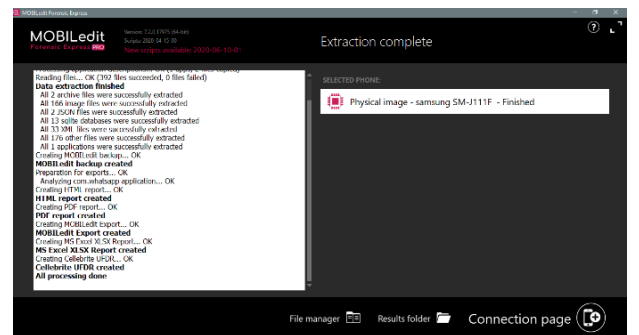


Figure 6. MOBILedit Forensic Express Extraction Process

Figure 6 shows the data extraction process, after the data extraction process is complete, the extracted files will be saved automatically in the directory selected by the investigator.

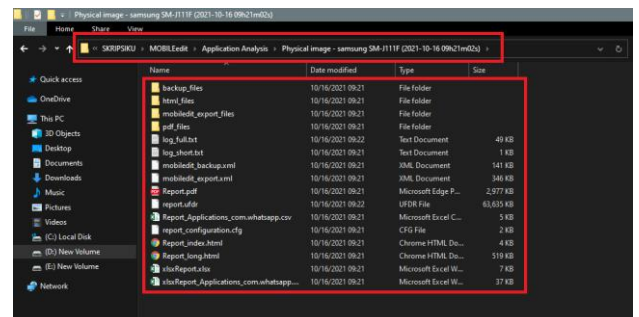


Figure 7. Data Extract Results

Figure 7 is a report of WhatsApp data extraction using Forensic MOBILedit in .txt, .html, pdf, and excel formats. Open the report file in Report.pdf format to find out the results of the data extraction report.

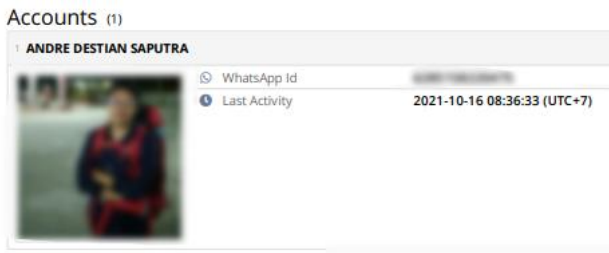


Figure 8. Perpetrator Account View

Figure 8 is the account information suspected of being a cyber prostitution actor with the name Andre Destian Saputra, with WhatsApp id numbered 62851xxxxxxx, and Last activity was seen on October 16, 2021, at 08.36 WIB.

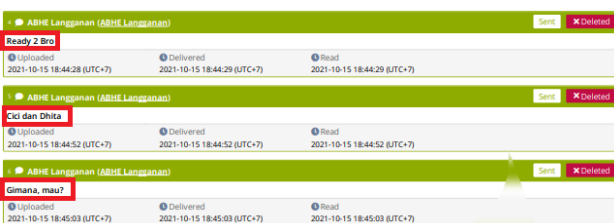
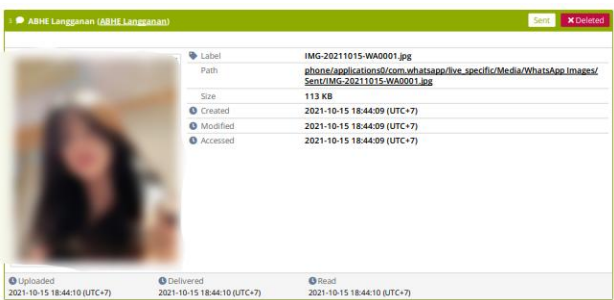
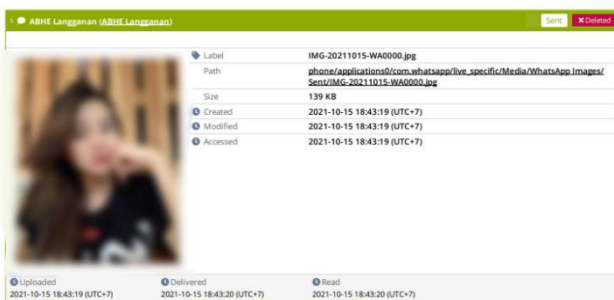
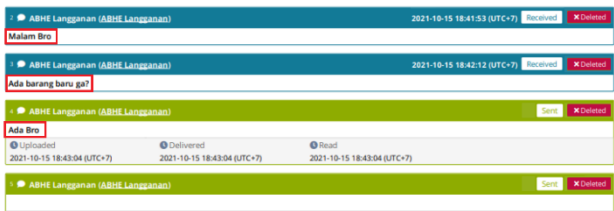


Figure 9. View of Deleted Conversations

In Figure 9, the conversation between the perpetrator and the cyber prostitution customer has also been successfully obtained, as shown in Figure 9. Several contacts were also found on the perpetrator's smartphone from the Report.pdf.

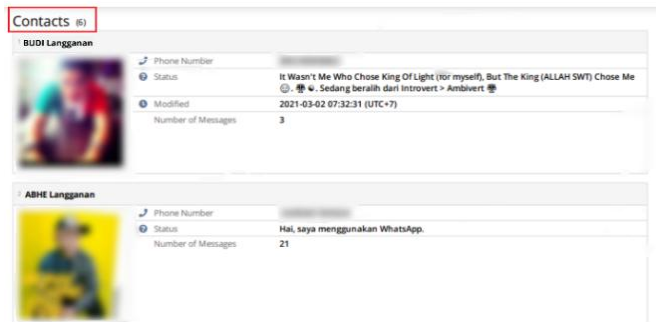


Figure 10. Contact Finding on Smartphone

In Figure 10, it can be seen that 6 contacts were found on the perpetrator's smartphone, there were also user photos, user numbers, and message statuses which has been found.

2.2.3.2 SQLite Studio

The stages of the analysis process begin by opening the SQLite Studio tool, the function of this tool can open a database with .db format. After getting all the data related to the WhatsApp application in the previous process, the next step is to open the "msgstore.db" database file, then select the "messages" table to display the conversation between perpetrators and cyber prostitution customers. The conversation between the two is shown in Figure 11 using the SQLite Studio tool.

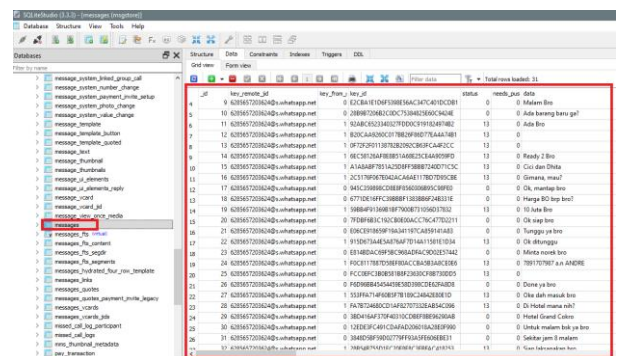


Figure 11 Evidence of Conversation that was found

Figure 11 is a display of conversation evidence findings from the SQLite Studio tool on the "msgstore.db" database table "messages". Other digital evidence that was found was in the form of contacts on the smartphones of cyber prostitution perpetrators, as shown in Figure 12.

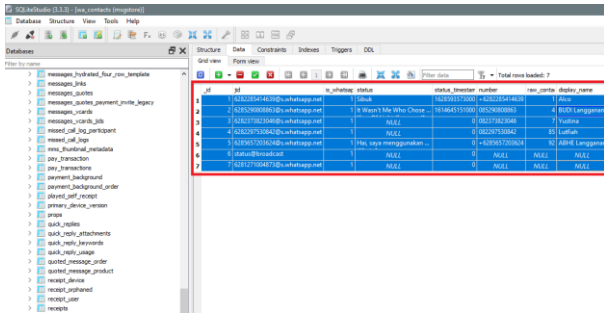


Figure 12 Finding Contacts on the Perpetrator Smartphone

Figure 12 shows the findings of data contacts that were successfully obtained from the forensic process carried out using SQLite Studio.

2.2.3.3 Beekeeper Studio

Stages of the analysis process can also use the Beekeeper Studio tool, the function of this tool can also open a database with.db format. After getting all the data related to the WhatsApp application in the previous process, the next step is also the same, by opening the "msgstore.db" database file, then selecting the "messages" table to display the conversation between the perpetrator and the cyber prostitution customer. Their conversation is shown in Figure 13 using the Beekeeper Studio tool.

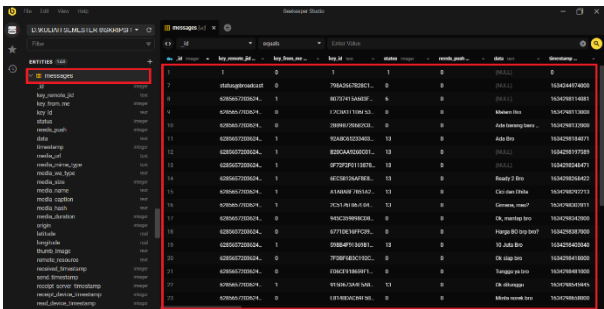


Figure 13 Evidence of Conversation that was found

Figure 13 is a display of conversation evidence findings from the SQLite Studio tool on the "msgstore.db" database table "messages". Other digital evidence that was found was in the form of contacts on the Smartphones of cyber prostitution actors, as shown in Figure 14.

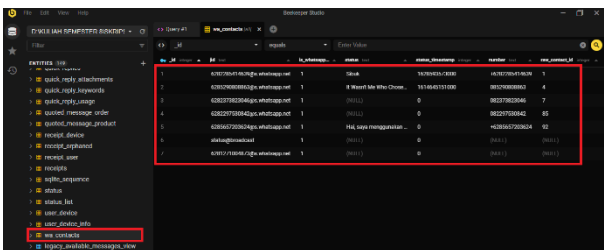


Figure 14 Finding contacts on the perpetrator smartphone

Figure 14 shows the findings of contacts data that were successfully obtained from the forensic process carried out using Beekeeper Studio.

2.2.4 Report

The report is the final stage and aims to present the analysis of the data found in the process of collection, examination, and analysis. The results of the evidence report consist of several tools used, namely: MOBILedit Forensic Express, SQLite Studio, and Beekeeper Studio. The three tools used produce different digital evidence findings. As can be seen in Table 2.

Table 2 The Finding of Digital Evidence

No	Digital Evidence Finding
1	<p>Tool MOBILedit Forensic Express</p>
2	<p>Tool SQLite Studio</p>
3	<p>Tool Beekeeper Studio</p>

From Table 2 above, the findings of evidence in the form of the conversation deleted by the perpetrator was successfully retrieved from a forensic process carried out by investigators, which later the digital evidence will be used as supporting evidence in the court process by adding other evidence findings.

2.2.5 The Results

After testing with various forensic tools, a comparison of the results of digital evidence can be obtained which can be seen in Table 3.

Table 3 Digital Evidence Finding Comparison

Information	Tools		
	MOBILedit Forensic Express	SQLite Studio	Beekeeper Studio
Message Conversation	✓	✓	✓
Time of Messages sent and received	✓	✗	✗
User Information	✓	✗	✗
Smartphone Contact	✓	✓	✓

From Table 3 above, the comparison table aims to see the final results obtained from the research process using multiple tools and differences in smartphone evidence results perpetrator. Basically, the result of some forensic tools used is a successful MOBILedit Forensic Express tool generate conversation evidence, location, time, user info, contacts, and pictures. SQLite Studio tool got proof of conversation that has been deleted but can't restore sent images, as well as Beekeeper Studio tool which succeeded in producing evidence of conversation but could not return the images sent which are suspected as evidence of a criminal act.

3. CONCLUSION

The digital forensic process carried out on the WhatsApp mobile-based online prostitution service has succeeded in obtaining digital evidence in the form of text conversations between the perpetrators and prostitution customers that were deleted on the Smartphone using the MOBILedit Forensic Express, SQLite Studio, and Beekeeper Studio tools. The process of finding evidence in research carried out refers to the NIST (National Institute Standards and Technology) stage with four stages in it, namely collection, examination, analysis, and reporting. Proof obtained using three forensic tools and obtained different results. Smartphones with rooting get complete digital proof results. Based on the percentage index measurement the number of each tool in the process of finding evidence, the conversation data gets 100% percentage, detail time and date messages were sent and received by 33%, smartphone contacts by 100%, and pictures by 33%. The digital evidence will be used as supporting evidence in the court process by adding other evidence findings.

4. REFERENCES

[1] AP Utami, "Mobile Forensics Analysis of Line Messenger on Illegal Drug Transaction Case using National Institute of Standard Technology (NIST) Method," vol. 183, no. 32, pp. 23–33, 2021.

[2] R. Fauzi, "Changes in Communication Culture for WhatsApp Users in the New Media Era," *JIKE : Jurnal Ilmu Komunikasi Efek*, vol. 1, no. 1, 2018.

[3] Statista Number of monthly active WhatsApp users worldwide from April 2013 to December 2017 (in millions)," www.statista.com, 2017. [Online]. Available: <https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/>.

[4] Sukardi. E, Pasaribu. D, Jennifer. G, and Kaliye "Eradicating Online Prostitution During the COVID-19 Pandemic Through Legal Dissemination Perspective of Dignified Justice Theory," *Jurnal Kajian Lemhannas RI*, vol 9, no. 1, p. 570, 2021

[5] M. Jannah, "Forensic Browser on Line Messenger Services for Handling Cyberfraud using National Institute of Standard Technology Method," vol. 183, no. 30, pp. 9–16, 2021.

[6] I. Anshori, K. E. Setya Putri, and U. Ghoni, "Analysis of Digital Evidence Facebook Messenger Applications on android smartphones Using the NIJ method," *IT Journal Research and Development*, vol. 5, no. 2, pp. 118–134, 2020.

[7] I. Riadi, and Sunardi. "Digital Forensic Analysis WhatsApp Application on Android-Based Smartphone," *SEMANTIKOM*, p. 95-98, 2017

[8] A. Yudhana, I. Riadi, and I. Anshori, "Digital Evidence Analysis of facebook messenger using the NIST method," *IT JOURNAL RESEARCH AND DEVELOPMENT*, vol. 3, no. 1, pp. 13–21, 2018.

[9] R. Y. Prasongko, A. Yudhana, and A. Fadhil. "Analisa Forensik Aplikasi Kakaotalk Menggunakan Metode National Institute Standard Technology," *SEMNASIF*, vol. 1, pp. 129–133, 2018.

[10] M. Unik and V. G. Larenda, "Android Investigation Analysis Forensic Short Message Service (SMS) On smartphones," *JOISIE (Journal Of Information Systems And Informatics Engineering)*, vol. 3, no. 1, p. 10, 2019.

[11] M. Fitriana, K. A. R. AR, and J. M. Marsya, "Application of the National Institute of Standards and Technology (NIST) method in Digital Forensic Analysis for Cyber Crime Handling," *Cyberspace: Journal of Information Technology Education*, vol. 4, no. 1, p. 29, 2020.

[12] N.A. Muhammad, *Digital Forensik: Practical Guide to Computer Investigation*. Jakarta: Salemba Infotek, 2012

[13] A. Prasad, and E. Studies, *Digital Forensics*. p. 182. 2010

[14] H. Nurhairani and I. Riadi, "Analysis Mobile Forensics on Twitter application using the National Institute of Justice (NIJ) method," *International Journal of Computer Applications*, vol. 177, no. 27, pp. 35–42, 2019.

[15] Tahiri, Soufiane. *Mastering mobile forensics*. Packt Publishing Ltd, 2016.

[16] Sudyana, Didik. *Learn to Recognize Digital Forensics*. Yogyakarta: Diandra, 2015

[17] S. M. Irwan, I. Riadi, and R. Umar, "Digital Forensic Analysis Beetalk Application for Cybercrime Handling Using the NIST Method," *SEMNASIF*, vol. 1, no. 1,

- 2018.
- [18] R. Jennifer, N. Kuntze, and C. Rudolph, "Security digital evidence," *Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, IEEE, 2010.
- [19] M. Jumiatmoko, "WhatsApp Messenger in a review of the benefits and etiquette," *Wahana Akademika: Jurnal Studi Islam dan Sosial*, vol. 3, no. 1, p. 51, 2016.
- [20] O. M. Bafadhal, "Ritual Communication using the WhatsApp application: Study of News Consumption Through WhatsApp Groups," *Jurnal Komunikasi Indonesia*, vol. 6, no. 1, 2018.
- [21] A. Wahid. *Crime Mayantara (Cyber crime)*. Bandung : Refika Aditama, 2005.
- [22] Rouse. M., (2018) *Cybercrime*. [Online]. Available: <https://www.coursehero.com/file/p70dkk8/Margaret-Rouse-Cybercrime-httpssearchsecuritytechtaragetcomdefinitioncybercrime/>
- [23] I. A. Anindia, and R. B. Sularto, "Criminal Law Policy in Efforts to Combat Prostitution as a Criminal Law Reform, " vol, no. 1, pp. 18-30, Jan. 2019.
- [24] Astuti Laras, "Formulation Policy on Cyber Sex Conducted by Children in a Restorative Justice Perspective," thesis, Yogyakarta, 2015.
- [25] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," 2006.
- [26] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, no. 3, p. 949, 2018.