Digital Forensic Analysis on Mobile-based Facebook Messenger services using National institute of Standard Technology Method

Dian Pertiwi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
This study uses research objects obtained from the website decision3.mahkamahagung.go.id with a chronology of events that occurred in the Facebook Messenger application, it was found that there were messages in the form of text and images containing the crime of extortion. This study conducted a data search process to obtain digital data from the mobile-based Facebook Messenger application. The process of collecting data from Facebook Messenger uses the National Institute of Standards Technology (NIST) method. The data collection process (Collection) begins with collecting data from the source used for extortion, namely from the perpetrator's smartphone. second, examination of evidence, third, after digital evidence is obtained, analysis is carried out, and finally the process of making reports based on analysis (reporting). This study aims to digital data on the Facebook messenger application using qualitative data. The results of the evidence were found in the form of text messages and pictures, as well as information on when to access Facebook messenger on a smartphone. The evidence produced uses several tools, namely MOBILedit Forensic Expressand Systools SQLite Viewer.

Keywords
Facebook Messenger, Cyber, Smartphone, NIST

1. INTRODUCTION
The rapid development of technology and information is felt in people's lives. As a result of the rapid and rapid development of technology and information, sooner or later it will change the behavior of society and human civilization globally because information technology makes the world borderless. It also spurred the emergence of new modes and crimes through information technology, one of which was social media. Social media that is often used is website-based technology that can change communication into an interactive dialogue. Some examples of social media that are widely used are YouTube, Facebook, Facebook Messenger, Blogs, Twitter, WhatsApp, and others.The Facebook Messenger application is one of the popular social media applications often used by mobile users, based on research results from napoleoncat.com.TheFacebook Messenger application certainly brings positive and negative impacts, one of the negative impacts is that some people who use Facebook Messenger have the intention to commit digital crimes.[1] Cybercrime is a technological crime committed by irresponsible parties to harm others.

Extortion is a threat to seek profit for himself and others. In the case of blackmail with threats of sharing private videos or photos, it is believed that there are many cases. Another extortion mode with the threat of sharing private videos or photos is also found in several cases of theft by hacking someone's social network account or email where sometimes the perpetrator finds videos or photos of victims stored on social networking profiles or e-mails. -letter. letter. the perpetrator blackmailed the account owner by threatening to distribute private videos or photos. Based on this, the data that will be sought in this study is digital data from the Facebook Messenger application that is used for extortion. The data search process was carried out using the National Institute of Standards and Standards method. Technology (NIST) tools MOBILeditForensic Express and Systools SQLite Viewer. Based on this background, the title of this research is "Digital Forensic Analysis on Mobile-based Facebook Messenger services using the National Institute and Standard Technology method".

1.1 Research Literature
1.1.1Previous Study
This previous study conducted a study entitled "Analysis of Skype Digital Evidence Recovery based on Android Smartphones Using the NIST Framework". The results of this study on the Oxygen tool cannot restore deleted data and the percentage of success using Belkasoft is 26%, the results of data recovery using the manual deletion method are 63% success using Oxygen and 44% of Belkasoft. While manual deletion of Oxygen is 61% Oxygen cannot restore data.[2]

Previous research conducted a study entitled "Forensic Analysis to detect the authenticity of digital ideals using the NIST method". The forensic tools used succeeded in helping to amaze the video file, especially to reveal the details of the filled file with hash valuesand metadata and reveal more clearly the real digital evidence which was analyzed by activating forensic tools in Video Cleaner to identify any changes with the frame method. 3].

This previous study conducted a study entitled "Facebook Lite Social Media Analysis with Forensic tools using the NIST

Method". Based on the results of the research process carried out, the results of the scenario using the Galaxy J2 Android Smartphone, by rooting, and installing the Facebook Lite application, making posts, and carrying out the investigation process using a forensic tool called MOBILedit Forensic, then analyzing using tools forensics and get the results of the

analysis that will become digital evidence.Theresults obtained in the use of the following forensic tools are Account ID, Image, Audio, Video using a National Institute Of Standards Technology (NIST) method.[4]

This previous study conducted a study entitled "NIST Method for Forensic Analysis of Digital Evidence on Android Devices" in its research to find digital evidence in the form of contact data, call logs, and messages that have been deleted on the Samsung Galaxy J1 Ace smartphone.Wondershare only reaches 30%, while the results of recovery with Oxygen forensics reach 73% of deleted data that can be restored. Thus, the data recovered from digital evidence with the Oxygen tool is highly recommended as evidence in proving criminal cases in court.[5]

This previous study conducted a study entitled "Acquisition of Digital Evidence for Viber Applications Using the National Institute of Standards Technology (NIST) Method".This study conducted data in the form of conversation messages that had been deleted by the perpetrators along with their accounts and call history.[6]

1.1.2Digital Forensic

Digital forensics is a scientific method that studies how to maintain, collect, validate, analyze, interpret, document, and present digital evidence from digital sources to facilitate the reconstruction of criminal events or help to anticipate actions that are proven to violate predetermined procedures[7]. Digital forensics has four stages, namely Digital Evidence Identification, Digital Evidence Storage, Digital Evidence Analysis, and Presentation[8].

1.1.3Forensic Mobile

Mobile Forensics is a branch of digital forensics which is concerned with the recovery of digital evidence or data from mobile devices under forensic sound conditions. The phrase cellular device usually refers to a cell phone, but can also refer to a digital device that has both internal memory and communication capabilities.[9]

1.1.4Digital Proof

Digital evidence can be in the form of data files, history, or logs. Digital evidence is the most important thing in a computer crime case because the criminal activity carried out is most likely recorded by the computer system on the computer's main storage media. Digital evidence can be known and seen at the time a crime is committed or after a crime has occurred[1]. Digital Evidence in question can be in the form of E-mail, word processor archives, spreadsheets, source code from applications, images, web browsers, bookmarks, cookies, and calendars [10].

1.1.5Smartphone

Smartphones in general have the advantage of accessing educational information, so many use them as a means to find the information they need [11]. Smartphone technology is getting more and more popular every year. One of the technologies with the largest number of users is an Android-based smartphone as the operating system [12]. Smartphones can be used as a learning tool where through a smartphone someone can learn new things through the content or messages that are distributed. In addition, smartphones are also used by a handful of people as lifestyle icons [13].

1.1.6Media Social

Social media is about being ordinary people who share ideas, work together, and collaborate to create creations, think, debate, find people who can be good friends, find partners, and build a community[14]. Social media is a medium that allows users to socialize and interact, share information and collaborate [15]. Social media is a tool or forum for providing news where the process of delivering this information can be done more practically, quickly, and is personal [16].

1.1.7Facebook Messenger

Facebook Messenger is a messaging service from Facebook that can be used for instant messaging which is specifically designed to communicate directly with fellow users. Facebook Messenger is a third-party application. With the three largest users, of course, it is also an opportunity to be used as a communication medium for negative purposes [17]. Facebook Messenger certainly brings positive and negative impacts, one of the negative effects is that some people who use Facebook Messenger commit digital crimes[1]

1.1.8Cybercrime

Cybercrime is a new type of crime that has emerged from globalization in this world. This crime is more dangerous than other crimes because its impact can cause a world war. It is undeniable that today's crime is growing as time goes by until now, there are many cases of this crime. All countries are competing to advance their technology for positive things, but many people misuse it for negative actions.[18] Based on the motive of its activities, cybercrime can be classified as Cybercrime as a pure crime, Cybercrime as a gray crime, Cybercrime that attacks individuals, Cybercrime that attacks copyright/property rights, and Cybercrime that attacks the government[19]. Crime cases in digital forensics are very vulnerable in any application, as long as the application provides features to send messages, pictures, and videos.[20]

1.1.9National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST) is the body responsible for developing standards, guidelines, and minimum requirements to provide sufficient information security for all assets and parties who have competence in the field of digital forensics [21]. NIST makes a method that has four stages in resolving and investigating Cyber Crime cases, the Collection, Examination, and Analysis stage, and the last one is Reporting [22].

The stages of the NIST method are as follows:

Figure 1. Stages of NIST Method

1.1.9.1 Collection

Collection The collection process is carried out for the identification, labeling, recording, and retrieval of data from relevant data sources by following procedures for maintaining data integrity.

1.1.9.2 Examination

The examination process is carried out for processing forensically collected data using a combination of various scenarios, both automatic and manual, as well as assessing and releasing data as needed while maintaining data integrity.

1.1.9.3 Analysis

The analysis process is carried out to examine the results of the examination process using technically and legally justified methods to obtain information that can be used to answer questions that are the impetus for conducting the examination.

1.1.9.4 Reporting

Reporting the results of the analysis which includes a description of the actions taken regarding the selected tools and procedures, determining other actions that need to be carried out eg carrying out forensic examinations of additional data sources, securing identified loopholes, or improving existing security controls and providing recommendations for improving policies, procedures, tools and other aspects of the forensic process. The results obtained will be presented in the form of percentages and written reports for documentation purposes. [23]

1.1.10 Digital Data

Digital data is defined as storing complex video, text, or audio information on a binary character or binary system. The data obtained is processed in digital form in the form of voice, video, or other binary data, so that it can be done on a computational program and stored in digital data [24]. digitization is a process of transformation into a format that can be read by a computer.[25]

2. METHODOLOGY

2.1 Research Scenario

This case simulation aims to provide an overview of the data search process carried out based on the crime of extortion in the Facebook Messenger application used in this study.

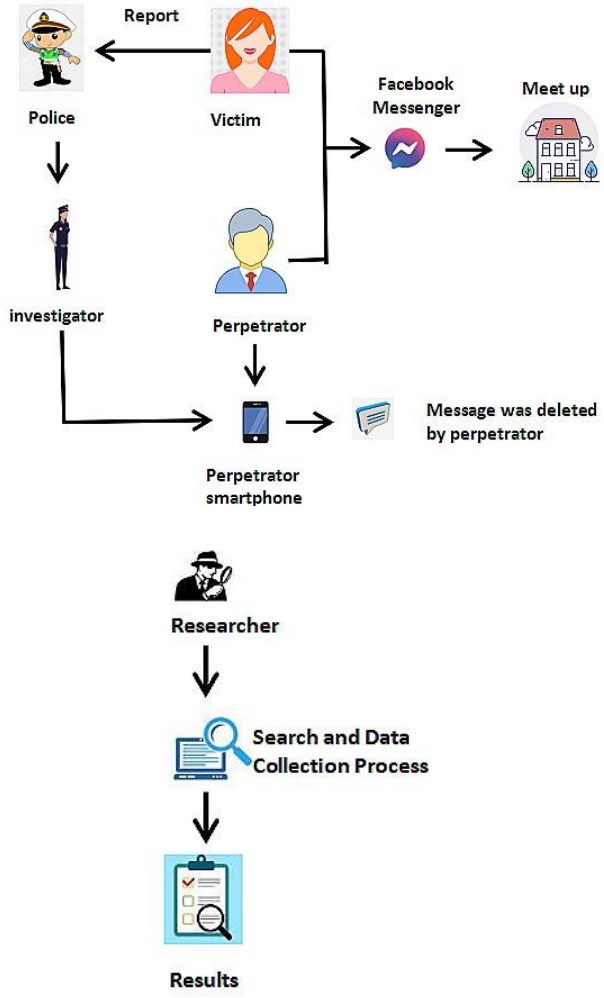


Figure 2.The flow of the Case Scenario on Facebook Messenger

In Figure 2, a case simulation begins with when the perpetrator offers a job through the Facebook messenger application, the job offered by the defendant is VCS (Video Call Sex) with a salary of 1,000,000 / VCS. Then when the victim is interested in the job following the mutual agreement, the perpetrator does things that make the victim feel aggrieved, namely when they do VCS (Video Call Sex) the perpetrator intentionally screenshots the image when the victim is not wearing clothes and uses the image as blackmail so that the victim follow whatever is ordered by the perpetrator. the victim reported to the authorities incident then the authorities carried out the investigation process and secured a smartphone belonging to the perpetrator. However, the perpetrator has deleted the message in the form of text and

images. The perpetrator's Facebook messenger account was then carried out a data search process related to the extortion case.

2.2 Research Stages

The research stage is a process by researchers searching for a study. The steps that will be used in this study using the National Institute of Standard and Technology (NIST) method have four stages, namely Collection, Examination, and Analysis, and the last is the Reporting process on a research object.

2.2.1Collection

The data collection stage is the initial stage carried out to collect data and look for data from digital sources. The data collection process is carried out via the perpetrator's smartphone which will be used by the Odin, SuperSU, and MOBILedit software. In obtaining digital data from the smartphone, a USB cable is needed as a liaison between the smartphone and the laptop which aims to obtain or collect digital data in the form of imaging files on the smartphone. The following are tools used by researchers can be seen in table 1.

Table 1. Evidence Found at the Crime Scene

No	Tool's name	Picture	Description
1	Smartphone		The Samsung Grand Prime brand is rooted, turned on, and connected to the internet.
2	USB Cable		The data cable used to connect to the smartphone

2.2.2Examination

At this stage the forensic investigation process will be carried out where the process of retrieving data or information contained on the perpetrator's smartphone, the data retrieval process is carried out using MOBILedit Forensic Express.

2.2.2.1 MOBILedit

The initial stage is using the MOBILedit Forensic Express tool to search for digital data as evidence on the perpetrator's smartphone. When opening the MOBILedit Forensic Express tool, make sure the smartphone is rooted first, then it must be connected to a laptop that has the MOBILedit tools in it. When the tool is run, make sure to see the results of extracting the data you are looking for, namely conversation messages and images contained in the Facebook Messenger application in the form of pdf files.

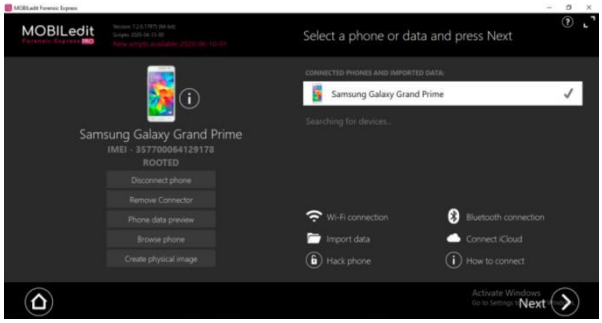


Figure 3. Acquisition of MOBILedit Forensic Express

Figure 3 shows the initial process which will carry out the acquisition on the perpetrator's smartphone using the MOBILedit Forensic Express tool where the data obtained will be continued using the Systools SQLite Viewer tool.

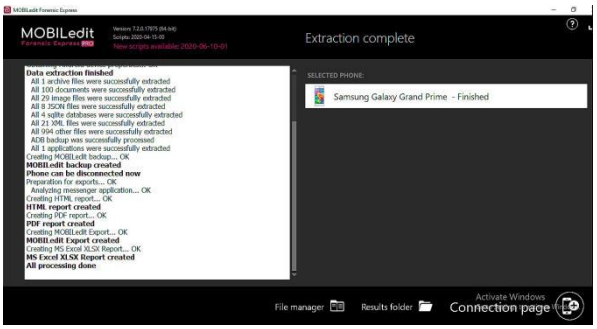


Figure 4.Data Acquisition Results

After the data extraction process is complete, the report file will be saved automatically. The results of the data extract can be seen in the folder"Samsung Galaxy Grand Prime (2021-12-26 02h31m55s)"

Figure 5. Digital Data Extraction Results Folder

The results of the digital data extraction process contain several folders and files, namely backup file folders, Html folders, MOBILedit export folders, PDF folders, Txt files, XML files, CFG files, HTML files, MS Excel worksheets, PDF files.

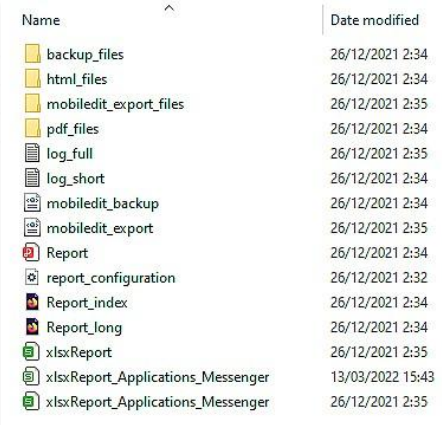


Figure 6. Contents of the Digital Data Extraction Result Folder

2.2.3Analysis

At this stage of analysis, the data obtained using the MOBILedit tool in The inspection stage is useful to ensure that the digital data that has been obtained is by the required results.

2.2.3.1 Analysis tools MOBILedit

The result of extracting data using the MOBILedit tool is a pdf file, where this file contains text message conversations and pictures between the victim and the perpetrator that can be used as evidence.

Figure 7. *Initial View of the Report.pdf File*

In Figure 8 the conversation between the perpetrator and the victim is a display of the conversation that has been successfully retrieved or recovered. The data obtained are user names, conversation times, and messages sent and received.

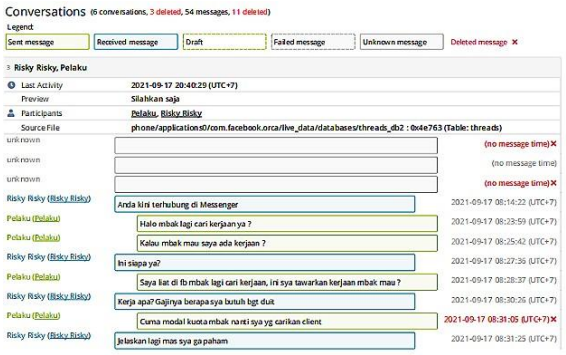


Figure 8.*Conversation Perpetrator and Victim*

Figure 9 is a view of the conversations that have been successfully retrieved or restored. The data obtained are user names, conversation times, and messages sent and received.

Figure 9. Conversation Messages of Perpetrators and Victims

Other data obtained are image files that can help strengthen that the perpetrators committed a crime as shown in Figure 10

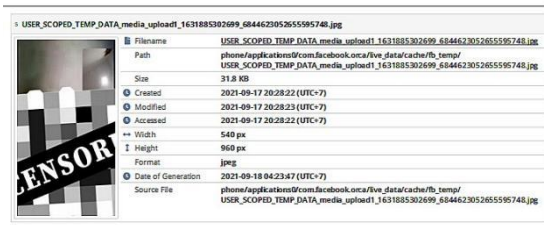


Figure 10. Image File View

2.2.3.1 Analysis tools Systools SQLite Viewer

In the data search process using the SysTools SQLite Viewer tool to get the data in the perpetrator's smartphone database. the first step is to open the SysTools SQLite Viewer tool, then click "Add File", in the Add File view to search for the database file then click "Add File" and select "messenger" to display message data in the form of text.

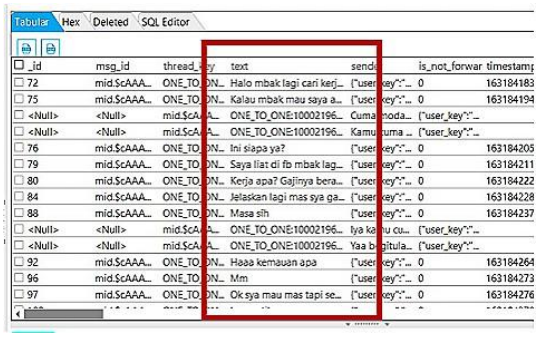


Figure 11.Messenger Table View

In Figure 11 is a view of the proof of the message in the form of a conversation on the messenger from the SysTools SQLite Viewer tool on the "messenger" database table. The evidence is the conversation of the extortionist on the perpetrator's smartphone which can be seen in the Text column.

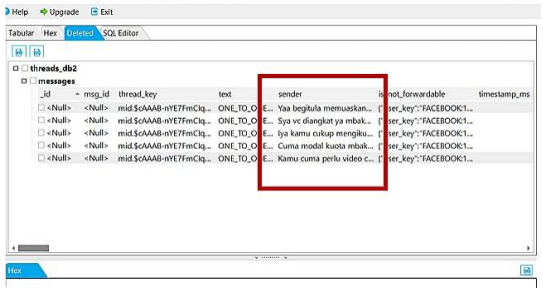


Figure 12.Display of Deleted Messages

Figure 12 message data in the form of text that has been deleted. then display the user table, select the "thread_user" menu, it will immediately display the table as shown in Figure 13.

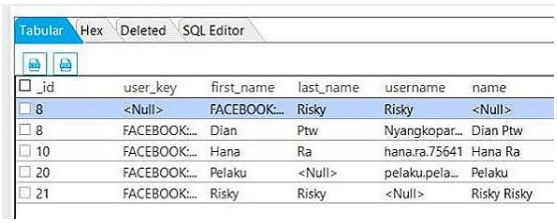


Figure 13.User Table Result Display

In Figure 13, the user table display has five users in the table. From the data search results using the SysTools SQLite Viewer tool, only conversations were found, while data in the form of images could not be obtained.

2.2.4Report

The results of the data search using the MOBILedit Forensic Express tools. These results include an overview of the data search process and the results of the data obtained. The software studied through the data search process in this study is the Facebook Messenger application that runs on a smartphone. Data was taken and analyzed. The results of the data obtained from the data search process are as follows:

Table 2. The Findings of Evidence

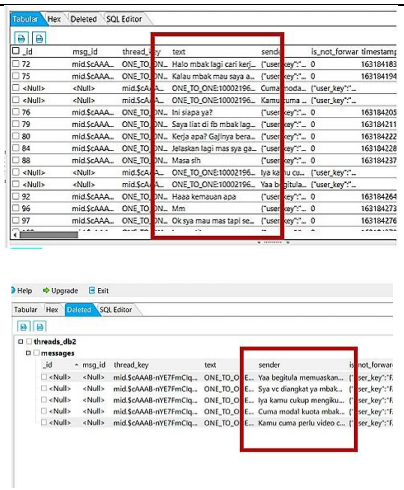
No	*Tools used*	Found data
1	MOBILedit Forensic Express	
2	Systools SQLite Viewer	

Table2 displays the final results obtained from the data search process on the mobile-based Facebook Messenger application that uses several tools to obtain data in the form of text messages between the perpetrator and the victim and pictures taken by the perpetrators, Facebook messenger account profiles, as well as information on accessing Facebook Messenger on smartphones.

2.2.5.Results

After testing with various forensic tools, it can beobtained a comparison of the results of digital evidence can be seenin Table 3

Table 3. Digital Evidence Finding Comparisonr

No	Data that Found	MOBILedit	Systools SQLite Viewer
1	Message Conversation	√	√
2	figure	√	-
3	Message Sent and Received Time	√	-
4	Account/Messenger ID	√	√

Table 3 shows the results of the data obtained from the analysis of the Facebook Messenger application using the MOBILedit Forensic Express tools and Systools SQLite Viewer tools. MOBILedit tools get digital data in the form of conversation messages that have been deleted or not deleted, pictures, Facebook messenger account/ID, time to receive and send messages, on Systools SQLite Viewer gets conversation message data and does not get pictures.

3. CONCLUSIONS

The forensic research process carried out on the mobile-based Facebook Messenger service with extortion cases has succeeded in obtaining digital evidence. Based on the search process or digital evidence carried out using the National Institute of Standards and Technology (NIST) method using four stages, namely collection, examination, analysis, and reporting. digital data search results as evidence using several tools, namely MOBILedit Forensic Express and Systools SQLite Viewer. The evidence obtained using two forensic tools has different results. Based on the measurement of the percentage index in the MOBILedit Forensic Express tools, the evidence found is that conversation messages get a percentage of 100%, images get a percentage of 50%, account information is 30%, and time and date of access are 70%, while the index measurement of the number of presentations is in the Systools SQLite Viewer tool. What was found was 100% conversational messages. Such evidence can be used in court as supporting evidence.

4. REFERENCES

[1] Yudhana, A., Riadi, I., & Anshori, I.2018. Facebook Messenger Digital Evidence Analysis Using the NistMethod. IT Journal Research and Development, 3(1),13-21.

[2] Yudhana, A., Fadlil, A., & Setyawan, M. R.2020. Analysis of Skype Digital Evidence Recovery based on Android Smartphones Using the NIST Framework. Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 4(4),682-690.

[3] Khairunnisak, K., Ashari, H., & Kuncoro, A. P. (2020). Forensic Analysis To Detect Authenticity Of Digital

Image Using The Nist Method. RESISTOR Journal (Computer System Engineering), *3*(2), 72-81.

[4] Bintang, R. A., Umar, R., & Yudhana, A. 2020. Facebook Lite Social Media Analysis with Forensic tools using the NIST Method. Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto), 21(2), 125-130.

[5] Umar, R., & Sahiruddin, S.2019. NIST Methods for Forensic Analysis of Digital Evidence On Android Devices.

[6] Syahib, M. I., Riadi, I., & Umar, R.2020. Digital Evidence Acquisition of Viber Application Using National Institute of Standards Technology (NIST) Method. J-SAKTI (Jurnal Sains Komputer dan Informatika), 4(1),170-178.

[7] Riadi, I., Umar, R., & Nasrulloh, I. M.2018. Digital Forensic Analysis On Frozen Solid State Drive With National Institute of Justice (NIJ) Method. Evo (Electronics, Informatics, and Vocational Education), 3(1), 70-82.

[8] Rosalina, V., & Saputra, D. H.2019. Development of a Digital Forensic Stage Model to Support Serang as a Free City.

[9] Putra, R. A., Fadlil, A., & Riadi, I.2017. Mobile Forensics on Android Based Smartwatch. Journal of Information Technology Engineering(JURTI), 1(1), 41-47.

[10] Prayudi, Yudi, And Dedy Setyo Afrianto. 2007."Anticipate Cybercrime Using Computer Techniques." 2007(Santi).

[11] Sahiruddin, S., Riyadi, I., & Sunardi, S.2017. Forensic Analysis of Recovery with Fingerprint Security on Android Smartphones. Proceedings of Sensei 2017,1(1).

[12] Imam Riadi, Rusydi Umar, and Arizona. (2016). Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method. International Journal of Computer Science and Information Security (IJCSIS), Vol. 15, No. 5, May 2017

[13] Daeng, I. T. M., Mewengkang, N. N., & Kalesaran, E. R. (2017). The use of smartphones in supporting lecture activities by students FISPOLUNSRAT Manado. Acta Diurna Komunikasi, 6(1).

[14] Strauss,A., & Corbin, J.2003.Qualitative Research. Yogyakarta: Pustaka Pelajar.

[15] Anggito, A., & Setiawan, J.2018. Qualitative research methodology. CV footsteps (footsteps Publisher).

[16] El, Oleh, Chris Natalia, S. I. Kom, And M. Si. 2016. "Teenagers, Social Media and Cyberbullying The Background of Teenagers as an Event to Connect with Social Media. People Tools To Do." 5.

[17] Ardiningtias, Syifa Riski, Study Program, Master of Informatics, Ahmad Dahlan University, Study Program, Electrical Engineering, And Ahmad Dahlan University. (2018). "Digital Investigations On Facebook Messenger." 19–26

[18] Wijaya, M. R., & Arifin, R.2020. Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime?. IJCLS (Indonesian Journal of Criminal Law Studies), 5(1), 63-74.

[19] Karen, E.2016. Cybercrime, Cyber Space, dan Cyber Law. Journal Times, 5(2), 35-42.

[20] Ambaranie. N.K.M.2017.This is the result of the work of the police in fighting cybercrime throughout.https://nasional.kompas.com/read/2017/12/29/17233911/ini-hasil-kerja-polriperangikejahatan-siber-sepanjang-2017, Accessed 1 April 2022

[21] Nasirudin, N., Sunardi, S., & Riadi, I.2020. Forensic Analysis of Android Smartphones Using the NIST Method and the MOBILedit Forensic Express Tool. J. Inform. Univ. Pamulang, 5(1), 89.

[22] Fitriana, M., Khairan, A. R., & Marsya, J. M.2020. Application of National Institute Of Standards And Technology (NIST) Methods in Digital Forensic Analysis for Cyber.Cyberspace Handling: Jurnal Pendidikan Teknologi Informasi, 4(1), 29-39.

[23] Sahiruddin, S.2019. NIST Methods for Forensic Analysis of Digital Evidence On Devices.

[24] Andayani, S.(2017). Digital archive management and ERMS. Shaut Al-Maktabah: Library Journal, Archives, and Documentation, 9(2), 175-182.

[25] Kawamoto, K. 2003. Digital Journalism: Emerging Media and The Changing Horizons of Journalism.USA: Rowman & Littlefield Publishers, Inc.