2022 6th INTERNATIONAL CONFERENCE ON
ENGINEERING AND APPLIED TECHNOLOGY (ICEAT)

CERTIFICATE

CERTIFIED THAT

Imam Riadi, Anton Yudhana, Galih Pramuja Inngam Fanani

BEST ARTICLE

In The 2022 6th International Conference on Engineering and Applied Technology (ICEAT)
held on October 19th, 2022 in Prapat, North Sumatra, Indonesia

AST-PTM Chairman

Ir. Teguh Marhendi, S.T., M.T., ASEAN.Eng., IPM

General Chair ICEAT 2022

Aster Rahayu, S.Si., M.Si., Ph.D.

Organized by : Hosted by : Jointly organized with : Supported by :

Mobile Forensic on MiChat Messenger Services using IDFIF V2 Framework

Author's Imam Riadi[1, a)], Anton Yudhana[2, b)], Galih Pramuja Inngam Fanani[3, c)]

[1]*Department of Information System, Universitas Ahmad Dahlan, 55191 Bantul, Yogyakarta, Indonesia.*
[2]*Department of Electrical Engineering, Universitas Ahmad Dahlan, 55191 Bantul, Yogyakarta, Indonesia.*
[3]*Department of Informatics, Universitas Ahmad Dahlan, 55164 Yogyakarta, Yogyakarta, Indonesia.*

[a)] Corresponding author: *imam.riadi@is.uad.ac.id*
[b)] *eyudhana@ee.uad.ac.id*
[c)]*galih2008048035@webmail.uad.ac.id*

Abstract. The rapid development of technology can cause problems for technology users themselves. One of the problems with technology like MiChat is that it is used as a means of communication to commit crimes. Examples of these problems include rampant online prostitution, fraud, online gambling and selling illegal drugs. Smartphones used in crimes can be taken by law enforcement officials as evidence. Valid evidence needs to be investigated using an approach to processing digital evidence called digital forensics. Integrated Digital Forensic Investigation Framework Version 2 (IDFIF v2) is one of the methods applied to investigate smartphones. The IDFIF v2 framework is the latest framework developed specifically for use in smartphone research. This research has several general stages: preparation, incident response, laboratory process, and presentation. The final result of this study is to report the results of database searches on smartphones and analyze smartphone evidence.

INTRODUCTION

Mobile devices are developing very rapidly along with technological developments [1]. One form of technology whose development can be directly enjoyed and applied in everyday life is the mobile phone (smartphone). Smartphone devices have the same functions as computers [2]. Android-based smartphones are one of the most popular types of smartphones and have many users [3]. Those who use it to access social media. The number of social media users in Indonesia has experienced rapid growth, reaching 191 million active users in January 2022 [4]. Figure 1 shows social media growth figures for Indonesia's active users.

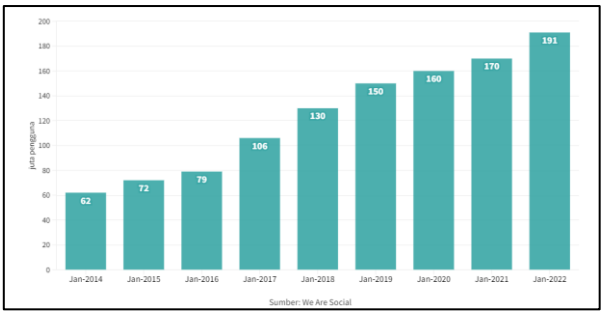


FIGURE 1. Social media growth statistics for active users in Indonesia in 2022.

The population of smartphone users in Indonesia is set to reach 370.1 million in 2022. Technological developments not only have a positive impact but also have a negative side. One of the negative impacts in question is when smartphones are used for unlawful acts involving social media platforms such as WhatsApp, LINE, Telegram,

and Signal [5, 6]. One application that is very popular in Indonesia with 50 million downloads on Google Play is MiChat [7]. MiChat functionally helps communicate among users, such as sharing media or chatting, but in Indonesia it is often associated with cybercrime [8], [11]. Such as pornography crimes, drug trafficking, online fraud, and others [10], [11], [12]. Table 1 shows some of the official news from the Republic of Indonesia police covering cases of misuse of the MiChat application.

TABLE 1. MiChat application cases in Indonesia.

No.	Year	Case
1.	2022	Dissemination of identity and immoral documents via MiChat in West Sumatra
2.	2021	Drug trafficking via MiChat App
3.	2020	Online fraud via MiChat in Samarinda
4.	2019	Human trafficking via MiChat in North Sulawesi
5.	2018	Murder of Sisca Icun Sulastri by Hidayat who met via MiChat in South Jakarta in Cimahi

This is a challenge for information technology forensics and law enforcement to investigate suspects in a crime case because the digital evidence that will be used as evidence has been deleted by the perpetrator. This digital evidence is in the form of data on smartphones, such as contact data, call logs, messages, videos, pictures, and documents that will be used as evidence of crimes in court [13], [14]. Digital Forensics is a scientific process or scientific endeavor based on the science of collecting, analyzing, and presenting evidence in court proceedings to assist in the disclosure of crimes through the disclosure of evidence authorized by laws and regulations [15], [16]. Mobile forensics is a branch of digital forensics that deals with recovering digital evidence and analyzing and presenting materialized entities from databases of smartphone devices.

IDFIF is the latest framework that has been developed to make it the standard investigative method for investigators, as IDFIF V2 has the flexibility to handle various types of digital evidence [17]. IDFIF V2 features a number of processes that have been adjusted after examining the investigation process and the procedure of collecting evidence collected at the crime scene [18],[19]. Live forensics is a forensic method used when the system is running [20]. Based on the problems described above, it is necessary to have forensic handling, especially mobile forensics, in helping to solve crime cases. In this research paper, the process of carrying out an investigation of digital evidence at a crime scene using a smartphone has four main stages, namely preparation (pre-process), TKP process (proactive process), examination of evidence in a digital forensic laboratory (reactive process), and reporting. The purpose of this research is to investigate the examination of digital evidence by implementing IDFIF V2 on the Android-based MiChat application on smartphones. In previous research, IDFIF V2 framework was only applied to SMS (Short Message Service).

METHODOLOGY

Research Methodology

The researcher uses a case study simulation to apply IDFIF V2 to analyze the MiChat application on a smartphone. This simulation was carried out with the aim of testing IDFIF V2 on the smartphone to find evidence of messages and media files used to commit criminal acts and turn the contents of the messages into evidence. In summary, the methods and stages of the research carried out can be described as in Figure. 2.

FIGURE 2. Methods and stages of research

Figure 2 is a method with several stages of research, namely:

1. The research problem is the initial stage in obtaining and determining the research topic for future investigation. It begins at this level by examining diverse occurrences, events, and information collected in various methods.
2. The literature review is expected to be able to unearth all information related to the problems to be studied and the object of research, as well as to provide a foundation for the direction of research to be carried out and to serve as a starting point for each researcher so that research can be used as a reference in the future.
3. Case Study is the process of implementing IDFIF Version 2 in the investigation process of the Android-based MiChat application, which has four main stages: preparation, crime scene processing, evidence examination in the digital forensics laboratory, and reporting on the results of the digital evidence examination. As seen in Figure 3.

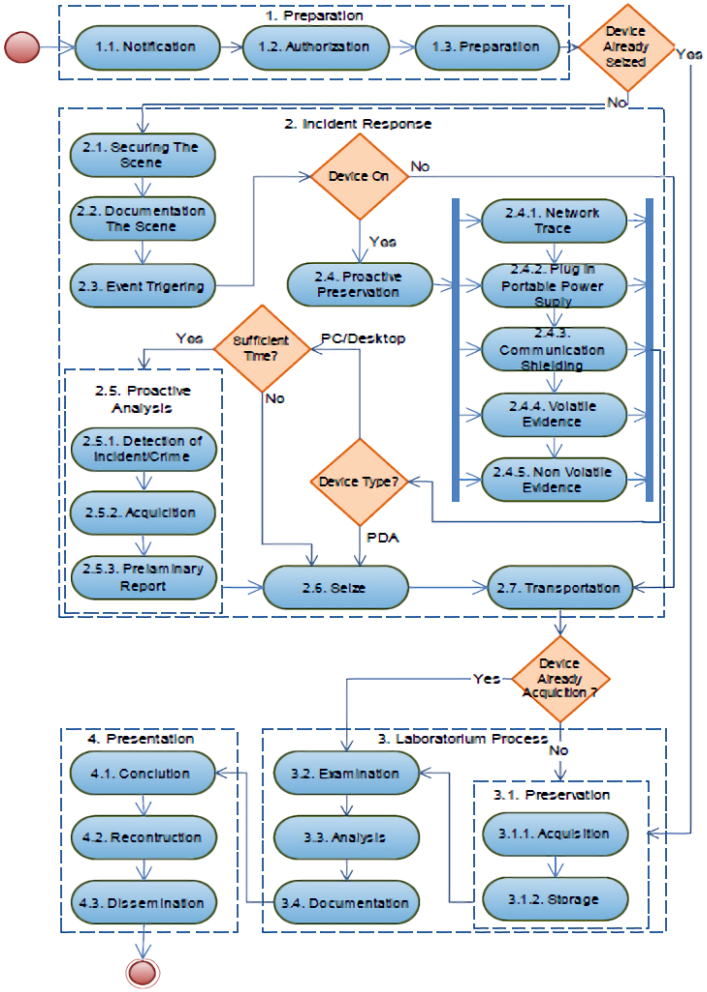


FIGURE 3. Model IDFIF version 2

4. The conclusion is the process of all the stages that have been carried out in the process of this research, from the process of handling physical evidence and obtaining digital items in the form of variables related to conversation time, the content of conversation messages, profiles of perpetrators and victims on MiChat messenger, and the data can be analyzed to determine whether it is consistent with the victim's reporting and whether there is a criminal act, until the final conclusion [17].

Research Case Scenario

The research was conducted by simulating drug trafficking crime cases. The simulation process is needed to assist researchers in determining the chronological process of the occurrence of the crime indication case, while the scenario can be seen in Figure. 4.

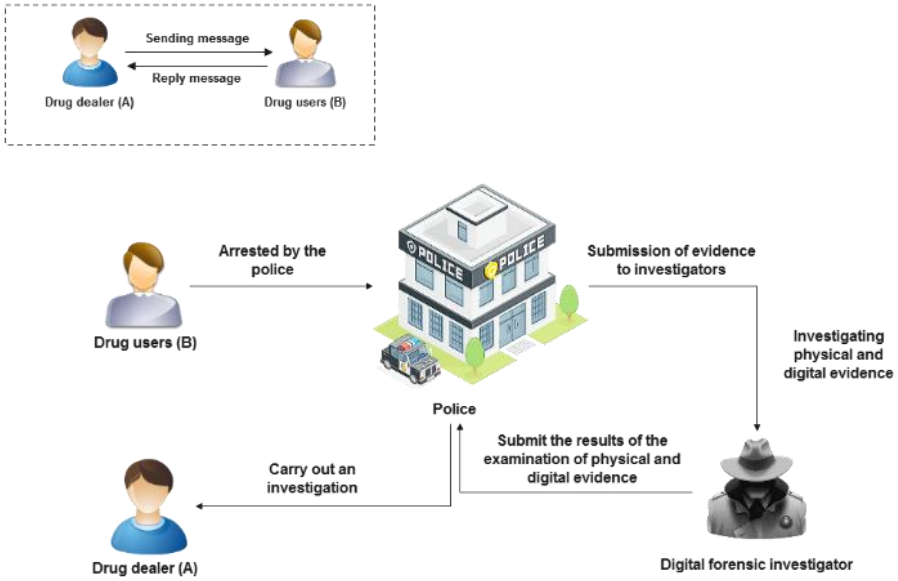


FIGURE 4. Drug trafficking case scenario process

Based on the case simulation in Figure. 2 there are two users who use the MiChat application to communicate, namely user A (Message Sender) and user B (Message Receiver). Through smartphone devices, both have MiChat instant Messenger accounts. From accounts owned by users, they are used to communicate with each other by buying and selling drugs, such as sending chat activities and media files. The authorities arrested user B for drug abuse. The next action by the authorities is to issue a search warrant to the user to secure the smartphone belonging to user B, which is used as a MiChat access medium to communicate with user A. This smartphone will be used as electronic evidence. For the next procedure, the investigator conducts an examination of user B's smartphone to find more information. After that, the evidence is handed over to the police for further arrest of user A.

RESULTS AND DISCUSSION

In dealing with this drug trafficking case, through the MiChat application on the smartphone, the investigator applied the IDFIF v2 handling procedure to resolve this. In general, The phases of the investigative process against digital evidence, whether computers or smartphones, include four major stages: preparation (pre-process), crime scene processing (proactive process), analysis of evidence in digital forensics laboratories (reactive process), and reporting on the outcomes of digital evidence assessment (post-process). The stages used in smartphone investigations can be seen in Figure. 5.

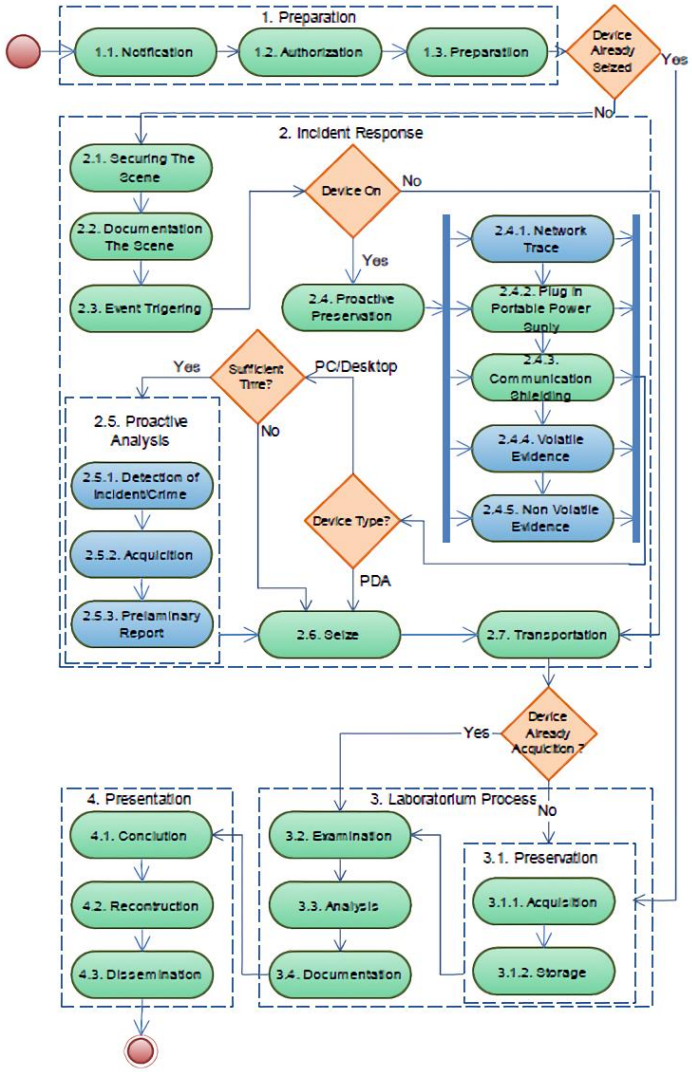


FIGURE 5. Stages of the IDFIF investigation process

Pre-Process Stages

Preprocessing is the first step in the analysis of digital evidence, particularly in smartphone investigations. Various preparations are undertaken in the investigative process at this stage, both for equipment and papers required. This level is subdivided into three sections, namely:

- Notification: Law enforcement agencies conduct investigations into drug trafficking reports through the MiChat application. Responsible law enforcement can be determined according to geographical criteria (location of the crime scene) or the nature of the crime. This notice is very important because the information collected here can determine the next steps of our investigation.
- Authorization: Law enforcers cooperate and oversee licensing procedures in obtaining access rights to telephone numbers during the process of tracking perpetrators (drug dealers). Then, after getting the perpetrator's smartphone number and ICCID number, the investigators conducted a track to find the location of the perpetrator's whereabouts.

- Preparation: Officers must gather all of the necessary equipment for the investigation, including personnel, investigation equipment, hardware, and software. The equipment used in the smartphone investigation process can be seen in Table 2.

TABEL 2. Smartphone investigation tool

Hardware and Software	Function
PC	Used to carry out the process of transferring digital data from smartphones to storage media for the analysis process
MOBILedit Forensic Express	Used for the physical imaging process or data backup of the MiChat application on a smartphone
Final Mobile Forensic	Used for further analysis of media files on extracted files.
USB Connector/ USB Dongle	Used to connect a smartphone to a computer to get full access to the smartphone
Portable Power Suplly	Is a device to increase smartphone battery power and is used to maintain the condition of the smartphone in an "on" condition.
Faraday Bag	A bag that is used to secure smartphones from data communication.
Digital camera	Used to take pictures at crime scenes as evidence that a crime has occurred
Storage Media	Used to store copies of digital evidence that has been obtained during an investigation.

Proactive Prosses

This is the first step in the investigation process. When the whereabouts of the drug dealers were identified, investigators rushed to their hiding places to carry out the process of arresting the perpetrators. The place used by the perpetrator to do that is called the TKP. The sub-stages are as follows:

- Securing the Scene: Investigators secure the actual crime scene by the officer who takes the first action at the crime scene so that the evidence is not lost, damaged, unchanged, or reduced, and does not differ in location, making it difficult or obscuring the processing of the crime scene.
- Event Triggering: After securing the crime scene, the investigator conducts an initial analysis process of an incident that occurred at the scene or crime scene so that the investigator can temporarily conclude the type of crime that was committed for further analysis in the digital foreground. The digital evidence discovered was one unit of the Asus Zenfone Z007 smartphone, which was used by the perpetrators to conduct drug buying and selling transactions.
- Proactive Preservation: Investigators secure smartphone evidence discovered at the crime scene so that the integrity of the data contained in the smartphone evidence is preserved until the analysis process is completed in the digital forensic laboratory.

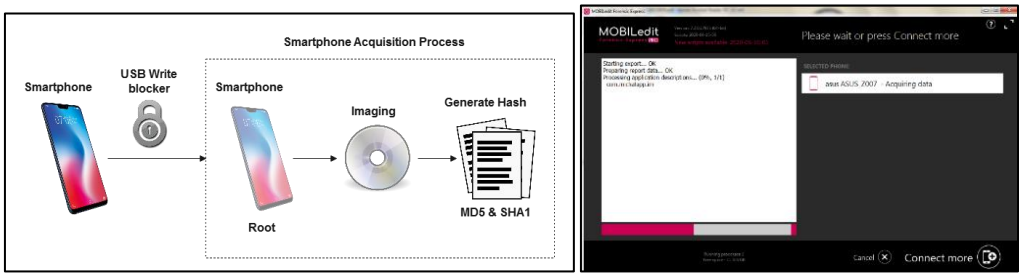
    1. Plug in portable power supply: In this case, the investigator secures the digital evidence to keep it alive by charging the smartphone evidence with a portable power source, considering that the condition of the smartphone battery is not always full, so it is necessary to carry out a charging procedure with the help of a portable power supply.
    2. Communication shielding: Investigators protect smartphone evidence by isolating data communications using a faraday bag so that there will be no data exchange or remote control processes through the available network.
- Seize: Investigators carry out the process of confiscation of smartphones found at the crime scene

- Transportation: Investigators carry out the process of transferring digital evidence in this case a smartphone device from the crime scene to the laboratory for further examination. In the process, the smartphone must be stored in a very safe condition so that when it arrives at the laboratory, it remains in good condition.

Reactive Process

This is a core stage of the smartphone investigation process. At this stage, the smartphone that has been obtained in the previous process is analyzed to obtain evidence related to the crime that occurred. This stage is divided into several stages, namely:

- Preservation: Investigators carry out the process of securing smartphones' evidence. The condition of the smartphone when in the acquisition process must be disconnected from existing data communications.
- Collection: Investigators took digital evidence from smartphone devices found at the crime scene. The acquisition process for smartphones uses the MOBILedit Forensic Express tools, namely performing physical imaging or backing up internal memory data, such as with the aim of finding digital evidence of drug trafficking cases on the MiChat application. It can be seen in Figure 7. is a physical imaging process using the MOBILedit Forensic Express tool.



(a) (b)

FIGURE 6. (a). Smartphone acquisition process flow, (b). Smartphone acquisition process using Mobiledit Forensic

The process of data acquisition on a smartphone takes no less than 1 hour. The results of the data acquisition can be seen in detail in the smartphone information contained in Table 3. After the acquisition process is complete, the next stage in preservation is storage. Specifications

TABLE 3. Detailed smartphone information

Specifications	Description
Manufacktur	Asus
Product	ASUS_Z007
Platform	Android 4.4.2
IMEI	357876069027680
SIM Card Country	Indonesia
ICCID	8962100759322537872
Total Storage	4.0 GB
Used Storage	2.6 GB

- Storage: The process of storing smartphone evidence in a predetermined location is carried out by investigators. The form and content of digital evidence must be stored in a sterile place. To really make sure there are no changes, this is very important because even a small change in digital evidence will change the results of the investigation. Digital evidence is by nature temporary (volatile), so its existence, if not careful, will be very easily damaged, lost, changed, or in an accident.
- Examinitation: Investigators carry out an examination process to reveal digital evidence, including those that may be hidden or lost on smartphone devices. The results are obtained through the application of the scientific method and should fully explain the content and state of the data. The process of examining digital evidence

must be carried out by a forensic expert, while the analysis process can be carried out by people other than forensic analysts, such as investigators or forensic examiners. Digital evidence digging digital evidence to find evidence of the MiChat application database on the perpetrator's smartphone device that has been extracted. The next step is to explore digital evidence on smartphones by finding the MiChat database in the acquisition data file that has been extracted and stored in storage C:\Users\GAL\Documents\MOBILedit Forensic Express\asus ASUS_Z007 (2022-01-23 01h06m38s)\ backup_files \ phone\ applications0\ com.MiChatapp.im\ backup\ db contains the encrypted MiChat database file as shown in Figure 8.

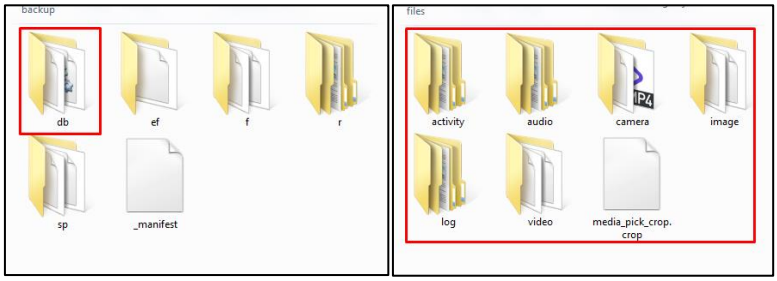


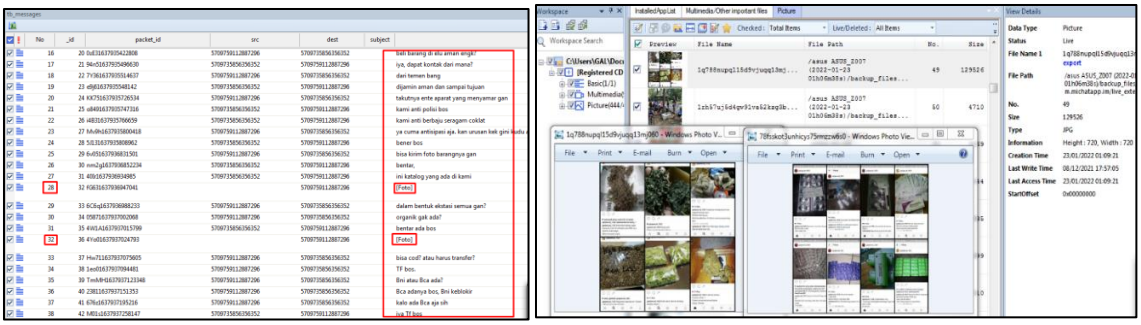
FIGURE 8. Extraction results of (a) database files chat, (b) database file media on the MiChat application

Figure 8 is a digital evidence file that was successfully extracted. It is a database file used to obtain conversation information and the perpetrator's phone number. Media files can also be used by investigators to provide supporting evidence for prosecuting the perpetrators of drug trafficking cases. The encrypted file from the database will be opened and can be exported to get information about the crime. The file storage location can be seen in Table 4.

TABLE 4. Location file backup laptop in storage

File Type	Storage Location	File Name
Db MiChat	C:\Users\GAL\Documents\MOBILedit Forensic Express\asus ASUS_Z007 (2022-01-23 01h06m38s)\backup_files\phone\applications0\com.MiChatapp.im\backup\db	5709735856356352social
Db Media MiChat	C:\Users\GAL\Documents\MOBILedit Forensic Express\asus ASUS_Z007 (2022-01-23 01h06m38s)\backup_files\phone\applications0\com.MiChatapp.im\live_external\files	Images Audio Video Cache

- Analysis: After conducting the examination process on the smartphone, the investigator conducted a study related to the drug trafficking case and the digital evidence obtained, then the investigator conducted an analysis of the database that had been collected to be able to detail the information on the evidence obtained using the Final Mobile Forensic tools, the first stage import database files on smartphone devices. During the examination and analysis process, the investigator conducts a technical review and compiles the relationship between the findings between the perpetrator and the smartphone obtained. In some cases it is sometimes necessary to collect physical and logical evidence in the form of data extraction, but in this case the evidence needed is the conversation between the perpetrator (drug dealer) and the buyer, the time of the conversation, and the identity of the perpetrator's profile located on the internal smartphone storage. The buyer asks the perpetrator if there are goods (drugs), then the perpetrator and the buyer plan a meeting somewhere to conduct a drug sale and purchase transaction. The message sent by the buyer to the perpetrator can be seen in Figure 9.



(a) (b)

FIGURE 9. (a). Evidence of Chat for drug transactions, (b). Photo evidence of drugs being traded by the perpetrators

On figure 9 (a). Evidence of conversations between drug dealers and buyers can be seen. In the picture above, the message is known as a private message type. It can also be seen that the message ID, buyer number, and message body can be customized. Conversations between drug dealers and buyers detected by Mobile Forensic Final Tools are a type of private message because they are only carried out by two people. The message ID numbers 28 and 32 show that the perpetrator (drug dealer) sent a picture message that was detected by the Final Mobile Forensic Tools with the name IMG-20211126-WA0001-1.jpg shown in Figure 9. (b).

- Documentation: After analyzing the discovered smartphones, the next step is to compile the findings from the analysis stage and submit them to the authorities. Findings are presented in a form that is easy to understand and supported by sufficient and acceptable evidence in the form of chain of custody and copies of data related to drug trafficking cases. Table 5. Information obtained during the investigation process with attached evidence.

TABLE 5. Information on investigation results of drug trafficking cases through MiChat communication media.

General Information Summary	
Information	**Description**
Evidance Number	1
Investigator	Galih Fanani
Case Name	Drug Trafficking
Device Name	ASUS_Z007
IMEI	357876069027680
Serial	8962100759322537872
Sofware Version	4.4.2
Digital Evidence	
Contact Drug Dealer	0895336753xxx
Contact Drug Users	0899917533xxx
Chat Conversation	File DB 5709735856356352social
Image files	File Image IMG-20211126-WA0001-1
Timestamp	23/01/2022 01:09:21

Post-Process

This is the closing stage of the investigation. This stage processes the evidence that has been used previously. This stage includes returning the evidence to its owner, storing the evidence in a safe place, and conducting a review of the investigation that has been carried out as an improvement for further investigations.

- Conclusion: The evidence and information discovered by the investigators are sufficient for the investigative team to charge suspects with drug trafficking and detain the perpetrators.
- Reconstruction: Furthermore, investigators must reconstruct based on the findings from the analysis that has been carried out so that the process of the perpetrator's activities can be known more clearly in carrying out the drug trafficking process.
- Socialization: The final step is to document the investigation process so that if other investigators come across a similar case, they can use this process as a reference in the smartphone investigation process.

.

CONCLUSION

MiChat is a popular messenger application in Indonesia for social networking where people can exchange personal information between users. This study uses the Integrated Digital Forensic Investigation Framework Version 2 which functions to find digital evidence in the form of a database derived from smartphone evidence. The process of physical imaging data on MiChat messenger is done using the MOBILedit express tool. The MiChat database found was then extracted using Final Mobile Forensic tools which produced information related to conversation times, user profiles, image files, telephone numbers and conversation content. The results of the evidence found are then used as case reports, to be used as evidence in court.

REFERENCES

[1] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile forensic tools evaluation for digital crime investigation," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, pp. 949–955, 2018, doi: 10.18517/ijaseit.8.3.3591.

[2] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic tools performance analysis on android-based blackberry messenger using NIST measurements," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 3991–4003, 2018, doi: 10.11591/ijece.v8i5.pp3991-4003.

[3] H. H. Lwin, W. P. Aung, and K. K. Lin, "Comparative Analysis of Android Mobile Forensics Tools," *2020 IEEE Conf. Comput. Appl. ICCA 2020*, 2020, doi: 10.1109/ICCA49400.2020.9022838.

[4] S. O'Dea, "Number of smartphone subscriptions worldwide from 2016 to 2027," *www.statista.com*, 2022. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ (accessed Jul. 07, 2022).

[5] I. Riadi, A. Fadlil, and A. Fauzan, "A study of mobile forensic tools evaluation on android-based LINE messenger," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 10, pp. 201–206, 2018, doi: 10.14569/IJACSA.2018.091024.

[6] A. N. Ichsan and I. Riadi, "Mobile Forensic on Android-based IMO Messenger Services using Digital Forensic Research Workshop (DFRWS) Method," *Int. J. Comput. Appl.*, vol. 174, no. 18, pp. 34–40, 2021, doi: 10.5120/ijca2021921076.

[7] G. Fanani, I. Riadi, and A. Yudhana, "MiChat Application Forensic Analysis Using Digital Forensics Research Workshop Method," vol. 6, no. 2, pp. 1263–1271, 2022, doi: 10.30865/mib.v6i2.3946.

[8] V. L. Schul'tz, V. V. Kul'ba, A. B. Shelkov, and L. V. Bogatyryova, "Scenario Analysis of Improving the Effectiveness of Cybercrime Investigation Management Problems," *IFAC-PapersOnLine*, vol. 54, no. 13, pp. 155–160, 2021, doi: 10.1016/j.ifacol.2021.10.437.

[9] K. D. O. Mahendra and I. K. Ari Mogi, "Digital Forensic Analysis Of MiChat Application On Android As Digital Proof In Handling Online Prostitution Cases," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 9, no. 3, p. 381, Feb. 2021, doi: 10.24843/JLK.2021.v09.i03.p09.

[10] V. A. Yuliani and I. Riadi, "Forensic Analysis WhatsApp Mobile Application On Android-Based Smartphones Using National Institute of Standard and Technology (NIST) Framework," *Int. J. Cyber-Security Digit. Forensics*, vol. 8, no. 3, pp. 223–231, 2019, doi: http://dx.doi.org/10.17781/P002615.

[11] C. Anglano, M. Canonico, and M. Guazzone, "Forensic analysis of the ChatSecure instant messaging application on android smartphones," *Digit. Investig.*, vol. 19, pp. 44–59, Dec. 2016, doi: 10.1016/j.diin.2016.10.001.

[12] A. Sanchez, N. Han, and P. Jones, "Mexico: Organized Crime and Drug Trafficking Organizations Related

papers T he St rat egic Implicat ions of t he Cárt el de Jalisco Nueva Generación," 2015. [Online]. Available: www.crs.gov
[13] N. Hamad and D. Eleyan, "Digital Forensics Tools Used in Cybercrime Investigation-Comparative Analysis," *J. Xi'an Univ. Archit. Technol.*, vol. xiv, no. May, pp. 113–127, 2022, doi: 10.37896/JXAT14.04/314909.
[14] A. Patel, D. P. Sharma, and P. D. Dholariya, "A Forensic Evidence Recovery from Android Device Applications," *Int. J. Sci. Res. Sci. Eng. Technol.*, vol. 3, no. 4, pp. 135–140, 2021, doi: 10.32628/ijsrset218321.
[15] S. H. Belshaw, "Next Generation of Evidence Collecting: The Need for Digital Forensics in Criminal Justice Education," *J. Cybersecurity Educ. Res. Pract.*, vol. 2019, no. 1, p. 3, 2019.
[16] B. Kumar Sharma, V. Yadav, M. Kaur Purba, Y. Sharma, V. Kumar, and P. Mehta, "Challenges, Tools, and Future of Mobile Phone Forensics," *J. Posit. Sch. Psychol.*, vol. 2022, no. 4, pp. 4463–4474, 2021, [Online]. Available: http://journalppw.com
[17] Ruuhwan, I. Riadi, and Y. Prayudi, "Application of Integrated Digital Forensic Investigation Framework v2 (IDFIF) in Smartphone Investigation Process," 2016. doi: http://dx.doi.org/10.26418/jp.v2i1.14369.
[18] B. Actoriano and I. Riadi, "Forensic Investigation on Whatsapp Web Using Framework Integrated Digital Forensic Investigation Framework Version 2," *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 4, pp. 410–419, 2018, [Online]. Available: https://www.researchgate.net/publication/327592240
[19] R. Dinnur Rahman and I. Riadi, "Framework Analysis of IDFIF V2 in WhatsApp InvestigationProcess on Android Smartphones," *Int. J. Cyber-Security Digit. Forensics*, vol. 8, no. 3, pp. 213–222, 2019, doi: 10.17781/p002610.
[20] M. S. Chang and C. P. Yen, "Forensic Analysis of Social Networks Based on Instagram," *Int. J. Netw. Secur.*, vol. 21, no. 5, p. 850, 2019, doi: 10.6633/IJNS.201909.