

Mobile Forensic MiChat Services for Handling Online Prostitution using National Institute of Justice Method

Adrian Hidayat Zain
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

The world's technological development is very fast, especially smartphones with a variety of functions and applications, including instant messaging like MiChat in Indonesia. MiChat offers features like "People Nearby", "Chat Trends", "Moments", and "Message Tree" for an interactive chat experience. However, these advances have also triggered negative impacts such as online prostitution. The research aims to find digital evidence of online prostitution in MiChat using the method of the National Institute of Justice (NIJ) which includes Identification, Collection, Examination, Analysis, and Reporting. The identification involves devices such as MOBILedit Forensics Express, Autopsy, and Systools SQLite Viewer. The results of this research found 1 image of transfer evidence, recovered 19 deleted conversation texts, and found 2 perpetrator contacts through user ID number analysis using Systools SQLite Viewer. It is hoped that in the future this research can be used as a reference for investigating online prostitution cases for other researchers in the future.

General Terms

Digital Forensics

Keywords

Mobile Forensics, MiChat, Online Prostitution, National Institute of Justice.

1. INTRODUCTION

The technological development of the world today is going very fast. One form of technology whose advances can be directly applied to everyday life is a handheld phone. (smartphone). Handheld phones today have many different functions and applications. One of the most commonly used applications is the instant messenger (IM) or instant messaging [1].

Instant Messaging allows you to send messages to each other quickly over the Internet. Based on research "Essential Digital Data For Every Country In The World" supported by Simon Kemp and our partners We Are Social and Hootsuite. There are 160 million active social media users in Indonesia, which is 59% of the total Indonesian population, and about 99% of active social network users use mobile phones [1].

One of the instant messaging services in Indonesia is MiChat. MiChat offers chat features like "People Nearby", "Chat Trends", "Moments", and "Message Tree" for a more interactive chat experience [2]. The MiChat feature is often used by people who are irresponsible for criminal activities such as online prostitution. People who abuse this app usually post the opening of the prostitution service and indicate the price of the service. One case of prostitution in Indonesia involved seven online prostitution prostitute who dragged several women who were allegedly commercial sex workers in

Surabaya and used the MiChat instant messaging app to sell themselves [3]. They use the "chatting with the nearest user" feature by uploading locations that can be connected to areas within a certain radius of distance, and once connected, users and prospective customers negotiate and make transactions with each other in the app.

The perpetrators often delete the message history to remove evidence of the transaction conversation, thus avoiding the legal trap and exacerbating online prostitution. Digital forensic analysis is needed to obtain data and collect valuable information deleted from the perpetrator's phone, such as conversation history and contacts, as evidence [4]. The research is expected to reduce the activity of online prostitution in the MiChat app. Mobile forensic methods use the National Institute of Justice (NIJ) standard with the software MOBILedit Forensic Express, Autopsy, and Systools SQLite Viewer. MOBILedit Forensics Express is used to scan mobile devices, while Autopsy and Systools SQLite viewer are used to analyze the scan results from MOBILedit Forensics Express.

2. RELATED WORKS

Herman, Anton Yudhana, Fitri Anggraini (2023) on "Acquisition of Android-based Tiktok Digital Evidence Using the Methods of the National Institute of Justice" discusses measures to acquire digital evidence on the TikTok application related to case pollution of good name and litigation. The research uses digital forensic methods based on the framework of the National Institute of Justice (NIJ), which consists of five stages: identification, collection, examination, analysis, and reporting. The researchers simulated scenarios of reputational pollution and threats on TikTok, including the uploading of blasphemous videos and the delivery of threat messages. The study aims to recover simulated data from smartphones in non-root and root conditions [5].

Syifa Riski Ardinintias, Sunardi, Herman (2021) on "Digital Investigation On Facebook Messenger Using the National Institute of Justice" aims to conduct a digital investigation with forensic tools MOBILedit Forensics and Wondershare Dr. Fone to obtain digital evidence from Facebook Messenger. Using the NIJ framework, the research focuses on pornography cases in Facebook Messenger on Android smartphones. Since the perpetrators often delete data to remove traces, the research is aimed at obtaining evidence such as pictures, videos, accounts, conversations, emails, time of occurrence, and voice messages that can be used in court [6].

Dina Yuliana, Trihastuti Yuniarti, Bitu Parga Zen (2023) on "Forensic Analysis Against Cyberbullying Cases on Instagram and WhatsApp Using the Methods of the National Institute of Justice" aims to analyze the cyber bullying cases using NIJ and three forensic applications: MOBILedit Forensic Express, Autopsy, and FTK Imager. The results showed almost all of the

scenario-appropriate data found through Autopsy and FTK Imager using a physical image from a MOBILedit extract on a rooted phone. FTK Imager requires knowledge of data location to facilitate search. MOBILedit did not find any deleted videos and files on Instagram, only storage files on WhatsApp. Autopsy is most effective in finding and reading almost all deleted data with cell phone notes in root condition [7].

Sunardi, Imam Riadi, Joko Triyanto (2021) on “Forensics Mobile Services WhatsApp on Smartwatch Using Methods of the National Institute of Justice” aims to analyze WhatsApp on Android-based smartwatches using the NIJ framework and the Wondershare Dr.Fone tool. This research includes stages of identification, research, collection, analysis, and reporting. The simulated case was a fraud in the employee selection test, with evidence of a smartwatch of the test participants. Potential evidence includes photos, videos, and documents. This research managed to collect 100% data such as photos, video, contacts, and documentation, but could not read chats, call history, or recover lost data [8].

Soni, Yulia Fatma, Rizki Anwar (2022) on “Acquisition of Digital Proof of BIP Instant Message Application Using the Method of the National Institute of Justice” aims to reveal deleted messages from BIP Messenger using the NIJ method. This research involves identification, collection, inspection, analysis, and reporting. Tools MOBILedit Forensic and Oxygen forensic SQLite Viewer are used. As a result, the NIJ method managed to identify evidence from BIP Messenger on an Android smartphone. All the tools were working fine, and deleted messages were successfully retrieved. This research is important for digital investigations and guidelines for law enforcement in identifying evidence from an instant messaging app on Android [9].

3. METHODOLOGY

The methodology in this research uses an approach designed to assist the process of settlement in Digital Forensic. This methodology aims to solve the problem of forensic investigation through structured stages, which can be used as a reference to uncover all digital evidence obtained.

3.1 Research Tools and Materials

When conducting the research, various software and hardware tools are employed to support the investigation. These tools are essential for ensuring accurate and thorough data collection and analysis. The selection of appropriate tools and materials is crucial for the success of the research. Here are the research tools and materials provided in Table 1 Software and Table 2 Hardware.

Table 1. Tools and Software Materials used in this research

Software	Spesification
MOBILedit Forensics Express	MOBILedit Forensic Express Pro 7.4.1.21057
Autopsy	for Windows 64-bit version 4.19.3
Systools SQLite Viewer	Systools SQLite Viewer v3.0 - FREEWARE
Operation System	Windows 11
MiChat	MiChat Mobile version 1.4.408

Table 2. Tools and Hardware Materials used in this research

Hardware	Spesification
Laptop	Lenovo Ideapad L340 Intel® Core™ i7-9750HF CPU @ 2.60GHz (12CPUs), Memory 16GB
Mobile Phone	Xiaomi Redmi Note 9, Memori 4GB
USB Connector Cable	USB Type-C

3.2 Research Phase

As for the stages of the method of the National Institute of Justice (NIJ). The stages in this research are implemented using a demonstrated method.

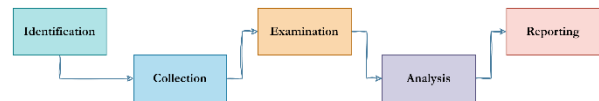


Figure 1: National Institute of Justice Method Scheme

Figure 1. provides a general overview of the NIJ Method consisting of the first stages of Identification, Collection, Examination, Analysis, and Reporting as the final stages, so it can be displayed as follows:

3.2.1 Identification

At the identification stage, data selection and sorting of digital crime evidence is carried out to support the investigation. This process involves labelling, identification, and recording to maintain the integrity and security of evidence. The relevant evidence is then taken for further proceedings [8].

3.2.2 Collection

At the collection stage, data is collected by searching, assembling, or making copies of items containing digital evidence. The primary purpose is to gather data from relevant sources while keeping the authenticity and uniqueness of digital evidence unchanged. [17].

3.2.3 Examination

At this stage of examination, there is a file testing phase in which files that have been obtained from the identification and clarification phase will be tested to obtain the desired information from the data that has been acquired [18].

3.2.4 Analysis

Phase analysis is a very important phase and should not be rushed, because this is where digital evidence must be found and revealed.

3.2.5 Reporting

The reporting stage covers the results of the investigation from the beginning to the end, including the evidence found, the methodology used, the conclusions of the case, and the metadata obtained during the research. [22].

3.3 Case Scenario

In the process of research has a scenario or simulation in the case of online prostitution on a mobile application in this case MiChat Mobile by conducting a message conversation (messages) which contains data and images between the perpetrators of the messenger found in the smartphone.

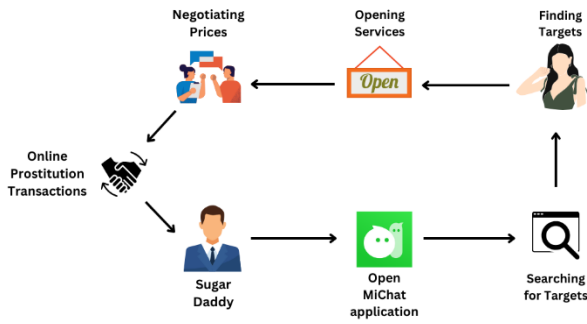


Figure 2: Case Scenario

Figure 2 shows an overview of the scenario or simulation that has been displayed and described in the review above then put a simulation illustration with the stages and courses of the illustration in the study as a whole where there are 3 stages in the simulation case illustration made in this case consists of Pre-incident, Incident, and Post-incident, and post-incidents, as follows:

3.3.1 Pre-Incident

The case began when the perpetrators of online prostitution, who claimed to be "sugar daddy," used the MiChat app with fake photos and profiles to attract vulnerable women or seek economic opportunities. The perpetrator sent a message to some women, offering money or material in exchange for sexual services. Negotiations are taking place between the perpetrator and the woman, accompanied by an exchange of serious evidence such as pictures of witnesses.

3.3.2 Incidents

Some women accepted the offender's offer and agreed to meet for prostitution, so the meeting was scheduled through the MiChat app. The offender, using fake photos and profiles, transferred money in exchange for agreed sexual services. The perpetrator's wife suspects her husband's strange movements and reports it to the authorities. To remove the trace, the perpetrators deleted the history of transaction messages on MiChat.

3.3.3 Post-incident

The cybercrime apparatus searched for evidence related to the case in accordance with a warrant, using forensic procedures and the framework of the National Institute of Justice. They're doing data recovery on the sugar daddy phone to return the prostitution conversation as evidence. During the process, the apparatusins the integrity and confidentiality of the evidence, ensuring that the evidence collected is robust for the development of the case and trial.

3.4 Research Process Flow

The course of the research process is a critical stage in the process of digital forensic investigation, often known as forensics imaging. This stage ensures the integrity and reliability of the collected data. Based on the study process, at this stage of data collection, the Core Acquisition Illustration is created. Here, the files that have been completed will be meticulously collected in full, ensuring that every piece of evidence is accounted for and preserved accurately for further analysis.

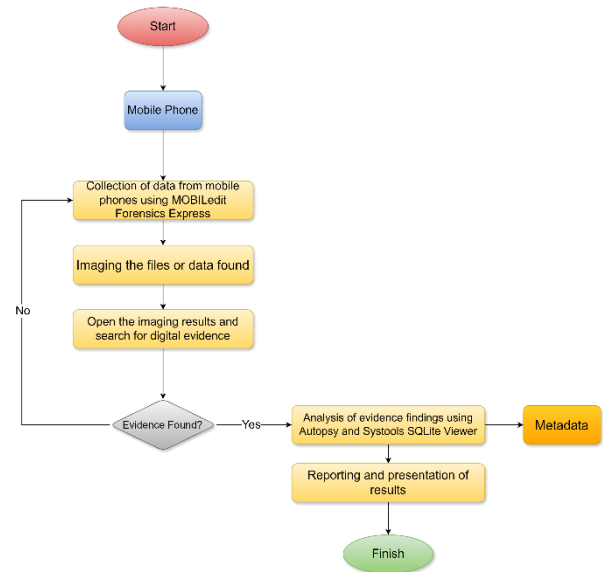


Figure 3: Research Process Flow

Figure 3. Gives a general overview of the research process that begins with starting after that will enter mobile phone then will continue to data identification then data collection with MOBILedit Forensic Express, data inspection and analysis with Autopsy and Systools SQLite Viewer and then drawn the last report until the process is completed.

4. RESULTS AND DISCUSSION

The research uses NIJ scientific methods for the maintenance, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence. NIJ methods ensure reliable and valid digital evidence, helping investigators solve similar crimes.

4.1 Data Collection Results

The research data was collected through a questionnaire in Google Form with 55 respondents. Selection of Google Forms facilitates access and increases participation. The results show MiChat is frequently used for online prostitution, strengthening the foundation and urgency of this mobile forensic research. This research is vital to uncover the misuse of MiChat for criminal purposes.

4.2 Implementation

The NIJ method, abbreviated for the National Institute of Justice, provides a standard and consistent forensic framework that is easy to use and easy to understand by technical and non-technical users. Based on the rules of digital forensics and the integrity of the authenticity of digital evidence, the forensic process follows the NIJ Forensic Method Procedure which consists of the following 5 stages:

4.2.1 Identification

The identification is an early stage in the search for digital evidence. At this stage, investigators prepare tools that will be used to assist the investigation. These tools are used because they have research-related functions and can find digital evidence. These tools consist of two types of hardware and software. Tools to be used can be seen in table 3.

Table 3. Preparation Tools

Tools Name	Type	Description
Mobile Phone	Hardware	Media used to retrieve data
Michat	Software	Object application for forensic activities
MOBILedit Forensics Express	Software	Tool for collect digital evidence by acquiring from applications that are being extracted on smartphones
Autopsy	Software	Tool used to analyze digital evidence files that have been collected with MOBILedit Forensics Express in particular files that cannot be opened directly
Systools SQLite Viewer	Software	Tools used to open and analyze the database of applications already collected with MOBILedit Forensics Express such as displaying the database structure, saved contacts, and chat text messages

4.2.2 Collection

The collection phase is a step to find and collect digital evidence that supports the disclosure of crime of prostitution through the MiChat application. Here is the evidence that was successfully seized by the authorities during the investigation process, the evidence obtained is a Xiaomi Redmi Note 9 smartphone.



Figure 4: Proof Item Xiaomi Redmi Note 9 Smartphone

Figure 4 Xiaomi Redmi Note 9 Smartphone with its specification system is important for forensic proceedings as it is used as evidence. To ensure that the process is running properly, it is necessary to know about the system and all specifications of Xiaomi redmi note 9 Smartphone that are evidence. Here are the specifications of the Xiaomi Redmi Note 9 Smartphone can be seen in table 4.

Table 4. Specifications for Smartphone Evidence

No.	Specification Type	Evidence Specifications
1	Brand	Xiaomi
2	Serial Model	Redmi Note 9 M2003J15SC
3	IMEI	865073058147563
4	Operation System	Android
5	Version of Operation System	11 RP1A.200720.011

In the process of collecting data acquisition using MOBILedit Forensics Express it is necessary to make sure that the smartphone is already rooted first, its purpose is to unlock all data and security access from the smartphone. After the rooting process is completed then further to dig into the complexity of the smartphone need to take important steps in the forensic

process involving activation of developer options in the menu of smartphone settings.

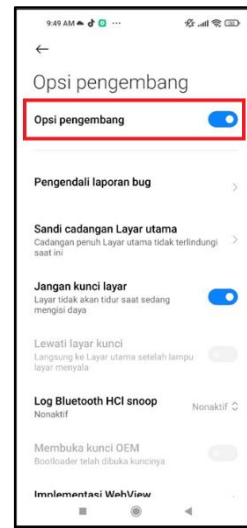


Figure 5: Smartphone Developer Options

Figure 5 shows a display of the developer option feature after access. This technique begins by pressing the version number on the smartphone seven times to open the developer option. Next, enable the 'stay awake' and USB debugging options. USB debugging is enabled to form a secure connection between the phone and the workstation via a USB cable.

4.2.2.1 Data collection using MOBILedit Forensics Express

Based on this, a process will be displayed using the mobile forensic express tools in the process of search collection, and data processing.

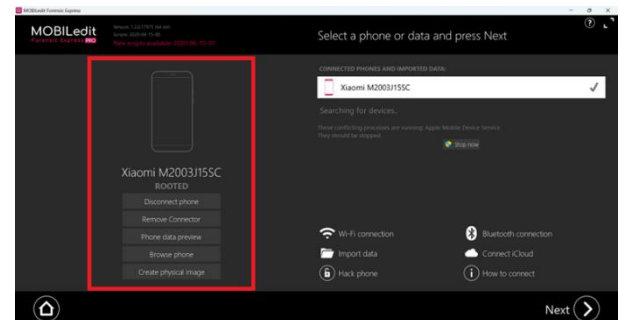


Figure 6: Smartphone Connected to MOBILedit

Figure 6 shows the initial view when users open the MOBILedit Forensic Express application. This view may contain a main navigation menu that allows users to access various features and functions of the application. Here, users can see the option to start a new project or open an existing one, facilitating further investigation without losing previously collected data. Additionally, the interface is designed to be user-friendly, ensuring that even those with minimal technical expertise can navigate through the application with ease. In addition, this view may provide quick access to a variety of commonly used forensic analysis functions, such as data extraction from mobile devices, text message analysis, and contact management.

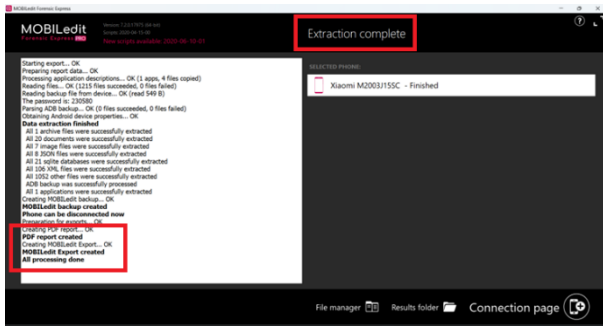


Figure 7: Extraction Completed view

Figure 7 shows the data export process is ongoing. Users are prompted to wait or choose the "Wait or press to connect more devices" option for connecting more devices. This view indicates that the system is extracting data until completed.

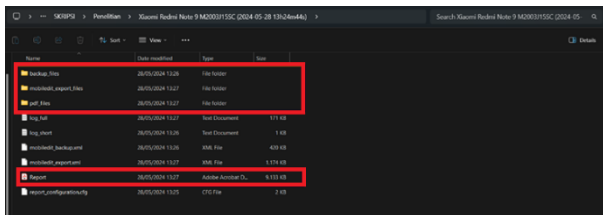


Figure 8: Storage Location Display

Figure 8. After extraction, PDF report files, backup files, and evidence export files are generated. Export files and backups will be further analyzed, while PDF reports make it easier for researchers and stakeholders to navigate and interpret information directly.

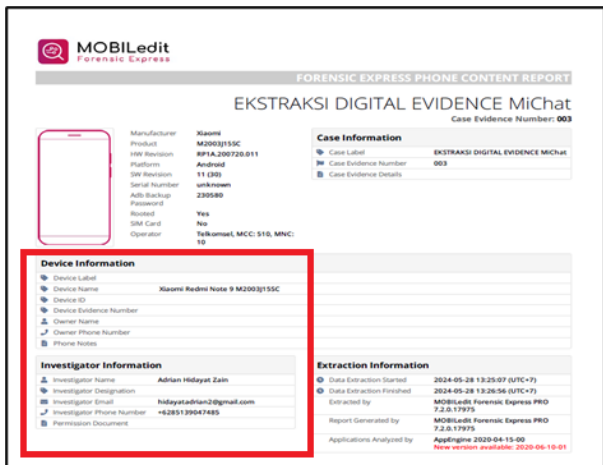


Figure 9: Extraction Results Report File Display

Figure 9 shows the image report of a rooted phone. This view includes Case Information with details of Case Label, Case Evidence, and case Evidence Details. The items displayed include Manufacturer, Product, HW Revision, Platform, SW Revision, Serial Number, IMEI, IMEI 2, Rooted, SIM Card, and Operator. In addition, there is Device Information that includes Device Label, Device Name, Device ID, Devices Evidence Number, Owner Name, Owners Phone Number, and Phone Notes.

4.2.3 Examination

At this stage, data obtained from the previous stage is examined in detail using forensic tools such as Autopsy and Systools SQLite Viewer to ensure the accuracy and integrity of digital evidence.

4.2.3.1 Autopsy Examination

Autopsy is used to examine files and data from the acquisition process, displaying images, videos, and documents, including files without extensions. This toolins the integrity of the acquired file, unlike opening it directly in the acquisition folder that could damage it.

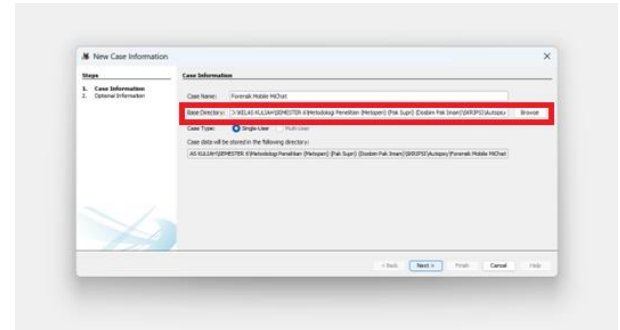


Figure 10: Input detailed information on the autopsy case created

Figure 10 shows the process of filling in details of the case information created like filling the case name created to the storage location of the Case created. The case is named for Mobile Forensics MiChat and is stored with the directory location D:\KELAS KULIAH\SEMESTER 6\Metodologi Penelitian (Metopen) (Pak Supri) (Doshim Pak Imam)\SKRIPSI\Autopsy. It will be imaged to maintain the authenticity of the evidence that has been extracted and then performed the process of imaging that is duplicate the original evidence according to forensic procedure so as not to damage the evidence.

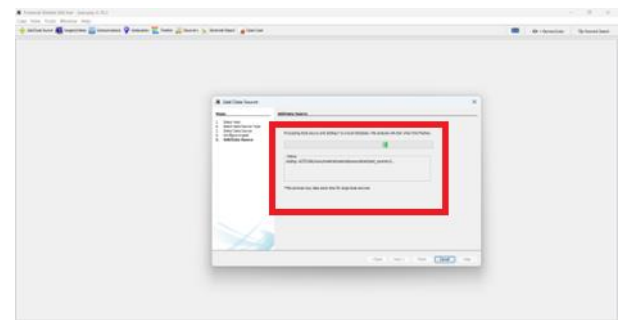


Figure 11: Local Disk Imaging Process in Autopsy

Figure 11 shows the process of imaging and reading files from local disks before displaying them in Autopsy. This process takes a few minutes and needs to be completed before examining the evidence. Imagings the integrity of digital evidence and ensures its structure remains intact. During this process, the original data is copied bit by bit into an image file, which can then be analyzed without the risk of damaging the original evidence. This step is essential in digital forensic investigations to ensure the accuracy and reliability of the analysis results.

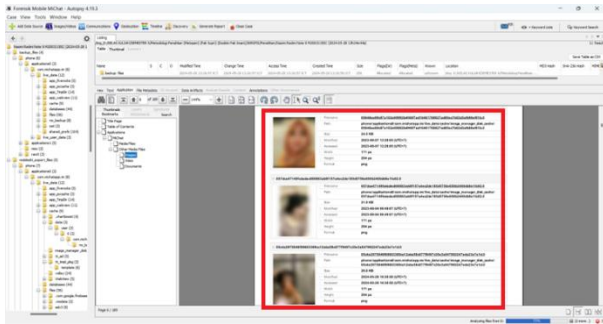


Figure 12: Inspection of images in the extraction results report

Figure 12 shows a photo inspection in a report that has a lot to do with illegal prostitution. The report also lists the image storage directory, mostly at phone/application0/com.michatapp.im/live_data/cache/image_manager_disk_cache/

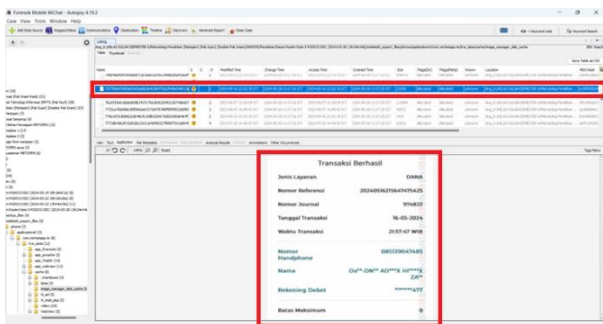


Figure 13: Check the image in the extracted directory

Figure 13 checks the images in the PDF report to verify their existence and authenticity. According to reports, the images are in the related directory. It also found pieces of image that matched the transfer transaction picture, although in an intact or cut condition.

4.2.3.2 Systools SQLite Viewer Examination

Systool SQLite viewer is used to examine the database of acquired applications, comparing the results with Autopsy. This tool facilitates SQLite database analysis, ins data integrity, and is useful in digital forensics. The user-friendly interface facilitates data navigation and interpretation, as well as enables data export in a variety of formats for further analysis or documentation.

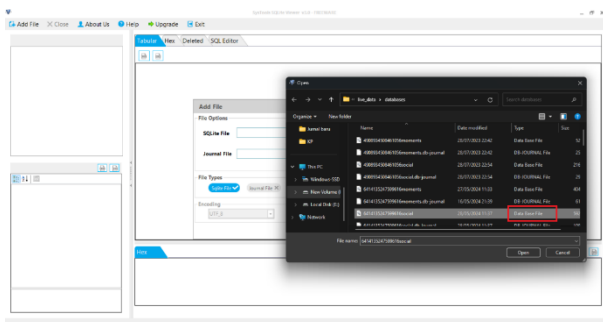


Figure 14: Input Database file

Figure 14 shows the process of identifying and collecting evidence that involves reviewing database files from acquisition folders. The entered files must be typed "Data Base File" to check the application database and find relevant user contacts and conversation text. These files are key elements in identifying and verifying the analyzed application information.

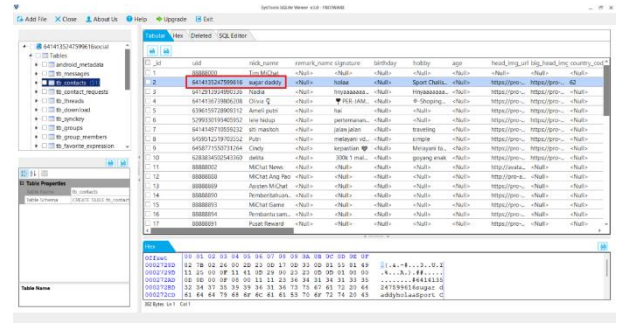


Figure 15: Identify Contact sugar daddy

Figure 15 shows the contents of tb_contact containing a list of identified contacts and found the name "sugar daddy" with the user id "6414135247599616" as expected in a red box marked as a marker for matching user id records of chat messages on the tb_message check table.

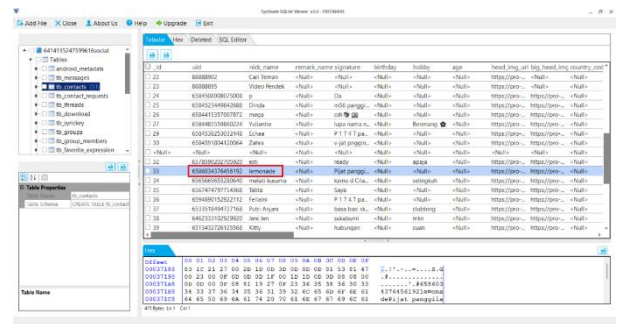


Figure 16: Identify Contact lemonade

Figure 16 shows the contents of tb_contact containing a list of identified contacts and there was also found the name "lemonade" with the user id "6586034376456192" as expected in the red box marked as a marker for matching the user ID record of the chat message on the check table Tb_message.

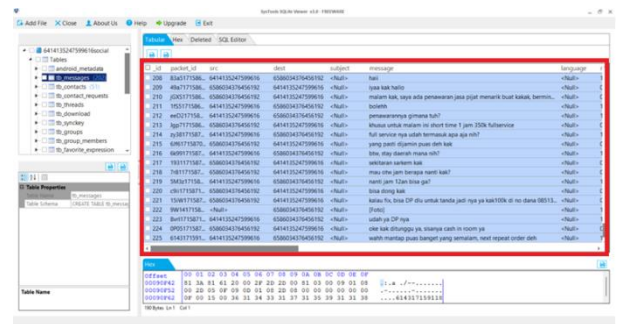


Figure 17: Chat Conversation Text Check

Figure 17 shows the tb_message table with the src, dest, and message columns. Src is the source, dest is the destination, and the message is the content of the conversation. Identified user id "sugar daddy" as "6414135247599616" and "lemonade" as "6586034376456192". The first message from "sugar daddy" contains "haii" to "lemonade", and the answer is "iyaa kak hallo". The next message contains an offer from "lemonade". From_id 208 to 225, identified conversations related to online prostitution.

4.2.4 Analysis

The analysis phase checks the collection and inspection results using MOBILedit Forensics Express, Autopsy, and Systools SQLite Viewer.

4.2.4.1 Analysis with MOBILedit Forensics Express

Most of the evidence relating to illegal prostitution is.

4.2.4.2 Analysis with Autopsy

Autopsy found evidence of online prostitution, including pictures of women tunasusila interacting with "sugar daddy" and clips of pictures of transaction evidence similar to those removed from smartphones. A detailed comparison of the two images is in Table 5.

Table 5. Comparison of images of transaction proof



Image of Proof of Transaction	Image of Autopsy Examination Results
	

Table 5 compares a transaction evidence image before it was deleted with a fragment of the transaction image found using Autopsy. Although the transaction nominal is not listed, the unique transaction number and transaction date and time are the same, namely 16-05-2024 21:57:47 WIB. This reinforces the verification results.

4.2.4.3 Analysis with Systools SQLite Viewer

Results of a database inspection with Systemols SQLite viewer found 51 contacts in tb_contact and 202 text messages in tb_message. Most of these messages are related to illegal prostitution, identified by the style of language used. In tb_contact, suspected contacts "sugar daddy" and "lemonade" were found, according to previously received reports. The findings provide strong evidence that reinforces the alleged illegal activity, suggesting a pattern of communication consistent with online prostitution. This information is vital for further investigation, as it links contacts and messages relevant to suspected criminal activity. The comprehensive analysis and cross-referencing of the contacts and messages have solidified the connections between the involved parties and the suspected illicit activities. These findings are instrumental in building a robust case against the perpetrators and ensuring that all digital traces are meticulously documented. Full details of the evidence found can be found in Table 6.

Table 6. Details of Conversation Text Evidence found in Systools SQLite Viewer

Information	Result	Description
Contact	1. User id : 6414135247599616 Name : sugar daddy 2. User id : 6586034376456192 Name : lemonade	Found
Text message	Source : 6414135247599616 Name : sugar daddy Message : haii Destination : 6586034376456192 (lemonade)	Found

Text message	Source : 6586034376456192 Name : lemonade Message: iyaa kak hallo Destination: 6414135247599616 (sugar daddy)	Found
Text message	Source : 6586034376456192 Name : lemonade Message: malam kak, saya ada penawaran jasa pijat menarik buat kakak, berminat? Destination: 6414135247599616 (sugar daddy)	Found
Text message	Source : 6414135247599616 Name : sugar daddy Message: bolehh Destination: 6586034376456192 (lemonade)	Found

Table 6 shows the results of using Systools SQLite Viewer to find evidence that has been removed by the perpetrator, such as contacts and conversations. In the table there are contacts from the perpetrator and 19 conversations between "sugar daddy" and "lemonade".

4.2.5 Reporting

This report contains digital evidence related to a case of online prostitution on MiChat Mobile. The evidence was found using MOBILedit Forensics Express, Autopsy, and Systools SQLite Viewer, from the smartphone of the offender who was seized the device. A thorough investigation and forensic analysis ensures the integrity of evidence for the legal process, following the standard methods of the National Institute of Justice. This meticulous approach not only safeguards the evidence but also enhances its credibility and admissibility in court. By meticulously analyzing the data, investigators were able to uncover key details and establish a strong connection between the suspect's activities and the alleged illegal operations. The comprehensive findings provide a clear picture of the offender's activities and interactions. The details of digital evidence can be seen in Table 7.

Table 7. Results of Digital Evidence Findings

Finding Items	MOBILedit Forensics Express	Autopsy	Systools SQLite Viewer	Amount
Perpetrator Contact	-	✓	✓	2
Image of proof of transfer/ transaction	✓	✓	-	1
Text of the perpetrator's conversation	-	-	✓	19
Total discoveries per Application	1	3	21	22

Table 7 contains digital evidence of cases of online prostitution via MiChat Mobile, using three forensic tools. MOBILedit

Forensics Express gathers evidence from the MiChat app and creates an acquisition report. Autopsy identifies photos, videos, contacts, and the perpetrator's account name. Systools SQLite Viewer finds a conversation database more complete than Autopsy. The percentage result of the proof of each tool is shown in Figure 18.

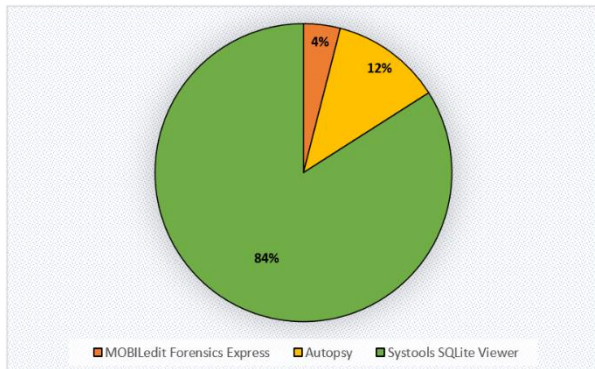


Figure 18: Graph of Percentage of Examination Findings Results

Figure 18 shows a comparative diagram of percentage findings during implementation. Systools SQLite Viewer leads with 84% of findings, mainly text conversations and contacts, highlighting its effectiveness in database extraction. Autopsy uncovered 12% of the evidence, focusing on contacts and images. MOBILEdit contributed 4%, primarily in collecting and extracting evidence from mobile devices. These differences likely stem from the varying capabilities of each tool. The report concludes with explanations following National Institute of Justice (NIJ) guidelines, covering identification, collection, examination, analysis, and reporting. This highlights the importance of using a comprehensive forensic approach to capture and analyze all critical data.

5. CONCLUSION

The research uses the method of the National Institute of Justice which consists of five stages: Identification, Collection, Examination, Analysis, and Reporting. Test results with this method give significant accuracy results and produce valid and accurate data. In the WhatsApp Mobile Forensics process on Online Fraud Cases, three tools are used: MOBILEdit Forensic Express, Autopsy, and Systools SQLite Viewer. Each of the tools has a different degree of accuracy in finding evidence, with MOBILEdit Forensic Express and Autopsi valid in finding image evidence, as well as Systool SQLite Viewer accurate in digging contact information history and text messages ever occurred.

6. REFERENCES

- [1] A. C. N. Hidayah and I. Riadi, "Digital Forensic Analysis on Mobile-based MiChat Services using National Institute of Standard Technology Method," *Int. J. Comput. Appl.*, vol. 184, no. 31, pp. 49–55, Oct. 2022, doi: 10.5120/ijca2022922387.
- [2] A. Andria, "Forensik Digital Sistem Informasi Berbasis Web," *JAMI J. Ahli Muda Indones.*, vol. 2, no. 2, pp. 33–44, Dec. 2021, doi: 10.46510/jami.v2i2.73.
- [3] C. Indonesia, "Tujuh Muncikari Prostitusi Online Ditangkap di Surabaya," *Trans Media*, 2020. <https://www.cnnindonesia.com/nasional/20200515113308-12-503655/tujuh-muncikari-prostitusi-online-ditangkap-di-surabaya> (accessed May 17, 2023).
- [4] D. Yuliana, T. Yuniati, and B. Parga Zen, "Analisis Forensik Terhadap Kasus Cyberbullying Pada Instagram dan Whatsapp Menggunakan Metode National Institute of Justice (NIJ)," *Cyber Secur. dan Forensik Digit.*, vol. 5, no. 2, pp. 52–59, Jan. 2023, doi: 10.14421/csecurity.2022.5.2.3734.
- [5] G. Pawitradi and I. K. Gede Suhartana, "Acquisition of LINE Digital Social Media Evidence Using the National Institute of Justice (NIJ) Method," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 8, no. 2, p. 129, Jan. 2020, doi: 10.24843/JLK.2019.v08.i02.p04.
- [6] H. A. Timor and I. Riadi, "Web Forensics on Tiktok Services using National Institute of Standards and Technology Method," *Int. J. Comput. Appl.*, vol. 185, no. 36, pp. 40–46, Oct. 2023, doi: 10.5120/ijca2023923157.
- [7] H. Herman, A. Yudhana, and F. Anggraini, "Akuisisi Bukti Digital Tiktok Berbasis Android Menggunakan Metode National Institute of Justice," vol. 10, no. 1, pp. 89–96, 2023, doi: 10.25126/jtiik.20231016416.
- [8] I. Gilbert Rian Mailangkay, E. Zakharia, A. Hadi, T. Informatika, and S. Palangka Raya, "Komparasi Analisis Bukti Digital Tiktok Lite Menggunakan Metode National Institute of Justice," *J. Sains Komput. Inform. (J-SAKTI)*, vol. 6, no. 2, pp. 661–670, 2022, doi: 10.30645/j-sakti.v6i2.
- [9] I. P. D. I. Putra and I. K. G. Suhartana, "Cyberbullying Analysis on WhatsApp Messenger Using the National Institute of Justice (NIJ) Method," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 9, no. 4, p. 501, May 2021, doi: 10.24843/JLK.2021.v09.i04.p07.
- [10] I. Riadi, S. Sunardi, and S. Sahiruddin, "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)," *J. Rekayasa Teknol. Inf.*, vol. 3, no. 1, p. 87, Jun. 2019, doi: 10.30872/jurti.v3i1.2292.
- [11] Jeki Kuswanto, Nur Asyifa, and I. Hadi Purwanto, "Akuisisi Google Drive Android Menggunakan Oxygen dan MOBILEdit Dengan Metode National Institute of Justice," *J. Inform. Teknol. dan Sains*, vol. 5, no. 1, pp. 141–147, Feb. 2023, doi: 10.51401/jinteks.v5i1.2523.
- [12] 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.
- [13] M. Prasetyo and I. Riadi, "Investigation Telegram based-on Web using National Institute of Standards and Technology Method," *Int. J. Comput. Appl.*, vol. 183, no. 50, pp. 8–15, Feb. 2022, doi: 10.5120/ijca2022921092.
- [14] MiChat PTE. Limited, "MiChat," 2018. <https://www.michat.sg/about/> (accessed May 21, 2023).
- [15] Muhammad Abdul Aziz, Wicaksono Yuli Sulistyono, and Sri Rahayu Astari3, "Komparatif Anti Forensik Aplikasi Instant Messaging Berbasis Web Menggunakan Metode Association of Chief Police Officers (ACPO)," *JURISTIK (Jurnal Ris. Teknol. Inf. dan Komputer)*, vol. 1, no. 01, pp. 8–15, Jun. 2021, doi: 10.53863/juristik.v1i01.341.

- [16] N. A. I. Maniar and T. Yuniati, "Implementasi Mobile Forensic Pada Aplikasi Michat dan Telegram Dengan Framework NIST 800-101," *Cyber Secur. dan Forensik Digit.*, vol. 5, no. 2, pp. 60–65, Jan. 2023, doi: 10.14421/csecurity.2022.5.2.3764.
- [17] N. Anwar, S. A. Akbar, A. Azhari, and I. Suryanto, "Ekstraksi Logis Forensik Mobile pada Aplikasi E-Commerce Android," *Mob. Forensics*, vol. 2, no. 1, pp. 1–10, Mar. 2020, doi: 10.12928/mf.v2i1.1791.
- [18] N. Fatmah and R. Indrayani, "Analisis Forensik Digital pada Solid State Drive Fungsi TRIM Menggunakan Tools Autopsy dan OSForensics," *J-SISKO TECH (Jurnal Teknol. Sist. Inf. dan Sist. Komput. TGD)*, vol. 5, no. 2, p. 185, Jul. 2022, doi: 10.53513/jsk.v5i2.5755.
- [19] R. Adijisman and I. Riadi, "Mobile Forensic on WhatsAppServices using National Institute of Standards and Technology Method," *Int. J. Comput. Appl.*, vol. 183, no. 29, pp. 41–48, Oct. 2021, doi: 10.5120/ijca2021921680.
- [20] S. Kemp, "DataReportal Digital 2020: Indonesia," *Digital 2020: Indonesia*, 2020. <https://datareportal.com/reports/digital-2020-indonesia> (accessed May 17, 2023).
- [21] S. P. F. W. Pratama, I. G. N. A. C. Putra, M. A. Hamid, C. Christian, and I. K. K. Merdana, "Analisis Forensik Digital pada Aplikasi Twitter di Android sebagai Bukti Digital dalam Penanganan Kasus Prostitusi Online," *JELIKU (Jurnal Elektron. Ilmu Komput. Udayana)*, vol. 10, no. 3, p. 271, Apr. 2022, doi: 10.24843/JLK.2022.v10.i03.p03.
- [22] S. R. A. Ardiningtias, S. Sunardi, and H. Herman, "Investigasi Digital Pada Facebook Messenger Menggunakan National Institute of Justice," *J. Inform. Polinema*, vol. 7, no. 4, pp. 19–26, Aug. 2021, doi: 10.33795/jip.v7i4.709.
- [23] S. Soni, Y. Fatma, and R. Anwar, "Akuisisi Bukti Digital Aplikasi Pesan Instan 'Bip' Menggunakan Metode National Institute Of Justice (NIJ)," *J. CoSciTech (Computer Sci. Inf. Technol.)*, vol. 3, no. 1, pp. 34–42, Jun. 2022, doi: 10.37859/coscitech.v3i1.3694.
- [24] S. Sunardi, I. Riadi, and J. Triyanto, "Forensics Mobile Layanan WhatsApp pada Smartwatch Menggunakan Metode National Institute of Justice," *JOINTECS (Journal Inf. Technol. Comput. Sci.)*, vol. 6, no. 2, p. 63, May 2021, doi: 10.31328/jointecs.v6i2.2315.
- [25] T. F. Efendi, R. Rahmadi, and Y. Prayudi, "Rancang Bangun Sistem Untuk Manajemen Barang Bukti Fisik dan Chain of Custody (CoC) pada Penyimpananan Laboratorium Forensika Digital," *J. Teknol. dan Manaj. Inform.*, vol. 6, no. 2, pp. 53–63, Dec. 2020, doi: 10.26905/jtmi.v6i2.4177.
- [26] T. Irawan and I. Riadi, "Mobile Forensic Signal Instant Messenger Services in Case of Web Phishing using National Institute of Standards and Technology Method," *Int. J. Comput. Appl.*, vol. 184, no. 32, pp. 30–40, Oct. 2022, doi: 10.5120/ijca2022922394.
- [27] Y. Safitri, I. Riadi, and S. Sunardi, "Mobile Forensic for Body Shaming Investigation Using Association of Chief Police Officers Framework," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 22, no. 3, pp. 651–664, Jul. 2023, doi: 10.30812/matrik.v22i3.2987.