Mobile Forensic Analysis of MiChat Application in Human Trafficking Cases using National Institute of Justice Method

Shantika Adila Putri
Department of Informatics Universitas Ahmad Dahlan Yogyakarta of Indonesia

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

ABSTRACT
This research investigates the misuse of the MiChat application in facilitating human trafficking activities in Indonesia by applying the digital forensic methodology developed by the National Institute of Justice (NIJ), which consists of five phases: identification, collection, examination, analysis, and reporting. Forensic analysis of the seized devices revealed 27 MiChat contact entries, 22 chat conversations between perpetrators and victims, and a suspicious user profile named Jordan Ghazafar with the bio HRD Mandala Spa. These findings demonstrate the app's role in enabling exploitation through anonymous communication features and highlight the effectiveness of the NIJ methodology in uncovering critical digital evidence. The results contribute to a deeper understanding of traffickers modus operandi and support the development of more effective law enforcement strategies and digital crime prevention frameworks in Indonesia.

Keywords
MiChat Application, Human Trafficking, Digital Forensics, National Institute of Justice.

1. INTRODUCTION
The rapid development of digital technology has significantly influenced the way people communicate and interact. While technological progress has brought many positive changes, it also opens opportunities for cybercrime, including online prostitution and human trafficking. One application that has gained public attention for its misuse in facilitating these crimes is MiChat. This messaging platform provides anonymous chat and a "people nearby" feature that is often exploited by individuals offering illegal sexual services [1][2][3]. Many users list sexual services in their profiles, set prices, and communicate with clients anonymously, making it difficult for authorities to detect such activities [4][5][6].

According to reports from the Indonesian Ministry of Communication and Informatics, more than 10 million MiChat accounts have been linked to suspected online prostitution activities [7]. Compared to other messaging or dating apps such as Tinder or Telegram, MiChat's minimal verification process and location-based features make it particularly vulnerable to exploitation [8][9]. The use of this platform by traffickers and sex workers illustrates how digital spaces can enable exploitation and increase challenges for law enforcement.

Although prostitution is regulated under Article 296 of the Indonesian Criminal Code (KUHP), and the distribution of immoral content is prohibited by Article 27 of the Information and Electronic Transactions (ITE) Law, online prostitution has not been explicitly defined or regulated [10]. This creates a legal gap that complicates enforcement and prosecution efforts [11]. This research applies the NIJ forensic method comprising identification, collection, examination, analysis, and reporting to investigate how MiChat is used in human trafficking cases and to demonstrate how digital evidence can support legal proceedings and victim protection.

2. LITERATURE STUDY
2.1 Digital Forensics
Digital forensics is a branch of forensic science that investigates data and discoveries within digital devices. Experts define it as a series of procedures and techniques used to identify and collect digital evidence that can be presented legally in court [12][13]. This field emerged as a response to the increasing number of cybercrime cases involving computer systems.

2.2 Mobile Forensics
Mobile forensics is the science of recovering digital evidence through forensic methods and mobile device conditions. With the advancement of technology, mobile forensic techniques have become essential in solving crimes involving mobile devices especially smartphones due to the variety of operating systems and types of criminal activities conducted through them [14].

2.3 Digital Evidence
Digital evidence refers to information stored in binary form that can be legally presented in court. Devices such as hard drives, flash drives, and smartphones are typical sources of digital evidence. Examination reports include details about the hardware used, procedures applied, and tools employed until the evidence is retrieved. These findings vary widely and are often inconsistent. If not properly handled by official investigators, digital evidence is prone to alteration, which may compromise its authenticity. Any changes can render the report invalid, falsified, or unusable [15][16]. The NIJ framework is applied to validate, preserve, collect, identify, interpret, and present digital evidence from digital sources to support criminal case reconstruction. In addition to procedures, digital forensics requires specific tools. The tools used in this Research include Oxygen Forensic Detective,

SysTools SQLite Viewer, and DB Browser for SQLite [17]. These tools were selected due to their capability to extract, read, and analyze key artifacts from applications like MiChat, which played a central role in the human trafficking case analyzed in this research.

2.4 MiChat
As of October 2018, MiChat is one of the most downloaded free messaging apps in Indonesia, ranked in the Top 5 Free Chat Apps on the Google Play Store. MiChat offers interactive features such as People Nearby to discover and chat with local users, Trending Chats to discussing popular topics, and Moments to sharing photos or videos with friends [18].

2.5 Human Trafficking
Human trafficking includes all forms of recruitment, transfer, and labor relocation for the purpose of human exploitation. It often involves violence, deception, or coercion. Exploitation may

include forced labor, sex work, slavery, and organ trade. The sale of children for adoption, begging, or religious purposes also constitutes child trafficking. As a hidden and highly organized activity, human trafficking affects individuals of all genders and ages. Since it is commonly facilitated by transnational criminal networks, human trafficking is considered a cross-border crime [19][20].

2.6 Digital Forensic Tools

Several forensic tools were utilized in this research to analyze data from the MiChat application. DB Browser for SQLite was used to directly read and analyze MiChat database files. It supports flexible SQL queries to inspect chat logs, contact lists, and other investigative data, and can recover deleted records without altering original content maintaining evidence integrity in human trafficking investigations [21]. Oxygen Forensic Detective is a professional-grade forensic software for mobile devices that enables the extraction, analysis, and visualization of data from smartphones, tablets, computers, and external storage. Its strong reporting capabilities and features like deep data recovery, geolocation mapping, and advanced visualization make it valuable for both criminal and civil case investigations [22]. SysTools SQLite Viewer, a free utility, is also used to open and examine SQLite databases such as; .db, .sqlite, .db3 without needing a server. With features such as table views, HEX mode, keyword search, and deleted record recovery, this tool is particularly effective for retrieving and documenting chat histories, media, and metadata from MiChat's backups for forensic purposes [23].

2.7 National Instate of Justice (NIJ)

This research adopts the NIJ method for forensic investigation, which is particularly effective for identifying deleted chat messages. The NIJ method offers a structured and systematic process consisting of five interconnected stages: identification, collection, examination, analysis, and reporting [24]. Each stage contributes to accurate and reliable results. The preservation stage involves selecting and organizing potential digital evidence, followed by collection, where data is gathered from valid sources while maintaining authenticity. In the examination phase, the collected files are inspected manually or automatically, often using hashing for validation. Analysis interprets the digital data through both technical and legal lenses to uncover valid forensic findings. This research's stages include (1) implementation and testing, (2) acquisition of evidence copies, and (3) digital forensic analysis, as shown in Figure

2.3. Finally, the reporting stage compiles the investigation results, detailing the tools and techniques used, simulated case scenarios, and recommendations for improving forensic procedures and tools [30]. Figure 1 illustrates the five key stages of the NIJ digital forensic methodology, serving as the framework for this research.

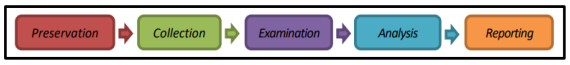


Figure 1: NIJ Digital Forensic Investigation Phases

3. RESEARCH METHOD

This research applies the investigative framework developed by the NIJ, which consists of five structured stages: identification, collection, examination, analysis, and reporting. In the identification stage, the suspected device, a Xiaomi Redmi A1 running Android 12 Go Edition, was recognized as potential digital evidence and carefully documented through photographs, IMEI registration, and seizure chronology in order to establish a valid chain of custody. The collection stage was performed using live acquisition because the smartphone was obtained in an active state. Oxygen Forensic Detective was employed to conduct a Full File System (FFS) extraction, producing 6.6 GB of data that was subsequently verified through SHA-256 hashing to maintain authenticity and integrity.

The examination stage involved a multi-tool approach to ensure the reliability of findings. SysTools SQLite Viewer enabled direct inspection of the raw SQLite database files, such as tb_messages and tb_contacts, in both tabular and hexadecimal modes without modifying the original data structure. To complement this, DB Browser for SQLite was used to query the database interactively, allowing specific filtering based on keywords, timestamps, and user identifiers. At the same time, Oxygen Forensic Detective reconstructed conversations and visualized communication patterns, providing timeline-based summaries that highlighted significant interactions between suspect and victim.

The analysis stage emphasized rigorous cross-validation across multiple forensic tools to ensure data reliability and integrity. For instance, SysTools and DB Browser consistently revealed the same set of twenty-seven MiChat contacts and twenty-two relevant chat messages, indicating a strong degree of data consistency. Meanwhile, Oxygen Forensic Suite corroborated these findings and further enriched the analysis by providing contextual insights through reconstructed timelines, highlighting user interactions over time and clarifying the sequence of communication events. This methodological triangulation demonstrated that each tool, despite its distinct functionalities and analytical strengths, yielded convergent evidence, thereby significantly reinforcing the credibility, reliability, and robustness of the overall forensic process. In the reporting stage, all validated digital artifacts including chat transcripts, user profiles, contact lists, timestamps, and associated metadata were meticulously organized and compiled into structured tables, visual figures, and comprehensive narrative descriptions A visual representation of this process is provided in Figure 2 [25].

Figure 2 : NIJ Method Stages

4. RESULTS AND DISCUSSION

This research investigates a simulated case of human trafficking involving the use of the MiChat application on an Android-based mobile device. The primary focus of this study was limited to a single device model, specifically the Xiaomi Redmi A1. While this allowed for a controlled environment, it also presents limitations in terms of generalizability. To enhance the validity and reliability of future research, it is recommended that subsequent studies incorporate a wider range of mobile devices, various versions of the Android operating system, and a larger dataset of chat conversations. This would allow for a more comprehensive evaluation of the forensic tools and methods used, as well as greater consistency across different environments.

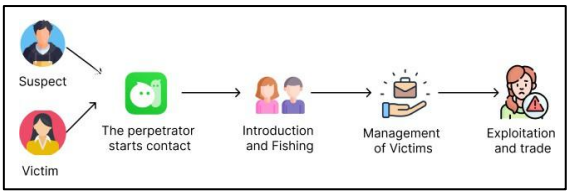


Figure 3: Pre-Incident Phase of Human Trafficking

Figure 3 in this phase, the perpetrator begins by creating a fake MiChat profile using a smartphone and poses as a professional job recruiter. He searches for potential victims by browsing nearby users and eventually targets a woman offering massage services. The perpetrator initiates a conversation, builds trust through frequent messaging, and offers an attractive out-of-town job. After the victim agrees, she is brought to a location where she is exploited. The perpetrator continues to use MiChat to coordinate with others and monitor the victim's actions.

Figure 4 : Incident Phase of Human Trafficking

Figure 4 once the crime is underway, the perpetrator senses the risk of being exposed and quickly deletes chats, contacts, and other traces within MiChat to avoid detection. Meanwhile, the victim manages to escape and report the incident. Although much of the evidence has been erased, she provides screenshots and profile information that she had saved beforehand. Authorities immediately initiate a digital forensic response to secure the remaining evidence on her mobile device.

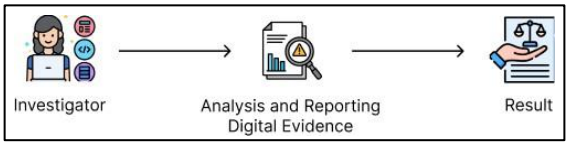


Figure 5 : Post Incident Phase of Human Trafficking

Figure 5 the digital forensic team performs a detailed investigation using forensic tools to extract and analyze data from the victim's phone. They recover deleted messages, contact lists, and metadata linked to the perpetrator's activity on MiChat. Based on the findings, a comprehensive report is generated which supports the legal process. The case proceeds to prosecution, and the victim receives necessary assistance for recovery.

4.1 Investigation Preparation

The preparation phase marks the initial and critical stage of the digital forensic investigation, following the guidelines of the National Institute of Justice (NIJ) framework. This phase is focused on securing, organizing, and thoroughly documenting digital evidence to ensure that all subsequent analysis is conducted in a systematic, lawful, and forensically sound manner. In the context of this research, the investigation was initiated after law enforcement received a report from a human trafficking victim, who stated that the MiChat application had been used as a tool for communication in the crime. Based on this report, authorities apprehended the suspect and confiscated a Xiaomi Redmi A1 smartphone believed to be involved in the trafficking activity. During this phase, the forensic team conducted detailed documentation of the device, including its physical condition, technical specifications, and the precise chronology of its seizure. These steps were essential to maintain the integrity of the digital evidence and to ensure its admissibility in legal proceedings. The overall process carried out during the preparation phase is visually summarized and presented in Figure 6.

Figure 6: Smartphone Evidence

Each detail in the table is organized neatly and systematically, providing an accurate technical perspective to support the forensic analysis and legal accountability process. The detailed specifications of the smartphone evidence are presented in Table 1.

Table 1: Smartphone Evidence Specifications

No	Type	Description
1	Brand	Xiaomi
2	Series	Redmi A1
3	IMEI	866681063463269
4	Operating System	Android
5	Version OS	12 (Go edition)

The preparation phase marks the initial stage of the digital forensic investigation, following the NIJ framework. This phase involves securing and documenting digital evidence to ensure a lawful analysis. The investigation began after authorities received a report involving MiChat application. The suspect was arrested, and a Xiaomi Redmi A1 smartphone was seized. The forensic team documented the device's condition and seizure timeline to preserve evidence integrity. Table 2 lists the hardware and software used, supporting transparency and reproducibility.

Table 2 : Investigation Supporting Devices and Tools

No	Equipment	Type	Description
1	Laptop	Hardware	Lenovo IdeaPad 3 14ADA6, AMD Series, AMD 3020e with Radeon Graphics, 1.20 GHz, 64-bit OS, x64-based processor.
2	USB Cable	Hardware	Robot USB Cable.
3	DB Browser for SQLite	Software	Manages and analyzes SQLite database structures, including executing SQL commands and exporting data for further analysis.
4	Oxygen Forensic Detective	Software	Collects, extracts, and analyzes data from digital devices.

5	SysTools SQLite Viewer	Software	Instantly displays the contents of SQLite database files without a database connection, useful for viewing raw data.

4.2 Data Collection

The collection phase in this investigation began with the seizure of a smartphone suspected to be used in a human trafficking case via the MiChat application. The device, a Xiaomi Redmi A1, was acquired in active condition, prompting the use of live data acquisition to preserve volatile data such as cache, system logs, and session files.

The process employed Oxygen Forensic Detective, which enabled a Full File System extraction, granting access to internal application directories and databases without altering original data.

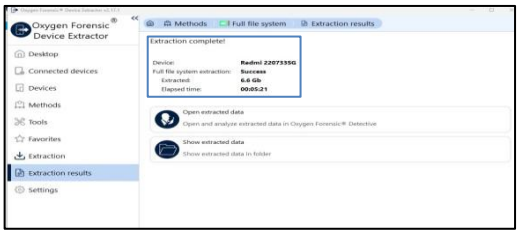


Figure 7: Extraction Results from MiChat Using Oxygen Forensic Detective

As seen in Figure 7, the extraction was successfully completed with a total size of 6.6 GB and verified through SHA-256 hash values to ensure data integrity. The results were stored in the forensic directory and analyzed using Oxygen Forensic Detective.

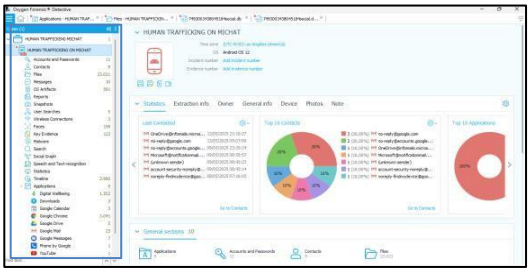


Figure 8 *:* Extracted MiChat Artifacts Displayed

As seen in Figure 8 illustrates the post-extraction interface, showing organized categories like contacts, chat messages, and app data. These digital artifacts form the foundation for further forensic analysis in the subsequent stages of this research.

4.3 Examination

The examination phase in this research was conducted after successfully extracting data from the suspect's Android smartphone using the full file system extraction method. This phase focused on identifying and analyzing digital artifacts originating from the MiChat application, which was suspected to be the main communication medium used by the perpetrator in the human trafficking case. The examination targeted internal directories of the MiChat app, particularly its SQLite database files, where message histories, user profiles, and activity logs were stored. Browser enabled interactive data exploration, including running specific SQL queries to isolate keywords, timestamps, or user IDs relevant to the trafficking case.

4.3.1 Examination using SysTools SQLite Viewer

Examination process was carried out using SysTools SQLite Viewer, a tool specifically designed to read and analyze SQLite database files without altering their structure. At this point, the focus was placed on reviewing the extracted database artifacts from the MiChat application, especially the tb_messages and tb_contacts tables that store the conversation history and user contact information. These tables provided valuable insights into user interactions, communication patterns, and potential relationships between users.

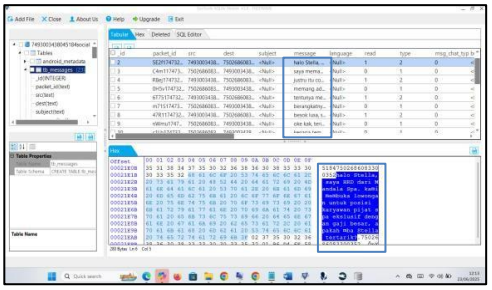


Figure 9 : Display of MiChat Conversation Using SysTools SQLite Viewer

As illustrated in Figure 9, the chat records between the perpetrator and the victim were successfully accessed through this tool. The database content was presented in a tabular format, displaying detailed message attributes such as message ID, sender, recipient, timestamp, and message content. Additionally, the hexadecimal view offered by the tool allowed the forensic investigator to cross-verify the raw data, ensuring the integrity and originality of the messages retrieved from the source file.

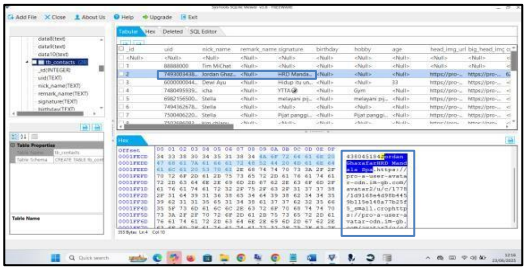


Figure 10 : Display Contact Data Using SysTools

Beyond just chat messages, SysTools SQLite Viewer also enabled examination of user profile metadata stored in the contact tables. As shown in Figure 10, one of the identified contacts named Jordan Ghazafar had a suspicious account bio labeled HRD Mandala Spa, which aligned with the victim's report about fraudulent job recruitment. The tool's clarity and structure helped extract patterns from the database, confirming the perpetrator's identity and intent.

4.3.2 Examination using DB Browser for SQLite

To complement the initial findings, a more advanced and interactive examination was conducted using DB Browser for SQLite. This open-source forensic tool offers the ability to browse, query, and export SQLite databases interactively, allowing for deeper exploration of the extracted MiChat data. The primary objective in this phase was to validate the previous findings and search for additional evidence that might have been overlooked. By leveraging DB Browser for SQLite, the forensic team could efficiently navigate through large volumes of data, filter relevant records, and uncover hidden or deleted messages that standard tools might miss. This approach enhanced the accuracy and completeness of the investigation, providing a clearer picture of the suspect's communication patterns.

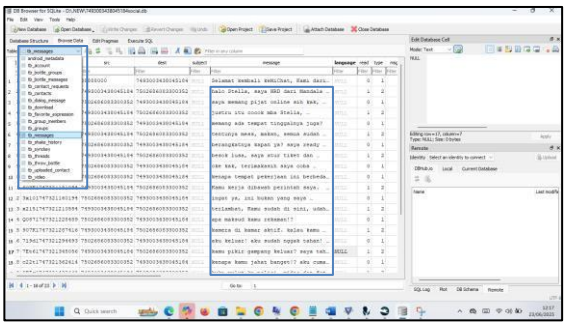


Figure 11 : MiChat Message Table View in DB Browser for SQLite

As depicted in Figure 11, the tb_messages table was opened and manually queried to isolate specific keywords, message types, or timestamps that correspond to significant events in the trafficking case. The tool's powerful filtering and SQL query features provided enhanced visibility into the structure and content of communications, allowing the forensic examiner to trace the exact chronology and context of each message.

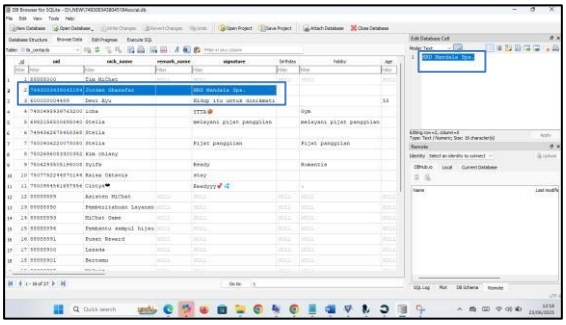


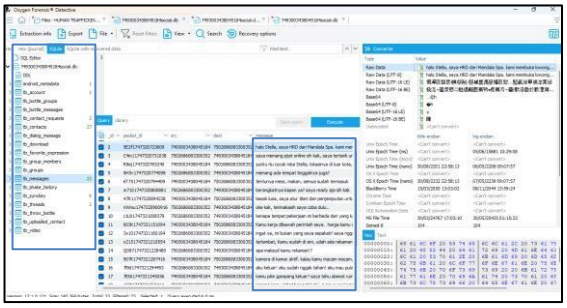
Figure 12 : MiChat Contact Table View in DB Browser for SQLite

In addition, Figure 12 highlights the results of inspecting the tb_contacts table, which reaffirmed the presence of the same suspicious user Jordan Ghazafar with the identical employment-related bio found earlier. DB Browser's export capability also enabled this structured data to be compiled into a report friendly format. This cross validation of data across tools not only confirmed the authenticity of digital evidence but also strengthened its admissibility in legal proceedings.

4.3.3 Examination using Oxygen Forensic Detective

The extracted data was imported into the Oxygen platform, where it was categorized and visualized for investigation. This application provides structured visual displays, including statistical summaries and artifact overviews, helping investigators identify patterns in the MiChat data.

Figure 13 : Display of MiChat Conversation Using Oxygen Forensic Detective



As depicted in Figure 13, This figure shows the reconstructed MiChat conversations within the Oxygen interface. The data includes chat sequences, helping to trace the suspect's activities and corroborate digital interactions relevant to human trafficking.

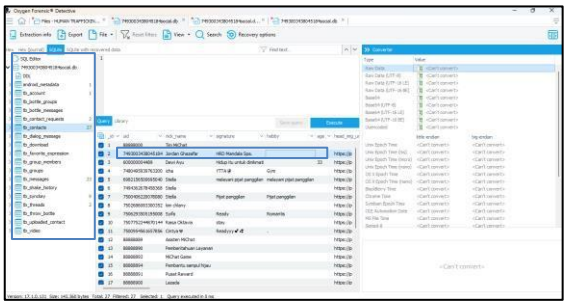


Figure 14 : Display of MiChat Contact Data Using Oxygen Forensic Detective

As shown in Figure 14, This figure presents the contact profile details extracted from MiChat. Attributes such as nickname, bio, and user establish links to criminal communications.

4.4 Analysis

The analysis phase served as a critical step in thoroughly examining the results obtained during the prior examination stage. By utilizing tools such as Oxygen Forensic Detective, SysTools SQLite Viewer, and DB Browser for SQLite, the researcher was able to extract, interpret, and validate key digital artifacts from the MiChat application. This process focused on uncovering message histories, contact data, activity logs, and metadata associated with the suspect's interactions. Cross-validation between tools confirmed the same twenty-seven contacts and twenty-two chat messages, while Oxygen added value by reconstructing the chronological timeline of conversations.

4.4.1 Findings from Analysis Using Oxygen Forensic Detective

The initial stage of analysis was performed using Oxygen Forensic Detective, which allowed the investigator to visualize communication records from the MiChat application in a structured timeline format. This tool provided detailed metadata, including exact timestamps such as a message sent on 15/05/2025 at 12:44:09, enabling a clear reconstruction of events. Features such as timeline visualization and keyword search helped trace interactions between the suspect and the victim, offering insight into the flow and content of conversations that suggested exploitation.

4.4.2 Findings from Analysis Using SysTools SQLite Viewer

A more detailed examination followed using SysTools SQLite Viewer, which enabled direct access to the raw database structure

without altering the original content. Through the tb_contacts table, the investigator identified the suspect's MiChat profile under the name Jordan Ghazafar, with a bio description of HRD Mandala Spa. Additional details such as the Indonesian country code +62 and phone number 089528533560 were also found. Using the hex view feature, the data's authenticity and integrity were verified. This evidence not only confirmed the suspect's digital identity but also linked the account directly to the recruitment element of the trafficking operation.

4.4.3 Findings from Analysis Using DB Browser for SQLite

The final stage of analysis involved DB Browser for SQLite, which allowed the investigator to execute SQL queries and perform precise filtering based on keywords, timestamps, and user identifiers. This tool enhanced the ability to track specific interactions and relationships within the database. By reviewing the same tables accessed earlier, such as tb_messages and tb_contacts, the findings from SysTools and Oxygen were validated for consistency. This cross-verification ensured that all communication artifacts were accurate and complete. The ability to export results into structured reports further strengthened the documentation process and contributed to a comprehensive understanding of the suspect's digital activities.

4.5 Reporting

The reporting phase presents a comprehensive summary of digital evidence gathered during the forensic investigation of a human trafficking case involving the MiChat application. The investigation followed the NIJ method, covering identification, collection, examination, analysis, and reporting stages to ensure data authenticity and legal integrity. The main device analyzed was a Xiaomi Redmi A1 (MediaTek Helio A22, 2GB RAM, 32GB storage). Using Oxygen Forensic Detective, SysTools SQLite Viewer, and DB Browser for SQLite, investigators conducted detailed data extraction and analysis. Oxygen enabled logical acquisition and timeline-based message views; SysTools allowed direct access to contact data and profile information; and DB Browser facilitated advanced keyword searches and SQL queries to isolate and verify critical conversations. Together, these tools revealed key artifacts such as user profiles, chat histories, contact lists, and timestamps providing solid digital evidence for prosecution. These conversations contain clear indicators of recruitment, manipulation, and coercion patterns that are consistent with digital grooming and trafficking tactics. The messages were successfully retrieved using forensic tools and parsed into readable formats during the analysis phase.

The complete content of these conversations, which were instrumental in reconstructing the timeline and context of the trafficking scheme, is summarized in Table 3.

Table 3 : Extracted MiChat Chat Content as Digital Evidence

Information	Conversation Content	Remarks
Conversation	kenapa tempat pekerjaan ini berbeda dari yang kamu bilang!? kok saya disuruh "layan" tamu!?	Found
Conversation	Kamu kerja dibawah perintah saya. harga kamu sudah di tentukan. diam dan ikuti aturan!	Found
Conversation	ingat ya, ini bukan yang saya sepakati! saya nggak mau kerja seperti ini!	Found
Conversation	terlambat, Kamu sudah di sini, udah ada rekaman kamu juga haha	Found
Conversation	apa maksud kamu rekaman!?	Found
Conversation	kamera di kamar aktif. kalau kamu macam macam, video kamu bisa viral kapan saja	Found
Conversation	aku keluar! aku sudah nggak tahan! aku mau pulang ke rumah	Found
Conversation	kamu pikir gampang keluar? saya tahu alamat rumahmu, nama orang tuamu, semuanya	Found
Conversation	kenapa kamu jahat banget!? aku cuma nyari kerja!	Found
Conversation	buka mulut ke polisi, video dan foto kamu langsung naik ke publik!	Found
Conversation	tolong.. hapus semuanya. aku janji nggak akan cerita ke siapa siapa..	Found
Conversation	kalau kamu berani ngomong ke siapa pun, kamu bakal nyesal!	Found
Conversation	kenapa kamu kaya gini? aku cuma nyari kerja!	Found
Conversation	semua pesan ini akan saya hapus. jadi kamu nggak punya bukti apa apa!	Found

These chat transcripts not only reveal the suspect's intent and actions but also demonstrate how digital communication can be weaponized for exploitation. The recovered messages serve as crucial evidence that supports the narrative of deception, control, and intimidation employed throughout the victim's recruitment and captivity process. Their forensic integrity, having been extracted and verified across multiple tools, ensures admissibility in legal proceedings and reinforces the value of digital forensics in human trafficking cases.

To offer a clear comparison of each tool's effectiveness in extracting digital evidence, Table 4 presents the findings organized by the forensic software utilized in the investigation.

Table 4 : Comparison of Digital Evidence Identified by Each Forensic Tool

No.	Type of Digital Evidence	Oxygen Forensic Detective	SysTools SQLite Viewer	DB Browser for SQLite	Total Findings
1.	MiChat account username of suspect	✓	✓	✓	1
2.	Suspect's phone number	✓	✓	✓	1
3.	Suspect's profile description	✓	✓	✓	1
4.	Country code of suspect's account	✓	✓	✓	1
5.	MiChat contact list	✓	✓	✓	27
6.	Chat messages between suspect and victim	✓	✓	✓	22
7.	Date and time of conversation	✓	✓	✓	1
8.	Victim's account information	✓	✓	✓	1

A summarized recap of the digital evidence is presented in Table 4. It shows that each forensic tool contributed to uncovering specific types of evidence, including the MiChat username, phone number, profile description, country code, full contact list, full conversation logs, timestamps, and victim account information. All tools Oxygen, SysTools, and DB Browser were able to extract these artifacts consistently. For instance, 27 contact entries and 22 relevant chat messages were identified and verified across all three tools, demonstrating the consistency and reliability of the forensic process.

In conclusion, this reporting phase ensured that all extracted data, ranging from message logs to technical identifiers, were thoroughly documented, cross-verified, and validated to maintain the highest level of accuracy. By adhering strictly to structured forensic principles and employing multiple complementary tools in tandem, the investigation achieved a robust standard of evidence reliability and integrity. This comprehensive approach not only strengthened the credibility of the digital findings but also significantly reinforced their legal admissibility in prosecuting the MiChat-based human trafficking case. Furthermore, detailed reporting and clear documentation provided a solid foundation for transparency and reproducibility, which are essential in forensic investigations.

5. CONCLUSIONS

Based on the analysis and discussion conducted in this research titled *Mobile Forensics of the MiChat Application in Human Trafficking Cases Using the National Institute of Justice (NIJ) Method,* it can be concluded that the application of the NIJ digital forensic framework has proven effective in systematically guiding the investigation of human trafficking activities facilitated through the MiChat application in Indonesia. The method, which consists of five structured stages identification, collection, examination, analysis, and reporting was thoroughly implemented using several forensic tools including Oxygen Forensic Detective, SysTools SQLite Viewer, and DB Browser for SQLite. These tools enabled the comprehensive extraction and interpretation of digital evidence from the suspect's Xiaomi Redmi A1 device, successfully revealing key elements such as intense communication containing trafficking indicators, user contact data, account metadata, usernames, phone numbers, and chat content. All digital evidence was processed in accordance with forensic standards to ensure its authenticity, integrity, and legal admissibility. Furthermore, data validation procedures were carried out rigorously throughout the investigation to maintain the evidentiary value of the findings. As a result, this research not only demonstrated the effectiveness of the NIJ method in digital forensics but also successfully addressed both of the research questions by uncovering how MiChat was utilized in human trafficking and by ensuring the reliability and legal relevance of the digital evidence gathered.

6. REFERENCES

[1] Adamu, H., Adamu Ahmad, A., Hassan, A., & Barau Gambasha, ad. (2021). IJRSI) |Volume VIII, Issue V. In International Journal of Research and Scientific Innovation. www.rsisinternational.org.

[2] Antari, P. E. D. (2022). Pemidanaan Terhadap Pekerja Seks Komersial Melalui Aplikasi Michat The Liability of Prostitute On Michat. Jurnal Selat, 9(2),123–147. https://doi.org/10.31629/selat.v9i2.4386.

[3] Binuko Paksi, A., Hafidhoh, ul, & Kariagil Bimonugroho, S. (2023). Perbandingan Model Pengembangan Perangkat Lunak Untuk Proyek Tugas Akhir Program Vokasi Program Studi D3 Teknologi Informasi, Politeknik Negeri Madiun (Vol. 14, Issue 1).

[4] Efendi, Z., & Eka Apriliani IAIN Pontianak, D. (2021). Analisis Komunikasi Pada Aplikasi MiChat Sebagai Sarana Media Prostitusi Online Di Pontianak. In Analisis Komunikasi pada Aplikasi MiChat (Vol. 4, Issue 2).

[5] Elektronik, J., Udayana, I. K., Dwi, K., Mahendra, O., Komang, I., & Mogi, A. (2021). Digital Forensic Analysis of Michat Applications on Android as Digital Proof in Handling Online Prostitution Cases.

[6] Gilang Ramadhan, A., & Susanti, R. (2022). Prostitusi Online dengan Menggunakan Aplikasi Michat Ditinjau dari Hukum Pidana. Jurnal Bevinding, 01. https://www.akurasi.id/covered-story/wajah-prostitusi-berbalut-

[7] Agung, Kecamatan, N., & Kabupaten Bima, W. (2021). Fenomena Prostitusi Online Dengan Menggunakan Aplikasi Michat Di Desa.

[8] Kurnadi Keamanan Siber, B., Ali Nurfadillah Keamanan Siber, F., Tegar Sabila Keamanan Siber, M., Raya Usa, J. H., Nutug, P., Ciseeng, K., & Bogor, K. (2024). Analisis Memory Forensics Windows Subsystem for Linux 2 (WSL2) Berbasis Hyper-V pada Windows 11 Berdasarkan Nist 800-

86. Jurnal Penelitian Sistem Informasi, 2(1), 178–

188. https://doi.org/10.54066/jpsi.v2i1.1594.

[9] Lestari, Y. D., Fitri, Y., Lubis, A., & Siregar, F. A. (2023). Analisis Perbandingan Kinerja Root Explorer Dan Oxygen Forensic Detective Pada Forensic Digital. Jurnal Fusion, 3(08). https://doi.org/10.54543/fusion.v3i05.350.

[10] Mualfah, D., Viransa, A., & Fu'adah Amran, H. (2023). Akuisisi Bukti Digital Pada Aplikasi Tamtam Messenger Menggunakan Metode National Institute of Justice(Vol. 3, Issue 1).

[11] Nurhairani, H., & Riadi, I. (2021). Analysis Mobile Forensics on Twitter Application using the National Institute of Justice (NIJ) Method. In International Journal of Computer Applications (Vol. 177).

[12] Ode Herman, L., Ode Muh Umran, L., Iba, L., Rajab, M., Ricky Ramadhan Rasyid, M., Ilmu Komunikasi, J., & Halu Oleo, U. (2023). Sosialisasi Pemanfaatan Aplikasi Michat sebagai Media Komunikasi Efektif melalui Fitur People Nearby Article history. 1(2), 76–80. https://doi.org/10.5243/kongga.v1i2.20.

[13] Rudi Parman, Perkembangan Teknologi Perangkat Komputer (Memory-Processor-Input Output). (2021). https://doi.org/10.13140/RG.2.2.34916.30082.

[14] Praktik, P., Prostitution, C., Aplikasi, P., Berdasarkan Kebijakan, M., Fitria, S., & Adhari, A. (2022). Sindi Fitria & Ade Adhari Penanggulangan Praktik Cyb+er Prostitution Pada Aplikasi MiChat Berdasarkan Kebijakan Kriminal Di Indonesia.

[15] Rachmie, S. (2021). Peranan Ilmu Digital Forensik Terhadap Penyidikan Kasus Peretasan Website. Litigasi, 21, 104–127.

[16] Riadi, I., & Dahlan, A. (2021). Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute of Justice. Jurti, 3(1). www.Belkasoft.com.

[17] Riadi, I., & Fadlil, A. (n.d.). Review Proses Forensik Optical Drive Menggunakan Metode National Institute of Justice (NIJ).

[18] Riadi, I., Ruslan, T., Dahlan Jl Soepomo Umbulharjo, A., & Yogyakarta, K. (n.d.). Forensik Multimedia Berbasis Mobile Menggunakan Metode National Institute of Justice.

[19] Rizki Setyawan, M., Yudhana, A., Fadlil, A., Dahlan, A., Studi Teknik Elektro, P., Ahmad Dahlan, U., & Jl Soepomo, Y. (2021). Seminar Nasional Teknologi Fakultas Teknik Universitas Krisnadwipayana. In Jakarta (Vol. 17).

[20] Rosita, M. (n.d.). Analisis Komparatif Performa FTK Imager dan Autopsy dalam Forensik Digital pada Flashdisk.

[21] Saad, S. K., Umar, R., Fadlil, A., Ahmad, U., Jl, D., & Soepomo, S. H. (2021). Analisis Forensik Aplikasi Dropbox pada Android menggunakan Metode NIJ pada Kasus Penyembunyian Berkas. In Jurnal Sains Komputer & Informatika (J-SAKTI (Vol. 4).

[22] Doni Arifandi, Pertanggungjawaban Pidana Terhadap Pelaku Human Trafficking Melalui Media Sosial. (2022).

[23] Soepomo, S. H. (2021). JEPIN (Jurnal Edukasi dan Penelitian Informatika).

[24] Soni, S., Fatma, Y., & Anwar, R. (2022). Akuisisi Bukti Digital Aplikasi Pesan Instan "Bip"Menggunakan Metode National Institute Of Justice (NIJ). Jurnal CoSciTech (Computer Science and Information Technology), 3(1), 34–42. https://doi.org/10.37859/coscitech.v3i1.3694.

[25] Yudhistira, A. A., & Jaya, J. N. U. (2022). Analisis Tingkat Penggunaan Aplikasi MiChat Sebagai Sarana Media Bisnis Prostitusi Online Menggunakan Metode TAM. Jurikom (Jurnal Riset Komputer),9(3),600. https://doi.org/10.30865/jurikom.v9i3.4159.