Digital Forensic Analysis of Cyberbullying Cases on WeChat Application using Digital Forensic Research Workshop

Fahreza Mandala Putra
Department of Informatics Universitas Ahmad Dahlan Yogyakarta of Indonesia

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

ABSTRACT
Cyberbullying on instant messaging platforms such as WeChat can cause significant psychological harm to victims. This study aims to identify and analyze digital evidence related to cyberbullying incidents on Android devices using a structured mobile forensic approach. The investigation adopted the Digital Forensics Research Workshop (DFRWS) framework and utilized MOBILedit Forensic for data acquisition and Autopsy for artifact analysis. Data integrity was maintained through cryptographic hash verification during the forensic process. The forensic examination successfully recovered 6 cyberbullying-related conversations from the perpetrator's device and 12 conversations from the victim's device, indicating the possibility of partial data deletion on the suspect's smartphone. Further analysis revealed that derogatory cyberbullying keywords were more dominant on the victim's device, representing 67% of the identified keywords, compared to 33% on the perpetrator's device. The results demonstrate that the DFRWS framework combined with forensic tools is effective in identifying, recovering, and validating application-level digital evidence in Android-based cyberbullying investigations.

Keywords
Autopsy; Cyberbullying; DFRWS; MOBILedit Forensic; WeChat.

1. INTRODUCTION
Digital technology has revolutionized communication through platforms like WhatsApp, Telegram, and WeChat, but it has also catalyzed cyberbullying. Findings in [1] show that many cyberbullying cases in Indonesia originate from social media. WeChat is highly vulnerable due to its multi-functional communication features, while research [2] highlights that instant messaging loopholes allow digital harassment to remain untraced. This phenomenon challenges law enforcement due to low reporting rates and low digital literacy among victims, making forensics vital to secure legally admissible evidence [3].

To address these technical hurdles, the DFRWS framework provides a structured six-stage lifecycle for digital investigations. As noted in [4], DFRWS offers superior flexibility and adaptability for platforms like WeChat compared to alternative methods. Conversely, traditional NIST and NIJ frameworks are typically optimized for static local storage rather than closed applications. For instance, the NIJ method faces strict limitations when extracting data from encrypted social media [5], making DFRWS preferred for classifying complex bullying elements [6].

The robustness of this methodology has been demonstrated in diverse case studies, including detecting cyberbullying on Signal [7] and espionage on Facebook [8]. While research [3] highlights DFRWS's robust documentation system, study [9] emphasizes its importance in guaranteeing evidence authenticity on applications like TikTok. Although addressing cyberbullying remains legally challenging due to weak proof verification on social media [10], forensics solves this [11], allowing DFRWS to secure encrypted apps like WeChat via device cloning and local artifact analysis [12].

Beyond its technical superiority, DFRWS assists forensic experts through systematic modules [13] and easily integrates linguistic analysis to detect targeted hate speech [14]. It has also become a benchmark practice in Indonesia, including for forensic parsing of TikTok video content [15]. Consequently, this study applies the DFRWS framework combined with a qualitative approach to analyze WeChat communication patterns to enhance mobile investigation efficiency, protect vulnerable users, and secure digital artifacts for cyberbullying legal proceedings.

2. LITERATURE STUDY

2.1 Digital Forensics
Digital forensics investigates cybercrimes by identifying, collecting, analyzing, and presenting valid electronic evidence [1], ensuring its admissibility in legal proceedings [2]. Divided into computer, mobile, and network forensics to bypass native security mechanisms [3], its primary objective in cyberbullying cases is to map the logical correlation between the perpetrator, victim, device, and timeline.

2.2 Mobile Forensics
Mobile forensics is a specialized branch of digital forensics [4] that focuses on the recovery of digital evidence from mobile devices [5]. This field has become increasingly important in the modern era because smartphones serve as the primary communication medium for society, which conversely aligns with the increasing rate of criminal activities executed via mobile endpoints [6].

2.3 Cybercrime
Cybercrime refers to illicit activities perpetrated through computers, networks, or the internet to harm individuals, businesses, and government entities [7], [8]. Driven by technological advancements, these offenses include severe personal attacks like cyberbullying. Given that cybercrime is subject to specific criminal laws depending on the nature of the offense [9], digital forensics plays a critical role by applying standardized methodologies to trace digital footprints, secure authentic evidence, and identify perpetrators.

2.4 Cyberbullying
Cyberbullying is defined as the intentional, systematic, and repeated act of harassment or defamation within the digital

ecosystem, serving as a direct infringement of privacy and a severe personal attack [7].

2.5 Wechat

WeChat is a multi-purpose communication service developed by Tencent that provides comprehensive features such as private and group chats, voice messages, video calls, timeline moments, and various digital services [8]. Due to its extensive user base and the rich metadata stored within its local databases, WeChat frequently becomes a critical source of digital evidence in forensic investigations involving instant messaging communications.

2.6 Digital Evidence

Digital evidence is the data generated from electronic objects involved in a specific case [5], acquired from sources like computers and smartphones. This evidence encompasses text logs, metadata, system logs, and network artifacts, which are paramount to reconstructing event chronologies and identifying perpetrators, provided it maintains its authenticity and integrity without modifications.

2.7 Digital Forensics Research Workshop

The Digital Forensics Research Workshop (DFRWS) is a standardized methodology consisting of six systematic stages for handling cybercrime investigations: Identification, Preservation, Collection, Examination, Analysis, and Presentation [9]. This framework is widely adopted for providing a structured, scientific approach to managing digital evidence, ensuring investigators maintain the chain of custody and evidentiary integrity throughout the case lifecycle.

2.8 MOBILedit

MOBILedit Forensic is a specialized digital forensic toolkit engineered for data extraction from mobile devices. The software is utilized to identify, extract, and secure logical and physical digital evidence stored within mobile smartphone systems, ensuring the retrieved data remains forensically sound [9].

2.9 Autopsy

Autopsy is an open-source digital forensic platform used by forensic experts to analyze disk images and extract critical digital evidence. The tool is highly effective for file system analysis, keyword searching, timeline analysis, and identifying hidden or deleted information embedded within database artifacts and system files [9].

3. RESEARCH METHOD

This research applies the Digital Forensics Research Workshop (DFRWS) framework, which consists of six sequential stages: Identification, Preservation, Collection, Examination, Analysis, and Presentation, as illustrated in Figure 1.

Figure 1: Stage of the DFRWS Method

The process initiates with Identification (recognizing smartphones, WeChat accounts, and chat logs), followed by Preservation (maintaining data integrity) and Collection (extracting raw data using MOBILedit Forensic). During Examination, the extracted payload is parsed and verified using cryptographic hashes, leading to Analysis to reconstruct the chronology of the cyberbullying event. Finally, Presentation systematically documents these verified forensic findings into a legally sound report.

4. RESULT AND DISCUSSION

This section analyzes a simulated WeChat cyberbullying case on Android using a three-stage approach (pre-incident, incident, and post-incident) within the DFRWS framework. It maps chronological events from group creation to investigation, illustrating the interactions that generate extractable digital traces. The initial pre-incident simulation is shown in Figure 2.

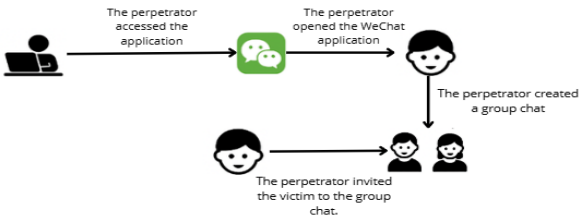


Figure 2: Pre-incident of Cyberbullying Case

During this initial phase, the perpetrator logs into WeChat, establishes a dedicated group chat, and populates it with several contact profiles along with the target victim before initiating any communication. Subsequently, the core criminal conflict occurs during the incident stage, which is depicted in Figure 3.

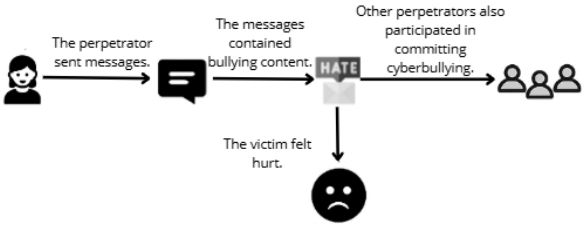


Figure 3: Incident of Cyberbullying Case

The incident stage captures the active cyberbullying offense, where the perpetrator disseminates explicit textual insults and defamatory remarks directed at the victim, thereby triggering other group members to participate in the harassment and inflicting severe emotional distress. The simulation concludes with the post-incident stage, as detailed in Figure 4.

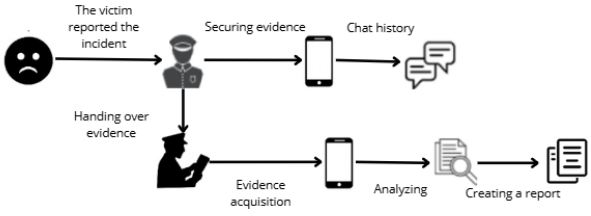


Figure 4: Post Incident of Cyberbullying Case

In this final phase, the victim files a formal complaint with law enforcement authorities by submitting preliminary chat screenshots. Upon receiving the report, investigators seize the smartphones of both parties under a strict chain of custody,

utilizing *MOBILedit Forensic* and *Autopsy* to extract and authenticate the digital artifacts required for legal proceedings.

4.1 Identification

During the Identification stage, an initial assessment was conducted to detect cyberbullying activities within WeChat based on a formal complaint filed by the victim, which included chat screenshots as investigative leads, as illustrated in Figure 5.

Figure 5: Screenshot of Chat Conversation Evidence

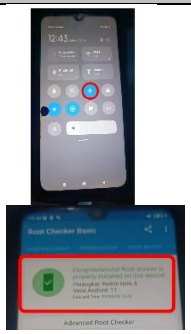
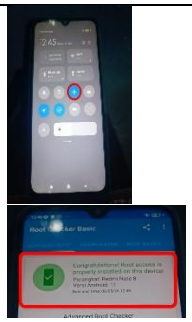
Forensic linguistic analysis of the screenshots revealed verbal harassment containing explicit slurs ("goblok", "bego", "gendut", "beban", and "cupu") sent by accounts "Djoko Sumitro" and "Djoko Putim" between April 30 and May 1, 2026, within a shared group chat.

Although providing critical direction, these screenshots are highly susceptible to manipulation and insufficient as standalone evidence. Consequently, this phase established the baseline to seize the physical smartphones of both the victim and suspects for untampered data acquisition.

4.2 Preservation

The Preservation stage was executed to maintain the chain of custody and data integrity throughout the forensic lifecycle. Upon seizure, both mobile devices were immediately isolated from external networks by enabling airplane mode to block cellular, Wi-Fi, and Bluetooth signals, mitigating the risk of remote-wiping or automatic data synchronization. The baseline preservation metadata for both endpoints are documented in Table 1.

Table 1: Preservation Table

Device name	Photo	Description
Victim's Smartphone (Redmi Note 8)		Isolated in airplane mode; verified in a pre-rooted state via Magisk, allowing administrative access for deep database extraction.
Perpetrator's Smartphone (Redmi Note 8)		Isolated in airplane mode; verified in a pre-rooted state via Magisk, ensuring readiness for physical acquisition without altering user data partitions.

Securing both devices in a pre-rooted state facilitates advanced data extraction without compromising core system partitions. By establishing these isolation protocols, the digital evidence remains untampered and forensically sound, ensuring that the analytical results derived under the DFRWS framework are legally admissible.

4.3 Collection

The Collection stage encompasses the systematic acquisition of digital evidence from the target Android devices via MOBILedit Forensic. Because both endpoints were pre-rooted, an advanced database extraction method was applied to bypass standard application sandbox restrictions, granting direct access to the root file systems where WeChat data resides without altering user files.

The forensic extraction isolated volatile and non-volatile WeChat artifacts, specifically targeting local database files containing chat histories, account profiles, and timestamps. Immediately following acquisition, the forensic software generated cryptographic hashes (MD5 and SHA-256) for each extracted file image to serve as the baseline for integrity verification, ensuring the data remains untampered during subsequent phases.

4.3.1 Collection of the perpetrator's smartphone

The primary evidence secured from the suspect consisted of an operational, unlocked Android smartphone with the WeChat application installed. The hardware specifications of this device are detailed in Table 2.

Table 2: Perpetrator's Evidence Table

Evidence Name	Photo	Description
Smartphone		Redmi Note 8 model, blue color, and in a rooted state. It has specifications of a Snapdragon 665 chipset, 4 GB RAM, and 64 GB storage.

Investigators enabled USB Debugging, allowing the forensic workstation to interface with the device's pre-existing Magisk root architecture for full superuser permissions. Data acquisition was executed using MOBILedit Forensic, performing an advanced extraction of protected WeChat directories containing chat databases and metadata logs, as illustrated in Figure 6.

Figure 6: Perpetrator's Smartphone Extraction Process

The software generated a structured output directory of compiled forensic reports and raw system exports, as documented in Figure 7.

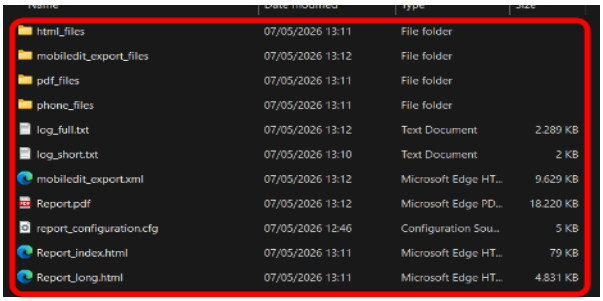


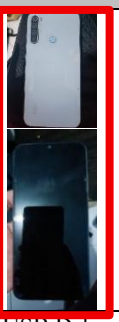
Figure 7: Perpetrator's Smartphone Extraction Results

The resulting extraction payload was securely written to the dedicated investigation directory: E:\EKSTRAKSI SKRIPSI\COLLECTION\HP PELAKU\Xiaomi Redmi Note 8 (HP PELAKU) (2026-05-07 12h46m39s). To preserve data integrity, a cryptographic hash value was computed for the entire directory prior to analysis.

4.3.2 Collection of the victim's smartphone

The secondary evidence secured from the victim consisted of an operational, unlocked Android smartphone with the WeChat application installed. The hardware specifications of the victim's device are detailed in Table 3.

Table 3: Victim's Evidence Table

Evidence Name	Photo	Description
Smartphone		Redmi Note 8 model, white color, and in a rooted state. It has specifications of a Snapdragon 665 chipset, 4 GB RAM, and 64 GB storage.

Investigators enabled USB Debugging to interface the forensic workstation with the device's pre-existing Magisk root architecture for full superuser permissions. Data acquisition was executed using MOBILedit Forensic, performing an advanced extraction of protected WeChat directories containing chat databases and metadata logs, as illustrated in Figure 8.

Figure 8: Victim's Smartphone Extraction Process

The software generated a structured output directory containing compiled forensic reports and raw system exports, as documented in Figure 9.

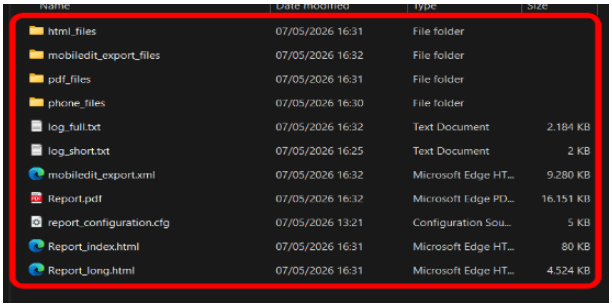


Figure 9: Victim's Smartphone Extraction Results

The resulting extraction payload was securely written to the dedicated investigation directory: E:\EKSTRAKSI SKRIPSI\COLLECTION\HP KORBAN\Xiaomi Redmi Note 8 (HP KORBAN) (2026-05-07 13h20m58s). To preserve data integrity, a cryptographic hash value was computed for the entire directory prior to analysis.

4.4 Examination and Analysis

Prior to analysis, duplicate copies of the extracted directories were generated as working copies to ensure the master forensic images remained unaltered. All subsequent operations were performed exclusively on these validated copies, as documented in Figure 10.

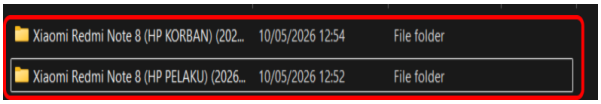


Figure 10: Duplication of Forensic Extraction Data

Deep forensic analysis was conducted using the Autopsy platform. The extracted database files from both smartphones were ingested into the forensic workstation for automated data indexing and metadata parsing to reconstruct application-level digital traces within the WeChat directory.

To optimize artifact recovery, a structured keyword search was executed within Autopsy utilizing a pre-defined dictionary of derogatory terms. This targeted search rapidly isolated conversation strings containing cyberbullying elements. Concurrently, metadata examination on the isolated chat artifacts extracted immutable communication timestamps and network identities, precisely mapping the chronological links between the suspect and the victim.

Ultimately, these findings provide an objective, accurate, and verifiable reconstruction of the cyberbullying activities within the WeChat application, satisfying the requirements of legal admissibility.

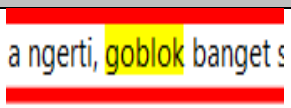
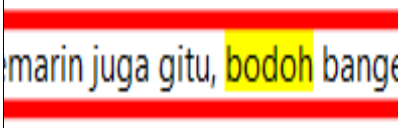
4.4.1 Analysis of the Perpetrator's Smartphone

The forensic analysis of the perpetrator's smartphone was conducted utilizing the validated working copy within the Autopsy platform to preserve evidence integrity. The automated data indexing and parsing phase is illustrated in Figure 11.

Figure 11: Perpetrator Data Indexing Process

Following indexing, a targeted keyword search was executed within Autopsy to isolate conversation logs matching the defamatory harassment patterns. The recovered artifacts are summarized in Table 3.

Table 3: Perpetrator Cyberbullying Artifacts

Photo	Description
	Successfully recovered explicit cyberbullying text containing the derogatory term **"goblok"** sent by the account profile **"Djoko Sumitro"** within the group chat titled **"Tugas Kelompok"**.
	Successfully recovered explicit cyberbullying text containing the derogatory term **"bodoh"** sent by the account profile **"Djoko Sumitro"** within the group chat titled **"Tugas Kelompok"**.

The conversation threads demonstrate a repetitive pattern of direct verbal abuse. Within the DFRWS framework, these operations satisfy the Analysis stage. To ensure absolute authenticity, the artifacts were cross-verified using MOBILedit Forensic and Autopsy.

Furthermore, a comparative timestamp analysis was conducted between the source extraction directory and the processed output to confirm that the operations did not modify the data layer, as illustrated in Figure 12.

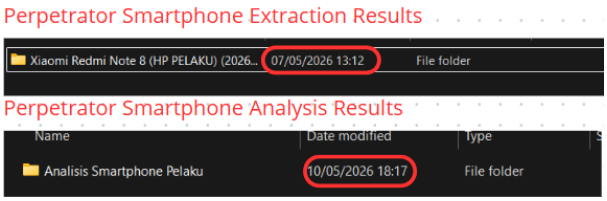


Figure 12: Perpetrator Timestamp Integrity

The chronological values in Figure 12 demonstrate an absolute correlation between the MAC times (Modified, Accessed, Created) of the raw and parsed data. This lack of variance proves that Autopsy operated in a read-only environment, validating the legal admissibility of the evidence.

4.4.2 Analysis of the Victim's Smartphone

The forensic analysis of the victim's smartphone was conducted by ingesting the validated working copy into Autopsy for automated data indexing and parsing, as illustrated in Figure 13.

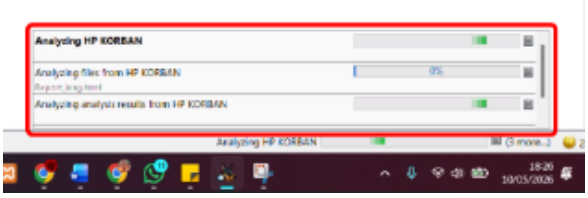
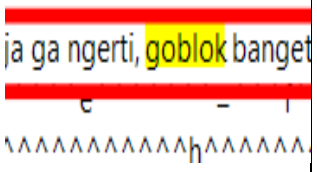
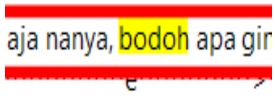
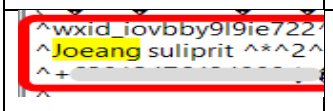
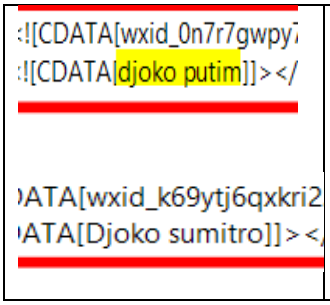


Figure 13: Victim Data Indexing Process

Following indexing, targeted keyword searches isolated conversation strings matching derogatory slurs and system-generated unique WeChat identifiers (wxid). The verified forensic findings are summarized in Table 4.

Table 4: Victim Cyberbullying Artifacts

Photo	Description
	Successfully recovered explicit cyberbullying text containing the derogatory term **"goblok"** sent by the account profile **"Djoko Sumitro"** within the group chat titled **"Tugas Kelompok"**.
	Successfully recovered explicit cyberbullying text containing the derogatory term **"bodoh"** sent by the account profile **"Djoko Putim"**.
	Successfully extracted system registry metadata identifying the victim as **"Joeang Suliprit"** (wxid_iovbby9l9ie722), and the suspects as **"Djoko Putim"** (wxid_0n7r7gwpy76m2

	2) and **"Djoko Sumitro"** (wxid_k69ytj6qxkri22).

A total of 12 distinct conversations containing cyberbullying elements were isolated from the victim's WeChat database. User profile data was mapped from local group membership logs to establish accountability, as documented in Table 5.

Table 5: Participant Identity Log

Username	Account Display Name	Forensic Role Assignment
wxid_iovbby9l9ie722	Joeang Suliprit	Victim
wxid_0n7r7gwpy76m22	Djoko Putim	Suspect / Perpetrator
wxid_k69ytj6qxkri22	Djoko Sumitro	Suspect / Perpetrator

This structural mapping links specific accounts directly to the criminal offense. To mathematically confirm that the analysis did not alter the underlying data layer, a comparative timestamp analysis was executed, as illustrated in Figure 14.

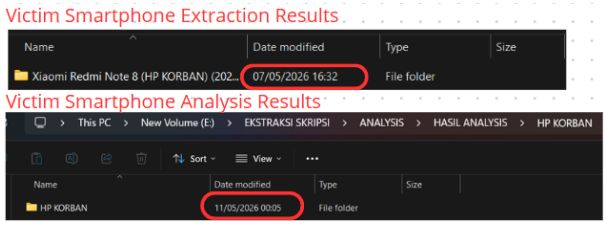


Figure 14: Victim Timestamp Integrity

The chronological values in Figure 14 demonstrate an absolute correlation between the MAC times (Modified, Accessed, Created) of the raw and parsed data. This lack of variance proves that Autopsy operated in a read-only environment, validating the legal admissibility of the digital evidence.

4.5 Presentation

The Presentation stage documents and presents the digital artifacts recovered from the validated working copies using MOBILedit Forensic and Autopsy. This reporting provides an objective summary of cyberbullying evidence found in WeChat. The aggregated forensic findings from both devices are summarized in Table 6.

Table 6: Evidence Findings Report

No	Artifact Classification	Forensic Status	Key Investigative Metadata
1	WeChat Account Data	Recovered	Account profiles and legal identities mapped
2	WeChat Chat Logs	Recovered	Abusive cyberbullying message payloads identified
3	Chat Timestamps	Not Found	-

As structured in Table 6, the investigation exposed critical evidence channels establishing undeniable links between the suspect profiles and the defamatory text streams. To map the technical correlation between the two seized endpoints, a comparative keyword cross-reference was executed using *MOBILedit*, focusing on the specific verbal insults defined in the research scope, as detailed in Table 7.

Table 7: Device Keyword Comparison

No	Targeted Cyberbullying Keyword	Victim's Smartphone	Suspect's Smartphone
1	“Goblok”	3 Recovered	1 Recovered
2	“Bodoh”	3 Recovered	1 Recovered
3	“Cupu”	3 Recovered	2 Recovered
4	“Beban”	2 Recovered	2 Recovered
5	“Gendut”	1 Recovered	0 Recovered

As shown in Table 7, a discrepancy exists regarding the volume of recovered keyword strings, where the victim’s device retained a higher density of abusive messages. This artifact variance is heavily influenced by mobile-specific variables, such as selective manual deletion by the perpetrator, background synchronization differences, or localized hardware extraction limitations. To visually conceptualize the evidentiary ratio between the endpoints, the aggregated keyword metrics are visualized in Figure 15.

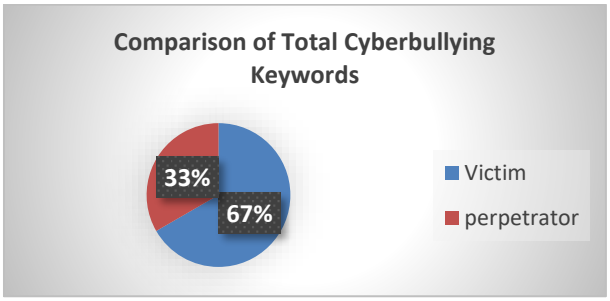


Figure 15: Keyword Distribution Diagram

Based on the evidence chart in Figure 15, 67% of the total abusive artifacts were securely parsed from the victim's smartphone, while the suspect's device yielded the remaining 33%. This output validates the effectiveness of dual-endpoint extraction.

These findings indicate that the digital artifacts recovered from both devices are mutually supportive and provide stronger evidential value than relying on evidence obtained from a single device. Therefore, conducting forensic analysis on both the suspect's and victim's smartphones contributes to a more comprehensive reconstruction of cyberbullying incidents.

4.6 Evaluation and Discussion

The results of this study demonstrate that the Digital Forensics Research Workshop (DFRWS) framework provides a systematic approach for investigating cyberbullying cases on the WeChat application. By following the six investigation stages, namely Identification, Preservation, Collection, Examination, Analysis, and Presentation, the forensic investigation was successfully conducted while maintaining the integrity of the digital evidence through cryptographic hash verification. The combination of MOBILedit Forensic and Autopsy also enabled investigators to recover application-level artifacts efficiently from Android smartphones.

The forensic investigation successfully recovered various categories of digital evidence, including user account information, chat conversations, communication metadata, and cyberbullying-related keywords. The recovered evidence from both smartphones complemented each other and strengthened the reconstruction of the cyberbullying incident. This cross-device verification increased the reliability of the investigation because similar artifacts were identified from both the victim's and the suspect's devices.

The comparison of the forensic results indicates that the victim's smartphone contained a larger number of recovered cyberbullying conversations than the suspect's smartphone. Specifically, twelve conversations were recovered from the victim's device, whereas six conversations were identified from the suspect's device. Likewise, the victim's smartphone contained 67% of the identified cyberbullying keywords, while the suspect's smartphone contained 33%. This discrepancy may be attributed to differences in local data synchronization, selective deletion of conversations by the suspect, application cache behavior, or variations in the remaining database artifacts available during extraction.

Furthermore, the use of two forensic tools contributed to improving the completeness of the investigation. MOBILedit Forensic was effective for extracting data from rooted Android devices, whereas Autopsy facilitated comprehensive artifact analysis through indexing, keyword searching, and metadata examination. The integration of these tools under the DFRWS framework allowed digital evidence to be identified, analyzed, and validated systematically.

Although the proposed approach successfully identified digital evidence related to cyberbullying on WeChat, this study was limited to a single simulated investigation involving two Android smartphones with similar hardware specifications. Future research may evaluate additional cyberbullying scenarios involving different Android versions, various WeChat releases, deleted-message recovery, and comparisons with other forensic methodologies to further validate the effectiveness of the proposed investigation approach.

5. CONCLUSIONS

Based on the research findings, it can be concluded that the Digital Forensics Research Workshop (DFRWS) framework was successfully implemented to investigate cyberbullying cases on the WeChat application through its six systematic stages: Identification, Preservation, Collection, Examination, Analysis, and Presentation. By integrating MOBILedit Forensic for data acquisition and Autopsy for artifact analysis, the investigation successfully recovered and validated critical digital evidence, including user account information, chat conversations containing cyberbullying content, and application metadata.

The evaluation results demonstrate that the proposed approach effectively supports the recovery and verification of digital evidence from both the suspect's and the victim's smartphones. A comparative analysis revealed that the victim's device contained a higher number of recovered cyberbullying conversations (12 conversations, representing 67% of the identified artifacts) than the suspect's device (6 conversations, representing 33%). This difference may be influenced by factors such as data synchronization, selective deletion of messages, or variations in locally stored application artifacts. The consistency of the recovered evidence from both devices indicates that cross-device analysis improves the reliability of reconstructing cyberbullying incidents and strengthens the forensic findings.

Overall, the integration of the DFRWS framework with MOBILedit Forensic and Autopsy provides a systematic and reliable approach for recovering, validating, and analyzing application-level digital evidence from Android-based WeChat investigations. Future research may extend this work by evaluating additional cyberbullying scenarios involving different Android versions, various WeChat releases, deleted-message recovery, and comparisons with other forensic tools or forensic methodologies to further validate and improve the effectiveness of mobile forensic investigations.

6. REFERENCES

[1] C. Cahyono, “Pengaruh Penggunaan Media Digital dan Peran Keluarga Terhadap Perilaku Sosial Para Remaja,” Jurnal Inovasi Pendidikan MH Thamrin, vol. 6, no. 1, pp. 114–124, Mar. 2022, doi: 10.37012/jipmht.v6i1.769.

[2] A. Prayogo, U. Dahlan, and I. Riadi, “Digital Forensic Signal Instant Messages Services in Case of Cyberbullying using Digital Forensic Research Workshop Method,” IJCA (Indonesian Journal of Chemical Analysis), vol. 184, pp. 975–8887, Oct. 2022, doi: 10.5120/ijca2022922393.

[3] I. Riadi, S. Sunardi, and P. Widiandana, “Cyberbullying Detection on Instant Messaging Services using Rocchio and Digital Forensics Research Workshop Framework,” Journal of Engineering Science and Technology, vol. 17, pp. 1408–1421, Apr. 2022.

[4] I. Riadi, S. Sunardi, and P. Widiandana, “Mobile Forensics for Cyberbullying Detection using Term Frequency - Inverse Document Frequency (TF-IDF),” Jurnal Ilmiah Teknik Elektro Komputer dan Informatika, vol. 5, pp. 68–76, Dec. 2019, doi: 10.26555/jiteki.v5i2.14510.

[5] Y. Arif, E. Alwi, and M. Asis, “Analisis Bukti Digital Direct Message Pada Twitter Menggunakan Metode National Institute Of Justice (NIJ),” INFORMAL:

Informatics Journal, vol. 8, p. 165, Aug. 2023, doi: 10.19184/isj.v8i2.34025.

[6] B. Sharma, N. Singh, S. Beniwal, and M. T. Beig, "Analyses of Social Media Networks Investigation in India -A Brief Overview," African Journal of Biological Sciences, vol. 6, pp. 4482–4493, Jun. 2024, doi: 10.33472/AFJBS.6.10.2024.4482-4493.

[7] B. Prasetyo and I. Riadi, "Investigation Cyberbullying on Kik Messenger using National Institute of Standards Technology Method," Int. J. Comput. Appl., vol. 172, pp. 34–41, Feb. 2021, doi: 10.5120/ijca2021921060.

[8] J. Triyanto and I. Riadi, "Analisis Investigasi Cyber espionage pada Facebook Menggunakan Digital Forensics Research Workshop (DFRWS)," vol. 23, no. 1, pp. 39–46, 2022, [Online]. Available: http://jurnalnasional.ump.ac.id/index.php/Techno

[9] H. S. Mikayla, A. Kusyanti, and P. H. Trisnawan, "Analisis Forensik Digital untuk Investigasi Kasus Cyberbullying pada Media Sosial Tiktok," Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 11, no. 5, pp. 1113–1124, Oct. 2024, doi: 10.25126/jtiik.2024118017.

[10] Marjun, Saroji, and F. Farhan, "Cyberbullying and Legal Protection for Victims in the Digital Era: A Case Study on Social Media Platforms," Hakim: Jurnal Ilmu Hukum dan Sosial, vol. 3, no. 1, pp. 955–973, Feb. 2025, doi: 10.51903/hakim.v3i1.2290.

[11] M. Rosita, "Analisis Komparatif Performa FTK Imager dan Autopsy dalam Forensik Digital pada Flashdisk."

[12] G. C. Fernandez, "Panduan Menumpas Cyberbullying dan Cybercrime di lingkungan reguler", inklusi dan SLB. 2023.

[13] K. Mmtc, A. Purwanti, I. Svinarky, Z. Nurhadi, and U. Salamah, "Pembinaan Etika Komunikasi Melalui Media Sosial Yang Sesuai Dengan Hukum Pada Remaja (Development of Communication Ethics Through Social Media In Accordance With The Law In Teenagers)," vol. 3, pp. 347–363, Jun. 2023, doi: 10.52434/medikom.v3i1.47.

[14] A. Syahid, D. Sudana, and A. D. Bachari, "Perundungan Siber (Cyberbullying) Bermuatan Penistaan Agama di Media Sosial yang Berdampak Hukum: Kajian Linguistik Forensik," Semantik, vol. 11, no. 1, pp. 17–32, Feb. 2022, doi: 10.22460/semantik.v11i1.p17-32.

[15] A. Q. I. Hidayat, E. I. Alwi, and A. W. M. Gaffar, "Studi Forensik Digital: Analisis Bukti Video TikTok dengan Metode DFRWS," Jurnal Minfo Polgan, vol. 13, no. 1, pp. 1138–1146, Aug. 2024, doi: 10.33395/jmp.v13i1.13966.

[16] I. Yuadi, S. Sos, and M. MT, Forensik Digital dan Analisis Citra. Cv. Ae Media Grafika, 2023.

[17] M. Salim et al., Pengantar Forensik Digital, 1st ed. Agam: Yayasan Tri Edukasi Ilmiah, 2024. Accessed: Jun. 22, 2025. [Online]. Available: https://books.google.co.id/books?hl=en&lr=&id=ASQ-EQAAQBAJ&oi=fnd&pg=PA1&dq=forensik+digital&ots=DAuvR0T6P7&sig=_I89SoJWy2-2Br8Kt5AVEkQwqJ8&redir_esc=y#v=onepage&q=forensik%20digital&f=false

[18] D. Hariyadi, Buku Panduan Dasar Forensik Digital. 2022.

[19] D. Mualfah and M. I. Syam, "Analisis perbandingan tools mobile forensic menggunakan metode national institute of justice (NIJ)," Jurnal CoSciTech (Computer Science and Information Technology), vol. 4, no. 1, pp. 283–292, 2023.

[20] T. Ruslan, I. Riadi, and S. Sunardi, "Analisis Forensik Digital Pada Whatsapp Dan Facebook Menggunakan Metode NIST," Jurnal Fasilkom, vol. 13, no. 02, pp. 286–292, 2023.

[21] T. Ruslan, I. Riadi, and S. Sunardi, "Forensik Multimedia Berbasis Mobile Menggunakan Metode National Institute of Justice," Jurnal SAINTEKOM, vol. 12, pp. 69–80, Mar. 2022, doi: 10.33020/saintekom.v12i1.210.

[22] F. Y. N. Sufi, D. K. Putri, and D. Suhartini, "Analisis Ancaman Cybercrime dan Peran Sistem Biometrik: Systematic Literature Review," in Seminar Nasional Akuntansi dan Call for Paper, 2023, pp. 19–29.

[23] H. Wijoyo, B. Jange, and F. Wongso, "Cyber Crime," 2024, pp. 9–22.

[24] R. Pansariadi and N. Soekorini, "Tindak Pidana Cyber Crime dan Penegakan Hukumnya," Binamulia Hukum, vol. 12, pp. 287–298, Dec. 2023, doi: 10.37893/jbh.v12i2.605.

[25] K. Rovida and S. Sasmini, "Evaluasi Sistem Hukum Indonesia dalam Menangani Cyberbullying Berbasis Teknologi Informasi dan Komunikasi," DIVERSI: Jurnal Hukum, vol. 10, no. 1, pp. 169–205, 2024.

[26] R. Handaya, "Manfaat Aplikasi WeChat Sebagai Media Interaksi Bagi Mahasiswa Fakultas Ilmu Komunikaasi Universitas Islam Riau," Universitas Islam Riau, Pekanbaru, 2020. Accessed: Jun. 22, 2025. [Online]. Available: https://repository.uir.ac.id/8288/1/139110115.pdf

[27] D. Yuliana, T. Yuniati, and B. P. Zen, "Analisis Forensik Terhadap Kasus Cyberbullying pada Instagram Dan Whatsapp Menggunakan Metode National Institute of Justice (NIJ)," Cyber Security dan Forensik Digital, vol. 5, no. 2, pp. 52–59, 2023.