Digital Forensic Analysis of TikTok Application in Defamation Cases using Digital Forensics Research Workshop Method

Arfin Nurhakim Mansur
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
The development of social media platforms such as TikTok not only provides benefits but also triggers cybercrimes, one of which is defamation. This study aims to uncover digital evidence in such cases using the Digital Forensics Research Workshop (DFRWS) method, which includes identification, preservation, collection, examination, analysis, and reporting. The extraction process was conducted using MOBILedit Forensics Express, Oxygen Forensic Detective, and DB Browser for SQLite. The results show that Oxygen achieved the highest success rate of 92% with 12 artifacts, while both MOBILedit and DB Browser achieved 85% with 11 artifacts each. Cross-validation ensured the authenticity of the digital evidence, proving that the DFRWS method is effective in TikTok forensic investigations and can support law enforcement in handling defamation cases on social media.

Keywords
Digital Forensics, Defamation, DFRWS, TikTok, Digital Evidence, Cybercrime.

1. INTRODUCTION
The development of information technology has brought significant changes to society, including shifts in behavior, ethics, and values due to the emergence of social media[1]. Social media has a positive impact on social change but also generates negative effects, such as the erosion of societal norms[2]. One of the most popular platforms is TikTok, which is widely used by various groups in Indonesia[3]. Its user base continues to grow daily, making it the most downloaded application in 2021[4][5]. Globally, by early 2024, TikTok had reached 1.56 billion active users, solidifying its position as one of the largest social media platforms in the world[6].

TikTok's popularity is also driven by feature innovations, such as the increase in video duration from 60 seconds to 3 minutes, and later up to 10 minutes in 2022[7]. However, the rise in social media usage has also been followed by an increase in cybercrimes, including defamation, bullying, and fraud[7][8]. Data from the Indonesian National Police (Polri) recorded a 37% increase in defamation cases, from 118 cases in January 2021 to 162 cases in January 2022, along with an increase in the number of regional police departments handling these cases, from 23 to 27[9][10]. This fact underscores that social media not only provides a space for expression but also carries a high potential for misuse.

To address this issue, digital forensics serves as an effective method for uncovering the truth of digital evidence and identifying perpetrators [11]. Various digital forensic approaches exist, such as the Digital Forensics Research Workshop (DFRWS), the National Institute of Justice (NIJ), the National Institute of Standards and Technology (NIST), the Systematic Digital Forensics Investigation Model (SRDFIM), and the Integrated Digital Forensic Investigation Framework (IDFIF). In this study, the DFRWS method was chosen because it provides systematic stages for acquiring, validating, and presenting digital evidence. This research focuses on the forensic analysis of defamation cases on TikTok using the MOBILedit Forensics tool[11].

2. LITERATURE REVIEW
2.1 Digital Forensics
Digital forensics is a branch of forensic science that focuses on extracting data from electronic evidence and processing it into intelligence data. This data can then be used for further actions and presented as evidence in legal prosecutions[12].

2.2 Stages of Digital Forensics
The stages of digital forensics begin with identification, which is the initial and fundamental process of determining the location, form, and storage method of digital evidence in order to facilitate the subsequent investigative steps. This is followed by preservation, considered the most critical and delicate stage, since any errors or negligence in maintaining the integrity of evidence may result in data loss, contamination, or reduced authenticity. The next stage is analysis, where the collected and preserved evidence is carefully processed, examined, and interpreted using appropriate forensic techniques to produce information that is relevant, accurate, and meaningful to the case. The final stage is presentation, which not only focuses on verifying and demonstrating the authenticity of the evidence but also aims to establish a clear relationship between the forensic findings and the case under investigation, ensuring that the results can be presented credibly in legal proceedings[12]. A summary of these stages can be seen in Figure 1, which illustrates the digital forensics process.

Figure 1: Digital Forensics Process

2.3 Digital Evidence
Digital evidence refers to the results of extraction or recovery from electronic devices, such as documents, email accounts, contacts, text messages, media files (audio, images, and video), as well as log files[13]. In cybercrime investigations, digital evidence needs to be managed using a forensic framework to ensure more efficient and effective collection and analysis. In practice, digital evidence is often associated with the use of

social media as a medium for committing crimes. However, digital evidence is highly susceptible to alteration, meaning that any modification may raise doubts about its authenticity. Even the slightest change has the potential to produce misleading conclusions and render the evidence inadmissible in legal proceedings. Therefore, maintaining the validity of digital evidence is crucial in the forensic process[14].

2.4 Tiktok

TikTok is a social media application that provides a wide variety of creative videos with audio backgrounds that users can utilize to create content[15]. This convenience allows users to produce unique videos that attract audience attention, making TikTok not only a source of entertainment but also an influential factor in social life, including aspects of language ethics. As a music-based platform, TikTok initially limited video duration to only 15 to 60 seconds. However, along with the increasing demand from content creators to engage viewers, in February 2022 TikTok extended the upload duration to up to 10 minutes[7].

2.5 Cybercrime

Cybercrime is a criminal act that exploits computer technology and the internet as its primary tools[13] often targeting computers as victims[16]. This activity is defined as a legal violation carried out through the use of information and communication technology, and over time it has evolved into a serious global threat. According to reports from PwC and RSA, the losses caused by cybercrime can even equal the national income of a country. This indicates that cybercrime has developed into an industry with high returns but relatively low risk[17]. In general, cybercrime can be categorized into three groups: crimes related to the confidentiality, integrity, and availability of data and computer systems; crimes in which computers are used as tools to commit offenses; and crimes concerning digital content[18].

2.6 Digital Forensic Tools

In the process of digital forensic investigation, several tools are employed according to their respective features and functionalities. MOBILedit Forensics Express is a forensic software capable of extracting, analyzing, and generating reports from smartphone data. This tool can retrieve various types of information, including deleted data, contacts, call history, text and multimedia messages, photos, videos, recordings, notes, reminders, calendars, passwords, as well as data from popular applications such as Facebook, WhatsApp, Signal, WeChat, Dropbox, Evernote, Skype, and Viber[19]. Meanwhile, Oxygen Forensics Detective is a software solution that supports data extraction from mobile devices, IoT, and cloud services[20]. This tool offers broad coverage with support for more than 45,000 applications and thousands of devices, equipped with features such as full file system extraction, timeline, social graphing, and location analysis. Moreover, Oxygen Forensic Detective can also import data from applications like TikTok, enabling digital artifacts such as conversations, metadata, and account activities to serve as crucial evidence in an investigation[21].

2.7 Digital Forensics Research Workshop (DFRWS)

The Digital Forensics Research Workshop (DFRWS) method is a widely used approach in digital forensic analysis to identify cybercrimes while also providing a centralized mechanism for recording and presenting evidence[22][23]. This method consists of six main stages, namely: identification, which determines the requirements and sources of evidence; preservation, to maintain the authenticity of data; collection, which involves acquiring digital evidence from various sources; examination, where data is filtered and prepared without altering its content; analysis, to assess the validity and effectiveness of forensic tools; and presentation, which systematically delivers the investigation results in an accessible and comprehensible manner[24].

3. RESEARCH METHOD

This research employs the Digital Forensics Research Workshop (DFRWS) method, which is one of the approaches commonly used in digital forensic analysis to indicate a digital crime[25]. The method consists of six main stages: Identification, Preservation, Collection, Examination, Analysis, and Presentation, as illustrated in Figure 2.

Figure 2: Stages of the DFRWS Method

Figure 2 illustrates the stages of the Digital Forensics Research Workshop (DFRWS) method, which consists of six main steps: identification, as the initial process to determine data requirements and sources of digital evidence; preservation, to maintain the authenticity of evidence and prevent alteration or manipulation; collection, as the stage of gathering data from relevant sources in a structured and well-documented manner; examination, which focuses on filtering significant data without altering its content; analysis, to understand the context and relationships among data in order to uncover the perpetrator's actions; and finally, presentation, which systematically delivers the analysis results along with explanations of the methods, tools, and supporting recommendations.

4. RESULTS AND DISCUSSION

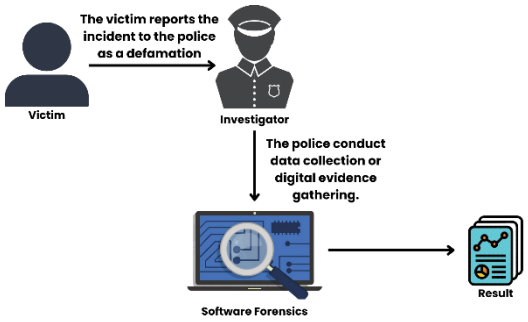
This research focuses on a cybercrime case involving defamation conducted through the TikTok application on an Android-based device. The case scenario is divided into three stages: pre-incident, incident, and post-incident.

Figure 3: Pre-Incident Stage

Figure 3 shows the pre-incident stage, where the victim creates and posts a video on their TikTok account to gain appreciation in the form of likes and comments from followers. The victim's video then appears on the perpetrator's TikTok feed, even though the perpetrator had not previously followed the victim's account. The perpetrator, who had disliked the victim from the beginning, felt disturbed and envious after viewing the victim's video.

Figure 4: Incident Stage

Figure 4 show the perpetrator, who dislikes the victim, initiating an act of defamation by sending direct messages (DMs) and posting comments on the victim's posts, as well as uploading a video containing slanderous content. The victim, upon seeing the perpetrator's posts and messages, felt harmed.



Gambar5: Post-Incident Stage

Figure 5 shows the victim, who felt harmed and did not accept the perpetrator's posts and messages, reporting the perpetrator to the police on charges of defamation. The victim explained the chronology of events and submitted preliminary evidence in the form of screenshots of the video and messages that had been sent by the perpetrator before being deleted. The police then conducted an investigation and examination of the devices and accounts used by the perpetrator. This process was carried out using forensic tools to extract and analyze data. From the results of the investigation, the police obtained valid and accountable digital evidence.

4.1 Identification

In the first stage, namely Identification, the process involves determining the sources of digital evidence and the devices involved, with the TikTok application as the main object of analysis. The identification focuses on relevant data such as comments, direct messages (DMs), and videos uploaded by the perpetrator, as well as the devices and tools used. The evidence analyzed was a Xiaomi Redmi 6A smartphone, as shown in Figure 6.

Figure 6: Smartphone Evidence

In addition, a documentation process was carried out to record important information from the smartphone, such as the device brand and model, operating system, storage capacity, and International Mobile Equipment Identity (IMEI) number. The specifications of the device are presented in Table 1.

Table 1. Device Specifications

No.	Spesification	Description
1.	Brand	Xiaomi Redmi 6a
2.	Operating System	Android 9
3.	Internal Memory	16 GB
4.	RAM	2 GB
5.	IMEI 1	860323044326546
6.	IMEI 2	860323044326556

Table 1 shows the specifications of the device used as the primary source of digital evidence in this research, including the brand, operating system, internal memory, RAM, and IMEI information.

Table 2. Research Tools

No.	Research Tools	Description
1.	Laptop	ASUS VivoBook AMD Ryzen 3 4300U
2.	Smartphone	Redmi 6a
3.	USB Cable	Connector data extraction
4.	Tiktok	Social media aplication

Table 2 show the devices used in this study, consisting of a laptop as the analysis medium, a Redmi 6A smartphone as the research object, a USB cable for the data extraction process, and the TikTok application as the primary source of digital evidence.

Table 3. Forensic Tools

No.	Forensics Tools	Description
1.	*MOBILedit Forensics Express*	Windows application for extracting smartphone data
2.	*Oxygen Forensics Detectine*	Windows application for extracting smartphone data
3.	*DB Browser for SQLite*	Windows application for extracting smartphone data

Table 3 show the forensic tools used in this study, namely MOBILedit Forensics Express for data extraction, Oxygen Forensic Detective for advanced analysis, and DB Browser for SQLite for reading and verifying the TikTok application database.

4.2 Preservation

The preservation stage is an essential process to maintain the integrity of digital evidence so that it remains intact, unaltered, and valid for further analysis. The initial step was carried out by isolating the device using airplane mode, thereby disconnecting it from cellular networks, Wi-Fi, and Bluetooth. In this way, the risk of data modification due to synchronization or updates can be prevented. The isolation process is shown in Figure 7.

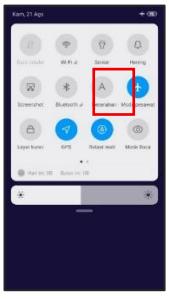


Figure 7: Device Isolation Using Airplane Mode

Figure 7 shows the smartphone device being isolated using airplane mode as supporting evidence that the preservation procedure was carried out in accordance with standards to maintain the authenticity of the digital evidence.

4.3 Collection

4.3.1. Collection using Mobiledit Forensics Express

The collection process was carried out using MOBILedit Forensics Express, which was connected via a USB cable. This tool was chosen because it is capable of copying and documenting digital artifacts from the TikTok application. By connecting the smartphone to the laptop, the data acquisition process could be performed directly. The extraction display can be seen in Figure 8.

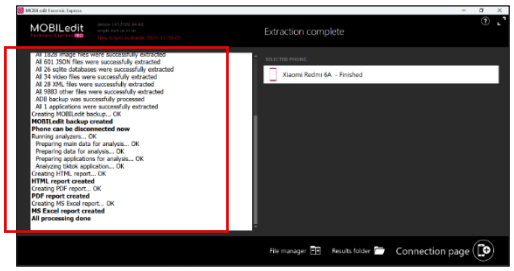


Figure 8: MOBILedit Extraction Process

Figure 8 shows the data extraction process on the Xiaomi Redmi 6A device carried out using MOBILedit Forensics Express. The display indicates that all files, databases, and application artifacts were successfully extracted and automatically processed into report formats such as PDF, HTML, and Excel. This process serves as an essential stage in digital forensic analysis, ensuring that all potential evidence is securely preserved and ready for examination.

4.4.2. Collection using Oxygen Forensic Detective

In addition to using MOBILedit Forensics Express, the collection process was also carried out with Oxygen Forensic Detective, which provides various extraction methods such as Android Agent, Backup, Physical, and Full File System. At this stage, the extraction was performed using the full file system method, as it is capable of obtaining data comprehensively, thereby providing broader data coverage. By using this method, the entire directory, databases, and application files on the device could be acquired, offering a greater opportunity to uncover digital artifacts.

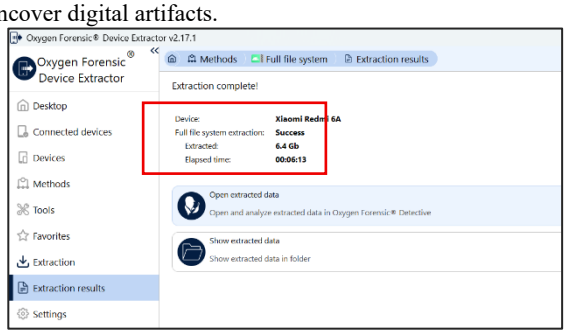


Figure 9. Oxygen Extraction Results

Figure 9 shows that the Xiaomi Redmi 6A device was successfully extracted using the full file system method. The total data extracted amounted to 6.4 GB, with a duration of approximately 6 minutes and 13 seconds. Once the process was completed, the data could be directly opened and analyzed using Oxygen Forensic Detective.

4.4 Examination

4.4.1. Examination using Mobiledit Forensics Express

The data extracted previously using MOBILedit Forensics Express was examined to review the initial information obtained from the device. This tool automatically generates reports in various formats, such as PDF, HTML, and Excel, containing a summary of the data resulting from the extraction process.

The examination process using MOBILedit is shown in Figures 10.

Figure 10: Device Details

Figure 10 shows the Device Properties details obtained from the extraction using MOBILedit Forensics Express. The figure presents information about the device, namely the Xiaomi Redmi 6A with Android 9 operating system. The data obtained includes the Android ID, device serial number, IMEI 1 and IMEI 2, root status, connection type, and phone number.

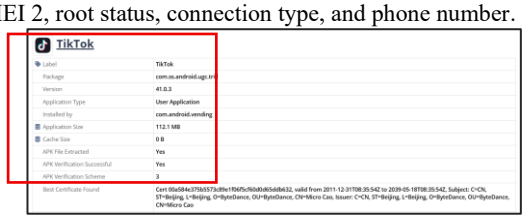


Figure 11: Application Details

Figure 11 displays the extraction results of the TikTok application using MOBILedit Forensics Express, including information on the application label, package, version, size, and APK verification details, which confirm that the application was successfully extracted and is valid. The report also presents a list of Android permissions, such as access to the camera, microphone, location, contacts, storage, and network, indicating that TikTok was installed and active.

4.5.1. Examination using Oxygen Forensic Detective

In addition to MOBILedit Forensics Express, Oxygen Forensic Detective was used to perform file system-level extraction, yielding more complete digital artifacts such as device information, accounts, messages, files, and TikTok-related system data. Its interactive interface also helps researchers categorize and trace relevant evidence efficiently.

The examination process using Oxygen is shown in Figures 12.

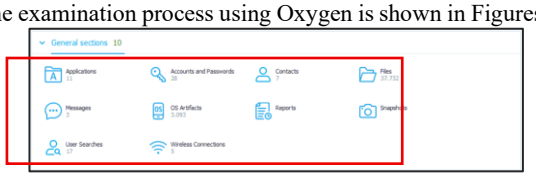


Figure 12: Oxygen General Section

Figure 12 shows the extraction results in Oxygen Forensic Detective's General Sections, displaying retrieved data types such as applications, accounts, contacts, messages, OS artifacts, searches, and wireless connections. This highlights the broad range of data successfully extracted from the device.

After obtaining an overview of the extraction results, the next step was to trace more specific data related to TikTok application activities. One of the key findings was user conversation information stored in the SQLite database, as shown in Figure 13.

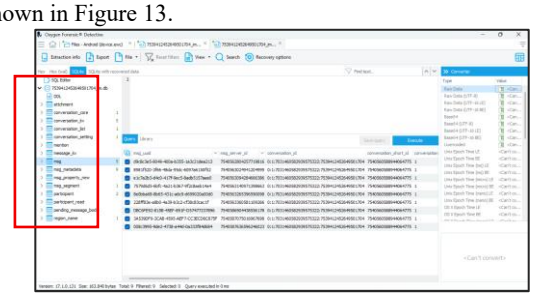


Figure 13: TikTok Database Structure

4.5 Analysis

4.5.1. Analysis using Mobiledit Forensics Express

At the analysis stage, MOBILedit Forensics Express was used to read the extraction results and present digital artifacts in HTML, PDF, or Excel reports. Important information such as device identity and TikTok account data (username, nickname, and user ID) could be analyzed in a structured manner. This data served as the basis for identifying the perpetrator and activities related to the case, as shown in Figure 14.

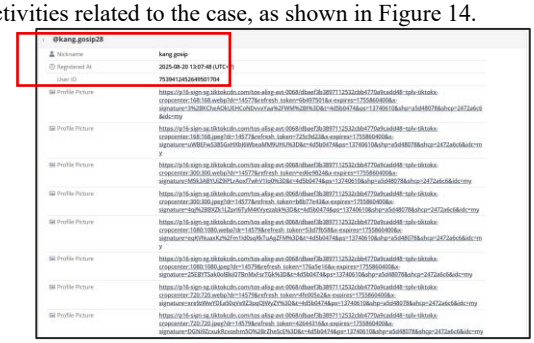


Figure 14: Perpetrator Account Details

Figure 14 shows the account details with the username @kang.gosip28, nickname "kang gosip," along with the registration date and unique user ID. In addition, the report also displays several profile image links stored on TikTok's server. This information reveals the identity of the account used on the device and can therefore serve as a basis for tracing further activities.

Figure 15: Conversation Artifacts

Figure 15 shows the conversation artifacts contained in the conversation_list table, where the data status is marked with the word "Delete." This indicates that the messages previously sent had been deleted by the perpetrator. Although the conversations were removed from the application, this information could still be identified from the extracted database file.

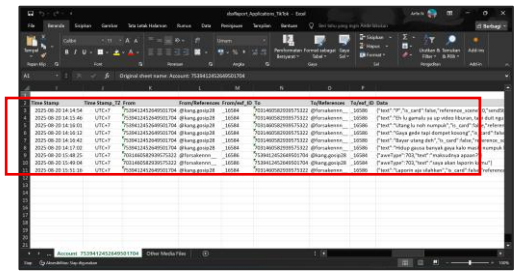


Figure 16: Excel Extraction Report

Figure 16 show the extraction results of TikTok conversations using MOBILedit Forensics Express in the form of an Excel report. The conversation data between the perpetrator and the victim is displayed in a structured manner, including the timestamp, sender identity (From), recipient (To), and message content. The Excel format also facilitates metadata validation, thereby strengthening the evidence of communication that indicates defamation.

Figure 17: Video Metadata from MOBILedit

Figure 17 shows a digital artifact in the form of a 7.5 KB TikTok cache file located in the *fresco_cache* directory. The file is identified as a thumbnail, with metadata of access and modification on August 20, 2025, supporting evidence of video upload activity.

4.5.2. Analysis using Oxygen Forensic Detective

After the analysis with MOBILedit, the next stage was carried out using Oxygen Forensic Detective, which is capable of extracting TikTok digital artifacts in greater depth. This tool presents metadata, conversations, media files, and account information from the directory *data/data/com.ss.android.ugc.trill/*. The analysis results from Oxygen complement the findings of MOBILedit and provide a more comprehensive overview of the perpetrator's account activities.

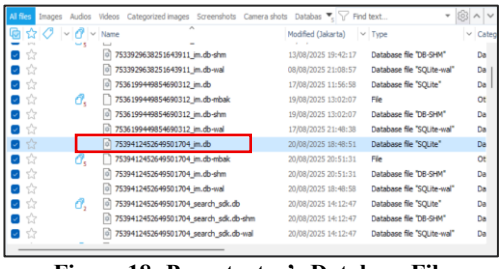


Figure 18: Perpetrator's Database File

Figure 18 shows the database files located in the directory *data/data/com.ss.android.ugc.trill/databases/*. The display reveals several files in the *.db*, *.db-shm*, and *.db-wal* formats, which are part of the database storage system. One of the main files analyzed was *7539412452649501704_im.db*, as it stores important data in the form of user conversation history and

interactions. The contents of *7539412452649501704_im.db* consist of conversation artifacts.

Figure 19: Deleted Conversations

Figure 19 displays the contents of the *7539412452649501704_im.db* database file analyzed with Oxygen. Although the messages had been deleted in the application, the raw data was still found in the directory */data/data/com.ss.android.ugc.trill/databases/*. The attribute *is_card = false* along with the readable conversation content serves as evidence that the messages once existed and were deliberately deleted.

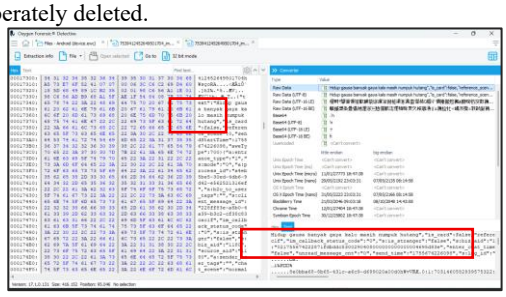


Figure 20: Video Caption

Figure 20 shows a fragment of raw data in hexadecimal format from the *7539412452649501704_im.db-wal* file located in the */data/data/com.ss.android.ugc.trill/databases/* directory. In this section, the caption "Hidup gausa banyak gaya kalo masih numpuk hutang" was successfully recovered even though the post had already been deleted. The fact that the caption is stored in the *-wal* file proves that the content was once uploaded and can serve as relevant digital evidence.

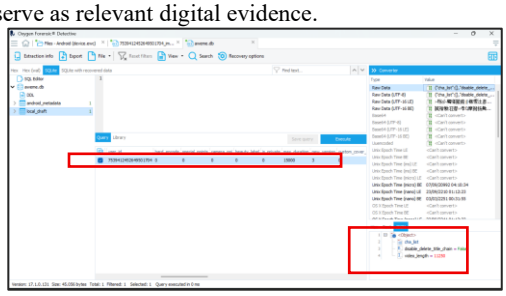


Figure 21: Video Metadata from Oxygen

Figure 21 show the analysis results of the *aweme.db* file located in the */data/data/com.ss.android.ugc.trill/databases/* directory. This database stores metadata of video uploads from the perpetrator's account. Although the original video file was not retrieved, the metadata shows a *user_id* corresponding to the perpetrator and a *video_length* of 11,250 ms (11.25 seconds), identical to the original video. This confirms that the video upload did in fact take place, even though the content has already been deleted.

4.5.3. Analysis using DB Browser for SQLite

After the analysis with MOBILedit and Oxygen, the next stage was carried out using DB Browser for SQLite to verify and further explore the relevant tables in more detail. The database files extracted with Oxygen were reloaded and manually examined to ensure data consistency and to identify conversations and video metadata. In this way, the digital evidence did not rely solely on Oxygen's automatic parsing but was also directly validated through queries, as shown in Figure 22.

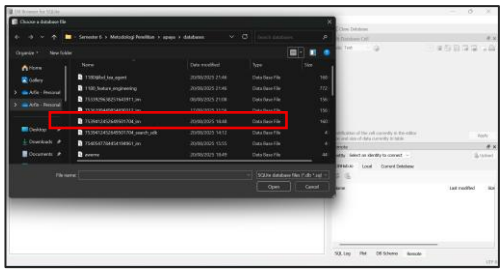


Figure 22: User Database File

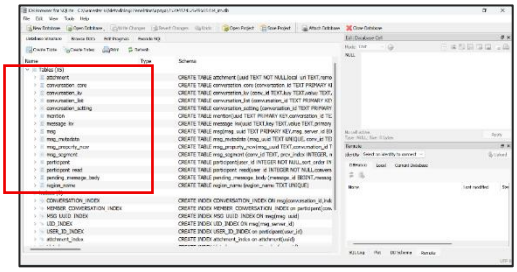


Figure 23: Database Structure from DB Browser

Figure 23 shows the selection of TikTok database files extracted, namely *7539412452649501704_im.db* (160 KB), which contains conversation data, and *aweme.db* (44 KB), which stores video metadata. Meanwhile, Figure 24 show the structure of *im.db* with 15 main tables, including the *msg* table that contains the perpetrator's conversations. From this structure, investigators can determine the relevant tables for further analysis.

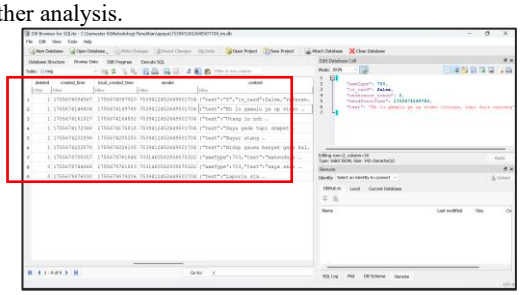


Figure 24: Contents of the *msg* Table

Figure 24 show the contents of the *msg* table from the *7539412452649501704_im.db* database, which contains conversations between the perpetrator and the victim. The *deleted* column with a value of 1 indicates that the messages had been deleted in the application but remained stored in the database. The *sender* column shows the perpetrator's user ID, while the *content* column presents the message in JSON format, including texts such as "Utang lu noh numpuk" and "Hidup gausa banyak gaya kalo masih numpuk hutang." These findings demonstrate that deleted messages can still be recovered and used as digital evidence.

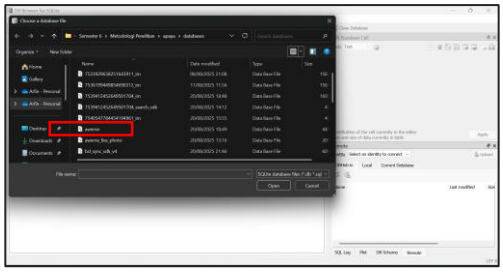


Figure 25: Video Artifact Database File

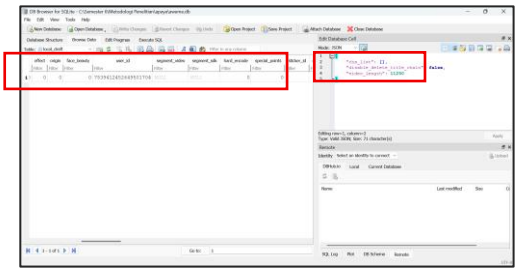


Figure 26: Video Artifacts

Figure 25 shows the *aweme.db* file opened with DB Browser, while Figure 26 show the analysis of the *local_draft* table containing the suspect's video information. The analysis revealed that user_id 7539412452649501704 corresponds to the suspect's account, with video metadata indicating a duration of 11.25 seconds, even though the original file had been deleted. This finding demonstrates that metadata from *aweme.db* can serve as additional evidence in the TikTok defamation case.

4.6 Presentation

The presentation stage aims to present the analysis results in a clear, structured, and comprehensible manner for relevant parties such as investigators, law enforcement, and the court. At this stage, the findings from identification to analysis are compiled into a report containing digital artifacts, validation, and interpretations that link the evidence to the defamation case on the TikTok application.

The forensic analysis was conducted using MOBILedit Forensics Express, Oxygen Forensic Detective, and DB Browser for SQLite, which produced digital evidence in the form of conversations, captions, and video metadata. The report not only presents raw data but also provides contextual explanations that can be legally justified, as shown in Table 4.

Table 4. Summary of Digital Evidence Findings

No	Digital Evidence	Quantity	Description	
1.	Account Information	1	Username : @kang.gosip28 Nickname : kang gosip User ID : 7539412452649501704	
2.	Conversation	9	Pelaku	Korban
			"P" "Eh lu gamalu ya up video liburan, tapi duit ngutang" "Utang lu noh numpuk" "Gaya gede tapi dompet kosong" "Bayar utang deh" "Hidup gausa banyak gaya kalo masih numpuk hutang" "Laporin aja silahkan"	"maksudnya apaan?" "saya akan laporin kamu"
3.	Video	1	Konten fitnah dengan format mp4	
4.	Video Caption	1	"Hidup gausa banyak gaya kalo masih numpuk hutang"	
5.	Contact	1	Username : @forsakennn__ Nickname : forsakennn__ User ID : 7031460582939575322	

Table 4 summarizes the digital evidence of the TikTok defamation case, consisting of the perpetrator's account information, nine conversations containing insults and threats, one defamatory video along with its supporting caption, and one related contact.

All digital findings are organized systematically to ensure they are easily understood by the authorities. In the presentation stage, the data is not only documented but also cross-compared across forensic tools to ensure consistency, completeness, and validity. A summary of the digital evidence findings from each tool is presented in Table 5.

Table 5: Findings of Each Tool

No	Type of Digital Evidence	MOBILedit Forensic	*Oxygen Forensic*	*DB Browser*	Total Digital Evidence
1.	Account Info	1	1	1	1
2.	Conversation	9	9	9	9
3.	Video	0	0	0	1
4.	Video Caption	0	1	0	1
5.	Contact	1	1	1	1
Total		11	12	11	13

Table 5 presents a comparison of digital evidence extracted using MOBILedit Forensic Express with a total of 11 artifacts, Oxygen Forensic Detective with 12 artifacts, and DB Browser for SQLite with 11 artifacts. All three tools consistently extracted the main artifacts such as account information, conversations, and contacts; however, differences were found in certain artifacts, such as video captions that were only detected by Oxygen, as well as videos that did not appear in any of the three tools but could be verified through the original evidence.

The success rate of each forensic tool is calculated using the following formula:

$$Par = \frac{\sum_x O}{\sum_X T} \times 100\%$$

Description:

Par : Accuracy value of the forensic application
$\sum_x O$: Number of data successfully extracted
$\sum_x O$: Total number of original data

The summary of the accuracy comparison of each tool can be seen in Table 6.

Table 6: Percentage of Tool Accuracy

No.	Forensics Tools	Percentage
1.	MOBILedit Forensic Express	85%
2.	Oxygen Forensic Detective	92%
3.	DB Browser for SQLite	85%

Table 6 presents a comparison of the success percentages of the three forensic tools, where Oxygen Forensic Detective recorded the highest accuracy rate of 92%, while MOBILedit Forensic Express and DB Browser for SQLite each achieved 85%. These results indicate that Oxygen is superior in extracting digital artifacts; however, the use of multiple tools remains essential to ensure consistency and validity of the evidence.
The extraction results show that all three tools—MOBILedit Forensics Express, Oxygen Forensic Detective, and DB Browser for SQLite—successfully retrieved key digital artifacts such as account information, messages, contacts, and video metadata. Oxygen achieved the highest success rate (92%), while MOBILedit and DB Browser each reached 85%. This difference is due to Oxygen's full file system extraction capability, which allows deeper recovery of deleted TikTok data. The recovered artifacts, including deleted conversations and video metadata containing defamatory captions, demonstrate that digital traces remain stored within TikTok's database even after deletion.

Each tool contributed differently to the forensic process: MOBILedit provided structured extraction and automatic reporting, Oxygen offered in-depth data visualization and artifact correlation, and DB Browser enabled manual verification of database integrity. Cross-validation among these tools improved accuracy and credibility, confirming that the DFRWS framework effectively guides a systematic and reproducible forensic investigation. The integration of multiple tools enhances both the quality and quantity of recovered artifacts, proving that this method is reliable for analyzing social media–based defamation cases.

The DFRWS framework demonstrates strong adaptability and practical value in digital forensic investigations. Its structured stages—from identification to presentation—ensure traceability, data integrity, and evidence validation, making it applicable to various social media platforms beyond TikTok, such as Instagram or Facebook. The method's modular design allows investigators to integrate multiple tools, enhancing accuracy while minimizing data loss. In practical implementation, DFRWS provides a clear guideline for law enforcement officers to reconstruct digital events systematically, verify deleted data, and present findings that are legally admissible. These strengths confirm that DFRWS is not only effective for TikTok defamation cases but also generalizable for broader cybercrime investigations involving mobile and social media applications.

5. CONCLUSION

The research results show that the DFRWS method was successfully applied to analyze digital evidence from the TikTok application using MOBILedit Forensics Express, Oxygen Forensic Detective, and DB Browser for SQLite. MOBILedit and DB Browser each identified 11 artifacts consisting of account information, conversations, and contacts, while Oxygen detected 12 artifacts including video captions. Validation confirmed the presence of 13 original artifacts with the addition of video and caption data, emphasizing that each tool has its strengths and limitations. Oxygen achieved the highest extraction accuracy of 92%, while MOBILedit and DB Browser each reached 85%, proving the effectiveness of the DFRWS framework in ensuring the validity and consistency of digital evidence in social media defamation cases.

Future research could focus on expanding the use of the DFRWS framework to other social media platforms such as Instagram, Facebook, or X (formerly Twitter), to assess its cross-platform applicability. In addition, the integration of automated extraction scripts or AI-based forensic analysis could improve efficiency and accuracy in identifying deleted or hidden digital artifacts. Exploring cloud-based data acquisition for TikTok and similar applications could also enhance the comprehensiveness of future digital forensic investigations.

6. REFERENCES

[1] Nurul Fatmawati, "Pengaruh Positif dan Negatif Media Sosial Terhadap Masyarakat," Kementrian Keuangan. Accessed: Apr. 20, 2024. [Online]. Available: https://www.djkn.kemenkeu.go.id/kpknl-semarang/baca-artikel/14366/Pengaruh-Positif-dan-Negatif-Media-Sosial-Terhadap-Masyarakat.html

[2] Rafiq A, "Dampak Media Sosial Terhadap Perubahan Sosial Suatu Masyarakat," Jurnal Ilmu Sosial dan Ilmu Politik, vol. Vol. 1 No. 1, pp. 18–29, 2020.

[3] Syacri Syahnakrie, "Pengaruh Media Sosial Tiktok Terhadap Generasi Muda (Remaja)," Kompasiana. Accessed: Apr. 20, 2024. [Online]. Available: https://www.kompasiana.com/syacri2511/601473f0d541df06af15f2f5/pengaruh-media-sosial-tiktok-terhadap-generasi-muda-remaja

[4] A. Ferniansyah, S. Nursanti, and L. Nayiroh, "Pengaruh Media Sosial Tiktok Terhadap Kreativitas Berpikir Generasi Z," vol. 6, no. 9, 2021, doi: 10.36418/syntax.

[5] Elsa Totti Bakistuta and M. Abduh, "Dampak Media Sosial Tiktok Terhadap Tindak Tutur Siswa Sekolah Dasar," Jurnal Elementaria Edukasia, vol. 6, no. 3, pp. 1201–1217, Sep. 2023, doi: 10.31949/jee.v6i3.6243.

[6] A. Z. Yonatan, "10 Media Sosial dengan Pengguna Terbanyak 2024," GoodStats. Accessed: Jul. 14, 2025. [Online]. Available: https://data.goodstats.id/statistic/10-media-sosial-dengan-pengguna-terbanyak-2024-CaJT1

[7] F. Anggraini, H. Herman, and A. Yudhana, "Analisis Forensik Aplikasi TikTok Pada Smartphone Android Menggunakan Framework Association of Chief Police Officers," JURIKOM (Jurnal Riset Komputer), vol. 9, no. 4, p. 1117, Aug. 2022, doi: 10.30865/jurikom.v9i4.4738.

[8] R. Novrianda Dasmen and F. Kurniawan, "Digital Forensik Deleted Cyber Crime Evidence pada Pesan Instan Media Sosial Digital Forensics Deleted Cyber Crime Evidence on Social Media Instant Messaging," 2021.

[9] M. Riskiyadi, "Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime," 2020.

[10] A. Muhammad, A. Syarif, H. Thalib, and N. Fadhilah Mappaselleng, "Efektivitas Penyidikan Terhadap Tindak Pidana Pencemaran Nama Baik Melalui Media Sosial:

Studi Kasus Di Polrestabes Makassar," Journal of Lex Generalis, 2022.

[11] Reski Badillah, Andi Yulia Muniar, Abd. Rahman, Febri Hidayat Saputra, Mansyur, and Supriadi Sahibu, "Digital Forensic Evidence Analysis In Revealing Defamation On Social Media (Twitter) Using The Static Forensics Method," Ceddi Journal of Information System and Technology (JST), vol. 2, no. 2, pp. 22–33, Dec. 2023, doi: 10.56134/jst.v2i2.45.

[12] Ponno Jesica Daun, Lumunon Theodorus H.W, and Gerungan Carlo A, "Penerapan Digital Forensik Dalam Pembuktian Pencemaran Nama Baik Di Dunia Maya 1," 2023. [Online]. Available: https://nasional.tempo.co/read/1616840/digital-

[13] M. Marzuki and T. Sutabri, "Analisis Forensik Media Sosial Michat Metode Digital Forensik Integrated Investigation Framework (IDFIF)," Blantika : Multidisciplinary Jornal, vol. 1, no. 2, 2023, [Online]. Available: https://blantika.publikasiku.id/176

[14] Ardiningtias Syifa Riski, Sunardi, and Herman, "Forensik Digital Kasus Penyebaran Pornografi pada Aplikasi Facebook Messenger Berbasis Android Menggunakan Kerangka Kerja National Institute of Justice," Jurnal Edukasi dan Penelitian Informatika, 2021.

[15] K. Aulia, P. Wardinasahira, N. L. Cintani, N. A. Nisrina, and E. Sholihatin, "Dampak Penggunaan Teknologi Internet Melalui Tiktok Akun Gosip Terhadap Etika Berbahasa," JURNAL SYNTAX IMPERATIF : Jurnal Ilmu Sosial dan Pendidikan, vol. 4, no. 2, pp. 146–155, May 2023, doi: 10.36418/syntax-imperatif.v4i2.230.

[16] H. Septya Mikayla, A. Kusyanti, P. H. Trisnawan3, and P. Korespondensi, "Analisis Forensik Digital Untuk Investigasi Kasus Cyberbullying Pada Media Sosial Tiktok," 2019, doi: 10.25126/jtiik.2023108017.

[17] N. Iman, A. Susanto, and R. Inggi, "Analisa Perkembangan Digital Forensik dalam Penyelidikan Cybercrime di Indonesia (Systematic Review)," Jurnal Telekomunikasi dan Komputer, vol. 9, no. 3, p. 186, Jan. 2020, doi: 10.22441/incomtech.v9i3.7210.

[18] Syamsul Arifin, M. Syahrul Borman, Nur Handayati, and Dudik Djaja Sidarta, "Peran Penyidik Kepolisian Negara Republik Indonesia Dalam Penegakan Hukum Cybercrime," 2024.

[19] I. Riadi, H. Herman, and N. H. Siregar, "Mobile Forensic of Vaccine Hoaxes on Signal Messenger using DFRWS Framework," MATRIK : Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 21, no. 3, pp. 489–502, Jul. 2022, doi: 10.30812/matrik.v21i3.1620.

[20] B. Suhardjono, A. Syah Putra, N. Aisyah, and V. Valentino, "ANALYSIS OF NIST METHODS ON FACEBOOK MESSENGER FOR FORENSIC EVIDENCE," Journal of Innovation Research and Knowledge, no. 8, Feb. 2022.

[21] Oxygen Forensics, "Oxygen Forensic Detective," Oxygen Forensics. Accessed: Jul. 23, 2025. [Online]. Available: https://www.oxygenforensics.com/en/products/oxygen-forensic-detective/

[22] Yudhana Anton, Riadi Imam, and Prasongko Riski Yudhi, Forensik WhatsApp Menggunakan Metode Digital Forensic Research Workshop (DFRWS). 2022.

[23] A. Yudhana, I. Riadi, I. Zuhriyanto, and A. Dahlan, "Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS)," vol. 20, no. 2, pp. 125–130, 2019, [Online]. Available: http://jurnalnasional.ump.ac.id/index.php/Techno

[24] I. Riadi, Herman, and N. H. Siregar, "Mobile Forensic Analysis of Signal Messenger Application on Android using Digital Forensic Research Workshop (DFRWS) Framework," Ingenierie des Systemes d'Information, vol. 27, no. 6, pp. 903–913, Dec. 2022, doi: 10.18280/ISI.270606.

[25] A. G. Prayogo and I. Riadi, "Digital Forensic Signal Instant Messages Services in Case of Cyberbullying using Digital Forensic Research Workshop Method," Int J Comput Appl, vol. 184, no. 32, pp. 21–29, Oct. 2022, doi: 10.5120/ijca2022922393.