Digital Forensic Analysis of Cyberbullying Cases on TikTok Application Service using National Institute of Justice Method

Florita Cinta Arum Kuncoro
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

Along with the rapid development of digital technology, the use of social media has also increased, including the risk of cybercrime such as cyberbullying. Social media applications in Indonesia, such as TikTok, are one of the most widely used and vulnerable to being used for such deviant behavior. This study aims to investigate cyberbullying cases in the group chat feature in the TikTok application. The object discussed is the TikTok application running on Android devices. This research uses the method of the National Institute of Justice (NIJ) with five main stages: preparation, collection, examination, analysis, and reporting. The tools used in the digital investigation process are Oxygen Forensic Detective and Belkasoft Evidence Center X. The results show that Oxygen Forensic Detective has a data extraction accuracy rate of 96%, while Belkasoft Evidence Center X has an accuracy rate of 78% and shows different results in detecting image data and deleted data. Based on the analysis results, both tools are able to extract information in the form of application data, user names, messages, contacts, and deleted messages. This research contributes to the development of digital forensic handling strategies in dealing with cyberbullying cases on social media platforms.

Keywords

NIJ; Cyberbullying; Forensic; TikTok; Digital Forensic

1. INTRODUCTION

The rapid development of digital technology has given birth to various new social media platforms with innovative features and systems to facilitate users in obtaining and disseminating information quickly. Social media is a website that allows individuals to create personal pages and communicate with friends to share information. Some of the biggest social media platforms today include Facebook, X, Instagram, TikTok, WhatsApp, and Line[1][2].

Social media has a very significant impact on daily life, especially in broadening horizons and knowledge through the rapid distribution of educational content. In addition, social media is also a space for discussion through online communities and expanding friendship networks.[3]. However, despite these benefits, social media also has negative impacts that cannot be ignored. Excessive use of technology can cause sleep disorders, form individualistic and less empathetic personalities, and encourage immoral actions. In fact, social media is often used by irresponsible parties to commit criminal acts such as fraud, extortion, rape, and cyberbullying[4]. As technology advances, the number of social media users in Indonesia also continues to increase. In early 2023, there were 167 million active social media users in Indonesia, or around 60.4% of the total population of 276.4 million. The highest percentage of active users is on WhatsApp (92.1%), followed by Instagram (86.5%), Facebook (83.8%), TikTok (70.8%), and Telegram (64.3%)[5]. The increasing number of social media apps has facilitated the creation of numerous major cybercrimes [6].

Of the various platforms, TikTok is one that deserves special attention because it shows very rapid user growth in Indonesia, with the number of users reaching 112.9 million and an increase of 2.8% compared to the previous year.[7]. TikTok is a short video-based platform that allows users to express their creativity through features such as filters, visual effects, and lip sync. Users can also send messages, make purchases, join group chats, and leave comments on viewed videos. However, these features also open up space for negative behavior, especially cyberbullying. TikTok's features can cause serious problems when used by children or teenagers who do not fully understand the dangers of social networking[8]. As the majority of its users are interested in text, photo and video content, TikTok has become a breeding ground for the spread of hoaxes and cyberbullying practices [9].

Cyberbullying is a form of intimidation carried out by utilizing digital technology[10][11]. Based on research, around 74% of cyberbullying cases in Indonesia occur through social media, with various forms such as flaming, harassment, denigration, impersonation, trickery, outing, and cyberstalking[12][13]. These actions have serious psychological, psychosocial, academic, and physical impacts on victims, such as mood disorders, depression, fatigue, loss of appetite, and decreased enthusiasm for activities [14][15].

With the increase in cyberbullying cases in Indonesia, a digital forensic investigation process is needed to uncover the perpetrators and obtain relevant evidence. Some methods that can be used include methods from the National Institute of Standards and Technology, National Institute of Justice, and Association of Chief Police Officers (ACPO). Digital forensic tools that can be used include Belkasoft Evidence Center, Magnet AXIOM, UFED Physical Analyzer, Autopsy, Oxygen Forensic, and MOBILedit Forensic[16]. Previous research by Pangestika Rona Leonsa in 2023 has proven the successful use of the ACPO method in digital forensic analysis of TikTok applications related to cyberbullying using tools such as MOBILedit Forensic Express, DB Browser for SQLite, and Magnet AXIOM. The results of the study successfully identified conclusive digital evidence in the form of bullying key words and user accounts that most often uttered them.[17]. These findings demonstrate the importance of using forensic tools in solving cyberbullying cases and serve as a basis for the exploration of other tools such as Oxygen Forensic and

Belkasoft Evidence Center with the National Institute of Justice method.

2. LITERATURE STUDY

2.1 Digital Forensics

Digital forensics is a science that studies the process of searching, analyzing, and reporting data from digital devices to support legal proceedings[18]. This process includes the stages of data collection, examination, analysis, and reporting. One of its branches is Mobile Device Forensic, which is forensics that focuses on digital evidence from mobile devices[19].

2.2 Digital Evidence

Digital evidence is information in digital form such as text, images, video, sound, or social media data that can be used as legal evidence[20][21]. Important principles in handling digital evidence include maintaining data authenticity, investigator competence, documentation of the investigation process, and full responsibility for legal procedures. In addition, there are five main characteristics of digital evidence, namely admissible, authentic, complete, reliable, and believable, which must be met so that the evidence can be accepted in the legal process legally and effectively[22][23].

2.3 Cyberbullying

Cyberbullying is an act of intimidation, harassment or bullying perpetrated digitally through social media or other online platforms[10][24]. It can be done individually or in groups, and has serious emotional and psychological impacts on the victim. Forms include flaming, harassment, denigration, impersonation, trickery, and cyberstalking[14][15].

2.4 Belkasoft Evidence Center X

Belkasoft Evidence Center X is a digital forensic investigation software that supports data analysis from computers, mobile devices, and the cloud. The main advantages of this tool include remote data acquisition capabilities through Belkasoft R, analysis of more than 1,500 popular apps such as WhatsApp, Telegram, and TikTok, easy-to-use data visualization, and cloud forensics features to access services such as iCloud and WhatsApp Web[25].

2.5 Oxygen Forensic Detective

Oxygen Forensics Detective s a digital forensics software capable of extracting, decoding and analyzing data from various mobile devices. It supports more than 40,000 app versions, offers integrated analysis tools such as OCR and data mapping, and supports breaking iOS and Android backup encryption. Extracted data can be exported to formats such as PDF, XLS, and XML[26].

2.6 National Institute of Justice

The National Institute of Justice (NIJ) digital investigation method includes five main stages, namely preparation, collection, examination, analysis, and reporting [27]. The preparation stage involves sorting out data that is worthy of being used as evidence. Collection is the collection of data from digital media without changing its authenticity. Examination is done to ensure the validity of the data. Analysis involves thorough data processing using legitimate techniques. Finally, reporting is the preparation of an investigation report that includes the tools and methods used in the investigation process.

3. RESEARCH METHOD

This research uses the method of the National Institute of Justice (NIJ) to conduct the investigation process, which consists of five stages, namely: preparation, collection, examination, analysis, and reporting. These stages are shown in Figure 1.

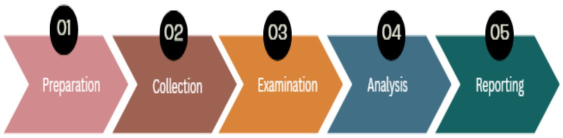


Figure 1: Stages of the NIJ Method

Figure 1 shows the stages in the National Institute of Justice (NIJ) method. The preparation stage includes organizing and identifying digital evidence, including documentation, labeling, and selecting forensic tools such as laptops, Oxygen Forensic, and Belkasoft Evidence Center. The collection stage focuses on the acquisition and careful archiving of digital evidence and metadata to preserve the authenticity and integrity of the data using tools such as Belkasoft and Oxygen. The examination stage involves forensic and manual inspection of the acquired files to ensure originality using forensic software. The analysis stage includes validation and interpretation of findings, such as linking artifacts from TikTok group conversations with cyberbullying case scenarios, as well as comparing data between victim and alleged perpetrator accounts. Finally, the reporting stage compiles a systematic and objective report of findings, which contains behavior patterns, digital footprints, and conclusions that support the investigation process of cyberbullying cases.

4. RESULT AND DISCUSSION

This research analyzes cyberbullying cases that occur through the TikTok application using a three-stage approach: pre-incident, incident, and post-incident. This approach refers to the stages of investigation in the National Institute of Justice (NIJ) method. Each stage was visually simulated to illustrate the complete process of cyberbullying. The first simulation, the pre-incident, can be seen in Figure 2.

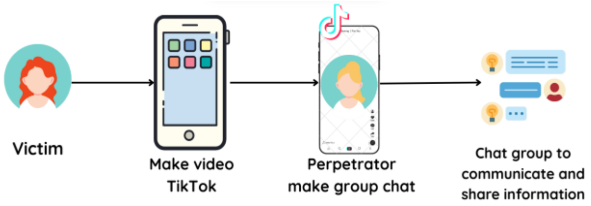


Figure 2 : Pre-incident of Cyberbullying Case

Figure 2 shows the initial scenario where User 2 created a group chat on the TikTok app with the aim of building friendships and sharing information between users, including the Perpetrator, Victim, and User 3. In the group, they actively discussed various topics related to TikTok, such as trends, tips, and creative ideas. The communication that occurs in this group is the starting point for interactions that then develop in a negative direction.

The second stage of the case simulation is the incident, as shown in Figure 3.

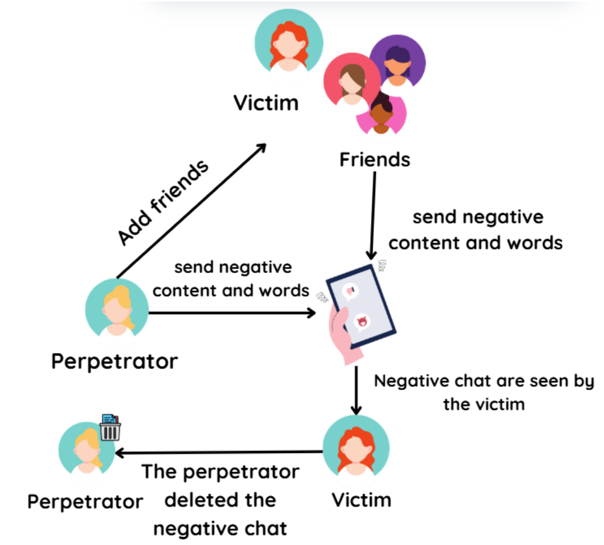

Victim
Friends
Add friends
send negative content and words
send negative content and words
Perpetrator
Negative chat are seen by the victim
The perpetrator deleted the negative chat
Perpetrator
Victim

Figure 3 : Incident of Cyberbullying Case

Figure 3 illustrates the incident when the perpetrator began sending negative words to the victim through the TikTok group chat. Remarks such as “Ugly”, “Stupid”, and the like began to be thrown repeatedly. These messages were read by the victim and had a psychological impact in the form of feeling left out, sad, and uncomfortable. To eliminate traces, the perpetrator then deletes the bullying messages that have been sent.

The final stage of the simulation is post-incident, as described in Figure 4.

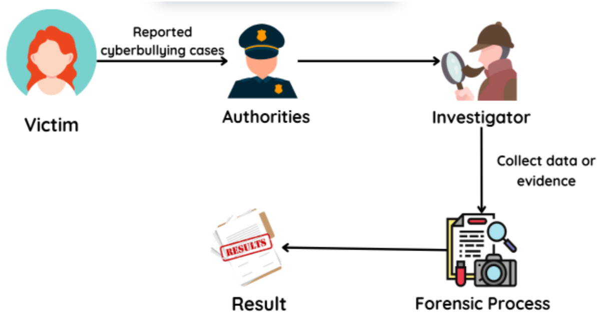


Figure 4 : Post Incident of Cyberbullying Case

In the post-event stage, the victim reports the bullying incident to the authorities, such as the police or related institutions. This report is followed up by investigators by conducting an investigation process, including the collection of digital evidence such as messages, screenshots, and videos. Furthermore, digital forensic analysis is carried out to reveal hidden or deleted data by the perpetrator. The results of this process will be used as evidence in the applicable legal process.

This simulation scenario was designed to reflect realistic cyberbullying interactions commonly found on social media platforms. Although this study focuses on TikTok, the methodology is applicable to other platforms such as WhatsApp, Discord, or Telegram. Future works can explore multi-platform evaluation or real-world case validation to generalize the effectiveness of these forensic tools.

4.1 Preparation

The preparation stage is carried out as the first step in the digital investigation process. At this stage, systematic collection and documentation of digital evidence is carried out to maintain data integrity during the investigation process. Evidence documentation can be seen in Figure 5.

Figure 5: Smartphone Digital Evidence

Figure 5 shows documentation of digital evidence that was successfully secured in the alleged cyberbullying case. The evidence is in the form of a Xiaomi Redmi A1 smartphone. After being confiscated, the device was documented, labeled, and recorded its complete specifications.

This documentation process includes device identification such as brand, IMEI number, operating system, and operating system version. Complete information about the evidence can be seen in Table 1.

Table 1 : Smartphone Evidence Specifications

No.	Type	Description
1.	Brand	Xiaomi
2.	Series	Redmi A1
3.	IMEI	869724062286229
4.	Operating System	Android
5.	Operating System Version	12

Furthermore, various supporting tools and devices were prepared to support the investigation process as shown in Table 2.

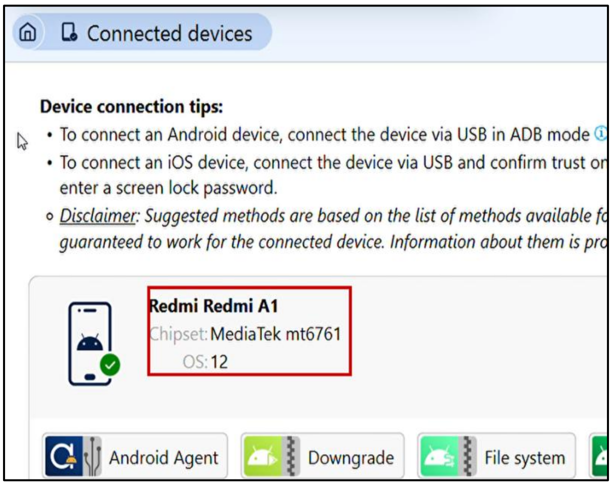
Table 2 : Tools Used

No.	Tools	Description
1.	Laptop	Laptop Asus TUF Dash F15 12th Gen Intel(R) Core(TM) i5-12450H 2.00 GHz
2.	USB Cable	-
3.	Belkasoft Evidence Center X	Analyzing and extracting digital artifacts
4.	Oxygen Forensic Detective	Collects, extracts and analyzes data
5.	Magisk	Rooting
6.	Tapin Recovery Instraller	Instraller Flashing prerooted files and boot patches for the rooting process

Table 2 shows the tools used in the investigation process. The hardware used is a Laptop and USB Cable. While the software used consists of Belkasoft Evidence Center X, Oxygen used consists of Belkasoft Evidence Center X, Oxygen Forensic Detective, Magisk, and Tapin Recovery Installer.

4.2 Collection

The collection stage is a critical first step in the digital forensic investigation process. Its main goal is to obtain data from devices suspected of containing digital evidence. This process must be conducted carefully and systematically to ensure the authenticity and integrity of the data so it remains admissible in legal proceedings. Once the device is properly prepared, data collection is carried out using Oxygen Forensic Detective. The Android device is connected to the forensic laptop, the Oxygen software is launched, a new case is created, and the Extract Device Data option is selected. Figure 8 shows the device successfully connected to the software for extraction.



Device connection tips:

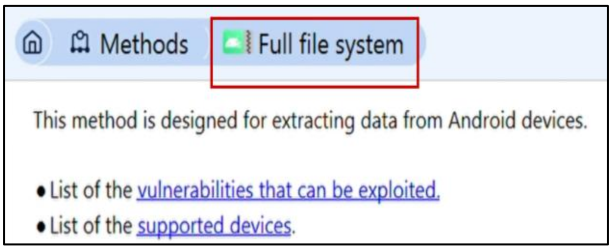
- To connect an Android device, connect the device via USB in ADB mode
- To connect an iOS device, connect the device via USB and confirm trust or enter a screen lock password.

○ *Disclaimer: Suggested methods are based on the list of methods available f guaranteed to work for the connected device. Information about them is pro*

Redmi Redmi A1
Chipset: MediaTek mt6761
OS: 12

Figure 8: Device Connected to Oxygen Forensic Detective

The extraction method used is Full System Extraction, as this method allows full access to the entire contents of the internal memory, including hidden or deleted data. This method was chosen specifically to extract deleted TikTok conversations, which cannot be obtained through normal logical methods. Figure 9 shows the display when the extraction method is selected on the device.

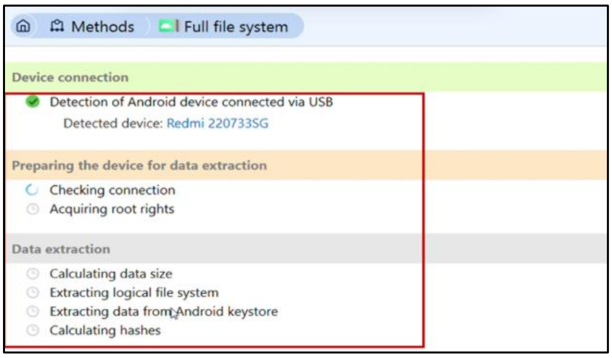


This method is designed for extracting data from Android devices.

- List of the vulnerabilities that can be exploited.
- List of the supported devices.

Figure 9 : Selected Method for Smartphone

Once the device is recognized and the extraction method is determined, the system verifies the connection and root privileges. The extraction process is then performed on the logical file system and data from the Android keystore, as shown in Figure 10, which shows the extraction process in progress. The collected data is then sized and hashed to verify integrity.



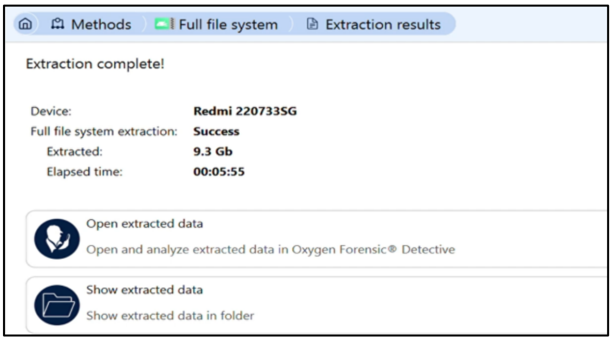
Device connection
Detection of Android device connected via USB
Detected device: Redmi 220733SG

Preparing the device for data extraction
Checking connection
Acquiring root rights

Data extraction
Calculating data size
Extracting logical file system
Extracting data from Android keystore
Calculating hashes

Figure 10: Extraction Process

The results of the extraction are displayed in the Extraction Results menu, as shown in Figure 11. In this case, a total of 7.7 GB of data was successfully extracted in 4 minutes 54 seconds with a status of Success, indicating that the extraction process ran thoroughly without problems.



Extraction complete!

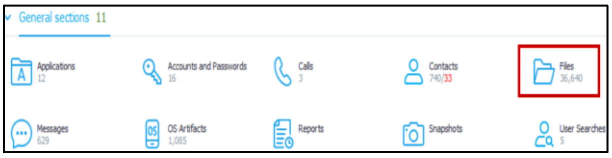
Device:	Redmi 220733SG
Full file system extraction:	Success
Extracted:	9.3 Gb
Elapsed time:	00:05:55

Open extracted data
Open and analyze extracted data in Oxygen Forensic® Detective

Show extracted data
Show extracted data in folder

Figure 11: Extraction Process Results

Once the process is complete, the extracted data can be analyzed through Oxygen Forensic Detective's main interface. In it, investigators can view information that has been structured by categories such as messages, contacts, media files, and system artifacts. Figure 12 shows a view of the data extraction results, including graphs of user interactions, activity history, and applications that have been installed on the device.



Applications 12
Accounts and Passwords 16
Calls 3
Contacts 740/33
Files 36,640
Messages 629
OS Artifacts 1,085
Reports
Snapshots
User Searches 5

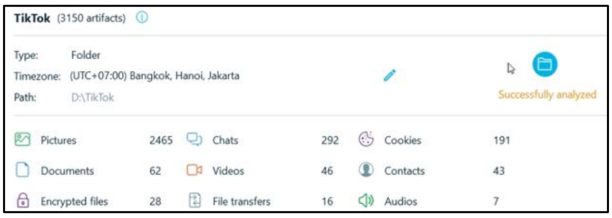
Figure 12: Data Extraction Results

4.3 Examination

The Examination stage aims to analyze the data that has been collected, specifically the database file named **7499094093168329736_im** from the TikTok application directory (**com.ss.android.ugc.trill**). This file was analyzed to reveal the communication history, including deleted messages.

4.3.1 *Examination with Belkasoft Evidence Center X*

The database files were analyzed using Belkasoft Evidence Center X, which is able to visually display the contents of the database and automatically identify digital artifacts such as messages, images, videos, contacts, documents, as well as encrypted files.



TikTok (3150 artifacts)

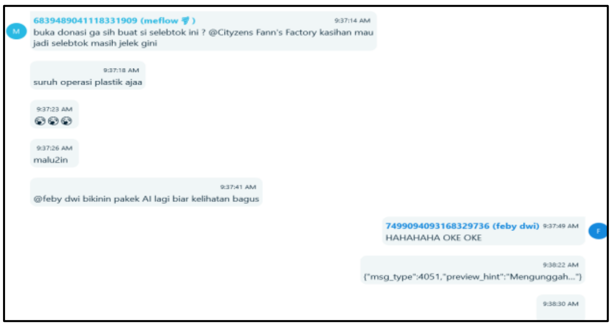
Type: Folder
Timezone: (UTC+07:00) Bangkok, Hanoi, Jakarta
Path: D:\TikTok

Successfully analyzed

Pictures	2465	Chats	292	Cookies	191
Documents	62	Videos	46	Contacts	43
Encrypted files	28	File transfers	16	Audios	7

Figure 13: Belkasoft Evidence Center X Data Analysis Process Results

Figure 13 shows the analysis results of 2947 successfully recognized artifacts, consisting of 2465 images, 46 videos, 285 conversations, 43 contacts, 58 documents, and 27 encrypted files. All artifacts are classified by type and displayed in a structured interface, making the search process easier.



6839489041118331909 (meflow 🪽) 9:37:14 AM
buka donasi ga sih buat si selebtok ini ? @Cityzens Fann's Factory kasihan mau jadi selebtok masih jelek gini

9:37:18 AM
suruh operasi plastik ajaa

9:37:23 AM
😭😭😭

9:37:26 AM
malu2in

9:37:41 AM
@feby dwi bikinin pakek AI lagi biar kelihatan bagus

7499094093168329736 (feby dwi) 9:37:49 AM
HAHAHAHA OKE OKE

9:38:22 AM
{"msg_type":4051,"preview_hint":"Mengunggah..."}

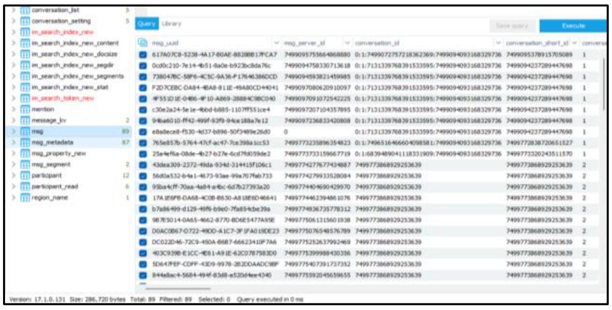
9:38:30 AM

Figure 14: Detailed View of Conversation Artifacts from TikTok

Figure 14 shows details of the successfully extracted conversation artifacts, including information on the time, sender, recipient, message direction, delivery status, and other metadata such as message deletion status. This view resembles the original application interface, but includes technical data useful for forensic analysis and documentation.

4.3.2 *Examination with Oxygen Forensic SQLite Viewer*

The examination continued using Oxygen Forensic SQLite Viewer which allows technical analysis of SQLite databases through the SQL Editor view.



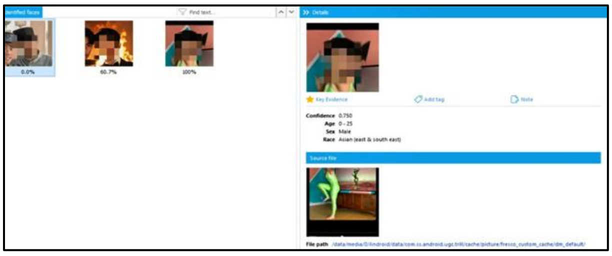
conversation_list 5
conversation_setting 5
im_search_index_new
im_search_index_new_content
im_search_index_new_docsize
im_search_index_new_segdir
im_search_index_new_segments
im_search_index_new_stat
im_search_token_new
mention
message_kv 2
msg 89
msg_metadata 87
msg_property_new
msg_segment 2
participant 12
participant_read 6
region_name 1

msg_uuid	msg_server_id	conversation_id	conversation_short_id	conversa
617A07C8-5238-4A17-80AE-88288B17FCA7	7499095755664868880	0:1:7499072757218362369:7499094093168329736	7499095378915705089	1
0cd0c210-7e14-4b51-8a0e-b923bc8da76c	7499094758330713618	0:1:7131339768391533595:7499094093168329736	7499094237289447698	1
7380478C-58F6-4C5C-9A36-F17646386DCD	7499094593821459985	0:1:7131339768391533595:7499094093168329736	7499094237289447698	1
F2D7CEBC-DA84-4BA8-811E-49A80CD44041	7499097080620910097	0:1:7131339768391533595:7499094093168329736	7499094237289447698	1
4F551D1E-0486-4F10-A869-28884C9BC040	7499097091072542225	0:1:7131339768391533595:7499094093168329736	7499094237289447698	1
c30e2a24-5e1e-4bbd-b885-1107ff551ce4	7499097207104357895	0:1:7131339768391533595:7499094093168329736	7499094237289447698	1
94ba6010-ff42-499f-93f9-94ce188a7e12	7499097236833420808	0:1:7131339768391533595:7499094093168329736	7499094237289447698	1
e8a8eced-f530-4d37-b896-50f3489e26d0	0	0:1:7131339768391533595:7499094093168329736	7499094237289447698	1
765e857b-5764-47cf-ac47-7ce398a1cc53	7499773235896354823	0:1:7496516466604098581:7499094093168329736	7499772838720651527	1
25a4ef6a-08de-4b27-b27e-6cd7fd059de2	7499773733159667719	0:1:6839489041118331909:7499094093168329736	7499773320243511570	1
43dea309-2372-49da-934d-314415f106c1	7499774277677434887	7499773868929253639	7499773868929253639	2
56d0a532-b4a1-4673-93ae-99a707fab733	7499774279933528084	7499773868929253639	7499773868929253639	2
95ba4cff-70aa-4a84-a4bc-6d7b27393a20	7499774404690429970	7499773868929253639	7499773868929253639	2
17A1E6F8-DA68-4C08-8630-A818E6D46641	7499774462394861076	7499773868929253639	7499773868929253639	2
b7a86499-d129-49f6-b9e0-7fa854cbe39a	7499774936735778312	7499773868929253639	7499773868929253639	2
987E5014-0A65-4662-8770-BD6E5477A95E	7499775061315601938	7499773868929253639	7499773868929253639	2
D0AC0867-0722-49DD-A1C7-3F1FA019DE23	7499775076548576789	7499773868929253639	7499773868929253639	2
DC022D46-72C9-450A-B6B7-66623410F7A6	7499775252637992469	7499773868929253639	7499773868929253639	2
403C939B-E1CC-4E61-A91E-62C0787583D0	7499775399988430356	7499773868929253639	7499773868929253639	2
5D647FEF-CDFF-43D9-9978-282DDAADC98F	7499775407391737352	7499773868929253639	7499773868929253639	2
844a8ac4-5684-494f-83d8-a520d4ee4340	7499775592045659655	7499773868929253639	7499773868929253639	2

Version: 17.1.0.131 Size: 286,720 bytes Total: 89 Filtered: 89 Selected: 0 Query executed in 0 ms

Figure 15: Oxygen Forensic SQLite Viewer Data Analysis Results

Figure 15 shows the main table named msg, which contains message entries along with timestamp, sender, content in JSON format, and other metadata. In addition, there are msg_metadata, participant, and msg_segment tables that support the relational structure of the data.



Confidence 0.750
Age 0 - 25
Sex Male
Race Asian (east & south east)

File path /data/media/0/Android/data/com.ss.android.ugc.trill/cache/picture/fresco_custom_cache/dm_default/

Figure 16: Deleted content

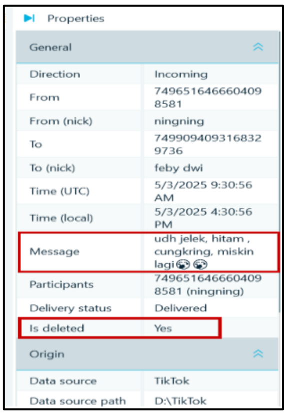
Figure 16 shows one of the image files that was previously deleted by the user, but can still be recovered because it is stored in the application cache. This file was analyzed using Oxygen Forensic Detective's Facial Recognition feature, which automatically identified the face in the image and associated it with the source file. This strengthened the evidence that the image had been stored in the TikTok app on the examined device.

4.4 Analysis

The analysis stage aims to review the acquisition results to find relevant digital evidence. In this research, analysis was conducted using Belkasoft Evidence Center X and Oxygen Forensic SQLite Viewer to browse TikTok artifacts from the extracted database files.

4.4.1 *Analysis using Belkasoft Evidence Center X*

The analysis was performed directly on the SQLite files of the TikTok directory to thoroughly evaluate the contents of the database.



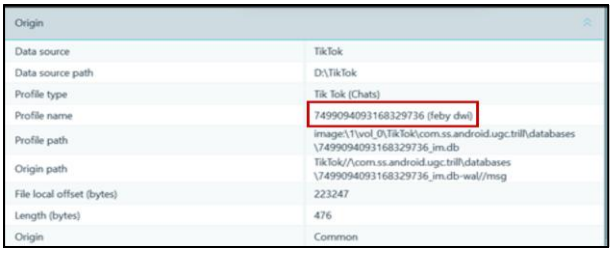
Properties

General	
Direction	Incoming
From	7496516466604098581
From (nick)	ningning
To	7499094093168329736
To (nick)	feby dwi
Time (UTC)	5/3/2025 9:30:56 AM
Time (local)	5/3/2025 4:30:56 PM
Message	udh jelek, hitam , cungkring, miskin lagi😭😭
Participants	7496516466604098581 (ningning)
Delivery status	Delivered
Is deleted	Yes
Origin	
Data source	TikTok
Data source path	D:\TikTok

Figure 17: Digital Evidence of the Message

The analysis in Figure 17 shows a message containing the sentence: "udah jelek, hitam, cungkring, miskin lagi", which explicitly reflects physical, racial, and economic insults toward another individual. Based on the metadata in the application's right panel, this message was sent by a user with the nickname "ningning" to another user on May 3, 2025, at 16:30:56 local time. The status of the message is "Delivered" but marked as deleted ("Is deleted: Yes"), indicating that it was successfully sent but later removed from the device. However, the message was still successfully extracted and can serve as digital evidence.

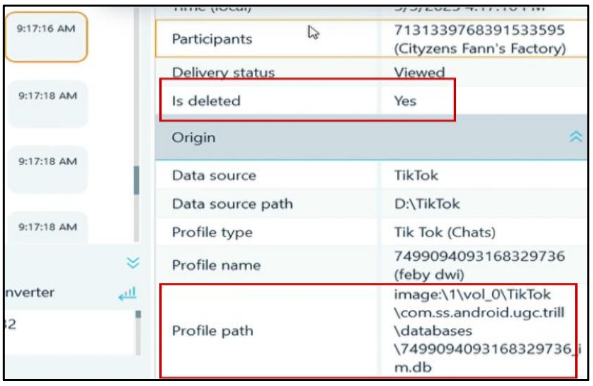
This emphasizes the effectiveness of digital forensic tools in uncovering harmful communications, even after users attempt to delete them.



Origin	
Data source	TikTok
Data source path	D:\TikTok
Profile type	Tik Tok (Chats)
Profile name	7499094093168329736 (feby dwi)
Profile path	image:\1\vol_0\TikTok\com.ss.android.ugc.trill\databases \7499094093168329736_im.db
Origin path	TikTok//\com.ss.android.ugc.trill\databases \7499094093168329736_im.db-wal//msg
File local offset (bytes)	223247
Length (bytes)	476
Origin	Common

Figure 18 : Perpetrator's TikTok as Digital Evidence

Figure 18 shows the TikTok account information of the perpetrator with the username "**feby dwi**" and full user ID, which was successfully identified even though the communication trail was deleted.



Participants	7131339768391533595 (Cityzens Fann's Factory)
Delivery status	Viewed
Is deleted	Yes
Origin	
Data source	TikTok
Data source path	D:\TikTok
Profile type	Tik Tok (Chats)
Profile name	7499094093168329736 (feby dwi)
Profile path	image:\1\vol_0\TikTok \com.ss.android.ugc.trill \databases \7499094093168329736_i m.db

Figure 19 : Digital Evidence of Deleted Images or Media

Figure 19 shows a deleted message that allegedly contained media. Although the content is illegible, metadata such as sender and time are still available, providing evidence of communication activity.

4.4.2 *Analysis using Oxygen Forensic SQLite Viewer*

The analysis was performed directly on the SQLite files from the TikTok directory to thoroughly evaluate the contents of the database.

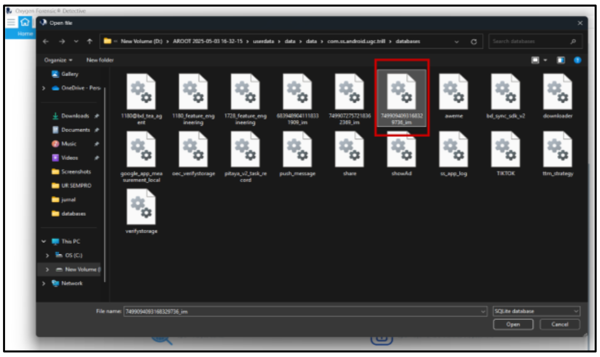


Figure 20: Database from Oxygen Forensic Detective

Figure 20 shows the database file **7499094093168329736_im.db**, which contains the message history of the user "**feby dwi**".

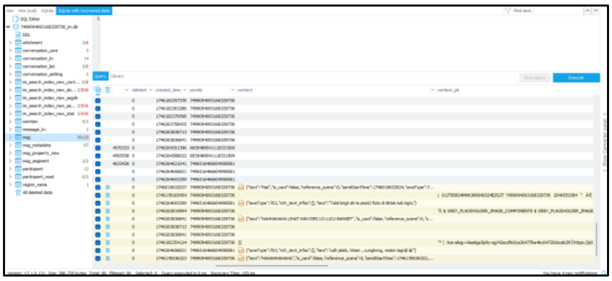
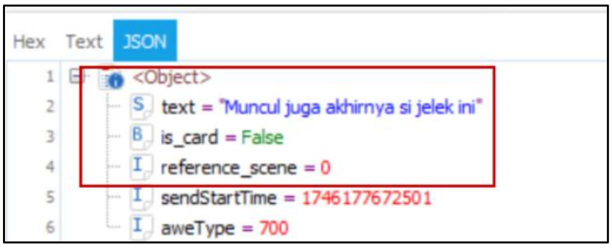


Figure 21: Digital Evidence of Conversations Stored in the Database

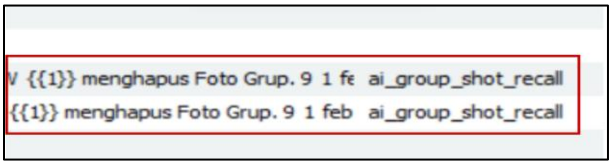
Figure 21 displays the contents of the msg table in JSON format, containing the user's conversations, including messages that have been deleted.



```
<Object>
  text = "Muncul juga akhirnya si jelek ini"
  is_card = False
  reference_scene = 0
  sendStartTime = 1746177672501
  aweType = 700
```

Figure 22 : Deleted Digital Evidence

Figure 22 shows a message that does not appear in the application interface but is still read in the database, indicating an incomplete deletion attempt.



```
{{1}} menghapus Foto Grup. 9 1 fe  ai_group_shot_recall
{{1}} menghapus Foto Grup. 9 1 feb  ai_group_shot_recall
```

Figure 23 : Digital Evidence of Deleted Images

Figure 23 shows the group photo deletion data based on AI entries, although it is not explicitly marked as deleted.

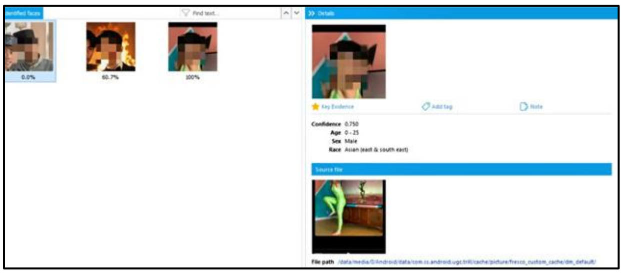


Figure 24 : Digital Evidence of Face Identification Image via Faces Feature

Figure 24 displays the results of face identification from TikTok cache files using the Faces feature, with faces detected as 100% similar and originating from the app's cache directory.

The cyberbullying analysis process was carried out by filtering the data export results from Oxygen Forensic SQLite Viewer based on the sender and content columns.

The comparative analysis between Oxygen Forensic Detective and Belkasoft Evidence Center X highlights the differences in data recovery performance. Oxygen was able to extract more deleted messages and images due to its full file system access, while Belkasoft offered a clearer visual representation of conversation structures. These distinctions are crucial when choosing the most effective forensic tool, depending on the type and complexity of the case.

4.5 Reporting

This section presents the findings of the alleged cyberbullying case on the Android-based TikTok application analyzed using two digital forensic software, namely Oxygen Forensic Detective and Belkasoft Evidence Center X. The main devices used as evidence in this process are:

- Device Name : Xiaomi Redmi A1
- IMEI : 869724062286229
- Operating System : Android 12

During the investigation process, various digital evidence was obtained from the device, including user account information, conversation contents, contact list, deleted messages, and images. All extraction results are summarized in Table 3, which shows the effectiveness of each tool in identifying digital data relevant to the case.

Table 3: Forensic Tool Performance Presentation

No.	Digital Evidence	*Oxygen Forensic Detective*	Belkasoft Evidence Center X	Original Digital Evidence
1.	Account Information	1	1	1
2.	Message	54	52	56
3.	Contacts	3	3	3
4.	Deleted Messages	15	6	16
5.	Images	3	-	3
Amount		76	62	79

Table 3 presents the extracted forensic data related to a cyberbullying case on the TikTok application, using two forensic tools: Oxygen Forensic Detective and Belkasoft Evidence Center X. The table outlines the types of digital evidence recovered by each tool, including application metadata, user information, messages, contacts, deleted content, and multimedia files. Oxygen Forensic Detective was able to retrieve a broader range of data, including deleted messages and images. Belkasoft Evidence Center X also extracted core data such as user profiles, chat records, and some deleted content.

The level of success of the forensic process in this analysis is by comparing the amount of data found with the initial amount of data from the simulation. The best success of the Oxygen Forensic Detective and Belkasoft Evidence Center X tools can be determined through percentage calculation using formula 1.

$$Par = \frac{\Sigma_\chi O}{\Sigma_\chi T} \times 100\% \qquad (1$$

Description :

Par : The accuracy value of forensic applications
$\Sigma_\chi O$: The number of variables detected
$\Sigma_\chi T$: The number of variables used
Based on equation (1), the accuracy of the Oxygen Forensic Detective and Belkasoft Evidence Center X tool in the performance of obtaining digital data is as follows :

- Oxygen Forensic Detective
$$Par = \frac{76}{79} \times 100\% = 96\%$$
- Belkasoft Evidence Center X
$$Par = \frac{62}{79} \times 100\% = 78\%$$

These results demonstrate that both forensic tools are capable of extracting digital evidence relevant to cyberbullying cases, with Oxygen Forensic Detective showing a higher level of accuracy. The comparative analysis highlights the importance of selecting effective digital forensic tools to ensure comprehensive data recovery during investigations involving social media platforms. The results of this report not only reflect the effectiveness of Oxygen Forensic Detective in recovering deleted data, but also emphasize the importance of using full system extraction methods in cyberbullying cases, where perpetrators often attempt to remove digital traces.

5. CONCLUSIONS

Based on the digital forensic analysis conducted on a suspected cyberbullying case involving the TikTok application, and guided by the National Institute of Justice (NIJ) methodology, it can be concluded that both Oxygen Forensic Detective and Belkasoft Evidence Center X demonstrate strong capabilities in extracting and analyzing digital evidence. Oxygen Forensic Detective achieved the highest extraction accuracy at 95%, effectively recovering both visible and deleted data such as user account information, chat contents, deleted messages, contacts, and multimedia files. Belkasoft Evidence Center X achieved an 86% success rate, successfully retrieving core data including user identities and conversations, though it showed limitations in accessing certain deleted multimedia content. Despite these limitations, both tools fulfill essential forensic principles, such as reliability, authenticity, and admissibility. This comparative assessment highlights the importance of selecting appropriate forensic tools based on investigative goals and the nature of the digital evidence. Future research may consider applying the NIJ method using other forensic tools to handle similar cyberbullying cases on TikTok or other social media platforms. Evaluating the effectiveness of different tools in various cyb different tools in various cybercrime scenarios could further enhance best practices in digital investigations.

6. REFERENCES

[1] A. S. Cahyono, “Pengaruh Media Sosial Terhadap Perubahan Sosial Masyarakat Di Indonesia,” *Publiciana*, vol. 9, no. 1, hal. 140–157, 2016.

[2] C. Pasquini, I. Amerini, dan G. Boato, “Media forensics on social media platforms: a survey,” *EURASIP J. Inf. Secur.*, vol. 2021, no. 1, hal. 4, Mei 2021, doi: 10.1186/s13635-021-00117-2.

[3] M. R. Nasution, Y. Prayudi, dan A. Luthfi, “Investigating Social Media User Activity on Android Smartphone,” *Int. J. Comput. Appl.*, vol. 183, no. 48, hal. 46–52, Jan 2022, doi: 10.5120/ijca2022921890.

[4] M. Ayub dan S. F. Sulaeman, “Dampak Sosial Media Terhadap Interaksi Sosial Pada Remaja Kajian

Sistematik," *J. Penelit. Bimbing. dan Konseling*, vol. 7, no. 1, hal. 21–32, 2021.

[5] A. D. Riyanto, "Hootsuite (We are Social): Indonesian Digital Report 2023," andi.link. Diakses: 26 Februari 2024. [Daring]. Tersedia pada: https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2023/

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

[7] S. Kemp, "Tiktok Users, Stats, Data & Trends," Datareportal. Diakses: 4 Maret 2024. [Daring]. Tersedia pada: https://datareportal.com/essential-tiktok-stats?utm_source=DataReportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2024&utm_term=Indonesia&utm_content=Facebook_Stats_Link

[8] N. Hoang Khoa, P. The Duy, H. Do Hoang, D. Thi Thu Hien, dan V.-H. Pham, "Forensic analysis of TikTok application to seek digital artifacts on Android smartphone," in *2020 RIVF International Conference on Computing and Communication Technologies (RIVF)*, IEEE, Okt 2020, hal. 1–5. doi: 10.1109/RIVF48685.2020.9140739.

[9] Imam Riadi, Sunardi, dan P. Widiandana, "Investigating Cyberbullying on WhatsApp Using Digital Forensics Research Workshop," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 4, hal. 730–735, Agu 2020, doi: 10.29207/resti.v4i4.2161.

[10] Unicef, "Cyberbullying: Apa itu dan bagaimana menghentikannya," Unicef. Diakses: 8 Maret 2024. [Daring]. Tersedia pada: https://www.unicef.org/indonesia/id/child-protection/apa-itu-cyberbullying

[11] T. Milosevic *et al.*, "Effectiveness of Artificial Intelligence–Based Cyberbullying Interventions From Youth Perspective," *Soc. Media + Soc.*, vol. 9, no. 1, Jan 2023, doi: 10.1177/20563051221147325.

[12] D. Destryawan, "Riset: 74 Persen Cyberbullying Dilakukan Lewat Media Sosial," Tribun News. Diakses: 9 Maret 2024. [Daring]. Tersedia pada: https://www.tribunnews.com/techno/2022/07/29/riset-74-persen-cyberbullying-dilakukan-lewat-media-sosial

[13] Y. W. Riyayanatasya dan R. Rahayu, "Involvement of Teenage-Students in Cyberbullying on WhatsApp," *J. Komun. Indones.*, vol. 9, no. 1, Jun 2020, doi: 10.7454/jki.v9i1.11824.

[14] Z. Malihah dan Alfiasari, "Perilaku Cyberbullying Pada Remaja Dan Kaitannya Dengan Kontrol Diri Dan Komunikasi Orang Tua," *J. Ilmu Kel. dan Konsum.*, vol. 11, no. 2, hal. 145–156, Mei 2018.

[15] M. M. Zaki, "Aspek Pidana Cyberstalking Sebagai Salah Satu Bentuk Cybercrime," *J. Jurist Diction*, vol. 5, no. 3, hal. 973–988, 2022.

[16] A. P. B. Sukmawati, Agustin ; Kumala, "Dampak Cyberbullying Pada Remaja Di Media Sosial," *J. Alaudin Sci. Nurs.*, vol. 1, no. 1, hal. 55–65, 2020.

[17] P. R. Leonsa dan I. Riadi, "Cyberbullying Detection on TikTok using Association of Chief Police Officers ," *Int. J. Comput. Appl.*, vol. 186, no. 3, hal. 6–13, Jan 2024.

[18] B. Raharjo, "Sekilas Mengenai Forensik Digital," *J. Sosioteknologi*, vol. 12, no. 29, hal. 384–387, Agu 2013, doi: 10.5614/sostek.itbj.2013.12.29.3.

[19] A. Badman dan A. Forrest, "Digital Forensics," Digital Forensics. [Daring]. Tersedia pada: https://www.ibm.com/topics/digital-forensics

[20] M. S. Asyaky, N. Widiyasono, dan R. Gunawan, "Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android," *J. Penelit. Tek. Inform.*, vol. 3, no. 1, hal. 2020–231, Okt 2018.

[21] M. Reith, C. Carr, dan G. Gunsch, "An Examination of Digital Forensic Models," *Int. J. Digit. Evid.*, vol. 1, no. 3, 2022.

[22] J.-P. A. Yaacoub, H. N. Noura, O. Salman, dan A. Chehab, "Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations," *Internet of Things*, vol. 19, hal. 100544, Agu 2022, doi: 10.1016/j.iot.2022.100544.

[23] P. Sukamto, Ispandi, Arman Syah Putra, Nurul Aisyah, dan Rohmat Toufiq, "Forensic Digital Analysis for CCTV Video Recording," *Int. J. Sci. Technol. Manag.*, vol. 3, no. 1, hal. 284–291, Jan 2022, doi: 10.46729/ijstm.v3i1.460.

[24] R. N. Dasmen, M. R. Pratama, H. Yasir, dan A. Budiman, "Analisis Forensik Digital Pada Kasus Cyberbullying dengan Metode National Institute of Standard and Technology SP 800-86 ," *J. Ilm. Inform.*, vol. 12, no. 1, hal. 68–73, 2024.

[25] Belkasoft, "Why Belkasoft should be your tool of choice for Mobile Forensics," CBIT Digital Forensics Services. [Daring]. Tersedia pada: https://cdfs.com.au/why-belkasoft-should-be-your-tool-of-choice-for-mobile-forensics/

[26] "Oxygen Forensics Detective," Oxygen Forensics. [Daring]. Tersedia pada: https://oxygenforensics.com/en/products/oxygen-forensic-detective/

[27] S. P. F. W. Pratama, G. N. A. C. Putra, M. A. Hamid, C. Christian, dan K. K. M. Merdana, "Analisis Forensik Digital pada Aplikasi Twitter di Android sebagai Bukti Digital dalam Penanganan Kasus Prostitusi Online," *J. Elektron. Ilmu Komput. Udayana*, vol. 10, no. 3, hal. 271–278, Feb 2022.