Cyberbullying Detection on TikTok using Association of Chief Police Officers

Pangestika Rona Leonsa
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
Along with increasingly rapid technological developments, the growth of social media users is also increasing, as is cybercrime activity. Social media applications in Indonesia, such as TikTok are ranked second with the most users in the world. So this application is vulnerable to cyber crimes such as cyberbullying. This research aims to investigate the TikTok application in cases of cyberbullying. The research object that will be discussed in this research is the Tiktok application which runs on Android-based smartphones. This research uses the Association of Chief Police Officers (ACPO) method which has four research stages: planning, collection, analysis, and presentation. The tools used in this research are MOBILedit Forensic Express, Magnet AXIOM, and DB Browser for SQLite. The research results show that the MOBILedit Forensic Express forensic tool obtained forensic accuracy calculation results with a percentage of 85%. AXIOM Magnet obtained forensic accuracy calculation results with a percentage of 91%. DB Browser for SQLite obtained forensic accuracy calculation results with a percentage of 87%. Based on research results, the tool can retrieve evidence in the form of application information, usernames, messages, contacts, and deleted messages.

Keywords
ACPO; Cyberbullying; Forensics; Mobile; TikTok.

1. INTRODUCTION
The growth of information technology which is proliferating every year makes it easy for its users to get information easily and quickly. Social media is also a place to get various information and communication with each other without being limited by space and time. There are several types of social media, including social networks, discussion forums, media Sharing networks, social blogging networks, etc [1], [2].
The number of social media used lately has an impact on social life and society [3]. The positive impact of the existence of social media is that it makes it easier for users to expand their relationships by communicating with many people without any limitations on distance and time [4]. On the other side, social media's disadvantages is making users addicted to the internet, vulnerable to the bad influence of others, decreasing face-to-face communication, and cybercrime [5].
Along with the rapid development of technology, the growth of social media users is also increasing. By early 2022, Indonesia had 191 million active social media users. The number of active social media users increased by 12.6% from 2021 to 2022. The most frequently used social media include WhatsApp (88.7%), Instagram (84.8%), Facebook (81.3%), TikTok (63.3%), and Telegram (62.3 %) [6]. The increasing number of social media apps has facilitated the creation of numerous major cybercrimes [7].
TikTok ranks third as the favorite social media in Indonesia with the second largest number of users of 112.9 million people [8]. TikTok is a social media service from China that focuses on video hosting so that users can create interesting videos equipped with filters and music provided [9]. TikTok features can cause major issues when used by a youngster or teenager who does not fully understand the dangers of the social network [10]. Because its users are primarily interested in text, photos, and videos, TikTok has turned into a haven for people who disseminate hoaxes and participate in cyberbullying [11].
Cyberbullying is an aggressive act that is carried out repeatedly both individually and in groups to scare, anger, or embarrass the victim by using digital technology [12]. Various digital platforms as a means of cyberbullying, social media is the digital platform where cyberbullying occurs most [13], [14]. As many as 95.6% of respondents said that there were many cases of cyberbullying in Indonesia [15], [16]. There are 4 forms of cyberbullying on TikTok including Flaming, Harassment, Denigration, and Trickery [17], [18].
Cases of cyberbullying in Indonesia need to be studied by conducting a forensic investigation process on the morning of the perpetrator. This research, it is hoped that it can help the process of investigating cyberbullying cases on the TikTok application service using the MOBILedit Forensic Express, Magnet Axiom, and DB Browser for SQLite using Association of Chief Police Officers (ACPO) method.

2. LITERATURE STUDY
2.1 Digital Forensic
Digital forensics is a category of forensic science that is used to search for or find digital evidence using the scientific method so that it can be accepted in court [19]. Digital forensics has several scientific categories such as Computer Forensics, Mobile Forensics, Digital Video and Photo Forensics, etc [20]. Mobile forensics is the science that studies the acquisition or recovery of digital evidence from smartphone to catch criminals who use smartphone [21].

2.2 Digital Evidence
Digital evidence is digital data from the acquisition of electronic evidence contained in electronic devices that can support or deny a particular crime, as well as provide clues that lead to a violation [22], [23] . The data can be in the form of files, images, text, videos, emails, and logs. There are 5 characters of digital evidence, including admissible, authentic, complete, reliable, and believable [24], [25].

2.3 Cyberbullying
Cyberbullying is individual or group behavior to hurt someone by using digital technology [18]. Since cyberbullying entails using online platforms to harass, threaten, or intimidate others and frequently has profound emotional and psychological

repercussions, it has become a major concern in today's digital age [26], [27]. Types of cyberbullying include flaming, harassment, denigration, outing, and cyberstalking [12], [15].

2.4 MOBILedit Forensic Express

MOBILedit Forensic Express is used to gather, examine, and generate reports on data extracted from smartphones that can assist investigators in collecting digital evidence using several stages [28]. This tool can restore deleted data such as chats, history, photos, videos, recordings, and contacts. MOBILedit Forensic Express has several advantages over other applications such as Physical data acquisition and analysis, Advanced Application Analytics, Deleted data recovery, and Easy to use user interface.

2.5 Magnet Axiom

Magnet Axiom is software that can extract evidence from various sources without being detected and eliminating data. Because it can analyze digital evidence from mobile, cloud, computer, and car sources as well as third-party extractions all in one case file, Magnet Axiom is one of the forensic programs that experts recommend [29]. Magnet Axiom can swiftly and automatically identify evidence pertinent to a case by utilizing strong and user-friendly analytical techniques.

2.6 DB Browser for SQLite

DB Browser for SQLite can be used to analyze and extract data from SQLite databases that are accessible on a variety of digital devices, including web browsers and mobile devices. Features created especially for forensic analysis that enable detectives to look into SQLite database contents and retrieve pertinent data [30]. Some of the primary functions and uses of DB Browser for SQLite in digital forensic investigations are database Analysis, data Extraction, and data Visualization.

2.7 Association of Chief Police Officers

In the area of digital forensics, the Association of Chief Police Officers (ACPO) uses a research methodology that is divided into four distinct stages that are well thought out in order to support comprehensive investigations and case resolutions [31], [32]. The first step involves meticulous preparation, and the second step relates to gathering relevant information. The third stage pays attention to the comprehensive examination of the gathered data, While the fourth stage is primarily focused on presenting the results and conclusions to pertinent stakeholders and authorities [33], [34].

3. RESEARCH METHODS

This research uses the Association of Chief Police Officers (ACPO) method to execute the investigation proses that has four research stages, namely plan, capture, analyze, and present. The Association of Chief Police Officers (ACPO) stage can be seen in Figure 1.

Figure 1: Stages of ACPO Method

Figure 1 show the step of Association of Chief Police Officers (ACPO) method. The plan stage is planning the equipment that will take during the research. The capture is the stage of recording, storing, capturing and collecting all the results obtained from the research process. The Analyze stage is the process of analyzing evidence found from the capture process. Present is the stage of presenting findings that can be accounted for [35].

4. RESULTS AND DISCUSSION

This research examines and analyzes cases of cyberbullying on the TikTok application using the Association of Chief Police Officers (ACPO). The study develops in three unique stages in order to completely investigate the phenomenon: pre-incident, incident, and post-event. The fist simulation, pre-incident can be seen in Figure 2.

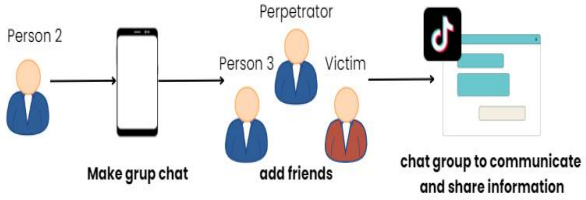

Figure 2: Pre-Incident of Cyberbullying Case

Figure 2, Person 2 created a chat group on the TikTok app with the intention of friendship and connection between them, particularly through the sharing of content and experiences pertaining to the TikTok platform. They actively discuss trends, tips, and tricks, and share creative videos and ideas to enrich their TikTok experience.

The second stage of case simulation is incident that can be seen in Figure 3.

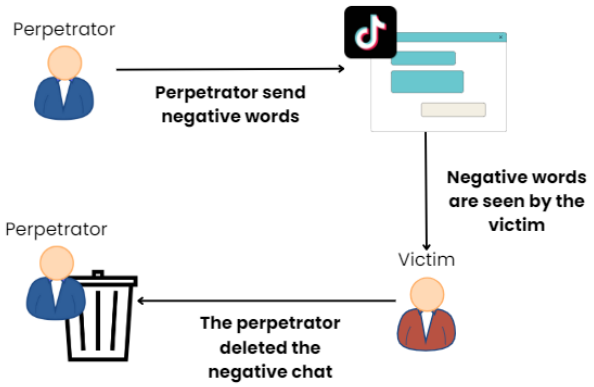

Figure 3: Incident of Cyberbullying Case

Figure 3 depicts the incident where the perpetrator uttered negative words towards the victim. The perpetrator repeatedly used words such as "Fat, Ugly, Stupid, etc." in the TikTok chat group. This action makes the victim feel isolated, depressed, and uncomfortable in the chat group. In fact, the perpetrator also deleted messages that offended the victim, trying to remove traces of the bullying that had occurred.

The last stage of case simulation is post-incident that can be seen in Figure 4.

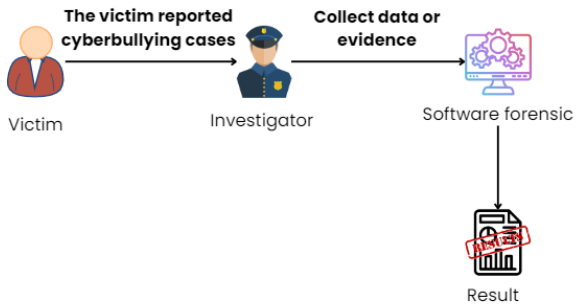

Figure 4: Post-Incident of Cyberbullying Case

Figure 4 The victim reported the cyberbullying case he experienced to the authorities. The victim showed proof of the perpetrator's account and conversations held in the TikTok chat group. The victim explained the chronology of what had happened and the police carried out an investigation and arrested the perpetrator.

4.1 Plan

The planning stage is carried out by documenting the evidence obtained. At this stage, planning is also carried out regarding the hardware and software used. The documentation of the evidence can be seen in Figure 5.

Figure 5: Evidence Obtained

Figure 5 shows that the evidence obtained is then documented. The documentation obtained is in the form of a smartphone with the XIOMI Redmi 4x.

The tools dan material that will be use in the form of hardware and software which can be seen in Table 1.

Table 1. Tools and Material

No	Tools and Materials	Description
1	Laptop	Lenovo Ideapad Intel(R) Core (TM) i3-6100U CPU @ 2.30GHz 2.30 GHz
2	Smartphone	XIOMI Redmi 4X
3	TikTok	Mobile applications
4	MOBILedit Forensic	Forensic software tool
5	Magnet AXIOM	Forensic software tool
6	DB SQL	Forensic software tool

Tabel 1 shows the tools and materials that will be use in this research. The hardware that will be use are Laptop and Smartphone. The software is MOBILedit Forensic, Magnet AXIOM and DB SQL

4.2 Capture

The first stage carried out in this process is to maintain digital evidence and check the authenticity of the evidence. Safeguarding digital evidence uses isolation techniques to avoid things that can damage digital evidence.

Figure 6: The Isolation Technique

Figure 6 show the isolation technique on a evidence where this step is carried out by changing the status of the smartphone to airplane mode.

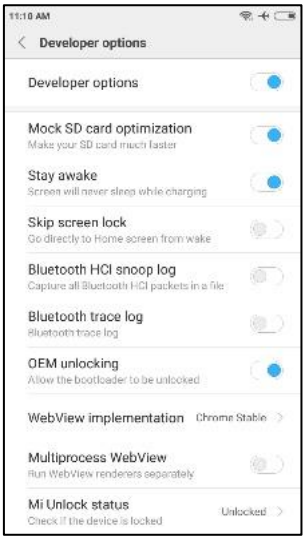

Figure 7: Developer Options

Figure 7 is the second stage which is to activate the developer option in the settings menu. The next step is to activate stay awake and enable USB debug. Stay awake is done so that the smartphone is not in sleep mode when carrying out the forensic process. Activating USB debug is used to connect to the USB connector on the workstation. The process of capturing digital

evidence in this research was carried out using the MOBILedit Forensic Express and Magnet AXIOM tools.

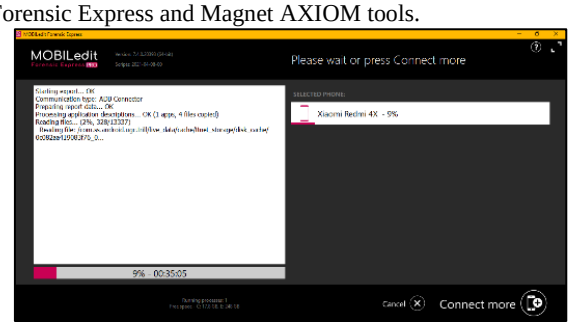

Figure 8: Extraction Process on Smartphone

Figure 8 is the process of extracting evidence using MOBILedit Forensic Express. MOBILedit produces various reports from the capture results that have been carried out.

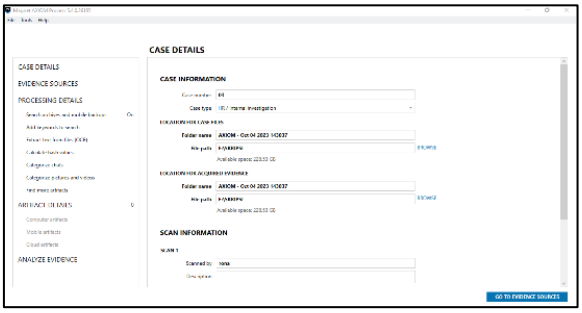

Figure 9: Case Details Menu on Magnet Axiom

Figure 9 is the process of capturing using Magnet Axiom by filling case information.

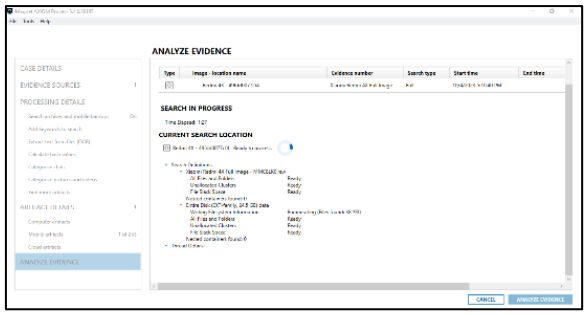

Figure 10: Capture Process Using Magnet Axiom

Figure 10 is the extraction process for evidence. The duration of this process varies depending on the data stored on the smartphone.

4.3 Analyze

This stage processes the data that was successfully captured at the capture stage using MOBILedit Forensic Express and Magnet AXIOM. The extracted data will be analyzed using MOBILedit Forensic Express, Magnet AXIOM, and DB Browser for SQLite.

4.3.1 *Analyze Using MOBILedit Forensic Express*

The resulting capture process provides a report in HTML form. This HTML file will then be analyzed to identify data that has been deleted by the perpetrator in this case. Based on the forensic evidence process, this reseach managed to find deleted message information, application information, account names and the time of the incident.

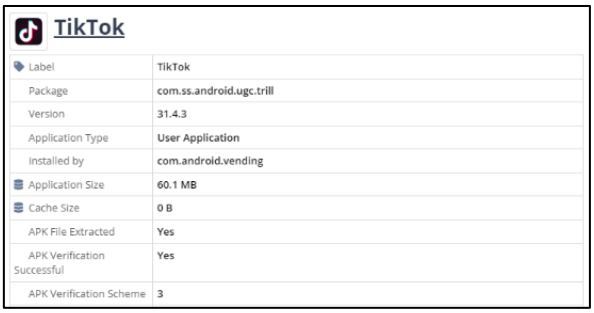

Figure 11: Aplication Information

Figure 11 is the application information used. TikTok, version 31.4.3, is the program that is being used by perpetrators to carry out cyberbullying acts.

Figure 12: Digital Evidence of Perpetrator's Tiktok Account

Figure 12 is the application user name. The search results succeeded in finding the nickname of the perpetrator of the cyberbullying crime. Nickname found in the name of "Azura Dua"

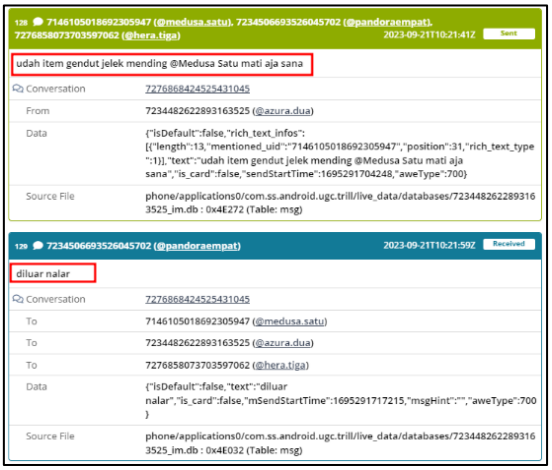

Figure 13: Digital Evidence of Messages

Figure 13 is the result of an analysis of bullying-related messages. Messages with the word "udah item gendut jelek mending @Medusa Satu mati aja sana" have been deleted by the perpetrator. The message is identical to the one that was sent by the perpetrator to the victim in terms of character quantity and timing. According to the HTML page report, no information was found indicating whether the message delivered had been removed or not.

4.3.2 *Analyze Using Magnet Axiom*

The analysis stage uses the AXIOM Magnet, namely from the extraction results in the capture process. At this stage, information is found in the form of account names, contacts and messages.

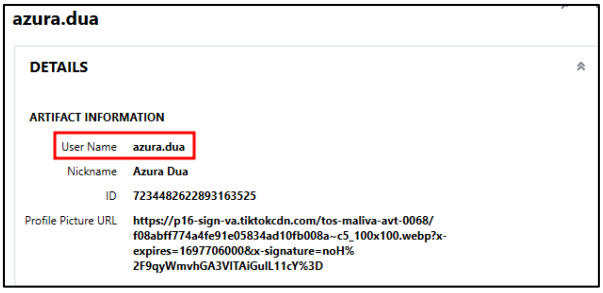

Figure 14: Digital Evidence of Perpetrator's Username

Figure 14 shows the username of the application user where the cyberbullying perpetrator is. This process succeeded in finding the perpetrator's username "azura.dua" with ID 7234482622893163525

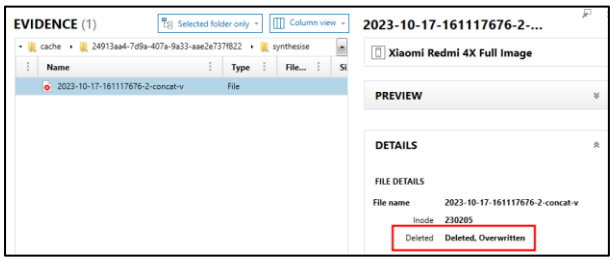

Figure 15: Digital Evidence of Deleted Video

Figure 15 is Digital Evidence of deleted video uploaded by the perpetrator in a cyberbullying case. Magnet Axiom succeeded in identifying videos but the file extension was not found.

Figure 16: Digital Evidence of Deleted Messages

Figure 16 shows messages that have been deleted by the perpetrator. The analysis results show that the message contains "udah item gendut jelek mending @Medusa Satu mati aja sana". The message was sent by 7234482622893163525. Magnet Axiom detected that the message had also been deleted by the sender. .

4.3.3 *Analyze Using DB Browser for SQLite*

The analysis stage uses DB Browser for SQLite, namely by analyzing the database files that have been acquired using MOBILedit Forensic Express. The database files are found in the acquisition folder phone\applications0\com.ss.android.ugc.trill\live_data\databases. The results obtained can strengthen the evidence in this research

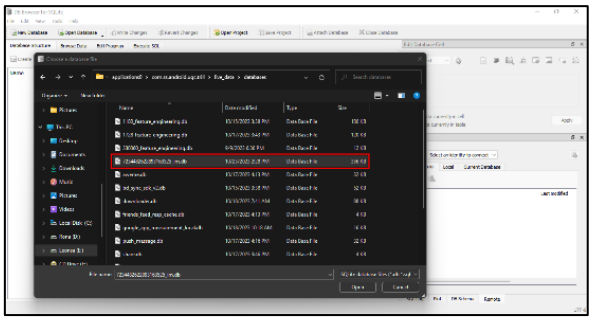

Figure 17: Database from MOBILedit Forensic

Figure 17 shows the database that will be analyzed. The database analyzed is a message database with the name 7234482622893163525_im.db in the msg table.

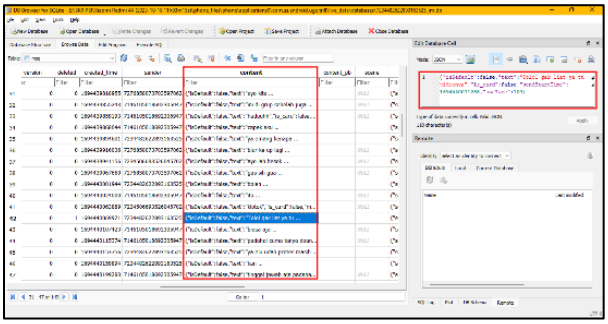

Figure 18: Digital Evidence of Conversations Stored in Database

Figure 18 is evidence of a conversation database found using DB Browser for SQLite. The next analysis process using DB Browser for SQLite is carried out by filtering the database. This process can be done by writing the number 1 in the deleted filter to find messages deleted by the perpetrator.

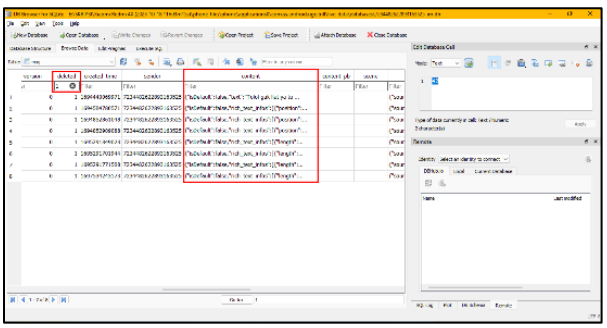

Figure 19: Digital Evidence of Deleted Conversations

Figure 19 shows messages deleted by the perpetrator. The results of this analysis found 8 messages that were deleted by the perpetrator.

4.4 Present

This present stage contains the results of findings on cyberbullying cases on the Tiktok Android application using the MOBILedit Forensic Express, Magnet AXIOM, and DB Browser for SQLite tools. The physical evidence found was a smartphone with the following specifications:

- Device name : Xiaomi Redmi 4X
- IMEI : 864744037340922
- Operating system : Android 7.1.2

Data obtained during the process of examining and analyzing digital evidence in the TikTok application using the MOBILedit Forensic Express, Magnet AXIOM and DB Browser for SQLite tools using the Association of Chief Police Officers (ACPO) method can be seen in table 2.

Table 2: List of digital evidence found

No.	Digital evidence	MOBILedit Forensic Express	Magnet AXIOM	DB Browser for SQLite	Original Digital Evidence
1	Application info	1	1	-	1
2	Account info	1	1	-	1
3	Conversation	127	127	127	140
4	Contact	3	3	-	3
5	Deleted Messages	-	8	8	8
6	Video	-	1	-	1
Amount		132	141	135	154

Table 2 shows all forensic results obtained from cyberbullying cases on the TikTok application in chat groups on three forensic tools. The MOBILedit Forensic Express tool can extract data on smartphone evidence. This tool can find evidence in the form of application information, usernames, conversations, and contacts. The AXIOM Magnet tool can extract and analyze the data found. In this application, the data found is application information, username, conversations, contacts, and deleted message information. The DB Browser for SQLite tool can identify deleted messages based on the results of the extraction that has been carried out in MOBILedit Forensic Express.

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 MOBILedit Forensic Express, Magnet Axiom, and DB Browser for SQLite tools can be determined through percentage calculations using formula 1.

$$Par = \frac{\Sigma ar0}{\Sigma arT}\ x\ 100\% \quad (1)$$

Description:

Par =The accuracy value of forensic applications

Σar0 =The number of variables detected

ΣarT =The number of variables used

Based on equation (1), the accuracy of the MOBILedit Forensic, Magnet Axiom, and DB Browser for SQLite tools in the performance of obtaining digital data is as follows:

- MOBILedit Forensic Express Performance

$$Par = \frac{132}{154}\ x\ 100\% = 85\%$$

- Magnet Axiom Performance

$$Par = \frac{141}{154}\ x\ 100\% = 91\%$$

- DB Browser for SQLite Performance

$$Par = \frac{135}{154}\ x\ 100\% = 87\%$$

5. CONCLUSIONS

Based on the results of research carried out with the title " Mobile Forensik on TikTok Application for cyberbullying using Association of Chief Police Officer (ACPO)" it can be concluded that the Association of Chief Police Officer (ACPO) method can be used in the forensic process of the Tiktok application to obtain digital evidence in cyberbullying cases. Deleted digital evidence can be recovered using MOBILedit Forensic Express, Magnet AXIOM and DB Browser for SQLite. In MOBILedit Forensic Express the results obtained are Application info, username, message and contact used by the perpetrator. MOBILedit Forensic Express tools cannot identify evidence in the form of messages deleted by the perpetrator. MOBILedit Forensic Express obtained forensic accuracy calculation results with a percentage of 85%. The AXIOM Magnet tool can obtain all digital evidence including Application info, usernames, messages, contacts and deleted messages. AXIOM Magnet obtained forensic accuracy calculation results with a percentage of 91%. DB Browser for SQLite can obtain evidence in the form of messages that have been deleted by the perpetrator. DB Browser for SQLite obtained forensic accuracy calculation results with a percentage of 87%. This study can help improve TikTok users' security and safety from cyberbullying. The ACPO framework used in this study can provide guidance and direction for investigations into TikTok-related cybercrimes.

6. REFERENCES

[1] N. Al Mutawa, I. Baggili, and A. Marrington, “Forensic Analysis of Social Networking Applications on Mobile Devices,” *Digit. Investig.*, vol. 9, no. 3, pp. 24–33, 2020, doi: 10.1016/j.diin.2012.05.007.

[2] C. Pasquini, I. Amerini, and G. Boato, “Media Forensics on Social Media Platforms: a Survey,” *Eurasip J. Inf. Secur.*, vol. 1, no. 4, pp. 2–19, 2021, doi: 10.1186/s13635-021-00117-2.

[3] R. Junco and S. R. Cotten, “Perceived Academic Effects of Instant Messaging use,” *Comput. Educ.*, vol. 56, no. 2, pp. 370–378, Feb. 2011, doi: 10.1016/j.compedu.2010.08.020.

[4] M. R. Nasution, Y. Prayudi, and A. Luthfi, "Investigating Social Media User Activity on Android Smartphone," *Int. J. Comput. Appl.*, vol. 183, no. 48, pp. 46–52, 2022, doi: 10.5120/ijca2022921890.

[5] C. Wu and J. Wang, "Analysis of Cyberterrorism and Online Social Media," *4th Int. Conf. Mod. Manag. Educ. Technol. Soc. Sci. (MMETSS 2019)*, vol. 351, no., pp. 925–927, 2019, doi: 10.2991/mmetss-19.2019.189.

[6] we are social dan hootsuite, "Hootsuite (We are Social): Indonesian Digital Report 2023." Accessed: Sep. 12, 2023. [Online]. Available: https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2023/

[7] V. L. Schul'tz, V. V. Kul'ba, A. B. Shelkov, and L. V. Bogatyryova, "Scenario Analysis of Improving the Effectiveness of Cybercrime Investigation Management Problems," *Int. Fed. Autom. Control - Pap. OnLine*, vol. 54, no. 13, pp. 155–160, 2021, doi: 10.1016/j.ifacol.2021.10.437.

[8] https://datareportal.com/, "Tiktok Users, Stats, Data & Trends." Accessed: Sep. 16, 2023. [Online]. Available: https://datareportal.com/essential-tiktok-stats?utm_source=DataReportal&utm_medium=Country_Article_Hyperlink&utm_campaign=Digital_2023&utm_term=Indonesia&utm_content=Facebook_Stats_Link

[9] P. Domingues, R. Nogueira, J. C. Francisco, and M. Frade, "Analyzing tiktok from a digital forensics perspective," *J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl.*, vol. 12, no. 3, pp. 87–115, 2021, doi: 10.22667/JOWUA.2021.09.30.087.

[10] N. Hoang Khoa, P. The Duy, H. Do Hoang, D. Thi Thu Hien, and V. H. Pham, "Forensic Analysis of TikTok Application to Seek Digital Artifacts on Android Smartphone," *Proc. - 2020 RIVF Int. Conf. Comput. Commun. Technol. RIVF 2020*, vol. 8, no. 4, pp. 6–11, 2020, doi: 10.1109/RIVF48685.2020.9140739.

[11] P. Widiandana, I. Riadi, and Sunardi, "Investigasi Cyberbullying pada WhatsApp Menggunakan Digital Forensics Research Workshop," *J. Eng. Sci. Technol.*, vol. 1, no. 3, pp. 730–735, 2019.

[12] T. Milosevic *et al.*, "Effectiveness of Artificial Intelligence Based Cyberbullying Interventions From Youth Perspective," *Soc. Media Soc.*, vol. 9, no. 1, pp. 2–12, 2023, doi: 10.1177/20563051221147325.

[13] Z. Khyioon Abdalrdha, A. Mohsin Al-Bakry, and A. K. Farhan, "A Survey on Cybercrime Using Social Media," *Iraqi J. Comput. Informatics*, vol. 49, no. 1, pp. 52–65, 2023, doi: 10.25195/ijci.v49i1.404.

[14] W. N. A. W. Ali, T. Q. Ni, and S. Z. S. Idrus, "Social Media Cyberbullying: Awareness and Prevention through Anti Cyberbully Interactive Video (ACIV)," *J. Phys. Conf. Ser.*, vol. 1529, no. 3, pp. 1–12, 2020, doi: 10.1088/1742-6596/1529/3/032071.

[15] A. A. A. Aradhana and C. S. Pangaribuan, "Cyberbullying in Media Social: A Mainstreaming the Victim Protection Principles in Indonesian Criminal Justice System," *Indones. Media Law Rev.*, vol. 1, no. 2, pp. 99–122, 2022, doi: 10.15294/imrev.v1i2.60587.

[16] N. Muthi'ah, U. Mono, and A. B. Perangin-Angin, "Indonesian Cyberbullying Issues: The Impoliteness in Communication," *Int. J. Educ. Lang. Relig.*, vol. 4, no. 2, p. 96, 2022, doi: 10.35308/ijelr.v4i2.5684.

[17] D. Setiana, T. Marlina, N. Norainna, B. Alifya, and S. Susanto, "Managing Cyberbullying Impacts In Time of Digital Ecosystem (Lesson Learned from TeensVictims-Actors Evidence from Jakarta)," *Adv. Soc. Sci. Educ. Humanit. Res.*, vol. 592, no. Iclhr, pp. 172–181, 2021.

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

[19] P. V Chavan, "Digital Forensics Based Analysis of Mobile Phones," *J. Android IOS Appl. Test.*, vol. 4, no. 3, pp. 5–8, 2019.

[20] H. Arshad, A. Bin Jantan, and O. I. Abiodun, "Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence," *J. Inf. Process. Syst.*, vol. 14, no. 2, pp. 346–376, 2020, doi: 10.3745/JIPS.03.0095.

[21] I. Riadi, A. Yudhana, and G. P. Inngam Fanani, "Mobile Forensic Tools for Digital Crime Investigation: Comparison and Evaluation," *Int. J. Saf. Secur. Eng.*, vol. 13, no. 1, pp. 11–19, 2023, doi: 10.18280/ijsse.130102.

[22] M. Reith, C. Carr, and G. Gunsch, "An Examination of Digital Forensic Models," 2002. doi: 10.1.1.13.9683.

[23] S. H. Belshaw, "Next Generation of Evidence Collecting: The Need for Digital Forensics in Criminal Justice Education," *J. Cybersecurity Educ. Res. Pract.*, vol. 1, no. 3, pp. 1–19, 2019, doi: 10.1109/JCERSP53098.2021.0011.

[24] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations," *Internet of Things (Netherlands)*, vol. 19, no. 4, pp. 56–66, 2022, doi: 10.1016/j.iot.2022.100544.

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

[26] A. T. Banowati and S. Nugraha, "Pengaruh Kepribadian Dark Triad terhadap Perilaku Cyberbullying pada Pengguna Media Sosial," *Bandung Conf. Ser. Psychol. Sci.*, vol. 4, no. 2, pp. 682–689, 2022, [Online]. Available: https://proceedings.unisba.ac.id/index.php/BCSPS/article/view/2879

[27] A. Monica Hartono, M. Syukron Febrianananda, D. Vita Achmada, P. Ilmu Komunikasi, and J. Ilmu Sosial, "Tiktok Sebagai PlatformVenting Mendorong Cyberbullying Gen-Z," *Pros. Semin. Nas. Ilmu Ilmu Sos. 2022*, vol. 2022, no. 13, pp. 13–22, 2022.

[28] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, "A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions," *IEEE Access*, vol. 10, no. 5, pp. 11065–11089, 2022, doi: 10.1109/ACCESS.2022.3142508.

[29] I. Riadi, R. Umar, and G. Fauzan, "Audio Forensics on Smartphone with Digital Forensics Research Workshop (DFRWS) Method," 2021. doi: https://doi.org/10.21512/commit.v15i1.6739.

[30] H. H. Lwin, W. P. Aung, and K. K. Lin, "Comparative Analysis of Android Mobile Forensics Tools," *2020 IEEE Conf. Comput. Appl.*, vol. 3, no. 1, pp. 1–6, 2020, doi: 10.1109/ICCA49400.2020.9022838.

[31] M. Iqbal and B. Soewito, "Digital Forensics on Solid State Drive (SSD) with TRIM Feature Enabled and Deep Freeze Configuration Using Static Forensic Methods and ACPO Framework Muhammad," *Int. J. Comput. Sci. Inf. Secur.*, vol. 18, no. 11, pp. 44–56, 2020, doi: https://doi.org/10.5281/zenodo.4428141.

[32] K. A. Latif, R. Hammad, T. T. Sujaka, K. Marzuki, and A. S. Anas, "Forensic Whatsapp Investigation Analysis on Bluestack Simulator Device Using Live Forensic Method With ACPO Standard," *Int. J. Inf. Syst. Technol.*, vol. 5, no. 3, pp. 331–338, 2021, doi: https://doi.org/10.30645/ijistech.v5i3.148.

[33] H. Lallie and L. Pimlott, "Applying the ACPO Principles in Public Cloud Forensic Investigations," *J. Digit. Forensics, Secur. Law*, 2012, doi: 10.15394/jdfsl.2012.1113.

[34] I. Riadi, A. Yudhana, and G. Fanani, "Comparative Analysis of Forensic Software on Android-based MiChat using ACPO and DFRWS Framework," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 7, no. 2, pp. 286–292, Mar. 2023, doi: 10.29207/resti.v7i2.4547.

[35] R. Y. Prasongko, A. Yudhana, and I. Riadi, "Analisis Penggunaan Metode ACPO (Association of Chief Police Officer) pada Forensik WhatsApp," *J. Sains Komput. Inform.*, vol. 6, no. 2, pp. 1112–1120, 2022, doi: 10.30645/j-sakti.v6i2.520.