# Forensic Investigation of a Cyberbullying Case on Platform X using Digital Forensic Research Workshop Method

Aisyah Syafi'i Nurjannah
Departement of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

## ABSTRACT
The rise in cyberbullying cases on social media has made digital forensic investigation a crucial approach for uncovering and proving perpetrators' activities in cyberspace. Platform X is one of the social media platforms vulnerable to misuse for bullying through user posts and interactions. This study aims to conduct a digital forensic investigation into a cyberbullying case on Platform X using the Digital Forensic Research Workshop (DFRWS) framework, uncover the digital traces left by the perpetrator, and analyze the application of the DFRWS stages in supporting the validation of digital evidence. The study employed a dead forensic method with a simulation approach based on a fake scenario. The investigation process was carried out through the stages of identification, preservation, collection, examination, analysis, and presentation, utilizing the software MOBILedit Forensic Express, SQLite DB Browser, and Oxygen Forensic Detective. The results show that the DFRWS framework supports a systematic investigative process and successfully identified 43 digital artifacts related to cyberbullying activities. These artifacts consisted of 2 account profiles, 37 tweets containing elements of cyberbullying, 3 deleted tweets, 2 search history records, and 2 GIF files used in the perpetrator's interactions. These findings made it possible to reconstruct the chronology of events and link the perpetrator's activities to the devices used, including deleted data. These findings made it possible to reconstruct the chronology of events and link the perpetrator's activities to the devices used. Thus, the application of the DFRWS framework can support the uncovering and substantiation of cyberbullying activities through relevant and admissible digital evidence in the law enforcement process.

### Keywords
Cyberbullying, DFRWS, digital evidence, digital forensics, Platform X.

## 1. INTRODUCTION
The development of digital technology and the increasing use of the internet have made social media an integral part of people's lives [1]. According to data from The Global Statistics, the number of internet and social media users in Indonesia continues to rise, with the platform X (formerly Twitter) becoming one of the most widely used social media platforms for sharing information and interacting directly [2]. As an open public forum, X allows users to express opinions, post comments, and share various types of content, such as text, images, and videos [3]. However, this freedom also creates opportunities for the misuse of social media, including the spread of hate speech and cyberbullying [4].

Cyberbullying is a form of bullying carried out through digital media, such as insults, harassment, the spread of false information, and repeated intimidation [5]. One case that garnered public attention in Indonesia was that of Luluk Sofiatul Jannah (Luluk Nuril) in 2023. A social media post containing insults directed at a student intern triggered a wave of attacks from netizens and had a negative impact on the victim's psychological well-being. This case demonstrates that social media activity can leave a digital trail that can be used as evidence in investigative processes [6].

One of the challenges in handling cyberbullying cases is the process of collecting and verifying digital evidence, especially when the perpetrator deletes the post or attempts to conceal their identity [7]. Therefore, the application of digital forensics is necessary to systematically identify, collect, analyze, and present digital evidence. One framework that can be used is the Digital Forensic Research Workshop (DFRWS), which consists of the stages of identification, preservation, collection, examination, analysis, presentation, and decision [15]. Compared to several other frameworks, such as NIST, NIJ, and ACPO, DFRWS has more detailed stages, making it suitable for investigations that require a structured process [12][15].

Several previous studies have applied digital forensics to social media, such as the analysis of digital evidence on the Threads platform [10], a live forensic-based investigation of cyberbullying on the X platform [11], an analysis of cyberbullying on TikTok [9], an investigation on WhatsApp [18], a comparison of forensic software on the X platform [19], and a test of the authenticity of deleted digital evidence [20].

## 2. STUDI LITERATUR
### 2.1 MOBILedit Forensic Express
MOBILedit Forensic Express is digital forensics software used to extract, analyze, and report data from various mobile devices. This software is capable of extracting various types of digital artifacts, such as messages, contacts, call history, multimedia files, app data, and even deleted data, and supports data analysis from various social media platforms.

### 2.2 Oxygen Forensic Detective
Oxygen Forensic Detective is digital forensic software used for the acquisition process, extraction, analysis, and reporting of digital evidence from various sources. In addition to supporting the recovery of deleted data, this software also allows the extraction and analysis processes to be performed within a single application, with support for multiple artifact types, making it easier for investigators to examine digital artifacts on mobile devices and social media.

## 2.3 SQLite DB Browser

SQLite DB Browser is a supporting software tool used to open and analyze SQLite-formatted database files. In digital forensic investigations, this application is used to examine database structures and trace digital artifacts stored locally on devices, such as conversation histories, account data, and application information.

## 2.4 Cyberbullying

Cyberbullying is a form of bullying carried out through digital media to hurt, intimidate, or humiliate others [22]. It can take the form of insults, the spread of false information, or repeated harassment via social media [23]. The widespread use of social media has increased the risk of cyberbullying incidents occurring across various online platforms. The effects of cyberbullying not only impact the victim's emotional well-being but can also lower self-esteem, trigger anxiety and depression [24], and in certain circumstances, may even lead to self-harm [25].

## 2.5 Digital Forensics

Digital forensics is the process of identifying, collecting, examining, analyzing, and reporting digital evidence to support legal proceedings [29]. In addition to helping uncover the perpetrator's activities, the application of digital forensics also preserves the authenticity and integrity of evidence [30]. Readiness in applying digital forensics is a key factor in effectively addressing cyber incidents [31].

## 2.6 Investigation Evidence Methods

Digital forensic investigation methods consist of live forensic and dead forensic. Live forensic is performed on devices that are still active to obtain volatile data stored in temporary memory [11], while dead forensic is performed on devices that have been turned off, so that the analysis focuses on stored data [12].

## 2.7 Digital Forensic Research Workshop (DFRWS)

Digital Forensic Research Workshop (DFRWS) is a digital forensic investigation framework used to systematically handle and analyze digital evidence [32]. This framework helps investigators maintain the integrity of evidence and ensures that each stage of the investigation is conducted in a structured manner so that the results obtained are reliable [33]. Additionally, DFRWS provides clear guidelines for handling digital evidence, from the identification stage to the presentation of investigation results from various types of digital evidence sources. With these systematic steps, the process of collecting, examining, and analyzing digital evidence can be carried out more effectively and purposefully. The framework is widely used in digital forensic investigations because it offers a clear and organized approach to evidence handling. Each stage has a specific objective that supports the identification, examination, and validation of digital evidence throughout the entire investigation process.. Furthermore, DFRWS supports investigators in reconstructing digital events based on the evidence obtained during the investigation. In this study, DFRWS was applied to facilitate a systematic investigation of a cyberbullying case on the X platform. The sequence of stages in the DFRWS framework used in this study is shown in Figure 1.


**Figure 1: Digital Forensic Research Workshop**

(DFRWS) Framework in Figure 1, the DFRWS framework consists of six stages identification, preservation, collection, examination, analysis, and presentation which are used to systematically identify, preserve, collect, examine, analyze, and present digital evidence [33].

## 2.8 Platform X

Platform X is a social media platform originally launched under the name Twitter in 2006 by Jack Dorsey, Biz Stone, Evan Williams, and Noah Glass. In 2023, Twitter officially changed its name to X after being acquired by Elon Musk, with a development strategy aimed at becoming an "everything app" that supports various digital services [3]. In addition to serving as a means of sharing information, this platform allows users to interact through features such as tweets, replies, retweets, and sharing multimedia content. The X platform's identity is shown in Figure 2.


**Figure 2: X Platform Logo and Interface**

Based on Figure 3, the X platform provides a space for public interaction that is fast-paced (real-time) and open. Characteristics these make X widely used for exchanging information and expressing opinions, but on the other hand, they also increase the potential for misuse, such as the spread of hate speech, verbal abuse, and cyberbullying [4]. Therefore, the X platform was selected as the research subject to examine the digital forensic investigation process regarding traces of cyberbullying activity.

# 3. RESEARCH METHODOLOGY

This study employs a static digital forensics method (dead forensics) by applying the Digital Forensic Research Workshop (DFRWS) framework to investigate a cyberbullying case on the X platform. The research was conducted through a scenario simulation using two smartphones: a Samsung Galaxy S20+ as the perpetrator's device and a Samsung Galaxy S21+ as the victim's device. The acquisition and analysis of digital evidence were performed using the software MOBILedit Forensic Express, Oxygen Forensic Detective, and SQLite DB Browser to obtain and validate the digital artifacts discovered during the investigation process.

## 3.1 Research Scenario Simulation

This study used a simulation approach based on a fake scenario to represent a cyberbullying case on Platform X. The scenario was designed to resemble real-world conditions and was

divided into three main phases: pre-incident, incident, and post-incident.

1. Pre-Incident

The pre-incident stage is a preparatory phase that depicts the initial interaction between the perpetrator's and victim's accounts on the X platform. In this stage, two fictitious accounts were created, each playing the role of the perpetrator and the victim, respectively. The scenario for the pre-incident stage is shown in Figure 3.

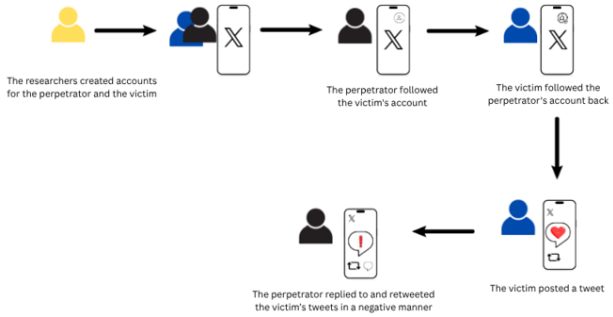


**Figure 3: Pre-Incident Simulation**

Based on Figure 3, the perpetrator's account begins interacting with the victim's account through follow and reply activities. The victim then posts neutral content, which the perpetrator subsequently targets for cyberbullying. This interaction serves as the starting point for the cyberbullying activities carried out in the simulation.

2. Insident

The incident stage depicts the cyberbullying carried out by the perpetrator against the victim via Platform X. These activities generate various digital traces that will later be analyzed during the investigation. The scenario for the incident stage is shown in Figure 4.


**Figure 4: Incident Simulation**

Based on Figure 4, the perpetrator replies to, retweets, and shares negative content containing elements of insults. After experiencing psychological and social impacts, the victim reports the incident, while the perpetrator attempts to delete some of the posts to erase their digital footprint.

3. Post-Insident

The post-incident stage is the phase in which a digital forensic investigation is conducted on the perpetrator's device. This stage begins after the device has been successfully secured as digital evidence. During this stage, digital artifacts are extracted, examined, and analyzed to uncover evidence related to the cyberbullying activity. The scenario for the post-incident stage is shown in Figure 5.


**Figure 5: Post-Incident Simulation**

Based on Figure 5, investigators performed data acquisition and analysis using MOBILedit Forensic Express, Oxygen Forensic Detective, and SQLite DB Browser. The results of the examination which included digital artifacts such as replies, tweets, images, videos, and metadata were then compiled into a forensic report to support the evidentiary process.

## 3.2 Digital Forensic Research Workshop Framework

This study applied the Digital Forensic Research Workshop (DFRWS) framework in the investigation and analysis of digital evidence in a cyberbullying case on Platform X. The application of this framework was adapted to the research scenario and the evidence-handling processes carried out during the investigation. The DFRWS workflow used in this study is shown in Figure 6.

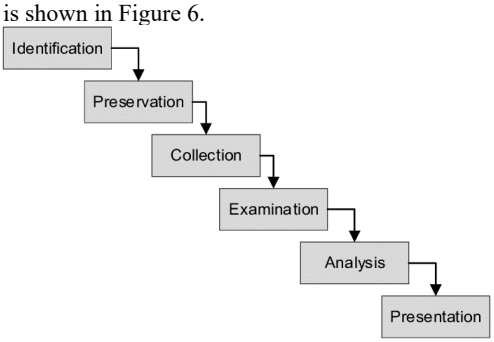


**Figure 6: Digital Forensic Research Workshop Framework**

1. Identification
   The identification stage begins when the victim reports experiencing cyberbullying on Platform X. Based on the report, investigators identify the incident, the perpetrator's smartphone, the X application, and the types of digital evidence that may support the investigation, such as account information, tweets, replies, deleted tweets, search history, and media files.
2. Preservation
   During the preservation stage, the perpetrator's smartphone is secured and isolated to prevent any modification or loss of digital evidence. This process ensures that the integrity and authenticity of the evidence are maintained before the forensic acquisition process begins.
3. Collection
   The collection stage involves extracting digital data from the perpetrator's smartphone using MOBILedit Forensic Express and Oxygen Forensic Detective. The acquisition focuses on obtaining X platform artifacts, including account data, tweets, replies, deleted tweets, search history, GIF media, metadata, and database files for further analysis.
4. Examination
   During the examination stage, the extracted data is examined to identify digital artifacts relevant to the cyberbullying case. Oxygen Forensic Detective is used to analyze the extracted data directly, while DB Browser for SQLite is used to examine the X platform database recovered from MOBILedit and identify deleted records and other stored artifacts.
5. Analysis
   The analysis stage aims to reconstruct the sequence of cyberbullying activities by correlating the recovered digital artifacts. Investigators analyze the interaction between the perpetrator and the victim, identify cyberbullying patterns, and verify that the recovered evidence is consistent with the simulated case scenario.
6. Presentation
   The presentation stage summarizes all investigation findings in a structured forensic report. The report presents

the recovered digital evidence, including account information, tweets, deleted tweets, search history, GIF media, and the comparison results obtained using MOBILedit Forensic Express, Oxygen Forensic Detective, and DB Browser for SQLite to support the investigation findings.

# 4. RESULT AND DISCUSSION

This chapter discusses the digital forensic investigation of a cyberbullying case on Platform X using the DFRWS framework. The study began with a simulated cyberbullying incident on Platform X, followed by data extraction and analysis from the perpetrator's device to obtain digital evidence that could be used in the evidentiary process.

## 4.1 Identification

Identification phase was conducted to identify the cyberbullying incident under investigation and to determine the devices and software used during the study. The software used included the X platform as the subject of the case, MOBILedit Forensic Express, Oxygen Forensic Detective, and SQLite DB Browser, which supported the extraction, examination, and analysis of digital evidence. In addition, the following hardware was used: a laptop as a workstation, a Samsung Galaxy S20+ smartphone as the perpetrator's device, a Samsung Galaxy S21+ smartphone as the victim's device, and a USB cable as the connection medium. As part of the identification process, a physical examination of the perpetrator's device was also conducted, as shown in Figure 7.

**Figure 7: The Perpetrator's Smartphone**

Figure 7. The Perpetrator's Smartphone That Was Successfully Secured Following the physical examination, the specifications of the perpetrator's device were recorded to determine the characteristics of the system to be analyzed. This information included the device's identity, storage capacity, operating system, and the security status of the device, which had rooted using Magisk. The details of the perpetrator's phone specifications are shown in Table 1.

**Tabel 1: Perpetrator's Phone Specification**

| Spesification | Description |
|---|---|
| **Brand** | Samsung Galaxy S20+ (SM-G985F) |
| **IMEI 1** | 353344117536719 |
| **IMEI 2** | 353345117536716 |
| **Memori Internal dan RAM** | 128 GB / 8 GB RAM |
| **Sistem Operasi** | Android 13 |
| **Security Status** | Modified (rooted via Magisk) |

Based on the findings in Table 1, the perpetrator's Samsung Galaxy S20+ was rooted, allowing access to the internal files and databases of the X app. In addition to the perpetrator's device, the victim's device was also examined to verify account identities and match digital artifacts related to cyberbullying activities during the study.

## 4.2 Preservation

The preservation phase was carried out to maintain the integrity and authenticity of the data on the evidence device prior to the acquisition process. After the suspect's Samsung Galaxy S20+ was secured, the device was immediately isolated from the network by enabling Airplane Mode. This step aims to prevent data synchronization, app updates, or remote data deletion that could potentially alter the condition of the evidence. Additionally, the X platform was force-stopped to prevent background activities that could alter the contents of the database and digital artifacts stored on the device. With the device isolated from the network and the app deactivated, data integrity can be maintained.

## 4.3 Collection

Data collection phase was conducted to obtain copies of digital data from the suspect's device using two different extraction methods: MOBILedit Forensic Express and Oxygen Forensic Detective. The use of these two forensic software tools was intended to produce results that could be compared and validated, thereby enhancing the reliability of the digital evidence discovered. The extraction process using MOBILedit Forensic Express is shown in Figure 8.

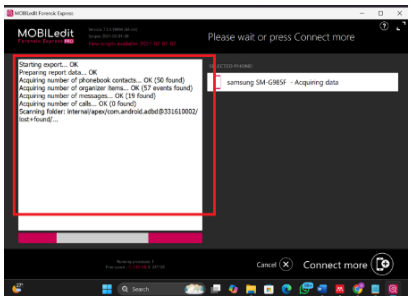


**Figure 8: The Process of Extracting Data from the Suspect's Phone Using the MOBILedit Forensic Express System**

Based on Figure 8, MOBILedit Forensic Express successfully copied data from the X platform directory (com.twitter.android) to the workstation laptop. The extraction results were then saved as a forensic report and raw data files, which were used in subsequent examination and analysis stages.

The second method was performed using Oxygen Forensic Detective software with a Full File System approach to obtain a more comprehensive view of the file structure and application databases. The extraction process using Oxygen Forensic Detective is shown in Figure 9.

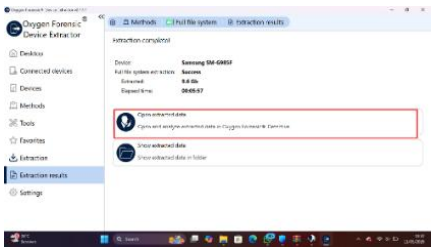

**Figure 9: Successful Extraction Process of the Suspect's Phone Using Oxygen Forensic Detective**

Based on Figure 9, the extraction process was successfully completed, and all acquired data was imported directly into the Oxygen Forensic Detective workspace. This data was subsequently used for examination, analysis of digital artifacts, and the search for evidence of cyberbullying both stored and deleted from the perpetrator's device.

## 4.4 Examination

The examination phase is conducted to review, filter, and validate the extracted data obtained from the perpetrator's device. The examination covers the extraction results from both MOBILedit Forensic Express and Oxygen Forensic Detective to ensure that the discovered digital artifacts are relevant to the cyberbullying case on Platform X. The examination of the MOBILedit Forensic Express extraction results is performed using the automated forensic report generated by the system, followed by a manual examination of the extracted SQLite database files using DB Browser for SQLite. The analysis focuses on several application databases containing user profile information, tweets, replies, deleted tweet records, search history, media references (GIFs), timestamps, and other metadata related to user activities. Meanwhile, Oxygen Forensic Detective is used to examine the same datasets directly through its built-in database analysis feature, allowing the recovered artifacts from both tools to be compared and validated. An example of the extraction report review results is shown in Figure 10.

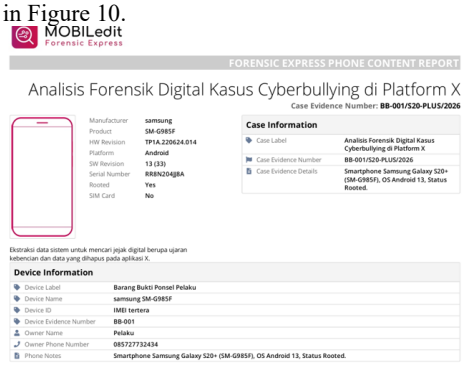


**Figure 10: Results of the MOBILedit Forensic Express Extraction Report Review**

Based on Figure 10, the extraction process was successful, and the data from Platform X has been copied to the investigator's storage medium. Further analysis was conducted using Oxygen Forensic Detective. The extraction results show that the system successfully grouped various digital artifacts from Platform X into several categories, such as accounts, users, tweets, search history, and app cache. The structure of these artifacts is shown in Figure 11.

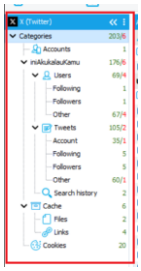

**Figure 11: Structure of Platform X Digital Artifacts in Oxygen Forensic Detective**

Based on Figure 11, the digital artifacts successfully obtained provide an overview of user activity on Platform X. This data serves as the foundation for tracing accounts, interactions, and tweets related to the alleged cyberbullying. To obtain more specific evidence, the examination continued in the "databases" folder stored within the Platform X directory. This folder contains various database files that store records of user activity and serve as the primary source for the forensic analysis process. The structure of the "databases" folder is shown in Figure 12.

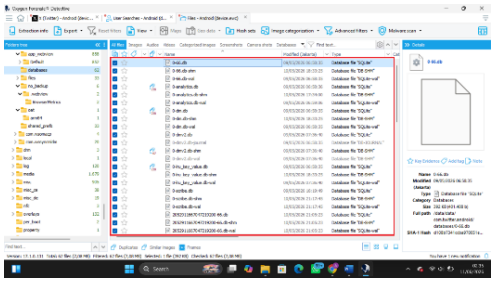

**Figure 12: Contents of Platform X's Databases Folder**

Based on Figure 12, a number of database files with the .db extension, along with other supporting files, were found. These files were then examined further to identify account data, tweets, and other digital artifacts related to cyberbullying activities on Platform X.

## 4.5 Analysist

The analysis phase was conducted to identify and substantiate cyberbullying activities based on the digital artifacts successfully obtained in the previous phase. The analysis was performed using several forensic software tools to obtain evidence that could complement and validate the investigation results. Key findings in this phase included evidence of deleted tweets, tweet content containing elements of bullying, interactions between the perpetrator and the victim, and the recovery of deleted tweets. The analysis began with an examination of the extraction report generated by MOBILedit Forensic Express. This report revealed indications of data deletion activities carried out by the perpetrator on Platform X. Evidence of these deletion activities is shown in Figure 13.

**Figure 13: Tweets Detected as Having Been Deleted**

Based on Figure 13 above, the MOBILedit Forensic Express system successfully detected tweets that had been deleted by the perpetrator. This finding indicates an attempt to erase digital traces; however, artifacts of this activity can still be identified through the forensic process, making them crucial evidence in the investigation.

Further analysis was conducted using DB Browser for SQLite by examining the `statuses` table in the platform X's main database file. This table stores the history of tweets recorded in the application, including those related to cyberbullying activities. The results of the Table statuses. Table examination are shown in Figure 14.

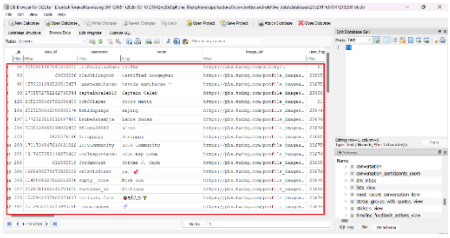

**Figure 14: Tweets Stored in the statuses Table**

Based on Figure 14, a tweet from the perpetrator was found containing the phrase "Lu tu sadar diri ajg udh jelek gendut dekil" which directed at the victim. This finding indicates that

the statuses table successfully stored text artifacts containing elements of insults and digital bullying. An analysis using Oxygen Forensic Detective was then conducted by examining the interaction history between the perpetrator's account and the victim's account on the X platform. This examination aimed to prove the existence of a direct connection between the two accounts. The results of this examination are shown in Figure 15.

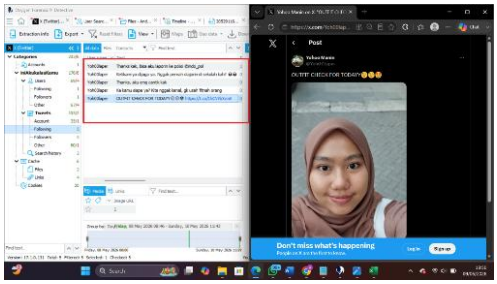

**Figure 15: Screenshot of the Tweet Interaction History Page with the Victim's Account**

Based on Figure 15 above, the system recorded the perpetrator's interaction with the victim's post that read "OUTFIT CHECK FOR TODAYY." This finding indicates that the perpetrator actively monitored and interacted with the victim's content, thereby strengthening the link between the two accounts. The next examination was conducted on the drafts database using the "SQLite with Recovered Data" feature in Oxygen Forensic Detective. This examination aimed to retrieve tweets that had been deleted but were still stored in the database artifacts. The results are shown in Figure 16.

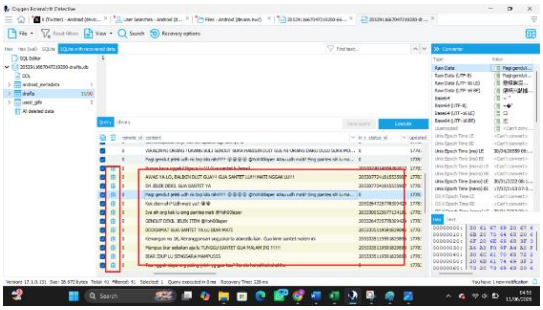

**Figure 16: Findings of Deleted Tweet Draft Content in the drafts Table**

Based on Figure 4.10, the system successfully recovered a tweet deleted by the perpetrator with the text "Yeah, people like you really deserve to die @Yoh00laper." This finding proves that tweet artifacts deleted from the app can still be recovered and used as digital evidence. Thus, the analysis results successfully demonstrated the existence of cyberbullying activity, the connection between the perpetrator and the victim, and the attempt to delete evidence that can still be uncovered through the digital forensic investigation process.

## 4.6 Presentasion

The final stage of the Digital Forensic Research Workshop (DFRWS) method is the presentation stage. At this stage, all digital investigation results obtained from the processes of identification, preservation, collection, examination, and analysis are compiled and presented in the form of a structured report. In this study, the presentation of results focuses on digital evidence related to cyberbullying on Platform X.

The evidence obtained includes the perpetrator's account information, the victim's account information, tweets linked related to cyberbullying activities, deleted tweets, and a comparison of findings from the forensic software used. This data was used to demonstrate the connection between the perpetrator's activities and the digital evidence discovered during the investigation. The presentation of evidence begins with the perpetrator's account information shown in Table 2.

**Table 2: Prepetrator's Acoount Information**

| Account Information | Description |
|---|---|
| Label | iniAku |
| *Nickname* | iniAkukalauKamu |
| Twitter ID | 2052911667047210000 |
| Address/Street | Neraka |
| Account Description | Manusia penuh dosa |
| Number of Followers | 1 account |
| Number of Following | 7 account |
| Number of Tweets | 34 tweets |

Based on Table 2, we successfully obtained profile information on the perpetrators' accounts used to carry out cyberbullying on Platform X. The data collected includes account identities, profile information, the number of followers, the number of accounts followed, and the number of tweets published. This information was used to identify the accounts that were the primary sources of cyberbullying activity in this study. Additionally, this profile information helped link the identified activities to the accounts used by the perpetrators. Information on tweets from the victim's account that were directly related to the perpetrator's account activity on Platform X is presented in Table 3.

**Table 3: Tweet Information from Victims' Accounts That Interacted with Perpetrators' Accounts**

| Tweets | Time | Quotes count |
|---|---|---|
| Thanks kak, bisa aku laporin ke polisi @indo_pol | 10/05/2026 11:43:36 (UTC+7) | 0 |
| Ketikannya dijaga ya. Nggak pernah diajarin di sekolah kah? | 09/05/2026 18:38:53 (UTC+7) | 0 |
| Thanks, aku emg cantik kak | 09/05/2026 18:38:27 (UTC+7) | 0 |
| Ka kamu siapa ya? Kita nggak kenal, gk usah fitnah orang | 09/05/2026 18:37:59 (UTC+7) | 0 |
| OUTFIT CHECK FOR TODAYY😉😉😍 https://t.co/CkCVVbXzmX | 08/05/2026 08:46:48 (UTC+7) | 1 |

Based on Table 3, this section presents the profile information of the perpetrators' accounts that were successfully retrieved; this information was used to carry out cyberbullying on the X platform. The data collected includes account identities, profile information, the number of followers, the number of accounts followed, and the number of tweets published. This information was used to identify the accounts that were the primary sources of cyberbullying activity in this study. In addition to account profile information, the investigation also uncovered several tweets that had been deleted by the perpetrators but were successfully recovered from digital artifacts. The findings regarding these deleted tweets are presented in Table 4.

**Table 4: Findings on Deleted Tweets**

| Deleted Tweets | Status |
|---|---|
| VIRALIN NI ORANG TUKANG BULI GENDUT SUKA HABISIN DUIT GUE... | Deleted |
| Pagi gendut jelek udh nk brp kilo nih???? @Yoh00laper Atau udh mati? Emg pantes sih lu mati cuma sampah bumi | Deleted |
| Iya sih org kek lu emg pantes mati @Yoh00laper | Deleted |

Based on Table 4, three tweets were found that had been deleted by the perpetrator from the X platform. Although they are no longer displayed on the app interface, the content of these tweets can still be recovered through database artifact analysis. This finding indicates that data deletion does not completely erase the digital traces stored on the device. A comparison was conducted of the digital artifact findings obtained using the software MOBILedit Forensic Express, Oxygen Forensic Detective, and DB Browser for SQLite. The results of this comparison are shown in Table 5.

**Table 5: Comparison of Digital Evidence Findings from Forensic Software**

| No. | Digital Evidence | MOBILedit Forensic Express | Oxygen Forensic Detective | DB Browser for SQLite |
|---|---|---|---|---|
| 1. | Account Profile | 2 Profiles | 2 Profiles | 2 Profiles |
| 2. | Active Tweets | 34 Tweets | 34 Tweets | 34 Tweets |
| 3. | Deleted Tweets | 2 Tweets | 3 Tweets | 2 Tweets |
| 4. | Search History | 0 Records | 2 Records | 0 Records |
| 5. | GIF Media Files | 2 Files | 2 Files | 2 Files |
| **Total Digital Artifacts Found** | | **40 Artifacts** | **42 Artifacts** | **40 Artifacts** |

Based on Table 5, all three software tools successfully identified key artifacts, including account profiles, active tweets, and GIFs. However, Oxygen Forensic Detective yielded a greater number of findings because it successfully recovered all deleted tweets as well as the account's search history. These results demonstrate that each software tool possesses distinct capabilities in retrieving digital artifacts from the X platform. Based on all the digital evidence that was successfully recovered, it was determined that the perpetrator's account was proven to have engaged in cyberbullying against the victim's account through various forms of interaction on the X platform. The evidence recovered includes active tweets, deleted tweets, a history of interactions with the victim, and other supporting artifacts successfully retrieved from the app's database. These findings indicate that the digital trail of the perpetrator's activities can still be traced even though some data has been deleted, and thus can be used as digital evidence in the investigation of cyberbullying cases.

# 5. CONCLUSION

Digital forensic investigation process for cyberbullying cases on the X platform can be conducted systematically using the Digital Forensic Research Workshop (DFRWS) framework, which consists of the stages of identification, preservation, collection, examination, analysis, and presentation. The application of these stages successfully uncovered various digital traces left by the perpetrator, including account profile information, active tweets, deleted tweets, search history, and GIFs, which can be used as digital evidence in the process of proving cyberbullying cases. In addition, validation of the investigation results using the software MOBILedit Forensic Express, Oxygen Forensic Detective, and DB Browser for SQLite showed that the digital artifacts obtained were consistent with the designed case scenario, the application of the DFRWS framework proved capable of supporting the process of uncovering and substantiating cyberbullying activities through digital evidence that is relevant, accurate, and admissible as digital evidence. The proposed investigation approach also provides a reference for conducting digital forensic investigations on social media platforms using a structured forensic framework. Future research may extend this work by evaluating the DFRWS framework using more diverse cyberbullying scenarios, different Android devices, additional forensic tools, and other social media platforms to further assess its applicability and effectiveness in broader digital forensic investigations.

# 6. REFERENCES

[1] M. Fikri and A. Junaidi, "Perubahan Pola Konsumsi Dan Gaya Hidup Masyarakat Indonesia Di Era Digital," Jurnal Pendidikan Sosial Indonesia, vol. 2, no. 1, p. 12, 2024, doi: 10.62238/jupsi.v2i1.139.

[2] W. F. Ramadhina Assidiq, M. D. U. Alfarhani, D. Nandhika, and M. F. Amirullah, "Analisis Peran Media Sosial Dalam Membentuk Identitas Nasional Generasi Milenial di Indonesia," Jurnal Sosial Teknologi, vol. 3, no. 9, pp. 772–775, Sep. 2023, doi: 10.59188/jurnalsostech.v3i9.912.

[3] Z. M. Aggriany and W. Kustiawan, "Analisis Penggunaan Media Sosial Twitter Sebagai Media Curhat oleh Kalangan Muslim Generasi Z," Reslaj : Religion Education Social Laa Roiba Journal, vol. 5, no. 6, pp. 3118–3133, Jun. 2023, doi: 10.47467/reslaj.v5i6.3737.

[4] E. Aprilia Hastuti, E. Widianti, and Y. A. Aryani, "Pengaruh Penggunaan Media Sosial Twitter Terhadap Kesehatan Mental Emosional Pada Remaja," Jurnal Keperawatan 'Aisyiyah, vol. 10, no. 1, pp. 1–9, Jun. 2023, doi: 10.33867/jka.v10i1.353.

[5] Syafruddin, A. Thaba, and R. Ananda, "Ujaran Kebencian pada Akun Twitter Es Teh: Tinjauan Linguistik Forensik," Semantik, vol. 13, no. 1, pp. 15–28, Feb. 2024, doi: 10.22460/semantik.v13i1.p15-28.

[6] M. Fitriana, K. A. AR, and J. M. Marsya, "Penerapan Metode National Institute of Standards and Technology (NIST) dalam Analisis Forensik Digital untuk Penanganan Cyber Crime," Cyberspace: Jurnal Pendidikan Teknologi Informasi, vol. 4, no. 1, p. 29, Jul. 2020, doi: 10.22373/cj.v4i1.7241.

[7] K. C. Bego, R. A. Fajar, R. A. Rahmad, Sunarto, and H. Budianto, "Tindak Pidana Cybercrime: Tantangan Hukum Pidana Dalam Menanggulangi Kejahatan di Dunia Maya," Jurnal Kolaboratif Sains, vol. 8, no. 1, pp. 506–511, 2025, doi: 10.56338/jks.v8i1.6740.

[8] D. Yuliana, T. Yuniati, and B. Parga Zen, "Analisis Forensik terhadap Kasus Cyberbullying pada Instagram dan WhatsApp Menggunakan Metode National Institute of Justice (NIJ)," Cyber Security dan Forensik Digital, vol. 5, no. 2, pp. 52–59, Jan. 2023, doi: 10.14421/csecurity.2022.5.2.3734.

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

[10] R. M. G. S. Bintang, D. A. Bahytsani, and A. A. Mudzakkar, "Analisis Bukti Digital Forensik pada Aplikasi Threads Menggunakan Metode Digital Forensic Research Workshop," Jurnal Informatika Komputer, Bisnis dan Manajemen, vol. 22, no. 2, pp. 1–10, May 2024, doi: 10.61805/fahma.v22i2.118.

[11] N. Halimah and F. Fachri, "Analisis Bukti Digital Twitter Web Menggunkan Live Forensic pada Kasus Cyberbullying," JATI (Jurnal Mahasiswa Teknik Informatika), vol. 9, no. 1, pp. 1005–1010, Dec. 2024, doi: 10.36040/jati.v9i1.12554.

[12] H. Yuliansyah, A. Yudhana, and F. Anggraini, "Akuisisi Bukti Digital Tiktok Berbasis Android Menggunakan Metode National Institute of Justice," Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 10, no. 1, pp. 89–96, Mar. 2023, doi: 10.25126/jtiik.2023106416.

[13] R. N. Dasmen, M. R. Pratama, H. Yasir, and A. Budiman, "Analisis Forensik Digital pada Kasus Cyberbullying dengan Metode National Institute of Standard and Technology SP 800-86," JURNAL ILMIAH INFORMATIKA, vol. 12, no. 01, pp. 68–73, Mar. 2024, doi: 10.33884/jif.v12i01.8344.

[14] I. Riadi, Sunardi, and Y. Safitri, "Analisis Forensik Cyberbullying pada Aplikasi IMO Messenger Menggunakan Metode Association of Chief Police Officers," Jurnal Bumigora Information Technology (BITe), vol. 5, no. 1, pp. 1–8, 2023, doi: 10.30812/bite/v5i1.2977.

[15] W. Y. Sulistyo, S. A. Pratiwi, and M. H. Z. Hidayatullah, "Analisis Forensik Citra di Platform X Menggunakan Metode Digital Forensic Research Workshop (DFRWS)," IDEALIS : InDonEsiA journaL Information System, vol. 8, no. 1, pp. 10–20, Jan. 2025, doi: 10.36080/idealis.v8i1.3293.

[16] E. H. Kusuma Dewi, A. Suharso, and C. Rozikin, "Implementasi Cosine Similarity dalam Analisis Investigasi Cyberbullying pada Twitter dengan Framework NIST," Cyber Security dan Forensik Digital, vol. 5, no. 1, pp. 12–22, Nov. 2022, doi: 10.14421/csecurity.2022.5.1.3397.

[17] N. M Zainudin, N. A. Hasbullah, M. Wook, S. Ramli, and N. A. Mat Razali, "Online Social Networks as Supporting Evidence for Digital Forensic Investigation: A Revised Model," in Proceedings of the International Conference on Industrial Engineering and Operations Management, Michigan, USA: IEOM Society International, Mar. 2021. doi: 10.46254/AN11.20210898.

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

[19] G. Z. Muflih, Sunardi, I. Riadi, A. Yudhana, and I. H. Azmi, "Comparison of Forensic Tools on Social Media Services Using the Digital Forensic Research Workshop Method (DFRWS)," JIKO (Jurnal Informatika dan Komputer), vol. 6, no. 1, pp. 52–61, Apr. 2023, doi: 10.33387/jiko.v6i1.5872.

[20] I. Wahyudi, A. Muntasa, M. Yusuf, and A. Hamzah, "Mengungkap Dan Menguji Keaslian Bukti Digital Pada Kejahatan Cybercrime Dengan Metode Digital Forensic Research Workshop," Jurnal Aplikasi Teknologi Informasi dan Manajemen (JATIM), vol. 2, no. 2, pp. 120–127, Dec. 2021, doi: 10.31102/jatim.v2i2.1068.

[22] S. Budi, Fauziah, and Roslinawati, "Analisis Faktor-Faktor yang Mempengaruhi Perilaku Cyberbullying melalui Penggunaan Media Sosial pada Remaja di SMA Negeri 6 Lhokseumawe," Jurnal Ilmiah Keperawatan (Scientific Journal of Nursing), vol. 9, no. 1, pp. 1–11, Feb. 2023, doi: 10.33023/jikep.v9i1.1345.

[23] E. L. Amanatin and B. Sekarningrum, "Causes and Forms of Cyberbullying among Teenagers in Indonesian Urban Areas: Cases of Jakarta, Bandung and Surabaya," JISPO Jurnal Ilmu Sosial dan Ilmu Politik, vol. 13, no. 2, pp. 233–254, Mar. 2024, doi: 10.15575/jispo.v13i2.27792.

[24] S. Alkatiri, S. Rukmini Devy, and N. I. Ubaidillah, "The Influence of Parental Interactions and Cyberbullying on the Psychological Impact of High School Adolescents in Sumbersari District, Jember," Jurnal Berkala Epidemiologi, vol. 12, no. 1, pp. 26–33, Jan. 2024, doi: 10.20473/jbe.V12I12024.26-33.

[25] C. K. Yemima, "Dampak cyberbullying pada Tingkat Emosional Remaja," Realita : Jurnal Bimbingan dan Konseling, vol. 8, no. 2, p. 2115, Oct. 2023, doi: 10.33394/realita.v8i2.8654.

[26] T. K. Boleng, V. Farera Pardede, and R. A. Fahlevie, "Jurnal Hukum Perlindungan Saksi dan Korban 'Menghadapi Tantangan Cyberbullying: Dampak dan Solusi,'" Jurnal Pendidikan Tambusui, vol. 8 Nomor 1, pp. 10250–10262, Feb. 2024, doi: 10.31004/jptam.v8i1.13932.

[27] F. P. Hidayat, S. Hardiyanto, F. H. Lubis, A. Adhani, and Zulfahmi, "Kemampuan Literasi Media Sebagai Upaya Mengantisipasi Cybercrime Pada Remaja Di Kota Medan," Jurnal Interaksi: Jurnal Ilmu Komunikasi, vol. 7. No 1, pp. 13–5, Jan. 2023, doi: 10.30596/ji.v7i1.12904.

[28] S. Subektiningsih and D. Hariyadi, "The Role of Digital Forensic Experts in Cybercrime Investigations in Indonesia Based on The Scopus Research Index," Building of Informatics, Technology and Science (BITS), vol. 4, no. 3, Dec. 2022, doi: 10.47065/bits.v4i3.2638.

[29] N. Aisyah et al., "Analisa Perkembangan Digital Forensik Dalam Penyidikan Cybercrime Di Indonesia Secara Systematic Review," Jurnal Esensi Infokom : Jurnal Esensi Sistem Informasi dan Sistem Komputer, vol. 6, no. 1, pp. 22–27, May 2022, doi: 10.55886/infokom.v6i1.452.

[30] W. N. D. K. Aji and N. K. Wardhani, "Pengaruh kompetensi auditor, penggunaan analitik big data, dan penggunaan forensik digital terhadap kualitas audit investigatif," AKURASI: Jurnal Riset Akuntansi dan Keuangan, vol. 6, no. 2, pp. 163–180, Jul. 2024, doi: 10.36407/akurasi.v6i2.1232.

[31] T. Rochmadi, A. Fadlil, and I. Riadi, "Tinjauan Pustaka Sistematis: Tantangan Dan Faktor-Faktor Pengembangan Kesiapan Forensik Digital," Cyber Security dan Forensik Digital, vol. 7, no. 2, pp. 81–89, Dec. 2024, doi:

10.14421/csecurity.2024.7.2.4861.

[32] M. N. Fadillah, R. Umar, and A. Yudhana, "Analisis forensik aplikasi dompet digital pada smartphone Android menggunakan metode DFRWS," Kumpulan Jurnal Ilmu Komputer (KLIK), vol. 9 No.2, pp. 265–278, Jul. 2022, doi: 10.20527/klik.v9i2.327.

[33] G. Fanani, I. Riadi, and A. Yudhana, "Analisis Forensik Aplikasi Michat Menggunakan Metode Digital Forensics Research Workshop," Jurnal Media Informatika Budidharma, vol. 6, no. 2, p. 1263, Apr. 2022, doi: 10.30865/mib.v6i2.3946.