Mobile Forensic Analysis of Child Pornography Cases on Twitter using Digital Forensic Research Workshop Method

Dini Rohmah
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

Twitter is a platform that plays an important role in the dissemination of information and digital interaction in Indonesia. Its ability to reach a large user base makes Twitter one of the most frequently misused applications in digital crimes, particularly in cases involving the distribution of child pornography content. In 2023, there were 156 recorded cases of child pornography content on Twitter. This research aims to obtain mobile forensic evidence related to the distribution of child pornography through the Twitter application using the Digital Forensic Research Workshop (DFRWS) methodology. This method consists of six stages: identification, preservation, collection, examination, analysis, and presentation. The data used in this investigation was taken from the perpetrator's rooted device, from which data extraction was performed using Magnet Axiom. The examination of evidence was then carried out with three forensic tools: Magnet Axiom, Autopsy, and Oxygen Forensic Detective. The digital evidence obtained through these tools includes direct messages sent by the victim, five deleted posts, the perpetrator's activity history, and image-based posting evidence. The investigation results showed that Magnet Axiom had the highest accuracy rate at 68%, successfully recovering deleted direct messages from the perpetrator, five captions posted by the perpetrator, as well as images and links that were shared. Oxygen Forensic recorded an accuracy rate of 50%, successfully recovering messages and metadata from two deleted posts. Meanwhile, Autopsy achieved an accuracy rate of 43.75%, successfully retrieving account information and deleted captions. The findings of this research indicate that the DFRWS method can be effectively applied in digital forensic investigations involving social media platforms.

Keywords

Child Pornography; DFRWS; Forensic; Mobile Forensic; Twitter;

1. INTRODUCTION

The development of information technology has had a significant impact on social life, particularly through the emergence of social media as a means of digital communication. However, behind these conveniences lie several negative consequences, one of which is the increasing number of child pornography cases on various platforms. Twitter is one such social media platform with a wide user reach. Indonesia ranks fifth in the world with a total of 24 million users, according to the Twitter Ad Reach Ranking report as of January 2023 [1].

Child pornography on social media is a non-physical sexual crime involving minors depicted in distributed content [2]. In 2020, child pornography was recorded as the highest category of child-related crimes in Indonesia, with 348 reported cases as of August 31, 2020 [3]. According to Sariaty Dinar, a junior legal drafter at the Ministry of Communication and Information Technology (Kemenkominfo), from 2016 to 2024, there have been 19,228 reported cases of child pornography across various platforms, including 156 cases involving Twitter [4].Several factors contribute to Twitter's vulnerability to misuse. First is the ease with which users can disseminate information through features like retweets and likes. Second, Twitter's new policy permitting the circulation of sexual content increases the likelihood of abuse, especially as child pornography is often disguised using coded keywords to bypass automated detection systems [5].

In an international case involving minors, the perpetrator lured victims through online gaming communities by building trust via shared gameplay and digital gifts like skins. This manipulation led victims to produce pornographic content. A similar 2025 case involved a perpetrator who downloaded content from Telegram and other social media, edited it into child pornography, and distributed it across eight Telegram channels, promoting it on Twitter [6][7]. In 2020, the Ministry of Communication and Information Technology reported handling 1.3 million negative content cases, including 1,062,558 pornographic content cases. By 2024, child pornography content had reached 5,566,015 reported cases, placing Indonesia second in the ASEAN region [8][9].

Given the rise of child pornography distribution on social media particularly on Twitter, which is open-access and now permits adult content there is a critical need for digital forensic investigations to obtain valid digital evidence in reported cases. This research applies the Digital Forensic Research Workshop (DFRWS) methodology, which includes the stages of identification, preservation, collection, examination, analysis, and presentation. To support the investigation process, three digital forensic tools Magnet Axiom, Autopsy, and Oxygen Forensic Detective were used to extract and analyze digital artifacts from the perpetrator's device. The integration of these tools ensures comprehensive evidence acquisition and enhances the reliability of the forensic findings.

This research aims to implement the DFRWS method in digital forensic analysis and validate digital evidence related to Twitter in child pornography cases. Through case simulations and the application of forensic tools, this research seeks to identify digital traces of perpetrators and extract critical artifacts such as file metadata, communication history, and the application's directory structure. The resulting evidence is expected to serve as a reference in legal proceedings and contribute to the development of prevention strategies for child-related digital sexual crimes in Indonesia.

2. LITERATURE STUDY

2.1 Digital Forensics

Digital forensics is a branch of forensic science that focuses on the recovery and investigation of content and criminal activity found within digital devices [10]. The foundation of digital forensics lies in the analysis, collection practices, and reporting of digital data. Digital forensics shows its own set of challenges and advantages one of which is the ease of duplicating digital data, which facilitates the investigative process [11]. Several steps are involved in conducting digital forensic investigations, including:

1. Preparation: Preparing all necessary tools and software required for the evidence collection process.
2. Data Collection: Gathering data from various sources to be used as digital evidence.
3. Investigation Modeling: Creating investigative models to understand the patterns and behaviors of the discovered data.
4. Analysis: Analyzing the collected data to determine whether any criminal activity has occurred.
5. Documentation and Reporting: Compiling documentation and reports related to the findings of the analysis [12].

2.2 X (Twitter)

Twitter is an internet-based social media service that allows users to send and read messages containing no more than 280 characters [13]. Users can post tweets in the form of text, photos, or videos. Through these tweet posts, users are able to engage and interact more closely with the individuals who share them [14]. Twitter is widely known for its speed in disseminating information and its broad user reach, enabling real-time global communication. This is largely due to the fact that most users share content in text form, which accelerates the distribution of data across the platform [15].

2.3 Digital Evidence

Digital evidence refers to any document or information used as proof, which is stored and preserved to support an ongoing investigation [16]. In the context of social media, digital evidence is utilized to help uncover crimes committed on these platforms. Due to its volatile nature, digital evidence is highly susceptible to alteration, and therefore must be handled promptly to ensure its authenticity and integrity [17].

2.4 Cybercrime Child Pornography

Child pornography is one of the serious issues arising from the advancement of information technology. The distribution of pornographic content is frequently carried out via the internet. The internet enables the unlimited and effortless duplication of images, which significantly facilitates the spread of this crime [18][19].

2.5 Digital Forensic Tools

In the digital forensic process, various software tools are used to support the investigation and analysis of digital evidence.

2.5.1 Magnet Axiom

Magnet Axiom is a digital forensic software used to examine data from computers and mobile devices. The application automatically analyzes and shows digital artifacts from various sources, such as hard drive, image files, cloud services, and operating systems like Android and iOS [20].

2.5.2 Autopsy

Autopsy is an open-source digital forensic software tool [21] used to analyze the authenticity and integrity of evidence found during criminal investigations and to generate reports for use in legal proceedings [22]. It is utilized by digital forensic investigators as a tool for collecting data from digital devices such as computers and other storage media. One of Autopsy's key features is its keyword search module, which enables investigators to efficiently identify relevant evidence within large volumes of data [23].

2.5.3 Oxygen Forensic Detective

Oxygen Forensic is a software application used in digital investigations to extract, analyze, and visualize data from various devices, particularly mobile devices such as smartphones. This tool is capable of accessing data from sources such as social media applications, communications, location data, documents, and even deleted files [24].

2.6 Digital Forensics Research Workshop (DFRWS)

The Digital Forensics Research Workshop (DFRWS) is a digital forensic methodology consisting of six stages: identification of investigative needs and potential evidence, preservation of data integrity, collection of evidence and data sources, examination of data while maintaining its original state, analysis to trace data origins and user activity, and presentation of findings in a clear and structured format [25].

3. RESEARCH METHOD

This research employs the Digital Forensic Research Workshop (DFRWS) methodology, which consists of six stages: identification, preservation, collection, examination, analysis, and presentation.

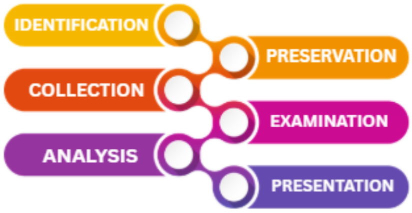


Figure 1 : Research Stages

As shown in Figure 1, the digital forensic process flow based on the DFRWS framework. The process begins with identifying devices and data related to the distribution of child pornography content, followed by preserving the integrity of the evidence, which includes calculating the hash values of copied files. Data collection is carried out using Magnet Axiom to extract information from the suspect's device, including application directories, system files, and Twitter databases. In the examination stage, data is filtered to ensure that only relevant information will be analyzed. The analysis stage uncovers the suspect's activities and traces of illegal content distribution, and all findings are then compiled and presented in the final stage. Finally, the presentation stage delivers a report of all the evidence that has been identified..

4. RESULT AND DISCUSSION

This research focuses on a cybercrime case involving the distribution of child pornography content in the form of photos and videos through the mobile-based twitter application. The case scenario is divided into three phases: pre-incident,

incident, post-insident. The investigation process in this case applies the digital forensic research workshop (DFRWS) methodology.

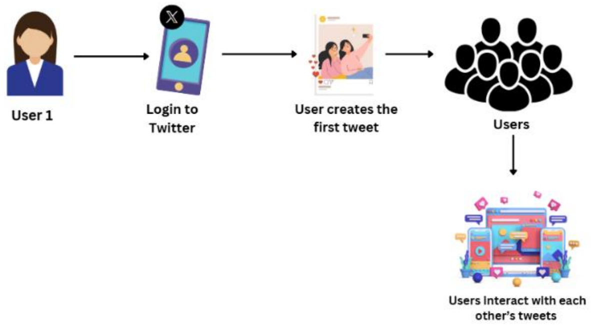

User 1
Login to Twitter
User creates the first tweet
Users
Users interact with each other's tweets

Figure 2 : Pre Incident Child Pornography Cases

As shown in Figure 2, the initial scenario in which user 1 (the victim) posts a tweet containing a photo with their younger sibling. The photo is then circulated and receives engagement in the form of comments and likes. Among the users who viewed and interacted with the post, the perpetrator was one of them expressing interest by liking and commenting on the post with compliments directed at the victim.

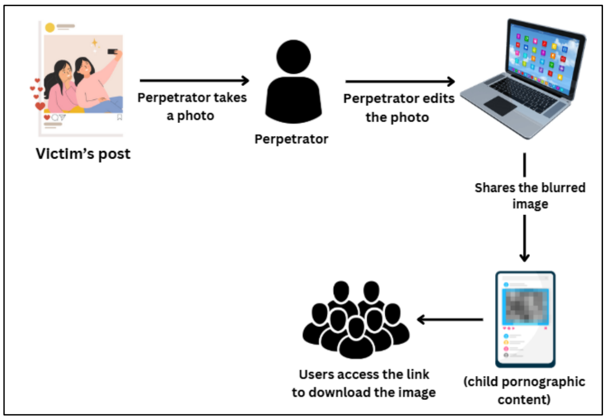

Victim's post
Perpetrator takes a photo
Perpetrator
Perpetrator edits the photo
Shares the blurred image
(child pornographic content)
Users access the link to download the image

Figure 3 : Incident Child Pornography Cases

As shown in Figure 3, shows the incident involving the distribution of child pornography content on Twitter. The perpetrator downloaded the victim's original post and edited it into a thumbnail for child pornographic content to be redistributed on the platform. The perpetrator used tweets with disguised keywords and included a Telegram link in the comment section to avoid detection by Twitter's security systems. The post eventually spread widely and even appeared on the victim's timeline. Upon seeing the post, the victim threatened the perpetrator by sending direct messages and posting threatening comments. In response, the perpetrator deleted the post and blocked the victim's account in an attempt to erase digital traces and prevent the victim from further accessing the perpetrator's profile.

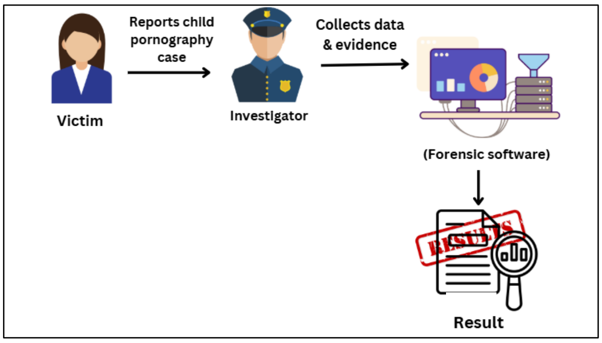


Figure 4 : Post Incident Child Pornography Cases

As shown in Figure 4, the victim reported the distribution of child pornographic content to the authorities, providing evidence in the form of screenshots of the shared posts and images. In response, the police initiated a follow-up investigation to identify and locate the perpetrator. After a series of investigative steps, the suspect was successfully located and apprehended by law enforcement. During the search, authorities found a mobile phone belonging to the suspect, which was strongly suspected to have been used to store, edit, and distribute child pornographic material. The device was then confiscated and handed over to the digital forensics team for in-depth analysis to support the verification of the digital evidence.

4.1 IDENTIFICATION

The identification stage is the initial step in the DFRWS method, aimed at recognizing relevant sources of digital evidence and ensuring the data originates from legitimate devices. This process involves labeling and documenting the device's technical specifications.

Figure 5 : Smartphone Digital Evidence

As shown in Figure 5, the documentation of the smartphone used by the perpetrator as a medium for distributing child pornography content. This documentation serves to support the recording of information related to the evidence device, such as the device brand, model, IMEI number, and other relevant details. The information is organized in a tabular format for further analysis.

Table 1 : Smartphone Evidence Specifications

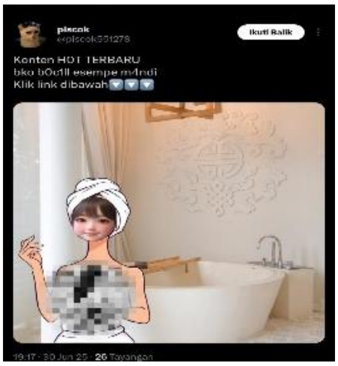
No	Type	Description
1	Brand	Xiomi
2	Series	Redmi 5A
3	IMEI	867796036710544
4	Operating System	Android
5	Operating System Version	11

As shown in Table 1, the specifications of the prepetrator's device, which will undergo an investigative to search digital evidence. Furthermore, to support the identification and extraction of digital data, investigators utilized a set of forensic software tools, as shown in Table 2.

Table 2 : Tools Used

Software	Function
Magnet Axiom	As a tool for extracting data from digital devices.
Autopsy	Tracing digital evidence from the disk image and creating an activity timeline
Oxygen Forensic	accessing hidden data, location, activity logs, and detailed application history.
Root Checker Basic	Verifying the root status on the Android device and ensuring that root access has been successfully granted.
SuperSu Pro	Managing root access permissions on Android devices and providing full control to applications that require superuser privileges.
Oxygen Forensic	accessing hidden data, location, activity logs, and detailed application history.

These software tools serve as supporting instruments in the digital forensic investigation process, each selected based on its specific functionality and relevance to the case. Their roles include extracting, analyzing, and presenting digital artifacts from the perpetrator's device to uncover potential evidence related to the distribution of child pornography.



Konten HOT TERBARU
bko bOc1ll esempe m4ndi
Klik link dibawah🔽🔽🔽

19:17 · 30 Jun 25 · 26 Tayangan

Figure 6 : Secreenshot Digital Evidence

As shown in Figure 6, the evidence submitted by the victim in the case of child pornography content distribution. The reported evidence consists of a screenshot of the perpetrator's post, which featured the victim's younger sibling in a pornographic context.

4.2 PRESERVATION

The preservation stage is carried out to protect the integrity and authenticity of digital evidence, preventing damage or tampering during the investigation process. Isolation is done by enabling airplane mode to avoid automatic synchronization or remote access by unauthorized parties, as shown in Figure 7.

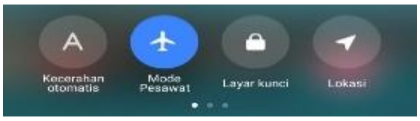
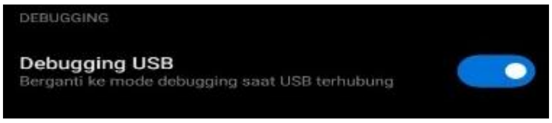


Figure 7 : Airplane Mode Activation

The next step is to enable Developer Options on the Android device. This feature must be activated to allow advanced settings access, including enabling USB Debugging, which allows the device to connect to the forensic computer via ADB (Android Debug Bridge).

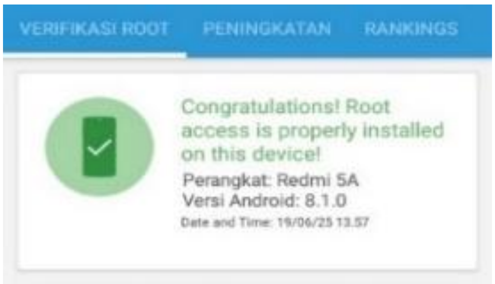


DEBUGGING

Debugging USB
Berganti ke mode debugging saat USB terhubung

Figure 8 : Debuging USB

As shown in Figure 8, the process of enabling Developer Options by tapping the device's build number seven times in the settings menu. Once activated, investigators can enable USB Debugging to perform imaging and further analysis. Enabling USB Debugging allows limited control of the device via a USB connection without unlocking the screen or accessing the main account. This step is carried out with the device in isolation to prevent any potential data changes during the acquisition process.



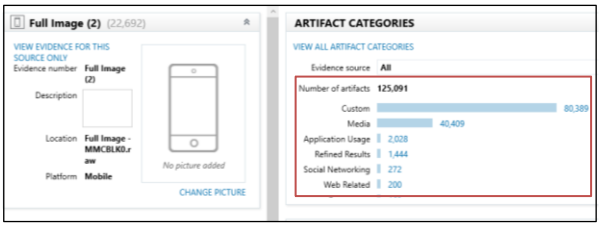
Congratulations! Root access is properly installed on this device!
Perangkat: Redmi 5A
Versi Android: 8.1.0
Date and Time: 19/06/25 13.57

Figure 9 : Root Checker Display for Rooting Process

As shown in Figure 9, the Root Checker Basic application installed on the perpetrator's device to verify that the device has been successfully rooted. Rooting was performed to support deep data extraction and allow access to all directories on the device.

4.3 Collection

This stage is carried out as part of the data collection process from the perpetrator's device without altering or damaging the integrity of the original data. Data extraction was conducted using Magnet Axiom software, with a primary focus on the Twitter application directory located in the system folder /data/data/com.twitter.android and the external storage directory /sdcard/Android/data/com.twitter.android. These directories contain various types of artifact data, which are classified into several folders to facilitate the examination and analysis process. Figure 10 shows the extracted data as shown in Magnet Axiom.


VIEW EVIDENCE FOR THIS SOURCE ONLY
No picture added
CHANGE PICTURE
VIEW ALL ARTIFACT CATEGORIES

Full Image (2) (22,692)

Evidence number: Full Image (2)
Description:
Location: Full Image - MMCBLK0.raw
Platform: Mobile

ARTIFACT CATEGORIES

Evidence source: All

Number of artifacts	125,091
Custom	80,389
Media	40,409
Application Usage	2,028
Refined Results	1,444
Social Networking	272
Web Related	200

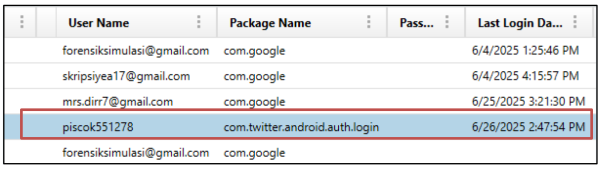
Figure 10 : Suspect Device Extraction Result

4.4 Examination

In this stage, the data obtained from the imaging or initial extraction process is examined to identify critical information such as images, documents, messages, and other artifacts that may indicate the occurrence of a criminal act.

4.4.1 Examination with Magnet Axiom

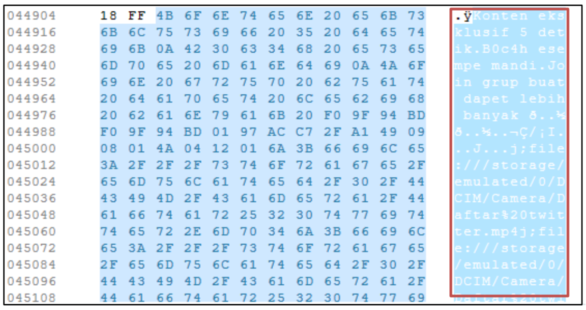
This examination focuses on identifying the account used in the twitter application and other activities related to the suspected distribution of illegal content through the platform. The process is carried out using the Magnet Axiom software, which is used not only to analyze the data but also to extract digital information from the prepetrator's device.



User Name	Package Name	Pass...	Last Login Da...
forensiksimulasi@gmail.com	com.google		6/4/2025 1:25:46 PM
skripsiyea17@gmail.com	com.google		6/4/2025 4:15:57 PM
mrs.dirr7@gmail.com	com.google		6/25/2025 3:21:30 PM
piscok551278	com.twitter.android.auth.login		6/26/2025 2:47:54 PM
forensiksimulasi@gmail.com	com.google		

Figure 11 : Prepetrator's Username

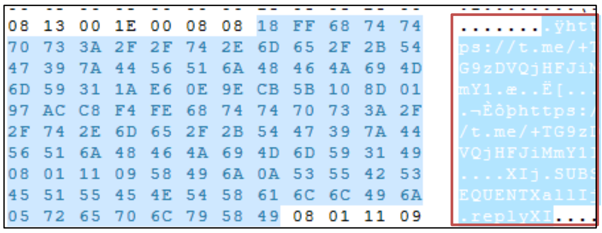
As shown in Figure 11, the email and username information used by the perpetrator to log in to the X application. The data indicates that the perpetrator's last login occurred on June 26, 2025.



```
044904    18 FF 4B 6F 6E 74 65 6E 20 65 6B 73    .ÿKonten eks
044916    6B 6C 75 73 69 66 20 35 20 64 65 74    klusif 5 det
044928    69 6B 0A 42 30 63 34 68 20 65 73 65    ik.B0c4h ese
044940    6D 70 65 20 6D 61 6E 64 69 0A 4A 6F    mpe mandi.Jo
044952    69 6E 20 67 72 75 70 20 62 75 61 74    in grup buat
044964    20 64 61 70 65 74 20 6C 65 62 69 68     dapet lebih
044976    20 62 61 6E 79 61 6B 20 F0 9F 94 BD     banyak ð..½
044988    F0 9F 94 BD 01 97 AC C7 2F A1 49 09    ð..½..¬Ç/¡I.
045000    08 01 4A 04 12 01 6A 3B 66 69 6C 65    ..J...j;file
045012    3A 2F 2F 2F 73 74 6F 72 61 67 65 2F    :///storage/
045024    65 6D 75 6C 61 74 65 64 2F 30 2F 44    emulated/0/D
045036    43 49 4D 2F 43 61 6D 65 72 61 2F 44    CIM/Camera/D
045048    61 66 74 61 72 25 32 30 74 77 69 74    aftar%20twit
045060    74 65 72 2E 6D 70 34 6A 3B 66 69 6C    ter.mp4j;fil
045072    65 3A 2F 2F 2F 73 74 6F 72 61 67 65    e:///storage
045084    2F 65 6D 75 6C 61 74 65 64 2F 30 2F    /emulated/0/
045096    44 43 49 4D 2F 43 61 6D 65 72 61 2F    DCIM/Camera/
045108    44 61 66 74 61 72 25 32 30 74 77 69
```

Figure 12 : Caption of the Perpetrator's Deleted Post

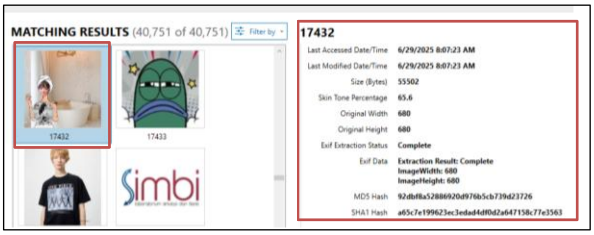
As shown in Figure 12, a post that was deleted by the perpetrator, it also includes information indicating that a video file named *twitter.mp4* was uploaded in that post, originating from the DCIM/Camera directory on the perpetrator's device.



```
08 13 00 1E 00 08 08 18 FF 68 74 74    ........ÿhtt
70 73 3A 2F 2F 74 2E 6D 65 2F 2B 54    ps://t.me/+T
47 39 7A 44 56 51 6A 48 46 4A 69 4D    G9zDVQjHFJiM
6D 59 31 1A E6 0E 9E CB 5B 10 8D 01    mY1.æ..Ë[...
97 AC C8 F4 FE 68 74 74 70 73 3A 2F    .¬Èôþhttps:/
2F 74 2E 6D 65 2F 2B 54 47 39 7A 44    /t.me/+TG9zD
56 51 6A 48 46 4A 69 4D 6D 59 31 49    VQjHFJiMmY1I
08 01 11 09 58 49 6A 0A 53 55 42 53    ....XIj.SUBS
45 51 55 45 4E 54 58 61 6C 6C 49 6A    EQUENTXallIj
05 72 65 70 6C 79 58 49 08 01 11 09    .replyXI....
```

Figure 13 : The Link Included in The Post

As shown in Figure 13, a link found in one of the posts deleted by the perpeptrator as a platform where users coulde additional child pornography content. This is one of five posts found in a file named 1936743361823879169-drafts.db-wal, which was successfully recovered during the forensic examination of the suspect's device. The presence of this file indicate that the suspect had composed several unpublished post instended for the twitter platform, suggesting premeditated actions. This finding further emphasizes the relevance of database-level artifacts in reconstructing user behavior and identifying criminal intent.



17432

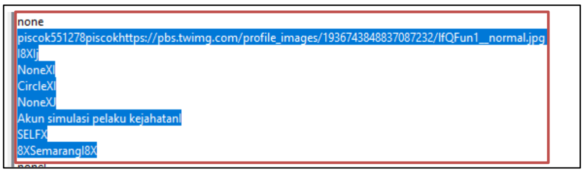
Last Accessed Date/Time	6/29/2025 8:07:23 AM
Last Modified Date/Time	6/29/2025 8:07:23 AM
Size (Bytes)	55502
Skin Tone Percentage	65.6
Original Width	680
Original Height	680
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 680 ImageHeight: 680
MD5 Hash	92dbf8a52886920d976b5cb739d23726
SHA1 Hash	a65c7e199623ec3edad4df0d2a647158c77e3563

Figure 14 : Deleted Post Photo

As shown in Figure 14, the results of image artifact identification found in the media folder. One of detected files is an image with ID 17432, uploade on June 29, 2025. The image is identical to the screenshot previously submitted by the victim.

4.4.2 Examination with Autopsy

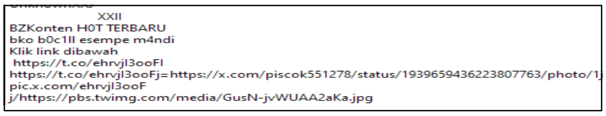
In this research, Autopsy was used to analyze data extracted from the Twitter application directory on the perpetrator's device. The analysis covered the entire contents of the Twitter cache and database files.



```
none
piscok551278piscokhttps://pbs.twimg.com/profile_images/1936743848837087232/lfQFun1__normal.jpg
I8XIj
NoneXI
CircleXI
NoneXJ
Akun simulasi pelaku kejahatanl
SELFX
8XSemarangI8X
```

Figure 15 : Account Information of The Perpetrator

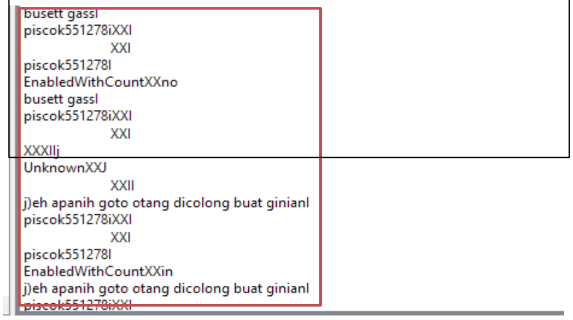
As shown in Figure 15, information indicating that the perpetrator created a Twitter account under the username piscok551278 and is located in Semarang.



```
                    XXII
BZKonten H0T TERBARU
bko b0c1ll esempe m4ndi
Klik link dibawah
 https://t.co/ehrvjl3ooFI
https://t.co/ehrvjl3ooFj=https://x.com/piscok551278/status/1939659436223807763/photo/1j
pic.x.com/ehrvjl3ooF
j/https://pbs.twimg.com/media/GusN-jvWUAA2aKa.jpg
```

Figure 16 : The Posted Status.

As shown in Figure 16, the analysis result of the file 1936476812330196-66-wal.db, where a post (tweet) was found with the caption "H0T TERBARU bko b0c1ll esempe m4ndi klik link dibawah ini" the perpetrator also posted a Telegram link intended to lead users to a paid Telegram group offering additional child pornographic content. This post had previously been published by the perpetrator and was later deleted from the Twitter platform.



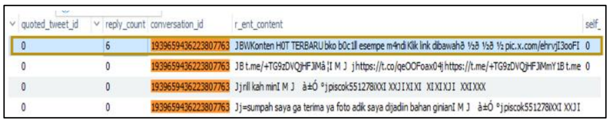
```
busett gassl
piscok551278iXXI
                    XXI
piscok551278I
EnabledWithCountXXno
busett gassl
piscok551278iXXI
                    XXI
XXXIIj
UnknownXXJ
                    XXII
j)eh apanih goto otang dicolong buat ginianl
piscok551278iXXI
                    XXI
piscok551278I
EnabledWithCountXXin
j)eh apanih goto otang dicolong buat ginianl
piscok551278iXXI
```

Figure 17 : Comment on The Perpetrator's Post

As shown in Figure 17, the comments from several users found on the perpetrator's post. The display clearly indicates that the comments appear on a post belonging to the username piscok551278; however, it does not provide information about the users who made the comments or the specific post being commented on.

4.4.3 Examination with Oxygen Forensic Detective

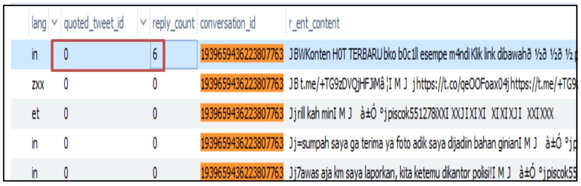
The examination was conducted using Oxygen Forensic Detective software on the Twitter application cache files obtained from the perpetrator's device.



quoted_tweet_id	reply_count	conversation_id	r_ent_content	self_
0	6	1939659436223807763	JBWKonten H0T TERBARU bko b0c1ll esempe m4ndi Klik link dibawahð ½ð ½ð ½ pic.x.com/ehrvjI3ooFI	0
0	0	1939659436223807763	JB t.me/+TG9zDVQjHFJiMâ ¦I M J jhttps://t.co/qeOOFoax04j https://t.me/+TG9zDVQjHFJiMmY1B t.me	0
0	0	1939659436223807763	Jjrill kah minI M J à±Ó °jpiscok551278iXXI XXJIXIXI XIXIXJI XXIXXX	
0	0	1939659436223807763	Jj=sumpah saya ga terima ya foto adik saya dijadiin bahan ginianI M J à±Ó °jpiscok551278iXXI XXJI	

Figure 18 : Deleted Status List

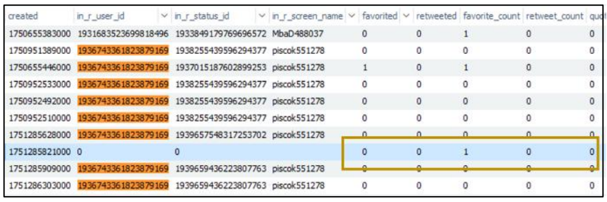
As shown in Figure 18, the posts were deleted from the perpetrator's device.



lang	quoted_tweet_id	reply_count	conversation_id	r_ent_content
in	0	6	1939659436223807763	JBWKonten H0T TERBARU bko b0c1ll esempe m4ndi Klik link dibawahð ½ð ½ð ½
zxx	0	0	1939659436223807763	JB t.me/+TG9zDVQjHFJiMâ ¦I M J jhttps://t.co/qeOOFoax04j https://t.me/+TG9
et	0	0	1939659436223807763	Jjrill kah minI M J à±Ó °jpiscok551278iXXI XXJIXIXI XIXIXJI XXIXXX
in	0	0	1939659436223807763	Jj=sumpah saya ga terima ya foto adik saya dijadiin bahan ginianI M J à±Ó °jp
in	0	0	1939659436223807763	Jj7awas aja km saya laporkan, kita ketemu dikantor polisi!I M J à±Ó °jpiscok55

Figure 19 : Number of Replies To Each Post

As shown in Figure 19, the account with user_id 1936743361823879169 and the username piscok551278 (the perpetrator) had posted a status with status_id 1939659436223807763. The post received a total of 6 replies from other users.



created	in_r_user_id	in_r_status_id	in_r_screen_name	favorited	retweeted	favorite_count	retweet_count	quo
1750655383000	1931683523699818496	1933849179769696572	MbaD488037	0	0	1	0	0
1750951389000	1936743361823879169	1938255439596294377	piscok551278	0	0	0	0	0
1750655446000	1936743361823879169	1937015187602899253	piscok551278	1	0	1	0	0
1750952533000	1936743361823879169	1938255439596294377	piscok551278	0	0	0	0	0
1750952492000	1936743361823879169	1938255439596294377	piscok551278	0	0	0	0	0
1750952510000	1936743361823879169	1938255439596294377	piscok551278	0	0	0	0	0
1751285628000	1936743361823879169	1939657548317253702	piscok551278	0	0	0	0	0
1751285821000	0	0		0	0	1	0	0
1751285909000	1936743361823879169	1939659436223807763	piscok551278	0	0	0	0	0
1751286303000	1936743361823879169	1939659436223807763	piscok551278	0	0	0	0	0

Figure 20 : Post Metadata

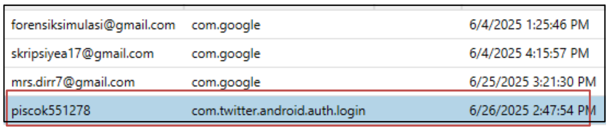
As shown in Figure 20, the metadata of each post that has been uploaded. The image shows that the statuses uploaded by the perpetrator with user_id 1936743361823879169 mostly have a value of zero (0) in the favorite_count, retweet_count, and reply_count columns. However, there is one entry that has a favorite_count value of 1.

4.5 ANALYSIS

This stage aims to understand the origin of the data and identify the source or owner of the discover information. The analysis involves investigative techniques to link the discovered data to the crime under investigation by examining message content, images, videos, and metadata from twitter.

4.5.1 Analysis with Magnet Axiom

Based on the analysis using Magnet Axiom, several important digital artifacts were discovered related to the perpetrator's activities on the X application. These artifacts provide a clear picture of the interaction patterns and digital traces left by the perpetrator. The findings serve as strong evidence to connect the perpetrator's online activities with the relevant digital evidence in the case under investigation.



forensiksimulasi@gmail.com	com.google	6/4/2025 1:25:46 PM
skripsiyea17@gmail.com	com.google	6/4/2025 4:15:57 PM
mrs.dirr7@gmail.com	com.google	6/25/2025 3:21:30 PM
piscok551278	com.twitter.android.auth.login	6/26/2025 2:47:54 PM

Figure 21 : Twitter Account Login Information

As shown in Figure 21, the login information of the X account used by the perpetrator. The extraction results revealed that the account with the username "pisock551278" was connected to the X application, with the last recorded login time on June 26, 2025, at 14:47:54 WIB.

Table 3 : Deleted Draft Posts

Information	Posts
Status	Konten eksklusif 5 detik B0c4h esempe mandi Join grup buat dapet lebih banyak
Status	Bok3p virall "b0cah esde open b0"
Status	Viralll video b0kep 3 menit b0cah esempe Join link
Status	Video h0t b0c11 esempe Fullnya akses link dibawah
Status	Konten H0T TERBARU bko b0c1ll esempe m4ndi Klik link dibawah
Direct Massage	dasar kurangajar
Direct Massage	sumpah saya akan langsung bawa ke jalur hukum

As shown in Table 3, the artifacts found in the draft-wal file. From the table, it can be observed that there are several posts containing explicit content with strong indications of child pornography. For example, a post with the caption "Konten eksklusif 5 detik bocah esempe mandi, join grup buat dapet lebih banyak". In addition to these posts, Magnet Axiom also displayed conversation artifacts (Direct Messages) that indicate interactions between the perpetrator and the victim.

4.5.2 Analysis with Oxygen Forensic

Based on the analysis of the draft-wal file extracted from the perpetrator's device, several digital artifacts were found in the form of posts on the X application.

Table 4 : Suspect's Detected Posts

Posts	Date
Video h0t b0c11 esempe Fullnya akses link dibawah	6/30/2025 12:09:14 PM
Konten H0T TERBARU bko b0c1ll esempe m4ndi Klik link dibawah	6/30/2025 12:16:57 PM

As shown in Table 4, the posts containing content with strong indications of child pornography, namely "Video h0t b0c11 esempe Fullnya akses link dibawah" and one post identical to the evidence submitted by the victim, namely "Konten H0T TERBARU bko b0c1ll esempe m4ndi Klik link dibawah". The posting artifacts were found to have been uploaded on the same date, June 30, 2025, which can be cross-referenced with the images discovered in the image_cache folder. This correlation indicates the suspect's deliberate actions and strengthens the link between the evidence and criminal intent.

4.5.3 Analysis with Oxygen Forensic

The analysis was conducted using Oxygen Forensic Detective software on the Twitter application cache files obtained from the perpetrator's device.

Table 5 : Comments on the Suspect's Posts

Information	Posts
Account Information	piscok551278,Semarang
Comment	awas aja km saya laporkan, kita ketemu dikantor polisi

As shown in Table 5, the artifacts related to the perpetrator's X account "pisock551278." The examination revealed a comment from the victim stating, "awas aja km saya laporkan, kita ketemu dikantor polisi." This artifact demonstrates that the victim directly responded to the perpetrator's post distributing illegal content, and that the victim was aware of and rejected such actions.

4.6 PRESENTATION

The presentation stage is the final phase in the DFRWS method, aimed at delivering the results of digital forensic analysis in a structured and easily understandable report. In this research, the presentation was carried out by compiling all evidence discovered during the investigation process—from identification, preservation, collection, examination, and analysis—into a single document that can be used by investigators or authorities in the law enforcement process.

In this research, three software tools were used to obtain evidence from the Twitter application. Magnet Axiom successfully recovered several deleted posts as well as direct messages (DMs) between the perpetrator and the victim. Autopsy revealed remaining posts, shared links, and related image files. Meanwhile, Oxygen Forensic Detective was able to extract metadata from each post and clarify the communication structure between users. The device used in this research was a laptop running Windows 10 Pro. The detailed specifications are shown in Table 6.

Table 6 : Device Specifications

Laptop	Lenovo Thinkpad x260
	DESKTOP-DH2UM5H
Processor	Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz 2.50 GHz
Installed RAM	8.00 GB (7.87 GB usable)
Storage	477 GB SSD V-GEN09SM24HS512HY 512GB
Graphics Card	Intel(R) HD Graphics 520 (128 MB)
System Type	64-bit operating system, x64-based processor

The device analyzed in this research was the perpetrator's smartphone, a Redmi A5, with a primary focus on the suspect's activity on Twitter. The investigation process was carried out using several forensic tools in accordance with standard procedures. The analysis revealed various digital activities conducted by the perpetrator on Twitter, including interactions through direct messages, content uploads, and data related to the user account. Furthermore, the forensic examination also highlighted artifacts stored within the device's cache and application data, which provided additional insight into the timeline of activities performed by the suspect. These artifacts included login information, timestamps of deleted posts, and metadata associated with shared media. By reconstructing this information, investigators were able to identify behavioral patterns and uncover evidence of attempts to conceal criminal activity, such as post deletions and account modifications. The structured analysis not only validated the effectiveness of the forensic tools employed but also demonstrated the importance of systematic methodology in digital forensic investigations, particularly in cases involving social media platforms like Twitter.

Table 7 : Evidence Matching Information

Digital Evidence	Total	Description
Account info	1	Username: piscok551278 User ID: 1936743361823879169
Conversation (DM)	2	1. dasar kurangajar 2. sumpah saya akan langsung bawa ke jalur hukum
Victim's photo download	1	data\com.google.android.gm\files\downloads
Photo Post	1	Konten H0T TERBARU bko b0c1ll esempe m4ndi Klik link dibawah
Comment	1	awas aja km saya laporkan, kita ketemu dikantor polisi

As shown in Table 7, the correlation of evidence found to confirm the direct connection between both parties in the case of child pornography content distribution through the X application. One of the pieces of evidence found is direct communication between the victim and the perpetrator. The victim sent messages saying, "dasar kurangajar" and "sumpah saya akan langsung bawa ke jalur hukum". These messages were received by the perpetrator on July 1, 2025. This artifact demonstrates two-way interaction, where the victim firmly rejected the perpetrator's actions and even threatened to pursue legal action.

Table 8 : Analysis Results Details

Evidence	Software			Original
	Magnet Axiom	Oxigen Forensic	Autopsy	
Account Information	2	2	1	2
Conversation	2	2	0	2
Deleted Posts	5	2	6	10
Images Post	1	1	1	1
Telegram Link	1	1	0	1
Total	11	8	7	16

As shown in Table 8, the results of a comparison between the original data and the artifacts successfully extracted by three forensic software tools Magnet Axiom, Oxygen Forensic, and Autopsy using the Digital Forensic Research Workshop (DFRWS) method. The evidence examined includes account information, conversations, deleted posts, images, and Telegram links. To measure the level of success, an accuracy calculation (Par) was applied using formula by comparing the number of artifacts successfully extracted with the total amount of original data. The formula is expressed as follows:

$$par = \frac{\sum xO}{\sum xT} \text{ x } 100\% \quad (1)$$

Description:
Par : Accuracy value of the forensic application
$\Sigma_\chi O$: Number of variables successfully detected
$\Sigma_\chi T$: Number of variables used (original data)

Based on the calculation using Formula 1, the accuracy level of the three forensic tools used Magnet Axiom, Oxygen Forensic, and Autopsy can be determined. The accuracy results for each tool are as follows:

1. Magnet Axiom :
$par = \frac{11}{16}$ x 100% = 68.75%
2. Oxygen Forensic :
$par = \frac{8}{16}$ x 100% = 50%
3. Autopsy :
$par = \frac{7}{11}$ x 100% = 43.75%

Based on the analysis, Magnet Axiom achieved the highest accuracy rate at 68.75%. This indicates that the majority of the original data could be extracted using this application, proving that Magnet Axiom is fairly reliable in supporting the investigation process. Furthermore, Oxygen Forensic obtained an accuracy rate of 50%. This value shows that although Oxygen Forensic was able to identify several important artifacts, the scope of data successfully extracted was only half of the total original data. Meanwhile, Autopsy achieved an accuracy rate of 43.75%, which means the application detected less than half of the available data.

Table 9 : Forensic Tools Performance Presentation

No	Forensic Tools	Accuracy Rate
1	Magnet Axiom	68.75%
2	Oxygen Forensic	50%
3	Autopsy	43.75%

As shown in Table 9, each forensic application has varying capabilities in extracting digital evidence. Magnet Axiom excels in terms of artifact completeness, Oxygen Forensic presents moderate results with certain advantages, while Autopsy tends to be more limited.

5. CONCLUSION

The digital evidence investigation related to the distribution of child pornography content on application X was successfully conducted through the suspect's device by applying the DFRWS method, which covers the stages of identification, preservation, collection, examination, analysis, and presentation. Three forensic tools were utilized in this process: Magnet Axiom, Autopsy, and Oxygen Forensic Detective. Magnet Axiom successfully extracted the entire directory on the suspect's device, particularly the com.twitter.android directory, revealing one image, one video, and five deleted posts (tweets). Autopsy retrieved one post (tweet), one image, and one video that had been posted and subsequently deleted by the suspect. Meanwhile, Oxygen Forensic Detective proved to be the most comprehensive tool, as it reinforced and complemented the findings of Magnet Axiom and Autopsy by providing a more complete view of the database structure, linking user IDs with statuses and comments, and confirming that the suspect's posts had indeed been deleted.

6. REFERENCES

[1] S. Kemp, "Digital 2023 Deep-Dive: Twitter Use Jumps After Elon Musk's Acquisition," https://datareportal.com/reports/digital-2023-deep-dive-the-potential-outlook-for-twitter.

[2] Nur Muhammad Fajar, "Waspada! Predator Seks Incar Anak-anak lewat Medsos & Gim Daring," https://tirto.id/waspada-predator-seks-incar-anak-anak-lewat-medsos-gim-daring-gWpn.

[3] D. H. Jayani, "KPAI Terima 526 Pengaduan Kasus Pornografi dan Kejahatan Anak di Dunia Maya," Databoks. Accessed: Jul. 27, 2025. [Online]. Available: https://databoks.katadata.co.id/demografi/statistik/36cd4ba02479271/kpai-terima-526-pengaduan-kasus-pornografi-dan-kejahatan-anak-di-dunia-maya

[4] D. Harahap, "Kominfo Temukan 19.228 Kasus Pornografi Anak Sepanjang 2016-2024," *https://mediaindonesia.com/politik-dan-hukum/675175/kominfo-temukan-19228-kasus-pornografi-anak-sepanjang-2016-2024*, Jun. 02, 2024.

[5] Aditya Rifan, "Kenapa Banyak Konten Dewasa di Twitter atau X? Ini Aturan Hukum yang Berlaku," *https://www.suara.com/tekno/2023/10/02/071500/kenapa-banyak-konten-dewasa-di-twitter-atau-x-ini-aturan-hukum-yang-berlaku*, Oct. 2023.

[6] D. Lesmana, "Analisis Beban Kerja menggunakan Metode Recommended Weight Limit dan Lifting Index," *J. Teknol.*, pp. 21–26, Jun. 2022, doi: 10.35134/jitekin.v12i1.66.

[7] W. Noviansyah, "Polda Metro Tangkap Pria Penjual Ribuan Konten Porno Anak Via Telegram," *https://news.detik.com/berita/d-7789490/polda-metro-tangkap-pria-penjual-ribuan-konten-porno-anak-via-telegram*, Feb. 21, 2025.

[8] dw.com, "Indonesia Sasaran Video Pornografi Anak," *https://www.dw.com/id/indonesia-menjadi-sasaran-video-pornografi-anak/a-42096327*, 2018.

[9] N. Rosa, "5,5 Juta Anak Indonesia Jadi Korban Pornografi, Menkopolhukam: Korban Murid PAUD-SMA Baca artikel detikedu, '5,5 Juta Anak Indonesia Jadi Korban Pornografi, Menkopolhukam: Korban Murid PAUD-SMA,'" *https://www.detik.com/edu/edutainment/d-7301739/5-5-juta-anak-indonesia-jadi-korban-pornografi-menkopolhukam-korban-murid-paud-sma*, Apr. 2024.

[10] Gusra Mishardila, "Analisia dan Pencarian Bukti Forensik Digital Pada Aplikasi Media Sosial Facebook dan Twitter Menggunakan Metode Statik Forensik,"

[11] Rahardjo Budi, "Sekilas Mengenai Forensik Digital," *https://www.researchgate.net/profile/Budi-Rahardjo-2/publication/267997362_Sekilas_Mengenai_Forensik_Digital/links/545f20770cf27487b44f165a/Sekilas-Mengenai-Forensik-Digital.pdf*, 2013.

[12] Permana Lutfi Aldri, Fachrul Hakim, Yazid Abdullah Subhi, and Putra Rivaldo, "Analisis Forensik Keaslian Gambar Menggunakan Autopsy ," vol. 1, pp. 41–41, Dec. 2023.

[13] Nabilah Hannani, "Pengertian Twitter Beserta Sejarah dan Manfaat Twitter yang Dibahas Secara Lengkap," https://www.nesabamedia.com/pengertian-twitter/.

[14] Putra Abi, "Twitter," https://www.berotak.com/twitter/.

[15] Solihin Fauzi, Siti awaliyah, and A. Muid Aris S, "Pemanfaatan Twitter Sebagai Media Penyebaran

Informasi Oleh Dinas Komunikasi dan Informatika," *https://e-journal.upr.ac.id/index.php/JP-IPS/article/view/2813/2391*, May 2021.

[16] A. S. Subekti, "Penggunaan Digital Forensik Dalam Pembuktian Tindak Pidana Pencemaran Nama Baik Melalui Media Sosial," *Univ. Airlangga*, pp. 1–19, 2019, [Online]. Available: https://repository.unair.ac.id/97887/9/BAB I.pdf

[17] M. Riskiyadi, "Forensic Investigation of Digital Evidence in Exposing Cybercrime," *CyberSecurity dan Forensik Digit.*, vol. 3, no. 2, pp. 12–21, 2020.

[18] V. Justicia and K. Kunci, "Perlindungan Hukum Terhadap Anak Korban Pornografi," vol. 10, no. 2, 2014.

[19] Arthani Ni Luh Gede Yogi Arthani, "Eksploitasi Anak Dalam Penyebaran Pornografi di Dunia Maya," *https://e-journal.unmas.ac.id/index.php/advokasi/article/view/90/85*, vol. 8, Dec. 2018.

[20] R. Harding, "Forensik Magnet, Aksioma Magnet - Pandangan Pertama." [Online]. Available: https://eforensicsmag.com/magnet-forensics-magnet-axiom-a-first-look/

[21] "Digital Forensics with Autopsy," https://medium.com/@tusharcool118/autopsy-tutorial-for-digital-forensics-707ea5d5994d.

[22] L. A. Permana, F. Hakim, Y. A. Subhi, and P. Rivaldo, "Analisis Forensik Keaslian Gambar Menggunakan Autopsy," 2023. [Online]. Available: https://jurnal.ittc.web.id/index.php/jct/

[23] Putri Sari Amanda, M Wandriansyah, Fito Nardian, and Alif Syahputra, "Penerapan Keyword Search Module Pada Autopsy," *https://jurnal.ittc.web.id/index.php/jct/article/view/432/442*, vol. 1, Dec. 2023.

[24] I. Faisal, A. Budiman, and E. I. Fitiria, "Penerapan Digital Forensics Research Workshop Dalam Akuisisi Evidence Forensik Aplikasi Snack Video," Sep. 2023.

[25] Wahyudi Imam, Arif Muntasa, Muhammad Yusuf, and Ardi Hamzah, "Mengungkap dan Menguji Keaslian Bukti Digital Pada Kejahatan Cybercrime Dengan Metode Digital Forensic Researh Workshop," *https://journal.uim.ac.id/index.php/jatim/article/view/1068/778*, vol. 2, Oct. 2021.