Forensic Analysis of Instagram Application Against Case of Spreading Hoax Content using National Institute of Justice Method

Dhea Aprila Hi Hakim
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

In the digital era, social media is the main means of sharing information, but platforms such as Instagram are often misused to spread hoaxes that can influence public opinion. This research aims to analyse and uncover digital evidence related to hoaxes on Instagram using the National Institute of Justice (NIJ) standard-based forensic method through five stages: preparation, collection, examination, analysis, and reporting. Data was extracted from rooted smartphones using Oxygen Forensic Detective, Belkasoft Evidence Center X, and Autopsy, focusing on digital artefacts such as DMs, captions, cached files, and metadata. The investigation results showed Oxygen Forensic Detective had the highest accuracy (95%), finding deleted DM messages, captions, images, videos, and account metadata. Autopsy recorded 86%, successfully recovering messages and captions but not media, while Belkasoft only 32% with limitations on media. These findings prove that deleted digital evidence can still be recovered, emphasising the important role of digital forensics in supporting legal proceedings against social media hoaxes.

Keywords

Digital Forensics, Instagram, Hoax Content, National Institute of Justice, Digital Evidence.

1. INTRODUCTION

In this digital era, social media has become one of the main platforms that focus on user presence and interaction and facilitate activities and collaboration between individuals [1]. Social media has not only strengthened social relationships, but has also brought great changes in people's lives, allowing anyone to participate in social activities without physical restrictions. One of its strategic benefits is as an effective communication medium for government agencies, especially in supporting the dissemination of direct, fast, and accurate information to the public [2]. With more than 4.62 billion active users in the world and around 191.4 million in Indonesia, social media has become an important means of information dissemination and social interaction in the technological era [3][4].

Instagram is a social media application that is very popular in various circles of Indonesian society. Its main function as a photo and video sharing platform makes it part of everyday communication [5]. The advantage of Instagram lies in its power to present interesting visual content, which allows users to share moments effectively [6]. However, behind these various benefits, Instagram is also often misused by irresponsible parties, especially in the spread of negative content such as hoaxes [7]. Cybercriminals usually take advantage of the freedom of access on social media to spread fake news, by first determining the target, manipulating information, and spreading it through fictitious accounts that do not include identity [8].

The spread of hoaxes is becoming increasingly dangerous because people tend to easily believe the information they receive, especially from sources that are considered trusted [9]. This has a serious impact because hoaxes can shape the wrong public opinion, cause unrest, and even trigger social conflict [10]. The Indonesian government itself has regulated sanctions against the spread of fake news through Articles 14 and 15 of Law Number 1 Year 1946 and Articles 28 and 45 of Law Number 19 Year 2016 on Electronic Information and Transactions [11]. One concrete example of a hoax case on Instagram is the spread of a fake link by the @info.bpjstku account on behalf of BPJS Ketenagakerjaan, which was later clarified as a hoax by Turnbackhoax.id [12]. This phenomenon shows the importance of applying digital forensic analysis as a systematic effort to identify and address the spread of hoaxes on social media.

2. LITERATURE STUDY

2.1 Digital Forensics

According to Prayudi [13], digital forensics is the application of science and techniques used to find, collect, secure, analyse, and interpret digital evidence. The main purpose of this process is to help reconstruct an event and ensure the validity of evidence in the legal process. In line with that, according to Muhammad Nuh Al-Azhar [14], digital forensics is divided into several areas of specialisation, such as computer forensics, mobile forensics, audio forensics, video forensics, and image forensics. The five specialisations are part of law enforcement efforts, because in the digital forensics process scientific and systematic procedures are applied to find facts related to a criminal act.

2.2 Digital Forensics Process

Digital forensics consists of four main stages, namely collection, examination, analysis, and reporting. The collection stage is carried out by identifying, securing, and duplicating digital data using forensic tools to maintain data authenticity. Furthermore, in the examination stage, investigators examine data and metadata to find traces of digital activity, such as browsing history, conversations, cache, or deleted files. The analysis stage involves using forensic methods and tools to extract and analyse data, including special techniques to find hidden data and link it to the perpetrator. Finally, in the reporting stage, forensic experts compile a report that summarises the results of the analysis, the parties involved, and recommendations for improvement so that similar incidents are not repeated, with this report being used as evidence in court and submitted to the authorities [15]. The process can be seen in Figure 1.

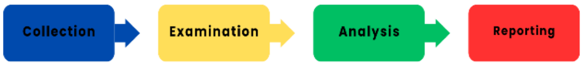


Figure 1 : Digital Forensics Process

2.3 Digital Evidence

Digital evidence is evidence in the form of document files, history files, or log files containing data related to a cybercrime case obtained from file extraction on electronic evidence. Where evidence in cybercrime cases is divided into two criteria, namely electronic evidence and digital evidence. Electronic evidence is evidence in the physical form of an electronic device or storage device [16].

2.4 Instagram

The term Instagram comes from the word "insta" which is taken from the word "instant" because this application allows users to display photos directly, and the word "gram" from "telegram" which is synonymous with sending information quickly. Thus, Instagram is designed as a platform for sharing photos and videos over the internet so that the message conveyed can be received quickly [17]. In addition, Instagram also functions as a social media that allows users to share, save, and edit photos or videos using the filters that have been provided to appear more attractive [18].

2.5 Cybercrime

Cybercrime is a criminal act committed through the internet network and can occur at any time and affect anyone, both individuals and companies, regardless of location. The motives for this crime also vary, ranging from just a fad to causing serious financial losses to victims [19]. According to Nawawi Arief [20], in a narrow sense, cybercrime is defined as computer crime that specifically targets computer systems or networks. While in a broad sense, cybercrime includes all new forms of crime that target computers, computer networks, and their use, including traditional crimes that are now carried out with the help of computer devices.

2.6 Digital Forensic Tools

Some tools commonly used in the digital forensics process include Belkasoft Evidence Center X, a software that serves to collect and analyse data from various devices, such as computers, mobile phones, and cloud storage services. In addition, Belkasoft is also equipped with data search features, tagging important information, and generating analysis reports [21]. Furthermore, Oxygen Forensic is an application specifically designed for the analysis of mobile devices, such as smartphones, with the ability to efficiently extract various types of data. Oxygen also provides a comprehensive reporting system to make it easier for examiners to read the details of the evidence found [22]. Meanwhile, Autopsy is an open-source digital forensics application equipped with a graphical interface to support the data analysis process. Autopsy is built on The Sleuth Kit (TSK), a collection of command-line tools that allow investigators to browse, search, and extract important information from various types of data more easily [23].

2.7 National Instate of Justice (NIJ)

The National Institute of Justice (NIJ) method is used to explain the stages of the investigation systematically to serve as a guideline in handling various digital forensic cases [24][25].

3. RESEARCH METHOD

This research uses the investigation process from the National Institute of Justice (NIJ) method, which consists of five stages, namely preparation, collection, examination, analysis, and report. The NIJ process can be seen in Figure 2.

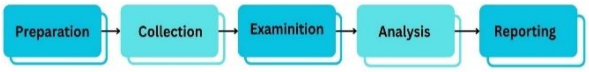


Figure 2 : NIJ Method Process

As shown in Figure 2, the research flow conducted through five main stages. In the preparation stage, the research scope was defined, focusing on hoax-related artefacts from the Instagram application, and three forensic tools were selected: Oxygen Forensic Detective, Belkasoft Evidence Center X, and Autopsy. Data collection was performed by acquiring a forensic image of the device and extracting application folders such as direct.db, WAL files, and cached media, while ensuring data integrity with hash verification (MD5/SHA-1). The examination stage involved verifying integrity, categorizing artefacts (direct messages, captions, cache), and identifying suspicious or deleted files. Analysis was conducted by interpreting artefacts to reconstruct user activities, including hoax-related captions, direct message communications, and cached promotional media, with cross-validation between tools to ensure reliability. Finally, the reporting stage documented the tools, procedures, and findings, supported by screenshots and extracted evidence to maintain objectivity and legal accountability.

4. RESULTS AND DISCUSSION

This research was conducted on a cybercrime case in the form of spreading hoax content through the Android-based Instagram application. The case scenario is divided into three stages, namely pre-incident, incident, and post- incident, which are shown in Figure 3.

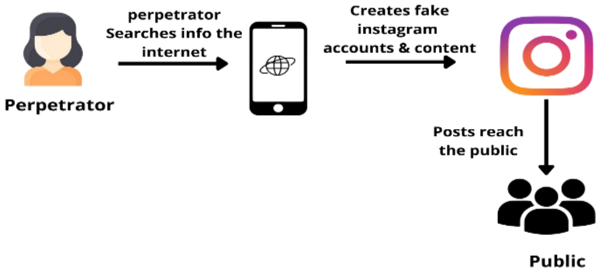


Figure 3: Pre Incident Hoax Content Dissemination

As shown in Figure 3, at this stage the perpetrator gathers information from various internet sources using a smartphone to create hoax content. After collecting sufficient data, the perpetrator creates a fake Instagram account and designs content with narratives and captions that appear legitimate. The fabricated content is then published through the newly created account, making it accessible to the public.

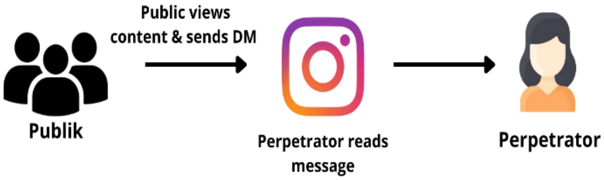


Figure 4 : Incidents of Hoax Content Dissemination

As shown in Figure 4, this stage illustrates the dissemination of hoax content, where the public begins to see the published material. The public reacts through comments and direct messages to the perpetrator's account. These interactions are used by the perpetrator to monitor the impact of the hoax content on public opinion and to measure the extent of its influence.

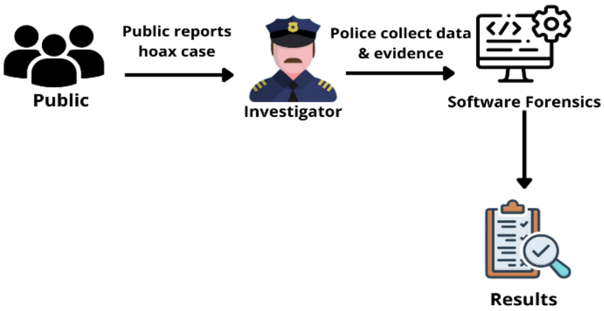


Figure 5 : Post Incident Hoax Content Dissemination

As shown in Figure 5, this stage represents the post-incident spread of hoax content. After the impact of the hoax content is felt by the community, the victim reports the incident to law enforcement officials, such as the police. The report is then forwarded to the investigation team for digital forensic examination. At this stage, investigators collect data and digital evidence, including posts, direct messages, and media files suspected of being used in the dissemination of false information. The digital evidence obtained is subsequently analyzed using forensic tools to uncover hidden information, including data deleted by the perpetrator. The results of this analysis serve as the basis for supporting the investigation and the legal proof process.

4.1 Investigation Preparation

The preparation phase began with the confiscation of Xiaomi Redmi 9A devices that were allegedly used in spreading hoax content on Instagram. An image of the evidence can be seen in Figure 6.

Figure 6 : Smartphone Evidence

All important device information, including IMEI number and operating system version, is documented as listed in Table 1.

Table 1 : Smartphone Evidence Specifications

No	Type	Description
1	Brand	Xiaomi
2	Series	Redmi 9A
3	IMEI	861716051087475
4	Operating System	Android
5	Versi OS	10

In addition, the supporting hardware and software used during the investigation are shown in Table 2.

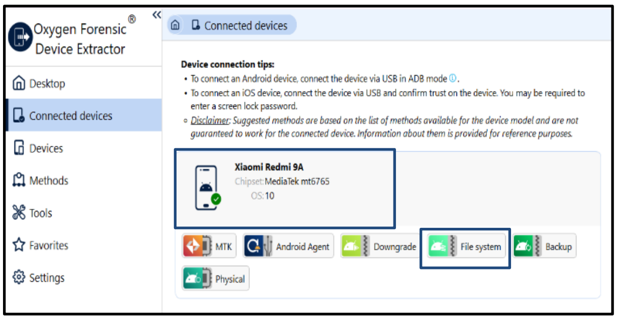
Table 2 : Investigation Supporting Devices

No	Tools	Type	Function
1	Laptop Lenovo	Hardware	Data
2	Kabel USB	Hardware	Device connection
3	Oxygen Forensik Detective	Software	Data extraction & analysis
4	Belkasoft Evidence Center X	Software	Digital artefact analysis
5	Autopsy	Software	File system & metadata

4.2 Data Collection

The data collection process was carried out on a Xiaomi Redmi 9A device using Oxygen Forensic Detective, Belkasoft Evidence Center, and Autopsy to ensure the authenticity of the acquired data. The collected data included the file system, Instagram application activity, messages, and other information relevant to the dissemination of hoax content.

As an initial step, the Developer Options were enabled on the device to allow technical configurations such as OEM Unlock and USB Debugging, enabling the forensic tools to recognize the device. The device was then rooted using magisk to grant full access to the file system without altering the original system partition (systemless). This method preserves data integrity, allowing the extraction of hidden Instagram data.



Device connection tips:

- To connect an Android device, connect the device via USB in ADB mode ⓘ.
- To connect an iOS device, connect the device via USB and confirm trust on the device. You may be required to enter a screen lock password.
- *Disclaimer: Suggested methods are based on the list of methods available for the device model and are not guaranteed to work for the connected device. Information about them is provided for reference purposes.*

Xiaomi Redmi 9A
Chipset: MediaTek mt6765
OS: 10

Figure 7 : Connection Process with Oxygen Forensics Detective

As shown in Figure 7, the device was connected to the laptop via ADB Mode so that Oxygen Forensic could detect device information such as model, chipset (MediaTek MT6765), and operating system (Android 10). The full file system extraction method was selected, which copies the entire file structure, including cache data, logs, activity history, and hidden information.

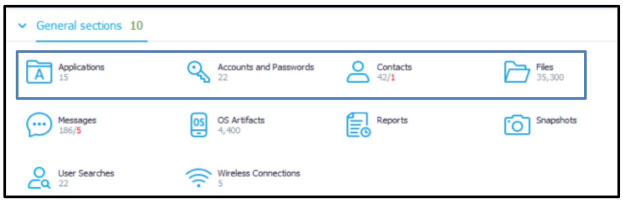


Figure 8 : Data Extraction Results

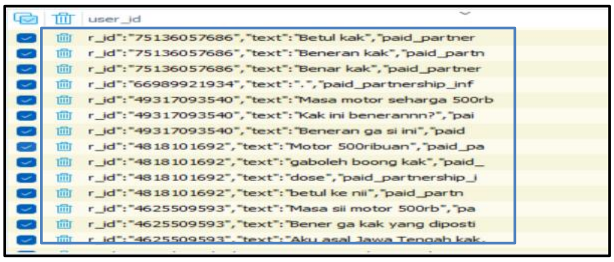
As shown in Figure 8, the extraction process involved several key steps: verifying the connection, obtaining root access, calculating the data size (10.7 GB), retrieving data from the Android Keystore (encrypted credential storage), and generating hash values to ensure data integrity. After approximately 15 minutes, the process was successfully completed, producing a full copy of the device's file system with a total size of 10.7 GB.

4.3 Examination

This stage aims to analyze extracted data to identify relevant evidence. Artifacts from Instagram, such as account information, messages, media files, and deleted data, were examined using Oxygen Forensic Detective, Belkasoft Evidence Center X, and Autopsy. The analysis explored file structures, app databases, and activity logs to trace digital footprints related to hoax dissemination. Each data point was evaluated and matched to the case context.

4.3.1 Findings with Oxygen Forensic Detective

The examination used Oxygen Forensic Detective to analyze mobile device artifacts, including app activity, messages, media, and account metadata. The analysis focused on artifacts related to hoax dissemination on Instagram by inspecting internal file structures using text and hex views.



```
user_id
r_id":"75136057686","text":"Betul kak","paid_partner
r_id":"75136057686","text":"Beneran kak","paid_partn
r_id":"75136057686","text":"Benar kak","paid_partner
r_id":"66989921934","text":".","paid_partnership_inf
r_id":"49317093540","text":"Masa motor seharga 500rb
r_id":"49317093540","text":"Kak ini benerannn?","pai
r_id":"49317093540","text":"Beneran ga si ini","paid
r_id":"4818101692","text":"Motor 500ribuan","paid_pa
r_id":"4818101692","text":"gaboleh boong kak","paid_
r_id":"4818101692","text":"dose","paid_partnership_i
r_id":"4818101692","text":"betul ke nii","paid_partn
r_id":"4625509593","text":"Masa sii motor 500rb","pa
r_id":"4625509593","text":"Bener ga kak yang diposti
r_id":"4625509593","text":"Aku asal Jawa Tengah kak
```

Figure 9 : Direct Mesage Analysis Results

As shown in Figure 9, direct Message (DM) found 15 messages that have been deleted but still recorded in the mutations table in the direct.db database. This finding shows communication activities related to the promotion of cheap motorbikes that are at the heart of the hoax.

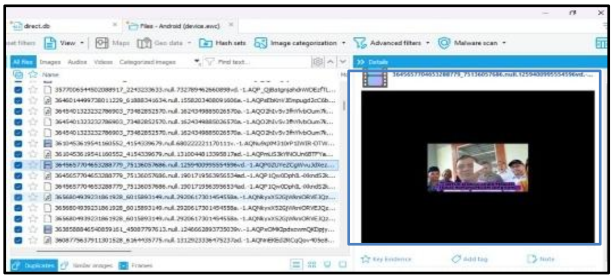
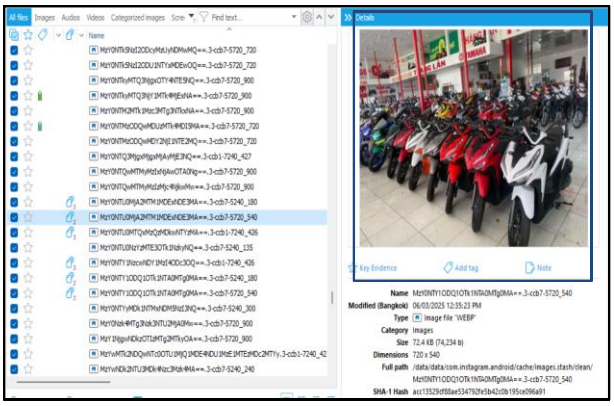


Figure 10 : Video and Image File Findings from Application Cache

As shown in Figure 10, the examination results of the Instagram videocache folder using Oxygen Forensic Detective. This folder stores .mp4 video files that are automatically saved when content is played through the application. One of the files has a duration of 30 seconds with a resolution of 720x1280 pixels, last modified on June 2, 2025, at 05:18:40 AM, and located at /data/data/com.instagram.android/cache/videocache/. This finding serves as evidence that the content was played or loaded on Instagram even after being deleted, while the recorded SHA-1 hash value ensures the integrity of the file.

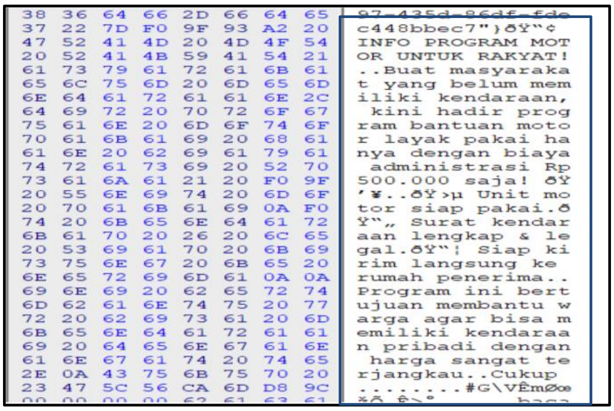


```
Name
MzY0NTk5NzI2ODcyMzUyNDMwMQ==.3-ccb7-5720_720
MzY0NTk5NzI2ODU1NTYxMDEwOQ==.3-ccb7-5720_720
MzY0NTkyMTQ3NjgxOTY4NTE5NQ==.3-ccb7-5720_900
MzY0NTkyMTQ3NjY1MTk4MjExNA==.3-ccb7-5720_900
MzY0NTM2MTk1Mzc3MTg3NTkxNA==.3-ccb7-5720_900
MzY0NTMzODQwMDUzMTk4MDI5MA==.3-ccb7-5720_720
MzY0NTMzODQwMDY2NjI1NTE2MQ==.3-ccb7-5720_720
MzY0NTQ3MjgxMjgxMjAyMjE3NQ==.3-ccb1-7240_427
MzY0NTQwMTMyMzIxNjAwOTA0Ng==.3-ccb7-5720_900
MzY0NTQwMTMyMzIzMjc4NjkwMw==.3-ccb7-5720_900
MzY0NTU0MjA2MTM1MDExNDE3MA==.3-ccb7-5240_180
MzY0NTU0MjA2MTM1MDExNDE3MA==.3-ccb7-5720_540
MzY0NTU0MTQxMzQzMDkwNTYzMA==.3-ccb1-7240_426
MzY0NTU0NzYzMTE3OTk1NzkyNQ==.3-ccb7-5240_135
MzY0NTY1NzcwNDY1MzI4ODc3OQ==.3-ccb1-7240_426
MzY0NTY1ODQ1OTk1NTA0MTg0MA==.3-ccb7-5240_180
MzY0NTY1ODQ1OTk1NTA0MTg0MA==.3-ccb7-5720_540
MzY0NTYyMDk1NTMxNDM5NzI3NQ==.3-ccb7-5240_300
MzY0Nzk4MTg3Nzk3NTU2MjA0Mw==.3-ccb7-5720_900
MzY1NjgwNDkzOTIzMTg2MTkyOA==.3-ccb7-5720_900
MzYwMTk2NDQwNTc0OTU1MjQ1MDE4NDU1MzE1MTEzMDc2MTYy.3-ccb1-7240_42
MzYwNDk2NTU3MDk4Nzc3Mzk4MA==.3-ccb7-5240_240
```

```
Name             MzY0NTY1ODQ1OTk1NTA0MTg0MA==.3-ccb7-5720_540
Modified (Bangkok) 06/03/2025 12:35:23 PM
Type             Image file "WEBP"
Category         Images
Size             72.4 KB (74,234 b)
Dimensions       720 x 540
Full path        /data/data/com.instagram.android/cache/images.stash/clean/
                 MzY0NTY1ODQ1OTk1NTA0MTg0MA==.3-ccb7-5720_540
SHA-1 Hash       acc13529df88ae534792fe5b42c0b195ce096a91
```

Figure 11 : Deleted Image Posts

As shown in Figure 11, the results of the analysis of the images.stash folder using Oxygen Forensic Detective, where a WEBP image file was found measuring 72.4 KB with a resolution of 720x540 pixels, last modified on 2 June 2025. The file is located in the directory data/data/com.instagram.android/cache/ images.stash/clean/ as a cache of content that has been accessed. The existence of this file, even though it no longer appears in the application, proves that images related to the spread of hoaxes have been accessed.



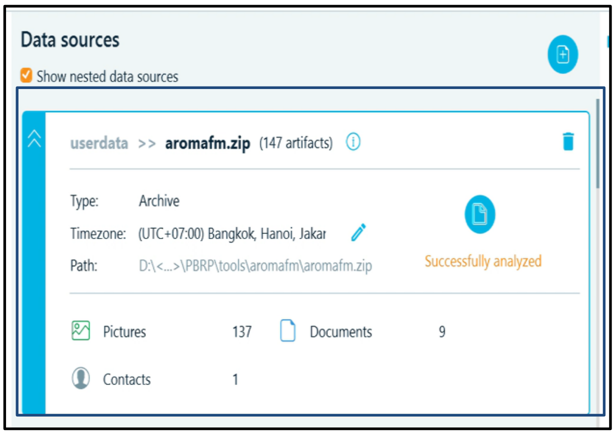
```
38 36 64 66 2D 66 64 65   97-435d-86df-fde
37 22 7D F0 9F 93 A2 20   c448bbec7"}ðŸ"¢ 
47 52 41 4D 20 4D 4F 54   INFO PROGRAM MOT
20 52 41 4B 59 41 54 21   OR UNTUK RAKYAT!
61 73 79 61 72 61 6B 61   ..Buat masyaraka
65 6C 75 6D 20 6D 65 6D   t yang belum mem
6E 64 61 72 61 61 6E 2C   iliki kendaraan,
64 69 72 20 70 72 6F 67    kini hadir prog
75 61 6E 20 6D 6F 74 6F   ram bantuan moto
70 61 6B 61 69 20 68 61   r layak pakai ha
61 6E 20 62 69 61 79 61   nya dengan biaya
74 72 61 73 69 20 52 70    administrasi Rp
73 61 6A 61 21 20 F0 9F   500.000 saja! ðŸ
20 55 6E 69 74 20 6D 6F   '¥..ðŸ›µ Unit mo
20 70 61 6B 61 69 0A F0   tor siap pakai.ð
74 20 6B 65 6E 64 61 72   Ÿ"„ Surat kendar
6B 61 70 20 26 20 6C 65   aan lengkap & le
20 53 69 61 70 20 6B 69   gal.ðŸ"¦ Siap ki
73 75 6E 67 20 6B 65 20   rim langsung ke
6E 65 72 69 6D 61 0A 0A   rumah penerima..
69 6E 69 20 62 65 72 74   Program ini bert
6D 62 61 6E 74 75 20 77   ujuan membantu w
72 20 62 69 73 61 20 6D   arga agar bisa m
6B 65 6E 64 61 72 61 61   emiliki kendaraa
69 20 64 65 6E 67 61 6E   n pribadi dengan
61 6E 67 61 74 20 74 65    harga sangat te
2E 0A 43 75 6B 75 70 20   rjangkau..Cukup 
23 47 5C 56 CA 6D D8 9C   ........#G\VÊmØœ
```

Figure 12 : Deleted video caption post

As shown in Figure 12, a hoax promotion caption "INFO PROGRAM MOTOR FOR RAKYAT! … only Rp 500,000!" was successfully recovered from the WAL (Write-Ahead Log) file, proving that the caption had indeed been created.

4.3.2 Findings with Belkasoft Evidence Centre X

Belkasoft Evidence Center was used to examine extracted data from Oxygen Forensic, focusing on Instagram artifacts such as messages and captions. The tool presents data in a structured format, facilitating the initial identification of user activity related to hoax dissemination.



Data sources

☑ Show nested data sources

userdata >> **aromafm.zip** (147 artifacts)

Type: Archive

Timezone: (UTC+07:00) Bangkok, Hanoi, Jakar

Path: D:\<...>\PBRP\tools\aromafm\aromafm.zip

Successfully analyzed

Pictures 137

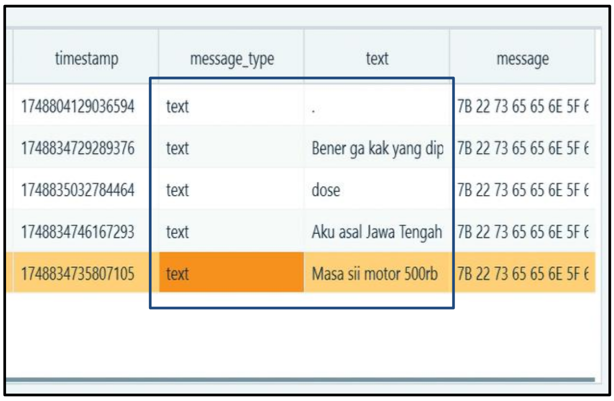
Documents 9

Contacts 1

Figure 13 : Results of Belkasoft Evidence Centre X Data Analysis Process

As shown in Figure 13, Belkasoft Evidence Center successfully imported and analyzed the aromafim.zip archive, which contained data acquired from the device as a source for digital artifact examination. The initial extraction process identified a total of 147 artifacts, consisting of 137 image files, 9 documents, and 1 contact.

The Belkasoft interface presents the information in a structured manner, including artifact categorization based on application types such as Android apps, file system, SMS, and WhatsApp, allowing investigators to easily filter artifacts relevant to the case. Additionally, the information panel displays details such as time zone, investigator name, and data storage path to maintain authenticity and forensic traceability. This well-organized interface supports further analysis of artifacts related to hoax content distribution.

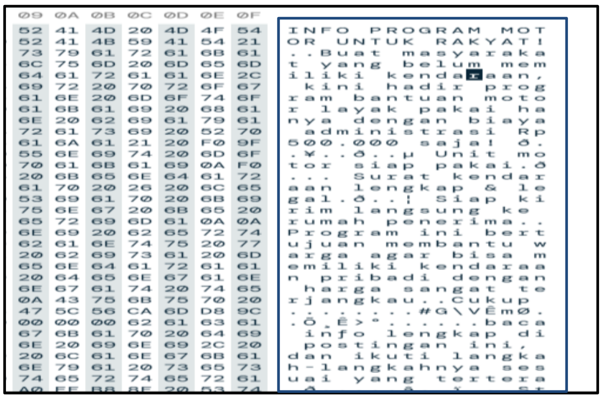


timestamp	message_type	text	message
1748804129036594	text	.	7B 22 73 65 65 6E 5F 6
1748834729289376	text	Bener ga kak yang dip	7B 22 73 65 65 6E 5F 6
1748835032784464	text	dose	7B 22 73 65 65 6E 5F 6
1748834746167293	text	Aku asal Jawa Tengah	7B 22 73 65 65 6E 5F 6
1748834735807105	text	Masa sii motor 500rb	7B 22 73 65 65 6E 5F 6

Figure 14 : Direct Message (DM) view has been deleted

As shown in Figure 14, direct Message (DM) view has been deleted, The examination was conducted using the SQLite Viewer feature in Belkasoft. From the analysis, Direct Message (DM) messages that were previously sent through the Instagram application were identified. Some of the messages that were successfully read included: "Bener ga kak yang dip", " Aku asal jawa tengah", and "Masa sii motor 500rb".

These messages are a strong indication that the account user was involved in a conversation related to the promotional content under investigation. These results also show that the database is still intact and able to store conversation data even after being deleted from the application.



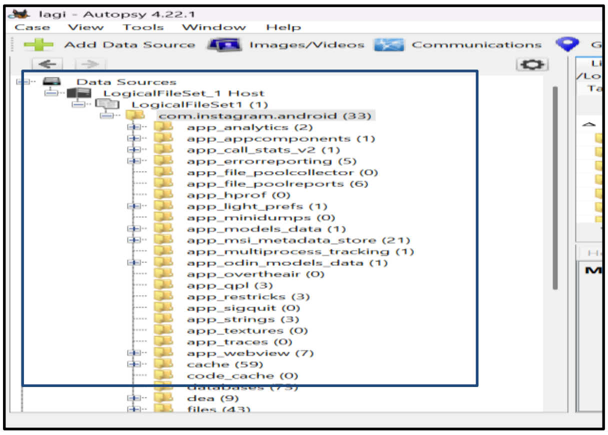
```
09 0A 0B 0C 0D 0E 0F
52 41 4D 20 4D 4F 54   INFO PROGRAM MOT
52 41 4B 59 41 54 21   OR UNTUK RAKYAT!
73 79 61 72 61 6B 61   ..Buat masyaraka
6C 75 6D 20 6D 65 6D   t yang belum mem
64 61 72 61 61 6E 2C   iliki kendaraan,
69 72 20 70 72 6F 67    kini hadir prog
61 6E 20 6D 6F 74 6F   ram bantuan moto
61 6B 61 69 20 68 61   r layak pakai ha
6E 20 62 69 61 79 61   nya dengan biaya
72 61 73 69 20 52 70    administrasi Rp
61 6A 61 21 20 F0 9F   500.000 saja! ð.
55 6E 69 74 20 6D 6F   .¥..ð..µ Unit mo
70 61 6B 61 69 0A F0   tor siap pakai.ð
20 6B 65 6E 64 61 72   ... Surat kendar
61 70 20 26 20 6C 65   aan lengkap & le
53 69 61 70 20 6B 69   gal.ð..¦ Siap ki
75 6E 67 20 6B 65 20   rim langsung ke
65 72 69 6D 61 0A 0A   rumah penerima..
6E 69 20 62 65 72 74   Program ini bert
62 61 6E 74 75 20 77   ujuan membantu w
20 62 69 73 61 20 6D   arga agar bisa m
65 6E 64 61 72 61 61   emiliki kendaraa
20 64 65 6E 67 61 6E   n pribadi dengan
6E 67 61 74 20 74 65    harga sangat te
0A 43 75 6B 75 70 20   rjangkau..Cukup
47 5C 56 CA 6D D8 9C   ..........#G\VÊmØ.
00 00 00 62 61 63 61   .Õ.Ê>°.......baca
67 6B 61 70 20 64 69    info lengkap di
6E 20 69 6E 69 2C 20    postingan ini,
20 6C 61 6E 67 6B 61   dan ikuti langka
6E 79 61 20 73 65 73   h-langkahnya ses
74 65 72 74 65 72 61   uai yang tertera
```

Figure 15 : View of deleted video caption post

As shown in Figure 15, the results of forensic analysis using Hexadecimal Viewer on the clips_75136057686-wal file, which is a write-ahead log file of user activity before it is saved to the main database. Analysis through Belkasoft managed to find pieces of captions containing promotional narratives, such as "INFO PROGRAM MOTOR FOR RAKYAT! only costs Rp500,000 only!". This finding proves that even though posts have been deleted, caption data is still stored in Instagram's database system and can be recovered through forensic analysis, thus potentially becoming valid evidence in legal investigations.

4.3.3 *Findings with Autopsy*

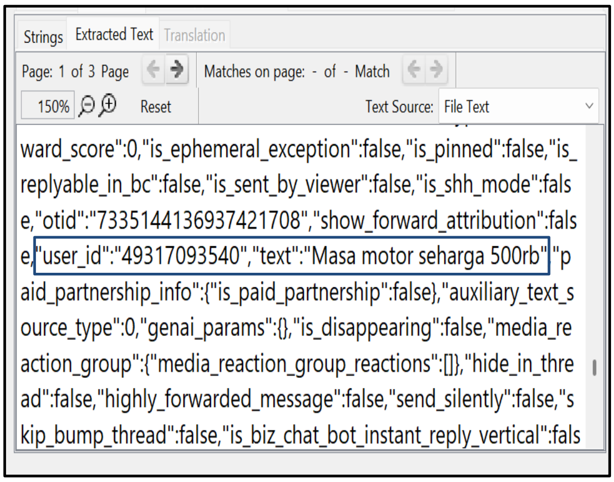
Autopsy was used as a supporting tool to explore Instagram app folder structures such as cache, databases, and system files from the extracted data obtained via Oxygen Forensic. It helps complement the identification of digital artifacts by presenting the file organization within the app system.



```
Data Sources
  LogicalFileSet_1 Host
    LogicalFileSet1 (1)
      com.instagram.android (33)
        app_analytics (2)
        app_appcomponents (1)
        app_call_stats_v2 (1)
        app_errorreporting (5)
        app_file_poolcollector (0)
        app_file_poolreports (6)
        app_hprof (0)
        app_light_prefs (1)
        app_minidumps (0)
        app_models_data (1)
        app_msi_metadata_store (21)
        app_multiprocess_tracking (1)
        app_odin_models_data (1)
        app_overtheair (0)
        app_qpl (3)
        app_restricks (3)
        app_sigquit (0)
        app_strings (3)
        app_textures (0)
        app_traces (0)
        app_webview (7)
        cache (59)
        code_cache (0)
        databases (73)
        dea (9)
        files (43)
```

Figure 16 : DM and Video Caption findings in Autopsy

As shown in Figure 16, the findings related to direct messages (dm) and video captions in autopsy. The initial examination using autopsy revealed the folder structure of the instagram application on android devices, specifically within the com.instagram.android directory. This directory contains several subfolders such as app_analytics, app_components, and app_resources, which store configuration files, cache data, and operational information. Autopsy presents this directory structure hierarchically along with associated metadata, making it easier to identify the location of digital artifacts. These findings serve as a crucial foundation for further artifact analysis and tracing.

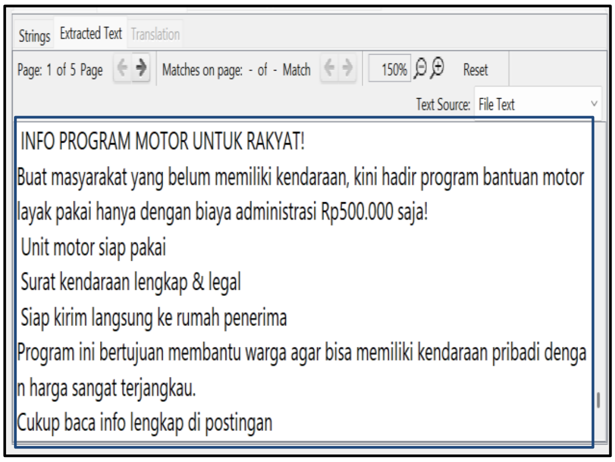


```
ward_score":0,"is_ephemeral_exception":false,"is_pinned":false,"is_
replyable_in_bc":false,"is_sent_by_viewer":false,"is_shh_mode":fals
e,"otid":"7335144136937421708","show_forward_attribution":fals
e,"user_id":"49317093540","text":"Masa motor seharga 500rb","p
aid_partnership_info":{"is_paid_partnership":false},"auxiliary_text_s
ource_type":0,"genai_params":{},"is_disappearing":false,"media_re
action_group":{"media_reaction_group_reactions":[]},"hide_in_thre
ad":false,"highly_forwarded_message":false,"send_silently":false,"s
kip_bump_thread":false,"is_biz_chat_bot_instant_reply_vertical":fals
```

Figure 17 : Result Direct Massage (DM)

As shown in Figure 17, the results of analysing the /com.instagram.android/ databases/ folder with Autopsy found the direct.db-journal file which functions as a SQLite temporary log. Through the Extracted Text feature, deleted conversations such as "Masa motor seharga 500rb" were identified, as well as important metadata (user ID, thread_id, timestamp).

This finding proves that deleted message artefacts remain in the journal file and are relevant as forensic evidence.



INFO PROGRAM MOTOR UNTUK RAKYAT!
Buat masyarakat yang belum memiliki kendaraan, kini hadir program bantuan motor
layak pakai hanya dengan biaya administrasi Rp500.000 saja!
Unit motor siap pakai
Surat kendaraan lengkap & legal
Siap kirim langsung ke rumah penerima
Program ini bertujuan membantu warga agar bisa memiliki kendaraan pribadi denga
n harga sangat terjangkau.
Cukup baca info lengkap di postingan

Figure 18 : Caption on Video Post

As shown in Figure 18, the image of the post identified during the examination. Analysis of the clips_75136057686-wal file in the Instagram database revealed promotional text offering cheap motorbikes for Rp500,000, including the phrase “INFO PROGRAM MOTOR FOR RAKYAT!”.

This content is suspected to be a hoax because it contains unrealistic claims. Although the original post was deleted, the data remains stored in the WAL file, serving as important digital evidence of hoax dissemination.

4.4 Analysis

The analysis stage is carried out on the digital data obtained to understand the context of each artefact and the relationship between data such as messages, media and metadata. The aim is to identify relevant evidence and develop patterns of digital activity that support the proof of the alleged spread of hoaxes.

The analysis utilised three main tools: Oxygen Forensic Detective to read the Instagram database structure and display communication artefacts (DMs, media cache, user activity), Belkasoft Evidence Center to drill down to the hexadecimal level, and Autopsy to open directory structures and file systems, including deleted artefacts.

4.4.1 Analysis Using Oxygen Forensic Detective

Analysis of the data/data/com.instagram.android/ folder revealed a database file (direct.db) containing 4,477 entries in the mutations table, including deleted messages such as "That's right sis" and "I'm from Central Java sis, if it's true I want it sis". These messages show persuasive communication patterns that support the spread of hoaxes. Metadata such as user_id and mutation_type confirm the authenticity of the data.

In addition, deleted media files were found in the cache folder: videos (MOV format, 30 seconds duration, valid SHA-1 hash) and images (.WEBP, 720x540 px) that match the narrative of the cheap motorbike promotion. Hoax captions, such as "INFO PROGRAM MOTOR FOR RAKYAT!....", were also detected in the clips_75136057686-wal file, although they were removed from the application.

4.4.2 Analysis Using Belkasoft Evidence Centre X

Belkasoft recovers deleted DM conversations, such as the message "It's true what sis posted here" (ID 4625509593 to account 75136057686) with deleted status. These artefacts, along with time and file path metadata, provide strong evidence of the hoax. WAL file analysis also found a Rp500,000 motorbike promotion caption identical to the perpetrator's user ID, reinforcing the artefact's connection to the main account.

4.4.3 Analysis Using Autopsy

Autopsy revealed artefacts in the direct.db-journal file that contained deleted conversations such as "Masa sii motorcycle 500rb" and important metadata (user_id, timestamp, thread_id). The WAL file (clips_75136057686-wal) also contains a caption with the theme of a cheap motorbike promotion for the Central Java region, indicating hoax content despite the post being deleted. This finding confirms that digital artefacts remain in the system and can be used as forensic evidence.

4.5 Reporting

The reporting process was conducted after all digital artefacts were analysed using Oxygen Forensic Detective, Belkasoft Evidence Center X, and Autopsy. The investigation focused on a Xiaomi Redmi 9A device (IMEI: 861716051087475, OS: Android 10) targeting the Instagram app. Key findings included the perpetrator's account information, Direct Message (DM) conversations, media (photos and videos), and captions containing hoax content. Each artefact is accompanied by metadata such as timestamp, file location, and hash value to ensure the authenticity and integrity of the digital evidence.

Furthermore, the correlation of these artefacts allowed investigators to reconstruct the timeline of activities carried out by the perpetrator. By cross-referencing account details, message exchanges, and shared media, the investigation not only identified the origin of the hoax but also provided verifiable digital proof that could be presented in court or used for further legal proceedings.

All data analysed were found to be valid and relevant as forensic evidence. A summary of the findings is presented in Table 3 Information on Hoax Content Dissemination Cases.

Table 3 : Summary of Hoax Content Dissemination Case Information

No	Digital Evidence	Total	Description	
1	Account info	1	Username: indonesiaviral2025 User ID: 75136057686	
2	Conversation (DM)	15	Victim	Perpetrators
			1.Kak ini beneran 2.Beneran ga si ini 3.Masa motor seharga 500rb 4.Bener ga kak yang diposting inii 5.Masa sii motor 500rb 6.Aku asal Jawa Tengah kak, kalo iya beneran aku mau kak 7.betul ke nii 8. motor 500ribua 9.gaboleh boong kak 10. dose	1. Benar kak 2. Bisa diliat postingannya, sudah banyak yang pesan kak 3. Beneran kak 4. Boleh kak 5. Betul kak
3	Contact	3	4625509593 (dheaprila._) 4818101692 (rarvinn) 49317093540 (skrepsedeay)	
4	Video posts	1	Cheap motorbike promotional content	
5	Photo post	1	30 seconds duration Format: .mp4	
6	Video caption	1	"INFO PROGRAM MOTOR UNTUK RAKYAT! hanya dengan biaya Rp 500.000 saja!"	

From this summary, it can be concluded that the perpetrator used Instagram to spread hoax information in the form of cheap motorbike promotions. The narratives found in DMs and captions are persuasive, trying to convince victims to believe the information.

During the analysis process, each tool provides different results in terms of its ability to read and extract data. A summary of the findings based on the tools is presented in Table 4.

Table 4 : List of Digital Evidence Found

Evidence	Oxygen	Belkasoft	Autopsy	Original
Message (DM)	15	4	15	15
Contacts	3	2	3	3
Videos	1	-	-	1
Images	1	-	-	1
Photo Captions	-	-	-	1
Video Captions	1	1	1	1
Total	21	7	19	22

As shown in Table 4, it can be concluded that Oxygen Forensic Detective is the best-performing tool, successfully extracting 21 artefacts, followed by Autopsy with 19 artefacts and Belkasoft Evidence Center X with 7 artefacts. Oxygen excelled as it was able to read database structures, Instagram cache files, and access artefacts that had been deleted. Autopsy was quite effective at finding hidden files in system directories, although it was not as comprehensive as Oxygen. Meanwhile, Belkasoft, while offering good data visualisation, has limitations in extracting information from cached files and deleted artefacts. The success rate of each forensic tool was calculated using Formula 1, namely:

$$Par = \frac{\Sigma_x O}{\Sigma_x T} \times 100\% \quad (1)$$

Description :
Par : The accuracy value of forensic applications
$\Sigma_x O$: The number of variables detected
$\Sigma_x T$: The number of variables used

Based on the investigation results, the amount of original data used was 22 artefacts, including DM conversations, contacts, media (images and videos), and captions. The accuracy calculation for each tool is shown in the following Table 5.

Table 5 : Calculation Results

No	Forensic Tools	Accuracy
1	Oxygen Forensik Detective	95%
2	Belkasoft Evidence Center X	32%
3	Autopsy	86%

As shown in Table 5, Oxygen Forensic Detective achieved the highest accuracy of 95 percent by extracting almost all critical artefacts, such as account IDs, Direct Messages, media files, metadata, and database structures, making it highly effective in uncovering hoax content. Autopsy ranked second with 86 percent accuracy, excelling in detecting database files and folder structures but lacking a full artefact display. Belkasoft Evidence Center X scored the lowest with 32 percent accuracy due to limited cache and caption extraction, although it remains useful for validating Direct Message content and metadata. Overall, the combination of these three tools with Oxygen as the primary tool, Autopsy for structural analysis, and Belkasoft for text validation provides the most comprehensive forensic results.

To provide a clearer comparison, the artefacts recovered by each forensic tool were summarized in Table 6. The table shows the types of artefacts, their storage locations within the Instagram application folder, and whether they were successfully recovered by Oxygen Forensic Detective, Belkasoft Evidence Center X, or Autopsy.

Table 6 : Comparison of artefact recovery results

Artefact	Loc.	Oxy	Belka	Auto	Status
Hoax caption	clips_wal	✓	✓	✓	Deleted
DM content	direct.db	✓	✓	✓	Deleted
Cached image	/cache/	✓	–	–	Deleted

The results show that Oxygen Forensic Detective provided the most comprehensive recovery, successfully extracting hoax captions, Direct Messages, and cached images, including those deleted by the user. Belkasoft Evidence Center X was also able to recover hoax captions and Direct Messages, but showed limitations in retrieving deleted cached images. Autopsy demonstrated more basic capabilities, detecting captions and Direct Messages but without full application-level parsing or recovery of cached media.

This indicates that Oxygen is best suited for Instagram-specific investigations due to its ability to parse application databases and recover deleted content, while Belkasoft can complement the process through its visualization features and partial artefact recovery. Autopsy, although more limited, remains useful for verifying metadata and providing lower-level file system inspection. These findings support the importance of applying multiple forensic tools to ensure completeness and reliability of digital evidence.

5. CONCLUSIONS

Digital forensic analysis of the Instagram application demonstrates that the implementation of the National Institute of Justice (NIJ) method, consisting of the Preparation, Collection, Examination, Analysis, and Reporting stages, was successfully applied to systematically recover digital artefacts such as Direct Messages (DMs), captions, images, and video files, including those deleted by users. The acquisition process was carried out through the full file system method on a rooted device using Magisk, enabling access to both active and deleted data. The integrity of the recovered evidence was maintained through metadata comparison, SHA-1 hash calculation, and cross-validation across different tools, ensuring that the evidence can be relied upon in legal proceedings. The comparative analysis of the three forensic tools revealed that Oxygen Forensic Detective provided the most comprehensive recovery, successfully extracting deleted captions, cached media, and conversation records. Belkasoft Evidence Center X complemented this process by recovering essential artefacts and offering strong visualization features, although it showed limitations in handling deleted cache files. Autopsy, in contrast, was primarily effective for identifying metadata and login artefacts but was less capable of interpreting Instagram-specific data. These findings highlight the importance of applying multiple forensic tools to achieve complete and reliable evidence recovery. Overall, the study confirms that the NIJ method, supported by a multi-tool approach, can effectively guide digital forensic investigations on social media platforms, while also pointing to future research opportunities related to encrypted content, cloud-based storage, and larger-scale datasets.

6. REFERENCES

[1] P. P. Sudin, R. Magdalena, E. S. Priowirjanto, and D. Soeikromo, “Penyalahgunaan Akun Instagram Perihal Penipuan Jual Beli Secara Online Ditinjau dari UU ITE dan Pasal 378 KUHP tentang Penipuan,” Journal of Education, Humaniora and Social Sciences (JEHSS), vol. 5, no. 1, pp. 20-26, Jul. 2022, doi:10.34007//jehss.v5il.8 42

[2] Y. E. Putri, F. M. Elita, and I. Gemiharto, “Pengaruh Media Sosial Instagram @Bps_Statistics Terhadap Ekuitas Merek Badan Pusat Statistik,” Ekspresi dan Persepsi : Jurnal Ilmu Komunikasi, vol. 6, no. 1, pp. 17–31, Feb. 2023, doi: 10.33822/jep.v6i1.4383.

[3] D. Yuliana, T. Yuniati, and B. P. Zen, “Analisis Bukti Digital Cyberbullying Pada Media Sosial Menggunakan Metode National Institut Of Standard And Technology (NIST) 800-101,” Ledger : Journal Informatic and Information Technology, vol. 1, no. 3, pp. 113–123, Aug. 2022, doi: 10.20895/ledger.v1i3.812.

[4] N. C. Febriani and A. Wijaya, “Komparasi Kejahatan di Twitter dan Instagram dengan Pendekatan Digital Forensic Investigation,” 2023.

[5] M. Ilham Haqqani Akademi Kepolisian Republik Indonesia, “Pemanfaatan Media Sosial Instagram Oleh Bhabinkamtibmas Guna Mengantisipasi Penyebaran Hoax Pemilu 2019 Di Polres Banyumas,” 2020.

[6] M. Vairagya Yogantari and dan I. Gusti Bagus Bayu Baruna Ariesta, “Konten Visual Instagram Sebagai Media Diseminasi Publik Tentang Covid-19,” 2021. [Online]. Available: http://senada.idbbali.ac.id

[7] I. Riadi, H. Herman, and I. A. Rafiq, “Mobile Forensic Investigation of Fake News Cases on Instagram Applications with Digital Forensics Research Workshop Framework,” International Journal of Artificial Intelligence Research, vol. 6, no. 2, Jul. 2022, doi: 10.29099/ijair.v6i2.311.

[8] S. Yuningsih, “Peran Humas Polres Metro Depok Dalam Menangani Informasi Berita Hoax Pada Media Sosial Instagram,” Seikat: Jurnal Ilmu Sosial, Politik dan Hukum, vol. 2, no. 1, pp. 1–10, Feb. 2023, doi: 10.55681/seikat.v2i1.361.

[9] A. Rahmadhany, A. Aldila Safitri, and I. Irwansyah, “Fenomena Penyebaran Hoax dan Hate Speech pada Media Sosial,” Jurnal Teknologi Dan Sistem Informasi Bisnis, vol. 3, no. 1, pp. 30–43, Jan. 2021, doi: 10.47233/jteksis.v3i1.182.

[10] J. K. Abdi, A. Najemi, D. Aga, and H. Prayudi, “Bahaya Penyampaian Berita Bohong Melalui Media Sosial,” 2021.[Online].Available:www.cnnindonesia.com/teknologi/20161229170130-185-182956/ada-800-ribu-situs-

[11] R. Mubarak and W. Trisna, “Analisis Yuridis terhadap Korban Penyebaran Berita Bohong (Hoax) di Media Sosial Juridical Analysis of Victims of News Spreading Hoax in Social Media,” Jurnal Ilmiah Penegakan Hukum, vol. 8, no. 1, 2021, doi: 10.31289/jiph.v 8i1.4214

[12] Kominfo, “[HOAKS] Akun Instagram BPJAMSOST EK,” Komdigi.

[13] R. A. Ramadhan, A. Kudus Zaini, J. Mardafora, P. Koresponden,: Rizdqi, and A. Ramadhan, “Pelatihan Investigasi Digital Forensik,” 2022.

[14] A. Aditya Wijanarko and A. Prakarsa, “Peran Digital Forensik dalam Pembuktian Tempus Delicti Sebagai Upaya Pertanggungjawaban Pidana Pelaku Pembuat Video Pornografi,” PAMPAS: Journal Of Criminal, vol. 2, p. 2021, 2021, [Online]. Available: https://www.kominfo.go.id/content/detail/8639/773-ribu-situs-diblokir-kemkominfo-setahun-

[15] A. Badman, “What Is Digital Forensics?” Accessed: Apr. 20, 2025. [Online].

[16] M. Riskiyadi, “Investigasi Forensik Terhadap Bukti Digital Dalam Mengungkap Cybercrime,” 2020.

[17] T. Trisno Mulyono, “Fotografi Instagram: Studi Literatur,” 2020. [Online]. Available: http://jurnal.usbypkp.ac.id/index.php/buanakomunikai

[18] Framuditya Bagas Saputra, Amyra Syalsabila, Yurni Fadhillah, and Ricky Firmansyah, "Peran Sosial Media Instagram Sebagai Media Komunikasi Bisnis Dalam Peningkatan Penjualan Perusahaan Mangkok Manis," Jurnal Kajian dan Penelitian Umum, vol. 1, no. 3, pp. 66–77, May 2023, doi:10.47861/jkpu-nalanda.v1i3.199

[19] H. C. Ratulangi, A. S. Wahongan, and F. R. Mewengkang, "Tindak Pidana Cyber Crime Dalam Kegiatan Perbankan."

[20] A. Suhaemin, "Karakteristik Cybercrime Di Indonesia," 2023.

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

[22] Y. D. Lestari, Y. Fitri, A. Lubis, and F. A. Siregar, "Analisis Perbandingan Kinerja Root Explorer Dan Oxygen Forensic Detective Pada Forensic Digital," Jurnal Fusion, vol. 3, no. 08, 2023, doi: 10.54543/ fusion.v3i05.350.

[23] Cyberly.Org, "What Is Autopsy?" Accessed: May 29, 2025.[Online].Available:Https://Www.Autopsy.Com/About/

[24] S. Marcellino, H. B. Seta, and W. Widi, "Analisis Forensik Digital Recovery Data Smartphone pada Kasus Penghapusan Berkas Menggunakan Metode National Institute Of Justice (NIJ)," Jurnal Informatik, 2023.

[25] A. Dwi Prasetyo et al., "Analisis Digital Forensik Spear Phishing Menggunakan Metode National Institute of Justice (Studi Kasus: Instagram Verified Account)," 2023.