

# Comparative Analysis of Digital Forensic Approaches for Hoax Content on TikTok Across Smartphone and Web Platforms

Imam Riadi<sup>1</sup>, Indah Rafni Yuni Pratiwi<sup>2</sup>, Abdul Fadlil<sup>3</sup>

<sup>1</sup>Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

<sup>2</sup>Department Informatics, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

<sup>3</sup>Department of Electrical Engineering,, Universitas Ahmad Dahlan, Yogyakarta, Indonesia

## Article Info

### Article history:

Received Feb 20, 2026

Revised June 08, 2026

Accepted June 19, 2026

### Keywords:

Digital Forensics

Hoax

TikTok

GCFIM

Investigation

## ABSTRACT

This research compares digital forensic approaches on the TikTok platform through web and smartphone environments using the Generic Computer Forensic Investigation Model (GCFIM). The study was conducted to support hoax investigations on social media through a systematic and legally accountable process consisting of the pre-process, acquisition and preservation, analysis, and presentation stages. Data acquisition and analysis were performed on Android smartphones and web browsers to obtain digital artifacts such as usernames, captions, videos, metadata, cache data, and user activity records. The results show that, in the web-based environment, Browser History Viewer achieved the highest recovery rate of 80%, followed by FTK Imager at 60%, while Browser History Examiner and Video Cache Viewer each achieved 40%. In the smartphone-based environment, Oxygen Forensic achieved a recovery rate of 40%, while MOBILedit Forensic achieved 20%. The findings also indicate that smartphone-based analysis provides more comprehensive application-level artifacts compared to web-based analysis. The implementation of GCFIM helped maintain evidence integrity and supported a structured investigation process. This research contributes a comparative evaluation of TikTok forensic investigations across mobile and web environments and is expected to serve as a reference for digital forensic practitioners and future cross-platform social media forensic investigations.

*This is an open access article under the CC BY-SA license.*



## Corresponding Author:

Imam Riadi,

Department of Information System,

Universitas Ahmad Dahlan,

Jl. Ahmad Yani (Ringroad Selatan) Tamanan Banguntapan Bantul Yogyakarta 55166, Indonesia.

Email: imam.riadi@uad.ac.id

## 1. INTRODUCTION

Cybercrime that exploits computer technology has grown rapidly alongside advances in internet technology [1]. One form of cybercrime that is causing concern is the spread of hoax content, which can influence public opinion and damage social integrity [2], [3], [4]. Social media platforms such as TikTok, with millions of active users, have become one of the main means of spreading hoax information [5], [6]. The spread of hoax content through TikTok can occur quickly and widely, potentially causing significant negative impacts [7]. Therefore, the detection and analysis of hoax content on TikTok using appropriate digital forensic methods is very important to prevent the spread of misinformation [8].

TikTok allows users to create and share short videos, but this platform has also become fertile ground for the spread of misinformation [9]. Cybercrime in the form of spreading hoaxes is often done by manipulating video content or descriptions embedded in the video [10]. In addressing this issue, a digital forensic approach has proven effective in obtaining evidence related to TikTok user activity, both through mobile applications and browser-based access, such as viewing history,

messages, comments, and even deleted videos [11]. Digital forensics is not limited to desktop computers, but also focuses heavily on mobile devices because the TikTok application leaves traces in the form of XML files, SQLite databases, video caches, and other artifacts in the internal memory of smartphones that can be extracted using tools such as Magnet AXIOM, MOBILedit Forensic Express, FTK Imager, and the like [11].

In analyzing hoax content spread through TikTok, there are two main approaches that can be used, namely web browser-based analysis and smartphone (mobile) analysis [12], [13]. These two approaches have different characteristics, with each producing a type of data that needs to be analyzed specifically [14], [15].

This research aims to compare the two approaches in analyzing hoax content on TikTok using the Generic Computer Forensic Investigation Model (GCFIM) [16], [17]. The novelty of this research lies in the integrated application of GCFIM to investigate hoax content on a single social media platform across two different access environments simultaneously, namely the TikTok web service and the TikTok mobile application. Previous studies have generally examined only one access medium at a time and rarely connected the artifact differences between environments to the implications for digital evidence handling. By applying GCFIM consistently to both environments and using the same hoax case scenario as a reference, this research seeks to identify which artifact categories can be obtained from each environment and how the differences in those artifacts affect the evidence chain in hoax investigations. GCFIM is a methodology that has been proven effective in digital forensic investigations, which includes five main stages: pre-process, acquisition & preservation, analysis, presentation, and post-process [18], [19], [20]. Each stage in GCFIM plays an important role in ensuring that the evidence collected is valid and accountable in court [21], [22], [23].

In the pre-process stage, this research began with identifying the devices used to access TikTok, either through a web browser or a smartphone. This process also included selecting the appropriate forensic tools for each approach [24], [25].

During the acquisition and preservation stage, digital data collected from both approaches will be copied and stored in a manner that preserves the integrity of the evidence [26]. This is important to ensure that the evidence collected is not contaminated or damaged during the collection process [27]. On web browsers, the data collected may include URL history, video cache, and cookies stored during TikTok usage. Meanwhile, on smartphones, the data that can be collected includes application files, user data, and media files that are uploaded or received through TikTok [28], [29].

At the analysis stage, the collected data is analyzed to identify evidence relevant to the dissemination of hoax content. Here, the two approaches are compared to assess their effectiveness in detecting and analyzing hoax content [30], [31]. After the analysis is done, the presentation stage will focus on presenting the findings discovered during the analysis process. The analysis results will be compiled into a clear and structured report, which can be used in further investigations or for legal purposes. This presentation aims to provide valid evidence that is admissible in court [32].

The final stage, post-process, involves evaluating the process that has been carried out, including verifying the accuracy and reliability of the methods used. Researchers will also provide recommendations for improving the forensic process in the future, based on the findings obtained during the analysis. Statistics on TikTok social media users, as shown in Figure 1.



Figure 1. Percentage of TikTok Users in Indonesia in 2025

The scale of TikTok adoption directly shapes the magnitude of the hoax dissemination problem on the platform, since a larger user base provides a wider channel through which misleading content can reach the public. Based on Figure 1, which shows data from a report by DataReportal by KEPIOS in February 2025, the number of active TikTok users in Indonesia who can be reached by advertisements is recorded at 108 million people. This figure reflects 37.8% of the total national population and 50.7% of the total internet users in Indonesia. This shows that more than half of internet users in Indonesia use TikTok, making this platform a huge potential target for advertisers. However, there has been a significant decline in TikTok's advertising reach compared to the previous quarter, namely -34.8% or a drop of around 57.4 million users. This decline is also evident in the annual comparison, with reach falling by -15.1% or the equivalent of 19.1 million users [33].

Demographic data shows that female TikTok users who can be reached by advertisements reach 50.8%, slightly higher than male users, who number 49.2%. When linked to the adult population aged 18 and above, the adoption rate of TikTok among Indonesians reached 53.5%, with adult female users accounting for 54.1% and adult male users reaching 52.8%. Despite the decline in advertising reach, TikTok remains a dominant platform with widespread penetration among adult users, particularly in the context of digital marketing and content distribution.

Through this research, deeper insights are expected regarding the comparative effectiveness of web browser and smartphone approaches in analyzing hoax content on TikTok. This research contributes a cross-platform forensic artifact mapping for TikTok hoax investigations and demonstrates how different acquisition levels influence artifact recovery within the GCFIM framework. In addition, the study provides practical reference points for selecting appropriate forensic acquisition approaches in social media investigations involving both mobile and web environments.

## 2. RESEARCH METHOD

This research will apply the GCFIM method, which is one of the investigation process models in the field of digital forensics developed to assist investigators or digital analysts in handling incidents in a systematic and structured manner. This is illustrated in Figure 2.

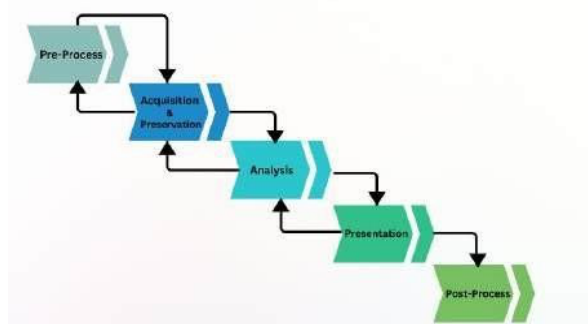


Figure 2. Research Method GCFIM

Figure 2 shows that the approach used in this research is a research scenario simulation designed to present a case of hoax content on the TikTok application. GCFIM (Generic Computer Forensic Investigation Model) has 5 stages: Pre-process, Acquisition & Preservation, Analysis, Presentation, and Post-Process, which are used in the digital investigation process [34]. Figure 2 is explained as follows:

1. Pre-Process  
At this stage, preparations are made before starting the investigation, such as obtaining approval letters from legal authorities, preparing the equipment to be used, and other preparations [35].
2. Acquisition & Preservation

This stage involves the identification, acquisition, collection, delivery, storage, and securing of data for analysis in the next stage. Data here refers to evidence collected from the scene of the incident.

3. Analysis

This stage is the main stage in forensic investigation. Analysis is performed on the data found to identify the crime that has occurred and find the perpetrator [36], [37].

4. Presentation

The results of the analysis are then documented and presented to the authorities. This stage is also crucial because the results of the analysis will be useless if the findings are presented incorrectly. Therefore, the authorities must be convinced of the results of the analysis.

5. Post-Process

This stage is the final stage in the investigation process. All physical and digital evidence is returned to the authorities for safekeeping. A review of the process is then conducted to make improvements and enhancements for future investigations.

## 2.1 Case Scenario

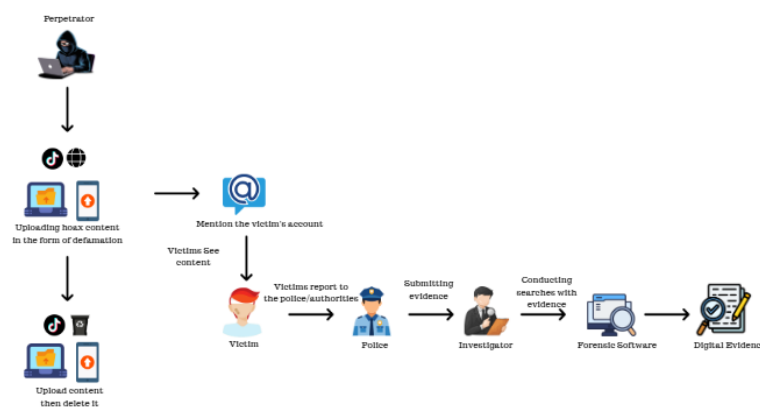


**Figure 3.** Scenario of The Spread of Hoax Content

Figure 3 is a scenario that simulates a hoax case on TikTok Web and Mobile, with the following explanation:

This scenario was created to describe the stages of forensic web browser and mobile investigation. This research scenario uses a laptop to detect hoax content spreading on the TikTok web service. This case scenario describes how the perpetrator uploaded hoax content that spread on the TikTok service running on a Mozilla Firefox web browser and mobile (smartphone). The party who feels aggrieved then reports the content to the authorities. The laptop used by the suspect becomes evidence for imaging using forensic applications. The case is then investigated by investigators using digital forensic software. The results of the investigation are in the form of digital evidence.

Programmed test parameters. In this case, the perpetrator's smartphone and laptop were subjected to a digital forensic process to find evidence. In addition to being test parameters, the purpose of creating this research scenario was to determine the actions to be taken during the research process. This scenario used a laptop to detect the spread of hoax content on the TikTok web browser. At this stage, the process of identifying evidence in this case is explained using images. The aggrieved party reported the content to the police, and the laptop used by the suspect became digital evidence using forensic applications, which were then investigated by investigators using forensic software.

The hoax content used in this scenario takes the form of short TikTok videos that contain misleading claims, presented through provocative captions and visuals that are not supported by the actual content of the video. To ensure that the content used in the experiment is genuinely categorized as a hoax, validation is performed against four predefined indicators, namely: (1) misleading or provocative captions, (2) a mismatch between the visual content of the video and its accompanying description, (3) the presence of suspicious external links, and (4) the absence of

verifiable sources. Content that meets at least two of these indicators is treated as a hoax sample within this research.

The content used in this experiment met three of the four predefined hoax indicators, namely the presence of a misleading and provocative caption, the absence of verifiable supporting sources, and the inclusion of an unsubstantiated accusation directed at a specific individual. Therefore, the content was classified as a hoax sample and used as the basis for the forensic investigation scenario in this research.

The test parameters used to compare the two access environments are defined operationally as follows: (a) the categories of digital artifacts that can be recovered, including profile photos, account names, video files, captions, comments, and URL or session metadata, (b) the success status of each artifact category, recorded as Found or Not Found per tool and per environment, and (c) the success rate per tool, calculated as the ratio of recovered artifact categories to the total number of targeted artifact categories, expressed as a percentage. These parameters are applied uniformly to both the web browser and smartphone environments so that the comparison between the two approaches is conducted on the same evaluation criteria.

To ensure ethical compliance and avoid the dissemination of actual misinformation, this research employed a controlled experimental scenario. A dedicated TikTok account created specifically for research purposes was used to upload simulated hoax content. The content consisted of a short video accompanied by the caption “Be careful, he often does scams @itsblue.sky3006”, which was intentionally designed as a sample hoax message for forensic analysis. No real individuals were targeted, and the account was operated solely within the scope of the experiment. The uploaded content was then accessed through both the TikTok mobile application and the TikTok web platform to generate digital artifacts for forensic investigation.

## 2.2 Justification of the Simulation Scenario

The simulation scenario in this research was developed based on several reported cases of hoax dissemination and defamation through TikTok in Indonesia [38], [39], [40], [41], [42]. These cases show that TikTok content containing misleading accusations, provocative captions, and unverified information may become the subject of legal investigations and produce various digital artifacts, such as usernames, captions, videos, metadata, and user activity records.

Therefore, the scenario in this research was designed as a controlled forensic simulation representing common characteristics found in TikTok hoax cases, thereby supporting the relevance and external validity of the research in the context of digital forensic investigations[43].

## 2.3 Research Tools and Materials

This Study utilizes several tools, as shown in Table 1.

**Table 1. Research Tools**

| No | Device        | Operating System       | Status                  | Function                          |
|----|---------------|------------------------|-------------------------|-----------------------------------|
| 1  | Oppo A57      | Android Lollipop 5.0.1 | Rooted                  | Research Object                   |
| 2  | Laptop Lenovo | Windows 11 64 Bit      | AMD RYZEN 7 8.00 GB RAM | Workstation for forensic analysis |
| 3  | USB Connector |                        |                         | Connect smartphone to workstation |

Several software tools used to support the study are listed in Table 2. The software is categorized into test software, operating systems, forensic tools, and analysis tools.

**Table 2. Supporting Software**

| No | Forensic Tool             | Version     | Function                     |
|----|---------------------------|-------------|------------------------------|
| 1  | TikTok                    | 2.17.351    | Software Test                |
| 2  | Windows 11                |             | Workstation Operating System |
| 3  | Oxygen Forensic Detective | 17.1.0.131  | Forensic & Analysis Tool     |
| 4  | Magnet Axiom              | 5.4.0.26185 | Forensic & Analysis Tool     |
| 5  | Exterro FTK Imager        | 4.7.3.81    | Forensic & Analysis Tool     |
| 6  | Browser History Examiner  |             | Forensic & Analysis Tool     |
| 7  | Browser History Viewer    |             | Forensic & Analysis Tool     |
| 8  | Video Cache Viewer        |             | Forensic & Analysis Tool     |

## 2.4 Comparison Method

This research uses an index calculation method to evaluate the performance of each forensic tool used on web browsers and mobile devices based on data obtained from experiments conducted [44]. the ratio formula below.

$$Pon = \frac{\sum Pn}{\sum Po} \times 100\% \quad (1)$$

Description:

$\sum pn$ : The number of digital evidence successfully found by the forensic tool.

$\sum po$ : Total number of digital evidence tested (total number of digital artifacts analyzed).

In addition to the basic ratio, each artifact category is given a weight that reflects its evidentiary importance in a hoax investigation. The weights used in this research are as follows: video content and captions are assigned a weight of 0.30 each because they directly carry the hoax narrative, comments and account identifiers are assigned a weight of 0.20 because they help establish the context and source of dissemination, and URL or session metadata are assigned a weight of 0.20 because they support traceability of the spread. The weighted score for each tool is calculated as the sum of the weights of the artifact categories successfully recovered, so that tools that recover more central artifacts receive a higher score than tools that recover only peripheral artifacts. The total weight is set to 1.00 to keep the scoring consistent across both environments.

## 3. RESULTS AND DISCUSSION

This research successfully obtained digital evidence through the process of data analysis and extraction on the social media platform TikTok. The analysis results will be presented using the GCFIM scheme.

### 3.1. Pre-Process

The pre-process stage involves determining the requirements needed for the digital forensic investigation based on the reported case. In this study, the evidence consisted of screenshots of hoax content disseminated through the TikTok platform, submitted by the victim. The screenshots contained essential information, including account usernames, content captions, profile photos, and video-related information, which served as the initial digital evidence for further analysis and verification. The collected source data are summarized in Table 3.

**Table 3.** Source Data Digital Evidence

| No | Digital Data     | Number |
|----|------------------|--------|
| 1  | Username/Account | 1      |
| 2  | Caption          | 1      |
| 3  | Video            | 1      |
| 4  | Profile Photo    | 1      |

Table 3 presents the types of digital evidence collected during the investigation, which form the basis for identifying hoax dissemination patterns and tracing the involvement of specific accounts.

The TikTok account used during the experiment was a controlled account created solely for forensic testing purposes. No real user accounts were involved in the dissemination of the simulated hoax content. This approach ensured ethical compliance and allowed the forensic process to be performed without affecting actual platform users.

### 3.2. Acquisition & Preservation

The acquisition and preservation stage focuses on securing and collecting digital evidence in a forensically sound manner. In this research, evidence acquisition was performed on both web and mobile environments. Web-based data were accessed using a laptop, while mobile data were acquired from a smartphone associated with the investigated activities.

Forensic acquisition on the laptop was conducted using FTK Imager to create a bit-by-bit copy of storage media. Meanwhile, mobile data acquisition was performed using Oxygen Forensic and MOBILedit Forensic. Throughout the process, a chain of custody was applied, and all analyses were

conducted on forensic copies to ensure the integrity and authenticity of the digital evidence. In terms of acquisition type, the laptop acquisition through FTK Imager is performed at the physical level, producing a bit-by-bit image of the storage media. The mobile acquisition through Oxygen Forensic is performed at the file system level, retrieving the file system structure of the device along with the application directory and database files of TikTok. The mobile acquisition through MOBILedit Forensic is performed at the logical level, retrieving user-accessible data such as account information, contacts, and stored media without reaching the lower file system layer. This combination of physical, file system, and logical acquisition is intended to capture different layers of digital artifacts on each environment within the limits of each tool.

## 1. Web Browser

In this section, the data acquisition process using FTK Imager for retrieving data from the web browser will be explained. The acquisition results obtained using FTK Imager are shown in Figure 4.

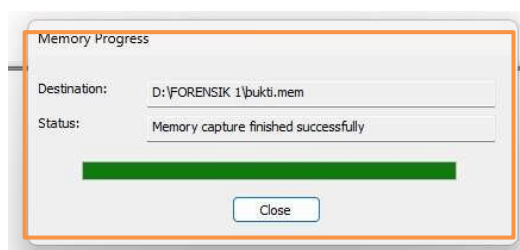


**Figure 4.** FTK Imager interface showing disk imaging and hash verification results

Figure 4 shows the successful data capture results using FTK Imager, which displays a bit-by-bit copy of the analyzed storage device. In this view, FTK Imager displays a summary of the completed capture process, with information about the storage location of the capture results and their successful status. The captured data is ready for further analysis, providing investigators with an accurate and complete copy of the examined storage media. FTK Imager also ensures the integrity of the captured data by generating a hash value, which is used to verify that the data has not been altered during the acquisition process.

## 2. Mobile

In this section, the data acquisition process using Oxygen Forensic for data collection or acquisition on a smartphone (mobile) will be explained. The data capture results using Oxygen Forensic are shown in Figure 5.

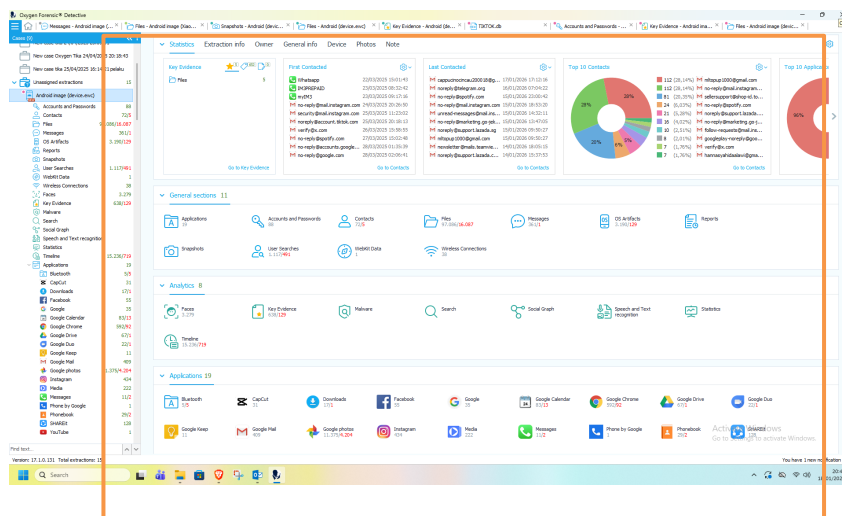


**Figure 5.** Display of Acquisition Results using Oxygen Forensic

Figure 5 shows the Oxygen Forensic interface used to analyze data extracted from a smartphone device. The display shows a summary of digital artifacts that include application information, accounts and credentials, contact data, media files, messages, and system artifacts. Oxygen Forensic also provides user activity statistics, data distribution graphs, and search and filter features based on category and time range, making it easier for investigators to identify digital data relevant to the case of hoax content dissemination on the TikTok platform. The results of the analysis using MOBILedit Forensic are shown in Figure 6.

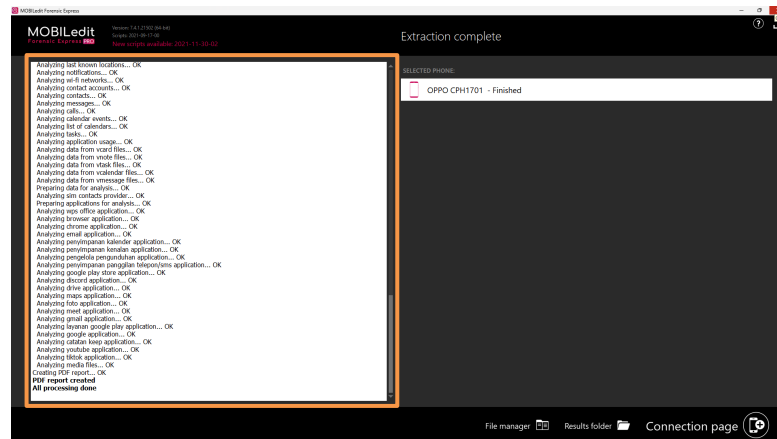


**Figure 6.** Acquisition Results Display using MOBILedit Forensic

Figure 6 shows the data extraction and analysis process using MOBILedit Forensic. This image shows the MOBILedit Forensic display at the Extraction Complete stage for the OPPO CPH1701 smartphone device. This process indicates that the initial extraction and analysis of various digital artifacts, such as contact data, messages, call history, media files, application data, and system artifacts, has been successfully completed. All of the data acquisition results are then stored in the D:\HOAX CASE 2\OPPO CPH1701 (2026-01-24 21h25m28s) folder, which is used as a forensic copy for further examination and analysis. This acquired data serves as digital evidence in the investigation of the spread of hoax content on the TikTok platform. Account Data Analysis Results.

### 3.3 Analysis

At the analysis stage, digital evidence is examined either manually or using forensic software. In this research, the analysis consists of two approaches: web-based analysis and mobile-based analysis. Web-based analysis focuses on identifying digital artifacts derived from browser activity, while mobile-based analysis examines data extracted from smartphone devices to obtain comprehensive information related to the investigated digital evidence.

The analysis process was guided by predefined hoax indicators, namely: (1) misleading or provocative captions, (2) a mismatch between video content and description, (3) the presence of suspicious external links, and (4) the absence of verifiable sources. These indicators were applied consistently to the artifacts recovered from each tool, both on the web browser and on the smartphone, so that the determination of whether a piece of content qualifies as a hoax was based on the same set of evidentiary criteria across both environments.

### 3.3.1 Web Browser Analysis Tools

### 1. FTK Imager

FTK Imager was used to examine browser-related artifacts and text-based evidence. As shown in Figure 8 and Table 2, the analysis successfully identified the perpetrator's username (@cincau) and a caption containing hoax-related content, indicating the presence of textual evidence relevant to the dissemination of misleading information on TikTok.

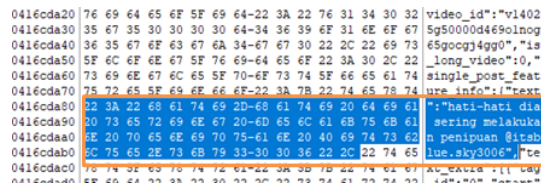


Figure 7. FTK Imager Data Collection Evidence

Figure 7 shows the first search result for the keyword “@itsblue.sky3006”. The result is a caption on TikTok with the user's caption. The caption reads, "Be careful, he often commits fraud @itsblue.sky3006". Table 4. Analysis results found using FTK Imager.

Table 4. Result Obtained Using FTK Imager

| No | Device   | Result                                                | Description |
|----|----------|-------------------------------------------------------|-------------|
| 1  | Username | @cincau                                               | Found       |
| 2  | Caption  | "Be careful, he often commits fraud @itsblue.sky3006" | Found       |

Table 4 shows the results found by FTK Imager, namely the username and caption created by the perpetrator. The caption reads "Be careful, he often commits fraud @itsblue.sky3006" and the perpetrator's username is "@cincau".

2. Browser History Examiner

Browser History Examiner was applied to analyze web browsing activities related to TikTok access. The results, presented in Figure 8, show visited URLs and access records associated with the platform, supporting the reconstruction of browsing activity during the hoax content dissemination process.

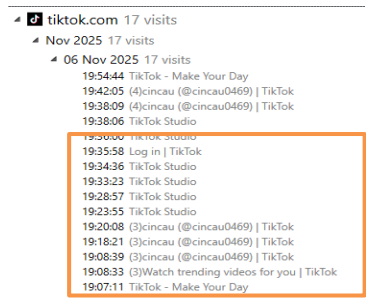


Figure 8. Browser History Examiner Analysis Results

3. Browser History Viewer

Browser History Viewer successfully identified visual artifacts, including profile photos and video thumbnails, supporting the analysis of browser-based hoax content dissemination.

4. Video Cache Viewer

Video Cache Viewer was used to retrieve cached video files stored in web browsers. The extracted video artifacts support the identification of multimedia content related to hoax dissemination activities.

3.3.2 Analysis Tools Mobile

1. Oxygen Forensic

Oxygen Forensic is used to open and analyze digital data extracted from mobile devices or smartphones. This tool displays structured information about user activity in applications and provides search and filtering features based on keywords, data types, and time ranges to facilitate the analysis of relevant data.

The data analyzed includes application account information, social media application artifacts (especially TikTok), media files, file metadata, and activity timestamps stored on the smartphone device. Oxygen Forensic supports the analysis of various mobile operating systems and is capable of presenting data in the form of a chronology of user activity. Profile photo findings in Figure 9.

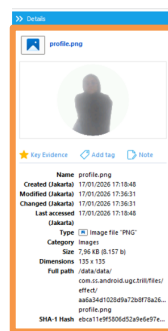


Figure 9. Profile Photo Findings from a TikTok Account using Oxygen Forensic

Figure 9 shows a digital artifact in the form of a TikTok account profile photo file that was successfully extracted using Oxygen Forensic from a smartphone device. The profile photo file is named *profile.png*, is in PNG format, is 7.96 KB in size, and has dimensions of 135 × 135 pixels. The file metadata shows the creation, modification, and last access times recorded on January 17, 2026 (WIB). In addition, the SHA-1 hash value used to ensure the authenticity and integrity of digital evidence is also displayed. This artifact is used as supporting evidence in the process of identifying accounts suspected of being involved in the dissemination of hoax content on the TikTok platform. Video File Findings in Figure 10.

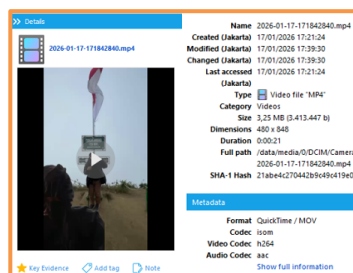


Figure 10. Video File Findings using Oxygen Forensic

Figure 10 shows digital artifacts in the form of video files that were successfully extracted using Oxygen Forensic from a smartphone device. The video file is named *2026-01-17-171842840.mp4* with MP4 format, size 3.25 MB, resolution 480 × 848 pixels, and duration 00:21 seconds. The file metadata shows the creation, modification, change, and last access times recorded on January 17, 2026 (WIB). In addition, the SHA-1 hash value is displayed as a marker of the authenticity and integrity of the digital evidence. This video file was used as the main evidence in the analysis of video content suspected of containing hoaxes on the TikTok platform.

## 2. MobileEdit Forensic

MOBILedit Forensic is used to analyze digital data extracted from mobile devices. The tool presents acquired data in a structured format and provides search and filtering functions to support efficient forensic analysis. In this research, MOBILedit Forensic was used to examine device information and social media application artifacts, particularly from TikTok, including account-related data and associated metadata. Results of account data analysis in Figure 11.

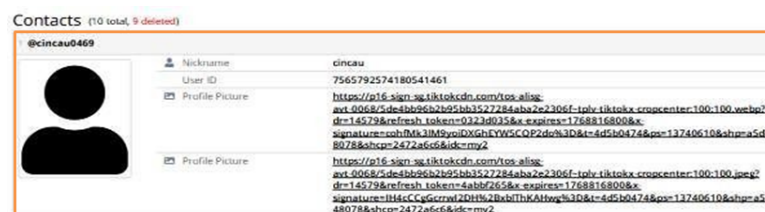


Figure 11. Results of Account Data Analysis

The analysis results are presented in the form of forensic reports. Figure 11 shows the results of account data analysis obtained from a smartphone, identifying account information such as username, user ID, and profile-related data. These findings demonstrate the linkage between the TikTok account and the examined device, supporting digital evidence identification in the investigation of hoax content dissemination.

### 3.3.3 Hoax Verification Process

In addition to extracting digital artifacts, this research implements a hoax verification process to ensure that the analyzed content can be classified as misleading or false information. This process is essential to strengthen the validity of the forensic investigation. First, metadata analysis was conducted on the extracted files, including video and image artifacts. The analysis focused on timestamps, file origin, and hash values to identify inconsistencies or indications of manipulation. Any mismatch in creation and modification times was considered a potential indicator of altered content.

Second, content consistency analysis was performed by examining the relationship between captions, usernames, and associated media. For example, captions containing accusations such as “this account is a scammer” were evaluated to determine whether they were supported by verifiable evidence or appeared as unsubstantiated claims.

Third, basic fact-checking was conducted by comparing the extracted content with publicly available information. This includes verifying whether the claims presented in the video or caption align with known facts or credible sources.

Fourth, provenance analysis was applied to identify the origin and distribution pattern of the content. This involves examining whether the content was reposted, edited, or taken out of context, which is a common characteristic of hoax dissemination. Through these verification steps, the research ensures that the identified digital artifacts are not only extracted but also validated as relevant evidence in the context of hoax dissemination on TikTok.

## 3.4 Presentation

The reporting stage is the final part of the presentation process within the GCFIM (Generic Computer Forensic Investigation Model) framework. At this stage, all results of digital forensic analysis of the Mozilla Firefox web browser and mobile devices used in the dissemination of hoax content via TikTok Web and the TikTok application are documented systematically and comprehensively. This report covers the findings from various forensic tools used during the investigation process, namely FTK Imager, Browser History Examiner, Browser History Viewer, Video Cache Viewer, Oxygen Forensic, and MOBILedit Forensic.

The purpose of this reporting stage is to present the analysis results in a measurable manner and to show a comparison of the capabilities of each forensic tool in extracting digital artifacts relevant to the case of hoax content dissemination. The results of the comparison between browser forensic tools are shown in Table 5.

**Table 5.** Comparison Results Between Browser Forensic Tools

| Digital Evidence | FTK Imager | Browser History Examiner | Browser History Viewer | Video Cache Viewer |
|------------------|------------|--------------------------|------------------------|--------------------|
| Photo/Thumbnail  | 0          | 0                        | 2                      | 0                  |
| Video            | 0          | 0                        | 0                      | 1                  |
| Caption          | 1          | 0                        | 0                      | 0                  |
| Username/Account | 1          | 1                        | 1                      | 0                  |
| Link             | 1          | 1                        | 1                      | 1                  |

Based on Table 5, a total of five categories of digital evidence were identified as reference indicators, namely photo/thumbnail, video, caption, username/account, and link. The comparison results indicate that Browser History Viewer demonstrated the highest evidence coverage by successfully identifying four out of five evidence categories, including photo/thumbnail, caption, username, and link. This suggests that Browser History Viewer provides broader visibility into browser-based artifacts related to hoax content dissemination.

FTK Imager was able to identify three categories of digital evidence, primarily text-based and

structural artifacts such as captions, usernames, and links, indicating its strength in recovering logical file and textual information. Meanwhile, Browser History Examiner identified two evidence categories, namely username and link, showing moderate capability in tracing user-related browsing activities. Video Cache Viewer also identified two evidence categories, focusing on cached video content and associated links, highlighting its specialization in multimedia artifact recovery rather than comprehensive browsing history analysis. The comparison results between mobile forensic tools are shown in Table 6.

**Table 6.** Comparison Results Between Mobile Forensic Tools

| Digital Evidence | Oxygen Forensic | MOBILedit Forensic |
|------------------|-----------------|--------------------|
| Photo/Thumbnail  | 1               | 0                  |
| Video            | 1               | 0                  |
| Caption          | 0               | 0                  |
| Username/Account | 0               | 1                  |
| Link             | 0               | 0                  |

Based on Table 6, five categories of digital evidence were used as reference indicators in the mobile forensic analysis, including photo/thumbnail, video, caption, username/account, and link. The results show that Oxygen Forensic was able to extract two categories of digital evidence, namely photos/thumbnails and video files, indicating its strength in recovering visual and multimedia artifacts from the TikTok application stored on the smartphone. This capability is particularly relevant for analyzing visual-based hoax content dissemination.

In contrast, MOBILedit Forensic identified only one category of digital evidence, namely username/account information. This indicates that MOBILedit Forensic is more effective in extracting basic account-related metadata rather than multimedia or content-level artifacts. The limited recovery of visual evidence suggests constraints in accessing or decoding application-level cached media on the examined device.

Overall, the comparison highlights that mobile forensic tools exhibit different extraction capabilities depending on the type of digital artifact targeted. Oxygen Forensic demonstrates stronger performance in multimedia evidence acquisition, while MOBILedit Forensic is more suited for basic user identity analysis. These differences emphasize the importance of selecting mobile forensic tools based on the specific objectives and evidence requirements of the investigation.

The results of the comparison not only show differences in the number of extracted artifacts but also indicate fundamental differences in data accessibility between platforms. The superior performance of smartphone-based analysis is attributed to direct access to application-level artifacts such as SQLite databases, cached media files, and internal storage data, which are not accessible in web-based environments.

In contrast, web-based forensic analysis relies primarily on browser-generated artifacts such as history, cookies, and cached files, which provide limited visibility into user activity within the TikTok platform. Therefore, the observed differences in evidence recovery are not solely caused by tool performance but are also influenced by the underlying system architecture and data access levels of each platform.

These findings highlight that mobile forensic analysis is more suitable for in-depth investigations, while web-based analysis is more appropriate for preliminary or surface-level investigations where direct device access is unavailable.

Therefore, the findings in this research should not be interpreted as indicating universally superior forensic tools, but rather as observations limited to the tested tools, acquisition methods, and experimental environments used in this research.

### 3.5 Post-Process

In the Post-Process stage, the results of the forensic analysis are compiled into a valid and accountable report. All digital evidence found during the investigation, such as profile photos, videos, captions, and usernames, are evaluated, validated, and stored to ensure the integrity of the evidence and the credibility of the investigation process. Thus, this stage is key to ensuring that the

evidence found can be used in legal proceedings related to the dissemination of hoax content on TikTok Web.

#### 4. CONCLUSION

This research compares web-based and smartphone-based digital forensic approaches for investigating hoax content on the TikTok platform using the Generic Computer Forensic Investigation Model (GCFIM). The results indicate that the two approaches demonstrate different levels of effectiveness in extracting digital artifacts. In the web-based environment, Browser History Viewer achieved the highest evidence recovery rate at 80%, followed by FTK Imager at 60%, while Browser History Examiner and Video Cache Viewer each achieved 40%. In the smartphone-based environment, Oxygen Forensic successfully extracted multimedia artifacts such as profile photos and videos with a recovery rate of 40%, whereas MOBILedit Forensic identified only username or account-related information with a recovery rate of 20%. The Post-Process stage was used to evaluate, validate, and compile the investigation results into a legally accountable forensic report.

Overall, the findings show that each forensic tool has distinct strengths and limitations depending on the investigation environment, whether web or mobile, and provide useful insights for digital forensic practitioners in handling TikTok-related hoax investigations. Several limitations of this research should also be acknowledged. First, the experiment was conducted using only a single Android device model and a single web browser, limiting the generalizability of the findings to other devices, operating systems, or browser environments. Second, the analysis was performed within a controlled simulation scenario using a limited number of hoax samples, while changes in TikTok application behavior or server-side mechanisms may affect artifact availability in future investigations. Third, the comparison focused only on the forensic tools used in this research, whereas other commercial or open-source tools may produce different artifact coverage and recovery results. Therefore, future research should involve a wider range of devices, browsers, forensic tools, and hoax scenarios to further improve cross-platform GCFIM-based forensic investigation procedures. Furthermore, the experiment relied on a controlled TikTok account and a simulated hoax scenario. Therefore, the findings may differ from investigations involving real-world cases where user behavior, platform interactions, and account activities are more complex.

#### ACKNOWLEDGEMENTS

The authors received no specific financial support or external funding for the research, authorship, and/or publication of this article

#### CONFLICT OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

#### DATA AVAILABILITY

The forensic copies and digital data associated with this study are securely stored within the designated local forensic directory. Due to privacy constraints and the sensitive nature of digital forensic artifacts, the replication files are not hosted in a public online repository but are available from the corresponding author upon reasonable request.

#### AUTHOR CONTRIBUTIONS

**Imam Riadi:** Conceptualization; Methodology; Supervision; Project Administration; Writing-Review & Editing. **Indah Rafni Yuni Pratiwi:** Data Curation; Software; Investigation; Validation; Writing-Original Draft. **Abdul Fadlil:** Methodology; Supervision; Writing-Review & Editing.

#### REFERENCES

- [1] J. Hawdon, "Cybercrime: Victimization, Perpetration, and Techniques," *American Journal of Criminal Justice*, vol. 46, pp. 837–842, 2021, doi: 10.1007/s12103-021-09652-7.

- [2] K. Sharma, F. Qian, H. Jiang, N. Ruchansky, M. Zhang, and Y. Liu, "Combating Fake News," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 10, pp. 1–42, 2019, doi: 10.1145/3305260.
- [3] F. Olan, U. Jayawickrama, E. Arakpogun, J. Suklan, and S. Liu, "Fake news on Social Media: the Impact on Society," *Information Systems Frontiers*, pp. 1–16, 2022, doi: 10.1007/s10796-022-10242-z.
- [4] P. A. R. Dewi, A. Dharmawan, G. G. Aji, M. D. Winata, and J. Wahyuni, "Mapping Hoaxes, Disinformation, and Hate Speeches in Indonesia," *Technium Social Sciences Journal*, 2023, doi: 10.47577/tssj.v50i1.9943.
- [5] C. Montag, H. Yang, and J. Elhai, "On the Psychology of TikTok Use: A First Glimpse From Empirical Findings," *Frontiers in Public Health*, vol. 9, 2021, doi: 10.3389/fpubh.2021.641673.
- [6] H. S. Alawi, I. Riaadi, and Sunardi, "Improving Credibility of Digital Evidence Investigation in E- Commerce Fraud Cases using ISO / IEC 27037," vol. 6, no. 2, pp. 479–495, 2025, doi: 10.59395/ijadis.v6i2.1408.
- [7] D. H. Lan and T. M. Tung, "Exploring fake news awareness and trust in the age of social media among university student TikTok users," *Cogent Social Sciences*, vol. 10, 2024, doi: 10.1080/23311886.2024.2302216.
- [8] Y. Huang, "Application of Digital Forensics in Cybercrime Investigations," *Applied and Computational Engineering*, 2025, doi: 10.54254/2755-2721/2025.22847.
- [9] R. Sampige, E. G. Rodgers, A. Huang, and D. Zhu, "Education and Misinformation: Exploring Ophthalmology Content on TikTok," *Ophthalmology and Therapy*, vol. 13, pp. 97–112, 2023, doi: 10.1007/s40123-023-00834-6.
- [10] C. Femi-Adeyinka, N. A. Kose, T. Akinsowon, and C. Varol, "Digital Forensics Analysis of YouTube, Instagram, and TikTok on Android Devices: A Comparative Study," *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, pp. 1–6, 2024, doi: 10.1109/isdfs60797.2024.10527244.
- [11] B. Al-Duwairi, A. S. Shatnawi, H. Jaradat, A. Al-Musa, and H. Al-Awadad, "On the Digital Forensics of Social Networking Web-based Applications," in *2022 10th International Symposium on Digital Forensics and Security (ISDFS)*, 2022, pp. 1–6. doi: 10.1109/ISDFS55398.2022.9800839.
- [12] F. Zahrah and I. Riadi, "Browser Forensics on Web-based Tiktok Applications using Digital Forensic Research Workshop Method," *International Journal of Computer Applications*, 2023, doi: 10.5120/ijca2023923009.
- [13] M. Ali *et al.*, "Analisis Forensik Pada Instagram dan Tik Tok Dalam Mendapatkan Bukti Digital Dengan Menggunakan Metode NIST 800-86," vol. 2, no. 1, pp. 44–54, 2024.
- [14] F. Anggraini, H. Herman, and A. Yudhana, "Analisis Forensik Aplikasi TikTok Pada Smartphone Android Menggunakan Framework Association of Chief Police Officers," *JURIKOM (Jurnal Riset Komputer)*, 2022, doi: 10.30865/jurikom.v9i4.4738.
- [15] R. N. Fauzi and N. Anwar, "Multimedia Forensic Analysis of TikTok Application Using National Institute of Justice (NIJ) Method," *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, 2023, doi: 10.26555/jiteki.v9i4.26924.
- [16] E. Egho-Promise, S. Idahosa, G. Asante, and A. Okungbowa, "Digital Forensic Investigation Standards in Cloud Computing," *Universal Journal of Computer Sciences and Communications*, 2024, doi: 10.31586/ujcsc.2024.923.
- [17] U. Changsan and P. Boonyopakorn, "Log4shell Investigate Based On Generic Computer Forensic Investigation Model," *2023 20th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, pp. 1–6, 2023, doi: 10.1109/ecti-con58255.2023.10153283.
- [18] M. Alex *et al.*, "A Process Model to Enhance the Accuracy of Digital Forensic Investigations: A case of National Identification and Registration Authority (NIRA-Uganda)," *East African Journal of Information Technology*, 2022, doi: 10.37284/eajit.5.1.1015.
- [19] M. Pilski, "Methods to acquisition digital evidence for computer forensics," *Studia Informatica. System and information technology*, 2022, doi: 10.34739/si.2022.26.05.

- [20] F. Alotaibi, A. Al-Dhaqm, Y. Al-Otaibi, and A. Alsewari, "A Comprehensive Collection and Analysis Model for the Drone Forensics Field," *Sensors (Basel, Switzerland)*, vol. 22, 2022, doi: 10.3390/s22176486.
- [21] A. Akinbi, Á. MacDermott, and A. Ismael, "A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models," *Digit. Investig.*, vol. 42–43, p. 301470, 2022, doi: 10.1016/j.fsidi.2022.301470.
- [22] N. Allah Rakha, "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations," *Mexican Law Review*, pp. 23–54, Feb. 2024, doi: 10.22201/ijj.24485306e.2024.2.18892.
- [23] R. Stoykova, S. Andersen, K. Franke, and S. Axelsson, "Reliability assessment of digital forensic investigations in the Norwegian police," *Digit. Investig.*, vol. 40, p. 301351, 2022, doi: 10.1016/j.fsidi.2022.301351.
- [24] I. Riadi, A. Yudhana, G. Pramuja, and I. Fanani, "Mobile Forensic Tools for Digital Crime Investigation: Comparison and Evaluation," *International Journal of Safety and Security Engineering*, 2023, doi: 10.18280/ijssse.130102.
- [25] A. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. Gadekallu, "A Comprehensive Survey on Computer Forensics: State-of-the-art, Tools, Techniques, Challenges, and Future Directions," *IEEE Access*, vol. PP, p. 1, 2022, doi: 10.1109/access.2022.3142508.
- [26] M. C. E. Lim *et al.*, "Analysis of Forensic Disk Imaging Tools for Data Acquisition and Preservation," *Journal of Informatics and Web Engineering*, 2025, doi: 10.33093/jiwe.2025.4.2.11.
- [27] M. R. Nasution, Y. Prayudi, and A. Luthfi, "Investigating Social Media User Activity on Android Smartphone," *International Journal of Computer Applications*, p., 2022, doi: 10.5120/ijca2022921890.
- [28] R. Abou-Elzhab, M. Al Rahmawy, and T. Hamza, "Comparative Study of Different Mobile Forensic Tools for Extracting Evidence from Android Devices," *Mansoura Journal for Computer and Information Sciences*, 2020, doi: 10.21608/mjcis.2020.321070.
- [29] N. J. Al-Ghamdi, M. Al-Akhras, and F. Alhosban, "Forensic Analysis of Health and Fitness Applications on Android," *International Journal of Information & Digital Security*, 2025, doi: 10.54878/6e0nbs05.
- [30] R. Prambudi, I. Riadi, and Murinto, "Analisis Forensik Mobile pada Aplikasi E-Commerce Menggunakan Metode Association of Chief Police Officers," *Cyber Security dan Forensik Digital*, 2025, doi: 10.14421/csecurity.2025.8.1.5234.
- [31] H. S. Mikayla, A. Kusyanti, and P. H. Trisnawan, "Analisis Forensik Digital untuk Investigasi Kasus Cyberbullying pada Media Sosial Tiktok," *Jurnal Teknologi Informasi dan Ilmu Komputer*, 2023, doi: 10.25126/jtiik.1078017.
- [32] I. Ismail and K. A. Z. Ariffin, "The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance," *PLOS One*, vol. 20, p., 2025, doi: 10.1371/journal.pone.0331683.
- [33] S. Kemp, "TikTok Users, Stats, Data & Trends for 2025," Datareportal, Kepios. Accessed: May 11, 2025. [Online]. Available: <https://datareportal.com/essential-tiktok-stats>
- [34] I. Riadi, A. Yudhana, and R. Saputra, "Forensik Video Pada CCTV Menggunakan Framework Generic Computer Forensics Investigation Model (GCFIM)," *JURIKOM (Jurnal Riset Komputer)*, 2023, doi: 10.30865/jurikom.v10i2.5888.
- [35] B. Meshram, V. Mendhe, and M. Singh, "Medical Forensics Principles and Cyber Crime Forensic Investigation Model," *Journal of Web Applications and Cyber Security*, 2024, doi: 10.48001/jowacs.2024.211-17.
- [36] H. Azam, M. I. Dulloo, M. H. Majeed, J. P. H. Wan, L. T. Xin, and S. R. Sindiramutty, "Cybercrime Unmasked: Investigating Cases and Digital Evidence," *International Journal of Emerging Multidisciplinaries: Computer Science & Artificial Intelligence*, 2023, doi: 10.54938/ijemdcasai.2023.02.1.255.

- [37] M. Fahmi, M. Nahdli, I. Riadi, and M. K. Biddinika, "Forensic Analysis of the WhatsApp Application Using the National Institute of Justice Framework," vol. 5, no. 2, pp. 113–122, 2024, doi: 10.59395/ijadis.v5i2.1328.
- [38] A. Bagus, "Kasus Pencemaran Nama Baik di TikTok, Seorang Wanita Laporkan Mantan Istri Pasangannya ke Polda Jatim," deliknews.com. Accessed: May 07, 2026. [Online]. Available: <https://www.deliknews.com/2025/03/05/kasus-pencemaran-nama-baik-di-tiktok-seorang-wanita-laporkan-mantan-istri-pasangannya-ke-polda-jatim/>
- [39] M. D. Leni, "Olla Ramlan Laporkan Akun Tiktok dan Instagram soal Pencemaran Nama Baik ke Polda Metro Jaya," Tempo.co. Accessed: May 07, 2026. [Online]. Available: <https://www.tempo.co/hukum/olla-ramlan-laporkan-akun-tiktok-dan-instagram-soal-pencemaran-nama-baik-ke-polda-metro-jaya-324860>
- [40] E. Erfinanto, "Kronologi Pelaporan Akun TikTok yang Menuduh Aaliyah Massaid Hamil di Luar Nikah," liputan6.com. Accessed: May 07, 2026. [Online]. Available: <https://www.liputan6.com/surabaya/read/5683686/kronologi-pelaporan-akun-tiktok-yang-menuduh-aaliyah-massaid-hamil-di-luar-nikah>
- [41] D. Apriliansyah, "Diduga Jadi Korban Pencemaran Nama Baik di TikTok, Seorang Wanita Tempuh Jalur Hukum," polrestapontianak.id. Accessed: May 07, 2026. [Online]. Available: <https://www.polrestapontianak.id/berita/diduga-jadi-korban-pencemaran-nama-baik-di-tiktok-seorang-wanita-tempuh-jalur-hukum>
- [42] D. Puspitasari, "Tasyi Athasyia Polisikan Akun TikTok soal Tudingan 'Black Campaign UMKM,'" news.detik.com. Accessed: May 07, 2026. [Online]. Available: <https://news.detik.com/berita/d-7817654/tasyi-athasyia-polisikan-akun-tiktok-soal-tudingan-black-campaign-umkm>
- [43] H. S. Alawi, I. Riadi, dan S. Sunardi, "Analisis Forensik Digital terhadap Kasus Penipuan pada E - Commerce Menggunakan Metode ACPO," *J. Inform. J. Pengemb. IT*, vol. 10, no. 3, hal. 789–801, 2025, doi: 10.30591/jpit.v10i3.8604.
- [44] M. Fahmi, M. Nahdli, I. Riadi, and M. K. Biddinika, "Comparison of Digital Forensic Tools for Drug Trafficking Cases on Instagram Messenger using NIST Method," vol. 11, no. 4, pp. 891–902, 2024, doi: 10.15294/sji.v11i4.13463.