

Web Forensic on TikTok Services in Hoax Cases using National Institute of Standards and Technology Method

Valerino Rifqi
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

The development of information technology provides opportunities for faster dissemination of information with a very broad scope. One platform that can be used for the dissemination of information is TikTok. The number of TikTok users makes the app vulnerable to drug abuse. The research is aimed at obtaining digital evidence of a hoax case on Google Chrome. The method used in this research is from the National Institute of Standards and Technology. The method has four stages of research: collection, examination, analysis, and reporting. The tools used in this study are FTK Imager, Browser History Capture, Browser History Examiner, and Video Cache Viewer. The results of this research show that forensic evidence can be collected by capturing RAM and cache using supported tools. FTK Imager obtained results for 1 caption, 1 user name, and 1 TikTok access link to log in to the perpetrator's account. The Browser History Examiner obtained evidence of the date and time of upload of the TikTok video, 1 photo of the perpetrator's profile, 1 video thumbnail, 1 username, and 1 link to the performer's TikTok. Video Cache Viewer succeeded in extracting 1 deleted video back into a playable whole video and 1 link. With effective methods and tools for identifying and collecting digital evidence, the process of investigating hoax cases can be done more efficiently and accurately. It helps authorities track the spread of hoaxes on TikTok and can be a reference for further research focused on digital forensics on other social media platforms.

Keywords

Chrome, Digital Forensics, Hoax, National Institute of Standards and Technology, TikTok.

1. INTRODUCTION

The rapid development of information technology provides an opportunity for faster dissemination of information with a very broad scope[1]. Complex and sophisticated technological developments resulted in increasing levels and variations of criminal activity as well. Such criminal acts are not only committed in the real world but also in the virtual world, the Internet is one of the facilities used for crime in the cyber world. (cybercrime)[2]. One of the platforms that can be used for the dissemination of information is social media. Social media is an internet-based platform that allows its users to carry out various forms of communication and social interaction through a number of features and supports, such as written, photo, audio, and video content[3]. Social media is one of the most important principles of information and communication technology that is highly valued by the global population. According to a new report from Hootsuite (We Are Social), as of February 2022, there are 462 million active social media users worldwide (58.4% of the world's population). By contrast, there are 191.4 million active users in Indonesia, reaching 170 million users, an increase of 12.6% from 2021. In

Indonesia, active social media users currently account for 68.9 percent of the estimated 277.7 million people[4].

The growth of social media is fairly stable from year to year. TikTok is used by users to share photos and videos, comment, and like uploaded videos. It is easy to understand social media as a digital platform that provides tools for each user to engage in social activities while producing content. Social media platforms allow users to communicate, connect, and share information and content in the form of images and videos at different frame rates. Every user will have access to locked content during the weekend. According to current thinking, the evolution of social media is a component of the growth of the Internet. Due to the impact of the past few years, social media has grown steadily and rapidly. It allows anyone with access to an internet connection to share information or content whenever they want and from wherever they are[5]. The excellence of TikTok in presenting short video content is so creative and exciting. Some users create content to get more attention and recognition, thus enhancing its sociality. Every uploaded piece of content can be fully explored if followed. As long as the content has the uniqueness of entertaining others, real-time feedback from the audience[6].

Today's dissemination of information or news often contains a lot of content that is not necessarily true and can even be categorized as fake news[7]. One of the kinds of crime that is currently growing rapidly is the spread of hoax news. By 2020, Polda Metro Jaya managed to resolve 443 cases involving hoaxes and hate speech, as well as delete 1,448 related social media accounts. Hoax news is generally spread through the manipulation of images or false information, with the aim of defaming a person, organization, or state agency. This action is considered unlawful and regulated by the ITE Act. (Electronic Information and Transactions Law)[8].

In this study, the NIST approach developed by the National Institute of Standards and Technology (NIST) was applied to collect digital forensic evidence, conduct investigations into hoax cases, and identify the necessary digital tools. The terms used to describe analysis include collection, examination, analysis, and reporting. Because it offers systematic and organized deductive analysis capabilities, the NIST method is used because it makes it easier to obtain the required data or evidence [9].

To facilitate the process of obtaining digital data, the study will analyze digital data obtained through the use of criminal investigations on the TikTok web. The aim of the project is to provide digital data, including the results of digital data analysis, that can be used to detect digital evidence of criminal activity, such as hoaxes, in court[10]. To anticipate that using tools like FTK Imager, Browser History Examiner, and Video Cache Viewer will make this digital evidence checking easier and more efficient. The aim of this research is to educate

readers about the use of ticker websites to explore digital evidence.

2. RELATED WORKS

Rizqi Rahmansyah, Carudin, and Azhari Ali Ridha (2021) on "Comparison of Digital Evidence Investigation Results on Facebook and Instagram Applications with NIST Methods," which discusses the spread of false news or hoaks on social media that can be accessed by the public through smart phones, require mobile forensic expertise to check digital evidence of suspects, both in the form of uploaded images and text messages that have been deleted. The researchers used the NIST method, which covers four aspects of forensics: collection, examination, analysis, and reporting. The investigation succeeded in finding digital evidence on the cell phone. Thus, the percentage of successful digital evidence obtained in the Instagram app is much higher than in the Facebook app, which is 75 percent for Instagram and 37.5 percent for Facebook. The timing of forensics after the removal of evidence also affects the results of the digital evidence obtained[11].

Soni, Regiolina Hayami, and Muhammad Hamadi (2022) on "Acquisition of Digital Evidence on Michat Applications on Smartphones Using the Methods of the National Institute of Standards and Technology (NIST)" throughout the article deal with cases of sex workers that are reported by various media in Indonesia. The perpetrators use the internet, both websites and social media like MiChat, to market themselves and women. The study uses the methodology of the National Institute of Standards and Technology (NIST) with four phases of forensics: collection, examination, analysis, and reporting. Based on the results of digital evidence gathering from two forensic tools, namely MobileEdit Forensic and Wondershare Dr.Fone, on two smartphone pieces of evidence, it appears that the recovery of MobileEdi Forensics data is more significant than Wondershare Dr.Fone[12].

Tomi Pandela, Priest of Riadi (2020), on "Browser Forensics on Web-based TikTok Applications," This stage of research uses forensic techniques as a measure to reveal details of contamination violations occurring in the TikTok web browser application, collecting forensic evidence by performing capture ram and cache using several tools that support data process collection, such as the FTK Imager tool, browser history capture, and video cache display. Evidence results generated by a number of tools are then analyzed to obtain digital evidence such as text, headline content, usernames of suspects and victims, photos of the profile of the suspect and the victim, video photo thumbnails, and source links from TikTok to which the suspect was accessed. Based on the tools used in this study, 80% of the items were obtained and 20% failed[13].

Rauhulloh Ayatulloh Khomeini, Noor Bintang, Rusydi Umar, and Anton Yudhana (2020) "Facebook Lite Social Media Analysis with Forensic Tools Using the NIST Method", This discussion raises digital crime evidence on the Facebook Lite application using forensic. In this research, the forensic tool that will be used is the forensic tool MOBILEedit Forensic Pro, with the help of the methods of the National Institute of Standards and Technology (NIST). The measures of collection, inspection, analysis, and reporting are used in this process. This investigation succeeded in finding the accounts used, audio, conversations, and images[14].

Dina Yuliana, Trihastuti Yuniati, Bitu Parga Zen, and Iqsyahiro Kresna A (2022), "Analysis of Digital Evidence of Cyberbullying on Social Media Using the Method National Institute of Standards and Technology (NIST) 800-10" In this

study, the acts of cyberbullies will always leave digital traces as evidence of conversations about crimes committed by perpetrators and victims on Instagram and Whatsapp. This research guide uses preservation, collection, examination, analysis, and reporting, which is the method of NIST Special Publication 800-101 Revision 1. MOBILEedit and Autopsy are applications used to dig digital evidence[4].

3. METHODOLOGY

3.1 Research Stages

This phase of research uses the methodology of the National Institute of Standards and Technology techniques applied to conduct forensic analysis. The first four steps of the NIST method are collection, examination, analysis, and reporting[15]. This method explains how to perform data analysis so that it can be used for a specific type of structured analysis so that it may be applied to a specific problem when trying to solve a particular problem that has already arisen. Explanation of 4 stages as in Figure 1.



Figure 1. National Institute of Standards and Technology

Figure 1. In the method scheme of the National Institute of Standards and Technology (NIST), there are several stages as follows:

3.1.1 Collection

Collections are the labeling, identification, recording, and retrieval of data from relevant data sources[16]. The following procedures to maintain data integrity The collection process is an early stage in conducting an investigation[17]. The collection phase is a series of activities to collect data to support the investigation process in order to search for evidence[18]. The data collected must be carefully processed and analyzed to provide accurate and relevant information.

3.1.2 Examination

Investigations involve the forensic analysis of various data collected using a mixture of automatic and manual methods to evaluate and extract relevant information while maintaining data integrity[19].

3.1.3 Analysis

Phase analysis involves evaluating the results of inspections by applying valid legal techniques and methods to obtain valuable information and answer questions that motivate data collection and research[13].

3.1.4 Reporting

Analysis results reporting may include an explanation of the measures used, a description of the choice of tools and procedures, a determination of what actions should be taken, such as conducting forensic inspections of additional data sources, ensuring that the vulnerabilities found are protected, enhancing existing security controls, and recommendations for improvements to policies, guidelines, processes, tools, and other aspects of the forensics process[20].

3.2 Research Scenario

The study illustrates a scenario of a cyber crime case, namely a perpetrator of a social media crime by attacking a victim with the act of spreading hoax content concerning the victim on social media.

3.2.1 Pre-Incident

The case scenario begins when the perpetrator feels jealous, disgusted, or hated by the victim, so the performer creates a fake account on social media with the intention of committing disrespectful behavior towards the victims on the platform. The purpose of the perpetrator is to make the victim feel ashamed or disturbed by an attack, as shown in Figure 2.

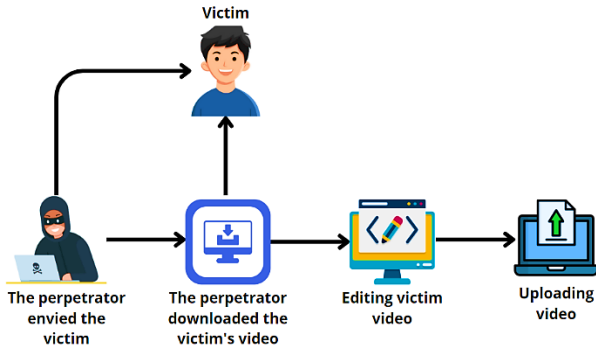


Figure 2. Pre-Incident Hoax

3.2.2 Incident

The incident began when the victim, an active touch user, routinely shared creative content and daily activities through his personal account. One day, the victim uploaded a video showing a pleasant vacation with his friends. However, without the victim's knowledge, one of the perpetrators, who was jealous and wanted to harm the victims, quickly captured the video. The perpetrator then creates a fake narrative and designs a new post on his own account, which attacks and poses a threat to a threat to the victim. In the post, the perpetrators spread false information that the victim was actually suffering from a mental disorder and had committed dangerous acts with the intention of jumping into the abyss. This post was accompanied by misleading and slanderous comments from the victims, which spread quickly on the platform. The victim, who soon learned about the post, felt very disturbed and felt that his reputation was threatened. Feeling unable to tolerate the act anymore, the victim decided to take legal action. With the help of a lawyer who is an expert in digital law, victims take steps to identify the perpetrators and bring this case to the realm of law as a crime in the social world, as show in Figure 3.

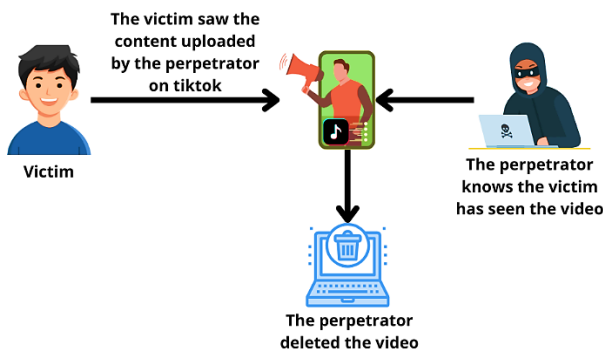


Figure 3. Case Incident Hoax

3.2.3 Post-Incident

The authority or investigators in charge of the cybercrime department directly acquire data from the laptop used by the suspect. By implementing forensic procedures with the National Institute of Standards and Technology approach, these data are used to secure the necessary digital evidence. Next, forensic analysis is done on the data. Suspect activity on the reconstructed tap platform, including login, video uploading,

and deletion of content. Relevant digital evidence is collected and analyzed to support further investigations. Once the analysis is complete, the data on the laptop is restored to its original condition. The forensic team prepared forensic reports detailing findings, analyses, and steps taken during the incident. This report is submitted to the law enforcement authorities, who will take further steps in the investigation and prosecution of the suspect.

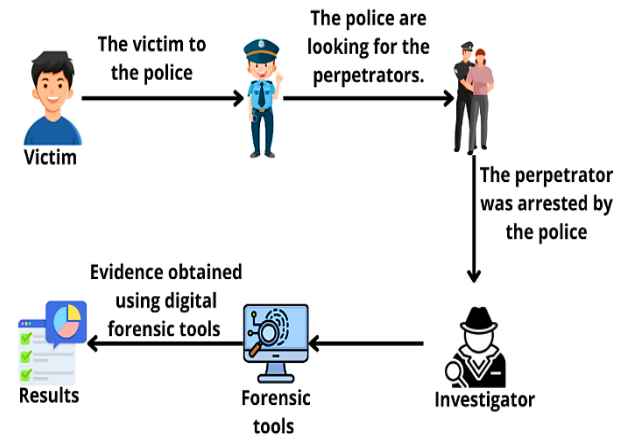


Figure 4. Post-Incident Hoax

3.3 Research Process Flow

The process of research is a phase in the process of digital forensic investigation, often known as forensic imaging. Awareness of the research process, then at this stage of data collection, make an acquisition illustration where the files that have been completed for the research will be collected in full. Can be seen in Figure 5.

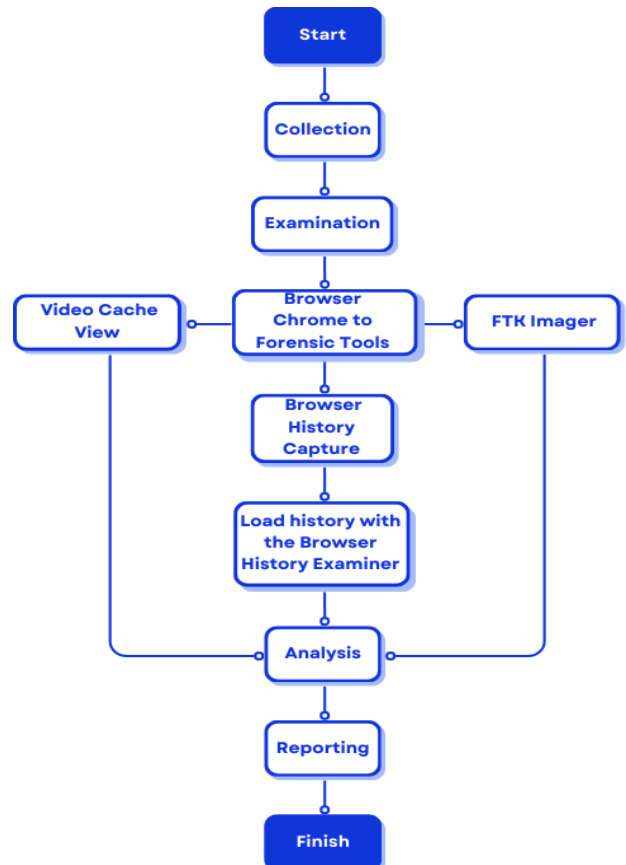


Figure 5. Stage of obtaining evidence

Figure 5. The research that begins after this will go into data collection, data inspection, which includes detection with FTK Imager, Video Cache View, Browser History Capture, Browsing History Examiner, Result Analysis and Result Record, and finally, completion.

4. RESULT AND DISCUSSION

This chapter deals with the research process that is done so that the results of this research process are obtained using the NIST method. Forensics uses a simulation of a post containing lies against others. This research is an application of the NIST method to the Web Token application that runs on the Chrome browser. This research can provide some information in the form of text, photos, and videos that can be used as digital evidence.

4.1 Collection

Collecting is the process of collecting evidence that presumably contains electronic evidence that can be used as a tool of evidence in legal proceedings. This stage is carried out by investigators to find, collect, and process documentation of evidence that exists at the scene of the case. The evidence used in this scenario is a laptop used by the suspect. In Table 1 below, there is the following evidence :

Table 1. Unit Details



No	Evidence Name	Image	Information
1	The Perpetrator's Laptop		The Acer AN515-56 was found in good condition and connected to the internet at the crime scene.
2	The Perpetrator's Charger		Acer AN515-56 laptop charger model ADP-135NB B, input 100-240V - 1.9A, output 19.5V = 6.92A, 135.0W

Table 1. documentation of evidence with specifications obtained from the scene of the case is an ACER laptop with type Nitro AN515-56 with Intel Core i5 (11300H 3.10GHz 3.11GHz) and RAM 8GB DDR4 as well as 512GB SSD storage with an OS Windows 10 found with condition on and mass connected to the internet.

4.2 Examination

This stage is a major step in the investigation to acquire evidence data from a suspect's laptop.

4.2.1 FTK Imager

FTK Imager is a review and imaging tool that is used to check files, folders on the hard disk location, CD/DVD, and network drives so that it can find digital evidence quickly, FTK Imager can view and restore files that have been deleted from the recycle bin, but have not been hit on the drive[21]. When processing data collection from RAM or capturing memory can use a forensic tool like FTK Imager.

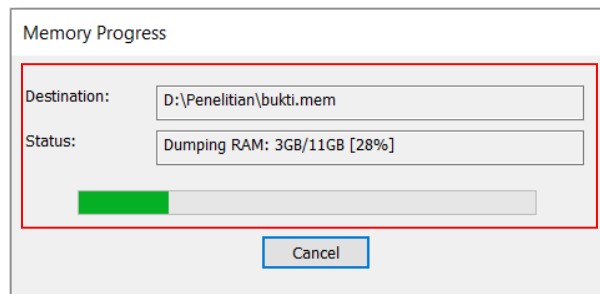


Figure 6. Memory progress

Figure 6. Data collection by capturing memory. The way to capture is by selecting the file menu and clicking on the memory capture feature. The result will be saved with the extension mem.

4.2.2 Browser History Capturer

This tool stores or collects information about online browsing history on a computer or other device[22]. The data that can be obtained from the acquisition of the browser is, among other things, history, cache, and archived history.

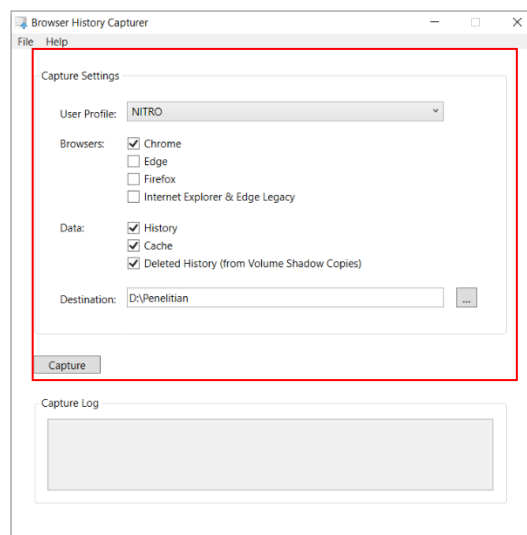


Figure 7. Acquisition Browser History Capturer

Figure 7. This application has the advantage of not having to be installed, so data collection is faster. But unfortunately, it can only be used in some browsers, such as Firefox, Chrome, and Internet Explorer and Edge. Files to be analyzed by the Browser History Examiner include Bookmarks, Cookies, Current Session, History, Last Sessions, Login Data, Preferences, Top Site, and Web Data.

4.2.3 Video Cache View

Video Cache Viewer is a tool used to retrieve video from browser applications such as Firefox, Opera, and Chrome. The acquisition process involves the phased extraction of video files from the video cache in the browser. All cache from the browser that is a browser will automatically be read by this tool. In Figure 8.

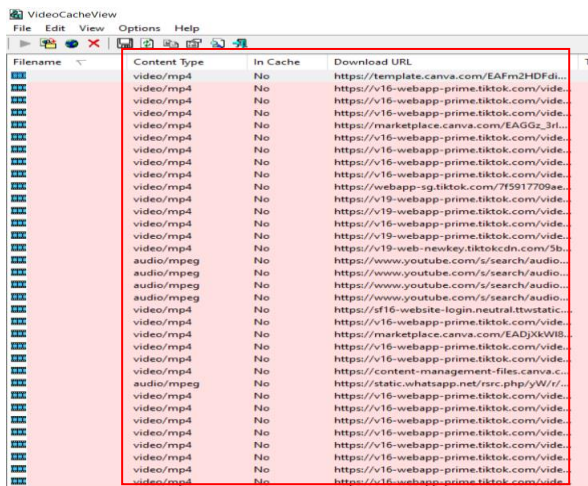


Figure 8. Acquisition Video Cache View

Figure 8. The display, when the tool is opened, will immediately perform the process of data acquisition on all the browsers that are present on the suspect laptop, according to the type mentioned earlier. At the time the tool has finished making the acquisition, all the results of the video obtained from various sources will be visible.

4.3 Analysis

The phase of analysis is the phase aimed at finding and removing evidence of a hoax carried out by the perpetrator from evidence that has passed the process of examination. [23]. The results that have been obtained will later be entered into a table to show a comparison of the results of several tools used. This analysis uses some tools used by researchers, such as:

4.3.1 FTK Imager

The evidence obtained during the next stage of the examination will be analyzed to find digital evidence or data that could be a clue. The FTK Imager tool will be used to analyze the results of the previous examination performed using the FTK Imager tool.

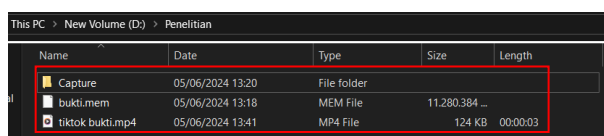


Figure 9. FTK Imager acquisition results

Figure 9. The acquisition file will then be analyzed. The process of collecting data or digital evidence will also be done with the features of the same tool for collecting evidence, as shown in Figure 10.

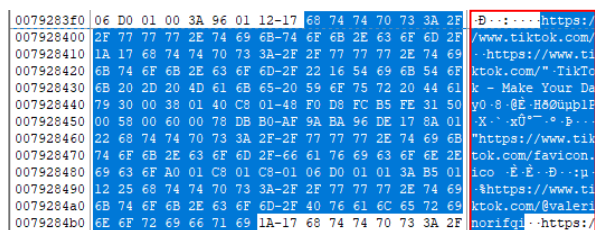


Figure 10. Keyword TikTok

Figure 10. is the result of the first search with the keyword "TikTok." The result is a login link in the TikTok with a username. The URL, https://www.tiktok.com/@valerinorifqi,

is the URL to the TikTok user profile with the username valerinorifqi.

4.3.2 Browser History Examiner

Opens the search history capture results on a web browser using the tool Browser History Examiner. The browser history examiner will display graphs of user search activity, there are filters to find more relevant data faster based on keywords and time/date ranges, and it can analyze and extract various types of data, such as previously visited websites, cookies, cache files, and download items. The browser history examiner will show details of data taken from the browser, such as access date and time data, url, email, browser used from the scanning history, loaded images, and previously loaded pages[24]. Browser History Examiner analyzes web history for Chrome, Firefox, and Internet Explorer web browsers on Windows platforms. With these features, users can easily navigate and filter data based on specific keywords or time frames, enabling faster and more accurate analysis.

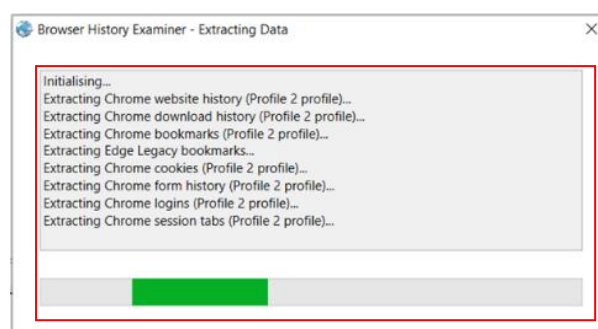


Figure 11. Extracting data

Figure 11. Extracting data capture from the capture results of the web browser browsing history. The Browser History Examiner will extract all the data contained in the "Capture" folder.

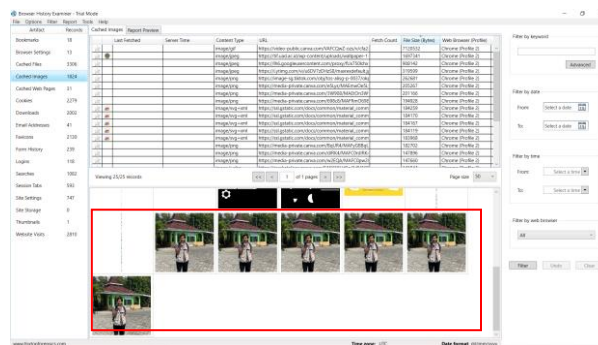


Figure 12. The perpetrator's profile photo

Figure 12. shows an image that was uploaded when the perpetrator accessed the tap. Image cache contains information about the type of content, URL, file size, and web browser used. In the image cache was found a photo of the perpetrator's profile on his ticking account.

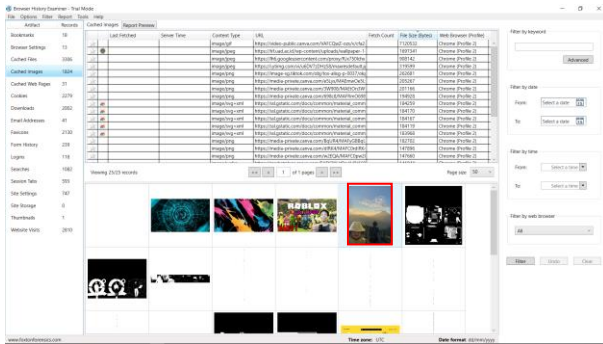


Figure 13. Perpetrator thumbnail

Figure 13. The result of Cached Image with the same parameters as before shows a thumbnail of the uploaded video content. The photo is from TikTok, which can be viewed from the URL of each photo. This thumbnail provides a visual overview of the content of the uploaded video, showing key elements or interesting moments that can attract the audience's attention. Through the listed URLs, you can directly access the original source of the photo on the TikTok platform, ensuring the authenticity and relevance of the content.

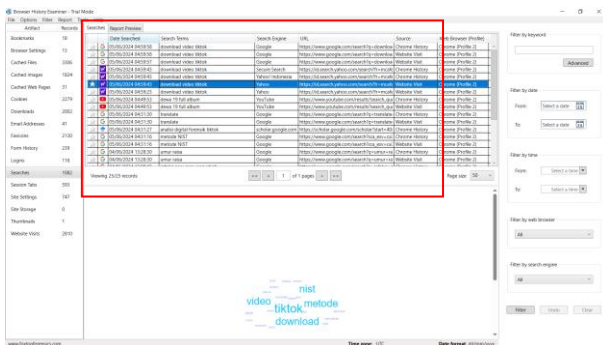


Figure 14. Perpetrator searches

Figure 14. is a search evidence that displays searched data, search terms, search engines, URLs, sources, and web browsers.

4.3.3 Video Cache View

Video cache viewer is a tool that collects stored videos from videos that are played in a browser. It is a video that can be stored based on its respective source. When the video can be acquired, it is saved to the storage and then opened manually one at a time using the video player application[25].



Figure 15. Extract from Video Cache View

Figure 15. It is seen that the video that has been extracted can be played like a regular video file. Video extracted from this cache can provide important information about the suspects' activity on the tap platform. Successfully extracted video evidence can be analyzed to understand the context and chronology of the event, as well as to identify the actions

carried out by the suspect in connection with the spread of hoax content in the tap.

4.4 Reporting

In this reporting process, the tools used for forensics will also be used to see the results and comparisons of each tool used. As for the information from the device in this study, it's a Windows 10-based laptop with details in Table 2.

Table 2. Evidence Specifications

Merk	Acer Nitro 5 AN515-56 11th Gen
Processor	Intel(R) Core(TM) i5-11300H @ 3.10GHz 3.11 GHz
Graphics	Inter(R) Iris(R) Xe Graphics & NVIDIA GeForce GT 1650
Memory	8GB DDR4
Monitor	15.6" FHD (1920 x 1080) LED IPS 144 hz

By following some inspection procedures, the evidence was analyzed with a few tools with their own functions and features, from the analysis of social media to the web. Then the results focused on some things related to the suspects and the web and social media. For more clarity, see Table 3.

Table 3. Results of digital forensic tools

No	Digital Evidence	Forensic Tools		
		FTK Imager	Browser History Examiner	Video Cache View
1	Image/Thumbnail	0	2	0
2	Video	0	0	1
3	Caption	1	0	0
4	Username	1	1	0
5	Link	1	1	1

Table 3. is the result of the discovery of evidence on a web tap site running on the Chrome web browser. On the tool, FTK Imager managed to obtain proof in the form of a username and text from the post headlines uploaded by the suspect. The username of the suspect is @valerinorifqi. The result obtained from the Video Vache Viewer is just a link - link from the video that is on the social media tap, for the video is successfully acquired because the video from the Web tap can be stored in the browser cache.

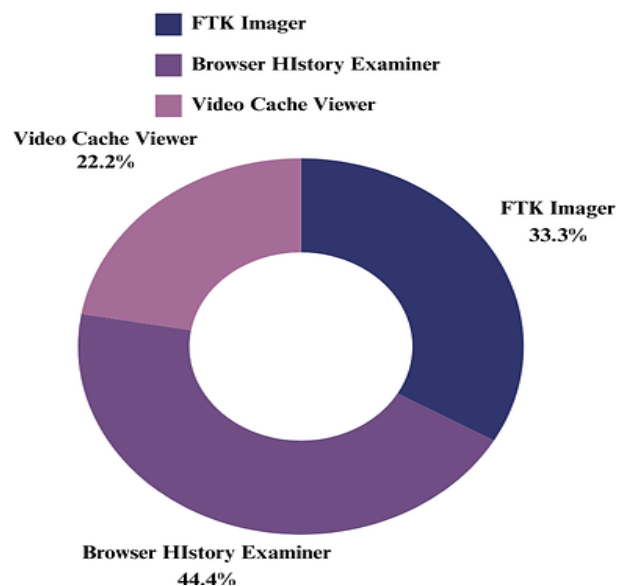


Figure 16. Presentation number of findings tools

Figure 16. shows a presentation of the number of findings on the three data collection tools, namely FTK Imager, Browser History Examiner, and Video Cache Viewer. From the presentation, you can see significant comparisons between the three in the process of data collection, such as captions, images, videos, files, and so on. FTK Imager has a total of 33.3% of presentations, with data obtained from 1 caption, 1 username, and 1 link. Browser History Examiner has the largest number of presentations with 44.4%, collecting 2 photos (1 profile photo and 1 video thumbnail), 1 user name, and one link. Meanwhile, Video Cache Viewer has 22.2% of the total presentations from 1 video and 1 hyperlink.

5. CONCLUSION

The methods of the National Institute of Standards and Technology can be used in the forensic process of Web TikTok to obtain digital evidence of a hoax case through four stages of collection, inspection, analysis, and reporting. Based on the test results, the NIST method provides significant accuracy and produces valid and reliable data. The results obtained in this study are forensic evidence collected with the capture ram and cache stages using a number of tools that support the data collection process, such as the tools used in this research, such as FTK Imager, Browser History Examiner, Browser History Capture, and Video Cache View. Based on the tools used in this investigation, 90% of the evidence was obtained and 10% failed, namely the suspect's password. For the future, it is necessary to consider method development, implementation on other platforms, and collaboration with industry. Thus, this research makes an important contribution to the field of digital forensics.

6. REFERENCES

- [1] P. Sitompul, D. Mahmudah, and M. P. Damanik, "Using Social Media and Meeting Employment Information Needs in the Young Workforce in the Time of the COVID-19 Pandemic," *Journal of Communication and Media Studies*, vol. 25, no. 2, p. 203, Dec. 2021, doi: 10.31445/jskm.2021.4399.
- [2] M. S. Fajar and M. F. Nur, "Review Tools Web Browser Forensics to Support Digital Evidence Search," *JEPIN (Journal of Educational and Informatics Research)*, vol. 5, pp. 67–73, Apr. 2019.
- [3] N. Istiani, "Fikih Social Media in Indonesia (Study Analysis of the Philosophy of Islamic Law in the Ethical Code of Netism Muhammadiyah)," vol. 6, no. 2, pp. 202–225, 2020.
- [4] D. Yuliana, T. Yuniati, B. P. Zen, and I. A. Kresna, "Analysis of Digital Evidence of Cyberbullying on Social Media Using the Method of the National Institute of Standards and Technology (NIST) 800-101," *LEDGER : Journal Informatic and Information Technology*, vol. 1, no. 3, pp. 113–123, Aug. 2022.
- [5] P. Syafrin Azwir and Nurbaiti, "Analysis of the Impact of Social Media as Media Promotion by Swara Prima Media, Rantau Rapat," *Journal of Computer Science, Economics, and Management (JIKEM)*, vol. 2, no. 2, pp. 3233-3243, 2022.
- [6] M. Romi, "DFXML Analysis for Supporting Identification and Management of Digital Artifacts on TikTok Applications," 2022.
- [7] A. Andika Putra, P. Maharani, and L. Indra Kesuma, "The Intelligent Use of Social Media in Countering Fake News (HOAX) in the University of Sjakhyakirti," *Journal of Dedication to the Society of Technological Innovation*, vol. 1, no. 1, pp. 13–17, 2023.
- [8] I. Wahyudi, A. Muntasa, M. Yusuf, and A. Hamzah, "Developing and Testing the Authenticity of Digital Evidence on Cybercrime by Digital Forensic Research Workshop," *Journal of Information Technology and Management (JATIM)*, vol. 2, no. 2, pp. 120–127, 2021.
- [9] A. Nofiyani and Mushlihudin, "Forensic Analysis of Web Phishing Using the Methods of the National Institute of Standards and Technology (NIST)," *Journal of Bachelor of Science in Computer Engineering*, vol. 8, no. 2, pp. 11–23, 2020.
- [10] F. Natsir, "Forensic Analysis of Content and Timestamps on TikTok Applications," *STRING (Technology Research and Innovation Writing Unit)*, vol. 6, pp. 203–209, Dec. 2021.
- [11] R. Rahmansyah, Carudin, and A. Ali Ridha, "The Comparison of Digital Evidence Investigations on Facebook and Instagram Applications with Nist Methods," *CyberSecurity and Digital Forensics*, vol. 4, no. 1, pp. 49–57, 2021.
- [12] Soni, R. Hayami, and Muhammad Hamadi, "Acquisition of Digital Evidence on Michat Applications on Smartphones Using the Methods of the National Institute of Standards and Technology (NIST)," *Journal CoSciTech (Computer Science and Information Technology)*, vol. 3, no. 3, pp. 283–290, Dec. 2022.
- [13] T. Pandela and I. Riadi, "Browser Forensics on Web-based TikTok Applications," *Int J Comput Appl*, vol. 175, no. 34, Dec. 2020, doi: 10.5120/ijca2020920897
- [14] R. Ayatulloh Khomeini Noor, R. Umar, and A. Yudhana, "Facebook Lite Social Media Analysis with Forensic Tools using NIST Methods," *TECHNO*, vol. 21, no. 2, pp. 125–130, 2020.
- [15] M. Prasetio, U. A. Dahlan, and I. Riadi, "Investigation Telegram based-on Web using National Institute of Standards and Technology Method," *Int J Comput Appl*, vol. 183, no. 50, pp. 975–8887, 2022.
- [16] C. Kus Herawati and I. Riadi, "Forensic Browser on Facebook Services using National Institute of Standards Technology Method," *Int J Comput Appl*, doi: 10.5120/ijca2021921683, 2021.
- [17] M. Na'im, A. Jum'ah, H. Wijaya, and R. R. Ismail, "Implementation of Digital Forensic Process Model (DFD) for Social Media Investigation with Hunchly Tools," 2023.
- [18] S. K. Saad and A. Fadlil, "Forensic Analysis of Dropbox Applications on Android Using the Nist Method," vol. 4, no. 1 2020.
- [19] I. Riadi, A. Fadlil, and M. I. Aulia, "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)," *JURNAL RESTI*, vol. 1, no. 3, pp. 820–828, 2020.
- [20] M. Rafika, D. Qibriya, A. Ambarwati, and K. E. Susilo, "Digital Forensic Analysis of Instant Messaging Applications in Android-based Smartphones for Digital Evidence," *Journal of Information Technology*, vol. 5, no. 2, pp. 114–121, 2021.

- [21] Exterro, “FTK Imager.” [Online]. Available: <https://www.exterro.com/ftk-imager> vol. 183, no. 29, pp. 975–8887, 10.5120/ijca2021921680, 2021.
- [22] H. A. Timor, U. A. Dahlan, and I. Riadi, “Web Forensics on TikTok Services using National Institute of Standards and Technology Method,” *Int J Comput Appl*, vol. 185, no. 36, pp. 975–8887, doi:10.5120/ijca2023923157, 2023.
- [23] R. Adijisman, U. A. Dahlan, and I. Riadi, “Mobile Forensic on WhatsAppServices using National Institute of Standards and Technology Method,” *Int J Comput Appl*, vol. 183, no. 29, pp. 975–8887, 10.5120/ijca2021921680, 2021.
- [24] K. V. P. S. G. Majeti, Y. V. L. S. Sundar, S. S. Ulichi, S. N. Mohanty, and S. SV, “Digital Forensic Advanced Evidence Collection and Analysis of Web Browser Activity,” *EAI Endorsed Transactions on Scalable Information Systems*, vol. 10, no. 5, pp. 1–8, 2023, doi:10.4108/eetsis.3357.
- [25] Nirsoft, “VideoCacheView.” [Online]. Available: https://www.nirsoft.net/utills/video_cache_view.html