Web Forensics on Tiktok Services using National Institute of Standards and Technology Method

Herdin Asmara Timor
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
Users use tiktok to share photos and videos, comment, and also features to like a video that is uploaded. More and more people use tiktok, but more and more irresponsible users whose accounts are used to torture others online. As a result, cyberbullying is still rampant on tiktok the investigation process in cyberbullying situations and to find the necessary seven digital evidence. The initial stage is the collection stage, where evidence such as files, documents, data, and physical evidence is collected. The examination stage is the stage of examining the data obtained from the previous location. The analysis stage is the stage of reviewing the data obtained from the last step the analysis stage, where the examination results are analyzed in depth. Finally, the reporting stage is the preparation of a report containing the results of the analysis that has been carried out. Tools FTK imager digital evidence of captions usernames of tiktok actors. Tools video cache view digital evidence of deleted video posts, content, and videos that have become images. tools browser history capturer digital evidence in the form of date, time of occurrence, and web browser. Tools browsing history view digital proof of activity history, namely date and time, caption uploads and web types, and user names. On tiktok, every action leaves a digital trail. Investigators can follow and collect evidence of various activities, such as captions, images, and posted videos.

Keywords
Bullying, Forensic Digital, National Institute of Standards and Technology, TikTok

1. INTRODUCTION
The development of social media is so rapid from year to year. Its users use tiktok to share photos and videos, comment and also features to like an uploaded video. Social media is easily understood as a digital platform that offers users tools to engage in social activities while producing content [1]. Social media platforms allow users to communicate, connect, and share information and content in images and videos of varying lengths. All users will have access to uploaded content for a full day [2]. The evolution of social media is a component of the development of the Internet. Social media has grown rapidly and rapidly due to its presence from a few decades ago. This allows anyone with access to an internet connection to disseminate information or content at any time and from any location. Almost everyone who Uses social media will be able to use and enjoy tiktok by 2022. tiktok users, especially in indonesia, are claimed to exceed 99.1 million users in April 2022 [3]. A total of 136.4 million users makes indonesia the second largest user after the United States. The average age of tiktok users in indonesia is 18 years and above, 66 percent female and 34 percent male. Undoubtedly, marketers can use these statistics to advance and strengthen their brands. One of the most widely used social media platforms, tiktok, offers a selection of videos with a maximum duration of three minutes [4]. According to data from the website data reportal and poll findings from cocial in 2021, there are 170 million active social media users in indonesia, 61.8% of the country's total population. Compared to 2020, this may increase by 10 million people or 6.3% [5]. Every year, more and more people use tiktok, but there are more and more irresponsible users whose accounts are used to torment others online. As a result, cyberbullying is still rampant on tiktok. Unfortunately, there has been a lot of cyberbullying and fraud on tiktok over the past three years [6]. Cyberbullying is carried out through intermediaries such as messages containing insulting or offensive sentences, such as abnormal, cowardly, strange, effeminate, stupid, terrible, crazy, ugly, dangerous, and hypocritical [7]. NIST approach, developed by the national institute of standards and technology, is used in this study to examine the results of digital forensics or investigation processes in cyberbullying situations and to find the necessary digital evidence [8]. Collection, examination, analysis, and reporting are the steps used to complete the analysis. NIST technique is used because it offers a systematic and structured analysis approach, making it easier to get the data or evidence need [9]. In obtaining digital evidence, this research will analyze the findings of investigations conducted on the evidence collected, emphasizing the issue of crime on the tiktok web [10]. This project aims to produce digital proof through results from digital evidence analysis, which can support evidence from criminal cases, including cyberbullying, in court [11]. Tools such as FTK Imager and other forensic tools are expected to facilitate and accelerate the discovery of digital evidence in this research [12]. The goal is to inform readers about using the tiktok web to find digital evidence.

2. LITERATURE STUDY
2.1 Digital Forensics
Digital forensics, or forensic science used to investigate a case in searching for forensic information and finding content on digital devices, is needed to know what cybercrime is. Digital forensic science courses require expertise in various fields, including legal studies [13]. According to the type of digital device used, the technical part of the investigation is divided into several sub branches, consisting of forensic data analysis, computer forensics, network forensics, and mobile device forensics. Current forensic procedures include seizure, forensic imaging, examination of digital materials, and report writing based on evidence collected from the results of the forensic process Tracking illicit activity in the cyber sphere is also strongly tied to digital forensics. Investigations can track out the perpetrators of cybercrimes with the aid of experts in digital forensics, gather digital evidence, and bring the necessary legal cases [13].

2.2 National Institute of Standard Technology

Forensic analysis procedures are performed using the national institute of standards and technology. Cybercrime cases are solved by the NIST method in four stages: collection, examination, analysis, and reporting are the first three stages. The following procedure outlines the stages of research so that can be carried out systematically and applied to solve existing problems. [14].

2.3 Chain Of Custody

Chain of Custody (CoC), or the process of recording evidence, guarantees the evidence's validity level. Electronic forensics of chain of custody requires caution due to the irregular nature of digital data. For example, different timestamps (modified-created access) in log files might contaminate the digital evidence, rendering it unusable as evidence in court. When a computer is acquired, the initial handling largely depends on whether the computer is turned on or off [15].

2.4 Pre Acquisition

Pre-Acquisition is everything to prepare for searching, identifying, and acquiring evidence in handling a case, such as equipment, computer hardware, and software that will be used for acquisition [16].

2.5 Core Acquisition

Core Acquisition is the core of acquisition where the digital forensic process runs when preparations for purchase have been fulfilled, and the forensic expert begins to carry out his duties according to applicable procedures such as collection, examination, analysis, and reporting [17].

2.6 Acquisition

The techniques used to conduct the acquisition should be comprehensive and competent in selecting the most appropriate means based on conditions, cost, and time and document the choice to use specific proper methods and instruments at the time of acquisition. The techniques should be applicable, repeatable with identical results, and able to demonstrate that the copy findings are the same as the original evidence [18].

2.7 Digital Evidence

Browser History Capturer lets easily capture web browser history from windows computers. The tool can be run from a USB dongle or via a remote desktop connection to record history from chrome, edge, firefox, and internet explorer web browsers. The history file is copied to the selected destination in its original format, allowing it to be analyzed later using the tool of choice [19].

2.8 Cyberbullying

Cyberbullying is a criminal practice that utilizes a computer or computer network as a tool, target, or setting for crime. Fraud, including online auctions, check cashing, credit cards (carding), guardianship, identity theft, and pornography, in this case, users, etc, are examples. Cyberbullying is illegal and harmful, and therefore, it is important to use digital forensic tools to uncover and combat these acts of cyberbullying. [20].

2.9 Data Recovery

Data Recovery is restoring a system or data to its original, undamaged state after it has been damaged, failed, or inaccessible [21].

2.10 Tiktok

Figure 1 tiktok is a social network offering unique and exciting resources for app users. It is simple to create entertaining short videos that will interest a large audience of the material made. In september 2016, tiktok, the introduction of the chinese social network and music video platform. The app is used to produce short movies with background music that are well liked by both adults and children [22].

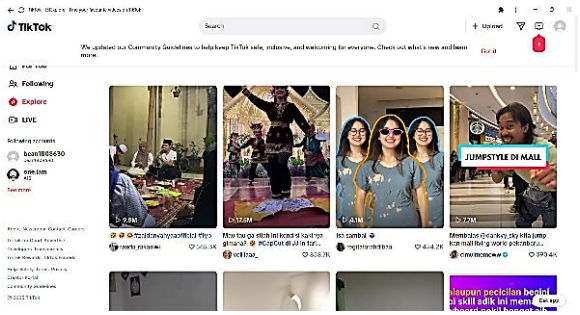

Figure 1. Tiktok View

2.11 FTK Imager

Access Data developed a digital forensic acquisition tool, FTK Imager. Although FTK Imager is free, its features and capabilities are on par with expensive paid applications. This makes it a popular choice among digital forensics professionals and cybercrime investigators, being able to access advanced tools at no extra cost. FTK Imager has several features that support the process of data acquisition from various devices, making it easier for investigators to collect digital evidence for investigative purposes [23].

2.12 Browsing History View

Browsing History View is a digital forensics tool that allows investigators to quickly evaluate and retrieve data about all websites that have been visited. Each entry in the table contains several important details, such as the title of the web page, the entire website URL, the date and time of the visit, down to the minute, and even information on how often the user visited the website. The tool displays the data in an easy-to-read table in the context of digital forensics. This tool is helpful because it allows investigators to carefully and deeply examine the traces of a user's online behavior to recognize specific web pages [24].

2.13 Browser History Capturer

Figure 2 an essential tool in the field of digital forensics is browser history capture. This tool stores or collects information about the online browsing history on a computer or other device. Using digital forensics tools, investigators can follow the trail of a user's online activities, including websites visited, pages viewed, date and time of access, and other essential facts for investigating cyberbullying and other online crimes. These tools allow forensic investigators to collect strong digital evidence during investigations and law enforcement activities. In addition, browser history recorders are essential for recovering data that the perpetrator may have destroyed. It can be vital evidence to identify crimes and take fair legal action.

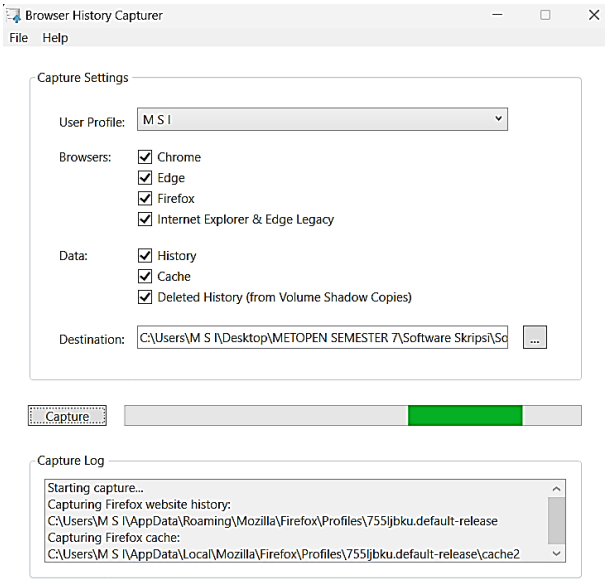

Figure 2. Browser History Capturer View

2.14 Video Cache View

Figure 3 tools that work by retrieving data from the browser's cache files and identifying video files based on the file extension used by the website [25]. Once a video file is found, users can click on it to play the video or save it into a separate file.

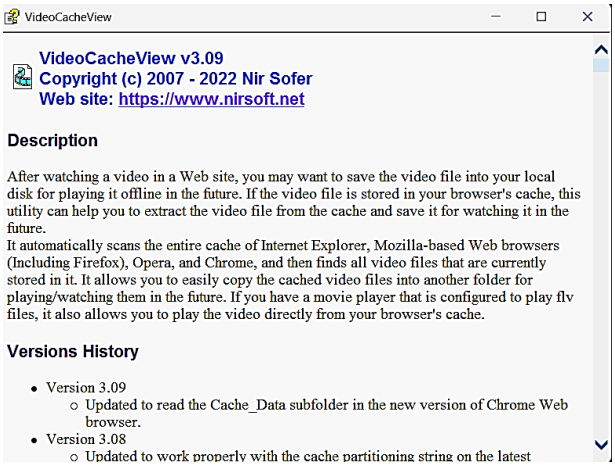

Figure 3. Video Cache View

2.15 Web Browser

The browser where tiktok Web does not use the application provided by the developer in playstore. tiktok web can be used without an application and is installed first using a web browser on a PC. A web browser is software designed to store all data users enter when using the internet, including passwords, timestamps, URL history, and search term Using tiktok web in a browser allows one to investigate and collect digital evidence related to cyberbullying on the platform. This is an essential step towards uncovering cybercrime and providing justice for victims of cyberbullying. A systematic and thorough examination of digital evidence is crucial to building a solid case against the perpetrators and ensuring they are held accountable for their actions. [26].

3. RESEARCH METHODS

This research uses the investigation process of the National Institute Of Standards And Technology digital forensic analysis step. The National Institute Of Standards And Technology step consists of 4 stages. The scheme of the four stages can be seen in Figure 4.

Figure 4. National Institute of Standards And Technology Step

Figure 4 illustrates the steps of the national institute of standards and technology step. The initial stage is the collection stage, where evidence such as files, documents, data, and physical evidence is collected. The next step is the examination stage of examining the data obtained from the previous location. After that, the analysis stage will get the results of each of the FTK imager tools, browser history capturer, browsing history view, and video cache view to get evidence of data results in the form of video photos and comments, and conversations on tiktok. The last stage is reporting [27]. At this stage, reporting will be carried out based on the results of the analysis that has been carried out.

4. RESULTS AND DISCUSSION

Figure 5, the perpetrator accesses tiktok with a chrome web browser using a laptop, then logs in to tiktok by entering their email and cellphone number, then verifies the data with the OTP code obtained on the perpetrator's cellphone after that, the perpetrator enters the OTP code into the laptop used to log in to tiktok after the computer is connected to tiktok the perpetrator creates bullying.

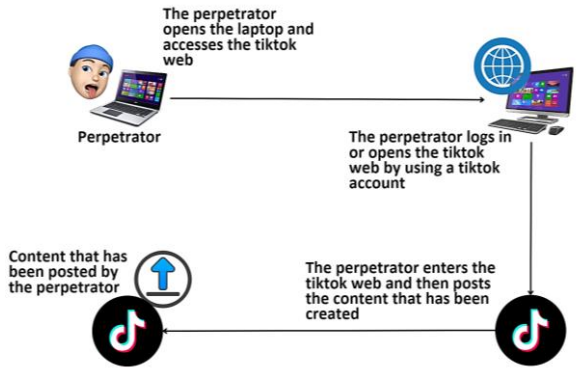

Figure 5. Pre-Incident Cyberbullying

content for the victim Figure 6 shows that the perpetrator's actions are recorded at this stage and take center stage in the investigation process. In this case simulation, the perpetrator's steps in bullying the victim on the tiktok platform have been successfully recorded and will become crucial digital evidence in the investigation. This stage plays a key role in documenting the acts of cyberbullying committed by the perpetrator. This process is essential in collecting digital evidence that will later be used in investigating this case. By recording the steps of the perpetrator, the investigating team can better understand the perpetrator's actions.

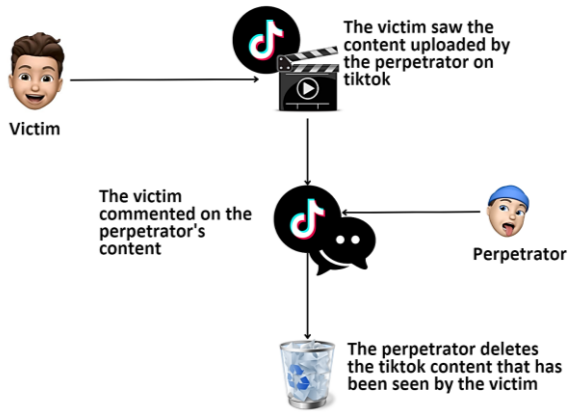

Figure 6. Case Incident Cyberbullying

Figure 6 of the incident on tiktok where the victim sees a post uploaded by the perpetrator, the victim becomes moody or insecure because the perpetrator's content contains bullying videos, so the victim feels bullied after that the victim comments on the perpetrator's content and the perpetrator deletes the content because the victim has seen the content created by the perpetrator. Also, the uploaded content has been watched a lot. The post incident stage can be seen in Figure 7.

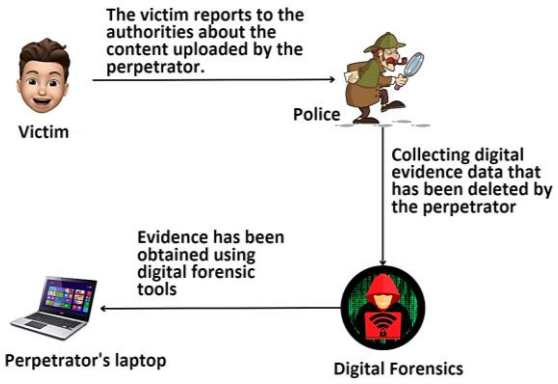

Figure 7. Post-Incident Cyberbullying

Figure 7, the victim who felt his good name was destroyed made a report to the authorities where the victim reported the content uploaded by the perpetrator. After that, the police or investigator collected digital evidence deleted by the perpetrator and then conducted digital forensics using several digital forensic tools.

4.1 Collection

The evidence collection stage is critical in the investigation process and is carried out carefully and thoroughly. This is done by preparing equipment or tools that will be used to obtain the necessary evidence. These tools include digital forensic software, specialized hardware, and various other devices needed. Details about the tools that will be used can be seen in Table 1. The evidence collection process must be carried out by applicable digital forensic standards and guidelines to ensure the integrity and validity of the evidence obtained. The stages in the National Institute Of Standards And Technology (NIST) method, namely Collection, Examination, Analysis, and Reporting, guide the collection and handling of digital evidence. This structured approach ensures that digital evidence is gathered and handled with high integrity and can be used effectively to support the law enforcement process.

Table 1. Tools and Materials

Name	Description
Laptop	Laptop media used to obtain data.
Tiktok	Tiktok object application for the forensic process
Web Browser	Web Browser application for accessing object applications
FTK Imager	FTK Imager the data obtained is evidence of captions written by the perpetrator.
Browser History Capturer	Browser History Capturer data in the form of capture logs on the available web.
Browsing Hitory View	I was browsing history view data obtained from the perpetrator's activity in the web browser and evidence of the perpetrator's bullying.
Video Cache View	Video Cache View digital evidence is obtained through videos and photos posted by the perpetrator on tiktok.

Each shows the tools investigators will prepare to investigate cyberbullying fraud cases and produce digital evidence. These tools consist of 2 types, namely hardware and software.

4.2 Examination

The examination stage is collecting, securing physical evidence, and collecting data. Physical evidence found is one laptop found in a lit state. Physical evidence can be seen in Figure 8.

Figure 8. Physical Evidence Of Laptop

Figure 8 shows the MSI laptop belonging to the perpetrator that has been found. The computer is then processed forensically by taking data which will be done through laptop capture using the browser and browser history capture tools. Stages in the RAM data retrieval process using the browser tool. The browser is used to retrieve data and information from memory.

4.3 Analysis

4.3.1 Analysis Tools FTK-Imager

Table 2, the FTK imager tool can see the results of the examination carried out using the FTK-Imager tool. The results of evidence can be found in the form of captions from the tiktok content that has been deleted, along with the username or account used by the perpetrator to enter tiktok.

Table 2. FTK Imager Tools Results

Information	Result	Description
Account username	bean1808639	Successful
Caption	You ugly, ugly person @user9563777420687	Successful

4.3.2 Analysis tools Video Cache View v3.09

Figure 9 of the video cache view v3.09 tool shows that the results of this tool display a list of all files currently stored in the cache. For each cached file, the following information is displayed: URL, content type, file size, last accessed time, expiration time, server name, server response, and more. Can easily select one or more items from the cache list, then extract the files to another folder or copy the list of URLs to the clipboard.

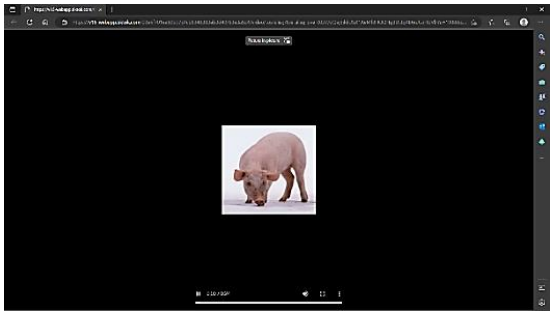

Figure 9. Video Cache View Tools Results

4.3.3 Analysis Tools Browsing History View v2.54

Figure 10 of the browsing history view tool shows the results of this tool reading the history data of different web browsers (mozilla firefox, google chrome, internet explorer, microsoft edge, opera) and displaying the browsing history of all these web browsers in one Table. The browsing history Table includes the following information: visited url, title, visit time, number of visits, web browser, and user profile. Browsing history view allows viewing the browsing history of all user profiles in a running system and getting the browsing history from an external hard drive. With this tool, users have better access to browsing history data, allowing more in depth analysis of online activities and using different web browsers.

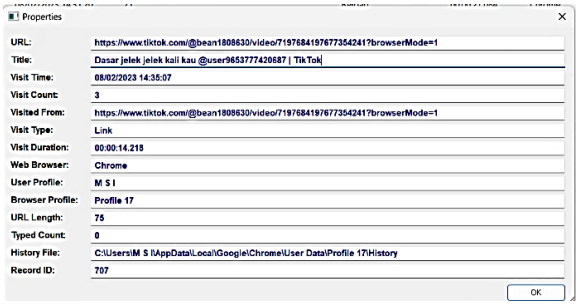

Figure 10. Browsing History View Tools Result

4.3.4 Analysis Tools Browser History Capturer v1.4.1

Figure 11, the tool can be seen recording web browser history from a Windows computer. The device can be run from a USB dongle or via a remote desktop connection to record history from Chrome, Edge, Firefox, and Internet Explorer web browsers. The history file is copied to the selected destination in its original format to be analyzed later using optional tools. Using this tool, the investigative team can collect relevant browsing history data to understand the perpetrators' cyberbullying acts in more detail and systematically with the methods used to provide digital solid evidence in this investigation for the cyberbullying case handled by the investigator.

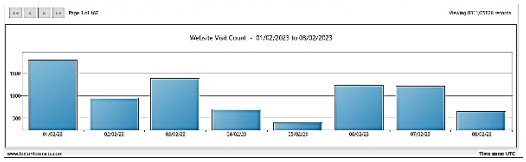

Figure 11. Browser History Capturer

4.3 Reporting

Table 3 of this reporting stage, the results of digital evidence successfully obtained from the steps using the NIST method have been carried out by the perpetrator in committing a crime on tiktok.

Table 3. Unit Details

Device Name	Processor RAM
Laptop MSI GF63	Laptop MSI GF63 Intel Core® Core™ i5-10500H @2.50GHz 8.0 GB

Table 3, the information obtained on the physical evidence found is a laptop that has been examined and analyzed to get the results of digital proof. Table 4 is the result of a report that has been found using forensic tools FTK imager, browsing history view, browser history capturer, and video cache view using the national institute of justice method of obtaining digital evidence that has been listed.

Table 4. Results of Digital Forensic Tools

Results	FTK Imager	Video Cache View	Browser History Capturer	Browsing History View
Username	✓			
Caption	✓			
Activity history			✓	✓
Caption uploads				✓
Video post		✓		
Image snippet		✓		
Type of web used				✓

Table 4 is digital evidence found from cyberbullying cases using four forensic tools. FTK imager tools can find digital proof in the form of captions of the username used by the perpetrator to enter the tiktok account. Video cache view tools find digital evidence through video posts that have deleted content and video pieces that have become images. The browser history capturer tool finds digital proof in the form of a web visit history in the form of the date and time of the incident and the web browser used. The last tool, browsing history view, finds digital evidence in the record of activity histories such as date and time, uploaded captions made, and the type of web used, username or user, and URL.

5. CONCLUSIONS

Forensic evidence is collected through various stages and tools, such as browser data capture, memory capture, browsing history view, and video cache. These tools include browser history capture, FTK imager, browsing history view, and video cache view. FTK Imager is utilized to uncover digital evidence like captions and usernames on tiktok accounts. Video Cache View helps find digital proof from deleted video posts and video fragments turned into images. Browser History Capturer reveals digital evidence in web visit history, including the date, time, and the web browser. Lastly, Browsing History View identifies digital evidence related to activity history, including date, time, caption uploads, web type, usernames, and URLs. This study employs the National Institute of Standards and Technology (NIST) method, which has proven effective in forensic processes on web-based applications, particularly tiktok, for collecting and analyzing digital evidence in cases of cyberbullying. The process encompasses four key stages: Collection, Examination, Analysis, and Reporting.

6. REFERENCES

[1] P. S. Azwir and N. Nurbaiti, "Analysis of the Effect of Social Media as a Promotional Media of PT Media Swara Prima, Rantau Rapat," JIKEM: Journal of Computer Science, Economics and Management, vol. 2, no. 2, pp. 3233-3243, 2022.

[2] M. A. Rizaty, "Indonesia's Tiktok Users are the Second Largest in the World," dataindonesia.id, 2022.

[3] D. Yuliana, T. Yuniati, and B. P. Zen, "Analysis of Digital Evidence of Cyberbullying on Social Media using the National Institute of Standard and Technology (Nist) 800-101 Method," LEDGER: Journal of Informatics and Information Technology, vol. 1, no. 3, pp. 113-123, 2022, doi: 10.20895/ledger.v1i3.812..

[4] A. Nofiyan and M. Mushlihudin, "Forensic Analysis of Web Phishing using the National Institute Of Standards And Technology (NIST) Method," JSTIE (Undergraduate Journal of Informatics Engineering) (E-Journal), vol. 8, no. 2, p. 53, 2020, doi: 10.12928/jstie.v8i2.16697.

[5] M. Riskiyadi, "Forensic Investigation of Digital Evidence in Uncovering Cybercrime," Cyber Security and Digital Forensics, vol. 3, no. 2, pp. 12-21, 2020, doi: 10.14421/csecurity.2020.3.2.2144.

[6] M. A. Aziz, I. Riadi, and R. Umar, "Web-based Line Messenger Forensic Analysis using the National Institute Of Justice (NIJ) Framework," National Seminar Informatics UPN "Veteran" Yogyakarta, vol. 2018, no. November, pp. 51-57, 2018.

[7] I. Riadi, R. Umar, and M. A. Aziz, "Instant Messaging Service Web Forensics using the Association of Chief Police Officers (ACPO) Method," Mobile and Forensics, vol. 1, no. 1, p. 30, 2019, doi: 10.12928/mf.v1i1.705.

[8] S. D. Utami, C. Carudin, and A. A. Ridha, "Live Forensic Analysis on Whatsapp Web to Prove Electronic Transaction Fraud Cases," Cyber Security and Digital Forensics, vol. 4, no. 1, pp. 24-32, 2021, doi: 10.14421/csecurity.2021.4.1.2416.

[9] T. Pandela and I. Riadi, "Browser Forensics on Web-based Tiktok Applications," Int J Comput Appl, vol. 175, no. 34, pp. 47-52, 2020, doi: 10.5120/ijca2020920897..

[10] T. Irawan and I. Riadi, "Mobile Forensic Signal Instant Messenger Services in Case of Web Phishing using National Institute of Standards and Technology Method," Int J Comput Appl, vol. 184, no. 32, pp. 30-40, 2022, doi: 10.5120/ijca2022922394.

[11] I. Gilbert Rian Mailangkay, E. Zakharia, A. Hadi, T. Informatika, and S. Palangka Raya, "Comparative Analysis of Tiktok Lite Digital Evidence using the National Institute of Justice Method," Journal of Computer Science & Informatics (J-SAKTI, vol. 6, no. 2, pp. 661-670, 2022.

[12] R. N. Dasmen and F. Kurniawan, "Digital Forensics of Deleted Cyber Crime Evidence on Social Media Instant MessagesDigital Forensics of Deleted Cyber Crime Evidence on Social Media Instant Messages," Techno.Com, vol. 20, no. 4, pp. 527-539, 2021, doi: 10.33633/tc.v20i4.5170.

[13] A. Andria, "Digital Forensics of Web-Based Information Systems," JAMI: Journal of Indonesian Young Experts, vol. 2, no. 2, pp. 33-44, 2021, doi: 10.46510/Jami.v2i2.73.

[14] M. Fitriana, K. A. AR, and J. M. Marsya, "Application of the National Institute of Standards and Technology (Nist) Method in Digital Forensic Analysis for Handling Cyber Crime," Cyberspace: Journal of Information Technology Education, vol. 4, no. 1, p. 29, 2020, doi: 10.22373/cj.v4i1.7241.

[15] T. F. Efendi, R. Rahmadi, and Y. Prayudi, "System Design for Physical Evidence Management and Chain of Custody (CoC) in Digital Forensics Laboratory Storage," Journal of Informatics Technology and Management, vol. 6, no. 2, pp. 53-63, 2020, doi: 10.26905/jtmi.v6i2.4177.

[16] P. D. Wibowo, Satriyo; Nugroho, "CoC, Key to Digital Evidence Accepted by the Court," detik.com, 2018.

[17] P. A. Mahatmavidya, "Understanding the Meaning, Purpose, Types as well as Examples of Acquisitions," mekari.com, 2022.

[18] Muhammad Abdul Aziz, Wicaksono Yuli Sulistyo, and Sri Rahayu Astari3, "Comparative Anti Forensics of Web-Based Instant Messaging Applications using the Association of Chief Police Officers (ACPO) Method," JURISTIK (Journal of Information Technology and Computer Research), vol. 1, no. 01, pp. 8-15, 2021, doi: 10.53863/juristic.v1i01.341.

[19] I. Wahyudi, A. Muntasa, M. Yusuf, and A. Hamzah, "Revealing and Testing the Authenticity of Digital Evidence in Cybercrime Crimes with the Digital Forensic Research Workshop Method," Journal of Information Technology Applications and Management (JATIM), vol. 2, no. 2, pp. 120-127, 2021, doi: 10.31102/jatim.v2i2.1068.

[20] P. Widiandana, Imam Riadi, and Sunardi, "Implementation of the Jaccard Method on WhatsApp

Messenger Cyberbullying Investigation Analysis using the National Institute of Standards and Technology Framework," Journal of RESTI (Systems Engineering and Information Technology), vol. 4, no. 6, 2020, doi: 10.29207/resti.v4i6.2635.

[21] M. S. Simanjuntak and J. Panjaitan, "Analysis of Data Recovery using Software," Journal of Universal Computer Informatics Engineering, vol. 1, no. 1, pp. 26-32, 2021.

[22] F. Natsir, "Forensic Analysis of Content and Timestamp on Tiktok Application," STRING (Unit Tulisan Riset dan Inovasi Teknologi), vol. 6, no. 2, p. 203, 2021, doi: 10.30998/string.v6i2.11454.

[23] M. F. Sidiq and M. N. Faiz, "Review of Web Browser Forensics Tools to Support Digital Evidence Search," Journal of Informatics Education and Research (JEPIN), vol. 5, no. 1, p. 67, 2019, doi: 10.26418/jp.v5i1.31430.

[24] B. Actoriano, U. A. Dahlan, I. Riadi, and U. A. Dahlan, "Forensic Investigation on Whatsapp Web using the Integrated Digital Forensic Investigation Framework Version 2," International Journal of Cyber Security and Digital Forensics (IJCSDF), no. September, 2018.

[25] E. Hakimah, K. Dewi, A. Suharso, and C. Rozikin, "Cosine Similarity Implementation In Investigation Analysis," CyberSecurity and Digital Forensics, vol. 5, no. 1, pp. 12-22, 2022.

[26] T. Rochmadi, "Live Forensics for Anti Forensic Analysis on Web Browser Case Study Browzar," Indonesian Journal of Business Intelligence (IJUBI), vol. 1, no. 1, p. 32, 2019, doi: 10.21927/ijubi.v1i1.878.

[27] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Digital Forensics Design on Twitter Application using Live Forensics Method," National Seminar on Informatics 2008 (semnasIF 2008), vol. 2018, no. November, pp. 86-91, 2018.