

Forensic Analysis of Website in Cyberbullying Cases on Instagram using National Institute of Justice Method

Fauza Radhiya Adriani
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 has facilitated communication through social media such as Instagram, but also raises the risk of cybercrime such as cyberbullying. This study aims to identify and analyze digital evidence from cyberbullying cases on Instagram Web using the National Institute of Justice (NIJ) method, which consists of five stages: preparation, collection, examination, analysis, and reporting. The investigation process utilizes digital forensic tools such as FTK Imager, Browser History Examiner, and Image Cache Viewer. The results show the discovery of comments, deleted messages, access history, and edited images as relevant evidence. The NIJ method has proven effective in solving cases, and this study is expected to serve as a reference in the application of digital forensics to similar cases.

Keywords

Cyberbullying, Instagram, Digital Evidence, National Institute of Justice.

1. INTRODUCTION

With the development of information technology, people are now increasingly familiar with social media as a means of communication and dissemination of information. Social media allows users to interact in real-time through internet-connected devices. One of the most popular and widely used platforms is Instagram. This application allows users to share photos, videos, and direct messages with other users. Instagram is also equipped with various features such as photo filters, location tagging, and the ability to tag other accounts. With these various conveniences, Instagram has become an active, open, and broad digital interaction space. Its users come from various age groups, from teenagers to adults. However, behind its popularity, social media can also be misused. Various cases of abuse, such as fraud, account hacking, and cyberbullying are rampant. This is a significant concern because it can have serious consequences for the victims [1][2]. Instagram users can tag other accounts in uploaded photos or videos. As of October 2023, the number of Instagram users in Indonesia reached 104.8 million [3]. Technological developments have had positive impacts, such as easier access to information, but also negative impacts, such as reduced direct social interaction and the emergence of negative behaviors, particularly among adolescents [4]. As the number of Instagram users increases, many people are misusing this platform to commit cybercrimes such as account hacking and cyberbullying, which are online crimes that can have serious consequences for victims [5][6]. Cyberbullying is an unacceptable act that attacks the victim mentally and physically through messages or media such as photos, videos, and audio. Its forms include flaming, harassment, denigration, impersonation, outing, trickery, exclusion, and cyberstalking.[7]. Research by Dina Yuliana,

Trihastuti Yuniati, and Bitu Parga Zen demonstrated that the NIJ method is effective in uncovering evidence of cyberbullying on Instagram and WhatsApp, with optimal results on rooted devices [8]. Rahmat Ingg and Heri Pebrianto Alam used the NIJ method in a forensic analysis of the Google Chrome browser on Android and successfully recovered various digital artifacts such as accounts, cache, history, and cookies [9]. Research by Herman, Anton Yudhana, and Fitri Anggraini on the Android-based TikTok application demonstrated that the NIJ method and the MOBILedit tool are capable of obtaining more comprehensive digital evidence on rooted devices [10]. Imam Riadi, Sunardi, and Yana Safitri used the Association of Police Officers method in a forensic analysis of the IMO Messenger application and successfully collected comprehensive digital evidence [11]. Febe Dwi Intan Permatasari applied a live forensics approach to analyze cyberbullying activity on Facebook and successfully recovered direct evidence such as statuses, comments, and browsing history on active devices [12].

2. LITERATURE STUDY

2.1 Digital Forensics

Digital Forensics is a part of forensic science that includes the recovery and investigation of data found on digital devices using various scientific methods to examine evidence so that it can be accepted in court [7].

2.2 Digital Evidence

Digital evidence is data from electronic devices such as text, audio, images, or video, including those that have been deleted. This data is retrieved through an extraction process and used as an aid in legal proceedings [13].

2.3 Instagram

Instagram is a photo-sharing app that allows users to take, edit, and share photos, as well as communicate through direct messaging. As of October 2023, the number of Instagram users in Indonesia reached 10.8 million [3]. This platform has become one of the most popular social media platforms, especially among students [14].

2.4 Cyberbullying

Cyberbullying refers to the act of using information and communication technologies such as social media to spread content that intimidates, degrades or emotionally hurts others. Cyberbullying takes various forms and can be carried out individually or in groups [15].

2.5 Web Browser

A web browser is software for accessing information on the internet [18]. Its functions include opening and displaying web pages, storing data, managing history and credentials, and

protecting against malicious sites [19]. Information is identified through sources such as web pages, images, or videos [20].

2.6 FTK Imager

FTK Imager is a forensic software used to create copies of data from storage devices such as hard drives and USB [21][22]. This tool supports a wide range of file formats, making it very useful for forensic professionals [23].

2.7 Browser History Examiner

Browser History Examiner is an application that displays web browsing history on a laptop, along with important information such as access times and accounts/emails used. This application is useful in supporting digital forensic investigations to find digital evidence [24].

2.8 Image Cache Viewer

Image Cache Viewer is an application that displays images from visited websites, complete with image URL, browser type, access time, and the image's origin site [25].

2.9 National Institute of Justice

The National Institute of Justice (NIJ) method is an approach in digital forensics used to obtain digital evidence through data extraction and analysis. In this study, the NIJ method was used because it has systematic stages including preparation, collection, examination, analysis, and reporting, all aimed at finding and processing digital evidence so that it can be used as valid evidence in legal proceedings [8].

3. RESEARCH METHODE

The investigative process in this study was implemented using the National Institute of Justice method. The National Institute of Justice method has four stages: collection, examination, analysis, and reporting. The steps are as shown in Figure 1.



Figure 1: Stages of the NIJ Method

Figure 1 shows the stages in the NIJ (National Institute of Justice) method used in the digital investigation process. This stage begins with preparation, namely preparing the necessary devices and tools such as FTK Imager, Browser History Examiner, and Image Cache Viewer. Next comes the digital data collection and examination stage, which aims to extract information such as hidden files, deleted data, and activity history on the evidence device. After that, the data is analyzed to uncover important evidence such as edited images, history of accessed sites, and user activity. Finally, the reporting stage is carried out to document all investigation results, including digital evidence, methods, and tools used in a systematic and accountable manner.

4. RESULT AND DISCUSSION

This study analyses cases of cyberbullying on Instagram using the NIJ method, which consists of three stages: pre-incident, incident, and post-incident. The pre-incident stage includes the preparation of tools, identification of potential evidence sources, and initial documentation before further investigation. The pre-incident stage is shown in Figure 2.

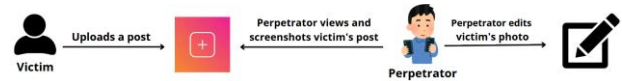


Figure 2 : Pre-incident of cyberbullying cases

Figure 2 shows that the incident began when the victim uploaded a post to her personal Instagram account, which the perpetrator followed. After seeing the post, the perpetrator intended to cyberbully her by taking a screenshot and then editing the victim's face to create a grotesque image, intended to ridicule and humiliate her. The second stage is the incident stage as shown in Figure 3.

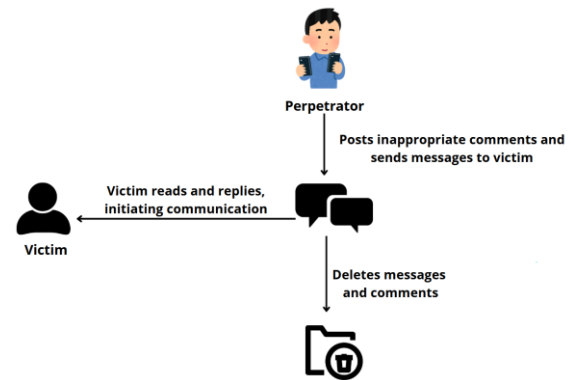


Figure 3: Incident of cyberbullying cases

Figure 3 shows the perpetrator sending demeaning comments and intimidating messages to the victim via direct message. Although communication initially occurred, the perpetrator continued to pressure the victim, sending a photo-edited image of her face to mock her. Disturbed, the victim threatened to report the perpetrator, urging him to stop. As a result, the perpetrator panicked and deleted all messages, comments, and the edited image to cover up any traces of the incident. The final stage is post-incident as shown in Figure 4.



Figure 4: Post incident of cyberbullying cases

Figure 4 shows that after experiencing cyberbullying, the victim reported the incident to the authorities. Investigators were then asked to investigate by collecting evidence in the form of chats, comments, and images based on the victim's report. The evidence found was examined using forensic tools to confirm its validity and identify the perpetrator.

4.1 Preparation

This stage is the initial step before the investigation, focusing on preparing tools and materials, including hardware and software. Investigators found evidence in the form of the perpetrator's laptop, which was turned on, and immediately secured it for further examination. This laptop later became the primary source for the forensic process, providing access to system data, stored conversations, and browsing activities that were crucial in uncovering the case, as illustrated and shown in Figure 5.



Figure 5: Laptop Evidence

Figure 5 shows the perpetrator's laptop, which served as the primary object of evidence in the investigation of this cyberbullying case. Prior to further analysis, the laptop's specifications were thoroughly examined. This examination was conducted to ensure that the device possessed adequate technical capabilities to support the digital investigation process, particularly in terms of storage capacity, processor performance, operating system, and other critical components. The perpetrator's laptop's specifications were crucial to the success of forensic software, particularly for extracting, recovering, and analyzing digital data related to the case. These specifications not only validated the feasibility of the forensic examination but also minimized potential errors that might occur during the data acquisition and analysis process, as shown in Table 1.

Table 1: Laptop Specifications

Laptop Specifications	
Brand	Asus Zenbook 13
Processor	AMD Ryzen 7 5700 U with Radeon Graphics 1.80 GHz
RAM	16.0 GB
SSD	1 TB

Table 1 shows the specifications of the perpetrator's laptop, which was used as primary evidence in the cyberbullying investigation. Examining the device's specifications is essential to ensure smooth digital data analysis, particularly in terms of storage capacity, processor type, operating system, and RAM. In addition to hardware, the investigation also required specialized software to extract, recover, and analyze digital data, helping investigators reconstruct digital traces and uncover crucial evidence. The selection of software was based on its reliability, compatibility with the available hardware, and ability to handle large volumes of forensic data, thereby supporting the overall accuracy and validity of the forensic examination, as shown in Table 2.

Table 2: List of Software

No	Software
1.	Instagram web
2.	FTK Imager 4.5.0.3
3.	Browserr History Examiner
4.	Image Cache Viewer

Table 2 shows the software utilized in the investigation, including FTK Imager for retrieving deleted chat data, Browser History Examiner for viewing the perpetrator's Instagram access history, and Image Cache Viewer for identifying images of the victim that had been deleted from messages.

4.2 Collection

The second stage involved gathering evidence, including the perpetrator's laptop, which was still on. RAM memory was captured using FTK Imager to ensure the authenticity of the data. The process is shown in the following Figure 6.

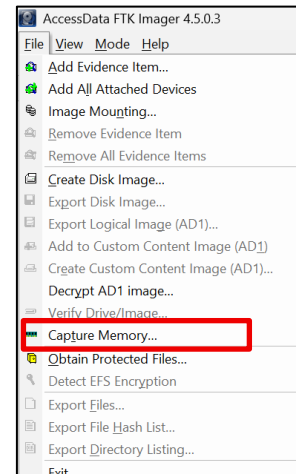


Figure 6: Memory capture feature on FTK Imager

Figure 6 shows the FTK Imager feature for capturing RAM memory, which is useful for capturing data on laptop activity while in use. Once the feature is selected, the data capture process will proceed as shown in Figure 7.

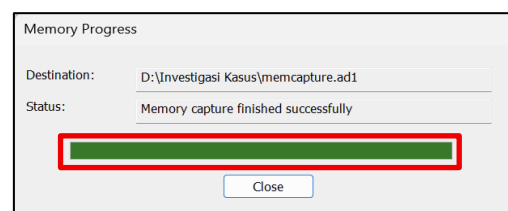


Figure 7: FTK Imager Memory Capture successful

Figure 7 shows the screen when the memory capture process is successful, and the results are automatically saved in the selected directory. These files, which contain important digital evidence for further analysis, are stored in various formats to ensure comprehensive examination. The integrity and organization of these files are crucial for the next stages of the investigation process. The folder containing the captured memory data can be accessed, as shown in Figure 8.

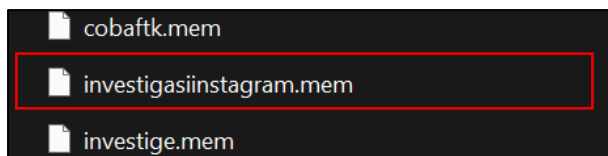


Figure 8: Capture Memory Results

Figure 8 shows a 17 GB .mem memory capture file stored in D:\Case Investigation. Subsequently, a web browser history capture was performed on the perpetrator's laptop to obtain evidence of access, including the time and type of browser used, such as Firefox, Chrome, Edge, and Internet Explorer. This process is shown in Figure 9.

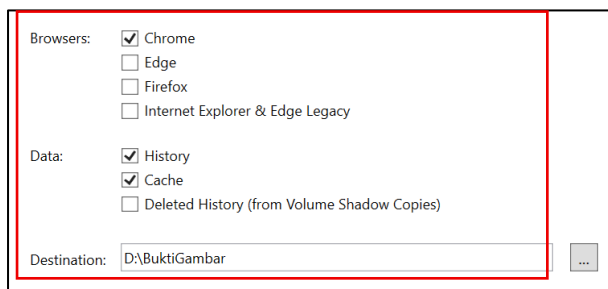


Figure 9: Capture Memory Browser History Examiner

Figure 9 shows the data capture process in Browser History Examiner, targeting the Google Chrome browser, which will display various historical data. After the capture process in Browser History Examiner is complete, the data is automatically saved in a folder named "capture" in the selected location. This storage method ensures that the captured data remains organized and easily accessible for subsequent forensic analysis, as shown in Figure 10.

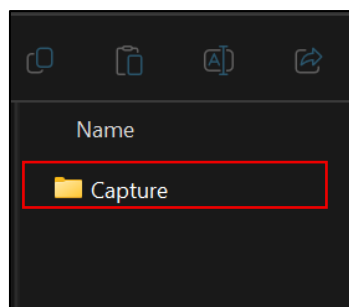


Figure 10: View After Capture History Process

Figure 10 shows the results of a browser history capture automatically saved in the "D:\BuktiGambar" folder. Next, Image Cache Viewer was used to find images that the perpetrator had deleted. This tool detects cached images from Instagram Web via Google Chrome, including edited images of the victim's face. The tool's display is shown in Figure 11.

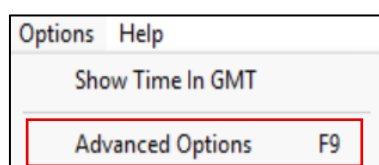


Figure 11: Display Selects Menu Options

Figure 11 shows the options menu in Image Cache Viewer for selecting browsers to scan. Several browsers are available to choose from, as shown in Figure 12.

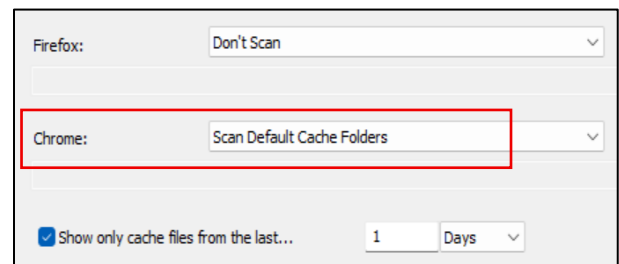


Figure 12: Display selects the folder to be scanned

Figure 12 shows the browser selection for scanning, and since the perpetrator used Google Chrome, the Chrome cache folder was scanned for image evidence.

4.3 Examination

After data collection, the next step is to examine the digital evidence to ensure it matches the victim's report. The evidence examined includes memory capture results (FTK Imager), web browsing history (Browser History Examiner), and cached images from Chrome. The examination is carried out carefully to identify the relationship between time, messages, and the perpetrator's activities, ensuring a clear and valid chronology of events.

4.3.1 FTK Imager

After memory capture, the .mem format file is checked by selecting the "add evidence item" menu to view the data contents, as shown in the Figure 13.

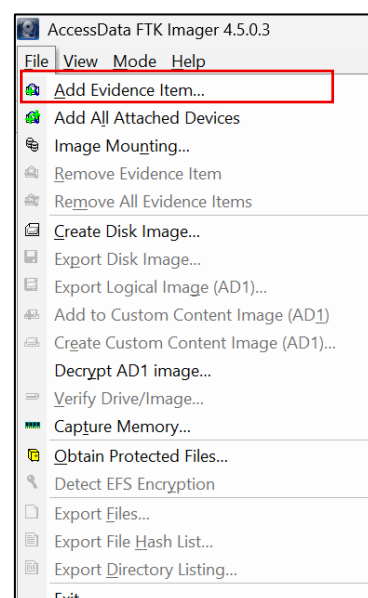


Figure 13: Add Evidence Menu Display in FTK Imager

Figure 13 shows the "add evidence item" menu in FTK Imager for adding evidence files. Since the file being examined is in .mem format, the "image file" type is selected based on its storage location. This step is essential to ensure that FTK Imager correctly recognizes and loads the memory image for further analysis. Accurate selection of the file type and location minimizes the risk of errors during the evidence loading

process, allowing investigators to proceed with a detailed examination of the memory content, as shown in Figure 14.

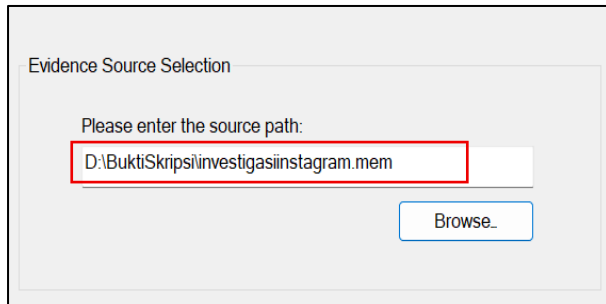


Figure 14: Select sources of evidence

Figure 14 shows the selection of the "Investigasiinstagram.mem" file from the D:\BuktiSkripsi\ directory for analysis in FTK Imager. This step aims to trace activity in the perpetrator's laptop memory, including evidence of deleted chats and comments as shown in Table 3.

Table 3 : Deleted comments and chats

003b78050	49 00 4D 00 20 00 3A 00-20 00 32 00 31 00 32 00	I-M-...-2-1-2-
003b78060	33 00 32 00 34 00 32 00-35 00 32 00 36 00 32 00	3-2-4-2-5-2-6-2-
003b78070	37 00 0A 00 4B 00 65 00-6C 00 61 00 73 00 20 00	7...K-e-l-a-s-
003b78080	3A 00 20 00 42 00 0A 00-31 00 20 00 6A 00 61 00	:-B...l-ja-
003b78090	6D 00 0A 00 6D 00 61 00-74 00 63 00 68 00 61 00	m...a-t-c-h-a-
003b780a0	6C 00 61 00 61 00 64 00-64 00 69 00 63 00 74 00	l-a-s-d-d-e-t
003b780b0	0A 00 6D 00 75 00 6B 00-61 00 6E 00 79 00 61 00	k-a-u-k-a-n-y-a
003b780c0	20 00 6A 00 65 00 6C 00-65 00 6B 00 20 00 62 00	j-e-l-e-k-b-
003b780d0	67 00 74 00 20 00 6B 00-61 00 6B 00 0A 00 39 00	r-t-k-a-k-k-9-
003b780e0	20 00 6D 00 65 00 6E 00-69 00 74 00 42 00 61 00	m-e-n-i-t-B-a-
003b780f0	6C 00 61 00 73 00 0A 00-31 00 20 00 6A 00 61 00	l-a-s...l-ja-
003b78100	6D 00 20 00 79 00 61 00-6E 00 67 00 20 00 6C 00	m-y-a-n-g-l-

05fb591d0	6D 00 0A 00 6D 00 75 00-6B 00 61 00 6E 00 79 00	m...m-u-k-a-n-y-
05fb591e0	61 00 20 00 6B 00 6F 00-20 00 61 00 6E 00 65 00	a-k-o-a-n-e-
05fb591f0	68 00 20 00 73 00 69 00-20 00 6B 00 61 00 6B 00	h-s-i-k-a-k-
05fb59200	0A 00 4D 00 61 00 73 00-75 00 6B 00 6B 00 61 00	-M-a-s-u-k-k-a-
05fb59210	6E 00 0A 00 41 00 6E 00-64 00 61 00 20 00 6D 00	n-A-n-d-a-m
05fb59220	65 00 6E 00 67 00 69 00-72 00 69 00 6D 00 0A 00	e-n-g-i-r-i-m...
05fb59230	6A 00 65 00 6C 00 65 00-6B 00 20 00 62 00 67 00	j-e-l-e-k-b-g
05fb59240	74 00 20 00 67 00 69 00-74 00 75 00 20 00 64 00	t-g-i-t-u-d
05fb59250	69 00 20 00 76 00 69 00-64 00 65 00 6F 00 6E 00	i-v-i-d-e-o-n
05fb59260	79 00 61 00 0A 00 4D 00-61 00 73 00 75 00 6B 00	y-a-M-a-s-u-k
05fb59270	6D 00 61 00 6E 00 0A 00-66 00 61 00 75 00 7A 00	k-a-n-f-a-u-d
05fb59280	61 00 61 00 64 00 72 00-0A 00 69 00 6E 00 69 00	a-a-d-r-i-n-i-

Table 3 shows that the perpetrator repeatedly sent comments and messages containing bullying, including edited photos of the victim's face, which disturbed the victim and led to him being reported to the authorities.

4.3.2 Browser History Examiner

This tool is used to capture the Google Chrome web browser history on the laptop of a discovered perpetrator. This tool can obtain evidence such as the date and time the perpetrator accessed Instagram Web, the perpetrator's Instagram username, the sites visited, and the number of visits. All of the perpetrator's browser activity is recorded in detail by this tool. Furthermore, this tool also allows for in-depth analysis of the perpetrator's browsing habits. The obtained data can be synchronized with other digital evidence to strengthen the chronology of events. This tool also supports various other browsers, allowing for a broader analysis. The recorded information can be exported as a report for forensic documentation purposes. These results are crucial as valid supporting evidence in legal proceedings. An example of the extracted data produced by this tool is shown in Figure 15.

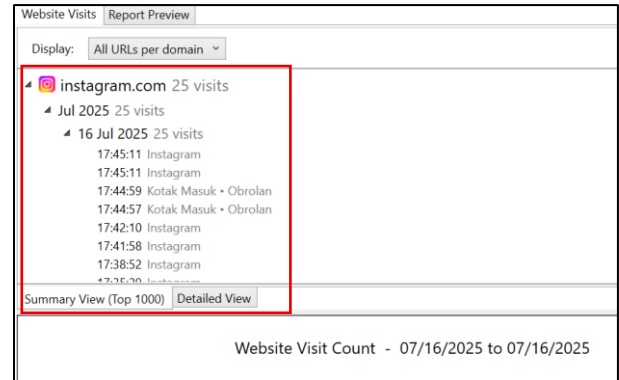


Figure 15: Extraction Result

Figure 15 shows the data extraction results, including "websites visited," "thumbnails," "cookies," and more. The left menu shows additional information, such as the perpetrator's access to Instagram Web along with the date and time.

4.3.3 Image Cache Viewer

The Image Cache Viewer tool is used to find edited images of the victim's face that the perpetrator sent via Instagram direct message before deleting them. This tool also displays other images accessed by the perpetrator, complete with URLs, dates, timestamps, and previews, making it easier to identify evidence. The image evidence obtained and stored in the cache is shown in Figure 16.

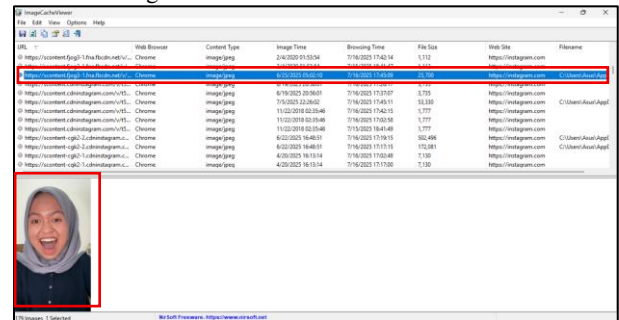


Figure 16: Image Evidence Deleted by the Perpetrator

Figure 16 shows evidence of an image of the victim's face that had been edited and deleted by the perpetrator, found in the laptop's cache folder. In addition to the image, information such as the browser used, access time, file size, URL, and image file name was also found.

4.4 Analysis

After the evidence collection and examination process is complete, the next crucial stage in the investigation is analyzing all the data and information obtained. This analysis aims to interpret and understand the contents of the recovered digital evidence to form the basis for establishing a chronology of events and strengthening suspicions about the perpetrator. In this case, the analysis was conducted on data obtained from various digital forensic tools, including FTK Imager, Browser History Examiner, and Image Cache Viewer. During this stage, each piece of evidence collected will be thoroughly examined to identify the interrelationships between each piece of evidence. The results of the analysis will help establish a coherent sequence of events, identify the perpetrator's role, and clarify their motives and methods of carrying out their actions.

4.4.1 Analysis Using FTK Imager

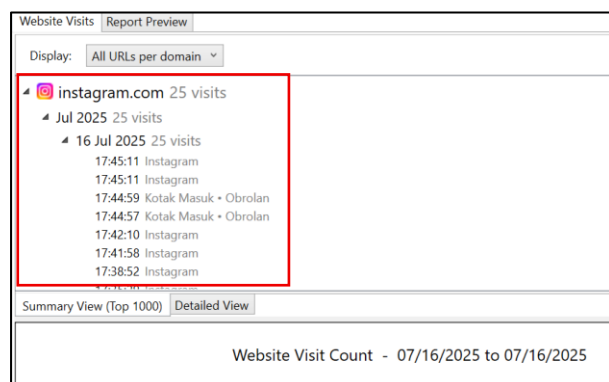
After conducting an examination of the FTK Imager tool, several pieces of evidence were found, including comments and messages sent by the perpetrator to the victim during the cyberbullying. The evidence found in this tool is shown in Table 4.

Table 4: Deleted comments and chats

Information	Result	Description
Comment	mukanya jelek bgt kak	Found
Conversation	mukanya kok aneh si kak	Found
Conversation	jelek bgt gitu di videonya	Found
Conversation	ada deh	Found
Conversation	penasaran yaa	Found
Conversation	liat ini deh	Found
Conversation	kayak bukan editan kan?wkwkwk	Found
Conversation	laporin aja coba gatakut	Found

4.4.2 Analysis Using Browser History Examiner

After conducting an inspection using the Browser History Examiner tool, several important pieces of evidence were discovered, such as the time the perpetrator accessed the website, which was July 16, 2025. Furthermore, the perpetrator's Instagram username and other technical information, including the type of browser used, Google Chrome, were also identified. This evidence strengthens the suspicion that the perpetrator carried out his actions through the device. All of this information was recorded in detail and can be used to support the process of compiling a chronology of events. This evidence is shown in Figure 17.



Brand	Asus Zenbook 13
Processor	AMD RYZEN 7 5700U With Radeon Graphics 1.80 Ghz
RAM	16.0 GB
SSD	1 TB

Figure 17: Website Visit History

4.4.3 Analysis using Image Cache Viewer

After examining the image with Image Cache Viewer, an edited image of the victim's face was found, sent by the perpetrator via direct message, and then deleted to cover any traces. Because the perpetrator's laptop was still on and the cache hadn't been cleared, the image file remained and was successfully identified without damage. This finding demonstrates how cached data can preserve crucial digital traces even after attempts at deletion, reinforcing its value in digital forensic investigations. The discovery of this image also

provided strong supporting evidence that directly linked the perpetrator's online activities with the act of cyberbullying, thereby strengthening the overall validity of the investigation. This evidence is shown in Figure 18.



Figure 18: Image Evidence

4.5 Reporting

The final stage of this research contains a report on the findings of evidence in a cyberbullying case on the Instagram application accessed through Google Chrome. The evidence is divided into two categories: physical and digital, with the digital evidence obtained using the tools FTK Imager, Browser History Examiner, and Image Cache Viewer. The specifications of the physical evidence are shown in Table 5 below.

Table 5: Laptop Specifications

Brand	Asus Zenbook 13
Processor	AMD RYZEN 7 5700U With Radeon Graphics 1.80 Ghz
RAM	16.0 GB
SSD	1 TB

Table 5 shows digital evidence in the cyberbullying case via Instagram Web that was successfully obtained using three main digital forensics tools: FTK Imager, Browser History Examiner, and Image Cache Viewer. Each tool plays a crucial role in the investigation process, revealing the perpetrator's activities in detail. FTK Imager was used to retrieve and recover data from the perpetrator's laptop memory, including the contents of previously deleted conversations or direct messages that were still stored in the system. Browser History Examiner was used to trace the perpetrator's browsing history, proving that the perpetrator accessed Instagram via the Google Chrome browser at specific times. Meanwhile, Image Cache Viewer was used to recover images that had been accessed or sent by the perpetrator, including crucial evidence in the form of a photo of the victim's face that had been edited and then deleted by the perpetrator. Collectively, the findings from these tools provided a comprehensive reconstruction of the perpetrator's actions and established a strong link between the digital traces and the cyberbullying incident. All digital evidence recovered from the examination using these tools is summarized and shown in Table 6.

Table 6: Details of digital evidence

No	Digital Evidence	FTK Imager	Browser History Examiner	Image Cache Viewer
1	Deleted chats	7	0	0
2	Deleted comment	1	0	0
3	Perpetrator's Instagram username	0	1	0
4	Web browser history	0	1	0
5	Deleted image	0	0	1

Table 6 shows the digital evidence recovered from the examination using several tools. FTK Imager revealed deleted chat history, Browser History Examiner found the perpetrator's Instagram username and visit history, and Image Cache Viewer successfully identified an edited image of the victim's face sent via direct message.

4.6 Evaluations

The evaluation of the investigation results shows that the National Institute of Justice (NIJ) method is effective in systematically recovering deleted artifacts such as chats, comments, and edited images from Instagram Web. Compared to previous studies that applied the NIJ method to WhatsApp and TikTok, this research produces consistent findings that demonstrate the reliability of the method in social media forensic investigations.

However, certain limitations were observed. The NIJ method has weaknesses in handling encrypted communication and activities conducted through private browsing modes, which reduce the possibility of obtaining complete evidence. The memory capture process using FTK Imager also required significant time and storage resources, as the extracted file reached 17 GB in size. Nevertheless, the integrity of the evidence was guaranteed through MD5 hashing, which confirmed that the data had not been altered during the examination process.

In terms of recovery success, this study managed to uncover seven deleted chats, one deleted comment, and one edited image that had been removed by the perpetrator. These findings prove that the NIJ method is capable of uncovering crucial evidence that can strengthen the legal process in cyberbullying cases. Therefore, the NIJ method can be considered a reliable and practical approach, although future research is needed to integrate additional techniques such as artificial intelligence to enhance efficiency and scalability in digital forensic investigations.

5. CONCLUSIONS

The conclusion of the study entitled "Website Forensic The conclusion of the study entitled "Website Forensic Analysis of Cyberbullying Cases on the Instagram Application Using the National Institute of Justice Method" shows that the digital forensic process was successfully carried out through five stages: preparation, collection, examination, analysis, and reporting. The investigation managed to reveal cyberbullying activities in the form of one deleted comment and seven deleted chats using FTK Imager, as well as the recovery of browsing history and an edited image through Browser History Examiner and Image Cache Viewer. Validation with MD5 hashing confirmed the authenticity of the evidence without

manipulation. This study highlights the effectiveness of the NIJ method in handling social media cyberbullying cases, proving that it can systematically uncover crucial digital artifacts. The findings can serve as a reference for law enforcement and forensic investigators in dealing with similar cases. However, the research also identified certain limitations, such as difficulties in analyzing encrypted data and the significant time required for memory capture on large storage devices.

Future research is recommended to apply the NIJ method to other platforms such as TikTok, WhatsApp Web, or Discord, and to integrate advanced technologies like artificial intelligence to improve efficiency, scalability, and automation in digital forensic investigations.

6. REFERENCES

- [1] R. R. Armayani, L. C. Tambunan, R. M. Siregar, N. R. Lubis, dan A. Azahra, "Analisis peran media sosial Instagram dalam meningkatkan penjualan online," *Jurnal Pendidikan Tambusai*, vol. 5, no. 3, pp. 8920–8928, 2021
- [2] A. Fajri Muttaqien, F. Hibatullah, and R. Wulandari, "Efektivitas Media Sosial Instagram Terhadap Pengungkapan Diri," *Jurnal Ilmu Komunikasi Dan Media Sosial (JKOMDIS)*, vol. 2, no. 3, p. 370, 2022, doi: 10.47233/jkomdis.v2i1.396.
- [3] R. Zulfiqui, B. N. Sari, and T. N. Padilah, "Analisis Sentimen ulasan pengguna aplikasi sosial media Instagram Pada Situs Google Playstore Menggunakan Naïve Bayes Classifier," *Jurnal Informatika dan Teknik Elektro Terapan*, vol. 12, no. 3, Aug. 2024, doi: 10.23960/jitet.v12i3.4995
- [4] M. Ayub dan S. F. Sulaeman, "Dampak sosial media terhadap interaksi sosial pada remaja: kajian sistematis," *Jurnal Penelitian Bimbingan dan Konseling*, vol. 7, no. 1, Mar. 2022.
- [5] V. Vera, M. Morisrona, dan H. A. Nurohman, "Keamanan Informasi pada Media Sosial Instagram," *Prosiding Seminar Nasional Teknologi Informasi dan Bisnis (SENATIB)*, 2024.
- [6] H. Septya Mikayla, A. Kusyanti, P. H. Trisnawan³, and P. Korespondensi, "Analisis Forensik Digital Untuk Investigasi Kasus Cyberbullying pada Media Sosial TikTok", doi: 10.25126/jtiik.2023108017.
- [7] D. Yuliana, T. Yuniati, dan B. P. Zen, "Analisis forensik terhadap kasus cyberbullying pada Instagram dan WhatsApp menggunakan metode NIJ," *Cyber Security dan Forensik Digital*, vol. 5, no. 2, pp. 52–59, Nov. 2022.
- [8] M. F. Hasa, A. Yudhana, and A. Fadlil, "Analisis Bukti Digital pada Storage Secure Digital Menggunakan Metode Static Forensic," *Jurnal Mobile and Forensics (MF)*, vol. 1, no. 2, pp. 76–84, 2019, doi: 10.12928/mf.v1i2.XXXX.
- [9] R. Inggi, H. P. Alam, P. Studi, S. Informasi, S. Bina, and B. Kendari, "Analisis forensik web browser pada perangkat Android," vol. 8, no. 1, 2023.
- [10] F. Anggraini, H. Herman, and A. Yudhana, "Akuisisi Bukti Digital Tiktok Berbasis Android Menggunakan Metode National Institute of Justice," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 10, no. 1, pp. 89–96, Mar. 2023, doi: 10.25126/jtiik.2023106416.

- [11] I. Riadi, Y. Safitri, and U. Ahmad Dahlan, “Hal. 1~8 Menggunakan Metode Association of Chief Police Officers,” *Jurnal Bumigora Information Technology (BITE)*, vol. 5, no. 1, pp. 1–8, 2023, doi: 10.30812/bite/v5i1.2977.
- [12] F. Dwi, “Analisis aktivitas cyber bullying pengguna Facebook melalui browser Chrome dengan pendekatan live forensics,” *JTM*, vol. 12, no. 1, pp. 21-27, Sep. 2023. [Online]. Available: <https://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/687>
- [13] J. A. Ginting, H. Setiawan, J. F. Andry, and I. G. Ngurah Suryantara, “Rekonstruksi dan Investigasi Digital Forensik pada Aplikasi Whatsapp Dengan Metode NIST : Kasus Pelecehan Seksual,” *Infotech: Journal of Technology Information*, vol. 10, no. 1, pp. 71–76, Jun. 2024, doi: 10.37365/jti.v10i1.249.
- [14] W. Situmorang and R. Hayati, “Media Sosial Instagram Sebagai Bentuk Validasi Dan Representasi Diri,” *Jurnal Sosiologi Nusantara*, vol. 9, no. 1, pp. 111–118, Jun. 2023, doi: 10.33369/jsn.9.1.111-118.
- [15] A. Afralia and D. Safitri, “Analisis Penyebab Maraknya Cyberbullying di Era Digital pada Remaja,” 2024. [Online]. Available: <https://jurnal.tiga-mutiara.com/index.php/jimi/index>
- [16] A. Sukmawati, A. Puput, and B. Kumala, “Dampak Cyberbullying Pada Remaja di Media Sosial.” [Online]. Available: <http://journal.uin-alauddin.ac.id/index.php/asjn/issue/view/1328>
- [17] F. A. Imani¹, A. Kusmawati², H. Moh, and A. Tohari³, “Pencegahan Kasus Cyberbullying Bagi Remaja Pengguna Sosial Media,” 2021.
- [18] H. Hariani, “Eksplorasi Web Browser dalam Pencarian Bukti Digital menggunakan SQLite,” *Jurnal INSTEK (Informatika Sains dan Teknologi)*, vol. 6, no. 1, Apr. 2021. doi: 10.24252/instek.v6i1.18638
- [19] B. C. Nugroho, N. D. W. Cahyani, dan S. A. Mugitama, “Analisis Dampak Pengaturan Mode Keamanan Browser Terhadap Kelengkapan Data Forensik,” *eProceedings of Engineering*, vol. 12, no. 1, Feb. 2025.
- [20] M. Rusdi Oktapalisa, W. Murti, and J. Informatika dan Komputer Jurnal Informatika dan Komputer, “Membuat Aplikasi Penjualan Pada CV. Sumber Bakti Mandiri Berbasis Website Menggunakan PHP dan MYSQL,” 2022.
- [21] M. Rosita, “Analisis komparatif performa FTK Imager dan Autopsy dalam forensik digital pada flashdisk,” *Info Kripto*, vol. 17, no. 3, pp. 40–48, Dec. 2023. doi: 10.56706/ik.v17i3.83.
- [22] R. Y. Herman and B. Triadi, “Analisis Computer Forensic Untuk Mendukung Prosesnya Penyelidikan Dalam Kasus Kejahatan,” 2023, doi: 10.22303/upu.1.1.2021.01-10.
- [23] W. Agustiono, D. Wulan Suci, and N. Prastiti, “Analisis Forensik Digital Menggunakan Metode NIST untuk Memulihkan Barang Bukti yang Dihapus Digital Forensic Analysis Using the NIST Method for Recovering Deleted Evidence,” *Jurnal Teknologi dan Informasi (JATI)*, vol. 14, 2024, doi: 10.34010/jati.v14i2.
- [24] H. Adamu, A. Adamu Ahmad, A. Hassan, and ad Barau Gambasha, “IJRSI |Volume VIII, Issue V,” 2021. [Online]. Available: www.rsisinternational.org.
- [25] F. Dzil Ikram and M. Koprari, “Forensic analysis on discord application using the National Institute of Standards and Technology (NIST) Method,” 2023. [Online]. Available: www.ejournal.isha.or.id/index.php/Mandiri.