

Digital Data Retrieval on Web-based Twitter Services using National Institute of Standard and Technology Method

Iraunasya Wiyanto
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

Technological developments are increasing. Technology helps make it easier for humans to communicate. In addition to having a good impact, advances in information technology and telecommunications also have a bad impact, namely the number of crimes related to internet applications. This study was conducted based on reports from original cases that had occurred. This research was conducted to collect digital data on laptop hardware related to cases of cyber harassment that occurred through a web-based Twitter application service. This research was conducted to scenario cases of sexual harassment (sexual harassment) using a web-based twitter service with google chrome. The process of searching and processing data is carried out using the stages of the National Institute of Standard and Technology (NIST), which has a collection, examination, analysis and reporting flow. This study obtains digital data from the acquisition results on the perpetrator's laptop and data extraction on web-based twitter running on google chrome. The results are then analyzed and matched with digital data evidence obtained by the police. The data obtained in the form of images and text captions that have been deleted, as well as email, username, password (perpetrator) and time of posting. Forensic processes were carried out with several tools with success rates, namely FTK Imager was successful at 50%, Browser History capture was successful at 100%, Browser History Viewer was successful at 100%, Browser History Examiner was successful at 50%. The findings of the evidence are the same as the reports found by the police.

Keywords

Forensic, Web, Twitter, NIST, Cyber Harassment

1. INTRODUCTION

The development of information technology at this time has developed [1]. Technology helps make it easier for humans to communicate. In addition to having a good impact, advances in information technology and telecommunications also have a bad impact, namely the number of crimes related to internet applications [2]. One of the most popular social media applications in the world, including in Indonesia, is Twitter[3]. Twitter is a website that offers social networking services in the form of microblogs to users so that it allows users to send and read tweets or Twitter statuses. Users can also upload photos and videos [4]. Social media crimes or cybercrime that often occur are such as pornography, cyberstalking, cyberbullying, and cyber harassment. *Cyber harassment* is a person who constantly pursues other people online with the intent of humiliate or frighten. According to

research by digital security firm Norton, 76% of 1,000 female respondents under the age of 30 have experienced online sexual harassment [5].

1.1 Research Literature

1.1.1 Previous Study

Anwar and Riadi (2017) have conducted a research entitled "Analysis of WhatsApp Messenger Smartphone Forensic Investigations Against Web-Based WhatsApp". This research was conducted to handle cases of wiretapping conversations on the WhatsApp application. This study uses the DFRW investigation model. In this investigative model, it has an Identification phase (Identification of WhatsApp crimes), Preservation (WhatsApp case processing), Collection (Securing WhatsApp evidence), Examination (Tracking WhatsApp evidence), Analysis (Comparison of investigative data), and Presentation (Documentation)[6].

Riskiyadi (2020) has conducted a research entitled "Forensic Investigation of Digital Evidence in Revealing Cybercrime". This study uses a static forensic method with a framework from the National Institute of Justice (NIJ) with a cybercrime case scenario in the form of a card with electronic evidence of a flash disk. The static forensic process with the framework from the National Institute of Justice (NIJ) has the stages of Identification, Collection, Examination, Analysis, and Reporting [7].

Riadi, Sunardi, and Widiandana (2019) have conducted a research entitled "Analysis of Forensic Investigation of Cyberbullying on WhatsApp Messenger using the Institute of Standards and Technology (NIST) Method". This research was conducted for the analysis methodology of forensic investigation of cyberbullying on WhatsApp using the NIST method. The method used for this research is using the NIST method and to identify acts of cyber bullying using the Cosine Similarity method [8].

Nofiyani and Mushihudin (2020) have conducted a study entitled "Forensic Analysis on Web Phishing Using the National Institute of Standards and Technology (NIST) Method". This research was conducted to facilitate investigators in analyzing digital evidence. The stages of the National Institute Of Standards And Technology (NIST) method consist of Collection (data collection), Examination (data acquisition), Analysis, Reporting reports [9].

Bintang, Umar, and Yudhana (2018) have conducted a study

with the title "Live Forensic Comparison Design on Instagram, Facebook, and Twitter Social Media Security on Windows 10". This research was conducted to obtain valid data evidence. In this study using the National Institute of Justice (NIJ) method with the stages of Collection, Examination, Analysis and Reporting [10].

1.1.2 DigitalForensic

Digital forensics is a method of investigating and analyzing data stored and retrieved from storage devices for the purpose of presentation in courts of law, civil or administrative proceedings [11]. Digital forensics is part of forensic science that is used to investigate and investigate a case in the investigation of evidence found on digital devices (digital devices), computers (hosts, servers), networks (networks), and applications [12]. Digital forensics has sub-disciplines namely, computer forensics, mobile forensics, memory forensics, network forensics, malware forensics, operating system forensics, image forensics, cloud computing forensics, and audio forensics [13]. Digital forensics can also be interpreted as the collection and analysis of data from various computer resources which include computer systems, computer networks, communication lines, and various storage media.[14]

1.1.3 Web Browser

Web browser is software to perform various activities on the Internet. Users utilize browsers for many functions such as information retrieval, access to email accounts, e-commerce, banking creation, instant messaging, online blogs, access to social networks. Information and interests are interconnected, all exchanges of information occur on the internet, including on social media to communicate [15]. Currently, there are more and more types of browsers and they are growing rapidly, including Mozilla Firefox, Google Chrome, Microsoft Chrome, Microsoft Edge, Internet Explore, Opera, Safari and others[16].

1.1.4 Digital Evidence

Evidence in cybercrime cases is divided into two, namely electronic evidence and digital evidence. Electronic evidence is evidence in the physical form of an electronic device or storage device. Digital evidence is evidence in the form of document files, history files, or log files containing data related to cybercrime cases obtained from electronic evidence [17].

1.1.5 Social Media

Social media is a site where someone can create a personal or personal web page and can connect with other people who are on the same social media to be able to share information or just communicate[18]. Social media is an online medium, with its users being able to easily participate, share, and create content including blogs, social networks, wikis, forums and virtual worlds [19].

1.1.6 Twitter

Twitter has become a social media that is not only used as a tool to communicate, but has also been used as a medium to get information and can also be used as an advertising medium [20]. Twitter is a type of microblogging social media that facilitates users to write and publish their activities and opinions[21].

1.1.7 Cybercrime

Cybercrime is a crime committed by a person or group of

people by using a computer or the internet. According to Pajar Pahrudin (2010) in his book "Computer Work Ethics", cybercrime is one of the negative impacts of technological developments, and has harmed modern life today. Cybercrime can be interpreted as an unlawful act carried out using a computer network as a means/tool or object. Computer crime (cybercrime) knows no geographical boundaries, this activity can be carried out at close range, or from a distance of thousands of kilometers with similar results [22]. Computer crime is a crime whose traces of criminal activity need to be analyzed to become evidence. Cybercrime is a crime that is carried out by using computers as tools, targets and places for crime, for example child sexual crimes, online fraud, bullying, identity fraud, hacking, Identity Theft, pornography, cyberstalking and many other crimes.[23]

1.1.8 Sexual Harassment

Sexual harassment or sexual harassment is not limited to rape and artificial physical violence, and some behaviors that are taken up and conduct that exhibits sexually detrimental ways may be described as sexually harassing behavior. Sexual violence and / or sexual harassment can be divided into 2 [24] namely:

1. Serious sexual violence.
2. Mild sexual violence.

Verbal harassment in cyberspace, both sexual and non-sexual that occurs is a form of habit that is reproduced. Verbal harassment against women is still the same, only the form is different [25].

1.1.9 National Institute of Standard Technology

National Institute of Standards and Technology is the national non-regulatory agency of the United States technology administration. The NIST cybersecurity program seeks to develop and apply innovative and practical security technologies and methodologies to enhance countries' ability to address computer and information security challenges. The National Institute of Standards and Technology is a forensic standard that has policy guidelines and standards to ensure each examiner follows the same workflow so that work is documented with repeatable and defensible results. The NIST cybersecurity program seeks to enable the greater development and application of innovative and practical security technologies and methodologies to enhance the ability of countries to address current and future computer and information security challenges [26].



Figure 1. Stages of NIST Method

Figure 1 shows the national institute of standard technology (NIST) stage has four stages to carry out the mobile forensics investigation process to obtain digital evidence. With the following explanation:

1. Collection (Data collection)
Collecting evidence data with the process of identification, collection, taking and recording evidence.
2. Examination (data acquisition)
The results of the collection of evidence are tested so that there is no change in information on the evidence.
3. Analysis
Checked evidence to obtain evidence related to the case.
4. Reporting (Reporting)
Reporting the results of the investigation obtained from

the investigation. The report contains the results of the analysis of evidence to assist the investigation process.

2. METHODOLOGY

2.1 Research Scenario

The case in this study is the case of a sexual abuse through web-

based Twitter social media. The simulation in this case is that the perpetrator posted a photo with a caption that led to harassment sexual in twitter. Twitter was accessed by the perpetrator using the chrome web browser.

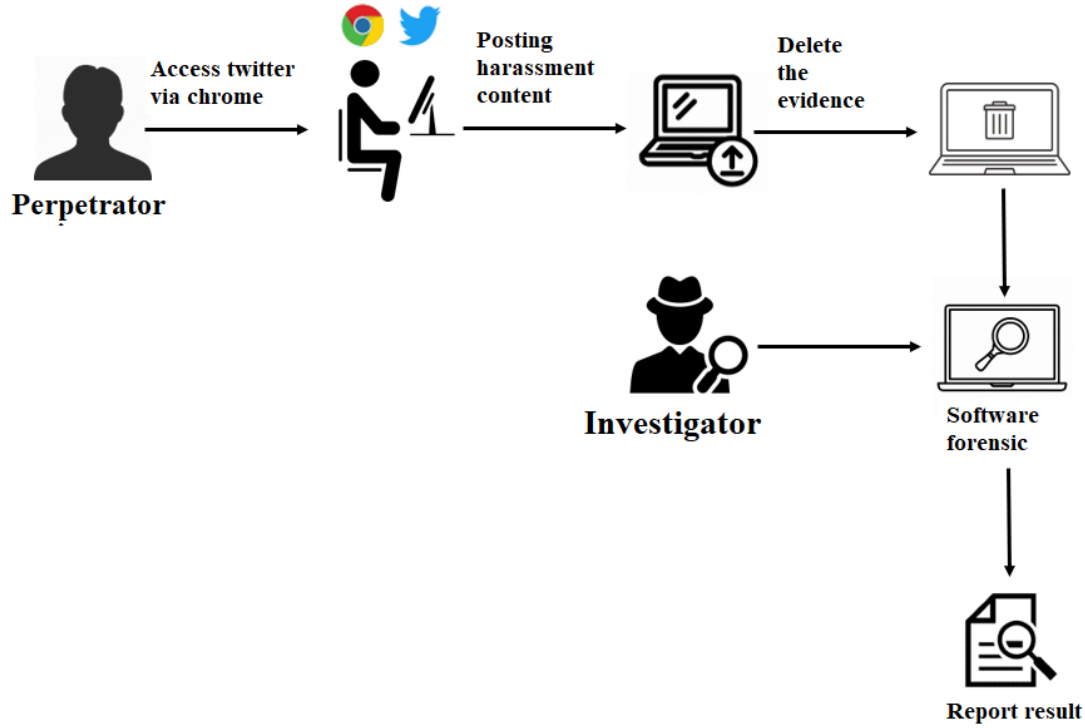


Figure 2. Flow of the Case Scenario on Twitter

Figure 2 The police arrested the perpetrator and the police secured evidence from the seller (suspect) who had made a transaction with the buyer (victim) through social media Facebook messenger using a smartphone. During the arrest the police got a smartphone after that the police secured the smartphone as evidence and stored it in an available place. The evidence is brought to the forensics department to carry out further investigations to obtain evidence and can be used as evidence in court. In the Facebook application messenger on a smartphone, a message was found that had been deleted by the seller (the suspect), to retrieve the deleted message in order to obtain evidence, the forensics carried out an examination using several procedures using software forensic.

2.2 Research Stages

The implementation stage in this research is to obtain digital data, investigators use the National Institute of Standard Technology (NIST) stage. Investigators use live forensics to search for digital data.

2.2.1 Collection

At the collection stage, which is the initial stage used by investigators to search, collect, and identify evidence obtained at the location of digital crimes. The process of collecting evidence based on data sources so that it will maintain data integrity. The evidence obtained in this study was the first, namely a laptop that was found to be turned on and connected to an internet connection, the second evidence was a laptop charger. The results of the discovery of the evidence are items

used by the perpetrators of the crime.

Table 1. Evidence Found at the Crime Scene



No	Name of Evidence	Figure	Description
1	Perpetrator's Laptop		The perpetrator's laptop is Lenovo G40-45 found at the crime scene with the state turned on and connected with network
2	Laptop Charging Cable		Charging cable The doer's Lenovo G40-45 with 100-240 V ~ 1.8 A input and 20 . output V and 3.25 A

Table 1 Evidence found by the police and submitted to investigators for analysis.

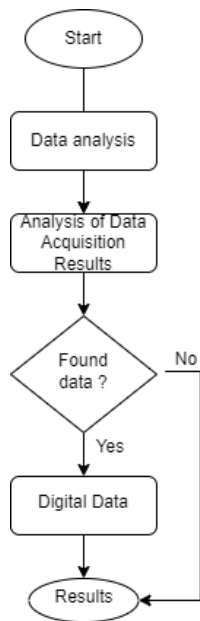


Figure 3. Investigation Flow

Figure 3 describes the flow of the investigation carried out by the investigator. The first step is to acquire data by capturing the RAM of the perpetrator's laptop using the RAM Capturer, after capturing the RAM, an Imaging file in MEM format is obtained. After that, an analysis of the RAM Capturer acquisition results was carried out using several forensic software such as FTK Imager which was used for Imaging RAM capturer files, Browser History Capturer which was used to acquire history from the browser, Browser History Examiner and Browser History Viewer which was used to read the acquisition results from the Browser. History Capture. In the analysis process, if successful, digital evidence will be found.

2.2.2 Examination

This stage is a very important stage in the forensic investigation process. At this stage, the process of taking over the information contained in the perpetrator's laptop will be carried out. The information acquisition process is carried out by means of live forensics, namely the taking of evidence with the laptop being turned on.

2.2.2.1 Belkasoft Live RAM Capture

Belkasoft Live RAM Capturer is a forensic tool used to capture memory. Forensic tools Belkasoft Live RAM Capturer is a tool used to acquire data stored in the RAM of a criminal's laptop to obtain digital evidence.

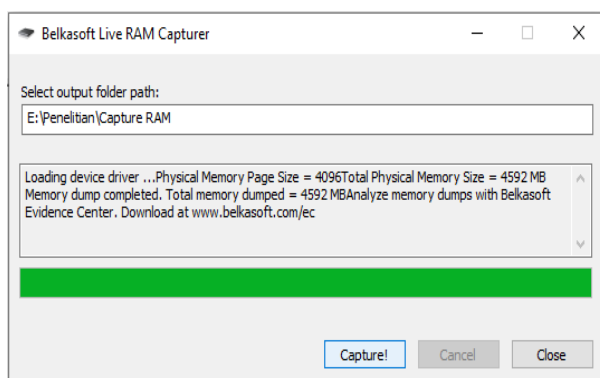


Figure 4. RAM acquisition

Figure 4 there is information displayed regarding the RAM data storage capacity of the perpetrator's laptop, which is 4592 Megabytes (MB). The results of the RAM data acquisition on the perpetrator's laptop are named 20211116.mem with a storage size of 4,702,208 KB. The resulting .mem file will then be hashed using the FTK Imager tool.

2.2.2.2 FTK Imager

The imaging process is carried out with the aim of maintaining the integrity of the acquired data by storing it in another storage location for data inspection by the investigator. The imaging process is carried out using the FTK Imager application. The acquired file with the file name 20211116.mem. will then be imaging using FTK Imager.

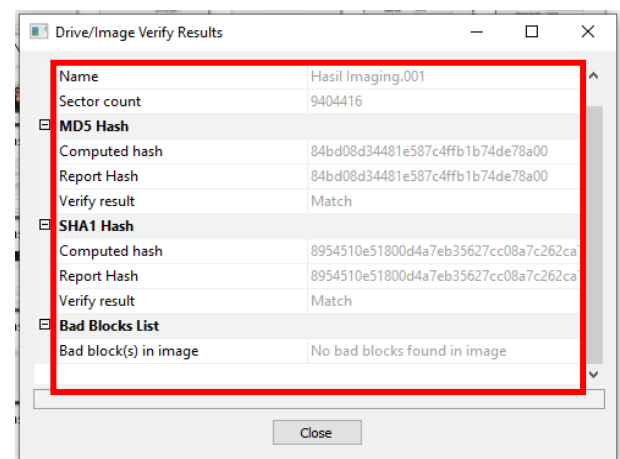


Figure 5. File hash value 20211116

Figure 5 displays the hash value of the imaging results. In this study, it can be seen that the MD5 Hash and SHA1 Hash values from the verified imaging file are the same or match the MD5 Hash and SHA1 Hash values from the original file. The same hash value means that the imaging process was successful without any changes to the file.

2.2.2.3 Browser History Capture

Browser History Capturer is a forensic tool that is used to acquire browsers especially on the chrome browser. In this study, the browser history capturer tool is used to retrieve data in the chrome browser. Then use the browser history examiner tool and browser history viewer to read the results of the acquisitions made by the browser history capturer tool.

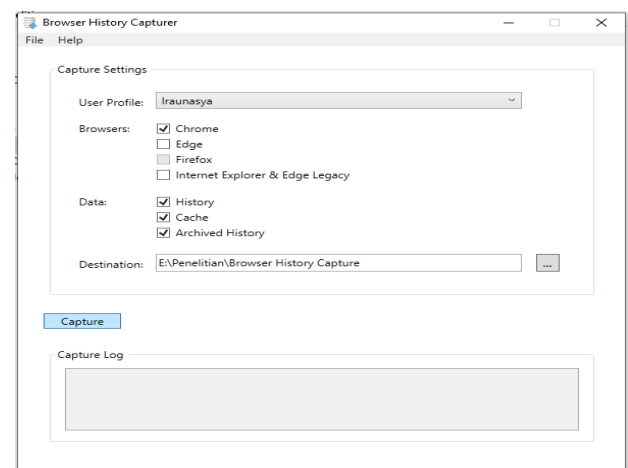


Figure 6. Start page browser history capturer

Figure 6 shows the browser history capturer. In this study, the browser that will be analyzed is the chrome browser, so in the "browser" section the investigator checks the chrome section. Meanwhile, in the "data" section, the investigator checked the History, Cache, Archived History section.

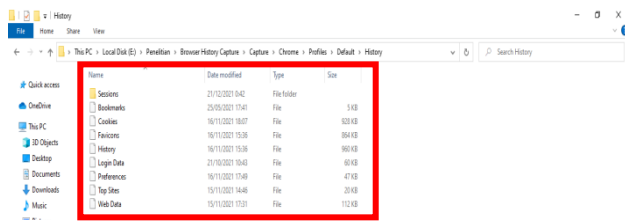


Figure 7. Fill in the captured history folder

Figure 7 shows the file contents of the History folder captured using the browser history capturer tool. In the History folder there is 1 folder with the name Sessions folder and 8 files with the file names Bookmarks, Cookies, Favicons, History, Login Data, Preferences, Top Sites, and Web Data. The next stage is to read the capture results on the browser history capturer tool using the browser history examiner tool and browser history viewer to obtain some data for digital evidence that strengthens the evidence at trial.

2.2.3 Analysis

The analysis stage is the stage to read and analyze the results that have been obtained at the Examination stage so that the resulting data is easy to read. This study uses several tools for the analysis process. The following are some of the tools used by the analyzer in this study.

2.2.3.1 Browser History Examiner

The analysis using the browser history examiner tool is carried out with the aim of analyzing the results obtained in the previous stage, namely the Examination stage.

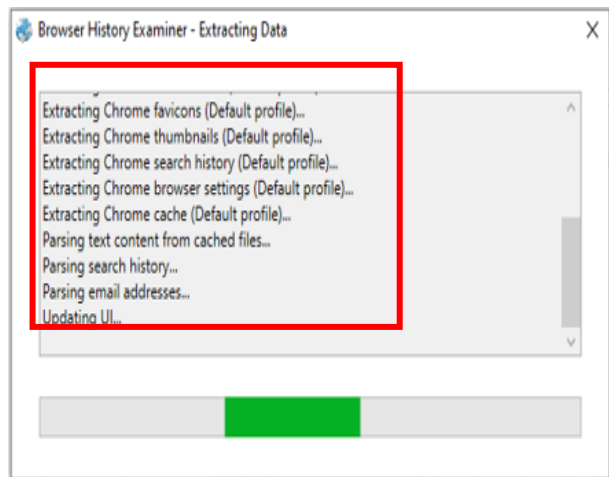


Figure 8. The process of analyzing in the Browser History Examiner application

Figure 8 shows the display during the process of generating data analysis obtained at the Examination stage. The results of the data obtained in the browser history examiner tool, which displays information on the chrome browser such as Bookmarks, Browser Settings, Cached Files, Cached Images, Cached Web Pages, Cookies, Downloads, Email Addresses, Favicons, From History, Logins, Searches, Session Tabs,

Thumbnails, Website Visits.

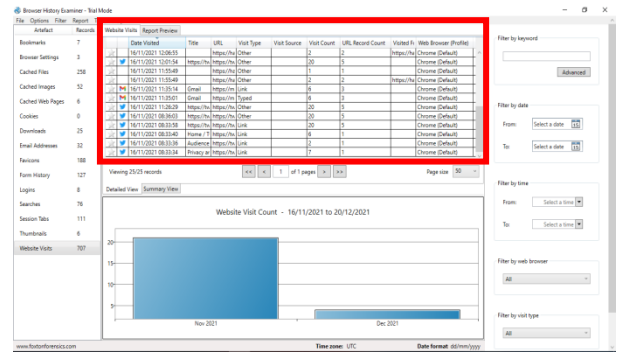


Figure 9. Website Visit as history data

Figure 9 shows "Website Visits" in the history of the chrome web browser. Figure 4.21 shows that the perpetrator accessed Twitter on November 16, 2021 at 12:01:54 and was done on the chrome browser.

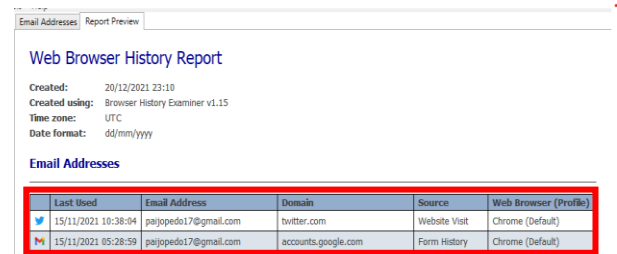


Figure 10. The perpetrator's username or email address

Figure 10 shows the email address of the perpetrator's laptop which was used to commit a digital crime that was captured on the login page, the perpetrator accessed twitter on the chrome browser on November 15, 2021 at 10:38:04.

2.2.3.2 Browser History Viewer

Browser history viewer is a tool used to analyze the results of the examination stage. This tool can generate the data needed in the trial. The data obtained in this tool is in the form of images captured in the browser history capturer application.

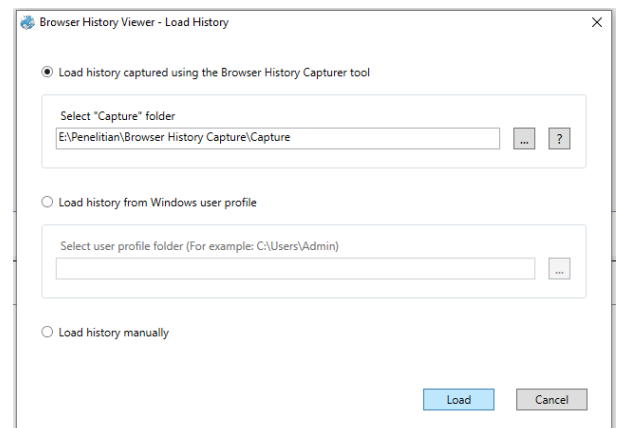


Figure 11. Browser history viewer tool

Figure 11 shows the initial view of the browser history viewer tool. Then click the file menu then click the load history menu, then it appears as shown in Figure 4.23. Then select the "Load history captured using the Browser History Capture tool" section and enter the location of the capture that was

obtained at the Examination stage.

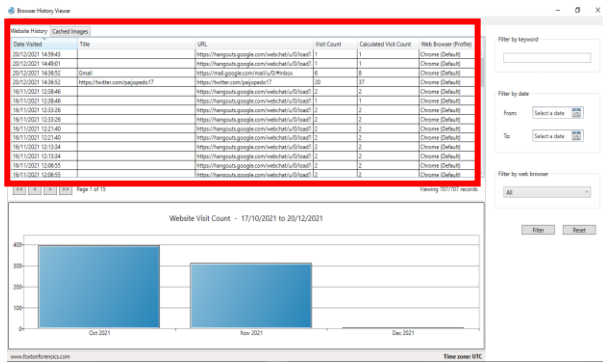


Figure 12. Extract Results

Figure 12 shows the initial view of the browser history viewer tool. Then click the file menu then click the load history menu, then it appears as shown in Figure 4.23. Then select the “Load history captured using the Browser History Capture tool” section and enter the location of the capture that was obtained at the Examination stage.

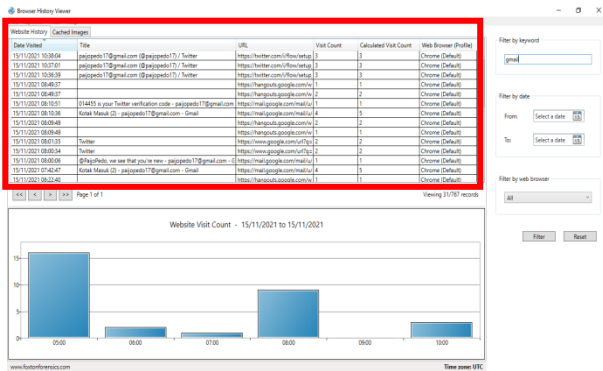


Figure 13. Evidence from Website History

Figure 13 shows the results from the website history with twitter parameters, the results obtained can be seen on the date of the incident, namely November 15, 2021 at 10:36:39 the perpetrator logged into a twitter account that was connected to a gmail account.

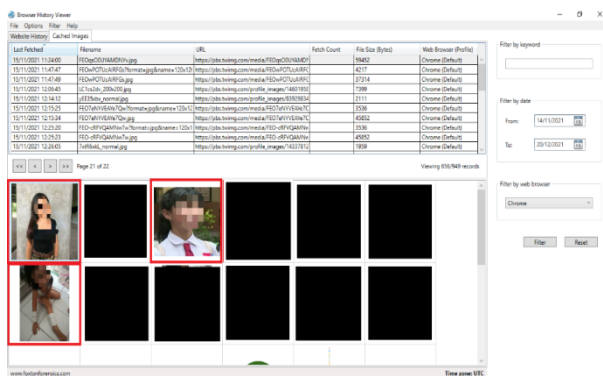


Figure 14. Proof of post photos from Cached Images

Figure 14 showing the results of photo posts made by perpetrators in the Cached Images category. The photo of the post was posted on November 15, 2021 at 11:24:00, at 11:47:49, and at 12:15:34 and there is some information about Filename, Url, File Size(Bytes), and Web Browser(profiles).

2.2.3.3 AccessData FTK Imager

The results obtained at the Examination stage which are carried out using the FTK Imager tool then produce the file name 20211116.mem which will be analyzed using the FTK Imager tool. The search results with the parameters "gmail" and "twitter" are like figure 15.

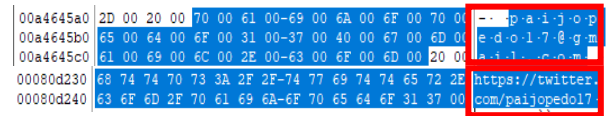


Figure 15. The perpetrator's email account and twitter username

Figure 15 is the email account and twitter username of the perpetrator that was found. The perpetrator used the email account p*****17@gmail.com and the twitter account @p*****17. Perpetrators login twitter by using the URL https://twitter.com which is accessed through the chrome browser.

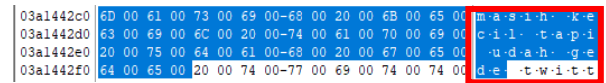


Figure 16. Proof of perpetrator's tweet post

Figure 16 is the perpetrator's tweet post. The perpetrator's tweets have context leading to harassment. From the results of the discovery of the perpetrator's posting data, it was found that the perpetrator's first tweet was “masih kecil tapi udah g*d*”. The perpetrator posted a comment on his first post, namely “kecilnya aja segitu apalagi gedanya”. Both posts have the intention of commenting on the victim's body shape. The posts of the two perpetrators that were found were yaitu “hobi aku suka anak sd”. The posts of the two perpetrators have the intention that the perpetrator has a sexual interest in small children. The third post that was found was “M*ngg*d* sejak dini”. The third post also intends to comment on the appearance of the victim. These posts lead to abuse of small children (victims) through social media twitter.

2.2.4 Reporting

Reporting is the last process that is carried out after obtaining digital evidence against the examination of analytical data carried out by the investigator. Reporting the results of the analysis includes an explanation of actions, identification of data results from forensic tools. This research software uses the Chrome browser using the Twitter web service.

Table 2. Findings of Evidence from Police

Evidence from the Police	Findings



Table 2 the digital data found in the RAM acquisition of the perpetrator's laptop in the form of text posts and cache from the web browser. The evidence found from the web browser is in the form of history in the chrome web browser, the email used in the chrome browser, the time used to access the chrome browser, cached images obtained when using the chrome browser.

2.2.5 Results

The results of the evidence that were successfully obtained with several tools used were then analyzed to find the history or history of web visits, access time, cache images, post caption text, email information, username and password for the perpetrator's account. The results can be seen in table 3.

Table 3. Results of twitter analysis based on google chrome web

No	Digital Evidence	Forensic Software			
		FTK Imager	Browser History Capture	Browser History Examiner	Browser History Viewer
1.	Image Post	-	✓	-	✓
2.	Text Posts	✓	✓	-	✓
3.	Link	-	✓	✓	✓
4.	Username	✓	✓	✓	✓
5.	E-mail	✓	✓	✓	✓
6.	Profile photo	-	✓	-	✓

Table 3 presents findings obtained from the analysis conducted on the Twitter service based on the Chrome web browser. The FTK Imager tool managed to get digital evidence in the form of text posts posted by the perpetrators, managed to get the perpetrator's twitter account username and the perpetrator's email. The Browser History Capturer tool generates a Capture folder containing Cache data and History data. Based on the Cache folder and the History folder, they managed to get digital evidence in the form of posting pictures, posting links, usernames, emails, and profile photos of the perpetrators. The Browser History Examiner managed to find digital evidence in the form of the link address used on the Chrome browser, the perpetrator's username and the perpetrator's email address. The Browser History Viewer tool managed to find digital evidence in the form of post images.

3. CONCLUSIONS

Based on the results of research that has been carried out with the title "Digital Data Retrieval on Web-Based Twitter Services using National Institute of Standard and Technology Method" which runs on the Chrome Browser service on Windows 10. The data used in this study were obtained from a scenario design made by the author by referring to cases that had occurred. This research scenarios cases of sexual violence that occur online through the twitter application. This case occurred through the twitter application which was accessed using a web browser on a laptop. The digital data retrieval process is carried out by acquiring ram using tools that support the data collection process such as Belkasoft Live RAM Capturer, Browser History Capture. Furthermore, the data were analyzed using the FTK Imager tool, Browser History Examiner, Browser History Viewer. The results of the evidence that were successfully obtained with several tools used were then analyzed and found history or history of web visits, access time, cache images, post caption text, email information, username and password for the perpetrator's account. The forensic process is carried out with several tools, the percentage of success of tools in obtaining digital data, namely FTK Imager is 50% successful, Browser History capture is 100% successful, Browser History Viewer is 100% successful, Browser History Examiner is successful 66%. The findings of the evidence are the same as the reports found by the police.

4. REFERENCES

- [1] SM Wisnu Budi, Aan Widayat Kusban, Muhammad, "Computer Forensic Analysis to Support the Investigation Process in Crime Cases," P. 12, 2015.
- [2] T. Rochmadi, "Live Forensics For Anti-Forensics Analysis On Private Portable Web Browser Live

- Forensics For Anti-Forensics Analysis On Private Portable Web Browser,” No. May, 2017.
- [3] R. Saputra And I. Riadi, “Forensic Browser Of Twitter Based On Web Services,” *Int. J. Comput. app.*, Vol. 175, No. 29, PP. 34–39, 2020.
- [4] M. Saifulloh And A. Ernanda, "Communication Privacy Management for Teenagers Using Alter Ego Accounts on Twitter," *Wacana, J. Ilm. Communal Science.*, Vol. 17, No. 2, P. 235, 2018.
- [5] Aprillia, I. (2017). *This Girl Has Experienced Sexual Harassment On Social Media, Here's How To Deal With Girlbanget.Grid.Id/Love-Life-And-Sex-Education/This-Girl-Has-Experienced-Sexual-Harassment-On-Social-Media-This-How-To Deal With It.*
- [6] N. Anwar And I. Riadi, "Forensic Investigation Analysis of Smartphone Messenger Whatsapp Against Web-Based Whatsapp," *J. Ilm. Tech. Electrical Computing. Dan Information.*, Vol. 3, No. 1, P. 1, 2017.
- [7] M. Riskiyadi, “Forensic Investigation of Digital Evidence in Revealing Cybercrime,” *Cybersecurity And Digit Forensics.*, Vol. 3, No. 2, PP. 12–21, 2020.
- [8] P. Widiandana, I. Riadi, And Sunardi, “Forensic Investigation Analysis of Cyberbullying on Whatsapp Messenger Using the Nist Method,” *Semin. Nas. technol. Fac. Engineering Univ. Krisnadwipayana*, Pp. 488–493, 2019.
- [9] A. Nofiyah, "Forensic Analysis of Web Phishing Using the National Institute Of Standards And Technology (Nist) Method," *Jstie (Jurnal Sarj. Tek. Inform.*, Vol. 8, No. 2, Pp. 11–23, 2020.
- [10] RAKN Bintang, R. Umar, And U. Yudhana, "Comparative Design of Live Forensics on Instagram, Facebook and Twitter Social Media Security in Windows 10," *Pros. Snst Ke -9 of 2018 Fak. Tek. Univ. Wahid Hasyim*, Pp. 125–128, 2018.
- [11] DT Yuwono, A. Fadlil, And S. Sunardi, “Performance Comparison Of Forensic Software For Carving Files Using Nist Method,” *J. Teknol. Dan Sist. Komput.*, Vol. 7, No. 3, Pp. 89–92, 2019.
- [12] S. Rachmie, “The Role of Digital Forensic Science Against Website Hacking Case Investigation,” *Litigation*, Vol. 21, No. 21, Pp. 104–127, 2020.
- [13] S. Dogan And E. Akbal, "Analysis Of Mobile Phones In Digital Forensics,” *2017 40th Int. Conv. Inf. Commun. Technol. Electron. M microelectrons. Mipro 2017 - Proc.*, pp. 1241–1244, 2017.
- [14] D. A. Putri and I. Riadi, “Forensic Mobile against Threat WhatsApp Services using National Institute of Standards Technology Method,” *Int. J. Comput. Appl.*, vol. 183, no. 30, pp. 1–8, 2021.
- [15] MN Faiz, R. Umar, And A. Yudhana, “Implementation of Live Forensics for Comparison of Browsers on Email Security,” *Jiska (Jurnal Inform. Sunan Kalijaga)*, Vol. 1, No. 3, PP. 108–114, 2017.
- [16] J. Bickford and P. Giura, “Safe Internet Browsing Using a Transparent Virtual Browser,” *Proc. - 2nd IEEE Int. Conf. Cyber Secur. Cloud Comput. CSCloud 2015 - IEEE Int. Symp. Smart Cloud, IEEE SSC 2015*, pp. 423–432, 2016.
- [17] I. Riadi, R. Umar, And IM Nasrulloh, “Digital Forensic Analysis on Frozen Solid State Drives Using the National Institute Of Justice (Nij) Method,” *Elinvo (Electronics, Informatics, Vocat. Educ.*, Vol. 3, No. 1, pp. 70–82, 2018.
- [18] AS Cahyono, “Anang Sugeng Cahyono, The Influence of Social Media on Social Change in Indonesian Society,” pp. 140–157.
- [19] N. Ainiyah, U. Ibrahimy, And S. Situbondo, “Millennial Adolescents and Social Media: Social Media as Educational Information Media for Millennial Youth,” Vol. 2, No. April, Pp. 221–236, 2018.
- [20] MS Nazir *Et Al.*, “The Impact of Twitter Use on Learning English,” *Spectrochim. Acta - Part A Mol. Biomol. Spectrosc.*, Vol. 192, No. 4, pp. 121–130, 2018
- [21] A. Husnusyifa, “Twitter is a type of microblogging social media that facilitates users to write their opinions. Historically, the presence and emergence of social media Twitter which provides a certain space or other social media, on the Twitter of other users,” *IDEA J. Hum.*, vol. 2, no. 2, pp. 120–133, 2019.
- [22] Y. Prayudi And DS Afrianto, “Anticipating Cybercrime Using,” *J. Fak. Huh. Uii*, Vol. 2005, No. Snati, 2005.
- [23] C. K. Herawati and I. Riadi, “Mobile Forensic of Facebook Services using National Institute of Standard Technology (NIST) Method,” *Int. J. Comput. Appl.*, vol. 183, no. 33, pp. 9–15, 2021.
- [24] YY H, “Verbal and Nonverbal Forms of Sexual Harassment of Female Workers (Content Analysis of Niki Caro's North Country Film),” 2007.
- [25] FN Rosyidah And MF Nurdin, “Distorted Behavior: Social Media as a New Space in Youth Sexual Harassment,” *J. Pemikir. And Researcher. social.*, Vol. 2, No. 2, PP. 38–48, 2018.
- [26] National Institute Of Standards AndTechnologyUs Department Of Commerce, “Nist Cybersecurity,” 2019.