

Web Forensic for Hate Speech Content on Twitter Services using National Institute of Standard Technology Method

Suryani

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 in addition to bringing many positive impacts also have negative impacts. The sophistication of various applications today allows the increase in crime cases online. These cases include gambling online, spreading hoax news, fraud, hate speech, cyberbullying, cyberporn, and other cyber cases. These crimes online are very often found in various social media applications, one of which is the Twitter application which is a social networking site that allows users to share things or events that are happening around the world. Users post tweets that can contain photos, videos, links, and text. This research conducts forensics on the Twitter application accessed via the web browser Chrome as the browser with the most users in Indonesia in 2020 according to Stat Counter. The research was conducted using case scenarios based on original cases obtained from various sources. The stages used in this research are the stages from the National Institute of Standards and Technology. These stages are collection, examination, analysis, and reporting. The process of collecting digital evidence is carried out using several forensic tools, namely Belkasoft RAM Capturer, FTK Imager, Browser History Capturer, and Browser History Viewer. This research produces digital evidence in the form of tweets previously deleted or posts that can be retrieved, along with other data. The percentage of results of the digital evidence that has been found successfully 100%. In Belkasoft RAM Capturer and FTK Imager is 50% with digital evidence of text posted, username, password, and web browser history. In Browser History Capturer and Browser History Viewer is 50% with digital evidence of image posted, web browser history, profile photo of the twitter account, and time accessed. The results of this research managed to find evidence of posts that have been deleted.

Keywords

Forensic, Hate speech, Twitter, Browser, NIST

1. INTRODUCTION

Information and communication technology is growing rapidly along with the discovery and development of science in the field of information and communication to help all mankind in accessing various information on the internet. Especially in the field of communication, not only can share information with certain people, but also with people around the world. Technological developments in addition to bringing many positive impacts also have negative impacts. The sophistication of various applications today, allows the increase in crime cases online, such as gambling online, the spread of news hoax, fraud, hate speech, cyberbullying, cyberporn, and other cyber cases. These crimes online are

very often found in various social media applications, one of which is the Twitter application.

These crimes can be analyzed and revealed through a digital forensics process. The process of disclosing digital evidence uses one of the stages used by investigators. The research stages used are methods from the National Institute of Standards and Technology (NIST) which consist of four stages, namely collection, examination, analysis, and reporting. The NIST method is a forensic method that has policy and standard work guidelines to ensure each examiner follows the same workflow so that work is documented and the results are repeatable and can be maintained[1].

1.1 Study Literature

1.1.1 Previous Study

This research refers to five previous studies, namely:

The first previous research entitled "Analysis of Forensic Investigations Cyberbullying on WhatsApp Messenger Using the method National Institute of Standards and Technology (NIST)." In this study, the process of evidence in the form of WhatsApp messages can be identified through the data acquisition process and analyzed using the method cosine similarity[1].

The second previous study with the title "Identification of Conversation Evidence Items for Applications Dual Apps WhatsApp on Xiaomi Phones Using the NIST Mobile Forensics Method." The tool that is the object of this research is the Smartphone Xiaomi Mi5 which has gone through the extraction process using Andriller and Laron. However, the process of using these two tools did not succeed in finding digital evidence in the form of WhatsApp conversations, so the extraction was done manually via the Android Debug Bridge (ADB)[2].

The third previous research is entitled "Digital Forensic Analysis of E-Commerce on Car Rental Websites Using the NIST Method." This study discusses the analysis process of a car rental website www.jetstarrental.com which has committed fraudulent actions. Conclusion Analysis of the website using ScamAviser shows a warning that the website is not safe. The results of the analysis using whoisdomain show that the website is registered through rumahWeb Indonesia and the owner's data server is under the Domain Data Guard located in Yogyakarta[3].

The fourth previous study entitled "NIST Method For Forensic Analysis of Digital Evidence on Android Devices" analyzed deleted data on the smartphone Samsung Galaxy J1 Ace, with the conclusion that the process recovery with the tool is Oxygen more recommended because the results

recovery reach 73% while recovery using tools Wondershare only reached 30%[4].

The last previous study entitled "Analysis and Comparison of Forensic Evidence for Social Media Applications Facebook and Twitter on Smartphones Android" found that all forensic evidence results on applications Facebook were found. Meanwhile, the Twitter application only managed to find an account name, location data, profile photo, cover photo, posts in the form of text, and posts in the form of images[5].

1.1.2 Digital Forensics

The handling of cybercrime cases is carried out through investigative activities known as digital forensics [6]. Digital Forensics is the application of computer science and technology for the benefit of legal evidence, which in this case is proving technological crimes or computer crimes that can be obtained scientifically to obtain digital evidence that can be used against violators[7]. Digital forensics arises from the number of crimes that occur in the use of computer systems as objects or as tools used for a crime or storage of evidence about a crime[8]. The purpose of digital forensics is to prove the existence of instructions that have occurred by conducting a crime scene investigation so that they can prove it from evidence such as computer systems, storage media, electronic documents, or data packets moving through computer networks [9]. The existence of evidence is very important in the investigation of cybercrime cases because, with the evidence, investigators can reveal cases of crimes that occurred with a complete chronology. In collecting digital evidence, several conditions or characteristics are needed so that digital evidence can be accepted by the court so that it can be followed up.

1.1.3 Web Browser

A web browser is a software used to access web pages to get clear and easy-to-read information. The information resource is identified with a Uniform Resource Identifier (URI) and will be a web page, image, video, or other content[10]. Web Browser is a tool to perform various activities on the Internet by users. Users use browsers for various functions such as information retrieval, access to email accounts, e-commerce, banking creation, instant messaging, online blogs, access to social networks [11]. Web browsers store large amounts of data about user activity during browsing, including cache files, Uniform Resource Identifiers (URLs), keywords, cookies[12]. Web browsers commonly used are: Mozilla Firefox, Google Chrome, Opera, and Apple Safari [13].

1.1.4 Digital Evidence

Digital evidence consists of 2 words, namely evidence and digital. Evidence is information that is used to establish or refute a fact. The evidence is divided into two, namely physical evidence and digital evidence[14]. Evidence from cases is cybercrime different from conventional crimes, where the handling of electronic evidence and digital evidence contained in it is susceptible to change or contamination, so electronic evidence must be packaged and stored properly in a safe place[15]. The evidence that has been obtained needs to be explored re-into some scenarios related to the investigation, including who has done it, what has been done (Example: use of any software), what process results were produced, when to do it[16]. Digital evidence is defined as electronic information such as electronic documentation, computer log files, data, reports, physical hardware, software, disk images, and so on, which are collected during computer investigations. However, it is not limited to, computer-generated files (such as log files

or generated reports) and human-generated files (such as spreadsheets, documents, or email messages)[17].

1.1.5 Twitter

Twitter is a website that offers a social network in the form of a microblog that allows users to send and read messages called tweets. According to [18] Twitter is also used to post various media such as images, videos, GIFs, links, as well as text with a limit of 280 characters known as tweets. Tweets will appear on the home page of other users who follow or follow, and vice versa. Users can reply, like, retweet, or resend a tweet posted by other users. In addition, users can also use the # sign (hashtag) to write messages based on topics[19]. Twitter can be accessed through various platforms such as iOS, Android, or a web browser by visiting the website www.twitter.com. Through the mobile application, Twitter is available on the Playstore and Appstore.

1.1.6 Hate Speech

Hate speech is termed as a form of *hate speech*. The word *hate* is positioned as a noun, so it means to hate. However, *hate* is positioned as a verb, it means to hate. In this context, *hate* is positioned as a noun, the same applies to speech[20]. Hate speech or hate speech is an utterance made by a person or group of people to a certain person or group that can indirectly hurt someone's heart or lead to bullying cases[21]. Hate speech is a linguistic phenomenon that is contrary to the concept of politeness in language as an indicator of linguistic intelligence and communication ethics [22]. Hate speech is defined as an utterance used to express hatred towards a person or group of people with the aim of insulting, humiliating. Hate speech can occur in various forms, such as Hate speech regarding religion, nationality, skin color, race, gender, and others[23].

1.1.7 National Institute of Standard Technology

The stages of the National Institute of Standard Technology are a forensic stage that has policy and standard work guidelines to ensure each examiner follows the same workflow so that work is documented and the results can be repeated and can be maintained [1].



Figure 1. Stages of NIST Method

Figure 1 represents 4 stages of NIST that can be used for the forensics process. The descriptions are as follows [24] :

1. Collection
The Collection stage is the process of labeling, identifying, recording, and retrieving data from relevant data sources with procedures to maintain integrity data.
2. Examination
The Examination stage is carried out by processing the data collected in the use of forensic combinations of various scenarios, either automatically or manually, as well as assessing the data and issuing data as needed while maintaining data integrity.
3. Analysis
The Analysis stage is the stage of analyzing the data that has been obtained using methods and techniques that are by applicable rules.
4. Reporting
The Reporting stage is the stage of reporting the results of the analysis which includes the description of the actions taken.

2. METHODOLOGY

2.1 Research Scenario

This research scenario is needed in the forensic process because it aims to carry out a forensic process on web-based Twitter to obtain and analyze evidence. In this research scenario, laptops are used as evidence that is suspected and will be investigated in crime research. The flow of the case scenario of this research can be seen in Figure 2.

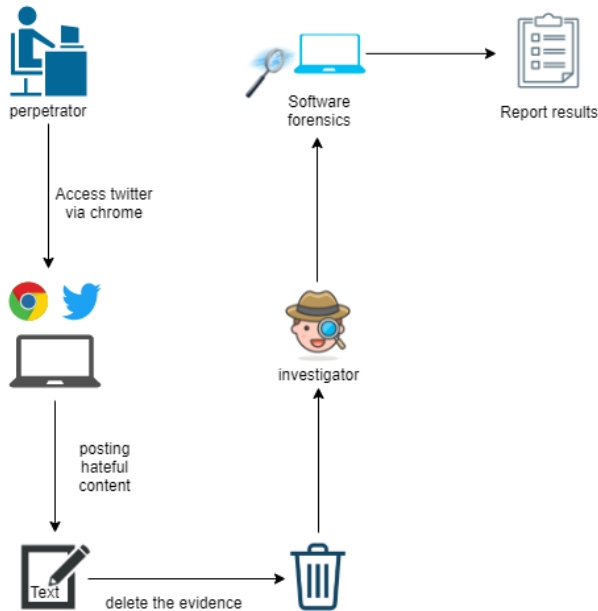


Figure 2. Flow of the Case Scenario on Twitter

Figure 2 shows the flow of case scenario which starts from the perpetrator accessing Twitter via the web browser Chrome which is already installed on the perpetrator's laptop. The perpetrator posted an article along with an image that led to a form of hate speech against a group. The Twitter account is in a conditioned public so that the post is spread and can be seen by the wider community, both those who follow the account and those who do not. People who felt aggrieved by the post reported it to the police by successfully submitting evidence in the form of screenshots of the perpetrator's tweet to the police before the post was deleted again by the perpetrator. The police secured evidence and carried out an investigation assisted by forensic experts to find digital evidence on the laptop used by the perpetrator to spread the hate speech content to obtain data related to hate speech cases on Twitter.

2.2 Research Stages

This implementation stage is carried out by investigators by carrying out a series of plots or activities carried out in the research process to find digital evidence. The purpose of the research scenario is to describe a simulation of the research process carried out based on criminal cases on Twitter that have occurred. The steps or stages used in this research use the National Institute of Standard and Technology (NIST) stages which have four stages, namely Collection, Examination, Analysis, and Reporting.

2.2.1 Collection

The data collection stage is the stage carried out to find, collect, and document the evidence that exists at the location of the case. The evidence will be secured to maintain the authenticity of the evidence because it will be used in the

investigation process. The evidence that is the object of this research is electronic evidence in the form of a laptop with a Windows operating system in which the Google Chrome application is installed which is indicated to be used by the perpetrator as a tool to commit crimes cyber. In addition to laptop evidence, other electronic evidence was also found, namely the laptop charger cable used by the perpetrator to charge the laptop.

Tabel 1. Physical Evidence Found



No	Name	Image	Description
1	Laptop of the perpetrator		Asus Zenbook that is found is online and connected to the internet
2	Laptop charging cable		The charging cable

Table 1 displays documentation of physical evidence found at the scene of the incident which was later collected by the police and handed over to investigators.

2.2.2 Examination

Stage Examination is a very important stage in the investigation process. At this stage, inspection, testing, and extracting information will be carried out from the data that has been collected. The investigation process at this stage will begin with data acquisition on the perpetrator's laptop. The data will be acquired using forensic tools aimed at obtaining a history of activity from Random Access Memory (RAM).

2.2.2.1 Belkasoft RAM Capturer

Forensic tools used in performing data acquisition is Belkasoft RAM Capturer. The Belkasoft RAM Capturer tool will capture memory on the perpetrator's laptop. The duration of time required to make an acquisition depends on the amount of RAM capacity on the perpetrator's laptop.

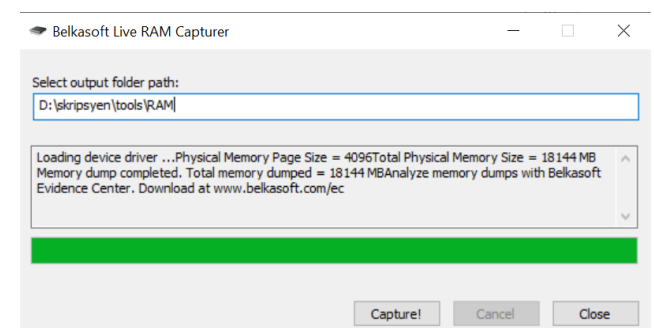


Figure 3. RAM Capturer Acquired Successfully

Figure 3 shows that capturing the RAM has been successfully carried out. The results of the RAM acquisition from the perpetrator's laptop are stored in the specified folder and adjusted to the section that says "Select output folder path". It can be seen in Figure 3 that the acquisition results will be

stored on partition D in the skripsyen\tools\RAM folder. During the acquisition process, there was information about the RAM size of the laptop, which was 18144 Megabytes (MB). The results of capturing the RAM obtained a file that has a size of approximately 18 GB. with the name is 20210920 and in .mem format.

2.2.2.2 FTK Imager

The imaging process is the next stage in the acquisition process which is carried out on the results of the acquisition. The imaging process is carried out so that the integrity of the data is maintained and cannot be changed so that it can be continued to the inspection stage. FTK Imager is a tool used in the imaging process.

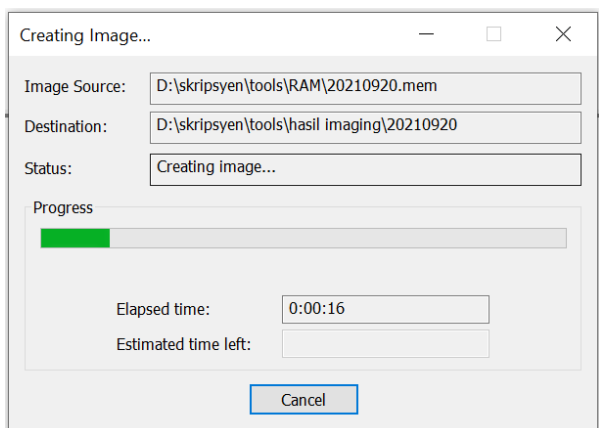


Figure 4. Process of Imaging Data

Figure 4 shows the process of imaging files from the results of Capture RAM 20210920.mem. Files of the Capture memory that are on drive D which are stored in the \skripsyen\tools\RAM\ folder which is then carried out by the imaging process will be stored in a different folder namely \skripsyen\tools\hasil imaging folder.

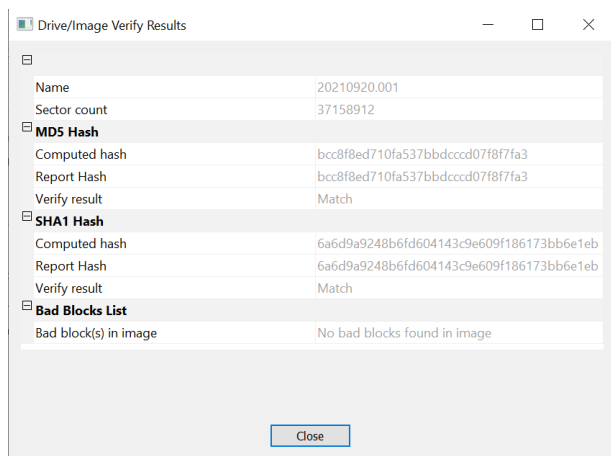


Figure 5. the Hashing Results of RAM

Figure 5 shows the hash value of the imaging results of Random Access Memory. There are two hashing results, namely the hash value in MD5 and the hash value in SHA1. The result of the two files is a match or match. The same hash value indicates that the imaging process was carried out perfectly, meaning that there were no changes to the file.

2.2.2.3 Browser History Capturer

Process Capture History is carried out to obtain results capture from the browser used by the perpetrator as a medium to

spreadcrime cyber content. Browser History Capturer tool can obtain data from web browsers Chrome, Edge, Firefox, as well as Internet Explorer & Edge Legacy. The data obtained can be in the form of web browsing history and cache.

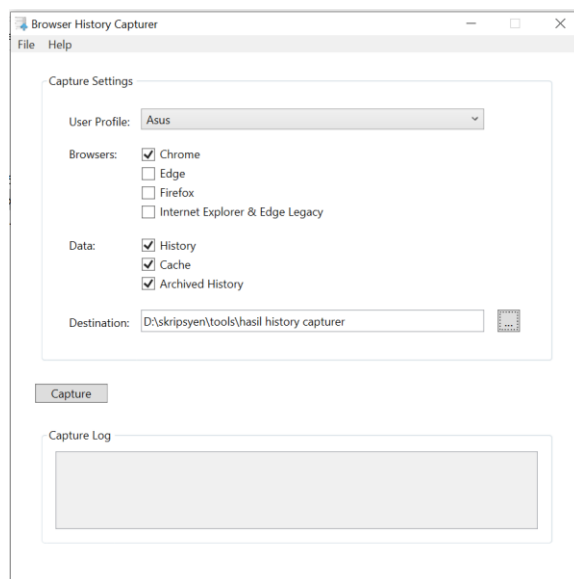


Figure 6. Display of Browser History Capturer

Figure 6 shows the initial view of Browser History Capturer. The 'sectionCapture Settings' is used to select the user profile, the type of browser used, the data you want to capture, and the 'Destination' section is the destination where the results are stored. Perpetrators spread hate speech content on Twitter that is accessed using the browser Chrome, so only a checklist is made on the browser Chrome, besides that, a checklist is also carried out on all types of data to be obtained.

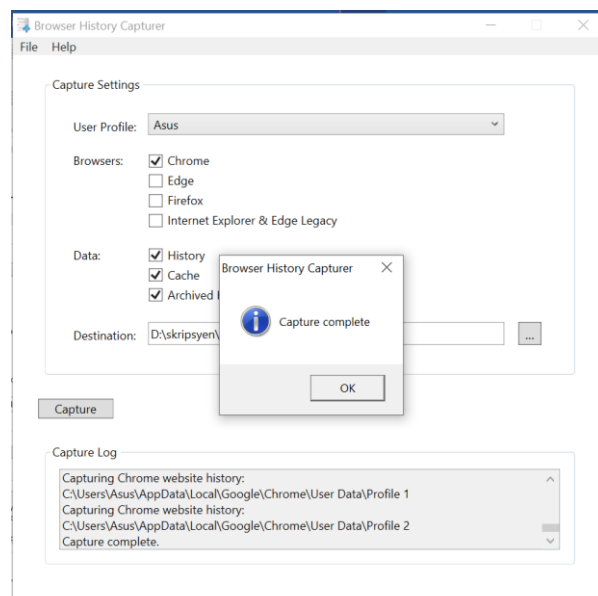


Figure 7. Process of Capturing Data from Browser Chrome

Figure 7 is a display of when the data capture process from the Chrome browser is successfully carried out. The results of the capture are stored in drive D:\skripsyen\tools\hasil history capturer.

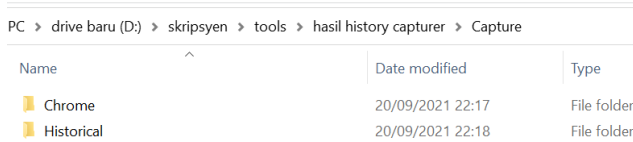


Figure 8. Capture Results File of Browser Chrome

Figure 8 shows the results of file Capture that a standalone into a folder named Capture. In the Capture folder, there are two more folders, namely Chrome and Historical. This research will take data from the two folders.

2.2.3 Analysis

The analysis stage is the stage to analyze and read the results of the data that has been obtained from the stages Collection to Examination. This analysis stage is carried out aiming to match the information obtained with the required information needs so that the information that will be issued is as needed and still maintains the integrity of the data. The results of the analysis of these data will be assessed and conclusions are drawn to be entered into the stage Reporting.

2.2.3.1 Analysis with FTK Imager

The previous stage has been carried out by using a RAM data acquisition tool Belkasoft RAM Capturer results obtained with the file name 20210920 shaped .mem format.



Figure 9. File of RAM Acquisition

The acquired file in Figure 9 will be analyzed using the tool FTK Imager to obtain the required information and data that will be used as digital evidence.

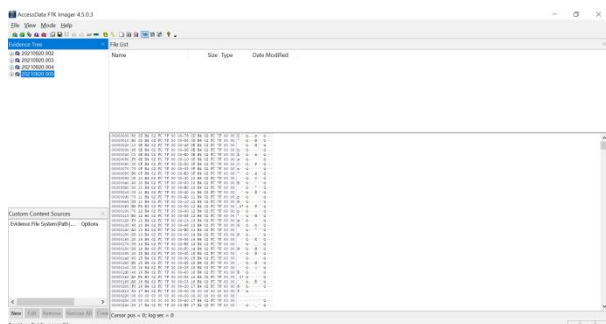


Figure 10. Display of FTK Imager

The display of FTK Imager can be seen in Figure 10. FTK Imager was used to read the results of Capture RAM. The column in the upper left corner displays the file items that have been added for analysis. The process of adding an item is done by clicking the File menu Add Evidence Item, then a dialog box will appear.

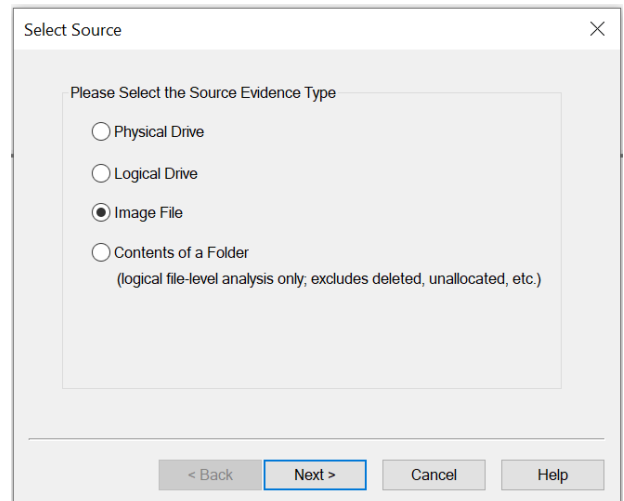


Figure 11. "Add Evidence" Dialog Box in FTK Imager

Figure 11 is the dialog box of Add Evidence. In the section 'Please Select the Source Evidence Type' select Image File, then go to the location of the acquired file and add the files to be analyzed to the FTK Imager. In the search process, investigators use the find feature by pressing the ctrl + f keys on the keyboard and then entering certain keywords related to the existing evidence. This is done to facilitate the search for digital evidence.

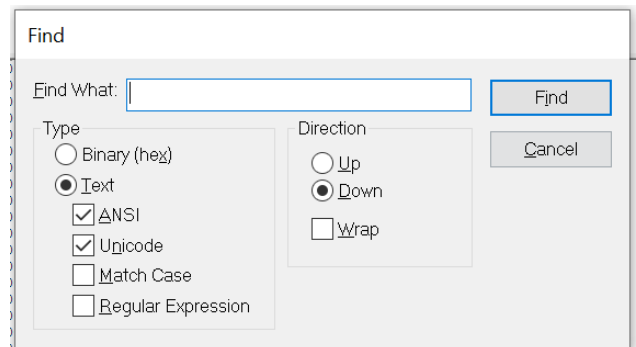


Figure 12. Parameter Search Process

Figure 12 shows the search by entering parameters in the 'Find What' column then pressing the 'Find' button. The first searched parameter is "Twitter", to obtain information that the perpetrator has accessed Twitter to commit a crime.

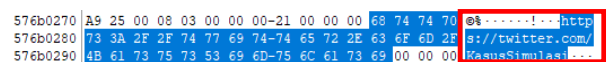


Figure 13. First Results for FTK Imager

Figure 13 shows that the perpetrator has accessed Twitter through the website <https://twitter.com/KasusSimulasi> and obtained a Twitter account with the name 'kasussimulasi'.

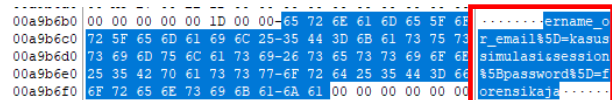


Figure 14. Second Results for FTK Imager

Figure 14 is the username and password used by the perpetrator to login to the Twitter account. There is a username with the name 'kasussimulasi' with the password 'forensikaja' which strengthens the evidence that the account with the username 'kasussimulasi' is an account belonging to

the perpetrator according to the screenshot evidence reported by the victim.

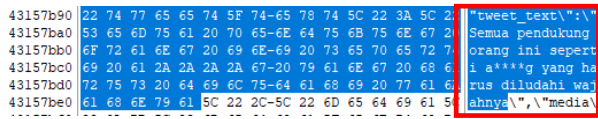


Figure 15. Third Results for FTK Imager

Figure 15 shows evidence in the form of text posted by the perpetrator on the Twitter account of the perpetrator which reads "Semua pendukung orang ini seperti a****g yang harus diludahi wajahnya". The sentence matches the screenshot the victim gave to the police.

2.2.3.2 Analysis with Browser History Viewer

Browser History Viewer is a tool used to read results Capture browser that has been carried out at the Examination stage using the Browser History Capturer tool. This tool can generate the data needed in the trial. The data obtained in this tool are images taken in the browser history capture application [25]. The data obtained from the tool are in the form of Website History, Cache Images, and Cached Web Pages.

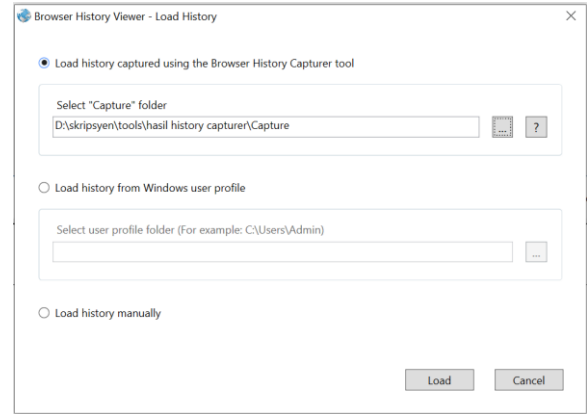


Figure 18. Load History of Browser Chrome File Capture

Figure 18 shows the dialog box of Load History. In the section 'Select "Capture" folder', find the location of the Capture Browser folder, namely on drive D:\skripsyen\tools\hasil history capturer\Capture then add it, then click the button 'Load' to analyze to the Browser History Viewer.

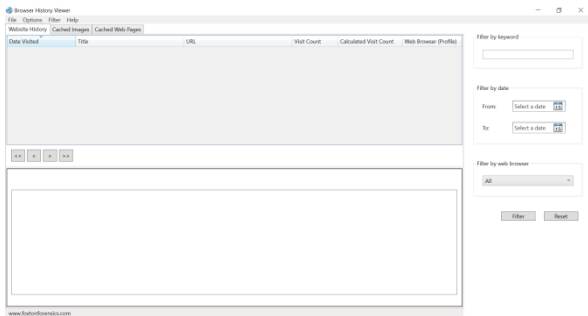


Figure 16. Display of Browser History Viewer

Figure 16 shows the display of the tool Browser History Viewer. In the previous stage, namely the Examination stage has been captured the Chrome browser by Browser History Capturer which results in a folder with the name Capture as shown in Figure 17. In this analysis, data will be retrieved from that folder.



Figure 17. The Result File of Capture Browser

Figure 17 shows the result file of the Capture Browser using Browser History Viewer tool. The result file data will be shown by clicking the file, then selecting the section 'Load History', and a dialog box will appear.

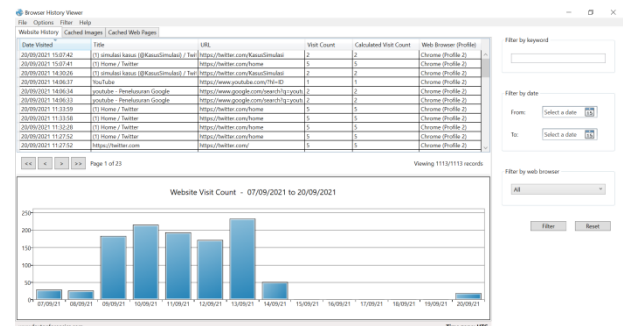


Figure 19. Data of Browser History

Figure 19 displays the data results of Capture the Chrome browser. The top left displays the information of Website History, Cache Images, and Cached Web Pages. On the right, three functions are used to make searching easier, namely 'Filter by Keyword' to search for data using certain keywords, 'Filter by date' to search for data according to a certain date, and 'Filter by web browser' to display activities only in browser the selected.

Date Visited	Title	URL	Visit Count	Calculated Visit Count	Web Browser (Profile)
20/09/2021 15:07:42	(1) simulasi kasus (@KasusSimulasi) / Twi	https://twitter.com/KasusSimulasi	2	2	Chrome (Profile 2)
20/09/2021 15:07:41	(1) Home / Twitter	https://twitter.com/home	5	5	Chrome (Profile 2)
20/09/2021 14:30:26	(1) simulasi kasus (@KasusSimulasi) / Twi	https://twitter.com/KasusSimulasi	2	2	Chrome (Profile 2)
20/09/2021 14:00:17	YouTube	https://www.youtube.com/watch?v=...	1	1	Chrome (Profile 2)
20/09/2021 14:00:14	google - Penelusuran Google	https://www.google.com/search?q=...	2	2	Chrome (Profile 2)
20/09/2021 14:00:13	google - Penelusuran Google	https://www.google.com/search?q=...	2	2	Chrome (Profile 2)
20/09/2021 11:33:59	(1) Home / Twitter	https://twitter.com/home	5	5	Chrome (Profile 2)
20/09/2021 11:33:58	(1) Home / Twitter	https://twitter.com/home	5	5	Chrome (Profile 2)
20/09/2021 11:33:28	(1) Home / Twitter	https://twitter.com/home	5	5	Chrome (Profile 2)
20/09/2021 11:27:52	(1) Home / Twitter	https://twitter.com/home	5	5	Chrome (Profile 2)
20/09/2021 11:27:51	https://twitter.com	https://twitter.com/	5	5	Chrome (Profile 2)
20/09/2021 11:27:40	Login on Twitter / Twitter	https://twitter.com/login	2	2	Chrome (Profile 2)
20/09/2021 11:27:40	Login on Twitter / Twitter	https://twitter.com/login	2	2	Chrome (Profile 2)

Figure 20. The Search Results Using Keyword "Twitter"

In the analysis process using the keyword "Twitter" to facilitate the search, the data that appears is only data related to Twitter, as in Figure 20, showing the history when the perpetrator logged into the perpetrator's Twitter account on 20/09/2021 at 11:27:40 through the web browser Chrome. On the same date but at a different time, until 15:07:42, it can be seen that the perpetrator is still accessing the Twitter account, besides that several other activities are also related to Twitter.

Time Accessed	Date Visited	Title	URL
	20/09/2021 15:07:42	1) simulasi kasus (@KasusSimulasi) / Twi	https://twitter.com/KasusSimulasi
	20/09/2021 15:07:41	1) Home / Twitter	https://twitter.com/home
	20/09/2021 14:30:26	1) simulasi kasus (@KasusSimulasi) / Twi	https://twitter.com/KasusSimulasi
	20/09/2021 11:33:59	1) Home / Twitter	https://twitter.com/home
	20/09/2021 11:33:58	1) Home / Twitter	https://twitter.com/home
	20/09/2021 11:32:28	1) Home / Twitter	https://twitter.com/home
	20/09/2021 11:27:52	1) Home / Twitter	https://twitter.com/home
	20/09/2021 11:27:52	https://twitter.com	https://twitter.com/
	20/09/2021 11:27:51	https://twitter.com	https://twitter.com/
	20/09/2021 11:27:40	login on Twitter / Twitter	https://twitter.com/login
	20/09/2021 11:27:40	login on Twitter / Twitter	https://twitter.com/login

Table 3 shows the findings of the evidence. There are the text posted by the perpetrator, username (@kasussimulasi) and password (forensikaja) of the perpetrator's Twitter account, and the web browser history. Browser History Capturer is used as a tool to record all activities on the web browser Chrome, which then is read using Browser History Viewer. It is found that the evidences are the images posted by the perpetrator, the web browser history, profile photo of the perpetrator Twitter account, and the time in the form of date and time of access.

3. CONCLUSION

The forensic process carried out with hate speech cases on web-based Twitter services has succeeded in obtaining digital evidence using the forensic tools. Belkasoftware RAM Capturer and FTK Imager found the digital evidence as much as 50% of text posted, username, password, and web browser history. Browser History Capturer and Browser History Viewer tools found the digital evidence as much as 50% of image posted, web browser history, profile photo of the twitter account, and time accessed. This research uses the stages of National Institute of Standard Technology so that it can be developed by using different stages. In addition, this research uses the Windows 10 operating system, so for further research it can be developed on other operating systems, such as Linux and macOS.

4. REFERENCES

[1] P. Widiandana, I. Riadi, and Sunardi, "Cyberbullying Forensic Investigation Analysis on Whatsapp Messenger Using the NIST Method" *Semin. Nas. Teknol. Fak. Teknik Univ. Krisnadwipayana*, pp. 488–493, 2019, [Online]. Available: <https://jurnal.teknikunkris.ac.id/index.php/semnastek2019/article/view/308>.

[2] D. Hariyadi and I. Y. Pasa, "Dual Apps Whatsapp on Xiaomi Smartphones" *J. INTEK*, vol. 1, pp. 1–7, 2018.

[3] G. H. A. Kusuma and Y. Fadhilah, "Digital Forensic Analysis of E-Commerce on Car Rental Websites Using the NIST Method" *Pros. Semin. Nas. SISFOTEK*, vol. 3, no. 1, pp. 228–234, 2019.

[4] R. Umar and Sahiruddin, "NIST Method For Forensic Analysis Of Digital Evidence On Android Devices" *Pros. SENDU_U_2019*, pp. 978–979, 2019.

[5] W. A. Mukti, S. U. Masrurroh, and D. Khairani, "Analysis and Comparison of Forensic Evidence Facebook and Twitter Social Media Applications on Android Smartphones" *J. Tek. Inform.*, vol. 10, no. 1, pp. 73–84, 2018, doi: 10.15408/jti.v10i1.6820.

[6] N. Iman, A. Susanto, and R. Inggi, "Analysis of the Digital Forensics in Cybercrime Investigations in Indonesia (Systematic Review)" *J. Telekomun. dan Komput.*, vol. 9, no. 3, p. 186, 2020, doi: 10.22441/incomtech.v9i3.7210.

[7] I. Riadi, R. Umar, and A. Firdonsyah, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," *Int. J. Comput.*

Sci. Inf. Secur., vol. 15, no. 5, pp. 3–8, 2017.

[8] A. Fauzan, I. Riadi, and A. Fadlil, "Digital Forensic Analysis On Line Messenger For Cybercrime Handling" *Annu. Res. Semin.*, vol. 2, no. 1, pp. 159–163, 2017, [Online]. Available: <http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/832/752>.

[9] S. Marini, "Digital Forensic Studies in Regulation in Indonesia" *Semin. Nas. Energi Tek*, pp. 103–106, 2018.

[10] T. Rochmadi, "Live Forensics for Anti-Forensic Analysis on a Web Browser Browzar Study Case" *Indones. J. Bus. Intell.*, vol. 1, no. 1, p. 32, 2019, doi: 10.21927/ijubi.v1i1.878.

[11] M. Jannah, "Forensic Browser on Line Messenger Services for Handling Cyberfraud using National Institute of Standard Technology Method," vol. 183, no. 30, pp. 9–16, 2021.

[12] 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.

[13] D. Setiawan, R. Setiawan, R. Karunia, and I. W. S. Wicaksana, "Comparing Web Browser Performances" *Ilmu Komput. Univ. Gunadarma*, vol. 1, no. 1, pp. 1–6, 2007.

[14] K. Widatama, "Digital Evidence Storage Cabinet Concept Using XML Language Structure" no. September, pp. 8–14, 2017.

[15] A. Ivanović, *The Way of Handling Evidence of Criminal Offences of Computer Crime*. 2018.

[16] Y. Prayudi and D. S. Afrianto, "Anticipate Cybercrime Using Forensic Computer Techniques" *J. Fak. Huk. UII*, vol. 2005, no. Snati, 2005, [Online]. Available: <https://www.neliti.com/publications/88691/antisipasi-cybercrime-menggunakan-teknik-komputer-forensik>.

[17] M. S. Ahmad, I. Riadi, and Y. Prayudi, "Live Forensics Investigation From User Side To Analyze Man in the Middle Attack Based on Evil Twin" *Ilk. J. Ilm.*, vol. 9, no. 1, pp. 1–8, 2017, doi: 10.33096/ilkom.v9i1.103.1-8.

[18] M. Saifulloh and A. Ernanda, "Communication Privacy Management for Teenagers Alter Ego Account Users on Twitter" *WACANA, J. Ilm. Ilmu Komun.*, vol. 17, no. 2, p. 235, 2018, doi: 10.32509/wacana.v17i2.652.

[19] R. Saputra and I. Riadi, "Forensic Browser of Twitter based on Web Services," *Int. J. Comput. Appl.*, vol. 175, no. 29, pp. 34–39, 2020, doi: 10.5120/ijca2020920832.

[20] M. Musyafaa, "Hate Speech: Perspectives and Ethics in Cyber Media" *J. Ilm. Syi'ar*, vol. 17, no. 2, p. 21, 2017, doi: 10.29300/syr.v17i2.891.

[21] H. Nurhairani and I. Riadi, "Analysis Forensics Mobile on Twitter Application using the National Institute of Justice (NIJ) Method," *Int. J. Comput. Appl.*, vol. 177, no. 27, pp. 35–42, 2019, doi: 10.5120/ijca2019919749.

[22] D. J. Ningrum, S. Suryadi, and D. E. Chandra Wardhana, "Hate Speech Study on Social Media" *J. Ilm. KORPUS*, vol. 2, no. 3, pp. 241–252, 2019, doi: 10.33369/jik.v2i3.6779.

- [23] T. Davidson, D. Warmesley, M. Macy, and I. Weber, “Automated hate speech detection and the problem of offensive language,” *Proc. 11th Int. Conf. Web Soc. Media, ICWSM 2017*, pp. 512–515, 2017.
- [24] A. Yudhana, I. Riadi, and I. Anshori, “Facebook Messenger Digital Evidence Analysis Using the NIST Method” *It J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.
- [25] C. K. Herawati, “Forensic Browser on Facebook Services using National Institute of Standards Technology Method,” vol. 183, no. 30, pp. 17–24, 2021.