Forensic Browser on Facebook Services using National Institute of Standards Technology Method

Cintia Kus Herawati
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta Indonesia

ABSTRACT
Advances in science and technology are increasingly developing, making the process of disseminating information easier. Social media is one of the media that serves to disseminate information. Facebook is one of the social media applications with 82% of users based on the total population in Indonesia. The high number of Facebook users makes many possibilities for digital crimes or cybercrime. Cybercrime is a crime that is carried out by making the computer a tool, target, and place of crime. One example of cybercrime that has the most cases is the spread of hoax news. Hoax is fake news that spreads and harms a certain party. In this study, will looked for digital evidence of the process of spreading hoax content that is accessed through the Chrome browser. This research was conducted using case scenarios adapted to the original case. The forensic process is carried out using the live forensic method by following the NIST (National Institute of Standards and Technology) stages, namely collection, examination, analysis, and reporting. This study uses forensic tools such as ftk imager, belkasoft RAM capture, browser history capture, browser history examiner, browser history viewer, and history reader. This study produces digital data that is by the evidence from the victim who was submitted to the police as report material. The data found were in the form of captions of the perpetrator's posts, comment text, history of web visits, web access time, usernames of perpetrators and victims' accounts, and cache images.Success of 50% in the form of text posts,link posts while the remaining 50% is found for images.

Keywords
Cybercrime, Facebook, Hoax, Live Forensic, BrowserT

1. INTRODUCTION
The progress of science and technology in the digital era is now growing very rapidly. Technology develops along with the convenience provided to be able to disseminate information. Information that is spread to the public can be in the form of positive or negative information.Hoax content is false or misguided news that is widespread in the community.The hoax content that spreads can come from individuals or organizations that intentionally create hoax content with the aim of seeking profit and harming other parties.Social media is one example of media that functioned as a tool for disseminating news. Facebook is an example of a social media application. Crime acts in the IT world are very diverse. Crime in cyberspace is known as Cybercrime. One of the crimes that occur in the IT world is the case of spreading hoax content on Facebook. One of the crimes that occur in the IT world is the case of spreading hoax content on Facebook.

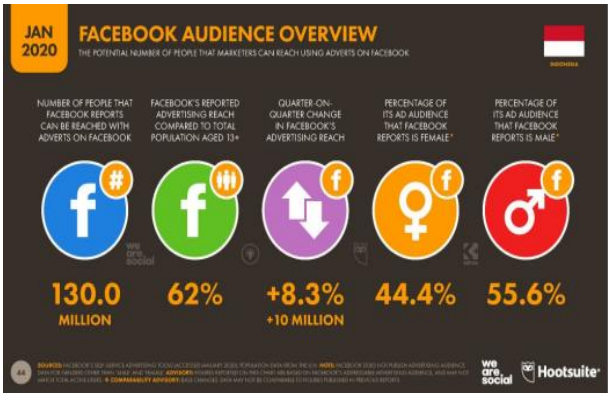


Figure 1. Facebook users in Indonesia (We Are Social, 2020)

Figure 1 describes the percentage of Facebook service users in Indonesia in 2020 that comes from We Are Social. Based on the total population in Indonesia, users of Facebook services are 82%. Service users of Facebook in Indonesia in 2020 amounted to 130 million

1.1.1 Previous Study
Majesty Fitriana, Khairan AR, Soul Malem Regis (2020), entitled "Implementation Method National Institute Of Standards And Technology (NIST) in Forensic Analysis Digital To Handling Cyber Crime" in this study discussing the software perpetrators are KingRoot (Smartphone Rooting tool), CWM (ClockworkMod) Recovery (installed CWM files), Flashify (to install CWM), AccessData FTK Imager (data imaging), WhatsApp Viewer (decrypts encrypted WhatsApp messages and opens WhatsApp messages decrypted), DB Browser for SQLite (opens wa.db folder to display phone contact details). The results in this previous study are the appearance of deleted WhatsApp chats, text messages, WhatsApp contacts, and the time of sending and receiving messages. [1]

WahyuIndriyanto, Dedy Hariyadi, Muhammad Habibi (2020) entitled "Digital Forensic Investigation and Analysis in Whatsapp Group Conversations Using NistSp 800-86 and Support Vector Machine" in this study discusses the results of SVM analysis resulting in negative sentiment values in messages group by 96.21%. The reason is that the structure of the use of words in group messages is too short. The use of the Subject-Predicate-Object-Description rule has not been applied to group messages. Therefore, message analysis using SVM has not reached the target [2].

RauhullohAyatulloh Khomeini Noor, Bintang, Rusydi Umar, Anton Yudhana (2020) entitled "Facebook Lite Social Media Analysis with Forensic tools using the NIST Method" in this

study discusses the research process using the Galaxy J2 Android Smartphone, the steps are taken are rooting the smartphone, and download the Facebook Lite application, send posts, and carry out the investigation process using the MOBILedit Forensic tool, after an analysis using the forensic tool then obtains the analysis results as digital evidence as supporting evidence in court. The results of the data obtained in the use of the forensic tool MOBILedit Forensic are ID, image, audio, video accounts that apply the National Institute Of Standards Technology (NIST) method[3].

Moh. Riskiyadi (2020) entitled "Forensic Investigation of Digital Evidence in Revealing Cybercrime" in this study discusses the results of forensic investigation research analysis of digital evidence originating from evidence in the form of flash disks, different treatment on flash disks gives different results in forensic analysis, showing values the hash is not equal from the given differential treatment. The results of file analysis on the first and second flash disk treatments, all simulation files that were stored in the flash disk before reformatting could be detected or recovered, but the third treatment did not get any file types. The FTK Imager and Autopsy software have not been able to perform data acquisition and analysis with permanent deletion and encryption (password) on a flash disk using Windows 10 built-in tools. [4]

SyukurIkhsani and BektiCahyoHidayanto (2016) entitled "Forensic Analysis of Whatsapp and LINE Messenger on Android Smartphones as a Reference in Providing Strong and Valid Evidence in Indonesia" this study discusses references in digital forensics, namely the WhatsApp application. While the LINE Messenger application is safer because it is not easy to analyze [5].

1.1.2 Digital Forensics

Digital Forensics is the application of computer science and technology that is used for the benefit of legal evidence (pro justice), to prove crimes that use high technology or computers naturally in order to utilize digital evidence against criminals [6]. Digital forensics is a field of science that combines the fields of computer science with law[7]. In digital forensics, there are two methods, namely static forensics and live forensics [8]. The digital forensic investigation framework consists of four phases: Preparation, Collection, Analysis, and Presentation [9].

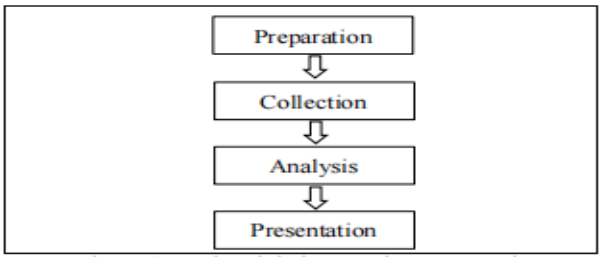


Figure 2.Digital forensic framework

Figure 2 describes the framework of a digital forensic investigation framework consisting of four phases: Preparation, Collection, Analysis, and Presentation.

Digital forensics can help technically in the collection of digital evidence to be presented in a trial in accordance with applicable law[10].

1.1.3 DigitalEvidence

Evidence is data sent or stored using a mobile device or computer that denies or supports a particular crime, or provides clues that point to important elements related to a violation [11].Digital evidence is information stored or transmitted in binary form that can be relied upon in court[12]. Digital evidence is evidence that is retrieved or recovered from electronic evidence. Forensic analysts must search for digital evidence, which can then investigate the connections between criminal cases[13]. Digital evidence from the Live Forensic process is legal evidence based on Law Number 11 of 2008 concerning Information and Electronic Transactions[14]. Digital evidence is evidence in the form of document files, history files, or log files containing data related to a cybercrime case obtained from file extraction on electronic evidence [15].

1.1.4 Web Browser

Web browser is an application or software used to search or surf the Internet in order to obtain information from a web[16]. A web browser is a program that can be used to retrieve HTML documents from a web server application that can be used to search and find various information. Popular web browsers are such as Mozilla Firefox, Internet Explorer, Google Chrome, and Opera [17].

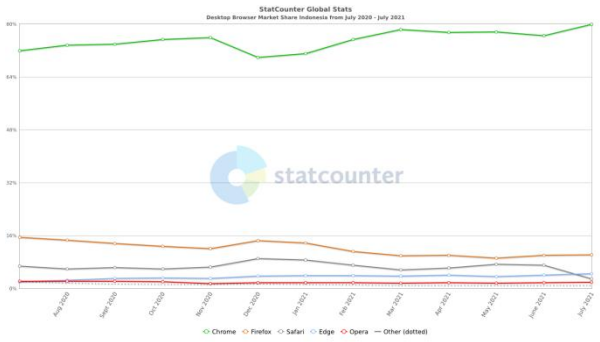


Figure 3. Desktop Browser Market Share Indonesia (July 2020 - July 2021)

Figure 3 explains the percentage of web browser usage in July 2020 - July 2021. Chrome browser is a web browser that has the highest percentage every year.

1.1.5 Cybercrime

Cybercrime is a crime committed by using a computer or computer network as a tool, target and place of crime, including child pornography, online fraud, bullying, identity fraud, and others [1]. Cybercrime according to the United Nations: any illegal behavior carried out through a victim's computer system or system or network, including crimes such as illegally possessing, offering or distributing information through a computer system or network[18]. Crimes committed on social media users can be identified through analysis of Volatile data contained in RAM [3]. Cybercrime can be interpreted as the use of computers as a tool to commit various modes of crime [19].

1.1.6 Content Hoax

Hoax is information or news that contains things that are not certain. Now information or news that is considered true is no longer easy to find. Not only by the mainstream media, but hoaxes are also now circulating in the community through online media. Channels that are widely used in the spread of

hoaxes are websites, at 34.90%, chat applications (Whatsapp, Line, Telegram) at 62.80%, and through social media (Facebook, Twitter, Instagram, and Path) which are the most common media. used which reached 92.40% [20].

1.1.7 Overview of Facebook Services Facebook

is a social media service with a very fast development in the IT world. Facebook has many features that make users comfortable using it. The features available on Facebook are that users can post photo and video content, there is a messenger feature that can be used to communicate with other Facebook account users and there is a story feature that can be used to post activities that are being carried out by the owner of the Facebook account then it will disappear automatically after 24 hours.

1.1.8 National Institute of Standards Technology

The National Institute of Standards and Technology (NIST) forensic method is a forensic method that has policy work guidelines and standards to ensure each examiner follows the same workflow so that work is documented and the results are repeatable and can be maintained [21].

Figure 4. Stages of the NIST Method

Figure 4 There are several stages in the NIST method, namely collection, examination, analysis, and reporting. The cellular stage of Forensic Analysis can be explained as follows:

1. Collection is labeling, identification, recording, and retrieval of data from data sources which is relevantwith the following procedures to maintain data integrity.

2. Examination is the processing of data collected in the forensic use of various combinationsscenarios, either automated or manual, and assessing and outputting data as needed whilemaintain data integrity.

3. Analysis is the analysis of the results of the examination using technically justified and legal methods.
4. Reporting is reporting the results of the analysis which includes the description of the actions taken.

2. Methodology

2.1 Research Scenario This

research will discuss digital forensics that is on a web-based Facebook service to reveal a crime case of spreading hoax content with digital evidence.The Facebook service is a type of social media application that has the opportunity for criminal acts to occur which is used by criminals. The method for this web forensic research is the National Institute of Standard Technology (NIST) by applying the steps contained in the method, which is expected to obtain evidence. digital. The hope of this research is that it can be a reference in investigating cases of spreading hoax content through social media.

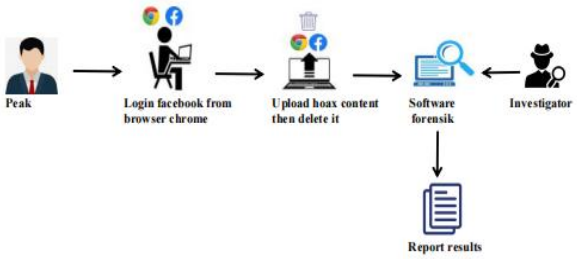


Figure 5.Flow of the Evidence Search Process

Figure 5 describes the scenario of how the perpetrators upload hoax content that spreads on the Facebook service running on the chrome browser. Those who feel aggrieved then report the content to the police. The laptop used by the suspect became evidence for imaging using forensic applications. Then the case is investigated by investigators using digital forensic software. The results of the investigation are in the form of digital evidence.

2.2 Research Stages

This research has stages where the case study simulation process can be carried out in stages to try to find evidence of crime from the Facebook web application based on digital evidence. The research stages can refer to the NISTmethod*(National Institute of Standards and Technology* [22]*).*

Figure 6.Stages of Implementation

Figure 6 describes the stages of NIST (National Institute of Standards and Technology) there are four steps taken to obtain digital evidence from the results of investigations of digital forensic crime cases. The following is an explanation of the implementation stages.

2.2.1 Collection

The stage includes identifying relevant data sources related to cases, labeling and recording[23]. At the collection stage, the initial stage is used by investigators to search for, collect, and identify evidence obtained at the location of digital crimes. The process of collecting evidence is 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.In table 1 below, the specifications of the laptop used by criminals are listed below.

Table 1.Digital Evidence

No	Digital Evidence	Picture	Information
1	Perpetrator's Laptop		The Asus-branded prepetrator's laptop was found to be alive and conneted to the internet network.
2	Laptop Charging Cable		The charging cable

Evidence collected will be subject to an acquisition process to view and look for digital evidence of evidence found. The laptop used by the perpetrator is an Asus brand with an Intel® Core™ i3-6006U CPU @ 2.00GHz, 4096MB RAM storage and storage A 1TB HDD with a Windows 10 OS found by the police with the condition turned on and connected to an internet connection. At the investigation stage, there are several paths that investigators must follow to obtain digital evidence. The following is the investigation flow that must be carried out by the investigator.

2.2.2 Examination

The examination stage is the main stage that must be carried out in conducting investigations to acquire data on laptops as evidence used by perpetrators in committing digital crimes. The process of acquiring a laptop is carried out using *live forensics*, namely the process of acquiring or returning data is carried out while the laptop is on and connected to an internet connection. The examination stage is the stage of examining and collecting simulation evidence data [24].

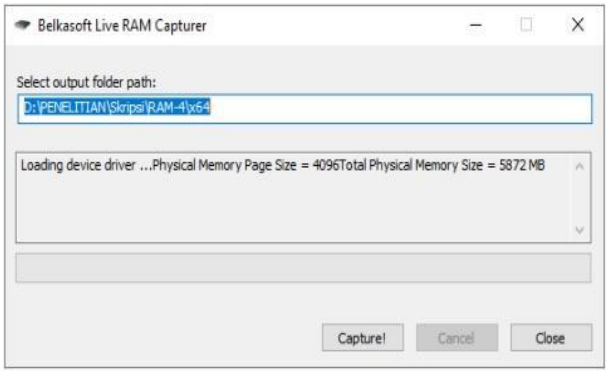


Figure 7. Tools Belkasoft Live RAM Capturer

Figure 7 shows the Belkasoft Live RAM Capturer tool when it acquired the perpetrator's laptop RAM. The results of the acquisition process will be stored in the storage that has been selected in the "Select output folder path" section.In this study, the results of the acquisition of the perpetrator's laptop RAM are stored on partition D in the PENELITIAN\Skripsi\RAM-4\x64 folder. If the location for storing the acquisition results is in accordance with what is desired, then to start acquiring data from the perpetrator's laptop RAM, by clicking the "Capture!".

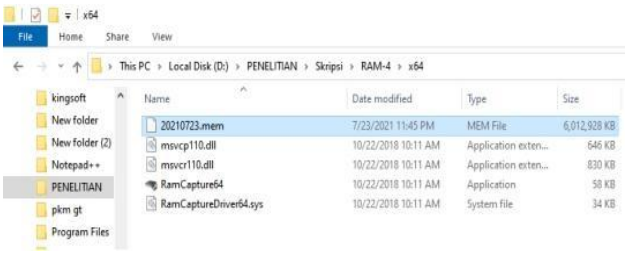


Figure 8. Results of Acquisition of Belkasoft Live RAM Capturer

Figure 8 shows the file names of the perpetrators' laptop RAM data acquisition results. The results of the RAM data acquisition on the perpetrator's laptop are named 20210723.mem with a storage size of 6,012,928 KB. The resulting .mem file will then be hashed using *thetool* FTK *Imager*.

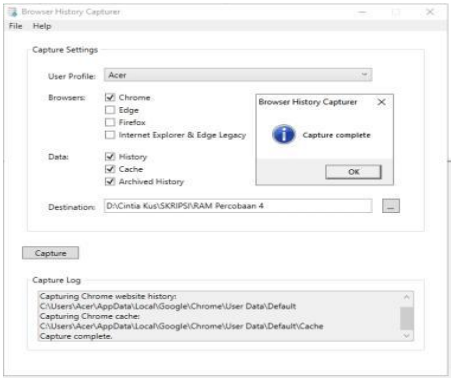


Figure 9. Capturer tool browser history capturer

Figure 9 shows the capture process on the browser history capturer tool has been successfully carried out.

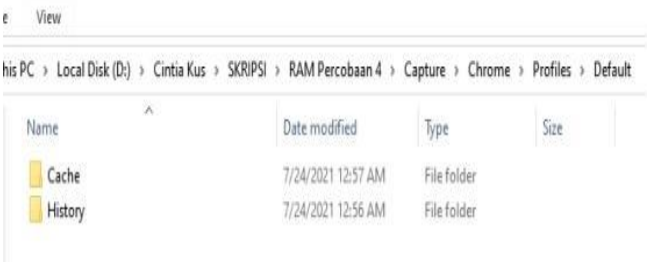


Figure 10. Contents of the capture folder

Figure 10 shows the results of the capture on the chrome browser, namely the Cache folder and the History folder.

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

Analysis using the browser history examiner tool is carried out to analyze the results obtained in the previous stage. The results of the data obtained in the browser history examiner tool, which displays information contained in 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.

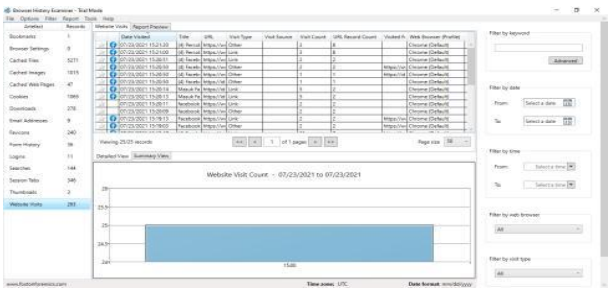


Figure 11. Website Visit as history data

Figure 11 displays "Website Visits" in the chrome web browser history. Figure 4.26 shows that the perpetrator accessed Facebook on July 23, 2021 at 15:21:20 and was done on the chrome browser.

Web Browser History Report

Created: 07/24/2021 01:41
Created using: Browser History Examiner v1.15
Time zone: UTC
Date format: mm/dd/yyyy

Email Addresses

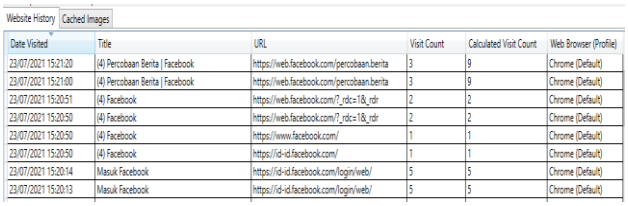
Last Used	Email Address	Domain	Source	Web Browser (Profile)
07/23/2021 14:32:19	percobaanberitahoax@gmail.com	web.facebook.com	Form History	Chrome (Default)

Figure 12. User name or email address of the perpetrator

Figure 12 displays the email address of the perpetrator's laptop used to commit a digital crime that was successfully captured on the login page, the perpetrator accessed Facebook in the Chrome browser on July 23, 2021 at 14:32:19 with the address email experiment beritahoax@gmail.com.

2.2.3.2 Browser History Viewer

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



Website History | Cached Images

Date Visited	Title	URL	Visit Count	Calculated Visit Count	Web Browser (Profile)
23/07/2021 15:21:20	(4) Percobaan Berita | Facebook	https://web.facebook.com/percobaan.berita	3	9	Chrome (Default)
23/07/2021 15:21:00	(4) Percobaan Berita | Facebook	https://web.facebook.com/percobaan.berita	3	9	Chrome (Default)
23/07/2021 15:20:51	(4) Facebook	https://web.facebook.com/?_rdc=1&_rdr	2	2	Chrome (Default)
23/07/2021 15:20:50	(4) Facebook	https://web.facebook.com/?_rdc=1&_rdr	2	2	Chrome (Default)
23/07/2021 15:20:50	(4) Facebook	https://www.facebook.com/	1	1	Chrome (Default)
23/07/2021 15:20:50	(4) Facebook	https://id-id.facebook.com/	1	1	Chrome (Default)
23/07/2021 15:20:14	Masuk Facebook	https://id-id.facebook.com/login/web/	5	5	Chrome (Default)
23/07/2021 15:20:13	Masuk Facebook	https://id-id.facebook.com/login/web/	5	5	Chrome (Default)

Figure 13. Evidence from Website History

Figure 13 shows the results from website history with Facebook parameters, the results obtained can be seen on the date of the incident, namely July 23, 2021 at 15:20:13, the perpetrator logged into the Facebook account using the User Name News Trial.

Figure 14. Figure 4.33 Proof of posting photos from Cached Images

Figure 14 shows the photos posted by perpetrators in the Cached Images category. The photo of the post was posted on July 23, 2021 at 14:54:56 and there is some information about Filename, Url, File Size(Bytes), and Web Browser(Profile).

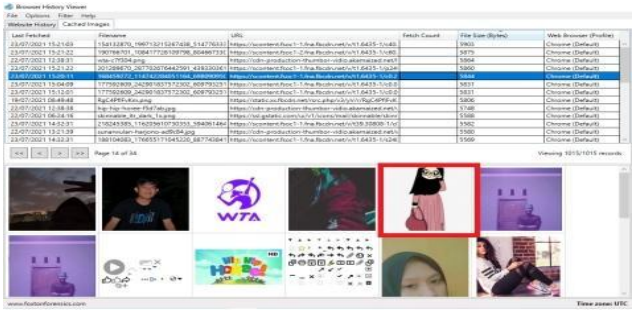
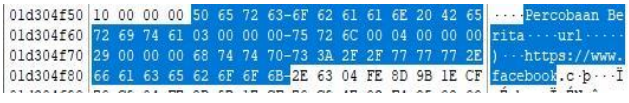


Figure 15. Proof of the victim's profile photo from CachedImages

Figure 15 shows proof of the profile photo of the victim's account with the user name CintiaHerawati on July 23, 2021 at 15:20:11. The proof of the photos from Facebook corresponds to the URL address on each photo and occurs in the Chrome web browser.

2.2.3.3 Analysis With FTK Imager

Tools FTK Imager as the manager of the data to be analyzed [25]. The results obtained at the stage, *Examination* which was carried out by the perpetrator's laptop RAM acquisition, resulted in the file name 20210723.mem which would be analyzed using the FTK Imager tool.



```
01d304f50  10 00 00 00 50 65 72 63-6F 62 61 61 6E 20 42 65  ····Percobaan Be
01d304f60  72 69 74 61 03 00 00 00-75 72 6C 00 04 00 00 00  rita····url·····
01d304f70  29 00 00 00 68 74 74 70-73 3A 2F 2F 77 77 77 2E  )···https://www.
01d304f80  66 61 63 65 62 6F 6F 6B-2E 63 04 FE 8D 9B 1E CF  facebook.c·þ···Ï
```

Figure 16. The result of the perpetrator's facebook user name

Figure 16 is the search result with the parameter "Facebook" as the username of the facebook account. The name of the perpetrator's facebook account is @Percobaanberita then login to Facebook using the URL https://www.facebook.

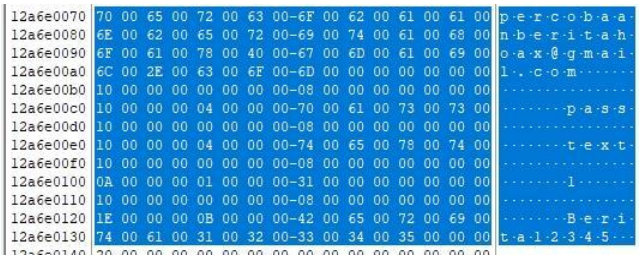


Figure 17. Evidence of passwords

Figure 17 is the finding of criminal account passwords. The perpetrator's account password is "Berita12345".

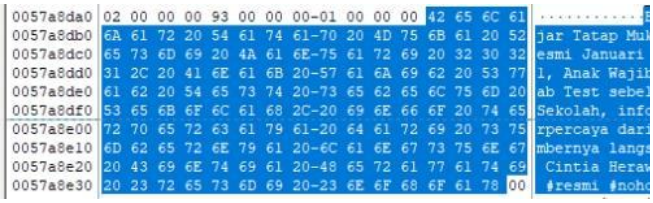


Figure 18. Finding captions for the perpetrator's posts.

Figure 18 shows the search results with the parameter "resmi" as in Figure 15, which shows the results of the caption that has been deleted by the perpetrator on the Facebook account with the user name of the new trial.

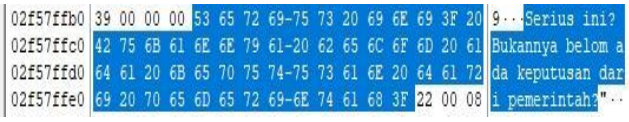


Figure 19. Findings of the first comment

Figure 19 shows the findings of the comment statement stating "Seriusini?Bukannyabelomadakeputusandaripemerintah?".

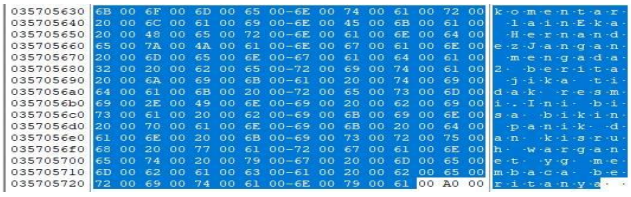


Figure 20. The findings of the second comment

Figure 20 shows the text of the second comment from Eka Hernandez's account which states "Jangan mengada2 berita, jikatidakresmiinibisabikinpanikdankisruhwarganetygmembacaberitanya".

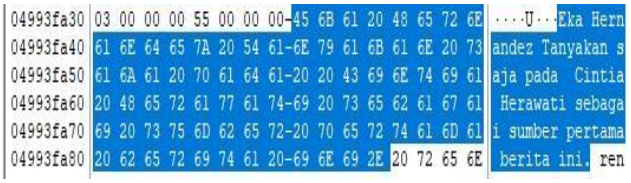


Figure 21. The findings of the third comment

Figure 21 shows the results of the conversation text findings on the comments given by the perpetrator's account (@PercobaanBerita) on the text the perpetrator answered "@Eka Hernandez Tanyakansajapada @CintiaHerawatisebagaisumberpertanyaanberitaini".

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. Information on hardware specifications for this study using a Windows 10-based laptop.

Table 2. Hardware Evidence This

No.	Nama	Keterangan
1.	*Processor*	Intel® Core™ i3-6006U CPU @ 2.00GHz
2.	*Graphics*	Intel ® HD Graphics 520 & NVIDIA GeForce MX110
3.	*Memory*	4096MB RAM
4.	*Harddisk*	1TB 5400 rpm SATA HDD

Researchs software uses the Chrome browser using the service *Facebook* web. This study uses several inspection steps so that it can obtain digital evidence. The analysis of the evidence was carried out using several forensic tools, from an analysis of the service *Facebook* web. The results of the analysis were carried out using tools such as Table 3.

Table 3. Analysis on Facebook Web Browser Chrome

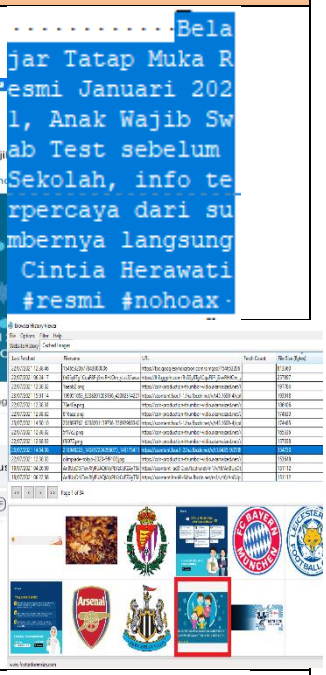
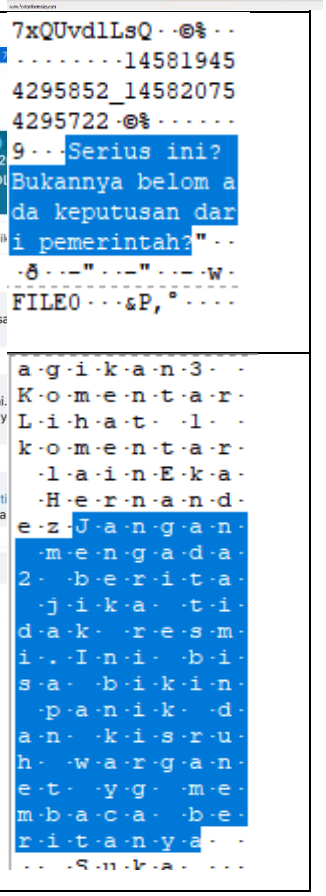
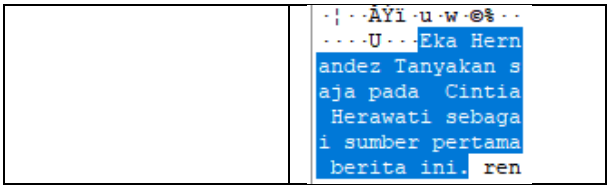
No	Evidence Digital	Software Forensik			
		FTK Imager	Browser History Capture	Browser History Examiner	Browser History Viewer
1	Post Pictures	-	✔	-	✔
2	Post Text	✔	✔	-	-
3	Link	-	✔	✔	✔
4	User Name	✔	✔	✔	-
5	Text comment	✔	-	-	-

In table 3 explains that the FTK Imager tool managed to get digital evidence in the form of text posts posted by the perpetrator, managed to get the username of the perpetrator's Facebook account (News Trial) and the victim (CintiaHerawati), then managed to get the text of the message conversation between the perpetrator and the victim. 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 text, posting links, usernames, profile photos of perpetrators and profile photos of victims. The Browser History Examiner managed to find digital evidence in the form of the perpetrator's user name (News Experiment) and the link address used on the Chrome browser.

2.2.5 *Results*

Basically *tools* are tools used to help obtain digital evidence. Evidence obtained from *tools* forensiccan be seen in table 4.

Table 4. Findings and evidence from victims

Digital evidence from victims	Findings
	
	
	

Based on table 4 there are similarities between evidence from victims used for reporting and digital evidence found by investigators after forensics was carried out. The evidence found in the acquisition of the perpetrator's laptop RAM was in the form of text posts and cache from the web browser. The evidence found from the web browser is in the form of a history of visits to the chrome browser, the email used in the chrome browser, the time used to access the chrome browser, cached images obtained when using the chrome browser.

3. CONCLUSION

The process of searching for digital evidence by collecting evidence found then acquiring ram using tools that support the data collection process such as Belkasoft Live RAM Capturer, Browser History Capture. After obtaining the data, then the data is analyzed using the FTK Imager tool, Browser History Examiner, Browser History Viewer. The results obtained from the forensic process of the Chrome browser by capturing RAM and cache using the live forensic method with the help of several tools, then analyzed to find digital evidence such as passwords, email accounts, text posts, the perpetrator's Facebook account username, the victim's Facebook account username. , and cached images. The findings of the evidence are the same as the report submitted by the victim to the police.

4. REFERENCES

[1] M. Fitriana, KA AR, and JM Marsya, "Application of the National Institute of Standards and Technology (Nist) Methods in Digital Forensic Analysis for Handling Cyber Crime," *Cybersp. J. Educator. Technol. inf.*, vol. 4, no. 1, p. 29, 2020, doi:10.22373/cj.v4i1.7241.

[2] MW Indriyanto, D. Hariyadi, and M. Habibi, "Digital Forensics Investigation and Analysis on Whatsapp Group Conversations Using NistSp 800-86 and Support Vector Machine Digital Forensics Investigation and Analysis on Whatsapp Group Chats Using NistSp 800-86 and Support Vector Machine," *Cyber Security. and Digit Forensics.*, vol. 3, no. 2, pp. 34–38, 2020.

[3] RA Bintang, R. Umar, and A. Yudhana, "Facebook Lite Social Media Analysis with Forensic Tools using the NIST Method," *Techno (Journal of Faculty of Tek. Univ. MuhammadiyahPurwokerto)*, vol. 21, no. 2, p. 125, 2020, doi:10.30595/techno.v21i2.8494.

[4] M. Riskiyadi, "Forensic Investigation of Digital Evidence in Revealing Cybercrime," *CyberSecurity and Forensic Digits.*, vol. 3, no. 2, pp. 12–21, 2020.

[5] S. Ikhsani and BC Hidayanto, "Forensic Analysis of Whatsapp and LINE Messenger on Android Smartphones as a Reference in Providing Strong and Valid Evidence in Indonesia," *J. Tek. ITS*, vol. 5, no. 2, 2016, doi:10.12962/j23373539.v5i2.17271.

[6] I. Riadi, S. Sunardi, and S. Sahiruddin, "Forensic Analysis of Recovery on Android Smartphones Using the

National Institute Of Justice (NIJ) Method," *J. RekayasaTeknol. inf.*, vol. 3, no. 1, p. 87, 2019, doi:10.30872/jurti.v3i1.2292.

[7] MS Asyaky, "Analysis and Comparison of Digital Evidence of Instant Messenger Applications on Android," *J. Researcher. Tech. information.*, vol. Vol. 3 No., No. 1, pp. 220–231, 2019.

[8] M. NurFaiz, W. AdiPrabowo, and M. FajarSidiq, "Comparative Study of Digital Forensics Investigations on Crime," *J. Informatics, Inf. syst. Softw. eng. app.*, vol. 1, no. 1, pp. 63–70, 2018, doi:10.20895/INISTA.V1I1.

[9] H. Iskandar *et al.*, "Digital Forensics Investigation Procedures of Smart Grid Environment," 2011.

[10] WY Sulistyo, I. Riadi, and A. Yudhana, "Application of SURF Techniques in Image Forensics for Digital Photo Engineering Analysis," *JUITA J. Inform.*, vol. 8, no. 2, p. 179, 2020, doi:10.30595/juita.v8i2.6602.

[11] T. Lestari *et al.*, "Proceedings of JOINT _ U 2019 ISBN : 978-979-3649-99-3 Proceedings of SENDI _ U 2019 ISBN : 978-979-3649-99-3," *Pros. SENDU_U_2019*, vol. 21, no. 1, pp. 978–979, 2019.

[12] I. Riadi, A. Yudhana, and MCF Putra, "Acquisition of Digital Evidence on Android-Based Instagram Messenger Using the National Institute Of Justice (NIJ) Method," *J. Tek. information. and Sis. inf.*, vol. 4, no. 2, pp. 219–227, 2018.

[13] BY Prasetyo and I. Riadi, "Investigation Cyberbullying on Kik Messenger using National Institute of Standards Technology Method," *Int. J. Comput. app.*, vol. 174, no. 17, pp. 34–41, 2021, doi:10.5120/ijca2021921060.

[14] SD Utami, C. Carudin, and AA Ridha, "Live Forensic Analysis on Whatsapp Web for Proving Electronic Transaction Fraud Cases," *Cyber Secur. and Digit Forensics.*, vol. 4, no. 1, pp. 24-32, 2021, doi:10.14421/csecurity.2021.4.1.2416.

[15] M. Riskiyadi, "Forensic Investigation of Digital Evidence in Revealing Cybercrime," *Cyber Secur. and Digit Forensics.*, vol. 3, no. 2, pp. 12–21, 2020, doi:10.14421/csecurity.2020.3.2.2144.

[16] H. HARIANI, "Web Browser Exploration in Searching Digital Evidence Using Sqlite," *J. INSTEK (Informatics Science and Technology*, vol. 6, no. 1, p. 66, 2021, doi: 10.24252/instek.v6i1 .18638.

[17] 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.

[18] 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.

[19] TE WIJATMOKO, "DIGITAL forensic READINES INDEX (DiFRI) FOR MEASURING READINESS RESPONSE Cybercrime ON REGIONAL OFFICE MINISTRY OF JUSTICE aND HUMAN rIGHTS DIY," *Cyber Secur. andForensic*Digits.,vol. 4, no. 1, pp. 18–23, 2021, doi: 10.14421/csecurity.2021.4.1.2235.

[20] C. Juditha, "Interaction of Hoax Communication in Social Media and its Anticipation," *J. Pekommas*, vol. 3, no. 1, pp. 31–34, 2018.

[21] P. Widiandana, I. Riadi, and Sunardi, "Investigative Analysis Forensic Cyberbullying on Whatsapp Messenger Using the NIST Method," *Semin. Nas. Technol. Fac. Engineering Univ. Krisnadwipayana*, pp. 488–493, 2019, [Online]. Available: https://jurnal.teknikunkris.ac.id/index.php/semnastek2019/article/view/308.

[22] MI Syahib, I. Riadi, and R. Umar, "Acquisition of Digital Evidence for Viber Applications Using the National Institute of Standards Technology (NIST) Method," *J-SAKTI (Journal of Komput. dan Inform.*, vol. 4, no. 1, p. 170, 2020, doi: 10.30645/j-sakti.v4i1.196

[23] MB Pakarti, DH Fudholi, and Y. Prayudi, "Digital Evidence Management to Improve Accessibility During the Covid-19 Pandemic, "*J. Ilm. SINUS*, vol. 19, no. 1, p. 27, 2021, doi: 10.30646/sinus.v19i1.502.

[24] Imam Riadi, Rusydi Umar, and MI Syahib, "Acquisition of Digital Evidence Viber Messenger Android Using the National Institute of Standards and Technology (NIST)," *MethodJ. RESTI (System Engineering and Information Technology)*, vol. 5, no. 1, pp. 45–54, 2021, doi: 10.29207/resti.v5i1 .2626.

[25] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Designing Digital Forensics on Twitter Applications Using Live Forensics Methods," *Semin. Nas. Inform. 2008 (semnasIF 2008)*, vol. 2018, no. November, pp. 86–91, 2018.