

Browser Forensic of Facebook Messenger on Cybercrime Case using National Institute of Standards and Technology Method

Lutfiah Atsari Sujud
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 Indonesia are very advanced and have become part of everyday life making it easier to disseminate information and communicate. Facebook Messenger is an instant messenger that has advantages in multi-platform that can be used by users to send text messages, pictures, voice messages, and videos. Apart from being used for positive activities, technology facilities can also be used to carry out negative activities. One of the negative effects is committing digital crimes. Digital crime. The most common digital crime is online prostitution. This study conducts a forensic investigation on a simulation of a crime in online prostitution cases using Facebook messenger as a communication medium on the chrome web browser with the NIST stage. The stages of the forensics National Institute of Standards and Technology (NIST) are collection, examination, analysis, and reporting. This study uses a laptop that is turned on and connected to the internet. The process of collecting data in this study uses several forensic tools, namely Belkasoft Live RAM Capture, FTK Imager, Browser History Capture, Browser History Viewer, and Browser History Examiner. The percentage results obtained based on the forensic tool used Belkasoft Live RAM Capture which was analyzed using the FTK Imager tools was 80% with proof of email, password, message, and account id. Browser History Capturer analyzed with forensic tool Browser History Viewer is 20% with proof of image posting, web browser history, Facebook Messenger account profile photo and access time. Tool Browser History Examiner is 20% with proof of email accessed. The results of this study managed to find messages that have been deleted.

Keywords

Forensics, Web Browser, NIST, Facebook Messenger

1. INTRODUCTION

The development of technology in Indonesia is very rapid and has become part of everyday life, the rapidity of technology makes it easier to disseminate information, communicate such as social media and instant messengers. One of the instant messengers where many crimes occur is Facebook Messenger. Based on data from Napoleon Cat, users of Facebook Messenger in Indonesia in September 2021 were 137,300,000 which accounted for 49.7% of the entire population. The increasing number of Facebook Messenger users certainly brings positive and negative impacts, one of the negative effects is committing digital crimes [1]. Digital crimes such as human trafficking/online prostitution, cyberbullying, fraud, extortion, spreading hoaxes, cyberporn, and others [2]. Digital crime, one of which is online prostitution that occurs on the

Facebook messenger service. Online prostitution is an activity that makes humans, especially in terms of sexuality, an object to be traded through electronic or online media. These digital crimes can be uncovered using digital forensics. One of the stages to assist investigators in the digital forensic process is the NIST stage[3]. NIST stages are Collection, Examination, Analysis, and Reporting.

1.1 Study Literature

1.1.1 Previous Study

This research related to the topic of the problem to be studied to be used as comparison material and reference in conducting research. The first research is entitled "Implementation of Live Forensics for Comparison of Browsers on Email Security". This research was conducted on Microsoft Edge browsers, Mozilla Firefox, and Google Chrome. In the forensics carried out by the three web browsers, they use two modes, namely modes public and private. The results of this study are in mode public only google chrome whose not found password is while in mode private displays the same result for the password, which is not visible [4].

The second research conducted a digital forensics research entitled "Live Forensics Comparison Design on Instagram, Facebook and Social Media Security Twitter on Windows 10". This study discusses the design to carry out the digital forensic process. The research design was carried out by involving three social media to compare security, namely Instagram, Facebook, and Twitter. All of the social media accounts involved are newly created accounts or special accounts for research [5].

The third research was conducted with the title "Analysis and Comparison of Forensic Evidence for Facebook and Social Media Applications on Twitter Android Smartphones". This study runs eleven scenarios including recovering deleted files using an Android mobile that has installed applications Twitter and Facebook and using a simulation method using the DB Browser for SQLite, SQLite Manager, and Root explorer tools. The results of this study indicate that all the evidence found in the Facebook application and application was Twitter only partially found[6].

The fourth research entitled "Forensic analysis of the KakaoTalk application using the method National Institute Standard Technology" which discusses the forensic analysis of the KakaoTalk application in handling cybercrime cases with Android smartphone evidence and for the process of removing digital evidence in the condition of a smartphone with rooting actions [7].

The last research entitled "Forensic Analysis of Telegram Desktop-based Applications using the National Institute of Justice (NIJ) Method" discussed analyzing the evidence on web telegrams that were synchronized with Telegrams based android. With the results, it can display the location of log files, caches Telegram, and digital evidence and can only display stickers or images using the tool FTK imager but no chat has been detected by the perpetrator against the victim [8].

1.1.2 Digital Forensics

Digital forensics is the implementation of the field of computer science and technology as well as scientific methods for proving digital crimes against the law to scientifically prove technological or computer crimes to obtain digital evidence from digital sources [9]. Digital forensics is a method used in the investigation process of electronic or digital evidence for the reconstruction of crimes cyber or assisting in the process of analyzing criminal cases, the course of the investigation that has been planned [10]. There are two digital forensics methods, namely static forensics and live forensics. Static forensics is focused on examining imaging results to analyze digital content and evidence, such as deleted files, web browsing history while Live forensics is a forensic investigation carried out on a powered system. This is because data will be lost if the computer is shut down or restarted. implementations are Live forensics usually used or stored in Random Access Memory (RAM) [11]. Digital forensics is a methodological framework consisting of techniques and procedures for finding and collecting digital evidence as legal evidence in court [12].

1.1.3 Computer Forensics

Computer forensics is the collection and analysis of data from various computer resources including computer systems, computer networks, communication lines, and various storage media that can be submitted in court proceedings [13]. These three things are considered regardless of whether computer forensics is applied because of purely forensic needs in a legal sense or other needs for managing information technology resources that involve computer forensics. Three things that need to be considered are principle, policy, and procedure [14].

1.1.4 Web Browser

The web browser is a software application used to retrieve and present web information resources. A web browser or browser is application software that users can use to access and view Web pages or web programs [15]. A web browser is an application for accessing websites over the Internet. Web browsers allow users to search for information, read email, communicate via instant messages or social media, use internet banking and shop through e-commerce websites [16]. Popular web browsers such as Mozilla Firefox, Internet Explorer, Google Chrome, and Opera [17].

1.1.5 Digital Evidence

Evidence for computer crimes is in the form of electronic evidence and digital evidence. Electronic evidence can be in the physical form of electronic devices or can be in the form of storage devices, while digital evidence can be inform the of document files, history files or files log containing related data that can be used as supporting information for decisionmakers [18]. Evidence is data information contained

in electronic devices to obtain digital evidence for example physical devices such as laptops, smartphones, and so on [19].

1.1.6 Facebook Messenger

Facebook Messenger is an instant messaging application that can send text, pictures, videos, and voice messages. This application exists for smartphones based on Android, iOS, and Windows. The Facebook Messenger application is used to make it easier for Facebook users to send messages between fellow Facebook users [20].

1.1.7 Cybercrime

Cybercrime is a criminal activity that makes a computer network or computer a tool and becomes a target for the crime scene or can also be called a virtual world crime [21]. Cybercrime is every activity of a person, group of people, legal entities that use computers as a means of committing crimes and computers as targets [22]. Cybercrime is divided into two major groups, namely Violent / Potentially Violent and Non-Violent [23].

1.1.8 Online Prostitution

Prostitution is an activity of prostitution or an activity that makes humans, especially in terms of sexuality, an object to be traded through electronic or online media. Online prostitution is carried out using the media because it is easier, cheaper, and more practical to trade through electronic or online media [24].

1.1.9 National Institute of Standards Technology

National Institute of Standards and Technology (NIST) is the body responsible for developing standards, guidelines, and minimum requirements to provide sufficient information security for all assets and parties who have competence in the field of digital forensics, methods it is used by central government agencies in America, but it is possible that it can be used by organizations such as academia, private investigators and others.

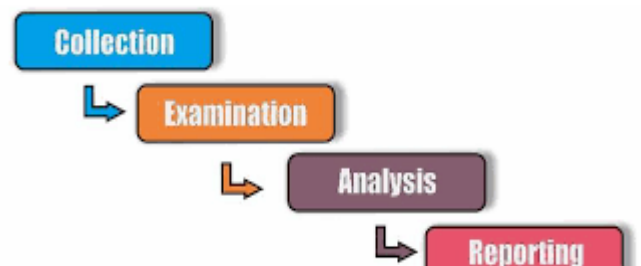


Figure 1. Stages of NIST Method

The stages that can be seen in Figure 1 are the NIST stages which consist of collection, examination, analysis, and reporting [25].

1. **Collection**
The Collection is to identify, label, record and obtain data from possible sources of relevant data, following guidelines and procedures that maintain data integrity.
2. **Examination**
The Examination is a process to protect evidence from damage and alteration by parties who are not responsible for the process collection in collecting electronic evidence and analyzing electronic data by forensic experts.

3. *Analysis*

The Analysis is to collect and examine to obtain evidence related to the case. Analyzing the results of the examination, using methods and techniques that can be legally justified to obtain information.

4. *Reporting*

Reporting is reporting on the results of investigations obtained from investigations related to the description of the actions used and contains the results of analyzing evidence so that the evidence helps the investigation process to find suspects.

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 a web-based Facebook messenger service to obtain and analyze evidence. In this scenario, the laptop is used as evidence that is suspected and will be investigated with online prostitution cases on Facebook messenger using a chrome web browser.

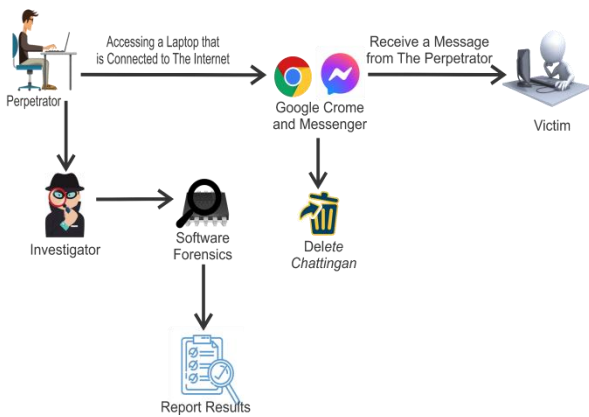


Figure 2. Flow of the Case Scenario on Messenger

Figure 2 explains that the suspect after being caught will confiscate evidence in the form of a laptop suspected of committing online prostitution using Facebook messenger, then handed over to the investigator to investigate the case that occurred by investigating the perpetrator's laptop. The investigator process will collect evidence using forensic tools that have been prepared to obtain digital evidence. The results obtained will be presented to the court.

2.2 **Research Stages**

The implementation stage is carried out in the research process to obtain digital evidence. This research refers to the method of NIST. The National Institute of Standards and Technology method is a forensic stage that has policy work guidelines and standards to ensure each investigator follows the same workflow so that work is documented and the results obtained can be repeated and can be maintained. The stages to be carried out are collection, examination, analysis, and reporting.

2.2.1 *Collection*

The data collection stage is the stage carried out to search for, collect and document the evidence at the location of the case. The evidence will be secured to maintain the authenticity of the evidence because it will be carried out 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 web browser is installed which is indicated to be used by the perpetrator as a tool to carry out cybercrime actions. In addition to the laptop, electronic evidence was also found in the form of a charging cable used by the perpetrator to charge the laptop.

Table 1. Physical Evidence



No	Evidence	Picture	Description
1	Laptop of the Perpetrator		Laptop of the perpetrator, namely Asus, which was found at the location, was turned on and connected to the internet network
2	The Charging		Cable the laptop charger cable used by the perpetrator

Table 1 shows the documentation of physical evidence found at the scene which was then collected by the police and handed over to the investigator.

2.2.2 *Examination*

Examination is the stage for data acquisition on the evidence found in the form of a laptop of the perpetrator to obtain evidence. At this stage, inspection, testing, and extracting information from the data that has been collected are carried out. The data acquisition process uses forensic tools to obtain activity history from *Random Access Memory* (RAM).

2.2.2.1 *Belkasoft Live RAM Capturer*

Forensic tools used to perform data acquisition stored on laptop RAM is Belkasoft Live RAM Capture. Belkasoft Live RAM Capture will record laptop memory data of perpetrators found to commit crimes. The process of capturing memory takes a long time depending on the amount of RAM memory on the perpetrator's laptop.

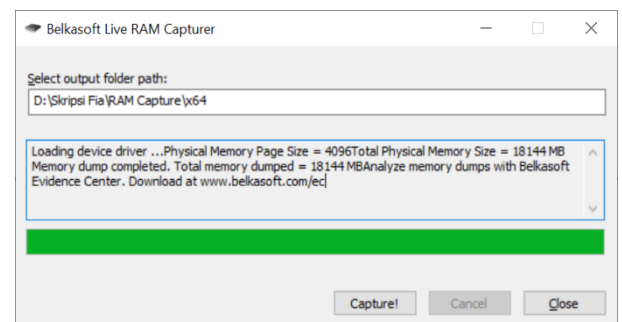


Figure 3. RAM Capturer Acquired Successfully

Figure 3 shows that RAM capture has been successfully performed. 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 D:\Fia script\RAM Capture\x64 folder. During the acquisition process, there is information about the RAM size of the laptop, which is 18144 Megabytes

(MB). The results of the RAM capture are obtained files that have a size of approximately 18 GB. with the name 20211006 and in.mem format.

2.2.2.2 FTK Imager

Tool to perform the imaging process of the captured RAM using the Belkasoft Live RAM Capture tool. 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.

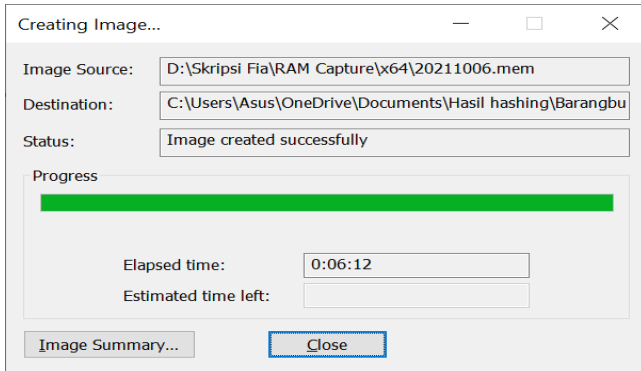


Figure 4. Process of Imaging Data

Figure 4 shows the imaging process from the captured RAM file with the 20211006.mem file that has been successfully carried out and the resulting file with the name Barangbukti.001.mem which is stored on the C:\Users\Asus\OneDrive\Document\Hasil hashing\.

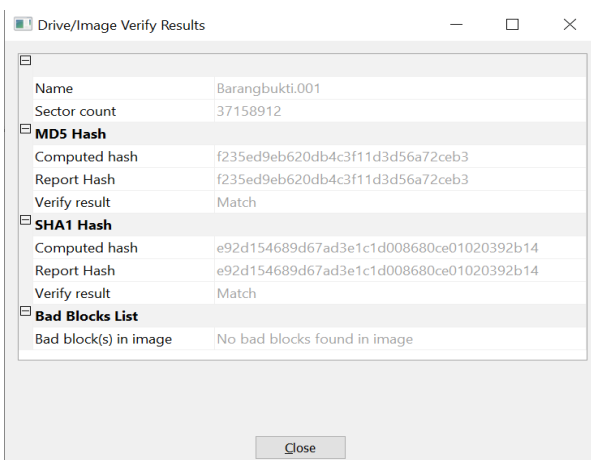


Figure 5. the Hashing Results of RAM

Figure 5 shows the hashing value of the RAM capture file which has an MD5 hash value and a SHA1 hash value. Hashing results in the form of a file with the name BarangBukti.mem proves that the original file with the imaging file has the same verified MD5 and SHA1 values so that the imaging process is carried out perfectly and there are no changes to the file.

2.2.2.3 Browser History Capturer

The history capture process is carried out to obtain results from browser activities used by perpetrators to commit cybercrimes. The browser history capture tool can be used for various web browsers such as Chrome, Edge, Firefox, and Internet Explorer. The data was obtained in the form of History, Cache, and Archived History.

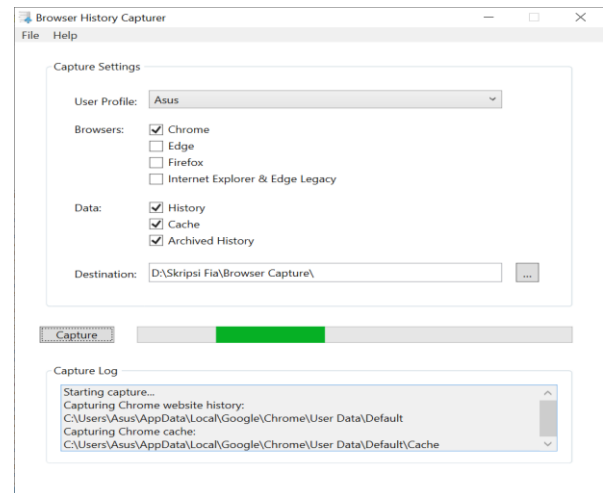


Figure 6. Display of Browser History Capturer

Figure 6 shows the initial view of the browser history capturer. The "Capture Settings" section is used to select the user profile, the type of browser used, the data you want to know such as history, cache, and archived history and the "Destination" section is where the captured results are stored. Perpetrators spread online prostitution content on the facebook messenger service which is accessed using chrome, so it is only checked on the chrome browser, besides that, a checklist is also carried out on all types of data that will be obtained and the results of the capture storage are stored in location.D:\SkripsiFia\Browser Capture\.

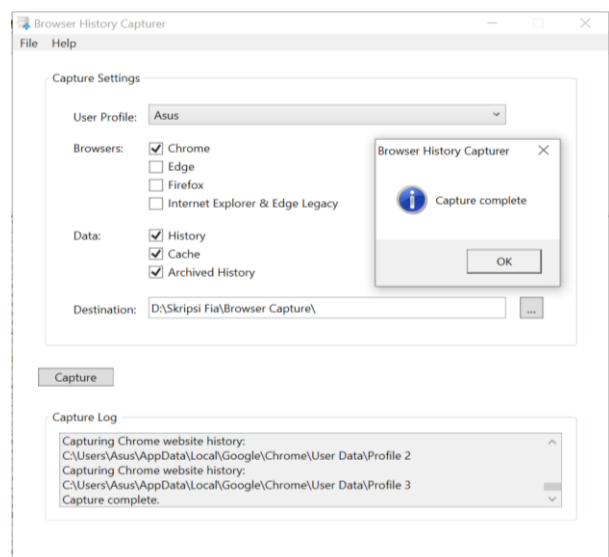


Figure 7. Process of Capturing Datafrom Browser Chrome

Figure 7 is the display when the data retrieval process from the Chrome browser is successfully carried out. Capture results are saved inD:\Skripsi Fia\Browser Capture\.

Name	Date modified	Type	Size
Chrome	06/10/2021 19:56	File folder	
Historical	06/10/2021 19:57	File folder	

Figure 8. Capture Results File of Browser Chrome

Figure 8 is the content of the results captured browser with a folder Named capture which contains the folders Chrome and Historical.

2.2.3 Analysis

Analysis is a stage to analyze and read the results of the data that has been obtained from the collection process to examination. This stage aims to match the information obtained with the information obtained while maintaining the integrity of the data. the results of the data analysis will be concluded for the reporting stage process.

2.2.3.1 Analysis with Browser History Viewer

Browser History Viewer is a tool used to read the results of the Google Chrome browser capture that has been carried out at the inspection stage using the browser history capture tool.

Name	Date modified	Type	Size
Capture	06/10/2021 20:26	File folder	

Figure 9. The Result File or Capture Browser

The figure 9 shows the file captured by the browser using the browser history capture tool. The data file will be displayed using the browser history viewer to obtain important data in accessing the chrome browser.

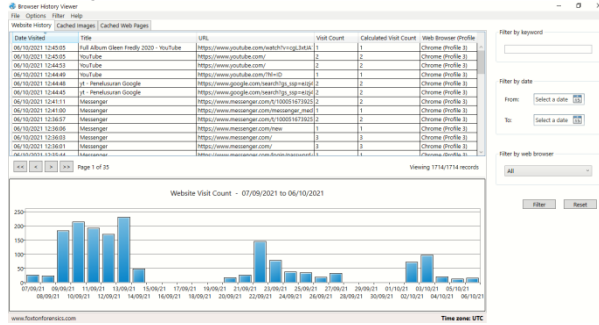


Figure 10. Data of History Browser Chrome

Figure 10 shows the results of history data accessed by perpetrators through the chrome browser which displays information, namely website history, cache images, and cached web pages. browser history viewer has a feature by using certain parameters. This study uses the Facebook messenger service so that it uses the "Messenger" parameter.

Date Visited	Title	URL	Visit Count	Calculated Visit Count	Web Browser (Profile)
06/10/2021 12:41:11	Messenger	https://www.messenger.com/t/100051673925966	2	2	Chrome (Profile 3)
06/10/2021 12:41:00	Messenger	https://www.messenger.com/messenger_media/thread_id=100...	1	1	Chrome (Profile 3)
06/10/2021 12:36:57	Messenger	https://www.messenger.com/t/100051673925966	2	2	Chrome (Profile 3)
06/10/2021 12:36:06	Messenger	https://www.messenger.com/new	1	1	Chrome (Profile 3)
06/10/2021 12:36:03	Messenger	https://www.messenger.com/	3	3	Chrome (Profile 3)
06/10/2021 12:36:01	Messenger	https://www.messenger.com/	3	3	Chrome (Profile 3)
06/10/2021 12:35:44	Messenger	https://www.messenger.com/login/password/	1	1	Chrome (Profile 3)
06/10/2021 12:34:47	Messenger	https://www.messenger.com/	3	3	Chrome (Profile 3)
06/10/2021 12:34:44	messenger login - Penelusuran Google	https://www.google.com/search?q=messenger+login&rlz=...	2	2	Chrome (Profile 3)
06/10/2021 12:34:44	messenger login - Penelusuran Google	https://www.google.com/search?q=messenger+login&rlz=...	2	2	Chrome (Profile 3)
23/09/2021 18:40:25	The Messengers - Penelusuran Google	https://www.google.com/search?q=the+messengers+and+2000000000	2	2	Chrome (Profile 2)
23/09/2021 18:49:23	The Messengers - Penelusuran Google	https://www.google.com/search?q=the+messengers+and+2000000000	2	2	Chrome (Profile 2)

Figure 11. The Search Results Using Keyword "Messenger"

In the analysis process using the keyword "Messenger" to make searching easier, the data that appears is only data related to the messenger, as in Figure 11 shows the history when the perpetrator logged in to the messenger account on October 6, 2021 at 12:35:44 via the chrome web browser. On the same date but at a different time, it was found that the perpetrator carried out new messaging activities with the victim id 100051673925966.



Figure 12. Images Cached First from Messenger.

Figure 12 shows a cached image that was successfully read by the browser history viewer tools. The evidence found in the cached image marked in red is very similar to the screenshot of the crime evidence given by the victim to the police. The image was sent by the perpetrator on October 6, 2021 at 12:04:01 pm via the chrome web browser.

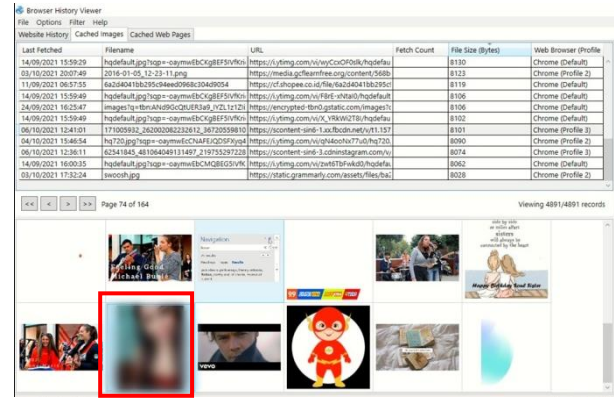


Figure 13. Image Cached Second from Messenger.

Figure 13 shows a cached image that is very similar to the image shown by the victim through the screenshot results.

2.2.3.2 Analysis with Browser History Examiner

A browser history examiner is a tool for examining or analyzing browser capture results that were previously done using Browser History Capture. The data used is the data in the capture folder. Browser history Examiner displays information consisting of Bookmarks, Browser Settings, Cache Files, Cache Images, Cache Web Pages, Cookies, Downloads, Email Addresses, Favicons, Form History, Logins, Searches, Session Tabs, Thumbnails, and Website Visits.

Last Used	Email Address	Domain	Source	Web Browser (Profile)
06/10/2021 12:36:05	percobaankasus@gmail.com	messenger.com	Saved Login	Chrome (Profile 3)
14/09/2021 16:00:57	percobaankasus@gmail.com	accounts.google.com	Form History	Chrome (Profile 2)
18/08/2021 07:56:09			Form History	Chrome (Default)
30/04/2021 15:58:55			Form History	Chrome (Default)
23/04/2021 05:28:12			Form History	Chrome (Default)
20/04/2021 14:01:40			Form History	Chrome (Default)
19/04/2021 15:41:49			Form History	Chrome (Default)
30/03/2021 09:03:27			Form History	Chrome (Default)

Figure 14. Email for Access Messenger

Figure 14 shows the email used by the perpetrator to log in to the messenger account via the chrome web browser, it can be seen that the email used is "percobaankasus@gmail.com".

2.2.3.3 Analysis with FTK Imager

The previous stage has been carried out using a RAM data acquisition tool using Belkasoft RAM Capture obtained with the file name 20211006.mem.

Name	Date modified	Type	Size
20211006.mem	06/10/2021 19:46	MEM File	18.579.456 KB
mvcvp110.dll	22/10/2018 10:11	Application extension	646 KB
msvcv110.dll	22/10/2018 10:11	Application extension	830 KB
RamCapture64.exe	22/10/2018 10:11	Application	58 KB
RamCaptureDriver64.sys	22/10/2018 10:11	System file	34 KB

Figure 15. File of RAM Acquisition

Figure 15 shows the capture results from the Belkasoft Live RAM Capture tool which will be analyzed using the FTK Imager tool to find digital evidence using email parameters that have been found in the browser history examiner tool, namely percobaankasus@gmail.com.

0639ab410	65 00 6D 00 61 00 69 00-6C 00 00 00 00 00 00	e-m-a-i-l-.....
0639ab420	10 00 00 00 00 00 00 00-08 00 00 00 00 00 00
0639ab430	38 00 00 00 18 00 00 00-70 00 65 00 72 00 63 00p-e-r-c
0639ab440	6F 00 62 00 61 00 61 00-6E 00 68 00 61 00 73 00	o-b-a-a-n-k-a-s-
0639ab450	7E 00 73 00 40 00 67 00-6D 00 61 00 69 00 6C 00	u-s-@-g-m-a-i-l
0639ab460	2E 00 63 00 6F 00 6D 00-0C 00 00 00 04 00 00 00c-o-m-.....
0639ab730	70 00 61 00 73 00 73 00-10 00 00 00 00 00 00 00	p-a-s-s-.....
0639ab740	08 00 00 00 00 00 00 00-22 00 00 00 0D 00 00 00
0639ab750	4B 00 61 00 73 00 75 00-73 00 66 00 6F 00 72 00 63	K-a-s-u-s-f-o-
0639ab760	65 00 6E 00 73 00 69 00-6B 00 00 00 00 00 00 00	e-n-s-i-k-.....

Figure 16. Email and Findings Password

Figure 16 shows the email and password used by the perpetrator to log in to the messenger account, the email used is "percobaankasus@gmail.com" and the password is "Kasusforensik".

12aeffd60	22 62 72 6F 20 61 64 61-20 79 61 6E 67 20 61 61	"bro ada yang ba
12aeffd70	72 75 2C 20 64 75 61 20-6F 72 61 6E 67 20 61 75	ru, dua orang bu
12aeffd80	61 74 20 6E 65 6D 65 6E-69 6E 20 6D 61 6C 61 6D	at nemenin malam
12aeffd90	20 6C 75 20 62 72 6F 5C-5C 5C 22 2C 5C 5C 5C 5C	22 lu bro\\\\"

Figure 17. Evidence of Conversation 1 for FTK Imager

Figure 17 shows evidence in the form of a conversation with the first message sent by the perpetrator to the victim which reads "bro ada yang baru, dua orang buatnemeninmalam lu bro".

1d4f4da10	39 35 2C 34 31 30 37 36-35 36 34 36 5D 2C 5C 22	95,410765646j,"
1d4f4da20	75 6D 75 72 20 62 65 72-61 70 61 20 62 61 6E 57	umur berapa bing
1d4f4da30	3F 5C 22 2C 66 61 6C 73-65 2C 5B 32 33 32 39 35	a",false,[23]95

Figure 18. Evidence of Conversation 2 for FTK Imager

Figure 18 shows the text of the second message sent by the victim to reply to the perpetrator's chat which reads "umurberapa bang?"

12cfa9120	22 74 65 78 74 5C 5C 5C-22 3A 5C 5C 5C 22 6D 6E	"text\\\\"
12cfa9130	73 69 68 20 6D 75 64 61-20 32 30 20 61 6E 20 61	sih muda 20 an k
12cfa9140	72 6F 2C 20 62 69 61 72-20 67 75 61 20 6B 69 72	ro, biar gua kir
12cfa9150	69 6D 69 6E 20 66 6F 74-6F 6E 79 61 20 6B 61 6D	imin fotonya kal
12cfa9160	61 75 20 74 65 72 74 61-72 69 6B 20 6D 6F 6E 67	au tertarik mong
12cfa9170	67 6F 9C 5C 9C 22 2C 5C-5C 5C 22 69 6E 69 74 6E	go\\\\"

Figure 19. Evidence of Conversation 3 for FTK Imager

Figure 19 shows evidence of the findings of the third message conversation from the perpetrator which contains "masihmuda 20 an bro, biarguakiriminfotonyakalautertarikmonggo".

15f464ad0	31 2E 31 35 37 35 32 2D-39 2F 31 36 37 36 35 30	1.15752-1147050
15f464ae0	36 30 36 5F 35 30 32 37-37 35 31 35 31 36 38 37	606_5027_9151087
15f464af0	32 32 38 5F 32 36 32 38-30 39 30 31 32 32 34 39	228_2628_9012249
15f464b00	38 30 35 30 33 39 33 5F-6E 2E 6A 70 67 3E 5F 6F	8050393_1.jpg?_n
15f464b10	63 5F 63 61 74 3D 31 30-32 26 63 63 62 3D 31 2D	c_cat=102accb=1-
18914fa60	5C 5C 2F 74 31 2E 31 35-37 35 32 2D 39 5C 5C 5C	75752-9\\
18914fa70	2F 81 37 31 30 30 35 39-33 32 5F 32 36 32 30 30	/171005332_26200
18914fa80	32 30 38 32 32 33 32 36-31 32 5F 33 36 37 32 30	2082232312_36720
18914fa90	35 35 39 38 31 30 33 35-34 31 35 36 30 33 5F 6E	55901033415603_n
18914faa0	2E 6A 70 67 3F 5F 6E 63-5F 63 61 74 3D 31 32 31	image_cat=111

Figure 20. Finding of Evidence File Image

Figure 20 shows the evidence of the image sent by the perpetrator but only in the form of the file name of the image.

1af150b20	35 39 35 5C 22 2C 20 5B-32 33 32 39 35 2C 34 31	606", "berap
1af150b30	30 37 36 35 36 34 36 5D-2C 5C 22 62 65 72 61 70	0765646j,"berap
1af150b40	61 20 70 65 72 6D 61 6C-61 6D 20 62 61 6E 67 3E	a permalam bang?

Figure 21. Evidence of Conversation 4 for FTK Imager

Figure 21 shows evidence of the fourth message sent by the victim to reply to the perpetrator's message containing "berapapermalam bang?"

382bf57e0	22 6D 75 72 61 68 20 62-75 61 74 20 62 75 61 74	"murah buat buat
382bf57f0	20 6C 75 20 62 72 6F 2C-20 70 65 72 6F 72 61 6E	lu bro, peroran
382bf5800	67 20 35 6A 74 61 20 62-65 62 61 73 20 64 69 61	g 5jta bebas dia
382bf5810	70 61 69 6E 20 75 6E 74-75 6B 20 68 6F 74 65 6C	pain untk hotel
382bf5820	20 74 65 72 69 6D 61 20-62 65 72 65 73 20 64 65	terima beres de
382bf5830	68 5C 5C 5C 22 2C 5C 5C-5C 22 69 6E 69 74 69 6E	h\\\\"

Figure 22. Evidence of Conversation 5 for FTK Imager

Figure 22 shows the findings of evidence of the fifth message sent by the perpetrator to the victim which contained "murahbuatbuatlu bro, perorangan 5jta bebadisainuntuk hotel terimaberesdeh".

1b7442490	34 31 30 37 36 35 36 34-36 5D 2C 5C 22 6B 65 6C	410765646j,"keb
1b74424a0	65 74 75 6C 61 6E 20 67-75 61 20 61 64 61 20 61	etulan gua ada a
1b74424b0	63 61 72 61 20 62 65 73-6F 6B 20 6D 61 6C 61 6D	cara besok malam
1b74424c0	2C 20 62 6F 6C 65 68 6C-61 68 20 67 75 61 20 70	, bolehlah gua d
1b74424d0	61 6B 65 20 6B 65 64 75-61 6E 79 61 5C 22 2C 6E	ake keduanya\\

Figure 23. Evidence of Conversation 6 for FTK Imager

Figure 23 shows the findings of evidence of the sixth message sent by the victim to reply to the perpetrator's message containing "kebetulangaada acara besokmalam, bolehlahguapakakeduanya".

3fbd5e780	5C 5C 22 3A 31 2C 5C 5C-5C 22 74 65 78 74 5C 5C	\\\\"
3fbd5e790	5C 22 3A 5C 5C 5C 22 73-69 61 70 20 62 72 6F 20	\\\\"siap bro,
3fbd5e7a0	20 74 6F 74 61 6C 20 31-30 6A 74 61 20 74 72 61	total 10jta tra
3fbd5e7b0	6E 73 66 65 72 20 6B 65-20 72 65 6B 65 6E 69 6E	nsfer ke rekenin
3fbd5e7c0	67 20 37 34 31 35 30 35-33 38 32 37 20 61 2E 6F	g 7415053827 a.n
3fbd5e7d0	20 42 61 67 75 73 20 53-75 6C 69 73 74 69 6A 6E	Bagus Sulistijo
3fbd5e7e0	6E 6F 5C 5C 5C 22 2C 5C 5C-5C 22 69 6E 69 74 6E	ne\\\\"

Figure 24. Evidence of Conversation 7 for FTK Imager

Figure 24 shows the findings of evidence of the seventh message sent by the perpetrator to the victim which contained "siap bro, total 10jta transfer kerekening 7415053827 a.n Bagus Sulistijono".

20b1ccee0	2C 66 61 6C 73 65 29 2C-5F 3D 3E 4C 53 2E 73 70	\\\\"
20b1ccee0	28 5C 22 31 32 34 5C 22-2C 20 5C 22 6F 6B 65 20	\\\\"124\\", \\\"oke
20b1ccee0	73 69 61 70 20 62 61 6E-67 5C 22 2C 55 2C 5B 30	siap bang\\",U,t

Figure 25. Evidence of Conversation 8 for FTK Imager

Figure 25 shows the evidence found in the conversation of the eighth message sent by the victim to be replied to containing "okesiap bang".

2.2.4 Reporting

Reporting is the final process of the NIST method and the process created to create a report on the results of the analysis carried out by investigators on the perpetrator's device in the form of a chrome web browser used to commit crimes according to the scenario that has been created. The results of the data found on the laptop RAM in the chrome web browser forensics with live forensics were found, to be used as digital evidence of the crimes committed by the perpetrators against the victims through the Facebook messenger service.

Table 2. Data Results Found

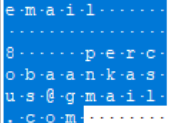
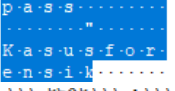
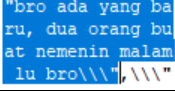
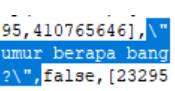
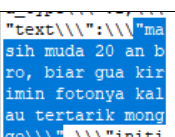
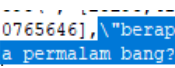
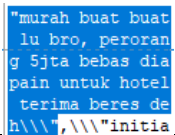
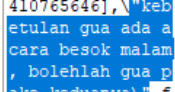
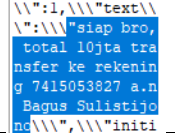
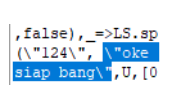

Digital Evidence	Findings	Text
Email		“percobaankasus@gmail.com”
Password		“Kasusforensik”
Text		“bro ada yang baru, dua orang buat nemenin malam lu bro”
Text		“umur berapa bang?”
Text		“masih muda 20 an bro, biar gua kirim fotonya kalau tertarik monggo”
Text		“berapa permalam bang?”
Text		“murah buat buat lu bro, perorang 5jta bebas diapain untuk hotel terima beres deh”
Text		“kebetulan ada acara besok malam, bolehlah guapake kedua”
Text		“siap bro, total 10jta transfer kerekening 7415053827 a.n Bagus Sulistijono”
Text		“oke siap bang”
Picture		sent by the perpetrator and the victim

Table 2 shows the evidence found from the RAM and Web browser chrome capture results, namely emails, passwords, text of conversations between perpetrators and victims, as well as photos sent by perpetrators and victims.

2.2.5 Results

The tools used in this research is the Chrome browser using the Facebook Messenger service. The digital evidence is then analyzed using several forensic tools. The results found in this study in the form of a text conversation between the perpetrator and the victim were found using the FTK Imager and the uploaded image sent by the perpetrator to the victim was found using the Browser History Capture tool.

Table 3. Comparison of results obtained from Several Tools

No	Information	Forensic Tools		
		Ram Capture + FTK Imager	Browser History Capture + Browser History Viewer	Browser History Examiner
1	Email	√	-	√
2	Password	√	-	-
3	A messaging conversation	√	-	-
4	Posts Pictures	-	√	-
5	Id account	√	-	-

Table 3 shows the evidence found using several forensic tools. Belkasoft Live RAM Capture and FTK Imager, Browser History Examiner get emails. Belkasoft Live RAM Capture and FTK Imager tools get Password, account ID and conversation text. Belkasoft Live RAM Capture is used to get the perpetrator's laptop RAM and FTK Imager is used to read the results of the RAM acquisition that has been obtained. Browser History Capture, Browser History Viewer, and Browser History Examiner only found evidence according to the scenario in the form of web pages, browsing history links, account logins, and posting pictures.

3. CONCLUSION

The web browser forensics process is carried out on the Facebook messenger service with cases of online prostitution obtaining digital evidence, namely making acquisitions of RAM using the Belkasoft Live RAM Capture and FTK Imager tools in the form of the perpetrator's account information, namely email and password, message conversation, time of message sender, perpetrator's account id and victims. The Browser History Capture, Browser History Viewer, and Browser History Examiner tools generate browser web pages, cache images, and time in messenger account access. The percentage results obtained based on forensic tools using Belkasoft Live RAM Capture which were analyzed using the FTK Imager tool were 80% with evidence of email, password, message, and account id. Browser History Capturer analyzed by forensic tool Browser History Viewer is 20% with proof of posting pictures, web browser history, Facebook Messenger account profile photo and access time. Tool Browser History Examiner is 20% with proof of email accessed. The results of this study managed to find messages that have been deleted.

4. REFERENCES

- [1] A. Yudhana, I. Riadi, and I. Anshori, "Analysis of Digital Evidence for Facebook Messenger Using the Nist Method," *It J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.
- [2] M. I. Syahib, I. Riadi, and R. Umar, Digital Forensic Analysis of Beetalk Applications for Cybercrime Handling Using the NIST Method," *Semin. Nas. Inform.*, vol. 2018, no. November, p. 134, 2018, [Online]. available: <http://jurnal.upnyk.ac.id/index.php/semnasif/article/view/2629>.
- [3] D. Hariyadi, U. Jenderal, and A. Yani, "Identification of Conversation Evidence on the Dual Apps Whatsapp Application," vol. 1, no. November, pp. 1–8, 2018.
- [4] M. N. Faiz, R. Umar, and A. Yudhana, "Implementation of Live Forensics for Comparison of Browsers in Email Security," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 1, no. 3, p. 108, 2017, doi: 10.14421/jiska.2017.13-02.
- [5] R. A. K. N. 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 Tahun 2018 Fak. Tech. Univ. Wahid Hasyim*, pp. 125–128, 2018.
- [6] W. A. Mukti, S. U. Masruroh, and D. Khairani, "Analysis and Comparison of Forensic Evidence for Facebook and Twitter Social Media Applications on Android Smartphones," *J. Tech. Information.*, vol. 10, no. 1, pp. 73–84, 2017, doi: 10.15408/jti.v10i1.6820.
- [7] R. Y. Prasongko, A. Yudhana, and A. Fadil, "Forensic analysis of Kakaotalk application using the national institute standard technology method," *Semin. Nas. Inform. 2018 (semnasIF 2018) UPN "Veteran" Yogyakarta, 24 November. 2018 ISSN 1979-2328*, vol. 2018, no. November, pp. 129–133, 2018.
- [8] I. G. Ngurah, G. Wicaksana, and I. K. G. Suhartana, "Forensic Analysis of Telegram Desktop-based Applications using the National Institute of Justice (NIJ) Method," vol. 8, no. 4, pp. 381–385, 2020.
- [9] I. Riadi, A. Fadlil, and M. I. Aulia, "Investigating Digital Optical Drive Evidence Using the National Institute of Standard and Technology (NIST)," *J. RESTI (Rekayasa Sist. dan Tech. Information)*, vol. 4, no. 5, pp. 820–828, 2020, doi: 10.29207/resti.v4i5.2224.
- [10] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile forensic tools evaluation for digital crime investigation," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, pp. 949–955, 2018, doi: 10.18517/ijaseit.8.3.3591.
- [11] T. Rochmadi, "Live Forensics for Anti-Forensic Analysis on a Web Browser Case Study Browzar," *Indonesia. J. Bus. Intell.*, vol. 1, no. 1, p. 32, 2019, doi: 10.21927/ijubi.v1i1.878.
- [12] S. Rachmie, "The Role of Digital Forensic Science in Investigation of Website Hacking Cases," *Litigasi*, vol. 21, no. 21, pp. 104–127, 2020, doi: 10.23969/litigasi.v21i1.2388.
- [13] F. Sulianta, *Computer Forensics*. Jakarta: PT Elex Media Komputindo, 2008.
- [14] F. Sulianta, *Forensic Engineering is the right way to solve computer problems*. Jakarta: PT Elex Media Komputindo, 2014.
- [15] Y. Firmansyah and Pitriani, "Application of the Waterfall SDLC Method in Making Member Service Applications at Cu Duta Usaha Bersama Pontianak," *J. Bianglala Inform.*, vol. 5, no. 2, pp. 53–61, 2017, [Online]. Available: <https://ejournal.bsi.ac.id/ejurnal/index.php/Bianglala/article/view/2703/1813>.
- [16] D. GDharanD and N. Meeran A R, "Forensic Evidence Collection by Reconstruction of Artifacts in Portable Web Browsers," *Int. J. Comput. Appl.*, vol. 91, no. 4, pp. 32–35, 2014, doi: 10.5120/15872-4862.
- [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] I. Riadi, R. Umar, and I. M. Nasrulloh, "Digital Forensic Analysis on Frozen SolidStateDrives with the National Institute of Justice (NIJ)," *Elinvo (Electronics, Informatics, Vocat. Educ.*, 2018, doi: 10.21831/elinvo.v3i1.19308.
- [19] 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.
- [20] S. R. Ardiningtias and H. , Sunardi2, "Digital Investigations on Facebook Messenger," pp. 19–26, 2018.
- [21] R. Rhamdhatul Muthia, Fairuz dan Arifin, "Criminal Law Studies in the Mayantara Crime Case (Cybercrime) In Case," vol. 5, no. April, pp. 21–39, 2019.
- [22] A. Antoni, "Cyber Crime in Online Listening," *Nurani J. Kaji. Syari'ah dan Masy.*, vol. 17, no. 2, pp. 261–274, 2018, doi: 10.19109/nurani.v17i2.1192.
- [23] 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.
- [24] D. Putra, Ichsan Ammanda; Pratimaratri, Uning; Wahyuni R, "The Use Of Forensic Digital Inprostitutional Criminal Online," 2018.
- [25] N. Nasirudin, S. Sunardi, and I. Riadi, "Forensic Analysis of Android Smartphones Using the NIST Method and the MOBILedit Forensic Express Tool," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, p. 89, 2020, doi: 10.32493/informatika.v5i1.4578.