

Browser Forensic for Cyber Fraud Case on Facebook Messenger Services using National Institute of Standard Technology Method

Chelsea Sept. Thiani Puri
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

Technology in the field of communication has increased over time, advances in communication technology can make it easier for people to interact in real-time and online using instant message. Facebook Messenger is one of the instant messaging applications that is widely used, besides being able to provide good effects, it also cannot avoid bad effects as a medium for committing internet crimes, internet crimes that can be committed through the Facebook Messenger service include online fraud, bullying, extortion, the spread of pornography, and others. In this study using a scenario of online social gathering fraud cases through the Facebook Messenger service running on the Chrome web browser by applying the NIST stages consisting of Collection, Examination, Analysis, and Reporting and using tools forensic consisting of Belkasoft Live RAM Capturer, FTK Imager, Browser History Capturer, Browser History Examiner, and Browser History Viewer. The percentage of results that have been obtained from Capture RAM using the BelkasoftLive RAM Capturer forensic tool which is read using the FTK Imager tool is 80% successful in obtaining evidence of Email, Password, Conversation Text and Web Browser History. In the capture results from the Chrome browser using the tool Browser History Capturer which was read with the forensic tool Browser History Examiner 40% succeeded in obtaining evidence of Email and Web Browser History, and using the tool Browser History Viewer 40% succeeded in obtaining Images and Web Browser History. The results of this research succeeded in obtaining digital evidence from fraud cases using a forensic process.

Keywords

Forensics, Browser, Messenger, Cybercrime, NIST

1. INTRODUCTION

advances in communication technology can make it easier for people to interact in *real-time* and *online* using instant messages that can be used as a communication medium to make it easier for an individual to send messages to other individuals with a wide range by utilizing the internet network. Facebook Messenger is one of the popular instant messaging applications used and can be accessed using a smartphone or website that is connected to an internet connection. Facebook Messenger in addition to being able to provide good effects for users, the application also cannot avoid the bad effects carried out by an individual by abusing it as a medium in committing criminal crimes. Criminal crimes committed by perpetrators by using social media as a medium for committing crimes in cyberspace

such as online fraud, extortion, spreading pornography, drug trafficking, planning murder, or bullying [1].

1.1 Study Literature

1.1.1 Previous Study

This research refers to five previous studies, namely:

Anton Yudhana, Imam Riadi, Ikhwan Anshori (2018) entitled "Analysis of Digital Evidence for Facebook Messenger Using the NIST Method". This research was conducted using a Galaxy V + smartphone that has the Facebook Messenger application. This research was conducted to find digital evidence on the Facebook Messenger application using the Oxygen forensic tool. The results of this study collected digital evidence in the form of conversational texts, audio and images that could not be found were videos[2].

Mulia Fitriana, Khairan AR, Jiwa Malem Marsya (2020) entitled "Application of the National Institute of Standards and Technology (NIST) Method in Digital Forensic Analysis for Cybercrime Handling". This study investigates pornographic cases conducted on the Whatsapp application to collect deleted digital evidence in the form of conversation texts, contact lists, profile photos, and others using the tool Whatsapp Viewer[3].

Rauhulloh Ayatulloh Khoemini Noor Bintang, Rusydi Umar, Anton Yudhana (2020) entitled "Analysis of Facebook Lite Social Media With Forensic Tools Using the NIST Method". This research was conducted using the Galaxy J2 Smartphone to make a post, an investigation to obtain digital evidence using the MOBILEdit Forensic tool. The results that have been obtained in this study are in the form of user ID, images, audio, and videos [4].

Moh. Riskiyadi (2020) entitled "Forensic Investigation of Digital Evidence in Revealing Cybercrime". The research uses the static forensic method with the object of research is a USB flash disk. Different treatments performed on flash disks obtained different results by showing different hash values for each treatment. The results of the analysis of the first and second treatments, namely all experimental results and those that had been stored before reformatting were successfully detected or recovered, while in the third treatment they did not get any results[5].

Ikhwan Anshori, Khairina Eka Setya Putri, Umar Ghoni (2020) entitled "Analysis of Digital Evidence for the Facebook Messenger Application on Android Smartphones Using the NIJ Method". This research was conducted using

the Galaxy V+ Plus Smartphone to obtain digital evidence from the Facebook Messenger application. The results of this study obtained evidence with a success rate of getting a 100% account, 55% chat, and 86% pictures using the MOBILEdit Forensic Express and Magnet AXIOM tools while using the Oxygen Forensic tool we managed to get a 100% account, 5% chat, and 86% pictures[6].

1.1.2 Digital Forensics

Digital forensics is the science of the process of maintaining, collecting, validating, analyzing, interpreting, documenting, and presenting digital data from electronic devices[7]. Forensics is an activity in conducting investigations and determining facts related to criminal crimes and other legal matters[8]. Digital forensics performs the process of recovering and analyzing data originating from digital devices such as smartphones, tablets, or computers [9]. There are two techniques used in digital forensics, namely live forensics, namely techniques to obtain RAM data from systems that are running or live (volatile), and static forensics, namely techniques to obtain data from permanent (non-volatile) storage such as hard disks, flash drives, CDs, SSDs[10].

1.1.3 Web Browser

Web browser is a software that can be used to access websites on the internet to obtain detailed information. Web information resources are identified with the Uniform Resource Identifier (URI) and as web pages, images, videos, or other media [11]. Web browsers can store browser history activities used by users in the form of information on websites visited, stored data or images, search information, cookies, and other information [12]. Several types of popular browsers that are often used are Google Chrome, Internet Explorer, Mozilla Firefox, Safari[13].

1.1.4 Digital Evidence

Evidence is data that has been obtained or recovered from an electronic device[14]. Digital evidence is information and data that has value for the investigation that is stored, sent, or received through electronic media[15]. Digital evidence is susceptible to changes that can affect the authenticity of the data if not handled properly. If there is a change in digital evidence it can cause the results in it to be wrong or the evidence to be useless [16]. Evidence of a cybercrime case is divided into two types, namely electronic evidence that is tangible in physical form from digital storage or device, while digital evidence is document files, log files, or history files in the form of data obtained from the extraction of evidence files from cybercrime cases[17]. Criminals in eliminating traces of actions will hide or delete all data obtained in criminal crimes that have been committed[18].

1.1.5 Facebook Messenger

Facebook Messenger is an instant messaging application that can be used via a smartphone, tablet, or computer. The services available in this application are sending messages in the form of text or voice to communicate. Facebook Messenger has services in the form of text, voice, or video messages to communicate [19].

1.1.6 Cybercrime

Cybercrime is an act that is carried out by utilizing digital devices and internet networks as a medium in committing crimes to gain profits at the expense of other parties [20]. Cybercrime is a crime using computer equipment as a

means of crime and digital forensics will provide answers related to digital crimes that occur with the questions of when, what, who, where, how, and why[21]. Cybercrime or cybercrime has a difference from crimes committed in person. The impact of crimes committed through social media is very influential on the victims [22]. Evidence of criminal crimes committed by users through social media can be identified by analyzing volatile data contained in RAM [23]. Cybercrime cases committed will leave a digital trace of the crime, the digital trace can be used as evidence[24].

1.1.7 Fraud

Fraud is a form of crime by committing various lies to gain individual or group benefits at the expense of other parties as described in Article 37 of the Criminal Code. One of the frauds committed is fraud in electronic transactions by utilizing electronic devices connected to an internet connection and carrying out various modes of fraud[25].

1.1.8 National Institute of Standard Technology

National Institute of Standard and Technology (NIST) is used to carry out the analytical steps of digital evidence or apply steps to obtain information data from digital evidence[26].



Figure 1. Stages of the National Institute of Standard and Technology

Figure 1 shows the stages of NIST which consist of several stages, namely as follows [27] :

1. Collection
Stage Collection is a series of data collection processes that include the process of identification, labeling, documentation, data retrieval from relevant data sources by protecting data integrity.
2. Examination
Stage Examination is the stage of examining data that has been collected using a forensic process automatically or manually by ensuring that the data obtained are genuine.
3. Analysis
Stage Analysis is the stage of analyzing data from the results of previous examinations, the data results will be analyzed in detail and thoroughly using methods that are justified by techniques and laws in proving the data.
4. Reporting
Stage Reporting is the stage of reporting the final results after obtaining digital evidence from the examination process and the results of the analysis of the investigated case are used as acceptable evidence.

2. METHODOLOGY

2.1 Research Scenario

Scenarios are needed to explain the stages of the forensic process in analyzing and obtaining evidence from web-based Facebook Messenger. In this research scenario, the evidence found is a notebook that will be investigated. The flow of this research case scenario can be seen in Figure 2.

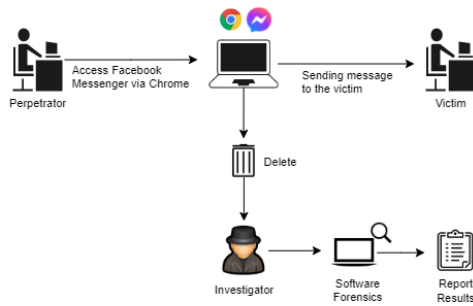


Figure 2. Flow of the Research Scenario

Figure 2 shows the flow of the case scenario of this research which started from the perpetrator accessing Facebook Messenger through the chrome browser. The perpetrator sends a message to the victim by offering an online social gathering slot, after the victim is interested in joining the social gathering then the perpetrator will ask the victim to send money to the perpetrator's account, the victim who feels disadvantaged because he does not get the results of the gathering then reports the incident to the police. The police will carry out the process of investigating the crime by securing evidence in the form of a laptop used by the perpetrator and submitting it to the investigator to investigate the evidence of the crime.

2.2 Research Stages

In the implementation stage, an investigator will carry out a series of search and data collection processes to obtain information related to the crime. The evidence was carried out through a web-based Facebook Messenger using a laptop by applying the NIST stage. The stages to be carried out consist of Collection, Examination, Analysis, Reporting.

2.2.1 Collection

The Collection stage is the initial stage of a series of data collection processes to support the investigation process in obtaining digital evidence. The evidence obtained was a laptop used by the perpetrators of the crime with the condition turned on and a charging cable. Information on the evidence belonging to the perpetrator can be seen in Table 1.

Table 1. Evidence Found at the Crime Scene



No	Evidence	Picture	Description
1	Laptop of the perpetrator		Laptop of the perpetrator, Asus was found at the scene in a condition that is turned on and connected to an internet connection
2	Charger		The cable charging used by the perpetrator

Table 1 shows the physical evidence found at the scene used by the perpetrator in committing a criminal crime which will be submitted to the investigator for investigation of evidence.

2.2.2 Examination

This stage is carried out by acquiring data contained in the perpetrator's laptop, the data acquisition process will be carried out using forensic tools to obtain activity history data from RAM storage and activity history from the web browser used by criminals while maintaining the authenticity of the data.

2.2.2.1 Belkasoft RAM Capturer

Belkasoft Live RAM Capturer is a forensic tool used to capture memory or RAM data acquisition from a criminal's laptop. The duration of the acquisition time depends on the RAM storage capacity of the criminal's laptop.

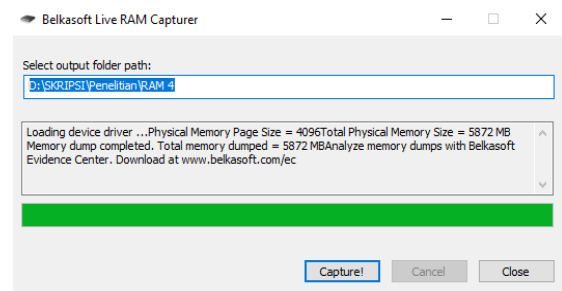


Figure 3. RAM Acquisition Has Been Successful

Figure 3 shows RAM data capture has been successfully carried out, the results of RAM data acquisition will be stored on partition D in the SKRIPSI/Research/RAM 4 folder with the RAM data size of 5872 MB. The result obtained from the acquisition of RAM is a file named 20211001 in .mem format with a size of 6,012,928 KB.

2.2.2.2 FTK Imager

After the volatile data has been successfully acquired, then the results of the acquisition are carried out by an imaging process, this imaging process is carried out by maintaining the integrity of the data so that the data does not change and can be examined by investigators. FTK Imager is a forensic tool used to perform the imaging process.

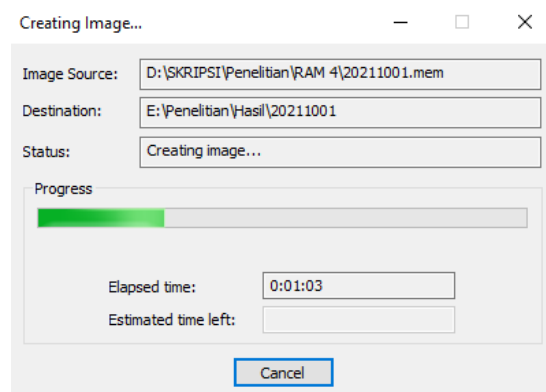


Figure 4. RAM Data Imaging Process

Figure 4 shows the imaging process carried out from the acquisition of RAM with the 20211001.mem file in partition D with the SKRIPSI\Penelitian\RAM 4\20211001.mem folder which will be stored in another storage in partition E with the Penelitian\ Hasil folder.

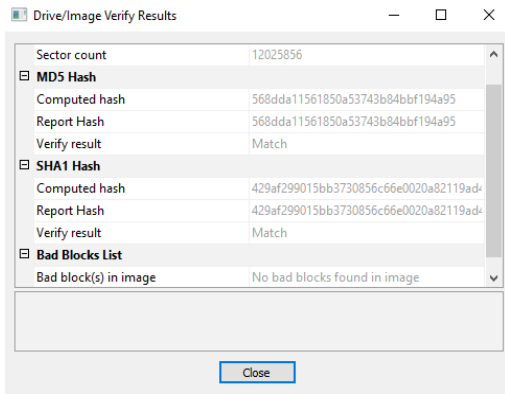


Figure 5. Hash Value Results

Figure 5 shows the hash value of the imaging results, there are two hash values, namely MD5 Hash and SHA1 Hash which are verified to match the original file. The same hash value indicates that the imaging process performed on the file has been successful with no changes.

2.2.2.3 Browser History Capturer

Browser History Capturer is a forensic tool used to retrieve data from web browsers used by perpetrators to commit crimes. Browser History Capturer can retrieve data from web browsers Chrome, Edge, Firefox, Internet Explorer & Legacy and the data can be obtained in the form of history, cache, and deleted history.

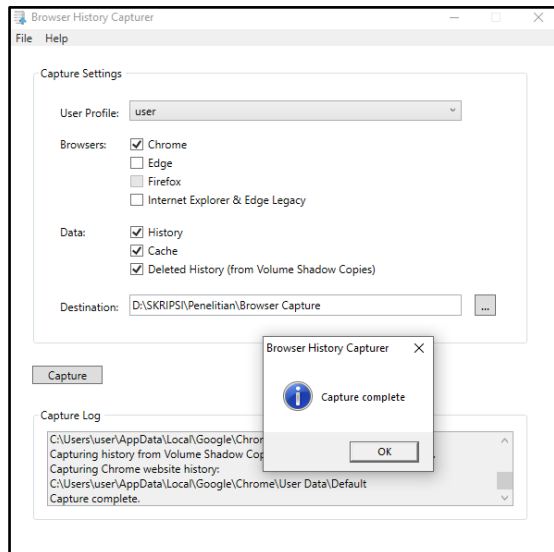


Figure 6. The Browser Capture Process Has Been Completed

Figure 6 shows the data capture process from the web browser used by the perpetrator has been successful. The capture results will be saved on partition D in the SKRIPSI\Penelitian\Browser Capture folder.

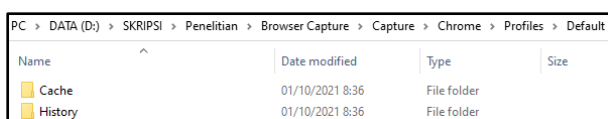


Figure 7. Cache and History Folders in the Capture Folder

Figure 7 shows the browser capture results that have been saved under the name of the Capture folder. In the Capture folder, there are two other folders named Cache and History.

2.2.3 Analysis

Stage Analysis is the stage to analyze or read the results of the data that has been obtained from the previous process. The results of the data will be examined in detail and thoroughly to obtain information as needed while maintaining the integrity of the data.

2.2.3.1 Browser History Examiner

Browser History Examiner is a forensic tool used to analyze or read the captured results from the Chrome browser obtained from the Browser History Capturer at the Examination stage. The results obtained from this tool are Bookmarks, Browser Settings, Cached Files, Cached Images, Cached Web Pages, Cookies, Downloads, Email Addressed, Favicons, Form History, Logins, Searches, Session Tabs, Thumbnails, and Website Visits.

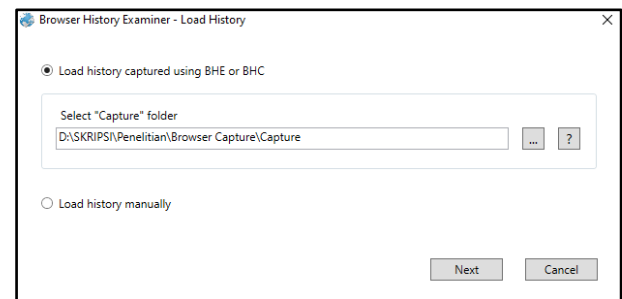


Figure 8. Load History from the Capture Folder

Figure 8 shows the load history menu display to select the data file to be used. In the "Select Capture Folder" section select the browser capture file located on partition D in the SKRIPSI\Penelitian\Browser Capture\Capture folder then click the "Load" button to continue the analysis process using the Browser History Examiner.

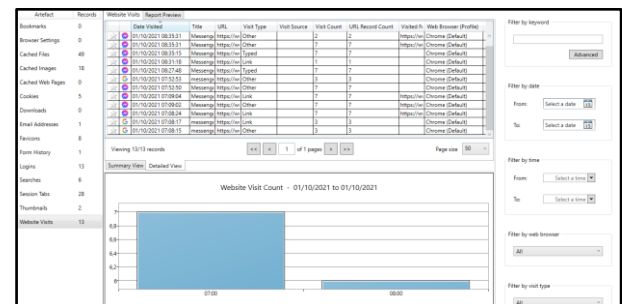


Figure 9. Display of the Browser History Examiner Tool

Figure 9 shows the results of data capture from the chrome browser which displays information on the type of artifacts you want to see from the chrome browser, browser history that has been accessed, graphs of browser access time, and search features to make it easier to search data using word filters, key, date, or web browser.

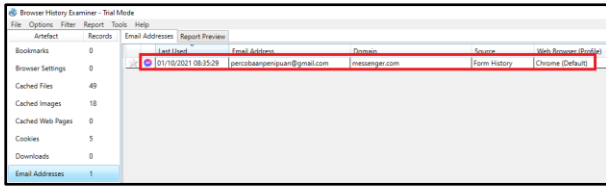


Figure 10. Perpetrator's EmailUsed to Login Messenger

Figure 10 shows the email belonging to the perpetrator in logging in to the Facebook Messenger service with the email address percobaanpenipuan@gmail.com which was accessed via the chrome web browser on October 01, 2021.

2.2.3.2 Browser History Viewer

Browser History Viewer is a forensic tool used to view or read the capture results from the chrome browser that have been obtained from the Browser History Capturer at the Examination stage. The results obtained from this tool are Website History and Cached Images from the chrome web browser. This data can be used as digital evidence in court.

Date Visited	Title	URL	Visit Count	Calculated Visit Count	Web Browser (Profile)
01/10/2021 08:35:32	Messenger	https://www.messenger.com/100004625624290	2	2	Chrome (Default)
01/10/2021 08:35:31	Messenger	https://www.messenger.com/100004625624290	2	2	Chrome (Default)
01/10/2021 08:35:31	Messenger	https://www.messenger.com/	7	7	Chrome (Default)
01/10/2021 08:35:15	Messenger	https://www.messenger.com/	7	7	Chrome (Default)
01/10/2021 08:31:18	Messenger	https://www.messenger.com/messenger_media?l=1	1	1	Chrome (Default)
01/10/2021 08:27:48	Messenger	https://www.messenger.com/	7	7	Chrome (Default)
01/10/2021 07:52:53	messenger - Penelusuran-Google	https://www.google.com/search?q=messenger&rlz=3	3	3	Chrome (Default)
01/10/2021 07:52:50	Messenger	https://www.messenger.com/	7	7	Chrome (Default)
01/10/2021 07:09:04	Messenger	https://www.messenger.com/	7	7	Chrome (Default)
01/10/2021 07:09:02	Messenger	https://www.messenger.com/	7	7	Chrome (Default)
01/10/2021 07:08:24	Messenger	https://www.messenger.com/	7	7	Chrome (Default)
01/10/2021 07:08:17	messenger - Penelusuran-Google	https://www.google.com/search?q=messenger&rlz=3	3	3	Chrome (Default)
01/10/2021 07:08:15	messenger - Penelusuran-Google	https://www.google.com/search?q=messenger&rlz=3	3	3	Chrome (Default)

Figure 11. Website History Results in Browser History Viewer

Figure 11 shows the results from website history with the results of the history of messenger pages that have been accessed. The results of the history show that the perpetrator accessed Facebook Messenger on October 1, 2021 at 07:08:24 using the chrome web browser.

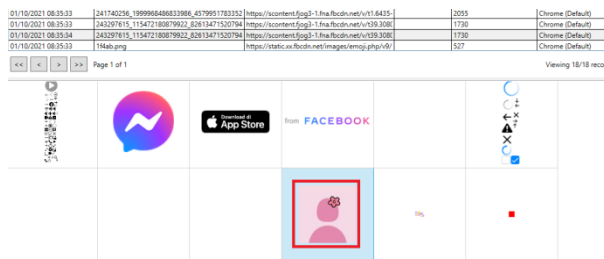


Figure 12. Cached Images Perpetrator's Profile Photo

Figure 12 shows the results of Cached Images in the form of a profile photo of the perpetrator's messenger account which was successfully taken from the chrome browser on October 01, 2021 at 08:35:34.

Date Visited	Title	URL	Visit Count	Calculated Visit Count	Web Browser (Profile)
01/10/2021 08:35:18	4h=AAu0eT5.png	https://static.xx.fbcdn.net/rsrc.php/v3j4c1a2m1/	1	1	Chrome (Default)
01/10/2021 08:35:33	241740256_199998486833866_4579951783352	https://content.fog3-1-fra.fbcdn.net/v/1.6435-	2055	2055	Chrome (Default)
01/10/2021 08:35:33	241740256_199998486833866_4579951783352	https://content.fog3-1-fra.fbcdn.net/v/1.6435-	2055	2055	Chrome (Default)
01/10/2021 08:35:33	243297615_115472180879922_82613471520794	https://content.fog3-1-fra.fbcdn.net/v/193-3008-	1730	1730	Chrome (Default)
01/10/2021 08:35:34	243297615_115472180879922_82613471520794	https://content.fog3-1-fra.fbcdn.net/v/193-3008-	1730	1730	Chrome (Default)
01/10/2021 08:35:33	184ab.png	https://static.xx.fbcdn.net/images/emogj.php/v/1	1	1	Chrome (Default)

Figure 13. Cached Images Victim's Profile Photo

Figure 13 shows the results of Cached Images in the form of a profile photo of the victim's Messenger account which was successfully taken from the chrome browser on October 1, 2021, at 08:35:33.

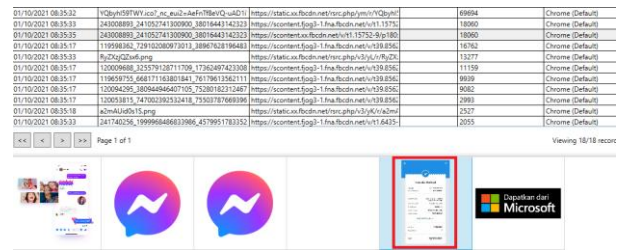


Figure 14. Cached Images of Payment Proofs

Figure 14 shows the results of Cached Images in the form of photos of proof of online social gathering payments sent by the victim to the perpetrator which were successfully taken from the chrome browser on October 1, 2021, at 08:35:353.

2.2.3.3 FTK Imager

The result of the RAM acquisition process using Belkasoft Live RAM Capturer produces a file named 20211001 with .mem format. The file will be used to obtain digital evidence using the FTK Imager tool.

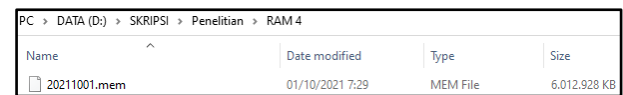


Figure 15. File from the Acquisition of RAM

Figure 15 displays files from the acquisition of RAM, the file will be analyzed and read the contents of the file to obtain information related to the crimes committed.

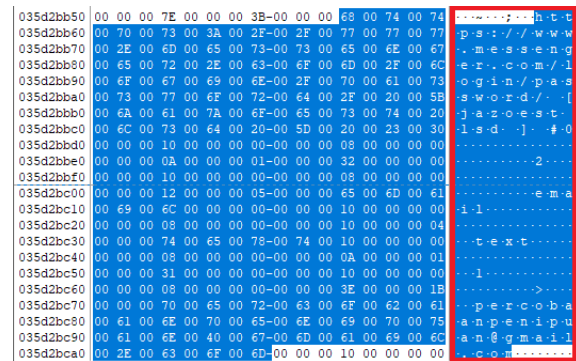


Figure 16. Results of Email Login Messenger Perpetrator's

Figure 16 shows the search results with the parameter "Messenger". The email used by the perpetrator to log in to Messenger is percobaanpenipuan@gmail.com with the URL https://www.messenger.com/login/password.

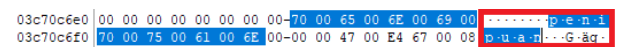


Figure 17. The perpetrator's Password Messenger

Figure 17 shows the findings in the form of a password from the perpetrator's Facebook Messenger account, namely penipuan.


```

0734bb000 41 72 69 73 61 6E 20 6D-65 6E 75 72 75 6E 20 67 arisan menurun g
0734bb010 65 74 20 36 20 4A 75 74-61 2F 31 20 6D 69 6E 67 et 6 Juta/1 ming
0734bb020 67 75 0D 0A 41 64 6D 69-6E 20 35 30 6B 2F 73 6C gu - Admin 50k/sl
0734bb030 6F 74 0D 0A 31 2E 20 28-41 64 6D 69 6E 29 0D 0A ot -1. (Admin)
0734bb040 32 2E 20 38 35 30 20 F0-9F 92 AB 0D 0A 33 2E 20 2. 850 $ -<- 3.
0734bb050 38 35 30 20 72 6F 6E 61-0D 0A 34 2E 20 38 30 30 850 rona -4. 800
0734bb060 20 F0 9F 92 AB 0D 0A 35-2E 20 37 35 30 20 6B 6F 8 -<- 5. 750 ko
0734bb070 6B 6F 0D 0A 36 2E 20 37-35 30 20 79 61 79 61 0D ko -6. 750 yaya
0734bb080 0A 37 2E 20 37 30 30 20-6C 69 6E 67 6C 69 6E 67 7. 700 lingling
0734bb090 0D 0A 38 2E 20 37 30 30-20 69 6C 61 6E 0D 0A 39 -8. 700 ilan
0734bb0a0 2E 20 36 30 30 20 67 61-6D 61 20 0D 0A 0D 0A 4B . 600 gama
0734bb0b0 65 65 70 20 6E 6F 20 63-61 6E 63 65 6C 0D 0A 53 eep no cancel
0734bb0c0 65 74 65 6C 61 68 20 6B-65 65 70 20 6E 6F 6D 6F etelah keep nomo
0734bb0d0 72 2C 20 63 61 6E 63 65-6C 20 64 65 6E 64 61 20 r, cancel denda
0734bb0e0 35 30 30 6B 0D 0A 0D 0A-54 72 61 6E 73 66 65 72 500k -Transfer

```

Figure 18. Evidence of the First Conversation

Figure 18 shows the findings using the “arisan” parameter. The search results obtained a text conversation sent by the perpetrator to the victim containing an online social gathering offer with a certain total income.

```

0155891f0 32 32 36 5D 2C 5C 22 53-6C 6F 74 20 79 61 6E 67 226],\Slot yang
015589200 20 6D 61 73 69 68 20 32-20 73 61 6D 61 20 34 20 masih 2 sama 4
015589210 78 61 20 6B 61 6B 20 3F 5C 22 2C 66 61 6C 73 65 ya kak \, false

```

Figure 19. Evidence of the Second Conversation

Figure 19 shows the findings in the form of a conversation text about the victim asking for an empty social gathering number slot.

```

06b0452f0 2C 5C 22 41 6E 64 61 3A-20 49 79 61 20 6B 61 6B \,Anda: Iya kak
06b045300 2C 20 6D 61 75 20 79 61-6E 67 20 6D 61 6E 61 3F mau yang mana?

```

Figure 20. Evidence of the Third Conversation

Figure 20 shows the findings in the form of a conversation text about the perpetrator agreeing and asking the victim which slot to follow.

```

03c7e2840 22 41 6B 75 20 6D 61 75-20 61 6D 62 69 6C 20 79 \Aku mau ambil y
03c7e2850 61 6E 67 20 73 6C 6F 74-20 32 20 6B 61 6B 5C 22 ang slot 2 kak\

```

Figure 21. Evidence of the Fourth Conversation

Figure 21 shows the findings in the form of a conversation text about the victim informing the number of the slot taken.

```

084706200 3A 20 54 72 61 6E 73 66-65 72 20 6B 65 20 72 65 : Transfer ke re
084706210 6B 20 42 52 49 3A 20 34-35 34 35 30 37 32 36 34 k BRI: 454507264
084706220 30 33 36 31 38 36 20 61-2F 6E 20 52 49 4E 41 20 036186 a/m RINA
084706230 45 4C 44 49 56 41 00 00-91 02 00 00 5F 00 00 00 ELDIVR

```

Figure 22. Evidence of the Fifth Conversation

Figure 22 shows the findings in the form of a text conversation about the perpetrator asking the victim to send money to the account number listed.

```

135aca8c0 61 3A 20 4A 61 6E 67 61-6E 20 6C 75 70 61 20 6B : Jangan lupa k
135aca8d0 69 72 69 6D 20 62 75 6B-74 69 20 74 72 61 6E 73 kirim bukti trans
135aca8e0 66 65 72 20 6B 61 6C 6F-20 73 75 64 61 68 20 64 fer kalo sudah d
135aca8f0 69 6B 69 72 69 6D 5C 22-2C 66 61 6C 73 65 2C 5B kirim \, false,

```

Figure 23. Evidence of the Sixth Conversation

Figure 23 shows the findings in the form of a text conversation about the perpetrator reminding the victim to send proof of transfer of arisan money to the perpetrator's account.

```

0484e5690 2C 5C 22 55 64 61 68 20-61 6B 75 20 74 66 20 6B \,Udah aku trf k
0484e5690 61 6B 5C 22 2C 66 61 6C-73 65 2C 5B 32 33 32 38 an \, false, [2323

```

Figure 24. Evidence of the Seventh Conversation

Figure 24 shows the findings in the form of a text conversation about the victim informing the perpetrator that the victim has sent the arisan money to the victim's account number.

```

15d032200 5C 5C 22 3A 5C 5C 5C 22-4F 6B 65 2C 20 6E 61 6E \,Oke, nan
15d032210 74 69 20 61 6B 75 20 68-75 62 75 6E 67 69 6E 20 ri aku hubungin
15d032220 6C 61 67 69 20 79 61 20-62 75 61 74 20 70 65 6E lagi ya buat pen
15d032230 63 61 69 72 61 6E 20 61-72 69 73 61 6E 20 6E 79 cairan arisan ny
15d032240 61 5C 5C 5C 22 2C 5C 5C-5C 22 69 6E 69 74 69 61 \,Oke,

```

Figure 25. Evidence of the Eighth Conversation

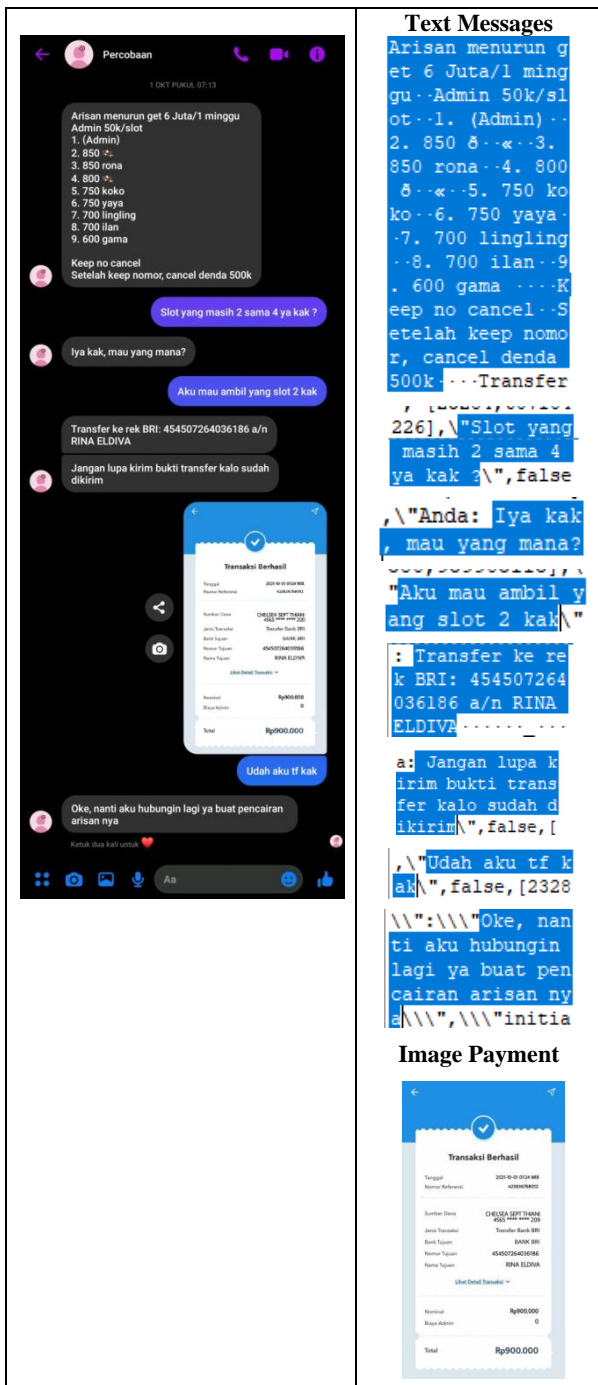
Figure 25 shows the findings in the form of a conversation text about the perpetrator informing the victim if the arisan disbursement will be accepted.

2.2.4 Reporting

Reporting is the last stage carried out by investigators after obtaining digital evidence. At this stage, the investigator will make a documentation report from the results of the analysis on the evidence found in detail. This Reporting stage explains the identification carried out, an explanation of the forensic process, and the data resulting from the use of forensic tools. The evidence found in this study will be compared with the evidence provided by the victim, which can be seen in Table 2.

Table 2. Findings Evidence from the perpetrator's laptop

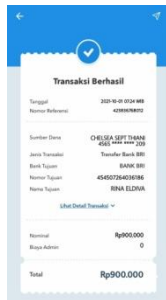
Evidence of messenger conversations from the victim's smartphone	The results of evidence found from the perpetrator's laptop
--	---



Text Messages

Arisan menurun g
et 6 Juta/1 ming
gu Admin 50k/sl
ot --1. (Admin) --
2. 850 8 -- 3.
850 rona -- 4. 800
8 -- 5. 750 ko
ko -- 6. 750 yaya
-- 7. 700 lingling
-- 8. 700 ilan -- 9
. 600 gama -- K
keep no cancel -- S
etelah keep nomo
r, cancel denda
500k -- Transfer
[226], Slot yang
masih 2 sama 4
ya kak ?", false
,"Anda: Iya kak
, mau yang mana?
"Aku mau ambil y
ang slot 2 kak"
: Transfer ke re
k BRI: 454507264
036186 a/n RINA
ELDIVA
a: Jangan lupa k
irim bukti trans
fer kalo sudah d
ikirim", false, [
,"Udah aku tf k
ak", false, [2328
": ""Oke, nan
ti aku hubungin
lagi ya buat pen
cairan arisan ny
a", ""initia

Image Payment



Based on Table 2, the digital evidence found on the perpetrator's laptop in the form of a history of conversational texts sent via Facebook Messenger has similarities with the conversation evidence provided by the victim. In the table, it can be seen that the perpetrator is the person who communicated with the victim via Facebook messenger, the digital evidence found on the perpetrator's laptop has similarities with the evidence of the conversation history on Facebook Messenger on the victim's smartphone such as conversation text and images.

2.2.5 Results

Results of the analysis that have been carried out in this study using forensic tools to obtain digital evidence and carry out forensic processes on Facebook Messenger running on the

Chrome web browser. The results of the analysis process using a forensic tool can be seen in Table 3.

Table 3. Results of the Analysis Using the Tool

No	Information	Forensic Tools		
		Belkasoft + FTK Imager	Browser History Capturer + Browser History Examiner	Browser History Capturer + Browser History Viewer
1	Email	✓	✓	-
2	Password	✓	-	-
3	Images	-	-	✓
4	Text Conversation	✓	-	-
5	Browser History	✓	✓	✓

Table 3 shows the results of the analysis that has been carried out on the Facebook Messenger service running on the Chrome web browser using forensic tools. The results obtained after performing the RAM Capturer to see RAM activity whose results were analyzed using FTK Imager managed to obtain digital evidence in the form of an email used by the perpetrator to log in to Messenger (percobaanpenipuan@gmail.com) and password (fraud), conversation text, and history. browsers. The Browser History Capturer tool that is used to capture the browser to view the history or activity of the web browser will be analyzed using the Browser History Examiner and Browser History Viewer. The Browser History Capturer tool managed to obtain digital evidence in the form of the perpetrator's email and web browser history. The Browser History Viewer tool managed to obtain digital evidence in the form of Images and Web Browser History.

3. CONCLUSION

The forensic process carried out with fraud cases on the web-based Facebook Messenger service has succeeded in obtaining digital evidence of the perpetrator's messenger account email, the perpetrator's messenger account password, images sent by the victim, profile photos of the perpetrator, and the victim, the text of the conversation between the perpetrator and the victim, and history web browser using forensic tools. The results were obtained using the tool Belkasoft Live RAM Capturer which was read using the tool FTK Imager with a percentage of 80% obtained evidence of Email, Password, Conversation Text, and Web Browser History. The results of browser capture using the tool Browser History Capturer which is read with the tool Browser History Examiner with a percentage of 40% obtain evidence of Email and Web Browser History. The tool Browser History Viewer with a percentage of 40% obtain evidence of Images and Web Browser History. This research applies the stages of the National Institute of Standard Technology (NIST), so that future research is expected to use different stages. This research using the Windows 10 operating system and using Chrome web browser, further research can be carried out on other operating systems, such as Linux and macOS by using other web browsers.

4. REFERENCES

[1] Y. N. Kunang and A. Khristian, "Implementation of Forensic Procedures for Whatsapp Artifact Analysis on

- Android Phones,” vol. 2, no. 1, pp. 59–68, 2016.
- [2] 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.
- [3] M. Fitriana, K. A. AR, and J. M. Marsya, “Application of the National Institute of Standards and Technology (Nist) Methods in Digital Forensic Analysis for Handling Cyber Crime,” *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 4, no. 1, p. 29, 2020, doi: 10.22373/cj.v4i1.7241.
- [4] R. A. Bintang, R. Umar, and A. Yudhana, “Analysis of Facebook Lite Social Media with Forensic tools using the NIST Method,” *Techno (Jurnal Fak. Tek. Univ. Muhammadiyah Purwokerto)*, vol. 21, no. 2, p. 125, 2020, doi: 10.30595/techno.v21i2.8494.
- [5] M. Riskiyadi, “Forensic Investigation of Digital Evidence in Revealing Cybercrime,” *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 2, pp. 12–21, 2020, doi: 10.14421/csecurity.2020.3.2.2144.
- [6] I. Anshori, K. E. Setya Putri, and U. Ghoni, “Analysis of Digital Evidence on Facebook Messenger Applications on Android Smartphones Using the NIJ Method,” *IT J. Res. Dev.*, vol. 5, no. 2, pp. 118–134, 2020, doi: 10.25299/itjrd.2021.vol5(2).4664.
- [7] 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.
- [8] N. Anggraini *et al.*, “Forensic Analysis of Whatsapp Messenger on Android Smartphones,” vol. XII, no. 1, pp. 83–100, 2020.
- [9] M. Iqbal and I. Riadi, “Forensic WhatsApp based Android using National Institute of Standard Technology (NIST) Method,” *Int. J. Comput. Appl.*, vol. 177, no. 8, pp. 1–7, 2019, doi: 10.5120/ijca2019919443.
- [10] M. F. Sidiq and M. N. Faiz, “Review of Web Browser Forensics Tools to Support Digital Evidence Searching,” *J. Edukasi dan Penelit. Inform.*, vol. 5, no. 1, p. 67, 2019, doi: 10.26418/jp.v5i1.31430.
- [11] T. Rochmadi, “Live Forensics for Anti-Forensic Analysis on a Web Browser Case Study Browzar,” *Indones. J. Bus. Intell.*, vol. 1, no. 1, p. 32, 2019, doi: 10.21927/ijubi.v1i1.878.
- [12] W. Sanjaya, B. Sugiantoro, and Y. Prayudi, “An Offline Forensic Method For Digital Artifact Analysis In TOR Browser On Linux Operating System,” *JITU J. Inform. Technol. Commun.*, vol. 4, no. 2, pp. 41–51, 2020, doi: 10.36596/jitu.v4i2.345.
- [13] D. Setiawan, R. Setiawan, R. Karunia, and I. W. S. Wicaksana, “Comparing Web Browser Performance,” *Ilmu Komput. Univ. Gunadarma*, vol. 1, no. 1, pp. 1–6, 2007.
- [14] B. Y. Prasetyo and I. Riadi, “Investigation Cyberbullying on Kik Messenger using National Institute of Standards Technology Method,” *Int. J. Comput. Appl.*, vol. 174, no. 17, pp. 34–41, 2021, doi: 10.5120/ijca2021921060.
- [15] A. P. Utami, “Mobile Forensics Analysis of Line Messenger on Illegal Drug Transaction Case using National Institute of Standard Technology (NIST) Method,” vol. 183, no. 32, pp. 23–33, 2021.
- [16] 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.
- [17] I. Riadi, R. Umar, and I. M. Nasrulloh, “Digital Forensic Analysis on Frozen Solid State Drive Using the National Institute of Justice (Nij),” *Elinvo (Electronics, Informatics, Vocat. Educ.)*, vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.
- [18] D. T. Yuwono and Y. W, “Comparative Analysis of File Carving with the Nist Method,” *J. Sains Komput. dan Teknol. Inf.*, vol. 2, no. 2, pp. 1–6, 2020, doi: 10.33084/jsakti.v2i2.1472.
- [19] T. D. Larasati, “Live Forensics Comparison of Instant Messenger Applications Live Forensics Analysis for Comparing Instant Messenger Applications (Line, Facebook, and Telegram) on Windows 10 Operating System. Live Forensics,” 2017.
- [20] A. Fauzan, I. Riadi, and A. Fadlil, “Digital Forensics Analysis on Line Messenger for Cybercrime Handling,” *Annu. Res. Semin.*, vol. 2, no. 1, pp. 159–163, 2017.
- [21] V. R. G. Leri and I. Riadi, “Data Search for Pornographic Content on Twitter Services using National Institute of Standard and Technology (NIST) Method,” *Int. J. Comput. Appl.*, vol. 183, no. 24, pp. 25–31, 2021, doi: 10.5120/ijca2021921610.
- [22] 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.
- [23] C. K. Herawati, “Forensic Browser on Facebook Services using National Institute of Standards Technology Method,” vol. 183, no. 30, pp. 17–24, 2021.
- [24] W. Y. Sulisty, 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.
- [25] S. D. Utami, C. Carudin, and A. A. Ridha, “Live Forensic Analysis on Whatsapp Web for Proving Electronic Transaction Fraud Cases,” *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 24–32, 2021, doi: 10.14421/csecurity.2021.4.1.2416.
- [26] S. K. Saad, R. Umar, and A. Fadlil, “Forensic Analysis of Dropbox Applications on Android Using the NIST Method,” *Semin. Nas. Din. Inform.*, pp. 119–123, 2020.
- [27] D. Muallfah and R. A. Ramadhan, “Digital Forensic Analysis of CCTV Camera Recordings Using the NIST (National Institute of Standards Technology) Method,” *IT J. Res. Dev.*, vol. 5, no. 2, pp. 171–182, 2020, doi: 10.25299/itjrd.2021.vol5(2).5731.