Forensic Analysis of Web-based Instant Messenger Applications using National Institute of Justice Method

Larassaty Chandra Pakaya
Departement of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

Currently, instant messenger applications are not only available in the form of applications on smartphones but can also be accessed through a web browser, one of which is Telegram Web. Using Telegram as a web platform provides convenience to its users. However, with this convenience, potential vulnerabilities can attract the attention of digital criminals or cybercrime. Therefore, this research aims to investigate forensic digital crimes related to web-based Telegram running on the Google Chrome browser using the National Institute of Justice (NIJ) Method and several forensic tools such as FTK Imager, Browser History Capturer, Browser History Examiner, and OSForensics. The results of this study are in the form of the perpetrator's telephone number obtained using Browser History Examiner,45 chats between the victim and the perpetrator that were deleted and the perpetrator's account obtained using FTK Imager, and images contained in the victim and perpetrator's chat such as two proof of transfer and three screenshots of tasks given by the perpetrator obtained using OSForensics.

Keywords

Cybercrime, Digital Evidence, Google Chrome, National Institute of Justice (NIJ), Telegram

1. INTRODUCTION

Since internet-based instant messenger (IM) services emerged, telecommunications have increased and spread quickly to Indonesia [1]. IM applications now have web-based services; IM application users can now use web-based IM application services in addition to smartphone-based applications, which can facilitate users, especially those who work more in front of a computer [2]. Instant messenger applications, especially those based on Web services, are more likely to be targeted by digital crime or cybercrime perpetrators. The vulnerability of web-based instant messenger applications can be utilized by irresponsible parties to commit digital crimes [3].

Telegram is one of the instant messenger application services that is growing in Indonesia [4]. Telegram is the world's 6th most popular instant messenger application. Telegram is an instant messenger service based on cloud and voice services. According to a source from Statista, The total number of users of this instant messaging application reached 550 million people as of January 2022 [5].

Currently, many widespread users of the Telegram application also raise several problems, including cybercrime, such as drug trafficking, terrorism, cyberbullying, fraud, movie piracy, illegal content, and human trafficking [6]. As reported by (www.detiknet.com), after Indo XXI and similar sites were taken down, piracy of movies and series became rampant on Telegram. In response, the Ministry of Communication and Information Technology (Kominfo) emphasized that would not hesitate to block. However, blocking cannot be done if the pirated movie or series is spread through private conversations on Telegram [7]. A comprehensive UN study explains that cybercrime is limited to targeting the confidentiality, integrity, and availability of data or computer systems [8].

Telegram apps can be used as digital evidence containing various information, including user profiles, text conversations, contact lists, images, friend invitations, app activity reports, and text statuses published by account owners or users. Various methods or frameworks can be used to collect such digital evidence from Telegram apps. Some of these include the National Institute of Justice (NIJ), Integrated Digital Forensics Identification Framework (IDFIF), Chain of Custody (COC), and National Institute of Standards and Technology (NIST). Each of these methods has different steps in the digital evidence acquisition process.

This research aims to obtain digital evidence of freelance fraud cases on Telegram that run on the Google Chrome web browser using the National Institute of Justice (NIJ) method. The stages carried out in the NIJ method include Preparation, Collection, Examination, Analysis, and Reporting. The NIJ method describes how the research process is carried out so that a more systematic understanding of the various stages of research can be used so that it can be used as a reference in further investigation [9].

2. LITERATURE STUDY

2.1 Digital Forensics

Digital forensics is a part of forensic science used to investigate and probe the discovery of digital device material (data) and contents [10]. Experts say digital forensics is a collection of methods, including techniques and procedures for searching and collecting physical and digital device-based evidence as legal evidence in the courtroom. Digital forensics must also be applied to find facts or evidence related to the crime so that the crime is apparent in court [11]. Based on the digital devices involved, digital forensics is technically divided into several branches, including Computer Forensics, Network Forensics, Application Forensics, and Device Forensics [12].

2.2 Digital Evidence

Digital evidence is an abstraction of some digital object or event. When a person operates a computer for various things, such as sending emails or other activities, the activity generates a data trail that can provide an event description of what happened before. Digital evidence is very vulnerable to data changes. Therefore, it requires extra careful handling to maintain the integrity of the evidence [13]. Digital evidence can be found on various devices such as computer hard drives, cell phones, iPads, Pen Drives, digital cameras, CDs, DVDs, diskettes, computer networks, the internet, etc. Digital evidence is often related to digital or electronic crimes, such as pornography, prostitution, identity theft, phishing, or fraud involving credit cards or ATMs [14].

2.3 Telegram

Telegram is an application that allows users to send end-to-end encrypted secret chat messages for added security [15]. Telegram can send pictures, videos, and documents such as Word, Excel, PDF, etc., without specifying the file size to be sent, and the location can also be sent easily. Telegram is a lightweight, fast, ad-free, and free application. The Telegram application can create groups of up to 5,000 people. Telegram can also be accessed using a computer [16]. The telegram logo can be seen in Figure 1.

Figure 1: Telegram logo

Figure 1 is the logo of the telegram instant messenger application. This application has advantages: Cloud-Based Massege, Secret Chat, Does not burden memory, Channel Features, automatic message deletion features, and telegram bot features [17].

2.4 Cybercrime

Cybercrime is a cybercrime committed by individuals or groups that attacks computer security systems or data. Cybercrime generally refers to illegal activities involving computers, other digital devices, or computer networks [18]. Currently, many cyber crimes sometimes occur without realizing it, such as cyberbullying, where many social media users sometimes say indecent words or comments that cause mental distress to someone [19].

2.5 Web Browser

A web browser is an application for browsing, rendering, and retrieving content from various information sources on the Internet network. This web browser can identify information sources from the internet network through web pages, videos, images or other content [20].

Figure 2: Types of Web Browsers

Figure 2 shows various browser logos, such as Google Chrome, Mozilla Firefox, Internet Explorer, Safari, Opera Mini, etc. Web browsers also have several benefits: ease of access, easy to download, and ease of browsing the internet [21].

2.6 FTK Imager

FTK Imager is a powerful digital evidence tool that can create drive or partition images, analyze data, and recover files [22]. The application can also mount images as physical drives and has very powerful access to digital evidence. Users can perform basic forensic analysis and recovery directly from within FTK Imager. This tool can also be used to capture the system registry and RAM. FTK Imager supports various image sources and hard drives and can convert images and other image types [23].

2.7 Browser History Capturer

Browser History Capturer easily capture web browser history from Windows computers. The tool can be run from a USB dongle or via a Remote Desktop connection to record history from Chrome, Edge, Firefox, Internet Explorer, etc web browsers. The history file is copied to the selected destination in its original format, allowing it to be analyzed later using the tool of choice [24].

2.8 Browser History Examiner

Browser History Examiner is a forensic software that can capture, extract, and analyze internet history from major desktop browsers such as Chrome, Edge, Firefox, Internet Explorer, and Safari. Browser History Examiner can analyze various data types, including website visits, searches, downloads, and cache files. Some of the features of Browser History Examiner include Website Activity Timeline, Remote Data Capture, Cached Image Viewer, Search History Parser, URL Category Database, Dynamic Reporting and Data Export, Advanced Filtering, Recover Deleted History, Cached Web Page Viewer, Email Address Parser, and SON Viewer. Browser History Examiner can filter data by keyword, time, URL, and category [24].

2.9 OSForensics

OSForensics is a digital forensics software that collects and analyzes digital evidence from operating systems. The software is developed by PassMark Software and is designed to assist forensic professionals in obtaining critical information from computers or other storage devices. Some of the main features of OSForensics include Forensic Search, File Analysis, Report Generation, Deleted File Recovery, and User Activity Timeline [25].

3. RESEARCH METHODS

This research uses the investigation process of the National Institute of Justice (NIJ) forensic analysis method. The NIJ method consists of 5 stages. The scheme of the five stages can be seen in Figure 3, providing a structured framework for conducting thorough hardware and software forensic analysis in freelance fraud cases.

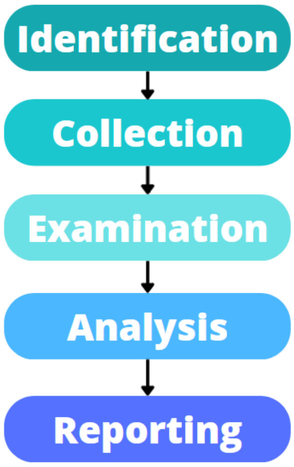


Figure 3 : National Institute of Justice method

Figure 3 illustrates the steps of the National Institute of Justice (NIJ) method. The initial stage is the identification stage, where all the equipment required for the investigation is prepared. The next step is the collection stage, where evidence such as files, documents, data, and physical evidence are collected. After that, the examination stage is the stage of examining the data obtained from the previous stage. The next step is the analysis stage, where the examination results are analyzed in depth. Finally, the reporting stage is the preparation of a report containing the results of the analysis that has been carried out.

4. RESULTS AND DISCUSSION

This research discusses the simulation of crime cases, especially cybercrime, in the case of freelance fraud on the Telegram web. The simulation is conducted in three sequential steps, starting with the pre-incident stage, then the incident stage, and ending with the post-incident stage. In the pre-incident phase, the perpetrator plans or prepares the fraudulent act against the victim. The pre-incident stage can be found in Figure 4.

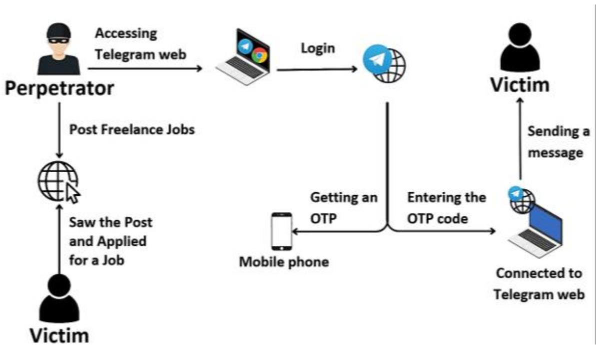


Figure 4 : Pre-Incident Freelance Fraud Case

Figure 4, the perpetrator accesses the telegram with a Chrome web browser using a laptop, then logs in to the telegram web by entering the telephone number and verifying with the OTP code obtained on the perpetrator's cellphone. After that, the perpetrator enters the OTP code. Into the laptop used to log in to the Telegram web. After the laptop is connected to the telegram web, the perpetrator sends a message to the victim.

The second stage in case simulation is the incident stage. The incident phase is where the perpetrator performs actions to deceive the victim. The incident stage can be seen in Figure 5.

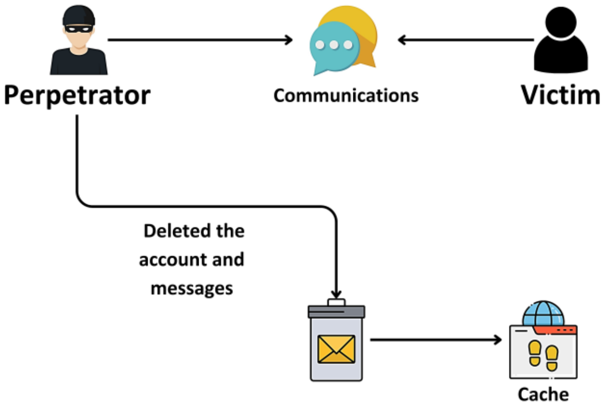


Figure 5 : Incidents of Freelance Fraud Cases

Figure 5, the victim who was tempted by easy work and high pay accepted the job. Finally, the victim communicated with the perpetrator via web telegram. After the victim accepted the offer, the perpetrator gave the victim the first task, like one of the actress's YouTube videos. After that, the victim completes the task and earns the income as promised, and so on. Until arriving at the fourth task, which is a special task. Here, the victim can transfer several amounts of money with high interest. Because she was interested, the victim chose the largest amount of money. After sending proof of transfer to the perpetrator, the victim is told to wait for verification for one hour. But after an hour, the perpetrator deleted the account and chatted with the victim.

The third stage in the case simulation is the post-incident stage. Post-incident is the phase after the perpetrator has successfully committed fraud against the victim. The post-incident stage can be seen in Figure 6.

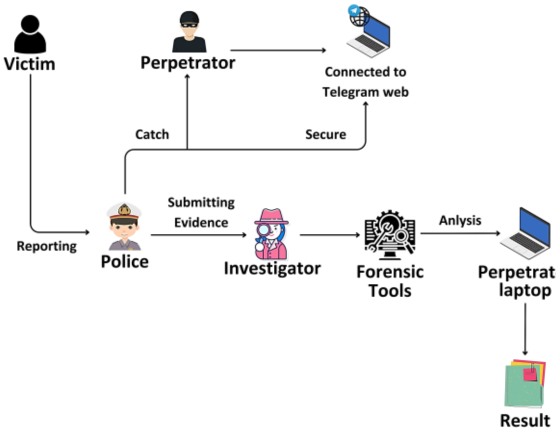


Figure 6 : Post Incident Freelance Fraud Case

In Figure 6, the victim who felt cheated reported the perpetrator to the police by showing evidence of the perpetrator's account and chat and proof of transfers made by the victim, as shown in the picture below. After receiving the report, the police arrested and confiscated the perpetrator's laptop as evidence. Furthermore, the evidence was handed over to the investigator to be analyzed using forensic tools to collect digital evidence that could be used in the investigation. After analyzing and obtaining digital evidence, the investigator reports the findings and ensures that every process follows applicable law.

4.1 Identification

The identification stage is the first step in the search for digital evidence, which involves preparing the tools used to support the investigation in collecting digital evidence. Details of the tools to be used can be found in Table 1.

Table 1 : Tools and Materials

Name	Description
Laptop	Media used to obtain data.
Telegram	Object application for forensic processes
Google Chrome	Web browser for object application access
FTK Imager	Produce evidence of the perpetrator's deleted chat and the perpetrator's username.
Browser History Capturer	Captures data from the web browser Google Chrome
Browser History Capturer	Captures data from the web browser Google Chrome
Browser History Examiner	Produce evidence in the form of a phone number used by the perpetrator when logging in to the telegram web.
OSForensics	Produce evidence of deleted images in conversations.

Table 1 shows the tools that will be set up to investigate freelance fraud cases and generate digital evidence. The tools consist of 2 types, namely hardware and software. Hardware executes software instructions and processes data in a computer or electronic device, making them essential components of the forensic process in uncovering and prosecuting fraudsters.

4.2 Collection

The collection stage is collecting, securing physical evidence and collecting data. Physical evidence found is one laptop found in a lit state. Physical evidence can be seen in Figure 7.

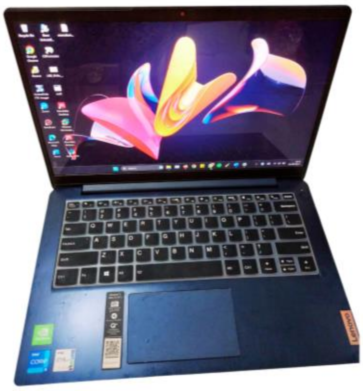


Figure 7 : Physical Evidence Found

Figure 7 shows the perpetrator's Lenovo laptop, which was found turned on. The laptop was then forensically processed by retrieving data from the laptop's RAM using the FTK Imager and Browser History Capturer tools.

Stages in the RAM data retrieval process using the FTK Imager tool. FTK Imager is used to retrieve data and information from memory. The memory retrieval feature can be seen in Figure 8.

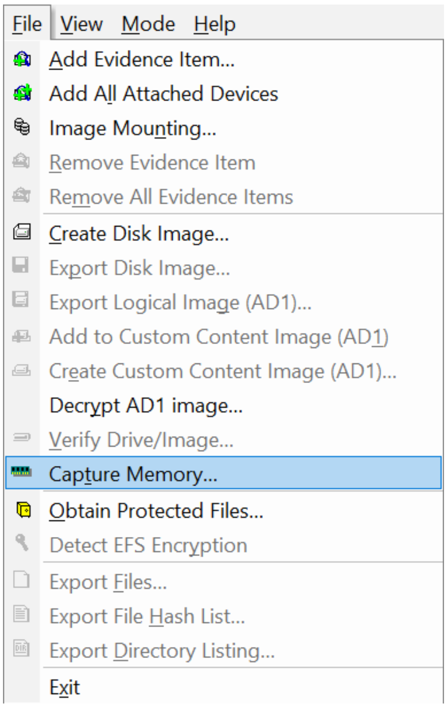


Figure 8 : FTK Imager Capture Memory feature

Figure 8 is the memory retrieval feature in FTK Imager. FTK Imager will retrieve data and information from all applications on the used device. The results of retrieving RAM data using the FTK Imager tool are files with the .mem extension. The results of this data retrieval are shown in Figure 9.

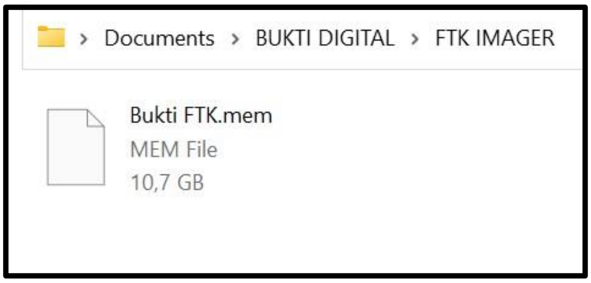
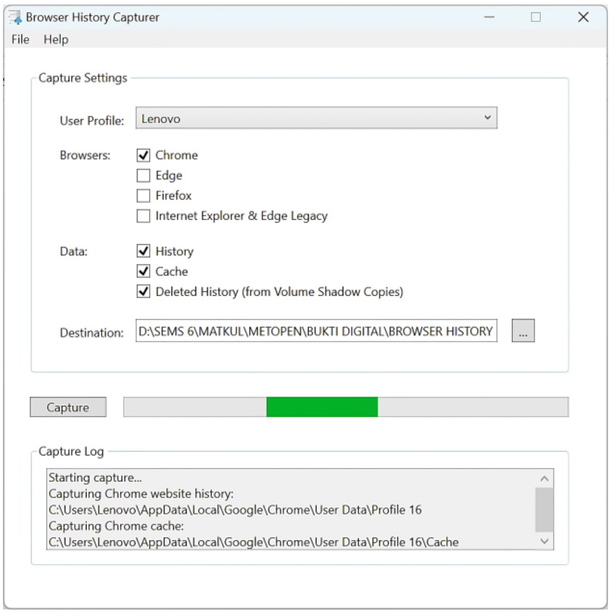


Figure 9 : FTK Imager Capture File

Figure 9 shows the result of the RAM data capture process, where the captured file is 10.7 GB and named "Bukti FTK.mem."

Stages in the process of capturing browsing history using the Browser History Capturer tool. This tool will retrieve data from the Google Chrome web browser. The capture process in the Browser History Capturer can be seen in Figure 10.



Browser History Capturer

Capture Settings

User Profile: Lenovo

Browsers: ☑ Chrome ☐ Edge ☐ Firefox ☐ Internet Explorer & Edge Legacy

Data: ☑ History ☑ Cache ☑ Deleted History (from Volume Shadow Copies)

Destination: D:\SEMS 6\MATKUL\METOPEN\BUKTI DIGITAL\BROWSER HISTORY

Capture Log

```
Starting capture...
Capturing Chrome website history:
C:\Users\Lenovo\AppData\Local\Google\Chrome\User Data\Profile 16
Capturing Chrome cache:
C:\Users\Lenovo\AppData\Local\Google\Chrome\User Data\Profile 16\Cache
```

Figure 10 : Browser History Capturer Capture Process

Figure 10 shows the browsing history capture process steps using the Browser History Capturer. This tool captures browsing history on the Google Chrome web browser. Browser History Capturer functions to record, analyze, and report browsing history on a web browser. The capture results can be seen in Figure 11.

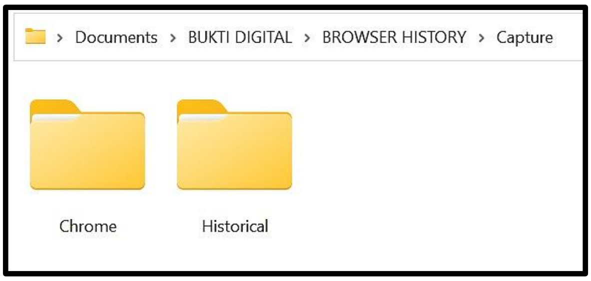


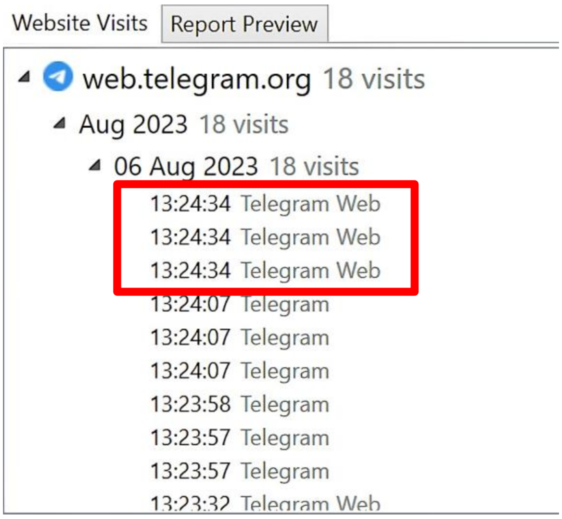
Figure 11 : Capture Results Browser History Capturer

Figure 11 shows the contents of the Capturer folder, namely the folder Chrome and Historical. These folders are the result of the Google Chrome web browser capture process.

4.3 Examination

At this stage, the data that has been obtained previously is examined. The examination is carried out on the captured memory data. To read the data that has been obtained, forensic tools such as FTK Imager, Browser History Examiner, and OSForensics are used.

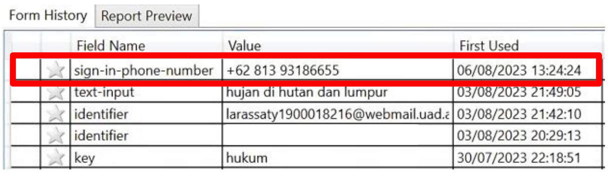
Browser History Examiner is used to open the capture results of the browsing history on the web browser. Browser History Examiner will take all the data in the "Capture" folder and perform an extraction process to collect the information contained in the browsing history. Using this tool, we will look for login information containing the perpetrator's phone number when accessing the web telegram.



```
web.telegram.org 18 visits
  Aug 2023 18 visits
    06 Aug 2023 18 visits
      13:24:34 Telegram Web
      13:24:34 Telegram Web
      13:24:34 Telegram Web
      13:24:07 Telegram
      13:24:07 Telegram
      13:24:07 Telegram
      13:23:58 Telegram
      13:23:57 Telegram
      13:23:57 Telegram
      13:23:32 Telegram Web
```

Figure 12 : Login Information

Figure 12 shows that the perpetrator accessed Telegram via the web version with that date and time.

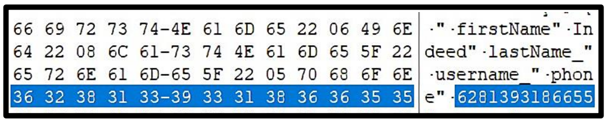


Field Name	Value	First Used
sign-in-phone-number	+62 813 93186655	06/08/2023 13:24:24
text-input	hujan di hutan dan lumpur	03/08/2023 21:49:05
identifier	larassaty1900018216@webmail.uad.a	03/08/2023 21:42:10
identifier		03/08/2023 20:29:13
key	hukum	30/07/2023 22:18:51

Figure 13 : Phone Number

Figure 13 shows that the perpetrator performed the login process using the phone number while accessing Telegram Web. This information shows that the perpetrator has used the phone number to log into the Telegram Web account, linking the login activity with access to the Telegram Web service.

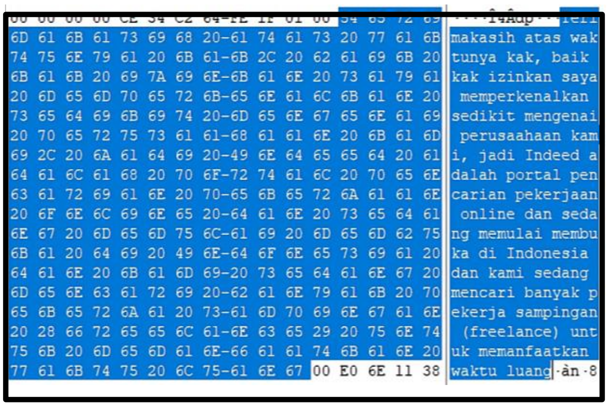
FTK Imager is used to read the captured RAM data. FTK Imager will read the RAM data that has been captured previously and is in the ".mem" format. By using this tool, can search for the perpetrator's account and the conversation between the perpetrator and the victim.



```
66 69 72 73 74-4E 61 6D 65 22 06 49 6E  ·"·firstName"·In
64 22 08 6C 61-73 74 4E 61 6D 65 5F 22  deed"·lastName_"
65 72 6E 61 6D-65 5F 22 05 70 68 6F 6E  ·username_"·phon
36 32 38 31 33-39 33 31 38 36 36 35 35  e"·6281393186655
```

Figure 14 : Perpetrator's Account

Figure 14 is the perpetrator's account obtained by searching using the keyword phone number used by the perpetrator when logging in. The name used by the perpetrator is "Indeed."

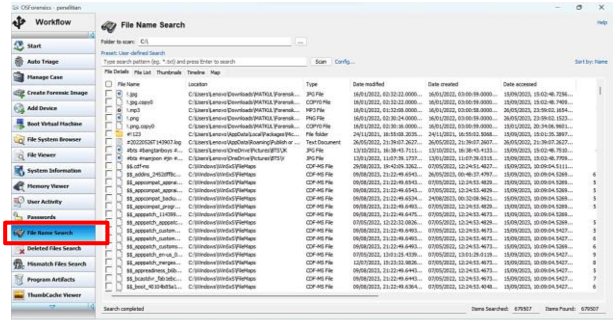


```
6D 61 6B 61 73 69 68 20-61 74 61 73 20 77 61 6B  makasih atas wak
74 75 6E 79 61 20 6B 61-6B 2C 20 62 61 69 6B 20  tunya kak, baik 
6B 61 6B 20 69 7A 69 6E-6B 61 6E 20 73 61 79 61  kak izinkan saya
20 6D 65 6D 70 65 72 6B-65 6E 61 6C 6B 61 6E 20   memperkenalkan 
73 65 64 69 6B 69 74 20-6D 65 6E 67 65 6E 61 69  sedikit mengenai
20 70 65 72 75 73 61 61-68 61 61 6E 20 6B 61 6D   perusaahaan kam
69 2C 20 6A 61 64 69 20-49 6E 64 65 65 64 20 61  i, jadi Indeed a
64 61 6C 61 68 20 70 6F-72 74 61 6C 20 70 65 6E  dalah portal pen
63 61 72 69 61 6E 20 70-65 6B 65 72 6A 61 61 6E  carian pekerjaan
20 6F 6E 6C 69 6E 65 20-64 61 6E 20 73 65 64 61   online dan seda
6E 67 20 6D 65 6D 75 6C-61 69 20 6D 65 6D 62 75  ng memulai membu
6B 61 20 64 69 20 49 6E-64 6F 6E 65 73 69 61 20  ka di Indonesia 
64 61 6E 20 6B 61 6D 69-20 73 65 64 61 6E 67 20  dan kami sedang 
6D 65 6E 63 61 72 69 20-62 61 6E 79 61 6B 20 70  mencari banyak p
65 6B 65 72 6A 61 20 73-61 6D 70 69 6E 67 61 6E  ekerja sampingan
20 28 66 72 65 65 6C 61-6E 63 65 29 20 75 6E 74   (freelance) unt
75 6B 20 6D 65 6D 61 6E-66 61 61 74 6B 61 6E 20  uk memanfaatkan 
77 61 6B 74 75 20 6C 75-61 6E 67 00 E0 6E 11 38  waktu luang·àn·8
```

Figure 15 : Evidence of the Perpetrator's Chat

Figure 15 shows the perpetrator's chat explaining and offering freelance work to the victim.

OSForensics was used to analyze the computer's physical memory (RAM) to find the images contained in the conversation between the victim and the perpetrator. The File Name Search feature in the File Searchimg section and the Indexing section was used to find images in the conversation.



File Name	Location	Type	Date modified	Date created	Date accessed
!.jpg	C:\Users\Lenovo\Downloads\MATKUL\Forensik...	JPG File	16/01/2022, 02:32:22.0000...	16/01/2022, 03:00:59.0000...	15/09/2023, 15:02:48.7256...
!.jpg.copy0	C:\Users\Lenovo\Downloads\MATKUL\Forensik...	COPY0 File	16/01/2022, 02:32:22.0000...	16/01/2022, 03:00:59.0000...	15/09/2023, 15:02:48.7409...
!.mp3	C:\Users\Lenovo\Downloads\MATKUL\Forensik...	MP3 File	16/01/2022, 01:32:08.0000...	16/01/2022, 03:00:58.0000...	26/05/2023, 23:59:02.1654...
!.png	C:\Users\Lenovo\Downloads\MATKUL\Forensik...	PNG File	16/01/2022, 02:30:24.0000...	16/01/2022, 03:00:59.0000...	26/05/2023, 23:59:02.1523...
!.png.copy0	C:\Users\Lenovo\Downloads\MATKUL\Forensik...	COPY0 File	16/01/2022, 02:30:16.0000...	16/01/2022, 03:00:59.0000...	15/01/2022, 20:34:06.9601...
#!123	C:\Users\Lenovo\AppData\Local\Packages\Mic...	File folder	24/11/2021, 16:55:08.2035...	24/11/2021, 16:55:02.5068...	15/09/2023, 15:01:35.3897...
#20220526T143907.log	C:\Users\Lenovo\AppData\Roaming\Publish or ...	Text Document	26/05/2022, 21:39:07.2627...	26/05/2022, 21:39:07.2607...	26/05/2022, 21:39:07.2627...
#bts #bangtanboys #...	C:\Users\Lenovo\OneDrive\Pictures\BTS\JK	JPG File	13/10/2021, 16:38:43.7111...	13/10/2021, 16:38:43.4133...	15/09/2023, 15:02:48.7510...
#bts #namjoon #jin #...	C:\Users\Lenovo\OneDrive\Pictures\BTS\Y	JPG File	13/01/2022, 11:07:39.1737...	13/01/2022, 11:07:39.0315...	15/09/2023, 15:02:48.7709...
$$.cdf-ms	C:\Windows\WinSxS\FileMaps	CDF-MS File	29/08/2023, 19:42:09.3262...	07/05/2022, 12:24:51.4827...	15/09/2023, 10:09:04.5111...
$$_addins_2452dffbc...	C:\Windows\WinSxS\FileMaps	CDF-MS File	09/08/2023, 21:22:49.6543...	26/05/2023, 00:48:37.4797...	15/09/2023, 10:09:04.5269...
$$_appcompat_apprai...	C:\Windows\WinSxS\FileMaps	CDF-MS File	09/08/2023, 21:22:49.6543...	07/05/2022, 12:24:53.4829...	15/09/2023, 10:09:04.5269...
$$_appcompat_apprai...	C:\Windows\WinSxS\FileMaps	CDF-MS File	09/08/2023, 21:22:49.6543...	07/05/2022, 12:24:53.4829...	15/09/2023, 10:09:04.5269...
$$_appcompat_backu...	C:\Windows\WinSxS\FileMaps	CDF-MS File	09/08/2023, 21:22:49.6534...	24/08/2023, 00:32:08.9621...	15/09/2023, 10:09:04.5269...
$$_appcompat_progr...	C:\Windows\WinSxS\FileMaps	CDF-MS File	09/08/2023, 21:22:49.6493...	07/05/2022, 12:24:53.4829...	15/09/2023, 10:09:04.5269...
$$_apppatch_114399...	C:\Windows\WinSxS\FileMaps	CDF-MS File	09/08/2023, 21:22:49.6475...	07/05/2022, 12:24:53.4673...	15/09/2023, 10:09:04.5269...
$$_apppatch_apppatc...	C:\Windows\WinSxS\FileMaps	CDF-MS File	07/05/2022, 12:22:32.0826...	07/05/2022, 12:24:53.4829...	15/09/2023, 10:09:04.5269...
$$_apppatch_custom...	C:\Windows\WinSxS\FileMaps	CDF-MS File	09/08/2023, 21:22:49.6493...	07/05/2022, 12:24:53.4673...	15/09/2023, 10:09:04.5427...
$$_apppatch_custom...	C:\Windows\WinSxS\FileMaps	CDF-MS File	09/08/2023, 21:22:49.6493...	07/05/2022, 12:24:53.4673...	15/09/2023, 10:09:04.5427...
$$_apppatch_customs...	C:\Windows\WinSxS\FileMaps	CDF-MS File	09/08/2023, 21:22:49.6493...	07/05/2022, 12:24:53.4673...	15/09/2023, 10:09:04.5269...
$$_apppatch_en-us_0...	C:\Windows\WinSxS\FileMaps	CDF-MS File	07/05/2022, 13:01:25.4339...	07/05/2022, 13:01:29.0119...	15/09/2023, 10:09:04.5427...
$$_apppatch_merges...	C:\Windows\WinSxS\FileMaps	CDF-MS File	12/07/2023, 15:23:32.9826...	07/05/2022, 12:24:53.4673...	15/09/2023, 10:09:04.5427...
$$_appreadiness_b6b...	C:\Windows\WinSxS\FileMaps	CDF-MS File	09/08/2023, 21:22:49.6443...	07/05/2022, 12:24:53.4673...	15/09/2023, 10:09:04.5427...
$$_bcastdvr_fab1ebc...	C:\Windows\WinSxS\FileMaps	CDF-MS File	09/08/2023, 21:22:49.6443...	07/05/2022, 12:24:53.4673...	15/09/2023, 10:09:04.5427...
$$_boot_40104b85a1...	C:\Windows\WinSxS\FileMaps	CDF-MS File	09/08/2023, 21:22:49.6364...	07/05/2022, 12:24:53.4048...	15/09/2023, 10:09:04.5427...

Search completed   Items Searched: 679507   Items Found: 679507

Figure 16 : Drive C Scan Results

Figure 16 is a scan of the C drive. It contains all the files contained on drive C. To speed up the image search, the file extension ".jpg" is used as shown in Figure 4.27.

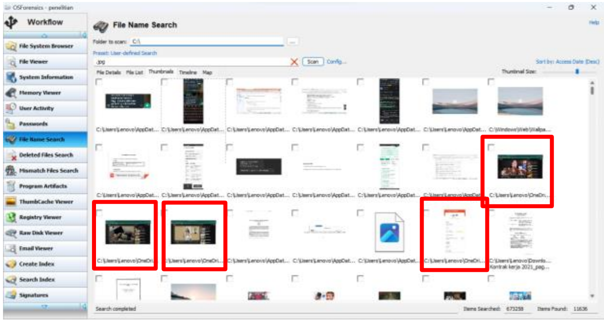
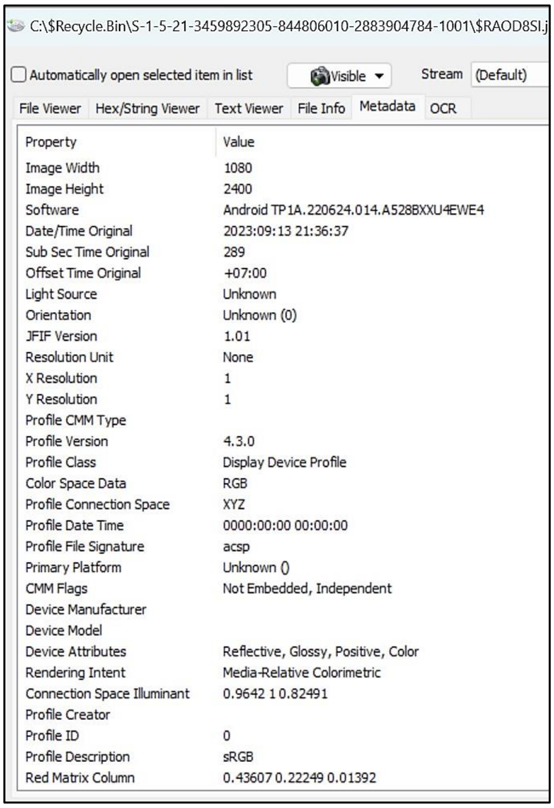


Figure 17 : Image Search Results

Figure 17 is the result of searching for images on drive C. To make it easier to see the image, a thumbnail view is used. From the image search results, evidence of transfers and screenshots of tasks given by the perpetrator to the victim were found.


C:\$Recycle.Bin\S-1-5-21-3459892305-844806010-2883904784-1001\$RAOD8SI.j
Visible
File Viewer
Hex/String Viewer
Text Viewer
File Info
Metadata
OCR

□ Automatically open selected item in list

Stream (Default)

Property	Value
Image Width	1080
Image Height	2400
Software	Android TP1A.220624.014.A528BXXU4EWE4
Date/Time Original	2023:09:13 21:36:37
Sub Sec Time Original	289
Offset Time Original	+07:00
Light Source	Unknown
Orientation	Unknown (0)
JFIF Version	1.01
Resolution Unit	None
X Resolution	1
Y Resolution	1
Profile CMM Type	
Profile Version	4.3.0
Profile Class	Display Device Profile
Color Space Data	RGB
Profile Connection Space	XYZ
Profile Date Time	0000:00:00 00:00:00
Profile File Signature	acsp
Primary Platform	Unknown ()
CMM Flags	Not Embedded, Independent
Device Manufacturer	
Device Model	
Device Attributes	Reflective, Glossy, Positive, Color
Rendering Intent	Media-Relative Colorimetric
Connection Space Illuminant	0.9642 1 0.82491
Profile Creator	
Profile ID	0
Profile Description	sRGB
Red Matrix Column	0.43607 0.22249 0.01392

Figure 18 : Image Metadata

Figure 18 shows one of the metadata of the proof of transfer image sent by the victim to the perpetrator. In this metadata we can see image specifications such as image access time

4.4 Analysis

4.4.1 Browser History Examiner Analysis

From the examination results using the Browser History Examiner, evidence was found showing that the perpetrator had logged in using a phone number and accessed Telegram Web. This evidence was identified based on the time match, where on 06/08/2023 at 13:24, it was seen that the perpetrator performed this action. Thus, it can be concluded that the perpetrator has logged into a Telegram Web account using a phone number to log in.

4.4.2 FTK Imager Analysis

Based on the FTK Imager examination results, several pieces of evidence were found related to the conversation between the victim and the perpetrator, the link sent by the perpetrator, and the Telegram account owned by the perpetrator. Details regarding the evidence found can be seen in Table 2

Table 2 : Evidence Found on FTK Imager

Information	Results	Description
Account	Name: Indeed Phone Number: 6281393186655	Found
Conversation	Hello, I am Staff from Indeed. I want to offer you a part-time job to supplement your income. Are you interested?	Found
Conversation	Okay, what's the job?	Found
Conversation	Subscribe and like our partner's YouTube	Found

	content by sending screenshots as proof. Payment is per 3 tasks, and for payment can choose.	
Conversation	Okay, I understand	Found
Conversation and links	Here is the link for the assignment https://youtu.be/ewL5n4S3WHU	Found
Conversation	I have finished the assignment.	Found
Conversation	Next, we have a special task; the condition is that you must first deposit IDR 50,000 for the new member fee. If you become a member, your income will increase by 50%.	Found
Conversation	Okay, where should I transfer to	Found
Conversation	Seabank 19791779740, include proof of transfer	Found
Conversation	I already transferred	Found
Conversation	okay, well, we'll check first. If it comes in later, we will tell you again. Thank you	Found
Conversation	Okay, I'll wait for it	Found

Table 2 shows the results of using the FTK Imager tool to find evidence that has been deleted by the perpetrator, such as accounts and conversations. In the table are perpetrator accounts, 45 conversations, and one account that was successfully found.

4.4.3 OSForensics Analysis

Based on the examination results using OSForensics, evidence was found in the form of a screenshot of the task given by the perpetrator to the victim. In addition, there was also evidence of transfers made by both the perpetrator and the victim.

4.5 Reporting

This report contains results or digital evidence related to freelance fraud cases on the Telegram web. This evidence was found through forensic tools such as FTK Imager, Browser History Capturer, Browser History Examiner, and OSForensics. This information was taken from the physical evidence of the perpetrator's laptop that had been seized by the police earlier. This laptop was then examined and analyzed to produce digital evidence. Details regarding the digital evidence found can be seen in Table 4.7, which lists the results found through forensic tools such as FTK Imager, Browser History Examiner, and OSForensics with the application of methods from the National Institute Of Justice.

Table 3 : Digital Evidence Findings

Findings	**FTK Imager**	**Browser History Examiner**	**OSForensics**
Login Information	-	✓	-
Account Information	✓	-	-
Conversation	✓	-	-
Text			
Image	-	-	✓

Table 3 lists the digital evidence identified in the Telegram web freelance fraud case, utilizing three different forensic tools. The Browser History Examiner successfully found digital evidence in the form of the phone number used to log in to the Telegram web. This information was found based on the access time on the Telegram web page and form history records that show the use of phone numbers when logging in. FTK Imager identified digital evidence through conversations between the perpetrator and the victim on the Telegram web. Meanwhile, OSForensics Tools found digital evidence in the form of screenshots.

5. CONCLUSIONS

Based on the results of research conducted in this thesis with the title "Forensic Analysis of Web-Based Instant Messenger Applications Using the National Institute of Justice Method," several important conclusions can be drawn, namely the National Institute of Justice (NIJ) method has been proven to be successfully applied in the forensic process on web-based instant messenger applications, especially on the Telegram web, to collect and analyze digital evidence in freelance fraud cases using the five stages in this method, namely preparation, collection, examination, analysis, and reporting. The results show that the Browser History Examiner tool can be used to identify the phone number used by the perpetrator in access to the Telegram web. FTK Imager proved its reliability in retrieving digital evidence through conversations or chats that the perpetrator had previously deleted. This tool successfully identified conversations between the perpetrator and the victim on the Telegram web. The OSForensics tool effectively analyzed images contained in the conversation, such as screenshots and proof of transfer sent by the perpetrator and victim. Through this research, it can be concluded that the application of the National Institute of Justice method and the use of forensic tools, such as Browser History Examiner, FTK Imager, and OSForensics, can reveal and analyze digital evidence in cases of freelance fraud through Telegram web.

6. REFERENCES

[1] G. Maulana Zamroni, R. Umar, and I. Riadi, “Forensic Analysis of Android-based Instant Messenger Applications,” 2016. [Online]. Available: http://ars.ilkom.unsri.ac.id

[2] S. K. Dirjen et al., “SINTA Accredited Rank 2 Comparative Web-based Instant Messenger Vulnerability Using the Association of Chief Police Officers Method," validity period starts, vol. 1, no. 3, pp. 813–819, 2017.

[3] I. Riadi, R. Umar, and M. A. Aziz, “Instant Messenger Service Web Forensics Using the Association of Chief Police Officers (ACPO) Method,” vol. 1, no. 1, pp. 1–10, 2019.

[4] I. G. Ngurah, G. Wicaksanaa, and I. K. G. Suhartanaa, “Forensic Analysis of Desktop-based Telegram Applications using the National Institute of Justice Methods (NIJ),” vol. 8, no. 4, pp. 381–385, 2020.

[5] “The Instant Messenger App with the Most Users in the World 2022 - GoodStats." https://goodstats.id/article/aplikasi-pesan-instan-with-users-most-in-the-world-2022-3tggF (accessed Nov. 30, 2022).

[6] M. S. Chang and C. Y. Chang, “Forensic analysis of LINE

messenger on android," Journal of Computers (Taiwan), vol. 29, no. 1, pp. 11–20, Feb. 2018, doi: 10.3966/199115992018012901002.

[7] "Movie Piracy on Telegram is Rampant, Kominfo is Ready to Block." https://inet.detik.com/law-and-policy/d-5384975/marathon-movie-piracy-on-telegram-kominfo-ready-to-block (accessed Nov. 30, 2022).

[8] I. Riadi, A. Fadlil, and A. Fauzan, "Evidence Gathering and Identification of LINE Messenger on Android Device." [Online]. Available: https://sites.google.com/site/ijcsis/

[9] I. Anshori, K. E. Setya Putri, and U. Ghoni, "Analysis of Digital Evidence of Facebook Messenger Applications on Android Smartphones Using the NIJ Method," IT Journal Research and Development, vol. 5, no. 2, pp. 118–134, 2020, doi: 10.25299/itjrd.2021.vol5(2).4664.

[10] S. Rachmie, "Digital Website," vol. 21, no. 1, pp. 104–127, 2020.

[11] S. Rizki, "Digital Forensic Analysis in revealing Cyber Crimes at the Preliminary Evidentiary Stage Cyber crimes that are growing rapidly require the Government to immediately make countermeasures in terms of laws and regulations," vol. 2, no. November, pp. 780–787, 2018.

[12] Aaron. Philipp, David. Cowen, and C. Davis, "Hacking exposed computer forensics : secrets & solutions," p. 518, 2010.

[13] Casey, Digital Evidence and Computer Crime. 2011. doi: 10.4018/978-1-59904-379-1.ch015.

[14] F. Sulianta, Komputer Forensik. 2008.

[15] I. Riadi, R. Umar, and I. M. Nasrulloh, "Digital Forensic Analysis of Frozen Solid State Drive with National Institute of Justice (NIJ) Method," Elinvo (Electronics, Informatics, and Vocational Education), vol. 3, no. 1, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.

[16] M. L. Ardiansyah, "Let's Know the Advantages and Disadvantages of the Telegram Application!," Carisinyal, 2021.

[17] M. G. Adiwibawa, L. Ariyani, and A. Saputra, ""Utilization of Telegram Bot for Automation of Payroll and Employee Information at PT MCS," Journal of Research and Application of Informatics Students (JRAMI), vol. 2, no. 01, 2021, doi: 10.30998/jrami.v2i01.746.

[18] A. A. Gillespie, Cybercrime: key issues and debates. Taylor and Francis, 2019. doi: 10.4324/9781351010283.

[19] Z. Malihah and A. Alfiasari, "Cyberbullying Behavior in Adolescents and Its Relationship with Self-Control and Parental Communication," Journal of Family and Consumer Sciences," Journal of Family and Consumer Sciences, vol. 11, no. 2, pp. 145–156, 2018, doi: 10.24156/jikk.2018.11.2.145.

[20] T. Rochmadi and Y. Prayudi, "Live Forensics for Anti-Forensics Analysis on Private Portable Web Browser," 2017.

[21] S. M. Cloud, "Google Chrome," Retrieved Oct, 2008, doi: 10.1016/S1754-4548(09)70096-8.

[22] S. Azizah, S. A. Ramadhona, and K. W. Gustitio, ""Digital Evidence Analysis on Telegram Messenger Using the NIST Framework," Repositor Journal, vol. 2, no. 10, pp. 1400–1405, 2020, doi: 10.22219/repositor.v2i10.1066.

[23] J. Panjaitan, A. C. Sitepu, A. Teknik, and D. Serdang, "Performance Analysis of Forensic Acquisition Tools to Create File Imaging in It Forensic Problems," Julyxxxx, vol. x, No.x, no. 2, p. 2021, 2021.

[24] "Browser History Capturer - Free tool to capture web browser history." https://www.foxtonforensics.com/browser-history-capturer/ (accessed Nov. 30, 2022).

[25] "PassMark OSForensics - Digital investigation." https://www.osforensics.com/ (accessed Aug. 01, 2023).