

Forensic Analysis of Online Fraud on Telegram Web using Digital Forensics Workshop Method

Kurnia Agustia Arifin
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT

The development of information technology has facilitated communication, but it has also increased digital crimes such as online fraud. Telegram Web as a popular messaging application has become one of the means of criminal action. This study aims to analyze cases of online fraud through Telegram Web using the Digital Forensics Research Workshop (DFRWS) method. The DFRWS methodology consists of six stages, namely identification, maintenance, collection, examination, analysis, and presentation. In the investigation process, several digital tools such as FTK Imager, Browser History Examiner, and Chrome DevTools were used to obtain digital evidence in the form of conversations, browser history, and image evidence. The results of the study show that the DFRWS method is effective in finding and validating hidden digital evidence, as well as assisting with legal investigations. This study is expected to be a reference in the development of digital crime investigations.

Keywords

Digital Forensics, Telegram Web, Online Fraud, DFRWS, Digital Evidence

1. INTRODUCTION

Telegram is a popular messaging application that uses end-to-end encryption to ensure the security of communications, but on the other hand it is often misused for illegal activities such as fraud, hate speech, and terrorism. This research aims to conduct digital forensic analysis of online fraud cases through the Telegram Web application by applying the Digital Forensics Research Workshop (DFRWS) method which consists of six stages, namely identification, storage, collection, examination, analysis, and presentation of digital evidence, as well as utilizing techniques such as disk imaging, file carving, metadata analysis, and timeline reconstruction to obtain evidence in the form of messages, call logs, media files, and other relevant data [1][2]. The application of the DFRWS method has been proven effective in various previous studies, such as the research of Fahrudin and Muflih (2025) who successfully recovered PGP-encrypted WhatsApp messages in drug cases [8], Sunardi et al. (2021) who extracted hidden steganography files using static forensics [9], Faisal et al. (2023) who uncovered evidence of hate speech in Snack Video with a 100% success rate using Oxygen Forensic [10], Zuhriyanto et al. (2021) who compared the accuracy of Twitter data extraction between MOBILedit and Belkasoft [11], and Wibowo et al. (2024) who proved the effectiveness of DFRWS in finding complete evidence on desktop Discord applications using Magnet Axiom [12]; All of these findings support that DFRWS-based digital forensics approaches are able to make a significant contribution to the investigation and countering of

cybercrime on various digital communication platforms, including Telegram.

2. LITERATURE STUDY

2.1 Digital Forensics

Digital forensics is a branch of forensic science that focuses on identifying, acquiring, analyzing, and presenting digital evidence in order to support the legal process. The term "forensic" comes from the Latin *forensis* which means "with respect to the law", and in the digital context includes activities involving information technology devices such as computers, networks, and storage media. Its main objective is to uncover and prove crimes that leave a digital footprint as valid legal evidence [13][14].

2.2 Forensic Analysis

Digital forensic analysis is a crucial stage in an investigation that aims to evaluate digital artifacts and the behavior of the system or application being analyzed. This process includes the interpretation of test results as well as an understanding of the consequences of the user's actions. In this study, the analysis focused on residual data (remnants) in memory or file systems to trace the activities that have been carried out by users or actors [15][16].

2.3 Digital evidence

Digital evidence is data that can be used to reconstruct events in criminal investigations, such as server logs, instant messages, emails, and file metadata. This evidence is easily modified or deleted, requiring a documentation and validation process that complies with scientific and legal standards. Therefore, the collection of digital evidence must be carried out by maintaining the authenticity of the data so that it can be legally accepted in court [17][18].

2.4 Telegram

Telegram is a cloud-based instant messaging app that offers a wide range of communication features such as private messages, groups, and channels. Telegram is known for its speed, security, and support for sending large files. However, Telegram is also vulnerable to abuse in various cybercrimes due to its high privacy and anonymity features, including in the case of online fraud [19].

2.5 Web Browser

A web browser is a software used to access information on the internet. Modern browsers such as Google Chrome, Mozilla Firefox, and Microsoft Edge allow users to carry out various activities such as information searching, communication, financial transactions, and social interactions. However,

browsers are also becoming a common medium in cyberattacks such as *phishing*, where perpetrators trick victims with fake links to steal personal information [20].

2.6 Online Scams

Online fraud is a form of digital crime that uses the internet to trick individuals or groups for financial gain or theft of personal data. The modes include fake online shopping, fictitious investments, phishing, and social engineering. According to the Rational Choice Theory, perpetrators choose criminal acts because of high reward and low risk, while Routine Activity Theory states that crime occurs when there are motivated perpetrators, vulnerable targets, and lack of supervision [21].

2.7 Forensic Tools

In digital investigations, various software is used to support the process of acquisition and analysis of digital evidence. FTK Imager is used to create forensic images and extract data from the device's memory. Browser History Examiner and Browser History Capture help you browse and record web browsing activity in its original format. Meanwhile, Chrome DevTools allows for live analysis of caches, metadata, and web artifacts, including from platforms such as Telegram Web [22][23][24][25].

2.8 Digital Forensics Workshop (DFRWS)

The Digital Forensics Research Workshop (DFRWS) methodology is a systematic framework for digital forensic investigations. DFRWS consists of six main stages, namely: identification, maintenance, collection, inspection, analysis, and presentation. This approach allows for a well-structured and documented investigative process, and is accountable before the law. With this method, investigators can collect data from various digital sources and compile it into legally and technically valid reports [26][27].

3. RESEARCH METHODE

This study uses the Digital Forensics Research Workshop (DFRWS) approach as the main method in digital forensic investigation. The method consists of six structured stages which include: identification, maintenance, collection, examination, analysis, and presentation. The schematic of the DFRWS method stages can be seen in Figure 1.

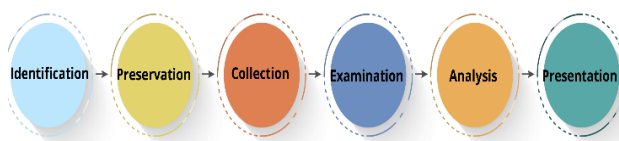


Figure 1: Stages of the DFRWS Methode

Figure 1 illustrates the Digital Forensics Research Workshop (DFRWS) method, which consists of six main stages. The identification stage aims to determine the needs of the investigation and the types of relevant digital evidence, which are divided into two categories: hardware and software. The collection stage involves discovering artifacts, such as conversation evidence using FTK Imager, image evidence using DevTools, and browser history using Browser History Examiner. Next, the examination stage focuses on data exploration to sort and organize information without altering its contents. The analysis stage includes the interpretation of digital artifacts to reveal the chronology of events, such as linking Telegram Web conversations with the interaction

patterns of perpetrators and victims. Finally, the presentation stage prepares a systematic and objective investigation report as the basis for legal considerations.

4. RESULT AND DISCUSSION

This study analyzed cases of online fraud that occurred through the Telegram application using a three-stage approach: pre-incident, incident, and post-incident. This approach refers to the stages of investigation in the Digital Forensics Workshop (DFRWS) method. Each stage is simulatively visualized to illustrate the overall fraud process. The first simulation, the pre-incident stage, can be seen in Figure 2.



Figure 2 : pre-incident stage of an online fraud case

Figure 2 shows the initial stages carried out by the perpetrator in the case of online fraud through the Telegram Web platform. The perpetrator first logged in to Telegram Web using a laptop device. After successfully logging in, the perpetrator began his action by sending random messages to a number of Telegram users. The message contains fraudulent modes in the form of attractive offers, such as selling concert tickets at a price that is more affordable than the market price, in order to attract attention and convince potential victims.

The second stage of this case simulation is the incident stage, as shown in Figure 3.

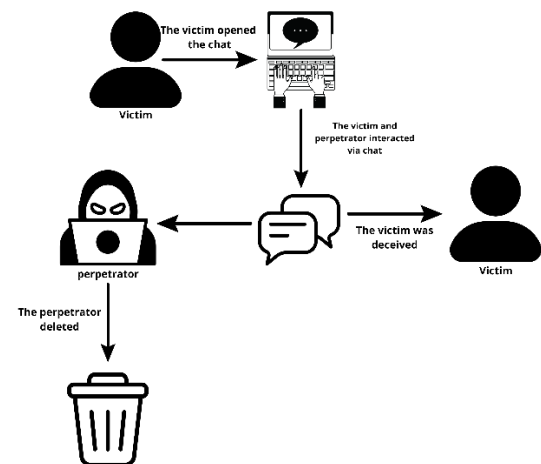


Figure 3 : incident stage of an online fraud case

Figure 3 depicts the stages when the victim receives a message from the perpetrator and feels interested in the offer submitted. The victim then started two-way communication through the Telegram application. After communication was established, the transaction between the perpetrator and the victim was successfully carried out. However, after the transaction, the perpetrator disappeared and deleted all conversations with the victim from the laptop device used, with the aim of eliminating traces and erasing digital evidence.

The final stage of this simulation is the post-incident stage, as described in Figure 4.

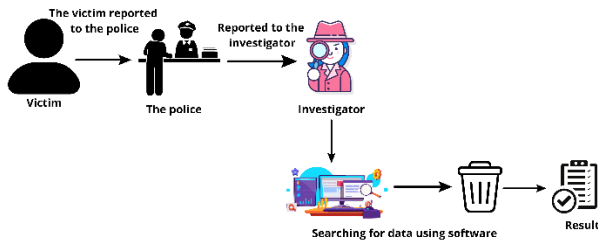


Figure 4 : Post-Incident Stage of an Online Fraud Case

Figure 4 shows the stages of reporting by victims who feel aggrieved by online fraud. The victim submitted evidence of transactions and conversations with the perpetrator. Furthermore, the process of examining and collecting digital evidence was carried out, including the recovery of deleted messages on Telegram. Evidence was obtained using the Digital Forensics Workshop method with the help of forensic devices.

4.1 Identification

The identification stage is the initial phase in the digital forensic process that aims to determine the necessary data, hardware, and software requirements. Forensic needs are divided into two categories, namely hardware and software. The hardware requirements for forensic processes can be seen in Table 1.

Table 1 : Laptop Specifications

Evidence Specifications	
Fire	Asus Vivobook Flip 14
Model Number	M7N0LP03C835309
Processor	AMD RYZEN 7 4700U With Radeon Graphics
RAM	8 GB
Window	Window 11

Table 1 provides a detailed overview of the hardware specifications utilized to optimize performance during the digital forensic identification process. At this particular stage, a comprehensive research scenario was carefully constructed to serve as a test parameter, simulating a situation in which the perpetrator sends messages to the victim. These digital messages are subsequently examined using forensic techniques to verify the authenticity and integrity of the digital evidence, ensuring it meets legal standards before being presented in court as admissible evidence. Beyond functioning merely as a benchmark for testing, this scenario also plays a crucial role in outlining and guiding the sequence of steps necessary throughout the research process. Furthermore, the software tools and platforms employed to support this investigation are systematically listed and explained in Table 2.

Table 2 : List of Software

Software
FTK – Imager
Browser History Capture
Browser History Examiner
DevTools Chrome
Sistem Operasi Window 11
Telegram Web
Chrome

Table 2 presents the results of a comprehensive identification of various software tools utilized throughout the digital forensic process, including during the simulation of pre-designed case scenarios. Each software listed serves a specific and critical function, ranging from the acquisition to the analysis of digital evidence, all of which play a significant role in ensuring the successful uncovering and verification of relevant digital data as part of the investigative process.

4.2 Preservation

The second stage, known as the maintenance stage, primarily aims to ensure the security and authenticity of digital evidence by isolating the involved devices and thoroughly validating data integrity. During this phase, digital evidence is carefully labeled to document the chain of custody, allowing every transfer or handling of the evidence to be traced and verified. This step is crucial to guarantee that no alterations, damage, or manipulations occur throughout the investigation process that could compromise the validity of the evidence. This procedure is visually illustrated in Figure 5.



Figure 5 : Laptop

4.3 Collection

The data collection stage is carried out using digital forensic tools to ensure that the integrity of the data source remains intact and is not altered or damaged. This process is essential, as any modified or unauthentic data cannot be used as valid evidence in investigations or legal proceedings. Therefore, data acquisition must be conducted carefully, following standard procedures, and using forensic software capable of recording hash values to verify that the acquired data is identical to the original source. This stage serves as a fundamental step in ensuring the authenticity and reliability of digital evidence.

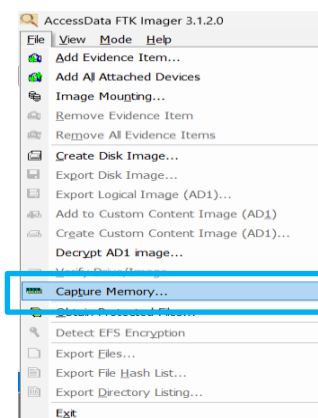


Figure 6 : Capture Memory feature in FTK Imager

Figure 6 shows the *Capture Memory* feature of the FTK Imager software used in the process of collecting data from RAM memory. This feature allows the extraction of data and information that is temporarily stored in the laptop's RAM, including activities when the perpetrator logs in to Telegram Web. The use of FTK Imager at this stage aims to obtain accurate and complete volatile digital evidence.

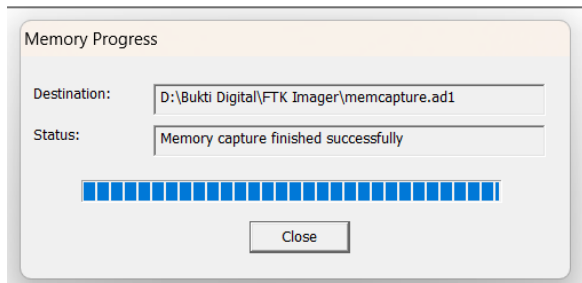


Figure 7 : FTK Imager Interface Performing RAM Capture

Figure 7 shows the *Capture Memory* process carried out by FTK Imager, where the duration of the process depends on the suspect's laptop RAM capacity of 8.23 GB. The extraction results are stored in *.mem format* in the D:\Digital Proof\FTK Imager directory.

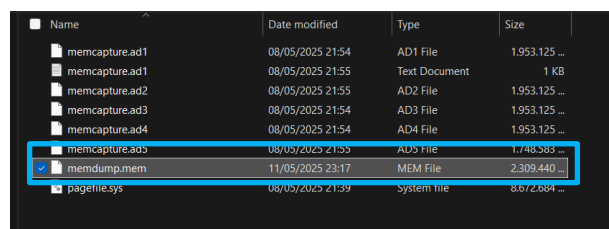


Figure 8 : Capture Results

Figure 8 shows the illustrate the results of the digital evidence examination obtained from RAM memory using the FTK Imager tool. The memory acquisition process produced a captured file that was systematically stored in the directory D:\Digital Proof\FTK Imager under the name *memdump.mem*. The file is approximately 13 GB in size, indicating that it contains the entire active memory content at the time of acquisition. This data can then be further analyzed in the forensic investigation to identify relevant digital traces related to the case being examined.

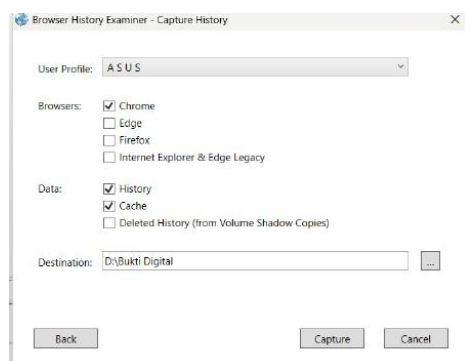


Figure 9 : Browser Interface to Be Captured

Figure 9 shows what the Browser History Examiner looks like when capturing browsing history and cache data from ASUS user profiles in Google Chrome, which is stored in the

D:\Digital Evidence directory as part of digital forensic analysis.

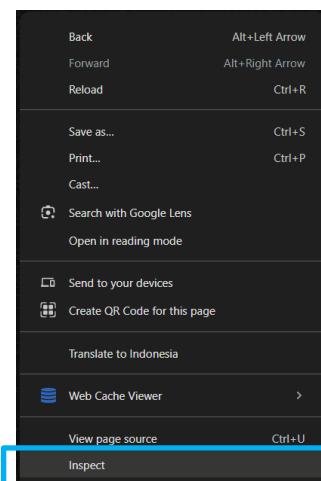


Figure 10 : Opening the Chrome Panel

Figure 10 shows the use of the right-click menu in Google Chrome to access the Inspect or DevTools feature, which investigators use to open the Application tab and analyze the Cache Storage to obtain digital artifacts such as important images or files as evidence.

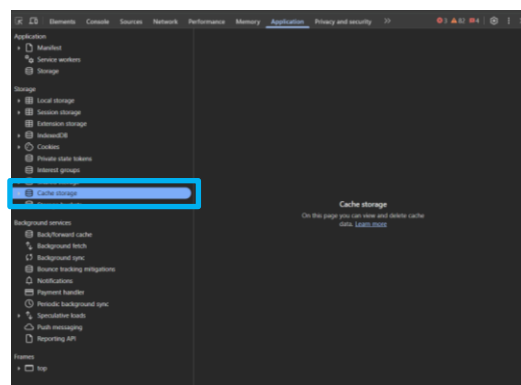


Figure 11 : Application Tab Display

Figure 11 shows the Application tab of Chrome DevTools when the Cache Storage option is selected, which allows users to view and delete cached data stored by websites.

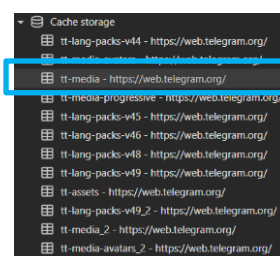


Figure 12 : Cache Storage Display

Figure 12 shows a Cache Storage view on the Application tab in Chrome DevTools that loads cache files from *web.telegram.org* sites, such as *tt-media*, *tt-assets*, and *tt-lang-packs*, which are relevant for client-side transient storage analysis in the context of web forensics.

4.4 Examination

The examination stage is carried out after the collection process, by analyzing the RAM capture data and web browsing history. The analysis was carried out using forensic tools such as FTK Imager, Browser History Examiner, Browser History Capture, and Chrome DevTools. The resulting RAM capture file is in ".mem" format and analyzed using FTK Imager, with the memdump.mem file stored in the *D:\Digital Proof\FTK Imager\memdump.mem* directory.

4.4.1 FTK-Imager

The initial step of data exploration in FTK Imager starts with the Add Evidence Item feature to load a ".mem" formatted RAM file such as memdump.mem stored in *D:\Digital Evidence\FTK Imager*. Once loaded, further analysis and examination of the data can be carried out in Figure 13.

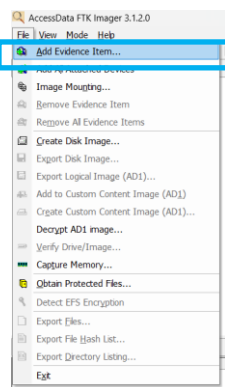


Figure 13 : Evidence Item Feature

Figure 13 shows the *Add Evidence Item* feature on the FTK Imager which is used to load and explore previously captured ".mem" RAM files.

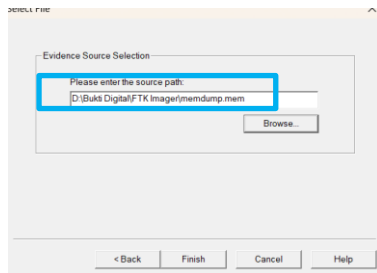


Figure 14 Evidence Source Selection

Figure 14 shows the *Evidence Source Selection* stage, where the user selects the *memdump.mem* file from the *D:\Digital Evidence\FTK Imager* directory for analysis.

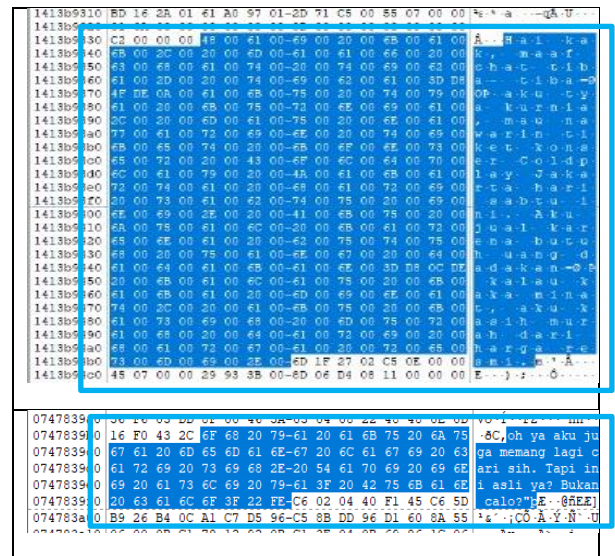


Figure 15 Perpetrator's Chat Offering Tickets

Figure 15 shows the chat when the performer introduces himself and offers Coldplay concert tickets at low prices and official claims.

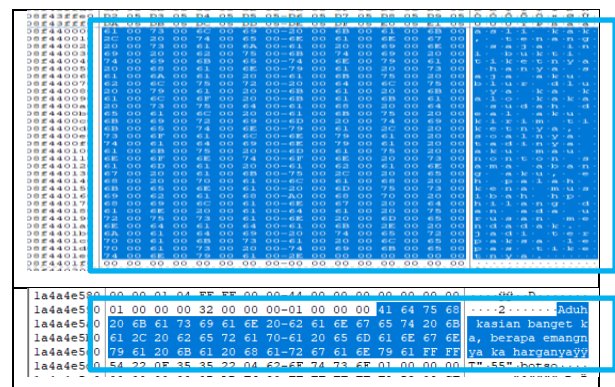


Figure 16 Perpetrator's Chat to the Victim

Figure 16 shows the chat when the perpetrator gives a reason for selling tickets to provoke pity, as well as convincing the victim by showing a deliberately blurred digital ticket. This tactic is used to build trust and make the victim believe that the situation is real and urgent.

4.4.2 Browser History Examiner

Browser History Examiner is used to analyze the search history of a web browser, displaying details such as access dates, URLs, emails, browser types, downloaded images, and pages visited. This tool helps track the login information of the perpetrator when accessing Telegram Web. In addition, it can also identify suspicious activity patterns that indicate potential fraud or manipulation by the perpetrator. The results of this analysis can serve as important digital evidence in investigations, helping to reconstruct the timeline of events and confirm the involvement of the perpetrator.

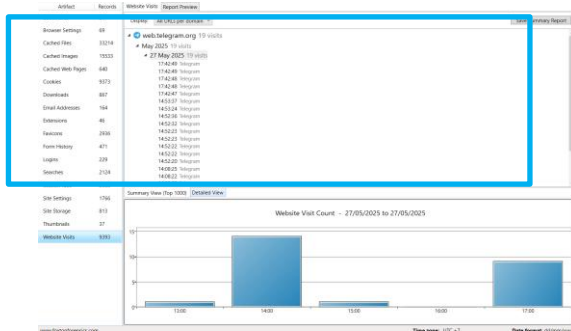


Figure 17 : Extraction Results

Figure 17 displays the extraction results from the *Capture* folder, containing various types of digital artifacts such as bookmarks, cookies, logins, and other browser-related data. One of the key findings in this process is the information related to the perpetrator's phone number, which can be traced through the *Form History*—a feature that records data input by the user into online forms. Additionally, artifacts from *Website Visits* provide further insight by listing the websites that were accessed, thereby strengthening the suspect's digital footprint and expanding the context of the investigation into suspicious online activities.

4.4.3 DevTools Chrome

DevTools Chrome was used in the investigation to directly examine browser activity, including page elements, network traffic, and temporary storage such as cookies, local storage, and session storage. The analysis was performed in real-time without the need for external files. Figure 18 shows the initial steps by pressing F12 or right-clicking and selecting the Inspect menu. This tool is useful for identifying cached data such as media files, login tokens, and other digital traces relevant to the investigation.

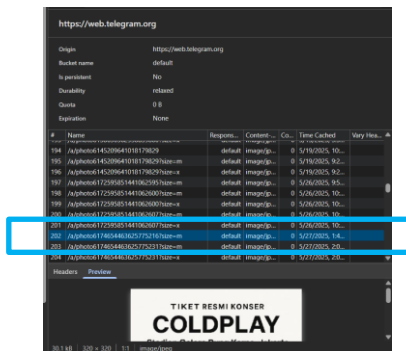


Figure 18 : Media in Cache Storage

Figure 18 shows what the Application tab looks like on Chrome DevTools when checking the Cache Storage of the Telegram Web site. It can be seen that there is an image file dated May 26, 2025 that displays digital evidence in the form of Coldplay concert tickets, which is temporarily stored in the browser's cache. This evidence was obtained even though the messages folder appeared empty, indicating that the perpetrator had deleted the message, but the rest of the data could still be found through the cache.

4.5 Analysis

The analysis stage was carried out to thoroughly evaluate the results obtained using FTK Imager, Browser History Examiner, and Chrome DevTools. The goal was to identify relevant digital

artifacts such as browsing history, form data, and login information related to fraudulent activity. Through this analysis, investigators were able to reconstruct the timeline of events and connect the digital evidence to the perpetrator's actions. In addition, the analysis helped uncover patterns or methods used by the perpetrator, including the platforms utilized, the timing of the activity, and interactions with the victim. Therefore, this stage plays a crucial role in the digital forensic investigation process, as it ensures that all collected evidence holds strong probative value and is legally admissible in court proceedings.

4.5.1 Analysis using FTK Imager

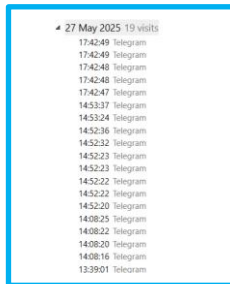
Based on the analysis conducted using FTK Imager, evidence was found in the form of a conversation between the perpetrator and the victim, indicating an attempt at fraud. The conversation contains a series of communications that reveal manipulation and deceit carried out by the perpetrator toward the victim. In the chat, the perpetrator attempted to gain the victim's trust by providing various excuses, such as system disruptions and false promises of payment, in order to delay the victim's realization of the ongoing fraud. This finding serves as a key piece of digital evidence supporting the suspicion of criminal activity. The detailed results of this finding are presented in Table 3.

Table 3 : Conversation

Information	Message	Statement
conversation	Hi sis, sorry to chat suddenly 🙏 I'm a gift, I want to offer tickets to the Coldplay Jakarta concert this Saturday. I sell it because I need impromptu 😊 money if you are interested, I give it cheaply from the official price.	Found
conversation	Hello, oh yes I'm looking for it too. But this is real, huh? Not a scalper?	Found
conversation	It's a lot of money, how much does it cost?	Found
conversation	The original price was 2 million, I sold it for 1,750 just to make it quick. If you're worried I can zoom a or video call to see the physical form of the ticket	Found
conversation	Where are you going to transfer?	Found
conversation	Thank you very much, this is 🙏 the account number: IRB: 0123456789 a.n tya kurnia if you have, I immediately send the full ticket pdf + ID ID I will let you calm down	Found
conversation	Okay, I'll transfer now.	Found
conversation	Yes.	Found
conversation	How about you, you've entered yet	Found
conversation	Sis?	Not Found
conversation	You're a!!	Not Found

4.5.2 Analysis using Browser History Examiner

Based on the results of the analysis with the Browser History Examiner, evidence of Telegram Web access history through the Chrome browser was found on May 27, 2025, which shows the interaction between the perpetrator and the victim can be seen in Figure 19.



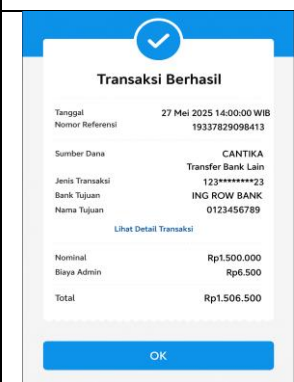
• 27 May 2025 '19 visits
17:42:49 telegram
17:42:49 telegram
17:42:48 telegram
17:42:48 telegram
17:42:47 telegram
14:53:37 telegram
14:53:24 telegram
14:52:36 telegram
14:52:32 telegram
14:52:23 telegram
14:52:23 telegram
14:52:22 telegram
14:52:22 telegram
14:52:20 telegram
14:08:25 telegram
14:08:22 telegram
14:08:20 telegram
14:08:16 telegram
13:39:01 telegram

Figure 19 : Website Visit History

4.5.3 Analysis using Chrome DevTools

Based on the analysis using Chrome DevTools, two image evidences were found through the Network and Application tabs, namely a blurred ticket image and a fake transfer proof. These findings support the indication of fraudulent activity by the perpetrator and can be seen in Table 4.

Table 4 : Image Evidence

	Found
	Found

4.6 Presentation

The final stage of this investigation involves presenting the results and drawing conclusions. FTK Imager successfully uncovered conversations between the perpetrator and the victim on Telegram Web, which served as crucial evidence in the digital analysis process. Browser History Examiner identified the specific time and date of the perpetrator's activity, supporting the reconstruction of the incident timeline. Meanwhile, Chrome DevTools revealed evidence in the form of blurred ticket images and proof of transfer from the victim, indicating an attempt at visual data manipulation by the perpetrator. This study was conducted using a Windows 10-

based laptop, as detailed in Table 5, to ensure compatibility and smooth operation of the digital forensic tools used.

Table 5 : Laptop Specifications

Brand	Asus Vivobook Flip 14
Processor	AMD RYZEN 7 4700U With Radeon Graphics
Graphics	AMD Radeon™ Graphics
Memory	8 GB
Hard disk	477 GB SSD
Monitor	14" FHD (1920×1080) IPS 250nits Anti-glare, 45% NTSC.

The software analyzed is Chrome with a focus on activity on Telegram Web. The examination was carried out according to procedures using several forensic tools. The results of the analysis display information related to the suspect's activities on Telegram Web, as shown in Table 6.

Table 6 : Details of Tool Results

No	Digital evidence	Forensic Software		
		FTK Imager	Story Examiner	DevTools Chrome
1	Photograph	0	0	2
2	Conversation	18	0	0
3	Deleted messages	18	0	0
4	History Browser Chrome	0	1	0

Table 6 summarizes the findings from Telegram Web via Chrome, where FTK Imager uncovers deleted conversations, Story Examiner and Story Capture show access history, as well as Chrome DevTools finds images of concert tickets and evidence of victim transfers.

5. CONCLUSIONS

Based on the results of the study, the collection and analysis of digital evidence in online fraud cases through Telegram Web can be effectively carried out using the Digital Forensic Research Workshop (DFRWS) method, which consists of six main stages from identification to presentation. FTK Imager and Chrome DevTools are capable of uncovering deleted conversations, retrieving visual evidence, and constructing event timelines. In the future, this research can be further developed through the use of more diverse datasets, AI integration, the application of cloud and mobile forensics, and digital evidence visualization to accelerate investigations and enhance law enforcement effectiveness.

6. REFERENCES

- [1] S. Azizah, S. A. Ramadhona, and K. W. Gustitio, "Analisis Bukti Digital pada Telegram Messenger Menggunakan Framework NIST," *REPOSITOR*, vol. 2, no. 10, pp. 1400–1405, 2020.
- [2] J. Triyanto, S. Sunardi, and I. Riadi, "Analisis Investigasi Cyber Espionage Pada Facebook Menggunakan Digital Forensics Research Workshop (DFRWS)," *Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto)*, vol. 23, no. 1, 2022, doi: 10.30595/techno.v23i1.9064.
- [3] N. Citra Dewi, T. Sutabri, and F. Putrawansyah, "Analisis Penyadapan Pada Telegram Dengan Network Forensic,"

- JIKO (Jurnal Informatika dan Komputer), vol. 7, no. 2, p. 183, Sep. 2023, doi: 10.26798/jiko.v7i2.789.
- [4] I. Riadi, T. Ruslan, A. Dahlan, J. Soepomo, Umbulharjo, and K. Yogyakarta, "Forensik Multimedia Berbasis Mobile Menggunakan Metode National Institute Of Justice."
- [5] M. S. Asyaky, N. Widiyasono, and R. Gunawan, "Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android," *Jurnal & Penelitian Teknik Informatika*, vol. 3, no. 1, 2018.
- [6] A. Yudhana, I. Riadi, I. Zuhriyanto, and A. Dahlan, "Analisis Live Forensics Aplikasi Media Sosial Pada Browser Menggunakan Metode Digital Forensics Research Workshop (DFRWS)," vol. 20, no. 2, pp. 125–130, 2019.
- [7] A. Yudhana, Imam Riadi, and Budi Putra, "Digital Forensic on Secure Digital High Capacity using DFRWS Method," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 6, no. 6, pp. 1021–1027, Dec. 2022, doi: 10.29207/resti.v6i6.4615.
- [8] A. Fahrudin, G. Z. Muflih, and T. Informatika, "Analisis Forensik Digital Pada Pesan Whatsapp Yang Terenkripsi Dengan Pretty Good Privacy (PGP) Menggunakan Framework DFRWS," vol. 9, no. 1, pp. 780–787, 2025.
- [9] S. Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti, I. Riadi, and M. Hajar Akbar, "Terakreditasi SINTA Peringkat 2 Penerapan Metode Static Forensics untuk Ekstraksi File Steganografi pada Bukti Digital Menggunakan Framework DFRWS," masa berlaku mulai, vol. 1, no. 3, pp. 576–583, 2017.
- [10] Elsyah indah Fitriah, "Penerapan Digital Forensics Research Workshop Dalam Akuisisi Evidence Forensik Snack Video," *Jurnal Komputer Teknologi Informasi dan Sistem Informasi (JUKTISI)*, vol. 2, no. 2, pp. 390–399, 2023, doi: 10.62712/juktisi.v2i2.108.
- [11] S. K. Dirjen et al., "Terakreditasi SINTA Peringkat 2 Analisis Perbandingan Tools Forensic pada Aplikasi Twitter Menggunakan Metode Digital Forensics Research Workshop," masa berlaku mulai, vol. 1, no. 3, pp. 829–836, 2017.
- [12] M. Wibowo, M. R. Firmansyah, and ..., "Analisis Bukti Digital Pada Aplikasi Discord Desktop Dengan Menggunakan Framework Dfrws," *Jurnal Teknologi ...*, vol. 15, no. 1, pp. 98–111, 2024.
- [13] I. Gunawan, O. Gregorius Grasia, and P. Studi Informatika, "Analisis Digital Forensic Aplikasi Pelacak Nomor Handphone Android Pihak Ketiga Menggunakan Metode Statis Dan Dinamis Digital Forensic Analysis Of Third Party Android Cellphone Number Tracker Applications Using Static And Dynamic Methods," *Seminar Nasional Hasil Penelitian & Pengabdian Masyarakat Bidang Ilmu Kompute*, vol. 2, p. 97, 2023.
- [14] L. Flueratoru, E. S. Lohan, and D. Niculescu, "Challenges in platform-independent UWB ranging and localization systems," *WiNTECH 2022 - Proceedings of the 2022 16th ACM Workshop on Wireless Network Testbeds, Experimental evaluation and CHaracterization, Part of MobiCom 2022*, pp. 9–15, 2022, doi: 10.1145/3556564.3558238.
- [15] Ramansyah, "Investigasi Bukti Digital pada Platform Cloud Gaming Menggunakan Framework FRED Studi Kasus pada Skygrid Cloud Gaming Services," pp. 1–66, 2021.
- [16] F. O. F. Science and K. Vincent, "Department Of Computing And Informatics Forensic Analysis Of Evernote Data Remnants On Windows 10," vol. 10, no. November, 2022.
- [17] Imam Riadi, Abdul Fadlil, and Muhammad Immawan Aulia, "Investigasi Bukti Digital Optical Drive Menggunakan Metode National Institute of Standard and Technology (NIST)," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 4, no. 5, pp. 820–828, 2020, doi: 10.29207/resti.v4i5.2224.
- [18] N. Maharani, A. Lamminar, N. Christiansen, and A. R. Rafidah, "Media Hukum Indonesia (MHI) Validitas Bukti Digital dan Legalitas Penangkapan Pada Kasus Peretasan Akun Media Sosial Rasio Patra Media Hukum Indonesia (MHI)," vol. 2, no. 3, pp. 75–81, 2024.
- [19] S. Adira Kania and D. Endrawati Subroto, "Analisis Penggunaan Telegram dan Youtube Untuk Meningkatkan Literasi Digital Mahasiswa Universitas Bina Bangsa," *Journal Of International Multidisciplinary Research*, pp. 186–192, 2023.
- [20] R. Inggis and H. P. Alam, "Analisis Forensik Web Browser," *Jurnal Sistem Informasi dan Teknik Komputer*, vol. 8, no. 1, pp. 215–220, 2023.
- [21] A. Anjani Nurdin et al., "Media Hukum Indonesia (MHI) Analisis Penipuan Online Melalui Media Sosial Dalam Perspektif Kriminologi," vol. 2, no. 2, p. 74, doi: 10.5281/zenodo.11183088.
- [22] Mega Rosita, "Analisis Komparatif Performa Ftk Imager dan Autopsy dalam Forensik Digital pada Flashdisk," *Info Kripto*, vol. 17, no. 3, 2023, doi: 10.56706/ik.v17i3.83.
- [23] H. Adamu, A. Ahmad Adamu, A. Adamu Ahmad, A. Hassan, and ad Barau Gambasha, "IJRSI [Volume VIII, Issue V," 2021. [Online]. Available: www.rsisinternational.org
- [24] L. Chandra Pakaya, U. Ahmad Dahlan, and I. Riadi, "Forensic Analysis of Web-based Instant Messenger Applications using National Institute of Justice Method," 2023. [Online]. Available: www.detiknet.com
- [25] J. M. Moreno, N. Vallina-Rodriguez, and J. Tapiador, "Chrowned by an Extension: Abusing the Chrome DevTools Protocol through the Debugger API," May 2023, [Online]. Available: <http://arxiv.org/abs/2305.11506>
- [26] L. Jupriadi Fakhri, I. Riadi, and A. Yudhana, "Forensic Tools Comparison on File Carving using Digital Forensics Research Workshop Framework," *Scientific Journal of Informatics*, vol. 10, no. 4, pp. 571–582, 2023, doi: 10.15294/sji.v10i4.46901.
- [27] R. M. Genggam et al., "Analisis Bukti Digital Forensik pada Aplikasi Threads Menggunakan Metode Digital Forensic Research Workshop," *Afrizal Ajuj Mudzakkar \ Afrizal Ajuj Mudzakkar*, vol. 22, no. 2, pp. 1–10, 2024.