Browser Forensic of Extortion Case on WhatsApp Web using National Institute of Justice Method

Cindy Amelia
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
WhatsApp is a messaging application for smartphones that can be used across platforms including Apple iOS, Android, Windows Phone, etc. Popularity WhatsApp’s among the public can be misused for negative purposes for the development of society itself. One example of a case that often occurs in the community is extortion through the application WhatsApp. This study will carry out a scenario of a crime of extortion that occurs using WhatsApp Web, WhatsApp runs on the Chrome Browser, this research uses the NIJ stage. The stages of the forensics National Institute of Justice (NIJ) are preparation, collection, examination, analysis, and reporting. This research uses a laptop with a condition that is connected to the internet and accesses WhatsApp via the Chrome browser. The process of collecting digital evidence through forensic tools, namely Belkasoft RAM Capturer, FTK Imager, Browser History Capturer, and Browser History Examiner. This research produces digital evidence, namely information on profile photos of perpetrators and victims, when accessing WhatsApp Web, WhatsApp Weblinks accessed via Chrome, as well as evidence of extortion chats that have been deleted by the perpetrators. The percentage of results obtained from the results of imaging data analysis using the FTK Imager tool is 50% in the form of a WhatsApp Web link and chat from the perpetrator to the victim, while the results from the Browser History Examiner are 50% in the form of a cache of the photo perpetrator, as well as the access time WhatsApp. This research uses the stages of the National Institute of Justice (NIJ), it is hoped that future research can use other stages. This research uses OS Windows 10, so it is hoped that for further research it can use OS Linux or macOS.

Keywords
Forensics, Chrome, WhatsApp Web, Extortion, NIJ

1. INTRODUCTION
The rapid development of instant messaging and social media application technology has facilitated people in living their daily lives, current instant messaging applications such as WhatsApp, Line, SMS, messenger, is not only used to share the news with family or friends but can be a place to earn a living. The growth of social media and instant messaging applications has facilitated many serious crimes.[1] These irresponsible individuals continue to change their strategy to utilize social media services and instant messaging applications to fulfill their own interests without thinking about the impact on others. WhatsApp is a messaging application for smartphones that can be used across platform.[2] WhatsApp uses internet data packages to send instant messages, by using WhatsApp one can have chatted online, share files, videos, and photos as well as other interesting features.[3] Popularity WhatsApp’s among the public can be misused for negative purposes for the development of society itself. One example of a case that often occurs in the community is extortion through the application WhatsApp.

1.1 Study Literature
1.1.1 Previous Study
The first previous research was entitled "Analysis of Forensic Investigations WhatsApp Messenger Smartphone Against WhatsApp Based Web-". This research shows that one can get complete access to all information on WhatsApp, be it WhatsApp Smartphone or WhatsApp Web[4]. Most chat applications follow the same pattern of synchronizing messages, contacts, and user data when syncing and updating conversation data periodically.[5] The approach taken gives a general outline for all similar applications that run on platforms Android and Windows such as Telegram and the like. This research can be useful for Mobile Forensic Analysis and Investigation on Android smartphones and multiple applications web-based browsers.[6]

A previous research both entitled "Analysis of Digital Evidence WhatsApp on Android Smartphone Using Methods". Live Forensic From the results of the identification carried out by analyzing the evidence on the Android Smartphone, it can be concluded that the acquisition, processes imaging and analysis run smoothly using the mobile edit application version 9.0.[7]

The third previous research entitled "Identification of WhatsApp Digital Evidence on Proprietary Operating Systems Using Live Forensic". This research states that live forensic techniques can be applied to the process of retrieving digital evidence from the desktop-based WhatsApp IM application on the Windows 8 operating system using the forensic tools FTK Imager. Digital evidence is obtained in the form of texts of WhatsApp conversations that occurred between the suspect and the victim which can be used as digital evidence related to cases of online shop fraud that occurred.[8]

The fourth previous research entitled "Live Forensic Analysis for Comparison of Instant Messenger Applications on the Windows 10 Operating System".[9] This research analyzes IM applications, namely Line Messenger, Facebook Messenger, and Telegram Messenger and obtains the results that the application of live forensic techniques to obtain digital evidence of activities using IM applications requires different tools and techniques, techniques and tools for live forensics itself also cannot be used on a long time, because if the RAM dies, dumping and analysis of evidence cannot be carried out.[10]

The fifth previous research entitled "Acquisition of Digital
Evidence on Android-Based Instagram Messenger Using the National Institute of Justice (NIJ) Method. The research was conducted to obtain digital evidence from the two smartphones used in cyberbullying cases. The data acquisition process uses the NIJ method which recommends several stages such as preparation, collection, examination, analysis, and reporting.[11] The acquisition process was carried out using the Oxygen Forensic application so as to get the desired results, namely digital evidence in the form of images/photos and conversations from social media Instagram installed on the smartphone. The process of acquiring digital evidence that was successfully obtained on Instagram on a smartphone in Root condition obtained the expected data in the form of photos and conversations while for smartphones that were not in Root condition the expected digital evidence was not obtained.[12]

1.1.2 Digital Forensics
Forensics is one of the branches of science used for the investigation and discovery of digital device content, the term digital forensics was originally synonymous with computer forensics, but has now been expanded to investigate all devices that can store digital data. Digital forensics is a discipline derived from computer security that deals with the finding of digital evidence after an event have occurred. Digital forensics activity itself is a process of identifying, maintaining, analyzing, and using digital evidence according to applicable law.[13]

1.1.3 Live Forensics
Basically live forensics has similarities with traditional forensic techniques in terms of the methods used, namely identification, storage, analysis, and presentation, only live forensics is a response to the shortcomings of traditional forensic techniques which cannot get information from data and information that only exists, when the system is running, for example, activities memory, network processes, swap files, running system processes, and information from files system.[14]

1.1.4 Computer Forensics
Forensics is the process of obtaining and analyzing digital information for use as evidence in civil, criminal, or administrative cases. Computer forensics is also often referred to as digital forensics, information technology forensics, or data forensics which is an investigative process in which researchers identify, maintain, analyze digital evidence consisting of various types.[15]

1.1.5 Digital Evidence
Evidence is information stored or transmitted inform a binary that can be used in court. Digital evidence is generally related to digital crimes such as crimes that use social media as a place to commit crimes so that digital evidence can be used to help prosecute all types of digital crimes.[16] Digital evidence is so susceptible to alteration that it can affect its authenticity if not handled properly. Any kind of alteration that contains digital evidence will lead to wrong conclusions, or the evidence will be unusable.[17]

1.1.6 WhatsApp Web
WhatsApp Web in principle functions to open an account WhatsApp via a computer device. This feature in the early period is easier to use over the web. The developer provides the barcode that needs to be scanned through the application WhatsApp mobile.[18] Scanning will directly open the application WhatsApp according to the working account on the smartphone used for scanning. Conversations contained in the application WhatsApp on smartphones will also be displayed on the version web. Synchronization will be done automatically if there is a change in one of the active applications.[19]

1.1.7 Cybercrime
In conducting investigations and analysis of a criminal case, both cybercrimeand conventional, an investigator must be able to position himself as a criminal (criminologist) in order to help facilitate investigation and case solving.[20] Because a criminologist of course already understands all kinds of crimes that are often committed by criminals which include social phenomena and actions that violate the law and the norms of society that apply.[21]

1.1.8 Chrome Browser
Google Chrome is a browser released by Google, the world's largest and leading search engine company. Google Chrome is also designed to run as fast as possible.[22] Chrome was first released by Google on September 2, 2008 when it was only for Microsoft Windows because it was still in beta status. Then on December 11, 2008, Google Chrome was released for all types of operating systems because it already has a stable version. And as of January 2012, Google Chrome is estimated to have reached 25-28% of all global browser users.[23]

1.1.9 National Institute of Justice (NIJ)
National Institute of Justice (NIJ) is the research, development, and evaluation agency of the United States Department of Justice. [24]

Figure 1: Stages of NIJ Method

- Preparation
- Collection
- Examination
- Analysis
- Reporting

a. Preparation, this stage is carried out by preparing the tools and materials needed to complete tasks during the investigation.
b. Collection, at this stage, activities are carried out to find data and information that can support the investigation process, as well as collect them and make copies of data obtained.
c. Examination, this stage is carried out searching for information data from data that has been collected in the previous stage which can be used as evidence. At this stage, the process of making digital evidence and document contents from the data obtained is seen as.
d. Analysis, this stage the activity of analyzing digital evidence from data that has been filtered in the previous stage to determine the significance and proof of.
e. Reporting, this stage is information presentation obtained from the stage Analysis.

2. METHODOLOGY

2.1 Research Scenario
Several steps were taken to find data that could potentially become evidence, namely preparation, collection, and examination. Volatile data was obtained from the live forensic
method in the form of conversational texts and delivery times, as well as usernames and passwords as additional data. The chrome browser will get information in the form of a history of web visits, access times, and cache images of images sent by perpetrators. In the analysis of this research, it aims to create case scenarios for research regarding the search for evidence of crimes cyber that occurred on WhatsApp. Web running on browser Google Chrome. Figure 2 describes the perpetrator accessing WhatsApp Web through the Chrome browser that has been installed on the laptop. The perpetrator sent a message to the victim through his WhatsApp account.

![Flow of the Case Scenario on WhatsApp Web](image)

In Table 1 are the tools and materials that will be used in analyzing and acquiring data from the evidence that has been found.

### Table 1. Tools and Materials

| No | Tools and Materials | Description |
|----|---------------------|-------------|
| 1  | Laptop              | Acer Travelmate P645-S |
| 2  | Google Chrome ver 89.0.4389.114 | Browser |
| 3  | RAM Capturer 64-bit version | RAM acquisition tools |

2.2 Collection

At this stage, the evidence is secured with the aim of protecting the authenticity of the evidence.

### Table 2. Physical Evidence Found

| No | Name of Evidence | Figure | Description |
|----|------------------|--------|-------------|
| 1  | Laptop           | ![Laptop](image) | Perpetrator's laptop was found to be turned on and connected to the Internet |
| 2  | Charger          | ![Charger](image) | Charging cable used by the perpetrator |

In Table 2 there are photos of evidence that have been collected by the police and then submitted to investigators. The evidence obtained is electronic evidence in the form of a laptop using the Windows operating system and in it there is a Google Chrome browser which is a communication tool used by perpetrators to commit cybercrime.

2.2.2 Examination

At the RAM data acquisition stage using forensic tools Belkasoft Live RAM Capturer, these tools are used for the acquisition of data stored in RAM electronic evidence found. The acquisition takes time, this time depends on the amount of RAM memory on the perpetrator’s laptop.

![Belkasoft Live RAM Capturer](image)

In Table 2 there are photos of evidence that have been collected by the police and then submitted to investigators. The evidence obtained is electronic evidence in the form of a laptop using the Windows operating system and in it there is a Google Chrome browser which is a communication tool used by perpetrators to commit cybercrime.

![Belkasoft Live RAM Capturer Acquired Successfully](image)
Figure 3 is the display of Belkasoft Live RAM Capturer on the initial screen. The column ‘Select output folder path’ is a column to write down the folder used to store the acquisition file. The RAM capture results are stored on the C:\Users\cindy amelia\Downloads\x64 drive with a file size of 9712 MB. After the volatile data in RAM has been successfully acquired, imaging is carried out to maintain data integrity and stored in other media storage and inspections are carried out.

Figure 4. the Hashing Results of RAM

Figure 4 shows the hash value of the data imaging results that have been carried out, it can be seen that the hash value on MD5 and SHA1 of the verified imaging file matches or is the same as the hash value on MD5 and SHA1 of the original file. This means if the hash value of the imaging file and the original file shows the same, then the imaging process is perfect and there are no changes to the file.

Figure 5. Display of Browser History Capturer

In figure 5 shows the browser history capturer when successfully capturing data from the chrome browser, the data captured by the capturer is stored on drive E:\Lectures\Semester 8\Thesis\RAM.

Figure 6. Capture Results File of Browser Chrome

Figure 6 shows the capturer files from the Browser History Capturer tools have been saved in a folder called Capture.

2.2.4 Analysis

The analysis stage is the process of searching for information in the form of digital evidence that has been data acquisition from RAM. The information sought is evidence of the perpetrator's chat threatening the victim which has been deleted by the perpetrator. This analysis uses forensic tools, namely Belkasoft RAM Capturer, FTK Imager, Browser History Capturer, and Browser History Examiner.

2.2.4.1 Browser History Examiner

Tools Browser History Examiner serves to check the capture results that have been done previously using the Browser History Capturer tool. At this stage, the data to be used is the data contained in the Capturer folder. At this stage will obtain information on the Chrome browser in the form of Browser Settings, Cache, Cookies, Bookmarks, History Website Visited, and others.

Figure 7. Result Data History Chrome

Figure 7 shows the historical data contained in the Capture folder, based on the history data that was successfully obtained, it can be seen that Whatsapp Web was accessed on October 3, 2021, at 16:00.

Figure 8. Activity Browser Access WhatsApp Web

In Figure 8 it can be seen that https://web.whatsapp.com/ was accessed on October 3, 2021, at 16:35:22 using the Chrome browser.
Figure 9. Image Cached of perpetrator's profile photo

Figure 9 shows the cache of the perpetrator profile photo circled by a red box.

Figure 10. Image Cached of victim’s profile photo

Figure 10 shows the cache of the victim profile photo circled by a red box.

2.2.4.2 Analysis With FTK Imager

FTK Imager is an Access Data Forensic ToolKit Imager which is one of the tools used in the world of digital forensics to perform data acquisition systems developed by AccessData companies. Where the acquisition system itself is a system that functions to retrieve, collect and prepare data, to process it to produce the desired data.

Figure 11. First Results for FTK Imager

In Figure 11 showing the findings with the keyword Whatsapp, it is seen that the Whatsapp site is accessed via https://web.whatsapp.com/. 

Figure 12. Second Results for FTK Imager

In Figure 12 it can be seen that in the first chat sent by the perpetrator to the victim, the perpetrator sent a blackmail message to the victim.

Figure 13. Third Results for FTK Imager

In Figure 13 you can see evidence of the second chat sent by the victim to the perpetrator, the victim asks the perpetrator's intention to threaten the victim.

Figure 14. Fourth Results for FTK Imager

In Figure 14 there is evidence of the chat of the three perpetrators to the victim, the perpetrator still threatens to spread photos of the victim's parents if the money he asks for is not given by the victim.

Figure 15. Fifth Results for FTK Imager

Figure 15 shows evidence of the chat of the four perpetrators to the victim.
2.2.5 Reporting
The reporting stage is the last stage of the stage National Institute of Justice (NIJ). At this stage, the investigator will make a document or record of the results of the analysis of the evidence that has been carried out in detail.

2.2.6 Results
Results will discuss the findings of the RAM data that has been acquired using several forensic tools, namely Belkasoft RAM Capturer, FTK Imager, Browser History Capture, and Browser History Examiner.

Table 3. Results Analysis On WhatsApp Web

| No | Information Data             | Forensic Tools                   |
|----|-------------------------------|----------------------------------|
|    |                               | FTK Imager | Browser History Examiner |
| 1  | WhatsApp Weblink              | √          | -                      |
| 2  | The perpetrator's chat with the victim | √          | -                      |
| 3  | Cache Photo Perpetrator       | -          | √                      |
| 4  | Access time                   | -          | √                      |

Table 3 displays the results found in analyzing WhatsApp Web used on the browser Chrome using tools forensic. As seen in the results from the FTK Imager, evidence was found in the form of a WhatsApp Weblink accessed by the perpetrator, as well as the perpetrator's chat with the victim. The Browser History Examiner tool displays the WhatsApp Weblink accessed via Chrome, the cache perpetrator's photo, and the time of the web access.

Table 4. The Findings of Evidence

Table 4 shows that the evidence found during the forensic process has similarities with the evidence brought by the victim as report evidence. The evidence found in RAM is the contents of the conversation between the perpetrator and the victim as well as the cached image from the browser. The evidence found from the Chrome browser is the history of visits to the Chrome browser, the time spent accessing Whatsapp Web on the Chrome browser, cached images of the perpetrator and victim, and evidence of conversations between the perpetrator and the victim.
3. CONCLUSION
In this research, the main focus is to find and collect evidence from the laptop used by the perpetrator in committing a crime to the victim. Chat that has been deleted by the perpetrator on WhatsApp which is accessed using a browser Chrome can be restored by retrieving volatile data on laptop RAM using tools Belkasoft RAM Capturer, then the data is Imaging using FTK Imager. As well as WhatsApp access history data on the Chrome browser, cached profile photos of perpetrators, and cached profile photos of victims using the Browser History Capturertools and Browser History Examiner. The percentage of results obtained from the results of imaging data analysis using the FTK Imager tool is 50% in the form of a WhatsApp Web link and chat from the perpetrator to the victim, while the results from the Browser History Examiner are 50% in the form of a cache of the photo perpetrator, a

4. REFERENCES
[1] N. Budhisantosa, “Analisis forensik komputer pada timestamps sistem berkas ntfs,” Forum Ilm. Fak. Ilmu Komput. Univ. Esa Unggul, vol. 13, 2016.
[2] I. Riadi, S. Sunardi, and S. Sahriruddin, “Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ),” J. Rekayasa Teknol. Inf., vol. 3, no. 1, p. 87, 2019.
[3] I. Riadi, R. Umar, and I. M. Nasrullah, “Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (NIJ),” Eleino (Electronics, Informatics, Vocat. Educ.), vol. 3, no. 1, pp. 70–82, 2018.
[4] I. Riadi, S. Sunardi, and M. E. Rauli, “Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics,” J. Tek. Elektro, vol. 10, no. 1, pp. 18–22, 2018.
[5] D. S. Yudhistira, “Metode Live Forensics Untuk Analisis Random Access Memory Pada Perangkat Laptop,” 2018.
[6] B. Sugiantoro et al., “Penerapan Framework Harmonised Digital Forensic Investigation Process (Hdfp) Untuk Mendapatkan Artifak the Implementation of Framework Harmonised Digital Forensic Investigation Process (Hdfip) To Get Artifacts Digital Evidence,” CyberSecurity dan Forensik Digit., vol. 1, no. 2, pp. 67–74, 2018.
[7] R. Umar, A. Yudhana, and M. Nur Faiz, “Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary,” Pros. Konf. Nas. Ke-4 Asos. Progr. Pascasarj. Perguru. Tinggi Muhamadiyah, pp. 207–211, 2016.
[8] T. Rochmadi, “Live Forensik Untuk Analisa Anti Forensik Pada Web Browser Studi Kasus Browserz,” Indones. J. Bus. Intell., vol. 1, no. 1, p. 32, 2019.
[9] D. S. I. Krisnadi, “Citra Forensik Dari Barang Bukti Elektronik Dengan Metode Physical Menggunakan Acquisition Tools Tableau Imager Dan Ftk Imager,” p. 16, 2020.
[10] T. Rochmadi, “Deteksi Bukti Digital Pada Adrive Cloud Storage Menggunakan Digital Evidence Detection in Adrive Cloud Storage Using Live,” CyberSecurity dan Forensik Digit., vol. 2, no. 2, pp. 21–24, 2019.
[11] E. C. Zatnika, N. Widiyasono, and A. I. Gufroni, “Teknik Live Forensics Dalam Investigasi Malware Pada Memori Komputer Dengan Volatility Framework Versi Windows,” Academia.Edu.
[12] I. Zuhriyanto, A. Yudhana, and I. Riadi, “Perancangan Digital Forensik pada Aplikasi Twitter Menggunakan Metode Live Forensics,” Semin. Nas. Inforn. 2008 (seminasIF 2008), vol. 2018, no. November, pp. 86–91, 2018.
[13] A. - Ahmadi, “Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ),” J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf., vol. 4, no. 1, p. 8, 2018.
[14] N. Anwar and I. Riadi, “Analisis Investigasi Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbasis Web,” J. Ilm. Tek. Elektro Komput. dan Inform., vol. 3, no. 1, p. 1, 2017.
[15] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, “1490-Artikel Text-2859-1-10-20190413,” Akuisisi Bukti Digital, Pada Instagram Messenger Berbas. Android Menggunakan Metod. Natl. Inst. Justice, vol. 4, pp. 219–227, 2018.
[16] S. D. Utami, C. Carudin, and A. A. Ridha, “Analisis Live Forensic Pada Whastapp Web Untuk Pembuktian Kasus Penipuan Transaksi Elektronik,” Cyber Secur. dan Forensik Digit., vol. 4, no. 1, pp. 24–32, 2021.
[17] 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.
[18] E. Wahyudi, M. Zulpahmi, K. Gunawan, and B. Imran, “ANALISIS BUKTI DIGITAL WHATSAPP PADA ANDROID SMARTPHONE,” vol. 10, no. 2, pp. 20–26, 2020.
[19] M. N. Faiz, R. Umar, and A. Yudhana, “Analisis Live Forensiks Untuk Perbandingan Keman E-mail Pada Sistem Operasi Proprietary,” Ilk. J. Ilm., vol. 8, no. 3, pp. 242–247, 2016.
[20] J. Moedjahedy, “Forensik komputer Studi Kasus: Universitas Klatab,” J. Sist. Inf. dan Teknol. Inf., vol. 5, no. 2, pp. 95–106, 2016.
[21] I. Saputra and M. N. Faiz, “Analisis dan Investigasi Forensik Digital Live Memory untuk Deteksi Tingkah Laku Agresi Pada Aplikasi Whatsapp,” Semin. Nas. dan Disk. Panel Multidisiplin Has. Penelit. Pengabdi. Kpd. Kpd. Masy., pp. 119–125, 2018.
[22] S. A. Mandowen, “Analisis forensik komputer pada lalu lintas jaringan,” J. Sains, vol. 16, no. 1, pp. 14–20, 2016.
[23] M. Fazarahma, “Forensik Browser pada Aplikasi Facebook Messenger Studi Kasus Ujaran Kebencian Forensik Browser pada Aplikasi Facebook Messenger Studi Kasus Ujaran Kebencian,” 2020.
[24] T. D. Larasati and B. C. Hidayanto, “Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10,” Sesindo, vol. 6, no. November, pp. 456–256, 2017.
[25] D. A. Putri, “Forensic Mobile against Threat WhatsApp Services using National Institute of Standards Technology Method,” vol. 183, no. 30, pp. 1–8, 2021.