Investigation Telegram based-on Web using National Institute of Standards and Technology Method

Marli Prasetio
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

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

ABSTRACT
The very rapid development of science and technology has an impact on the growth of information that is getting faster and easier to access and disseminate, both through print and internet media. In distributing this information, the easiest way to use internet media is an application to exchange messages, for example, Telegram messenger. It is undeniable that many cybercrime cases use Telegram, one of which is for the promotion of online prostitution. Handling crime using an application that requires the internet, requires a forensic investigation that plays a role in the Telegram messenger investigation process to obtain digital evidence. The method used in this study used the National Institute of Standards and Technology (NIST) with the stages of collection, examination, analysis, and reporting. The application of this method is used as a reference in obtaining data in the evidence that the perpetrator is suspected of being used in carrying out the action. In obtaining evidence, the researcher investigates the message conversation data via the Telegram messenger application, such as the contents of the conversation related to the criminal case to be investigated. The evidence that has been collected is then analyzed to find the data needed in the investigation process using the FTK Imager and MOBILedit Forensic Express. Furthermore, the researcher makes a report on the results of the analysis carried out in accordance with the stages and applicable laws.

Keywords
Telegram, MobileForensics, Investigation, Cybercrime, NIST.

1. INTRODUCTION
The very rapid development of science and technology also has an impact on the growth of information, including scientific information. This development was felt to be accelerating because it was caused by the ease of disseminating information through both print and internet media [1]. From the development of the internet, the so-called website emerged. A website or site is a collection of pages that are used to display text information, still or motion images, sound, animation, and or a combination of all of them, both static and dynamic in nature which forms a series of interrelations, each of which is linked to page networks. The relationship between one website page and other website pages is called a hyperlink, while the text that is used as a connecting medium is called Hypertext [2]. Telegram is a cloud-based application with an end-to-end encryption system, self-destruction messages, and a multi data center infrastructure. The ease of access provided by telegram can run on almost all platforms and makes it easy for administrators to build notification systems by utilizing the open Application Programming Interface (API) facility provided by telegram via a bot that can be used to send messages automatically. Cloud base on telegram allows the sending process to be much faster and has a large storage medium [3]. The Telegram application allows it to be abused by its users. The reality that occurs today is one of them as a medium for promoting online prostitution. One of the cases that occurred was the arrest of a person who misused the Telegram service as a media for promoting online prostitution [4]. The method used to carry out the analysis stage of digital evidence or a stage to obtain information from digital evidence in this study is the National Institute of Standards and Technology (NIST) method with the steps carried out in the analysis, namely collection or identification of data retrieval from data sources. The next stage is an examination, namely processing the collected data. Then, the analysis is the analysis of the results of the examination with justified technical methods. The last stage is reporting where this stage is used to report the results of the analysis which includes the actions taken [5].

1.1 Literature Review
1.1.1 Previous Studies
Research conducted in 2018 by Imam Riadi, Anton Yudhana, and Muhamad Caesar Febriansyah Putra resulted in the "Acquisition of Digital Evidence on Android-Based Instagram Messenger Using the National Institute of Justice (NIJ) method". In this study, digital evidence will be acquired using the Oxygen forensic application so as to get the desired results, namely images/photos and conversations/chats from social media Instagram installed on a smartphone [6]. Research conducted in 2018 by Anton Yudhana, Imam Riadi, and Ikhwan Anshori resulted in "Analysis of Digital Evidence for Facebook Messenger Using the National Institute of Standards and Technology (NIST) method". In this study, a scenario has been carried out, using the Galaxy V + SM-G31HZ Smartphone, carrying out the rooting process, installing the Facebook Messenger application, creating messages, carrying out investigations using a forensic tool called Oxygen forensics, then analyzing the forensic software, the results of the analysis will be reported as evidence [5][16]. Research conducted in 2018 by Muhammad IrwanSyahib, Imam Riadi, and Rusydi Umar produced "Digital Forensic Analysis OfBeetalk Application For Cybercrime Handling Using Nist Method". In this study using the National Institute of Standards Technology (NIST) method which consists of several stages including collection, examination, analysis, reporting with the hardware used, namely laptops and cellphones and software. which is used is the BeeTalk application. Meanwhile, forensic tools used include Kingroot, OXYGEN Forensics, and MOBILedit Forensics [8][17].Research conducted in 2017 by Nuril Anwar and Imam Riadi produced "Forensic Investigation Analysis of WhatsApp Messenger Smartphones Against Web-Based WhatsApp". In this study, the WhatsApp evidence on smartphones and WhatsApp web browsers will produce a dual

digital evidence comparison involving cross-platforms, namely Android (mobile forensic) and Windows (computer forensic), the two operating systems produce different characteristics [9][7]. Research conducted in 2018 by Muhammad Abdul Aziz, Imam Riadi, and Rusydi Umar produced "Web-Based Line Messenger Analysis Using Framework National Institute Of Justice (NIJ)". In this study, a simulation of LINE Messenger conversation tapping was carried out by logging into the web-based Line Messenger application through a QR code scan using the victim's smartphone as a search for the presence of digital evidence after the tapping process [10][18].

1.1.2 Digital Forensics

Digital forensics is computer science and technology that uses analysis and investigation techniques to identify, collect, examine and store evidence/information stored/encoded on computers or digital storage media as evidence in uncovering criminal cases that can be legally justified [11][19]. The purpose of digital forensics is to prove an incident that has occurred by investigating the crime scene so that it can prove from evidence such as computer systems, computer storage media (hard disks, CD-ROMs, USB), electronic documents (E-mail), network traffic. and others [12].

1.1.3 Evidence

Evidence is a very important part of a criminal case. From the evidence, the investigation team and forensic analysis can reveal the case with a complete chronology[13].

1.1.4 Website

A website is a collection of pages on a domain on the internet that is created for a specific purpose and is interconnected and can be accessed widely through the home page using a browser and consists of a URL [14].

1.1.5 Telegram

Telegram is a cloud-based application and encryption system that provides end-to-end encryption, self-destruction messages, and a multi-datacenter infrastructure. Cloud base on telegram allows a much faster-sending process and large storage media [3].

1.1.6 NIST (National Institute of Standards Technology)

The National Institute of Standards and Technology (NIST) offers a forensic staged model. The model has stages, namely Collection, Examination, Analysis, and Reporting. An explanation of the stages of the NIST method can be seen in Figure 1.

Figure 1. Stages of the NIST Method

Collection is the labeling, identification, recording, and retrieval of data from relevant data sources using the following procedures to maintain data integrity. Examination is the processing of data collected in a combination of forensic use of various scenarios, whether automatic or manual and assessing and extracting data according to your needs while maintaining data integrity. Analysis is the analysis of the results of an examination using technically justified and legal methods. Reporting is reporting the results of the analysis which includes describing the actions taken [5].

2. METHODOLOGY

2.1 Research Scenario

The pimp or the perpetrator has a conversation with a potential prostitution service user and provides an account contact that will serve the potential user (woman), then the potential user has a conversation with the woman via Telegram chat. Furthermore, the investigator will search, collect, and document the evidence found. In addition to collecting data and documenting, this stage also describes the design of the analysis process as in Figure 2 which explains how investigators get evidence in chat conversations.

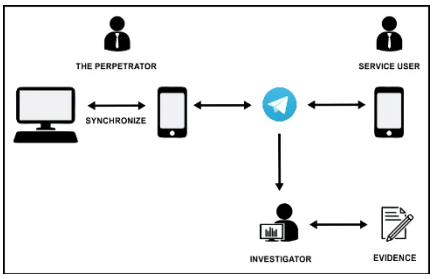


Figure 2. Flow of Evidence Search Process

In Figure 2 it can be defined that the perpetrator and customer are having a conversation via Telegram chat messages where their conversation is stored in the browser cache used, then the investigator conducts an analysis through the device used, namely a computer/laptop. After that, the investigator conducts a crime scene (Place of Case) with the findings that can be used as evidence that will be presented as evidence in the trial process.In the process of identifying evidence, the investigator gets a computer/laptop that contains data to be used in the investigation process. After all the data related to the telegram is obtained, the investigator then looks for digital information to be analyzed to strengthen the evidence. In looking for digital evidence, investigators use the FTK Imager and MobileEdit Forensic Express to help the analysis process. Furthermore, the investigator makes a report related to the results of the analysis carried out in the previous stage and ensures that every process carried out is in accordance with applicable legal rules.

2.2 Research Stages

At the initial stage, evidence is maintained which aims to sterilize evidence from irresponsible parties, then enter the imaging process which aims to backup or duplicate the data contained in the evidence without changing any of the data contained therein. After the evidence is finished imaging, the next step is analysis of the data that has been imaging. In the final stage, the reporting process is carried out from a series of stages that have been carried out, then the report is used as a parameter as evidence of crime based on the findings of evidence and a series of stages as well as an analysis process.The report or reporting that is presented is in the form of a table of findings from the data collected through a series of processes in the previous stages, namely the collection stage which is the stage of collecting evidence, after that the examination stage is the stage for processing data from the evidence found including imaging data. Then the next stage is the analysis stage, which is the last stage before the reporting process. In the analysis stage, an examination of the contents of the data in evidence is carried out in order to provide information about the perpetrator of the crime in the case. From a series of stages that have been carried out, the final information can be presented regarding the findings of the data from the evidence.The following are the stages of the

research process carried out [15][20], including in Figure 3.

Figure 3. Research Stages

2.2.1 Evidence
Evidence was gathered from the perpetrator.

2.2.2 Preservation
This stage includes the process of collecting, searching, and documenting evidence. In addition, the sterile level of evidence is also maintained so that no change occurs.

2.2.3 Acquisition
The process of collecting and obtaining evidence, namely conversation messages, is then carried out by imaging or duplicating the conversation messages for further investigation.

2.2.4 Examination & Analysis
The process by which investigators can carry out exploration, analysis, and reveal the results of imaging from the previous acquisition stage to obtain data related to the perpetrator or criminal act contained in the Telegram application. At this stage, further checks are carried out to ensure that the conversation message contains online prostitution chats.

2.2.5 Reporting
The process of reporting the results of the analysis of the results of the examination and the data obtained from the investigation process.

3. RESULT AND DISCUSSION
The identification phase is carried out to obtain evidence that can be obtained on smartphones and laptops in the form of a smartphone Telegram message conversation database and web Telegram message conversations on the Google Chrome browser. The analysis phase was used to find data differences between the discovery of the Telegram web and the Telegram smartphone using the NIST method.The system identification stage used in this study consists of several components in the form of Software Requirements and Hardware Requirements.The need for software used to find the results of the perpetrator's conversation, the researchers used the Telegram application, FTK Imager, and MOBILedit Forensic Express.The hardware requirements used in this study using 1 laptop and 1 smartphone for research objects as well as simulations in the search for evidence of perpetrators of crime with the specifications of 1 laptop with specifications in Table 1 and 1 smartphone with specifications in Table 2.

Table 1.Laptop Evidence Specifications

Evidence	Brand	CPU	Model	RAM	OS Version
Laptop	Asus ROG	Intel Core i7-2.20GHz	GL503GE	RAM : 8192MB	Windows 10

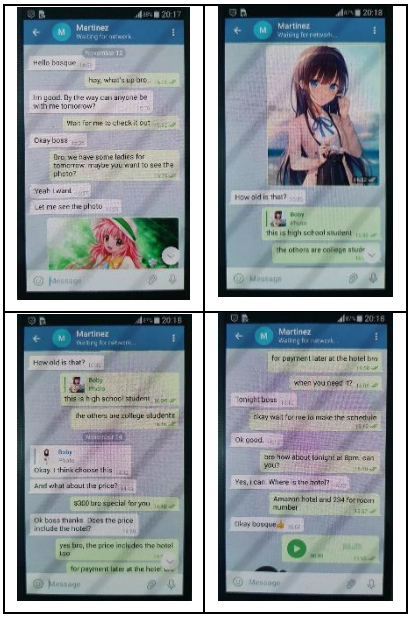
Table 2.Evidence Smartphone Specifications

Evidence	Brand	Series	Model	Imei	OS Version
Smartphone	Samsung	RF1D94204LA	GT-I9190	357960051031833	Android Kitkat(4.4.2)

3.1 Examination
In general, the stages of the investigation process on digital evidence, both laptops, and smartphones have 4 stages, namely preservation, acquisition, examination & analysis, and report as a result of the analysis. The following is an explanation of the 4 stages.

3.1.1 Preservation
This stage is the initial stage of searching, collecting data, and documenting evidence. The sample used for testing this research as evidence for analysis is in the form of a laptop and a smartphone that is rooted in a screen without password security. The initial stage in the form of searching for evidence is carried out by the police as the party with the authority over this matter. The results of the search in the form of evidence found at the crime scene are then submitted to the investigator for data collection and analysis to obtain digital evidence which will then be useful in the trial process. The final stage is documentation carried out on evidence of misuse of applications, namely laptops and smartphones, as well as several photos of the results of conversations between the perpetrators and customers via smartphone devices which will then be investigated. The results of conversation photos on smartphones can be seen in table 3.

Table 3.Photo Conversation Results on a Smartphone



In table 3 are some photos of the conversation between the perpetrator and the customer on the perpetrator's smartphone found at the crime scene which will later be matched to the extraction results on a laptop or smartphone, then the evidence found at the crime scene can be seen in table 4.

Table 4. Evidence found at the crime scene

No.	Evidence Name	Image	Information
1.	The Perpetrator's Smartphone		Samsung GT-I9190 smartphone is rooted and not in screen security mode
2.	The Perpetrator's Laptop		Asus Rog GL503GE laptop is turned off, without a password and not connected to the network
3.	The Perpetrator's Smartphone Charger		smartphone charger for Samsung GT-I9091, not the original Samsung with an output of 5.0 V and 2.0 A.

4.	The Perpetrator's Laptop Charger		Original Asus Rog GL503GE laptop charger with 19.5 V and 7.7 A output.

In table 4, the evidence obtained at the scene of the crime is laptops and smartphones and all supporting evidence without touching it directly so that the investigator's fingerprints do not remain on the evidence, and maintain its authenticity.As for the specifications of evidence found at the crime scene, it can be seen in table 5.

Table 5.Evidence Specifications

Evidence	Brand	Series & CPU	Model	Imei& RAM	OS Version
Smartphone	Samsung	RF1D94204LA	GT-I9190	35796005103 1833 RAM : 1.5GB	Android Kitkat(4.4. 2)
Laptop	Asus ROG	Intel Core i7-2.20GHz	GL503 GE	RAM : 8192MB	Windows 10

In addition to collecting and documenting evidence, at this stage there is also preparation and planning for how the laptops and smartphones will be analyzed and what tools and tools are needed to support this process.

3.1.2 Acquisition

Acquisition (Acquisition) is the stage where researchers clone and take digital evidence from laptops and smartphones found at the crime scene so that the original evidence is maintained to its authenticity. The process uses forensic tools, namely MOBILedit Forensic Express.

3.1.2.1 Acquisition from smartphone

The acquisition process on a smartphone requires a forensic tool capable of imaging data completely, to get more access rights the smartphone must be rooted for imaging using tools, one of which is MOBILedit Forensic Express for the data cloning process on a smartphone. as well as a way to secure evidence so that the data we analyze can be compared with the original data.MOBILedit Forensic Express is able to extract data from smartphone devices and imaging files by selecting the Create Physical Image option. This time, MOBILedit Forensic Express will acquire an imaging result file, which is a file with an .img extension. After that, there is still the smartphone imaging process, evidence that has been detected by MOBILedit Forensic Express tools, and the ongoing process of imaging data.From the acquisition process in Physical Imaging, the results obtained in .img format can be seen in Figure 4.

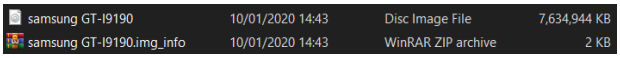


Figure 4.Results of Physical Imaging Smartphone

After the Imaging Physical results are obtained as shown in Figure 4, the next process to open the .img file requires FTK Imager tools.

3.1.2.2 Acquisition from Laptop

The acquisition process on a laptop requires FTK Imager forensic tools to image data on a local disk to find out information that the perpetrator uses the Google Chrome browser to abuse using Telegram web connected to Telegram Smartphone. The acquisition process using FTK Imager is the initial stage for imaging the internal memory on the perpetrator's laptop, in this study the acquisition stage of the laptop imaged data on the internal memory C: devoted only to the C: \ Users \ ASUS \ AppData \ Local \ folder. Googl e \ Chrome as in Figure 5.

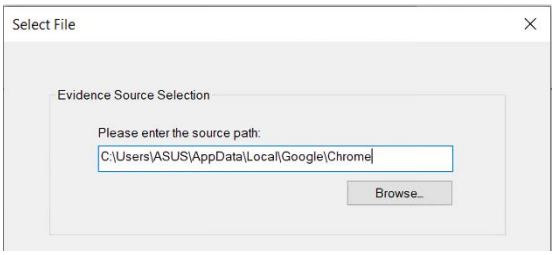


Figure 5.Localdisc C Chrome Imaging Process

In Figure 5, the localdisc C imaging process, especially the Chrome folder, has been selected, so the next process is to fill in the evidence information to give marks such as case number, evidence number, unique description, examiner, and notes so that the imaging file can be identified. The next process is the destination for storing the imaging files. Investigators carry out storage with a destination as shown in Figure 6.

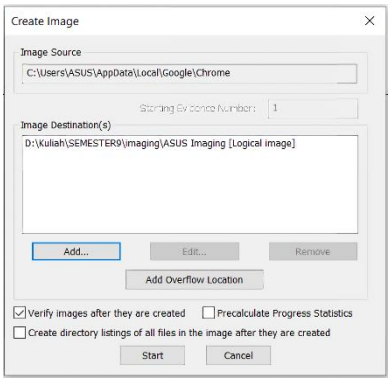


Figure 6. Destination for Imaging File Storage

In Figure 6, the destination for storing imaging files is to save the results of imaging data in the desired folder and also fill in the file name according to the evidence being studied. After all processes are complete, a hash will be obtained from the imaging file that has been created. As in Figure 7.

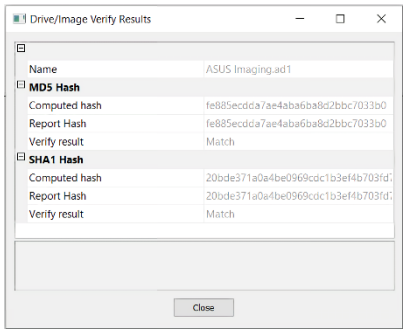


Figure 7.Hashing the Imaging File

In Figure 7 hashing file imaging, we can find out the hash of the imaging file which will then be matched with the hash of digital evidence which will be investigated so that the evidence obtained and the evidence under investigation is the same and does not change the results of the investigation.

3.1.3 Examination & Analysis

This examination and analysis phase aims to uncover and analyze data on the results of the acquisition stage to obtain the data needed for the investigator's investigation process which will then be useful in the criminal trial process. This

process uses several forensic tools to analyze the results of previous cloning, including MOBILeditForensic Express and FTK Imager.

3.1.3.1 Extraction and Exploration of Digital Evidence on Smartphones

At this stage, to open the imaging results that have been done previously from a smartphone device requires FTK Imager forensic tools so that the imaging results can be read by investigators.The process of extracting imaging results on a smartphone is an initial display of the FTK Imager, which has not yet been imported into the .img extension file so that the file can be read by investigators. The next process is to import the previously saved imaging files from MOBILedit Forensic Express into FTK Imager with the extension .img, as shown in Figure 8.

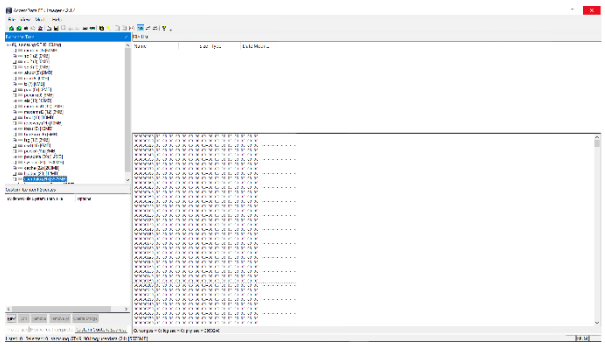
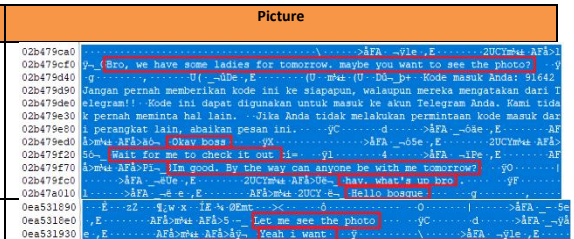
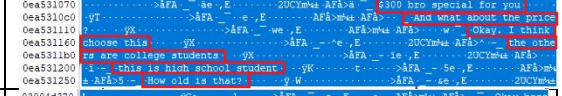
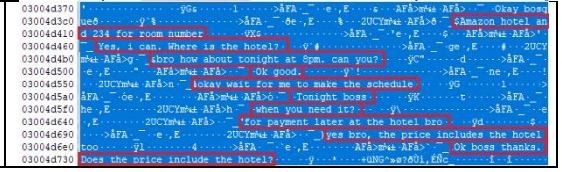


Figure 8. Import Imaging Results on a Smartphone

In Figure 8, the MOBILedit Forensic Express imaging results can be opened using the FTK Imager tool, then we select user data on the evidence tree to find conversation messages indicated by online prostitution trials according to the case in this study by referring to the results of conversation photos on smartphones found on crime scene. As in table 6.

Table 6.Results of Exploration of Conversation Messages on Smartphones

No	Picture
1	
2	
3	
4	

In table 6, the results of the exploration of conversation messages on the smartphone found the contents of the conversation between the perpetrator and the customer, including text messages, photo extensions sent by the perpetrator and audio recorded by the perpetrator.

3.1.3.2 Extraction and Exploration of Digital Evidence on Laptops

At this stage, the exploration of digital evidence is by finding the Telegram database on the Google Chrome browser in the laptop directory as an activity of the perpetrator to carry out the action, to find the Telegram database on the device, the laptop directory can be found in the localdisc C directory, can be seen in Figure 9.

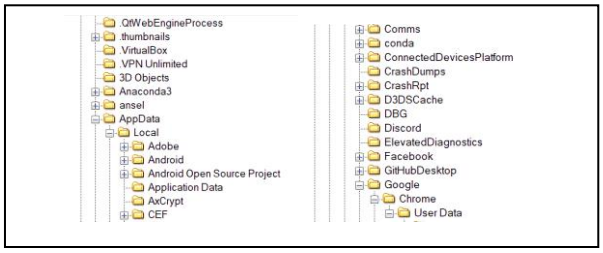


Figure 9.Google Chrome Database Folder

In Figure 9 above the google chrome database folder is located on localdisc C, namely C: \ Users \ ASUS \ AppData \ Local \ Google \ Chrome \ UserData \ Default, in the default folder there is a Google Chrome database to be used as digital evidence about the perpetrator's activities using Google Chrome for cases of online prostitution via the web telegram application. In the default folder, there are several files and folders of the perpetrator's activity in using Google Chrome as digital evidence which can be evidence of online prostitution crimes, can be seen in Figure 10.

Figure 10.Google Chrome Default Folders and Files

In Figure 10, the default Google Chrome folders and files, there are files and folders for the activity of the perpetrator using Google Chrome such as the cache folder as a storage place and to speed up Google Chrome access and also a location to explore the Telegram database on Google Chrome. The following is the location of the Telegram cache file and database storage can be seen in table 7.

Table 7.Location of Cache File Storage on Laptop

File Type	Storage Location	File Name
Cache	C:\UseR\ASUS\AppData\Local\Google\Chrome\User Data\Default\Cache	Cache
Db SQLite	C:\UseR\ASUS\AppData\Local\Google\Chrome\User Data\Default\IndexedDB	Cache

In table 7, the location of cache file storage on a laptop that has been found, the next process will be extracted using the FTK Imager tool. Can be seen in figure 11.

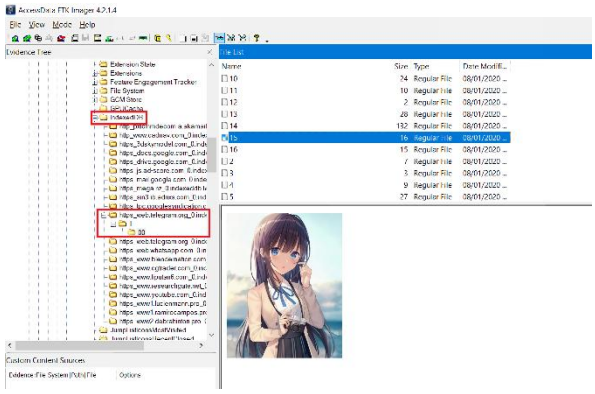


Figure 11.Database Extraction Results on Google Chrome

Figure 11 shows the database exploration process on the Google Chrome browser using the FTK Imager tool. The image is an artifact contained in the Google Chrome browser database. The image of the woman was previously contained in a Web Telegram chat message.

3.1.4 Reporting

All data that had been previously found in the analysis process on the perpetrator's smartphone and laptop were used to reveal a case of the message conversation that was obtained. After analyzing the perpetrator's android smartphone and laptop, it can be seen that the process of implementing mobile forensics on smartphones and the web on laptops related to the telegram application can obtain evidence and information in the investigation process, investigators find indications of digital evidence of a crime in the form of database files on smartphone devices and cache files on laptop devices, but in this study researchers only focused on conversation messages that were found in the database. The results of the analysis have been able to answer questions about the information desired by the researcher. The information obtained from digital evidence is as follows.

3.1.4.1 Analysis Results on Smartphone

The results of the analysis on the smartphone device evidence obtained in the physical image imaging process with the extension .img get the same location for the conversation message file storage as the findings of the perpetrator's smartphone conversation message photo at the crime scene, as in Figures 12 and 13.

Figure 12.Results of Perpetrators' Smartphone Conversation Photos at crime scene

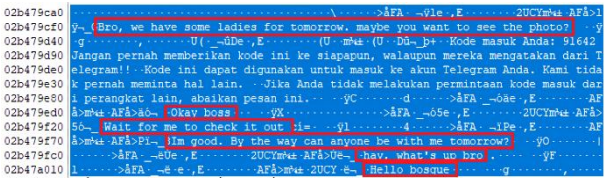


Figure 13. Investigation Results of Perpetrators Smartphone

Figures 12 and 13 match the evidence found at the crime scene and evidence that has gone through the forensic process. The photos obtained at the smartphone scene are not connected to any connection, the smartphone is also not in screen security mode and is rooted. In the extraction process, the smartphone imaging results also produce smartphone information used by the perpetrator.Such information among other smartphone brands, types, platforms, IMEI, root status, etc. Account information is also detected by MOBILedit Forensic Express.The results of smartphone investigations through the mobile forensic process obtained conversation messages between the perpetrator and the customer, smartphone information and account information.

3.1.4.2 Results of Analysis on a Laptop

The results of the analysis on laptops, evidence on laptop devices that are obtained in the directory C: \ Users \ ASUS \ AppData \ Local \ Google \ Chrome \ UserData \ Default \ IndexedDB is the location of the laptop file storage, namely the Google Chrome cache file which contains photo files of women which is the same as the conversation message on the perpetrator's smartphone, as in figure 14 and 15.

Figure 14.Photo Result of Conversation Message at crime scene

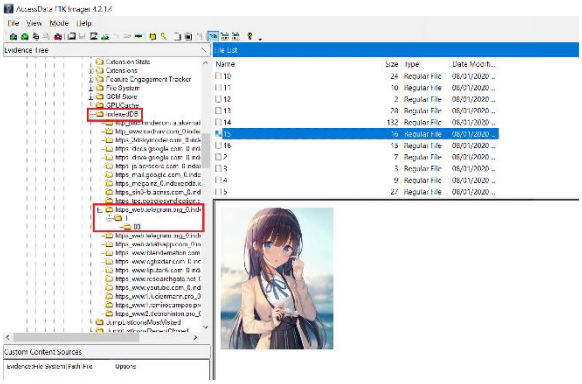


Figure 15.Investigation Results of the Perpetrator's Laptop

Figures 14 and 15 are the results of matching photos of the findings of conversation messages at the crime scene and the results of the perpetrator's laptop forensic process using the FTK Imager tool. In the forensic process using FTK Imager, only image files were obtained while conversation files or other files were not found.

3.1.4.3 Comparison Table of Invesigation Results

The following table shows the comparison of the results of investigations conducted by investigators, it can be seen in table 8.

Findings	Smartphone	Laptop
Conversation Text	✓	
Smartphone Information	✓	
Account Information	✓	
Media		✓

4. CONCLUSION

Based on the findings of evidence at the crime scene and digital evidence on Telegram Web on a laptop that has been synchronized with Telegram on a smartphone that produces information on crimes committed by perpetrators related to online prostitution. In conducting the investigation, the information presented is the disclosure of online prostitution crimes from findings in the form of evidence artifacts in the form of chat message conversation sessions between the perpetrator and the customer, smartphone information, account information, and obtaining other media files that can be used as evidence. Based on the stages and flow of the NIST carried out in this study, it produces the files needed by the investigator by imaging the perpetrator's smartphone using the MOBILedit Forensic Express tool to get the physical results file which can then be reviewed by extracting the file using the FTK Imager tool with match the conversation text found on the perpetrator's smartphone one by one. Meanwhile, the files found by investigators on the laptop used the FTK Imager by finding the Telegram database on the Google Chrome browser as an activity of the perpetrator. Suggestions that can be given for further research are to use more tools, related to this research, only to get a few files of findings as evidence found.

5. REFERENCES

[1] Hasugian, J. (2005). Pemanfaatan Internet Penggunaan Internet Oleh Mahasiswa pada Perpustakaan USU DepartemenStudiPerpustakaan dan Informasi. 1(1).

[2] RahmatHidayat. (2010). Cara PraktisMembangun Website Gratis. Jakarta: PT Elex Media Komputindo.

[3] Fahana, J., Umar, R., &Ridho, F. (2017). QUERY :JurnalSistemInformasi Volume : 01 , Number : 02 , October 2017 ISSN 2579-5341 (online) Pemanfaatan Telegram SebagaiNotifikasiSeranganuntukKeperluanForensikJaringan QUERY : JurnalSistemInformasi Volume : 01 , Number : 02 , October 2017 . 5341(October), 6–14.

[4] Sugiyatmi, T. A. (2019). DayaRusak dan AkarMasalahProstitusi Online. Retrieved from http://kaltim.tribunnews.com/2019/01/12/daya-rusak-dan-akar-masalah-prostitusi-online

[5] Yudhana, A., Riadi, I., &Anshori, I. (2018). Analisis Bukti Digital Facebook Messenger MenggunakanMetode NIST. 3(1), 13–21.

[6] Imam Riadi, Anton Yudhana, Muhamad Caesar Febriansyah Putra. (2018). Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ), Volume 4, No. 2.

[7] Yudhana, A., Umar, R., Ahmadi, A. (2019). Digital Evidence Identification on Google Drive in Android Device Using NIST Mobile Forensic Method. 6(1). Scientific Journal of Informatics

[8] Muhammad Irwan Syahib, Imam Riadi, Rusydi Umar. (2018). Analisis Forensik Digital Aplikasi BeeTalk untuk Penanganan Cybercrime Menggunakan Metode NIST.

[9] Nuril Anwar, Imam Riadi. (2017). Analisis Investigasi Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbasis Web, Volume 3, No. 1.

[10] Muhammad Abdul Aziz, Imam Riadi, Rusydi Umar. (2018). Analisis Forensik Line Messenger Berbasis Web Menggunakan Framework National Institute Of Justice (NIJ).

[11] Saputra, A. P., &Widiyasono, N. (2018). Analisis Digital Forensik pada File Steganography (Studikasus : PeredaranNarkoba). Jurnal Teknik Informatika Dan SistemInformasi, 3(1), 179–190. https://doi.org/10.28932/jutisi.v3i1.594

[12] Marini, S. (2018). Kajian digital ForensikdalamRegulasi di Indonesia. Seminar Nasional Energi& Tek, 103–106.

[13] Ruuhwan, R., Riadi, I., &Prayudi, Y. (2016). Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone. JurnalEdukasi Dan PenelitianInformatika (JEPIN), 2(1). https://doi.org/10.26418/jp.v2i1.14369

[14] Waryanto. (). Pengertian Website LengkapdenganJenis dan 2018Manfaatnya. https://www.niagahoster.co.id/blog/pengertian-website/#Apa_itu_Website

[15] Kunang, Y. N., &Khristian, A. (2016). ImplementasiprosedurforensikuntukanalisisartefakWhatsapp pada ponsel android. Annual Research Seminar, 2(1), 59–68. http://ars.ilkom.unsri.ac.id

[16] Yuwono, D. T., Fadlil, A., Sunardi. (2019). Perbandingan Kinerja Perangkat Lunak Forensik untuk File Carving denganMetode NIST. 7(3), 89-92. Jurnal Teknologi dan Sistem Komputer

[17] Zuhriyanto, I., Yudhana, A., Riadi,I. (2020). Analisis Perbandingan Tools Forensic pada Aplikasi Twitter Menggunakan Metode Digital Forensics Research Workshop. 4(5). 829 – 836. http://jurnal.iaii.or.id

[18] Riadi, I., Umar, R., Aziz, M. A. (2020). Komparatif Web-based Instant Messaging Vulnerability Menggunakan Metode Association of Chief Police Officers. 4(5). 813 – 819. http://jurnal.iaii.or.id

[19] Sunardi, Riadi, I., Akbar, M. H. (2020). Penerapan Metode Static Forensics untuk Ekstraksi File Steganografipada Bukti Digital Menggunakan Framework DFRWS. 4(3). 576 – 583. http://jurnal.iaii.or.id

[20] Prasongko, R. Y., Yudhana, A., Fadil, A., (2018). Analisa Forensik Aplikasi Kakaotalk Menggunakan Metode National Institute Standard Technology. 129-133. Seminar Nasional Informatika 2018