Jurnal Elektronik Ilmu Komputer Udayana
Volume 8, No 4. May 2020

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Forensic Analysis of Telegram Desktop-based Applications using the National Institute of Justice (NIJ) Method

I Gusti Ngurah Guna Wicaksana[a1], I Ketut Gede Suhartana[a2]
[a]Department of Computer Science,
Universitas Udayana
Bali, Indonesia
[1]gunawicak1@gmail.com

Abstract

The development of telecommunications has increased very rapidly since the internet-based instant messaging service has spread rapidly to Indonesia. Telegram application is one of the growing and well-known application services in Indonesia, Desktop or smartphone-based Telegram applications, it is very possible to use digital crimes by using services, user personal information, or by hacking the Telegram application. This study explains the stages of investigation of cybercrime cases that occurred in desktop-based telegram. The method used for this research refers to the stage of investigation that was carried out in previous studies, namely using the National Institute of Justice (NIJ) method with the stages of the preparation stage, the collection stage, the examination stage, the analysis stage, and the reporting stage. The media used in this study is a desktop-based Telegram application that is synchronized with an Android-based Telegram. In this process, the location of the log file, cache, and digital proof image file was obtained in the conversation of a desktop-based Telegram application. Digital forensic evidence obtained is expected to strengthen evidence of criminal cases in court in the form of digital evidence analysis results.

Keywords: *Telecommunications, Digital Forensic, Telegram, Investigation, Cybercrime*

1. Introduction

Instant messaging (IM) services have changed the way people communicate to each other in recent years. Although, it is not new at means of communication but the emergence of smartphones and mobile broadband technologies stimulated the evolution of communication patterns between people and organizations.

One of the instant messaging applications that is currently popular and developing is telegram, Telegram is an instant messaging service based on cloud services and voice over internet protocol (IP) launched two brothers Nikolai and Pavel Durov in 2013. This application can be used on devices with operating systems Android, iOS, Windows Phone, Windows NT, macOS, and Linux.

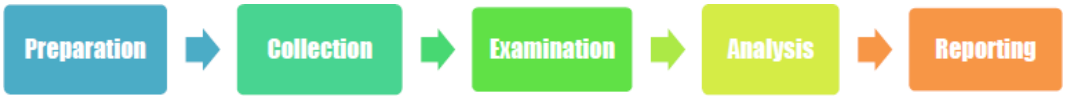
In 2014, Telegram was referred to as the best-selling messaging application in 46 countries. In March 2018, Telegram claimed to have 200 million active users per month. Although not specifically mentioned, Telegram users in Indonesia are estimated to also reach millions of people [1].

Telegram application users are many and widespread also bring several problems one of which is cybercrime such as drug trafficking, terrorism, cyber-bullying, and human trafficking [2] . The UN comprehensive study explains that Cybercrime is limited in the number of actions against the confidentiality, integrity and availability of data or computer systems [3]. Cybercrime has now become the number one threat of short message applications, to complete short message-based Cybercrime, investigators need to conduct a forensic analysis of victims and suspects' devices in order to find digital evidence

(Capstone, 2018) [4]. Analysis on digital forensics can use the National Institute of Justice method or can use the National Institute of Standards and Technology method [5]. Based on previous research, it can be known what potential evidence is contained in the short message application such as date / time, text message, and picture / photo [6] . Research conducted is expected to produce digital evidence that can strengthen evidence of criminal cases in court in the form of digital evidence analysis results.

2. Reseach Methods

This study adapted the NIJ forensic analysis method investigation process. That method used to describe how the description of the research process being carried out in order to be able known stages of this study more systematically so that it can be used as a reference on further research. The stages of the research method can be seen in Figure 1.



Picture 1. Stages of Research Methods

This research method is divided into several stages namely the preparation stage, the collection stage, the examination stage, the analysis phase, and the reporting stage, the NIJ method stage is explained in full as follows :

The first stage is preparation or preparation is an activity to prepare equipment to perform the tasks required in the investigation process. At this stage therein there is a process of preparing tools that will be used in the investigation process.

The second stage is the collection or collection is the process of finding documents, and collecting data or make copies of physical objects that have digital evidence in them. Collection phase in this process digital data collection is carried out from a relevant source in order can maintain the originality of digital evidence from the possibility of change.

The third stage is examination, this stage is the stage for examining evidence digitally obtained through the forensic process manually or automatically and for ensure that the digital evidence obtained is as original as obtained at the place of occurrence crime.

The fourth stage is analysis, after obtaining the digital evidence needed from the stage previous investigation, then the digital evidence obtained was analyzed in detail using a method that has been scientifically and legally recognized in order to determine the significance of evidence the digital.

The fifth stage is reporting, after going through the analysis phase of digital evidence obtained, Then reporting from the results of the analysis consists of a description of the activities that have been carried out carried out in the investigation process, an explanation of the tools used in the investigation process, the investigation method that has been used, the determination of the supporting actions of the investigation that has been done, as well as providing some recommendations as material for evaluating supporting elements which contained in digital forensic [5] [7].

3. Result and Discussion

3.1 File Exploration

Forensic analysis results in this study were obtained by using methods and tools to assist researchers in finding the data needed in the forensic investigation process. This study begins by creating a Telegram media account for the Telegram conversation simulation process, then in the process of this research the selection of tools to retrieve data on the Telegram account is conducted. FTK Imager was chosen as a tool used in this study. The next step is to collect digital evidence by exploring in the laptop directory to find the SQLite Telegram database on the internal hard drive, from the exploration process found the location of the SQLite database at

p-ISSN: 2301-5373
e-ISSN: 2654-5101

C:\Users\Guna Wicaksana\AppData\Roaming\Telegram Desktop\tdata\user_data\cache\0\5A l . The default folder which is the location of SQLite

The telegram database contains a database of all Google Chrome activities in the form of files and folders such as cache and logs. The findings of the investigation related to desktop-basedtelegram can be seen in Table 1:

Table 1. Exploration Results on Laptops

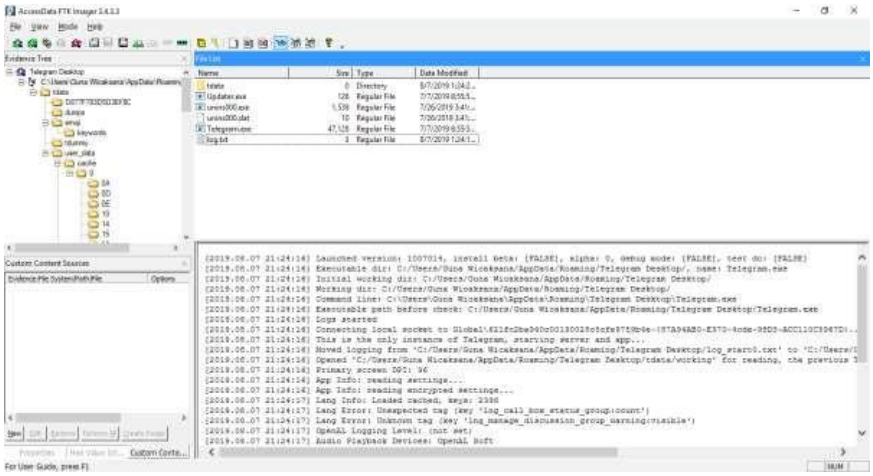
File Type	Storage Location	File Name
Log File	C:\Users\Guna Wicaksana\AppData\Roaming\Telegram Desktop	Log.txt
Cache	C:\Users\Guna Wicaksana\AppData\Roaming\Telegram Desktop\tdata\user_data\cache\0\16	E8939B 698ACF
Db	C:\Users\Guna Wicaksana\AppData\Roaming\Telegram Desktop\tdata\user_data\cache\0\5A	DB3728 CEB30 A

3.2 Analysis

The analysis phase of this research is carried out by analyzing the digital evidence obtained utilizing supporting tools and literature to be able to achieve the objectives of the research. The testing standards in this study utilize digital forensic tools that are widely used and available free of charge, namely FTK Imager.

3.2.1 Log File Location Analysis

This research is an analysis process related to the location of Telegram artifact applications using FTK Imager tools. Based on the research data in Table 1 the location of the Telegram application log file can be determined. The Telegram application log file can be viewed using FTK Imager tools as shown in Picture 2.



Picture 2. Telegram Dekstop Application

Based on Picture 2, it can be seen that the location of the log file is in the Desktop Telegram folder in the folder besides the Telegram application log file, there are also several other files. In the log file there is the word "user_data" this proves that the log file is a Telegram application log file.

3.2.2 Cache File Analysis

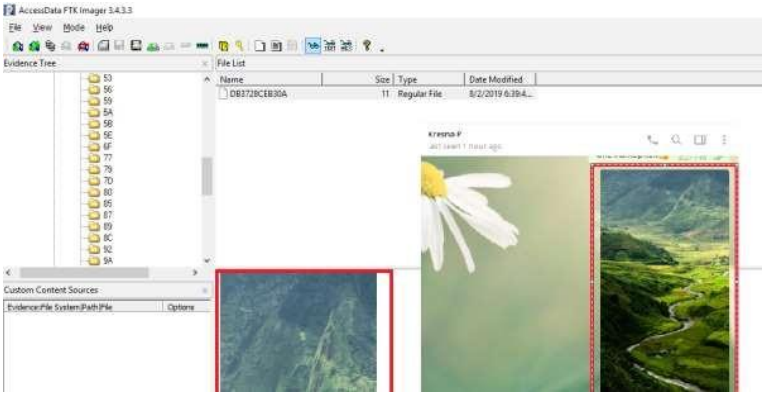
This research is an analysis related to the validity of the Telegram application cache files found in the exploration process using the help of FTK Imager tools. Based on exploration results in Table 1, the location of the Telegram application cache file, the location of the Telegram application cache file can be seen using the FTK Imager tools as shown in Figure 3.

Picture 3. Test the Validity of the Cache File

Based on Picture 3 it can be seen that the location of the Telegram application cache file is in the Cache folder, in that folder there is a cache file of all application activities. The cache file shows the same Telegram sticker image as the chat on the Telegram app on a PC. This proves that the cache file is the original cache file of the Telegram application.

3.2.3 Digital Evidence Analysis

Analysis of the digital evidence file obtained after the exploration process is carried out using the help of FTK Imager tools. Based on exploration results in Table 1, the location of the Telegram digital evidence file is known, the location of the digital evidence file can be seen using the FTK Imager tools as shown in Figure 4.



Picture 4. Digital Evidence on Telegram Chat

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Based on the findings of digital evidence in Figure 4, a study was carried out by deleting the Telegram application chat containing digital evidence on a smartphone, after the chat was removed, it was rechecked on the digital evidence file and the result was that the digital evidence file was intact. This proved that the digital proof file was not will disappear even if the chat on the Telegram application has been deleted. The results of this study are expected to obtain digital evidence that can be used to assist the trial process.

4. Conclusion

Telegram is one of the short message applications that are widely used in Asian countries, specifically Telegram is widely used by users who prefer attractive appearance and emoji features that provide many choices in expressing the purpose of a conversation. This research uses the NIJ method, the method has several stages, namely the Preparation stage, the Collection stage, the Examinition stage, the Analysis stage and the Reporting stage. This research uses a web-based Telegram application media that is synchronized with an Android-based Telegram. In this process, the location of the log file, cache, and digital evidence from the simulation of crime was obtained through the process of tapping the victim's Android-based Telegram application. Digital evidence obtained from the laptop directory exploration process using the FTK Imager tool is not lost even though the chat on the Telegram application of victims and perpetrators has been removed. Digital forensic evidence obtained is expected to strengthen evidence of criminal cases in court in the form of digital evidence analysis results.

References

[1] H. Widowati, "katadata.co.id," 23 5 2019. [Online]. Available: These 10 Telegram Specificationshttps://katadata.co.id/berita/2019/05/23/ini-10-keajuan-telegram-application -order- training-whatsapp.

[2] R. Umar, G. Maulana and I. Riadi, "A Comparative Study of Forensic Tools for WhatsApp Analysis," *International Journal of Advanced Computer Science and Applications,* 2017.

[3] A. Fadlil, I. Riadi and A. Fauzan, "Evidence Gathering and Identification of LINE Messenger on Android Device," *International Journal of Computer Science and Information Security,* 2018.

[4] M. Chang and C. Chang, "Forensic analysis of LINE messenger on android," *Journal of Computers (Taiwan),* 2018.

[5] I. Riadi, R. Umar and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (NIJ)," 2018.

[6] I. Riadi, A. Yudhana and M. Caesar Febriansyah Putra, "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice Institute Of Justice Institute of Justice," *Jour,* pp. 219-227, 2018.

[7] M. Faiz, R. Umar and A. Yudhana, "Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email," *JISKa,* pp. 108-114, 2017.