International Journal of Information System & Technology
Akreditasi No. 158/E/KPT/2021 | Vol. 6, No. 1, (2022), pp. 145-151

National Institute of Standards And Technology (NINST) Method for Cyber Crime Using Forensic Data on Smartphone

Imam Zaenuddin[1], Yosua Novembrianto Simorangkir[2], Arman Syah Putra[3]

[1]Faculty of Informatics Management, STMIK Pranata Indonesia, Indonesia
[2,3]Faculty of Information System, STMIK Insan Pembangunan, Indonesia

imamzaenuddin@gmail.com[1], yosua.simorangkir@rocketmail.com[2], armansp892@gmail.com[3]

Abstract

The background of this research is how to use the NIST method on crimes that use forensic data on smartphones, using the NIST method it will be known whether the method is the right one to use in case solving methods, especially cybercrime cases. The method used in this study is to use the ethnic method which consists of collection, examination, analysis and reporting. With these 4 methods, it can be used to find out which data is used as crime data on smartphones that have been checked. The problem raised in this study is how to find out data that has been lost on a smartphone by using that data and using ethnic methods so that it can open the veil of crime in cyberspace. The purpose of this study is how to find the right data to be used as evidence, as evidence of crime using ethnic methods on smartphones.

Keywords: *Investigations, WhatsApp Application, Evidence, Crime, Conversation Data.*

1. Introduction

The rapid development of technology can cause problems for the technology itself, this makes the internet as one of the media used for data theft of organizations, individuals and governments. Cybercrime is based on the type of activity such as Unauthorized Access, a crime committed by someone by entering a computer network system without the permission of the owner of the computer network system he enters, Illegal Contents, a crime by entering data or information into the internet and is considered unlawful, Spreading viruses intentionally such as Malware by damaging software. The problem that will be raised in this research is how to find out the stages that will be obtained from an application called WhatsApp to obtain evidence that can be legally accounted for so that the evidence can bind lawbreakers, especially in the field of cybercrime [1]. There are several stages used to obtain evidence, especially digital evidence, one of which is by using the NIST method which combines several methods into one with high technology standards. The National Institute of Standards And Technology (NIST) is the non-regulatory national body of the United States technology administration. The agency's mission is to promote and create measures, standards, and technologies to increase productivity, support trade, and improve the quality of life for all [2].

The NIST cybersecurity program security in the cyber field is now widely used with several methodologies to get better evidence, especially digital evidence which is widely used by developed and developing countries to secure programs used by the government and continue to develop better security [3]. The ultimate goal of this development is to develop protection techniques for forensic data in order to get better information based on applications, on mobile phones that extract data so that forensic data can be taken as evidence

ISSN : 2580-7250

in court. In any forensic examination of an Android phone, a good forensic methodology must be observed. Smartphone devices are now an important source of digital evidence who have a relationship with social media in order to obtain evidence of data that can be accounted for [4]. However, the difference between smartphone devices is a challenge for investigators or forensic investigators to develop methods and techniques that are tailored to investigate various cybercrime cases [5]. Smartphone forensics is part of forensics that takes data from smartphones to find data that has been used or deleted so that the data is protected and not used as evidence. As evidence in court because the data on the smartphone cannot be lost and stored in the phone memory and can be used as evidence as evidence of a crime and can be accounted for in court. The development of smartphones from year to year is growing because technology is increasingly sophisticated and the use of technology on smartphones continues to grow so that smartphones can be used for many things and can make it easier for humans to do their daily work [6]. The use of chat applications on smartphones has been widely used by many people. Therefore, almost one million people per day use chat applications on smartphones so that they can connect with many parties and make their daily work easier. Therefore, the use of chat applications on smartphones is a gap for crime to continues to be developed because there are many weaknesses in smartphones that are found by criminals in carrying out their actions [7]. WA is supported by encryption features to ensure the security of its users' data. The popularity and features provided by WA can be misused by the public for criminal purposes, such as drug trafficking, terrorist activities, assassination planning, and other criminal activities through the available features [8]. The variable of this development is the investigation of WhatsApp Messenger digital evidence. Through a series of standard stages according to digital forensic procedures, so that the idea or design and the proposed design of WhatsApp Investigation includes several main components, both at the investigative stage.

2. Research Methodology

The method used is the WhatsApp forensic investigation method which involves the process scheme, namely the WhatsApp attack pentest and WhatsApp wiretapping flowchart, so that the results of a comparison of investigations on two devices will be obtained including WhatsApp on Smartphone with Android operating system and WhatsApp Web on computer with Windows platform so that later there is a comparison normalization table for the exploration of digital evidence findings which state that crimes are related to WhatsApp messenger service messages. The stages in the National Institute of Standards and Technology (NIST) method below are the stages carried out in the NIST method, as follows:

1) Collection (Data collection) at this stage, what is done is the collection of evidence by the process of identification, collection, return and recording of evidence.
2) Examinerion (Data acquisition) at this stage the results of the collection of evidence are tested so that there is no change in information on the evidence.
3) Analysis At this stage, evidence is examined to obtain evidence related to the case.
4) Reporting (Reporting) Reporting the results of the investigation obtained from the investigation contains the results of the analysis of evidence so that the evidence helps the investigation process to find the suspect.

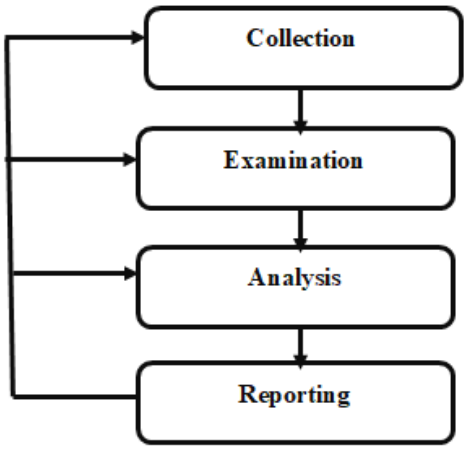

Figure 1. New Method of Waterfall

3. Result and Discussion

In this development I developed a WhatsApp Messenger digital evidence investigation. Through a series of standard stages according to digital forensic procedures, so that the idea or design and the proposed design of WhatsApp Investigation includes several main components, both at the investigative stage. The stages of cellular forensic analysis can be described as follows:

a) Collection (Data collection).
The smartphone used has been rooted. Rooting is the process of unlocking total access on an Android smartphone. Mobile Forensics can be performed on a variety of smartphones, however, in this research, the focus is on smartphone forensics with the Android platform. As the number of smartphones that are rich in various features makes it a challenge to create forensic investigation tools or standards specific to each platform. In the collection process using Android.

b) Examinerion (Data acquisition).
The examination process is a test on the WhatsApp Messenger application using the Oxygen forensic tool. Because the Oxygen tool extracts all applications on the smartphone, including WhatsApp, which is used as evidence of wiretapping. This can happen due to the android smartphone synchronizing the account with the phonebook. The synchronization process will later be linked to the WhatsApp Web application contained in the forensics browser on a computer with a Windows platform.

c) Analysis.
Forensic investigations of Microsoft Windows operating systems, by understanding forensic concepts and artifacts of the core components of the windows platform and their applications. Computer forensics will discuss how to recover, analyze, and authenticate forensic data on Windows systems, track specific user activity in application or program files, and identify findings for use in forensic digital incident response in this case WhatsApp Web's ability to read similar applications on smartphones in relation to cybercrime litigation.

d) Reporting (Reporting).
At the reporting stage, the results of the analysis that have been carried out, along with the results of the forensic tool.

Table 1. Windows Browser Forensics

"Windows" WhatsApp Web Application Browser Forensics				
	System Windows	**Web Browser Forensics (Mozilla)**	**Web Browser Forensics (Chrome)**	**Network Capture**
File Type store	Database On System	Cookies.sqlite formhistory.sqlite content-prefs.sqlite	Cookies.sqlite formhistory.sqlite content-prefs.sqlite	Data Package captured network
Data Type	boolean, float, int, long, strings	Path of database .sqlite	Path of database .sqlite	Data Package captured .pcap
Location	\Program Files\Mozilla Firefox\browser \Program Files\Google\Chrome\Application	\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles	\Users\Administrator\AppData\Local\Google\Chrome\User Data	Log files in/data/data/files
Acces Level	Administrator (image windows)	Administrator (image windows)	Administrator (image windows)	Network (level layer)
Forensic Use	Source of forensic digital data investigation	Source of forensic digital data investigation	Source of forensic digital data investigation	Forensic data from the results of network access capture

The SQLite database can be used as a support for digital investigative actions in relation to helping investigators to collect WhatsApp Web artifacts. Digital evidence with the WhatsApp Web database has data that can be explored as evidence, including:

a) Website Browser Mozilla;
b) Website Browser Chrome.

Based on the SQLite data found in the sub-directory above, the WhatsApp Web conversation database will then be extracted with a certain method (text classification) according to the evidence of WhatsApp on the Smartphone.Based on the flowchart image in figure 2, it is explained that installing the WhatsApp application first and then informing the WhatsApp application, so that WhatsApp can authenticate the data, there are two choices yes or no, if you choose yes, then there are two choices, namely using smartphone media or using website media, both requires synchronization of data from a phonebook or smartphone, otherwise the smartphone in the network will facilitate the re-application of WhatsApp information.

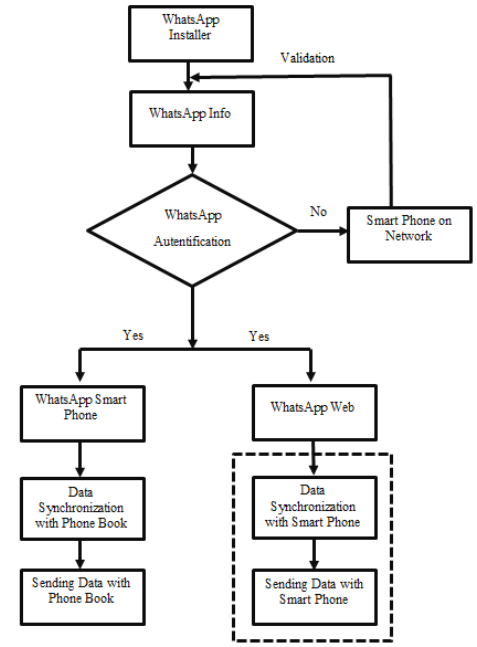

Figure 2. Flowchart Diagram

Based on the usecase diagram, it can be explained that there are two actors, namely analysis and system, with use case save data, extract Smartphone data, Smartphone investigations, history from browser export file in browser, Network analysis, and give result, all of them it will lead to a system that has been analyzed by an analyst. Based on the activity diagram in Figure 3, it can be explained that the analysis begins in mobile forensics, after getting a share of the data, which is then stored on a device or smartphone, which is stored on internal storage, then the data is extracted by the system, so that it can be known who is tapping the forensic.

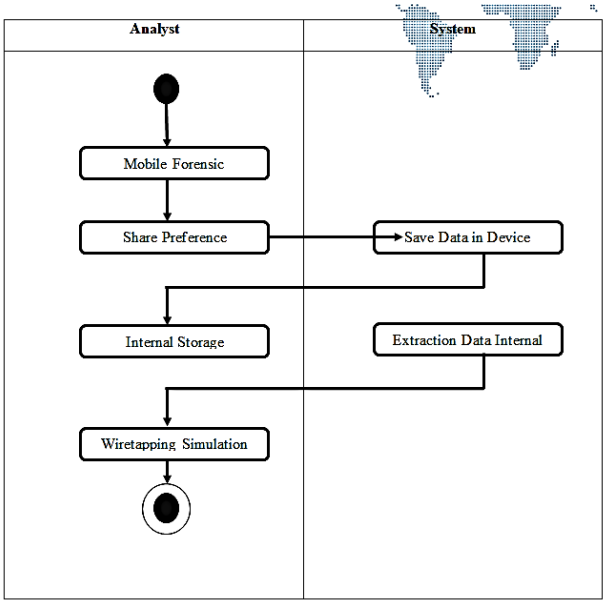

Figure 3. Activity Diagram

4. Conclusion

WhatsApp has become a popular application for social networking where people can exchange personal information along with their mobility. This research has shown that a person can gain complete access to all information on WhatsApp, be it WhatsApp Smartphone or WhatsApp Web. The results that have been obtained are conversational text, images and audio. It is hoped that in the future more research can be carried out on the interpretation of WhatsApp conversation data in the form of journals or other manuscripts as further literature.

References

[1] H. W. Arman Syah Putra, "“Intelligent Traffic Monitoring System (ITMS) for Smart City Based on IoT Monitoring”," *1st 2018 Indonesian Association for Pattern Recognition International Conference, INAPR 2018 - Proce vol*, 2019.

[2] A. S. Putra, H. Warnars, F. Gaol, B. Soewito and E. Abdurachman, "A Proposed surveillance model in an Intelligent Transportation System (ITS)," *1st 2018 Indonesian Association for Pattern Recognition International Conference, INAPR 2018 - Proce vol. , 25*, pp. 1-10, January 2019.

[3] A. S. Putra, "Konsep Kota Pintar Dalam Penerapan Sistem Pembayaran Menggunakan Kode QR Pada Pemesanan Tiket Elektronik," *TEKINFO Jurnal Ilmiah Teknik Informatika*, vol. 21, pp. 1-15, 2020.

[4] I. Ramadhan, A. Kurniawan and A. S. Putra, "Penentuan Pola Penindakan Pelanggaran Lalu Lintas di DKI Jakarta Menggunakan Metode Analytic Network Process (ANP)," *IKRA-ITH INFORMATIKA: Jurnal Komputer dan Informatika*, vol. 5, no. 1, pp. 51-57, 2020.

[5] A. Saputra, A. Fahrudin, A. S. Putra, N. Aisyah and V. Valentino, "The Effectiveness of Learning Basic Mathematics through Dice Games for 5-6 Years Old at TKIT Al-Muslim," *International Journal of Educational Research & Social Sciences*, vol. 2, no. 6, pp. 1698-1703, 2021.

[6] . V. H. Valentino, H. S. Setiawan, M. T. Habibie, R. Ningsih, D. Katarina and A. S. Putra, "Online And Offline Learning ComparisonIn The New Normal Era," *International Journal of Educational Research & Social Sciences (IJERSC)*, vol. 2, no. 2, p. 449–455, 2021.

[7] V. Valentino, H. S. Setiawan, . A. Saputra, Y. Haryanto and A. S. Putra, "Decision Support System for Thesis Session Pass Recommendation Using AHP (Analytic Hierarchy Process) Method," *Journal International Journal of Educational Research & Social Sciences*, pp. 215-221, 2021.

[8] R. Wirawan, N. Aisyah, A. Rahman, B. S. Rahmawati, A. Medikano, A. Sebayang and A. S. Putra, "Perancangan Aplikasi Website Menggunakan Macromedia Dreamweaver Mx Untuk Budi Daya Anggrek (Studi Kasus Toko Anggrek Berseri)," *TEKINFO*, vol. 22, no. 2, pp. 77-86, 2021.

Authors

1st Author
Imam Zaenuddin
Faculty of Informatics Management, STMIK Pranata Indonesia
imamzaenuddin@gmail.com

2nd Author
Yosua Novembrianto Simorangkir
Faculty of Information System, STMIK Insan Pembangunan
yosua.simorangkir@rocketmail.com

3rd Author
Arman Syah Putra
Faculty of Information System, STMIK Insan Pembangunan
armansp892@gmail.com