International Journal of Information System & Technology
Akreditasi No. 158/E/KPT/2021 | Vol. 6, No. 1, (2022), pp. 152-158

Investigations Using The Whatsapp Application By Analyzing Evidence of Crime In Conversation Data

Priyono[1], Bilal Abdul Wahid[2], Priatno[3], Risdiandri Iskandar[4], Ali Akbar[5], Arman Syah Putra[6]

[1,2,3]Faculty of Engineering and Informatics, Bina Sarana Informatika University, Indonesia
[4,5]Faculty of Industrial Technology, Gunadarma University, Indonesia
[6]Faculty of Information System, STMIK Insan Pembangunan, Indonesia

priyono.pyo@bsi.ac.id[1], bilal.baw@bsi.ac.id[2], priatno.prn@bsi.ac.id[3], risdiandri@staff.gunadarmac.id[4], akbarjawas@gmail.com[5], armansp892@gmail.com[6]

Abstract

The background of this research is to find evidence in an application called WhatsApp by analyzing data in the form of conversations or chats from 2 people who are suspected of having their conversations contain suspicious words, therefore by analyzing their conversations, errors or violations will be known conducted. The method used in this study uses the latest waterfall concept, which has been modified in order to help find answers to the problems raised. The problem raised in this study is to find evidence in the conversations carried out in the WhatsApp application. The purpose of this research is to find strong evidence so that it can be used as evidence in court and save suspicious conversation data.

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

1. Introduction

The development of communication technology is indeed very fast growing now with the internet of things, development will be more advanced because wherever and whenever you can have a conversation through writing or video, with this, communication will be smoother so you can see both parties through video communication call. Therefore, this very rapid development needs to be balanced with the protection that is carried out in order to limit the occurrence of crime in the telecommunications world with good protection Technology users will feel safe and comfortable using the technology and can feel protected from personal things that they want to hide and unknown to others [1]. Crime is said to be cybercrime, which has started to develop a lot, which was originally only a fraud by telephone, now it is developing through the internet of things. With the development of crime, the police must also balance the criminals in committing their crimes so that the police can prevent and arrest the perpetrators of crime, especially in the field of cybercrime. Which continues to develop along with the times and technology. Therefore, with the existence of ITE (Electronic Information and Transaction) law no. 11 of 2008 criminals in the field of cybercrime will continue to be arrested and will continue to be sought through digital evidence on smartphones or computers used by criminals who commit crimes in the field of cybercrime. Therefore, with digital evidence, it will be increasingly strong evidence of the digital crime. The method I use in this development is EDA (exploratory data analysis). In simple terms,

ISSN : 2580-7250

EDA is a data exploration process that aims to understand the contents of the data in more detail. The more information collected, the better the understanding [2].

The purpose of developing this journal is to get a conclusion that with the new method used to develop the journal, the author will get better and more detailed results than the previous method. Regarding the definition of the meaning of a smartphone, he explained that it was a cellular phone device that was equipped with various features. Therefore, apart from being a telecommunication tool, a smartphone can also be used for business purposes that can be used by entrepreneurs and the general public [3]. Forensic is a way to find out crimes that have been committed by using past data so that the data can be used as evidence in court that can punish criminals for committing crimes. In digital forensics, evidence will be found on Smartphones or computers connected to the internet so that the data can be used as evidence in court and strong in law for criminals who have committed crimes in the field of cybercrime [4]. The digital evidence includes, among others: laptops, mobile phones, notebooks, and other technological devices that have a storage area and can be analyzed. The variable from the development carried out by the author is data from crime case scenarios, because based on many articles used so that there are codes that exist in the criminal code that can be used in cases that are recorded in secret and can be developed as digital evidence in prosecution in court [5].

2. Research Methodology

The old method used is the DFIF method where there are 5 stages [6], namely the literature reviews stage, observation & data collection, extraction model, DFIF investigation, and documentations [7].

Figure 1. Metode DFIF

The new method that will be used by the author in this development is the waterfall method. Where there are also 5 stages, namely data identification, data collection, investigation, data analysis, and results and conclusions [8].

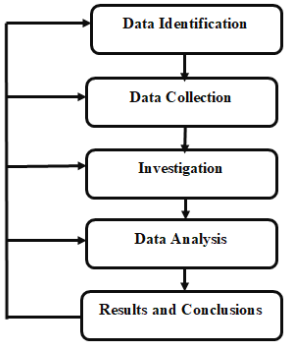

Figure 2. New Method of Waterfall

3. Result and Discussion

In this development, the author uses a scenario of a luxury car smuggling crime case. Because according to article 112 of the Criminal Code, it is not allowed to use original cases because the records of criminal cases are very confidential.

a) Data identification

To identify the data, the authors identify data from the scenarios of the crime of embezzlement of luxury cars that have been made. The scenarios that have been made include conversations via chat and calls between buyers and sellers as well as physical evidence obtained from the iPhone X smartphone as evidence.

Figure 3. iPhone X smartphone

b) Data collection At this stage, the authors collect evidence of chat and telephone calls on the iPhone X smartphone which allegedly contain conversations and transactions between buyers and sellers.

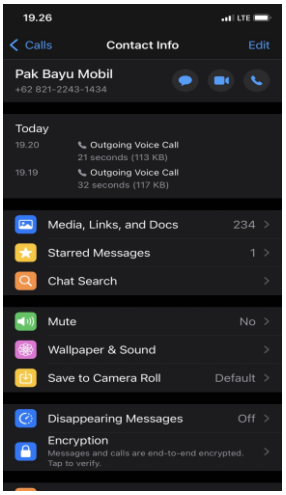

Figure 4. Contact Info

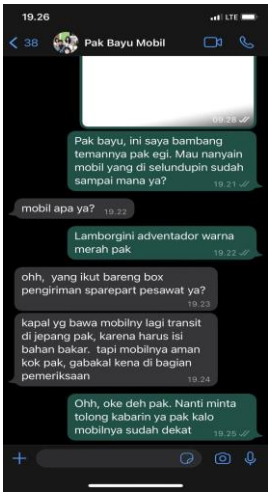

Figure 5. Chat for Evidence I

c) Investigation

The investigation is carried out by examining digital data for digital that is relevant to existing physical evidence.

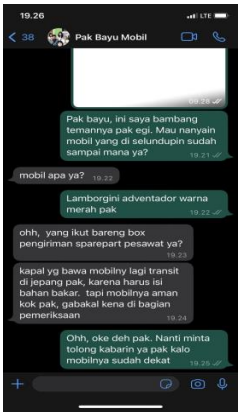

Figure 6. Chat for Evidence II

Figure 7. The Car

d) Data analysis

In this section, the author analyzes the data from the data that has been obtained from the previous 3 stages. Where we will find out whether the digital evidence is relevant to the physical evidence that has been obtained.

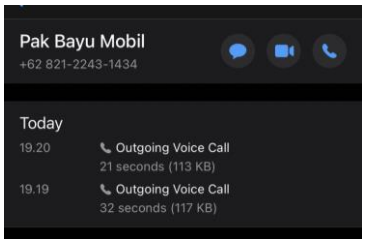

Figure 8. First Analysis Chat

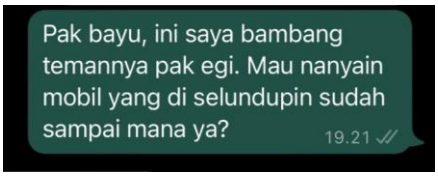

Figure 9. Second Analysis Chat

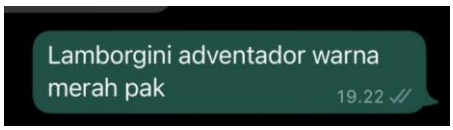

Figure 10. Third Analysis Chat

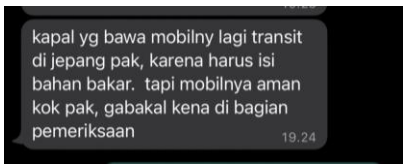

Figure 11. Fourth Analysis Chat

Figure 12. Fifth Analysis Chat

Based on the analysis of evidence from digital evidence in the form of chats and calls found on the iPhone X between buyers and sellers as well as physical evidence of a red Lamborghini Adventador that had arrived and was found. From the analysis of this evidence data, it shows that it is true that the iPhone X is evidence from luxury car buyers used to communicate in luxury car smuggling transactions.

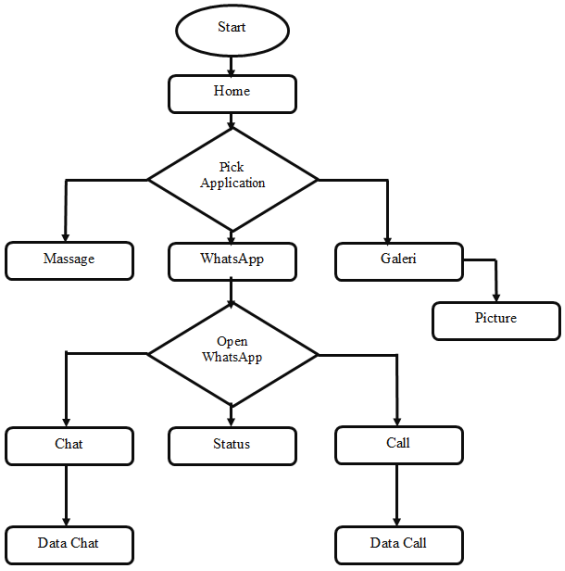

Figure 13. Flowchart

Based on Figure 13, the flowchart starts from opening the WhatsApp application and then selecting the chat and call section, to get data from chats and calls, in order to find out the flow of errors.

4. Conclusion

From the results of the development using the waterfall method in the scenario of a luxury car smuggling crime case, it can be concluded that the method used to develop the journal was successful because in its development the author succeeded in developing it by obtaining relevant digital evidence and more accurate analysis using the latest waterfall method. Future research by building software that can directly detect fraud that occurs in WhatsApp media, without having to detect and analyze further.

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] H. W. F. G. B. S. E. A. Arman Syah Putra, " “A Proposed surveillance model in an Intelligent Transportation System (ITS)”," *1st 2018 Indonesian Association for Pattern Recognition International Conference, INAPR*, 2019.

[3] A. S. Putra, L. H. S. W. Harco , S. A. Bahtiar , T. Agung , . S. Wayan and H. K. Chu-, "Gamification in the e-Learning Process for children with Attention Deficit Hyperactivity Disorder (ADHD)," *Indonesian Association for Pattern Recognition International Conference (INAPR) IEEE*, pp. 182-185, 2018.

[4] I. Yuniasih, T. Agustina, L. Linggariama, A. S. Putra and N. Aisyah, "Factors Affecting The Amount Of Money Circulating In Indonesia," *Journal of Innovation Research and Knowledge*, vol. 1, no. 12, pp. 1735-1748, 2022.

[5] S. Suhardjono, P. Handayani, H. Sugiarto, N. Aisyah and A. S. Putra, "Forensic Analysis Video Metadata Authenticity Detection," *Journal of Innovation Research and Knowledge*, vol. 1, no. 12, pp. 1727 - 1734, 2022.

[6] E. P. Ningrum, R. Vikaliana, S. Rachmawati, N. Joesah, . A. S. Putra and N. Aisyah, "nternal Control System Applied To Online Based Company Accounting Information Systems," *International Journal of Information System & Technology*, vol. 5, no. 6, pp. 754-760, 2022.

[7] R. F. Ramayani, R. Endrekson, H. Purnomo, A. . S. Putra and B. Givan, "The Effect Of Leadership, Salary And Benefits On Employee Loyalty In Export Import Companies," *Journal of Innovation Research and Knowledge*, vol. 1, no. 12, pp. 1759-1766, 2022.

[8] T. . A. Kurniawan, A. S. Putra and . N. Aisyah, "Analysis Search Data Using The National Institute Of Standard And Technology (NIST) Method On Cybercrime," *Journal of Innovation Research and Knowledge*, vol. 1, no. 12, pp. 1767-1774, 2022.

Authors

1st Author
Priyono
Faculty of Engineering and Informatics, Bina Sarana Informatika University
priyono.pyo@bsi.ac.id

2nd Author
Bilal Abdul Wahid
Faculty of Engineering and Informatics, Bina Sarana Informatika University
bilal.baw@bsi.ac.id

3rd Author
Priatno
Faculty of Engineering and Informatics, Bina Sarana Informatika University
priatno.prn@bsi.ac.id

4th Author
Risdiandri Iskandar
Faculty of Industrial Technology, Gunadarma University
ajinurrohman7@gmail.com

5th Author
Ali Akbar
Faculty of Industrial Technology, Gunadarma University
akbarjawas@gmail.com

6th Author
Arman Syah Putra
Faculty of Information System, STMIK Insan Pembangunan
armansp892@gmail.com