Jurnal Elektronik Ilmu Komputer Udayana
Volume 9 No. 3, February 2021

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

Digital Forensic Analysis of Michat Applications on Android as Digital Proof in Handling Online Prostitution Cases

Kadek Dwi Oka Mahendra[a1], I Komang Ari Mogi[a2]

[a]Informatics Department, Faculty of Science and Mathematic, Udayana University
Jimbaran, Bali, Indonesia
[1]Mahendraoka999@gmail.com
[2]Arimogi@cs.unud.ac.id

Abstract

Smartphone technology and the Internet are very popular lately, especially with various features, one of which is social media applications. But behind all that, social media such as MiChat are very vulnerable to becoming a crime facility, one of which is Online Prostitution. They use the "chat with the closest user" feature by uploading a status that can be connected to the surrounding area within a certain distance radius and after connecting the perpetrators and their potential customers will mutually negotiate and transact until they finally have a meeting. In order to eliminate digital evidence in the form of transaction conversations in the message, usually the perpetrator will delete the history of the message which results in the loss of data that can be used as evidence and the perpetrator can avoid legal traps, which ultimately online prostitution will be increasingly prevalent. To follow up on the Online Prostitution activity, it is necessary to do mobile forensics to find evidence which is then useful to be given to the authorities. This study uses the National Institute of Justice (NIJ) method.

Keywords: *Smartphone, MiChat, Prostitution Online, Mobile Forensic, NIJ.*

1. Introduction

The development of the world technology this time is very fast. One form of technology whose development can be directly applied in everyday life is a *Mobile* phone (*smartphone*). Today's *Mobile* phones have many features and various applications, one of the most frequently used applications is the Instant Messaging (IM) application [1]. With instant messaging it is possible to send messages to each other quickly through an internet network intermediary. Based on research conducted by *Simon Kemp* and the team at *Kepios* with the support of partners, namely the *We Are Social* and *Hootsuite* organization entitled "*Essential Digital Data For Every Country In The World*" The total active social media users in Indonesia are 160 million or 59% of the total population in Indonesia, and around 99% percentage of active social media users who access through cell phones [2].

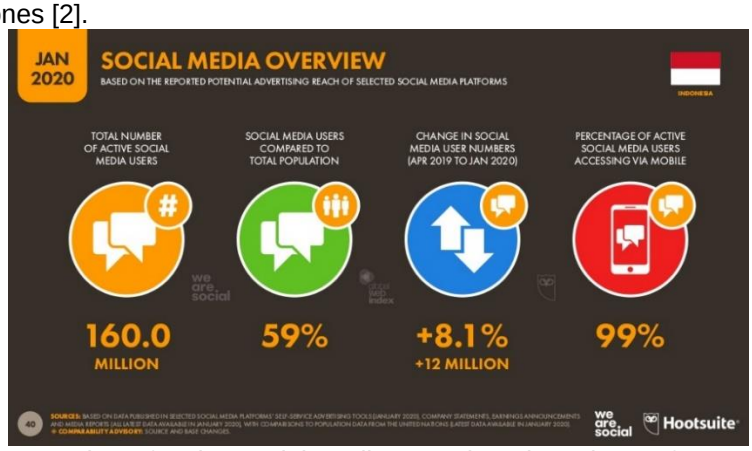


Figure 1. Number of active social media users in Indonesia as of January 2020

One of the instant messaging in Indonesia is *MiChat*. *MiChat* is one of the free messaging apps available on *smartphone*s and was in the Top 5 “Free Chat Apps” on the Google Play Store Indonesia as of October 2018. *MiChat* offers chat features like “Nearby People”, “Chat Trends” and “Moments” for the chat experience more interactive [3].

Figure 2. *MiChat* Social Media Application Logo

However, the features available on *MiChat* are often used to carry out criminal purposes by irresponsible individuals such as *Online Prostitution*. People who abuse this application usually post a status of opening *Prostitution* services and display prices for these business services. One of the cases of *Prostitution* that occurred in Indonesia was the raid on seven *Online Prostitution pimp*s together with a number of women who were suspected of being commercial sex workers in Surabaya by using the *MiChat* messaging application service to peddle themselves [4]. They use the "chat with the closest user" feature by uploading a status that can be connected to the surrounding area within a certain distance radius and after connecting the *pimp*s and potential customers will mutually negotiate and transact in the application.

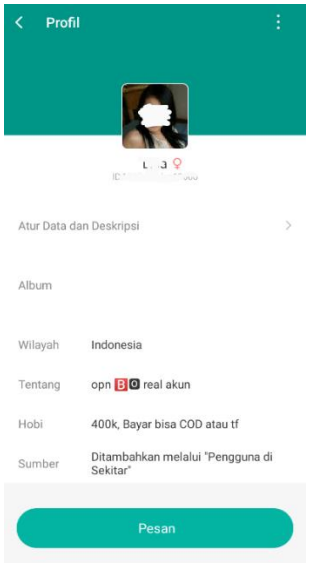


Figure 3. How *Online Prostitution* promote themselves on the *MiChat* application

However, in order to eliminate digital evidence in the form of transaction conversations in the message, usually the perpetrator will delete the history of the message which results in the loss of data that can be used as evidence and the perpetrator can avoid legal traps that eventually *online prostitution* is increasingly rampant. Therefore, digital *forensic* analysis is needed to obtain data and collect valuable deleted information on the *smartphone* of the *prostitution* in the form of a history of conversations and contacts to be used as evidence. For this reason, it is hoped that the research carried out can solve problems and reduce *online prostitution* activities in the *MiChat* application. In *mobile forensics* using the *National Institute of Justice* (NIJ) method and by using the *MOBILedit Forensic Express software* and *SysTools SQLite Viewer*. *MOBILedit Forensic Express* is a tool that investigators use to check *mobile* devices. This *software* is good enough to get phone system information and other information such as contact lists and messages [5]. Meanwhile, *SysTools SQLite Viewer* is a *software* used to view database files compatible with *SQLite.*

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

The previous studies related to this research include:

1. Research entitled “Identifikasi Bukti Digital SKYPE di *Smartphone Android* dengan Metode *National Institute of Justice* (NIJ)” conducted by Muhammad Rizki Setyawan, Anton Yudhana, Abdul Fadlil from Ahmad Dahlan University, in 2019. They acquired one of the instant messenger applications on *Android*, namely SKYPE for handling cybercrime cases using the *National Institute of Justice* (NIJ) method with the help of *software Mobiledit Forensic*s [6].
2. Research entitled “Acquisition of LINE Digital Social Media Evidence Using the *National Institute of Justice* (NIJ) Method” conducted by Gede Pawitradi and I Ketut Gede Suhartana from Udayana University, in 2019. They acquired one of the LINE social media applications on *Android* for handling cyberbullying cases using the *National Institute of Justice* (NIJ) method with the help of *Mobiledit Forensic software* and DB Browser for SQLite [7].
3. Research entitled “Akuisisi Bukti Digital Pada Instagram *Messenger* Berbasis *Android* Menggunakan Metode *National Institute of Justice* (NIJ)” conducted by Imam Riadi, Anton Yudhana, Muhammad Caesar Febriyansah Putra from Ahmad Dahlan University, in 2018. They analyzed the data on the perpetrator's *smartphone* which became digital evidence of crimes indicated by cyberbullying using the *National Institute of Justice* (NIJ) method and with the help of OXYGEN *Forensic software* [8].
4. Research entitled “Analysis *Mobile Forensic*s on Twitter Application using the *National Institute of Justice* (NIJ) Method” conducted by Hijrah Nurhairani and Imam Riadi from Ahmad Dahlan University, In 2019. They analyzed *smartphone* data to search for evidence of crimes that occurred on social media Twitter using the *National Institute of Justice* (NIJ) method and with the help of DB Browser for SQLite *software*, SQLiteManager and Root Explorer applications [9].
5. Research entitled “Analisis Forensik Aplikasi Dropbox pada *Android* menggunakan Metode NIJ pada Kasus Penyembunyian Berkas” conducted by Saleh Khalifah Saad, Rusydi Umar and Abdul Fadlil from Ahmad Dahlan University, in 2020. They analyzed data on the Dropbox application to deal with crime with *smartphone* media evidence using the *National Institute of Justice* (NIJ) Method with the help of the USB Connector Application, Oxygen *Forensic*s, *Mobile* edit *Forensic* [10].

2. Reseach Methods

In this study, it refers to the investigative process used by the *National Institute of Justice* (NIJ) method which serves to explain the stages of the research being carried out so that it is used as a reference for solving problems. This method recommends a basic stage in the *Forensic* process, namely preparation, collection, examination, analysis and reporting. The stages of the *National Institute of Justice* (NIJ) method are described as follows:

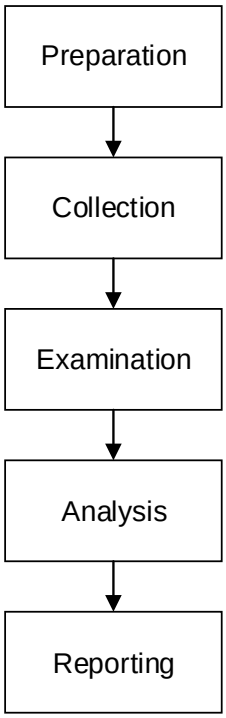


Figure 4. The *National Institute of Justice* (NIJ) method

In the flow chart above, it is explained that the *National Institute of Justice* (NIJ) Method has five basic stages in the *Forensic* process which begins with preparation which is the process of preparing equipment to be used to perform the tasks required in the investigation. Then collection is the process of searching for documents, collecting or making copies of physical objects containing electronic evidence. Then examination wherein the process of making the electronic evidence visible and documenting the content and system, data reduction is done to identify the evidence. After that, the analysis is where the process is the evidence for the examination stage in order to determine the significance and probability value. And the last one is reporting which in this process makes examination records of all cases [11].

3. Result and Discussion

In this study using examples of cases of *Online Prostitution*. In an example of a simulated case where the perpetrator or *pimp* was raided by police disguised as a customer, evidence was obtained from the perpetrator in the form of a *smartphone* with the *Vivo 1606 Y53* brand, which contained the *MiChat* application as a means of promoting self-promotion and transactions. In the *MiChat* application, the perpetrator has an account with an ID, namely "Lisa". As a follow-up, the authorities confiscated the *smartphone* of the prostitute for further investigation. In investigations, Investigators use the *National Institute of Justice* (NIJ) method which has five basic stages in *Forensic*s, namely preparation, collection, examination, analysis and reporting.

3.1 Preparation

In this preparation process, the task is to prepare all the tools used as evidence and the tools used during the investigation process. The tools and evidence used can be seen in the table below.

Table 1. Tools and evidence

No.	Information	Tools and Evidence	Specification
1.	*Hardware*	*Laptop*	*ASUS A456UR Intel Core i5-7200U, Windows 10 64-bit*
2.	*Hardware*	*Smartphone*	*Vivo 1606 Y53 Marshmallow 6.0.1*

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

			Funtouch OS 3.0, already in the *root* condition
3.	*Software*	*Mobiledit Forensic Express*	*Program Version 7.2.0.17975 (64-bit)*
4.	*Software*	*SysTools SQLite Viewer*	*Program Version 3.0*

3.2 Collection

In this process, investigators collect physical data and documentation, and collect data on the suspect's *Smartphone*.

Figure 5. *Smartphone* evidence

The image above is a documentation of physical evidence from a communication device in the form of a *smartphone* with the Vivo 1606 Y53 brand used by the perpetrators to transact *Online Prostitution*. The *smartphone* uses the *Android* Operating System version 6.0.1 or it can be called *Android* Marshmallow which has *MiChat* social media installed, and is in root condition. Furthermore, investigators will retrieve data on the *smartphone* by cloning, this aims to avoid changing data or deleting data which will later become digital evidence.

3.3 Examination

In this process, the investigator checks the data on the *smartphone*. With the help of the *Mobiledit Forensic Express* tool that is already installed on the laptop, if it is connected to the perpetrator's *smartphone*, *Mobiledit* will display the *IMEI* and *IMSI* number information from the *smartphone*, as shown below.

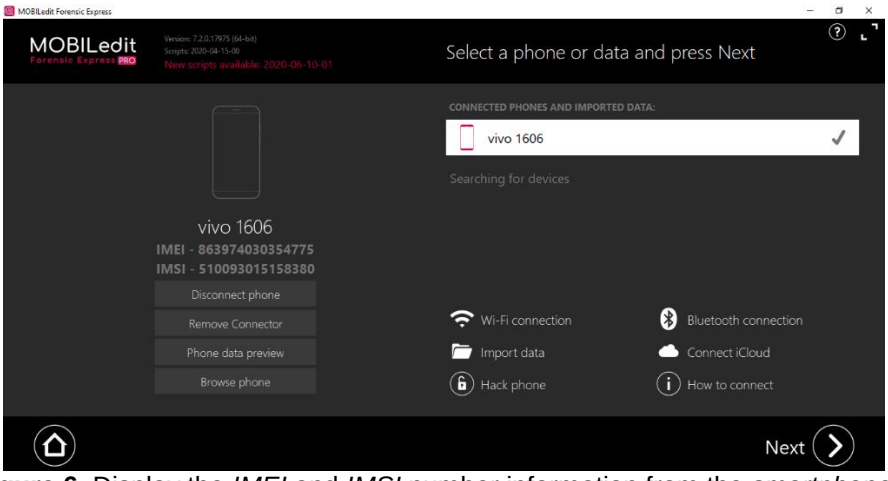


Figure 6. Display the *IMEI* and *IMSI* number information from the *smartphone*

In the examination process, various types of data were obtained from the perpetrator's *smartphone*, and of course *MiChat* social media can also be read, as shown below.

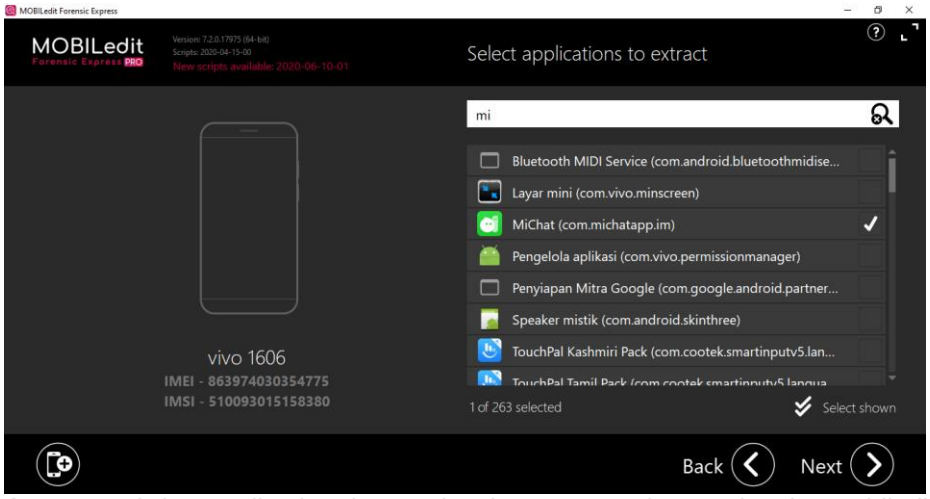


Figure 7. *MiChat* Application data retrieval on a *smartphone* using the *Mobiledit Forensics Express*

Then extract data from the *MiChat* application and obtain various files which will be stored in the laptop storage. Like the picture below.

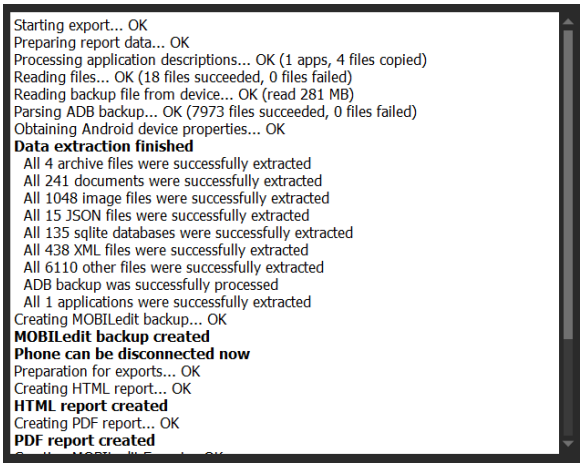


Figure 8. The results of data retrieval on the perpetrator's *Smartphone*

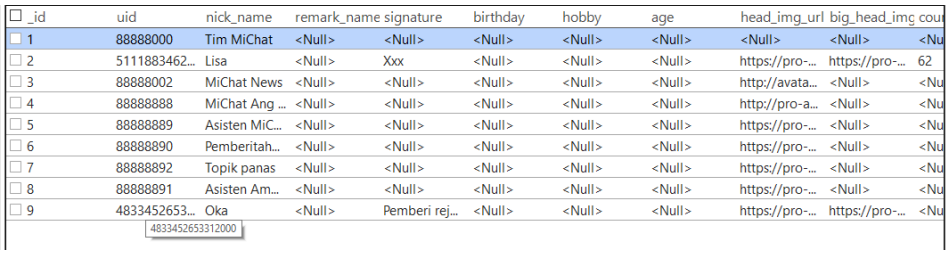
Because the perpetrator uses the *MiChat* social media, further checking is carried out on the files from the *MiChat* social media in the form of a folder with the name com.*MiChat*app.im. Then the contents in the *MiChat* folder (com.MiChatapp.im) were analyzed. From the analysis results found several files in the form of a database with SQLite format. To find out the contents of the database file, *SysTools SQLite Viewer software* is needed for further analysis.

3.4 Analysis

Based on the analysis of the contents of the sub folder and the database from the *MiChat* folder (com.MiChatapp.im), it was found that important data that can be used to support the investigation is a database called "5111883462244352social". From the results of investigations using *SysTools SQLite Viewer*, the database "5111883462244352social" has 22 tables. First, the investigator wants to find out who the contacts were stored in the previous

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

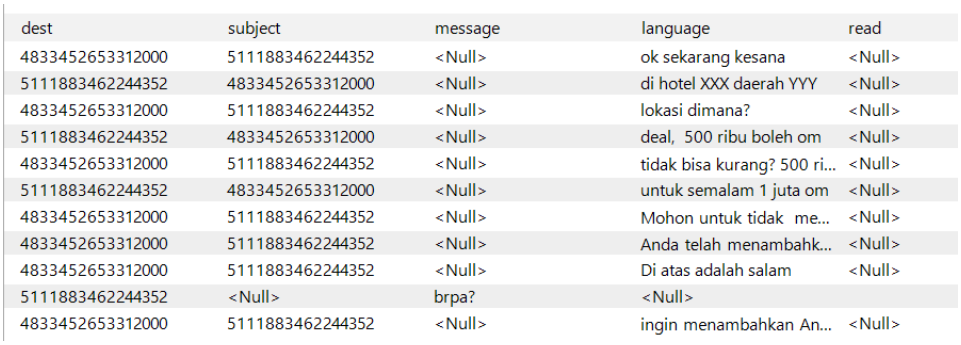
perpetrator's account. So in the *SysTools SQLite Viewer* the investigator opens the "*tb_contacts*" table. In "*tb_contacts*" there are 9 contacts and it appears that there is a contact with the name "Oka" who is suspected of being one of the *Online Prostitution* customers with uid "4833452653312000". Can be seen in the image below.



_id	uid	nick_name	remark_name	signature	birthday	hobby	age	head_img_url	big_head_img	cou
1	88888000	Tim MiChat	<Null>	<Null>	<Null>	<Null>	<Null>	<Null>	<Null>	<Nu
2	5111883462...	Lisa	<Null>	Xxx	<Null>	<Null>	<Null>	https://pro-...	https://pro-...	62
3	88888002	MiChat News	<Null>	<Null>	<Null>	<Null>	<Null>	http://avata...	<Null>	<Nu
4	88888888	MiChat Ang ...	<Null>	<Null>	<Null>	<Null>	<Null>	http://pro-a...	<Null>	<Nu
5	88888889	Asisten MiC...	<Null>	<Null>	<Null>	<Null>	<Null>	https://pro-...	<Null>	<Nu
6	88888890	Pemberitah...	<Null>	<Null>	<Null>	<Null>	<Null>	https://pro-...	<Null>	<Nu
7	88888892	Topik panas	<Null>	<Null>	<Null>	<Null>	<Null>	https://pro-...	<Null>	<Nu
8	88888891	Asisten Am...	<Null>	<Null>	<Null>	<Null>	<Null>	https://pro-...	<Null>	<Nu
9	4833452653...	Oka	<Null>	Pemberi rej...	<Null>	<Null>	<Null>	https://pro-...	https://pro-...	<Nu

Figure 9. Contents of the *tb_contacts* table

Then the investigator investigated further by opening the "*tb_messages*" table to find out traces of the conversation between the *Online Prostitution*. In the table "*tb_messages*" there are 11 traces of conversation between the perpetrator and uid "4833452653312000" which is "Oka" one of the *Online Prostitution* customers. Can be seen in the image below.



dest	subject	message	language	read
4833452653312000	5111883462244352	<Null>	ok sekarang kesana	<Null>
5111883462244352	4833452653312000	<Null>	di hotel XXX daerah YYY	<Null>
4833452653312000	5111883462244352	<Null>	lokasi dimana?	<Null>
5111883462244352	4833452653312000	<Null>	deal, 500 ribu boleh om	<Null>
4833452653312000	5111883462244352	<Null>	tidak bisa kurang? 500 ri...	<Null>
5111883462244352	4833452653312000	<Null>	untuk semalam 1 juta om	<Null>
4833452653312000	5111883462244352	<Null>	Mohon untuk tidak me...	<Null>
4833452653312000	5111883462244352	<Null>	Anda telah menambahk...	<Null>
4833452653312000	5111883462244352	<Null>	Di atas adalah salam	<Null>
5111883462244352	<Null>	brpa?	<Null>	
4833452653312000	5111883462244352	<Null>	ingin menambahkan An...	<Null>

Figure 10. The contents of the *tb_messages* table

In the picture above, there is a conversation between the perpetrator and one of the customers who mutually make an *Online Prostitution* transaction. Furthermore, the results of the analysis can be used as digital evidence for cases of *Online Prostitution* by using the *MiChat* social media application as a forum.

3.5 Reporting

The method used in this investigation is the *National Institute of Justice* (NIJ) method which has 5 basic stages, namely preparation, collection, examination, analysis and reporting. The first thing that was done was to prepare the tools used during the investigation, namely: Laptop, *Smartphone*, *Mobiledit Forensic Express*, *SysTools SQLite Viewer*. The next stage is the collection stage where the investigator collects physical evidence, namely the perpetrator's *smartphone* and then the data is cloned so that data integrity is maintained, as well as carrying out data collection. The third stage is an examination of the data contained in the perpetrator's *smartphone*, which will then be carried out in a deeper analysis. In this investigation, the investigator used two different *software*, namely *Mobiledit Forensic Express* and *SysTools SQLite Viewer*. *Mobiledit Forensic Express* is used when extracting and obtaining data on the perpetrator's *smartphone* and the *MiChat* application folder (com.MiChatapp.im) is obtained. After a more in-depth analysis, an important data that can support the investigation is obtained, namely the "5111883462244352social" database. To open database files, the *SysTools SQLite Viewer software* is used. From the results of the investigation the database has 22 tables. The investigator first checked the contact table and

found 9 stored contacts. Then the investigator checks the table messages to check the conversations of the perpetrator with *Prostitution* customers. From message checking, digital evidence was obtained that it was true that the perpetrator had committed *Online Prostitution* transactions, and later the digital evidence could be presented in court.

4. Conclusion

The purpose of this study is to help solve the problem of *online prostitution* on the *MiChat* social media application by analyzing evidence obtained from online prostitutes by conducting simulations using the *National Institute of Justice* (NIJ) method and research tools in the form of *MOBILedit forensic express software* and *SysTools SQLite Viewer*. Which is expected to be used to carry out forensic analysis on the *MiChat* social media application. The *National Institute of Justice* (NIJ) method consists of 5 basic forensic stages, namely preparation, collection, examination, analysis and reporting. In the preparation process, tools for investigation are prepared. Then in the process of collecting and examining with *MOBILedit forensic express*, important data is obtained that can support the investigation in the form of *MiChat* data (*com.michatapp.im*). Then the data is analyzed further. From the results of the analysis found traces of chat between the perpetrators and their customers. From the traces of the chat, it can be seen that the perpetrator and one of his customers made an *online prostitution* transaction on the *MiChat* application. Furthermore, the results of the analysis can be used as digital evidence which the perpetrators can later account for.

References

[1] Riski, Y. P., Anton, Y., Abdul, Fadil., “Analisis Forensik Aplikasi Kakaotalk Menggunakan Metode National Institute Standard Technology”, SemnasIF, ISSN: 1979-2328, 2018.

[2] Simon Kemp, "DataReportal", 18 February 2020. [*Online*]. Available: https://datareportal.com/reports/digital-2020-indonesia. [Accessed: 07- Okt- 2020].

[3] *MICHAT* PTE. LIMITED, "*MiChat*”, *MiChat*, 2018. [*Online*]. Available: https://www.*MiChat*.sg [Accessed: 25- Sept- 2020].

[4] Trans Media, "CNN Indonesia", 15 Mei 2020. [*Online*]. Available: https://www.cnnindonesia.com/nasional/20200515113308-12-503655/tujuh-muncikari-prostitusi-*Online*-ditangkap-di-surabaya. [Accessed: 07- Okt- 2020].

[5] Imam, R., Sunardi, Sahirudin, “Analisis Forensik Recovery pada *Smartphone Android* menggunakan metode *National Institute of Justice* (NIJ)”, JURTI, Vol.3 No.1, 2019.

[6] Setyawan, M. R., Anton, Y., Fadlil, A., “Identifikasi Bukti Digital SKYPE di *Smartphone Android* dengan Metode *National Institute of Justice* (NIJ)”, Seminar Nasional Teknologi Fakultas Teknik Universitas Krisnadwipayana, 2019.

[7] Pawitradi, G., Suhartana, I. K. G.,“Acquisition of LINE Digital Social Media Evidence Using the *National Institute of Justice* (NIJ) Method”, Jurnal Elektronik Ilmu Komputer Udayana Volume 8, No.2, 2019.

[8] Riadi, I., Anton, Y., Febriansyah Putra, M. C., “Akuisisi Bukti Digital Pada Instagram *Messenger* Berbasis *Android* Menggunakan Metode *National Institute of Justice* (NIJ)”, Jurnal Teknik Informatika dan Sistem Informasi, Volume 4 No. 2, 2018.

[9] Hijrah N., Imam R., “Analysis *Mobile Forensic*s on Twitter Application using the *National Institute of Justice* (NIJ) Method”, International Journal of Computer Applications, Volume 177 – No. 27, 2019.

[10] Saleh K. S., Rusydi U., Abdul F., “Analisis Forensik Aplikasi Dropbox pada *Android* menggunakan Metode NIJ pada Kasus Penyembunyian Berkas”, Jurnal Sains Komputer & Informatika (J-SAKTI), Volume 4 Nomor 2, 2020.

[11] Faiz, M. N., Umar, R., & Yudhana, A. “Analisis Live *Forensic*s Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary”, ILKOM Jurnal Ilmiah, 8(3), 242-247, 2016.

This page is intentionally left blank