CyberSecurity and Digital Forensics e-ISSN: 2615-8442
Vol. 5, No. 2, November 2022, p.60-65

MOBILE FORENSIC IMPLEMENTATION IN MICHAT AND TELEGRAM APPLICATIONS WITH NIST 800-101 FRAMEWORK

Nadia Ayu Isroh Maniar[1], Trihastuti Yuniati[2]

[1, 2]Institut Teknologi Telkom Purwokerto
Email: [1]18102242@ittelkom-pwt.ac.id, [2]trihastuti@ittelkom-pwt.ac.id

Abstract

Social media is a platform for online communication that allows people to interact without being limited by space and time. One of the commonly used applications for criminal activities such as online prostitution is MiChat and Telegram, because these applications are easily accessible and allow users to send photos and videos. Cybercrime evidence can be in the form of electronic and digital evidence. Electronic evidence is the physical form of electronic devices involved in a crime, while digital evidence is documents, history or logs containing data related to the crime. This study examines the implementation of forensic techniques on mobile devices using the MiChat and Telegram applications. The aim is to collect and analyze data that can be used as evidence in an investigation. This study uses the framework of the National Institute of Standards and Technology Special Publication 800-101 Revision 1 and uses FTK Imager and MOBILedit Forensic as assistance tools. The results show that FTK Imager obtained more digital evidence compared to MOBILedit Forensic, and the acquisition of digital evidence on the Telegram application obtained fewer evidences compared to the MiChat application. The successfully obtained digital evidence includes conversation messages, images, videos, and voice notes. and the acquisition of digital evidence on the Telegram application obtained fewer evidences compared to the MiChat application. The successfully obtained digital evidence includes conversation messages, images, videos, and voice notes. and the acquisition of digital evidence on the Telegram application obtained fewer evidences compared to the MiChat application. The successfully obtained digital evidence includes conversation messages, images, videos, and voice notes.

Keywords*: cybercrime, digital forensics, michat, nist, telegram*

1. INTRODUCTION

Socializing online through social media allows people to communicate with each other without being constrained by space and time(Nimda, 2012). Social media has been widely accepted by the community and even now almost all people use social media for school purposes such as sending assignments or discussing with other friends, unlike those who are already working social media can be used to promote their wares or send progress reports on assignments or work done. already done, due to the Covid-19 pandemic so the work must be done Work From Home (WFH). This situation causes the use of social media to increase.

Based on data from We are Social and Hootsuite, there are 202.6 million internet users in Indonesia in January 2021. Meanwhile, there are 345.3 million active cellular networks or 125.6% of the total population, because there are residents who use more from a smartphone to do activities on the internet(Riyanto, 2021). This shows that internet users in Indonesia are very high and many people have more than one device to access the internet. Even though social media has grown and many people use it for socializing, some people also use it for criminal activities.(Mukti, Masruroh and Khairani, 2018). Hinsa Siburian, Head of the National Cyber and Crypto Agency (BSSN), stated that from January to August 2021, Indonesia experienced 888,711,736 cyber attacks.(cnnindonesia.com, 2021). The rise of smartphone, social media and internet users in Indonesia is currently being misused to commit crimes (cybercrime) such as human trafficking, cyberbullying, fraud, extortion, trade in illegal goods, drug trafficking, and many more.(System et al., 2021). This shows that Indonesia is experiencing a lot of cyber attacks and needs to improve cyber security to reduce the risk of such attacks. Smartphones are often used as a tool to commit crimes, such as sending messages containing threats or spreading hoaxes.This shows that the use of technology must be properly monitored and managed to reduce the risk of crimes committed through technology.

The MiChat and Telegram applications are two examples of applications that are misused for online prostitution. This is because this application is easily

accessible and can be used to send photos and videos. According to data from the Indonesian Child Protection Commission (KPAI) there were 35 cases of sexual exploitation, human trafficking and child labor that occurred between January and April 2021. Of the total cases, 60% of cases were carried out via social media, of which 41% of cases used MiChat application(Jayani, 2021). In the crime cases above, it is necessary to have digital evidence from crime cases with social media as evidence in court(Star, Umar and Yudhana, 2020).

Cybercrime evidence can be in the form of physical electronic devices or digital files containing related data. Electronic evidence can be in the form of electronic devices involved in crimes, while digital evidence can be in the form of document files, history, or logs that contain information related to crimes.(Riadi, Umar and Nasrulloh, 2018). This study uses the MOBILedit Forensic Express application and the FTK Imager tool as tools to search for digital evidence.

Based on this background, the authors conducted a study entitled "Implementation of Mobile Forensics in MiChat and Telegram Applications with the Nist 800-101 Method". The MiChat and Telegram applications were chosen because based on data from KPAI, the MiChat application is the online media most widely used in crimes of sexual exploitation and human trafficking, while Telegram is one of the instant messenger applications most often used by Indonesians to exchange communications. This research is expected to produce a comparison of the amount of evidence obtained between the MiChat and Telegram applications using the National Institute of Standards and Technology method.

2. RESEARCH METHODS

2.A. Method

The National Institute Of Standards Technology (NIST) method, is a framework that is often used because NIST regulates standard guidelines and best practices in managing risks related to all forms related to science and information technology(View of Implementing the NIST Method for Denial of Service (DOS) Attack Analysis on Internet of Things (IoT) Devices, no date). This method is used to describe how step by step in detail and systematically, so as to solve existing problems. The purpose of this method is used to defend the results obtained so that they can be used as legal evidence(Ahmadi, Akbar and Mandala Putra, 2021). The stages in the National Institute of Standards And Technology (NIST) Special Publication 800-101 Revision 1 method are shown in Figure 1(Study et al., 2021):

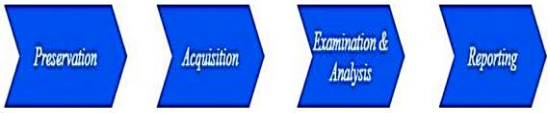

Figure 1. NIST Special Publication 800-101 Revision 1 method

1. *preservation*

   At this stage what is being done is collecting data from the media which will be identified during research and labeling while still following procedures in maintaining data authenticity.
2. *Acquisition*

   This stage is the stage of collecting data when it is processed using forensic methods automatically or manually, as well as assessing and removing the data as needed while maintaining data integrity.
3. *Examination & Analysis*

   At this stage the stages of inspection and analysis of data are carried out in accordance with the rules so as to obtain data to be used as evidence related to the case.
4. *reporting*

   At this stage the results of the investigation obtained from the investigation contain the results of the analysis of reported evidence so that this evidence can assist in the investigation process to find the suspect.

2.B. Tools and materials

The software used in this study are:

1. *MiChat*version 1.4.118 and Telegram version 8.2.7 as social media applications used for online prostitution transactions
3. *FTK Imager*version 4.5.0 and MOBILedit Forensic Express version 7.4.1 (64 bit) as tools for digital evidence acquisition using digital forensic techniques

To be able to run the software mentioned above, hardware with certain specifications is required. The hardware used in this study are:

1. Laptop with Intel Core i5 processor, Windows 64bit OS, used for cloning and acquisition of digital evidence using FTK Imager tools version 4.5.0 and MOBILedit Forensic version 7.4.1 (64 bit)
2. USB cableused to transfer data from cellphone clones to laptops
3. *Flashdisk*to save cloned data
4. OPPO A37 cellphone as a device used by pimps in scenarios of online prostitution crimes using the MiChat and Telegram applications
4. WIKO HARRY cell phoneas a device used by prostitutes in scenarios of online prostitution crimes using the MiChat and Telegram applications
5. OPPO A3S mobile phoneas a device used by customers in scenarios of online prostitution crimes using the MiChat and Telegram applications

2.C. Data collection

The data source used in this study is data from documentation of scenario simulations that have been made by researchers to serve as digital evidence. The objects to be used in this study are conversation history, voice notes, pictures, and videos. The data that will be collected for this research is only done once, but if the data has not been found, the data collection will continue until the desired digital evidence is found. Figure 2 is a scenario that will be carried out in the study.

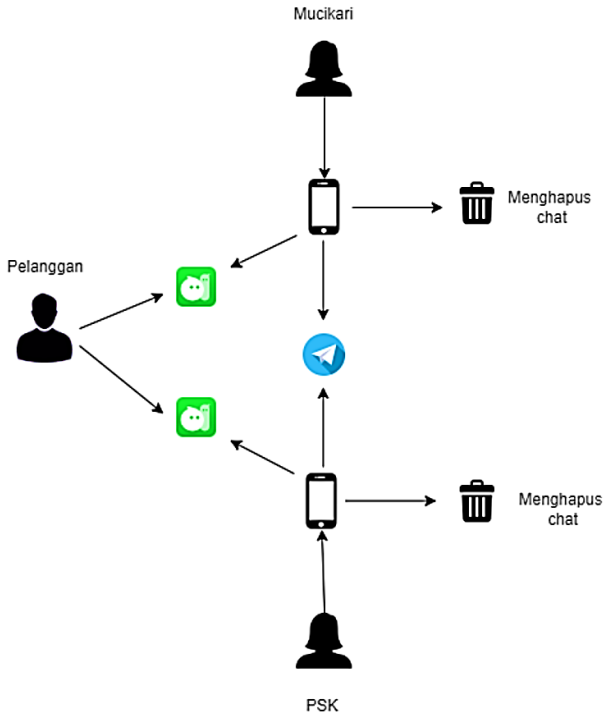

Figure 2. Data Collection Simulation Scenario

The explanation of the scenario flow shown in Figure 2 is as follows:

1. Pimps communicate with customers through the MiChat application
2. Pimps provide information to customers about prostitutes to be employed
3. After an agreement is obtained between the pimp and the customer, the pimp then informs the prostitute via the Telegram application that there will be someone using their services.
4. Pimps provide customer contact to CSWs
5. PSK communicates with customers using the MiChat application
6. Pimps, prostitutes and customers deleted all chat messages on the MiChat and Telegram apps to destroy evidence
7. An investigation and investigation was carried out to obtain digital evidence on the pimp's cell phone (OPPO A37) in the MiChat and Telegram applications

3. RESULTS AND DISCUSSION

3.A. *preservation*

In the first stage of NIST 800-101, namely the preservation stage, cellphones or evidence used by pimps, namely the OPPO A37 cellphone, will be secured for the identification and labeling process. The cell phone evidence was then isolated by putting it in airplane mode and turning it off so it could not be accessed and modified by unauthorized parties prior to the investigation.

3.B. *Acquisition*

In the next NIST 800-101 stage, namely the acquisition stage, the data contained on the mobile device was taken forensically using FTK Imager tools version 4.5.0 and MOBILedit Forensic Express version 7.4.1. The cellphone device that is evidence is in a non-root condition to maintain the integrity of the evidence. Table 1 shows the information on the OPPO A37 cellphone used by the pimps who made the acquisition.

Table 1. OPPO A37 Mobile Phone Device Information

Mobile Device Information	
Phone Device Owner Name	D*** Y******
Phone Device Name	OPPO A37
Model Number	A37
Operating system	Android 10
IMEI	865**********
***Memory*external**	There is
SIM Card	There is
Password	There is

Based on Table 1 it is known that the device to be used for investigation is in a non-root condition and has external memory and a SIM card. In order to get data on a cellphone with non-root conditions, a data cloning is carried out where the cellphone transfers the data via USB to the laptop and then transfers it to the flash drive. Figure 3 is the location for cloning OPPO A37 cellphone data stored on the LOCAL DISK (F:), this data will later be used as testing material in non-root conditions.

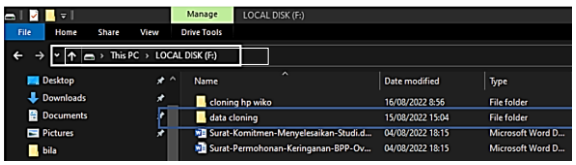

Figure 3. Cloning Data on Flashdisk

3.C. *Examination & Analysis*

In the third stage of NIST 800-101, namely Examination & Analysis, a search for digital evidence was carried out using forensic techniques using two tools, MOBILedit Forensic Express and

FTK Imager. The digital evidence in question is conversation messages between pimps and customers and PSK conversation messages with customers from pre-made scenarios. Digital evidence that was successfully or unsuccessfully obtained using forensic techniques using the two tools is then recorded, so that further evidence can be obtained from the Telegram and MiChat applications using MOBILedit Forensic Express and FTK Imager.

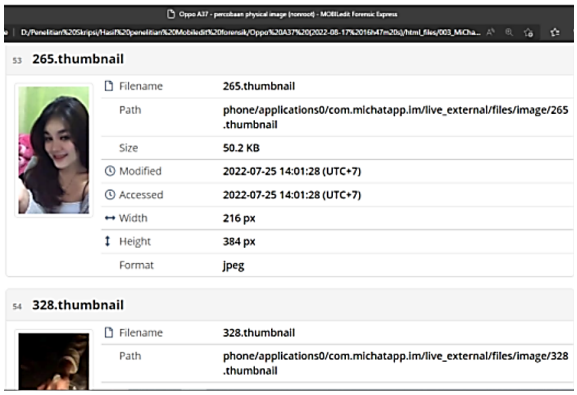

Figure 4. Digital evidence in the form of photos on the MOBILedit Forensic tools

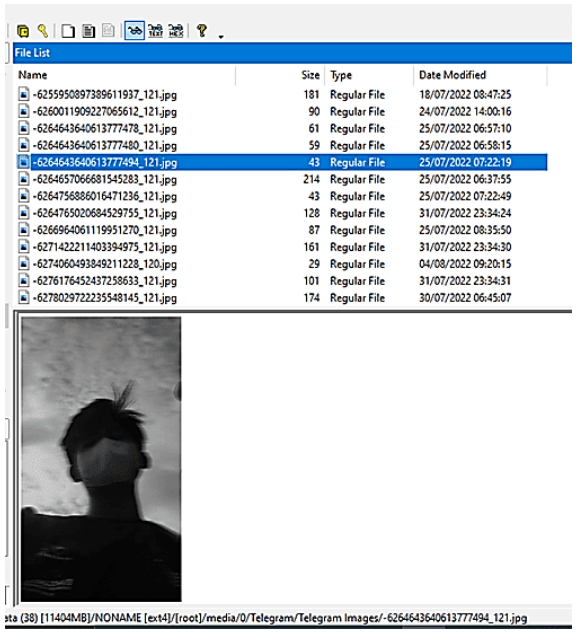

Figure 5. Digital evidence in the form of images on the FTK Imager tools

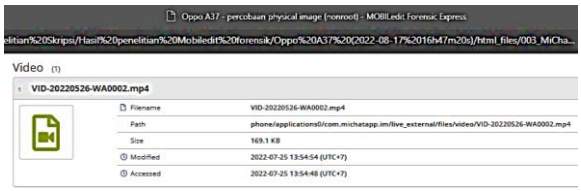

Figure 6. Digital evidence in the form of video on the MOBILedit Forensic tools

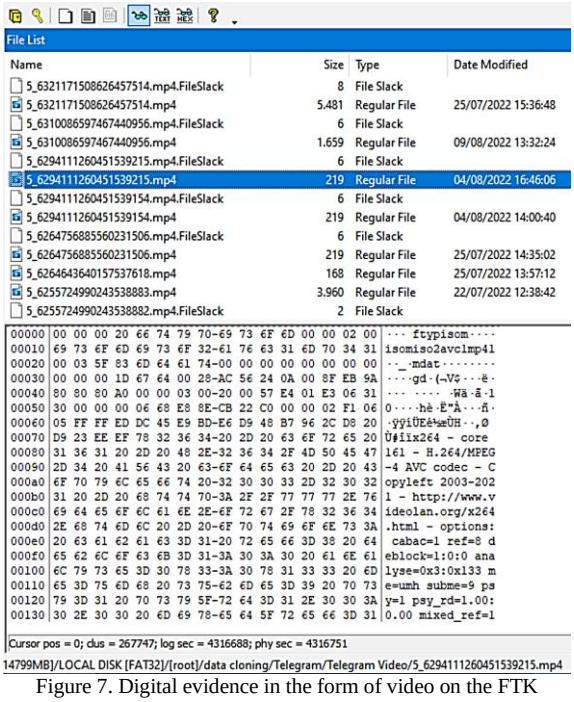

Figure 7. Digital evidence in the form of video on the FTK Imager tool

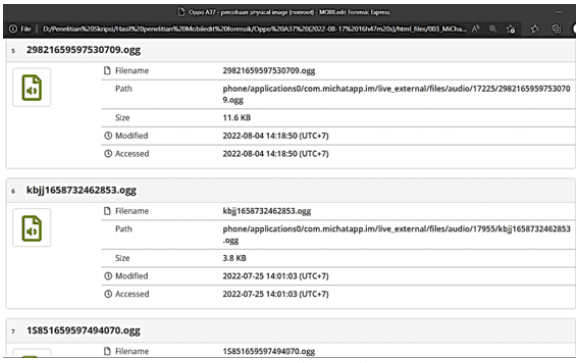

Figure 8. Digital evidence in the form of voice messages on the MOBILedit Forensic tools

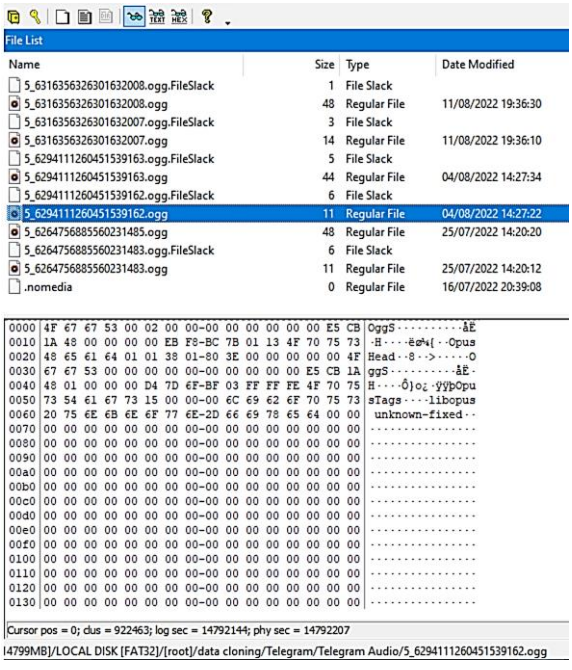

Figure 9. Digital evidence in the form of a voice message on the FTK Imager tool

3.D. *reporting*

Reporting is the last stage of NIST 800-101. After examining and acquiring digital evidence using the MOBILedit Forensic Express and FTK Imager tools, the next step is to compile a report on the results of the analysis that has been found as a whole. In general, the results of acquiring digital evidence in the MiChat and Telegram applications using the MOBILedit Forensic Express and FTK Imager tools are shown in Table 2.

Table 2. Results of acquisition of digital evidence in the MiChat and Telegram applications with the MOBILedit Forensic Express and FTK Imager tools

Evidence	FTK Imager		MOBILedit Forensic Express	
	MiChat	Telegram	MiChat	Telegram
Text	X	X	X	X
Picture	V	V	V	V
Videos	V	V	V	X
Voice notes	V	V	V	X

Information:

X = not found

V = found successfully

4. CONCLUSIONS AND RECOMMENDATIONS

4.A. Conclusion

Based on the results of digital forensic research that has been carried out by applying the National Institute of Standards And Technology (NIST) Special Publication 800-101 Revision 1 framework using the MOBILedit Forensic and FTK Imager tools for the MiChat and Telegram applications, it can be concluded that:

1. The results of the acquisition using both MOBILedit Forensic and FTK Imager tools only managed to find digital evidence in the form of images, videos, and voice notes while messages in the form of text conversations were not found.
2. Of the two tools used in this study, overall the FTK Imager tool was able to obtain more digital evidence results than MOBILedit Forensic.

4.B. Suggestion

Suggestions for further research are:

1. Acquiring digital evidence in applications other than MiChat and Telegram so that the security level of each application can be determined.
2. Using tools other than MOBILedit Forensic and FTK Imager to determine the level of acquisition that each tool can obtain.

BIBLIOGRAPHY

AHMADI, AHWAN, AKBAR, T. AND MANDALA PUTRA, H. 2021. Perbandingan Hasil Tool Forensik Pada File Image *Smartphone* Android Menggunakan Metode Nist, *JIKO (Jurnal Informatika dan Komputer)*, 4(2), pp. 92–97. doi: 10.33387/jiko.v4i2.2812.

BINTANG, R. A., UMAR, R. AND YUDHANA, A. 2020. Analisis Media Sosial Facebook Lite dengan *tools* Forensik menggunakan Metode NIST, *Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto)*, 21(2), p. 125. doi: 10.30595/techno.v21i2. 8494.

CNNINDONESIA.COM. 2021. *BSSN: Ada 888 Juta Serangan Siber Sepanjang 2021*, *www.cnnindonesia.com*. Available at: https://www.cnnindonesia.com/nasional/20210913131225-12-693494/bssn-ada-888-juta-serangan-siber-sepanjang-2021 (Accessed: 12 November 2021).

JAYANI, D. H. 2021. *Kasus Prostitusi Anak Paling* Banyak *Terjadi lewat Aplikasi MiChat*, *databoks.katadata.co.id*. Available at: https://databoks.katadata.co.id/datapublish/2021/06/03/kasus-prostitusi-anak-paling-banyak-terjadi-lewat-aplikasi-michat (Accessed: 7 November 2021).

MUKTI, W. A., MASRUROH, S. U. AND KHAIRANI, D. 2018. Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter pada *Smartphone* Android, *Jurnal Teknik Informatika*, 10(1), pp. 73–84. doi: 10.15408/jti.v10i1.6820.

NIMDA. 2012. *Apa itu Sosial Media*, *http://www.unpas.ac.id/*. Available at: http://www.unpas.ac.id/apa-itu-sosial-media/ (Accessed: 7 November 2021).

RIADI, I., UMAR, R. AND NASRULLOH, I. M. 2018. Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute of Justice (NIJ), *Elinvo (Electronics, Informatics, and Vocational Education)*, 3(1), pp. 70–82. doi: 10.21831/elinvo.v3i1.19308.

RIYANTO, A. D. 2021. *Hootsuite (We are Social): Indonesian Digital Report 2021*, *andi.link*. Available at: https://andi.link/hootsuite-we-are-social-indonesian-digital-report-2021/ (Accessed: 7 November 2021).

RIADI, I., UMAR, R. AND SYAHIB, M. I. 2021. Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode Nasional Institute of Standards and Technology (NIST), *Jurnal Resti*, 1(10), pp. 45–54.

MUSHLICH, M.M.A.S., IZZUDDIN, M.A., AND RIDWAN., M. 2021. Analisis Kinerja

Aplikasi Forensik Open-Source Pada Ponsel Cerdas Berbasis Android Dalam Mendapatkan Bukti Digital, *Jurnal Inovasi Informatika Universitas Pradita (JII)*, 6(2), pp. 86-97. doi: https://doi.org/10.51170/jii.v6i2.175

ARSADA. L., AND MUSLIM. A. 2021. Penerapan Metode NIST untuk Analisis Serangan Denial of Service (DOS) pada Perangkat Internet of Things (IoT), *Jurnal Ilmiah KOMPUTASI*, 20(2), pp. 275-281.