Cybercrime Data Search Fraud Case on Mobile based MiChat Service

Dimas Amirul Mu'minin
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT

The development of software such as Smartphones in this era is very fast along with technological development. Social media is the most popular technology today, one of which is MiChat. The search feature for nearby users on MiChat presents many users who can bring up cybercrime, pornography,gambling online, fraud and cyberbullying. This research uses the method of the National Institute of Standards and Technology (NIST) to uncover evidence of fraud on the application MiChat. National Institute of Standards and Technology (NIST) is a method with four stages, namely collection, examination, analysis, and reporting. This research begins with the stages of collecting, examining, analyzing, and reporting using two Smartphones with different conditions, namely Smartphones with conditions root and not rooted. The results of this study are in the form of proof with the condition that the Smartphone has been rooted and the Smartphone has not been rooted. The condition of the smartphone that has been rooted has found evidence in the form of account information MiChat, pictures and profile photos between the perpetrator and the victim, while on the Smartphone that is not rooted the evidence is not found at all but is used to compare the smartphone of the perpetrator. Evidence in the form of media data obtained from Smartphone rooted with a forensic success rate of more than 50% proves that there has been an act of fraud between the perpetrator and the victim and forensics carried out on a smartphone has succeeded in recovering the evidence needed to prove the fraud.

Keywords

Forensic, MiChat, Smartphone, NIST

1. INTRODUCTION

Technological developments in Indonesia are growing rapidly in everyday life, where the internet is a necessity for some people[1].The rapid development of technology has brought convenience and other advantages, the internet is also a problem, namely crime in cyberspace or cybercrime which is increasingly diverse. The rapid development of this technology is followed by the development of software such as social media, now there are many social media services such as MiChat, Instagram, Twitter, and Whatsapp. Almost everyone from all walks of life has a social media application, because social media is used for various needs, such as for communicating, selling, and entertainment facilities[2].

Smartphonesand the internet are very popular lately, especially with various features, one of which is social media applications. But behind it all, there are social media like MiChat that are very vulnerable to being a crime facility. This has the potential for cybercrime such as online fraud or extortion and other crimes[3].This study aims to restore deleted data in the form of data on smartphone deviceswhich are evidence to prove cases of online fraud onservices MiChat[4]. Utilization of digital forensic knowledge in analyzing a smartphone is needed, especially in terms of digital investigations[5].

1.1 Study Literature

1.1.1 Previous Study

Imam Riadi, Anton Yudhana, and Muhammad Caesar Febriansyah Putra (2017) conducted a study entitled "Analysis of Recovery for Digital Evidence Instagram Messengers Using theMethod National Institute of Standard and Technology (NIST)". This study aims to collect evidence in the form of (Messages and Pictures) from smartphones used by perpetrators to send pornographic content to victims. Themethods National Institute of Standards and Technology (NIST) used in the investigation process are collection, examination, analysis, and reporting. This stage is carried out using several tools used in the investigation process in cases of cyber pornography on theapplication Instagram.

Rusydi Umar, and Sahiruddin (2019) conducted a study entitled “Method NIST for Forensic Analysis of Digital Evidence on Devices Android". This study found digital evidence in the form of contact data, call logs and messages that have been deleted on smartphones, so it can be concluded that recovery with the tool Wondershare only reaches 30%, while the results of recovery with oxygen forensics reach 73% of deleted data can be restored. Thus, the data recovered from digital evidence with the tool is oxygen highly recommended as evidence in proving criminal cases in court.

Riski Yudhi Prasongko, Anton Yudhana, and Abdul Fadil (2018) conducted a research analysis entitled “Forensic Analysis ofApplications KakaoTalk Using theMethod National Institute Standard Technology (NIST). This research uses the method NIST and research tools that are expected to be used to perform forensic analysis on the application KakaoTalk. Then during the process of removing digital evidence from the application KakaoTalk ,required rooting on the Android smartphone is. Digital evidence is expected from the appointment process and forensic analysis can help the process of investigating a digital crime.

Tayomi Dwi Larasati, and Bekti Cahyo Hidayanto (2017) conducted a study entitled "Analysis of Live Forensics for Comparison ofApplications Instant Messenger on theOperating System Windows 10". This research was conducted for applications, Instant Messenger popularnamely Facebook, Line Messenger, and Telegram on theplatform Windows 10. From the analysis, we find out which applications are easy and difficult to obtain data as digital evidence. Scenario testing was carried out by experimental means in the form of ordinary conversation data and deletion of messages or conversations. Using Winhex and Belsoft Evidence Center tools that are used to analyze digital data.

Moh. Riskiyadi (2020) conducted a study entitled "Forensic Investigation of Digital Evidence in Revealing Cybercrime". The results of this study indicate that the use of thetools is FTK Imager and Autopsy able to acquire and analyze permanently deleted files and the use of passwords on flash with the drivesBitLocker Drive Encryption Tool, both tools cannot acquire and analyze permanently deleted or reformatted files. These studies are the reference that forms the basis for conducting research[6].In carrying out the removal of evidence or acquisitions on the application Instant Messenger, some previous research did not apply the scenario of the disappearance or deletion of evidence first. Meanwhile, this research will acquire digital evidence with the scenario of the disappearance or deletion of evidence from the conversation of the perpetrator first. Theapplication MiChatwas chosen because this application is being loved because it can search for users using features around users in near and far distances. This study aims to prove whether digital evidence of criminals using the application MiChatreacquired that has been removed or deleted can be used using forensic tools and the framework of the method National Institute of Standards and Technology (NIST).

1.1.2 Digital Forensics

Digital forensics is a part of science that involves returning to the original state and investigation of things found in digital devices, related to computer crimes[7]. Digital forensics is a newly developing field but is growing rapidly in line with the rapid use of information technology. Various sciences and tools have been developed to facilitate investigators in collecting data and assembling it to prove crimes that have occurred. As a new science, of course, it still takes time to reach maturity. One of the problems faced by digital forensics is the rapid development of digital science and technology. Mastery of this rapidly developing technology is a challenge for digital investigators and law enforcement[8]. Efforts to increase understanding and abilities must continue to be improved[9].

1.1.3 Forensics Mobile

Mobile forensics is a branch of digital forensic[10]relating to the recovery of digital evidence or data from devices, mobile but may be associated also with a digital device that has an internal memory and communication skillsdevice. After the cybercrime occurs the criminal leaves a trace which indicates some critical information needed to prove the characteristics of that criminal like the attack time, and the date and where it happened and the tool used, the investigatorsneed tools to match between the criminal and the cybercrime using evidence[11]. Mobile forensics is forensics where data is taken from smartphones, the results of which can be used as evidence. The digital forensic process is carried out to look for digital evidence that can be recognized and used as legal evidence in the legal realm[12]. This evidence can be used as a basis when investigating a case by law enforcement agencies. There is a lot of evidence that can be extracted from cell phones including contact numbers, logs, calls,messages, sms, audio files, emails and internet history[13].

1.1.4 Digital Evidence

Evidence is information stored or transmitted in binary form that can be relied upon in court. Especially for digital evidence related to mobile devices such as smartphones, it can be found in call history, phonebook, sms and mms, photos, audio, video and others. Digital evidence is generally related to digital crimes such as crimes that use social media as a place to commit crimes, so digital evidence is used to assist in prosecuting all types of digital crimes[14].

1.1.5 MiChat

MiChat is one of the instant messaging applications in Indonesia, MiChat applications is one of the free messaging applications available on smartphones and is included in the Top 5 "Free Chat Applications" on the Google Play Store Indonesia as of October 2018. MiChat offers chat features such as "Neighbourhood Users", “Trending Chat”, and “Multimedia Messaging”. Currently Social media is widely used online for various purposes, be it for promotional purposes, interacting with people in various parts of the world or just sharing their daily lives. Social media is also increasingly widespread and increasing in number, in Indonesia itself has a lot of social media which later became popular and widely used. MiChat is one of the many social media sites that can be downloaded for free in Indonesia.

1.1.6 Cybercrime

Cybercrime can occur in various electronic devices, such as android smartphones[15].Cybercrime is a crime that uses information technology as a crime target, and digital forensics is basically, answering the questions: when, what, who, where, how and why related to digital crime[16]. The emergence of cases of internet crime or cybercrime in Indonesia, such as intrusion on the target site can cause abnormal conditions on the victim's site, credit card break-ins and trade fraud online (e-commerce), and defamation carried out through online media or social networks. The rise of cases cybercrime has become a serious crime, so that the government, especially law enforcement officers, must be able to balance its technical capabilities to be able to uncover and deal with the perpetrators in the event of a case cybercrime and most importantly the ability to be able to prosecute perpetrators cybercrime by preparing the right and firm legal umbrella so that able to ensnare and punish the perpetrators of cybercrime.

1.1.7 National Institute of Standard Technology

The National Institute of Standard Technology stage is a forensic stage that has standard policies and work guidelines to ensure each investigator follows the same workflow so that work is documented and the results can be repeated and can be maintained. So that the research flow is known in a structured manner and can be a reference in completing systematic research, then based on the research method, a forensic work step is made which is used to describe the stages and steps of the research to be carried out without reducing the process that has been proposed by the researchermethod NIST[17].

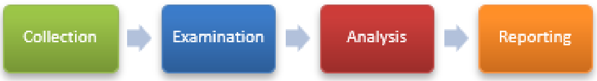


Figure 1. Stage of NIST Method

Explanation of the stages and steps in the NIST method in Figure 1 are as follows:

1. Collection
   Identify, label, record, and retrieve data from relevant data sources.
2. Examination

Perform processing of data collected automatically or manually, and ensure that the data obtained in the form of digital evidence is in accordance with that obtained at the scene of a computer crime, digital evidence needs to be validated files on the existing digital evidence.

3. Analysis
   Analyzing the examination of evidence technically and legally to obtain useful information on digital evidence and can be accounted for scientifically and legally.
4. Reporting
   Reporting is carried out after obtaining digital evidence from the analysis data examination process which includes a description of the actions taken, an explanation of the tools, an explanation of the methods used and providing recommendations to improve policies, procedures, equipment and other aspects of the forensic process[18].

2. METHODOLOGY

2.1 Research Scenario

In this study, the smartphone is already rooted. The research design begins by creating an engineering scenario that is run to obtain digital evidence[19]. In this study, a complete scenario is made with the activities carried out on the application MiChat. In the scenarioit is explained between the perpetrator and the victim using a Smartphone interacting with the service MiChat where the perpetrator uses the nearest search feature to find the victim who will be deceived. After communicating, the perpetrator asked the victim to meet somewhere.

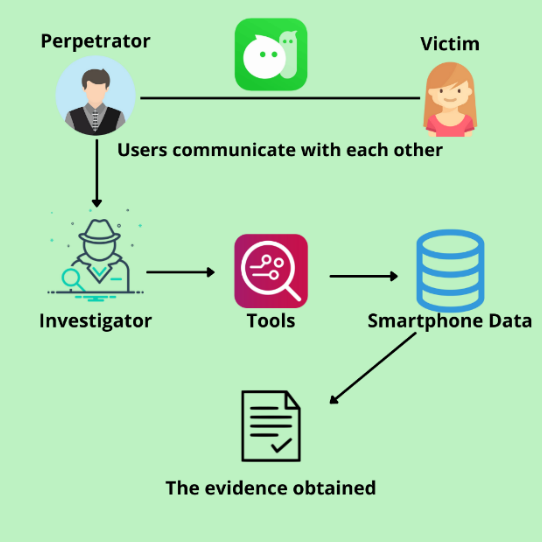


Figure 2. Flow of the Case Scenario on MiChat

The Figure 2 shows investigation process is usually focused on simple data such as call data, and communications such as email or sms, as well as data that has been deleted from storage media smartphones. The researcher then conducted a search for evidence with data recovery on the smartphone perpetrator'susing thetools MOBILedit Forensic Express, Autopsy and DB Browser. Data recovery is a process to restore data from lost, damaged, or inaccessible conditions to a normal initial condition[20].

2.2 Research Stages

Research stages is a process where the investigator will carry out the forensic process with the stages listed in the method NIST. The steps or stages used in this study use the National Institute of Standards and Technology (NIST) stages which have four stages, namely Collection, Examination, Analysis, and Reporting.

2.2.1 Collection

Collection is the initial stage of the search for digital evidence where smartphones are used for forensic and documentation needs. Evidence incases is cybercrime divided into two criteria, namely electronic evidence and digital evidence[21]. This stage collects, identifies, records or retrieves data from relevant data sources according to procedures to maintain data integrity. The evidence proposed is two smartphone devices. To keep the evidence original and undamaged, maintaining data integrity can be done by isolating physical evidence and making backups in the form of cloning or image files of the evidence[22]. The smartphone used is the one written as the smartphone perpetrators and the smartphone victim's, in table 1 it can be seen the results of the documentation of the evidence specifications secured by the authorities then with the help of a USB cable used to be able to obtain data on both smartphones.

Table 1. Physical Evidence Found

No	Name	Photo Smartphone	Description
1	Smartphone 1		*Samsung Galaxy Grand Prime* used by the perpetrator
2	Smartphone 2		*iPhone 6s* used by a victim
3	data cable usb		connecting cable android
4	data cable lightning		connecting cable iPhone

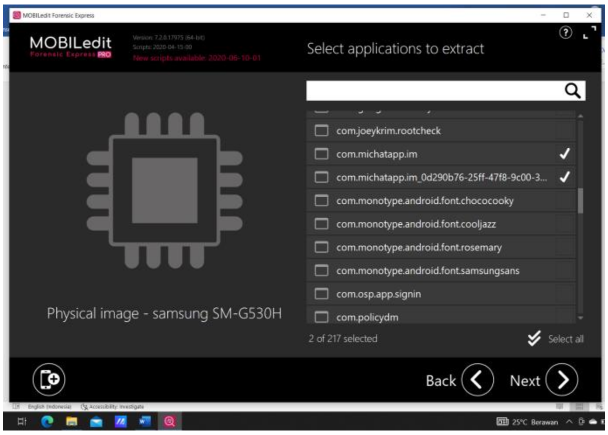
Table 1 is a table that displays documentation of physical evidence found at the crime scene which is then collected by the police and handed over to investigators.

2.2.2 Examination

This examination stage is an advanced stage for data acquisition in the form of digital evidence from the evidence found in the previous table on these two smartphones . Later, data acquisition will be carried out using the MOBILedit Forensic Express, Autopsy Tools and DB Browser to read any data that can be obtained on the smartphone of the perpetrator and victim. These tools embody the techniques and procedures for producing ongoing reconstructions of events, to help digital forensics investigators create lists of evidence that can dictate information about innocent or guilty suspects[23].

2.2.2.1 MOBILedit Forensic Express

First open the MOBILedit Forensic Express tool, then the investigator chooses application analysis to extract application data on the smartphone[24], the application to be extracted is MiChat, by running a checklist of data stored in the folder com.michatapp.im, as shown in figure 3. a smartphone is rooted connected to a PC/Laptop using cable usb to perform the data acquisition process with thetool MOBILedit Forensic Express[25]. If connected, the display on thetool MOBILedit Forensic Express will appear as shown in Figure 3:



Version: 7.2.0.17975 (64-bit)
Scripts: 2020-04-15-00
New scripts available: 2020-06-10-01

Select applications to extract

Physical image - samsung SM-G530H

- □ com.joeykrim.rootcheck
- □ com.michatapp.im ✓
- □ com.michatapp.im_0d290b76-25ff-47f8-9c00-3... ✓
- □ com.monotype.android.font.chococooky
- □ com.monotype.android.font.cooljazz
- □ com.monotype.android.font.rosemary
- □ com.monotype.android.font.samsungsans
- □ com.osp.app.signin
- □ com.policydm

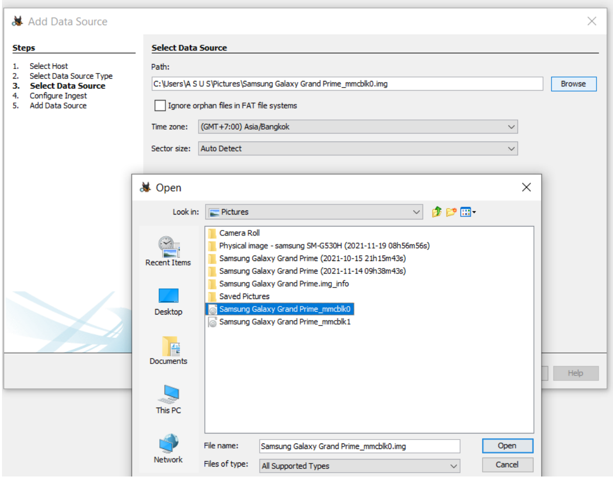
2 of 217 selected

Figure 3. Acquisition of MOBILedit Forensic Express

Figure 3 shows that acquisition was smartphone carried out using the tool MOBILedit Forensic Express which later the data obtained will be continued using the Autopsy tool.

2.2.2.2 Autopsy

In the Autopsy tool, the data acquisition process smartphone perpetrator'scannot be used directly, but uses the results of data acquisition by the MOBILedit Forensic Express tool which is useful for completing the acquisition of strong digital evidence.



Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Path: C:\Users\A S U S\Pictures\Samsung Galaxy Grand Prime_mmcblk0.img

□ Ignore orphan files in FAT file systems

Time zone: (GMT+7:00) Asia/Bangkok

Sector size: Auto Detect

Open

Look in: Pictures

- Camera Roll
- Physical image - samsung SM-G530H (2021-11-19 08h56m56s)
- Samsung Galaxy Grand Prime (2021-10-15 21h15m43s)
- Samsung Galaxy Grand Prime (2021-11-14 09h38m43s)
- Samsung Galaxy Grand Prime.img_info
- Saved Pictures
- Samsung Galaxy Grand Prime_mmcblk0
- Samsung Galaxy Grand Prime_mmcblk1

File name: Samsung Galaxy Grand Prime_mmcblk0.img

Files of type: All Supported Types

Figure 4. Autopsy Acquisition

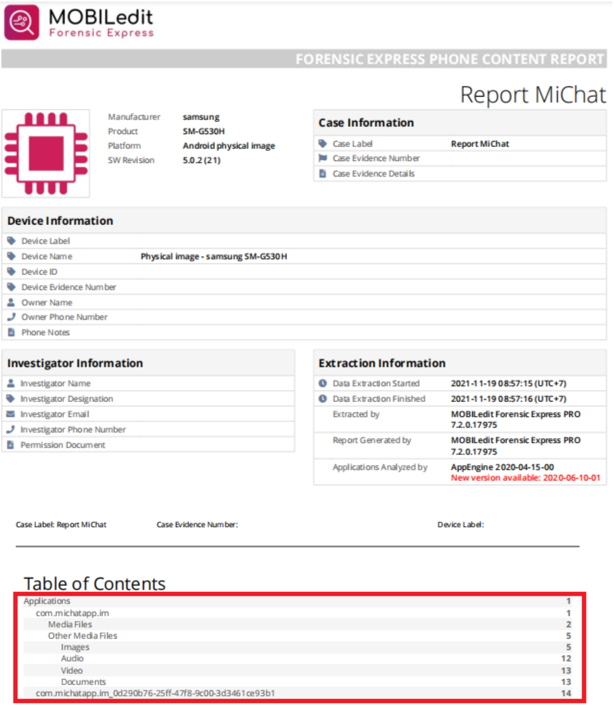
Figure 4 shows how the data acquisition process in the Autopsy tool begins by entering the data acquisition results from the previous process.

2.2.3 Analysis

At this stage of analysis , the data that has been obtained in the previous stage, namely examination, is to ensure that the data obtained are in accordance with the results desired by the investigator, namely the evidence found in accordance with what was submitted by the victim. Analysis of digital evidence includes the collection of important digital data and reading of digital evidence[26].

2.2.3.1 Analysis by MOBILeditForensic Express

Results examination on a smartphone in the root and then displayed by opening the report file in the folder of acquisitions that use MOBILedit Forensic Express as shown in Figure 5, which shows the results specifications smartphone. of the perpetrator'sacquired.



FORENSIC EXPRESS PHONE CONTENT REPORT

Report MiChat

Manufacturer	samsung
Product	SM-G530H
Platform	Android physical image
SW Revision	5.0.2 (21)

Case Information	
Case Label	Report MiChat
Case Evidence Number	
Case Evidence Details	

Device Information	
Device Label	
Device Name	Physical image - samsung SM-G530H
Device ID	
Device Evidence Number	
Owner Name	
Owner Phone Number	
Phone Notes	

Investigator Information	
Investigator Name	
Investigator Designation	
Investigator Email	
Investigator Phone Number	
Permission Document	

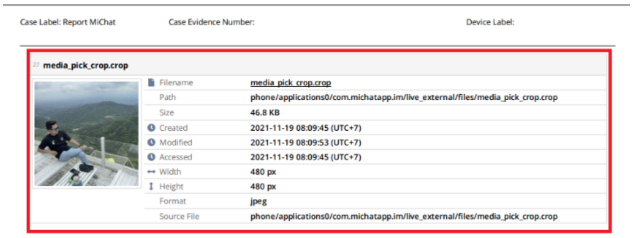
Extraction Information	
Data Extraction Started	2021-11-19 08:57:15 (UTC+7)
Data Extraction Finished	2021-11-19 08:57:16 (UTC+7)
Extracted by	MOBILedit Forensic Express PRO 7.2.0.17975
Report Generated by	MOBILedit Forensic Express PRO 7.2.0.17975
Applications Analyzed by	AppEngine 2020-04-15-00 New version available: 2020-06-10-01

Case Label: Report MiChat Case Evidence Number: Device Label:

Table of Contents

Figure 5. The results of the MOBILedit Forensic Express

In Figure 5 above, there is information about the smartphone perpetrator's, which has been physically images. The results show that there are profile photos of the perpetrators, media such as videos and voice conversations that occur between the perpetrator and the victim.



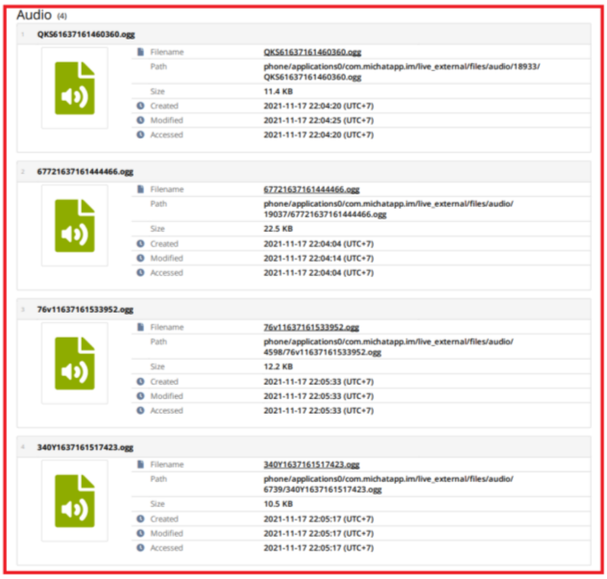
Case Label: Report MiChat Case Evidence Number: Device Label:

media_pick_crop.crop

Filename	media_pick_crop.crop
Path	phone/applications0/com.michatapp.im/live_external/files/media_pick_crop.crop
Size	46.8 KB
Created	2021-11-19 08:09:45 (UTC+7)
Modified	2021-11-19 08:09:53 (UTC+7)
Accessed	2021-11-19 08:09:45 (UTC+7)
Width	480 px
Height	480 px
Format	jpeg
Source File	phone/applications0/com.michatapp.im/live_external/files/media_pick_crop.crop

Figure 6. The profile photo of the perpetrator

The profile photo of the perpetrator is found in Figure 6 in the report file and will be used as evidence to be returned compared to the evidence of the victim's statement.



Audio (4)

1 QKS61637161460360.ogg

Filename: QKS61637161460360.ogg
Path: phone/applications0/com.michatapp.im/live_external/files/audio/18933/QKS61637161460360.ogg
Size: 11.4 KB
Created: 2021-11-17 22:04:20 (UTC+7)
Modified: 2021-11-17 22:04:25 (UTC+7)
Accessed: 2021-11-17 22:04:20 (UTC+7)

2 67721637161444466.ogg

Filename: 67721637161444466.ogg
Path: phone/applications0/com.michatapp.im/live_external/files/audio/19037/67721637161444466.ogg
Size: 22.5 KB
Created: 2021-11-17 22:04:04 (UTC+7)
Modified: 2021-11-17 22:04:14 (UTC+7)
Accessed: 2021-11-17 22:04:04 (UTC+7)

3 76v11637161533952.ogg

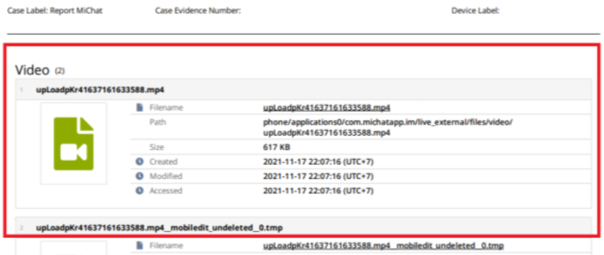
Filename: 76v11637161533952.ogg
Path: phone/applications0/com.michatapp.im/live_external/files/audio/4598/76v11637161533952.ogg
Size: 12.2 KB
Created: 2021-11-17 22:05:33 (UTC+7)
Modified: 2021-11-17 22:05:33 (UTC+7)
Accessed: 2021-11-17 22:05:33 (UTC+7)

4 340Y1637161517423.ogg

Filename: 340Y1637161517423.ogg
Path: phone/applications0/com.michatapp.im/live_external/files/audio/6739/340Y1637161517423.ogg
Size: 10.5 KB
Created: 2021-11-17 22:05:17 (UTC+7)
Modified: 2021-11-17 22:05:17 (UTC+7)
Accessed: 2021-11-17 22:05:17 (UTC+7)

Figure 7. Evidence of Voice Conversation

Figure 7 shows the findings of voice conversations that occurred on the service MiChat between the perpetrator and the victim.



Case Label: Report MiChat   Case Evidence Number: Device Label:

Video (2)

1 upLoadpKr41637161633588.mp4

Filename: upLoadpKr41637161633588.mp4
Path: phone/applications0/com.michatapp.im/live_external/files/video/upLoadpKr41637161633588.mp4
Size: 617 KB
Created: 2021-11-17 22:07:16 (UTC+7)
Modified: 2021-11-17 22:07:16 (UTC+7)
Accessed: 2021-11-17 22:07:16 (UTC+7)

2 upLoadpKr41637161633588.mp4_mobiledit_undeleted_0.tmp

Filename: upLoadpKr41637161633588.mp4_mobiledit_undeleted_0.tmp

Figure 8. Video Evidence Video

Evidence in mp4 format found in Figure 8 on the inspection smartphone using the MOBILedit Forensic Express tool.

2.2.3.2 *Analysis by Autopsy*

Tools are used to facilitate investigators conducting investigations. From the data physical image carried out by the MOBILedit Forensic Express tool, it is entered for a new case in the autopsy tool and will bring up additional deleted data on the smartphone perpetrator's. Figure 9 is a display of data obtained through the Autopsy tool using the MOBILedit Forensic Express physical image tool data. Data that is not contained in the tool MOBILedit ForensicExpress,the autopsy tool found additional data that both can be used as evidence are accurate.

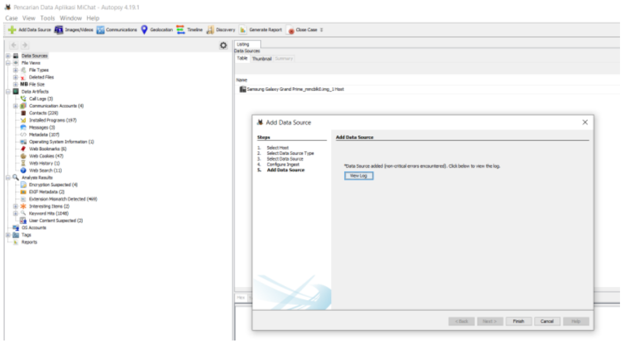


Figure 9. Display of deleted data

Figure 9 shows that there are three sections in the data source, namely File Views, Data Artifacts, and Analysis Results.data smartphone Deleted Can be viewed in Deleted Files.

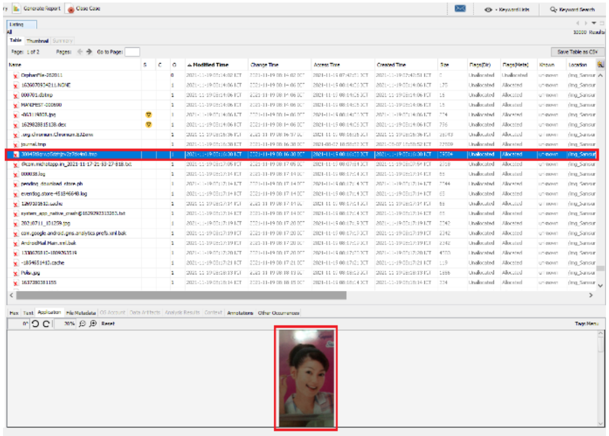


Figure 10. Deleted photos in conversations

Figure 10 shows the findings of deleted images on the smartphone perpetrator'ssent by the victim.

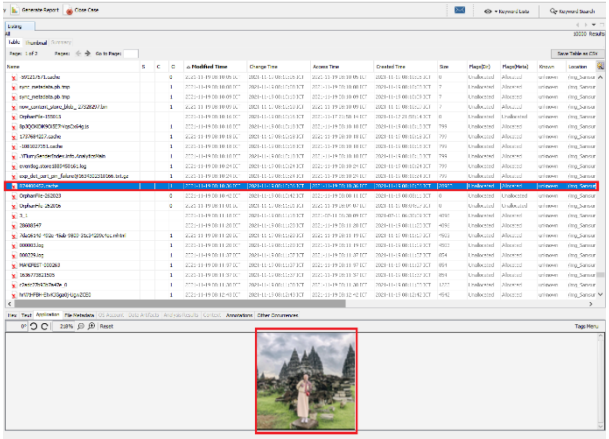


Figure 11. The profile photo of the victim on MiChat

In Figure 11 found the profile photo of the victim on the application MiChat. The perpetrator's profile picture is also found in the autopsy tool as shown in Figure 12.

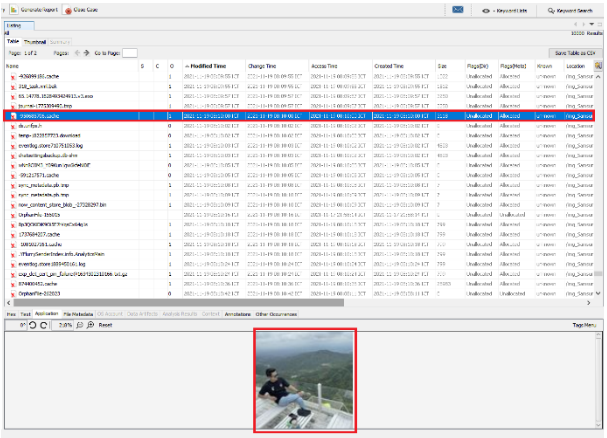


Figure 12. The profile photo of the perpetrator on MiChat

Figure 12 shows the findings of the profile photo of the perpetrator, which means that the victim's statement is in accordance with the findings of the investigator and the perpetrator is found guilty.

2.2.4 Reporting

The reporting stage is the last stage of the method National Institute of Standards and Technology (NIST). The Process reporting reports the results of the analysis of evidence found in the previous process[27].At this stage the investigator will document the results of the analysis of the evidence found in detail. The reporting stage includes a description of the identification, explanation of the forensic process, and data from the use of forensic tools.

2.2.5 Results

At this stage is a conclusion from the results of the previous stages that have been carried out using the MOBILedit Forensic ExpressTool and Autopsy. The software that went through the forensic process in this study was a smartphone using a service MiChat -based mobile. The evidence is analyzed using several forensic tools, the analysis results obtained from the forensic process using forensic tools can be seen in Table 2.

Table 2. Comparison of Evidence Found obtained from Several Tool

No	Digital Evidence	Forensic Tool	
		MOBILeditForensic Express + DB Browser	Autopsy
1	Conversation Text	No	No
2	Images/Photos profile	Yes	Yes
3	Account Information	Yes	Yes
4	Video	Yes	No
5	Voicemail	Yes	No

Table 2 shows the findings obtained from analyzing the MiChat application on a mobile-based smartphone using the forensic tools MOBILedit Forensic Express and Autopsy. The data found included other media (images, videos, and voice messages), and account information on MiChat services such as perpetrator/victim profile photos and account information. The use of the DB Browser for SQLite forensic tool is to open the result database file.

Table 3. The Findings of Evidence

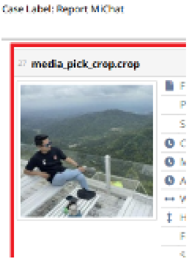
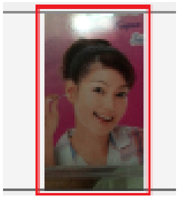
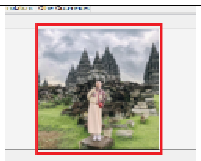
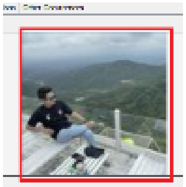
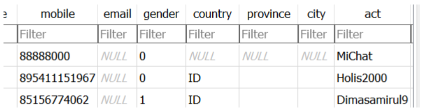
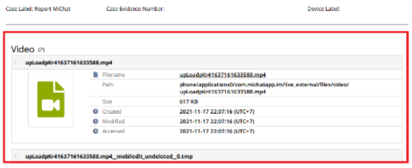
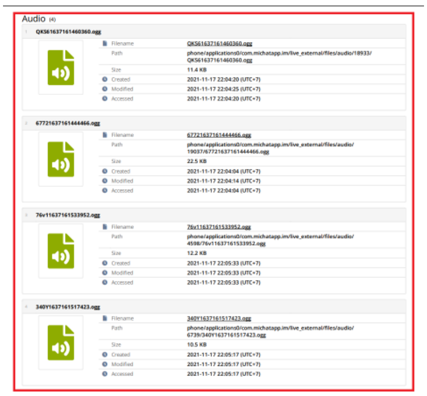
Digital Evidence	Findings
Images/photos profile	 Case Label: Report MiChat media_pick_crop.crop   
Account information	 mobile | email | gender | country | province | city | act Filter | Filter | Filter | Filter | Filter | Filter | Filter 88888000 | NULL | 0 | NULL | NULL | NULL | MiChat 895411151967 | NULL | 0 | ID | | | Holis2000 85156774062 | NULL | 1 | ID | | | Dimasamirul9
Video	 Case Label: Report MiChat Case Evidence Number: Device Label: Video (2) 1 upLoadpKr41637161633588.mp4 Filename upLoadpKr41637161633588.mp4 Path phone/applications0/com.michatapp.im/live_external/files/video/upLoadpKr41637161633588.mp4 Size 617 KB Created 2021-11-17 22:07:16 (UTC+7) Modified 2021-11-17 22:07:16 (UTC+7) Accessed 2021-11-17 22:07:16 (UTC+7) 2 upLoadpKr41637161633588.mp4__mobiledit_undeleted_0.tmp
Voicemail	 Audio (4) 1 QKS61637161460360.ogg Filename QKS61637161460360.ogg Path phone/applications0/com.michatapp.im/live_external/files/audio/18933/QKS61637161460360.ogg Size 11.4 KB Created 2021-11-17 22:04:20 (UTC+7) Modified 2021-11-17 22:04:25 (UTC+7) Accessed 2021-11-17 22:04:20 (UTC+7) 2 67721637161444466.ogg Filename 67721637161444466.ogg Path phone/applications0/com.michatapp.im/live_external/files/audio/19037/67721637161444466.ogg Size 22.5 KB Created 2021-11-17 22:04:04 (UTC+7) Modified 2021-11-17 22:04:14 (UTC+7) Accessed 2021-11-17 22:04:04 (UTC+7) 3 76v11637161533952.ogg Filename 76v11637161533952.ogg Path phone/applications0/com.michatapp.im/live_external/files/audio/4598/76v11637161533952.ogg Size 12.2 KB Created 2021-11-17 22:05:33 (UTC+7) Modified 2021-11-17 22:05:33 (UTC+7) Accessed 2021-11-17 22:05:33 (UTC+7) 4 340Y1637161517423.ogg Filename 340Y1637161517423.ogg Path phone/applications0/com.michatapp.im/live_external/files/audio/6739/340Y1637161517423.ogg Size 10.5 KB Created 2021-11-17 22:05:17 (UTC+7) Modified 2021-11-17 22:05:17 (UTC+7) Accessed 2021-11-17 22:05:17 (UTC+7)

Table 3 shows the evidence findings. Username of perpetrator (Holis2000) and victim (Dimasamirul9) in database file. MOBILedit Forensic Express finds perpetrator profile photos, audio and video. Autopsy displays images in the victim's conversation and profile photos of perpetrators and victims.

3. CONCLUSION

The forensic process carried out with fraud cases on MiChat-based cellular services was partially successful in obtaining digital evidence using forensic tools. Based on the results of this study, comparing the results of data extraction from the Samsung SM-G530H smartphone, it can be concluded that the use of appropriate forensic tools to extract the data obtained, the data extracted and analyzed using the stages of the National Institute of Standards and Technology (NIST) method. The MOBILedit Forensic Express tool provides an accuracy index value of more than 50%, higher than Autopsy with a value of 40%. For further research, it is hoped that you can use other or new tools, also try to use the latest smartphones and the latest iOS-based smartphones.

4. REFERENCES

[1] M. Sumenge, “Fraud Using Internet Media in the Form of Buying and Selling Online,” *Lex Crim.*, vol. 2, no. 4, pp. 102–112, 2013.

[2] I. Zuhriyanto *et al.*, "Forensic Digital Design In Applications," *Semin. Nas. Inform.*, vol. 2018, no. November, pp. 86–91, 2018.

[3] K. Dwi, O. Mahendra, and I. K. Ari, "Digital Forensic Analysis of Michat Applications on Android as Digital Proof in Handling Online Prostitution Cases," vol. 9, no. 3, pp. 381–390, 2021.

[4] R. Umar and Sahiruddin, "Nist Method For Forensic Analysis Of Digital Evidence On Android Device," *Pros. SENDU_U_2019*, pp. 978–979, 2019.

[5] ahwan ahmadi, T. Akbar, and H. Mandala Putra, "Comparison of Forensic Tool Results on Android Smartphone Image Files Using the Nist Method," *JIKO (Jurnal Inform. dan Komputer)*, vol. 4, no. 2, pp. 92–97, 2021, doi: 10.33387/jiko.v4i2.2812.

[6] Z. Akbar, B. Nugraha, and M. Alaydrus, "Whatsapp Forensics On Android Smartphone : a Survey," *Sinergi*, vol. 20, no. 3, p. 207, 2016, doi: 10.22441/sinergi.2016.3.006.

[7] R. Rizal, I. Riadi, and Y. Prayudi, "Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device," *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 4, pp. 382–390, 2018.

[8] N. Iman, A. Susanto, and R. Inggi, "Analysis of the Development of Digital Forensics in Cybercrime Investigations in Indonesia (Systematic Review)," *J. Telekomun. dan Komput.*, vol. 9, no. 3, p. 186, 2020, doi: 10.22441/incomtech.v9i3.7210.

[9] A. Fauzan, I. Riadi, and A. Fadlil, "Digital Forensic Analysis On Line Messenger For Cybercrime Handling," *Annu. Res. Semin.*, vol. 2, no. 1, pp. 159–163,2017,[Online].Available:http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/832/752.

[10] N. Nasirudin, S. Sunardi, and I. Riadi, "Forensic Analysis of Android Smartphones Using the NIST Method and the MOBILedit Forensic Express Tool," *J. Inform. Univ. Pamulang*, vol. 5, no. 1, p. 89, 2020, doi: 10.32493/informatika.v5i1.4578.

[11] M. Dweikat, D. Eleyan, and A. Eleyan, "Digital Forensic Tools Used in Analyzing Cybercrime," *J. Univ. Shanghai Sci. Technol.*, vol. 23, no. 3, pp. 367–379, 2021, doi: 10.51201/jusst12621.

[12] I. F. Rohman, N. Widiyasono, and R. Gunawan, "Jurnal Sustainable :Journal of Applied Research and Industry Results Digital Evidence Analysis Simulation Skype Applications Android-Based using NIST SP 800 - 101 R1," vol. 08, no. 01, 2019.

[13] S. Madiyanto, H. Mubarok, and N. Widiyasono, "Mobile Forensics Investigation Process on IOS Based Smartphone," *J. Rekayasa Sist. Ind.*, vol. 4, no. 01, pp. 93–98, 2017, doi: 10.25124/jrsi.v4i01.149.

[14] M. I. Syahib, I. Riadi, and R. Umar, "Digital Forensic Analysis Beetalk Application for Handling Cybercrime Using the NIST Method," *Semin. Nas. Inform.*, vol. 2018, no. November, p. 134, 2018, [Online].Available:http://jurnal.upnyk.ac.id/index.php/semnasif/article/view/2629.

[15] I. Riadi, "Examination of Digital Evidence on Android-based LINE Messenger," *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 3, pp. 336–343, 2018, doi: 10.17781/p002472.

[16] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "1490-Article Text-2859-1-10-20190413,"Digital Evidence Acquisition on Android-Based Instagram Messenger Using National Institute Justice Method, vol. 4, pp. 219–227, 2018.

[17] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic tools performance analysis on android-based blackberry messenger using NIST measurements," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 3991–4003, 2018, doi: 10.11591/ijece.v8i5.pp3991-4003.

[18] I. Riadi, A. Yudhana, M. Caesar, and F. Putra, "Instagram Messenger Digital Evidence Recovery Analysis Using the National Institute of Standards and Technology (Nist) Method," *Semin. Nas. Teknol. Inf. dan Komun. - Semant.*, pp. 161–166, 2017.

[19] F. Mobile, P. Kasus, and C. Fraud, "Mobile Forensics in Cyber Fraud Cases Signal Messenger Service Using the NIST Method," vol. 3, no. 28, pp. 137–144, 2022.

[20] M. Fitriana, K. A. AR, and J. M. Marsya, "Application of the National Institute of Standards and Technology (NIST) Methods in Digital Forensic Analysis for Handling Cyber Crime," *Cybersp. J. Pendidik. Teknol. Inf.*, vol. 4, no. 1, pp. 29–39, 2020, doi: 10.22373/cj.v4i1.7241.

[21] M. Riskiyadi, "Forensic Investigation of Digital Evidence in Exposing Cybercrime," *CyberSecurity dan Forensik Digit.*, vol. 3, no. 2, pp. 12–21, 2020.

[22] R. A. K. N. Bintang, R. Umar, and U. Yudhana, "Live forensics comparison design on Instagram, Facebook and Twitter social media security on Windows 10," *Pros. SNST ke-9 Tahun 2018 Fak. Tek. Univ. Wahid Hasyim*, pp. 125–128, 2018.

[23] S. Ferreira, M. Antunes, and M. E. Correia, "Exposing manipulated photos and videos in digital forensics analysis," *J. Imaging*, vol. 7, no. 7, 2021, doi: 10.3390/jimaging7070102.

[24] D. A. Putri, "Forensics Mobile Against Threat Cases Through WhatsApp Services," pp. 1–8.

[25] R. Y. Prasongko, A. Yudhana, and A. Fadil, "Forensic analysis of the KakaoTalk application using the National Institute Standard Technology method," *Semin. Nas. Inform. 2018 (semnasIF 2018) UPN "Veteran" Yogyakarta, 24 Novemb. 2018 ISSN 1979-2328*, vol. 2018, no. November, pp. 129–133, 2018.

[26] T. D. Larasati and B. C. Hidayanto, "Live Forensics Analysis For Comparison Of Instant Messenger Applications On Windows 10 Operating System," *Sesindo*, vol. 6, no. November, pp. 456–256, 2017.

[27] R. Umar, I. Riadi, and G. Maulana, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 12, pp. 69–75, 2017, doi: 10.14569/ijacsa.2017.081210.