Digital Forensic Analysis on Mobile-based MiChat Services using National Institute of Standard Technology Method

Adinda Cintya Nur Hidayah
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 technology is increasing, mobile phones have now developed into smartphones. Smartphones can make it easier for users to communicate, do learning and many things with the support of the internet. The internet has a good impact on its users but of course, there are also bad effects because anyone can access it. This research was conducted based on real cases that have occurred, to collect digital data on smartphones. Digital data is very important in helping to uncover cybercrimes but digital data that has been deleted from the device cannot be recovered in its entirety. This study will simulate cases of online prostitution using MiChat services. This research was conducted to find out how digital data from mobile-based MiChat services can be obtained. This research uses the National Institute of Standard Technology (NIST) method. This method has four stages, namely the stages of collection, examination, analysis, and reporting. The tool to be examined is a rooted cell phone used in online prostitution transactions. This study shows the data found from the MiChat application which can be obtained using the MOBILedit Forensic Express, Autopsy and DB Browser for SQLite tools. The data that can be found from the tool used is a message in the form of a photo of the user's profile, proof of a transaction, a voice message, user data of the linked MiChat account, and the time the transaction occurred.

Keywords

NIST, Data Digital, MiChat, Smartphone, Android, Online Prostitution, Cyber Porn, Forensic Mobile

1. INTRODUCTION

The development of technology in Indonesia is increasingly rapid in everyday life where the internet has become one of the necessities for the lives of some people [1]. Especially during the pandemic that hit the world, people are increasingly spending their activities using smartphones with internet connections for school or working from home (WFH). Smartphones and the internet are very popular these days, especially with their various features: social media apps. One type of social media that is very actively used is instant messaging. Instant Messaging can facilitate communication even remotely by privately sending messages, pictures and videos to someone. Technological developments in addition to bringing many positive impacts also have negative impacts. The sophistication of various applications today allows for an increase in online crime cases, such as cyberporn, online gambling, spreading hoax news, fraud, hate speech, cyberbullying, and many other cyber cases. Online crimes related to online prostitution can be found on various social media and instant messaging applications, and MiChat is one of them. In Indonesia itself, many cases useMiChat as a means of transaction. Several cases related to online prostitution through MiChat have also been recorded in district courts in several regions in Indonesia.

1.1 Study Literature

1.1.1 Previous Study

The first research entitled "Forensic WhatsApp based on Android using the National Institute of Standard Technology (NIST) Method" explains maintaining digital evidence when the smartphone is rooted and non-rooted. The evidence that has been obtained and stored is carried out by imaging which is then analyzed for the level of similarity. The use of different forensic tools will produce mixed results. [2].

The second in the research "Analysis of the Distribution Pattern of Pornography on Social Media with Social Network Analysis" explain the use of data collection methods based on certain keywords that will produce a picture, although not complete, of this phenomenon to To get a large dataset of more than 1500 data, it takes about two hours interval between data collection time [3].

The third researchentitled "Web Browser Exploration in Searching Digital Evidence Using SQLITE" explains what information can be obtained from a web browser database using SQLite, the results of which will be very helpful in searching digital data, although not all data can be obtained. but with a combination of other tools, data can be obtained [4].

The fourth in the research "Live Memory Acquisition Method for Digital Artifact Searching for Laptop Memory Devices Based on Simulation of Cyber Crime Cases" proves that a device’s memory can store users' internet activities. Tests carried out on three data acquisitions of digital artefacts can produce three different percentages [5].

The last research entitled "Forensic investigation analysis of cyberbullying on Whatsapp Messenger using the NIST method" describes the use of text mining to identify evidence that can lead to cases of cyberbullying. The use of the cosine similarity method to check the level of similarity between two objects. [6].

1.1.2 Digital Forensic

The handling of cybercrime cases is carried out through investigative activities known as digital forensic [7]. Digital Forensic is the application of computer science and technology for the benefit of legal evidence, which in this case is proving technological crimes or computer crimes that can be obtained scientifically to obtain digital evidence that can be used against violators[8].Digital forensic is evidence with the characteristics of having suitability in supporting factual evidence and uncovering events based on convincing statistical evidence [10].The purpose of digital forensic is to prove the existence of instructions that have occurred by conducting a crime scene investigation so that they can prove it from evidence such as computer systems, storage media, electronic documents, or data packets moving through computer networks [9].

1.1.3 *Forensic Mobile*

Mobile forensic is a branch of digital forensic[10]Mobile forensic is the science of recovering digital evidence, or data from mobile devices, using acceptable methods[11]. Mobile forensicis 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].

1.1.4 *Digital Evidence*

Data is the result of observations made directly on an event, which symbolizes an object or concept in the real world[13]. Data has a definition as a fact or anything that is referred to as the result of an observation of a natural phenomenon. The result of direct observation of events or facts of phenomena in the real world, data includes writing or pictures that are equipped with certain values[14]. The use of data (after processing and analyzing) for decision-makers is an objective basis in the decision-making process or policy. Digital evidence consists of 2 words, namely evidence and digital. Evidence is information that is used to establish or refute a fact. The evidence is divided into two, namely physical evidence and digital evidence[16]. Evidence from cases of cybercrime is different from conventional crimes, where the handling of electronic evidence and digital evidence contained in it is susceptible to change or contamination, so electronic evidence must be packaged and stored properly in a safe place[17].

1.1.5 *MiChat*

MiChat is a mobile communication app for people to connect with family and friends through fun chat features. MiChat is a complete communication tool that functions as both a social media and an application for its users to exchange messages. MiChat was launched and published in April 2018. MiChat is a great messenger app that's not much different from WeChat's design but has some differences in its features. MiChat will provide close friendship suggestions.

1.1.6 *CyberPorn*

One of the problems of cybercrime that is very troubling and has received attention from various circles is the problem of cybercrime in the field of decency. The types of cybercrime in the field of decency that are often disclosed are cyber pornography (especially child pornography) and cybersex [18].Cyber porn is an act that uses cyberspace to create, display, distribute, and publish pornography and obscene material on a site[19].

1.1.7 *National Institute of Standard Technology*

The National Institute of Standard Technology stage is an inspection stage that has standard policies and work guidelines to ensure each inspection follows the workflow so that the work can be repeated and can be maintained. So that the flow is carried out in a structured manner and can be identified based on a systematic solution, the research method uses forensic work steps that are used to describe the stages and stages of theresearch to be carried out. without researchers reducing that which has been proposed by the NIST metode method [20].

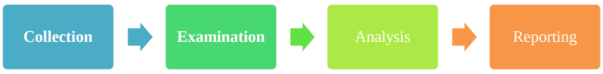


Figure 1. Stages of National Institute of Standard Technology

Figure 1shows 4 stages of NIST that can be used for the forensic process. The descriptions are as follows [21] :

1. Collection
   The Collection stageis the process of labelling, identifying, recording, and retrieving data from relevant data sources with procedures to maintain the integrity of data.
2. Examination
   The Examination stage is carried out by processing the data collected in the use of forensic combinations of various scenarios, either automatically or manually, as well as assessing the data and issuing data as needed while maintaining data integrity.
3. Analysis
   The Analysis stage is the stage of analyzing the data that has been obtained using methods and techniques that are by applicable rules.
4. Reporting
   The Reporting stage is the stage of reporting the results of the analysis which includes the description of the actions taken.

2. METHODOLOGY

2.1 Research Scenario

In this study, the smartphone was in a root condition. Research design begins with creating an engineered scenario that is executed to obtain digital evidence[22].This simulation uses a simulation of a case that has existed previously and is modified to suit the research. The case raised is online prostitution on the MiChat service that runs on Android-based phones. The initial stage in this research is creating an account on the MiChat application, then the customer starts contacting the perpetrator or pimp asking about the availability of their online prostitution service, and then communication occurs between the two accounts who have become friends on the MiChat service. In communication through the message feature on MiChat, online prostitution transactions occur. During the transaction, this prostitution service also sends a picture of the woman it offers on the day and dates the customer needs it and the customer sends proof of the transaction.

The flow of the case scenario of this research can be shown in Figure 2.

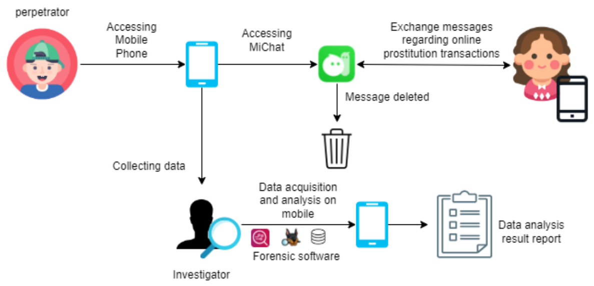

perpetrator
Accessing Mobile Phone
Accessing MiChat
Exchange messages regarding online prostitution transactions
Message deleted
Collecting data
Data acquisition and analysis on mobile
Forensic software
Investigator
Data analysis result report

Figure 2.The flow of the Case Scenario on MiChat

Figure 2 shows the flow ofthe case scenario which starts from the process of searching and collecting message data in the form of text, images and sound data. The explanation of the case simulation in Figure 2 is as follows:

1. Perpetrators and Customers conduct online prostitution transactions through the MiChat application;
2. After the transaction is complete, the MiChat application message on the cellphone is deleted by the perpetrator;
3. Next, root the perpetrator's smartphone;
4. Researchers collect data related to online prostitution transactions;
5. Furthermore, the data that has been collected will be examined further;
6. In the last stage, the results of data collection and search are presented in tabular form.

2.2 Research Stages

The research stage is a process that is applied by an investigator to carry out the forensic process. The steps or stages used in this research use the stages of the National Institute of Standards and Technology (NIST) which has four stages, namely Collection, Examination, Analysis, and Reporting.

2.2.1 Collection

Data collection is very important as an early stage to collect and search data from digital sources. The data collection process can be done via a smartphone where there are conversations related to online prostitution. The smartphone will be rooted first with the help of the Odin and SuperSU applications, MOBILedit Forensic Express will function during the Imaging process of data files on the cellphone. In addition, a USB cable is also needed to connect the cellphone to a laptop to access cellphone data. The following tools are used in this research:

Table 1. Physical Evidence Found

No	Name	Image	Description
1	Smartphone Samsung J1 Ace (Duos)		The phone used by the perpetrator is rooted and the message is deleted
2	Smartphone Samsung A7 (2018)		Customer's phone, not root condition
3	USB Cable Connector		Cable connecting smartphones and laptops in the process of analysis

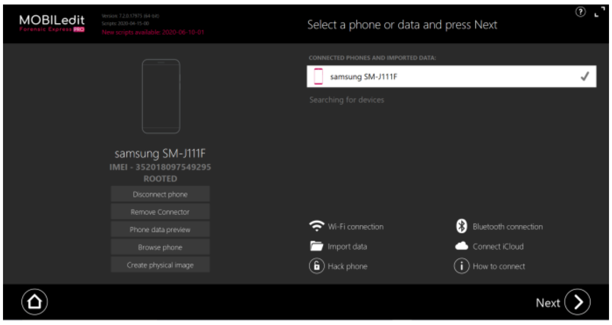
Table 1 shows documentation of physical evidence in the form of smartphone devices used by pimps and customers related to online prostitution.

2.2.2 Examination

This Examination stage is an advanced stage of the data collection process in the form of evidence contained in the previous table such as two smartphones and a connector cable.These tools apply techniques and procedures to generate re-enactments of ongoing events, to help digital forensic 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 toolsto perform data acquisition on smartphones, and then the investigator chooses application analysis to extract application data on the smartphone[24].


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

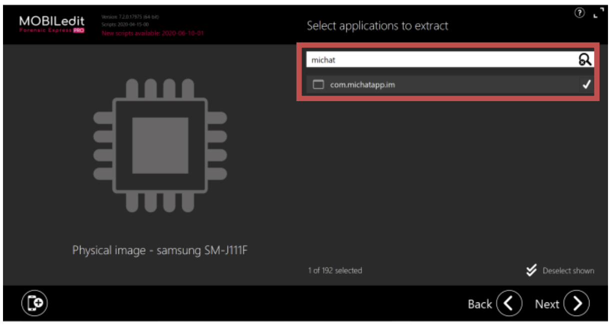
Select a phone or data and press Next

CONNECTED PHONES AND IMPORTED DATA:
samsung SM-J111F ✓
Searching for devices

samsung SM-J111F
IMEI - 352018097549295
ROOTED

Figure 3. Smartphone connected toMOBILEdit Forensic Express

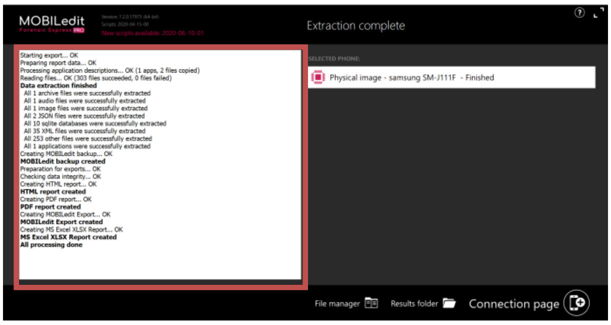
Figure 3 shows the smartphonepotition is rooted and connected to a PC/Laptop using a cable USB to perform the data acquisition process with the tools MOBILedit Forensic Express[25].That Process is called Physical Image, this process is carried out to make a copy of the data and keep the original data so that there is no damage during the analysis process.The time in the imaging file process depends on the size of the contents of the smartphone used.



MOBILedit
Forensic Express PRO
Version: 7.2.0.17975 (64-bit)
Scripts: 2020-04-15-00
New scripts available: 2020-06-10-01
Select applications to extract
michat
□ com.michatapp.im ✓
Physical image - samsung SM-J111F
1 of 192 selected
Deselect shown
Back
Next

Figure 4. Acquisition of MOBILedit Forensic Express

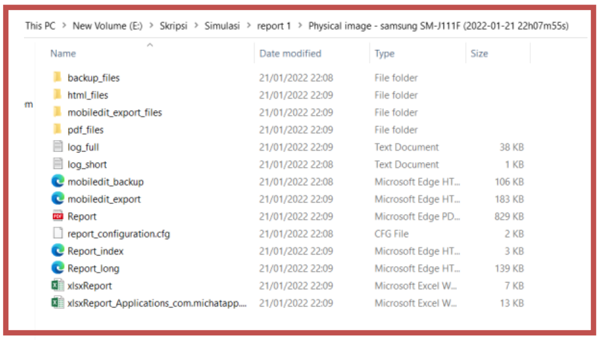
Figure 4shows a page on the Mobiledit Forensic Express tool in the application section to be extracted and can be selected according to the application to be analyzed. In this study, Michat was chosen as the application that will perform the extraction.The application to be extracted which can be searched directly with the search engine feature and selected by checking the data in the folder named com.michatapp.im for MiChatthat acquisition smartphone was carried out using the tool MOBILedit Forensic Express.



```
Starting export... OK
Preparing report data... OK
Processing application descriptions... OK (1 apps, 2 files copied)
Reading files... OK (303 files succeeded, 0 files failed)
Data extraction finished
 All 1 archive files were successfully extracted
 All 1 audio files were successfully extracted
 All 1 image files were successfully extracted
 All 2 JSON files were successfully extracted
 All 10 sqlite databases were successfully extracted
 All 35 XML files were successfully extracted
 All 253 other files were successfully extracted
 All 1 applications were successfully extracted
Creating MOBILedit backup... OK
MOBILedit backup created
Preparation for exports... OK
Checking data integrity... OK
Creating HTML report... OK
HTML report created
Creating PDF report... OK
PDF report created
Creating MOBILedit Export... OK
MOBILedit Export created
Creating MS Excel XLSX Report... OK
MS Excel XLSX Report created
All processing done
```

Figure 5. Data Acquisition Results

Figure 5 shows the display of data in the MiChat application that has been successfully acquired using the MOBILedit Forensic Express tool without any error messages displayed in the process, the error message will be marked with writing in red. Next step to see the results of data acquisition, you can directly click the Results Folder, after whichwill be directed to the data acquisition folder that was successfully store.



This PC > New Volume (E:) > Skripsi > Simulasi > report 1 > Physical image - samsung SM-J111F (2022-01-21 22h07m55s)

Name	Date modified	Type	Size
backup_files	21/01/2022 22:08	File folder	
html_files	21/01/2022 22:09	File folder	
mobiledit_export_files	21/01/2022 22:09	File folder	
pdf_files	21/01/2022 22:09	File folder	
log_full	21/01/2022 22:09	Text Document	38 KB
log_short	21/01/2022 22:08	Text Document	1 KB
mobiledit_backup	21/01/2022 22:08	Microsoft Edge HT...	106 KB
mobiledit_export	21/01/2022 22:09	Microsoft Edge HT...	183 KB
Report	21/01/2022 22:09	Microsoft Edge PD...	829 KB
report_configuration.cfg	21/01/2022 22:08	CFG File	2 KB
Report_index	21/01/2022 22:09	Microsoft Edge HT...	3 KB
Report_long	21/01/2022 22:09	Microsoft Edge HT...	139 KB
xlsxReport	21/01/2022 22:09	Microsoft Excel W...	7 KB
xlsxReport_Applications_com.michatapp....	21/01/2022 22:09	Microsoft Excel W...	13 KB

Figure 6. Display of Saved Data Results

Figure 6 shows reporting results from the data extraction process that has been carried out have file types including backup_files, mobile_export_files and pdf_file which are shown in the image.

2.2.3 *Analysis*

At this analysis stage, the data that has been obtained in the previous stage, namely the examination stage, is to ensure that the data obtained are by the results required in the investigation. the evidence found is adjusted to what was submitted by the victim to the investigator. Digital evidence analysis includes the collection of critical digital data and the reading of digital evidence.

2.2.3.1 *Analysis by MOBILeditForensic Express*

The results of Examination data on a smartphone that has been rooted and opened are the results of the reporting file from the acquisition folder taken via the MOBILedit Forensic Express tool.

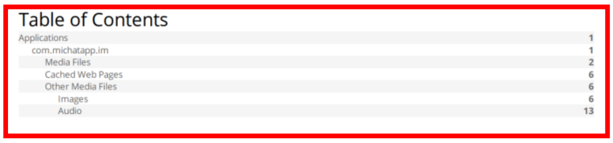
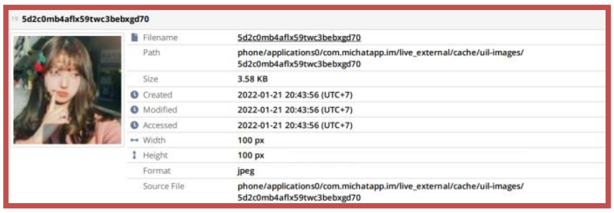


Table of Contents

Applications	1
com.michatapp.im	1
Media Files	2
Cached Web Pages	6
Other Media Files	6
Images	6
Audio	13

Figure 7. PDF Report MOBILedit Forensic Express

Figure 7shows information related to smartphone specifications acquired with MOBILedit Forensic Express and the data detected by the MOBILedit Forensic Express tool can be seen on the table of contents page, the table is a display of data results obtained by the MOBILedit Forensic Express tool.

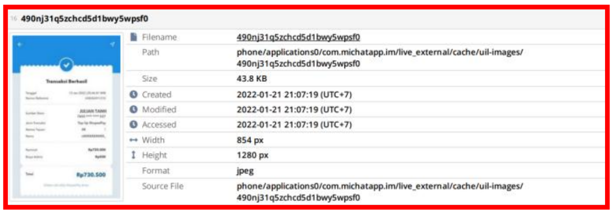


5d2c0mb4aflx59twc3bebxgd70

Filename	5d2c0mb4aflx59twc3bebxgd70
Path	phone/applications0/com.michatapp.im/live_external/cache/uil-images/ 5d2c0mb4aflx59twc3bebxgd70
Size	3.58 KB
Created	2022-01-21 20:43:56 (UTC+7)
Modified	2022-01-21 20:43:56 (UTC+7)
Accessed	2022-01-21 20:43:56 (UTC+7)
Width	100 px
Height	100 px
Format	jpeg
Source File	phone/applications0/com.michatapp.im/live_external/cache/uil-images/ 5d2c0mb4aflx59twc3bebxgd70

Figure 8. The Profile Photo of the Perpetrator

Figure 8shows that in the PDF file there is a profile photo of the pimp or the owner of a commercial sex worker.

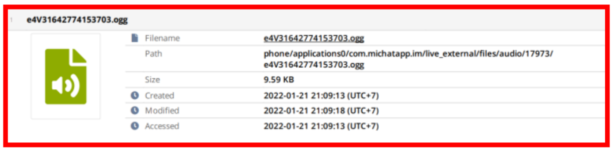


490nj31q5zchcd5d1bwy5wpsf0

Filename	490nj31q5zchcd5d1bwy5wpsf0
Path	phone/applications0/com.michatapp.im/live_external/cache/uil-images/ 490nj31q5zchcd5d1bwy5wpsf0
Size	43.8 KB
Created	2022-01-21 21:07:19 (UTC+7)
Modified	2022-01-21 21:07:19 (UTC+7)
Accessed	2022-01-21 21:07:19 (UTC+7)
Width	854 px
Height	1280 px
Format	jpeg
Source File	phone/applications0/com.michatapp.im/live_external/cache/uil-images/ 490nj31q5zchcd5d1bwy5wpsf0

Figure 9. Deleted photo in conversation

Figure 9shows a picture of the proof transfer sent by the customer to the perpetrator which has been deleted from the perpetrator's cellphone.



e4V31642774153703.ogg

Filename	e4V31642774153703.ogg
Path	phone/applications0/com.michatapp.im/live_external/files/audio/17973/ e4V31642774153703.ogg
Size	9.59 KB
Created	2022-01-21 21:09:13 (UTC+7)
Modified	2022-01-21 21:09:18 (UTC+7)
Accessed	2022-01-21 21:09:13 (UTC+7)

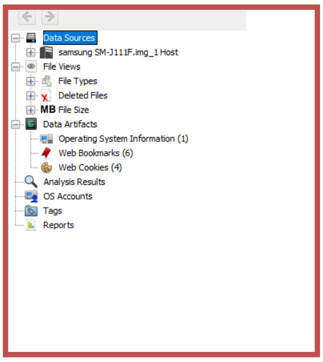
Figure 10. Evidence of Voice Conversation

Figure 10 shows the audio file sent in the massage room, which data can be opened and listened to when clicked directly on the MOBILedit Forensic Express PDF Report file.

2.2.3.2 *Autopsy*

The next step is to open the Autopsy tool to add data search results that have previously been done using the MOBILedit Forensic Express tool. Imaging results on the MOBILedit

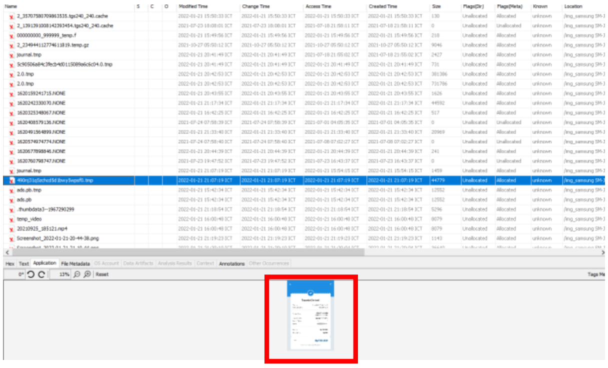
Forensic Express tool will be used in data retrieval using theAutopsy tool.



- Data Sources
  - samsung SM-J111F.img_1 Host
- File Views
  - File Types
  - Deleted Files
  - MB File Size
- Data Artifacts
  - Operating System Information (1)
  - Web Bookmarks (6)
  - Web Cookies (4)
- Analysis Results
- OS Accounts
- Tags
- Reports

Figure 11. Autopsy Results

Figure 11 shows the final results of the data search process performed on the Autopsy tools.



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
2_35707580709863535.tgs240_240.cache				2022-01-21 15:50:33 ICT	2022-01-21 15:50:33 ICT	2022-01-21 15:50:33 ICT	2022-01-21 15:50:33 ICT	130	Unallocated	Allocated	unknown	/img_samsung SM-J
2_1391391008142393454.tgs240_240.cache				2021-07-23 18:08:01 ICT	2021-07-23 18:08:01 ICT	2021-07-18 21:58:11 ICT	2021-07-18 21:58:11 ICT	0	Unallocated	Unallocated	unknown	/img_samsung SM-J
000000000_999999_temp.f				2022-01-21 15:49:56 ICT	2022-01-21 15:49:56 ICT	2022-01-21 15:49:56 ICT	2022-01-21 15:49:56 ICT	218	Unallocated	Allocated	unknown	/img_samsung SM-J
2_2349441127746111819.temp.gz				2021-10-27 05:50:12 ICT	2021-10-27 05:50:12 ICT	2021-10-27 05:50:12 ICT	2021-10-27 05:50:12 ICT	9046	Unallocated	Allocated	unknown	/img_samsung SM-J
journal.tmp				2022-01-21 20:41:49 ICT	2022-01-21 20:41:49 ICT	2021-07-18 21:55:02 ICT	2021-07-18 21:55:02 ICT	2427	Unallocated	Allocated	unknown	/img_samsung SM-J
5c90506a84c3fecb4d0115089a6c6c04.0.tmp				2022-01-21 20:41:49 ICT	2022-01-21 20:41:49 ICT	2022-01-21 20:41:49 ICT	2022-01-21 20:41:49 ICT	731	Unallocated	Allocated	unknown	/img_samsung SM-J
2.0.tmp				2022-01-21 20:42:53 ICT	2022-01-21 20:42:53 ICT	2022-01-21 20:42:53 ICT	2022-01-21 20:42:53 ICT	381386	Unallocated	Allocated	unknown	/img_samsung SM-J
2.0.tmp				2022-01-21 20:42:53 ICT	2022-01-21 20:42:53 ICT	2022-01-21 20:42:53 ICT	2022-01-21 20:42:53 ICT	731786	Unallocated	Allocated	unknown	/img_samsung SM-J
1620159241715.NONE				2022-01-21 20:43:55 ICT	2022-01-21 20:43:55 ICT	2022-01-21 20:43:55 ICT	2022-01-21 20:43:55 ICT	1626	Unallocated	Allocated	unknown	/img_samsung SM-J
1620242330070.NONE				2022-01-21 21:17:34 ICT	2022-01-21 21:17:34 ICT	2022-01-21 21:17:34 ICT	2022-01-21 21:17:34 ICT	44592	Unallocated	Allocated	unknown	/img_samsung SM-J
1620325348067.NONE				2022-01-21 16:42:25 ICT	2022-01-21 16:42:25 ICT	2022-01-21 16:42:25 ICT	2022-01-21 16:42:25 ICT	517	Unallocated	Allocated	unknown	/img_samsung SM-J
1620408579136.NONE				2021-07-24 07:58:39 ICT	2021-07-24 07:58:39 ICT	2021-07-01 04:05:35 ICT	2021-07-01 04:05:35 ICT	0	Unallocated	Unallocated	unknown	/img_samsung SM-J
1620491564899.NONE				2022-01-21 21:33:40 ICT	2022-01-21 21:33:40 ICT	2022-01-21 21:33:40 ICT	2022-01-21 21:33:40 ICT	20969	Unallocated	Allocated	unknown	/img_samsung SM-J
1620574974774.NONE				2021-07-24 07:58:40 ICT	2021-07-24 07:58:40 ICT	2021-07-08 07:02:27 ICT	2021-07-08 07:02:27 ICT	0	Unallocated	Unallocated	unknown	/img_samsung SM-J
1620677898846.NONE				2022-01-21 20:44:39 ICT	2022-01-21 20:44:39 ICT	2022-01-21 20:44:39 ICT	2022-01-21 20:44:39 ICT	241	Unallocated	Allocated	unknown	/img_samsung SM-J
1620760798747.NONE				2021-07-23 19:47:52 ICT	2021-07-23 19:47:52 ICT	2021-07-23 16:43:37 ICT	2021-07-23 16:43:37 ICT	0	Unallocated	Unallocated	unknown	/img_samsung SM-J
journal.tmp				2022-01-21 21:07:19 ICT	2022-01-21 21:07:19 ICT	2022-01-21 15:54:15 ICT	2022-01-21 15:54:15 ICT	1459	Unallocated	Allocated	unknown	/img_samsung SM-J
490nj31q5echcd5d1bwy5wpsf0.tmp				2022-01-21 21:07:19 ICT	2022-01-21 21:07:19 ICT	2022-01-21 21:07:19 ICT	2022-01-21 21:07:19 ICT	44779	Unallocated	Allocated	unknown	/img_samsung SM-J
ads.pb.tmp				2022-01-21 15:42:34 ICT	2022-01-21 15:42:34 ICT	2022-01-21 15:42:34 ICT	2022-01-21 15:42:34 ICT	12552	Unallocated	Allocated	unknown	/img_samsung SM-J
ads.pb				2022-01-21 15:42:34 ICT	2022-01-21 15:42:34 ICT	2022-01-21 15:42:34 ICT	2022-01-21 15:42:34 ICT	12552	Unallocated	Allocated	unknown	/img_samsung SM-J
.thumbdata3--1967290299				2022-01-21 21:18:54 ICT	2022-01-21 21:18:54 ICT	2022-01-21 21:18:54 ICT	2022-01-21 21:18:54 ICT	5296	Unallocated	Allocated	unknown	/img_samsung SM-J
temp_video				2022-01-21 16:00:48 ICT	2022-01-21 16:00:48 ICT	2022-01-21 16:00:48 ICT	2022-01-21 16:00:48 ICT	8079	Unallocated	Allocated	unknown	/img_samsung SM-J
20210925_185121.mp4				2022-01-21 16:00:48 ICT	2022-01-21 16:00:48 ICT	2022-01-21 16:00:48 ICT	2022-01-21 16:00:48 ICT	8079	Unallocated	Allocated	unknown	/img_samsung SM-J
Screenshot_2022-01-21-20-44-38.png				2022-01-21 21:19:23 ICT	2022-01-21 21:19:23 ICT	2022-01-21 21:19:23 ICT	2022-01-21 21:19:23 ICT	1143	Unallocated	Allocated	unknown	/img_samsung SM-J

Figure 12. Data finding Transfer Proof Photos in Deleted MiChat Conversations

Figure 12 shows During the Autopsy data check, it was found that there was evidence in the form of picture or images file the transfer of transaction for online prostitution services via MiChat messages.

2.2.3.3 *DB Browser for SQLite*

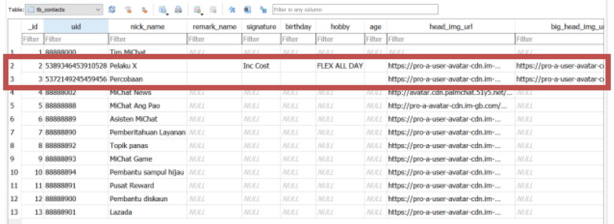


Table: tb_contacts

	_id	uid	nick_name	remark_name	signature	birthday	hobby	age	head_img_url	big_head_img_url
1	1	88888000	Tim MiChat	NULL	NULL	NULL	NULL	NULL	NULL	NULL
2	2	5389346453910528	Pelaku X		Inc Cost		FLEX ALL DAY		https://pro-a-user-avatar-cdn.im-...	https://pro-a-user-avatar-c
3	3	5372149245459456	Percobaan						https://pro-a-user-avatar-cdn.im-...	https://pro-a-user-avatar-c
4	4	88888002	MiChat News	NULL	NULL	NULL	NULL	NULL	http://avatar.cdn.palmchat.51y5.net/...	NULL
5	5	88888888	MiChat Ang Pao	NULL	NULL	NULL	NULL	NULL	http://pro-a-avatar-cdn.im-gb.com/...	NULL
6	6	88888889	Asisten MiChat	NULL	NULL	NULL	NULL	NULL	https://pro-a-user-avatar-cdn.im-...	NULL
7	7	88888890	Pemberitahuan Layanan	NULL	NULL	NULL	NULL	NULL	https://pro-a-user-avatar-cdn.im-...	NULL
8	8	88888892	Topik panas	NULL	NULL	NULL	NULL	NULL	https://pro-a-user-avatar-cdn.im-...	NULL
9	9	88888893	MiChat Game	NULL	NULL	NULL	NULL	NULL	https://pro-a-user-avatar-cdn.im-...	NULL
10	10	88888894	Pembantu sampul hijau	NULL	NULL	NULL	NULL	NULL	https://pro-a-user-avatar-cdn.im-...	NULL
11	11	88888891	Pusat Reward	NULL	NULL	NULL	NULL	NULL	https://pro-a-user-avatar-cdn.im-...	NULL
12	12	88888900	Pembantu diskaun	NULL	NULL	NULL	NULL	NULL	https://pro-a-user-avatar-cdn.im-...	NULL
13	13	88888901	Lazada	NULL	NULL	NULL	NULL	NULL	https://pro-a-user-avatar-cdn.im-...	NULL

Figure 13. Contact Data Table Obtained with DB Browser for SQLite tools

Figure 13 shows one of the tables from the database from MiChat Massager that was successfully obtained, namely is the id_contact table, the table shows the contact information data contained in the MiChat application and successfully stored in the database. One of the columns in the data, namely thenick_name shows the name of user that connect with the smartphone and head_image_url column can be opened to display the user's profile photo.

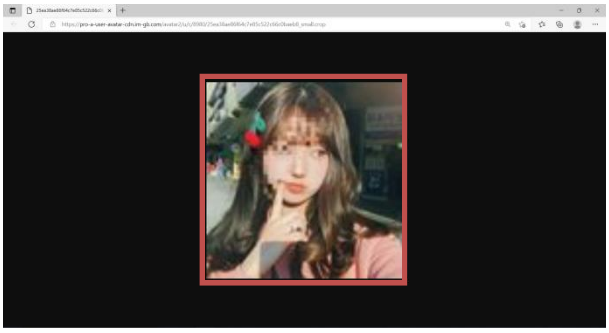


Figure 14. Display the Perpetrator's Profile Photo from the Database

Figure 14 shows the data results obtained from DB Browser for SQLite in the id_contact table in the head_image_url column which is directly directed to the browser.

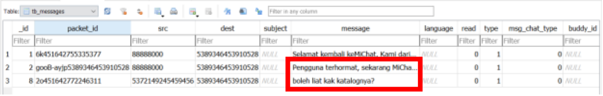


Table: tb_messages

	_id	packet_id	src	dest	subject	message	language	read	type	msg_chat_type	buddy_id
1	1	6k451642755335377	88888000	5389346453910528	NULL	Selamat kembali keMiChat, Kami dari...	NULL	0	1	0	NULL
2	2	gooB-ayjp5389346453910528	88888000	5389346453910528	NULL	Pengguna terhormat, sekarang MiCha...	NULL	0	1	0	NULL
3	8	2o451642772246311	5372149245459456	5389346453910528	NULL	boleh liat kak katalognya?	NULL	0	1	0	NULL

Figure 15. Message Data that has not been Deleted

Figure 15 shows the database from MiChatmessager in the table name tb_messagechecked through DB Browser for SQLite only shows messages that are still in database and haven't been deleted and doesn't store data regarding messages that have been deleted.

2.2.4 *Report*

The reporting stage is the last in the National Institute of Standards and Technology (NIST) method. The reporting process will report all the results of the analysis of the evidence found in the previous process [26]. 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, an explanation of the forensic process, and data from the use of forensic tools.

2.2.5 *Result*

The final results that can be processed from the MiChat service research use several tools to find data on the perpetrator's smartphone. The results obtained from the MOBILedit Forensic Express tool managed to find image and audio data. Autopsy tools succeeded in obtaining image data from the conversation. DB Browser for SQLite managed to get account data information and remaining messages that have not been deleted from the phone. Data Viewer CSV is very useful to make it easier to search smartphone data. Tests that have been carried out with various tools obtained data search reports generated from MOBILedit Forensic Express, Autopsy and DB Browser for SQLite.

The results of the analysis obtained from the forensic process using forensic tools can be shown in Table 2.

Table 2. Comparison of Evidence Found obtained from Several Tools

No	Digital Evidence	Forensic Tools		
		MOBILedit Forensic Express	Autopsy	DB Browser for SQLite
1	Deleted Text Message	-	-	-
2	UnDeleted Text Messages	-	-	√
3	Profile Picture	√	-	√
4	Image in conversation	√	√	-
5	Audio	√	√	-

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, voice messages, messages that have not been deleted), and account information on MiChat services such as profile photos of perpetrators/victims and account information in database. The use of the DB Browser forensic tool for SQLite is to open the result database file been captured, and successfully found some evidence.

Table3. The Findings of Evidence

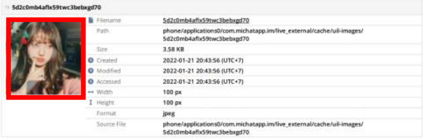
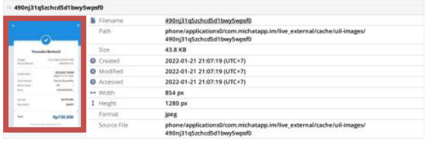
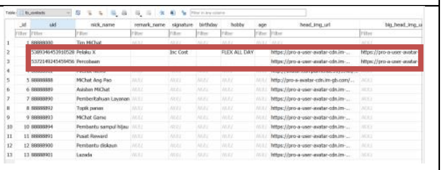
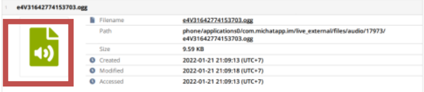
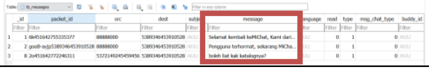
Digital Evidence	Findings
Images/Photo profile	 5d2c0mb4aflx59twc3bebxgd70 Filename 5d2c0mb4aflx59twc3bebxgd70 Path phone/applications0/com.michatapp.im/live_external/cache/uil-images/5d2c0mb4aflx59twc3bebxgd70 Size 3.58 KB Created 2022-01-21 20:43:56 (UTC+7) Modified 2022-01-21 20:43:56 (UTC+7) Accessed 2022-01-21 20:43:56 (UTC+7) Width 100 px Height 100 px Format jpeg Source File phone/applications0/com.michatapp.im/live_external/cache/uil-images/5d2c0mb4aflx59twc3bebxgd70
Images in Deleteted Conversations	 490nj31q5zchcd5d1bwy5wpsf0 Filename 490nj31q5zchcd5d1bwy5wpsf0 Path phone/applications0/com.michatapp.im/live_external/cache/uil-images/490nj31q5zchcd5d1bwy5wpsf0 Size 43.8 KB Created 2022-01-21 21:07:19 (UTC+7) Modified 2022-01-21 21:07:19 (UTC+7) Accessed 2022-01-21 21:07:19 (UTC+7) Width 854 px Height 1280 px Format jpeg Source File phone/applications0/com.michatapp.im/live_external/cache/uil-images/490nj31q5zchcd5d1bwy5wpsf0
Account Information	 Table: fb_contacts _id uid nick_name remark_name signature birthday hobby age head_img_url big_head_img_u 1 1 88888000 Tim MiChat NULL NULL NULL NULL NULL NULL NULL 2 5389346453910528 Pelaku X Inc Cost FLEX ALL DAY https://pro-a-user-avatar-cdn.im-... https://pro-a-user-avatar 3 5372149245459456 Percobaan https://pro-a-user-avatar-cdn.im-... https://pro-a-user-avatar 4 [illegible] 5 5 88888888 MiChat Ang Pao NULL NULL NULL NULL NULL http://pro-a-avatar-cdn.im-gb.com/... NULL 6 6 88888889 Asisten MiChat NULL NULL NULL NULL NULL https://pro-a-user-avatar-cdn.im-... NULL 7 7 88888890 Pemberitahuan Layanan NULL NULL NULL NULL NULL https://pro-a-user-avatar-cdn.im-... NULL 8 8 88888892 Topik panas NULL NULL NULL NULL NULL https://pro-a-user-avatar-cdn.im-... NULL 9 9 88888893 MiChat Game NULL NULL NULL NULL NULL https://pro-a-user-avatar-cdn.im-... NULL 10 10 88888894 Pembantu sampul hijau NULL NULL NULL NULL NULL https://pro-a-user-avatar-cdn.im-... NULL 11 11 88888891 Pusat Reward NULL NULL NULL NULL NULL https://pro-a-user-avatar-cdn.im-... NULL 12 12 88889900 Pembantu diskaun NULL NULL NULL NULL NULL https://pro-a-user-avatar-cdn.im-... NULL 13 13 88889901 Lazada NULL NULL NULL NULL NULL https://pro-a-user-avatar-cdn.im-... NULL
Voice	 e4V31642774153703.ogg Filename e4V31642774153703.ogg Path phone/applications0/com.michatapp.im/live_external/files/audio/17973/e4V31642774153703.ogg Size 9.59 KB Created 2022-01-21 21:09:13 (UTC+7) Modified 2022-01-21 21:09:18 (UTC+7) Accessed 2022-01-21 21:09:13 (UTC+7)
Undeleted Massage	 Table: fb_messages _id packet_id src dest subje message language read type msg_chat_type buddy_id 1 1 6k4516427553335377 88888000 5389346453910528 NULL Selamat kembali keMiChat, Kami dari... NULL 0 1 0 NULL 2 2 gooB-ayjp5389346453910528 88888000 5389346453910528 NULL Pengguna terhormat, sekarang MiCha... NULL 0 1 0 NULL 3 8 2o4516427772246311 5372149245459456 5389346453910528 NULL boleh liat kak katalognya? NULL 0 1 0 NULL

Table 3 shows the evidence findings. Username of the perpetrator (Pelaku X) and victim (Percobaan) in a 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

Digital data on the MiChat application that has been deleted cannot be fully recovered,The data that can be found from the tool used is a message in the form of a photo of the user's profile, proof of a transaction, a voice message, user data of the linked MiChat account, and the time the transaction occurred.The MOBILedit Forensic Express tool provides an accuracy index value of 60%, higher than Autopsy and DB Browser for SQLite with a value of 40%. For further research, it is hoped that you can use other or new tools, and 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] M. Ramadhan, and I. Riadi. 2019. Forensic WhatsApp-based Android using the National Institute of Standard Technology (NIST) Method. International Journal of Computer Applications, 177(8), 1-7.

[3] M. T. A, A. Iriani, and D. H. F. Manongga. (2018). Analysis of the Distribution Pattern of Pornography on Social Media with Social Network Analysis, no 1 (9). Journal of Buana Informatics.

[4] Hariani. (2021). Web Browser Exploration In Searching Digital Evidence Using Sqlite. Journal of INSTEK (Informatics Science and Technology), 6(1), 66. https://doi.org/10.24252/instek.v6i1.18638.

[5] M. A. Yaqin, T. A. Cahyanto, andN. Q Fitriyah. (2021). Live Memory Acquisition Method for Searching Digital Artifacts of Laptop Memory Devices Based on Simulation of Cybercrime Cases. BIOS: Journal of Information Technology and Computer Engineering, 2(2), 87-94. https://doi.org/10.37148/bios.v2i2.28.

[6] P. Widiandana, I. Riadi, and Sunardi. 2019. Analysis of cyberbullying forensic investigations on Whatsapp Messenger using the NIST method. In: National Seminar on Technology, Faculty of Engineering, Univ. Krisnadwipayana. https://jurnal.teknikunkris.ac.id/index.php/semnastek2019/article/view/308.

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

[8] I. Riadi, R. Umar, and A. Firdonsyah, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," *Int. J. Comput. Sci. Inf. Secure.*, vol. 15, no. 5, pp. 3–8, 2017.

[9] Casey, E. (2004) "Digital Evidence and Computer Crime", 2nd ed., p. 20.

[10] S. Marini, "Digital Forensic Studies in Regulation in Indonesia" *Semin. Nas. Energi Tek*, pp. 103–106, 2018.

[11] W. Jansen, and R. Ayers. (2007), Guidelines on Cell Phone Forensics, Special Publication (NIST SP),

National Institute of Standards and Technology, Gaithersburg, MD (Accessed March 18, 2021).

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

[13] P. L. Pendit. (1992). "The Meaning of Information: Continuation of a Debate," in Indonesian Librarianship: Potential and Challenges, eds. Antonius Bangun et al. Jakarta: Kesaint-Blanc.

[14] S. Chamidi. (2004). "Relationship between Educational Data and Information and Educational Planning," Journal of Education and Culture (48) 10, p. 314.

[15] S. H. Situmorang, S. H. (2010). Data Analysis for Management and Business Research. Medan: USU Press.

[16] K. Widatama, "Digital Evidence Storage Cabinet Concept Using XML Language Structure" no. September, pp. 8–14, 2017.

[17] A. Ivanović, The Way of Handling Evidence of Criminal Offences of Computer Crime. 2018.

[18] B. N. Arief (2006). Mayantara Crime: The Development of Cyber Crime Studies In Indonesia. PT Raja Grafindo Persada: Jakarta, p. 42.

[19] F. Sulianta (2010) CyberPorn - Business or Crime. PT Elex Media Komputindo: Jakarta.

[20] 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.

[21] A. Yudhana, I. Riadi, and I. Anshori, "Facebook Messenger Digital Evidence Analysis Using the NIST Method" *It J. Res. Dev.*, vol. 3, no. 1, pp. 13–21, 2018, doi: 10.25299/itjrd.2018.vol3(1).1658.

[22] 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.[23] A. M. Yusuf. (2014). Quantitative, Qualitative, & Joint Research. Jakarta: Kencana.

[23] 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.

[24] 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.

[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] 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.