IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 13, No. 1, February, 2023, pp. 11-19
Journal homepage: http://iieta.org/journals/ijsse

Mobile Forensic Tools for Digital Crime Investigation: Comparison and Evaluation

Imam Riadi[1*], Anton Yudhana[2], Galih Pramuja Inngam Fanani[3]

[1] Department of Information System, Universitas Ahmad Dahlan, Yogyakarta 55164, Indonesia
[2] Department of Electrical Engineering,Universitas Ahmad Dahlan, Yogyakarta 55164, Indonesia
[3] Master Program of Informatics, Universitas Ahmad Dahlan, Yogyakarta 55164, Indonesia

Corresponding Author Email: imam.riadi@is.uad.ac.id

https://doi.org/10.18280/ijsse.130102

Received: 2 August 2022
Accepted: 7 January 2023

Keywords:
digital forensic, DFRWS, mobile forensic, Michat, smartphone

ABSTRACT

The advancement of new technology is quickening. Because of the features and applications available on mobile devices, smartphones are gradually taking over the role of computers. One of them is a multi-platform instant messaging application with various features that can bring people together, but the negative aspect is that it is used to commit digital crimes. Digital evidence is required in the investigation of digital crimes, In order to obtain digital evidence, a set of forensic tools is required to carry out the forensic process of physical evidence. The goal of this research is to describe and contrast the forensic process. These tools are currently based on digital evidence obtained through the stages of the Digital Forensic Research Workshop. MEF, DB4S, OFD, and FMF are the forensic tools used in this study. According to the findings, FMF has the highest extraction capability for obtaining digital evidence, OFD has advantages in terms of data acquisition features, and MFE has advantages in identification, physical evidence preservation, and cloning.

1. INTRODUCTION

Smartphones are growing more advanced with every new technological development. Smartphones are gradually taking over the role of computers due to the features and applications available on mobile devices [1]. The importance of using smartphones in the digital era is that it makes it easier for people to exchange information around the world. Practicality, portability, and many application features are important factors. However, the greater the advancement of smartphones, the greater the negative impact if not balanced with responsibility [2, 3]. Android-based smartphones are one of the most popular types of smartphones and have many users. Due to the very high demand for mobility, on the other hand, the price is also very varied. Figure 1 shows the number of smartphone users from the last 7 years in the world. It can be seen that the number of smartphone users has increased significantly every year. Starting in 2022, the number of smartphone users will increase by around 6,000 million users in the world [4]. Along with the development of smartphone use followed by increasingly varied social media, the choice of using instant messengers is also increasing. Examples include Whatsapp, LINE, Telegram, and Signal [5-7]. However, more and more activities conducted using instant messenger features have the potential to be exploited by users who are not responsible for cybercrime crimes [8-10]. Data based on NUMBEO shows that Venezuela is a country with the highest crime index in the world, reaching 83.16, and Indonesia occupies the 15th position in the crime rate in Asia, with an index value reaching 46.06 above Vietnam out of a total of 44 registered Asian countries [11].

In Indonesia, there are several cases of crimes involving short messaging applications. One of them is the MiChat application, which is very popular in Indonesia with 50 million downloads on Google Play [12, 13]. Michat functionally helps communicate among users, such as through various media sharing or chatting [14, 15]. Michat is often associated with abusive activity for criminal purposes. If investigators find evidence of criminal infringement on a MiChat message, they will look at the messaging service artifact to find out what happened [16, 17]. Various cases involving the MiChat application in Indonesia [18-22] are as shown in Table 1. These are cases in the last 5 years that occurred in Indonesia through the Michat application.

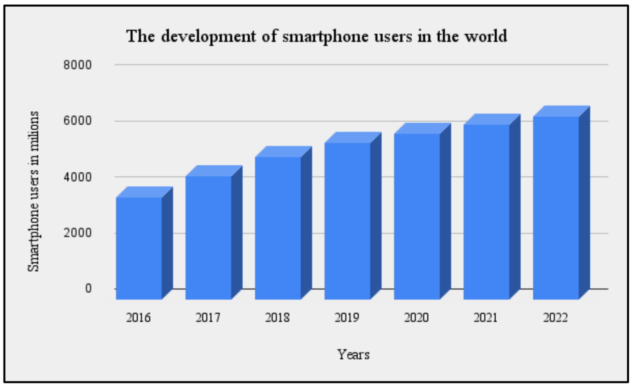


Figure 1. Development of smartphone usage from 2016 to 2022 in the world

Based on the problems described in Table 1. It is necessary to have forensic handling, especially mobile forensics, in helping to solve crime cases [23-25]. Mobile forensic tools are needed that can help investigators to extract artifacts, decrypt, and analyze data in dealing with cybercrime cases involving mobile devices [26-28]. Investigators also need to use supporting methods to assist the handling process in a structured and efficient manner.

The goal of this research was to compare the effectiveness of forensic tools for extracting artifacts from messages, contacts, images, videos, audio, and web caches. To support Michat application testing on Android-based smartphone devices, the Digital Forensics Research Workshop (DFRWS) method was chosen. MOBILedit Forensic Express (MFE), DB Browser for SQLite (DB4S), Oxygen Forensic Detective (OFD), and Final Mobile Forensic are the tools used (FMF). The results of this study are in the form of digital evidence in the form of text chat files, contacts, images, audio, video, and web caches. Based on the six pieces of evidence, the most efficient forensic tools will be determined so that they can assist investigators in handling cases involving digital evidence quickly and validly.

2. LITERATURE REVIEW

There are many challenges in the field of mobile forensics, one of which is limited resources, in the sense that the rapid development of mobile technology and the increase in the number of smartphone devices are not matched by the development of mobile forensic technology and the development of mobile forensic technology [29, 30]. Existing forensic tools to overcome these challenges need to do a comparative analysis of instant messaging features and forensic tools [31, 32]. Comparisons are not only on the performance of forensic tools but also on forensic frameworks such as the National Institute of Justice (NIJ) [26, 33]. Integrated Digital Forensic Investigation Framework (IDFIF) [34] dan Digital Forensics Research Workshop (DFRWS) [35, 36].

In a study, Sutikno et al. [37] compared instant messaging features. An investigation has been launched into the three services, WhatsApp, Viber, and Telegram. The result of this study, in third place, is that Viber has a very functional security feature as its main feature. In second place, Telegram provides synchronization capabilities, lightning-fast service, reliable backup, and enhanced security features. The first place is WhatsApp because it is the most popular among smartphone users in the world, accounting for about 60% of the total. Despite the fact that WhatsApp dominates the social media space due to its simplicity and is backed by the giant that is Facebook, Telegram offers a better platform.

Another study conducted by Dogan and Akbal [38] using Oxygen Forensic Suite 2014 and MOBILedit Forensics revealed that each forensic tool has advantages and disadvantages. Digital crime cases involving smartphone devices require the use of a variety of forensic tools with varying capabilities. According to the findings of this study, MOBILedit Forensics has a run time advantage, while Oxygen Forensic Suite 2014 has an advantage in terms of artifact analysis.

In a study, Osho and Ohida compared the performance of four different mobile forensic tools to obtain from android-based smartphones with a concentration on deleted data [39]. The purpose of this study is to determine how various types of data artifacts that exist in various types of mobile phones can be extracted in different ways using AccessData FTK imager, Encase, MOBILedit, and Oxygen Forensic Suite.

Table 1. MiChat cases that occurred in Indonesia

No.	Year	Case
1.	2022	Dissemination of identity and immoral documents via MiChat in West Sumatra
2.	2021	Drug trafficking through the MiChat Application in West Java and East Java
3.	2020	Online fraud via MiChat in Samarinda
4.	2019	Human trafficking via Michat in North Sulawesi
5.	2018	The murder of Sisca Icun Sulastri by Hidayat who met via Michat in South Jakarta in Cimahi

Table 2. Summary of previous research

Name	Title	Tools	Results
(Sutikno et al, 2019)	WhatsApp, viber and telegram: Which is the best for instant messaging?	WhatsApp, Viber, dan Telegram	WhatsApp is the most popular among smartphone users in the world, accounting for about 60%, as simplicity dominates the social media space.
(Dogan and Akbal, 2017)	Analysis of mobile phones in digital forensics	Oxygen Forensic Suite 2014 dan MOBILedit Forensics	MOBILedit Forensics has an advantage in terms of run time, while Oxygen Forensic Suite 2014 has an advantage in terms of artifact analysis.
(Osho and Ohida, 2019)	Comparative Evaluation of Mobile Forensic Tools	menggunakan Cellebrite UFED dan XRY	XRY is better than Cellebrite UFED at acquiring most types of artifacts, while Cellebrite UFED is better at maintaining the integrity of digital evidence.
(Padmanabhan et al, 2020)	Comparative analysis of commercial and open source mobile device forensic tools	The Sleuth Kit (TSK) Autopsy, SANS SIFT, MOBILedit Forensics, and Cellebrite UFED	Open source forensic tools have advantages in user numbers, flexibility, GUI-based capabilities, logging capabilities, and good error tolerance.
(Riadi et al, 2022)	Mobile Forensic Tools for Digital Crime Investigation: Comparison and Evaluation	MOBILedit Forensic Express (MFE), DB Browser for SQLite (DB4S), Oxygen Forensic Detective (OFD), and Final Mobile Forensic are the tools used (FMF)	This study will compare mobile forensic tools and discover their strengths to find the best combination of tools.

Padmanabhan et al. [40], compared and analyzed proprietary and open source forensic tools. The tools compared were The Sleuth Kit (TSK) Autopsy, SANS SIFT, MOBILedit Forensics, and Cellebrite UFED. According to the findings of this study, open source forensic tools have advantages in terms of user count, flexibility in terms of use with console commands or GUI-based applications, logging capabilities, and error tolerance. Meanwhile, proprietary forensic tools outperform generic forensic tools in terms of processing speed, data extraction accuracy, analytical skills, and ability to recover deleted data.

To obtain digital evidence from the MiChat App, this investigative process necessitates an analytical structure and a set of forensic tools. In this study, the researcher will attempt to describe the investigative steps taken to obtain digital evidence as well as conduct a comparative analysis of the performance of forensic tools based on the digital evidence and digital features obtained. Table 2 is a summary of previous research.

2.1 Mobile digital and mobile forensics

Digital forensics is the use of computer science and technology for the purpose of obtaining digital evidence that can be used against perpetrators. Mobile Forensic is one of many areas of Digital Forensic [41].

Mobile Forensics is the science that performs the process of recovering digital evidence from mobile devices in an appropriate manner under forensic conditions. Mobile forensics is required as mobile-based services become more popular and attract more users. The popularity of mobile computing and mobile commerce is increasing the demand for mobile transactions [42, 43].

The difficulty in conducting cellular transactions stems from the large number of cellular service providers with fast and secure networks. To protect users from abuse by irresponsible individuals, online transactions made via mobile devices must be highly secure.

2.2 Digital evidence

If digital evidence is not handled properly, it will become fragile, changeable, and vulnerable. Any type of alteration involving digital evidence will either lead to incorrect conclusions or become obsolete. Determination of the steps taken in the acquisition of digital evidence in accordance with [44, 45]:

1. Digital media as evidence.
2. Physical arrangement of digital storage media.
3. Use Write-Protect, hashing, and other techniques to ensure the integrity and authenticity of digital evidence.
4. Only authorized people have access to digital evidence, and no one may use electromagnetic devices near digital evidence.
5. Storage conditions and media configuration documentation.
6. Duplicate/imaging digital evidence procedures and devices used for digital forensic data acquisition are substandard.
7. Information documentation and digital device configuration.

2.3 Oxigen forensic detective

OFD is data extraction and analysis software for mobile phones, smartphones, and tablets. The tool provides a number of hash algorithms, one of which can be selected for each investigation case. The OFD can also provide general information about the smartphone and the networks connected to it. Another useful feature of this tool is the ability to recover all contacts, SMS, MMS, and user files [46, 24].

2.4 MOBILedit forensic express

MFE is a forensic tool that can perform both logical and physical acquisitions, similar to OFD. The software can obtain phone system information as well as other information such as contacts, text messages, and pictures. MOBILedit supports calendar, notes, reminders, raw app data, IMEI, operating system, firmware including SIM details (IMSI), ICCID, contact book, call history, text messages, multimedia files, and location area information [15, 47].

2.5 Cybercrime

Despite the fact that cybercrime is a popular and widely used term, there is no universally accepted standard definition of cybercrime. However, several organizations, including the United Nations, have begun to define cybercrime (United Nations). Cybercrime is defined by the United Nations as any illegal behavior committed through the provision of a computer system or system or network, including crimes such as illegal possession, provision, or distribution of information via a computer system or network [48, 49]. Cybercrime is defined as a crime committed with the use of information technology as an instrument or target, and digital forensics essentially answers the following questions: when, what, who, where, how, and why it is committed [25]. This is accomplished by employing a computer network as a tool or a computer as an object, for profit or not, and there are elements that can cause harm to others.

3. Material and Method

The goal of this research is to use the DFRWS method to evaluate and compare. Based on the features and the ability to find digital evidence according to predetermined parameters by measuring the level of accuracy.

3.1 Research subject

The subjects used in this study are mobile forensics tools used to identify MiChat applications on Android-based smartphones. The digital evidence contained in the MiChat application will be analyzed based on the parameters that have been determined.

3.2 Research Stages

This study uses the research steps conducted by DFRWS. The research phase consists of 6 stages as shown in Figure 2.

1. Identification: The investigator conducts an examination or identification to determine the need for investigation and the evidence carried out by the investigator.
2. Preservation: Investigators carry out maintenance to maintain digital evidence to ensure its authenticity and deny claims that the evidence has been destroyed.

3. Collection: During the collection stage, evidence will be collected, preserved, objects will be prepared, and research tools will be prepared.
4. Examination: The inspection stage will include the identification of data that can be used as evidence. After deciding which data to collect, the data collection process will be forensically tested.
5. Analysis: The collected data will be analyzed to find items that can be used as evidence, and then conclusions will be drawn.
6. Reporting: The final forensic step is to report the forensic activities from start to finish, as well as the results of the analysis, in the form of a written or oral report.

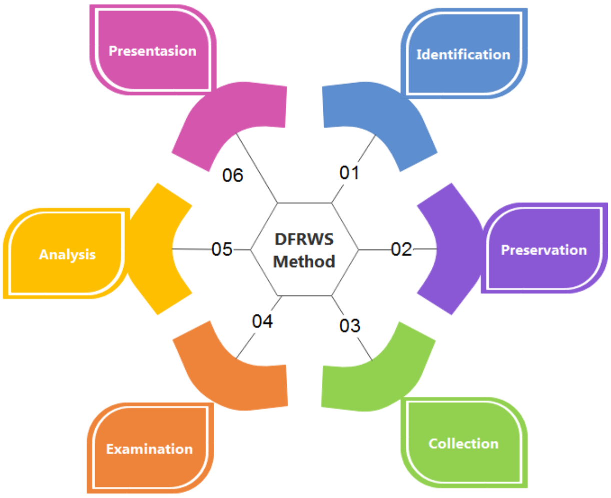


Figure 2. DFRWS forensic methodolog

3.3 Research tools

Table 3 shows the hardware and software used to test the extraction of MiChat artifacts from Android-based devices.

Tabel 3. Tools and devices for research

No.	Tools and Device	Version	Function
1.	Asus Zenfone C	Android Kitkat, Procesor Intel Atom	Smartphone devise for the experiment
2.	Laptop Asus K46 CM	Windows 7, 64 Bit, 4 GB RAM	A computer-aided extraction and analysis device
3.	USB Connector	Type Micro	USB connector is used to connect a smartphone device to a computer
4.	MiChat Messenger	1.4.126	Instant Messaging application
5.	MOBILedit Forensic Express	7.3.1	Physical Imaging
6.	DB Browser for SQLite	3.12.2	Analysi Data Base
5.	Oxygen Forensic Detective	12.3	Tool for extraction and analysis
6.	Final Mobile Forensic	v2019.07.05.	Tool for extraction and analysis
7.	Hashing Tools	1.2	Validation evidence digital

Based on Table 3, software and hardware used consist of one Asus Zenfone C smartphone device as an experimental device, an Asus laptop as a data extraction and data analysis device, a USB connector as a connecting medium between a smartphone installed with MiChat and an analysis laptop, and five forensic tools for physical imaging and data backup, database analysis, and further analysis.

3.4 Experiment simulation

The experiment was conducted in a closed and noise-free environment, so the smartphone device was set to airplane mode. The device will be unable to receive calls or messages from outside sources while in airplane mode. This is necessary to maintain the data's authenticity and integrity. The workstation is not connected to the Internet and is free of malware that could interfere with the test results. Figure 3 is an experimental simulation.

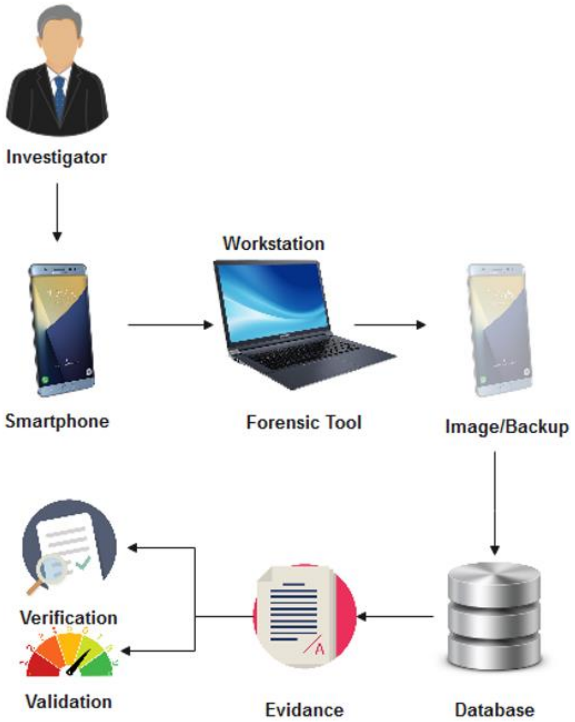


Figure 3. Experiment simulation

Figure 3. Illustrates the data acquisition simulation, and the process flow is as follows:

1. Investigators identify a Asus Zenfone C smartphone that is designated as physical evidence, which has the MiChat application installed, and maintenance or isolation of evidence is carried out so that the integrity of the data is safe and does not change.
2. Workstations that have been installed with forensic tools function for the process of collecting digital evidence by performing backups or imaging data using forensic tools, which will then analyze the database file.
3. Examination is done by extracting data from the database. The analysis stage is to find evidence that can be used as supporting evidence in the trial of a crime case.
4. The evidence that has been found will be validated for its authenticity and verified to determine whether the data is consistent with the case that occurred. After the process is complete, an evaluation is carried out to compare the

forensic tools that have been used, and from these results, it can help the investigation process in the future.

4. RESULT AND DISCUSSION

The DFRWS method's function is not restricted to retrieving relevant digital evidence as just a step in resolving digital crime submitted to court, but it can also be used in a comparative evaluation of the performance of forensic tools used. The findings of this study's comparative analysis of these forensic tools will be presented at the reporting stage. The following are the steps for collecting and analyzing data using the DFRWS method:

4.1 Identification

Identification determines which device to process. This study succeeded in identifying the Asus Zenfone C smartphone, which was used as physical evidence for the drug trafficking case that occurred. With some specifications in detail shown in Table 4.

Table 4. Identification results of Asus Zenfone C

Bukti Fisik	Spesifikasi	Information
	Manufacturer	Asus
	Product	Asus_Z007
	HW Revision	KVTA9L
	Platform OS	Android 4.4.2 KitKat
	Chipset	Intel Atom Z2520
	RAM	1 GB
	ADB Backup Password	1234
	IMEI	237876069027680
	Rooted	Yes
	Simcard	Yes

4.2 Preservation

The stage of isolating the smartphone from the telecommunications network (airplane mode). Quarantine processes must be in place to avoid anything that could compromise or affect digital evidence's integrity and disprove claims that evidence has been destroyed. After the isolation process, evidence backup will be carried out in the form of cloning or processing of evidence image files using equipment that clones smartphones into safes.

4.3 Collection

Table 5. MiChat application data backup information

Physical Imaging	Keterangan
Fine Name	Asus-ASUS_z007
Size	210 MB
Duration Imaging	1 hour 06 menit 38 sekon
Time Taken	23/01/2022, 16:22 WIB

At this stage, the collection of evidence is carried out to maintain the integrity of the physical and digital evidence so that it does not change. Many applications can be used for cloning or physical imaging. In this study, the Asus Zenfone C smartphone cloning process was carried out using MFE. The cloning process and results are as shown in Figure 4. In Table 5, information from the MiChat application data was successfully backed up.

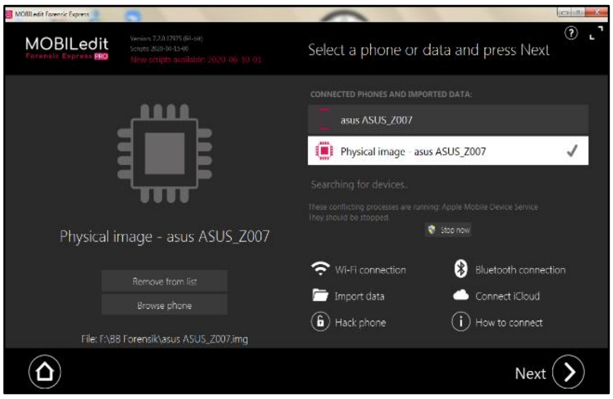
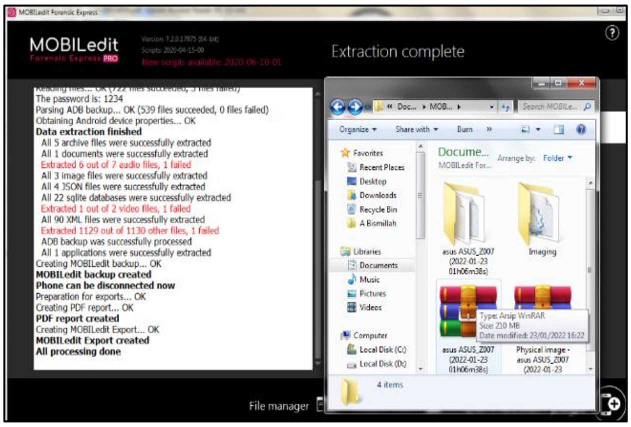

MOBILedit Forensic Express
MOBILedit
Forensic Express PRO
Version: 7.2.0.17975 (64-bit)
Scripts: 2020-04-15-00
New scripts available: 2020-06-10-01
Select a phone or data and press Next
CONNECTED PHONES AND IMPORTED DATA:
asus ASUS_Z007
Physical image - asus ASUS_Z007
Searching for devices.
These conflicting processes are running: Apple Mobile Device Service
They should be stopped.
Stop now
Physical image - asus ASUS_Z007
Remove from list
Browse phone
File: F:\BB Forensik\asus ASUS_Z007.img
Wi-Fi connection
Bluetooth connection
Import data
Connect iCloud
Hack phone
How to connect
Next

Figure 4. Physical Imaging using MFE

4.4 Examination

Examination is the stage of examining the data collected from the imaging process by extracting artifacts. The selection of artifacts is very important considering that there are many types of extracted artifacts, such as log files and databases, that can be analyzed further. The investigation process uses forensic techniques and tools to analyze and process data evidence so that the digital evidence sought can be found. Other things, such as filtering hash files, also need to be done to validate the authenticity of digital evidence. In Figure 5, investigators carry out the imaging file extraction process using the MFE tool. In Table 6, types of digital evidence that will be extracted from physical evidence have been determined and will be used as parameters for this research.



```
Reading files... OK (722 files succeeded, 3 files failed)
The password is: 1234
Parsing ADB backup... OK (539 files succeeded, 0 files failed)
Obtaining Android device properties... OK
Data extraction finished
  All 5 archive files were successfully extracted
  All 1 documents were successfully extracted
  Extracted 6 out of 7 audio files, 1 failed
  All 3 image files were successfully extracted
  All 4 JSON files were successfully extracted
  All 22 sqlite databases were successfully extracted
  Extracted 1 out of 2 video files, 1 failed
  All 90 XML files were successfully extracted
  Extracted 1129 out of 1130 other files, 1 failed
  ADB backup was successfully processed
  All 1 applications were successfully extracted
Creating MOBILedit backup... OK
MOBILedit backup created
Phone can be disconnected now
Preparation for exports... OK
Creating PDF report... OK
PDF report created
Creating MOBILedit Export... OK
MOBILedit Export created
All processing done
```

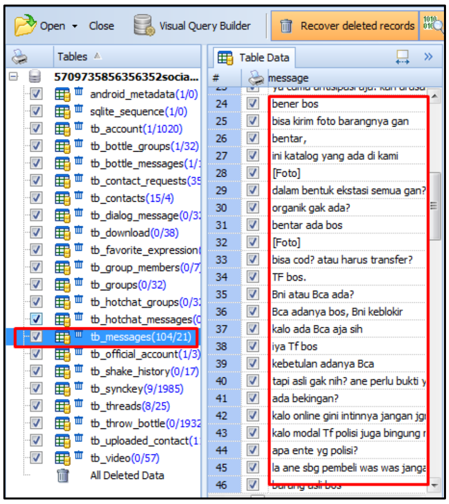
Figure 5. Imaging file extraction process

Table 6. Parameters of digital evidence in research

No.	Digital evidence	Description
1.	Contact	A list of Michat contact, including number
2.	Chat	Data from a MiChat user's conversation
3.	Images	Images file transferred among MiChat User
4.	Audio	Audio file transferred among MiChat User
5.	Video	Video file transferred among MiChat User
6.	Cache web	share a web link in a Michat conversation

4.5 Analysis

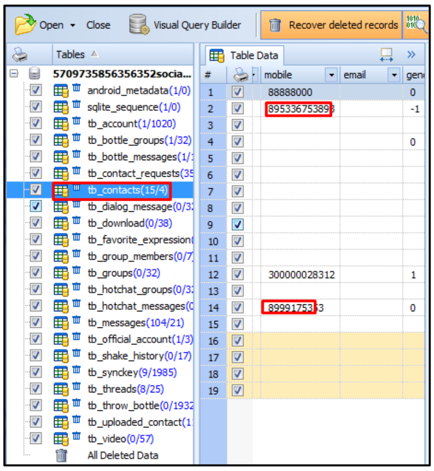
Analysis is a process in which the results of the examination are viewed as a whole in order to obtain digital evidence. This stage restricts the search process to specific points that are linked to specific data or applications. The MiChat application is the search limitation in this study. The analysis stage carried out by OFD resulted in a data conversation with one of the MiChat contacts with indications of drug trafficking transactions, as shown in Figure 6 and Figure 7. Analysis of MiChat contacts suspected of being the perpetrator's phone number The offender profile of a girl is shown in Figure 8.



5709735856356352socia...
- android_metadata(1/0)
- sqlite_sequence(1/0)
- tb_account(1/1020)
- tb_bottle_groups(1/32)
- tb_bottle_messages(1/
- tb_contact_requests(35
- tb_contacts(15/4)
- tb_dialog_message(0/3
- tb_download(0/38)
- tb_favorite_expression
- tb_group_members(0/7
- tb_groups(0/32)
- tb_hotchat_groups(0/3
- tb_hotchat_messages(
- tb_messages(104/21)
- tb_official_account(1/3)
- tb_shake_history(0/17)
- tb_synckey(9/1985)
- tb_threads(8/25)
- tb_throw_bottle(0/1932
- tb_uploaded_contact(1
- tb_video(0/57)
- All Deleted Data

#		message
24	☑	bener bos
25	☑	bisa kirim foto barangnya gan
26	☑	bentar,
27	☑	ini katalog yang ada di kami
28	☑	[Foto]
29	☑	dalam bentuk ekstasi semua gan?
30	☑	organik gak ada?
31	☑	bentar ada bos
32	☑	[Foto]
33	☑	bisa cod? atau harus transfer?
34	☑	TF bos.
35	☑	Bni atau Bca ada?
36	☑	Bca adanya bos, Bni keblokir
37	☑	kalo ada Bca aja sih
38	☑	iya Tf bos
39	☑	kebetulan adanya Bca
40	☑	tapi asli gak nih? ane perlu bukti y
41	☑	ada bekingan?
42	☑	kalo online gini intinnya jangan jg
43	☑	kalo modal Tf polisi juga bingung r
44	☑	apa ente yg polisi?
45	☑	la ane sbg pembeli was was janga
46	☑	barang asli bos

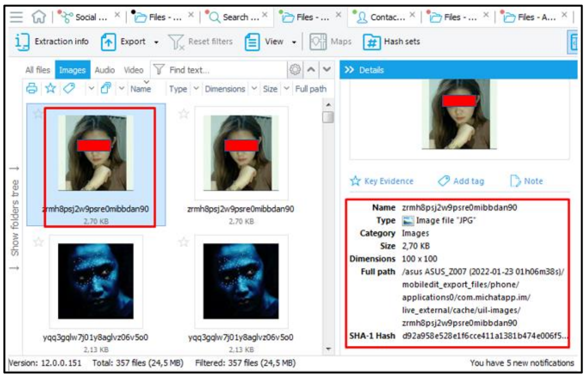
Figure 6. Digital text chat and contact data on OFD tools



5709735856356352socia...
- android_metadata(1/0)
- sqlite_sequence(1/0)
- tb_account(1/1020)
- tb_bottle_groups(1/32)
- tb_bottle_messages(1/
- tb_contact_requests(35
- tb_contacts(15/4)
- tb_dialog_message(0/3
- tb_download(0/38)
- tb_favorite_expression
- tb_group_members(0/7
- tb_groups(0/32)
- tb_hotchat_groups(0/3
- tb_hotchat_messages(
- tb_messages(104/21)
- tb_official_account(1/3)
- tb_shake_history(0/17)
- tb_synckey(9/1985)
- tb_threads(8/25)
- tb_throw_bottle(0/1932
- tb_uploaded_contact(1
- tb_video(0/57)
- All Deleted Data

#		mobile	email	gen
1	☑	88888000		0
2	☑	895336753898		-1
3	☑			
4	☑			0
5	☑			
6	☑			
7	☑			
8	☑			
9	☑			
10	☑			
11	☑			
12	☑	300000028312		1
13	☑			
14	☑	8999175333		0
15	☑			
16	☑			
17	☑			
18	☑			
19	☑			

Figure 7. Digital text chat and contact data on OFD tools



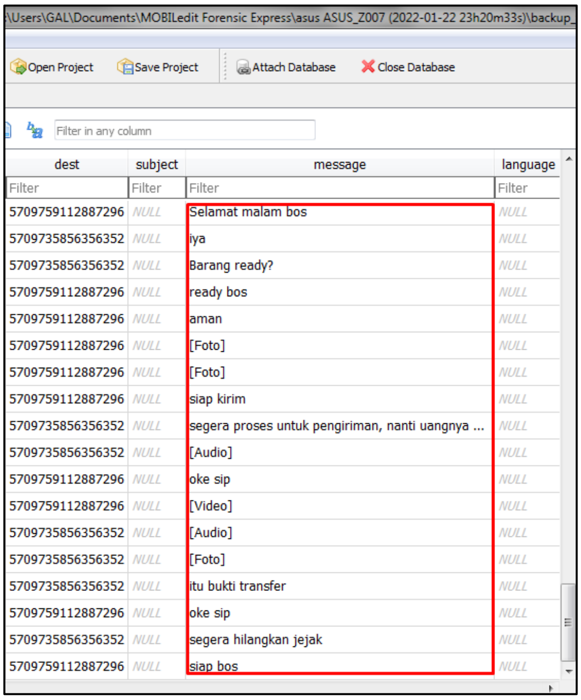
zrmh8psj2w9psre0mibbdan90 2,70 KB
zrmh8psj2w9psre0mibbdan90 2,70 KB
yqq3gqlw7j01y8aglvz06v5o0 2,13 KB
yqq3gqlw7j01y8aglvz06v5o0 2,13 KB

Name	zrmh8psj2w9psre0mibbdan90
Type	Image file "JPG"
Category	Images
Size	2,70 KB
Dimensions	100 x 100
Full path	/asus ASUS_Z007 (2022-01-23 01h06m38s)/mobiledit_export_files/phone/applications0/com.michatapp.im/live_external/cache/uil-images/zrmh8psj2w9psre0mibbdan90
SHA-1 Hash	d92a958e528e1f6cce411a1381b474e006f5...

Version: 12.0.0.151 Total: 357 files (24,5 MB) Filtered: 357 files (24,5 MB) You have 5 new notifications

Figure 8. Images data on OFD tools

Based on the results of the analysis using OFD tools, there are indications of drug trafficking transactions. To get more detailed data, an analysis of the next tool is carried out. The results of the examination using the DB4S tool did not produce images or photos due to software limitations, but the conversation data was obtained completely. The analysis shows exactly the same conversation as the one shown in OFD. Figure 9 shows the outcomes of conversational analysis using DB4S.



\Users\GAL\Documents\MOBILedit Forensic Express\asus ASUS_Z007 (2022-01-22 23h20m33s)\backup_

dest	subject	message	language
Filter	Filter	Filter	Filter
5709759112887296	NULL	Selamat malam bos	NULL
5709735856356352	NULL	iya	NULL
5709735856356352	NULL	Barang ready?	NULL
5709759112887296	NULL	ready bos	NULL
5709759112887296	NULL	aman	NULL
5709759112887296	NULL	[Foto]	NULL
5709759112887296	NULL	[Foto]	NULL
5709759112887296	NULL	siap kirim	NULL
5709735856356352	NULL	segera proses untuk pengiriman, nanti uangnya ...	NULL
5709735856356352	NULL	[Audio]	NULL
5709759112887296	NULL	oke sip	NULL
5709759112887296	NULL	[Video]	NULL
5709735856356352	NULL	[Audio]	NULL
5709735856356352	NULL	[Foto]	NULL
5709735856356352	NULL	itu bukti transfer	NULL
5709759112887296	NULL	oke sip	NULL
5709735856356352	NULL	segera hilangkan jejak	NULL
5709759112887296	NULL	siap bos	NULL

Figure 9. Digital text chat data on DB4S tools

As for FMF tools, they are used to obtain digital data for audio, video, and web caches to complete the required data so that the objectives of this research can be achieved.

4.6 Presentasion

Presentation is the last stage in the DFRWS method. The presentation will be presented in two tables, one for software features and one for digital evidence obtained by each device. The results of the comparison based on features are as shown in Table 7.

Table 7. Comparison results of forensic tools features

Tools Feature	Mobil edit express	DB browser SQL	Oxigen forensic detectiv	Final mobile forensic
Android OS	√	-	√	√
Other OS	√	-	√	√
Support all apps	√	√	√	√
Timestamp	-	-	√	√
Digital forensic research workshop prosses support				
Identification	√	-	√	-
Preservation	√	-	√	√
Collection	√	-	√	√
Examination	√	-	√	√
Forensic analysis	-	√	√	√
Presentastion	√	-	√	√

According to the experimental results, the researchers used calculations with index numbers to determine the performance of each forensic tool. The index number is calculated as an overall score index, as shown in Eq 1.

$$par = \frac{\sum ar0}{\sum arT} \times 100\% \qquad (1)$$

Information:
Par=Index number as a percentage
ar0=Forensic Tools-obtained Evidence/Digital Artifacts
arTTotal Digital Evidence/Artifact

Based on the DFWRS method, OFD has a powerful advantage, by calculating the index number of each forensic tool using equation 1. OFD has the highest index score of 100 percent, MFE and FMF have index numbers of 80% and 90%, respectively. Comparison results based on digital evidence as shown in Table 8.

Table 8. Evaluate the capabilities of forensic tools based on digital evidence

No	MiChat Digital Evidence	Forensic Tools			
		Mobil Edit Express	DB browser SQL	Oxigen Forensic Detectiv	Final Mobile Forensic
1	Chat	-	√	√	√
2	Contact	-	√	√	√
3	Images	√	-	√	√
4	Audio	√	-	√	√
5	Video	√	-	√	√
6	Cache web	√	-	-	√

Table 8 shows the outcomes of the performance analysis performed on each forensic tool in relation to the digital evidence obtained. Using the same equation, OFD got a performance index score of 83.3%. MFE received a performance index score of 66.7%, FMF received a good score 100% on the performance index because it obtained most six categories of MiChat digital evidence.

4.7 Discussion

Based on an analysis of the comparison and evaluation of the capabilities of mobile forensic tools in handling digital crime cases through the MiChat application and by applying the DFRWS method, which is already qualified to handle digital evidence according to procedures from the initial stages of identification, preservation, collection, examination, analysis, and reporting, Analysis using four forensic tools, namely MFE, DB4S, OFD, and FMF, obtained evidence of text chat, contacts, images, audio, video, and web cache. The best forensic tool for acquiring evidence is FMF, with a success index of 100%, but it has the disadvantage that it takes a long time during the acquisition process. In terms of forensic features, OFD is more capable, but the weakness is that many features are locked, with an index score of 83.3%. This research contributes to the world of cybercrime involving smartphone devices and can later provide a reference to an investigator regarding the best mobile forensic tools. It can also be used to analyze crimes involving data loss or data recovery. Based on the differences from previous comparison studies of mobile forensic tools in handling evidence, especially Android-based applications on smartphones, the results of previous studies can be seen in Table 9.

5. Conclusions

Based Based on the discussion in Table 7. It is possible to conclude that, when comparing the capabilities of these four forensic tools, FMF tools have the highest index score of 100%, followed by OFD with an index score of 83.3%, and MFE with an index score of 83.3% and a score of 66.7%. MFE has a weakness in extracting digital chat evidence and MiChat contacts. However, in terms of data feature capabilities, OFD has the highest index score of 100%, while MFE and FMF have 88.9%. Based on the results, FMF has the best ability to obtain digital evidence, OFD has the best features, and MFE has the best physical evidence preservation and cloning. So it is hoped that in the future, this research can contribute new references for investigators handling cybercrime cases.

Table 9. Comparison of previous research with research that has been done

Name	Title	Results	advantages
(Osho and Ohida, 2019)	Comparative Evaluation of Mobile Forensic Tools	XRY is better than Cellebrite UFED at acquiring most types of artifacts, while Cellebrite UFED is better at maintaining the integrity of digital evidence.	Cellebrite UFED is better at maintaining the integrity of digital evidence so that the data does not change.
(Padmanabhan et al, 2020)	Comparative analysis of commercial and open source mobile device forensic tools	Open source forensic tools have advantages in user numbers, flexibility, GUI-based capabilities, logging capabilities, and good error tolerance.	Open-source forensic tools have the advantage of flexibility, easy-to-use GUI-based capabilities, and good logging capabilities.
(Riadi et al, 2022)	Mobile Forensic Tools for Digital Crime Investigation: Comparison and Evaluation	FMF outperforms OFD in terms of obtaining most digital evidence with timestamps and recovering deleted data. While OFD is better in the completeness of the features offered and has a modern, easy look, MEF has good physical imaging capabilities for data backup. DB4S only has the ability to extract database files.	Using four forensic tools with different capabilities so that it can provide an alternative combination of the best tools to acquire digital data.

REFERENCES

[1] Umar, R., Riadi, I., Zamroni, G.M. (2018). Mobile forensic tools evaluation for digital crime investigation. International Journal on Advanced Science Engineering and Information Technology, 8(3): 949-955. https://doi.org/10.18517/ijaseit.8.3.3591

[2] Buctot, D.B., Kim, N., Kim, S.H. (2021). Comparing the Mediating Effect of Adolescent Lifestyle Profiles on the Relationship between Smartphone Addiction and Health-related Quality of Life Among Male and Female Senior High School Students in the Philippines. International Journal of Mental Health and Addiction, https://doi.org/10.1007/s11469-021-00609-9

[3] Agrawal, A.K., Khatri, P., Sinha, S.R. (2018). Comparative study of mobile forensic tools. Advances in Data and Information Sciences, 38: 39-47. https://doi.org/10.1007/978-981-10-8360-0_4

[4] O'Dea, S. (2022). Number of smartphone subscriptions worldwide from 2016 to 2027. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. Accessed successfully on July 7th, 2022.

[5] Ichsan, A.N., Riadi, I. (2021). Mobile forensic on android-based IMO messenger services using Digital Forensic Research Workshop (DFRWS) Method. International Journal of Computer Applications, 174(18): 34-40. https://doi.org/10.5120/ijca2021921076

[6] Zamroni G.M., Riadi, I. (2020). Mobile forensic tools validation and evaluation for instant messaging. International Journal on Advanced Science Engineering and Information Technology, 10(5): 1860-1866. https://doi.org/10.18517/ijaseit.10.5.7499

[7] Ahmed, W., Shahzad, F., Javed, A.R., Iqbal, F., Ali, L. (2021). WhatsApp network forensics: Discovering the IP addresses of suspects. In 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 2021, pp. 1-7. https://doi.org/10.1109/NTMS49979.2021.9432677

[8] Trisnasenjaya, H. (2019). Forensic analysis of android-based WhatsApp Messenger Against Fraud Crime Using The National Institute of Standard and Technology Framework. International Journal of Cyber-Security and Digital Forensics, 8(1): 89-97. https://doi.org/http://dx.doi.org/10.17781/P002567

[9] Schul'tz, V.L., Kul'ba, V.V., Shelkov, A.B., Bogatyryova, L.V. (2021). Scenario analysis of improving the effectiveness of cybercrime investigation management problems. IFAC-PapersOnLine, 54(13): 155-160. https://doi.org/10.1016/j.ifacol.2021.10.437

[10] Anglano, C., Canonico, M., and Guazzone, M. (2016). Forensic analysis of the ChatSecure instant messaging application on android smartphones. Digital Investigation, 19: 44-59. https://doi.org/10.1016/j.diin.2016.10.001

[11] Numbeo,. (2022). No Crime Index by Country 2022 Mid-Year. https://www.numbeo.com/crime/rankings_by_country.jsp. Accessed successfully on Jul. 07th 2022.

[12] Rauf, M., Prasetio, A., Sos, S., Si, M. (2021). Communication activities match search applications on michat media. In e-Proceeding of Management, 1559-1571.

[13] Fanani, G., Riadi, I., Yudhana, A. (2022). Michat application forensic analysis using digital forensics research workshop method. 6(2): 1263-1271. https://doi.org/10.30865/mib.v6i2.3946

[14] Mahendra K.D.O., Mogi, I.K.A. (2021). Digital forensic analysis of michat application on android as digital proof in handling online prostitution cases. JELIKU, 9(3): 381. https://doi.org/10.24843/JLK.2021.v09.i03.p09

[15] Riadi, I., Umar, R., Firdonsyah, A. (2018). Forensic tools performance analysis on android-based blackberry messenger using NIST measurements. International Journal of Electrical and Computer Engineering, 8(5): 3991-4003. https://doi.org/10.11591/ijece.v8i5.pp3991-4003

[16] Patel, A., Sharma, D.P., Dholariya, P.D. (2021). A forensic evidence recovery from android device applications. International Journal of Scientific Research in Science, Engineering and Technology, 3(4): 135-140. https://doi.org/10.32628/ijsrset218321

[17] Whitaker, J., Mabey, M., Ahn, J.G., Doupé, A. (2018). Forensic analysis on mobile devices. TICEC, 2: 57-72. https://doi.org/10.1007/978-3-030-02828-2

[18] Pessel, H.P. (2022). Spreading immoral documents via MiChat, 19-year-old student arrested by ditreskrimsus west sumatra police. Kriminal. https://pesisirselatan.sumbar.polri.go.id/index.php/2022/04/26/sebarkan-dokumen-asusila-lewat-michat-mahasiswa-19-tahun-diamankan-ditreskrimsus-polda-sumbar

[19] Maulana, S. (2021). The Story of a Man in Samarinda, Fooled by Open BO MiChat to Lose Millions of Rupiah. https://kaltim.suara.com/read/2021/04/14/164208/kisah-pria-di-samarinda-tertipu-open-bo-michat-hingga-rugi-jutaan-rupiah?page=all

[20] Pasha, Y. (2020). Nyambi Trades Drugs, Police Arrested Prostitutes in MiChat. https://jabar.idntimes.com/news/jabar/bagus-f/nyambi-dagang-narkoba-psk-di-michat-ditangkap-polisi

[21] Utama L., Hari, A. (2019). North Sulawesi Police Unravel Human Trafficking Through the MiChat Application. https://www.viva.co.id/berita/nasional/1182565-polda-sulut-bongkar-perdagangan-manusia-lewat-aplikasi-michat

[22] Anwar, A. (2018). Sisca Icun Sulastri's murder, this is how MiChat is abused. https://metro.tempo.co/read/1158644/pembunuhan-sisca-icun-sulastri-begini-michat-disalahgunakan

[23] Kamble, D.R., Jain, N. (2015). Digital forensic tools : a comparative approach. International Journal of Advance Research In Science and Engineering, 8354(4): 157-168.

[24] Himanshu, S.B., Garg, G. (2021). Comparative analysis of acquisition methods in digital forensics. In 2021 Fourth International Conference on Computational Intelligence and Communication Technologies (CCICT), Sonepat, India, 2021, pp. 129-134. https://doi.org/10.1109/CCICT53244.2021.00035

[25] Hamad, N., Eleyan, D. (2022). Digital forensics tools used in cybercrime investigation-comparative analysis. Journal of Xi'an University of Architecture & Technology, 113-127. doi: 10.37896/JXAT14.04/314909.

[26] Anwar, N., Mardhia, M.M., Ryanto, L. (2021). Live forensics on GPS inactive smartphone. Mobile and Forensics, 3(1): 32-44.

https://doi.org/10.12928/mf.v3i1.3847

[27] Kukuh, M., Riadi, I., Prayudi, Y. (2018). Forensics acquisition and analysis method of IMO messenger. International Journal of Computer Applications, 179(47): 9-14. https://doi.org/10.5120/ijca2018917222

[28] Nasution, M.R., Prayudi, Y., Luthfi, A. (2022). Investigating social media user activity on android smartphone. International Journal of Computer Applications, 183(48): 46-52. https://doi.org/10.5120/ijca2022921890

[29] Sai, D.M., Prasad, N.R.G.K., Dekka, S. (2015). The forensic process analysis of mobile device. International Journal of Computer Science and Information Technologies, 6(5): 4847-4850.

[30] P. Domingues, M. Frade, L. M. Andrade, and J. V. Silva, "Digital forensic artifacts of the your phone application in Windows 10," *Digit. Investig.*, vol. 30, no. December 2018, pp. 32-42, 2019, https://doi.org/10.1016/j.diin.2019.06.003

[31] Z. Liao, F. Wang, S. Wu, D. Ming, B. Xi, and B. Chen, "Digital forensics design of IOS operating system," *ACM Int. Conf. Proceeding Ser.*, vol. 8, no. 422, pp. 232–236, 2019, https://doi.org/10.1145/3341069.3341081

[32] Agrawal, A.K., Khatri, P., Sinha, S.R. (2018). Comparative study of mobile forensic tools. Advances in Data and Information Sciences, 38: 39-47. https://doi.org/10.1007/978-981-10-8360-0_4

[33] Nurhairani, H., Riadi, I. (2019). Analysis mobile forensics on twitter application using the National Institute of Justice (NIJ) Method. International Journal of Computer Applications, 177(27): 975-8887.https://doi.org/10.5120/ijca2019919749

[34] Ruuhwan, I.R., Prayudi, Y. (2016). Application of integrated digital forensic investigation framework v2 (IDFIF) in smartphone investigation process. Jurnal Edukasi dan Penelitian Informatika, 2(1). https://doi.org/http://dx.doi.org/10.26418/jp.v2i1.14369

[35] Choi, J., Yu, J., Hyun, S., Kim, H. (2019). Digital forensic analysis of encrypted database files in instant messaging applications on Windows operating systems: Case study with KakaoTalk, NateOn and QQ messenger. Digital Investigation, 28: S50-S59. https://doi.org/10.1016/j.diin.2019.01.011

[36] Garfinkel, S., Farrell, P., Roussev, V., Dinolt, G. (2009). Bringing science to digital forensics with standardized forensic corpora. Digital Investigation, 6(4): https://doi.org/https://doi.org/10.1016/j.diin.2009.06.016

[37] Sutikno, T., Handayani, L., Stiawan, D., Riyadi, M.A., Subroto, I.M.I. (2016). WhatsApp, viber and telegram: Which is the best for instant messaging?. International Journal of Electrical and Computer Engineering, 6(3): 909-914. https://doi.org/10.11591/ijece.v6i3.10271

[38] Dogan, S., Akbal, E. (2017). Analysis of mobile phones in digital forensics. In 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2017, pp. 1241-1244. https://doi.org/10.23919/MIPRO.2017.7973613

[39] Osho, O., Ohida, S.O. (2016). Comparative evaluation of mobile forensic tools. International Journal of Information Technology and Computer Science, 8(1): 74-83. https://doi.org/10.5815/ijitcs.2016.01.09

[40] Padmanabhan, R., Lobo, K., Ghelani, M., Sujan,D., Shirole, M. (2017). In Comparative analysis of commercial and open source mobile device forensic tools. 2016 Ninth International Conference on Contemporary Computing (IC3), Noida, India, 2016, pp. 1-6. https://doi.org/10.1109/IC3.2016.7880238

[41] Grispos, G., Tursi, F., Choo, K.K.R., Mahoney, W., Glisson, W.B. (2021). A digital forensics investigation of a smart scale IoT ecosystem. In 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, 2021, pp. 710-717. https://doi.org/10.1109/TrustCom53373.2021.00104

[42] Du, X., Le-Khac, N.A., Scanlon, M. (2017). Evaluation of digital forensic process models with respect to digital forensics as a service. Computer Science, 573-581. https://arxiv.org/abs/1708.01730

[43] Ajijola, A.,Zavarsky, P., Ruhl, R. (2014). A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012. In World Congress on Internet Security (WorldCIS-2014), London, UK, 2014, pp. 66-73. https://doi.org/10.1109/WorldCIS.2014.7028169

[44] Daware, S., Dahake, S., Thakare, V.M. (2012). Mobile forensics : Overview of digital forensic, computer forensics vs. mobile forensics and tools. International Journal of Computer Applications, 2012(7-8): 975-8887.

[45] Lwin, H.H., Aung, W.P., Lin, K.K. (2020). Comparative analysis of android mobile forensics tools. In 2020 IEEE Conference on Computer Applications(ICCA), Yangon, Myanmar, 2020, pp. 1-6. https://doi.org/10.1109/ICCA49400.2020.9022838

[46] G. Alendal, S. Axelsson, G.O. Dyrkolbotn, "Chip chop - smashing the mobile phone secure chip for fun and digital forensics," *Forensic Sci. Int. Digit. Investig.*, vol. 37, no. 21, pp. 301191, 2021, https://doi.org/10.1016/j.fsidi.2021.301191

[47] Khan, A. (2018). Comparative study of various digital forensics logical acquisition tools for android smartphone's internal memory: A case study of Samsung Galaxy S5 and S6. International Journal of Advanced Research in Computer Science, 9(1): 357-369. https://doi.org/10.26483/ijarcs.v9i1.5303

[48] Atmaja, G.A.S., Mogi, I.K.A. (2021). Acquisition of digital evidence in online scam cases (CyberCrime) on Whatsapp chat application using NIST method. JELIKU, 9(4): 511. https://doi.org/10.24843/jlk.2021.v09.i04.p08

[49] Goni, I., Gumpy, J.M., Maigari, T.U., Muhammad, M., Saidu, A. (2020). Cybersecurity and cyber forensics: machine learning approach. Machine Learning Research, 5(4): 46. https://doi.org/10.11648/j.mlr.20200504.11