Malaysian Journal of Computing, 7 (2): 1162-1177, 2022
Copyright © UiTM Press
eISSN: 2600-8238 online

COMPARATIVE ANALYSIS OF LOGICAL ACQUISITION USING WONDERSHARE DR. FONE, MOBILEDIT FORENSIC, AND FONEPAW ON ANDROID PHONES

Nuraimi Farhana Salimi[1], Nor Bakiah Abd Warif[2*] & Nor-Syahidatul N Ismail[3]

[1]*Centre for Information Security Research, Faculty of Computer Science & Information Technology, Universiti Tun Hussein Onn Malaysia, Batu Pahat, Malaysia*

[2]*Faculty of Computing, College of Computing and Applied Sciences,Universiti Malaysia Pahang, Pekan, Pahang, Malaysia*

[1]ai180267@siswa.uthm.edu.my, [*2]norbakiah@uthm.edu.my, [3]nadiahismail@ump.edu.my,

ABSTRACT

The increasing number of mobile phone usage in storing confidential information, such as mobile online transactions has led to the growing number of research in mobile forensic. There are lot of crimes may happen through mobile phones, such as smishing, bluejacking, and malware attacks. Mobile forensic is a way of collecting any digital evidence on the mobile phone. Logical acquisition is one of the methods for mobile forensic. The methodology for logical acquisition consists of identification, isolation, acquisition, analysis, and documentation. This research aims to study, perform and analyze logical acquisition using Wondershare Dr. Fone for Android, MOBILedit Forensic, and FonePaw for Android in Android-based phones which are Oppo F9 and Samsung S7 Edge. The analysis is based on percentage of capability and time taken for each tested mobile forensic tool on the two selected Android phones. The results show that FonePaw for Android gets the highest average capability (97%) with the shortest time while MOBILedit Forensic obtains the lowest average capability (74%) with the longest time taken. This research may help the forensic investigators team to determine the suitability of mobile forensic tools with Android phones based on the Android features and type of files.

Keywords: *Android Forensic, Android Phones, Data Extraction, Logical Acquisition, Mobile Forensic*

Received for review: 07-02-2022; Accepted: 26-09-2022; Published: 01-10-2022
DOI: 10.24191/mjoc.v7i2.16968

1. Introduction

Technology nowadays is part of our daily life. This technology can help to make our life easier. One of the inventions of this technology is mobile phones. Mobile phones may help us in many ways such as, to make a phone call, exchange messages, online business and commerce, online transactions, store and manage personal data, social networking web browsing, and multimedia capturing (Abdulhamid *et al.*, 2018). Each of the mobile phones has an operating system that works to run different application software and program inside the mobile phone. A few examples of operating systems that reside in mobile phones such as Google's Android, Apple's iOS, and Microsoft's Windows Phone. Android is one of the operating systems based on the Linux kernel (Khan & Hussain Mansuri, 2018). The examples of Android operating system versions are Android Nougat, Android Marshmallow, and the latest Android 11. Manufacturer company that has been using Android in their devices are Samsung, Sony, Realme, Vivo, Huawei, HTC, Motorola and numerous other manufacturers.

Due to the increasing number of mobile phone usage, there are lot of cybercrimes that happen on a mobile phone. The examples of mobile phone crimes are bluejacking and blue bugging, vishing and smishing (Joshi & Parekkh, 2016), (Meshram & Thool, 2014). The reason why logical acquisition is important in mobile forensic is logical acquisition can preserve any digital evidence in its most original form and this process did not cause any harm to the original data. To carry out logical acquisition, there are lots of mobile forensic tools that can be used. The reality of research in the domain of mobile forensic is decision-making on which tools are suitable to be used. There are lots of mobile forensic tools available in the market such as AccessData FTK Imager, Paraben Seizure, MOBILedit Forensic, Encase, and AFLogical OSE (Lwin *et al.*, 2020), (Raji *et al.*, 2018). Some of the tools are priceable and some are open-source versions. The problem with open-source tools is the numbers of data that can be acquired are very limited and sometimes the type of features is not eligible to be acquired (Al-Sabaawi & Foo, 2019). Therefore, the objectives of this research are to study, perform and analyze logical acquisition using Wondershare Dr Fone for Android, MOBILedit Forensic and FonePaw for Android in Oppo F9 and Samsung S7 Edge Android phone. The findings of this research will assist the industries and researchers or the law enforcement team to determine whether the mobile forensic tools are suitable with the specific mobile phones to help in solving investigations and gain the evidence.

2. Literature Review

This section discusses types of mobile forensic data acquisition methods and the existing research about comparative analysis based on logical acquisition.

2.1 Mobile Forensic Data Acquisition

Mobile forensic data acquisition consists of five methods which are manual acquisition, logical acquisition, hex-dump analysis, chip-off, and micro read. Figure 1 shows the mobile forensic data acquisition method.

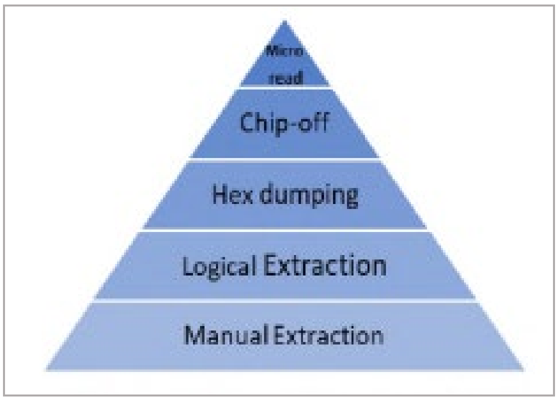

Figure 1. Mobile forensic data acquisition level (Alatawi *et al.*, 2020).

The first level; manual acquisition is a conventional interface such as display console, touch controls, and keypad that are used to browse into a document data form. The investigator team accesses the information stored by just reviewing the mobile phone documentation (Alatawi *et al.*, 2020). The second level is a logical acquisition where the explanation will be explained in detail in Section 2.2. The next level is a hex-dump analysis that also known as a physical acquisition where it is a method that attempts to gather the maximum amount of bit-by-bit of logical storage objects of a memory device while minimizing loss of data (Tajuddin & Manaf, 2015). The physical acquisition included diagnosing the mobile phone's random-access memory (RAM) that is not easily accessible but with the help of forensics software, the contents of the flash memory able to be downloaded. Meanwhile, the fourth level is chip-off where physical removal of the mobile phone's flash memory for the acquisition of data and at the same time gives investigators team a comprehensive review of the mobile phone (Alghafli *et al.*, 2012). One of the several methods that can be used for de-soldering flash memory from a Printed Circuit board is by using Thin Small-Outline Package (TSOP) or micro–Ball Grid Array (BGA) (Alghafli *et al.*, 2012). As the flash memory has successfully been removed from the mobile phone, investigators create a binary image of the chip, and the data obtained will be analysed. The last level of mobile forensic data acquisition method is micro read which is the highest in the pyramid of data acquisition level. It shows that this method is the hardest compared to other methods. For this method, a high-power electron microscope is needed so that the investigators can review and record the physical observation of the gates (NAND or NOR) on the electronic chip on the circuit (Lohiya *et al.*, 2015). This method comes very useful when the memory chip of the devices is physical damage.

2.2 Logical Acquisition

Logical acquisition is a mobile forensic data acquisition method where the interface between the investigator's workstation and mobile has been set up using USB, Wi-Fi, or Bluetooth to allow information to be passed to the workstation. Most Android mobile phones are able to perform logical acquisition as this method is an easy, reliable and secure acquisition process from Android mobile phones. From the connection that has been established between workstation and mobile phone, a series of commands are exchanged in the connection (Lohiya *et al.*, 2015). The data in the mobile phone is acquired from the flash memory of smartphones with the help of various mobile forensic tools. Examples of forensic tools that can be used for logical acquisition are SAFT, AFLogical, LiME Module, OSAF-TK (Open-Source Android Forensic Toolkit), Santoku Linux, WhatsApp Extract, Andriller, and Nandroid Backups (Khan & Hussain Mansuri, 2018). The logical acquisition is easier and simple for the investigator's team because of the direct interaction between systems data structure with the tools used. The data that has successfully been acquired will be analysed to obtain valid value instead of directly using an original file from the mobile phones. The advantages of logical acquisition are this method provides a high level of data abstractions and supports low technical complexity while the disadvantages are this method has restricted and limit the number of accesses to the data and yet the recovery to the deleted data is not supported (Alatawi *et al.*, 2020).

Table 1 lists several related works that implement the logical acquisition using existing mobile forensic tools. Based on the table, Sathe and Dongre (2018) acquire data from Samsung Galaxy Grand Duos GT-19082 model with Android 4.2.2 using Wondershare Dr. Fone for the Android. From the table, they are able to collect the undeleted and deleted data in the devices. However, based on the logical acquisition technique, only data that is available in the mobile devices will be recovered fully into the workstation and only a certain amount of deleted data will recover with the trial version. It stated that Wondershare Dr. Fone for Android is able to generate data of 8.2GB with respect to time factor by taking 48 minutes to complete the acquisition process. By the time taken to complete the acquisition, authors have come to the conclusion that when time is not a key factor to the investigations, Wondershare Dr. Fone for Android is recommended for thorough forensic investigation.

In research done by Riadi *et al.* (2020), Samsung J5 2015 SM-J500G model with Android version 5.1 and Samsung J1 Ace SM-J111F with Android version 5.1 is undergone logical acquisition using Wondershare Dr. Fone for Android. In this work, the total handset data for contacts, call history, and messages are recorded separately. Samsung J5 2015 SM-J500G model with Android version 5.1 is labeled as Smartphone 1 while Samsung J1 Ace SM-J111F with Android version 5.1 is labeled as Smartphone 2. The total handset data for Smartphone 1 and Smartphone 2 are tabulated in Table 2. The process of logical acquisition on Smartphone 1 is only able to acquire call history where all 12 call history records are acquired successfully while the contacts and messages cannot be acquired. Similarly, only call history with 11 records is able to acquire successfully for Smartphone 2.

Table 1. Comparative analysis related works.

Work	Smartphone	Forensic Tools	Data Acquired	Capability of tool
Data Acquisition Techniques in Mobile Forensic (Sathe & Dongre, 2018)	Samsung Galaxy Grand Duos GT-19082 Android Version 4.2.2	Wondershare Dr. Fone for Android	659 Contacts 212 Messages 1357 Call Logs 9006 Images 494 Audios 159 Videos 379 Documents	Total of data not provided, however, able to include 59% physical acquisition in 48 minutes
Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST (Riadi *et al.*, 2020)	Smartphone 1 - Samsung J5 2015 SM-J500G Android Version 5.1	Wondershare Dr. Fone for Android	0 Contacts 12 Call Logs 0 Messages	31% logical acquisition
	Smartphone 2 - Samsung J1 Ace SM-J111F Android Version 5.1	Wondershare Dr. Fone for Android	0 Contacts 11 Call Logs 0 Messages	34% logical acquisition
Analisis Forensik Recovery Pada Smartphone Android Menggunakan Metode National Institute of Justice (Riadi *et al.*, 2019)	Samsung Galaxy J5 Android Version 5.1	Wondershare Dr. Fone for Android	95 Messages 19 Call Logs 590 Contacts 0 Images 0 Videos	Total data not provided, however, able to include physical acquisition
	Samsung Galaxy J5 Android Version 5.1	MOBILedit Forensic	2 Messages 0 Call Logs 195 Contacts 0 Images 0 Videos	Total data not provided

Last but not least, in research that has been done by Riadi *et al.* (2019), Samsung Galaxy J5 with Android version 5.1 is undergone logical acquisition using Wondershare Dr. Fone for Android and MOBILedit Forensic. The results of the experiment show that Wondershare Dr. Fone for Android able to acquire deleted data while only data that exist in the Android phone are successfully acquired by MOBILedit Forensic.

Table 2. Total handset data of Smartphone 1 and Smartphone 2 (Riadi *et al.*, 2020).

Items	Smartphone 1	Smartphone 2
Contacts	13	10
Call History	12	11
Messages	14	11

Based on the related works (Sathe & Dongre, 2018), (Riadi *et al.*, 2020) and (Riadi *et al.*, 2019), that discussed about Wondershare Dr. Fone for Android, there is conflict results whether Wondershare Dr. Fone for Android is able to acquire messages and contacts or not. This is because in the paper written by Sathe & Dongre (2018), and Riadi *et al.*, (2019), there are messages and contacts that successfully acquired while in paper written by Riadi *et al.* (2020), contacts and messages cannot be acquired. Besides that, Wondershare Dr. Fone for Android is able to acquire data types such as contacts, SMS, images, audio, video, WhatsApp messages, and WhatsApp attachments in Sathe and Dongre (2018) while only able to acquire call history in by Riadi *et al.* (2020).

Besides of Wondershare Dr. Fone for Android and MOBILedit Forensic, there is another tool that also can be used for logical acquisition which is FonePaw for Android. However, there is no research on this tool as their medium to undergoes logical acquisition on Android phones. FonePaw for Android is a risk-free mobile forensic tool that allows users to scan, preview, and recover files including photos, contacts, messages, and documents from Android phones securely (Zinge & Chatterjee, 2018). The deleted files still exist on the phone in the condition that the deleted files have not been overwritten and factory reset should not be done on the phone could also be acquired by the tool.

3. Methodology

This section discussed the methodology used in performing the logical acquisition. The related steps in the methodology will be explained in detail. Figure 2 shows the mobile forensic model stated in the paper written by Sathe and Dongre (2018) and Dogan and Akbal (2017) to be used in this research. The model starts with identification, followed by isolation, acquisition, analysis, and reporting. These steps are developed to make sure that all the digital evidence of Android be handled in a forensically sound manner and will be discussed in the next subsections.

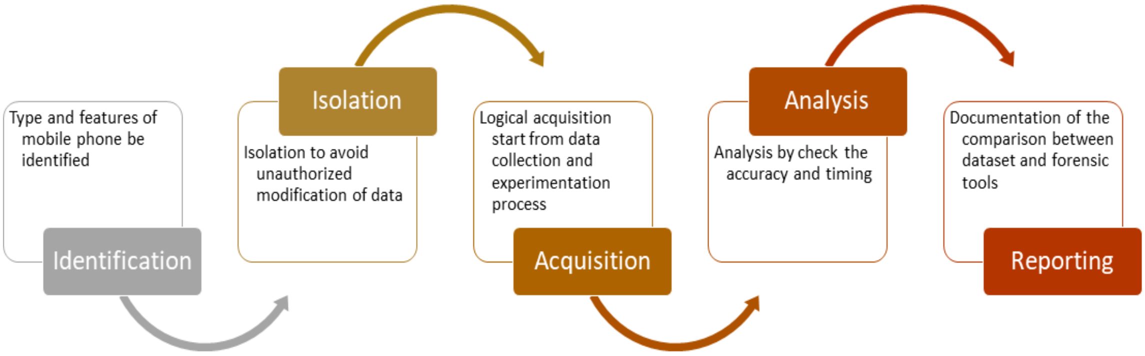
Type and features of mobile phone be identified
Identification
Isolation
Isolation to avoid unauthorized modification of data
Logical acquisition start from data collection and experimentation process
Acquisition
Analysis
Analysis by check the accuracy and timing
Documentation of the comparison between dataset and forensic tools
Reporting

Figure 2. The mobile forensic model stated in Sathe and Dongre (2018) and Dogan and Akbal (2017).

3.1 Identification

The forensic investigator's team starts by identifying the devices and evidence that they expected to gain from the Android phones. The forensic investigator also should identify the information regarding the model, manufacturer, and type of the Android devices. Currently, there are a variety of mobile phones that used Android as their operating system but came from a different manufacturer. So, it is expected that each Android phones have different structures and features. It is very important for the forensic investigator's team to require good experience in identifying and analyzing digital data of the specific data due to various brands of Android phones. In this research, the type and features of Android phones used for the experiments are listed in table 3.

Table 3. Hardware requirement for logical acquisition of Oppo F9 and Samsung S7 Edge

Hardware	Version	System
Oppo F9	Android Version 10.0	Processor: Octa Core Installed Memory (RAM): 6.00 GB Kernel Version 4.14.141
Samsung S7 Edge	Android Version 8.0	Processor: Octa Core Installed Memory (RAM): 4.00 GB Kernel Version 3.18.91

3.2 Isolation

Isolation is a compulsory step in every forensic investigation. In this step, the targeted mobile phones are isolated from any network connection to avoid any unauthorized modification from an outside source. Data integrity of the data can be protected so every data acquired can be used as legitimate digital evidence during the investigation. The isolation process can be done by switching on the airplane mode of the phones and the Subscriber Identification Module (SIM) card will be removed from the phone. After all these processes are done, the next steps are acquisition.

3.3 Acquisition

Once the phone has been isolated from the networks, the acquisition process may begin. In this step, digital data is acquired from the targeted Android phones. Data such as SMS and contact logs will be acquired from the forensics investigator's workstation. To begin this process, the Android phone must be connected to the workstation via USB. In order to allow communication between the workstation and Android phone, USB debugging should be enabled on Android phones.

The logical acquisition will be carried out to acquire a variety type of datasets of SMS, call logs, images, videos, audios, and documents from Android phones. The process on how logical acquisition using mobile forensic tools is mentioned in (Tayeb & State, 2019) portrays in Figure 3. We will use similar steps in the figure for the experiments on the Oppo F9 and Samsung S7 Edge with different mobile forensic tools; Wondershare Dr. Fone for Android, MOBILedit Forensic, FonePaw for Android. Table 4 shows the system requirements for each tool.

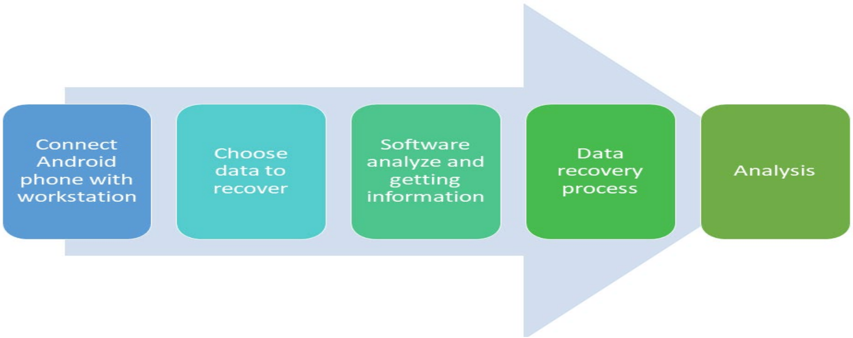
Connect Android phone with workstation
Choose data to recover
Software analyze and getting information
Data recovery process
Analysis

Figure 3. Logical acquisition method discussed in [19].

Table 4. Software requirement for logical acquisition of Oppo F9 and Samsung S7 Edge.

Software	**Version**	**System**
Wondershare Dr. Fone for Android	Version 10.0.12	Operating System: Microsoft Windows 10 64 bit CPU: 1GHz RAM: 256MB
MOBILedit Forensic	Version 7.1.0	Operating System: Microsoft Windows 10 32 bit CPU: i5 8th Gen RAM: 16GB
FonePaw for Android	Version 3.8.0	Operating System: Microsoft Windows 10 64-bit CPU: 1GHz RAM: 1G

The processes in the Figure 3 are listed below:

1. The targeted Android phone will be connected to the workstation. On Android phones, USB debugging mode must be turned on by changing the settings of the Android phone to developer mode. The purpose of turning on the USB debugging mode is to enable Android phones to communicate with Android SDK over a USB connection that allows and support Android phones to transfer data from an Android phone to a workstation.

2. On the three mobile forensic tools, forensic investigators can choose what data types they want to acquire. The data types chosen must be similar for each tool, thus, the results gained from the experiments can be analyzed thoroughly for the comparative analysis.

3. Mobile forensic tools then will be getting the information that has been selected during data types selection for the recovery phase. The time taken for each of the mobile forensic might varies as the amount of data choose to be acquired is different for each Android phone.

4. After the information has been analyzed and collected, the interfaces will group all the information based on their data types. It will help forensic investigators to analyze the information. All the information can be recovered into the workstation with just one click. The forensic investigator can place the folders of acquisition in the folder that existed on the workstation.

3.4 Analysis

After processing and acquiring data from the Android phone, the forensic investigator needs to check the verification of the capabilities of the tools based on the data acquired from the Android phone. Verification of capabilities can be proved by comparing the acquired data with the actual data in handset (Md. Salleh *et al.*, 2014). According to Md. Salleh *et al.* (2014), a forensic tool shall have the ability to logically acquire all application supported data objects present in internal memory.

$$Capability = \frac{Number\ of\ extracted\ data}{Number\ of\ handset\ data}\ x\ 100\% \qquad (1)$$

Forensic tools capability can be judged by the performance based on capability formula as shown in Equation (1). The capabilities of the tools are measured in terms of the probability number of successful acquisitions of a particular type of digital evidence by a specific forensics tool. As an additional measurement for the capabilities of the tools, the time taken of the forensic tools to finish all the acquisition methods also been recorded. This is because the tested tools do not automatically provide the extraction time.

3.5 Documentation

These are the last steps in this research. Documentation steps should occur throughout the progress of the research. Documentation can help in the examination process when all information is recorded. From the previous step, it stated that the capabilities of the tools and time took are recorded. Moreover, the documentation part also states the physical condition of the phone and tools that are used during the examination. From the documentation, any irrelevant acquired data can be excluded from further investigation.

4. Experimental Setup

In this research, the logical acquisition of mobile forensic tools on Android phones is performed using Wondershare Dr. Fone for Android, MOBILedit Forensic, and FonePaw for Android. The experiments started by enabling USB debugging on both Android phones which are Oppo F9 running with Android version 10 and Samsung S7 Edge running with Android version 8. Different sets of data are available on each phone to determine whether the size of data may affect the capabilities of the tools and the time taken for each logical acquisition process to complete. The handset data of Oppo F9 and Samsung S7 Edge are recorded in Table 5.

Table 5. Handset data in Oppo F9 with Android version 10 and Samsung S7 Edge running with Android version 8.

Items	Data in Oppo F9 with Android version 10	Data in Samsung S7 Edge with Android version 8
Contacts	1490	259
Photos	301	3030
Video	7	184
Audio	38	32
Messages	161	31
Call Logs	510	500
Documents	127	55
Total	2634	4091

4.1 Results and Discussion

This section will discuss the results of the experiment and performed analysis from the capabilities of the tools and time taken for the datasets on both Android phones. The results of logical acquisition done by Wondershare Dr. Fone for Android, MOBILedit Forensic, and FonePaw for Android on Oppo F9 and Samsung S7 Edge are recorded. All the results are calculated based on Equation (1) that can be referred in Section 3.4 and further analyzed in the next subsections.

4.1.1 Capability of the Tools

Figure 4 shows a bar chart graph based on the capability of Wondershare Dr. Fone for Android, MOBILedit Forensic, and FonePaw for Android in data acquisition for Oppo F9 and Samsung S7 Edge. As we can see in the figure, the highest capability of the mobile forensic tool with Oppo F9 is FonePaw for Android as they succeeded in acquiring 2511 out of 2634 data with 95% of capability. Almost all types of data are able to be acquired by the tool, but have limitations on documents type. The lowest capability of tool for Oppo F9 is Wondershare Dr. Fone for Android with 89% as only 2334 out of 2634 data are acquired successfully. The tool failed to acquire any data for messages and documents.

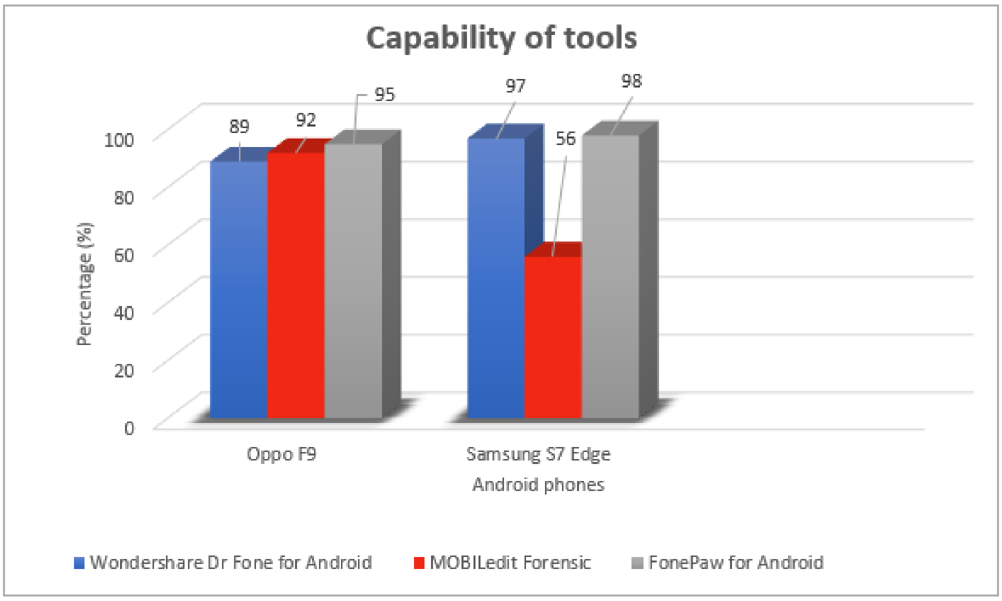

Figure 4. The capability of tools based on the acquisition of Oppo F9 and Samsung S7 Edge.

Similar with Oppo F9 results, the highest capability of tool for Samsung S7 Edge is also FonePaw for Android. The tool obtained 98% capability as they have succeeded in acquiring all types of data in Samsung S7 Edge except for documents. From that, 4036 data out of 4091 handset data are acquired successfully. However, 55 documents data are unable to be obtained. Meanwhile, the lowest capability of tools in acquiring Samsung S7 Edge handset data is MOBILedit Forensic with only 56% of capability as they are only able to acquire 2278 data from 4091 handset data. MOBILedit Forensic is able to acquire all contacts, audios, messages, call logs, and documents, but not photos and video resulting to the downfall of the acquisition percentage.

4.1.2 Analysis on Data Type

The visualization of data acquired based on their files will be discussed in this section. Figure 5 is the graph of acquisition of contacts on both Oppo F9 and Samsung S7 Edge. All mobile forensic tools are able to acquire all contacts that are available in the Oppo F9 and Samsung S7 Edge. A total of 1490 data are acquired for Oppo F9 and 259 data are acquired for Samsung S7 Edge. All contacts are stored with the same details such as name and mobile number. Some of the contacts are also used for other communication applications such as WhatsApp and Telegram. After the acquisition, the contacts that used for WhatsApp and Telegram will caused a duplicate in the CSV file and increase the total of the row of contacts.

So, crosscheck been done on Wondershare Dr. Fone for Android, MOBILedit Forensic, and FonePaw for Android on Oppo F9 and Samsung S7 Edge to check the number of contacts acquired. Only MOBILedit Forensic on Oppo F9 acquire the contacts exactly as the same as Oppo F9 handset data. It may be because the version of Android of Oppo F9 is the latest version.

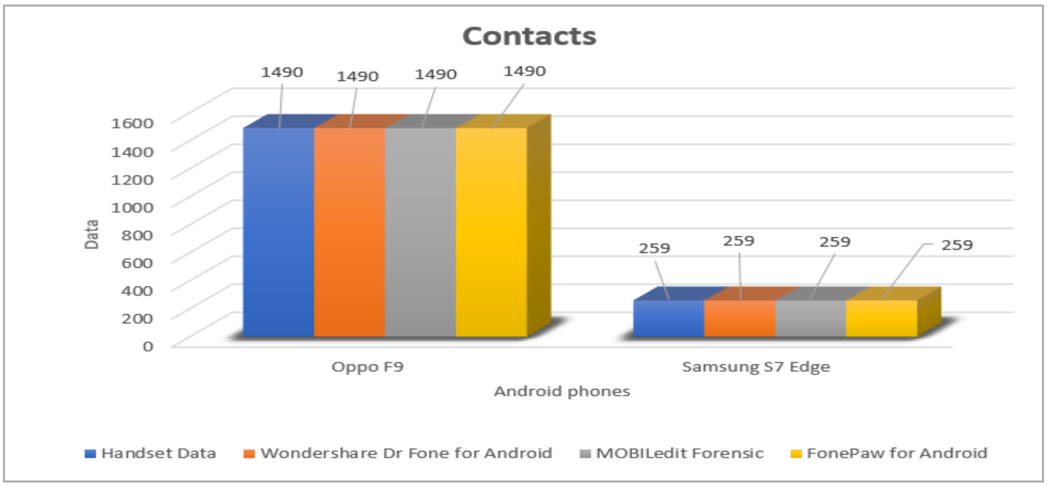

Figure 5. Contact acquisition of three mobile forensic tools on Oppo F9 and Samsung S7 Edge

Figure 6, Figure 7, and Figure 8 show acquisition on Oppo F9 and Samsung S7 Edge using Wondershare Dr. Fone for Android, MOBILedit Forensic, and FonePaw for Android for a photo, video, and audio respectively. The results of the photo acquisition show that the lack of capability of MOBILedit Forensic to acquire photos as it is only able to acquire less than half of the original handset data on both of the phones compared to other mobile forensic tools that are able to acquire all of the photos of handset data. For the video acquisition, the result of the acquisition shows that MOBILedit Forensic is not capable enough of acquiring media. The video acquisition for Samsung S7 Edge resulting the downfall of the capability of MOBILedit Forensic as only 1 of 184 videos able to be acquired. While in audio acquisition, MOBILedit Forensic and FonePaw for Android were able to acquire all handset data of audios while Wondershare Dr. Fone for Android did not fully acquire audio data in each of the phones.

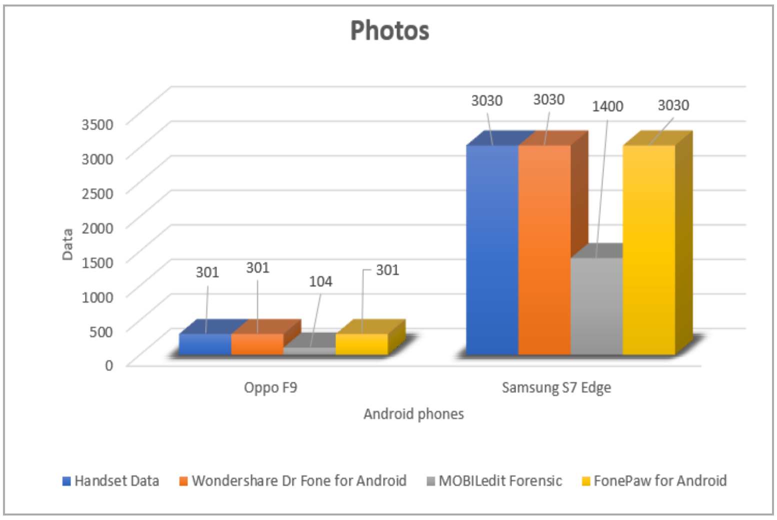

Figure 6. Photo acquisition of three mobile forensic tools on Oppo F9 and Samsung S7 Edge

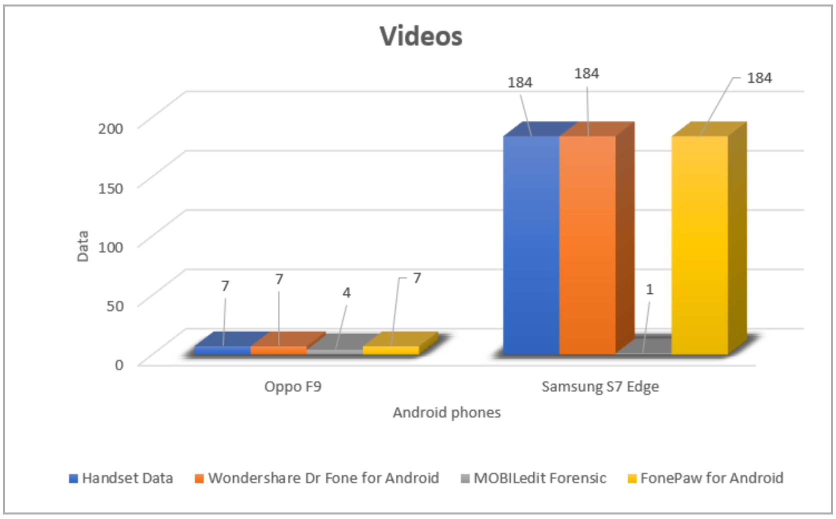

Figure 7. Video acquisition of three mobile forensic tools on Oppo F9 and Samsung S7 Edge

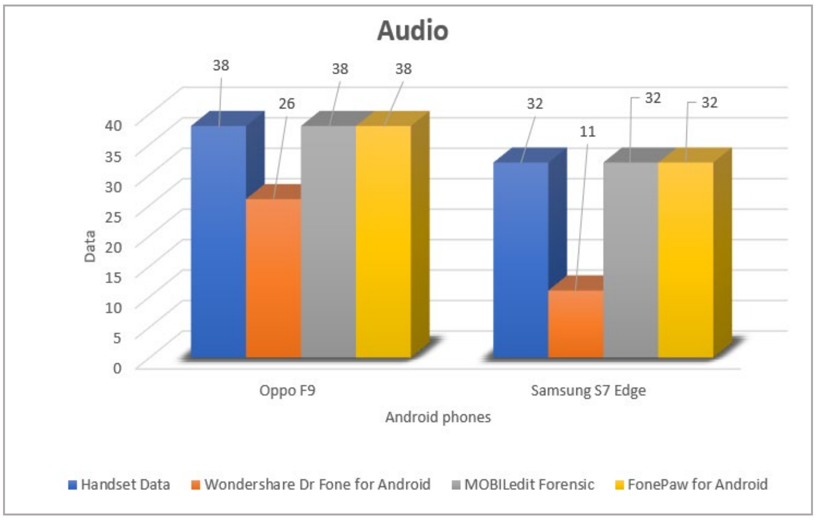

Figure 8. Audio acquisition of three mobile forensic tools on Oppo F9 and Samsung S7 Edge

Figure 9 and Figure 10 show the results of acquisition on Oppo F9 and Samsung S7 Edge using Wondershare Dr. Fone for Android, MOBILedit Forensic, and FonePaw for Android for messages and call logs respectively. Wondershare Dr. Fone resulting 0 acquisition for both Oppo F9 and Samsung S7 Edge while for other two mobile forensic tools show full acquisition on messages of both phones. For call logs, all of the mobile forensic tools are able to acquire full acquisition on a number of call logs on Oppo F9 and Samsung S7 Edge. The total of call logs acquired are the total number of incoming calls, outgoing calls, missed calls, and rejected calls on both phones.

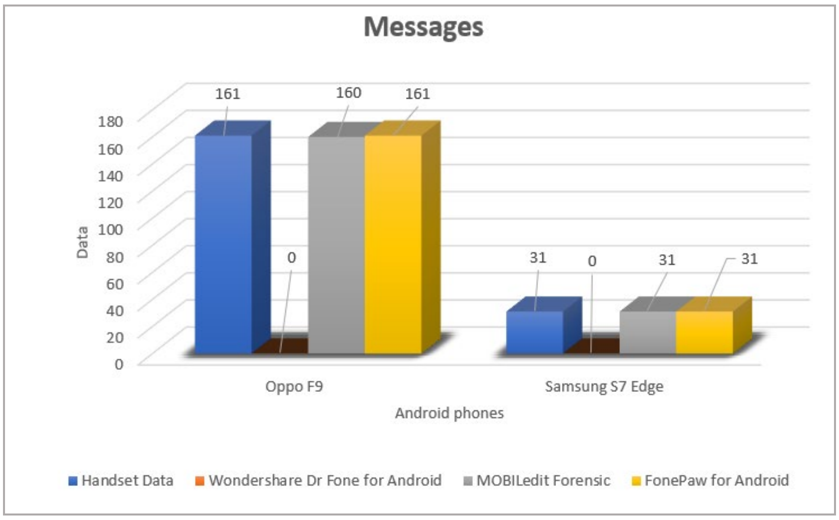

Figure 9. Messages acquisition of three mobile forensic tools on Oppo F9 and Samsung S7 Edge

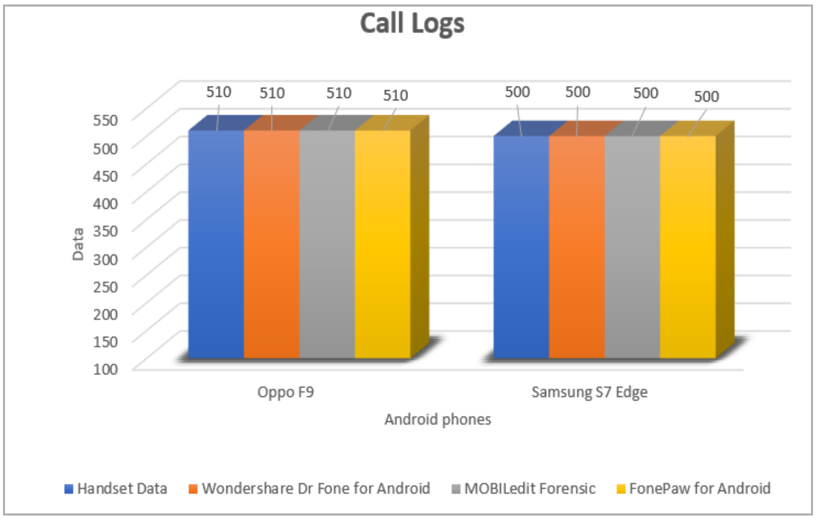

Fig. 10. Call logs acquisition of three mobile forensic tools on Oppo F9 and Samsung S7 Edge

The last acquisition for this research is the acquisition of documents. Figure 11 shows the acquisition of documents on both Oppo F9 and Samsung S7 Edge. For both, Oppo F9 and Samsung S7 Edge, Wondershare Dr. Fone for Android show 0 acquisition as they are not able to acquire any documents from the phones. However, the results for FonePaw for Android are different for both of the phones. This is because the limit of acquisition for the tool has been used to acquire another large file such as photos and videos, resulting in the failure of Documents from the Samsung S7 Edge acquisition.

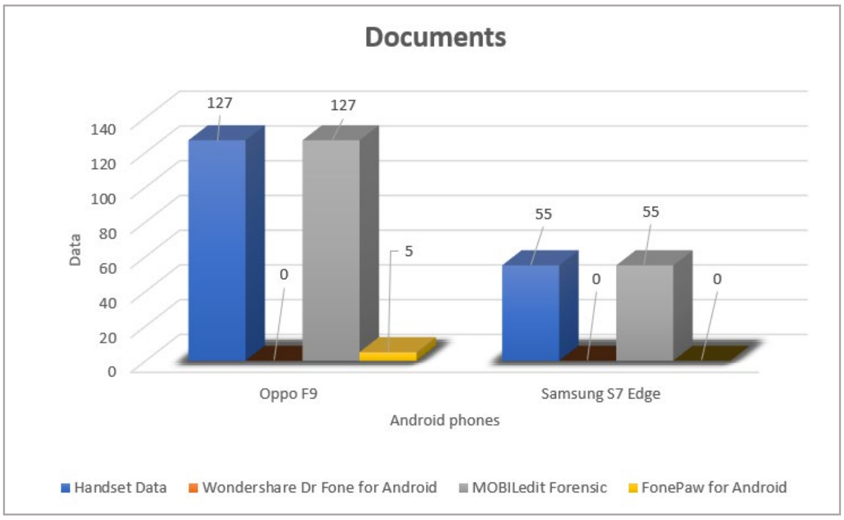

Figure 11. Documents acquisition of three mobile forensic tools on Oppo F9 and Samsung S7 Edge

4.1.3 Time Taken

Figure 12 portrays the time taken for each of the mobile forensic tools; Wondershare Dr. Fone for Android, MOBILedit Forensic, and FonePaw for Android on Oppo F9 and Samsung S7 Edge in each experiment. The time is recorded from the connection between Android phones and mobile forensic tools until the process of recovery of data is completed.

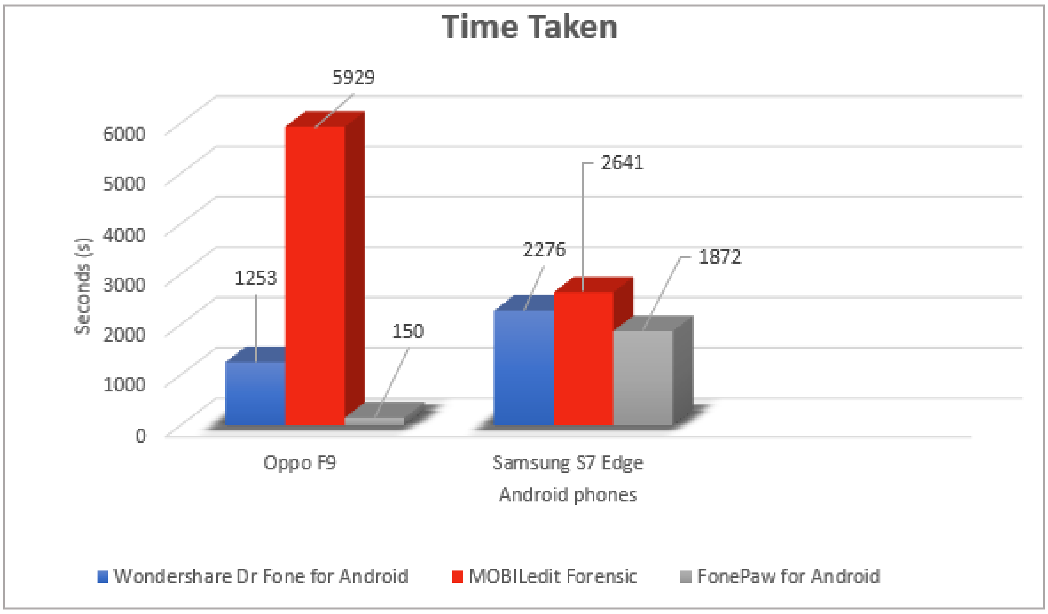

Figure 12. Time is taken for the acquisition of three mobile forensic tools on Oppo F9 and Samsung S7 Edge.

Based on the figure, the shortest time taken for logical acquisition for Oppo F9 and Samsung S7 Edge is FonePaw for Android as it only takes 150s equals to 2 minutes 30 seconds and 1872 seconds which is 31 minutes 12 seconds, respectively. At the same time, MOBILedit Forensic takes the longest time taken which require 5929 seconds for Oppo F9 and 2641 seconds for Samsung S7 Edge to complete the acquisition of the data.

Figure 13 shows the average of the capability between two Android phones. FonePaw for Android has the highest average of capability with 97% and the time was taken is suitable with the results. The lowest average of capability is MOBILedit Forensic with 74% longer time taken. It can be concluded that the recommended mobile forensic tool for these experiments is FonePaw for Android based on the acquisition capability of percentage and time taken to complete the acquisition.

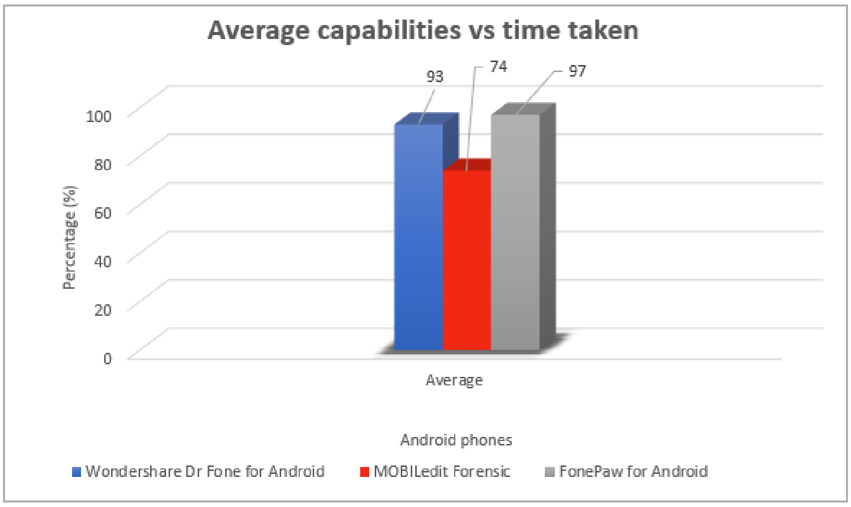

Figure 13. Average capabilities of three mobile forensic tools on Oppo F9 and Samsung S7 Edge.

5. Conclusions

Mobile forensic data acquisition consists of various types of data which each of them are specified for certain cases. The datasets that are used in this research including contacts, photos, video, audio, messages, call logs, and documents from two Android-based phones which are Oppo F9 and Samsung S7 Edge. By using Wondershare Dr. Fone for Android, MOBILedit Forensic, and FonePaw for Android, both datasets will be acquired from both Android phones and a comparison analysis between both data obtained. From the comparative analysis, the highest capability of the tool on Oppo F9 is FonePaw for Android with 95% of capability while the lowest is Wondershare Dr. Fone for Android with 89%. Meanwhile, the highest capability of the tool on Samsung S7 Edge is FonePaw for Android with 98% of capability while the lowest with 56% capability is MOBILedit Forensic.

It can be concluded that as the number of handset data is higher and the number of acquisitions is lower, it will cause the percentage of the capability of the tools to decrease compared to other tools. Based on the results of the acquisition, the patterns of acquisition can be seen where Wondershare Dr. Fone for Android is able to acquire all handset data except messages and documents while MOBILedit Forensic lacks in acquiring media such as photos and videos and FonePaw for Android may differ as the number of limits for acquisition has been reached based on the difference in the number of handset data. In a conclusion, both Android phones have successfully undergone logical acquisition on Wondershare Dr. Fone for Android, MOBILedit Forensic, and FonePaw for Android. So, by having this research, it may help the law enforcement team to find suitable mobile forensic tools based on their Android features and types of files acquired.

6. Acknowledgement

This research was supported by the Ministry of Higher Education (MOHE) through Fundamental Research Grant Scheme (FRGS/1/2020/ICT04/UTHM/02/1).

References

Abdulhamid, S., Waziri, V., Idris, I., Gbolahan, A., & Alhassan, J. (2018). A forensic evidence recovery from mobile device applications. *International Journal of Digital Enterprise Technology, 1*, 79.

Alatawi, H., Alenazi, K., Alshehri, S., Alshamakhi, S., Mustafa, M., & Aljaedi, A. (2020). Mobile forensics: A review. *2020 International Conference on Computing and Information Technology, ICCIT 2020*, (pp. 1-6).

Alghafli, K., Jones, A., & Martin, T. (2012). Forensics data acquisition methods for mobile phones. *2012 International Conference for Internet Technology and Secured Transactions, ICITST 2012*, (pp. 265-269).

Al-Sabaawi, A., & Foo, E. (2019). A comparison study of android mobile forensic for retrieving files system. *International Journal of Computer Science and Security (IJCSS), 13*, 148.

Dogan, S., & Akbal, E. (2017). Analysis of mobile phones in digital forensics. *40th Internation Convention on Information and Communincation Technology, Electronics and Microeletronics, MIPRO 2017*, (pp. 1241-1244).

Joshi, J., & Parekkh, C. (2016). Android smartphone vulnerailities: A survey. *2016 International Conference on Advance in Computing, Communication and Automation, ICACCA*, (pp. 1-5).

Khan, A., & Hussain Mansuri, Z. (2018). Comparative study of various digital forensics logical acquisition tools for android smartphones internal memory: A case study of Samsung Galaxy S5 and S6. *Journal of Advances Research in Computer Science, 1*(1), 357-369.

Lohiya, R., John, P., & Shah, P. (2015). Survey on mobile forensics. *International Journal of Computer Applications, 118*(16), 6-11.

Lwin, H., Aung, W., & Lin, K. (2020). Comparative analysis of android mobile forensics tools. *2020 IEEE Conference on Computer Applications, ICCA 2020*, (pp. 1-6).

Md. Salleh, R., Mohd., M., & Baharin Khalid, K. (2014). Validation of digital forensics tools for android tablet. *Journal of Information Assurance and Security, 9*, 19-26.

Meshram, P., & Thool, R. (2014). A survey paper on vulnerabilities in android OS and security of android devices. *2014 IEEE Global Conference on Wireless Computing and Networking*, (pp. 174-178).

Raji, M., Wimmer, H., & Haddad, R. (2018). Analyzing data from android smartphone while comparing between two forensic tools. *IEEE Southeastcon 2018*, (pp. 1-6).

Riadi, I., Sunardi, S., & Sahiruddin, S. (2019). Analisis forensik recovery pada smartphone android menggunakan metode National Institude of Justice (NIJ). *Jurnal Rekayasa Teknologi Informasi (JURTI), 3*(1), 87.

Riadi, I., Sunardi, S., & Sahiruddin, S. (2020). Perbandingan tool forensic data recovery berbasis android menggunakan metode NIST. *Jurnal Teknologi Informasi dan Ilmu Komputer, 7*(1), 197-204.

Sathe, S., & Dongre, N. (2018). Data acquisition techniques in mobile forensics. *Proceeding of the 2nd International Conference on Inventive System and Control, ICISC 2018*, (pp. 280-286).

Tajuddin, T., & Manaf, A. (2015). Forensic investigation and analysis on digital evidence discovery through physical acquisition on smartphone. *2015 Worl Congress on Internet Security, WorldCIS 2015*, (pp. 132-138).

Tayeb, H., & State, S. (2019). Android mobile device forensics: A review. *7th Internation Symposium on Digital Forensics and Security, ISDFS 2019*, (pp. 1-7).

Zinge, P., & Chatterjee, M. (2018). Comprehensive study of digital forensics branches and tools. *The International Journal of Forensic Computer Science, 13*(1), 22-28.