Forensics Acquisition and Analysis Method of IMO Messenger

Muchamad Kukuh Tri Haryanto
Department of Informatics
Universitas Islam Indonesia
Yogyakarta of Indonesia

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

Yudi Prayudi
Department of Informatics
Universitas Islam Indonesia
Yogyakarta of Indonesia

ABSTRACT
Nowadays, Instant Messenger (IM) applications (apps) have always been a main area of research for forensic examiners. IM apps are used by most of the people in the world since its' low cost to operator centered messaging services. Digital forensic examiners often conduct forensic analysis of Instant Messenger application for Android devices. After considering the existing research work in this field, this paper focused on conducting forensic analysis on IM's for android devices IMO. Tests were conducted on two android devices. The tests consisted of installing the IMO application on each Android device, conducting common user activities through the application, acquiring the physical image of each acquired logical image. The forensic analysis was aimed at finding the ways of determining the structure of folders in IMO application. If so, what and where are the contents of those folders to be used as forensic evidence? The test results show that the structure of folders in IMO application can be analyzed by acquisition process and it is stored on internal memory of Android devices in which it has consisted of 6 folders, in which 2 folders of them have subfolders that are consisted of image and videos from user activities and it could be studied by forensic examiners.

Keywords
Instant messenger application, Android, IMO, forensic examiners.

1. INTRODUCTION
Instant Messenger Application has proven to become a result of technology innovation which is practice and instant as a tool of sharing information. This application is used since they are low cost to operator centered messaging services. Beside for communication,

these applications can also be used for transaction both online and offline which enclosed the user numbers as their personal contacts. There are a lot of features of Instant Messenger Applications such as instant text messaging, group chats, sharing of photos, videos, and audio calls.

Since there are many functions of IM apps which can be used by the users, it cannot be detected whether they use it for good or crime activities. Phishers, fraudsters, child predators, terrorist groups and organized cybercriminals also use IM apps for their advantages. RSA Anti Freud Command Center (AFCC) said that cybercrime activities increased to 73% from 2013 until 2015 in all of the world and it caused financial loss of US 325 million. It is also said that in 2015 the cybercrime activities is done through the mobile internet, while 61% of deception exceeds mobile phones [1]. IM apps became the rich data sources for forensic examiners in their investigation and find evidence as the main sources in forensic research.

The rise of cybercrime made digital evidence become an inseparable part of the judicial system. Digital evidence, therefore, can be found from mobile phones, computers, ATM, and surveillance cameras. It is hard to imagine crime without any elements of digital evidence [2]. Mobile device forensics is a specialty in the field of digital forensics. Mobile device forensics is a science of discovering digital evidence from a mobile device under forensically sounds condition using accepted methods.

The forensic examination of mobile devices is a defiance for forensic examiners. Data that are found in mobile devices usually must be extracted by intervening on the devices [3].

IMO is one of instant messenger which is used by social media users. This application gives data transmission in real time through the internet that helps the users for sending a text message, group chats, sharing of photos, videos, and audio calls. IMO, therefore, is one of potential IM application that is used by cybercrime for their business. Although IMO apps are popular for social media users, there has been limited published research focused on identifying and analyzing forensic artifacts related to IMO apps. This paper, then, aims to analyze the ways of finings the folder structure and to investigate the contents of that folder. It is important to be done for maintaining the integrity of data in that application.

The structure of this paper is as follows: in section 2 related work from the digital forensic community is discussed. Section 3 concentrates on the outline of research methodology and procedures adopted followed by tests results in section 4 and discussion on the findings in section 5. Section 6 summarizes concluding remarks and future works. This paper, finally, ends with related references.

1.1 Literature Review
1.1.1 Digital Forensic
In recent years, digital forensic is very important because it becomes an integral part of the judicial system. The definition of digital forensic is proposed by some experts who studied about it. Miller, as one of those experts, said that digital forensics is the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidences derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminals or helping to anticipating unauthorized actions shown to be disruptive to planned operations [4].

Another definition is also proposed by Azhar (2012). As one of the digitals forensic experts, he said that digital forensics is the application of computer technology and science for studying and analyzing electronic artefacts and digital

artefacts in accordance with those digital artefacts for analyzing the relationship of those digital artefacts in order to detect the criminals activities and the position of criminals can be traced and caught for justifying their actions [5].

Digital forensic, therefore, has some science branch. One of them is forensic mobile. Forensic mobile is a branch of digital forensic that can restore digital evidence or mobile data with the application of justifying method [6].

Digital forensic can investigate mobile equipment which gives a lot of evidence of the use and the ability of that equipment in line with the restoration of information as an artifact [7]. Digital forensic, then, will develop quickly in line with the development of mobile phones.[8]

Research in the forensic investigation has focused on acquiring the physical image of Android devices using multiple methods and have analyzed various forensic artifacts such as call logs, lists of contacts, SMS/MMS, etc [9]. A study on how to analyze an android device forensically, especially focusing on the "HTC Incredible" phone is done by Racioppo et al in 2012 [10]. This study, then, introduced the use of Android devices for finding the artifacts in forensic investigation[11].

A research on the design and implementation of Android apps in collecting the useful data for internal investigation, including policy, violations, intellectual property theft, misuse, embezzlement, sabotage, and espionage is done in 2013 [12]. It is shown that digital forensic is important and needed in the Android forensic investigation[13].

1.1.2 SQLite

SQLite is a database which has a special characteristic of ACID compliant and has a small library code. SQLite is an open, database sources that are stable and it is popular because of its' small equipment, including Android. Android serves rational database for all applications that use SQLite [14]. This application can manage relational database engine for saving the data safety and efficiently. SQLite is structured in runtime Android, as a result, every Android application every Android application can make the basic data of SQLite[15]. There are some reasons why SQLite is very compatible with an Android application. First, the configuration of its database is null. It means that there is not database configuration for developers, so it is cheap to be used. It does not have a server and there is not running process of SQLite database [16].

This picture describes the architecture of the SQLite library. The information here is useful to those who want to understand or modify the inner workings of SQLite. as illustrated in Figure 1 below

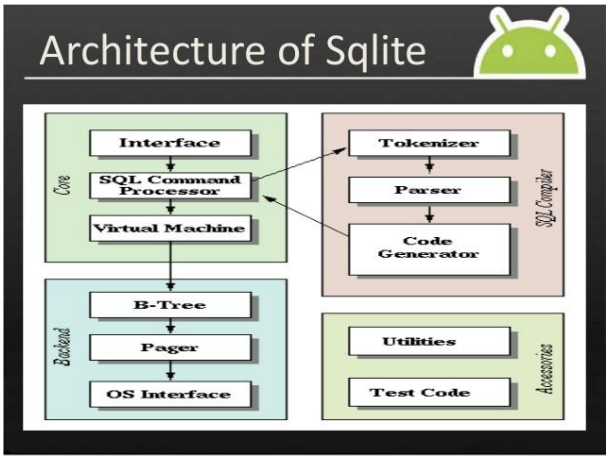

Figure 1. Architecture of SQLite

There are different functions of SQLite both in Browser Firefox and Smartphone Android. In Browser Firefox, SQLite is used for saving the configuration, bookmark, and the history of the website. In Android smartphone, then, SQLite usually is used for saving person contacts. SQLite, therefore, supports all of the platforms [17].

SQLite is an embedded database that is very popular now. There are many features, they are (1) no-dependency, (2) serverless and zero configuration, (3) compliance, and (4) has a lot of platforms [18]. Beside of those advantages, SQLite also has many disadvantages. They are: (1) some of SQLite syntax are not supported by right and outer join. The security of SQLite is not good. Since the system is limited to reading/write security, the security system must be managed by business logic layer application. To manage it, it is a need to apply a cryptography algorithm that can encrypted administrator data on SQLite database [19].

2. RESEARCH METHODOLOGY

2.1 Research Steps

In this research, the first step is conducting literature study that has a relationship with the research object. Furthermore, after finding the research object, the second step is carrying out a simulation of cases and accomplishing the scenario design to perform digital forensic investigation stage. Then, in IMO chat analysis phase, the activity that will be done is searching digital object in which it will later. The last step is making report analysis as the most important activity in the digital forensic stages.

Figure 2. Research Steps

2.2 Library Studies

Literature study means conducting research by studying and reading the literature that has a correlation **w**ith the problems that become the objects of research. Library study that is done as the first step in conducting a research had an aim for finding a problem to be studied. It means that the evidence or assertion in which the problem to be studied has not been answered or unsolved satisfactorily or has never been researched by people concerning the purpose, data, and methods, analysis and results for the same time and place. The literature study process can be seen in Figure 3 below:

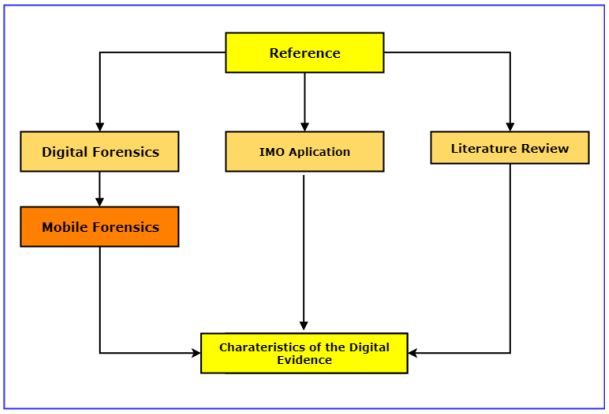

Figure 3. the literature study process

In collecting data related to the object of research, it is done by collecting reference materials that related to this research through books, articles, papers, journals, papers, and visited some websites related to mobile forensic, android architecture.

2.3 Examination

It is the data processing stage collected by digital forensics using a combination of various scenarios, both automatic and manual, as well as assessing and releasing the data accordingly needs while maintaining data integrity.

2.4 Simulations and Scenarios on IMO

The National Bureau of Standards (NIST) is a non-regulatory body of the Technology Administration of the United States Department of Commerce said that to test all tools and devices in conducting test must be included. Simulation is a necessary process for the operation of a model to mimic the actual behavior of the system. The goal is to prove the problem s formulation in this study. Simulation is done because it is not possible to investigate in a real case. Simulation is done by arranging scenario as shown in Figure 4

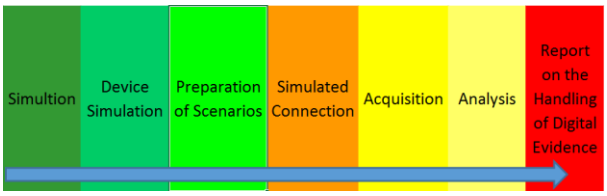

Figure 4. Simulation Procedures

The simulation will be conducted at UII Digital Forensic Research Center (Pusfid). In doing the simulation, it takes two smartphone devices Samsung Tab 3.8 and Samsung GT-S5312, then both devices communicating and sending chatting each other, sending pictures and video calling. The next step is to acquire or imaging towards both of those smartphones using Linux Santoku.

Software/software specifications that are used for digital evidence analysis, in this case, are as follows:

Table 1. The Software Requirements

No	Software	Functionality
1	Linux Santoku	Operating system Investigator laptop for acquisition
2	SQLiteman	Software to view results of data acquisition under Linux
3	DB Browser for SQLite	Software for analysis of data acquisition results

2.5 The Scenario Construction

In this step the scenarios to be performed are as follows[20]:

a. Smartphones based Android connected each other to the internet to communicate using the IMO Instant messenger app.
b. Communication by using the IMO app by making chatting, sending pictures and video calls in accordance with the simulation of connections which are made.
c. In the next step done the acquisition/imaging of both smartphones is using Linux to get imaging which will be analyzed.
d. In this step, an analysis of the IMO Evidence of both smartphones devices to obtain the digital evidence that is needed.
e. The last step is to perform an SQLite Record analysis towards the evidence that is found to obtain important information related to the IMO Instant messenger application.

2.6 Acquisition

The acquisition is an imaging process or a process to get data especially mobile phone devices that are used to commit criminal activities. In the process of gathering digital evidence, there are 3 extraction techniques that are used in mobile phone devices such as Physical Collection, Logical collection, and File System Extraction (Pardhasaradhi Chintalapati, 2015).

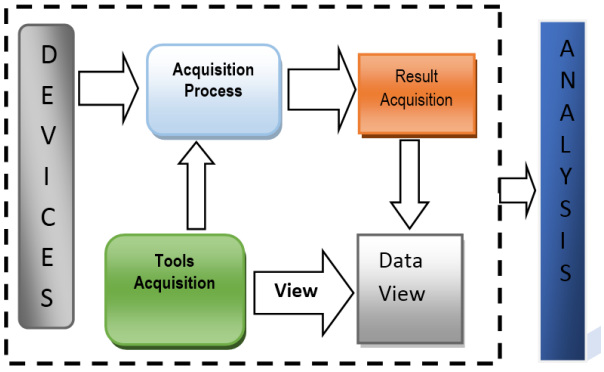

Figure 5. Data Acquisition Process

Aquisition process has some general steps, they are[21]:

a. Duplication of digital forensics is the technique of doubling the identical evidences to ensure the integrity of results and resources.
b. Hashing is conducted in order to find out the degree of similarity in the results of the original source of duplication.

c. Forensic extraction is the process in which data is taken or the forensic Analysis tools After getting the files or digital artefacts that are desired from the Investigation process to find out the metadata, time, user log, as well as how that data can be processed, read, and understood.

The final step of the forensic process is reporting. In this step, each of the findings and data analysis of SQLite on IMO application is presented in accordance with the analysis data that has been done. The findings data will be attached to the research analysis.

3. RESULT AND DISCUSSION

The simulations were conducted at the Center for Forensic Digital Studies (PUSFID) University Islam Indonesia. The imaging or acquisition process is a process for obtaining data, especially on smartphone devices used for crime. There are 3 extraction techniques commonly used in the process of gathering digital evidence of smartphones. These techniques are physical extraction, logical extraction, and file system extraction. Physical extraction is a bit-by-bit copy of all the flash memory of a mobile device which by this technique allows the full acquisition of hidden or deleted files. Logical extraction is an acquisition of a mobile device with a bit of bit in logical storage which includes files and directories that are in logical storage (file system). This acquisition allows the structure of the data system easier to be extracted and managed. File System Extraction, then, is an acquisition of files contained in the memory of mobile devices in which by this technique allows us to gain access to all the files contained in the memory of the mobile device (allocated space), including images, videos, database files, file systems, and logs.

The case study of forensic analysis of databases on IMO applications is obtained from the internal memory of IMO applications installed. Mobile phones are used in this study, there are 2 namely Smartphone Samsung Tab 3.8 and Samsung GT - S 5312, which serve as evidence by acquisition or imaging process to obtain data cloning or duplicate with the aim not to damage digital evidence. Tools or Applications OSE AF logical using Applications that run on Santoku Linux Operating system. Data acquisition process can be described in Figure 5.

The Acquisition process starts from cloning from the Smartphone's internal memory into SD card, then the process of making the file 'dd'. To ensure that the acquisition or imaging process performed can be accounted for or authenticated from the backup file obtained hash values as follows Figure 5.

3.1 Hashing

One common way of testing the integrity of a digital data is to use a hash function. The hash function is an algorithm that generates a digital data into a series of random characters in the same number. Hash also includes one form of cryptography without a key (unkeyed cryptosystem). When doing forensics, usually hashing algorithms use MD5 and SHA-1. In addition, hash has another name that is also widely known is "one-way function". This means the hash can not be returned in the description

Figure 6 describes the process of hashing to get evidence. The process of taking the Serial Hash on the acquisition file

Md5sum (space) (The location of the .dd file)

Md5sum /home/santoku/forensic/gts5312.dd

Md5sum /home/santoku/forensic/st311v2.dd

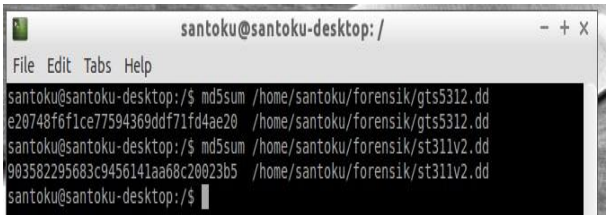

Figure 6. Hashing Of Digital Evidence

The hash value of the Samsung Smartphone Tab. 3.8 is shown in Table 2 and the hash value of Samsung GT-S 5312 hash value is shown in Table 3.

Table 2. Result Of Samsung Tab

No	Name	Info
1	File Dump	Path Smartphone Samsung Tab. 3.8 Size (bytes) 31.972.130.81 MD5903582295683c9456141aa68c20023 b5

Table 3. Result Of Samsung GT - S 5312

No	Name	Info
1	File Dump	Path Samsung GT - S 5312 Size (bytes) 1.975.448.064 MD5 6e20748f6f1ce77594369ddf71fd4ae20

From the process of acquisition of Samsung Smartphone Tab 3.8 and Samsung GT - S 5312 using "AF Logical OSE" shows that there is no constraints or problems in that process because the Linux Operation System Santoku reads USB driver fully [21]. The extract results that can be found in the chat IMO application consists of several folders such as the lib folder, cache, databases, files, no_backup, and shared_pref, as shown in figure 7.

Racioppo & Murthy (2012) in his study aims to know the contents of the directory on the HTC phone. Likewise, Iqbal et al (2014) also aim to know the contents of text data directory on the iPhone devise that runs on iO56 and Samsung Galaxy Android 4.1. However, Swati Bushan Deb & Sudhir Misra (2017) conducting case studies on IMO and Hike Messenger applications does not explain or know the contents of the data directory. They only explain the location or position of data directories in IMO and Hike Messenger applications. While here, the author, analyzes the evidence to find out the location and the contents of data contained in instant messenger IMO on 2 Smartphone Samsung Tab 3.8 and Samsung GT - S 5312. After the acquisition process, the extraction results in the Imo chat application showed that there were six folders. They were lib folder, cache folder, database folder, files folder, no-back up folder, and shared-pref folder. The results of the discovery of the six folders of the evidence are shown in detail in figure 7 below:

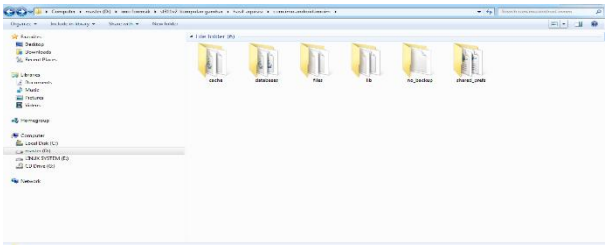

Figure 7. Folder Structure in IMO Application

In IMO application consisted of six folders, in which several folders filled with sub folders and no sub folders. 4 folders do not have sub folder (lab, files, no back-up, and shared-pref). there were 2 folders (cache and database) have sub folders. Directories in each folder are shown in Table 4 below:

Table 4. The directory in IMO application

No	older Name	The Contents of Folder
1	Lib	-
2	Cache	5 subfolder : - Exocatche - Com.android.renderscript.catche - Image_manager_disk_catche - webviewcatcheChromium - webviewcatcheChromiumStaging 10 file Image
3	Database	1 subFolder : - com.google.android.gms.ads.db 4 file database
4	Files	-
5	No_backup	-
6	Shared_prefs	-

After those folders are opened one by one, it is found some evidence that can be analyzed, they are the cache folder and database folder. In both those folders contains a collection of files from IMO user activities in the form of image and video files. In the cache folder, there are some image files and an eyecatcher subfolder containing 1 video file.

From the data obtained, it showed the details of the file name, file location, file size, and timestamp description when the image file is created. The location of all the image files is available at com.imo.adroid.IMO / cache. While the type/type of the image file is RIFF audio. The image file size varies from the largest size to 74.0 KB, and the smallest size is 20.1 KB. Besides the 10 image files, there is also 1 video file in the cache folder.

The type of video file is MPEG-4 with the size of 1.1 MB. Further analysis of the databases folder found 1 subfolder and some files that existed SQLite (*. Db) which can be opened by using SQLiteman Application on Linux Santoku or DB Browser for SQLite on windows. The DB files can be seen in Figure 8.

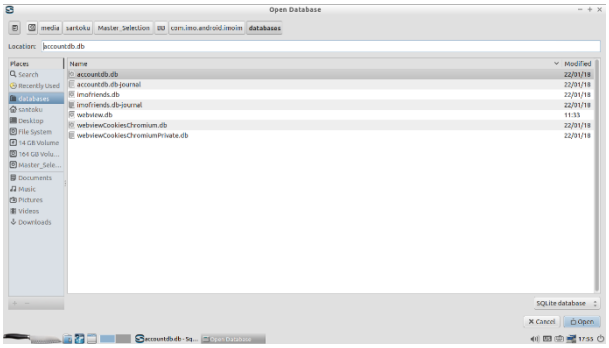

Figure 8. Structure Of DB Files

Figure 9 is the database file accountdb, there are two (2) tables which are filled with data, namely: account table and android metadata. In a table account, there is 1 user with a Serpente username that refers to the email name registered on the smartphone account. While in the android metadata table there is data content,

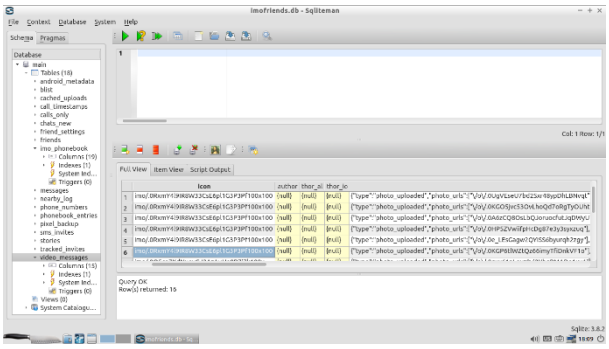

Figure 9. Video_message in database immofriends

4. CONCLUSION AND FUTURE WORK

The investigation process conducted on Samsung Tab 3.8 and Samsung GT-S5312 related to IMO application research can be summarized as follows: The process of acquisition method research using NIST with the use of AF OSE Application running Linux system to santoku can find the folder structure and its contents in the IMO application. The application running AF OSE logic on Linux system santoku also can read and show that there are 6 folders in the IMO application ie lib, cache, database, file, back_up, and no. shared_pref. of the six folders, it is just a folder and captures a database that has subfolders. Subfolders contain a collection of image and video files from the IMO user event app.After the six folders successfully opened, there are only 2 folders that have sub-folders containing images and video. which can be a reference to complement the evidence.

This research of SQlite Database on IMO Application using Linux Santoku for it's aquisition is only able to find Log-Video Call. Therefore, it is expected for the next research is able to search Video Call files on IMO Application based Android.

5. REFERENCES

[1] A. Fauzan, I. Riadi, and A. Fadlil, "*Digital Forensic of Line Messenger for Handling Cybercrime*," *Annu. Res. Semin.*, vol. 2, no. 1, pp. 159–163, 2017.

[2] A. S. and J.-P. V. B. Richard de Beer, "*Anti Forensics: A Practitioner perspective*," *Int. J. Cyber Secur. Digit. Forensics*, vol. 4 no.2, 2015.

[3] A. Simão, F. Sícoli, L. Melo, F. Deus, and R. Sousa Júnior, "*Acquisition and Analysis of Digital Evidence in Android Smartphones*," *Int. J. Forensic Comput. Sci.*, vol. 6, no. 1, pp. 28–43, 2011.

[4] D. A. Miller, J. B. Grand, T. F. Fondell, and M. Anthony, "*A Road Map for Digital Forensic Research*," *J. Anim. Ecol.*, vol. 75, no. 1, pp. 101–110, 2006.

[5] M. . Al-Azhar, Forensic Digital: *Practical Guide of Computer Investigation*. 2012.

[6] D. C. Harrill and R. P. Mislan, "*A Small Scale Digital Device Forensics ontology*," *Small Scale Digit. Device Forensics J.*, vol. 1, no. 1, pp. 1–7, 2007.

[7] R. Ayers, W. Jansen, and S. Brothers, "*Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1*)," *NIST Spec. Publ.*, vol. 1, no. 1, p. 85, 2014.

[8] 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.

[9] J. Lessard and G. C. Kessler, "*Android Forensics : Simplifying Cell Phone Examinations,*" *Small Scale Digit. Device Forensics J.*, vol. 4, no. 1, pp. 1–12, 2010.

[10] C. Racioppo and N. Murthy, "*Android Forensics : A Case Study of the ' HTC Incredible ' Phone*," *Proc. Student-Faculty Res. Day*, pp. 1–8, 2012.

[11] I. Riadi, Sunardi;, and A. Firdonsyah, "Forensic Investigation Technique on Android's Blackberry Messenger using NIST Framework," *Int. J. Cyber-Security Digit. Forensics*, vol. 16, no. 4, pp. 198–205, 2017.

[12] J. Grover, "Android forensics: *Automated data collection and reporting from a mobile device*," *Digit. Investig.*, vol. 10, no. SUPPL., 2013.

[13] A. Prayogo, I. Riadi, and A. Luthfi, "*Mobile Forensics Development of Mobile Banking Application using Static Forensic*," *Int. J. Comput. Appl.*, vol. 160, no. 1, pp. 5–10, 2017.

[14] D. R. Hipp, "*About SQLite*." [Online]. Available: https://www.sqlite.org/about.html. [Accessed: 02-Jan-2018].

[15] R. Meier, *Professional Android Application Development*. Wiley publishing,Inc, 2009.

[16] Mulyadi, *Create applications for Android*. Yogyakarta: Multimedia Center Publishing, 2010.

[17] A. Nugroho, *Developing applications Using C # Database and SQLite Servers*. Yogyakarta: CV. Andi Offset, 2010.

[18] S. T. Bhosale, T. Patil, and P. Patil, "*SQLite : Light Database System,*" *Int. J. Comput. Sci. Mob. Comput.*, vol. 4, no. 4, pp. 882–885, 2015.

[19] D. Ariyus, *An Introduction of Cripthograpy: Theories Analysis and Implementation*. Yogyakarta: CV. Andi Offset, 2008.

[20] M. P. Aji, I. Riadi, and A. Lutfhi, *"The digital forensic analysis of snapchat application using XML records*," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 19, pp. 4992–5002, 2017.

[21] R. Ruuhwan, I. Riadi, and Y. Prayudi, "Evaluation of integrated digital forensics investigation framework for the investigation of smartphones using soft system methodology," *Int. J. Electr. Comput. Eng.*, vol. 7, no. 5, pp. 2806–2817, 2017.