IDENTIFICATION OF DIGITAL EVIDENCE FACEBOOK MESSENGER ON MOBILE PHONE WITH NATIONAL INSTITUTE OF STANDARDS TECHNOLOGY (NIST) METHOD

[1]Anton Yudhana, [2]Imam Riadi, [3]Ikhwan Anshori

[1]Department of Electrical Engineering,Universitas Ahmad Dahlan, Indonesia
[2]Department of Information System,Universitas Ahmad Dahlan, Indonesia
[3]Department of Informatics, Universitas Ahmad Dahlan, Indonesia
Jl. Prof. Dr. Soepomo, S.H., Umbulharjo, Yogyakarta, Indonesia
[1]eyudhana@ee.uad.ac.id, [2]imamriadi@is.uad.ac.id, [3]ikhwananshoriuad@gmail.com

Abstract

Facebook Messenger is a popular social media. The increasing number of Facebook Messenger users certainly has a positive and negative impact, one of the negative effects is being used for digital crime. One of the sciences to get digital evidence is to do Digital forensics. Digital forensics can be done on a smartphone used by criminals. This research will carry out as much evidence of digital crime as possible from Facebook Messenger. In this study the forensic devices, Magnet AXIOM and Oxygen Forensics Suite 2014 were used using the National Institute of Standards Technology (NIST) method. NIST has work guidelines for both policies and standards to ensure that each examiner follows the same workflow so that their work is documented and the results can be repeated and maintained. The results of the research in the Magnet AXIOM and Oxygen Forensics Suite 2014 get digital evidence in the form of accounts, conversation texts, and images. This study successfully demonstrated the results of an analysis of forensic devices and digital evidence on Facebook Messenger. The results of the performance evaluation of forensic tools in the acquisition process using AXIOM Magnets are considered the best compared to Oxygen Forensics Suite 2014.

Keywords: Digital, Forensic, Facebook, Messenger, NIST.

INTRODUCTION

Currently, social media users are getting faster, one of them is Facebook Messenger, Facebook Messenger, social media application, which ranks second only to whatsapp is very popular. The increase in the number of Facebook Messenger users certainly has the effect of good and bad, one of the bad effects is that some people who use Facebook Messenger commit digital crimes. If the smartphone is evidence in criminal cases and Facebook Messenger is installed on a smartphone, If the smartphone is evidence in criminal cases and Facebook Messenger is installed on a smartphone, Figure 1 is the most downloaded social

media application graph in the Android Playstore application. Facebook Messenger is a social media application second after WhatsApp and under Facebook Messenger there are several popular social media applications, among others, imo, viber, skype, truecaller, browser, Line, WeChat, and Zaio. The total whatsapp applications for active users are 483,4m and Faebook Messenger reaches 397,0m.

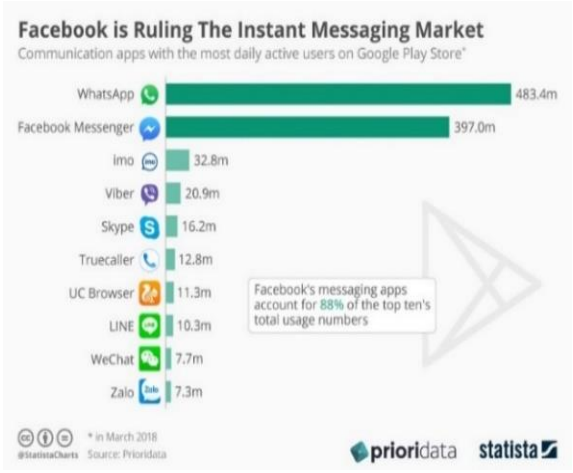


Fig. 1 Graph of facebook messenger users

In Figure 1 the Facebook Messenger application is a user with criminal purposes such as drug trafficking, terrorist activity, planning murder, and other criminal activities. Crime will definitely leave evidence, evidence as a report of crime in court.

Forensic analysis will provide details that will help investigators and investigative institutions to solve and link cases with reported crimes. Android is a set of open source software elements specifically designed and developed by Google for mobile devices. Although it has been designed and developed for mobile devices (for example, smartphones, tablets, etc.) [1].

Cellular forensics is a branch of digital forensics that deals with the recovery of digital evidence or data from mobile devices under healthy foren

sic conditions. The method used in this study was to raise evidence using a forensic method [2] [3].

The researcher will conduct forensic analysis on smartphones using several forensic tools with forensic tested methodologies, the results of the analysis will support evidence that has value validity before the law and can be used as a tool to resolve digital criminal cases [4] [5].

Live forensics is an analysis technique that involves data that runs on systems or volatile data that is generally stored in Random Access Memory (RAM) [6] [7]. Especially in the case of dead computers, forensic technology has been developed to investigate digital evidence directly [8] [9]. Dead Forensics is a technique that requires data stored permanently on a hard disk storage device [10] [11].

Security is a challenge for forensic information technology and law enforcement to investigate smartphones from someone who was made a suspect in a crime case [12] [13] . Based on the background above, we will conduct research on the analysis of digital evidence on Android-based Facebook Messenger using the National Institute of Standards Technology (NIST) method. Our study used a forensic tool called Magnet Axiom and Oxigen Forensic.

NIST METHOD

The method used to analyze digital evidence or the stage for obtaining information from digital evidence is the NIST method. Based on Figure 2, this can be explained in the following stages of cellular Forensic Analysis [14] :

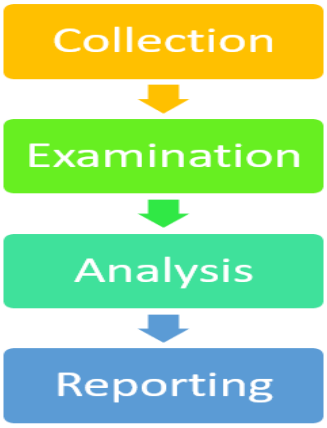


Fig. 2 NIST method process

- Collection is labeling, identifying, recording, and retrieving data from data sources that are relevant to the following procedures to maintain data integrity.
- Examination is the processing of data collected in forensic use in a combination of various scenarios, whether automatic or manual, and assessing and releasing data according to your needs while maintaining data integrity.
- Analysis is the analysis of examination results using justified technical methods and laws.
- Reporting is reporting the results of an analysis that includes describing the actions taken.

Table 2. Facebook messenger artifact

Artifact
User Account
Text
Image

Table 2 additional parameters listed are essential for investigator during investigation related to Facebook Messenger.

Table 3. Nist forensic tool parameters

Core Assertions	Optional Assertions	Core Features Requerements	Optional Features Requerement
MDT-CA-01	MDT-AO-01	MDT-CR-01 A	MDT-RO-01 A
MDT-CA-02	MDT-AO-02	MDT-CR-02 A	MDT-RO-02 A
MDT-CA-03	MDT-AO-03	MDT-CR-03 A	MDT-RO-31 A
MDT-CA-04	MDT-AO-04		
MDT-CA-05	MDT-AO-05		
MDT-CA-06	MDT-AO-06		
MDT-CA-07	MDT-AO-07		
MDT-CA-08			
MDT-CA-09			

The researcher used parameters from NIST as on Table 3 NIST lists the measurement parameters of forensic tools on two written reports entitled mobile device tool the additional parameters are more focused on the abilities of forensic tools to extract artifacts from Facebook Messenger for logical acquisition and physical acquisition [15] [16].

RESULT AND DISCUSSION

The results of the research that we did have obtained results. The process of obtaining evidence on an Android smartphone uses Axiom Magnet forensic software. Table 1 is a tool and material used, there is 1 Acer E14 laptop that has been installed with Windows 10 OS, 1 piece of Samsung galaxy V + SM-G318HZ Smartphone which contains Kitkat Android OS 4.4.4.

Facebook messenger android application installed on a Samsung Galaxy V + SM-G318HZ Smartphone and using Magnet Axiom Forensics and Oxigen Forensics Suite tools.

Table 1. Experiment tools

	Name	**Specification**	**Hardware/ Software**
1	Laptop	Acer E14, Windows10	Hardware
2	Smart phone	Samsung Galaxy V+ SM-G318HZ	Hardware
3	Facebook Messenger	Android application	Software
4	Magnet Axiom Forensics	Tools Forensics	Software
5	Oxigen Forensics Suite	Tools Forensics	Software

The researcher used calculations with index numbers to determine the performance of each forensic tool in accordance with the experiment results. The calculation of index number used is unweighted index [17].

$$Pon = \frac{\sum Pn}{\sum Po} \; x \; 100\%$$

Information :

ΣPo = The Result of Data Acquisition Tools

ΣPn = The Total Number Of Parameters

Pon = Percentage results are expected

The first to do the stage collection. Collection is labeling, identifying, recording, and retrieving data from data sources that are relevant to the following procedures to maintain data integrity. Retrieving data from data sources that are relevant to the following procedures to maintain data integrity. In the collection process using Android.

Fig. 3 Smartphone samsung galaxy v+ SM-G318HZ

In figure 3 is the Smartphone that is used, namely samsung galaxy v+ SM-G318HZ. The smartphone used is the rooting process. Rooting is the process of opening total access on an Android smartphone. In the collection process using Android. Android used for this researchkitkat version 4.4.4. The smartphone used is samsung galaxy v+ SM-G318HZ.

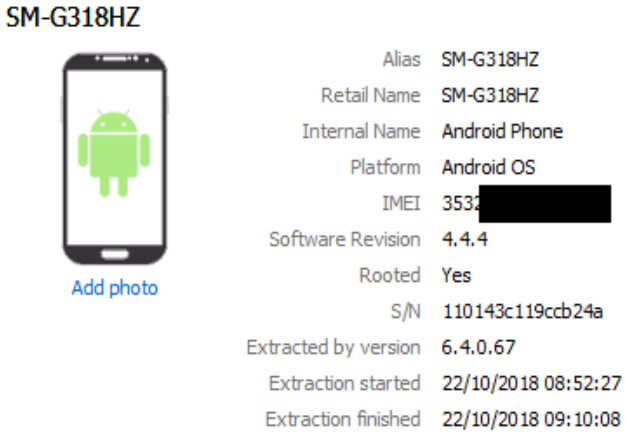


Fig 4. Oxygen forensic smartphone information

Table 4. Spesification smartphone

Brand	Samsung
Serial	Galaxy
Model	V+
Model #	SM-G318HZ
IMEI	353248072061xxx
OS	Android
Version	4.4.4 (Kitkat)
CPU	ARM Cortex-A7 Dual-core 1.2 GHz

Figure 4 and Table 4 explains the specifications on the Samsung Galaxy V + SM-G318HZ smartphone that are read by Oxigen Forensics Suite .

The second performs the stage examination. Examination is the processing of data collected in forensic use in a combination of various scenarios, whether automatic or manual, and assessing and releasing data according to your needs while maintaining data integrity.

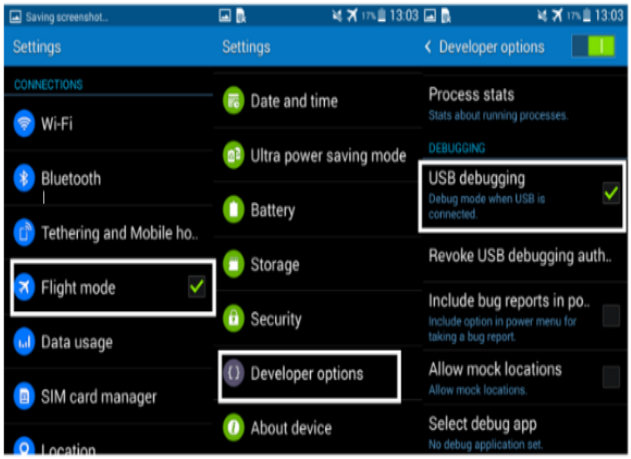


Fig. 5 Stage of examination on a smartphone

Figure 5 is the examination stage, the phone has been installed with facebook messenger, in the smartphone settings it is set to flight mode settings so that no internet data is running, then activate USB debugging developer options.

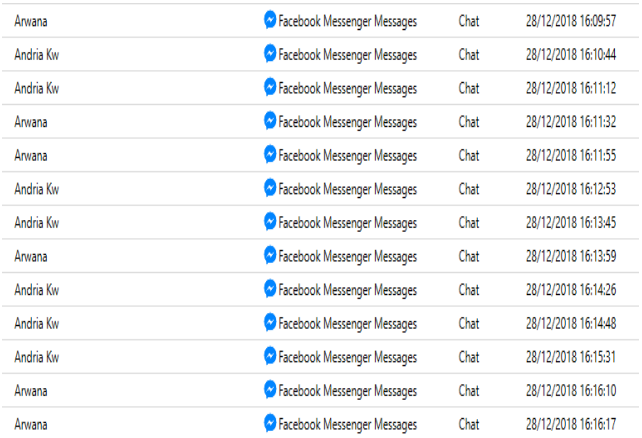


Fig 6. Examination using magnet axiom forensics

Figure 6 there is a display of evidence that will be examined. the picture contains text message and image data.

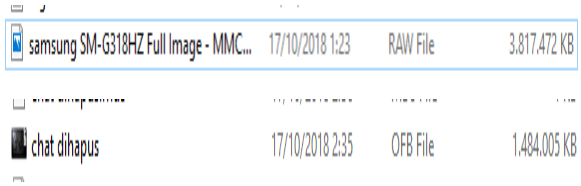


Fig. 7. Dump file using a forensics magnet axiom and oxigen forensics suite

Figure 7 is the result of a dump file on Axiom Forensics Magnet and Oxigen Forensics Suite . This stage is done to back up data from a smartphone by cloning data per byte so that it can resemble the original data, the results of processing image data cannot be changed or added and reduced but only can be opened using other forensic devices for inspection purposes.

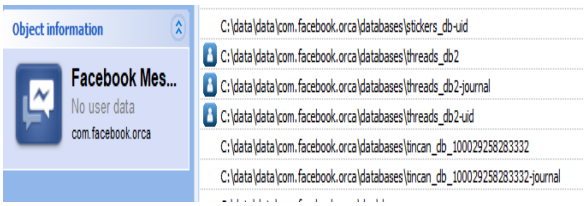


Fig 8. Examination using oxigen forensic suite

Figure 8 there is a display of evidence that will be examined. the picture contains text message and image data.

The third performs the stage analysis. In the analysis phase using the Magnet Axiom Forensics and Oxigen Forensics Suite tools. The results were in the form of user accounts, text conversations and images.

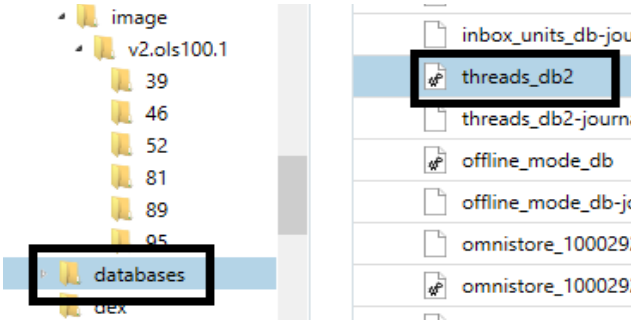
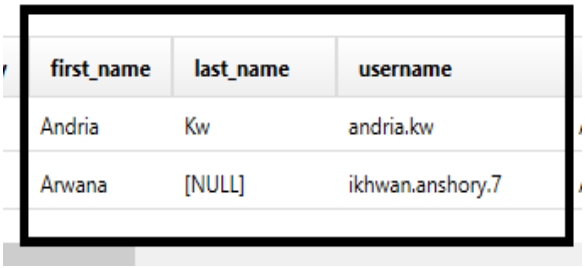


Fig. 9 The database magnet axiom forensics.

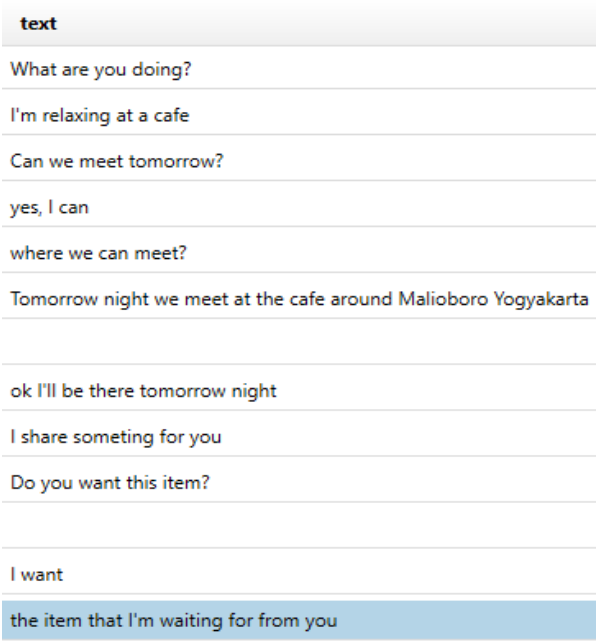
Figure 9 shows the text and user account in the database. there is a database and threads_db2 is contained in it, in thread_db2 there is a user account and text conversation.



first_name	last_name	username
Andria	Kw	andria.kw
Arwana	[NULL]	ikhwan.anshory.7

Fig. 10 Conversation account results

Figure 10 is the result of a conversation account on Facebook Messenger, the account named "Andria Kw and Arwana".



text
What are you doing?
I'm relaxing at a cafe
Can we meet tomorrow?
yes, I can
where we can meet?
Tomorrow night we meet at the cafe around Malioboro Yogyakarta
ok I'll be there tomorrow night
I share someting for you
Do you want this item?
I want
the item that I'm waiting for from you

Fig. 11 Conversation results obtained

timestamp_ms
1546013397057
1546013444301
1546013472881
1546013492337
1546013515060
1546013573355
1546013625550
1546013639055
1546013666538
1546013688532
1546013731693
1546013770418
1546013777803

Fig. 12 Timestamp conversation results obtained

Figure 11 is the result of the conversation obtained and figure 12 is the timestamp for each message on Facebook Messenger using Magnet Axiom.

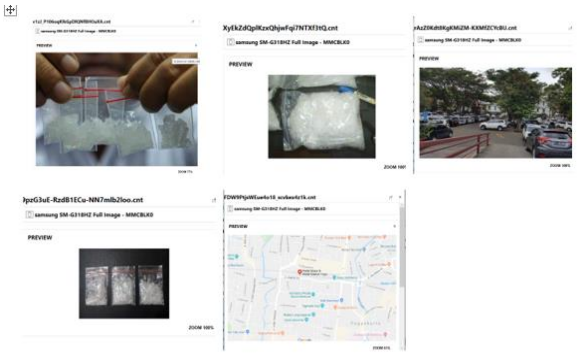


Fig. 13 The results obtained are in the form of an image

Figure 13 there are results of images on facebook messenger using Magnet Axiom Forensics. In the picture there are five types of images, there are three pictures of drugs, one map image and one picture of a region.

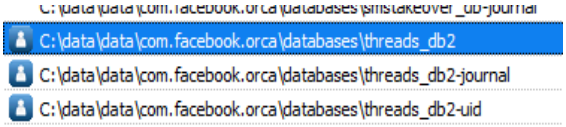


Fig. 14 The database contains accounts and text conversations

Figure 14 there is a database and threads_db2 is contained in it, in thread_db2 there is a user account and text conversation.

first_name	last_name	username	name
And<TRIAL>	Kw	andr<TRIAL>	Andr<TRI...
Arw<TRIAL>		ikhwan.a<TRIAL>7	Arw<TRIAL>

Fig. 15 Conversation account results

Figure 15 is the result of a conversation account on Facebook Messenger, the account named "Andria Kw and Arwana".

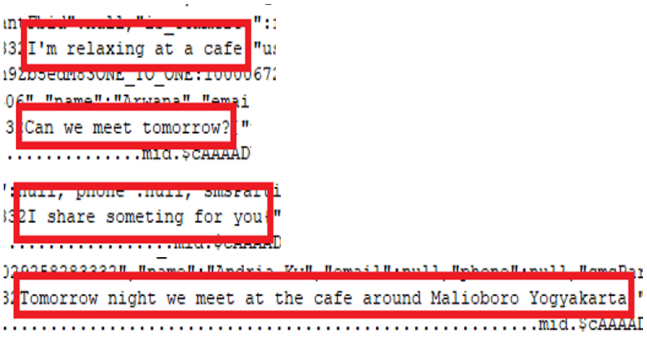


Fig. 16 Conversation results obtained

Figure 16 is the result of the conversation obtained on Facebook Messenger using Oxigen Forensics Suite.

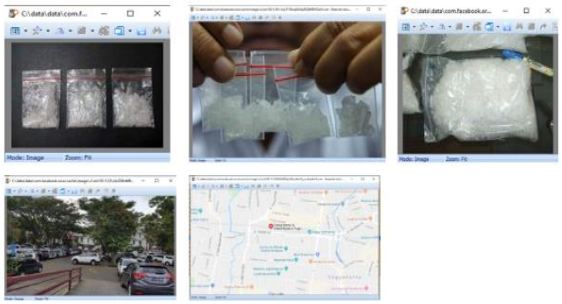


Fig. 17 The results obtained are in the form of an image

Figure 17 there are results of images on facebook messenger using Axiom Forensic. In the picture there are five types of images, there are three pictures of drugs, one map image and one picture of a region.

The fourth performs the stage reporting. Reporting is reporting the results of an analysis that includes describing the actions taken. Table 4 explains the comparison tools, namely Magnet Axiom Forensics and Oxigen Forensics Suite . From the comparison results obtained different results that the Oxigen Forensics Suite tool obtained a value of 79% while the Axiom Forensics Magnet got a value of 75%. From these results it can be seen that Oxigen Forensics has a higher rating than the Axiom Forensics Magnet using the parameter NIST method.

Table 4. The results of the parameter

Measurement Parameter		**Forensic Tools**	
		Magnet Axiom Forensics	Oxigen Foremsics Suite
Core Assertions	MDT-CA-01	√	√
	MDT-CA-02	-	-
	MDT-CA-03	-	-
	MDT-CA-04	-	-
	MDT-CA-05	√	√
	MDT-CA-06	√	√
	MDT-CA-07	√	√
	MDT-CA-08	√	√
	MDT-CA-09	√	√
Optional Assertions	MDT-AO-01	√	√
	MDT-AO-02	-	-

Optional Assertions	MDT-AO-03	√	√
	MDT-AO-04	-	√
	MDT-AO-05	√	√
	MDT-AO-06	√	√
	MDT-AO-07	√	√
Core Features Requirements	MDT-CR-01 A	√	√
	MDT-CR-02 A	-	-
	MDT-CR-03 A	√	√
Optional Features Requirements	MDT-RO-01 A	√	√
	MDT-RO-02 A	-	-
	MDT-RO-03 A	√	√
Logical Acquisition Artifact	User account	√	√
	Image	√	√
	Text	√	√
Indext Score		75%	79%

CONCLUSION

Based on the results obtained in this study the results of the comparison of Oxigen Forensics Suite tools and Axiom Magnets on Facebook Messenger using NIST method parameters have found that the Axiom Magnet has a value of 75% and Oxigen Forensics Suite of 79%. Subsequent research can add other tools to get accurate results.

BIBLIOGRAPHY

[1] P. Albano, A. Castiglione, G. Cattaneo, and A. De Santis, "A Novel Anti-Forensics Technique for the Android OS," no. November 2016, 2011.

[2] U. Rusydi, R. Imam, and Z. Guntur Maulana, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, p. 949, 2018.

[3] N. Al Mutawa, I. Baggili, and A. Marrington, "Forensic analysis of social networking applications on mobile devices," *Digit. Investig.*, vol. 9, no. SUPPL., 2012.

[4] 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.

[5] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Slod State Drive Dengan Metode National Institute of Justice (Nij)," vol. 3, no. May, pp. 70–82, 2018.

[6] E. Wahyudi, U. I. Indonesia, I. Riadi,

U. A. Dahlan, Y. Pray, and U. I. Indonesia, “Virtual Machine Forensic Analysis And Recovery Method For Recovery And Analysis Digital Evidence,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 16, no. 2, pp. 1–7, 2018.

[7] V. L. L. Thing, K. Ng, and E. Chang, “Live Memory Forensics of Mobile Phones By Vrizlynn Thing , Kian-Yong Ng and Ee-Chien Chang,” 2010.

[8] R. Ahmed and R. V Dharaskar, “Mobile Forensics : an Overview , Tools , Future trends and Challenges from Law Enforcement perspective,” pp. 312–323.

[9] R. Ayers and R. P. Mislan, “Hashing Techniques for Mobile Device Forensics,” vol. 3, no. 1, pp. 1–6, 2009.

[10] R. Imam and P. Yudi, “Evaluation of Integrated Digital Forensics Investigation Framework for the Investigation of Smartphones Using Soft System Methodology,” vol. 7, no. 5, pp. 2806–2817, 2017.

[11] F. Albanna and I. Riadi, “Forensic Analysis of Frozen Hard Drive Using Static Forensics Method,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 1, pp. 173–178, 2017.

[12] 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.

[13] X. Lee, C. Yang, S. Chen, and J. Wu, “Design and Implementation of Forensic System in Android Smart Phone,” pp. 1–11.

[14] R. Umar, I. Riadi, and Z. Guntur Malulana, “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.

[15] U. Rusydi, R. Imam, and M. Bashor fauzan, “Acquisition Of Email Service Based Android,” vol. 3, no. 4, pp. 1–9, 2018.

[16] Imam, 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.

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