HASIL CEK_60020397_Point-C5-IRD-850GB-Mobile Forensic Tools Validation and Evaluation for Instant Messaging

by Imam Riadi 60020397

Submission date: 11-Dec-2020 09:32AM (UTC+0700)

Submission ID: 1471625587

File name: rensic_Tools_Validation_and_Evaluation_for_Instant_Messaging.pdf (1.49M)

Word count: 5216

Character count: 27967

International Journal on
Advanced Science
Engineering
Information Technology

Vol.10 (2020) No. 5
ISSN: 2088-5334

Mobile Forensic Tools Validation and Evaluation for Instant Messaging

Guntur M. Zamroni[a,1], Imam Riadi[a,2]

[a]*Department of Informatics Engineering, Universitas Ahmad Dahlan, Yogyakarta, 55191, Indonesia*
E-mail: [1]guntur.zamroni@tif.uad.ac.id; [2]imam.riadi@is.uad.ac.id

***Abstract*—Mobile technology is experiencing rapid development from year to year. Various types of models and operating systems are available on the market, followed by the development of applications for mobile devices. Behind the development of mobile technology, mobile devices are often used for crime. To handle a case related to a mobile device, an investigator needs to use forensic methodologies. Investigator also needs to know which tools are capable of handling mobile forensics of a specific artefact or mobile devices since each forensic tool has its limitation. The rapid development of mobile technology and the lack of understanding of forensic tools sometimes become an obstacle for an investigator in handling a case. This research conducted a forensic analysis of WhatsApp (WA) application on the Samsung Galaxy S4 and Samsung A3 using the logical acquisition of 3 forensic tools, namely: WA Key/DB Extractor, Oxygen Forensics, and Magnet AXIOM. National Institute of Standards and Technology (NIST) forensic tool parameters and additional parameters related to WA artefact s were used to evaluate forensic tools which will then be calculated to find acquisition capability index for each forensic tool. Acquisition capability index is expected to provide an overview and recommendations regarding forensic tools for conducting WA forensic analysis. Based on the acquisition capability index, Magnet AXIOM has advantages over Oxygen Forensics, and WA Key/DB Extractor in conducting forensic analysis of WA artefact s on Samsung Galaxy S4 and Samsung A3 with 77.77%. Thus it can be concluded that Magnet AXIOM is recommended to be used in handling WA artefacts.**

***Keywords*— mobile forensics; NIST; WhatsApp; validation; acquisition.**

I. Introduction

WhatsApp (WA) is one of the smartphone applications that are quite popular. This can be seen from the increase in the number of WA users from year to year. WA globally has increased the number of active users per month, as shown in Fig. 1. In April 2013 WA had a total of 200 million users per month, and in December 2017 WA had 1.5 billion users per month [1]. WA had a total of 20.5 million users in 2017 in the United States, and it is predicted that by 2021 there will be 25.6 million users, as shown in Fig. 2 [2]. In Indonesia alone, in March 2017, WA ranked first for the Instant Messaging application, with 35.8 million users [3]. WA is a popular Instant Messaging application on smartphones with a percentage value of 60%, followed by Viber and Telegram [4].

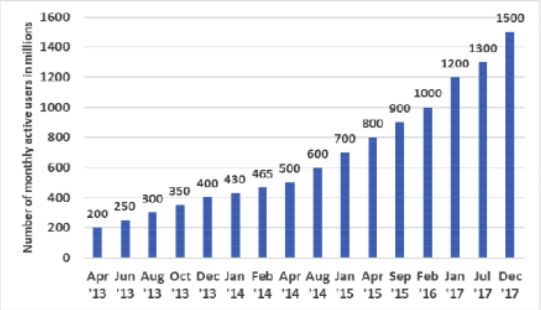

Fig. 1 Number of Monthly Active WA Users Globally

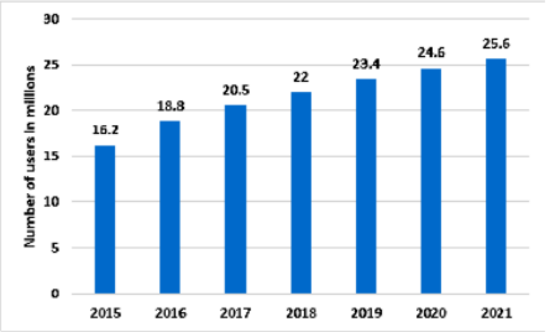

Fig. 2 Number of WA Users in the United States of America

Behind the popularity of WA, there have been several cases of crimes involving WA such as media to spread hoaxes, sexual harassment, pornography, bullying, drug trafficking, human trafficking, and data theft [5]–[8]. WA also has been used as a tool to search for evidence in handling crime cases [9], [10]. For handling a case with evidence in the form of a mobile device, a specific forensic methodology is needed. A forensic methodology known as the National Institute of Standards and Technology forensic methodology (NIST) explained the method for conducting mobile forensic analysis consisting of preservation, acquisition, examination and analysis, and reporting stages [11]. It explained artefacts from smartphone devices that can be used as evidence such as contact lists, text messages, instant messaging conversations, images, audio and video, document files, geolocation and so on.

There have been several studies related to the forensic mobile operating system of Android, WA, and other Instant Messaging applications. A forensic analysis of WA applications on iPhone devices with the operating system of iOS 5.0.1 using Oxygen Forensics and UFED Cellebrite [12]. From the experiment results, it can be seen that although Oxygen Forensics had access to limited devices compared to UFED Cellebrite in terms of Web History, Cookies, Passwords, User Accounts, and Web Bookmarks, Oxygen Forensics has the advantage of getting more information about the WA application.

Forensic analysis has been studied on Blackberry Messenger using the NIST methodology and Andriller forensic tool [13]. NIST forensic methods could be applied to digital evidence acquiring process from Blackberry Messenger on Android operating system. Another study conducted a forensic analysis using Oxygen Forensics and MOBILedit tools [14]. It seems that MOBILedit has faster performance than Oxygen Forensics. Researchers also argue that live analysis is not recommended in the process of investigating a case involving a smartphone device because it can damage the evidence. Each forensic tool has its strengths and weaknesses. For this reason, it is necessary to use more than one forensic tool in handling a case.

Forensic tools could be used to compare the capabilities of data acquisition among smartphone devices [15]. The parameters used in this test are runtime and the type of acquisition (live or static). From the testing, it can be seen that the Forensics Toolkit is superior in terms of runtime compared to Digital Detective Blade v1.13 and Kernel Database Recovery. The researcher also recommends using the Forensics Toolkit for static type data.

The validation of the forensic WA Key/DB Extractor 4.7 and Belkasoft Evidence was tested and resulting in a fact that forensic tool used successfully fulfilled the Samsung Galaxy S4 artefact validation test [16]. Although the study was unsuccessful in getting all the artefacts, the forensic tools were stated to fulfil repeatability and reproducibility tests as similar artefacts, and the same number of artefacts were found.

Android devices have to dominate the smartphone market [17]. For this reason, an understanding and solution is needed to investigate a case related to Android devices. Knowing the type of software and hardware from an Android device is crucial to determine the type of forensic tool used to conduct an investigation. Hence, we need a standard to measure the performance of forensic tools. The standards of forensic tools and features that should be owned by a forensic tool were discussed in the previous studies [18], [19]. These features include the acquisition process and the ability of forensic tools to make acquisitions on a logical, physical, and UICC basis.

Mobile forensic has several challenges such as the absence of a standard method for data acquisition processes, the large number and version of the operating system for smartphones which makes it necessary to update forensic tools and techniques for conducting mobile forensic [20], [21], [22]. The rapid development of mobile technology such as the emergence of new models and types of smartphones, operating system updates, hardware and software updates become a challenge for forensic analysts to be able to adjust to such changes [23].

From the explanation above, researchers conducted a forensic analysis of the WA application and tools evaluation. The forensic tools used in this research were Oxygen Forensics, Magnet AXIOM (trial ver), and WA Key/DB Extractor. Samsung Galaxy S4 and Samsung A3 devices with Android 5.0 Lollipop and Android 6.0 Marshmallow were used for the experiment. Android Lollipop and Android Marshmallow are Android operating systems that are widely used by smartphone users [24]. The differences between this research and previous studies are that this research emphasizes on the validation aspects of forensic acquisition and evaluation of forensic tools using the parameters of forensic tools from NIST and additional parameters focused on WA artefacts on Samsung Galaxy S4 and Samsung A3 devices. This research was expected to provide recommendations for mobile forensic tools and help investigators to handle cases related to WA and Android devices.

II. Materials and Method

A. *Materials*

The materials used in this research were divided into two types, hardware and software. Table 1 shows the hardware used for the research. This research used two smartphone devices as research objects which were, Samsung Galaxy S4 with the Android version 5.0 Lollipop and Samsung A3 with the Android version 6.0 Marshmallow. Desktop computers used as workstations for analysis and USB connectors were used as a medium to connect smartphone devices to desktop workstations. Table 2 shows the software used in the research. The software used was divided into software test, operating systems, forensic tools, and analysis tools.

TABLE I
Hardware Materials

No	Hardware	Description
1	Samsung Galaxy S4 GT-I9500	Android Lollipop, Unrooted, Experiment Device
2	Samsung A3 SM-A310F	Android Marshmallow, Unrooted, Experiment Device
3	Desktop, Intel i5-4440, 8,00 GB RAM	Windows 7 64 Bit
4	USB Connector	Smartphone and workstation connecting device

TABLE II
SOFTWARE MATERIALS

No	Software	Version	Description
1	WhatsApp	2.17.351	Testing Software
2	Windows 7		Workstation Operating System
3	WA DB/Key Extractor	4.7	Forensic Tool
4	Oxygen Forensics 4.7	6.4.0.67	Forensic Tool
5	Magnet AXIOM	2.7.1.12070	Forensic Tool
6	Igorware Hasher x64		Hashing Tool

B. Method

This research focused on the forensic analysis process and forensic tools evaluation. Therefore researchers used two approaches, namely: Forensic Analysis and Tools Evaluation. Fig. 3 shows a forensic analysis stage used in this research. In the Forensic analysis stage, researchers simulated the use of the WA application on Samsung Galaxy S4 and Samsung A3. The simulations resembled the daily use of WA applications such as sending and receiving messages, voice and video calls and transferring files in the form of images, videos and documents.

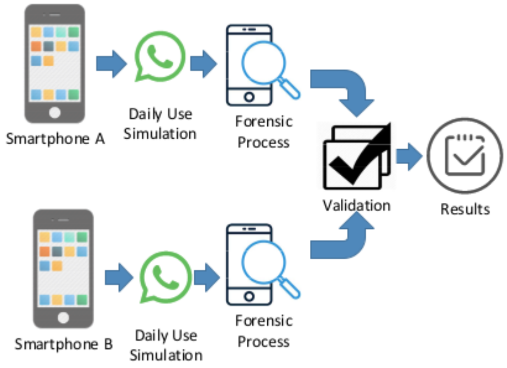

Fig. 3 Forensic Analysis Stages

The forensic analysis then carried out using forensic methodology from NIST, which has four stages, namely: Preservation, Acquisition, Examination & Analysis, and Reporting. Preservation conducted by made a logical backup of evidence followed with Acquisition where WA artefact s will be identified and extracted from logical backup files [25]. Examination & analysis then carried out to find proof followed by Reporting. Validation and results analysis was carried out after the forensic process. Validation was conducted to prove that the forensic process and forensic tools are suitable to use, and the results can be accepted as evidence before the law. There were two main validation stages: repeatability and reproducibility. Repeatability test is conducted by doing repeated testing two times or more of the same object using the same forensic tool within small time differences. At the reproducibility test, a similar object will be tested using two or more different forensic tools within small time differences [11]. Hashing will be used as an additional validation tool. Hashing can be used to identify evidence, verify data, authenticate data, and view data integrity [26]. The hashing value calculation is needed to find out the hashing value of a file. The hashing value provides unique values regarding data as well as DNA testing. If the evidence is modified, the hashing value will be different [27]. Igorware Hasher x64 was used as a hashing tool to find and compare the hashing values of 2 or more artefacts from the acquisition of forensic tools. After the validation stage, it was continued by analyzing the results using measurement parameters.

Forensic tools evaluation conducted by analyzing forensic process and results, as shown in Fig. 4. Mobile forensic tools parameters used in this research. NIST, in the publication entitled "Mobile Device Specification Tool Version 2.0" and "Mobile Device Test Tool Assertions and Test Plan Version 2.0" provided parameters regarding forensic tools [18], [19]. Table 3 shows the parameters of the NIST forensic tool used in this research to analyze and measure the results of the forensic process. This research was limited to logical acquisitions by adjusting to the conditions of the smartphone devices used in the experiment. The physical acquisition was not used because the smartphone devices used in the research were unrooted, and the UICC was not used because WA artefacts are not at the UICC.

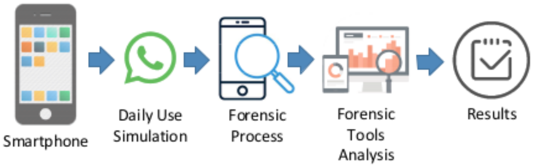

Fig. 4 Tools Evaluation Stages

TABLE III
NIST FORENSIC TOOLS PARAMETERS

Core Assertions	Core Assertions
MDT-CA-01	MDT-CR-01 A
MDT-CA-02	MDT-CR-02 A
MDT-CA-03	MDT-CR-03 A
MDT-CA-04	
MDT-CA-05	
MDT-CA-06	
MDT-CA-07	
MDT-CA-08	
MDT-CA-09	

TABLE IV
WA ARTEFACT S PARAMETERS

Artefact
WA Contact List
WA Logs
Text
Image
Video
Document

This research applied additional parameters in the form of WA artefact s as in Table 4 to strengthen the analysis of the abilities of forensic tools in conducting WA forensic analysis [28]. The analysis results were then calculated using an unweighted index number and ended with the conclusion stage, where the researcher concluded from the research. Index numbers provide a comparison of values that are easy to understand and can be used for various types of data [29]. In this research index numbers were used to determine the acquisition capabilities of forensic tools based on parameters from NIST with the calculation equation of:

$$P_{on} = \frac{P_n}{P_o} \times 100 \qquad (1)$$

III. Results and Discussion

Validation aims to test that the forensic process and the evidence do not change and the integrity is maintained so that it can be recognized before the law. There are three types of validation tests used, namely: repeatability, reproducibility, and hashing. Repeatability and reproducibility were main validation tests. Hashing test was used as an additional validation test.

A. Repeatability

Table 5, Table 6, and Table 7 show the results of repeatability test performed on Samsung Galaxy S4. Forensic tools used successfully acquired Samsung Galaxy S4 artefact s. From the repeatability test, it can be seen that the number of artefact s obtained from 2 different acquisition processes have the same number of artefact s.

TABLE V
Repeatability Test on Samsung Galaxy S4 Using Oxygen Forensics

No	Artefact Type	Acquisition 1	Acquisition 2
1	Text	17	17
2	Image	629	629
3	Video	18	18
4	Document	11	11
5	Contact List	910	910
6	WA Log	5	5

TABLE VI
Repeatability Test on Samsung Galaxy S4 Using Magnet AXIOM

No	Artefact Type	Acquisition 1	Acquisition 2
1	Text	-	-
2	Image	640	640
3	Video	1	1
4	Document	4	4
5	Contact List	333	333
6	WA Log	-	-

TABLE VII
Repeatability Test on Samsung Galaxy S4 Using WA Key/DB Extractor

No	Artefact Type	Acquisition 1	Acquisition 2
1	Text	44	44
2	Image	3	3
3	Video	-	-
4	Document	-	-
5	Contact List	1173	1173
6	WA Log	2	2

Oxygen Forensics successfully acquired Samsung A3 artefact s but did not get any WA artefact s as shown in Table 8. Table 9 shows the number of artefacts s from acquisition using Magnet AXIOM. Magnet AXIOM was not able to retrieved Text artefact and WA Log artefact. WA Key/DB Extractor did not successfully carry out the acquisition process, so it did not get artefact s from Samsung A3 as shown in Table 10.

TABLE VIII
Repeatability Test on Samsung A3 Using Oxygen Forensics

No	Artefact Type	Acquisition 1	Acquisition 2
1	Text	-	-
2	Image	-	-
3	Video	-	-
4	Document	-	-
5	Contact List	-	-
6	WA Log	-	-

TABLE IX
Repeatability Test on Samsung A3 Using Magnet AXIOM

No	Artefact Type	Acquisition 1	Acquisition 2
1	Text	-	-
2	Image	12448	12448
3	Video	116	116
4	Document	49	49
5	Contact List	350	350
6	WA Log	-	-

TABLE X
Repeatability Test on Samsung A3 Using WhatsApp Key/DB Extractor

No	Artefact Type	Acquisition 1	Acquisition 2
1	Text	n/a	n/a
2	Image	n/a	n/a
3	Video	n/a	n/a
4	Document	n/a	n/a
5	Contact List	n/a	n/a
6	WA Log	n/a	n/a

Table 11 shows the repeatability test results of the forensic tools used in the research. All forensic tools used successfully fulfil repeatability tests for logical acquisition on Samsung Galaxy S4. For repeatability tests on Samsung A3, only WA Key/DB Extractor did not meet the test because WA Key/DB Extractor could not make an acquisition. Oxygen Forensics did not retrieve any WA artefact s on Samsung A3. Even so, Oxygen Forensics was stated to fulfil the repeatability test because of the same number of artefact s other than WA artefact s were found from 2 successful acquisition processes.

TABLE XI
Repeatability Test Results

No	Smartphone Device	Oxygen Forensics	Magnet AXIOM	WA Key/DB Extractor
1	Samsung Galaxy S4	√	√	√
2	Samsung A3	√	√	-

B. Reproducibility

Table 12 shows the results of the reproducibility test for forensic tools used. All forensic tools used fulfilled the logical reproducibility acquisition tests on Samsung Galaxy S4. Although the number of artefact s from acquisition result using Oxygen Forensics and Magnet AXIOM was different, Oxygen Forensics and Magnet AXIOM met the Reproducibility test due to the similarity of the artefacts from WA acquisition result. WA Key/DB Extractor did not meet the reproducibility test for Samsung A3 as it could not acquire, so no artefacts were obtained.

TABLE XII
REPRODUCIBILITY TEST ON SAMSUNG GALAXY S4

No	Artefact Type	Oxygen Forensics	Magnet AXIOM	WA Key/DB Extractor
1	Text	17	-	44
2	Image	629	640	3
3	Video	18	1	-
4	Document	11	4	-
5	Contact List	910	333	1173
6	WA Log	5	-	2

Oxygen Forensics successfully acquired Samsung A3 but failed in finding any WA artefacts, as shown in Table 13. Even though Oxygen Forensics was unable to get WA artefacts, artefacts other than WA were successfully obtained so that they could be used as comparative artefacts to test the reproducibility test. Magnet AXIOM managed to get images, videos, documents, and contact list artefacts. WA Key/DB Extractor had no results because it did not successfully acquire Samsung A3. Seeing the explanation above, Oxygen Forensics and Magnet AXIOM successfully met the reproducibility test. WA Key/DB Extractor failed to make an acquisition.

TABLE XIII
REPRODUCIBILITY TEST ON SAMSUNG A3

No	Artefact Type	Oxygen Forensics	Magnet AXIOM	WA Key/DB Extractor
1	Text	-	-	n/a
2	Image	-	12448	n/a
3	Video	-	116	n/a
4	Document	-	49	n/a
5	Contact List	-	350	n/a
6	WA Log	-	-	n/a

Table 14 shows the results of the reproducibility test of forensic tools on Samsung Galaxy S4 and Samsung A3. From the table, it can be seen that Oxygen Forensics and Magnet AXIOM fulfilled the reproducibility tests on Samsung Galaxy S4 and Samsung A3. WA Key/DB Extractor only managed to meet the reproducibility test on Samsung Galaxy S4. WA Key/DB Extractor did not meet the reproducibility test on Samsung A3 because it failed to acquire any artefacts that could be used for comparison.

TABLE XIV
REPRODUCIBILITY TEST RESULTS

No	Smartphone Device	Oxygen Forensics	Magnet AXIOM	WA Key/DB Extractor
1	Samsung Galaxy S4	√	√	√
2	Samsung A3	√	√	-

C. Hashing

Table 15 and Table 16 shows a comparison of the hashing values of Samsung Galaxy S4 and Samsung A3 artefacts as a result of the acquisition of Oxygen Forensics. From the table, we can see that the hashing values of Artefact s 1 and Artefact s 2 for both devices are different. Hash value testing shows that almost all forensic tools do not meet the hashing values tests, as shown in Table 17. This is understandable because the object of testing in the form of a smartphone device has a dynamic and ever-changing environment [11]. By the 3 forensic tools used, only the WA Key/DB Extractor had successfully fulfilled the hashing test for Samsung Galaxy S4 artefacts. WA Key/DB Extractor's artefacts had the same hashing values because WA Key/DB Extractor only acquired databases from WA. The artefacts of other forensic tools had different hashing values because they conducted full acquisition of smartphone devices used for testing. With full acquisitions, slight changes in mobile devices such as changes in date and time could affect the value of hashing.

TABLE XV
HASH VALUE TEST RESULTS

No	Smartphone Device	Oxygen Forensics	Magnet AXIOM	WA Key/DB Extractor
1	Samsung Galaxy S4	-	-	√
2	Samsung A3	-	-	-

TABLE XVI
SAMSUNG GALAXY S4 ARTEFACT S HASH VALUE COMPARISON

No	Forensic Tools	Artefact	Acquisition Date & Time	File Size	SHA-1 hash value
1	Oxygen Forensics	1	26 December 2017/11:59	94.752 KB	78282a2517f63ca5e461120745b482f9fa5c77a1
2		2	26 December 2017/17:49	94.752 KB	06dbb69930b1e40e1274bd154cc86cb28516ce95
3	Magnet AXIOM	1	23 December 2017/19:01	15.388.672 KB	0b82b1e5526aec5486a951325304ac2310a227fc
4		2	23 December 2017/22:07	15.388.672 KB	6762c552366b126ebae268f960ecab8a1b168806
5	WA Key/DB Extractor	1	21 December 2017/18:07	296 KB	073bf62a45c1f4c94f98b616948ac8ad1ad835c4
6		2	21 December 2017/18:09	296 KB	073bf62a45c1f4c94f98b616948ac8ad1ad835c4

TABLE XVII
SAMSUNG A3 ARTEFACT S HASH VALUE COMPARISON

No	Forensic Tools	Artefact	Acquisition Date & Time	File Size	SHA-1 Hash Value
1	Oxygen Forensics	1	2 March 2018/15:39	5.600 KB	a88f21327f8eae7606480908b9af26a57895e018
2		2	2 March 2018/15:41	5.600 KB	5be0f96057f05dd650299c9af82155ed84b33130
3	Magnet AXIOM	1	21 December 2017/10:50	1.863.266 KB	90ca69d68aa2fa4ea98741de21e75fd8f0a58c3c
4		2	21 December 2017/11:24	1.864.437 KB	ef8d468e61b6e43741807517540c659d1414bcd2
5	WA Key/DB Extractor	1	n/a	n/a	n/a
6		2	n/a	n/a	n/a

D. Analysis of Acquisition Capabilities Index of Forensic Tools

The index shows the performance of forensic tools based on the parameters used. The parameters used in this research were forensic tool parameters from NIST, and additional parameters focused on WA artefact s [18], [19], [28]. Table 18 shows the results of evaluating forensic tools for logical acquisition on Samsung Galaxy S4 using the Android 5.0 Lollipop operating system. Oxygen Forensics did not successfully meet MDT-CA-02, MDT-CA-03, MDT-CA-04, and MDT-CR-02A parameters. Oxygen Forensics successfully met all WA artefact parameters. The Magnet AXIOM just did not meet MDT-CA-04 and MDT-CR-02A parameters. The Magnet AXIOM failed to fulfil the WA log artefact parameters and text message artefact parameters. WA Key/DB Extractor only managed to get 4 parameters from NIST, which were MDT-CA-07, MDT-CA-08, MDT-CR-01A, and MDT-CR-03A. However, WA Key/DB Extractor successfully met the artefact parameters of the WA contact list, WA log artefact s, text message artefact s, and image file artefact s.

TABLE XVIII
SAMSUNG GALAXY S4 LOGICAL ACQUISITION EVALUATION RESULTS

Parameters		Forensic Tools		
		Oxygen Forensics	Magnet AXIOM (Trial ver)	WA Key/DB Extractor
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	√	√	-
Core Features Requirements	MDT-CR-01A	√	√	√
	MDT-CR-02A	-	-	-
	MDT-CR-03A	√	√	√
Logical Acquisition Artefact	WA Contact List	√	√	√
	WA Log	√	-	√
	Text	√	-	√
	Image	√	√	√
	Video	√	√	-
	Document	√	√	-

Equation (1) was used to calculate the ability index of a forensic tool to make logical acquisitions. From Table 14 it can be seen that the ability index of Oxygen Forensics to make logical acquisitions on the Samsung Galaxy S4 is (14/18) x 100 = 77.77%. Magnet AXIOM had an acquisition capability index of (14/18) x 100 = 77.77%. WA Key/DB Extractor had an acquisition ability index of (8/18) x 100 = 44.44%.

Table 19 shows the results of evaluating forensic tools for logical acquisition on Samsung A3 using the Android 6.0 Marshmallow operating system. From the table it can be seen that Oxygen Forensics did not succeed in fulfilling NIST MDT-CA-02, MDT-CA-03, MDT-CA-04, and MDT-CR-02A parameters, nor did Oxygen Forensics succeed in fulfilling additional parameters regarding the WA artefact s provided. The Magnet AXIOM failed to meet NIST MDT-CA-04 and MDT-CR-02A parameters. Magnet AXIOM successfully fulfilled the parameters of contact list artefact, image file artefact s, video file artefact s, and document file artefact s. WA Key/DB Extractor failed in fulfilling all parameters used because it could not perform logical acquisition processes on Samsung A3.

TABLE XIX
SAMSUNG A3 LOGICAL ACQUISITION EVALUATION RESULTS

Parameters		Forensic Tools		
		Oxygen Forensics	Magnet AXIOM (Trial ver)	WA Key/DB Extractor
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	√	√	-
Core Features Requirements	MDT-CR-01A	√	√	-
	MDT-CR-02A	-	-	-
	MDT-CR-03A	√	√	-
Logical Acquisition Artefact	WA Contact List	-	√	-
	WA Log	-	-	-
	Text	-	-	-
	Image	-	√	-
	Video	-	√	-
	Document	-	√	-

From Table 19 the ability index of logical acquisition of forensic tools can be calculated using Equation (1). Oxygen Forensics had an ability index of (8/18) x 100 = 44.44%. The Magnet AXIOM had an ability index of (14/18) x 100 = 77.77%. WA Key/DB Extractor failed in making logical acquisitions on Samsung A3.

IV. CONCLUSIONS

From the results can be seen that forensic tools used met validation tests for logical acquisition on Samsung Galaxy S4. WA Key/DB Extractor failed to fulfil validation tests for logical acquisition on Samsung A3; therefore, WA Key/DB Extractor not recommended to conduct forensic analysis on Samsung A3. Oxygen Forensics and Magnet AXIOM have the ability index to make logical acquisitions on Samsung Galaxy S4, which are equal to 77.77%. Magnet AXIOM had the advantage of acquiring WA artefact s that could not be done by Oxygen Forensics such as WA log artefact s and text messages. Even though WA Key/DB Extractor had the smallest ability index, WA Key/DB Extractor successfully met contact list artefact parameters, WA log artefact s, text message artefact s, and image file artefact s. The highest ability index for logical acquisitions on Samsung A3 was obtained by Magnet AXIOM with a value of 77.77% and followed by Oxygen Forensics with a value of 44.44%. WA Key/DB Extractor failed in making logical acquisitions on Samsung A3. Magnet AXIOM and Oxygen Forensics managed to meet most of the NIST parameters used. However, the Magnet AXIOM outperformed Oxygen Forensics in fulfilling the additional parameters of the WA artefact provided by the researcher.

From the research, it can be concluded that the acquisition ability index can be used to assist investigators in determining the type of forensic tool that should be used to handle a case related to WA on a device with the Android operating system. From the results obtained, the researcher argued that the acquisition ability with unweighted value index was deemed not to reflect the ability of forensic tools accurately due to several parameters that had a more significant role than other parameters in helping to find evidence on a mobile device. For that, in the future, it is necessary to analyze with different calculations to get more accurate results. Mobile forensic analysis related to Instant Messaging applications other than WA on the latest Android operating system or other operating systems also needs to be done given the diversification that exists in mobile technology.

REFERENCES

[1] statista.com, “Number of monthly active WhatsApp users worldwide from April 2013 to July 2017 (in millions),” 2017. https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/ (accessed Nov. 10, 2017).

[2] statista.com, “Numbers of WhatsApp users in the United States from 2015 to 2021 (in millions),” 2018. https://www.statista.com/statistics/558290/number-of-whatsapp-users-usa/ (accessed Jan. 25, 2018).

[3] comScore.com, “comScore Announces Launch of MMX Multi-Platform, As Well As Major Enhancements to Mobile Metrix in Indonesia with Introduction of Mobile Consumer Panel Data,” *comScore Inc.*, 2017. https://www.comscore.com/Insights/Press-Releases/2017/3/comScore-Announces-Launch-of-MMX-Multi-Platform-Indonesia (accessed Jan. 25, 2018).

[4] T. Sutikno, L. Handayani, D. Stiawan, M. A. Riyadi, and I. M. I. Subroto, “WhatsApp, viber and telegram: Which is the best for instant messaging?,” *Int. J. Electr. Comput. Eng.*, vol. 6, no. 3, pp. 909–914, 2016, doi: 10.11591/ijece.v6i3.10271.

[5] A. Griffin, “WhatsApp: After Killings in India, How The Messaging App is Being Used to Spread Deadly Fake News,” 2018. https://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-india-killings-latest-update-explained-app-fake-hoax-rumours-a8428746.html.

[6] Vix.com, “5 Crimes That People Do On WhatsApp And Can Actually Be Reported,” 2018. https://www.vix.com/en/apps-internet/530661/5-crimes-people-do-whatsapp-and-can-actually-be-reported.

[7] Techzim.co.zw, “How WhatsApp Is Aiding Criminal Activity, We Should Copy The Shady Guys,” 2018. https://www.techzim.co.zw/2018/07/how-whatsapp-has-aided-criminal-actvivity/.

[8] A. Nurlitasari, “Hacker Manfaatkan WhatsApp untuk Curi Data Pribadi Pengguna,” 2018. https://techno.okezone.com/read/2018/08/09/207/1934241/hacker-manfaatkan-whatsapp-untuk-curi-data-pribadi-pengguna.

[9] M. Chin, “Here’s how one WhatsApp photo led to 11 drug-trafficking convictions,” 2018. https://mashable.com/2018/04/16/police-use-whatsapp-to-catch-criminal/#03i.1j8.tmq2.

[10] A. Kusumadewi and J. P. Sasongko, “Polisi Usut Percakapan ‘Jessica-Mirna’ yang Beredar di Sosmed,” 2016. http://www.cnnindonesia.com/nasional/20160121080758-12-105715/polisi-usut-percakapan-jessica-mirna-yang-beredar-di-sosmed/ (accessed Nov. 10, 2017).

[11] 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, doi: 10.6028/NIST.SP.800-101r1.

[12] M. Al-Hadadi and A. AlShidhani, “Smartphone Forensics Analysis: A Case Study,” *Int. J. Comput. Electr. Eng.*, vol. 5, no. 6, pp. 576–580, 2013, doi: 10.7763/IJCEE.2013.V5.776.

[13] I. Riadi, R. Umar, and A. Firdonsyah, “Identification Of Digital Evidence On Android ’ s,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 5, pp. 3–8, 2017.

[14] S. Dogan and E. Akbal, “Analysis of Mobile Phones in Digital Forensics,” *MIPRO 2017*, pp. 1241–1244, 2017, doi: 10.23919/MIPRO.2017.7973613.

[15] E. C. Cankaya and B. Kupka, “A survey of digital forensics tools for database extraction,” *FTC 2016 - Proc. Futur. Technol. Conf.*, no. December, pp. 1014–1019, 2017, doi: 10.1109/FTC.2016.7821727.

[16] R. Umar, I. Riadi, and G. M. Zamroni, “Mobile Forensic Tools Evaluation for Digital Crime Investigation,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, p. 949, 2018, doi: 10.18517/ijaseit.8.3.3591.

[17] A. Abdallah, M. Alamin, A. Babiker, and N. Mustafa, “A Survey on Mobile Forensic for Android Smartphones,” *IOSR J. Comput. Eng.*, vol. 17, no. 1, pp. 2278–661, 2015, doi: 10.9790/0661-17211519.

[18] National Institute of Standards and Technology, “Mobile Device Tool Specification Version 2.0,” 2016, [Online]. Available: https://www.cftt.nist.gov/documents/Mobile Device Tool Secification_v2.0.pdf.

[19] National Institute of Standards and Technology, “Mobile Device Tool Test Assertions and Test Plan Version 2.0,” 2016, [Online]. Available: https://www.cftt.nist.gov/documents/Mobile_Device_Tool_Test_Assertions_and_Test_Plan_v2.0.pdf.

[20] K. D. Lutes and R. P. Mislan, “Challenges in Mobile Phone Forensics,” *Imeti 2008 Int. Multi-Conference Eng. Technol. Innov. Vol I, Proc.*, pp. 348–352, 2008.

[21] N. Santos, “Mobile Forensics : Android,” 2015.

[22] R. Ahmed, Q. M. Computech, and A. Mtech, “Mobile phones now vital source of evidence in investigations,” pp. 1–4, 2016.

[23] D. M. Sai, N. R. G. K. Prasad, and S. Dekka, “The Forensic Process Analysis of Mobile Device,” *Int. J. Comput. Sci. Inf. Technol.*, vol. 6, no. 5, pp. 4847–4850, 2015.

[24] statista.com, “Android operating system share worldwide by OS version from 2013 to 2018*,” 2018. https://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/.

[25] I. Riadi, R. Umar, and A. Sugandi, “Web forensic on kubernetes cluster services using grr rapid response framework,” *Int. J. Sci. Technol. Res.*, vol. 9, no. 1, pp. 3484–3488, 2020.

[26] R. Ahmed, D. V. Rajiv, and T. M. Vilas, “Forensic Presevation of Digital Evidence on Mobile Devices from the Perspective of Efficient Generalized Forensics Framework for Mobile Devices (EGFFMD),” *Int. J. Adv. Res. Comput. Sci.*, vol. 5, no. 4, pp. 28–29, 2014.

[27] Magnet Forensics, “12 Tips for Presenting Digital Evidence in Court From Before the Case To Delivering Testimony 12 Tips for Presenting,” 2017.

[28] R. Umar, I. Riadi, and G. Maulana, “A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 12, pp. 69–75, 2017, doi: 10.14569/IJACSA.2017.081210.

[29] C. Gaffney, “How to Calculate Index Number,” *Leaf Group Ltd*, 2018. https://bizfluent.com/how-5339534-calculate-index-numbers.html (accessed Jun. 24, 2018).

HASIL CEK_60020397_Point-C5-IRD-850GB-Mobile Forensic Tools Validation and Evaluation for Instant Messaging

ORIGINALITY REPORT

4%	3%	1%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	kursorjournal.org Internet Source	2%
2	"Information Technology - New Generations", Springer Science and Business Media LLC, 2018 Publication	1%
3	insightsociety.org Internet Source	1%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		