

HASIL CEK_03 Forensic Tools

by 03 Forensic Tools

Submission date: 18-May-2022 09:31AM (UTC+0700)

Submission ID: 1838783339

File name: 03 Forensic Tools.pdf (1.4M)

Word count: 5623

Character count: 31909

Forensic Tools Performance Analysis on Android-based Blackberry Messenger using NIST Measurements

Imam Riadi¹, Rusydi Um¹⁰, Arizona Firdonsyah³

¹Department of Information Systems, Universitas Ahmad Dahlan, Indonesia

^{2,3}Department of Informatics, Universitas Ahmad Dahlan, Indonesia

Article Info

Article history:

Received May 15, 2018

Revised Jul 25, 2018

Accepted Aug 2, 2018

Keyword:

Blackberry messenger

Digital evidence

Forensics

Smartphone

Tool

ABSTRACT

Blackberry Messenger is one of the popularly used instant messaging applications on Android with user's amount that increase significantly each year. The increase off Blackberry Messenger users might lead to application misuse, such as for committing digital crimes. To conduct investigation involving smartphone devices, the investigators need to use forensic tools. Therefore, a research on current forensic tool's performance in order to handle digital crime cases involving Android smartphones and Blackberry Messenger in particular need to be done. This research focuses on evaluating and comparing three forensic tools to obtain digital evidence from Blackberry Messenger on Android smartphones using parameter from National Institute of Standard Technology and Blackberry Messenger's acquired digital evidences. The result shows that from comparative analysis conducted, Andriller gives 25% performance value, Oxygen Forensic Suite gives 100% performance value, and Autopsy 4.1.1 gives 0% performance value. Related to National Institute of Standard Technology parameter criterias, Andriller has performance value of 47.61%. Oxygen Forensic Suite has performance value of 61.90%. Autopsy 4.1.1 has performance value of 9.52%.

6

Copyright © 2018 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Imam Riadi,

Department of Information System,

Universitas Ahmad Dahlan,

Jalan Prof. Dr. Soepomo, S.H. Janturan, Warungboto, Umbulharjo, Kota Yogyakarta, 55164, Indonesia.

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

1. INTRODUCTION

Increasingly advanced technology has led to an enormous variety of mobile-based services, particularly mobile-based services that using smartphones. 2 types of multi-user mobile-based services with lots of users are personal cloud computing and instant messaging. Cloud computing is a technology services that are offered by the cloud service provider (CSP), among other types of deals platform as a service (PaaS), infrastructure as a service (IaaS) and software as a service (SaaS). This service provides a wide range of facilities and benefits for consumers, among others, is the provision of self-service, elasticity, and pay per use [1]. Instant messaging is a technology that enables real-time text-based communication between two or more participants that utilizing the internet or intranet. A server that provides messaging services is commonly called Messenger [2].

Android based smartphone which introduced to the public in 2005 has become the most popular operating system with significantly increasing users each year. Based on survey report by Statista [3], in 2013, over 967 million units of smartphones were sold to consumers worldwide and in the final quarter of 2013, almost 78 % of smartphone sold is Android based smartphones. Based on unit shipments of these smartphones, Android's market share increased significantly in 2014 with the company holding over 80 percent of

the global smartphone operating system market in the first quarter of 2014, and as shown on Figure 1, in 2017, 1.32 billion Android smartphones were sold around the world.

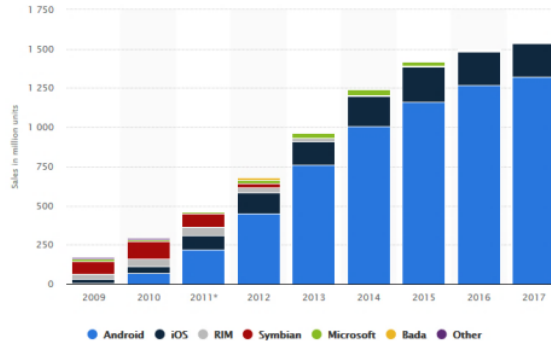


Figure 1. Statistics of android market share

Social network, or Instant Messaging applications are being more widely used among users and new types of such applications are created by developers, such as WhatsApp, Viber, Facebook, Telegram, Line, WeChat, Beetalk [4], and Blackberry Messenger. Instant messaging became one of the popular smartphone feature with more than 1.4 billion users in 2015, and the growth in popularity of messaging apps is projected to continue. E Marketer, an independent survey agency, predicts that by 2018, the number of instant messaging application users worldwide will reach 2 billion and represent 80% of smartphone users, as shown on Figure 2 [5].

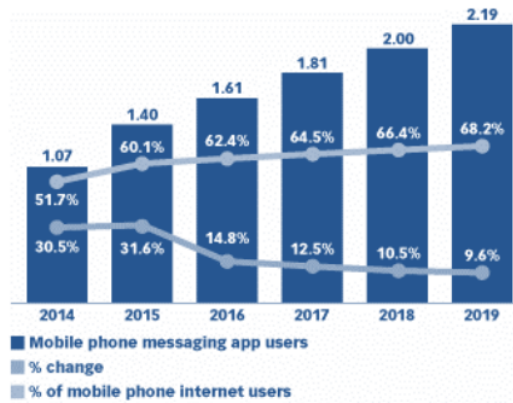


Figure 2. Statistics of instant messaging application user

One of the most popular instant messaging applications is Blackberry Messenger (BBM), although recently the use of BBM tends to decrease, but in some Asian countries, especially in Indonesia, BBM is still a leading application with lots of users, as shown in the results survey of GfK in Figure 3 [6].

In addition to the large amount of users, BBM also has numerous features, for example sending and receiving text messages, pictures, videos, and documents. BBM’s large amount of users and good features can be a magnet for someone who has criminal purpose such as drug trafficking, prostitution, cyber-bully,

and so on. There are some example of cases involving BBM applications in Indonesia as shown on Table 1 [7].

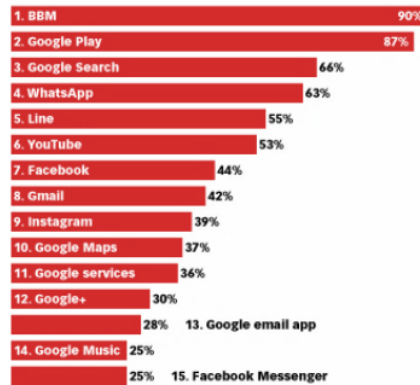


Figure 3. Statistics of BBM users in Indonesia

Table 1. Example of Digital Crime Cases using BBM

No	Year	Case
1	2014	Pornography using BBM at Banyuwangi
2	2015	Parliament member's BBM account hacked at Jakarta
3	2016	Online fraud using BBM at Palopo
4	2016	Identity theft using BBM at Palembang
5	2017	Online prostitution's transaction using BBM at Pekanbaru

To solve digital crime cases involving smartphones, the investigator needs to do mobile forensics. Mobile forensics is science that performs the process of digital evidence recovery from a mobile device using the appropriate way with forensic conditions [8]. The investigator will conduct forensic analysis on the smartphone using some forensic tools with a forensically-tested methodology, the analysis results will become a supporting evidence that have validity value before the law and can be used as tool to solve digital criminal cases [9]. Primarily there are 3 different methods on mobile forensics acquisition techniques [10]:

- Manual Acquisition.** In this technique the investigator will manually create the acquisition by directly looking at the contents of the smartphone device to find evidence. The investigator will takes pictures of each screen that containing the required data while browsing the device. The advantage of this technique is that it does not require any tools to conduct data acquisition, but this technique also have disadvantages, the data that can be acquired is only the data that visible on the device and is time consuming.
- Physical Acquisition.** In this technique the investigator will clone a smartphone device and conduct forensic analysis on the clone using a set of different forensic tools.
- Logical Acquisition.** In this technique the investigator will conduct the data acquisition found in the smartphone device to be subsequently analyzed. Here data /information available on the phone is acquired using automated tools for synchronizing smartphone and PC.

There are many challenges on mobile forensics fields, one of these challenges is the lack of resources, in the meaning that rapid development of mobile technology and the increasing amount of smartphone devices are not put in a balance by the development of forensic mobile technology and the existing forensic tools [11]. To overcome these challenges, a comparative analysis on instant messaging features and forensic tools need to be done. The comparison is not only on forensic tool's performance, but also on forensic frameworks such as National Institute of Justice (NIJ) [12], Hybrid Evidence Investigation [13], and Integrated Digital Forensic Investigation Framework (IDFIF) [14].

Sutikno, Handayani, and Stiawan et al [15] conducted a study to compare instant messaging features. The objects of the research is WhatsApp, Viber, and Telegram. The result of this research shows that WhatsApp is the most popular among the world's users of the smartphones with about 60%, followed by Viber and, in third place, Telegram. Viber is the most functional messenger, but if the main concern is the security of communication, it is wiser to opt for Telegram. Telegram offers capability of synchronization, super fast service, reliable backup and better security feature. Although WhatsApp dominates the social

media space due to its simplicity and backed by giant i.e. Facebook, Telegram is essentially providing better platform than others..

On forensic field, Umar, Riadi, and Zamroni [16] uses Belkasoft Evidence Center, WhatsApp Key/DB Extractor, and Oxygen Forensic Suite 2014 performed comparisons and analysis of proprietary and open source forensic tools, the object for analysis is WhatsApp, a multiplatform instant messaging application, and the smartphone used for analysis is Android-based smartphone. The result of this research shows that Belkasoft Evidence Center has the highest index number, WhatsApp Key/DB Extractor has superiority in terms of costs, and Oxygen Forensic Suite 2014 has superiority in obtaining WhatsApp artifact.

In other research conducted by Dogan and Akbal [17] Oxygen Forensic Suite 2014 and MOBILedit Forensics, The Researchers explain that every forensic tool has its own advantages and disadvantages. Digital crime cases related to smartphone devices should handled using several forensic tools that have different capabilities. The outcome of this research shows that MOBILedit Forensics has advantages in terms of run time, while Oxygen Forensic Suite 2014 has an advantage in terms of artifact analysis.

Other comparative analysis research is conducted by Maurya, Awasthy, Singh, and Vaish [18] The Researchers using 2 proprietary forensic tools and 3 open source forensic tools, The Researchers conclude that many of the features that are present in proprietary forensic tools are also present in open source tools. Even there are certain features that provided by open source tool but proprietary tool does not, for example: SHA-1 hashing is not provided in EnCase but available in open source tools. Open source tools also have the advantages on cost, these tools are easy to buy due to no or negligible cost.

Comparison and analysis of proprietary and open source forensic tools also conducted by Padmanabhan, Lobo, Ghelani, Sujan, and Shirole [19], the tools put into comparison are The Sleuth Kit (TSK) Autopsy, SANS SIFT, MOBILedit Forensics, and Cellebrite UFED. The conclusion of this research are: open source forensic tools have advantages in the number of users, flexibility in terms of use with console commands or GUI- based applications, logging capability, and good in tolerating errors. Meanwhile, proprietary forensic tools are superior in terms of process speed, data extraction accuracy, analytical skills, and ability to restore deleted data.

According to research conducted by Salem, Popov and Kubi [20] using Cellebrite UFED and XRY, the outcome shows that XRY is better than Cellebrite UFED for acquiring most of the artifact types, while Cellebrite UFED is better on preserving the integrity of digital evidence.

2. RESEARCH METHOD

This research's objective was to evaluate 3 forensic tools: Andriller, Oxygen Forensic Suite and Autopsy 4.1.1 based on framework and parameters from NIST and additional parameters from The Researchers in terms of the ability to acquire and analysis digital evidences from Blackberry Messenger on Android-based smartphone.

2.1. Research tools and parameters

The tools that used for this research are divided into two parts: Experimental tools and Forensic tools as shown on Table 2 and Table 3.

The National Institute of Standard and Technology (NIST) has published a test plan to measure the performance of a forensic tool in a publication entitled "Mobile Device Tool Test Assertions and Test Plan ver. 2" [21] and "Mobile Device Tool Specification ver. 2" [22]. NIST provides a total of 42 measurement parameters and methods to measure the performance of forensic tools based on the results of each test plan. However, not all parameters were used in this research. Parameters that used in this research are shown on Table 4 and Table 5.

Table 2. Experiment Tools

No	Experiment Tools	Description
1	Smartphone 1	Sony Xperia Z, Android Lollipop 5.1.1
2	Smartphone 2	Samsung Galaxy A5 2015, Android Lollipop 5.0.1
3	Blackberry Messenger	Multiplatform Instant Messaging application
4	Notebook	Asus SonicMaster X450J, OS Windows 10 64bit
5	USB Cable	A data cable that can be used to connect smartphone to notebook

Table 3. Forensic Tools

No	Forensic Tools	Description
1	Andriller	Windows-Based Proprietary Applications that can be used to acquire digital evidence on a smartphone
2	Oxygen Forensic Suite	Windows-Based Proprietary Applications that can be used to acquire digital evidence on a smartphone
3	Autopsy 4.1.1	Windows and Linux-based Open Source Applications that can be used to acquire digital evidence from multiple sources

Table 4. NIST Core and Optional Assertion Parameters for Forensic Tools

Mobile Device Tool-Core Assertion (MDT-CA)		
Core Assertion ID	Test Assertion	Comments
MDT-CA-01	1. If a mobile device forensic tool provides support for connectivity of the target device then the tool shall successfully recognize the target device via all tool-supported interfaces (e.g., cable, Bluetooth, IrDA).	Connect supported device via tool-supported interface(s); Acquire data.
MDT-CA-02	If connectivity between the mobile device and mobile device forensic tool is disrupted then the tool shall notify the user that connectivity has been disrupted.	Begin acquisition; Disconnect interface or interrupt connectivity (i.e., unplug cable) during acquisition.
MDT-CA-03	8. If a mobile device forensic tool completes acquisition of the target device without error then the tool shall have the ability to present acquired data objects in a useable format via either a preview-pane or generated report.	Acquire device data; Review data for readability in a useable format.
MDT-CA-04	If a mobile device forensic tool completes acquisition of the target device without error then subscriber and equipment related information shall be presented in a useable format.	Acquisition of MSISDN, IMSI, IMEI, MEID/ESN
MDT-CA-05	If a mobile device forensic tool completes acquisition of the target device without error then all supported data elements shall be presented in a useable format.	Acquisition of tool supported data elements
MDT-CA-06	If a mobile device forensic tool provides the user with an "Acquire All" device data objects acquisition option then the tool shall complete the acquisition of all data objects without error.	Acquire all supported device data objects
MDT-CA-07	If a mobile device forensic tool provides the user with an "Select All" individual device data objects then the tool shall complete the acquisition of all individually selected data objects without error.	Acquire all supported device data objects by individually selecting each supported data object
MDT-CA-08	If a mobile device forensic tool provides the user with the ability to "Select Individual" device data objects for acquisition then the tool shall acquire each exclusive data object without error.	Acquire each supported device data object individually
MDT-CA-09	If a mobile device forensic tool completes two consecutive logical acquisitions of the target device without error then the payload (data objects) on the mobile device shall remain consistent.	Perform two consecutive logical acquisitions; check mobile device for payload modifications
Mobile Device Tool-Assertions Optional (MDT-AO)		
Optional Assertion ID	Test Assertion	Comments
MDT-AO-10	If a mobile device forensic tool provides the examiner with the remaining number of authentication attempts then the application should provide an accurate count of the remaining PIN attempts.	Input incorrect PIN; Check tool output for correct number of remaining PIN attempts
MDT-AO-11	If a mobile device forensic tool provides the examiner with the remaining number of PUK attempts then the application should provide an accurate count of the remaining PUK attempts.	Input incorrect PUK; Check tool output for correct number of remaining PUK attempts
MDT-AO-12	If the mobile device forensic tool supports a physical acquisition of the target device then the tool shall complete the acquisition without error.	Physical Acquisition; Data is presented in a useable format.
MDT-AO-13	If the mobile device forensic tool supports proper display of non-ASCII characters then acquired data containing non-ASCII characters should be presented in their native format.	Acquisition of data containing non-ASCII characters
MDT-AO-15	If the mobile device forensic tool supports hashing for individual data objects then the tool shall present the user with a hash value for each supported data object.	Acquire data; Check known hash values for consistency
MDT-AO-16	If the mobile device forensic tool supports acquisition of GPS data then the tool shall present the user with the longitude and latitude coordinates for all GPS-related data in a useable format.	Acquire data; Check GPS data for consistency

Table 5. NIST Core and Optional Requirement Parameters for Forensic Tools

Mobile Device Tool-Core Requirement (MDT-CR)	
Core Requirement ID	Comments
MDT-CR-01	A mobile device forensic tool shall have the ability to recognize supported devices via suggested interfaces (e.g., cable, Bluetooth)
MDT-CR-02	A mobile device forensic tool shall have the ability to notify the user of connectivity errors between the device and application during data extraction

Core Requirement ID	Mobile Device Tool-Core Requirement (MDT-CR) Comments
MDT-CR-03	A mobile device forensic tool shall have the ability to perform a logical data extraction of supported data objects without modification
Requirement Optional ID	Mobile Device Tool-Requirement Optional (MDT-RO) Comments
MDT-RO-01	A mobile device forensic tool shall have the ability to perform a physical data extraction for supported devices
MDT-RO-02	A mobile device forensic tool shall have the ability to notify the user of connectivity errors between the device and application during a physical data extraction
MDT-RO-03	A mobile device forensic tool shall have the ability to perform a physical data extraction (boot loader, JTAG, ISP) of readable memory without modification

The measurement parameters are divided into 4 types, namely Core Assertions, Optional Assertions, Core Requirements, and Optional Requirements. Core Assertions leads to logical acquisition features and capabilities, Optional Assertions leads to physical acquisition features and capabilities, Core Requirements leads to logical acquisition requirements that a forensic tool shall have, and Optional Requirements leads to physical acquisition requirements that a forensic tool shall have. The Researchers does not include the parameters of MDT-CA-10 and the parameters on Universal Integrated Circuit Card (UICC) because the data on BBM application are stored in the internal memory, not UICC.

There are several additional measurement parameters added by The Researchers as shown in Table 6. The additional parameters are more focused on the abilities of forensic tools to extract digital evidences from BBM for logical acquisition and physical acquisition that essential for forensic investigator during investigation of digital crime cases related to BBM.

Table 6. Additional BBM Artifacts

No	BBM Artifacts
1	BBM Account Profile
2	Contact List (PIN Included)
3	Conversation Data
4	Images

2.2. Research methodology

This research uses the Mobile Forensic framework issued by the National Institute of Standards and Technology (NIST). NIST Mobile Forensic consists of 4 consecutive stages as illustrated in Figure 4 [23].



Figure 4. NIST mobile forensic stages

Based on Figure 4, it can be described the mobile forensic analysis stages as follows [24]:

- Collection:** This phase contained the process of identify, label, record, and retrieve data from relevant data sources by following data integrity preservation procedures. In this phase, no forensic tools used since forensic examiners will conduct the investigation based on physical data physical evidences.
- Examination:** In this phase actual data is gathered from physical evidence. In an ideal case the data is forensically copied from the phone as well as from the SIM Card. In some cases technical difficulties can prevent a digital accusation of the device. In a worst case scenario only screen captures of the phone can be gathered.
- Analysis:** Analyze the results of the examination by using technically and legally justified methods to obtain useful information and answer the questions that encourage the collection and examination. The analysis conduct is not only how to present the digital evidence as a tool on court, but also how to determine forensic tool's performance that used on physical evidence.

- d. Reporting: The last step is the most important. This phase is the presentation of the outcome of the whole process in a conclusive manner and offer the other party information about the forensic tools evaluation and methods used.



3. RESULTS AND ANALYSIS

The functionality of NIST Mobile Forensics Framework is not limited to extracting and retrieving digital evidence as a tool to resolve digital crime cases that presented in court, but this framework is also can be implemented on a comparison analysis of forensic tool performance as conducted in this research. The results of the comparison analysis of this forensic tool will be presented at the reporting stage. The stages of comparative analysis conducted using NIST Mobile Forensics Framework are described as follows:

3.1. Collection

At this stage, collection and data recording of physical evidence is conducted. This physical evidence data collection process includes the image of physical evidence, brands, specifications, operating systems, IMEI, and other data that can be extracted from physical evidences without using any forensic tools. In this research the collected physical evidence is in the form of 2 android-based smartphones. The result of this stage is as shown on Table 7.

Table 7. Physical Evidence's Specification

Physical Evidence 1	
	Brand Sony Serial Xperia Model Z Model # C6602 IMEI 355666050620xxx OS Android Version 5.1.1 (Lollipop) Processor Quad core 1.5 GHz Krait
Physical Evidence 2	
	Brand Samsung Serial Galaxy Model A Model # SM-A500F IMEI - OS Android Version 6.0.1 (Marshmallow) Processor Quad core 1.2 GHz Cortex-A53

3.2. Examination

Examination is the process of physical evidence backup and retrieval of digital data that contained in it. At this stage the cloning process of physical evidence is conducted. In this research, the cloning process conducted by using MOBILedit Forensic Express [25]. MOBILedit Forensic Express is a tool with backup and cloning features, by using this feature, forensic examiners are able to maintain the integrity of physical and digital evidences. The process and the result is as shown on Figure 5.

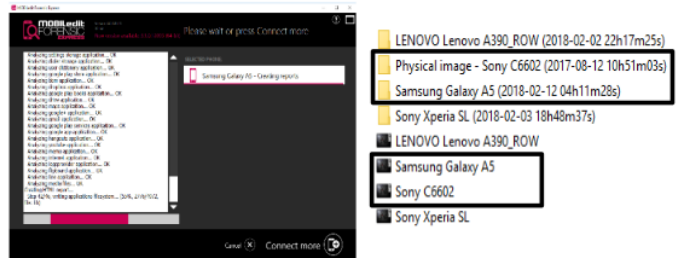


Figure 5. Cloning process and results

In this stage, the retrieval process of digital evidence will be conducted by using Andriller, Oxygen Forensic Suite, and Autopsy 4.1.1.

3.2.1. Andriller

Examination process that conducted using Andriller resulted an integrated HTML report that contained all the data extracted from physical evidence, the examination process for both physical evidences shown on Figure 6.

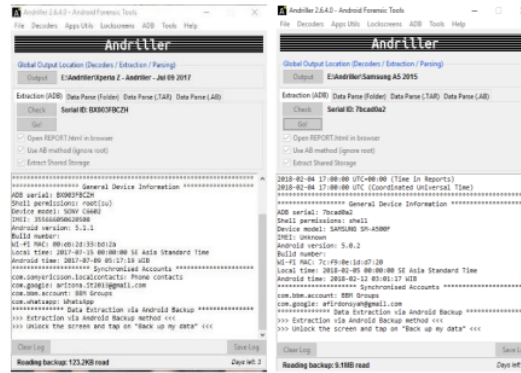


Figure 6. Examination process using Andriller

Forensic examiners then will be able to navigate through the generated HTML report to find digital evidence needed. The result from both physical evidences shown on Figure 7.

[Andriller Report] SONY C6602 IMEI:355666050620508		[Andriller Report] SAMSUNG SM-A500F IMEI:Unknown	
Type	Data	Type	Data
ADB serial:	BX303FBC2H	ADB serial:	7bcad0a2
Shell permissions:	root(su)	Shell permissions:	shell
Manufacturer:	SONY	Manufacturer:	SAMSUNG
Model:	C6602	Model:	SM-A500F
IMEI:	355666050620508	IMEI:	Unknown
Android version:	5.1.1	Android version:	5.0.2
Build name:		Build name:	
WiFi MAC:	00:eb:2d:33:bd:2a	WiFi MAC:	7c19:0e:1d:d7:20
Local time:	2017-07-15 00:00:00 SE Asia Standard Time	Local time:	2018-02-05 00:00:00 SE Asia Standard Time
Android time:	2017-07-09 05:17:19 WIB	Android time:	2018-02-12 03:01:17 WIB
Accounts:	com.sonyericson.localcontacts: Phone contacts com.google.arizona.h2013@gmail.com com.bbm.account: BBM Groups com.whatsapp: WhatsApp	Accounts:	com.bbm.account: BBM Groups com.google.afirdonsyah@gmail.com
Filesystem:	Shared Storage (2,221)	Filesystem:	Shared Storage (29)
System:	Wi-Fi Passwords (2)	System:	Wi-Fi Passwords (0)
Communications data:	SMS Messages (2)	System:	Android Download History (6)
Applications data:	BlackBerry Messenger (158)	Applications data:	BlackBerry Messenger (36)

Figure 7. Andriller's examination result

The examination result then will be analyzed and compared to other forensic tools used in this research and the comparative analysis result will be presented in Reporting phase.

3.2.2. Oxygen forensic suite

Oxygen Forensic has the ability to perform logical acquisition and physical acquisition. Examination process that conducted on both physical evidences using Oxygen Forensic Suite as the forensic tool is as shown on Figure 8.

Examination result that acquired using Oxygen Forensic Suite provide complete data of physical evidence that contained Device Information, Forensic Examiner's Identity, List of Contact, and Installed Application, BBM included. Figure 9 showed examination result from both physical evidences.

Same with Andriller, Forensic Examiners then will be able to navigate through this generated report to find digital evidence needed. This examination result also will be analyzed and compared to other forensic tools used in this research and the comparative analysis result will be presented in Reporting phase.



Figure 8. Examination process using oxygen forensic suite

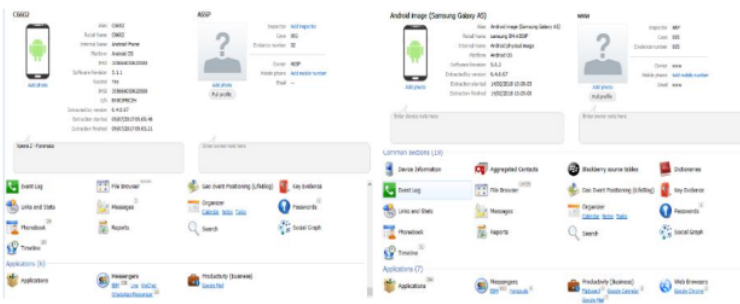


Figure 9. Oxygen forensic Suite's examination result

3.2.3. Autopsy 4.1.1

Autopsy does not have data examination feature for the Android platform, digital evidence examination process can be done through image/cloning of physical evidence (logical examination). The examination result of both physical evidence is as in Figure 10.

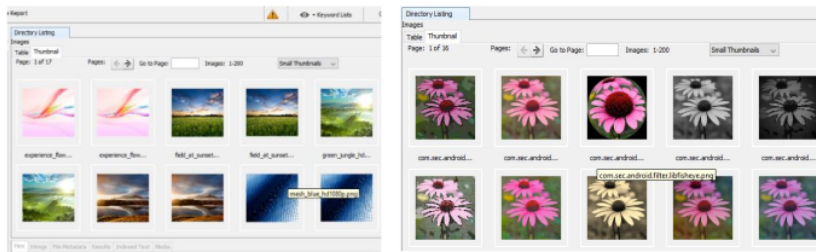


Figure 10. Autopsy 4.1.1's examination result

3.3. Analysis

Analysis is a stage to check and compare Examination result thoroughly to get the performance analysis forensic tool used. This stage limits the searching process to a certain point that connected to certain data or application. At this research, the search limit is BBM.

Forensic Tools Performance Analysis on Android-based Blackberry Messenger using ... (Imam Riadi)

Based on the examination process conducted, Andriller was able to conduct physical acquisition only. Andriller have many shortcomings in terms of Core Assertions and Optional Assertions. The examination result shows that Andriller was able to get some information regarding smartphone devices, such as IMEI (International Mobile Equipment Identity), ADB Serial, Manufacturer, and Android version. From the NIST parameters used, Andriller succeeded in meeting the criteria of MDT-CA-01, MDT-CA-02, MDT-CA-03, MDT-CA-04, MDT-CA-05, MDT-CA-06, MDT-AO-12, MDT-RO-01, MDT-RO-02, and MDT-RO-03. As for additional parameter added by The Researchers, Andriller was able to acquire digital evidence in the form of Conversation Data as shown on Figure 11.

Figure 11. Andriller’s conversation data

As for Oxygen Forensic Suite, this forensic tool was able to conduct both physical and logical acquisition. The examination result also provides information on smartphone devices, such as IMEI, Manufacturer, and Android version. From the NIST parameters used, Oxygen Forensic Suite succeeded in meeting the criteria of MDT-CA-01, MDT-CA-02, MDT-CA-03, MDT-CA-04, MDT-CA-05, MDT-CA-06, MDT-CA-09, MDT-AO-12, MDT-RO-01, MDT-RO-02, MDT-RO-03, and MDT-CR-03. As for additional parameters added by The Researchers, Oxygen Forensic Suite was able to acquire all type of additional parameters from both physical evidences as shown on Figure 12, Figure 13, Figure 14, and Figure 15, as in accordance to MDT-AO-13 NIST Parameter.



Figure 12. Oxygen forensic suite’s BBM account profile artifact

Figure 13. Oxygen forensic suite’s BBM chat artifact



Figure 14. Oxygen forensic suite's BBM contact list artifact

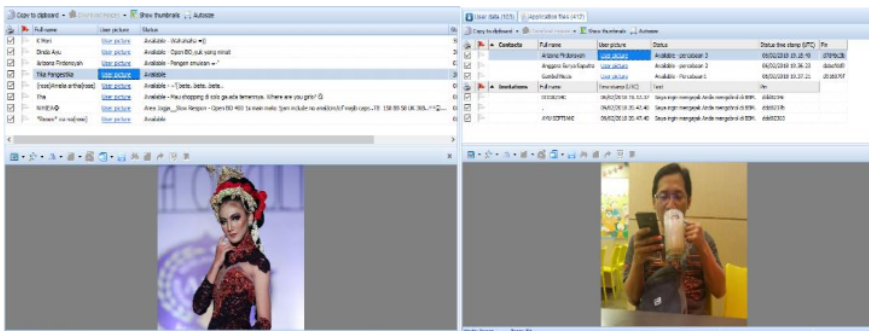


Figure 15. Oxygen forensic suite's BBM image artifact

The analysis performed on Autopsy 4.1.1's examination result shows that Autopsy was able to do logical acquisition only, as in accordance to MDT-CA-09 and MDT-CR-03 NIST parameter. Analysis conducted in term of additional parameters added by The Researchers does not give the expected result because Autopsy 4.1.1 does not have the file decryption feature to open the encryption of BBM database file, in other words, extraction using Autopsy gives zero result.

3.4. Reporting

The last stage on NIST mobile forensic framework is reporting. At this stage all the analysis's result will be presented in detail and all analysis result related to forensic tool performance comparison that obtained from BBM application is documented. The report will be presented in the form of comparative table based on NIST Parameters as shown on Table 8.

Table 8. Evaluation Results

Measurement Parameters		Forensic Tools		
		Andriller	Oxygen Forensic Suite	Autopsy 4.1.1
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-10	-	-	-
	MDT-AO-11	-	-	-
	MDT-AO-12	√	√	-
	MDT-AO-13	-	√	-
	MDT-AO-14	-	-	-
	MDT-AO-15	-	-	-

Measurement Parameters		Andriller	Oxygen Forensic Suite	Autopsy 4.1.1
Core Features	MDT-AO-16	-	-	-
	MDT-CR-01	-	-	-
	MDT-CR-02	-	-	-
Optional Features	MDT-CR-03	-	√	√
	MDT-RO-01	√	√	-
	MDT-RO-02	√	√	-
	MDT-RO-03	√	√	-

Andriller is only capable of conducting physical acquisition. However, Andriller successfully obtained BBM Conversation Data. From experimental results using Oxygen Forensic Suite, almost all core parameters and optional of NIST are met entirely. Autopsy 4.1.1 did not meet all the NIST parameters except for parameters related to logical acquisition.

On additional parameters added by The Researchers, The Researchers 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 as shown in Equation (1).

$$Par = \frac{\sum arO}{\sum art} \times 100\% \quad (1)$$

Table 9 shows the results of performance analysis conducted on each forensic tool. Andriller got 25% performance index score by only managed to acquire 1 type of BBM artifact, Oxygen Forensic Suite got 100% performance index score because it successfully acquired all 4 types of BBM artifacts, and Autopsy 4.1.1 did not get any artifact (zero result).

Table 9. Performance Index Scores

Physical Evidence 1				
No	BBM Artifact	Andriller	Oxygen Forensic Suite	Autopsy 4.1.1
1	Account Profile	-	√	-
2	Contact List	-	√	-
3	Chat	√	√	-
4	Image	-	√	-
	Performance Index Score	25 %	100 %	0 %
Physical Evidence 2				
No	BBM Artifact	Andriller	Oxygen Forensic Suite	Autopsy 4.1.1
1	Account Profile	-	√	-
2	Contact List	-	√	-
3	Chat	√	√	-
4	Image	-	√	-
	Performance Index Score	25 %	100 %	0 %

Related to the evaluation results based on NIST parameter criterias, The Researchers used the same formula to determine the performance of each forensic tool in accordance with the experiment results. Based on the calculation conducted, Andriller has performance index value of 47.61%. Oxygen Forensic Suite has performance index value of 61.90%. Autopsy 4.1.1 has performance index value of 9.52%.

4. CONCLUSION

Based on parameters added by The Researchers, Oxygen Forensic Suite has the highest index performance score at 100%, followed by Andriller with index performance score at 25%, and Autopsy 4.1.1 did not give any result (zero result) due to the absence of file and image decryption feature for mobile device. Related to NIST parameter criterias, Oxygen Forensic Suite still has the highest index performance score at 61.90% and meets almost all NIST parameter criterias. Andriller is on the 2nd with index performance score at 47.61% and meets 10 NIST parameter criterias. Autopsy 4.1.1 has the lowest index performance value at 9.52% due to the absence of document decryption feature and only meets 2 NIST parameter criterias. Andriller indeed met many NIST parameter criterias, however, Andriller manages to get only conversation data artifact using physical acquisition. Oxygen Forensic Suite has the highest performance score among the three forensic tools used, but Oxygen Forensic Suite has weakness in terms of options to select data for

acquisition due to limited options on data extraction menu. Oxygen Forensic Suite successfully extracts all BBM artifact via logical acquisition and physical acquisition. For future work, there are more performance evaluations on forensic tools that can be conducted to get an overview on what forensic tool that best for digital forensic investigations.

REFERENCES

- [1] N. Widiyasono, *et al.*, "Investigation on the Services of Private Cloud Computing by Using ADAM Method", *Int. J. Electr. Comput. Eng.*, vol. 6, no. 5, pp. 2387-2395, 2016.
- [2] Husni, "The Design of Instant Messaging System", vol. 4, no. 3, pp. 177-186, 2015.
- [3] Statista, "Global Smartphone sales by Operating System from 2009 to 2017 (in millions)", 2018, <https://www.statista.com/statistics/263445/global-smartphone-sales-by-operating-system-since-2009/>.
- [4] M. Dadkhah, *et al.*, "Social network applications and free online mobile numbers: Real risk", *Int. J. Electr. Comput. Eng.*, vol. 5, no. 2, pp. 175-176, 2015.
- [5] eMarketer, "Mobile Messaging to Reach 1.4 Billion Worldwide in 2015 Penetration is highest in Latin America", 2015, <https://www.emarketer.com/Article/Mobile-Messaging-Reach-14-Billion-Worldwide-2015/1013215>.
- [6] eMarketer, "Infatuation with Messaging Apps Continues in Indonesia," 2016, <https://www.emarketer.com/Article/Infatuation-with-Messaging-Apps-Continues-Indonesia/1013808>.
- [7] I. Riadi, *et al.*, "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.
- [8] I. Z. Yadi and Y. N. Kunang, "Konferensi Nasional Ilmu Komputer (KONIK) 2014 Forensic Analysis on Android Platform", in *Konferensi Nasional Ilmu Komputer (KONIK)*, 2014.
- [9] R. Ayers, *et al.*, "Guidelines on Mobile Device Forensics", *NIST Spec. Publ.*, vol. 1, pp. 800-101, 2014.
- [10] N. R. Roy, *et al.*, "Android Phone Forensic: Tools and Techniques", *Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCA 2016*, pp. 605-610, 2017.
- [11] D. M. Sai, *et al.*, "The Forensic Process Analysis of Mobile Device", *Int. J. Comput. Sci. Inf. Technol.*, vol. 6, no. 5, pp. 4847-4850, 2015.
- [12] J. Ashcroft, "A Guide for First Responders", United States Dep. Justice Off. Justice, p. 93, 2001.
- [13] S. Permatasari, *et al.*, "Mobile Forensic Analysis using Hybrid Evidence Investigation Method on Smartphone", Univ. Siliwangi Tasikmalaya, 2015.
- [14] R. Ruuhwan, *et al.*, "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.
- [15] T. Sutikno, *et al.*, "WhatsApp, viber and telegram: Which is the best for instant messaging?", *Int. J. Electr. Comput. Eng.*, vol. 6, no. 3, pp. 909-914, 2016.
- [16] R. Umar, *et al.*, "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.
- [17] S. Dogan and E. Akbal, "Analysis of Mobile Phones in Digital Forensics", *2017 40th Int. Conv. Inf. Commun. Technol. Electron. Microelectron.*, pp. 1241-1244, 2017.
- [18] N. Maurya and J. Awasthi, "Analysis of Open Source and Proprietary Source Digital Forensic Tools", *Int. J. Adv. Eng. Glob. Technol.*, vol. 3, no. 7, pp. 916-922, 2015.
- [19] R. Padmanabhan, *et al.*, "Comparative Analysis of Commercial and Open Source Mobile Device Forensic Tools", *2016 9th Int. Conf. Contemp. Comput. IC3 2016*, 2017.
- [20] S. Saleem, *et al.*, "Evaluating and Comparing Tools for Mobile Device Forensics Using Quantitative Analysis", *Stock. Univ.*, pp. 264-282, 2013.
- [21] National Institute of Standards and Technology, "Mobile Device Tool Test Assertions and Test Plan Version 2.0", 2016.
- [22] National Institute of Standards and Technology, "Mobile Device Tool Specification Version 2.0", 2016.
- [23] B. Garnett, "Triage Forensics: Leveraging Digital Forensics during Incident Response", 2017, <https://blogs.cisco.com/security/triage-forensics-leveraging-digital-forensics-during-incident-response>.
- [24] I. Riadi, *et al.*, "Identification of Digital Evidence on Android's Blackberry Messenger using NIST Mobile Forensic Method", *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 5, pp. 156-160, 2017.
- [25] S. G. Punja and R. P. Mislán, "Mobile Device Analysis", *Small Scale Digit. Device Forensics J.*, vol. 2, no. 1, pp. 1941-6164, 2008.

HASIL CEK_03 Forensic Tools

ORIGINALITY REPORT

10%

SIMILARITY INDEX

7%

INTERNET SOURCES

6%

PUBLICATIONS

8%

STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Maryland, University College Student Paper	2%
2	jurnal.iaii.or.id Internet Source	2%
3	Submitted to Champlain College Student Paper	1%
4	Submitted to Ahlia University Student Paper	1%
5	Nur Widiyasono, Imam Riadi, Ahmad Luthfie. "Investigation on the Services of Private Cloud Computing by Using ADAM Method", International Journal of Electrical and Computer Engineering (IJECE), 2016 Publication	1%
6	faiz.dosen.itelkom-pwt.ac.id Internet Source	<1%
7	www.ijcaonline.org Internet Source	<1%

8	www.slideshare.net Internet Source	<1 %
9	ijece.iaescore.com Internet Source	<1 %
10	Fatwa Tentama, Subardjo Subardjo, Muhamad Hasan Abdillah. "Motivation to learn and social support determine employability among vocational high school students", International Journal of Evaluation and Research in Education (IJERE), 2019 Publication	<1 %
11	Submitted to University of Arizona Student Paper	<1 %
12	"Information Technology - New Generations", Springer Science and Business Media LLC, 2018 Publication	<1 %
13	iaescore.com Internet Source	<1 %
14	Submitted to Colorado State University, Global Campus Student Paper	<1 %
15	ojs.unud.ac.id Internet Source	<1 %
16	www.ukessays.com Internet Source	<1 %

Exclude quotes On

Exclude matches Off

Exclude bibliography On