Forensic Investigation Technique on Android's Blackberry Messenger using NIST Framework

By SUNARDI

International Journal of Cyber-Security and Digital Forensics (IJCSDF) 6(4): 198-205
The Society of Digital Information and Wireless Communications (SDIWC), 2017 ISSN: 2305-0012

Forensic Investigation Technique on Android's Blackberry Messenger using NIST Framework

Imam Riadi[1], Sunardi[2], and Arizona Firdonsyah[3]
[1] Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[2,3] Master of Informatics Engineering, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
(imam.riadi@mti.uad.ac.id, sunardi@mti.uad.ac.id, arizona.f@gmail.com)

ABSTRACT

In the past few years, there has been a rapid increase in the number of smartphone users. this can be seen with various brands and platforms of smartphones that sold almost every week. One of smartphone platform with a huge amount of users is Android. The rapid development of Android smartphone technology has an impact on the growing number of applications developed for Android platform, including instant messaging applications. Blackberry Messenger (BBM) is one of the multi-platform instant messaging applications with the amount of users that increase significantly each year, causing the possibility of digital crimes that occured by digital crime perpetrator is also significantly increased. In the process of investigating digital crime cases, digital evidences are required to solve these cases. To obtain digital evidences, a technique of forensic investigation on physical evidence has been conducted. This paper studies three widely used mobile forensics tools namely, Oxygen Forensic Suite, Andriller, and Belkasoft Evidence Center in extracting data from BBM application that installed on an Android based smartphone using a framework developed by NIST. The results of this research were presented in the form of recorded conversations, BBM Personal Identification Number (BBM PIN), pictures, and conversation timestamp.

KEYWORDS

Android, Digital Evidence, Blackberry Messenger, Digital Forensics, NIST

1 INTRODUCTION

According to Statista [1], in 2016, the number of smartphone users is estimated to reach 2.1 billion. By 2018, more than 36 percent of the world's population is expected to use smartphones, about 10 percent higher than 2011. As shown on Figure 1, the number of mobile phonec users in the world is predicted to pass the five billion mark by 2019.

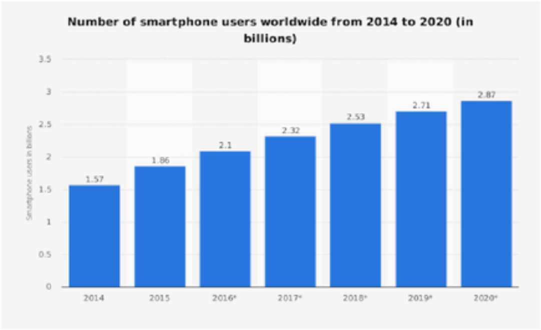


Figure 1. Graphical statistics of smartphone users.

Among those smartphone users, Android and iOS are the two most popular smartphone operating systems in the industry. This rapid development of Android smartphone sales has an impact on the growing number of applications developed for the Android OS, including instant messaging applications. Developers are competing to create instant messaging applications with user friendly features, one of these application is Blackberry Messenger (BBM). A survey conducted by Global Web Index [2], stated that in direct comparison with its competitors, BBM ranked 2nd on worldwide users with 81% registered users, Figure 2 shows the graph.

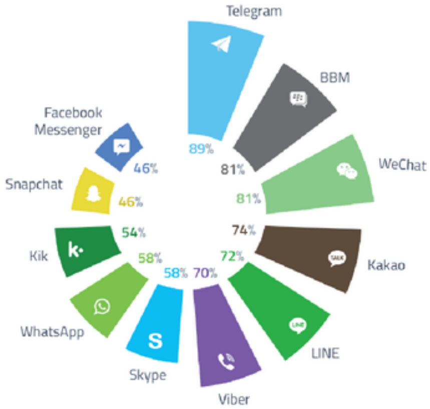


Figure 2. Graphical statistics of BBM users worldwide.

As for Indonesia, a survey conducted by Singaporean online survey organizations We Are Social [3] at 2016, Blackberry Messenger users ranked first with 19% of users, followed by WhatsApp users with with 14% , the graph shown on Figure 3.

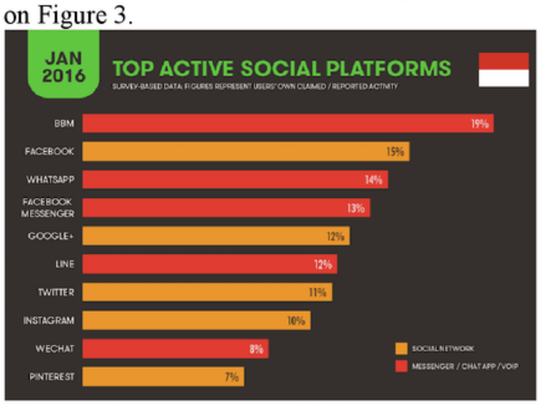


Figure 3. Graphical statistics of BBM users in Indonesia

The increasing of BBM users, in addition to lots of positive impacts that caused, also caused many negative impacts. Many people took advantage of BBM's user friendly features to perform digital crimes such as prostitution, pornography, identity theft, cyberbully, etc. Table 1 shows some examples of digital crimes occured by using BBM at Indonesia [4,5,6,7,8].

Table 1. Digital crime that using BBM (observation)

No	Year	Case
1	2014	Pornography via BBM at Banyuwangi
2	2015	BBM Account hacking at Jakarta
3	2016	Online fraud via BBM at Palopo
4	2016	Identity theft via BBM at Palembang
5	2017	Online prostitution via BBM at Pekanbaru

In the process for solving digital crime cases, necessary supporting evidence is needed. If an android based smartphone became the physical evidence on a case that Blackberry Messenger application was installed, then the application can be analyzed to obtain digital evidence that can be expected to assist law enforcement in solving the cases of digital crimes. The main topic of this paper are to emphasize on the forensic investigation process and to compare mobile forensics tools used in this research by using a framework developed by National Institute of Standard and Technology (NIST) [9].

2 LITERATURE REVIEW

2.1 Mobile Forensics

Mobile Forensics is a science that performs the process of digital evidence recovery from a mobile device using the appropriate way with forensic conditions [10]. The initial research work in this field has focused on acquisition techniques and general forensic analysis of smart devices [11]. This was shown in Burnette's work in 2002 where he discussed the forensic examination of older versions of the BlackBerry and the hardware and software used for acquisition [12].

2.2 Cyber Crime

The website of Interpol in cyber crime section stated "Cyber crime is one of the fastest growing areas of crime". These crime cases include attacks against computer data and systems, identity theft, sexual abuse images, internet auction fraud, the deployment of viruses, and various scams such as phishing [13].

According to the UN (United Nations), cybercrime is: "any illegal behaviour committed by means on relation to, a computer system offering or system or network, including such crime as illegal possession in, offering or distributing information by means of computer system or network". Another definition of Cybercrime is a crime using information technology as instrument or target, and digital forensics, in essence, answer the questions: when, what, who, where, how and why related to digital crime [14]. There are many kinds of cybercrimes: one of the example is cyberbullying, a term that refers to the use of information technology to bully people to send or post text that is intimidating or threatening others [15].

2.3 Digital Evidence

Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a mobile phone, a personal digital assistant (PDA), a CD, and a flash card in a digital camera, among other places. Digital evidence is commonly associated with digital or electronic crime, such as pornography, prostitution, identity theft, phishing, or credit card fraud. However, digital evidence is now used to prosecute all types of crimes, not just digital crimes [16].

2.4 Android

Android is architected in the form of a software stack comprising applications, an operating system, run-time environment, middleware, services and libraries. Each layer of the stack, and the corresponding elements within each layer, are tightly integrated and carefully tuned to provide the optimal application development and execution environment for mobile devices as shown on Figure 4 [17].

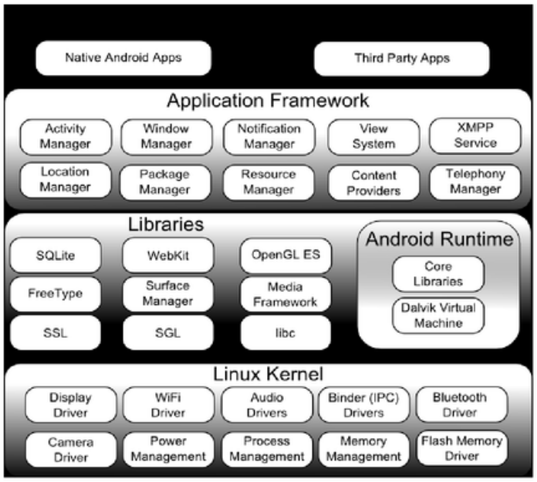


Figure 4. Android Architecture

2.5 Blackberry Messenger

BlackBerry Messenger (BBM) is an application of instant messaging that is developed by Research In Motion (RIM), and originally created for BlackBerry smartphone [18]. As technology advances, BBM is moving beyond Blackberry devices, BBM now become a multi-platfom application that can be installed on Android, iOS, and Windows based smartphone. Since it was created in August 2005, BBM has evolved from a pure messaging application for communication (text and video) to a social eco-system unifying chat, social, commerce and services including games [19].

2.6 Oxygen Forensic Suite

Oxygen Forensic Suite is a forensic software for extraction and analysis of data from cell phones, smartphones and tablets [20]. This tool offers several hash algorithms and one of which can be selected in each investigation case. Oxygen Forensic Suite also has the capability to provide general information about the smartphone and the network that the device was connected to. The other useful capability from this tool is recovered all contacts, SMS, MMS, and user's files [21].

2.7 Andriller

Andriller is a utility which consists of various tools for serving various purposes which includes cracking of screen lock pattern, PIN and passwords, decoding of encrypted databases and files, data extraction automatically and unpacking of android backups. This tool kit solves many of mobile forensics needs for the Android OS [22].

2.8 Belkasoft Evidence Center

Belkasoft Evidence Center is a tool for investigators that can be used to acquire, search, analyze, store and share digital evidence found inside computer and mobile devices. This toolkit will extract digital evidences from multiple sources such as hard drives, drive images, memory dumps, iOS, Blackberry and Android backups. Belkasoft Evidence Center will automatically analyze the data source and lay out the most forensically important artifacts for investigator to review, examine, and report [23].

3 METHODOLOGY

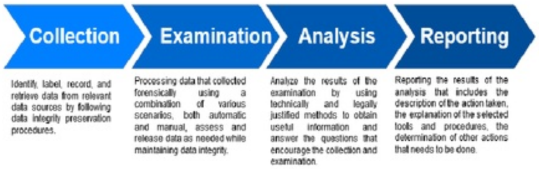
The National Institute of Standard and Technology (NIST) has published a framework for mobile device investigation guide called NIST Mobile Forensics, that contained 4 consecutive steps [24]:

1. Collection: or sometimes called Preservation, this process consist of the steps in gathering and documenting the evidence from the perpetrator, the owner, or at the crime scene. Care has to be taken to preserve other forms of evidence.
2. Examination: or sometimes called Acquisition, in this phase actual data is gathered from the device. In an ideal case the data is forensically copied from the phone as well as from the SIM Card. In some cases technical diffculties can prevent a digital accusation of the device. In a worst case scenario only screen captures of the phone can be gathered.
3. Analysis: Now the gathered data is analyzed for clues regarding the possible crime. The analysis can either be done by hand or with

the help of software tools. There are many software tools available for that purpose. It is important to use different software tools to gather more detailed analysis. Care has to be taken not to miss a crucial piece of evidence solely because one particular tool didn't have the right feature.

4. Reporting: The last step is the most important. Between the gathering of evidence and the presentation in court a signifcant amount of time can pass. An examiner must be able to present his evidence in a conclusive manner and offer the other party information about the tools and methods used.

Figure 5 shows the graphical picture of these 4 consecutive stages.



Identify, label, record, and retrieve data from relevant data sources by following data integrity preservation procedures.

Processing data that collected forensically using a combination of various scenarios, both automatic and manual, assess and release data as needed while maintaining data integrity.

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.

Reporting the results of the analysis that includes the description of the action taken, the explanation of the selected tools and procedures, the determination of other actions that needs to be done.

Figure 5. NIST Mobile Forensics Stages

4 RESULTS AND DISCUSSION

4.1 Collection

Collection or Preservation is the earliest stage in mobile forensic methods, and the first thing to do is to search, collect and document the evidence. In this research the evidence is in the form of an android-based smartphone. The result of this stage is as follows:

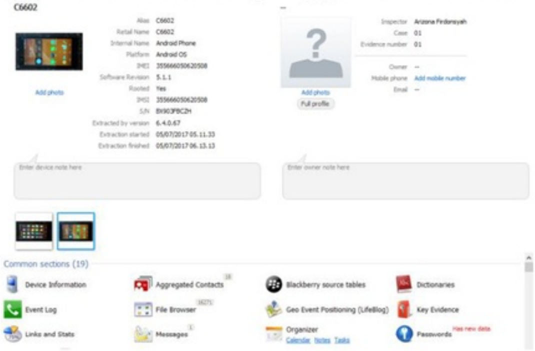
Table 2. Evidence's Specification

No	Specification Type	Physical Evidence's Specification
1	Brand	Sony
2	Brand Series	Xperia Z
3	Model Number	C6602
4	OS	Android
5	Processor	Quad core 1.5 GHz

Figure 6. Android Smartphone as Physical Evidence

4.2 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. The cloning process can be done using various tools, such as MOBILedit Forensic Express [25]. Figure 7 shows the examination result using Oxygen Forensic Suite.



C6602

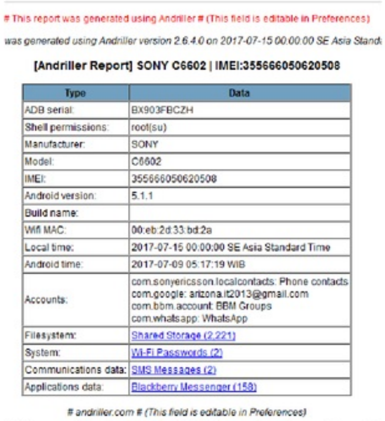
Alias C6602
Retail Name C6602
Internal Name Android Phone
Platform Android OS
IMEI 355666050620508
Software Revision 5.1.1
Rooted Yes
IMSI 355666050620508
S/N BX903FBC2H
Extracted by version 6.4.0.67
Extraction started 05/07/2017 05.11.33
Extraction finished 05/07/2017 06.13.13

Inspector Arizona Firdonsyah
Case 01
Evidence number 01
Owner --
Mobile phone Add mobile number
Email --

Figure 7. Oxygen Forensic Suite's Examination Result

Oxygen Forensic Suite's examination result provide complete data of physical evidence that contained Device Information, Forensic Examiner's Identity, List of Contact, and Installed Application, BBM included.

For examination process that conducted using Andriller, the result provided is an integrated HTML report that contained all the data extracted from physical evidence. Forensic examiner is able to navigate through the HTML formatted report to find digital evidences. The report shown on figure 8.



This report was generated using Andriller # (This field is editable in Preferences)

was generated using Andriller version 2.6.4.0 on 2017-07-15 00:00:00 SE Asia Stand

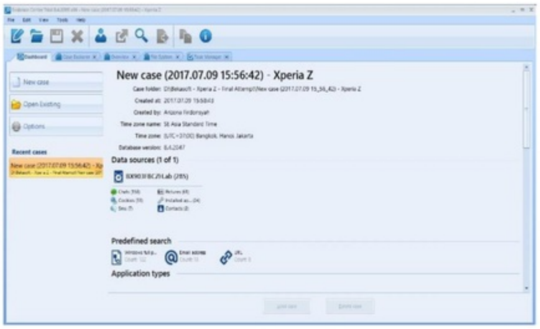
[Andriller Report] SONY C6602 | IMEI:355666050620508

Type	Data
ADB serial:	BX903FBCZH
Shell permissions:	root(su)
Manufacturer:	SONY
Model:	C6602
IMEI:	355666050620508
Android version:	5.1.1
Build name:	
Wifi MAC:	00:eb:2d:33:bd:2a
Local time:	2017-07-15 00:00:00 SE Asia Standard Time
Android time:	2017-07-09 05:17:19 WIB
Accounts:	com.sonyericsson.localcontacts: Phone contacts com.google: arizona.it2013@gmail.com com.bbm.account: BBM Groups com.whatsapp: WhatsApp
Filesystem:	Shared Storage (2,221)
System:	Wi-Fi Passwords (2)
Communications data:	SMS Messages (2)
Applications data:	Blackberry Messenger (158)

# andriller.com # (This field is editable in Preferences)

Figure 8. Andriller's Examination Result

For Belkasoft Evidence Center, the results given from the Examination stage are relatively similar to Oxygen Forensic Suite, ie in the form of complete data on physical evidence and applications installed on the physical evidence, including BBM. Figure 9 shows the result of Examination from Belkasoft Evidence Center.



New case (2017.07.09 15:56:42) - Xperia Z

Case folder: D:\Belkasoft - Xperia Z - Final Attempt\New case (2017.07.09 15_56_42) - Xperia Z
Created at: 2017.07.09 15:58:43
Created by: Arizona Firdonsyah
Time zone name: SE Asia Standard Time
Time zone: (UTC+07:00) Bangkok, Hanoi, Jakarta
Database version: 8.4.2047

Data sources (1 of 1)

Figure 9. Belkasoft Evidence Center's Examination Result

From the results of this Examination stage, an analysis will be conducted to find digital evidence related to a digital crime case. In this research will be sought digital evidence generated from BBM application.

4.3 Analysis

Analysis is a stage to look Examination result thoroughly to acquire digital evidences. 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.

Analysis stage conducted by Oxygen Forensic Suite resulted in the form of BBM contact pictures that shows some young girls in an inappropriate pose like shown at Figure 10 (due to inappropriate content, part of the picture's been covered).

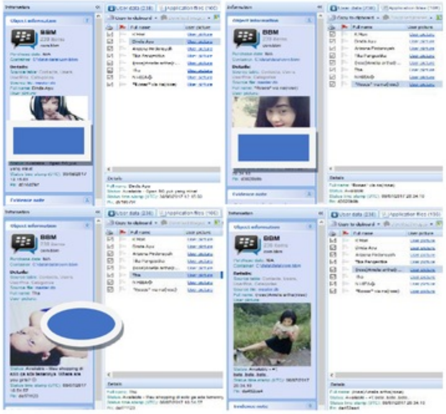
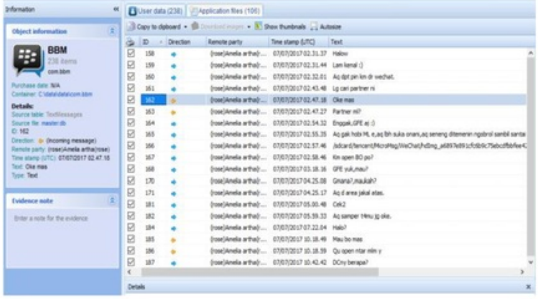


Figure 10. Oxygen Forensic Suite's Contact Analysis

The analysis process also resulted a data conversation with one of the BBM contact that used an unusual and inappropriate language just like shown on Figure 11.



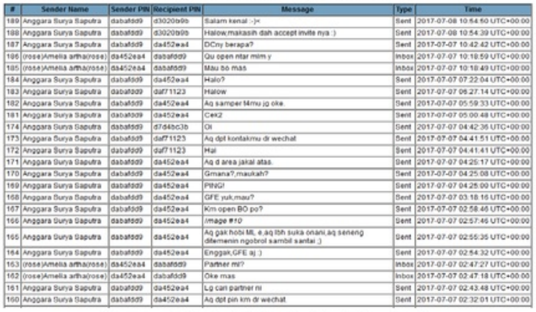
ID	Direction	Remote party	Time stamp (UTC)	Text
158		(rose)Amelia artha(r...	07/07/2017 02.31.37	Halow
159		(rose)Amelia artha(r...	07/07/2017 02.31.44	Lam kenal :)
160		(rose)Amelia artha(r...	07/07/2017 02.32.01	Aq dpt pin km dr wechat.
161		(rose)Amelia artha(r...	07/07/2017 02.43.48	Lg cari partner ni
162		(rose)Amelia artha(r...	07/07/2017 02.47.18	Oke mas
163		(rose)Amelia artha(r...	07/07/2017 02.47.27	Partner ml?
164		(rose)Amelia artha(r...	07/07/2017 02.54.32	Enggak,GFE aj :)
165		(rose)Amelia artha(r...	07/07/2017 02.55.35	Aq gak hobi ML e,aq lbh suka onani,aq seneng ditemenin ngobrol sambil santa
166		(rose)Amelia artha(r...	07/07/2017 02.57.46	/sdcard/tencent/MicroMsg/WeChat/hdImg_a6897e891cfc6b9c75ebcdfbbfee4C
167		(rose)Amelia artha(r...	07/07/2017 02.58.46	Km open BO po?
168		(rose)Amelia artha(r...	07/07/2017 03.18.16	GFE yuk,mau?
170		(rose)Amelia artha(r...	07/07/2017 04.25.08	Gmana?,maukah?
171		(rose)Amelia artha(r...	07/07/2017 04.25.17	Aq d area jakal atas.
181		(rose)Amelia artha(r...	07/07/2017 05.00.48	Cek2
182		(rose)Amelia artha(r...	07/07/2017 05.59.33	Aq samper t4mu jg oke.
184		(rose)Amelia artha(r...	07/07/2017 07.22.04	Halo?
185		(rose)Amelia artha(r...	07/07/2017 10.18.49	Mau bo mas
186		(rose)Amelia artha(r...	07/07/2017 10.18.59	Qu open ntar mlm y
187		(rose)Amelia artha(r...	07/07/2017 10.42.42	DCny berapa?

Object information
BBM
238 items
com.bbm
Purchase date: N/A
Container: C:\data\data\com.bbm
Details:
Source table: TextMessages
Source file: master.db
ID: 162
Direction: (Incoming message)
Remote party: (rose)Amelia artha(rose)
Time stamp (UTC): 07/07/2017 02.47.18
Text: Oke mas
Type: Text

Evidence note
Enter a note for the evidence

Figure 11. Oxygen Forensic Suite's Chat Analysis

Based on the result above, there is an indication of an online prostitution transaction that happened. To gain more detailed data, analysis of the next tool is conducted. Andriller's examination result did not produce any pictures or photos due to the software limitation but the conversation's data is fully acquired. The analysis shows a conversation that exactly the same like shown on Oxygen Forensic Suite. Figure 12 shows the conversation analysis result.



#	Sender Name	Sender PIN	Recipient PIN	Message	Type	Time
189	Anggara Surya Saputra	dabafdd9	d3020b9b	Salam kenal :-)<	Sent	2017-07-08 10:54:50 UTC+00:00
188	Anggara Surya Saputra	dabafdd9	d3020b9b	Halow,makasih dah accept invite nya :)	Sent	2017-07-08 10:54:39 UTC+00:00
187	Anggara Surya Saputra	dabafdd9	da452ea4	DCny berapa?	Sent	2017-07-07 10:42:42 UTC+00:00
186	(rose)Amelia artha(rose)	da452ea4	dabafdd9	Qu open ntar mlm y	Inbox	2017-07-07 10:18:59 UTC+00:00
185	(rose)Amelia artha(rose)	da452ea4	dabafdd9	Mau bo mas	Inbox	2017-07-07 10:18:49 UTC+00:00
184	Anggara Surya Saputra	dabafdd9	da452ea4	Halo?	Sent	2017-07-07 07:22:04 UTC+00:00
183	Anggara Surya Saputra	dabafdd9	daf71123	Halow	Sent	2017-07-07 06:27:14 UTC+00:00
182	Anggara Surya Saputra	dabafdd9	da452ea4	Aq samper t4mu jg oke.	Sent	2017-07-07 05:59:33 UTC+00:00
181	Anggara Surya Saputra	dabafdd9	da452ea4	Cek2	Sent	2017-07-07 05:00:48 UTC+00:00
174	Anggara Surya Saputra	dabafdd9	d7d4bc3b	Oi	Sent	2017-07-07 04:42:36 UTC+00:00
173	Anggara Surya Saputra	dabafdd9	daf71123	Aq dpt kontakmu dr wechat	Sent	2017-07-07 04:41:51 UTC+00:00
172	Anggara Surya Saputra	dabafdd9	daf71123	Hai	Sent	2017-07-07 04:41:41 UTC+00:00
171	Anggara Surya Saputra	dabafdd9	da452ea4	Aq d area jakal atas.	Sent	2017-07-07 04:25:17 UTC+00:00
170	Anggara Surya Saputra	dabafdd9	da452ea4	Gmana?,maukah?	Sent	2017-07-07 04:25:08 UTC+00:00
169	Anggara Surya Saputra	dabafdd9	da452ea4	PING!	Sent	2017-07-07 04:25:00 UTC+00:00
168	Anggara Surya Saputra	dabafdd9	da452ea4	GFE yuk,mau?	Sent	2017-07-07 03:18:16 UTC+00:00
167	Anggara Surya Saputra	dabafdd9	da452ea4	Km open BO po?	Sent	2017-07-07 02:58:46 UTC+00:00
166	Anggara Surya Saputra	dabafdd9	da452ea4	/image #10	Sent	2017-07-07 02:57:46 UTC+00:00
165	Anggara Surya Saputra	dabafdd9	da452ea4	Aq gak hobi ML e,aq lbh suka onani,aq seneng ditemenin ngobrol sambil santai ;)	Sent	2017-07-07 02:55:35 UTC+00:00
164	Anggara Surya Saputra	dabafdd9	da452ea4	Enggak,GFE aj :)	Sent	2017-07-07 02:54:32 UTC+00:00
163	(rose)Amelia artha(rose)	da452ea4	dabafdd9	Partner ml?	Inbox	2017-07-07 02:47:27 UTC+00:00
162	(rose)Amelia artha(rose)	da452ea4	dabafdd9	Oke mas	Inbox	2017-07-07 02:47:18 UTC+00:00
161	Anggara Surya Saputra	dabafdd9	da452ea4	Lg cari partner ni	Sent	2017-07-07 02:43:48 UTC+00:00
160	Anggara Surya Saputra	dabafdd9	da452ea4	Aq dpt pin km dr wechat	Sent	2017-07-07 02:32:01 UTC+00:00

Figure 12. Andriller's Chat Analysis

As for Belkasoft Evidence Center, due to software's trial limitation, this tool is only able to produce a random part of the BBM data as shown on Figure 13.

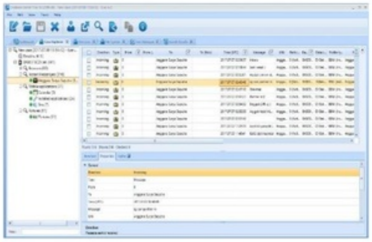
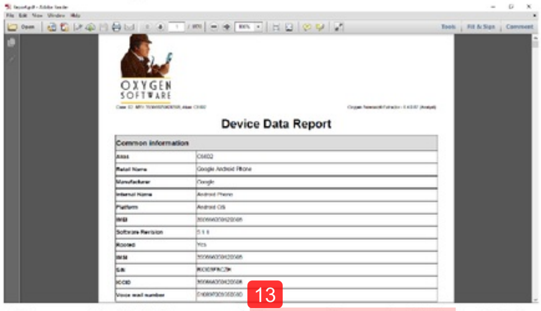


Figure 13. Belkasoft's Analysis Result

4.4 Reporting

The last stage on the mobile forensic investigation method is reporting. At this stage all the analysis's result will be discussed and presented in detail and all artifacts related to the previously obtained from BBM application that showing some indications of a digital crime is documented. The report can be presented based on each tool used on the investigation or by overall report contained all result from all investigation tools.

Oxygen Forensic Suite has the ability to create full reports in various formats, including PDF, the document format that most frequently used. Full Reports from Oxygen Forensic in PDF format is shown in Figure 14



Device Data Report

Common information	
Alias	C6602
Retail Name	Google Android Phone
Manufacturer	Google
Internal Name	Android Phone
Platform	Android OS
IMEI	[illegible]
Software Revision	5.1.1
Rooted	Yes
IMSI	[illegible]
S/N	[illegible]
ICCID	[illegible]
Voice mail number	[illegible]

Figure 14. Full Report of Oxygen Forensic Suite in PDF

Oxygen Forensic Suite is also able to create partial reports that refer to one application only, in this research, partial reports are made from the BBM application as shown in Figure 15.

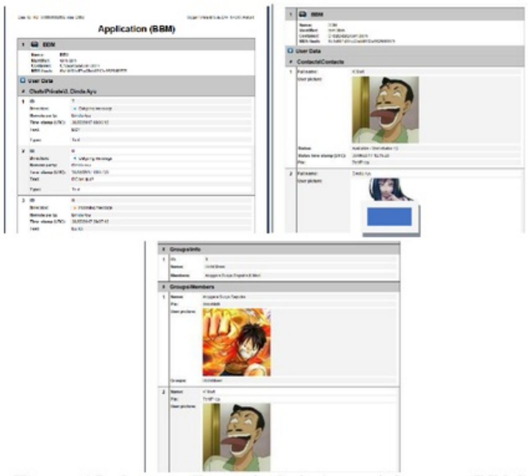
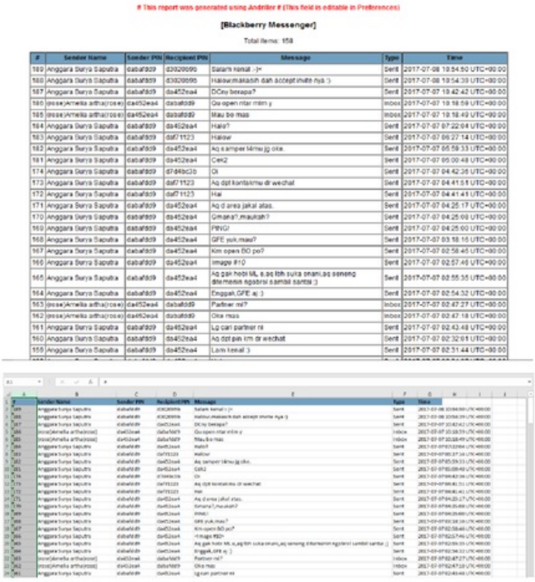


Figure 15. Oxygen Forensic Suite's partial report (BBM)

Andriller's report generation capability is not as good as Oxygen Forensic Suite or Belkasoft Evidence Center. Compared to both forensic tools, Andriller is a lightweight forensic application with simple features. Reports generated from BBM application are just tables containing conversation recordings. Supported formats are also only in HTML and MS-Excel form. Figure 16 shows the report from Andriller.



This report was generated using Andriller # (This field is editable in Preferences)

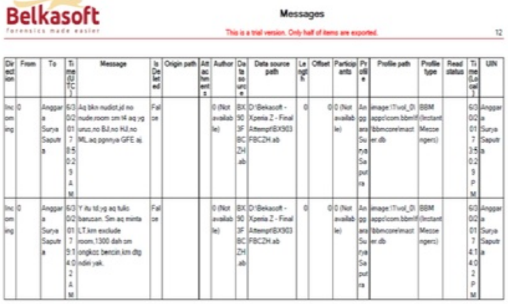
[Blackberry Messenger]

Total items: 158

#	Sender Name	Sender PIN	Recipient PIN	Message	Type	Time
189	Anggara Surya Saputra	dabafdd9	d3020695	Salam kenal :-)<	Sent	2017-07-08 10:54:50 UTC+00:00
188	Anggara Surya Saputra	dabafdd9	d3020695	Halow,makasih dah accept invite nya :)	Sent	2017-07-08 10:54:39 UTC+00:00
187	Anggara Surya Saputra	dabafdd9	da452ea4	DCny berapa?	Sent	2017-07-07 10:42:42 UTC+00:00
186	(rose)Amelia artha(rose)	da452ea4	dabafdd9	Qu open ntar mlm y	Inbox	2017-07-07 10:18:59 UTC+00:00
185	(rose)Amelia artha(rose)	da452ea4	dabafdd9	Mau bo mas	Inbox	2017-07-07 10:18:49 UTC+00:00
184	Anggara Surya Saputra	dabafdd9	da452ea4	Halo?	Sent	2017-07-07 07:22:04 UTC+00:00
183	Anggara Surya Saputra	dabafdd9	daf71123	Halow	Sent	2017-07-07 06:27:14 UTC+00:00
182	Anggara Surya Saputra	dabafdd9	da452ea4	Aq samper t4mu jg oke.	Sent	2017-07-07 05:59:33 UTC+00:00
181	Anggara Surya Saputra	dabafdd9	da452ea4	Cek2	Sent	2017-07-07 05:00:48 UTC+00:00
174	Anggara Surya Saputra	dabafdd9	d7d4bc3b	Oi	Sent	2017-07-07 04:42:36 UTC+00:00
173	Anggara Surya Saputra	dabafdd9	daf71123	Aq dpt kontakmu dr wechat	Sent	2017-07-07 04:41:51 UTC+00:00
172	Anggara Surya Saputra	dabafdd9	daf71123	Hai	Sent	2017-07-07 04:41:41 UTC+00:00
171	Anggara Surya Saputra	dabafdd9	da452ea4	Aq d area jakal atas.	Sent	2017-07-07 04:25:17 UTC+00:00
170	Anggara Surya Saputra	dabafdd9	da452ea4	Gmana?,maukah?	Sent	2017-07-07 04:25:08 UTC+00:00
169	Anggara Surya Saputra	dabafdd9	da452ea4	PING!!!	Sent	2017-07-07 04:25:00 UTC+00:00
168	Anggara Surya Saputra	dabafdd9	da452ea4	GFE yuk,mau?	Sent	2017-07-07 03:18:16 UTC+00:00
167	Anggara Surya Saputra	dabafdd9	da452ea4	Km open BO po?	Sent	2017-07-07 02:58:46 UTC+00:00
166	Anggara Surya Saputra	dabafdd9	da452ea4	Image #10	Sent	2017-07-07 02:57:46 UTC+00:00
165	Anggara Surya Saputra	dabafdd9	da452ea4	Aq gak hobi ML, a,aq lbh suka onani,aq seneng ditemenin ngobrol sambil santai :)	Sent	2017-07-07 02:55:35 UTC+00:00
164	Anggara Surya Saputra	dabafdd9	da452ea4	Enggak,GFE aj :)	Sent	2017-07-07 02:54:32 UTC+00:00
163	(rose)Amelia artha(rose)	da452ea4	dabafdd9	Partner ml?	Inbox	2017-07-07 02:47:27 UTC+00:00
162	(rose)Amelia artha(rose)	da452ea4	dabafdd9	Oke mas	Inbox	2017-07-07 02:47:18 UTC+00:00
161	Anggara Surya Saputra	dabafdd9	da452ea4	Lg cari partner ni	Sent	2017-07-07 02:43:48 UTC+00:00
160	Anggara Surya Saputra	dabafdd9	da452ea4	Aq dpt pin km dr wechat	Sent	2017-07-07 02:32:01 UTC+00:00
158	Anggara Surya Saputra	dabafdd9	da452ea4	Lam kenal :)	Sent	2017-07-07 02:31:44 UTC+00:00

Figure 16. Andriller's partial report (BBM)

As for Belkasoft Evidence Center, the report generation ability is actually quite good, but due to the limitations of the trial version software, the resulting report is only 50%, and taken at random, as shown in Figure 17.



Messages

This is a trial version. Only half of items are exported.

12

Direction	From	To	Time (UTC)	Message	Is Deleted	Origin path	Attachments	Author	Data source	Data source path	Length	Offset	Participants	Profile	Profile path	Profile type	Read status	Time (Local)	UIN
Incoming	0	Anggara Surya Saputra	6/30/2017 8:50:29 AM	Aq bkn nudist,jd no nude room sm t4 aq yg unuc,no BJ,no HJ,no ML,aq pgnnya GFE aj.	False			0 (Not available)	BX903FBCZH.ab	D:\Belkasoft - Xperia Z - Final Attempt\BX903FBCZH.ab	0	0	0 (Not available)	Anggara Surya Saputra	image:\T\vol_0\app\com.bbm\f\bbmcore\master.db	BBM (Instant Messengers)		6/30/2017 3:50:29 PM	Anggara Surya Saputra
Incoming	0	Anggara Surya Saputra	6/30/2017 9:14:02 AM	Y itu td,yg aq tulis batasan. Sm aq minta LT,km exclude room,1300 dah sm ongkos bencin,km dtg ndiri yak.	False			0 (Not available)	BX903FBCZH.ab	D:\Belkasoft - Xperia Z - Final Attempt\BX903FBCZH.ab	0	0	0 (Not available)	Anggara Surya Saputra	image:\T\vol_0\app\com.bbm\f\bbmcore\master.db	BBM (Instant Messengers)		6/30/2017 4:14:02 PM	Anggara Surya Saputra

Figure 17. Belkasoft's partial report (BBM)

These generated reports from all forensic tools used are expected to become a supporting evidence that can be used in the investigation and solving process of digital crime cases. The chosen method and report's presentation format generally based on the policies of local law enforcements, on the other words, local law enforcements might use local presentation format.

5 CONCLUSION

Based on the forensics investigation stages that have been discussed about BBM's digital evidence analysis on Android platform, several things that can be concluded are: There are various way to get digital datas from BBM that installed on Android-based that depends on various factor also, such as type of vendor, smartphone screen security, transfer protocol used, and also BBM and Android version.

Mobile Forensics is needed because mobile-based services are increasing and getting more users, with the growing popularity of mobile computing and mobile commerce, the need of mobile transactions are also getting higher and the chance for digital crimes occured also increased significantly.

There are various forensic tools that can be used by forensic examiners to acquire digital data from physical evidences, various tools means various capabilities also. Some evaluations on forensic tools can be conducted to get an overview what tool that best for digital forensic investigations.

REFERENCES

1. Statista: Number of smartphone users worldwide from 2014 to 2020 (in billions). Available at https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/. Accessed on August 2, 2017.

2. Jason Mander: Telegram, BBM and WeChat users keenest on transferring money. Available at http://blog.globalwebindex.net/chart-of-the-day/telegram-bbm-and-wechat-users-keenest-on-transferring-money/. Accessed on August 3, 2017

3. Judith Balea: The latest stats in web and mobile in Indonesia (INFOGRAPHIC). Available at https://www.techinasia.com/indonesia-web-mobile-statistics-we-are-social. Accessed on : August 3, 2017.

4. Liputan 6 News: Ditipu Pria Asing Foto Bugil ABG Banyuwangi Menyebar di Internet. Available at http://news.liputan6.com/read/2099669/ditipu-pria-asing-foto-bugil-abg-banyuwangi-menyebar-di-internet?source=search. Accessed on : August 5, 2017.

5. Hernowo Anggie: Blackberry Di-Hack, Ki Kusumo Lapor ke Mabes Polri. Available at http://showbiz.liputan6.com/read/2207179/blackberry-di-hack-ki-kusumo-lapor-ke-mabes-polri?source=search. Accessed on : August 5, 2017.

6. Mei Amelia R: Polda Metro Bekuk Al Gazali Cs di Palopo Atas Kejahatan Hacker BBM dan Penipuan. Available at https://news.detik.com/berita/3120102/polda-metro-bekuk-al-gazali-cs-di-palopo-atas-kejahatan-hacker-bbm-dan-penipuan. Accessed on August 9, 2017

7. Dolly Rosana: Polisi Selidiki Kasus Pembajakan Identitas aplikasi BBM. Available at http://www.antaranews.com/berita/567216/polisi-selidiki-kasus-pembajakan-identitas-aplikasi-bbm. Accessed on August 8, 2017.

8. Safar Sijabat: Aurel Sediakan Jasa Layanan Seks Via Medsos di Kota Pekanbaru. Available at https://www.tribratanews.com/aurel-sediakan-jasa-layanan-seks-via-medsos-di-kota-pekanbaru/, accessed on August 11, 2017.

9. Anggie Khristian, Yessi Novaria Kunang, and Siti Sa'uda: Forensic Analysis of Whatsapp's Artefact On Android Platform. Bina Darma University. Available at http://digilib.binadarma.ac.id/download.php?id=1336 , 2016.

10. Ilman Zuhri Yadi and Yessi Novaria Kunang: Forensic Analysis on Android Platform. National Conference of Computer Science (Konferensi Nasional Ilmu Komputer (KONIK)). Available at http://eprints.binadarma.ac.id/2191/1/ilman%20zy-%20analisis%20forensik%20android.2.pdf., 2014

11. Asif Iqbal, Andrew Marrington, and Ibrahim Baggili: Forensic Artifacts of the ChatOn Instant Messaging Application. 8th International Workshop on Systematic Approaches to Digital Forensics Engineering. Available at https://pdfs.semanticscholar.org/1265/425a5b91345656b6b9201b3fe24d0a46d015.pdf., 2013

12. Michael W Burnette: Forensic Examination of a RIM (BlackBerry) Wireless Device. Rogers & Hardin LLP. Available at http://web.archive.org/web/20070718221442/http%3A//www.rh-law.com/ediscovery/Blackberry.pdf., 2002

13. Masoud Nosrati, Mehdi Hariri, and Alireza Shakarbeygi: Computer and Internet: From a Chronological View. Internasional Journal of Economy, Management, and Social Sciences. Available at

http://waprogramming.com/papers/5145ceefb2fa72.01222710.pdf., 2013.

14. Imam Riadi, Jazi Eko Istiyanto, Ahmad Ashari, and Subanar: Log Analysis Techniques using Clustering in Network Forensics. International Journal of Computer Science and Information Security (IJCSIS), Vol. 10, No.7, July 2012, pp. 23-30.

15. Hariani and Imam Riadi: Detection Of Cyberbullying On Social Media Using Data Mining Techniques. International Journal of Computer Science and Information Security (IJCSIS),Vol. 15, No. 3, March 2017, pp. 244-250.

16. National Institute of Justice (NIJ): Digital Evidence and Forensics. Available at https://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx. Accessed on August 15, 2017.

17. Venkateswara Rao V and ASN Chakravarthy: Survey on Android Forensic Tools and Methodologies. International Journal of Computer Applications (IJCA), Vol. 154, No.8, November 2016, pp. 17-21.

18. Tajudin: The Occurence of Code Switching on Personnal Message of Blackberry Messenger. Journal of English and Education, 2013, pp. 103-112.

19. BBM: About BBM. Available at https://www.bbm.com/en/about.html. Accessed on August 10, 2017.

20. Oxygen Forensic: Smart Forensics for Smartphones. Available at https://www.oxygen-forensic.com/en/. Accessed on August 5, 2017.

21. SeyedHossein Mohtasebi, Ali Dehghantanha, and Hoorang Ghasem Broujerdi: Smartphone Forensic: A Case Study with Nokia E5-00 Mobile Phone. International Journal of Digital Information and Wireless Communications (IJDIWC), 2011, pp. 651-655.

22. Andriller: Andriller – Android Forensic Tools. Available at http://andriller.com/. Accessed on August 7, 2017

23. Belkasoft Evidence Center: Belkasoft Evidence Center 2017. Available at https://belkasoft.com/ec, accessed on August 11, 2017.

24. Lars Woolleschensky: Cell Phone Forensics. Seminararbeit Ruhr-Universit¨at Bochum. Available at https://www.emsec.rub.de/media/crypto/attachments/files/2011/04/cell_phone_forensics.pdf., 2007.

25. Mohammad Junaid, Jai Prakash Tewari, Rajeev Kumar, and Abhishek Vaish: Proposed Methodology

26. on Smart Phone Forensic Tool. Asian Journal of Computer Science and Technology, Vol. 4, No. 2, 2015, pp. 1-5.

Forensic Investigation Technique on Android's Blackberry Messenger using NIST Framework

ORIGINALITY REPORT

17%

SIMILARITY INDEX

PRIMARY SOURCES

1	www.crypto.rub.de Internet	114 words — 4%
2	www.ijcaonline.org Internet	103 words — 4%
3	www.bestvalueschools.com Internet	49 words — 2%
4	Asif Iqbal, Andrew Marrington, Ibrahim Baggili. "Forensic artifacts of the ChatON Instant Messaging application", 2013 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE), 2013 Crossref	48 words — 2%
5	www.bbm.com Internet	38 words — 1%
6	sumuri.com Internet	33 words — 1%
7	www.secureedd.com Internet	22 words — 1%
8	select-st.ru Internet	21 words — 1%
9	cocoa.ethz.ch Internet	12 words — < 1%
10	www.latestgadgetsindia.com	

	Internet	9 words — < 1 %
11	link.springer.com Internet	9 words — < 1%
12	dione.lib.unipi.gr Internet	9 words — < 1%
13	Knackmuss, Jenny, and Reiner Creutzburg. "Enterprise mobility management (EMM) - a way to increase the security of mobile devices", Mobile Devices and Multimedia Enabling Technologies Algorithms and Applications 2015, 2015. Crossref	8 words — < 1%
14	www.oxygen-forensic.com Internet	8 words — < 1%
15	Kathleen Biblowitz, Shashi Bellam, Giselle Mosnaim. "Improving Asthma Outcomes in the Digital Era: A Systematic Review", Pharmaceutical Medicine, 2018 Crossref	8 words — < 1%

EXCLUDE QUOTES	ON	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	ON		