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

Imam Riadi¹, Sunardi², and Arizona Firdonsyah³

¹ Department of Information System, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
² Master of Informatics Engineering, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
³ (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 platforms 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 occurred 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 phone users in the world is predicted to pass the five billion mark by 2019.

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 applications 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.
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)

<table>
<thead>
<tr>
<th>No</th>
<th>Year</th>
<th>Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2014</td>
<td>Pornography via BBM at Banyuwangi</td>
</tr>
<tr>
<td>2</td>
<td>2015</td>
<td>BBM Account hacking at Jakarta</td>
</tr>
<tr>
<td>3</td>
<td>2016</td>
<td>Online fraud via BBM at Palopo</td>
</tr>
<tr>
<td>4</td>
<td>2016</td>
<td>Identity theft via BBM at Palembang</td>
</tr>
<tr>
<td>5</td>
<td>2017</td>
<td>Online prostitution via BBM at Pekanbaru</td>
</tr>
</tbody>
</table>

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].

![Android Architecture](image)

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-platform 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 difficulties 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 significant 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.

**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>
<thead>
<tr>
<th>No</th>
<th>Specification Type</th>
<th>Physical Evidence’s Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Brand</td>
<td>Sony</td>
</tr>
<tr>
<td>2</td>
<td>Brand Series</td>
<td>Xperia Z</td>
</tr>
<tr>
<td>3</td>
<td>Model Number</td>
<td>C6602</td>
</tr>
<tr>
<td>4</td>
<td>OS</td>
<td>Android</td>
</tr>
<tr>
<td>5</td>
<td>Processor</td>
<td>Quad core 1.5 GHz</td>
</tr>
</tbody>
</table>

**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.

**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.

**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.

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).

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.

Figure 10. Oxygen Forensic Suite’s Contact Analysis

Figure 11. Oxygen Forensic Suite’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.
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.

![Figure 14. Full Report of Oxygen Forensic Suite in PDF](image)

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)](image)

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.

![Figure 16. Andriller’s partial report (BBM)](image)

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.

![Figure 17. Belkasoft’s partial report (BBM)](image)

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 data 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


