HASIL CEK_10 Identification

by 10 Identification

Submission date: 18-May-2022 09:32AM (UTC+0700)
Submission ID: 1838783437
File name: 10 Identification.pdf (1.39M)
Word count: 3397
Character count: 19220

Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method

Article *in* International Journal of Computer Science and Information Security, · May 2017

CITATIONS
44

READS
2,648

3 authors, including:

Imam Riadi
Ahmad Dahlan University
236 PUBLICATIONS **1,474** CITATIONS

SEE PROFILE

Arizona Firdonsyah
Ahmad Dahlan University
8 PUBLICATIONS **98** CITATIONS

SEE PROFILE

International Journal of Computer Science and Information Security (IJCSIS),
Vol. 15, No. 5, May 2017

Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method

Imam Riadi
Department of Information System
Ahmad Dahlan University
Yogyakarta, Indonesia
imam.riadi@is.uad.ac.id

Rusydi Umar
Department of Informatics Engineering
Ahmad Dahlan University
Yogyakarta, Indonesia
rusydi_umar@rocketmail.com

Arizona Firdonsyah
Magister of Informatics Engineering
Ahmad Dahlan University
Yogyakarta, Indonesia
arizona.f@gmail.com

***Abstract*— Smartphone technology is getting more popular year by year. One of the technologies with large number of users is Android-based smartphone. As one of the smartphones operating system, Android is quite competitive within the smartphone market. The number of Android smartphone users also give effect to the development and the use of mobile applications, including instant messenger application. One of instant messenger applications that widely used is Blackberry Messenger (hereinafter shortened as BBM). The increasing number of users of BBM has certainly brought positive and negative effects, one of the negative effects is that some persons that using BBM to perform digital crimes such as pornography and fraud may be rocketing. If a smartphone becomes an evidence in a criminal case and BBM was installed on that smartphone, then on this application digital evidence can be identified and that can be expected an option to assist law enforcements in uncovering digital crimes. As for the way this research done, there are various methods that can be used in the process of forensic analysis and digital evidence identification, the method used in this research is mobile forensic method which is based on upon the available guidelines prepared by the National Institute of Standards and Technology (NIST). The results of the research are presented in the form of recorded conversations, BBM Personal Identification Number (BBM PIN), name of the sender and the recipient, and the conversation time (timestamp) are expected to provide an overview of the steps that can be applied in the field of Android forensic analysis**

Keywords: Digital Evidence, Blackberry Messenger, Digital Forensic

I. INTRODUCTION

Mobile devices have become a daily necessity for every individual. The most commonly used mobile device in everyday communication is the smartphone, there are many Operating Systems for smartphone, one of them is Android. Android-based smartphones are widely used for making calls, sending messages, e-mail, and communication through social networks and instant messaging. One of the most popular instant messaging applications is Blackberry Messenger (BBM). Based on the article from Forbes contributor, Terro Kuittinen, in some countries such as Britain, India, and South Africa Blackberry Messenger has beaten its competitors with the highest and the number of users that continues to increase every year [1]. As for Indonesia, based on a survey conducted by online survey organizations JakPat at 2016, Blackberry Messenger users ranked first with 80.31% of users, followed by WhatsApp users with with 72.78% [2], the graph shown in Figure 1 [2].

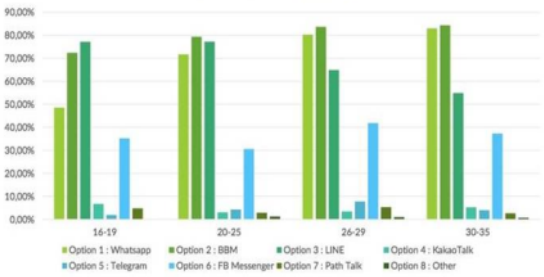

Fig 1. Graphical percentage of Instant Messenger application users in Indonesia

The Increasing users of instant messaging applications, especially Blackberry Messenger, certainly bring many positive impacts, especially in the field of wireless communication, but in addition, the increase in the number of Blackberry Messenger users is also caused by many negative impacts. Many individuals are have misused the practical use of Blackberry Messenger to commit digital crimes such as fraud, pornography, identity theft, drug sales, etc. Figure 2 [3] shows a graph of increasing numbers of crime using a mobile device based on a report issued by the RSA Anti-Fraud Command Center (AFCC), which states that with increasing transactions using a mobile device, in the 4th quarter of 2015, 61% of crimes done through mobile devices, including the smartphone, and the total increase of digital crime through mobile devices from 2013 to 2015 is 173% [3].

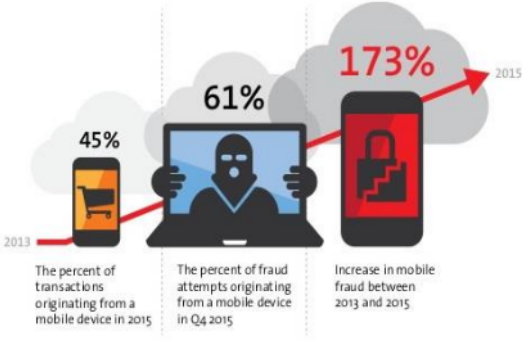

Fig 2. Graphical percentage of of digital crime increase using mobile device

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

In the process for solving digital crime cases, necessary supporting evidence is needed. One of the evidence that can be used to assist law enforcement in solving cases of digital crime is digital evidence obtained from Android smartphones. If on the smartphone Blackberry Messenger was installed, then the application can be analyzed to obtain digital evidence that is expected to assist law enforcement in solving the cases of digital crimes. Based on this background, the authors choose the title of research Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method.

The method used in this research is a mobile forensic method based on guidelines made by the National Institute of Standards and Technology (NIST) [4]. This research aims to analyze how the mobile forensic work in the process of gathering digital evidence related to Blackberry Messenger application.

II. Literature Review

A. Digital Forensic and Mobile Forensic

Digital Forensic is the application of science and computer technology for the benefit of legal proof (pro justice), which in this case is to prove the crime of high-tech or computer crime scientifically to be able to get digital evidence that can be used against offenders [5]. Digital Forensic has many fields, one them is Mobile Forensic.

Mobile Forensic is a science that performs the process of digital evidence recovery from a mobile device using the appropriate way with forensic conditions [6]. Mobile Forensic 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. The quality and speed of the mobile service provider must be comparable to the number of mobile transactions that occur. The challenge of mobile transactions lies in the large number of mobile service providers with high speed and secure networks. Online transactions performed using mobile devices must have high security and protect users from the misuse of irresponsible persons [7].

B. Digital Evidence

Digital evidence is fragile, volatile and vulnerable if it is not handled properly. All kinds of changes containing digital evidence will lead to the wrong conclusions, or the evidence would be useless. Determination of the steps the acquisition of digital evidence performed in observance of:

- Digital media as evidence.
- The physical layout of digital storage media.
- Integrity and authenticity of digital evidence using Write-Protect, hashes, and more.
- Access to digital evidence only given for the who were given the authority and no-one the use of devices electromagnetic close to digital evidence.
- Documentation of conditions and media configuration a digital storage.
- The digital evidence duplicate/imaging using procedure and devices substandard data digital forensic acquisition.
- Documentation of informat ion and do the configuration on digital devices [8].

C. Cybercrime

Although Cybercrime is a term that is quite popular and frequently used, there is no standard definition of cybercrime that has been agreed. However, some organizations have begun to provide a definition of cybercrime, including the UN (United Nations). According to the UN, cybercrime in its broadest sense 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 question : when, what, who, where, how and why related to digital crime [9]. From that definition, cybercrime is formulated as an act against the law that is done by using computer network as a tool or computer as an object, either to gain profit or not, and there are elements that can be harmful to others [10]. There are many kinds of cybercrimes, one of the example is cyberbullying, cyberbullying is a term that refers to the use of information technology to bully people to send or post text that is intimidating or threatening [11].

D. Android

Android is an open source operating system for Google's Linux-based smartphones. Android has been developed by Google as an open operating system that provides freedom for hardware manufacturers and phone operators to develop their operating systems and applications. The open nature of Android encourages developers to build a large number of applications and upload them to the Android Market. These applications can be used by users by downloading them from Android Market, then install them on their smartphone [12].

E. Blackberry Messenger

The official website of Blackberry Messenger, www.bbm.com, informs that BBM is one of the instant messaging applications for mobile devices originally used only for smartphones with Blackberry OS, but as the evolving nature of digital communication era, BBM's functionality switches into across platform applications, Nowadays, BBM is not only used in BlackBerry devices, but it can be also used on the Android platform, iOS, and Windows. Since its creation in August 2005, BBM, originally a text messaging application limited to text-only functions, has added features that make communication more 'live' like stickers, emoticons, timed messages, BBM Group, Video Call, and more Other services [13]. Site detik.com describes the workings of BBM applications as in Figure 3 [14].

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

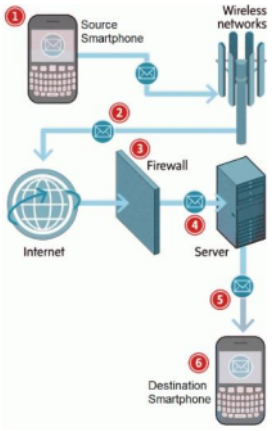

Fig 3. A Brief chart of BBM workflow

F. Andriller

Andriller is one of the software that can be used for forensic analysis purposes on smartphones. This application is a cross platform application that operates on Microsoft Windows and Ubuntu Linux. Andriller has the ability to perform non-destructive analysis on Android devices, such as : extracting and decoding data automatically, unlocking the lockscreen pattern, lifting the SMS and MMS data, and application databases.Andriller can also generate reports in HTML and Excel formats [15] Some examples of Andriller features can be seen in Figure 4 [16].

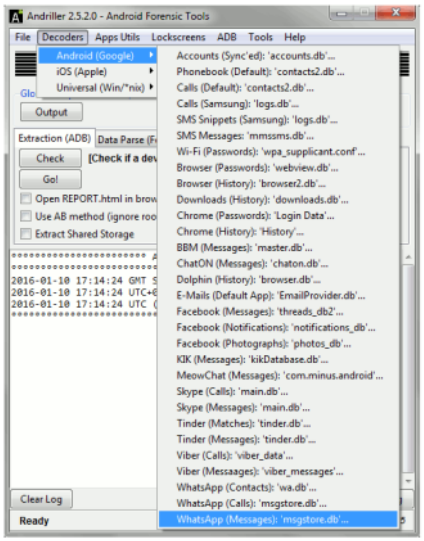

Fig 4. Example of Andriller's Features

III. Materials and Method

A. Materials

Forensic tools generally require considerable resources when doing the process of acquiring digital evidences, therefore a set of strong supporting devices are required. The tools and supporting hardware in this research can be seen in table 1.

TABLE I
THE MATERIALS

No.	Material	Description
1	Notebook	Asus SonicMaster X450J, OS Windows 10 64bit
2	Data Cable	A data cable that can be used to connect laptop with smartphone
3	Smartphone	Sony Xperia Z, OS Android Lollipop
4	Andriller	Windows-Based Applications that can be used to acquire digital evidence on a smartphone
5	Blackberry Messenger	Instant Messenger multiplatform application.

B. Method

This research uses the Mobile Forensic method which is a method of digital evidence analysis on mobile devices. This method is issued by the National Institute of Standards and Technology (NIST). NIST Mobile Forensic consists of 4 consecutive stages as illustrated in Figure 5 [17].

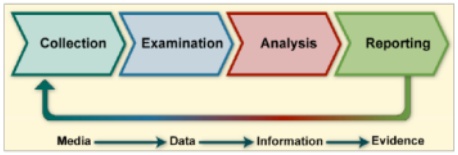

Fig 5. NIST Mobile Forensic Stages

Based on Figure 5, it can be described the mobile forensic analysis stages as follows:

1. Collection : dentify, label, record, and retrieve data from relevant data sources by following data integrity preservation procedures.
2. Examination : 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.
3. 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.
4. Reporting : 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 (eg, forensic examination from additional data sources, securing identified gaps, or increasing security controls), and provide recommendations for refining policies, procedures, tools, and other aspects of the forensic process.

IV. Result and Discussion

This research is an attempt to apply the NIST Mobile Forensic method on Blackberry Messenger installed on Android smartphones. To do so, a sample case is given as

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

the source of material data analysis and digital evidence. In this sample case, it is assumed that an Android smartphone was found. The smartphone's condition was fine, and the owner was allegedly becoming a victim of a blackmail under the online sex transaction. Based on existing reports, the crime occurs in Blackberry Messenger applications used by victims. The investigation team then followed up with a digital forensic analysis to obtain the evidence contained in the Blackberry Messenger.

A. *Collection*

At this stage, the investigation team is collecting the evidence from the owner. The evidence is 1 piece of Sony Xperia Z smartphone with 2GB of RAM, Lollipop Android OS, in it installed Blackberry Messenger.

Fig 6. Android Smartphone as Evidence

B. *Examination*

At this stage, an examination of the Blackberry Messenger installed on the smartphone was conducted to acquire the digital evidence contained in the application. The tool used in this research is Andriller, which is one of the forensic tool for Android smartphones. Figure 7 shows a screenshot of the data acquiring process on Blackberry Messenger.

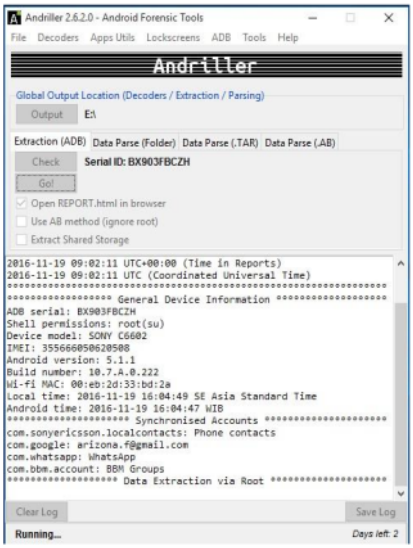

Fig 7. Data Acquiring Process on BBM

Based on the results of the acquiring data process, the investigation team was able to obtained data recording conversations that occur on the Blackberry Messenger in the form of a table containing the data of sender name, PIN sender, message recipient (PIN), message content, message type, and message time as shown in figure 8.

Fig 8. Data Acquiring Process Result

C. *Analysis*

At this stage, analysis of the results from digital evidence acquiring process on Blackberry Messenger is done. As shown in Figure 9, from the acquired conversation data, there are several messages indicating a digital crime case in the form of a blackmail. In the conversation data, it is also possible to send some image files in certain sizes but can not be displayed because of the limitations of the forensic tool used.

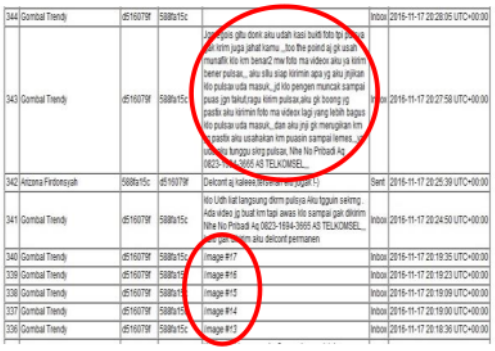

Fig 9. Indicating Evidence of Blackmail

D. *Reporting*

This stage is the stage of reporting the results from digital evidence acquiring process and analysis performed. For this reporting stage, Andriller is able to generate reports and logs automatically in HTML format and text files with extension .txt. This HTML-formatted report can be accessed through the browser, this report contains the acquired data from the analyzed smartphone, the data contained : e-mail accounts, wifi passwords, applications installed on smartphones, sms, and call logs. Figure 10 shows the report in HTML format.

https://sites.google.com/site/ijcsis/
ISSN 1947-5500

[Andriller Report] SONY C6602 | IMEI:355666050620508

Type	Data
ADB serial:	BX903FBCZH
Android ID:	ae2ef07b46d37fd5
Shell permissions:	root(su)
Manufacturer:	SONY
Model:	C6602
IMEI:	355666050620508
Android version:	5.1.1
Build name:	10.7.A.0.222
Wifi MAC:	00:eb:2d:33:bd:2a
Bluetooth MAC:	00:eb:2d:06:fe:56
Bluetooth name:	Gembel Necis
Local time:	2016-11-19 16:04:49 SE Asia Standard Time
Android time:	2016-11-19 16:04:47 WIB
Accounts:	com.sonyericsson.localcontacts: Phone contacts com.google: arizona.f@gmail.com com.whatsapp: WhatsApp com.bbm.account: BBM Groups
System:	Synchronised Accounts (4)
System:	Wi-Fi Passwords (3)
Web browser:	Google Chrome History (34)
Communications data:	Contacts (688)
Communications data:	Call logs (6)
Communications data:	SMS Messages (26)
Applications data:	WhatsApp Contacts (255)
Applications data:	WhatsApp Calls (16)
Applications data:	WhatsApp Messages (482)
Applications data:	Blackberry Messenger (177)

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

Fig 10. Andriller's HTML Version Report

Andriller also has the ability to generate reports in text format with the name "Andriller.txt", the contents of this report is similar to the HTML formatted report, it's just that there is no link to access other reports. The contents of this report is in the form of the result's logs of the acquiring data process that performed such as: the date of data acquiring process, Android version, IMEI, and other data as shown in Figure 11.

Fig 11. Andriller's .txt Version Report

The digital forensic steps that have been carried out in this sample case can also been carried out for another cybercrime cases. The complexity of searching and acquiring digital evidence for cybercrime cases using smartphones as mentioned in 2013 RSA report [14] surely will be more complicated and requires wider knowledge, skills and experiences. The availability of supporting tools is also very much needed. This research at least can be the first step in the efforts to handle more complex cybercrime cases, and to help further research, especially on digital forensic fields.

V. Conclusion

Based on the results of analysis and discussion in this research, there are several things that can be concluded were : NIST Mobile Forensic method can be applied to the digital evidence acquiring process from Blackberry Messenger on Android smartphone using Andriller tool. Based on the acquired data, Andriller is only able to acquire digital evidence in the form of conversation data, the name of the sender of the message, PIN of the sender and the recipient of the message along with the date of the conversation. The image data does not appear when the data acquiring process is done.

Based on the description of the above research's results, some suggestions that can be given for further development and research were : In addition to the NIST Mobile Forensic method, there are several other methods that can be used in the process of acquiring and analyzing digital evidence, with more detailed and complete processes. More methods are expected to provide more accurate results. The use of tools in the acquiring digital evidence process can also be combined with other tools that have different capabilities that can provide support among tools to produce better reports.

References

[1] Terro Kuittinen, "*Exclusive New Survey Shows BlackBerry's BBM Beating WhatsApp And SnapChat In Key Markets*". Available at http://www.forbes.com/sites/terokuittinen/2013/11/26/exclusive-new-survey-shows-blackberrys-bbm-beating-whatsapp-and-snapchat-in-key-markets/#4a0055b92dd8, accessed on November 07, 2016.

[2] Ketut Krisna Wijaya, "*JAKPAT's Survei Result: BBM still ruled Indonesia at the beginning of 2016*". Available at https://id.techinasia.com/aplikasi-blackberry-messenger-indonesia, accessed on November 10, 2016.

[3] RSA, "*2016:The Current State of Cybercrime*," RSA Anti Fraud Command Center, Canada, 2016.

[4] 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.

[5] Riky Ramadhan, A. Haidar Mirza, and Ilman Zuhri Yadi, "*Forensic Analysis for Blackberry Messenger on Android and Blackberry*". Available at : http://digilib.binadarma.ac.id/download.php?id=954., 2013.

[6] 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

[7] Nuril Anwar, Imam Riadi, and Ahmad Luthfi, *"Forensic SIM Card Cloning Using Authentication Algorithm"*, International Journal of Electronics and Information Engineering, Vol.4, No.2, PP.71-81, June 2016 (DOI: 10.6636/IJEIE.201606.4(2).03), 2016

[8] Faiz Albanna, Imam Riadi, "*Forensic Analysis of Frozen Hard Drive Using Static Forensics Method*", International Journal of Computer Science and Information Security (IJCSIS), Vol. 15, No. 1, January 2017.

[9] Imam Riadi, Jazi Eko Istiyanto, Ahmad Ashari, and Subanar, "*Log Analysis Techniques using Clustering in Network Forensics*", (IJCSIS)

International Journal of Computer Science and Information Security, Vol. 10, No.7, July 2012.

[10] Yudi Prayudi, "*Digital Forensics Analysis On Blackberry To Support Cybercrime Case Handling Using Smartphones*", Resarchgate, Available at: https://www.researchgate.net/publication/257137348, 2013.

[11] Hariani, 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.

[12] Satish Bommisetty, Rohit Tamma, and Heather Mahalik, "*Practical Mobile Forensic*", PACKT Publishing, Birmingham, UK, 2014.

[13] Blackberry Limited, "*About BBM*", Available at http://www.bbm.com/id/about.html, accessed on November 11, 2016

[14] Fino Yurio Kristo, *"Peeking the way Blackberry Messenger works"*. Available at http://inet.detik.com/read/2013/10/25/100240/2395223/317/mengintip-cara-kerja-blackberry-messenger, accessed on November 30, 2016

[15] Andriller, "*Andriller – Android Forensic Tool*", Available at http://www.andriller.com, accessed on November 15, 2016

[16] Karen Kent, Suzanne Chevalier, Tim Grance, and Hung Dang, *"Guide to Integrating Forensic Techniques into Incident Response"*, National Institute of Standard and Technology, US Department of Commerce, Available at nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf, 2006.

[17] RSA, "2013:The Current State of Cybercrime, "RSA Anti Fraud Command Center, Canada, 2013

HASIL CEK_10 Identification

ORIGINALITY REPORT

8%	6%	5%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to American Public University System Student Paper	2%
2	www.scribd.com Internet Source	2%
3	www.gwern.net Internet Source	1%
4	docshare.tips Internet Source	1%
5	Submitted to School of Business and Management ITB Student Paper	1%
6	Mohammed Nowshad Ruhani Chowdhury, Ezaz Ahmed, Md. Abu Dayan Siddik, Akhlak Uz Zaman. "Heart Disease Prognosis Using Machine Learning Classification Techniques", 2021 6th International Conference for Convergence in Technology (I2CT), 2021 Publication	1%
7	forense.info Internet Source	

<1%

8	archive.org Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		