

RINGKASAN BUKTI KORESPONDENSI

Judul Artikel : Mobile Forensic Tools Evaluation for Digital Crime Investigation
Penulis : Rusydi Umar, Imam Riadi, Guntur Maulana Zamroni
Jurnal : (IJASEIT) International Journal on Advanced Science, Engineering and Information Technology Vol. 8 No. 3 (2018): 20 Juni 2018



1. Lampiran 1	:	Penulis melakukan submission artikel pada 4 Oktober 2017
2. Lampiran 2	:	Pada tanggal 9 Oktober 2017, penulis menerima pemberitahuan terkait revisi artikel (<i>revisions required</i>)
3. Lampiran 3	:	Penulis mengirimkan hasil revisi pada tanggal 9 Oktober 2017
4. Lampiran 4	:	Pada tanggal 31 Maret 2018, penulis menerima pemberitahuan terkait hasil <i>review</i> dari <i>reviewer</i> (<i>revision required</i>)
5. Lampiran 5	:	Penulis mengirimkan hasil revisi kedua pada tanggal 3 April 2018
6. Lampiran 6	:	Pada tanggal 24 Mei 2018, penulis menerima notifikasi bahwa artikel diterima (<i>accept submission</i>)
7. Lampiran 7	:	Pada tanggal 20 Juni 2018 artikel diterbitkan

Lampiran 1

#3591 Summary

[SUMMARY](#) [REVIEW](#) [EDITING](#)

Submission

Authors	Rusydi Umar, Imam Riadi, Guntur Maulana Zamroni
Title	Mobile Forensic Tools Evaluation for Digital Crime Investigation
Original file	3591-7607-1-SM.DOC 2017-10-04
Supp. files	None
Submitter	Guntur Maulana Zamroni 
Date submitted	October 4, 2017 - 08:59 PM
Section	Articles
Editor	Rahmat Hidayat 
Abstract Views	4

Mobile Forensic Tools Evaluation for Digital Crime Investigation

Rusydi Umar[#], Imam Riadi^{*}, Guntur Maulana Zamroni[#]

[#] Department of Informatics Engineering, Ahmad Dahlan University, Jl. Prof. Dr. Soepomo, Warungboto, Umbulharjo, Yogyakarta, 55164
E-mail: rusydi_umar@rocketmail.com

^{*}Department of Information System, Ahmad Dahlan University, Jl. Prof. Dr. Soepomo, Warungboto, Umbulharjo, Yogyakarta, 55164
E-mail: imam.riadi@is.uad.ac.id

[#]Department of Informatics Engineering, Ahmad Dahlan University, Jl. Prof. Dr. Soepomo, Warungboto, Umbulharjo, Yogyakarta, 55164
E-mail: gunturmz@yahoo.com

Abstract— Instant Messaging is a popular smartphone’s application. One example of Instant Messaging application is WhatsApp. WhatsApp is widely used judging from its users that reach more than 1 Billion users in January 2017. WhatsApp’s security recently has been updated with latest encryption type and technology by implementing end-to-end encryption. The number of users or possible crime target and security features in WhatsApp can lead to crime by people that have criminal intentions. Investigators need to use mobile forensic methodologies and tools for investigating smartphone and to find crime evidences. However, investigators often facing challenges during investigation because incompatibility between forensic tools and mobile technology. This research will conduct an experiment using available forensic tools with NIST forensic method for extracting latest WhatsApp’s artifacts. Forensics tools capabilities will be evaluated and compared to find its strengths and weaknesses.

Keywords— mobile forensic, whatsapp, extraction.

I. INTRODUCTION

Smartphones experience rapid development along with the development of technology. Smartphones are slowly beginning to replace the role of computers with the increasing number of features and applications available on mobile devices [1]. Trend of smartphone usage is expected to increase seen from the features offered by smartphones such as various applications, power usage, process speed, pricing, practicality and ease of carrying.

The latest generation of smartphones has the ability and power far above its predecessors that make smartphones now can be used for household activity or office work [2]. Fig. 1 shows the number of smartphone and computer device users. We can see the number of smartphone users has obtained increasing significant number compared to the number of computer users. Starting in 2014 the number of smartphone users began to outperform the number of computer users [1].

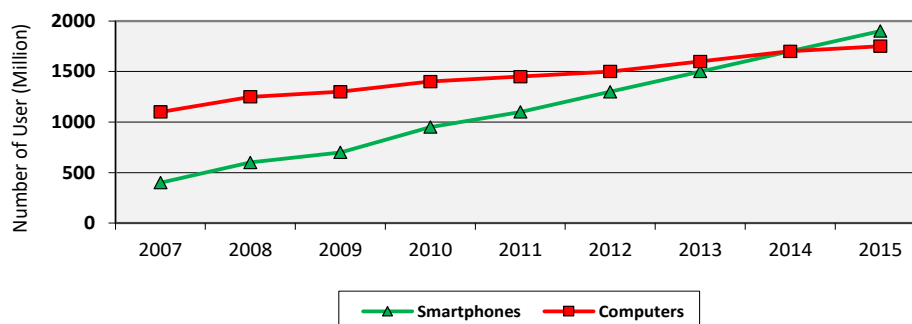


Fig. 1 Number of computer and smartphone users

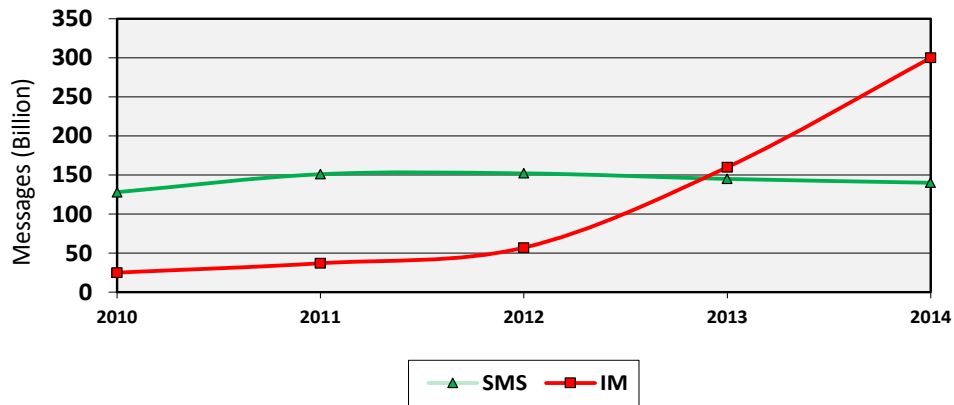


Fig. 2 Number of Messages Sent Using SMS and IM in United Kingdom

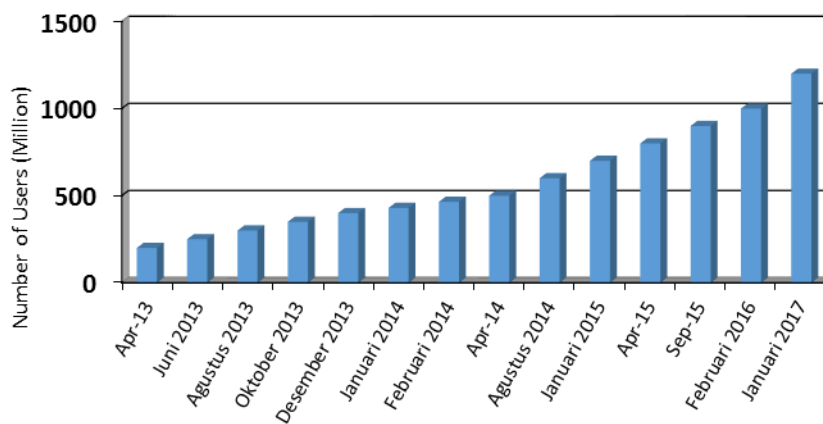


Fig. 3 Number of WhatsApp Users

The Instant Messaging (IM) application is one of the most commonly used applications for mobile device users. IM begins to replace the role of Short Message Services (SMS) to communicate through message delivery. Fig. 2 shows the trend of message delivery with SMS and IM in the UK. The number of message delivery using SMS from 2010 to 2014 tend to experience stable conditions. While the number of message delivery using IM has increased significantly starting in 2012 with the number of messages sent for 57 billion messages/year until 2014 with messages sent for 300 billion/year [3].

WhatsApp is one of the popular IM applications and is used by lots of people to communicate. Fig. 3 shows an increase in the number of WhatsApp users from 200 Million users in April 2013 to 1 Billion in February 2016 and 1.2 Billion in January 2017 [4]. According to [5], WhatsApp is a popular application with 60% of users, followed by Viber and Telegram.

WhatsApp cannot be separated from misuse as for criminal purposes. Under these circumstances the investigator will check out WhatsApp's artifact to look for evidence of a criminal offense. The case of "cyanide coffee" is one example of the case where the WhatsApp artifacts were analyzed to search for evidence in the investigation [6].

To conduct an analysis the investigator needs to use a method along with a forensically tested tools. Investigators should be able to extract the artifacts, decryption, and analyze the data contained within the mobile device to assist the investigation process because data such as conversation messages and images can be evidence [7].

References [8] conducted an analysis of forensic mobile technologies and forensic tools. Forensic analysis has several constraints such as hardware differences, security features, technological lag and forensic tool costs, anti-forensic techniques, and many other. In April 2016, WhatsApp implemented an end-to-end encryption feature that came with the latest encryption. This feature makes the sent messages to be encrypted and can only be read by those eligible to receive the message. This security feature provides difficulties and challenges for forensic investigators and analysis because the available forensics tools must be able to keep up with the development of WhatsApp technology [9].

There are several studies on mobile forensic analysis. References [10] conducted forensic analysis of Telegram, Line, and KakaoTalk applications on Android devices. They tried to conduct a forensic analysis process on unencrypted conversations and encrypted conversations. The tools used in the research were ADB (Android Debugging Bridge), SQLite

Browser, Hex Editor Neo, Busybox, Root Browser, Nandroid Backup, Shark for Root, dex2jar. References [10] used a methodology from McKemish which has 4 stages: Identification, Preservation, Analysis, and Presentation. References [10] managed to investigate unencrypted and encrypted conversations from all three applications.

References [11] attempted to perform a forensic analysis on WhatsApp version 2.11.186 which has been equipped with .crypt encryption. The tools used were WhatsApp Xtract for the extraction and decryption process, and SQLite Browser for the analysis process. The researcher succeeded in extraction and .crypt decryption.

References [12] conducted a forensic analysis on WhatsApp that has used .crypt7 encryption. The tools used in the research were ADB, WhatsApp Key/DB Extractor 2.2, WhatsApp Viewer, WhatsApp Extract, dan SQLite Spy. Researchers managed to extract and decrypt WhatsApp artifacts. Researchers reminded about the importance of paying attention to the development and changes in mobile technology to be able to perform forensic analysis.

References [13] evaluated and compared 2 forensic methodologies, ISO/IEC methodology and NIST methodology. Ajijola, et al concluded that there is no methodology covering all forensic issues. The ISO/IEC methodology has advantages over non-technical processes and problems. NIST has the advantage of selecting and using forensic tools. Each methodology needs to be constantly updated following the development of digital technology.

Looking at the background, the dynamics of mobile technology, previous research, and mobile forensic challenges, researchers will try to conduct comparative evaluation forensic tools that serve to extract artifacts in the form of messages, images, videos and documents with NIST forensic methodology in the latest version of WhatsApp in Android-based devices. The tools used are ADB, WhatsApp Key/DB Extractor 4.7, and Belkasoft Evidence (trial version). Forensic tools are tested to run the WhatsApp database extraction and decryption process that has been updated with .crypt12 end-to-end encryption. The results of extraction, decryption, and validation of forensic tools will be compared in order to have the conclusions.

II. METHODOLOGY

The purpose of this research was to evaluate and compare the Belkasoft Evidence (trial version) and WhatsApp Key/DB Extractor forensic tools, especially in terms of the extraction capabilities of the latest WhatsApp artifacts on Android-based devices that have used .crypt12 encryption.

A. Research Steps

This research used a research step made by the National Institute of Stanford and Technology [7]. The NIST research stage consists of 4 stages as in Fig. 4.

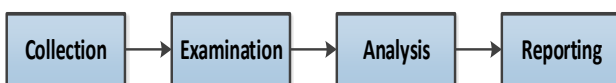


Fig. 4 NIST Forensic Methodology

- 1) *Collection*: In the collection stage, there will be the acquisition of evidence, preservation of evidence, preparation of objects and research tools.
- 2) *Examination*: At the examination stage, there will be process of identifying data that can be used as evidence. After determining which data will be taken, the data retrieval process will be done in a forensically tested way.
- 3) *Analysis*: The data which have been taken will be analyzed to look for things that can be used as evidence and then conclusion will be taken
- 4) *Reporting*: The last stage of the forensic step is to report forensic activity from beginning to the end along with the results of the analysis into the form of a written report or oral report.

This research focused on the examination stage. The examination stage is further elaborated into several stages as in Fig. 5. Identification is done to find data or artifacts to be taken and possibly produce evidence to assist investigation. After determining the data or artifacts to be taken, it will proceed to the data retrieval process.

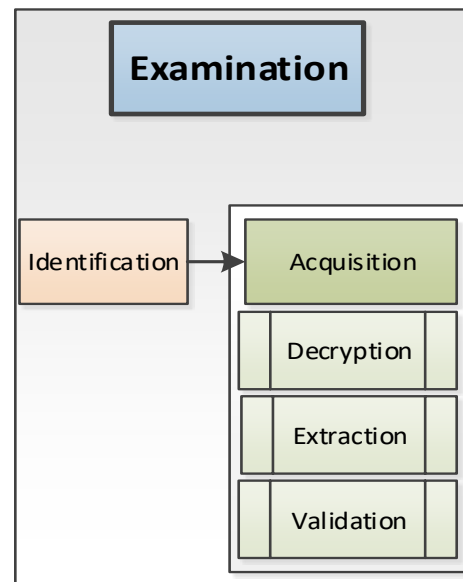


Fig. 5 Steps of Examination

WhatsApp has been equipped with an encryption feature that aims to hide messages [14]. This encryption feature can interfere with the investigation process. Therefore, a tool that can perform decryption and data extraction is needed. Validation using repeatability and reproducibility according to the NIST method will be performed to ensure that the results of the extraction process performed are correct and there is no data manipulation. Repeatability is done by repeated extraction processes in time adjacent to the same object and forensic tool. While reproducibility is done by using the same object but with different forensic tools.

B. Research Tools

The hardware and software used to experiment on the extraction of WhatsApp artifacts from an Android-based device can be seen in Table 1.

TABLE I
RESEARCH TOOLS AND DEVICES

No.	Tool and Device	Information
1	Samsung Galaxy S4 GT-I9500 with 5.0.1 Lollipop operation system	Smartphone device for experiment
2	WhatsApp ver. 2.17.147	Instant Messaging application
3	Workstation with operational system of Windows 7 64 Bit, Intel i5-4440, 4,00 GB	Computer device for extraction and analysis
4	USB Cable	USB connector to connect smartphone device and computer
5	Android Debugging Bridge	Software to support a communication between smartphone and computer
6	WhatsApp Key/DB Extractor 4.7	Extraction tool
7	Belkasoft Evidence (ver trial)	Extraction and analysis tool
8	SQLite Studio	Analysis tool

C. Experiment Simulation

The experiments were conducted in a closed and noise free condition, meaning that the smartphone device was changed to Airplane Mode. With Airplane Mode the device will not be able to receive outside calls and messaging. This is important to maintain the authenticity and integrity of the data. The workstations used are not connected to the Internet and are free from malware that may influence the results of the experiment.

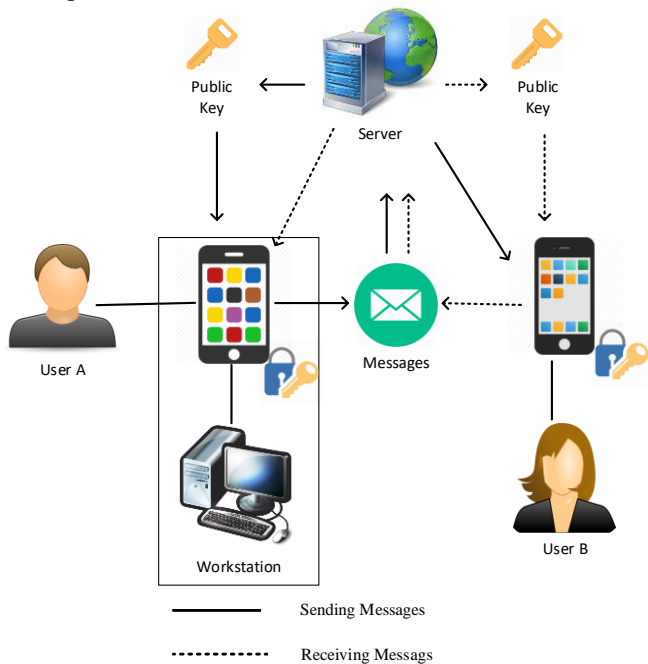


Fig. 6 Experiment Simulation

Fig. 6 describes the simulation of the experimental tool. To send a message to User B, User A will request a public key on the server which will then be used for message encryption. User B then uses the private key to decrypt the message.

User A's Smartphone will be used for forensic analysis. Smartphones with the Android 5.0.1 operating system and WhatsApp 2.17.147 are used for everyday activities such as sending and receiving messages, pictures, videos, and documents which will be connected using a USB cable with workstations that use Windows 64 Bits, ADB, WhatsApp Key/DB Extractor 4.7, and Belkasoft Evidence.

III. RESULTS AND DISCUSSION

A. Extraction results using Belkasoft Evidence

In experiments conducted using Belkasoft Evidence (trial ver) the message artifact of WhatsApp text was not obtained, but video, image, and document artifacts were successfully obtained. Information about the video artifact can be seen in the properties column. Belkasoft provides video file information such as file name, file size, and access date. The size of the extracted video file has different video pixel duration and size according to the original file on the smartphone. Video artifacts can be played and viewed so that it is helpful in the investigation process in the search of evidence as described in Fig. 7. Image artifacts can be zoomed to see clearer images and help with double clicking as well as displaying information from image files such as filename, access date, pixel size, and file size as in Fig. 8. The pixel size and file size of the image artifact match the original size of the original file on the smartphone.

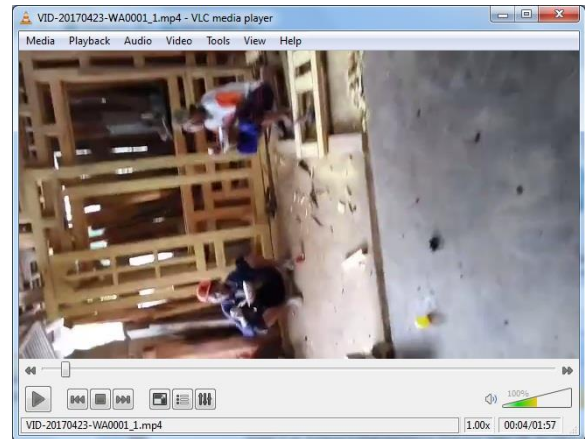


Fig. 7 Video artifact detail of Belkasoft Evidence

Metadata information from documents such as maker name, software used, file name, and file size can be known. The document artifact can be opened so that the investigator can see the contents of the document.

B. Extraction results using Belkasoft Evidence

WhatsApp Key / DB Extractor only manages to get text message artifacts and images. No video and document

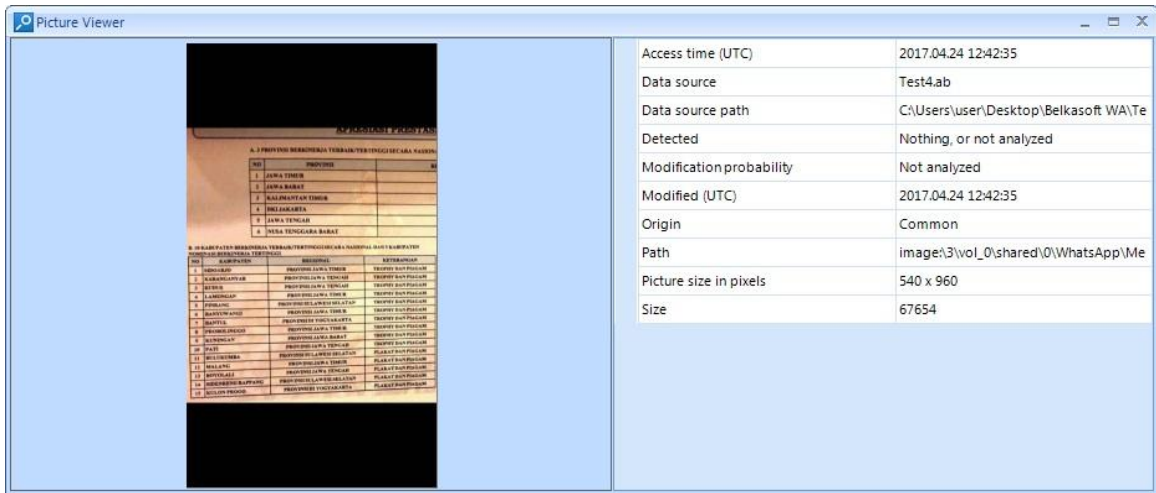


Fig. 8 Picture artifact detail of Belkasoft Evidence

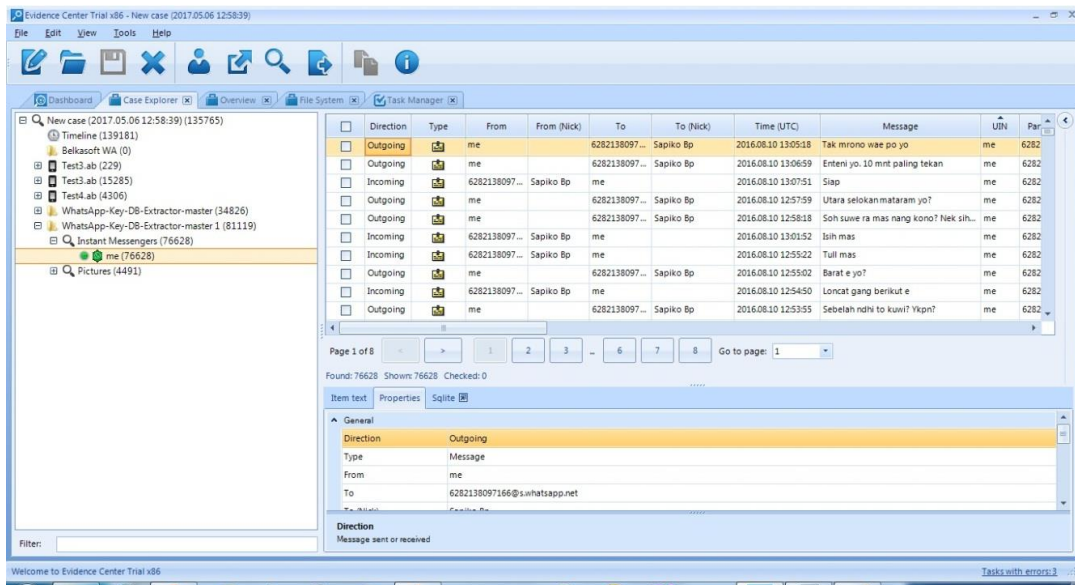


Fig. 9 WhatsApp Key/DB Extractor Message Artifact

artifacts were found. Fig. 9 shows the text message artifacts that were successfully obtained. The text message artifact is in the file "msgstore.db".

Information such as message sender, message recipient, message content, time of sending or receiving messages, and file attachment can be known. Such information will be very useful in the investigation process. WhatsApp Key/DB Extractor manage to get the existing group information in WhatsApp. Groups' name and members can be found in the artefact. WhatsApp Key / DB Extractor manages to get the entire contact WhatsApp information in the "wa.db" file artifact. Contact artifacts are opened by using SQLite Studio as shown in Fig. 10. Contact details such as phone numbers and contact names are known.

The image artifact is obtained using the WhatsApp Key/DB Extractor. Just like Belkasoft Evidence, WhatsApp Key/DB Extractor also shows information from image files such as filename, access date, pixel size, and file size. The image can be zoomed by double click but the zoomed image will break as shown in Fig. 11. This is because the pixel size

of the image obtained only measures 56 x 100 pixels or in accordance with the thumbnail size in WhatsApp. The size applies to all extracted images using WhatsApp Key/DB Extractor.

status_timestamp	number	raw_contact_id	display_name
0	0222531	997	MM itb
1473441122000	0822207	1956	Tornado Nano Seller
0	+628388	2333	Calon Koki 11
0	+622749	1111	Yusuf servis ac
1430971391000	+628574	889	Didit
1423072923000	+628574	846	Arif net
1471952553000	+628572	1850	Jogjaringan Isp
0	+628389	1040	Rahmat net no laen
0	+601393	835	Alif Arena
1478700523000	0813254	1071	Seller char ao twinbrother
0	+601766	837	Alwi Skate
0	0878392	1901	Yanto Buang Material
1478973985000	+601690	1097	Wawan Setiawan
1464963504000	0857439	1023	Pak raharjo instalasi listrik
0	+628520	986	Mbak pipit pakdhe kelik
1470224229000	+628157	909	Fauzan Tehnisi
1410859388000	0857299	1826	Magma Seller
0	0856433	961	Mas Bejo roti bakar
0	0274563	1940	Univ Ahmad Dahlan
1464188106000	0858787	900	Dwi servis ac stikes
0	0877382	916	Gunawan atlantica onlen joki jogja
1478792857000	+628577	1996	Mas Oji Jkt
1478006823000	+628128	981	Mbak Mega
0	0857763	895	DN indo joki

Fig. 10 WhatsApp Contact List Artifact

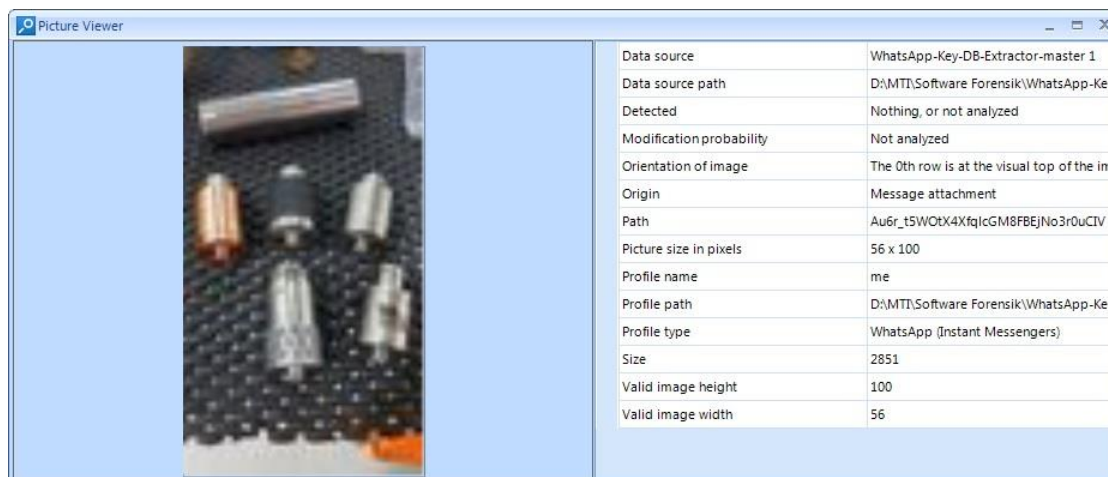


Fig. 11 WhatsApp Key/DB Extractor Picture Detail

C. Discussion

Table 2 shows the artifacts obtained. WhatsApp Key / DB Extractor only manages to extract text message and images artifacts. Message information such as message body, message recipient, message sender, chat group, chat group participant, all contacts on WhatsApp either name or phone number is successfully obtained. This is certainly very useful in helping the investigation process to look for evidence of crime. WhatsApp Key/DB Extractor managed to get the image artifact, but in size of 56 x 100 pixels. Unlike the WhatsApp Key/DB Extractor, Belkasoft Evidence (trial ver) manages to get images, video and document artifacts.

TABLE III
FORENSIC TOOLS COMPARISON

Artifact Type	Belkasoft Evidence (trial ver)	WhatsApp Key/DB Extractor
Text Message	-	√
Image	√	√
Video	√	-
Document	√	-

Image artifacts obtained using Belkasoft Evidence (trial ver) have better quality than WhatsApp Key/DB Extractor artifacts. Belkasoft Evidence (trial ver) does not get text message artifacts.

The extraction results using Belkasoft (trial ver) and WhatsApp Key/DB Extractor are repeated to ensure the similarity of the results obtained. This needs to be done to test the validation of results from forensic tools according to the NIST method. From the validation test result, both Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor meet validation test of repeatability and reproducibility as in Table 3.

TABLE IIIII
FORENSIC TOOLS VALIDATION

Tools Validation	Belkasoft Evidence (trial ver)	WhatsApp Key/DB Extractor
Repeatable	√	√
Reproducible	√	√

IV. CONCLUSIONS

Based on the results of testing conducted on WhatsApp 2.17.147 with .crypt12 encryption, Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor meet validation test of repeatability and reproducibility. WhatsApp Key/DB Extractor dominates in the extraction ability of text message artifacts. Belkasoft Evidence (trial ver) has advantages in extraction abilities for images, videos, and documents. Further research on WhatsApp artifact extraction abilities in non-Android platforms needs to be done considering the WhatsApp application is available for many platforms.

REFERENCES

- [1] D. Chaffey, "Smart Insight Marketing Intelligence Ltd," Smart Insight, 1 March 2017. [Online]. Available: <http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/>.
- [2] C. Bonnington, "CNMN Collection," 2 October 2015. [Online]. Available: <https://www.wired.com/2015/02/smartphone-only-computer/>.
- [3] L. Garratt and S. Poulter, "Associated Newspapers Ltd," 13 January 2014. [Online]. Available: <http://www.dailymail.co.uk/sciencetech/article-2538488/SMS-takes-seat-IM-number-texts-sent-Britain-falls-time.html>.
- [4] "Statista Inc," January 2017. [Online]. Available: <https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/>.
- [5] T. Sutikno, L. Handayani, D. Stiawan, A. R. Riyadi and I. M. Subroto, "WhatsApp, Viber and Telegram: which is the Best for Instant Messaging?," *International Journal of Electrical and Computer Engineering*, vol. 6, no. 3, pp. 909-914, June 2016.
- [6] A. Kusumadewi and J. P. Sasongko, "Cable News Network Inc," 21 January 2016. [Online]. Available: <http://www.cnnindonesia.com/nasional/20160121080758-12-105715/polisi-usut-percakapan-jessica-mirna-yang-beredar-disosmed/>.
- [7] R. Ayers, S. Brothers and W. Jansen, "Guidelines on Mobile Device Forensics," National Institute of Standards and Technology, 2014.
- [8] D. Sai, N. R. Prasad and S. Dekka, "The Forensics Process Analysis of Mobile Device," *International Journal of Computer Science and Information Technology*, vol. 6, no. 5, pp. 4847-4850, 2015.
- [9] J. Koum and B. Acton, "WhatsApp," 5 April 2016. [Online]. Available: <https://blog.whatsapp.com/10000618/end-to-end-encryption>.
- [10] G. B. Satrya, P. T. Daely and S. Y. Shin, "Android Forensics Analysis:

Private Chat on Social Messenger,” *IT Convergence Engineering*, 2016.

- [11] S. Sahu, “An Analysis of WhatsApp Forensics in Android Smartphones,” *International Journal of Engineering Research*, vol. 3, no. 5, pp. 349-350, 1 May 2014.
- [12] L. P. Gudipaty and K. Y. Jhala, “WhatsApp Forensics: Decryption of Encrypted WhatsApp Databases on Non Rooted Android Devices,” *Journal Information Technology & Software Engineering*, vol. 5, no. 2, 2015.
- [13] A. Ajijola, P. Zavorsky and R. Ruhl, “A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101,” in *World Congress on Internet Security*, 2014.
- [14] C. Metz, “CNMN Collection,” 4 May 2016. [Online]. Available: <https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/>.
- [15] S. Curtis, “Telegraph Media Group Ltd,” 13 January 2014. [Online]. Available: <http://www.telegraph.co.uk/technology/news/10568395/Instant-messaging-overtakes-texting-in-the-UK.html>.

Lampiran 2

Editor/Author Correspondence

Editor Subject: [IJASEIT] Revision Required

[DELETE](#)

2017-

10-09

11:39

AM

Guntur Maulana Zamroni:

We have reached a decision regarding your submission to International Journal on Advanced Science, Engineering and Information Technology, "Mobile Forensic Tools Evaluation for Digital Crime Investigation".

Our decision is to: Revision Required

The metadata still only 1st author, please add all of the authors in by adding more author under the first author.

Authors are MUST present their articles in the section structure:

1. INTRODUCTION
2. MATERIAL AND METHOD
3. RESULTS AND DISCUSSION
4. CONCLUSION.

Please be sure that the manuscript is up to date. It is expected that 30% of references are to recent papers (2015 - 2017).

The main references are international journals and proceeding. All references should be to the most pertinent and up-to- date sources. References are written in Vancouver style. Reference from Internet: Avoid wherever possible.

Please re-upload your revision into journal system NOT via email. Thanks


Editor

International Journal on Advanced Science, Engineering and Information Technology
<http://insightsociety.org/ijaseit/index.php/ijaseit>

Lampiran 3

PeerReview

Round 1

Review Version	3591-7608-1-RV.DOC 2017-10-04
Initiated	2017-10-26
Last modified	2018-03-31
Uploaded file	Reviewer B 3591-9142-1-RV.DOC 2017-12-11
Editor Version	None
Author Version	3591-7696-1-ED.DOC 2017-10-09  3591-7696-2-ED.DOC 2018-04-03

Mobile Forensic Tools Evaluation for Digital Crime Investigation

Rusydi Umar[#], Imam Riadi^{*}, Guntur Maulana Zamroni[#]

[#] Department of Informatics Engineering, Ahmad Dahlan University, Jl. Prof. Dr. Soepomo, Warungboto, Umbulharjo, Yogyakarta, 55164
E-mail: rusydi_umar@rocketmail.com

^{*}Department of Information System, Ahmad Dahlan University, Jl. Prof. Dr. Soepomo, Warungboto, Umbulharjo, Yogyakarta, 55164
E-mail: imam.riadi@is.uad.ac.id

[#]Department of Informatics Engineering, Ahmad Dahlan University, Jl. Prof. Dr. Soepomo, Warungboto, Umbulharjo, Yogyakarta, 55164
E-mail: gunturmz@yahoo.com

Abstract— Instant Messaging is a popular smartphone’s application. One example of Instant Messaging application is WhatsApp. WhatsApp is widely used judging from its users that reach more than 1 Billion users in January 2017. WhatsApp’s security recently has been updated with latest encryption type and technology by implementing end-to-end encryption. The number of users or possible crime target and security features in WhatsApp can lead to crime by people that have criminal intentions. Investigators need to use mobile forensic methodologies and tools for investigating smartphone and to find crime evidences. However, investigators often facing challenges during investigation because incompatibility between forensic tools and mobile technology. This research will conduct an experiment using available forensic tools with NIST forensic method for extracting latest WhatsApp’s artifacts. Forensics tools capabilities will be evaluated and compared to find its strengths and weaknesses.

Keywords— mobile forensic, whatsapp, extraction.

I. INTRODUCTION

Smartphones experience rapid development along with the development of technology. Smartphones are slowly beginning to replace the role of computers with the increasing number of features and applications available on mobile devices [1]. Trend of smartphone usage is expected to increase seen from the features offered by smartphones such as various applications, power usage, process speed, pricing, practicality and ease of carrying.

The latest generation of smartphones has the ability and power far above its predecessors that make smartphones now can be used for household activity or office work [2]. Fig. 1 shows the number of smartphone and computer device users. We can see the number of smartphone users has obtained increasing significant number compared to the number of computer users. Starting in 2014 the number of smartphone users began to outperform the number of computer users [1].

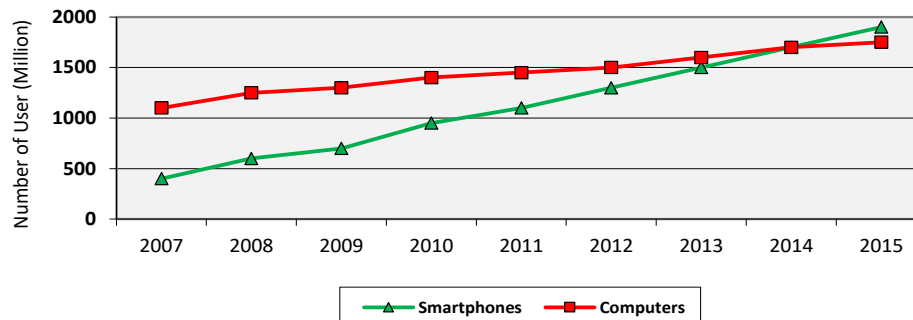


Fig. 1 Number of computer and smartphone users

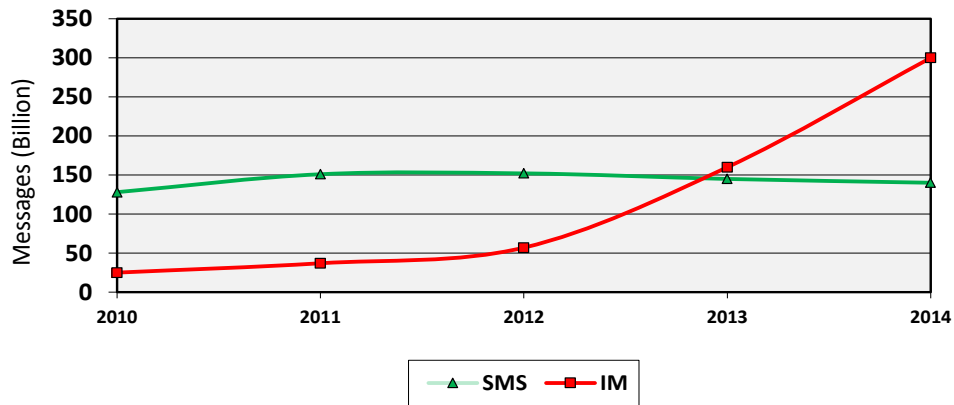


Fig. 2 Number of Messages Sent Using SMS and IM in United Kingdom

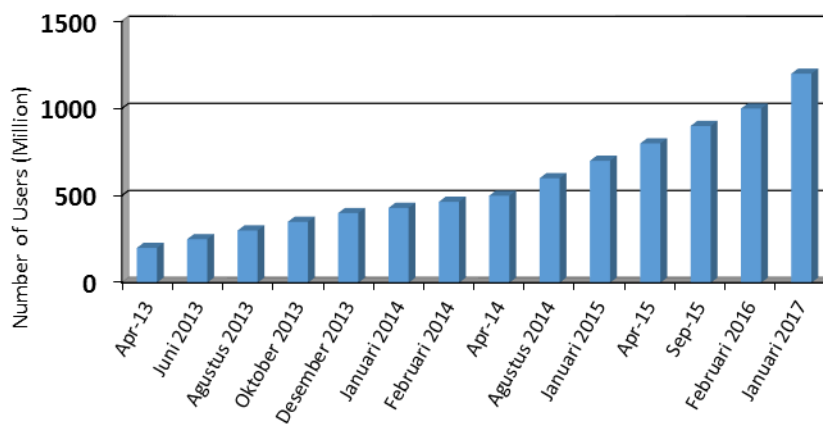


Fig. 3 Number of WhatsApp Users

The Instant Messaging (IM) application is one of the most commonly used applications for mobile device users. IM begins to replace the role of Short Message Services (SMS) to communicate through message delivery. Fig. 2 shows the trend of message delivery with SMS and IM in the UK. The number of message delivery using SMS from 2010 to 2014 tend to experience stable conditions. While the number of message delivery using IM has increased significantly starting in 2012 with the number of messages sent for 57 billion messages/year until 2014 with messages sent for 300 billion/year [3].

WhatsApp is one of the popular IM applications and is used by lots of people to communicate. Fig. 3 shows an increase in the number of WhatsApp users from 200 Million users in April 2013 to 1 Billion in February 2016 and 1.2 Billion in January 2017 [4]. According to [5], WhatsApp is a popular application with 60% of users, followed by Viber and Telegram.

WhatsApp cannot be separated from misuse as for criminal purposes. Under these circumstances the investigator will check out WhatsApp's artifact to look for evidence of a criminal offense. The case of "cyanide coffee" is one example of the case where the WhatsApp artifacts were analyzed to search for evidence in the investigation [6].

To conduct an analysis the investigator needs to use a method along with a forensically tested tools. Investigators should be able to extract the artifacts, decryption, and analyze the data contained within the mobile device to assist the investigation process because data such as conversation messages and images can be evidence [7].

References [8] conducted an analysis of forensic mobile technologies and forensic tools. Forensic analysis has several constraints such as hardware differences, security features, technological lag and forensic tool costs, anti-forensic techniques, and many other. In April 2016, WhatsApp implemented an end-to-end encryption feature that came with the latest encryption. This feature makes the sent messages to be encrypted and can only be read by those eligible to receive the message. This security feature provides difficulties and challenges for forensic investigators and analysis because the available forensics tools must be able to keep up with the development of WhatsApp technology [9].

There are several studies on mobile forensic analysis. References [10] conducted forensic analysis of Telegram, Line, and KakaoTalk applications on Android devices. They tried to conduct a forensic analysis process on unencrypted conversations and encrypted conversations. The tools used in the research were ADB (Android Debugging Bridge), SQLite

Browser, Hex Editor Neo, Busybox, Root Browser, Nandroid Backup, Shark for Root, dex2jar. References [10] used a methodology from McKemish which has 4 stages: Identification, Preservation, Analysis, and Presentation. References [10] managed to investigate unencrypted and encrypted conversations from all three applications.

References [11] attempted to perform a forensic analysis on WhatsApp version 2.11.186 which has been equipped with .crypt encryption. The tools used were WhatsApp Xtract for the extraction and decryption process, and SQLite Browser for the analysis process. The researcher succeeded in extraction and .crypt decryption.

References [12] conducted a forensic analysis on WhatsApp that has used .crypt7 encryption. The tools used in the research were ADB, WhatsApp Key/DB Extractor 2.2, WhatsApp Viewer, WhatsApp Extract, dan SQLite Spy. Researchers managed to extract and decrypt WhatsApp artifacts. Researchers reminded about the importance of paying attention to the development and changes in mobile technology to be able to perform forensic analysis.

References [13] evaluated and compared 2 forensic methodologies, ISO/IEC methodology and NIST methodology. Ajijola, et al concluded that there is no methodology covering all forensic issues. The ISO/IEC methodology has advantages over non-technical processes and problems. NIST has the advantage of selecting and using forensic tools. Each methodology needs to be constantly updated following the development of digital technology.

Looking at the background, the dynamics of mobile technology, previous research, and mobile forensic challenges, researchers will try to conduct comparative evaluation forensic tools that serve to extract artifacts in the form of messages, images, videos and documents with NIST forensic methodology in the latest version of WhatsApp in Android-based devices. The tools used are ADB, WhatsApp Key/DB Extractor 4.7, and Belkasoft Evidence (trial version). Forensic tools are tested to run the WhatsApp database extraction and decryption process that has been updated with .crypt12 end-to-end encryption. The results of extraction, decryption, and validation of forensic tools will be compared in order to have the conclusions.

II. MATERIAL AND METHOD

The purpose of this research was to evaluate and compare the Belkasoft Evidence (trial version) and WhatsApp Key/DB Extractor forensic tools, especially in terms of the extraction capabilities of the latest WhatsApp artifacts on Android-based devices that have used .crypt12 encryption.

A. Research Steps

This research used a research step made by the National Institute of Stanford and Technology [7]. The NIST research stage consists of 4 stages as in Fig. 4.

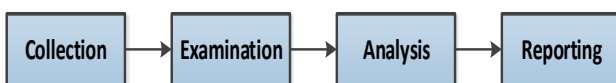


Fig. 4 NIST Forensic Methodology

- 1) *Collection*: In the collection stage, there will be the acquisition of evidence, preservation of evidence, preparation of objects and research tools.
- 2) *Examination*: At the examination stage, there will be process of identifying data that can be used as evidence. After determining which data will be taken, the data retrieval process will be done in a forensically tested way.
- 3) *Analysis*: The data which have been taken will be analyzed to look for things that can be used as evidence and then conclusion will be taken
- 4) *Reporting*: The last stage of the forensic step is to report forensic activity from beginning to the end along with the results of the analysis into the form of a written report or oral report.

This research focused on the examination stage. The examination stage is further elaborated into several stages as in Fig. 5. Identification is done to find data or artifacts to be taken and possibly produce evidence to assist investigation. After determining the data or artifacts to be taken, it will proceed to the data retrieval process.

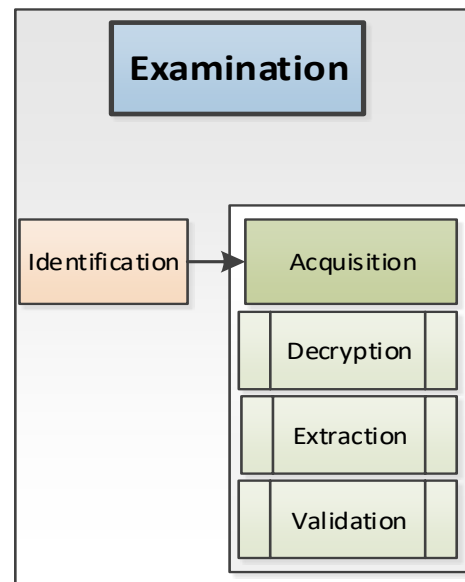


Fig. 5 Steps of Examination

WhatsApp has been equipped with an encryption feature that aims to hide messages [14]. This encryption feature can interfere with the investigation process. Therefore, a tool that can perform decryption and data extraction is needed. Validation using repeatability and reproducibility according to the NIST method will be performed to ensure that the results of the extraction process performed are correct and there is no data manipulation. Repeatability is done by repeated extraction processes in time adjacent to the same object and forensic tool. While reproducibility is done by using the same object but with different forensic tools.

B. Research Tools

The hardware and software used to experiment on the extraction of WhatsApp artifacts from an Android-based device can be seen in Table 1.

TABLE I
RESEARCH TOOLS AND DEVICES

No.	Tool and Device	Information
1	Samsung Galaxy S4 GT-I9500 with 5.0.1 Lollipop operation system	Smartphone device for experiment
2	WhatsApp ver. 2.17.147	Instant Messaging application
3	Workstation with operational system of Windows 7 64 Bit, Intel i5-4440, 4,00 GB	Computer device for extraction and analysis
4	USB Cable	USB connector to connect smartphone device and computer
5	Android Debugging Bridge	Software to support a communication between smartphone and computer
6	WhatsApp Key/DB Extractor 4.7	Extraction tool
7	Belkasoft Evidence (ver trial)	Extraction and analysis tool
8	SQLite Studio	Analysis tool

C. Experiment Simulation

The experiments were conducted in a closed and noise free condition, meaning that the smartphone device was changed to Airplane Mode. With Airplane Mode the device will not be able to receive outside calls and messaging. This is important to maintain the authenticity and integrity of the data. The workstations used are not connected to the Internet and are free from malware that may influence the results of the experiment.

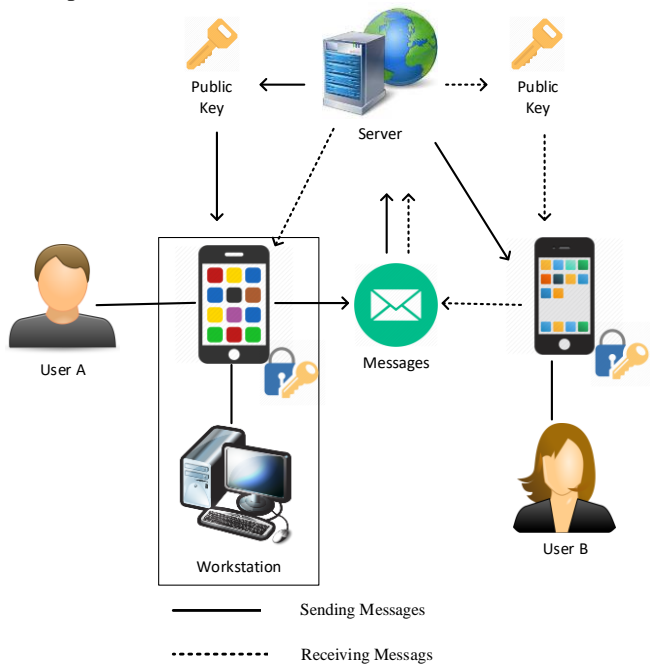


Fig. 6 Experiment Simulation

Fig. 6 describes the simulation of the experimental tool. To send a message to User B, User A will request a public key on the server which will then be used for message encryption. User B then uses the private key to decrypt the message.

User A's Smartphone will be used for forensic analysis. Smartphones with the Android 5.0.1 operating system and WhatsApp 2.17.147 are used for everyday activities such as sending and receiving messages, pictures, videos, and documents which will be connected using a USB cable with workstations that use Windows 64 Bits, ADB, WhatsApp Key/DB Extractor 4.7, and Belkasoft Evidence. Each forensic tools will conduct extraction process twice to ensure the validity of forensic tools.

III. RESULTS AND DISCUSSION

A. Extraction results using Belkasoft Evidence

In experiments conducted using Belkasoft Evidence (trial ver) the message artifact of WhatsApp text was not obtained, but video, image, and document artifacts were successfully obtained. Information about the video artifact can be seen in the properties column. Belkasoft provides video file information such as file name, file size, and access date. The size of the extracted video file has different video pixel duration and size according to the original file on the smartphone. Video artifacts can be played and viewed so that it is helpful in the investigation process in the search of evidence as described in Fig. 7. Image artifacts can be zoomed to see clearer images and help with double clicking as well as displaying information from image files such as filename, access date, pixel size, and file size as in Fig. 8. The pixel size and file size of the image artifact match the original size of the original file on the smartphone.

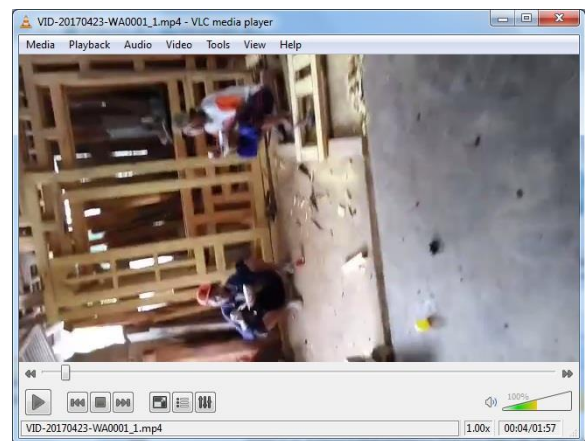


Fig. 7 Video artifact detail of Belkasoft Evidence

Metadata information from documents such as creator's name, software used, file name, and file size can be known. The document artifact can be opened so that the investigator can see the contents of the document.

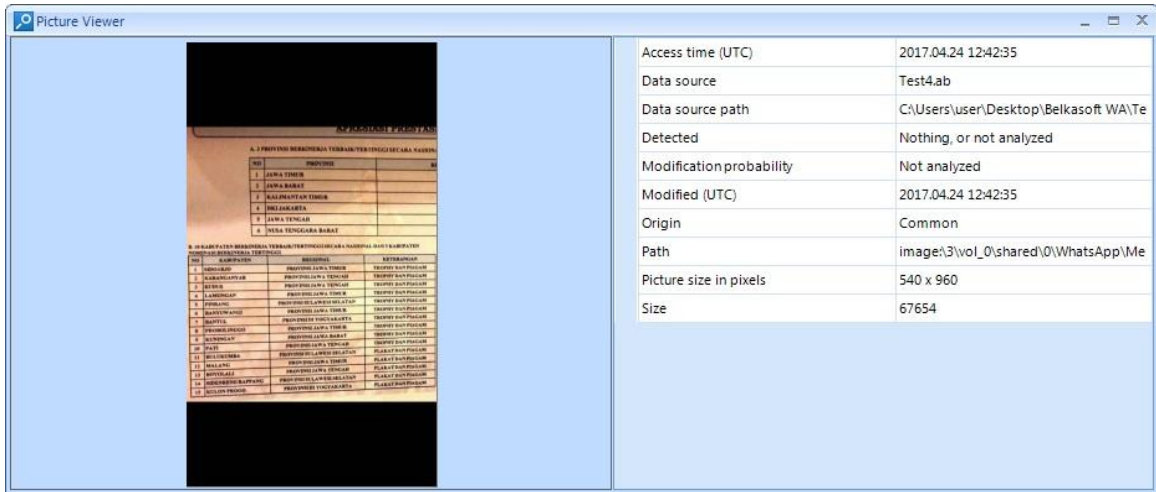


Fig. 8 Picture artifact detail of Belkasoft Evidence

B. Extraction results using WhatsApp Key/DB Extractor

WhatsApp Key / DB Extractor only manages to get text message artifacts and images. No video and document artifacts were found. Fig. 9 shows the text message artifacts that were successfully obtained. The text message artifact is in the file "msgstore.db".

Information such as message sender, message recipient, message content, time of sending or receiving messages, and file attachment can be known. Such information will be very useful in the investigation process. WhatsApp Key/DB Extractor manage to get the existing group information in WhatsApp. Groups' name and members can be found in the artefact. WhatsApp Key / DB Extractor manages to get the entire contact WhatsApp information in the "wa.db" file

artifact. Contact artifacts are opened by using SQLite Studio as shown in Fig. 10. Contact details such as phone numbers and contact names are known.

The image artifact is obtained using the WhatsApp Key/DB Extractor. Just like Belkasoft Evidence, WhatsApp Key/DB Extractor also shows information from image files such as filename, access date, pixel size, and file size. The image can be zoomed by double click but the zoomed image will break as shown in Fig. 11. This is because the pixel size of the image obtained only measures 56 x 100 pixels or in accordance with the thumbnail size in WhatsApp. The size applies to all extracted images using WhatsApp Key/DB Extractor.

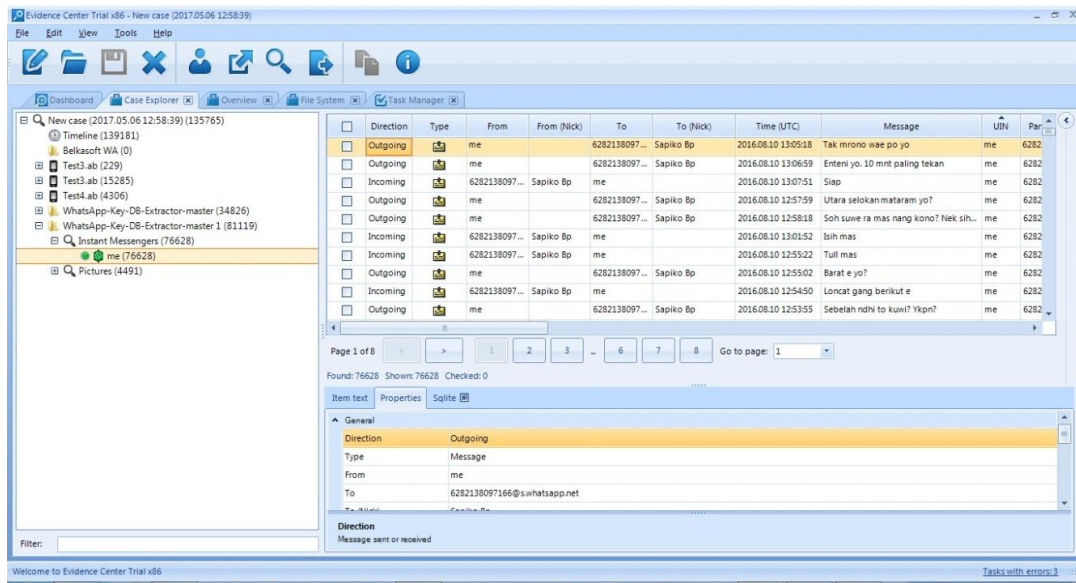


Fig. 9 WhatsApp Key/DB Extractor Message Artifact

status_timestamp	number	raw_contact_jd	display_name
0	0222531	997	MM itb
1473441122000	0822207	1956	Tornado Nano Seller
0	+628386	2333	Calon Koki 11
0	+622749	1111	Yusuf servis ac
1430971391000	+628574	889	Didit
1423072923000	+628574	846	Arif net
1471952553000	+628572	1850	Jogjaringan Isp
0	+628389	1040	Rahmat net no laen
0	+601393	835	Alif Arena
1478700523000	0813254	1071	Seller char ao twinbrother
0	+601766	837	Alwi Skate
0	0878392	1901	Yanto Buang Material
1478973985000	+601690	1097	Wawan Setiawan
1464963504000	0857439	1023	Pak raharjo instalasi listrik
0	+628520	986	Mbak pipit pakdhe kelik
1470224229000	+628157	909	Fauzan Tehnisi
1410859388000	0857299	1826	Magma Seller
0	0856433	961	Mas Bejo roti bakar
0	0274563	1940	Univ Ahmad Dahlan
1464188106000	0858787	900	Dwi servis ac stikes
0	0877382	916	Gunawan atlantica onlen joki jogja
1478792857000	+628577	1996	Mas Oji Jkt
1478006823000	+628128	981	Mbak Mega
0	0857763	895	DN indo joki

Fig. 10 WhatsApp Contact List Artifact

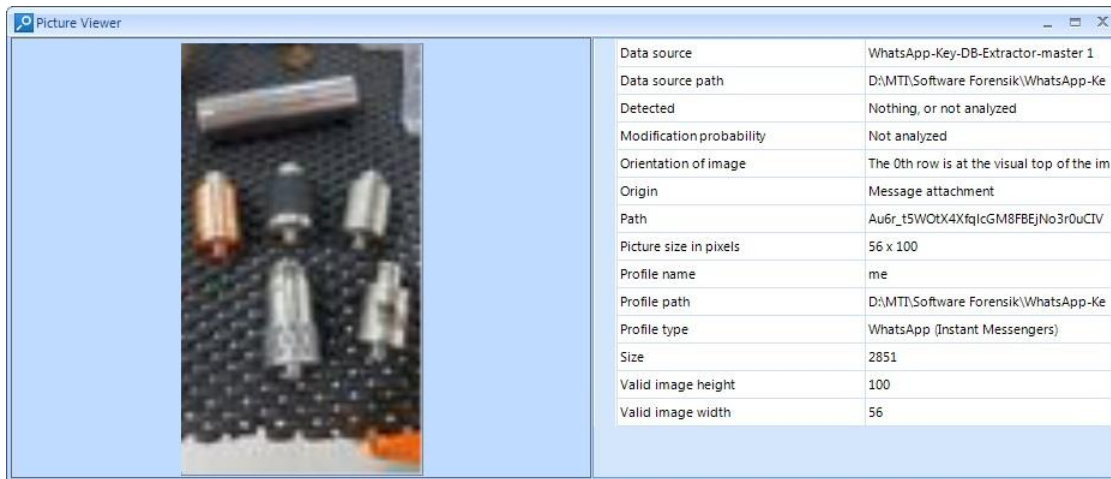


Fig. 11 WhatsApp Key/DB Extractor Picture Detail

C. Discussion

Table 2 shows the artifacts obtained. WhatsApp Key / DB Extractor only manages to extract text message and images artifacts. Message information such as message body, message recipient, message sender, chat group, chat group participant, all contacts on WhatsApp either name or phone number is successfully obtained. This is certainly very useful in helping the investigation process to look for evidence of crime. WhatsApp Key/DB Extractor managed to get the image artifact, but in size of 56 x 100 pixels.

TABLE III
FORENSIC TOOLS COMPARISON

Artifact Type	Belkasoft Evidence (trial ver)	WhatsApp Key/DB Extractor
Text Message	-	√
Image	√	√
Video	√	-
Document	√	-

Unlike the WhatsApp Key/DB Extractor, Belkasoft Evidence (trial ver) manages to get images, video and document artifacts. Image artifacts obtained using Belkasoft Evidence (trial ver) have better quality than WhatsApp Key/DB Extractor artifacts. Belkasoft Evidence (trial ver) does not get text message artifacts.

The extraction results using Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor are repeated to ensure the similarity of the results obtained. This needs to be done to test the validation of results from forensic tools according to the NIST method. Table 3 and Table 4 shows the number of artifacts obtained using Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor. Experiments conducted using Belkasoft Evidence (trial ver) resulted in the same number of artifacts as shown in Table 3. Table 4 shows the number of artifacts obtained using WhatsApp Key/DB Extractor.

TABLE III
BELKASOFT EVIDENCE (TRIAL VER) ARTIFACTS COMPARISON

Artifact Type	Belkasoft Evidence (trial ver) 1 st Extraction	Belkasoft Evidence (trial ver) 2 nd Extraction
Text Message	-	-
Image	2086	2086
Video	43	43
Document	26	26

TABLE IV
WHATSAPP KEY/DB EXTRACTOR ARTIFACTS COMPARISON

Artifact Type	WhatsApp Key/DB Extractor 1 st Extraction	WhatsApp Key/DB Extractor 2 nd Extraction
Text Message	44	44
Image	3	3
Video	-	-
Document	-	-

From the validation test result, both Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor meet validation test of repeatability and reproducibility as in Table 5. Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor are conducted to perform extraction twice to check repeatability test. Both Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor meet repeatability test since each tools' tests have the same number of artifacts. Although the number of artifacts from each forensic tools are different, Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor meet reproducibility test because same image files are found in both artifacts from each forensic tools.

TABLE V
FORENSIC TOOLS VALIDATION

Tools Validation	Belkasoft Evidence (trial ver)	WhatsApp Key/DB Extractor
Repeatable	√	√
Reproducible	√	√

IV. CONCLUSION

Based on the results of testing conducted on WhatsApp 2.17.147 with .crypt12 encryption, Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor meet validation test of repeatability and reproducibility. WhatsApp Key/DB Extractor dominates in the extraction ability of text message artifacts. Belkasoft Evidence (trial ver) has advantages in extraction abilities for images, videos, and documents. Further research on WhatsApp artifact extraction abilities in non-Android platforms needs to be done considering the WhatsApp application is available for many platforms.

REFERENCES

- [1] Chaffey D. Smart Insight Marketing Intelligence Ltd. [Online]; 2017. Available from: <http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/> HYPERLINK
- [2] Curtis S. The Telegraph. [Online]; 2014. Available from: <http://www.telegraph.co.uk/technology/news/10568395/Instant-messaging-overtakes-texting-in-the-UK.html> HYPERLINK
- [3] Garratt L, Poulter S. Daily Mail Online. [Online]; 2014. Available from: <http://www.dailymail.co.uk/sciencetech/article-2538488/SMS-takes-seat-IM-number-texts-sent-Britain-falls-time.html> HYPERLINK
- [4] Gudipaty LP, Jhala KY. WhatsApp Forensics: Decryption of Encrypted WhatsApp Databases on Non Rooted Android Devices. Journal Information Technology & Software Engineering. 2015; 5(2).
- [5] Koum J, Acton B. WhatsApp. [Online]; 2016. Available from: <https://blog.whatsapp.com/10000618/end-to-end-encryption> HYPERLINK
- [6] Kusumadewi A, Sasongko JP. CNN Indonesia. [Online]; 2016. Available from: <http://www.cnnindonesia.com/nasional/20160121080758-12-105715/polisi-usut-percakapan-jessica-mirna-yang-beredar-di-sosmed/> HYPERLINK
- [7] Metz C. Wired. [Online]; 2016. Available from: <https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/> HYPERLINK
- [8] Sahu S. An Analysis of WhatsApp Forensics in Android Smartphones. International Journal of Engineering Research. 2014 May 1; 3(5): p. 349-350.
- [9] Sai D, Prasad NR, Dekka S. The Forensics Process Analysis of Mobile Device. International Journal of Computer Science and Information Technology. 2015; 6(5): p. 4847-4850.
- [10] Satrya GB, Daely PT, Shin SY. Android Forensics Analysis: Private Chat on Social Messenger. IT Convergence Engineering. 2016.
- [11] Statista. [Online]; 2017. Available from: <https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/> HYPERLINK
- [12] Sutikno T, Handayani L, Stiawan D, Riyadi AR, Subroto IM. WhatsApp, Viber and Telegram: which is the Best for Instant Messaging? International Journal of Electrical and Computer Engineering. 2016 June; 6(3): p. 909-914.
- [13] Bonnington C. Wired. [Online]; 2015. Available from: <https://www.wired.com/2015/02/smartphone-only-computer/> HYPERLINK
- [14] Ajijola A, Zavorsky P, Ruhl R. A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101. In World Congress on Internet Security; 2014: Institute of Electrical and Electronics.
- [15] Ayers R, Brothers S, Jansen W. Guidelines on Mobile Device Forensics. , Department of Commerce; 2014.
- [16] Cankaya EC, Kupka B. A Survey of Digital Forensics Tools for Database Extraction. In Future Technologies Conference; 2016; San Francisco: IEEE. p. 1014-1019.
- [17] Dogan S, Akbal E. Analysis of Mobile Phones in Digital Forensics. In MIPRO; 2017; Opatija. p. 1241-1244.

Lampiran 4

Editor Subject: [IJASEIT] Revision Required

[DELETE](#)

2018-
03-31
11:44
AM

Guntur Maulana Zamroni:

We have reached a decision regarding your submission to International Journal on Advanced Science, Engineering and Information Technology, "Mobile Forensic Tools Evaluation for Digital Crime Investigation".

Our decision is to: Revision Required

Editor

Reviewer B:

See attach file (login into journal system)


International Journal on Advanced Science, Engineering and Information Technology
<http://insightsociety.org/ijaseit/index.php/ijaseit>

Close

Lampiran 5

PeerReview

Round 1

Review Version	3591-7608-1-RV.DOC 2017-10-04
Initiated	2017-10-26
Last modified	2018-03-31
Uploaded file	Reviewer B 3591-9142-1-RV.DOC 2017-12-11
Editor Version	None
Author Version	3591-7696-1-ED.DOC 2017-10-09 3591-7696-2-ED.DOC 2018-04-03 

Mobile Forensic Tools Evaluation for Digital Crime Investigation

Rusydi Umar[#], Imam Riadi^{*}, Guntur Maulana Zamroni[#]

[#] Department of Informatics Engineering, Ahmad Dahlan University, Jl. Prof. Dr. Soepomo, Warungboto, Umbulharjo, Yogyakarta, 55164
E-mail: rusydi_umar@rocketmail.com

^{*}Department of Information System, Ahmad Dahlan University, Jl. Prof. Dr. Soepomo, Warungboto, Umbulharjo, Yogyakarta, 55164
E-mail: 1

[#]Department of Informatics Engineering, Ahmad Dahlan University, Jl. Prof. Dr. Soepomo, Warungboto, Umbulharjo, Yogyakarta, 55164
E-mail: gunturmz@yahoo.com

Abstract— Instant Messaging is a popular smartphone’s application. One example of Instant Messaging application is WhatsApp. WhatsApp is widely used judging from its users that reach more than 1 Billion users in January 2017. WhatsApp’s security recently has been updated with latest encryption type and technology by implementing end-to-end encryption. The number of users or possible crime target and security features in WhatsApp can lead to crime by people that have criminal intentions. Investigators need to use mobile forensic methodologies and tools for investigating smartphone and to find crime evidences. However, investigators often facing challenges during investigation because incompatibility between forensic tools and mobile technology. This research will conduct an experiment using available forensic tools with NIST forensic method for extracting latest WhatsApp’s artifacts. Forensics tools capabilities will be evaluated and compared to find its strengths and weaknesses.

Keywords— mobile forensic, whatsapp, extraction.

I. INTRODUCTION

Smartphones experience rapid development along with the development of technology. Smartphones are slowly beginning to replace the role of computers with the increasing number of features and applications available on mobile devices [1]. Trend of smartphone usage is expected to increase seen from the features offered by smartphones such as various applications, power usage, process speed, pricing, practicality and ease of carrying.

The latest generation of smartphones has the ability and power far above its predecessors that make smartphones now can be used for household activity or office work [2]. Fig. 1 shows the number of smartphone and computer device users. We can see the number of smartphone users has obtained increasing significant number compared to the number of computer users. Starting in 2014 the number of smartphone users began to outperform the number of computer users [1].

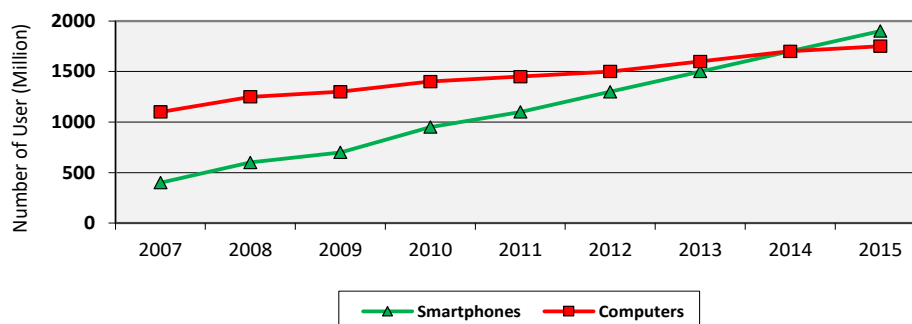


Fig. 1 Number of computer and smartphone users

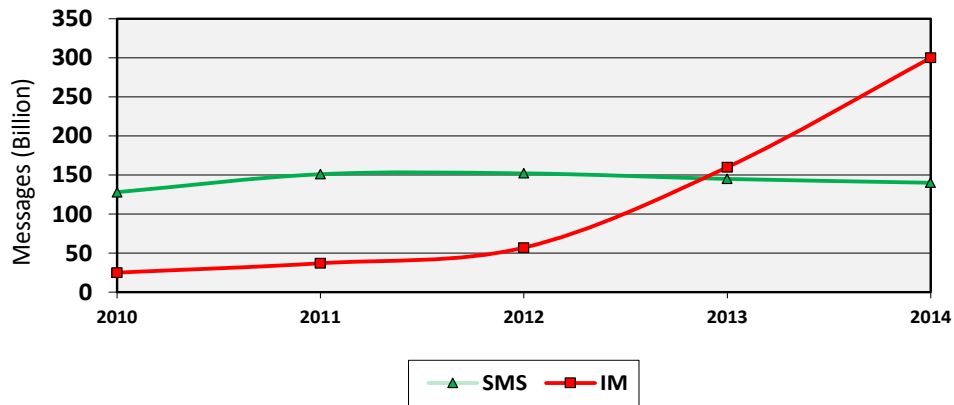


Fig. 2 Number of Messages Sent Using SMS and IM in United Kingdom

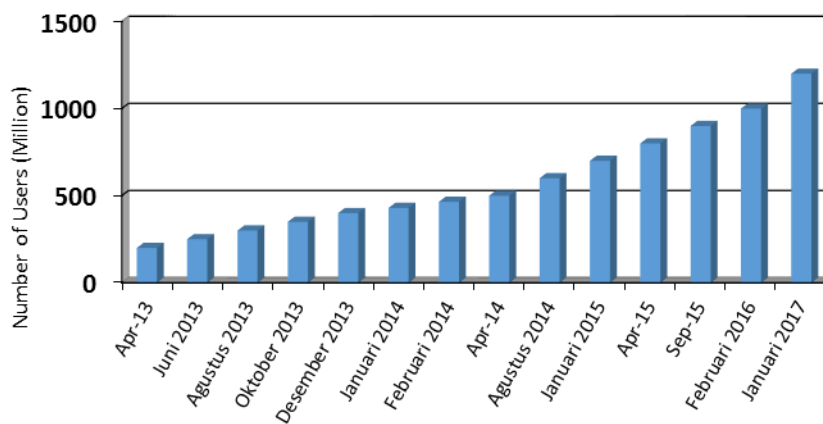


Fig. 3 Number of WhatsApp Users

The Instant Messaging (IM) application is one of the most commonly used applications for mobile device users. IM begins to replace the role of Short Message Services (SMS) to communicate through message delivery. Fig. 2 shows the trend of message delivery with SMS and IM in the UK. The number of message delivery using SMS from 2010 to 2014 tend to experience stable conditions. While the number of message delivery using IM has increased significantly starting in 2012 with the number of messages sent for 57 billion messages/year until 2014 with messages sent for 300 billion/year [3].

WhatsApp is one of the popular IM applications and is used by lots of people to communicate. Fig. 3 shows an increase in the number of WhatsApp users from 200 Million users in April 2013 to 1 Billion in February 2016 and 1.2 Billion in January 2017 [4]. According to [5], WhatsApp is a popular application with 60% of users, followed by Viber and Telegram.

WhatsApp cannot be separated from misuse as for criminal purposes. Under these circumstances the investigator will check out WhatsApp's artifact to look for evidence of a criminal offense. The case of "cyanide coffee" is one example of the case where the WhatsApp artifacts were analyzed to search for evidence in the investigation [6].

To conduct an analysis the investigator needs to use a method along with a forensically tested tools. Investigators should be able to extract the artifacts, decryption, and analyze the data contained within the mobile device to assist the investigation process because data such as conversation messages and images can be evidence [7].

References [8] conducted an analysis of forensic mobile technologies and forensic tools. Forensic analysis has several constraints such as hardware differences, security features, technological lag and forensic tool costs, anti-forensic techniques, and many other. In April 2016, WhatsApp implemented an end-to-end encryption feature that came with the latest encryption. This feature makes the sent messages to be encrypted and can only be read by those eligible to receive the message. This security feature provides difficulties and challenges for forensic investigators and analysis because the available forensics tools must be able to keep up with the development of WhatsApp technology [9].

There are several studies on mobile forensic analysis. References [10] conducted forensic analysis of Telegram, Line, and KakaoTalk applications on Android devices. They tried to conduct a forensic analysis process on unencrypted conversations and encrypted conversations. The tools used in the research were ADB (Android Debugging Bridge), SQLite

Browser, Hex Editor Neo, Busybox, Root Browser, Nandroid Backup, Shark for Root, dex2jar. References [10] used a methodology from McKemish which has 4 stages: Identification, Preservation, Analysis, and Presentation. References [10] managed to investigate unencrypted and encrypted conversations from all three applications.

References [11] attempted to perform a forensic analysis on WhatsApp version 2.11.186 which has been equipped with .crypt encryption. The tools used were WhatsApp Xtract for the extraction and decryption process, and SQLite Browser for the analysis process. The researcher succeeded in extraction and .crypt decryption.

References [12] conducted a forensic analysis on WhatsApp that has used .crypt7 encryption. The tools used in the research were ADB, WhatsApp Key/DB Extractor 2.2, WhatsApp Viewer, WhatsApp Extract, dan SQLite Spy. Researchers managed to extract and decrypt WhatsApp artifacts. Researchers reminded about the importance of paying attention to the development and changes in mobile technology to be able to perform forensic analysis.

References [13] evaluated and compared 2 forensic methodologies, ISO/IEC methodology and NIST methodology. Ajijola, et al concluded that there is no methodology covering all forensic issues. The ISO/IEC methodology has advantages over non-technical processes and problems. NIST has the advantage of selecting and using forensic tools. Each methodology needs to be constantly updated following the development of digital technology.

Looking at the background, the dynamics of mobile technology, previous research, and mobile forensic challenges, researchers will try to conduct comparative evaluation forensic tools that serve to extract artifacts in the form of messages, images, videos and documents with NIST forensic methodology in the latest version of WhatsApp in Android-based devices. The tools used are ADB, WhatsApp Key/DB Extractor 4.7, and Belkasoft Evidence (trial version). Forensic tools are tested to run the WhatsApp database extraction and decryption process that has been updated with .crypt12 end-to-end encryption. The results of extraction, decryption, and validation of forensic tools will be compared in order to have the conclusions.

II. MATERIAL AND METHOD

The purpose of this research was to evaluate and compare the Belkasoft Evidence (trial version) and WhatsApp Key/DB Extractor forensic tools, especially in terms of the extraction capabilities of the latest WhatsApp artifacts on Android-based devices that have used .crypt12 encryption.

A. Research Steps

This research used a research step made by the National Institute of Stanford and Technology [7]. The NIST research stage consists of 4 stages as in Fig. 4.

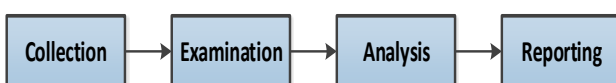


Fig. 4 NIST Forensic Methodology

- 1) *Collection*: In the collection stage, there will be the acquisition of evidence, preservation of evidence, preparation of objects and research tools.
- 2) *Examination*: At the examination stage, there will be process of identifying data that can be used as evidence. After determining which data will be taken, the data retrieval process will be done in a forensically tested way.
- 3) *Analysis*: The data which have been taken will be analyzed to look for things that can be used as evidence and then conclusion will be taken
- 4) *Reporting*: The last stage of the forensic step is to report forensic activity from beginning to the end along with the results of the analysis into the form of a written report or oral report.

This research focused on the examination stage. The examination stage is further elaborated into several stages as in Fig. 5. Identification is done to find data or artifacts to be taken and possibly produce evidence to assist investigation. After determining the data or artifacts to be taken, it will proceed to the data retrieval process.

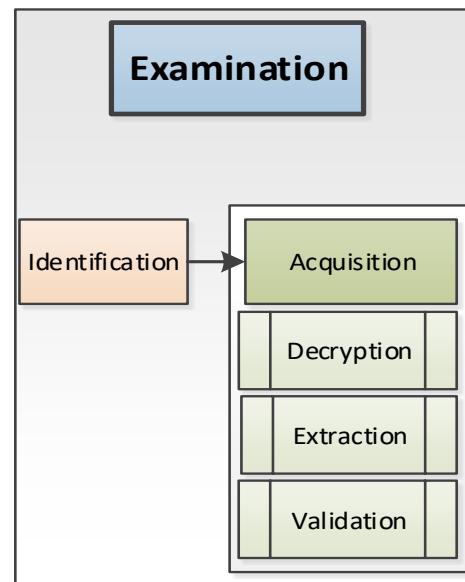


Fig. 5 Steps of Examination

WhatsApp has been equipped with an encryption feature that aims to hide messages [14]. This encryption feature can interfere with the investigation process. Therefore, a tool that can perform decryption and data extraction is needed. Validation using repeatability and reproducibility according to the NIST method will be performed to ensure that the results of the extraction process performed are correct and there is no data manipulation. Repeatability is done by repeated extraction processes in time adjacent to the same object and forensic tool. While reproducibility is done by using the same object but with different forensic tools.

B. Research Tools

The hardware and software used to experiment on the extraction of WhatsApp artifacts from an Android-based device can be seen in Table 1.

TABLE I
RESEARCH TOOLS AND DEVICES

No.	Tool and Device	Information
1	Samsung Galaxy S4 GT-I9500 with 5.0.1 Lollipop operation system	Smartphone device for experiment
2	WhatsApp ver. 2.17.147	Instant Messaging application
3	Workstation with operational system of Windows 7 64 Bit, Intel i5-4440, 4,00 GB	Computer device for extraction and analysis
4	USB Cable	USB connector to connect smartphone device and computer
5	Android Debugging Bridge	Software to support a communication between smartphone and computer
6	WhatsApp Key/DB Extractor 4.7	Extraction tool
7	Belkasoft Evidence (ver trial)	Extraction and analysis tool
8	SQLite Studio	Analysis tool

C. Experiment Simulation

The experiments were conducted in a closed and noise free condition, meaning that the smartphone device was changed to Airplane Mode. With Airplane Mode the device will not be able to receive outside calls and messaging. This is important to maintain the authenticity and integrity of the data. The workstations used are not connected to the Internet and are free from malware that may influence the results of the experiment.

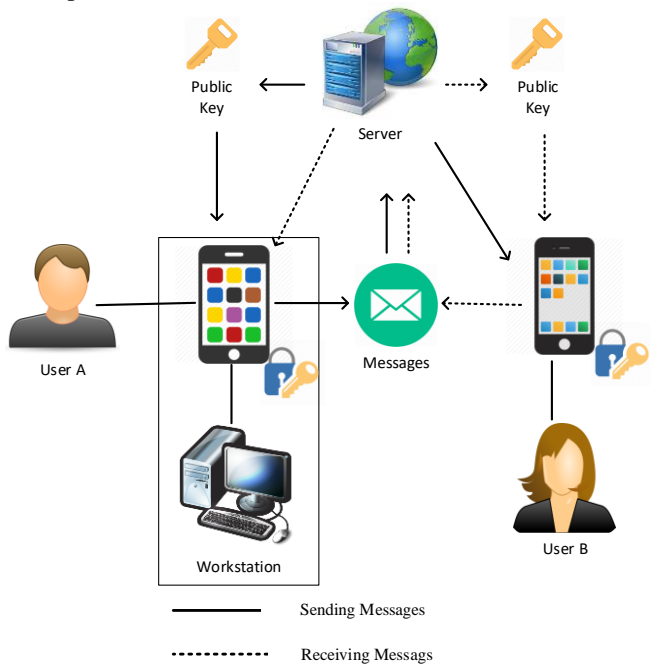


Fig. 6 Experiment Simulation

Fig. 6 describes the simulation of the experimental tool. To send a message to User B, User A will request a public key on the server which will then be used for message encryption. User B then uses the private key to decrypt the message.

User A's Smartphone will be used for forensic analysis. Smartphones with the Android 5.0.1 operating system and WhatsApp 2.17.147 are used for everyday activities such as sending and receiving messages, pictures, videos, and documents which will be connected using a USB cable with workstations that use Windows 64 Bits, ADB, WhatsApp Key/DB Extractor 4.7, and Belkasoft Evidence. Each forensic tools will conduct extraction process twice to ensure the validity of forensic tools.

III. RESULTS AND DISCUSSION

A. Extraction results using Belkasoft Evidence

In experiments conducted using Belkasoft Evidence (trial ver) the message artifact of WhatsApp text was not obtained, but video, image, and document artifacts were successfully obtained. Information about the video artifact can be seen in the properties column. Belkasoft provides video file information such as file name, file size, and access date. The size of the extracted video file has different video pixel duration and size according to the original file on the smartphone. Video artifacts can be played and viewed so that it is helpful in the investigation process in the search of evidence as described in Fig. 7. Image artifacts can be zoomed to see clearer images and help with double clicking as well as displaying information from image files such as filename, access date, pixel size, and file size as in Fig. 8. The pixel size and file size of the image artifact match the original size of the original file on the smartphone.

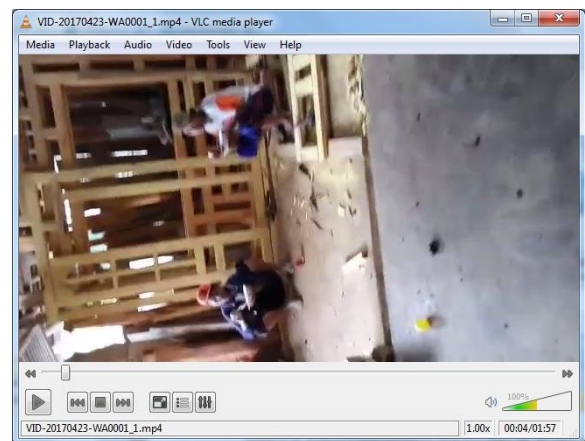


Fig. 7 Video artifact detail of Belkasoft Evidence

Metadata information from documents such as creator's name, software used, file name, and file size can be known. The document artifact can be opened so that the investigator can see the contents of the document.

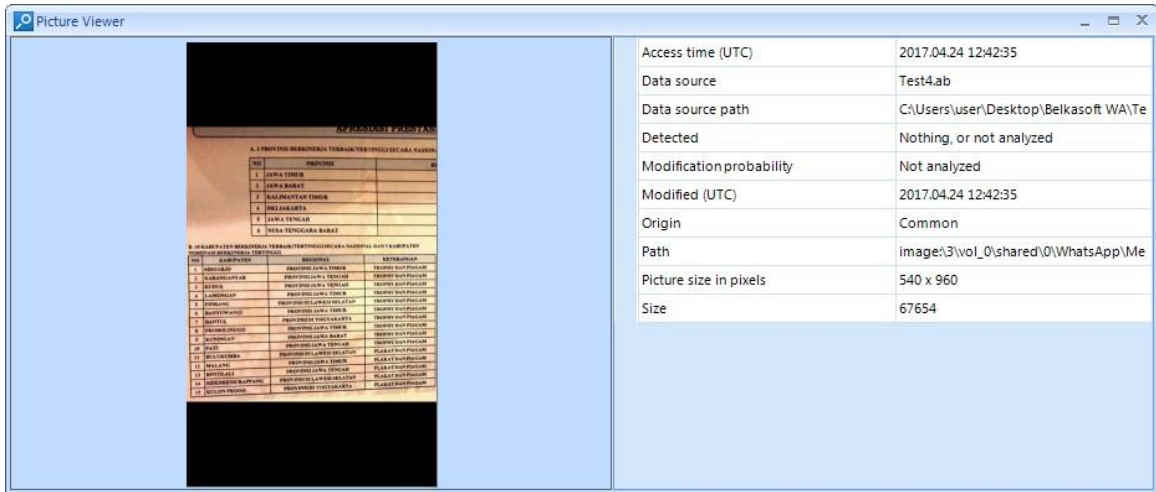


Fig. 8 Picture artifact detail of Belkasoft Evidence

B. Extraction results using WhatsApp Key/DB Extractor

WhatsApp Key / DB Extractor only manages to get text message artifacts and images. No video and document artifacts were found. Fig. 9 shows the text message artifacts that were successfully obtained. The text message artifact is in the file "msgstore.db".

Information such as message sender, message recipient, message content, time of sending or receiving messages, and file attachment can be known. Such information will be very useful in the investigation process. WhatsApp Key/DB Extractor manage to get the existing group information in WhatsApp. Groups' name and members can be found in the artefact. WhatsApp Key / DB Extractor manages to get the entire contact WhatsApp information in the "wa.db" file

artifact. Contact artifacts are opened by using SQLite Studio as shown in Fig. 10. Contact details such as phone numbers and contact names are known.

The image artifact is obtained using the WhatsApp Key/DB Extractor. Just like Belkasoft Evidence, WhatsApp Key/DB Extractor also shows information from image files such as filename, access date, pixel size, and file size. The image can be zoomed by double click but the zoomed image will break as shown in Fig. 11. This is because the pixel size of the image obtained only measures 56 x 100 pixels or in accordance with the thumbnail size in WhatsApp. The size applies to all extracted images using WhatsApp Key/DB Extractor.

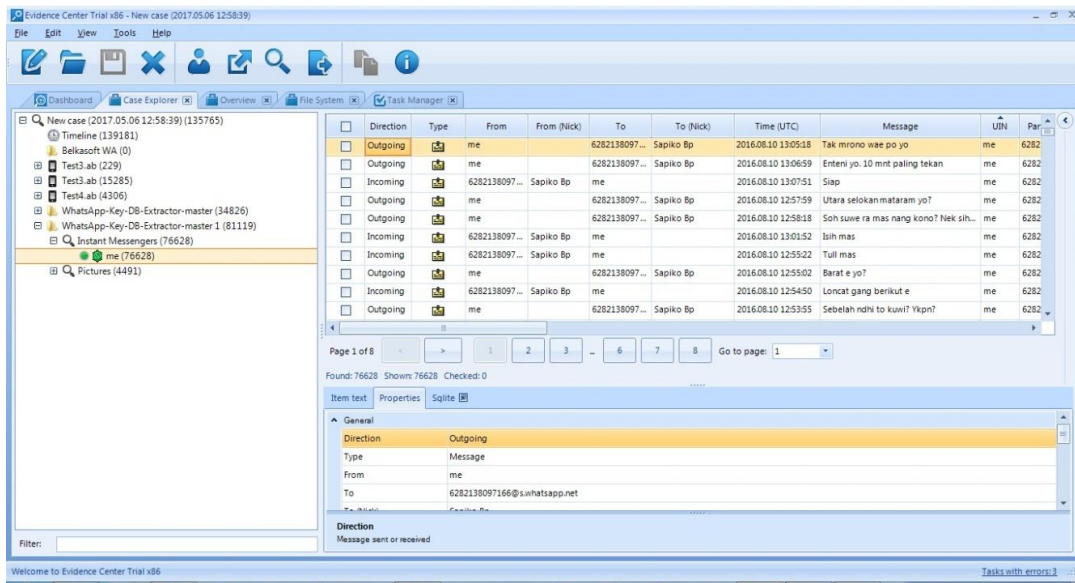


Fig. 9 WhatsApp Key/DB Extractor Message Artifact

status_timestamp	number	raw_contact_jd	display_name
0	0222531	997	MM itb
1473441122000	0822207	1956	Tornado Nano Seller
0	+628386	2333	Calon Koki 11
0	+622749	1111	Yusuf servis ac
1430971391000	+628574	889	Didit
1423072923000	+628574	846	Arif net
1471952553000	+628572	1850	Jogjaringan Isp
0	+628389	1040	Rahmat net no laen
0	+601393	835	Alif Arena
1478700523000	0813254	1071	Seller char ao twinbrother
0	+601766	837	Alwi Skate
0	0878392	1901	Yanto Buang Material
1478973985000	+601690	1097	Wawan Setiawan
1464963504000	0857439	1023	Pak raharjo instalasi listrik
0	+628520	986	Mbak pipit pakdhe kelik
1470224229000	+628157	909	Fauzan Tehnisi
1410859388000	0857299	1826	Magma Seller
0	0856433	961	Mas Bejo roti bakar
0	0274563	1940	Univ Ahmad Dahlan
1464188106000	0858787	900	Dwi servis ac stikes
0	0877382	916	Gunawan atlantica onlen joki jogja
1478792857000	+628577	1996	Mas Oji Jkt
1478006823000	+628128	981	Mbak Mega
0	0857763	895	DN indo joki

Fig. 10 WhatsApp Contact List Artifact

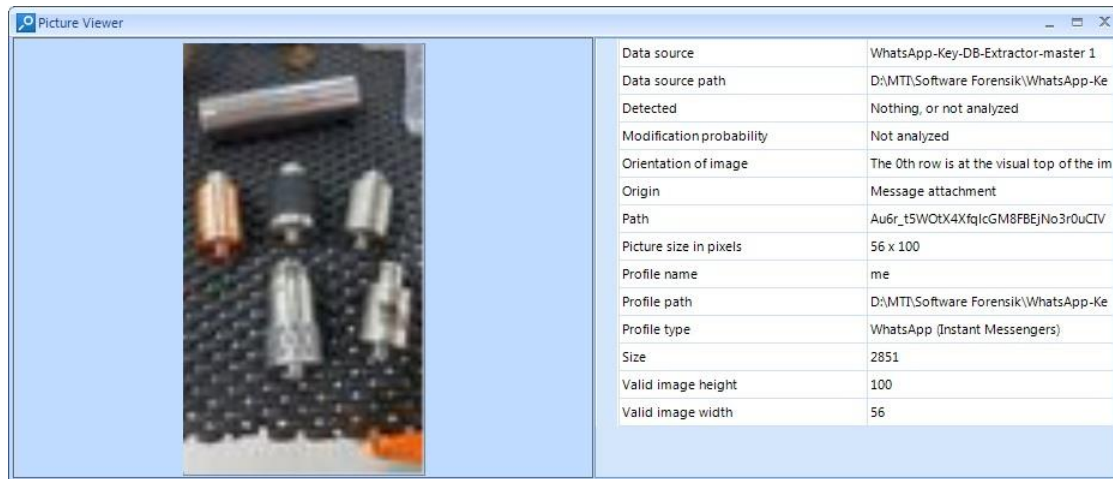


Fig. 11 WhatsApp Key/DB Extractor Picture Detail

C. Discussion

Table 2 shows the artifacts obtained. WhatsApp Key / DB Extractor only manages to extract text message and images artifacts. Message information such as message body, message recipient, message sender, chat group, chat group participant, all contacts on WhatsApp either name or phone number is successfully obtained. This is certainly very useful in helping the investigation process to look for evidence of crime. WhatsApp Key/DB Extractor managed to get the image artifact, but in size of 56 x 100 pixels.

TABLE III
FORENSIC TOOLS COMPARISON

Artifact Type	Belkasoft Evidence (trial ver)	WhatsApp Key/DB Extractor
Text Message	-	√
Image	√	√
Video	√	-
Document	√	-

Unlike the WhatsApp Key/DB Extractor, Belkasoft Evidence (trial ver) manages to get images, video and document artifacts. Image artifacts obtained using Belkasoft Evidence (trial ver) have better quality than WhatsApp Key/DB Extractor artifacts. Belkasoft Evidence (trial ver) does not get text message artifacts.

The extraction results using Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor are repeated to ensure the similarity of the results obtained. This needs to be done to test the validation of results from forensic tools according to the NIST method. Table 3 and Table 4 shows the number of artifacts obtained using Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor. Experiments conducted using Belkasoft Evidence (trial ver) resulted in the same number of artifacts as shown in Table 3. Table 4 shows the number of artifacts obtained using WhatsApp Key/DB Extractor. Although the number of artifacts from Belkasoft Evidence (ver trial) and WhatsApp Key/DB Extractor are different, same image files can be found in the artifacts from Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor.

TABLE III
BELKASOFT EVIDENCE (TRIAL VER) ARTIFACTS COMPARISON

Artifact Type	Belkasoft Evidence (trial ver) 1 st Extraction	Belkasoft Evidence (trial ver) 2 nd Extraction
Text Message	-	-
Image	2086	2086
Video	43	43
Document	26	26

TABLE IV
WHATSAPP KEY/DB EXTRACTOR ARTIFACTS COMPARISON

Artifact Type	WhatsApp Key/DB Extractor 1 st Extraction	WhatsApp Key/DB Extractor 2 nd Extraction
Text Message	44	44
Image	3	3
Video	-	-
Document	-	-

From the validation test result, both Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor meet validation test of repeatability and reproducibility as in Table 5. Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor are conducted to perform extraction twice to check repeatability test. Both Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor meet repeatability test since each tools' tests have the same number of artifacts. Although the number of artifacts from each forensic tools are different, Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor meet reproducibility test because both artifacts have same image files.

TABLE V
FORENSIC TOOLS VALIDATION

Tools Validation	Belkasoft Evidence (trial ver)	WhatsApp Key/DB Extractor
Repeatable	√	√
Reproducible	√	√

IV. CONCLUSION

Based on the results of testing conducted on WhatsApp 2.17.147 with .crypt12 encryption, Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor meet validation test of repeatability and reproducibility. WhatsApp Key/DB Extractor dominates in the extraction ability of text message artifacts. Belkasoft Evidence (trial ver) has advantages in extraction abilities for images, videos, and documents. Further research on WhatsApp artifact extraction abilities in non-Android platforms needs to be done considering the WhatsApp application is available for many platforms.

REFERENCES



- [1] Chaffey D. Smart Insight Marketing Intelligence Ltd. [Online].; 2017. Available from: <http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/> HYPERLINK
- [2] Curtis S. The Telegraph. [Online].; 2014. Available from: <http://www.telegraph.co.uk/technology/news/10568395/Instant-messaging-overtakes-texting-in-the-UK.html> .
- [3] Garratt L, Poulter S. Daily Mail Online. [Online].; 2014. Available from: <http://www.dailymail.co.uk/sciencetech/article-2538488/SMS-takes-seat-IM-number-texts-sent-Britain-falls-time.html> .
- [4] Gudipaty LP, Jhala KY. WhatsApp Forensics: Decryption of Encrypted WhatsApp Databases on Non Rooted Android Devices. *Journal Information Technology & Software Engineering*. 2015; 5(2).
- [5] Koum J, Acton B. WhatsApp. [Online].; 2016. Available from: <https://blog.whatsapp.com/10000618/end-to-end-encryption> .
- [6] Kusumadewi A, Sasongko JP. CNN Indonesia. [Online].; 2016. Available from: <http://www.cnnindonesia.com/nasional/20160121080758-12-105715/polisi-usut-percakapan-jessica-mirna-yang-beredar-di-sosmed/> .
- [7] Metz C. Wired. [Online].; 2016. Available from: <https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/> .
- [8] Sahu S. An Analysis of WhatsApp Forensics in Android Smartphones. *International Journal of Engineering Research*. 2014 May 1; 3(5): p. 349-350.
- [9] Sai D, Prasad NR, Dekka S. The Forensics Process Analysis of Mobile Device. *International Journal of Computer Science and Information Technology*. 2015; 6(5): p. 4847-4850.
- [10] Satrya GB, Daely PT, Shin SY. Android Forensics Analysis: Private Chat on Social Messenger. *IT Convergence Engineering*. 2016.
- [11] Statista. [Online].; 2017. Available from: <https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/> .
- [12] Sutikno T, Handayani L, Stiawan D, Riyadi AR, Subroto IM. WhatsApp, Viber and Telegram: which is the Best for Instant Messaging? *International Journal of Electrical and Computer Engineering*. 2016 June; 6(3): p. 909-914.
- [13] Bonnington C. Wired. [Online].; 2015. Available from: <https://www.wired.com/2015/02/smartphone-only-computer/> .
- [14] Ajjola A, Zavarsky P, Ruhl R. A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101. In *World Congress on Internet Security*; 2014: Institute of Electrical and Electronics.
- [15] Ayers R, Brothers S, Jansen W. Guidelines on Mobile Device Forensics. , Department of Commerce; 2014.
- [16] Cankaya EC, Kupka B. A Survey of Digital Forensics Tools for Database Extraction. In *Future Technologies Conference*; 2016; San Francisco: IEEE. p. 1014-1019.
- [17] Dogan S, Akbal E. Analysis of Mobile Phones in Digital Forensics. In *MIPRO*; 2017; Opatija. p. 1241-1244.

Lampiran 7

#3591 Summary

[SUMMARY](#) [REVIEW](#) [EDITING](#)

Submission

Authors	Rusydi Umar, Imam Riadi, Guntur Maulana Zamroni
Title	Mobile Forensic Tools Evaluation for Digital Crime Investigation
Original file	3591-7607-1-SM.DOC 2017-10-04
Supp. files	None
Submitter	Guntur Maulana Zamroni 
Date submitted	October 4, 2017 - 08:59 PM
Section	Articles
Editor	Rahmat Hidayat 
Abstract Views	4

Status

Status	Published Vol 8, No 3 (2018)
Initiated	2018-06-20
Last modified	2018-06-29

Submission Metadata

Authors

Name	Rusydi Umar 
Affiliation	Universitas Ahmad Dahlan
Country	Indonesia
Bio Statement	Department of Informatics Engineering
Name	Imam Riadi 
Affiliation	Universitas Ahmad Dahlan
Country	Indonesia
Bio Statement	Department of Information System
Name	Guntur Maulana Zamroni 
Affiliation	Universitas Ahmad Dahlan
Country	Indonesia
Bio Statement	Department of Informatics Engineering
Principal contact for editorial correspondence.	

Mobile Forensic Tools Evaluation for Digital Crime Investigation

Rusydi Umar[#], Imam Riadi^{*}, Guntur Maulana Zamroni[#]

[#] Department of Informatics Engineering, Ahmad Dahlan University, Jl. Prof. Dr. Soepomo, Warungboto, Umbulharjo, Yogyakarta, 55164
E-mail: rusydi_umar@rocketmail.com

^{*}Department of Information System, Ahmad Dahlan University, Jl. Prof. Dr. Soepomo, Warungboto, Umbulharjo, Yogyakarta, 55164
E-mail: 1

[#]Department of Informatics Engineering, Ahmad Dahlan University, Jl. Prof. Dr. Soepomo, Warungboto, Umbulharjo, Yogyakarta, 55164
E-mail: gunturmz@yahoo.com

Abstract— Instant Messaging is a popular smartphone’s application. One example of Instant Messaging application is WhatsApp. WhatsApp is widely used judging from its users that reach more than 1 Billion users in January 2017. WhatsApp’s security recently has been updated with latest encryption type and technology by implementing end-to-end encryption. The number of users or possible crime target and security features in WhatsApp can lead to crime by people that have criminal intentions. Investigators need to use mobile forensic methodologies and tools for investigating smartphone and to find crime evidences. However, investigators often facing challenges during investigation because incompatibility between forensic tools and mobile technology. This research will conduct an experiment using available forensic tools with NIST forensic method for extracting latest WhatsApp’s artifacts. Forensics tools capabilities will be evaluated and compared to find its strengths and weaknesses.

Keywords— mobile forensic, whatsapp, extraction.

I. INTRODUCTION

Smartphones experience rapid development along with the development of technology. Smartphones are slowly beginning to replace the role of computers with the increasing number of features and applications available on mobile devices [1]. Trend of smartphone usage is expected to increase seen from the features offered by smartphones such as various applications, power usage, process speed, pricing, practicality and ease of carrying.

The latest generation of smartphones has the ability and power far above its predecessors that make smartphones now can be used for household activity or office work [2]. Fig. 1 shows the number of smartphone and computer device users. We can see the number of smartphone users has obtained increasing significant number compared to the number of computer users. Starting in 2014 the number of smartphone users began to outperform the number of computer users [1].

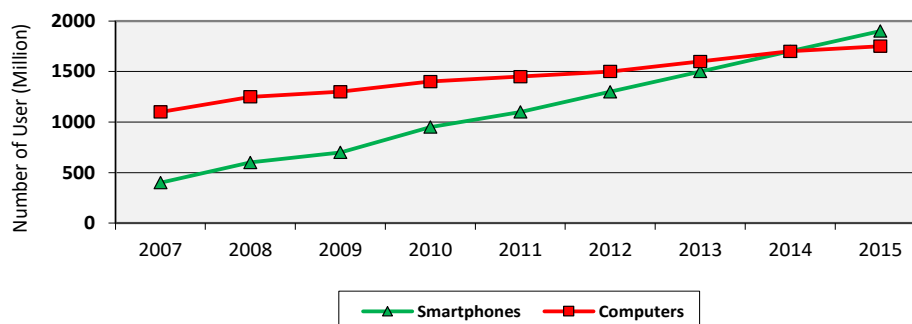


Fig. 1 Number of computer and smartphone users

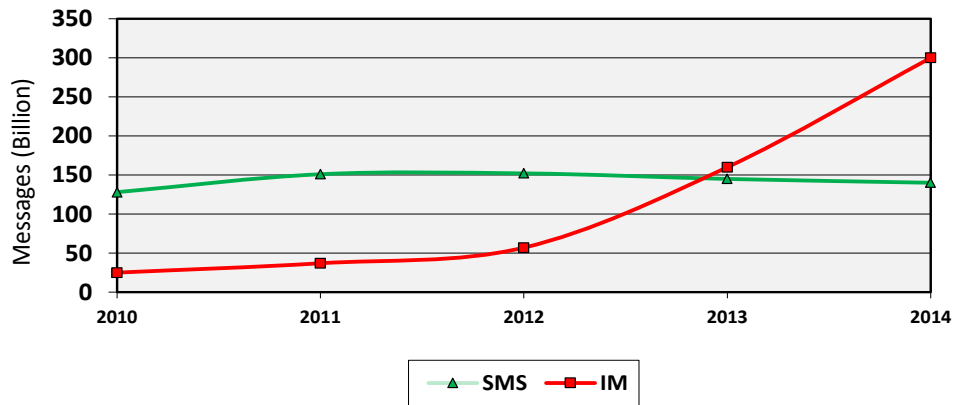


Fig. 2 Number of Messages Sent Using SMS and IM in United Kingdom

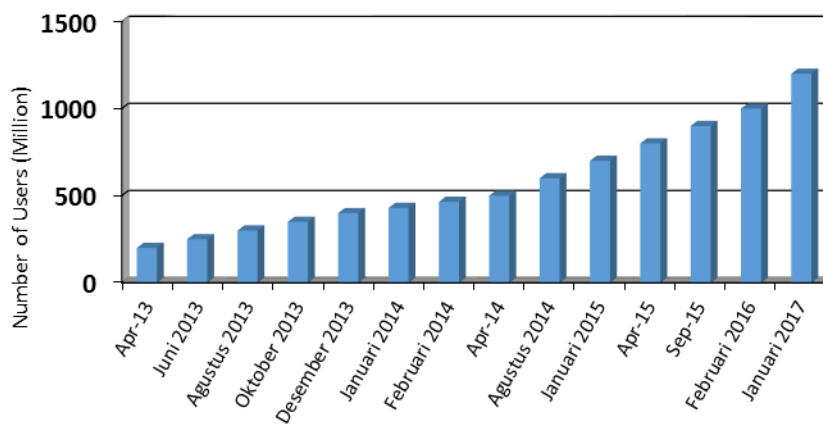


Fig. 3 Number of WhatsApp Users

The Instant Messaging (IM) application is one of the most commonly used applications for mobile device users. IM begins to replace the role of Short Message Services (SMS) to communicate through message delivery. Fig. 2 shows the trend of message delivery with SMS and IM in the UK. The number of message delivery using SMS from 2010 to 2014 tend to experience stable conditions. While the number of message delivery using IM has increased significantly starting in 2012 with the number of messages sent for 57 billion messages/year until 2014 with messages sent for 300 billion/year [3].

WhatsApp is one of the popular IM applications and is used by lots of people to communicate. Fig. 3 shows an increase in the number of WhatsApp users from 200 Million users in April 2013 to 1 Billion in February 2016 and 1.2 Billion in January 2017 [4]. According to [5], WhatsApp is a popular application with 60% of users, followed by Viber and Telegram.

WhatsApp cannot be separated from misuse as for criminal purposes. Under these circumstances the investigator will check out WhatsApp's artifact to look for evidence of a criminal offense. The case of "cyanide coffee" is one example of the case where the WhatsApp artifacts were analyzed to search for evidence in the investigation [6].

To conduct an analysis the investigator needs to use a method along with a forensically tested tools. Investigators should be able to extract the artifacts, decryption, and analyze the data contained within the mobile device to assist the investigation process because data such as conversation messages and images can be evidence [7].

References [8] conducted an analysis of forensic mobile technologies and forensic tools. Forensic analysis has several constraints such as hardware differences, security features, technological lag and forensic tool costs, anti-forensic techniques, and many other. In April 2016, WhatsApp implemented an end-to-end encryption feature that came with the latest encryption. This feature makes the sent messages to be encrypted and can only be read by those eligible to receive the message. This security feature provides difficulties and challenges for forensic investigators and analysis because the available forensics tools must be able to keep up with the development of WhatsApp technology [9].

There are several studies on mobile forensic analysis. References [10] conducted forensic analysis of Telegram, Line, and KakaoTalk applications on Android devices. They tried to conduct a forensic analysis process on unencrypted conversations and encrypted conversations. The tools used in the research were ADB (Android Debugging Bridge), SQLite

Browser, Hex Editor Neo, Busybox, Root Browser, Nandroid Backup, Shark for Root, dex2jar. References [10] used a methodology from McKemish which has 4 stages: Identification, Preservation, Analysis, and Presentation. References [10] managed to investigate unencrypted and encrypted conversations from all three applications.

References [11] attempted to perform a forensic analysis on WhatsApp version 2.11.186 which has been equipped with .crypt encryption. The tools used were WhatsApp Xtract for the extraction and decryption process, and SQLite Browser for the analysis process. The researcher succeeded in extraction and .crypt decryption.

References [12] conducted a forensic analysis on WhatsApp that has used .crypt7 encryption. The tools used in the research were ADB, WhatsApp Key/DB Extractor 2.2, WhatsApp Viewer, WhatsApp Extract, dan SQLite Spy. Researchers managed to extract and decrypt WhatsApp artifacts. Researchers reminded about the importance of paying attention to the development and changes in mobile technology to be able to perform forensic analysis.

References [13] evaluated and compared 2 forensic methodologies, ISO/IEC methodology and NIST methodology. Ajijola, et al concluded that there is no methodology covering all forensic issues. The ISO/IEC methodology has advantages over non-technical processes and problems. NIST has the advantage of selecting and using forensic tools. Each methodology needs to be constantly updated following the development of digital technology.

Looking at the background, the dynamics of mobile technology, previous research, and mobile forensic challenges, researchers will try to conduct comparative evaluation forensic tools that serve to extract artifacts in the form of messages, images, videos and documents with NIST forensic methodology in the latest version of WhatsApp in Android-based devices. The tools used are ADB, WhatsApp Key/DB Extractor 4.7, and Belkasoft Evidence (trial version). Forensic tools are tested to run the WhatsApp database extraction and decryption process that has been updated with .crypt12 end-to-end encryption. The results of extraction, decryption, and validation of forensic tools will be compared in order to have the conclusions.

II. MATERIAL AND METHOD

The purpose of this research was to evaluate and compare the Belkasoft Evidence (trial version) and WhatsApp Key/DB Extractor forensic tools, especially in terms of the extraction capabilities of the latest WhatsApp artifacts on Android-based devices that have used .crypt12 encryption.

A. Research Steps

This research used a research step made by the National Institute of Stanford and Technology [7]. The NIST research stage consists of 4 stages as in Fig. 4.

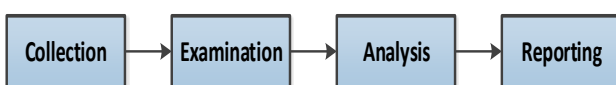


Fig. 4 NIST Forensic Methodology

- 1) *Collection*: In the collection stage, there will be the acquisition of evidence, preservation of evidence, preparation of objects and research tools.
- 2) *Examination*: At the examination stage, there will be process of identifying data that can be used as evidence. After determining which data will be taken, the data retrieval process will be done in a forensically tested way.
- 3) *Analysis*: The data which have been taken will be analyzed to look for things that can be used as evidence and then conclusion will be taken
- 4) *Reporting*: The last stage of the forensic step is to report forensic activity from beginning to the end along with the results of the analysis into the form of a written report or oral report.

This research focused on the examination stage. The examination stage is further elaborated into several stages as in Fig. 5. Identification is done to find data or artifacts to be taken and possibly produce evidence to assist investigation. After determining the data or artifacts to be taken, it will proceed to the data retrieval process.

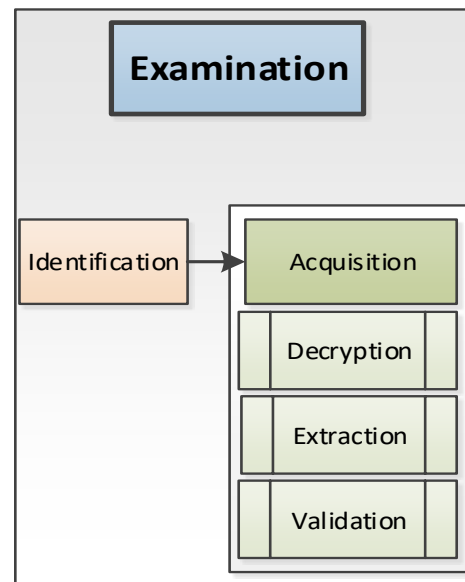


Fig. 5 Steps of Examination

WhatsApp has been equipped with an encryption feature that aims to hide messages [14]. This encryption feature can interfere with the investigation process. Therefore, a tool that can perform decryption and data extraction is needed. Validation using repeatability and reproducibility according to the NIST method will be performed to ensure that the results of the extraction process performed are correct and there is no data manipulation. Repeatability is done by repeated extraction processes in time adjacent to the same object and forensic tool. While reproducibility is done by using the same object but with different forensic tools.

B. Research Tools

The hardware and software used to experiment on the extraction of WhatsApp artifacts from an Android-based device can be seen in Table 1.

TABLE I
RESEARCH TOOLS AND DEVICES

No.	Tool and Device	Information
1	Samsung Galaxy S4 GT-I9500 with 5.0.1 Lollipop operation system	Smartphone device for experiment
2	WhatsApp ver. 2.17.147	Instant Messaging application
3	Workstation with operational system of Windows 7 64 Bit, Intel i5-4440, 4,00 GB	Computer device for extraction and analysis
4	USB Cable	USB connector to connect smartphone device and computer
5	Android Debugging Bridge	Software to support a communication between smartphone and computer
6	WhatsApp Key/DB Extractor 4.7	Extraction tool
7	Belkasoft Evidence (ver trial)	Extraction and analysis tool
8	SQLite Studio	Analysis tool

C. Experiment Simulation

The experiments were conducted in a closed and noise free condition, meaning that the smartphone device was changed to Airplane Mode. With Airplane Mode the device will not be able to receive outside calls and messaging. This is important to maintain the authenticity and integrity of the data. The workstations used are not connected to the Internet and are free from malware that may influence the results of the experiment.

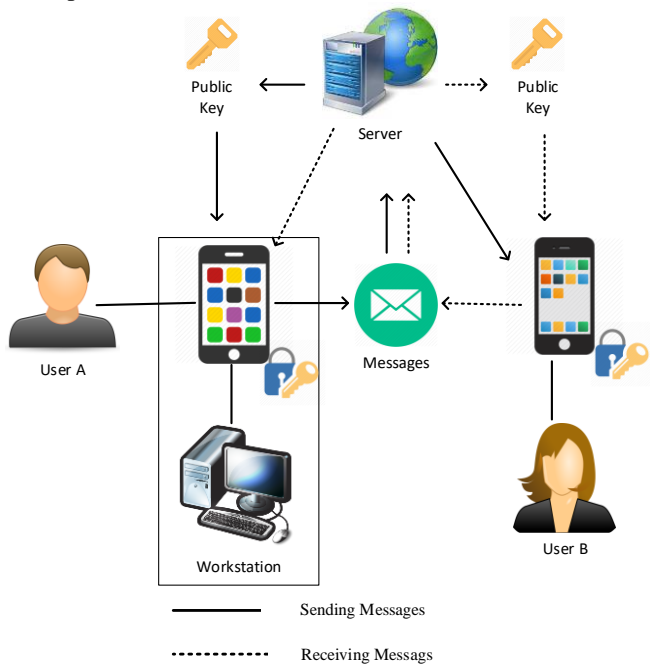


Fig. 6 Experiment Simulation

Fig. 6 describes the simulation of the experimental tool. To send a message to User B, User A will request a public key on the server which will then be used for message encryption. User B then uses the private key to decrypt the message.

User A's Smartphone will be used for forensic analysis. Smartphones with the Android 5.0.1 operating system and WhatsApp 2.17.147 are used for everyday activities such as sending and receiving messages, pictures, videos, and documents which will be connected using a USB cable with workstations that use Windows 64 Bits, ADB, WhatsApp Key/DB Extractor 4.7, and Belkasoft Evidence. Each forensic tools will conduct extraction process twice to ensure the validity of forensic tools.

III. RESULTS AND DISCUSSION

A. Extraction results using Belkasoft Evidence

In experiments conducted using Belkasoft Evidence (trial ver) the message artifact of WhatsApp text was not obtained, but video, image, and document artifacts were successfully obtained. Information about the video artifact can be seen in the properties column. Belkasoft provides video file information such as file name, file size, and access date. The size of the extracted video file has different video pixel duration and size according to the original file on the smartphone. Video artifacts can be played and viewed so that it is helpful in the investigation process in the search of evidence as described in Fig. 7. Image artifacts can be zoomed to see clearer images and help with double clicking as well as displaying information from image files such as filename, access date, pixel size, and file size as in Fig. 8. The pixel size and file size of the image artifact match the original size of the original file on the smartphone.

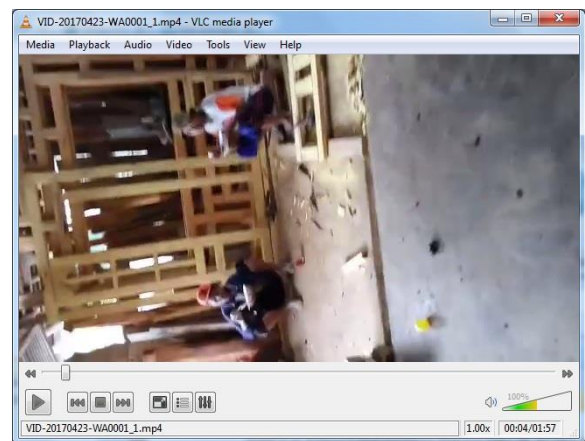


Fig. 7 Video artifact detail of Belkasoft Evidence

Metadata information from documents such as creator's name, software used, file name, and file size can be known. The document artifact can be opened so that the investigator can see the contents of the document.

status_timestamp	number	raw_contact_jd	display_name
0	0222531	997	MM itb
1473441122000	0822207	1956	Tornado Nano Seller
0	+628386	2333	Calon Koki 11
0	+622749	1111	Yusuf servis ac
1430971391000	+628574	889	Didit
1423072923000	+628574	846	Arif net
1471952553000	+628572	1850	Jogjaringan Isp
0	+628389	1040	Rahmat net no laen
0	+601393	835	Alif Arena
1478700523000	0813254	1071	Seller char ao twinbrother
0	+601766	837	Alwi Skate
0	0878392	1901	Yanto Buang Material
1478973985000	+601690	1097	Wawan Setiawan
1464963504000	0857439	1023	Pak raharjo instalasi listrik
0	+628520	986	Mbak pipit pakdhe kelik
1470224229000	+628157	909	Fauzan Tehnisi
1410859388000	0857299	1826	Magma Seller
0	0856433	961	Mas Bejo roti bakar
0	0274563	1940	Univ Ahmad Dahlan
1464188106000	0858787	900	Dwi servis ac stikes
0	0877382	916	Gunawan atlantica onlen joki jogja
1478792857000	+628577	1996	Mas Oji Jkt
1478006823000	+628128	981	Mbak Mega
0	0857763	895	DN indo joki

Fig. 10 WhatsApp Contact List Artifact

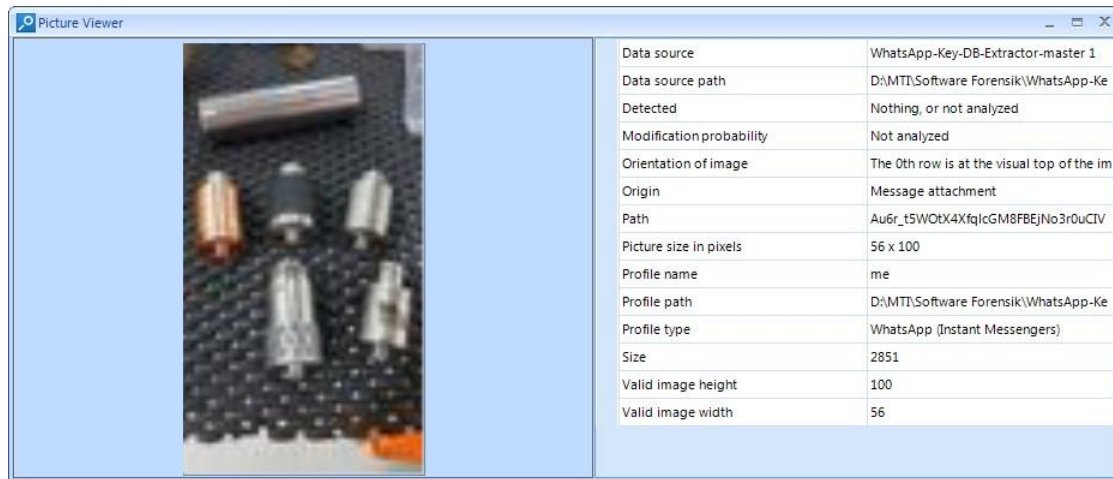


Fig. 11 WhatsApp Key/DB Extractor Picture Detail

C. Discussion

Table 2 shows the artifacts obtained. WhatsApp Key / DB Extractor only manages to extract text message and images artifacts. Message information such as message body, message recipient, message sender, chat group, chat group participant, all contacts on WhatsApp either name or phone number is successfully obtained. This is certainly very useful in helping the investigation process to look for evidence of crime. WhatsApp Key/DB Extractor managed to get the image artifact, but in size of 56 x 100 pixels.

TABLE III
FORENSIC TOOLS COMPARISON

Artifact Type	Belkasoft Evidence (trial ver)	WhatsApp Key/DB Extractor
Text Message	-	√
Image	√	√
Video	√	-
Document	√	-

Unlike the WhatsApp Key/DB Extractor, Belkasoft Evidence (trial ver) manages to get images, video and document artifacts. Image artifacts obtained using Belkasoft Evidence (trial ver) have better quality than WhatsApp Key/DB Extractor artifacts. Belkasoft Evidence (trial ver) does not get text message artifacts.

The extraction results using Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor are repeated to ensure the similarity of the results obtained. This needs to be done to test the validation of results from forensic tools according to the NIST method. Table 3 and Table 4 shows the number of artifacts obtained using Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor. Experiments conducted using Belkasoft Evidence (trial ver) resulted in the same number of artifacts as shown in Table 3. Table 4 shows the number of artifacts obtained using WhatsApp Key/DB Extractor. Although the number of artifacts from Belkasoft Evidence (ver trial) and WhatsApp Key/DB Extractor are different, same image files can be found in the artifacts from Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor.

TABLE III
BELKASOFT EVIDENCE (TRIAL VER) ARTIFACTS COMPARISON

Artifact Type	Belkasoft Evidence (trial ver) 1 st Extraction	Belkasoft Evidence (trial ver) 2 nd Extraction
Text Message	-	-
Image	2086	2086
Video	43	43
Document	26	26

TABLE IV
WHATSAPP KEY/DB EXTRACTOR ARTIFACTS COMPARISON

Artifact Type	WhatsApp Key/DB Extractor 1 st Extraction	WhatsApp Key/DB Extractor 2 nd Extraction
Text Message	44	44
Image	3	3
Video	-	-
Document	-	-

From the validation test result, both Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor meet validation test of repeatability and reproducibility as in Table 5. Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor are conducted to perform extraction twice to check repeatability test. Both Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor meet repeatability test since each tools' tests have the same number of artifacts. Although the number of artifacts from each forensic tools are different, Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor meet reproducibility test because both artifacts have same image files.

TABLE V
FORENSIC TOOLS VALIDATION

Tools Validation	Belkasoft Evidence (trial ver)	WhatsApp Key/DB Extractor
Repeatable	√	√
Reproducible	√	√

IV. CONCLUSION

Based on the results of testing conducted on WhatsApp 2.17.147 with .crypt12 encryption, Belkasoft Evidence (trial ver) and WhatsApp Key/DB Extractor meet validation test of repeatability and reproducibility. WhatsApp Key/DB Extractor dominates in the extraction ability of text message artifacts. Belkasoft Evidence (trial ver) has advantages in extraction abilities for images, videos, and documents. Further research on WhatsApp artifact extraction abilities in non-Android platforms needs to be done considering the WhatsApp application is available for many platforms.

REFERENCES

- [1] Chaffey D. Smart Insight Marketing Intelligence Ltd. [Online].; 2017. Available from: <http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/> HYPERLINK
- [2] Curtis S. The Telegraph. [Online].; 2014. Available from: <http://www.telegraph.co.uk/technology/news/10568395/Instant-messaging-overtakes-texting-in-the-UK.html> HYPERLINK
- [3] Garratt L, Poulter S. Daily Mail Online. [Online].; 2014. Available from: <http://www.dailymail.co.uk/sciencetech/article-2538488/SMS-takes-seat-IM-number-texts-sent-Britain-falls-time.html> HYPERLINK
- [4] Gudipaty LP, Jhala KY. WhatsApp Forensics: Decryption of Encrypted WhatsApp Databases on Non Rooted Android Devices. *Journal Information Technology & Software Engineering*. 2015; 5(2).
- [5] Koum J, Acton B. WhatsApp. [Online].; 2016. Available from: <https://blog.whatsapp.com/10000618/end-to-end-encryption> HYPERLINK
- [6] Kusumadewi A, Sasongko JP. CNN Indonesia. [Online].; 2016. Available from: <http://www.cnnindonesia.com/nasional/20160121080758-12-105715/polisi-usut-percakapan-jessica-mirna-yang-beredar-di-sosmed/> HYPERLINK
- [7] Metz C. Wired. [Online].; 2016. Available from: <https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/> HYPERLINK
- [8] Sahu S. An Analysis of WhatsApp Forensics in Android Smartphones. *International Journal of Engineering Research*. 2014 May 1; 3(5): p. 349-350.
- [9] Sai D, Prasad NR, Dekka S. The Forensics Process Analysis of Mobile Device. *International Journal of Computer Science and Information Technology*. 2015; 6(5): p. 4847-4850.
- [10] Satrya GB, Daely PT, Shin SY. Android Forensics Analysis: Private Chat on Social Messenger. *IT Convergence Engineering*. 2016.
- [11] Statista. [Online].; 2017. Available from: <https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/> HYPERLINK
- [12] Sutikno T, Handayani L, Stiawan D, Riyadi AR, Subroto IM. WhatsApp, Viber and Telegram: which is the Best for Instant Messaging? *International Journal of Electrical and Computer Engineering*. 2016 June; 6(3): p. 909-914.
- [13] Bonnington C. Wired. [Online].; 2015. Available from: <https://www.wired.com/2015/02/smartphone-only-computer/> HYPERLINK
- [14] Ajijola A, Zavarsky P, Ruhl R. A Review and Comparative Evaluation of Forensics Guidelines of NIST SP 800-101. In *World Congress on Internet Security*; 2014: Institute of Electrical and Electronics.
- [15] Ayers R, Brothers S, Jansen W. Guidelines on Mobile Device Forensics. , Department of Commerce; 2014.
- [16] Cankaya EC, Kupka B. A Survey of Digital Forensics Tools for Database Extraction. In *Future Technologies Conference*; 2016; San Francisco: IEEE. p. 1014-1019.
- [17] Dogan S, Akbal E. Analysis of Mobile Phones in Digital Forensics. In *MIPRO*; 2017; Opatija. p. 1241-1244.