International Journal on
Advanced Science
Engineering
Information Technology

Vol.8 (2018) No. 3
ISSN: 2088-5334

Mobile Forensic Tools Evaluation for Digital Crime Investigation

Rusydi Umar[#1], Imam Riadi[*2], Guntur Maulana Zamroni[#3]

[#] *Department of Informatics Engineering, Ahmad Dahlan University, Jl. Prof. Dr. Soepomo, Warungboto, Umbulharjo, Yogyakarta, 55164*
E-mail: [1]rusydi_umar@rocketmail.com E-mail: [3]gunturmz@yahoo.com

**Department of Information System, Ahmad Dahlan University, Jl. Prof. Dr. Soepomo, Warungboto, Umbulharjo, Yogyakarta, 55164*
E-mail: [2]imam.riadi@is.uad.ac.id

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 finding out the crime evidence. However, investigators are often facing challenges during the investigation because of incompatibility between forensic tools and mobile technology. This research will 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]. The 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 computing 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].

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. Meanwhile, the number of message delivery using IM 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 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] analyzed mobile forensic 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 others. 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.

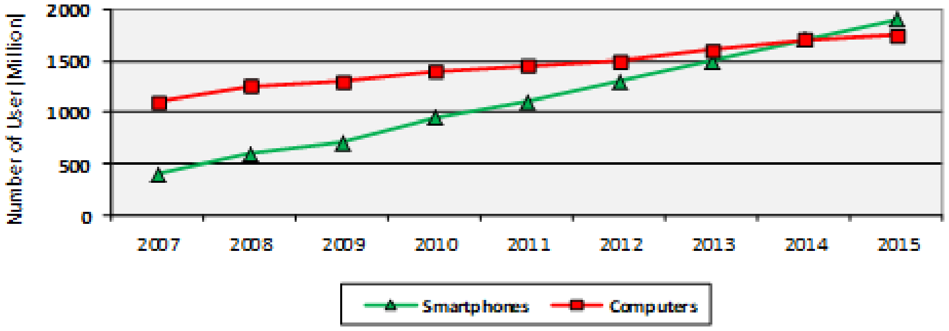


Fig. 1 Number of computer and smartphone users

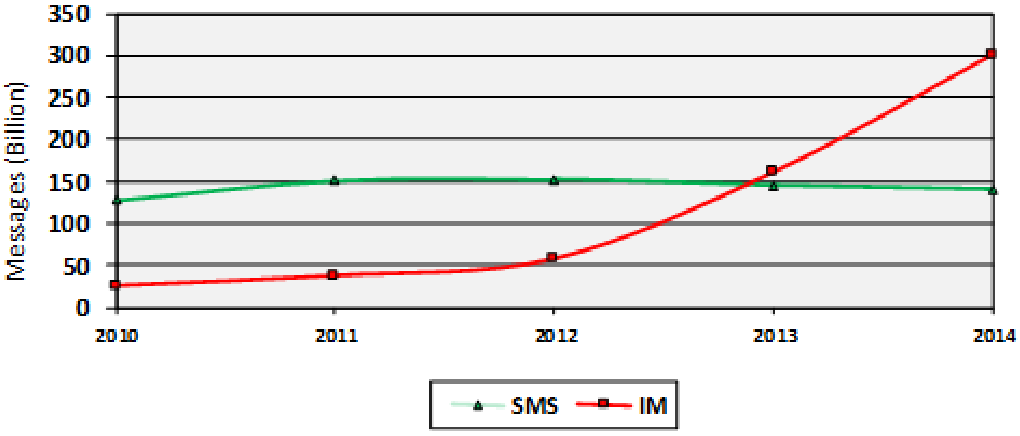


Fig. 2 Number of Messages Sent Using SMS and IM in the United Kingdom

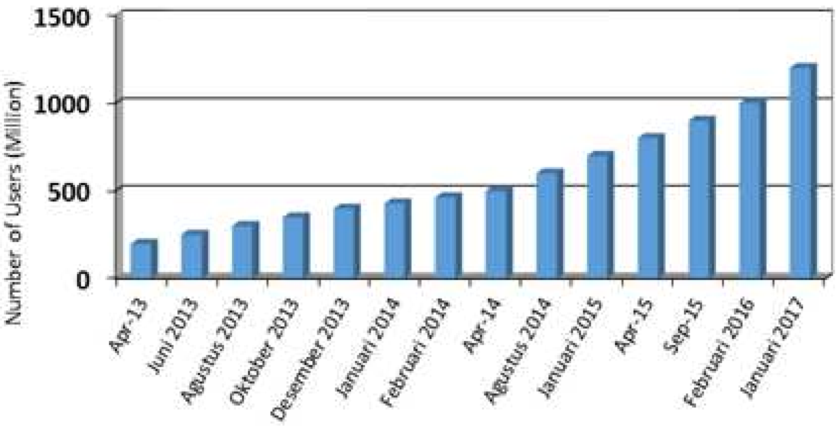


Fig. 3 Number of WhatsApp Users

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 McKemmish which has four 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 two 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 updated continuously 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 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 regarding 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.

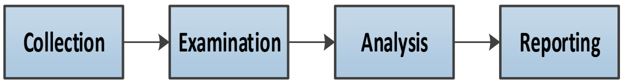


Fig. 4 NIST Forensic Methodology

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 a 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 the conclusion will be taken
4) *Reporting*: The last stage of the forensic step is to report forensic activity from the 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 made to find data or artifacts to be taken and possibly produce evidence to assist the investigation. After determining the data or artifacts to be taken, it will proceed to the data retrieval process.

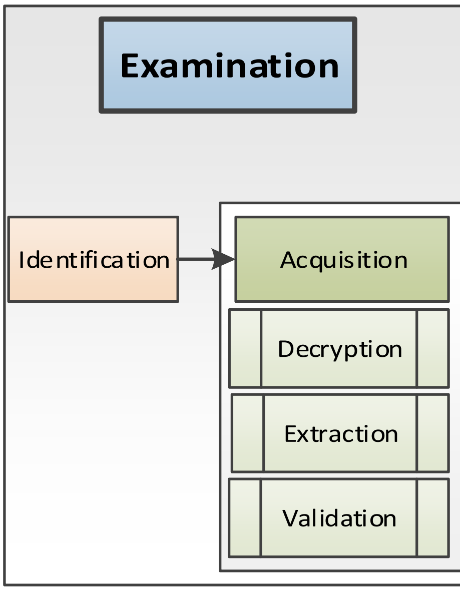


Fig. 5 Steps of Examination

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. Repeated extraction processes do repeatability in time adjacent to the same object and forensic tool. Meanwhile, 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 devise for the experiment
2	WhatsApp ver. 2.17.147	Instant Messaging application
3	Workstation with an operating system of Windows 7 64 Bit, Intel i5-4440, 4,00 GB	A computer devise for extraction and analysis
4	USB Cable	USB connector to connect smartphone device and computer
5	Android Debugging Bridge	Software to support 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.

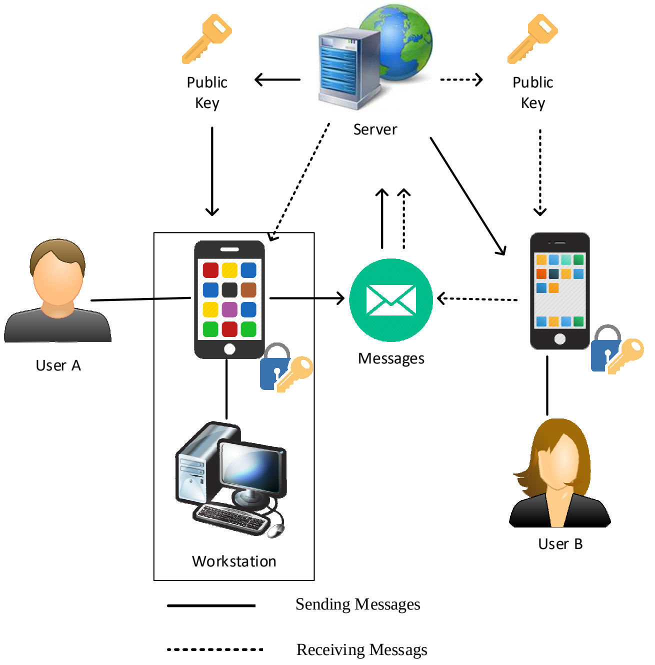


Fig. 6 Experiment Simulation

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 search of evidence as described in Fig. 7. Image artifacts can be zoomed to see more explicit 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.

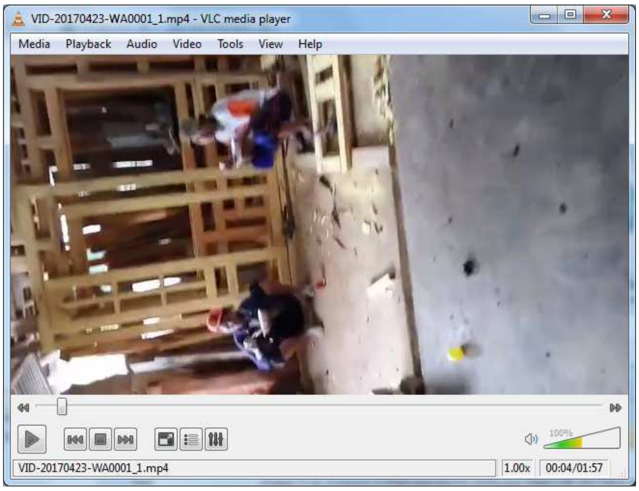
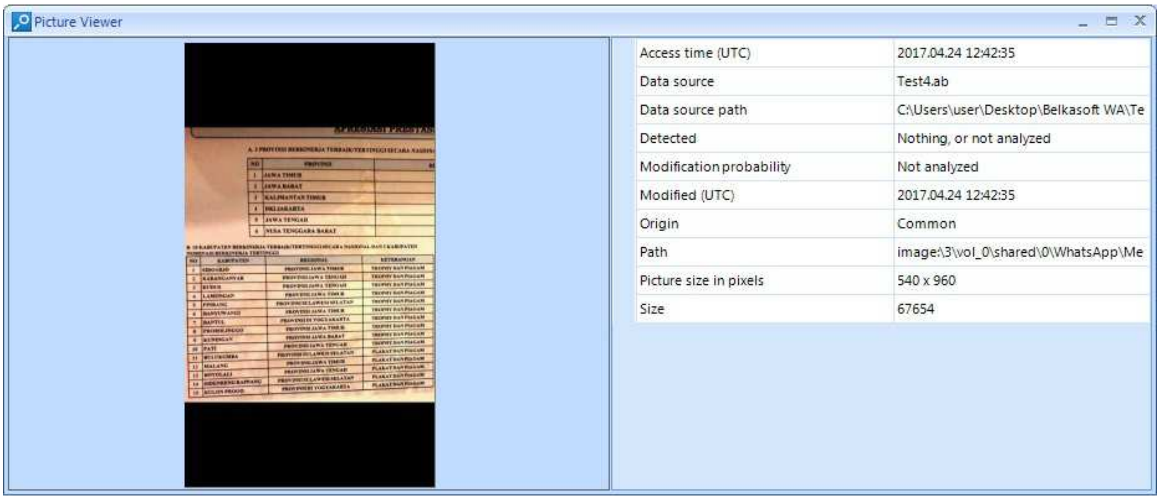

VID-20170423-WA0001_1.mp4 - VLC media player
Media
Playback
Audio
Video
Tools
View
Help
100%
VID-20170423-WA0001_1.mp4
1.00x
00:04/01:57

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.



Picture Viewer

Access time (UTC)	2017.04.24 12:42:35
Data source	Test4.ab
Data source path	C:\Users\user\Desktop\Belkasoft WA\Te
Detected	Nothing, or not analyzed
Modification probability	Not analyzed
Modified (UTC)	2017.04.24 12:42:35
Origin	Common
Path	image\3\vol_0\shared\0\WhatsApp\Me
Picture size in pixels	540 x 960
Size	67654

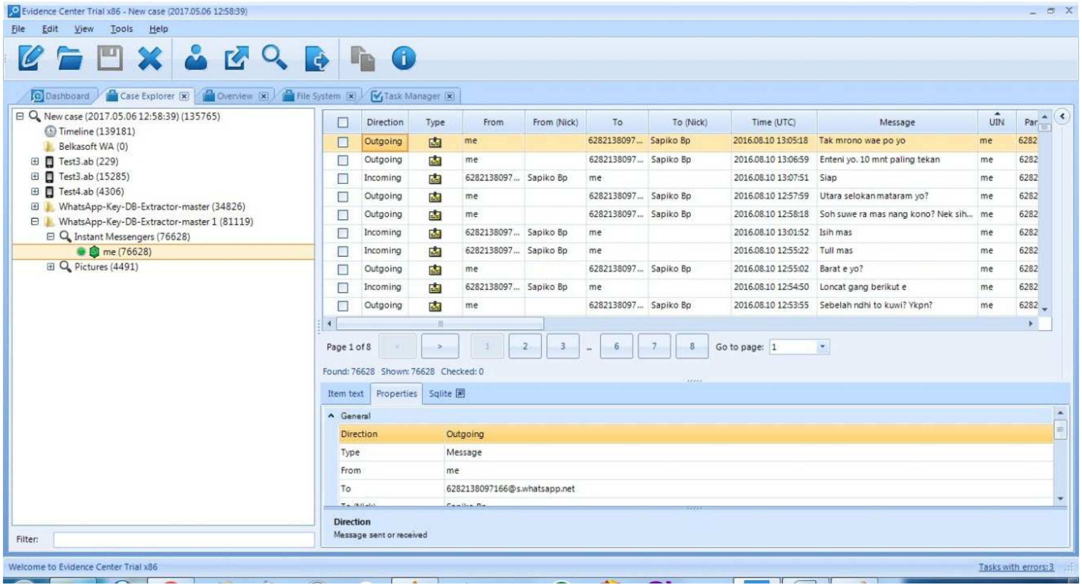
Fig. 8 Picture artifact detail of Belkasoft Evidence

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 beneficial to 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 artifact. 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. Double click can zoom the image, 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 by the thumbnail size in WhatsApp. The size applies to all extracted images using WhatsApp Key/DB Extractor.



Evidence Center Trial x86 - New case (2017.05.06 12:58:39)

- New case (2017.05.06 12:58:39) (135765)
  - Timeline (139181)
  - Belkasoft WA (0)
  - Test3.ab (229)
  - Test3.ab (15285)
  - Test4.ab (4306)
  - WhatsApp-Key-DB-Extractor-master (34826)
  - WhatsApp-Key-DB-Extractor-master 1 (81119)
    - Instant Messengers (76628)
      - me (76628)
    - Pictures (4491)

Filter:

□	Direction	Type	From	From (Nick)	To	To (Nick)	Time (UTC)	Message	UIN	Par
□	Outgoing		me		6282138097...	Sapiko Bp	2016.08.10 13:05:18	Tak mrono wae po yo	me	6282
□	Outgoing		me		6282138097...	Sapiko Bp	2016.08.10 13:06:59	Enteni yo. 10 mnt paling tekan	me	6282
□	Incoming		6282138097...	Sapiko Bp	me		2016.08.10 13:07:51	Siap	me	6282
□	Outgoing		me		6282138097...	Sapiko Bp	2016.08.10 12:57:59	Utara selokan mataram yo?	me	6282
□	Outgoing		me		6282138097...	Sapiko Bp	2016.08.10 12:58:18	Soh suwe ra mas nang kono? Nek sih...	me	6282
□	Incoming		6282138097...	Sapiko Bp	me		2016.08.10 13:01:52	Isih mas	me	6282
□	Incoming		6282138097...	Sapiko Bp	me		2016.08.10 12:55:22	Tull mas	me	6282
□	Outgoing		me		6282138097...	Sapiko Bp	2016.08.10 12:55:02	Barat e yo?	me	6282
□	Incoming		6282138097...	Sapiko Bp	me		2016.08.10 12:54:50	Loncat gang berikut e	me	6282
□	Outgoing		me		6282138097...	Sapiko Bp	2016.08.10 12:53:55	Sebelah ndhi to kuwi? Ykpn?	me	6282

Page 1 of 8 < > 1 2 3 .. 6 7 8 Go to page: 1

Found: 76628 Shown: 76628 Checked: 0

General

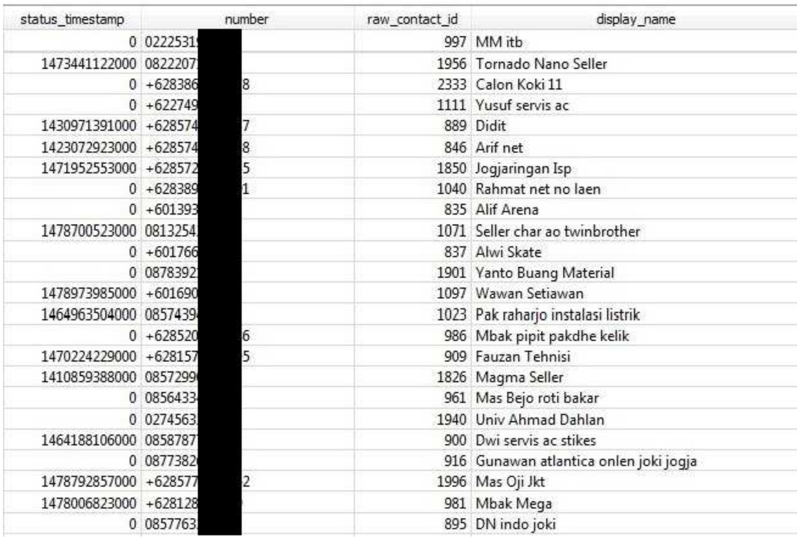
Direction	Outgoing
Type	Message
From	me
To	6282138097166@s.whatsapp.net

Direction
Message sent or received

Welcome to Evidence Center Trial x86

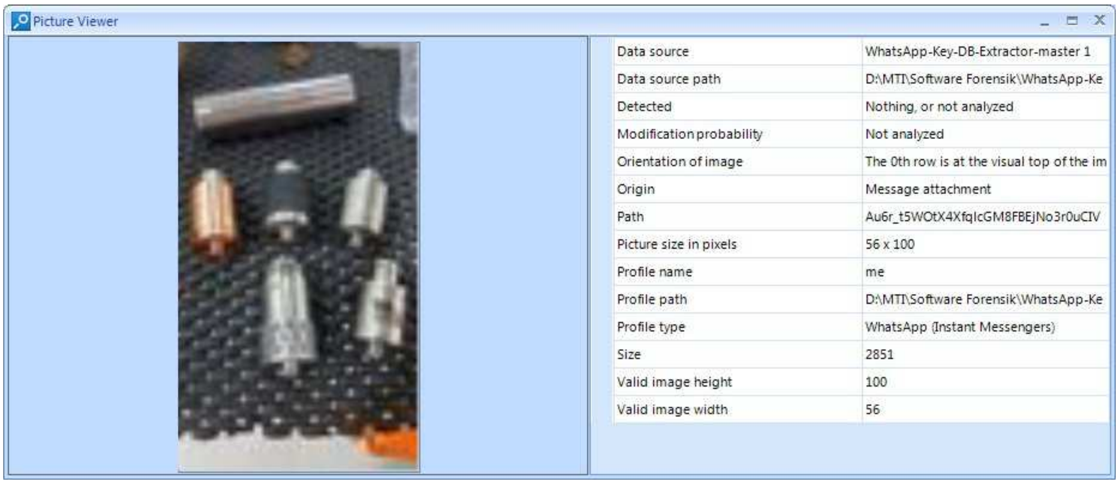
Tasks with errors:3

Fig. 9 WhatsApp Key/DB Extractor Message Artifact



status_timestamp	number	raw_contact_id	display_name
0	0222531[redacted]	997	MM itb
1473441122000	0822207[redacted]	1956	Tornado Nano Seller
0	+628386[redacted]8	2333	Calon Koki 11
0	+622749[redacted]	1111	Yusuf servis ac
1430971391000	+628574[redacted]7	889	Didit
1423072923000	+628574[redacted]8	846	Arif net
1471952553000	+628572[redacted]5	1850	Jogjaringan Isp
0	+628389[redacted]1	1040	Rahmat net no laen
0	+601393[redacted]	835	Alif Arena
1478700523000	0813254[redacted]	1071	Seller char ao twinbrother
0	+601766[redacted]	837	Alwi Skate
0	0878392[redacted]	1901	Yanto Buang Material
1478973985000	+601690[redacted]	1097	Wawan Setiawan
1464963504000	0857439[redacted]	1023	Pak raharjo instalasi listrik
0	+628520[redacted]6	986	Mbak pipit pakdhe kelik
1470224229000	+628157[redacted]5	909	Fauzan Tehnisi
1410859388000	0857299[redacted]	1826	Magma Seller
0	0856433[redacted]	961	Mas Bejo roti bakar
0	0274563[redacted]	1940	Univ Ahmad Dahlan
1464188106000	0858787[redacted]	900	Dwi servis ac stikes
0	0877382[redacted]	916	Gunawan atlantica onlen joki jogja
1478792857000	+628577[redacted]2	1996	Mas Oji Jkt
1478006823000	+628128[redacted]	981	Mbak Mega
0	0857763[redacted]	895	DN indo joki

Fig. 10 WhatsApp Contact List Artifact



Data source	WhatsApp-Key-DB-Extractor-master 1
Data source path	D:\MTI\Software Forensik\WhatsApp-Ke
Detected	Nothing, or not analyzed
Modification probability	Not analyzed
Orientation of image	The 0th row is at the visual top of the im
Origin	Message attachment
Path	Au6r_t5WOtX4XfqIcGM8FBEjNo3r0uCIV
Picture size in pixels	56 x 100
Profile name	me
Profile path	D:\MTI\Software Forensik\WhatsApp-Ke
Profile type	WhatsApp (Instant Messengers)
Size	2851
Valid image height	100
Valid image width	56

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 indeed very useful in helping the investigation process to look for evidence of a 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) 1st Extraction	Belkasoft Evidence (trial ver) 2nd 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 1st Extraction	WhatsApp Key/DB Extractor 2nd 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 is 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

[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 of 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, Setiawan 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] 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 Fransisco: IEEE. p. 1014-1019.

[17] Dogan S, Akbal E. Analysis of Mobile Phones in Digital Forensics. In MIPRO; 2017; Opatija. p. 1241-1244.