A Comparative Study of Forensic Tools For WhatsApp Analysis Using NIST Measurements

By Imam Riadi

A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements

Rusydi Umar
Department of Informatics Engineering
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

Guntur Maulana Zamroni
Magister of Information Technology
Universitas Ahmad Dahlan
Yogyakarta, Indonesia

***Abstract*—One of the popularly used features on Android smartphone is WhatsApp. WhatsApp can be misused, such as for criminal purposes. To conduct investigation involving smartphone devices, the investigators need to use forensic tools. Nonetheless, the development of the existing forensic tool technology is not as fast as the development of mobile technology and WhatsApp. The latest version of smartphones and WhatsApp always comes up. Therefore, a research on the performance of the current forensic tools in order to handle a case involving Android smartphones and WhatsApp in particular need to be done. This research evaluated existing forensic tools for performing forensic analysis on WhatsApp using parameters from NIST and WhatsApp artifacts. The outcome shows that Belkasoft Evidence has the highest index number, WhatsApp Key/DB Extractor has superiority in terms of costs, and Oxygen Forensic has superiority in obtaining WhatsApp artifact.**

Keywords*—*Whatsapp; acquisition; NIST parameters; artifact

I. Introduction

Smartphones with the Android operating system were introduced to the public in 2007; and it became the most popular operating system in 2011, judging from the sales [1]. In the fourth quarter of 2016 the number of smartphone sales with android operating system is 379.98 million units, as shown in Fig. 1.

Some popular smartphone features are messaging (88%), email (70%), Facebook (62%), camera (62%), and WhatsApp (51%) [2]. In [3], authors conducted a survey on instant messaging application, WhatsApp, Viber, and Telegram. From the survey results, WhatsApp tops the list at 60%. In terms of the user number, WhatsApp has increased significantly from year to year [4]. As of July 2017, the number of WhatsApp users has as many as 1.3 billion users as in Fig. 2. WhatsApp has various features, for instance sending and receiving text messages, pictures, videos, and documents. WhatsApp also comes with phone call and video call features. WhatsApp has been equipped with end-to-end encryption technology that serves to secure sent messages. With end-to-end encryption, the messages sent can only be read by senders and recipients [5].

It is impossible to separate WhatsApp from misuse. The large number of users and the end-to-end encryption technology used can be a magnet for someone with a criminal purpose such as drug trafficking, cyber-bullying, trafficking, and so on. There are some cases involving IM or WhatsApp applications [6]. In a case involving smartphone devices, the investigator needs to do mobile forensics. Mobile forensics is one of the forensic digital branches that learn on how to perform evidence recovery from a smartphone device. The investigator will perform forensic analysis of smartphone devices using forensic tools with a forensically-tested methodology, thus the analysis results are valid before the law and can be used as means of evidence [7].

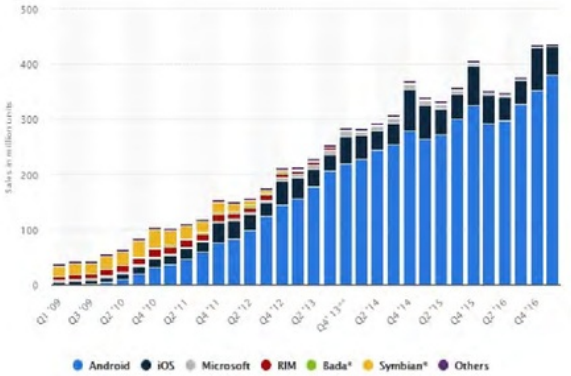


Fig. 1. Statistics of smartphone operating systems.

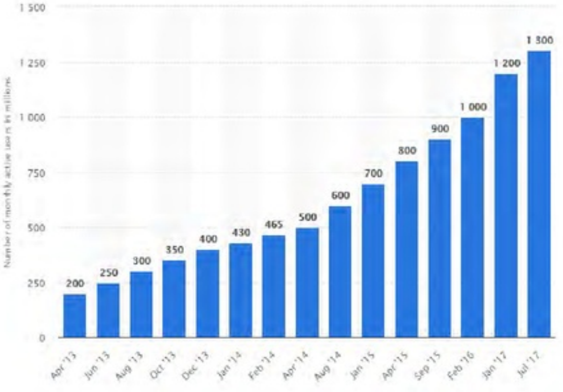


Fig. 2. Number of WhatsApp user statistics.

According to [8], there are three forensic acquisition techniques: manual, physical, and logical. In the manual acquisition, the investigator will manually create the acquisition by directly looking at the contents of the smartphone device to find evidence. The advantage of manual acquisition is that investigators do not require forensic tools to create acquisitions. Manual acquisition has constraints in terms of the integrity of the evidence as investigators will directly examine the evidence which may result in the possibility of data changes. In physical acquisition, the investigator will clone a smartphone device. The cloning results will then be analyzed using forensic tools. In logical acquisition, the investigator will perform the data acquisition found in the smartphone device to be subsequently analyzed.

In [9], authors performed forensic analyzes using Oxygen Forensic and MOBILedit. The researchers argue that every forensic tool has its own advantages and disadvantages. It can be handled using several forensic tools that have different capabilities in addressing cases related to smartphone devices. MOBILedit has advantages in terms of run time, while Oxygen Forensic has an advantage in terms of artifact analysis. In other research conducted by [10] using Oxygen Forensic tools managed to find artifacts of call logs, text messages, media files (photos, video, audio), internet data, geolocation, applications, and social media data. In [10], authors also explained that mobile forensic has several challenges, such as: malicious programs, lack of availability of tools, password recovery, accidental reset, and anti-forensic techniques.

In [11], authors performed comparisons and analysis of commercial forensic and open source tools. The tools put into comparison are TSK Autopsy, SIFT, MOBILedit, and Cellebrite UFED. The researcher believes that No. 1 forensic tool is perfect for performing all processes. Open source forensic tools have advantages in the number of users, flexibility in terms of use with console commands or GUI-based applications, logging capability, and good in tolerating errors. Meanwhile, commercial forensic tools are superior in terms of process speed, data extraction accuracy, and analytical skills. Commercial forensic tools also have the ability to restore deleted data. In [12], authors also conducted mobile forensic analysis using Celebrite UFED in order to determine the extent of forensic tool performance. In [12], authors obtained information on IMSI and ICCID. The artifacts, such as call logs, social media chat, contact list, email, SMS, and media files (audio, documents, image, video) also retrieved. In [12], authors added that each of the forensic tools has the possibility to produce different outputs. Therefore, an investigator should know what forensic tool he should use for a case.

The development of mobile technology and the large number of smartphone devices on the market become a challenge for investigators. One of the challenges of mobile forensics is the lack of resources in the sense that the rapid development of mobile technology and the growing number of smartphone devices are not put in a balance by the development of forensic mobile technology and the existing forensic tools [13].

NIST released a test plan to measure the performance of a forensic tool in a publication entitled "Mobile Device Tool Test Assertions and Test Plan ver. 2" and "Mobile Device Tool Specification ver. 2" [14], [15]. NIST argues that increasing the number of smartphone devices each year gives problems in forensics cases. Therefore, a method is needed to measure the ability of forensic tools on the market. NIST provides 42 measurement parameters and methods to measure the performance of forensic tools based on the results of each test plan.

Judging from the development of mobile technology and WhatsApp technology, WhatsApp's popularity, the possibility of cases involving WhatsApp, and previous research, the researcher conducted a comparative evaluation of forensic tools for WhatsApp analysis on Android-based smartphones. The forensic tools used are WhatsApp DB/Key Extractor, Belkasoft Evidence, and Oxygen Forensic. The performance and ability to perform WhatsApp forensic analysis from each forensic tool will be evaluated using the NIST forensic tool parameter and additional parameters from the researcher. The research' results will be used as a recommendation for investigators when handling cases related to WhatsApp.

II. METHODOLOGY AND TOOLS

The objective of this study was to evaluate forensic tools. WhatsApp DB/Key Extractor, Belkasoft Evidence and Oxygen Forensic will be evaluated based on parameters from NIST and additional parameters from researchers in terms of the ability to perform WhatsApp's forensic analysis on Android.

A. *Research Methodology*

The research used the steps as in Fig. 3. The steps of the research are divided into four: experiment simulation, forensic analysis, analysis result, and conclusion.

- Experiment Simulation: Fig. 4 shows the experimental simulations performed. User A's smartphone device will be used to communicate with User B and simulates the daily use of WhatsApp, such as sending messages, making calls, receiving pictures. User A's Smartphone then will be used for forensic analysis in the next step. User A's smartphone used in the research is Samsung Galaxy S4 GT-I9500 with Android Lollipop 5.0.1 operating system and it has been rooted. WhatsApp version used in this research is version 2.17.351.

- Forensic Analysis: The researches will perform forensic analysis on smartphone devices using the WhatsApp DB/Key Extractor, Belkasoft Evidence, and Oxygen Forensic. The forensic analysis will be conducted under closed conditions in the sense that smartphone devices will be converted into Airplane Mode to maintain data integrity.

- Result Analysis: The performance of each forensic tool will then be analyzed using NIST parameters and additional parameters from the researcher. The parameters used are adjusted to the objective of the research, namely, WhatsApp analysis.

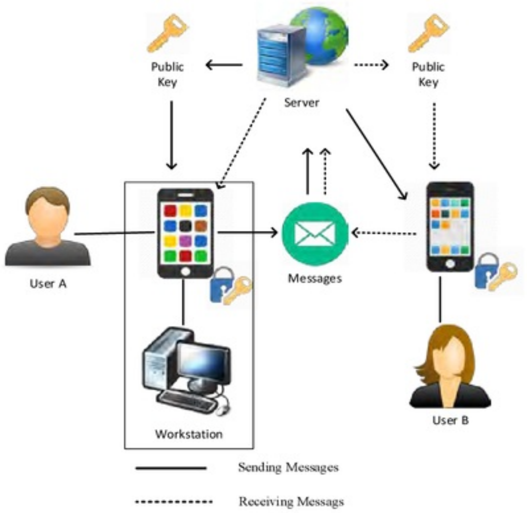


Fig. 3. Experiment simulation.

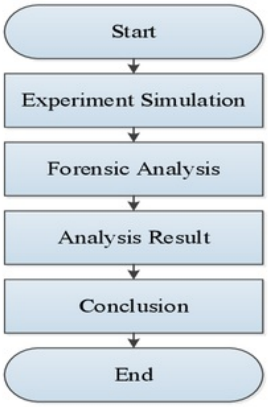


Fig. 4. Research methodology.

- Conclusion: The evaluation of forensic tools using NIST parameters and additional parameters are presented.

B. Research Tools

The research tools used in this research are divided into two: Experimental tools and forensic tools. Table I describes the experimental tools used in the research. Table II describes the forensic tools used in the research.

TABLE I. EXPERIMENT TOOLS

No	Experiment Tool	Description
1	Samsung Galaxy S4 GT-I9500	Android Lollipop 5.0.1, Rooted
2	WhatsApp	Instant Messaging application, Ver. 2.17.351
3	Workstation	Windows 7 64 Bit, Intel i5-4440, 4.00 GB RAM
4	USB Cable	Connecting smartphone to workstation

TABLE II. FORENSIC TOOLS

No.	Forensic Tool	Version	Description
1	WhatsApp DB/Key Extractor	4.7	Open source
2	Belkasoft Evidence (Trial ver)	8.4	Proprietary
3	Oxygen Forensic	6.4.0.67	Proprietary

TABLE III. NIST FORENSIC TOOL PARAMETERS

Core Assertions	Optional Assertions	Core Features Requirements	Optional Features Requirement
MDT-CA-01	MDT-AO-01	MDT-CR-01 A	MDT-RO-01 A
MDT-CA-02	MDT-AO-02	MDT-CR-02 A	MDT-RO-02 A
MDT-CA-03	MDT-AO-03	MDT-CR-03 A	MDT-RO-03 A
MDT-CA-04	MDT-AO-04		
MDT-CA-05	MDT-AO-05		
MDT-CA-06	MDT-AO-06		
MDT-CA-07	MDT-AO-07		
MDT-CA-08			
MDT-CA-09			

Here, the researcher used parameters from NIST as on Table III. NIST lists the measurement parameters of forensic tools on two written reports entitled "Mobile Device Tool Specification" and "Mobile Device Tool Test Assertions and Test Plan". The measurement parameters are divided into cores and optional. The division is done based on the type of acquisition made. Core leads to logical acquisition features and capabilities. Meanwhile, optional leads more to physical acquisition features and capabilities. In this research, the researcher does not include the parameters of MDT-CA-10 and the parameters on Universal Integrated Circuit Card (UICC) because the data on WhatsApp application are in the internal memory, not on UICC.

Researcher adds several additional measurement parameters as shown in Table IV. The additional parameters are more focused on the abilities of forensic tools to extract artifacts from WhatsApp for logical acquisition and physical acquisition. Additional parameters listed are essential for investigator during investigation related to WhatsApp.

TABLE IV. WhatsApp ARTIFACT

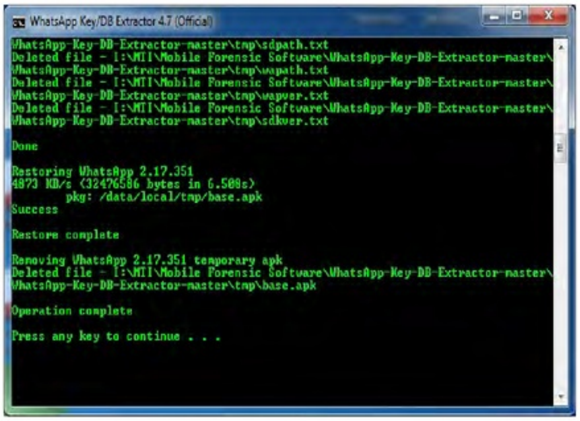
Artifact
Contact lists WhatsApp
Call Log WhatsApp
Text
Images
Video
Documents

III. Results and Discussion

A. WhatsApp DB/Key Extractor

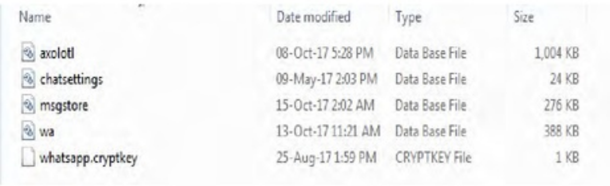
WhatsApp Key/DB Extractor can only conduct logical acquisition. Fig. 5 shows the acquisition process conducted using WhatsApp Key/DB Extractor. WhatsApp Key/DB Extractors have many shortcomings in terms of Core Assertions and Optional Assertions. Looking from experiment results, WhatsApp Key/DB Extractor did not get any information regarding smartphone devices, such as (International Mobile Equipment Identity) IMEI or (International Mobile Subscriber Identity) IMSI. From the NIST parameters used, WhatsApp Key/DB Extractor only succeeded in meeting the criteria of MDT-CA-07, MDT-CA-08, MDT-CR-01 A, and MDT-CR-03 A.

Fig. 6 shows the acquisition results located in the *WhatsApp-Key-DB-Extractor/extracted* folder. WhatsApp DB/ Key Extractor can only do data acquisition alone, thus opening the acquisition results need to use other tools. In the present research, Belkasoft Evidence is used to open the acquisition result of WhatsApp Key/DB Extractor. The *wa.db* file contains the WhatsApp's contact list. Contact information, for example contact names and contact numbers, can be found as shown in Fig. 7. Meanwhile, *msgstore.db* file contains the communication logs that are performed using WhatsApp. WhatsApp Key/DB Extractor manages to get the text message artifact as shown in Fig. 8. Message information such as message content, sender and recipient of message, timestamp, and file attachment can also be found. WhatsApp Key/DB Extractor can also do text acquisition in non-latin writing in accordance to MDT-CA-08. In this research, the researcher successfully retrieved Japanese letter for the experiment.



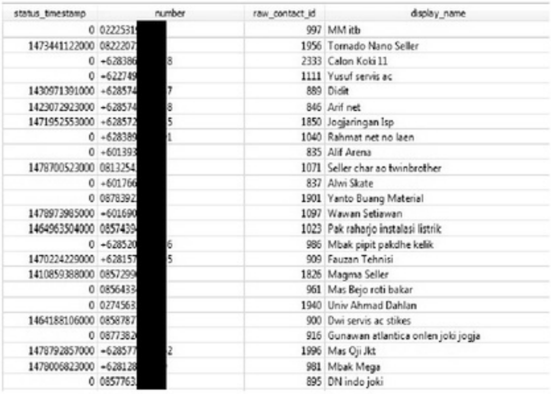
```
WhatsApp-Key-DB-Extractor-master\tmp\sdpath.txt
Deleted file - I:\MTI\Mobile Forensic Software\WhatsApp-Key-DB-Extractor-master\
WhatsApp-Key-DB-Extractor-master\tmp\wapath.txt
Deleted file - I:\MTI\Mobile Forensic Software\WhatsApp-Key-DB-Extractor-master\
WhatsApp-Key-DB-Extractor-master\tmp\wapver.txt
Deleted file - I:\MTI\Mobile Forensic Software\WhatsApp-Key-DB-Extractor-master\
WhatsApp-Key-DB-Extractor-master\tmp\sdkver.txt

Done

Restoring WhatsApp 2.17.351
4873 KB/s (32476586 bytes in 6.508s)
        pkg: /data/local/tmp/base.apk
Success

Restore complete

Removing WhatsApp 2.17.351 temporary apk
Deleted file - I:\MTI\Mobile Forensic Software\WhatsApp-Key-DB-Extractor-master\
WhatsApp-Key-DB-Extractor-master\tmp\base.apk

Operation complete

Press any key to continue . . .
```

Fig. 5. WhatsApp Key/DB extractor acquisition process.



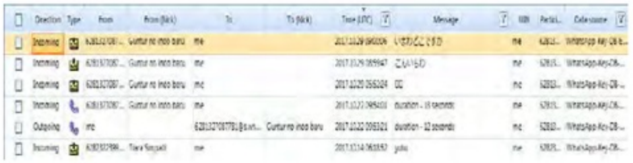
Name	Date modified	Type	Size
axolotl	08-Oct-17 5:28 PM	Data Base File	1,004 KB
chatsettings	09-May-17 2:03 PM	Data Base File	24 KB
msgstore	15-Oct-17 2:02 AM	Data Base File	276 KB
wa	13-Oct-17 11:21 AM	Data Base File	388 KB
whatsapp.cryptkey	25-Aug-17 1:59 PM	CRYPTKEY File	1 KB

Fig. 6. WhatsApp Key/DB extractor acquisition results.



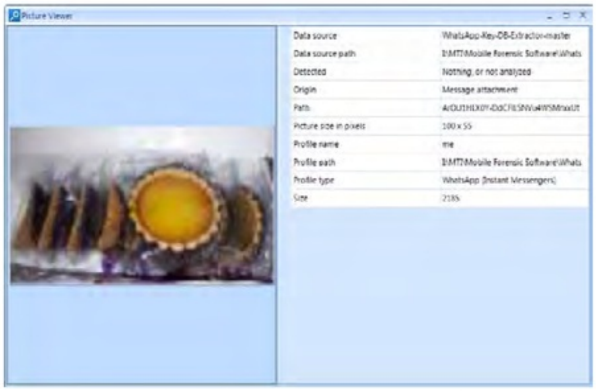
status_timestamp	number	raw_contact_id	display_name
0	022253[redacted]	997	MM itb
1473441122000	0822207[redacted]	1956	Tornado Nano Seller
0	+628386[redacted]8	2333	Calon Koki 11
0	+622749[redacted]	1111	Yusuf servis ac
1430971391000	+628574[redacted]7	889	Didit
1423072923000	+628574[redacted]8	846	Arif 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. 7. WhatsApp Key/DB extractor contact list.



Direction	Type	From	From (Nick)	To	To (Nick)	Time (UTC)	Message	UIN	Partici...	Data source
Incoming		6281327087...	Gunturno indo baru	me		2017.11.29 06:00:06	いちおここまで	me	6281...	WhatsApp Key DB E...
Incoming		6281327087...	Gunturno indo baru	me		2017.11.29 05:59:47	こんにちは	me	6281...	WhatsApp-Key-DB-...
Incoming		6281327087...	Gunturno indo baru	me		2017.10.26 05:52:24	口口	me	6281...	WhatsApp-Key-DB-...
Incoming		6281327087...	Gunturno indo baru	me		2017.10.22 09:54:01	duration - 18 seconds	me	6281...	WhatsApp-Key-DB-...
Outgoing		me		6281327087781@s.wh...	Gunturno indo baru	2017.10.22 09:53:21	duration - 12 seconds	me	6281...	WhatsApp-Key-DB-...
Incoming		6281327898...	Tiara Siregar	me		2017.11.14 06:10:57	yuks	me	6281...	WhatsApp-Key-DB-...

Fig. 8. Message artifact on WhatsApp Key/DB extractor.



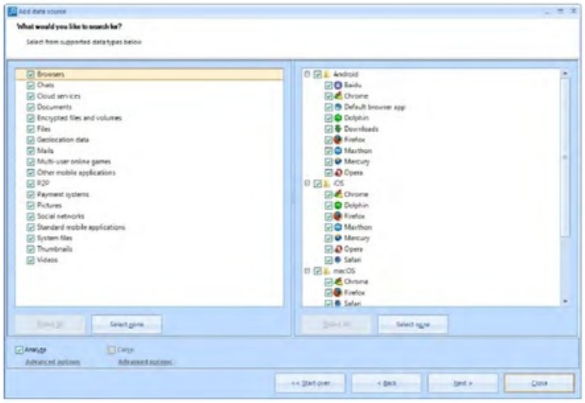
Data source	WhatsApp-Key-DB-Extractor-master
Data source path	I:\MTI\Mobile Forensic Software\Whats
Detected	Nothing, or not analyzed
Origin	Message attachment
Path	ArOU1HLX0Y-DdCFiLSNVu4WSMnaxUt
Picture size in pixels	100 x 55
Profile name	me
Profile path	I:\MTI\Mobile Forensic Software\Whats
Profile type	WhatsApp (Instant Messengers)
Size	2185

Fig. 9. WhatsApp Key/DB extractor image artifact.

WhatsApp Key/DB Extractor managed to get the image artifact with its metadata as shown in Fig. 9. Image artifacts can be zoomed but the zoomed image will blur out. WhatsApp/DB Key Extractor image artifact has a weakness in terms of resolution. The image artifact obtained has a small image resolution according to the thumbnail size in WhatsApp. The video and document artifacts cannot be obtained using WhatsApp Key/DB Extractor.

B. Belkasoft Evidence

Belkasoft Evidence has the ability to perform logical acquisition and physical acquisition. From the experimental results, Belkasoft Evidence almost meets all criteria of core parameters and optional NIST. Belkasoft Evidence provides information on smartphone devices, such as IMEI in accordance to NIST MDT-CA-06 parameters. Belkasoft Evidence is also accompanied by an option to select the data to be acquired individually or as a whole, as shown in Fig. 10 in accordance to the parameters of MDT-CA-01, MDT-CA-02, and MDT-CA-03. Investigators can choose what data needed for acquisition and will reduce acquisition run time. Fig. 11 shows the notification when there is a disruption to the acquisition process using Belkasoft Evidence. Notification feature during connection interruption is in accordance with MDT-CA-04 NIST parameter.


Add data source

What would you like to search for?

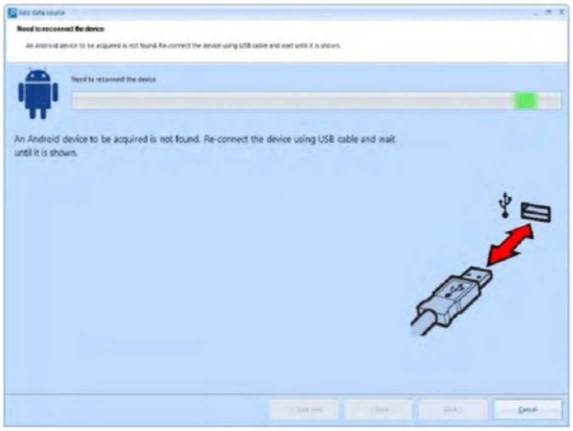
Select from supported data types below

- ☑ Browsers
- ☑ Chats
- ☑ Cloud services
- ☑ Documents
- ☑ Encrypted files and volumes
- ☑ Files
- ☑ Geolocation data
- ☑ Mails
- ☑ Multi-user online games
- ☑ Other mobile applications
- ☑ P2P
- ☑ Payment systems
- ☑ Pictures
- ☑ Social networks
- ☑ Standard mobile applications
- ☑ System files
- ☑ Thumbnails
- ☑ Videos

- ☑ Android
  - ☑ Baidu
  - ☑ Chrome
  - ☑ Default browser app
  - ☑ Dolphin
  - ☑ Downloads
  - ☑ Firefox
  - ☑ Maxthon
  - ☑ Mercury
  - ☑ Opera
- ☑ iOS
  - ☑ Chrome
  - ☑ Dolphin
  - ☑ Firefox
  - ☑ Maxthon
  - ☑ Mercury
  - ☑ Opera
  - ☑ Safari
- ☑ macOS
  - ☑ Chrome
  - ☑ Firefox
  - ☑ Safari

☑ Analyze   ☐ Carve

Fig. 10. Belkasoft evidence acquisition options menu.


Add data source

Need to reconnect the device

An Android device to be acquired is not found. Re-connect the device using USB cable and wait until it is shown.

Need to reconnect the device

An Android device to be acquired is not found. Re-connect the device using USB cable and wait until it is shown.

Fig. 11. Belkasoft evidence error notification.

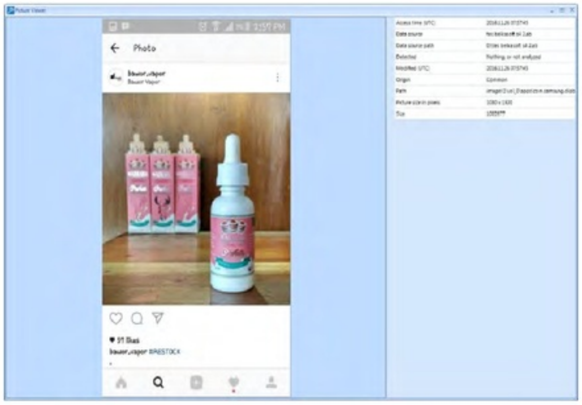

Access time (UTC)	[illegible]
Data source	[illegible]
Data source path	[illegible]
Detected	Nothing or not analyzed
Modified (UTC)	[illegible]
Origin	Common
Path	[illegible]
Picture size in pixels	1080 x 1920
Size	[illegible]

Fig. 12. Belkasoft evidence image artifact.

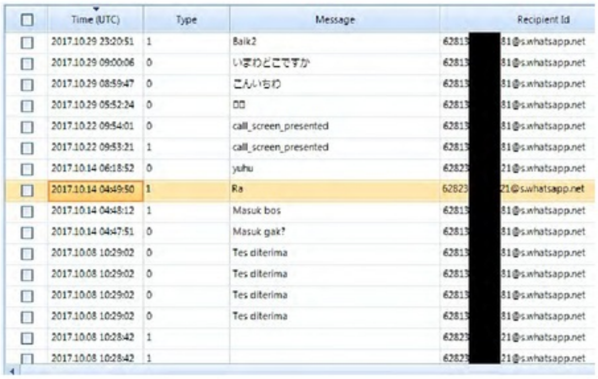

☐	Time (UTC)	Type	Message	Recipient Id
☐	2017.10.29 23:20:51	1	Baik2	62813[redacted]81@s.whatsapp.net
☐	2017.10.29 09:00:06	0	いまわどこですか	62813[redacted]81@s.whatsapp.net
☐	2017.10.29 08:59:47	0	こんいちわ	62813[redacted]81@s.whatsapp.net
☐	2017.10.29 05:52:24	0	□□	62813[redacted]81@s.whatsapp.net
☐	2017.10.22 09:54:01	0	call_screen_presented	62813[redacted]81@s.whatsapp.net
☐	2017.10.22 09:53:21	1	call_screen_presented	62813[redacted]81@s.whatsapp.net
☐	2017.10.14 06:18:52	0	yuhu	62823[redacted]21@s.whatsapp.net
☐	2017.10.14 04:49:50	1	Ra	62823[redacted]21@s.whatsapp.net
☐	2017.10.14 04:48:12	1	Masuk bos	62813[redacted]81@s.whatsapp.net
☐	2017.10.14 04:47:51	0	Masuk gak?	62813[redacted]81@s.whatsapp.net
☐	2017.10.08 10:29:02	0	Tes diterima	62813[redacted]81@s.whatsapp.net
☐	2017.10.08 10:29:02	0	Tes diterima	62813[redacted]81@s.whatsapp.net
☐	2017.10.08 10:29:02	0	Tes diterima	62813[redacted]81@s.whatsapp.net
☐	2017.10.08 10:29:02	0	Tes diterima	62813[redacted]81@s.whatsapp.net
☐	2017.10.08 10:28:42	1		62823[redacted]21@s.whatsapp.net
☐	2017.10.08 10:28:42	1		62823[redacted]21@s.whatsapp.net

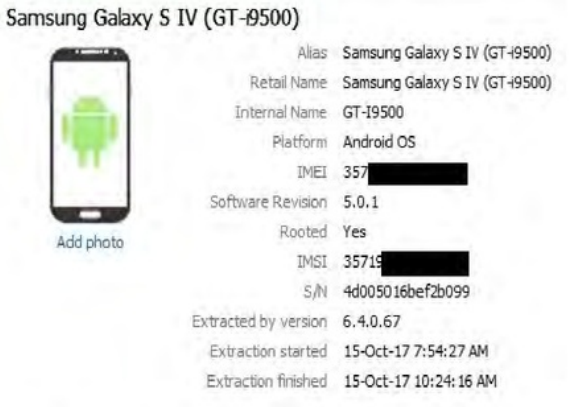
Fig. 13. Belkasoft evidence message artifact.

In logical acquisition, Belkasoft Evidence failed to retrieve contact list artifact of WhatsApp, WhatsApp call log, and text messages. The researcher only managed to find images, video, and document artifacts. Video and document artifact files can be opened, simplifying the analysis process. Fig. 12 shows image artifact obtained using Belkasoft Evidence. The image artifact obtained comes with considerably large pixel resolution, so that it not blurred when being zoomed in.

Text message artifact is successfully obtained using the physical acquisition Belkasoft Evidence as in Fig. 13. The timestamp information, the contact number of the sender and the recipient of the message can be found. Japanese letter used for experiment and successfully read by Belkasoft Evidence in accordance with NIST MDT-AO-06 parameter.

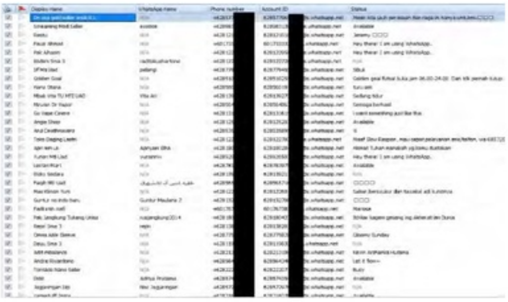
C. Oxygen Forensic

Just like Belkasoft Evidence, Oxygen Forensic has the ability to perform logical acquisition and physical acquisition. Oxygen Forensic successfully obtains smartphone device information as shown in Fig. 14. Information regarding IMEI and IMSI is able to obtain according to NIST MDT-CA-06 parameter. Oxygen Forensic only has one feature to choose entire data acquisition according to NIST parameter MDT-CA-01, and does not have feature to individually select the data to be acquired.


Samsung Galaxy S IV (GT-i9500)

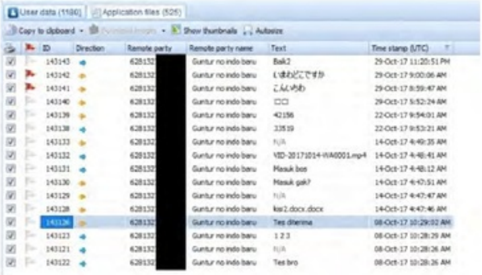
Alias	Samsung Galaxy S IV (GT-i9500)
Retail Name	Samsung Galaxy S IV (GT-i9500)
Internal Name	GT-I9500
Platform	Android OS
IMEI	357[redacted]
Software Revision	5.0.1
Rooted	Yes
IMSI	35719[redacted]
S/N	4d005016bef2b099
Extracted by version	6.4.0.67
Extraction started	15-Oct-17 7:54:27 AM
Extraction finished	15-Oct-17 10:24:16 AM

Fig. 14. Oxygen forensic smartphone information.



Display name	WhatsApp name	Phone number	Account ID	Status
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	[illegible] □□□
[illegible]	[illegible]	[redacted]	[redacted]@s.whatsapp.net	Available
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	Jeremy □□□
Fauzi Ahmad	N/A	[redacted]	[redacted]@s.whatsapp.net	Hey there! I am using WhatsApp.
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	Hey there! I am using WhatsApp.
[illegible] Sma 3	[illegible]	[redacted]	[redacted]@s.whatsapp.net	N/A
[illegible]	pelangi	[redacted]	[redacted]@s.whatsapp.net	Sibuk
Golden Goal	N/A	[redacted]	[redacted]@s.whatsapp.net	Golden goal futsal buka jam 06.00-24.00 Dan tdk pernah tutup
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	[illegible]
[illegible]	Vita Ari	[redacted]	[redacted]@s.whatsapp.net	Sedang tidur
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	Semoga berhasil
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	I want something just like this
Angie Shop	N/A	[redacted]	[redacted]@s.whatsapp.net	Available
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	9
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	[illegible]
[illegible]	[illegible]	[redacted]	[redacted]@s.whatsapp.net	[illegible]
[illegible]	[illegible]	[redacted]	[redacted]@s.whatsapp.net	Hey there! I am using WhatsApp.
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	Available
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	N/A
[illegible]	[illegible]	[redacted]	[redacted]@s.whatsapp.net	□□□□
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	[illegible]
Guntur no indo baru	Guntur Maulana 2	[redacted]	[redacted]@s.whatsapp.net	□□□
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	[illegible]
[illegible]	[illegible]	[redacted]	[redacted]@s.whatsapp.net	[illegible]
[illegible]	[illegible]	[redacted]	[redacted]@s.whatsapp.net	N/A
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	Gloomy Sunday
[illegible] Sma 3	N/A	[redacted]	[redacted]@s.whatsapp.net	N/A
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	[illegible]
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	Let it flow~
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	Busy
[illegible]	[illegible]	[redacted]	[redacted]@s.whatsapp.net	Available
[illegible]	[illegible]	[redacted]	[redacted]@s.whatsapp.net	N/A
[illegible]	N/A	[redacted]	[redacted]@s.whatsapp.net	Available

Fig. 15. Oxygen forensic contact list artifact.



ID	Direction	Remote party	Remote party name	Text	Time stamp (UTC)
143143		628132[redacted]	Guntur no indo baru	Baik2	29-Oct-17 11:20:51 PM
143142		628132[redacted]	Guntur no indo baru	いまどこですか	29-Oct-17 9:00:06 AM
143141		628132[redacted]	Guntur no indo baru	こんいちわ	29-Oct-17 8:59:47 AM
143140		628132[redacted]	Guntur no indo baru	□□	29-Oct-17 5:52:24 AM
143139		628132[redacted]	Guntur no indo baru	42156	22-Oct-17 9:54:01 AM
143138		628132[redacted]	Guntur no indo baru	33519	22-Oct-17 9:53:21 AM
143133		628132[redacted]	Guntur no indo baru	N/A	14-Oct-17 4:49:35 AM
143132		628132[redacted]	Guntur no indo baru	VID-20171014-WA0001.mp4	14-Oct-17 4:48:41 AM
143131		628132[redacted]	Guntur no indo baru	Masuk bos	14-Oct-17 4:48:12 AM
143130		628132[redacted]	Guntur no indo baru	Masuk gak?	14-Oct-17 4:47:51 AM
143129		628132[redacted]	Guntur no indo baru	N/A	14-Oct-17 4:47:47 AM
143128		628132[redacted]	Guntur no indo baru	kai2.docx.docx	14-Oct-17 4:47:46 AM
143126		628132[redacted]	Guntur no indo baru	Tes diterima	08-Oct-17 10:29:02 AM
143123		628132[redacted]	Guntur no indo baru	1 2 3	08-Oct-17 10:28:29 AM
143121		628132[redacted]	Guntur no indo baru	N/A	08-Oct-17 10:28:26 AM
143122		628132[redacted]	Guntur no indo baru	Tes bro	08-Oct-17 10:28:26 AM

Fig. 16. Oxygen forensic message artifact.

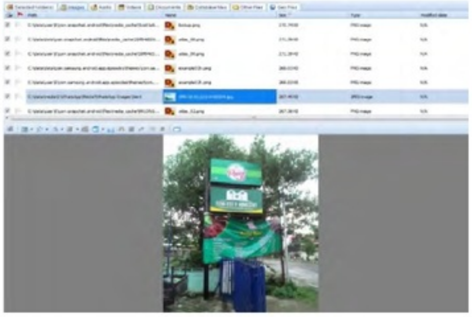


Fig. 17. oxygen forensic image artifact.

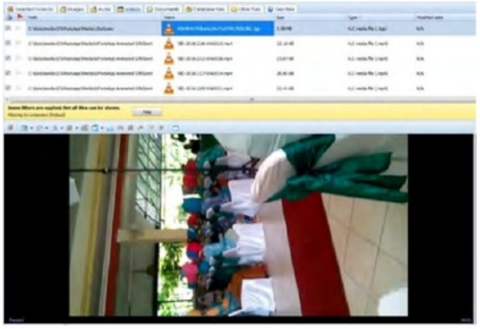


Fig. 18. Oxygen forensic video artifact.

Fig. 15 shows WhatsApp contact list artifacts obtained using Oxygen Forensic. Contact name and contact number information can be determined and can be used to assist in the investigation process. From the logical acquisition and physical acquisition, text message artifact can be generated as in Fig. 16. Information such as message sender, message recipient, message content, and timestamp is successfully obtained. Text messages in non-Latin writing are also successfully read by Oxygen Forensic according to NIST parameters MDT-CA-08 and MDT-AO-06.

Oxygen Forensic also manages to obtain document, image, and video artifacts. Fig. 17 indicates the image artifacts successfully obtained by Oxygen Forensic. The image artifacts obtained have sufficiently good quality that they do not blur when the image is zoomed in to see them more clearly.

Oxygen Forensic managed to retrieve video artifacts. The video artifacts obtained by using Oxygen Forensic can be played so that it can help the investigation process if video file content is necessary to be viewed as in Fig. 18. Information regarding file names, video format, and video size can be found.

D. Discussion

The researcher used calculations with index numbers to determine the performance of each forensic tool in accordance with the experiment results. The calculation of index number used is unweighted index as shown in (1). Table V indicates the evaluation results of forensic tools using NIST measurement parameters and additional parameters from the researcher.

$$Pon = \frac{\sum Pn}{\sum Po}\ x\ 100\% \qquad (1)$$

Equation (1) used to calculate the index number from each forensic tool. WhatsApp Key/DB Extractor has an index number of 23.52%. Belkasoft Evidence has an index number of 88.23%. Oxygen Forensic has an index number of 82.35%.

WhatsApp Key/DB Extractor is only capable of conducting logical acquisition and requires another tool to read WhatsApp Key/DB Extractor acquisition result. However, WhatsApp Key/DB Extractor successfully obtained WhatsApp Contact List Artifacts, WhatsApp call log, text messages, and images. The image artifacts obtained have a thumbnail size pixel resolution, which will blurry when being zoomed in.

From experimental results using Belkasoft Evidence, all core parameters and optional NIST are almost met entirely. Belkasoft Evidence did not meet the parameters of MDT-CA-08 for failing to get message artifacts in non-Latin writing. Logical acquisition using Belkasoft Evidence cannot successfully get the contact list artifact on WhatsApp, WhatsApp call log, and text messages. However, document, image and video artifacts are successfully obtained and can be opened to assist the investigation process.

Similar to Belkasoft Evidence, Oxygen Forensic is able to perform logical acquisition and physical acquisition. Oxygen Forensic has disadvantage in terms of options for selecting data to be acquired. Oxygen Forensic cannot individually select the data to be acquired. From the experiments, Oxygen Forensic did not have any notification feature to notify investigators when connection problem occurs during acquisition process. Oxygen Forensic successfully obtained all artifacts according to parameters, either with logical acquisition or physical acquisition.

TABLE V. EVALUATION RESULTS

Measurement Parameter		**Forensic Tools**		
		WhatsApp DB/Key Extractor	***Belkasoft Evidence (Trial ver)***	***Oxygen Forensic***
Core Assertions	MDT-CA-01	-	√	√
	MDT-CA-02	-	√	-
	MDT-CA-03	-	√	-
	MDT-CA-04	-	√	-
	MDT-CA-05	-	√	√
	MDT-CA-06	-	√	√
	MDT-CA-07	√	√	√
	MDT-CA-08	√	-	√
	MDT-CA-09	-	√	√
Optional Assertions	MDT-AO-01	-	√	√
	MDT-AO-02	-	√	-
	MDT-AO-03	-	√	√
	MDT-AO-04	-	√	√
	MDT-AO-05	-	√	√
	MDT-AO-06	-	√	√
	MDT-AO-07	-	√	√
Core Features Requirements	MDT-CR-01 A	√	√	√
	MDT-CR-02 A	-	√	-
	MDT-CR-03 A	√	√	√
Optional Features Requirements	MDT-RO-01 A	-	√	√
	MDT-RO-02 A	-	√	-
	MDT-RO-03 A	-	√	√
Logical Acquisition Artifact	WhatsApp Contact List	√	-	√
	WhatsApp Call Log	√	-	√
	Text	√	-	√
	Image	√	√	√
	Video	-	√	√
	Document	-	√	√
Physical Acquisition Artifact	WhatsApp Contact list	-	√	√
	WhatsApp Call Log	-	√	√
	Text	-	√	√
	Image	-	√	√
	Video	-	√	√
	Document	-	√	√

IV. CONCLUSION

Belkasoft has the highest index number at 88.23%, followed by Oxygen Forensic with index number at 82.35%, and WhatsApp DB/ Key Extractor with index number at 23.52%. WhatsApp Key/DB Extractor has weakness in keeping up with the NIST parameter criteria. However, WhatsApp Key/DB Extractor manages to get text message artifacts, WhatsApp contact lists, and WhatsApp call logs using logical acquisition. WhatsApp Key/DB Extractor also has superiority in terms of cost because it is an open source forensic tool. Belkasoft Evidence has the highest index number among the three forensic tools used. Belkasoft Evidence almost meets all the NIST parameters. Belkasoft Evidence has an obstacle in obtaining WhatsApp artifacts using logical acquisition. With logical acquisition, Belkasoft Evidence is unable to get WhatsApp contact list artifacts, WhatsApp call logs, and text messages. Oxygen Forensic has weakness in terms of options to select data for acquisition and notification if there is a connection disruption during the acquisition process. Oxygen Forensic successfully fulfills all WhatsApp artifact parameters with logical acquisition and physical acquisition. Despite Belkasoft Evidence having the highest index number and WhatsApp Key/DB Extractor superiority in terms of cost, Oxygen Forensic is more superior in obtaining WhatsApp artifacts, either through logical acquisition or physical acquisition.

REFERENCES

[1] Statista, "Global smartphone sales to end users from 1st quarter 2009 to 1st quarter 2017, by operating system (in million units)," 2017. [Online]. Available: https://www.statista.com/statistics/266219/global-smartphone-sales-since-1st-quarter-2009-by-operating-system/. [Accessed: 10-Nov-2017].

[2] "REVEALED: Top uses of our smartphones and calling doesn't even make the list," 2017. [Online]. Available: revealed: Top uses of our smartphones - and calling doesn't even make the list%0A%0A. [Accessed: 10-Nov-2017].

[3] T. Sutikno, L. Handayani, D. Stiawan, M. A. Riyadi, and I. M. I. Subroto, "WhatsApp, viber and telegram: Which is the best for instant messaging?," Int. J. Electr. Comput. Eng., vol. 6, no. 3, pp. 909–914, 2016.

[4] Statista, "Number of monthly active WhatsApp users worldwide from April 2013 to July 2017 (in millions)," 2017. [Online]. Available: https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/. [Accessed: 10-Nov-2017].

[5] J. Koum and B. Acton, "End-to-end encryption," 2016. [Online]. Available: https://blog.whatsapp.com/10000618/end-to-end-encryption. [Accessed: 10-Nov-2017].

[6] B. Bennet, "With Islamic State using instant messaging apps, FBI seeks access to data," Los Angeles Times, 2015. [Online]. Available: http://www.latimes.com/world/middleeast/la-fg-terror-messaging-20150608-story.html. [Accessed: 17-Nov-2017].

[7] R. Ayers, W. Jansen, and S. Brothers, "Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1)," NIST Spec. Publ., vol. 1, no. 1, p. 85, 2014.

[8] N. R. Roy, A. K. Khanna, and L. Aneja, "Android phone forensic: Tools and techniques," Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA 2016, pp. 605–610, 2017.

[9] S. Dogan and E. Akbal, "Analysis of Mobile Phones in Digital Forensics," MIPRO 2017, pp. 1241–1244, 2017.

[10] G. M. Jones and S. G. Winster, "Forensics Analysis On Smart Phones Using Mobile Forensics Tools," Int. J. Comput. Intell. Res., vol. 13, no. 8, pp. 1859–1869, 2017.

[11] I. Technology, R. Padmanabhan, K. Lobo, M. Ghelani, D. Sujan, and M. Shirole, "Comparative Analysis of Commercial and Open Source Mobile Device Forensic Tools," 2014.

[12] T. B. Tajuddin and A. A. Manaf, "Forensic investigation and analysis on digital evidence discovery through physical acquisition on smartphone," 2015 World Congr. Internet Secur. WorldCIS 2015, pp. 132–138, 2015.

[13] D. M. Sai, N. R. G. K. Prasad, and S. Dekka, "The Forensic Process Analysis of Mobile Device," Int. J. Comput. Sci. Inf. Technol., vol. 6, no. 5, pp. 4847–4850, 2015.

[14] National Institute of Standards and Technology, "Mobile Device Tool Test Assertions and Test Plan Version 2.0," 2016.

[15] National Institute of Standards and Technology, "Mobile Device Tool Specification Version 2.0," 2016.

A Comparative Study of Forensic Tools For WhatsApp Analysis Using NIST Measurements

ORIGINALITY REPORT

9%

SIMILARITY INDEX

PRIMARY SOURCES

1	icbbd2017.globalconf.org Internet	28 words — 1%
2	www.ncjrs.gov Internet	25 words — 1%
3	jubilaeumsportrait.de Internet	25 words — 1%
4	Sascha Alpers, Andreas Oberweis, Maria Pieper, Stefanie Betz, Andreas Fritsch, Gunther Schiefer, Manuela Wagner. "PRIVACY-AVARE: An approach to manage and distribute privacy settings", 2017 3rd IEEE International Conference on Computer and Communications (ICCC), 2017 Crossref	20 words — < 1%
5	droidors.com Internet	20 words — < 1%
6	Jana Uramova, Pavel Segec, Marek Moravcik, Jozef Papan, Tomas Mokos, Marek Brodec. "Packet capture infrastructure based on Moloch", 2017 15th International Conference on Emerging eLearning Technologies and Applications (ICETA), 2017 Crossref	19 words — < 1%
7	www.ijcst.com Internet	18 words — < 1%
8	K.-K.R. Choo, A. Dehghantanha. "Contemporary Digital Forensics Investigations of Cloud and	17 words — < 1%

	Mobile Applications", Elsevier BV, 2017 Crossref	
9	www.cs.cf.ac.uk Internet	16 words — < 1%
10	Taniza Binti Tajuddin, Azizah Abd Manaf. "Forensic investigation and analysis on digital evidence discovery through physical acquisition on smartphone", 2015 World Congress on Internet Security (WorldCIS), 2015 Crossref	15 words — < 1%
11	Saurav Yadav, Aviral Apurva, Pranshu Ranakoti, Shashank Tomer, Nihar Ranjan Roy. "Android vulnerabilities and security", 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), 2017 Crossref	15 words — < 1%
12	www.strategicstudiesinstitute.army.mil Internet	15 words — < 1%
13	Alan J. Reid. "Chapter 2 A Brief History of the Smartphone", Springer Nature America, Inc, 2018 Crossref	15 words — < 1%
14	dblp.dagstuhl.de Internet	14 words — < 1%
15	www.express.co.uk Internet	14 words — < 1%
16	Radhika Padmanabhan, Karen Lobo, Mrunali Ghelani, Dhanika Sujan, Mahesh Shirole. "Comparative analysis of commercial and open source mobile device forensic tools", 2016 Ninth International Conference on Contemporary Computing (IC3), 2016 Crossref	14 words — < 1%
17	cco.ndu.edu Internet	13 words — < 1%

18	www.matec-conferences.org Internet	13 words — < 1%
19	www.faqs.org Internet	13 words — < 1%
20	mti.uad.ac.id Internet	12 words — < 1%
21	ijain.org Internet	11 words — < 1%
22	www.thingser.com Internet	10 words — < 1%
23	Ping Wang, Matt Rosenberg, Hubert D’Cruze. "Chapter 13 Integration of Mobile Forensic Tool Capabilities", Springer Nature America, Inc, 2018 Crossref	9 words — < 1%

EXCLUDE QUOTES	OFF	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	OFF		