View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Kinetik: Game Technology, Information System, Computer Network, Computing,...

Instant Messaging Forensic Tools Comparison on Android Operating System

Guntur Maulana Zamroni[*1], **Imam Riadi**[2]
[1]Universitas Ahmad Dahlan/Department of Informatics Engineering
[2]Universitas Ahmad Dahlan/Department of Information System
guntur.zamroni@tif.uad.ac.id[*1], imam.riadi@is.uad.ac.id[2]

Abstract

WhatsApp (WA) is one of the Instant Messaging (IM) applications used by many people. WA and mobile devices cannot be separated from the possibility of misuse such as for criminal purposes. To handle a crime case involving a mobile device, the investigator needs to use suitable forensic tools and mobile forensic methodology so that the results can be approved and accepted by the law. This research conducted a forensic analysis of WA on unrooted Samsung C9 Pro devices using Belkasoft Evidence, Oxygen Forensic, Magnet AXIOM, and WA Key/DB Extractor. This research gives suggestion about forensic tools for conducting forensic analysis related to WA. WA artifacts that could be used as a crime evidence such as chat messages, logs, contact list, and files are used as a parameters. From the research can be seen that there is no tool that can be used to obtain all the WA artifact parameters used in the research. The combination of the Magnet AXIOM and WA Key/DB Extractor is known to get the best results and meets the WA artifact parameters.

Keywords: *Artifacts, Instant Messaging, Mobile Forensics, WhatsApp*

1. Introduction

WhatsApp (WA) is a popular Instant Messaging (IM) application. WA ranks first among the IM applications seen from the number of users. Until October 2018, WA has a total of 1.5 billion users per month as shown in Figure 1 [1], [2]. The highest number of WA users is in India with 160 million users [3]. In Indonesia WA is also the most popular IM application with 35,799,000 users [4]. WA has features for exchanging text messages, images, videos and documents. WA is also capable of making voice call and video call calls.

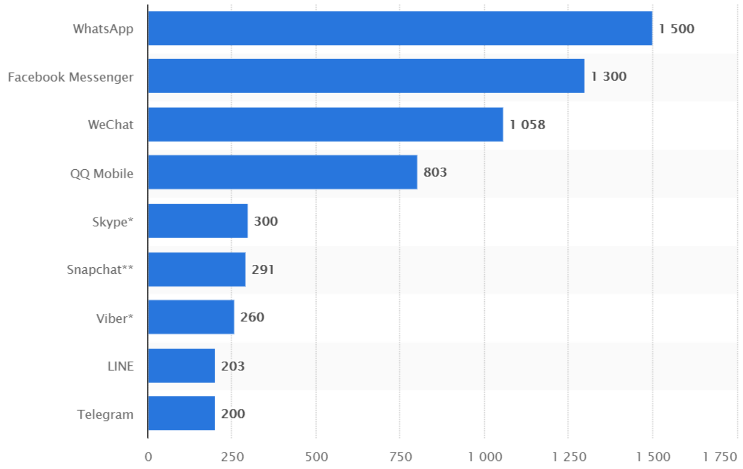


Figure 1. Number of Active WA Users Monthly [1]

WA has been equipped with an encryption feature that makes the messages or communications carried out using WA can only be read by the sender or recipient of WA communications [5]. Someone can intercept WA communications, but will not be able to read the contents of the message because it has been encrypted. Along with the growing number of users and technology in WA, there have been several cases involving WA applications, either as a tool

Zamroni, G., & Riadi, I. (2019). Instant Messaging Forensic Analysis on Android Operating System. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 4(2). doi:http://dx.doi.org/10.22219/kinetik.v4i2.735
Receive December 20, 2018; Revise March 09, 2019; Accepted March 13, 2019

for crime or as evidence of crime. There has been crimes related to WA such as sexual abuse and child pornography, cyberbullying, harassment, sharing music and images illegally, drugs trafficking, human smuggling, hacking, and data stealing [6], [7], [8]. In Indonesia, investigators managed to solved a crimes using WA conversation as an evidence [9].

Mobile forensics is needed to conduct forensic analysis relating to evidence in the form of a mobile device. Mobile forensics methodology is a framework or steps to carry out forensic analysis processes on mobile devices using steps and tools that are forensically tested so the results of the obtained forensic processes can be recognized in the eyes of the law, which are data integrity and free of contamination [10]. A forensic framework or methodology is needed to ensure the integrity of the obtained evidence. The integrity of the evidence can be maintained if the forensic process carried out does not affect or change the data from the results of the forensic process. Forensic methodology is also needed to reduce the possibility of damage to evidence due to mistakes when conducting forensic analysis process because the data inside mobile devices is very vulnerable to loss or damage [11]. The National Institute of Standards and Technology (NIST) offered a methodology as shown in Figure 2 [12]. The methodology has 4 stages, which are Collection, Examination, Analysis, and Reporting.

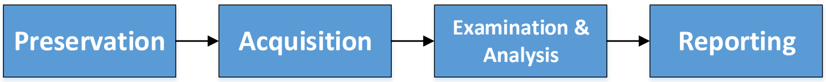


Figure 2. NIST Mobile Forensic Methodology [12]

There have been several studies related to IM forensic analysis, WA applications, and mobile devices. Reference [13] performed forensic analysis of WA applications on iPhone devices with the iOS 5.0.1 operating system using Forensic Oxygen and UFED Cellebrite. From the results of experiments conducted it can be seen that although Oxygen Forensic has the access to the limited devices compared to UFED Cellebrite in terms of Web History, Cookies, Passwords, User Accounts, and Web Bookmarks, Oxygen Forensic has the advantage of getting more information about the WA application.

Reference [14] conducted a survey of mobile forensic devices for Android devices. The forensic tools that are compared are Android Debug Bridge, Open Source Android Forensics, Andriller, AFLogical, WA Extract, and Skype Extractor. Researchers added that Android devices have dominated the smartphone market. For this reason, an understanding and solution are needed to investigate Android devices. Knowing the type of software and hardware from an Android device is crucial to determine the type of forensic tools that will be used to conduct an investigation.

Reference [15] conducted forensic analysis using forensic Oxygen Forensic and MOBILedit. From the research can be seen that MOBILedit has a faster performance than Oxygen Forensic. The researcher also argues that live analysis is not recommended in the process of investigating a case involving a smartphone device because it can damage the evidence. Each forensic tool has its own strengths and weaknesses. For this reason, it is necessary to use more than one forensic tool in handling a case.

Reference [16] performed the validation tests of the forensic tools namely WA Key / DB Extractor 4.7 and Belkasoft Evidence with the results that the forensic tools used has successfully fulfilled the Samsung Galaxy S4 artifact validation test. Even though they do not succeed in getting all the artifacts, the forensic tools are stated to fulfill repeatability and reproducibility tests because researchers found some artifacts that were similar and same number of artifacts.

Reference [17] conducted forensic analysis of Line applications on Sony Xperia Z devices using Oxygen Forensic and MOBILedit. The researcher used NIST forensic methodology to conduct forensic analysis. From the research it is known that MOBILedit has a better performance than Oxygen Forensic.

Reference [12] describes several types of mobile device artifacts that have the potential to be used as evidence, including the following: cellular service provider information, mobile device information, date & time, contact list, calendar information, text messages, call logs, e -mail, photos, audio, IM applications, browsing activities, geolocation, and others. Reference [12] also classified mobile forensics into five types according to the level of acquisition and the level of complexity. The purpose of this grouping is to make it easier for investigators to classify and compare the processes and results of acquisition of each forensic tool. Figure 3 shows the level of acquisition capability of a forensic tools [12]. The higher the level of acquisition, the more complicated the acquisition process will be.

1. Manual Extraction
   Investigators will conduct analysis by make a direct contact to mobile devices. Investigators will read, write, and taking images of what is displayed on mobile devices' screen.
2. Logical Extraction
   Logical extraction is conducted when investigators do not have root access to mobile devices. Logical extraction become a basic feature on most forensic tools.
3. Hex Dumping/JTAG
   Hex Dumping/JTAG also called as physical extraction is conducted when investigators have root access to mobile devices. Deleted data can be retrieved by using physical extraction.
4. Chip-Off
   Chip-Off used when mobile device is broken. Mobile device's chip will be taken out and put into other mobile device so investigators can read data inside that chip.
5. Micro Read
   Investigators will collect mobile device's chip and read it using high powered microscope.

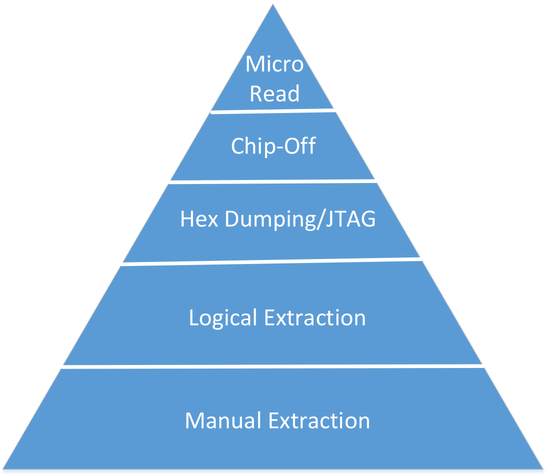


Figure 3. Forensic Tools Classification [12]

In order for the results of the mobile forensic analysis process to be accepted by the law, forensic analysis and forensic tools that will be used must meet the validation test. Validation test is needed to test whether the results of the obtained forensic process are correct, accurate, credible, and maintain the data integrity. The law will not acknowledge forensic results if forensic tools used for analysis do not meet validation test because the data integrity will be questionable. There are two types of validation tests: repeatability and reproducibility [12], [18].

1. Repeatability
   Forensic process is carried out repeatedly in the adjacent time using the same research methods, research objects, and research tools. Repeatability test aimed to check whether forensic tool gives constant and identical results.
2. Reproducibility
   Forensic process is carried out repeatedly in the adjacent time using the same research methods, research objects and different research tools. Reproducibility test aimed to check whether each forensic tool gives identical results.

The fast development of mobile technology that is not followed by the development of forensic tools technologies become one of the obstacles often faced by an investigator when handling a case related to mobile devices [19]. Reference [20] added that mobile forensic has several other challenges such as: malicious programs, mobile device security features, possibility of human errors, and anti-forensic techniques.

From the explanation above, the researcher conducted an analysis of forensic devices available on the market to conduct mobile forensic analysis of WA applications on Samsung C9 Pro devices that is using Android 7.0 Nougat operating system in unrooted condition. This research aims to see whether the currently available forensic tools are able to carry out forensic analysis of WA application on Samsung C9 Pro devices and the outcome can be used as a reference for investigators when handling with a case related to WA. This research used NIST forensic methodology with parameters in the form of WA artifacts that can be used as an evidence. The difference between this research and previous researches is that this research is conducted on different objects and the latest Android 7.0 Nougat operating system.

2. Research Method

This research aims to conduct forensic analysis of WA applications on Samsung C9 Pro devices and test the ability of forensic tools to obtain WA artifacts. Forensic tools used are Belkasoft Evidence, Oxygen Forensic, Magnet AXIOM, and WA Key/DB Extractor.

2.1 Methodology

Figure 4 shows the stages used in this research. The research steps are divided into four: WA Activities Simulation, Forensic Analysis, Forensic Results Analysis, and finally Conclusion.

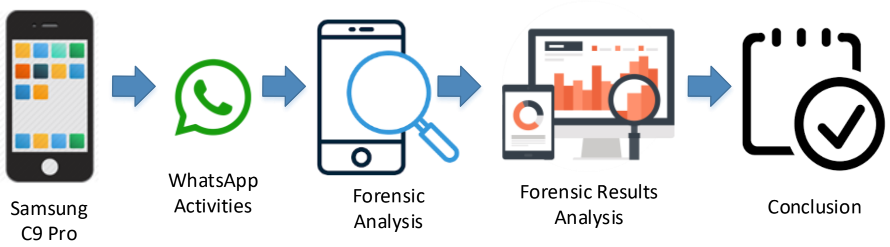


Figure 4. Research Stages

1. WA Activities Simulation
   At this stage the researcher simulates daily WA usage such as chatting, sending and receiving files, making voice call or video call, and so on.
2. Forensic Analysis
   At this stage the researcher conducts forensic analysis of the WA application using the Belkasoft Evidence, Oxygen Forensic, Magnet AXIOM, and WA Key/DB Extractor forensic tools. The NIST mobile forensic methodology is used as a framework for conducting forensic analysis. NIST mobile forensic methodology has four stages: preservation, acquisition, examination & analysis, and reporting.
   - Preservation is the process of securing evidence and maintaining data security in it. The evidence is received and taken over during ownership of the forensic analysis process. The smartphone device is then isolated from communication using Faraday Bag or by changing the status of the smartphone into Airplane Mode.
   - In the Acquisition stage, a smartphone device is identified to find information about the type of smartphone, the type of evidence taken, the type of software and hardware, to be later proceeded with the preparation of the object of research and preparation of research tools for the following forensic processes. Acquisition process conducted using logical acquisition because Samsung C9 Pro was in unrooted condition.
   - At the examination & analysis stage, the decrypted and extracted data will then be examined and analyzed to find information that can be used as evidence to assist the investigation process. This information can be in the form of contact numbers, time, text messages, geolocation, images, videos, calendars, and others.
   - The final stage of the forensic analysis process is reporting. Reporting can be in written reports such as documentation or oral reports in the form of presentations. In the Reporting stage all forensic processes are explained from the beginning of the preservation process to the end, along with the results and conclusions of the analysis.
3. Forensic Results Analysis
   The researcher performed tests of the forensic results. First, the researcher conducted the validation tests which are divided into two: repeatability and reproducibility. The researcher then analyzed forensic tools acquisition results using parameters. The research parameters used are WA artifacts which might be used as an evidence of a crime as in Table 1.
4. Conclusion
   The researcher explained the conclusions from the conducted research.

Table 1. WA Artifact Parameters

Artifact Type
Chat
Image
Video
Document
Contact List
WA Log

2.2 Materials

The research materials used can be divided into two categories: hardware and software. Table 2 shows the types of hardware used in the research. Table 3 shows the types of software used in this research.

Table 2. Hardware Requirements

No	Hardware	Description
1	Workstation	Used for forensic analysis
2	Samsung C9 Pro	Research object. Equipped with Android 7.0 Nougat Operating System, Unrooted Condition
3	USB Connector	Connector device

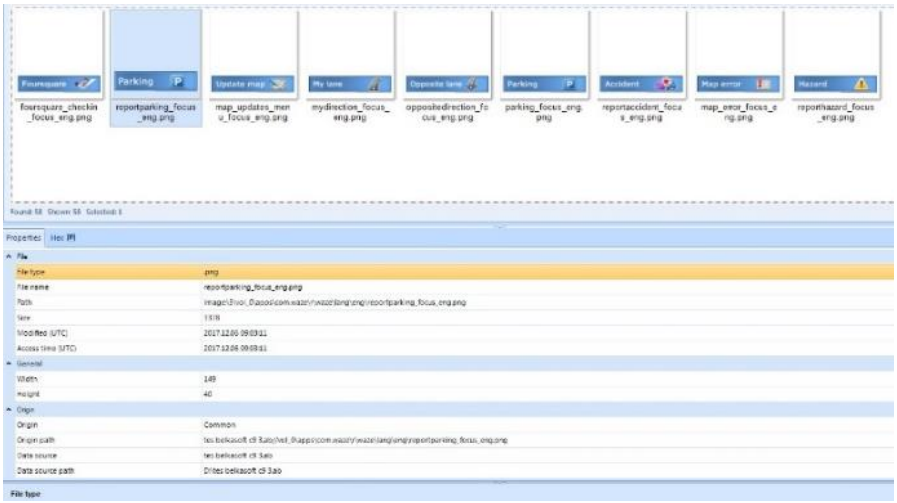
Table 3. Software Requirements

No	Software	Version	Description
1	WA	2.17.351	Research object
2	Windows 7		Worksation’s Operating System
3	WA DB/Key Extractor	4.7	Forensic Tool
4	Belkasoft Evidence	8.4	Forensic & analysis tool
5	Oxygen Forensic 4.7	6.4.0.67	Forensic & analysis tool
6	Magnet AXIOM	2.7.1.12070	Forensic & analysis tool
7	SQL Studio	3.1.1	Analysis tool

3. Results and Discussion

3.1 Forensic Analysis

Samsung C9 Pro used in this research was in unrooted condition. Hence logical acquisition used for conducting forensic analysis. Figure 5 shows image files that are successfully acquired using Belkasoft Evidence. The acquired image files have pixel size in accordance to its original size. The file can be opened so the investigator can see the image more clearly. Belkasoft Evidence gets information on image file metadata such as file size and access time. Belkasoft Evidence can also provide information if the image file contains pornographic content or if the image file has been modified or manipulated.


Foursquare
Parking
Update map
My lane
Opposite lane
Parking
Accident
Map error
Hazard
foursquare_checkin_focus_eng.png
reportparking_focus_eng.png
map_updates_menu_focus_eng.png
mydirection_focus_eng.png
oppositedirection_focus_eng.png
parking_focus_eng.png
reportaccident_focus_eng.png
map_error_focus_eng.png
reporthazard_focus_eng.png
Found: 58 Shown: 58 Selected: 1
Properties
Hex

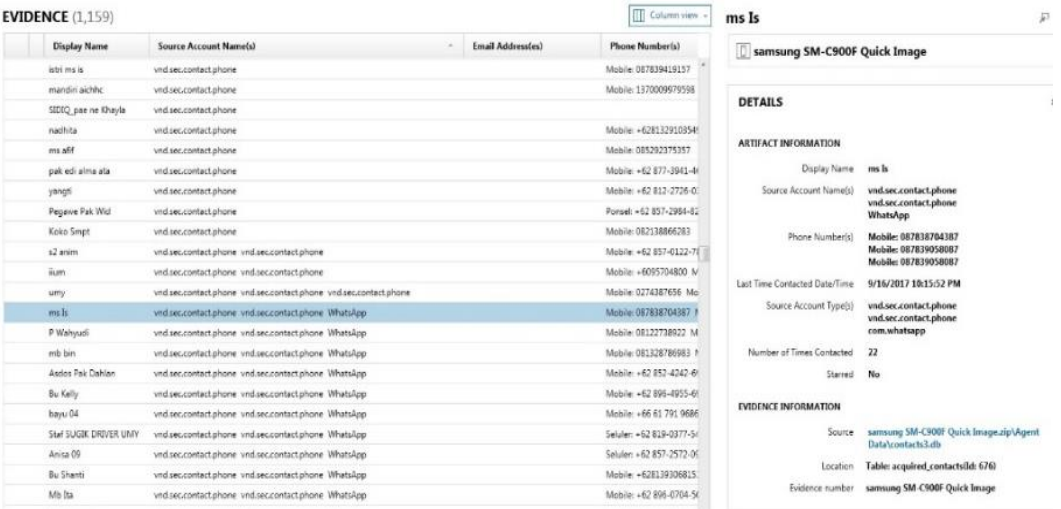
File	
File type	.png
File name	reportparking_focus_eng.png
Path	image\Evol_0apps\com.waze\r\waze\lang\eng\reportparking_focus_eng.png
Size	1518
Modified (UTC)	2017.12.06 09:03:11
Access time (UTC)	2017.12.06 09:03:11
General	
Width	149
Height	40
Origin	
Origin	Common
Origin path	tes belkasoft c9 3.ab\vol_0\apps\com.waze\r\waze\lang\eng\reportparking_focus_eng.png
Data source	tes belkasoft c9 3.ab
Data source path	D:\tes belkasoft c9 3.ab

File type

Figure 5. Image Artifact of Samsung C9 Pro Using Belkasoft Evidence

Belkasoft Evidence also successfully acquired the Samsung C9 Pro device video file artifact. The acquired video file can be played so that the investigator can view the contents of the video file which can help the investigation processes. Although Belkasoft Evidence managed to acquired image files and video files from Samsung C9 Pro, files that are acquired are not related to WA. Thus it can be a problem when facing cases related to WA. Researchers argue that the reason Belkasoft Evidence did not manage to retrieve WA's artifacts is because Belkasoft Evidence did not manage to decrypt the files since WA's artifact are encrypted.

Magnet AXIOM managed to acquire WA Samsung C9 Pro contact list artifacts as shown in Figure 6. Contact list artifact provides metadata such as WA identity, telephone number, and contact name. Magnet AXIOM also successfully acquired image artifacts as shown in Figure 7. The acquisition image file can be opened so the investigator can view the contents of the image file. The acquired image quality using Magnet AXIOM has a good quality with pixel size according to the original file. Some important metadata information such as date, name of the device used to take pictures, the GPS position where the image is taken, can be known.



EVIDENCE (1,159)

Display Name	Source Account Name(s)	Email Address(es)	Phone Number(s)
istri ms is	vnd.sec.contact.phone		Mobile: 087839419157
mandiri aichhc	vnd.sec.contact.phone		Mobile: 1370009979598
SIDIQ_pae ne Khayla	vnd.sec.contact.phone		
nadhita	vnd.sec.contact.phone		Mobile: +62813291035
ms afif	vnd.sec.contact.phone		Mobile: 085292375357
pak edi alma ala	vnd.sec.contact.phone		Mobile: +62 877-3941-4
yangti	vnd.sec.contact.phone		Mobile: +62 812-2726-0
Pegawe Pak Wid	vnd.sec.contact.phone		Ponsel: +62 857-2984-82
Koko Smpt	vnd.sec.contact.phone		Mobile: 082138866283
s2 anim	vnd.sec.contact.phone vnd.sec.contact.phone		Mobile: +62 857-0122-7
iium	vnd.sec.contact.phone vnd.sec.contact.phone		Mobile: +6095704800 M
umy	vnd.sec.contact.phone vnd.sec.contact.phone vnd.sec.contact.phone		Mobile: 0274387656 Mo
ms Is	vnd.sec.contact.phone vnd.sec.contact.phone WhatsApp		Mobile: 087838704387 M
P Wahyudi	vnd.sec.contact.phone vnd.sec.contact.phone WhatsApp		Mobile: 08122738922 M
mb bin	vnd.sec.contact.phone vnd.sec.contact.phone WhatsApp		Mobile: 081328786983 M
Asdos Pak Dahlan	vnd.sec.contact.phone vnd.sec.contact.phone WhatsApp		Mobile: +62 852-4242-6
Bu Kelly	vnd.sec.contact.phone vnd.sec.contact.phone WhatsApp		Mobile: +62 896-4955-6
bayu 04	vnd.sec.contact.phone vnd.sec.contact.phone WhatsApp		Mobile: +66 61 791 9686
Staf SUGIK DRIVER UMY	vnd.sec.contact.phone vnd.sec.contact.phone WhatsApp		Seluler: +62 819-0377-5
Anisa 09	vnd.sec.contact.phone vnd.sec.contact.phone WhatsApp		Seluler: +62 857-2572-0
Bu Shanti	vnd.sec.contact.phone vnd.sec.contact.phone WhatsApp		Mobile: +628139306815
Mb Ita	vnd.sec.contact.phone vnd.sec.contact.phone WhatsApp		Mobile: +62 896-0704-5

ms Is

samsung SM-C900F Quick Image

DETAILS

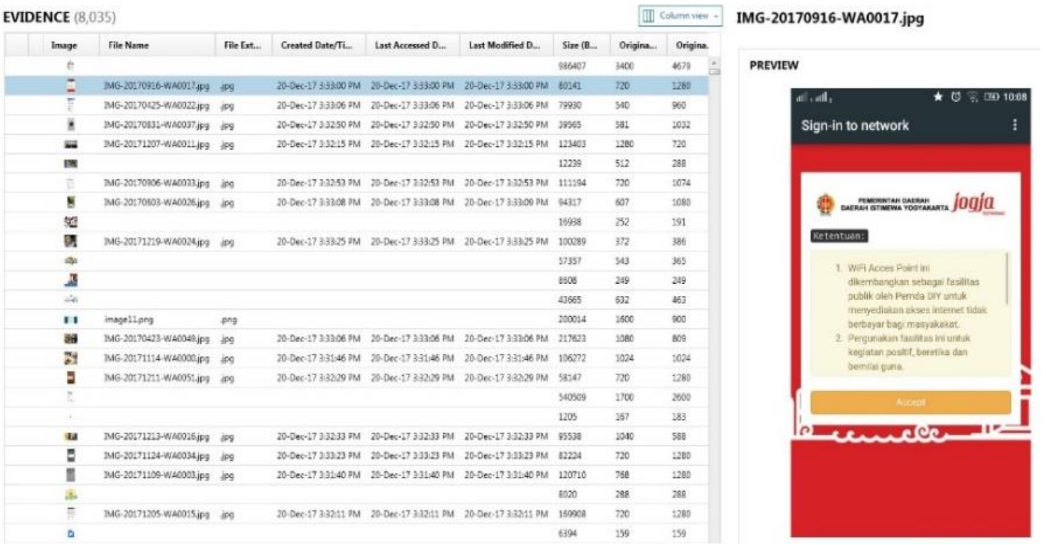
ARTIFACT INFORMATION

Display Name	ms Is
Source Account Name(s)	vnd.sec.contact.phone vnd.sec.contact.phone WhatsApp
Phone Number(s)	Mobile: 087838704387 Mobile: 087839058087 Mobile: 087839058087
Last Time Contacted Date/Time	9/16/2017 10:15:52 PM
Source Account Type(s)	vnd.sec.contact.phone vnd.sec.contact.phone com.whatsapp
Number of Times Contacted	22
Starred	No

EVIDENCE INFORMATION

Source	samsung SM-C900F Quick Image.zip\Agent Data\contacts3.db
Location	Table: acquired_contacts(Id: 676)
Evidence number	samsung SM-C900F Quick Image

Figure 6. Contact List Artifact of Samsung C9 Pro Using Magnet AXIOM



EVIDENCE (8,035)

Image	File Name	File Ext...	Created Date/Ti...	Last Accessed D...	Last Modified D...	Size (B...	Origina...	Origina.
						986407	3400	4679
	IMG-20170916-WA0017.jpg	.jpg	20-Dec-17 3:33:00 PM	20-Dec-17 3:33:00 PM	20-Dec-17 3:33:00 PM	80141	720	1280
	IMG-20170425-WA0022.jpg	.jpg	20-Dec-17 3:33:06 PM	20-Dec-17 3:33:06 PM	20-Dec-17 3:33:06 PM	79930	540	960
	IMG-20170831-WA0037.jpg	.jpg	20-Dec-17 3:32:50 PM	20-Dec-17 3:32:50 PM	20-Dec-17 3:32:50 PM	39565	581	1032
	IMG-20171207-WA0011.jpg	.jpg	20-Dec-17 3:32:15 PM	20-Dec-17 3:32:15 PM	20-Dec-17 3:32:15 PM	123403	1280	720
						12239	512	288
	IMG-20170906-WA0033.jpg	.jpg	20-Dec-17 3:32:53 PM	20-Dec-17 3:32:53 PM	20-Dec-17 3:32:53 PM	111194	720	1074
	IMG-20170603-WA0026.jpg	.jpg	20-Dec-17 3:33:08 PM	20-Dec-17 3:33:08 PM	20-Dec-17 3:33:09 PM	94317	607	1080
						16938	252	191
	IMG-20171219-WA0024.jpg	.jpg	20-Dec-17 3:33:25 PM	20-Dec-17 3:33:25 PM	20-Dec-17 3:33:25 PM	100289	372	386
						57357	543	365
						8608	249	249
						43665	632	463
	image11.png	.png				200014	1600	900
	IMG-20170423-WA0049.jpg	.jpg	20-Dec-17 3:33:06 PM	20-Dec-17 3:33:06 PM	20-Dec-17 3:33:06 PM	217623	1080	809
	IMG-20171114-WA0000.jpg	.jpg	20-Dec-17 3:31:46 PM	20-Dec-17 3:31:46 PM	20-Dec-17 3:31:46 PM	106272	1024	1024
	IMG-20171211-WA0051.jpg	.jpg	20-Dec-17 3:32:29 PM	20-Dec-17 3:32:29 PM	20-Dec-17 3:32:29 PM	58147	720	1280
						540509	1700	2600
						1205	167	183
	IMG-20171213-WA0016.jpg	.jpg	20-Dec-17 3:32:33 PM	20-Dec-17 3:32:33 PM	20-Dec-17 3:32:33 PM	95538	1040	588
	IMG-20171124-WA0034.jpg	.jpg	20-Dec-17 3:33:23 PM	20-Dec-17 3:33:23 PM	20-Dec-17 3:33:23 PM	82224	720	1280
	IMG-20171109-WA0003.jpg	.jpg	20-Dec-17 3:31:40 PM	20-Dec-17 3:31:40 PM	20-Dec-17 3:31:40 PM	120710	768	1280
						8020	288	288
	IMG-20171205-WA0015.jpg	.jpg	20-Dec-17 3:32:11 PM	20-Dec-17 3:32:11 PM	20-Dec-17 3:32:11 PM	169908	720	1280
						6394	159	159

IMG-20170916-WA0017.jpg

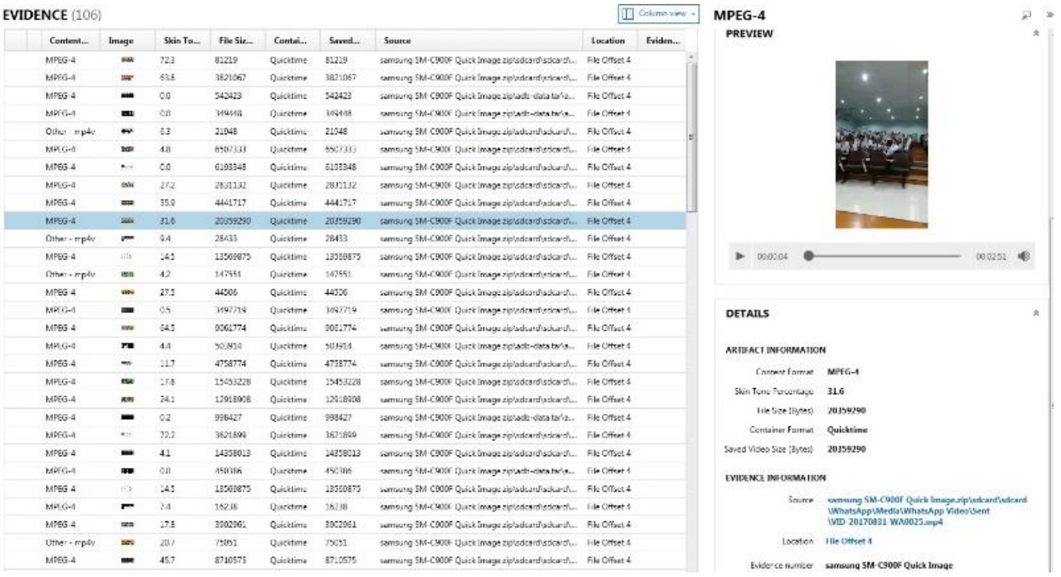
Sign-in to network

Ketentuan:

1. WiFi Acces Point ini dikembangkan sebagai fasilitas publik oleh Pemda DIY untuk menyediakan akses internet tidak berbayar bagi masyakakat.
2. Pergunakan fasilitas ini untuk kegiatan positif, beretika dan bernilai guna.

Figure 7. Image Artifact of Samsung C9 Pro Using AXIOM

Figure 8 shows the acquisition video file using Magnet AXIOM. Magnet AXIOM has successfully acquired video files properly. The acquisition video file can be played so it can help the executed investigation process. The information obtained on video artifact metadata include: date and time of making the video file, the last date and time to access and make modifications, and the size of the video file.



EVIDENCE (106)

	Content...	Image	Skin To...	File Siz...	Contai...	Saved...	Source	Location	Eviden...
	MPEG-4		72.3	81219	Quicktime	81219	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		63.8	3821067	Quicktime	3821067	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		0.0	542423	Quicktime	542423	samsung SM-C900F Quick Image.zip\adb-data.tar\a...	File Offset 4	
	MPEG-4		0.0	349448	Quicktime	349448	samsung SM-C900F Quick Image.zip\adb-data.tar\a...	File Offset 4	
	Other - mp4v		6.3	21048	Quicktime	21048	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		4.8	6507333	Quicktime	6507333	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		0.0	6103348	Quicktime	6103348	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		27.2	2831132	Quicktime	2831132	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		35.9	4441717	Quicktime	4441717	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		31.6	20359290	Quicktime	20359290	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	Other - mp4v		9.4	28433	Quicktime	28433	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		14.5	13569875	Quicktime	13569875	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	Other - mp4v		4.2	147551	Quicktime	147551	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		27.5	44506	Quicktime	44506	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		0.5	3497719	Quicktime	3497719	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		64.5	9061774	Quicktime	9061774	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		4.4	503914	Quicktime	503914	samsung SM-C900F Quick Image.zip\adb-data.tar\a...	File Offset 4	
	MPEG-4		11.7	4758774	Quicktime	4758774	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		17.8	15453228	Quicktime	15453228	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		24.1	12918908	Quicktime	12918908	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		0.2	998427	Quicktime	998427	samsung SM-C900F Quick Image.zip\adb-data.tar\a...	File Offset 4	
	MPEG-4		72.2	3621899	Quicktime	3621899	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		4.1	14358013	Quicktime	14358013	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		0.0	450386	Quicktime	450386	samsung SM-C900F Quick Image.zip\adb-data.tar\a...	File Offset 4	
	MPEG-4		14.5	13569875	Quicktime	13569875	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		7.4	16238	Quicktime	16238	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		17.8	3902961	Quicktime	3902961	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	Other - mp4v		20.7	75051	Quicktime	75051	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	
	MPEG-4		45.7	8710575	Quicktime	8710575	samsung SM-C900F Quick Image.zip\sdcard\sdcard\...	File Offset 4	

MPEG-4

PREVIEW

DETAILS

ARTIFACT INFORMATION

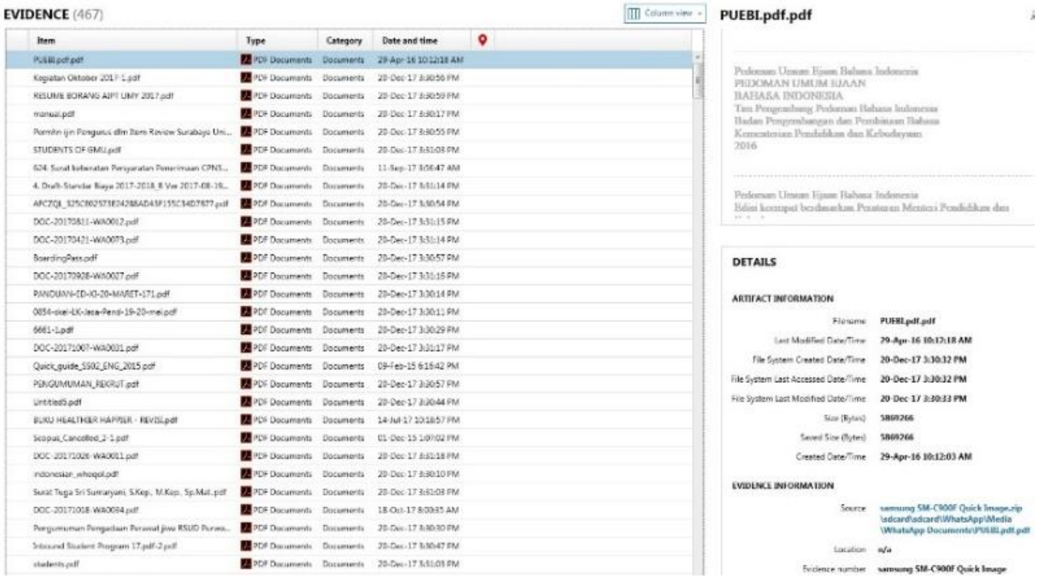
Content Format	MPEG-4
Skin Tone Percentage	31.6
File Size (Bytes)	20359290
Container Format	Quicktime
Saved Video Size (Bytes)	20359290

EVIDENCE INFORMATION

Source	samsung SM-C900F Quick Image.zip\sdcard\sdcard\WhatsApp\Media\WhatsApp Video\Sent\VID 20170831 WA0025.mp4
Location	File Offset 4
Evidence number	samsung SM-C900F Quick Image

Figure 8. Video Artifact of Samsung C9 Pro Using Magnet AXIOM

Magnet AXIOM has managed to get the Samsung C9 Pro document file artifact as shown in Figure 9. The acquisition document file can be opened to view the contents of the document file. This is important because it can help the investigation process if the investigator needs to view the contents of the document file. Some document file metadata information such as file name, date and time of the last document access and modification, file size, file creator, date and time can be known.



EVIDENCE (467)

Item	Type	Category	Date and time
PUEBI.pdf.pdf	PDF Documents	Documents	29-Apr-16 10:12:18 AM
Kegiatan Oktober 2017-1.pdf	PDF Documents	Documents	20-Dec-17 3:30:56 PM
RESUME BORANG AIPT UMY 2017.pdf	PDF Documents	Documents	20-Dec-17 3:30:59 PM
manual.pdf	PDF Documents	Documents	20-Dec-17 3:30:17 PM
Permhn ijn Pengurus dlm Item Review Surabaya Uni...	PDF Documents	Documents	20-Dec-17 3:30:55 PM
STUDENTS OF GMU.pdf	PDF Documents	Documents	20-Dec-17 3:31:03 PM
624. Surat keterangan Persyaratan Penerimaan CPNS...	PDF Documents	Documents	11-Sep-17 3:06:47 AM
4. Draft-Standar Biaya 2017-2018_8 Ver 2017-08-19...	PDF Documents	Documents	20-Dec-17 3:31:14 PM
APCZQL_325C802573E2428BAD43F155C34D7877.pdf	PDF Documents	Documents	20-Dec-17 3:30:54 PM
DOC-20170811-WA0012.pdf	PDF Documents	Documents	20-Dec-17 3:31:15 PM
DOC-20170421-WA0073.pdf	PDF Documents	Documents	20-Dec-17 3:31:14 PM
BoardingPass.pdf	PDF Documents	Documents	20-Dec-17 3:30:57 PM
DOC-20170928-WA0027.pdf	PDF Documents	Documents	20-Dec-17 3:31:16 PM
PANDUAN-ED-XI-20-MARET-171.pdf	PDF Documents	Documents	20-Dec-17 3:30:14 PM
0854-skel-LK-Jasa-Pend-19-20-mei.pdf	PDF Documents	Documents	20-Dec-17 3:30:11 PM
6661-1.pdf	PDF Documents	Documents	20-Dec-17 3:30:29 PM
DOC-20171007-WA0031.pdf	PDF Documents	Documents	20-Dec-17 3:31:17 PM
Quick_guide_SS02_ENG_2015.pdf	PDF Documents	Documents	09-Feb-15 6:16:42 PM
PENGUMUMAN_REKRUT.pdf	PDF Documents	Documents	20-Dec-17 3:30:57 PM
Untitled5.pdf	PDF Documents	Documents	20-Dec-17 3:30:44 PM
BUKU HEALTHIER HAPPIER - REVISI.pdf	PDF Documents	Documents	14-Jul-17 10:18:57 PM
Scopus_Cancelled_2-1.pdf	PDF Documents	Documents	01-Dec-15 1:07:02 PM
DOC-20171026-WA0011.pdf	PDF Documents	Documents	20-Dec-17 3:31:18 PM
indonesian_whoqol.pdf	PDF Documents	Documents	20-Dec-17 3:30:10 PM
Surat Tega Sri Sumaryani, S.Kep., M.Kep., Sp.Mat..pdf	PDF Documents	Documents	20-Dec-17 3:31:03 PM
DOC-20171018-WA0094.pdf	PDF Documents	Documents	18-Oct-17 8:00:35 AM
Pengumuman Pengadaan Perawat jiwa RSUD Purwo...	PDF Documents	Documents	20-Dec-17 3:30:30 PM
Inbound Student Program 17.pdf-2.pdf	PDF Documents	Documents	20-Dec-17 3:30:47 PM
students.pdf	PDF Documents	Documents	20-Dec-17 3:31:03 PM

PUEBI.pdf.pdf

Pedoman Umum Ejaan Bahasa Indonesia
PEDOMAN UMUM EJAAN
BAHASA INDONESIA
Tim Pengembang Pedoman Bahasa Indonesia
Badan Pengembangan dan Pembinaan Bahasa
Kementerian Pendidikan dan Kebudayaan
2016

Pedoman Umum Ejaan Bahasa Indonesia
Edisi kompat berdasarkan Peraturan Menteri Pendidikan dan

DETAILS

ARTIFACT INFORMATION

Filename	PUEBI.pdf.pdf
Last Modified Date/Time	29-Apr-16 10:12:18 AM
File System Created Date/Time	20-Dec-17 3:30:32 PM
File System Last Accessed Date/Time	20-Dec-17 3:30:32 PM
File System Last Modified Date/Time	20-Dec-17 3:30:33 PM
Size (Bytes)	5869266
Saved Size (Bytes)	5869266
Created Date/Time	29-Apr-16 10:12:03 AM

EVIDENCE INFORMATION

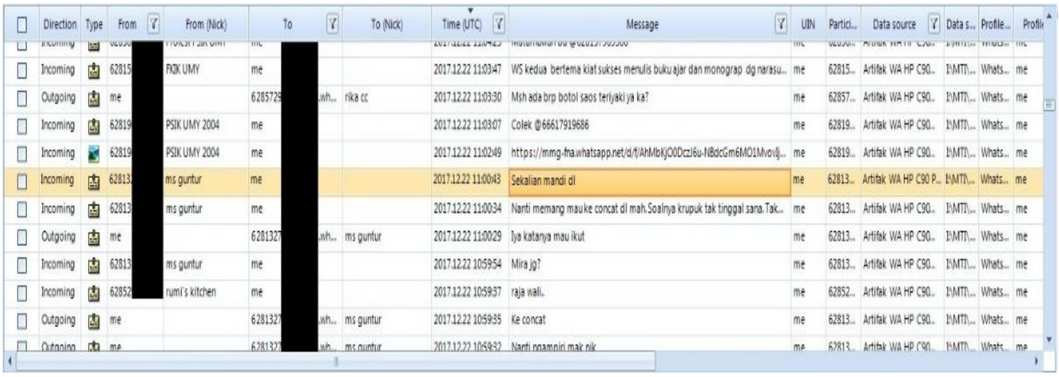
Source	samsung SM-C900F Quick Image.zip\sdcard\sdcard\WhatsApp\Media\WhatsApp Documents\PUEBI.pdf.pdf
Location	n/a
Evidence number	samsung SM-C900F Quick Image

Figure 9. Document Artifact of Samsung C9 Pro Using Magnet AXIOM

Oxygen Forensic managed to get information about the type and series of smartphone devices, operating system versions, operating system status, IMEI, IMSI, and serial numbers. The information on the acquisition process such as the version of the forensic tool used, date and time of the acquisition, and the duration of the acquisition process, can also be known. Oxygen Forensic is unable to get the WA contact list artifacts, WA logs, chat artifacts, image file artifacts, video file artifacts, and the document file artifacts. Researchers argue that the reason why Oxygen Forensic did not manage to retrieve WA artifacts is because it did not support logical acquisition at Samsung C9 Pro smartphone’s type and its Android version.

WA Key/DB Extractor do not have the ability to do an analysis. Therefore, to do the analysis of WA Key/DB Extractor artifacts, other supporting tools are needed. In this study Belkasoft

Evidence and SQL Studio are used as tools to help analyze artifacts from the acquisition of WA Key/DB Extractor. The Key/DB Extractor has managed to get call log artifacts, contact list artifacts, chat artifacts, and Samsung C9 Pro device image file artifacts. The video file artifacts and document file artifacts are not successfully obtained by WA Key/DB Extractor. Figure 10 shows text message artifacts as a result of the acquisition of a Samsung C9 Pro device using the WA Key/DB Extractor. WA Key/DB Extractor can acquire text messages in non-latin writing. Message content in the form of emoticons was not successfully obtained using WA Key/DB Extractor. Investigators can find out important information related to text message artifacts such as communication directions, message content, message sender and recipient, time and date of communication.



☐	Direction	Type	From	From (Nick)	To	To (Nick)	Time (UTC)	Message	UIN	Partici...	Data source	Data s...	Profile...	Profil
☐	Incoming	▣	62815[redacted]	FKIK UMY	me	[redacted]		2017.12.22 11:03:47	WS kedua bertema kiat sukses menulis buku ajar dan monograp dg narasu...	me	62815...	Artifak WA HP C90...	I:\MT\...	Whats...	me
☐	Outgoing	▣	me	[redacted]	6285729[redacted].wh...	rika cc	2017.12.22 11:03:30	Msh ada brp botol saos teriyaki ya ka?	me	62857...	Artifak WA HP C90...	I:\MT\...	Whats...	me
☐	Incoming	▣	62819[redacted]	PSIK UMY 2004	me	[redacted]		2017.12.22 11:03:07	Colek @66617919686	me	62819...	Artifak WA HP C90...	I:\MT\...	Whats...	me
☐	Incoming	🖼	62819[redacted]	PSIK UMY 2004	me	[redacted]		2017.12.22 11:02:49	https://mmg-fna.whatsapp.net/d/f/AhMbKjO0DczI6u-NBdcGm6MO1Mvovlj...	me	62819...	Artifak WA HP C90...	I:\MT\...	Whats...	me
☐	Incoming	▣	62813[redacted]	ms guntur	me	[redacted]		2017.12.22 11:00:43	Sekalian mandi dl	me	62813...	Artifak WA HP C90 P...	I:\MT\...	Whats...	me
☐	Incoming	▣	62813[redacted]	ms guntur	me	[redacted]		2017.12.22 11:00:34	Nanti memang mauke concat dl mah.Soalnya krupuk tak tinggal sana.Tak...	me	62813...	Artifak WA HP C90...	I:\MT\...	Whats...	me
☐	Outgoing	▣	me	[redacted]	6281327[redacted].wh...	ms guntur	2017.12.22 11:00:29	Iya katanya mau ikut	me	62813...	Artifak WA HP C90...	I:\MT\...	Whats...	me
☐	Incoming	▣	62813[redacted]	ms guntur	me	[redacted]		2017.12.22 10:59:54	Mira jg?	me	62813...	Artifak WA HP C90...	I:\MT\...	Whats...	me
☐	Incoming	▣	62852[redacted]	rumi's kitchen	me	[redacted]		2017.12.22 10:59:37	raja wali..	me	62852...	Artifak WA HP C90...	I:\MT\...	Whats...	me
☐	Outgoing	▣	me		6281327[redacted].wh...	ms guntur	2017.12.22 10:59:35	Ke concat	me	62813...	Artifak WA HP C90...	I:\MT\...	Whats...	me
☐	Outgoing	▣	me		6281327[redacted].wh...	ms guntur	2017.12.22 10:59:32	Nanti ngampiri mak nik	me	62813...	Artifak WA HP C90...	I:\MT\...	Whats...	me

Figure 10. Chat Artifacts of Samsung C9 Pro Using WA Key/DB Extractor

WA Key/DB Extractor have successfully obtained the artifact of the Samsung C9 Pro device image file as shown in Figure 11. WA Key/DB Extractor have weaknesses in terms of acquiring the image file artifacts. The obtained image file artifacts have a small resolution (100 x 55 or 55 x 100) according to the size of the thumbnail therefore the image file appears in low quality when it is zoomed-in.

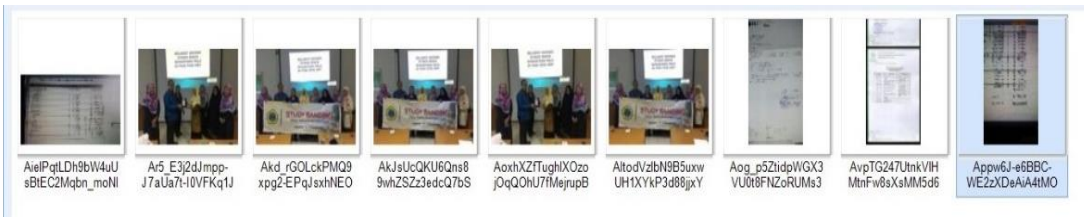
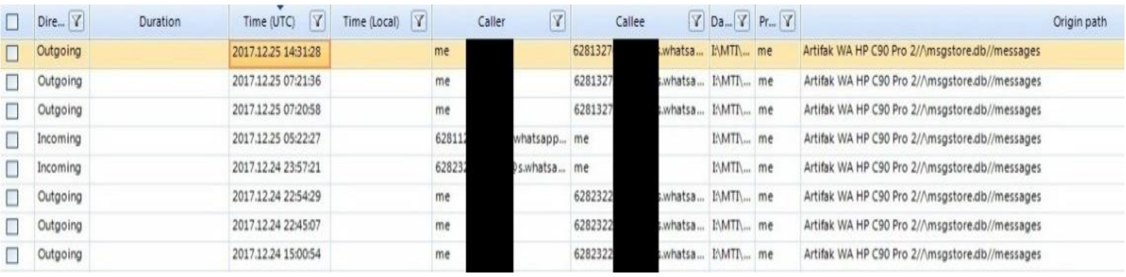

AielPqtLDh9bW4uU sBtEC2Mqbn_moNl
Ar5_E3j2dJmpp-J7aUa7t-I0VFKq1J
Akd_rGOLckPMQ9 xpg2-EPqJsxhNEO
AkJsUcQKU6Qns8 9whZSZz3edcQ7bS
AoxhXZfTughlXOzo jOqQOhU7fMejrupB
AltodVzlbN9B5uxw UH1XYkP3d88jjxY
Aog_p5ZtidpWGX3 VU0t8FNZoRUMs3
AvpTG247UtnkVIH MtnFw8sXsMM5d6
Appw6J-e6BBC-WE2zXDeAiA4tMO

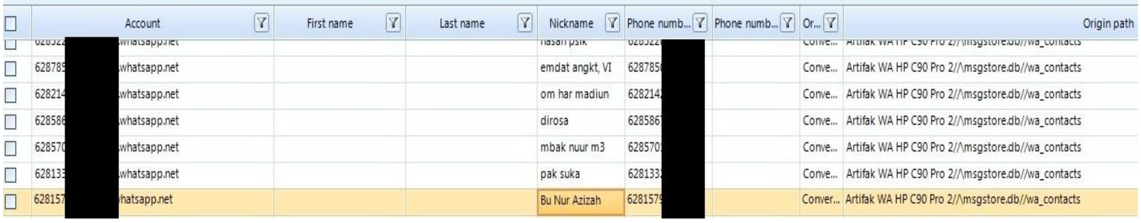
Figure 11. Image Artifacts of Samsung C9 Pro Acquired Using WA Key/DB Extractor

Figure 12 shows the log call artifact resulting from the acquisition of the Samsung C9 Pro device using the WA Key/DB Extractor. Investigators can find out some important metadata information for investigation of call log artifacts such as the direction of communication of calls, date and time of communication, and who are involved in the communication being carried out. WA Key/DB Extractor also managed to get the Samsung C9 Pro device contact list artifact as shown in Figure 13. Contact list metadata information such as WA account information, contact name, and telephone number can be found from contact list artifact.



☐	Dire...	Duration	Time (UTC)	Time (Local)	Caller	Callee	Da...	Pr...	Origin path
☐	Outgoing		2017.12.25 14:31:28		me [redacted]	6281327[redacted].whatsa...	I:\MT\...	me	Artifak WA HP C90 Pro 2//\msgstore.db//messages
☐	Outgoing		2017.12.25 07:21:36		me [redacted]	6281327[redacted].whatsa...	I:\MT\...	me	Artifak WA HP C90 Pro 2//\msgstore.db//messages
☐	Outgoing		2017.12.25 07:20:58		me [redacted]	6281327[redacted].whatsa...	I:\MT\...	me	Artifak WA HP C90 Pro 2//\msgstore.db//messages
☐	Incoming		2017.12.25 05:22:27		62811[redacted]whatsapp...	me [redacted]	I:\MT\...	me	Artifak WA HP C90 Pro 2//\msgstore.db//messages
☐	Incoming		2017.12.24 23:57:21		62823[redacted]s.whatsa...	me [redacted]	I:\MT\...	me	Artifak WA HP C90 Pro 2//\msgstore.db//messages
☐	Outgoing		2017.12.24 22:54:29		me [redacted]	6282322[redacted].whatsa...	I:\MT\...	me	Artifak WA HP C90 Pro 2//\msgstore.db//messages
☐	Outgoing		2017.12.24 22:45:07		me [redacted]	6282322[redacted].whatsa...	I:\MT\...	me	Artifak WA HP C90 Pro 2//\msgstore.db//messages
☐	Outgoing		2017.12.24 15:00:54		me [redacted]	6282322[redacted].whatsa...	I:\MT\...	me	Artifak WA HP C90 Pro 2//\msgstore.db//messages

Figure 12. WA Log Artifacts of Samsung C9 Pro Acquired Using WA Key/DB Extractor



□	Account	First name	Last name	Nickname	Phone numb...	Phone numb...	Or...	Origin path
□	[redacted] whatsapp.net			hasan psik	[redacted]		Conve...	Artifak WA HP C90 Pro 2//\msgstore.db//wa_contacts
□	628785 [redacted] whatsapp.net			emdat angkt, VI	628785 [redacted]		Conve...	Artifak WA HP C90 Pro 2//\msgstore.db//wa_contacts
□	628214 [redacted] whatsapp.net			om har madiun	628214 [redacted]		Conve...	Artifak WA HP C90 Pro 2//\msgstore.db//wa_contacts
□	628586 [redacted] whatsapp.net			dirosa	628586 [redacted]		Conve...	Artifak WA HP C90 Pro 2//\msgstore.db//wa_contacts
□	628570 [redacted] whatsapp.net			mbak nuur m3	628570 [redacted]		Conve...	Artifak WA HP C90 Pro 2//\msgstore.db//wa_contacts
□	628133 [redacted] whatsapp.net			pak suka	628133 [redacted]		Conve...	Artifak WA HP C90 Pro 2//\msgstore.db//wa_contacts
□	628157 [redacted] hatsapp.net			Bu Nur Azizah	628157 [redacted]		Conver...	Artifak WA HP C90 Pro 2//\msgstore.db//wa_contacts

Figure 13. Contact List Artifact of Samsung C9 Pro Acquired Using WA Key/DB Extractor

3.2 Validation

Table 4 shows the repeatability test results performed on Samsung C9 Pro devices logically using Belkasoft Evidence, Magnet AXIOM, Oxygen Forensic, and WA Key/DB Extractor. Of the two carried acquisition processes carried by Belkasoft Evidence, the obtained artifacts have similarities in content and number, thus it can be stated that Belkasoft Evidence fulfills the test of logical acquisition repeatability on Samsung C9 Pro devices. Magnet AXIOM meets the logical acquisition repeatability tests on Samsung C9 Pro devices by looking at the similarity in the number of artifacts and artifact contents from the two carried out acquisition processes. Although the Oxygen Forensic has not been able to obtain the WA artifacts, Oxygen Forensic meets the logical acquisition repeatability tests on Samsung C9 Pro devices because similarities were found on non-WA Artifacts. Of the two acquisition processes carried out by WA Key/DB Extractor, there are similarities in terms of the number of artifacts and contents of the artifacts therefore the WA Key/DB Extractor meets the repeatability test on Samsung C9 Pro devices.

Table 4 also shows the reproducibility tests of forensic tools conducted on Samsung C9 Pro devices. Belkasoft Evidence, Oxygen Forensic, Magnet AXIOM, and WA Key/DB Extractor managed to fulfill the reproducibility test for the logical acquisition on Samsung C9 Pro devices. Although the types and number of artifacts obtained using Belkasoft Evidence, Magnet AXIOM, and WA Key/DB Extractor are different, but there are similarities found in artifacts from forensic tools used for the forensic processes. Oxygen Forensic has successfully acquired the Samsung C9 Pro device. Although Oxygen Forensic did not managed to acquire WA artifacts, researcher found similarities in non-WA Artifacts compared to Belkasoft Evidence artifacts and Magnet AXIOM artifacts. Hence it can be said that Oxygen Forensic fulfills the reproducibility test for logical acquisition on Samsung C9 Pro devices. All forensic tools used this research meet the logical acquisition repeatability test and reproducibility test on Samsung C9 Pro devices as shown in Table 5.

Table 4. Repeatability and Reproducibility Test of Forensic Tools

No	Artifact Type	Belkasoft Evidence		Magnet AXIOM		Oxygen Forensic		WA Key/DB Extractor	
		Test 1	Test 2	Test 1	Test 2	Test 1	Test 2	Test 1	Test 2
1	Chat	-	-	-	-	-	-	502939	502939
2	Image	58	58	2938	2938	-	-	28888	28888
3	Video	10	10	39	39	-	-	-	-
4	Document	-	-	359	359	-	-	-	-
5	Contact List	-	-	803	803	-	-	2884	2884
6	WA Log	-	-	-	-	-	-	1483	1483

Table 5. Repeatability Test and Reproducibility Test Results

	Belkasoft Evidence	Magnet AXIOM	Oxygen Forensic	WA Key/DB Extractor
Repeatability	√	√	√	√
Reproducibility	√	√	√	√

Table 6 shows a comparison of the acquisition results of WA applications on Samsung C9 Pro devices using the Belkasoft Evidence, Magnet AXIOM, Oxygen Forensic, and WA Key/DB Extractor. From the table, it can be seen that Belkasoft Evidence and Oxygen Forensic do not meet all the WA artifact parameters used on the research. Researchers argue it may be caused by forensic tools incapabilities to decrypt WA's artifacts and forensic tools did not support to conduct forensic analysis on Samsung C9 Pro used in this research. Magnet AXIOM has managed to get artifacts along with data from the image files, videos, documents, and contact lists. Chat artifacts and call logs are unsuccessfully obtained by the Magnet AXIOM. WA Key/DB Extractor have successfully made acquisitions by retrieving the chat artifacts, contact lists, WA logs, and image file artifacts. The image artifacts obtained using the WA Key/DB Extractor has a small size in resolution so it cannot be seen clearly when zoomed-in.

Forensic tools used in this research have successfully fulfilled the repeatability and reproducibility validation tests, thus the data obtained from the forensic devices can be used and accepted by the law. Belkasoft Evidence successfully acquired Samsung C9 Pro. Although Belkasoft Evidence has succeeded in obtaining the image and video artifacts, however the obtained artifacts of images and videos were not the artifacts from the WA application. Therefore, Belkasoft Evidence is not recommended for conducting WA forensic analysis. Magnet AXIOM managed to retrieve the artifacts of the images, videos, documents, and contact lists, along with their metadata. Oxygen Forensic did not manage to retrieve any WA artifacts. WA Key/DB Extractor successfully performed the logical acquisition processes and managed to retrieve chat, images, contact lists, and WA Log artifacts.

Table 6. WA Artifacts Parameter Analysis

Artifact Type	Belkasoft Evidence	Magnet AXIOM	Oxygen Forensic	WA Key/DB Extractor
Chat	-	-	-	√
Image	-	√	-	√
Video	-	√	-	-
Document	-	√	-	-
Contact List	-	√	-	√
WA Log	-	-	-	√

4. Conclusion

Based on the conducted research, researchers suggest that the combination of Magnet AXIOM and WA Key/DB Extractor will provide the best results because it will retrieve all of the WA artifacts that are used as parameters on this research. Looking at the fast development and diversification of the mobile device market these days, researcher suggest that further research regarding other IM applications on mobile devices with the latest version of forensic tools, latest Android operating system and other operating systems needs to be done in the future.

References

[1] J. Constine, "WhatsApp hits 1.5 billion monthly users. $19B? Notbad.," *TechCrunch*, 2018. [Online]. Available: https://techcrunch.com/2018/01/31/whatsapp-hits-1-5-billion-monthly-users-19b-not-so-bad/. [Accessed: 09-Dec-2018].

[2] statista.com, "Most popular mobile messaging apps worldwide as of October 2018, based on number of monthly active users (in millions)," 2018. [Online]. Available: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/. [Accessed: 09-Dec-2018].

[3] R. K. Nistanto, "Ini Negara dengan Jumlah Pengguna WhatsApp Terbanyak di Dunia," *Kompas.com*, 2016. [Online]. Available: http://tekno.kompas.com/read/2016/11/17/06150017/ini.negara.dengan.jumlah.pengguna.whatsapp.terbanyak.di.dunia. [Accessed: 25-Jan-2018].

[4] A. H. Pratama, "Laporan comScore: WhatsApp Adalah Aplikasi Mobile Terpopuler di Indonesia," *Tech In Asia*, 2017. [Online]. Available: https://id.techinasia.com/comscore-whatsapp-adalah-aplikasi-terpopuler-di-indonesia. [Accessed: 25-Jan-2018].

[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] Vix.com, "5 Crimes That People Do On WhatsApp And Can Actually Be Reported," 2018. [Online]. Available: https://www.vix.com/en/apps-internet/530661/5-crimes-people-do-whatsapp-and-can-actually-be-reported.

[7] Techzim.co.zw, "How WhatsApp Is Aiding Criminal Activity, We Should Copy The Shady Guys," 2018. [Online]. Available: https://www.techzim.co.zw/2018/07/how-whatsapp-has-

aided-criminal-actvivity/.

[8] A. Nurlitasari, “Hacker Manfaatkan WhatsApp untuk Curi Data Pribadi Pengguna,” 2018. [Online]. Available: https://techno.okezone.com/read/2018/08/09/207/1934241/hacker-manfaatkan-whatsapp-untuk-curi-data-pribadi-pengguna.

[9] A. Kusumadewi and J. P. Sasongko, “Polisi Usut Percakapan ‘Jessica-Mirna’ yang Beredar di Sosmed,” 2016. [Online]. Available: http://www.cnnindonesia.com/nasional/20160121080758-12-105715/polisi-usut-percakapan-jessica-mirna-yang-beredar-di-sosmed/. [Accessed: 10-Nov-2017].

[10] eForensics Magazine, “Introduction to Mobile Forensics,” 2015. .

[11] H. H. Khaleel, “Focused Digital Forensic Methodology,” *Forensic Focus*, 2017. [Online]. Available: https://articles.forensicfocus.com/2017/10/13/focused-digital-forensic-methodology/. [Accessed: 13-Feb-2018].

[12] 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, Pp. 85, 2014.

[13] M. Al-Hadadi and A. AlShidhani, “Smartphone Forensics Analysis: A Case Study,” *Int. J. Comput. Electr. Eng.*, Vol. 5, No. 6, Pp. 576–580, 2013.

[14] A. Abdallah, M. Alamin, A. Babiker, and N. Mustafa, “A Survey on Mobile Forensic for Android Smartphones,” *IOSR J. Comput. Eng.*, vol. 17, no. 1, pp. 2278–661, 2015.

[15] S. Dogan and E. Akbal, “Analysis of Mobile Phones in Digital Forensics,” *MIPRO 2017*, Pp. 1241–1244, 2017.

[16] R. Umar, I. Riadi, and G. M. Zamroni, “Mobile Forensic Tools Evaluation for Digital Crime Investigation,” *Int. J. Adv. Sci. Eng. Inf. Technol.*, Vol. 8, No. 3, Pp. 949, 2018.

[17] I. Riadi, A. Fadlil, and A. Fauzan, “A Study of Mobile Forensic Tools Evaluation on Android-Based LINE Messenger,” *Int. J. Adv. Comput. Sci. Appl.*, Vol. 9, No. 10, Pp. 201–206, 2018.

[18] National Institute of Standards and Technology, “General Test Methodology for Computer Forensic Tools.” 2001.

[19] N. Santos, “Mobile Forensics : Android,” 2015.

[20] 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.