Mobile and Forensics
Vol. 4, No. 2, September 2022, pp. 115-126
ISSN: 2714-6685 (online), 2656-6257 (print)
DOI: http://dx.doi.org/10.12928/mf.v1i1.XXX

Comparison of Forensic Tool Results on Android Smartphone Backup Files Using NIST Method

Permana Bangun Pangestu[a,1], Muhammad Koprawi[a,2*]
[a]Falkutas Ilmu Komputer, Universitas AMIKOM Yogyakarta, Indonesia
[1]Permana.20@students.amikom.ac.id, [2]koprawi@amikom.ac.id
[*]Correspondence email

Abstract

Smartphone technology currently developing not only has a positive impact but can also have a negative impact if it is used to commit crimes which can be called cybercrime. Choosing the right forensic tools is very important when conducting an investigation. So it is necessary to research the results of the comparative analysis of the performance of forensic tools on android smartphone backup files. The National Institute of Standards and Technology (NIST) method was used in this study as a parameter and for the digital evidence obtained. The results of the extraction of the OPPO A37f android smartphone from the MOBILedit tools acquired android backup files and the analysis results from using the Magnet AXIOM tools with a data accuracy rate of 39.3% from the predetermined variables. The Oxygen Forensic Tools obtained a data accuracy rate of 28.6% from the variable that has been determined. The Belkasoft Evidence Center tools can get a data accuracy rate of 35.7% of the predetermined variables. The results of this study can be concluded that the Magnet Axiom tool has a high level of accuracy compared to the Oxygen Forensic and Belkasoft Evidence Center tools in extracting data from android smartphone backup files.

Keywords: Mobile Forensic Tools, Smartphone, Android Backup, NIST

INTRODUCTION

Mobile device technology is increasingly developing, bringing human life to the virtual world community. One of them is a smartphone, whose use continues to increase yearly. Smartphones have more advantages than ordinary cell phones that can only be used to make voice calls and send short messages (Short Message). The benefits of smartphones include being able to communicate on social networks and make video calls. In Indonesia, the most popular Android-type smartphone today, as reported on the Mobile operating system Market Share Indonesia, with an android smartphone usage rate of 91.37% [1].

The increasing use of smartphones raises several problems, especially in a cyber crime known as cybercrime. Crimes committed can hide or delete digital evidence to eliminate evidence of crimes committed by the perpetrators. This digital evidence can be in the form of smartphone data, such as contact data, call logs, messages, videos, pictures, and document files that will be used as evidence of crimes in court [2].

Digital forensic knowledge in an investigation is needed, especially in analyzing a smartphone device. Forensic tools must also support success in an investigative process. The maximum success of an examiner in extracting data from a smartphone is

Article History: *Received April 22, 2022; Revised July 06, 2022; Accepted August 06, 2022*

not only fixated on one tool but by trying other tools. In addition, the variety of Android devices' uses presents challenges in choosing the right forensic tools to extract and analyze effectively [3].

Various studies have been carried out on comparing forensic tools on smartphones based on the Android operating system using the National Institute of Standards and Technology (NIST) method. One of these studies is that conducted by Riadi, Yudhana, and Putra (2018) [4], using the NIST method by comparing mobile forensic tools on the Instagram application with an Android-based operating system. This research uses AXIOM Magnet and Oxygen Forensic tools to obtain digital evidence. Other studies, such as those conducted by Ahmadi, Akbar, and M Putra (2021) [5], Used the Belkasoft Evidence Center and Magnet AXIOM tools to compare the performance of the tools against Android Smartphone Image Files using the NIST method.

The method used in this study also uses the National Institute of Standards and Technology (NIST) method because this method of obtaining digital evidence is more devoted to handling mobile devices. This method measures the stages and flow of research to be carried out so that it can be used as a guide in forensic activities to get effective results. The NIST method has several stages: Collection, Examination, Analysis, and Reporting. In this study, we will simulate android backup files from the OPPO A37f android smartphone as a comparison of three tools: Magnet AXIOM v 4.10.0.23663, Oxygen Forensic v 12.0.0.151, and Belkasoft Evidence Center v 9.9800.4928. The selection of the three tools is based on exposure from the background and several references, as well as the support base on the installed mobile forensic tools. The android backup file is a backup of some or all that is stored on an android device. The backup file is obtained using the Android Debug Bridge (ADB) extracted from the android smartphone [6].

METHODS

The method used is the National Institute of Standards and Technology (NIST) which is divided into four (4) stages, namely Collection, Examination, Analysis, and Reporting, as shown in Figure 1[7].

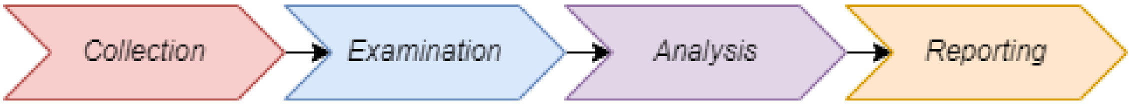


Figure 1. The Stage of NIST mobile forensic method

The explanation of the National Institute of Standards and Technology (NIST) method scheme is as follows:

Collection

This stage is also known as the preservation stage. The collection is a collection or identification of evidence used in the form of hardware from which the data will be taken to be used as digital evidence of a digital crime case. During the forensic process, all smartphones will be isolated by turning off telecommunication connections or activating airplane mode so that there is no active network to avoid data modification and maintain the integrity of the collected evidence. At this stage, the imaging process or copying of data against physical evidence is carried out using the MOBILedit Enterprise tool to get an android backup file.

Examination

It is the stage of processing data collected by digital forensics using a combination of various scenarios, both automatic and manual, as well as assessing and releasing data as needed while maintaining data integrity. Furthermore, the digital backup android file data from the imaging results are extracted using the Oxygen Forensics, Magnet Axiom, and Belkasoft Evidence Center tools.

Analysis

Conduct analysis of examination results using technically and legally justified methods to obtain helpful information and answer questions that serve as an impetus for collection and examination. This analysis stage is carried out after getting the desired digital file or data from the previous inspection process. The results of the analysis carried out to obtain several files that were successfully extracted using these mobile forensic tools were then successfully obtained.

Reporting

The reporting stage is the process of reporting the analysis results, which includes data information that has been found and is used as the final report of the forensic process. The following is the process scheme using the NIST method in this study, as shown in Figure 2.

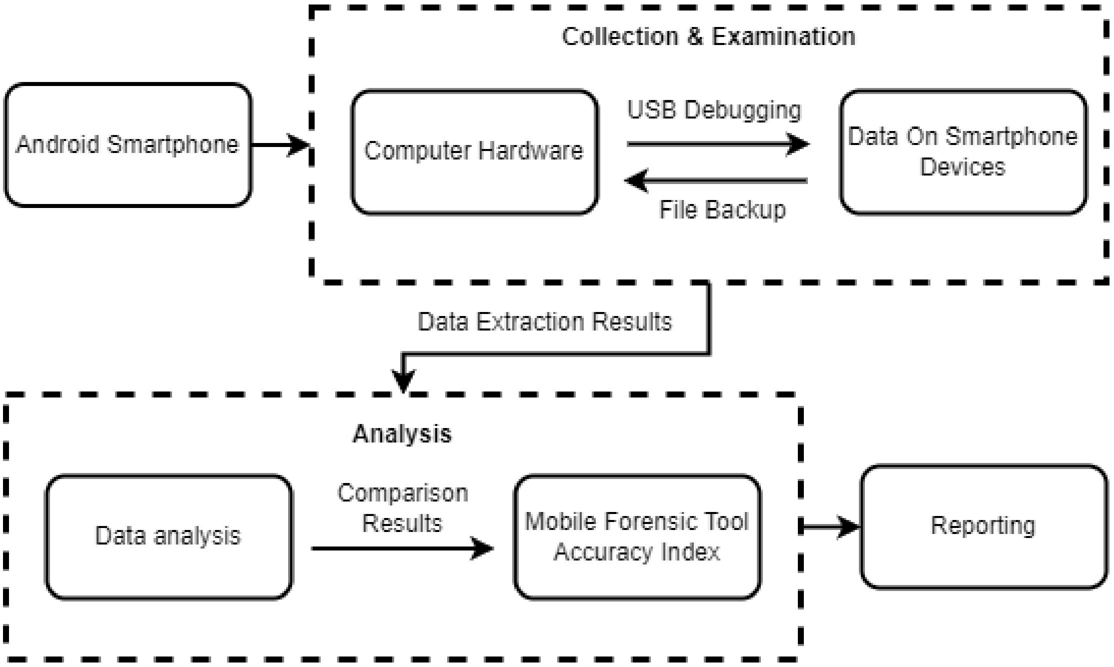


Figure 2. Process using the NIST method

The preparation and implementation of scenarios are carried out to get maximum results. The smartphone forensic process uses a guidebook from the National Institute of Standards and Technology (NIST), Mobile Device Tool Specifications, Test Assertions, and Test Cases [8]. The parameters above are divided into Core Features and Optional Features. The parameters used to analyze the application performance are presented in Table 1.

Table 1. Tools performance parameters

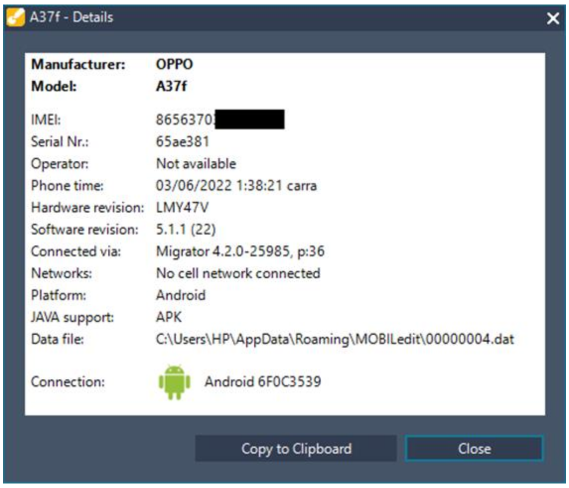
Parameter		Description
Core Features	MDT-CR-01	A mobile device forensic tool extracts and presents all supported data artifacts from a mobile device image file.
	MDT-CR-02	The tool renders text correctly.
	MDT-CR-03	A mobile device forensic tool does not modify a mobile device image file being examined.
	MDT-CR-04	A mobile device forensic tool notifies the tool user if a mobile device image file has been modified.
	MDT-CA-01	The tool presents all subscriber and equipment information available from an image file.
	MDT-CA-02	The tool presents all PIM (address book, calendar & notes) data available from an image file.
	MDT-CA-03	The tool presents all call data (call type (incoming, outgoing, missed), date-time stamps, duration) available from an image file.
	MDT-CA-04	The tool presents all message (SMS, MMS & instant messages) data available from an image file.
	MDT-CA-05	The tool presents all stand-alone (audio, documents, graphic & video,) files available from an image file.
	MDT-CA-06	The tool presents all browsing (history & bookmarks) data available from an image file.
	MDT-CA-07	The tool presents all email data available from an image file.
	MDT-CA-08	The tool presents all social media application data available from an image file.
	MDT-CA-09	The tool presents all geo-location application data available from an image file.
	MDT-CA-10	Presented text is rendered with the correct character glyphs.
	MDT-CA-11	The tool does not modify an image file.
	MDT-CA-12	If an image file is modified, the tool notifies the user that a change has been made to the image file.
Optional Features	MDT-RO-01	A mobile device forensic tool creates an image file from a physical memory acquisition (e.g., boot loader).
	MDT-RO-02	A mobile device forensic tool creates an image file from a logical acquisition of all supported memory artifacts.
	MDT-RO-03	mobile device forensic tool creates an image file from a logical acquisition of selected memory artifacts.
	MDT-RO-04	A mobile device forensic tool creates an image file from an acquisition of the mobile device file system.
	MDT-RO-05	A mobile device forensic tool notifies the user if there is a failure to access a connected mobile device.
	MDT-RO-06	A mobile device forensic tool notifies the user if an acquisition is interrupted before completion.
	MDT-AO-01	An image file is created of physical memory.
	MDT-AO-02	An image file is created containing supported memory artifacts.
	MDT-AO-03	An image file is created containing selected artifacts.
	MDT-AO-04	An image file is created of the device file system.
	MDT-AO-05	The user is notified if the tool fails to establish a connection or acquire data from a connected mobile device.
	MDT-AO-06	The user is notified if an acquisition is disrupted.

RESULT AND DISCUSSIONS

After the scenario process is successfully carried out, the next step is to find information and analyze the Android backup file to obtain evidence as has been scripted. The process of analyzing the backup android file using measurements from NIST. Four (4) stages are Collection, Examination, Analysis, and Reporting.

Collection

At this stage, data is collected and recorded from physical evidence. In forensic analysis at this stage, the smartphone needs to be isolated by activating airplane mode so that there is no active network to avoid data modification. The Android used in this study is the OPPO A37f smartphone. The following specifications for the smartphone used can be seen in Figure 3.



A37f - Details

Manufacturer:	**OPPO**
Model:	**A37f**
IMEI:	8656370[redacted]
Serial Nr.:	65ae381
Operator:	Not available
Phone time:	03/06/2022 1:38:21 carra
Hardware revision:	LMY47V
Software revision:	5.1.1 (22)
Connected via:	Migrator 4.2.0-25985, p:36
Networks:	No cell network connected
Platform:	Android
JAVA support:	APK
Data file:	C:\Users\HP\AppData\Roaming\MOBILedit\00000004.dat
Connection:	Android 6F0C3539

Figure 3. Smartphone specifications used

The following process in this stage is imaging or copying data to be used as an android backup file which Mobile Forensic tools will process. Copying data or imaging is done using the MOBILedit tool with the help of a data cable as a connector. MOBILedit Enterprise is only used for imaging processes and cannot perform inspection and analysis of the acquired data. Because MOBILedit Enterprise is used to access mobile data and modify content, perform backups and restores, access applications, manage files, and others, as shown in Figure 4.

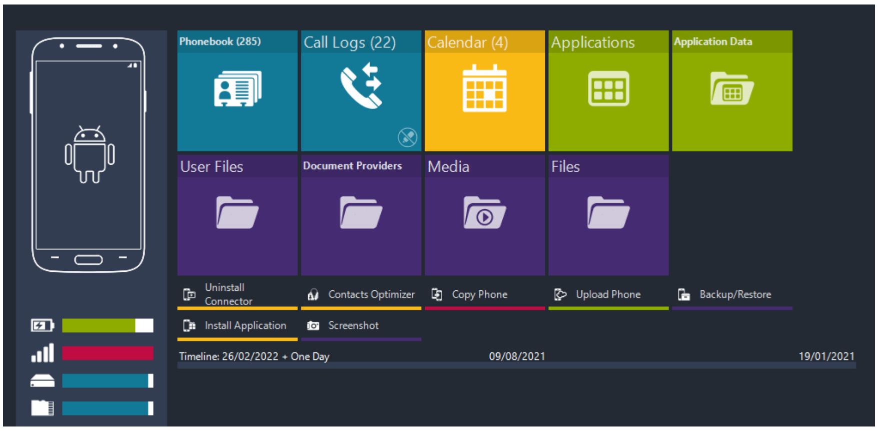
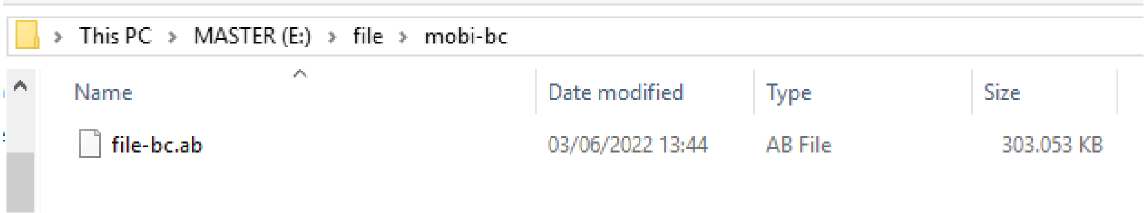


Figure 4. MOBILedit Enterprise features view.

The imaging process uses the ADB Unclocked mode technique, which uses the USB debugging permission process by confirming prior permissions from the smartphone [9]. Quoted from the official android developer website https://developer.android.com/ (2022), ADB is a tool that allows communication between computers and connected android devices. The backup android file from imaging can be seen in Figure 5.



› This PC › MASTER (E:) › file › mobi-bc

Name	Date modified	Type	Size
file-bc.ab	03/06/2022 13:44	AB File	303.053 KB

Figure 5. Imaging backup Android files

Examination

At this stage, the inspection process is carried out on the data that has been collected in the previous location. This process includes retrieving or extracting digital data on android backup files with tools to be tested, including Magnet Axiom, Oxygen Forensic, and Bekalsoft Evidence Center.

The extraction process carried out using mobile forensic tools has several differences. The AXIOM Magnet Tools require a longer time to extract compared to the Belkasoft Evidence Center. Then Oxygen forensics requires the fastest time in the extraction process compared to Magnet AXIOM and Belkasoft Evidence Center, as shown in Figure 6.

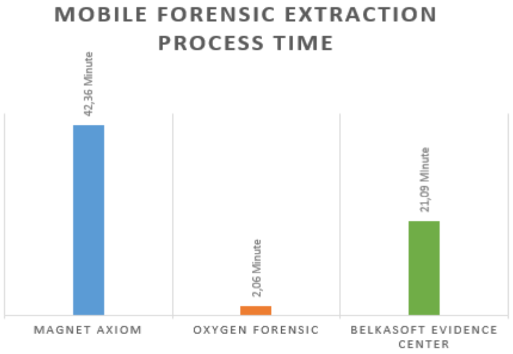


Figure 6. Mobile forensics extraction process time

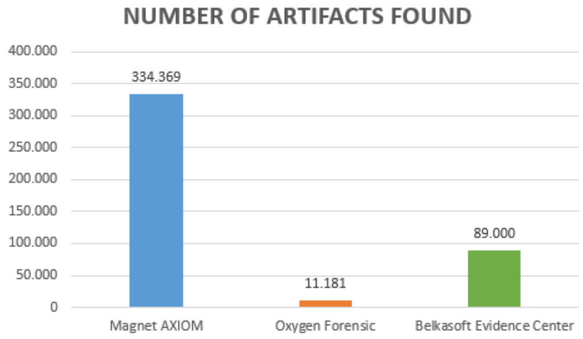
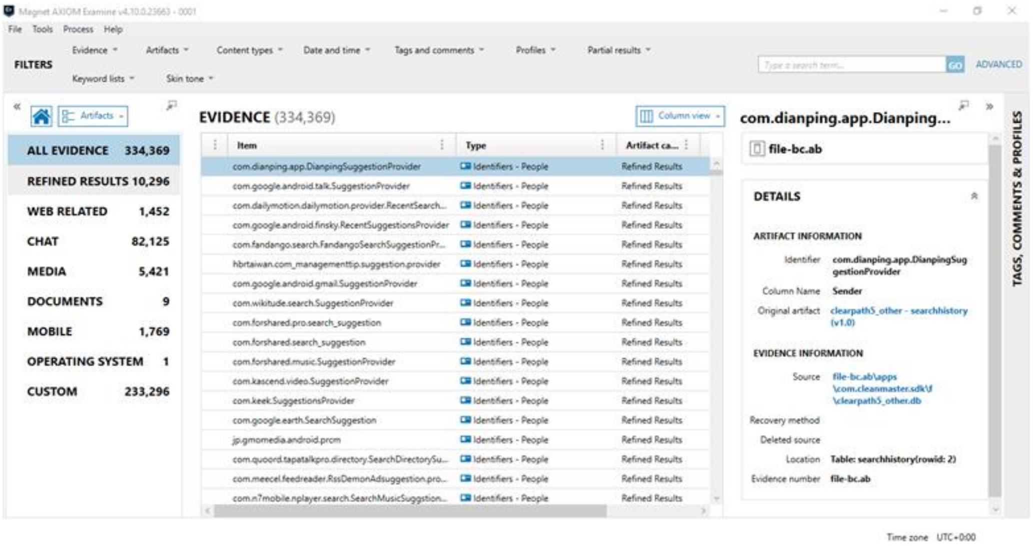


Figure 7. The number of artifacts found.

Furthermore, at the stage of the results obtained, Magnet AXIOM got more artifacts than the Belkasoft Evidence Center, and Oxygen Forensic managed to get the fewest artifacts, which can be seen in Figure 7.

Analysis

The analysis stage examines and compares the results to get the performance of mobile forensic tools. This stage is carried out from the results of the Examination stage or data extraction for android backup files with the results obtained as shown in Figure 8 with AXIOM Magnet tools, Figure 9 with Oxygen Forensic tools, and Figure 10 with Belkasoft Evidence Center tools.



EVIDENCE (334,369)

ALL EVIDENCE	334,369
REFINED RESULTS	10,296
WEB RELATED	1,452
CHAT	82,125
MEDIA	5,421
DOCUMENTS	9
MOBILE	1,769
OPERATING SYSTEM	1
CUSTOM	233,296

Item	Type	Artifact ca...
com.dianping.app.DianpingSuggestionProvider	Identifiers - People	Refined Results
com.google.android.talk.SuggestionProvider	Identifiers - People	Refined Results
com.dailymotion.dailymotion.provider.RecentSearch...	Identifiers - People	Refined Results
com.google.android.finsky.RecentSuggestionsProvider	Identifiers - People	Refined Results
com.fandango.search.FandangoSearchSuggestionPr...	Identifiers - People	Refined Results
hbrtaiwan.com_managementtip.suggestion.provider	Identifiers - People	Refined Results
com.google.android.gmail.SuggestionProvider	Identifiers - People	Refined Results
com.wikitude.search.SuggestionProvider	Identifiers - People	Refined Results
com.forshared.pro.search_suggestion	Identifiers - People	Refined Results
com.forshared.search_suggestion	Identifiers - People	Refined Results
com.forshared.music.SuggestionProvider	Identifiers - People	Refined Results
com.kascend.video.SuggestionProvider	Identifiers - People	Refined Results
com.keek.SuggestionsProvider	Identifiers - People	Refined Results
com.google.earth.SearchSuggestion	Identifiers - People	Refined Results
jp.gmomedia.android.prcm	Identifiers - People	Refined Results
com.quoord.tapatalkpro.directory.SearchDirectorySu...	Identifiers - People	Refined Results
com.meecel.feedreader.RssDemonAdsuggestion.pro...	Identifiers - People	Refined Results
com.n7mobile.nplayer.search.SearchMusicSuggstion...	Identifiers - People	Refined Results

com.dianping.app.Dianping...

file-bc.ab

DETAILS

ARTIFACT INFORMATION

Identifier com.dianping.app.DianpingSuggestionProvider
Column Name Sender
Original artifact clearpath5_other - searchhistory (v1.0)

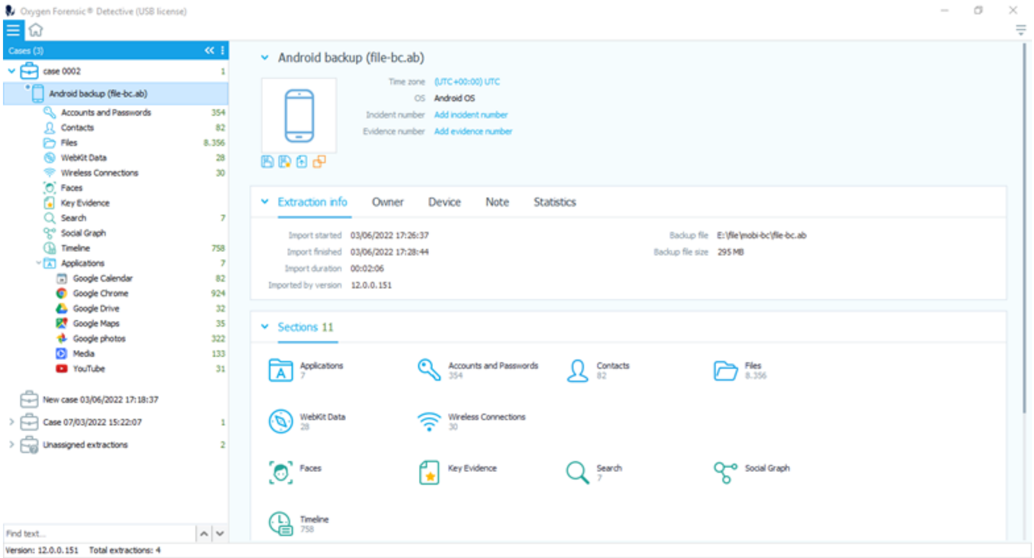
EVIDENCE INFORMATION

Source file-bc.ab\apps\com.cleanmaster.sdk\f\clearpath5_other.db
Recovery method
Deleted source
Location Table: searchhistory(rowid: 2)
Evidence number file-bc.ab

Time zone UTC+0:00

Figure 8. Extraction results on AXIOM Magnet tools

The results of the OPPO A37f smartphone data analysis from Figure 8 using the Magnet AXIOM tool get several files such as Refined Results, Web Related, Chat, Media, Documents, Mobile, Operating System, and Custom.



case 0002	1
Android backup (file-bc.ab)	
Accounts and Passwords	354
Contacts	82
Files	8.356
WebKit Data	28
Wireless Connections	30
Faces	
Key Evidence	
Search	7
Social Graph	
Timeline	758
Applications	7
Google Calendar	82
Google Chrome	924
Google Drive	32
Google Maps	35
Google photos	322
Media	133
YouTube	31
New case 03/06/2022 17:18:37	
Case 07/03/2022 15:22:07	1
Unassigned extractions	2

Version: 12.0.0.151 Total extractions: 4

Android backup (file-bc.ab)

Time zone (UTC +00:00) UTC
OS Android OS
Incident number Add incident number
Evidence number Add evidence number

Extraction info

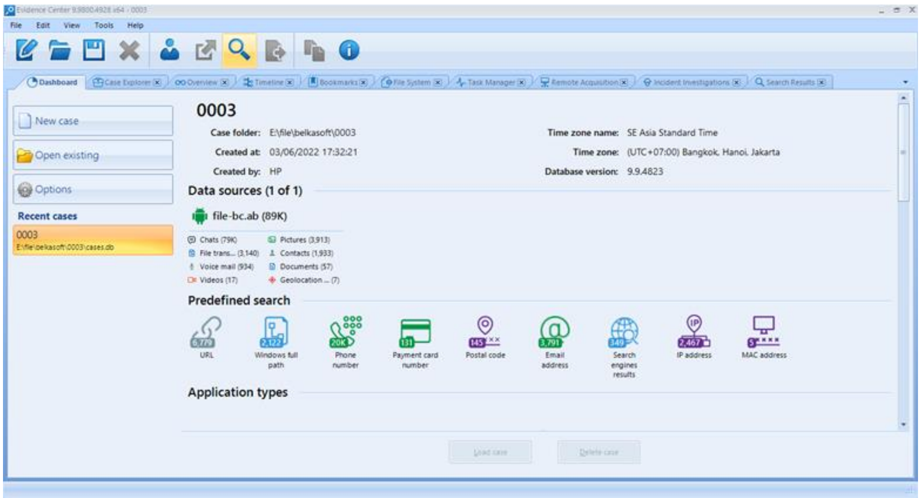
Import started 03/06/2022 17:26:37
Import finished 03/06/2022 17:28:44
Import duration 00:02:06
Imported by version 12.0.0.151
Backup file E:\file\mobi-bc\file-bc.ab
Backup file size 295 MB

Sections 11

Applications	7
Accounts and Passwords	354
Contacts	82
Files	8.356
WebKit Data	28
Wireless Connections	30
Faces	
Key Evidence	
Search	7
Social Graph	
Timeline	758

Figure 9. Extraction results on Oxygen Forensic tools

The analysis carried out by the Oxygen Forensic tool in Figure 9 gets several files, including Applications, Account and Password files, Contacts, Files, Webkit Data, Wireless Connections, Faces, Key Evidence, Search, Social Graph, and Timeline.



Recent cases
0003
E:\file\belkasoft\0003\cases.db

0003

Case folder: E:\file\belkasoft\0003
Created at: 03/06/2022 17:32:21
Created by: HP
Time zone name: SE Asia Standard Time
Time zone: (UTC+07:00) Bangkok, Hanoi, Jakarta
Database version: 9.9.4823

Data sources (1 of 1)

file-bc.ab (89K)

Chats (79K)
Pictures (3,913)
File trans... (3,140)
Contacts (1,933)
Voice mail (934)
Documents (57)
Videos (17)
Geolocation ... (7)

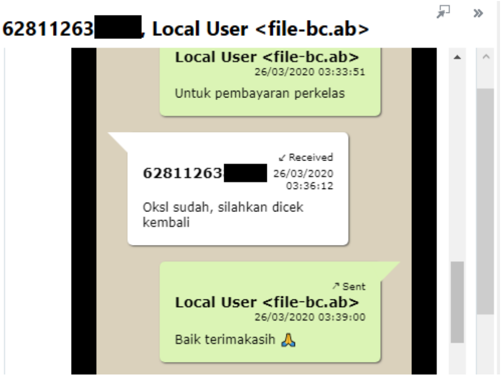
Predefined search

6,779 URL
2,122 Windows full path
20K Phone number
131 Payment card number
145 Postal code
3,791 Email address
349 Search engines results
2,467 IP address
5 MAC address

Application types

Figure 10. Extraction results on Belkasoft Evidence Center tools

Figure 10 is an analysis carried out by the Belkasoft Evidence Center tool to get several files, namely, Browser, Chats, Contacts, Documents, File transfers, Geolocation data, Pictures, Videos, and Voice mail. The Magnet AXIOM and Belkasoft Evidence Center tools have met the MDT-CR-02 criteria, namely being able to combine text correctly and MDT-CA-04, namely, being able to display message data (SMS, MMS, and Instant Messages) from conversations on the Whatsapp application as shown in Figure 11 for the AXIOM Magnet and Figure 12 for the Belkasoft Evidence Center.



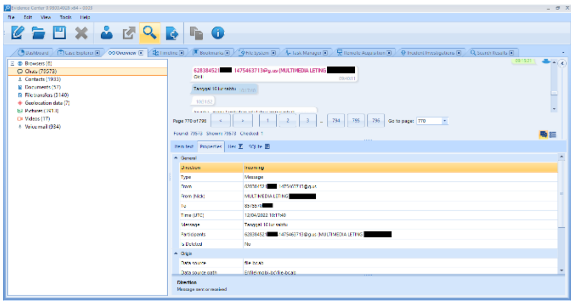
62811263[redacted], Local User <file-bc.ab>

Local User <file-bc.ab>
26/03/2020 03:33:51
Untuk pembayaran perkelas

62811263[redacted]
Received
26/03/2020 03:36:12
Oksl sudah, silahkan dicek kembali

Sent
Local User <file-bc.ab>
26/03/2020 03:39:00
Baik terimakasih 🙏

Figure 11. The Magnets AXIOM can combine text and display messages



Browsers (8)
Chats (79573)
Contacts (1933)
Documents (57)
File transfers (3140)
Geolocation data (7)
Pictures (3913)
Videos (17)
Voice mail (934)

628384521[redacted] 1475463713@g.us (MULTIMEDIA LETING [redacted]
Tanggal 16 lur sabtu

Page 770 of 796 Go to page: 770
Found: 79573 Shown: 79573 Checked: 1

General

Direction	Incoming
Type	Message
From	[illegible][redacted] 1475463713@g.us
From (Nick)	MULTIMEDIA LETING [redacted]
To	[illegible][redacted]
Time (UTC)	12/04/2022 10:17:40
Message	Tanggal 16 lur sabtu
Participants	628384521[redacted] 1475463713@g.us (MULTIMEDIA LETING [redacted]
Is Deleted	No

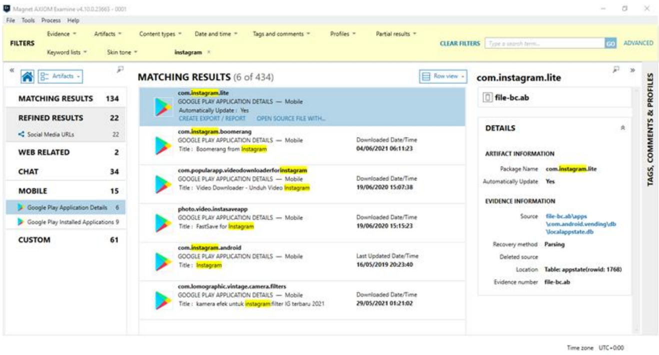
Origin

Data source	file-bc.ab
Data source path	E:\file\mobi-bc\file-bc.ab

Direction
Message sent or received

Figure 12. The Belkasoft Evidence Center can combine text and display messages.

The process carried out with the AXIOM Magnet tool found more artifacts than the Oxygen Forensic and Belkasoft Evidence Center tools. The AXIOM Magnet tool has successfully met the MDT-CA-8 parameter criteria, namely, that the AXIOM Magnet tool can display Instagram social media application data which can be seen in the following Figure 13.



MATCHING RESULTS	134
REFINED RESULTS	22
Social Media URLs	22
WEB RELATED	2
CHAT	34
MOBILE	15
Google Play Application Details	6
Google Play Installed Applications	9
CUSTOM	61

MATCHING RESULTS (6 of 434)

com.instagram.lite
GOOGLE PLAY APPLICATION DETAILS — Mobile
Automatically Update : Yes

com.instagram.boomerang
GOOGLE PLAY APPLICATION DETAILS — Mobile
Title : Boomerang from Instagram
Downloaded Date/Time 04/06/2021 06:11:23

com.popularapp.videodownloaderforinstagram
GOOGLE PLAY APPLICATION DETAILS — Mobile
Title : Video Downloader - Unduh Video Instagram
Downloaded Date/Time 19/06/2020 15:07:38

photo.video.instasaveapp
GOOGLE PLAY APPLICATION DETAILS — Mobile
Title : FastSave for Instagram
Downloaded Date/Time 19/06/2020 15:15:23

com.instagram.android
GOOGLE PLAY APPLICATION DETAILS — Mobile
Title : Instagram
Last Updated Date/Time 16/05/2019 20:23:40

com.lomographic.vintage.camera.filters
GOOGLE PLAY APPLICATION DETAILS — Mobile
Title : kamera efek untuk instagram filter IG terbaru 2021
Downloaded Date/Time 29/05/2021 01:21:02

com.instagram.lite
file-bc.ab

DETAILS

ARTIFACT INFORMATION
Package Name com.instagram.lite
Automatically Update Yes

EVIDENCE INFORMATION
Source file-bc.ab\apps\com.android.vending\db\localappstate.db
Recovery method Parsing
Deleted source
Location Table: appstate(rowid: 1768)
Evidence number file-bc.ab

Figure 13. The Magnet AXIOM can display social media application data.

Reporting

At this stage, the results of the analysis are reported based on the tests that have been carried out as a whole. The following is a report on the performance of the forensic tools presented in Figure 14.

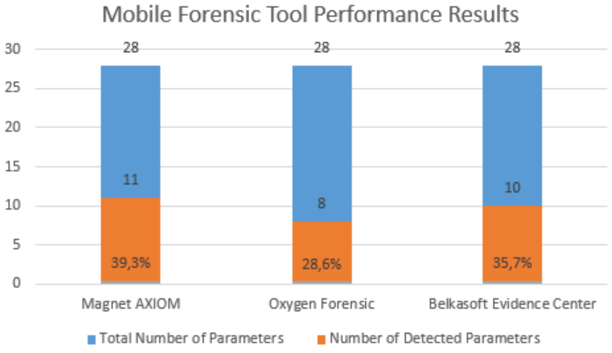


Figure 14. Forensic tools performance results

Report on the performance test results of each mobile forensic tool obtained with scenarios and parameter variables determined at the planning stage. The capabilities of each mobile forensic device can be calculated using a formula to get the desired accuracy index [10].

$$Par = \frac{\sum ar0}{\sum ar\,T} x\ 100\% \qquad (1)$$

Where Par is forensic tool accuracy index number, ar0 is number of detected variables and arT is all variables used

The accuracy index is used to measure the extent of the ability of each tool to extract data [5]. In this case, from an OPPO A37f backup android file which can be calculated as follows:

Magnet AXIOM:

$$Par = \frac{11}{28} \times 100\% = 39.3\%$$

Oxygen Forensic:

$$Par = \frac{28}{28} \times 100\% = 28.6\%$$

Belkasoft Evidence Center:

$$Par = \frac{10}{28} \times 100\% = 35.7\%$$

The results of testing the performance of mobile forensic tools on android backup files using the National Institute of Standards and Technology (NIST) method in detail can be seen in Table 2.

Table 2. Parameter result comparison

Parameter		Tools Mobile Forensic		
		Magnet AXIOM	Oxygen Forensic	Belkasoft Evidence Center
Core Features	MDT-CR-01	✓	✓	✓
	MDT-CR-02	✓	×	✓
	MDT-CR-03	✓	✓	✓
	MDT-CR-04	×	×	×
	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	✓	×	✓
	MDT-CA-10	×	×	×
	MDT-CA-11	✓	✓	✓
	MDT-CA-12	×	×	×
Optional Features	MDT-RO-01	×	×	×
	MDT-RO-02	×	×	×
	MDT-RO-03	×	×	×
	MDT-RO-04	×	×	×
	MDT-RO-05	×	×	×
	MDT-RO-06	×	×	×
	MDT-AO-01	×	×	×
	MDT-AO-02	×	×	×
	MDT-AO-03	×	×	×
	MDT-AO-04	×	×	×
	MDT-AO-05	×	×	×
	MDT-AO-06	×	×	×

CONCLUSIONS

The conclusion from the results of the research that has been done regarding comparing the results of forensic tools on android smartphone backup files using the NIST method is that the forensic tools used do not always meet every parameter set.

The results of the analysis of forensic tools as a whole, the Magnet AXIOM succeeded in extracting the longest time and got the highest accuracy index value of 39.3% with 11 parameters out of 28 fulfilled, followed by Belkasoft Evidence Center with extraction time faster than the Magnet AXIOM and an accuracy index score of 35.7% with 10 of the 28 parameters met. The Oxygen forensics extracted the fastest time between AXIOM Magnet and Belakssoft Evidence Center and had the lowest index performance value of 28.6%, which only met the 8 parameters of the 28 parameters set.

REFERENCES

[1] Statcounter, "Mobile Operating System Market Share Indonesia," 2022. https://gs.statcounter.com/os-market-share/mobile/indonesia

[2] I. Riadi, P. Studi Magister Teknik Informatika, and U. S. Ahmad Dahlan Yogyakarta Jl Soepomo Janturan, "Data Recovery Dengan Keamanan Fingerprint Pada Smartphone Android," *Semantikom.Unira.Ac.Id*, 2018.

[3] I. Z. Yadi and Y. N. Kunang, "Forensik Pada Platform Android," *Konf. Nas. Ilmu Komput.*, pp. 141–148, 2014.

[4] I. Riadi, A. Yudhana, and M. C. F. Putra, "Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method," *Sci. J. Informatics*, vol. 5, no. 2, pp. 235–247, 2018, doi: 10.15294/sji.v5i2.16545.

[5] A. ahmadi, T. Akbar, H. M. Putra, "Perbandingan Hasil Tool Forensik Pada File Image Smartphone Android Menggunakan Metode Nist," *JIKO (Jurnal Inform. dan Komputer)*, vol. 4, no. 2, pp. 92–97, 2021, doi: 10.33387/jiko.v4i2.2812.

[6] Fileinfo.com, "AB File Extension," 2022.

[7] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," *Natl. Inst. Stand. Technol.*, 2006.

[8] NIST, "Mobile Device Forensic Tool Specification , Test Assertions and Test Cases," no. May, pp. 1–18, 2019, [Online]. Available: https://www.nist.gov/system/files/documents/2019/07/11/mobile_device_forensic_tool_test_spec_v_3.0.pdf

[9] R. Rahmansyah, "Perbandingan Hasil Investigasi Barang Bukti Digital Pada Aplikasi Facebook Dan Instagram Dengan Metode Nist," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, pp. 49–57, 2021, doi: 10.14421/csecurity.2021.4.1.2421.

[10] I. Riadi, R. Umar, and A. Firdonsyah, "Forensic tools performance analysis on android-based blackberry messenger using NIST measurements," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 5, pp. 3991–4003, 2018, doi: 10.11591/ijece.v8i5.pp3991-4003.

AUTHORS BIBLIOGRAPHY

Permana Bangun Pangestu Born in Pacitan, East Java, on January 20, 1999, he is currently studying for a Bachelor's Degree in Computer Engineering at Universitas Amikom Yogyakarta. Research fields related to digital forensics. Email: Permana.20@students.amikom.ac.id

Muhammad Koprawi obtained a Bachelor's degree in Computer (S.Kom.), S1-Informatics Engineering Study Program STMIK AMIKOM Yogyakarta, graduated in 2013. Received a Master of Engineering (M.Eng) Postgraduate Program in Electrical Engineering (Information Technology) Unversitas Gadjah Mada Yogyakarta, graduated in 2017. Currently a Lecturer at Universitas Amikom Yogyakarta in the S1-Computer Engineering Study Program. Research fields related to Software Engineering and Web Security. Email: koprawi@amikom.ac.id