

JIKO

by Ahwan Ahmadi

Submission date: 11-Mar-2021 11:13PM (UTC-0800)

Submission ID: 1531016516

File name: 02-2812-7346-1-RV.docx (1.84M)

Word count: 2672

Character count: 16023

PERBANDINGAN HASIL TOOL FORENSIK PADA FILE *IMAGE* SMARTPHONE ANDROID MENGGUNAKAN METODE NIST

Ahwan Ahmadi¹, Taufik Akbar²

Program Studi Teknik Komputer, Fakultas Teknik Universitas Hamzanwadi
Jln. Prof. M.Yamin No.35 Pancor Lombok Timur

Email: ¹ahwanahmadi71@gmail.com, ²Aliakbar.akbar266@gmail.com

³
(Naskah masuk: dd mmm yyyy, diterima untuk diterbitkan: dd mmm yyyy)

Abstrak

Salah satu cara mengamankan suatu file agar tidak berubah-ubah pada sebuah teknik forensik digital adalah dengan cara membuat *cloning* suatu *devices* atau menyalin keseluruhan file pada suatu *devices* (smartphone) kedalam bentuk suatu file yaitu dalam bentuk file *Image* yang bisa dibuka dimanapun dan dengan tools apapun yang mendukung terbukanya file *Image* hasil *cloning* suatu *devices*. Penggunaan tools forensik digital khususnya *forensics mobile* tergantung dari pilihan *examiner* dalam melakukan ekstraksi data dari file *Image* tersebut. Metode *National Institute of Standard and Technology* (NIST) digunakan dalam penelitian ini dengan tahapan seperti *Collection/Preservation, Examination, Analysis* dan *Reporting*. Hasil ekstraksi yang kemudian dianalisa dengan menggunakan metode NIST didapatkan hasil dari penggunaan tool forensik seperti Belkasoft Evidence Center berhasil melakukan ekstraksi data dari sebuah file *Image* smartphone android Samsung GT-S5282 dengan tingkat akurasi ekstraksi data sebesar 66,66% dari variabel yang sudah ditentukan dan juga ditemukan file panggilan dan pesan yang sudah terhapus di *devices* pengguna. Tool Magnet AXIOM mendapatkan tingkat akurasi dari smartphone yang sama sebesar 55,55% dari variabel yang sudah ditentukan dan dalam proses analisis ditemukan banyak sekali file *carving* dalam *devices* pengguna. Hasil penelitian ini dapat disimpulkan bahwa tool Belkasoft Evidence Center lebih memiliki kinerja yang baik daripada tool Magnet AXIOM dalam proses ekstraksi data dari sebuah file *Image* smartphone android. Hasil penelitian ini bisa dijadikan sebagai rujukan bagi para *examiner* dalam menentukan tool forensik digital yang mumpuni dalam menangani sebuah kasus kejahatan digital.

Kata kunci: Digital Forensik Tools, Smartphone, *Image* File, NIST

COMPARISON OF FORENSIC TOOL RESULTS ON ANDROID SMARTPHONE IMAGE FILES USING NIST METHOD

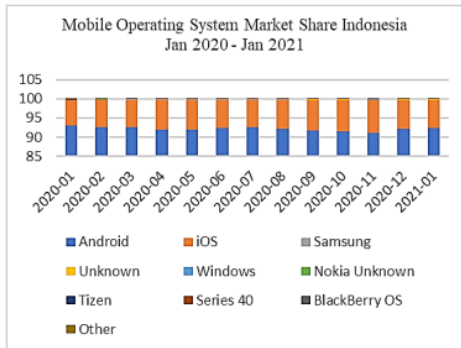
Abstract

One way to secure a file so that it doesn't change in a digital forensics technique is by cloning a device or copying the entire file on a device (smartphone) into a file, namely in the form of an image file that can be opened anywhere and with any tools. Which supports the opening of the Image file from cloned devices. The use of digital forensics tools, especially mobile forensics, depends on the choice of the examiner in extracting data from the image file. The National Institute of Standard and Technology (NIST) method was used in this study with stages such as *Collection / Preservation, Examination, Analysis* and *Reporting*. The extraction results were then analyzed using the NIST method, the results obtained from the use of forensic tools such as the Belkasoft Evidence Center successfully extracted data from an Android smartphone image file Samsung GT-S5282 with data extraction accuracy rate of 66.66% from predetermined variables and also found deleted call and message files on user services. The AXIOM Magnet Tool gets an accuracy rate from the same smartphone of 55.55% of the predetermined variables and in the analysis process found a lot of carving files in the user's devices. The results of this study can be concluded that the Belkasoft Evidence Center tool has better performance than the AXIOM Magnet tool in the data extraction process from an Android smartphone image file. The results of this study can be used as a reference for examiners in determining a digital forensic tool that is capable of handling a digital crime case.

Keywords: Digital Forensic Tools, Smartphones, Image Files, NIST

1. PENDAHULUAN

Smartphone semakin hari semakin berkembang pesat seiring dengan munculnya vendor-vendor baru yang dikeluarkan oleh masing-masing perusahaan smartphone. Di Indonesia Smartphone yang paling populer masih dikuasai oleh Smartphone bertipe Android seperti yang di tunjukkan pada Gambar 1, dimana di Indonesia sendiri tingkat penggunaan smartphone android mencapai persentase diangka 92.32% [1].



Gambar 1. Pangsa Pasar Sistem Operasi Seluler di Indonesia.

Smartphone android pada kuartal keempat mencapai angka penjualan sebesar 379.98 unit ditahun 2016 [2]. Dengan berbagai fitur yang semakin hari semakin bervariasi dengan kemudahan dalam mendapatkan aplikasi dari *play store* yang dapat diunduh secara gratis. Aplikasi yang didapatkan dari *Play store* juga sudah banyak yang mendekati aplikasi-aplikasi yang ada dikomputer PC atupun Leptop [3].

Pemanfaatan pengetahuan digital forensic dalam menganalisa sebuah smartphone bisa sangat di butuhkan terutama dalam hal investigasi digital. Digital forensic itu sendiri merupakan sebuah ilmu yang digunakan dalam membantu penegak hukum untuk mengatasi masalah kejahatan digital [4].

Penggunaan tools-tool foresik digital juga mendukung keberhasilan dari sebuah proses investigasi. Penggunaan tools dengan menerapkan kombinasi atau mencoba tools-tools lain yang tidak berpaku pada satu tools saja akan memberikan hasil yang maksimal kepada seorang examiner dalam melakukan ekstraksi data dari sebuah smartphone.

Fokus penelitian ini akan membandingkan tools forensic dengan pendekatan metode *National Institute of Standard and Technology* (NIST) pada hasil ekstraksi data dari sebuah file *Image* smartphone android yang tidak menyentuh langsung pada perangkatnya melainkan hasil ekstraksi dalam bentuk file *Image*. File *Image* sendiri merupakan file hasil ekstraksi data dari bentuk fisik smartphone android yang dicloning, biasanya tujuannya untuk melihat file-file yang dihapus dan proses ini tidak peduli apakah file yang di cloning ada isinya atau tidak.

2. METODE PENELITIAN

Penelitian ini menggunakan metode dari *National Institute of Standard and Technology* (NIST). Metode ini digunakan untuk menjabarkan bagaimana tahapan demi tahapan secara rinci dan sistematis, sehingga dapat menyelesaikan permasalahan yang ada. Melakukan teknik forensic dan analisa yang benar memungkinkan memiliki tingkat keberhasilan 100% dalam mengumpulkan data forensik [5].

Metode NIST terdiri dari 4 tahapan yaitu *Collection, Examination, Analysis, dan Reporting*. Skema metode NIST mobile forensik disajikan pada Gambar 2 [6].



Gambar 2. Skema metode NIST mobile forensik

Penjelasan dari skema metode *National Institute of Standard and Technology* (NIST) adalah sebagai berikut:

1. Collection/Preservation

Tahap ini disebut juga tahap preservasi. Collection merupakan koleksi, atau identifikasi barang bukti yang digunakan berupa perangkat keras yang akan diambil datanya untuk digunakan sebagai bukti digital dari suatu kasus kejahatan digital. Proses ini dilakukan dengan mengikuti langkah pengamanan integritas data.

2. Examination

Examination merupakan proses pengambilan data pada barang bukti menggunakan tool forensic terpercaya sehingga data yang diperoleh memiliki integritas tinggi.

3. Analysis

Tahap ini adalah proses menganalisis dan mengevaluasi kembali data yang ditemukan dari hasil examination.

4. Reporting

Tahap reporting merupakan proses pelaporan hasil analisis yang meliputi informasi data yang berhasil ditemukan yang dijadikan sebagai laporan akhir proses forensic yang dilakukan.

2.1. Skenario Kasus

Skenario kasus dibutuhkan untuk melakukan proses forensic pada smartphone dengan beberapa variabel untuk mendapatkan hasil yang maksimal dibuat skenario kasus dapat dilihat pada Gambar 3.



Gambar 3. Flowchart Proses Forensik

Setelah smartphone didapatkan file *Imagena* kemudian dilakukan proses ekstraksi dengan prosedur *Forensics Mobile Phone* untuk dapat dilihat hasilnya. Dalam memudahkan pencarian data digital dalam sebuah proses forensik, maka difokuskan untuk membuat variabel pencarian data digital seperti pada Tabel 1.

Tabel 1. Variabel yang Digunakan

1	Browser/Web Related
2	Calendar
3	Calls
4	Contacts
5	Documents
6	Encrypted files
7	Installed Application
8	Mail
9	Other Files
10	P2p
11	Pictures
12	Pesan/Chat
13	Videos
14	Wifi Connection
15	Thumbnails
16	Mobile Application
17	Instant messenger
18	Operating System
19	Custom
20	Social Networking
21	AMR Files
22	Carved audio
23	Google WebP Images
24	Photoshop Files
25	Refined Results
26	Custom
27	Delete Files
28	Files Carving

Melalui tabel variabel tersebut akan dilakukan proses *Forensics Mobile Phone* untuk mendapatkan data digital yang sesuai.

2.2. Belkasoft Evidence Center

Belkasoft Evidence Center adalah salah satu perangkat lunak yang direkomendasikan untuk para praktisi digital forensik dengan kemampuan yang di miliki perangkat lunak ini seperti memperoleh,

mencari, dan menganalisa bukti digital baik dari perangkat Komputer maupun mobile. Belkasoft Evidence Center memiliki kemampuan ekstraksi data dari berbagai sumber seperti *hard drive, drive Image cloud, memmory dumps, Android* dan berbagai jenis *platform* lainnya. Belkasoft Evidence Center akan menganalisa sumber data dan artefak yang paling penting secara otomatis yang tersedia pada perangkat *devices* dan menyajikannya kepada *examiner* untuk dianalisa lebih lanjut dan hasil akhir dari proses forensiknya akan menjadi sebuah laporan data yang dicari [7].

2.3. Magnet Axiom

Magnet Axiom adalah salah satu dari perangkat lunak digital forensik yang bisa direkomendasikan bagi para penggiat digital forensik karna Software ini memiliki kemampuan untuk menangkap dan menganalisa *smartphone, komputer, cloud, IoT* dan hasil *imaging* dari *software* lain. Magnet Axiom dapat menyederhanakan investigasi dengan menampilkan barang bukti yang relevan sebagai artefak yang mudah untuk dilihat dan membantu setiap langkah dalam proses *akuisisi, recovery* data, analisa dan pelaporan [8].

3. HASIL dan PEMBAHASAN

3.1. Tahapan Collection/Preservation

Metode *National Institute of Standard and Technology (NIST)* merupakan salah satu dari metode digital forensik yang populer digunakan dengan tahapan yang cukup lengkap dan mudah dipahami dalam menemukan data digital. Proses mendapatkan data digital pada *smartphone android* menggunakan beberapa perangkat lunak forensik digital diantaranya *Belkasoft Evidence Center* dan *Magnet Axiom*. Berikut adalah Tabel 2 dan Tabel 3 tentang informasi perangkat *software dan hardware* yang digunakan dalam penelitian ini.

Tabel 2. Alat Penelitian

No	Tool Penelitian	Keterangan
1	Laptop	Lenovo IdeaPad S340, Windiws 10 64 bit
2	File Image Smartphone	Samsung GT-S5282

Tabel 3. Tools Forensik

No	Forensik Tool	Keterangan
1	Belkasoft Evidence Center	Berbasis windows, aplikasi yang dapat digunakan untuk memperoleh data digital pada <i>smartphone</i>
2	Magnet Axiom	Berbasis windows, aplikasi yang dapat digunakan untuk memperoleh data digital pada <i>smartphone</i>

Tahapan pertama yang dilakukan sesuai dengan metode NIST adalah proses mengidentifikasi atau *Collection file Image* *smartphone* yang didapatkan yang nantinya akan dijadikan acuan pada pencarian

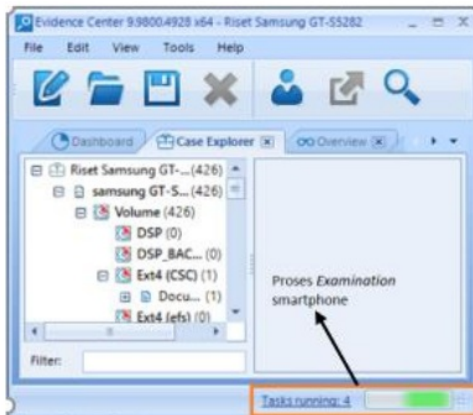
data digital sesuai dengan variabel yang sudah dibuat. File *Image* dari smartphone dapat di lihat pada Gambar 4 serta dilakukan tahapan *Peservation* untuk mengamankan *devices* agar data yang didapatkan tidak berubah secara signifikan dengan cara menempatkan file *Image* pada satu perangkat media penyimpanan dan tidak menggabungkannya dengan file lain.

Name	Date modified	Type	Size
samsung GT-S5282	1/6/2021 11:47 PM	Disc Image File	3,817,472 KB
samsung GT-S5282.img_info	1/6/2021 11:47 PM	WinRAR ZIP archive	17 KB

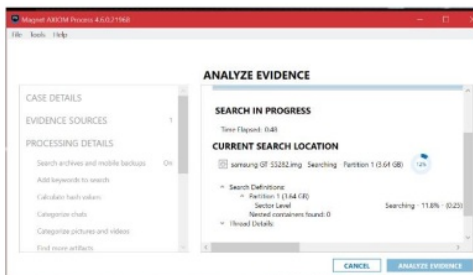
Gambar 4. File *Image* Smartphone Penelitian

3.2. Tahapan Examination

Tahapan Examination dilakukan apabila tahapan Collection dan Preservation sudah dilakukan dengan baik dan benar, selanjutnya menerapkan proses dari tahapan examination yaitu proses pengambilan atau ekstraksi data digital file *Image* smartphone yang sudah ada pada Tabel 2 dengan tool forensik yang ditunjukkan pada Gambar 5 dan 6 dengan tool yang akan diuji diantaranya Belkasoft Evidence Center dan Magnet AXIOM.



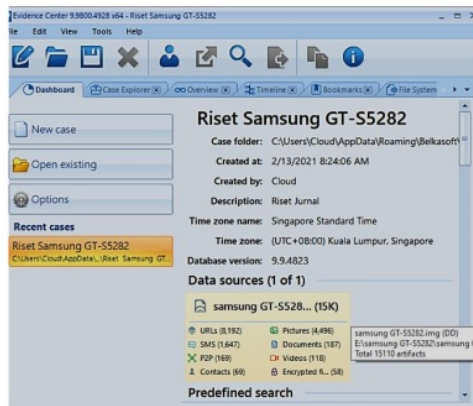
Gambar 5. Proses Examination dengan tool Belkasoft Evidence Center



Gambar 6. Proses Examination dengan tool Magnet AXIOM

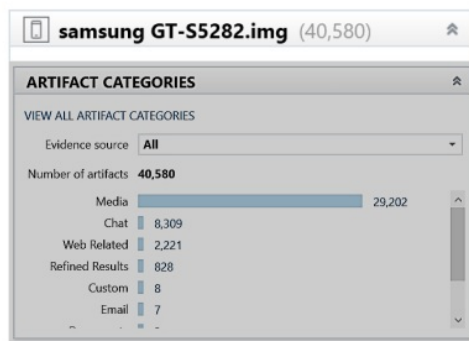
3.3. Tahapan Analisis

Analisa dilakukan dari hasil tahapan Examination atau ekstraksi data file *Image* smartphone dengan hasil yang didapatkan seperti yang ditunjukkan pada Gambar 7 dengan tools Belkasoft Evidence Center dan Gambar 8 dengan tool Magnet AXIOM.



Gambar 7. Hasil ekstraksi data Samsung GT-S5282 dengan Belkasoft Evidence Center

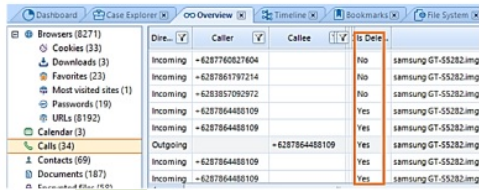
Hasil Analisa data smartphone Samsung GT-S5282 dari Gambar 7 dengan menggunakan tool Belkasoft Evidence Center memperlihatkan beberapa data digital yang berhasil diekstraksi dari sebuah file *Image* smartphone seperti file *URLs*, *SMS*, *P2P*, *Contacts*, *Pictures*, *Documents*, *Videos*, *Encrypted files* dengan total 15110 artifak yang ditemukan oleh aplikasi.



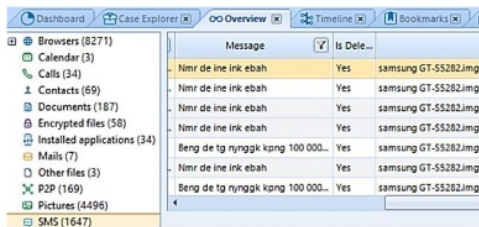
Gambar 8. Hasil ekstraksi data Samsung GT-S5282 dengan tool Magnet AXIOM

Analisa yang dilakukan oleh tool Magnet AXIOM pada Gambar 8 mendapat beberapa file diantaranya file *Media*, *Chat*, *Web Related*, *Refined Results*, *Custom*, *Email*, *Documents*, *OS*, *Social Networking* dengan total artifak yang berhasil di ekstraksi berjumlah 40,580 file. Proses Analisis dengan menggunakan tool Belkasoft Evidence Center ditemukan beberapa file yang sudah dihapus oleh

22 pemilih *devices* seperti yang di tunjukkan pada Gambar 9 dan Gambar 10.



Gambar 9. panggilan keluar dan masuk yang terhapus *didevices*



Gambar 10. pesan yang terhapus *didevices*

Proses yang dilakukan dengan tool Magnet AXIOM menemukan banyak file *carving* (File carving digunakan untuk pemulihan data [9]) pada hasil ekstraksi data dan tidak menemukan file yang terhapus seperti 13 nya dengan tool Belkasoft Evidence Center seperti yang ditunjukkan pada Gambar 11.

EVIDENCE (110)			
Cont...	Save...	S...	Recovery M...
Quicktime	3947662	samsu...	Carving
Quicktime	19570146	samsu...	Carving
Quicktime	1039703	samsu...	Carving
Quicktime	903880	samsu...	Carving
Quicktime	14132985	samsu...	Carving
Quicktime	4726476	samsu...	Carving
Quicktime	20971520	samsu...	Carving
Quicktime	4762787	samsu...	Carving
Quicktime	4704465	samsu...	Carving
Quicktime	1987785	samsu...	Carving
Quicktime	136204	samsu...	Carving
Quicktime	2301478	samsu...	Carving
Quicktime	4720126	samsu...	Carving
Quicktime	1014332	samsu...	Carving

Gambar 11. file carving yang ditemukan pada data hasil ekstraksi

3.4. Reporting

Tahapan akhir dari metode NIST adalah Reporting atau pelaporan terhadap proses yang dilakukan untuk menampilkan kembali hasil yang dilakukan pada tahapan sebelumnya setelah dilakukan ekstraksi data dari tool yang berbeda.

Perbandingan data hasil ekstraksi dari sebuah file *Image* smartphone samsung GT-S5282 menggunakan tool Belkasoft Evidence Center dan Magnet AXIOM dengan menggunakan variabel yang dapat dilihat pada Tabel 1. Variabel data digital hasil ekstraksi dari

5 kedua tool forensik yang digunakan dapat dilihat lebih detail pada Tabel 3.

Tabel 3. Hasil Variabel

No	Hasil Ekstraksi Yang Didapat	Tool	
		Jumlah Hasil Ekstraksi dari Belkasoft Evidence Center	Jumlah Hasil Ekstraksi dari Magnet AXIOM
1	Browser/Web Related	✓	5
2	Calender	✓	x
3	Calls	✓	x
4	Contacts	✓	x
5	Documents	✓	✓
6	Encrypted files	✓	x
7	Installed Application	✓	x
8	Mail	✓	✓
9	Other Files	✓	x
10	P2p	✓	x
11	Pictures	✓	✓
12	Pesan/Chat	✓	✓
13	Videos	✓	✓
14	Wifi Connection	✓	x
15	Thumbnails	✓	x
16	Mobile Application	✓	x
17	Instant messenger	✓	x
18	Operating System	x	✓
19	Custom	x	✓
20	Social Networking	x	✓
21	AMR Files	x	✓
22	Carved audio	x	✓
23	Google WebP Images	x	✓
24	Photoshop Files	x	✓
25	Refined Results	x	✓
26	Deleted Files	✓	x
27	File Carving	x	✓
Indeks Score		18	15



Gambar 12. Jumlah Data Yang Diperoleh

Keseluruhan hasil yang didapatkan berdasarkan pengujian dari kedua tool, skenario dan variabel yang sudah ditentukan pada tahapan perencanaan. Kemampuan masing-masing tool dapat dihitung dengan menggunakan rumus untuk mendapatkan indeks akurasi yang diinginkan [10].

$$Par = \frac{\sum ar_0}{\sum ar_T} \times 100\% \quad (1)$$

Par adalah angka indeks akurasi alat forensik ar₀ adalah jumlah variabel yang terdeteksi ar_T jumlah keseluruhan variabel yang digunakan Indeks akurasi digunakan untuk mengukur sejauh mana kemampuan masing-masing tools dalam melakukan ekstraksi data dari sebuah file *Image* samsung GT-S5282 yang dapat dihitung seperti berikut :

Belkasoft Evidence Center :

$$Par = \frac{18}{27} \times 100\% = 66,66\%.$$

Magnet AXIOM :

$$Par = \frac{15}{27} \times 100\% = 55,55\%.$$

Berdasarkan perhitungan indeks akurasi dari alat dan teknik forensik yang digunakan dalam ekstraksi data dengan variabel yang sudah ditentukan maka didapatkan hasil dengan tool Belkasoft Evidence Center mendapat tingkat akurasi sebesar 66,66% dan tool Magnet AXIOM sebesar 55,55%.

4. KESIMPULAN

Berdasarkan hasil penelitian ini perbandingan hasil ekstraksi data dari sebuah file *Image* smartphone samsung GT-S5282, dapat disimpulkan bahwa penggunaan tool forensik yang sesuai dalam melakukan ekstraksi data didapatkan banyak sekali data walaupun devices tidak ada secara fisik hanya mendapatkan file *Image* saja, akan tetapi data yang berhasil diekstraksi dan melakukan analisa lebih mendalam dari file tersebut dapat memberikan gambaran seperti file *browser, calls, document, contacts, delete files, file carving* dan data lainnya dapat diekstraksi dengan baik menggunakan metode *National Institute of Standard and Technology (NIST)*. Tool Belkasoft Evidence Center memberikan nilai indeks akurasi sebesar 66,66% dengan 18 variabel dari 27 total variabel yang terpenuhi, lebih tinggi dari Magnet AXIOM dengan nilai 55,55% dari 27 variabel yang sudah ditentukan hanya 15 variabel yang terpenuhi.

5. DAFTAR PUSTAKA

- [1] Statcounter, 2021. "Mobile Operating System Market Share Indonesia". Tersedia [https://gs.statcounter.com/os-market-share/mobile/indonesia] diakses 9 Februari 2021.
- [2] I. Riadi, S. Sunardi, and Sahiruddin, "Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 1, pp. 197–204, 2020, doi: 10.25126/jtiik.202071921.

- [3] A.-Ahmadi, "Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ)," *J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf.*, vol. 4, no. 1, p. 8, 2018, doi: 10.24014/coreit.v4i1.5803.
- [4] A. L. Messenger, "A Study Mobile Forensic Tools Evaluation on," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 10, pp. 201–208, 2018.
- [5] R. A. Putra, A. Fadlil, and I. Riadi, "Forensik Mobile Pada Smartwach Berbasis Android," *Jurti*, vol. 1, no. 1, pp. 41–47, 2017.
- [6] R. Umar, I. Riadi, and G. M. Zamroni, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," no. June, 2018, doi: 10.18517/ijaseit.8.3.3591.
- [7] I. Riadi, S. Sunardi, and S. Sahiruddin, "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)," *J. Rekayasa Teknol. Inf.*, vol. 3, no. 1, pp. 87–95, 2019.
- [8] Bounga, 2021. "Magnet Axiom". Tersedia [https://bounga.id/products/magnet-axiom] diakses 14 Februari 2021.
- [9] D. T. Yuwono and Y. W., "Analisis Perbandingan Carving Dengan Metode Nist," *J. Sains Komput. dan Teknol. Inf.*, vol. 2, no. 2, pp. 1–6, 2020, doi: 10.33084/jsakti.v2i2.1472.
- [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.

ORIGINALITY REPORT

23%

SIMILARITY INDEX

22%

INTERNET SOURCES

8%

PUBLICATIONS

6%

STUDENT PAPERS

PRIMARY SOURCES

1	jtiik.ub.ac.id Internet Source	6%
2	jurnal.iaii.or.id Internet Source	3%
3	Submitted to Universitas Brawijaya Student Paper	1%
4	ojs.uho.ac.id Internet Source	1%
5	idoc.pub Internet Source	1%
6	journal.unilak.ac.id Internet Source	1%
7	repository.its.ac.id Internet Source	1%
8	Submitted to School of Business and Management ITB Student Paper	1%
9	jurnal.upnyk.ac.id	

Internet Source

1%

10

digilib.isi.ac.id

Internet Source

1%

11

ejournal.unkhair.ac.id

Internet Source

1%

12

repository.unpas.ac.id

Internet Source

1%

13

fr.scribd.com

Internet Source

1%

14

media.neliti.com

Internet Source

1%

15

e-journal.hamzanwadi.ac.id

Internet Source

1%

16

dev.kinetik.umm.ac.id

Internet Source

<1%

17

ejournal.uin-suska.ac.id

Internet Source

<1%

18

repositor.umm.ac.id

Internet Source

<1%

19

www.neliti.com

Internet Source

<1%

20

Olivia Michelle, Agustinus Fritz Wijaya.

<1%

"Strategic Planning for IS/IT Using Ward and Peppard at Maman Elektronik Sokaraja",
INTENSIF: Jurnal Ilmiah Penelitian dan
Penerapan Teknologi Sistem Informasi, 2020

Publication

21

123dok.com

Internet Source

<1%

22

journal.upgris.ac.id

Internet Source

<1%

23

download.garuda.ristekdikti.go.id

Internet Source

<1%

24

www.rifkadroid.com

Internet Source

<1%

25

motivasionline.com

Internet Source

<1%

26

pemerogaman.blogspot.com

Internet Source

<1%

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off