JIKO (Jurnal Informatika dan Komputer)
Vol. 4, No. 2, Agustus 2021, hlm. 92-97
DOI: 10.33387/jiko

Akreditasi KEMENRISTEKDIKTI, No.36/E/KPT/2019
p-ISSN: 2614-8897
e-ISSN: 2656-1948

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

Ahwan Ahmadi[1], Taufik Akbar[2], Hadian M Putra[3]

[1,2,3]Program Studi Teknik Komputer, Fakultas Teknik Universitas Hamzanwadi
Email: [1]ahwanahmadi71@gmail.com, [2]Aliakbar.akbar266@gmail.com, [3]hadian_mandala@hamzanwadi.ac.id

(Naskah masuk: 18 Februari 2021, diterima untuk diterbitkan: 21 Mei 2021)

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*an 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 *Coolection/Preservation*, *Examination, Analysis* dan *Reporting*. Hasil ekstraksi kemudian dianalisa dengan menggunakan metode NIST didapatkan hasil dari penggunaan *tools* forensik 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 ditentukan dan juga ditemukan file panggilan dan pesan yang sudah terhapus di*devices* pengguna. *Tools* 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 *tools* Belkasoft Evidence Center lebih memiliki kinerja yang baik daripada *tools* Magnet AXIOM dalam proses *exstraksi* data dari sebuah file *Image* smartphone android. Hasil penelitian ini bisa dijadikan sebagai rujukan bagi para examiner dalam menentukan *tools* forensik digital yang mumpuni dalam menangani sebuah kasus kejahatan digital.

Kata kunci: Tool Digital Forensik , Smartphone, File image, NIST

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

Abstract

One way to secure a file so that it does not change in a digital forensic 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 an Image file from cloned devices. The use of digital forensic 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 phases such as Coolection / Preservation, Examination, Analysis and Reporting. The extraction results were then analyzed using the NIST method. The results obtained from the use of Belkasoft Evidence Center forensic tools were successful in extracting data from an image file of the Samsung GT-S5282 android smartphone with an accuracy rate of data extraction of 66.66% of the specified variables and also found a call file and messages that have been deleted on user services. The AXIOM Magnet Tools get 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 on 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 digital forensic tools that are capable of handling a digital crime case.

Keywords: *Digital Forensic Tools, Smartphone, Image file, NIST*

1. PENDAHULUAN

Smartphone semakin hari semakin berkembang pesat seiring dengan munculnya *vendor-vendor* baru

yang dikeluarkan oleh masing-masing perusahaan smartphone, hampir setiap minggu perkembangan merk dan fitur terus berkembang [1]. Di Indonesia smartphone yang paling populer masih dikuasai oleh smartphone bertipe Android seperti yang dilansir pada *Mobile operating system Market Share* Indonesia, dimana diindonesia sendiri tingkat penggunaan smartphone android mencapai peresentasi diangka 92.32% [2].

Mobile operating system Market Share Indonesia dari bulan Januari 2020 sampai dengan bulan Januari 2021 smartphone android terus mengalami peningkatan terlebih pada kuartal keempat mencapai angka penjualan sebesar 379.98 unit ditahun 2016 [3]. Smartphone android bisa digunakan oleh setiap orang yang ingin menggunakannya dengan berbagai fitur yang semakin hari semakin bervariasi dengan kemudahan dalam mendapatkan aplikasi dari *play store* yang dapat diunduh secara gratis [4]. Aplikasi yang didapatkan dari *Play store* juga sudah banyak yang mendekati aplikasi-aplikasi yang ada dikomputer PC ataupun Leptop [5], kemampuan dari aplikasi-aplikasi smartphone juga telah mencangkup banyak sekali penggunaan termasuk game, *social* media, perbankan online dan saham perdagangan [6].

Pemanfaatan pengetahuan digital forensik dalam menganalisa sebuah smartphone bisa sangat di butuhkan terutama dalam hal investigasi digital. Digital forensik sendiri merupakan sebuah ilmu yang digunakan dalam membantu penegak hukum untuk mengatasi masalah kejahatan digital [7], dalam hal ini dimaksudkan untuk pembuktian tindak kejahatan digital dan mendapatkan bukti digital yang valid [8].

Penggunaan *tools-tools* 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* forensik 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 di*cloning*, biasanya tujuannya untuk melihat file-file yang dihapus dan proses ini tidak perduli apakah file yang di*cloning* ada isinya atau tidak.

2. METODE PENELITIAN

Metode dan tahapan proses forensik digital telah banyak dikembangkan oleh penyidik dan praktisi forensik [9]. 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 permasalah yang ada. Metode yang digunakan bertujuan untuk mempertahankan hasil yang didapatkan, sehingga bisa dijadikan sebagai bukti hukum [10].

Metode NIST terdiri dari 4 tahapan yaitu *Collection*, *Examination*, *Analysis*, dan *Reporting*. Skema metode NIST *mobile forensics* disajikan pada Gambar 1 [11].

Gambar 1. Skema metode NIST *mobile forensics*

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 *tools* forensik terpercaya sehingga data yang diperoleh memiliki integritas tinggi.

3. *Analysis*

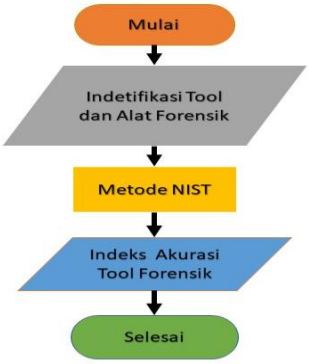
Tahap ini adalah proses menganalisis dan mengevaluasi kembali data yang ditemukan dari hasil *examination*.

4. *Reporting*

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

2.1. Skenario Kasus

Skenario kasus dibutuhkan untuk melakukan proses forensik pada smartphone dengan beberapa variabel, untuk mendapatkan hasil yang maksimal dibuat skenario kasus dapat dilihat pada Gambar 2.



Gambar 2. *Flowchart* Proses Forensik

Setelah smartphone didapatkan file *Image*nya 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	*Calender*
3	*Calls*
4	*Contacts*
5	*Documents*
6	*Encypted files*
7	*Installed Application*
8	*Mail*
9	*Other Files*
10	*P2p*
11	*Pictures*
12	*Pesan/Chat*
13	*Vidios*
14	*Wifi Connection*
15	*Thumbnails*
16	*Mobile Applicatiion*
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, Ios, Android* dan berbagai jenis *platform* lainnya. Belkasoft Evidence Center akan menganalisa sumber data dan artifak 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 [12].

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 artifak yang mudah untuk dilihat dan membantu setiap langkah dalam proses *akuisisi, recovery* data, analisa dan pelaporan [13].

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.

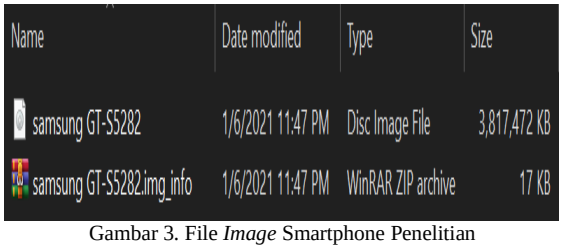
Tabel 2. Alat Penelitian

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 smartphone
2	Magnet Axiom	Berbasis windows, aplikasi yang dapat digunakan untuk memperoleh data digital pada smartphone

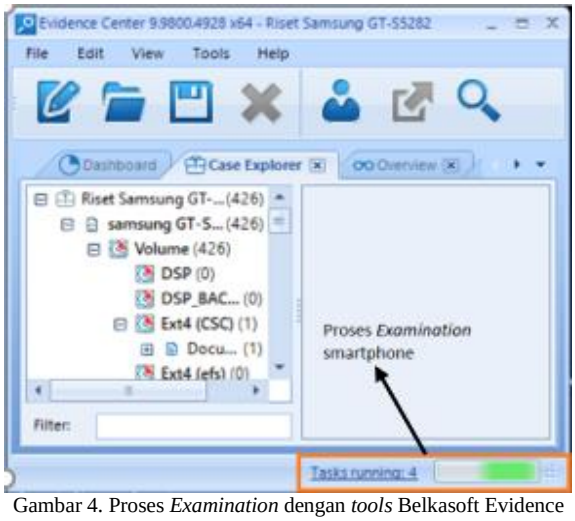
Tahapan pertama yang dilakukan sesuai dengan metode NIST adalah proses mengidentifikasi atau *Collection* file *Image* smartphone yang didapatkan yang nantinya akan dijadikan acuan pada pencarian data digital sesuai dengan variabel yang sudah dibuat. File *Image* dari smartphone dapat dilihat pada Gambar 3 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.



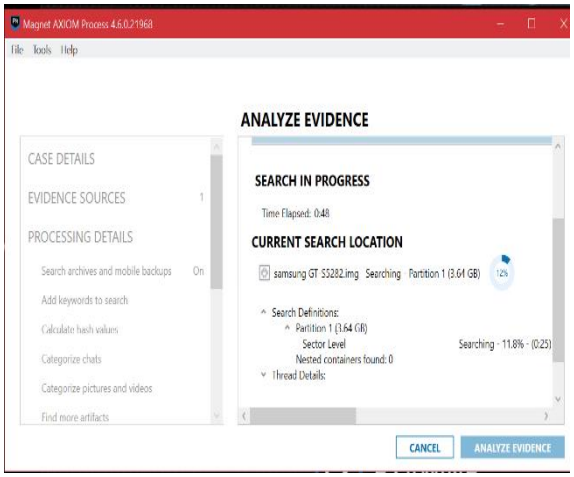
Gambar 3. File *Image* Smartphone Penelitian

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 *tools* forensik yang ditunjukkan pada Gambar 4 dan 5 dengan tool yang akan diuji diantaranya Belkasoft Evidence Center dan Magnet AXIOM.



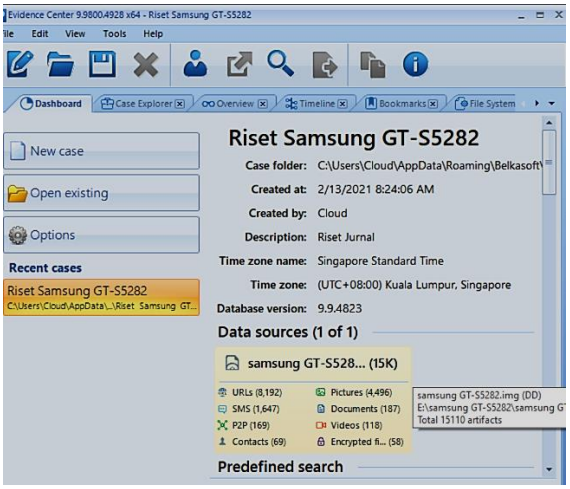
Gambar 4. Proses *Examination* dengan *tools* Belkasoft Evidence Center



Gambar 5. Proses *Examination* dengan *tools* Magnet AXIOM

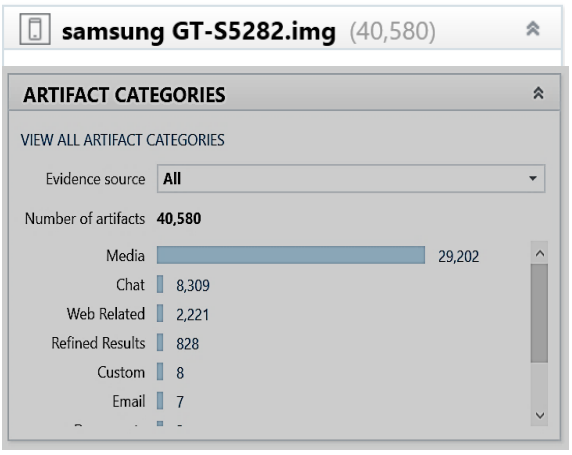
3.3. Tahapan *Analisis*

Analisa dilakukan dari hasil tahapan *Examination* atau ekastraksi data file *Image* smartphone dengan hasil yang didapatkan seperti yang ditunjukkan pada Gambar 6 dengan *tools* Belkasoft Evidence Center dan Gambar 7 dengan *tools* Magnet AXIOM.



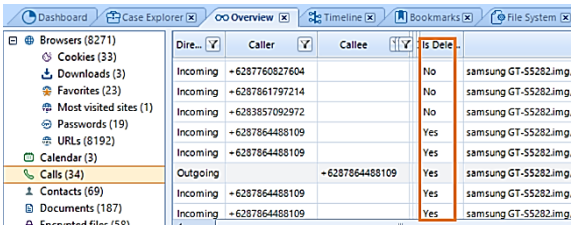
Gambar 6. Hasil ekstraksi data Samsung GT-S5282 dengan Belkasoft Evidence Center

Hasil Analisa data smartphone Samsung GT-S5282 dari Gambar 6 dengan menggunakan *tools* Belkasoft Evidence Center memperlihatkan bebarapa data digital yang berhasil diekstraksi dari sebuah file *Image* smartphone seperti file *URLs*, *SMS*, *P2P*, *Contacts*, *Pictures*, *Documents*, *Vidios*, *Encypted files* dengan total 15110 artifak yang ditemukan oleh aplikasi.

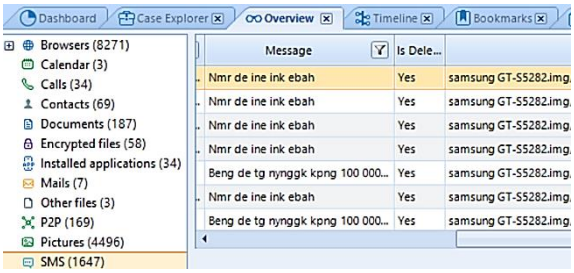


Gambar 7. Hasil ekstraksi data Samsung GT-S5282 dengan *tools* Magnet AXIOM

Analisa yang dilakukan oleh *tools* Magnet AXIOM pada Gambar 7 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 *tools* Belkasoft Evidence Center ditemukan beberapa file yang sudah dihapus oleh pemilik *devices* seperti yang di tunjukkan pada Gambar 8 dan Gambar 9.

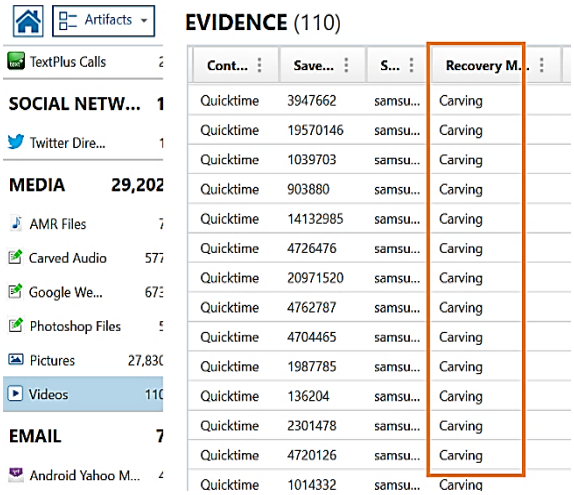


Gambar 8. Panggilan keluar dan masuk yang terhapus di*devices*



Gambar 9. Pesan yang terhapus di*devices*

Proses yang dilakukan dengan *tools* Magnet AXIOM menemukan banyak sekali file *carving* (*files carving* digunakan untuk pemulihan data [14]) pada hasil ekstraksi data dan tidak menemukan file yang terhapus seperti halnya dengan *tools* Belkasoft Evidence Center seperti yang ditunjukkan pada Gambar 10.



Gambar 10. File *carving* yang ditemukan pada data hasil ekstraksi

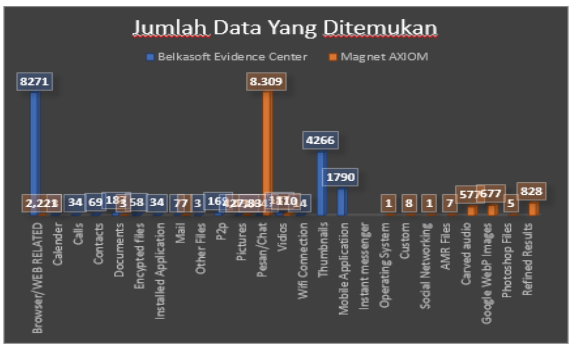
3.4. *Reporting*

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 *tools* yang berbeda.

Perbandingan data hasil ektraksi dari sebuah file *Image* smartphone samsung GT-S5282 mengunakan *tools* Belkasoft Evidence Center dan Magnet AXIOM dengan menggunakan variabel yang dapat dilihat pada Tabel 1. Variabel data digital hasil ekstraksi dari kedua *tools* forensik yang digunakan dapat dilihat lebih detail pada Tabel 3.

Tabel 3. Hasil Variabel

No	Hasil Ekstraksi Yang Didapat	*Tools*	
		Jumlah Hasil Ekstraksi dari Belkasoft Evidence Center	Jumlah Hasil Ekstraksi dari Magnet AXIOM
1	*Browser/Web Related*	✓	✓
2	*Calender*	✓	x
3	*Calls*	✓	x
4	*Contacts*	✓	x
5	*Documents*	✓	✓
6	*Encypted files*	✓	x
7	*Installed Application*	✓	x
8	*Mail*	✓	✓
9	*Other Files*	✓	x
10	*P2p*	✓	x
11	*Pictures*	✓	✓
12	*Pesan/Chat*	✓	✓
13	*Vidios*	✓	✓
14	*Wifi Connection*	✓	x
15	*Thumbnails*	✓	x
16	*Mobile Applicatiion*	✓	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 berdasrkan pengujian dari kedua *tools*, skenario dan variabel yang sudah ditentukan pada tahapan perencanaan. Kemampuan masing-masing *tools* dapat dihitung dengan menggunakan rumus untuk mendapatkan indeks akurasi yang diinginkan [15].

$$Par = \frac{\sum ar0}{\sum arT} \; x \; 100\% \qquad (1)$$

Par adalah angka indeks akurasi alat forensik
ar0 adalah jumlah variabel yang terdeteksi

arT 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 = $\frac{18}{27}\ x\ 100\% = 66{,}66\%$.

Magnet AXIOM :
Par = $\frac{15}{27}\ x\ 100\% = 55{,}55\%$.

Berdasarkan perhitungan indeks akurasi dari alat dan teknik forensik yang digunkan dalam ekstraksi data dengan variabel yang sudah ditentukan maka didapatkan hasil dengan *tool* Belkasoft Evidence Center mendaptkan tingkat akurasi sebesar 66,66% dan *tools* 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 *tools* 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). *Tools* 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] I. Riadi, S. Sunardi, and A. Firdonsyah, 2018. "Comparative Analysis of Forensic Software on Android-based Blackberry Messenger using NIJ Framework," *Proceeding Electr. Eng. Comput. Sci. Informatics*, vol. 5, no. 5, pp. 16–18, doi: 10.11591/eecsi.v5i5.1615.

[2] Statcounter, 2021. "Mobile Operating System Market Share Indonesia". Tersedia [https://gs.statcounter.com/os-market-share/mobile/indonesia] diakses 9 Februari

[3] I. Riadi, S. Sunardi, and Sahiruddin, 2020. "Perbandingan Tool Forensik Data Recovery Berbasis Android Menggunakan Metode NIST," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 7, no. 1, pp. 197–204, doi: 10.25126/jtiik.202071921.

[4] M. RG Hattari, S. Lutfi, and A. Khairan, 2018. "Perancangan Aplikasi Android Sistem Informasi Akademik Universitas Khairun Ternate," *JIKO (Jurnal Inform. dan Komputer)*, vol. 1, no. 2, pp. 76–84, doi: 10.33387/jiko.v1i2.773.

[5] A. Ahmadi, 2018. "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, doi: 10.24014/coreit.v4i1.5803.

[6] X. Lin, T. Chen, T. Zhu, K. Yang, and F. Wei, 2018. "Automated forensic analysis of mobile applications on android devices," *Proc. Digit. Forensic Res. Conf. DFRWS 2018 USA*, vol. 26, pp. S59–S66, doi: 10.1016/j.diin.2018.04.012.

[7] A. L. Messenger, 2018. "A Study of Mobile Forensic Tools Evaluation on," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 10, pp. 201–206.

[8] I. Riadi, S. Sunardi, and M. E. Rauli, 2018. "Identifikasi Bukti Digital WhatsApp pada Sistem Operasi Proprietary Menggunakan Live Forensics," *J. Tek. Elektro*, vol. 10, no. 1, pp. 18–22, doi: 10.15294/jte.v10i1.14070.

[9] M. N. Faiz, W. A. Prabowo, and M. F. Sidiq, 2018. "Studi Komparasi Investigasi Digital Forensik pada Tindak Kriminal," *J. Informatics, Inf. Syst. Softw. Eng. Appl.*, vol. 1, no. 1, pp. 63–70, doi: 10.20895/INISTA.V1I1.

[10] I. Zuhriyanto, Anton Yudhana, and Imam Riadi, 2020. "Comparative analysis of Forensic Tools on Twitter applications using the DFRWS method," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 4, no. 5, pp. 829–836, doi: 10.29207/resti.v4i5.2152.

[11] R. Umar, I. Riadi, and G. M. Zamroni, 2018. "Mobile Forensic Tools Evaluation for Digital Crime Investigation," no. June, doi: 10.18517/ijaseit.8.3.3591.

[12] I. Riadi, S. Sunardi, and S. Sahiruddin, 2019. "Analisis Forensik Recovery pada Smartphone Android Menggunakan Metode National Institute Of Justice (NIJ)," *J. Rekayasa Teknol. Inf.*, vol. 3, no. 1, pp. 87–95.

[13] D. T. Yuwono and Y. W, 2020. "Analisis Perbandingan File Carving Dengan Metode Nist," *J. Sains Komput. dan Teknol. Inf.*, vol. 2, no. 2, pp. 1–6, doi: 10.33084/jsakti.v2i2.1472.

[14] Bounga, 2021."Magnet Axiom". Tersedia [https://bounga.id/products/magnet-axiom] diakses 14 Februari 2021.

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