JISKA (Jurnal Informatika Sunan Kalijaga)
Vol. 7, No. 2, MEI, 2022, Pp. 134 – 142
ISSN: 2527 – 5836 (print) | 2528 – 0074 (online)

Perbandingan *Forensic Tools* pada Instagram Menggunakan Metode NIST

Irhash Ainur Rafiq [(1)*], Imam Riadi [(2)], Herman [(3)]
[1,3] Informatika, Fakultas Teknologi Industri, Universitas Ahmad Dahlan, Yogyakarta
[2] Sistem Informasi, Fakultas Sains dan Teknologi Terapan, Universitas Ahmad Dahlan, Yogyakarta
e-mail : irhash67@gmail.com, imam.riadi@is.ud.ac.id, hermankaha@mti.uad.ac.id.
* Penulis korespondensi.
Artikel ini diajukan 15 Februari 2022, direvisi 6 April 2022, diterima 7 April 2022, dan dipublikasikan 25 Mei 2022.

Abstract

The development of communication media continues to increase with the emergence of various communication applications on smartphones, which are currently very developed from limited communication media to social media. This change in the flow of communication applications gives a new color to communication, not just exchanging messages and sounds but also exchanging videos and pictures. This development was also followed by the rise of digital crimes in the form of defamation, fraud, and hoax news by spreading posts and then deleting them after the news spread widely. This research was conducted to obtain digital evidence with the help of special applications such as Belkasoft Evidence and Axiom Magnets using the NIST method. The results of this study show that the Magnet Axiom is better with an accuracy rate of 83.3% while Belkasoft Evidence is only 50%.

Keywords: Android, Forensics, Digital Evidence, Instagram, Cybercrime, NIST

Abstrak

Perkembangan media komunikasi terus meningkat dengan banyaknya muncul berbagai aplikasi komunikasi pada *smartphone*, yang saat ini sudah sangat berkembang dari sebatas media komunikasi menjadi media sosial. Perubahan arus aplikasi komunikasi ini memberikan warna baru dalam berkomunikasi bukan hanya sekedar bertukar pesan dan suara tetapi juga bisa bertukar video dan gambar. Perkembangan ini juga diikuti dengan maraknya tindak kejahatan digital yang berupa pencemaran nama baik, penipuan dan berita *hoax* dengan menyebarkan postingan-postingan kemudian menghapusnya setelah berita tersebut tersebar luas. Penelitian ini dilakukan untuk mendapatkan bukti digital dengan bantuan aplikasi khusus seperti Belkasoft Evidence dan Magnet Axiom menggunakan metode NIST. Hasil Penelitian ini menunjukan Magnet Axiom lebih baik dengan tingkat akurasi 83.3% sementara Belkasoft Evidence hanya 50%.

Kata Kunci: Android, Forensik, Bukti Digital, Instagram, Kejahatan Digital, NIST

1. PENDAHULUAN

Teknologi *smartphone* semakin populer pertahunnya. Salah satu teknologi dengan jumlah pengguna yang terbanyak adalah *smartphone* berbasis Android sebagai sistem operasinya (Anwar & Riadi, 2017). Dengan kemajuan teknologi *smartphone* akan mempengaruhi fungsi utamanya sebagai alat komunikasi, Madiyanto et al., (2017) menyatakan *smartphone* dapat digunakan sebagai asisten pribadi, karena dapat menyimpan berbagai macam dokumen maupun data pribadi. *Smartphone* kini sudah sudah masuk ke semua golongan masyarakat sehingga prilaku kehidupan sehari-hari di masyarakat ikut berubah (Nasirudin et al., 2020b). Makin berkembangnya *smartphone* kini secara perlahan mulai menggantikan peran komputer dengan meningkatkan jumlah fitur dan aplikasi yang tersedia pada perangkat seluler (Imam Riadi, Sunardi, 2020). Peningkatan teknologi informasi saat ini tanpa disadari juga memberikan fasilitas oknum tertentu untuk melakukan kejahatan di dunia maya (Satrya & Nasrullah, 2020).

JISKA (Jurnal Informatika Sunan Kalijaga)
Vol. 7, No. 2, MEI, 2022: 134 – 142

Smartphone saat ini memiliki dua sistem operasi yang sangat populer yaitu Android dan iOS. Android pertama kali rilis pada tahun 2007 dengan versi sistem android A (Astro) dan terus berkembang hingga sekarang versi O (Oreo) uniknya pada sistem operasi Android ini menggunakan inisial pada tiap versinya menggunakan nama-nama makanan, di setiap *update*-nya sistem operasi Android mengalami banyak perkembangan, secara visual, konseptual, ataupun dari segi fungsional (Raphael, 2017). Beberapa sistem operasi *Android* yang telah rilis dijelaskan pada Tabel 1 (Krajci & Cummings, 2013).

Tabel 1 Perkembangan Versi Sistem Operasi Android

No	Versi Sistem Operasi	Tahun Rilis
1	Astro (1.0)	2007
2	Cupcake (1.5)	2009
3	Donut (1.6)	2009
4	Éclair (2.0)	2009
5	Froyo (2.2)	2010
6	Gingerbread (2.3)	2010
7	Honeycomb (3.0)	2011
8	Ice Cream Sandwich (4.0)	2011
9	Jelly Bean (4.1)	2012
10	KitKat (4.4)	2013
11	Lollipop (5.0)	2014
12	Marshmallow (6.0)	2015
13	Nougat (7.0)	2016
14	Oreo (8.0)	2017

Instant Messaging (IM) merupakan salah satu aplikasi seluler yang sangat populer. Salah satu jenis aplikasi IM adalah *WhatsApp* (WA) (Anwar & Riadi, 2017). *Instant messaging* (IM) merupakan suatu aplikasi obrolan *online* yang menawarkan pesan teks secara *real-time* serta transmisi *file* audio, video, dan gambar melalui internet (Riadi et al., 2019). Instagram merupakan aplikasi sosial paling populer di Indonesia dikalangan pengguna *smartphone*. Instagram merupakan gambaran dari kata *Instant-Telegram* yang berarti aplikasi ini dapat bertukar informasi dengan cepat baik dalam bentuk gambar, video, suara, dan pesan teks ke jejaring 135ocial lainnya. Instagram *messenger* atau lebih akrab dengan istilah *direct messenger* (DM) merupakan fitur yang dapat digunakan untuk saling betukar pesan, gambar, dan video ke pengguna lainnya. Hal ini berpotensi terjadinya praktik kejahatan digital seperti prostitusi *online* dengan cara menawarkan diri menggunakan gambar dan kata-kata yang tidak senonoh ke pengguna Instagram lainnya. Sedangkan untuk halaman beranda atau *feed* dan juga status atau *story* dapat disalahgunakan menjadi media penyebaran berita *hoax* dan pencemaran nama baik dengan meng-*upload* foto atau video yang dapat langsung dilihat oleh semua pengguna Instagram. Segala informasi yang pernah di-*upload* pada sosial media dapat digunakan menjadi bahan penyelidikan oleh penyidik dalam suatu tindak pidana (Alisabeth & Restu Pramadi, 2020). Platform sosial media saat ini sangat mudah diakses dan pembuatan akun baru, sehingga menjadi lahan bagi para oknum pelaku tindak kejahatan digital beraksi (Nieborg & Helmond, 2019).

Penegak hukum saat ini sudah tidak kesulitan dalam menangani tindakan kriminal digital ini, karena saat ini sudah banyak ilmu foreksik digital yang diterapkan begitu pula aplikasi pendukungnya. Forensik digital telah mengalami pertumbuhan cukup cepat dan telah diterapkan ke dalam komputer, *database*, jaringan, internal memori, dan forensik bergerak. Forensik bergerak adalah cabang forensik digital yang berkembang pesat dan memiliki banyak sub-cabang sesuai dengan vendor perangkat seluler yang ada (Satrya & Nasrullah, 2020). *Digital forensic* dapat dimanfaatkan pada beberapa kondisi, terutama dalam investigasi tindak pidana digital atau *cybercrime* (Horsman, 2020).

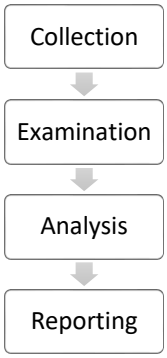
Forensik digital berkaitan dengan pemulihan bukti atau data digital dari perangkat seluler dengan kondisi *forensically sound* (Wirara et al., 2020)). Dalam UU ITE nomor 11 tahun 2008 pada pasal

5 ayat (1) menyatakan bukti digital dapat digunakan sebagai alat bukti hukum yang sah untuk membantu dalam proses hukum (Wirara et al., 2020). *Mobile forensic* menjadi proses yang wajib dilakukan saat menangani tindak kejahatan digital, karena dengan *mobile forensic* dapat menemukan bukti digital apapun yang sudah dihapus pada perangkat *mobile* (Madiyanto et al., 2017). Analisis pada *digital forensic* akan memberikan rincian yang detail sehingga membantu penyidik dalam memecahkan kasus kejahatan yang dilaporkan (Mehrotra & Mehtre, 2013).

Penelitian ini merupakan lanjutan dari beberapa penelitian sebelumnya seperti penelitian dari Nasirudin dengan judul "Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express". Penelitian ini melakukan pengembalian data dari beberapa aplikasi yang sudah dihapus pada *smartphone* Samsung Galaxy A8 menggunakan MOBILedit Forensic Express (Nasirudin et al., 2020a). Sedangkan penelitian ini menggunakan aplikasi Instagram dengan bantuan *tools* yang berbeda yaitu Belkasoft Evidence dan Magnet Axiom. Pada penelitian ini investigasi dilakukan dengan mengembalikan bukti digital yang sudah dihapus berupa (gambar, video, dan pesan teks) yang sebelumnya sempat di-*upload* pada aplikasi Instagram dari perangkat *smartphone* Android.

2. METODE PENELITIAN

Objek penelitian pada kasus ini yaitu Samsung Galaxy J2 Prime. Pada penelitian ini menggunakan metode *National Institute of Standards and Technology* (NIST), NIST sendiri merupakan sebuah lembaga yang bertanggung jawab akan standar pengembangan dan keamanan terhadap pihak yang berwewenang dalam *digital forensic* (Rahmansyah, 2021). Dalam proses analisis forensik untuk mendapatkan bukti digital. Tahapan metode NIST yaitu *collection, examination, analysis, dan reporting* seperti pada Gambar 1.



Gambar 1 Tahap Metode NIST

1) *Collection*
Collection merupakan tahap awal pada metode NIST, pada tahap *collection* dilakukan tindakan koleksi, dokumentasi, isolasi, dan preservasi barang bukti.

2) *Examination*
Examination merupakan tahap kedua dengan tindakan yang dilakukan di antaranya *backup data* dan *imaging system* yang mendukung format *image* dan dapat digunakan dengan *tools* berformat *image*.

3) *Analysis*
Analysis merupakan tahap di mana hasil *examination* dikumpulkan dan diperiksa dengan metode yang dibenarkan secara hukum untuk mendapatkan informasi yang berguna.
4) *Reporting*
Reporting adalah tahap terakhir yang dilakukan guna memberikan laporan detail dari setiap tahap forensik yang sudah dilakukan untuk memberikan rekomendasi perbaikan kebijakan, prosedur, alat, dan aspek lain dalam *forensic.*

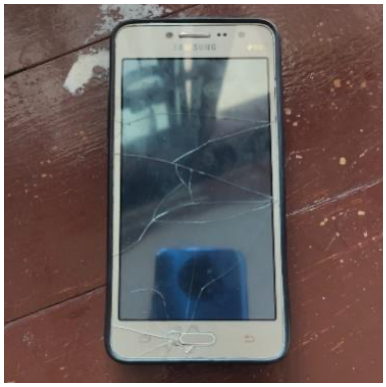
2.1 Skenario Kasus

Simulasi ini mengangkat kasus pencemaran nama baik di mana tersangka memposting sebuah gambar dan video pada halaman beranda dan story Instagram-nya yang menyinggung pihak lain secara sadar dan sengaja, setelah postingan tersebut dilihat dan tersebar kepada banyak views tersangka menghapus postingannya itu dengan keadaan postingannya sudah tersebar kemana-mana. Penelitian ini akan mengembalikan data postingan yang sudah dihapus tersebut pada *smartphone* tersangka menggunakan aplikasi Belkasoft Evidence dan Magnet Axiom.

3. HASIL DAN PEMBAHASAN

3.1 *Collection*

Tahap *Collection* yaitu tahap pengumpulan barang bukti dalam bentuk fisik yaitu barang digital berupa perangkat smartphone yang digunakan dalam penelitian. *Smartphone* yang menjadi barang bukti harus sangat diperhatikan dan dijaga karena bersifat rentan mengalami kerusakan yang mengakibatkan data di dalamnya yang akan menjadi barang bukti menjadi lenyap atau *corrupted,* sehingga data tidak dapat terbaca (Mahendra & Ari Mogi, 2021). Tahap *collection* sangat penting agar menjamin tidak ada perubahan dalam bentuk apapun pada barang bukti digital, karena dapat memberikan kesimpulan yang salah sehingga bukti dinyatakan tidak sah (Rochmadi, 2019) seperti pada Gambar 2.



Gambar 2 *Smartphone* yang Digunakan Sebagai Barang Bukti

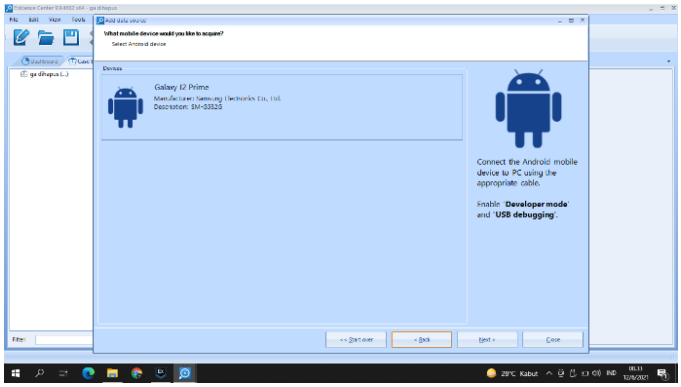
Proses ini selain mengumpulkan barang bukti dalam bentuk fisik juga mencatat spesifikasi dari barang bukti. Berikut adalah spesifikasi barang bukti yang digunakan pada Tabel 2.

Tabel 2 Spesifikasi Barang Bukti yang Digunakan

Spesifikasi	Barang Bukti
Tipe	Samsung Galaxy J2 Prime
Nomor Model	SM-G532G
Nomor Serial	-
OS (versi)	Android (Marshmallow)
Processor	Quad-core 1.4 GHz
RAM	1.5 GB
ROM	8 GB
Rooted	*UnRooted*

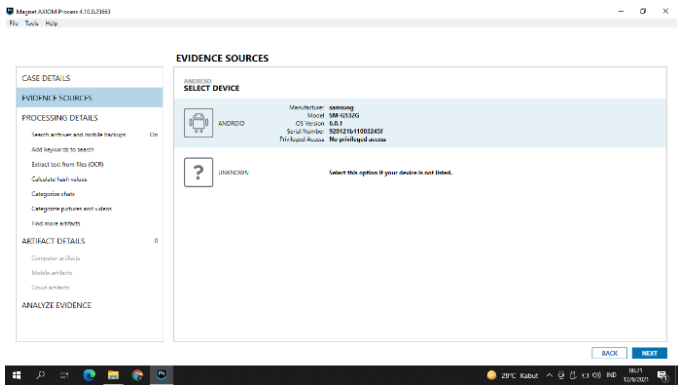
3.2 *Examination*

Setelah dicatat secara detail kondisi spesifikasi barang bukti akan diamankan dengan dimatikan layan data atau mode terbang, kemudian dilanjutkan pengamanan data menggunakan aplikasi Belkasoft Evidence dengan beberapa tahapan seperti pada Gambar 3.



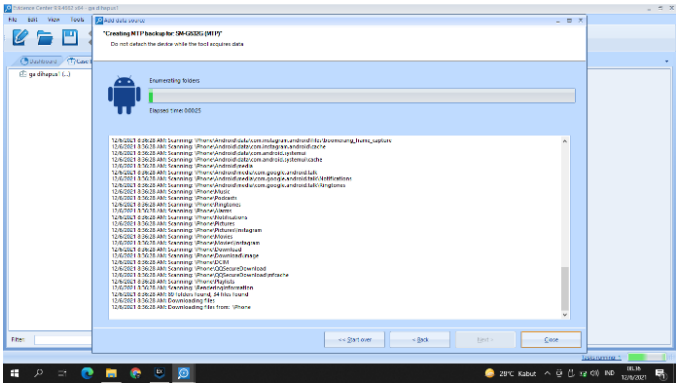
Gambar 3 Barang Bukti Tersambung dengan Aplikasi Belkasoft Evidence

Setelah barang bukti berhasil terhubung dengan aplikasi Belkasoft Evidence maka akan tampil informasi berupa merk, nomor model, versi sistem operasi, dan serial number dari barang bukti. Berbeda dengan Magnet Axiom saat *smartphone* terhubung maka informasi yang diberikan seperti pada Gambar 4.



Gambar 4 Barang Bukti Terhubung dengan Aplikasi Magnet Axiom

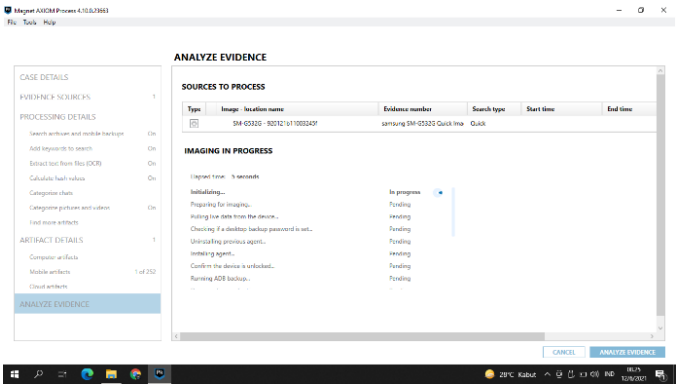
Setelah barang bukti dipastikan terhubung sempurna dengan aplikasi *forensic* maka bisa dilakukan tindakan *backup* seperti pada Gambar 4.



Gambar 5 Proses Backup dengan Aplikasi Belkasoft Evidence

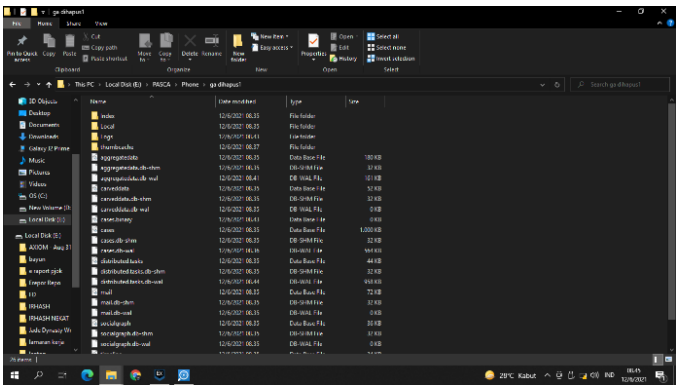
Proses *backup* pada aplikasi Belkasoft Evidence memakan pada barang buti ini memakan waktu 3 menit 9 detik. Sedangkan proses *backup* pada aplikasi Magnet axiom seperti pada Gambar 6.

JISKA (Jurnal Informatika Sunan Kalijaga)
Vol. 7, No. 2, MEI, 2022: 134 – 142



Gambar 6 Proses *Backup* dengan Aplikasi Magnet Axiom

Proses *backup* pada aplikasi Magnet Axiom juga tidak memakan lebih singkat dari aplikasi Belkasoft Evidence hanya 19 detik. Setelah proses *backup* selesai maka akan didapatkan beberapa *file* yang sudah terfilter kedalam beberapa folder seperti pada Gambar 7.



Gambar 7 Hasil yang Didapat dari Proses *Backup*

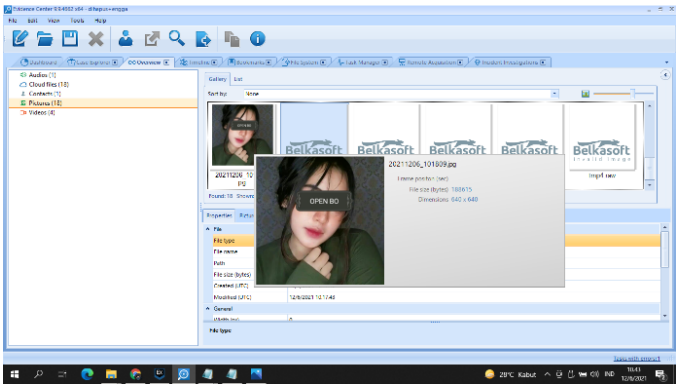
Setelah *file backup* didapatkan seperti Gambar 7 maka dapat dilanjutkan keproses berikutnya yaitu *analysis.*

3.3 *Analysis*

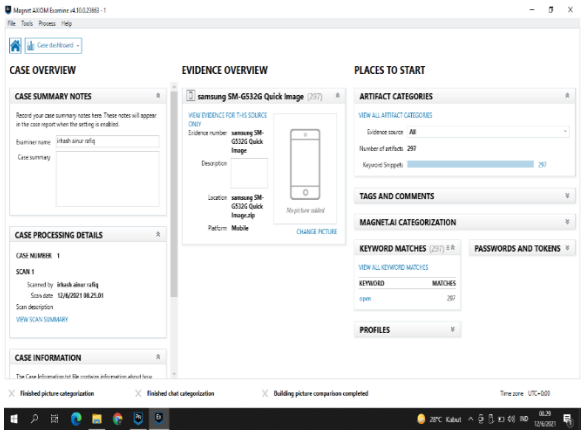
Pada tahap *analysis* setelah barang bukti terhubung keaplikasi akan dilakukan *recovery data* yang sudah dihapus dari barang bukti dan akan menjadi pendukung dalam penyelesaian kasus kejahatan digital. Proses *analysis* dilakukan dengan cara manual yaitu mengamati setiap data yang ditemukan pada saat *backup* dan *recovery* untuk menemukan bukti-bukti digital yang diinginkan seperti pada Gambar 8.

Dari hasil *analysis* hasil ekstraksi dari aplikasi Belkasoft Evidence berhasil ditemukan barang bukti yang berupa gambar dan video yang berasal dari halaman beranda Instagram dan juga *direct message* yang sudah dihapus maupun yang belum, sayangnya tidak didapatkan artefak dari sisi *story* dan *text* pada *direct message*-nya. Sedangkan hasil *analysis* dari aplikasi Magnet Axiom seperti pada Gambar 9.

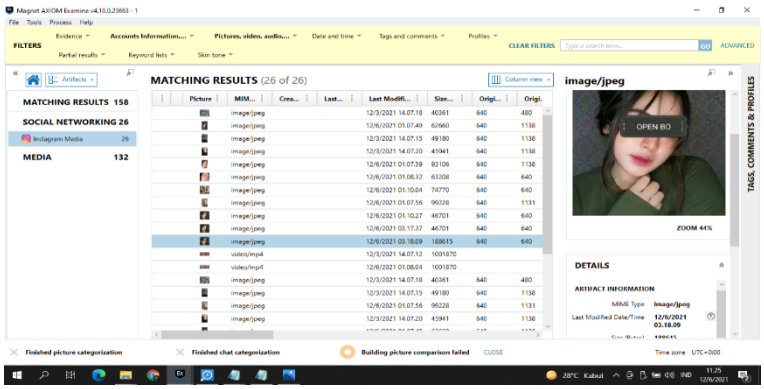
Hasil *analysis* dari aplikasi Magnet Axiom menemukan 297 artefak dari beberapa kategori, untuk bukti yang ditemukan hampir sama dengan apa yang ditemukan pada aplikasi Belkasoft Evidence yaitu bukti dalam bentuk video dan gambar yang berasal dari postingan di *feed* dan *direct message* seperti pada Gambar 10.



Gambar 8 Proses *Analysis* Hasil *Backup* dan *Recovery* pada Aplikasi Belkasoft Evidence



Gambar 9 Proses *Analysis* Hasil *Backup* dan *Recovery* pada Aplikasi Magnet Axiom



Gambar 10 Barang Bukti yang Ditemukan dengan Aplikasi Magnet Axiom

3.4 *Reporting*

Setelah dianalisis dari barang bukti yang ditemukan dari skenario kasus ini yang menggunakan *smartphone* Samsung Galaxy J2 Prime dalam keadaan belum di-*root* dapat disimpulkan penerapan forensik masih bisa mendapatkan beberapa bukti digital berupa gambar dan video yang digunakan sebagai media penipuan dan pencemaran nama baik.

Hasil analisis menggunakan aplikasi Belkasoft Evidence dan Magnet Axiom pada aplikasi Instagram ditemukan beberapa perbedaan fitur dan kemampuan dari kedua aplikasi tersebut. Perbandingan tingkat keberhasilan aplikasi Belkasoft Evidence dan Magnet Axiom dalam menemukan bukti digital seperti pada Tabel 3.

Tabel 3 Hasil Variabel

No	Informasi	Belkasoft Evidence	Magnet Axiom
1	Versi Aplikasi	304.2.0.17.118	304.2.0.17.118
2	Akun	Tidak Ditemukan	Ditemukan
3	Email	Tidak Ditemukan	Ditemukan
	Direct Message		
4	Image	Ditemukan	Ditemukan
5	Video	Ditemukan	Ditemukan
6	Text	Tidak Ditemukan	Tidak Dtiemukan
	Feed		
7	Image	DItemukan	Ditemukan
8	Video	Ditemukan	Ditemukan
	Story		
9	Video	Tidak Ditemukan	Tidak Ditemukan
10	Waktu Kejadian	Tidak Ditemukan	Ditemukan
11	URL	Ditemukan	Ditemukan
12	IP Address	Tidak Ditemukan	Ditemukan
Keberhasilan (%)		**50**	**83.3**

Perbandingan hasil kinerja *tools* pada *smartphone* Samsung Galaxy J2 Prime dalam keadaan belum *root* menggunakan kedua aplikasi forensik memiliki hasil kinerja berikut dalam mengembalikan data Belkasoft Evidence 50%, Magnet Axiom 83.3%. Hasil ini didapat dari perhitungan perbandingan angka indeks tertimbang dengan rumus pada Pers. (1).

$$\frac{x}{y} * 100(persen) = n \qquad (1)$$

Di mana x merupakan jumlah bukti ditigal yang berhasil ditemukan oleh aplikasi *forensic*, y adalah jumlah keseluruhan bukti digital yang harus ditemukan, dan n menunjukkan nilai persentase bukti digital yang ditemukan dari keseluruhan bukti digital yang dicari.

Perhitungan kinerja Belkasoft Evidence*,* hasil kinerja = $\frac{6}{12} * 100 = 50\%$

Perhitungan kinerja Magnet Axiom*,* hasil kinerja = $\frac{10}{12} * 100 = 83.3\%$

4. KESIMPULAN

Berdasarkan dari hasil akuisisi artefak yang sudah hilang menggunakan aplikasi forensik Belkasoft Evidence dan Magnet Axiom*,* menunjukan pada penggunaan di *smartphone* Android aplikasi Magnet Axiom performanya lebih optimal dari yang lain karena hasil kinerjanya memiliki nilai 83.3%. Untuk pengembangan penelitian berikutnya dapat digunakan metode baru dan juga mengkondisikan *smartphone* dalam keadaan sudah di-*root* untuk mendapatkan hasil yang lebih baik lagi.

DAFTAR PUSTAKA

Alisabeth, C., & Restu Pramadi, Y. (2020). Forensic Analysis of Instagram on Android. *IOP Conference Series: Materials Science and Engineering*, *1007*(1), 012116. https://doi.org/10.1088/1757-899X/1007/1/012116

Anwar, N., & Riadi, I. (2017). Analisis Investigasi Forensik WhatsApp Messanger Smartphone Terhadap WhatsApp Berbasis Web. *Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, *3*(1), 1. https://doi.org/10.26555/jiteki.v3i1.6643

Horsman, G. (2020). ACPO principles for digital evidence: Time for an update? *Forensic Science International: Reports*, *2*(January), 100076. https://doi.org/10.1016/j.fsir.2020.100076

Imam Riadi, Sunardi, S. (2020). Perbandingan Tool Forensik Data Recovery Berbasis Android

Menggunakan Metode NIST. *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK)*, *7*(1), 197–204. https://doi.org/10.25126/jtiik.202071921

Krajci, I., & Cummings, D. (2013). History and Evolution of the Android OS. In *Android on x86* (Issue November, pp. 1–8). Apress. https://doi.org/10.1007/978-1-4302-6131-5_1

Madiyanto, S., Mubarok, H., & Widiyasono, N. (2017). Proses Investigasi Mobile Forensics Pada Smartphone Berbasis IOS. *Jurnal Rekayasa Sistem & Industri (JRSI)*, *4*(1), 93–98. https://doi.org/10.25124/jrsi.v4i01.149

Mahendra, K. D. O., & Ari Mogi, I. K. (2021). Digital Forensic Analysis Of Michat Application On Android As Digital Proof In Handling Online Prostitution Cases. *JELIKU (Jurnal Elektronik Ilmu Komputer Udayana)*, *9*(3), 381. https://doi.org/10.24843/JLK.2021.v09.i03.p09

Mehrotra, T., & Mehtre, B. M. (2013). Forensic analysis of Wickr application on android devices. *2013 IEEE International Conference on Computational Intelligence and Computing Research*, *68*(8), 1–6. https://doi.org/10.1109/ICCIC.2013.6724230

Nasirudin, N., Sunardi, S., & Riadi, I. (2020a). Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express. *Jurnal Informatika Universitas Pamulang*, *5*(1), 89–94. https://doi.org/10.32493/informatika.v5i1.4578

Nasirudin, N., Sunardi, S., & Riadi, I. (2020b). Analisis Forensik Smartphone Android Menggunakan Metode NIST dan Tool MOBILedit Forensic Express. *Jurnal Informatika Universitas Pamulang*, *5*(1), 89. https://doi.org/10.32493/informatika.v5i1.4578

Nieborg, D. B., & Helmond, A. (2019). The political economy of Facebook's platformization in the mobile ecosystem: Facebook Messenger as a platform instance. *Media, Culture & Society*, *41*(2), 196–218. https://doi.org/10.1177/0163443718818384

Rahmansyah, R. (2021). Perbandingan Hasil Investigasi Barang Bukti Digital pada Aplikasi Facebook dan Instagram dengan Metode NIST. *Cyber Security Dan Forensik Digital*, *4*(1), 49–57. https://doi.org/10.14421/csecurity.2021.4.1.2421

Raphael, J. (2017). *Android versions: A living history from 1.0 to today*. Computerworld. https://www.computerworld.com/article/3235946/android-versions-a-living-history-from-1-0-to-today.html

Riadi, I., Umar, R., & Aziz, M. A. (2019). Forensik Web Layanan Instant Messaging Menggunakan Metode Association of Chief Police Officers (ACPO). *Mobile and Forensics*, *1*(1), 30. https://doi.org/10.12928/mf.v1i1.705

Rochmadi, T. (2019). Deteksi Bukti Digital pada Adrive Cloud Storage Menggunakan Live Forensik. *Cyber Security Dan Forensik Digital*, *2*(2), 65–68. https://doi.org/10.14421/csecurity.2019.2.2.1455

Satrya, G. B., & Nasrullah, A. A. (2020). Analisis Forensik Android: Artefak pada Aplikasi Penyimpanan Awan Box. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *7*(3), 521. https://doi.org/10.25126/jtiik.2020732220

Wirara, A., Hardiawan, B., & Salman, M. (2020). Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan "WhatsApp." *Teknoin*, *26*(1), 66–74. https://doi.org/10.20885/teknoin.vol26.iss1.art7