Jurnal Infosecure Vol.4 No.2, Oktober 2023
p-ISSN: 2087-1023
MTI-UNLA

Perbandingan Tools Mobile Forensic Pada Simulasi Kasus Cyber Sexual Harassment Berdasarkan Metode National Institute Of Standards And Technology

Dikky Taopik Purwa Irawan[1], Aisyah Nuraeni[2], Hadi Prasetyo Utomo[3]

Program Studi Informatika, Fakultas Teknik, Universitas Langlangbuana[1,2,3]

[1]dikkytaopik.pi@gmail.com

[2]aisyahnuraeni20@gmail.com

[3]hadi@informatika.unla.ac.id

Abstrak— Penelitian ini bertujuan untuk membandingkan dua alat forensik, yaitu Magnet Axiom dan MobilEdit Forensic Express dalam konteks penanganan kasus cyber sexual harassment. Metode penelitian eksperimental dengan tahapan forensik dari National Institute Of Standards And Technology (NIST) digunakan untuk mengukur kemampuan keduanya dalam mengidentifikasi artifak terkait kasus tersebut. Hasil penelitian menunjukan bahwa kedua alat forensik ini mampu menemukan berbagai artifak yang relevan, walaupun dengan beberapa perbedaan. Magnet Axiom tidak dapat memulihkan pesan yang dihapus oleh terduga pelaku, namun tetap mampu menemukan artifak lain seperti informasi akun telegram dan kontak korban. Di sisi lain, MobilEdit Forensic Express mampu mengambil pesan yang dihapus, meskipun memerlukan aplikasi pihak ketiga untuk membaca isi database pesan yang dihapus. Dalam analisis perbandingan, MobilEdit Forensic Express meraih index score yang lebih tinggi dibandingkan Magnet Axiom. Kesimpulannya, MobilEdit Forensic Express lebih efektif dalam menangani kasus cyber sexual harassment berdasarkan index score yang diperoleh.

Kata kunci— Alat, forensik, artifak, cyber sexual harassment, eksperimental, perbandingan, NIST.

I. PENDAHULUAN

Dalam era digital saat ini, penggunaan alat-alat forensik digital memiliki peran yang sangat penting dalam meningkatkan hasil dari proses investigasi. Pentingnya menggunakan berbagai alat forensik digital, bukan hanya terbatas pada satu alat, menjadi kunci untuk memaksimalkan ekstraksi data dari perangkat smartphone. Kombinasi dan pengujian berbagai alat forensik yang berbeda dapat memberikan hasil yang optimal dalam mengumpulkan informasi dari perangkat [1].

Forensik digital merupakan penerapan ilmu dan teknik untuk mengindentifikasi, menemukan, menghimpun, mengamankan, menganalisis, mengartikan, dan menyajikan barang bukti digital terkait dengan suatu peristiwa yang terjadi untuk membangun kembali kronologi peristiwa serta menegaskan integritas proses hukum [2]. Mobile Forensic merupakan bagian dari digital forensik yang tengah menarik perhatian, terutama karena mayoritas masyarakat kini memiliki smartphone yang digunakan untuk keperluan bisnis maupun pribadi [3].

Beberapa penelitian sebelumnya telah mencoba membandingkan efektivitas berbagai alat forensik digital dalam mengidentifikasi dan mengambil bukti digital dari perangkat mobile. Sebagai contoh, penelitian dalam [4] menggambarkan penggunaan alat forensik seperti Oxygen Forensic Detective dan Belkasoft Evidence Center dalam mengidentifikasi bukti digital dalam kasus tertentu. Hasilnya menunjukkan tingkat akurasi yang berbeda antara kedua alat tersebut. Sementara dalam [5] juga melakukan penelitian serupa dengan hasil yang mengindikasikan perbedaan dalam kemampuan MOBILedit Forensic Express dan Belkasoft Evidence Center dalam mengambil variabel yang relevan.

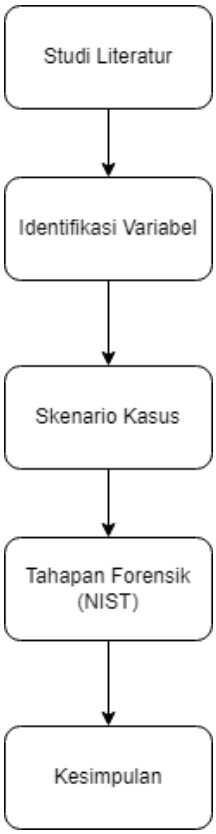
Pentingnya peran forensik digital semakin diperkuat oleh meningkatnya penggunaan perangkat seluler, terutama smartphone, di Indonesia. Data menunjukkan peningkatan signifikan dalam jumlah pengguna smartphone, yang mencapai 370,1 juta pada tahun 2022 [6]. Namun, pertumbuhan ini juga berdampak pada peningkatan kejahatan siber termasuk cyber sexual harassment, seperti yang terjadi pada tahun 2018 kepada penyanyi dangdut terkenal yaitu via vallen yang menerima pesan mesum dari bintang sepakbola melalui instagram [7]. Banyak juga individu yang terlibat dalam aktivitas kriminal menggunakan smartphone berbasis Android, dengan sengaja menghapus berkas-berkas atau informasi-informasi yang terkait dengan kejahatan yang dilakukan. Tujuannya adalah untuk menghilangkan jejak digital yang dapat digunakan sebagai bukti, dengan maksud menghindari konsekuensi hukum yang lebih serius akibat bukti digital tersebut [8].

Dalam konteks ini, forensik digital menjadi kunci dalam mengungkap dan mendalami peristiwa tertentu, terutama dalam kasus cyber crime. Bukti digital yang diambil dari perangkat komunikasi digital dan komputer dapat digunakan untuk mengumpulkan alat bukti kasus kejahatan terutama dalam membantu penegakan hukum pada tindak kejahatan di dunia komputer (*cyber crime*) [9]. Oleh karena itu, penelitian ini memiliki relevansi yang tinggi dalam mendukung upaya penegakan hukum dan penanganan kasus-kasus kejahatan

digital. Selain itu, metode dan pedoman yang dikeluarkan oleh National Institute of Standards and Technology (NIST) juga menjadi landasan penting dalam melakukan forensik digital yang akurat dalam penelitian ini, serta memastikan bahwa bukti digital yang ditemukan dapat diterima secara hukum dalam proses peradilan.

II. METODE

Metode penelitian yang digunakan dalam penelitian ini adalah eksperimental dan metode forensik menggunakan NIST (*National Institute Of Standards And Tecnology*). Dengan tahapan penelitian sebagaimana terlihat pada Gambar. 1 dibawah.



Gambar. 1 Tahapan Penelitian

Rincian mengenai tahapan penelitian diatas akan dijelaskan sebagai berikut:

1. Studi Literatur
   Tahap ini dilakukan untuk membaca dan mempelajari referensi-referensi yang terkait dengan permasalahan. Referensi-referensi yang diambil berasal dari jurnal, buku, maupun internet.
2. Identifikasi Variabel
   Menentukan variabel yang akan digunakan untuk mengetahui *index score* dari masing masing *tool*.
3. Skenario Kasus
   Pada tahap ini dibuat skenario kasus *cyber sexual harassment.*
4. Tahapan Forensik

   Tahapan forensik yang dilakukan dalam penelitian ini, menggunakan metode National Institute Of Standards Technology (NIST) menurut [10] ada 4 tahapan yang harus dilakukan yaitu sebagai berikut:

   1. Collection
      Proses ini dilakukan untuk proses identifikasi dan pengumpulan data yang terkait dengan kasus, setelah itu dilakukan proses *rooting* pada *smartphone*, lalu dilakukan isolasi data dengan menyalakan mode pesawat pada *smartphone* terduga pelaku.
   2. Examination
      Proses examination dilakukan untuk pemrosesan dan pembacaan data yang dikumpulkan secara forensik terhadap *smartphone* xiaomi redmi 5a, yang merupakan *smartphone* milik terduga pelaku dengan tetap menjaga keaslian data.
   3. Analisys
      Analysis dilaksanakan guna memeriksa hasil dari proses *examination* dengan memilah *artifact-artifact* yang relevan dengan kasus *cyber sexual harassment* dan terhadap variabel.
   4. Reporting
      Tahap ini dilakukan setelah mendapatkan hasil analisis dari artifak digital yang telah diperoleh dari hasil *examination*. Selanjutnya pada tahap ini dilakukan pelaporan dengan memberikan *index score* pada variabel yang terbaca oleh masing masing *tools* lalu memasukkan rumus metode perbandingan untuk mengetahui seberapa efektif *tools* untuk membaca data dari smartphone milik terduga pelaku.

5. Membuat Kesimpulan
   Pada tahap ini dibuatkan kesimpulan tentang hasil pembacaan data dari kedua *tool* terhadap variabel yang telah ditentukan lalu menarik kesimpulan dari *index score* yang didapatkan pada masing masing *tool* untuk mengatahui *tool* mana yang lebih efektif terhadap skenario kasus.

III. HASIL DAN PEMBAHASAN

A. Identifikasi Variabel

Untuk mencapai hasil yang optimal dibutuhkan beberapa variabel untuk mengukur akurasi dari ke 2 tool yang digunakan, variabel yang akan digunakan terlihat pada Tabel 1 berikut.

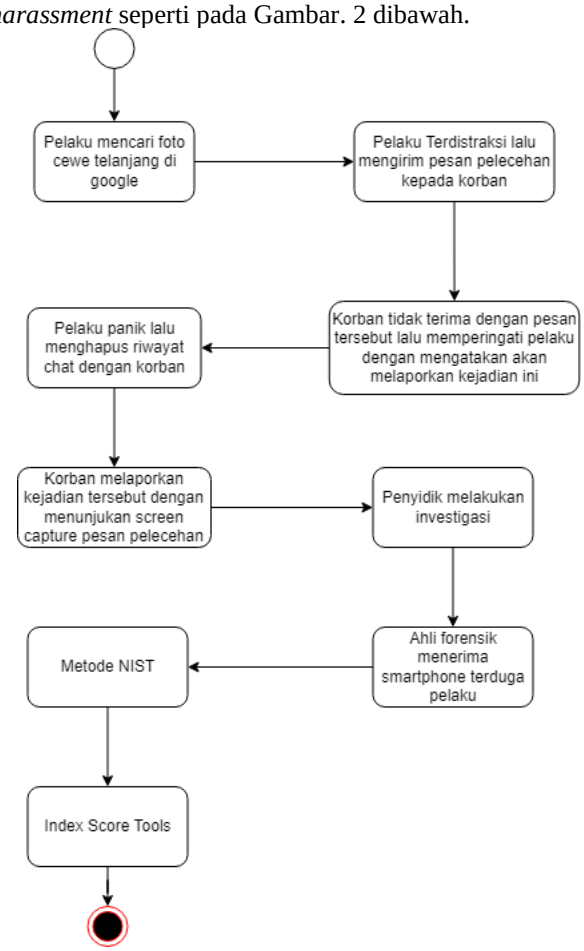
TABEL 1
Identifikasi Variabel

No	Variabel
1	Browser/Web related
2	Application Info
3	Call Logs
4	Contacts
5	Account Info
6	Installed Application
7	Mail
8	Pictures
9	Deleted Chat

10	Videos
11	Wifi Connection
12	IP Address
13	Delete Files
14	Location

B. Skenario Kasus

Pada tahap ini dibuat skenario kasus *cyber sexual harassment* seperti pada Gambar. 2 dibawah.



Gambar. 2 Skenario Kasus

C. Tahapan Forensik

1. Collection

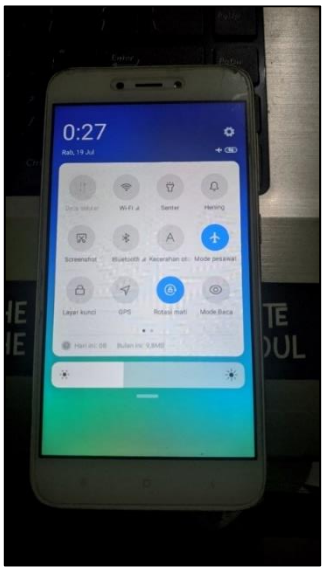
Tahap collection merupakan pengumpulan smartphone terduga pelaku yang menyangkut tindak pidana kejahatan untuk bisa diinvestigasi lebih lanjut. Proses pertama adalah pendokumentasian *smartphone* terduga pelaku seperti terlihat pada Gambar. 3 dibawah.

Gambar. 3 Smartphone Terduga Pelaku

Proses kedua adalah dengan melakukan *rooting* pada *smartphone* yang akan diektraksi datanya supaya *tools* mendapatkan hak akses penuh. Proses *root* menggunakan cara memasang *TWRP* terlebih dahulu supaya bisa menginstall *magisk* yang merupakan aplikasi *super user* di dalam *smartphone.* Terlihat pada Gambar. 4 merupakan hasil dari proses *rooting* yang sukses.

Gambar. 4 Proses *Root* Sukses

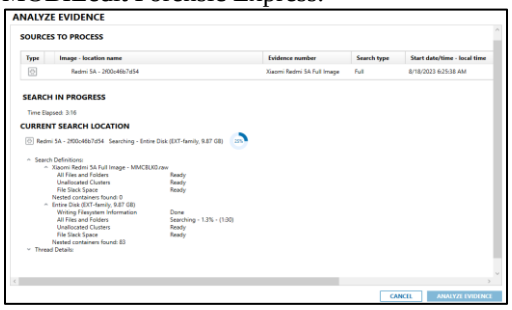
Lalu proses terakhir yaitu mengisolasi *smartphone* terduga pelaku dengan cara menyalakan mode pesawat, untuk menjaga integritas data supaya tidak berubah secara signifikan disaat melakukan ektraksi data oleh *tools.* Seperti terlihat pada Gambar. 5 berikut.



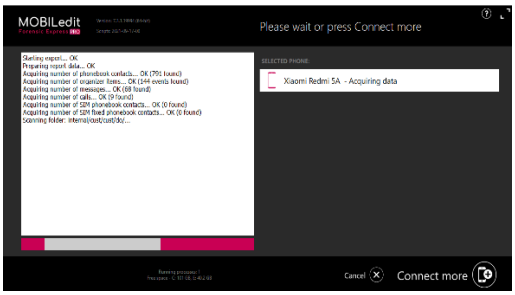
Gambar. 5 Isolasi *Smartphone* Terduga Pelaku

2. *Examination*

Tahap ini adalah proses dimana akuisisi data dilakukan oleh *tools* dari *smartphone* terduga pelaku. Seperti terlihat pada Gambar. 6 merupakan proses akuisisi dari Magnet Axiom sementara pada Gambar. 7 merupakan proses akuisisi dari MOBILedit Forensic Express.



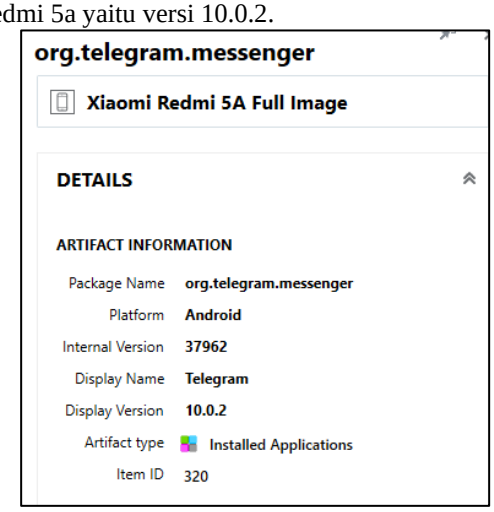
Gambar. 6 Akuisisi Magnet Axiom



Gambar. 7 Akuisisi MOBILedit Forensic Express

3. *Analysis*

Tahap ini adalah proses melihat dan memilah artifak yang terkait dengan kasus. Kedua *tool* dapat menemukan beberapa artifak yang terkait seperti info aplikasi telegram, info akun telegram, kontak telegram bernama cindy, dll. Pada MOBILedit Forensic Express dapat menemukan database pesan yang dihapus, sementara pada Magnet Axiom tidak ditemukan. Gambar. 8 menunjukan artifak info aplikasi pada tool Magnet Axiom terlihat versi telegram yang terinstall pada *smartphone* xiaomi redmi 5a yaitu versi 10.0.2.



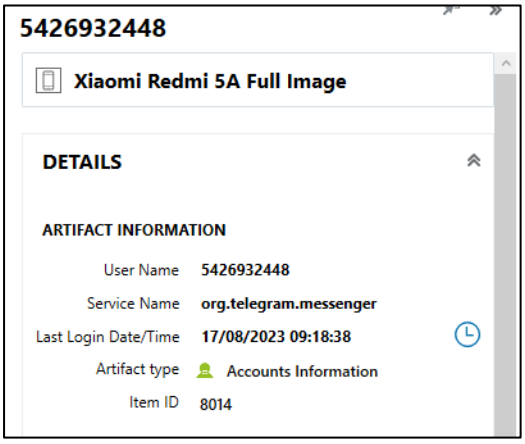
Gambar. 8 Info aplikasi Magnet Axiom

Sementara pada Gambar. 9 menunjukan artifak info aplikasi dari *tool* MOBILedit Forensic Express terlihat versi telegram yang terinstall yaitu versi 10.0.2 lalu terlihat *permission* apa saja yang diminta oleh telegram terhadap *smartphone* xiaomi redmi 5a.

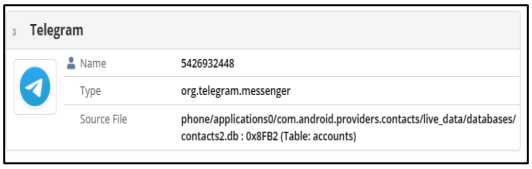
Gambar. 9 Info aplikasi MOBILedit Forensic Express

Lalu kedua *tool* dapat menemukan artifak info akun yang login di telegram pada *smartphone* terduga pelaku, tetapi kedua *tool* hanya dapat menemukan user

id telegram tetapi untuk *username* dan *display name* tidak dapat ditemukan. Seperti terlihat pada Gambar. 10 dibawah merupakan artifak info akun yang terbaca oleh Magnet Axiom. Sementara Gambar. 11 merupakan artifak akun info yang berhasil dibaca oleh MOBILedit Forensic Express. Pada hasil pembacaan kedua *tool* didapatkan user id dari akun telegram terduga pelaku adalah 5426932448.

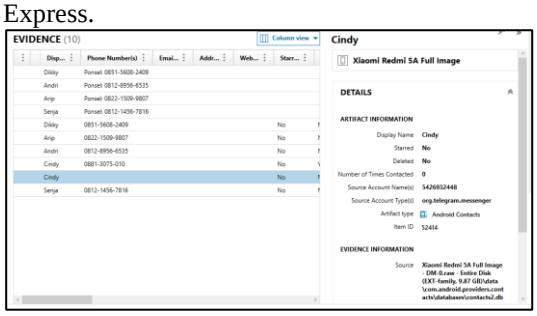


Gambar. 10 Akun info Magnet Axiom

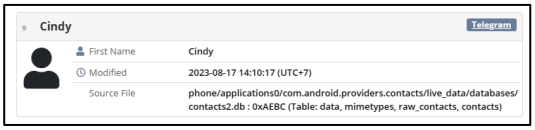


Gambar. 11 Akun info MOBILedit Forensic Express

Kedua *tool* dapat menemukan kontak bernama cindy yang terhubung ke telegram. Seperti terlihat pada Gambar. 12 merupakan artifak kontak dari Magnet Axiom terlihat kontak dengan nama cindy terhubung ke telegram dan berasal dari akun dengan user id 5426932448 sedangkan Gambar. 13 merupakan artifak kontak dari MOBILedit Forensic Express.

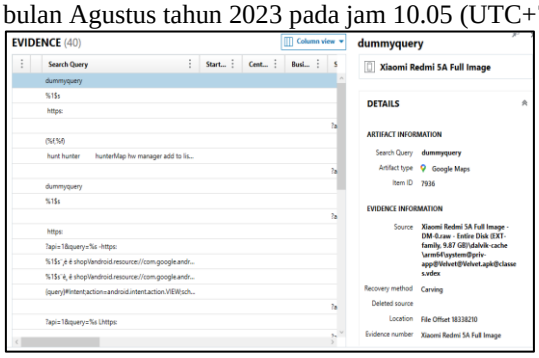


Gambar. 12 Kontak Magnet Axiom

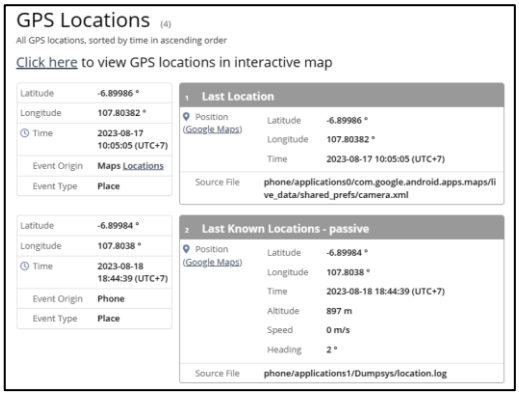


Gambar. 13 Kontak MOBILedit Forensic Express

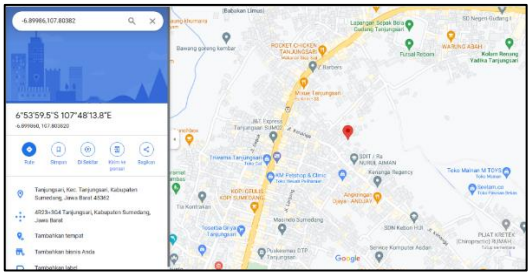
Untuk artifak lokasi, Magnet Axiom dapat menemukan lokasi tetapi metadatanya sulit dibaca dan tidak bisa langsung dibuka dan dilihat seperti terlihat pada Gambar. 14 sementara pada MOBILedit Forensic Express seperti terlihat pada Gambar. 15 lokasi dapat ditemukan serta metadata mudah dibawa serta dapat langsung melihat *pin* dimana posisi terakhir terduga pelaku berada dan posisi terakhir terduga pelaku terbaca berada adalah di Kecamatan Tanjungsari Kabupaten Sumedang pada tanggal 17 bulan Agustus tahun 2023 pada jam 10.05 (UTC+7).



Gambar. 14 Location Magnet Axiom



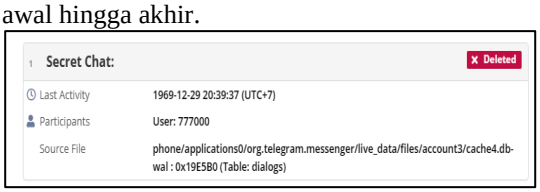
Gambar. 15 Location MOBILedit Forensic Express



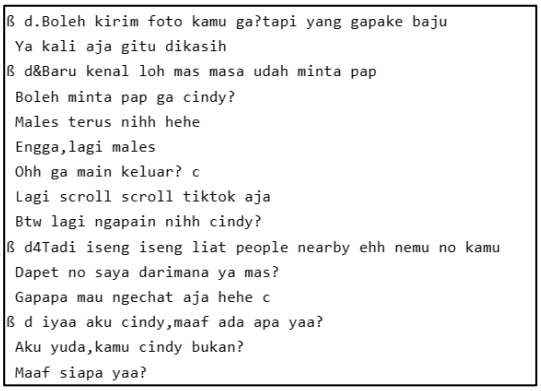
Gambar. 16 Location Pin MOBILedit Forensic Express

Artifak pesan yang dihapus pada Magnet Axiom tidak dapat ditemukan, sementara pada MOBILedit Forensic Express dapat ditemukan meskipun hanya database pesan yang dihapusnya saja yang ditemukan dan memerlukan aplikasi pihak ketiga untuk membuka dan membaca database tersebut. Untuk database pesan dihapus yang terbaca bisa dilihat pada Gambar. 17 dan untuk hasil pembacaan menggunakan

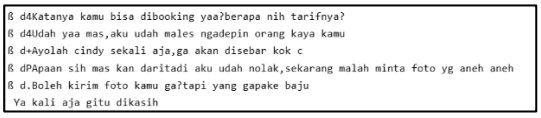
aplikasi filext.com terlihat pada Gambar. 18 dan Gambar. 19 dibawah meskipun unsur pesan pelecehannya dapat ditemukan tetapi karena urutan pesannya menjadi tidak beraturan sehingga menyebabkan sulit untuk merunut pesan tersebut dari awal hingga akhir.



Gambar. 17 Database pesan dihapus



Gambar. 18 Hasil Pembacaan Database 1



Gambar. 19 Hasil Pembacaan Database 2

4. Report

Dalam tahap report ini dapat dilihat hasil variabel yang terbaca oleh masing masing tools seperti pada Tabel 2 dibawah.

TABEL 2

Variabel yang terbaca

No	Varibel	Magnet Axiom	MobilEdit Forensic Express
1	Browser History	✓	✓
2	Application Info	✓	✓
3	Calls Log	✓	✓
4	Contacts	✓	✓
5	Account Info	✓	✓
6	Installed Application	✓	✓
7	Mail	✓	✓
8	Pictures	✓	✓
9	Chat Deleted	x	✓
10	Videos	✓	✓
11	Wifi Connection	✓	✓
12	IP Address	x	x
13	Deleted Files	x	✓
14	Location	✓	✓
Index Score		11	13

Keseluruhan hasil tersebut diperoleh berdasarkan pembacaan tools terhadap smartphone milik terduga pelaku yakni xiaomi redmi 5a, skenario dan variabel yang telah ditentukan pada tahap perencanaan.

Indeks akurasi untuk mengukur kemampuan masing masing *tools* terhadap *smartphone* dapat dihitung menggunakan rumus [3].

$$Pon = \frac{\sum Pn}{\sum Po} \times 100\%$$

"Pon" mencerminkan hasil persentase yang diharapkan, "ΣPn" menggambarkan jumlah variabel yang berhasil terdeteksi, dan "ΣPo" mewakili jumlah variabel yang digunakan dalam evaluasi.

Dengan menggunakan rumus yang telah disebutkan diatas, dapat dihitung index akurasi untuk menilai kemampuan masing masing tool forensik sebagai berikut.

Magnet Axiom:

$$Pon = \frac{\sum 11}{\sum 14} \times 100\% = 78.57\%$$

MobilEdit Forensic Express:

$$Pon = \frac{\sum 13}{\sum 14} \times 100\% = 92.86\%$$

Berdasarkan perhitungan indeks akurasi tool forensik dan teknik forensik dengan variabel yang digunakan maka masing masing tool mendapatkan hasil Magnet Axiom mendapatkan akurasi sebesar 78,57% dengan 11 variabel terbaca dari 14 variabel yang telah ditentukan sementara MobilEdit Forensic Express akurasi sebesar 92,86% dengan 13 variabel terbaca dari 14 variabel yang telah ditentukan.

IV. SIMPULAN

Magnet Axiom dan MobilEdit Forensic Express mampu menemukan artifak artifak yang terkait dengan kasus cyber sexual harassment. Meskipun Magnet Axiom tidak dapat membaca pesan pelecehan yang dihapus oleh terduga pelaku kepada korban tetapi dapat menemukan artifak lain terkait kasus cyber sexual harassment seperti info akun telegram, kontak korban, dll. Sementara pada tool MobilEdit Forensic Express mampu menemukan artifak pesan yang dihapus oleh terduga pelaku meskipun membutuhkan aplikasi pihak ketiga untuk membaca isi database pesan yang dihapus. Dengan

rumus dan variabel yang telah ditentukan didapat index akurasi dari masing masing *tool*. Untuk Magnet Axiom mendapatkan index akurasi lebih rendah sementara pada MOBILedit Forensic Express mendapatkan index akurasi lebih tinggi. Untuk itu dapat disimpulkan bahwa MOBILedit Forensic Express lebih efektif daripada Magnet Axiom terhadap variabel yang telah ditentukan karena mendapatkan index akurasi lebih tinggi.

REFERENSI

[1] Ahwan ahmadi, T. Akbar, and H. Mandala Putra, "Perbandingan Hasil Tool Forensik Pada file image smartphone android Menggunakan metode NIST," JIKO (Jurnal Informatika dan Komputer), vol. 4, no. 2, pp. 92–97, 2021. doi:10.33387/jiko.v4i2.2812.

[2] E. Army, Bukti Elektronik dalam Praktik Peradilan. Sinar Grafika, 2020.

[3] A. Heriyanto, "Procedures And Tools For Acquisition And Analysis Of Volatile Procedures And Tools For Acquisition And Analysis Of Volatile Memory On Android Smartphones Memory On Android Smartphones," A. P, 2013, doi: https://doi.org/10.4225/75/57b3c9bafb86f.

[4] Desti Mualfah, Muhammad Iqbal Syam, and Baidarus, "Analisis perbandingan tools mobile forensic menggunakan metode national institute of justice (NIJ)," Jurnal Computer Science and Information Technology, vol. 4, no. 1, pp. 283–292, May 2023, doi: https://doi.org/10.37859/coscitech.v4i1.4767.

[5] I. Zuhriyanto, A. Yudhana, and I. Riadi, "Analisis Perbandingan Tools Forensic pada Aplikasi Twitter Menggunakan Metode Digital Forensics Research Workshop," JURNAL RESTI (Rekayasa Sistem dan Teknologi Informasi), vol. Vol. 4 No. 5 (2020) 829 - 836, 2021.

[6] S. Kemp, "Mobile connections in Indonesia in 2022," https://datareportal.com/reports/digital-2022-indonesia#:~:text=Mobile%20connections%20in%20Indonesia%20in%202022&text=GSMA%20Intelligence's%20numbers%20indicate%20that,percent)%20between%202021%20and%202022, (accessed August. 20, 2023).

[7] T. Mulyono, "Via Vallen Akhirnya Buka-Bukaan soal Pesan Mesum dari Bintang Sepakbola, Ini Kronologi Lengkap," Surya.co.id, https://surabaya.tribunnews.com/2018/06/06/via-vallen-akhirnya-buka-bukaan-soal-pesan-mesum-dari-bintang-sepakbola-ini-kronologi-lengkap (accessed August. 15, 2023).

[8] I. Riadi, S. Sunardi, and S. Sahiruddin, "Analisis forensik recovery pada smartphone android Menggunakan metode national institute of justice (NIJ)," Jurnal Rekayasa Teknologi Informasi (JURTI), vol. 3, no. 1, p. 87, 2019. doi:10.30872/jurti.v3i1.2292

[9] S. Rachmie, "PERANAN ILMU DIGITAL FORENSIK TERHADAP PENYIDIKAN KASUS PERETASAN WEBSITE," Jurnal Litigasi, no. 21, pp. 104–127, Jul. 2020, doi: 10.23969/litigasi.v21i1.2388.

[10] Rusydi Umar, S. Sahiruddin, and S. Sahiruddin, "METODE NIST UNTUK ANALISIS FORENSIK BUKTI DIGITAL PADA PERANGKAT ANDROID", Proceeding SENDI_U, pp. 124-130, Jul. 2019.