IT Journal Research and Development (ITJRD)
Vol.5, No.2, Maret 2021, E-ISSN : 2528-4053 | P-ISSN: 2528-4061
DOI : 10.25299/itjrd.2021.vol5(2).4664

Analisis Barang Bukti Digital Aplikasi Facebook Messenger Pada Smartphone Android Menggunakan Metode NIJ

Ikhwan Anshori[1], Khairina Eka Setya Putri[2], Umar Ghoni[3]
Jurusan Sistem Informasi, STMIK Muhammadiyah Paguyangan Brebes[1,2]
Jurusan Teknik Informatika, STMIK Muhammadiyah Paguyangan Brebes[3]
ikhwananshori@stmikmpb.ac.id[1], khairinaeka@stmikmpb.ac.id[2], umarghoni@stmikmpb.ac.id[3]

Article Info

History :

Dikirim 20 Februari 2020
Direvisi 29 Juli 2020
Diterima 19 Agustus 2020

Kata Kunci:

Digital Forensik
Facebook Messenger
Mobile Forensik
Metode NIJ

Abstrak

Facebook Messenger menjadi media sosial yang popular di tahun 2019 dan meningkat sangat pesat perkembangannya dari tahun ke tahun. Meningkatnya jumlah pengguna tentu membawa dampak positif dan negatif. Dampak negatif banyak terdapat kasus kejahatan yang terjadi dan terbukti dipersidangan. Forensik digital dapat dilakukan pada *smartphone* yang digunakan para pelaku kejahatan. Pada penelitian ini tool yang kami gunakan adalah *Oxygen Forensic, MOBILedit Forensic Express,* dan *Magnet AXIOM.* Penelitian ini mengacu pada proses investigasi yang digunakan metode *National Institute Of Justice* (NIJ). Metode pada penelitian ini berdasarkan pedoman forensik perangkat mobile yang dibuat oleh *National Institute of Justice* (NIJ). Hasil yang didapatkan dari penelitian ini adalah MOBILedit Forensic Express mendapatkan bukti digital berupa 2 akun, 11 chat dan 26 gambar dengan persentase berupa 100% dalam mendapatkan akun, 55% dalam mendapatkan chat dan 86% dalam mendapatkan gambar. Dapat disimpulkan bahwa MOBILedit Forensic Express memiliki kinerja yang baik dalam mendapatkan bukti digital. Magnet AXIOM mendapatkan bukti digital berupa 2 akun, 11 chat dan 26 gambar dengan persentase berupa 100% dalam mendapatkan akun, 55% dalam mendapatkan chat dan 86% dalam mendapatkan gambar. Dapat disimpulkan bahwa Magnet AXIOM memiliki kinerja yang baik dalam mendapatkan bukti digital, Oxygen Forensic Suite 2014 mendapatkan bukti digital berupa 2 akun, 1 chat dan 26 gambar dengan persentase berupa 100% dalam mendapatkan akun, 5% dalam mendapatkan chat dan 86% dalam mendapatkan gambar. Dapat disimpulkan bahwa Oxygen Forensic Suite 2014 memiliki kinerja yang kurang baik dalam mendapatkan bukti digital pada Facebook Messenger.

Koresponden:

Ikhwan Anshori
Jurusan Sistem informasi
STMIK Muhammadiyah Paguyungan Brebes
Brebes, Jawa Tengah
Email : ikhwananshori@stmikmpb.ac.id

1. PENDAHULUAN

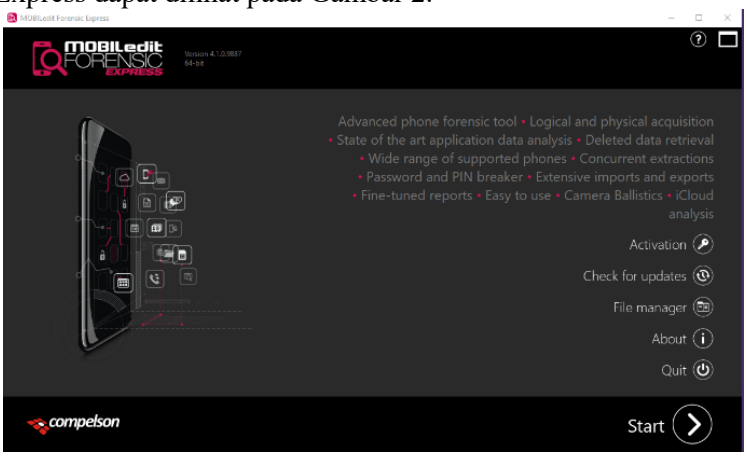
Media sosial adalah salah satu teknologi yang sangat pesat perkembangannya dan sangat populer dikalangan masyarakat khususnya di Indonesia. Salah satu aplikasi media sosial terpopuler adalah Facebook Messenger [1].

Kejahatan digital yang bisa dilakukan di Facebook Messenger sebagai media komunikasi untuk tujuan kriminal misalnya seperti perdagangan narkoba, kegiatan teroris, perencanaan pembunuhan, dan kegiatan kriminal lainnya. Kejahatan tersebut pasti akan meninggalkan barang bukti, barang bukti tersebut sebagai laporan tindak kejahatan di pengadilan. Penyelesaian kasus-kasus kejahatan digital pada aplikasi Facebook Messenger tentunya memerlukan bukti digital sebagai alat bantunya, bukti digital tersebut dapat berupa profil pemilik akun, chat, data kontak, gambar, *log report* aplikasi, video, voice chat dan *timestamp*. Pada Penelitian ini dilakukan skenario percakapan yang di indikasi mengarah ke criminal, proses akuisisi bukti digital pada penelitian ini dilakukan menggunakan alat bantu berupa perangkat lunak forensik Pada penelitian ini tool yang digunakan adalah *Oxygen Forensic, MOBILedit Forensic Express,* dan *Magnet AXIOM*.

Oxygen Forensic Suite 2014 adalah perangkat lunak forensik produksi Oxygen Forensic Inc., yang digunakan untuk keperluan ekstraksi dan analisis data dari ponsel, smartphone dan tablet. Penggunaan protokol berbayar yang canggih memungkinkan Oxygen Forensic Suite 2014 untuk mengekstrak data lebih banyak dan menjamin pengoperasian tanpa merusak barang bukti. Perangkat lunak ini banyak digunakan oleh petugas penegak hukum, pemerintah, militer, penyelidik swasta dan spesialis forensik lainnya.

Gambar 1. Tampilan awal Oxigen Forensics Suite 2014

MOBILedit Forensic Express adalah perangkat lunak yang digunakan untuk melakukan ekstraksi, analisa data, dan membuat laporan hasil ekstraksi data pada smartphone. Tampilan MOBILedit Forensic Express dapat dilihat pada Gambar 2.



Gambar 2. Tampilan awal MOBILedit Forensics

Magnet AXIOM merupakan perangkat lunak forensik produksi Magnet Forensic yang dapat memproses dan menyiapkan bukti digital dari smartphone dan komputer menjadi satu dokumen laporan. Magnet AXIOM adalah alat pemeriksaan yang membantu profesional forensik dengan cepat menemukan data yang paling relevan dan memvisualisasikannya untuk analisis yang lebih baik. Magnet AXIOM banyak digunakan oleh profesional di bidang forensika digital untuk mencari bukti yang tidak dapat ditemukan oleh aplikasi forensik yang lain, melakukan verifikasi data, dan mengintegrasikan gambar yang diperoleh dengan alat lain ke dalam satu dokumen laporan untuk proses pemeriksaan. Magnet AXIOM merupakan platform penyelidikan produksi Magnet Forensics, salah satu pemimpin global dalam pengembangan perangkat lunak forensik digital yang menerima, memeriksa dan mengalokasikan informasi dari komputer, smartphone , dan tablet. Magnet AXIOM memungkinkan pakar forensik untuk memperoleh, mempelajari, dan menganalisa bukti digital dari komputer, smartphone , dan tablet.

Gambar 3. Tampilan Awal Magnet Axiom

Ada banyak tool lainnya yang bisa digunakan untuk proses akuisisi bukti digital pada penelitian ini, seperti Andriller dan Autopsy, namun pada penelitian ini hanya menggunakan 3 tool karena untuk membatasi tujuan pada penelitian ini. Pada suatu kasus kejahatan teknologi komputer yang terjadi pada umumnya akan meninggalkan jejak aktivitas kejahatan. Jejak aktivitas yang terkait dengan tindak kejahatan tersebut dapat dijadikan sebagai barang bukti. Barang bukti kejahatan komputer dapat berupa barang bukti elektronik dan barang bukti digital. Barang bukti elektronik dapat berupa bentuk fisik dari perangkat elektronik tersebut atau dapat berupa media simpan, sedangkan barang bukti digital dapat berupa file dokumen, file history, atau file log yang berisikan data-data terkait yang dapat dijadikan sebagai informasi pendukung pengambil keputusan. Barang bukti elektronik dan barang bukti digital menjadi hal terpenting dalam suatu kasus kejahatan komputer, karena aktivitas tindak kejahatan komputer yang dilakukan terekam oleh sistem komputer pada media penyimpanan utama perangkat komputer [2].

Pada langkah kerja forensik dapat mengimplementasikan salah satu kerangka kerja dari beberapa standar yang digunakan dalam proses forensik seperti dari *National Institute of Standards and Technology* (NIST), *National Institute of Justice* (NIJ), *Integrated Digital Forensics Investigation Framework* (IDFIF), *Digital Forensic Research Work Shop* (DFRWS), atau kerangka kerja proses forensik lainnya [3].

Penelitian yang dilakukan Riadi et al (2018) berdasarkan parameter yang ditambahkan oleh Peneliti, Oxygen Forensic Suite memiliki indeks tertinggi skor kinerja sebesar 100%, diikuti oleh Andriller dengan skor kinerja indeks sebesar 25%, dan Autopsi 4.1.1 tidak memberikan hasil apa pun (hasil nol) karena tidak adanya fitur dekripsi file dan gambar untuk perangkat seluler. Terkait dengan kriteria parameter NIST, Oxygen Forensic Suite masih memiliki skor kinerja indeks tertinggi di 61,90% dan memenuhi hampir semua kriteria parameter NIST. Andriller berada di peringkat 2

dengan skor kinerja indeks sebesar 47,61% dan memenuhi 10 kriteria parameter NIST. Autopsy 4.1.1 memiliki nilai kinerja indeks terendah sebesar 9,52% karena tidak adanya fitur dekripsi dokumen dan hanya memenuhi 2 kriteria parameter NIST. Andriller memang memenuhi banyak kriteria parameter NIST, namun, Andriller berhasil mendapatkan hanya artefak data percakapan menggunakan akuisisi fisik. Oxygen Forensic Suite memiliki skor kinerja tertinggi di antara tiga alat forensik yang digunakan, tetapi Oxygen Forensic Suite memiliki kelemahan dalam hal opsi untuk memilih data untuk Andriller pada tanggal 2 dengan skor kinerja indeks pada 47,6 [4].

Penelitian yang dilakukan Riadi et al (2017) Belkasoft memiliki paling tinggi nomor indeks 88,23%, diikuti oleh Oxygen Forensic dengan nomor indeks 82,35%, dan WhatsApp DB/Key Extractor dengan nomor indeks 23,52%. WhatsApp Key/DB Extractor memiliki kelemahan mengikuti kriteria parameter NIST. Namun, WhatsApp Key/DB Extractor mengelola untuk mendapatkan artefak pesan teks, akun WhatsApp daftar, dan log panggilan WhatsApp menggunakan akuisisi logis. WhatsApp Key / DB Extractor juga memiliki keunggulan dalam hal biaya karena merupakan alat forensik open source. Belkasoft Evidence memiliki angka indeks tertinggi di antara ketiga alat forensik yang digunakan. Bukti Belkasoft hamper memenuhi semua parameter NISST. Bukti Belkasoft memiliki hambatan dalam memperoleh artefak WhatsApp menggunakan logika perolehan. Dengan akuisisi logis, Belkasoft Evidence tidak dapat memperoleh artefak daftar akun WhatsApp, log panggilan WhatsApp, dan pesan teks. Oksigen Forensik memiliki kelemahan dalam hal opsi untuk memilih data untuk akuisisi dan pemberitahuan jika ada gangguan koneksi selama proses akuisisi. Oksigen Forensik berhasil memenuhi semua parameter artifak WhatsApp dengan akuisisi logis dan akuisisi fisik. Meskipun Belkasoft Bukti memiliki nomor indeks tertinggi dan keunggulan WhatsApp Key/DB Extractor dalam hal biaya, Oksigen Forensik lebih unggul dalam memperoleh WhatsApp artefak, baik melalui logika akuisisi atau fisik perolehan [5].

Penelitian yang dilakukan Fadlil et al (2018) kemampuan analitik dari MOBILedit Forensic memiliki yang tertinggi nomor indeks sebanyak 76,19% sedangkan Oxygen Forensic memiliki 61,90% dari angka indeks. Dalam hal ini analisis LINE messenger. Oksigen Forensik bisa lebih baik dalam laporan data daripada forensik MOBILedit. MOBILedit memiliki batasan dalam mengekstraksi video di LINE messenger. Namun, MOBILedit Forensic tidak memiliki fungsi manajemen kasus seperti pada Oxygen Forensic, tetapi MOBILedit sangat efisien dalam hal laporan data dan ekstraksi data [6].

Penelitian yang dilakukan Fadlil et al (2017) penyelesaian kasus-kasus kejahatan pada Smartwatch tentunya perlu bukti-bukti yang ada di dalam Smartwatch itu, hal ini merupakan tantangan baru bagi penyidik dalam megungkap kejahatan yang ada dalam smartwatch. Metode-metode yang dapat digunakan dalam proses pengambilan Barang bukti yang ada di dalam Smartwatch adalah NIST Mobile Forensics, NIJ Forensics, Integrated Digital forensics Identification Framework (IDFIF) dan Chain of Custody (CoC), masing-masing metode ini memiliki proses dan langkah yang berbeda juga. Sedangkan dalam penelitiaan ini peneliti menggunakan pengembangan metode dari metode NIJ Forensics. Setelah melakukan uji coba serta analisis forensic menggunakan tool MOBILedit forensic pada msartwatch telah mendapatkan hasil dalam mengumpulkan data berupa sms, data akun, dan data panggilan pada smartwatch [7].

Penelitian yang dilakukan Umar et al (2018) pertumbuhan informasi dan komunikasi teknologi sangat cepat. Email adalah salah satu media yang digunakan untuk bertukar informasi data, gambar dan lain-lain. Seiring pesatnya perkembangan pertukaran informasi dan komunikasi, menyebabkan kejahatan cyber berkembang. Jadi untuk para pelaku kejahatan cyber atau cybercrime dibutuhkan bukti. Kejahatan yang dilakukan oleh cybercrime dapat menjadi forensik pada email. Penelitian ini akan melakukan forensik pada email dengan cara mengakuisisi email berbasis android sebagai bukti digital dengan menggunakan metode NIST. Pada tahap pengumpulan bukti dilakukan pada smartphone Android lollipop 5.0.2 jenis Xiaomi Mi4i, untuk melakukan akuisisi pada email berbasis Android maka email harus dibuka menggunakan browser. Dalam penelitian ini menggunakan browser asli dari android. Pada fase pengujian, dari serangkaian proses yang telah dilakukan dalam memperoleh alamat IP pengirim di header email, selain alamat IP pengirim ditemukan juga alamat IP penerima, alamat email pengirim, protokol email, email pengirim waktu, waktu email yang diterima dan enkripsi email. Pada tahap akhir proses akuisisi di email berhasil

dilakukan dengan memperoleh alamat IP mengirim email di header sebagai bukti digital. Dalam penelitian selanjutnya dapat melacak alamat IP dari pengirim email [8].

Penelitian yang dilakukan Yudhana et al (2017) penggunaan metode National Institute of Justice (NIJ) mengurutkan tahapan forensic digital dengan mulai dari Identification, Examination, Analysis, dan Reporting dengan sangat baik. Metode ini banyak digunakan dalam menangani kasus kejahatan digital. Hasil akuisisi kemudian akan di analisa dengan cara menerjemahkan kode-kode hexsa hasil akuisisi sehingga menghasilkan Barang bukti yang yang bisa di mengerti oleh hakim nantinya [9].

Penelitian yang dilakukan Riaidi et al (2018) berdasarkan hasil dari penelitian yang telah dilakukan pada implementasi salah satu software pembeku drive yaitu Shadow Defender yang dapat membekukan suatu drive frozen Solid State Drive (SSD) dan terbukti berpengaruh terhadap praktik eksaminasi dan analisa forensik terhadap didapatkannya bukti- bukti digital. Tidak semua file dapat direstorasi dengan baik karena struktur file dan data sudah rusak, serta catatan pengguna komputer (recent activity) dan sejarah internet (history internet) tercatat ketika fitur pembeku drive diaktifkan. Jika dilakukan perhitungan tingkat prosentase keberhasilannya hanya memiliki nilai 28,7% yang diperoleh dari 85 file yang disiapkan untuk implementasi dan pengujian dan hasil file dari eksaminasi dan yang berhasil direstorasi hanya 25 file. Sehingga dapat menjadi hambatan dalam proses forensik digital (digital forensics) oleh penyidik dan hasil dari penyidikan masih sangat sedikit informasi yang didapatkan dari Barang bukti digital [10].

Penelitian yang dilakukan Riadi et al (2017) whatsapp telah menjadi aplikasi populer untuk jejaring sosial dimana orang dapat bertukar informasi pribadi beserta mobilitas yang mereka geluti. Penelitian ini telah menunjukkan bahwa seseorang dapat memperoleh akses lengkap ke semua informasi di WhatsApp baik itu whatsapp smartphone maupun whatsapp web. Sebagian besar aplikasi chat mengikuti pola sinkronisasi pesan, kontak dan data pengguna yang sama saat syinc dan memperbarui data percakapan secara berkala. Pendekatan yang diambil memberi garis besar umum untuk semua aplikasi serupa yang berjalan di perangkat ber-platform Android maupun Windows seperti Telegram dan sejenisnya. Penelitian ini dapat bermanfaat untuk Mobile Forensic Analysis dan Investigation pada smartphone Android dan aplikasi ganda berbasis web browser. Database QR Code membutuhkan autentikasi terhadap smartphone hanya sekali setiap saat login pertama kali sehingga dibutuhkan kewaspadaan penggunanya seperti penggunaan pattern lock pada smartphone dan login user password pada komputer penggunanya. Proses akuisisi langsung terhadap smartphone korban dan analisis web browser pada komputer. Diharapkan kedepan lebih banyak penelitian yang dapat dilakukan pada interpretasi data percakapan WhatsApp dalam bentuk jurnal atau naskah lain sebagai literatur selanjutnya [11].

Penelitian yang dilakukan Yadi & Kunang (2014) kesimpulan dari penelitian ini memperlihatkan keberhasilan implementasi pada platform Tool pengujian. Lingkungan forensik testing dibangun sebelum menguji tools. Benchmark diidentifikasi dengan cara mengumpulkan informasi bukti secara manual dari ponsel. Kemudian hasil awal ini diuji kembali dengan mengekstrak data menggunakan forensic tools untuk kedua ponsel yang berbeda versi sistem operasi Android. Dari hasil yang diperoleh bisa didapatkan kesimpulan sebagai berikut:

1. Masing-masing tool yang diuji menggunakan methodology yang berbeda untuk mengekstrak data. Misalnya pada MOBILedit tidak mendukung ekstraksi data dari SD card sementara tools lain bisa. Sedangan untuk android versi froyo tidak bisa dilakukan ekstraksi data untuk memori internal ponsel menggunakan FTK imager.
2. Semua tools tersebut kecuali proses ekstraksi manual menggunakan aplikasi agent untuk mengambil data dari ponsel Android. Kesulitan utama dari proses analisis forensik dengan platform android ini adalah dukungan aplikasi agent (adb driver) masing-masing tool untuk semua jenis ponsel android yang tidak semuanya bisa dikenali.
3. Dari hasil pengujian yang dilakukan tool Oxygen memiliki fitur report yang lebih lengkap dibandingkan tool ektraksi android forensik MOBILedit dan AFLogical. Tool ini hampir bisa mengekstrasi keseluruhan data aktual dari kontak ponsel, call log, sms-mms, kalender file gambar, video, dan file lainnya.

4. Untuk ekstraksi file barang bukti yang sudah dihapus atau diformat, proses analisis ponsel menggunakan cara ekstraksi manual dengan proses pembuatan image merupakan cara terbaik yang bisa dilakukan [12].

Pada penelitian ini mengadaptasi dan mengimplementasikan metode analisa forensik dari *National Institute of Justice* (NIJ). Metode ini untuk menjelaskan bagaimana tahapan penelitian yang akan dilakukan sehingga dapat diketahui alur dan langkah-langkah penelitian secara sistematis sehingga dapat dijadikan pedoman dalam menyelesaikan permasalahan yang ada. Melakukan teknik forensik dan analisa forensik berdasarkan metode yang benar akan memiliki keberhasilan hampir 100% dalam mengumpulkan data forensik [13].

2. METODE PENELITIAN

Penelitian ini mengacu pada proses investigasi yang digunakan metode *National Institute Of Justice* (NIJ). Metode ini merekomendasikan sebuah tahapan dasar dalam proses forensik, yaitu persiapan, koleksi, pemeriksaan, analisis dan pelaporan. Metode penelitian yang digunakan berdasarkan pedoman forensik perangkat mobile yang dibuat oleh *National Institute of Justice* (NIJ) dengan langkah-langkah sebagai berikut:

Penulis menjabarkan tahapan forensik pada Gambar 4.

Gambar 4. Pedoman forensik perangkat mobile yang dikembangkan oleh NIJ

1. Persiapan

   Peneliti mengidentifikasi masalah dan mengumpulkan informasi tentang masalah yang akan dihadapi. proses mempersiapkan peralatan untuk melakukan tugas yang diperlukan dalam penyelidikan. Koleksi adalah proses mencari dokumen, dan mengumpulkan atau membuat salinan benda fisik yang mengandung barang bukti elektronik.
2. Koleksi

   Peneliti mengajukan solusi yang mungkin untuk dilakukan dalam pemecahan masalah dari hasil identifikasi masalah dan informasi dari hasil tahap pertama. proses membuat bukti elektronik terkihat dan mendokumentasikan konten dan sistem, reduksi data dilakukan untuk meidentifikasi bukti.
3. Pemeriksaan

   Setelah mendapatkan solusi yang mungkin di lakukan dari tahap kedua, peneliti kemudian melakukan uji coba terhadap smartphone dari setiap solusi yang mungkin dilakukan untuk pemecahan masalah.
4. Analisis

   Melakukan evaluasi dari hasil yang di dapat dari hasil uji coba yang dilakukan dari setiap solusi agar di lakukan untuk pemecahan masalah.
5. Laporan

   Melaporkan hasil uji coba yang meliputi penggambaran tindakan yang dilakukan.

3. HASIL DAN PEMBAHASAN

3.1 Persiapan

Pada penelitian ini membutuhkan alat dan bahan seperti laptop, 2 buah *smartphone,* Kabel data USB, Facebook Messenger, dan 3 tool forensik yaitu MOBILedit Forensic Express, Magnet Axiom dan Oxigen Forensics Suite 2014.

Tabel 1. Alat dan bahan yang dibutuhkan

No.	Nama Alat dan Bahan	Deskripsi	*Hardware/Software*
1.	Laptop	Acer E14, Windows 10	*Hardware*
2.	*Smartphone*	Samsung Galaxy V+ SM-G318HZ, Samsung Galaxy Trend Plus GT-S7580	*Hardware*
3.	Kabel Data Mikro USB	Kabel Data	*Hardware*
4.	Facebook Messenger	Aplikasi Android	*Software*
5.	MOBILedit Forensic Express	Alat Forensik	*Software*
6.	Magnet AXIOM	Alat Forensik	*Software*
7.	Oxigen Forensic Suite	Alat Forensik	*Software*

3.2 Koleksi

Tahap selanjutnya adalah tahap dimana peneliti mengajukan solusi yang dilakukan untuk pemecahan masalah dari hasil identifikasi masalah dan informasi hasil tahap pertama. Tahap ini peneliti menggunakan 2 Smartphone Android dengan merk Samsung Galaxy V+ SM-G318HZ, Samsung Galaxy Trend Plus GT-S7580 bertujuan untuk objek dalam tahap pengujian, kemudian menggunakan solusi untuk mengembalikan data yang telah dihapus dengan menggunakan 3 tool forensik yaitu *MOBILedit Forensic Express, dan Oxigen Forensics Suite 2014.*

Gambar 5. Smartphone yang digunakan

Tabel 2. Spesifikasi Smartphone

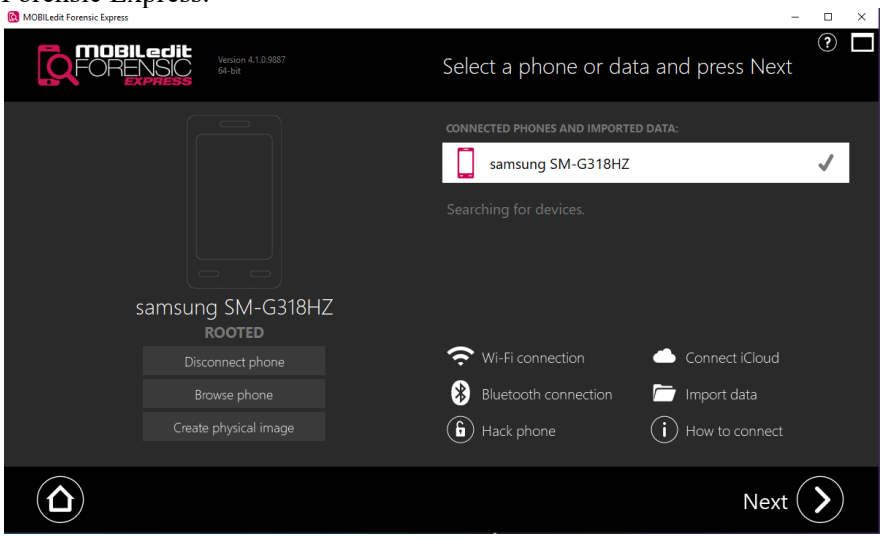
Jenis Spesifikasi	*Smartphone* 1	*Smartphone* 2
Merek	Samsung	Samsung
Seri	Galaxy	Galaxy

Model	V+	Tren Plus
Nomor Model	SM-G318HZ	GT-S7580
IMEI	353248072061xxx	3549000647xxx
OS	Android	Android
Versi OS	4.4.2 (KitKat)	v4.2 (Jelly Bean)
Processor	ARM Cortex-A7 Dual-core 1.2 GHz	Dual core, 1.2 GHz

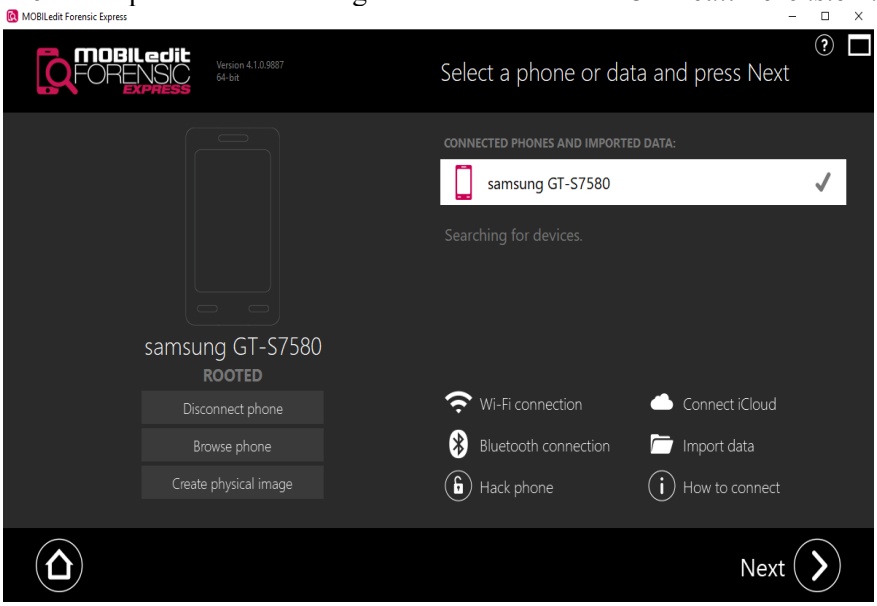
3.3 Pemeriksaan

a. Pemeriksaan pada *MOBILedit Forensic Express*

Tool forensik yang digunakan pada tahap Pemeriksaan ini adalah MOBILedit Forensic Express. MOBILedit Forensic Express dapat membuat backup dan imaging sistem karena mendukung berbagai format image, yang dapat digunakan pada berbagai tool forensik. Pemeriksaan dengan MOBILedit Forensic Express memiliki 2 cara, yang pertama yaitu Barang bukti harus terkoneksi terlebih dahulu pada komputer atau laptop tempat MOBILedit Forensic Express di-install. Gambar 2 dan 3 terdapat Smartphone 1 dan Smartphone 2 yang telah tersambung dan terdeteksi oleh MOBILedit Forensic Express.



Gambar 6. Smartphone 1 tersambung dan terdeteksi oleh *MOBILedit Forensic Express*



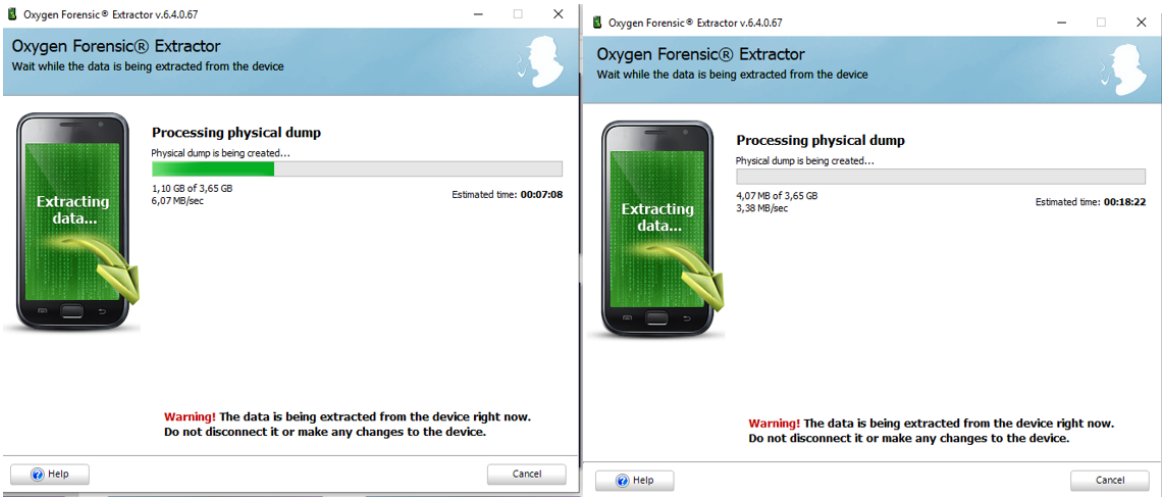
Gambar 7. Smartphone 2 tersambung dan terdeteksi oleh *MOBILedit Forensic Express*

b. Pemeriksaan pada *Oxigen Forensics Suite 2014*

Pemeriksaan dengan *Oxygen Forensic Suite 2014* dapat dilakukan dengan ekstraksi langsung dari *Logical Extraction* dan *Physical Extraction. Physical Extraction* dapat dilakukan dengan ketentuan bahwa smartphone harus terkoneksi terlebih dahulu pada laptop tempat *Oxygen Forensic Suite 2014* ter-install. *Oxygen Forensic Suite 2014* adalah perangkat lunak forensik produksi *Oxygen Forensic Inc*., yang digunakan untuk keperluan ekstraksi dan analisis data dari ponsel, smartphone dan tablet. Penggunaan protokol berbayar yang canggih memungkinkan *Oxygen Forensic Suite 2014* untuk mengekstrak data lebih banyak dan menjamin pengoperasian tanpa merusak barang bukti. Perangkat lunak ini banyak digunakan oleh petugas penegak hukum, pemerintah, militer, penyelidik swasta dan spesialis forensik lainnya. Gambar 4 menunjukkan informasi 2 *smartphone* yang telah terdeteksi oleh *Oxygen Forensic Suite 2014*.

Gambar 8. Informasi 2 Smartphone

Oxygen Forensic Suite 2014 akan mulai melakukan ekstraksi. Tampilan proses ekstraksi yang sedang berjalan untuk 2 Barang bukti seperti Gambar 9.



Gambar 9. Proses Ekstraksi

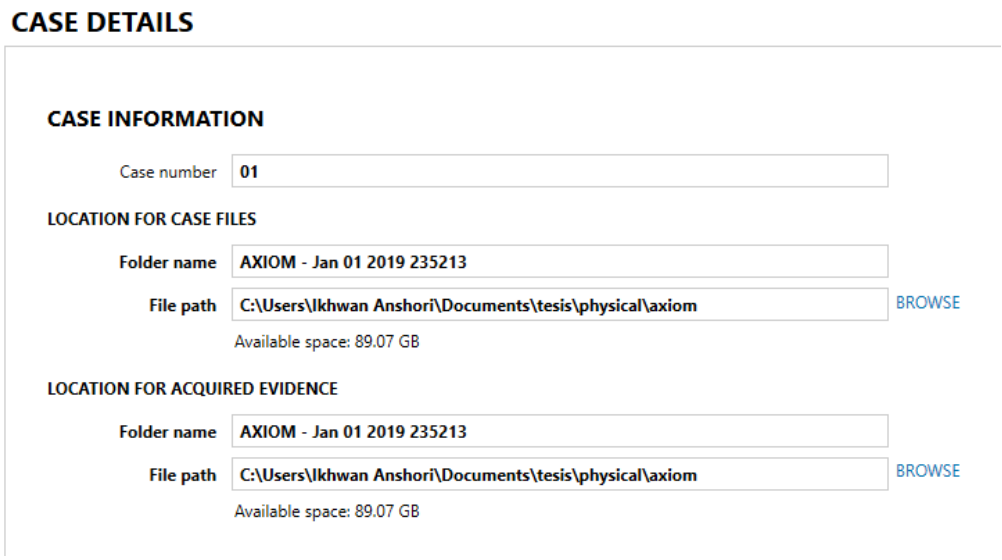
c. Pemeriksaan pada *Magnet AXIOM*

Pemeriksaan dengan *Magnet AXIOM* mampu melakukan *live extraction* dan ekstraksi melalui *physical image*, adapun pada penelitian ini akan dilakukan ekstraksi melalui tahap *live extraction. Magnet AXIOM* banyak digunakan oleh profesional di bidang forensika digital untuk

mencari bukti yang tidak dapat ditemukan oleh aplikasi forensik yang lain, melakukan verifikasi data, dan mengintegrasikan gambar yang diperoleh dengan alat lain ke dalam satu dokumen laporan untuk proses pemeriksaan.

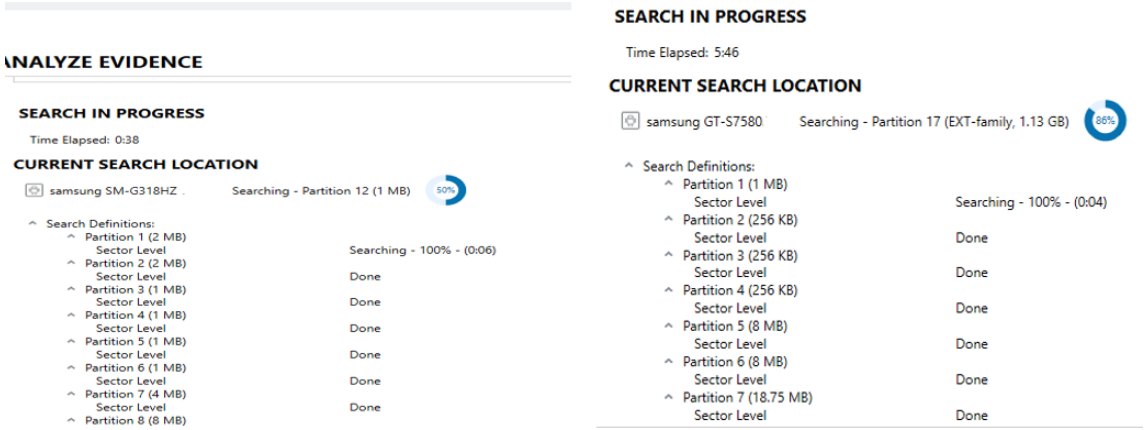
Magnet AXIOM merupakan platform penyelidikan produksi *Magnet Forensics*, salah satu pemimpin global dalam pengembangan perangkat lunak forensik digital yang menerima, memeriksa dan mengalokasikan informasi dari komputer, smartphone, dan tablet.

Proses pertama, *Magnet AXIOM* akan meminta pengguna untuk mengisi detil kasus berupa informasi kasus, lokasi penyimpanan file kasus, dan lokasi penyimpanan hasil ekstraksi tampilannya seperti Gambar 10.



Gambar 10. *Input Case Information*

Magnet AXIOM akan mulai melakukan ekstraksi data. Lamanya proses ekstraksi dapat bervariasi bergantung pada besarnya data yang terdapat pada barang bukti. Gambar 11 menunjukkan proses ekstraksi yang sedang berlangsung pada Smartphone 1 dan Smartphone 2.



Gambar 11. Proses Ekstraksi

3.4 Analisis

Tahap Analysis merupakan tahap untuk melihat hasil dari tahap Pemeriksaan secara detil untuk mendapatkan bukti digital. Tahap ini membatasi proses pencarian pada bagian tertentu dari hasil yang didapat pada tahap Pemeriksaan. Pembatasan ini dapat berupa hal-hal yang berhubungan dengan data atau aplikasi tertentu. Penelitian ini membatasi pencarian bukti digital pada hasil yang

didapat dari aplikasi Facebook Messenger. Hasil analisis yang diperoleh kemudian dibuat tabel perbandingan dari masing-masing-perangkat lunak untuk mendapatkan kombinasi perangkat lunak yang direkomendasikan pada penyelesaian suatu kasus kejahatan digital pada perangkat dan aplikasi tertentu. Hasil analisis berdasarkan kemampuan dan fitur masing-masing perangkat lunak yang digunakan pada penelitian ini adalah sebagai berikut:

a. Analysis dengan *MOBILedit Forensic Express*

MOBILedit Forensic Express adalah perangkat lunak yang digunakan untuk melakukan ekstraksi, analisa data, dan membuat laporan hasil ekstraksi data pada *smartphone*. *MOBILedit Forensic Express* tidak memiliki fitur untuk melakukan *decrypt file* pada aplikasi Facebook Messenger, sehingga saat ekstraksi dilakukan tidak didapatkan hasil yang signifikan. Informasi yang didapat terkait aplikasi Facebook Messenger pun hanya sebatas ukuran file dan waktu instalasi Facebook Messenger saja, seperti pada Gambar 12.

Messenger

Label	Messenger
Package	com.facebook.orca
Version	196.0.0.29.99
Application Type	User Application
Application Size	40.7 MB
Data Size	120.9 MB
Cache Size	2.8 MB
First Installed	2018-12-22 00:44:30 (UTC+7)
Last Updated	2018-12-22 00:44:30 (UTC+7)
RAM Usage	50.8 MB

Messenger

Label	Messenger
Package	com.facebook.orca
Version	195.0.0.28.99
Application Type	User Application
Application Size	40.2 MB
Data Size	111.3 MB
Cache Size	2.2 MB
First Installed	2018-11-29 10:47:08 (UTC+7)
Last Updated	2018-12-20 22:15:25 (UTC+7)
RAM Usage	36.9 MB

Gambar 12. Hasil Info Facebook Messenger

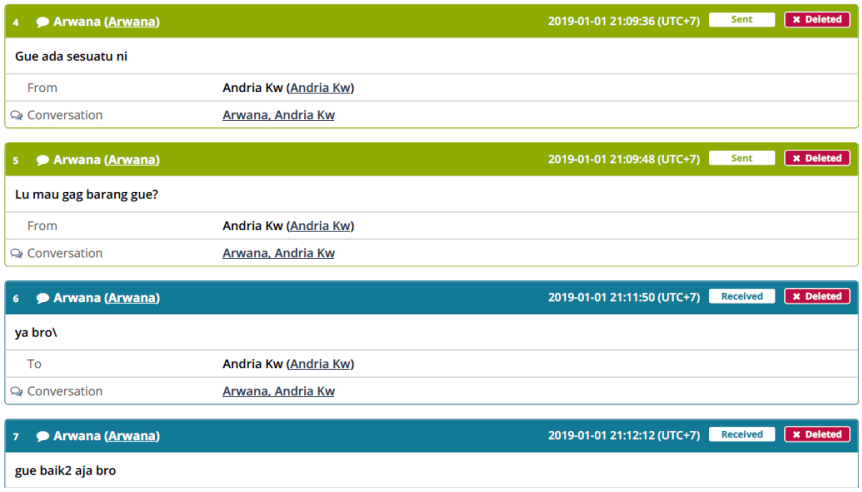
Pada Gambar 13 terdapat informasi pemilik akun Facebook Messenger yang telah terinstall pada *Smartphone* 1 dan Smartphone 2. Pemilik akun bernama Andria KW, *Brithday* 1991-05-17 dan *Phone Number* +6282172300xxx.

Andria Kw

Facebook ID	100029258283332
Birthday	1991-05-17
Phone Number	+628217230[redacted]
Picture Url	https://scontent.xx.fbcdn.net/v/t1.0-1/c31.0.80.80a/p80x80/43253583_101774924141117_7402032859394867200_n.jpg?_nc_cat=111&_nc_eui2=AeEOPRbd6eZQw1feRUPgv1d6OXnf1kIGULcNTNcEWTYfT15SdnrZ4MmpuzakVjftjapnaOm7LE7ruuT3AZSenZuS&_nc_ad=z-m&_nc_cid=1101&_nc_ht=scontent.xx&oh=dde39059cf12813fde69e3998ce85e05&oe=5C9947D5
Picture Url	https://scontent.xx.fbcdn.net/v/t1.0-1/c31.0.80.80a/p80x80/43253583_101774924141117_7402032859394867200_n.jpg?_nc_cat=111&_nc_eui2=AeEOPRbd6eZQw1feRUPgv1d6OXnf1kIGULcNTNcEWTYfT15SdnrZ4MmpuzakVjftjapnaOm7LE7ruuT3AZSenZuS&_nc_ad=z-m&_nc_cid=1101&_nc_ht=scontent.xx&oh=dde39059cf12813fde69e3998ce85e05&oe=5C9947D5
Picture Url	https://scontent.xx.fbcdn.net/v/t1.0-1/c47.0.120.120a/p120x120/43253583_101774924141117_7402032859394867200_n.jpg?_nc_cat=111&_nc_eui2=AeEOPRbd6eZQw1feRUPgv1d6OXnf1kIGULcNTNcEWTYfT15SdnrZ4MmpuzakVjftjapnaOm7LE7ruuT3AZSenZuS&_nc_ad=z-m&_nc_cid=1101&_nc_ht=scontent.xx&oh=35fa5ae04aaee628d8ab2760130e0b76&oe=5C9B09BA
Picture Url	https://scontent.xx.fbcdn.net/v/t1.0-

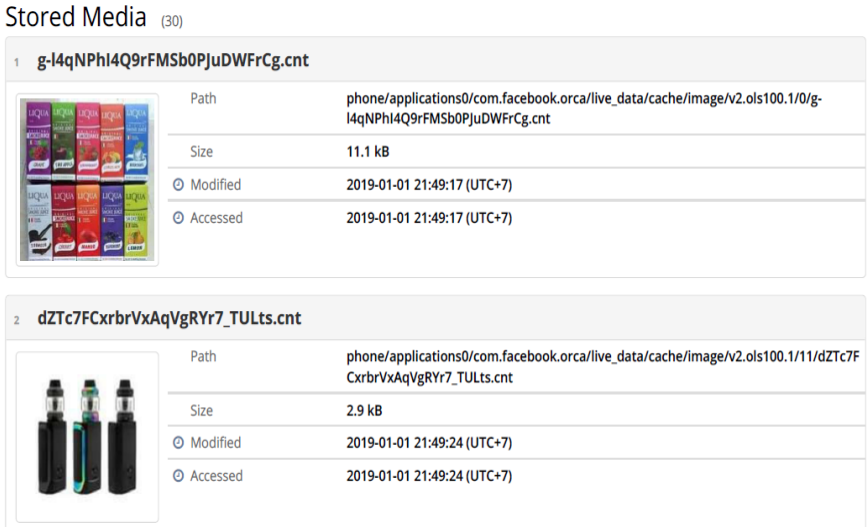
Gambar 13. Informasi Pemilik Akun Facebook Messenger

Hasil ekstraksi yang dilakukan menggunakan MOBILedit Forensic Express dapat menampilkan chat dapat dilihat pada Gambar 14.



Gambar 14. Hasil Reporting Percakapan di Facebook Messenger

MOBILedit Forensic Express dapat pula menampilkan gambar terlihat pada Gambar 15.



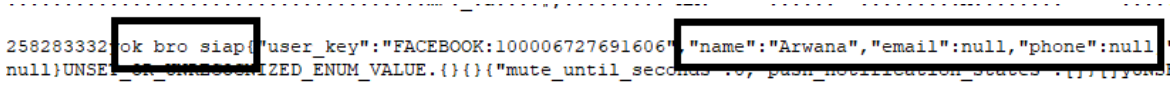
Gambar 15. Hasil *Reporting* Gambar di Facebook Messenger

b. Analysis dengan *Oxigen Forensics Suite 2014*

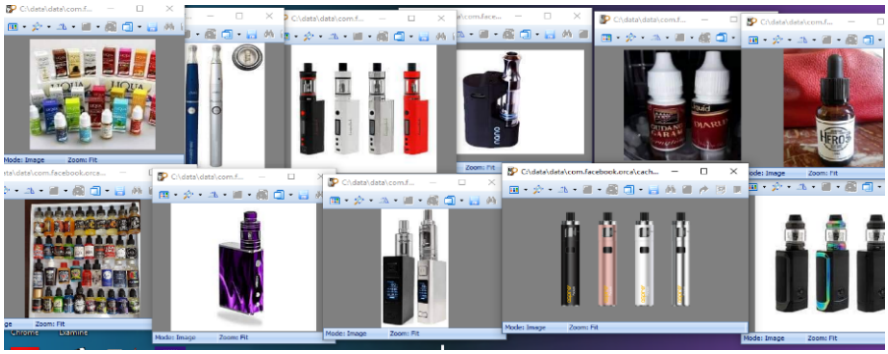
Hasil ekstraksi yang didapatkan dari proses pemeriksaan berupa akun Facebook Messenger, data percakapan, dan gambar. Pada Oxigen Forensics Suite 2014 dapat menampilkan 2 akun Facebook Messenger dapat dilihat pada Gambar 16. Kemudian didapatkan 1 data percakapan yang dapat dilihat pada Gambar 17 dan dapat menampilkan gambar sebanyak 26 gambar seperti pada Gambar 18.

user_key	first_name	last_name	username	name	is_messenger_user
FACEBOOK:100<TRIAL>XXXXX	And<TRIAL>	Kw	andr<TRIAL>	Andr<TRI...	1
FACEBOOK:100<TRIAL>XXXXX	Arw<TRIAL>		ikhwan.a<TRIAL>7	Arw<TRIAL>	1

Gambar 16. Informasi Akun



Gambar 17. Hasil Reporting Percakapan di Facebook Messenger



Gambar 18.Tampilan Hasil Gambar

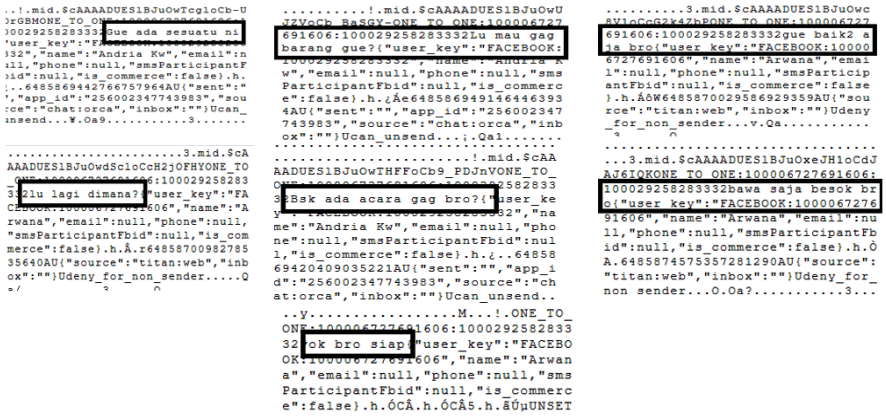
c. Analysis dengan Magnet AXIOM

Hasil ekstraksi yang didapatkan dari proses Pemeriksaan yang telah dilakukan pada Smartphone 1 dan Smartphone 2 mendapatkan hasil berupa data 2 akun Facebook Messenger, 11 data percakapan, dan 26 gambar. Gambar 19 menunjukkan hasil berupa akun Facebook Messenger pemilik akun bernama Andria KW dan Arwana. Gambar 20 menunjukkan chat dan pada Gambar 21 menunjukkan hasil berupa gambar.

threadusers

_id	user_key	first_name	last_name	username	name	is_messenger_user	profile_pic_square	profile_type
3	FACEBOOK:100029258283332	Andria	Kw	andria.kw	Andria...	1	[{"url":"https://sconten...	user
4	FACEBOOK:100006727691606	Arwana	[NULL]	ikhwan.an...	Arwana	1	[{"url":"https://sconten...	user

Gambar 19. Informasi Akun



Gambar 20. Hasil Reporting Percakapan di Facebook Messenger

Gambar 21. Tampilan Hasil Gambar

3.5 Laporan

Tahap Reporting/ Pelaporan merupakan tahap pembuatan laporan hasil analisis, yang mencakup deskripsi mengenai kasus yang terjadi, metodologi forensik yang dilakukan, teknik dan alat forensik yang digunakan, ada atau tidaknya tindakan, pedoman, prosedur, perangkat, dan aspek lain yang sekiranya diperlukan. Tahap Reporting pada penelitian ini meliput ringkasan mengenai smartphone yang digunakan dan prosedur forensik yang dilakukan serta perbandingan tool forensik yang digunakan. Informasi smartphone yang digunakan yang akan dilaporkan yaitu: bukti fisik berupa 2 unit smartphone berbasis Android dengan rincian.

1. Samsung Galaxy V+ SM-G318HZ, OS Android v4.4.2 Kitkat (Smartphone 1).
2. Samsung Galaxy Trend Plus GT-S7580, OS Adroid v4.2 Jelly Bean (Smartphone 2).

Aplikasi yang akan dianalisis bukti digitalnya adalah aplikasi Facebook Messenger yang terpasang pada Smartphone 1 dan Smartphone 2 yang berbasis Android. Dalam simulasi kasus dilakukan pembuatan data bukti digital berupa 2 akun, 20 chat dan 30 gambar.

Prosedur pemeriksaan yang dilakukan terhadap yang ditemukan adalah sebagai berikut:

1. Smartphone yang diakuisisi dan dilakukan proses penghilangan jangkauan sinyal dengan mengaktifkan airplane mode.
2. Proses cloning Smartphone 1 dan Smartphone 2 dilakukan menggunakan MOBILedit Forensic Express dengan mengkoneksikannya ke Laptop Merk Acer, Model E14, OS Windows 10 64 bit, kapasitas harddisk 500 GB.
3. Ekstraksi dan analisis terhadap bukti digital dari aplikasi Facebook Messenger dilakukan menggunakan MOBILedit Forensic Express, Oxygen Forensic Suite 2014, Magnet AXIOM. Pada Smartphone 1 dan Smartphone 2 dilakukan pemeriksaan berdasarkan prosedur metode NIST. Hasil pemeriksaannya adalah sebagai berikut:
   a. Ditemukan informasi terkait aplikasi yang digunakan yaitu Facebook Messenger.
   b. Analisis yang dilakukan pada bukti digital yang diambil dari aplikasi Facebook Messenger juga menemukan akun, chat dan gambar.
   c. Alat bantu forensik berupa perangkat lunak yang digunakan pada proses pengambilan bukti digital terdiri dari 3 jenis dengan fitur dan kemampuan yang bermacam-macam.

Tabel 3. Hasil bukti digital

No	Bukti Digital	Alat Forensik		
		MOBILedit Forensic Express	Oxygen Forensic Suite 2014	Magnet AXIOM
1	Akun	2	2	2
2	Chat	11	1	11
3	Gambar	26	26	26

Tabel 3 menunjukkan hasil bukti digital dari *MOBILedit Forensic Express* didapatkan 2 akun, 11 chat dan 26 gambar, hasil dari *Oxygen Forensic Suite 2014* didapatkan 2 akun, 1 chat dan 26 gambar, dan hasil *Magnet AXIOM* didapatkan 2 akun, 11 chat dan 26 gambar.

Tabel 4. Persentase bukti digital

No	Bukti Digital	Alat Forensik		
		MOBILedit Forensic Express	Oxygen Forensic Suite 2014	Magnet AXIOM
1	Akun	100%	100%	100%
2	Chat	55%	5%	55%
3	Gambar	86%	86%	86%

Tabel 4 terdapat persentase bukti digital dari alat forensik *MOBILedit Forensic Express* mendapatkan bukti digital dengan persentase berupa 100% akun, 55% dalam mendapatkan chat dan 86% gambar. *Magnet AXIOM* mendapatkan bukti digital dengan persentase berupa 100% akun, 55 chat dan 86% gambar. *Oxygen Forensic Suite 2014* mendapatkan bukti digital dengan persentase berupa 100% akun, 5% chat dan 86% gambar.

4. KESIMPULAN

Hasil yang didapatkan dari proses penelitian mengenai analisis forensik bukti digital pada aplikasi Facebook Messenger yang berjalan pada smartphone Android memberikan beberapa kesimpulan sebagai berikut:

1. Bukti digital didapatkan berupa akun, chat dan gambar yang terkait dengan simulasi kasus perdagangan liquid vape narkoba. Proses forensik dengan metode NIST dan alat forensik dapat digunakan dalam proses ekstraksi bukti digital pada Facebook Messenger yang terpasang pada perangkat smartphone Samsung Galaxy V+ SM-G318HZ dan Samsung Galaxy Trend Plus GT-S7580.
2. Bedasarkan bukti digital yang didapatkan pada 3 alat forensik dapat disimpulkan sebagai berikut:
   a. MOBILedit Forensic Express mendapatkan bukti digital berupa 2 akun, 11 chat dan 26 gambar dengan persentase berupa 100% dalam mendapatkan akun, 55% dalam mendapatkan chat dan 86% dalam mendapatkan gambar. Dapat disimpulkan bahwa MOBILedit Forensic Express memiliki kinerja yang baik dalam mendapatkan bukti digital pada Facebook Messenger.
   b. Magnet AXIOM mendapatkan bukti digital berupa 2 akun, 11 chat dan 26 gambar dengan persentase berupa 100% dalam mendapatkan akun, 55% dalam mendapatkan chat dan 86% dalam mendapatkan gambar. Dapat disimpulkan bahwa Magnet AXIOM memiliki kinerja yang baik dalam mendapatkan bukti digital pada Facebook Messenger.
   c. Oxygen Forensic Suite 2014 mendapatkan bukti digital berupa 2 akun, 1 chat dan 26 gambar dengan persentase berupa 100% dalam mendapatkan akun, 5% dalam mendapatkan chat dan 86% dalam mendapatkan gambar. Dapat disimpulkan bahwa Oxygen Forensic Suite 2014 memiliki kinerja yang kurang baik dalam mendapatkan bukti digital pada Facebook Messenger.

DAFTAR PUSTAKA

[1] A. Yudhana, I. Riadi, and I. Anshori, "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist," vol. 3, no. 1, pp. 13–21, 2018.
[2] V. No, G. M. Zamroni, R. Umar, and I. Riadi, "Analisis Forensik Aplikasi Instant Messaging Berbasis Android," vol. 2, no. 1, pp. 102–105, 2016.
[3] A. Firdonsyah, I. Riadi, and Sunardi, "Analisis Forensik Bukti Digital Blackberry Messenger Pada Android," *Semin. Nas. Click Karawang*, pp. 25–29, 2016.
[4] 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.
[5] R. Umar, I. Riadi, and Z. Guntur Malulana, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 12, pp. 69–75, 2017, doi: 10.14569/IJACSA.2017.081210.
[6] A. L. Messenger, "A Study of Mobile Forensic Tools Evaluation on," vol. 9, no. 10, pp. 201–206, 2018, doi: 10.14569/IJACSA.2018.091024.
[7] R. A. Putra, A. Fadlil, and I. Riadi, "Forensik Mobile Pada Smartwach Berbasis Android," *Jurti*, vol. 1, no. 1. pp. 41–47, 2017.
[8] U. Rusydi, R. Imam, and M. Bashor fauzan, "Acquisition Of Email Service Based Android," vol. 3, no. 4, pp. 1–9, 2018, doi: http://dx.doi.org/10.22219/kinetik.v3i4.637.
[9] A. Yudhana, R. Umar, and A. Ahmadi, "Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ)," vol. X, no. X, pp. 8–13.
[10] I. Riadi, R. Umar, and I. M. Nasrulloh, "Analisis Forensik Digital Pada Frozen Slod State Drive Dengan Metode National Institute of Justice (Nij)," vol. 3, no. May, pp. 70–82, 2018, doi: 10.21831/elinvo.v3i1.19308.
[11] G. M. Zamroni, "Analisis Forensik Instant Messaging (WhatsApp) Berbasis Android," 2018.
[12] Y. K. IZ Yadi, "Analisis Forensik pada Platform Android," *Anal. Forensik pada Platf. Android - Konf. Nas. Ilmu Komput. (KONIK), 2014*.
[13] U. Rusydi, R. Imam, and Z. Guntur Maulana, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 3, p. 949, 2018, doi: 10.18517/ijaseit.8.3.3591.

BIOGRAFI PENULIS

Ikhwan Anshori, M.Kom obtained Bachelor Degree in Computer Science from Stmik Amik Riau in 2017, obtained Master of Informatics Engineering from Ahmad Dahlan University in 2019. he has been a Lecturer with the Department of Information Systems, STMIK Muhammadiyah Paguyangan Brebes, since 2019. His current research interests include digital forensics, and decision making system.

Khairina Eka Setya Putri, M.Kom obtained Bachelor Degree in Computer Science from Atma Jaya Yogyakarta University in 2015, obtained Master of Informatics Engineering from Ahmad Dahlan University in 2019. he has been a Lecturer with the Department of Information Systems, STMIK Muhammadiyah Paguyangan Brebes, since 2019. His current research interests include digital forensics, and decision making system.

Umar Ghoni, M.Kom obtained Bachelor Degree in Computer Science from Jenderal Soedirman University in 2009, obtained Master of Informatics Engineering from Dian Nuswantoro University in 2016. he has been a Lecturer with the Department of Informatics Engineering, STMIK Muhammadiyah Paguyangan Brebes, since 2018. His current research interests include programming algorithm, and decision making system.