SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Jurnal & Penelitian Teknik Informatika
Volume 3 Nomor 1, Oktober 2018
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android

Muhammad Sidik Asyaky
Universitas Siliwangi
Tasikmalaya, Indonesia
sidik.asyaky14@student.unsil.ac.id

Nur Widiyasono
Universitas Siliwangi
Tasikmalaya Indonesia
nur.widiyasono@unsil.ac.id

Rohmat Gunawan
Universitas Siliwangi
Tasikmalaya, Indonesia
rohmatgunawan@unsil.ac.id

***Abstract*—** Perkembangan jumlah pengguna aplikasi *Instant Messenger* (IM) yang sangat pesat menyebabkan naiknya potensi tindakan kriminal dilakukan melalui aplikasi IM. Fitur keamanan data aplikasi IM yang ditujukan untuk melindungi privasi penggunanya, digunakan oleh pelaku kriminal untuk menyembunyikan bukti digital dari aktivitas kriminalnya. Penelitian ini membahas mengenai analisa dan perbandingan bukti digital dari aplikasi IM pada *Android* yang telah diunduh sebanyak 500 juta orang di *Play Store*, yaitu *WhatsApp*, *Telegram*, *Line*, dan *IMO*. Proses analisa dilakukan pada bukti digital dari penggunaan fitur yang ada di aplikasi IM, sehingga proses pengumpulan data dibantu dengan simulasi dari beberapa skenario yang berpotensi terjadi dalam tindakan kriminal. Teknik akuisisi data dilakukan dengan metode *physical imaging* untuk mendapatkan akses penuh pada memori *smartphone*. Hasil analisa disimpulkan dalam bentuk tabel perbandingan yang dapat dirujuk oleh investigator forensik ketika melakukan investigasi aplikasi IM yang diteliti. Hasil analisa menyatakan bahwa bukti digital dari aktivitas tukar menukar pesan, berkas media, dan kontak ditemukan. Hasil analisa juga memberikan penjelasan mengenai kemungkinan untuk menganbil bukti digital yang dihapus dan bagaimana cara memulihkannya dengan teknik *data carving*.

Keywords—*Android*; bukti digital; forensik; *instant messenger*.

I. PENDAHULUAN

Jumlah pengguna aplikasi *Instant Messenger* (IM) dari tahun ke tahun berkembang sangat pesat, dengan 5 miliar jumlah pengguna aktif setiap bulannya pada tahun 2017 [1]. Aplikasi IM telah menggantikan *Short Message Service* (SMS) sebagai aplikasi komunikasi jarak jauh, dengan alasan aplikasi IM memiliki sifat mudah diakses dan murah. Kepopuleran aplikasi IM menyebabkan munculnya berbagai aplikasi dengan kategori *instant messaging* yang menawarkan fitur dan kualitas yang berbeda-beda. Salah satu fitur penting yang paling dicari oleh pengguna pada aplikasi IM adalah keamanan, yang menyebabkan pengembang aplikasi IM berlomba-lomba untuk memberikan fitur keamanan data terbaik untuk melindungi privasi penggunanya.

Fitur keamanan aplikasi IM yang baik memberikan dampak positif bagi penggunanya, namun ada juga dampak negatifnya. Fitur keamanan data privasi ini bisa digunakan oleh sebagian orang untuk melindunginya saat melakukan tindakan kriminal. Tindakan kriminal yang dapat ditemukan melalui aplikasi IM contohnya adalah penipuan dan ujaran kebencian, di samping itu aplikasi IM dapat digunakan sebagai alat komunikasi teroris. Perusahaan keamanan *Trend Micro* menyebutkan bahwa 34% dari 2301 akun terlibat terorisme yang dianalisa, menggunakan *Telegram* untuk berkomunikasi [2]. Forensik digital adalah bidang ilmu yang digunakan untuk menginvestigasi kejahatan yang berhubungan dengan perangkat digital. Proses forensik digital dilakukan untuk mencari bukti digital yang dapat diakui dan dijadikan bukti yang sah di ranah hukum.

Aplikasi IM yang digunakan pada penelitian ini adalah *Telegram*, *Line*, *IMO*, dan *WhatsApp*. Aplikasi tersebut adalah 4 dari 13 aplikasi IM *Android*

terpopuler di Indonesia [3] yang sudah lebih dari 500 juta kali diunduh di *Play Store*, selain itu *WhatsApp* dan *Telegram* adalah aplikasi yang banyak digunakan teroris untuk berkomunikasi. Penelitian ini bertujuan untuk menginvestigasi bukti digital dari keempat aplikasi tersebut melalui simulasi dari beberapa skenario yang mencakup skenario pemakaian fitur-fitur aplikasi IM yang sering digunakan, serta skenario yang dapat menghilangkan bukti digital. Bukti digital dan perubahan yang disebabkan oleh aktivitas yang dilakukan pada skenario tersebut, dianalisa dan disimpulkan ke bentuk tabel. Proses analisa dilakukan untuk menyimpulkan karakteristik bukti digital dari masing-masing aplikasi IM yang diteliti. Penelitian ini hanya fokus terhadap *smartphone* yang memiliki sistem operasi *Android*, karena *Android* adalah sistem operasi *smartphone* yang paling populer di tahun 2017 [4].

II. TINJAUAN PUSTAKA

A. *Analisis*

Definisi kata analisis menurut Kamus Besar Bahasa Indonesia (KBBI), yaitu penyelidikan terhadap suatu peristiwa untuk mengetahui keadaan yang sebenarnya. Analisis dalam penelitian ini berarti menyelidiki bukti digital aplikasi IM yang ditemukan berdasarkan simulasi dari beberapa skenario sehingga dapat diketahui karakteristiknya.

B. *Forensik Digital*

Forensik digital (*digital forensics*) adalah salah satu cabang ilmu forensik yang berkaitan dengan bukti legal yang ditemui pada perangkat digital. Forensik digital adalah bidang ilmu yang menggabungkan bidang keilmuan komputer dengan hukum. Definisi forensik digital adalah aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk kepentingan pembuktian hukum, yang dalam hal ini adalah untuk membuktikan kejahahatan yang menggunakan perangkat komputer atau computer crime, sehingga bisa mendapatkan bukti - bukti digital yang dapat digunakan untuk menjerat pelaku kejahatan tersebut [5].

Forensik digital dilakukan dengan tujuan untuk mendapatkan bukti digital yang relevan dalam kasus hukum. Bukti digital adalah informasi yang tersimpan dalam bentuk digital yang bisa dijadikan bukti di ranah hukum. Manfaat forensik digital adalah sebagai berikut:

1. Keperluan mendapatkan bukti pendukung berbentuk digital dalam tindakan kriminal dan perkara pelanggaran hukum.
2. Rekonstruksi insiden keamanan sistem komputer.
3. Sebagai upaya pencarian keputusan yang tepat untuk pemulihan akibat kerusakan sistem.
4. *Troubleshooting* sistem komputer yang melibatkan *hardware* ataupun *software*.
5. Keperluan untuk memahami sistem komputer ataupun perangkat digital lainnya dengan lebih baik.

Forensik digital memiliki beberapa jenis yang dikategorikan oleh perangkat atau media yang diinvestigasi, salah satunya yang digunakan pada penelitian ini adalah *mobile device forensics*. Forensik perangkat *mobile* adalah metodologi ilmiah dengan tujuan mengekstrak bukti digital yang ada pada perangkat *mobile* dalam konteks hukum. Mengekstrak bukti digital berarti memulihkan, mengumpulkan, dan menganalisis data yang disimpan di dalam memori perangkat *mobile*. Forensik *mobile* adalah ilmu yang terus berkembang yang menghadirkan tantangan bagi komunitas forensik dan penegak hukum karena perkembangan teknologi *mobile* yang sangat cepat [6].

C. *Instant Messenger*

Instant Messenger (pesan instan) atau sering disebut "IM" adalah suatu aplikasi pengiriman pesan secara *real-time* melalui perantara jaringan internet dari suatu perangkat digital ke perangkat digital lainnya.

Pengguna IM di Indonesia cukup banyak, umumnya mayoritas pengguna berasal dari kaum pelajar dan mahasiswa. Hasil survey pada tahun 2017 yang dilakukan Kementrian Komunikasi dan Informatika Republik Indonesia menyebutkan bahwa 84.76% responden adalah pengguna aktif aplikasi *Instant Messenger*. Aplikasi IM yang paling diminati oleh responden adalah aplikasi *WhatsApp* [7].

D. *Android Operating System*

Android adalah sistem operasi dengan sumber terbuka atau *open source* yang dirilis perusahaan *Google* di bawah lisensi *Apache*. Sifat sistem operasi *Android* yang *open source* memungkinkan sistem operasi ini untuk dimodifikasi dan didistribusikan secara bebas oleh para pengembang *smartphone*, operator nirkabel, dan pengembang aplikasi. *Android* memiliki sejumlah besar komunitas pengembang aplikasi (*apps*) yang memperluas fungsionalitas perangkat, umumnya ditulis dalam bahasa pemrograman *Java* dan *Kotlin*. Pengguna aktif perangkat *Android* mencapai total lebih dari 2 milyar di seluruh dunia pada bulan Mei 2017 [8].

E. *Penelitian Terkait*

Penelitian yang membahas proses investigasi forensik untuk mencari bukti digital pada aplikasi *Instant Messenger* telah dilakukan, seperti penelitian [9] yang menjelaskan tentang langkah-langkah untuk memperoleh data aplikasi *WhatsApp* yang dienkripsi menjadi data yang bisa dibaca dan dianalisis untuk kemudian dijadikan sebagai barang bukti. Penelitian serupa telah dilakukan terhadap aplikasi *Line* dalam [10], yang fokus kepada bukti digital yang ditemukan saat melakukan *chatting* mode normal dan *chatting* menggunakan fitur *private chat* milik *Line*. Penggunaan skenario untuk melakukan analisa forensik telah dilakukan pada aplikasi *WhatsApp* dan *Telegram* dalam [11] dan [12] yang merekonstruksi daftar kontak dan pesan, serta menjelaskannya dengan informasi yang ada pada berkas log. Penelitian [13] menganalisa forensik digital aplikasi *Telegram* pada Android yang menggunakan tahapan identifikasi, *preserving*, analisa, dan presentasi/laporan. Bukti digital yang dicari adalah aktivitas aplikasi dan pengguna, informasi kontak, perpesanan, berkas *media*, data yang dihapus. Hasil analisis yang dilakukan memberikan informasi bagaimana merekonstruksi dan memberikan penjelasan terhadap pesan yang dikirim oleh pengguna pada aplikasi *Telegram*. Penelitian forensik digital aplikasi IM tidak terbatas hanya pada proses investigasi bukti digital, tetapi telah dilakukan dalam bentuk perbandingan bukti digital aplikasi IM pada *iOS* dan *Android*. Penelitian tersebut dilakukan dengan menggunakan fitur *Logical Extraction Analysis* dan *Filesystem Extraction Analysis* via aplikasi UFED untuk mencari bukti digital dari masing-masing aplikasi [14]. Perbandingan juga dilakukan pada *tool* atau *software* yang dapat digunakan untuk menginvestigasi forensik aplikasi *WhatsApp*, yang menyatakan bahwa *Belkasoft* adalah *sofware* yang paling efektif untuk melakukan investigasi forensik aplikasi *WhatsApp* [15].

III. METODOLOGI PENELITIAN

A. *Pembuatan Skenario untuk Aplikasi*

Skenario dibuat untuk merekontruksi aksi relevan yang mungkin pengguna lakukan dalam tindakan kriminal dan menyembunyikan jejaknya. Pembuatan skenario dilakukan berdasarkan hasil analisa fungsionalitas aplikasi serta referensi dari situs berita nasional dan internasional tentang bagaimana tindakan kriminal melalui aplikasi IM dilakukan. Skenario mencakup fitur-fitur aplikasi IM yang berpotensi digunakan untuk tindakan kriminal dan aksi yang bisa dilakukan pengguna untuk menyembunyikan jejak dari tindakan kriminal, yaitu:

1. Tukar menukar pesan dengan satu kontak
2. Tukar menukar pesan dengan grup
3. Mengirim dan menerima *geo-location* melalui *Google Maps*
4. Kirim berkas media seperti gambar, video dan suara
5. Menggunakan fitur *secret chat*
6. Melakukan *voice call* dan *video call*
7. Menghapus kontak
8. *Block* kontak
9. Menghapus riwayat pesan
10. Menghapus riwayat panggilan
11. *Retract* pesan
12. *Uninstall* aplikasi.

Skenario tersebut dilakukan ke setiap aplikasi IM yang diteliti untuk menjalankan fitur-fitur yang dimiliki oleh aplikasi sehingga dapat diketahui apakah bukti digital dari penggunaan fitur tersebut dapat ditemukan dan diketahui karakteristiknya. Beberapa dari skenario diatas adalah aktivitas yang dapat merubah bukti digital, sehingga yang dianalisa adalah perubahan yang disebabkan oleh aktivitas tersebut pada bukti digital terkait.

B. *Proses Forensik*

Proses forensik dilakukan mengikuti *guidelines* forensik *mobile National Institute of Standards and Technology* (NIST) [16]. Tahapannya terdiri dari:

1. *Preservation*, yaitu proses mengamankan *smartphone* yang akan diinvestigasi agar data tidak berubah sebelum dianalisa
2. *Collection*, yaitu proses akuisisi data yang dilakukan menggunakan metode *physical acquisition*, selain itu log jaringan juga akan diakuisisi menggunakan metode *live acquisition* dengan menggunakan *Shark for Root* yang terpasang pada *smartphone* untuk menangkap paket lalu lintas jaringan. Langkah-langkah yang digunakan untuk mengakuisisi *physical image smartphone* adalah:
   a) Memastikan *smartphone* sudah dalam keadaan *rooted* agar dapat menggunakan perintah dd (*data dump).*
   b) Menghubungkan *smartphone* dengan laptop menggunakan kabel data USB. S*martphone* telah mengizinkan USB *debugging*.
   c) *Forward* tcp adb ke *port* yang tidak sedang digunakan.

d) Menggunakan perintah "**adb –d shell**" untuk membuka *session* agar dapat berinteraksi dengan *smartphone*.

e) Menggunakan perintah "**su**" untuk mendapatkan hak akses *root* ke *smartphone*.

f) Menggunakan *data dump* untuk melakukan *imaging*, dengan perintah "**dd if=/dev/block/mmcblk0 | busybox nc –l –p 9876**". Perintah tersebut bermaksud untuk melakukan *data dump* dari partisi "mmcblk0" via *Netcat* yang ada di *Busybox* melalui *port* 9876.

g) Membuka *command prompt* baru pada folder yang terdapat "netcat.exe", dan menggunakan perintah "**netcat.exe 127.0.0.1 9876 > deviceImage.dd**". Perintah tersebut dilakukan untuk menerima data yang datang melalui *port* 9876 via *Netcat* dan disimpan dengan nama "deviceImage.dd".

3. *Examination*, yaitu proses pemeriksaan terhadap *physical image smartphone* menggunakan aplikasi *FTK Imager*. *Physical image smartphone* diberi *hash Message Digest* 5 (MD5) sebelum diperiksa untuk menjaga integritas data.

4. *Analysis*, yaitu proses analisa bukti digital yang ditemukan pada tahap *examination* untuk membuat kesimpulan dari bukti digital tersebut. *Network traffic* juga dianalisa untuk mendukung bukti digital yang ditemukan dari masing-masing aplikasi *Instant Messenger*. *Database* aplikasi *Instant Messenger* yang relevan akan dibuka dan diperiksa menggunakan *DB Browser for SQLite*.

5. *Report*, yaitu proses pelaporan dimana investigator melaporkan hasil beserta prosedur investigasi yang dilakukan ke pihak yang bersangkutan. Pelaporan dalam penelitian ini adalah perbandingan dari bukti digital yang telah disimpulkan dari tahap analisis.

C. *Hardware dan Software yang Digunakan*

Perangkat keras dan perangkat lunak yang digunakan dalam penelitian ini bisa dilihat dalam Tabel 1 dan Tabel 2. Perangkat lunak yang digunakan dalam penelitian ini bersifat tidak berbayar.

Tabel 1. Hardware yang Digunakan

No.	Hardware	Kegunaan
1	Laptop	Komputer untuk keperluan investigasi
2	Samsung Galaxy Tab 3 T111	*Smartphone* yang akan diinvestigasi
3	Kabel data	Penghubung antara laptop dan *smartphone* untuk akuisisi data

Tabel 2. Software yang Digunakan

No.	Software	Kegunaan
1	*Kingoroot*	Aplikasi untuk *root smartphone*
2	*WhatsApp* versi 2.18.142	Aplikasi *Instant Messenger* yang akan diinvestigasi dan dibandingkan
3	*Telegram* versi 4.8.7	
4	*Line versi 8.6.1*	
5	*IMO versi 9.8.000000010121*	
6	*DB Browser for SQLite*	Aplikasi untuk membuka *database SQLite*
7	*FTK Imager*	Aplikasi untuk membuka berkas *image smartphone* dan memberikan *hash* untuk menjaga integritas data
8	*Shark for Root*	Aplikasi untuk *live acquisition* lalu lintas data pada jaringan
9	*Hex Editor*	Aplikasi untuk membuka berkas dalam bentuk *binary*

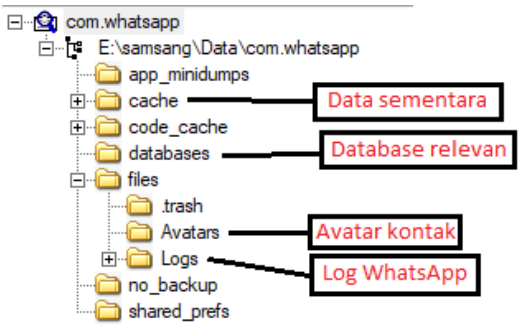
IV. HASIL DAN PEMBAHASAN

A. *Analisis Forensik Aplikasi WhatsApp*

Tabel 3. Lokasi Bukti Digital Aplikasi *WhatsApp*

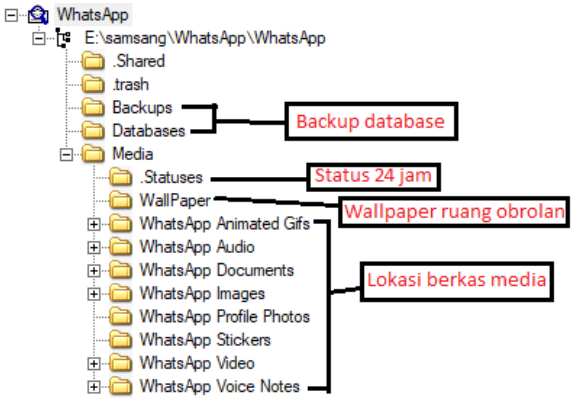
Bukti Digital	Lokasi
Riwayat pesan	/data/data/com.whatsapp/databases/msgstore.db
Riwayat panggilan	/data/data/com.whatsapp/databases/msgstore.db
Kontak	/data/data/com.whatsapp/databases/wa.db
Berkas media	/sdcard/WhatsApp/Media

Lokasi bukti digital dari aplikasi *WhatsApp* dapat dilihat pada Tabel 3. *WhatsApp* memiliki dua direktori yang relevan terhadap investigasi untuk mencari bukti digital. Direktori tersebut adalah "data/data/com.whatsapp/" dan "/sdcard/WhatsApp/". Struktur direktori "com.whatsapp" dapat dilihat pada Gambar 1, dan struktur direktori "WhatsApp" dapat dilihat pada Gambar 2.



Gambar 1. Struktur Direktori com.whatsapp

Direktori "com.whatsapp" hanya bisa ditemukan pada *smartphone* yang telah di *root*. Direktori ini menyimpan *database* yang digunakan oleh *WhatsApp* pada direktori "databases". *WhatsApp* memiliki dua *database* yang relevan untuk investigasi, yaitu "wa.db" dan "msgstore.db". *WhatsApp* menyimpan foto profil pengguna di dalam direktori "files", sedangkan foto profil kontak disimpan di direktori "files/Avatars" dengan ekstensi berkas ".j", yang bisa dibuka dengan aplikasi pembuka gambar. *WhatsApp* menyimpan data sementara pada direktori "cache" yang mungkin bisa membantu investigasi seperti foto profil kontak yang terakhir dilihat.



Gambar 2. Struktur Direktori WhatsApp

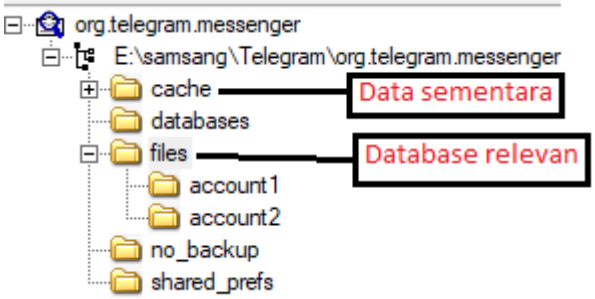
Direktori "WhatsApp" dapat ditemukan pada direktori "sdcard/". Direktori tersebut menyimpan *backup* akun *WhatsApp* yang dienkrip menggunakan "crypt12", dan hanya bisa dibuka jika memiliki *encryption key* yang dapat ditemukan pada direktori "com.whatsapp/files/". Berkas media yang dikirim lewat *WhatsApp* seperti gambar, suara, dan video disimpan pada direktori "WhatsApp/media/".

B. Analisis Forensik Aplikasi Telegram

Tabel 4. Lokasi Bukti Digital Aplikasi *Telegram*

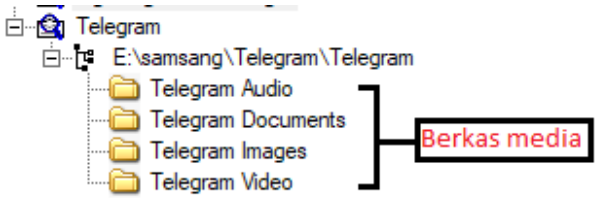
Bukti Digital	Lokasi
Riwayat pesan	/data/data/org.telegram.messenger /files/cache4.db
Riwayat panggilan	/data/data/org.telegram.messenger /files/cache4.db
Kontak	/data/data/org.telegram.messenger /files/cache4.db
Berkas media	/sdcard/Telegram/

Lokasi bukti digital dari aplikasi *Telegram* dapat dilihat pada Tabel 4. *Telegram* memiliki dua direktori yang relevan terhadap investigasi untuk mencari bukti digital, yaitu "data/data/org.telegram.messenger/" yang hanya bisa ditemukan jika memiliki hak akses *root* terhadap *smartphone*, dan direktori "sdcard/Telegram" yang dapat ditemukan tanpa memiliki hak akses *root*. Struktur dari kedua direktori tersebut dapat dilihat pada Gambar 3 dan Gambar 4.



Gambar 3. Struktur Direktori org.telegram.messenger

Data sementara yang digunakan *Telegram* ada pada direktori "org.telegram.messenger/cache/". Data yang disimpan disini adalah *thumbnail avatar* kontak, pratinjau media atau dokumen, dan berkas yang dikirim lewat *Secret Chat*. Data relevan terhadap investigasi forensik dapat ditemukan pada *database* "cache4.db".



Gambar 4. Struktur Direktori Telegram

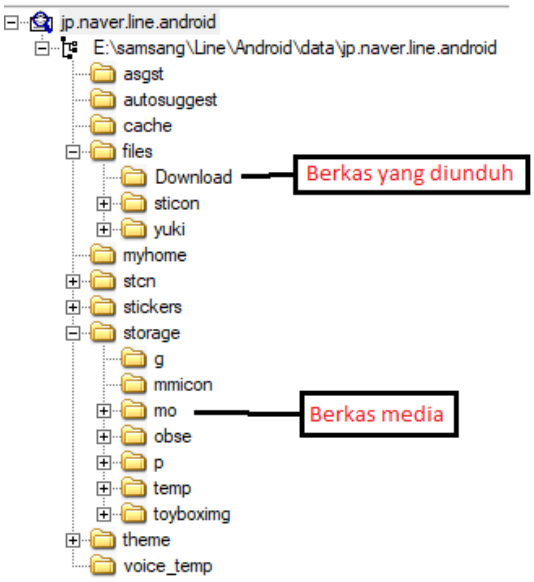
Direktori "sdcard/Telegram/" menyimpan berkas-berkas gambar, suara, video, dan dokumen yang dikirim ataupun diterima melalui aplikasi *Telegram*.

C. *Analisis Forensik Aplikasi LINE*

Tabel 5. Lokasi Bukti Digital Aplikasi *LINE*

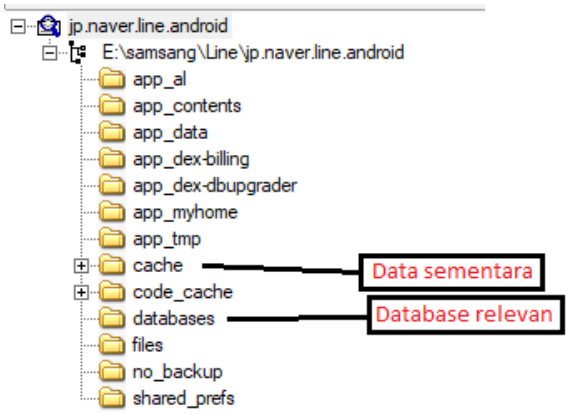
Bukti Digital	Lokasi
Riwayat pesan	/data/data/jp.naver.line.Android/databases/naver_line
Riwayat panggilan	/data/data/jp.naver.line.Android/databases/call_history
Kontak	/data/data/jp.naver.line.Android/databases/naver_line
Berkas media	/sdcard/Android/data/jp.naver.line.Android/storage/mo/

Lokasi bukti digital dari aplikasi *LINE* dapat dilihat pada Tabel 5. Direktori *LINE* yang menyimpan data relevan terhadap investigasi forensik, yaitu direktori "/data/data/jp.naver.line.Android/" dan "/sdcard/Android/data/jp.naver.line.Android/". Strukturnya bisa dilihat pada Gambar 5 dan Gambar 6.



Gambar 5. Struktur Direktori sdcard/…/jp.naver.line.android

LINE menyimpan berkas dokumen atau media seperti gambar, video dan sebagainya pada direktori "jp.naver.line.Android/storage/mo/", sedangkan berkas yang diunduh dapat ditemukan pada direktori "jp.naver.line.Android/files/Download/".



Gambar 6. Struktur Direktori jp.naver.line.android

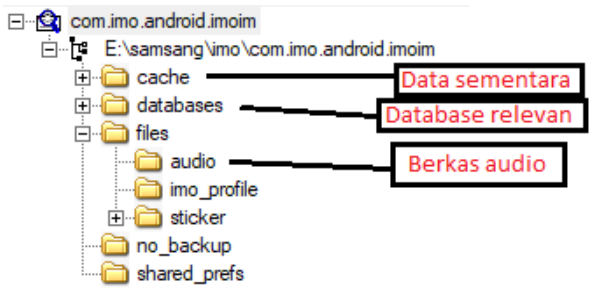
Database yang digunakan aplikasi *LINE* ada pada "/data/data/jp.naver.line.Android/databases/". *LINE* menyimpan data riwayat pesan dan kontak di *database* "naver_line", yang dapat dibuka dengan *DB Browser for SQLite*.

D. *Analisis Forensik Aplikasi IMO*

Tabel 6. Lokasi Bukti Digital Aplikasi *IMO*

Bukti Digital	Lokasi
Riwayat pesan	/data/data/com.imo.Android.imoim/databases/imofriends.db
Riwayat panggilan	/data/data/com.imo.Android.imoim/databases/imofriends.db
Kontak	/data/data/com.imo.Android.imoim/databases/imofriends.db
Berkas media	/sdcard/IMO/

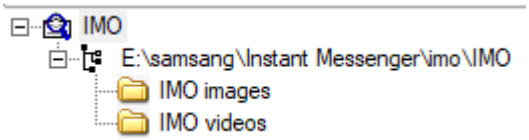
Lokasi bukti digital dari aplikasi *IMO* dapat dilihat pada Tabel 6. Direktori *IMO* yang relevan terhadap investigasi forensik, yaitu "/data/data/com.imo.Android.imoim/" yang hanya bisa ditemukan jika memiliki hak akses *root* dan "/sdcard/IMO". Struktur direktorinya dapat dilihat pada Gambar 7 dan Gambar 8.



Gambar 7. Struktur Direktori com.imo.android.imoim

Direktori data sementara atau *cache* menyimpan foto profil pengguna dengan ekstensi ".webp" yang dapat dibuka melalui *web browser*. *IMO* menyimpan

gambar yang terakhir dibuka dengan ekstensi ".0", yang dapat dibuka menggunakan *VLC Media Player*. Gambar tersebut disimpan *IMO* pada direktori "/cache/". *Database* yang digunakan *IMO* disimpan pada direktori "/databases/". *Database* utama *IMO* yang menyimpan riwayat pesan, riwayat panggilan, dan kontak adalah "imofriends.db".

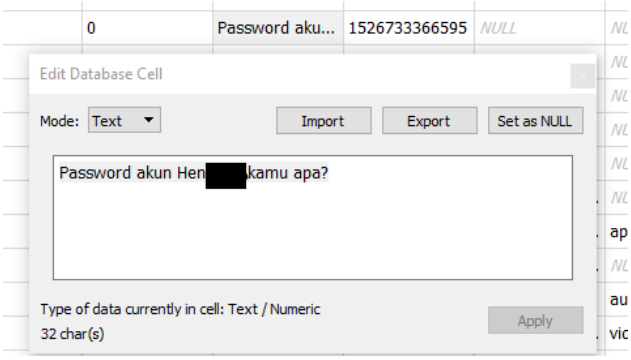


Gambar 8. Struktur Direktori IMO

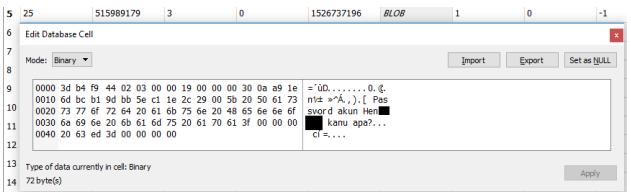
IMO menyimpan berkas media yang diterima atau dikirim lewat aplikasi pada direktori "sdcard/IMO".

E. Analisa dan Perbandingan Bukti Digital Berdasarkan Skenario

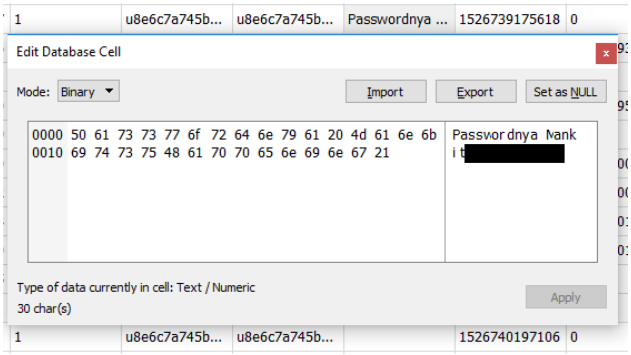
Skenario 1: Skenario tukar menukar tukar menukar pesan dengan satu kontak dilakukan dengan isi pesan "Password akun Hexxxxx kamu apa?" yang dikirim lewat *smartphone* yang diinvestigasi, lalu dibalas oleh lawan kontak yang isi pesannya berisi "Passwordnya ManxxxHapxxx!". Bukti digital pesan dari masing-masing aplikasi IM dapat ditemukan. Bukti digital dapat dilihat pada Gambar 9 untuk *WhatsApp*, Gambar 10 untuk *Telegram*, Gambar 11 untuk *LINE*, dan Gambar 12 untuk *IMO*.



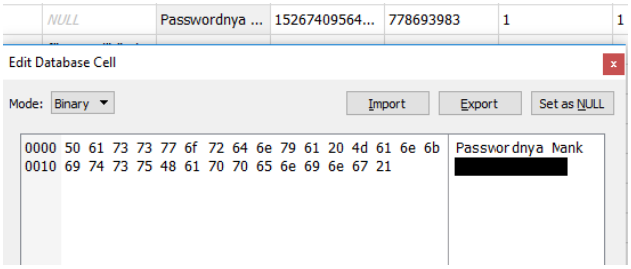
Gambar 9. Bukti Digital Skenario Satu pada *WhatsApp*



Gambar 10. Bukti Digital Skenario Satu pada *Telegram*

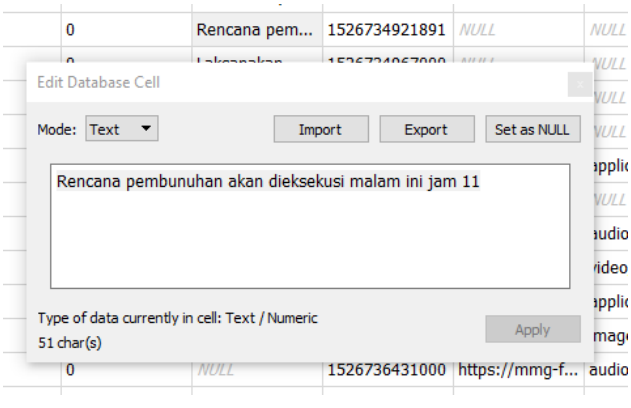


Gambar 11. Bukti Digital Skenario Satu pada *LINE*

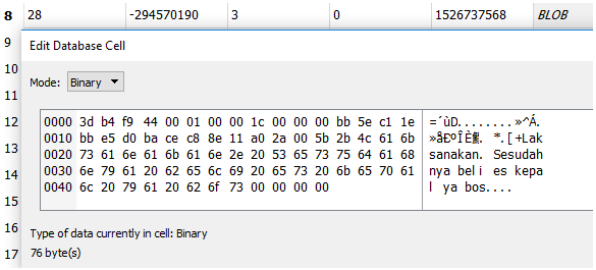


Gambar 12. Bukti Digital Skenario Satu pada *IMO*

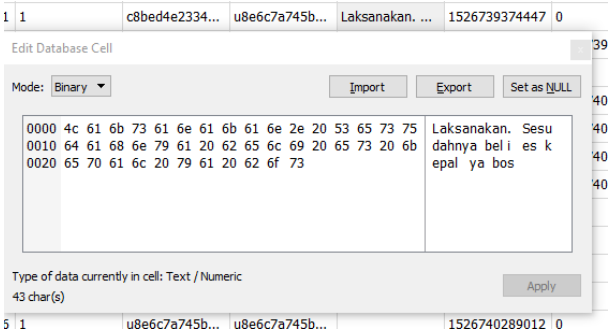
Skenario 2: Skenario tukar menukar pesan dengan grup dilakukan pada grup *Assin* yang akan mengeksekusi rencana pembunuhannya. Pesan berisi "Rencana pembunuhan akan dieksekusi malam ini jam 11" dikirim melalui *smartphone* yang diinvestigasi, lalu dibalas oleh salah satu anggota grup dengan pesan berisi "Laksanakan. Sesudahnya beli es kepal ya bos". Bukti digital dari skenario ini tidak jauh berbeda dengan skenario satu, dan semua bukti digital dari skenario 2 dapat ditemukan. bukti digital dapat dilihat pada Gambar 13 untuk WhatsApp, Gambar 14 untuk Telegram, Gambar 15 untuk LINE, dan Gambar 16 untuk IMO.



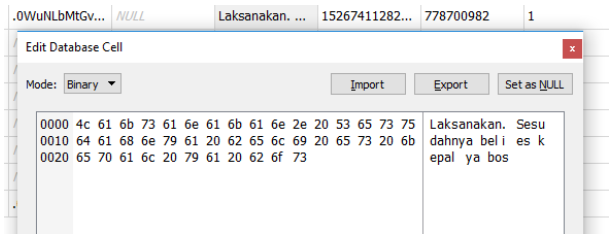
Gambar 13. Bukti Digital Skenario Dua pada *WhatsApp*



Gambar 14. Bukti Digital Skenario Dua pada *Telegram*

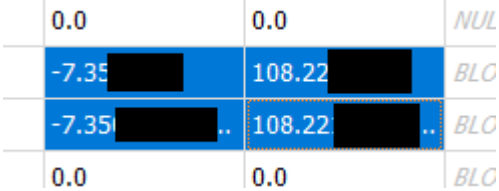


Gambar 15. Bukti Digital Skenario Dua pada *LINE*

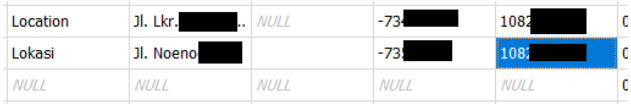


Gambar 16. Bukti Digital Skenario Dua pada *IMO*

Skenario 3: Skenario mengirim dan menerima *geo-location* melalui *Google Maps* dikirim melalui *smartphone* yang diinvestigasi dan lawan obrolan. Skenario ini hanya dilakukan terhadap *WhatsApp*, *Telegram*, dan *Line*, karena *IMO* tidak memiliki fitur *share location*. Bukti digital yang ditemukan pada aplikasi *WhatsApp* berbentuk *latitude* dan *longitude* lokasi yang dibagikan, sedangkan bukti digital yang ditemukan pada *LINE* adalah *latitude* dan *longitude* dilengkapi dengan alamat. Bukti digital dari fitur *share location* tidak ditemukan untuk aplikasi *Telegram*. Bukti digital dapat dilihat pada Gambar 17 untuk *WhatsApp* dan Gambar 18 untuk *LINE*.



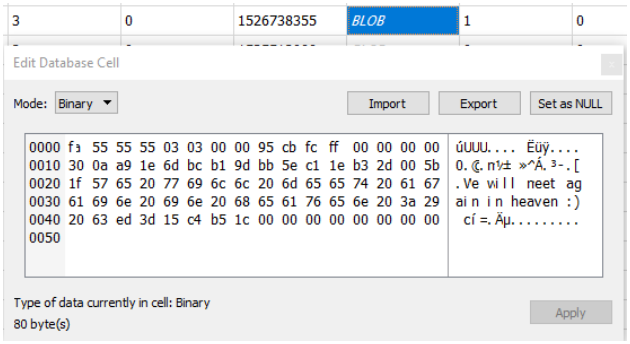
Gambar 17. Bukti Digital Skenario Tiga pada *WhatsApp*



Gambar 18. Bukti Digital Skenario Tiga pada *LINE*

Skenario 4: Skenario kirim dan menerima berkas media dibagi menjadi 4 media, yaitu dokumen (.pdf), rekaman video, gambar, dan rekaman suara. Skenario pengiriman berkas dokumen tidak dilakukan pada aplikasi *IMO*, karena aplikasi *IMO* tidak memiliki fitur kirim berkas dokumen. Hasil dari simulasi skenario empat adalah semua berkas media yang diterima dan dikirimkan ditemukan pada masing-masing direktori aplikasi IM yang menyimpan data media terkait, sedangkan berkas gambar dan dokumen yang dikirim ada pada direktori sumbernya.

Skenario 5: Skenario mengirim pesan dengan fitur *Secret Chat* hanya dilakukan pada aplikasi *Telegram* karena aplikasi IM lain yang dianalisis tidak memiliki fitur yang setara dengan fitur *Secret Chat* milik *Telegram*. Isi pesan yang dikirim lewat *smartphone* yang diinvestigasi adalah "*We will meet again in heaven* :)" dan mengirimkan berkas gambar. Bukti digital dari fitur *Secret Chat* dapat ditemukan di tempat yang sama dengan pesan mode normal. Pesan yang menggunakan fitur *Secret Chat* pada *Telegram* dapat diberikan waktu penghancur otomatis, sehingga pesan dapat hilang dari *smartphone* pengirim dan penerima setelah waktu yang diberikan habis. Bukti digital dari pesan atau berkas media yang hilang setelah waktu penghancuran otomatis habis tidak ditemukan. Bukti digital dari pesan mode *Secret Chat* jika sempat terakuisisi dapat dilihat pada Gambar 19.

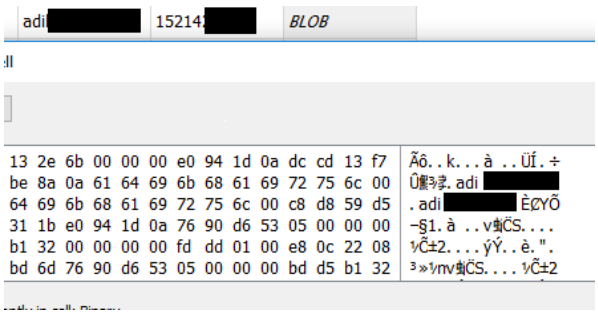


Gambar 19. Bukti Digital Skenario Lima pada *Telegram*

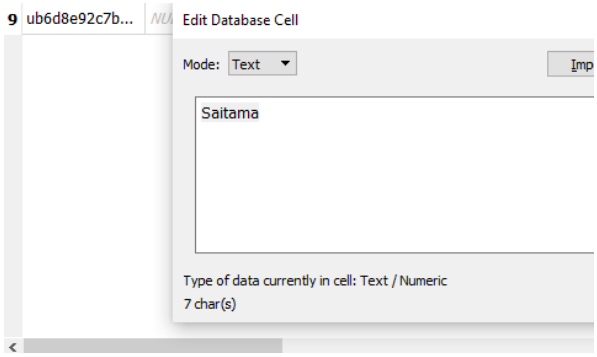
Skenario 6: Skenario melakukan *voice call* dan *video call* dilakukan melalui *smartphone* yang akan diinvestigasi ke kontak lain. Durasi panggilan dilakukan selama 5 detik. Bukti digital dari skenario ini dapat ditemukan dari setiap aplikasi IM. Lokasi bukti digital dapat dilihat pada *database* yang sama dengan *database* yang menyimpan data pesan untuk

aplikasi *WhatsApp*, *Telegram*, dan *IMO*, sedangkan bukti digital skenario enam dapat ditemukan pada *database* "call_history" untuk aplikasi *LINE*.

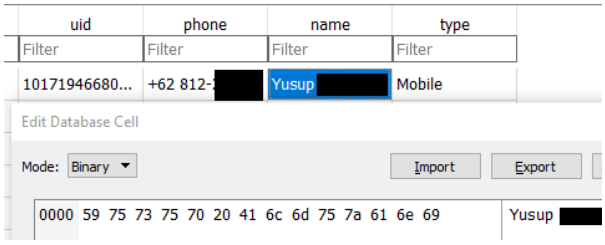
Skenario 7: Skenario menghapus kontak dilakukan dengan menghapus salah satu kontak yang ada. Kontak yang dihapus bernama "Saitama" untuk *WhatsApp* dan *Line*. Kontak yang dihapus bernama "Yusup" untuk *IMO*. Kontak yang dihapus bernama "Adi" untuk *Telegram*. Semua kontak masih terdapat pada masing-masing *database* aplikasi IM yang menyimpan data kontak, meskipun telah dihapus. Kontak *WhatsApp* yang dihapus hanya akan menyisakan *jid* (id pengguna *WhatsApp*) tanpa dilengkapi data nama kontak. Data kontak *Telegram*, *LINE*, dan *IMO* yang dihapus masih utuh informasinya seperti yang bisa dilihat pada Gambar 20 untuk Telegram, Gambar 21 untuk LINE, dan Gambar 22 untuk IMO.



Gambar 20. Bukti Digital Skenario Tujuh pada *Telegram*

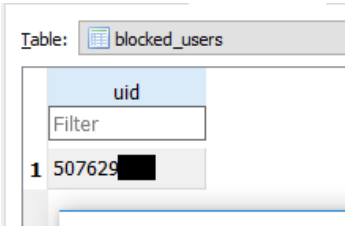


Gambar 21. Bukti Digital Skenario Tujuh pada *LINE*

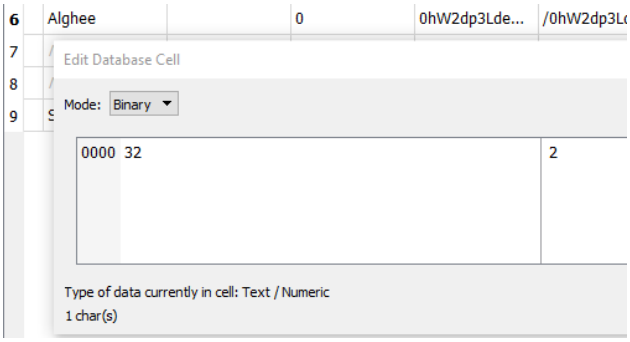


Gambar 22. Bukti Digital Skenario Tujuh pada *IMO*

Skenario 8: Skenario blokir kontak dilakukan dengan memblokir salah satu kontak yang ada. Kontak yang diblokir bernama "Alghee" untuk *WhatsApp* dan *Line*. Kontak yang diblokir bernama "Sidik" untuk *IMO*. Kontak yang diblokir bernama "Wawang" untuk *Telegram*. Bukti digital yang memberitahukan bahwa kontak diblokir tidak ditemukan pada aplikasi *WhatsApp*, tetapi kontak masih terdaftar pada *database*, sedangkan aplikasi *IMO* menyimpan tanda blokir di *server IMO*, sehingga jika pengguna aplikasi *IMO* sedang offline, tidak akan bisa melihat daftar kontak yang diblokir. Tanda kontak diblokir pada aplikasi *Telegram* adalah kontak terdapat pada tabel "blocked_users" dalam *database* "cache4.db", sedangkan tanda kontak diblokir pada aplikasi LINE adalah kontak yang memiliki nilai "2" pada kolom status. Bukti digital dapat dilihat pada Gambar 23 untuk *Telegram*, dan Gambar 24 untuk *LINE*.



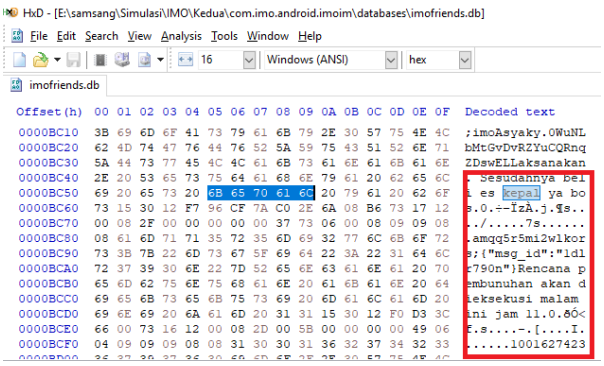
Gambar 23. Bukti Digital Skenario Delapan pada *Telegram*



Gambar 24. Bukti Digital Skenario Delapan pada *LINE*

Skenario 9: Skenario ini menghapus semua riwayat pesan yang dikirim pada skenario dua. Aplikasi *WhatsApp* dan *Telegram* menggunakan *Write-Ahead Logging*, yaitu tempat dimana setiap transaksi database *SQLite* disimpan terlebih dahulu sebelum di-*commit* ke *database* utama, sehingga ketika pesan dihapus, pesan masih berada pada *database* utama. Jika transaksi hapus telah di-*commit* ke *database* utama, maka pesan yang dihapus pada *WhatsApp* dan *Telegram* tidak akan dapat ditemukan. Pesan yang dihapus akan tetap berada pada *database* jika *database* belum *vacuum*. *Vacuum* adalah proses membangun ulang *database* sehingga ruang kosong

pada *database* dapat digunakan kembali. Jika *database* belum *vacuum*, maka pesan yang dihapus dapat dilihat melalui *hex editor* seperti Gambar 25 yang membuka database *IMO* dengan aplikasi *HxD*.

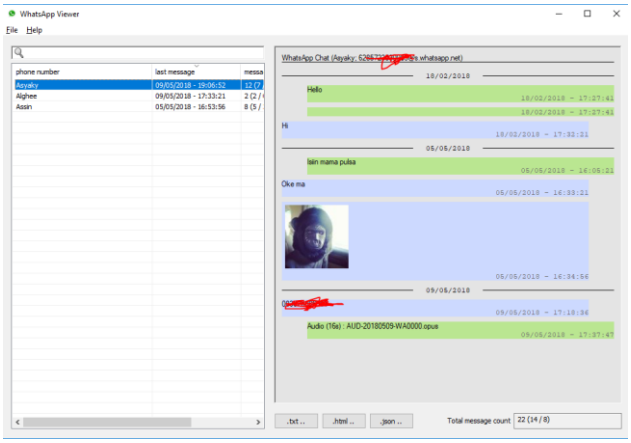


Gambar 25. Pesan pada aplikasi *IMO* yang dihapus

Skenario 10: Skenario ini menghapus riwayat panggilan. Hasil dari aktivitas penghapusan riwayat panggilan sama dengan aktivitas menghapus pesan. Riwayat panggilan yang dihapus dapat ditemukan pada *WhatsApp* dan *Telegram* jika belum di-*commit* ke *database* utama. Riwayat panggilan yang dihapus pada LINE masih ada pada *database* "call_history".

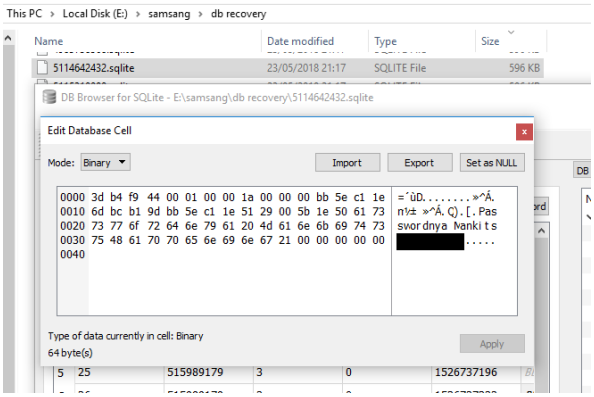
Skenario 11: Skenario ini me-*retract* atau menarik pesan dan berkas media yang telah terkirim. Skenario ini hanya dilakukan pada aplikasi *WhatsApp*, *Telegram*, dan *LINE*, karena *IMO* tidak memiliki fitur tarik pesan. Pesan yang ditarik setelah terkirim pada aplikasi *WhatsApp* dan *Telegram* tidak ditemukan karena pesan yang dikirim belum tersimpan pada *database* utama. Ketika pesan ditarik, pesan tersebut masih ada di berkas *Write-Ahead Logging*, sehingga jika berkas WAL tersebut dibuka dengan *hex editor* atau *tool database forensic* maka akan ditemukan. Berkas media yang di-*retract* akan hilang dari perangkat penerima, tetapi berkas media dapat ditemukan dengan teknik *data carving* atau *recovery*.

Skenario 12: Skenario *uninstall* aplikasi dilakukan untuk memastikan data apa saja yang masih tersimpan pada *smartphone* setelah aplikasi *Intant Messenger* dicabut dari *smartphone*. Keempat aplikasi IM yang dicabut instalasinya hanya meninggalkan berkas media yang diterima melalui aplikasi tersebut, kecuali *WhatsApp* yang menyimpan *backup database* yang dienkrip menggunakan "crypt12" pada direktori "sdcard/WhatsApp". *Database* tersebut dapat dibuka melalui *tool WhatsApp Viewer* dengan mendekrip *database* menggunakan *key* yang ada pada direktori "com.whatsapp/files/". Berkas *key* tersebut akan hilang ketika aplikasi *WhatsApp* dicabut, tetapi jika berkas *key* tersebut berhasil di-*recover*, maka *database* dapat didekrip. *Database WhatsApp* yang dibuka melalui *tool WhatsApp Viewer* dapat dilihat pada Gambar 26.



Gambar 26. Membuka *backup database* dengan *WhatsApp Viewer*

Database yang terhapus memiliki kemungkinan untuk di-*recover* jika waktu penghapusan *database* tersebut belum lama. *DiskDigger* adalah salah satu aplikasi yang dapat digunakan untuk me-*recover* berkas *database*, untuk lebih jelasnya dapat dilihat pada Gambar 27 yang menunjukan *database Telegram* yang berhasil di-*recover* dengan nama "5114642432.sqlite" dan dibuka melalui aplikasi *DB Browser for SQLite*.



Gambar 27. *Database Recovery*

Kesimpulan dan perbandingan dari bukti digital yang didapatkan berdasarkan skenario yang dilakukan, dapat dilihat pada Tabel 7. Bukti digital skenario 1 sampai skenario 6 dilengkapi dengan data identitas pengirim, *Unix epoch timestamp*, dan data lainnya yang mendukung bukti digital pada tabel yang bersangkutan. Skenario 7 sampai skenario 12 adalah aktivitas yang dapat menghilangkan bukti digital, sehingga yang menentukan apakah bukti digital ditemukan atau tidak ditemukan pada Tabel 7 adalah ketersediaan bukti digital yang bersangkutan setelah usaha *recovery* atau *data carving* dilakukan.

Tabel 7. Kesimpulan dan Perbandingan Bukti Digital Berdasarkan Skenario

Bukti digital skenario	Instant Messenger			
	WhatsApp	Telegram	LINE	IMO
1	✓	✓	✓	✓
2	✓	✓	✓	✓
3	✓	×	✓	-
4	✓	✓	✓	✓
5	-	✓	-	-
6	✓	✓	✓	✓
7	✓	✓	✓	✓
8	×	✓	✓	×
9	✓	✓	×	✓
10	✓	✓	✓	✓
11	✓	✓	×	-
12	✓	✓	✓	✓

Keterangan :

✓ : Ditemukan

× : Tidak ditemukan

- : Skenario tidak dilakukan

F. Investigasi Network Forensics

Hasil investigasi forensik jaringan yang dilakukan ke aplikasi IM tidak mendapatkan data yang relevan untuk dijadikan bukti digital, namun setidaknya mendapatkan informasi mengenai *IP address server* dan protokol komunikasi yang digunakan masing-masing aplikasi IM saat simulasi dilakukan. Hasil investigasi dapat dilihat pada Tabel 8.

Tabel 8. Hasil Investigasi *Network Forensics*

Aplikasi	**Protokol Komunikasi**	***IP address server***
WhatsApp	SSL	169.47.40.154
Telegram	SSL	91.108.56.160
LINE	TLSv1.2	203.104.174.19
IMO	SSL	192.12.31.103

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Hasil analisa bukti digital yang dilakukan berdasarkan 12 skenario telah disimpulkan dalam Tabel 7. Investigator forensik akan mengalami kesulitan ketika pengguna aplikasi dapat melakukan aksi seperti skenario 9 dan 11, karena riwayat pesan dan panggilan yang dihapus memiliki potensi yang kecil untuk bisa dipulihkan, sehingga aktivitas pada skenario 11 adalah cara yang ampuh untuk tidak meninggalkan bukti digital saat melakukan komunikasi yang mengandung unsur kriminal. Aplikasi *LINE* adalah aplikasi yang paling baik dalam menjaga privasi obrolan dan melindungi data dari investigator forensik, karena pesan atau panggilan yang dihapus pada *LINE* tidak memiliki kemungkinan untuk dipulihkan kembali. *LINE* juga menggunakan enkripsi *end-to-end* pada komunikasi antara *smartphone* dengan *server* seperti yang bisa dilihat pada Tabel 8.

B. Saran

Penelitian selanjutnya, dapat difokuskan ke fitur lainnya yang ada pada aplikasi IM. Penelitian serupa dapat dilakukan ke sistem operasi selain *Android*, karena setiap sistem operasi memiliki struktur yang berbeda sehingga teknik akuisisi data yang digunakan pada penelitian ini tidak akan bekerja.

REFERENSI

[1] HubSpot, "Messaging apps have over 5B monthly active users," 2017. [Online]. Available: https://research.hubspot.com/charts/messaging-apps-have-over-4b-monthly-active-users. [Accessed: 14-Feb-2018].

[2] T. Micro, "Dark Motives Online," 2016. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/overlapping-technologies-cybercriminals-and-terrorist-organizations. [Accessed: 14-Feb-1018].

[3] A. Mushanif, "Top 13 Aplikasi Chat Android Terbaik Yang Banyak Digunakan," 2017. [Online]. Available: https://www.yatekno.com/aplikasi-chat-android/. [Accessed: 16-Feb-2018].

[4] M. Broadband, "The most popular operating systems on smartphones," 2017. [Online]. Available: https://mybroadband.co.za/news/software/228981-the-most-popular-operating-systems-on-smartphones-and-pcs.html. [Accessed: 16-Feb-2018].

[5] M. N. Al-Azhar, *Digital Forensic : Panduan Praktis Investigasi Komputer*. Jakarta: Salemba Infotek, 2012.

[6] S. Tahiri, *Mastering Mobile Forensics*. Birmingham: Packt Publishing Ltd, 2016.

[7] D. N. Utami, "Indonesia Hobi Chatting, WhatsApp Nomor Satu," 2018. [Online]. Available: http://gadget.bisnis.com/read/20180212/280/737506/indonesia-hobi-chatting-whatsapp-nomor-satu. [Accessed: 14-Feb-2018].

[8] B. Popper, "Google announces over 2 billion monthly active devices on Android," 2017. [Online]. Available: https://www.theverge.com/2017/5/17/15654454/android-reaches-2-billion-monthly-active-users. [Accessed: 14-Feb-2018].

[9] G. M. Zamroni, R. Umar, and I. Riadi, "Analisis Forensik Aplikasi Instant Messaging Berbasis Android," *Annu. Res. Semin.*, vol. 2, no. 1, pp. 102–105, 2016.

[10] A. Iqbal, H. Alobaidli, A. Almarzooqi, and A. Jones, "LINE IM app Forensic Analysis," *12th Int. Conf. High-capacity Opt. Networks Enabling/Emerging Technol. (HONET-ICT 2015) poster*, no. IM, 2015.

[11] C. Anglano, "Forensic analysis of whats app messenger on Android smartphones," *Digit. Investig.*, vol. 11, no. 3, pp. 201–213, 2014.

[12] C. Anglano, M. Canonico, and M. Guazzone, "Forensic analysis of Telegram Messenger on Android smartphones," *Digit. Investig.*, vol. 23, no. December, pp. 31–49, 2017.

[13] G. B. Satrya, P. T. Daely, and M. A. Nugroho, "Digital forensic analysis of Telegram Messenger on Android devices," *2016 Int. Conf. Inf. Commun. Technol. Syst.*, pp. 1–7, 2016.

[14] C. Sgaras, M. T. Kechadi, and N. A. Le-Khac, "Forensics acquisition and analysis of instant messaging and VoIP applications," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8915, pp. 188–199, 2015.

[15] R. Umar, I. Riadi, and G. Maulana, "A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurements," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 12, 2017.

[16] R. Ayers, W. Jansen, and S. Brothers, "Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1)," *NIST Spec. Publ.*, vol. 1, no. 1, p. 85, 2014.