ANALISIS FORENSIK DIGITAL PADA APLIKASI INSTANT MESSAGING DI SMARTPHONE BERBASIS ANDROID UNTUK BUKTI DIGITAL

Maghvirna Rafika Dhewi Qibriya[1], Awalludiyah Ambarwati[2], Kunto Eko Susilo[3]

[1, 2]*Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Narotama*
[3]*Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Narotama*
[1 2 3] Jl. Arief Rachman Hakim 51, Sukolilo, Surabaya
maghvirna.rafika@gmail.com[1], ambarwati1578@yahoo.com[2],
kunto.eko.susilo@narotama.ac.id[3]

Abstract - Digital forensics is the development of forensic science that is specifically used to uncover digital-based crime cases including cyber crimes. The criminal activity in the cyber world that is troubling many parties is a fraud case launched through an instant messenger application. In this study, an analysis of cyber crime cases will be carried out on the WhatsApp messenger and Telegram messenger applications which are operated on mobile devices with the Android operating system using guidelines from the National Institute of Standards and Technology (NIST) SP 80-100 Rev. 1. Conducting an experiment with variations of normal usage scenarios without any modification and deleting some messages as an indication of anti-forensic measures. Data from each experiment to be acquired using the MOBILedit Forensic Express tool and analyzed with the FTK Imager and Autopsy tools. Based on the results of the analysis, only the WhatsApp messenger application can provide valid digital evidence. The characteristics of the digital proof of WhatsApp based on the message structure are key_remote_jid, key_id, data, timestamp, and recent_timestamp. As for Telegram messenger, it cannot provide digital evidence because it does not find important data in the entire directory of this application. In terms of data security, the WhatsApp messenger application has a higher level of vulnerability because it is considered easy to practice, while the security level of the Telegram messenger application is superior because not much important data is obtained and analyzed. The high level of security also results in complex forensic actions in a crime case
Keywords - Digital Forensic, Mobile Forensic, Instant Messenger, dan NIST..

Abstrak - Digital forensik merupakan pengembangan dari ilmu forensik yang khusus digunakan untuk mengungkap suatu kasus kejahatan berbasis digital termasuk kasus cyber crime (kejahatan siber). Akvititas kriminal di dunia siber yang cukup meresahkan banyak pihak adalah kasus penipuan yang dilancarkan melalui aplikasi instant messenger (pesan instan). Pada penelitian ini akan dilakukan analisa kasus cyber crime pada aplikasi WhatsApp messenger dan Telegram messenger yang dioperasikan pada prangkat mobile dengan sistem operasi android menggunakan guideline dari National Institute of Standards and Technology (NIST) SP 80-100 Rev. 1. Dilakukan sebuah eksperimen dengan variasi skenario penggunaan normal tanpa ada modifikasi apapun dan melakukan penghapusan pada beberapa pesan sebagai indikasi tindakan anti forensik. Data dari setiap eksperimen akan diakuisisi menggunakan tools MOBILedit Forensic Express dan dianalisis dengan tools FTK Imager dan Autopsy. Berdasarkan dari hasil analisa pada kedua aplikasi instant messenger, hanya aplikasi WhatsApp messenger yang dapat memberikan bukti digital yang valid. Karakteristik bukti digital dari WhatsApp berdasarkan dengan struktur pesan adalah key_remote_jid, key_id, data, timestamp, dan received_timestamp. Sedangkan untuk Telegram messenger tidak dapat memberikan bukti digital dikarenakan tidak ditemukannya data penting pada seluruh direktori aplikasi ini. Dari sisi keamaan data aplikasi WhatsApp messenger memiliki tingkat kerentanan lebih tinggi karena kemudahan dalam melakukan praktik forensik, Sedangkan untuk tingkat keamanan pada aplikasi Telegram messenger dinilai lebih unggul karena tidak banyak data penting yang bisa didapat dan dianalisis. Tingkat sekuritas yang tinggi juga berakibat pada rumitnya tindakan forensik dalam pengungkapan sebuah kasus kejahatan.
Kata Kunci - Forensik digital, *Mobile Forensic, Instant Messenger*, dan NIST.

I. PENDAHULUAN

Berkembangnya kemajuan teknologi informasi khususnya pada aspek mayantara tentu memberikan banyak manfaat bagi manusia. Namun, seiring dengan banyaknya kemudahaan yang didapat, angka kejahatan dalam dunia siber juga semakin melambung dengan modus yang bervariasi. Salah satu kejahatan siber yang marak terjadi adalah kasus *fraud* dengan modus penipuan jual beli secara *online*. *Instant messenger* (IM) menjadi salah satu medium yang digunakan para pelaku kejahatan dalam melakukan aksinya. Aplikasi pesan instan yang populer dan banyak digunakan di Indonesia adalah WhatsApp *messenger*. Aplikasi

perpesanan lain terdapat Telegram *messenger*, meskipun pengguna aplikasi ini tidak sebanyak WhatsApp *messenger* tetap tidak menutup kemungkinan bahwa tindak kejahatan tidak dilakukan pada aplikasi ini.

Dari permasalahan yang disebutkan di atas, terdapat sebuah bidang ilmu yang dapat membantu dalam proses pembuktian kasus kejahatan siber yaitu forensik digital. Ilmu forensik digital muncul sebagai solusi untuk memecahkan kejahatan yang memanfaatkan teknologi informasi sebagai alat bantu, sasaran, maupun tempat kejadian [1]. Forensik digital merupakan ilmu yang digunakan untuk kepentingan bukti hukum, yang dalam hal ini adalah membuktikan kejahatan komputer secara ilmiah untuk bisa didapatkan bukti digital yang valid [2].

Dalam sebuah penelitian yang dilakukan oleh Asyaky dimana penelitian ini membandingkan bukti digital yang ditemukan pada 4 aplikasi pesan instan meliputi Telegram, Line, IMO, dan WhatsApp dengan menerapkan 12 skenario. Berdasarkan hasil analisis dapat disimpulkan bahwa 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 lantaran aplikasi ini menggunakan enkripsi end-to-end pada komunikasi antara smartphone dengan server dengan protokol keamanan data TLSv1.2 [3].

Zamroni, Umar, dan Riadi melakukan analisa forensik pada aplikasi pesan *instant messenger* WhatsApp berbasis android dan mendapatkan hasil dengan berhasilnya melakukan ekstraksi artefak percakapan aplikasi ini meskipun percakapan tersebut telah dihapus dari perangkat. Kendala dari penelitian ini adalah sulitnya melakukan tindakan forensik apabila tersangka terindikasi melakukan tindakan anti forensik yaitu mengambil dan menghilangkan penyimpanan eksternal (*memory external*) karena *database* cadangan dari aplikasi WhatsApp *messenger* tersimpan pada penyimpanan tersebut [4].

Pada penelitian ini, penulis akan melakukan forensik digital pada kasus *cybercrime* penipuan *online shop* yang dieksekusi melalui IM WhatsApp dan Telegram pada *smartphone* berbasis android. Penulis menggunakan tools pendukung untuk melakukan ekstraksi dan juga analisis bukti digital. Dari hasil analisis tersebut, diharapkan dapat membantu memberikan informasi mengenai validitas sebuah data digital yang mampu dijadikan sebagai bukti digital yang otentik dan dapat dipertanggung jawabkan di pengadilan.

A. Forensik Digital

Forensik merupakan kegiatan untuk melakukan investigasi dan menetapkan fakta yang berhubungan dengan kejadian kriminal dan permasalahan hukum lainnya. Forensik digital merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi materi (data) yang ditemukan pada perangkat digital (komputer, *handphone, tablet*, PDA (*Personal Digital Assistant), networking devices, storage*, dan sejenisnya) [5].

Dalam pandangan yuridis, digital forensik, merupakan syarat mutlak yang harus dilakukan supaya dokumen elektronik dapat digunakan sebagai alat bukti dari mulai penyelidikan, penyidikan, penuntutan dan persidangan, maupun dalam proses persidangan pidana. Tanpa melalui digital forensik, maka suatu dokumen elektronik tidak dapat digunakan sebagai alat bukti karena tidak dapat dijamin kesahihan dari dokumen elektronik tersebut [6].

B. Bukti Digital

Definisi dari bukti digital adalah informasi elektronik yang dikumpulkan pada saat melakukan investigasi pada sebuah kasus, yang melibatkan perangkat-perangkat digital seperti email, transaksi perbankan *online*, foto, riwayat *web*, maupun audio dan video [7].

C. Mobile Forensic

Mobile Forensic adalah ilmu yang melakukan proses pemulihan bukti digital dari perangkat seluler menggunakan cara yang sesuai dengan kondisi forensik [2].

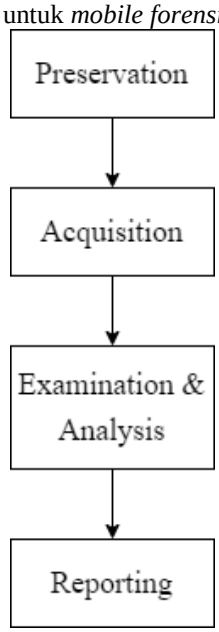
D. Tools Forensik

Dalam praktiknya, para examiner memerlukan alat atau *tools* pendukung untuk membantu seluruh kegiatan forensik agar lebih bukti yang sedang dianalisis mendapat nilai validitas lebih tinggi, dalam penelitian ini tools yang digunakan antara lain:

1. MOBILedit Forensic Express
   MOBILedit merupakan *tool* forensik yang memungkinkan penyidik untuk memperoleh secara logik, mencari dan memeriksa perangkat ponsel. *Tool* ini menggunakan beberapa mekanisme konektivitas terutama konektivitas nirkabel dibandingkan *tool* sejenis. *Software* ini cukup baik digunakan untuk memperoleh informasi sistem telepon dan informasi lainnya seperti daftar kontak dan pesan [8].
2. FTK Imager
   Forensic Toolkit Imager (FTK Imager) merupakan aplikasi *digital forensic* yang dioperasikan saat proses penyidikan menggunakan teknik *live* atau *static* atau bahkan keduanya [9].
3. Autopsy
   Autopsy merupakan platform forensik digital dan antarmuka grafis dari The Sleuth Kit yang memfokuskan upayanya terhadap volume dan sistem *file*. Autopsy menyediakan platform agar *application-layer modules* dapat beroperasi, tanpa khawatir tentang akses *file* dan penyalinan data intermiten [10].

E. Forensic Guideline

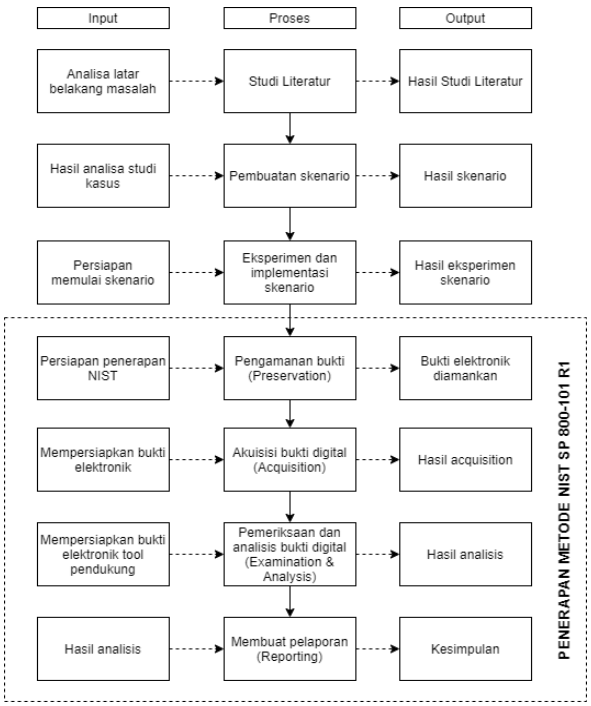
Tahapan penelitian mengacu pada *guideline* yang dirumuskan oleh badan dari Departemen Perdagangan Amerika Serikat yaitu *National Institute of Standards and Technology* (NIST). NIST telah mempublikasikan NIST SP 800-101 R1 yang di dalamnya memuat pedoman khusus untuk *mobile forensic* [11].



Gambar 1. Tahapan Forensik NIST SP 800-101 R1

II. METODE PENELITIAN

Pada Gambar 2 akan dijelaskan mengenai alur penelitan atau langkah-langkah yang dilakukan dalam penelitian ini.



Gambar 2. Metodologi Penelitian.

1. Studi Literatur
   Tahapan awal penelitian adalah menganalisa dan mengkaji informasi atau studi kasus yang terkait dengan digital forensik dari penelitian-penelitan sebelumnya dan juga buku-buku. Selain itu juga dilakukan *research* pada kasus-kasus nyata yang dialami oleh segelintir pihak terkait dengan topik penelitian. Hasil dari *research* tersebut menjadi rujukan penulis dalam merancang skenario pada penelitian ini.
2. Pembuatan Skenario
   Pembuatan skenario percakapan yang bereferensi pada kasus yang sudah terjadi sebelumnya. Skenario percakapan juga termasuk perpesanan media berupa foto, audio dan video. Tokoh yang terlibat pada skenario ini adalah korban (pembeli) dan tersangka (penjual online shop). Skenario yang dilakukan yaitu dengan penggunaan normal dan melakukan modifikasi penghapusan pada beberapa pesan.
3. Eksperimen dan Implementasi Skenario
   Skenario percakapan yang telah dibuat akan dijalankan pada perangkat yang telah disiapkan yaitu *smartphone* dengan merk Samsung Galaxy Galaxy Grand Prime dengan model SM-G530H yang digunakan tersangka dan *smartphone* dengan merk Samsung Galaxy J7 Pro dengan model SM-G730G yang digunakan korban.
4. Pengamanan Bukti
   Bukti yang diamankan adalah bukti elektronik, yaitu barang fisik yang digunakan untuk menjalankan tindak kejahatan. Tujuan dari pengamanan barang bukti elektronik disini adalah untuk menghindari adanya perubahan data atau informasi yang ada dalam bukti elektronik. Pada penelitian ini, bukti elektronik yang diamankan adalah *smartphone* yang digunakan tersangka dalam ekeperimen skenario.
5. Akuisisi Data Digital
   Tindakan akuisisi data pada penelitian ini dengan melakukan *imaging* pada bukti elektronik yang ditemukan. Tindakan *imaging* dibantu dengan tools MoBILEdit Forensic Express. Sebelum melakukan *physical imaging* pada *smartphone* tersangka, perangkat tersebut sudah dalam keadaan *root* agar data yang didapatkan menyeluruh.
6. Analisis Bukti Digital
   Tahap selanjutnya adalah melakukan *examination* dan *analysis* yaitu pemeriksaan terhadap bukti digital yang berhasil diakuisisi untuk selanjutnya dilakukan proses analisis. Pada proses analisis, dibantu menggunakan tool FTK Imager dan Autopsy guna mendapat bukti digital dengan nilai validitas tinggi dan lebih akurat.
7. Laporan
   Tahap terakhir adalah reporting atau pelaporan dari hasil analisis yang sudah dilakukan.

III. HASIL DAN PEMBAHASAN

Dari hasil eksperimen kedua skenario dan akuisisi dari kedua aplikasi *instant messenger*, berikut adalah proses pemeriksanan dan analisis dari penelitian ini:

A. Pemeriksaan Data Digital

Sebelum melakukan analisis, dilakukan pemeriksaan terlebih dahulu terkait ketersediaan data yang berhasil diekstrak pada proses physical imaging dari tool MOBILEdit. Berikut adalah ketersediaan hasil data digital berdasarkan eksperimen dari setiap skenario

1. Hasil Eksperimen Skenario 1

   Eksperimen pertama dijalankan dengan kondisi normal tanpa adanya modifikasi apapun. Informasi mengenai ketersediaan data dari eksperimen skenario 1 terdapat pada Tabel 1.

Tabel 1. Semesta Pembicaraan

Tools	WhatsApp	Telegram
FTK Imager	Data lengkap	Data media
Autopsy	Data lengkap	Data media

Dari tabel 1 di atas diperoleh hasil bahwa untuk aplikasi WhatsApp data yang didapatkan lengkap pada kedua tools, sedangkan untuk aplikasi Telegram data yang berhasil didapatkan hanya data media saja.

2. Hasil Eksperimen Skenario 2

   Eksperimen kedua dijalankan ada penghapusan pada beberapa pesan di kedua aplikasi IM. Informasi mengenai ketersediaan data dari eksperimen skenario 1 terdapat pada Tabel 2.

Tabel 2. Ketersediaan Data

Tools	WhatsApp	Telegram
FTK Imager	Data lengkap	Data media
Autopsy	Data lengkap	Data media

Sesuai dengan tabel 2 di atas bahwa pada scenario 2 juga didapat hasil yang sama layaknya tabel 1 bahwa data pada aplikasi WhatsApp didapatkan lengkap pada kedua tools dan pada aplikasi Telegram hanya didapat data media.

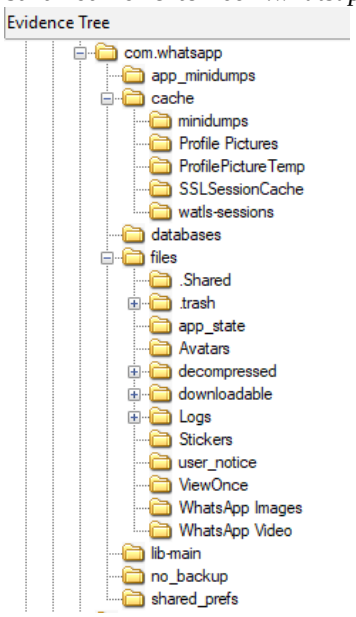
B. Analisis Data Digital

Langkah lanjutan dari pemeriksaan ketersediaan data adalah melakukan analisis data digital yang tersimpan pada kedua aplikasi IM.

1. Lokasi Data WhatsApp

   Aplikasi WhatsApp messenger terdeteksi menyimpan data pada 2 lokasi, direktori tersebut adalah *WhatsApp* dan *com.whatsapp*.

   Pada perangkat bukti elektronik di penelitian ini, direktori WhatsApp tersimpan di *memory internal*, sedangkan untuk direktori *com.whatsapp* terletak di sub-direktori folder data. Data penting yang dijadikan sebagai sumber data analisis pada penelitian terletak pada direktori ini. Berikut adalah susunan dari direktori *com.whatsapp.*



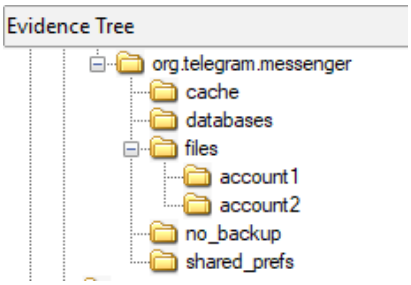
Gambar 3. Struktur Direktori WhatsApp

Berdasarkan pada Gambar 3 di atas, aplikasi WhatsApp memiliki 7 folder utama dan 17 sub-direktori di dalamnya

2. Lokasi Data Telegram

   Sama halnya dengan aplikasi WhatsApp, aplikasi Telegram *messenger* juga terdeteksi menyimpan data pada 2 lokasi dengan nama direktori *Telegram* dan *com.telegram*.

   Direktori *Telegram* tersimpan *memory internal*, untuk direktori *com.telegram* sub-direktori folder data. Berikut adalah susunan dari direktori *com.telegram.*



Gambar 4. Struktur Direktori Telegram

Terlihat dari Gambar 4, aplikasi Telegram memiliki 5 folder utama serta terdapat 2 sub-direktori di dalamnya.

C. Analisis Bukti Digital

Setelah dilakukan analisis, maka langkah selanjutnya adalah proses analisis bukti digital yang ada dalam kedua aplikasi *instant messenger*:

1. Kategorisasi Bukti Digital

Berdasarkan hasil analisis struktur direktori beserta konten di dalamnya, dilakukan klasifikasi data-data penting serta data-data pendukung dalam proses penelitian ini, antara lain:

Tabel 3. Data Penting

WhatsApp	Telegram
wa.db	Database tidak ditemukan
msgstore.db	

Database wa.db pada aplikasi WhatsApp menyimpan data kontak baik yang sudah disimpan oleh pengguna ataupun kontak yang belum disimpan namun melakukan interaksi di WhatsApp. Dalam *database* ini, tabel yang menjadi konsentrasi adalah tabel *wa_contacts* karena seluruh informasi mengenai kontak terpapar pada tabel ini.

Database msgstore.db pada aplikasi WhatsApp menyimpan seluruh riwayat pesan yang ada di WhatsApp termasuk media yang ada di dalamnya. Dalam *database* ini, tabel yang menjadi konsentrasi adalah tabel *messages* karena seluruh informasi yang dibutuhkan mengenai percakapan dan pesan pada aplikasi terletak pada tabel ini.

Pada aplikasi Telegram *messenger*, baik menggunakan tools FTK Imager atau Autopsy, tidak ditemukan *database* yang memuat data penting seperti *database* utama atau *database* cadangan (*backup*) di direktori *Telegram* atau direktori *org.telegram*.

Data pendukung adalah data media yang ada pada aplikasi termasuk *database backup* atas seluruh riwayat aktivitas yang dilakukan selama penggunaan aplikasi. Dari masing masing aplikasi, data pendukung dapat ditemukan di direktori *WhatsApp* untuk aplikasi WhatsApp *messenger* dan direktori *Telegram* untuk aplikasi Telegram *messenger*. Berikut adalah rincian informasi mengenai data pendukung yang berhasil ditemukan:

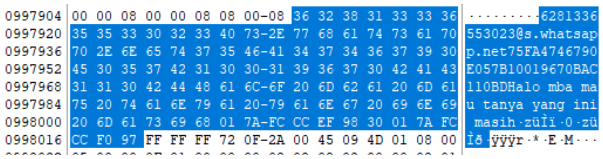
Tabel 4. Data Pendukung

Kategori		WhatsApp	Telegram
Media	Audio	Ditemukan	Ditemukan
	Document	Ditemukan	Tidak ditemukan
	Foto	Ditemukan	Ditemukan
	Profile Photo	Ditemukan	Tidak ditemukan
	Video	Ditemukan	Ditemukan
Database Backup		Ditemukan	Tidak ditemukan

2. Struktur Pesan

Dalam penelitian ini struktur pesan merupakan *object* yang menyusun sebuah pesan pada aplikasi. Berikut merupakan hasil struktur pesan yang ditampilkan pada aplikasi FTK Imager pada setiap aplikasi:

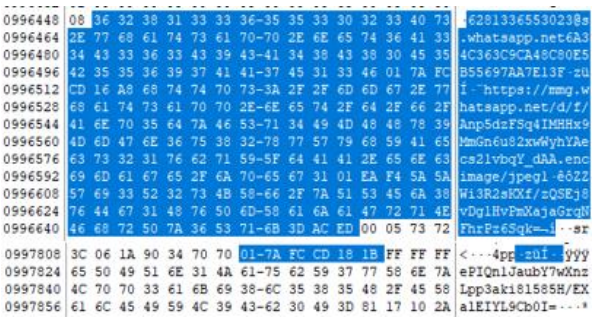
a. Struktur Pesan WhatsApp



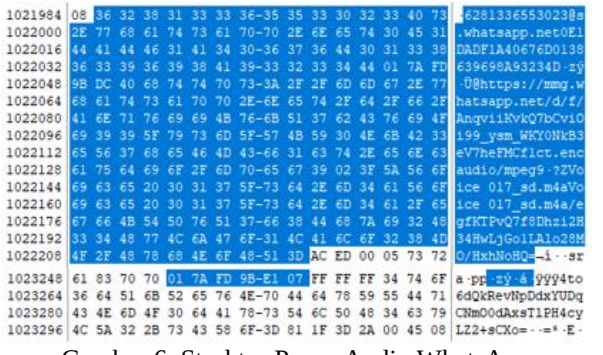
Gambar 4. Struktur Pesan Teks WhatsApp

Tabel 5. Penjelasan Struktur Pesan Teks

Data	Keterangan
6281336553023@s.whatsapp.net	ID atau nomor dari partner komunikasi
75FA4746790E057B10019670BAC110BD	Kode pesan pada aplikasi WhatsApp
Halo mba mau tanya yang ini masih	Isi dari pesan (berupa teks)
.züÌï. Hexa: 017AFCCCEF98 Decimal: 1627738927000	Kode *unix timestamps* yang menunjukkan waktu pengiriman pesan. Apabila dikonversi dari *decimal* ke *human date* akan menunjukkan waktu pengiriman.
.züÌð. Hexa: 017AFCCCF097 Decimal: 1627738927255	Kode *unix timestamps* yang menunjukkan kapan pesan diterima. Apabila dikonversi dari decimal ke human date akan menunjukkan waktu pesan diterima.



Gambar 5. Struktur Pesan Image WhatsApp



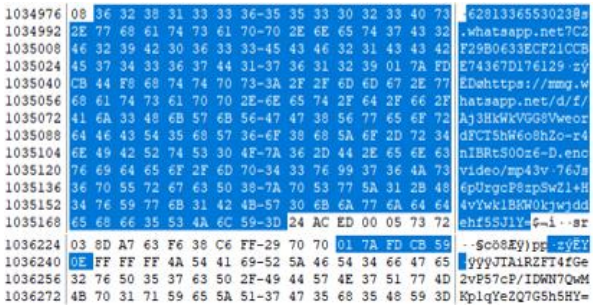
Gambar 6. Struktur Pesan Audio WhatsApp

Tabel 6. Penjelasan Struktur Pesan Image

Data	Keterangan
6281336553023@s.whatsapp.net	ID atau nomor dari partner komunikasi
6A34C363C9CA48C80E5B55697AA7E13F	Kode pesan pada aplikasi WhatsApp
.züÍ.¨ Hexa: 017AFCCD16A8 Decimal: 1627738937000	Kode *unix timestamps* yang menunjukkan waktu pengiriman pesan. Apabila dikonversi dari *decimal* ke *human date* akan menunjukkan waktu pengiriman.
https://mmg.whatsapp.net/d/f/Anp5dzFSq4IMHHx9MmGn6u82xwWyhYAecs21vbqY_dAA.enc	URL atau link dari media yang dikirim (*encrypted*).
image/jpeg	Jenis pesan atau format pesan yang dikirim.
ZZWi3R2sKXf/zQSEj8vDg1HvPmXajaGrqNFhrPz6Sqk=	Enkripsi media base64 hash SHA256 dari file yang dikirim.
.züÍ.. Hexa: 017AFCCD181B Decimal: 1627738937371	Kode *unix timestamps* yang menunjukkan kapan pesan diterima. Apabila dikonversi dari decimal ke human date akan menunjukkan waktu pesan diterima.

Tabel 7. Penjelasan Struktur Pesan Audio

Data	Keterangan
6281336553023@s.whatsapp.net	ID atau nomor dari partner komunikasi
E1DADF1A40676D0138639698A93234D	Kode pesan pada aplikasi WhatsApp
.zý.Ü@ Hexa: 017AFD9BDC40 Decimal: 1627752488000	Kode *unix timestamps* yang menunjukkan waktu pengiriman pesan. Apabila dikonversi dari *decimal* ke *human date* akan menunjukkan waktu pengiriman.
https://mmg.whatsapp.net/d/f/AnqviiKvkQ7bCviOi99_ysm_WKY0NkB3eV7heFMCf1ct.enc	URL atau link dari media yang dikirim (*encrypted*).
audio/mpeg	Jenis pesan atau format pesan yang dikirim.
Voice 017_sd.m4a	Nama dari file yang dikirim (dilengkapi format file).
Voice 017_sd.m4a	Caption dari media/file yang dikirim
/egfKTPvQ7f8Dhzi2H34HwLjGo1LAlo28MO/HxhNoHQ=	Enkripsi media base64 hash SHA256 dari file yang dikirim.
.zý.á.	Kode *unix timestamps* yang menunjukkan kapan pesan diterima. Apabila dikonversi dari decimal ke human date akan menunjukkan waktu pesan diterima.



Gambar 7. Struktur Pesan Video WhatsApp

Tabel 8. Penjelasan Struktur Pesan Video

Data	Keterangan
6281336553023@s.whatsapp.net	ID atau nomor dari partner komunikasi
7C2F29B0633ECF21CCBE74367D176129	Kode pesan pada aplikasi WhatsApp
.zýËDø Hexa: 017AFDCB44F8 Decimal: 1627755595000	Kode *unix timestamps* yang menunjukkan waktu pengiriman pesan. Apabila dikonversi dari *decimal* ke *human date* akan menunjukkan waktu pengiriman.
https://mmg.whatsapp.net/d/f/Aj3HkWkVGG8VweordFCT5hW6o8hZo-r4nIBRtS0Oz6-D.enc	URL atau link dari media yang dikirim (*encrypted*).
video/mp4	Jenis pesan atau format pesan yang dikirim.
6Js6pUrgcP8zpSwZ1+H4vYwk1BKW0kjwjddehf5SJlY=	Enkripsi media base64 hash SHA256 dari file yang dikirim.
.zýËY. Hexa: 017AFDCB590E Decimal: 1627755600142	Kode *unix timestamps* yang menunjukkan kapan pesan diterima. Apabila dikonversi dari decimal ke human date akan menunjukkan waktu pesan diterima.

b. Struktur Pesan Telegram

Untuk aplikasi Telegram, tidak dapat ditemukan data penting atau data pendukung dari data pesan percakapan hasil ekperimen skenario.

D. Pelaporan Hasil Analisis

Berdasarkan dari hasil pemeriksaan dan analisis percakapan teks dan media, didapatkan hasil bahwa dari kedua apliksi *instant messenger* yang dilakukan pengujian, hanya satu aplikasi yaitu WhatsApp *messenger* yang dapat menghasilkan barang bukti digital yang validitasnya dapat dibuktikan. Selain pembuktian dari data penting, WhatsApp memberikan bantuan berupa data pendukung yang cukup lengkap.

Untuk aplikasi Telegram *messenger*, tidak dapat ditemukan informasi apapun mengenai skenario dan hasil eksperimen yang dilakukan pada penelitian ini.

E. Perbandingan Data Digital

Berdasarkan hasil analisis dari ketersediaan data penting dan pendukung serta struktur direktori dan pesan, akan dijabarkan secara umum jangkauan data yang dapat dijangkau oleh setiap tools yang digunakan yang selanjutnya dapat dijadikan perbandingan dalam mmpertimbangkan cakupan data dari tools FTK Imager dan Autopsy. Pada Tabel 8 telah diberikan hasil perbandingan dari data penting dan pendukung pada setiap aplikasi yang didapatkan, perbandingan antar tools yang digunakan dan perbandingan aplikasi *instant messenger.*

1. Data Penting

Berdasarkan pada tabel 9 di bawah, data penting yang dapat ditemukan pada *tools* FTK Imager dan Autopsy hanya pada aplikasi WhatsApp *messenger* dengan rincian data yang ditemukan antara lain, ID Sender (identitas pengirim), Data (isi percakapan), Key ID (identitas pesan pada aplikasi), Timestamp (waktu pengiriman dan penerimaan pesan).

Sedangkan untuk aplikasi Telegram *messenger* tidak dapat ditemukan data penting apapun di seluruh direktori aplikasi ini.

Tabel 9. Perbandingan Data Penting

Tools/ Aplikasi	User ID	Sender ID	Data	Key ID	Time stamp
FTK Imager					
WhatsApp	–	√	√	√	√
Telegram	–	–	–	–	–
Autopsy					
WhatsApp	–	√	√	√	√
Telegram	–	–	–	–	–

2. Data Pendukung

Berdasarkan pada tabel 10 di bawah, *tools* FTK Imager dan Autopsy berhasil mendapat data pendukung dari kedua aplikasi. Pada aplikasi WhatsApp ditemukan data pendukung *picture, audio, video* serta *database backup* yang berisi Riwayat penggunaan aplikasi dantelah dienkripsi oleh WhatsApp.

Kemudian pada aplikasi Telegram ditemukan berhasil ditemukan data picture, audio dan video, untuk database backup tidak berhasil ditemukan.

Tabel 10. Perbandingan Data Pendukung

Tools/ Aplikasi	Picture	Audio	Video	Database Backup
FTK Imager				
WhatsApp	√	√	√	√
Telegram	√	√	√	–
Autopsy				
WhatsApp	√	√	√	√
Telegram	√	√	√	–

F. Perbandingan Data Digital

Pembahasan keamanan disini lebih mengacu pada aksesibilitas dan ketersediaan data yang tersimpan di direktori kedua aplikasi tersebut. Dari hasil pengamatan penulis, aplikasi WhatsApp *messenger* adalah salah satu aplikasi perpesanan yang mudah untuk dilakukan analisis forensik karena selain ketersediaan data yang cukup lengkap, WhatsApp messenger memiliki struktur data yang sederhana dan manajemen kelola data yang sangat teroganisir. Hal tersebut memberikan kemudahan bagi para examiner atau praktisi forensik dalam melakukan pembuktian data digital. Sehingga dengan adanya kemudahan yang diberikan, akan membantu kecepatan pengungkapan suatu kasus kejahatan maupun untuk membuktikan sebuah kronologi terkait pesan dalam aplikasi WhatsApp *messenger*.

Namun, hal tersebut berlaku sebaliknya untuk aplikasi Telegram *messenger*. Aplikasi ini meiliki tingkat keamanan lebih tinggi dibandingkan WhatsApp *messenger*. Dari sisi ketersediaan data, Telegram *messenger* hanya menyediakan data yang bersifat artefak (cache) dan data media (*image, document, audio, video*). Dalam melakukan analisis forensik, examiner akan sedikit lebih sulit karena *database* percakapan pada aplikasi sangat dilindungi sehingga tidak banyak data penting yang dapat diungkap dari aplikasi ini.

.

IV. KESIMPULAN

Berdasarkan hasil dari penelitian pada analisis forensik digital pada aplikasi WhatsApp *messenger* dan Telegram *messenger*, didapat beberapa simpulan. Pertama, di antara kedua aplikasi *instant messenger* yang telah dianalisis, hanya WhatsApp *messenger* yang dianggap mampu memberikan sebuah bukti digital yang valid dan dapat dibuktikan validitasnya. Kedua, dalam hal karakteristik bukti digital, setiap aplikasi memiliki ciri khas dan keunikannya masing-masing tergantung dari struktur pesan aplikasi tersebut. Untuk aplikasi WhatsApp messenger, karakteristik bukti digital yang berhasil didapatkan berupa key_remote_jid, key_id, data, timestamp, dan received_timestamp. Terkahir, aplikasi WhatsApp *messenger* memiliki tingkat kerentanan yang tinggi karena kemudahan dalam melakukan praktik forensik mulai dari *acquisition* hingga *analysis* dalam pembuktian tersangka dari kronologi percakapan. Sedangkan untuk tingkat keamanan pada aplikasi Telegram *messenger* dinilai lebih unggul karena tidak banyak data penting yang bisa didapat dan dianalisis. Tingkat sekuritas yang tinggi juga berakibat pada rumitnya tindakan forensik dalam pengungkapan sebuah kasus kejahatan karena bukti digital sulit untuk ditemukan.

DAFTAR PUSTAKA

[1] F. Yudha, "USB Analisys Tool Untuk Investigasi Forensika Digital," *Teknoin*, vol. 21, no. 4, pp. 200–206, 2015, doi: 10.20885/teknoin.vol21.iss4.art6.

[2] I. Riadi, R. Umar, and A. Firdonsyah, "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 5, pp. 155–160, 2017.

[3] M. S. Asyaky, "Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android," *J. Penelit. Tek. Inform.*, vol. Vol. 3 No, no. 1, pp. 220–231, 2019.

[4] G. M. Zamroni, R. Umar, and I. Riadi, "Analisis Forensik Aplikasi Instant Messaging Berbasis Android," in *Annual Research Seminar*, 2016, pp. 102–105, 2016, [Online]. Available: http://ars.ilkom.unsri.ac.id.

[5] B. Raharjo, "Sekilas Mengenai Forensik Digital," *J. Sosioteknologi*, vol. 12, no. 29, pp. 384–387, 2013, doi: 10.5614/sostek.itbj.2013.12.29.3.

[6] Noffezar, Fitriati, and I. Faniyah, "Penggunaan Alat Bukti Digital Dalam Komputer Forensik Pada Penyidikan Tindak Pidana Mayantara Di Direktorat Kriminal Khusus Polda Sumbar," *UNES J. Swara Justisia*, vol. 2, no. 4, pp. 411–419, 2019.

[7] M. N. Al-Azhar, *Digital Forensic: Practical Guidelines for Computer Investigation*, 1st ed. Jakarta: Salemba Infotek, 2012.

[8] I. Z. Yadi and Y. N. Kunang, "Forensik Pada Platform Android," in *Konferensi Nasional Ilmu Komputer (KONIK)*, 2014, pp. 141–148, [Online]. Available: http://eprints.binadarma.ac.id/2191/.

[9] M. F. Sidiq and M. N. Faiz, "Review Tools Web Browser Forensics untuk Mendukung Pencarian Bukti Digital," *J. Edukasi dan Penelit. Inform.*, vol. 5, no. 1, pp. 67–73, 2019, doi: 10.26418/jp.v5i1.31430.

[10] R. Padmanabhan, K. Lobo, M. Ghelani, D. Sujan, and M. Shirole, "Comparative analysis of commercial and open source mobile device forensic tools," *2016 9th Int. Conf. Contemp. Comput. IC3 2016*, 2017, doi: 10.1109/IC3.2016.7880238.

[11] W. Jansen and R. Ayers, "Guidelines on Cell Phone Forensics," *NIST*, vol. 800, no. 101, pp. 1–104, 2007, [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800101/SP800-101.pdf.