JIKO (Jurnal Informatika dan Komputer)
Vol. 7, no. 2, September 2023, hal. 183–190
e-ISSN : 2477-3964 — p-ISSN : 2477-4413
DOI: dx.doi.org/10.26798/jiko.v7i2.789

ANALISIS PENYADAPAN PADA TELEGRAM DENGAN NETWORK FORENSIC

Nadiya Citra Dewi[1], **Tata Sutabri**[2], dan **Ferry Putrawansyah**[3],
[1,3]Program Studi Magister Teknik Informatika dan Universitas Bina Darma, Indonesia
[2]Program Studi Teknik Informatika dan Institut Teknologi Pagar Alam, Indonesia
Email: nadiyacitradewi5@gmail.com[1], tatasutabri@gmail.com[2]

Abstrak

Perkembangan dunia komunikasi dan telekomunikasi sangat meningkat tajam semenjak layanan pengiriman pesan instan berbasis internet berbasis social media merambat cepat ke Indonesia. Telegram merupakan salah satu social media yang memberikan layanan pengirim pesan instan multiplatform berbasis Cloud Computing yang bersifat gratis dan nirlaba. Kelebihan telegram yakni mampu memberikan layanan berbagai fitur yang belum dikembangkan aplikasi sejenis yakni diantarnya pengiriman file besar yang mampu dikirim melalui aplikasi telegram. Fitur ini tentunya dapat mempermudah pertukaran informasi maupun data namun hal ini memberikan celah keamanan yang melibatkan kedua device yakni smartphone dan Komputer. Penanganan tindak kejahatan yang melibatkan piranti digital perlu ditingkatkan sehingga dapat membantu proses peradilan akan efek yang ditimbulkanya. Metode Investigasi forensic digital turut berperan serta terhadap penindakan penyalahgunaan fitur layanan pesan instan telegram diantaranya Langkah investigasi penanganan kasus penyadapan percakapan telegram melalui serangkaian tahapan baku sesuai proses dan prosedur forensika digital. Digital Forensik dengan barang bukti Telegram pada Smartphone dan Telegram Web Brwoser akan menghasilkan perbandingan dual digital evidence yang melibatkan lintas platform yaitu Android (mobile forensics) dan Windows (computer forensics). Dengan diterapkannya metode Investigasi forensic pada Telegram yang melibatkan skema proses yaitu pentest Telegram attack dan flowchart penyadapan Telegram maka akan diperoleh hasil perbandingan investigasi terhadap dua devices mencakup Telegram on Smartphone dengan sistem operasi Android dan Telegram Web pada komputer sehingga didapatkan ekplorasi temuan digital evidence yang menyatakan bahwa hal tersebut merupakan tindak kejahatan yang berkaitan dengan pesan layanan Telegram massanger sehingga pengguna mengetahui alur tindak kejahatan telegram dan dapat mengantisipasinya.
Kata Kunci: *Forensik, Investigasi, Smartphone, Telegram*

Abstract

The development of the telecommunication world has increased sharply since internet-based instant messaging services based on social media have spread rapidly to Indonesia. Telegram is one of the social media that provides free and non-profit Cloud Computing-based multi-platform instant messaging services. The advantage of Telegram is that it is able to provide services with various features that have not been developed by similar applications, namely sending large files that can be sent via the Telegram application. Of course, this feature can facilitate the exchange of information and data, but this provides a security gap that involves both devices, namely smartphones and computers. The handling of crimes involving digital devices needs to be improved so that they can assist the judicial process regarding the effects they cause. Digital forensic investigation methods also play a role in the prosecution of abuse of telegram instant messaging service features, including steps to investigate cases of wiretapping telegram conversations through a series of standard stages according to digital forensics processes and procedures. Digital Forensics with Telegram evidence on Smartphones and Telegram Web Browser will produce dual digital evidence comparisons that involve cross platforms, namely Android (mobile forensics) and Windows (computer forensics). By applying the forensic Investigation method to forensic Telegram which involves a process scheme, namely the pentest Telegram attack and the Telegram wiretapping flowchart, results of a comparison of investigations of two devices will be obtained, including Telegram on Smartphone with the Android operating system and Telegram Web on computers with the Windows platform so that there will be The comparison normalization table will explore digital evidence findings which state that crimes are related to Telegram messenger service messages so that users know the flow of Telegram crimes and can anticipate them.
KeyWords: *Forensik, Investigasi, Smartphone, Telegram*

I. PENDAHULUAN

Perkembangan media sosial dan aplikasi pesan instan telah tumbuh secara eksponensial dan telah memfasilitasi pengembangan banyak tindak *cyber crime* kejahatan *cyber* dan aktivitas jahat yang serius [1]. Para *Hacker* terus mengubah strategi untuk dapat masuk secara *anonymous* ke akun user yang telah disusupi. Penyalahgunaan media sosial dan pesan instan dalam layanan mobile memungkinkan penjahat dunia maya memanfaatkan layanan ini untuk tujuan yang tidak baik jahat seperti memeras pemilik akun, membagikan informasi hoaks sampai ke menguras tabungan [2]. Banyak sekali media sosial dan penyedia pesan instan telah memperluas layanan mereka ke *platform* empiris,yang memperburuk situasi karena pengguna berada dalam bahaya kehilangan lebih banyak lagi informasi pribadi [3].

Telegram merupakan aplikasi layanan pengiriman pesan instan (*Chatting*) multiplatform berbasis *cloud Computing* yang bersifat *open source* nirlaba. Saat ini telegram tersedia untuk perangkat telepon seluler bersistem operasi android maupun IoS dan juga sistem perangkat komputer (Windows, OS X, Linux) sehingga para pengguna dapat mengirim pesan, foto, video, stiker, audio, dan dokumen berukuran besar. Telegram dikembangkan oleh Telegram Messenger LLP dan didukung oleh wirausahawan Rusia Pavel Durov. Kode pihak kliennya berupa perangkat *open source* namun mengandung *blob binari*, dan kode sumber

This Article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

JIKO (Jurnal Informatika dan Komputer)
Vol. 7, no. 2, September 2023, hal. 183–190
e-ISSN : 2477-3964 — p-ISSN : 2477-4413
DOI: dx.doi.org/10.26798/jiko.v7i2.789

untuk versi terbaru tidak selalu segera dipublikasikan, sedangkan kode sisi servernya bersumber tertutup dan berpaten namun masih memiki sisi kemanan yang lemah.

Forensik Smartphone adalah bagian dari metode forensik digital, dan mengacu padaupenyelidikan dan perolehan artefak pada *smartphone*. Ancaman baru terhadap ponsel membuat ilmu forensik menjadi tantangan yang menantang dalam beberapa tahun terakhir. Jumlah pengguna ponsel meningkat diuseluruh dunia dan menimbulkan masalah dan tantangan yang luar biasa. Literatur yang uelevan dengan forensik *smartphone*, fokus penelitian ini pada arsitektur sistem operasi *smartphone* dan teknik antiforensik. Ini juga membahas bukti digital dari aplikasi *smartphone* [4]. Forensik Android telah berkembang dari waktu ke waktu dengan menawarkan peluang dan tantangan menarik yang signifikan. Metode forensik diperlukan untuk memastikan keberhasilan proses pengambilan data-data tersebut. Penelitian ini akan menjelaskan langkah-langkah untukumemperoleh data aplikasi Telegram, dari data yang telah dienkripsi menjadi data yang dapat dibaca dan dianalisis untuk kemudian dapat digunakan sebagai barang bukti yang baik [5]. Di satu sisi, menjadi *platform open source* Android memberi pengembang kebebasan untuk berkontribusi pada pertumbuhan pasar Android yang pesat, sementara di sisi lain pengguna Android mungkin tidak menyadari implikasi keamanan dan privasi pemasangan aplikasi ini di ponsel mereka. Pengguna mungkin menganggap bahwa perangkat yang terkunci sandi melindungi informasi pribadi mereka, namun aplikasi mungkin menyimpan informasi pribadi pada perangkat, dengan cara yang mungkin tidak diantisipasi pengguna. Dalam penelitian ini akan berkonsentrasi pada satu aplikasi yang disebut 'Telegram', aplikasi jejaring sosial yang populer. Penelitia akan membentuk garis besar tentang bagaimana penyidik forensik dapat mengekstrak informasi yanguberguna dari telegram dan dari aplikasi serupa yang terpasang di platform Android. Area fokus penelitian adalah ekstraksi udan analisis data pengguna aplikasi dariupenyimpanan eksternal *non-volatile* dan memori *volatile* (RAM) perangkat Android [6].

Instant Messaging (IM) merupakan salah satu aplikasi seluler yang sangat popular. Salah satu jenis aplikasi IM adalah Telegram. Pengguna Telegram jumlahnya mencapai 1 Milyar setiap bulannya. Telegram didukung oleh fitur enkripsi untuk menjamin keamanan data para penggunanya. Kepopuleran dan fitur yang diberikan Telegram dapat disalahgunakan masyarakat untuk tujuan kriminal, seperti perdagangan narkoba, kegiatan teroris, perencanaan pembunuhan, dan kegiatan kriminal lainnya melalui fitur-fitur yang tersedia. Pihak berwenang dapat menggunakan data-data dalam Telegram sebagai barang bukti.

Secara forensik memperoleh dan menganalisis data yang tersimpan perangkat dan lalu lintas jaringan dari 20 aplikasi pesan instan yang populer untuk Android. investigator dapat mengkonstruksikan beberapa atau seluruh isi pesan dari 16 dari 20 aplikasi yang diuji yang mencerminkan keburukan pada tindakan keamanan dan privasi yang digunakan oleh aplikasi ini, namun dapat dianggap positif untuk tujuan pengumpulan bukti digital oleh praktisi forensik digital. Penelitian ini menunjukkan fitur aplikasi pesan instan mana yang meninggalkan jejak pembuktian yang memungkinkan data tersangka direkonstruksi sebagian, dan apakah forensik jaringan atau forensik perangkat memungkinkan dilakukannya rekonstruksi aktivitas tersebut. Peneliti menunjukkan bahwa dalam banyak kasus dapat merekonstruksi data seperti : kata sandi, *screenshot* yang diambil oleh aplikasi, gambar, video, audio yang dikirim, pesan yang dikirim, sketsa, gambar profil dan lain-lain [1].

Berdasarkan pernyataan peneliti terdahulu diatas dapat dikembangkan Analisis Investigasi Forensik *Telegram Messenger smartphone* terhadap Telegram dengan studi kasus penyadapan percakapan Telegram, dengan mempertimbangkan beberapa aspek seperti pernyataan peneliti terdahulu penelitian lanjutan dihadapkan pada berbagai jenis perangkat *smartphone* selama penanganan kasus investigasi forensik [7]. Perangkat *smartphone* saat ini menjadi sumber penting *digital evidenc*e yang relevan dengan pengguna media sosial dan aktivitas instan Messenger [8]. Namun, perbedaan antara perangkat smartphone menjadi tantangan penyidik atau investigator forensik untuk mengembangkan metode dan teknik yang disesuaikan untuk penyelidikan berbagai kasus cybercrime [9].

II. Metode Penelitian

A. Network Forensics

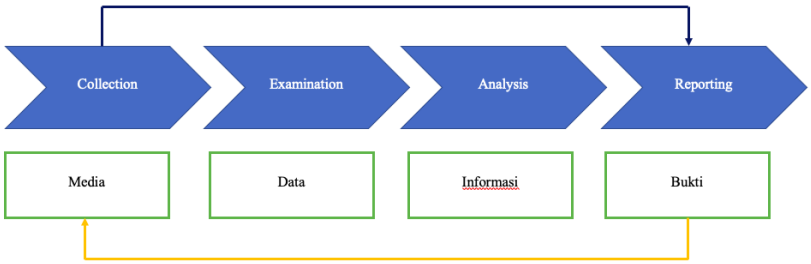
Network Forensik ialah sebuah cabang ilmu forensik, untuk penemuan buktiudigital dan seringukali dikaitkan dengan kejahatan komputer digital. Awalnya istilah digital forensik ini disebut dengan forensik komputer tetapi kini di perluas untuk semua perangkat yang dapat menyimpan bukti digital. Landasan dari sebuah digital forensik ialah pengumpulan, analisis, dan pembuktian data digital [3].

B. National Institute of Standards Technology (NIST)

Metode forensic *National Institute of Standards Technology* (NIST) adalah tahapan untuk mendapatkan informasi dari bukti digital yaitu dengan menggunakan metode NIST. Transformasi pertama terjadi saat data yang dikumpulkan diperiksa, lalu mengekstrak data dari Media dan mengubahnya menjadi format yang bisa diproses oleh alat forensik. Kedua, data ditransformasikan menjadi informasi melalui analisis.

This Article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

JIKO (Jurnal Informatika dan Komputer)
Vol. 7, no. 2, September 2023, hal. 183–190
e-ISSN : 2477-3964 — p-ISSN : 2477-4413
DOI: dx.doi.org/10.26798/jiko.v7i2.789



Gambar 1: Tahap Analisa

1) *Collection* adalah pelabelan, identifikasi, rekaman, dan pengambilan data dari sumber data yang relevan dengan prosedur pada tahap analisa untuk menjaga integritas data. 2) *Examination* adalah pengolahan data yang dikumpulkan dalam penggunaan forensik kombinasi berbagai skenario, baik otomatis atau manual, serta menilai dan mengeluarkan data sesuai kebutuhan sambil mempertahankan integritas data. 3) *Analysis* adalah analisis hasil pemeriksaan dengan menggunakan metode teknis uang dibenarkan oleh hukum. 4) *Reporting* adalah melaporkan hasil analisis yang meliputi penggambaran tindakan yang dilakukan.

C. Telegram Analysis

Telegram dirancang untuk memudahkan pengguna saling berkirim pesan teks, audio, video, gambar dan sticker dengan aman. Tak hanya aman, telegram juga merupakan aplikasi berbagi pesan yang instan atau cepat. Telegram sendiri adalah aplikasi yang dikembangkan oleh perusahaan Telegram FZ LLC dan Telegram Messenger Inc asal Rusia. Aplikasi ini rilis pada tahun 2013 lalu. Telegram juga merupakan istilah untuk surat atau berita yang pengirimannya disalurkan melalui pesawat morse, teleks , atau teleprinter. Pada saat sebelum adanya *smartphone*, Telegram cukup populer di kalangan masyarakat. Cara kerja telegram yakni aplikasi Telegram adalah aplikasi yang berbasis *cloud*. Artinya, penggunanya dapat dimudahkan untuk mengakses satu akun Telegram dari perangkat yang berbeda dan secara bersamaan berbeda dari Whatsapp dengan system kerja bahwa data WhatsApp disimpan dalam memori Internal smartphone setelah *package installer* WhatsApp ter-install, secara otomatis sinkronisasi dengan kontak telepon menunjukkan pengguna yang sudah menggunakan Telegram. Sebagai sebuah aplikasi, Telegram tentunya memiliki sejumlah keunggulan. Berikut beberapa keunggulan aplikasi Telegram: 1) Telegram adalah aplikasi gratis dan akan terus gratis atau tidak akan pernah ada iklan atau biaya untuk selamanya, 2) Telegram mengirim pesan lebih cepat karena berbasis *cloud*, 3) Telegram lebih ringan ketika dijalankan, ukuran aplikasi lebih kecil Telegram versi v3.31 untuk Android yang dikeluarkan pada 25 November 2015 memiliki ukuran 16.00 MB (16,775,108 bytes), 4) Telegram dapat diakses dari berbagai perangkat secara bersamaan diantaranya, *smartphone*, tablet, komputer, laptop dan lain-lain, 5) Telegram mengizinkan penggunanya untuk berbagi berbagai macam jenis file, seperti foto, video, file (doc,zip,mp3) dengan ukuran maksimum 1,5 GB per file. Selain beberapa keunggulan yang telah dijelaskan sebelumnya, ada salah satu fitur yang menjadi keunggulan dari aplikasi Telegram, yakni fitur *bot*. *Bot* merupakan aplikasi pihak ketiga yang dapat dijalankan di dalam Telegram. Pengguna dapat mengirim pesan, perintah, dan *online request*. Pembuat *bot* dapat mengontrol *bot* menggunakan HTTPS ke API Telegram.

Dengan dukungan versi baru Telegram Web yang berjalan di komputer, setelah dilakukan *scan QR Code* Telegram yang terjadi sinkronisasi dengan aplikasi *Telegram on Smartphone* baik itu kontak telepon, percakapan dan data yang melekat di *smartphone* penggunanya dapat pula diakses melalui Telegram Web. Hal ini menunjukkan pengguna yangusudah menggunakan Telegram Web memiliki tingkat *vulnerability*, dimana pesan Telegram yang terdapat di *smartphone* dapat pula diakses di Telegram Web dengan kata lain kemungkinan dilakukan penyadapan bilamana komputer atau *smartphone* digunakan dalam satu waktu oleh orang lain tanpa sepengatahuan penggunanya maka memungkinkan pula pelaku penyadapan dapat mengkases percakapan obrolan secara detail termasuk gambar, video, kontak dan sebagainya.

Masalah utama setelah terjadi sinkronisasi data Telegram *smartphone* dan komputer adalah intervensi pihak yang terlibat penyalahgunaan layanan (penyadapan aplikasi dual Telegram), sehingga muncul gagasan atau desain dan rancangan usulan *Telegram Investigation* meliputi beberapa kompunen utama baik tahapan investigasi serta ditekankan pada poin dasar diantaranya meliputi 1) *Telegram Evidence*; berupa fisik dari *smartphone* dan komputer korban beserta tindak kriminal dan penanganannya. 2) Riset *Goal Investigation Method* ; proses penanganan barang bukti dari memperoleh, akuisisi serta merepresentasikan skema kasus. 3) *Forensics Tools Investigator*; merupakan *software forensic* dalam hal ekplorasi, eksaminasi dan reporting berkenaan terhadap barang bukti penyadapan Telegram 4) *Digital Evidence Risk*; Resiko yang ditimbulkan pasca penyadapan berupa layanan Telegram ; Chat, File Sharing dan sinkronisasi, serta komputer browser (Telegram Web) memerlukan penanganan yang lebih terkait akuisisi dataudari Telegram Web tersebut. Tahapan prosesupenangananuinvestigasi penyadapan Telegram setelah dikondisikan terhadap skema kasus serta pengembangan tahapan investigasi mobile forensik dan network forensik maka dapat diperoleh tahapan seperti pada Tabel I [11].

This Article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

JIKO (Jurnal Informatika dan Komputer)
Vol. 7, no. 2, September 2023, hal. 183–190
e-ISSN : 2477-3964 — p-ISSN : 2477-4413
DOI: dx.doi.org/10.26798/jiko.v7i2.789

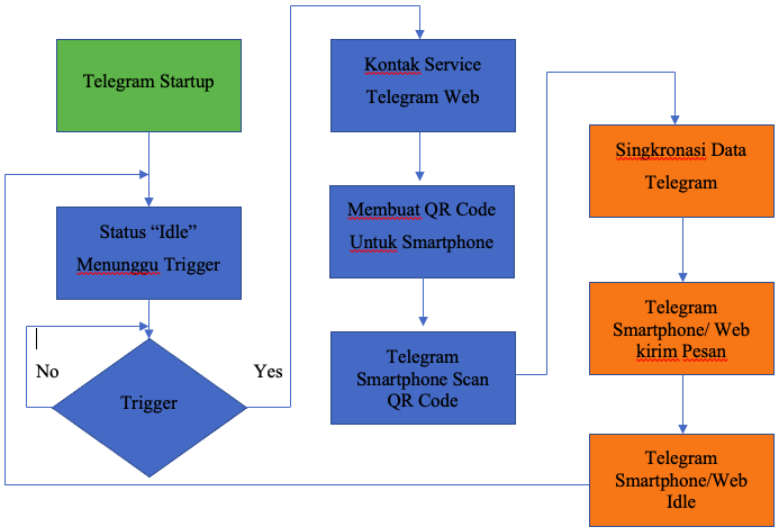
Tabel I: Proses Investigasi Penyadapan Percakapan Telegram

Identification	Preservation	Collection	Examination	Analysis	Presentation
Identifikasi kejahatan Telegram	Pengolahan kasus Telegram	Pengamatan Barang Bukti Telegram	Pelacakan Barang Bukti Telegram	komparasi Data dan Investigasi	Dokumentasi
Profil kejahatan telegran	Chain of custody / Kronologis telegram attack	Teknik Investigasi Telegram	Validasi Barang Bukti Telegram	Pengolahan temuan barang Bukti	Klasifikasi Investigator
Audit dan Analisis Kasus	Manaejemn waktu investigasi		Filtering arang bukti		Penyataan saran dan tindakan
	Pengolahan kasus telegram		Pencocokan barang bukti		Interpretasi data telegram
			Penemuan data tersembunyi		

Berdasarkan Tabel I diatas maka terlihat bahwa Prosedur Investigasi penyadapan pada percakapan Telegram diperoleh penekanan pada poin *Preservation*, sebagai tahapan yang memerlukan penanganan yang lebih khususnya *smartphone* dengan aplikasi Telegram Web.

D. Simulasi Penyadapan Telegram

Rancangan simulasi penyadapan percakapan Telegram dalam hal ini akan dijelaskan skema pengujian aplikasi Telegram sebagai dalam hal ini menyangkut keberadaan barang bukti digital pasca terjadi penyadapan, sehingga diketahui respon terhadap masing-masing aplikasi antara Telegram pada Smartphone terhadap Telegram Web tampak seperti Gambar 2 :



Gambar 2: Alur Kerja Serangan Telegram

Simulasi penyadapan percakapan Telegram dari Gambar diatas difokuskan pada sinkronisasi data baik data Telegram pada *smartphone* ataupun pada web browser, selanjutnya kedua aplikasi tersebut sampai dapat mengakses aplikasi secara bersamaan secara identik. Lebih lengkapnya dapat dilihat pada gambar yang diberi warna orange diatas.

E. Flowchart Serangan Telegram

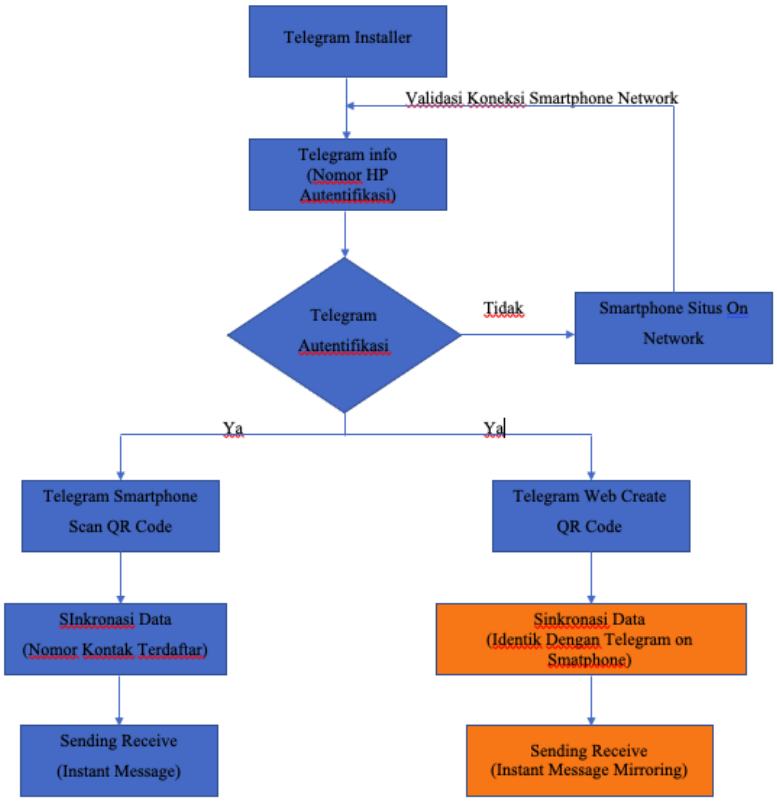
Flowchart Penyadapan Telegram merupakan penyesuaian terhadap simulasi penyadapan percakapan Telegram pada bagian sebelumnya, selanjutnya dikondisikan terhadap prinsip kerja terjadinya serangan, hal ini dapat dikatakan seperti penyadapan serta bagaimana motif kejahatan ini dapat terjadi seperti halnya penyalahgunaan privasi percakapan. Modifikasi dari prinsip kerja pentest Telegram dari Gambar 2 berupa diagram alir dari seluruh proses *Traffic Chanel Attack* untuk selanjutnya dikomparasi dengan keadaan terjadinya penyadapan melalui pesan singkat Telegram sesaat setelah dilakukannya *Attack* yang sesuai dengan tema penelitian sehingga diperoleh diagram alur proses baru yang sesuai dengan penelitian terkait Telegram yang melibatkan penyalahgunaan wewenang layanan telekomunikasi yakni dalam hal ini membaca pesan tanpa sepengetahuan pemilik akun (penyadapan) serta pelaku juga dapat mengirim pesan Telegram, sehingga tercipta alur proses baru seperti tampak pada diagram proses pada Gambar 3 dibawah.

Dengan diterapkannya metode investigasi Telegram forensik yang melibatkan skema proses yaitu pentest Telegram attack dan flowchart penyadapan Telegram maka akan diperoleh hasil perbandingan investigasi terhadap dua devices mencakup Telegram

This Article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

JIKO (Jurnal Informatika dan Komputer)
Vol. 7, no. 2, September 2023, hal. 183–190
e-ISSN : 2477-3964 — p-ISSN : 2477-4413
DOI: dx.doi.org/10.26798/jiko.v7i2.789

on Smartphone dengan sistem operasi Android dan Telegram Web on komputer yang ber-*platform* Windows sehingga nantinya terdapat Tabel normalisasi perbandingan akan ekplorasi temuan *digital evidence* yang menyatakan tindak kejahatan kaitannya dengan pesan layanan *Telegram messenger*.



Gambar 3: Flowchart Penyadapan Telegram

Motif kejahatan dengan pemanfaatan sinkronisasi dual aplikasi baik yang terdapat pada *smartphone* atau pada aplikasi web browser dapat terjadi bilamana *smartphone* korban tentunya dalam keadaan *status on network data* akses, demikian pula aplikasi web browser juga diutuhkan akses internet. Bilamana *smartphone* korban tidak dalam keadaan terkoneksi dengan internet dengan kata lain pelaku tindak kejahatan yang akan memanfaatkan sinkronisasi data Telegram tidak akan memperoleh data yang terbarukan *up to date* pasca sinkronisasi data Telegram. Skema tersebut dapat diperjelas pada *flowchart* penyadapan percakapan Telegram, yang berkaitannya dengan tingkat kerentanan atau *vulnerability* sebuah aplikasi pesan instant.

III. Hasil dan Pembahasan

A. *Mobile Forensics*

Digital Forensik dengan barang bukti Telegram pada *Smartphone* dan Telegram Web Brwoser akan menghasilkan komparasi *dual digital evidence* yang melibatkan lintas *platform* yaitu Android (*mobile forensics*) dan Windows (*computer forensics*), kedua sistem operasi tersebut menghasilkan karakteristik yang berbeda, baik dari tahap akuisisi barangubukti, penanganan, ekplorasi sampai pelaporan investigasi. *Mobile Forensics* dapat dilakukan pada berbagai *smartphone*, akan tetapi pada penelitian ini lebih difokuskan pada forensik smartphone ber-*platform* Android. Seiring meningkatnya jumlah *smartphone* yang kaya berbagai fitur membuat tantangan dalam membuat *tools* investigasi forensik atau standar khusus untuk masing-masing *platform*.

Bukti digital dalam perangkat mobile memiliki sifat yang mudah rentan tertimpa dengan data baru atau bahkan terhapus. Perangkat mobile sendiri menggunakan memori internal (*flash memory*), meskipun tidak menutup kemungkinan ekternal memori juga dapat dilakukan prose investigasi digital karena melibatkan penyimpanan data satu sama lain. Keuntungan menggunakan *flash memory* adalah ketahanannya terhadap suhu dan tekanan yang tinggi sehingga lebih sulit untuk dihancurkan. Dilihat dari sudut pandang forensik hal ini menguntungkan invesigator karena *flash memory* dapat berisi informasi yang sudah dihapus bahkan setelah seseorang berusaha untuk menghancurkan barang bukti masih dapat dilakukan *recovery data*. Berikut Alur *logical* nya:

1) ***Shared Preference***

Android menyediakan tiga cara untuk menyimpan data di *device*. Jika hanya untuk menyimpan sedikit data (beberapa variabel), maka mengunakan *shared preferences* seperti pada tahap investigasi *mobile forensics* yang melibatkan aplikasi

This Article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

JIKO (Jurnal Informatika dan Komputer)
Vol. 7, no. 2, September 2023, hal. 183–190
e-ISSN : 2477-3964 — p-ISSN : 2477-4413
DOI: dx.doi.org/10.26798/jiko.v7i2.789

pada sistem operasi Android Mobile. *Shared Preferences* adalah mekanisme untuk menyimpan pasangan *key-value* untuk tipe data primitif (*integer, double, string,float, booelan* dan *string*). *Shared Preferences* cocok untuk penggunaan data kecil seperti menyimpan setting aplikasi dan informasi mengenai *user interface*. Data dalam *shared preferences* disimpan dalam *device* android dalam bentuk XML. *Shared preferences* memiliki kondisi bilamana data cukup kompleks dan sering memerlukan pencarian (akses random) maka akan dibutuhkan database terkait, namun jika ukuran datanya besar dan tidak dibutuhkan sebuah pencarian spesifik maka dapat dialokasikan pada memori eksternal seperti MicroSD card untuk dapat dibaca komputer, atau memerlukan format yang yang sangat spesifik dalam penggunaannya.

2) ***Internal Storage***
Mobile Forensics Investigation dalam mengektraksi internal memori *smartphone* menggunakan *Oxygen forensic* dikarenakan *tools Oxygen* mengekstrak semua aplikasi didalam *smartphone* tak terkecuali Telegram yang dijadikan barang bukti penyadapan. Hal ini dapat terjadi diakibatkan *smartphone* android melakukan sinkronisasi *account* dengan phonebook. Proses sinkronisasi nantinya akan dikaitkan dengan aplikasi Telegram Web yang terdapat pada forensik browser pada komputer ber-*platform* windows.
3) ***External Storage***
Pada proses investigasi pada eksternal memori dilakukan secara manual. Ekstraksi berbeda bila dibandingkan dengan mengekstraksi data pada *smartphone*. Proses ini dilakukan dengan membuat *image* dari *digital evidence MicroSD card* dengan menggunakan *tools FTK Imager* beserta proses analisisnya.
4) ***Network Capture* (Simulasi Penyadapan Percakapan Telegram)**
Nmap bekerja pada ponsel *root* dan *non root*. Pada ponsel yang *non root investigator* dalam ekplorasinya akan terbatas pada fungsi yang dimungkinkan sebagai pengguna *non-root* (yaitu File System, Pemindaian SYN, dll.). Nmap (*Network Mapper*) merupakan sebuah *tools open source* untuk eksplorasi berdasarkan paket data yang Nmap *capturing*. Nmap dirancang untuk memeriksa jaringan besar secara cepat, meskipun dapat pula bekerja terhadap *host* tunggal. Nmap menggunakan paket *IP raw* dalam cara yang canggih untuk menentukan *host* mana saja yang tersedia pada jaringan, layanan (nama aplikasi dan versi) apa yang diberikan, sistem operasi apa yang digunakan, apa jenis *firewall/filter* paket yang digunakan, dan sejumlah karakteristik lainnya. Meskipun Nmap umumnya digunakan untuk audit keamanan, namun banyak investigator forensik digital dalam mengawasi lalulintas data yang terdapat pada *smartphone*. Keseluruhan dari proses ekplorasi serta temuan dari investigasi *mobile forensics* terkait *Telegram Messenger Smartphone Android* dapat disajikan seperti Tabel II :

Tabel II: Android Telegram Forensics

"Android" Telegram Aplication Data storage Forensics				
	Shared Preference	**Internal Storage**	**External Storage**	**Network Capture**
File Type stored	Key-value XML Format	Dibutuhkan hak akses (Developer Mode/root)	Hak akses penuh	ConGambarasi data network berbasis (Capture Network Access)
Data Type	Integer, double, string, float, boolean, dan string	Ekstraksi data (digital evidence)	Ekstraksi data (digital evidence)	hex value
Location	/data/data/com.telegram	/data/data/subdirectory	/mnt/sdcard or emulated SD card on /mnt/emmc	log files in /data/data/files
Access Level	Developer mode / root access	Developer mode / root access	Format FAT32 (Recovery Mode)	Network level
Forensic Use	Sumber data forensic (jika root akses)	Sumber data forensic (jika root akses)	Sumber data forensic (digital evidence)	Sumber data forensic (log digital evidence)

Database SQLite dapat digunakan sebagai pendukung tindakan investigasi digital dalam kaitannya membantu penyidik untuk mengumpulkan artefak Telegram. *Digital evidence* dengan database Telegram memiliki data yang dapat diekplorasi sebagai barang bukti diantaranya ;

1) File **msgstore.db** terletak di stuktur file android "*/data/data/com.telegram*" yang menyimpan pesan yang dikirim maupun diterima oleh pengguna aplikasi Telegram *Smartphone*.
2) File **telegram.db** terletak di lokasi yang sama "*/data/data/com.telegram*" dan menyimpan semua kontak Telegram

B. Windows (ComputeruForensics)

Windows Forensic Analysis berfokus pada investigasi forensik digital terhadap sistem operasi Microsoft Windows, dengan memahami konsep forensik dan artefak dari komponen inti *platform* windows beserta aplikasinya. *Computer forensics* akan membahas bagaimana memulihkan (*Recovery*), menganalisis (*Analysis*), dan *authentication data forensik* pada sistem Windows, melacak aktivitas pengguna tertentu di aplikasi atau program file, dan mengidentifikasi temuan untuk digunakan dalam respon insiden digital forensik dalam hal ini kemampuan Telegram Web dalam membaca aplikasi sejenis pada *smartphone* dalam kaitannya litigasi tindak kejahatan *cybercrime*. Sama halnya *tools* akuisisi pada eksternal memori *smartphone* digunakan *FTK Imager* sebagai akuisisi data partisi beserta system windows yang nantinya akan dijadikan alat images barang bukti dalam kegiatan investigasi file dan folder pada *hard disk local drive*. *FTK imager* juga mempunyai peran penting dalam otoritas

This Article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

JIKO (Jurnal Informatika dan Komputer)
Vol. 7, no. 2, September 2023, hal. 183–190
e-ISSN : 2477-3964 — p-ISSN : 2477-4413
DOI: dx.doi.org/10.26798/jiko.v7i2.789

barang bukti digital, FTK mampu membuat *file hash SHA1* atau *MD5*, mengekspor *file* dan *folder* dari *images forensic* ke *disk partition*, meninjau dan memulihkan *file* yang telah dihapus dari *Recycle Bin* (dengan syarat blok data mereka belum ditimpa), dan *mount images Forensic* untuk melihat isinya di Windows Explorer.

1) ***Web Browser Forensics***
   FoxAnalysis dan *Chrome Analysis* adalah perangkat lunak forensik untuk mengekstrak dan menganalisis riwayat internet dari *browser web Chrome*. Banyak jenis data dapat dianalisis termasuk kunjungan situs web, penelusuran, unduhan, file masuk tersimpan dan file dalam *cache*. Data yang diekstrak mencakup *bookmark*, *cookies*, *download*, *login*, situs yang paling banyak dikunjungi, sesi tersimpan dan kunjungan ke situs.
2) **Restore Evidence dari SQLite Database**
   Struktur database rekaman tentang pengguna Telegram disimpan di *disk partisi system windows*. Investigator dapat megekplorasi *file* yang tersimpan hasil akses *web browser* baik yang terhapus atau sebagian dari struktur halaman *SQLite*. *Recover data delete* untuk mengakses bukti digital dari halaman yang dihapus, investigator forensik perlu menganalisa ”*Cell Pointer Array*” yang merupakan jenis database yang menyimpan alamat setiap *cell array*. Analisis *history browser* atau forensik *database SQLite* hal ini dapat dibuktikan dengan mengekstrak bukti dari riwayat browser yang berisi informasi seperti ; *download*, *password*, *web url*, riwayat browser dan masih banyak lagi aktivitas penting lainnya. Tabel ”url” adalah tabel yang paling relevan yang menyimpan informasi dari semua URL yang dikunjungi termasuk kontak server Telegram web.
3) ***NetworkaCapture* (SimulasiaPenyadapan Percakapan Telegram)**
   Wireshark Analysis adalah *tools* yang ditujukan untuk melakukan analisa paket data jaringan. Wireshark melakukan monitoring paket secara realatime selanjutnya Wireshark melakukan penangkapan data dan menampilkannya selengkap mungkin. Keseluruhan dari proses ekplorasi serta temuan dari investigasi web browser terkait Telegram web dapat disajikan seperti Tabel III :

Tabel III: Windows Telegram Web Forensics

”Windows” Telegram Web Application Browser Forensic				
	System Windows	**Web Browser Forensic (Mozilla)**	**Web Browser Fprensic (Chrome)**	**Network Capture**
File Type Storage	Database On System	Cookies SQLite fromhistory sqlite content-prefs sqlite	Cookies SQLite fromhistory sqlite content-prefs sqlite	packet data Capture Network
Data Type	boolean, float, int, long, strings	path of database-sqlite	path of database-sqlite	Paket data Capture pcap
Location	/Program files/Mozilla Firefox/Browser /Program Files/Google/Chrome/Application	/User/Administrotor/AppData /Local/Mozilla/Firefox/Profiles	/User/Administrator/AppData /Local/Google/Chrome/User Data	Log File in /data/files
Access Level	Administrator (image windows)	Administrator (image windows)	Administrator (image windows)	Network (Level layer)
Forensics Use	Sumber investigasi sumber data digital forensik	Sumber investigasi sumber data digital forensik	Sumber investigasi sumber data digital forensik	forensik data dari hasil capture network akses.

Database SQLite dapat digunakan sebagai pendukung tindakan investigasi digital dalam kaitannya membantu penyidik untuk mengumpulkan artefak Telegram Web. *Digital evidence* dengan database Telegram Web memiliki data yang dapat diekplorasi sebagai barang bukti diantaranya;

1) Web Browser Forensics (Mozilla) /Users/Administrator/AppData/Local/Mozilla/Firefox/Profiles
2) Web Browser Forensics (Chrome) /Users/Administrator/AppData/Local/Google/Chrome/User Data. Berdasarkan data SQLite yang ditemukan di sub-directory diatas selanjutnya akan diektraksi database percakapan Telegram Web dengan metode tertentu (pengklasifikasian teks) sesuai dengan barang bukti Telegram pada Smartphone.

IV. SIMPULAN

Telegram 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 Telegram baik itu Telegram *Smartphone* maupun Telegram Web. Sebagian besar aplikasi *chat* mengikuti pola sinkronisasi pesan, kontak dan data pengguna yang sama saat *sync* dan memperbarui data percakapan secara berkala. Pendekatan yang diambil memberi garis besar umum untuk semua aplikasi serupa yang berjalan di perangkat bersistem operasi Android maupun Windows seperti WhatsApp 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 Telegram dalam bentuk jurnal atau naskah lain sebagai literatur selanjutnya.

This Article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

JIKO (Jurnal Informatika dan Komputer)
Vol. 7, no. 2, September 2023, hal. 183–190
e-ISSN : 2477-3964 — p-ISSN : 2477-4413
DOI: dx.doi.org/10.26798/jiko.v7i2.789

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Bapak Tata Sutabri yang telah membimbing dan memberikan masukan serta dukungan secara moril dan materil sehingga penelitian dapat selesai pada waktunya

PUSTAKA

[1] DanielaWalnycky, Ibrahim Baggili, Andrew Marrington, Jason Moore, Frank Breitinger,(2015). Digital Investigation 14. 2015
[2] E.C., Turnbull. Digita l Evidence on Mobile Devices, In E.Casey, Digital Evidence and Computer Crime (3rd Edition ed.), Academic Press, 2011.
[3] J. Lyle, "Digital Forensic Research Conference TestingaDisk Imaging Tools." [Online]. 2016
[4] Mubarak Al-Hadadi and Ali AlShidhani. Smartphone Forensics Analysis: A Case Study International Journal of Computer and Electrical Engineering. 2013
[5] Guntur Maulana Zamroni, Rusydi Umar, Imam Riadi. Analisis Forensik Aplikasi Instant Messaging Berbasis Android. 2016
[6] Hartanto, AAT. Panduan Aplikasi Smartphone. Gramedia Pustaka Utama, 2010.
[7] M. Damshenas, A. Dehghantanha, R. Mahmoud. A survey on digital forensics trends, Int. J. Cyber Secur. Digit.Forensic.2014
[8] Tata Sutabri , E. Nopiyanti , Firman SA, AJ Susanto , N Setiyowati. Investigation Analysis Of Patient Safety Incident At X Hospital Jakarta. International Respati Health Conference (IRHC). 2019
[9] Tata Sutabri. Komputer Dan Masyarakat. Andi Offset. Jogjakarta. 2013
[10] Imam Riadi, Rusydi Umar and Arizona. Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method. International Journal of Computer Science and Information Security (IJCSIS). 2017
[11] N Anwar, I. R. (2016). Forensic SIM Card Cloning Using Authentication. Int. J. of Electronics and Information Engineering Vol.4, No.2, PP.71-81, 2016
[12] S. Mohtasebi, A. Dehghantanha. Defusing the hazards of social network services, Int. J. Digit. Inf. Wirel.Commun. 1.2011
[13] S. Mohtasebi, A. aDehghantanha, H.G. Broujerdi. Smartphone forensics: a case study with Nokia E5-00 mobilephone, Int. J. Digit. Inf. Wirel. Commun. 2012
[14] F.N. Dezfouli, A. aDehghantanha, B. Eterovic-Soric, K.-K.R. Choo. Investigating social networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms, Aust. J. Forensic Sci. 46(4). 2016

This Article is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.