Analisis Investigasi Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbasis Web

Rizki Budi Santoso

[1]*Jurusan Teknik Informatika Universitas Muhammadiyah Jember*
Jln. Karimata 49 Jember 68121 INDONESIA
[1]*rizkibudi72@gmail.com*

Abstrak*-Perkembangan telekomunikasi meningkat sangat pesat semenjak layanan pesan instan berbasis internet merambat cepat ke Indonesia. WhatsApp adalah aplikasi pesan instan paling populer dibanding layanan pesan instan lain, menurut situs website statista pengguna per Januari 2017 sebanyak 1,2 miliar orang secara aktif menggunakan aplikasi ini. Seiring pembaruan WhatsApp berbagai fitur disematkan dalam aplikasi ini diantaranya Whatsapp Berbasis Web untuk Komputer, fitur ini mempermudah pengguna dalam berbagi file tertentu serta dapat tersinkronisasi terhadap smartphone maupun komputer penggunanya. Disamping sisi positif yang didapati aplikasi, WhatsApp juga memberikan celah keamanan akan privasi penggunanya salah satunya yaitu penyadapan percakapan yang melibatkan kedua devices ; smartphone dan komputer. Penanganan tindak kejahatan yang melibatkan piranti digital perlu ditekankan sehingga dapat membantu proses peradilan akan efek yang ditimbulkannya. Investigasi Forensika Digital turut berperan serta terhadap penindakan penyalahgunaan fitur layanan pesan instan WhatsApp diantaranya langkah investigasi penanganan kasus penyadapan percakapan WhatsApp melalui serangkaian tahapan baku sesuai prosedur forensika digital. Eksplorasi barang bukti (digital evidence) percakapan WhatsApp akan menjadi acuan akan tindak kejahatan penyadapan telekomunikasi yang selanjutnya akan dilakukan report investigation forensics yang melibatkan barang bukti smartphone dan komputer korban.*

Kata kunci : *Forensik; Investigasi; WhatsApp Messenger Web.*

Pendahuluan

Pertumbuhan eksponensial media sosial dan aplikasi pesan instan telah memfasilitasi pengembangan banyak kejahatan *cyber* dan aktivitas jahat yang serius [12]. Penjahat dunia maya terus mengubah strategi mereka untuk menargetkan media sosial yang berkembang pesat dan pengguna pesan yang ketat. Penyalahgunaan media sosial dan pesan instan dalam layanan *mobile* memungkinkan penjahat dunia maya memanfaatkan layanan ini untuk tujuan jahat [14] seperti menyebarkan kode berbahaya, dan mendapatkan dan menyebarkan informasi rahasia. Banyak media sosial dan penyedia pesan instan telah memperluas layanan mereka ke *platform* empiris, [3] yang memperburuk situasi karena pengguna berada dalam bahaya kehilangan lebih banyak lagi informasi pribadi [8].

1.

Menurut data statistik *website statista* menunjukkan jumlah pengguna *WhatsApp* aktif bulanan di seluruh dunia per-Januari 2017. Pada bulan tersebut, aplikasi perpesanan *mobile* mengumumkan lebih dari 1,2 miliar pengguna aktif bulanan, naik dari lebih dari 1 miliar pada bulan Februari 2016. Layanan ini salah satu aplikasi seluler terpopuler di seluruh dunia. *WhatsApp* adalah layanan pesan cepat lintas *platform* untuk *smartphone* yang mengandalkan internet untuk pengiriman pesan. Berdasarkan model berlangganan berbiaya rendah, *WhatsApp* adalah alternatif yang murah untuk mengirim pesan teks melalui SMS, terutama

untuk pesan internasional atau grup. Aplikasi perpesanan *mobile* memungkinkan pengguna berbagi pesan teks, gambar dan video. Di Amerika Serikat, pengguna *WhatsApp* berjumlah 18,8 juta pengguna pada tahun 2016 dan diperkirakan akan tumbuh menjadi 25,6 juta pengguna pada tahun 2021.
[17]

WhatsApp adalah aplikasi pesan untuk *smartphone* yang mampu berjalan lintas *platform* diantaranya ; *Apple iOS, BlackBerry, Android, Symbian Nokia Series* 40 dan *Windows Phone*. *WhatsApp Messenger* menggunakan paket data internet sama halnya seperti layananan *email, browsing web*, dan layanan *instant messenger*s lainnya. Aplikasi *WhatsApp Messenger* menggunakan koneksi data *mobile* serta WiFi untuk melangsungkan komunikasi data, dengan menggunakan *WhatsApp*, seseorang dapat melakukan obrolan *online*, berbagi file, bertukar foto dan fitur lainnya yang menarik penggunanya. [5]

WhatsApp secara resmi mengumumkan peluncuran fitur resmi bernama *WhatsApp Web* pada tanggal 22 Januari 2015. Fitur ini mencoba memfasilitasi penggunaan aplikasi ini untuk pengguna berbasis komputer. Sepertihalnya *WhatsApp* berbasis *smartphone*, fitur ini membutuhkan koneksi internet sebagai jalur penyampaikan informasi. *WhatsApp* bekerja melalui portal *online* yang disediakan oleh domain. *WhatsApp Web* pada prinsipnya berfungsi untuk membuka akun *WhatsApp* melalui perangkat komputer. Fitur ini pada periode awal lebih mudah digunakan melalui aplikasi *browser*. Sinkronisasi dibutuhkan untuk membuka akun *WhatsApp* melalui *web*. Pengembang menyediakan *barcode* yang perlu dipindai melalui aplikasi *WhatsApp mobile*. Pemindaian akan secara langsung membuka aplikasi *Whatsapp* sesuai dengan akun yang berfungsi pada telepon genggam yang digunakan untuk pemindaian. Percakapan yang terdapat pada aplikasi *WhatsApp* di telepon seluler akan turut disajikan pada versi *web*. Sinkronisasi akan dilakukan secara otomatis apabila terjadi perubahan pada salah satu aplikasi yang aktif. [16]

Mubarak Al-Hadadi and Ali AlShidhani (2013). Forensik *Smartphone* adalah bagian dari forensik digital, dan mengacu pada penyelidikan dan perolehan artefak pada *smartphone*. Ancaman baru terhadap ponsel membuat ilmu forensik menjadi tantangan yang menantang dalam beberapa tahun terakhir. Jumlah pengguna ponsel meningkat di seluruh dunia dan menimbulkan masalah dan tantangan yang luar biasa. Literatur yang relevan dengan forensik *smartphone*, fokus penelitian ini pada arsitektur sistem operasi *smartphone* dan teknik antiforensik. Ini juga membahas bukti digital dari aplikasi *smartphone*. Dalam penelitian ini, melalui pertimbangan jenis kejahatan yang melibatkan *smartphone*, sebuah studi kasus nyata dari Negara Kesultanan Oman dipresentasikan. Studi kasus ini melakukan eksperimen praktis terhadap sumber yang teridentifikasi untuk bukti yang nantinya dapat digunakan dalam sistem peradilan.[9]

Imam Riadi, Rusydi Umar and Arizona Firdonsyah (2017). Teknologi *smartphone* semakin populer pertahunnya. Salah satu teknologi dengan jumlah pengguna yang terbanyak adalah *smartphone* berbasis *android*s sebagai sistem operasinya. Android cukup kompetitif di dalam pasar *smartphone*. Jumlah pengguna *smartphone android* juga memberi efek untuk pengembangan dan penggunaan aplikasi *mobile*, termasuk aplikasi *instant messenger* diantaranya aplikasi yang banyak digunakan adalah *Blackberry Messenger* (selanjutnya disingkat sebagai BBM). Meningkatnya jumlah pengguna BBM tentu membawa efek positif dan negatif, salah satunya efek negatifnya adalah beberapa orang yang menggunakan BBM melakukan meningkatkan tindak kejahatan digital seperti pornografi dan kecurangan, jika *smartphone* menjadi bukti dalam kasus pidana dan BBM dipasang di *smartphone* itu, di sini aplikasi bukti digital dapat diidentifikasi dan dapat juga diharapkan menjadi pilihan untuk membantu penegakan hukum dalam mengungkap kejahatan digital. Adapun cara penelitian ini dilakukan dengan berbagai macam metode yang dapat digunakan dalam proses analisis forensik dan Identifikasi bukti digital, metode yang digunakan dalam penelitian ini adalah metode forensik *mobile* yang didasarkan pada ketersediaan pedoman yang disiapkan oleh *National Institute of Standards* dan Teknologi (NIST). Hasil penelitian disajikan pada bentuk rekaman percakapan, BBM *Personal Identification* Nomor (PIN BBM), nama pengirim dan penerima, dan waktu percakapan *(timestamp)* diharapkan dapat memberikan Ikhtisar langkah-langkah yang dapat diterapkan di bidang analisis forensik *android*.[6]

Thakur, Neha S (2013). Forensik *Android* telah berkembang dari waktu ke waktu dengan menawarkan peluang dan tantangan menarik yang signifikan. 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 *'WhatsApp'*, aplikasi jejaring sosial yang populer. Penelitia akan membentuk garis besar tentang bagaimana penyidik forensik dapat mengekstrak informasi yang berguna dari *WhatsApp* dan dari aplikasi serupa yang terpasang di *platform* Android. Area fokus penelitian adalah ekstraksi dan analisis data pengguna aplikasi dari penyimpanan eksternal *non-volatile* dan memori *volatile* (RAM) perangkat Android.[15]

Guntur Maulana Zamroni, Rusydi U, Imam R (2016). *Instant Messaging* (IM) merupakan salah satu aplikasi seluler yang sangat popular. Salah satu jenis aplikasi IM adalah *WhatsApp* (WA). Pengguna WA jumlahnya mencapai 1 Milyar setiap bulannya. WA didukung oleh fitur enkripsi untuk menjamin keamanan data para penggunanya. Kepopuleran dan fitur yang diberikan WA dapat disalahgunakan masyarakat untuk tujuan kriminal, seperti perdagangan narkoba, kegiatan teroris, perencanaan pembunuhan, dan kegiatan kriminal lainnya melalui fiturfitur yang tersedia. Pihak berwenang dapat menggunakan data-data dalam WA sebagai barang bukti. Metode forensik diperlukan untuk memastikan keberhasilan proses pengambilan data-data tersebut. Penelitian ini akan menjelaskan langkah-langkah untuk memperoleh data aplikasi WA, dari data yang telah dienkripsi menjadi data yang dapat dibaca dan dianalisis untuk kemudian dapat digunakan sebagai barang bukti. [4]

Daniel Walnycky (2015). 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 *WhatsApp Messengersmartphone* terhadap *WhatsApp* berbasis *Web* dengan studi kasus penyadapan percakapan *WhatsApp*, 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 evidence* yang relevan dengan pengguna media sosial dan aktivitas instan *Messenger*[13]. Namun, perbedaan antara perangkat *smartphone* menjadi tantangan penyidik atau investigator forensik untuk mengembangkan metode dan teknik yang disesuaikan untuk penyelidikan berbagai kasus *cybercrime*[11].

2. Metode Penelitian

Data *WhatsApp* disimpan dalam memori Internal *smartphone* setelah *pekage installer WhatsApp* ter-*install*, secara otomatis sinkronisasi dengan kontak telepon menunjukkan pengguna yang sudah menggunakan *WhatsApp*. Saat ponsel dengan *installer WhatsApp* dihidupkan, Proses *"com.whatsapp"* menerima sinyal untuk memulai layanan *'ExternalMediaManage'* dan *'MessageService'* yang Berjalan di latar belakang telepon sampai telepon dinyalakan. Dengan dukungan versi baru *WhatsApp Web* yang berjalan dikomputer, setelah dilakukan scan *QR Code WhatsApp* yang terjadi sinkronisasi dengan aplikasi *WhatsApp on Smartphone* baik itu kontak telepon, percakapan dan data yang melekat di *smartphone* penggunanya dapat pula diakses melalui *WhatsApp Web*. Hal ini menunjukkan pengguna yang sudah menggunakan *WhatsApp Web* memiliki tingkat *vulnerability*, dimana pesan *WhatsApp* yang terdapat di *smartphone* dapat pula diakses di *WhatsApp 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 *WhatsApp smartphone* dan komputer adalah intervensi pihak yang terlibat penyalahgunaan layanan (penyadapan aplikasi *dual WhatsApp*), sehingga muncul gagasan atau desain dan rancangan usulan *WhatsApp Investigation* meliputi beberapa kompunen utama baik tahapan investigasi serta ditekankan pada poin dasar diantaranya meliputi :

- *WhatsApp Evidence* ; berupa fisik dari *smartphone* dan komputer korban beserta tindak kriminal dan penanganannya.
- *Riset Goal Investigation Methode* ; proses penanganan barang bukti dari memperoleh, akuisisi serta merepresentasikan skema kasus.
- *Forensics Tools Investigator* ; merupakan *software forensic* dalam hal ekplorasi, eksaminasi dan *reporting* berkenaan terhadap barang bukti penyadapan *WhatsApp.*
- *Digital Evidence Risk* ; Resiko yang ditimbulkan pasca penyadapan berupa layanan *WhatsApp ; Chat, File Sharing* dan sinkronisasi, serta komputer *browser (WhatsApp Web)* memerlukan penanganan yang lebih terkait akuisisi data dari *WhatsApp Web* tersebut.

Tahapan proses penanganan investigasi penyadapan *WhatsApp* setelah dikondisikan terhadap skema kasus serta pengembangan tahapan investigasi *mobile forensik* dan *network* forensik maka dapat diperoleh tahapan seperti pada tabel 1 :

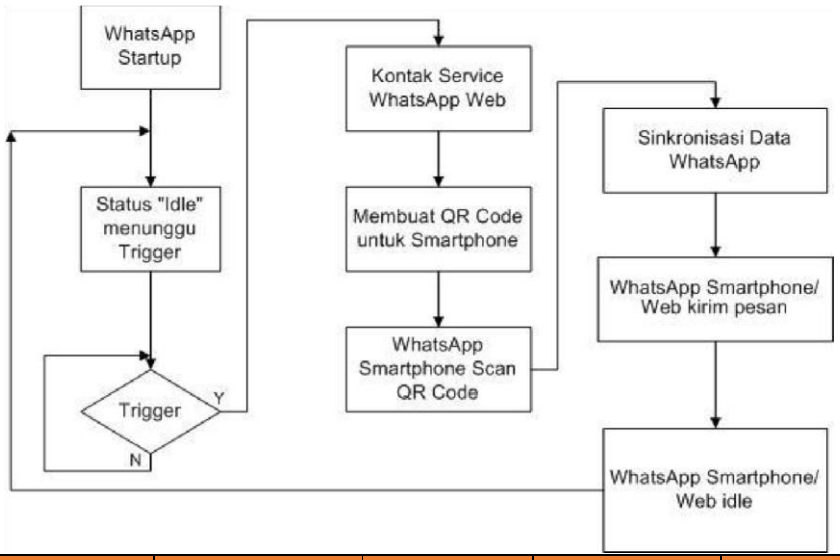
Tabel 1. Proses Investigasi Penyadapan Percakapan WhatsApp [10]

Identification	Preservation	Collection	Examination	Analysis	Presentation
Identifikasi kejahatan WhatsApp	Pengolahan kasus WhatsApp	Pengaman an barang bukti WhatsApp	Pelacakan barang bukti WhatsApp	Komparasi data investigasi	Dokumentasi
Profil kejahatan WhatsApp	Chain of custody/ kronologis WhatsApp Attack	Teknik investigasi WhatsApp	Validasi barang bukti WhatsApp	Pengolahan temuan barang bukti	Klarifikasi invistigator
Audit dan analisa kasus	Manajemen waktu investigasi		Filtering barang bukti		Pernyataan, saran dan tindakan
	Pengolahan kasus WhatsApp		Pencocokan barang bukti		Interpretasi data WhatsApp
			Penemuan data tersembunyi		

Berdasarkan Tabel 1. Proses Investigasi penyadapan percakapan *WhatsApp* diatas diperoleh penekanan pada poin yang diberi tanda warna Simulasi penyadapan percakapan *WhatsApp* dari Gambar diatas difokuskan pada sinkronisasi data baik data *WhatsApp* 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 *rectangle* diatas.

berbeda, sebagai tahapan yang memerlukan penanganan yang lebih menurut porsi atau peran investigator digital forensik khususnya *smartphone* dengan aplikasi *WhatsApp*.

2.1. Simulasi Penyadapan Percakapan WhatsApp



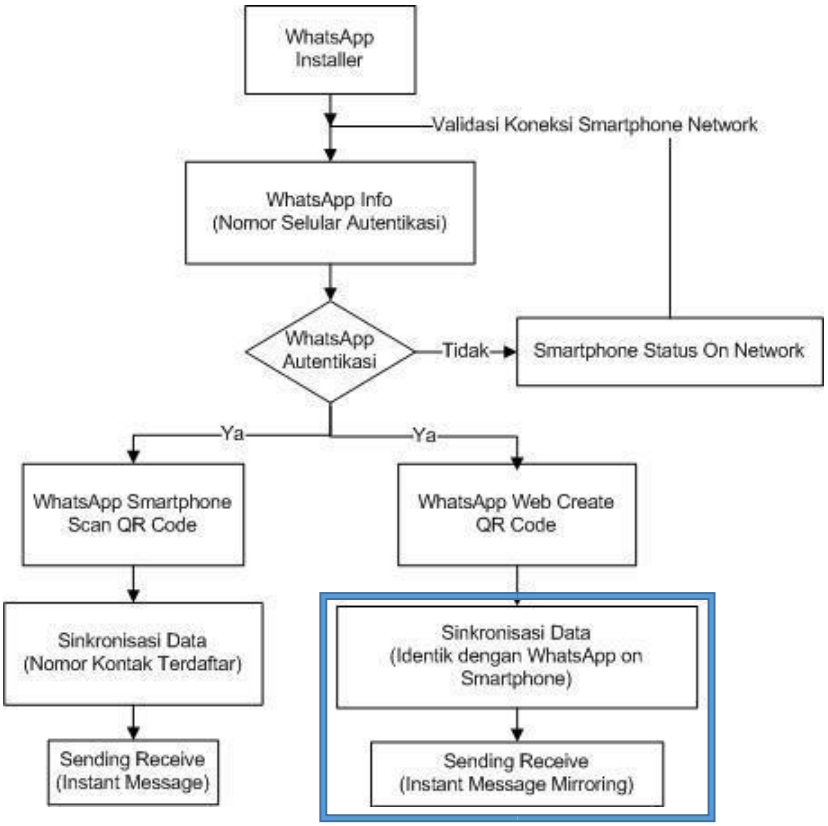
Gambar 1. Alur Kerja Serangan WhatsApp

Rancangan simulasi penyadapan percakapan *WhatsApp* dalam hal ini akan dijelaskan skema pengujian aplikasi *WhatsApp* sebagai dalam hal ini menyangkut keberadaan barang bukti digital pasca terjadi penyadapan, sehingga diketahui respon terhadap masing-masing aplikasi antara *WhatsApp pada Smartphone* terhadap *WhatsApp Web* tampak seperti Gambar 1.

2.2. Flowchart Serangan WhatsApp

Flowchart Penyadapan *WhatsApp* merupakan penyesuaian terhadap simulasi penyadapan percakapan WhatsApp 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*

WhatsApp dari Gambar 1. berupa diagram alir dari seluruh proses *Traffic Chanel Attack* untuk selanjutnya dikomparasi dengan keadaan terjadinya penyadapan melalui pesan singkat *WhatsApp* sesaat setelah dilakukannya *Attack* yang sesuai dengan tema penelitian sehingga diperoleh diagram alur proses baru yang sesuai dengan penelitian terkait WhatsApp yang melibatkan penyalahgunaan wewenang layanan telekomunikasi yakni dalam hal ini membaca pesan tanpa sepengetahuan pemilik akun (penyadapan) serta pelaku juga dapat mengirim pesan *WhatsApp*, sehingga tercipta alur proses baru seperti tampak pada diagram proses pada Gambar 2 dibawah.



Gambar 2. *Flowchart* Penyadapan WhatsApp

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

WhatsApp tidak akan memperoleh data yang terbarukan *up to date* pasca sinkronisasi data *WhatsApp*. Skema tersebut dapat diperjelas pada *flowchart* penyadapan percakapan *WhatsApp*, yang berkaitannya dengan tingkat kerentanan atau *vulnerability* sebuah aplikasi pesan *instant*.

Dengan diterapkannya metode investigasi *WhatsApp* forensik yang melibatkan skema proses yaitu *pentest WhatsApp attack* dan *flowchart* penyadapan *WhatsApp* maka akan diperoleh hasil perbandingan investigasi terhadap dua *devices* mencakup *WhatsApp on Smartphone* dengan sistem operasi *Android* dan *WhatsApp 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 *WhatsApp massanger*.

3. Analisis dan Hasil

Digital Forensik dengan barang bukti *WhatsApp* pada *Smartphone* dan *WhatsApp 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 barang bukti, penanganan, ekplorasi sampai pelaporan investigasi.

3.1. Android (Mobile Forensics)

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*.

Menurut E.Casey Tumbull, menjelaskan mengapa perangkat *mobile* merupakan sumber berharga sebagai bukti digital dan berisi informasi penting yang tidak tersedia pada perangkat lain. Selain itu sifat personaliti dari perangkat tersebut membuatnya mudah untuk membuktikan jejak yang mengaitkan perangkat ke individu [2]

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 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 ekternal seperti *MicroSD card* untuk dapat dibaca komputer, atau memerlukan format yang yang sangat spesifik dalam penggunaannya.

Internal Storage

Mobile Forensics Investigation dalam mengektraksi internal memori *smartphone* menggunakan *Oxygen forensic* dikarenakan *tools Oxygen* mengekstrak semua aplikasi didalam *smartphone* tak terkecuali *WhatsApp* yang dijadikan barang bukti penyadapan. Hal ini dapat terjadi diakibatkan *smartphone android* melakukan sinkronisasi *account* dengan *phonebook*. Proses sinkronisasi nantinya akan dikaitkan dengan aplikasi *WhatsApp*
Web yang terdapat pada forensik *browser* pada komputer ber-*platform windows*

External Storage

Pada proses investigasi pada ekternal memori dilakukan secara manual. Ekstraksi berbeda bila dibandingkan dengan mengekstraksi data pad *smartphone*. Proses ini dilakukan dengan membuat *image* dari *digital evidence MicroSD card* dengan menggunakan *tools FTK Imager* beserta proses analisisnya.

Network Capture (Simulasi Penyadapan Percakapan WhatsApp)

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 *WhatsApp Messenger Smartphone Android* dapat disajikan seperti tabel 2 :

Tabel 2. Android WhatsApp Forensics

"Android" WhatsApp Application 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 accses)

Data Type	Integer, double, string,float, booelan dan string	Ekstraksi data (digital evidence)	Ekstraksi data (digital evidence)	hex values

Tabel 3. Android WhatsApp Forensics (Lanjutan)

Location	/data/data/com.android.phone/shared_prefs	/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 forensik (jika root access)	Sumber data forensik (jika root access)	Sumber data forensik (digital evidence)	Sumber data forensik (log digital evidence)

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

- *File msgstore.db* terletak di stuktur file android *"/data/data/com.whatsapp"* yang menyimpan pesan yang dikirim maupun diterima oleh pengguna aplikasi *WhatsApp Smartphone*.
- *File wa.db* terletak di lokasi yang sama *"/data/data/com.whatsapp"* dan menyimpan semua kontak *WhatsApp.*

3.2. Windows (Computer Forensics)

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 *(Analys)*, 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 *WhatsApp Web* dalam membaca aplikasi sejenis pada *smartphone* dalam kaitannya litigasi tindak kejahatan *cybercrime*. Sama halnya *tools* akuisisi pada ekternal 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 barang bukti digital, FTK mampu membuat *file hash* SHA1 atau MD5, mengekspor *file* dan *folder* dari *images* forensik ke *disk partition*, meninjau dan memulihkan *file* yang telah dihapus dari *Recycle Bin* (dengan syarat blok data mereka belum ditimpa), dan *mount images* forensik untuk melihat isinya di *Windows Explorer*.

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.

Restore Evidence dari SQLite Database

Struktur *database* rekaman tentang pengguna *WhatsApp* 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 *WhatsApp web*.

Network Capture (Simulasi Penyadapan Percakapan WhatsApp)

Wireshark Analys adalah *tools* yang ditujukan untuk melakukan analisa paket data jaringan. *Wireshark* melakukan monitoring paket secara *real time* selanjutnya *Wireshark* melakukan penangkapan data dan menampilkannya selengkap

mungkin. Keseluruhan dari proses ekplorasi serta temuan dari investigasi *web browser* terkait *WhatsApp web* dapat disajikan seperti tabel 4 :

Tabel 4. Windows WhatsApp Web Forensics

"Windows" WhatsApp Web Application Browser Forensics				
	System Windows	**Web Browser Forensics (Mozilla)**	**Web Browser Forensics (Chrome)**	**Network Capture**
File Type stored	Databases On System	Cookies.sqlite formhistory.sqlite content-prefs.sqlite	Cookies.sqlite formhistory.sqlite content-prefs.sqlite	Paket data captured network
Data Type	boolean, float, int, long, strings	Path of database .sqlite	Path of database .sqlite	Paket data captured .pcap
Location	\Program Files\Mozilla Firefox\browser \Program Files\Google\Chrome\Application	\Users\Administrator\AppData\Local\Mozilla\Firefox\Profiles	\Users\Administrator\AppData\Local\Google\Chrome\User Data	Log files in/data/data/files
Access Level	Administrator (image windows)	Administrator (image windows)	Administrator (image windows)	Network (level layer)
Forensic Use	Sumber investigasi data digital forensik	Sumber investigasi data digital forensik	Sumber investigasi 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 *Whatsapp Web*. *Digital evidence* dengan *database WhatsApp Web* memiliki data yang dapat diekplorasi sebagai barang bukti diantaranya ;

- *Web Browser Forensics (Mozilla) \Users\Administrator\AppData\Local\Mozilla\ Firefox\Profiles*
- *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 *WhatsApp Web* dengan metode tertentu (pengklasifikasian teks) sesuai dengan barang bukti *WhasApp* pada *Smartphone.*

4. Kesimpulan

WhatsApp telah menjadi aplikasi populer untuk jejaring sosial dimana orang dapat bertukar informasi pribadi beserta mobilitas yang mereka geluti. Penelitian ini telah menunjukkan bahwa seseorang dapat memperoleh akses lengkap ke semua informasi di *WhatsApp* baik itu *WhatsApp Smartphone* maupun *WhatsApp Web*. Sebagian besar aplikasi *chat* mengikuti pola sinkronisasi pesan, kontak dan data pengguna yang sama saat *syinc* dan memperbarui data percakapan secara berkala. Pendekatan yang diambil memberi garis besar umum untuk semua aplikasi serupa yang berjalan di perangkat ber-*platform Android* maupun *Windows* seperti *Telegram* dan sejenisnya. Penelitian ini dapat bermanfaat untuk *Mobile Forensic Analysis* dan *Investigation* pada *smartphone Android* dan aplikasi ganda berbasis *web browser*. *Database QR Code* membutuhkan autentikasi terhadap *smartphone* hanya sekali setiap saat *login* pertama kali sehingga dibutuhkan kewaspadaan penggunanya seperti penggunaan *pattern lock* pada *smartphone* dan *login user password* pada komputer penggunanya. Proses akuisisi langsung

terhadap *smartphone* korban dan analisis *web browser* pada komputer. Diharapkan kedepan lebih banyak penelitian yang dapat dilakukan pada interpretasi data percakapan *WhatsApp* dalam bentuk jurnal atau naskah lain sebagai literatur selanjutnya.

Referensi

[1] Daniel Walnycky, Ibrahim Baggili, Andrew Marrington, Jason Moore, Frank Breitinger,(2015). *Digital Investigation 14* (2015) S77eS84. DFRWS 2015 USA Network and device forensic analysis of Android social-messaging applications

[2] E.C., Turnbull, (2011). *Digital Evidence on Mobile Devices*, In E.Casey, Digital Evidence and Computer Crime (3rd Edition ed.), Academic Press, 2011.

[3] F.N. Dezfouli, A. Dehghantanha, B. Eterovic-Soric, K.-K.R. Choo, (2016). *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) 469–488, http://dx.doi.org/10.1080/00450618.2015.1066854.

[4] Guntur Maulana Zamroni, Rusydi Umar, Imam Riadi. *Analisis Forensik Aplikasi Instant Messaging Berbasis Android*. (2016). http://seminar.ilkom.unsri.ac.id/index.php/ars/article/view/808/741

[5] Hartanto, AAT. *Panduan Aplikasi Smartphone*, halaman 100. Gramedia Pustaka Utama, 2010. ISBN 100-6762-33-5

[6] Imam Riadi, Rusydi Umar and Arizona. (2016). *Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method*. International Journal of Computer Science and Information Security (IJCSIS), Vol. 15, No. 5, May 2017

[7] M. Damshenas, A. Dehghantanha, R. Mahmoud,(2014). *A survey on digital forensics trends*, Int. J. Cyber Secur. Digit.Forensic. 3 (2014) 1–26.

[8] M. Taylor, G. Hughes, J. Haggerty, D. Gresty, P. Almond, (2012). *Digital evidence from mobile telephone applications, Comput. Law Secur*. Rev. 28 (2012) 335–339, http://dx.doi.org/10.1016/j.clsr.2012.03.006.

[9] Mubarak Al-Hadadi and Ali AlShidhani. (2013). *Smartphone Forensics Analysis: A Case Study* International Journal of Computer and Electrical Engineering, Vol. 5, No. 6, December 2013

[10] 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, June 2016 , 71-81.

[11] S. Mohtasebi, A. Dehghantanha, (2011). *A mitigation approach to the privacy and malware threats of social network services*, in : Digital Information Processing and Communications, Communications in Computer and Information Science, vol. 189, Springer, Berlin, Heidelberg, 2011, pp. 448–459, http://dx.doi.org/10.1007/978-3-642-22410-2_39.

[12] S. Mohtasebi, A. Dehghantanha, (2011). *Defusing the hazards of social network services*, Int. J. Digit. Inf. Wirel.Commun. 1 (2011) 504–516.

[13] S. Mohtasebi, A. Dehghantanha,(2013). *Towards a unified forensic investigation framework of smartphones*, Int. J. Comput. Theory Eng. 5 (2013) 351–355, http://dx.doi.org/10.7763/IJCTE.2013.V5.708.

[14] S. Mohtasebi, A. Dehghantanha, H.G. Broujerdi,(2012). *Smartphone forensics: a case study with Nokia E5-00 mobilephone*, Int. J. Digit. Inf. Wirel. Commun. 1 (2012) 651–655.

[15] Thakur, Neha S., *Forensic Analysis of WhatsApp on Android Smartphones* (2013). University of New Orleans Theses and Dissertations. Paper 1706.

[16] http://ensiklo.com/2015/01/bagaimana-cara-instalasi-whatsapp-untuk-desktop-pc-atau komputer/ (Senin 01 Juni 2017 12.23)

[17] https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/
(Minggu, 18 Juni 2017 05.08)