Identifikasi Bukti Digital pada Akuisisi Perangkat Mobile dari Aplikasi Pesan Instan "WhatsApp"

Ayubi Wirara [1)], Bangkit Hardiawan 2[2)], Muhammad Salman[3)]

Departemen Teknik Elektro, Fakultas Teknik Universitas Indonesia [1)]
Badan Siber dan Sandi Negara, Jakarta [2)]
Departemen Teknik Elektro, Fakultas Teknik Universitas Indonesia [3)]
E-Mail: ayubi.wirara@ui.ac.id; ayubi.wirara@bssn.go.id[1)], bangkit.hardiawan@bssn.go.id[2)], muhammad.salman@ui.ac.id[3)]

ABSTRAK

Aplikasi pesan instan menjadi salah satu alasan utama untuk seorang pengguna menggunakan internet. Saat ini WhatsApp menjadi aplikasi pesan instan dengan pengguna terbesar di indonesia karena beragam fitur yang telah didukung. Hal ini tentu saja membuat WhatsApp bukan hanya digunakan untuk bertukar informasi biasa tapi juga informasi terkait kasus kejahatan. Sehingga bukti digital aplikasi pesan instan WhatsApp pada smartphone menjadi potensial dalam berbagai kasus kriminal dan proses persidangan. Pada penelitian ini dilakukan analisis terhadap bukti digital whatsapp yang dapat diperoleh dalam proses akuisisi perangkat smartphone. Target perangkat yang diakuisisi pada penelitian ini adalah smartphone berbasis android dan iOS. Hasil ekstraksi didapatkan beberapa bukti digital aplikasi WhatsApp yang berhasil didapatkan meskipun perangkat tidak dilakukan proses root/jailbreak terlebih dahulu.

Kata kunci: aplikasi pesan instan, WhatsApp, forensik digital

Identification Digital Evidence on Acquisition of Mobile Device from Instant Messaging Application "WhatsApp"

ABSTRACT

Instant messaging applications are one of the main reasons for a user using the internet. Currently WhatsApp is an instant messaging application with the biggest users in Indonesia because of the various features that are supported. This is surely make WhatsApp not only used to exchange ordinary information but also information related to crime cases. So, digital evidence instant messaging applications WhatsApp on smartphones has the potential to lead to criminal cases and legal proceed. In this research an analysis of whatsapp digital evidence can be obtained in the acquisition process smartphone devices. The target devices acquisition in this research are smartphone based Android and iOS. The extraction results obtained some digital evidence of the WhatsApp application that was successfully obtained even though the device was not root / jailbreak first.

Keywords: Instant messaging application, WhatsApp, Digital Forensics

1. Pendahuluan

Berdasarkan laporan statistik per Januari 2019 dari Hootsuite dan We are social, (2019, 30 Januari) pun didapatkan dari 268 juta populasi 150 juta atau sebanyak 56% sebagai pengguna internet. Hal tersebut membuat semakin pesatnya perusahaan menciptakan aplikasi – aplikasi yang menggunakan media internet untuk menghubungkannya.

Salah satu aplikasi yang mengalami perkembangan yang sangat pesat adalah aplikasi *chatting* atau pesan instan. Perkembangannya yang sangat pesat saat ini telah menggeser penggunaan layanan *Short Message Service* (SMS) yang terbatas hanya dalam bentuk pesan teks dan panjang hanya 160 karakter. Salah satu aplikasi pesan instan yang saat ini banyak digunakan terutama di Indonesia adalah WhatsApp. Saat ini juga

beragam fitur telah tersedia bukan hanya pesan teks, tapi juga panggilan suara, panggilan video, gambar, suara, lokasi hingga dokumen berukuran besar dengan maksimal 100 MB. Sehingga tidak dapat dipungkiri saat ini orang – orang lebih memilih menggunakan WhatsApp untuk mengirim sebuah file/dokumen dibandingkan dengan penggunaan surat elektronik (e-mail).

Menurut Walnycky dkk (2015), bukti digital berupa aplikasi pesan instan seperti WhatsApp pada smartphone menjadi sangat potensial dalam beragam jenis kasus kriminal dan proses persidangan. Hal ini dikarenakan WhatsApp menawarkan kepada pengguna alternatif pengiriman pesan teks sekaligus bermacam fitur didalamnya yang sebelumnya telah disebutkan.

Selain kasus kriminal, WhatsApp juga digunakan dalam penyebaran konten negatif, terutama hoaks. Seperti data yang telah dilansir pada situsnya kominfo.go.id (Tri Haryanto, Agus), pada 24 Januari 2019, pada tahun 2018 terdapat 1.440 aduan konten negatif dimana tiga terbesar adalah sebanyak 733 aduan terkait konten yang meresahkan (hoaks), 162 aduan terkait penipuan, dan 151 aduan terkait fitnah.

Beberapa penelitan terkait analisa forensik pada aplikasi chat WhatsApp diantaranya adalah pada tahun 2014 Cosimo Anglano (2014) melakukan analisis forensik pada WhatsApp di smartphone android dengan hasil ekstraksi didapatkan beberapa informasi maupun artefak dan juga lokasi tempat penyimpanan informasi tersebut. Pada tahun 2016, Syukur I., dan Bekti C. (2016) membandingkan hasil ekstraksi database dan keamanan WhatsApp dan LINE. Pada tahun 2017 Rusydi Umar, dkk (2017) membandingkan tiga tools forensik (WhatsApp DB/Key Extractor, Belkasoft Evidence, dan Oxygen Forensic) dengan hasil Belkasoft Evidence memiliki indeks tertinggi terhadap NIST parameter dari ketiga tools tersebut (Rusydi Umar, dkk, 2017).

Meskipun begitu, dirasa perlu dilakukan pengembangan penelitian terkait analisa forensik pada WhatsApp terkait fitur *update* serta beberapa kondisi yang memungkinkan terjadi dalam kasus kriminal misal penerusan chat, penghapusan, ambil alih (*hijack*) akun. Pada paper ini bukan hanya dilakukan analisa pada perangkat android tapi juga menganalisa pada perangkat iOS. Proses akuisisi dibantu oleh *tools* digital forensik yang telah umum digunakan para ahli digital forensik. Penelitian ini diharapkan dapat memberikan kontribusi untuk mengetahui jejak digital yang ditinggalkan WhatsApp pada perangkat android dan iOS.

2. Landasan Teori

2.1. WhatsApp

WhatsApp merupakan salah satu aplikasi pesan yang paling banyak digunakan untuk penyampaian pesan teks maupun konten (audio, video, gambar, lokasi, dan kontak) secara gratis, yang telah digunakan hampir 800 juta pengguna dan telah dibeli oleh facebook pada tahun 2014 seharga 19 miliar dollar (Karpisek dkk, 2015). Pada tahun 2016 (WhatsApp Inc.), WhatsApp telah mengklaim bahwasanya kirim terima pesan, voice dan video call antara pengirim dan penerima telah dilakukan proses enkripsi secara *end-to-end* untuk versi WhatsApp yang dikeluarkan diatas 31 Maret 2016.

WhatsApp sendiri menyimpan semua percakapannya dalam sebuah database di masing – masing perangkat pengguna WhatsApp. Aplikasi WhatsApp telah menerapkan enkripsi untuk melindungi file database-nya. Format file database terenkripsi WhatsApp adalah *msgstore.db.crypt* yang saat ini telah menggunakan *crypt12*. Secara *default*, file *msgstore.db.crypt* disimpan di perangkat dalam direktori *SDcard /WhatsApp /Databases*. Untuk melakukan dekripsi database WhatsApp tersebut diperlukan *filekey* yang disimpan dalam */data/data/com.whatsapp/files/* yang dapat diperoleh jika telah mendapatkan akses sebagai *root* (Yesi dan Anggie, 2017).

2.2. Digital Forensik

Digital forensik (Sengul dan Erhan, 2017) didefinisikan sebagai analisis data

seperti audio, video, dan lainnya yang diperoleh setelah dilakukan pemeriksaan perangkat elektronik untuk membantu dalam proses hukum. Di Indonesia sendiri bukti digital atau informasi elektronik dan/atau dokumen elektronik dalam UU ITE nomor 11 tahun 2008 pada pasal 5 ayat (1) telah menjadi alat bukti hukum yang sah.

2.3. *Mobile* Forensik

Menurut Ntantogian, dkk (2014) mobile digital forensik atau mobile forensik merupakan cabang forensik digital yang berkaitan dengan pemulihan bukti atau data digital dari perangkat seluler dengan kondisi *forensically sound*.

Terdapat banyak tantangan dan kesulitan yang dihadapi dalam mendapatkan bukti digital dalam perangkat seluler. Beberapa diantaranya menurut Sai, dkk (2015) adalah perbedaan hardware mobile phone, fitur keamanannya, kurangnya sumber daya, seperti kabel USB, baterai, dan charger untuk perangkat mobile yang berbeda, teknik anti-forensik, bukti yang dinamis atau dengan mudah berubah, adanya proses reset secara tidak sengaja, perubahan perangkat, pemulihan *passcode*, dan program *malicious*.

2.4. Proses Digital Forensik

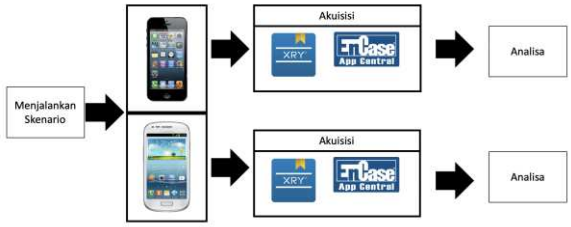
Menurut NIST SP 800-86 (2006) proses tahapan dalam digital forensik dibagi menjadi empat tahapan. Keempat tahapan tersebut adalah sebagai berikut.

1. *Collection,* merupakan tahapan pertama dalam proses digital forensik yang bertujuan untuk mengidentifikasi sumber data yang potensial dan mengakuisisi datanya.
2. *Examination,* merupakan tahapan pemeriksaan data – data yang termasuk didalamnya adalah penilaian dan penggalian informasi dari data yang telah dikumpulkan sebelumnya.
3. *Analysis, merupakan* proses analisis dari data yang dapat mengidentifikasi orang, tempat, item, dan peristiwa yag terkait sehingga dapat diambil kesimpulan.
4. *Report*, merupakan proses dalam mempersiapkan dan mempresentasikan informasi yang dihasilkan dari fase analisis.

Secara khusus alur proses untuk *mobile* forensik sendiri menurut Jones dan Winster (2017) terdiri atas *seizure*, *acquisition*, *examination/analysis*, dan *report generating*. *Seizure* bertujuan untuk menjaga barang bukti, *acquisition* bertujuan untuk mengambil data dari perangkat, *examination/analysis* merupakan proses pemeriksaan dan analisis dari data, dan *report generating* merupakan pelaporan hasil / informasi dalam bentuk *non-technical*.

3. Metodologi

Metode penelitian dilakukan dengan terlebih dahulu melakukan instalasi aplikasi WhatsApp pada perangkat mobile phone. Pada penelitian ini mobile phone yang digunakan tidak dilakukan proses *Root / Jailbreak*. Proses *Root* merupakan suatu proses untuk mendapatkan *high privilege* dalam suatu OS sehingga secara virtual dapat melakukan apapun seperti *unmounting file systems*, *killing* proses, atau menjalankan beberapa *command* (Nguyen-vu dkk, 2017). Proses *jailbreak* merupakan proses yang mengizinkan pengguna untuk melakukan instalasi dan eksekusi aplikasi yang tidak diizinkan oleh apple (Ovens dan Morison, 2016). Selanjutnya dijalankan skenario percakapan yang telah disiapkan pada Tabel 1. Setelah dijalankan skenario tersebut, dilakukan akuisisi dan ekstraksi pesan dengan menggunakan *tools* forensik. Selanjutnya adalah dilakukan proses analisa dari data yang berhasil diekstraksi. Berikut adalah alur metodologi penelitiannya.



Gambar 1. Alur Metodologi Penelitian

3.1. Skenario Percakapan

Berikut adalah *list* skenario yang dijalankan pada penelitian ini.

Tabel 1. Skenario Percakapan Penelitian

No	Skenario
1	Transmisi, hapus, dan meneruskan chat teks
2	Transmisi, hapus, meneruskan attachment
3	Grup chat
4	Pengambilalihan akun

3.2. Perangkat dan Tools Aplikasi yang digunakan

Berikut adalah perangkat mobile phone yang digunakan dan dilakukan akuisisi pada penelitian ini.

3.2.1 Android Mobile Phone
- Merk: Samsung Galaxy S3 mini
- Model: GT-I8190N
- Versi Android: 4.1.2 (Jelly Bean)2.19.188
- Versi WhatsApp yang diinstall: 2.19.188

3.2.2 iOS Mobile Phone
- Merk: iPhone 5
- Model: A1429
- Versi Android: 8.1.2
- Versi WhatsApp yang diinstall: 2.19.50

3.2.3 Laptop Intel (R) Core (TM) i7-7700HQ CPU @ 2.80 GHz, RAM 16 GB untuk proses mobile forensik.

Tools yang digunakan dalam melakukan akuisisi data pada perangkat mobile, adalah:
1. XRY version 8.0.0
2. Encase Mobile Forensic version 8.09.00.192

4. Hasil Dan Pembahasan

4.1. Analisis Artefak WhatsApp

Hasil proses akuisisi yang dilakukan terhadap mobile phone baik Android maupun iOS didapatkan artefak yang mengandung informasi percakapan WhatsApp. Beberapa artefak kunci yang dibutuhkan dalam proses investigasi pada perangkat android terdapat dalam database SQLite *msgstore.db* dan *wa.db* (Lone dkk, 2015). Sementara pada perangkat iOS terdapat dalam database *ChatStorage.sqlite* dan *ContactsV2.sqlite*. Semuanya tersebut terangkum dalam Tabel 2 berikut.

Tabel 2. Artefak WhatsApp Pada Android dan iOS

Artefak	Android Mobile Phone	iOS Mobile Phone
Directory Database	/data/data/com.whatsapp/databases	/private/var/mobile/Containers/Shared/AppGroup/group.net.whatsapp.WhatsApp.shared/
Database Chat	msgstore.db	ChatStorage.sqlite
Tabel isi chat	messages	ZWAMESSAGE
Tabel isi data media	messages	ZWAMEDIAITEM
Database kontak	wa.db	ContactsV2.sqlite
Tabel isi kontak	wa_contacts	ZWAADDRESSBOOK-CONTACT
Directory File Log	/data/data/com.whatsapp/files/Logs	Tidak Ditemukan
File Logs	whatsapp-yyyy-mm-dd.log, whatsapp.log	Tidak Ditemukann

Semua informasi daftar kontak yang ditambahkan pengguna WhatsApp disimpan di tabel *wa_contacts* dalam database *wa.db* untuk perangkat android. Informasi kontak pada iOS juga disimpan dalam database *ContactsV2.sqlite* pada tabel *ZWAADDRESSBOOK-CONTACT*. Informasi yang tersimpan diantaranya adalah nomor kontak dan status info akun WhatsApp. WhatsApp mendefinisikan masing-masing nomor menjadi WhatsApp ID dengan struktur [nomor]@s.whatsapp.net. Selain data kontak, WhatsApp juga menyimpan semua history chat (baik android dan iOS) dalam database perangkat seperti yang tertera dalam Tabel 2. File log juga bisa didapatkan, akan tetapi hanya pada perangkat android. Lokasi file seperti yang tertera pada Tabel 2. Log tersebut berisi *history* proses yang dilakukan aplikasi WhatsApp saat digunakan.

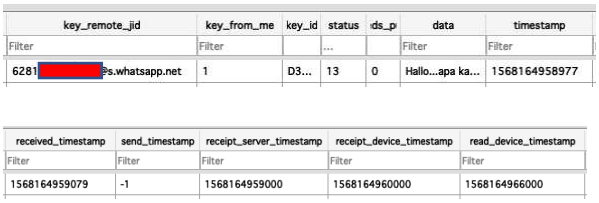
4.2. Analisis Pesan Teks

4.2.1. *Android Mobile Phone*

Semua percakapan yang terekam pada database dalam tabel *messages*. Isi tabel diantaranya adalah *field key_remote_jid* merupakan WhatsApp ID kontak yang menjadi partner dalam bertukar pesan. *Field* data merupakan isi pesan, akan bernilai NULL jika pesannya bukan pesan teks. Timestamp merupakan identitas waktu dari pesan tersebut (waktu pembuatan/pengiriman pesan). Timestamp yang digunakan pada perangkat android adalah unix epoch time. Beberapa timestamp yang juga disimpan dalam tabel *messages* dan dapat mengandung informasi, diantaranya adalah:

- *received_timestamp* merupakan waktu pesan disampaikan karena *received_timestamp* equivalent dengan *timestamp*. *received_timestamp* akan bernilai 0 jika pesan telah dihapus.
- *receipt_server_timestamp* yang merupakan waktu server menerima pesan, akan bernilai -1 jika *key_form_me* adalah 0.
- *receipt_device_timestamp* merupakan waktu perangkat penerima menerima pesan, akan bernilai -1 jika *key_form_me* adalah 0.
- *read_device_timestamp* merupakan waktu penerima membaca isi pesan, akan bernilai -1 jika *key_form_me* adalah 0, dan akan bernilai NULL jika pesan dihapus.

Berikut adalah pembacaan pesan dalam database *msgstore.db*.



key_remote_jid	key_from_me	key_id	status	ds_p	data	timestamp
Filter	Filter		...		Filter	Filter
6281[redacted]s.whatsapp.net	1	D3...	13	0	Hallo...apa ka...	1568164958977

received_timestamp	send_timestamp	receipt_server_timestamp	receipt_device_timestamp	read_device_timestamp
Filter	Filter	Filter	Filter	Filter
1568164959079	-1	1568164959000	1568164960000	1568164966000

Gambar 2. Isi Percakapan Berdasarkan Tabel Messages Pada Database

Berdasarkan Gambar 2 diatas dapat diketahui perangkat android tersebut mengirim pesan berupa teks kepada nomor 6281xxx dengan isi "Hallo…apa kabar...". Hasil konversi waktu unix epoch time didapatkan pesan ditransmisi pada hari rabu tanggal 11 September 2019, dengan rincian sebagai berikut.

- Waktu pesan ditransmisikan pukul 8.22.39,079 AM GMT+07:00.
- Waktu pesan diterima server pukul 8.22.39 AM GMT+07:00.
- Waktu pesan diterima penerima pukul 8.22.40 AM GMT+07:00.
- Waktu pesan dibaca penerima adalah hari rabu tanggal 11 September 2019 pada pukul 8.22.46 AM GMT+07:00.

Hasil pemeriksaaan database sesuai dengan log yang tercatat dalam whatsapp-yyyy-mm-dd.log. Berdasarkan informasi pada log diketahui *event* untuk pengiriman pesan dikelompokkan dalam *ReaderThread* dengan keterangan sebagai berikut.

- Pesan ditransmisikan ke server dengan keterangan xmpp/reader/read/message-received-by-server. Hal ini sesuai dengan timestamp 1568164959000.
- Pesan telah diterima penerima dengan keterangan xmpp/reader/read/status-update-from-target dan status "5". Timestamp yang tercatat sesuai yaitu 1568164960000.
- Pesan telah dibaca penerima dengan keterangan xmpp/reader/read/status-update-from-target dan status "13". Timestamp yang tercatat sesuai yaitu 1568164966000.

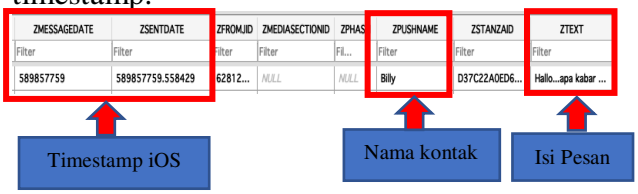
4.2.2. *iOS Mobile Phone*

Percakapan dalam perangkat iOS tersimpan dalam tabel *ZWAMESSAGE*. Berikut adalah beberap *field* tabel yang mengandung informasi percakapan adalah:

- *Z_PK* merupakan nomor pesan.
- *ZISFORMME* merupakan tanda pesan masuk atau keluar. Nilai 1 adalah pesan keluar dan nilai 0 adalah pesan masuk.
- *ZFROMJID* merupakan WhatsApp ID partner dalam bertukar pesan. Jika *ZISFROMME* adalah 1 maka nilainya NULL, dan jika *ZISFROMME* adalah 0 maka isinya WhatsApp ID partner. Kebalikan dari nilai *ZFROMJID* adalah *ZTOJID*.

- *ZPUSHNAME* merupakan nama kontak WhatsApp. Jika *ZISFROMME* adalah 1 maka nilainya NULL, dan jika *ZISFROMME* adalah 0 maka isinya nama kontak WhatsApp.

Field ZMESSAGEDATE dan *ZSENTDATE* merupakan timestamp WhatsApp dalam perangkat iOS. Timestamp yang digunakan berdasarkan Core Data timestamp.



Gambar 3. Isi Percakapan Berdasarkan Tabel *ZWAMESSAGE* Pada Database

Berdasarkan isi tabel *ZWAMESSAGE* pada Gambar 3 diatas diketahui perangkat iOS menerima pesan teks dari kontak bernama Billy dengan kontak ID 62812xxx@s.whatsapp.net. Isi pesan teks yang diterima "Hallo…apa kabar…". Timestamp yang tercatat harus dikonversi terlebih dahulu untuk menunjukkan waktu penerimaan pesan. Hasil konversi dari Core Data timestamp pesan diterima pada hari rabu tanggal 11 September 2019 pukul 8.22.39 AM GMT+07:00.

4.3. Analisis File *Attachment*

Pengiriman file attachment akan tercatat dalam database yang sama dengan pesan teks seperti yang ditunjukkan pada Tabel 2 sebelumnya. Pesan dengan *attachment* file berada pada tabel yang sama dengan pesan teks untuk perangkat android tetapi berbeda tabel untuk perangkat iOS.

4.3.1. *Android Mobile Phone*

Pesan dengan file attachment akan mengisi beberapa kolom pada tabel *messages*. Beberapa *field* yang terisi saat dilakukan transmisi berupa file attachment adalah sebagai berikut.

- *media_url* merupakan URL file yang ditransmisikan. Jenis file *attachment* gambar, audio, video, dan file dokumen/pdf berisi URL terenkripsi dengan ekstensi *.enc.
- *media_mime_type* berisi jenis mime file yang ditransmisikan.
- *media_wa_type* berisi keterangan dari jenis pesan

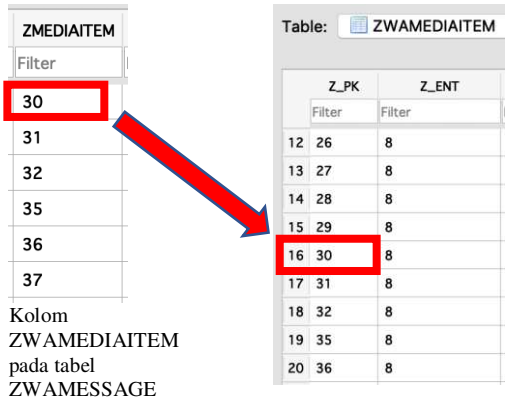
Tabel 3. Keterangan dari *media_wa_type*

media_wa_type	**Keterangan**
0	teks / url dari link
1	gambar
2	audio / voice recorder
3	video dari kamera / galeri
4	file kartu kontak
5	geo position
9	semua *attachment* dokumen (misal pdf, ppt, excel, word, txt, audio video, gambar)

- *media_size* berisi ukuran file attachment yang ditransmisikan.
- *media_name* berisi 128-bit hexadesimal jika *key_form_me* 1 dan status 5, 80-bit hexadesimal jika *key_form_me* 0 dan status 0, lainnya berisi nama media/file attachment yang ditransmisikan.
- *media_caption* berisi caption dari media/file attachment yang ditransmisikan.
- *media_hash* berisi nilai hash SHA256 dari suatu media yang dikirim dengan format base64 (khusus untuk *message_type* =1,2,3,9). Nilai hash dapat menjamin *integrity* dari sebuah file sehingga dengan *integrity* yang sama dapat dipastikan file tersebut adalah file yang sama.

4.3.1. *iOS Mobile Phone*

Pada perangkat iOS, informasi lengkap terkait file attachment tidak sepenuhnya berada dalam tabel *ZWAMESSAGE* tapi terdapat dalam tabel *ZWAMEDIAITEM*. Meskipunn begitu, kedua tabel tersebut saling terkait satu sama lain. Pada tabel *ZWAMESSAGE* terdapat kolom *ZWAMEDIAITEM* yang menunjukkan nomor *Z_PK* pada tabel *ZWAMEDIAITEM* seperti ditunjukkan Gambar 4 berikut.



Kolom ZWAMEDIAITEM pada tabel ZWAMESSAGE

Gambar 4. Relasi Tabel *ZWAMESSAGE* Dengan Tabel *ZWAMEDIAITEM*

Berikut adalah keterangan pada tabel *ZWAMEDIAITEM*:

- *ZFILESIZE* merupakan ukuran file / media yang ditransmisikan (dalam byte).
- *ZMEDIALOCALPATH* menunjukkan path lokasi file pada perangkat.
- *ZMEDIAURL* berisi URL file yang ditransmisikan sama seperti kolom *media_url* pada perangkat android.
- *ZTITLE* berisi judul atau caption dari file attachment.

Informasi nilai hash file media dapat dilihat dalam *ZVCARDNAME* dalam tabel *ZWAMEDIAITEM* berupa Hash SHA256 dengan format base64.

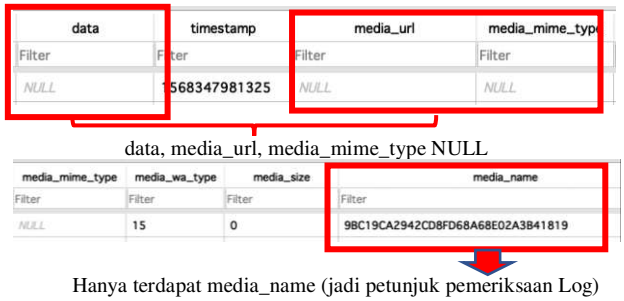
4.4. Analisis Pesan Grup

Pada saat grup dibuat, WhatsApp membangkitkan WhatsApp ID dengan format [nomor pembuat grup]-[timestamp]@g.us. Timestamp yang dibangkitkan menunjukkan waktu pembuatan grup tersebut.

Misalnya diketahui ID 6285xxx-1568863751 @g.us. Berdasarkan ID tersebut dapat diketahui grup tersebut dibuat oleh nomor 6285xxx pada hari kamis tanggal 19 September 2019 pada pukul 10.29.11 AM GMT +07.00.

4.5. Analisis Penghapusan dan Penerusan Pesan

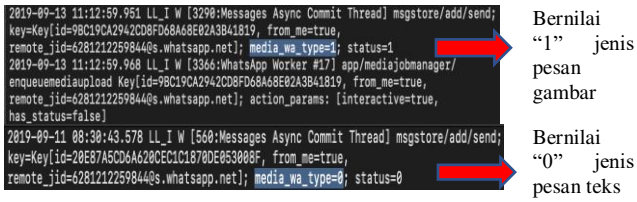
Saat dilakukan pemeriksaan pada file database, proses penghapusan hanya meninggalkan bukti digital adanya transmisi pesan dari suatu ID ke ID yang lain dengan waktu transmisinya. Akan tetapi tidak diketahui isi pesan yang ditransmisikan tersebut [NULL] dan tidak dapat dibedakan pesan tersebut dengan/tanpa attachment. Pada android misalnya, pesan tersebut ditandai dengan *media_wa_type* = 15 dan selengkapnya dapat terlihat seperti pada Gambar 5 berikut.



Gambar 5. Isi Kolom Tabel message Saat Pesan Dihapus

Pendekatan yang dapat dilakukan untuk perangkat android adalah dengan memeriksa file log. Pemeriksaan dilanjutkan pada history log dengan menggunakan informasi *media_name* pada tabel database. Hasil pemeriksaan Log dengan menggunakan keyword yang ditinggakan pada *media_name* didapatkan informasi sebagai berikut.

- Pada baris *Messages Async Commit Thread* terdapat informasi *media_wa_type* yang menunjukkan jenis file yang dikirim seprerti yang ditunjukkan pada tabel 3. Perbandingan informasi Log untuk pesan teks dan gambar dapat dilihat pada Gambar 6 berikut.



Gambar 6. Perbandingan Isi Log Baris *Messages Async Commit Thread*

- Pada baris *WriterThread* terdapat informasi mediaType yang ditransmisikan. Pada Gambar 7, satu pesan yang dihapus mengandung attachment gambar karena

mediaType=image. Sementara satunya lagi NULL yang berarti pesan berupa teks.

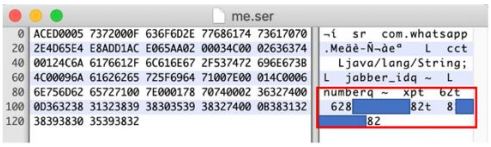
Gambar 7. Perbandingan *WriterThread*

Sementara pada iOS pendekatan yang dilakukan untuk pesan yang dihapus adalah melakukan pemeriksaan pada perangkat penerima atau pengirim pesan kepada perangkat iOS tersebut. Hal ini dikarenakan tidak ditemukan file log pada aplikasi WhatsApp pada iOS.

Sementara untuk pesan yang diteruskan tidak dapat ditentukan asal pesan tersebut bermula tetapi hanya diketahui pesan tersebut merupakan pesan yang diteruskan. Pada perangkat android, pesan yang diteruskan tercatat dicatat dalam kolom *forwarded* pada tabel *message*. *Forwarded* bernilai "1" untuk pesan yang diteruskan dan bernilai "0" untuk pesan yang tidak diteruskan.

4.6. Analisis Pengambilalihan Akun

Berdasarkan Manjushree (2017), terdapat dua pendekatan *hijack* (pengambilalihan) akun WhatsApp yang mungkin dilakukan. Salah satu prosesnya adalah yang dilakukan pada penelitian ini yaitu mengambil OTP verifikasi yang dikirim melalui SMS. Analisis dilakukan dengan asumsi pelaku memiliki kemampuan mendapatkan SMS tersebut. Pendekatan yang dilakukan pertama adalah dilakukan adalah memeriksa WhatsApp ID yang saat ini *login* pada smartphone tersebut dan kedua adalah melakukan pemeriksaan pesan WhatsApp yang disebarkan dengan asumsi pelaku masih *login* dengan akun tersebut. Hasil pemeriksaan dan analisis pada perangkat android dapat dilihat pada file *me.ser* yang tersimpan dalam direktori */data /data /com.whatsapp /files* seperti yang terlihat dalam Gambar 8 berikut.



Gambar 8. Hasil Pemeriksaan File me.ser

Sementara pada perangkat iOS hal tersebut dapat dilihat pada tabel *ZWAMESSAGE*. jika *field ZMESSAGESTATUS* = 0 maka *field ZFROMJID* adalah WhatsApp ID / Grup yang menjadi lawan percakapan dan *field ZTOJID* adalah WhatsApp ID yang saat ini digunakan *login* pada perangkat

5. Kesimpulan

Pada paper ini menunjukkan bahwasanya bukti digital aplikasi WhatsApp masih dapat diperoleh. Saat ini tools forensik sudah bisa mendapatkan data WhatsApp tanpa harus dilakukan root/jailbreak terlebih dahulu meskipun tools forensik tersebut tidak semuanya *support* terhadap perangkat mobile yang ada saat ini. Pada penelitian ini, baik perangkat android maupun iOS, semua data WhatsApp yang tersimpan di dalam database berhasil didapatkan. Sehingga peneliti dapat melakukan rekonstruksi terkait percakapan yang dilakukan. Selain database, data WhatsApp yang menarik perhatian tentu saja log WhatsApp yang mencatat semua proses yang WhatsApp lakukan. Meskipun begitu hanya perangkat android yang terdapat *event* log untuk aplikasi WhatsApp.

Penelitian pada paper ini belum berhasil melakukan recovery terhadap isi pesan yang telah dihapus. Selain itu masih menjadi bahan penelitian selanjutnya bagaimana dari aspek kriptografi sehingga dapat diketahui mekanisme manajemen kunci yang diterapkan WhatsApp dalam menjamin aspek kerahasiaannya.

Daftar Pustaka

Anglano, Cosimo. (2014). Forensic Analysis of WhatsApp Messenger on Android. *Digital Investigation Journal*, vol.11, no.3, pp. 201 – 203, September 2014.

Dogan, Sengul dan Erhan, A. (2017). *Analysis of Mobile Phones in Digital Forensics*. MIPRO 2017.

Hootsuite & We Are Social. (2019, 30 Januari). *Digital 2019 Global Digital Overview*. 25 Agustus 2019. https://datareportal.com/reports/digital-2019-global-digital-overview.

I, Syukur dan Bekti, C. H. (2016). Analisa Forensik WhatsApp dan LINE Messenger pada Smartphone Android sebagai Rujukan dalam Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia. *JURNAL TEKNIK ITS*, vol.5, no.2, 2016.

Jones, G. Maria, dan S. Godfrey Winster. (2017). Forensics Analysis on Smart Phones Using Mobile Forensics Tools. *International Journal of Computational Intelligence Research*, vol. 13, No. 8 (2017), pp.1859 – 1869.

Karpisek, F., Baggili, I., dan Breitinger, F. (2015). WhatsApp Network Forensics: Decrypting and Understanding the WhatsApp Call Signaling Messages. *Digital Investigation*, 15, 110 – 118.

Kent, Karen. Dkk. (2006). *Guide to Integrating Forensic Techniques into Incident Response*. NIST Special Publication 800-86, Agustus 2006.

Lone, A. H., Badroo, F. A., dan Chudhary, K. R. (2015). Implementation of Forensics Analysis Procedures for WhatsApp and Viber Android Applications. *IJCA* (0975 - 8887) vol. 128 – No. 12, Oktober 2015.

Nguyen-vu, L., Chau, NT., Kang, S., dan Jung, S. (2017). Android Rooting: An Arm Race between Evasion and Detection. *Security and Communication Networks*, 2017 (3): 1 – 13, Oktober 2017.

Novaria Kunang, Yesi dan Anggie Khristian. (2017). Implementasi Prosedur Forensik Untuk Aplikasi Whatsapp Pada Ponsel Android. *Jurnal Informatika*, vol.11, No.1, Januari 2017.

Ntantogian, C., Apostolopoulos D., Marinakis G., dan Xenakis C. (2014). Evaluating the Privacy Of Android Mobile Applications Under Forensic Analysis. *Computers & Security,* 42, 66-76. doi: 10.1016/j.cose.2014.01.004.

Ovens, K. M., dan Morison, G. (2016). Forensic Analysis of Kik Messsenger on iOS Devices. *Digital Investigation*, 17, 40 – 52.

Sai, D. M., Prasad, N. R. G. K., dan Dekka, Satish. (2015). The Forensics Process Analysis of Mobile Device. *IJCSIT*, vol. 6 (5), 2015, 4847 – 4850.

Tri Haryanto, Agus. (2019, 24 Januari) *Kominfo Beberkan Sederet Kasus Hoax di WhatsApp*. 26 Agustus 2019. https://www.kominfo.go.id /content/detail/16023/kominfo-beberkan-sederet-kasus-hoax-di-whatsapp/0/sorotan_media.

Umar, Rusydi., Riadi, Imam., dan M. Zamroni, Guntur. (2017). A Comparative Study of Forensic Tools for WhatsApp Analysis using NIST Measurement. *International Journal of Advanced Computer Science and Applications*, vol.8, no.12, 2017.

V, Manjushree C. (2017). WHATSAPP HACKABILITY. *International Research Journal of Computer Science,* vol.4, no.5. Mei 2017.

Walnycky, D., Ibrahim Baggili, Andrew Marrington, Jason Moore, Frank Breitinger. (2015). Network and Device Forensics Analysis of Android Social-Messaging Applications. *Digital Investigation*, vol.14, Agustus 2015, Hal.S77-S84.

WhatsApp Inc. (2017). *WhatsApp Encryption Overview Technical Whitepaper*. 19 Desember 2017.