Prosiding
ANNUAL RESEARCH SEMINAR 2016
6 Desember 2016, Vol 2 No. 1

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

Analisis Forensik Aplikasi Instant Messaging Berbasis Android

Guntur Maulana Zamroni, Rusydi Umar, Imam Riadi
Magister Teknik Informatika
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
gunturmz@yahoo.com, rusydi.umar@mti.uad.ac.id, imam.riadi@mti.uad.ac.id

***Abstrak-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 fitur-fitur 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.**

Kata Kunci—mobile forensik; whatsapp; ekstraksi

I. PENDAHULUAN

Perangkat seluler mengalami perkembangan yang pesat seiring dengan perkembangan teknologi. Perangkat seluler lambat laun mulai menggantikan peran computer dengan semakin banyaknya fitur dan aplikasi yang tersedia pada perangkat seluler, salah satu aplikasi tersebut adalah aplikasi *Instant Messaging* (IM).

Aplikasi IM merupakan salah satu aplikasi yang sering digunakan oleh pengguna perangkat seluler. IM mulai mengganti peran *Short Message Services* (SMS) untuk berkomunikasi melalui pengiriman pesan [1]. WA merupakan salah satu aplikasi IM yang popular dan digunakan oleh banyak orang untuk berkomunikasi. Gambar 1 dan Gambar 2 menjelaskan jumlah pengguna aplikasi WA. Menurut data [2], hingga bulan Februari 2016, terdapat pengguna aktif WA sebanyak 1 Milyar tiap bulannya. Jumlah tersebut mengalami peningkatan dibandingkan jumlah pengguna WA pada bulan Januari 2015 yang sebanyak 700 juta pengguna aktif tiap bulannya. WA setiap harinya melayani pengiriman pesan sebanyak 42 Milyar.

Gambar 2 Statistik WhatsApp

WA menyediakan banyak fitur seperti pengiriman pesan, *group chat*, *video call*, pengiriman file, telepon, dan telah dilengkapi dengan enkripsi untuk keamanan data. Untuk menggunakan WA, pengguna perangkat cukup mengunduh aplikasi dari Google Playstore apabila menggunakan perangkat berbasis Android dan dari App Store apabila menggunakan perangkat iOS. *Username* yang digunakan berupa nomor telepon seluler (contoh: 08xxxxxxxxx@s.whatsapp.net) dengan proses authentifikasi secara otomatis menggunakan SMS. WA kemudian secara otomatis akan melakukan sinkronisasi dengan daftar kontak yang ada pada perangkat seluler sehingga akan memudahkan penggunaan. Berbeda dengan SMS atau panggilan telepon yang mengenakan biaya per-SMS atau permenit panggilan telepon, WA dapat digunakan dengan

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

koneksi Internet atau paket data seluler tanpa dikenakan biaya tambahan.

Jumlah pengguna WA dan fitur keamanan yang ada memungkinan WA akan digunakan sebagai media komunikasi untuk tujuan kriminal seperti perdagangan narkoba, kegiatan teroris, perencanaan pembunuhan, dan kegiatan kriminal lainnya. Pada kondisi seperti itu, perangkat seluler akan digunakan oleh penyidik sebagai barang bukti [3] [4] [5].

Penelitian ini akan memaparkan langkah-langkah forensik yang dilakukan seperti ekstraksi artifak, dekripsi, dan analisis data dari aplikasi WA pada perangkat seluler berbasis Android.

II. KAJIAN PUSTAKA

Komputer dan perangkat seluler mulai digunakan untuk tindakan kriminal, dan untuk melakukan penyidikan diperlukan digital forensik atau mobile forensik. Mobile forensik adalah sebuah cara untuk melakukan *recovery* barang bukti yang berbentuk digital dari sebuah perangkat seluler dengan tata cara forensik dan metode yang dapat diterima [6] [7].

WA merupakan sebuah aplikasi IM yang popular dan tidak mungkin lepas dari penggunaan yang salah seperti untuk tujuan kriminal [3] [5]. Penyidik harus dapat melakukan ekstrasi artifak, dekripsi, dan analisis data-data yang terdapat di dalam perangkat seluler tersebut untuk membantu proses penyidikan karena data-data seperti percakapan dan gambar dapat saja menjadi barang bukti. Penyidik juga dapat melakukan intersep pesan WA. WA telah menerapkan fitur enkripsi baru pada bulan April 2016 dengan menerapkan fitur *end-to-end encryption* untuk percakapan antara dua orang, *group chat, video call*, pengiriman file, dan telepon [8]. *End-to-end encryption* ini memastikan bahwa hanya yang berhak menerima pesan, video, file, dan telepon tersebut yang dapat menerima dan membacanya.

Sahu pada tahun 2014 [9], telah melakukan analisis forensik WA pada perangkat Android yang telah di-root. Penelitian tersebut menggunakan alat dengan bahasa pemrograman Python untuk ekstraksi data.

Satrya, Shin, Daely pada tahun 2016 [10], melakukan analisis forensik pada aplikasi Telegram, Line, dan KakaoTalk. Penelitian tersebut menunjukkan pentingnya arsip percakapan, data base, *log packet* sebagai barang bukti yang berhubungan dengan kasus *cyber crime*.

Gudipaty, Jhala pada tahun 2015 [11], melakukan penelitian forensik pada WA dengan menggunakan tujuh alat untuk membantu analisis forensik. Penelitian tersebut berhasil melakukan dekrip database WA yang menggunakan enkripsi crypt7. Penelitian tersebut juga memaparkan bahwa seorang investigator sebaiknya juga memperhatikan perkembangan dan perubahan teknologi WA untuk dapat melakukan analisis forensik.

III. METODOLOGI PENELITIAN

Penelitian ini menggunakan metodologi berupa langkah-langkah untuk melakukan ekstraksi artifak dan analisis. Secara umum dapat digambarkan pada Gambar 3.

Gambar 3 Metodologi Penelitian

1. Identifikasi

   Data-data yang mungkin dapat digunakan sebagai barang bukti dan membantu proses penyidikan akan dicari.

2. Ekstraksi

   Data-data yang telah diidentifikasi pada langkah sebelumnya akan diekstrak artifaknya ke dalam bentuk yang dapat dibaca oleh manusia dan akan digunakan pada langkah selanjutnya.

3. Analisis

   Analisis data-data atau artifak yang telah diekstraksi untuk mengambil kesimpulan.

4. Presentasi

   Kesimpulan dari proses forensik akan dipaparkan untuk digunakan sebagai barang bukti.

Perangkat keras dan perangkat lunak digunakan untuk melakukan percobaan ekstraksi artifak dari perangkat seluler Android.

Perangkat keras yang digunakan adalah Samsung Galaxy S4 GT-I9500 Unrooted dengan Sistem Operasi Android versi 5.0.1 Lollipop dan WA 2.16.352. Komputer dengan spesifikasi: Sistem Operasi Windows 7 64 Bit, Intel i5-4440, 4.00 GB RAM. USB connector untuk menghubungkan perangkat seluler dengan computer.

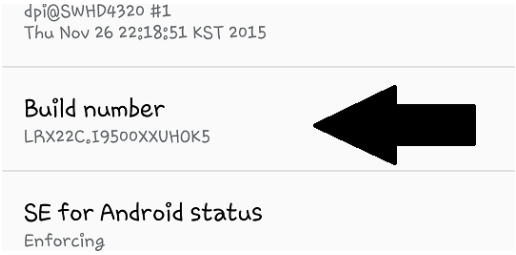
Perangkat lunak yang digunakan adalah Android Debugging Bridge 1.4.3. ADB untuk melakukan komunikasi dan bypass debug dengan perangkat Android. WhatsApp Key/DB Extractor 4.7 untuk melakukan ekstraksi artifak dari perangkat Android. WhatsApp Key/DB Extractor 4.7 yang digunakan merupakan versi terbaru dan telah diupdate untuk mengikuti perkembangan dari enkripsi WA yang telah beralih

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

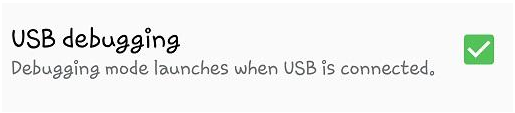
dari .crypt7 dan .crypt8 ke .crypt12. SQLite Studio 3.1.1 digunakan untuk membaca dan menganalisa hasil ekstraksi.

Langkah-Langkah Forensik

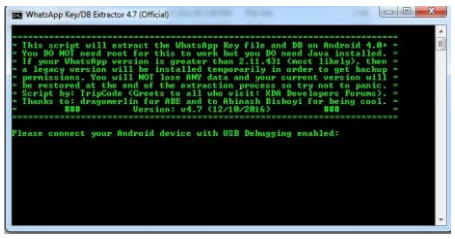
1. Opsi *Developer options* diaktifkan terlebih dahulu pada perangkat seluler dengan cara menyentuh *Build number* sebanyak tujuh kali. Pada opsi *Developer options*, aktifkan opsi *USB debugging* seperti dijelaskan pada Gambar 4 dan Gambar 5.
2. Perangkat seluler dihubungkan dengan komputer.
3. Instal *adb-setup-1.4.3.exe* untuk komunikasi dan melakukan debug [12].
4. Aplikasi *WhatsApp Key DB Ekstract* kemudian digunakan untuk dekrip dan ekstraksi WA. Masukkan *password* untuk *backup* atau kosongkan apabila tidak menggunakan *password* seperti dijelaskan pada Gambar 6.



Gambar 4. Android Build Number

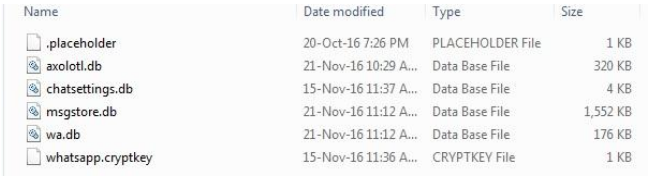


Gambar 5. USB debugging



Gambar 6. WhatsApp DB Key Extract

5. Gambar 7 memperlihatkan hasil ekstraksi yang diletakkan pada folder *extracted*. *Wa.db* berisi kontak WA dan *msgstore.db* berisi komunikasi yang dilakukan melalui aplikasi WA.



Gambar 7. Hasil Ekstraksi

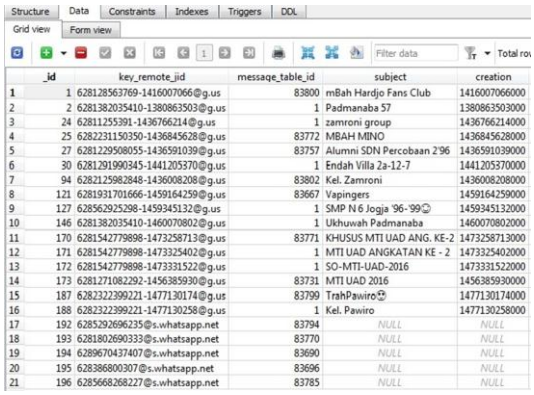
6. Aplikasi SQLite Studio atau aplikasi serupa digunakan untuk membaca hasil ekstraksi.

IV. HASIL DAN PEMBAHASAN

Aplikasi SQLite Studio digunakan untuk membaca file hasil ekstraksi dan melihat komunikasi yang terjadi di dalam WA, baik dalam bentuk percakapan antara dua orang atau melalui grup, komunikasi telepon, pengiriman file. Langkah-langkah forensik dilakukan dengan berbagai kondisi percobaan.

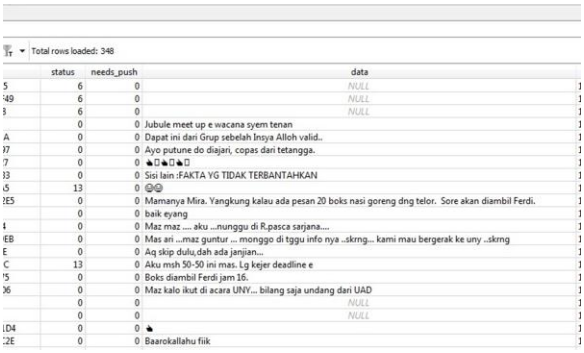
Tabel 1 Kondisi Percobaan

Arsip Percakakan WhatsApp Dihapus	Memory Eksternal Terpasang	Koneksi Internet	Mendapatkan Arsip Percakapan
Tidak	Ya	Ya	Ya
Ya	Ya	Ya	Ya
Ya	Tidak	Ya	Tidak
Ya	Tidak	Tidak	Tidak

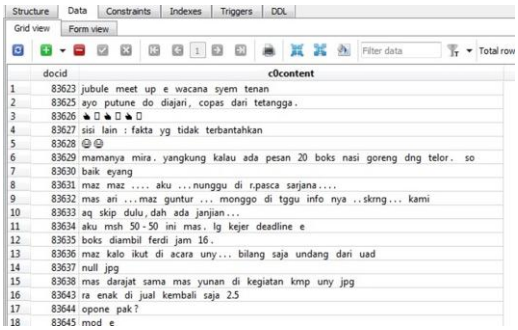


Gambar 8 Percakapan Grup

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id



Gambar 9 Percakapan WhatsApp 1



Gambar 10 Percakapan WhatsApp 2

Penelitian berhasil melakukan ekstraksi artifak komunikasi dari aplikasi WA pada perangkat berbasis Android seperti pada Gambar 8, Gambar 9, dan Gambar 10. Tetapi untuk percobaan dengan tidak menggunakan memory eksternal, tidak berhasil didapat arsip percakapan pada WA dan hanya mendapatkan kontak WA. Dengan alat yang digunakan, peneliti hanya berhasil melihat nama file saja dan belum berhasil untuk melihat file yang dikirim melalui WA seperti gambar atau video.

V. KESIMPULAN

Penelitian ini menggunakan langkah-langkah forensik yang terbukti berhasil untuk melakukan ekstraksi artifak percakapan dari aplikasi WA yang berbasis Android meskipun arsip percakapan telah dihapus dari perangkat. Hanya saja penyidik akan menemui kesulitan untuk melakukan forensik apabila pelaku dapat mengambil dan menghilangkan memory eksternal atau memory tambahan pada perangkat seluler karena *database* WA ter-backup pada memory eksternal tersebut. Peneliti juga mengalami kendala untuk melihat file-file yang dikirim melalui WA dan hanya dapat melihat nama file saja.

DAFTAR PUSTAKA

[1] S. Perez, "Facebook Messenger and WhatsApp combined see 3 times more messages than SMS," TechCrunch, AOL Inc, 12 April 2016, https://techcrunch.com/2016/04/12/facebook-messenger-and-whatsapp-combined-see-3-times-more-messages-than-sms/, Akses terakhir 23 November 2016.

[2] "Number of monthly active WhatsApp users worldwire from April 2013 to February 2016 (in millions)," Statista, February 2016, https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/, Akses terakhir 23 November 2016.

[3] A. Kusumadewi, J. P. Sasongko, "Polisi usut percakapan 'jessica-mirna' yang beredar di sosmed," CNN Indonesia, TransMedia, 21 Januari 2016, http://www.cnnindonesia.com/nasional/20160121080758-12-105715/polisi-usut-percakapan-jessica-mirna-yang-beredar-di-sosmed/, Akses terakhir 23 November 2016.

[4] Y. Ben-Moshe, "Solving cases with mobile forensic analysis," Criminal Law & Justice Weekly, Criminal Law & Justice, 21 September 2013, https://www.criminallawandjustice.co.uk/features/Solving-Cases-Mobile-Forensic-Analysis, Akses terakhir 23 November 2016.

[5] S. Prather, "Minnesota detective crack the case with digital forensic," Star Tribune, 6 Oktober 2014, http://www.startribune.com/when-teens-went-missing-digital-forensics-cracked-case/278132541/, Akses terakhir 23 November 2016.

[6] R. Ayers, S. Brothers, W. Jansen, "Guidelines on mobile device forensics," National Institute of Standards and Technology, NIST Special Publication 800-101 Revision 1.

[7] S. E. Goodison, R. C. Davis, B. A. Jackson, "Digital evidence and the U.S. criminal justice system," National Institute of Justice, RAND Corporation, 2015.

[8] Jan, Brian, "end –to-end encryption," WhatsApp Blog, WhatsApp Inc, 5 April 2016, https://blog.whatsapp.com/10000618/end-to-end-encryption, Akses terakhir 23 November 2016.

[9] S,Sahu, "An analysis of whatsapp in android smartphones," International Journal of Engineering Research Volume No. 3, Issue No. 5, pp. 349-350, May 2014.

[10] G. B. Satrya, S. Y. Shin, P. T. Daely, "Android forensic analysis: private chat on social messenger," IEEE Conference Paper, Research Gate, July 2016.

[11] L. P. Gudipaty, K. Y. Jhala, "Whatsapp forensics: decryption of encrypted whatsapp databases on non rooted android devices," Journal Information Technology & Software Engineering 2015, 5:2, May 2015.

[12] C. Liu, "Using android debug bridge," Developer.com, QuinStreet Inc, 6 November 2015, http://www.developer.com/ws/android/using-android-debug-bridge.html, Akses terakhir 23 November 2016.