Digital Forensik dan Analisis dari Social Messenger Beetalk pada Sistem Operasi Android

Ananda Faisal Faritz

NIM: 1301144324

Telkom University

Fakultas Informatika

Jalan Telekomunikasi Nomor 1, Sukapura, Bojongsoang, Bandung, Jawa Barat, Indonesia

e-mail: [anandafaisalf20@gmail.com](mailto:anandafaisalf20@gmail.com)

**Abstrak—** Social Messenger merupakan aplikasi yang dibutuhkan untuk pengiriman informasi antara suatu perangkat dengan perangkat lainnya sehingga aplikasi tersebut dapat diapakai oleh banyak orang. Kebanyakan social messenger dapat dipasangkan pada perangkat smartphone yang memiliki sistem operasi seperti Android, sehingga pihak pengembang dapat mencari informasi lebih dalam lagi agar dapat mengembangkan aplikasi tersebut. Tetapi pihak hacker dapat menggunakan keuntungan tersebut sehingga dapat terjadi serangan ke aplikasi tersebut. Sehingga dibutuhkannya forensic digital dan analisis yang dilakukan agar dapat mengetahui serangan apa dan jenis serangan tersebut dengan cara melihat file apk dan database dari aplikasi tersebut. Pada penelitian ini digunakan aplikasi Beetalk yang dipasangkan pada dua perangkat. Proses analisis juga dapat menganalisis dari *contact information, chat info, recent info, blocked user,* dan *call history*.

**Kata Kunci**— *Beetalk, apk, database, digital forensik, android forensic.*

**Abstract— Social Messenger is an application needed for the delivery of information between a device with other devices so that the application can be used by many people. Most social messenger can be paired on smartphone devices that have an operating system like Android, so the developers can search for more information in order to develop the application. But the hacker can use these advantages so that an attack can occur to the application. So the need for digital forensic and analysis done in order to know what attacks and types of attacks by looking at apk files and databases of the application. In this study used Beetalk applications are paired on two devices. The analysis process can also analyze from contact information, chat info, recent info, blocked users, and call history.**

**Keywords**— *Beetalk, apk, database, digital forensik, android forensic.*

1 PENDAHULUAN

—————————— ◆ ——————————

EKNOLOGI pada saat ini sudah berkembang pesat termasuk di bidang sosial media. Pengguna dari sosial media tersebut kebanyakan pengguna smartphone dan menggunakan jaringan internet. Perkembangan ini juga diikuti dengan bertambahnya pengguna dari sosial media tersebut secara pesat. Sayangnya, perkembangan ini juga diikuti dengan masalah dari cybercrime yang menyebabkan kerugian pada pihak pengembang maupun pihak pengguna sosisal media, seperti penyebaran virus, spyware, penipuan, sabotase maupun kegiatan teror di

T

dunia digital.

Dengan adanya kegiatan cybercrime, maka dilakukan forensik digital untuk keperluan investigasi tindak kriminal, rekrnstruksi perkara insiden keamanan, upaya pemulihan sistem, dan penyelesaian masalah pada hardware dan software dengan tahapan:

1. Pengumpulan bukti yang mendukung penyelidikan

2. Pemeliharaan bukti-bukti yang ada

3. Analisa secara mendalam terhadap bukti-bukti yang ada

4. Menyajikan dan menguraikan detail laporan penyelidikan dengan bukti-bukti yang sudah dianalisa

Pada bagian II akan dijelaskan tentang tinjauan literatur yang berhubungan dengan penelitian ini. Bagian III akan dijelaskan tentang metode yang digunakan dalam proses forensik. Bagian IV akan dijelaskan tentang proses analisis pada data yang telah didapatkan. Dan pada bagian V berisi tentang kesimpulan dari proses dan hasil yang didapatkan.

2 PEKERJAAN TERKAIT

Sistem operasi merupakan system operasi yang memiliki

sifat open source sehingga pihak pengembang dari smartphone maupun aplikasi dapat dengan mudah mengembangkan lebih dalam, tetapi tidak menutup kemungkinan pihak hacker tidak melakukan hal ilegal di dalamnya dan menggali dasar-dasar sistem. Sebelum membahas penelitian lebih dalam, mari lihat bebeapa pekerjaan yang dilakukan di bidang ini.

2.1 Android

Android merupakan system operasi open source berbasis Linux yang dirancang untuk perangkat smartphone dan tablet yang dikembangkan oleh Android Inc. selanjutnya diakuisisi oleh Google. Android memiliki sejumlah komunitas pengembangan aplikasi yang umumnya ditulis dalam Bahasa pemrograman Java dengan menggunaan pengembangan perangkat lunak Android (SDK). Android memungkinkan penggunanya mengunduh dan memasang APK agar dapat menggunakan aplikasi dari sistus pihak ketiga. Memori flash memory pada perangkat Android dibagi menjadi beberapa partisi, misalnya “/system” untuk system operasi dan “/data” untuk pemasangan aplikasi dan data pengguna. Berbeda dengan distribusi Linux, pemilik perangkat Android tidak diberikan akses root pada system operasi, dan partisi sensitive seperti /system bersifat read- only. Namun, akses root dapat diperoleh dengan cara memanfaatkan kelemahan keamanan pada Android, cara ini sering digunakan oleh komunitas open source untuk meningkatkan kinerja perangkat, namun bias dimanfaatkan oleh pihak lain yang menyebarkan virus dan perangkat perusak.

2.2 Forensik Digital

Forensik digital merupakan cabang ilmu forensic yang berkaitan dengan bukti illegal yang ditemui pada

computer dan media penyimpanan digital dengan tujuan untuk menjabarkan keadaan kini dari suatu artefak digital. Di dalam forensic digital ada beberapa tahap yang dilakukan, yaitu:

1) Acquisition (Pengumpulan)

Tahapan ini merupakan tahapan yang sangat menentukan Karena bukti-bukti yang didapatkan akan sangat mendukung penyelidikan untuk mengajukan seseorang ke pengadilan dan diproses sesuai hukum. Media digital bias dijadikan sebagai barang bukti mencakup system computer, media penyimpanan, smart card, SMS, e-mail, cookies, log file, dokumen, bahkan paket yang berpindah dalam jaringan.

2) Preservation (Pemeliharaan)

Tahapan ini melindungi bukti-bukti dari kerusakan, perubahan, dan penghilangan oleh pihak-pihak tertentu. Bukti harus tidak berubah ketika belum diserahkan kepada ahli forensic untuk diteliti.

3) Analysis (Analisa)

Bukti yang telah didapatkan perlu diteliti kembali ke dalam sejumlah scenario yang berhubungan dengan tindak pengusutan, antara lain siapa yang telah melakukan, apa yang telah dilakukan, hasil proses apa yang telah dihasilkan, dan waktu melakukan.

4) Presentation (Presentasi)

Menyajikan dan menguraikan secara detil laporan penyelidikan dengan bukti-bukti yang sudah dianalisa secara mendalam dan dapat dipertanggung jawabkan scara ilmiah di pengadilan. Laporan harus di cek ulang secara langsung dengan saksi yang ada, baik saksi yang terlibat langsung maupun tidak langusng.

2.3 Aplikasi Beetalk

BeeTalk merupakan aplikasi sosial media yang menghubungkan kepada orang-orang terdekat di tempat pengguna dengan minat yang sama pada suatu hal. Pengguna dapat melihat foto profil dan juga usia orang lain. Jika ada pengguna lain yang jaraknya hanya beberapa meter, pengguna akan mendapatkan pemberitahuan.

2.4 *Tools*

Digunakan tools MOBILedit Forensics untuk mengambil data dari suatu aplikasi yang telah terpasang pada perangkat smartphone. Data yang diambil berekstensi .ab file. Kemudian digunakan tools adb extractor untuk merubah file .ab menjadi .rar. File tersebut kemudian diekstraksi dan dapat dibaca oleh analisis.

3. METODOLOGI RISET

**3.1** Metodologi Android

Di dalam metodologi ini mengikuti tahapan dari forensic, yaitu:

1) Pengumpulan: Dalam tahap ini dilakukan ekstraksi informasi dari smartphone yang dilakukan. Smartphone yang digunakan adalah

Samsung Galaxy S4 yang telah dilakukan root dan Asus Zenfone 2 dengan tipe Z00D yang belum dilakukan root. Masing-masing smartphone dipasangkan aplikasi social messenger Beetalk.

2) Pemeliharaan: Pada informasi yang didapat dilakukan pemeliharaan dengan cara dokumentasi. Pada system dilakukan backup data dengan menggunakan tools MobilEdit Forensics. Setelah dilakukan backup data, digunakan tools DB browser SQLite untuk membuka isi database dan ABE.jar untuk melakukan unpack file berekstens AB.

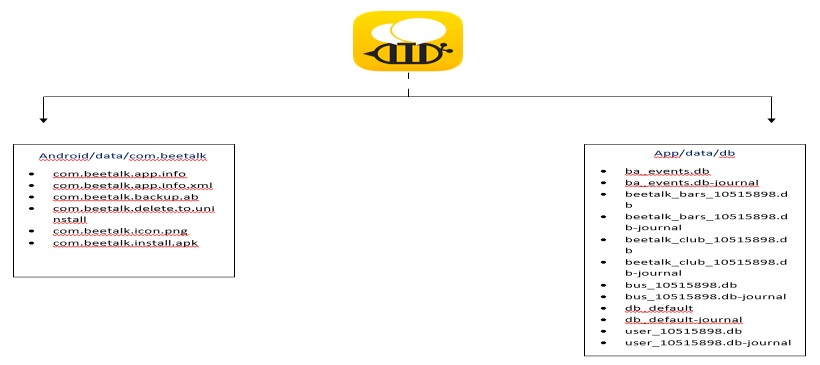
3) Analisa: Dalam hal ini terdapat tiga aktivitas yang dilakukan, yang pertama pengambilan data pada aplikasi Beetalk, kemudian yang kedua pengekstrakan data yang sudah diambil agar dapat dibaca. Yang terakhir dilakukan analisis dari data yang sudah diambil. Dalam data tersebut terdapat banyak file yang dapat dijadikan bukti.

4) Presentasi: Digital forensic sangat berkaitan erat

dengan hukum pada pengadilan. Sehingga data yang didapat haruslah dapat dimengerti oleh pihak pengadilan. Pada tahap ini dilakukan pembuatan laporan dan dokumentasi agar pihak pengadilan dapat memahami laporan yang telah dibuat.

3.2 Persiapan Penelitian

Pada penelitian yang akan dilakukan kita menggunakan aplikasi Beetalk pada perangkat android. Aktivitas yang dilakukan berhubungan dengan contact information dan chatting. Test yang pertama dilakukan menggunakan Asus Zenfone 2 dengan tanpa rooting. Adapun bagian-bagian yang dilakukan analis anatara lain.



*Gambar 3.2.1 Beetalk forensik analisis*

Fig.1 merupakan bagian-bagian yang terdapat pada Beetalk dengan device Asus Zenfone 2 tanpa root. Terdapat bagian Storage file dan Database, namun pada penelitian ini berfokus pada Database user bb\_account\_info, bb\_chat\_msg\_info, bb\_discussion\_chat\_msg\_info, bb\_discussion\_id\_info, bb\_user\_info.

Penelitian kedua dilakukan menggunakan device

Samsung Galaxy S4 Mini yang sudah di root. Adapun bagian-bagian yang akan dilakukan analisis sama seperti penelitian yang pertama.

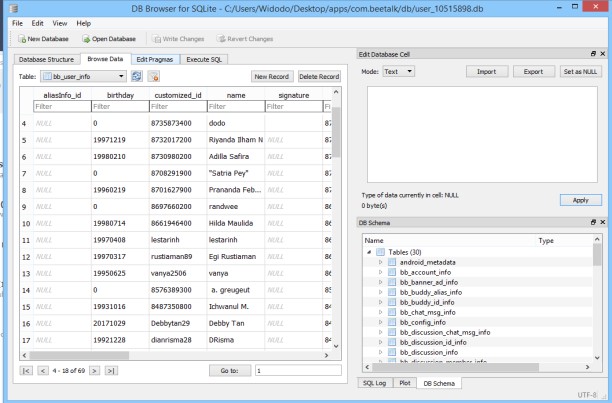
**4.** ANALISA

**4.1** Forensik Beetalk

A. Post-mortem Investigation of Line

1. Contact Information

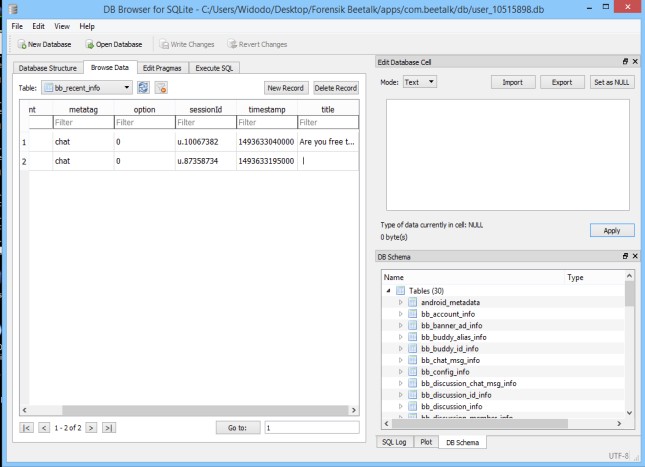
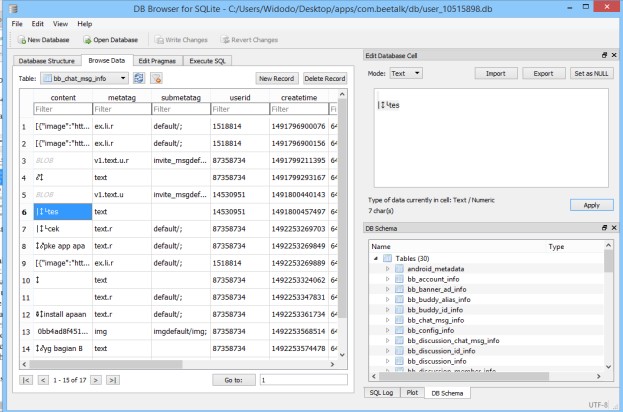
Database beetalk yang didapat memiliki banyak info. Pada table bb\_account\_info menyimpan informasi mengenai kontak yang terdapat pada beetalk. Adapun file yang berisi info kontak yatu bb\_user\_info. Pada file tersebut menampilkan nama kontak, birthday, userID, dan gender. Adapun file yang ditampilkan seperti gambar dibawah ini.



*Gambar 4.1.1 Contact Information*

2. Chat Info

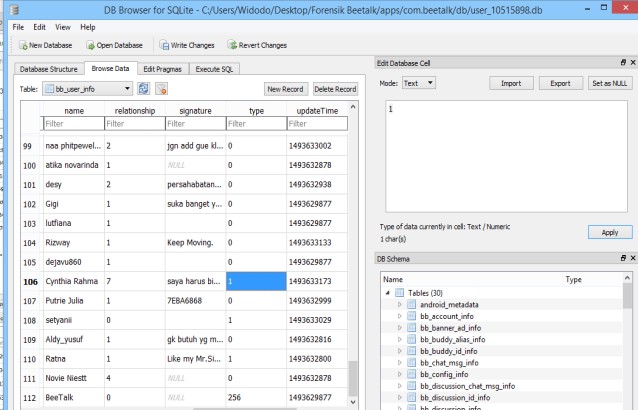
Chat info didapat dari database bb\_user, dan masuk ke chat\_mssg\_info. Disini dapat dilihit history chat user, group, ataupun multichat. Adapun yang ditampilkan antara lain content pesan, userid, dan waktu.



*Gambar 4.1.3 Recent Info*

4. Blocked User

Pada database juga dapat diketahui user-user yang sudah di block. Adapun databasenya adalah bb\_user\_info. Dengan melihat type pada akun yang terdaftar. Dengan biner 0 menunjukan akun normal dan biner 1 menunjukan user yang sudah di block.



*Gambar 4.1.4 Blocked User*

3. Recent Info

*Gambar 4.1.2 Chat Info*

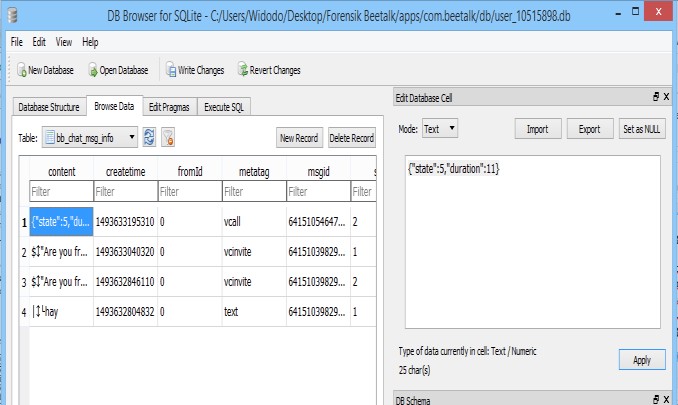
5. Call History

Pada database juga dapat diketahui history call maupun video call yang sudah user hubungi. Adapun databasenya adalah bb\_chat\_msg\_info. Dengan melihat metatag yang berisi fungsionalitas yang dilakukan , melihat konten yang berisi “*{"state":5,"duration":11}*” yaitu history call yang berdurasi 11 detik.

Dilakukan prosedur dengan melihat pada folder

Android/data/com.beetalk untuk melihat file apk dan folder app/data/db untuk melihat isi dari database tersebut.

Recent info berisi mengenai hal-hal yang baru saja diakses oleh pengguna aplikasi. Sehingga dengan membuka database bb\_recent\_info dapat diketahui hal-hal yang baru saja diakses. Adapun yang ditampilkan dalam database tersebut antara lain metatag yang berisi jenis fungsionalnya, timestamp yang berisi waktu dijalankan fungsionalitas.



*Gambar 4.1.5 Call History*

**5.** KESIMPULAN

**5.1.** Kesimpulan

Jadi, pada penelitian ini dapat diambil kesimpulan bahwa pada aplikasi Beetalk ini dapat diambil informasi data yang telah didapat dengan menggunakan berbagai tools yang digunakan. Terdapat dua macam perangkat yang digunakan, seperti perangkat yang telah dilakukan root dan perangkat yang belum dilakukan root. Terdapat perbedaan pada dua perangkat tersebut, seperti pada perangkat yang telah di-root terdapat file berekstensi .dex, sedangkan pada perangkat yang tidak di-root tidak memiliki file tersebut. Sehingga kedua perangkat tersebut dapat dianalisis dan terdapat *contac information, chat info, recent info, blocked user*, dan *call history*.

REFERENSI

Gandeva Bayu Satrya, M. A. (2016). Digital Forensics Study of Internet Messenger: Line Artifact Analysis ind Android OS.

Syukur Ikhsani, B. C. (2016). Analisa Forensik Whatsapp

dan LINE Messenger pada Smartphone Android sebagai Rujukan dalam Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia.

Thakur, N. S. (2013). Forensics Analysis of WhatsApp on Android Smartphones. New Orleans: University of New Orleans.