ANALISA FORENSIK APLIKASI KAKAOTALK MENGGUNAKAN METODE NATIONAL INSTITUTE STANDARD TECHNOLOGY

Riski Yudhi Prasongko [(1)], Anton Yudhana [(2)], Abdul Fadil [(3)]
[(1)(2)(3)]Teknik Informatika, Universitas Ahmad Dahlan
Jalan Prof. Dr. Soepomo, S.H., Janturan, Warungboto, Umbulharjo, Yogyakarta, Indonesia
e-mail : riskiyudhi90@gmail.com

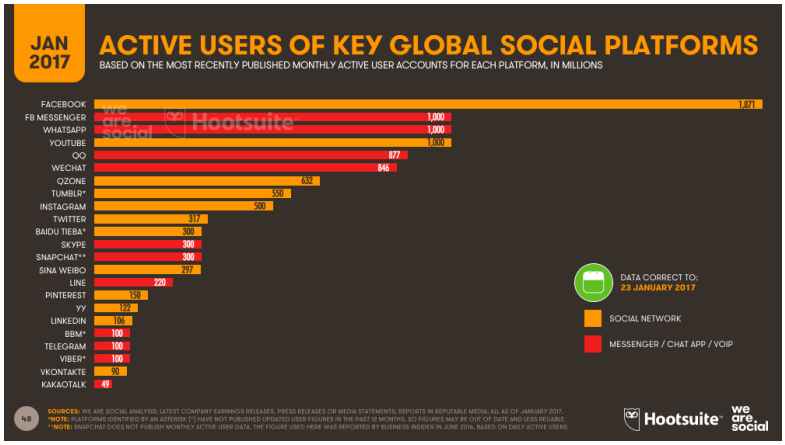
Abstrak
Perkembangan teknologi internet dan smartphone semakin pesat dan diikuti juga oleh meningkatnya penggunaan pesan instan salah satunya KakaoTalk yang mengakses menggunakan smartphone berbasis Android. salah satu permasalahan yang bisa disalah gunakan dalan pesan instan ini adalah tindak kejahatan yang memanfaatkan media pesan instan seprti KakaoTalk. Dengan semakin populernya dan fitur yang diberikan Kakao Talk ini dapat disalahgunakan oknum-oknum tertentu untuk tujuan kriminal, banyak tindak kejahatan seperti pembunuhan berencana, pornografi, penipuan, perjudian, perdagangan narkoba, Jika smartphone digunakan sebagai barang bukti dalam kasus pidana, maka sebuah analisis digital forensik dapat dilakukan untuk mendapatkan barang bukti digital berupa riwayat percakapan, gambar, dokumen, dan video. Bukti digital ini diharapkan dapat membantu dalam proses penegakan hukum untuk mengungkap kejahatan digital

***Kata Kunci** : Kakao Talk, Bukti DIgital, Andriod, NIST, CyberCrime*

1. PENDAHULUAN

Perkembangan dunia teknologi sekarang ini sangatlah pesat, seperti halnya perkembangan teknologi smartphone yang bersistem operasi andriod yang sudah banyak dilengkapi oleh fitur-fitur canggih. Semakin banyak fitur dan aplikasi instan massange tersedia pada perangkat smartphone, salah satunya aplikasi instan messange KakaoTalk.

Aplikasi pesan instan adalah kategori piranti lunak untuk *mobile* yang sudah diramaikan oleh sejumlah nama. Seperti WhatsApp, Facebook Messenger, Line, WeChat, Telegram. KakaoTalk adalah satu dari sekian banyak aplikasi pesan lintas *platform* yang tersedia untuk *smartphone*, selain yang disebutkan di atas. Meski popularitasnya tak segemerlap WhatsApp, LINE dan Facebook Messenger, namun aplikasi tersebut termasuk dari sedikit aplikasi dengan pengguna terbanyak di dunia.



Gambar 1. Daftar Aplikasi Pengirim Pesan Terfavorit per Januari 2017
https://i2.wp.com/www.ideaimaji.com/blog/wp-content/uploads/2018/03/Slide048.png

Meskipun hasil survei di atas menempatkan aplikasi *KakaoTalk* berada di peringkat terakhir dan penggunanya lebih sedikit dibandingkan dengan pengguna aplikasi *instant messaging* yang lain, tetapi tidak menutup kemungkinan aplikasi *KakaoTalk* disalahgunakan oknum-oknum tertentu untuk melakukan tujuan criminal melalui fitur-fitur yang tersedia.

Dimana dengan meningkatnya pengguna aplikasi *KakaoTalk* maka akan berdampak pada peningkatan aktivitas kejahatan digital, yang mana banyak tindak kejahatan yang menggunakan aplikasi

KakaoTalk.
Maka diperlukan analisis digital forensik untuk memperoleh data dan bukti, serta mengumpulkan informasi berharga pada smartphone Android. Jika smartphone digunakan sebagai barang bukti dalam
kasus pidana, maka sebuah analisis digital forensik dapat dilakukan untuk mendapatkan barang bukti digital berupa riwayat percakapan, gambar, dokumen, dan video. Bukti digital ini diharapkan dapat membantu dalam proses penegakan hukum untuk mengungkap kejahatan digital

.

2. TINJAUAN PUSTAKA

Proses investigasi yang baik dan terangkatnya bukti digital pada Line messenter di perangkat smartphone Android. Proses collection atau pengumpulan data diawali dengan rooting menggunakan tool Zenfone RootKit untuk mempermudah pengangkatan data-data yang ada di dalam perangkat Android. Kemudian perangkat Android yang telah di-root, direcovery menggunakan tool Kamas Lite atau AFLogical. Diharapkan data-data yang direcovery dapat menunjukan file percakapan pada aplikasi Line yang berupa teks maupun gambar. (Ammar , 2016)

Penelitian 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 (Guntur, 2016)

Pendekatan ekstraksi database WhatsApp yang diterapkan berhasil mengekstrak percakapan chatting yang disimpan di memori internal maupun external menggunakan key WhatsApp extractor dan decryptor untuk mengkonversi database backup ke dalam database teks yang dapat dilihat di browser basis data SQLite. Tahapan ini bisa membuka sesi chat yang sudah terhapus berdasarkan backup data yang tersimpan baik secara otomatis oleh aplikasi WhatsApp maupun backup manual. (Kunang, 2016)

Analisa Forensik WhatApp dan Line Messenger pada Smartphone Android sebagai Rujukan dalam Menyediakan Barang Bukti yang Kuat dan Valid di Indonesia. Penelitian ini berhasil mengambil database berisikan kontak, percakapan, artefak file penyusun aplikasi dan file-file media seperti gambar, video, suara.(Syukur, 2016)

Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android. Proses analisa dilakukan pada bukti digital dari penggunaan fitur yang ada di aplikasi IM, sehingga proses pengumpulan data dibantu dengan simulasi dari beberapa skenario yang berpotensi terjadi dalam tindakan kriminal. Teknik akuisisi data dilakukan dengan metode physical imaging untuk mendapatkan akses penuh pada memori smartphone. Hasil analisa disimpulkan dalam bentuk tabel perbandingan yang dapat dirujuk oleh investigator forensik ketika melakukan investigasi aplikasi IM yang diteliti. Hasil analisa menyatakan bahwa bukti digital dari aktivitas tukar menukar pesan, berkas media, dan kontak ditemukan. Hasil analisa juga memberikan penjelasan mengenai kemungkinan untuk menganbil bukti digital yang dihapus dan bagaimana cara memulihkannya dengan teknik data carving. (Muhammad, 2018)

Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist. NIST memiliki panduan kerja baik itu kebijakan dan standar untuk menjamin setiap examiner mengikuti alur kerja yang sama sehingga pekerjaan mereka terdokumentasikan dan hasilnya dapat di ulang dan dapat dipertahankan. Hasil penelitian ini tool Oxygen forensic mendapatkan text percakapan, waktu percakapan dikirimkan, pesan audio, gambar, yang tidak didapatkan berupa video.(Ikhwan, 2018)

Pada aplikasi media sosial Twitter bukti forensik yang ditemukan hanya nama akun, data lokasi, photo profile, cover photo, tweet (posting) berupa teks dan tweet (posting) berupa gambar. Sedangkan bukti forensic berupa nomor telepon, tanggal lahir, direct berupa gambar tidak ditemukan. Tidak ada perbedaan hasil pencarian bukti forensic dengan menggunakan aplikasi SQLite Manager maupun DB Browser for SQLite. Berdasarkan pemaparan tersebut dapat disimpulkan bahwa bukti forensik lebih banyak ditemukan pada media sosial Facebook dan tidak ada perbedaan hasil pencarian bukti forensik dengan menggunakan aplikasi SQLite Manager maupun DB Browser for SQLite (Mukti,. 2017)

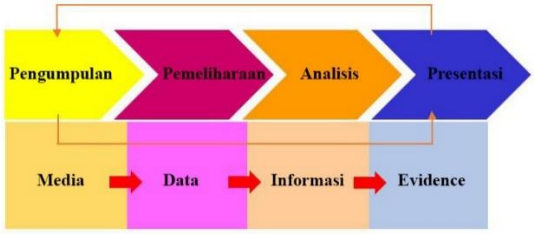
Tidak semua file dapat direstorasi dengan baik karena struktur file dan data sudah rusak, serta catatan pengguna komputer (recent activity) dan sejarah internet (history internet) tercatat ketika fitur pembeku drive diaktifkan. Jika dilakukan perhitungan tingkat prosentase keberhasilannya hanya memiliki nilai 28,7% yang diperoleh dari 85 file yang disiapkan untuk implementasi dan pengujian dan hasil file dari eksaminasi dan yang berhasil direstorasi hanya 25 file. Sehingga dapat menjadi hambatan dalam proses forensik digital (digital forensik) oleh penyidik dan hasil dari penyidikan masih sangat sedikit informasi yang didapatkan dari barang bukti digital.(Nasrulloh, 2018)

Suatu percakapan dapat dianalisis kemunculan kata menggunakan term frequency yang tervisualisasi dalam bentuk wordcloud. Namun banyaknya percakapan belum bisa teranalisis berdasarkan topik percakapan dalam hal ini dugaan tindak kejahatan. Melalui kerjasama dengan pihak Kepolisian analisis percakapan menggunakan term frequency akan lebih mudah menemukan indikasi sebuah percakapan terkait dugaan kejahatan.(Hariyadi,2016)

Dari hasil pengujian yang dilakukan tool Oxygen memiliki fitur report yang lebih lengkap dibandingkan tool ektraksi android forensik MOBILedit dan AFLogical. Tool ini hampir bisa mengekstrasi keseluruhan data aktual dari kontak ponsel, call log, sms-mms, kalender file gambar, video, dan file lainnya. (Yadi, 2014)

3. METODE PENELITIAN

Dalam penelitian ini menggunakan metode Mobile Forensic yang dibuat oleh National Institute of Standard and Technology (NIST). Metode tersebut terdapat beberapa tahapan diantaranya yaitu: Pengumpulan (Collection), Pememliharaan (Preservation), Analisis /memilah-milah (Filtering), Presentasi (Presentation). Seperti yang digambarkan dalam alur metodologi berikut ini :



Gambar 2
Tahap-tahap digital forensik

1. Pengumpulan (Collection)

Merupakan serangkaian kegiatan untuk mengumpulkan data-data sebanyak mungkin untuk mendukung proses penyidikan dalam rangka pencarian barang bukti. 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 hingga akhirnya dijebloskan ke tahanan.

2. Pemeliharaan (Preservation)

Memelihara dan menyiapkan bukti-bukti yang ada. Termasuk pada tahapan ini melindungi bukti-bukti dari kerusakan, perubahan dan penghilangan oleh pihak-pihak tertentu. Bukti harus benar-benar steril artinya belum mengalami proses apapun ketika diserahkan kepada ahli digital forensik untuk diteliti. Kesalahan kecil pada penanganan bukti digital dapat membuat barang bukti digital tidak diakui di pengadilan.

3. Analisis /memilah-milah (Filtering)

Dalam tahapan ini alat-alat bukti yang telah "diamankan" dipilah-pilah. Data-data yang ada, sebagian tidak berhubungan dengan perkara yang sedang diinvesitigasi. Di sini kejelian dari sang investigator sangat dibutuhkan untuk memilih data-data dan bukti-bukti yang dibutuhkan untuk mengungkap suatu perkara.

4. Presentasi (Presentation)

Menyajikan dan menguraikan secara detail laporan penyelidikan dengan bukti-bukti yang sudah dianalisa
secara mendalam dan dapat dipertanggung jawabkan secara ilmiah di pengadilan.

Tabel 1. Alat dan Bahan yang digunakan dalam penelitian.

No	Nama Alat dan Bahan	Spesifikasi	Keterangan
1	Laptop	Acer aspire V5-471 series core(TM) i5-3317U CPU @1.70GHz	Perangkat Keras
2	Smartphone	Lenove a6000 Dual SIM	Perangkat Keras
3	Mobile Edit Forensic	Alpikasi Windows yang dapat digunakan untuk mengangkat bukti digital pada smartphone Android	Perangkat Lunak
4	KingRoot	Aplikasi Android yang digunakan untuk membantu memperoleh akses rooting	Perangkat Lunak

4. HASIL DAN PEMBAHASAN

Anlisa forensik digital pada KakaoTalk untuk penanganan cybercrime menggunakan National Institute of Standards and Technology (NIST). Terdapat beberapa langkah dalam metode ini yaitu. pengumpulan, pemeliharaan, analisis, dan prasentasi. Di dalam penelitian langkah kerja/prosedur dapat dijabarkan secara singkat adalah. Melakukan akuisisi (pengambilan) barang bukti berupa smartphone Android yang akan dianalisis kemudian Melakukan proses rooting dengan aplikasi KingRoot pada smartphone Android yang akan dianalisis, Melakukan proses pengangkatan barang bukti digital dari aplikasi KakaoTalk dengan menggunakan softwere MOBILedit Forensic Tool. Setelah itu Membuat laporan hasil pengangkatan dan analisa barang bukti digital yang sudah didapat. Untuk hasil yang diharapkan dari penelitian ini adalah proses analisis bisa berjalan dengan baik dan mendapatkan barang bukti digital dari KakaoTalk pada smartphone Android yang digunakan sebagai objek penelitian selanjutnya.

5. KESIMPULAN

Penelitian ini menggunakan metode NIST Mobile Forensic dan alat-alat penelitian yang diharapkan dapat digunakan untuk melakukan analisis forensik pada aplikasi KakaoTalk. Kemudian pada saat proses pengangkatan barang bukti digital dari KakaoTalk diperlukan tindakan rooting untuk smartphone Android. Bukti digital yang diharapkan dari proses pengangkatan dan analisis forensik dapat membantu proses penyelidikan suatu kejahatan digital.

DAFTAR PUSTAKA

Fauzan, Annar. 2016. Analisa Forensik Digital Pada Line Messenger untuk Penanganan Cybercrime. Yogyakarta: Annual Research Seminar 2016. Vol. 2, No.1.

Zamroni, Guntur Maulana. 2016. Analisa Forensik Aplikasi Insta Messaging Berbasis Android. Yogyakarta: Annual Research Seminar 2016. Vol. 2, No.1.

Kunang, Yeni Novanias, Anggie Khristian. 2016. Implemantasi Prosedur Forensik untuk Analasis Artefak Whatsapp pada Ponsel Android. Yogyakarta: Annual Research Seminar 2016. Vol. 2, No.1.

Ikhsan, Syukur, Bekti Cahyo Hidayanto. 2016. Analisa Forensik Whatsapp dan Line Messenger pada Smartphone Android sebagai Rujukan dalam menyediakan Barang Bukti yang Kuat dan Valid di Indonesia. Surabaya: JURNAL TEKNIK ITS. Vol. 5, No. 2.

Asyaky, Muhammad Sidik. 2018. Analisis dan Perbandingan Bukti Digital Aplikasi Instant Messenger Pada Android. Tasikmalaya: Sinkron Jurnal & Penelitian Teknik Informatika 2018. Vol. 3, No.1.

Anshori, Ikhwan. 2018. Analisis Bukti Bigital Facebook Messenger Menggunakan Metode Nist. Yogyakarta: IT Journal Research and Development 2018. Vol. 3, No.1.

Mukti, Wisnu Ari. 2017. Analisa dan Perbandingan Bukti Forensik Aplikasi Media Sosial Facebook dan Twitter Pada Smartphone Android. Jakarta: Jurnal Teknik Invormatika 2017. Vol.10, No. 1.

Nasrulloh, Imam Mahfudl. 2018. Analisis Forensik Digital Pada Frozen Solid State Drive Dengan Metode National Institute Of Justice (NIJ). *ELINVO(Electronics, Informatics, and Vocational Education), 2018,3(1), 70-82*

Hariyadi, Dedy. 2016. Analisis Konten Dugaan Tindak Kejahatan Dengan Barang Bukti Digital Blackberry Messenger. TEKNOMATIKA, 2016. Vol. 9, No. 1.

Yadi, Ilman Zuhri. 2014. Analisis Forensik Pada Platform Android. Konferensi Nasional Ilmu Komputer (KONIK) 2014