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 Digital Pada Line Messenger Untuk Penanganan *Cybercrime*

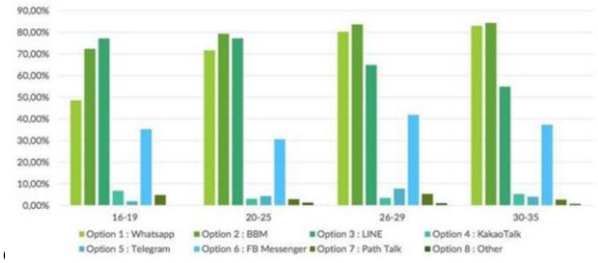
Ammar Fauzan, Imam Riadi, Abdul Fadlil
Magister Teknik Informatika
Universitas Ahmad Dahlan
Yogyakarta, Indonesia
fauzan.ammar@gmail.com, imam.riadi@mti.uad.ac.id, fadlil@uad.ac.id

***Abstrak* — Aplikasi-aplikasi *instant messenger* yang beredar di masyarakat, berpotensi digunakan untuk kejahatan dengan menggunakan layanan, data pengguna, maupun peretasan aplikasi itu sendiri. *Instant messenger* merupakan platform bagi para penggunanya untuk berkomunikasi jarak jauh. Line merupakan salah satu aplikasi *instant messenger* yang cukup banyak digunakan di Indonesia. Kajian dalam penelitian ini adalah dengan menjabarkan langkah-langkah investigasi kasus *cybercrime* yang terjadi di aplikasi *Line Messenger.* Metode penelitian mengacu pada proses investigasi yang telah dilakukan oleh penelitian-penelitian sebelumnya, yaitu terdiri dari tahapan *preservation, collection, examination,* dan *analysis*. Penelitian ini bertujuan untuk menganalisis penanganan kasus *cyberbullying* dengan memunculkan data bukti *cyberbullying* yang terjadi melalui aplikasi Line. Penelitian yang dilakukan dapat bermanfaat untuk menambah wawasan tentang teknik pengungkapan bukti digital pada kasus *cybercrime*.**

Kata Kunci : forensik, line messenger, cybercrime, android, investigasi

I. PENDAHULUAN

Data survei pengguna aplikasi di Indonesia, yang dilakukan lembaga survei *online* JakPat (data awal tahun 2016), bahwa pengguna Blackberry Messenger menempati peringkat pertama dengan 80,31 % pengguna, disusul WhatsApp dengan 72,78 % pengguna, dan di posisi ketiga adalah LINE dengan 71,33 persen (lihat "*Gambar 1*"). Berdasarkan data tersebut, kejahatan cyber tentu saja sangat mungkin terjadi pada aplikasi line messenger. Laporan yang dikeluarkan oleh RSA Anti Fraud Command Center (AFCC), menyebutkan bahwa dari tahun 2013 hingga 2015 terjadi peningkatan aktivitas cybercrime mencapai 173% di seluruh dunia dengan total kerugian mencapai angka US$ 325 Milyar. Laporan tersebut juga melaporkan bahwa pada tahun 2015 sebesar 45% transaksi dilakukan melalui saluran mobile, sedangkan sebesar 61% penipuan terjadi melalui perangkat mobile [1].



Gambar 1. Grafik prosentase pengguna aplikasi *instant messenger*

di antaranya adalah pornografi, perjudian *online*, *cyber-stalking, cyber-tresspass,* dan *cyberbullying*. Semua jenis kejahatan *cyber* tersebut sudah tercantum di dalam undang-undang negara Indonesia. Dasar hukum pidana untuk kejatahan *cyber* di Indonesia, dimuat dalam UU no. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang berisi ketentuan pidana bagi pelaku *cyber crime* [2].

Cyberbullying merupakan salah satu dampak negatif yang saat ini menghampiri para remaja [3]. Di Indonesia, kasus *cyberbullying* menempati peringkat tiga dunia. Sebanyak 91% laporan *cyberbullying* dialami oleh anak-anak [4]. Hal ini sangat ironis mengingat Indonesia dikenal dengan masyarakat yang ramah dan menjaga budaya sopan santun.

Penelitian ini bertujuan untuk menganalisis proses investigasi kasus *cyberbullying* dan memunculkan data bukti *cyberbullying* yang terjadi pada aplikasi Line "*Gambar 2"*.

Gambar 2. Logo aplikasi Line

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

II. KAJIAN PUSTAKA

2.2. *Kajian Penelitian Terdahulu*

Penelitian ini mengacu pada penelitian-penelitian sebelumnya, di antaranya :

- Penelitan berjudul *LINE IM app Forensic Analysis*, tahun 2015, yang dilakukan oleh Asif Iqbal, dkk. Mereka memunculkan data yang dapat di-recover dari sebuah pesan terhapus pada aplikasi Line menggunakan SQLite DB browser [5].
- Penelitian berjudul *Forensic Analysis of WhatsApp Messenger on Android Smartphones*, tahun 2014, yang dilakukan oleh Cosimo Anglano. Ia melakukan pengungkapan data artefak dari Whatsapp menggunakan *tool* YouWave, SQLiteMan, dan Notepad++ [6]
- Penelitian berjudul *Forensic Analysis of Instant messenger Applications on Android Devices*, tahun 2013, yang dilakukan oleh Aditya Mahajan, dkk. Mereka memunculkan data artefak pada aplikasi Whatsapp dan Vibe menggunakan aplikasi Celebrite [7].
- Penelitan berjudul Analisis Forensika Digital Pada Blackberry Untuk Penanganan Kasus Cybercrime Menggunakan Smartphone, tahun 2013, yang dilakukan oleh Yudi Prayudi dan Muhammad Iqbal. Mereka menganalisis cara mengangkat data yang bisa dijadikan bukti forensic pada kasus Cybercrime non-violent menggunakan tool FTK Imager [8]

2.3. *Cyber Crime*

Cybercrime menurut PBB : "setiap perilaku ilegal yang dilakukan dengan cara di kaitannya dengan, korban sistem komputer atau sistem atau jaringan, termasuk kejahatan seperti kepemilikan ilegal, menawarkan atau mendistribusikan informasi melalui sistem komputer atau jaringan." [9]. Berdasarkan pengertian tersebut, *cybercrime* dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan perangkat elektronik sebagai alat atau perangkat elektronik sebagai objek, baik untuk memperoleh keuntungan atau tidak, serta ada unsur merugikan pihak lain [10].

Terdapat banyak ragam kategori untuk mendalami apa yang dimaksud dengan *cybercrime* salah satunya adalah dengan membagi *cybercrime* menjadi dua kelompok besar, yaitu : *Violent / potentially violent*, dan *Non-Violent*. *Violent/Potentially violent* adalah penyalahgunaan komputer yang akan berdampak secara fisik pada orang lain. Secara garis besar terbagi dalam 3 kelompok utama yaitu :

- *Cyberterrorism*, yaitu kegiatan yang mengarah pada aktivitas terorisme dengan memanfaatkan media *cyberspace*.
- *Cyber bullying*, yaitu upaya untuk menimbulkan ketakutan pada diri seseorang dengan merendahkan kehormatan orang lain.
- *Child pornography*, kejahatan ini melibatkan tiga kelompok yaitu mereka yang terlibat untuk *create, distribute*, dan akses material pornografi.

Non-Violent adalah penyalahgunaan komputer yang tidak berdampak langsung pada fisik seseorang namun lebih pada kerugian secara sistemik. Terbagi ke dalam lima kelompok utama yaitu :

- *Cybertrespass*, yaitu akses terhadap *resource* komputer secara ilegal.
- *Cybertheft*, yaitu pencurian informasi atau data penting. Sejumlah aktivitas yang dapat dikatagorikan dalam *cyberthetf* adalah : *Emblezzlement* (penggunaan uang atau properti perusahaan yang tidak seharusnya, misalnya mengubah status kepemilikan data/transfer secara ilegal, *Industrial Espionage*, yaitu akses ilegal untuk mendapatkan data-data penting perusahaan/organisasi (misalnya laporan keuangan, daftar *costumer*, dokumen rapat, dll.).
- Plagiarisme, yaitu pengakuan karya orang lain sebagai karya individu.
- *Piracy*, termasuk di dalamnya adalah *copyrighted software*, *music, movies, book*.
- *Identity Theft*, pencurian data-data personal (bank account, credit card, email). DNS Cache Poisoning, manipulasi DNS cache sehingga mengganggu transmisi jaringan.
- *Cyberfraud*, umumnya berupa undangan email untuk bekerja sama dalam hal investasi, sosial, dan pertolongan.
- *Destructive Crime*, yaitu aktivitas yang berdampak pada kerusakan atau kehilangan data seperti : virus, trojan, hacking, DoS.
- *Others crime* seperti : penawaran jasa prostitusi, judi online, penjualan obat-obat terlarang, *money laundering*, penawaran barang-barang yang tidak lazim diperjual-belikan dalam wilayah hukum tertentu (misalnya untuk Indonesia jual beli arca, hewan langka, dll.) [11].

2.4. *Aplikasi Line Messenger*

Line adalah aplikasi *instant messenger* yang diluncurkan di Jepang sejak Juni 2011 [12]. Aplikasi LINE menggunakan sistem nomor telepon seluler penggunanya sebagai basis untuk saling berhubungan. Aplikasi Line saat ini tersedia untuk *gadget* yang memiliki sistem operasi iOS dan Android.

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

Berkaitan dengan populernya aplikasi *instant messenger*, didukung dengan adanya fitur-fitur yang menarik dan membantu proses komunikasi interpersonal lebih efektif. Di antara fitur *instant messenger* Line yang sering digunakan adalah [13] :

- *Personal Chat*
  Fitur ini merupakan fitur utama yang diberikan oleh Line sebagai sarana komunikasi dengan pengguna Line lainnya secara private. Fitur *personal chat* ini pengguna Line dapat melakukan percakapan secara bebas tentang apa saja.
- Share Foto atau Gambar
  Line memberikan fitur berbagai foto atau gambar baik secara personal melalui personal chat, ataupun melalui diskusi grup. Fitur ini memungkinkan pengguna memilih untuk mengambil gambar atau foto secara langsung dengan kamera ataupun mengambil dari galeri.
- *Free Call*
  Free Call memungkinkan pengguna Line dapat menelpon pengguna Line lain dengan gratis karena menggunakan jaringan internet. Cara menggunakannya adalah dengan memilih teman yang ingin ditelepon lalu pilih "Panggil".
- *Sticker*
  Layaknya *emoticon*, *sticker* juga dapat digunakan untuk mengekspresikan sesuatu dengan bentuk dan gambar yang lebih besar, lebih lucu, dan lebih menarik.
- *Timeline*
  Line menyediakan fitur timeline yang bisa digunakan untuk bersosial media layaknya timeline di facebook.
- Grup
  Line menyediakan fitur grup agar pengguna dapat berbincang-bincang dengan pengguna Line lebih dari satu pengguna .

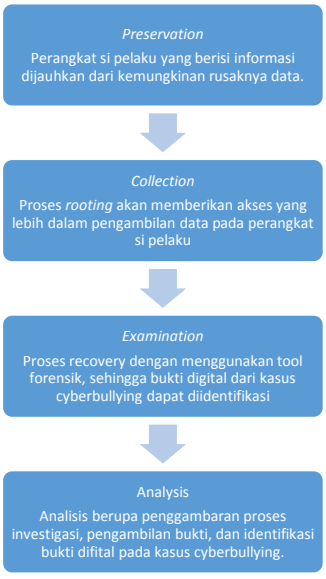
2.5. *Proses Investigasi Forensik digital*

Forensik digital muncul dari banyaknya kriminal yang terjadi pada penggunaan sistem komputer sebagai objek atau sebagai alat yang digunakan untuk sebuah kejahatan atau sebuah penyimpanan bukti tentang kriminal. Kelompok peneliti seperti Computer Analysis and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), the Technical Working Group on Digital Evidence (TWGDE), dan the National Intitute of Justice (NIJ), dibentuk untuk mendiskusikan ilmu forensik digital sebagai disiplin ilmu termasuk kebutuhan sebuah pendekatan standarisasi untuk eksperimen [14]. Ravneet Kaur dan Amandeep Kaur menjelaskan dalam jurnal ilmiahnya tentang proses investigasi forensik digital, yaitu : preservation, collection, examination, and analysis. Mereka juga menyebutkan beberapa hal tentang pentingnya mengetahui model proses investigasi forensik digital karena implementasinya akan berdampak pada [15] :

- Pencegahan dari kejahatan yang terjadi pada calon korban.
- Suksesnya pelacakan dari kejadian yang menjadi petunjuk krimina, dan menentukan jenis perkara dari pihak yang terlibat.
- Membawa pelaku kejahatan ke pengadilan. Mengubah mekanisme pencegahan di lokasi yang perlu dicegah agar tidak kejadian tidak terulang kembali.
- Mengubah standar yang digunakan dalam pengamanan perusahaan untuk mengamankan jaringan perusahaan mereka.
- Bagaimana setiap orang yang mengakses lingkungan digital ini dapat meningkatkan kewaspadaannya tentang kerentanan dan langkah-langkah pencegahan.

III. METODOLOGI PENELITIAN

Metode penelitian pada penelitian ini mengacu pada proses investigasi yang dijelaskan oleh Ravneet Kaur, Amandeep Kaur dalam jurnal ilmiahnya [15]. Metode tersebut terdiri dari beberapa tahapan yang penulis jabarkan pada *"Gambar 3"* :.



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

- *Preservation*
  Upaya menjaga agar bukti digital kasus *cyberbullying* tidak hilang.
- *Collection*
  Mencari dan mengumpulkan informasi yang relevan dengan proses investigasi. Semua informasi yang ada dalam perangkat si pelaku dikumpulkan dan diklasifikasi.
- *Examination*
  Pencarian sistematik dari bukti-bukti yang berhubungan dengan kasus *cyberbullying*. Hasil dari tahap ini adalah berupa data gambar, teks, maupun suara yang ditemukan dalam kumpulan informasi.
- *Analysis*
  Tujuan dari analisis adalah untuk menggambarkan kesimpulan dari bukti-bukti yang ditemukan, sehingga dapat mengidentifikasi konten/file yang dapat dijadikan barang bukti pada kasus *cyberbullying.*

2.6. *Alat dan Bahan*

Alat dan bahan yang diperlukan dalam investigasi forensik digital ini dapat dilihat pada Tabel 1 berikut :

Tabel 1. Daftar Alat dan Bahan

No.	Nama Alat dan Bahan	Deskripsi/Spesifikasi	Keterangan
1.	Satu buah laptop	Merk Asus A455L, *dual boot* Windows 10 dan Kali Linux.	Perangkat Keras
2.	Satu Buah Smartphone	Merk Asus Zenfone 5, Android Lollipop, terinstal Line.	Perangkat Keras
3.	ZenFone RootKit	Aplikasi yang digunakan untuk melakukan *rooting smartphone* Android khususnya Asus Zenfone	Perangkat Lunak
4.	KAMAS Lite	Aplikasi yang digunakan untuk mengangkat data-data aplikasi pada *smartphone*	Perangkat Lunak
5.	AFLogical OSE	Aplikasi berbasis Linux yang dapat digunakan untuk mengangkat bukti digital pada *smarthone* Android	Perangkat Lunak

2.7. *Rancangan Sistem*

Sebuah skenario rekayasa harus dijalankan untuk mendapatkan bukti digital. Pada penelitian ini peneliti memb uat sebuah skenario lengkap dari aktivitas yang dilakukan pada Line messenger. Tujuan adanya skenario ini agar menjadi *road map* dari informasi yang diperlukan untuk di-*recovery*. Skenario tersebut yaitu :

- Membuat akun Line (Akun A)
- Menambahkan teman (Akun B)
- Akun A melakukan chatting terhadap akun B (kondisi normal)
- Akun A mengirimkan gambar kepada akun B (kondisi normal)
- Akun A mengirimkan chatting berisi konten *cyberbullying* terhadap akun B yang menjadi korban, "ini pesan *bully*"
- Akun A mengirimkan gambar berisi konten *bullying*
- Menghapus semua data (tulisan dan voice message) konten *bullying* dari perangkat akun A.

Pesan yang dihapus dari Line messenger akan diungkap dari perangkat si pelaku menggunakan *tools*. Skenario di atas dijelaskan pada "*Gambar 4*" berikut :

Gambar 4. Gambaran skenario kasus *cyber bullying*

Investigasi diawali dari tahap pemeliharaan (*preservation*). Pemeliharaan yang dimaksud adalah bukti fisik berupa perangkat *smartphone* tidak boleh rusak. Kemudian dilakukan pengumpulan data (*collection).* Pengumpulan data dilakukan dengan melakukan *rooting* pada perangkat si pelaku (Akun A). Hal ini dilakukan karena beberapa instant messenger biasanya menyimpan data-datanya di *root*, termasuk data yang sudah terhapus.

Setelah proses *rooting*, data yang sudah siap dimunculkan dan diuji (*examination*) dengan alat forensik Kamas Lite dan AFLogical OSE. Kedua *tool* ini dipakai oleh peneliti untuk membandingkan *tool* mana yang lebih handal dalam me-*recovery* data pada perangkat *smartphone* Android.

Langkah terakhir yang dilakukan dalam investigasi ini adalah melakukan analisis. Analisis yang dihasilkan merupakan gambaran dari proses yang terjadi dalam sebuah proses forensik digital pada Line messenger di *smartphone* Android.

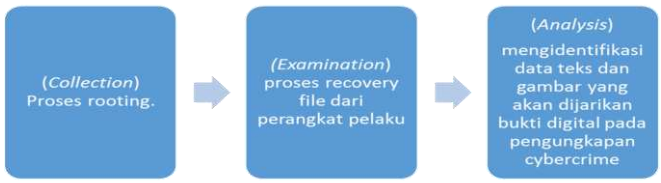
IV. HASIL DAN PEMBAHASAN

Analisis forensik digital pada line messenger untuk penanganan *cybercrime* diawali dengan beberapa langkah,

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

yakni *preservation*, *collection*, *examination*, dan pada akhirnya adalah *analysis.* Analisis yang dihasilkan merupakan gambaran dari semua proses investigasi. Proses investigasi dilakukan pada perangkat pelaku.

Hasil yang diharapkan dari penelitian ini adalah 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*, di*recovery* menggunakan *tool* Kamas Lite atau AFLogical. Diharapkan data-data yang direcovery dapat menunjukan file percakapan pada aplikasi Line yang berupa teks maupun gambar. Secara garis besar, proses analisis dijelaskan pada "*Gambar 5".*



Gambar 5. Proses pengangkatan data barang bukti digital pada penanganan *cybercrime*

Proses analisis forensik digital pada Line *messenger* dapat diperluas pada kajian-kajian berikutnya. Hasil dari proses analisis forensik digital yang telah dilakukan ini diharapkan dapat menjadi salah satu bahan acuan untuk proses investigasi pada kasus-kasus sejenis, khususnya pada media elektronik.

DAFTAR PUSTAKA

[1] RSA, "2016: Current State of Cybercrime," 2013. [Online]. Available: https://www.rsa.com/content/dam/rsa/PDF/2016/05/2016-current-state-of-cybercrime.pdf. [Accessed 5 November 2016]

[2] "STKS," 2015. [Online]. Available: http://www.stks.ac.id/wp-content/uploads/2015/10/UU-NO.-11-TAHUN-2008-TTG-ITE.pdf. [Accessed 23 November 2016].

[3] Maulanz, Pengaruh Cyberbullying Terhadap Kesehatan Mental Remaja, Aceh: Fakultas Kesehatan Masyarakat Muhammadiyah Aceh, 2016.

[4] F. B. Walean, Interviewee, [Interview]. 6 10 2015.

[5] Asif Iqbal, Hanan Alobaidli, Ahmed Almarzooqi, Andy Jones, "LINE IM app Forensic Analysis," in *12th International Conference on High-capacity Optical Networks and Enabling/Emerging Technologies (HONET-ICT 2015)* , Islamabad, 2016.

[6] C. Anglano, "Forensic Analysis of WhatsApp Messenger on Android Smartphones," *Digital Investigation Journal,* vol. XI, no. 3, p. 201–213, 2014.

[7] Aditya Mahajan, M. S. Dahiya, H. P. Sanghvi, "Forensic Analysis of Instant Messenger Applications on Android Device," *International Journal of Computer Applications* , vol. 68, no. 8, pp. 38-44, 2013.

[8] Yudi Prayudi, Muhammad Iqbal, "Analisis Forensika Digital Pada Blackberry Untuk Mendukung Penanganan Kasus Cybercrime Menggunakan Smartphone," in *SINAPTIKA*, Yogyakarta, 2013

[9] United Nations, "unodc.org," Februari 2013. [Online]. Available: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. [Accessed 5 November 2016].

[10] J. Clough, Cybercrime Principles, Cambridge, UK: Cambridge University Press, 2010.

[11] S. Ghosh and E. Turrin, Cybercrimes: A Multidisciplinary Analysis, Verlag, Berlin: Springer, 2010.

[12] Line, "Linecorp.com," Mobile Application, [Online]. Available: https://linecorp.com/en/company/info. [Accessed 5 November 2016].

[13] M. T. Suryadi, The Best Android Apps for Chatting, Yogyakarta: Andi, 2014.

[14] Michael Noblett, Mark.M.Pollitt, and Lawrence Presley, "Recovering and Examining Computer," *Forensic Science Communications,* vol. 2, no. 4, 2000.

[15] Ravneet Kaur, Amandeep Kaur, "Digital Forensics," *International Journal of Computer Applications,* pp. 5-9, 2012.