IDENTIFIKASI BUKTI DIGITAL SKYPE DI SMARTPHONE ANDROID DENGAN METODE NATIONAL INSTITUTE OF JUSTICE (NIJ)

Muhammad Rizki Setyawan[1], Anton Yudhana[2], Abdul Fadlil[3]

[1]Program Studi Magister Teknik Informatika, Universitas Ahmad Dahlan, Yogyakarta
[2,3]Program Studi Teknik Elektro, Universitas Ahmad Dahlan, Yogyakarta
Jl. Prof. Dr. Soepomo, S.H., Janturan, Yogyakarta
Email: muhammad1808048026@webmail.uad.ac.id, Email: eyudhana@ee.uad.ac.id,
Email: fadlil@mti.uad.ac.id

Abstrak. Perkembangnan teknologi sekarang memudah masyarakat dalam berbagi informasi dan melakukan aktivitas komunikasi dengan menggunakan aplikasi *instant messanger.* Skype merupakan salah satu *instant messanger* multi-platform yang dapat digunakan oleh user dalam mengirim text, audio, video dan gambar. Teknologi semakin canggih tidak hanya dapat digunakan untuk melakukan kegiatan positif, tetapi dapat juga digunakan untuk melakukan kegiatan negatif yaitu dapat digunakan untuk tindakan *cybercrime*. Pada saat tindakan kejahatan pasti akan meninggalkan barang bukti. Dalam menyelesaikan masalah *cybercrime* yang menggunakan IM, penyidik perlu melakukan digital forensik terhadap perangkat seluler berupa *smartphone* yang digunakan dalam melakukan kejahatan untuk menemukan bukti digital, Pengangkatan barang bukti akan tersebut menggunakan digital forensik. Penelitian ini bertujuan untuk medapatkan bukti digital kasus penipuan online yang ada pada Skype dengan menggunakan metode National Institute of Justice (NIJ). Hasil dari penelitian digunakan sebagai bukti pendukung oleh penyidik dalam menangani kasus kejahatan.

Kata kunci: Cybercrime, Digital Forensik, Skype, NIJ

Abstract. Technology development now makes it easier for people to share information and conduct communication activities by using instant messenger applications. Skype is one of the multi-platform instant messanger that can be used by users in sending text, audio, video and images. More sophisticated technology can not only be used to carry out positive activities, but can also be used to carry out negative activities which can be used for cybercrime. At the moment the crime will definitely leave evidence. In solving the problem of cybercrime that uses IM, investigators need to conduct digital forensics on mobile devices in the form of smartphones used to commit crimes to find digital evidence, Appointment of evidence will use digital forensics. This study aims to obtain digital evidence of online fraud cases that are on Skype using the National Institute of Justice (NIJ) method. The results of the study were used as supporting evidence by investigators in handling criminal cases.

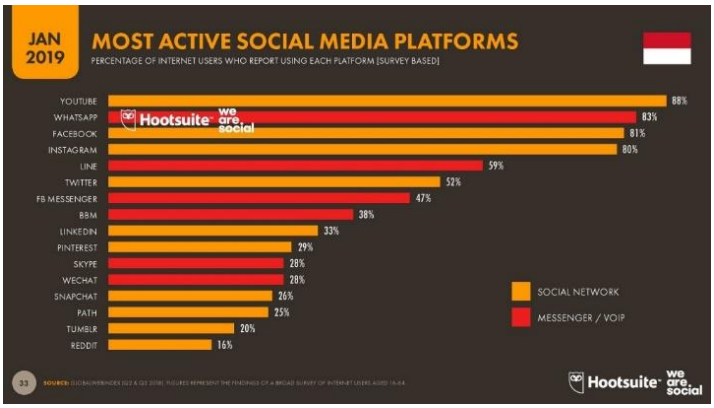
Keywords: Cybercrime, Digital Forensic, Skype, NIJ

1. PENDAHULUAN

Instant Messanger merupakan aplikasi chat online untuk mengirim pesan, audio, video dan image file menggunakan koneksi jaringan internet. Penggunaan IM memberikan masyarakat kemudahan untuk melakukan kegiatan komunikasi. *Instant messanger* seperti Skype, LINE, WhatsApp, BBM dan Facebook Messanger

merupakan beberapa aplikasi yang sering digunakan di indonesia. Munculnya perangkat seperti Smartphone, Tablet computer, personal komputer dan kemudahan internet membuat penggunaan aplikasi seperti IM sangat popular (Ming Sang Chang, 2018).

Skype adalah aplikasi komunikasi yang berspesialisasi dalam menyediakan obrolan video dan panggilan suara antara perangkat melalui Internet. Skype juga menyediakan layanan *instant messanger*. Pengguna dapat mengirimkan teks, video, audio dan gambar. Skype dapat digunakan di berbagai sistem operasi seperti Windows, MAC, iOS, dan Android.



Gambar 1. Grafik Pengguna Skype Messanger di Indonesia

Grafik pada Gambar 1 menjelaskan pengguna Skype yang semakin banyak selain memberi manfaat dapat juga memberikan potensi untuk terjadinya aktivitas *cybercrime* seperti penipuan, pornografi, *cyberstalking*, *cyberbullying* dan *cyber-tresspass.* Dalam menyelesaikan masalah *cybercrime* yang menggunakan IM, penyidik perlu melakukan digital forensik terhadap perangkat seluler berupa *smartphone* yang digunakan dalam melakukan kejahatan untuk menemukan bukti digital. Dalam melakukan analisis pada bidang mobile forensik memiliki banyak tantangan tersendiri salah satunya bukti digital yang rapuh terhadap perubahan data serta penambahan jumlah perangkat *smartphone* dan aplikasi IM yang memiliki spesifikasi yang berbeda sehingga dalam melakukan analisis memerlukan proses yang berbeda.

Berdasarkan masalah diatas, penelitian bertujuan untuk menemukan bukti digital kasus penipuan online yang ada pada Skype *messanger* di *smartphone android* dengan menggunakan metode National Institute of Justice (NIJ). Hasil dari penelitian ini dapat digunakan untuk menjadi bukti pendukung oleh penyidik dalam menangani kasus kejahatan. Penelitian dengan tema sejenis pernah dilakukan beberapa peneliti sebagai berikut:

1. Arizona Firdonsyah (2018) dengan judul "Forensic Tools Performance Analysis on Android-based Blackberry Messenger using NIST Measurements". Melakukan penelitian tentang kemampuan tool forensic pada aplikasi Blackberry Messenger. Hasil yang didapatkan yaitu Andriller mendapat 25%, Oxygen Forensic Suite mendapatkan 100% dan Autopsy 4.1.1 mendapatkan 0%. Berdasarkan parameter National Institute of Standard Technology Andriller mendapatkan 47.61%, Oxygen Forensic Suite mendapatkan 61.90% dan Autopsy 4.1.1 mendapatkan 9.52%.
2. Muhamad Caesar Febriansyah Putra (2018) dengan judul "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)". Melakukan penellitian untuk mendapatkan bukti digital kasus *cyberbulling* di Instagram. Hasil yang didapat pada smartphone dalam kondisi Root yakni berupa gambar dan percakapan sedangkan untuk smartphone tidak dalam kondisi Root tidak didapatkan barang bukti digital.
3. Ahwan Ahmadi (2018) dengan judul "Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ)" Melakukan penelitian untuk mendapat barang bukti tindak kejahatan digital pada media cloud storage google drive pada android. Hasil analisis yang di dapatkan menggunakan tool Oxygen Forensics berupa akun email, Extensi file, Gambar, dan File Zip. Sedangkan tool Mobile Edit Forensik hanya bisa mendapatkan akun email.
4. Ikhwan Anshori (2018) dengan judul "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist". Melakukan penelitian pengangkatan barang bukti kejahatan digital dari facebook Messenge menggunakan metode Nist dan tool *Oxygen Forensic*. Hasil yang didapatkan berupa barang bukti text percakapan, waktu percakapan dikirimkan, pesan audio, gambar, yang tidak didapatkan berupa video.
5. Ammar Fauzan (2016) dengan judul "Analisa Forensik Digital Pada Line Messenger untuk Penanganan Cybercrime". Melakukan penelitian untuk penanganan *cybercrime* pada Line Messanger menggunakan tool

Zenfone Rootkit untuk proses root smartphone dan Kamas Lite ata AFLogical untuk melakukan recovery. Hasil penelitian data yang direcovery dapat menunjukan file pesan text maupun gambar yang ada pada aplikasi Line.

2. LANDASAN TEORI

2.1 Digital Forensics

Menurut M. N. Al-Azhar (2012) digital forensik merupakan aplikasi bidang ilmu pengetahuan dan teknologi komputer untuk pembuktian hukum, yang dalam hal ini adalah digunakan untuk membuktikan tindakan kejahatan berteknologi tinggi atau cybercrime secara ilmiah hingga bisa mendapatkan bukti digital untuk menjerat pelaku kejahatan. Digital forensics memiliki banyak cabang satu dari cabang yang ada yaitu mobile forensics. Digital forensik pada intinya adalah untuk membantu memulihkan, menganalisa, dan mempresentasikan materi berbasis digital sehingga dapat dipergunakan sebagai alat bukti yang sah di pengadilan.

2.2 Mobile Forensics

Mobile forensics merupakan cabang dari forensik digital yang berkaitan dengan pemulihan bukti digital dari perangkat mobile yang dilakukan sesuai dengan kondisi forensik (Firdonsyah, 2017). Perangkat selular frase biasanya merujuk ke ponsel, namun juga dapat berhubungan dengan perangkat digital yang memiliki memori internal dan kemampuan komunikasi (Karpisek, 2015). Penggunaan perangkat seluler seperti Smartphone dalam melakukan kegiatan kejahatan semakin tinggi, sehingga dengan adanya forensik pada perangkat seluler dapat membantu penyidik untuk mengatasi kasus-kasus yang berhubungan dengan pernagkat seluler (Anggara, 2017).

2.3 Bukti Digital

Bukti digital merupakan informasi yang disimpan atau dikirim dalam bentuk biner yang dapat diandalkan dipengadilan (D. J Daniels dan S.V Hart, 2004). Bukti digital itu rapuh, jika tidak di tangani secara benar (Firdonsyah, 2017). Pergantian pada data menyebabkan perubahan pada hasil investigasi, sehingga perangkat yang menjadi barang bukti perlu di mode isolasi. Tujuannya untuk menghindari data terhapus dan berubah pada kondisi apapun. Barang bukti digital dapat ditemukan di perangkat seperti hard drive, flash disk, smartphone, routers, tablets, dan alat seperti GPS (M. N. O. Sadiku, dkk, 2017)

2.4 Cybercrime

Cybercrime merupakan suatu kegiatan kejahatan yang dilakukan di dunia maya menggunakan informasi teknologi sebagai target kejahatan. Tindak cybercrime seperti pornografi, penculikan, pemerasan, penipuan online, cyberbully dan lainnya. Semua jenis kejahatan yang terjadi pada dunia maya sudah tercantum di dalam undang-undang negara Indonesia. Dasar hukum pidana untuk kejahatan pada dunia maya di Indonesia, dimuat dalam UU no. 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) yang berisiketentuan pidana bagi pelaku cybercrime (Febriansyah, 2017). **Dalam melakukan kegiatan kejahatan, para penjahat di dunia maya terus melakukan perubahan strategi dalam menargetkan media social dan *isntan mesanger* yang berkembang. Penggunaan media social dan *isntan mesanger* dapat disalah gunakan sehingga memungkinkan dapat di manfaatkan untuk melakukan kegiatan kejahatan (Nur, 2016).**

2.5 Skype

Skype adalah aplikasi komunikasi yang berspesialisasi dalam menyediakan obrolan video dan panggilan suara antara perangkat melalui Internet. Skype juga menyediakan layanan instant messanger. Pengguna dapat mengirimkan teks, video, audio dan gambar. Skype dapat digunakan di berbagai sistem operasi seperti Windows, MAC, iOS, dan Android.

3. METODOLOGI PENELITIAN

Dalam proses investigasi metode yang digunakan yaitu metode *National Institute of Justice* (NIJ). Dalam metode tersebut digunakan dalam memudahkan mejabarkan gambaran proses penelitian yang dilakukan agar bisa diketahui tahapan penelitian ini secara lebih sistematis. Tahapan metode secara lengkap dipaparkan pada Gambar 2.

Gambar 2. Tahapan dalam Metode NIJ

Penjelasan dari tahapan-tahapan dari metode *National Institute of Justice* (NIJ) adalah sebagai berikut:

a. *Preservation*
   Melakukan upaya menjaga keutuhan dan pengamanan barang bukti yang telah ditemukan agar tidak hilang atau berubah.
b. *Collection*
   Melakukan kegiatan pengumpulan data untuk mendukung proses penyidikan dalam mencari barang bukti kejahatan digital.
c. *Examination*
   Melakukan pemeriksaan data yang dikumpulkan secara forensik baik secara otomatis atau manual, serta memastikan bahwa data yang didapat berupa file tersebut asli.
d. *Analysis*
   Setelah mendapatkan data-data dari proses sebelumnya, maka perlu dilakukan tahapan selanjutnya yaitu analisis data yang bertujuan untuk menentukan bukti signifikan dan nilai dari pembuktian.
e. *Reporting*
   Melakukan pembuatan laporan dari barang bukti digital yang didapat melalui proses pemeriksaan dan analisis.

Alat dan Bahan

Alat dan bahan yang diperlukan pada proses melakukan forensik digital dapat di lihat pada Tabel 1.

Tabel 1. Daftar Alat dan Bahan

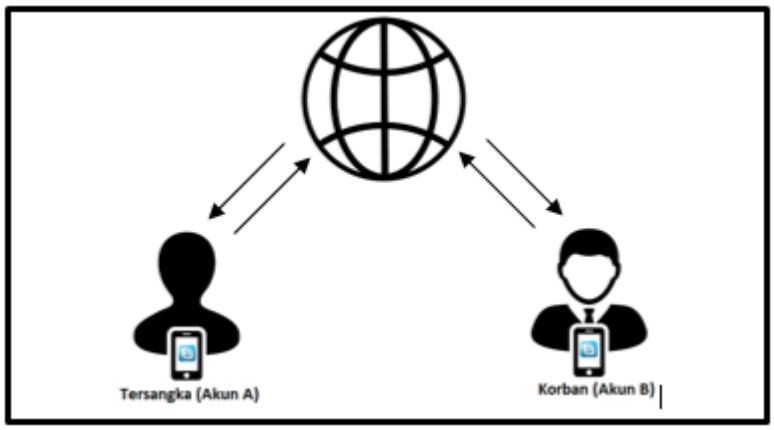
No	Nama Alat dan Bahan	Deskripsi / Spesifikasi
1	Satu buah Laptop	Merk ASUS A46CB *boot* windows 10
2	Satu buah Smartphone	Merk Samsung GT i8262 Android 4.1.2 sudah terinstal skype
3	iRoot	Software untuk melakukan rooting di smartphone berbasis Android
4	Mobile Edit Forensic	Software untuk mengangkat data-data di aplikasi pada smartphone

Rancangan Skenario

Sebuah skenario rekayasa harus dijalankan untuk mendapatkan bukti digital. Pada penelitian ini dilakukan sebuah skenario dari kegiatan yang dilakukan di aplikasi Skype. Tujuan daari scenario agar mempermudah investigasi dari kasus penipuan online. Skenario tersebut yaitu:

1. Membuat akun Skype (Akun A)
2. Mencari akun korban di Skype (Akun B)
3. Akun A mengirimkan (Pesan dan Gambar) kepada akun B (kondisi normal)
4. Akun A mengirimkan konten berisi penipuan (Pesan dan Gambar) terhadap akun B
5. Menghapus semua data (Pesan dan Gambar) konten penipuan dari perangkat akun A

Pesan yang telah dihapus dari Skype akan diungkap dari perangkat si pelaku menggunakan tools forensik. Skenario di atas dijelaskan pada Gambar 3 berikut:



Gambar 3. Proses skenario komunikasi Akun A dan Akun B

4. HASIL DAN PEMBAHASAN

Proses analisis forensik digital pada skype untuk penanganan penipuan online menggunakan metode *National Institute of Justice* (NIJ) diawali beberapa tahap yaitu tahap pertama *preservation*, pada proses ini barang bukti perangkat *smartphone* yang ditemukan dilakukan pemeliharaan agar tidak terjadi kerusakan atau hilang. Tahap Kedua yaitu *collection*, pada proses ini melakukan pengumpulan data diawali dengan melakukan rooting pada perangkat smartphone dengan aplikasi iRoot. Hal ini dilakukan agar saat pengangkatan data yang ada menjadi lebih mudah. Tahap ketiga yaitu *Examination*, pada proses ini perangkat Android yang telah di-root, data akan dijadikan bukti digital berupa (Pesan dan Gambar) yang akan diambil menggunakan tool Mobile Edit Forensic dari aplikasi skype yang tersimpan di memori penyimpanan di android. Tahap ke-empat yaitu *Analysis*, data yang telah didapat pada proses sebelumnya kemudian dianalisis data text dan gambar yang nantinya digunakan sebagai bukti digital dalam penangan kasus *cybercrime*. Tahap terakhir yaitu *Reporting*, selanjutnya pada proses ini dilakukan pembuatan laporan hasil dari tahapan-tahapan atau proses dalam pengangkatan dan analisa barang bukti digital yang didapat.

5. KESIMPULAN

Dari uraian yang dijabarkan di atas dengan metode *National Institute of Justice* (NIJ). Hasil peneliti ini mampu mengakuisisi salah satu aplikasi instant messanger yang ada di android yaitu Skype. Hasil yang didapat dari penelitan dapat digunakan sebagai bukti pendukung oleh penyidik dalam menangani kasus kejahatan dan acuan penyidik dalam mencari barang bukti pada kasus-kasus *cybercrime* di aplikasi skype.

Saran dari penulis ada banyak tool-tool forensik dan metode yang dapat digunakan, penelitian selanjutnya akan lebih baik dengan tools dan metode yang berbeda. Penggunaan tool forensik yang berbeda bisa memberikan banyak informasi dari data hasil akuisisi, karena tool forensik memiliki kekurangan dan keunggulan.

DAFTAR PUSTAKA

Al-Azhar, M. N (2012). Digital Forensic, Panduan Praktis Investigasi Komputer. Jakarta. Salemba Infotek.

Ahmadi, A., Yudhana, A. Umar, R. "Akuisisi Data Forensik Google Drive Pada Android Dengan Metode National Institute of Justice (NIJ)". Jurnal CoreIT Vol. 4, No. 1, pp. 8-13, Juni 2018.

Anshori, I., Yudhana, A. & Riadi, I. "Analisis Bukti Digital Facebook Messenger Menggunakan Metode Nist." 3(1): 13–21, 2018.

D. J. Daniels and S. V Hart, "Forensic Examination of Digital Evidence : A Guide for Law Enforcement," U.S. Dep. Justice Off. Justice Programs Natl. Inst. Justice Spec., vol. 44, no. 2, pp. 634–111, 2004.

F, Annar. Riadi, I. & Fadlil, A. "Analisa Forensik Digital Pada Line Messenger untuk Penanganan Cybercrime". Annual Research Seminar. Vol. 2, No.1, pp. 156-163, 2016.

Firdonsyah, A., Riadi, I. & Umar, R."Forensic Tools Performance Analysis on Android-based Blackberry Messenger using NIST Measurements". International Journal of Electrical and Computer Engineering, 8(5): 3991–4003, 2018

Firdonsyah, A., Riadi, I. & Umar, R. "Identification Of Digital Evidence On Android's Blackberry Messenger Using NIST Mobile Forensic Method," International Journal of Computer Science and Information Security (IJCSIS), vol. 15, no. 5, pp. 155–160, 2017

I. Riadi, A. Yudhana & M. Caesar Febriansyah Putra, "Analisis Recovery Bukti Digital Instagram Messangers Menggunakan Metode National Institute Of Standards and Technology (NIST)," Prosiding Seminar Nasional Teknologi Informasi dan Komunikasi (SEMANTIKOM), 2017, pp. 161–166, 2017

Karpisek, F., Baggili, I., & Breitinger, F."WhatsApp network forensics : Decryption and understanding the WhatsApp call signaling messages. Digital Investigation. 2015; 15: 110-118.

Ming Sang Chang and Chih Yen Chang," Forensic Analysis of LINE Messenger on Android", Journal of Computers Vol. 29, No. 1, pp. 11-20, 2018.

R. Anggara Putra, R. Umar, I. Riadi, "Forensik Mobile pada Smartwatch Berbasis Android," Jurnal Rekayasa Teknologi Informasi, vol. 1, no. 1,pp. 41–47, 2017.

Muhamad Caesar, & Febriansyah Putra , Riadi, I. & Yudhana, A. 2018. "Akuisisi Bukti Digital Pada Instagram Messenger Berbasis Android Menggunakan Metode National Institute Of Justice (NIJ)". Jurnal Teknik Informatika dan Sistem Informasi, Vol. 4, No. 2, pp. 219-227, Agustus 2018.

M. N. O. Sadiku, M. Tembely, and S. M. Musa, "International Journal of Advanced Research in Digital Forensics," vol. 7, no. 4, pp. 274–276, 2017.

M. Nur Faiz, R. Umar, A. Yudhana, "Analisis Live Forensics Untuk Perbandingan Kemananan Email Pada Sistem Operasi Proprietary," Jurnal Ilmiah ILKOM, 2016, vol. 8, no. 3, pp. 242–247, 2016.

Zuhriyanto, I., Yudhana, A. & Riadi, I. "Perancangan Digital Forensik Pada Aplikasi Twitter Menggunakan Metode Live Forensics". SemnasIF Vol. 1, No. 1, pp. 86-91, November 2018.