PEMERIKSAAN NETWORK FORENSIK TERHADAP BARANG BUKTI DIGITAL AKUN MEDIA SOSIAL MENGGUNAKAN METODE OTOMATISASI SOFTWARE SECARA ONLINE

Hery Priyanto*, Tris Zeno Alkindi, Hasta Saputra, Agus Dwi Setiyono, Panji Zulfikar Sidik

Puslabfor Bareskrim Polri, Indonesia

*Correspondence E-mail: herypriyanto2004@gmail.com

ARTICLE INFO

Article history:

Received 15 July 2021

Revised 25 August 2021

Accepted 22 September 2021

Available online 19 October 2021

Keywords: network, medsos, otomatisasi

Kata kunci: network, account, otomatitasion

DOI:

<https://doi.org/10.54579/jfe.v1i3.3>

How to Cite :

Priyanto, H., Alkindi, T. Z., Saputra, H., Setiono, A. D., Sidik, P. Z. (2021). Pemeriksaan Network Forensik Terhadap Barang Bukti Digital Akun Media Sosial Menggunakan Metode Otomatisasi Software Secara Online. *Journal of Forensic Expert*, 1(3), 8-18.

ABSTRACT

The development of information technology is currently very fast, which is marked by the ease with which people have computers and smartphones and access social media through high-speed internet in Indonesia. This condition has started several years ago, and shows that Indonesia has entered the digital era. The digital era brings many benefits to human life, as well as emerging new types of crime that are increasingly complex, namely cyber crime or known as cyber crime. This cyber crime is very detrimental and has a negative impact on the security and comfort of the community, economic stability and the condition of security and social security and the Indonesian state defense system, for this reason a professional investigation process is needed by Polri investigators. One of the roles of the Polri Labfor is to support the tasks of Polri investigators in terms of scientific evidence (Scientific Crime Investigation), especially the examination of digital evidence in the form of social media accounts, the problem that arises is that the inspection process at the Polri Labfor against digital evidence is still manual, so the process requires it takes a long time and the data/information obtained is incomplete and comprehensive. For this reason, it is necessary to examine and analyze digital evidence in the form of social media accounts using the Online Software Automation method. The results obtained using this method are obtaining complete data/information and having categorization capabilities, especially on data faces or mapping analysis based on a person's face from digital evidence in the form of social media accounts.

ABSTRAK

Perkembangan teknologi informasi saat ini sangat pesat yang ditandai dengan semakin mudahnya masyarakat untuk memiliki komputer dan *smartphone* serta mengakses media sosial melalui *internet* berkecepatan tinggi di Indonesia. Kondisi ini sudah dimulai sejak beberapa tahun yang lalu, dan menunjukkan bahwa Indonesia sudah memasuki era digital. Era digital tersebut membawa banyak manfaat bagi kehidupan manusia, di samping juga muncul jenis kejahatan baru yang semakin lama semakin berkembang kompleks, yaitu *cyber crime* atau dikenal dengan istilah tindak pidana siber. Tindak pidana siber ini sangat merugikan dan berdampak negatif pada keamanan dan kenyamanan masyarakat, stabilitas ekonomi dan kondisi kamtibmas serta sistem pertahanan negara Indonesia, untuk itu diperlukannya proses penyidikan yang profesional oleh penyidik Polri. Salah satu peran Labfor Polri adalah mendukung tugas penyidik Polri dalam hal pembuktian secara ilmiah (Scientific Crime Investigation) khususnya pemeriksaan terhadap barang bukti digital berupa akun media sosial, permasalahan yang muncul adalah proses pemeriksaan di Labfor Polri terhadap bukti digital tersebut masih manual, sehingga prosesnya membutuhkan waktu yang cukup lama dan data/informasi yang didapatkan tidak lengkap dan menyeluruh. Untuk itu diperlukannya proses pemeriksaan dan analisa terhadap bukti digital berupa akun media sosial menggunakan metode Otomatisasi Software secara Online. Hasil yang didapat menggunakan metode ini adalah didapatkannya data-data/informasi secara lengkap dan mempunyai kemampuan kategorisasi khususnya pada data *faces* atau analisa pemetaan berdasarkan wajah seseorang dari bukti digital berupa akun media sosial.

Pendahuluan

Penyelidikan dan penyidikan kasus tindak pidana siber tidak hanya berhenti dalam pencarian dan menemukan tersangka, namun kasus tersebut perlu dibuktikan secara ilmiah bahwa memang benar tersangka memang benar adalah pelakunya dengan didukung bukti-bukti yang kuat secara ilmiah dan hukum. Salah satu fenomena tindak pidana siber saat ini yaitu munculnya berbagai jenis kasus pencemaran nama baik dan berita hoax dengan menggunakan akun media sosial seperti *facebook* dan *twiter*, yaitu selama periode bulan maret di saat pandemi covid 19 terdapat 13 isu hoax terkait covid 19 dan total isu hoax terkait covid 19 sebanyak 1.470 berdasarkan data per 10 Maret 2021 (Antara, 2021). Para pelaku kejahatan siber bekerja dengan menggunakan akun media sosial antara lain facebook/twiter, mereka menggunakan akun-akun tersebut untuk membuat berita-berita hoax dan membuat dapat tersebarnya atau teraksessnya informasi tersebut di masyarakat umum. Barang bukti dalam kejahatan siber tidak hanya berbentuk barang bukti elektronik, namun dapat juga berupa barang bukti digital yang merupakan barang bukti berupa *files*, *web history*, akun media sosial dan *log files* yang merupakan bukti jejak-jejak digital dari suatu kejahatan siber. Untuk itu, investigasi tindak pidana siber sangat membutuhkan kehadiran ahli-ahli Digital Forensik untuk dapat mengungkap dan membuktikan kasus-kasus tersebut. Puslabfor sebagai ujung tombak dan tulang punggung SCI (Scientific Crime Investigation) telah membangun kemampuan Digital Forensik sejak sekitar tahun 2000 yang menitikberatkan pada pembangunan kompetensi SDM yang berbasis *knowledge* (pengetahuan), *skill* (keterampilan) dan *attitude* (sikap) sebagai pemeriksa ahli agar kuat legitimasinya sehingga dapat diterima sebagai Keterangan Ahli di dalam persidangan. Mengikuti perkembangan teknologi informasi, kasus-kasus cyber crime dan computer-related crime menjadi semakin tinggi jumlahnya dan semakin kompleks khususnya kejahatan yang menggunakan media sosial. Hal ini menuntut Puslabfor untuk semakin berkembang dalam memberikan dukungan teknis digital forensik guna pengungkapannya. Tuntutan tersebut mencakup pengembangan system dan metode pemeriksaan dan Analisa barang bukti Media Sosial, sehingga Puslabfor mampu memberikan pemeriksaan digital forensik yang maksimal dalam mendukung tugas penyidik untuk proses pembuktian secara ilmiah.

Sejalan dengan bertambahnya jumlah barang bukti dan perkembangan teknologi yang cepat khususnya barang bukti akun media sosial dan cloud yang berkaitan dengan tindak pidana ITE, *Computer Crime* dan *Computer Related Crime* serta perubahan perilaku masyarakat Indonesia yang mengarah kepada penggunaan media sosial (*facebook*, *twiter*, *instagram*, *tiktok*, *youtube*, *email*, dll) dan tren *internet* secara masif dan tinggi di tahun 2021. Tingginya penggunaan media sosial di Indonesia tersebut tentunya juga akan berdampak negatif kepada perkembangan tindak pidana yang menggunakan media sosial seperti penyebaran konten pornografi, berita hoax dan radikalisme. Beberapa rentetan kasus kejahatan siber yang terjadi di Indonesia dengan menyalahgunakan akun media sosial yaitu isu tujuh kontainer berisi surat suara yang sudah dicoblos di tanjung priok yang dilakukan oleh tersangka IK dan kabar tersebut beredar luas di media sosial seperti *youtube*, *twiter*, *facebook*, *instagram* hingga *whatsapp* (Kompas, 2019), kasus penyebaran konten pronografi yang dilakukan oleh GA dan NB yang beredar di media sosial dengan durasi 19 detik yang beredar di *twiter* menjadi trending topic dan menjadi berita viral di akhir tahun 2020 (Kompas, 2020) dan isu mengenai hoaks covid 19 di

media sosial mencapai 1.819 isu dengan sebaran mencapai 4.163 unggahan (Ditjen Aptika, 2021).

Dengan latar belakang rentetan kasus-kasus kejahatan siber yang menggunakan akun media sosial tersebut menjadi tantangan bagi penyidik Polri untuk membuktikan ada atau tidaknya jejak digital yang tertinggal yaitu berupa barang bukti digital akun media sosial yang digunakan oleh seseorang, sehingga penyidik harus mampu membuktikan keterkaitan antara bukti digital dengan tersangka. Permasalahan yang muncul adalah bagaimana penyidik membuktikan bahwa seorang tersangka benar menggunakan akun media sosialnya untuk melakukan kejahatan siber dan adakah bukti yang mendukung bahwa segala ucapannya yang mengarah pada kejahatan siber masih tertinggal dalam bentuk jejak digital. Untuk itu dalam penelitian ini sangat penting khususnya dalam hal pembuktian secara ilmiah sebagai upaya mendukung tugas penyidik untuk menyajikan fakta fakta dan bukti bukti digital ada atau tidaknya suatu tindak pidana kejahatan siber yang menggunakan akun media sosial melalui pemeriksaan dan analisa dengan menggunakan metode otomatisasi software secara online. Dalam dunia maya hampir semua dapat dilakukan, media sosial mampu menyediakan platform bagi penggunanya untuk dapat berbicara, memberikan pendapat tentang suatu hal tanpa sensor atau kontrol yang diawasi, dikarenakan hal tersebutlah maka akan timbul penyalahgunaan akun media sosial yang mengarah kepada kejahatan siber. Pemeriksaan *network* forensik dapat dijadikan acuan untuk membuat terang suatu tindak pidana dengan menyajikan bukti – bukti digital, yang mana bukti tersebut dapat dijadikan salah satu bukti yang sah di depan pengadilan yaitu melalui keterangan ahli dan surat (Berita Acara Pemeriksaan Laboratoris Kriminalistik Barang Bukti) yang mengacu ke dalam Pasal 184 ayat (1) Kitab Undang Undang Hukum Acara Pidana (KUHP) disebutkan bahwa alat bukti yang sah adalah keterangan saksi, keterangan ahli, surat, petunjuk dan keterangan terdakwa. Dikarenakan pentingnya barang bukti digital tersebut dalam memberikan petunjuk atau pengungkapan kasus kejahatan *network*, Untuk itu penanganan barang bukti digital akun Medsos harus sesuai dengan prinsip-prinsip dasar digital forensik yang mengacu kepada guidelines internasional seperti yang diterbitkan oleh Association of Chief Police Officers (ACPO) dan 7Safe di Inggris, dan oleh National Institute of Justice yang berada di bawah Department of Justice, Amerika Serikat. Dengan penanganan barang bukti digital akun Medsos yang benar, diharapkan hasil pemeriksaan dan analisa bidang *network* forensik dapat menunjukkan secara ilmiah kepemilikan akun dan bukti bukti digital yang ada di dalam akun tersebut untuk mendukung tugas penyidik dalam mengungkap kejahatan.

Pemeriksaan *network* forensik dengan metode otomatisasi software secara online dipengaruhi oleh beberapa faktor, yaitu ; jenis akun medsos, password akun medsos dan software yang digunakan untuk melakukan ekstraksi secara *online*. Pengertian otomatisasi yang kata dasarnya adalah otomatis, kata ini berasal dari bahasa Inggris (Automatic) yang berarti bekerja sendiri, dalam KBBI otomatisasi adalah pergantian tenaga manusia dengan tenaga mesin secara otomatis melakukan dan mengatur pekerjaan, sedangkan software adalah data yang diprogram, disimpan dan diformat secara digital dengan fungsi tertentu dan online mengandung arti dalam jaringan (daring) yaitu yang terhubung ke suatu jaringan internet sehingga pengertian dari metode otomatisasi software secara online dapat diartikan sebagai metode yang dilakukan oleh suatu data yang telah diprogram yang terhubung langsung dengan jaringan internet. Dalam penelitian ini faktor yang akan dianalisis adalah kemampuan melakukan ekstraksi terhadap data-

data dan informasi digital yang berada di suatu akun medsos dengan menggunakan metode otomatisasi software secara online. Selama ini pemeriksaan dan analisa terhadap barang bukti akun medsos dilakukan secara manual atau live analysis. Diharapkan dalam penelitian ini dapat diketahui kemampuan software oxygen cloud extractor untuk mengambil data-data digital secara lengkap.

Metode

Extraction atau proses ekstraksi terhadap dari barang bukti digital akun medsos dilakukan dengan metode otomatisasi secara online yang mana prosesnya dilakukan dengan memasukkan nama akun dan password serta kode verifikasi tertentu jika diperlukan dengan menghubungkan perangkat *software* melalui jaringan internet dan melakukan akses secara otomatis ke server suatu akun medsos. Dalam penelitian ini dilakukan *extraction* dengan metode otomatisasi software oxygen cloud extractor untuk mendapatkan data-data dan informasi yaitu data akun, *contacts*, *files*, *messages*, *faces*, dan *statistics*. Dalam penelitian ini juga menggunakan 5 (lima) tahapan proses forensik dari *National Institute of Justice* (NIJ) yaitu :

Gambar 1. Lima tahapan proses forensik dari *National Institute of Justice* (NIJ)

Pemeriksaan *network* forensik dapat dilakukan dengan beberapa software baik yang bersifat open source maupun closed source. Software tersebut juga bervariasi ada yang hanya bisa melakukan pemeriksaan dan analisa terhadap beberapa akun medsos saja, namun ada juga yang bisa mencakup semua jenis medsos. *Software* ekstraksi yang digunakan dalam penelitian ini yaitu *Oxygen Forensic Cloud Extractor* versi 7.4.0.34.

Sampel

Sampel dalam penelitian ini adalah barang bukti 1 (satu) akun medsos facebook dengan *user name* : mcbill1914@gmail.com.

HASIL DAN PEMBAHASAN

Hasil

Tahapan proses ekstraksi terhadap barang bukti akun media sosial dengan menggunakan metode otomatisasi software secara online yaitu tahapan Identification : melakukan identifikasi terhadap barang bukti digital yaitu berupa akun media sosial *facebook*; Collection : melakukan uji otentifikasi terhadap barang bukti digital berupa akun media sosial facebook telah sesuai dengan user dan password dan menjaga integritas barang bukti dari perubahan; Examination : melakukan pemeriksaan/akuisisi dengan proses ekstraksi dari barang bukti digital akun media sosial facebook dan melakukan verifikasi dengan hash analysis SHA1; Analysis : Melakukan proses analisa terhadap hasil ekstraksi atau parsing dari barang bukti digital akun media sosial yang sesuai dengan data-data investigatif kasus dan Reporting : Pembuatan report dalam bentuk PDF files yang menjelaskan proses tahapan atau tindakan yang dilakukan oleh pemeriksa digital forensik

Tahapan penggunaan *software* (dokumentasi dan koneksi dari sampel barang bukti)

Menggunakan Software *Oxygen Forensic Cloud Extractor* versi 7.4.0.34

Melakukan proses pencarian jenis akun medsos yang akan diperiksa dan dianalisa yaitu *facebook*, maka tampilan pada gambar bertuliskan aplikasi *facebook* pada gambar 1.

Gambar 1. Aplikasi Medsos *facebook*.

Selanjutnya melakukan analisa dengan memasukkan authentication parameters berupa user name dan password pada gambar 2.

Gambar 2. Username : mcbill1914@gmail.com dan password : xxxxxxx

Metode otomatisasi secara online dengan cara melakukan koneksi secara otomatis ke server medsos facebook dan memvalidasi bahwa akun tersebut tervalidasi di server facebook serta melakukan otomatisasi kategori data-data dan informasi yang akan dilakukan ekstraksi (Gambar 3)

Gambar 3. Validasi dan otomatisasi

Proses esktraksi secara otomatisasi ke akun medsos facebook dengan user name : mcbill1914@gmail.com.

Gambar 4.Extracting data from clouds services

Analisis hasil ekstraksi

Hasil ekstraksi terhadap barang bukti 1 (satu) akun medsos facebook dengan *user name* : mcbill1914@gmail.com dilakukan dengan menggunakan oxygen forensic detective didapatkan hasil sebagai berikut :

Gambar 5. Analisa terhadap file *cloud backup* : 4642AFBAA65447959D82E64336E05B8F_14042021_170645.ocb dengan source files yaitu : main.db3.

Analisis Data

Perhitungan tingkat keberhasilan data-data dan informasi yang berhasil di ekstraksi dengan metode otomatisasi secara online dilakukan dengan menghitung jumlah data hasil ekstraksi pada *contacts*, *files*, *messages*, *faces*, *key evidence*, *timeline* dan *aplication facebook*.

Hasil parsing pemeriksaan *network* forensik terhadap ekstraksi metode *otomatisasi* secara *online* terhadap barang bukti 1 (satu) akun medsos facebook dengan *user name* : mcbill1914@gmail.com dengan menggunakan *software Oxygen Forensic Cloud Extractor* versi 7.4.0.34 yaitu:

Tabel 1. Tabulasi data-data dan informasi yang berhasil di ekstraksi.

No	Jenis data dan informasi	Jumlah
1	<i>Contacts</i>	1,625
2	<i>Files</i>	1,586
3	<i>Messages</i>	31
4	<i>Faces</i>	911
5	<i>Key Evidence</i>	1
6	<i>Timeline</i>	31
7	<i>Application facebook</i>	1,897

Data *last contacted*

Gambar 6. Data *last contacted*

Data top 10 *contacts*

Gambar 7. Data 10 *contacts*

Data top 10 *groups*

Gambar 8. Data 10 *groups*

Data faces filtes

Gambar 9. Data filters faces

Pembahasan

Metode ekstraksi pemeriksaan dan analisa terhadap barang bukti akun medsos secara otomatisasi *software* secara *online* merupakan metode yang paling efektif dikarenakan data-data dan informasi yang di dapat jauh lebih banyak dan lengkap khususnya terhadap data-data digital berupa last contacted, top 10 contacts, top 10 groups dan faces filters. Terdapat banyak data-data yang berhasil di ekstraksi menggunakan metode ini. Sebagai contoh data-data digital yang didapatkan yaitu terpetakakannya secara otomatis 10 (sepuluh) kontak yang paling sering dihubungi melalui akun medsos barang bukti yang mana data ini sangat diperlukan oleh penyidik untuk memudahkan melakukan trace kepada siapa saja akun tersebut sering berhubungan; 10 (sepuluh) kontak groups yang sering terhubung dengan akun barang bukti ini, yang mana data-data tersebut sangat berguna bagi penyidik khususnya pada tindak pidana terorisme dan radikalisme dimana penyidik membutuhkan data atau bukti bukti bahwa akun tersebut paling banyak berkomunikasi dengan grup apa saja dan data digital berupa face filters yang secara otomatis dapat memetakan dan atau mengkatagorikan data-data digital berdasarkan gambar wajah seseorang berdasarkan jenis kelamin, ras (*asian*, *black*, *hispanic* dan *white*), umur (antara 0-25, 25-30, 30-35 dan 70+) dan asesoris yang dipakai (tanpa asesoris, menggunakan kacamata, topi, masker dan *reading glasses*) hal ini sangat diperlukan penyidik dan pemeriksa forensik untuk mempercepat proses pencarian dan indexing serta analisa terhadap identitas seseorang. Pada

penelitian ini menggunakan software *Oxygen Forensic Cloud Extractor* versi 7.4.0.34 dengan metode yaitu otomatisasi software secara *online*.

Berdasarkan hasil yang didapatkan dari analisa *parsing* dan *decoding* terhadap barang bukti 1 (satu) akun medsos facebook dengan *user name* : *mcbill1914@gmail.com* khususnya pada jumlah data – data digital, didapatkan bahwa data – data digital yang dapat dilakukan ekstraksi dan decoding lebih banyak dan lengkap berupa *last contacted*, *top 10 contacts*, *top 10 groups* dan *faces filters*.

Kemampuan mendapatkan data-data digital pada barang bukti akun medsos dengan menggunakan metode otomatisasi software secara online tersebut dikarenakan karena proses otomatisasi yang mampu menembus server akun medsos tersebut dan keunggulan dalam melakukan data decoding terhadap *file* main.db3. Keunggulan dari metode ini yaitu penghematan waktu, yang mana proses ekstraksi dapat dilakukan lebih cepat secara otomatis yang sebelumnya dilakukan secara manual, penghematan dari aspek biaya yang mana proses ekstraksi dilakukan secara otomatis tanpa membutuhkan tenaga manusia secara menyeluruh, proses otomatisasi dapat mengurangi resiko kesalahan analisa jika dilakukan secara manual dan proses ekstraksi lebih muktahir karena menggunakan teknologi software yang otomatis sehingga pemeriksaan dan analisa terhadap barang bukti akun media sosial dapat dilakukan secara efektif dan efisien.

Penutup

Berdasarkan penelitian ini, disimpulkan bahwa pemeriksaan dengan menggunakan metode otomatisasi software secara *online* terhadap barang bukti 1 (satu) akun medsos facebook dengan *user name* : mcbill1914@gmail.com dengan menggunakan software *Oxygen Forensic Cloud Extractor*, yang mana hasil ekstraksi yang di dapat khususnya *last contacted*, *top 10 contacts*, *top 10 groups* dan *faces filters* mampu mendapatkan data-data secara lengkap dan mempunyai kemampuan kategorisasi khususnya pada data *faces* atau analisa pemetaan berdasarkan wajah seseorang. Implikasi dari data-data dan informasi yang lengkap tersebut dapat membantu tugas penyidik terhadap pengungkapan kasus kejahatan siber yang menggunakan akun media sosial, yang mana dari data-data dan informasi tersebut dapat membuktikan jejak jejak digital yang mengarah kepada kejahatan siber dan dapat memberikan informasi kepada penyidik mengenai pengembangan kasus lebih lanjut seperti jejak jaringan atau koneksi jejaring pelaku kejahatan siber lainnya yang terkoneksi dengan tersangka.

Daftar Pustaka

- ACPO, 7Safe (2008). Good Practice Guide for Computer-Based Electronic Evidence. UK ACPO and 7Safe.
- Al-Azhar, M.N. (2012). "Digital Forensic: Panduan Praktis Investigasi Komputer". Salemba Infotek, Jakarta.

Al-Azhar, M.N. (2021). “Seri 1 Digital Forensik Panduan Umum digital Forensik pada Platform Windows, Linux, Mac, & Mobile”. Salemba Infotek, Jakarta.

Facebook. Dapat di akses di <https://www.facebook.com/>.

ISO/IEC 27037 tentang Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence.

National Institute of Justice (2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement. US National Institute of Justice.

OXYGEN.2021.FORENSIC. Dapat di akses di <https://www.oxygen-forensic.com/en/products/oxygen-forensic-detective>.

oxygen-forensic-detective (2019). “Manual book Oxygen Forensic Cloud Extractor”. Washington, U.S.

Peraturan Kepala Pusat Laboratorium Forensik Badan Reserse Kriminal Polri Nomor 1 Tahun 2014 tentang Standar Operasional Prosedur Pemeriksaan dan Analisa Digital Forensik.