

PERANCANGAN PERBANDINGAN *LIVE FORENSICS* PADA KEAMANAN MEDIA SOSIAL INSTAGRAM, FACEBOOK DAN TWITTER DI WINDOWS 10

Rauhulloh Ayatulloh Khomeini Noor Bintang^{1*}, Rusydi Umar² dan Anton Yudhana¹

¹Program Studi Teknik Informatika, Universitas Ahmad Dahlan

²Program Studi Sistem Informasi, Universitas Ahmad Dahlan

Jl. Prof. Dr. Soepomo, Umbulharjo, Janturan Yogyakarta 55164.

*Email : rauhulloh1708048021@webmail.uad.ac.id

Abstrak

Berkembangnya teknologi terutama di media sosial saat ini semakin mempermudah untuk bertukaran suatu informasi. Banyaknya pengguna media sosial tersebut tidak mengerti akan keamanan suatu media sosial. Teknik digital forensik digunakan dengan melakukan analisis komputer atau perangkat lunak digital. Analisis digital forensik terbagi menjadi 2 kategori yaitu Dead/Tradisional dan Live. Analisis Dead menyangkut data yang tersimpan permanen di dalam suatu perangkat, sedangkan Analisis Live analisis yang bersifat sementara atau data yang disimpan dalam perangkat lunak. Paper ini mengusulkan analisis forensik live disistem menggunakan Operasi Sistem Windows10 yg terbaru saat ini. Metode yang akan digunakan yaitu National Institute of Justice (NIJ) dengan tahapan berikut Collection, Examination, Analysis dan Reporting. Metode berikut diharapkan dapat menghasilkan bukti digital forensik yang dapat mengetahui tingkat keamanan pada media sosial Facebook, Instagram dan Twitter.

Kata kunci : *Live Forensics, Media Sosial, Browser.*

1. PENDAHULUAN

Pada era informasi saat ini pengguna *media sosial* selain sebagai alat untuk mengirim dan menerima informasi juga sebagai tempat untuk menyimpan suatu data informasi karena media sosial terhubung dengan berbagai akun media sosial. Pengguna akun media sosial saat ini bertambah banyak dari tahun ke tahun seiring dengan jumlah penggunaanya terus bertambah. Teknologi informasi adalah salah satu bukti perkembangan teknologi yang semakin pesat.

Media sosial adalah sebuah media yang terhubung dengan internet secara online sehingga para pengguna dapat melakukan aktifitas seperti *sharing*, berpartisipasi, didalam dunia maya meliputi website, blogger, ataupun jejaring sosial. Media sosial berfungsi untuk memudahkan pengguna melakukan interaksi sosial dengan menggunakan teknologi melalui internet sehingga mengubah cara penyebaran informasi sebelumnya yang bersifat penyebaran informasi yang dapat diterima oleh banyak pengguna yang menggunakan media sosial. Media sosial yang sering digunakan saat ini diantara lain media sosial *facebook*, *Instagram* maupun *twitter* maupun media sosial lain nya.

Sejarah internet (*International Networking*) yaitu berawal dari penelitian untuk pertahanan pada perang dunia pertama. Internet menjadi sangat penting dalam kehidupan sehari-hari, aplikasi yang digunakan untuk melakukan internet biasa disebut dengan browser. Jenis browser saat ini semakin banyak dan berkembang dengan pesat diantaranya Mozilla Firefox, Google Chrome, Microsoft Edge, Internet Explore, Opera, Safari dan lainnya (Bickford & Giura, 2015).

Analisis digital forensic umumnya ada dua, yakni dead forensic dan live forensic. Dead forensic merupakan suatu teknik yang membutuhkan data yang disimpan secara permanen dalam perangkat media penyimpanan umumnya hardisk. Live forensic yaitu suatu teknik analisis dimana menyangkut data yang berjalan pada system atau data volatile yang umumnya tersimpan pada Random Access Memory (RAM) atau transit pada jaringan (Faiz, Umar, & Yudhana, 2016).

Digital forensics pada intinya adalah menemukan bukti digital bisa tersimpan pada penyimpanan computer sementara, penyimpanan permanen, USB, CD, lalu lintas jaringan, dan lainnya. Digital forensic kemudian berkembang menjadi sesuatu yang penting dalam keamanan informasi. Keterlibatan suatu perangkat atau media dalam kejahatan computer dibedakan menjadi tiga yaitu :

- Komputer menjadi tujuan
- Komputer menjadi sarana untuk membuat kejahatan
- Komputer berfungsi menyimpan segala informasi yang mengandung tindak pidana.

Teknik live forensics ini sangat bergantung pada keadaan komputer yang sedang menyala, karena membutuhkan data yang berjalan pada Random Access Memory (RAM). Data pada RAM disebut juga data volatile atau data sementara yaitu data yang hanya terdapat saat komputer menyala jika komputer mati maka data itu akan hilang. Data volatile ini berisi data penting seperti username, password, file akses, file modifikasi, aplikasi yang digunakan, kata kunci pencarian. Username dan password merupakan hal yang penting dalam suatu akun seperti email. Email ini biasanya mengirimkan sesuatu yang penting bahkan data privasi suatu perusahaan atau penggunanya. (Faiz, Umar, & Yudhana, 2016).

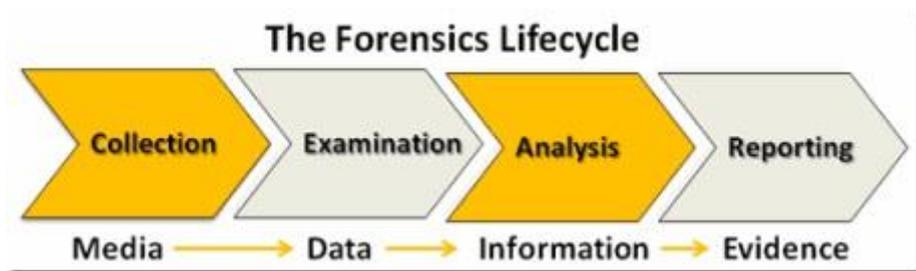
Penelitian yang dilakukan oleh Ellick M. Chan tahun 2011 pada disertasinya bahwa urutan langkah dalam membantu menangani suatu masalah digital forensics yaitu :

1. Preparation : Siapkan peralatan dan alat-alat untuk melakukan tugas-tugas yang diperlukan selama penyelidikan.
2. Collection : Cari, dokumen, dan mengumpulkan atau membuat salinan dari objek fisik yang berisi bukti elektronik.
3. Examination : Membuat bukti elektronik terlihat dan dokumen dari isi sistem. Reduksi data dilakukan untuk mengidentifikasi bukti.
4. Analysis : Menganalisis bukti dari tahap Pemeriksaan untuk menentukan fi signigance dan nilai pembuktian.
5. Reporting : Buat catatan pemeriksaan setelah setiap kasus..

2. METODOLOGI

2.1. Metode Penelitian

Berdasarkan penelitian yang dilakukan oleh Ellick M. Chan maka peneliti akan menggunakan metodologi penelitian The U.S. National Institute of Justice (NIJ) yang digambarkan dengan alur pada Gambar 1.



Gambar 1. Metode Tahapan Digital *Forensics Method*.

Berikut adalah penjelasan dari tahapan *National Institute of Justice (NIJ)* :

1. *Collection* (Pengumpulan)
Merupakan tahapan awal, yakni melakukan analisis kebutuhan mengumpulkan barang yang ingin dilakukan penyelidikan seperti *imaging, record*, berdasarkan sumber data yang akurat.
2. *Examination* (Pemeriksaan)
Dalam tahapan ini melakukan pemeriksaan terhadap data yang telah di kumpulkan pada tahap *Collection*.
3. *Analysis* (Analisa)
Dalam tahapan ini dilakukan analisa hasil pemeriksaan dengan menggunakan metode yang sudah ditetapkan untuk mengetahui keseluruhan informasi yang dibutuhkan.
4. *Reporting* (Laporan)
Dalam tahapan ini dilakukan melaporkan dan menjelaskan apa yang telah dianalisis kemudian dipaparkan barang bukti yang telah ditemukan dan didokumentasikan secara rinci.

2.2. Alat dan Bahan

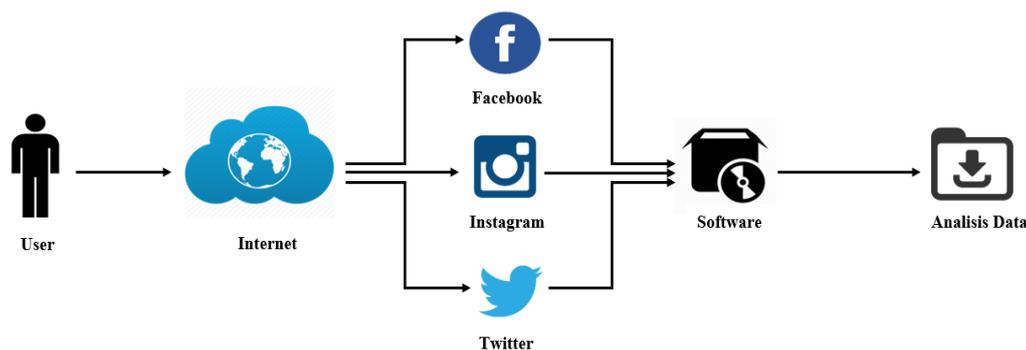
Alat dan materil yang digunakan pada penelitian ini meliputi:

- a. Perangkat keras
1 unit laptop Asus A46C

- b. Perangkat lunak
 - Sistem Operasi Windows 10 64bit
 - Software FTK Imager
 - Media Sosial (Facebook, Instagram, Twitter)

2.3. Rancangan Sistem

Sebuah rancangan untuk mendapatkan suatu bukti digital untuk dilakukan analisis. Pada penelitian ini menganalisa dari ketiga media sosial tersebut sehingga mengeluarkan data analisis. Sebuah rancangan digambarkan pada gambar 2 berikut:



Gambar 2. Tahapan Analisis

Pada gambar 2 dilakukan tahapan analisis terhadap tiga media sosial berbeda yaitu *Facebook*, *Instagram*, dan *Twitter*. Dimana tahap akhir nanti mengeluarkan suatu data analisis dari perangkat lunak FTK imager.

3. HASIL DAN PEMBAHASAN

Untuk melakukan analisis forensik media sosial pada perangkat laptop atau komputer di butuhkan sebuah metode dan tools guna membantu peneliti guna mencari data untuk di investigasi forensik. Penelitian ini diawali dengan membuat akun media sosial *Facebook*, *Instagram* dan *Twitter*, Selanjutnya penelitian ini melakukan pemilihan tools untuk mengambil data pada akun media sosial berikut. Pada tahap ini tools yang akan digunakan menggunakan tools FTK Imager sebagai pengelola pada data yang akan di analisis.

Selanjutnya pada saat membuat akun media sosial *Facebook*, *Instagram* dan *Twitter* di lakukan dengan cloning data dan Hashing data fungsi nya yaitu meyakinkan bahwa akun media sosial *Facebook*, *Instagram* dan *Twitter* menjadi nilai yang merepresentasikan string asli atau akun asli. Tahapan berikutnya yaitu akun media sosial tersebut akan di analisis untuk mendapatkan data yang dapat menjadi barang bukti data forensik yang valid.

Pada tahapan terakhir dilakukan *reporting* atau laporan hasil penelitian mengenai data pada media sosial berupa barang bukti data yang valid pada media sosial tersebut, dalam *reporting* juga menjelaskan tahapan-tahapan atau proses yang digunakan untuk mendapatkan barang bukti yang dibutuhkan agar data tersebut terbukti asli atau valid.

4. KESIMPULAN

Penelitian ini menggunakan *The U.S National Institute of Justice* (NIJ) sebagai metode, metode ini memiliki beberapa tahapan (*Collection*, *Examination*, *Analysis* dan *Reporting*) berikut dijalankan menggunakan perangkat lunak (*tools FTK Imager*) sebagai bahan pendukung untuk mengetahui keamanan masing-masing pada media sosial (*facebook*, *twitter*, dan *instagram*). Untuk meyakinkan bahwa akun media sosial (*facebook*, *twitter* dan *instagram*) menjadi nilai yang merepresentasikan string asli atau akun asli lakukan dengan cloning data dan Hashing data fungsi. Berdasarkan hasil dari tahapan-tahapan metode yang dilakukan, proses analisis mengenai data pada media sosial (*facebook*, *twitter*, dan *facebook*) berupa barang bukti data yang valid (asli atau palsu).

DAFTAR PUSTAKA

- Anwar, nuril and Riadi, I. (2017), Analisis Investigasi Forensik WhatsApp Messenger Smartphone Terhadap WhatsApp Berbasis Web, *Jurnal Ilmiah Teknik Elektro Komputer dan Informatika*, 3(1), pp. 1–10.
- Bickford, J., dan Giura, P. (2015), Safe Internet Browsing using a Transparent Virtual Browser. IEEE, pp. 423-432.
- Faiz, M. N. *et al.* (2016), Analisis Live Forensics Untuk Perbandingan Keamanan Email Pada Sistem Operasi Proprietary, *Jurnal Ilmiah ILKOM*, 8(3), pp. 242–247.
- Faiz, M. N., Umar, R. and Yudhana, A. (2017), Implementasi Live Forensics untuk Perbandingan Browser pada Keamanan Email, *JISKa*, 1(February), pp. 108–114.
- Larasati, T. D. and Hidayanto, B. C. (2017), Analisis Live Forensics Untuk Perbandingan Aplikasi Instant Messenger Pada Sistem Operasi Windows 10, *Sesindo*, 6(November), pp. 456–256.
- Prasetyo, A., Teknik, F. and Telkom, U. (2015), Identifikasi Bukti Digital Pada Sim Card Untuk Mobile Forensic Digital Evidence Identification on Sim Card for Mobile, 2(2), pp. 6408–6414.
- Soliha, S. F. (2015), Tingkat Ketergantungan Pengguna Media Sosial Dan Kecemasan Sosial, *Interaksi: Jurnal Ilmu Komunikasi*, 4(1), pp. 1–10. doi: 10.14710/INTERAKSI,4,1,1-10.
- Umar, R., Yudhana, A. and Faiz, M. N. (2016), Analisis Kinerja Metode Live Forensics Untuk Investigasi Random Access Memory Pada Sistem Proprietary, *Prosiding Konferensi Nasional Ke- 4 Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM)*, (April), pp. 207–211.
- Utami, A. D. and Purnama, B. E. (2012), Pemanfaatan jejaring sosial sebagai media bisnis online (studi kasus di Batik Solo 85), *Seruni FTI UNSA*, 1, pp. 1–7.
- W, Y., Riadi, I. and Yudhana, A. (2016), Analisis Keamanan Websserver Menggunakan Metode Penetrasi Testing, *Annual Research Seminar*, 2(1), pp. 300–304.