RANCANGAN INVESTIGASI FORENSIK EMAIL DENGAN METODE *NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY* (NIST)

Mustafa[1*], **Imam Riadi**[2] **dan Rusydi Umar**[1]
[1]Program Studi Teknik Informatika, Universitas Ahmad Dahlan
[2]Program Studi Sistem Informasi, Universitas Ahmad Dahlan
Jl. Prof. Dr. Soepomo,S.H, Warungboto, Yogyakarta 55164
[*]Email: mustafa.ramliannor@gmail.com

Abstrak

Ilmu forensik merupakan ilmu yang relatif baru dan bahkan belum banyak dikenal di kalangan masyarakat. Kejahatan di dunia cybercrime memiliki banyak variasi berbeda dengan dunia nyaya, salah satunya adalah pemalsuan atau spam email, dimana spam email tersebut dapat menjadi alat transportasi konten berbahaya dalam sebuah jaringan. Permasalahan yang timbul pada saat ini adalah sangat jarang penelitian yang dilakukan dalam hal investigasi forensik dalam menghadapi kejahatan dalam dunia cyber, khususnya dalam email spam tersebut. Metode yang digunakan adalah National Institute of Standards and Technology (NIST) dengan tahapan Collection, Examination, Analisys dan Reporting. Metode ini diharapkan dapat menghasilkan bukti digital yang dapat digunakan dalam proses penegakan hukum untuk mengungkap kejahatan digital.

Kata kunci : *email forensic, email, cyber, komputer forensik*

1. PENDAHULUAN

Ilmu forensik yaitu merupakan penggunaa teknik atau metode saint untuk memberikan bukti yang benar pada sebuah pengadilan atau pemerikasaan hukum yang terkait (Jansen, 2008). Secara umum ilmu forensik adalah cara untuk menemukan jawaban dari pernyataan-pernyataan yang sering muncul pada proses penyelidikan peristiwa atau kejadian (Karsono, 2012). Metode komputer forensik adalah pencarian, menyita dan pencarian informasi yang terkait. Mencari dan menyita merupakan metode yang pertama dilakukan untuk mencari bukti, sedangkan pencarian informasi sebagai pelengkap data sebagai barang bukti tersebut (Budiman, 2001). Komputer forensik juga bisa menentukan potensi bukti legal dalam penyelidikan dan analisis komputer (Utdirartatmo, 2001). Dari hasil pengujian dan analisi sistem pengamanan jaringan komputer dapat di rancang dengan bukti forensik jaringan komputer, setelah dibuat sistem pengamanan jaringan komputer, penyerang tidak mampu melakukan serangan pada waktu yang akan datang dengan menggunakan cara yang sama (Fadlil, 2017).

Internet forensics merupakan penelusuran dan investigasi sumber kejahatan dari internet sekaligus mempelajari hal-hal didalamnya (Rafiudin, 2009). Digital forensics analysis pada umumnya ada dua, yaitu *dead forensics* dan *live forensics* (Umar, 2016). *Dead forensic* merupakan 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 sistem atau *data volatile* yang umumnya tersimpan pada *Random Access Memory* (RAM) atau *transit* pada jaringan (Riadi, 2013). Bagian penting dalam digital forensik yaitu keaslian dari barang bukti digital (Agrawal, 2011). Melakukan investigasi melalui tahapan pendekatan prosedur pemeriksaan digital forensik digital adalah cara valid untuk mendapatkan pembuktian (Alharbi, 2011).

Salah satu cabang dari forensik komputer adalah *e-mail* forensik, dimana email atau *electronic mail* (Kurniawan, 2005), merupakan salah satu layanan internet yang sering digunakan dalam masyarakat berupa surat elektronik berbasis *file text*, namun dengan perkembangan teknologi email lebih atraktif dengan penggunanya, jadi email tidak hanya mengirim *file text*, tapi juga dapat mengirimi file lainya, seperti video, gambar, audio dan file ekstensi lainnya. Secara umum email dapat didefinisikan sebagai media pengiriman, penerimaan dan penyimpanan pesan dengan sistem komunikasi elektronik berupa internet. Dari uraian tersebut menjeleskan bahwa email mulai dari menulis, mengirim, diterima sampai dengan dibaca dilakukan secara elektronik (Kakunsi, 2012). Email memiliki dua bagian yaitu *header* dan *body*. Bagian untuk membawa informasi yang

membutuhkan routing email, baris subjek dan *timestamps* adalah *header*. Sedangkan pesan atau data yang disampaikan pada peneriam yaitu *body* (Hoiriyah, 2016).

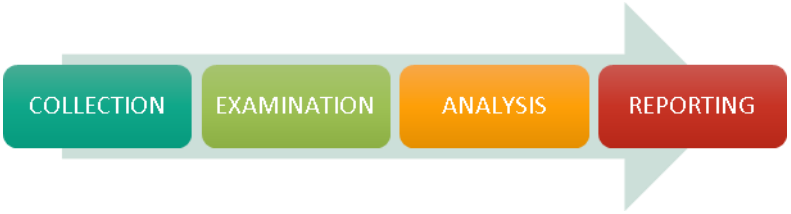
Forensik email dapat diartikan sebagai tindakan pengamanan, pengecekkan, serta menelusuri tentang email palsu dan melakukan pencarian bukti-bukti tentang kejahatan yang menggukan email palsu (Karsono, 2012) Kejahatan yang sering ditemukan menggukan email salah satunya bertujuan mencuri indormasi pribadi dari pemilik (korban) atau ingin mendapatkan akses tidak sah. Kejahatan email tersebut bisa dilakakan dengan cara *spam email*, scam (penipuan), *email spoofing*, dan *phishing* (situs palsu). Akibat kejahatan terbsebut efek negatif pada pemilik bisa kerugian finansial (Ojha, 2012).

National Institute of Standards and Technology (NIST) merupakan metode yang digunakan untuk melakukan forensik analisis. Metode ini sudah banyak digunakan sebagai acuan analisis forensik, contoh pada analisis yang berbasis android, seperti dilakukan Wijaya (2017) yang mengunakan metode NIST untuk menganalisis aplikasi telegram pada *smartphone*.

2. METODOLOGI

2.1. Metode Penelitan

Proses investigasi penelitian ini menggunakan metode *National Institute of Standards and Technology* (NIST). Metode ini mengacu pada tahapan dasar dalam sebuah analisi forensik, yaitu *collection*, *examination*, *analysis*, dan *reporting* yang ditunjukkan pada Gambar 1.



Gambar 1. Tahapan dalam metode *National Institute of Standards and Technologu (NIST)*

Tahapan dalam metode *National Institute of Standards and Technology* (NIST) tersebut adalah sebagai berikut:

a. Collection
Tahap koleksi melakukan indentifikasi, *label*, *record*, dan *retrieve* data dari sumber data yang relevan dengan mengikuti prosedur pelestarian integritas data.

b. Examination
Tahap pemeriksaan melakukan pengolahan data yang dikumpulkan secara forensik dengan menggunakan kombinasi berbagai skenario, baik otomatis maupun manual, menilai dan melepaskan data sesuai kebutuhan sambil menjaga integritas data.

c. Analysis
Tahap analisis melakukan analisa hasil pemeriksaan dengan menggunakan metode yang secara teknis dan legal dibenarkan untuk mendapatkan informasi yang berguna dan menjawab pertanyaan yang mendorong pengumpulan dan pemeriksaan.

d. Reporting
Tahap pelaporan yakni melaporkan hasil analisis yang mencakup deskripsi tindakan yang diambil, penjelasan tentang alat dan prosedur yang dipilih, penentuan tindakan lain yang perlu dilakukan (misalnya pemeriksaan forensik dari sumber data tambahan, pengamanan yang teridentifikasi kesenjangan, atau peningkatan kontrol keamanan), dan memberikan rekomendasi untuk memperbaiki kebijakan, prosedur, peralatan, dan aspek lain dari proses forensik.

2.2. Alat dan Bahan

Dalam penelitian ini diperlukan alat dan bahan untuk mendukung proses investigasi forensik, yaitu sebagai berikut:

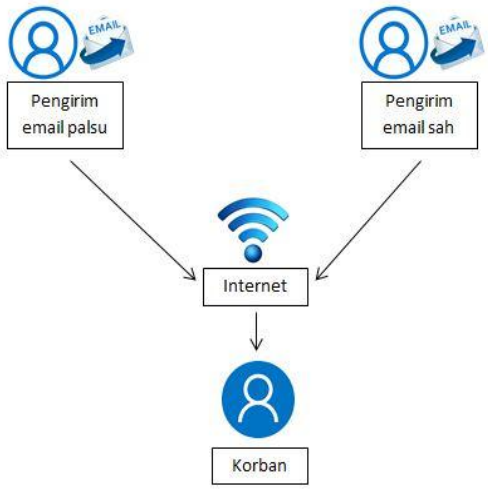
a. Perangkat keras
   1) 1 buah laptop Lenovo ideapad 300S

ISBN 978-602-99334-9-9

b. Perangkat lunak
   1) Sistem operasi Windows 10 64 bit
   2) Software Aid4Mail Forensic

2.3. Rancangan Sistem

Sebuah skenario dirancang untuk mendapatkan bukti digital untuk kemudian dianalisis. Pada penelitian ini skenario yang dibuat berupa pengiriman email yang palsu dan yang sah. Skenario digambarkan pada gambar 2.



Gambar 2. Rancangan Skenario Sistem

Pada skenario ini dilakukan pengiriman email dari dua akun berbeda, dimana salah satu akun mengirim email yang benar dan sah, sedangkan akun yang satu lagi mengirimkan email palsu kepada korban, baik isi email tersebut merugikan maupun tidak.

3. HASIL DAN PEMBAHASAN

Untuk melakukan analisis forensik email pada sistem komputer dibutuhkan sebuah metode dan tools yang akan membantu investigator untuk melakukan investigasi forensic. Penelitian ini dimulai dengan pemilihan tools untuk membuat sebuah email palsu, yang kemudian dikirimkan kepada korban sesuai dengan skenario. Tools yang digunakan dalam pembuatan email palsu hendaknya mempunyai akses bebas dan mudah digunakan. Sedangkan untuk metode yang digunakan pada saat tahapan analisis email palsu tersebut adalah Header analysis, dimana pada setiap bagian header email memuat *field-field seperti From, To, Subject, Date, Received*, dan yang lainnya.

Selanjutnya pada saat skenario pembuatan email palsu, dilakukan dengan memanipulasi field pada header email dan juga pesan yang meyakinkan bahwa email tersebut benar-benar email yang sah dan asli. Pada saat yang sama juga dikirimkan email yang sah dan asli dari akun yang benar. Kemudian email-email yang dikirim tersebut akan masuk ke *inbox email* korban, maka dari itu perlu dilakukan pengecekan email dengan cara masuk ke akun email korban. Selanjutnya email tersebut akan di analisis untuk mendapatkan data yang dapat menjadi barang bukti yang valid.

Pada tahapan terakhir dilakukan reporting atau pelaporan hasil analisis yang berupa barang bukti yang valid konten dari email palsu tersebut, dalam pelaporan juga dijelaskan proses atau tahapan yang digunakan dalam mendapatkan barang bukti yang dibutuhkan.

4. KESIMPULAN

Penelitian yang menggunakan *National Institute of Standards and Technology* (NIST) dengan pendekatan *Header Analysis* menghasilakan pola pemalsuan email yang berupa subjek, alamat dan tanggal email yang palsu. Selain itu investigasi email forensik ini juga menghasilkan: 1) Alamat

email pengirim email palsu; 2) memeriksa protokol inisiasi pesan (HTTP, SMTP); 3) memeriksa ID pesan; 4) alamat IP pengirim. Aspek lain yang dapat mengontrol analisis forensik meliputi format penyimpanan alamat email, ketersiadaan cadangan email ketika email tersebut dipindah dan protokol yang digunakan dalam menganalisis email.

DAFTAR PUSTAKA

Agrawal, A., Gupta, M., dan Gupta, S.C., (2012), Systematic Digital Forensic Investigasi Model, *International Journal of Computer Science and Security (IJCSS)* Vol.5 No.1 Hal.118-131.

Alharbi, S., Jahnke, J.W., dan Traore, I., (2011), The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review, *International Journal of Security and Its Aplications (IJCSIA)*, Vol.5 No.4 Hal.59-72.

Budiman, R., (2001), Komputer Forensik: Apa dan Bagaimana?, *Jurnal Fakultas Teknik Elektro dan Informatika*, Institut Teknologi Bandung, Jawa Barat.

Fadlil, A., Riadi, I., dan Aji, S., (2017), Pengembangan Sistem Pengamanan Jaringan Komputer Berdasarkan Analisis Forensik Jaringan, *Jurnal Ilmu Teknik Elektro Komputer dan Informatika (JITEKI)Vol.3, No.1 hal.11-19.*

Hoiriyah, Sugiantoro, B., dan Prayudi, Y., (2016), Investigasi Forensik pada email Spoofing menggukan Metode Header Analysis, *Jurnal Ilmiah Dasi*, Vol. 17 No 4 Hal 20-25.

Jansen, W., Delaitre, A., dan Moener, L., (2008), Overcoming Impediments to Call Phone Forensics, *Procidings of the 41st Annual Hawaii International Conference on System Sciences, pp 483.*

Kakunsi, O., (2012), Penipuan Penawaran Pekerjaan Melalui E-Mail, *Lex Crimen, Vol.1, No.2.*

Karsono, K., (2012), Forensik E-mail, *Forum ilmiah Vol. 9 Hal 58-75.*

Kurniawan, H., (2005), *Panduan Praktis Instalasi Email Server Gratis Berbasis Windows Menggunakan Mail Server*, Jakarta: PT. Elek Media Komputindo.

Rafiudin, R. (2009), *Investigasi Sumber-sumber Kejahatan Internet: Internet Forensics*, (N. WK, Ed.), Andi. doi: 10987654321.

Riadi, I., Eko, J., Ashari, A., dan Sunardi, (2013), Internet Forensics Framework Based-on Clustering *International Journal of Advanced Computer Science and Applications, Vol.4 No.12 Hal.115-123.*

Ojha, G., dan Tak, G.K., (2012), Novel Approach Againts Email Attacts Derived from User Awarenes Based Techniques, *International Journal of Information Technology Convergence and servives, Vol.2 No.4.*

Umar, R., Yudhana, A., dan Faiz, M.N., (2016), Analisis Kenerja Metode Live Forensics untuk Investigasi Random Access Memory pada Sistem Proprietary, dalam *Prosiding Konferensi Nasional Ke-4 Asosiasi Program Pascasarjana Perguruan Tinggi Muhammadiyah (APPPTM), pp. 207-211.*

Utdirartatmo, F., (2001), Tinjauan Analisis Forensik dan Kontribusinya Pada Keamanan Sistem Komputer, *Junal Fakultas Teknik Elektro dan Informatika*, Institut Teknologi Bandung, Jawa Barat.

Wijaya, H., Riadi, I., dan Sunardi, (2017), Analisis Forensik Digital Aplikasi Telegram pada Smartphone Berbasis Android, *Seminar Nasional Teknologi Informasi dan Komunikasi (SEMANTIKOM) Hal 93-95.*

ISBN 978-602-99334-9-9