Jurnal Informatika: Jurnal Pengembangan IT (JPIT), Vol.04, No.02, Mei 2019 ISSN: 2477-5126
DOI: 10.30591/jpit.v4i2.1134, pp:120-122 e-ISSN: 2548-9356

Review Article : Investigasi Forensik Email dengan Berbagai Pendekatan dan *Tools*

Imam Riadi[1], Rusydi Umar[2] Mustafa[3]
[1, 3] Program Studi Magister Teknik Informatika, Universitas Ahmad Dahlan
[2]Program Studi Sistem Informasi, Universitas Ahmad Dahlan
[1,2,3]Jl. Prof. Dr. Soepomo,S.H, Warungboto, Yogyakarta 55164
[1]imam.riadi@is.uad.ac.id, [2]rusydi.umar@rockermail.com, [3]mustafa.ramliannor@gmail.com

Abstract **- Computer forensic science is a relatively new science and not even widely known among the public. Unlike the real world, crime in the world of computers and the internet has so many variations, one of which is forgery or spam email, where spam e-mail can be a means of transporting malicious content on a network. The problem that arises at this time is that very little research is conducted in the case of forensic investigations in the face of crime in the cyber world, especially in the spam e-mail. The method used is observation of literature, in this case in the form of original articles that analyze about crimes that use email, including the flow and tools used. The results obtained in this article review are that each investigation and tools approach has advantages and disadvantages of each, so that users can adjust to their needs.**

Abstrak **– Komputer forensik atau yang dikenal dengan istilah digital forensik adalah salah satu cabang ilmu forensik yang berkaitan dengan bukti legal yang dapat ditemukan pada media penyimpanan digital. Cabang ilmu ini digunakan untuk menjabarkan fakta yang akan menjadi bukti dalam proses hukum. Berbeda dengan di dunia nyata, kejahatan di dunia komputer dan internet memiliki variasi yang begitu banyak, salah satunya adalah pemalsuan atau biasa disebut *email spam*, dimana *email spam* tersebut dapat menjadi alat transportasi informasi yang berbahaya dalam sebuah jaringan. Permasalahan yang kemudian muncul pada saat ini adalah proses yang digunakan dalam setiap tahapan digital forensik sangat bermacam-macam dan memiliki kelebihan dan kekurangan yang berbeda-beda. Maka dari itu diperlukan observasi literatur yang dalam hal ini berupa original artikel yang menganalisis tentang kejahatan yang menggunakan *email*, termasuk alur dan *tools* yang digunakan. Hasil yang didapatkan pada review artikel ini adalah setiap pendekatan investigasi dan tools memiliki kelebihan dan kekurangan masing-masing, sehingga pengguna dapat menyesuaikan dengan kebutuhan.**

Kata Kunci: email forensic, cybercrime, komputer forensik, forensi tools

I. PENDAHULUAN

Komputer forensik atau yang juga sering dikenal dengan istilah digital forensik merupakan salah satu cabang ilmu forensik yang berkaitan dengan pengumpulan bukti-bukti legal yang dapat ditemukan pada komputer dan media penyimpanan lainnya [1]. Forensik merupakan sebuah proses ilmiah dalam mengumpulkan, menganalisis, dan menampilkan berbagai bukti pada sidang pengadilan karena adanya suatu kasus hukum. Hal ini berbeda dengan pengertian forensik pada umumnya, komputer forensik dapat diartikan sebagai proses pengumpulan dan analisis data dari berbagai sumber daya komputer yang mencakup sistem komputer, baik itu jaringan, jalur komunikasi, dan berbagai media penyimpanan yang diajukan dalam sidang pengadilan [2].

Forensik merupakan kegiatan investigasi dan menetapkan fakta yang berhubungan dengan permasalahan kriminal atau hukum. Forensik digital merupakan bagian dari ilmu forensik yang melingkupi penemuan dan investigasi data yang ditemukan dalam perangkat digital [3]. Penggunaan metode forensik yang sesuai merupakan faktor yang sangat penting untuk mendukung proses investigasi tindak kejahatan yang lebih efektif dan efisien dalam menangani sebuah kasus cyber crime [4]. Bagian penting dalam digital forensik yaitu keaslian dari barang bukti digital [6]. Melakukan investigasi melalui tahapan pendekatan prosedur pemeriksaan digital forensik digital adalah cara valid untuk mendapatkan pembuktian. Temuan barang bukti digital yang didapat oleh investigator langsung mengarah untuk kepentingan rekontruksi kasus yang dihadapi [7]. Salah satu cabang dari forensik komputer adalah email forensik, dimana email atau electronic mail merupakan salah satu layanan internet yang sering digunakan dalam masyarakat berupa surat elektronik berbasis teks, tetapi dengan adanya perkembangan teknologi, email tidak hanya dapat mengirim *file* dalam bentuk teks, melainkan juga audio, foto, video dan file ekstensi lainnya[8]. Hal ini menyebabkan terdapatnya ancaman serius yang mengikuti kemudahan yang diberikan oleh email dengan memanfaatkan fitur tersebut sebagai media kejahatan di dunia cyber, karena email merupakan alat transportasi utama bagi spam dan konten berbahaya lainnya yang ada pada jaringan. 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 [9].

Salah satu kejahatan yang sering ditemukan yang melibatkan email adalah *Email Spamming* dan *Email Spoofing* [10]. Email Spoofing adalah email yang dikirimkan dengan sengaja di palsukan supaya terlihat seolah-olah

*) **penulis korespondensi**: Mustafa
Email: mustafa.ramliannor@gmail.com

dikirim dari *email* yang sah, sedangkan *Email Spamming* merupakan *spam* atau junk mail yang mengacu kepada pengiriman email ke sembarang orang untuk tujuan yang tidak diperlukan bahkan untuk tujuan yang jahat [11]. Maka dari itu sangat penting halnya untuk mengetahui cara mengatasi kejahatan dalam bidang email tersebut

II. PENELITIAN YANG TERKAIT

Hoiriyah dkk, melakukan penelitian tentang pendeteksian *email Spoofing* dengan pendekatan investigasi *Header Analysis*, dimana dari hasil penelitiannya tersebut didapatkan tiga pola *Spoofing*[12], yaitu: (1) *Email spoofing* yang memalsukan tanggal dan alamat email; (2) *Email spoofing* yang memalsukan tanggal pengirimannya saja; (2) Email spoofing yang memalsukan alamat pengirimnya saja. Kemudian dari hasil analisis, deteksi adanya *email spoofing* dapat dilihat dengan menggunakan metode *Header Analysis* dengan menggunakan *field-field* yang memuat informasi yang dibutuhkan seperti *Form*, *Message-ID*, *Receive* dan *Date*.

Devendran dkk, melakukan studi yang membandingkan 5 (lima) tools berdasarkan sembilan kriteria, yaitu: memasukkan file kedalam disk, opsi pencarian, informasi yang disediakan, kemampuan pemulihan, format yang didukung, format visualisasi yang didukung, sistem operasi yang didukung, format ekspor, dan dukungan perangkat lainnya[13]. Hasil analisis menunjukkan bahwa *Add4Mail* dapat menganalisis email yang ada pada hard disk maupun pada server jarak jauh dan dapat mengumpulkan informasi paling banyak dibandingkan tools yang lain. Sedangkan tools Paraben Examiner dapat mnyediakan informasi tidak hanya header email, teapi juga isi dan lampiran yang ada pada email, selain itu *tools* ini juga memiliki pemulihan email yang paling bagus diantara yang lainnya karena dapat memulihkan email yang sudah dihapus.

Penelitian lainnya adalah yang dilakukan oleh Gurpal Singh Chhabra, dkk dengan judul "*Review of E-mail System, Security Protocols and Email Forensics*" dimana pada jurnal ini dijelaskan tentang arsitektur dan cara kerja email, teknik-teknik investigasi email forensik, dan *tools* yang digunakan dalam email forensik. Selain itu dalam penelitian ini juga dijelaskan tentang masalah keamanan dan kerentanan yang terjadi dalam sistem email. *Tools* forensik yang dijelaskan dalam penelitian ini adalah *MailXaminer*, *Aid4Mail*, *Digital Forensic Framework* (DFF), *Email TrackerPro*, Paraben EMX, dan *Email Tracer*[14].

Penelitian lainnya dilakukan oleh Swapnil Gupta, dkk dalam jurnalnya yang berjudul " *E-Mail Header A Forensic Key to Examine an E-Mail*". Dalam penelitian ini dijelaskan tentang bagian-bagian dari header email, mulai dari struktur, lokasi, protokol, formasi serta pemeriksaan forensiknya. Dalam pemeriksaan forensik dengan menggunakan header email, penelitian ini membagi menjadi 2 bagian *header*, yaitu "*Message Header*" dan "*Envelope Header*" untuk kemudian di analisis satu persatu[15].

Tariq Banday pada penelitiannya yang berjudul "*Techniques and Tools for Forensic Investigation of Email*" menjelaskan tentang tools dan teknik yang digunakan dalam melakukan penyelidikan email forensik. Teknik investigasi yang dijelaskan dalam penelitian ini meliputi *header analysis*, *bait tactics*, *server investigation*, *network device investigation*, *software embedded identifiers*, dan *sender mailer fingerprints*. Sedangkan untuk *tools* email forensik yang dibandingkan sebanyak sebelas *tools* yang sering digunakan dan memiliki format yang mudah untuk melakukan identifikasi email spam[16].

III. METODE PENELITIAN

Metode yang digunakan adalah observasi literatur, dalam hal ini berupa artikel ilmiah yang menganalisis tentang kejahatan yang menggunakan *email*, termasuk alur dan *tools* yang digunakan.

1) Kriteria Inklusi:

- Artikel penelitian terkait dengan kejahatan email dan metode analisisnya.
- Artikel penelitian berbahasa Inggris atau Indonesia.
- Artikel penelitian yang memuat simulasi kasus kejahatan email.
- Artikel penelitian yang menggunakan *tools* yang dapat diakses gratis.

2) Kriteria Eksklusi:

- Artikel penelitian yang hanya memuat materi kejahatan internet, tidak spesifik pada kejahatan email.
- Artikel penelitian yang tidak dapat diakses gratis fulltext.

IV. HASIL DAN PEMBAHASAN

A. Teknik Investigasi Email Forensik

Dibawah ini merupakan beberapa teknik pendekatan dalam investigasi email forensik:

- *Bait Tactics*
- *Header Analysis*
- *Server Investigation*
- *Software Embedded Identifiers*
- *Sender Mail Fingerprints*
- *Network Device Investigation*

B. Tools Email Forensik

Dari banyak *tools* yang dapat digunakan dalam investigasi kejahatan dalam bidang email, beberapa tidak dapat di akses atau didownload secara gratis, jadi pengguna harus mengeluarkan biaya untuk dapat memiliki atau mengakses tools tersebut, dibawah ini dijelaskan beberapa tools yang dapat diakses tanpa bayar:

1) Email Tracker Pro

Cara kerja dari *tools* ini adalah dengan menganalisis header email untuk mendeteksi alamat IP pengirim pesan sehingga dapat dilacak. Tools ini juga dapat melacak beberapa email dalam waktu yang bersamaan dan juga dapat memprediksi kota yang kemungkinan besar berasal dari pengirim email. Fitur utama dari tools ini adalah pembuatan laporan yang langsung dikirim ke ISP pengirim sehingga dapat menuntut pengirim pesan.

2) Aid4Mail Forensic

Pada *tools* ini, pencarian email dapat dilakukan pada format pdf yang di ekspor ke tools. *Tools* ini dapat mem-filter

email berdasarkan teks, waktu, tanggal, kata kunci, operator logika, dan ekspresi reguler, konten header dan isi pesan. Selain itu, kemampuan dari tools ini adalah dapat memfilter email yang sudah digandakan dan dapat memulihkan kembali *email yang sudah dihapus.*

3) Adcomplain

Tools ini dapat digunakan untuk melaporkan email dan postingan yang tidak pantas atau email spam yang biasanya digunakan dalam penipuan atau "cara menghasilkan uang dengan cepat". *Tools* ini secara otomatis akan menganalisis pesan, menyusun laporan penyalahgunaan dan mengirimkan laporan ke penyedia layanan internet dengan menggunakan heade analysis yang valid.

4) Email Tracer

Tools ini bekerja dengan menelusuri alamat IP pengirim dan detail lainnya dari *header* sebuah email, kemudian menghasilkan laporan HTML secara terperinci mengenai analisis header tersebut. Hasil laporan berupa detail kota dari pengirim serta letak lokasi geografis dari asal email. Selain itu, *tools* ini memiliki fasilitas pencarian kata kunci pada konten email termasuk lampiran dan klasifikasinya.

5) Digital Forensic Framework

Tools ini dapat menganalisis email yang tersimpan di dalam hard disk. Pencarian dapat dilakukan berdasarkan konten atau isi email, tag, dan waktu. Selain itu, tools ini dapat menunjukkan rincian tanggal dan waktu kapan email tersebut dikirim.

V. KESIMPULAN

Kejahatan yang terjadi melalui email, seperti pengancaman, penipuan dan pencurian informasi rahasia semakin hari semakin bertambah. Siapapun dan melakukan hal tersebut, termasuk dalam hal ini adalah setelah pengiriman, pelaku akan menghapus barang bukti yang berupa email tersebut. Maka dari itu perlu adanya forensik email untuk menganalisis email-email yang berbaya tersebut. Analisis email dapat menggunakan beberapa pendekatan seperti *Header Analysis Email Structure*, *IP Tracing*, *Bait Tactics*, *Email Header Tracing*, *Investigasi Server* maupun yang lainnya. Sedangkan untuk Tools yang digunakan pun bermacam-macam dan memiliki kelebihan dan kekurangan masing-masing, sehingga pengguna dapat memilih *Tools* sesuai dengan keinginan dan kebutuhan.

DAFTAR PUSTAKA

[1] F.Utdirartatmo,"Tinjauan Analisis Forensik dan Kontribusinya Pada Keamanan Sistem Komputer", *Junal Fakultas Teknik Elektro dan Informatika*, Institut Teknologi Bandung, Jawa Barat, 2001.
[2] K. Karsono, "Forensik E-mail", *Forum ilmiah Vol. 9 Hal 58-75*, 2012.
[3] B. Rahardjo, "Sekilas Mengenai Forensik Digital", *Jurnal Sosioteknologi*, FSRD-ITB Ed.29 Hal.384-387, 2013.
[4] R. Umar, A. Yudhana, dan M.N. Faiz, "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, pp. 207-211*, 2016.
[5] I. Riadi, J. Eko, A. Ashari, dan Sunardi, "Internet Forensics Framework Based-on Clustering", *International Journal of Advanced Computer Science and Applications, Vol.4 No.12 Hal.115-123*, 2013.
[6] R. Budiman, "Komputer Forensik: Apa dan Bagaimana?", *Jurnal Fakultas Teknik Elektro dan Informatika*, Institut Teknologi Bandung, Jawa Barat, 2001.
[7] Y. Prayudi, "Problema dan Solusi Digital Chain of Custody dalam Proses Investigasi", *SENASTI*, 2014.
[8] H. Kurniawan, "*Panduan Praktis Instalasi Email Server Gratis Berbasis Windows Menggunakan Mail Server"*, Jakarta: PT. Elek Media Komputindo, 2005.
[9] A. Fadlil, I. Riadi dan S. Aji, "Pengembangan Sistem Pengamanan Jaringan Komputer Berdasarkan Analisis Forensik Jaringan", *Jurnal Ilmu Teknik Elektro Komputer dan Informatika (JITEKI)Vol.3, No.1 hal.11-19*, 2017.
[10] K. Karsono, "Forensik E-Mail", *E-journal Esa Unggul*, 2012.
[11] G. Ojha dan G.K. Tak, "Novel Approach Againts Email Attacts Derived from User Awarenes Based Techniques", *International Journal of Information Technology Convergence and servives, Vol.2 No.4*, 2012.
[12] Hoiriyah, B. Sugiantoro, Y. Prayudi, "Investigasi Forensik pada E-mail Spoofing menggunakan Metode Header Analysis", *Jurnal Ilmiah DASI* Vol.17 No.4 hlm 20-25, 2012.
[13] V.K. Devendran, H. Shahriar, dan V. Clincy, "A Comparative Study of Email Forensic Tools", *Journal of Information Security* Vol., 111-117, 2015.
[14] G.S. Chhabra, and D.S. Bajwa, "Review of Email System, Security Protocols and Email Forensic", *International Journal of Computer Science & Communication Network* Vol.5(3), 201-211, 2016.
[15] S. Gupta, K. Gupta and A. Singla, "Email Header-A Forensic Key to Examine an Email", *International Research Journal of Engineering and Technology* Vol.3 (2), 2016.
[16] M.T. Banday, "Techniques and Tools for Forensic Investigation of Email", *International Journal of Network Security & Its Applications*, Vol.3 No.6, 2011.