ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman 36295-36303
Volume 8 Nomor 2 Tahun 2024

# Analisis Forensik *Email* Menggunakan Metode *Digital Forensics Research Workshop* pada Studi Kasus *Email* Palsu

**La Ode Muhammad Saidi[1], Wa Ode Miranda[2]**
[1,2] Rekayasa Sistem Komputer, Universitas Muhammadiyah Buton
email: saidilm8@gmail.com

**Abstrak**

Surat elektronik biasa juga disebut *electronic mail* (*email*) adalah kegiatan mengirim dan menerima pesan yang disampaikan secara elektronik melalui jaringan komputer. email juga merupakan salah satu identitas seseorang atau organisasi yang dapat dipercaya untuk mengirimkan pesan kepada penerima pesan. Hal ini tentunya dapat menjadi salah satu cara untuk melakukan kejahatan digital, misalnya dengan menggunakan *email* milik orang lain atau organisasi lain kemudian mengirimkan pesan kepada seseorang dengan tujuan pencemaran nama baik, memberikan ancaman, mengirimkan pesan yang bersifat pornografi, mengirimkan pesan yang berisi malware dengan tujuan mencuri data, dan masih banyak lagi. Untuk mengetahui apakah alamat email tersebut asli atau palsu maka perlu dilakukan analisis forensik *email*. Penelitian ini menggunakan metode *Digital Forensics Research Workshop*.

**Kata kunci:** *Analisis Email Forensik, Digital Forensics Research Workshop, Studi Kasus, Email Palsu*

**Abstract**

Electronic mail, also known as electronic mail (email), is the activity of sending and receiving messages delivered electronically via a computer network. Email is also one of the identities of a person or organization that can be trusted to send messages to the recipient of the message. This can of course be one way to commit digital crime, for example by using an email belonging to another person or another organization then sending a message to someone with the aim of defaming them, giving threats, sending pornographic messages, sending messages containing malware with the aim of stealing data, and much more. To find out whether the email address is real or fake, it is necessary to carry out forensic analysis of the email. This research uses the Digital Forensics Research Workshop method.

**Keywords:** *Forensic Email Analysis, Digital Forensics Research Workshop, Case Study, Fake Email*

## PENDAHULUAN

Email palsu merupakan aktivitas pengiriman pesan menggunakan akun email yang tidak benar atau akun orang lain tanpa diketahui oleh pemilik sah dengan tujuan pencemaran nama baik, pemberian ancaman, pengiriman pesan pornografi, pengiriman pesan yang mengandung malware, pencurian data, dan masih banyak lagi. Analisis forensik email adalah langkah-langkah yang dilakukan untuk penyelidikan terhadap akun email atau pesan email dengan tujuan untuk memberikan bukti-bukti terhadap status dari akun maupun pesan email tersebut sehingga dapat dipertanggungjawabkan untuk pengambilan keputusan.

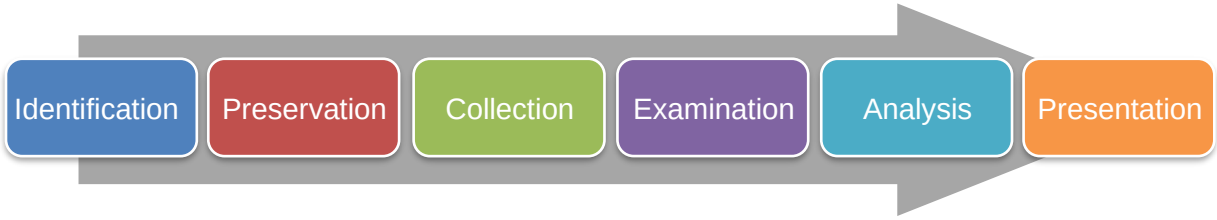
Penelitian tentang *email* palsu atau pesan palsu telah banyak dilakukan. Berikut ini beberapa penelitian yang telah dilakukan, penelitian yang dilakukan oleh Mishra, Pilli, & Joshi (2012) yang melakukan penelitian terhadap e-mail spoofing dengan membandingan waktu pengiriman e-mail (sending time) dan waktu penerimaan pesan (last server email receiving time). Sedangkan dipenelitian yang lainnya Banday juga menjelaskan, Analisis forensik dari pesan e-mail bertujuan untuk menemukan sejarah pesan dan identitas semua entitas yang terlibat. Selain analisis pesan, e-mail forensik juga melibatkan investigasi beberapa client atau server komputer

yang diduga digunakan atau disalahgunakan untuk pemalsuan e-mail, hal tersebut melibatkan pemeriksaan favorit Internet, Cookies, History, diketik URL, Temporary Internet Files, Auto penyelesaian Entries, Bookmarks, Kontak, Preferences, Cache, dll. Analisis email bertujuan untuk menemukan bukti dari sumber dan isi pesan *email*, identifikasi pengirim yang sebenarnya, penerima, tanggal dan waktu ketika pesan dikirim, dan lain-lain. Sedangkan analisis forensik dari pesan *email* bertujuan untuk menemukan sejarah pesan dan identitas semua entitas yang terlibat. Selain analisis pesan, forensik *email* juga melibatkan investigasi terhadap client atau server komputer yang diduga digunakan atau disalahgunakan untuk aktivitas pelanggaran *email*. (Banday, M. T.,2011).

Forensik *email* mengacu pada studi rincian *email* termasuk sumber dan isi email, untuk mengidentifikasi pengirim dan penerima pesan yang sebenarnya, tanggal/waktu transmisi, catatan rinci transaksi email serta maksud pengirimnya.) Literature Review of Email Forensics, Pranali P. Hatole & Dr. Shobha K. Bawiskar. Penelitian sebelumnya oleh Hoiriyah, melakukan investigasi forensik pada email spoofing menggunakan metode header analysis yang hanya mengacu pada header field seperti from, massege-ID, date, dan Received (last). Berdasarkan penelitian sebelumnya maka peneliti merasa perlu dilakukan pengembangan analisis forensik email, olehnya itu dilakukanlah sebuah penelitian baru dengan judul analisis forensik *email* metode *Digital Forensics Research Workshop* pada studi kasus email palsu.

## METODE

Metode yang digunakan dalam penelitian ini adalah *DFRWS* (*Digital Forensics Research Workshop*), *DFRWS* memiliki 6 tahap yaitu *identification*, *preservation*, *collection*, *examination*, *analysis*, *presentation*. Metode *DFRWS* bertujuan membantu mendapatkan bukti dan mekanisme terpusat untuk merekam informasi yang dikumpulkan (Anton Yudhana, Imam Riadi, Ikhsan Zuhriyanto).




**Gambar 1. Metode Penelitian *DFRWS (Digital Forensics Research Workshop)***

## HASIL DAN PEMBAHASAN

### Studi Kasus Email Palsu

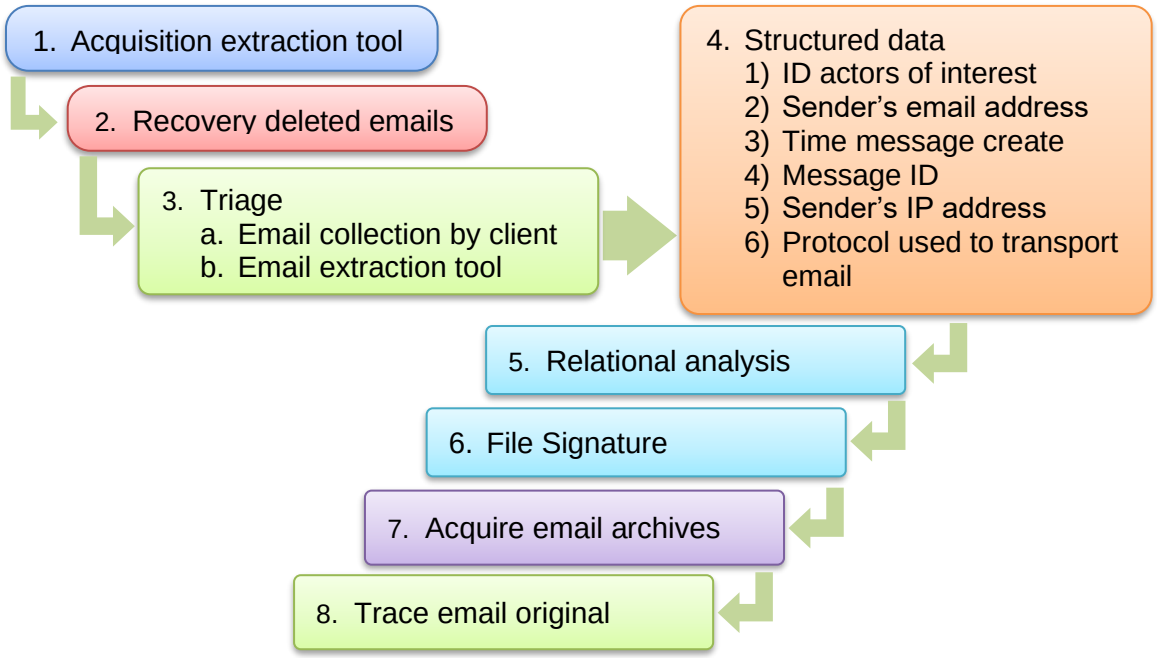
Berikut adalah ilustrasi dari simulasi kasus ujicoba yang akan dilakukan :


**Gambar 2. Ilustrasi simulasi kasus pengiriman emal palsu oleh pelaku kepada korban**

Pengiriman email palsu dilakukan oleh dua orang yang berbeda terhadap seorang target/korban. Penyerang pertama menggunakan alamat *email* inudin11@gmail.com dan penyerang kedua menggunakan alamat *email* budi@gmail.com.

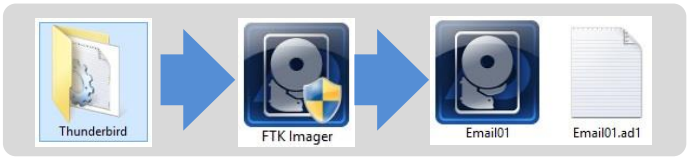
**Analisis Kasus**

1. *Identification*
   Tahap ini dilakukan identifikasi terhadap alamat *email* yang menjadi barang bukti, identifikasi bertujuan untuk menemukan data-data *email* dari pelaku, dengan menggunakan email client tools.
2. *Preservation*
   Tahap ini dilakukan proses akuisisi terhadap barang bukti yang telah diamankan dengan metode hashing menggunakan software *AccessData FTK Imager* dengan tujuan untuk mengamankan barang bukti agar tidak dirusak.
3. *Collection*
   Tahap memilah *email* berdasarkan *client email* yang selanjutnya akan dilakukan ekstrasi data – data email menggunakan *email extraction tools*. Software yang digunakan adalah *Mozilla Thunderbird*.
4. *Examination*
   Tahap selanjutnya melakukan pemeriksaan *email*, tahap ini bertujuan untuk mengetahui data–data yang terdapat dari pesan *email*. Selain itu, pemeriksaan juga dilakukan untuk menentukan pesan yang dikirim berasal dari akun *email* asli atau palsu.
5. *Analysis*
   Analisis *email* dilakukan menggunakan teknik data terstruktur. Teknik data terstruktur pada penelitian ini memiliki 8 tahap utama yaitu :



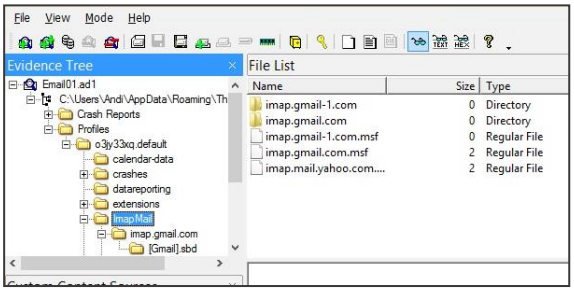

**Gambar 3. Analisis forensik email teknik data terstruktur**

6. *Presentation*
   Selanjutnya penyajian informasi yang dihasilkan dari tahap analisis. Adapun informasi yang dihasilkan adalah :
   a. Akuisisi dilakukan menggunakan *software AccessData FTK Imager*, dengan hasil sebagai berikut :




**Gambar 4. Ilustrasi akuisisi barang bukti**

b. *Recovery deleted emails*
Tujuan *recovery* adalah untuk menemukan dan mengembalikan data–data *email* yang terhapus dengan cara diekspor atau diekstrak kembali.




**Gambar 5. *Recovery data emails***

Pada gambar 5, dilakukan proses pencarian untuk menemukan data–data *email* yang diduga dihapus. Penghapusan data–data email bertujuan untuk menghilangkan bukti kejahatan pelaku. Pada penelitian yang dilakukan, proses *recovery* menggunakan *software AD FTK Imager*.

c. *Triage*, tahap ini menghasilkan hasil penyimpanan data *email* berupa sebuah folder yang dibuat untuk mengoleksi dan memilah *email* berdasarkan *client*, dan dilakukan Proses ekstrasi *email* dengan tujuan untuk menampilkan data – data yang terdapat pada setiap *email*.

d. *Structured data*
Analisis dilakukan berdasarkan *structured data* atau *header* pada setiap pesan *email*.

*1) ID actors of interest*
Berdasarkan data *header* pada *email* dari studi kasus dapat dikatakan bahwa semua pesan tersebut merupakan pesan dari orang yang sah karena memiliki nilai yang sama, namun kesamaan dari nilai masing – masing *email* tidak dapat menjamin bahwa *email* tersebut bukan *email* palsu.

**Tabel 1. Data konten dari masing – masing *email***

| Subjek | Nama | From | Return-Path |
|---|---|---|---|
| Studi Kasus 1 | *inudin* | *inudin11@gmail.com* | *inudin11@gmail.com* |
| Studi Kasus 2 | *Budi* | *budi@gmail.com* | *budi@gmail.com* |

Berdasarkan tabel 1, dapat dijelaskan bahwa pada *email* tesebut terdapat 2 pesan dengan subjek Studi Kasus 1 memiliki identitas inudin dan Studi Kasus 2 memiliki identitas Budi.

2) Sender's email address
Tahap ini dilakukan pemeriksaan terhadap alamat *email* pengirim, jika dilihat dari *Return-Path* dan *From* pesan *email* dapat dikatakan bahwa semua alamat *email* pengirim merupakan dari alamat *email* yang sah, namun jika diteliti berdasarkan beberapa *header email,* maka akan terlihat beberapa perbedaan informasi dari masing – masing alamat *email*. Seperti yang dijelaskan pada tabel berikut :

**Tabel 2. Informasi alamat *email* pengirim**

| *From* | *Return-Path* | *Received from* | *Received-SPF* | *Autentication* | | | | *Received by* | *Status* |
|---|---|---|---|---|---|---|---|---|---|
| | | | | *dkim* | *spf* | *dmarc* | *header* | | |
| *inudin11@gmail.com* | *inudin11@gmail.c* | *mail05.parking.ru* | *softfail, transitioning, not* | *-* | *softfail, transitioning,* | *fail* | *gmail.com* | *mail05.parking.ru* | *spoofing* |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | *om* | | *designate* | | *not designate* | | | | |
| *budi@gmail.com* | *budi@gmail.com* | *emkei.cz* | *softfail, transitioning, not designate* | *-* | *softfail, transitioning, not designate* | *fail* | *gmail.com* | *emkei.cz* | *spoofing* |

Selanjutnya kita dapat memeriksa validasi dari masing – masing alamat *email* pengirim. Pada penelitian yang dilakukan, pengecekan validasi *email* menggunakan situs *https://centralops.net/co/EmailDossier.aspx* : Pengecekan validasi pada alamat
Hasil pemeriksaan tersebut dapat dilihat pada tabel berikut.

**Tabel 3. Pemeriksaan alamat *email***

| Alamat Email | Kode Pemeriksaan | Informasi Pemeriksaan | Status |
|---|---|---|---|
| *inudin11@gmail.com* | *250* | *ok* | *spoofing* |
| *budi@gmail.com* | *550* | *does not exist* | *spoofing* |

Berikut adalah beberapa kode respon server SMTP dari pemeriksaan *email* berdasarkan penelitian studi kasus yang dilakukan :

a) Server siap, kode 220 merupakan pesan selamat datang yang berarti server *email dossier* dapat bekerja dengan baik
b) Sukses, kode 250 merupakan pesan bahwa server berhasil mengirimkan pesan.
c) Gagal, kode 550 merupakan pesan bahwa server gagal memeriksa alamat email dengan kata lain bahwa alamat email tersebut tidak ada.
d) Kesalahan, kode 500, 501, 502, 504, atau 421 merupakan pesan bahwa terdapat kesalahan pada alamat email diantaranya kesalahan penulisan sintaks (500), *email* tidak valid (510), *email* belum diaktifkan (502), kesalahan penulisan sintaks (504), dan server *email* tidak tersediah (421).
e) Ukuran berlebih, kode 552 merupakan pesan bahwa ukuran pesan terlalu besar
f) Alamat *email* salah, kode 553 merupakan pesan bahwa terdapat alamat *email* yang salah dalam melakukan transaksi *email*.
g) *Email spam*, kode 554 merupakan pesan bahwa transaksi telah gagal, hal tersebut dikarenakan server berpikir bahwa *email* tersebut adalah *spam* atau alamat *IP* dari *email* tersebut telah masuk dalam daftar hitam.

3) *Time message create*
tahap ini dilakukan untuk menganalisis waktu pembuatan pesan, diketahui bahwa pesan *email* dikirim dengan menggunakan satu waktu saja berdasarkan waktu kapan *email* tersebut dikirim. Namun pada waktu tersebut tidak terdapat informasi waktu dari provider *email* sah, misalnya *received by mail.yahoo.com*. Jadi dapat dipastikan pesan email tersebut adalah palsu atau tidak sah. Salah satu ciri dari *email* palsu atau *spoofing* adalah tidak terdapat waktu *Received* dan koordinat *Time Zone* yang digunakan adalah tidak sesuai dengan lokasi pengiriman email.

4) *Message ID*
Diketahui message ID dari email *inudin11@gmail.com* adalah *26813B639E6E442B995024C13A285EA2@corp.parking.ru*, dengan menggunakan *provider email* adalah *@corp.parking.ru*.
Jika dilihat berdasarkan ID pesan dapat dikatakan masing – masing *email* memiliki ID pesan yang berbeda – beda hal tersebut tidak dapat dipastikan bahwa pesan email tersebut adalah berasal dari email yang sah. Namun jika diteliti berdasarkan *email provider* maka akan ditemukan kesalahan *provider* yang digunakan oleh pengirim

email, misalnya alamat email yang digunakan adalah *inudin11@gmail.com* seharusnya memiliki *email provider* adalah *mail.gmail.com* namun dalam studi kasus *email provider* yang dimiliki adalah *corp.parking.ru*, hal tersebut juga terjadi pada alamat email *budi@gmail.com* yang memiliki *email provider* berbeda yaitu *emkei.cz*. Diketahui *corp.parking.ru* dan *emkei.cz* merupakan sebuah situs yang memberikan layanan untuk mengirim pesan email *spoofing*.

5) *Sender's IP address*
Merupakan tahap memeriksa alamat *IP* dari pengirim pada studi kasus 1 *email spoofing*, untuk mengetahuinya kita dapat melihatnya dari *Received-SPF: client-ip*. Diketahui alamat *client IP* adalah *195.128.120.25*, alamat tersebut merupakan alamat *IPV4*. Berdasarkan studi kasus yang dilakukan, diketahui bahwa alamat email yang digunakan oleh *inudin11@gmail.com* yaitu menggunakan *gmail* atau *google*. Selanjutnya kita dapat memeriksa keaslian dari *IP client* tersebut. Dalam penelitian ini pemeriksaan keaslian *IP client* menggunakan situs situs *https://who.is/whois-ip/ip-address*.

**Tabel 4. alamat *client IP email* pengirim**

| Alamat email | Alamat IP | *Organization* | Email Domain | Status |
|---|---|---|---|---|
| *inudin11@gmail.com* | *195.128.120.25* | *RIPE Network Coordination Centre (RIPE)* | *@parking.ru* | *Spoofing* |
| *budi@gmail.com* | *46.167.245.116* | *RIPE Network Coordination Centre (RIPE)* | *@finaltek.com* | *Spoofing* |

Tabel 7, menjelaskan bahwa pada *client IP email spoofing* yang memiliki alamat *inudin11@gmail.com* dan *budi@gmail.com* masih menggunakan alamat IPV4 dengan menggunakan *organization RIPE Network Coordination Centre*. Jadi, berdasarkan hasil penelitian dapat disimpulkan bahwa penggunaan domain email *@gmail.com* dengan alamat *client IP email* menggunakan IPV4 merupakan alamat *IP* dari *email spoofing.*

6) *Protocol used to transport email*
Menjelaskan bahwa alamat email *budi@gmail.com* menggunakan protokol SMTP, hal tersebut dapat dibuktikan dari informasi *Received* dan *Authentication spf*.

**Tabel 5. protokol yang digunakan pengirim**

| Alamat Email | Protokol | Status |
|---|---|---|
| *inudin11@gmail.com* | *SMTP* | *spoofing* |
| *budi@gmail.com* | *SMTP* | *spoofing* |

Tabel 5, menjelaskan bahwa semua *email* baik *email* sah maupun *email spoofing* menggunakan protokol yang sama yaitu *SMTP*. *SMTP* (*Simple Mail Transfer Protocol*) adalah protokol standar untuk mengirim *email* di Internet. Secara *default*, protokol *SMTP* bekerja pada empat *port*:

a) *Port 25* adalah port default SMTP yang tidak dienkripsi.
b) Port 465 adalah port yang memiliki keamanan atau disebut juga *Secure* SMTP/SMTPS/SSMTP.
c) *Port 2525* adalah port SMTP dengan enkripsi TLS
d) *Port 587* adalah port SMTP dengan enkripsi TLS.

e. *Relational analysis*
Tahap ini dilakukan proses pemeriksaan informasi kontak lain yang berhubungan dengan *email* pelaku. Pada tahap tersebut dapat diketahui kepada siapa saja pelaku melakukan pengiriman pesan email. Hal tersebut bisa menjadi petunjuk untuk pengembangan kasus.

f. *File Signature*
Pemeriksaan *file signature* bertujuan untuk mengetahui informasi apa saja yang berhubungan dengan pelaku misalnya informasi tempat kerja, alamat kantor, nomor telepon, alamat website dan lain – lain.
Berdasarkan penelitian yang dilakukan bahwa pada alamat email *legitimate* dapat dilakukan pengaturan file signature sedangkan pada alamat email spoofing tidak dapat dilakukan pengaturan.

**Tabel 6. keterangan file signature**

| Alamat email | Status | Keterangan |
|---|---|---|
| *inudin11@gmail.com* | *spoofing* | Tidak Dapat dilakukan pengaturan file signature |
| *budi@gmail.com* | *spoofing* | Tidak Dapat dilakukan pengaturan *file signature* |

Tabel 6, menjelaskan bahwa *file signature* pada email palsu tidak dapat dilakukan pengaturan.

g. *Acquire email archives*
Tahap ini dilakukan pemeriksaan terhadap arsip *email* dari pengirim. Pemeriksaan bertujuan untuk menemukan pesan – pesan yang berada pada kotak arsip dari setiap email. Pada penelitian ini pemeriksaan arsip pesan dilakukan dengan menggunakan *software Parabean's Email Examiner* yang memungkinkan untuk menemukan arsip email dari pelaku yang masih tersimpan.
Berdasarkan hasil pemeriksaan penelitian yang dilakukan bahwa tidak ditemukan file arsip yang menjadi inti dari pemeriksaan pada tahap ini. Pemeriksaan file arsip memungkinkan investigator menemukan pesan – pesan email yang berkaitan atau memiliki hubungan dengan pesan dari masing – masing pengirim email, hal tersebut dapat digunakan sebagai kelengkapan penyelidikan.

h. *Trace email original*
Tujuan dari tahap ini adalah untuk menelusuri dan menemukan jejak atau keaslian *email* dari masing – masing pengirim. Pada penelitian yang dilakukan, pemeriksaan pada tahap ini menggunakan situs *http://www.traceemail.com/trace-email-address.html* dengan memasukan data dari *header email* agar dapat menemukan jejak pelaku.
Adapun hasil dari trace email dapat dilihat pada tabel berikut :

**Tabel 7. hasil trace email**

| Information | Pengirim Ke 3 | Pengirim Ke 4 |
|---|---|---|
| *Email Address* | *inudin11@gmail.com* | *budi@gmail.com* |
| *IP Address* | *195.128.120.25* | *46.167.245.116* |
| *Hostname* | *Mail05.parking.ru* | *Emkei.cz* |
| *Country* | *Russian Federation (RU)* | *Czech Republic (CZ)* |
| *State* | *Moskva* | *Stredocesky Kraj* |
| *City* | *Moscow* | *Mesice* |
| *Postcode* | *101990* | *250 64* |
| *ISP* | *parking.ru* | *UPC Ceska Republica* |
| *Organization* | *Grant-Partk-Intertet Ltd* | *Zdenek Klauda – FinalTek.com* |
| *Latitude* | *55.738600* | *50.196500 (50°11'53"N)* |
| *Longitude* | *37.606800* | *14.517000 (14°31'12"E)* |
| *Time* | *22:44:09 +0300* | *07:55 local time* |
| Status | *spoofing* | *spoofing* |

Berdasarkan penelitian yang dilakukan bahwa tidak semua email dapat menampilkan informasi yang lengkap.

**Hasil**

Penelitian ini menghasilkan pengembangan tahapan dalam analisis forensik *email*. Berikut ini perbandingan menggunakan parameter terhadap setiap tahapan pada penelitian sebelumnya dengan tahapan yang telah dikembangkan.

**Tabel 11. Perbedaan tahapan sebelumnya dengan yang dikembangkan**

| | Tahapan | *Tahapan* | | Keterangan |
|---|---|---|---|---|
| | | Lama | Baru | |
| 1 | Acquisition extraction tool | | √ | Tidak ada pada penelitian sebelumnya |
| 2 | Recovery deleted emails | | √ | Tidak ada pada penelitian sebelumnya |
| 3 | Triage | | √ | |
| | a *Email collection by client* | | √ | Tidak ada pada penelitian sebelumnya |
| | b *Email extraction tool* | | √ | |
| 4 | Structured data | √ | √ | |
| | a *ID actors of interest* | √ | √ | |
| | b *Examining sender's e-mail address,* | √ | √ | |
| | c *Examining time message create* | √ | √ | |
| | d *Examining message ID* | √ | √ | |
| | e *Examining sender's IP address* | | √ | Tidak ada pada penelitian sebelumnya |
| | f *Protocol used to transport email* | | √ | Tidak ada pada penelitian sebelumnya |
| 5 | Relational analysis | | √ | Tidak ada pada penelitian sebelumnya |
| 6 | *Signature data* | | √ | Tidak ada pada penelitian sebelumnya |
| 7 | *Acquire email archives* | | √ | Tidak ada pada penelitian sebelumnya |
| 8 | *Trace email original* | | √ | Tidak ada pada penelitian sebelumnya |

**SIMPULAN**

Adapun kesimpulan dari penelitian ini adalah adanya perbedaan tahapan analisis yang dilakukan dengan penelitian sebelumnya yang mana pada penelitian sebelumnya analisis dilakukan pada *header email* yang berfokus pada *from*, *Message ID*, *date*, dan *received* (*last*), sedangkan pada penelitian ini ada beberapa tahapan baru yaitu :

1. Acquisition extraction tool
2. *Recovery deleted emails*
3. *Triage*
   a. *Email collection by client*
   b. *Email extraction tool*
4. *Structured data*
   a. *ID actors of interest*
   b. *Sender's email address*
   c. *Time message create*
   d. *Message ID*
   e. *Sender's IP address*
   f. *Protocol used to transport email*
5. *Relational analysis*
6. *File Signature*
7. *Acquire email archives*
8. *Trace email original*

## DAFTAR PUSTAKA

Banday, M. T. (2011). Techniques and Tools for Forensic Investigation of E- Mail. *International Journal of Network Security & Its Applications (IJNSA)*, *3*(6), 227–241.

Banday, M. T. (2011). Technology Corner: Analysing E-mail Headers For Forensic Investigation. *Journal of Digital Forensics, Security and Law*, *6*(2), 49–64. Retrieved from http://ojs.jdfsl.org/index.php/jdfsl/article/view/34

Pranali P. Hatole & Dr. Shobha K. Bawiskar (2017). Literature Review of Email Forensics. *Imperial Journal of Interdisiplinary Research (IJIR) Vol-3*, *3*(1), 82–86. http://doi.org/10.7763/JACN.2015.V3.146

Hatole, P. P., & Bawiskar, S. K. (2017). Literature Review of Email Forensics. *Imperial Journal of Interdisciplinary Research (IJIR)*, *3*(4), 1436–1439. Retrieved from https://www.onlinejournal.in/IJIRV3I4/250.pdf

Jafari, F., & Satti, R. S. (2015). Comparative Analysis of Digital Forensic Models. *Journal of Advances in Computer Networks*, *3*(1), 82–86. http://doi.org/10.7763/JACN.2015.V3.146

Devendran, V. K., Shahriar, H., & Clincy, V. (2015). A Comparative Study of Email Forensic Tools. *Journal of Information Security*, *06*(02), 111–117. http://doi.org/10.4236/jis.2015.62012

Hoiriyah, Sugiantoro, B., & Prayudi, Y. (2016). Investigasi Forensik Pada Email Spoofing Menggunakan Metode Header Analysis. *Dasi, Amikom*, *17*(4), 20–25. http://ojs.amikom.ac.id/index.php/dasi/article/view/1553/1431

Nikolaos, K., & Andreas, A. (2016). Charalambous Elisavet Bratskas Romaios Karkas George Email forensic tools : A roadmap to email header analysis through a cybercrime use case. *Journal of Polish Safety and Reliability Association*, *7*(1), 21–28.

Sutisna, M. A., & Riadi, I. (2018). *ANALISISA FORENSIK PADA E-MAIL SPOOFING Abstraksi*. *4*(1), 38–43.

Suryana, A. L., Akbar, R. El, & Widiyasono, N. (2016). Investigasi Email Spoofing dengan Metode Digital Forensics Research Workshop (DFRWS). *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *2*(2), 111–117. https://doi.org/10.26418/jp.v2i2.16821