

**ANALISIS FORENSIK EMAIL MENGGUNAKAN
METODE *DIGITAL FORENSICS RESEARCH WORKSHOP*
PADA STUDI KASUS *EMAIL PALSU***

**La Ode Muhammad Saidi¹, Wa Ode Miranda²
Universitas Muhammadiyah Buton**

E-mail: saidilm8@gmail.com¹, waodemiranda97@gmail.com²

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*

1. 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 membandingkan 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).

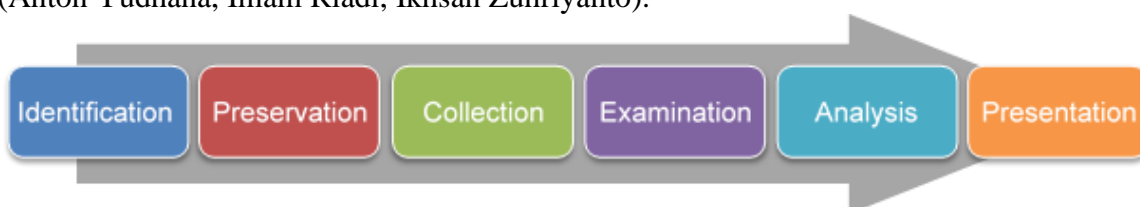
Forensik email mengacu pada studi rincian email termasuk sumber dan isi email, untuk mengidentifikasi pengirim dan penerima pesan yang sebenarnya, tanggal/waktu transmisi, catatan rinci transaksi email serta maksud pengirimnya.) *Literature Review of Email Forensics, Pranali P. Hatole & Dr. Shobha K. 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.

2. METODE PENELITIAN

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*)

3. HASIL DAN PEMBAHASAN

Studi Kasus Email Palsu

Berikut adalah ilustrasi dari simulasi kasus ujicoba yang akan dilakukan:



Gambar 2. Ilustrasi simulasi kasus pengiriman email 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

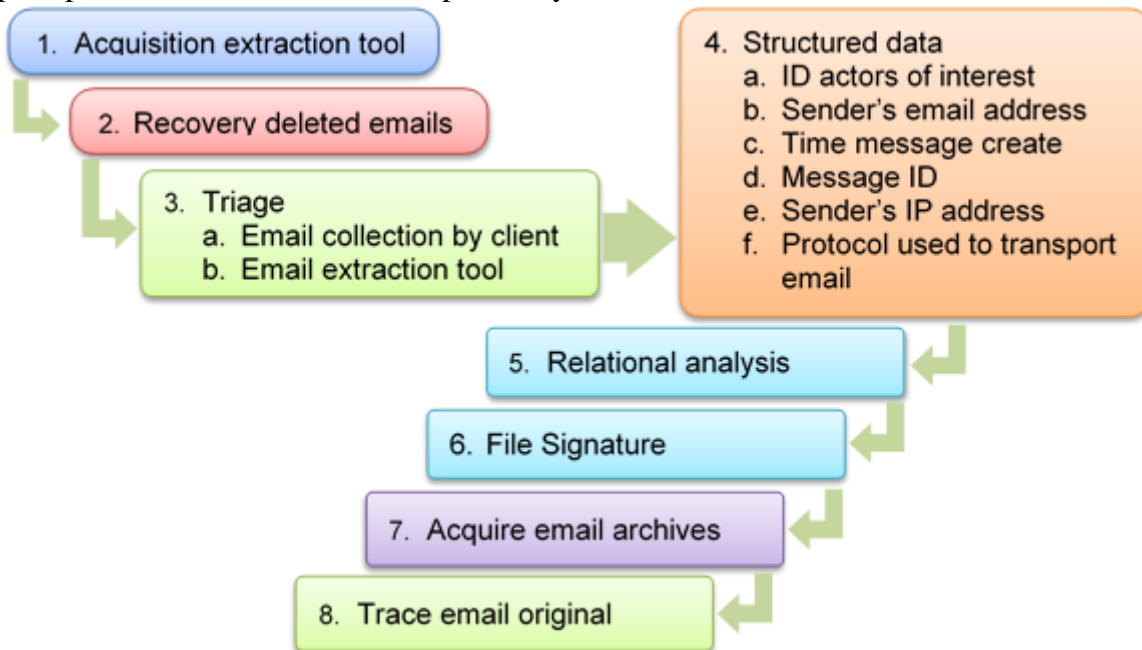
Tahap memilah email berdasarkan client email yang selanjutnya akan dilakukan ekstraksi data – data email menggunakan email extraction tools. Software yang digunakan adalah Mozilla Thunderbird.

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:

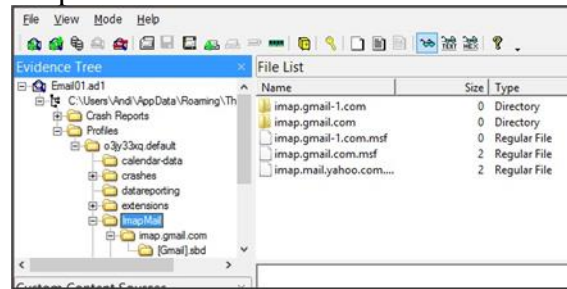
1. Akuisisi dilakukan menggunakan software AccessData FTK Imager, dengan hasil sebagai berikut:



Gambar 4. Ilustrasi akuisisi barang bukti

2. 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.

3. 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.
4. Structured data

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

a. 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	<i>inudin</i>	<i>inudin11@gmail.com</i>	<i>inudin11@gmail.com</i>
Studi Kasus 2	<i>Budi</i>	<i>budi@gmail.com</i>	<i>budi@gmail.com</i>

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

b. 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	Autentification				Received by	Status
				dkim	spf	dmarc	header		
<i>inudin11@gmail.com</i>	<i>inudin11@gmail.com</i>	<i>mail05.parking.ru</i>	<i>softfail, transitioning, not designate</i>	-	<i>softfail, transitioning, not designate</i>	<i>fail</i>	<i>gmail.com</i>	<i>mail05.parking.ru</i>	<i>spoofing</i>
<i>budi@gmail.com</i>	<i>budi@gmail.com</i>	<i>emkei.cz</i>	<i>softfail, transitioning, not designate</i>	-	<i>softfail, transitioning, not designate</i>	<i>fail</i>	<i>gmail.com</i>	<i>emkei.cz</i>	<i>spoofing</i>

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
<i>inudin11@gmail.com</i>	250	<i>ok</i>	<i>spoofing</i>
<i>budi@gmail.com</i>	550	<i>does not exist</i>	<i>spoofing</i>

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

- 1) Server siap, kode 220 merupakan pesan selamat datang yang berarti server email dossier dapat bekerja dengan baik.
- 2) Sukses, kode 250 merupakan pesan bahwa server berhasil mengirimkan pesan.
- 3) Gagal, kode 550 merupakan pesan bahwa server gagal memeriksa alamat email dengan kata lain bahwa alamat email tersebut tidak ada.
- 4) 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 tersedia (421).
- 5) Ukuran berlebih, kode 552 merupakan pesan bahwa ukuran pesan terlalu besar.
- 6) Alamat email salah, kode 553 merupakan pesan bahwa terdapat alamat email yang salah dalam melakukan transaksi email.
- 7) 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.

c. *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.

d. *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.

e. *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 <https://who.is/whois-ip/ip-address>.

Tabel 4. alamat client IP email pengirim

Alamat email	Alamat IP	Organization	Email Domain	Status
<i>inudin11@gmail.com</i>	195.128.120.25	RIPE Network Coordination Centre (RIPE)	@parking.ru	Spoofing
<i>budi@gmail.com</i>	46.167.245.116	RIPE Network Coordination Centre (RIPE)	@finaltek.com	Spoofing

Tabel 4, 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.

f. *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
<i>inudin11@gmail.com</i>	SMTP	spoofing
<i>budi@gmail.com</i>	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:

- 1) Port 25 adalah port default SMTP yang tidak dienkripsi.
- 2) Port 465 adalah port yang memiliki keamanan atau disebut juga Secure SMTP/SMTPS/SSMTP.
- 3) Port 2525 adalah port SMTP dengan enkripsi TLS.
- 4) Port 587 adalah port SMTP dengan enkripsi TLS.

5. *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.

6. 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
<i>inudin11@gmail.com</i>	<i>spoofing</i>	Tidak Dapat dilakukan pengaturan file signature
<i>budi@gmail.com</i>	<i>spoofing</i>	Tidak Dapat dilakukan pengaturan file signature

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

7. 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 Parabeen'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.

8. 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
<i>Email Address</i>	<i>inudin11@gmail.com</i>	<i>budi@gmail.com</i>
<i>IP Address</i>	<i>195.128.120.25</i>	<i>46.167.245.116</i>
<i>Hostname</i>	<i>Mail05.parking.ru</i>	<i>Emkei.cz</i>
<i>Country</i>	<i>Russian Federation (RU)</i>	<i>Czech Republic (CZ)</i>
<i>State</i>	<i>Moskva</i>	<i>Stredocesky Kraj</i>
<i>City</i>	<i>Moscow</i>	<i>Mesice</i>
<i>Postcode</i>	<i>101990</i>	<i>250 64</i>
<i>ISP</i>	<i>parking.ru</i>	<i>UPC Ceska Republica</i>
<i>Organization</i>	<i>Grant-Parik-Intertet Ltd</i>	<i>Zdenek Klouda – FinalTek.com</i>

Information	Pengirim Ke 3	Pengirim Ke 4
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

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 8. 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		√	Tidak ada pada penelitian sebelumnya		
	a	<i>Email collection by client</i>	√			
	b	<i>Email extraction tool</i>	√			
4	Structured data	√	√			
	a	<i>ID actors of interest</i>	√		√	
	b	<i>Examining sender's e-mail address,</i>	√		√	
	c	<i>Examining time message create</i>	√		√	
	d	<i>Examining message ID</i>	√		√	
	e	<i>Examining sender's IP address</i>			√	Tidak ada pada penelitian sebelumnya
	f	<i>Protocol used to transport email</i>			√	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		

4. KESIMPULAN

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 Interdisciplinary 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). ANALISIS 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>