PENGEMBANGAN *FRAMEWORK* UNTUK INVESTIGASI EMAIL *FORENSICS* MENGGUNAKAN METODE *SYSTEMS DEVELOPMENT LIFE CYCLE* (SDLC)

LA ODE MUHAMMAD SAIDI

14917145

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensik Digital

Program Studi Magister Teknik Informatika

Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia

2017

Lembar Pengesahan Pembimbing

Pengembangan *Framework* untuk Investigasi Email *Forensics* menggunakan Metode *Systems Development Life Cycle* (SDLC)

Nama : La Ode Muhammad Saidi
NIM : 14917145

Yogyakarta, Maret 2017

Pembimbing I,	Pembimbing II,
Dr. Bambang Sugiantoro, MT	Yudi Prayudi, S.Si, M.Kom

Lembar Pengesahan Penguji

Pengembangan *Framework* untuk Investigasi Email *Forensics* menggunakan Metode *Systems Development Life Cycle* (SDLC)

Nama : La Ode Muhammad Saidi

NIM : 14917145

Yogyakarta, Maret 2017

Tim Penguji,

Dr. Bambang Sugiantoro, MT

Ketua

Yudi Prayudi, S.Si, M.Kom

Anggota I

Dr. Imam Riadi, M.Kom

Anggota II

Mengetahui,

Ketua Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia

Dr. R. Teduh Dirgahayu, ST.,M.Sc

Abstrak

Electronic mail (email) merupakan sistem digital yang bertujuan untuk mengirim dan menerima pesan elektronik melalui suatu jaringan *client – server*. Hampir semua orang diseluruh dunia menggunakan email untuk mengirim pesan dikarenakan prosesnya yang mudah dan cepat. Terkadang setiap satu orang memiliki jumlah akun lebih dari satu akun. Banyaknya pengguna email serta mudahnya dalam bertransaksi membuat segelintir orang memanfaatkannya untuk melakukan tindakan kejahatan misalnya dengan membuat identitas palsu, mengirimkan pesan palsu dan lain - lain. Oleh sebab itu investigasi email *forensics* sangat berperan penting dalam hal ini. Agar proses investigasi berjalan dengan baik maka dibutuhkan sebuah *framework* yang dapat membantu para investigator untuk melakukan penyelidikan berdasarkan tahap demi tahap. *Framework* yang dibuat dalam penelitian ini merupakan pengembangan dari *framework* sebelumnya. *Framework* yang dikembangkan akan menghasilkan tahapan investigasi email *forensics* mulai dari tahap awal sebelum berada di tempat kejadian perkara, analisis barang bukti yang ditemukan, pemeriksaan email dan penyerahan kembali barang bukti.

Kata kunci :

Framework, investigasi, forensik email, SDLC

Abstract

Electronic mail (email) is a digital system that aims to send and receive electronic messages via a network client - server. Almost all people around the world use email to send messages because the process is simple and fast. Sometimes every single person has a number of accounts in more than one account. The number of email users and ease in transaction makes a few people use it to commit crimes for example by creating a false identity, send false messages and others - others. Therefore, email forensics investigation is very important in this regard. In order for the investigation process goes well we need a framework that can help the investigators to conduct an investigation based on step by step. Framework made in this study is a development of the previous framework. Framework developed will generate email forensics investigation stages ranging from early stage before being at the crime scene, analyzing evidence found, email checking and re-delivery of items of evidence.

Keywords

Framework, investigation, email forensics, SDLC.

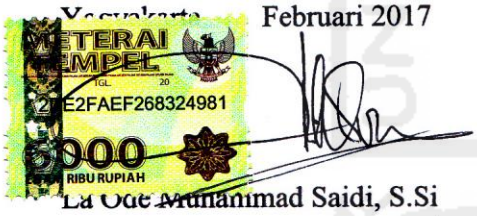
Pernyataan keaslian tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Untuk material yang membutuhkan izin, saya juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan material tersebut dalam tesis ini.

Yogyakarta, Februari 2017



La Ode Muhammad Saidi, S.Si

Publikasi selama masa studi

Tidak ada publikasi yang menjadi bagian dari tesis

Kontribusi yang diberikan oleh pihak lain dalam tesis ini

Tidak ada kontribusi dari pihak lain.

Halaman Persembahan

Segala puji bagi Allah SWT yang tidak pernah tidur, tidak pernah merasa lelah dan pemilik segala kesempurnaan, serta salawat bagi Rasulullah SAW rahmat bagi semesta alam.

Kepersembahkan karyaku ini kepada orang yang tersayang dan kurindukan selama masa studi, istri dan anakku. Melalui ini juga penulis menghanturkan permohonan maaf yang sebesar-besarnya kepada istriku yang terpaksa kutinggalkan saat masih masa nifas seminggu setelah melahirkan, dan kepada anakku yang terpaksa juga kutinggalkan pada umur 1 minggu yang seharusnya pada masa itu mereka masih sangat membutuhkanku untuk berada disisi mereka.

Kepada almarhumah ibuku yang terpaksa ku tinggalkan saat masih dalam keadaan sakit, melalui ini juga penulis bersembah sujud memohon ampunan dosa terbesar sampai terkecilpun, dan tidak sempat melihatnya untuk terakhir kalinya sebelum ibu menghembuskan nafas terakhir. Maafkan anakmu.

Semua penulis terpaksa lakukan untuk masa depan rumah tanggaku.

Semua penulis terpaksa lakukan untuk membanggakan ibu.

Kata Pengantar

Assalamu ‘Alaikum Wr. Wb.

Segala puji dan syukur bagi Allah SWT penguasa semesta alam serta pemilik segala kesempurnaan. Alhamdulillah penulis ucapkan karena atas rahmat, hidayyah dan karunia-Nya sehingga penulis senantiasa diberikan kesehatan, ketabahan dan kemudahan dalam menyelesaikan tesis ini dengan segenap kemampuan. Tidak lupa pula penulis hanturkan salam dan salawat kepada Rasulullah SAW dan para sahabat-sahabat serta keluarganya yang telah membimbing umat manusia ke jalan yang lebih baik.

Melalui tesis ini penulis ucapkan permohonan maaf dan terima kasih yang tak terhingga kepada kepada kedua orang tua yang telah mendidik, merawat, dan melindungi penulis dan seluruh anak-anaknya tanpa membeda-bedakan dengan kesungguhan hati sejak kecil sampai kapanpun yang tiada merasa letih dan bosan serta pengorbanannya yang tak terhingga tanpa mengharapkan imbalan sekecil apapun baik secara materil maupun moril. Khususnya kepada ibu, penulis bersembah sujud mengharap ampunan dosa karena tidak sempat bertatap muka untuk terakhir kalinya sebelum menghembuskan nafas di dunia dan pergi meninggalkan penulis untuk selamanya.

Meskipun dalam proses penyelesaian tesis ini penulis diperhadapkan dengan berbagai kendala dan rintangan namun karena adanya bimbingan, bantuan dan dorongan dari berbagai pihak, baik secara langsung maupun tidak langsung sehingga tesis ini dapat terselesaikan.

Tentu tidaklah berlebihan kiranya pada kesempatan ini penulis mengucapkan terima kasih kepada semua pihak yang telah memberikan bantuannya selama penyelesaian tesis ini sebagai sebuah penghargaan kepada :

1. Bapak Ir. H. Soekarno sebagai Presiden pertama Republik Indonesia yang bersedia meluangkan waktunya untuk meresmikan Sekolah Tinggi Islam (STI), yang kemudian berganti menjadi UII. Bapak Drs. H. Mohammad Hatta Wakil Presiden pertama Republik Indonesia yang bersedia meluangkan waktunya untuk meresmikan Universitas Islam Indonesia (UII).
2. Bapak Dr. Ir. Harsoyo, M.Sc sebagai Rektor UII, bapak Dr. Ing. Ilya Fajar Maharika, MA., IAI sebagai Wakil Rektor I, bapak Dr. Nur Feriyanto, M.Si sebagai Wakil Rektor II, dan bapak Dr. Abdul Jamil, SH, MH sebagai Wakil Rektor III.
3. Bapak Dr. R. Teduh Dirgahayu, ST., M.Sc. sebagai Ketua Program Pascasarjana Fakultas Teknologi Industri Universitas Islam Indonesia.

4. Bapak Yudi Prayudi, S.Si., M.Kom. selaku Ketua Jurusan Forensika Digital FTI UII sekaligus sebagai Pembimbing II yang telah meluangkan waktunya dalam membimbing dan membantu serta memudahkan penulis selama penulisan tesis ini.
5. Bapak Dr. Bambang Sugiantoro, M.T. selaku pembimbing I yang telah meluangkan waktunya dalam membimbing dan membantu serta memudahkan penulis selama penulisan tesis ini.
6. Bapak Dr. Imam Riadi, M. Kom selaku Penguji III yang telah memberikan masukan, saran, dan kritikan kepada penulis sebagai perbaikan untuk menjadi lebih baik lagi.
7. Segenap Dosen dan Staf UII Yogyakarta yang telah memberikan bantuan, motivasi, dan bimbingan serta waktu luangnya dalam berdiskusi dengan penuh kesabaran dan keikhlasan.
8. Afrilah Andi Aris sebagai sahabatku dan semua rekan – rekan pascasarjana FTI UII khususnya Jurusan Forensika Digital angkatan X yang tidak bisa penulis tuliskan satu-persatu yang selalu membantu penulis selama proses perkuliahan di UII Yogyakarta.
9. Kakak-kakak serta ipar-ipar yang selalu memotifasi penulis dengan penuh ketabahan.

Akhirnya hanya kepada Allah SWT penulis serahkan segala usaha yang telah dilakukan. Harapan penulis semoga tesis ini dapat bermanfaat bagi kita semua, Amiiin…

Yogyakarta, Februari 2017

La Ode Muhammad Saidi, S.Si

Daftar Isi

Daftar Tabel

Daftar Gambar

Takarir dan Singkatan

SDLC	:	*Systems Development Life Cycle*
Email	:	*Electronic Mail*
dkk	:	dan kawan–kawan
IEFAF	:	*Integrated E-Mail Forensic Analysis Framework*
URL	:	*Uniform Resource Locator*
IDFIF	:	*Integrated Digital Forensics Investigation Framework*
IIF	:	*Investigasi and Intelijen Framework*
HTTP	:	*Hypertext Transfer Protocol*
POP3	:	*Post Office Protocol versi 3*
IMAP	:	*Internet Message Access Protocol*
SMTP	:	*Simple Mail Transport Protocol*
Cc	:	*Carbon copy*
Bcc	:	*Blind carbon copy*
IP	:	*Internet Protocol*
Gmail	:	*Google Mail*
Ymail	:	*Yahoo Mail*
SSL	:	*Secure Socket Layer*
AD FTK	:	*Access Data Forensic ToolKit*
MD5	:	*Message Digest algortihm 5*
SHA1	:	*Secure Hash Algorithm 1*
IPV4	:	*Internet Protocol version 4*
IPV6	:	*Internet Protocol version 6*
RIPE	:	*Réseaux IP Européens*
TLS	:	*Transport Layer Security*
ISP	:	*Internet Service Provider*

Bab I Pendahuluan

1.1 Latar Belakang

Electronic Mail atau biasa disingkat juga email yang dalam bahasa Indonesia diartikan sebagai "surat elektronik" merupakan sebuah sistem yang bertujuan untuk mengirim dan menerima pesan elektronik berupa file gambar, audio, video, dan lain-lain dari satu orang ke orang lain di belahan dunia melalui jaringan internet. Email juga dapat memungkinkan penggunanya untuk mengirimkan pesan ke banyak penerima dalam waktu singkat secara bersamaan. Selain tujuan tersebut, email juga digunakan sebagai salah satu syarat untuk membuat akun di media sosial misalnya *facebook*, alamat blog, dan lain sebagainya. Banyaknya manfaat dan kemudahan yang disediakan oleh email sehinggga dapat membantu pekerjaan manusia dalam hal mengirim dan menerima pesan secara elektronik.

Berdasarkan sebuah survei yang berasal dari *The Radicati Group, Inc* bahwa laporan statistik pengguna email di seluruh dunia pada tahun 2015 hampir mencapai nilai 2,6 milyar pengguna sedangkan tahun 2019 diperkirakan mencapai lebih dari 2,9 milyar pengguna dengan jumlah akun sebanyak lebih dari 4,3 – 5,5 milyar akun. Untuk lebih jelasnya dapat dilihat pada tabel berikut :

Tabel 1. 1 Jumlah pengguna dan akun email tahun 2015 serta perkiraan sampai dengan tahun 2019

	2015	**2016**	**2017**	**2018**	**2019**
Worldwide Email Accounts (B)	4,353	4,626	4,920	5,243	5,594
%Growth		*6%*	*6%*	*7%*	*7%*
Worldwide Email Users* (B)	2,586	2,672	2,760	2,849	2,943
% Growth		*3%*	*3%*	*3%*	*3%*
Average Accounts Per User	1.7	1.7	1.8	1.8	1.9

Sumber : (The Radicati Group, Email Statistics Report, 2015-2019).

Salah satu kelemahan email adalah pemalsuan identitas oleh penggunanya, kelemahan tersebut merupakan sebagian dari masalah email dan masalah yang melibatkan email tersebut tentu saja membutuhkan investigasi. Investigasi yang dilakukan harus melalui tahapan-tahapan

yang sesuai agar tidak terjadi kesalahan atau menimbulkan permasalahan baru dalam proses insvestigasi. Menurut Devendran, dkk, bahwa e-mail forensik mengacu pada studi tentang sumber dan isi e-mail sebagai bukti untuk mengidentifikasi pengirim yang sebenarnya dan penerima pesan, data / waktu transmisi, catatan rinci transaksi e-mail, maksud dari pengirim, dll. Penelitian ini melibatkan investigasi metadata, pencarian kata kunci, port scanning, dll untuk penulis atribusi dan identifikasi penipuan e-mail. Terdapat 6 tahapan dalam teknik investigasi forensik pada email yaitu *header analysis, bait tactics, server investigation, network device investigation, software embedded identifiers,* dan *sender mailer fingerprints*. (Banday, 2011). 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. (Banday, M. T.,2011)

Investigasi email *forensics* merupakan penyelidikan terhadap sebuah email dengan mencatat atau merekam fakta melakukan peninjauan, percobaan, dan sebagainya, dengan tujuan memperoleh jawaban atas pertanyaan tentang suatu peristiwa, aktivitas dan sebagainya). Dalam melakukan proses investigasi email *forensics* terdapat teknik atau tahapan yang harus dilakukan misalnya seperti yang disebutkan oleh Chhabra dan Bajwa (2012) yang menjelaskan bahwa terdapat 6 teknik investigasi dan forensik email yaitu *header investigation, server investigation, network and network device investigation, investigation of software embedded details, investigation and discovery of hidden emails,* dan *investigation of anti forensic activity*. (Chhabra & Bajwa, 2012). Menurut Marwan, penyelidikan terhadap e-mail meliputi: *examining sender's e-mail address, examining message initiation protocol (HTTP, SMTP), examining message ID,* dan *examining sender's IP address*, selain itu terdapat beberapa aspek lain dalam penyelidikan e-mail yaitu *storage format of email, availability of backup copy of email,* dan *protocol used to transport email*. (Devendran, dkk 2015)

Menyadari pentingnya sebuah panduan tentang tahapan-tahapan dan teknik investigasi email *forensics* untuk menghasilkan pembuktian yang bersifat ilmiah maka para peneliti terus mengembangkannya dalam bentuk teknik investigasi dan framework. Framework yang membahas tentang teknik investigasi email terakhir kali dikembangkan pada tahun 2011 selebihnya hanya mengembangkan secara teknik saja tanpa membuatkan dalam bentuk framework. Seperti penelitian yang dilakukan tentang framework untuk penyelidikan data email, framework tersebut menghasilkan 5 tahapan yaitu *acquisition*, *importation*, *triage*, *analysis*, dan *presentation*. (Haggerty, dkk, 2011)

Permasalahan dari penelitian-penelitian sebelumnya yang membahas tentang *framework* dan teknik dalam melakukan investigasi dan forensik email adalah masih terdapat beberapa tahapan yang bisa menjadi sebuah permasalah baru diantaranya belum adanya tahapan persiapan dan pada proses analisis email belum menjelaskan secara detail bagaimana cara melakukan analisis email *forensics*. Penelitian yang dilakukan adalah pengembangan *framework* yang membahas tentang tahapan investigasi email forensik yang dilakukan oleh Haggerty, dkk (2011), yang digabungkan dengan teknik investigasi email forensik yang dilakukan oleh Devendran, dkk (2015), Chhabra & Bajwa, (2012), Banday, (2011), Chhabra & Bajwa, (2012) sehingga bisa dijadikan sebagai pedoman oleh penyidik.

Berdasarkan permasalahan diatas, maka penelitian yang akan dilakukan ini adalah pengembangan *framework* investigasi email *forensics* berdasarkan perpaduan antara *framework* yang dikembangkan oleh Haggerty, dkk (2011) dengan teknik investigasi email *forensics* yang dikembangkan oleh Devendran, dkk (2015), Chhabra & Bajwa, (2012), Banday, (2011), Chhabra & Bajwa, (2012) sehingga dapat dijadikan standar pengguunaan oleh para penyidik investigator khususnya dalam email *forensics*.

Systems Development Life Cycle (SDLC) merupakan suatu proses pembuatan dan pengubahan sistem serta model dan metodologi yang digunakan untuk mengembangkan sebuah sistem. Menurut Rhodes, SDLC memiliki 5 tahapan yaitu *planning, analysis, design, implementation,* dan *maintenance*. (Rhodes, 2012). Tahapan SDLC tersebut dapat dijadikan sebagai tolak ukur untuk membangun framework baru. Sama halnya sebuah sistem, *framework* juga merupakan sekumpulan dari tahapan – tahapan yang saling berhubungan antara satu dengan lain dimana dalam tahapan utamanya terdapat sub-tahapan yang mendukung kinerja dari tahapan utama tersebut. Dalam pengembangannya sebuah *framework* harus memiliki tahapan atau metode agar proses pengembangan dapat tersusun dengan rapi.

Berdasarkan penjelasan dari SDLC diatas dapat dikatakan bahwa SDLC dapat dijadikan sebagai metode dalam penelitian ini untuk mengembangkan sebuah *framework* dari *framework* sebelumnya. Beberapa pendukung dari metode SDLC adalah bahwa pengembangan *framework* memerlukan sebuah persiapan, analisis, desain, dan implementasi dan pemeliharaan. Penelitian yang dilakukan akan menghasilkan sebuah pengembangan *framework* yang dikembangkan dari *framework* sebelumnya dengan teknik investigasi khususnya dibidang investigasi email *forensics* yang diharapkan dapat digunakan oleh para investigator sebagai standar *framework* dalam investigasi email *forensics*.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, yang menjadi rumusan masalah dalam penelitian yang dilakukan adalah :

1. Bagaimana mengembangkan sebuah *framework* berdasarkan *framework* sebelumnya khususnya tentang investigasi email *forensics*.
2. Bagaimana kinerja framework yang telah dikembangkan pada kebutuhan investigasi email *forensics*.

1.3 Batasan Masalah

Batasan masalah yang ditetapkan dalam penelitian ini adalah sebagai berikut :

1. Penelitian ini dilakukan hanya terkait pada pengembangan *framework* dan *framework* yang dikembangkan adalah terkait investigasi email *forensics*.
2. Simulasi kasus yang dilakukan pada penelitian ini adalah jenis kejahatan *spoofing email* berbasis *web based mail*.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah diatas, yang menjadi tujuan dalam penelitian yang dilakukan adalah :

1. Dapat mengembangkan sebuah *framework* investigasi email *forensics* berdasarkan *framework* sebelumnya.
2. Dapat melakukan ujicoba terhadap kinerja dari *framework* tersebut pada sebuah contoh kasus.

1.5 Manfaat Penelitian

Manfaat dilakukannya penelitian ini adalah sebagai berikut:

1. Memberikan kemudahan bagi para investigator dalam melakukan investigasi khususnya pada email *forensics*.
2. Sebagai referensi bagi penelitian lain yang mengambil kajian penelitian yang sama dan sebagai wawasan untuk pengembangan penelitian selanjutnya.

1.6 Review Penelitian

Telah banyak dilakukan penelitian tentang investigasi dan forensik email. Beberapa penelitian yang telah dilakukan sebelumnya antara lain adalah penelitian yang dilakukan oleh Hadjidj, dkk

(2009) melakukan penelitian tentang penggunaan sebuah platform analisis terpadu di mana seorang analis keamanan dapat melakukan berbagai tugas yang berhubungan dengan analisis e-mail yang disebut sebagai IEFAF (*Integrated E-Mail Forensic Analysis Framework*), IEFAF terdiri dari lima sub-modul yang dapat digunakan secara terpisah atau bersama-sama untuk membangun dan mengeksplorasi model pendukung keputusan. Modul ini adalah *inter-database browser, statistics explorer, data mining explorer, weka submodule,* dan *e-mail explorer*.

Menurut Banday (2011) bahwa e-mail forensik mengacu pada studi tentang sumber dan isi e-mail sebagai bukti untuk mengidentifikasi pengirim yang sebenarnya dan penerima pesan, data / waktu transmisi, catatan rinci transaksi e-mail, maksud dari pengirim, dll. Penelitian ini melibatkan investigasi metadata, pencarian kata kunci, port scanning, dll untuk penulis atribusi dan identifikasi penipuan e-mail. Terdapat 6 tahapan dalam teknik investigasi forensik pada email yaitu *header analysis, bait tactics, server investigation, network device investigation, software embedded identifiers,* dan *sender mailer fingerprints*. Ditahun yang sama penelitian serupa juga dilakukan oleh Banday (2011) melakukan penelitian terhadap analisis forensik dari pesan e-mail yang 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.

Penelitian ditahun yang sama juga dilakukan oleh Haggerty, dkk, (2011) membangun sebuah *framework* untuk penyelidikan data email, framework tersebut meliputi 5 tahap yaitu *acquisition, importation, triage, analysis,* dan *presentation*.

Penelitian berikutnya oleh Chhabra dan Bajwa, (2012) melakukan penelitian dibidang forensik email yang menjelaskan bahwa terdapat 6 teknik investigasi dan forensik email yaitu *header investigation, server investigation, network and network device investigation, investigation of software embedded details, investigation and discovery of hidden emails,* dan *investigation of anti forensic activity*.

Penelitian selanjutnya oleh Rahayu dan Prayudi (2014) melakukan penelitian tentang *integrated digital forensics investigation framework* (IDFIF) menggunakan metode *sequential logic*, *framework* yang dihasilkan merupakan hasil evaluasi dari 6 model *framework* yang kemudian menghasilkan sebuah *framework* baru yang dibagi menjadi 4 tahapan investigasi forensik digital yaitu *pre-process, proactive, reactive,* dan *post-process*.

Penelitian yang serupa dilakukan oleh Alan, dkk (2014) melakukan penelitian tentang *Investigasi and Intelijen Framework* (IIF) model ekstraksi bukti digital untuk proses penyelidikan tersebut menghasilkan 4 tahapan yaitu *preparation and identification, strategy and*

priority, examination and analysis, dan *reporting and documentation*. Dalam penelitian tersebut mereka menggunakan konsep 4W (*when, where, who,* dan *how*).

Penelitian selanjutnya oleh Devendran, dkk (2015), penyelidikan terhadap e-mail meliputi: *examining sender's e-mail address, examining message initiation protocol (HTTP, SMTP), examining message ID,* dan *examining sender's IP address*, selain itu terdapat beberapa aspek lain dalam penyelidikan e-mail yaitu *storage format of email, availability of backup copy of email,* dan *protocol used to transport email*. (Devendran, dkk 2015)

Satti dan Jafari (2015) yang mengusulkan sebuah framework baru tentang proses investigasi forensik pada domain tertentu. *Framework* tersebut dikembangkan melalui evaluasi dari 9 *framework*. Pada model tersebut dihasilkan 10 tahapan investigasi.

Menurut (Rhodes, 2012) bahwa *Systems Development Life Cycle* (SDLC) merupakan suatu proses pembuatan dan pengubahan sistem serta model dan metodologi yang digunakan untuk mengembangkan sebuah sistem. Menurut Rhodes, SDLC memiliki 5 tahapan yaitu *planning, analysis, design, implementation,* dan *maintenance*. (Rhodes, 2012).

Tabel 1. 2 Rangkuman Literatur Review

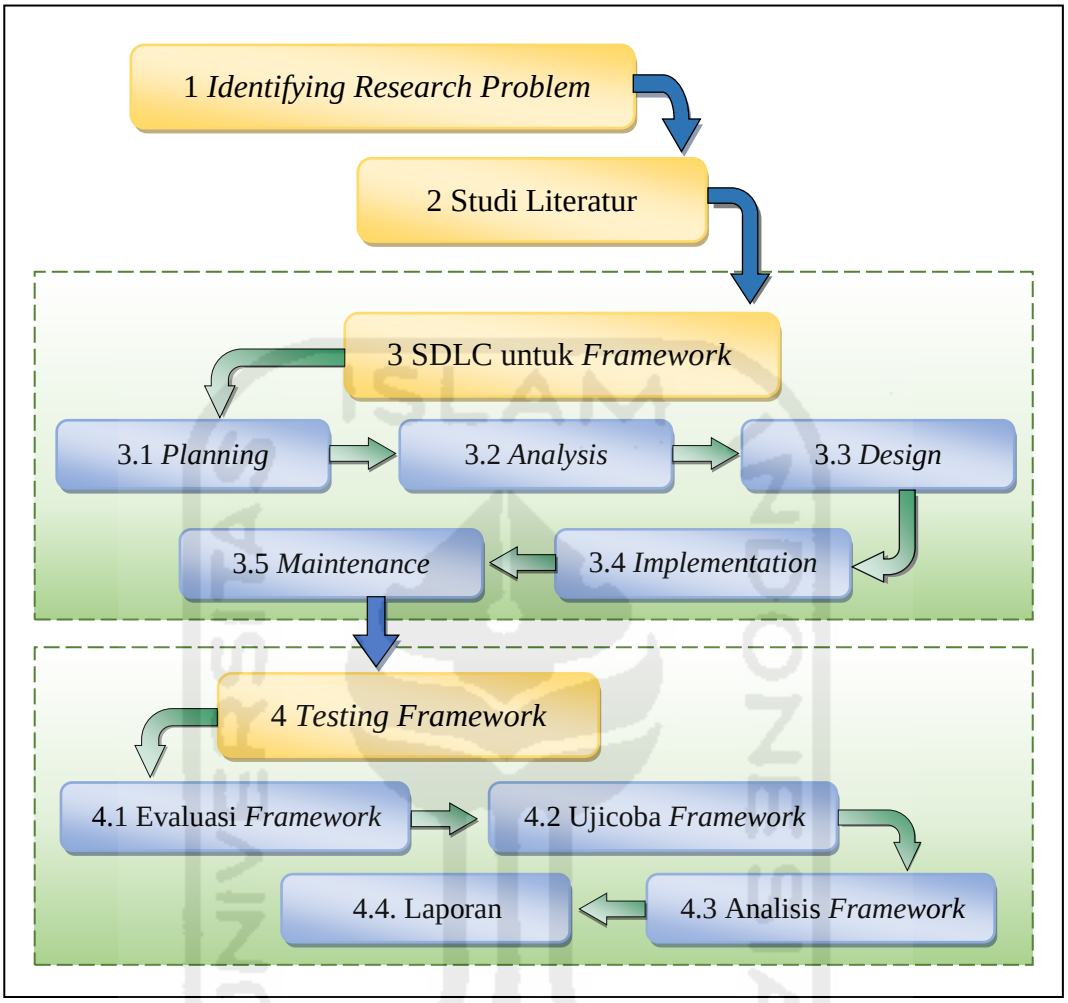
Paper Utama	Teknik Investigasi Email Forensik	Model *Framework*	Pengembangan *Framework*
Jafari, F., & Satti, R. S. (2015).	-	*Domain specific cyber forensics investigation process model*	Menggabungkan 9 jenis *framework* sebelumnya untuk menghasilkan *framework* baru.
Devendran, V. K., Shahriar, H., & Clincy, V. (2015).	Menghasilkan 7 tahapan penyelidikan email	-	-
Alan, Kelvin, Anthony and Zetta (VXRL). (2014).	Menghasilkan 4 tahapan investigasi bukti digital	-	
Rahayu, Y. D., & Prayudi, Y. (2014).	-	*Integrated Digital Forensics Investigation Framework* (IDFIF)	Menggabungkan 6 jenis *framework* dan mengeliminasi tahapan yang sama menjadi satu *framework* baru dengan metode sequential logic.
Chhabra, G. S., & Bajwa, D. S. (2012).	Menghasilkan 6 tahapan dalam teknik investigasi forensik pada email	-	-
Banday, M. T. (2011).	Menghasilkan 6 teknik investigasi dan forensik email	-	-
Haggerty, J., Karran, A., Lamb, D., & Taylor, M. (2011).	Menghasilkan 5 tahap penyelidikan data email	*A Framework for the Forensic Investigation of Unstructured Email*	Mengembangkan sebuah *framework* dari Hadjidj, dkk (2009)
Hadjidj, R., Debbabi, M., Lounis, H., Iqbal, F., Szporer, A., & Benredjem, D. (2009).	Menghasilkan 5 modul analisis data email	*Towards an integrated e-mail forensic analysis framework. Digital Investigation*	Menggabungkan 2 jenis *framework* dan melakukan analisis terhadap tahapan yang sama menjadi satu *framework* baru (IEFAF)

Lanjutan **Tabel 1. 2** Rangkuman Literatur Review

Paper Utama	Teknik Investigasi Email Forensik	Model *Framework*	Pengembangan *Framework*
Usulan Penelitian	Menghasilkan beberapa tahapan investigasi email *forensics*	Pengembangan *framework* untuk investigasi email *Forensics*	Menggabungkan 1 *framework* dan 3 teknik investigasi email *forensics*
	Masalah yang diangkat dalam penelitian ini adalah pengembangan *framework* investigasi email *forensics* yang telah dilakukan sebelumnya oleh Haggerty, & dkk (2011) yang digabungkan dengan 3 jenis teknik investigasi email *forensics* sebelumnya oleh Devendran, dkk (2015), Chhabra & Bajwa, (2012), dan Banday, M. T. & dkk (2011) sehingga dapat mempermudah investigator dalam melakukan investigasi email *forensics* dan bisa dijadikan sebagai standar investigasi khususnya pada email *forensics*. *Framework* email *forensics* yang dikembangkan oleh Haggerty, & dkk (2011) masih perlu untuk dilakukan pengembangan berdasarkan teknik investigasi email *forensics*. Solusi yang ditawarkan adalah mengembangkan sebuah *framework* dengan menggunakan metode *Systems Development Life Cycle* (SDLC).		

1.7 Metodologi Penelitian

Agar penelitian ini terarah maka penelitian ini menggunakan beberapa tahapan metode, yang dapat dilihat pada gambar dibawah ini.



Gambar 1. 1 Metode Penelitian

Gambar diatas menunjukkan penelitian ini menggunakan 4 tahapan utama metodologi penelitian yakni :

(1) *Identifying Research Problem*, (2) Studi Literatur, (3) SDLC untuk *Framework* terdiri dari 5 tahapan yaitu *planning*, *analysis*, *design*, *implementasi*, dan *maintenance*, (4) *Testing Framework* terdiri dari 3 tahapan yaitu, evaluasi *framework*, ujicoba *framework*, analisis *framework*, dan laporan.

1.8 Sistematika Penulisan

Tahapan ini memberikan gambaran secara umum tentang penyusunan penelitian yang dilakukan, dalam sistematika penulisan terbagi dalam beberapa BAB yaitu :

Bab I Pendahuluan

Pendahuluan, merupakan pengantar terhadap permasalahan yang akan diteliti. Di dalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan.

Bab II Landasan Teori

Pada Bab ini menjelaskan teori-teori yang terkait untuk memecahkan masalah dalam penelitian yang dilakukan.

Bab III Metodologi Penelitian

Bab ini membahas tentang langlah-langkah penelitian, kebutuhan perangkat keras dan perangkat lunak yang akan digunakan, desain dan perancangan antarmuka framework yang akan dibuat, serta implementasinya pada sebuah studi kasus.

Bab IV Hasil dan Pembahasan

Hasil dan Pembahasan, berisi tentang pembahasan penyelesaian masalah yang diteliti dengan membangun sebuah *framework* dan cara pengujian serta penerapannya pada sebuah studi kasus sesuai dengan permasalahan yang di usulkan.

Bab V Kesimpulan dan Saran

kesimpulan dan Saran, memuat kesimpulan-kesimpulan dari hasil penelitian dan saran-saran yang perlu diperhatikan berdasar keterbatasan yang ditemukan dan asumsi-asumsi yang dibuat selama melakukan penelitian dan juga rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.

Bab II Landasan Teori

2.1 *Framework*

Framework atau dalam bahasa Indonesia disebut juga sebagai kerangka kerja. *Framework* juga dapat diartikan sebagai tahapan-tahapan yang terstruktur dan saling berhubungan antara satu dengan lainnya untuk membentuk sebuah aturan berdasarkan pokok permasalahan yang didesain sedemikian rupa agar dapat dipahami oleh penggunanya untuk menyelesaikan suatu permasalahan tertentu. *Framework* juga dapat di artikan sebagai kumpulan script (terutama class dan function yang dapat membantu developer/ programmer dalam menagani berbagai masalah-masalah dalam pemrograman seperti koneksi ke database, pemanggilan variabel, dan file. Sehingga developer lebih fokus dan lebih cepat membangun aplikasi. (Rosmala & Gandalisha, 2011)

2.2 Email

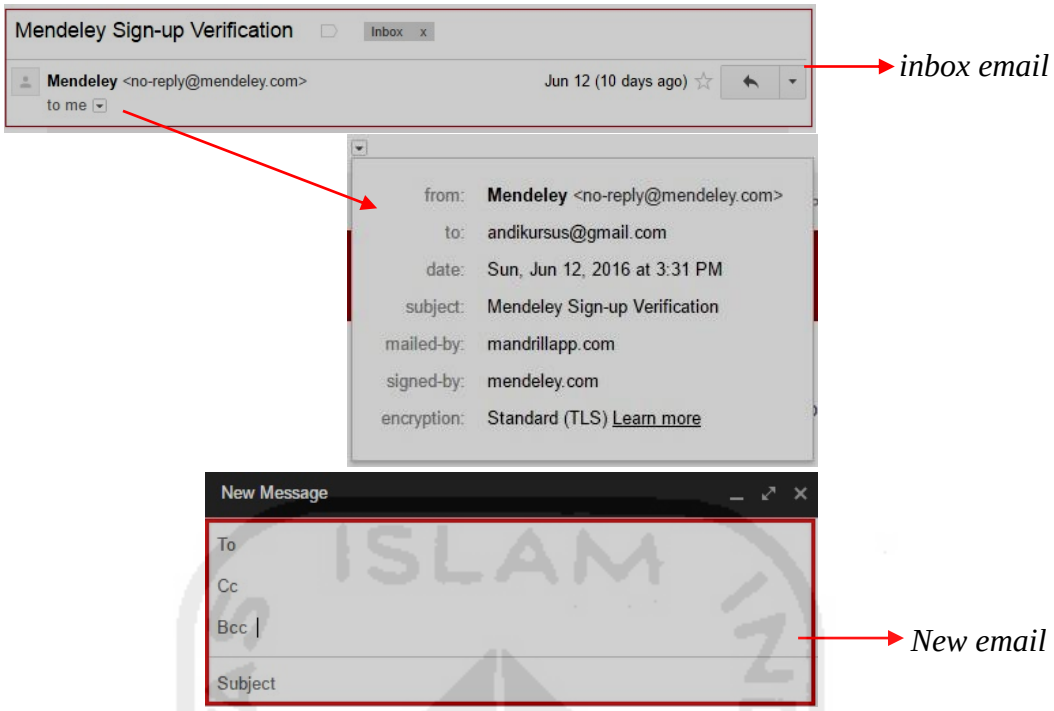
Electronic Mail atau biasa disingkat juga email dalam bahasa Indonesia diartikan sebagai "surat elektronik" merupakan sebuah sistem yang bertujuan untuk menulis, mengirim, menerima dan menyimpan pesan elektronik berupa file gambar, audio, video, dan lain-lain dari satu orang ke orang lain di belahan dunia melalui jaringan internet. Email juga dapat memungkinkan penggunanya untuk mengirimkan pesan ke banyak penerima dalam waktu singkat secara bersamaan. Selain tujuan tersebut, email juga digunakan sebagai salah satu syarat untuk membuat akun di media sosial misalnya *facebook,* alamat blog, dan lain sebagainya. Banyaknya manfaat dan kemudahan yang disediakan oleh email sehinggga dapat membantu pekerjaan manusia dalam hal mengirim dan menerima pesan secara elektronik.

2.2.1 Struktur Email

Menurut Devendran, dkk (2015) Email memiliki dua bagian besar yaitu *header* dan *body*. Sedangkan menurut Haggerty & dkk, (2011), analisis email terdiri dari dua bagian penting yaitu *stuructured data* dan *unstuctured data.*

1. *Header* merupakan bagian dari email yang terstruktur mencakup beberapa bagian informasi penting dalam pesan email.

Adapun gambar berikut adalah contoh *header* pada salah satu email.



Gambar 2. 1 Contoh *header*

Berikut bagian-bagian informasi penting pada *header* :

- *From:* alamat email dan nama opsional dari pengirim pesan
- *To:* alamat email dan nama opsional dari penerima pesan
- *Subject:* subyek atau perihal merupakan ringkasan singkat dari isi pesan
- *Date:* waktu setempat dan tanggal saat pesan ditulis
- *Cc:* singkatan dari *Carbon copy*, memungkinkan untuk mengirim salinan email ke seseorang atau banyak orang. Orang yang memiliki alamat email pada kotak "*To:*" akan dapat melihat alamat email siapa saja yang di "*Cc*".
- *Bcc:* singkatan dari "*Blind Carbon Copy*", memungkinkan untuk mengirim salinan email ke seseorang tanpa diketahui oleh penerima email yang terdapat pada kotak "*To:*" dan "*Cc*:".
- *Received:* pelacakan informasi pesan yang dihasilkan oleh server mail yang sebelumnya telah ditangani.
- *Content-Type:* informasi tentang bagaimana pesan ditampilkan.
- *Reply-To:* alamat email yang digunakan untuk membalas pesan ke pengirim.
- *Mailed-by:* informasi tentang server penyedia email dari pengirim pesan.
- *Signed-by:* informasi tentang nama domain dari server mail pengirim pesan

2. *Body* merupakan isi surat atau pesan yang tak terstruktur yang ditulis atau dilampirkan dari file yang telah disimpan sebelumnya kedalam komputer, juga berisi *signature*

block. Selain itu terdapat fasilitas yang berfungsi untuk mengatur pesan teks dalam *body*, yaitu :

- *Formatting options* merupakan format pengaturan teks yang ditulis secara langsung pada kotak *body*, format tersebut terdiri dari pengaturan *font, size, bold, italic, underline, text color, align, numbered list, bulleted list, indent, quote,* dan *remove formating*.
- *Attach files* berfungsi untuk menyisipkan file yang berasal dari komputer.
- *Insert files using drive* berfungsi untuk menyisipkan file yang berasal dari *google drive*.
- *Insert photo* berfungsi untuk menyisipkan gambar atau foto.
- *Insert link* berfungsi untuk menyisipkan link pada alamat website dan email.
- *Insert emoticon* berfungsi menyisipkan ikon gambar emotikon
- *Insert Gif* berfungsi menyisipkan gambar dengan *type Gif*.

Adapun gambar berikut adalah contoh *body* pada salah satu email.

Gambar 2. 2 Contoh *body* dan *formatting options* pada pesan email

Selain dari kedua bagian tersebut juga terdapat satu bagian penting dari struktur email yaitu *signature* atau *file signature* yang merupakan informasi tentang pengirim pesan, misalnya nama kantor, alamat kantor, nomor telepon dan lain-lain

2.2.2 Bentuk Komunikasi Email

Bentuk komunikasi menggunakan email dibedakan menjadi 5 yaitu :

1. *Point to Point*, yaitu mengirimkan email langsung ke sebuah alamat tertentu. Biasanya komunikasi ini digunakan hanya pada satu orang pengiriman atau hanya dengan satu alamat email antara pengirim dan penerima saja.
2. *Carbon copy* (*Cc*), yaitu mengirim salinan pesan email kepada orang lain baik satu atau lebih dari satu orang selain dari *point to point* sebuah email, selain ditujukan ke sebuah alamat utama juga dikirimkan tembusannya ke alamat lain. Orang yang memiliki alamat email pada kotak "*To:*" akan dapat melihat alamat email siapa saja yang di "*Cc*". Komunikasi ini digunakan apabila pesan email yang akan dikirim lebih dari satu alamat email atau dikirim sebagai tembusan.

3. *Blind carbon copy* (BCC) adalah komunikasi lanjutan dari komunikasi *Carbon copy* (Cc) yang memungkinkan pengirim melakukan pengiriman salinan email kepada alamat email tertentu untuk dirahasiakan kepada alamat email yang terdapat pada *Carbon copy* (Cc) atau dengan kata lain bahwa pesan email yang dikirim oleh pengirim kepada alamat email yang terdapat pada *Blind carbon copy* (Bcc) tidak dapat diketahui oleh alamat email yang ditulis pada *Carbon copy* (Cc). Komunikasi ini digunakan apabila pesan email yang akan dikirim lebih dari satu alamat email dan sebagian lainnya tidak boleh mengetahui kepada siapa saja pengirim melakukan pengiriman email tersebut, biasanya komunikasi ini digunakan untuk mengirim pesan pada atasan atau pimpinan.
4. *Distribution List* yaitu komunikasi dengan menggunakan email secara satu arah. Biasanya ini dibuat oleh orang yang berkepentingan untuk menyebarluaskan informasi tertentu (pengumuman, berita harian, update mengenai perkembangan suatu proyek, buletin, jurnal, dan sebagainya), tetapi tidak mengharapkan adanya respon dari para penerima emailnya. Untuk itu yang harus dilakukan adalah membuat sebuah alamat tertentu khusus untuk keperluan ini. Bila pengelola distribution list mengirimkan sebuah email ke alamat tersebut, maka alamat itu akan mem-forward email tadi ke semua alamat email yang menjadi pelanggan (subscriber) dari distribution list.
5. *Discussion List* seringkali juga disebut *mailing list* atau *milis*. Bentuknya hampir sama dengan *distribution list*. Ada 2 *discussion list* yang sering dibuat yaitu secara terbatas dan secara terbuka atau bebas. Untuk dapat bergabung ke dalam sebuah milis pertama-tama seseorang harus mendaftar terlebih dahulu berdasarkan aturan yang telah ditetapkan. Perbedaan dari kedua *milis* tersebut adalah apabila *milis* tersebut dibuat secara terbatas maka pendaftar akan diseleksi terlebih dahulu oleh admin apakah disetujui bergabung atau tidak dan apabila *milis* tersebut dibuat secara terbuka atau bebas maka pendaftar tidak memerlukan seleksi admin untuk menyetujui atau menolak permohonan menjadi anggota milis.

2.2.3 Analisis Email

Menurut Banday (2011), analisis email bertujuan untuk menemukan bukti dari sumber dan isi pesan e-mail, 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, email forensik juga melibatkan investigasi terhadap client atau server komputer yang diduga digunakan atau disalahgunakan untuk aktivitas pelanggaran email. Pemeriksaan tersebut diantaranya *Internet favorites, Cookies, History, Typed URL's,*

Temporary Internet Files, Auto- completion Entries, Bookmarks, Contacts, Preferences, Cache, dan lain-lain. Terdapat beberapa perangkat lunak *open source* yang telah dikembangkan untuk melakukan *email header analysis* guna mengumpulkan bukti terhadap aktivitas kejahatan yang melibatkan email.

Analisis email bisa dimulai dari kotak surat penerima yang berisi pesan e-mail. Analisis ini melibatkan penyelidikan dari kedua informasi kontrol yaitu *header* dan *body*. Berbagai perangkat lunak telah dikembangkan untuk membantu analisis email maupun penyelidikan forensik email, diantaranya *eMailTrackerPro* (www.emailtrackerpro.com), *EmailTracer* (www.cyberforensics.in), *Adcomplain* (www.rdrop.com/users/billmc/adcomplain.html), *Aid4Mail Forensic* (www.aid4mail.com), *AbusePipe* (www.datamystic.com/abusepipe.html), *AccessData's FTK* (www.accessdata.com/), *EnCase Forensic* (www.guidancesoftware.com), *FINALeMAIL* (www.finaldata. com), *Sawmill-GroupWise* (www.sawmill.net), *Forensics Investigation Toolkit* (FIT) (www.edecision4u.com/FIT.html), *Paraben (Network) E-mail Examiner* (www.paraben.com/email-examiner.html), dan lain-lain.

2.3 Investigasi Email *Forensics*

Investigasi email *forensics* sangat dibutuhkan karena mengingat hampir disetiap penjuru dunia menggunaan email sebagai salah satu media atau sistem untuk mengirim, menerima dan menyimpan data secara elektronik yang dapat memberikan banyak kemudahan. Selain itu juga banyaknya aktivitas-aktivitas pelanggaran hukum yang melibatkan email sebagai media penggaran yang ada.

2.3.1 Investigasi Forensik

Investigasi adalah upaya penelitian, penyidikan, pengusutan, pencarian, pemeriksaan dan pengumpulan data, informasi dan temuan lainnya untuk mengetahui atau membuktikan kebenaran dan atau kesalahan sebuah fakta yang kemudian menyajikan kesimpulan atas rangkaian temuan dan susunan kejadian.

Forensika adalah suatu proses ilmiah dalam mengumpulkan, menganalisis, dan menghadirkan berbagai bukti dalam sidang pengadilan terkait adanya suatu kasus hukum. Bidang forensika tersebut juga berkembang terhadap komputer. Menurut Yeni & Prayudi (2014), forensika komputer adalah suatu proses mengidentifikasi, memelihara, menganalisis, dan menggunakan bukti digital menurut hukum yang berlaku. Ruang lingkup dari komputer forensik merupakan aktivitas yang berhubungan dengan pemeliharaan, identifikasi, pengambilan, penyaringan dan dokumentasi bukti komputer dalam kejahatan

komputer. Dari proses - proses tersebut dapat dilakukan analisis dan penyelidikan untuk menentukan potensi bukti-bukti yang legal (Nursyamsi, 2010).

Data-data yang dapat dipakai dan diambil dari sumber daya komputer diantaranya terdapat pada sistem komputer, jaringan komputer, jalur komunikasi, media penyimpanan, aplikasi komputer dan lain-lain. Data tersebut dapat diolah sesuai dengan prosedur yang berlaku sehingga dapat dijadikan sebagai bukti yang legal dan sah (Yeni & Prayudi, 2014).

2.3.2 Email *Forensics*

Email *forensics* dilakukan karena banyaknya pengguna email yang menjadikannya sebagai media untuk melakukan tindakan kejahatan atau ilegal dengan tujuan beragam salah satunya menyadap atau mengintip email orang lain untuk mendapatkan informasi yang dianggap penting untuk keuntungan pribadi. Tujuan email *forensics* adalah untuk menemukan bukti dari permasalahan yang ada. Email *forensics* itu sendiri merupakan proses ilmiah yang melibatkan persiapan investigasi dan forensika terhadap sebuah email terkait adanya kasus hukum untuk menemukan bukti dari permasalahan dan membuktikan kebenaran dari hasil temuan tersebut berdasarkan prosedur hukum yang berlaku.

Untuk mengidentifikasi dengan benar tentang informasi penting seperti nama atau identitas penerima, jalur yang digunakan untuk mengangkut email antara pengirim dan penerima, aplikasi *client-side* yang digunakan untuk menulis email, *timestamp* ketika pesan dibuat, ID pesan yang unik, dan lain–lain dalam literatur, pemeriksaan dan pengungkapan informasi kunci dari email yang dikenal sebagai email forensik. (Devendran, dkk, 2015).

2.3.3 Teknik Investigasi Email *Forensics*

Teknik investigasi merupakan cara atau langkah-langkah yang terstruktur yang dilakukan untuk menemukan bukti atau untuk menyelesaikan permasalahan yang ada.

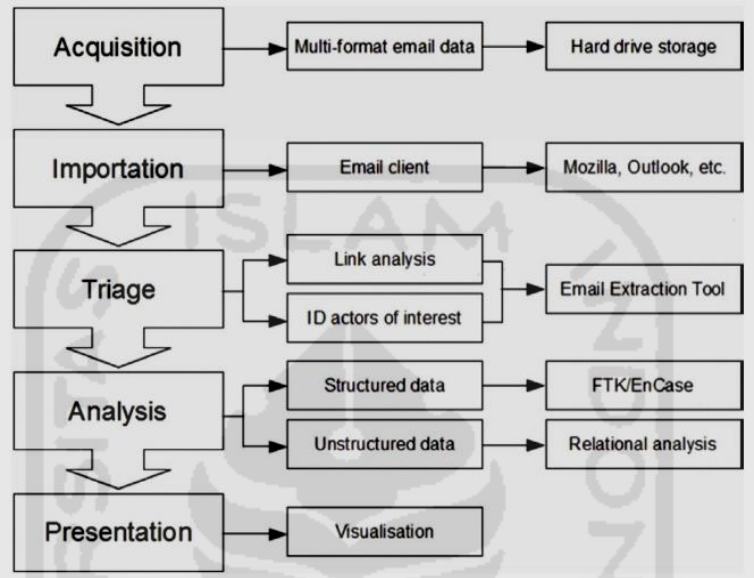
Investigasi email forensik mengacu pada studi tentang sumber dan isi email sebagai bukti untuk mengidentifikasi pengirim yang sebenarnya dan penerima pesan, data / waktu transmisi, catatan rinci transaksi email, maksud dari pengirim, dll. Penelitian ini melibatkan investigasi metadata, pencarian kata kunci, port scanning, dll untuk penulis atribusi dan identifikasi penipuan email. Terdapat 6 tahapan dalam teknik investigasi forensik pada email yaitu *header analysis, bait tactics, server investigation, network device investigation, software embedded identifiers,* dan *sender mailer fingerprints*, (Banday, dkk, 2011).

Sedangkan menurut Chhabra dan Bajwa, (2012) menjelaskan bahwa terdapat 6 teknik investigasi dan forensik email yaitu *header investigation, server investigation,*

network and network device investigation, investigation of software embedded details, investigation and discovery of hidden emails, dan *investigation of anti forensic activity*.

2.3.4 *Framework* Investigasi Email *Forensics*

Framework investigasi email *forensics* digunakan sebagai tahapan atau pola kerja dalam menangani email forensic, menurut Haggerty & dkk, (2011) ada beberapa tahapan dalam *framework* investigasi email *forensics* adalah sebagai berikut:



Gambar 2. 3 *Framework* investigasi email *forensics*

Sumber : *A framework for the forensic investigation of unstructured email relationship data (2011).*

Merujuk pada gambar 2.3 diatas, terdapat 5 tahapan *framework* investigasi email *forensics*, yaitu tahapan (1) *acquisition*, tahapan (2) *improtation*, tahapan (3) *triage*, tahapan (4) *analysis*, (5) *presentation*.

2.4 Barang Bukti

Barang bukti berarti temuan yang didapat dari hasil investigasi. Secara umum barang bukti identik dengan temuan dari investigasi sebuah tindak kejahatan. Menurut Rahayu (2014) bahwa dari barang bukti ini tim investigasi dan analis forensik dapat mengungkap kasus dengan kronologis yang lengkap. Barang bukti dapat dikelompokan menjadi bukti fisik dan non-fisik.

Dalam ilmu komputer forensik dikenal dengan nama bukti digital. Bukti digital itu sendiri adalah setiap data digital yang memiliki relevansi dengan pertanyaan hukum. Dalam hal ini, bukti digital ini mirip dengan bukti fisik, jenis bukti yang ada di pada ilmu forensik klasik (seperti biologi forensik atau kedokteran forensik). Tidak seperti bukti fisik, bukti digital tidak terkait dengan bukti fisik (misalnya, pita magnetik) yang menyimpan data. Nilai bukti digital secara teratur terletak pada informasi yang dikodekan dalam data yang tersimpan. Dalam kasus

dikatakan perangkat penyimpanan fisik sangat penting (misalnya, hard disk dari komputer tertentu disita di tempat tertentu). Namun secara langsung dapat dikatakan bahwa bukti digital adalah kombinasi dari keduanya (Dardick, dkk, 2014).

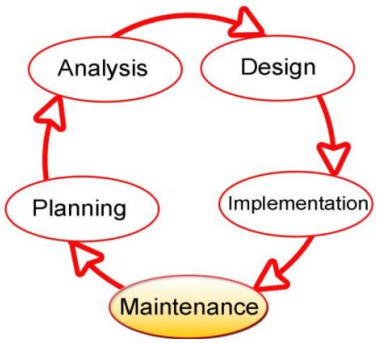
Menurut Al- Azhar (2012) barang bukti diklasifikasikan menjadi 2 bagian:

1. Barang bukti elektronik merupakan barang bukti yang bersifat fisik dan dapat dikenali secara visual sehingga tim investigasi dan tim analisis dapat memahami dan mengenali masing barang bukti tersebut. Jenis barang bukti tersebut antara lain:
   - Komputer, Laptop, Handphone
   - Router, Switch, Kamera,
   - Flashdisk, Harddisk, dan lain-lain
2. Barang bukti digital merupakan barang bukti yang di ekstrak atapun direcovery dari barang bukti elektronik. Jenis barang bukti ini yang harus dicari oleh analis forensik yang kemudian akan diteliti keterkaitan barang. bukti tersebut dengan kasus kejahatan. Contoh-contoh barang bukti digital antara lain adalah *logical file, Deleted file, lost file, File slack, Log File, Encrypted file, Steganography file, Office File, Audio File, Video file, Image file, Email, User ID dan Password, Short Message Service (SMS), Multimedia Message Service (MMS)* dan *Call logs*.

2.5 *Systems Development Life Cycle* (SDLC)

Systems Development Life Cycle (SDLC) yang berarti siklus hidup pengembangan sistem atau *system life cycle* yang berarti siklus hidup sistem. Pada dasarnya SDLC merupakan suatu model dan motodologi yang digunakan untuk mengembangkan sebuah sistem yang ada. *Systems Development Life Cycle* (SDLC) merupakan suatu proses pembuatan dan pengubahan sistem serta model dan metodologi yang digunakan untuk mengembangkan sebuah sistem.

SDLC memiliki 5 tahapan yaitu *planning, analysis, design, implementation,* dan *maintenance,* (Rhodes, 2012). Seperti pada gambar berikut :



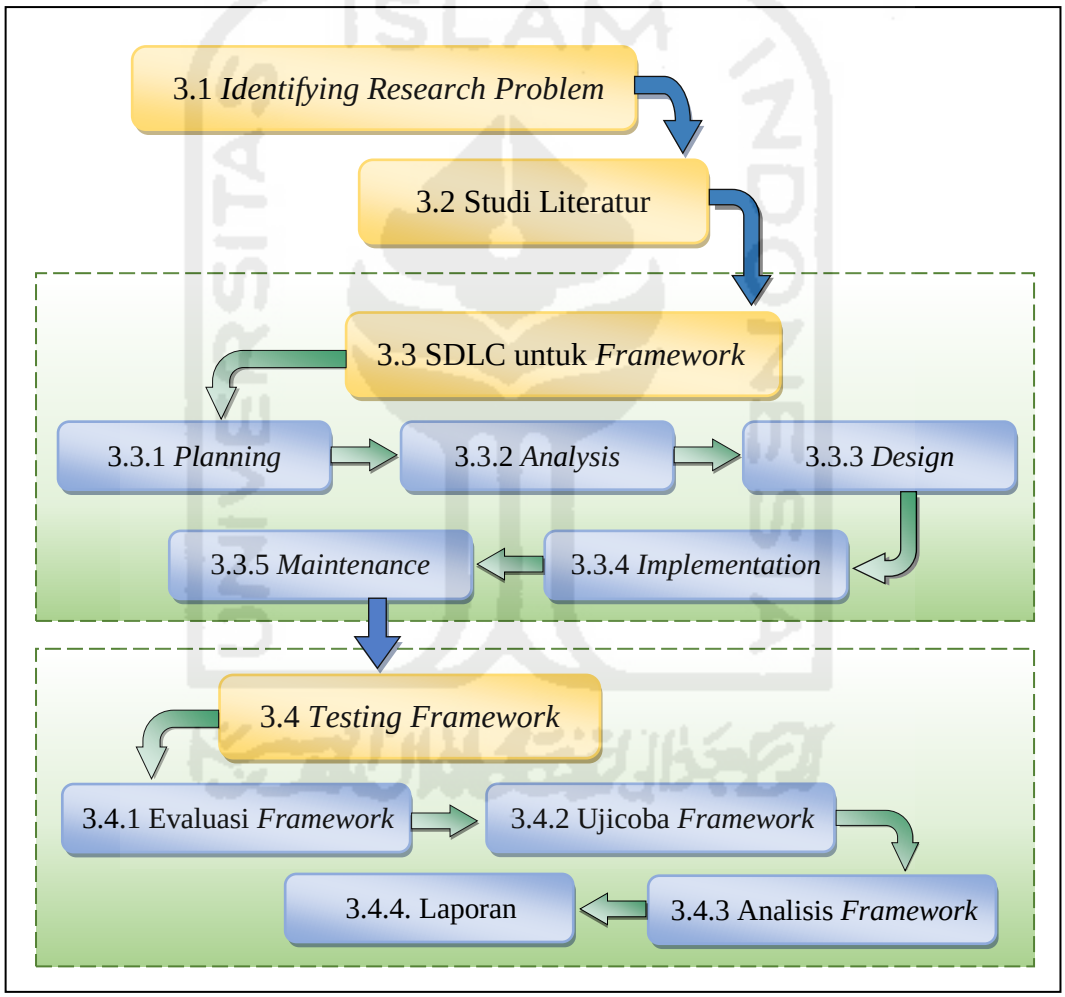
Gambar 2. 4 Tahapan SDLC
Sumber : The Systems Development Life Cycle (SDLC) as a Standard : Beyond the Documentation (2012)

Tahapan diatas dapat dijelaskan sebagai berikut :

1. *Planning* atau tahap perencanaan bertujuan untuk mengidentifikasi dan memprioritaskan sistem apa saja yang akan dikembangkan, dan sasaran-sasaran yang ingin dicapai.
2. *Analysis* atau tahap analisis sistem merupakan tahap penelitian atas sistem yang telah ada dengan tujuan untuk merancang sistem baru atau memperbaharui sistem yang sudah ada. Pada tahap ini dilakukan aktivitas studi literatur untuk menentukan suatu kasus yang bisa ditangani oleh sistem, juga melakukan identifikasi terhadap sistem sebelumnya untuk dilakukan pengembangan sistem.
3. *Design* atau tahap perancangan sistem merupakan tahap untuk menetukan proses tahapan atau teknik untuk menerapkan sistem baru atau sistem yang dikembangkan dari sistem sebelumnya. Proses perancangan juga memerlukan analisa terhadap fungsi dari tiap-tiap tahapan atau teknik yang dibangun.
4. *Implementation* atau tahap implentasi sistem merupakan tahap untuk mengimplementasikan rancangan dari tahap-tahap sistem yang dibangun atau dikembangkan serta melakukan uji coba terhadap sistem tersebut.
5. *Maintenance* atau tahap pemeliharaan sistem merupakan proses pemeliharaan sistem selama penggunaan agar tetap mampu beroperasi secara benar.

Bab III Metodologi Penelitian

Pada bab ini menjelaskan tentang metodologi penelitan yang dilakukan. Penelitian yang akan dilakukan kali ini akan melalui beberapa tahapan agar penelitian dapat berjalan secara sistematis. Adapun tahapan-tahapan pada penelitian yang dilakukan terdiri dari 5 tahapan, seperti pada gambar berikut :



Gambar 3. 1 Metode Penelitian

Metodologi penelitian tersebut digunakan berdasarkan *review* dari penelitian yang terkait sebelumnya. Metodologi penelitian tersebut bertujuan untuk mengembangkan penelitian sebelumnya. Dalam penelitan ini dilakukan analisis untuk mengetahui tahapan-tahapan apasaja yang dapat diterapkan dalam *framework* investigasi email *forensics*. *Framework* dianalisis dan diuji coba agar dapat menghasilkan kesimpulan pengembangan dan pemanfaatan dengan baik. Metodologi penelitian ini meliputi 4 tahapan utama yaitu *Identifying Research Problem*, Studi

Literatur, SDLC untuk *Framework* yang terdiri dari 5 yaitu *Planning, Analysis, Design, Implementation,* dan *Maintenance*, *Testing Framework* yang terdiri dari 3 tahap yaitu Ujicoba *Framework,* Analisis *Framework,* Evaluasi *Framework.* Pembahasan dari metodologi penelitian tersebut dapat diuraikan sebagai berikut:

3.1 *Identifying Research Problem*

Identifying Research Problem merupakan langkah awal yang dilakukan untuk memperoleh dan menentukan topik penelitian yang akan diteliti lebih lanjut. Pada tahapan ini dimulai dengan melihat berbagai fenomena, kejadian dan informasi yang didapatkan dengan berbagai cara yang berhubungan dengan penelitian yang dilakukan.

Dalam penelitian yang akan dilakukan adalah pengembangan *framework* investigasi email *forensics* oleh Haggerty, & dkk (2011) yang digabungkan dengan 3 jenis teknik investigasi email *forensics* sebelumnya oleh Devendran, dkk (2015), Chhabra & Bajwa, (2012), dan Banday, M. T. & dkk (2011) dengan tujuan untuk mempermudah investigator dalam melakukan investigasi email *forensics* dan bisa dijadikan sebagai standar investigasi khususnya pada email *forensics*. *Framework* email *forensics* yang dikembangkan oleh Haggerty, & dkk (2011) masih perlu untuk dilakukan pengembangan berdasarkan teknik investigasi email *forensics*. Solusi yang ditawarkan adalah mengembangkan sebuah *framework* dengan menggunakan metode *Systems Development Life Cycle* (SDLC).

3.2 Studi Literatur

Studi literatur dilakukan untuk mendapatkan informasi mengenai topik penelitian yang dilakukan. Studi literatur dapat bersumber dari dokumen, buku, artikel, atau bahan tertulis lainnya yang berupa teori, atau penemuan sebelumnya, baik bersifat *online source* maupun *offline source.*

Studi literatur dilakukan pada penelitian yang telah dilakukan sebelumnya terkait dengan *framework* investigasi forensika digital, *framework investigasi email forensics,* teknik investigasi dan analisa email *forensics*, teori-teori tentang email dan investigasi email *forensics*, dan teori tentang *systems development life cycle* (SDLC) tentang pedoman analisis, desain, evaluasi, testing dan kesimpulan sehingga dapat menunjang tujuan akhir dari penelitian yang dilakukan.

Pada tahap pertama dilakukan studi literatur yang bertujuan untuk menjelaskan kajian pustaka dari teori-teori penunjang yang mendukung konstruksi penelitian. Kegiatan ini dilakukan dengan membaca buku, jurnal, artikel laporan penelitian, dan situs-situs di internet. Keluaran dari studi literatur ini adalah terkoleksinya referensi yang relevan dengan rumusan masalah.

Tujuannya adalah untuk memperkuat permasalahan serta sebagai dasar teori dalam melakukan studi dan juga menjadi dasar untuk melakukan penelitian.

Studi literatur dilakukan dengan cara mencari atau mengumpulkan bahan-bahan yang berhubungan dengan penelitian ini melalui:

- Buku, literaur ini didapatkan di perpustakaan atau dengan cara membeli serta buku yang didapat dari beberapa situs di internet.
- Artikel atau jurnal, literatur ini didapatkan dari beberapa situs di internet. *Keyword* yang digunakan adalah framework, investigasi forensik, email forensik, *Sistems Development Life Cycle* (SDLC) dan beberapa *keyword* lain yang berkaitan dengan penelitian yang dilakukan. Artikel yang digunakan adalah artikel yang berasal dari dalam negeri maupun luar negeri.
- Penelitian sebelumnya, literatur ini didapatkan dari internet dan dari perpustakaan. Topik atau tema yang dicari adalah yang berhubungan dengan penelitian yang dilakukan.

3.3 SDLC untuk *Framework*

Tahapan-tahapan yang harus dilakukan dalam melakukan evaluasi terhadap pengembangan *framework* sehingga dapat dijadikan sebagai *framework* standar dalam investigasi email *forensics* terdapat 5 tahap proses yang dimuat pada tabel SDLC seperti yang tertera pada tabel berikut ini.

Tabel 3. 1 Tahapan SDLC pada proses pengembangan *framework*

No	Tahapan SDLC	Pengembangan *Framework*
1	*Planning*	*Planning* atau tahap perencanaan merupakan tahap awal dari proses pengembangan *framework*. Tahap ini bertujuan untuk melakukan ekstraksi terhadap tahapan pada *framework* dan teknik investigasi email *forensics* dan sasaran-sasaran yang ingin dicapai. Pada tahap ini pengumpulan data dapat dilakukan berdasarkan *identifying research problem* terhadap *framework* dan teknik terkait investigasi email *forensics* pada penelitian sebelumnya.
2	*Analysis*	*Analysis* atau tahap analisis merupakan tahap penelitian atas *framework* dan teknik terkait investigasi email *forensics* yang telah ada sebelumnya dengan tujuan untuk mengembangkannya dalam bentuk *framework*. Pada tahap ini dilakukan proses identifikasi terhadap tahapan investigasi email *forensics* pada penelitian sebelumnya.

Lanjutan **Table 3.1** Tahapan SDLC pada proses pengembangan *framework*

No	Tahapan SDLC	Pengembangan *Framework*
3	*Design*	Tahapan ini merupakan langkah ketiga pada proses desain dalam pengembangan *framework* investigasi email *forensics*. Tahap ini dilakukan proses eliminasi terhadap tahapan-tahapan yang sama dan dijadikan sebagai tahapan ini dalam pengembangan *framework*. Pada tahapan ini juga diperlukan sebuah bentuk untuk perancangan pada pengembangan *framework*. Bentuk pengembangan yang digunakan dalam desain penelitian ini adalah menggunakan *state chart diagram*.
4	*Implementation*	*Implementation* atau tahap implentasi merupakan tahap untuk mengimplementasikan rancangan dari setiap tahapan - tahapan *framework* yang telah dikembangkan. Pada tahap ini dibangun sebuah *framework* yang telah dikembangkan.
5	*Maintenance*	*Maintenance* atau tahap pemeliharaan merupakan proses pemeliharaan *framework* selama penggunaan.

Berdasarkan tabel 3.2 diatas, maka tahapan SDLC pada proses pengembangan *framework* dapat dijelaskan sebagai berikut :

3.3.1 *Planning*

Planning atau tahap perencanaan merupakan tahap awal dari proses pengembangan *framework*. Tahap ini bertujuan untuk melakukan ekstraksi terhadap tahapan pada *framework* dan teknik investigasi email *forensics* dan sasaran-sasaran yang ingin dicapai. Pada tahap ini pengumpulan data dapat dilakukan berdasarkan *framework* dan teknik terkait investigasi email *forensics* pada penelitian sebelumnya.

Proses ekstraksi digunakan untuk melakukan ekstraksi terhadap tahapan *framework* investigasi *email forensics* dan teknik investigasi email forensik yang ada sebelumnya. Proses ini dilakukan dengan cara mengekstrak tahapan-tahapannya dalam dalam sebuah tabel penelitian yang dilakukan terkait *framework* dan teknik investigasi email *forensics* oleh Haggerty, & dkk (2011) yang digabungkan dengan 3 jenis teknik investigasi email *forensics* sebelumnya oleh Devendran, dkk (2015), Chhabra & Bajwa, (2012), dan Banday, M. T. & dkk (2011). Berikut adalah gambar dari proses ekstrasi tahapan *framework* dan teknik investigasi email *forensics* yang dilakukan sebelunya.

Gambar 3. 3 Proses ekstraksi tahapan investigasi

Hasil pencarian tersebut akan diektraksi dalam sebuah tabel yang memuat tentang tahapan-tahapan dari penelitian sebelumnya yang dapat digunakan sebagai bahan kajian dalam penelitian ini. Berikut contoh tabel yang digunakan.

Tabel 3. 2 Ekstrasi tahapan *framework* dan tahap investigasi email *forensics*

No	Paper Utama	Jenis Penelitian	Tahapan/Teknik
1	Nama Peneliti & judul$_1$	*Framework*$_1$	Jumlah tahapan$_1$
2	Nama Peneliti & judul$_2$	Teknik Investigasi$_2$	Jumlah tahapan$_2$
3	Nama Peneliti & judul$_3$	Tahap Investigasi$_3$	Jumlah tahapan$_3$
4	Nama Peneliti & judul$_4$	Tahap Investigasi$_4$	Jumlah tahapan$_4$

Berdasarkan penjelasan diatas, maka tahapan proses *planning* dapat dirangkum berdasarkan tabel berikut.

Tabel 3. 3 Input output pada proses *planning*

Input	Proses	Output
Tahapan *framework* dan teknik investigasi email *forensics* dari penelitian sebelumnya	*Planning*	Tabel ekstraksi tahapan investigasi yang memuat tentang jumlah dari *framework* dan teknik investigasi email forensics dari penelitian sebelumnya

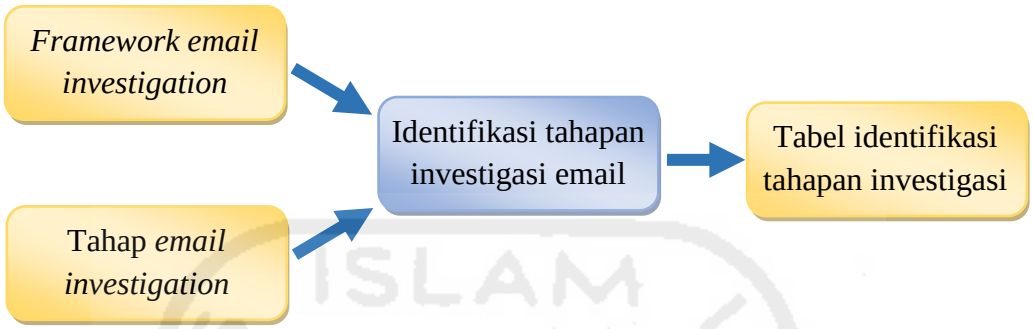
3.3.2 *Analysis*

Analysis atau tahap analisis merupakan tahap kedua dalam penelitian yang dilakukan. Tahap ini bertujuan untuk melakukan identifikasi terhadap *framework* dan teknik investigasi email *forensics* yang akan dikembangkan dan sasaran-sasaran yang ingin dicapai.

Adapun hal yang harus dilakukan pada tahapan ini adalah melakukan identifikasi terhadap *framework* dan teknik terkait investigasi email *forensics* untuk mengetahui kekurangannya masing-masing dengan cara mengumpulkan data dan informasi yang akan

mendukung analisis terutama pada proses penanganan investigasi email *forensics* secara umum.

Hasil dari proses identifikasi akan dimuat pada tabel identifikasi. Berikut adalah gambar proses identifikasi terdapat tahapan *framework* dan teknik investigasi email *forensics*.



Gambar 3. 5 Proses identifikasi tahapan investigasi

Dalam tahap ini dilakukan proses identifikasi terhadap tahapan *framework* dan teknik untuk untuk investigasi email *forensics* yang telah dikembangkan sebelumnya. Seluruh proses di urai tiap tahapannya dan kemudian di analogikan dan diterminologikan dan kemudian seluruh tahapan di petakan dalam tabel.

1. Identifikasi Tahapan *Framework* Investigasi Email *Forensics*

   Proses ini digunakan untuk melakukan identifikasi terhadap tahapan-tahapan dalam *framework* investigasi email *forensics* sehingga dapat terlihat jelas tujuan dari setiap tahapan-tahapan pada *framework* tersebut.
2. Identifikasi Teknik Investigasi Email *Forensics*

   Proses ini digunakan untuk melakukan identifikasi terhadap tahapan-tahapan dalam teknik investigasi email *forensics* sehingga dapat terlihat jelas tujuan dari setiap tahapan-tahapan dari teknik yang telah dikembangkan sebelumnya.

   Kemudian seluruh tehapan tersebut dipetakan kembali pada sebuah tabel dan diberi urutan sesuai dengan urutannya dalam *framework* dan tahapan analisis email *forensics*. Namun, apabila dari seluruh tahapan tersebut terdapat beberapa tahapan yang sama maka untuk tahapan yang sama akan diberi *ID* yang sama untuk memudahkan proses evaluasi terhadap *framework*.

Tabel 3. 4 Identifikasi tahapan *framework* dan teknik investigasi email *forensics*

Identifikasi	*Framework*	Teknik Investigasi$_1$	Tahap Investigasi$_2$	Tahap Investigasi$_3$
Tahapan$_1$				
Tahapan$_2$				
Tahapan$_{...n}$				

Berdasarkan penjelasan diatas, maka tahapan proses *analysis* dapat dirangkum berdasarkan tabel berikut.

Tabel 3. 5 Input output pada proses *analysis*

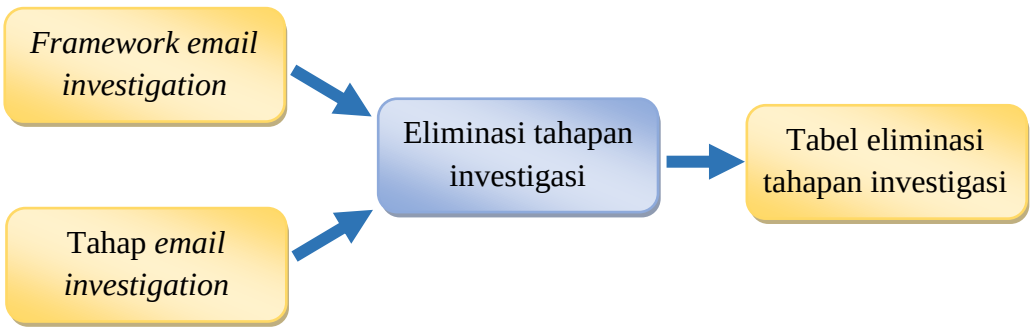
Input	Proses	Output
Tabel ekstraksi tahapan investigasi yang memuat tentang jumlah dari *framework* dan teknik investigasi email forensics dari penelitian sebelumnya	*Analysis*	Tabel identifikasi tahapan investigasi dari *framework* dan teknik investigasi email forensics dari penelitian sebelumnya

3.3.3 *Design*

Tahapan ini merupakan langkah ketiga pada proses desain dalam pengembangan *framework* investigasi email *forensics*. Tahap ini dilakukan proses eliminasi dan normalisasi terhadap tahapan-tahapan yang sama dan dijadikan sebagai tahapan inti dalam pengembangan *framework*. Pada tahapan ini juga diperlukan sebuah bentuk untuk perancangan pada pengembangan *framework*. Bentuk pengembangan yang digunakan dalam desain penelitian ini adalah menggunakan *state chart diagram*. Proses desain merupakan tahapan perancangan dari pengembangan *framework* sebelumnya yang kemudian dihasilkan sebuah *framework* baru. Tahapan yang telah dijabarkan pada tabel sebelumnya akan dieliminasi, sehingga muncul tahapan-tahapan inti yang akan dibangun menjadi sebuah *framework* menggunakan *state chart diagram* (Kohn, 2012).

1. Proses eliminasi tahapan *framework* dan teknik investigasi untuk pengembangan *framework* investigasi email *forensics*

   Pada tahap ini dilakukan proses eliminasi terhadap state-state (tahapan) yang maknanya sama. State-state yang tidak tereliminasi diasumsikan sebagai proses-proses utama dalam *framework*. Berikut adalah ilustrasi eliminasi terhadap tahapan-tahapan *framework* dan teknik investigasi email *forensics*.



Gambar 3. 7 Proses eliminasi tahapan investigasi

Tahap desain juga dilakukan dengan cara eliminasi. Eliminasi dilakukan pada tahapan yang memiliki arti yang ssama, sedangkan tahapan-tahapan yang tidak tereliminasi akan dijadikan sebagai salah satu tahapan atau sub-tahapan dari *framework* yang akan dibangun. Eliminasi tersebut akan dilakukan pada sebuah tabel eliminasi. Kemudian seluruh istilah dipetakan kembali pada sebuah tabel dan diberi urutan sesuai dengan urutannya. Untuk tahapan yang sama akan diberi *ID* yang sama untuk memudahkan proses evaluasi.

Tabel 3. 6 Eliminasi tahapan *framework* dan teknik investigasi email *forensics*

Tahapan *Framework* dan Analisis Email Forensik	*ID Framework*	Tahapan *Framework* yang Dikembangkan
$Tahapan_1$	1	$Tahapan_1$
$Tahapan_2$	1.1	$Tahapan_2$
$Tahapan_{.....}$	$1._n$	$Tahapan_{.....}$
$Tahapan_{...n}$	$n._n$	$Tahapan_{...n}$

Setelah melakukan proses pendefinisian setiap sub proses yang ada, maka pada tahap ini adalah melakukan kontruksi dan evaluasi terhadap model *framework* investigasi email *forensics* dengan cara melakukan perbandingan-perbandingan dengan teknik investigasi email *forensics* sehingga dapat diketahui tahapan-tahapan yang harus di sempurnakan pada pengembangan *framework* tersebut sehingga menghasilkan sebuah *framework* yang lebih baik dari sebelumnya.

2. Normalisasi *framework* dan teknik investigasi untuk pengembangan *framework* investigasi email *forensics*

   Normalisasi adalah proses untuk mengorganisasikan elemen dengan cara melakukan eleminasi terhadap grup elemen yang berulang-ulang (Jogiyanto, 2005). Pada bagian ini dilakukan proses perbandingan dari *framework* dan teknik investigasi dengan *framework* investigasi email *forensics* yang telah dikembangkan sehingga dapat dijadikan sebagai standar investigator dalam melakukan investigasi terhadap email *forensics*.

   Tabel 3. 7 Perbandingan *framework* dan teknik sebelumnya dengan *framework yang* telah dikembangkan terkait investigasi email *forensics*

Tahapan *Framework*	Analisis Email Forensik	Terdapat pada Pengembangan *Framework* Bagian:
$Tahapan_1$		
$Tahapan_2$		
$Tahapan_{...n}$		

Berdasarkan penjelasan diatas, maka tahapan proses *desain* dapat dirangkum berdasarkan tabel berikut.

Tabel 3. 8 Input output pada proses *design*

Input	Proses	Output
Tabel identifikasi tahapan investigasi dari *framework* dan teknik investigasi email forensics dari penelitian sebelumnya	*Design*	Tabel eliminasi dan normalisasi tahapan investigasi dari *framework* dan teknik investigasi email forensics dari penelitian sebelumnya

3.3.4 *Implementation*

Implementation atau tahap implentasi merupakan tahap untuk mengimplementasikan rancangan dari setiap tahapan - tahapan *framework* yang telah dikembangkan. Pada tahap ini akan dilakukan proses pengembangan *framework* berdasarkan tahapan-tahapan ini yang telah dikembangkan dari *framework* dan teknik investigasi email *forensics* dari penelitan sebelumnya. Proses pengembangan *framework* akan dibuat dalam bentuk *state chart diagram* menggunakan program aplikasi *microsoft visio*. Bentuk dari proses pengembangan *framework* akan dibuat secara berurutan berdasarkan tahapan awal dan subtahapan awal sampai dengan tahapan akhir dan subtahapan akhir sehingga dapat membentuk sebuah *framework* jadi yang bisa digunakan untuk melakukan investigasi email *forensics*.

Berdasarkan penjelasan diatas, maka tahapan proses *implementation* dapat dirangkum berdasarkan tabel berikut.

Tabel 3. 9 Input output pada proses *implementation*

Input	Proses	Output
Tabel eliminasi dan normalisasi tahapan investigasi dari *framework* dan teknik investigasi email forensics dari penelitian sebelumnya	*Implementation*	Membangun *framework* yang telah dikembangkan

3.3.5 *Maintenance*

Maintenance atau tahap pemeliharaan merupakan proses pemeliharaan *framework* selama penggunaan. Tahap ini juga merupakan tahap pengecekan terhadap *framework* untuk terus memberikan dukungan terhadap penggunanya agar tetap mampu beroperasi secara benar melalui tahapan-tahapan dalam *framework* yang telah dikembangkan sesuai dengan kebutuhan.

Berdasarkan penjelasan diatas, maka tahapan proses *maintenance* dapat dirangkum berdasarkan tabel berikut.

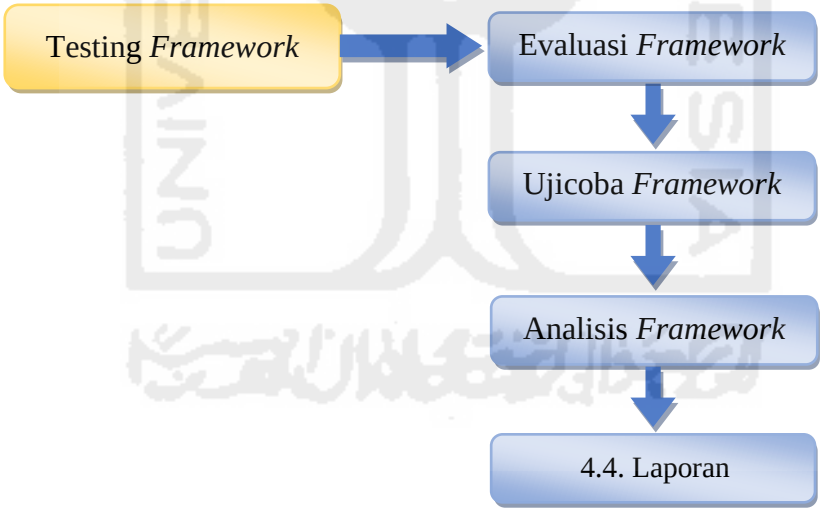
Tabel 3. 10 Input output pada proses *maintenance*

Input	Proses	Output
Membangun *framework* yang telah dikembangkan	*Maintenance*	Pemeliharaan/ pengecekan kembali *framework* yang telah dikembangkan

3.4 *Testing Framework*

Testing merupakan tahap yang bertujuan untuk menentukan kelayakan dari *framework* yang telah dikembangkan dari penelitian sebelumnya. Untuk melakukan *testing* tersebut maka dibuatlah tahapan-tahapan dari proses *testing* tersebut yaitu tahap ujicoba, tahap analisis, dan tahap evaluasi yang dilakukan pada penanganan investigasi email *forensics*. Hal ini dimaksudkan agar dapat diketahui proses kerja dari tahapan-tahapan yang dilakukan ketika dalam proses investigasi email *forensics*, sehingga *framework* tersebut dapat menjadi rujukan bagi para investigator untuk digunakan dalam penanganan investigasi email *forensics*.

Berikut adalah gambar ilustrasi dari tahapan *testing* pada penelitian ini.



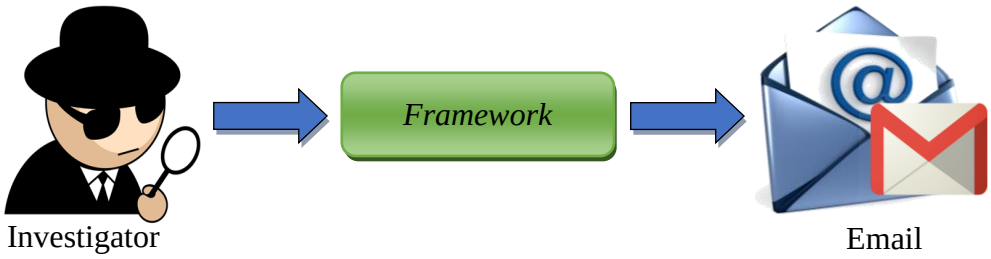
Gambar 3. 9 Tahapan *testing* penelitian

3.4.1 Evaluasi *Framework*

Tahap ini merupakan tahap pertama dalam melakukan *testing* yang bertujuan untuk menentukan kelayakan dari *framework* yang telah dikembangkan dari penelitian sebelumnya.

Studi kasus yang sudah dirancang akan dilakukan analisis terhadap sebuah pesan email dengan memanfaatkan *tools* email *forensics* yang telah disiapkan. Pesan email diasumsikan telah disalahgunakan sehingga perlu dilakukan proses investigasi email

forensics dengan memanfaatkan *framework* yang telah dikembangkan tersebut. Studi kasus ini dilakukan untuk memastikan bahwasanya tahapan-tahapan *framework* yang telah dikembangkan ini sesuai dengan tahapan investigasi email *forensics* dalam kondisi riil. Studi kasus ini diilustrasikan pada Gambar berikut:



Gambar 3. 11 Ilustrasi investigasi email *forensics*

Kesiapan sebuah penelitian untuk studi kasus ini harus diperhatikan demi keberhasilan yang maksimal meliputi kebutuhan sistem baik *hardware* maupun *software.* Dibawah ini merupakan sebagian besar kebutuhan sistem yang digunakan dalam studi kasus penelitian yang dilakukan diantaranya adalah:

1. *Hardware*(Perangkat Keras)
   a. Laptop
      - *Processor Intel(R) Pentium(R) CPU B960 @2.20GHz*
      - *RAM 2 GB,*
      - *Hardisk 500 GB*
2. *Software*(Perangkat Lunak)
   a. *Software* Penelitian
      - *Windows 8.1 Enterprise 64 bit*
   b. *Software* simulasi dan analisis investigasi *email forensics*
      - Layanan penyedia email (Gmail dan Yahoo), *Mail Client Thunderbird*
      - Situs *fake mailer* yang digunakan untuk mengirim email *spoofing* dan situs *traces mail*
      - *eMailTrackerPro v 10.0b, Paraben's E-mail Examiner,* dan *FTK Imager*

3.4.2 Ujicoba *Framework*

Tahapan ini merupakan tahap dilakukan skenario dan proses simulasi kasus terhadap kejahatan dengan menggunakan email misalnya email *spoofing* yang kemudian akan dilakukan analisis dengan menggunakan *framework* yang telah dikembangkan. Dalam proses analisis juga akan menjabarkan dan melakukan identifikasi dari tiap-tiap tahapan *framework* dan teknik investigasi email *forensics* serta *framework* yang telah dikembangkan.

3.4.3 Analisis *Framework*

Tahapan penelitian ini adalah melakukan tindakan evaluasi pada *framework* yang telah dikembangkan dengan *framework* sebelumnya. Evaluasi tersebut dilakukan berdasarkan hasil dari ujicoba pada setiap tahapan - tahapannya. Tahapan evaluasi tersebut merupakan proses perbandingan terhadap *framework* yang dikembangkan dengan *framework* sebelumnya.

Tabel 3. 11 Perbandingan *framework* yang telah dikembangkan dengan *framework* dan teknik investigasi email *forensics* sebelumnya.

Framework yang Dikembangkan	*Framework* Sebelumnya	Analisis Email Forensik
$Tahapan_1$	$Tahapan_1$	$Tahapan_1$
$Tahapan_2$	$Tahapan_2$	$Tahapan_2$
$Tahapan_{...n}$	$Tahapan_{...n}$	$Tahapan_{...n}$

3.4.4 Laporan

Tahap ini berisi laporan hasil analisis *framework* dengan melakukan perbandingan kelebihan dan kekurangan dari *framework* yang dikembagkan dan *framework* yang sebelumnya.

Tabel 3. 12 Kelebihan dan kekurangan *framework*

Framework	Kelebihan	Kekurangan
$Tahapan_1$	$Tahapan_1$	$Tahapan_1$
$Tahapan_2$	$Tahapan_2$	$Tahapan_2$
$Tahapan_{...n}$	$Tahapan_{...n}$	$Tahapan_{...n}$

Bab IV Hasil dan Pembahasan

4.1 SDLC untuk Pengembangan *Framework*

Terdapat 5 tahapan proses dalam *System Development Life Cycle (CDLC)* yang digunakan dalam proses pengembangan investigasi email *forensics*, yaitu :

1. *Planning*
2. *Analysis*
3. *Design*
4. *Implementation*
5. *Maintenance*

4.1.1 *Planning*

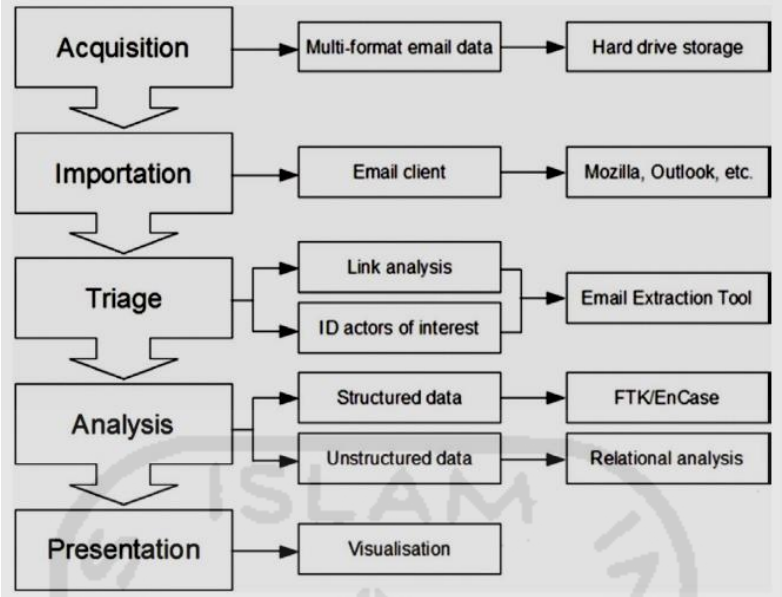
Planning merupakan tahap awal dari proses pengembangan *framework* yang bertujuan untuk melakukan ekstraksi terhadap tahapan pada *framework* dan Tahap investigasi email *forensics* pada penelitian sebelumnya.

a. *Framework* Investigasi Email Forensik

Menurut Haggerty & dkk, (2011), terdapat 5 tahapan dalam *framework* investigasi email *forensics* adalah sebagai berikut :

1. Tahap 1, *Acquisition*, meliputi :
   - *Multi-formal email data*
   - *Hard drive storage*
2. Tahap 2, *Importation*, meliputi :
   - *Email client*
   - *Mozilla, Outlook, etc.*
3. Tahap 3, *Triage*, meliputi :
   - *Link analysis* dan *ID actors of interest*
   - *Email extraction tool*
4. Tahap 4, *Analysis*, meliputi :
   - *Structured data* dan *Unstructured data*
   - *Relational analysis*
5. Tahap 5, *Presentation*, meliputi :

➢ *Visualisation*



Gambar 4. 1 *Framework* investigasi email *forensics*
Sumber : *A framework for the forensic investigation of unstructured email relationship data (2011)*

b. Tahap Investigasi Email Forensik

Menurut Devendran, dkk (2015), mengatakan bahwa penyelidikan terhadap email meliputi 7 tahapan yaitu :

1. Tahap 1, *Examining sender's email address,*
2. Tahap 2, *Examining message initiation protocol (HTTP, SMTP),*
3. Tahap 3, *Examining message ID,*
4. Tahap 4, *Examining sender's IP address,*
5. Tahap 5, *Storage format of email,*
6. Tahap 6, *Availability of backup copy of email,*
7. Tahap 7, *Protocol used to transport email.*

c. Teknik Investigasi Email Forensik

Menurut Chhabra dan Bajwa, (2012) terdapat 6 teknik investigasi dan forensik email yaitu :

1. Teknik 1, *Header investigation,*
2. Teknik 2, *Server investigation,*
3. Teknik 3, *Network and network device investigation,*
4. Teknik 4, *Investigation of software embedded details,*
5. Teknik 5, *Investigation and discovery of hidden emails,*
6. Teknik 6, *Investigation of anti forensic activity.*

Sedangkan menurut Banday, M. T. & dkk (2011) menerangkan bahwa terdapat 6 teknik investigasi forensik pada email yaitu :

1. Teknik 1, *Header analysis,*
2. Teknik 2, *Bait tactics,*
3. Teknik 3, *Server investigation,*
4. Teknik 4, *Network device investigation,*
5. Teknik 5, *Software embedded identifiers,*
6. Teknik 6, *Sender mailer fingerprints*.

Berikut adalah tabel ekstraksi *framework* dan tahap investigasi email forensik dari penjelasan diatas :

Tabel 4. 1 Ekstraksi tahapan *framework* dan teknik investigasi email *forensics*

No	Paper Utama	Jenis Penelitian	Tahapan
1	Haggerty, J., Karran, A., Lamb, D., & Taylor, M. (2011). A framework for the forensic investigation of unstructured email relationship data.	*Framework* investigasi email forensik	5 tahapan
2	Devendran, V. K., Shahriar, H., & Clincy, V. (2015). A Comparative Study of Email Forensic Tools	Tahapan investigasi email forensik	7 tahapan

Berdasarkan penjelasan diatas, maka tahapan proses *planning* dapat dirangkum berdasarkan tabel input-output berikut.

Tabel 4. 2 Input-output pada proses *planning*

Input	Proses	Output
1. *Framework* investigasi email forensic 2. Tahapan investigasi email forensic	*Planning*	1. 5 tahapan 2. 7 tahapan

4.1.2 *Analysis*

Tahapan ini dilakukan proses identifikasi dari ekstraksi tahapan *framework* dan Tahap investigasi email *forensics* pada tahap *planning* untuk mengetahui kekurangannya masing-masing dengan cara mengumpulkan data dan informasi yang akan mendukung analisis terutama pada proses penanganan investigasi email *forensics* secara umum.

Seluruh proses diurai tiap tahapannya kemudian seluruh tahapan di petakan dalam sebuah tabel.

1. Identifikasi *Framework* Investigasi Email *Forensics*

   Proses ini digunakan untuk melakukan identifikasi terhadap tahapan-tahapan dalam *framework* investigasi email *forensics* sehingga dapat terlihat jelas tujuan dari setiap tahapan-tahapan pada *framework* tersebut.

   Menurut Haggerty & dkk, (2011) terdapat 5 tahapan dalam *framework* investigasi email *forensics* adalah sebagai berikut :

   1. Tahap 1, *Acquisition*, merupakan proses akuisisi barang bukti email untuk keperluan analisis, proses akuisisi meliputi :
      - *Multi-formal email data,* proses akuisisi dilakukan pada seluruh data email.
      - *Hard drive storage,* merupakan tempat penyimpanan yang digunakan untuk proses akuisisi data email
   2. Tahap 2, *Importation*, merupakan tahap pengimporan data email, meliputi :
      - *Email client*, merupakan *email client* yang terdapat pada barang bukti.
      - *Mozilla, Outlook, etc,* merupakan software yang menyediakan fasilitas email.
   3. Tahap 3, *Triage*, merupakan proses awal analisis email, meliputi:
      - *Link analysis*, merupakan analisis terhadap *link* yang ada pada data email
      - *ID actors of interest,* merupakan ID para pelaku yang berkepentingan
      - *Email extraction tool*, merupakan alat atau *software* yang digunakan untuk melakukan ekstraksi data email.
   4. Tahap 4, *Analysis*, merupakan tahap analisa dari data email, meliputi :
      - *Structured data*, merupakan proses data email terstruktur
      - *Unstructured data*, merupakan proses data email tidak terstruktur
      - *Relational analysis*, merupakan hasil dari proses analisis data email yang relasional.
   5. Tahap 5, *Presentation*, merupakan tahap presentasi yang meliputi :
      - *Visualisation*, merupakan visualisasi dari proses penyajian data.

2. Identifikasi Tahapan Investigasi Email *Forensics*

   Proses ini digunakan untuk melakukan identifikasi terhadap tahapan-tahapan dalam teknik investigasi email *forensics* sehingga dapat terlihat jelas tujuan dari setiap tahapan-tahapan dari teknik yang telah dikembangkan sebelumnya.

   Menurut Devendran, dkk (2015), mengatakan bahwa penyelidikan terhadap email meliputi 7 tahapan yaitu :

   1. Tahap 1, *Examining sender's email address*, merupakan tahap yang dilakukan untuk memeriksa alamat email pengirim.

2. Tahap 2, *Examining message initiation protocol (HTTP, SMTP),* merupakan proses pemeriksaan pesan inisiasi protokol.
3. Tahap 3, *Examining message ID,* merupakan kegiatan pemeriksaan terhada pesan ID.
4. Tahap 4, *Examining sender's IP address*, merupakan kegiatan pemeriksaan alamat IP pengirim.
5. Tahap 5, *Storage format of email,* merupakan format penyimpanan email yang dapat memungkinkan membaca berbagai jenis format yang bisa dilakukan untuk analisis forensik dengan menggunakan catatan editor dan menerapkan pencarian reguler berbasis ekspresi.
6. Tahap 6, *Availability of backup copy of email*, merupakan salinan cadangan yang tersedia dari email klien. Untuk webmail, salinan selalu disimpan di sisi server.
7. Tahap 7, *Protocol used to transport email*, merupakan protokol yang digunakan untuk mentransport email.

Ilustrasi yang digunakan untuk merangkum visualisasi *framework* dan tahapan untuk investigasi email *forensics* dapat dilihat pada tabel berikut.

Tabel 4. 3 Identifikasi *framework* dan tahapan investigasi email *forensics*

Identifikasi	*Framework* Investigasi	Tahapan Investigasi	Nilai ID
Tahap 1	Tahap *Acquisition* • *Multi-formal email data* • *Hard drive storage*	Tahap *Examining sender's e-mail address,*	1 1.1 1.1.1
Tahap 2	Tahap *Importation* • *Email client* • *Mozilla, Outlook, etc*	Tahap *Examining message initiation protocol (HTTP, SMTP)*	2 2.1 2.1.1
Tahap 3	Tahap *Triage* • *Link analysis* • *ID actors of interest* • *Email extraction tool*	Tahap *Examining message ID*	3 3.1 3.2 3.3
Tahap 4	Tahap *Analysis* • *Structured* data • *Unstructured data* • *Relational analysis*	Tahap *Examining sender's IP address*	4 4.1 4.2 4.2.1
Tahap 5	Tahap *Presentation* ➢ Visualisation	Tahap *Storage format of email*	5 5.1
Tahap 6		Tahap *Availability of backup copy of email*	6
Tahap 7		Tahap *Protocol used to transport email*	7

Berdasarkan penjelasan diatas, maka tahapan proses *analysis* dapat dirangkum berdasarkan tabel berikut.

Tabel 4. 4 Input output pada proses *analysis*

Input		Proses	Output
Framework Investigasi	Analisis Email Forensik		
Tahap *Acquisition* ➢ *Multi-formal email data* ➢ *Hard drive storage*	Tahap *Examining sender's e-mail address,*	*Analysis*	1 1.1 1.1.1
Tahap *Importation* ➢ *Email client* ➢ *Mozilla, Outlook, etc*	Tahap *Examining message initiation protocol (HTTP, SMTP)*		2 2.1 2.1.1
Tahap *Triage* ➢ *Link analysis* ➢ *ID actors of interest* ➢ *Email extraction tool*	Tahap *Examining message ID*		3 3.1 3.2 3.3
Tahap *Analysis* ➢ *Structured* data ➢ *FTK/EnCase* ➢ *Unstructured data* ➢ *Relational analysis*	Tahap *Examining sender's IP address*		4 4.1 4.2 4.2.1
Tahap *Presentation* ➢ *Visualisation*	Tahap *Storage format of email*		5 5.1
	Tahap *Availability of backup copy of email*		6
	Tahap *Protocol used to transport email*		7

4.1.3 *Design*

1. Proses eliminasi *framework* dan tahapan investigasi untuk pengembangan *framework* investigasi email *forensics*

   Eliminasi dilakukan pada tahapan yang memiliki arti yang sama, sedangkan tahapan-tahapan yang tidak tereliminasi akan dijadikan sebagai salah satu tahapan atau sub-tahapan dari *framework* yang akan dibangun. Untuk tahapan yang sama akan diberi *ID* yang sama untuk memudahkan proses evaluasi.

Sebelum melakukan eliminasi data terlebih dahulu dilakukan proses pendefinisian setiap tahapan atau sub-tahapan dari tahapan *framework* dan tahapan investigasi guna menentukan urutan dari setiap tahapan-tahapannya. Berikut adalah tabel ilustrasi dari pendefinisian tahapan – tahapan *framework* investigasi.

Tabel 4. 5 Pendefinisian tahapan *framework* dan tahapan analisis email

Tahapan	Urutan Tahapan dan *Framework* Investigasi	
	Tahapan *Framework*	Analisis Email Forensik
Acquisition	1	
Multi-formal email data	1.1	
Hard drive storage	1.1.1	
Tahap *Importation*	2	
Email client	2.1	
Mozilla, Outlook, etc	2.1.1	
Triage	3	
Link analysis	3.1	
ID actors of interest	3.2	
Email extraction tool	3.3	
Analysis	4	
Structured data	4.1	
FTK/EnCase	4.1.1	
Unstructured data	4.2	
Relational analysis	4.2.1	
Presentation	5	
Visualisation	5.1	
Examining sender's e-mail address,		4.1.1
Examining message initiation protocol (HTTP, SMTP)		4.1.2
Examining message ID		4.1.3
Examining sender's IP address		4.1.4
Storage format of email		1.1.1
Availability of backup copy of email		4.1.5
Protocol used to transport email		4.1.6

Setelah melakukan proses pendefinisian setiap sub proses yang ada, maka tahap selanjutnya adalah melakukan proses eliminasi terhadap model *framework* investigasi email *forensics* berdasarkan urutan tertinggi dengan terminologi yang sama sehingga dapat diketahui tahapan-tahapan yang harus di sempurnakan pada pengembangan *framework* tersebut sehingga menghasilkan sebuah *framework* yang lebih baik dari sebelumnya.

Tabel 4. 6 Identifikasi urutan tertinggi dengan terminologi yang sama

Tahapan	Urutan Tahapan dan *Framework* Investigasi	
	Tahapan *Framework*	Analisis Email Forensik
Acquisition	1	
Multi-formal email data	1.1	
Storage format of email		1.1.1
Hard drive storage	1.1.1	
Tahap *Importation*	2	
Email client	2.1	
Mozilla, Outlook, etc	2.1.1	
Triage	3	
Link analysis	3.1	
ID actors of interest	3.2	
Email extraction tool	3.3	
Analysis	4	
Structured data	4.1	
FTK/EnCase	4.1.1	
Examining sender's e-mail address,		4.1.1
Examining message initiation protocol (HTTP, SMTP)		4.1.2
Examining message ID		4.1.3
Examining sender's IP address		4.1.4
Availability of backup copy of email		4.1.5
Protocol used to transport email		4.1.6
Unstructured data	4.2	
Relational analysis	4.2.1	
Presentation	5	
Visualisation	5.1	

Berdasarkan pendefinisian setiap sub proses yang ada, berdasarkan urutan tertinggi dengan terminologi yang sama masih terdapat kekurangan dalam tahapan investigasi email forensik sehingga membutuhkan tahapan baru.

Tabel 4. 7 Pemberian tahapan baru

Tahapan	Tahapan *Framework*	Analisis Email Forensik	*New Step*
Acquisition	1		
Multi-formal email data	1.1		
Storage format of email		1.1.1	
Hard drive storage	1.1.1		
Importation	2		
Email client	2.1		
Mozilla, Outlook, etc	2.1.1		
Triage	3		
Link analysis	3.1		
ID actors of interest	3.2		
Email extraction tool	3.3		
Analysis	4		
Structured data	4.1		
FTK/EnCase	4.1.1		
Examining sender's e-mail address,		4.1.1	
Examining time message create			4.1.2
Examining message ID		4.1.3	
Examining sender's IP address		4.1.4	
Availability of backup copy of email		4.1.5	
Protocol used to transport email		4.1.6	
Unstructured data	4.2		
Relational analysis	4.2.1		
Presentation	5		
Visualisation	5.1		
Pre-Process			1
Notification			1.1
Autorization			1.2
Preparation			1.3

Lanjutan **Table 4.7** Pemberian tahapan baru

Tahapan	Tahapan *Framework*	Analisis Email Forensik	*New Step*
Proactive			2
Proactive collection			2.1
Obtain a bit-by-bit image of email information			2.2
Securing the Scene			2.3
Reactive			3
Idenfitication			3.1
Analysis			3.2
Examination			3.3
Examination email headers			3.3.1
Analyze email headers			3.3.2
Recovery deleted emails			3.4
Acquire email archives			3.5
Trace email original			3.6
Post-process			4
Returns evidence			4.1
Store evidence			4.2
retrospect			4.3

Berdasarkan tabel 4.7 diatas terdapat empat urutan tahapan baru yang memiliki terminologi yang sama dengan tahapan sebelumnya. Dari tahapan baru tersebut terdapat tahapan yang memiliki urutan teratas sehingga perlu dilakukan perbaikan urutan tahapan berdasarkan tahapan dengan urutan teratas.

Tabel 4. 8 Urutan tahapan yang memiliki tahapan baru

Tahapan	Tahapan *Framework*	Analisis Email Forensik	*New Step*
Pre-Process			1
Notification			1.1
Autorization			1.2
Preparation			1.3
Proactive			2
Proactive collection			2.1

Lanjutan **Tabel 4.8** Urutan tahapan yang memiliki tahapan baru

Tahapan	Tahapan *Framework*	Analisis Email Forensik	*New Step*
Obtain a bit-by-bit image of email information			2.2
Securing the Scene			2.3
Reactive			3
Idenfitication			3.1
Acquisition	3.2		
Multi-formal email data	3.2.1		
Storage format of email		3.2.2	
Hard drive storage	3.2.3		
Analysis	3.4		
Importation	3.5		
Email client	3.5.1		
Mozilla, Outlook, etc	3.5.2		
Triage	3.6		
Link analysis	3.6.1		
ID actors of interest	3.6.2		
Email extraction tool	3.6.3		
Structured data	3.7		
FTK/EnCase	3.7.1		
Examination			3.8
Examining sender's e-mail address,		3.8.1	
Examining time message create			3.8.2
Examining message ID		3.8.3	
Examining sender's IP address		3.8.4	
Availability of backup copy of email		3.8.5	
Protocol used to transport email		3.8.6	
Examination email headers			3.8.7
Analyze email headers			3.8.8
Unstructured data	3.9		
Relational analysis	3.9.1		
Recovery deleted emails			3.10

Lanjutan **Tabel 4.8** Urutan tahapan yang memiliki tahapan baru

Tahapan	Tahapan *Framework*	Analisis Email Forensik	*New Step*
Acquire email archives			3.11
Trace email original			3.12
Presentation	4		
Report & Visualisation	4.1		
Post-process			5
Returns evidence			5.1
Store evidence			5.2
Retrospect			5.3

Setelah melakukan urutan pada tahapan dan sub-tahapan, maka langkah selanjutnya adalah melakukan eliminasi terhadap tahapan dan sub-tahapan yang memiliki terminologi yang sama kemudian dijadikan sebagai satu tahapan atau sub-tahapan baru yang menjadi tahapan atau sub-tahapan utama dalam pengembangan *framework* investigasi email forensik.

Tabel 4. 9 Urutan tahapan yang memiliki tahapan baru

Tahapan	Tahapan *Framework*	Analisis Email Forensik	*New Step*
Pre-Process			1
Notification			1.1
Autorization			1.2
Preparation			1.3
Proactive			2
Proactive collection			2.1
Obtain a bit-by-bit image of email information			2.2
Securing the Scene			2.3
Reactive			3
Idenfitication			3.1
Acquisition			3.2
Multi-formal email data	3.2.1		
Hard drive storage	3.2.2		
Analysis	4		
Acquisition extraction tool			4.1

Lanjutan **Tabel 4.9** Urutan tahapan yang memiliki tahapan baru

Tahapan	Tahapan *Framework*	Analisis Email Forensik	*New Step*
Recovery deleted emails			4.2
Triage	4.3		
Email collection	4.3.1		
Email client	4.3.2		
Email extraction tool	4.3.3		
Examination			5
Structured data	5.1		
ID actors of interest	5.1.1		
Examining sender's e-mail address,		5.1.2	
Examining time message create		5.1.3	
Examining message ID		5.1.4	
Examining sender's IP address		5.1.5	
Protocol used to transport email		5.1.6	
Unstructured data	5.2		
Relational analysis	5.2.1		
Signature data	5.3		
Acquire email archives			5.4
Trace email original			5.5
Presentation	6		
Report & Visualisation	6.1		
Post-process			7
Returns evidence			7.1
Store evidence			7.2
Retrospect			7.3

2. Normalisasi *framework* dan tahapan investigasi

   Pada bagian ini dilakukan proses perbandingan dari *framework* dan tahapan investigasi sebelumnya dengan *framework* investigasi email *forensics* yang telah dikembangkan.

Tabel 4. 10 Perbandingan *framework* dan tahapan investigasi sebelumnya dengan *framework yang* telah dikembangkan

Framework Investigasi	Terdapat pada Pengembangan *Framework* bagian :	Tahapan Investigasi	Terdapat pada Pengembangan *Framework* bagian :
Acquisition ➢ *Multi-formal email data* ➢ *Hard drive storage*	➢ *3.2* ➢ *3.2.1* ➢ *3.2.2*	*Examining sender's e-mail address,*	*5.1.2*
Importation ➢ *Email client* ➢ *Mozilla, Outlook, etc*	➢ *4.1* ➢ *4.3.2* ➢ *4.3.3*	*Examining message initiation protocol (HTTP, SMTP)*	*5.1.3*
Triage ➢ *Link analysis* ➢ *ID actors of interest* ➢ *Email extraction tool*	➢ *4.3* ➢ *4.3.3* ➢ *5.1.1*	*Examining message ID*	*5.1.4*
Analysis ➢ *Structured data* ➢ *Unstructured data* ➢ *Relational analysis*	➢ *4* ➢ *5.1* ➢ *5.2*	*Examining sender's IP address*	*5.1.5*
Presentation ➢ *Visualisation*	➢ *6* ➢ *6.1*	*Storage format of email*	*3.2.2*
		Availability of backup copy of email	*5.4*
		Protocol used to transport email	*5.1.6*

Berdasarkan penjelasan diatas, maka tahapan proses *desain* dapat dirangkum berdasarkan tabel berikut.

Tabel 4. 11 Input output pada proses *design*

Input		Proses	Output	
Tahapan *Framework*	Tahapan Investigasi	*Design*	Tahapan yang Dikembangkan	Urutan Tahapan
Acquisition	*Examining sender's e-mail address,*		*Pre-Process*	1
Multi-formal email data	*Examining message initiation protocol (HTTP, SMTP)*		*Notification*	1.1
Hard drive storage	*Examining message ID*		*Autorization*	1.2
Importation	*Examining sender's IP address*		*Preparation*	1.3
Email client	*Storage format of email*		*Proactive*	2
Mozilla, Outlook, etc	*Availability of backup copy of email*		*Securing the Scene*	2.1
Triage	*Protocol used to transport email*		*Obtain a bit-by-bit image of email information*	2.2
Link analysis			*Proactive collection*	2.3
ID actors of interest			*Reactive*	3
Email extraction tool			*Idenfitication*	3.1
Analysis			*Acquisition*	3.2
Structured data			*Multi-formal email data*	3.2.1
Unstructured data			*Hard drive storage*	3.2.2
Relational analysis				
Presentation			*Analysis*	4
Visualisation			*Acquisition extraction tool*	4.1
			Recovery deleted emails	4.2
			Triage	4.3
			Email collection by client	4.3.1

Lanjutan **Tabel 4.11** Input output pada proses *design*

Input		Proses	Output	
Tahapan *Framework*	Tahapan Investigasi	*Design*	Tahapan yang Dikembangkan	Urutan Tahapan
			Email extraction tool	4.3.2
			Examination	5
			Structured data	5.1
			ID actors of interest	5.1.1
			Examining sender's e-mail address,	5.1.2
			Examining time message create	5.1.3
			Examining message ID	5.1.4
			Examining sender's IP address	5.1.5
			Protocol used to transport email	5.1.6
			Unstructured data	5.2
			Relational analysis	5.2.1
			Signature data	5.3
			Acquire email archives	5.4
			Trace email original	5.5
			Presentation	6
			Report & Visualisation	6.1
			Post-process	7
			Returns evidence	7.1
			Store evidence	7.2
			Retrospect	7.3

4.1.4 *Implementation*

Tahap *implementation* bertujuan untuk membangun konstruksi *framework* berdasarkan tahapan dan sub-tahapan yang telah dikembangkan. Proses konstruksi dari *framework* yang dikembangkan akan dibuat dalam bentuk *state chart diagram* menggunakan program aplikasi *microsoft visio*. Bentuk dari proses pengembangan *framework* akan dibuat secara berurutan berdasarkan tahapan awal dan sub-tahapan awal sampai dengan tahapan akhir

dan subtahapan akhir sehingga dapat membentuk sebuah *framework* jadi yang bisa digunakan untuk melakukan investigasi email *forensics*. Berikut adalah penjelasan secara rinci dari konstruksi tahapan dan sub-tahapan *framework* yang dikembangkan, yaitu :

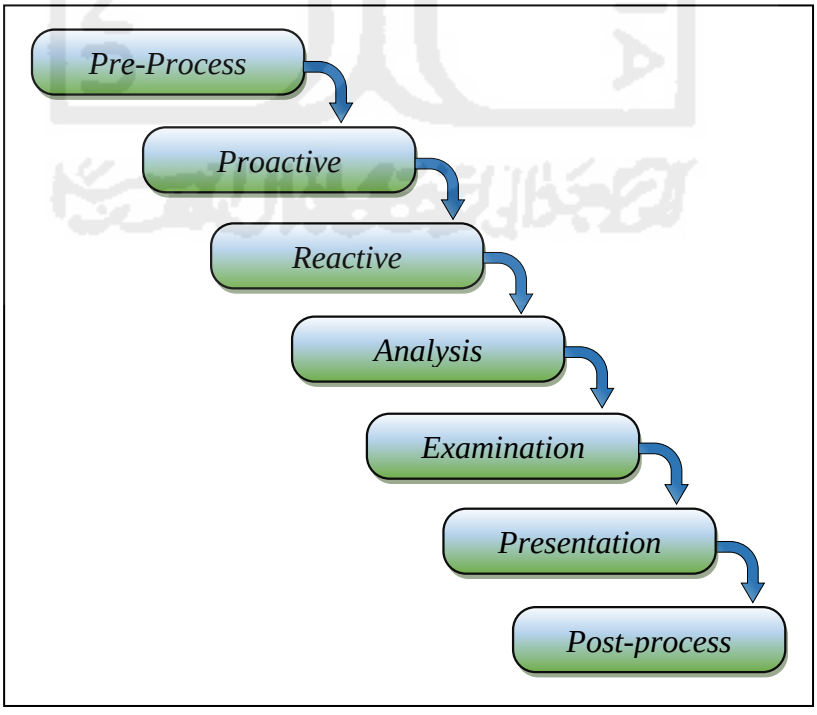
1. *Pre-Process*, meliputi *Notification, Autorization*, dan *Preparation*.
2. *Proactive,* meliputi *Proactive collection, Obtain a bit-by-bit image of email information,* dan *Securing the Scene.*
3. *Reactive* meliputi *Idenfitication,* dan *Acquisition*

   Yang mana pada *Acquisition* terdapat *Multi-formal email data* dan *Hard drive storage*
4. *Analysis,* meliputi *Acquisition extraction tool, Recovery deleted emails,* dan *Triage.*

   Yang mana pada *Triage* terdapat *Email collection by client* dan *Email extraction tool.*
5. *Examination,* meliputi *Structured data, Unstructured data, Signature data, Acquire email archives,* dan *Trace email original*.

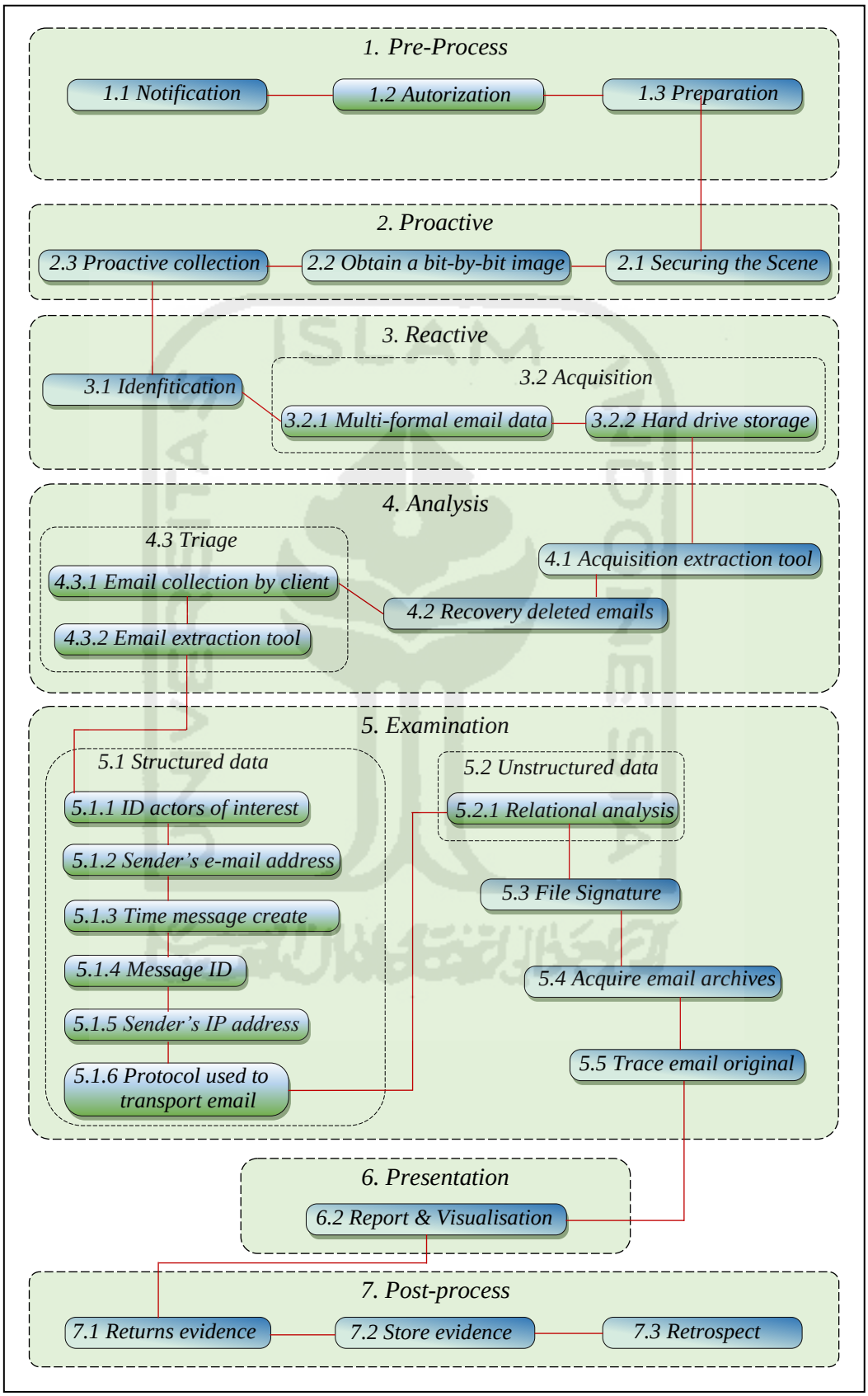
   Yang mana pada *Structured data* terdapat *ID actors of interest, Examining sender's e-mail address, Examining time send message, Examining message ID, Examining sender's IP address*, dan *Protocol used to transport email*. Yang mana pada *Unstructured data* terdapat *Relational analysis*
6. *Presentation*, meliputi *Report & Visualisation*
7. *Post-process,* meliputi *Returns evidence, Store evidence,* dan *Retrospect*

Berdasarkan penjelasan diatas, secara garis besar *framework* ini dibagi menjadi 7 tahapan utama, seperti yang ditujukan pada gambar berikut :



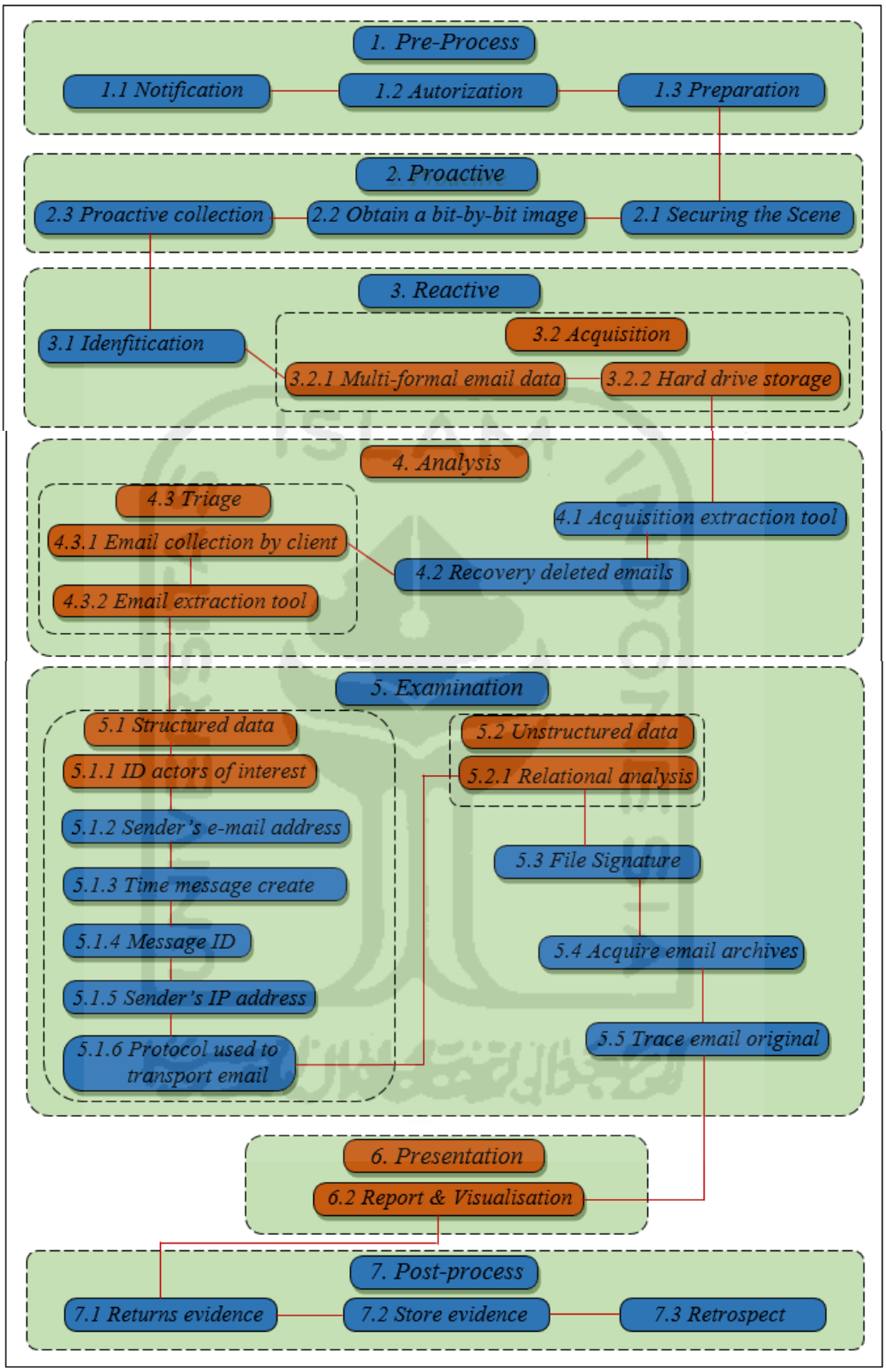
Gambar 4. 2 Tahapan utama *framework* yang dikembangkan

Berikut adalah detail tahapan utama dan sub-tahapan dari *framework* yang telah dikembangkan, seperti gambar berikut :



Gambar 4. 3 Detail *framework* yang telah dikembangkan

➢ Model *Framework* dari tahapan yang telah dikembangkan



Gambar 4. 4 Tahapan baru Framework yang dikembangkan

Tahapan utama *framework*

Tahapan *framework* sebelumnya

Tahapan baru f*ramework* yang dikembangkan

Tabel 4. 12 Detail *framework* yang telah dikembangkan

Tahapan *Framework*	Urutan Tahapan
Pre-Process	1
Notification	1.1
Autorization	1.2
Preparation	1.3
Proactive	2
Securing the Scene	2.1
Obtain a bit-by-bit image of email information	2.2
Proactive collection	2.3
Reactive	3
Idenfitication	3.1
Acquisition	3.2
Multi-formal email data	3.2.1
Hard drive storage	3.2.2
Analysis	4
Acquisition extraction tool	4.1
Recovery deleted emails	4.2
Triage	4.3
Email collection by client	4.3.1
Email extraction tool	4.3.2
Examination	5
Structured data	5.1
ID actors of interest	5.1.1
Examining sender's e-mail address,	5.1.2
Examining time message create	5.1.3
Examining message ID	5.1.4
Examining sender's IP address	5.1.5
Protocol used to transport email	5.1.6
Unstructured data	5.2
Relational analysis	5.2.1
Signature data	5.3
Acquire email archives	5.4
Trace email original	5.5
Presentation	6
Report & Visualisation	6.1
Post-process	7
Returns evidence	7.1
Store evidence	7.2
Retrospect	7.3

Penjelasan dari setiap tahapan dan sub-tahapan *framework* tersebut :

1. *Pre-Process* merupakan tahapan awal yang dilakukan untuk investigasi email forensik. Tahap ini terdapat 3 tahapan yang dilakukan, yaitu :
   1.1 *Notification* merupakan tahap menemukan atau mendapat informasi atau laporan tentang adanya aktivitas kejahatan.
   1.2 *Autorization* merupakan tahap mendapatkan hak untuk melakukan penyelidikan, misalnya setiap proses investigasi harus memiliki surat izin peyelidika, harus memiliki surat izin melakukan penelitian terhadap akun email korban atau tersangka.
   1.3 *Preparation* merupakan tahap untuk menyiapkan segala kebutuhan dalam penyelidikan diantaranya menyiapkan alat dan bahan, personil, dan kebutuhan penyelidikan lainnya.
2. *Proactive* merupakan tahapan yang dilakukan pada tempat kejadian perkara, pada tahapan ini terdapat 3 tahapan yang dilakukan, yaitu :
   2.1 *Proactive collection* merupakan aktivitas yang dilakukan untuk mendapat, menemukan serta mengoleksi barang bukti ditempat kejadian perkara.
   2.2 *Obtain a bit-by-bit image of email information* merupakan tahap untuk mendapatkan informasi email berdasarkan bit per bit yang mencurigakan kemudian disimpan menggunakan metode *hasing*.
   2.3 *Securing the Scene* merupakan tahapan untuk mengamankan tempat kejadian perkara dan melindungi integritas barang bukti.
3. *Reactive* merupakan tahap yang dilakukan selanjutnya setelah barang bukti diamankan, pada tahap ini terdapat 2 tahapan yaitu :
   3.1 *Idenfitication* merupakan tahapan yang dilakukan untuk mengidentifikasi barang bukti yang telah diamankan.
   3.2 *Acquisition* merupakan tahapan untuk melakukan proses akuisisi terhadap barang bukti, pada tahap ini terdapat *Multi-formal email data* yakni tahapan melakukan akuisisi terhadap seluruh email dan *Hard drive storage* yakni media penyimpanan yang digunakan untuk menyimpan hasil akusisi.
4. *Analysis,* pada tahap analisis ini terdapat 3 tahapan yang dilakukan, yaitu :
   4.1 *Acquisition extraction tool* merupakan tahapan untuk melakukan ekstrasi data dari akuisisi sebelumnya dengan menggunakan alat bantu.
   4.2 *Recovery deleted emails* merupakan aktivitas mengembalikan email – email yang telah terhapus.

4.3 *Triage* merupakan aktivitas memilah email, tahap ini meliputi *Email collection by client* yakni aktivitas mengoleksi email berdasarkan klient dan *Email extraction tool* yakni alat bantu yang digunakan untuk mengekstrak email berdasarkan klien email.

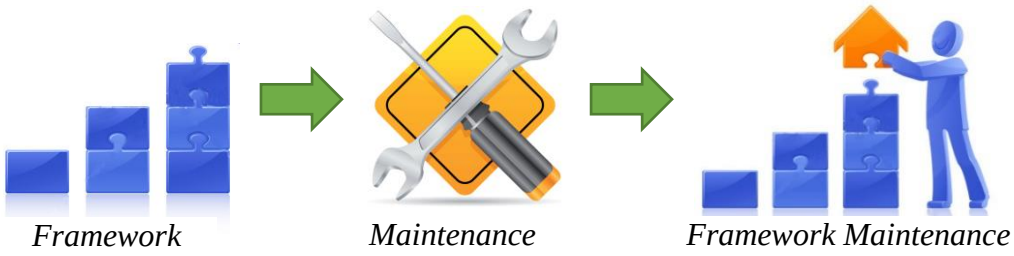
5. *Examination* merupakan tahap pemeriksaan email, pada tahap ini terdapat 5 tahapan yang dilakukan, yaitu :
   5.1 *Structured data* merupakan tahapan pemeriksaan email berdasarkan data terstruktu atau *header*, tahap ini meliputi 6 tahap pemeriksaan, yaitu *ID actors of interest* yakni pemeriksaan identitas pelaku, *Examining sender's e-mail address* yakni aktivitas memeriksa alamat email pengirim, *Examining time message create* yakni memeriksa waktu pesan dibuat, *Examining message ID* yakni memeriksa identitas pesan, *Examining sender's IP address* yakni memeriksa alamat IP pengirim, dan *Protocol used to transport email* yakni memeriksa protokol yang digunakan dalam mentranspor email..
   5.2 *Unstructured data*, merupakan tahapan pemeriksaan email berdasarkan data tidak terstruktu atau *body*, tahap ini meliputi *Relational analysis*
   5.3 *File Signature* merupakan tahap menganalisis *file signature* dari konten email.
   5.4 *Acquire email archives* tahap untuk mendapatkan arsip email.
   5.5 *Trace email original* merupakan tahap untuk melacak keaslian email.
6. *Presentation* merupakan tahap menyajikan hasil, tahap ini meliputi :
   6.1 *Report & Visualisation* merupakan tahapan menyajikan hasil dalam bentuk laporan dan presentasi.
7. *Post*-process merupakan tahap akhir dari proses investigasi, pada tahap ini terdapat 3 tahapan yang dilakukan yaitu :
   7.1 *Returns evidence* merupakan pengembalian barang bukti kepada pemiliknya
   7.2 *Store evidence* merupakan tahap menyimpan barang bukti hasil akuisisi.
   7.3 *Dissemination* merupakan tahap melakukan review pada investigasi yang telah dilaksanakan sebagai perbaikan pada penyelidikan berikutnya.

Tabel 4. 13 Input output pada proses *Implementation*

Input	Proses	Output
Tabel eliminasi dan normalisasi tahapan investigasi seperti yang ditunjukan pada tabel 4.11 sebelumnya.	*Implementation*	*Framework* yang telah dikembangkan seperti ditujukan pada gambar 4.2 dan gambar 4.3 diatas

4.1.5 *Maintenance*

Maintenance atau tahap pemeliharaan dilakukan agar *framework* yang dikembangkan mampu beroperasi secara benar sesuai dengan kebutuhan investigasi email forensik. Berikut adalah ilustrasi pemeliharaan *framework* :



Gambar 4. 5 Ilustrasi pemeliharaan *framework*

Berdasarkan penjelasan diatas, maka tahapan proses *maintenance* dapat dirangkum berdasarkan tabel berikut.

Tabel 4. 14 Input output pada proses *Maintenance*

Input	Proses	Output
Framework yang telah dikembangkan	*Maintenance*	Pemeliharaan/ pengecekan kembali *framework* yang telah dikembangkan

4.2 *Testing Framework*

Pengujian dalam penelitian ini dilakukan dengan 4 tahap yaitu :

4.2.1 Evaluasi *Framework*

Evaluasi dilakukan untuk menentukan perbandingan terhadap *framework* dan tahapan investigasi email *forensics* sebelumnya dengan *framework* investigasi email *forensics* yang telah dikembangkan. Ilustrasi perbandingan *framework* dapat dilihat pada tabel 4.15.

Tabel 4. 15 Perbandingan *framework* dan tahapan forensik email

Framework yang Dikembangkan	Framework Sebelumnya	Analisis Email
Pre-Process		
Notification		
Autorization		
Preparation		
Proactive		
Proactive collection		
Obtain a bit-by-bit image of email information		
Securing the Scene		

Lanjutan **Tabel 4.15** Perbandingan *framework* dan tahapan forensik email

Framework yang Dikembangkan	Framework Sebelumnya	Analisis Email
Reactive		
Idenfitication		
Acquisition	√	
Multi-formal email data	√	
Hard drive storage	√	√
Analysis		
Acquisition extraction tool	√	
Recovery deleted emails		
Triage	√	
Examination		
Structured data	√	
ID actors of interest		
Examining sender's e-mail address,		√
Examining message initiation protocol		√
Examining message ID		√
Examining sender's IP address		√
Protocol used to transport email		√
Unstructured data		
Relational analysis		
Signature data		
Acquire email archives		√
Trace email original		
Presentation		
Report & Visualisation	√	
Post-Process		
Returns evidence		
Store evidence		
Retrospect		

Tanda *ceklist* "√" menunjukan bahwa tahapan sebelumnya memiliki kesamaan dengan tahapan yang telah dikembangkan. Dari tabel diatas dapat dilihat bahwa dalam pengembangan *framework* email forensik terdapat banyak tahapan baru yang dibuat hal tersebut berarti bahwa *framework* sebelumnya masih terdapat kekurangan. Berdasarkan tabel 4.14 diatas menunjukan bahwa *framework* yang dikembangkan memiliki tahapan penanganan investigasi email forensik yang lebih lengkap dibanding sebelumnya.

4.2.2 Ujicoba *Framework*

Ujicoba pada penelitian ini adalah jenis kejahatan *spoofing email*. Hal tersebut dikarenakan banyaknya kasus kejahatan yang berbasis *spoofing email*, salah satu faktor *spoofing email* adalah karena banyaknya situs gratis atau *tools* yang menyediakan *spoofing email* serta kemudahan dalam melakukannya.

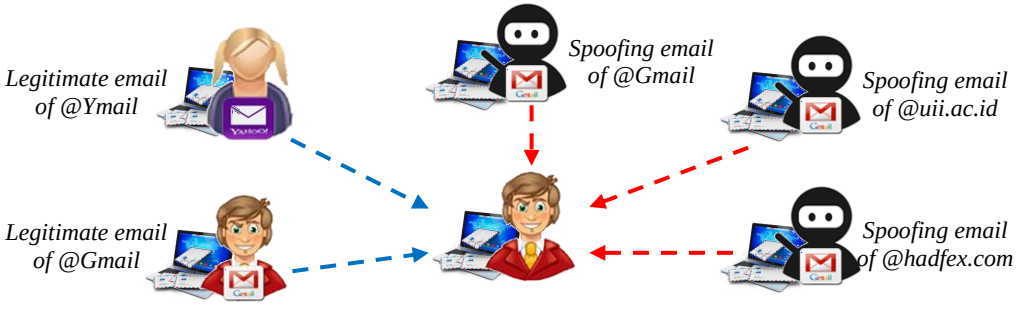
1. Skenario

Skenario dalam penelitian ini akan membahas tentang tahapan – tahapan kejahatan dengan melibatkan transaksi email. Dalam skenario ini terdapat beberapa tahapan yang dilakukan yaitu persiapan *tools*, simulasi dan analisis dengan menggunakan framework yang telah dikembangkan sehingga akan menghasilkan suatu kesimpulan dari hasil analisis tersebut. Berikut penjelasan tahapan skenario :

- Tahapan dimulai dari menyediakan *tools* yang digunakan yaitu koneksi internet, penyediaan perangkat keras dalam penelitian ini digunakan lima buah laptop yang mana pada dua buah laptop digunakan untuk aktivitas kejahatan, duah bual laptop lainnya digunakan untuk mengirim email asli sedangkan laptop yang satunya digunakan sebagai target kejahatan, selanjutnya menyediakan perangkat lunak yaitu *mail client Thunderbird*, penyedia layanan email yaitu *Yahoo* dan *Gmail* kemudian memilih situs-situs penyedia layanan untuk pengiriman *email spoofing*.
- Tahapan selanjutnya adalah simulasi, aktifitas yang dilakukan dalam tahapan ini ialah melakukan instalasi perangkat lunak yang digunakan dan membuat akun atau menggunakan akun yang sudah ada kemudian melakukan pengiriman *legitimate email* kepada target selanjutnya akan dikirim *email spoofing* menyerupai *legitimate email* yang telah dikirimkan sebelumnya.
- Tahap selanjutnya adalah melakukan analisis dengan menggunakan framework yang telah dikembangkan.

2. Simulasi

Berikut adalah ilustrasi dari simulasi kasus ujicoba yang akan dilakukan :

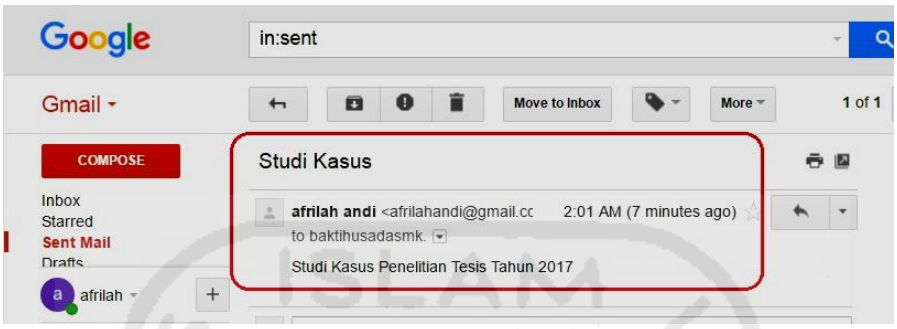


Gambar 4. 6 Ilustrasi simulasi kasus

➢ **Pengiriman Email Sah (*Legitimate Email*)**

Pengiriman email sah dilakukan oleh dua orang dengan menggunakan alamat email asli yang sah. Pengirim tersebut memiliki alamat email yang berbeda yaitu pada email satu menggunakan *gmail* dan yang satunya lagi menggunakan *ymail*.

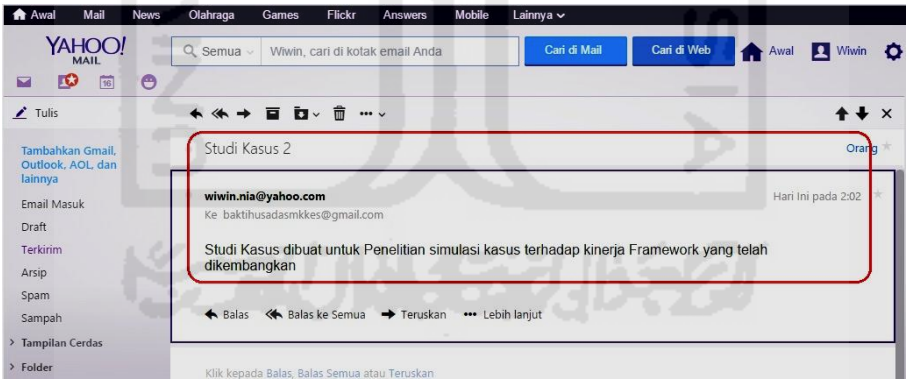
Pengirim pertama menggunakan alamat asli yaitu *"afrilahandi@gmail.com"*,



Gambar 4. 7 ilustrasi pengiriman pesan menggunakan gmail

Gambar 4.7 merupakan ilustrasi dari pengiriman pesan email menggunakan layanan *gmail* yang diberi judul "Studi Kasus" dengan alamat email asli pengirim yaitu *"afrilahandi@gmail.com"* kepada penerimaan pesan dengan alamat *baktihusadasmkkes@gmail.com*

Sedangkan pengirim kedua menggunakan alamat asli yaitu *"wiwin.nia@yahoo.com"*.



Gambar 4. 8 Ilustrasi pengiriman pesan menggunakan Ymail

Gambar 4.8 merupakan ilustrasi dari pengiriman pesan email menggunakan layanan *ymail* yang diberi judul "Studi Kasus 2" dengan alamat email asli pengirim yaitu *"wiwin.nia@yahoo.com"* kepada penerimaan pesan dengan alamat *"baktihusadasmkkes@gmail.com"*.

➢ **Pengiriman *Email Spoofing***

Pengiriman *email spoofing* dilakukan oleh dua orang yang berbeda dengan menggunakan layanan dari situs-situs yang tersedia di internet. Adapun situs *fake mailer* yang digunakan dalam simulasi penelitian ini adalah *www.emkei.cz* dan *www.anonymailer.net*.

Simulasi pertama

Simulasi kedua dilakukan pengiriman email spoofing, proses pengiriman menggunakan alamat email *budi@gmail.com*. Pesan email dikirim pada alamat email *baktihusadasmkkes@gmail.com* melalui situs *www.emkei.cz*. Pengiriman dapat dikatakan berhasil apabila terdapat pesan "*E-mailcsent successfully*" yang berarti bahwa pesan email berhasil dikirim, seperti pada gambar beriktu :

Pengiriman telah berhasil

Pengiriman email spoofing kasus 1

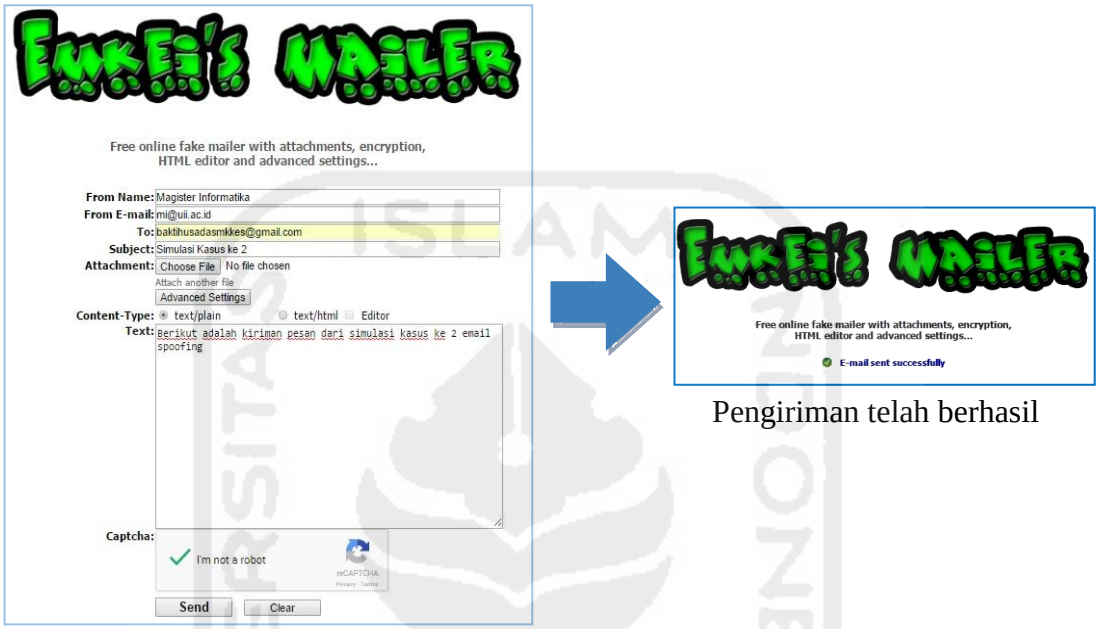
Gambar 4. 9 Ilustrasi kasus 1 pengiriman pesan email spoofing

Gambar 4.9 merupakan ilustrasi pengiriman email *spoofing* kasus 1 menggunakan situs *www.emkei.cz* dengan data sebagai berikut :

- *From Name* : berisi nama pengirim, pada penelitian ini yaitu "Budi".
- *From E-mail* : berisi alamat email pengirim, yaitu *budi@gmail.com.*
- *To* : berisi alamat email penerima, yaitu *baktihusadasmkkes@gmail.com.*
- *Subject* : berisi judul dari pesan, yaitu "Studi Kasus 2"
- *Attachement* : berisi lampiran file yang akan dikirim, pada penelitian ini tidak menyertakan lampiran.
- *Content-Type* : berisi tipe dari konten pesan yang akan digunakan, dalam penelitian menggunakan *content text/plain*.
- *Text* : berisi pesan email dalam bentuk teks, yaitu "Studi Kasus ke 2 menggunakan *emkei.cz.*
- *Captcha* : berisi kode *captcha* yang menandakan anda bukan robot.
- *Send* : merupakan perintah untuk mengirim pesan email *spoofing*.

Simulasi Kedua

Simulasi kedua dilakukan pengiriman email spoofing, proses pengiriman menggunakan alamat email *mi@uii.ac.id*. Pesan email dikirim pada alamat email *baktihusadasmkkes@gmail.com* melalui situs *www.emkei.cz*. Pengiriman dapat dikatakan berhasil apabila terdapat pesan "*E-mailcsent successfully*" yang berarti bahwa pesan email berhasil dikirim, seperti pada gambar beriktu :



Pengiriman email spoofing kasus 2

Pengiriman telah berhasil

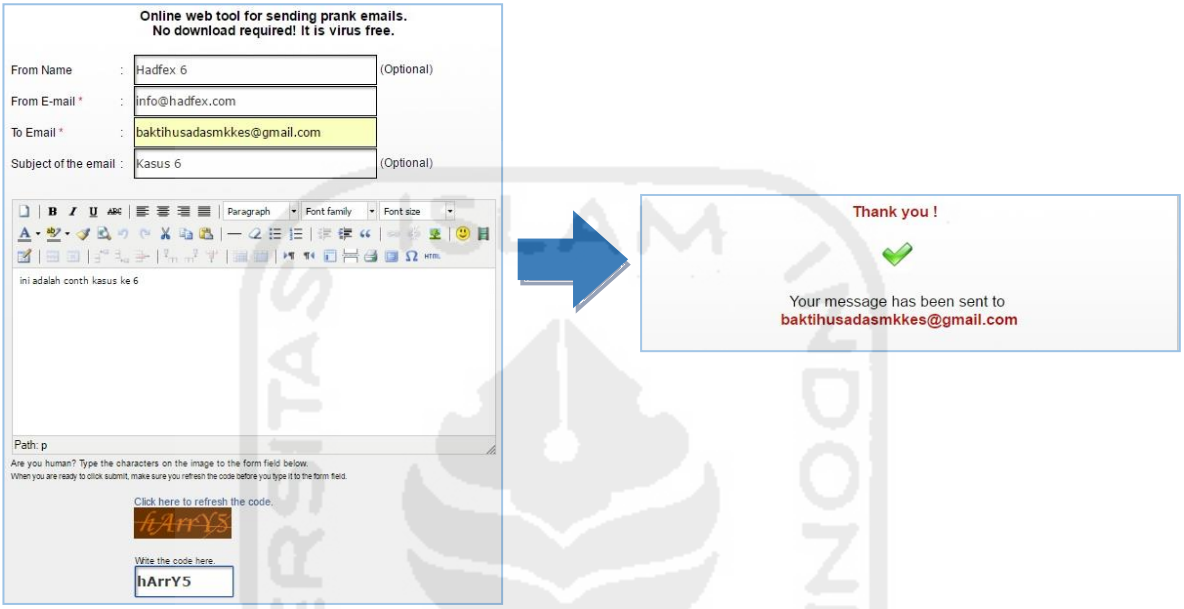
Gambar 4. 10 Ilustrasi kasus 2 pengiriman pesan email spoofing

Gambar 4.10 merupakan ilustrasi pengiriman email *spoofing* kasus 2 menggunakan situs *www.emkei.cz* dengan data sebagai berikut :

- *From Name* : berisi nama pengirim, pada penelitian ini yaitu "Magister Informatika".
- *From E-mail* : berisi alamat email pengirim, yaitu *mi@uii.ac.id.*
- *To* : berisi alamat email penerima, yaitu *baktihusadasmkkes@gmail.com.*
- *Subject* : berisi judul dari pesan, yaitu "Simulasi Kasus ke 2"
- *Attachement* : berisi lampiran file yang akan dikirim, pada penelitian ini tidak menyertakan lampiran.
- *Content-Type* : berisi tipe dari konten pesan yang akan digunakan, dalam penelitian menggunakan *content text/plain.*
- *Text* : berisi pesan email dalam bentuk teks, yaitu "Berikut adalah kiriman pesan dari simulasi kasus ke 2 email spoofing".
- *Captcha* : berisi kode *captcha* yang menandakan anda bukan robot.
- *Send* : merupakan perintah untuk mengirim pesan email *spoofing*.

Simulasi Ketiga

Simulasi kedua dilakukan pengiriman email spoofing, proses pengiriman menggunakan alamat email *info@hadfex.com*. Pesan email dikirim pada alamat email baktihusadasmkkes@gmail.com melalui situs *www.anonymailer.net*. Proses pengiriman dikatakan berhasil apabila terdapat pesan "*Thank you !*" yang berarti bahwa pesan pesan anda telah berhasil dikirim, seperti pada gambar berikut :



Gambar 4. 11 Ilustrasi kasus 3 pengiriman kasus email spoofing

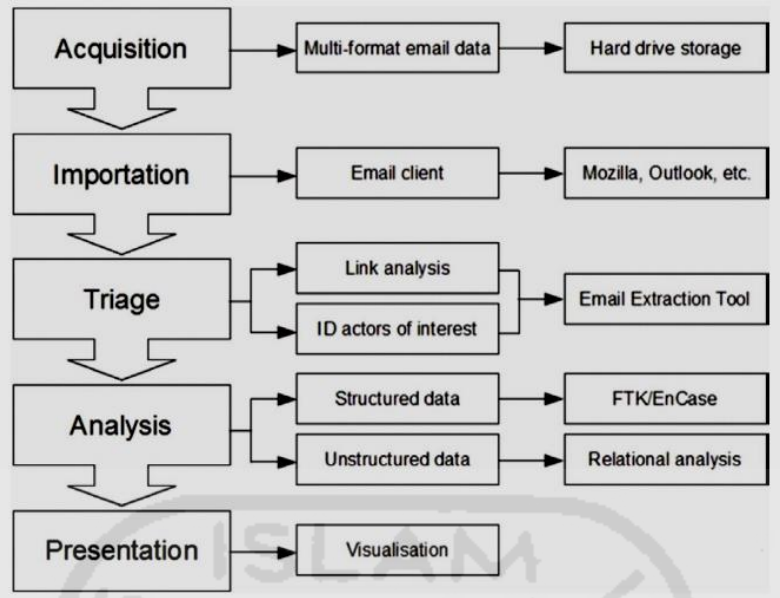
Gambar 4.11 merupakan ilustrasi pengiriman email *spoofing* kasus 3 menggunakan situs *www.anonymailer.net* dengan data sebagai berikut :

- *From Name* : berisi nama pengirim, pada penelitian ini yaitu "Hadfex 6".
- *From E-mail* : berisi alamat email pengirim, yaitu "*info@ hadfex.com*".
- *To Email* : berisi alamat email penerima, yaitu "*baktihusadasmkkes@gmail.com*".
- *Subject of the email* : berisi judul dari pesan, yaitu "Kasus 6"
- *Path* : berisi pesan email, yaitu "ini adalah contoh kasus ke 6"
- *Write the code here* : berisi tulisan kode. Kode pada setiap pesan berbeda-beda.
- *Submit* : merupakan perintah untuk mengirim pesan email *spoofing*.

3. Analisis

Framework Sebelumnya

Penanganan barang bukti terhadap email menggunakan *framework* yang telah dikembangkan sebelumnya. Berikut adalah gambar dari *framework* investigasi forensik email teknik tidak terstruktur yang dikembangkan sebelumnya oleh Haggerty & dkk, (2011) :



Gambar 4. 12 *Framework* sebelumnya

Berikut penjelasan dari *framework* diatas :

Acquisition merupakan akuisisi barang bukti yang ditemukan dan merupakan tahap awal yang dilakukan dalam penangan kasus kejahatan email. Proses akuisisi melibatkan seluruh data email formal kemudian hasilnya disimpan dalam media penyimpanan. Proses tersebut sebaiknya dilakukan setelah olah tempat kejadian perkara guna mengidentifikasi barang bukti yang ditemukan. Olah tempat kejadian perkara merupakan hal penting dalam proses penanganan sebuah kasus guna mencari, menemukan, mengidentifikasi, mengumpulkan dan mengamankan barang bukti. Selain itu juga dalam proses investigasi perlu memiliki izin atau surat perintah penggeledahan yang resmi yang mana dalam surat izin tersebut harus mencakup bahasa yang tepat untuk melakukan pemeriksaan pada komputer dan server email. Selain surat perintah, dalam melakukan aktivitas penanganan barang bukti haruslah menggunakan alat dan bahan yang memiliki izin berdasarkan standar yang telah ditetapkan dalam mekanisme penyelidikan.

Selanjutnya tahap *importation*, merupakan tahap melakukan proses ekstraksi data email berdasarkan *email klien* dengan menggunakan *software email client.*

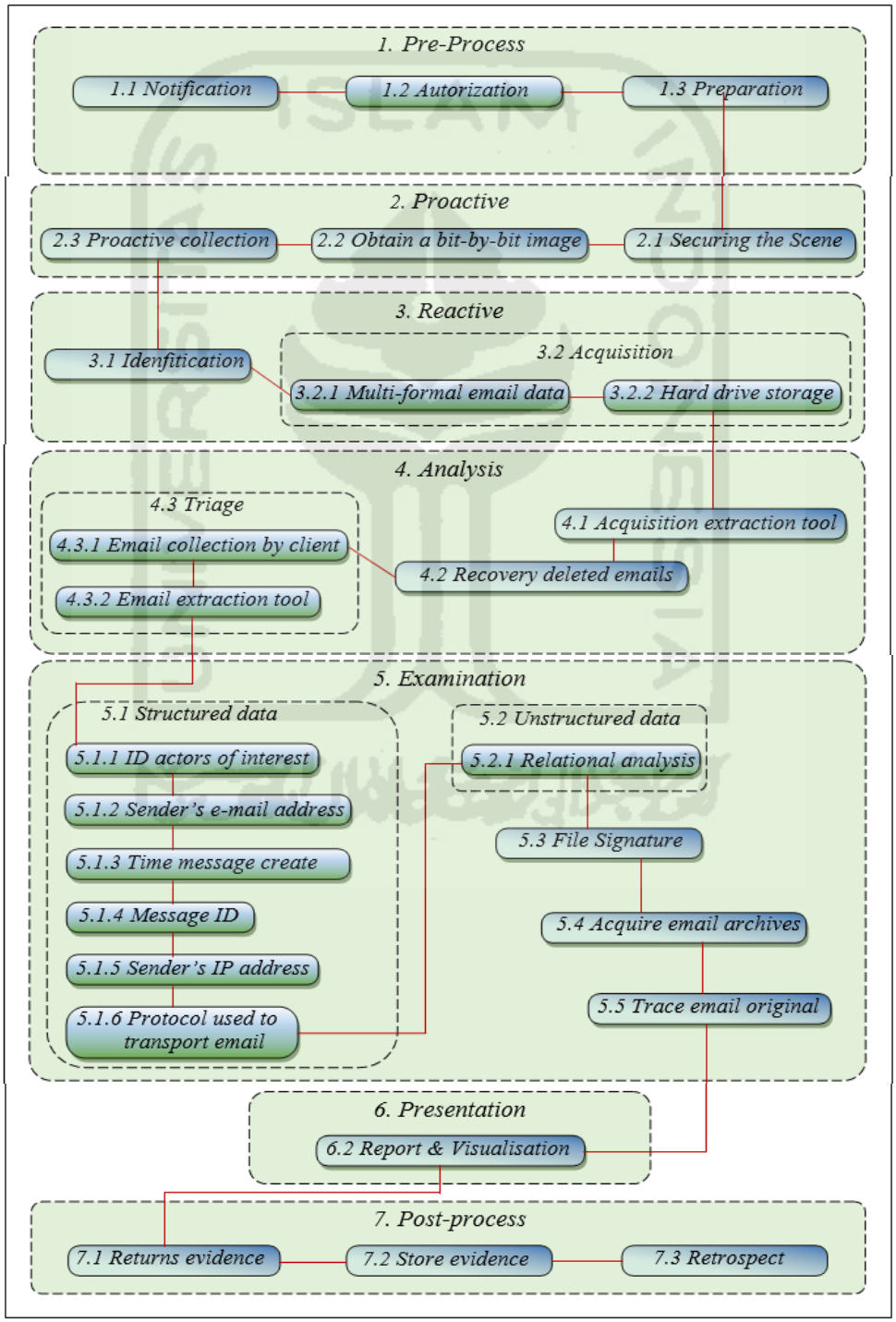
Selanjutnya tahap *triage*, merupakan tahap untuk memilah data email berdasarkan *link analysis* dan identitas pelaku atau pemilik email, proses ini juga dilakukan dengan menggunakan *software email extraction tool*.

Selanjutnya tahap *analysis*, secara umum analisis email forensik difokuskan pada *structured data* dan unstructured data, namun pada framework diatas tidak dijelaskan secara detail bagaiamana proses analisis email dengan *stuctured data*. Hal ini dapat membuat bingung para investigator dalam melakukan analisanya.

Tahap terakhir dari *framework* diatas adalah *presentation* dengan membuat *visualisation* dari hasil analisis. Pada tahap *presentation* seharusnya dilakukan juga dengan pembuatan laporan hasil analisis sebelum dibuatkan visualisasi presentasinya. Selain tahap tersebut sebaiknya dibuat tahap selanjutnya tentang penyimpanan barang bukti dan peninjauan kembali terhadap penelitian yang dilakukan guna penelitian lebih lanjut.

Framework yang Dikembangkan

Penanganan barang bukti terhadap email menggunakan *framework* yang telah dikembangkan.



Gambar 4. 13 *Framework* yang telah dikembangkan

Berikut penjelasan proses penangan investigasi barang bukti email forensik terhadap studi kasus dengan menggunakan *framework* yang telah dikembangkan :

1. *Pre-Process,*

Tahap pertama yang dilakukan adalah *Pre-Process*, pada tahap ini investigator menyiapkan segala sesuatu yang dibutuhkan dalam penyelidikan. Tahap *pre-process* meliputi 3 sub-tahapan, yaitu :

1.1 *Notification*, tahap menyiapkan berkas laporan tentang adanya kasus kejahatan, misalnya menyiapkan laporan pengaduan dan *Form Chain of Custody digital evidence*.

Gambar 4. 14 Ilustrasi *notification*

Laporan pengaduan bertujuan sebagai bahan dasar tentang adanya tindak kejahatan sehingga perlu diadakan investigasi, sedangkan *form chain of custody digital evidence* bertujuan untuk mencatat data personal penyidik sampai dengan data dan konten barang bukti digital yang ditemukan di tempat kejadian perkara dan data lain sesuai mekanisme penyidikan.

1.2 *Autorization*, memiliki hak dalam melakukan proses investigasi secara sah menurut hukum yang berlaku, misalnya memiliki surat perintah penyelidikan dari pihak berwenang. Surat perintah harus sesuai dengan konten penyelidikan yang dilakukan, misalnya penggeledahan dan pengamanan tempat kejadian perkara, menyita barang bukti, melakukan akses atau analisis terhadap barang bukti, dan konten lain yang berhubungan dengan proses investigasi, serta melakukan analisis pada akun email dari barang bukti yang dianalisis.

1.3 *Preparation*, menyiapkan segala kebutuhan dalam proses investigasi diantaranya menyiapkan alat dan bahan, personil, dan kebutuhan penyelidikan lainnya. Alat dan bahan yang digunakan seharusnya dapat diakui atau diijinkan untuk dapat digunakan baik dalam proses awal investigasi sampai dengan tahap akhir investigasi.

2. *Proactive*

Tahap selanjutnya adalah *proactive* yaitu aktivitas yang dilakukan oleh investigasi apabila telah berada di tempat kejadian perkara. Tahap ini meliputi :

2.1 Securing the Scene, invetigator akan mengamankan tempat kejadian perkara seperti memberikan garis Polisi atau *Police line* dan melindungi tempat kejadian perkara dan integritas barang bukti.

2.2 *Obtain a bit-by-bit image*, tahap menyimpan data atau aktivitas yang sedang berlangsung berdasarkan *biy-by-bit* dalam bentuk image dengan menggunakan menggunakan metode *hashing*.

2.3 *Proactive collection*, mengoleksi dan menyita barang bukti yang ditemukan ditempat kejadian perkara. Berikut adalah gambar dari contoh barang bukti yang bisa digunakan untuk transaksi email.

Gambar 4. 15 Contoh barang bukti

Gambar 4. 14 diatas merupakan contoh barang bukti digital yang bisa digunakan sebagai alat transaksi email.

3. *Reactive*

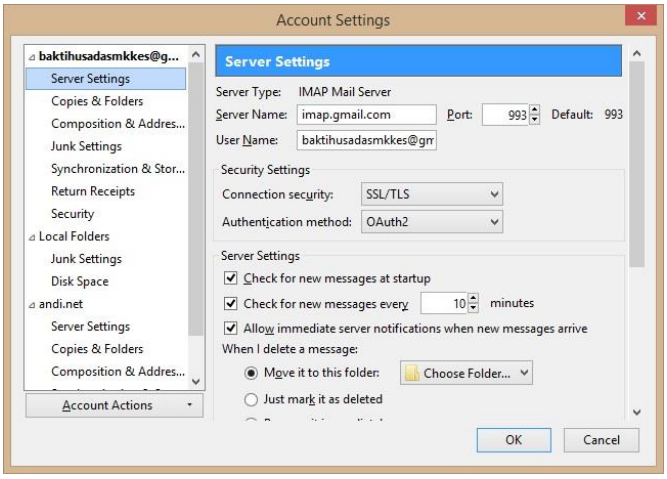
Tahap reactive terdiri dari 2 tahapan, yaitu :

3.1 *Idenfitication*, mengidentifikasi barang bukti yang telah diamankan.

Proses identifikasi dilakukan dengan menentukan barang bukti digital yaitu akun email yang digunakan oleh pelaku terhadap korbannya dalam studi kasus terdapat 2 orang pelaku dengan alamat email yang berbeda. Tahap identifikasi bertujuan untuk menemukan data-data email dari pelaku, dengan menggunakan *email client tools* yaitu *Mozilla Thunderbird* untuk membuat folder khusus terdapat masing – masing email pelaku. Berikut adalah gambar dari pengaturan *email client Mozilla Thunderbird* :

Gambar 4. 16 Persiapan instalasi *Mozilla Thunderbird*

Gambar 4.16 merupakan proses awal dari instalasi *email client Mozilla Thunderbird* yang bertujuan untuk membuat folder dari setiap email client agar dapat dilakukan akuisisi dari setiap akun email.



Gambar 4. 17 Proses pengaturan akun email pada Mozilla Thunderbird

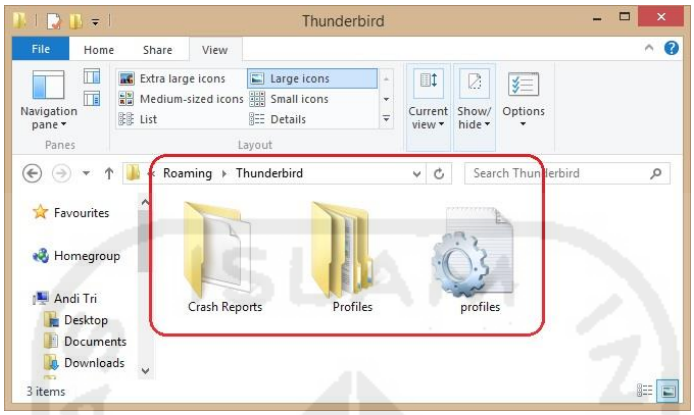
Gambar 4.17 merupakan tahap pengaturan *Mozilla Thunderbird* terhadap akun email yang akan dilakukan akuisisi. Berdasarkan penelitian yang dilakukan bahwa identifikasi yang pertama dilakukan adalah pada akun email target atau korban yaitu *baktihusadasmkkes@gmail.com* menggunakan protokol email yaitu IMAP dengan port 993. Pada *Mozilla Thunderbird* terdapat 2 protokol yang dipilih salah satunya yaitu :

1. POP3 (*Post Office Protocol versi 3*) adalah protokol email standar yang digunakan untuk menerima email dari server jauh ke klien email lokal. POP3 memungkinkan untuk men-download pesan email pada komputer lokal dan membacanya bahkan ketika komputer sedang offline. Secara default, protokol POP3 bekerja pada dua port:
   - *Port 110* adalah port default POP3 yang tidak dienkripsi.
   - *Port 995* adalah port yang memiliki keamanan atau disebut juga *Secure POP3* (SSL-POP).
2. IMAP (*Internet Message Access Protocol*) adalah protokol email yang digunakan untuk mengakses email pada web server jauh dari klien lokal. Secara default, protokol IMAP bekerja pada tiga port:
   - *Port 143* adalah port standar yang tidak dienkripsi.
   - *Port 993* adalah port yang memiliki keamanan atau disebut juga IMAP4 over SSL (IMAPS).
   - *Port 585* adalah port yang memiliki keamanan atau disebut juga *Secure IMAP* (*IMAP4-SSL*).

Pada penelitian yang dilakukan menggunakan protokol IMAP.

3.2 Acquisition, melakukan akuisisi terhadap barang bukti yang telah diamankan dengan menggunakan *hashing*. Tahap ini meliputi 2 tahap, yaitu :

3.2.1 Multi-formal email data, proses akuisisi dilakukan pada seluruh data email yang terdapat pada barang bukti. Tahap akuisisi pada penelitian dilakukan pada akun email target atau korban untuk selanjutnya dianalisis agar dapat menemukan akun email dari pelaku. Proses akuisisi dilakukan pada file *Mozilla Thunderbird* yang telah diinstal. Seperti pada gambar berikut :



Gambar 4. 18 Folder Mozilla Thunderbird

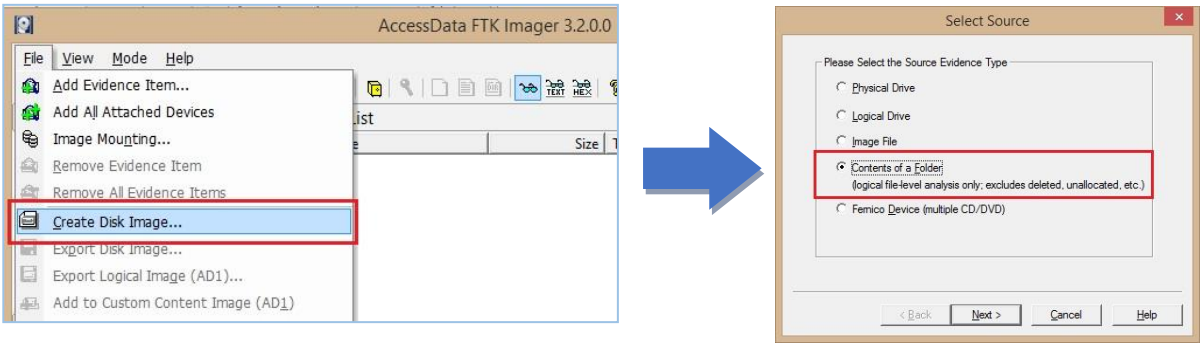
3.2.2 Hard drive storag, menyimpan hasil proses akusisi pada media penyimpanan yang telah disiapkan sebelumnya dan akan digunakan untuk penyelidikan lebih lanjut. Media penyimpanan yang digunakan harus memiliki kapasitas lebih besar dari pada kapasitas barang bukti yang diakuisis.

Ilustrasi akuisisi pada penelitian yang dilakukan menggunakan software *AccessData FTK Imager versi 3.2.0.0. AccessData Forensic ToolKit Imager* atau biasa di sebut "*AD FTK Imager*" merupakan salah satu *tools forensics* yang dikembangkan oleh perusahaan AccessData yang digunakan dalam dunia forensik digital untuk melakukan sistem akuisisi data terhadap barang bukti elektronik dan barang bukti digital. Berikut adalah proses persiapan akuisisi :

Gambar 4. 19 Persiapan awal instalasi AD FTK Imager v 3.2.0.0

Gambar 4.19 merupakan proses awal dari instalasi *AD FTK Imager v 3.2.0.0*. Secara umum *AD FTK Imager* digunakan untuk melakukan akuisisi pada bukti digital (*digital*

evidence) untuk dapat dijadikan sebagai bahan penelitian selanjutnya tanpa harus mengganggu data asli dari bukti digital tersebut.

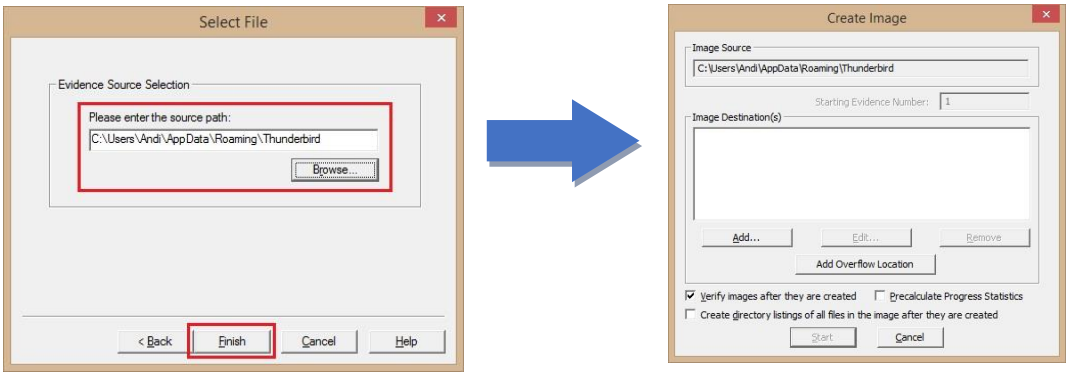


Gambar 4. 20 Ilustrasi *Imaging*

Gambar 4.20 merupakan tahap proses *imaging* pada bukti akun email. Dari gambar tersebut terdapat 5 pilihan sumber yang dipilih, yaitu :

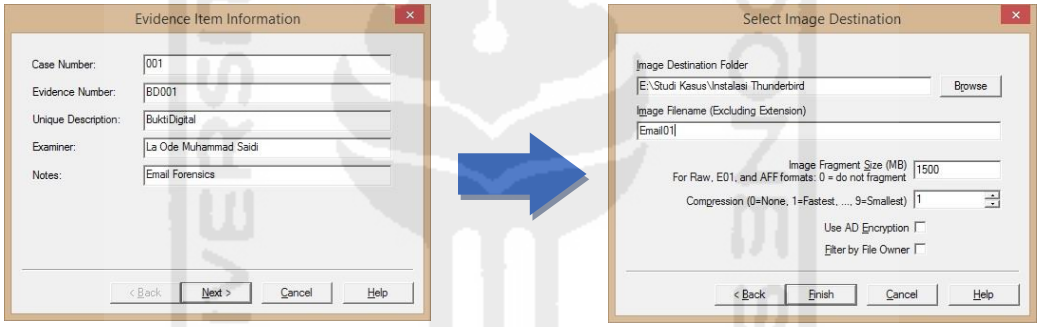
1. *Physical Drive*, perintah ini dipilih apabila sumber berasal dari komponen atau driver fisik misalnya kita akan melakukan akuisisi terhadap *harddisk*, *flashdisk*, dan lain-lain. Akuisisi akan dilakukan pada seluruh data yang terdapat pada *harddisk* dan *flashdisk*.
2. *Logical Drive*, perintah ini dipilih apabila sumber berupa drive logis yang terdapat pada computer, misalnya pada partisi C, D, E, dan lain-lain. Pada sumber ini proses akuisisi hanya akan dilakukan pada partisi tertentu saja, misalnya dalam satu komputer terdapat 3 partisi yaitu partisi C dan partisi D, maka salah satu dari partisi tersebut yang akan diakuisisi sedangkan partisi yang lainnya tidak diakuisisi.
3. *Image File*, perintah ini dipilih apabila sumber merupakan file *cloning* atau kompresi dari suatu drive/folder/CDROM yang menjadi sebuah file *imaging* dengan ekstensiaon ISO, VC4, dan lain-lain.
4. *Contents of a Folder*, perintah ini dipilih apabila sumber berasal dari folder dan file didalamnya termasuk sub folder. Sumber ini biasanya digunakan apabila kita akan melakukan akuisisi hanya pada sebuah folder tertentu saja termasuk semua file yang berada didalamnya.
5. *Fernico Device (Multiple CD/DVD)*, perintah ini dipilih apabila sumber berasal dari banyak CD/DVD. Pada perintah ini dapat dilakukan proses akuisisi pada banyak CD/DVD sekaligus.

Dalam studi kasus penelitian ini dipilih perintah *Contents of a folder*, karena data yang akan diakuisisi hanya pada sebuah folder tertentu saja yaitu folder *Thunderbird* termasuk semua file yang berada didalamnya.



Gambar 4. 21 proses seleksi sumber bukti

Gambar 4.21 merupakan proses seleksi sumber bukti yang akan diakuisisi, pada penelitian ini sumber bukti yang akan diakuisisi adalah *Local Disk (C:) > Users > Andi > AppData > Roaming > Thunderbird*. Setelah menentukan sumber data yang akan diakuisisi maka langkah berikutnya adalah menentukan informasi dari bukti, seperti pada gambar berikut :



Gambar 4. 22 informasi bukti dan menentukan folder penyimpanan akuisisi

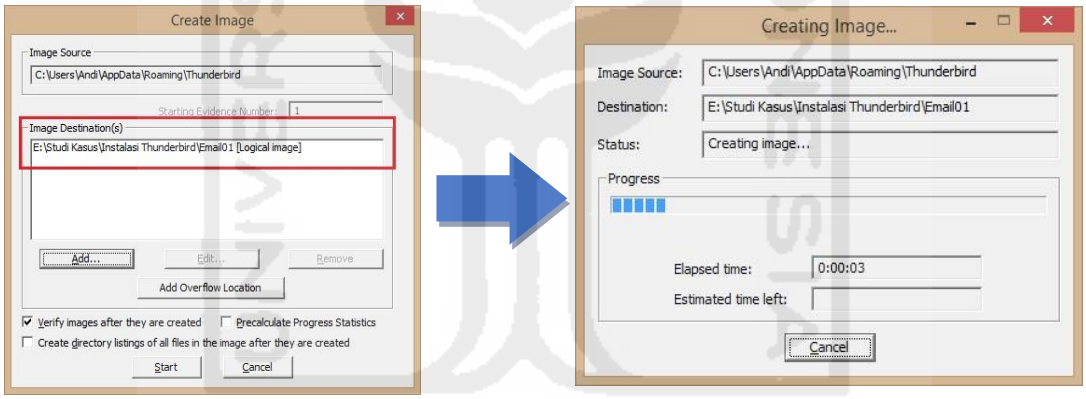
Gambar 4.22 pada bagian pertama merupakan proses pengisian data informasi tentang bukti yang, pada penelitian yang dilakukan informasi bukti adalah :

- *Case Number :* merupakan nomor kasus pada penelitian yaitu 001.
- *Evidence Number :* merupakan nomor bukti pada penelitian yaitu BD001.
- *Unique Description :* merupakan deskripsi unik pada penelitian yaitu BuktiDigital.
- *Examiner :* merupakan pemeriksa barang bukti, pada penelitian adalah La Ode Muhammad Saidi
- *Notes :* merupakan catatan ringkas terhadap barang bukti, pada penelitian ini adalah Email Forensics.
- Sedangkan gambar 4.22 bagian kedua merupakan perintah untuk memilih tempat penyimpanan yang akan digunakan untuk menyimpan hasil akuisisi yang dilakukan. Pada bagian kedua tersebut terdapat beberapa pilihan yaitu :
- *Image Destination Folder :* merupakan folder tempat menyimpan hasil akuisisi, pada perintah ini terdapat perintah *Browse* yang berfungsi untuk menentukan atau memilih

tempat yang digunakan untuk menyimpan hasil akuisisi, pada penelitian ini hasil akuisisi disimpan pada partisi *E:\Studi Kasus\Instalasi Thunderbird*.

- *Image Filename (Excluding Extension) :* merupakan perintah untuk menuliskan nama file dari hasil akuisisi yang dilakukan. Pada penelitian ini nama yang digunakan adalah Email01.
- *Image Fragment Size (MB) :* merupakan perintah untuk menentukan berapa besar ukuran file setiap penggalan atau bagian dengan satuan MB. Ukuran file setiap bagian akan menentukan berapa banyak penggalan hasil akuisisi yang akan dihasilkan, misalnya kita akan melakukan akuisisi pada sebuah *flashdisk* dengan ukuran kapasitas sebesar 6 GB maka *Image Fragment Size* ditentukan lebih besar dari ukuran kapasitas *flashdisk* tersebut yaitu 7000, jika hal tersebut tidak dilakukan makan hasil akuisisi akan terbagi – bagi menjadi 4 file dengan ekstensi *ad1*. Pada penelitian yang dilakukan *Image Fragment Size* yang digunakan adalah 1500 yang merupakan ukuran default dari *AD FTK Imager* dengan ekstensi file *ad1*.

Langkah selanjutnya adalah memulai proses akuisisi, seperti gambar berikut :



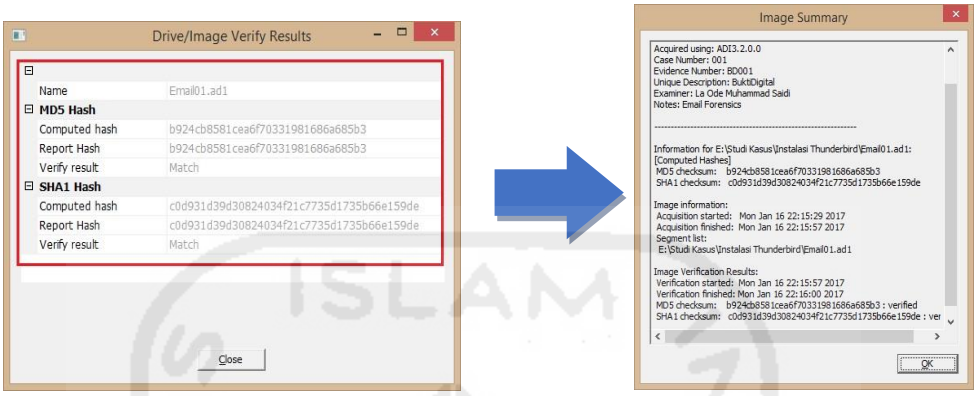
Gambar 4. 23 memulai proses akusisi

Gambar 4.23 bagian kesatu merupakan ilustrasi dari informasi akuisisi, yaitu :

- *Image Source :* merupakan sumber file yang akan diakuisisi. Sumber file pada penelitian ini adalah partisi *C:\Users\Andi\AppData\Roaming\Thunderbird*.
- *Image Destination(s) :* merupakan tempat tujuan atau tempat untuk menyimpan hasil dari akuisisi yang dilakukan. Pada penelitian ini hasil akuisisi disimpan pada partisi *E:\Studi Kasus\Instalasi Thunderbird\Email01*.
- *Add :* merupakan perintah untuk menambahkan sumber folder yang akan diakuisisi seperti pada langkah sebelumnya.
- *Verify images after they are created :* pada penelitian ini dipilih.

Sedangkan gambar 4.23 pada bagian kedua merupakan proses akuisisi sedang berlangsung, pada biasanya proses akuisisi akan memakan waktu yang lama tergantung besarnya ukuran data yang akan diakuisisi.

Langkah selanjutnya adalah melakukan verifikasi terhadap hasil akuisisi. Verifikasi data sangat diperlukan guna menjaga intefritas data.



Gambar 4. 24 proses verifikasi hasil akuisisi

Gambar 4.24 bagian pertama merupakan proses verifikasi hasil akuisisi dari folder yang dilakukan yang bertujuan untuk menjaga integritas data dengan menentukan menggunakan metode *hashing* atau *hash value. Hash value* merupakan nilai unik yang dihasilkan oleh suatu algoritma/perhitungan matematis yang berasal dari suatu file *imaging*, verifikasi *hash value* biasa dilakukan dengan menggunakan *checksum*. Ada beberapa jenis hash yang perlu diketahui yaitu *MD5, SHA-1, SHA-256, SHA-384, SHA-512, RIPEMD-128, TIGER,* dan *PANAMA.* Sedangkan jenis – jenis checksum adalah *CRC16, CRC32,* dan *ADLER32*. Pada penelitian ini *hash* yang digunakan adalah :

MD5 Hash : b924cb8581cea6f70331981686a685b3

SHA1 Hash : c0d931d39d30824034f21c7735d1735b66e159de

MD5 checksum: b924cb8581cea6f70331981686a685b3 : verified

SHA1 checksum: c0d931d39d30824034f21c7735d1735b66e159de : verified

Berikut adalah ilustrasi proses akuisi menggunakan metode *hashing*.

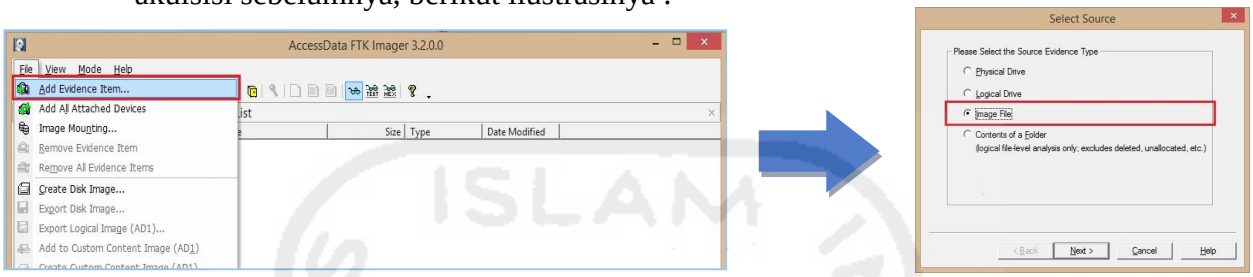
Sumber folder | Akuisisi | Hasil akuisisi dengan metode *hashing*

Gambar 4. 25 Ilustrasi akusisi barang bukti

4. *Analysis*

Berikutnya adalah tahap analisis yang terdiri dari 3 tahapan, yaitu :

4.1 Acquisition extraction tool, melakukan ekstrasi data dari akuisisi sebelumnya dengan menggunakan alat bantu yang direkomendasikan atau mendukung kegiatan analisis. Pada studi kasus penelitian yang dilakukan, *acquisition extraction tool* menggunakan software *AD FTK Imager versi 3.2.0.0* untuk melakukan ekstraksi data dari hasil akuisisi sebelumnya, berikut ilustrasinya :



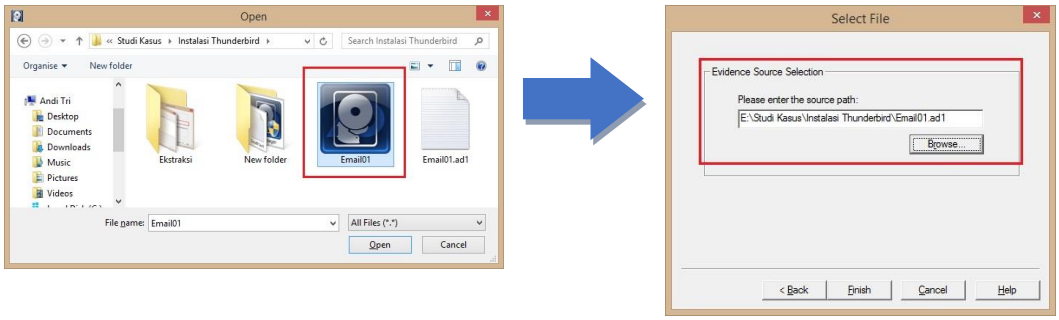
Gambar 4. 26 proses menambah bukti yang akan diekstrak

Pada gambar 4.26 bagian pertama merupakan perintah untuk menambakan item barang bukti yang akan di ekstrak, sedangkan pada bagian kedua merupakan perintah untuk memilih sumber dari barang bukti yang akan diekstrak. Pada perintah *Select Source* terdapat 4 pilihan yaitu :

1. *Physical Drive*, perintah ini dipilih apabila sumber berasal dari komponen atau driver fisik misalnya kita akan melakukan ekstrasi terhadap *harddisk*, *flashdisk,* dan lain-lain. Ekstrasi akan dilakukan pada seluruh data yang terdapat pada *harddisk* dan *flashdisk*.
2. *Logical Drive*, perintah ini dipilih apabila sumber berupa drive logis yang terdapat pada computer, misalnya pada partisi C, D, E, dan lain-lain. Pada perintah ini proses ekstrasi hanya akan dilakukan pada satu partisi saja.
3. *Image File*, perintah ini dipilih apabila sumber merupakan file *cloning* atau kompresi atau *imaging* dari suatu drive/folder/CDROM yang menjadi sebuah file *imaging* dengan ekstensiaon ad1, E01, ISO, VC4, dan lain-lain.
4. *Contents of a Folder*, perintah ini dipilih apabila sumber berasal dari folder dan file didalamnya termasuk sub folder. Sumber ini biasanya digunakan apabila kita akan melakukan ekstraksi hanya pada sebuah folder tertentu saja termasuk semua file yang berada didalamnya.

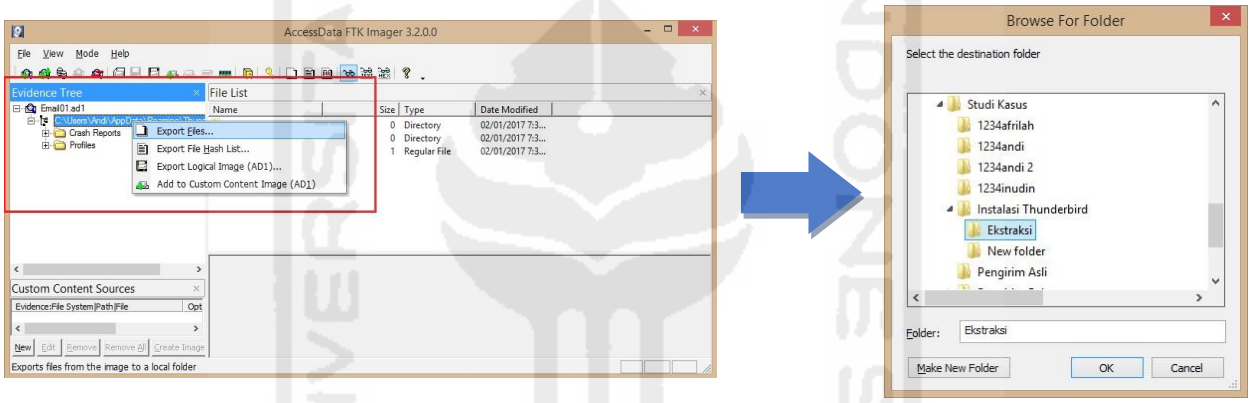
Pada penelitian yang dilakukan diketahui bahwa sumber yang akan diekstrak adalah berupa file *imaging* dengan ekstensi *ad1*, jadi yang menjadi pilihan pada penelitian ini adalah *Image File*.

Langkah selanjutnya adalah menentukan file yang akan diekstrak.



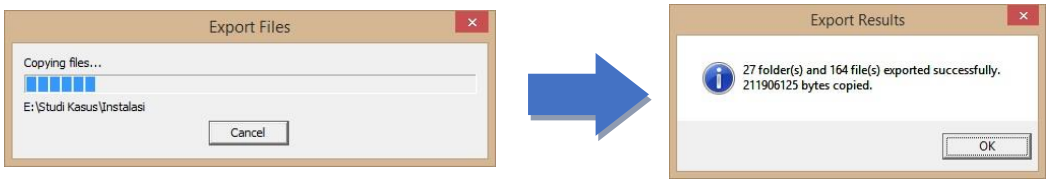
Gambar 4. 27 Proses memilih file bukti yang akan diekstrak

Pada gambar 4.27 merupakan proses memilih sumber file yang akan diekstrak setelah sebelumnya telah dilakukan akuisisi *imaging file*. Pada penelitian ini digunakan data hasil akuisisi sebelumnya yaitu file *imaging* dengan nama file *Email01* dengan ekstensi *ad1*.



Gambar 4. 28 proses ekstrasi bukti

Gambar 2.28 bagian pertama merupakan perintah untuk melakukan ekspor atau ekstrak file dari barang bukti imaging yang telah dipilih sebelumnya. Sedangkan bagian kedua merupakan proses menentukan tempat atau folder dimana hasil ekspor atau ekstrak file akan disimpan. Pada penelitian ini, tempat atau folder penyimpanan hasil ekspor atau ekstrak file adalah pada partisi *E:\Studi Kasus\Instalasi*

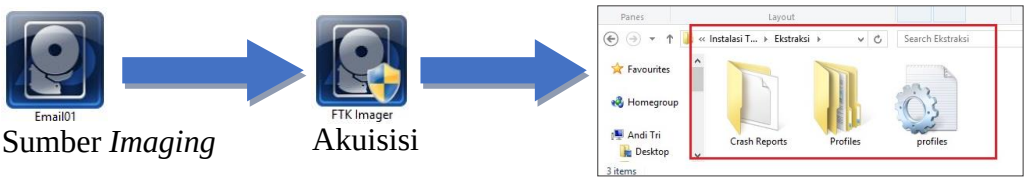


Gambar 4. 29 proses ekstraksi sedang berlangsung

Pada gambar 4.29 bagian pertama merupakan proses ekspor atau ekstrasi file sedang berlangsung, biasanya proses akan membutuhkan waktu berdasarkan besar ukuran suatu file yang akan dieskpor atau diekstrak. Sedangkan bagian kedua merupakan informasi tentang hasil ekspor atau ekstraksi dari file tersebut, berdasarkan

penelitian yang dilakukan diketahui informasi tentang file tersebut adalah terdapat 27 folder dan 164 file dengan jumlah ukuran file adalah 211906125 *bytes*.

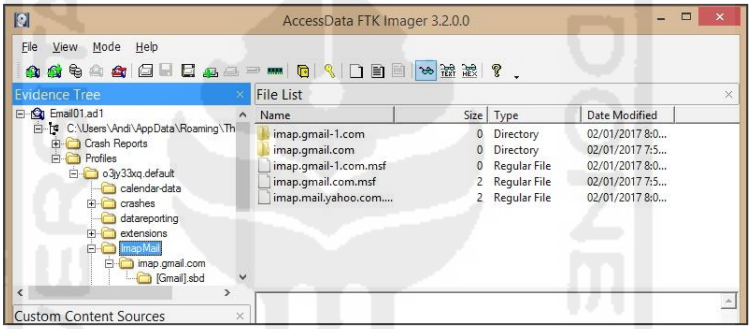
Berikut adalah ilustrasi dari proses ekstrasi file :



Sumber *Imaging* Akuisisi Hasil Ekstraksi

Gambar 4. 30 ilustrasi ekstraksi bukti *imaging*

4.2 *Recovery deleted emails*, melakukan proses *recovery* terdapat data – data email untuk menemukan data atau pesan – pesan email yang terhapus. Tujuan *recovery* adalah untuk menemukan dan mengembalikan data – data email yang terhapus dengan cara diekspor atau diekstrak kembali.



Gambar 4. 31 proses *recovery* data email

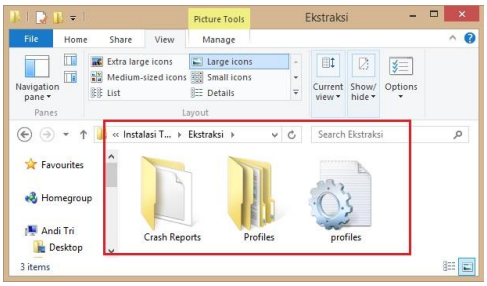
Gambar 4.31 merupakan proses mencari dan menemukan data – data email yang diduga dihapus oleh pemilik akun. Penghapusan data – data email bertujuan untuk menghilangkan bukti kejahatan pelaku. Pada penelitian yang dilakukan, proses *recovery* menggunakan *software AD FTK Imager versi 3.2.0.0*, namun tidak ditemukan data – data email yang terhapus.

4.3 *Triage*, merupakan tahap memilah email berdasarkan *client email* yang selanjutnya akan dilakukan ekstrasi data – data email menggunakan *email extraction tools* , tahap ini terdiri dari 2 tahapan, yaitu :

4.3.1 *Email collection by client*, merupakan tahap mengoleksi email berdasarkan *email client*. Proses koleksi dilakukan dengan cara membuat masing – masing folder berdasarkan *email client*. Pada penelitian yang dilakukan hanya dibuatkan dalam bentuk satu folder.

4.3.2 *Email extraction tool*, tahap selanjutnya adalah melakukan ekstraksi email berdasarkan *email client* dengan menggunakan alat bantu. Proses ekstrasi dapat dilakukan dengan 2 cara yaitu :

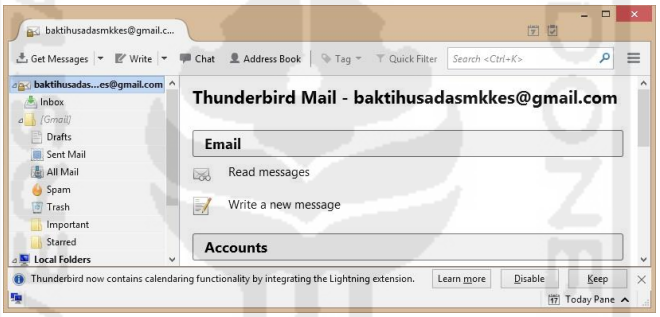
1. Membuka file direktori hasil ekspor dari tahap sebelumya yang telah disimpan pada disk komputer. *E:\Studi Kasus\Instalasi Thunderbird\Ekstraksi*.



Gambar 4. 32 file direktori email dari hasil ekstraksi sebelumnya

2. Membuka data email dengan menggunakan *software email client*.

Pada penelitian yang dilakukan dengan memilih langkah kedua yaitu dengan menggunakan *software email client* yaitu *Mozilla Thunderbird versi 45.6.0* untuk membuka data – data yang terdapat pada akun email.



Gambar 4. 33 Ilustrasi *email extraction*

Gambar 4.33 menunjukan proses ekstraksi email menggunakan salah satu akun email yang menjadi target atau korban kejahatan email. Proses ekstrasi email dengan tujuan untuk menampilkan data – data yang terdapat pada setiap email.

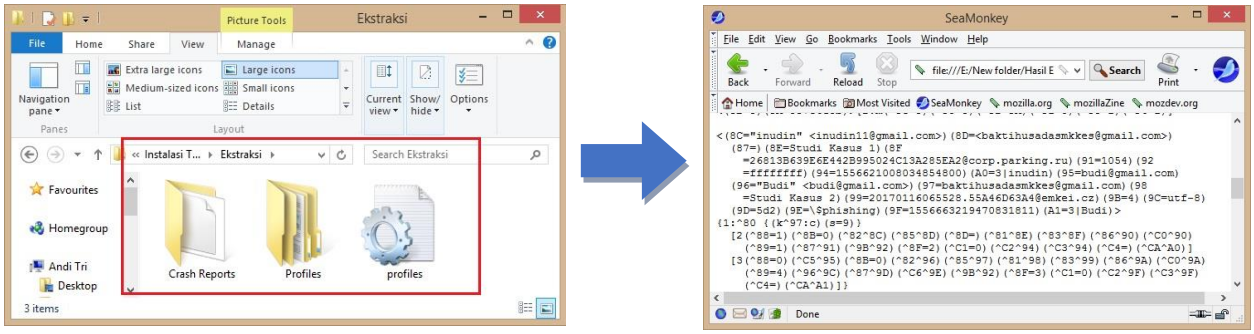
5. *Examination*

Tahap selanjutnya melakukan pemeriksaan email, tahap ini bertujuan untuk mengetahui data – data yang terdapat dari pesan email. Selain itu, pemeriksaan juga dilakukan untuk menentukan apakah pesan yang dikirim berasal dari akun email asli atau palsu. Tahap ini memiliki 5 sub-tahapan yang harus dilakukan, yaitu :

5.1 *Structured data*

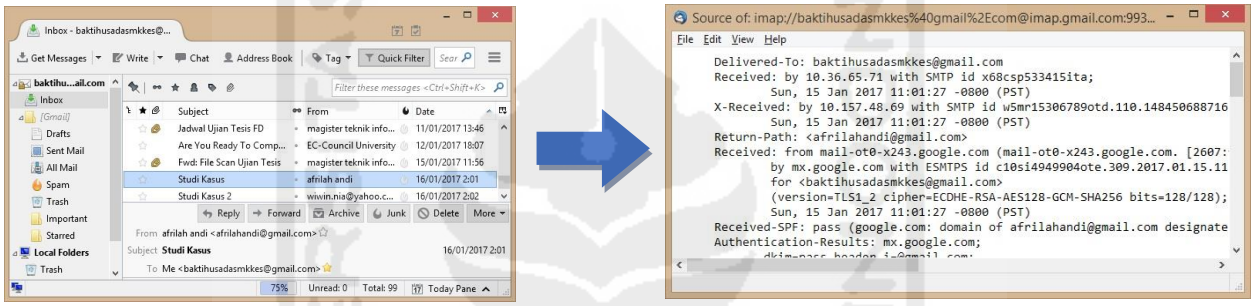
Tahap ini bertujuan untuk melakukan pemeriksaan berdasarkan *structured data* atau *header* pada setiap pesan email. Proses pemeriksaan *header* dapat dilakukan dengan 2 cara yaitu :

1. Membuka file direktori hasil ekspor dari tahap sebelumya yang telah disimpan pada disk komputer. *E:\Studi Kasus\Instalasi Thunderbird\Ekstraksi*, menggunakan *software email ekstraction tools* yaitu *SeaMonkey versi 2.46*.



Gambar 4. 34 Ilustrasi memeriksa identitas pelaku

2. Membuka langsung dengan menggunakan *software email client*. Pada penelitian yang dilakukan dengan memilih langkah kedua yaitu dengan menggunakan *software email client* yaitu *Mozilla Thunderbird versi 45.6.0* untuk membuka data – data yang terdapat pada akun email.

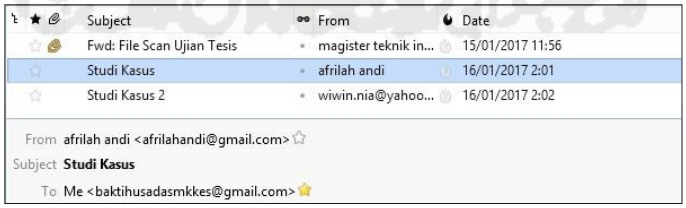


Gambar 4. 35 ilustrasi pemeriksaan *header email*

Tahap *structured data* ini juga terdiri dari 6 sub-tahap pemeriksaan yang harus dilakukan, yaitu :

5.1.1 ID actors of interest, memeriksa identitas pelaku. Berikut adalah ilustrasi identitas pelaku :

1. Konten email dari afrilah andi <afrilahandi@gmail.com> :



Gambar 4. 36 konten ke 1 email sah (*legitimate*)

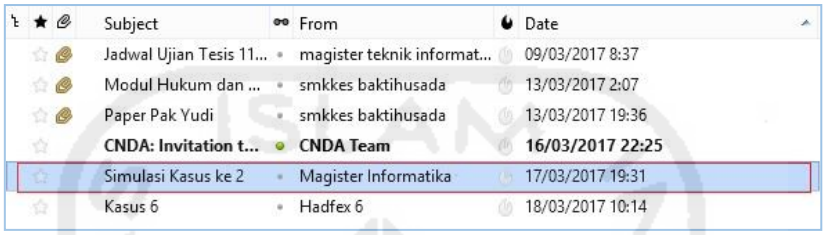
2. Konten email dari wiwin.nia@yahoo.com

Gambar 4. 37 konten ke 2 email sah (*legitimate*)

3. Konten email dari budi@gmail.com

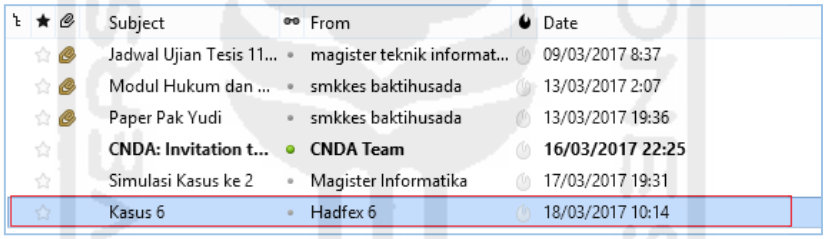
Gambar 4. 38 konten ke *1 email spoofing*

4. Konten email dari mi@uii.ac.id



Gambar 4. 39 konten ke 2 *email spoofing*

5. Konten email dari mi@uii.ac.id

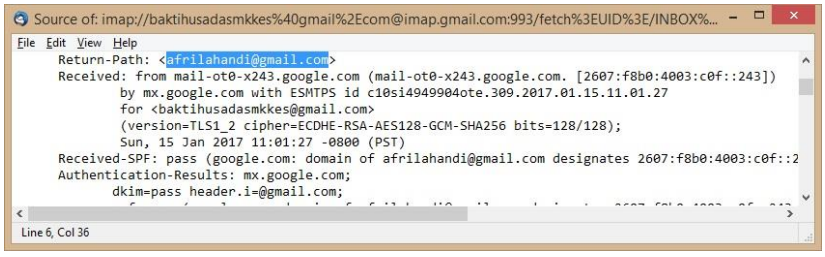


Gambar 4. 40 konten ke 3 *email spoofing*

Gambar 4.36 – 4.40 merupakan penggalan dari pesan email yang menampilkan identitas masing – masing pelaku. Jika dilihat dari konten pesan email dapat dikatakan bahwa semua pesan tersebut merupakan dari orang yang sah, namun masing – masing email berasal dari *mail server* yang berbeda.

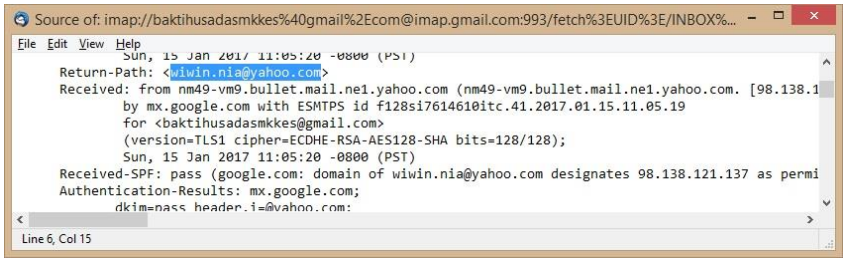
Jika diteliti berdasarkan *Return-Path* dari *header email*, maka akan tampak informasi asal dari masing – masing pengirim email. Berikut adalah *header email* dari masing – masing pesan email yang dikirim :

1. *Header email* yang berasal dari afrilah andi



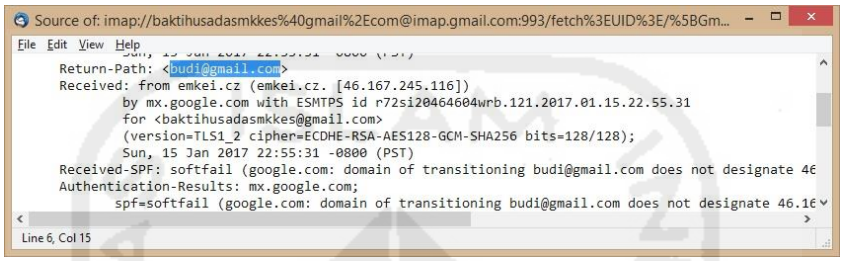
Gambar 4. 41 *Return-Path* ke 1 email sah (*legitimate*)

2. *Email header* yang berasal dari wiwin.nia@yahoo.com



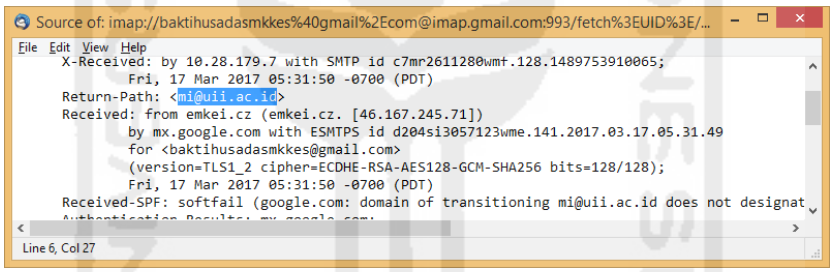
Gambar 4. 42 *Return-Path* ke 2 email sah (*legitimate*)

3. *Email header* yang berasal dari Budi



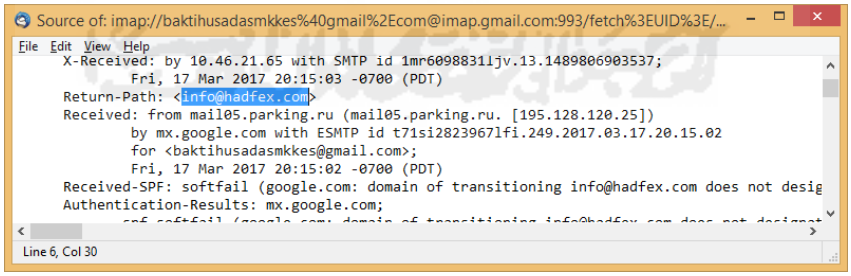
Gambar 4. 43 *Return-Path* ke 1 *email spoofing*

4. *Email header* yang berasal dari Magister Informatika



Gambar 4. 44 *Return-Path* ke 2 *email spoofing*

5. *Email header* yang berasal dari Hadfex



Gambar 4. 45 *Return-Path* ke 3 *email spoofing*

Gambar 4.41 – 4.45 merupakan penggalan dari *header email* yang menampilkan *Return-Path* dari masing – masing pelaku. Jika dilihat dari konten pesan email dan informasi yang terdapat pada *Return-Path* dapat dikatakan bahwa semua pesan tersebut merupakan dari orang yang sah karena memiliki nilai yang sama, namun kesamaan dari nilai masing – masing email tidak dapat menjamin bahwa email tersebut sah (*legitimate*) atau palsu.

Tabel 4. 16 Data konten dari masing – masing email

Subjek	Nama	From	Return-Path	Status
Studi Kasus 1	*afrilah andi*	*afrilahandi@gmail.com*	*afrilahandi@gmail.com*	*Legitimate*
Studi Kasus 2	*wiwin.nia@yahoo.com*	*wiwin.nia@yahoo.com*	*wiwin.nia@yahoo.com*	*Legitimate*
Studi Kasus 1	*Budi*	*budi@gmail.com*	*budi@gmail.com*	*Spoofing*
Studi Kasus 2	*Magister Informatika*	*mi@uii.ac.id*	*mi@uii.ac.id*	*Spoofing*
Studi Kasus 3	*Hadfex 6*	*info@hadfex.com*	*info@hadfex.com*	*Spoofing*

Berdasarkan tabel 4.16 dapat dikatakan bahwa semua pesan email yang dikirim oleh masing – masing email baik email sah (*legitimate*) maupun email palsu (*spoofing*) memiliki nilai yang sama sehingga tidak dapat diketahui apakah email tersebut sah atau tidak. Berikut adalah hasil dari identitas pengirim email :

Tabel 4. 17 Identitas masing – masing email

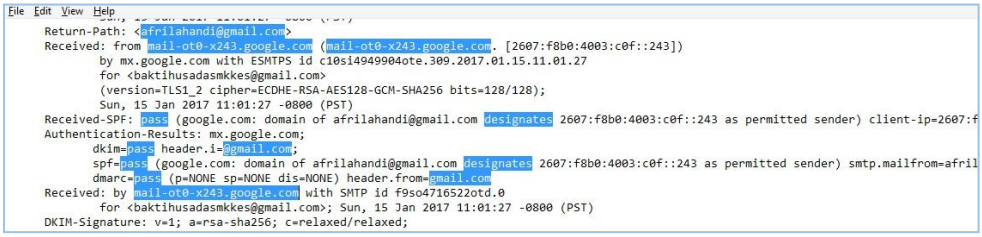
Subjek	Nama
Studi Kasus	*afrilah andi*
Studi Kasus 2	*wiwin.nia@yahoo.com*
Studi Kasus 1	*Budi*
Studi Kasus 2	*Magister Informatika*
Studi Kasus 3	*Hadfex*

Berdasarkan tabel 4.17 bahwa idetitas pesan dapat dijelaskan sebagai berikut :

Pada email sah (*legitimate*) terdapat 2 pesan email yaitu Studi Kasus 1 dengan identitas afrilah andi dan Studi Kasus 2 dengan identitas *wiwin.nia@yahoo.com*, sedangkan pada email palsu (*spoofing*) terdapat 3 pesan email yaitu Studi Kasus 1 dengan identitas *Budi*, Studi Kasus 2 dengan identitas Magister Informatika, dan Studi Kasus 3 dengan identitas Hadfex.

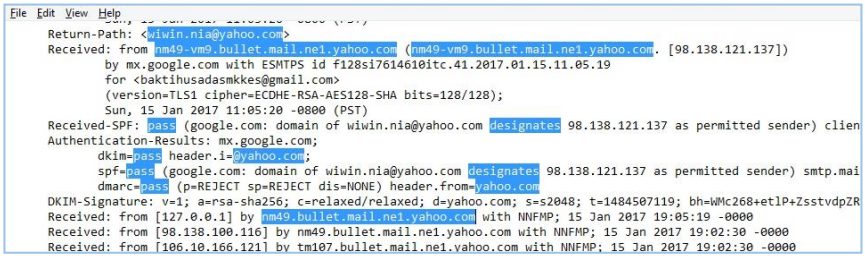
5.1.2 Examining sender's e-mail address, tahap memeriksa alamat email pengirim. Berikut adalah ilustrasi pemeriksaan terhadap alamat email pengirim dilihat berdasarkan *header email* :

1. *Email header* sah dari Studi Kasus 1



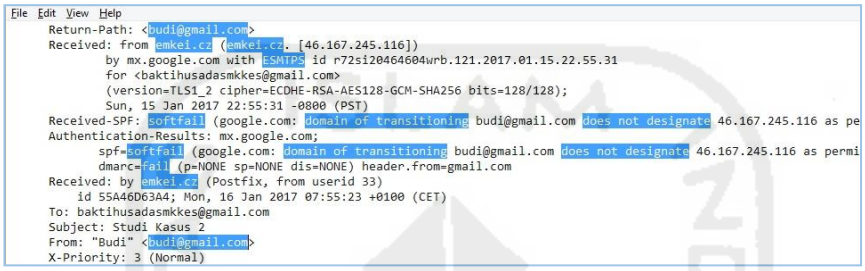
Gambar 4. 46 Ilustrasi memeriksa alamat email sah ke 1

2. *Email header* sah dari Studi Kasus 2



Gambar 4. 47 Ilustrasi memeriksa alamat email sah ke 2

3. *Email header spoofing* dari Studi Kasus 1



Gambar 4. 48 ilustrasi memeriksa alamat email *spoofing* ke 1

4. *Email header spoofing* dari Studi Kasus 2

Gambar 4. 49 ilustrasi memeriksa alamat email *spoofing* ke 2

5. *Email header spoofing* dari Studi Kasusu 3

Gambar 4. 50 ilustrasi memeriksa alamat email *spoofing* ke 3

Gambar 4.46 – 4.50 merupakan penggalan dari *header email* yang menampilkan alamat email masing – masing pengirim. Jika dilihat dari *Return-Path* dan *From* dari masing–masing pesan email dapat dikatakan bahwa semua alamat email pengirim merupakan dari alamat email yang sah, namun jika diteliti berdasarkan beberapa header mail

maka akan terlihat beberapa perbedaan informasi dari masing – masing alamat email.

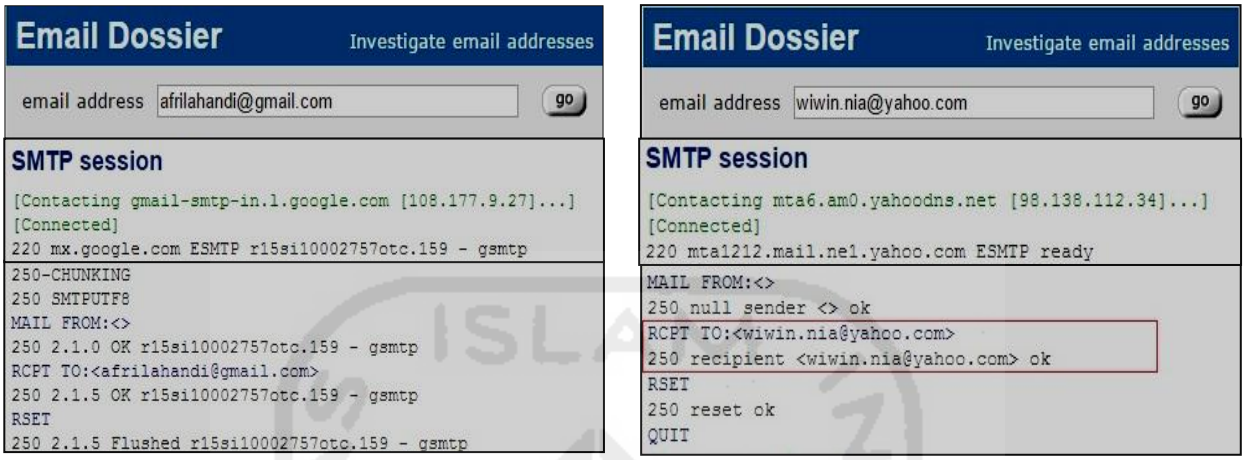
Tabel 4. 18 Informasi alamat email pengirim

From	*Return-Path*	*Received from*	*Received-SPF*	*Autentication*				*Received by*	*Error-To*	*Reply-To*	*Status*
				dkim	*spf*	*dmarc*	*header*				
afrilahandi@gmail.com	*afrilahandi@gmail.com*	*mail.google.com*	*pass, designates*	*pass*	*pass, designates*	*pass*	*gmail.com*	*Mail.google.com*			*legitimate*
wiwin.nia@yahoo.com	*wiwin.nia@yahoo.com*	*mail.yahoo.com*	*pass, designates*	*pass*	*pass, designates*	*pass*	*yahoo.com*	*mail.yahoo.com*			*legitimate*
budi@gmail.com	*budi@gmail.com*	*emkei.cz*	*softfail, transitioning, not designate*	*-*	*softfail, transitioning, not designate*	*fail*	*gmail.com*	*emkei.cz*			*spoofing*
mi@uii.ac.id	*mi@uii.ac.id*	*emkei.cz*	*softfail, transitioning, not designate*	*-*	*softfail, transitioning, not designate*	*-*	*-*	*emkei.cz*	*mi@uii.ac.id*	*mi@uii.ac.id*	*spoofing*
info@hadfex.com	*info@hadfex.com*	*mail05.parking.ru*	*softfail, transitioning, not designate*	*-*	*softfail, transitioning, not designate*	*-*	*-*	*Web38 by mail05.parking.ru*	*-*	*-*	*spoofing*

Berdasarkan tabel 4.18 terdapat beberapa perbedaan antara alamat email *legitimate* dan *spoofing* yaitu :

Received from dan *Received by*, informasi yang terdapat pada alamat email *ligitamate* adalah *mail.google.com* dan *mail.yahoo.com* yang merupakan provider dari email sah, sedangkan pada alamat email *spoofing* adalah *mail05.parking.ru* dan *emkei.cz* merupakan layanan untuk mengirim email *spoofing*. Selain itu juga terdapat informasi *Received-SPF* dan *Autentification spf* pada alamat email *legitimate* adalah *pass* dan *designates*, sedangkan pada alamat email *spoofing* adalah *softfail, transitioning,* dan *not designates* serta pada alamat email spoofing tidak terdapat informasi *Autentucation dkim*. Selain itu juga sebagian email *spoofing* memiliki pesan *Error-To* dan *Reply-To* misalnya pada kasus alamat email mi@uii.ac.id yang berarti bahwa terdapat kesalahan email.

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 email *afrilahandi@gmail.com* dan *wiwin.nia@yahoo.com* menggunakan *email dossier* :

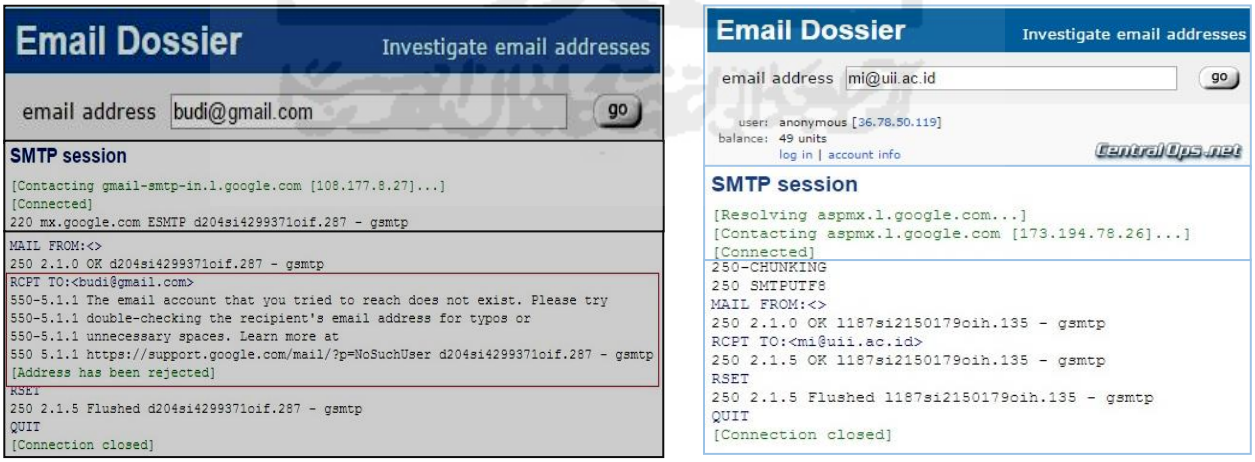


Pengecekan validasi *afrilahandi@gmail.com* Pengecekan validasi *wiwin.nia@yahoo.com*

Gambar 4. 51 pengecekan validasi email sah

Pada gambar 4.51 menjelaskan bahwa email dengan alamat *afrilahandi@gmail.com* dan *wiwin.nia@yahoo.com* merupakan alamat email sah yang dibuktikan dengan penyataan dari *RCPT TO* (recipient) adalah *ok* dengan kode 250 yang berarti alamat email tersebut adalah sah dan dapat diterima. Menandakan bahwa email tersebut telah dibuat atau pernah dibuat.

Selanjutnya dilakukan pengecekan validasi pada alamat email *budi@gmail.com*, *mi@uii.ac.id*, dan *info@hadfex.com* menggunakan *email dossier* :



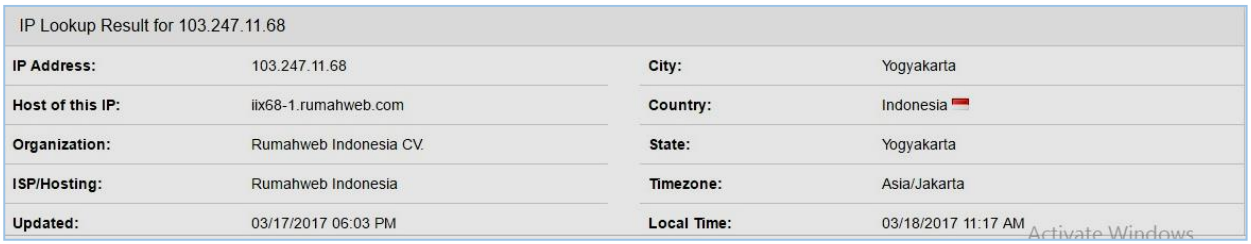
Pengecekan validasi *budi@gmail.com* Pengecekan validasi *mi@uii.ac.id*

Gambar 4. 52 pengecekan validasi email *spoofing*

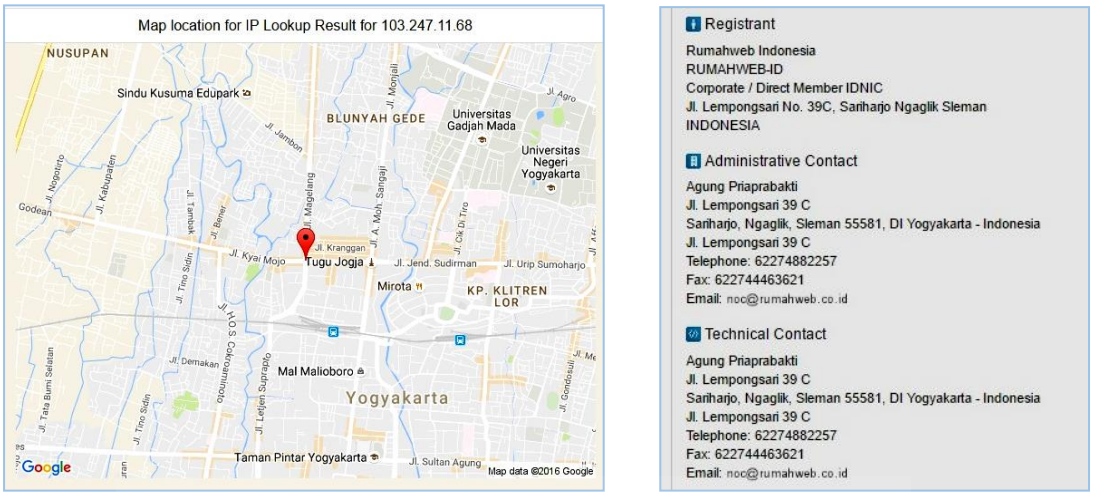
Pengecekan validasi email *info@hadfex.com*

Gambar 4. 53 pengecekan validasi email *spoofing*

Pada gambar 4.52 dan 4.53 menjelaskan bahwa email dengan alamat *budi@gmail.com* tersebut tidak sah hal tersebut dibuktikan dengan informasi pada *RCPT TO: the email account that you tried to reach does not exist*, kode 550 yang berarti bahwa server gagal memeriksa alamat email dengan kata lain bahwa alamat email tersebut tidak ada atau belum pernah dibuat sebelumnya. Sedangkan email dengan alamat *mi@uii.ac.id* tersebut menjelaskan bahwa alamat email tersebut sah yang dibuktikan dengan penyataan dari *RCPT TO* (recipient) adalah *ok* dengan kode 250 yang berarti alamat email tersebut adalah sah dan dapat diterima. Selanjutnya pada email dengan alamat *info@hadfex.com* menjelaskan bahwa tidak terdapat informasi yang menjelaskan tentang legalitas dari email tersebut, namun pada informasi *SMTP session* terdapat alamat *IP address* dari email tersebut yaitu 103.247.11.68, IP tersebut dapat digunakan untuk mengecek legalitas dari email tersebut. Pengecekan legalitas email berdasarkan *IP address* dilakukan menggunakan situs *http://ipaddress.com/*, berikut adalah ilustrasi hasil dari pengecekan *IP address* dari email *info@hadfex.com*.



Gambar 4. 54 Pengecekan *IP address*



Gambar 4. 55 Pengecekan *IP address*

Gambar 4.54 dan 4.55 merupakan hasil dari pengecekan IP address dari alamat email *info@hadfex.com* menggunakan situs *http://ipaddress.com/*, berdasarkan hasil tersebut dapat dipastikan bahwa alamat email *info@hadfex.com* merupakan alamat email yang sah atau pernah dibuat hal tersebut dibuktikan dengan organisasi yang digunakan adalah Rumahweb Indonesia CV merupakan salah satu penyedia domain di kota Yogykarta.

Tabel 4. 19 Pemeriksaan alamat email

Alamat Email	Kode Pemeriksaan	Informasi Pemeriksaan	Status
afrilahandi@gmail.com	*250*	*ok*	*legitimate*
wiwin.nia@yahoo.com	*250*	*ok*	*legitimate*
budi@gmail.com	*550*	*does not exist*	*spoofing*
mi@uii.ac.id	*250*	*ok*	*spoofing*
info@hadfex.com	-	*Timed Out*	*spoofing*

Tabel 4.19 merupakan hasil pemeriksaan email. Berdasarkan hasil penelitian tersebut dapat disimpulkan bahwa alamat email dengan kode 250 dan informasi pemeriksaan adalah *ok* menandakan bahwa email tersebut pernah atau telah dibuat. Sedangkan alamat email dengan kode 550 dan informasi *does not exist* menandakan bahwa email tersebut belum pernah dibuat, sedangkan untuk alamat email yang tidak menampilkan kode pemeriksaan menandakan email tersebut harus diselidiki lagi berdasarkan *IP address* yang ditampilkan untuk menemukan legalitas email tersebut. Berikut adalah beberapa kode respon server SMTP dari pemeriksaan email berdasarkan penelitian studi kasus yang dilakukan :

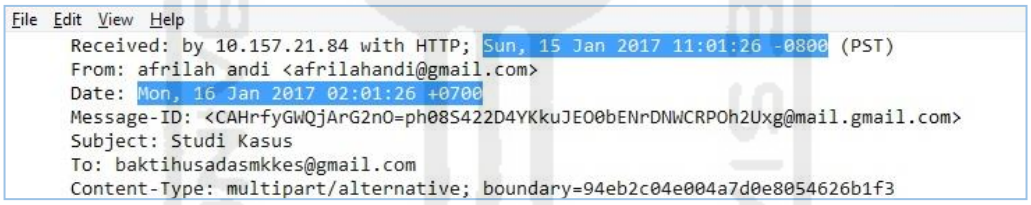
1. Server siap, kode 220 merupakan pesan selamat datang yang berarti server *email dossier* dapat bekerja dengan baik

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 tersediah (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.

5.1.3 Examining time message create, memeriksa waktu kapan pesan dibuat,

Berikut adalah ilustrasi pemeriksaan terhadap waktu kapan pesan dibuat berdasarkan *header email* :

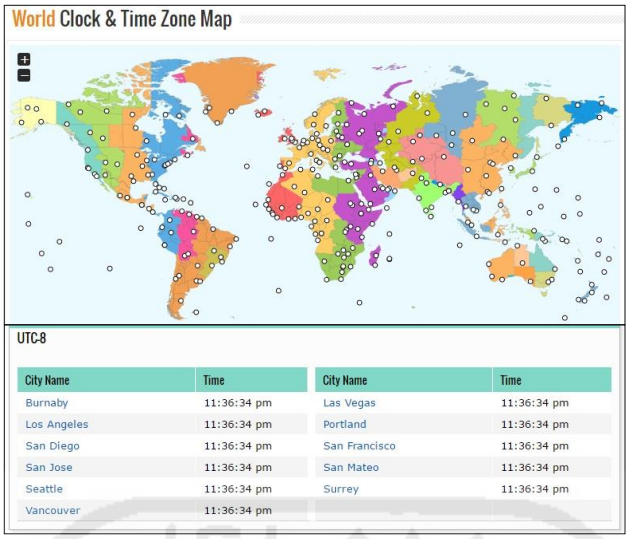
1. Waktu yang berasal dari *Header email* sah Studi Kasus 1:



Gambar 4. 56 Ilustrasi memeriksa waktu pesan dibuat

Gambar 4.50 menjelaskan bahwa pesan email dikirim dengan menggunakan 2 waktu yang berbeda yaitu :

1. Waktu berdasarkan protokol pemrosesan email yaitu *HTTP; Sun, 15 Jan 2017 11:01:26 -0800*. HTTP merupakan protokol yang digunakan oleh *web browser* saat pengiriman pesan email, *Sun, 15 Jan 2017* merupakan hari, tanggal, bulan, dan tahun pesan email dikirim, 11:01:26 adalah waktu/jam pengiriman emai, sedangkan -0800 adalah koordinat waktu atau *time zone* untuk mengirim email. Untuk mengetahui informasi dari waktu tersebut maka dilakukan pengelidikan lebih lanjut agar dapat dipastikan secara benar darimana asal waktu tersebut. Berikut adalah ilustrasi pengecekan time zone menggunakan situs *http://localtimes.info*.



Gambar 4. 57 kota di dunia dengan *time zone -0800*

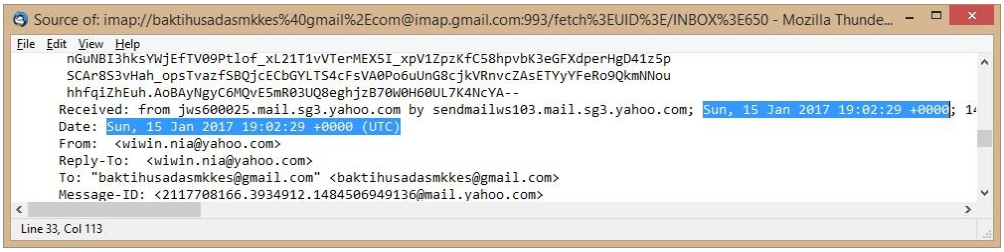
Gambar 4.57 merupakan ilustrasi beberapa kota di dunia yang menggunakan *time zone -0800*.

2. Waktu berdasarkan lokasi pengiriman email yaitu *Mon, 16 Jan 2017 02:01:26 +0700*. *+0700* merupakan *Email Time Zone Indicator* waktu atau *time zone* yang digunakan untuk mengirim email berdasarkan lokasi pengiriman. Pengecekan dilakukan menggunakan situs *http://localtimes.info*.

Gambar 4. 58 kota di dunia dengan *time zone +0700*

Gambar 4.58 merupakan ilustrasi dari beberapa kota di dunia yang menggunakan *time zone +0700* dan salah satunya adalah Jakarta yang merupakan ibu kota negara Indonesia.

2. Waktu yang berasal dari *Header email* sah dari Studi Kasus 2:



Gambar 4. 59 ilustrasi memeriksa waktu pesan

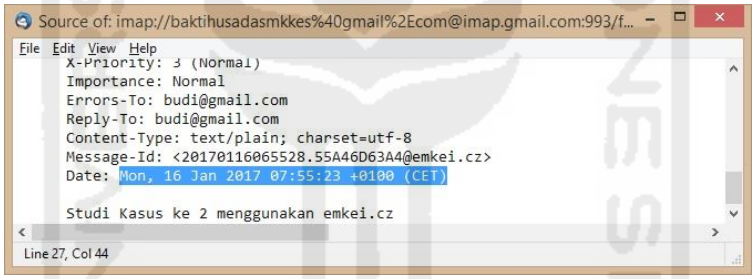
Gambar 4.59 menjelaskan bahwa pesan email dikirim dengan menggunakan waktu yang sama berdasarkan waktu pemrosesan email yaitu *Sun, 15 Jan 2017*

19:02:29 +0000 (UTC). +0000 merupakan *Email Time Zone Indicator* atau *time zone* yang digunakan untuk mengirim email berdasarkan lokasi pengiriman. Pemeriksaan time zone dilakukan menggunakan situs *www.worldtimeserver.com*

Gambar 4. 60 ilustrasi time menggunakan UTC +0000

Gambar 4.54 merupakan ilustrasi waktu yang digunakan pada koordinat UTC +0000, berdasarkan penjelasan gambar dikatakan bahwa waktu dengan *Coordinated Universal Time* (UTC) +0000 lebih lambat 7 jam dengan negara Indonesia. Jadi waktu pengiriman email adalah Sun, 15 Jan 2017 19:02:29 dijumlahkan 7 jam menjadi Mon, 16 Jan 2017 02:02:29 waktu di negara Indonesia.

3. Waktu yang berasal dari *Header email spoofing* dari Studi Kasus 1 :



Gambar 4. 61 ilustrasi memeriksa waktu pesan

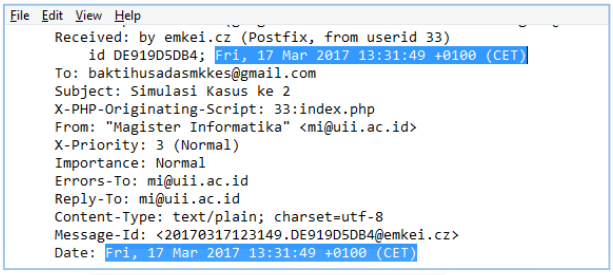
Gambar 4.61 menjelaskan bahwa pesan email dikirim dengan menggunakan satu waktu saja berdasarkan waktu kapan email tersebut dikirim yaitu *Mon, 16 Jan 2017 22:44:09 +0100. +0100* merupakan *Email Time Zone Indicator* yang digunakan untuk mengirim pesan. Namun pada waktu tersebut tidak terdapat informasi waktu dari provider email sah, misalnya *received by mail.yahoo.com*. Jadi dapat dipastikan pesan email tersebut adalah palsu atau tidak sah.

City Name	Time	City Name	Time
Addis Ababa	12:13:28 pm	Ankara	12:13:28 pm
Antananarivo	12:13:28 pm	Asmara	12:13:28 pm
Baghdad	12:13:28 pm	Dar es Salaam	12:13:28 pm
Djibouti	12:13:28 pm	Doha	12:13:28 pm
Istanbul	12:13:28 pm	Kampala	12:13:28 pm
Kuwait City	12:13:28 pm	Minsk	12:13:28 pm
Mogadishu	12:13:28 pm	Moscow	12:13:28 pm
Nairobi	12:13:28 pm	Riyadh	12:13:28 pm
Sanaa	12:13:28 pm		

Gambar 4. 62 ibu kota negara dengan koordinat +0300

Gambar 4.62 merupakan ilustrasi beberapa ibu kota negara yang menggunakan koordinat +0300. Jadi dapat dipastikan bahwa pesan email yang dikirim menggunakan waktu dari salah satu negara tersebut.

4. Waktu yang berasal dari *Header email spoofing* dari Studi Kasus 2 :



Gambar 4. 63 ilustrasi memeriksa waktu pesan

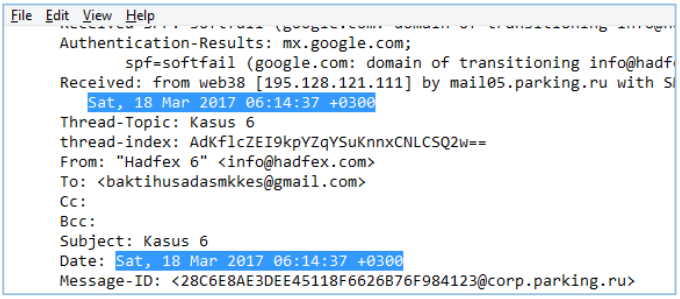
Gambar 4.63 menjelaskan bahwa pesan email dikirim dengan menggunakan satu waktu saja berdasarkan waktu kapan email tersebut dikirim yaitu *Fri, 17 Mar 2017 13:31:49 +0100*. *+0100* merupakan *Email Time Zone Indicator* yang digunakan untuk mengirim pesan. Berikut adalah ilustrasi pengecekan time zone dengan waktu *+0100*.

City Name	Time	City Name	Time
Abuja	10:49:53 am	Algiers	10:49:53 am
Amsterdam	10:49:53 am	Bangui	10:49:53 am
Berlin	10:49:53 am	Bratislava	10:49:53 am
Brazzaville	10:49:53 am	Brussels	10:49:53 am
Budapest	10:49:53 am	Copenhagen	10:49:53 am
Essen	10:49:53 am	Kinshasa	10:49:53 am
Lagos	10:49:53 am	Libreville	10:49:53 am
Ljubljana	10:49:53 am	Luanda	10:49:53 am
Madrid	10:49:53 am	Milan	10:49:53 am
Ndjamena	10:49:53 am	Niamey	10:49:53 am
Oslo	10:49:53 am	Paris	10:49:53 am

Gambar 4. 64 ibu kota negara dengan koordinat +0100

Gambar 4.64 merupakan ilustrasi beberapa ibu kota negara yang menggunakan koordinat +0100. Jadi dapat dipastikan bahwa pesan email yang dikirim menggunakan waktu dari salah satu negara tersebut.

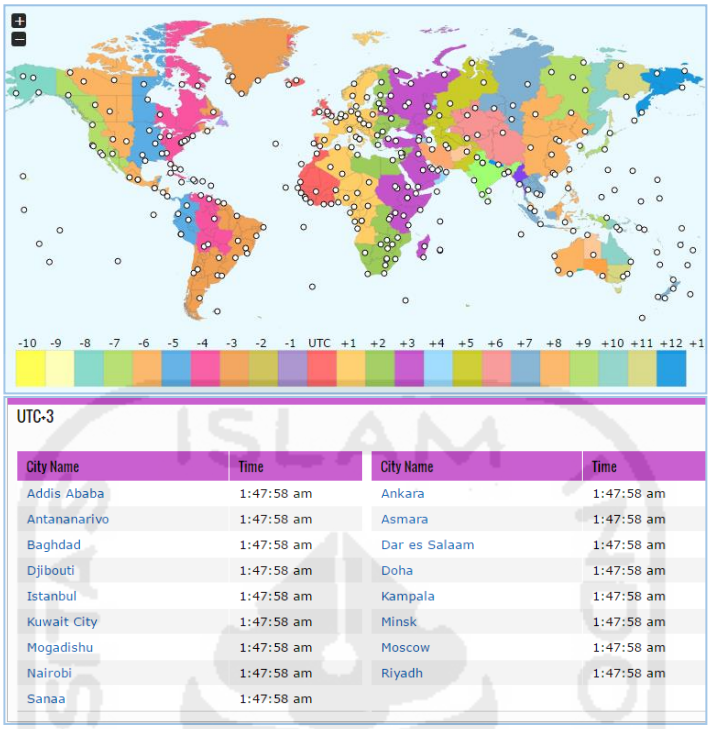
5. Waktu yang berasal dari *email header spoofing* studi kasus 3



Gambar 4. 65 Ilustrasi memeriksa wakti pesan

Gambar 4.65 menjelaskan bahwa pesan email dikirim dengan menggunakan satu waktu saja berdasarkan waktu kapan email tersebut dikirim yaitu *Sat, 18 Mar 2017 06:14:37*

+0300. *+0300* merupakan *Email Time Zone Indicator* yang digunakan untuk mengirim pesan. Berikut adalah ilustrasi pengecekan time zone dengan waktu *+0300*.



Gambar 4. 66 Ilustrasi pengecekan wilayah dengan time zone +0300

Gambar 4.65 merupakan ilustrasi beberapa wilayah yang menggunakan koordinat *time zone +0300*. Jadi dapat dipastikan bahwa pesan email yang dikirim menggunakan waktu dari salah satu negara tersebut.

Hasil pengecekan waktu email dibuat kemudian dirangkum dalam tabel berikut guna mempermudah melihat perbedaan.

Tabel 4. 20 ringkasan informasi waktu dari pesan email

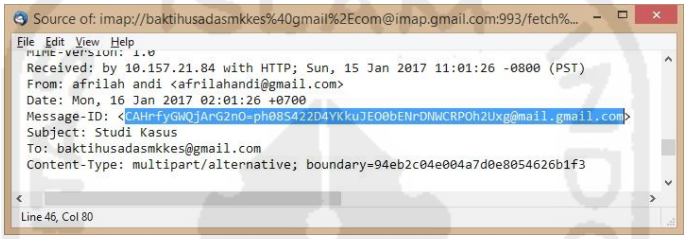
Alamat Email	*Received*	*Date*	*Time Zone*	Status
afrilahandi@gmail.com	*Sun, 15 Jan 2017 11:01:26*	*Mon, 16 Jan 2017 02:01:26*	*-0800* dan *+0700*	*Legitimate*
wiwin.nia@yahoo.com	*Sun, 15 Jan 2017 19:02:29*	*Sun, 15 Jan 2017 19:02:29*	*+0000*	*Legitimate*
budi@gmail.com	-	*Mon, 16 Jan 2017 22:44:09*	*+0100*	*Spoofing*
mi@uii.ac.id	-	*Fri, 17 Mar 2017 13:31:49*	*+0100*	*Spoofing*
info@hadfex.com	-	*Sat, 18 Mar 2017 06:14:37*	*+0300*	*Spoofing*

Tabel 4.20 menjelaskan bahwa salah satu ciri dari email *spoofing* adalah tidak terdapat waktu *Received*. Selain itu pada pesan email *legitimate* dan *spoofing* terdapat *time zone* yang digunakan sebagai wilayah mengirim pesan. Banyaknya wilayah pada koordinat tertentu menyulitkan dalam menentukan darimana wilayah sebenarnya pesan email tersebut dikirim

5.1.4 Examining message ID yakni memeriksa identitas pesan.

ID pesan merupakan nomor identitas pesan unik yang diberikan oleh sistem pemrosesan email yang akan ditampilkan pada *header* pesan. Berikut adalah ilustrasi pemeriksaan terhadap nomor ID dari pesan email yang dibuat berdasarkan *header email* :

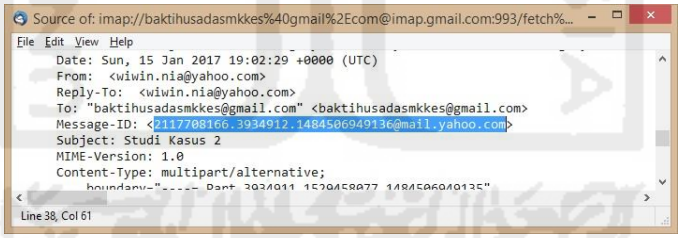
1. ID pesan dari *Header email* sah Studi Kasus 1



Gambar 4. 67 Ilustrasi memeriksa ID pesan

Pada gambar 4.59 diketahui ID pesan dari email *afrilahandi@gmail.com* adalah *CAHrfyGWQjArG2nO=ph08S422D4YKkuJEO0bENrDNWCRPOh2Uxg@mail.gmail.com*, dengan menggunakan *domain* adalah *@gmail.com*.

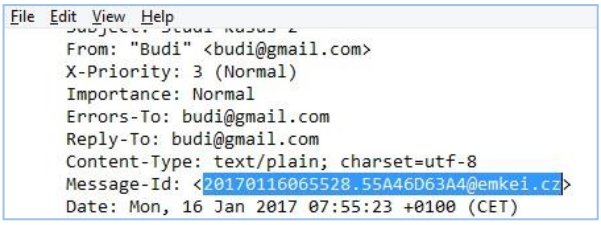
2. ID pesan dari *Header email* sah dari Studi Kasus 2



Gambar 4. 68 ilustrasi pemeriksaan ID pesan

Pada gambar 4.60 diketahui ID pesan dari email *wiwin.nia@yahoo.com* adalah *2117708166.3934912.1484506949136@mail.yahoo.com*, dengan menggunakan *domain* adalah *@mail.yahoo.com*

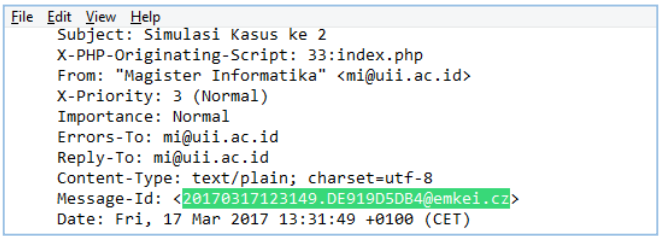
3. ID pesan dari *Header email spoofing* dari Studi Kasus 1



Gambar 4. 69 ilustrasi pemeriksaan ID pesan

Pada gambar 4.69 diketahui ID pesan dari email *budi@gmail.com* adalah *20170116065528.55A46D63A4@emkei.cz*, dengan menggunakan *domain* adalah *@emkei.cz*.

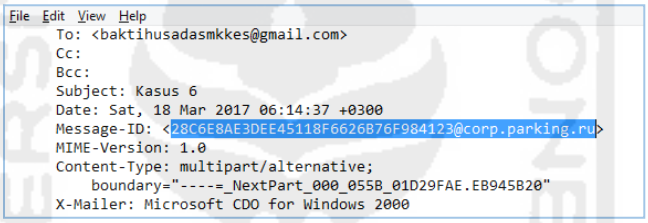
4. ID pesan dari *Header email spoofing* dari Studi Kasus 2



Gambar 4. 70 ilustrasi pemeriksaan ID pesan

Pada gambar 4.70 diketahui ID pesan dari email *mi@uii.ac.id* adalah *20170317123149.DE919D5DB4@emkei.cz*, dengan menggunakan *domain* adalah *@emkei.cz*.

5. ID pesan dari *header email spoofing* dari Studi Kasus 3



Gambar 4. 71 ilustrasi pemeriksaan ID pesan

Pada gambar 4.71 diketahui ID pesan dari email *info@hadfex.com* adalah *28C6E8AE3DEE45118F6626B76F984123@corp.parking.ru*, dengan menggunakan *domain* adalah *@corp.parking.ru*.

Hasil dari pemeriksaan dari masing–masing ID pesan dapat dilihat pada tabel 4.21.

Tabel 4. 21 ID pesan pada masing – masing pesan email

Alamat Email	ID Pesan	*domain Email*	Status
afrilahandi@gmail.com	*CAHrfyGWQjArG2nO=ph08S422D4YKkuJEO0bENrDNWCRPOh2Uxg*	*@gmail.com*	*Legitimate*
wiwin.nia@yahoo.com	*2117708166.3934912.1484506949136*	*@mail.yahoo.com*	*Legitimate*
budi@gmail.com	*20170116065528.55A46D63A4*	*emkei.cz*	*Spoofing*
mi@uii.ac.id	*20170317123149.DE919D5DB4*	*@emkei.cz*	*Spoofing*
info@hadfex.com	*28C6E8AE3DEE45118F6626B76F984123*	*@corp.parking.ru*	*Spoofing*

Tabel 4.21 merupakan ID pesan dari masing – masing pesan email yang dikirim, 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 atau tidak. Namun jika diteliti berdasarkan *domain email* yang digunakan, maka akan ditemukan kesalahan *domain* yang digunakan oleh pengirim email, misalnya alamat email yang digunakan adalah *budi@gmail.com* seharusnya memiliki *email provider* adalah *@gmail.com* namun dalam studi kasus *domain email* yang dimiliki adalah *corp.parking.ru*, hal tersebut juga terjadi pada alamat email *mi@uii.ac.id* yang memiliki *domain email* berbeda yaitu *emkei.cz* dan alamat email *info@hadfex.com* yang memiliki *domain email* yaitu *@corp.parking.ru* . Diketahui *emkei.cz* dan *corp.parking.ru* merupakan sebuah situs yang memberikan layanan untuk mengirim pesan email *spoofing*. Berdasarkan penjelasan tersebut maka dapat dipastikan bahwa pesan email yang memiliki ID pesan dengan *provider* yang sama dapat dipastikan itu adalah pesan yang berasal dari alamat email yang sah, sebaliknya apabila pesan yang memiliki ID pesan dengan *provider* yang berbeda dengan alamat email alamat email dapat dipastikan bahwa pesan tersebut berasal dari alamat email yang tidak sah. Dari studi kasus yang menjadi ID pesan tidak sah adalah *20170116065528.55A46D63A4@emkei.cz, 20170317123149.DE919D5DB4@emkei.cz* dan *28C6E8AE3DEE45118F6626B76F984123@corp.parking.ru*

5.1.5 Examining sender's IP address yakni memeriksa alamat IP pengirim.

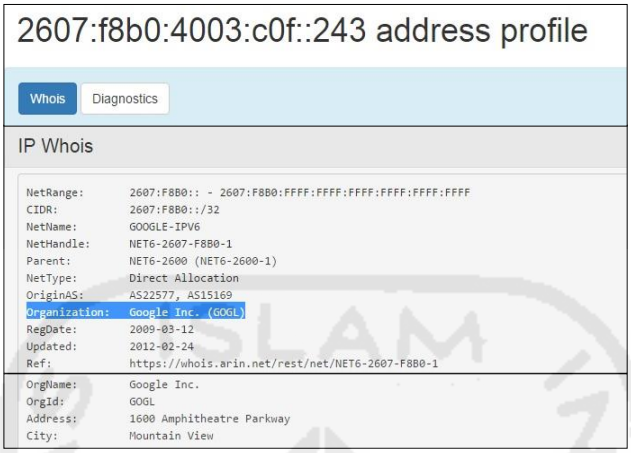
Alamat IP merupakan alamat Internet Protocol yang diberikan oleh sistem pemrosesan email dalam mengirim pesan yang akan ditampilkan pada *header* pesan. Alamat IP yang akan diperiksa adalah alamat IP versi 4 (IPV4) dan IP versi 6 (IPV6). Berikut ilustrasi pemeriksaan alamat IP dari pengirim pesan email berdasarkan *header email* :

1. Alamat IP pengirim dari *header email* sah Studi Kasus 1

Gambar 4. 72 Ilustrasi memeriksa alamat IP pengirim

Gambar 4.72 merupakan tahap memeriksa alamat IP dari pengirim, untuk mengetahuinya kita dapat melihatnya dari *Received-SPF: client-ip*. Berdasarkan gambar tersebut diketahui alamat *client IP* menggunakan IPV6 yaitu *2607:f8b0:4003:c0f::243*, yang berasal dari alamat email *afrilahandi@gmail.com*.

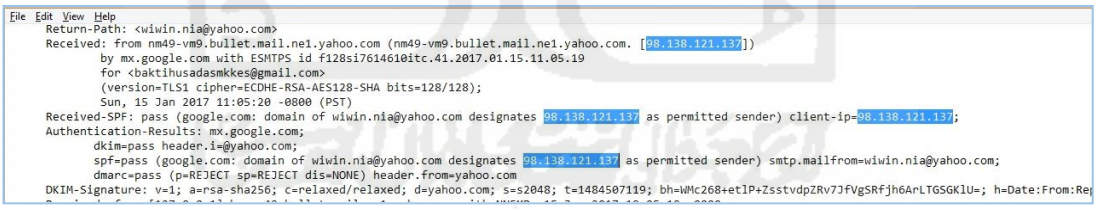
Selanjutnya kita dapat memeriksa keaslian dari IP *client* tersebut. Dalam penelitian ini pemeriksaan keaslian IP *client* menggunakan situs situs *https://who.is/whois-ip/ip-address*. Pelitian yang dilakukan adalah pemeriksaan keaslian *provider* yang digunakan.



Gambar 4. 73 pemeriksaan *IP client*

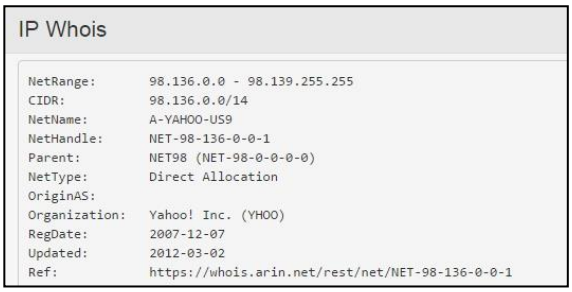
Gambar 4.73 merupakan ilustrasi dari proses pemeriksaan keaslian alamat *IP client* dari alamat email *afrilahandi@gmail.com*, berdasarkan gambar tersebut dapat dikatakan bahwa *IP client* dari *gmail.com* menggunakan IPV6 yaitu *2607:f8b0:4003:c0f::243* dan merupakan *IP client* yang sah, hal tersebut dibuktikan dengan penyataan dari *Organization : Google.Inc (GOGL)*. Menandakan bahwa email tersebut berasal dari *provider* yang sah.

2. Alamat IP pengirim dari *header email* sah dari Studi Kasus 2



Gambar 4. 74 pemeriksaan *IP client* pada Studi Kasus 2

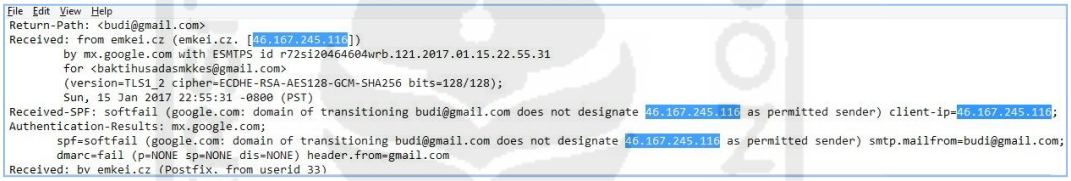
Gambar 4.74 merupakan tahap memeriksa alamat IP dari pengirim pada studi kasus 2, untuk mengetahuinya kita dapat melihatnya dari *Received-SPF: client-ip*. Berdasarkan gambar tersebut diketahui alamat *client IP* menggunakan IPV4 yaitu *98.138.121.137*, diketahui bahwa alamat email yang digunakan adalah *wiwin.ani@yahoo.com*. Selanjutnya kita dapat memeriksa keaslian dari *client IP* tersebut. Dalam penelitian ini pemeriksaan keaslian *client IP* menggunakan situs situs *https://who.is/whois-ip/ip-address*. Pelitian yang dilakukan adalah pemeriksaan keaslian *provider* yang digunakan.



Gambar 4. 75 pemeriksaan keaslian *IP client*

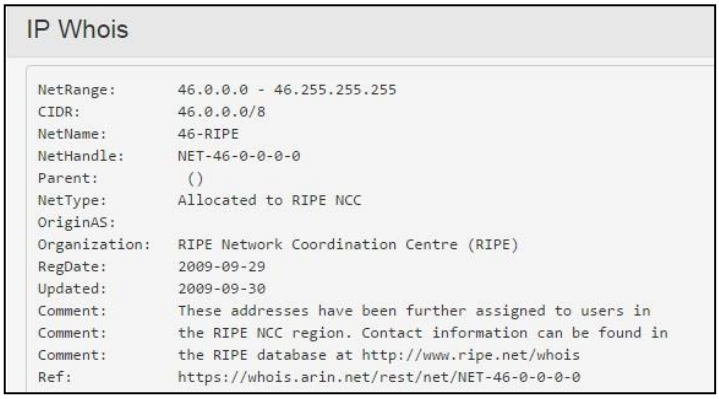
Gambar 4.75 merupakan proses pemeriksaan keaslian alamat *IP client* pada Studi Kasus 2 dari alamat email *wiwin.nia@yahoo.com*, berdasarkan gambar tersebut dapat dikatakan bahwa *IP client* dari *ymail.com* menggunakan IPV4 yaitu *98.138.121.137* tersebut merupakan *IP client* yang sah, hal tersebut dibuktikan dengan penyataan dari *Organization : Yahoo! Inc. (YHOO)*. Menandakan bahwa email tersebut berasal dari *provider* yang sah.

3. Alamat IP pengirim dari *header email spoofing* dari Studi Kasus 1



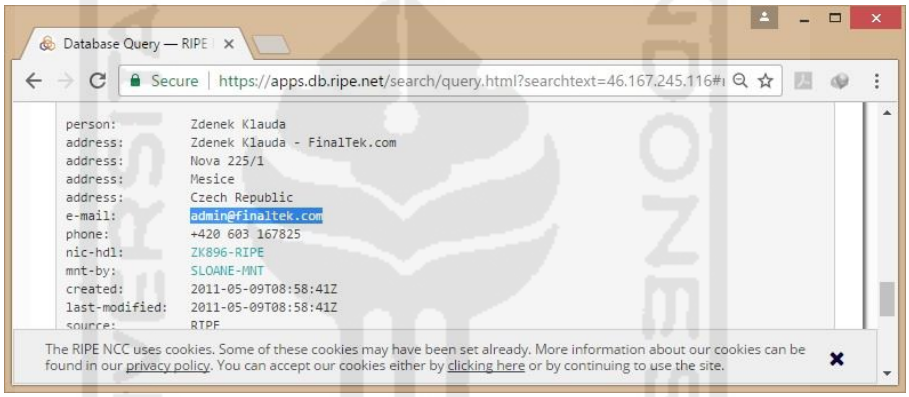
Gambar 4. 76 pemeriksaan *IP client*

Gambar 4.76 merupakan tahap memeriksa alamat IP dari pengirim pada studi kasus 1 email *spoofing*, untuk mengetahuinya kita dapat melihatnya dari *Received-SPF: client-ip*. Berdasarkan gambar tersebut diketahui alamat *client IP* adalah *46.167.245.116*, alamat tersebut merupakan alamat IPV4. Berdasarkan studi kasus yang dilakukan, diketahui bahwa alamat email yang digunakan oleh *budi@gmail.com*. 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*.



Gambar 4. 77 pemeriksaan keaslian *IP client*

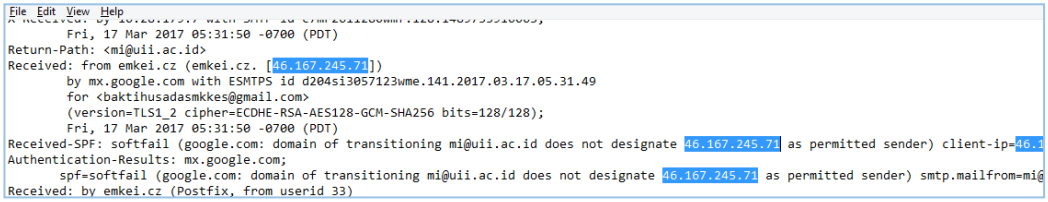
Gambar 4.77 merupakan proses pemeriksaan keaslian alamat *client IP* dari alamat email *budi@gmail.com*, berdasarkan gambar tersebut dapat dikatakan bahwa *IP client* menggunakan *provider gmail.com* dengan IPV4 yaitu *46.167.245.116* tersebut merupakan *IP client* yang tidak sah, hal tersebut dibuktikan dengan penyataan dari *Organization : RIPE Network Coordination Centre (RIPE)*, menandakan bahwa email tersebut tidak berasal dari *provider gmail* yang ada pada *google* yang seharusnya berasal pada pernyataan *Organization* adalah *Google.Inc (GOGL)*. Selain itu juga terdapat pernyataan dari *Comment : these address have been further assigned to users in the RIPE NCC region. Contact information can be found in the RIPE database at http://www.ripe.net/whois*, menandakan bahwa alamat *client IP* tersebut telah dialihkan pada RIPE NCC. Selanjutnya memeriksa *client IP* pada *RIPE database* melalui situs *www.ripe.net/whois*.



Gambar 4. 78 memeriksa *RIPE database*

Gambar 4.78 merupakan proses pemeriksaan *RIPE database* dengan *client IP* adalah *46.167.245.116.* Berdasarkan hasil pencarian gambar tersebut menjelaskan bahwa *client IP* tersebut menggunakan *domain finaltek.com* untuk mengirim pesan email. Hal ini dapat membuktikan bahwa *client IP* yang digunakan oleh alamat email *budi@gmail.com* adalah tidak sah.

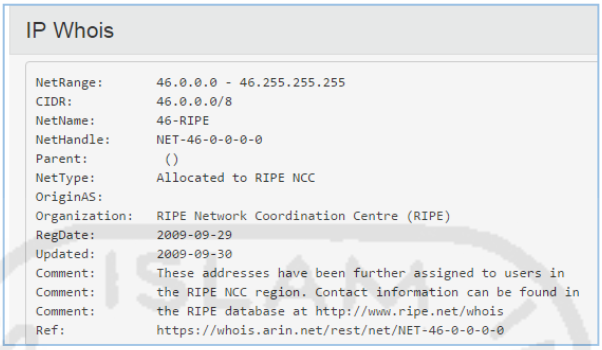
4. Alamat IP pengirim dari *header email spoofing* dari Studi Kasus 2



Gambar 4. 79 memeriksa *client IP*

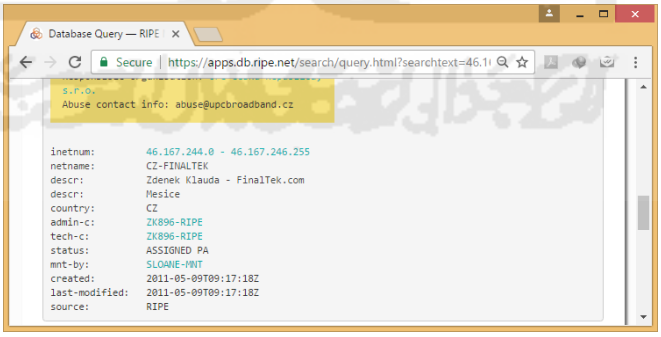
Gambar 4.79 merupakan tahap memeriksa alamat IP dari pengirim pada studi kasus email *spoofing*, untuk mengetahuinya kita dapat melihatnya dari *Received-SPF: client-ip*. Berdasarkan gambar tersebut diketahui alamat *client IP* adalah

46.167.245.71, alamat tersebut merupakan alamat IPV4. Berdasarkan studi kasus yang dilakukan, diketahui bahwa alamat email yang digunakan oleh *mi@uii.ac.id*. 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*.



Gambar 4. 80 Pemeriksaan informasi *IP client*

Gambar 4.80 merupakan proses pemeriksaan keaslian alamat *client IP* dari alamat email *mi@uii.ac.id*, berdasarkan gambar tersebut dapat dikatakan bahwa *IP client* menggunakan *provider gmail.com* dengan IPV4 yaitu *46.167.245.71* tersebut merupakan *IP client* yang tidak sah, hal tersebut dibuktikan dengan pernyataan dari *Comment : these address have been further assigned to users in the RIPE NCC region. Contact information can be found in the RIPE database at http://www.ripe.net/whois*, menandakan bahwa alamat *client IP* tersebut telah dialihkan pada RIPE NCC. Selanjutnya memeriksa *client IP* pada *RIPE database* melalui situs *www.ripe.net/whois*.



Gambar 4. 81 memeriksa *RIPE database*

Gambar 4.81 merupakan proses pemeriksaan *RIPE database* dengan *client IP* adalah *46.167.245.116*. Berdasarkan hasil pencarian gambar tersebut menjelaskan bahwa *client IP* tersebut menggunakan *domain finaltek.com* untuk mengirim pesan email. Hal ini dapat membuktikan bahwa *client IP* yang digunakan oleh alamat email *mi@uii.ac.id* adalah tidak sah.

5. Alamat IP pengirim dari *header email spoofing* dari Studi Kasus 3

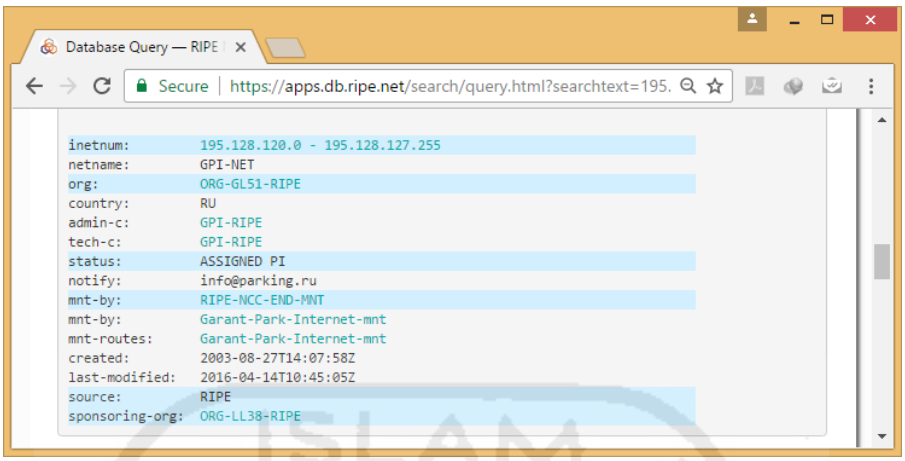
Gambar 4. 82 memeriksa *IP client*

Gambar 4.82 merupakan tahap memeriksa alamat IP dari pengirim pada studi kasus 3 *email spoofing*, untuk mengetahuinya kita dapat melihatnya dari *Received-SPF: client-ip*. Berdasarkan gambar tersebut 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 adalah *info@hadfex.com*. 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*.

Gambar 4. 83 memeriksa keaslian *client IP*

Gambar 4.83 merupakan proses pemeriksaan keaslian alamat *IP client* dari alamat email *info@hadfex.com*, berdasarkan gambar tersebut dapat dikatakan bahwa *IP client* dari *gmail.com* menggunakan IPV4 yaitu *195.128.120.25* tersebut merupakan *IP client* yang tidak sah, hal tersebut dibuktikan dengan penyataan dari *Organization : RIPE Network Coordination Centre (RIPE)*, menandakan bahwa email tersebut tidak berasal dari domain yang sah misalnya saja *domain gmail* yang ada pada *google*. Selain itu juga terdapat pernyataan dari *Comment : these address have been further assigned to users in the RIPE NCC region. Contact information can be found in the RIPE database at http://www.ripe.net/whois*, menandakan bahwa alamat *client IP*

tersebut telah dialihkan pada RIPE NCC. Selanjutnya memeriksa *client IP* pada *RIPE database* melalui situs *www.ripe.net/whois*.



Gambar 4. 84 memeriksa *RIPE database*

Gambar 4.84 merupakan proses pemeriksaan *RIPE database* dengan *client IP* adalah *195.128.120.25.* Berdasarkan hasil pencaharian gambar tersebut dijelaskan bahwa *client IP* tersebut memiliki informasi yang didapat dari *domain @parking.ru* untuk mengirim pesan email. Hal ini dapat membuktikan bahwa *client IP* yang digunakan oleh alamat email *info@hadfex.com* adalah tidak sah.

Tabel 4. 22 alamat *client IP email* pengirim

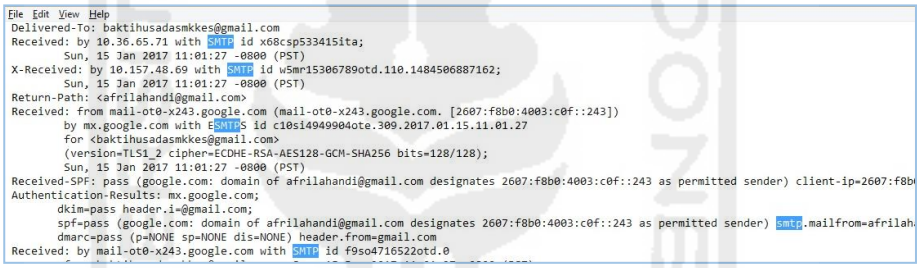
Alamat email	Alamat IP	*Organization*	Email Domain	Status
afrilahandi@gmail.com	*2607:f8b0:4003:c0f::243*	*Google.Inc (GOGL)*	*@google.com*	*Legitimate*
wiwin.nia@yahoo.com	*98.138.121.137*	*Yahoo! Inc. (YHOO)*	*@yahoo-inc.com*	*Legitimate*
budi@gmail.com	*46.167.245.116*	*RIPE Network Coordination Centre*	*@finaltek.com*	*Spoofing*
mi@uii.ac.id	*46.167.245.71*	*RIPE Network Coordination Centre*	*@finaltek.com*	*Spoofing*
info@hadfex.com	*195.128.120.25*	*RIPE Network Coordination Centre*	*@parking.ru*	*Spoofing*

Tabel 4.22 menjelaskan bahwa pada *client IP email legitimate* yang menggunakan *email organization* yaitu *Google.Inc (GOGL)* seharusnya menggunakan alamat IPV6 sebaliknya apabila *client IP* tersebut menggunakan alamat IPV4 maka masih diragukan keasliannya dan harus dilakukan pemeriksaan alamat IP klien email. Berikutnya, pada *client IP email legitimat* yang menggunakan *email organiation* yaitu *Yahoo! Inc. (YHOO)* masih menggunakan alamat IPV4. Jadi dapat disimpulkan bahwa *client IP email lgitimate* harus berasal dari *organization* penyedia layanan email yang sah seperti *google* dan *yahoo*.

Sedangkan pada *client IP email spoofing* yang memiliki alamat *budi@gmail.com*, *mi@uii.ac.id* dan *info@hadfex.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 dan *IP address* yang menggunakan *organization RIPE Network Coordination Centre* serta menggunakan domain email *@parking.ru* dan *@finaltek.com* merupakan alamat *IP* dari *email spoofing*.

5.1.6 Protocol used to transport email yakni memeriksa protokol yang digunakan dalam mentranspor email. Pemeriksaan bertujuan untuk mengetahui protokol apa saja yang digunakan oleh pelaku untuk mengirim email. Berikut ilustrasi pemeriksaan protokol yang digunakan untuk mengirim pesan email berdasarkan *header email* :

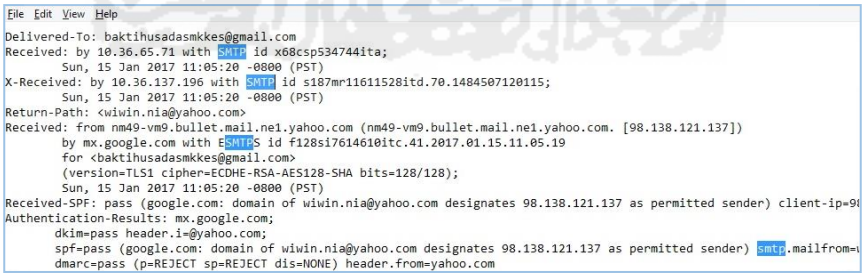
1. Protokol pengirim dari *header email* sah Studi Kasus 1



Gambar 4. 85 Ilustrasi memeriksa protokol yang digunakan

Gambar 4.85 menjelaskan bahwa alamat email *afrilahandi@gmail.com* menggunakan protokol SMTP, hal tersebut dapat dibuktikan dari informasi *Received* dan *Authentication spf*.

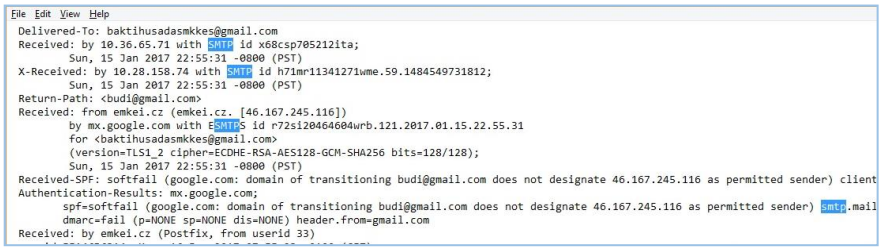
2. Protokol pengirim dari *header email* sah dari Studi Kasus 2 :



Gambar 4. 86 ilustrasi memeriksa protokol yang digunakan

Gambar 4.86 menjelaskan bahwa alamat email *wiwin.nia@yahoo.com* menggunakan protokol SMTP, hal tersebut dapat dibuktikan dari informasi *Received* dan *Authentication spf*.

3. Protokol pengirim dari *header email spoofing* dari Studi Kasus 1



Gambar 4 87 ilustrasi memeriksa protokol yang digunakan

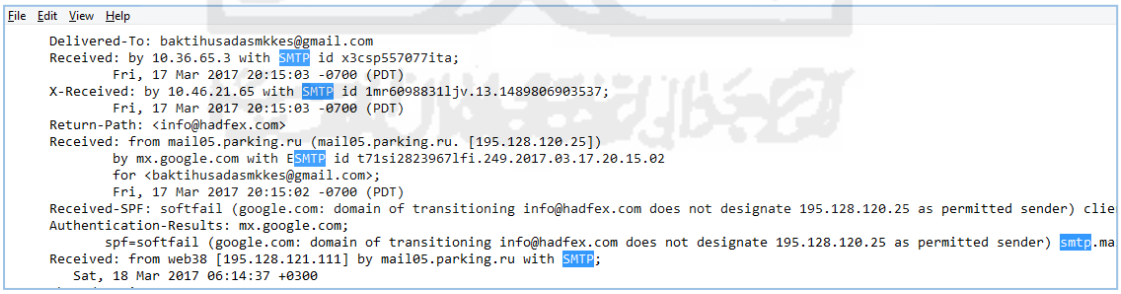
Gambar 4.87 menjelaskan bahwa alamat email *budi@gmail.com* menggunakan protokol SMTP, hal tersebut dapat dibuktikan dari informasi *Received* dan *Authentication spf*.

4. Protokol pengirim dari *header email spoofing* dari Studi Kasus 2

Gambar 4. 88 ilustrasi memeriksa protokol yang digunakan

Gambar 4.88 menjelaskan bahwa alamat email *budi@gmail.com* menggunakan protokol SMTP, hal tersebut dapat dibuktikan dari informasi *Received* dan *Authentication spf*.

5. Protokol pengirim dari *header email spoofing* dari Studi Kasus 3



Gambar 4. 89 Ilustrasi memeriksa protokol yang digunakan

Gambar 4.89 menjelaskan bahwa alamat email *budi@gmail.com* menggunakan protokol SMTP, hal tersebut dapat dibuktikan dari informasi *Received* dan *Authentication spf*.

Untuk lebih jelasnya, maka hasil pemeriksaan protokol yang digunakan untuk mentraspor pesan dari masing–masing email dibuatkan dalam sebuah tabel 4.23 sebagai berikut:

Tabel 4. 23 protokol yang digunakan pengirim

Alamat Email	Protokol	Status
afrilahandi@gmail.com	*HTTP, SMTP,* dan *ESMTPS*	*legitimate*
wiwin.ani@yahoo.com	*NNFMP* dan *SMTP*	*legitimate*
budi@gmail.com	*SMTP*	*spoofing*
mi@uii.ac.id	*SMTP* dan *ESMTPS*	*spoofing*
info@hadfex.com	*SMTP* dan *ESMTP*	*spoofing*

Tabel 4.23 menjelaskan bahwa semua email baik email sah maupun email *spoofing* menggunakan protokol yang sama yaitu SMTP. Studi kasus yang dilakukan dalam penelitian ini menggunakan email berbasis web. Ada beberapa protokol yang digunakan dalam melakukan transaksi email, diantaranya yaitu :

a. HTTP (*Hypertext Transfer Protocol*) adalah protokol jaringan berbasisi *client server* yang menjadi penghubung dan mentransfer informasi melalui jaringan internet. Secara default HTTP bekerja pada dua port :
   - *Port* 80 adalah port standar yang tidak dienkripsi.
   - *Port 443* adalah port yang memiliki keamanan atau biasa disebut *HTTPS* (SSL/TLS).

b. POP3 (*Post Office Protocol versi 3*) adalah protokol email standar yang digunakan untuk menerima email dari server jauh ke klien email lokal. POP3 memungkinkan untuk men-download pesan email pada komputer lokal dan membacanya bahkan ketika komputer sedang offline. Secara default, protokol POP3 bekerja pada dua port:
   - *Port 110* adalah port default POP3 yang tidak dienkripsi.
   - *Port 995* adalah port yang memiliki keamanan atau disebut juga *Secure POP3* (SSL-POP).

c. IMAP (*Internet Message Access Protocol*) adalah protokol email yang digunakan untuk mengakses email pada web server jauh dari klien lokal. Secara default, protokol IMAP bekerja pada tiga port:
   - *Port 143* adalah port standar yang tidak dienkripsi.
   - *Port 993* adalah port yang memiliki keamanan atau disebut juga IMAP4 over SSL (IMAPS).
   - *Port 585* adalah port yang memiliki keamanan atau disebut juga *Secure IMAP* (*IMAP4-SSL*).

d. SMTP (*Simple Mail Transfer Protocol*) adalah protokol standar untuk mengirim email di Internet.

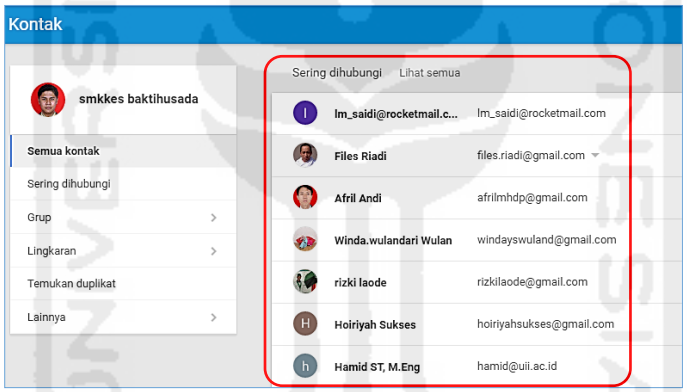
   Secara default, protokol SMTP bekerja pada empat port:

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

e. NNFMP (*Newman No-Frills Mail Protocol*) adalah protokol internal yang dimiliki oleh *yahoo* untuk jalur lalu lintas email namun tidak diakui oleh IANA.

5.2 Unstructured data, merupakan tahapan pemeriksaan email berdasarkan data tidak terstruktur, tahap ini meliputi :

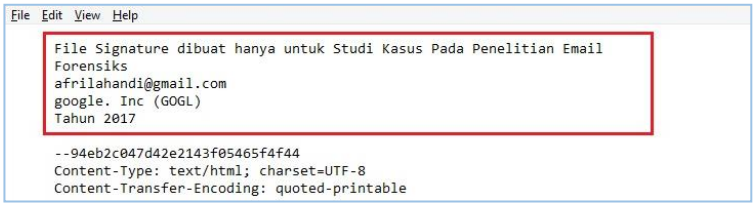
5.2.1 Relational analysis, tahap ini dilakukan proses pemeriksaan informasi kontak lain yang berhubungan dengan email pelaku.



Gambar 4. 90 Ilustrasi memeriksa informasi kontak lain dari email pelaku

Gambar 4.90 menjelaskan tentang hubungan email target/pelaku dengan email lain yang pernah melakukan transaksi email. Pada tahap diatas invetigator dapat mengetahui kepada siapa saja pelaku/target melakukan transaksi email, misalnya saja email yang sering dihubungi oleh pelaku.

5.3 File signature yakni memeriksa *file signature* dari pesan email. Pemeriksaan bertujuan untuk mengetahui informasi apa saja yang berhubungan dengan pelaku misalnya informasi tempat kerja, alamat kantor, nomor telepon, alamat website dan lain – lain. Berikut ilustrasi pemeriksaan *file signature* dari pesan email berdasarkan *header email* :



Gambar 4. 91 Ilustrasi *file signature* pada pesan email masuk

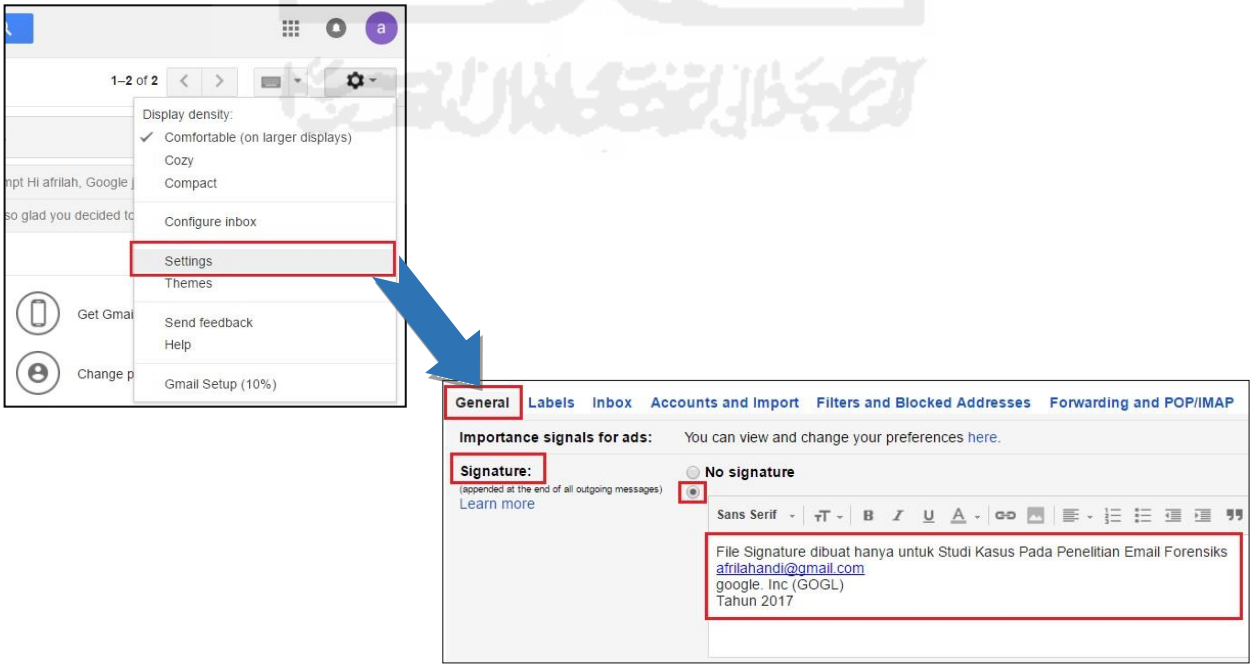
Gambar 4.91 merupakan contoh *file signature* yang terdapat pada pesan emal dengan alamat email *afrilahandi@gmail.com*. *File signature* merupakan informasi tentang pengirim yang dapat diatur secara otomatis untuk ditampilkan kepada semua alamat email yang dituju ataupun tidak ditampilkan oleh pengirim. Berdasarkan penelitian yang dilakukan bahwa pada alamat email *legitimate* dapat dilakukan pengaturan file signature sedangkan pada alamat email spoofing tidak dapat dilakukan pengaturan.

Tabel 4. 24 keterangan file signature

Alamat email	Status	Keterangan
afrilahandi@gmail.com	*legitimate*	Dapat dilakukan pengaturan *file signature*
wiwin.ani@yahoo.com	*legitimate*	Dapat dilakukan pengaturan *file signature*
budi@gmail.com	*spoofing*	Tidak Dapat dilakukan pengaturan file signature
mi@uii.ac.id	*spoofing*	Tidak Dapat dilakukan pengaturan *file signature*
info@hadfex.com	*spoofing*	Tidak Dapat dilakukan pengaturan *file signature*

Tabel 4.24 menjelaskan bahwa *file signature* merupakan salah satu cara untuk mengetahui apakah pesan email tersebut sah atau tidak. Berdasarkan penelitian yang dilakukan bahwa pada email sah (*legitimate*) dapat dilakukan pengaturan pada *file signature* sedangkan pada email *spoofing* tidak dapat dilakukan pengaturan pada *file signature*.

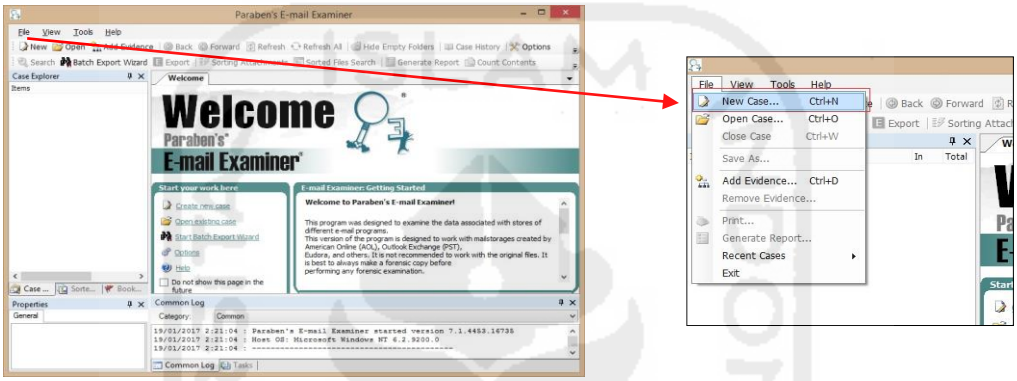
Berikut adalah ilustrasi pengaturan pada file signature menggunakan akun gmail : langkah pertama adalah masuk pada akun alamat gmail, kemudian pada *shortcut settings* pilih *Settings*, seperti pada gambar 4.92 barikut ini:



Gambar 4. 92 pengaturan *file signature*

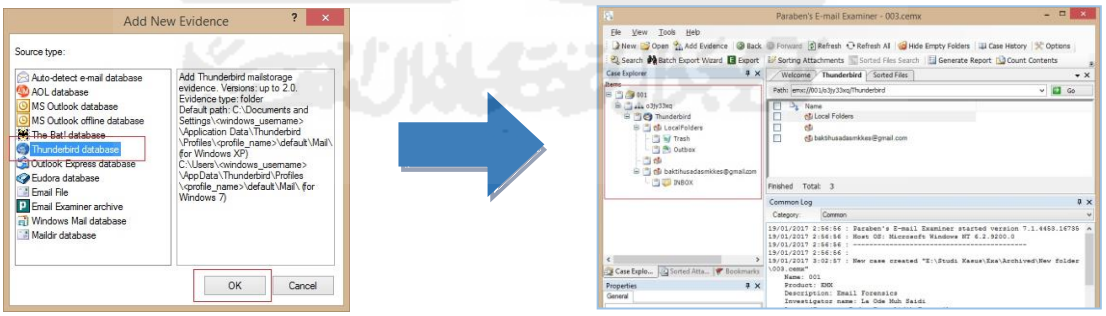
Langkah kedua adalah pilih menu *General* kemudian *scroll* kebawah pada pilihan *Signature* hilangkan centang pada *No Signature* kemudian pada area teks ketikan informasi *signature* anda secara ringkas. Setelah *file signature* diatur maka langkah terakhir adalah klik *save changes*

5.4 *Acquire email archives*, pada 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.



Gambar 4. 93 memulai kasus baru

Gambar 4.93 menjelaskan cara untuk menambahkan kasus baru terhadap barang bukti email yang ada. Perintah tersebut adalah *file* > *New Case* atau dengan menekan kombinasi Ctrl + N secara bersamaan, langkah berikutnya adalah menambahkan informasi tambahan dan kemudian hasil kasus tersebut. Selanjutnya akan masuk pada tahap inti yaitu memilih type dari *client email* yang akan diperiksa.



Gambar 4. 94 memilih tipe/jenis *client email*

Gambar 4.82 menjelaskan perintah untuk memilih tipe atau jenis *client email* dari sumber barang bukti. Pada penelitian ini yang menjadi tipe *client email* adalah *thunderbird* sebab yang menjadi bukti pemeriksaan adalah alamat email dari target atau korban, sebagaimana telah dijelaskan pada simulasi kasus sebelumnya sehingga tipe barang bukti *client email* yang dipilih adalah *thunderbird database*. 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.

5.5 *Trace email original* merupakan tahap selanjutnya pada pemeriksaan email. 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. Berikut ilustrasi penelitiannya :

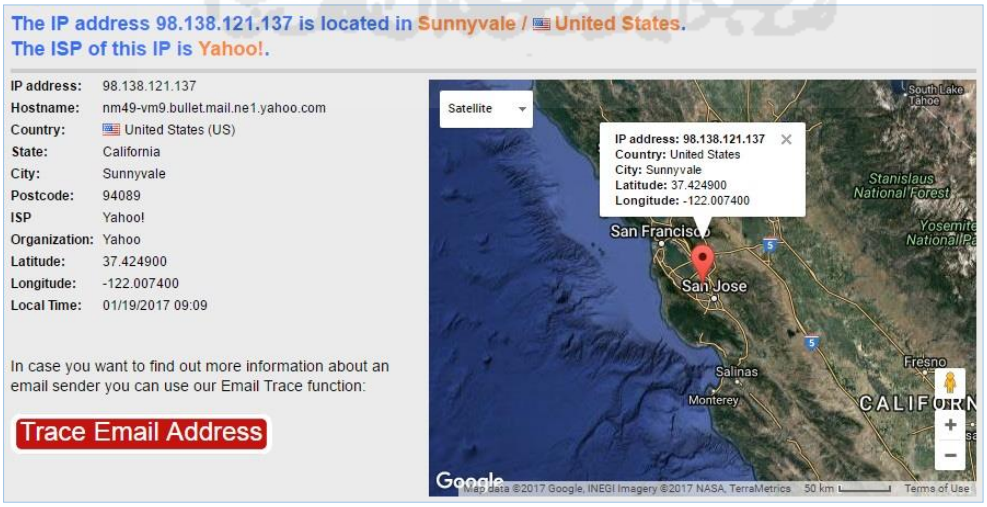
Email sah pada studi kasus 1

IP Address	2607:f8b0:4003:c0f::243
Location	United States, Oklahoma, Tulsa
Latitude & Longitude	36.153980, -95.992780 (36°9'14"N 95°59'34"W)
ISP	Google Inc.
Local Time	19 Jan, 2017 10:11 AM (UTC -06:00)
Domain	google.com
Net Speed	-
IDD & Area Code	(1) 918
ZIP Code	74192
Weather Station	Tulsa (USOK0537)

Gambar 4. 95 *tracer email* sah dari studi kasus 1

Gambar 4.95 merupakan hasil dari *tracer email* pada alamat email sah studi kasus 1 yang dilakukan menggunakan menggunakan situs *http://www.ip2logation.com*, sedangkan penelusuran *latitude & longitude* menggunakan website *https://www.google.co.id/maps*.

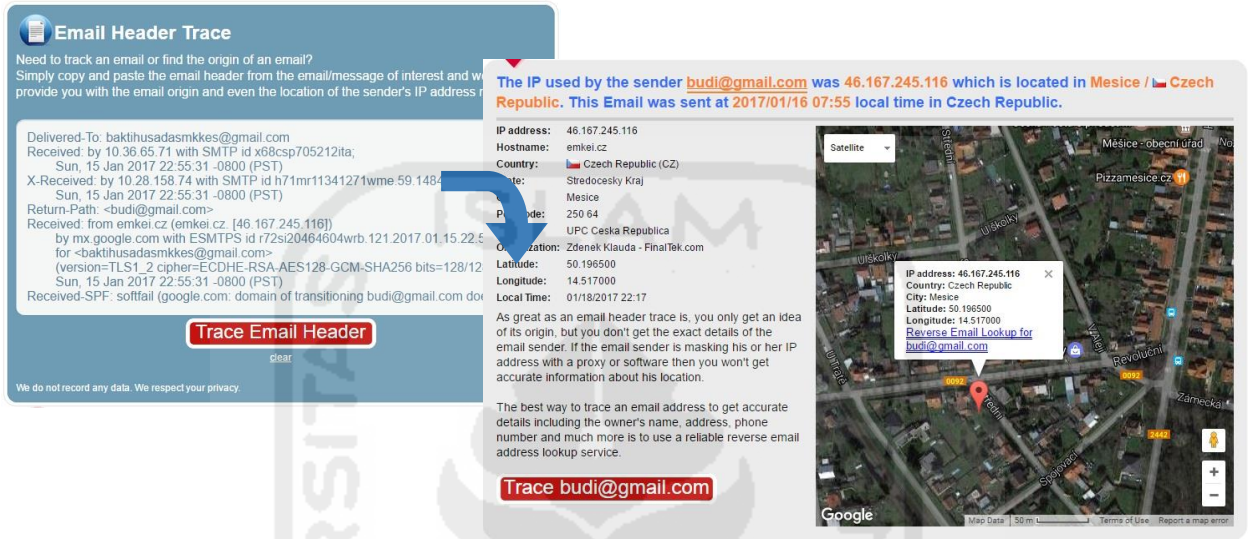
Email sah studi kasus 2



Gambar 4. 96 *tracer email* sah studi kasus 2

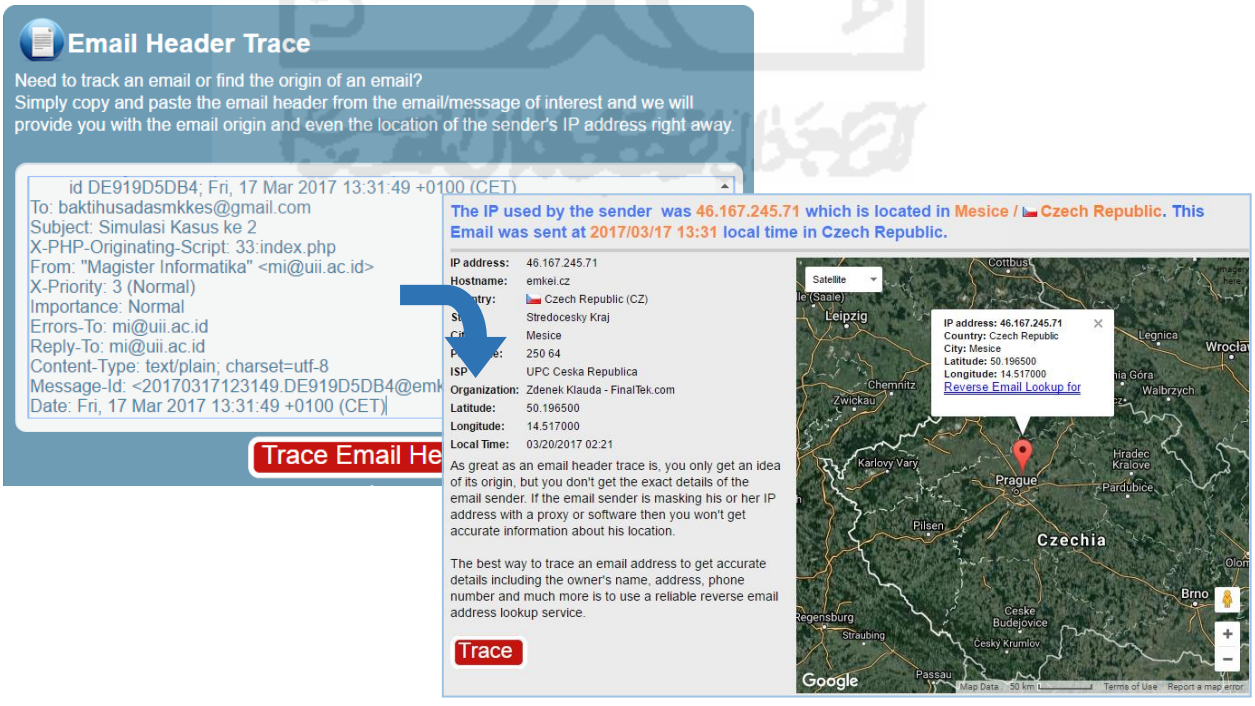
Gambar 4.96 merupakan hasil dari *tracer email* pada pengirim kedua menggunakan situs *http://www.traceemail.com* dan *https://db-ip.com* dengan cara memasukan memasukan alamat IP email tersebut. Berdasarkan penelitian ditemukan beberapa point penting dalam pemeriksaan *tracer email* yang dilakukan yaitu *IP address, Hostname, sender's email address, country, ISP, Organization,* dan *map of latitude and longitude*.

Email spoofing studi kasus 1



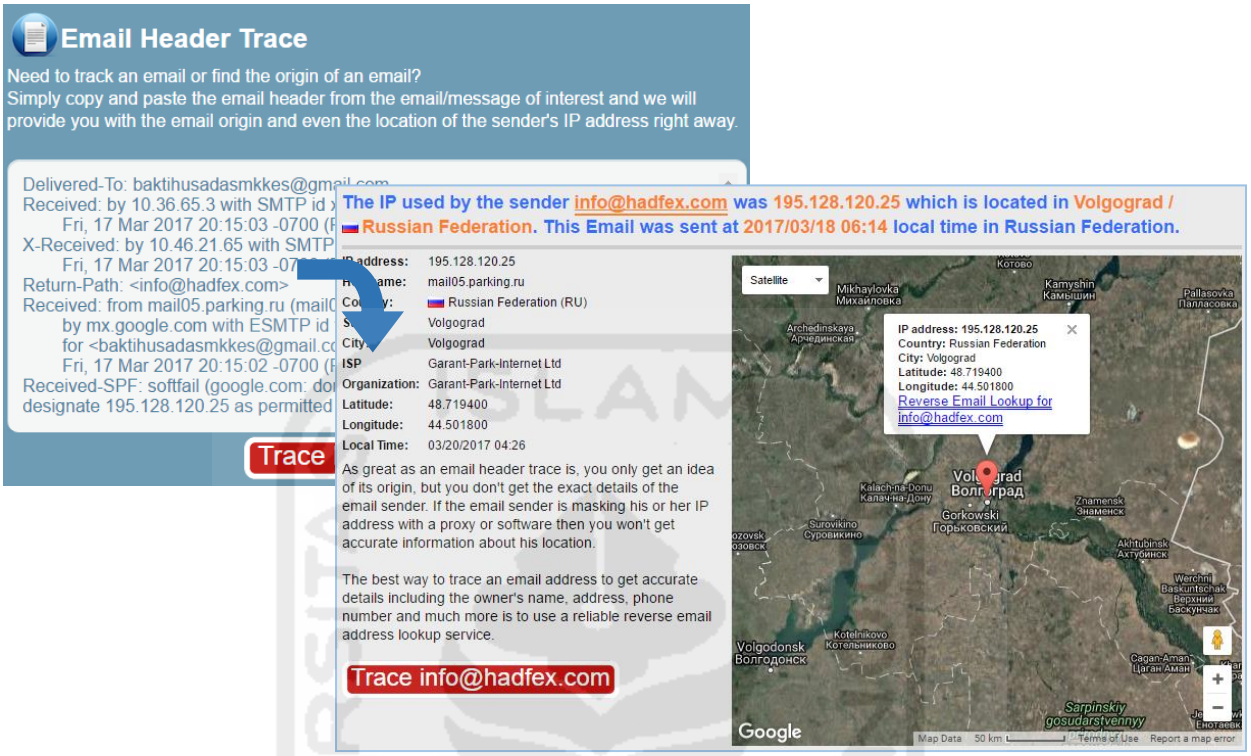
Gambar 4. 97 *tracer email spoofing* studi kasus 1

Gambar 4.85 merupakan hasil dari *tracer email* pada pengirim ketiga menggunakan situs *http://www.traceemail.com/trace-email-header.html* dengan cara memasukan data – data yang terdapat pada *header* pesan email tersebut.



Gambar 4. 98 *trace email spoofing* studi kasus 2

Gambar 4.98 merupakan hasil dari *tracer email spoofing* pada studi kasus 2 menggunakan situs *http://www.traceemail.com/trace-email-header.html* dengan cara memasukan data – data yang terdapat pada *header* pesan email tersebut.



Gambar 4. 99 *tracer email spoofing* studi kasus 3

Dari pemeriksaan *tracer email* yang dilakukan terhadap empat pesan email yang dikirim terdapat beberapa informasi penting yang berhubungan dengan keberadaan email pelaku, yaitu diantaranya :

1. *Email address.*
2. *IP address*
3. *Hostname*
4. *Country*
5. *State*
6. *City*
7. *Postcode*
8. *ISP*
9. *Organization*
10. *Latitude & longitude*
11. *Date & time*

Tabel 4. 25 Hasil *trace email* dari masing – masing *header*

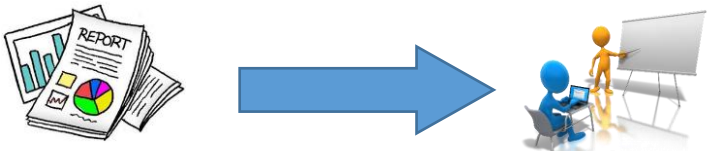
Information	*Tracer email* sah studi kasus 1	*Tracer email* sah studi kasus	*Tracer email spoofing* studi kasus 1	*Tracer email spoofing* studi kasus 2	*Tracer email spoofing* studi kasus 3
Email Address	*afrilahandi@gmail.com*	*wiwin.nia@yahoo.com*	*budi@gmail.com*	*mi@uii.ac.id*	*info@hadfex.com*
IP Address	*2607:f8b0:4003:c0f::243*	*98.138.121.137*	*46.167.245.116*	*46.167.245.71*	*195.128.120.25*
Hostname	*mail-ot0-x243.google.com*	*nm49-vm9.bullet.mail.ne1.yahoo.com*	*Emkei.cz*	*Emkei.cz*	*mail05.parking.ru*
Country	*United States (US)*	*United States (US)*	*Czech Republic (CZ)*	*Czech Republic (CZ)*	*Russian Federation (RU)*
State	*Oklahoma*	*California*	*Stredocesky Kraj*	*Stredocesky Kraj*	*Volgograd*
City	*Tulsa*	*Sunnyvale*	*Mesice*	*Mesice*	*Volgograd*
Postcode	*74102*	*94089*	*250 64*	*250 64*	
ISP	*Google. Inc*	*Yahoo!*	*UPC Ceska Republica*	*UPC Ceska Republica*	*Garant-Park-Internet Ltd*
Organization	*Google. Inc*	*Yahoo*	*Zdenek Klauda – FinalTek.com*	*Zdenek Klauda – FinalTek.com*	*Garant-Park-Internet Ltd*
Latitude	*36.154 (36° 9' 14.40" N)*	*37.424900*	*50.196500 (50°11'53"N)*	*50.196500 (50°11'53"N)*	*48.719400*
Longitude	*-95.9928 (95° 59' 34.08" W)*	*-122.007400*	*14.517000 (14°31'12"E)*	*14.517000 (14°31'12"E)*	*44.501800*
Date	*Mon, 16 Jan 2017*	*Sun, 15 Jan 2017*	*2017/01/16*	*2017/03/20*	*03/20/2017*
Time	*02:01:26 +0700*	*19:02:29 +0000 (UTC)*	*07:55 local time*	*02:21 local time*	*04:26 local time*
Status	*legitimate*	*legitimate*	*spoofing*	*spoofing*	*spoofing*

Tabel 4.25 menjelaskan tentang temuan hasil *trace* dari berapa *header email* yang menjadi studi kasus dalam penelitian ini. Temuan tersebut berupa informasi tentang masing – masing asal pesan pengirim email. Berdasarkan penelitian yang dilakukan bahwa informasi yang ditampilkan merupakan informasi tentang pengiriman email oleh provider atau domain.

6. *Presentation*

Merupakan tahap menyajikan hasil, tahap ini meliputi :

6.1 Report & visualisation merupakan tahapan menyajikan hasil investigasi dalam bentuk laporan dan presentasi.



Report *Visualisation*

Gambar 4. 100 Ilustrasi *Trace email original*

Gambar 4.100 menjelaskan tentang ilustrasi pembuatan laporan dalam bentuk *hardcopy* dan visualisasi dalam bentuk slide presentasi laporan hasil investigasi yang dilakukan. Laporan dibuat berdasarkan mekanisme pembuatan laporan investigasi yang ada pada masing – masing institut penegak hukum sesuai prosedur yang ditetapkan.

Adapun ringkasan laporan penelitian dari studi kasus yang dilakukan adalah sebagai berikut :

1. Identifikasi Kasus
   a. Deskripsi Kasus

   Berdasarkan studi kasus penelitian yang dilakukan, kasus berawal dari laporan korban sebagai pemohon yang mendapat kiriman pesan email mencurigakan kemudian meminta kepada penyidik untuk dilakukan penyelidikan. Alamat email yang dimiliki oleh korban adalah *baktihusadasmkkes@gmail.com.*

   b. Ringkasan Kasus

Pemohon	Bp. Sutrisno, Kepala Sekolah SMK Bakti Husada
Alamat Pemohon	Jl. Lingkar Utara, Depok, Sleman, Yogyakarta
Penyidik	LM. Saidi (Lab. Digital Foresik UII)
Waktu	Sabtu 14 Januari 2017, Pukul 15.30 WIB
Nomor Kasus	001/FD/I/2017

2. Deskripsi Barang Bukti

   Melakukan penyitaan terhadap 1 buah laptop yang digunakan oleh korban dalam melakukan transaksi email. Kemudian melakukan akuisisi terhadap email yang dimiliki oleh korban untuk selanjutnya ditindak lanjuti. Proses akuisisi disertakan dengan nilai *hashing* untuk menjaga integritas barang bukti, berikut adalah *hashing* dari akuisisi barang bukti :

MD5 Hash *: b924cb8581cea6f70331981686a685b3*

SHA1 Hash *: c0d931d39d30824034f21c7735d1735b66e159de*

Berikut hasil verifikasi nilai *hashing* dari *MD5 Hash* dan *SHA1 Hash* :

MD5 checksum *: b924cb8581cea6f70331981686a685b3 : verified*

SHA1 checksum *: c0d931d39d30824034f21c7735d1735b66e159de : verified*

3. Proses *examination* barang bukti

   a. Team

   Dibentuk tim investigasi berdasarkan surat perintah nomor xx/x/I/2017, dengan susunan tim adalah sebagai berikut :

   - *Lead examiner :* La Ode Muh. Saidi
   - *Co. Examiner :* Ahmad Wahyudi

   b. Prosedur

   - Melakukan peng-*copy*-an hasil akuisisi yang dilakukan dari barang bukti yang disita untuk kemudian ditindak lanjuti.
   - Menyiapkan *environment system* untuk keperluan eksaminasi.
   - Mengunakan beberapa aplikasi dan situs website untuk kepentingan melihat isi email serta informasi pesan digital lainnya dari email tersebut.
   - Bukti yang akan dianalisis adalah satu buah alamat email milik korban yang kemudian dibuatkan *screenshot* yang mengarahkan pada temuan yang dikehendaki sesuai dengan target informasi yang diharapkan.
   - Melakukan expose hasil baik secara internal team maupun eksternal kepada pemohon.

   c. Waktu dan Tempait

   - Proses eksaminiasi mulai dilakukan pada hari Sabtu 14 Januari 2017 jam 15.30 WIB - selesai.
   - Tempat proses eksaminasi adalah Laboratorium Forensika Digital Teknik Informatika UII.

4. Hasil Eksaminasi

   Hasil eksaminasi yang dilakukan berdasarkan penelitian dari barang bukti email adalah ditemukannya empat buah pesan email dengan masing – masing pesan memiliki alamat email yang berbeda dan beberapa informasi penting yang berhubungan dengan pesan email yang diterima oleh korban yang selanjutnya dirangkum dalam sebuah tabel.

Tabel 4. 26 *Examination* penelitian studi kasus

Information	*Tracer email* sah studi kasus 1	*Tracer email* sah studi kasus	*Tracer email spoofing* studi kasus 1	*Tracer email spoofing* studi kasus 2	*Tracer email spoofing* studi kasus 3
Email Address	*afrilahandi@gmail.com*	*wiwin.nia@yahoo.com*	*budi@gmail.com*	*mi@uii.ac.id*	*info@hadfex.com*
IP Address	*2607:f8b0:4003:c0f::243*	*98.138.121.137*	*46.167.245.116*	*46.167.245.71*	*195.128.120.25*
Hostname	*mail-ot0-x243.google.com*	*nm49-vm9.bullet.mail.ne1.yahoo.com*	*Emkei.cz*	*Emkei.cz*	*mail05.parking.ru*
Country	*United States (US)*	*United States (US)*	*Czech Republic (CZ)*	*Czech Republic (CZ)*	*Russian Federation (RU)*
State	*Oklahoma*	*California*	*Stredocesky Kraj*	*Stredocesky Kraj*	*Volgograd*
City	*Tulsa*	*Sunnyvale*	*Mesice*	*Mesice*	*Volgograd*
Postcode	*74102*	*94089*	*250 64*	*250 64*	
ISP	*Google. Inc*	*Yahoo!*	*UPC Ceska Republica*	*UPC Ceska Republica*	*Garant-Park-Internet Ltd*
Organization	*Google. Inc*	*Yahoo*	*Zdenek Klauda – FinalTek.com*	*Zdenek Klauda – FinalTek.com*	*Garant-Park-Internet Ltd*
Latitude	*36.154 (36° 9' 14.40" N)*	*37.424900*	*50.196500 (50°11'53"N)*	*50.196500 (50°11'53"N)*	*48.719400*
Longitude	*-95.9928 (95° 59' 34.08" W)*	*-122.007400*	*14.517000 (14°31'12"E)*	*14.517000 (14°31'12"E)*	*44.501800*
Date	*Mon, 16 Jan 2017*	*Sun, 15 Jan 2017*	*2017/01/16*	*2017/03/20*	*03/20/2017*
Time	*02:01:26 +0700*	*19:02:29 +0000 (UTC)*	*07:55 local time*	*02:21 local time*	*04:26 local time*
Status	*legitimate*	*legitimate*	*spoofing*	*spoofing*	*spoofing*

Tabel 4.26 merupakan laporan hasil pemeriksaan terhadap pesan email yang dikirim dari beberapa alamat email yang berbeda. Dari pemeriksaan tersebut ditemukan beberapa informasi yang terdapat pada pada masing–masing *header email*. Pada pemeriksaan juga diketahui terdapat beberapa pesan sah dan tidak sah yang dikirim dari alamat email yang sah dan tidak sah. Namun pada informasi tersebut juga ditemukan terdapat alamat email yang mengirimkan pesan tidak sah. Dengan kata lain bahwa pelaku menggunakan alamat email sah orang lain untuk mengirim pesan tidak sah.

5. Kesimpulan Penelitian
    1. Berdasarkan hasil pemeriksaan yang dilakukan terhadap alamat email *baktihusadasmkkes@gmail.com*, ditemukan empat buah pesan yang dikirim dari alamat email yang berbeda-beda.
    2. Dari pesan email yang ditemukan terdapat dua buah pesan yang menggunakan alamat email sah (*legitimate*) yaitu afrilahandi@gmail.com dan wiwin.ani@yahoo.com dan dua buah pesan email *spoofing* yaitu inudin11@gmail.com dan budi@gmail.com.

7. *Post-Process*

Merupakan tahap akhir dari proses investigasi, pada tahap ini terdapat 3 tahapan yang dilakukan yaitu :

7.1 *Returns evidence* merupakan pengembalian barang bukti kepada pemiliknya

Barang bukti siap dikembalikan Barang bukti diterima pemiliknya

Gambar 4. 101 Ilustrasi *report & visualisation*

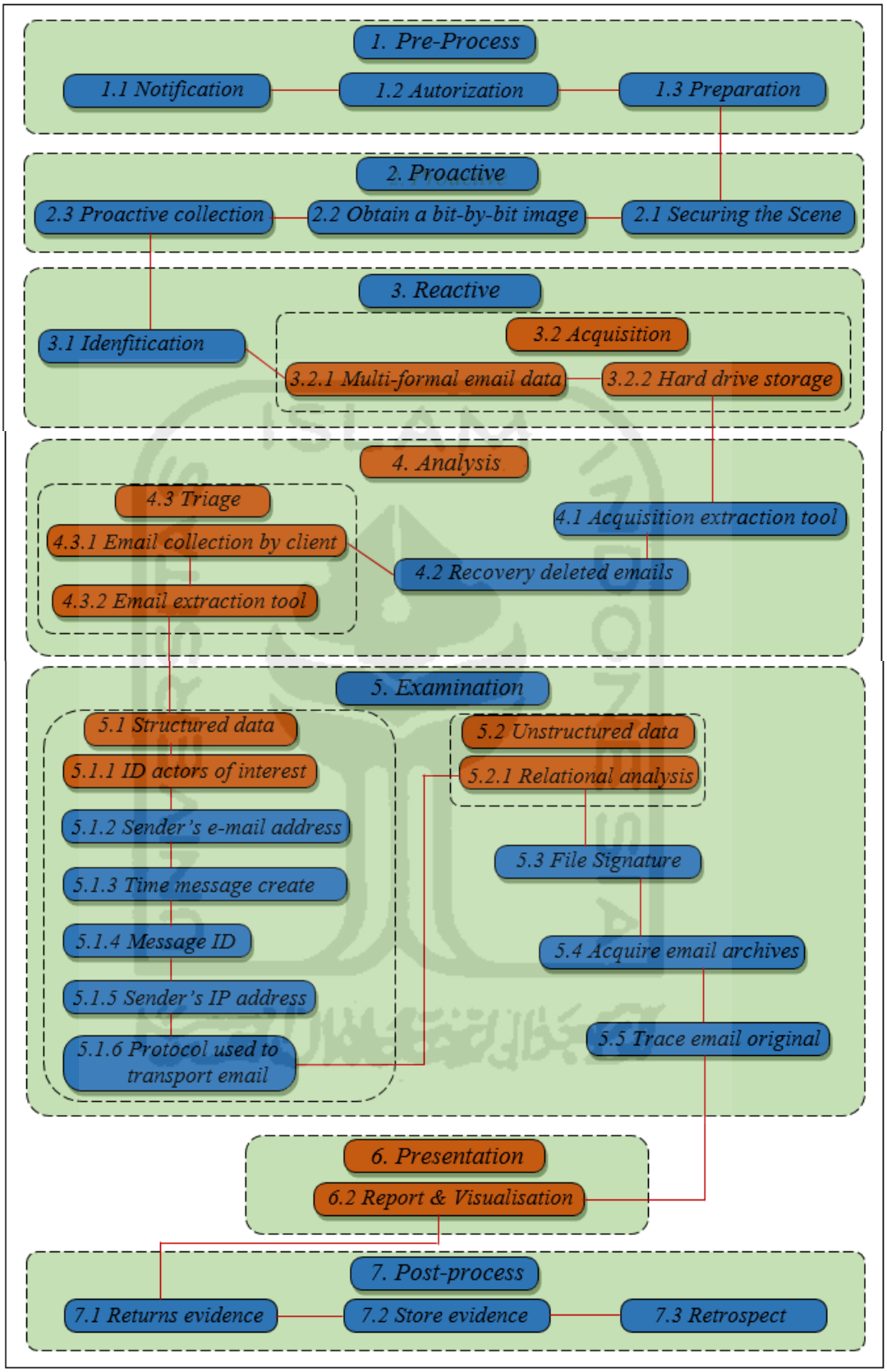
Gambar diatas menjelaskan tentang ilustrasi pengembalian barang bukti oleh penyidik dan diterima oleh pemilik, apabila barang bukti tersebut masih layak dikembalikan.

7.2 *Store evidence* merupakan tahap menyimpan barang bukti hasil akuisisi dan barang bukti asli apabila barang bukti tersebut tidak layak untuk dikembalikan atau masih memiliki ikatan hukum untuk proses selanjutnya.

7.3 *Dissemination* merupakan tahap melakukan *review* pada investigasi yang telah dilaksanakan sebagai perbaikan pada penyelidikan berikutnya.

4.2.3 Analisis *Framework*

Proses analisis dilakukan terhadap kerja dari *framework* yang telah dikembangkan berdasarkan ujicoba dari skenario kasus yang telah dijabarkan pada tahap pertama dalam proses *testing* penelitian ini. Analisis dilakukan melalui proses perbandingan menggunakan parameter terhadap setiap tahapan *framework* sebelumnya dan *framework* yang telah dikembangkan. Analisa framework dapat dilakukan dengan berdasarkan pada gambar 4.102 berikut:



Gambar 4. 102 Perbedaan *framework*

Tahapan *framework* sebelumnya

Tahapan baru f*ramework* yang dikembangkan

Berdasarkan gambar 4.102 diatas, maka dapat disimpulkan beberapa perbedaan antara *framework* sebelumnya dengan *framework* yang telah dikembangkan yang kemudian dirangkum dalam tabel 4.27 berikut ini:

Tabel 4. 27 Perbedaan *framework* sebelumnya dengan yang dikembangkan

Tahapan				*Framework*		Keterangan
				Lama	Baru	
1	*Pre-Process*				√	Tidak terdapat tahap *pre-process*, seharusnya tahap ini dilakukan sebab sangat penting dalam penanganan awal sebelum melakukan penyidikan terhadap barang bukti.
	1.1	*Notification*			√	
	1.2	*Autorization*			√	
	1.3	*Preparation*			√	
2	*Proactive*				√	Tidak terdapat tahap *practive,* seharusnya tahap ini dilakukan sebab tahap ini bertujuan untuk melakukan penyidikan awal di tempat kejadian perkara.
	2.1	*Securing the Scene*			√	
	2.2	*Obtain a bit-by-bit image of email information*			√	
	2.3	*Proactive collection*			√	
3	*Reactive*				√	
	3.1	*Identification*		√	√	
	3.2	*Acquisition*		√	√	
		3.2.1	*Multi-formal email data*	√	√	
		3.2.2	*Hard drive storage*	√	√	
4	*Analysis*				√	
	4.1	*Acquisition extraction tool*		√	√	
	4.2	*Recovery deleted emails*		√	√	
	4.3	*Triage*		√	√	
		4.3.1	*Email collection by client*	√	√	
		4.3.2	*Email extraction tool*	√	√	
5	*Examination*				√	Pada *framework* sebelumnya dilakukan tahap pemeriksaan namun berdasarkan penelitiannya, pemeriksaan dilakukan pada unstructured mail.
	5.1	*Structured data*		√	√	
		5.1.1	*ID actors of interest*	√	√	

Lanjutan **Tabel 4.27** Perbedaan *framework* sebelumnya dengan yang dikembangkan

Tahapan				*Framework*		Keterangan
				Lama	Baru	
		5.1.2	*Examining sender's e-mail address,*		√	
		5.1.3	*Examining time message create*		√	
		5.1.4	*Examining message ID*		√	
		5.1.5	*Examining sender's IP address*		√	
		5.1.6	*Protocol used to transport email*		√	
	5.2	*Unstructured data*		√	√	
		5.2.1	*Relational analysis*	√	√	
	5.3	*Signature data*			√	
	5.4	*Acquire email archives*			√	
	5.5	*Trace email original*			√	
6	*Presentation*			√	√	
	6.1	*Report & Visualisation*		√	√	
7	*Post-process*				√	Pada *framework* sebelumnya tidak ada tapanan *post-process*.
	7.1	*Returns evidence*			√	
	7.2	*Store evidence*			√	
	7.3	*Retrospect*			√	

Berdasarkan tabel perbandingan tersebut dapat dilihat kelebihan dan kekurangan dari masing – masing framework, yaitu :

Kelebihan :

1. *Framework* sebelumnya memiliki tahapan yang lengkap dalam proses investigasi forensik email berbasis *unstructure email*.
2. *Framework* yang dikembangkan memiliki tahapan yang lengkap terhadap proses investigasi forensik email berbasis *header email* dan *file signature*.

Kekurangan :

1. *Framework* sebelumnya, pada tahapan utama maupun subtahapan tidak terdapat tahap *pre-process,* seharusnya tahap ini dilakukan sebab sangat penting dalam penanganan awal sebelum melakukan penyidikan terhadap barang bukti, selain itu juga tidak terdapat tahap *practive,* seharusnya tahap ini dilakukan sebab tahap ini bertujuan untuk melakukan penyidikan awal di tempat kejadian perkara. Pada tahap analisis tidak terdapat penjelasan terhadap tahap *recovery deleted emails*, hal ini penting dilakukan untuk menemukan email yang telah terhapus yang diduga memiliki hubungan dengan pesan yang dikirim. Pada tahap *examination* sebagian dilakukan, namun tidak dijelasin secara detail tahap pemeriksaan terhadap *file signature, Acquire email archives,* dan *Trace email original*. Selanjutnya tidak ada penjelasan tentang tapanan *post-process*.
3. *Framework* yang dikembangkan hanya dapat digunakan pada investigasi forensik email pada studi kasus *email spoofing* jenis *web base mail*. Serta hanya dilakukan *examination* pada *structured mail* namun tidak menjelaskan secara detail tentang pemeriksaan *unstructured mail*

Berikut ini adalah perbedaan framework sebelumnya dan framework yang telah dikembangkan dirangkum dalam bentuk tabel :

Tabel 4. 28 Kelebihan dan kekurangan *framework*

Nama Pengembang	Framework	Kelebihan	Kekurangan
Saidi (2017)	Pengembangan *Framework* Investigasi Email *Forensics*	Memiliki tahapan yang lengkap untuk penanganan investigasi email forensik berbasis *stuctured email*, dan *file signature*	Berdasarkan simulasi kasus penelitian, *framework* hanya dapat digunakan pada investigasi forensik email jenis *web based mail*.
Haggerty, Alexander, David, dan Taylor (2011)	*A Framework for the Forensic Investigation of Unstructured Email Relationship Data*	Memiliki tahapan yang lengkap untuk forensik email berbasis *unstructured email*.	1. Tidak terdapat tahap *pre-process,* seharusnya tahap ini dilakukan sebab sangat penting dalam penanganan awal terhadap barang bukti,

Lanjutan **Tabel 4.28** Kelebihan dan kekurangan *framework*

Nama Pengembang	Framework	Kelebihan	Kekurangan
			2. Tidak terdapat tahap *practive*, tahap ini dilakukan sebab sangat penting dalam penanganan barang bukti di TKP. 3. Dibanding dengan *framework* yang dikembangkan. Pada *framework* sebelumnya tidak dijelaskan secara detail tentang *examination* pada *structured mail*. 4. Tidak ada penjelasan tentang tapanan *post-proces.*

Bab V Penutup

5.1 Kesimpulan

Adapun kesimpulan yang dapat disimpulkan dari penelitian yang telah dilakukan adalah sebagai berikut :

a. Kaitan antara *framework* dengan *Systems Development Life Cycle (SDLC)* adalah keduanya memiliki karakteristik yang sama yaitu memiliki elemen – elemen yang saling berhubungan antara satu dengan lainnya yaitu pada *framework* memiliki tahapan–tahapan antara tahapan satu dengan tahapan yang lain memiliki hubungan, selain itu *framework* juga memiliki batasan yakni hanya tertuju pada kasus tertentu yatiu pada setiap *framework* hanya memiliki tahapan–tahapan untuk satu tujuan tertentu. Metode *Systems Development Life Cycle (SDLC)* dapat digunakan untuk proses pengembangan *framework* karena memiliki tahapan – tahapan yang dibutuhkan dalam pengembangannya. Dalam pengembangan *framework* dibutuhkan beberapa tahapan yang ada pada SDLC yaitu *planning, analysis, design, implementation,* dan *maintenance*.
b. *Framework* yang dikembangkan menghasilkan 7 tahapan utama dan 29 subtahapan dengan jumlah keseluruhan tahapan adalah 36 tahapan.
c. Berdasarkan simulasi kasus penelitian, *framework* yang dikembangkan dapat digunakan pada kasus kejahatan *spoofing email* dengan jenis email adalah *web based mail*.

5.2 Saran

Sebagai pengembangan penelitian selanjutnya, perlu memperhatikan beberapa faktor berikut:

1. Pengujian dari *framework* yang telah dikembangkan harus dilakukan pada email yang berbeda misalnya email jenis *POP3* atau *email client server.*
2. Melakukan pengembangan terhadap tahapan–tahapannya sehingga tahapan tersebut dapat digunakan pada seluruh barang bukti yang ditemukan di tempat kejadian perkara dan semua jenis email.
3. Melakukan pengembangan framework sehingga dapat digunakan dalam bentuk teknik *email forensics* lainnya selain teknik *header* (*structured mail*) dan *unstructured mail*.

Daftar Pustaka

Alan, Kelvin, Anthony and Zetta (VXRL). (2014). Investigation and Intelligence Framework (IIF) – an evidence extraction model for investigation _ Forensic Focus - Articles. (n.d.). from : https://articles.forensicfocus.com/2014/11/29/investigation-and-intelligence-framework-iif-an-evidence-extraction-model-for-investigation/

Al-Azhar, M. N. (2012). Digital Forensic : Panduan Praktis Investigasi Komputer. Jakarta. Penerbit Salemba Infotek.

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

Chhabra, G. S., & Bajwa, D. S. (2012). Review of E-mail System, Security Protocols and Email Forensics. *International Journal of Computer Science & Communication Networks*, *5*(3), 201–211.

Dardick, G. S., Endicott-popovsky, B., Gladyshev, P., Kemmerich, T., & Rudolph, C. (n.d.) (2014). *Edited by Executive Summary* (Vol. 4).

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

Haggerty, J., Karran, A., Lamb, D., & Taylor, M. (2011). A framework for the forensic investigation of unstructured email relationship data. *International Journal of Digital Crime and Forensics*, *3*(3), 1–18. From http://doi:10.4018/jdcf.2011070101

Hadjidj, R., Debbabi, M., Lounis, H., Iqbal, F., Szporer, A., & Benredjem, D. (2009). Towards an integrated e-mail forensic analysis framework. *Digital Investigation*, *5*(3-4), 124–137. Retrieved from http://dx.doi.org/10.1016/j.diin.2009.01.004

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

Kohn, M. D. D., Eloff, M. M. M., & Eloff, J. H. P. H. P. (2013). Integrated dig ensic process model. *Computers and Security*, *38*, 103–115. http://doi.org/10.1016/j.cose.2013.05.001

Kota, V. K. (2014). A Monograph on Data Mining Techniques for Email Forensics, 1–5.

Lalla, H., & Flowerday, S. (2010). Towards a Standardised Digital Forensic Process: E-mail Forensics. *Issa*. http://doi.org/CFP1066I-CDR

Rhodes, D. L. (2012). The Systems Development Life Cycle (SDLC) as a Standard : Beyond the Documentation. *SAS Global Forum 2012: Planning and Support*, 1–5.

Rahayu, Y. D., & Prayudi, Y. (2014). Membangun Integrated Digital Forensics Investigation Frameworks (IDFIF) Menggunakan Metode Sequential Logic. *Seminar Nasional SENTIKA*, *2014*(Sentika)

Rahayu, Y. D. (2014). Konsep Integrated Digital Forensics Investigation Framework (IDFIF) Sebagai Standar Perbandingan Framework Investigasi. http://doi.org/10.1017/CBO9781107415324.004

The Radicati Group, I. (2015). Email Statistics Report, 2015-2019. *Email Statistics Report*, *44*(0), 4. Retrieved from http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf