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

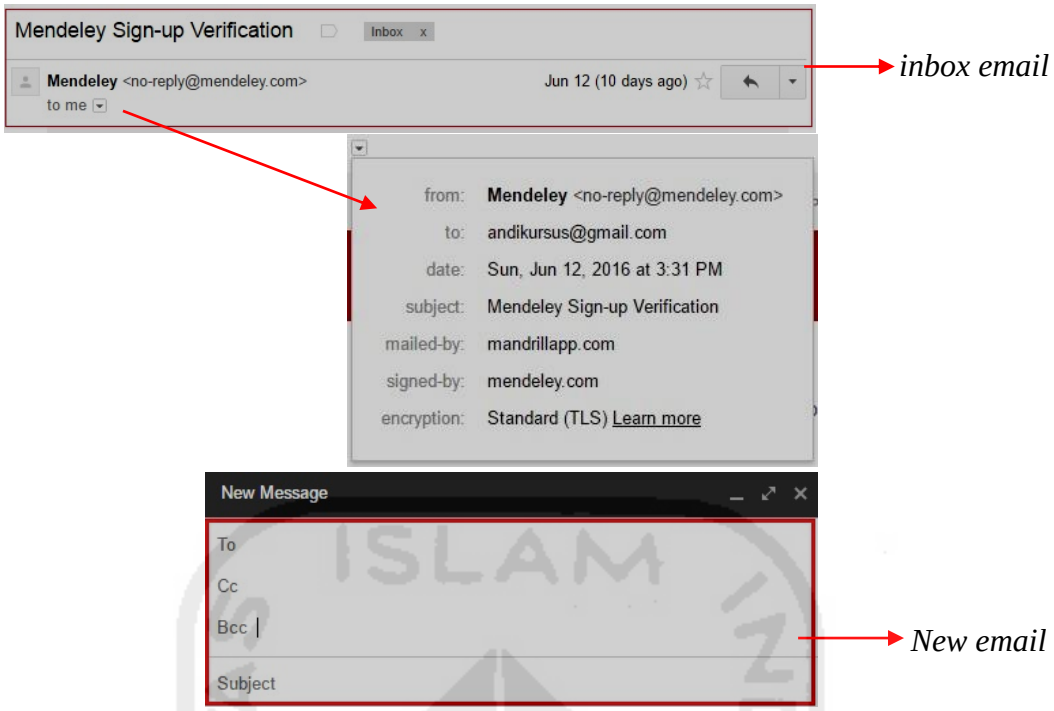
Electronic Mail atau biasa disingkat juga email dalam bahasa Indonesia diartikan sebagai "surat elektronik" merupakan sebuah sistem yang bertujuan untuk menulis, mengirim, menerima dan menyimpan pesan elektronik berupa file gambar, audio, video, dan lain-lain dari satu orang ke orang lain di belahan 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.

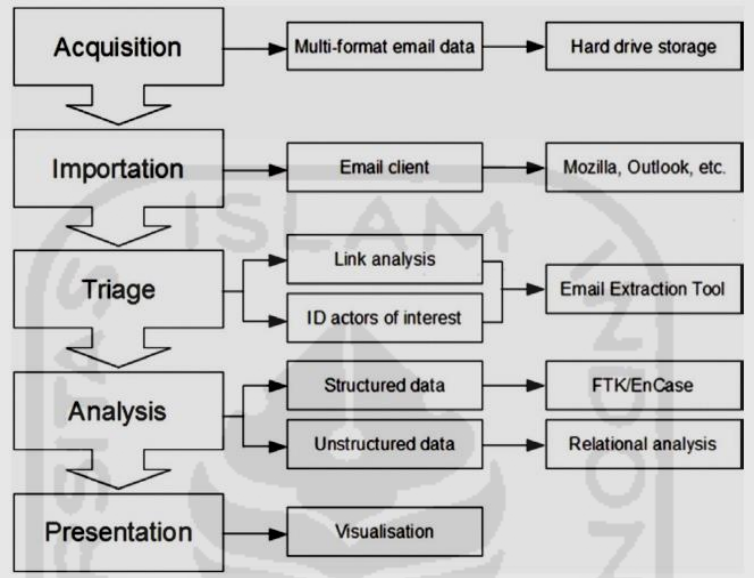
Investigasi email forensik mengacu pada studi tentang sumber dan isi email sebagai bukti untuk mengidentifikasi pengirim yang sebenarnya dan penerima pesan, data / waktu transmisi, catatan rinci transaksi email, maksud dari pengirim, dll. Penelitian ini melibatkan investigasi metadata, pencarian kata 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).

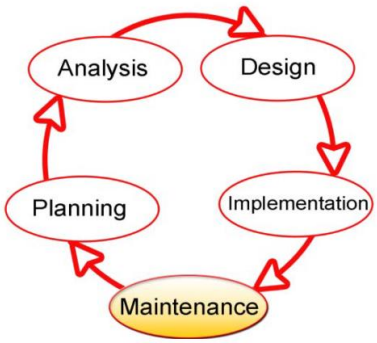
Menurut Al- Azhar (2012) barang bukti diklasifikasikan menjadi 2 bagian:

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.