

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 sehingga 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 membuat 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 permasalahan 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), Bandy, (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), Bandy, (2011), Chhabra & Bajwa, (2012) sehingga dapat dijadikan standar penggunaan oleh para penyidik investigator khususnya dalam email *forensics*.

Systems Development Life Cycle (SDLC) merupakan suatu proses pembuatan dan perubahan 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*.

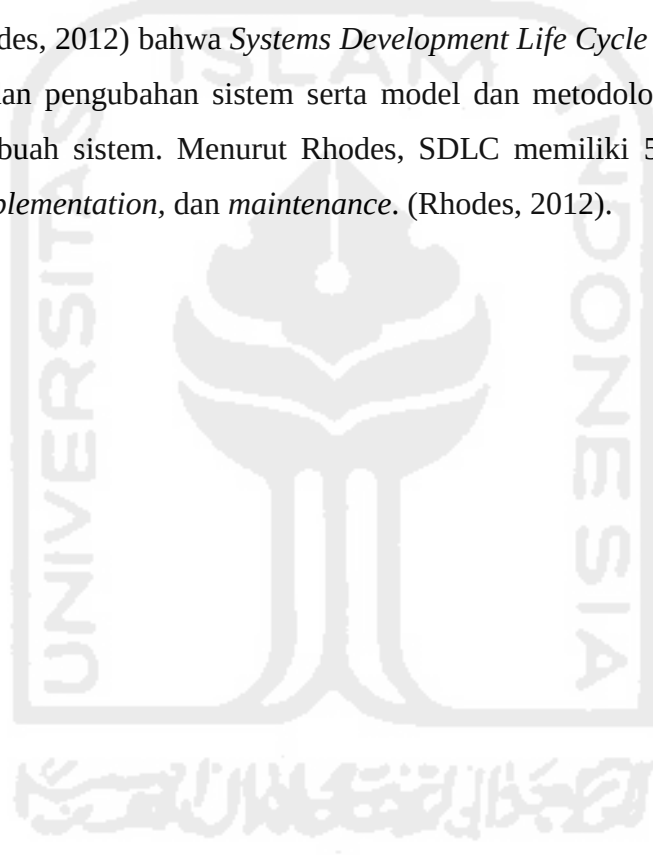
Penelitian yang serupa dilakukan oleh Alan, dkk (2014) melakukan penelitian tentang *Investigasi and Intelijen Framework* (IIF) model ekstraksi bukti digital untuk proses penyelidikan tersebut menghasilkan 4 tahapan yaitu *preparation and identification*, *strategy and*

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 perubahan 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

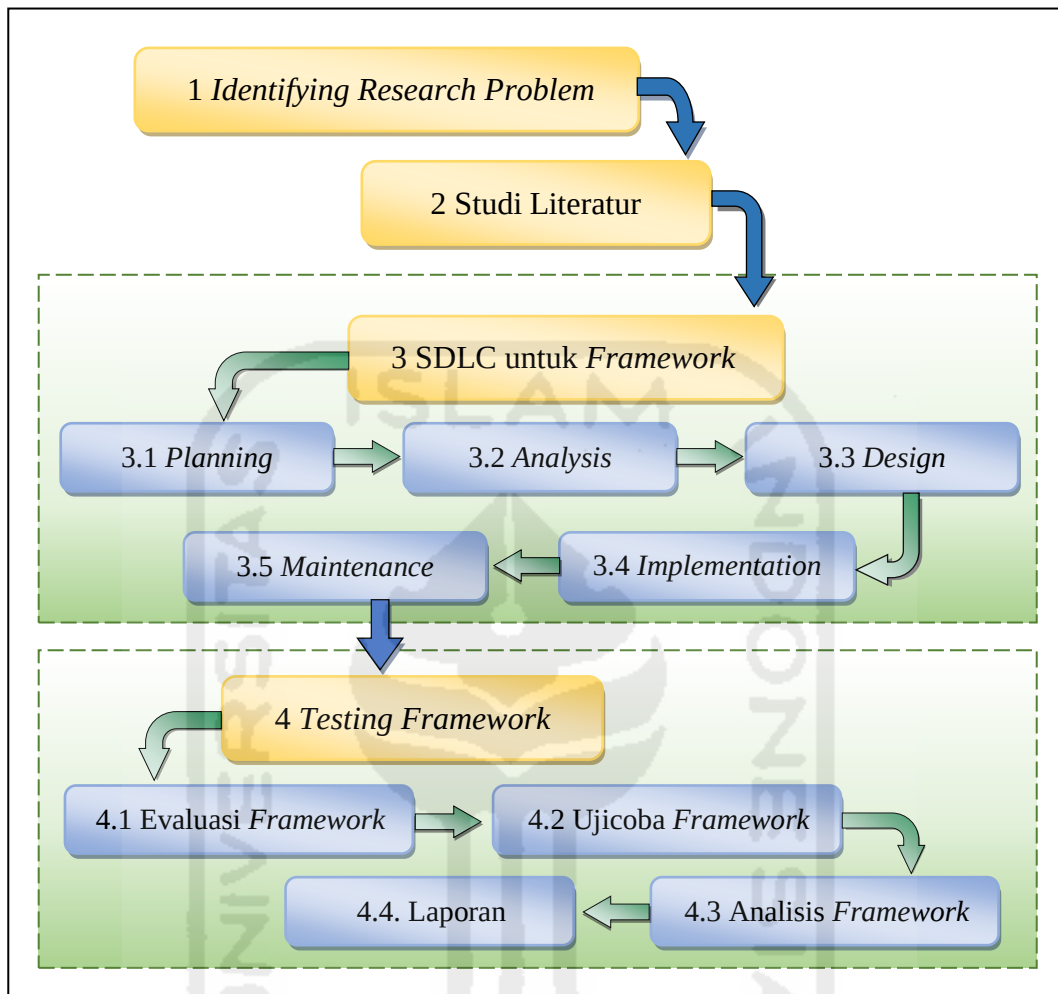
Paper Utama	Teknik Investigasi Email Forensik	Model <i>Framework</i>	Pengembangan <i>Framework</i>
Jafari, F., & Satti, R. S. (2015).	-	<i>Domain specific cyber forensics investigation process model</i>	Menggabungkan 9 jenis <i>framework</i> sebelumnya untuk menghasilkan <i>framework</i> baru.
Devendran, 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).	-	<i>Integrated Digital Forensics Investigation Framework (IDFIF)</i>	Menggabungkan 6 jenis <i>framework</i> dan mengeliminasi tahapan yang sama menjadi satu <i>framework</i> 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	<i>A Framework for the Forensic Investigation of Unstructured Email</i>	Mengembangkan sebuah <i>framework</i> dari Hadjidj, dkk (2009)
Hadjidj, R., Debbabi, M., Lounis, H., Iqbal, F., Szporer, A., & Benredjem, D. (2009).	Menghasilkan 5 modul analisis data email	<i>Towards an integrated e-mail forensic analysis framework. Digital Investigation</i>	Menggabungkan 2 jenis <i>framework</i> dan melakukan analisis terhadap tahapan yang sama menjadi satu <i>framework</i> baru (IEFAF)

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

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