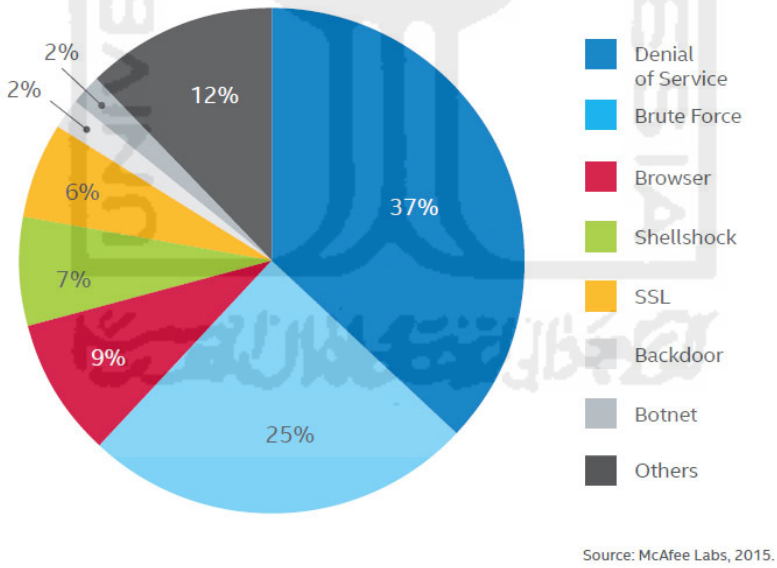
Bab 1 Pendahuluan

1.1 Latar Belakang

Adanya jaringan komputer merupakan salah satu terobosan bagi dunia komputer yang disertai dengan ancaman dan *hacking* jaringan, yang terkait dengan sistem informasi sampai penyalahgunaan data dan informasi. Peningkatan ancaman dan serangan pada keamanan jaringan komputer pada web server dunia seperti terlihat pada Gambar 1.1 dalam laporan (Nguyen, Tran, Ma, & Sharma, 2014) yang masuk di *file log* terlihat paling umum saat ini adalah *Browser, Brute Force, DDoS (Distributed Denial of Service), SSL, Scan, DNS, dan Backdoor*. ("McAfee Labs Threats Report," 2016).



Gambar 1. 1 Top Network Attack

Sumber: Labolatori McAfee ("McAfee Labs Threats Report," 2016)

Serangan web server pada gambar 1.1 membuktikan bahwa semakin banyaknya terjadi kasus *hacking* pada bidang *web server*, serangan yang dapat mengakibatkan akses web lambat,

flooding data, bahkan pencurian informasi dan data melalui jaringan (internet) membuat peretas memiliki banyak waktu untuk melakukan serangan terhadap target serangan (Cahyanto & Prayudi, 2014). Hal tersebut merupakan dampak negatif yang diperoleh dari berkembangnya teknologi jaringan komputer. Berkaitan dengan hal tersebut, muncul suatu bidang teknologi dan komputer yang relatif berkembang pada saat ini, yaitu *network forensic* (Nguyen et al., 2014). *Network forensic* (forensik jaringan) merupakan cabang *digital forensics* yang menggunakan teknik secara ilmiah yang terbukti untuk mengumpulkan, menggunakan, mengidentifikasi, menguji, menganalisis, mendokumentasi ulang dan dapat mempresentasikan barang bukti digital dari beberapa sumber bukti digital dalam memproses dan mengirimkannya dimana bukti ditangkap dari jaringan dan dipresentasikan berdasarkan pengetahuan dari serangan yang di dapat dari *file log* yang berasal dari komputer (forensik komputer) (palmer, 2001).

File log merupakan mekanisme pencatatan yang dilakukan pada sebuah *web server* dengan menyimpan data setiap pengunjung yang mengirimkan permintaan ke *web server* ke dalam suatu file yang dinamakan *file log web server* (Iswardani & Riadi, 2016). Data pengunjung yang terdapat pada *web server log* akan sangat bermanfaat apabila nantinya terdapat suatu permasalahan yang terjadi terhadap *web server*, khususnya apabila terjadi serangan. *Web server* yang sering terindikasi serangan memiliki dampak yang serius maka dalam *web server* harus menerapkan sebuah keamanan jaringan berupa *firewall* yang digunakan untuk mengarahkan paket data yang tidak dikehendaki. Akan tetapi data yang masuk ke dalam *log firewall* mempunyai karakteristik yang tidak dapat dibaca secara langsung, sehingga menyulitkan seorang admin dalam membaca *log file* yang masuk.

Berdasarkan permasalahan tersebut, ada beberapa konsep yang digunakan untuk keamanan jaringan adalah NIDS (*Network Intrusion Detection System*) yang berdasarkan *anomaly* jaringan, HIDS (*Host Intrusion Detection System*) yang berdasarkan *anomaly host* dan khusus untuk forensik digunakan konsep NFAT (*Network Forensik Analysis Tools*). NFAT adalah alat untuk menangkap lalu lintas jaringan, menganalisis lalu lintas jaringan sesuai dengan kebutuhan pengguna, dan memungkinkan pengguna sistem untuk menemukan hal-hal yang berguna dan menarik tentang lalu lintas yang dianalisis (Sindhu & Meshram, 2012)

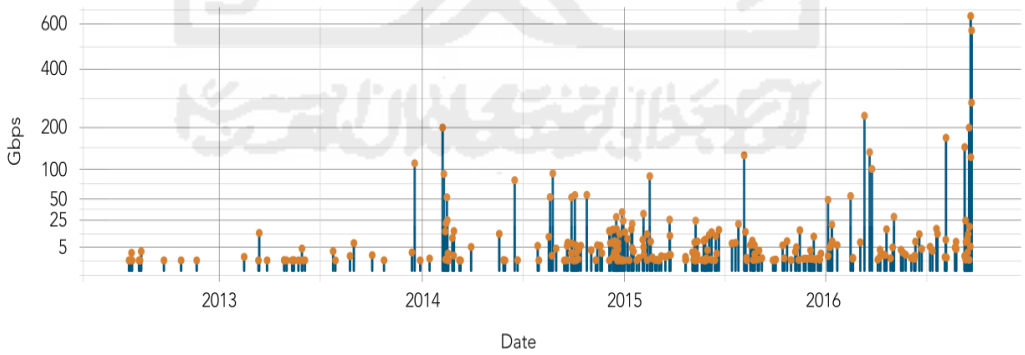
Dalam implementasi NFAT (*Network Forensic Analysis Tool*) bukti pengintaian yang akan dilakukan adalah dengan cara memeriksa protokol TCP (*Transmission Control Protocol*), UDP (*User Datagram Protocol*), IP (*Internet Protocol*), yang melewati trafik jaringan. Sedangkan untuk bukti serangan dan pelanggaran di jaringan akan diketahui jika ada aktivitas yang tidak biasa seperti dalam hal komunikasi jaringan, protokol dan *port*, koneksi ke dalam,

koneksi ke luar, gagal koneksi, dan trafik *pee-to-peer*. (“Guide to Integrating Forensic Techniques into Incident Response,” n.d.)

Untuk memerangi kejahatan pada *web server* digunakan perangkat lunak yang dapat digunakan untuk melakukan identifikasi pelaku terkait dengan serangan web server diantaranya IDS (*Intruction Detection System*) (Stiawan et al., 2012) salah satunya Snort (“Introduction to Snort A . Sniffer Mode,” n.d.). Snort dapat melakukan deteksi adanya penyusupan terhadap *web server* dengan cara menganalisis data log. IDS digunakan sebagai salah satu solusi yang dapat digunakan untuk membantu dan menganalisa paket-paket yang berbahaya.

Pada penelitian forensik jaringan pada web server ini dihususkan untuk mendeteksi serangan *flooding* yang dengan sengaja penyerang mengirimkan serangan untuk mengacaukan atau menghentikan sebuah layanan. Serangan *flooding* berupa serangan DoS (*Denial of Service*) dan DDoS (*Distributed Desnial of Service*) terhadap sebuah server di dalam jaringan (“Design & Deployment Of Testbed Based On ICMPv6 Flooding Attack,” 2014). Namun sayangnya saat ini Snort belum tentu terpasang dalam suatu web server, padahal untuk melakukan konfigurasi Snort bersama *firewall* dapat berkontribusi menjadi solusi permasalahan dalam mendeteksi dan membaca *log* serangan *web server*.

Untuk melakukan konfigurasi Snort tersebut akan diterapkan dalam lingkungan Universitas Muhammadiyah Magelang. Yang mana serangan *flooding* terjadi semakin meningkat cukup signifikan dari tahun ke tahun. Peningkatan statistik serangan *flooding* dapat dilihat pada gambar 1.2.



Gambar 1. 2 Statistik Flooding Attack

Gambar 1.2 menjelaskan statistik grafik peningkatan signifikan antara tahun 2013 hingga 2016. Untuk itu peneliti akan melakukan penelitian yang berfokus pada deteksi serangan fooding, kemudian analisis forensik akan digunakan untuk membantu menganalisis hasil dari deteksi

serangan flooding pada web server pada jaringan komputer di biro Teknologi Informasi dan Komunikasi (TIK) yang merupakan pusat jaringan di Universitas Muhammadiyah Magelang. Maka dari itu diperlukan mekanisme untuk mengkonfigurasikan Snort dalam mendeteksi serangan dan investigasi penyelidikan kasus-kasus yang sering terjadi berdasarkan semua *file log flooding* yang diambil selama penelitian berlangsung.

1.2 Rumusan Masalah

Rumusan masalah dalam penelitian ini adalah:

a. Apakah pemasangan Snort mampu memberikan informasi dalam mendeteksi serangan *flooding*?
b. Bagaimana hasil analisis *file log* Snort dalam menemukan barang bukti digital forensik?

1.3 Batasan Masalah

Didalam melaksanakan kegiatan penelitian ini ada beberapa batasan masalah, yaitu:

a. Uji coba dilakukan dalam lingkungan Universitas Muhammadiyah Magelang.
b. Simulasi serangan diambil dari rekaman Snort yang telah terpasang.
c. Dalam mendapatkan log file serangan ini di ambil di ruang lab biro TIK Universitas Muhammadiyah Magelang.
d. Mendeteksi kinerja serangan *web server* menggunakan Snort.
e. Bukti digital forensik ditinjau dari file log Snort selama simulasi berlangsung.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dibuat maka dapat iambil tujuan penelitian ini sebagai berikut:

a. Pemasangan Snort untuk memberikan informasi dalam mendeteksi serangan *flooding*.
b. Menganalisis *file log* Snort untuk mendapatkan barang bukti digital forensik.

1.5 Manfaat Penelitian

Manfaat yang dapat diperoleh dari hasil penelitian adalah sebagai berikut:

a. Pemasangan Snort untuk memberikan informasi dalam mendeteksi serangan.

b. Mengetahui bukti digital forensik dari *file log* Snort.

1.6 Review Penelitian

Resi Utami Putri (Putri, R U. 2012) forensik jaringan merupakan ilmu keamanan komputer yang berkaitan dengan investigasi untuk menemukan sumber serangan pada jaringan berdasarkan bukti log, mengidentifikasi, menganalisa serta merekontruksi ulang kejadian tersebut. Metode yang digunakan adalah model proses forensik *(The Forensic Proces Model)* yang terdiri dari tahap pengoleksian, pemeriksaan analisis dan pelaporan. Penelitian ini telah mendapatkan 68 IP *Address* yang melakukan tindakan illegal SQL Injection pada server www.ugm.ac.id. Dan kebanyakan penyerang menggunakan tools SQL *injection* yaitu Havij dan SQLMap.

Ismi Junita Rahmawati (Rahmawati, IJ. 2012) *Intruction Berbasis System* (IDS) berbasis jaringan NIDS untuk layananan *Infrastrukture as aService* (IaaS) yang diimplementasikan pada *open cloud computing*. Dengan menggunakan mirroring traffic pada switch, traffic akan diarahkan *traffic* akan diarahkan ke *NIDS* sehingga *NIDS* mampu memantau semua traffic jaringan yang berasal dari luar *server cloud* maupun *traffic* yang antar *virtual machine* di dalam *server cloud*. Tugas utamanya adalah memantau aktivitas yang mencurigakan dari luar *cloud computing* dan antar *host* di dalam *cloud computing* dan memberikan laporan ke administrator jaringan jika ada serangan yang terjadi di lingkungan sistem (Junita Rahmawati, 2012).

Penelitian yang dilakukan Ira Vaoliya Shafitri (Shafitri , I. 2012) Serangan Pada Keamanan Sistem Jaringan Komputer Melalui *Email* , menyatakan bahwa Potensi serangan dapat memyebabkan ancaman yaitu adanya akses tidak terotorisasi pada informasi data dimana hal ini terjadi kelemahan sistem keamanan jaringan komputer dan adanya kesalahan sistem atau kerusakan sistem komputer karena adanya serangan dari *Hacker*. Oleh karena itu dibutuhkan sebuah sistem yang bisa mendeteksi adanya serangan secara *realtime respons*, Intrusion *Detection System (IDS)* adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan intrusi (penyusupan).

(Lipeng, Xingyuan, Huilin, & Wang, 2013) teknologi IDS bertujuan untuk mengidentifikasi intruksi ilegal yang tersembunyi pada jaringan lalu lintas yang diserang, penelitian ini berkomitmen untuk menyediakan sutu metode generasi yang sistematis dan dan ilmiah untuk menghindari berbagai bentuk serangan dengan menggunakan kerangka kerja dan rekomendasi untuk pertahanan dari serangan yang masuk.

Adi Cahyanto Log merupakan sebuah file yang berisi data atau informasi mengenai daftar tindakan, kejadian dan aktifitas yang telah terjadi di dalam suatu sistem. Dari beberapa log yang ada data log tersebut belum tentu sesuai dengan yang diinginkan dan dicari, maka pada saat ini tersedia beberapa aplikasi perangakat lunak salah satunya IDS atau program signature lain untuk dapat melacak keberadaan pelaku yang menggunakan *IP Address log* yang sudah tersimpan untuk menemukan bukti digital dan penelitian ini juga menggunakan DNS *(Domain Name System) blacklist* dan informasi GeoIP untuk mengidentifikasi identitas penyerang yang potensial (Cahyanto & Prayudi, 2014).

Suteva, Natasa Mileva, Aleksandra, Loleski, Mario (Suteva, Mileva, & Loleski, 2014) menggunakan post-mortem komputer analisis forensik baik dari penyerang dan mesin korban, menemukan beberapa artefak. Skenario dari tiga jenis serangan: SQL Injection, XSS, dan inklusi file jarak jauh dengan injeksi byte null. Penyerang yang menggunaan shells untuk serangan, meningalkan bukti pada kedua mesin. Pada mesin penyerang, jejak yang ditemukan di file sejarah browser, browser sementara penyimpanan, dan berkas bash_history. Pada mesin korban, jejak ditemukan dalam sistem file dan file log. Ini artefak dapat membantu untuk mengidentifikasi dan kadang-kadang untuk merekonstruksi serangan, dan bahkan lebih valid untuk bukti pengadilan.

Nattawat Khamphakdee, Nunnapus Benjamas, Saiyan Saiyod. (Khamphakdee, N. Dkk. 2014 dalam keamanan sebuah data dalam suatu organisasi berperan sangat penting yang harus di lidungi untuk mrngurangi resiko dari berbagai macam serangan. Snort *Intrucsion Detection System* adalah salah satu alat keamanan jaringan yang telah banak digunakan untuk mencocokkan lalu lintas paket data dalam penyelidikan berbagai serangan yang masuk. Snort jugan digunakan untuk membandingkan efektifitas serangan yang masuk agar mendapatkan hasil akurasi dengan membandingkan deteksi *scoring* untuk medeteksi waktu. (Khamphakdee, 2014).

Rami Al-Dalky (Al-Dalky, R. 2014) dalam penelitian NIDS dalam beberapa tahun terahir memeliki tingkat kecepatan pemrosesan paket dan *real time* mendeteksi lalu lintas yang berbahaya. Snort yang digunakan sebagai aplikasi threaded satu-satunya pengolahan dalam mendeteksi kemampuan lalu lintas yang masuk. Dalam desain aturan snort diturunkan ke dalam

lapisan hardware berbasis NetFPGA. Dan digunakan brdasarkan Bloom menyaring dalam menganalisis dan menyaring paket ang datang dengan *field header* dengan aturan yang digunakan.

Yogi Surya Nugrogo (Nugroho, Y S. 2015) dalam penelitian analisis dimana tujuannya untuk menginvesigasi dan menganalisis serangan DDOS dengan menggunakan metode Naive Bayes dengan cara mengumpulkan semua file log dan mengklarifikasikan waktu serangan. Digunakan metode Naive Bayes, dalam penelitian ini menunjukkan bahwa:

1. Penelitian ini telah mengklarifikasikan kecepatan dari serangan DDOS baik menggunakan TCP maupun UDP.
2. Penelitian ini dapat menyimpulkan bahwa serangan DDOS menggunakan mengguakan TCP maupun UDP dapat membuat kinerja server lebih berat karena server dikirimkan paket berulang kali.

Penelitian ini dapat menyimpulkan bahwa agar CPU dapat menyimpan traffic log ang akan digunakan sebagai barang bukti maka harus memiliki hardisk yang besar, karena file log yang tersimpa sangatlah besar. (Studi, Informatika, Sains, Teknologi, & Kalijaga, 2015)

Penelitian yang dilakukan Mr. Vrushank Shah, Dr. A.K Aggarwal (Shah, V., Aggarwal. 2015) bahawa serangan DOS adalah situasi penyerang dimana penyerang mencoba untuk mencegah penggunaan dari layanan tertentu untuk merusak layanan target. IDS sistem detksi yang lebih efisien dibandingkan dengan firewall dalam mendeteksi serangan DOS karena lalu lintas internal, namun sistem IDS tunggal terkadang agal dalam mendeteksi serangan baru dan memberikan peringatan palsu yang lebih besar. Penelitian ini menggunakan metode heterogen untun mendeteksi serangan DOS karena lebih efisien dalam mendeteksi alert ang masuk ke dalam sistem IDS. (Shah & Aggarwal, 2015). Agar lebih jelas maka literatur riview dijelaskan pada tabel dibawah ini:

Tabel 1. 1 Tabel Literatur Review

No.	Paper Utama	Metode dan Pendeteksian	Penelitian Serangan Tertinggi		Metode Investigasi	Kesimpulan
			Brute Force	*Flooding Attack*		
1	Resi Utami Putri (2012)	Log untuk mengidentifikasi serangan SQL Injection	–	–	Model Proses Forensik	Mengetahui serangan SQL Injection
2	Ismi Junita Rahmawati (2012)	mirroring traffic pada switch	–	–	–	Memantau aktifitas di luar cloud Computing
3	Ira Vaoliya Shafitri (2012)	NIDS (Network Intrution Detection System)	–	–	–	IDS dapat melakukan inspeksi terhadap lalu lintas inbound dan outbound dalam sebuah sistem atau jaringan
4	Lipeng, Xingyuan, Huilin, & Wang (2013)	Kerangka kerja, dan rekomendasi	√	–	–	menormalkan lalu lintas jaringan dan mendeteksi lalu lintas yang abnormal dengan bebagai teknik serangan
5	Adi Cahyanto (2013)	Mengambil file log	–	–	Hidden Marcov	algorima *forward-backward*, dan algoritma *baum-welch*

Tabel 1. 2 Cont'd Litelatur Review

No.	Paper Utama	Metode dan Pendeteksian	Penelitian Serangan Tertinggi		Metode Investigasi	Kesimpulan
			Brute Force	*Flooding Attack*		
6	Suteva, Natasa Mileva, Aleksandra, Loleski, Mario (2014)	–	–	–	Post-mortem Komputer	Serangan SQL Injection XXS meninggalkan bukti di mesin penyerang dan korban
7	Nattawat Khamphakdee, Nunnapus Benjamas, Saiyan Saiyod (2014)	*Rules Of Network Probe Attack Detection*	–	–	–	Mengelompokkan hasil klarifikasi serangan yang masuk ke dalam lalu lintas web server
8	Rami Al-Dalky (2014)	*NetFPGA-based Bloom Filter*	√	–	–	Penggunaan CPU dalam paket loss saat menggunakan Snort NetFPGA
9	Mr. Vrushank Shah, Dr. A.K Aggarwal (2015)	*IDS alerts for Detecting DOS Attacks*	–	√	–	(DOS, -DOS,) apabila prosentasi $^{\delta}$ DOS atau –DOS
10	Yogi Surya Nugrogo (2015	Mendeteksi DDoS	–	√	Naïve Bayes	Kecepatan dalam menangkal serangan DDoS

Tabel 1. 3 Con't Litelatur Review

No.	Paper Utama	Metode dan Pendeteksian	Penelitian Serangan Tertinggi		Metode Investigasi	Kesimpulan
			Brute Force	*Flooding Attack*		
Usulan Penelitian		NIDS (Network Intrution Detection System) File Log dari snort	√	√	Model Proses Forensik	Menganalisis karakteristik file log NIDS jenis serangan yang dihasilkan dari Snort, Pengujian pemasangan snort dapat memberikan informasi kepada administrator dalam membantu mendeteksi serangan/penyusupan dalam mendapatkan bukti digital forensik.
		Untuk mengurangi resiko serangan, maka diperlukan mekanisme pengaman dalam mengurangi tingkat kerentanan terhadap sebuah sistem *intruction detection* (IDS). IDS ini menggunakan aplikasi *snort* berbasis *open source* yang dapat memberikan *file output* dari *snort* berupa *log Network Intruction Detection System* hususnya Flooding Attack yang mempunyai tingkat serangan tertinggi, maka Snort dapat membantu seorang admin dalam mengimprementasikan *file text* serangan yang sulit dipahami oleh masyarakat awam dan membantu menemukan bukti-bukti digital serangan yang menuju ke server Maka model proses forensik akan membantu dalam memvisualisasikan *file log* serangan agar dapat dipahami oleh masyarakat awam				

1.7 Metode Penelitian

Susunan laporan penelitian ini perlu metodologi penyelesaian secara sistematis, peneltian ini menggunakan beberapa tahap berupa:

Gambar 1. 3 Metodologi Penelitian

1. *Literatur Review*

   Studi litelatur dilakukan untuk mendapatkan informasi mengenai topic penelitian yang dapat bersumber dari dokumen, buku, artikel, atau bahan tertulis lainya yang berupa teori, laporan penelitian, atau penemuan sebelumnya, baik bersifat *online* maupun *offline source*.
2. Identifikasi sistem

   Merupakan tahap perancangan dan implementasi snort yang akan digunakan sebagai objek penelitian.
3. Konfigurasi Snort

   Tahap konfigurasi snort dimulai dari instalasi snort kemudian melakukan konfigurasi snort.
4. Simulasi Kasus

   Merupakan tahap dilakukannya simulasi kasus penggunaan snort dalam mendeteksi adanya penyusupan atau serangan. Simulasi kasus bertujuan untuk melakukan pengujian snort seberapa besar manfaat snort untuk memberikan informasi kepada administrator dalam mendeteksi penyusup atau serangan.
5. Analisis

   Tahap ini dilakukan untuk melakukan investigasi dalam menemukan bukti serangan, mengelompokkan jenis serangan apa yang terjadi, IP siapa yang melakukan serangan, kapan serangan itu terjadi, dimana serangan itu terjadi, bagaimana serangan tersebut bisa terjadi, dan mengapa itu terjadi.
6. Laporan

   Tahap ini dilakukan untuk mereport semua data yang telah di analisis yang digunakan sebagai bukti digital yang sah dan dapat diterima secara umum.

1.8 Sistematika Penulisan

Untuk mempermudah proses pembahasan dalam penelitian, maka dibuat sistematika penulisan pada penelitian ini:

BAB I PENDAHULUAN

Pendahuluan, merupakan pengantar terhadap permasalahan yang akan dibahas. Didalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, manfaat penelitian, tujuan penelitian, metodologi penelitian, serta sistematika penulisan.

BAB II LANDASAN TEORI

Pada Bab ini menjelaskan teori-teori yang digunakan untuk memecahkan masalah dalam penelitian ini. Teori yang dibahas pada bagian ini merupakan teori yang berhubungan dengan *web foensics*

BAB III METODOLOGI PENELITIAN

Bab ini membahas tentang langlah-langkah penelitian dan gambaran umum langkah penyelesaian.

BAB IV PEMBAHASAN

Hasil dan Pembahasan, berisi tentang pembahasan penyelesaian masalah yang diangkat yaitu dengan melakukan analisis dan uji coba.

BAB V KESIMPULAN DAN SARAN

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