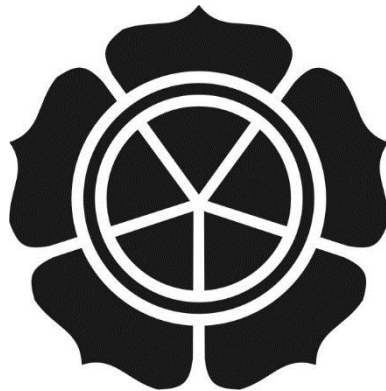


**ANALISIS SERANGAN MALWARE MENGGUNAKAN WIRESHARK
PADA SIMULASI JARINGAN DI MININET**

SKRIPSI



disusun oleh:

Basilus Yance Pramono

12.11.6007

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2015**

**ANALISIS SERANGAN MALWARE MENGGUNAKAN WIRESHARK
PADA SIMULASI JARINGAN DI MININET**

SKRIPSI

Untuk memenuhi sebagian persyaratan
Mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



disusun oleh

Basilus Yance Pramono

12.11.6007

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2015**

PERSETUJUAN

SKRIPSI

**ANALISIS SERANGAN MALWARE MENGGUNAKAN WIRESHARK
PADA SIMULASI JARINGAN DI MININET**


yang dipersiapkan dan disusun oleh

Basilus Yance Pramono

12.11.6007

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 8 September 2015

Dosen Pembimbing,


Bayu Setiaji, M.Kom
NIK. 190302216

PENGESAHAN

SKRIPSI

**ANALISIS SERANGAN MALWARE MENGGUNAKAN WIRESHARK
PADA SIMULASI JARINGAN DI MININET**

yang disusun oleh

Basilus Yance Pramono

12.11.6007

telah dipertahankan di depan Dewan Penguji
pada tanggal 17 September 2015

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Ali Mustopa, M.Kom
NIK. 190302192



Bayu Setiaji, M.Kom
NIK. 190302216



Melwin Syafrizal, S.Kom, M.Eng
NIK. 190302105



Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 29 September 2015



KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001



PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu yang terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggungjawab saya pribadi.

Yogyakarta, 29 September 2015



Basilus Yance Pramono

NIM. 12.11.6007

MOTTO

- ❖ Lihatlah ke atas untuk memacu diri dan lihatlah ke bawah untuk bersyukur.
- ❖ Belajarlah mengalah hingga tak ada seorang pun mampu mengalahkanmu dan belajarlah merendah hingga tak seorang pun mampu merendahkanmu (Gobin Vashdev).
- ❖ Lakukanlah “SEKARANG” terkadang “NANTI” akan menjadi “TIDAK PERNAH”.
- ❖ Saat-saat “LUAR BIASA SULIT” dalam perjuangan adalah “PERTANDA” bahwa “KESUKSESAN SUDAH MENDEKAT”
- ❖ Jangan menunggu karena tidak akan pernah ada waktu yang benar-benar tepat.

PERSEMBAHAN

Puji syukur kepada Tuhan yang maha kuasa, yang telah melimpahkan rahmat serta karuniaNya sehingga tugas akhir ini dapat terselesaikan dengan baik dan lancar.

Dengan segenap hati dan jiwa tugas akhir ini saya persembahkan kepada :

- ❖ Kedua orang tua, Bapak Marianus Sempana dan Ibu tercinta Maria Magdalena Yanti, yang telah memberikan segalanya, yang tak henti – hentinya memberikan doa dan dukungan serta semangat untuk saya.
- ❖ Adik tercinta Melania Fitri telah memberikan doa dan dukungan.
- ❖ Bapak dan Ibu Dosen STMIK AMIKOM Yogyakarta yang telah banyak memberikan ilmu selama penulis kuliah.
- ❖ Sahabat – sahabat saya, Ari, Anas, Azis, Danang, Fani, Bondan, Dono, Riki, Bima, Ikwon yang selalu mendukung dan menyemangati saya.
- ❖ Teman – teman kelas 12S1TI-04 yang selalu membantu, terimakasih banyak bimbingannya.
- ❖ Semua pihak yang telah membantu dalam penyusunan skripsi ini yang tidak dapat disebutkan satu persatu.

KATA PENGANTAR

Puji dan syukur penulis panjatkan untuk Tuhan yang Maha Esa yang telah memberikan rahmat, karunia dan kekuatan sehingga penulis dapat menyelesaikan skripsi yang berjudul **“Analisis Serangan Malware Menggunakan Wireshark Pada Simulasi Jaringan di Mininet”** dapat terselesaikan dengan baik dan tepat waktu.

Skripsi ini disusun sebagai salah satu syarat kelulusan bagi setiap mahasiswa STMIK AMIKOM Yogyakarta. Selain itu juga merupakan suatu bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang program Strata-1 dan untuk memperoleh gelar Sarjana Komputer.

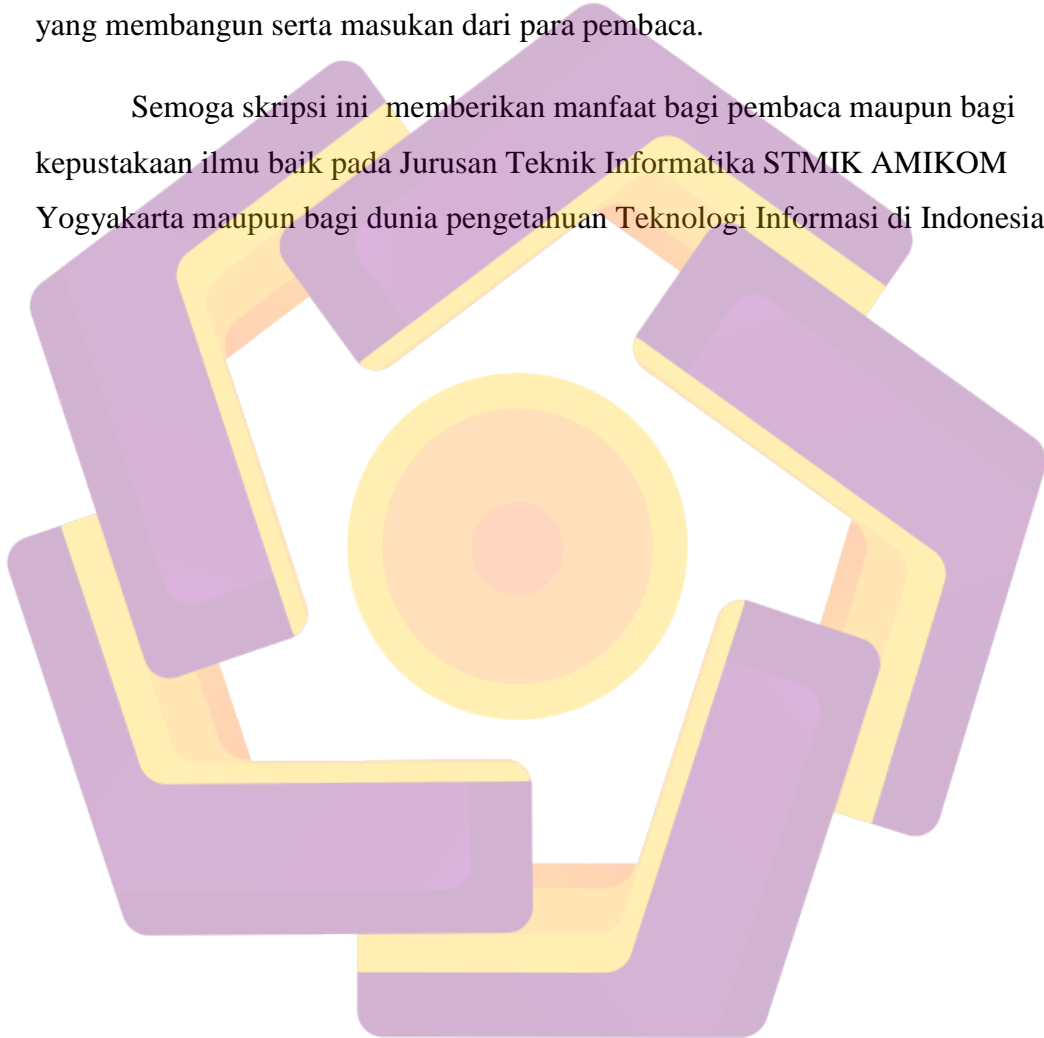
Pembuatan skripsi ini pun tidak lepas dari berbagai pihak yang telah banyak membantu. Untuk itu pada kesempatan ini penulis ingin mengucapkan terima kasih kepada :

1. Tuhan yang maha kuasa atas rahmat-Nya.
2. Orang Tua tercinta Bapak Marianus Sempana dan Ibu Maria Magdalena Yanti serta adik saya Melania Fitri yang banyak memberikan bantuan moril, material, arahan dan selalu mendoakan keberhasilan dan keselamatan selama menempuh pendidikan.
3. Bapak Prof. Dr. M. Suyanto, M.M selaku ketua Sekolah Tinggi Manajemen Informatika dan Komputer STMIK AMIKOM Yogyakarta.
4. Bapak Sudarmawan, MT selaku ketua jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
5. Bayu Setiaji, M.Kom selaku dosen pembimbing yang telah banyak membantu dan membimbing dalam proses pengerjaan skripsi ini.
6. Bapak dan Ibu Dosen STMIK AMIKOM Yogyakarta yang telah banyak memberikan ilmu selama penulis kuliah.
7. Teman-teman 12 S1-TI-04

8. Semua pihak yang tidak dapat penulis sebut satu persatu yang telah membantu dalam penyelesaian penulisan skripsi ini.

Dalam pelaksanaan dan pembuatan program serta skripsi ini saya menyadari bahwa masih banyak kekurangan-kekurangan baik yang disadari maupun tidak disadari, oleh karena itu saya sangat mengharapkan kritik dan saran yang membangun serta masukan dari para pembaca.

Semoga skripsi ini memberikan manfaat bagi pembaca maupun bagi kepastakaan ilmu baik pada Jurusan Teknik Informatika STMIK AMIKOM Yogyakarta maupun bagi dunia pengetahuan Teknologi Informasi di Indonesia.



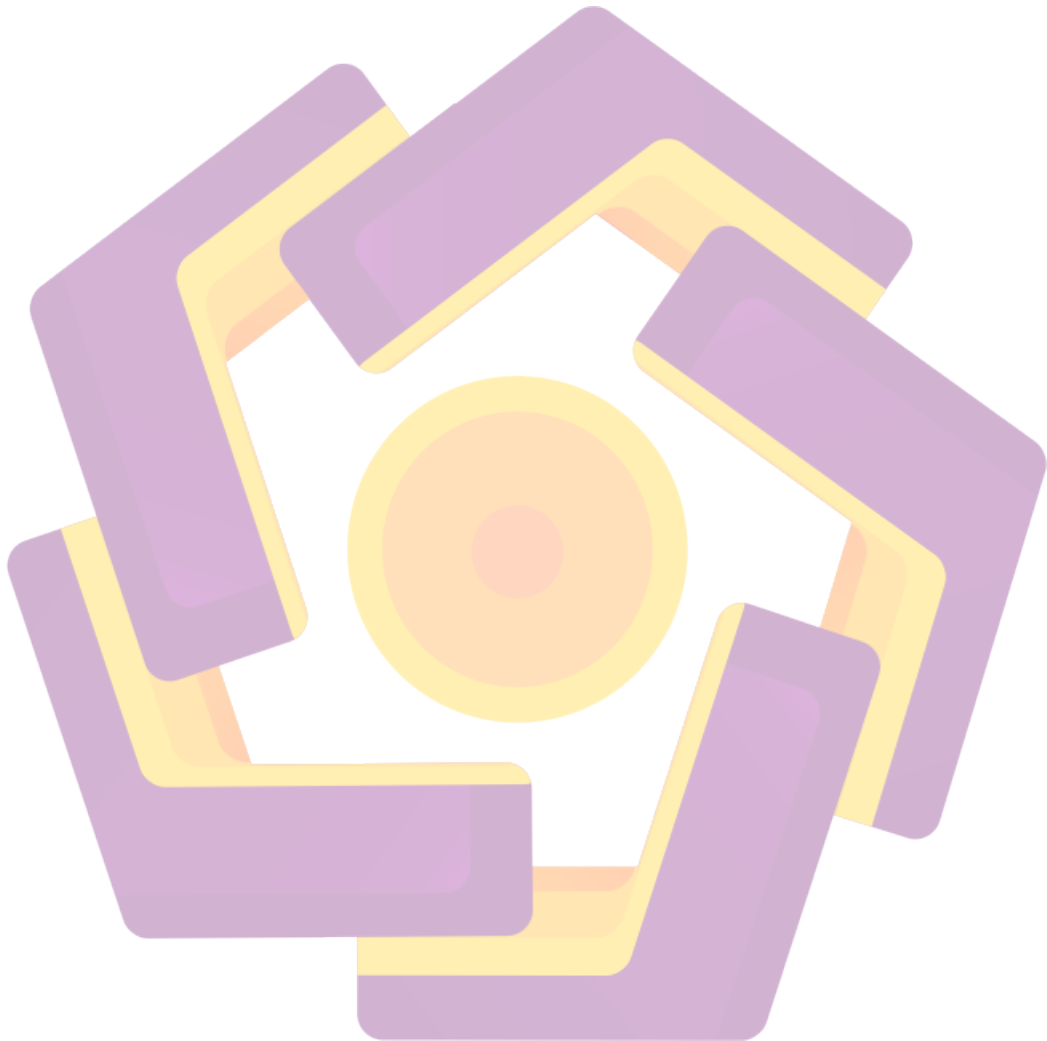
DAFTAR ISI

COVER.....	i
PERSETUJUAN.....	ii
PENGESAHAN.....	iii
PERNYATAAN.....	iv
MOTTO.....	v
PERSEMBAHAN.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL.....	xiii
DAFTAR GAMBAR.....	xiv
INTISARI.....	xvi
ABSTRACT.....	xvii
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang Masalah.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah.....	3
1.4 Maksud dan Tujuan Penelitian.....	3
1.5 Metode Penelitian.....	4
1.5.1 Metode Pengumpulan Data.....	4
1.5.2 Metode Analisis.....	4
1.5.3 Metode Pengembangan.....	5
1.5.4 Metode Testing.....	5
1.6 Sistematika Penulisan.....	5
BAB II LANDASAN TEORI.....	7
2.1 Tinjauan Pustaka.....	7
2.2 Dasar Teori.....	9
2.2.1 Pengertian Jaringan Komputer.....	9
2.2.1.1 Peer to Peer.....	9
2.2.1.2 Client-Server.....	10

2.2.2	Sejarah Jaringan Komputer.....	11
2.2.3	Mininet.....	15
2.2.4	Firewall.....	15
2.2.5	Malware.....	15
2.2.5.1	Malware Tipe Infeksi.....	16
2.2.5.2	Malware Tipe Terselubung.....	17
2.2.5.3	Malware Tipe Profit-Oriented.....	18
2.2.6	Wireshark.....	20
2.2.7	Topologi Jaringan.....	21
2.2.7.1	Topologi Bus.....	21
2.2.7.2	Topologi Ring.....	22
2.2.7.3	Topologi Star.....	23
2.2.7.4	Topologi Daisy-Chain (Linier).....	24
2.2.7.5	Topologi Tree/ Hierarchical.....	25
2.2.7.6	Topologi Mesh dan Full Connected.....	26
2.2.7.7	Topologi Hybrid.....	27
2.2.8	Protokol-Protokol Jaringan.....	27
2.2.8.1	TCP/IP.....	27
2.2.8.2	IPX/SPX.....	28
2.2.8.3	NETBIOS.....	29
2.2.8.4	DECNet.....	30
2.2.8.5	PPP.....	30
2.2.8.6	AppleTalk.....	31
2.2.8.7	SNA.....	31
2.2.8.8	SNMP.....	32
2.2.8.9	SLIP.....	33
2.2.9	Analisis Malware.....	33
2.2.9.1	Teknik Analisa.....	35
BAB III ANALISA DAN PERANCANGAN SISTEM.....		36
3.1	Desain Arsitektur Jaringan.....	36
3.2	Gambaran Umum Tentang Malware.....	36

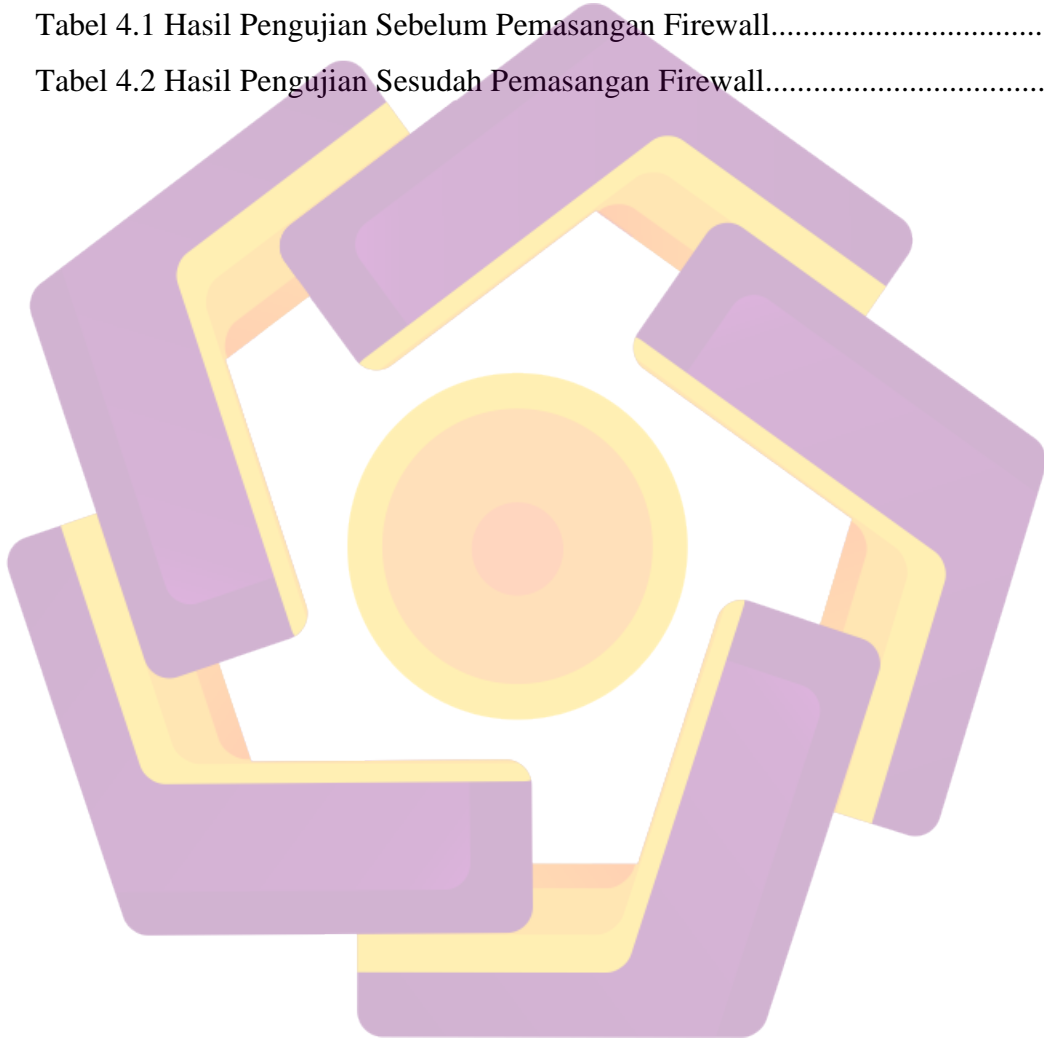
3.3	Tahap-Tahap Penelitian.....	37
3.4	Analisis Masalah.....	38
3.5	Analisa Keamanan Jaringan.....	38
3.6	Analisa Kebutuhan Sistem.....	39
3.6.1	Kebutuhan Perangkat Keras.....	39
3.6.2	Kebutuhan Perangkat Lunak.....	40
3.7	Alasan Melakukan Analisa Malware.....	41
3.8	Skenario Penyerangan.....	41
3.9	Hipotesis Solusi.....	42
BAB IV IMPLEMENTASI DAN PEMBAHASAN.....		43
4.1	Implementasi.....	43
4.1.1	Instalasi Mininet.....	43
4.2	Pembahasan.....	47
4.2.1	Tampilan Konfigurasi.....	47
4.2.2	Tampilan xterm Penyerang.....	48
4.2.3	Tampilan xterm Target.....	49
4.2.4	Tampilan xterm Analisis 1.....	50
4.2.5	Tampilan xterm Analisis 2.....	51
4.2.6	Wireshark Analyzer.....	52
4.3	Pengujian Sistem.....	52
4.3.1	Pengujian pada Komputer Penyerang.....	52
4.3.2	Pengujian pada Komputer Analisis.....	53
4.4	Pembahasan.....	56
4.4.1	Analisis Traffic.....	56
4.4.2	Analisa Protokol.....	56
4.5	Firewall.....	58
4.6	Rekomendasi.....	60
BAB V PENUTUP.....		62
5.1	Kesimpulan.....	62
5.2	Saran.....	62
DAFTAR PUSTAKA.....		64

LAMPIRAN



DAFTAR TABEL

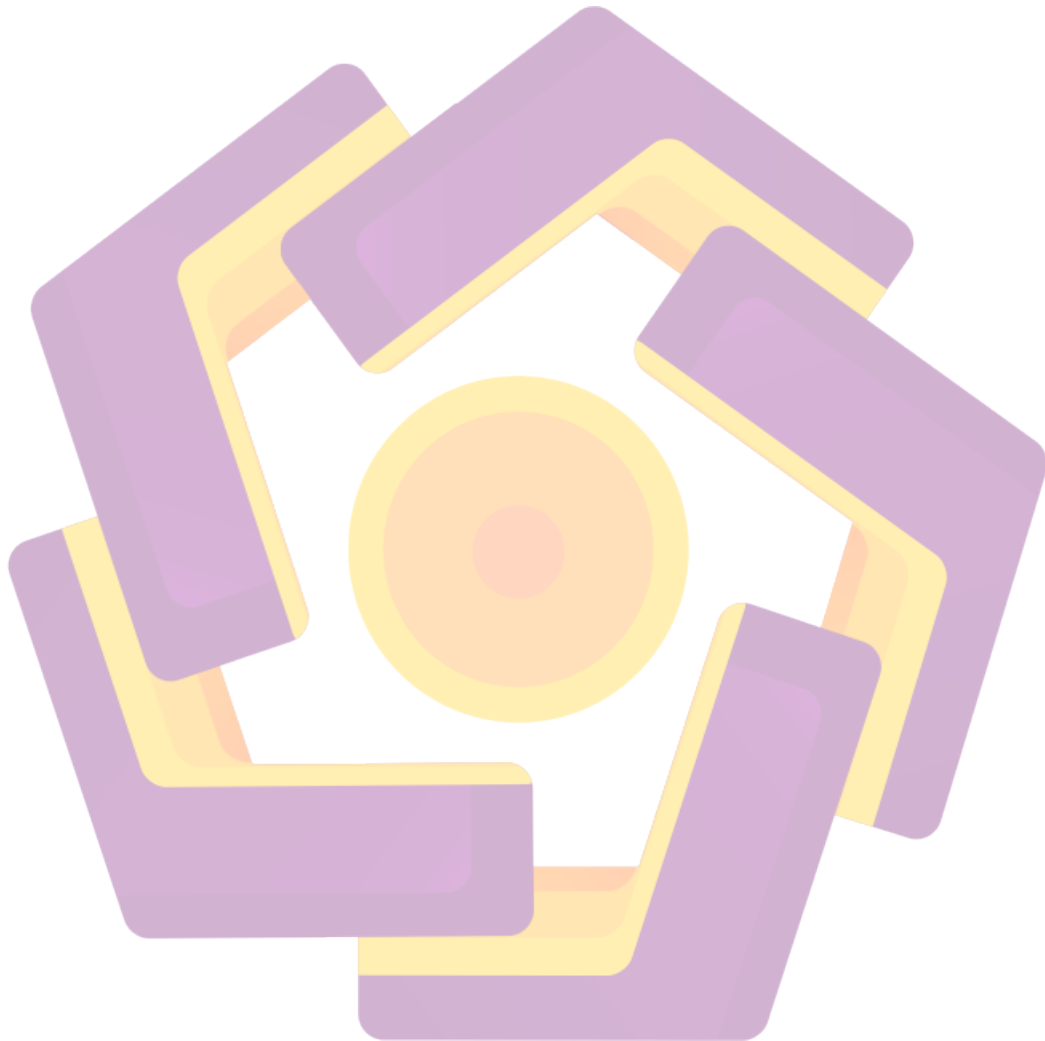
Tabel 2.1 Total Malware yang Diunduh.....	7
Tabel 2.2 Model Lapisan Pada Network Netware.....	29
Tabel 2.3 Protokol AppleTalk dan Lapisan Model OSI.....	31
Tabel 3.1 Spesifikasi Laptop.....	40
Tabel 4.1 Hasil Pengujian Sebelum Pemasangan Firewall.....	61
Tabel 4.2 Hasil Pengujian Sesudah Pemasangan Firewall.....	61



DAFTAR GAMBAR

Gambar 2.1	<i>Peer to Peer</i>	10
Gambar 2.2	<i>Model Client-Server dengan Delicated Server</i>	11
Gambar 2.3	Jaringan Komputer Model TSS.....	12
Gambar 2.4	Jaringan Komputer Model Distributed Processing.....	14
Gambar 2.5	Topologi Bus.....	22
Gambar 2.6	Topologi Ring.....	23
Gambar 2.7	Topologi Star.....	24
Gambar 2.8	Topologi Linier.....	25
Gambar 2.9	Topologi Tree.....	25
Gambar 2.10	Topologi Mesh.....	26
Gambar 2.11	Topologi Hybrid.....	27
Gambar 3.1	Desain Arsitektur Jaringan.....	36
Gambar 3.2	Tahap-Tahap Penelitian.....	37
Gambar 3.3	Grafik Jenis Penyusupan Keamanan Jaringan 2014.....	38
Gambar 4.1	Proses Update Packet.....	44
Gambar 4.2	Proses Upgrade Packet.....	45
Gambar 4.3	Install Git di Linux.....	46
Gambar 4.4	Instalasi Mininet.....	47
Gambar 4.5	Tampilan Konfigurasi.....	48
Gambar 4.6	Tampilan Xterm Penyerang.....	49
Gambar 4.7	Tampilan Xterm Target.....	50
Gambar 4.8	Tampilan Analisis 1.....	51
Gambar 4.9	Tampilan Analisis 2.....	52
Gambar 4.10	Tampilan Wireshark Analyzer Tool.....	52
Gambar 4.11	Tampilan Penyerang Berhasil Memanggil Malware.....	53
Gambar 4.12	Proses Analisis 1 Berjalan.....	54
Gambar 4.13	Proses Analisis 2 Berjalan.....	55
Gambar 4.14	Tampilan Proses Keseluruhan.....	55
Gambar 4.15	Tampilan Traffic Data.....	56

Gambar 4.16	Gambaran Sebelum Protokol TCP di Buka.....	57
Gambar 4.17	Tampilan Isi Protokol TCP.....	57
Gambar 4.18	Tampilan Pemasangan Firewall.....	58
Gambar 4.19	Tampilan Setelah Pemasangan Firewall.....	59
Gambar 4.20	Tampilan Traffic Data Setelah Pemasangan Firewall.....	60



INTISARI

Komputer yang terhubung ke internet akan memperbesar kemungkinan terjadinya ancaman atau gangguan terhadap keamanan sistem jaringan. *Malware* dalam bentuk *virus*, *worm*, dan *trojan horses* merupakan ancaman bagi keamanan dalam jaringan komputer. *Malware* telah dirancang seaneh mungkin untuk membuat celah didalam sistem. Setiap orang mengalami kemungkinan besar untuk terserang *malware* dalam sistem komputer yang dimiliki karena *malware* dapat menyerang melalui media disk maupun internet, sms, chat.

Banyak yang beranggapan serangan *malware* dapat ditangani dengan antivirus. *Malware* mempunyai sistem pertahanan sendiri dan sangat dimungkinkan untuk menyembunyikan diri dari antivirus pada komputer atau bahkan bahayanya bisa menginfeksi antivirus itu sendiri. Dengan alasan tersebut dibutuhkan sebuah solusi dari serangan *malware*. Analisis serangan *malware* menekankan pada proses monitoring. Monitoring untuk melihat terjadi serangan *malware* pada sistem komputer dapat dilihat dengan wireshark pada simulator mininet.

Dalam penelitian ini dilakukan pada jaringan dengan menggunakan wireshark pada simulator mininet bertujuan untuk mengetahui serangan *malware* pada sistem komputer untuk memberikan proteksi. Pada tahap ini pemasangan firewall dan antivirus akan meminimalisir serangan *malware* dengan membatasi port yang diakses. *Malware* dapat ditangani dengan mengetahui cara kerja kemudian dianalisa untuk mengetahui informasi yang dibawa oleh *malware* ketika melakukan serangan kedalam sistem komputer.

Kata kunci : Malware, Mininet, Wireshark, Firewall, Jaringan

ABSTRACT

A computer connected to the internet will enlarge the possibility of threat or disruption of network system security. Malware in the form of viruses, worms, and trojan horses is a threat to the security in computer networks. Malware has been designed as powerful as possible to create a loophole in the system. Each person's experience is likely to be stricken with malware in computer systems owned because malware can invade through the disk media or the internet, sms, chat.

Many who assume malware attacks can be dealt with antivirus. Malware has its own defense system and it is very possible to hide itself from antivirus on a computer or even the danger could infect the antivirus itself. With the excuse it needs a solution from malware attacks. Analysis of malware attacks highlight the monitoring process. Monitoring to see the occurred malware attacks on computer systems can be seen with wireshark on a simulator dimininet.

In the study conducted on the network using wireshark on a simulator mininet aims to know the attacks of malware on your computer system to provide protection. At this stage of the installation of firewall and antivirus will minimize malware attacks by limiting the ports are accessible. Malware can be handled by knowing how to work and then analyzed to find out the information carried by the malware when an attack into the computer system.

Keywords: Malware, Mininet, Wireshark, Firewall, Jaringan