ANALISIS FORENSIK JARINGAN *VIRTUAL ROUTER* MENGGUNAKAN *FRAMEWORK NIST SP800-86*

SKRIPSI

disusun oleh

Koresy Butarbutar

16.11.0779

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

ANALISIS FORENSIK JARINGAN *VIRTUAL ROUTER* MENGGUNAKAN *FRAMEWORK NIST SP800-86*

SKRIPSI

disusun oleh

Koresy Butarbutar

16.11.0779

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

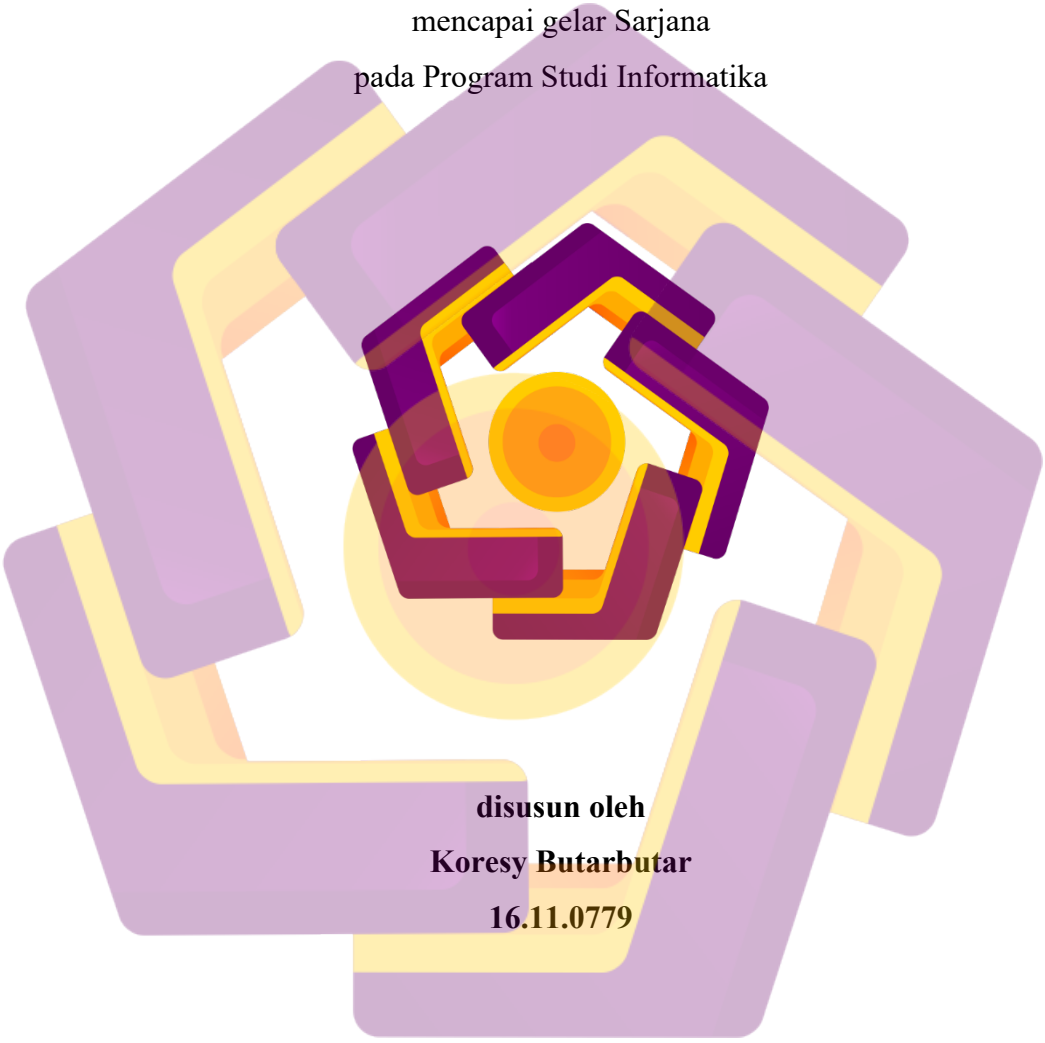
ANALISIS FORENSIK JARINGAN *VIRTUAL ROUTER* MENGGUNAKAN *FRAMEWORK NIST SP800-86*

SKRIPSI

untuk memenuhi sebagian persyaratan

mencapai gelar Sarjana

pada Program Studi Informatika



disusun oleh

Koresy Butarbutar

16.11.0779

PROGRAM SARJANA
PROGRAM STUDI INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2021

PERSETUJUAN

SKRIPSI

ANALISIS FORENSIK JARINGAN *VIRTUAL ROUTER* MENGGUNAKAN *FRAMEWORK NIST SP800-86*

yang dipersiapkan dan disusun oleh

Koresy Butarbutar

16.11.0779

telah disetujuai oleh Dosen Pembimbing Skripsi

pada tanggal 5 Februari 2021

Dosen Pembimbing,

Ali Mustopa, M.Kom

NIK. 190302105

PENGESAHAN

SKRIPSI

ANALISIS FORENSIK JARINGAN *VIRTUAL ROUTER* MENGGUNAKAN *FRAMEWORK NIST SP800-86*

yang dipersiapkan dan disusun oleh

Koresy Butarbutar

16.11.0779

telah dipertahankan di depan Dewan Penguji
pada tanggal 18 Februari 2021

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Ali Mustopa, M.Kom **NIK. 190302105**	_____
Ahlihi Masruro, M.Kom **NIK. 190302148**	_____
Ainul Yaqin, M.Kom **NIK. 190302255**	_____

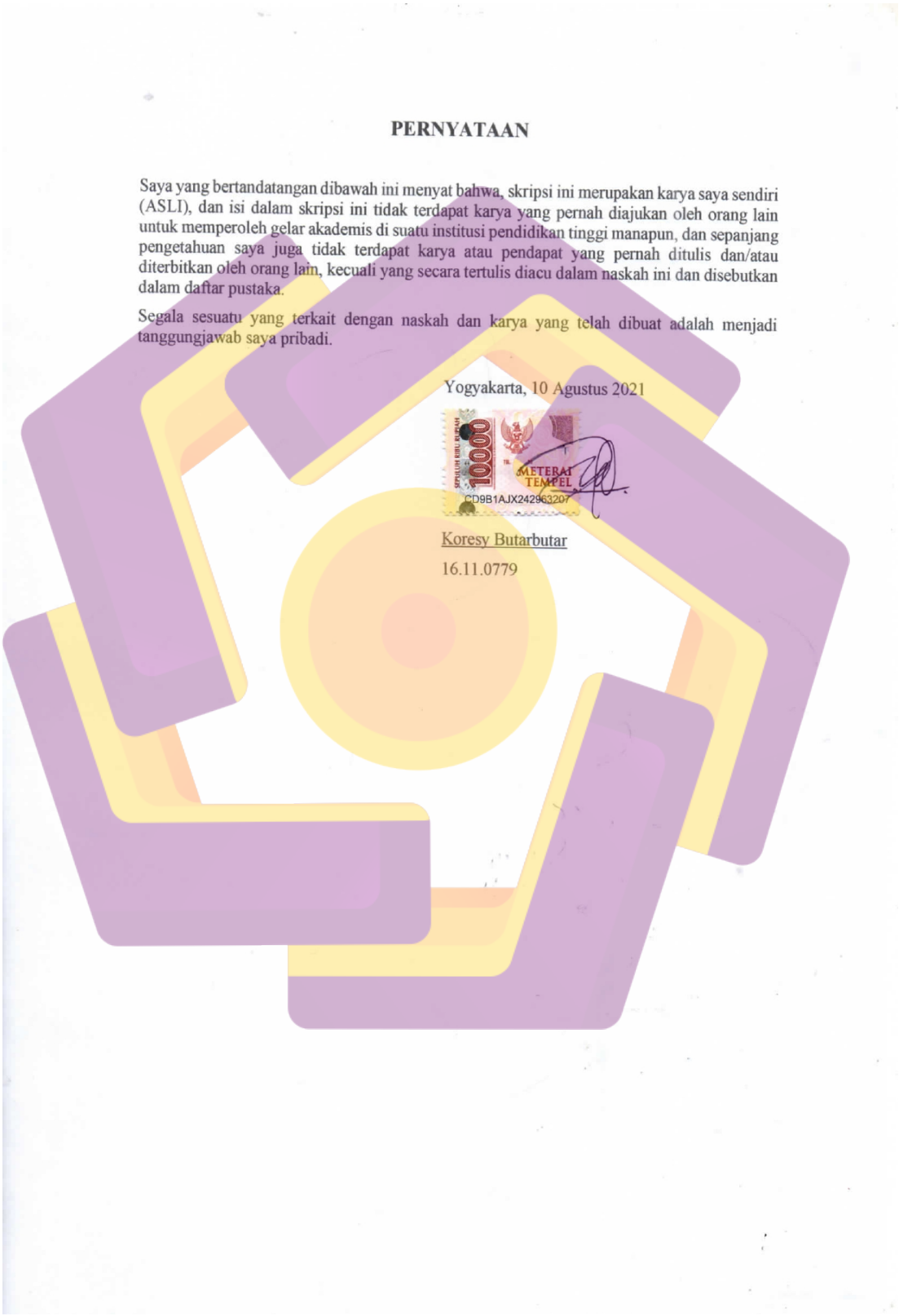
Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 18 Februari 2021

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, M.Kom

NIK. 190302096

PERNYATAAN



PERNYATAAN

Saya yang bertandatangan dibawah ini menyat 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, 10 Agustus 2021

Koresy Butarbutar

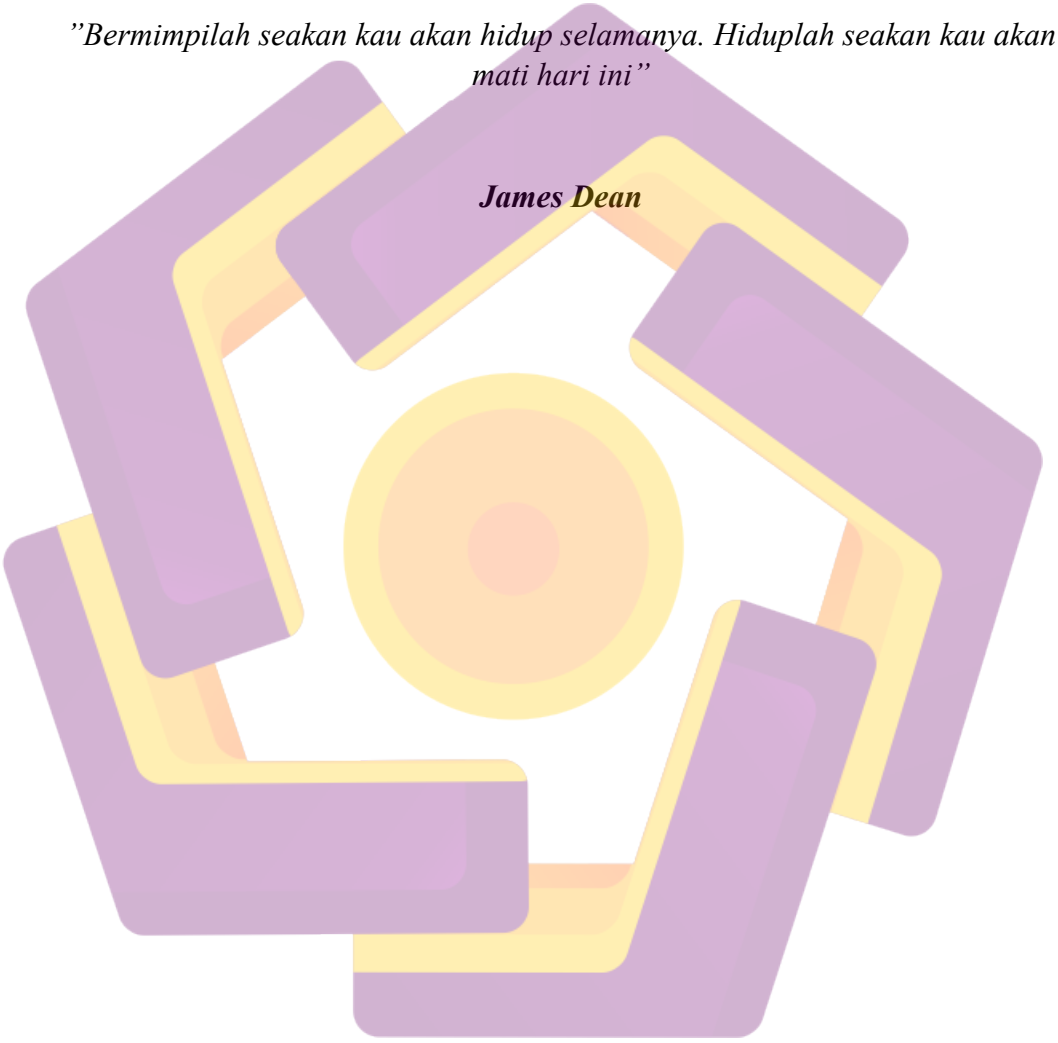
16.11.0779

MOTTO

” Juara adalah pecundang yang berhasil bangkit dan mencoba sekali lagi”

”Bermimpilah seakan kau akan hidup selamanya. Hiduplah seakan kau akan mati hari ini”

James Dean



PERSEMBAHAN

Puji syukur saya panjatkan kehadirat Tuhan Yesus Kristus yang telah memberikan nikmat dan berkat yang luar biasa kepada saya, sehingga saya dapat menyelesaikan skripsi ini dengan baik dan selalu diberi kemudahan dalam pengerjaannya. Penelitian ini tak lepas dari dukungan doa serta semangat dari orang-orang spesial yang berada di dekat saya, oleh karena itu saya ingin mempersembahkan dan mengucapkan terimakasih kepada :

1. Bapak Meris Butarbutar dan Ibu Risma Simanjuntak selaku orang tua yang telah memberikan dukungan dalam bentuk apapun dan dengan ikhlas diberikan kepada saya. Terimakasih karena sudah mau mengorbankan banyak hal untuk kebahagiaan anakmu ini sebagai alasan saya untuk menyelesaikan skripsi ini.
2. Seluruh keluarga, saudara, dan sahabat yang selalu memberikan semangat dan dukungan untuk menyelesaikan skripsi ini.
3. Seluruh saudara PERMATA di Yogyakarta, terkhusus Anak Jayapura Angkatan 16 Universitas Amikom yang telah memberikan semangat, dukungan, dalam proses pengerjaan skripsi ini. Nama kalian tidak ditulis dalam persembahan ini, tetapi akan selalu saya ingat selama hidup saya.
4. Teman-teman 16 S1IF 12 untuk kenangan indah yang pernah kita lewati bersama selama perkuliahan. Terimakasih atas semua bantuan dan ilmu yang pernah kalian bagi kepada saya.

KATA PENGANTAR

Segala puji dan syukur kepada Tuhan Yesus Kristus, berkatnya peneliti dapat menyelesaikan skripsi yang berjudul ANALISIS FORENSIK JARINGAN *VIRTUAL ROUTER* MENGGUNAKAN *FRAMEWORK NIST SP800-86*, Skripsi ini ditujukan untuk memenuhi salah satu syarat kelulusan program sarjana pada jurusan Informatika, Universitas Amikom Yogyakarta.

Penulis sangat menyadari bahwa dalam penulisan skripsi ini sangat jauh dari kesempurnaan. Walaupun sangat sederhana, tanpa bantuan dari berbagai pihak pastinya penulis akan mengalami berbagai macam kesulitan. Oleh karena itu dalam kesempatan ini, penulis mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. M. Suyanto, M.M. selaku Rektor Universitas Amikom Yogyakarta.
2. Bapak Hanif Al Fatta, M.Kom selaku Dekan Fakultas Ilmu Komputer Jurusan Informatika Universitas Amikom Yogyakarta.
3. Bapak Ali Mustopa M.Kom selaku dosen pembimbing.
4. Bapak dan Ibu Dosen Universitas Amikom Yogyakarta yang telah banyak memberikan ilmunya selama penulis kuliah.
5. Kedua orang tua dan saudara-saudara yang selalu mendukung penulis dalam segala hal.

Peneliti menyadari masih banyak kekurangan yang ada dalam skripsi ini dan semoga skripsi ini dapat bermanfaat bagi peneliti dan pembacanya.

Yogyakarta, 8 Agustus 2021

Koresy Butarbutar

NIM. 16.11.0779

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Jaringan komputer berkembang dengan sangat pesat, baik di instansi-instansi komersil, dunia akademik, bahkan rumah-rumah penduduk yang membutuhkan akses internet. Internet merupakan sebuah singkatan dari *Interconnection Networking*, atau yang berarti jaringan yang terhubung secara luas. Internet merupakan keterkaitan jaringan komputer melalui standard yang disebut *global Transmission Control Protocol atau Internet Protocol TCP/IP* yang terdapat sistem pertukaran paket komunikasi yang berasal melalui data.

Penelitian ini mengimplementasikan jaringan *virtual router* sebagai objek peninjauan lalu lintas jaringan yang berjalan pada perangkat keras router dengan pemanfaatan alat analisis jaringan pada sistem operasi *windows*. Kerangka kerja yang digunakan dalam penelitian adalah *National Institute of Standards and Technology (NIST)*. Penelitian diakhiri dengan penemuan bukti lalu lintas yang tidak biasa menggunakan alat analisis forensik *Wireshark dan Microsoft Network Monitor*.

Pengungkapan bertujuan untuk dapat menemukan IP *address* penyusup dari aplikasi *wireshark* dan *Microsoft Network Monitor*, dengan melakukan analisis bukti paket jaringan yang telah disiapkan. Lalu lintas jaringan telah berhasil di rekam secara langsung dengan menggunakan alat *Wireshrak*, dilanjutkan dengan memvalidasi bukti antara alat analisis *wireshark* dan *microsoft network monitor*. Hasil analisis forensik jaringan *virtual router* menggunakan *framework nist SP800-86* adalah penyerangan benar terjadi, terbukti pada protokol *ARP*, bahwa komunikasi terputus antara 192.168.10.5 sebagai klien dengan 192.168.10.254 sebagai server akibat dari *broadcast* secara terus menerus yang dilakukan oleh alamat 192.168.10.252 dan alamat 192.168.20.253. Berdasarkan penelitian ini pada kerangka kerja *NIST* menggunakan sistem yang telah dibangun dengan objek *virtual router* dapat digunakan analis untuk mendeteksi serangan siber secara konsisten.

Kata kunci : Jaringan, Analisis

ABSTRACT

Computer networks are developing very rapidly, both in commercial institutions, in the academic world, and even in people's homes that need internet access. Internet is an acronym for Interconnection Networking, or which means a network that is widely connected. The Internet is a computer network linkage through a standard called the global Transmission Control Protocol or Internet Protocol TCP / IP, which has a system of exchanging communication packets originating through data.

This study implements a virtual router network as an object for reviewing network traffic running on router hardware by utilizing network analysis tools on the Windows operating system. The framework used in the research is the National Institute of Standards and Technology (NIST). The research will end with the discovery of unusual traffic evidence using the Wireshark forensic analysis tool and Microsoft Network Monitor.

The disclosure aims to be able to find the intruder's IP address from the Wireshark application and Microsoft Network Monitor, by analyzing evidence of network packets that have been prepared. Network traffic has been recorded directly using the Wireshrak tool, followed by validating the evidence between the Wireshark analysis tool and the Microsoft Network Monitor. The results of the virtual router network forensic analysis using the nist SP800-86 framework are true attacks, proven by the ARP protocol, that communication is lost between 192.168.10.5 as a client and 192.168.10.254 as a server as a result of continuous broadcast which is also proven in the ICMP protocol. Based on this research, the NIST framework uses a system that has been built with a virtual router object that analysts can use to detect cyber attacks consistently.

Keyword : Network, Analysis