

**ANALISIS SERANGAN *DDOS* PADA *RESOURCE SERVER*  
MENGUNAKAN *WIRESHARK***

**SKRIPSI**



Disusun Oleh

**Ahmad Fauzi Irwan**

**15.11.9302**

**PROGAM SARJANA  
PROGAM STUDI INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS AMIKOM YOGYAKARTA  
YOGYAKARTA**

**2021**

**ANALISIS SERANGAN *DDOS* PADA *RESOURCE SERVER*  
MENGUNAKAN *WIRESHARK***

**SKRIPSI**

untuk memenuhi persyaratan  
mencapai gelar Sarjana  
pada Program Studi Informatika



disusun oleh

**Ahmad Fauzi Irwan**

**15.11.9302**

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

# PERSETUJUAN

## SKRIPSI

### ANALISIS SERANGAN *DDOS* PADA *RESOURCE SERVER* MENGUNAKAN *WIRESHARK*

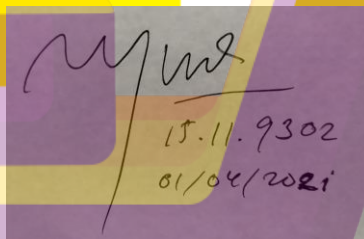
yang dipersiapkan dan disusun oleh

**Ahmad Fauzi Irwan**

**15.11.9302**

telah disetujui oleh Dosen Pembimbing Skripsi  
pada tanggal  
1 April 2021

**Dosen Pembimbing**



Handwritten signature and stamp of the supervisor, Yudi Sutanto, with the student ID 15.11.9302 and the date 01/04/2021.

**Yudi Sutanto, S.Kom, M.Kom.**

**NIK. 190302039**

# PENGESAHAN

## SKRIPSI

### ANALISIS SERANGAN *DDOS* PADA *RESOURCE SERVER* MENGUNAKAN *WIRESHARK*

yang dipersiapkan dan disusun oleh

**Ahmad Fauzi irwan**

**15.11.9302**

telah dipertahankan di depan Dewan Penguji

pada tanggal

**Nama Penguji**

**Tanda Tangan**

**Andika Agus Slameto. M.Kom**

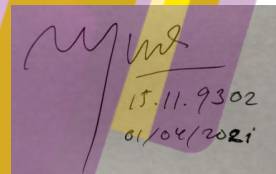
**NIK. 190302109**

**Mulia Sulistyono. M.Kom**

**NIK. 190302248**

**Yudi Sutanto. M.Kom**

**NIK. 190302039**



Handwritten signature and date: 15.11.9302  
01/04/2021

Skripsi ini telah diterima sebagai salah satu persyaratan

untuk memperoleh gelar Sarjana Komputer

Tanggal 1 April 2021

**DEKAN FAKULTAS ILMU KOMPUTER**

**Hanif AlFatta. M.Kom**

**NIK. 190302096**

## 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, 21 April 2021



Ahmad Fauzi Irwan

NIM. 15.11.9302

## MOTTO

*“A lesson without pain is meaningless. For you cannot gain something without sacrificing something else in return. But once you have recovered it and made it your own. You will gain an irreplaceable heart.”*

**- Edward Elric -**

“Tidak ada pengalaman sia-sia, yang terpenting adalah kau bisa memanfaatkannya atau tidak.”

**- World Trigger -**

“Jika kau tau banyak pilihan namun tak mengambil pilihan itu maka hidupmu akan membosankan.”

**- Haikyuu -**

## PERSEMBAHAN

Alhamdulillah segala puji syukur atas kehadiran Allah SWT yang telah memberikan limpahan rahmat dan karunia-Nya sehingga penelitian ini dapat dilakukan dan diselesaikan dengan sebaik-baiknya. Penulis juga ucapkan terimakasih untuk dukungan dan bantuan semua pihak yang membantu selesainya penelitian ini. Ucapan terimakasih saya persembahkan kepada :

1. Kedua orang tua dan semua keluarga yang senantiasa memberikan dukungan dan do'a kepada saya.
2. Bapak Yudi Susanto, S.Kom, M.Kom selaku dosen pembimbing yang telah banyak memberikan bimbingan, pelajaran, serta ilmu yang sangat bermanfaat.
3. Teman-teman kelas 15-S1IF-12 yang menjadi teman seperjuangan dari awal perkuliahan hingga saat ini.
4. Sahabat-sahabat rantau, yang banyak memberikan dukungan dan kritik menuliskan skripsi ini.
5. Yesi Rahmawati, S.S, yang telah membatu dalam proses penulisan skripsi dari awal sampai selesai.
6. Sahabat nongki kelas 12 yang sudah menemani, memberikan dorongan dan bersenang-senang bersama selama perkuliahan

## DAFTAR ISI

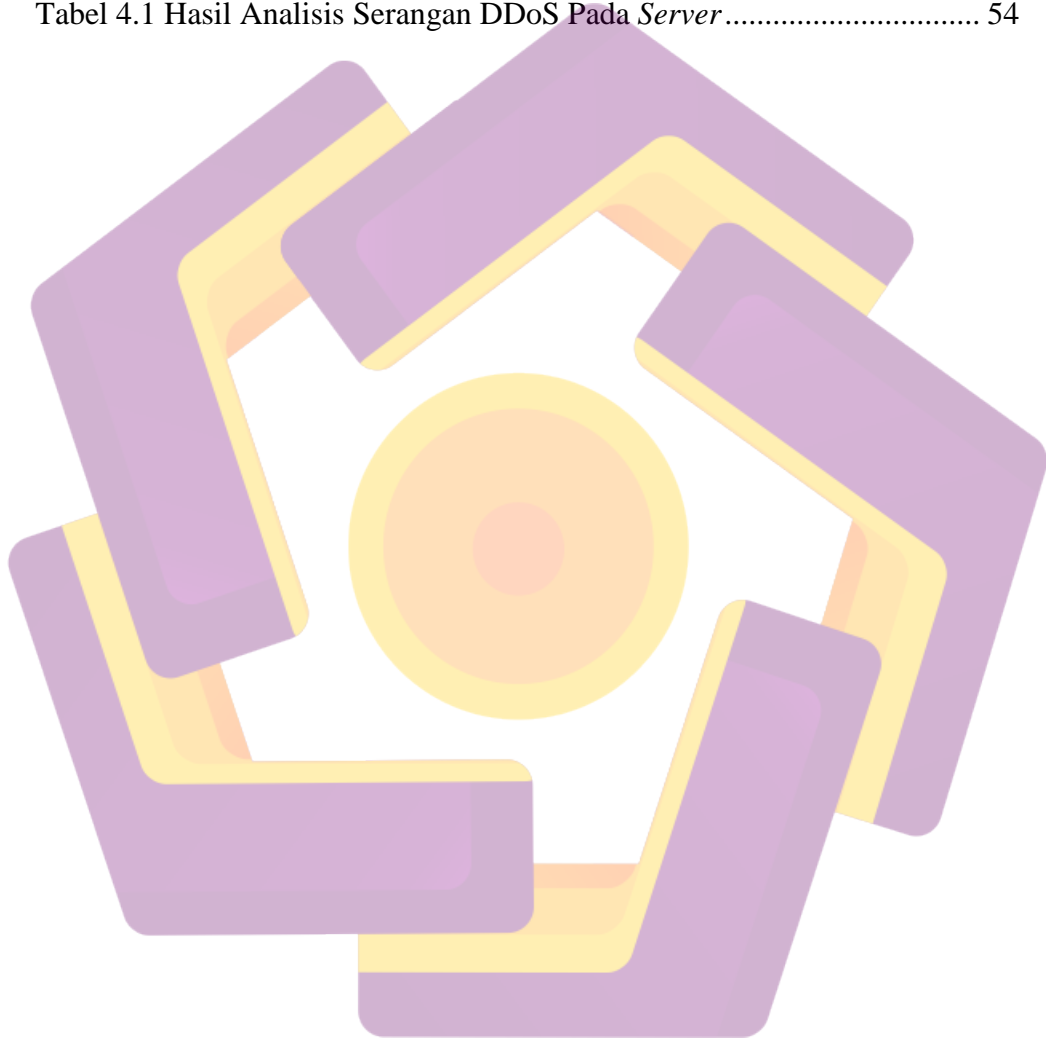
ANALISIS SERANGAN <i>DDOS</i> PADA <i>RESOURCE SERVER</i> MENGUNAKAN <i>WIRESHARK</i> .....	i
ANALISIS SERANGAN <i>DDOS</i> PADA <i>RESOURCE SERVER</i> MENGUNAKAN <i>WIRESHARK</i> .....	ii
PERSETUJUAN .....	iii
PENGESAHAN .....	iv
PERNYATAAN.....	iv
MOTTO .....	vi
PERSEMBAHAN.....	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	x
DAFTAR GAMBAR .....	xi
INTISARI.....	xiii
<i>ABSTRACT</i> .....	xiv
BAB I.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah .....	2
1.3 Batasan Masalah.....	3
1.4 Maksud dan Tujuan Penelitian .....	3
1.5 Manfaat Penelitian.....	4
1.6 Metode Penelitian.....	4
1.6.1 Studi Literatur .....	5
1.6.2 Metode Pengumpulan Data.....	5
1.6.3 Perancangan Sistem .....	5
1.6.4 Analisis Sistem.....	5
1.7 Sistematika Penulisan.....	5
BAB II.....	8
2.1 Kajian Pustaka .....	8
Tabel 2.1 Matriks Perbandingan Penelitian.....	12
Tabel 2.2 Matriks Perbandingan Penelitian.....	13
Tabel 2.3 Matriks Perbandingan Penelitian.....	14



2.2	Landasan Teori .....	15
2.2.1	Serangan <i>DDoS</i> .....	15
2.2.2	<i>Network Protocol Analyzer</i> .....	18
2.2.3	<i>Process of Attack</i> .....	19
2.2.4	<i>Resource Server</i> .....	19
2.2.5	<i>Wireshark</i> .....	20
2.2.6	<i>HPing3</i> .....	21
2.2.7	<i>Laragon</i> .....	22
2.2.8	<i>Appache</i> .....	23
2.2.9	<i>Live Forensics</i> .....	23
BAB III	.....	26
3.1.1	Analisis Kebutuhan .....	26
3.1.1	<i>Software</i> .....	26
3.1.2	<i>Hardware</i> .....	28
3.2	Alur Penelitian .....	30
3.2.1	Proses Pembuktian Data .....	32
BAB IV	.....	34
4.1	Rancangan Simulasi Serangan .....	34
4.2	Alur Pengujian Serangan <i>DDoS (Distributed Denial of Service)</i> .....	35
4.3	Analisis Serangan <i>DDoS TCP SYN Flood</i> pada Lalu-Lintas <i>Server</i> .....	37
4.3.1	Proses Penyerangan Menggunakan Aplikasi <i>HPing3</i> .....	38
4.4	Penbuktian Data .....	43
4.4.1	<i>Log Activity</i> .....	46
4.4.2	<i>IP Address List</i> .....	48
4.4.3	<i>IO Graph</i> .....	50
4.4.4	<i>Flow Graph</i> .....	52
4.5	Laporan Hasil Pengujian Analisis Serangan <i>DDoS</i> pada <i>Server</i> .....	54
BAB 5	.....	56
5.1	Kesimpulan .....	56
5.2	Saran .....	57
DAFTAR PUSTAKA	.....	59
LAMPIRAN	.....	61

## DAFTAR TABEL

Tabel 2.1 Matriks Perbandingan Penelitian .....	12
Tabel 2.2 Matriks Perbandingan Penelitian .....	13
Tabel 2.3 Matriks Perbandingan Penelitian .....	14
Tabel 4.1 Hasil Analisis Serangan DDoS Pada <i>Server</i> .....	54



## DAFTAR GAMBAR

Gambar 2.1 Diagram urutan TCP SYN Flood .....	16
Gambar 2.2 Ilustrasi SYN Flood.....	17
Gambar 3.1 Tampilan Awal Laragon 4.0.....	28
Gambar 3.2 Tampilan Fisik Huawei B310 .....	29
Gambar 3.3 Tahapan Penelitian .....	30
Gambar 3.4 Tahap Pembuktian Data dengan Metode Live Forensics .....	32
Gambar 4.1 Rancangan Simulasi Serangan .....	35
Gambar 4.2 Skenario Penyerangan .....	36
Gambar 4.3 Lalu-lintas Pada Wireshark Sebelum Serangan DDoS .....	37
Gambar 4.4 Serangan <i>Hping3 DDoS TCP SYN Flood</i> .....	38
Gambar 4.5 <i>Capture Wireshark (no filtering logical) Setelah Diserang</i> ....	39
Gambar 4.6 <i>Capture Wireshark (with filtering logical) Setelah Diserang</i> ..	39
Gambar 4.7 <i>Monitoring Server Sebelum Diserang</i> .....	41
Gambar 4.8 <i>Monitoring Server Setelah Diserang</i> .....	42
Gambar 4.9 Pembuktian Data Menggunakan Metode Live Forensics .....	43
Gambar 4.10 Hasil Capture Setelah Diserang TCP SYN Flood.....	46
Gambar 4.11 <i>IP Address List Setelah Diserang TCP SYN Flood</i> <i>(no filtering logical)</i> .....	48
Gambar 4.12 <i>Address List Setelah Diserang TCP SYN Flood</i> <i>(with filtering logical)</i> .....	49
Gambar 4.13 Hasil IO Graph Setelah Diserang TCP SYN Flood <i>(no filtering logical)</i> .....	51

Gambar 4.14 Hasil IO Graph Setelah Diserang TCP SYN Flood  
(with filtering logical) ..... 51  
Gambar 4.15 Flow Line Graph Kondisi Setelah Diserang..... 53



## INTISARI

Masalah serangan Distributed Denial of Service (DDoS) pada suatu jaringan web/server terus meningkat di lingkungan masyarakat, khususnya serangan DDoS yang dilakukan oleh oknum tertentu dan ditujukan pada jaringan *Server* orang lain untuk memperoleh hak akses. Tidak jarang, serangan yang dilakukan menyebabkan jaringan *server* yang ditargetkan menjadi down (lumpuh) karena tidak mampu melayani permintaan user yang memiliki hak akses secara sah, sehingga diperlukan analisis serangan DDoS pada *Server*.

Serangan Distributed Denial of Service (DDoS) adalah serangan jaringan terstruktur yang berasal dari berbagai sumber dan berkumpul untuk membentuk arus paket besar. Serangan DDoS bertujuan untuk menghabiskan sumber daya *server* dan mengganggu layanan yang tersedia pada jaringan target dengan membanjiri bandwidth atau sistem kapasitas pemrosesan yang membuat jaringan *server* target menjadi kelebihan beban.

Wireshark adalah alat yang dapat digunakan untuk mendeteksi serangan DDoS pada jaringan *Server* dan melakukan analisis lalu lintas jaringan yang memiliki fungsi Filtering Logical untuk mendeteksi serangan DDoS pada *Server* dan menggali informasi serta menarik data forensik sebagai bukti digital serangan DDoS pada *server* melalui metode live forensics. Output yang dihasilkan penelitian ini berhasil menarik data informasi serangan DDoS terkait data Log Activity, IP Address List, IO graph dan Flow graph.

Kata Kunci: Serangan *DDoS (Distributed Denial of Service)*, *Resource Server*, *Live Forensic*, *Filtering Logical*.

## ABSTRACT

*The problem of Distributed Denial of Service (DDoS) attacks on a web network/server continues to increase in the community, especially DDoS attacks carried out by certain persons and aimed at other people's Server networks to gain access rights. Not infrequently, attacks are carried out causing the targeted server network to be down (paralyzed) because it is unable to serve user requests that have legitimate permissions, so it is necessary to analyze DDoS attacks on the Server.*

*Distributed Denial of Service (DDoS) attacks are structured network attacks that come from a variety of sources and come together to form a large package stream. DDoS attacks aim to consume server resources and disrupt services available on the target network by flooding bandwidth or processing capacity systems that make the target server network overloaded.*

*Wireshark is a tool that can be used to detect DDoS attacks on server networks and perform network traffic analysis that has a Logical Filtering function to detect DDoS attacks on servers and dig up information and pull forensic data as digital evidence of DDoS attacks on servers through live forensics methods. The output produced by this study successfully pulled DDoS attack information data related to Log Activity data, IP Address List, IO graph and Flow graph.*

*Keywords: Distributed Denial of Service (DDoS), Resource Server, Live Forensic, Filtering Logical.*