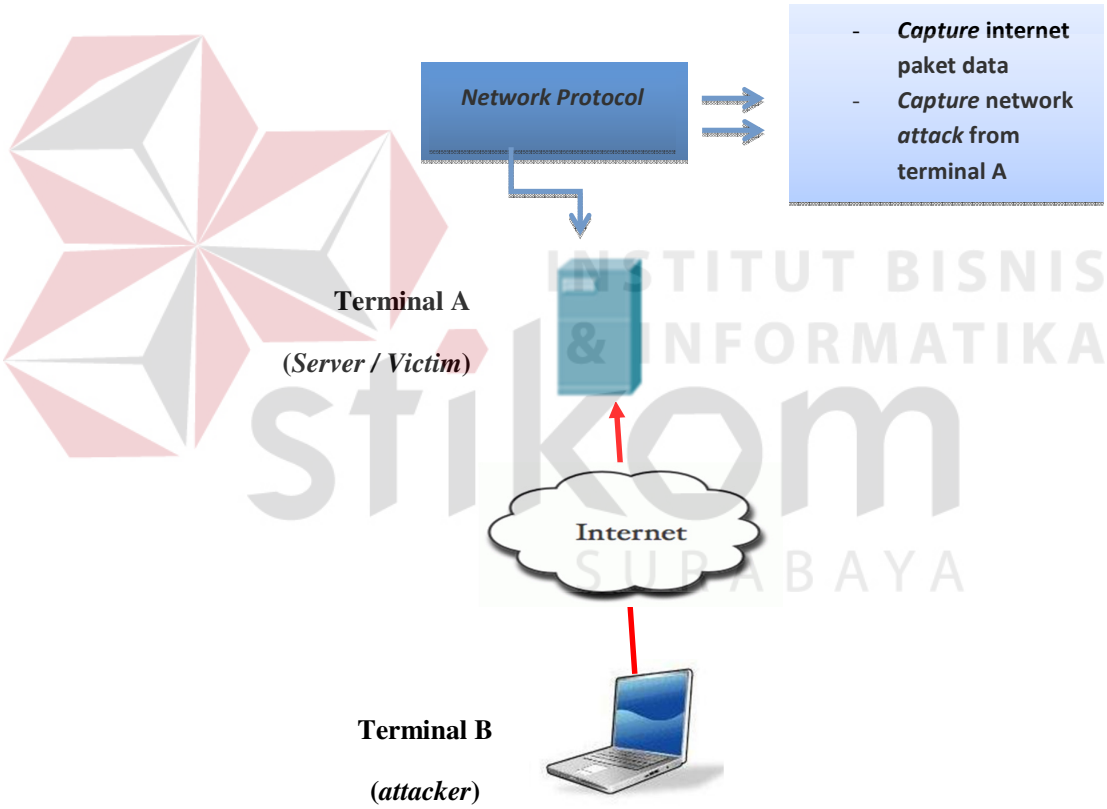
BAB III

METODE PENELITIAN

3.1 Desain Penelitian

Untuk mendapatkan hasil yang sesuai tujuan yang diinginkan diperlukan sebuah rancangan untuk mempermudah dalam memahami sistem yang akan dibuat, maka akan dibuat sebuah Simulasi jaringan yang dapat dilihat pada Gambar 3.1.

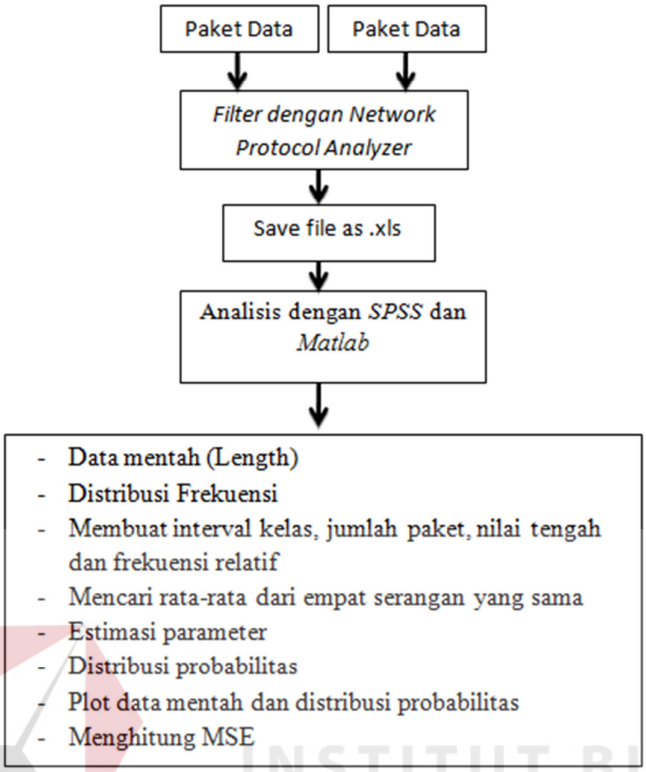


Gambar 3.1. Simulasi Jaringan

Dari Simulasi jaringan di atas dapat diketahui bagaimana cara mendapatkan paket data dari lalu lintas jaringan menggunakan *Network Protocol Analyzer*. Terminal A bertindak melakukan analisis terhadap lalu lintas jaringan

dengan menggunakan *Network Protocol Analyzer* untuk mengambil paket data dalam jaringan, tetapi sebelumnya dalam penelitian ini terminal A berada dalam kondisi terhubung langsung dengan internet.Terminal A dapat menangkap paket yang yang melintasi lalu lintas jaringan dengan *Network Protocol Analyzer. Network Protocol Analyzer* akan mendeteksi paket-paket data atau informasi yang melintas di dalam jaringan termasuk aktifitas yang dilakukan terminal B di dalam jaringan, selain itu aplikasi ini dapat membaca data secara langsung dari *Ethernet, Token-Ring, FDDI,* serial (*PPP* dan *SLIP*), *802.11 wireless LAN*, dan koneksi ATM.

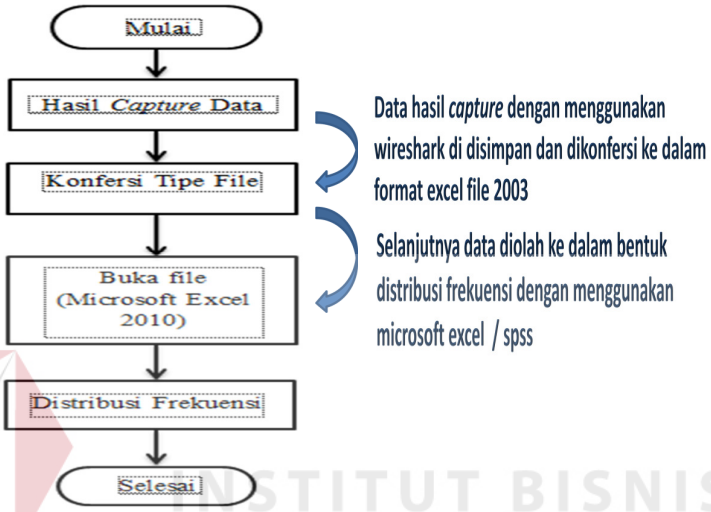
Terminal B yang juga terhubung langsung dengan terminal A dan difungsikan sebagai pihak yang bertindak melakukan serangan (*attack*) terhadap terminal A. Terminal B melakukan *attack* terhadap terminal A dengan menggunakan beberapa jenis serangan di antaranya *SYN Attack, PING Flood dan UDP Flood*. Untuk lebih detailnya bisa dilihat pada blok diagram pada Gambar 3.2.



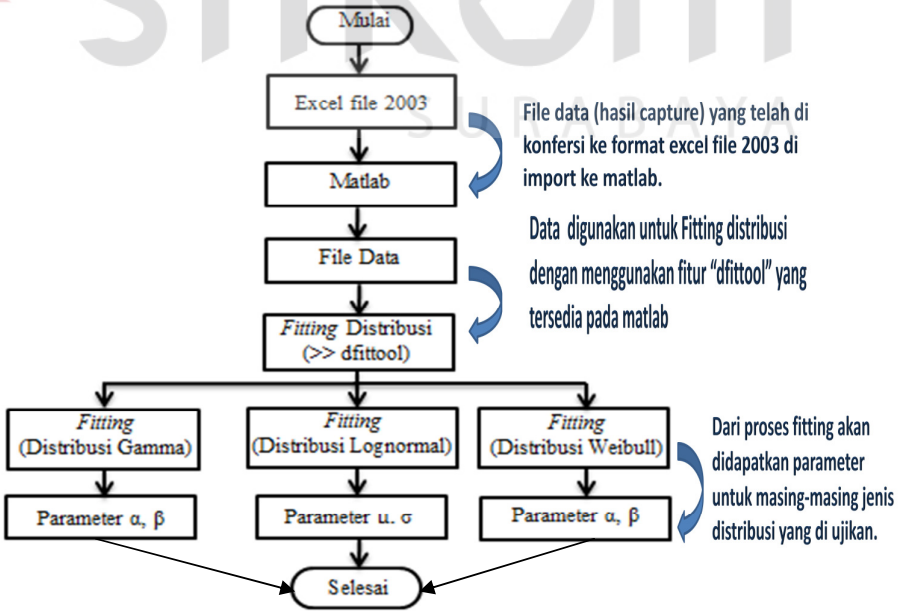
Gambar 3.2. Diagram Blok Proses Analisis

Setelah paket data di dapatkan dengan menggunakan Network Protocol Analyzer selanjutnya file diolah dengan menggunakan excel, spss dan matlab. Selanjutnya menghitung panjang paket data (byte) dalam rentang waktu tertentu.Selanjutnya memodelkan panjang paket (byte) ke dalam bentuk kurva distribusi frekuensi untuk mengetahui bentuk distribusi probabilitasnya pada setiap paket data yang terkena serangan *SYN Attack*, *PING Flood* dan UDP Flood.Selanjutnya melakukan estimasi untuk mengetahui parameter dari setiap distribusi probabilitas yang telah dibuat serta mencari nilai MSE agar serangan tersebut lebih mendekati dengan distribusi gamma, lognormal atau weibull dan akhirnya mendapatkan kesimpulan yang sesuai dengan tujuan analisis.

Detail tentang alur pengerjaan Tugas Akhir ini, di bawah ini terdapat flowchart cara mencari distribusi frekuensi dan estimasi parameter pada pada distribusi gamma,lognormal dan weibull, dapat dilihat pada flowchart pada Gambar 3.3 dan Gambar 3.4.

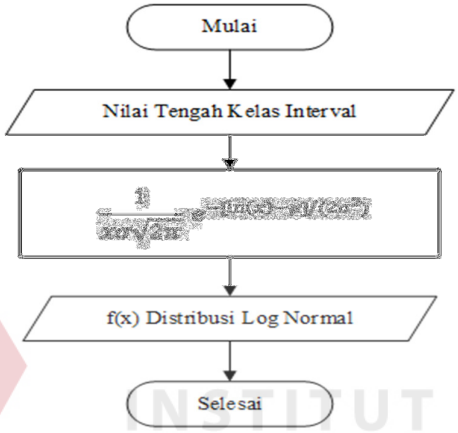


Gambar 3.3. Flowchart Distribusi Frekuensi.

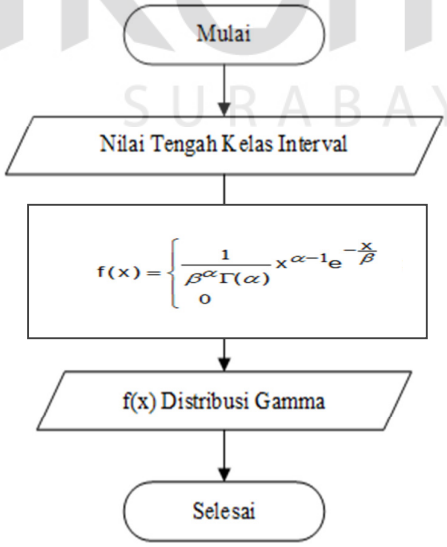


Gambar 3.4. flowchart distribusi fitting.

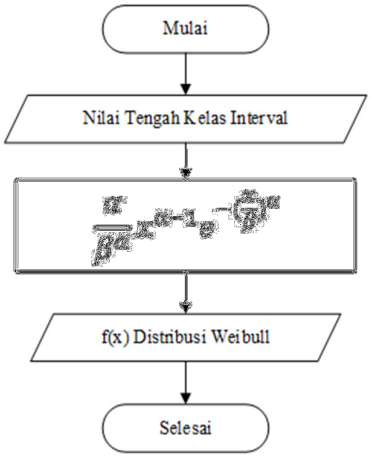
Setelah proses perhitungan dengan distribusi fitting untuk distribusi gamma, lognormal dan weibull, langkah selanjutnya melakukan proses perhitungan pada distribusi probabilitas yaitu distribusi gamma,lognormal dan weibull.detail flowchatnya dapat dilihat pada Gambar 3.5, Gambar 3.6 dan Gambar 3.7.



Gambar 3.5. Flowchart Distribusi Lognormal.



Gambar 3.6. Flowchart Distribusi Gamma.



Gambar 3.7. Flowchart Distribusi Weibull.

3.2 Peralatan dan perlengkapan penilitian

a. Dua Unit Laptop

Laptop ini digunakan sebagai alat untuk serangan dan juga sebagai alat untuk menangkap paket data dari serangan DoS Attack.

b. Dua Unit Modem

Modem ini digunakan untuk sebagai koneksi internet yang nantinya dipakai untuk aliran paket data dari attacker menuju victim

c. Aplikasi Wireshark

Aplikasi wireshark ini untuk menangkap paket data yang nanti akan digunakan untuk penelitian

d. Aplikasi Microsoft excel, SPSS dan Matlab

Aplikasi Microsoft excel ini digunakan untuk wadah dari proses statistik dan digunakan untuk perhitungan *MSE*. Selanjutnya aplikasi SPSS ini digunakan untuk mencari distribusi frekuensi pada paket data mentah.Dan aplikasi Matlab digunakan untuk estimasi parameter, distribusi probabilitas dan plot data.

3.3 Prosedur Penelitian

3.3.1 Parameter Penelitian

Penelitian ini menggunakan beberapa parameter yang dapat menghasilkan nilai distribusi probabilitas dan nilai *MSE* yaitu *UDP Attack*, *PING Flood* dan *SYN Attack*.

3.3.2 Metode Pengambilan Data

Metode pengambilan paket data adalah dengan menggunakan *Network Protocol Analyser* yaitu *Wireshark*, dengan cara Terminal A sebagai server/victim bertindak melakukan analisis terhadap lalu lintas jaringan dengan menggunakan *Network Protocol Analyzer* untuk mengambil paket data dalam jaringan, tetapi sebelumnya dalam penelitian ini terminal A berada dalam kondisi terhubung langsung dengan internet. Terminal A dapat menangkap paket yang melintasi lalu lintas jaringan dengan *Network Protocol Analyzer. Network Protocol Analyzer* akan mendeteksi paket-paket data atau informasi yang melintas di dalam jaringan termasuk aktifitas yang dilakukan terminal B sebagai Attacker di dalam jaringan.

Terminal B yang juga terhubung langsung dengan terminal A dan difungsikan sebagai pihak yang bertindak melakukan serangan (attack) terhadap terminal A. Terminal B melakukan attack terhadap terminal A dengan menggunakan beberapa jenis serangan di antaranya *SYN Attack*, *PING Flood* dan UDP Flood.

3.3.3 Metode Klarifikasi Data

Metode klasifikasi data menggunakan distribusi probabilitas,distribusi ini terdiri dari distribusi *Gamma*, distribusi *Lognormal* dan distribusi

Weibull.Distribusi probabilitas ini digunakan untuk memodelkan karakteristik dari DoS Attack dan untuk mendapat hasil dari nilai *MSE*.

3.4 Cara Kerja Sistem Secara Keseluruhan

Laptop *attacker* menggunakan *OS Backtrack* 5, *OS Backtrack* merupakan operating system yang mempunyai kelebihan bisa melakukan penetrasi terhadap jaringan dan juga melakukan serangan terhadap jaringan. *OS Backtrack* ini terhubung dengan koneksi internet modem *Smartfren* dan *Server* menggunakan menggunakan *OS Ubuntu* yang terhubung dengan koneksi internet modem *Smartfren*. Langkah-langkah serangan :

A. Buka terminal pada sisi *Server/Victim* ketikkan ifconfig, nanti akan muncul dengan jelas *IP Address* yang didapat dari modem *Smartfren,* buka juga *Network Protocol Analyser* yaitu *Wireshark*.

B. Selanjutnya buka terminal pada sisi *Attacker,* lakukan instalasi *hping3*yang nantinya akan digunakan *Attacker* untuk proses serangan ketik *HPING3* dan *NMAP* sudah siap untuk dipakai serangan, untuk rentang waktu masing-masing serangannya selama 3 menit, serangan ini tidak bisa dilakukan terlalu lama dikarenakan *wireshark* sendiri tidak bisa menampung terlalu banyak paket data.

C. Pada sisi *Attacker* lakukan serangan

   Menggunakan *HPING* ketik :

   a. Sudo hping3 –I u1 -S[*IP Address Server/Victim*], ini merupakan metode serangan *SYN Attack*.

   b. Sudo hping3 –I u1 -2[*IP Address Server/Victim*], ini merupakan metode serangan *UDP Flood*.

c. *Sudo hping3* –I u1 -1 [*IP Address Server/Victim*], ini merupakan metode serangan *PING Flood*.

Menggunakan *NMAP* ketik :

a. sudo nmap -sS -O [*IP Address Server /victim*], ini merupakan metode serangan *SYN Attack*.

b. sudo nmap -sU -O [*IP Address Server /victim*], ini merupakan metode serangan *UDP Attack*.

c. sudo nmap -PE -sn [*IP Address Server /victim*] –oN, ini merupakan metode serangan *PING Flood*.

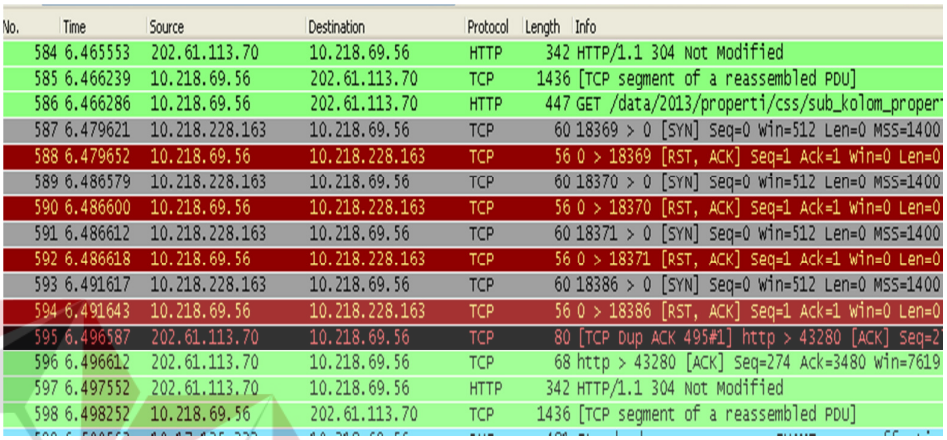
D. Pada sisi *Server / Victim buka Wireshark.*

a. *Wireshark* disini merupakan *network protocol analyser*yang digunakan untuk mencapture paket data, jadi apabila terdapat paket data dalam jumlah besar datang secara serentak maka akan bisa terdeteksi oleh *Wireshark*. *Wiresahark* ini nanti akan mencapture paket data dari serangan *SYN Attack* terlebih dahulu, setelah itu paket data dari serangan *UDP Flood* dan yang terakhir paket data dari serangan *PING Flood*.

b. Untuk lebih jelasnya bisa dilihat pada Gambar 3.8, Gambar 3.9 dan Gambar 3.10.

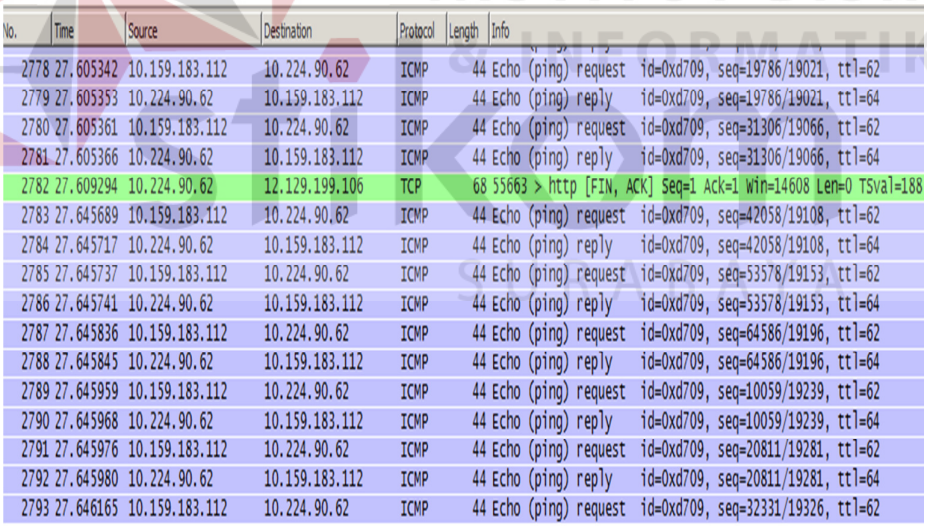
No.	Time	Source	Destination	Protocol	Length	Info
25479	72.290088	10.158.166.203	10.231.163.24	UDP	44	Source port: 64032 Destination port: 0
25480	72.295565	10.231.163.24	112.78.131.2	TCP	56	54201 > http [ACK] Seq=2518 Ack=359 Win=16616 Len=0
25481	72.297137	10.158.166.203	10.231.163.24	UDP	44	Source port: 64078 Destination port: 0
25482	72.297149	10.158.166.203	10.231.163.24	UDP	44	Source port: 64123 Destination port: 0
25483	72.297150	10.158.166.203	10.231.163.24	UDP	44	Source port: 64168 Destination port: 0
25484	72.297151	10.158.166.203	10.231.163.24	UDP	44	Source port: 64214 Destination port: 0
25485	72.297152	10.158.166.203	10.231.163.24	UDP	44	Source port: 64261 Destination port: 0
25486	72.297153	10.158.166.203	10.231.163.24	UDP	44	Source port: 64307 Destination port: 0
25487	72.297154	10.158.166.203	10.231.163.24	UDP	44	Source port: 64352 Destination port: 0
25488	72.297273	10.158.166.203	10.231.163.24	UDP	44	Source port: 64397 Destination port: 0
25489	72.297277	10.158.166.203	10.231.163.24	UDP	44	Source port: 64488 Destination port: 0
25490	72.297332	10.158.166.203	10.231.163.24	UDP	44	Source port: 64442 Destination port: 0
25491	72.297337	10.158.166.203	10.231.163.24	UDP	44	Source port: 64536 Destination port: 0
25492	72.297464	10.158.166.203	10.231.163.24	UDP	44	Source port: 64581 Destination port: 0
25493	72.297478	10.158.166.203	10.231.163.24	UDP	44	Source port: 64629 Destination port: 0
25494	72.297567	10.158.166.203	10.231.163.24	UDP	44	Source port: 64675 Destination port: 0

Gambar 3.8. Paket Data *UDP Attack* di *Wireshark*



No.	Time	Source	Destination	Protocol	Length	Info
584	6.465553	202.61.113.70	10.218.69.56	HTTP	342	HTTP/1.1 304 Not Modified
585	6.466239	10.218.69.56	202.61.113.70	TCP	1436	[TCP segment of a reassembled PDU]
586	6.466286	10.218.69.56	202.61.113.70	HTTP	447	GET /data/2013/properti/css/sub_kolom_proper
587	6.479621	10.218.228.163	10.218.69.56	TCP	60	18369 > 0 [SYN] Seq=0 Win=512 Len=0 MSS=1400
588	6.479652	10.218.69.56	10.218.228.163	TCP	56	0 > 18369 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
589	6.486579	10.218.228.163	10.218.69.56	TCP	60	18370 > 0 [SYN] Seq=0 Win=512 Len=0 MSS=1400
590	6.486600	10.218.69.56	10.218.228.163	TCP	56	0 > 18370 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
591	6.486612	10.218.228.163	10.218.69.56	TCP	60	18371 > 0 [SYN] Seq=0 Win=512 Len=0 MSS=1400
592	6.486618	10.218.69.56	10.218.228.163	TCP	56	0 > 18371 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
593	6.491617	10.218.228.163	10.218.69.56	TCP	60	18386 > 0 [SYN] Seq=0 Win=512 Len=0 MSS=1400
594	6.491643	10.218.69.56	10.218.228.163	TCP	56	0 > 18386 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
595	6.496587	202.61.113.70	10.218.69.56	TCP	80	[TCP Dup ACK 495#1] http > 43280 [ACK] Seq=2
596	6.496612	202.61.113.70	10.218.69.56	TCP	68	http > 43280 [ACK] Seq=274 Ack=3480 Win=7619
597	6.497552	202.61.113.70	10.218.69.56	HTTP	342	HTTP/1.1 304 Not Modified
598	6.498252	10.218.69.56	202.61.113.70	TCP	1436	[TCP segment of a reassembled PDU]

Gambar 3.9. Paket Data *SYN Attack* di *Wireshark*



No.	Time	Source	Destination	Protocol	Length	Info
2778	27.605342	10.159.183.112	10.224.90.62	ICMP	44	Echo (ping) request id=0xd709, seq=19786/19021, ttl=62
2779	27.605353	10.224.90.62	10.159.183.112	ICMP	44	Echo (ping) reply id=0xd709, seq=19786/19021, ttl=64
2780	27.605361	10.159.183.112	10.224.90.62	ICMP	44	Echo (ping) request id=0xd709, seq=31306/19066, ttl=62
2781	27.605366	10.224.90.62	10.159.183.112	ICMP	44	Echo (ping) reply id=0xd709, seq=31306/19066, ttl=64
2782	27.609294	10.224.90.62	12.129.199.106	TCP	68	55663 > http [FIN, ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=188
2783	27.645689	10.159.183.112	10.224.90.62	ICMP	44	Echo (ping) request id=0xd709, seq=42058/19108, ttl=62
2784	27.645717	10.224.90.62	10.159.183.112	ICMP	44	Echo (ping) reply id=0xd709, seq=42058/19108, ttl=64
2785	27.645737	10.159.183.112	10.224.90.62	ICMP	44	Echo (ping) request id=0xd709, seq=53578/19153, ttl=62
2786	27.645741	10.224.90.62	10.159.183.112	ICMP	44	Echo (ping) reply id=0xd709, seq=53578/19153, ttl=64
2787	27.645836	10.159.183.112	10.224.90.62	ICMP	44	Echo (ping) request id=0xd709, seq=64586/19196, ttl=62
2788	27.645845	10.224.90.62	10.159.183.112	ICMP	44	Echo (ping) reply id=0xd709, seq=64586/19196, ttl=64
2789	27.645959	10.159.183.112	10.224.90.62	ICMP	44	Echo (ping) request id=0xd709, seq=10059/19239, ttl=62
2790	27.645968	10.224.90.62	10.159.183.112	ICMP	44	Echo (ping) reply id=0xd709, seq=10059/19239, ttl=64
2791	27.645976	10.159.183.112	10.224.90.62	ICMP	44	Echo (ping) request id=0xd709, seq=20811/19281, ttl=62
2792	27.645980	10.224.90.62	10.159.183.112	ICMP	44	Echo (ping) reply id=0xd709, seq=20811/19281, ttl=64
2793	27.646165	10.159.183.112	10.224.90.62	ICMP	44	Echo (ping) request id=0xd709, seq=32331/19326, ttl=62

Gambar 3.10. Paket Data *PING Flood* di Wireshark

E. Selanjutnya paket data *SYN Attack*, *UDP Flood*, dan *PING Flood* di simpan dan dikonversi ke excel 2003 agar bisa dianalisis nantinya memakai aplikasi *SPSS* dan *MATLAB.*

F. Selanjutnya membuat interval kelas untuk paket data length, agar data ribuan saat disajikan dalam bentuk histogram atau grafik bisa dibaca dengan baik. Setelah membuat interval kelas, mencari nilai tengah dan frekuensi relatif yang digunakan nanti dalam penyajian atau pemodelan histogram dan grafik.

G. Selanjutnya Melakukan estimasi α dan β, menggunakan aplikasi *Matlab*, metode yang digunakan MLE (*Maximum likelihood estimation*), Likelihood Estimation (MLE) adalah metode yang dikenal dalam penetapan model data secara statistik. Metode ini menyeleksi nilai-nilai dari parameter-parameter model, dan memaksimalkan fungsi likelihood-nya. Metode MLE akan memberikan pendekatan estimasi yang akurat sepanjang kasusnya terdefinisi dengan baik dan terdistribusi normal, rumus pada matlab yang digunakan untuk estimasi parameter α dan β pada distribusi *Weibull* "[*parmhat,parmci*] = *wblfit*(data)" , rumus pada matlab yang digunakan untuk estimasi parameter αdan β pada distribusi *Gamma* "[*phat,pci*] = gamfit(data)" dan rumus pada matlab yang digunakan untuk estimasi parameter mudan sigma pada distribusi *Lognormal* "[*parmhat,parmci*] = logn(data)".

H. Setelah melakukan estimasi parameter, masukkan parameter distribusi *Weibull*ke rumus distribusi *Weibull*dan parameter distribusi *Gamma* ke rumus distribusi *Gamma dan parameter Lognormal masukkan kedalan rumus distribusi Lognormal*.

I. Plot *UDP Attack* yaitu data mentah dengan distribusi *Gamma*, *Lognormal*, *Weibull* dan untuk *SYN Attack*, *PING Flood*juga sama prosesnya.

J. Kesalahan rata-rata kwadrat atau *MSE* (*Mean Square error*) merupakan metode alternatif dalam mengevaluasi suatu teknik peramalan, dimana setiap kesalahan atau residual dikuadratkan yang biasanya menghasilkan kesalahan yang lebih kecil tetapi kadang-kadang menghasilkan yang sangat besar.

Rumus untuk *MSE*,

$$MSE = \frac{\sum_{t=1}^{n} \left(Y_t - \overline{Y_t}\right)^2}{n}$$

Y_t = Data

$\overline{Y_t}$ = Distribusi probabilitas

N = Banyaknya data

Metode *MSE* ini nantinya akan digunakan untuk mencari tingkat eror terkecil yang dijadikan patokan untuk pendekatan ke distribusi *Weibull*, distribusi *Gamma* atau distribusi *Lognormal,* apabila *MSE* distribusi *Weibull* lebih kecil nilainya dari pada distribusi *Gamma* maka paket data serangan tersebut adalah distribusi *Weibull*. dan juga sama untuk distribusi *Weibull* atau distribusi *Lognormal*.