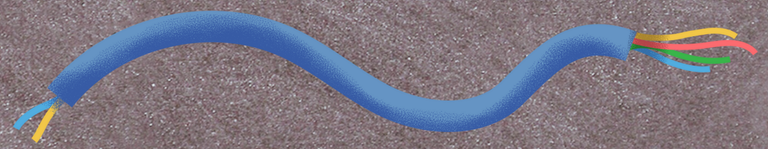
DDOS PROVING USING



Johannes [2501983736]

Richard M.H.T., Tan [2502008952]

Jeremy Julian [2501998845]

Immanuel Billy C.S. [2540132723]

DDOS?

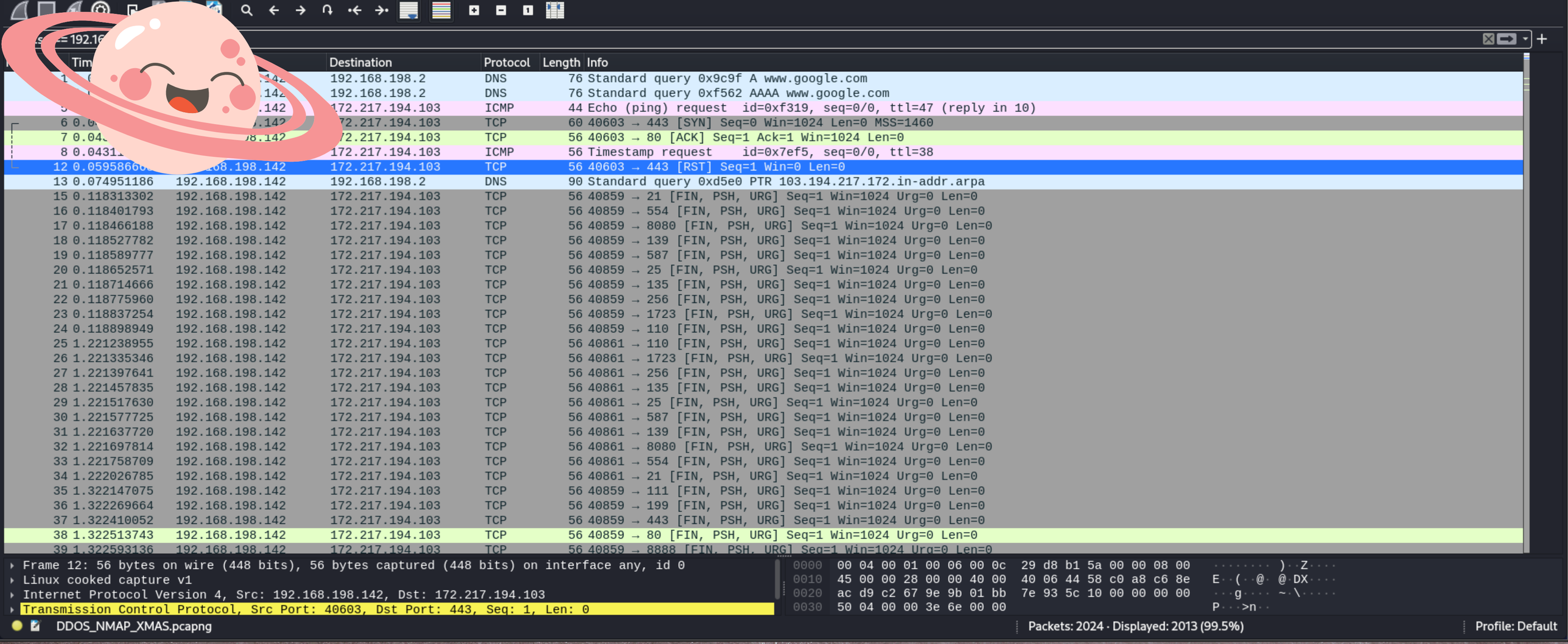
DDOS attack atau Distributed Denial of Service merupakan serangan cyber dengan cara mengirimkan fake traffic atau lalu lintas palsu ke suatu sistem atau server secara terus menerus. Dampaknya, server tersebut tidak dapat mengatur seluruh traffic sehingga menyebabkan down.

BAGAIMANA CARA MENGETAHUI SEDANG DI DDOS

menggunakan live packet capture di Networking anda sehingga bisa melihat semua traffic yang masuk dan keluar dari server atau jaringan anda.

Contoh: Wireshark

mari kita lihat beberapa contoh yang bisa dijadikan sebagai gambaran DDoS sedang terjadi



	Tim		Destination	Protocol	Length	Info
1		.142	192.168.198.2	DNS	76	Standard query 0x9c9f A www.google.com
		.142	192.168.198.2	DNS	76	Standard query 0xf562 AAAA www.google.com
5		.142	172.217.194.103	ICMP	44	Echo (ping) request id=0xf319, seq=0/0, ttl=47 (reply in 10)
6	0.0	.142	72.217.194.103	TCP	60	40603 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.04	8.142	72.217.194.103	TCP	56	40603 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
8	0.0431		172.217.194.103	ICMP	56	Timestamp request id=0x7ef5, seq=0/0, ttl=38
12	0.05958660	68.198.142	172.217.194.103	TCP	56	40603 → 443 [RST] Seq=1 Win=0 Len=0
13	0.074951186	192.168.198.142	192.168.198.2	DNS	90	Standard query 0xd5e0 PTR 103.194.217.172.in-addr.arpa
15	0.118313302	192.168.198.142	172.217.194.103	TCP	56	40859 → 21 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
16	0.118401793	192.168.198.142	172.217.194.103	TCP	56	40859 → 554 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
17	0.118466188	192.168.198.142	172.217.194.103	TCP	56	40859 → 8080 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
18	0.118527782	192.168.198.142	172.217.194.103	TCP	56	40859 → 139 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
19	0.118589777	192.168.198.142	172.217.194.103	TCP	56	40859 → 587 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
20	0.118652571	192.168.198.142	172.217.194.103	TCP	56	40859 → 25 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
21	0.118714666	192.168.198.142	172.217.194.103	TCP	56	40859 → 135 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
22	0.118775960	192.168.198.142	172.217.194.103	TCP	56	40859 → 256 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
23	0.118837254	192.168.198.142	172.217.194.103	TCP	56	40859 → 1723 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
24	0.118898949	192.168.198.142	172.217.194.103	TCP	56	40859 → 110 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
25	1.221238955	192.168.198.142	172.217.194.103	TCP	56	40861 → 110 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
26	1.221335346	192.168.198.142	172.217.194.103	TCP	56	40861 → 1723 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
27	1.221397641	192.168.198.142	172.217.194.103	TCP	56	40861 → 256 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
28	1.221457835	192.168.198.142	172.217.194.103	TCP	56	40861 → 135 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
29	1.221517630	192.168.198.142	172.217.194.103	TCP	56	40861 → 25 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
30	1.221577725	192.168.198.142	172.217.194.103	TCP	56	40861 → 587 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
31	1.221637720	192.168.198.142	172.217.194.103	TCP	56	40861 → 139 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
32	1.221697814	192.168.198.142	172.217.194.103	TCP	56	40861 → 8080 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
33	1.221758709	192.168.198.142	172.217.194.103	TCP	56	40861 → 554 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
34	1.222026785	192.168.198.142	172.217.194.103	TCP	56	40861 → 21 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
35	1.322147075	192.168.198.142	172.217.194.103	TCP	56	40859 → 111 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
36	1.322269664	192.168.198.142	172.217.194.103	TCP	56	40859 → 199 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
37	1.322410052	192.168.198.142	172.217.194.103	TCP	56	40859 → 443 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
38	1.322513743	192.168.198.142	172.217.194.103	TCP	56	40859 → 80 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
39	1.322593136	192.168.198.142	172.217.194.103	TCP	56	40859 → 8888 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

```
▸ Frame 12: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 192.168.198.142, Dst: 172.217.194.103
▸ Transmission Control Protocol, Src Port: 40603, Dst Port: 443, Seq: 1, Len: 0

0000  00 04 00 01 00 06 00 0c  29 d8 b1 5a 00 00 08 00   ........ )..Z....
0010  45 00 00 28 00 00 40 00  40 06 44 58 c0 a8 c6 8e   E..(..@. @.DX....
0020  ac d9 c2 67 9e 9b 01 bb  7e 93 5c 10 00 00 00 00   ...g.... ~.\.....
0030  50 04 00 00 3e 6e 00 00                            P...>n..
```

DDOS_NMAP_XMAS.pcapng | Packets: 2024 · Displayed: 2013 (99.5%) | Profile: Default

Disini kita bisa melihat bahwa Destination yang dikirim adalah ip tersebut, dan itu ternyata berketerusan sampai 2000an packet yang dikirim ke destination tersebut

No.	Time	Source	Destination	Protocol	Length	Info
1991	3.985582745	192.168.198.142	172.217.194.103	TCP	56	40861 → 3031 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
1992	3.985641840	192.168.198.142	172.217.194.103	TCP	56	40861 → 1011 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
1993	3.985700835	192.168.198.142	172.217.194.103	TCP	56	40861 → 6699 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
1994	3.988596583	192.168.198.142	172.217.194.103	TCP	56	40868 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
1995	3.988673476	192.168.198.142	172.217.194.103	TCP	56	40861 → 1185 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
1996	3.988731472	192.168.198.142	172.217.194.103	TCP	56	40861 → 902 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
1998	3.992034484	192.168.198.142	172.217.194.103	TCP	56	40861 → 9502 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
1999	3.992117577	192.168.198.142	172.217.194.103	TCP	56	40861 → 8291 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2000	3.995396292	192.168.198.142	172.217.194.103	TCP	56	40861 → 1024 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2001	3.995480285	192.168.198.142	172.217.194.103	TCP	56	40861 → 8300 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2002	3.995549579	192.168.198.142	172.217.194.103	TCP	56	40861 → 5988 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2003	3.995615973	192.168.198.142	172.217.194.103	TCP	56	40861 → 2399 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2004	3.995681867	192.168.198.142	172.217.194.103	TCP	56	40861 → 3268 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2005	3.995748961	192.168.198.142	172.217.194.103	TCP	56	40861 → 5811 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2006	3.995814855	192.168.198.142	172.217.194.103	TCP	56	40861 → 3323 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2007	3.995903248	192.168.198.142	172.217.194.103	TCP	56	40861 → 1084 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2008	3.995975342	192.168.198.142	172.217.194.103	TCP	56	40861 → 8333 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2009	3.996047135	192.168.198.142	172.217.194.103	TCP	56	40861 → 1009 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2010	3.998610512	192.168.198.142	172.217.194.103	TCP	56	40861 → 888 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2011	3.998676706	192.168.198.142	172.217.194.103	TCP	56	40861 → 5357 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2012	3.998735201	192.168.198.142	172.217.194.103	TCP	56	40861 → 3871 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2013	3.998791696	192.168.198.142	172.217.194.103	TCP	56	40861 → 8084 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2014	3.998864890	192.168.198.142	172.217.194.103	TCP	56	40861 → 617 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2015	3.998922685	192.168.198.142	172.217.194.103	TCP	56	40861 → 2046 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2016	4.001694144	192.168.198.142	172.217.194.103	TCP	56	40861 → 1187 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2017	4.001776136	192.168.198.142	172.217.194.103	TCP	56	40861 → 1048 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2018	4.001861229	192.168.198.142	172.217.194.103	TCP	56	40861 → 3551 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2019	4.001929323	192.168.198.142	172.217.194.103	TCP	56	40861 → 1533 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2020	4.001997317	192.168.198.142	172.217.194.103	TCP	56	40861 → 14000 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2021	4.002065612	192.168.198.142	172.217.194.103	TCP	56	40861 → 5631 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2022	4.002134305	192.168.198.142	172.217.194.103	TCP	56	40861 → 50300 [FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
2023	6.494194758	192.168.198.142	152.195.38.76	TCP	56	51524 → 80 [ACK] Seq=1 Ack=1 Win=63945 Len=0

dan ternyata source mengirimkan 2000an packet tersebut ke Destination hanya dalam waktu 3 detik saja, ini sudah merupakan bukti bahwa DDoS sedang terjadi karena human biasa tidak dapat mengirimkan request sebanyak itu dalam waktu yang pendek

KALAU TIDAK OBVIOUS SEPERTI ITU?

ada cara lain, yaitu di dalam menu statistics, ada conversations, kita klik menu tersebut dan melihat - lihat ada conversations terjadi dimana saja.

DDOS_NMAP_XMAS.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Wireshark · Conversations · DDOS_NMAP_XMAS.pcapng

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

Filter list for specific type

Ethernet | IPv4 · 4 | IPv6 | TCP · 2007 | UDP · 2

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.198.142	54046	23.215.35.94	80	2	118 bytes	972	1	56 bytes	1	62 bytes	2.657811	0.0002		
192.168.198.142	51524	152.195.38.76	80	2	118 bytes	2006	1	56 bytes	1	62 bytes	6.494195	0.0005		
192.168.198.142	40603	172.217.194.103	443	3	178 bytes	0	2	116 bytes	1	62 bytes	0.042995	0.0166	55 kbps	29 kbps
192.168.198.142	40603	172.217.194.103	80	2	118 bytes	1	1	56 bytes	1	62 bytes	0.043057	0.0007		
192.168.198.142	40859	172.217.194.103	21	1	56 bytes	2	1	56 bytes	0	0 bytes	0.118313	0.0000		
192.168.198.142	40859	172.217.194.103	554	1	56 bytes	3	1	56 bytes	0	0 bytes	0.118402	0.0000		
192.168.198.142	40859	172.217.194.103	8080	1	56 bytes	4	1	56 bytes	0	0 bytes	0.118466	0.0000		
192.168.198.142	40859	172.217.194.103	139	1	56 bytes	5	1	56 bytes	0	0 bytes	0.118528	0.0000		
192.168.198.142	40859	172.217.194.103	587	1	56 bytes	6	1	56 bytes	0	0 bytes	0.118590	0.0000		
192.168.198.142	40859	172.217.194.103	25	1	56 bytes	7	1	56 bytes	0	0 bytes	0.118653	0.0000		
192.168.198.142	40859	172.217.194.103	135	1	56 bytes	8	1	56 bytes	0	0 bytes	0.118715	0.0000		
192.168.198.142	40859	172.217.194.103	256	1	56 bytes	9	1	56 bytes	0	0 bytes	0.118776	0.0000		
192.168.198.142	40859	172.217.194.103	1723	1	56 bytes	10	1	56 bytes	0	0 bytes	0.118837	0.0000		
192.168.198.142	40859	172.217.194.103	110	1	56 bytes	11	1	56 bytes	0	0 bytes	0.118899	0.0000		
192.168.198.142	40859	172.217.194.103	111	1	56 bytes	22	1	56 bytes	0	0 bytes	1.322147	0.0000		
192.168.198.142	40859	172.217.194.103	199	1	56 bytes	23	1	56 bytes	0	0 bytes	1.322270	0.0000		
192.168.198.142	40859	172.217.194.103	443	1	56 bytes	24	1	56 bytes	0	0 bytes	1.322410	0.0000		
192.168.198.142	40859	172.217.194.103	80	1	56 bytes	25	1	56 bytes	0	0 bytes	1.322514	0.0000		
192.168.198.142	40859	172.217.194.103	8888	1	56 bytes	26	1	56 bytes	0	0 bytes	1.322593	0.0000		
192.168.198.142	40859	172.217.194.103	113	1	56 bytes	27	1	56 bytes	0	0 bytes	1.322680	0.0000		
192.168.198.142	40859	172.217.194.103	143	1	56 bytes	28	1	56 bytes	0	0 bytes	1.322760	0.0000		
192.168.198.142	40859	172.217.194.103	53	1	56 bytes	29	1	56 bytes	0	0 bytes	1.322840	0.0000		
192.168.198.142	40859	172.217.194.103	3306	1	56 bytes	30	1	56 bytes	0	0 bytes	1.322918	0.0000		
192.168.198.142	40859	172.217.194.103	3389	1	56 bytes	31	1	56 bytes	0	0 bytes	1.323002	0.0000		
192.168.198.142	40859	172.217.194.103	445	1	56 bytes	43	1	56 bytes	0	0 bytes	1.427384	0.0000		
192.168.198.142	40859	172.217.194.103	5900	1	56 bytes	44	1	56 bytes	0	0 bytes	1.427456	0.0000		

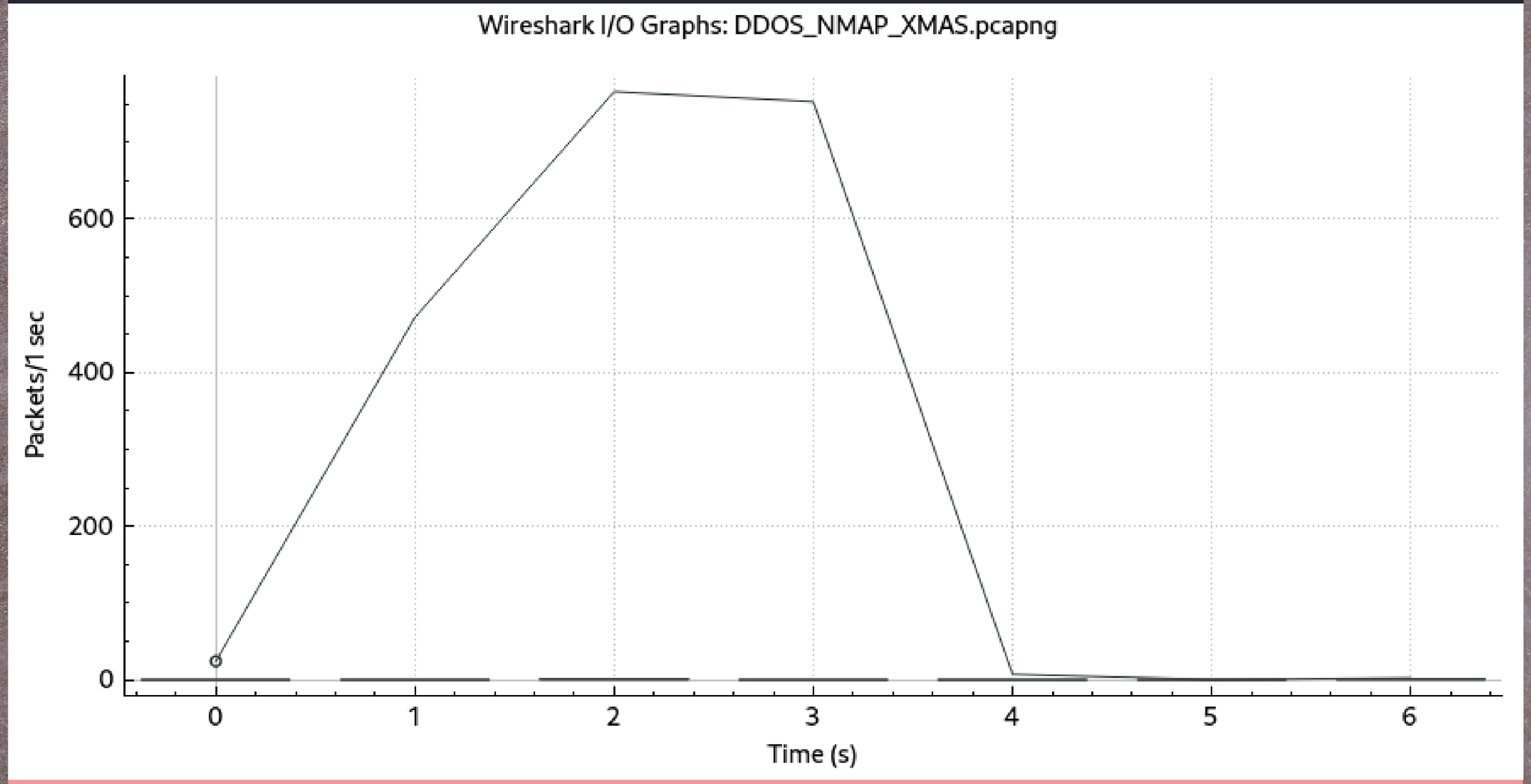
Close Help

```
▸ Frame 12: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 192.168.198.142, Dst: 172.217.194.103
▸ Transmission Control Protocol, Src Port: 40603, Dst Port: 443, Seq: 1, Len: 0

0000  00 04 00 01 00 06 00 0c  29 d8 b1 5a 00 00 08 00   ........ )..Z....
0010  45 00 00 28 00 00 40 00  40 06 44 58 c0 a8 c6 8e   E..(..@. @.DX....
0020  ac d9 c2 67 9e 9b 01 bb  7e 93 5c 10 00 00 00 00   ...g.... ~.\.....
0030  50 04 00 00 3e 6e 00 00                            P...>n..
```

DDOS_NMAP_XMAS.pcapng | Packets: 2024 · Displayed: 3 (0.1%) | Profile: Default

dari sini kita bisa melihat conversation yang dilakukan dan yang sedang terjadi, disini kita bisa melihat bahwa bila Packet B+A itu hasilnya 0, bisa safe to assume bahwa itu sedang diserang DDoS



atau kita bisa melihat melalui statistics menu, dan melihat di I/0 graphs, yang normalnya hanya 1 - 2 packets kekirim untuk satu modular, tetapi bisa dilihat graphnya bahwa hal ini tidaklah normal dan menjadi indikasi bahwa DDoS sedang dilakukan.

Itulah tiga cara menganalisis dan dan memastikan bahwa DDoS sedang dilakukan ke suatu address.

THANK YOU VERY MUCH!