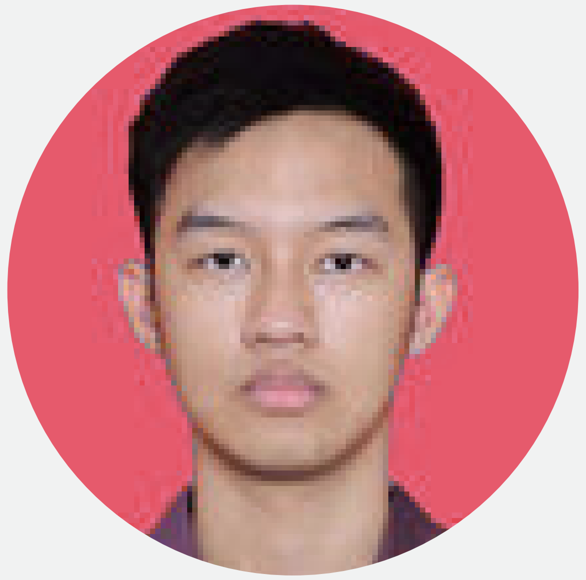
DDOS

Computer Forensic | DDOS

ANGGOTA KELOMPOK

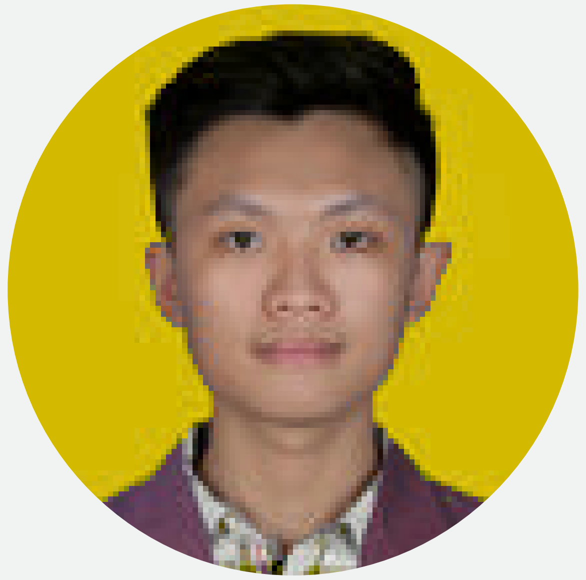
CHRISTINA
2502004235



HUGO
2501997016

MADE
2502005723

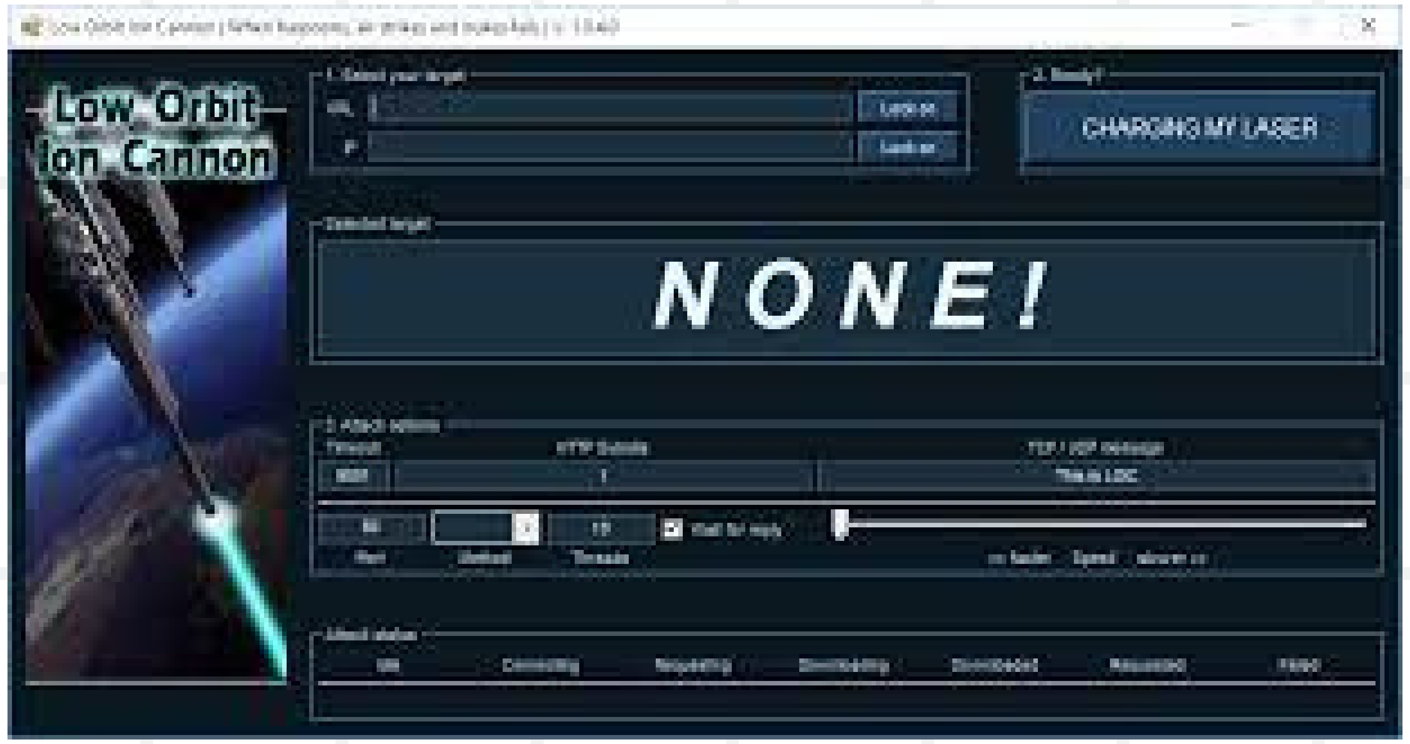
JONATHAN
2501986611



MAX
2502011360

TOOLS THAT WE USE

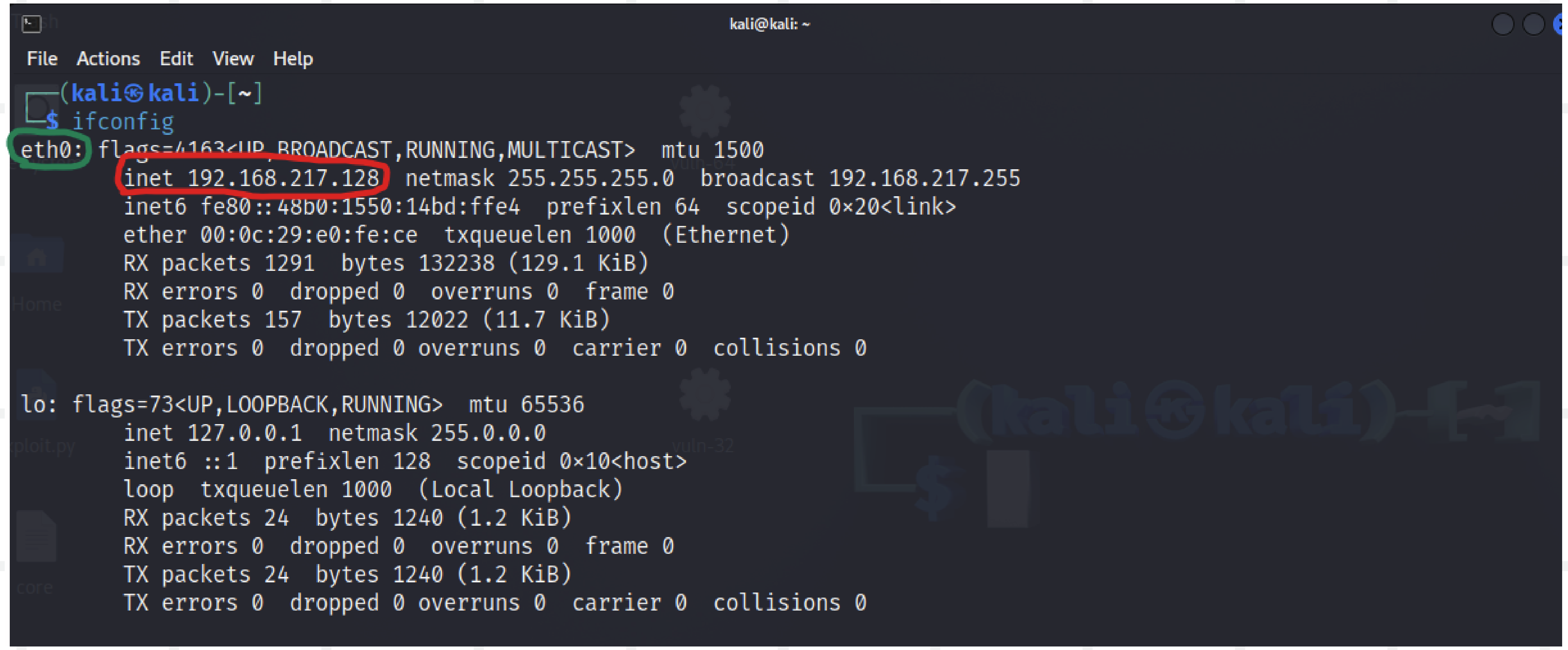
Wireshark
Aplikasi untuk melihat packet



Timeout: 9001
HTTP Subsite: /
TCP / UDP message: This is LOIC
Port: 80
Threads: 10
☑ Wait for reply
<= faster Speed slower =>

Low Orbit Ion Cannon (LOIC)
Aplikasi untuk DDOS

DOCUMENTATION

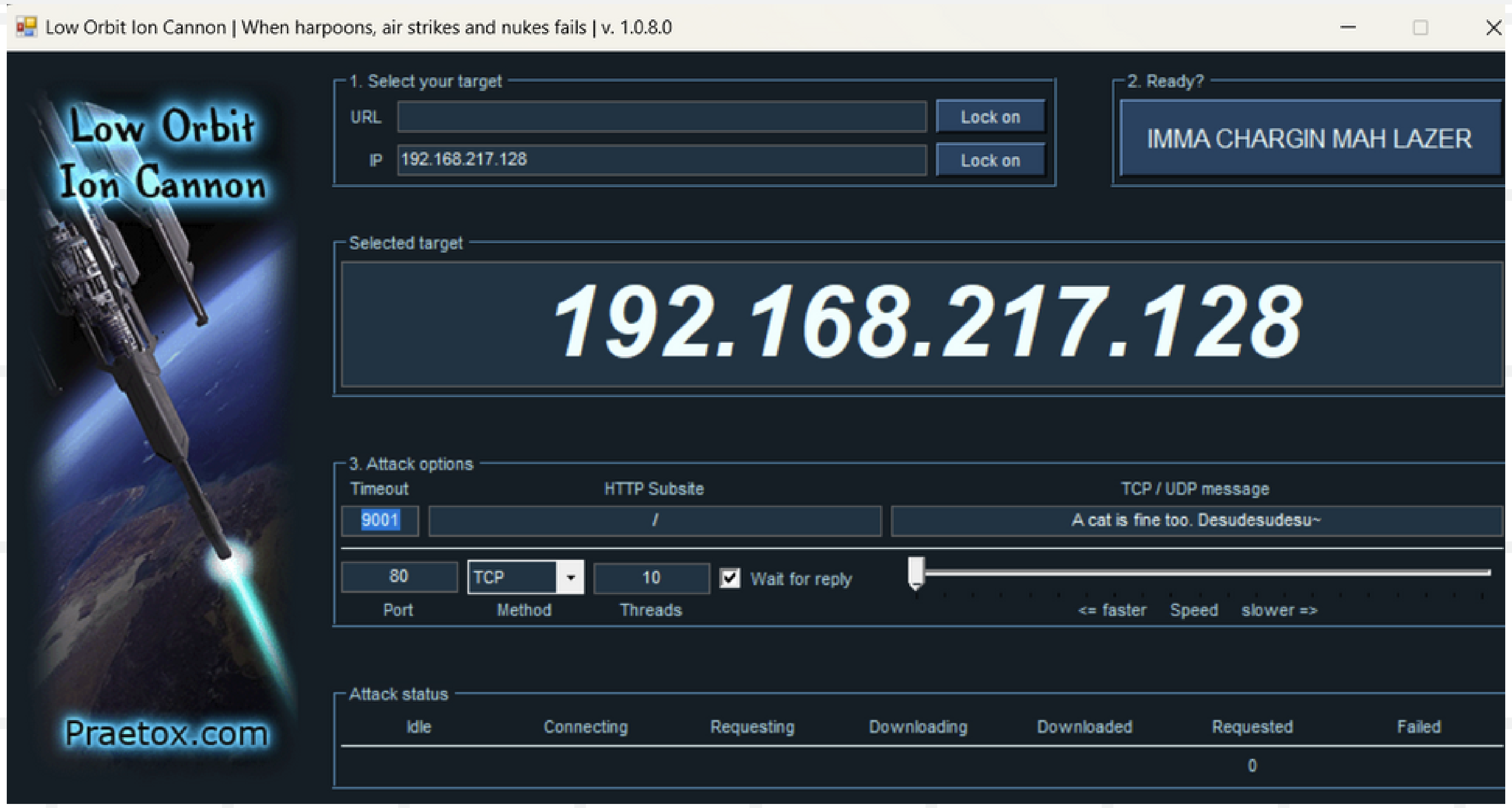


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.217.128  netmask 255.255.255.0  broadcast 192.168.217.255
        inet6 fe80::48b0:1550:14bd:ffe4  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e0:fe:ce  txqueuelen 1000  (Ethernet)
        RX packets 1291  bytes 132238 (129.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 157  bytes 12022 (11.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1240 (1.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1240 (1.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Kita liat IP target kita (dilingkari merah) dan sekalian kita liat ethernet interface (dilingkari hijau) yang dipakai

DOCUMENTATION



Low Orbit Ion Cannon | When harpoons, air strikes and nukes fails | v. 1.0.8.0

IP 192.168.217.128

Selected target: 192.168.217.128

Timeout: 9001

HTTP Subsite: /

TCP / UDP message: A cat is fine too. Desudesudesu~

Port: 80

Method: TCP

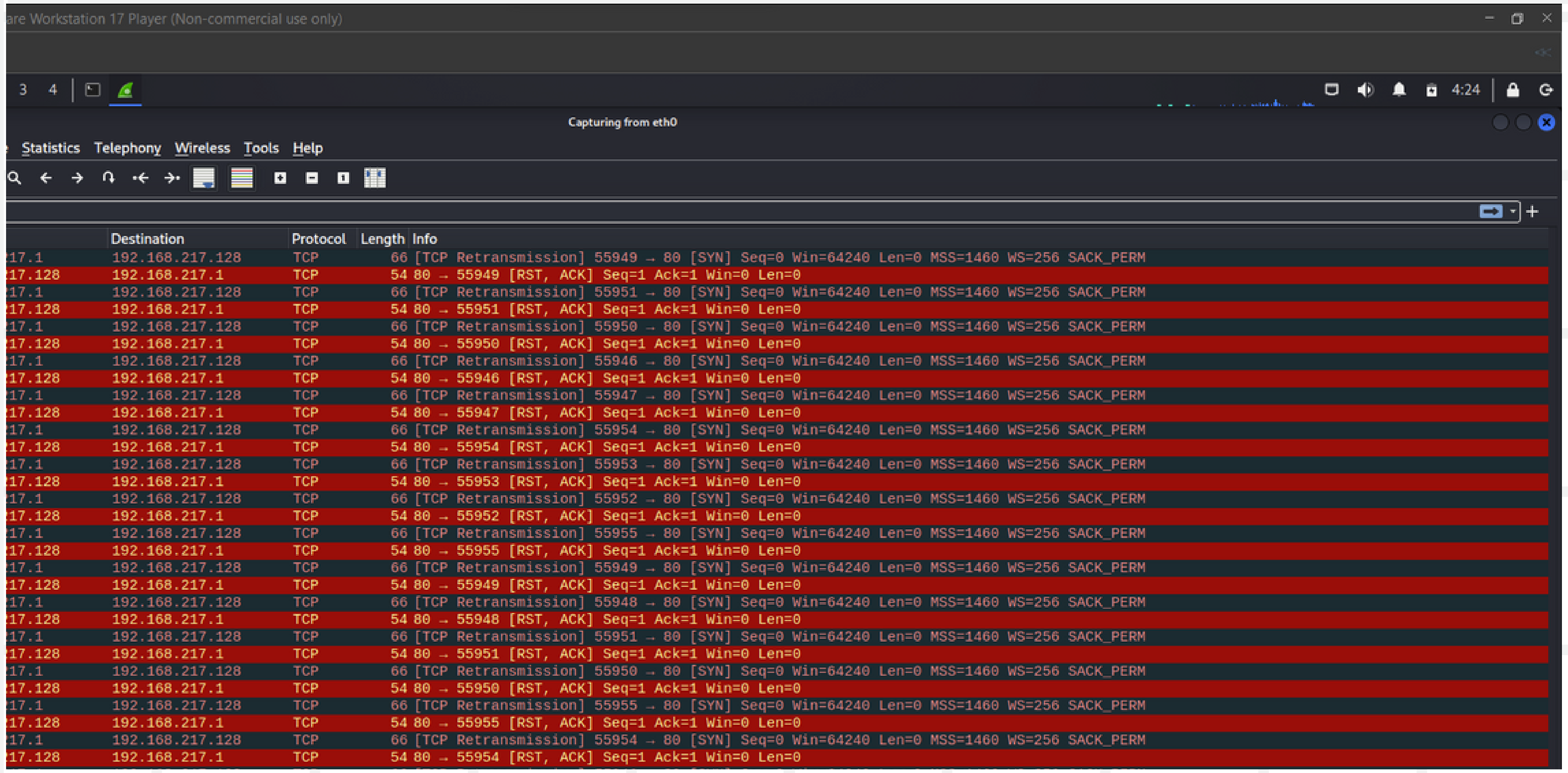
Threads: 10

☑ Wait for reply

Requested: 0

Selanjutnya di PC attacker kita masukkan IP dan methodnya. Jika sudah kita pencet “IMMA CHARGIN MAH LAZER”

DOCUMENTATION



```
         Destination      Protocol  Length Info
17.1     192.168.217.128  TCP       66 [TCP Retransmission] 55949 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17.128   192.168.217.1    TCP       54 80 → 55949 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17.1     192.168.217.128  TCP       66 [TCP Retransmission] 55951 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17.128   192.168.217.1    TCP       54 80 → 55951 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17.1     192.168.217.128  TCP       66 [TCP Retransmission] 55950 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17.128   192.168.217.1    TCP       54 80 → 55950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17.1     192.168.217.128  TCP       66 [TCP Retransmission] 55946 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17.128   192.168.217.1    TCP       54 80 → 55946 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17.1     192.168.217.128  TCP       66 [TCP Retransmission] 55947 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17.128   192.168.217.1    TCP       54 80 → 55947 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17.1     192.168.217.128  TCP       66 [TCP Retransmission] 55954 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17.128   192.168.217.1    TCP       54 80 → 55954 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17.1     192.168.217.128  TCP       66 [TCP Retransmission] 55953 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17.128   192.168.217.1    TCP       54 80 → 55953 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17.1     192.168.217.128  TCP       66 [TCP Retransmission] 55952 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17.128   192.168.217.1    TCP       54 80 → 55952 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17.1     192.168.217.128  TCP       66 [TCP Retransmission] 55955 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17.128   192.168.217.1    TCP       54 80 → 55955 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17.1     192.168.217.128  TCP       66 [TCP Retransmission] 55949 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17.128   192.168.217.1    TCP       54 80 → 55949 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17.1     192.168.217.128  TCP       66 [TCP Retransmission] 55948 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17.128   192.168.217.1    TCP       54 80 → 55948 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17.1     192.168.217.128  TCP       66 [TCP Retransmission] 55951 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17.128   192.168.217.1    TCP       54 80 → 55951 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17.1     192.168.217.128  TCP       66 [TCP Retransmission] 55950 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17.128   192.168.217.1    TCP       54 80 → 55950 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17.1     192.168.217.128  TCP       66 [TCP Retransmission] 55955 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17.128   192.168.217.1    TCP       54 80 → 55955 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17.1     192.168.217.128  TCP       66 [TCP Retransmission] 55954 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17.128   192.168.217.1    TCP       54 80 → 55954 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Jika kita kembali lagi ke PC Victim, bisa diliat di wireshark kalau ada yang mencoba mengirim packet secara banyak di victim pc kita