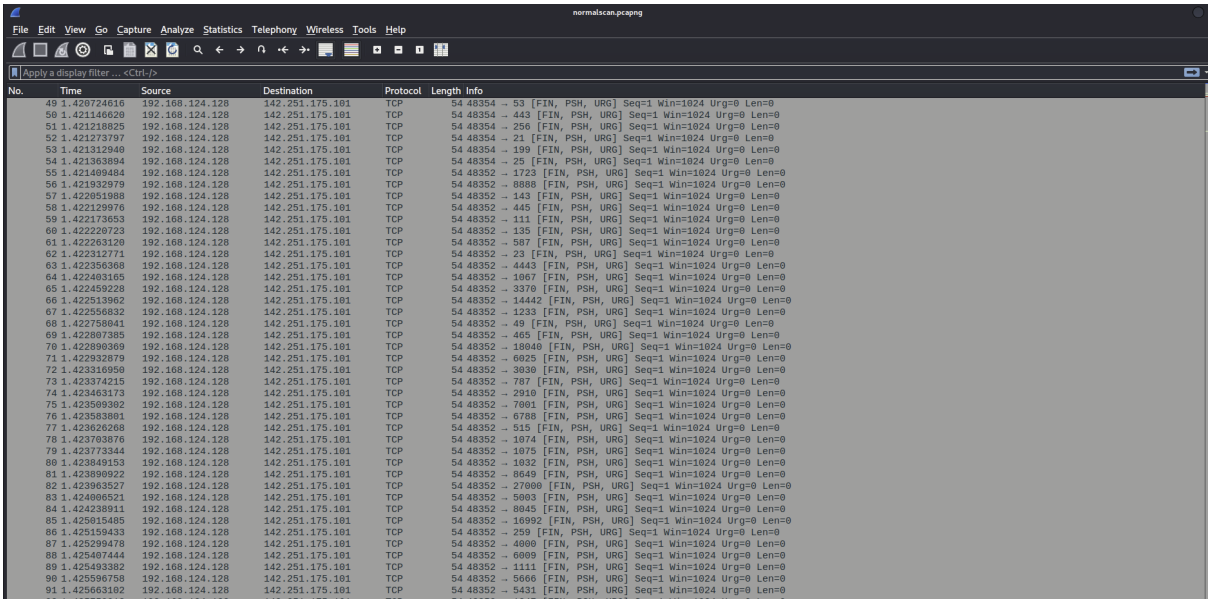
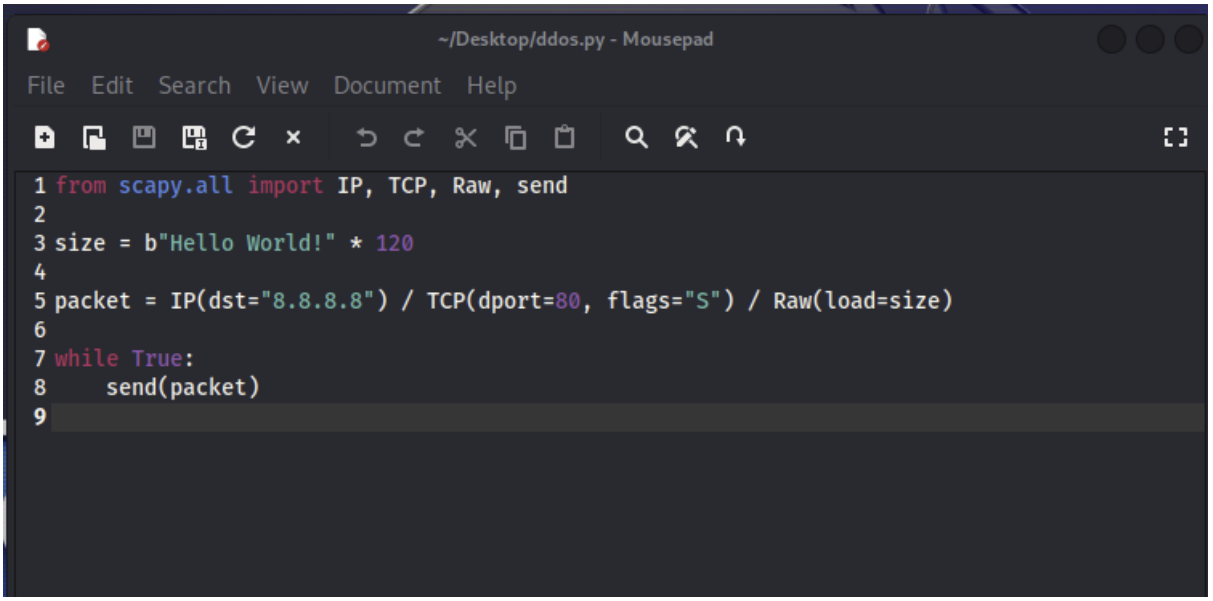
Kelompok:
2501981270 - AGUSTINUS LEONARDO DWITAMA
2501989550 - MUHAMAD DWI APRIYANTO
2502001864 - RAVI DEEVAN SATYAKI
2501965052 - KEVIN MORRIS ARMANDO
2501983723 - NATANAEL FRANSISCO

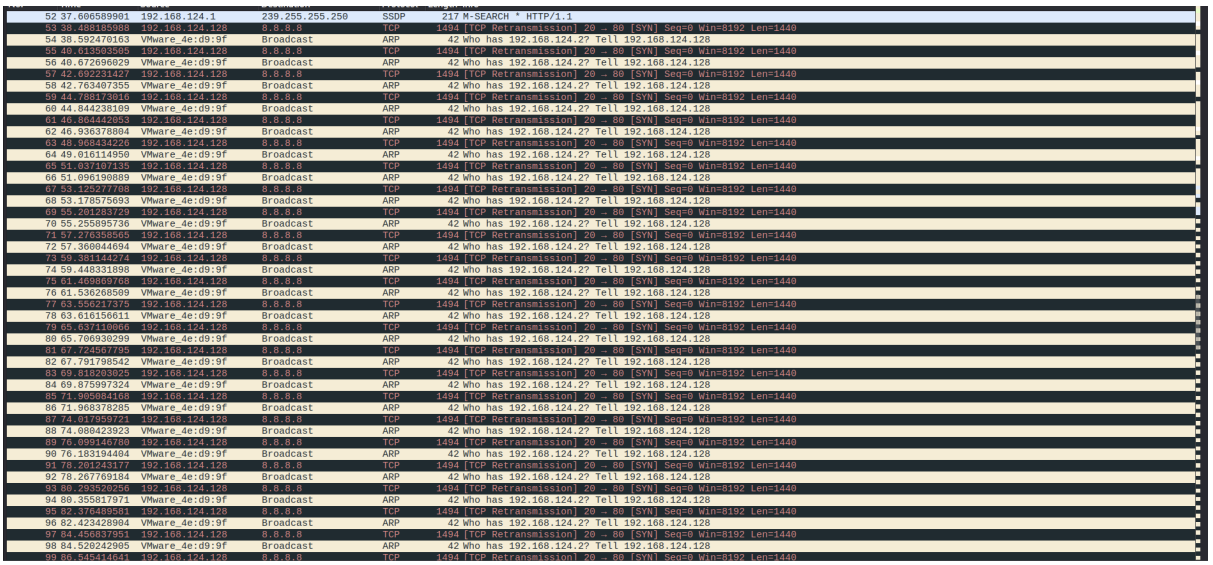
Wireshark Forensics

Normal nmap scan activity on Wireshark



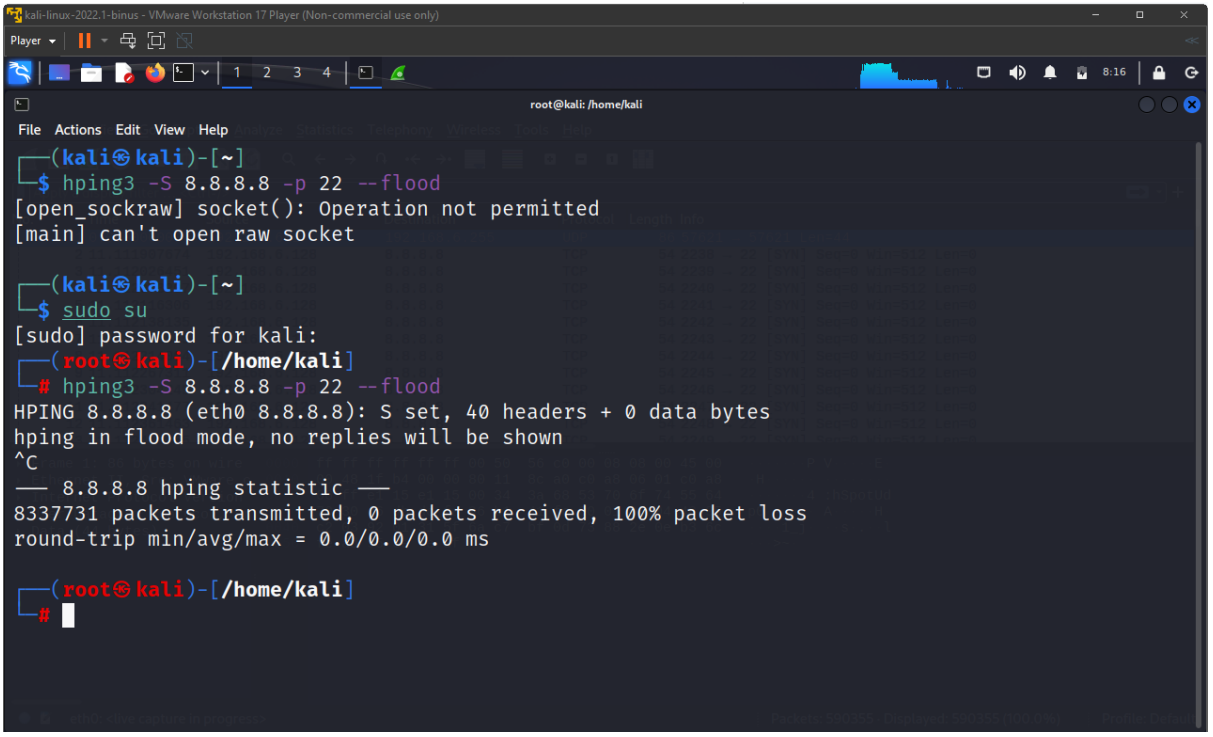
DDoS SYN Flood using python





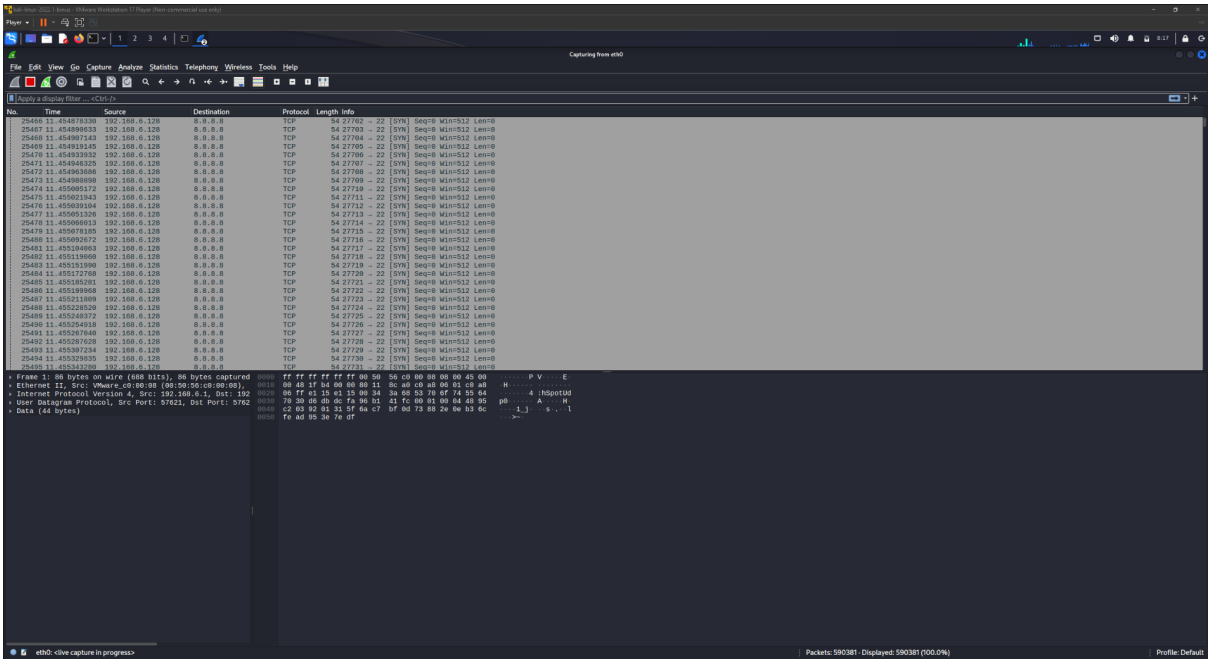
Pada DDOS attack ini, script python melakukan flood pada TCP dengan meminta request dengan length 1494 dan ARP dengan length 42. ARP merupakan protokol yang akan menanyakan MAC address ke server yang di attack lalu memberi tahukan jawabannya ke ip address kita.

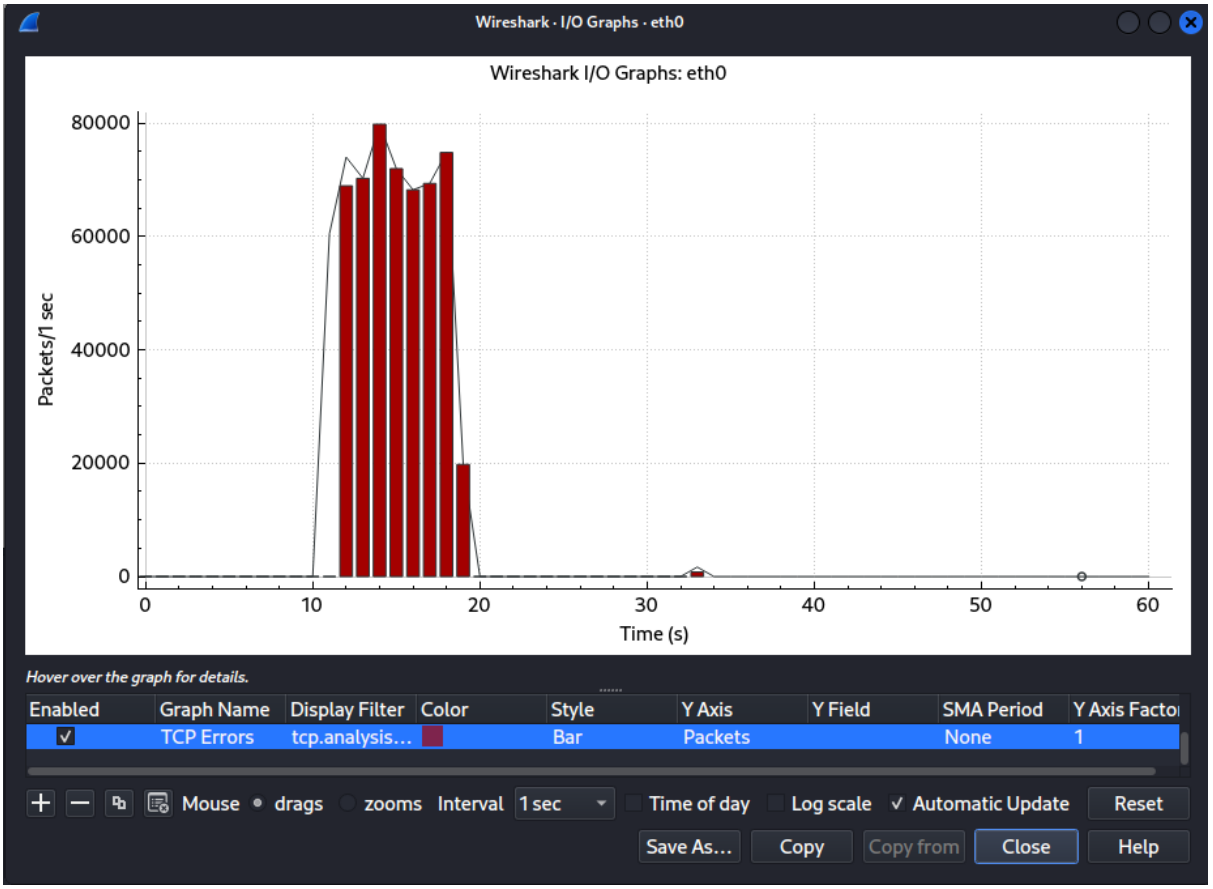
Perform DoS attack using hping3



gunakan command:
hping3 -S (Target IP Address) -p 22 –flood

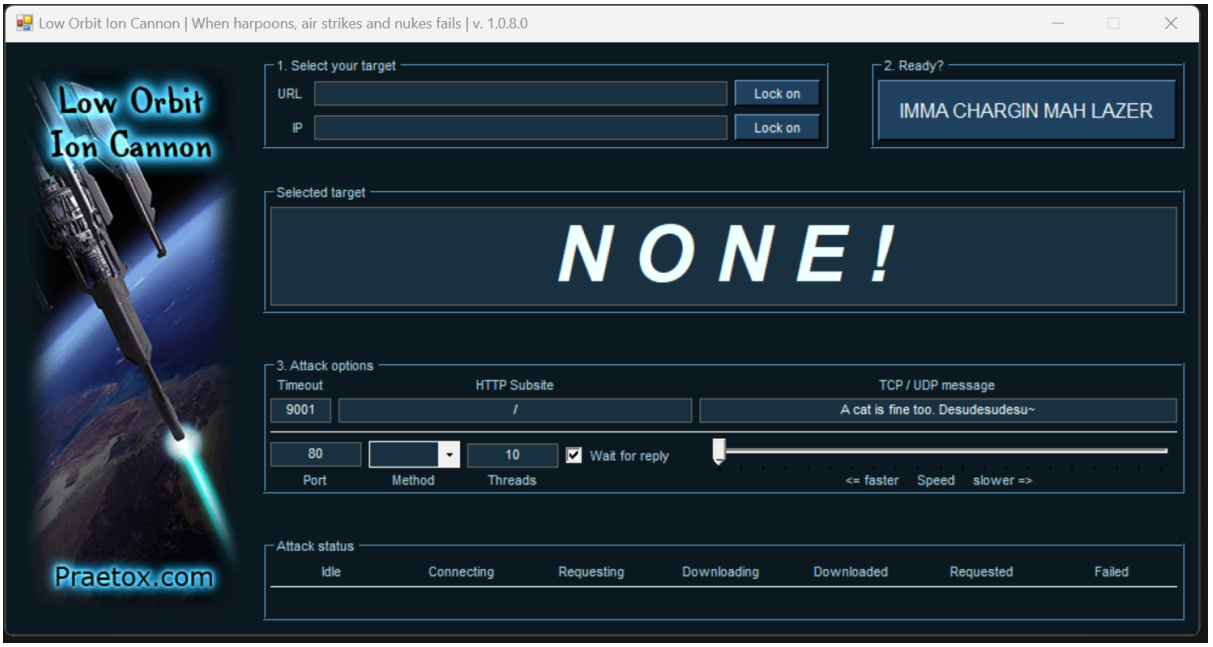
Disini kami menggunakan target 8.8.8.8 yang merupakan IP address dari google.com.

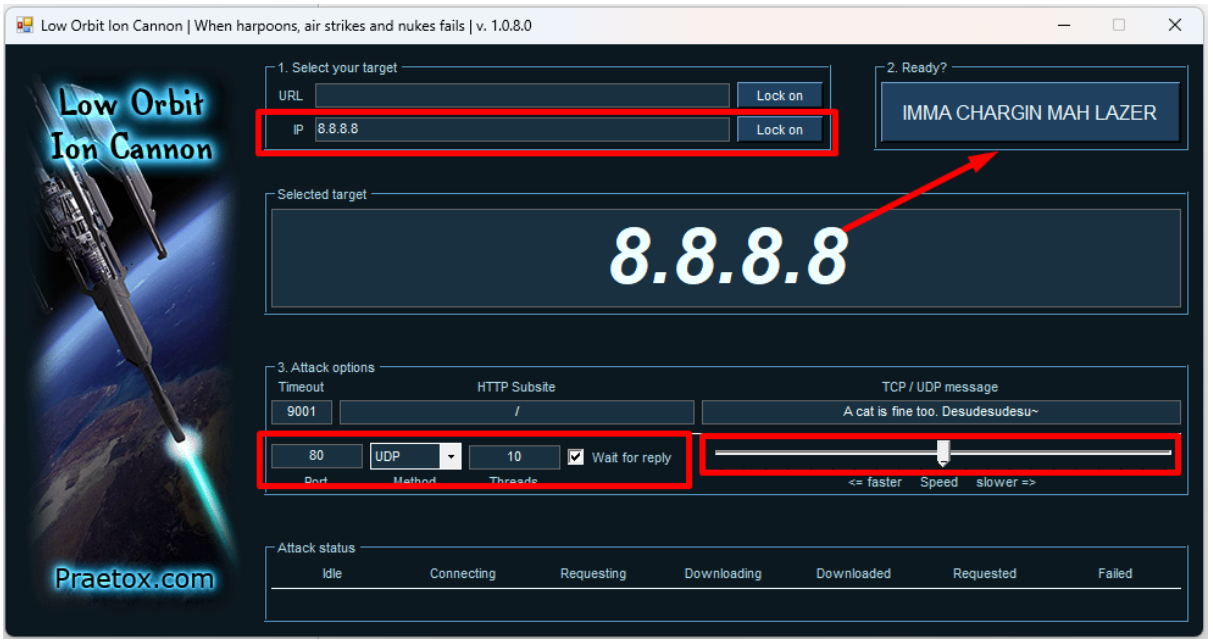




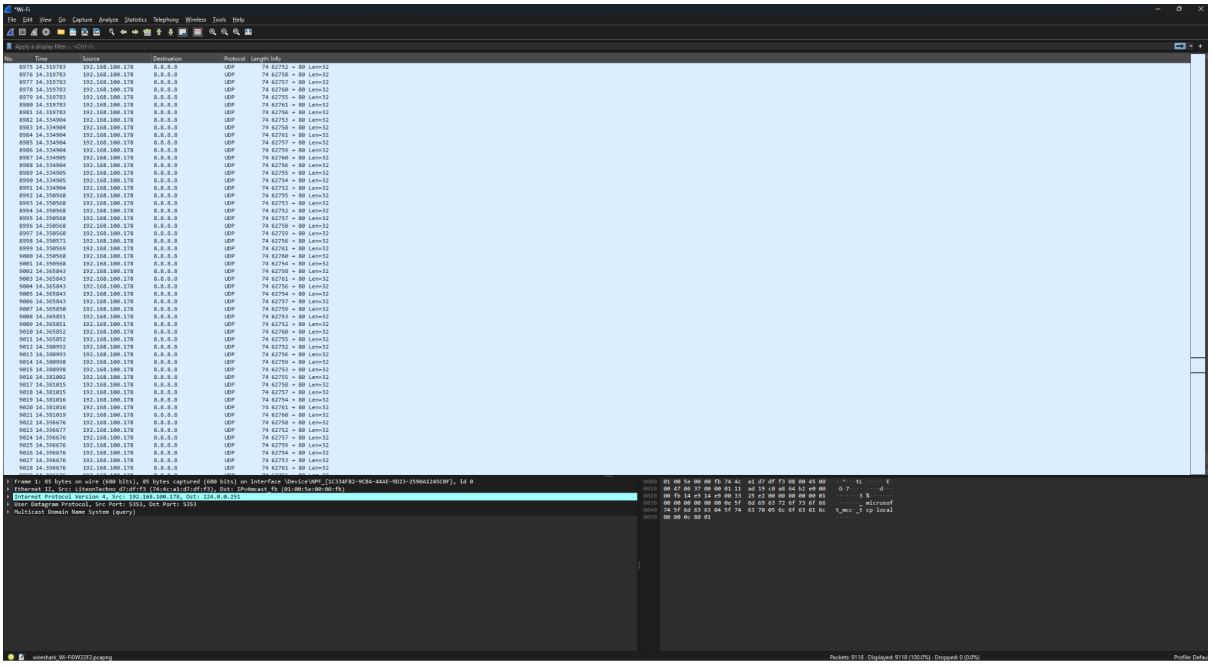
Dapat terlihat jelas pada wireshark I/O graph bahwa Kali Linux mengirimkan mengirimkan sangat banyak packets pada rentang waktu 10 - 20 detik.

Perform DDOS using Low Orbit Ion Cannon





masukkan IP Address dari google 8.8.8.8 dan dapat memilih ingin menggunakan metode UDP, TCP, HTTP.



Terlihat pada wireshark, aplikasi tersebut mencoba memflooding IP target pada protokol UDP.