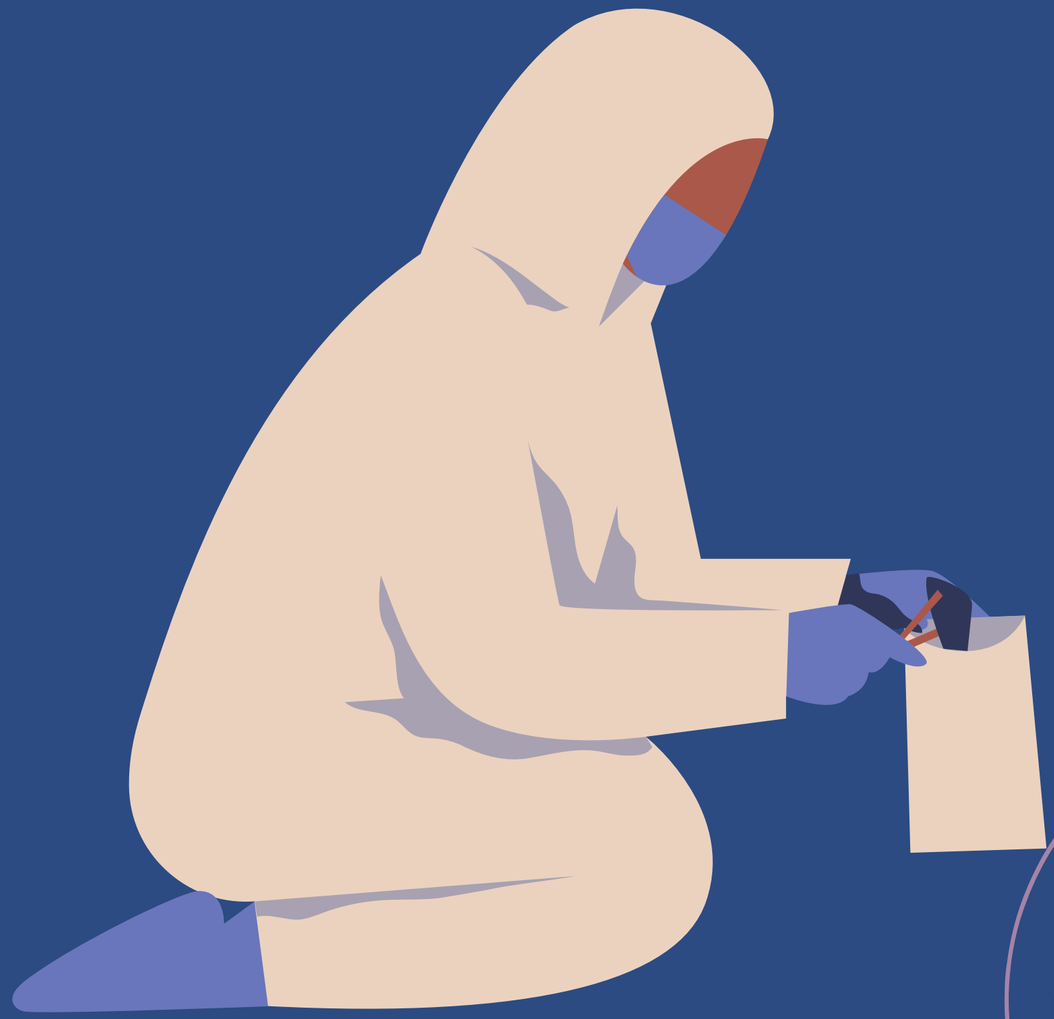
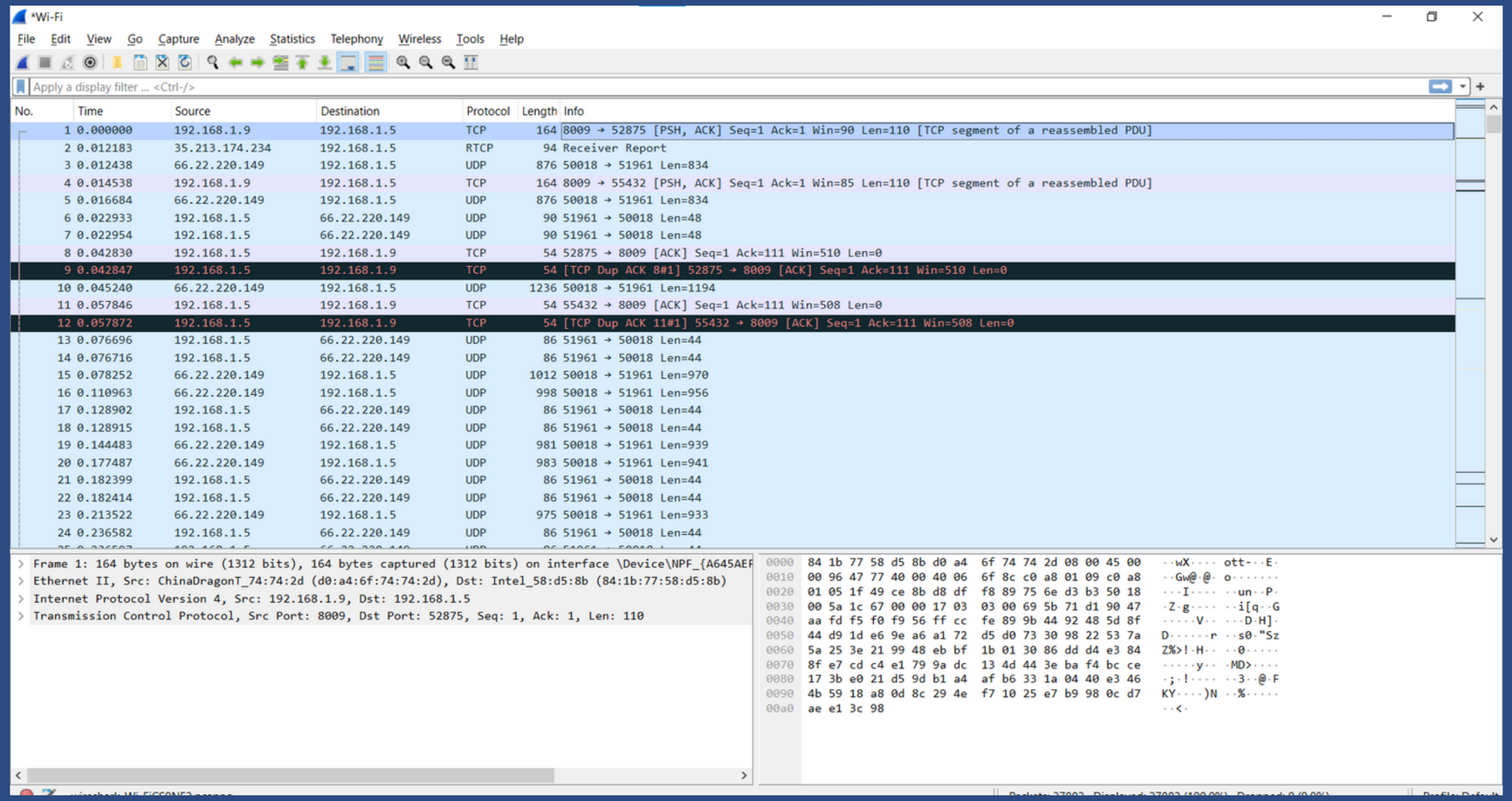
Tugas Forensic Wireshark

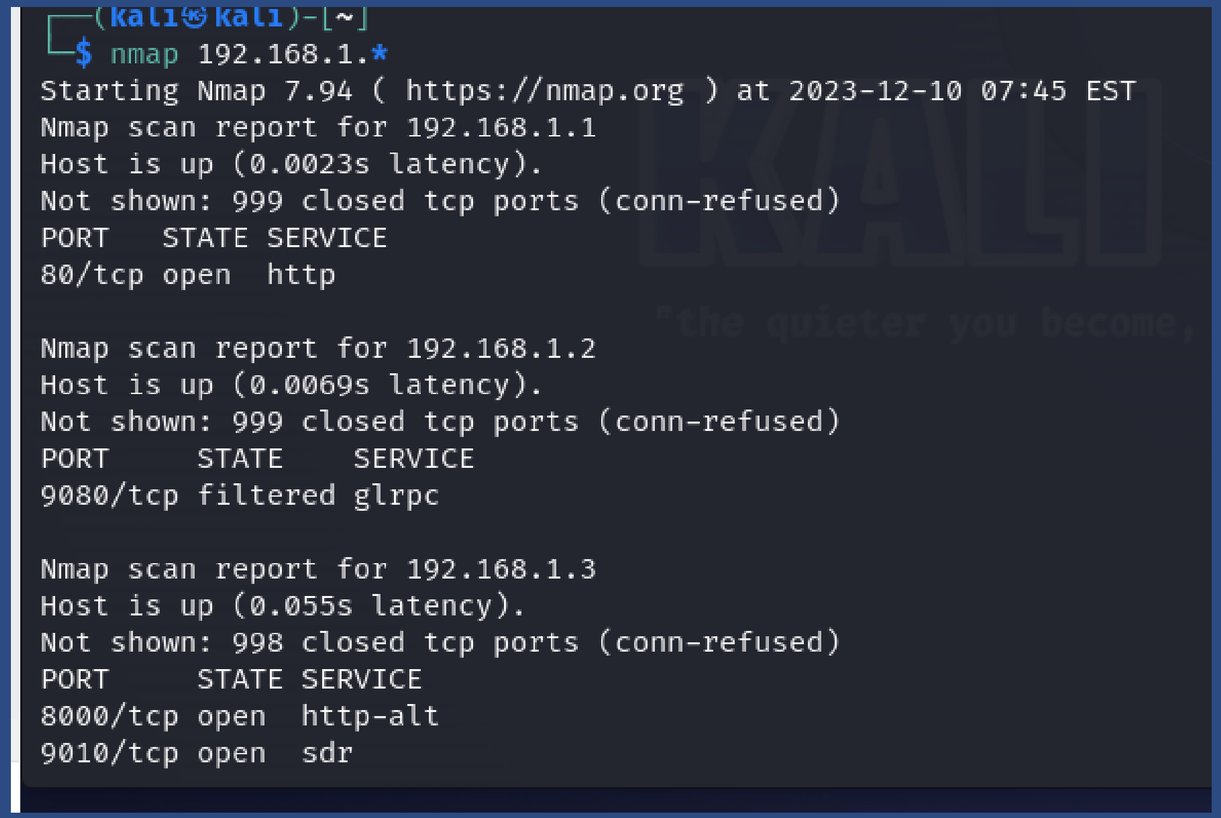
2540125384 – Benedicto Marvelous Alidajaya
2540118933 – John Orlond
2540124702 – Matthew Kurniawan



Menggunakan wireshark



- Disini saya mencoba untuk menggunakan wireshark pada sebuah Wi-Fi
- Terdapat bebrapa akitivitas

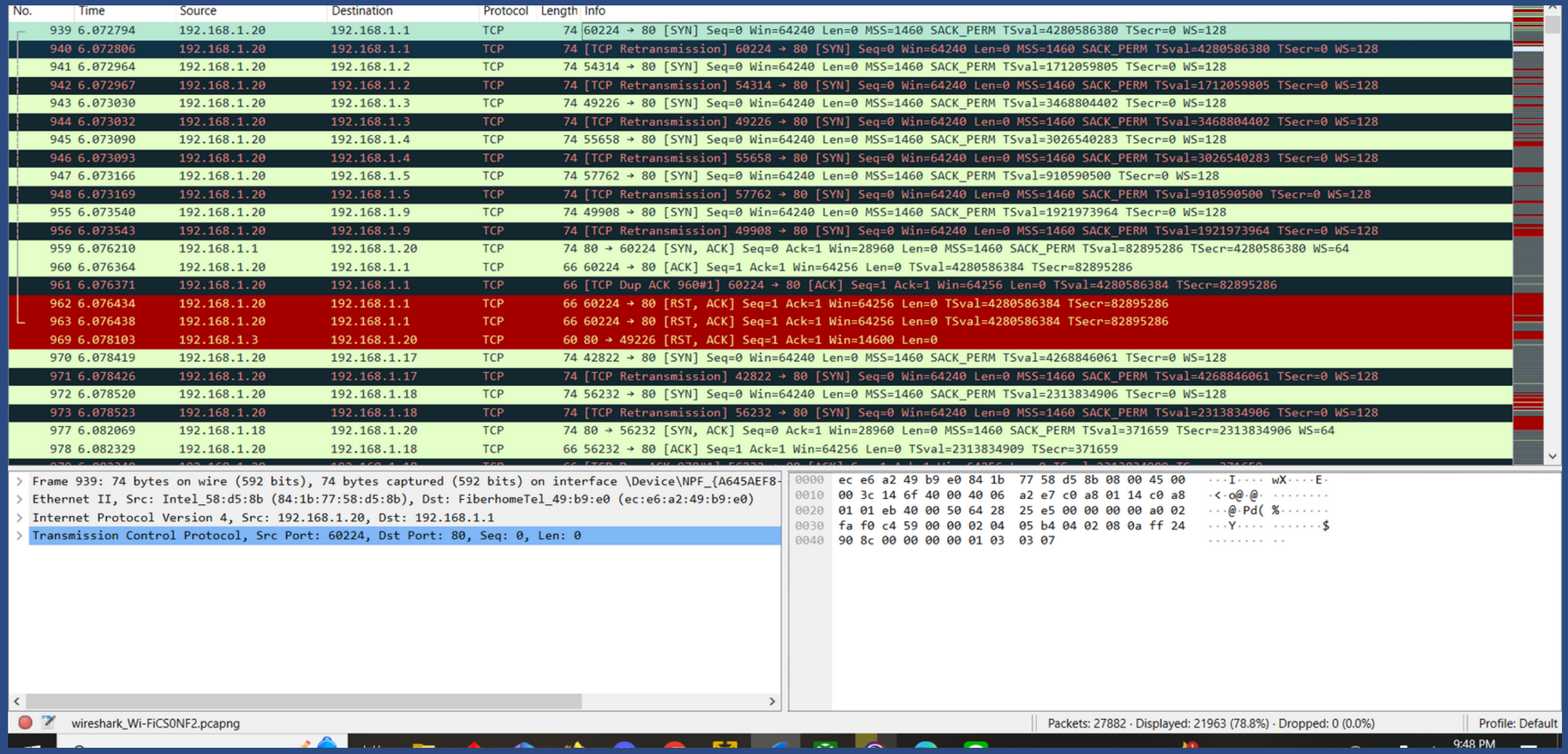


NMAP

Disini saya menggunakan nmap untuk melihat semua IP yang terdaftar dan melihat port yang terbuka di dalam IP address tersebut.

Mengidentifikasi NMAP menggunakan Wireshark

Jika kita lihat pada Wireshark, disini saya(192.168.1.20) terlihat mengeksplor network dengan melakukan request dengan length yang pendek ke ip yang tersedia dan juga port yang terbuka. Kita dapat mengetahui bahwa hal tersebut nmap juga dengan cara melihat paket SYN dengan bytes yang relatif kecil (74). Selain itu, packet SYN berdatangan dengan waktu yang relatif singkat/berdekatan yang menandakan hal ini adalah 3 way handshake. Pada akhirnya, nmap berhasil melakukan 3 way handshake dan menemukan port 80.

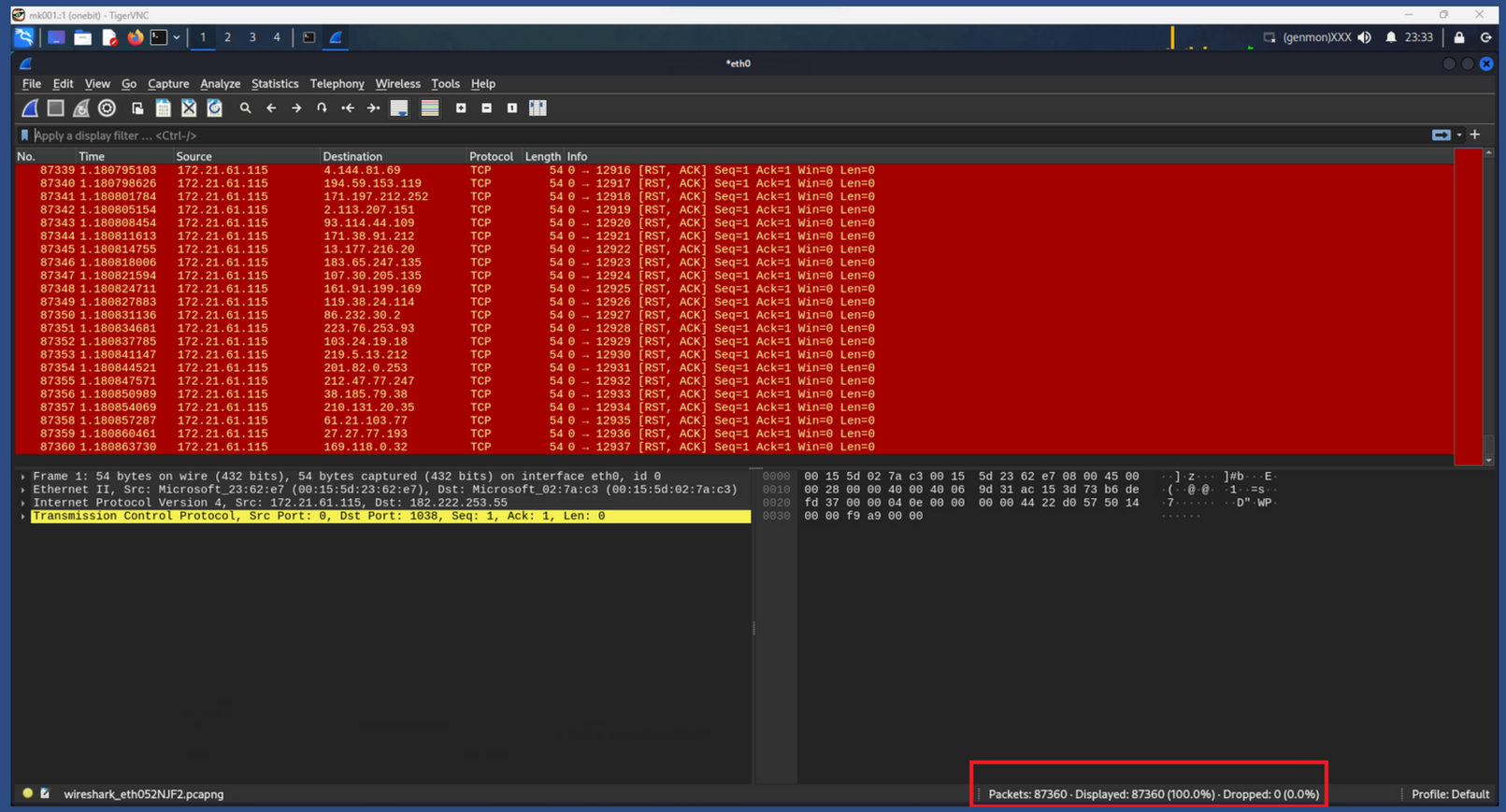


DOS

```
┌──(root㉿mk001)-[/home/onebit]
└─# hping3 -c 20000 -d 120 -S --flood --rand-source 172.21.61.115
HPING 172.21.61.115 (eth0 172.21.61.115): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

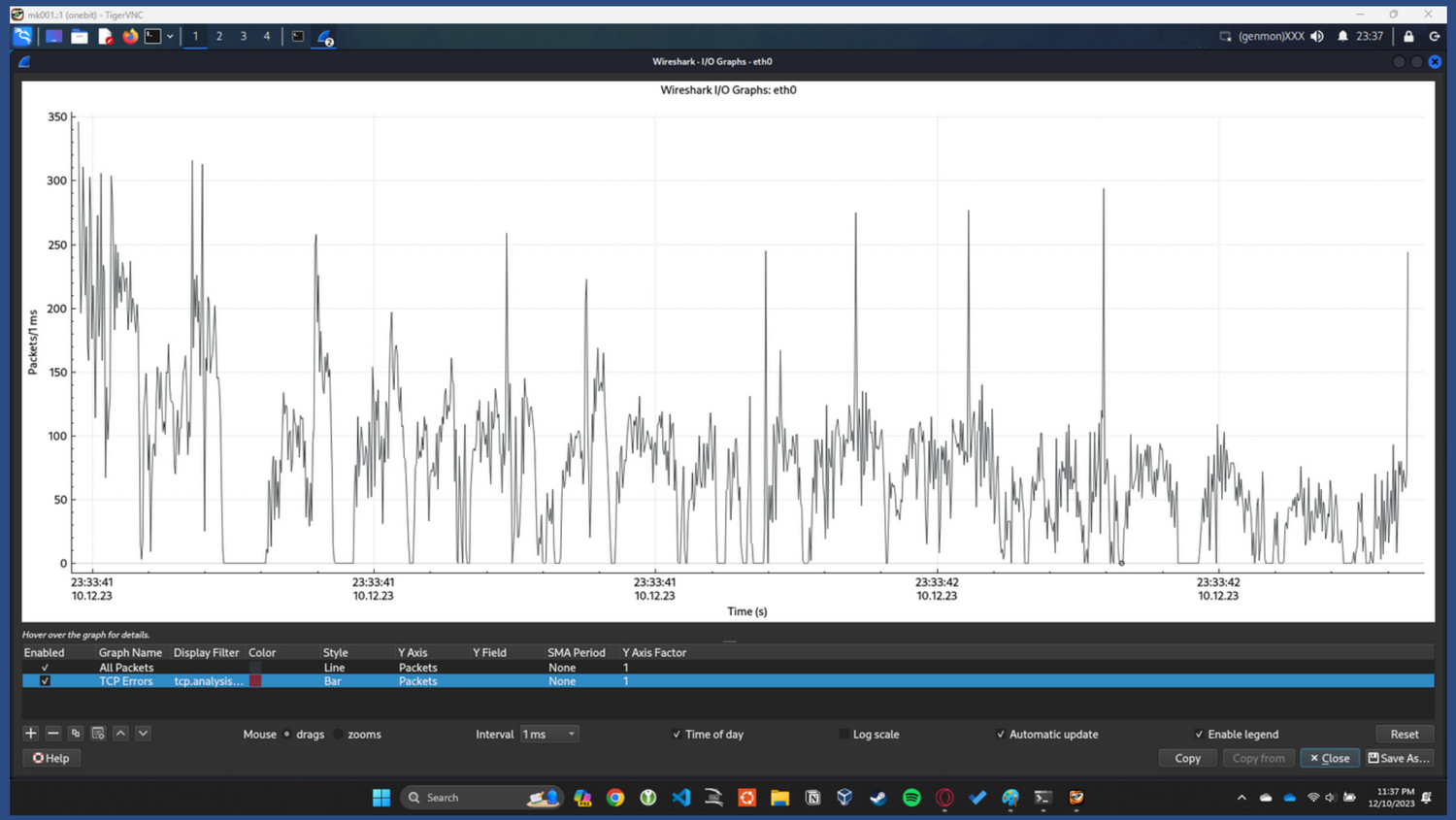
- Disini kita mencoba untuk melakukan dos ke (172.21.61.115) kita sendiri dengan melakukan floding, disini kita akan mengirimkan 20000 packet dengan size 120 byte.

Identifikasi DOS



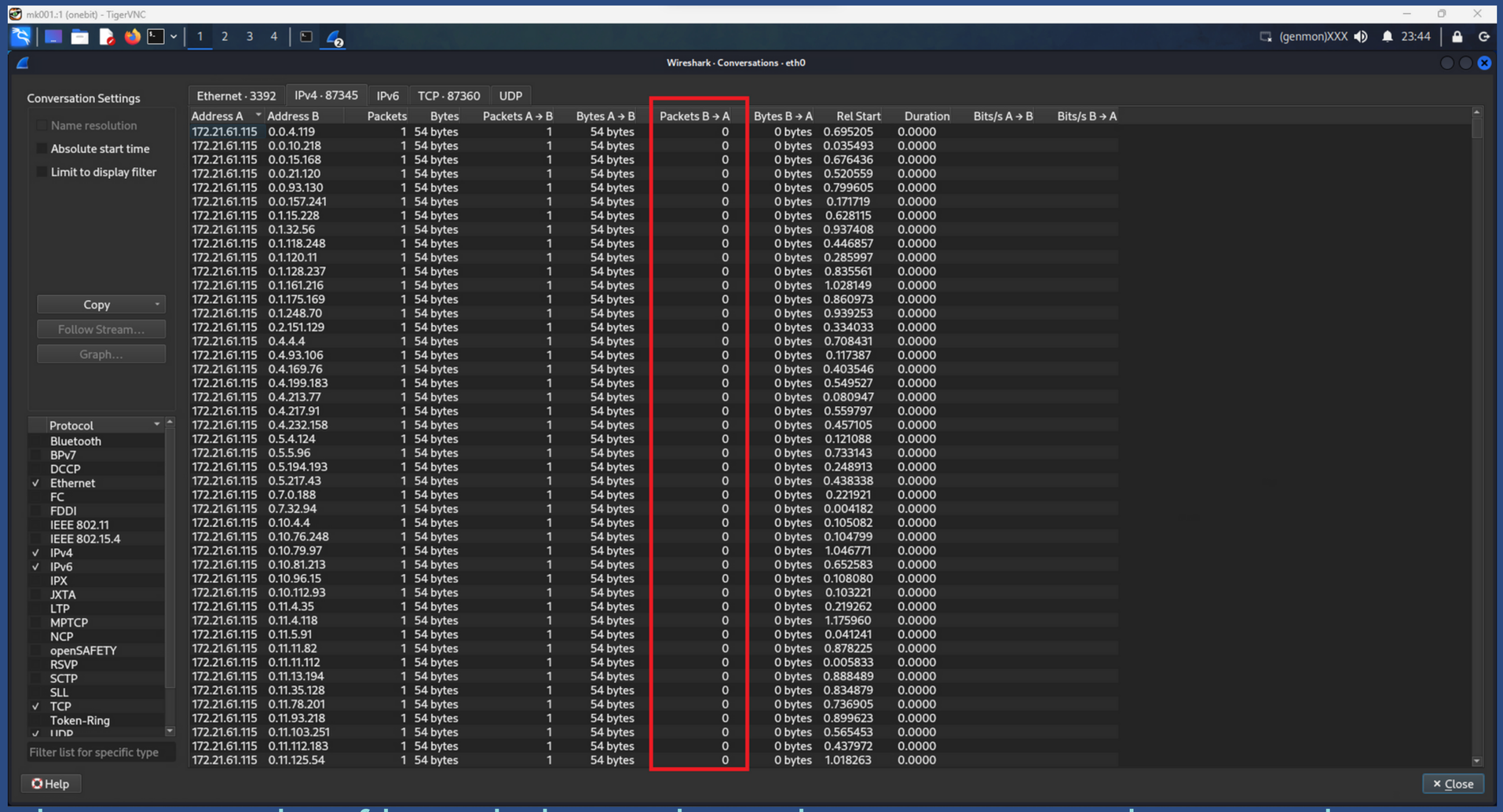
- Dengan menggunakan wireshark kita bisa melihat bahwa packet yang dikirim sebanyak 87ribu. Dimana packet tersebut dikirimkan oleh 172.21.61.115(kita)

Identifikasi DOS



- Dengan menggunakan wireshark kita juga bisa melihat rate packet yang dikirim /1ms

Identifikasi DOS



Ethernet · 3392 | IPv4 · 87345 | IPv6 | TCP · 87360 | UDP

Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
172.21.61.115	0.0.4.119	1	54 bytes	1	54 bytes	0	0 bytes	0.695205	0.0000		
172.21.61.115	0.0.10.218	1	54 bytes	1	54 bytes	0	0 bytes	0.035493	0.0000		
172.21.61.115	0.0.15.168	1	54 bytes	1	54 bytes	0	0 bytes	0.676436	0.0000		
172.21.61.115	0.0.21.120	1	54 bytes	1	54 bytes	0	0 bytes	0.520559	0.0000		
172.21.61.115	0.0.93.130	1	54 bytes	1	54 bytes	0	0 bytes	0.799605	0.0000		
172.21.61.115	0.0.157.241	1	54 bytes	1	54 bytes	0	0 bytes	0.171719	0.0000		
172.21.61.115	0.1.15.228	1	54 bytes	1	54 bytes	0	0 bytes	0.628115	0.0000		
172.21.61.115	0.1.32.56	1	54 bytes	1	54 bytes	0	0 bytes	0.937408	0.0000		
172.21.61.115	0.1.118.248	1	54 bytes	1	54 bytes	0	0 bytes	0.446857	0.0000		
172.21.61.115	0.1.120.11	1	54 bytes	1	54 bytes	0	0 bytes	0.285997	0.0000		
172.21.61.115	0.1.128.237	1	54 bytes	1	54 bytes	0	0 bytes	0.835561	0.0000		
172.21.61.115	0.1.161.216	1	54 bytes	1	54 bytes	0	0 bytes	1.028149	0.0000		
172.21.61.115	0.1.175.169	1	54 bytes	1	54 bytes	0	0 bytes	0.860973	0.0000		
172.21.61.115	0.1.248.70	1	54 bytes	1	54 bytes	0	0 bytes	0.939253	0.0000		
172.21.61.115	0.2.151.129	1	54 bytes	1	54 bytes	0	0 bytes	0.334033	0.0000		
172.21.61.115	0.4.4.4	1	54 bytes	1	54 bytes	0	0 bytes	0.708431	0.0000		
172.21.61.115	0.4.93.106	1	54 bytes	1	54 bytes	0	0 bytes	0.117387	0.0000		
172.21.61.115	0.4.169.76	1	54 bytes	1	54 bytes	0	0 bytes	0.403546	0.0000		
172.21.61.115	0.4.199.183	1	54 bytes	1	54 bytes	0	0 bytes	0.549527	0.0000		
172.21.61.115	0.4.213.77	1	54 bytes	1	54 bytes	0	0 bytes	0.080947	0.0000		
172.21.61.115	0.4.217.91	1	54 bytes	1	54 bytes	0	0 bytes	0.559797	0.0000		
172.21.61.115	0.4.232.158	1	54 bytes	1	54 bytes	0	0 bytes	0.457105	0.0000		
172.21.61.115	0.5.4.124	1	54 bytes	1	54 bytes	0	0 bytes	0.121088	0.0000		
172.21.61.115	0.5.5.96	1	54 bytes	1	54 bytes	0	0 bytes	0.733143	0.0000		
172.21.61.115	0.5.194.193	1	54 bytes	1	54 bytes	0	0 bytes	0.248913	0.0000		
172.21.61.115	0.5.217.43	1	54 bytes	1	54 bytes	0	0 bytes	0.438338	0.0000		
172.21.61.115	0.7.0.188	1	54 bytes	1	54 bytes	0	0 bytes	0.221921	0.0000		
172.21.61.115	0.7.32.94	1	54 bytes	1	54 bytes	0	0 bytes	0.004182	0.0000		
172.21.61.115	0.10.4.4	1	54 bytes	1	54 bytes	0	0 bytes	0.105082	0.0000		
172.21.61.115	0.10.76.248	1	54 bytes	1	54 bytes	0	0 bytes	0.104799	0.0000		
172.21.61.115	0.10.79.97	1	54 bytes	1	54 bytes	0	0 bytes	1.046771	0.0000		
172.21.61.115	0.10.81.213	1	54 bytes	1	54 bytes	0	0 bytes	0.652583	0.0000		
172.21.61.115	0.10.96.15	1	54 bytes	1	54 bytes	0	0 bytes	0.108080	0.0000		
172.21.61.115	0.10.112.93	1	54 bytes	1	54 bytes	0	0 bytes	0.103221	0.0000		
172.21.61.115	0.11.4.35	1	54 bytes	1	54 bytes	0	0 bytes	0.219262	0.0000		
172.21.61.115	0.11.4.118	1	54 bytes	1	54 bytes	0	0 bytes	1.175960	0.0000		
172.21.61.115	0.11.5.91	1	54 bytes	1	54 bytes	0	0 bytes	0.041241	0.0000		
172.21.61.115	0.11.11.82	1	54 bytes	1	54 bytes	0	0 bytes	0.878225	0.0000		
172.21.61.115	0.11.11.112	1	54 bytes	1	54 bytes	0	0 bytes	0.005833	0.0000		
172.21.61.115	0.11.13.194	1	54 bytes	1	54 bytes	0	0 bytes	0.888489	0.0000		
172.21.61.115	0.11.35.128	1	54 bytes	1	54 bytes	0	0 bytes	0.834879	0.0000		
172.21.61.115	0.11.78.201	1	54 bytes	1	54 bytes	0	0 bytes	0.736905	0.0000		
172.21.61.115	0.11.93.218	1	54 bytes	1	54 bytes	0	0 bytes	0.899623	0.0000		
172.21.61.115	0.11.103.251	1	54 bytes	1	54 bytes	0	0 bytes	0.565453	0.0000		
172.21.61.115	0.11.112.183	1	54 bytes	1	54 bytes	0	0 bytes	0.437972	0.0000		
172.21.61.115	0.11.125.54	1	54 bytes	1	54 bytes	0	0 bytes	1.018263	0.0000		

- Kita bisa mengidentifikasi bahwa jika ada ip yang terkirim packet namun tidak mengembalikan packet kembali maka ada kemungkinan bahwa itu merupakan DOS