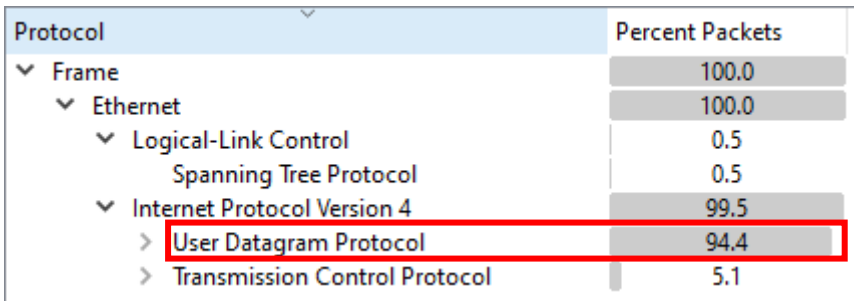
The Transport Layer

Bogdan Tatu – Gr. 3.1

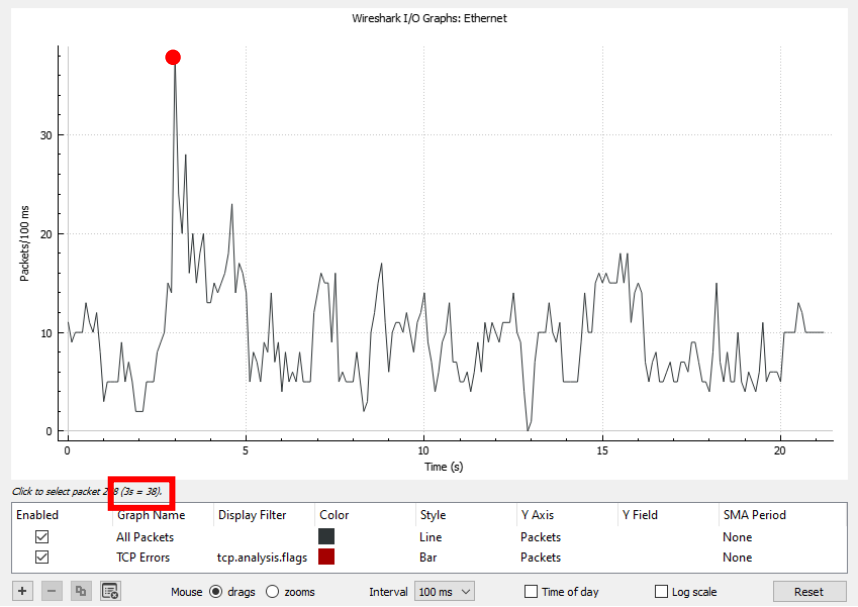
I. Statistics

1. UDP – 94.4% (I was on discord at the time)

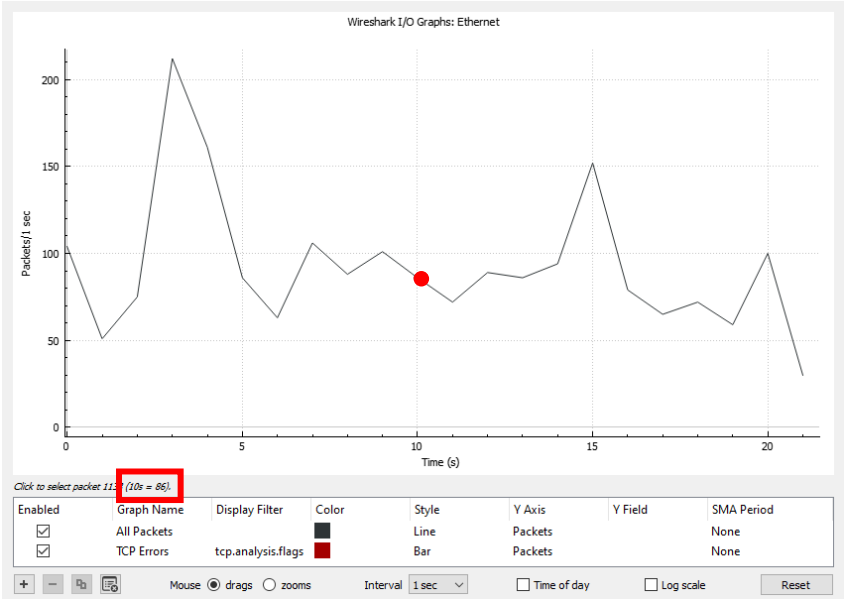


2. I/O Graph

a. 38 packets – 3s after start

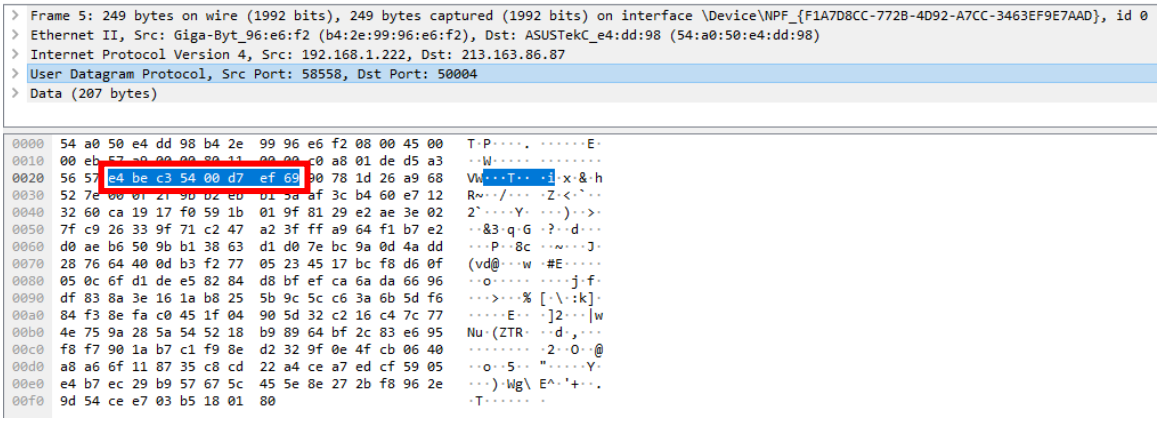


b. Second 10: 86pks/s



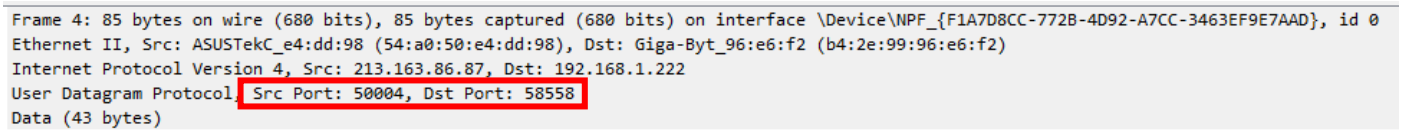
II. UDP

3. UDP Header Length: 8 bytes

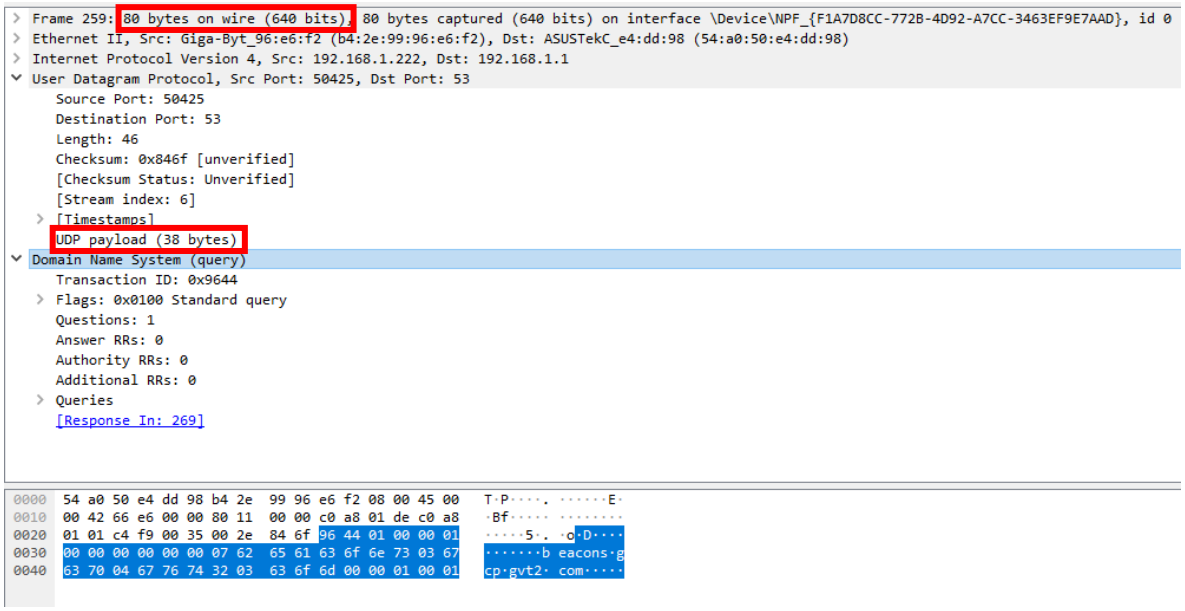


4. 4th UDP Frame:

- Source Port: 50004
- Destination Port: 58558



5. DNS Headers Length: Frame Length – Payload = 80 – 38 = 42 bytes

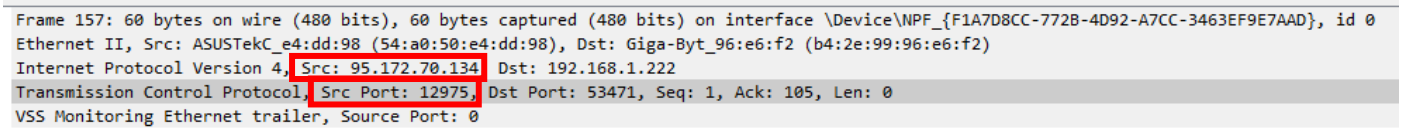


III. TCP

6. SRC Socket 10th TCP Frame: 95.172.70.134:12975

SRC IP Address: 95.172.70.134

SRC TCP Port: 12975



7. Difference between SYN and SYN-ACK

153	1.782561	192.168.1.222	192.168.1.113	TCP	164	58718 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=63470 Len=110 [TCP segment of a reassembled PDU]
154	1.784650	192.168.1.113	192.168.1.222	TCP	164	8009 → 58718 [PSH, ACK] Seq=1 Ack=111 Win=65535 Len=110 [TCP segment of a reassembled PDU]

SYN Time: 1.782561 seconds

SYN-ACK Time: 1.784650 seconds

Difference: 0.002089 seconds

8. Sum of all Headers TCP Packet: Frame Length – Payload = 239 – 185 = 54 bytes

```
Frame 169: 239 bytes on wire (1912 bits), 239 bytes captured (1912 bits) on interface \Device\NPF_{F1A7D8CC-772B-4D92-A7CC-3463EF9E7AAD}, id 0
Ethernet II, Src: Giga-Byt_96:e6:f2 (b4:2e:99:96:e6:f2), Dst: ASUSTekC_e4:dd:98 (54:a0:50:e4:dd:98)
Internet Protocol Version 4, Src: 192.168.1.222, Dst: 208.70.247.107
Transmission Control Protocol, Src Port: 58733, Dst Port: 443, Seq: 102, Ack: 1392, Len: 185
    Source Port: 58733
    Destination Port: 443
    [Stream index: 2]
    [TCP Segment Len: 185]
    Sequence Number: 102    (relative sequence number)
    Sequence Number (raw): 2036707638
    [Next Sequence Number: 287    (relative sequence number)]
    Acknowledgment Number: 1392    (relative ack number)
    Acknowledgment number (raw): 956146127
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window: 63949
    [Calculated window size: 63949]
    [Window size scaling factor: -1 (unknown)]
    Checksum: 0x8b0c [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (185 bytes)
```