

The Transport Layer

Bogdan Tatu – Gr. 3.1

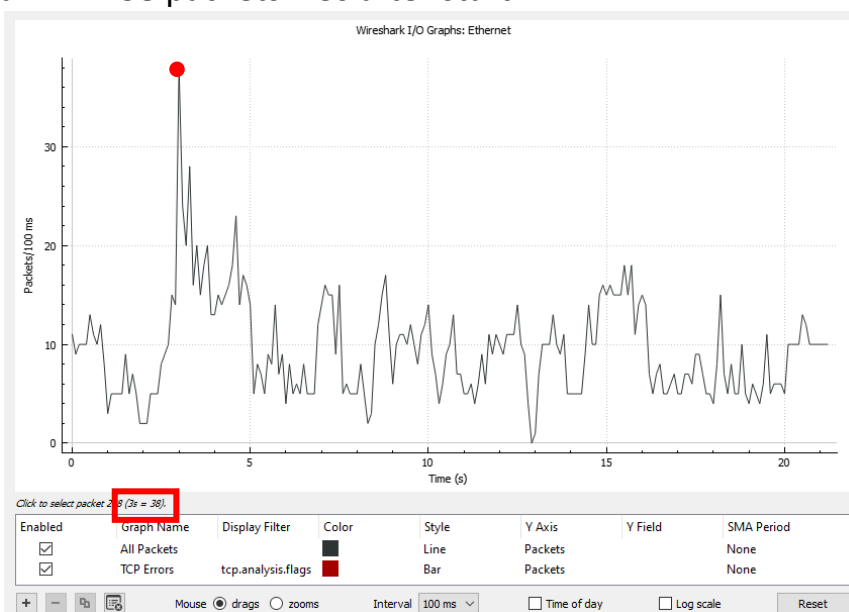
I. Statistics

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

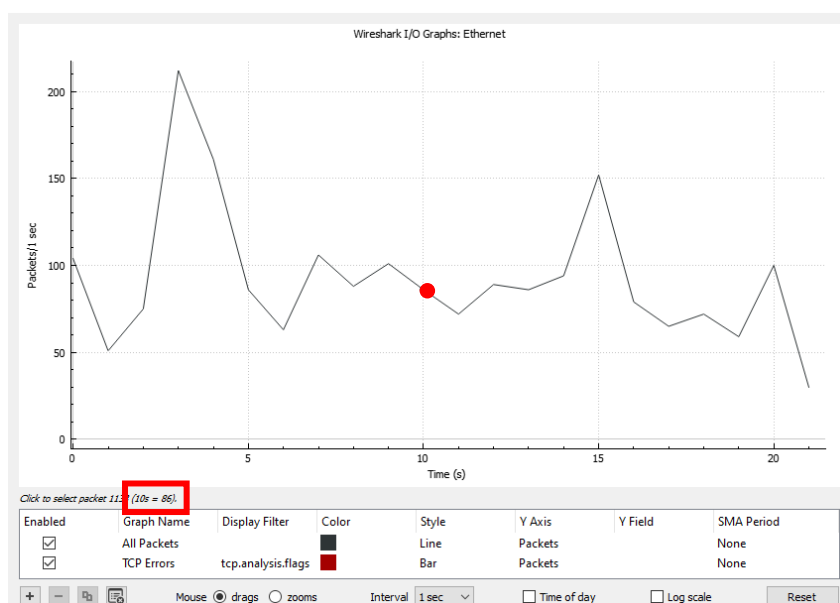
Protocol	Percent Packets
▼ Frame	100.0
▼ Ethernet	100.0
▼ Logical-Link Control	0.5
Spanning Tree Protocol	0.5
▼ Internet Protocol Version 4	99.5
> User Datagram Protocol	94.4
> Transmission Control Protocol	5.1

2. I/O Graph

a. 38 packets – 3s after start



b. Second 10: 86pk/s



II. UDP

3. UDP Header Length: 8 bytes

```
> Frame 5: 249 bytes on wire (1992 bits), 249 bytes captured (1992 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: 213.163.86.87
> User Datagram Protocol, Src Port: 58558, Dst Port: 50004
> Data (207 bytes)
```

```
0000 54 a0 50 e4 dd 98 b4 2e 99 96 e6 f2 08 00 45 00  T.P.... .E.
0010 00 eb f3 00 00 00 00 11 00 00 c0 a8 01 de d5 a3  .W....
0020 56 57 e4 be c3 54 00 d7 ef 68 90 78 1d 26 a9 68  V....T... x & h
0030 52 7e 00 01 21 90 b2 e0 01 3a af 3c b4 60 e7 12  R.../... Z<...
0040 32 60 ca 19 17 f0 59 1b 01 9f 81 29 e2 ae 3e 02  2'....Y...>
0050 7f c9 26 33 9f 71 c2 47 a2 3f ff a9 64 f1 b7 e2  .&3 q G ? d...
0060 d0 ae b6 50 9b b1 38 63 d1 d0 7e bc 9a 0d 4a dd  .P..8c ...J.
0070 28 76 64 40 0d b3 f2 77 05 23 45 17 bc f8 d6 0f  (vd@...w #E....
0080 05 0c 6f d1 de e5 82 84 d8 bf ef ca 6a da 66 96  .o.... j.f...
0090 df 83 8a 3e 16 1a b8 25 5b 9c 5c c6 3a 6b 5d f6  .>...% [.\:k]
00a0 84 f3 8e fa c0 45 1f 04 90 5d 32 c2 16 c4 7c 77  .E... ]2...w
00b0 4e 75 9a 28 5a 54 52 18 b9 89 64 bf 2c 83 e6 95  Nu. (ZTR... d...
00c0 f8 f7 90 1a b7 c1 f9 8e d2 32 9f 0e 4f cb 06 40  .>...2..O...@
00d0 a8 a6 6f 11 87 35 c8 cd 22 a4 ce a7 ed cf 59 05  .o...5... "....Y.
00e0 e4 b7 ec 29 b9 57 67 5c 45 5e 8e 27 2b f8 96 2e  .>Wg\ E^'+...
00f0 9d 54 ce e7 03 b5 18 01 80                      .T.....
```

4. 4th UDP Frame:

- Source Port: 50004
- Destination Port: 58558

```
Frame 4: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{F1A7D8CC-772B-4D92-A7CC-3463EF9E7AAD}, id 0
Ethernet II, Src: ASUSTekC_e4:dd:98 (54:a0:50:e4:dd:98), Dst: Giga-Byt_96:e6:f2 (b4:2e:99:96:e6:f2)
Internet Protocol Version 4, Src: 213.163.86.87, Dst: 192.168.1.222
User Datagram Protocol, Src Port: 50004, Dst Port: 58558
Data (43 bytes)
```

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

```
> Frame 259: 80 bytes on wire (640 bits), 80 bytes captured (640 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: 192.168.1.1
> User Datagram Protocol, Src Port: 50425, Dst Port: 53
  Source Port: 50425
  Destination Port: 53
  Length: 46
  Checksum: 0x846f [unverified]
  [Checksum Status: Unverified]
  [Stream index: 6]
  [Timestamps]
  UDP payload (38 bytes)
  Domain Name System (query)
    Transaction ID: 0x9644
    > Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
    > Queries
      [Response In: 269]
```

```
0000 54 a0 50 e4 dd 98 b4 2e 99 96 e6 f2 08 00 45 00  T.P.... .E.
0010 00 42 66 e6 00 00 00 11 00 00 c0 a8 01 de c0 a8  .Bf....
0020 01 01 c4 f9 00 35 00 2e 84 6f 96 44 01 00 00 01  .S... d.D....
0030 00 00 00 00 00 00 07 62 65 61 63 6f 6e 73 03 67  .>...b eacons:g
0040 63 70 04 67 76 74 32 03 63 6f 6d 00 00 01 00 01  cp.gvt2. com....
```

III. TCP

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

SRC IP Address: 95.172.70.134

SRC TCP Port: 12975

```
Frame 157: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{F1A7D8CC-772B-4D92-A7CC-3463EF9E7AAD}, id 0
Ethernet II, Src: ASUSTekC_e4:dd:98 (54:a0:50:e4:dd:98), Dst: Giga-Byt_96:e6:f2 (b4:2e:99:96:e6:f2)
Internet Protocol Version 4, Src: 95.172.70.134, Dst: 192.168.1.222
Transmission Control Protocol, Src Port: 12975, Dst Port: 53471, Seq: 1, Ack: 105, Len: 0
VSS Monitoring Ethernet trailer, Source Port: 0
```

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:eb:f2 (04:2e:99:96:e6:f2), Dst: ASUSTek_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)
```