Protocol Deep Dive: TCP and UDP

PROTOCOL INTRODUCTION

Aaron Staines
NETWORK/SYSTEM ENGINEER | CCISO

Course Overview

Overview of TCP and UDP

Operational theory

Deep dive packet analysis

Troubleshooting

Module Overview

Criticality of TCP and UDP

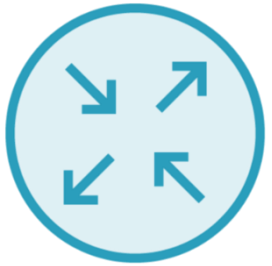
What are ports?

What is TCP?

What is UDP?

Criticality of TCP and UDP

Criticality of TCP and UDP



Criticality of TCP and UDP

TCP and UDP – transportation

TCP

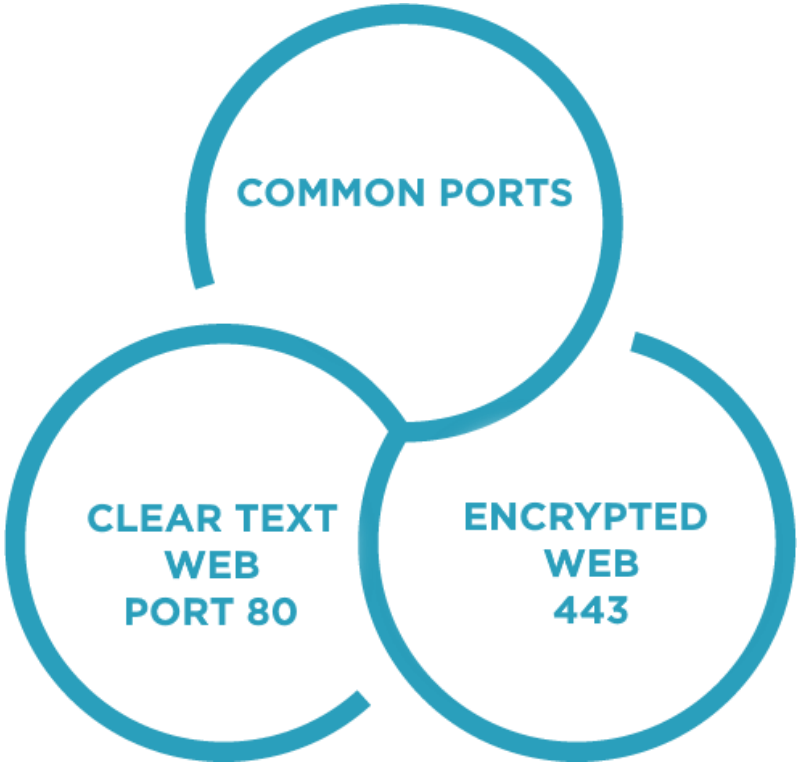
- Reliable transportation
- Critical applications

UDP

- Best effort
- Online Games

What Is a Port?

What Is a Port?



Ports are services (think supermarket)

Port range is over 65,000

Ports can be malicious

Zenmap

Scan Tools Profile Help

Target: 192.168.1.1 Profile: Quick scan Scan Cancel

Command: nmap -T4 -F 192.168.1.1

Hosts Services

OS Host

Nmap Output Ports / Hosts Topology Host Details Scans

Details

Filter Hosts

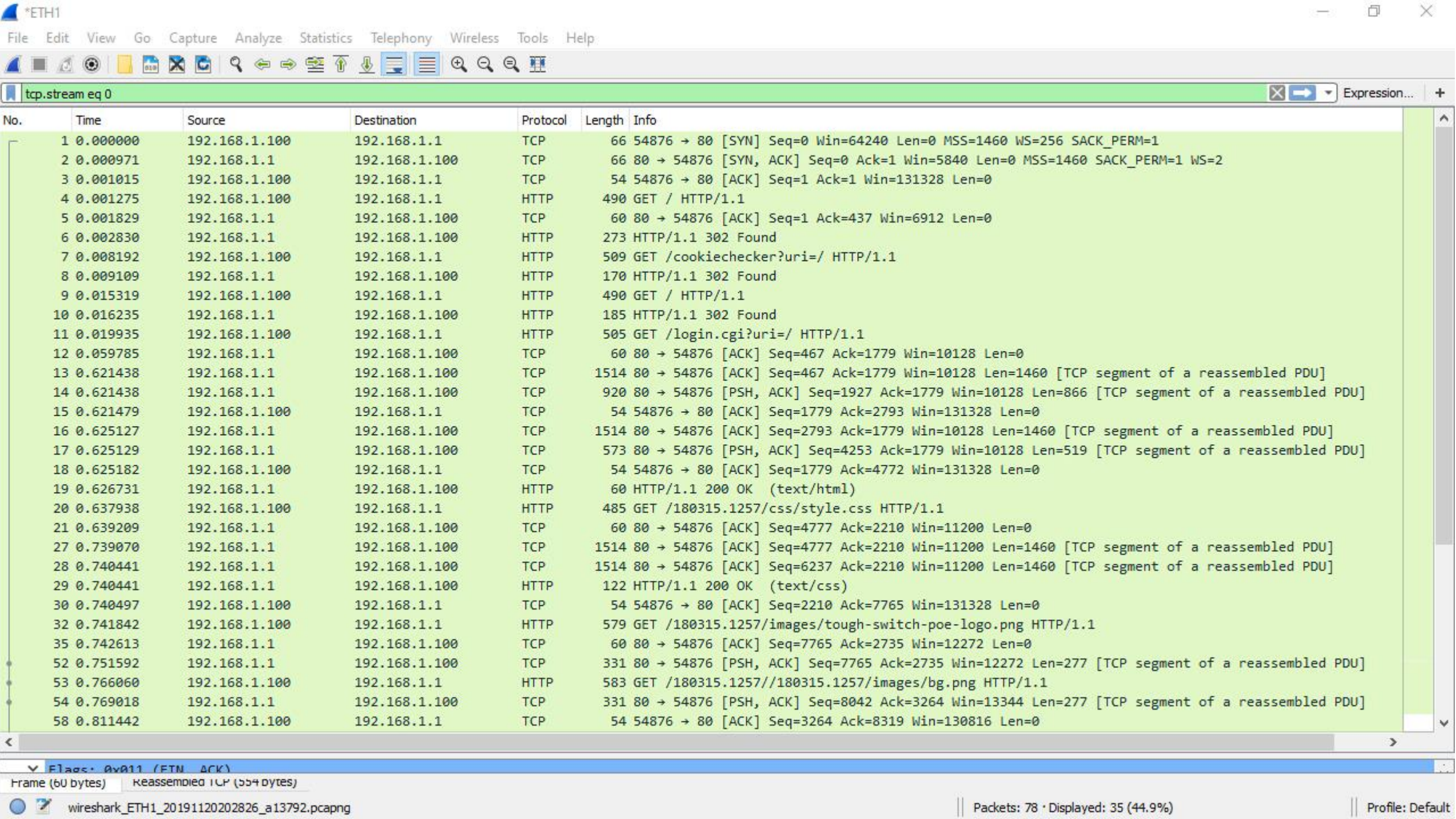
What Is TCP?

What Is TCP?

TCP – think reliable

Reliable methodology

- Established sessions – three-way handshake
- Error recovery – send missing chunks
- Session termination – establish termination


*ETH1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.1.100 192.168.1.1 TCP 66 54876 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2 0.000971 192.168.1.1 192.168.1.100 TCP 66 80 → 54876 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=2
3 0.001015 192.168.1.100 192.168.1.1 TCP 54 54876 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
4 0.001275 192.168.1.100 192.168.1.1 HTTP 490 GET / HTTP/1.1
5 0.001829 192.168.1.1 192.168.1.100 TCP 60 80 → 54876 [ACK] Seq=1 Ack=437 Win=6912 Len=0
6 0.002830 192.168.1.1 192.168.1.100 HTTP 273 HTTP/1.1 302 Found
7 0.008192 192.168.1.100 192.168.1.1 HTTP 509 GET /cookiechecker?uri=/ HTTP/1.1
8 0.009109 192.168.1.1 192.168.1.100 HTTP 170 HTTP/1.1 302 Found
9 0.015319 192.168.1.100 192.168.1.1 HTTP 490 GET / HTTP/1.1
10 0.016235 192.168.1.1 192.168.1.100 HTTP 185 HTTP/1.1 302 Found
11 0.019935 192.168.1.100 192.168.1.1 HTTP 505 GET /login.cgi?uri=/ HTTP/1.1
12 0.059785 192.168.1.1 192.168.1.100 TCP 60 80 → 54876 [ACK] Seq=467 Ack=1779 Win=10128 Len=0
13 0.621438 192.168.1.1 192.168.1.100 TCP 1514 80 → 54876 [ACK] Seq=467 Ack=1779 Win=10128 Len=1460 [TCP segment of a reassembled PDU]
14 0.621438 192.168.1.1 192.168.1.100 TCP 920 80 → 54876 [PSH, ACK] Seq=1927 Ack=1779 Win=10128 Len=866 [TCP segment of a reassembled PDU]
15 0.621479 192.168.1.100 192.168.1.1 TCP 54 54876 → 80 [ACK] Seq=1779 Ack=2793 Win=131328 Len=0
16 0.625127 192.168.1.1 192.168.1.100 TCP 1514 80 → 54876 [ACK] Seq=2793 Ack=1779 Win=10128 Len=1460 [TCP segment of a reassembled PDU]
17 0.625129 192.168.1.1 192.168.1.100 TCP 573 80 → 54876 [PSH, ACK] Seq=4253 Ack=1779 Win=10128 Len=519 [TCP segment of a reassembled PDU]
18 0.625182 192.168.1.100 192.168.1.1 TCP 54 54876 → 80 [ACK] Seq=1779 Ack=4772 Win=131328 Len=0
19 0.626731 192.168.1.1 192.168.1.100 HTTP 60 HTTP/1.1 200 OK (text/html)
20 0.637938 192.168.1.100 192.168.1.1 HTTP 485 GET /180315.1257/css/style.css HTTP/1.1
21 0.639209 192.168.1.1 192.168.1.100 TCP 60 80 → 54876 [ACK] Seq=4777 Ack=2210 Win=11200 Len=0
27 0.739070 192.168.1.1 192.168.1.100 TCP 1514 80 → 54876 [ACK] Seq=4777 Ack=2210 Win=11200 Len=1460 [TCP segment of a reassembled PDU]
28 0.740441 192.168.1.1 192.168.1.100 TCP 1514 80 → 54876 [ACK] Seq=6237 Ack=2210 Win=11200 Len=1460 [TCP segment of a reassembled PDU]
29 0.740441 192.168.1.1 192.168.1.100 HTTP 122 HTTP/1.1 200 OK (text/css)
30 0.740497 192.168.1.100 192.168.1.1 TCP 54 54876 → 80 [ACK] Seq=2210 Ack=7765 Win=131328 Len=0
32 0.741842 192.168.1.100 192.168.1.1 HTTP 579 GET /180315.1257/images/tough-switch-poe-logo.png HTTP/1.1
35 0.742613 192.168.1.1 192.168.1.100 TCP 60 80 → 54876 [ACK] Seq=7765 Ack=2735 Win=12272 Len=0
52 0.751592 192.168.1.1 192.168.1.100 TCP 331 80 → 54876 [PSH, ACK] Seq=7765 Ack=2735 Win=12272 Len=277 [TCP segment of a reassembled PDU]
53 0.766060 192.168.1.100 192.168.1.1 HTTP 583 GET /180315.1257//180315.1257/images/bg.png HTTP/1.1
54 0.769018 192.168.1.1 192.168.1.100 TCP 331 80 → 54876 [PSH, ACK] Seq=8042 Ack=3264 Win=13344 Len=277 [TCP segment of a reassembled PDU]
58 0.811442 192.168.1.100 192.168.1.1 TCP 54 54876 → 80 [ACK] Seq=3264 Ack=8319 Win=130816 Len=0
Flags: 0x011 (FIN, ACK)
Frame (60 bytes)
Reassembled TCP (554 bytes)
wireshark_ETH1_20191120202826_a13792.pcapng
Packets: 78 · Displayed: 35 (44.9%)
Profile: Default

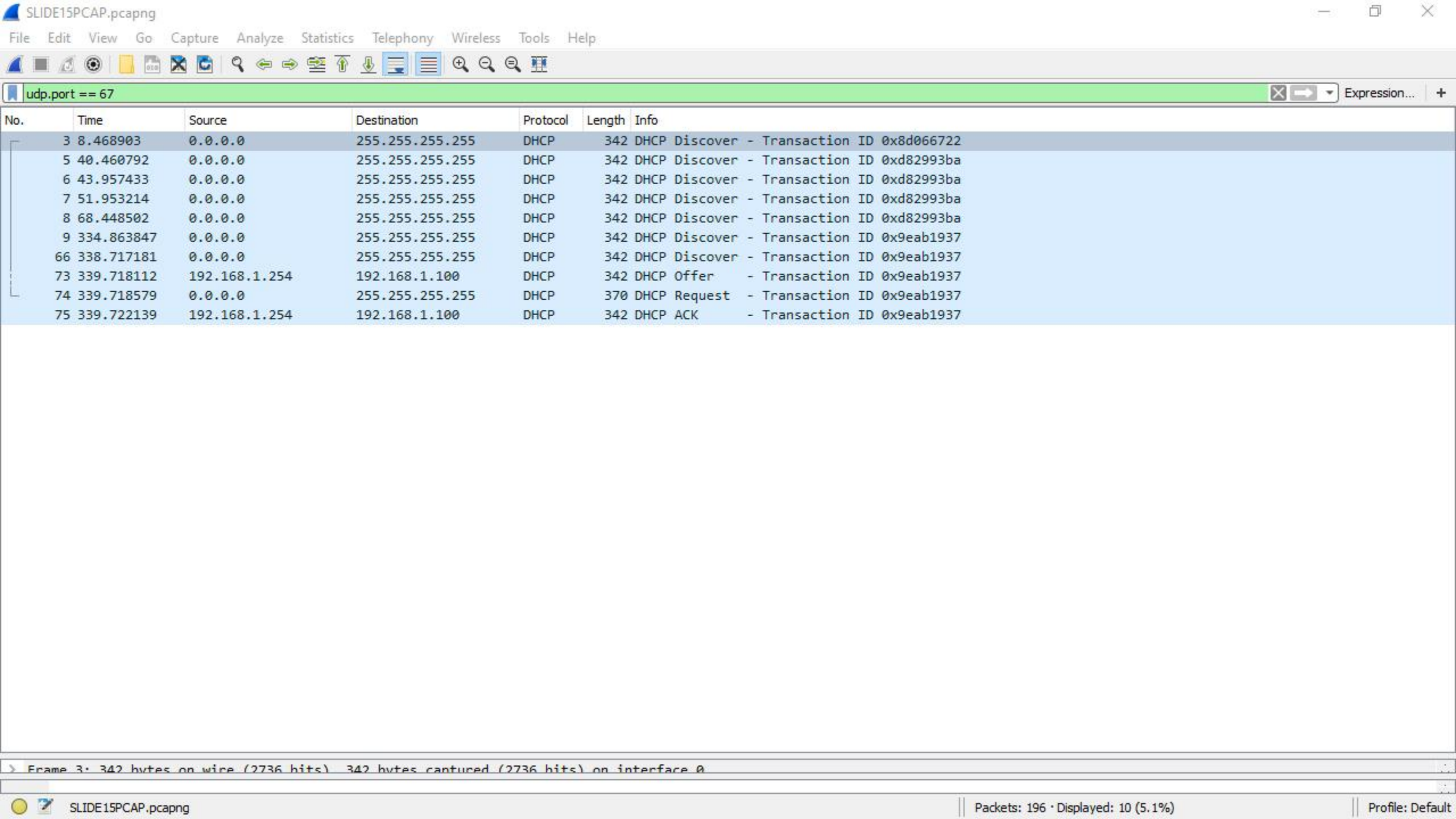
What Is UDP?

What Is UDP?

UDP transport

- Best effort – cell phone call
- Not unreliable – bad vehicle

UDP – lightweight


SLIDE15PCAP.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.port == 67
Expression...
No. Time Source Destination Protocol Length Info
3 8.468903 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x8d066722
5 40.460792 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0xd82993ba
6 43.957433 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0xd82993ba
7 51.953214 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0xd82993ba
8 68.448502 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0xd82993ba
9 334.863847 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x9eab1937
66 338.717181 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x9eab1937
73 339.718112 192.168.1.254 192.168.1.100 DHCP 342 DHCP Offer - Transaction ID 0x9eab1937
74 339.718579 0.0.0.0 255.255.255.255 DHCP 370 DHCP Request - Transaction ID 0x9eab1937
75 339.722139 192.168.1.254 192.168.1.100 DHCP 342 DHCP ACK - Transaction ID 0x9eab1937
Frame 3: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
SLIDE15PCAP.pcapng
Packets: 196 · Displayed: 10 (5.1%)
Profile: Default

Module Review

Critical operations of TCP and UDP

A port is a service

TCP is the reliable protocol

UDP is the best effort protocol