

Output :

The image displays two screenshots of the Wireshark network traffic analysis tool. Both screenshots show a packet capture on interface 'DeviceNPF_{8010020A-6203-40A5-A1D0-019F95869C01}'.

Top Screenshot:

- Packet List:** Shows 292 packets. Packet 287 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.
- Packet Details:**
 - Ethernet II, Src: Dell_E77ae41 (30:80:12:c7:ae:41), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - Internet Protocol Version 4, Src: 192.168.34.70, Dst: 23.45.151.49
 - Transmission Control Protocol, Src Port: 52741, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
- Packet Bytes:** Shows the raw packet data in hexadecimal and ASCII.

Bottom Screenshot:

- Packet List:** Shows 1196 packets. Packet 1071 is selected, showing details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol.
- Packet Details:**
 - Ethernet II, Src: Dell_E77ae41 (30:80:12:c7:ae:41), Dst: TP-Link_3a:39:54 (b4:b0:24:3a:39:54)
 - Internet Protocol Version 4, Src: 192.168.34.70, Dst: 23.45.151.49
 - Transmission Control Protocol, Src Port: 52741, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
- Packet Bytes:** Shows the raw packet data in hexadecimal and ASCII.

Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.34.70

No.	Time	Source	Destination	Protocol	Length	Info
1083	84.255675	192.168.34.70	31.13.79.53	TCP	54	52440 → 443 [ACK] Seq=285 Ack=534 Win=514 Len=0
1084	84.265743	192.168.34.70	31.13.79.53	TLSv1.2	126	Application Data
1085	84.267260	31.13.79.53	192.168.34.70	TCP	60	443 → 52440 [ACK] Seq=534 Ack=357 Win=1412 Len=0
1115	88.493209	192.168.34.70	74.125.200.188	TCP	55	[TCP Keep-Alive] 52004 → 5228 [ACK] Seq=1 Ack=1 Win=512 Len=1
1116	88.553795	74.125.200.188	192.168.34.70	TCP	66	[TCP Keep-Alive ACK] 5228 → 52004 [ACK] Seq=1 Ack=2 Win=265 Len=0 SRE=2
1136	93.563141	31.13.79.53	192.168.34.70	TLSv1.2	124	Application Data
1137	93.605330	192.168.34.70	31.13.79.53	TCP	54	52440 → 443 [ACK] Seq=357 Ack=604 Win=514 Len=0
1138	93.621584	192.168.34.70	31.13.79.53	TLSv1.2	124	Application Data
1139	93.623340	31.13.79.53	192.168.34.70	TCP	60	443 → 52440 [ACK] Seq=604 Ack=427 Win=1412 Len=0
1140	93.828557	31.13.79.53	192.168.34.70	TLSv1.2	126	Application Data
1141	93.872368	192.168.34.70	31.13.79.53	TCP	54	52440 → 443 [ACK] Seq=427 Ack=676 Win=513 Len=0
1152	94.731411	117.18.232.200	192.168.34.70	TCP	60	[TCP Keep-Alive] 443 → 52757 [ACK] Seq=8827 Ack=1213 Win=69120 Len=0
1153	94.731551	192.168.34.70	117.18.232.200	TCP	54	[TCP Keep-Alive ACK] 52757 → 443 [ACK] Seq=1213 Ack=8828 Win=261888 Len=0
1198	99.176301	31.13.79.53	192.168.34.70	TLSv1.2	183	Application Data
1199	99.186237	192.168.34.70	31.13.79.53	TLSv1.2	126	Application Data
1200	99.187787	31.13.79.53	192.168.34.70	TCP	60	443 → 52440 [ACK] Seq=605 Ack=499 Win=1412 Len=0

> Frame 11: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{8010020A-6203-4045-A1D8-019F95889001}, id 0
> Ethernet II, Src: Dell_e7:ae:30 (30:d0:42:e7:ae:30), Dst: TP-Link_3a:39:54 (b4:b0:24:3a:39:54)
> Internet Protocol Version 4, Src: 192.168.34.70, Dst: 23.45.151.49
> Transmission Control Protocol, Src Port: 52741, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

0000 54 b0 24 3a 39 54 30 d0 42 e7 ae 30 08 00 45 00 ...\$!70: B: 0: E:
0010 00 28 b9 4f 40 00 80 06 00 00 c0 a8 22 46 17 2d ...(: 08: ...: Pf:~
0020 97 31 ce 05 01 bb e2 a6 2c a4 e9 b2 d1 f0 50 11 ...:.....P:
0030 03 ff 91 67 00 00 ...g...

Wireshark_EthernetDIEW11.pcapng

Packets: 1214 · Displayed: 460 (37.9%)

Profile: Default

Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.34.70 && ip.addr == 20.49.110.129

No.	Time	Source	Destination	Protocol	Length	Info
960	67.712620	192.168.34.70	20.49.110.129	TLSv1.2	85	Application Data
962	67.914860	20.49.110.129	192.168.34.70	TLSv1.2	85	Application Data
963	67.962778	192.168.34.70	20.49.110.129	TCP	54	51956 → 8883 [ACK] Seq=32 Ack=92 Win=516 Len=0
1644	142.924977	192.168.34.70	20.49.110.129	TLSv1.2	85	Application Data
1646	143.125750	20.49.110.129	192.168.34.70	TLSv1.2	85	Application Data
1647	143.175281	192.168.34.70	20.49.110.129	TCP	54	51956 → 8883 [ACK] Seq=63 Ack=63 Win=515 Len=0

> Frame 1644: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface \Device\NPF_{8010020A-6203-4045-A1D8-019F95889001}, id 0
> Ethernet II, Src: Dell_e7:ae:30 (30:d0:42:e7:ae:30), Dst: TP-Link_3a:39:54 (b4:b0:24:3a:39:54)
> Internet Protocol Version 4, Src: 192.168.34.70, Dst: 20.49.110.129
0100 = Version: 4
.... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 71
Identification: 0xa056 (41046)
> Flags: 0x00, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.34.70
Destination Address: 20.49.110.129
> Transmission Control Protocol, Src Port: 51956, Dst Port: 8883, Seq: 32, Ack: 32, Len: 31
> Transport Layer Security
0000 54 b0 24 3a 39 54 30 d0 42 e7 ae 30 08 00 45 00 ...\$!70: B: 0: E:
0010 00 47 a0 56 40 00 80 06 00 00 c0 a8 22 46 16 31 ...gV0:....Pf:~
0020 2a 31 ca f4 22 b3 c3 3d 46 29 bd 06 cf b1 50 18 ...:....F):k:P:
0030 02 04 05 da 00 00 17 03 03 00 1a 00 00 00 00 ...e.....
0040 00 00 14 ee d3 f1 2b d5 e7 13 91 e0 0b 5b 7d 05 ...:~+.....[:
0050 5e 51 ad f8 85 ...Q...

Destination Address (ip.dst), 4 bytes

Packets: 2189 · Displayed: 6 (0.3%)

Profile: Default

Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

tcp.port == 80 || udp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
1	2.09	192.168.34.70	192.168.34.70	TCP	1494	443 → 52767 [ACK] Seq=1 Ack=1 Win=2052 Len=1440 [TCP segment of a reassembled PDU]
2	2.09	192.168.34.70	192.168.34.70	TCP	1494	443 → 52767 [ACK] Seq=1441 Ack=1 Win=2052 Len=1440 [TCP segment of a reassembled PDU]
3	2.09	192.168.34.70	192.168.34.70	TLSv1.2	932	Server Hello, Certificate, Server Key Exchange, Server Hello Done
4	2.70	20.72.205.209	192.168.34.70	TCP	54	52767 → 443 [ACK] Seq=1 Ack=2081 Win=517 Len=0
5	2.70	20.72.205.209	192.168.34.70	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
6	2.70	20.72.205.209	192.168.34.70	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
7	2.70	20.72.205.209	192.168.34.70	TLSv1.2	123	Application Data
8	2.70	20.72.205.209	192.168.34.70	TCP	54	52767 → 443 [ACK] Seq=159 Ack=3879 Win=513 Len=0
9	2.70	20.72.205.209	192.168.34.70	TLSv1.2	141	Application Data
10	2.70	20.72.205.209	192.168.34.70	TLSv1.2	287	Application Data
11	2.70	20.72.205.209	192.168.34.70	TLSv1.2	92	Application Data
12	2.70	20.72.205.209	192.168.34.70	TLSv1.2	92	Application Data
13	2.70	20.72.205.209	192.168.34.70	TLSv1.2	178	Application Data
14	2.70	20.72.205.209	192.168.34.70	TCP	60	443 → 52767 [ACK] Seq=5917 Ack=517 Win=2050 Len=0
15	2.70	20.72.205.209	192.168.34.70	TCP	54	52767 → 443 [ACK] Seq=517 Ack=4041 Win=512 Len=0
16	2.70	20.72.205.209	192.168.34.70	TCP	54	52767 → 443 [FIN, ACK] Seq=517 Ack=4041 Win=512 Len=0

> Frame 2: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{8010020A-6203-4045-A10B-010F95889001}, id 0

> Ethernet II, Src: TP-Link_3a:39:54 (b4:80:24:3a:39:54), Dst: Dell_e7:ae:30 (30:d0:42:e7:ae:30)

> Internet Protocol Version 4, Src: 20.72.205.209, Dst: 192.168.34.70

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 1480

Identification: 0xa8f3 (43251)

> Flags: 0x00, Don't fragment

.... 0000 0000 0000 = Fragment Offset: 0

Time to Live: 109

Protocol: TCP (6)

Header Checksum: 0x9a34 [validation disabled]

[Header checksum status: Unverified]

Source Address: 20.72.205.209

Destination Address: 192.168.34.70

> Transmission Control Protocol, Src Port: 443, Dst Port: 52767, Seq: 1, Ack: 1, Len: 1440

0010 05 c8 a8 f3 40 00 6d 06 9a 34 14 48 cd d1 c0 a8 ...@m-4-H-...

0020 22 46 01 bb ce 1f 18 06 4e ee f2 c5 d5 69 50 10 ...F.....N...p...

0030 08 04 70 4f 00 00 16 03 03 0e a9 02 00 00 5e 03 ...p.....P...E...

0040 03 64 1d 4f 00 22 11 17 50 af a6 a2 25 14 3d ...Q...P...E...

0050 71 19 5a 93 54 a0 de 05 9e dd 1b c0 83 a2 cf ee ...q'Z'.....HL...

0060 c1 20 85 3d 00 00 37 17 cd 87 17 83 7f 48 4c da ...-7.....HL...

0070 20 1a de c5 f9 50 24 58 46 2b 18 54 56 b5 c4 e5 ...PjK Fa-TV...

0080 08 2f c0 30 00 00 16 00 10 00 05 00 03 02 68 32 .../0.....h2...

0090 00 17 00 00 ff 01 00 01 00 00 00 00 0b 00 0c ...-0.....

00a0 d2 00 8c cf 00 05 ed 30 82 05 e9 30 82 03 d1 a0 ...-0.....

00b0 03 00 02 02 02 13 00 00 01 e2 1f ef 34 6d 38 ...-3.....dnd...

00c0 b5 fb 58 00 00 00 01 e2 30 0d 06 09 2a 86 48 ...X.....0...H...

00d0 86 f7 0d 01 01 06 05 30 7e 31 0b 30 09 06 03 ...-0-1-0-...

00e0 55 04 06 13 02 55 53 13 13 30 11 06 03 55 04 08 ...U...USI...0...U...

00f0 13 0a 57 61 73 68 69 6e 67 74 6f 6e 31 10 30 0e ...-Hashin gton1 0...

0100 06 03 55 04 07 13 07 52 65 64 6d 6f 6e 64 31 1e ...U...R edmond1 0...

0110 30 1c 06 03 55 04 13 15 4d 69 63 72 6f 73 6f ...0...U...Microso...

0120 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 31 28 ...ft Corpo ration1(

0130 30 26 06 03 55 04 03 1f 4d 69 63 72 6f 73 6f ...00...U...Microso...

0140 66 74 20 53 65 63 75 72 65 20 53 65 72 76 65 72 ...ft Secur e Server

Transmission Control Protocol

Packets: 262 / Displayed: 22 (8.4%)

Profile: Default

Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

tcp.port == 80 || udp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
1	2.051659	20.72.205.209	192.168.34.70	TCP	1494	443 → 52767 [ACK] Seq=1 Ack=1 Win=2052 Len=1440 [TCP segment of a reassembled PDU]
2	2.051659	20.72.205.209	192.168.34.70	TCP	1494	443 → 52767 [ACK] Seq=1441 Ack=1 Win=2052 Len=1440 [TCP segment of a reassembled PDU]
3	2.051659	20.72.205.209	192.168.34.70	TLSv1.2	932	Server Hello, Certificate, Server Key Exchange, Server Hello Done
4	2.051659	20.72.205.209	192.168.34.70	TCP	54	52767 → 443 [ACK] Seq=1 Ack=2081 Win=517 Len=0
5	2.051659	20.72.205.209	192.168.34.70	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
6	2.051659	20.72.205.209	192.168.34.70	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
7	2.051659	20.72.205.209	192.168.34.70	TLSv1.2	123	Application Data
8	2.051659	20.72.205.209	192.168.34.70	TCP	54	52767 → 443 [ACK] Seq=159 Ack=3879 Win=513 Len=0
9	2.051659	20.72.205.209	192.168.34.70	TLSv1.2	141	Application Data
10	2.051659	20.72.205.209	192.168.34.70	TLSv1.2	287	Application Data
11	2.051659	20.72.205.209	192.168.34.70	TLSv1.2	92	Application Data
12	2.051659	20.72.205.209	192.168.34.70	TLSv1.2	92	Application Data
13	2.051659	20.72.205.209	192.168.34.70	TLSv1.2	178	Application Data
14	2.051659	20.72.205.209	192.168.34.70	TCP	60	443 → 52767 [ACK] Seq=5917 Ack=517 Win=2050 Len=0
15	2.051659	20.72.205.209	192.168.34.70	TCP	54	52767 → 443 [ACK] Seq=517 Ack=4041 Win=512 Len=0
16	2.051659	20.72.205.209	192.168.34.70	TCP	54	52767 → 443 [FIN, ACK] Seq=517 Ack=4041 Win=512 Len=0

> Frame 2: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface \Device\NPF_{8010020A-6203-4045-A10B-010F95889001}, id 0

> Ethernet II, Src: TP-Link_3a:39:54 (b4:80:24:3a:39:54), Dst: Dell_e7:ae:30 (30:d0:42:e7:ae:30)

> Internet Protocol Version 4, Src: 20.72.205.209, Dst: 192.168.34.70

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 1480

Identification: 0xa8f3 (43251)

> Flags: 0x00, Don't fragment

.... 0000 0000 0000 = Fragment Offset: 0

Time to Live: 109

Protocol: TCP (6)

Header Checksum: 0x9a34 [validation disabled]

[Header checksum status: Unverified]

Source Address: 20.72.205.209

Destination Address: 192.168.34.70

> Transmission Control Protocol, Src Port: 443, Dst Port: 52767, Seq: 1, Ack: 1, Len: 1440

0010 05 c8 a8 f3 40 00 6d 06 9a 34 14 48 cd d1 c0 a8 ...@m-4-H-...

0020 22 46 01 bb ce 1f 18 06 4e ee f2 c5 d5 69 50 10 ...F.....N...p...

0030 08 04 70 4f 00 00 16 03 03 0e a9 02 00 00 5e 03 ...p.....P...E...

0040 03 64 1d 4f 00 22 11 17 50 af a6 a2 25 14 3d ...Q...P...E...

0050 71 19 5a 93 54 a0 de 05 9e dd 1b c0 83 a2 cf ee ...q'Z'.....HL...

0060 c1 20 85 3d 00 00 37 17 cd 87 17 83 7f 48 4c da ...-7.....HL...

0070 20 1a de c5 f9 50 24 58 46 2b 18 54 56 b5 c4 e5 ...PjK Fa-TV...

0080 08 2f c0 30 00 00 16 00 10 00 05 00 03 02 68 32 .../0.....h2...

0090 00 17 00 00 ff 01 00 01 00 00 00 00 0b 00 0c ...-0.....

00a0 d2 00 8c cf 00 05 ed 30 82 05 e9 30 82 03 d1 a0 ...-0.....

00b0 03 00 02 02 13 00 00 01 e2 1f ef 34 6d 38 ...-3.....dnd...

00c0 b5 fb 58 00 00 00 01 e2 30 0d 06 09 2a 86 48 ...X.....0...H...

00d0 86 f7 0d 01 01 06 05 30 7e 31 0b 30 09 06 03 ...-0-1-0-...

00e0 55 04 06 13 02 55 53 13 13 30 11 06 03 55 04 08 ...U...USI...0...U...

00f0 13 0a 57 61 73 68 69 6e 67 74 6f 6e 31 10 30 0e ...-Hashin gton1 0...

0100 06 03 55 04 07 13 07 52 65 64 6d 6f 6e 64 31 1e ...U...R edmond1 0...

0110 30 1c 06 03 55 04 13 15 4d 69 63 72 6f 73 6f ...0...U...Microso...

0120 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 31 28 ...ft Corpo ration1(

0130 30 26 06 03 55 04 03 1f 4d 69 63 72 6f 73 6f ...00...U...Microso...

0140 66 74 20 53 65 63 75 72 65 20 53 65 72 76 65 72 ...ft Secur e Server

Time to Live (ttl): 1 byte

Packets: 313 / Displayed: 22 (7.0%)

Profile: Default

[illegible]