

Module – 4

Wireshark Tool

Introduction

MODULE-4 WIRESHARK TOOL

→ INTRODUCTION:

- Wireshark formerly known as Ethereal is one of the most powerful tools in a network security analysts kit. Wireshark can peer inside the network and examine the details of traffic at a variety of levels using connection level information and to the bits comprising a single packet.

Features of Wireshark: -

- Features of Wireshark:
 - ① Available in both Unix and Windows.
 - ② Ability to capture live packets from various interfaces
 - ③ Filters packet with many criteria.
 - ④ Can save & merge captured packets.
- The flexibility and depth of inspection allows the valuable tool to analyze security events and troubleshoot network security device issues.
- The installation of this is easily available as we can find the source code at www.wireshark.org and we have the links that are compatible with Linux and x32 bit and x64 bit systems.

- Features of Wireshark:
 - ① Available in both Unix and Windows.
 - ② Ability to capture live packets from various interfaces.
 - ③ Filters packet with many criteria.
 - ④ Can save & merge captured packets.
- The flexibility and depth of inspection allows the valuable tool to analyze security events and troubleshoot network security device issues.
- The installation of this is easily available as we can find the source code at www.wireshark.org and we have the links that are compatible with Linux and x32 bit and x64 bit systems.

Commands in Wireshark

1. Http Filter

The screenshot shows the Wireshark interface with the filter bar set to `http`. The packet list displays four HTTP packets. The packet details pane shows the structure of the selected packet (No. 3919), including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
3919	75.457122	192.168.0.104	188.184.21.108	HTTP	518	GET / HTTP/1.1
3930	75.606666	188.184.21.108	192.168.0.104	HTTP	932	HTTP/1.1 200 OK (text/html)
3940	75.642234	192.168.0.104	188.184.21.108	HTTP	425	GET /favicon.ico HTTP/1.1
3953	75.796842	188.184.21.108	192.168.0.104	HTTP	268	HTTP/1.1 200 OK (image/vnd.microsoft.icon)

Frame 3919: 518 bytes on wire (4144 bits), 518 bytes captured (4144 bits) on interface \Device\NPF_{BC48A256-A123-4AC6-831E-749BF536FD46}, id 0
Ethernet II, Src: IntelCor_a7:d4:ab (e4:5e:37:a7:d4:ab), Dst: Tp-LinkT_d5:39:f2 (d8:47:32:d5:39:f2)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 188.184.21.108
Transmission Control Protocol, Src Port: 50861, Dst Port: 80, Seq: 1, Ack: 1, Len: 464
Hypertext Transfer Protocol

2. Ip.addr==192.168.0.____

The screenshot shows the Wireshark interface with the filter bar set to `ip.addr == 192.168.0.104`. The packet list displays 17 packets, including STUN, TCP, and UDP traffic. The packet details pane shows the structure of the selected packet (No. 3919), including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
6406	176.554516	52.113.92.108	192.168.0.104	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 49.207.221.97:11777
6407	176.557712	192.168.0.104	52.109.124.92	TCP	54	50249 → 443 [ACK] Seq=517 Ack=469 Win=512 Len=0
6408	176.627032	192.168.0.104	52.114.54.16	STUN	264	Allocate Request bandwidth: 350 realm: 5sqZ# with nonce[Malformed Packet]
6409	176.666702	52.114.54.16	192.168.0.104	STUN	214	Allocate Success Response lifetime: 60 MAPPED-ADDRESS: 52.114.54.16:3479 XOR-MAPPED-ADDRESS: 49.207.221.97:11776 bandwidth: 350
6410	176.693648	192.168.0.104	52.113.92.108	UDP	141	50030 → 3480 Len=99
6411	176.994661	192.168.0.104	52.113.92.108	UDP	158	50045 → 3481 Len=116
6412	176.994874	192.168.0.104	52.113.92.108	UDP	158	50047 → 3480 Len=116
6413	177.025390	52.113.92.108	192.168.0.104	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 49.207.221.97:11778
6414	177.034634	52.113.92.108	192.168.0.104	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 49.207.221.97:11779
6415	177.102261	192.168.0.104	52.113.92.108	UDP	158	50002 → 3480 Len=116
6416	177.116479	52.113.92.108	192.168.0.104	UDP	113	3480 → 50002 Len=71
6417	177.139365	52.113.92.108	192.168.0.104	UDP	117	3480 → 50030 Len=75

Frame 3919: 518 bytes on wire (4144 bits), 518 bytes captured (4144 bits) on interface \Device\NPF_{BC48A256-A123-4AC6-831E-749BF536FD46}, id 0
Ethernet II, Src: IntelCor_a7:d4:ab (e4:5e:37:a7:d4:ab), Dst: Tp-LinkT_d5:39:f2 (d8:47:32:d5:39:f2)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 188.184.21.108
Transmission Control Protocol, Src Port: 50861, Dst Port: 80, Seq: 1, Ack: 1, Len: 464
Hypertext Transfer Protocol

3. Ip.src == 192.168.0.104

Wireshark capture showing packets with source IP 192.168.0.104. The capture is filtered on 'ip.src == 192.168.0.104'. The packet list shows 15 packets, all of which are UDP. The packet details pane shows the structure of a packet (Frame 3919): Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	ip.src_host	Source	Destination	Protocol	Length	Info
1	ip.src_host	192.168.0.104	52.113.92.108	UDP	158	50030 → 3480 Len=116
2	ip.src_host	192.168.0.104	52.113.92.108	UDP	145	50030 → 3480 Len=103
3	ip.src_host	192.168.0.104	52.113.92.108	UDP	158	50002 → 3480 Len=116
4	ip.src_host	192.168.0.104	52.113.92.108	UDP	158	50045 → 3481 Len=116
5	ip.src_host	192.168.0.104	52.113.92.108	UDP	93	50047 → 3480 Len=51
6	ip.src_host	192.168.0.104	52.113.92.108	UDP	1269	50047 → 3480 Len=1227
7	ip.src_host	192.168.0.104	52.113.92.108	UDP	1269	50047 → 3480 Len=1227
8	ip.src_host	192.168.0.104	52.113.92.108	UDP	145	50030 → 3480 Len=103
9	ip.src_host	192.168.0.104	52.113.92.108	UDP	158	50047 → 3480 Len=116
10	ip.src_host	192.168.0.104	52.113.92.108	UDP	145	50030 → 3480 Len=103
11	ip.src_host	192.168.0.104	52.113.92.108	UDP	145	50030 → 3480 Len=103
12	ip.src_host	192.168.0.104	52.113.92.108	UDP	141	50030 → 3480 Len=99

> Frame 3919: 518 bytes on wire (4144 bits), 518 bytes captured (4144 bits) on interface \Device\NPF_{BC48A256-A123-4AC6-831E-749BF536FD46}, id 0
> Ethernet II, Src: IntelCor_a7:d4:ab (e4:5e:37:a7:d4:ab), Dst: Tp-LinkT_d5:39:f2 (d8:47:32:d5:39:f2)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 188.184.21.108
> Transmission Control Protocol, Src Port: 50861, Dst Port: 80, Seq: 1, Ack: 1, Len: 464
> Hypertext Transfer Protocol

Source Address: IPv4 address | Packets: 7997 - Displayed: 3810 (47.6%) | Profile: Default

4. Ip.dst == 192.168.0.104

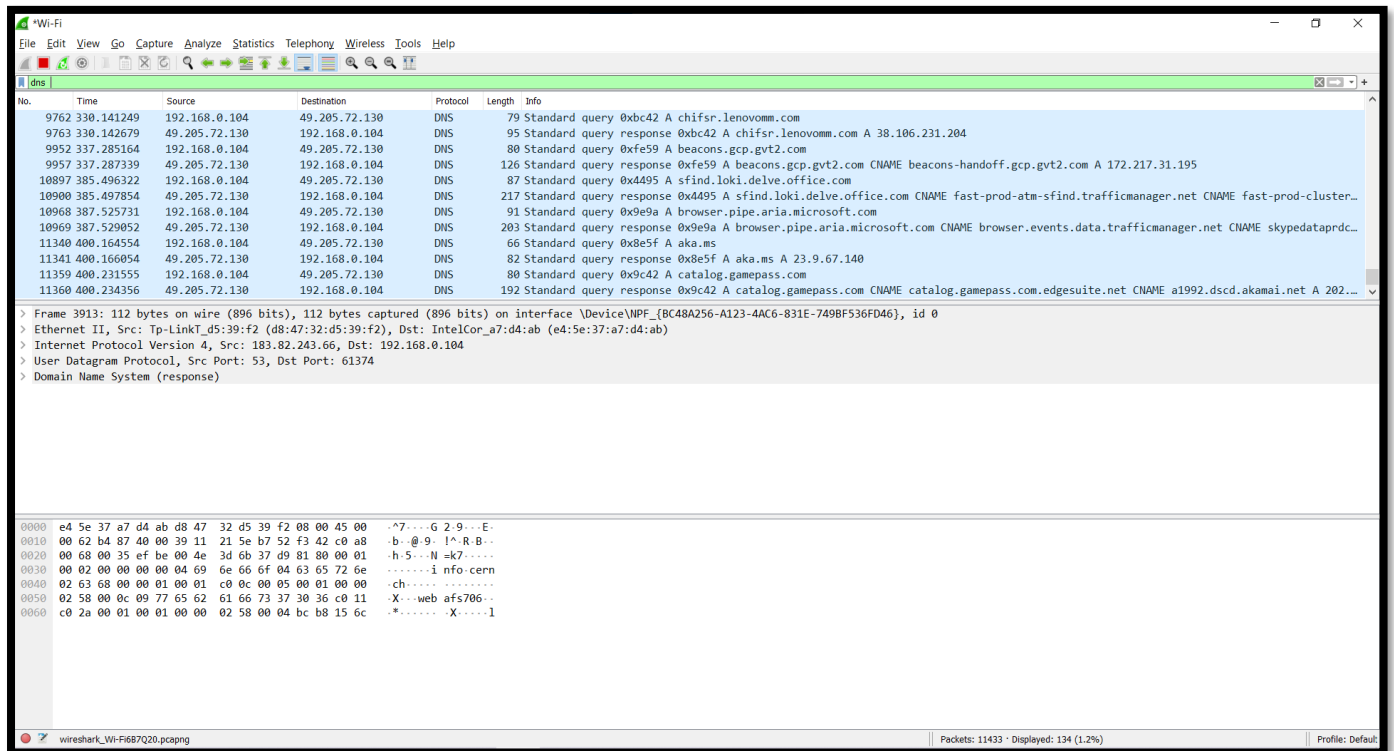
Wireshark capture showing packets with destination IP 192.168.0.104. The capture is filtered on 'ip.dst == 192.168.0.104'. The packet list shows 15 packets, all of which are UDP. The packet details pane shows the structure of a packet (Frame 3916): Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	ip.dst_host	Source	Destination	Protocol	Length	Info
1	ip.dst_host	52.113.92.108	192.168.0.104	UDP	81	3480 → 50002 Len=39
2	ip.dst_host	52.113.92.108	192.168.0.104	UDP	1257	3480 → 50002 Len=1215
3	ip.dst_host	52.113.92.108	192.168.0.104	UDP	1257	3480 → 50002 Len=1215
4	ip.dst_host	52.114.16.141	192.168.0.104	TLSv1.2	283	Application Data
5	ip.dst_host	52.113.92.108	192.168.0.104	UDP	184	3480 → 50002 Len=142
6	ip.dst_host	52.113.92.108	192.168.0.104	UDP	230	3480 → 50002 Len=188
7	ip.dst_host	52.113.92.108	192.168.0.104	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 49.207.221.97:11779
8	ip.dst_host	52.113.92.108	192.168.0.104	UDP	84	3480 → 50002 Len=42
9	ip.dst_host	52.113.92.108	192.168.0.104	UDP	117	3480 → 50030 Len=75
10	ip.dst_host	52.113.92.108	192.168.0.104	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 49.207.221.97:11778
11	ip.dst_host	52.113.92.108	192.168.0.104	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 49.207.221.97:11777
12	ip.dst_host	52.113.92.108	192.168.0.104	STUN	114	Binding Success Response XOR-MAPPED-ADDRESS: 49.207.221.97:11776

> Frame 3916: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{BC48A256-A123-4AC6-831E-749BF536FD46}, id 0
> Ethernet II, Src: Tp-LinkT_d5:39:f2 (d8:47:32:d5:39:f2), Dst: IntelCor_a7:d4:ab (e4:5e:37:a7:d4:ab)
> Internet Protocol Version 4, Src: 202.241.208.54, Dst: 192.168.0.104
> Transmission Control Protocol, Src Port: 443, Dst Port: 50839, Seq: 4531, Ack: 1415, Len: 0

Destination Address: IPv4 address | Packets: 9260 - Displayed: 4783 (51.7%) | Profile: Default

5. Dns or tcp

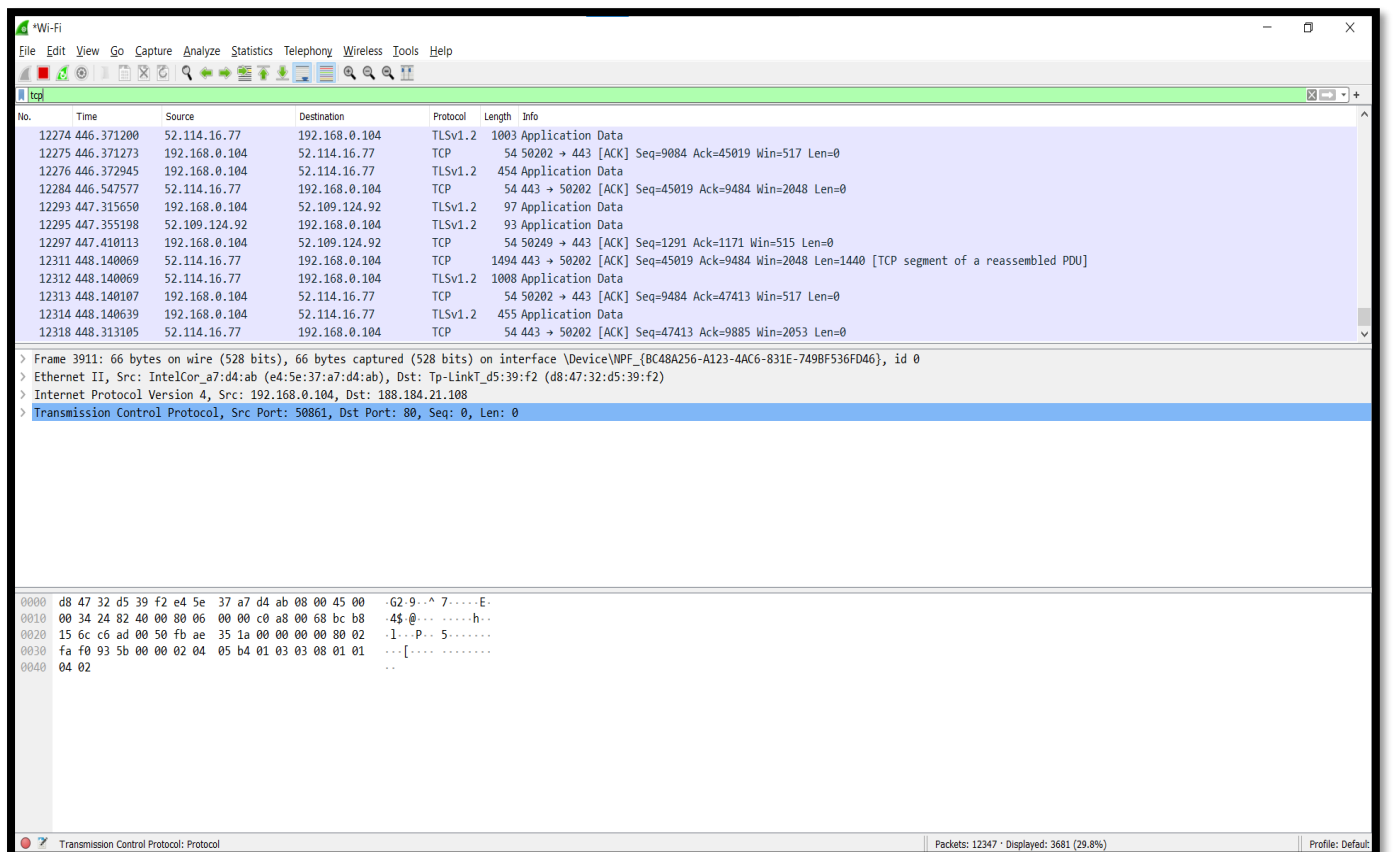


The image shows a Wireshark capture of DNS traffic. The packet list pane displays several DNS queries and responses. The packet details pane shows the structure of a DNS response, including the Ethernet II header, Internet Protocol Version 4 header, and User Datagram Protocol header. The packet bytes pane shows the raw data of the DNS response, including the domain name system response.

No.	Time	Source	Destination	Protocol	Length	Info
9762	3.30.141249	192.168.0.104	49.205.72.130	DNS	79	Standard query 0xbc42 A chifsr.lenovomm.com
9763	3.30.142679	49.205.72.130	192.168.0.104	DNS	95	Standard query response 0xbc42 A chifsr.lenovomm.com A 38.106.231.204
9952	3.37.285164	192.168.0.104	49.205.72.130	DNS	80	Standard query 0xfe59 A beacons.gcp.gvt2.com
9957	3.37.287339	49.205.72.130	192.168.0.104	DNS	126	Standard query response 0xfe59 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 172.217.31.195
10897	3.38.496322	192.168.0.104	49.205.72.130	DNS	87	Standard query 0x4495 A sfind.loki.delve.office.com
10900	3.38.497854	49.205.72.130	192.168.0.104	DNS	217	Standard query response 0x4495 A sfind.loki.delve.office.com CNAME fast-prod-atm-sfind.trafficmanager.net CNAME fast-prod-cluster...
10968	3.38.525731	192.168.0.104	49.205.72.130	DNS	91	Standard query 0x9e9a A browser.pipe.aria.microsoft.com
10969	3.38.529052	49.205.72.130	192.168.0.104	DNS	203	Standard query response 0x9e9a A browser.pipe.aria.microsoft.com CNAME browser.events.data.trafficmanager.net CNAME skypedatprd...
11340	4.00.164554	192.168.0.104	49.205.72.130	DNS	66	Standard query 0x8e5f A aka.ms
11341	4.00.166054	49.205.72.130	192.168.0.104	DNS	82	Standard query response 0x8e5f A aka.ms A 23.9.67.140
11359	4.00.231555	192.168.0.104	49.205.72.130	DNS	80	Standard query 0x9c42 A catalog.gamepass.com
11360	4.00.234356	49.205.72.130	192.168.0.104	DNS	192	Standard query response 0x9c42 A catalog.gamepass.com CNAME catalog.gamepass.com.edgesuite.net CNAME a1992.dscd.akamai.net A 202...

> Frame 3913: 112 bytes on wire (896 bits), 112 bytes captured (896 bits) on interface \Device\NPF_{BC48A256-A123-4AC6-831E-749BF536FD46}, id 0
> Ethernet II, Src: Tp-LinkT_d5:39:f2 (d8:47:32:d5:39:f2), Dst: IntelCor_a7:d4:ab (e4:5e:37:a7:d4:ab)
> Internet Protocol Version 4, Src: 183.82.243.66, Dst: 192.168.0.104
> User Datagram Protocol, Src Port: 53, Dst Port: 61374
> Domain Name System (response)

0000 e4 5e 37 a7 d4 ab d8 47 32 d5 39 f2 08 00 45 00 :^7....G 2.9...E-
0010 00 62 b4 87 40 00 39 11 21 5e b7 52 f3 42 c0 a8 :b...@.9. I^R.B..
0020 00 68 00 35 ef be 00 4e 3d 6b 37 d9 81 80 00 01 :h.5...N=k7.....
0030 00 02 00 00 00 04 69 6e 66 6f 04 63 65 72 6a :.....I nfo.cern
0040 02 63 68 00 00 01 00 01 c0 0c 00 05 00 01 00 00 :ch.....
0050 02 58 00 0c 09 77 65 62 61 66 73 37 30 36 c0 11 :X...web afs706..
0060 c0 2a 00 01 00 01 00 00 02 58 00 04 bc b8 15 6c :*.....X.....l



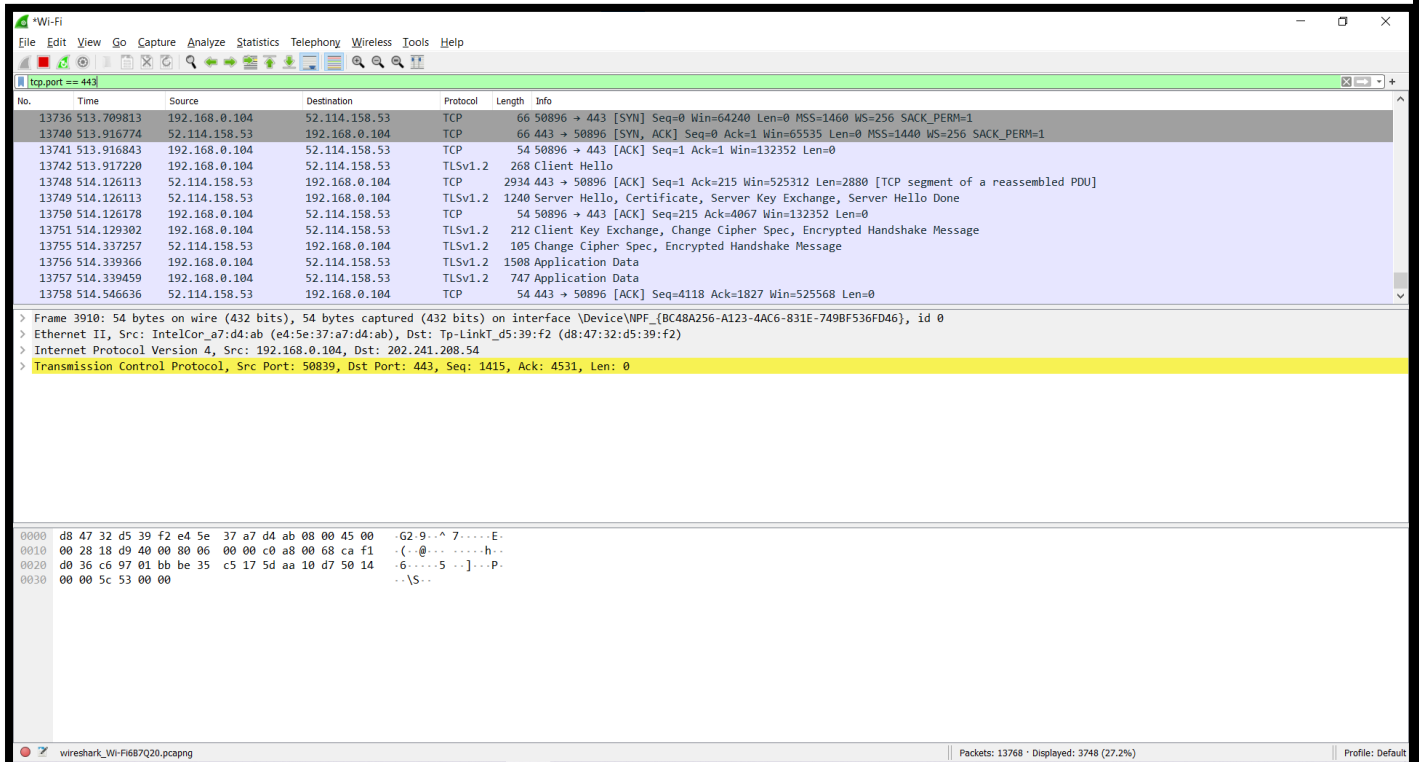
The image shows a Wireshark capture of TCP traffic. The packet list pane displays several TCP segments. The packet details pane shows the structure of a TCP segment, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. The packet bytes pane shows the raw data of the TCP segment, including the domain name system response.

No.	Time	Source	Destination	Protocol	Length	Info
12274	4.46.371200	52.114.16.77	192.168.0.104	TLSv1.2	1003	Application Data
12275	4.46.371273	192.168.0.104	52.114.16.77	TCP	54	50202 → 443 [ACK] Seq=9084 Ack=45019 Win=517 Len=0
12276	4.46.372945	192.168.0.104	52.114.16.77	TLSv1.2	454	Application Data
12284	4.46.547577	52.114.16.77	192.168.0.104	TCP	54	443 → 50202 [ACK] Seq=45019 Ack=9484 Win=2048 Len=0
12293	4.47.315650	192.168.0.104	52.109.124.92	TLSv1.2	97	Application Data
12295	4.47.355198	52.109.124.92	192.168.0.104	TLSv1.2	93	Application Data
12297	4.47.410113	192.168.0.104	52.109.124.92	TCP	54	50249 → 443 [ACK] Seq=1291 Ack=1171 Win=515 Len=0
12311	4.48.140069	52.114.16.77	192.168.0.104	TCP	1494	443 → 50202 [ACK] Seq=45019 Ack=9484 Win=2048 Len=1440 [TCP segment of a reassembled PDU]
12312	4.48.140069	52.114.16.77	192.168.0.104	TLSv1.2	1008	Application Data
12313	4.48.140107	192.168.0.104	52.114.16.77	TCP	54	50202 → 443 [ACK] Seq=9484 Ack=47413 Win=517 Len=0
12314	4.48.140639	192.168.0.104	52.114.16.77	TLSv1.2	455	Application Data
12318	4.48.313105	52.114.16.77	192.168.0.104	TCP	54	443 → 50202 [ACK] Seq=47413 Ack=9885 Win=2053 Len=0

> Frame 3911: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{BC48A256-A123-4AC6-831E-749BF536FD46}, id 0
> Ethernet II, Src: IntelCor_a7:d4:ab (e4:5e:37:a7:d4:ab), Dst: Tp-LinkT_d5:39:f2 (d8:47:32:d5:39:f2)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 188.184.21.108
> Transmission Control Protocol, Src Port: 50861, Dst Port: 80, Seq: 0, Len: 0

0000 d8 47 32 d5 39 f2 e4 5e 37 a7 d4 ab 08 00 45 00 :G2.9...^ 7....E-
0010 00 34 24 82 40 00 80 06 00 00 c0 a8 00 68 bc b8 :4\$.@.....h..
0020 15 c6 c6 ad 00 50 fb ae 35 1a 00 00 00 00 80 02 :.1..P...S.....
0030 fa f0 93 5b 00 00 02 04 05 b4 01 03 03 08 01 01 :...[.....
0040 04 02 :..

6. Tcp.port == 443



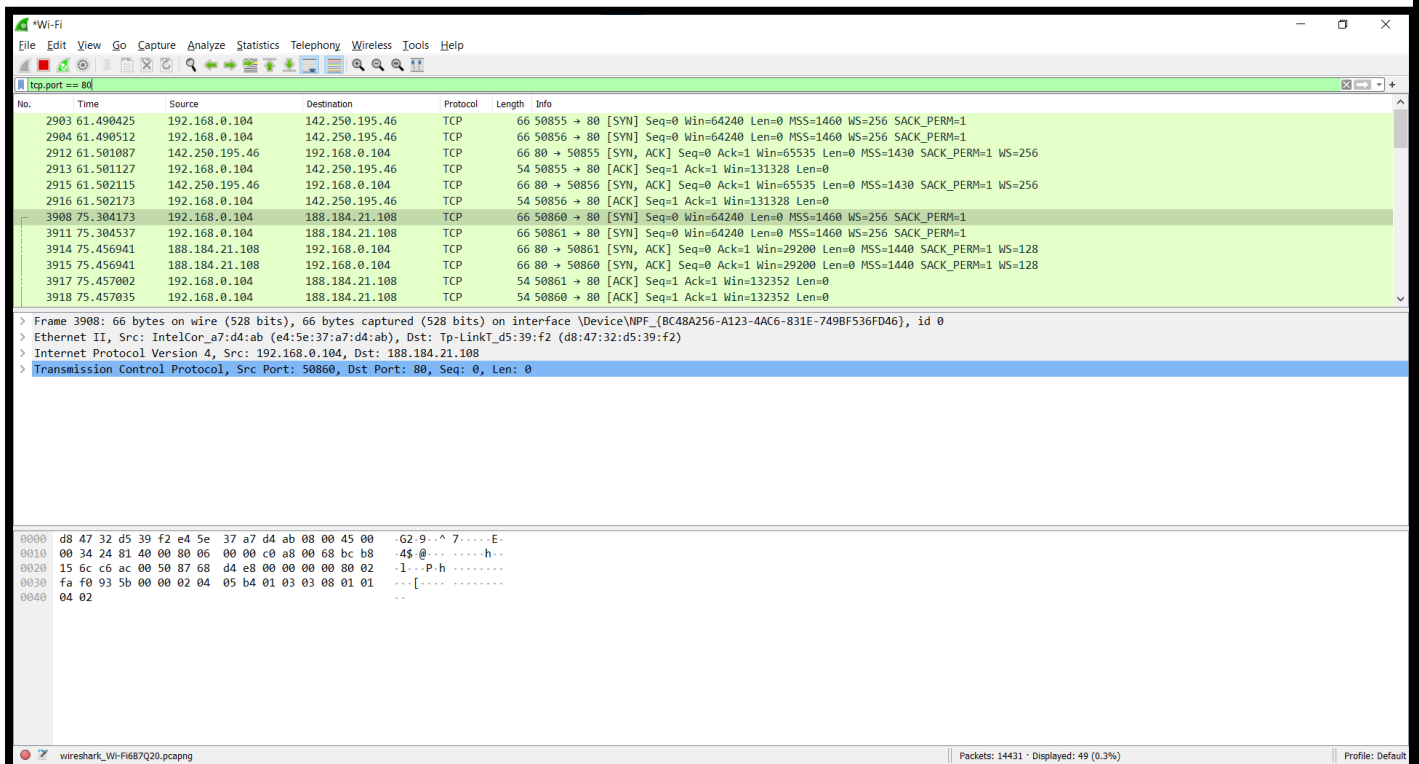
Wireshark capture showing TCP traffic on port 443. The capture is filtered by 'tcp.port == 443'. The packet list shows several packets, including a SYN packet (Seq=0, Win=64240, Len=0, MSS=1460, WS=256, SACK_PERM=1) and an ACK packet (Seq=1, Ack=1, Win=132352, Len=0). The packet details pane shows the selected packet (No. 13758) with the following details:

- Frame 3910: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{BC48A256-A123-4AC6-831E-749BF536FD46}, id 0
- Ethernet II, Src: IntelCor_a7:d4:ab (e4:5e:37:a7:d4:ab), Dst: Tp-LinkT_d5:39:f2 (d8:47:32:d5:39:f2)
- Internet Protocol Version 4, Src: 192.168.0.104, Dst: 202.241.208.54
- Transmission Control Protocol, Src Port: 50839, Dst Port: 443, Seq: 1415, Ack: 4531, Len: 0

The packet bytes pane shows the raw data of the selected packet:

```
0000 d8 47 32 d5 39 f2 e4 5e 37 a7 d4 ab 00 00 45 00 62 9...^ 7....E-
0010 00 28 18 d9 40 00 00 06 00 00 c0 a8 00 68 ca f1 ( @... ..h..
0020 d0 36 c6 97 01 bb be 35 c5 17 5d aa 10 d7 50 14 6...5 ..]...P-
0030 00 00 5c 53 00 00 ..\S..
```

7. Tcp.port == 80



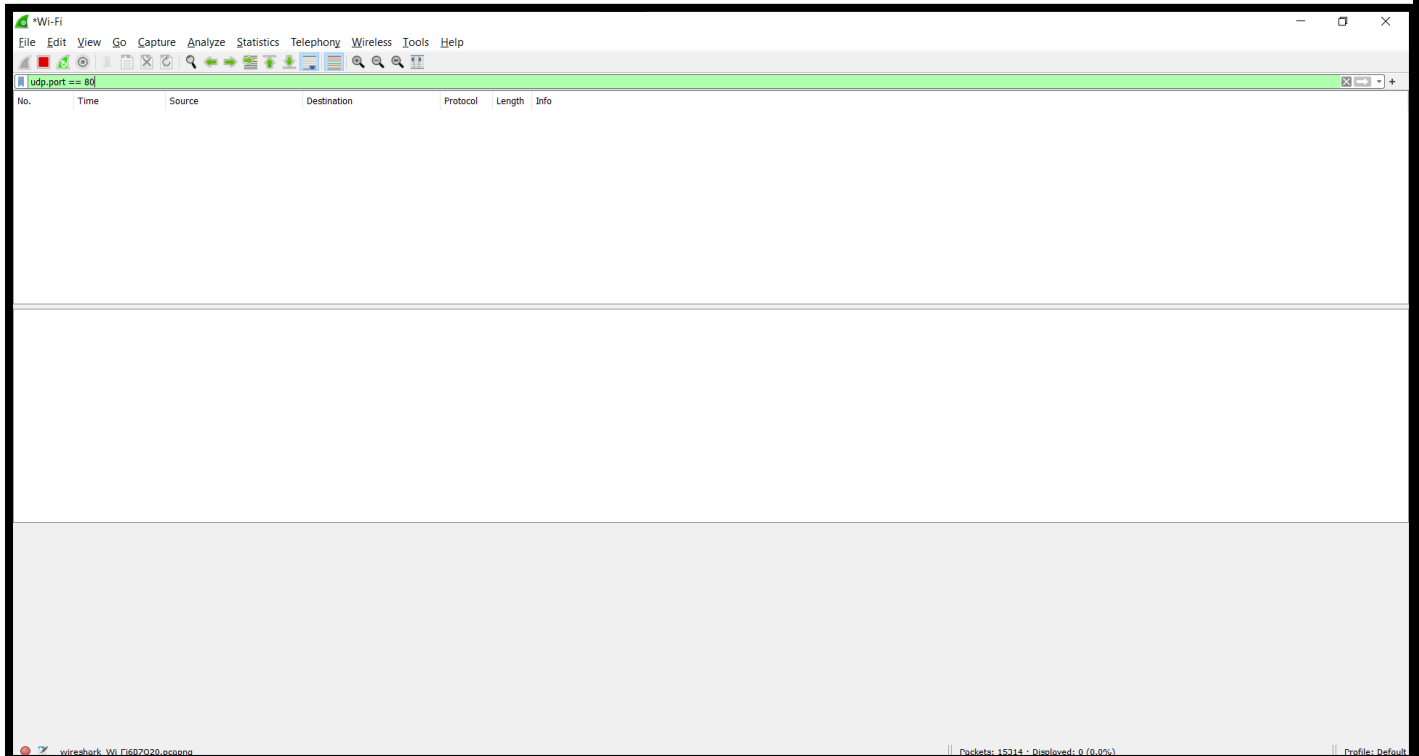
Wireshark capture showing TCP traffic on port 80. The capture is filtered by 'tcp.port == 80'. The packet list shows several packets, including a SYN packet (Seq=0, Win=64240, Len=0, MSS=1460, WS=256, SACK_PERM=1) and an ACK packet (Seq=1, Ack=1, Win=132352, Len=0). The packet details pane shows the selected packet (No. 3908) with the following details:

- Frame 3908: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{BC48A256-A123-4AC6-831E-749BF536FD46}, id 0
- Ethernet II, Src: IntelCor_a7:d4:ab (e4:5e:37:a7:d4:ab), Dst: Tp-LinkT_d5:39:f2 (d8:47:32:d5:39:f2)
- Internet Protocol Version 4, Src: 192.168.0.104, Dst: 188.184.21.108
- Transmission Control Protocol, Src Port: 50860, Dst Port: 80, Seq: 0, Len: 0

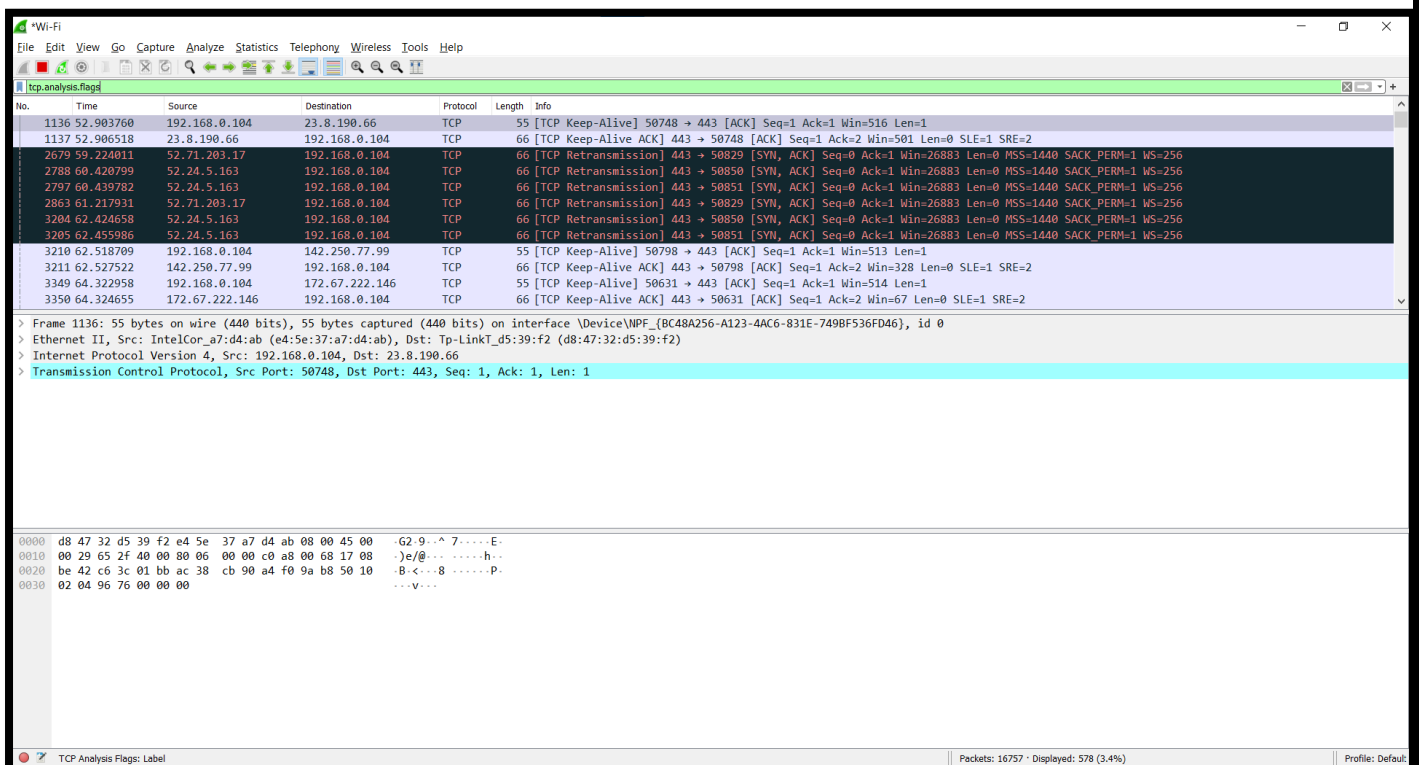
The packet bytes pane shows the raw data of the selected packet:

```
0000 d8 47 32 d5 39 f2 e4 5e 37 a7 d4 ab 08 00 45 00 62 9...^ 7....E-
0010 00 34 24 81 40 00 00 06 00 00 c0 a8 00 68 bc b8 4$ @... ..h..
0020 15 6c c6 ac 00 50 87 68 d4 e8 00 00 00 00 80 02 1...P:h .....
0030 fa f0 93 5b 00 00 02 04 05 b4 01 03 03 08 01 01 ...[.....
0040 04 02 ..
```

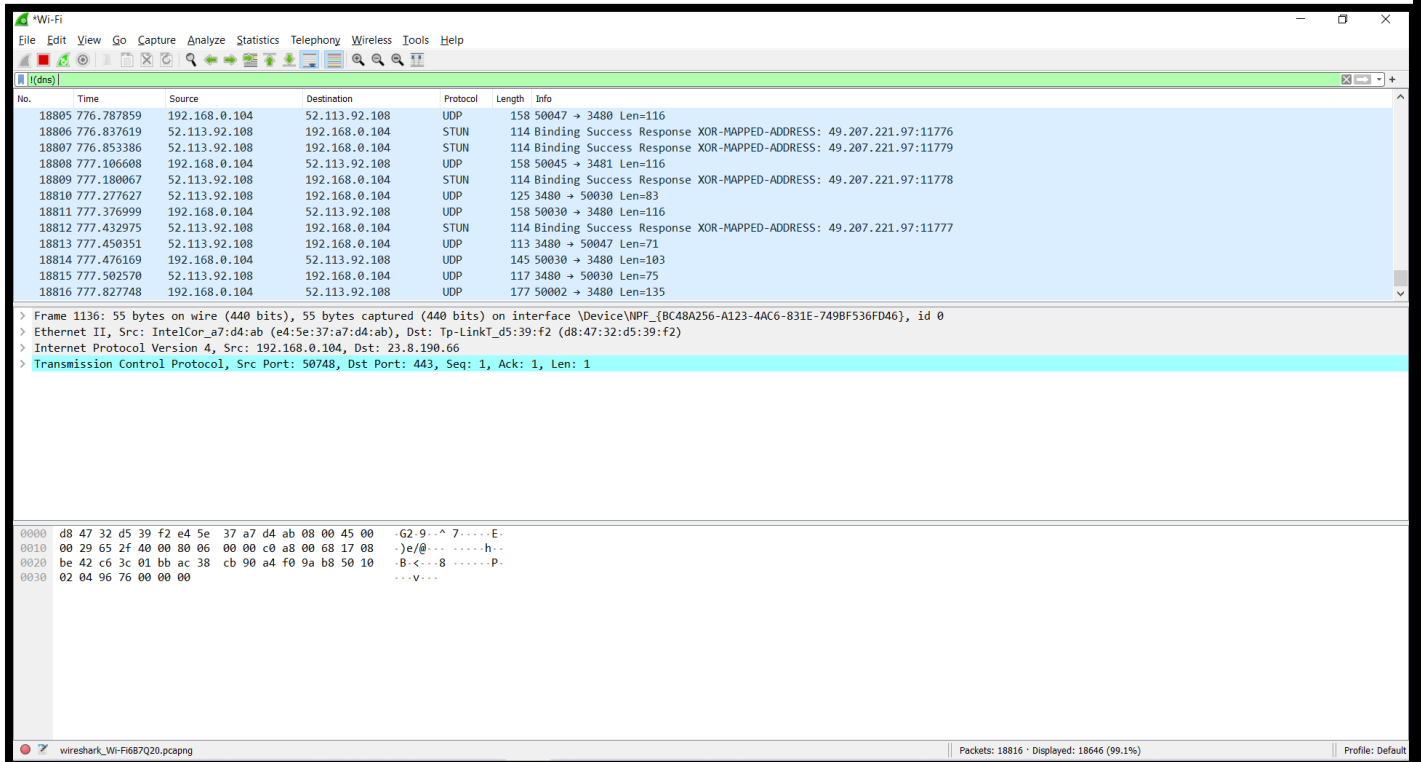

8. Udp.port == 80



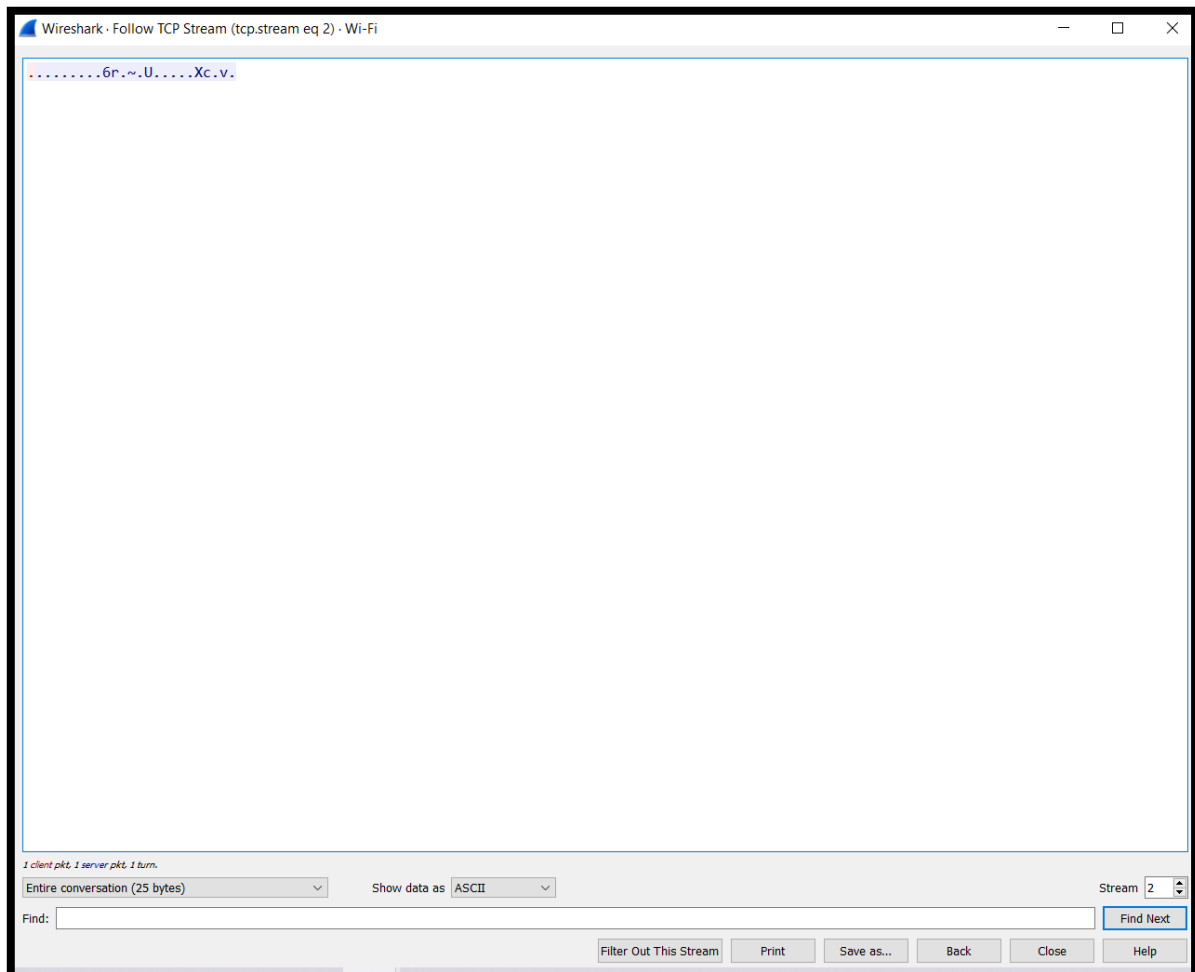
9. Tcp.analysis.flags



10. !(udp)



11. Follow tcp stream



12. Tcp contains google

Wireshark capture showing a TCP connection to googleapis.com. The packet list shows a GET request from 192.168.0.104 to 188.184.21.108 on port 80. The packet details show the HTTP request structure. The packet bytes show the raw data including the 'g.google apis.com' string.

No.	Time	Source	Destination	Protocol	Length	Info
450	23.397678	192.168.0.104	142.250.196.170	TLSv1.3	571	Client Hello
1227	56.550863	192.168.0.104	142.250.76.34	TLSv1.3	571	Client Hello
1834	58.100979	192.168.0.104	216.58.197.34	TLSv1.3	649	Client Hello
1882	58.149892	192.168.0.104	216.58.197.34	TLSv1.3	649	Client Hello
1890	58.160917	192.168.0.104	142.250.182.36	TLSv1.3	571	Client Hello
2457	58.849392	192.168.0.104	142.250.77.98	TLSv1.3	648	Client Hello
3132	61.882208	192.168.0.104	142.250.71.2	TLSv1.3	640	Client Hello
3919	75.457122	192.168.0.104	188.184.21.108	HTTP	518	GET / HTTP/1.1
8501	277.302449	192.168.0.104	172.217.166.110	TLSv1.3	571	Client Hello

> Frame 450: 571 bytes on wire (4568 bits), 571 bytes captured (4568 bits) on interface \Device\NPF_{BC48A256-A123-4AC6-831E-749BF536FD46}, id 0
> Ethernet II, Src: IntelCor_a7:d4:ab (e4:5e:37:a7:d4:ab), Dst: Tp-LinkT_d5:39:f2 (d8:47:32:d5:39:f2)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 142.250.196.170
> Transmission Control Protocol, Src Port: 50807, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
> Transport Layer Security

0000 d8 47 32 d5 39 f2 e4 5e 37 a7 d4 ab 00 00 45 00 -G2-9...^7....E-
0010 02 2d ab 31 40 00 00 06 00 00 c0 a8 00 68 8e fa -lg... ..h-
0020 c4 aa c6 77 01 bb c0 5f 7b 8c ff 83 47 a2 50 18 -..W... {...G.P-
0030 02 01 16 d5 00 00 16 03 01 02 00 01 00 01 fc 03 -.....-
0040 03 36 e3 98 c4 46 a2 e1 c4 97 8b 31 5f 7f cc fd -6...F... ..1...
0050 47 6b 6c 6a 9c 24 f8 2e 61 df 21 59 ac 0a e3 19 -Gklj\$. .a.IY...
0060 41 20 99 2a c4 5c 8f 07 01 3e 32 73 1f a9 49 4c -A .*:\... ->2s..IL
0070 73 2a f7 1f 5b e7 9f b7 24 0a 08 c2 44 f0 56 89 -s*-[... \$...D.V-
0080 d1 39 00 20 ba ba 13 01 13 02 13 03 c0 2b c0 2f -9-+/-
0090 c0 2c c0 30 cc a9 cc a8 c0 13 c0 14 00 9c 00 9d -.,0-
00a0 00 2f 00 35 01 00 01 93 8a 8a 00 00 00 00 20 -./:5-
00b0 00 1e 00 00 1b 73 61 66 65 62 72 6f 77 73 69 6e -.....saf ebrowsin
00c0 67 2e 67 6f 6f 6f 6c 65 61 70 69 73 2e 63 6f 6d -.....g.google apis.com
00d0 00 17 00 00 ff 01 00 01 00 00 0a 00 0a 00 08 4a -.....-J

13. Tcp.response.code==200

Wireshark capture showing HTTP responses with status code 200. The packet list shows three HTTP responses from 188.184.21.108 to 192.168.0.104. The packet details show the HTTP response structure. The packet bytes show the raw data including the 'text/html' and 'image/vnd.microsoft.icon' strings.

No.	Time	Source	Destination	Protocol	Length	Info
3930	75.606666	188.184.21.108	192.168.0.104	HTTP	932	HTTP/1.1 200 OK (text/html)
3953	75.796842	188.184.21.108	192.168.0.104	HTTP	268	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
13265	488.460625	192.168.0.1	192.168.0.104	HTTP	294	HTTP/1.1 200 OK

> Frame 3930: 932 bytes on wire (7456 bits), 932 bytes captured (7456 bits) on interface \Device\NPF_{BC48A256-A123-4AC6-831E-749BF536FD46}, id 0
> Ethernet II, Src: Tp-LinkT_d5:39:f2 (d8:47:32:d5:39:f2), Dst: IntelCor_a7:d4:ab (e4:5e:37:a7:d4:ab)
> Internet Protocol Version 4, Src: 188.184.21.108, Dst: 192.168.0.104
> Transmission Control Protocol, Src Port: 80, Dst Port: 50861, Seq: 1, Ack: 465, Len: 878
> Hypertext Transfer Protocol
> Line-based text data: text/html (13 lines)

0000 e4 5e 37 a7 d4 ab d8 47 32 d5 39 f2 08 00 45 28 -^7....G 2.9...E{
0010 03 96 cb b9 40 00 2c 06 ec 4b bc b8 15 6c c0 a8 -...@, .K...l...
0020 00 68 00 50 c6 ad ed bb b6 f0 fb ae 36 eb 50 18 -h.P... ..6.P-
0030 00 ed 07 e2 00 00 48 54 54 50 2f 31 2e 31 20 32 -.....HT TP/1.1.2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e -00 OK..D ate: Mon
0050 2c 20 30 33 20 4d 61 79 20 32 30 32 31 20 30 34 - , 03 May 2021 04
0060 3a 35 30 3a 34 38 20 47 4d 54 0d 0a 53 65 72 76 -:50:48 G MT..Serv
0070 65 72 3a 20 41 70 61 63 68 65 0d 0a 4c 61 73 74 -er: Apac he..Last
0080 2d 4d 6f 64 69 66 69 65 64 3a 20 57 65 64 2c 20 --Modifie d: Wed,
0090 30 35 20 46 65 62 20 32 30 31 34 20 31 36 3a 30 -05 Feb 2 014 16:0
00a0 30 3a 33 31 20 47 4d 54 0d 0a 45 54 61 67 3a 20 -0:31 GMT ..ETag:
00b0 22 32 38 36 2d 34 66 31 61 61 64 62 33 31 30 35 -"286-4f1 aadb3105
00c0 63 30 22 0d 0a 41 63 63 65 70 74 2d 52 61 6e 67 -c0"...Acc ept-Rang
00d0 65 73 3a 20 62 79 74 65 73 0d 0a 43 6f 6e 74 65 -es: byte s...Conte

14. Tcp.flags.syn==1

The image shows a Wireshark packet capture window titled "Wi-Fi". The filter bar at the top is set to "tcp.flags.syn==1". The packet list pane shows several TCP packets, with the selected packet (No. 3915) highlighted in blue. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
3172	61.952967	52.114.36.47	192.168.0.104	TCP	66	443 → 50857 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
3204	62.424658	52.24.5.163	192.168.0.104	TCP	66	[TCP Retransmission] 443 → 50858 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1440 SACK_PERM=1 WS=256
3205	62.455986	52.24.5.163	192.168.0.104	TCP	66	[TCP Retransmission] 443 → 50851 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1440 SACK_PERM=1 WS=256
3233	63.030475	192.168.0.104	142.250.196.78	TCP	66	50859 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3234	63.039186	142.250.196.78	192.168.0.104	TCP	66	443 → 50859 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1430 SACK_PERM=1 WS=256
3392	65.467395	52.71.203.17	192.168.0.104	TCP	66	[TCP Retransmission] 443 → 50829 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1440 SACK_PERM=1 WS=256
3437	66.572136	52.24.5.163	192.168.0.104	TCP	66	[TCP Retransmission] 443 → 50858 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1440 SACK_PERM=1 WS=256
3438	66.572136	52.24.5.163	192.168.0.104	TCP	66	[TCP Retransmission] 443 → 50851 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1440 SACK_PERM=1 WS=256
3908	75.304173	192.168.0.104	188.184.21.108	TCP	66	50860 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3911	75.304537	192.168.0.104	188.184.21.108	TCP	66	50861 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3914	75.456941	188.184.21.108	192.168.0.104	TCP	66	80 → 50861 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=128
3915	75.456941	188.184.21.108	192.168.0.104	TCP	66	80 → 50860 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=128

> Frame 3915: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{BC48A256-A123-4AC6-831E-749BF536FD46}, id 0
> Ethernet II, Src: Tp-LinkT_d5:39:f2 (d8:47:32:d5:39:f2), Dst: IntelCor_a7:d4:ab (e4:5e:37:a7:d4:ab)
> Internet Protocol Version 4, Src: 188.184.21.108, Dst: 192.168.0.104
> Transmission Control Protocol, Src Port: 80, Dst Port: 50860, Seq: 0, Ack: 1, Len: 0

0000 e4 5e 37 a7 d4 ab d8 47 32 d5 39 f2 08 00 45 28 ^7...G 2 9...E(
0010 00 34 00 00 40 00 2c 06 bb 67 bc b8 15 6c c0 a8 4 @, , 'g' 1..
0020 00 68 00 50 c6 ac a3 83 05 60 87 68 d4 e9 80 12 h P 'h'....
0030 72 10 9d 9d 00 00 02 04 05 a0 01 01 04 02 01 03 n
0040 03 07 ..