

## Network Traffic Analysis with Wireshark

1. With the use of Wireshark I can analyze the different packets going through my private network. I filter by http and tcp, by specific IP address (10.0.2.4) and by specific port (80)

Wireshark packet capture window showing a list of packets filtered by 'http'. The selected packet is number 22, an OCSP response from 10.0.2.4 to 23.219.155.48. The packet details pane shows the structure: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, Hypertext Transfer Protocol, and Online Certificate Status Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length
22	0.294487805	10.0.2.4	23.219.155.48	OCSP	485
23	0.304296142	23.219.155.48	10.0.2.4	OCSP	944
73	0.621689850	10.0.2.4	23.219.155.48	OCSP	485
77	0.632530571	23.219.155.48	10.0.2.4	OCSP	944
80	0.637203463	10.0.2.4	23.219.155.48	OCSP	485
81	0.645650820	23.219.155.48	10.0.2.4	OCSP	944
150	1.090341534	10.0.2.4	34.107.221.82	HTTP	364
151	1.097580222	34.107.221.82	10.0.2.4	HTTP	269
173	1.752641481	10.0.2.4	23.219.155.48	OCSP	485
182	1.767792542	23.219.155.48	10.0.2.4	OCSP	944
200	2.024195317	10.0.2.4	142.250.189.131	OCSP	485

Frame 22: 485 bytes on wire (3880 bits)  
Ethernet II, Src: PCSSystemtec\_51:45:e5, Dst: 10.0.2.15  
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 23.219.155.48  
Transmission Control Protocol, Src Port: 54432, Dst Port: 80  
Hypertext Transfer Protocol  
Online Certificate Status Protocol

Wireshark packet capture window showing a list of packets filtered by 'tcp'. The selected packet is number 22, a TCP reset from 10.0.2.4 to 23.219.155.48. The packet details pane shows the structure: 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.	Time	Source	Destination	Protocol	Length
7	0.032502574	10.0.2.4	35.190.72.216	TCP	74
8	0.039782213	35.190.72.216	10.0.2.4	TCP	60
9	0.039812478	10.0.2.4	35.190.72.216	TCP	54
10	0.042790780	10.0.2.4	35.190.72.216	TLSv1.3	73
11	0.054894526	35.190.72.216	10.0.2.4	TLSv1.3	297
12	0.054918638	10.0.2.4	35.190.72.216	TCP	54
13	0.055037297	35.190.72.216	10.0.2.4	TLSv1.3	205
14	0.055043821	10.0.2.4	35.190.72.216	TCP	54
19	0.286717117	10.0.2.4	23.219.155.48	TCP	74
20	0.294263773	23.219.155.48	10.0.2.4	TCP	60
21	0.294292538	10.0.2.4	23.219.155.48	TCP	54

Frame 22: 485 bytes on wire (3880 bits)  
Ethernet II, Src: PCSSystemtec\_51:45:e5, Dst: 10.0.2.15  
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 23.219.155.48  
Transmission Control Protocol, Src Port: 54432, Dst Port: 80  
Hypertext Transfer Protocol  
Online Certificate Status Protocol

Wireshark interface showing a packet capture on interface \*eth0. The filter is set to `ip.addr == 10.0.2.4`. The packet list shows 13 packets, with packet 3 selected. The packet details pane shows the structure of the selected packet (Frame 3: 89 bytes on wire (712 bits)).

No.	Time	Source	Destination	Protocol	Length
3	0.000163192	10.0.2.4	8.8.8.8	DNS	89
4	0.000168314	10.0.2.4	8.8.8.8	DNS	89
5	0.031083336	8.8.8.8	10.0.2.4	DNS	167
6	0.031499593	8.8.8.8	10.0.2.4	DNS	241
7	0.032502574	10.0.2.4	35.190.72.216	TCP	74
8	0.039782213	35.190.72.216	10.0.2.4	TCP	60
9	0.039812478	10.0.2.4	35.190.72.216	TCP	54
10	0.042790780	10.0.2.4	35.190.72.216	TLSv1.3	732
11	0.054894526	35.190.72.216	10.0.2.4	TLSv1.3	2974
12	0.054918638	10.0.2.4	35.190.72.216	TCP	54
13	0.055037297	35.190.72.216	10.0.2.4	TLSv1.3	209

Frame 3: 89 bytes on wire (712 bits), 88 bytes captured (704 bits) on interface \*eth0  
Ethernet II, Src: PCSSystemtec\_51:45:e5, Dst: 08:00:00:08:00:00  
Internet Protocol Version 4, Src: 10.0.2.4, Dst: 8.8.8.8  
User Datagram Protocol, Src Port: 49453, Dst Port: 53  
Domain Name System (query)

wires...capng | Packets: 21608 · Displayed: 21606 (100.0%) · Dropped: 0 (0.0%) · Profile: Default

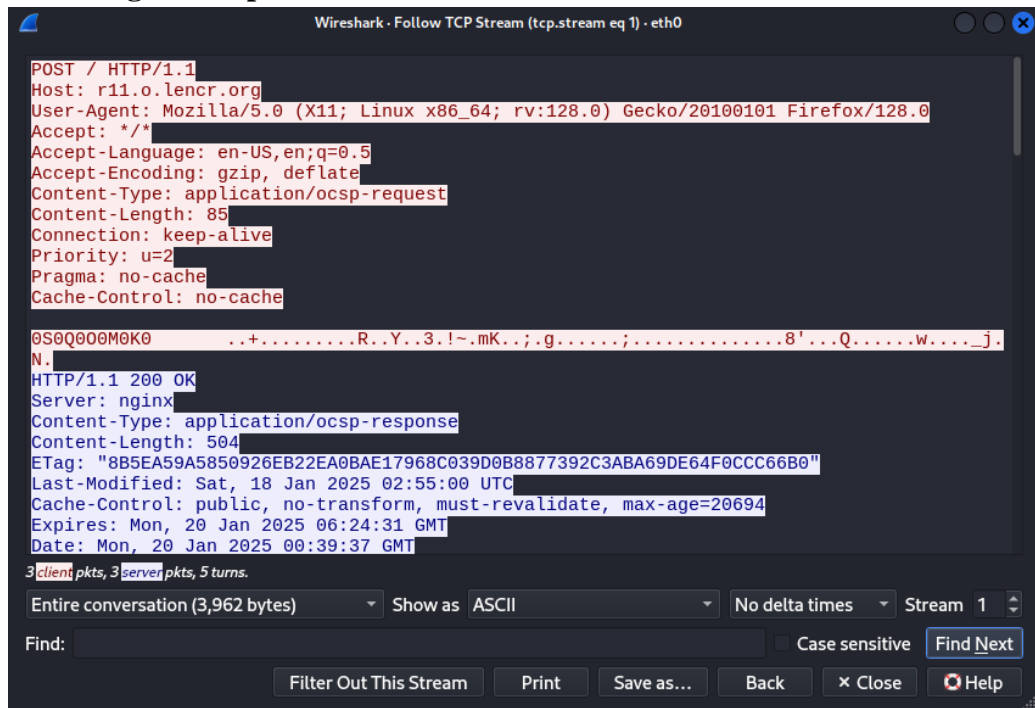
Wireshark interface showing a packet capture on interface \*eth0. The filter is set to `tcp.port == 80`. The packet list shows 11 packets, with packet 77 selected. The packet details pane shows the structure of the selected packet (Frame 77: 943 bytes on wire (7544 bits)).

No.	Time	Source	Destination	Protocol	Length
19	0.286717117	10.0.2.4	23.219.155.48	TCP	74
20	0.294263773	23.219.155.48	10.0.2.4	TCP	60
21	0.294292538	10.0.2.4	23.219.155.48	TCP	54
22	0.294487805	10.0.2.4	23.219.155.48	OCSP	483
23	0.304296142	23.219.155.48	10.0.2.4	OCSP	944
24	0.304324246	10.0.2.4	23.219.155.48	TCP	54
73	0.621689850	10.0.2.4	23.219.155.48	OCSP	483
74	0.622132811	10.0.2.4	23.219.155.48	TCP	74
75	0.629336347	23.219.155.48	10.0.2.4	TCP	60
76	0.629360679	10.0.2.4	23.219.155.48	TCP	54
77	0.632530571	23.219.155.48	10.0.2.4	OCSP	944

Frame 77: 943 bytes on wire (7544 bits), 943 bytes captured (7544 bits) on interface \*eth0  
Ethernet II, Src: 52:54:00:12:35:00 (52:54:00:12:35:00), Dst: 08:00:00:08:00:00  
Internet Protocol Version 4, Src: 23.219.155.48, Dst: 10.0.2.4  
Transmission Control Protocol, Src Port: 80, Dst Port: 49453  
Hypertext Transfer Protocol  
Online Certificate Status Protocol

wireshar...2.pcapng | Packets: 21608 · Displayed: 749 (3.5%) · Dropped: 0 (0.0%) · Profile: Default

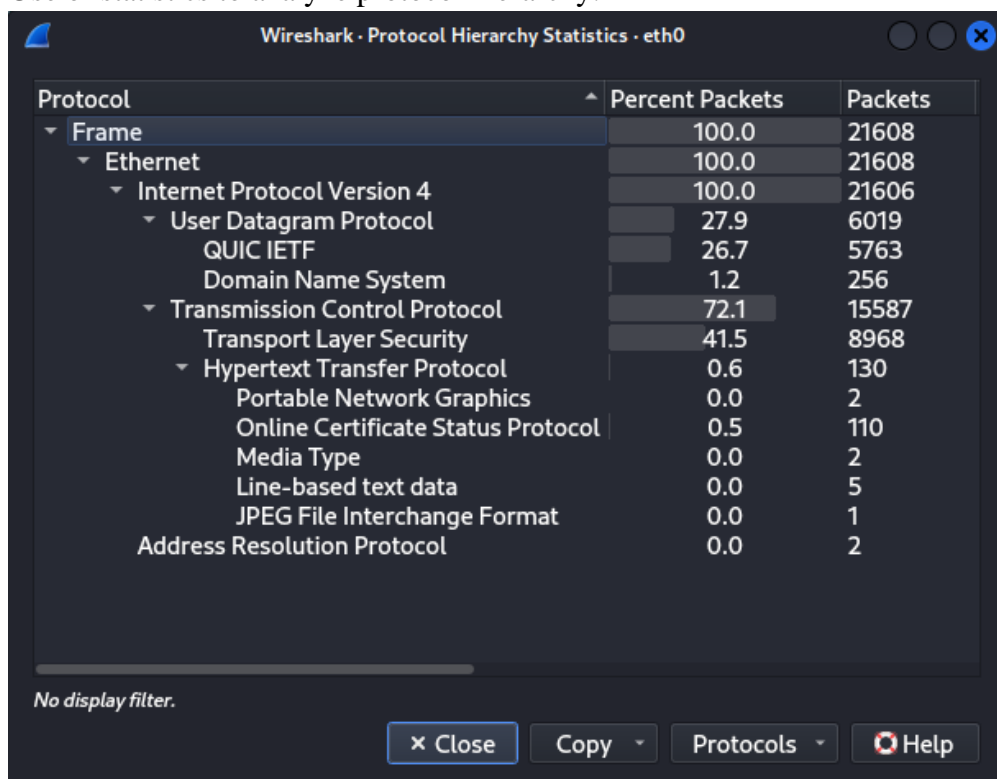
## 2. Following a TCP packet



You can observe the interaction of the packet between client and server, it gives important information about the packet, however the message is encrypted.

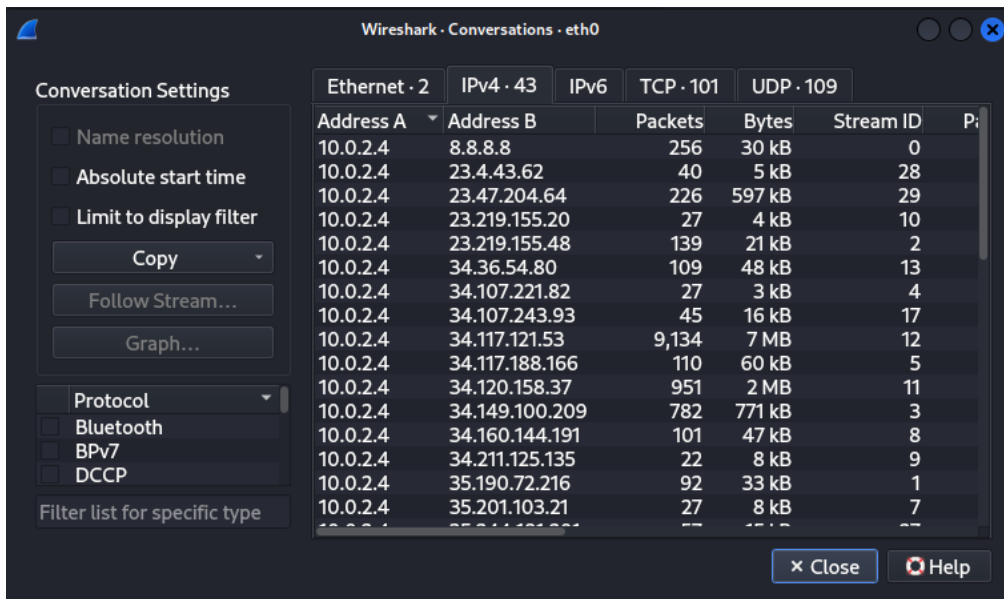
## 3. Advanced Analysis

Use of statistics to analyze protocol hierarchy:



I can see the breakdown of the protocols used in the capture.

Use of statistics to analyze the conversations:



Wireshark - Conversations - eth0

Conversation Settings

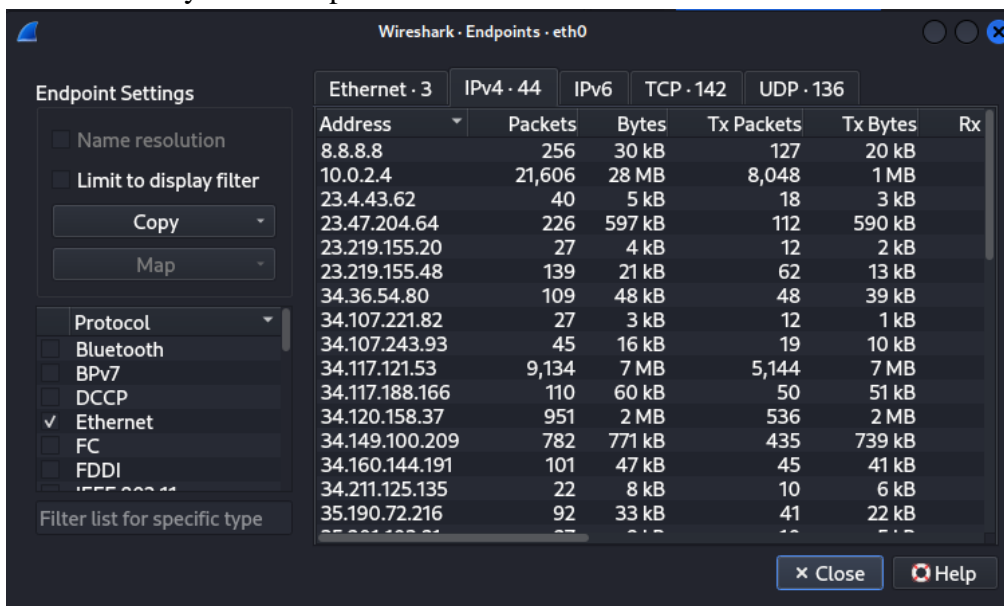
- ☐ Name resolution
- ☐ Absolute start time
- ☐ Limit to display filter
- Copy
- Follow Stream...
- Graph...
- Protocol
- ☐ Bluetooth
- ☐ BPv7
- ☐ DCCP
- Filter list for specific type

Ethernet · 2	IPv4 · 43	IPv6	TCP · 101	UDP · 109
Address A	Address B	Packets	Bytes	Stream ID
10.0.2.4	8.8.8.8	256	30 kB	0
10.0.2.4	23.4.43.62	40	5 kB	28
10.0.2.4	23.47.204.64	226	597 kB	29
10.0.2.4	23.219.155.20	27	4 kB	10
10.0.2.4	23.219.155.48	139	21 kB	2
10.0.2.4	34.36.54.80	109	48 kB	13
10.0.2.4	34.107.221.82	27	3 kB	4
10.0.2.4	34.107.243.93	45	16 kB	17
10.0.2.4	34.117.121.53	9,134	7 MB	12
10.0.2.4	34.117.188.166	110	60 kB	5
10.0.2.4	34.120.158.37	951	2 MB	11
10.0.2.4	34.149.100.209	782	771 kB	3
10.0.2.4	34.160.144.191	101	47 kB	8
10.0.2.4	34.211.125.135	22	8 kB	9
10.0.2.4	35.190.72.216	92	33 kB	1
10.0.2.4	35.201.103.21	27	8 kB	7

Close Help

I can analyze the communication pairs and their traffic statistics.

Use of to analyze the endpoints:



Wireshark - Endpoints - eth0

Endpoint Settings

- ☐ Name resolution
- ☐ Limit to display filter
- Copy
- Map
- Protocol
- ☐ Bluetooth
- ☐ BPv7
- ☐ DCCP
- ☒ Ethernet
- ☐ FC
- ☐ FDDI
- ☐ IEEE 802.11
- Filter list for specific type

Ethernet · 3	IPv4 · 44	IPv6	TCP · 142	UDP · 136
Address	Packets	Bytes	Tx Packets	Tx Bytes
8.8.8.8	256	30 kB	127	20 kB
10.0.2.4	21,606	28 MB	8,048	1 MB
23.4.43.62	40	5 kB	18	3 kB
23.47.204.64	226	597 kB	112	590 kB
23.219.155.20	27	4 kB	12	2 kB
23.219.155.48	139	21 kB	62	13 kB
34.36.54.80	109	48 kB	48	39 kB
34.107.221.82	27	3 kB	12	1 kB
34.107.243.93	45	16 kB	19	10 kB
34.117.121.53	9,134	7 MB	5,144	7 MB
34.117.188.166	110	60 kB	50	51 kB
34.120.158.37	951	2 MB	536	2 MB
34.149.100.209	782	771 kB	435	739 kB
34.160.144.191	101	47 kB	45	41 kB
34.211.125.135	22	8 kB	10	6 kB
35.190.72.216	92	33 kB	41	22 kB

Close Help

I can analyze traffic statistics for specific endpoints.

Conclusion:

I have successfully captured network traffic and performed basic analysis. This setup allows me to explore and understand network traffic, which is an essential skill in cybersecurity fields.