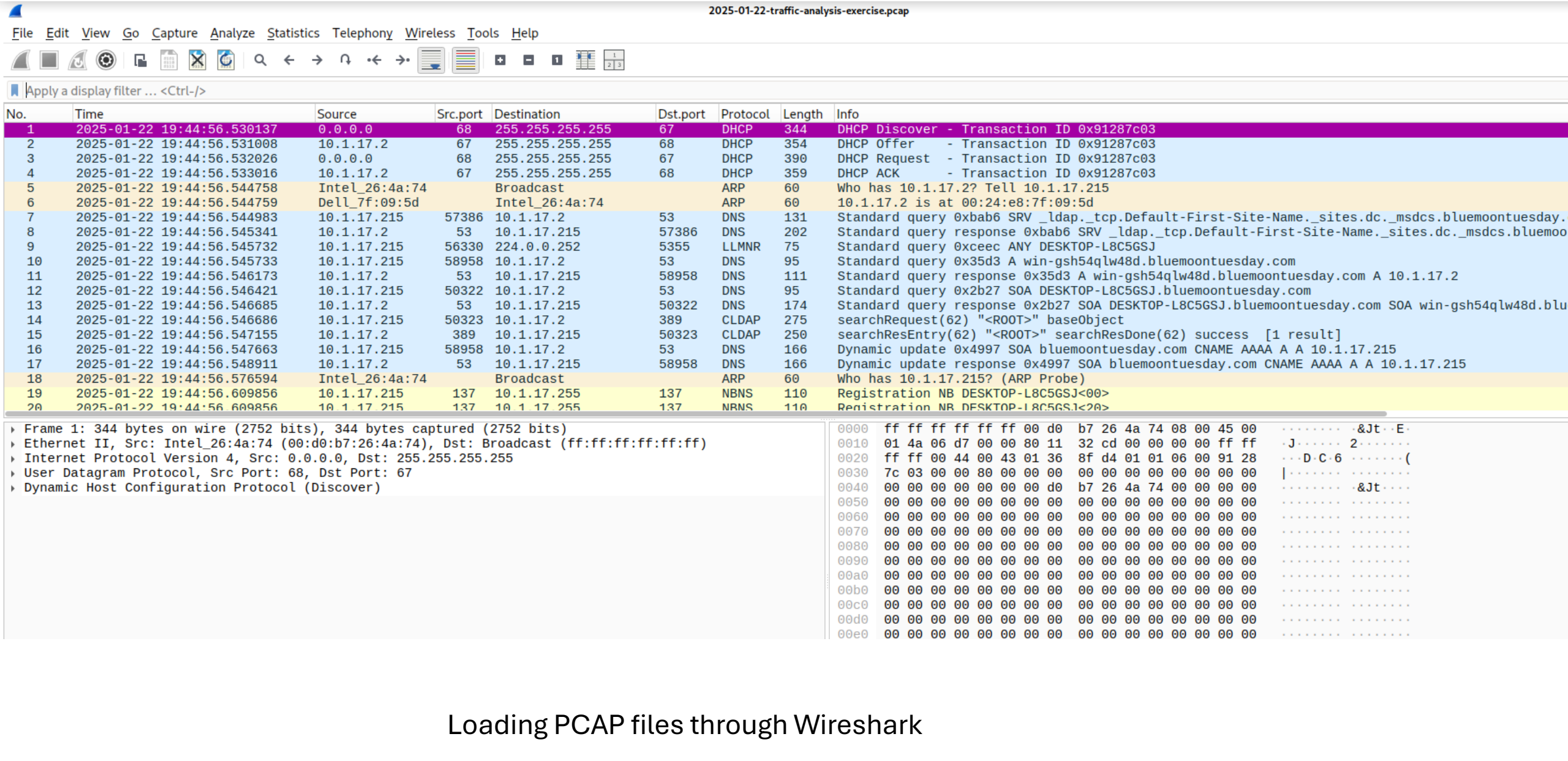
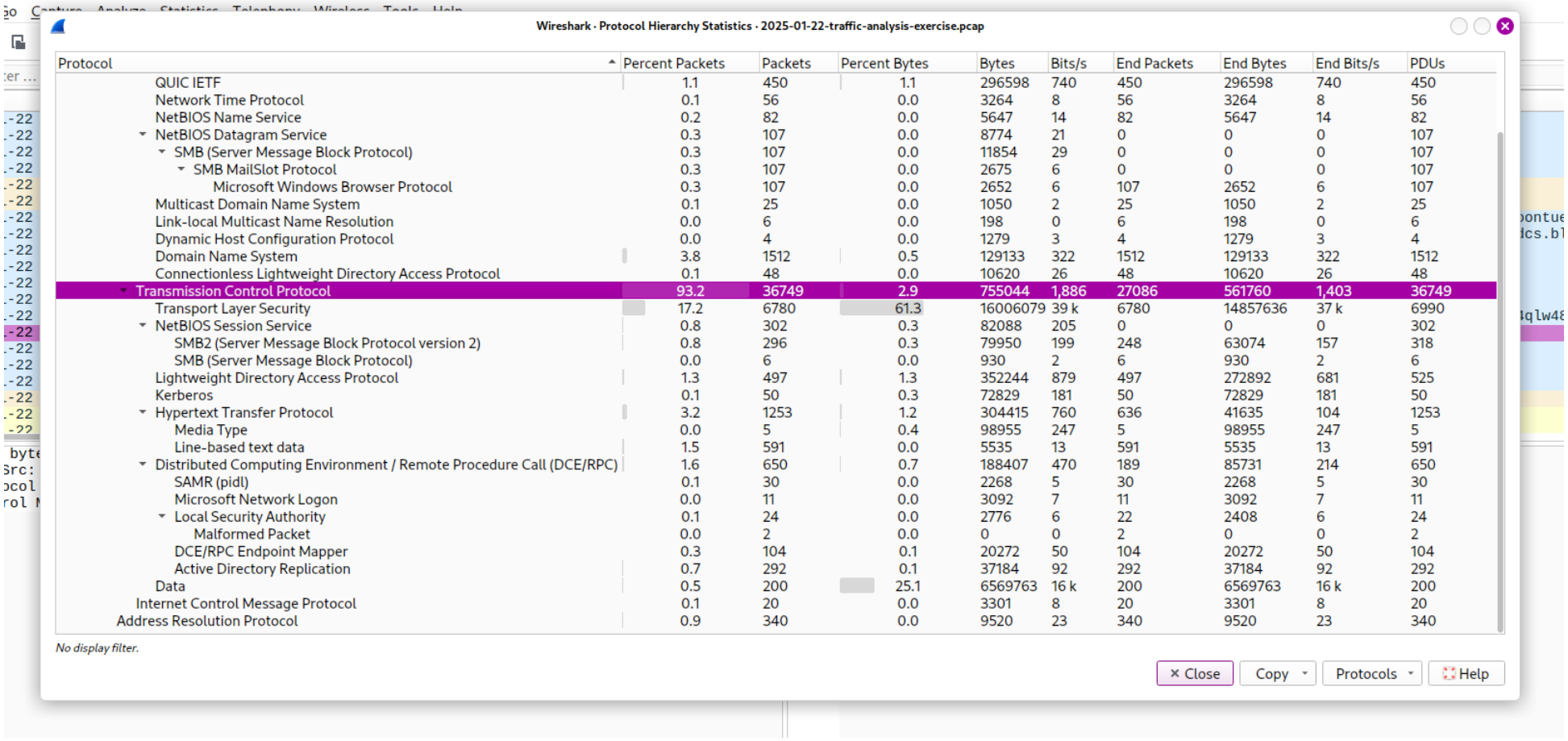
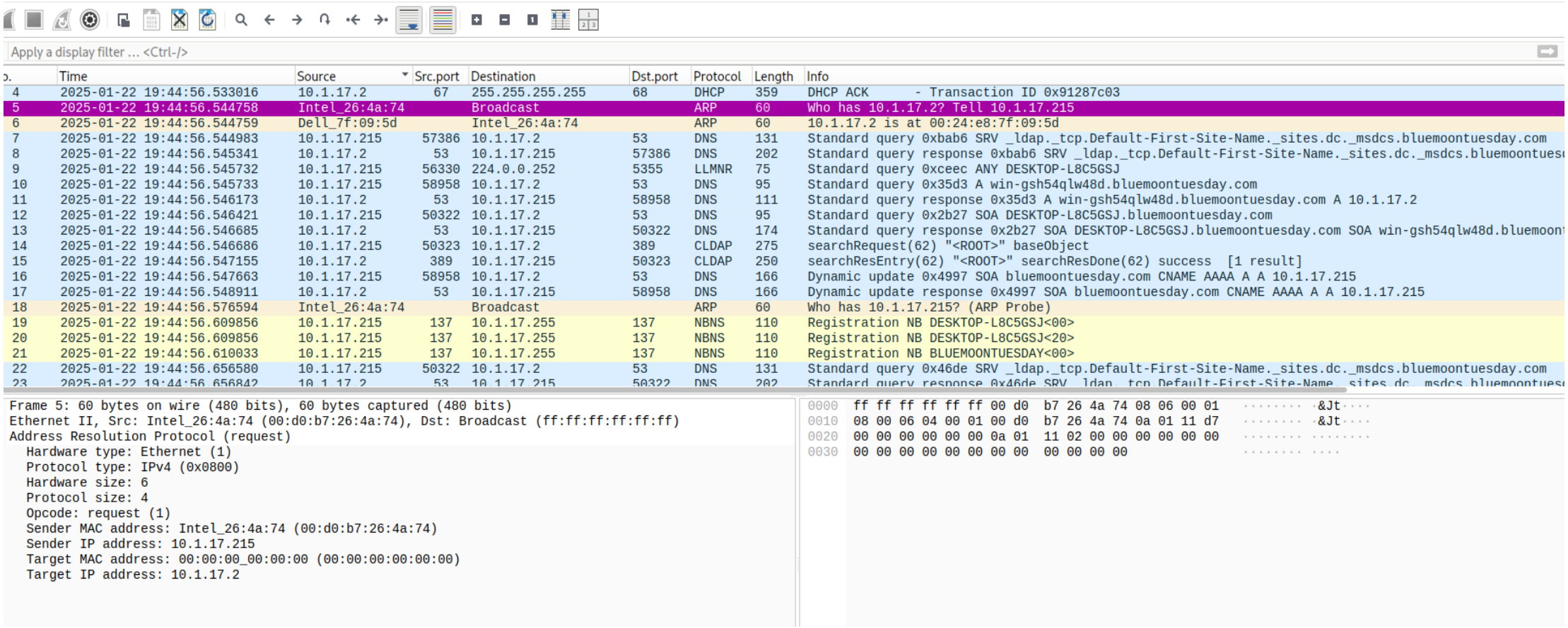


Loading PCAP files through Wireshark

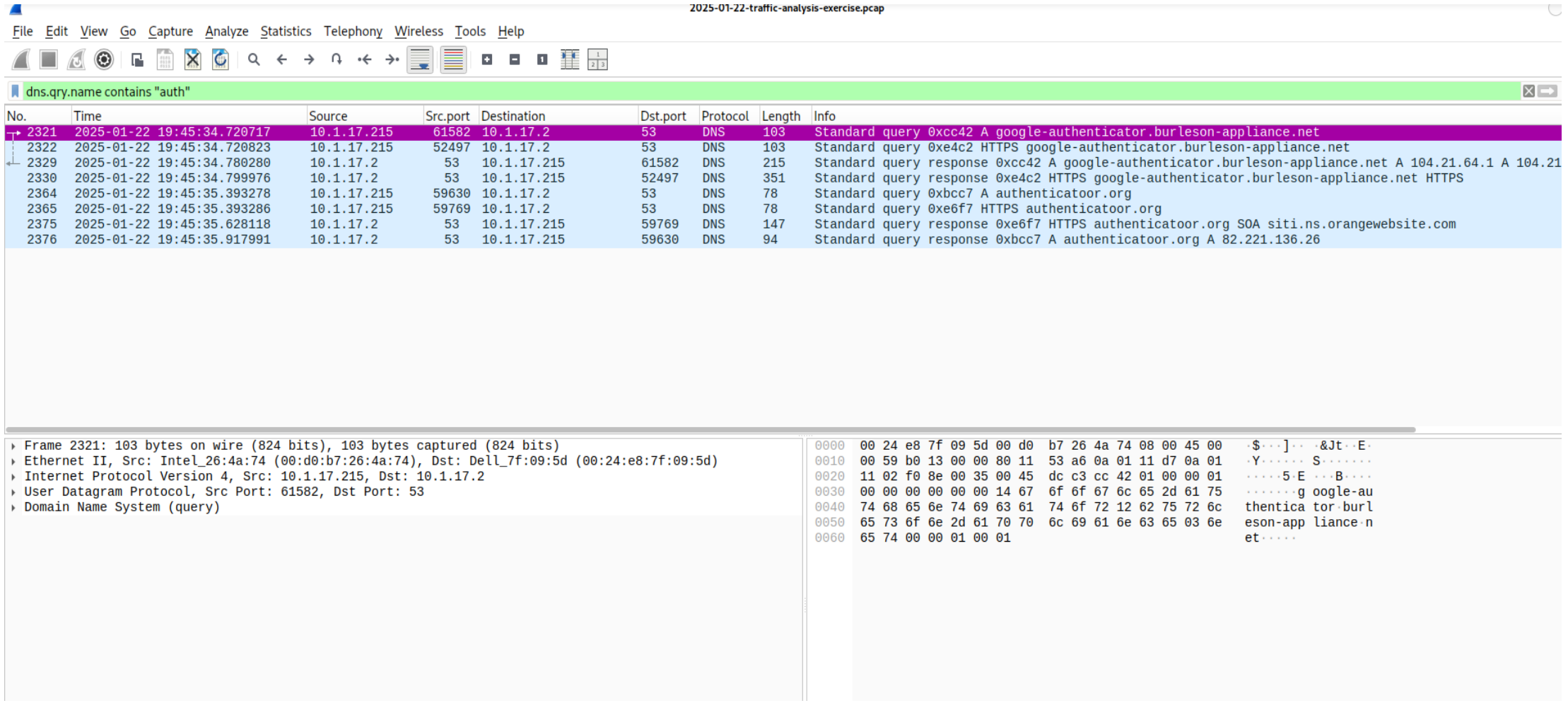


Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
QUIC IETF	1.1	450	1.1	296598	740	450	296598	740	450
Network Time Protocol	0.1	56	0.0	3264	8	56	3264	8	56
NetBIOS Name Service	0.2	82	0.0	5647	14	82	5647	14	82
NetBIOS Datagram Service	0.3	107	0.0	8774	21	0	0	0	107
SMB (Server Message Block Protocol)	0.3	107	0.0	11854	29	0	0	0	107
SMB MailSlot Protocol	0.3	107	0.0	2675	6	0	0	0	107
Microsoft Windows Browser Protocol	0.3	107	0.0	2652	6	107	2652	6	107
Multicast Domain Name System	0.1	25	0.0	1050	2	25	1050	2	25
Link-local Multicast Name Resolution	0.0	6	0.0	198	0	6	198	0	6
Dynamic Host Configuration Protocol	0.0	4	0.0	1279	3	4	1279	3	4
Domain Name System	3.8	1512	0.5	129133	322	1512	129133	322	1512
Connectionless Lightweight Directory Access Protocol	0.1	48	0.0	10620	26	48	10620	26	48
Transmission Control Protocol	93.2	36749	2.9	755044	1,886	27086	561760	1,403	36749
Transport Layer Security	17.2	6780	61.3	16006079	39 k	6780	14857636	37 k	6990
NetBIOS Session Service	0.8	302	0.3	82088	205	0	0	0	302
SMB2 (Server Message Block Protocol version 2)	0.8	296	0.3	79950	199	248	63074	157	318
SMB (Server Message Block Protocol)	0.0	6	0.0	930	2	6	930	2	6
Lightweight Directory Access Protocol	1.3	497	1.3	352244	879	497	272892	681	525
Kerberos	0.1	50	0.3	72829	181	50	72829	181	50
Hypertext Transfer Protocol	3.2	1253	1.2	304415	760	636	41635	104	1253
Media Type	0.0	5	0.4	98955	247	5	98955	247	5
Line-based text data	1.5	591	0.0	5535	13	591	5535	13	591
Distributed Computing Environment / Remote Procedure Call (DCE/RPC)	1.6	650	0.7	188407	470	189	85731	214	650
SAMR (pidl)	0.1	30	0.0	2268	5	30	2268	5	30
Microsoft Network Logon	0.0	11	0.0	3092	7	11	3092	7	11
Local Security Authority	0.1	24	0.0	2776	6	22	2408	6	24
Malformed Packet	0.0	2	0.0	0	0	2	0	0	2
DCE/RPC Endpoint Mapper	0.3	104	0.1	20272	50	104	20272	50	104
Active Directory Replication	0.7	292	0.1	37184	92	292	37184	92	292
Data	0.5	200	25.1	6569763	16 k	200	6569763	16 k	200
Internet Control Message Protocol	0.1	20	0.0	3301	8	20	3301	8	20
Address Resolution Protocol	0.9	340	0.0	9520	23	340	9520	23	340

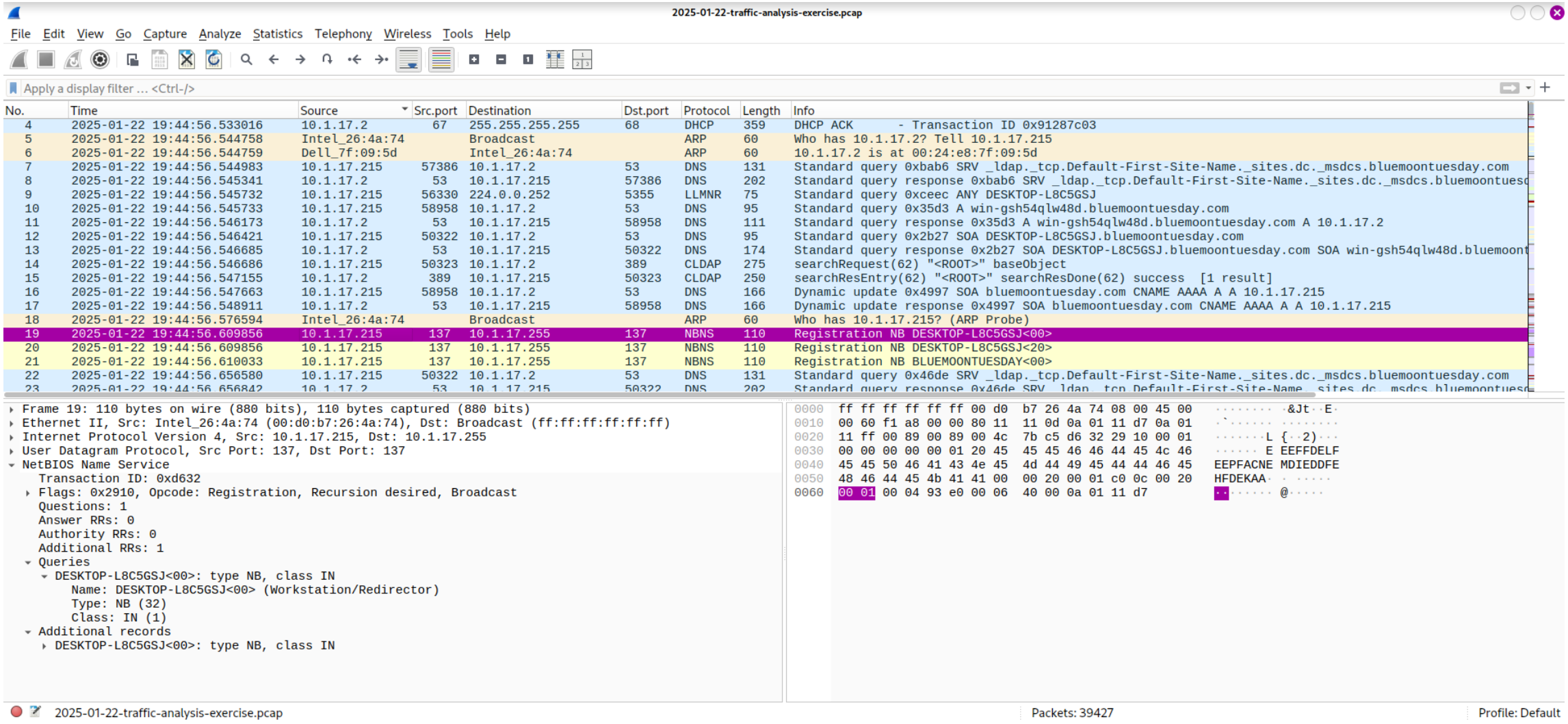
The first thing I do is go through statistics > protocol hierarchy and see where the traffic is moving the most, and I see through TCP.



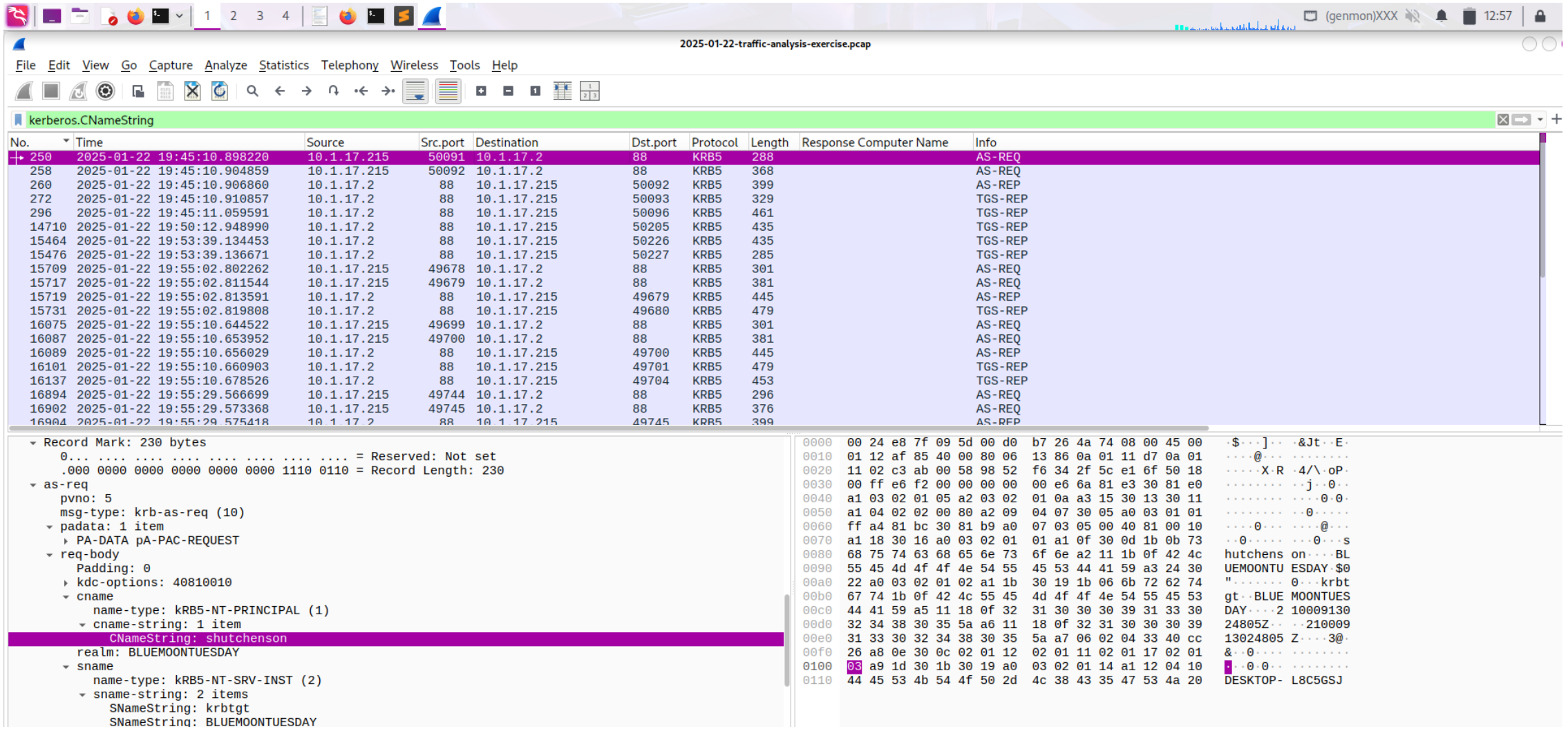
Checking through the traffic, where I can see the broadcast requesting the 10.1.17.215, to tell who has 10.1.17.2. It says it resides at this so-and-so MAC address.



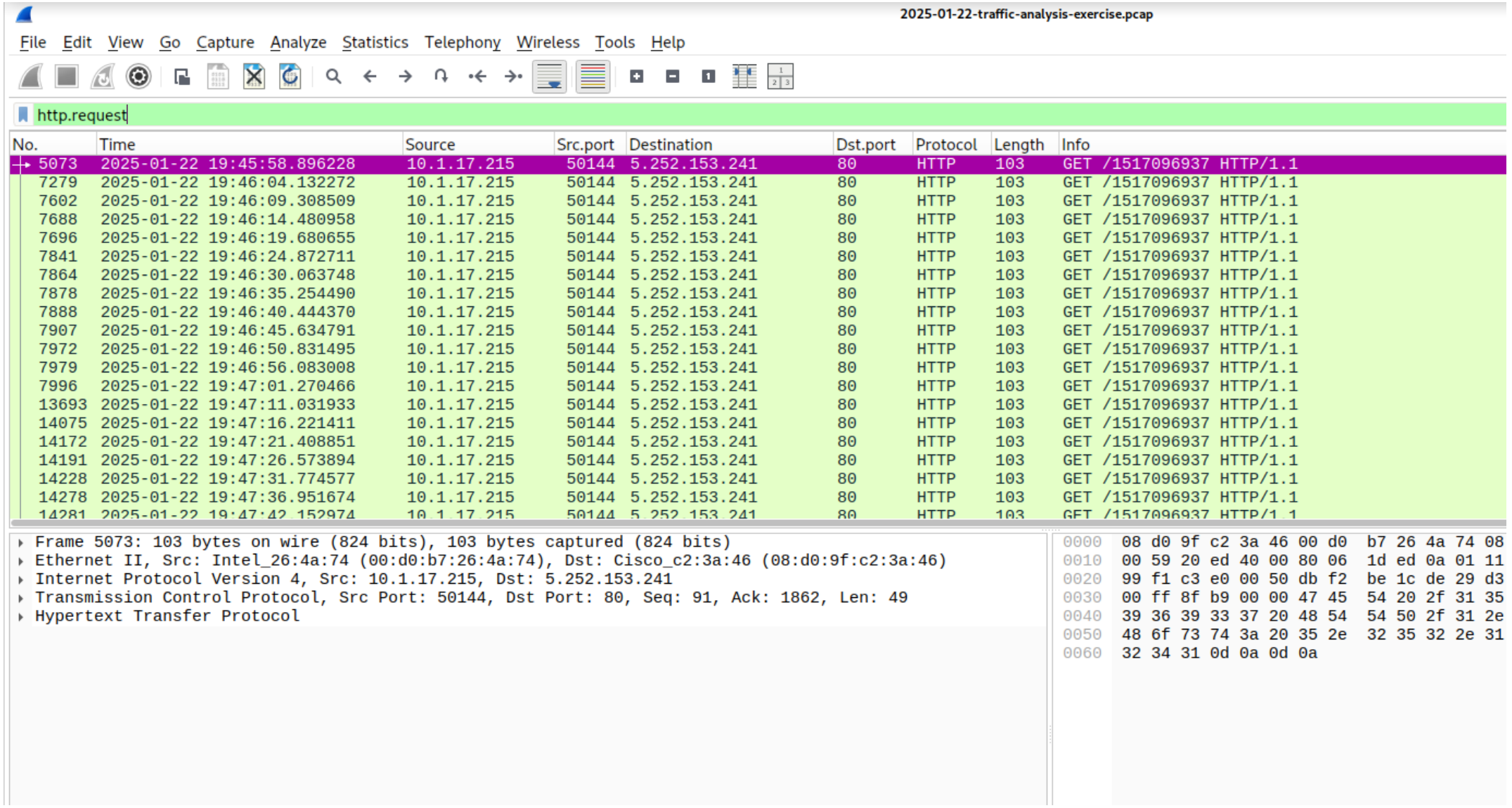
As it says, fake Google Authenticator, I looked through the search as “dns.qry.name contains ‘auth’”, where it gave me a few packets as I can see the typo name as “authenticatoor.org” – flag 1
Where the source address or infected IP that accessed the fake auth is 10.1.17.215 – flag 2



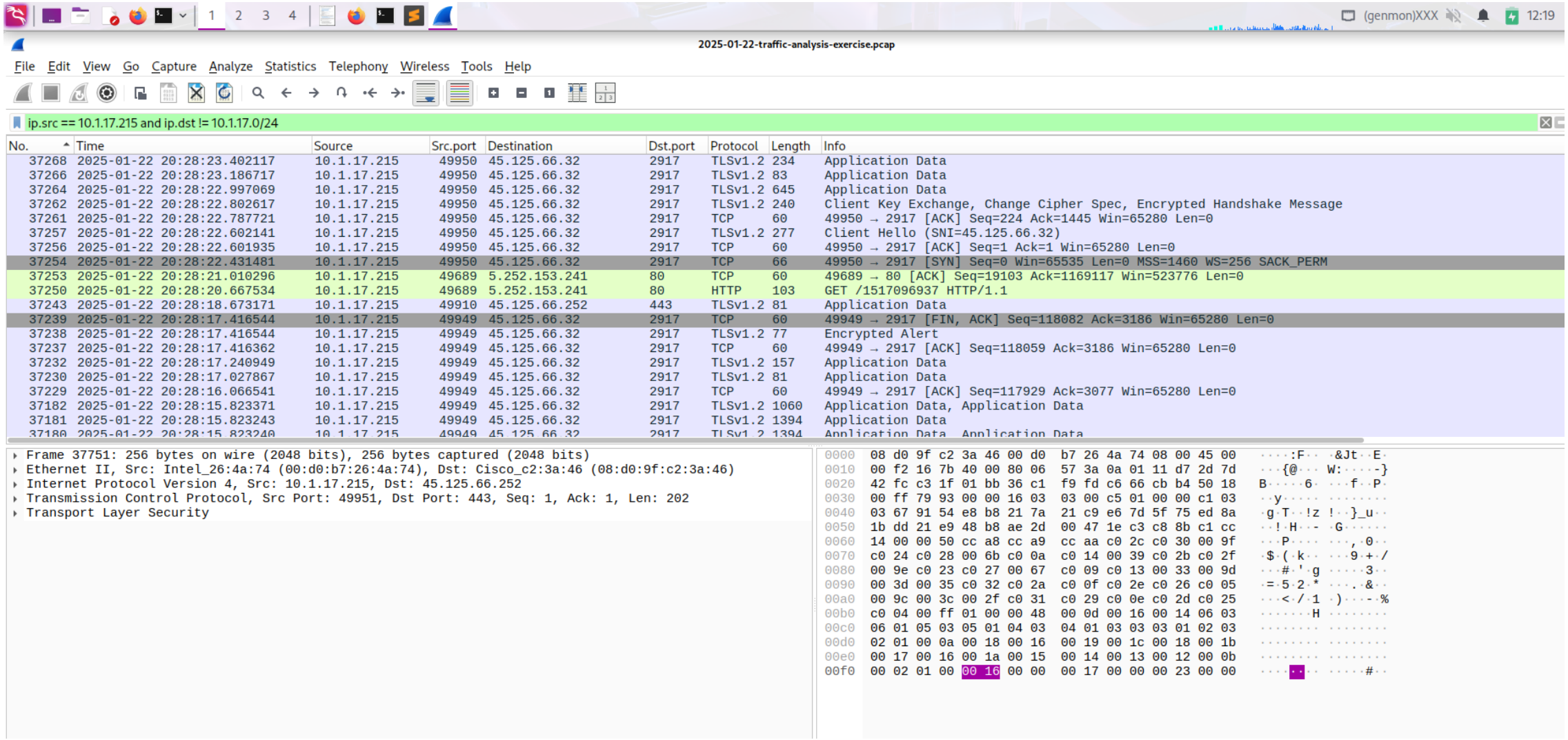
The source address that accessed a malicious website and its hostname are at NBNS > Queries > Desktop>Name



As I searched through the traffic to find the username, I used “kerberos,.CNameString”
It resides at the src.ip = 10.1.17.215.



To find the C2 beaconing, first, I used the “http.request” and found the first C2 server.



After applying another search request where the traffic is leaving the source IP found multiple entries.
These external IPs were involved in callback traffic post-infection, handling command and control communications.