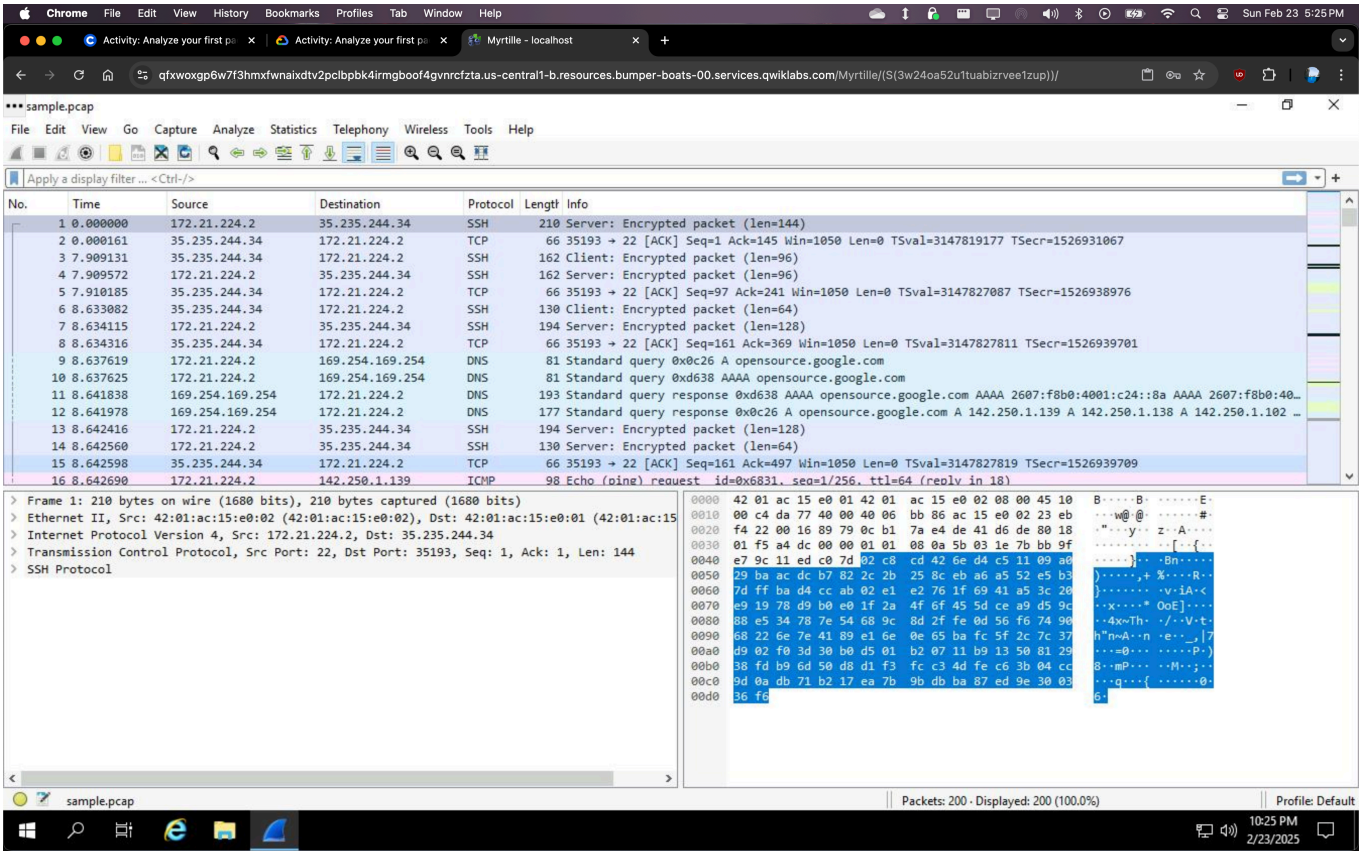
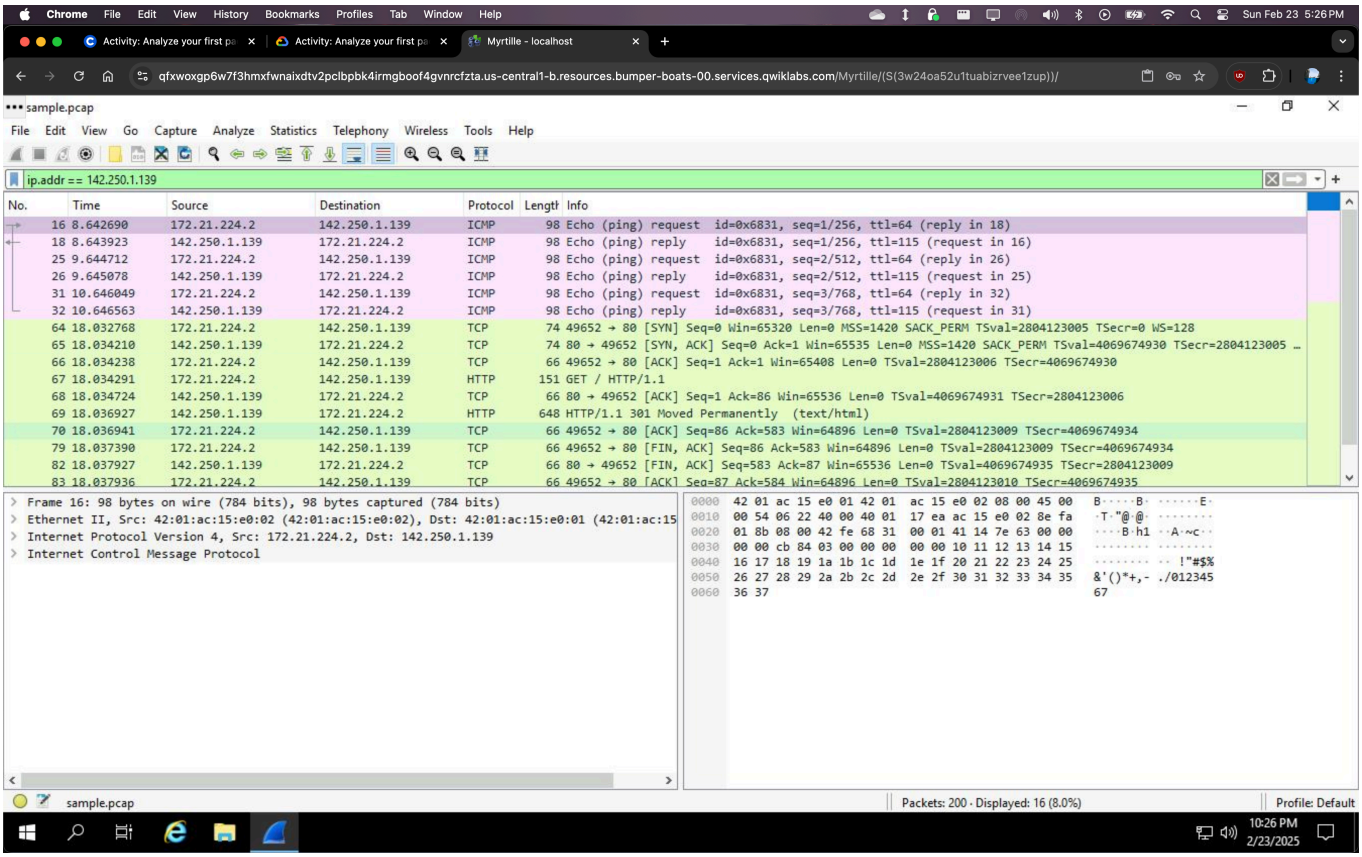
wireshark-ex1

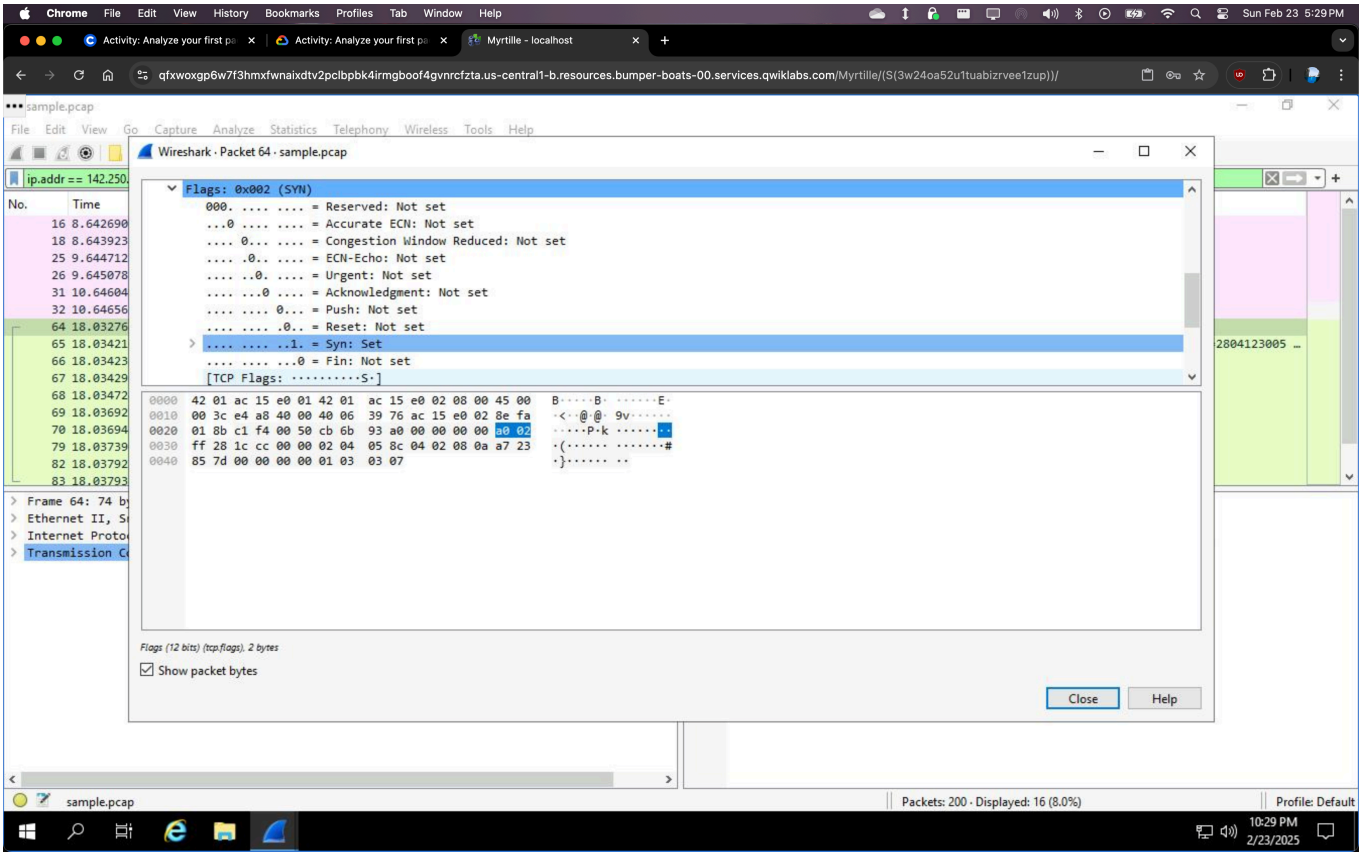
Example of using **Wireshark** to analyze network traffic and packets.



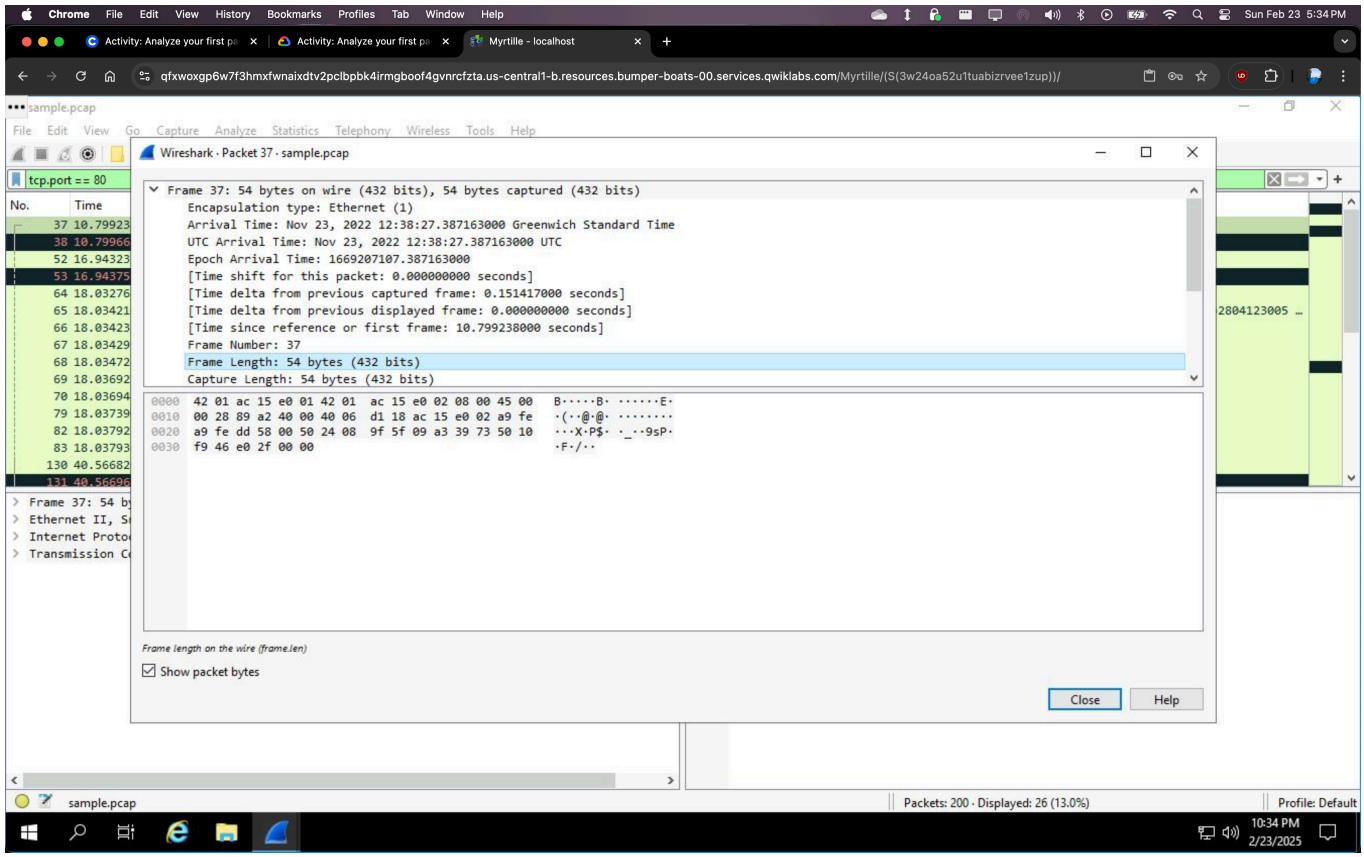
Filtering by IP:



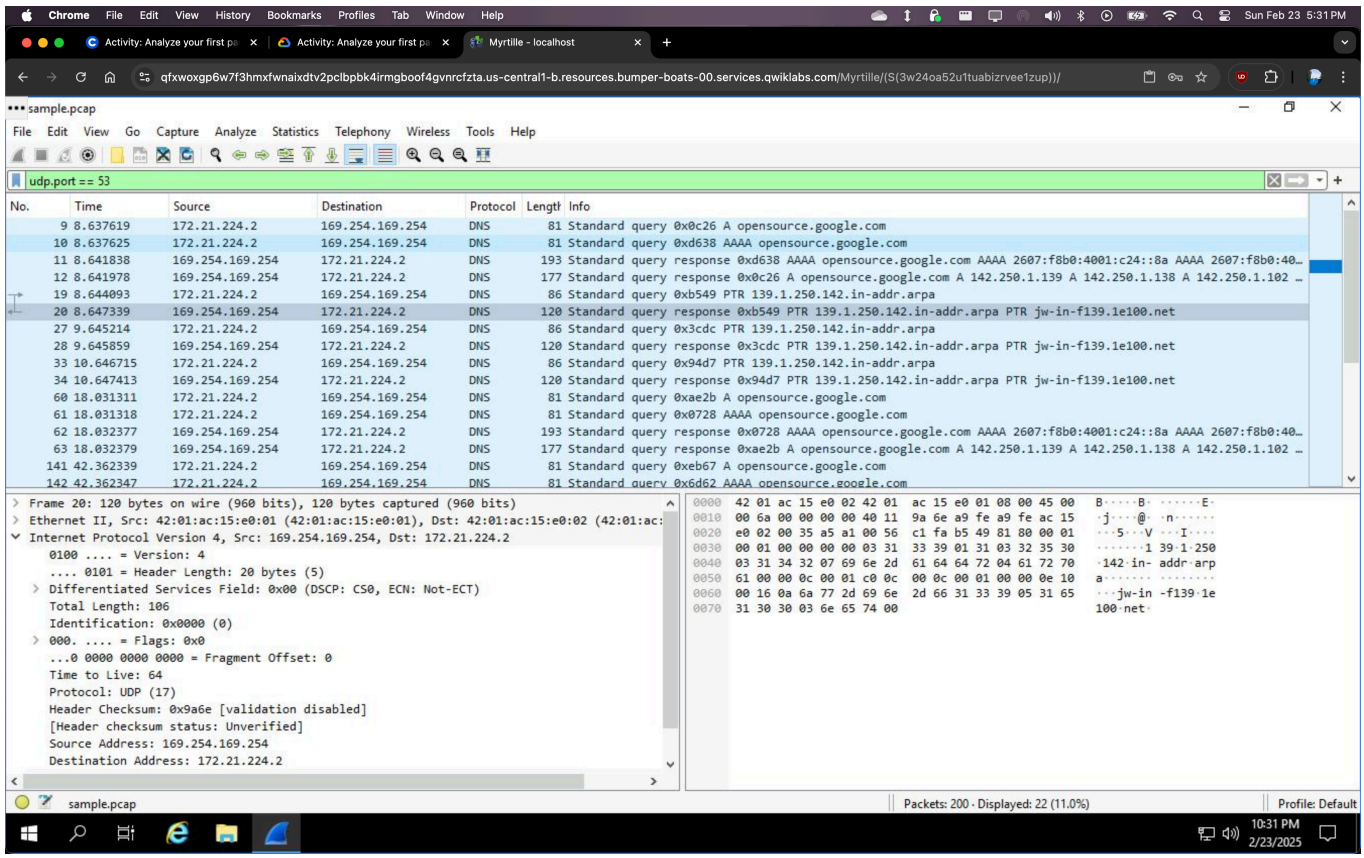
The packets of the filtered IPresults.

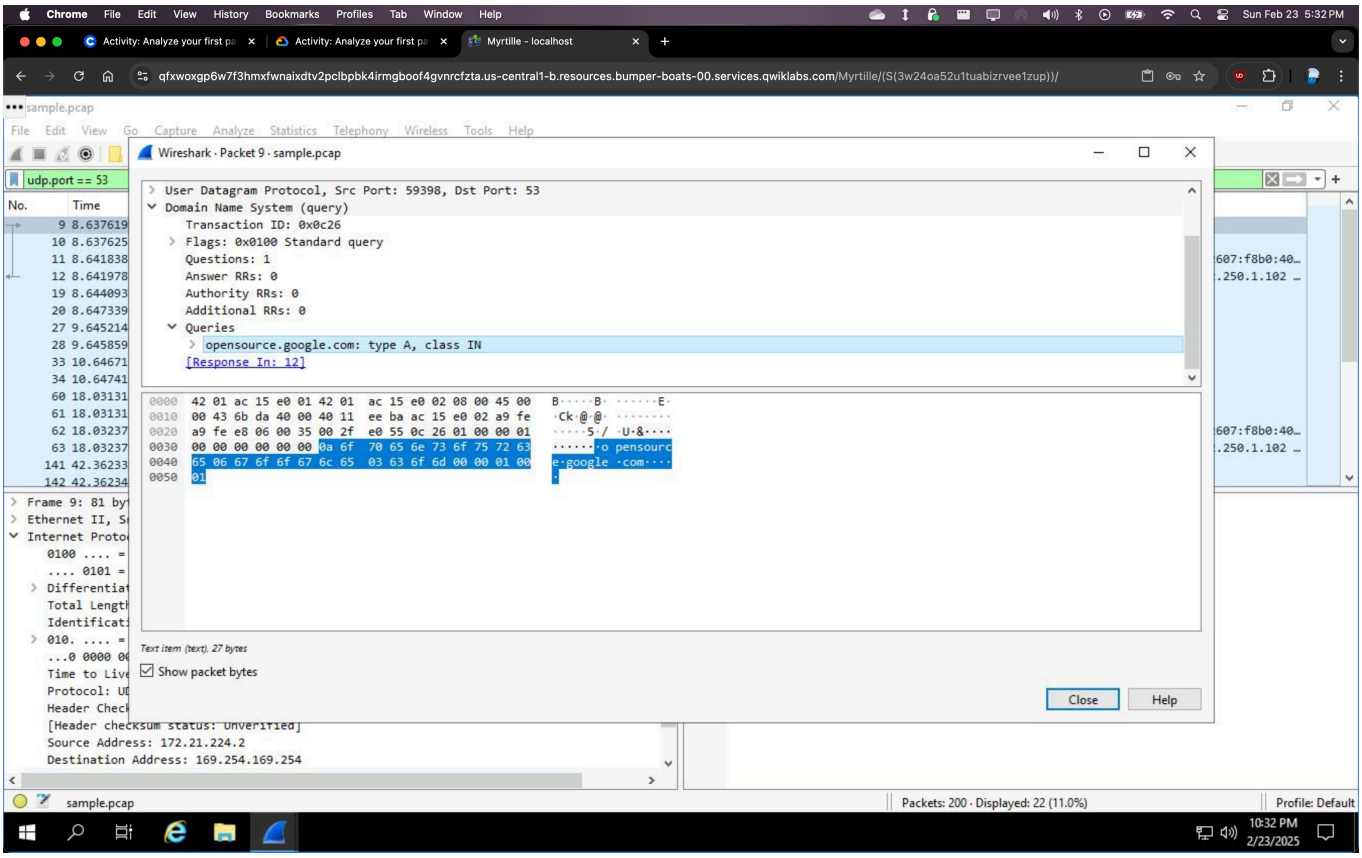


Filtering for all tcp protocol traffic:



Filtering for DNS queries and lookups:




Wireshark · Packet 9 · sample.pcap
User Datagram Protocol, Src Port: 59398, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x0c26
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
opensource.google.com: type A, class IN
[Response In: 12]
0000 42 01 ac 15 e0 01 42 01 ac 15 e0 02 08 00 45 00
0010 00 43 6b da 40 00 40 11 ee ba ac 15 e0 02 a9 fe
0020 a9 fe e8 06 00 35 00 2f e0 55 0c 26 01 00 00 01
0030 00 00 00 00 00 00 0a 6f 70 65 6e 73 6f 75 72 63
0040 65 06 67 6f 6f 67 6c 65 03 63 6f 6d 00 00 01 00
0050 01
Text item (text), 27 bytes
Show packet bytes
Close
Help
sample.pcap
Packets: 200 · Displayed: 22 (11.0%)
Profile: Default