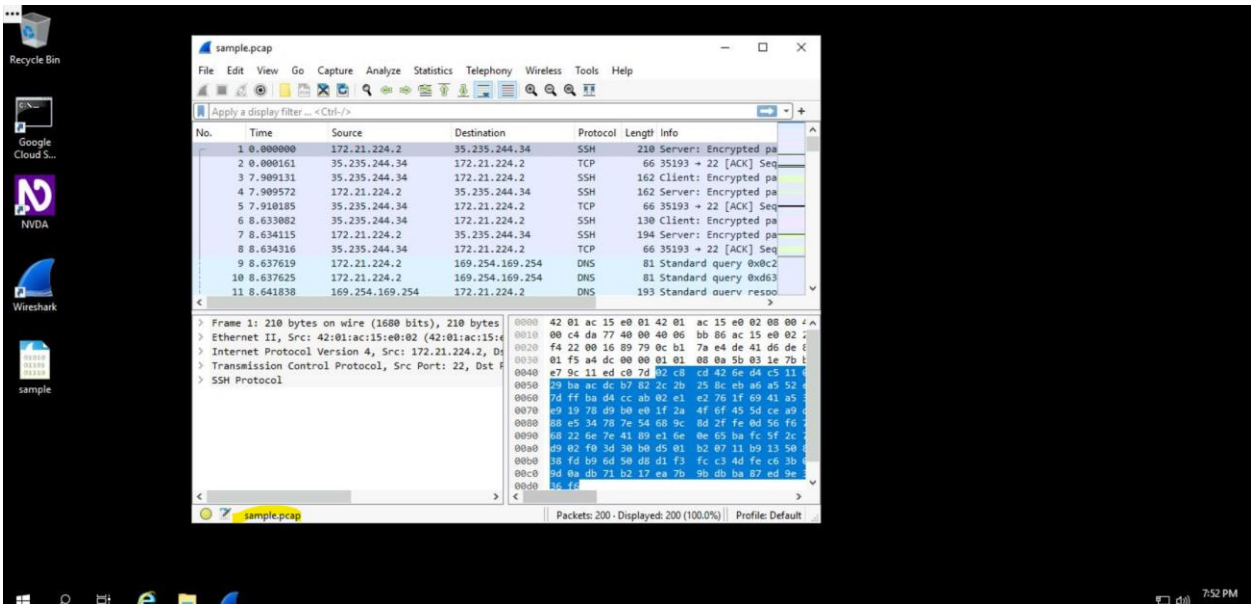
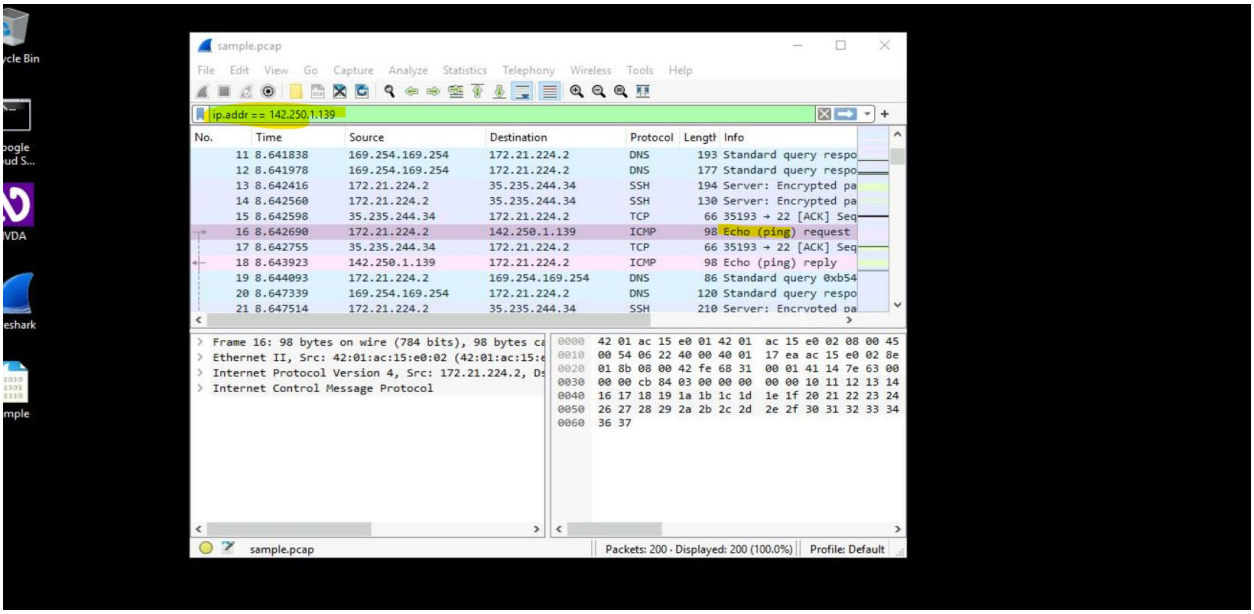
Analyzing packets using Wireshark

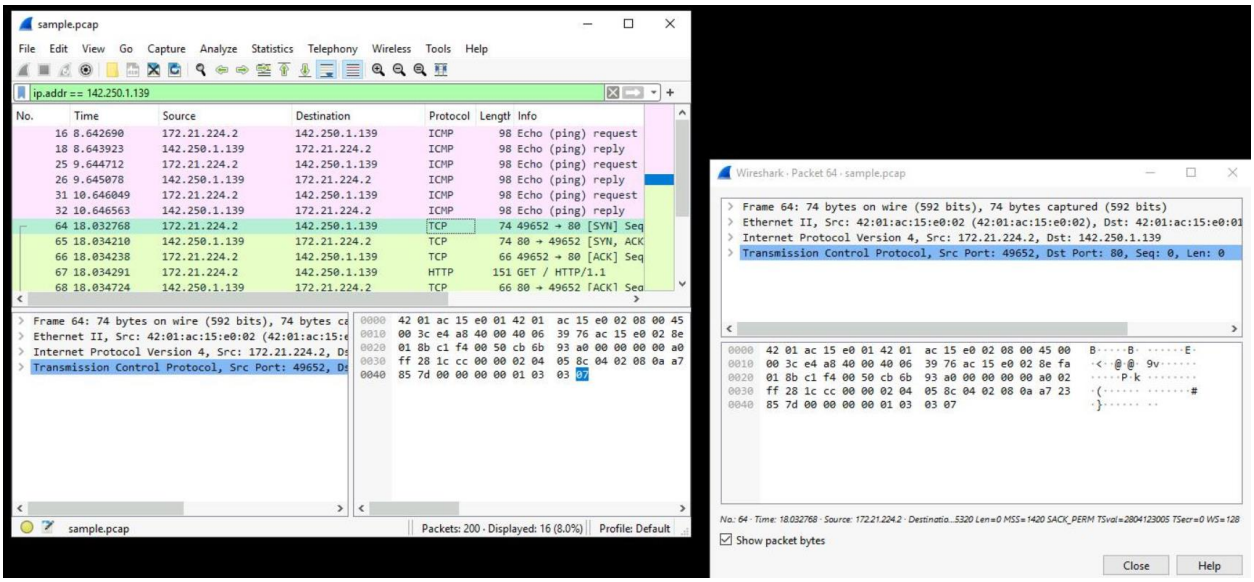
After reviewing the data and scrolling down until noticing a “Ping request” in the Info column:



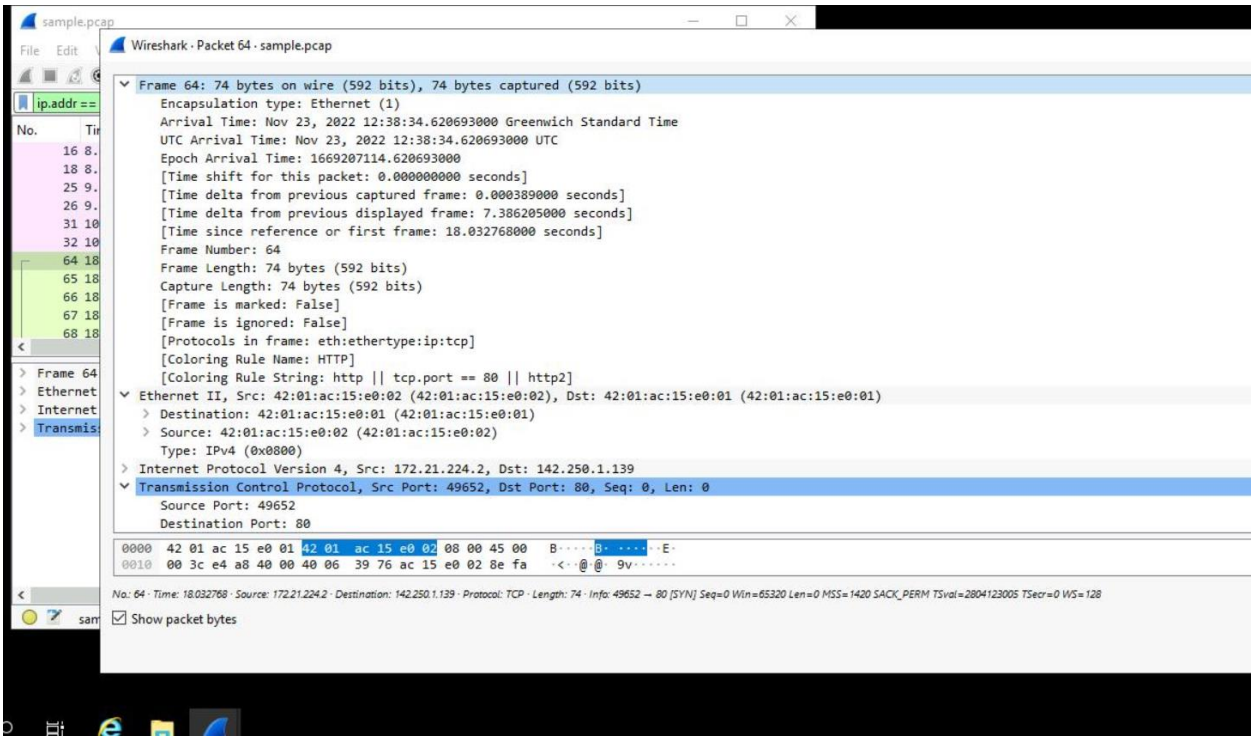
then filtering by that Destination address:



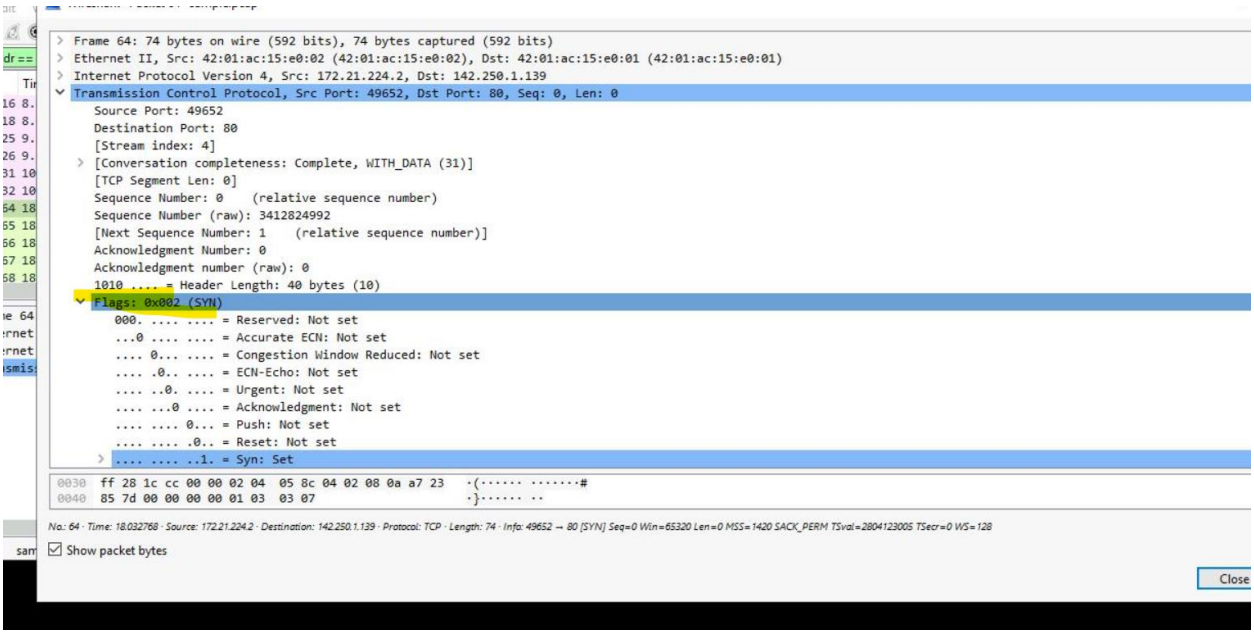
Selecting the first TCP protocol with the matching address, to inspect its subtrees on the right screen dump:



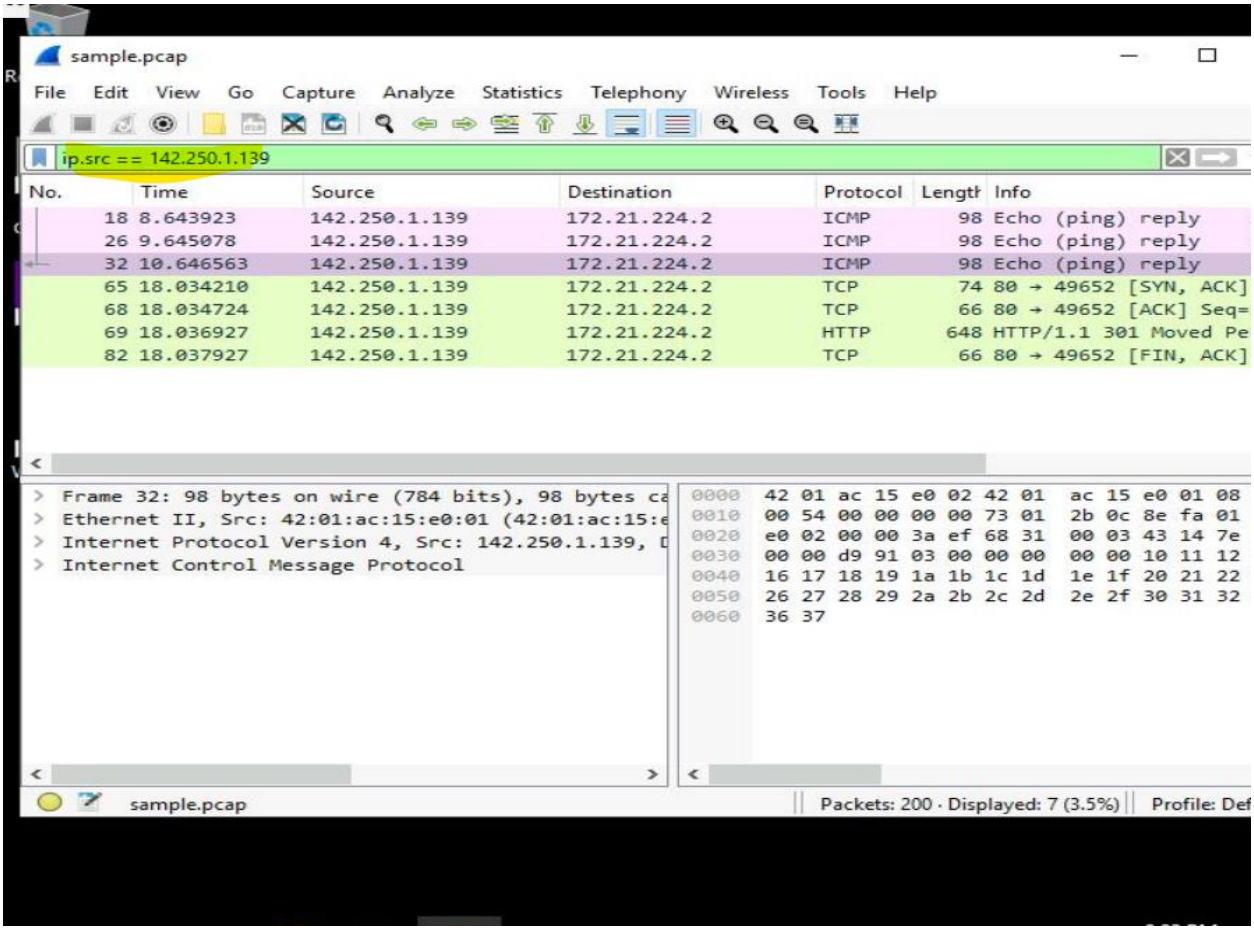
Here I'm able to see the overall network packet, source & destination MAC addresses, IP data which is TCP communicating on port 80:



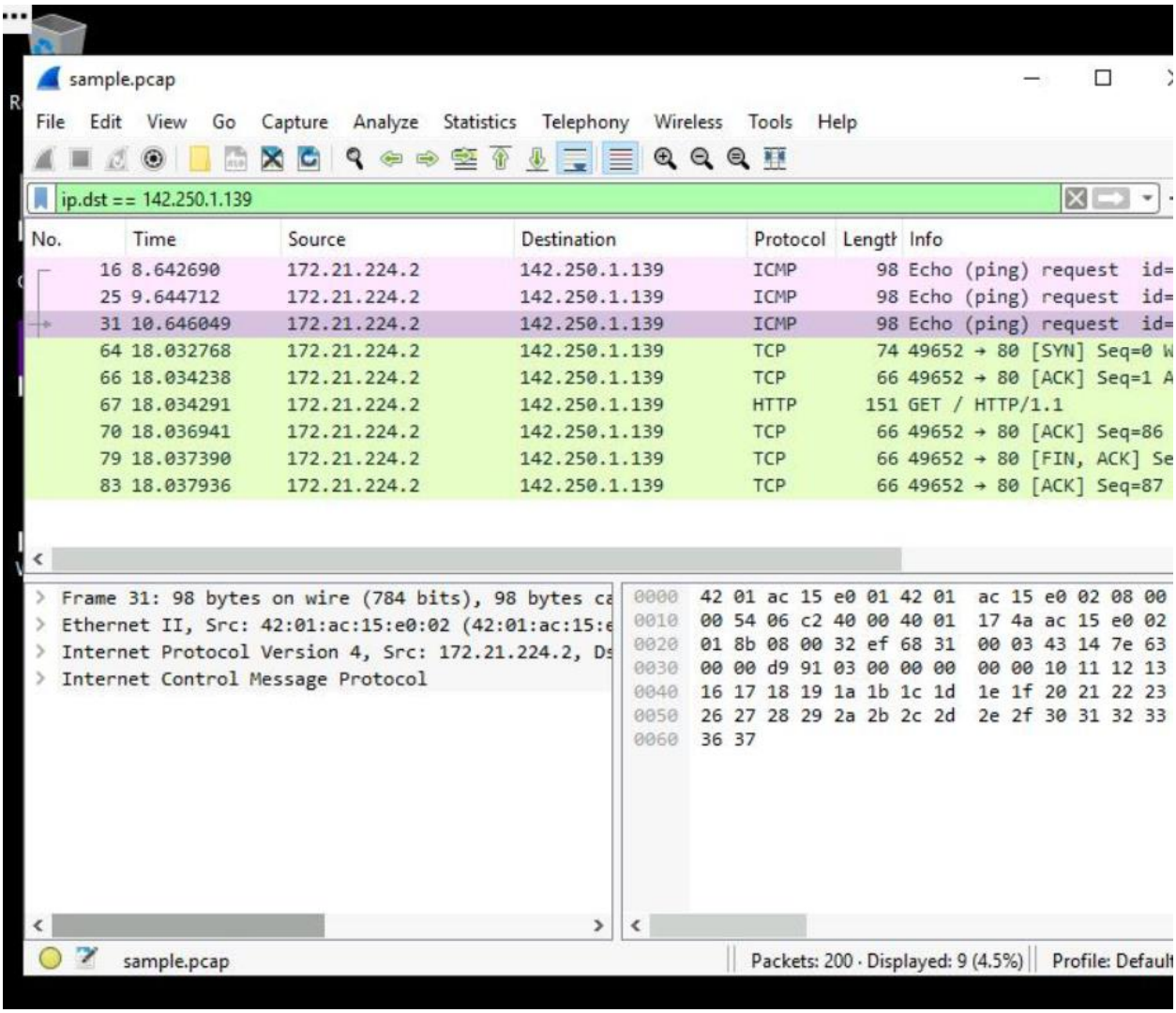
I can also review the flags within the TCP subtree:



Next, I'll run a filter using the same IP for source to inspect where the packets are coming from:



Then by destination, to understand where they're going:


sample.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst == 142.250.1.139
No. Time Source Destination Protocol Length Info
16 8.642690 172.21.224.2 142.250.1.139 ICMP 98 Echo (ping) request id=
25 9.644712 172.21.224.2 142.250.1.139 ICMP 98 Echo (ping) request id=
31 10.646049 172.21.224.2 142.250.1.139 ICMP 98 Echo (ping) request id=
64 18.032768 172.21.224.2 142.250.1.139 TCP 74 49652 → 80 [SYN] Seq=0 W
66 18.034238 172.21.224.2 142.250.1.139 TCP 66 49652 → 80 [ACK] Seq=1 A
67 18.034291 172.21.224.2 142.250.1.139 HTTP 151 GET / HTTP/1.1
70 18.036941 172.21.224.2 142.250.1.139 TCP 66 49652 → 80 [ACK] Seq=86
79 18.037390 172.21.224.2 142.250.1.139 TCP 66 49652 → 80 [FIN, ACK] Se
83 18.037936 172.21.224.2 142.250.1.139 TCP 66 49652 → 80 [ACK] Seq=87
Frame 31: 98 bytes on wire (784 bits), 98 bytes ca
Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e
Internet Protocol Version 4, Src: 172.21.224.2, Ds
Internet Control Message Protocol
0000 42 01 ac 15 e0 01 42 01 ac 15 e0 02 08 00
0010 00 54 06 c2 40 00 40 01 17 4a ac 15 e0 02
0020 01 8b 08 00 32 ef 68 31 00 03 43 14 7e 63
0030 00 00 d9 91 03 00 00 00 00 00 10 11 12 13
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33
0060 36 37
sample.pcap
Packets: 200 · Displayed: 9 (4.5%)
Profile: Default