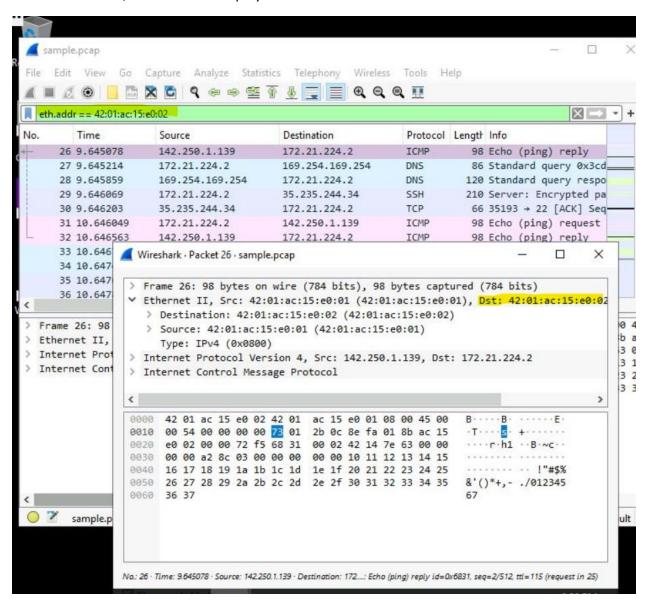
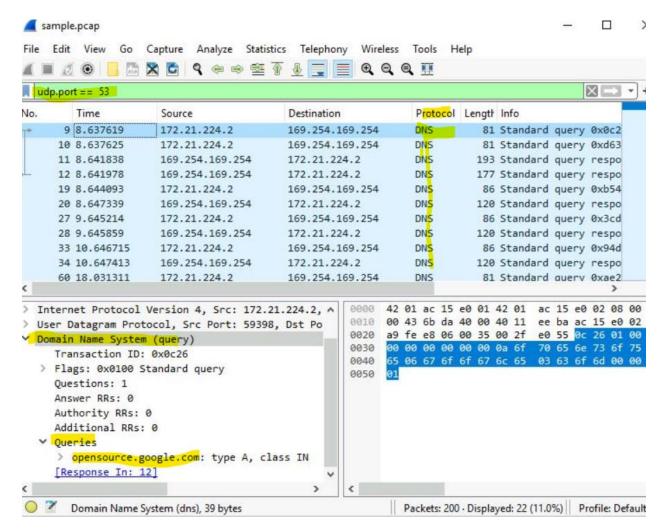
Filtering p-cap to examine MAC Address, DNS, & TCP data

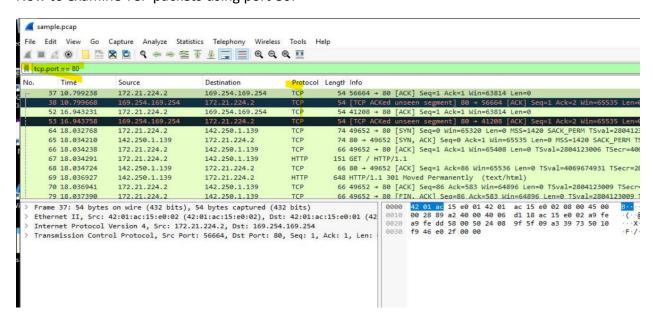
Next, I'll filter by a specific Ethernet MAC Address; by selecting the first packet and drilling into the Eth II subtree, the MAC will display as either the source or destination MAC address:



Filtering in Wireshark to explore DNS packets using port 53, and by drilling into the DNS subtree through Queries it shows the website that was queried:



Now to examine TCP packets using port 80:



By selecting the first packet, I can drill into the subtrees to review anything I prefer, for instance Time to live (TTL) [max numbers of hops a packet is allowed to pass through before discarded], src & destination addresses, byte size, protocol, ect:

```
•• Wireshark · Packet 37 · sample.pcap
Frame 37: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
     Encapsulation type: Ethernet (1)
     Arrival Time: Nov 23, 2022 12:38:27.387163000 Greenwich Standard Time
     UTC Arrival Time: Nov 23, 2022 12:38:27.387163000 UTC
     Epoch Arrival Time: 1669207107.387163000
     [Time shift for this packet: 0.000000000 seconds]
     [Time delta from previous captured frame: 0.151417000 seconds]
      [Time delta from previous displayed frame: 0.000000000 seconds]
      [Time since reference or first frame: 10.799238000 seconds]
     Frame Number: 37
     Frame Length: 54 bytes (432 bits)
     Capture Length: 54 bytes (432 bits)
     [Frame is marked: False]
     [Frame is ignored: False]
     [Protocols in frame: eth:ethertype:ip:tcp]
     [Coloring Rule Name: HTTP]
     [Coloring Rule String: http || tcp.port == 80 || http2]
> Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
Internet Protocol Version 4, Src: 172.21.224.2, Dst: 169.254.169.254
     0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
   > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
     Total Length: 40
     Identification: 0x89a2 (35234)
   > 010. .... = Flags: 0x2, Don't fragment
      ...0 0000 0000 0000 = Fragment Offset: 0
     Time to Live: 64
     Protocol: TCP (6)
     Header Checksum: 0xd118 [validation disabled]
     [Header checksum status: Unverified]
     Source Address: 172.21.224.2
0000 42 01 ac 15 e0 01 42 01 ac 15 e0 02 08 00 45 00
                                                          B .... - B . . . . - E
0010 00 28 89 a2 40 00 40 06 d1 18 ac 15 e0 02 a9 fe
                                                         · (··@·@· ······
```