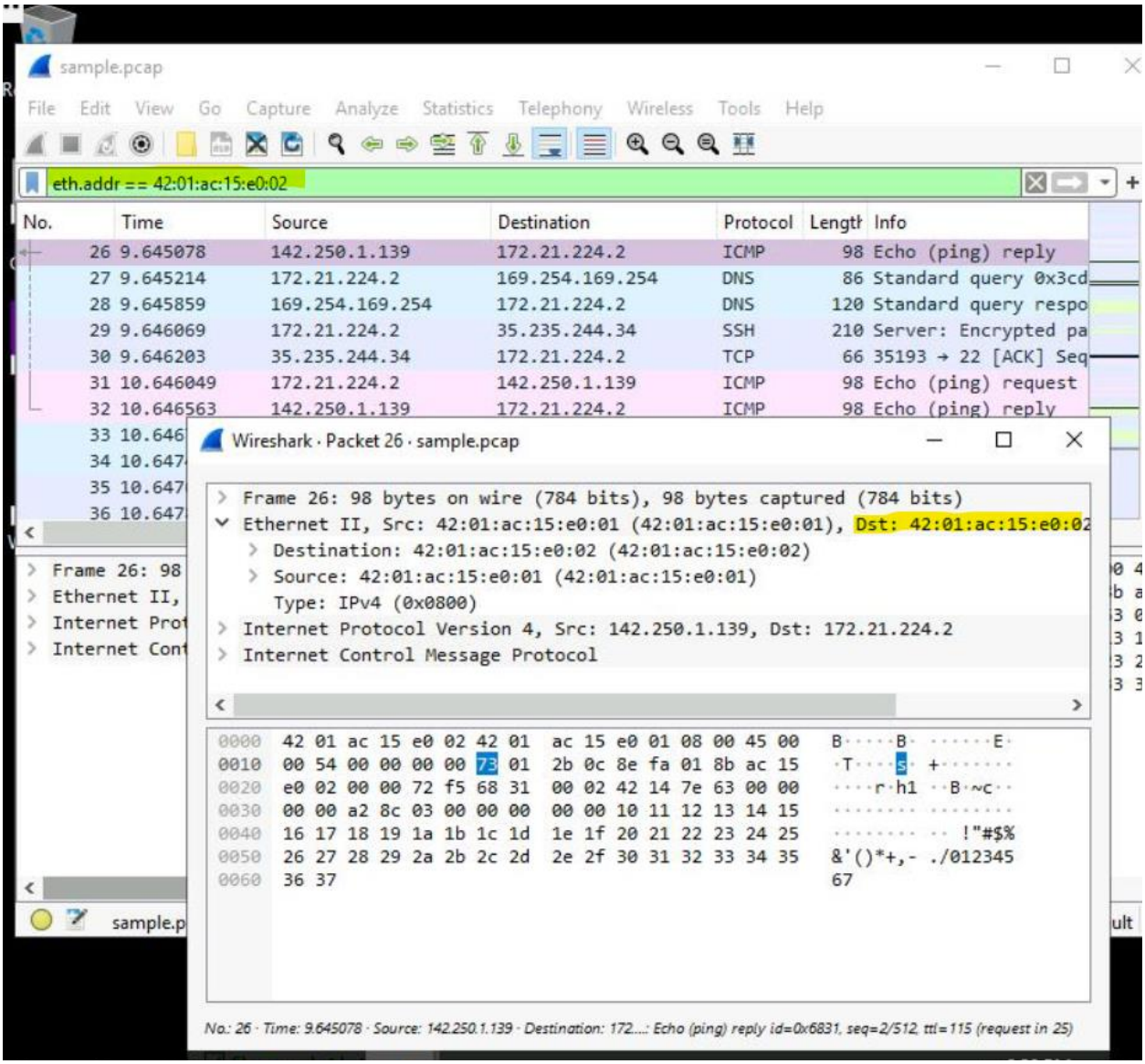
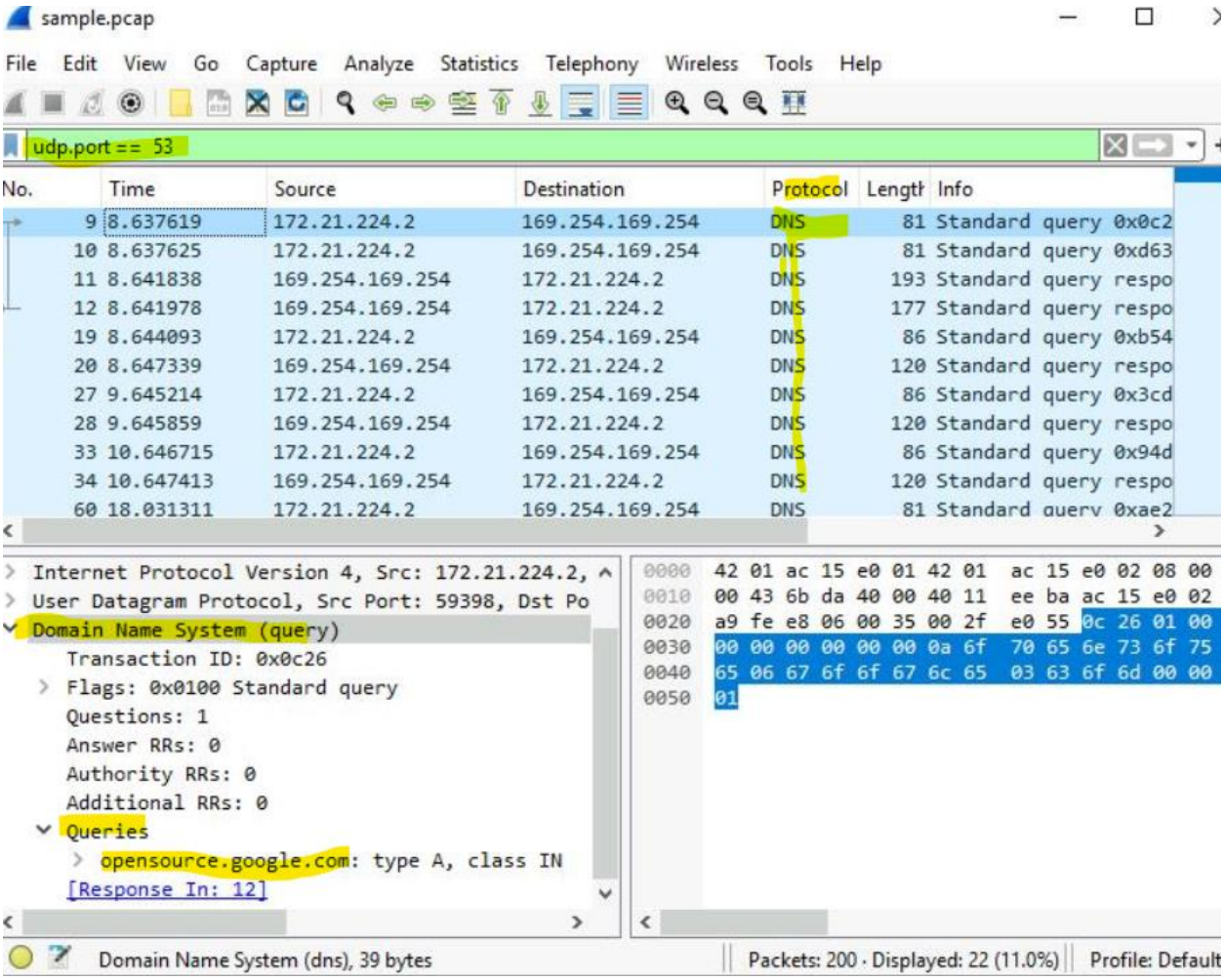
Filtering p-cap to examine MAC Address, DNS, & TCP data

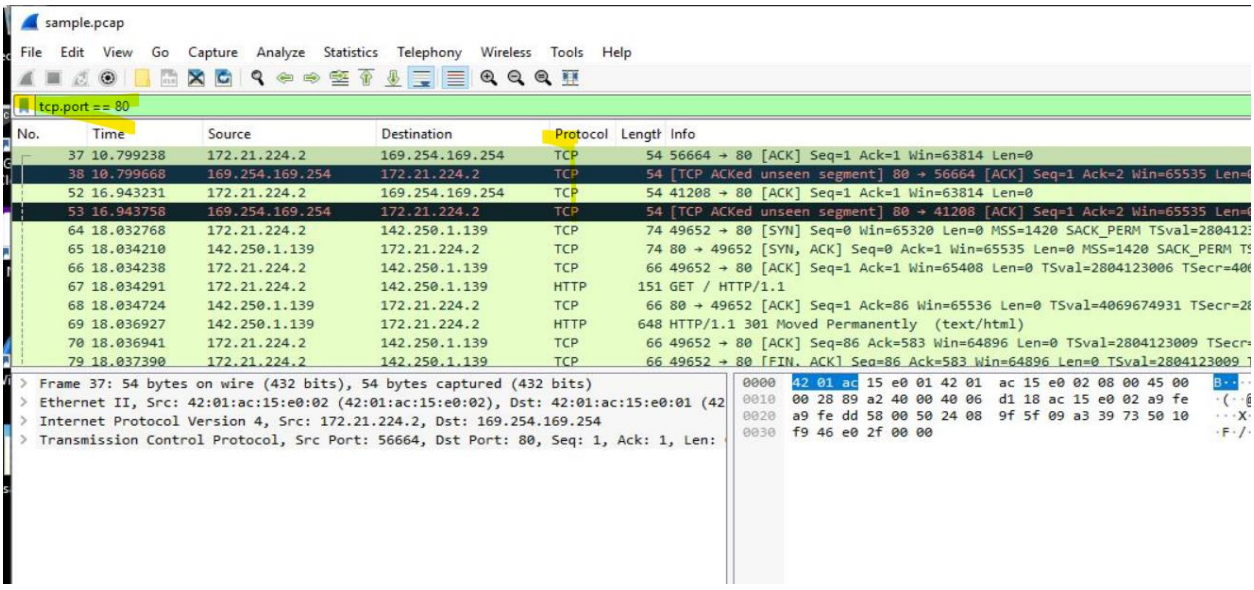
Next, I'll filter by a specific Ethernet MAC Address; by selecting the first packet and drilling into the Eth II subtree, the MAC will display as either the source or destination MAC address:



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: