1) What is the purpose of using filter in Wireshark?

Ans: Filters helps you focus on specific types of network traffic, making it easier to analyze and troubleshoot issue without being overwhelmed by all the data.

2) Which network interface did you use for capturing packets? Why?

An You would typically use the network interface that is connected to the internet or the local network you want to analyze. This allows you a capture relevant traffic.

Q3) Name at least 3 different protocols you observed during the capture.

→ Common protocols you might observe include
- HTTP (for web traffic)
- DNS (for domain name resolution)
- TCP (for reliable data transmission)

Q4) What is the IP address for your system (Source IP)?

Ans: You can find your system's IP address in Wireshark by looking at the source IP of any packet capture packet capture. It usually starts with "192.168." or "10.x" for local network.

Q5) What is one destination IP you communicate with during the capture?

Looks for any packet where your system's IP is the source. The destination IP will be the address

of the server or device your communicate with (eg: a website's IP)

6) Find a DNS query in your capture. What domain name was being looked up?

An Look for packets with the DNS protocol. You can find a query that shows a domain name like "example.com" being looked up.

07) Pick one HTTP packets and describe its source...

Ans Select an HTTP packets and check the details. The source IP is your system's IP, the destination IP is the web server's IP, and ~~most~~ the ~~non~~ Host name is usually found in the HTTP header.
eg: "Host: www.example.com"):

8) Which filter showed the most traffic? Why do you think that is?

Ans The HTTP filter often shows the most traffic because web browsing generates a lot of request and responses. Many user access website frequently leading to high HTTP ~~trapp~~ traffic.

9) Did you observe any encrypted traffic...?
Yes, you can tell if traffic is encrypted by looking for packets with the "TLS" or "SSL" protocol. These packet usually indicate secure connection, like HTTPS website.

10) What's the difference between 'ip.addr == x.x.x.x' and ip.src == x.x.x.x?

ip.addr == x.x.x.x : This filter shows packets where the IP address is either the source or destination.

ip.src == x.x.x.x : This filter shows only packets where the IP address is the source

11) FIND A TCP handshake (SYN, SYN-ACK, ACK)

→ A TCP handshake involve three steps:

1. SYN : your system sends a SYN packets to initiate a connection.
2. SYN - ACK : The server respond with a SYN-ACK packets to acknowledge the request.
3. Ack : your system sends an Ack packets to confirm the connection is established

12) What's one interesting thing you noticed in your network traffic?

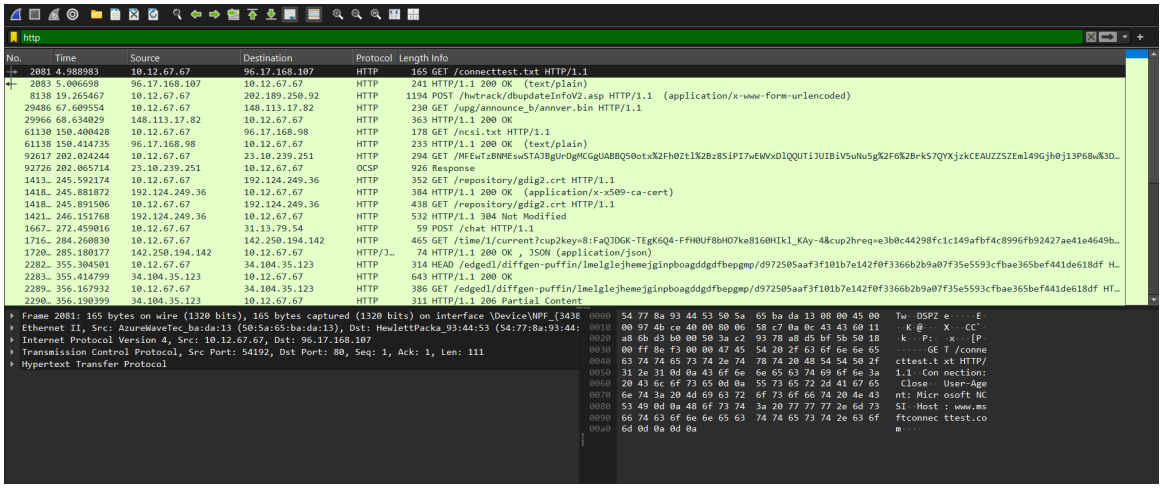
→ You might notice unusual traffic patterns, such as a high number of DNS queries, unexpected IP addresses communicating with your system, or a lot of encrypted traffic, which could indicate secure browsing or potential security concerns.

Assignment-12

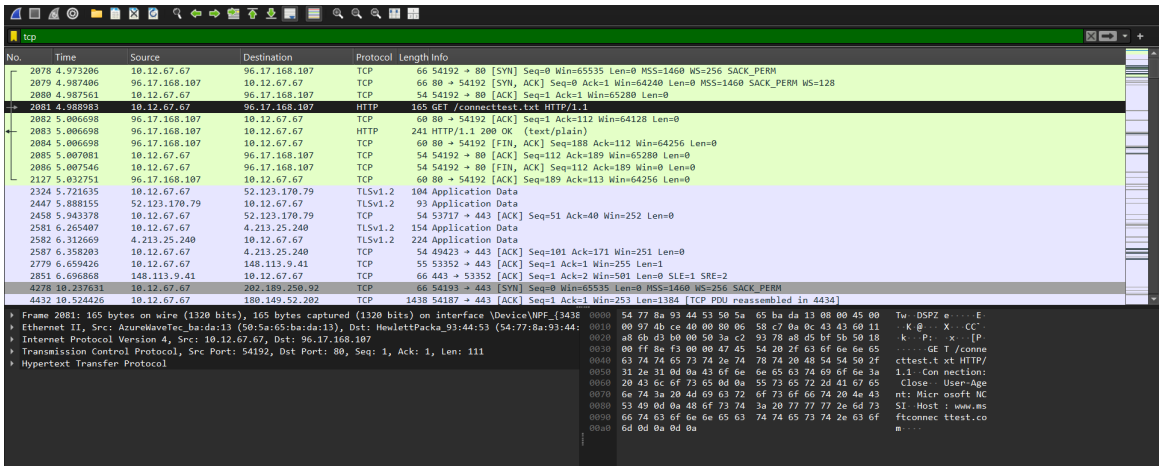
Wireshark display filters :-

1. Protocol-Based Filters

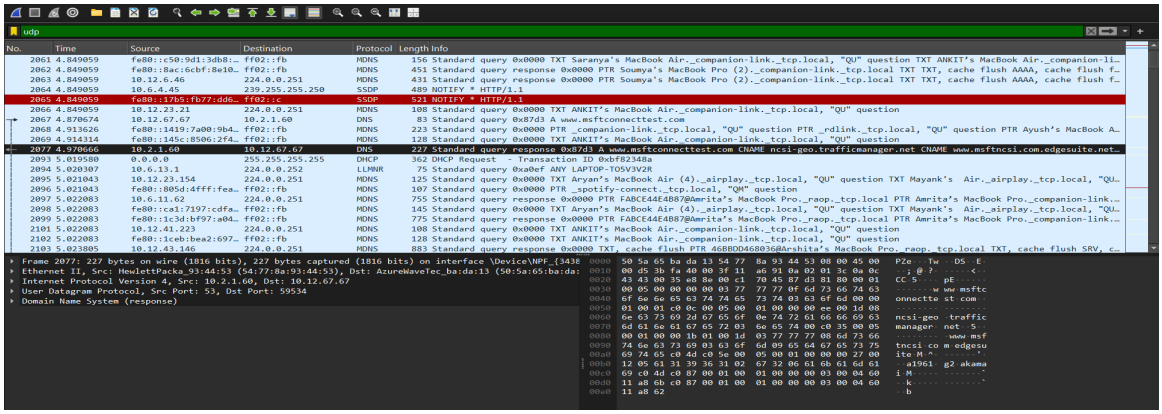
- **http – Shows only HTTP traffic**



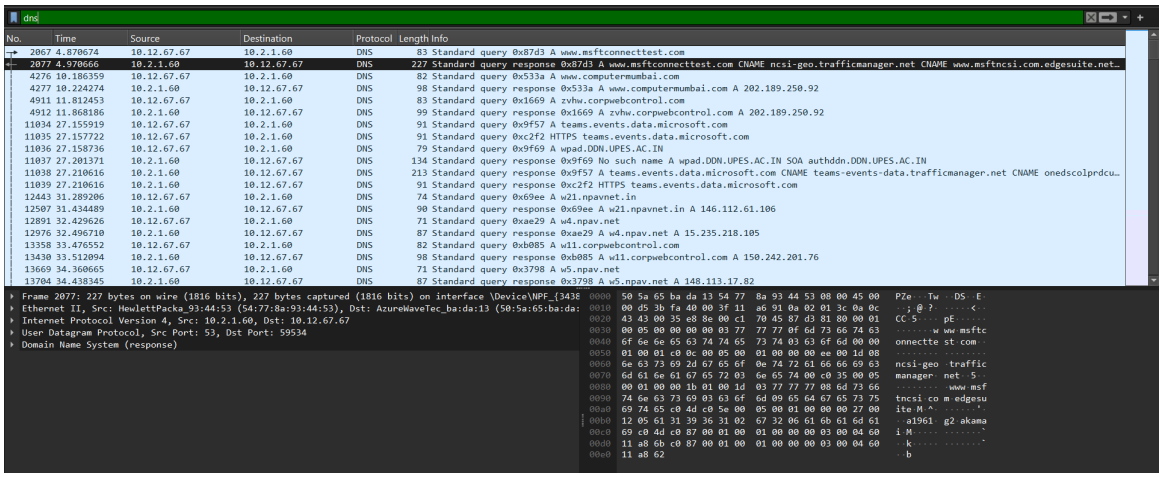
- **tcp – Displays only TCP packets**



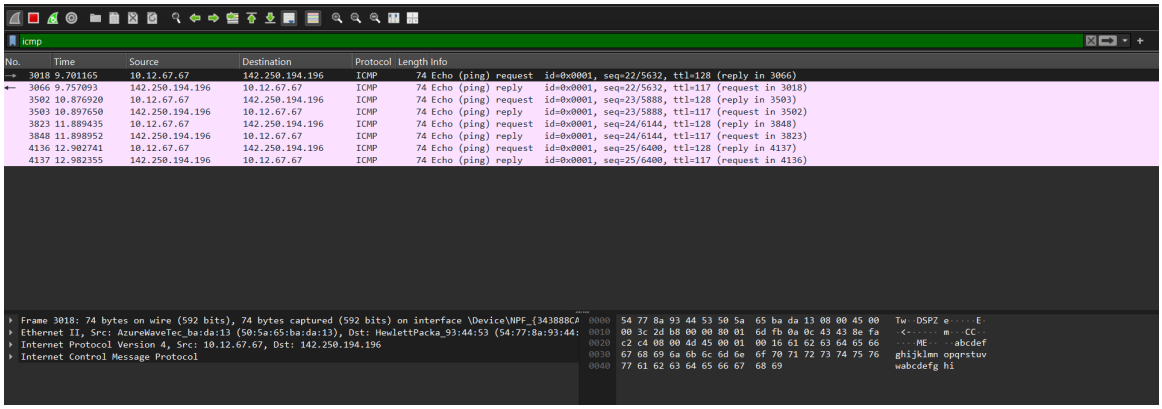
- **udp – Displays only UDP packets**



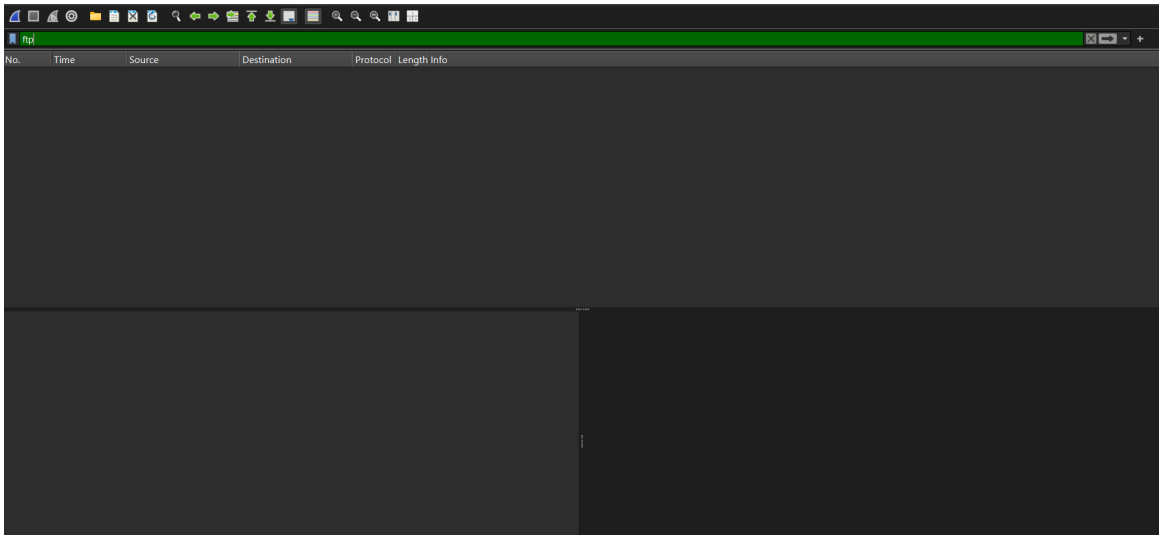
- **dns – Shows only DNS traffic**



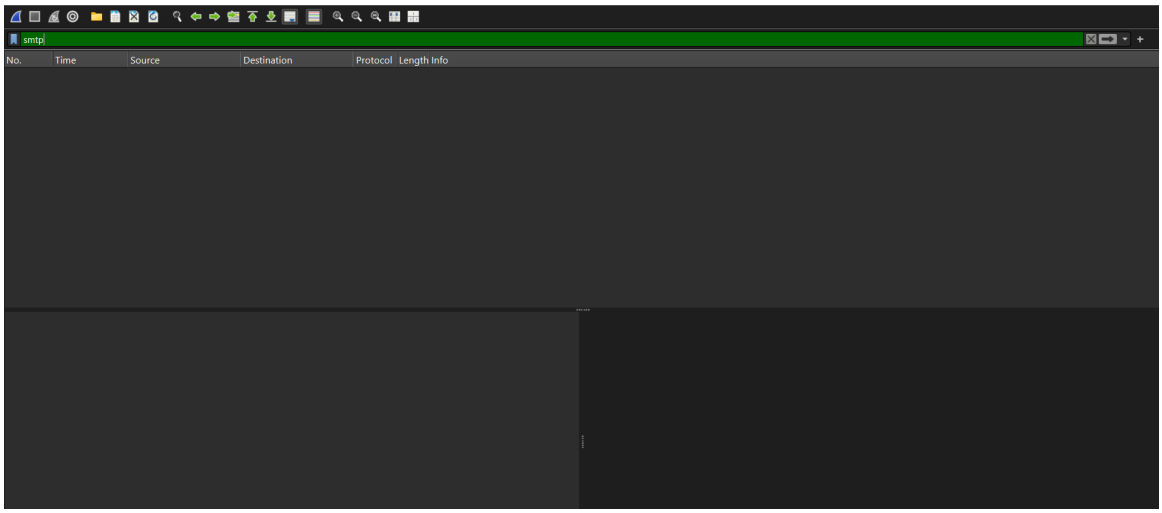
- **icmp – Filters ICMP packets (e.g., ping)**



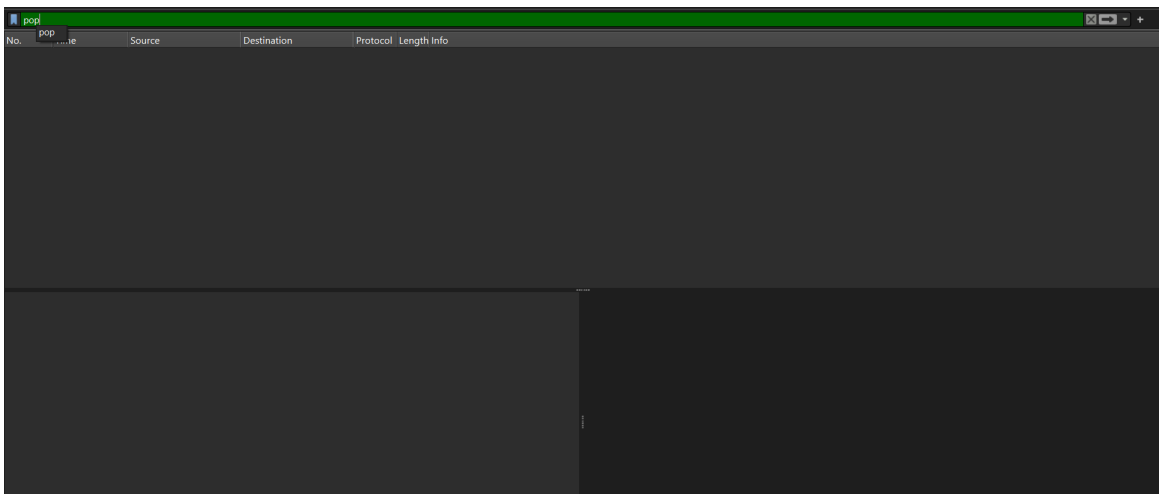
- **ftp – Filters FTP traffic**



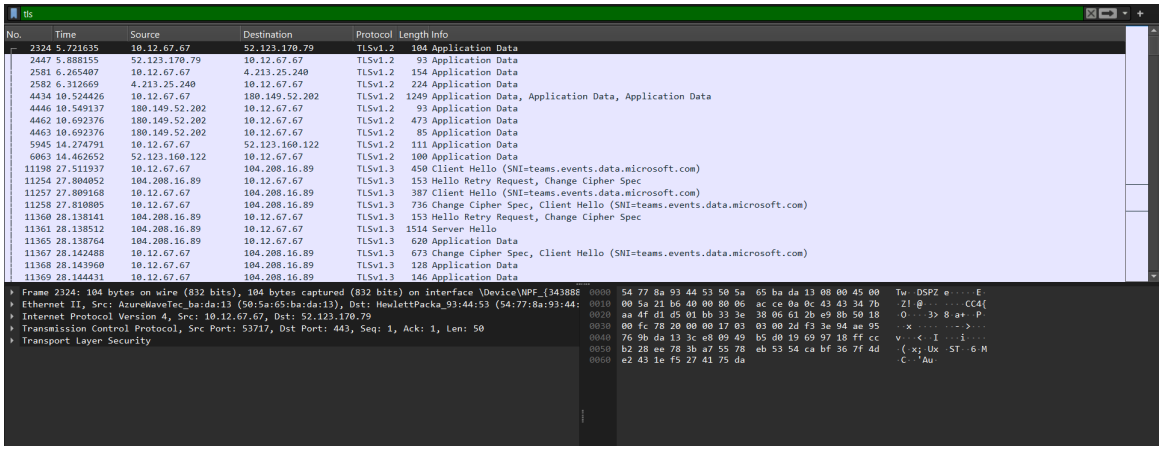
- **smtp – Filters SMTP (email sending)**



- **pop – Filters POP3 (email receiving)**

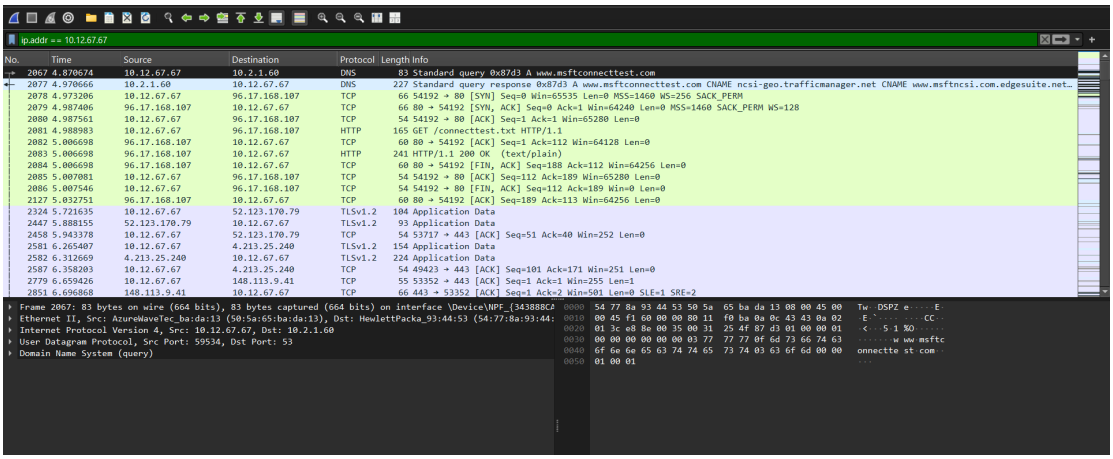


- **tls or ssl – Filters encrypted traffic (HTTPS)**

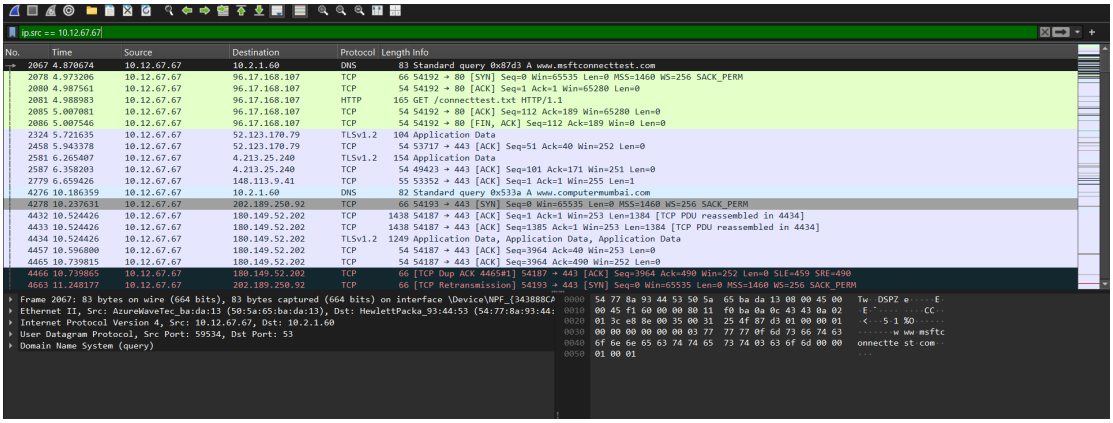


2. IP Address Filters

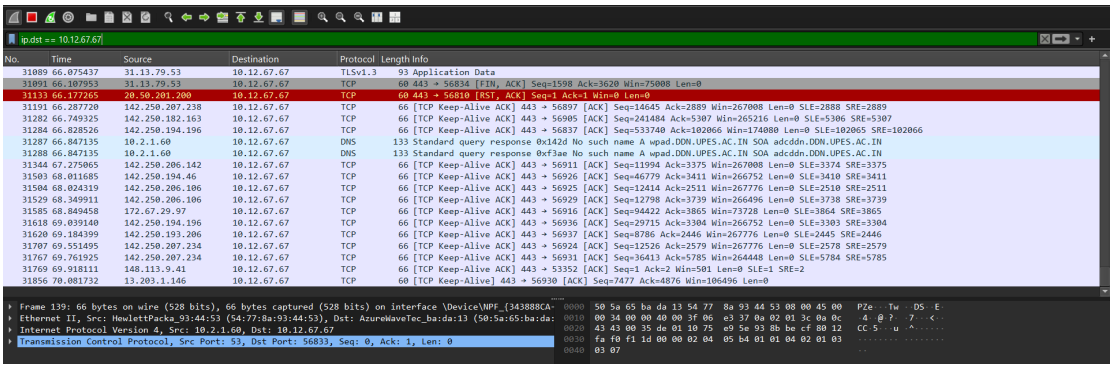
- **ip.addr == 192.168.1.1 – Shows all traffic to/from a specific IP**



- **ip.src == 192.168.1.1 – Traffic from a specific IP**

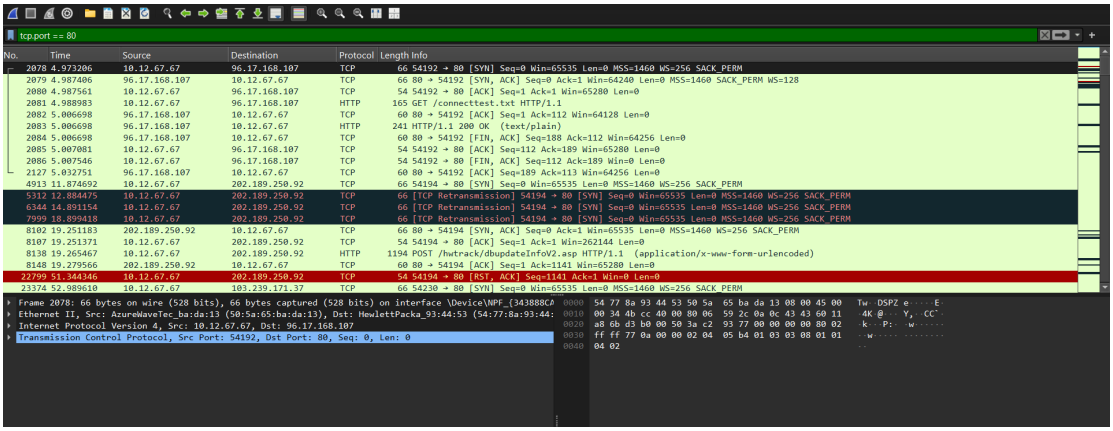


- **ip.dst == 8.8.8.8 – Traffic to a specific IP**

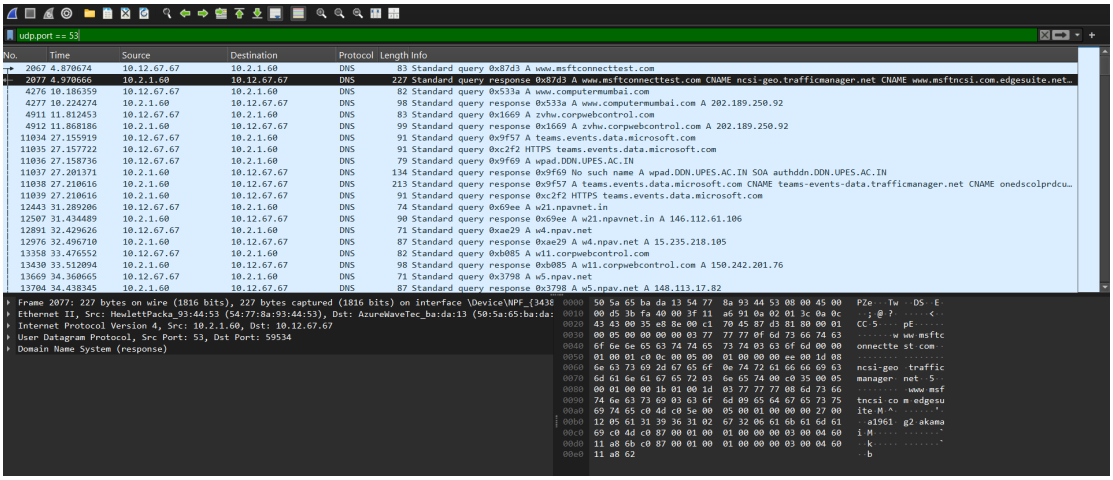


3. Port Filters

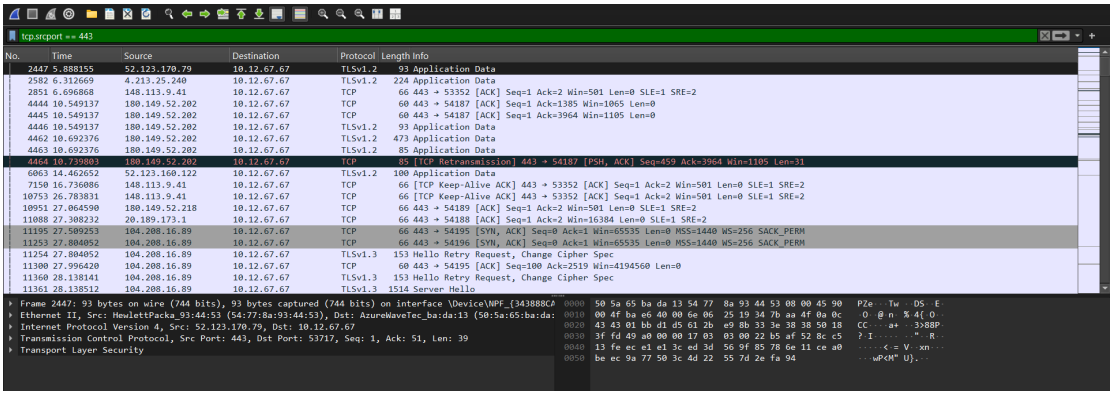
- **tcp.port == 80 – Shows HTTP traffic on port 80**



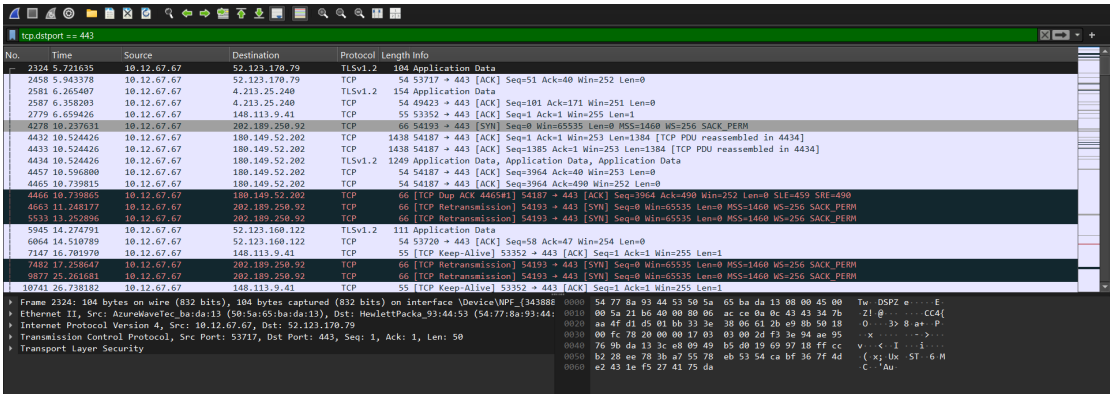
- **udp.port == 53 – Shows DNS traffic over UDP**



- **tcp.srcport == 443 – HTTPS traffic from server**

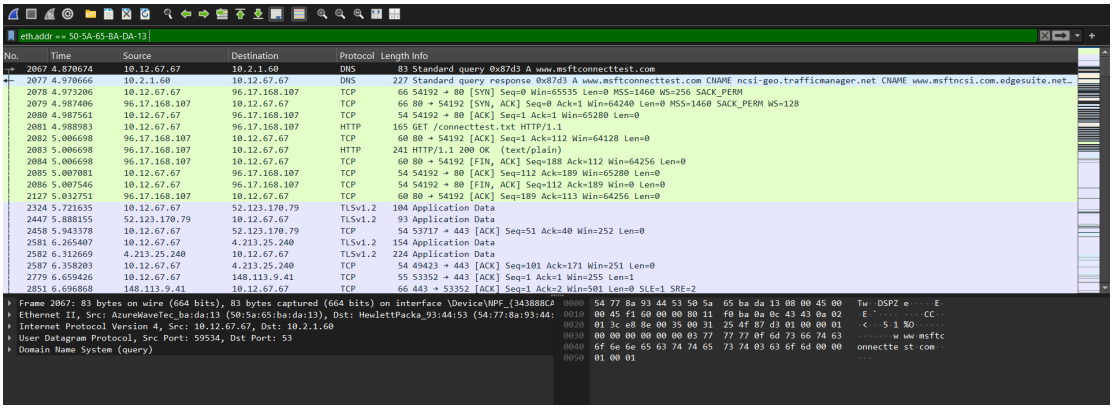


- **tcp.dstport == 443 – HTTPS traffic to server**

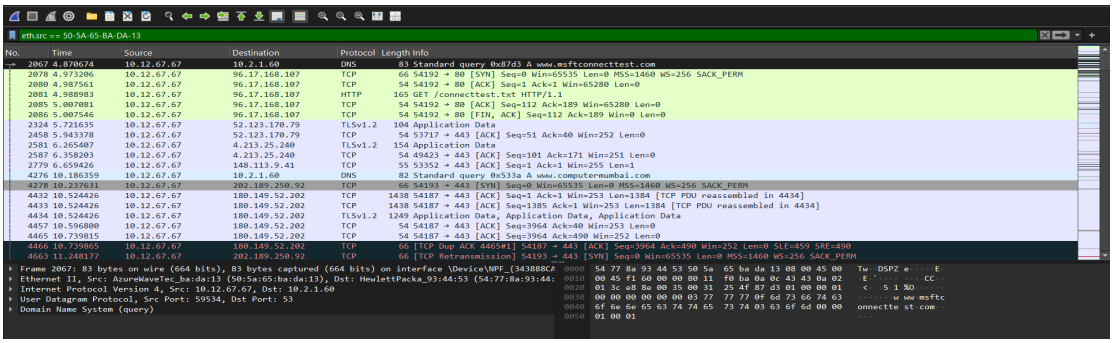


4. **MAC Address Filters**

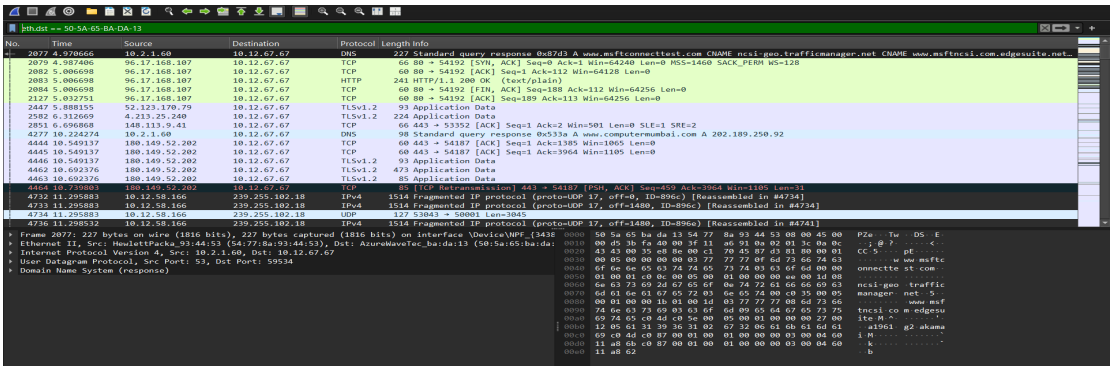
- **eth.addr == 00:11:22:33:44:55 – Traffic to/from a specific MAC address**



- **eth.src == 00:11:22:33:44:55 – Traffic from MAC**

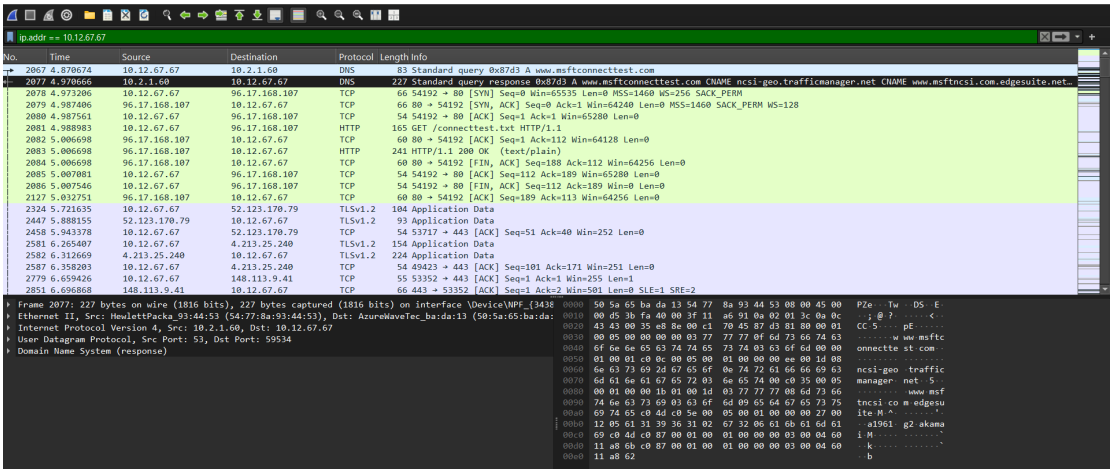


- **eth.dst == 00:11:22:33:44:55 – Traffic to MAC**



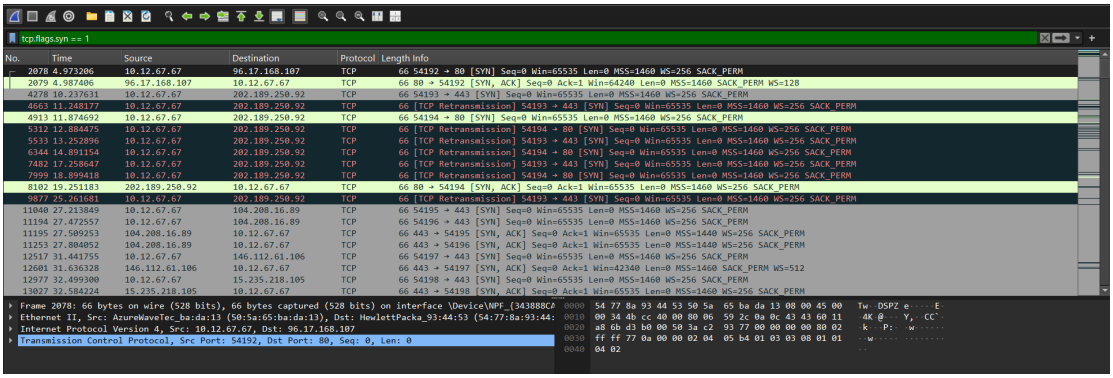
5. **Network Filters**

- **ip.addr == 192.168.0.0/24 – Traffic within a subnet**

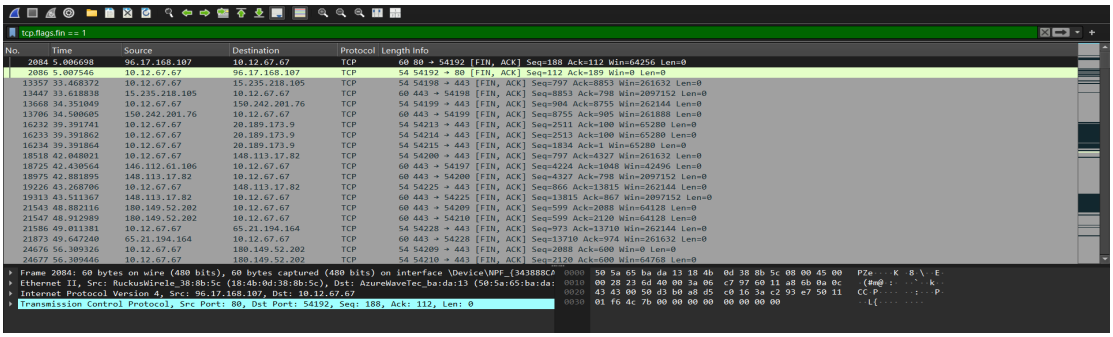


6. TCP Flags

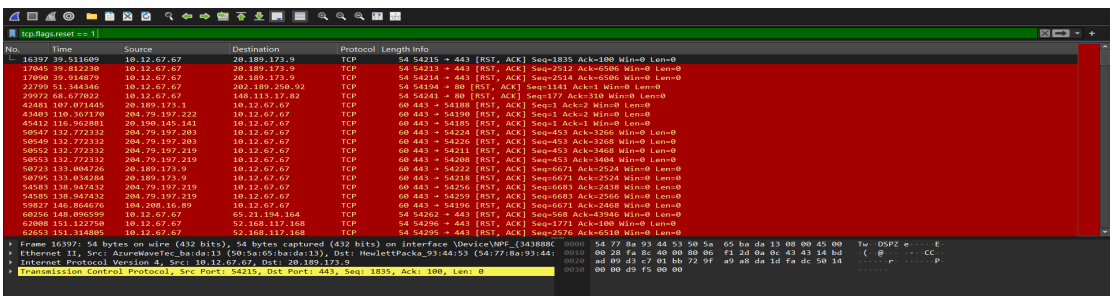
- **tcp.flags.syn == 1 – SYN packets (start of TCP handshake)**



- **tcp.flags.fin == 1 – FIN packets (end of session)**

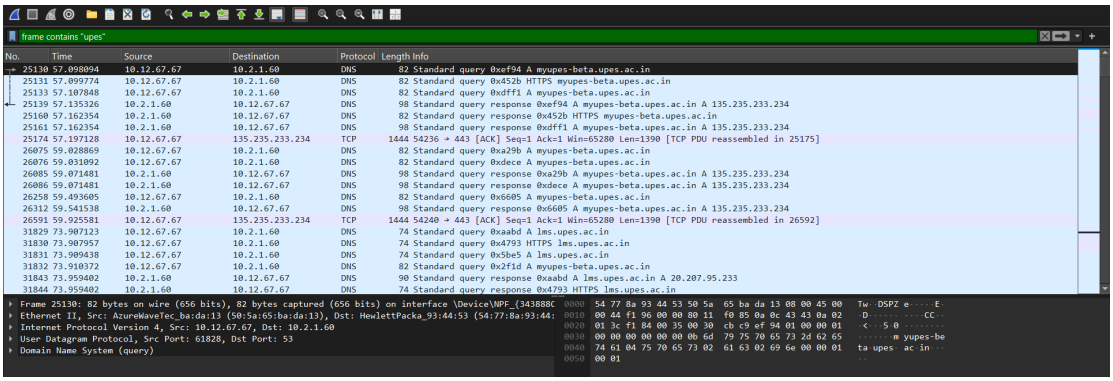


- **tcp.flags.reset == 1 – RST packets (reset connection)**

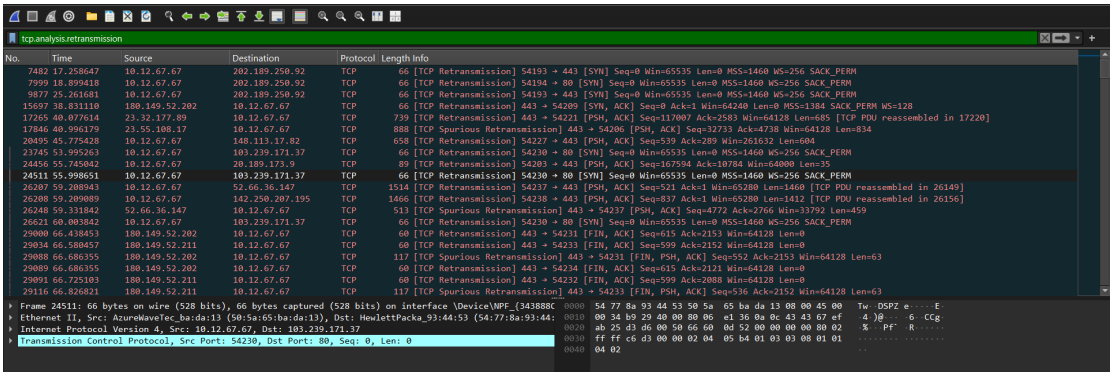


7. Other Useful Filters

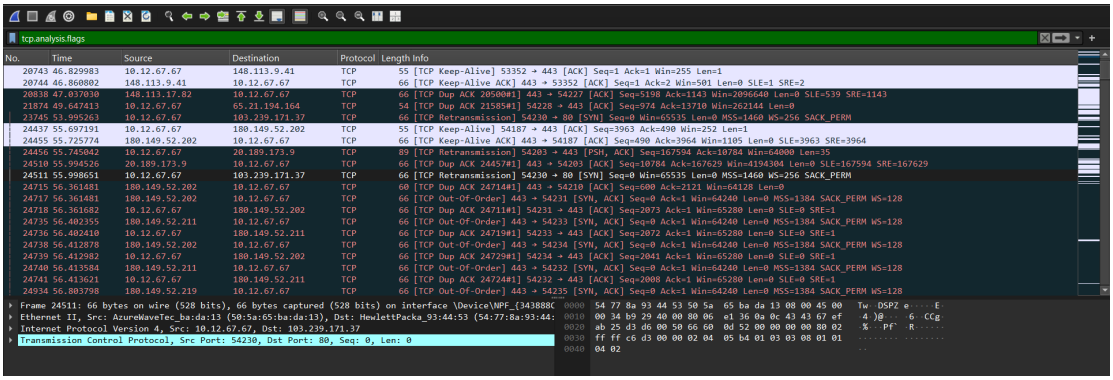
- **frame contains "text" – Packets containing specific text**



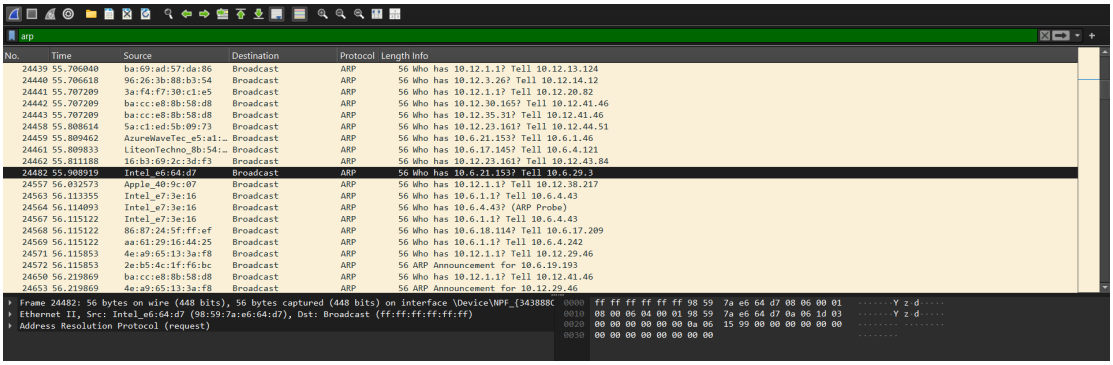
- **tcp.analysis.retransmission – Shows retransmitted packets**



- **tcp.analysis.flags – Flags abnormal TCP behavior**



- **arp – Filters ARP requests/replies**


arp
No. Time Source Destination Protocol Length Info
24439 55.706040 ba:69:ad:57:da:86 Broadcast ARP 56 Who has 10.12.1.1? Tell 10.12.13.124
24440 55.706618 96:26:3b:88:b3:54 Broadcast ARP 56 Who has 10.12.3.26? Tell 10.12.14.12
24441 55.707209 3a:f4:f7:30:c1:e5 Broadcast ARP 56 Who has 10.12.1.1? Tell 10.12.20.82
24442 55.707209 ba:cc:e8:8b:58:d8 Broadcast ARP 56 Who has 10.12.30.165? Tell 10.12.41.46
24443 55.707209 ba:cc:e8:8b:58:d8 Broadcast ARP 56 Who has 10.12.35.31? Tell 10.12.41.46
24458 55.808614 5a:c1:ed:5b:09:73 Broadcast ARP 56 Who has 10.12.23.161? Tell 10.12.44.51
24459 55.809462 AzureWaveTec_e5:a1:… Broadcast ARP 56 Who has 10.6.21.153? Tell 10.6.1.46
24461 55.809833 LiteonTechno_8b:54:… Broadcast ARP 56 Who has 10.6.17.145? Tell 10.6.4.121
24462 55.811188 16:b3:69:2c:3d:f3 Broadcast ARP 56 Who has 10.12.23.161? Tell 10.12.43.84
24482 55.908919 Intel_e6:64:d7 Broadcast ARP 56 Who has 10.6.21.153? Tell 10.6.29.3
24557 56.032573 Apple_40:9c:07 Broadcast ARP 56 Who has 10.12.1.1? Tell 10.12.38.217
24563 56.113355 Intel_e7:3e:16 Broadcast ARP 56 Who has 10.6.1.1? Tell 10.6.4.43
24564 56.114093 Intel_e7:3e:16 Broadcast ARP 56 Who has 10.6.4.43? (ARP Probe)
24567 56.115122 Intel_e7:3e:16 Broadcast ARP 56 Who has 10.6.1.1? Tell 10.6.4.43
24568 56.115122 86:87:24:5f:ff:ef Broadcast ARP 56 Who has 10.6.18.114? Tell 10.6.17.209
24569 56.115122 aa:61:29:16:44:25 Broadcast ARP 56 Who has 10.6.1.1? Tell 10.6.4.242
24571 56.115853 4e:a9:65:13:3a:f8 Broadcast ARP 56 Who has 10.12.1.1? Tell 10.12.29.46
24572 56.115853 2e:b5:4c:1f:f6:bc Broadcast ARP 56 ARP Announcement for 10.6.19.193
24650 56.219869 ba:cc:e8:8b:58:d8 Broadcast ARP 56 Who has 10.12.1.1? Tell 10.12.41.46
24653 56.219869 4e:a9:65:13:3a:f8 Broadcast ARP 56 ARP Announcement for 10.12.29.46
Frame 24482: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{343888C
Ethernet II, Src: Intel_e6:64:d7 (98:59:7a:e6:64:d7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 98 59 7a e6 64 d7 08 06 00 01 ·····Y z·d·····
0010 08 00 06 04 00 01 98 59 7a e6 64 d7 0a 06 1d 03 ·····Y z·d·····
0020 00 00 00 00 00 00 0a 06 15 99 00 00 00 00 00 00 ···· ····
0030 00 00 00 00 00 00 00 00 ····