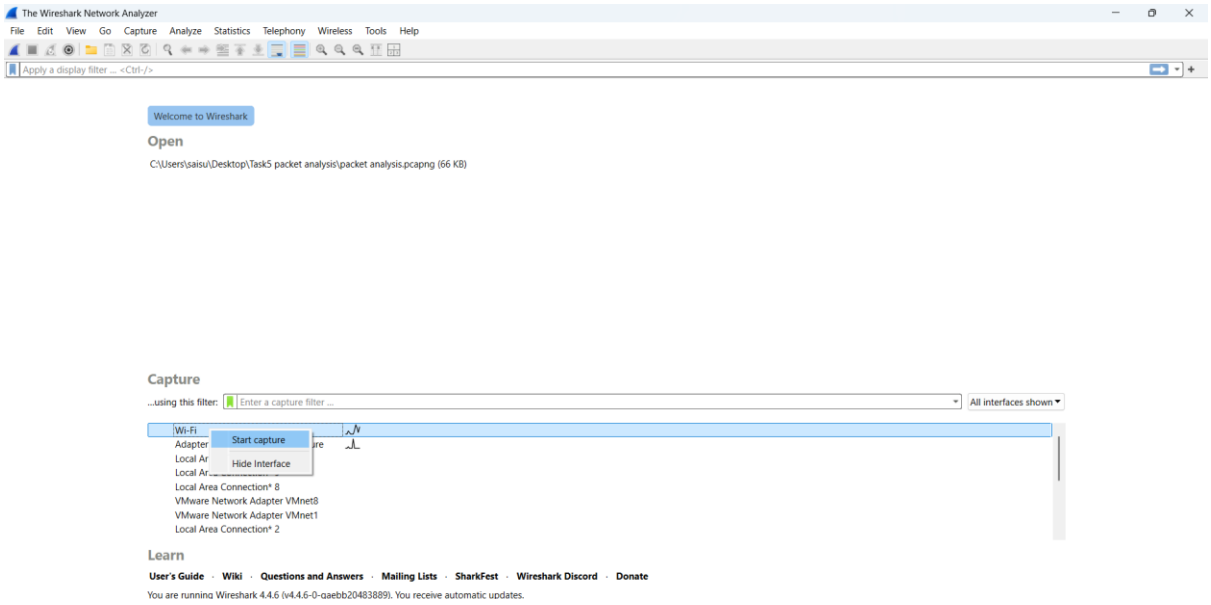
TASK 5 - Packet Capture using Wireshark

Wireshark

1. Click on the Wi-Fi tab below after opening the Wireshark tool



2. Open the command prompt and ping any domain of your choice

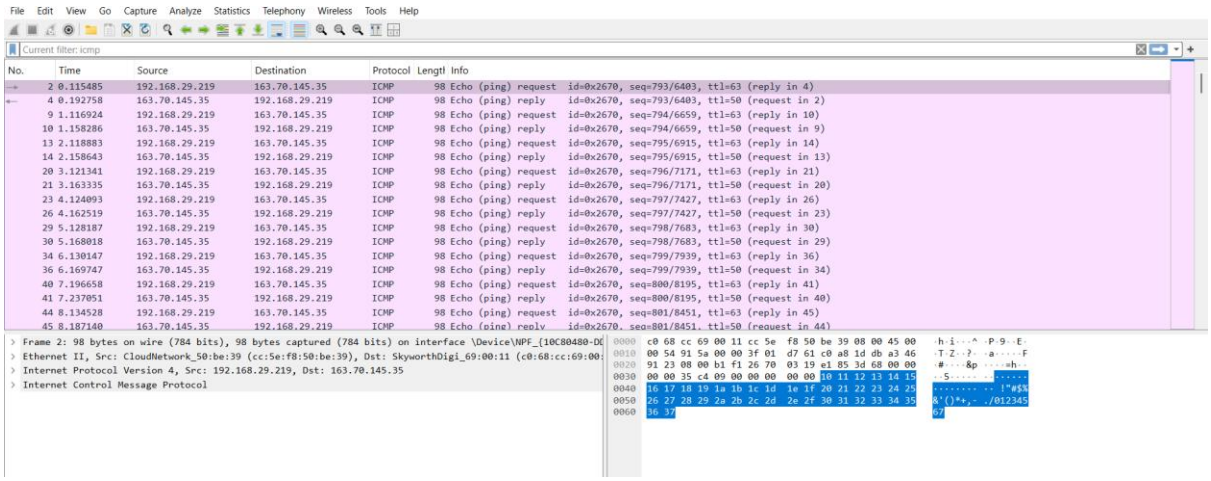
```
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\saisu> ping www.google.com

Pinging www.google.com [2404:6800:4002:817::2004] with 32 bytes of data:
Reply from 2404:6800:4002:817::2004: time=47ms
Reply from 2404:6800:4002:817::2004: time=48ms
Reply from 2404:6800:4002:817::2004: time=77ms
Reply from 2404:6800:4002:817::2004: time=79ms

Ping statistics for 2404:6800:4002:817::2004:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 47ms, Maximum = 79ms, Average = 62ms
PS C:\Users\saisu> ping www.facebook.com

Pinging star-mini.c10r.facebook.com [2a03:2880:f33d:1:face:b00c:0:25de] with 32 bytes of data:
Reply from 2a03:2880:f33d:1:face:b00c:0:25de: time=18ms
Reply from 2a03:2880:f33d:1:face:b00c:0:25de: time=17ms
Reply from 2a03:2880:f33d:1:face:b00c:0:25de: time=34ms
Reply from 2a03:2880:f33d:1:face:b00c:0:25de: time=34ms

Ping statistics for 2a03:2880:f33d:1:face:b00c:0:25de:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 34ms, Average = 25ms
PS C:\Users\saisu> ping www.amazon.com

Pinging d3ag4hukkh62yn.cloudfront.net [2600:9000:264e:7c00:7:49a5:5fd4:b121] with 32 bytes of data:
Reply from 2600:9000:264e:7c00:7:49a5:5fd4:b121: time=13ms
Reply from 2600:9000:264e:7c00:7:49a5:5fd4:b121: time=32ms
Reply from 2600:9000:264e:7c00:7:49a5:5fd4:b121: time=31ms
Reply from 2600:9000:264e:7c00:7:49a5:5fd4:b121: time=31ms

Ping statistics for 2600:9000:264e:7c00:7:49a5:5fd4:b121:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 13ms, Maximum = 32ms, Average = 26ms
PS C:\Users\saisu>
```

3. All the packets are captured by the Wireshark tool

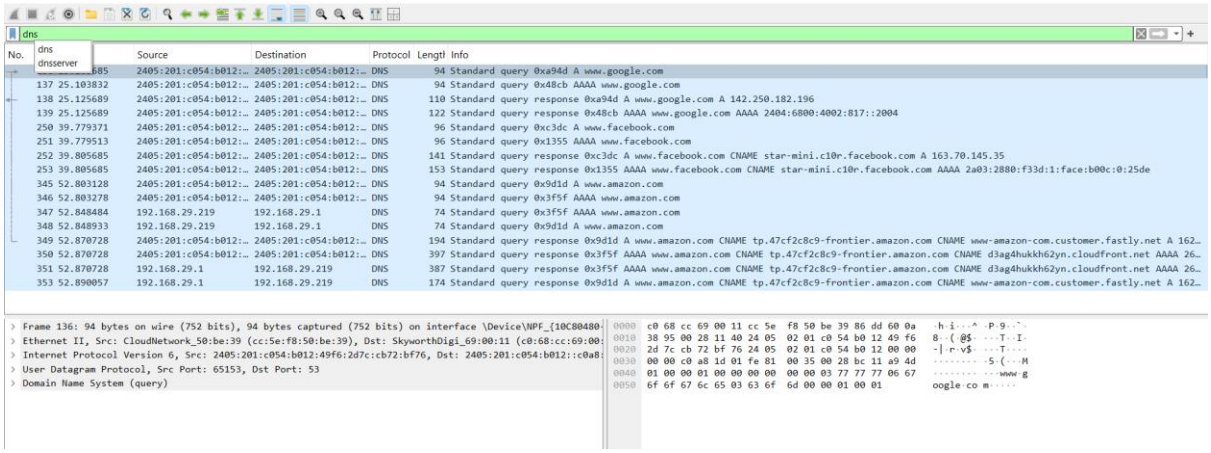
4. Stop the capture and save the file

Packet Analysis

1. Open the saved Wireshark file to analyze the packets

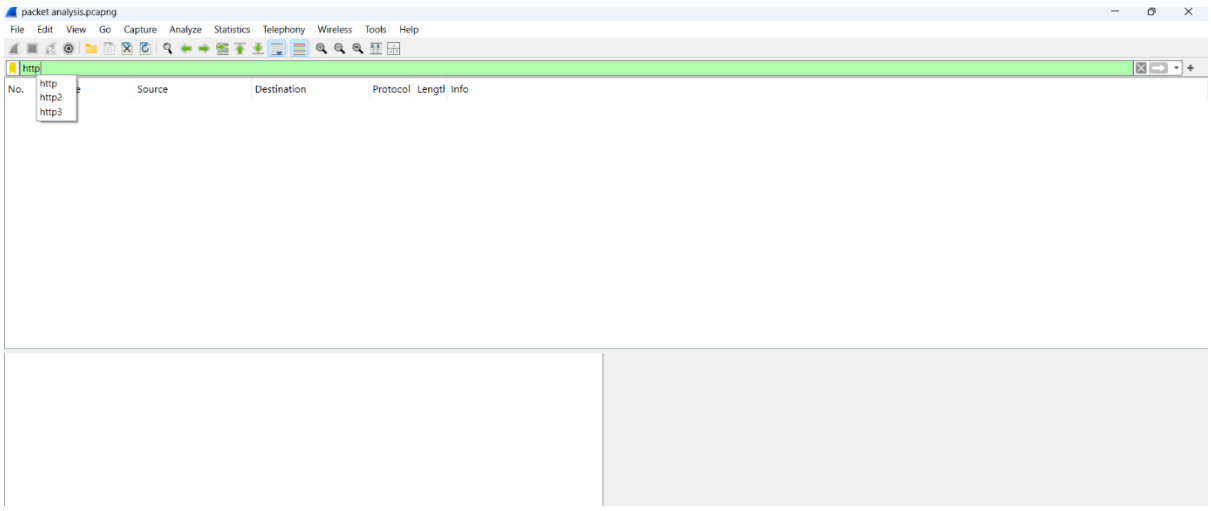


2. Filtered the packets with **DNS** protocol

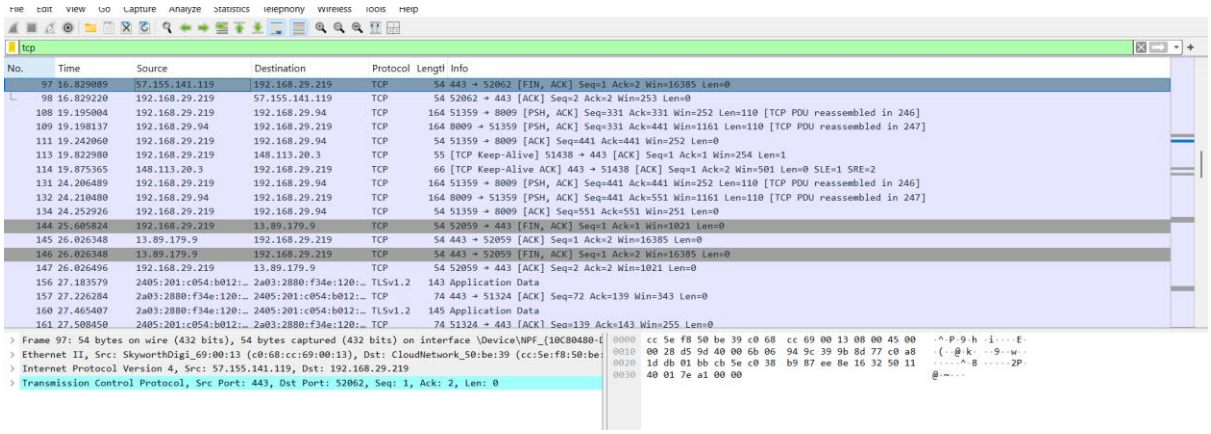


3. There are packets with DNS queries sent for each domain that are pinged using command prompt and the respective response

4. Let us filter the **HTTP** packets from the saved file

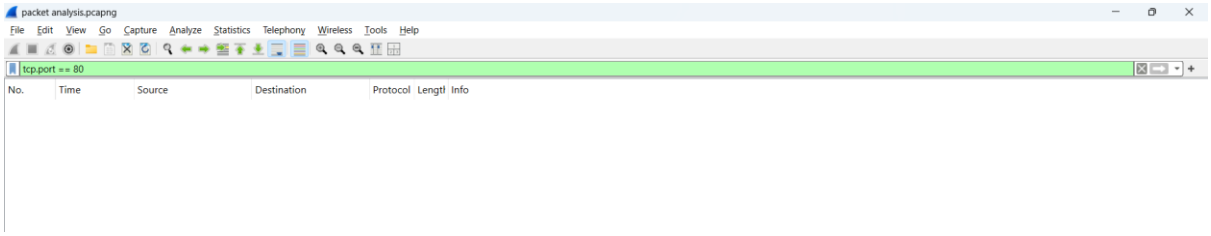


5. Filtering the packets with **TCP** protocol

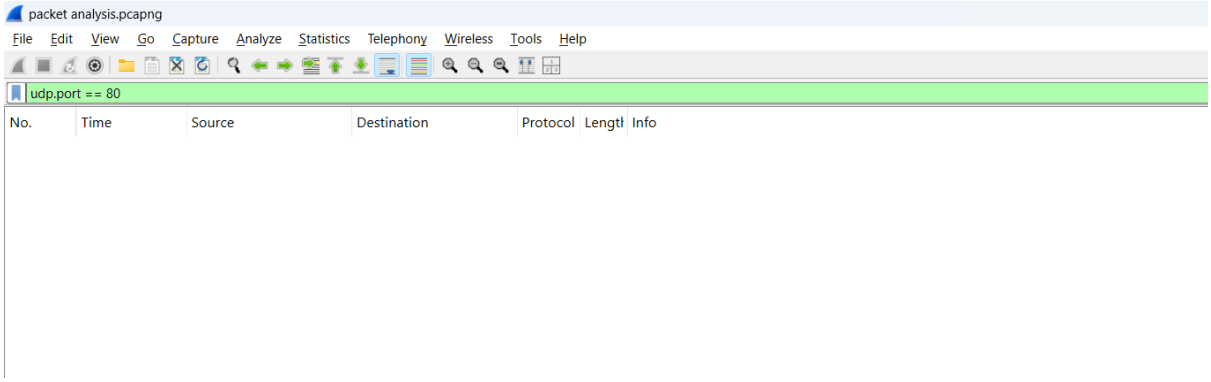


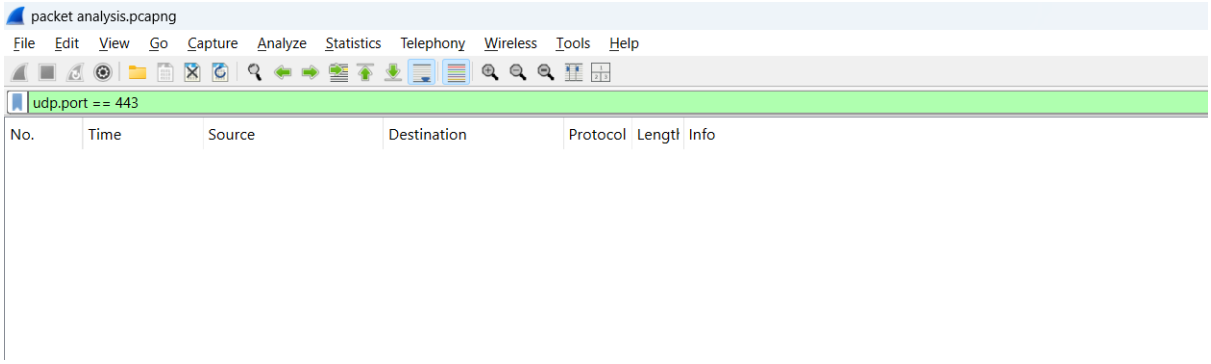
6. In this capture, we can also look at the port numbers associated with the protocol. Port number 443 indicates that it uses a secure communication method

7. We can also filter protocols along with port numbers. There are no port numbers **80** in the captured packets

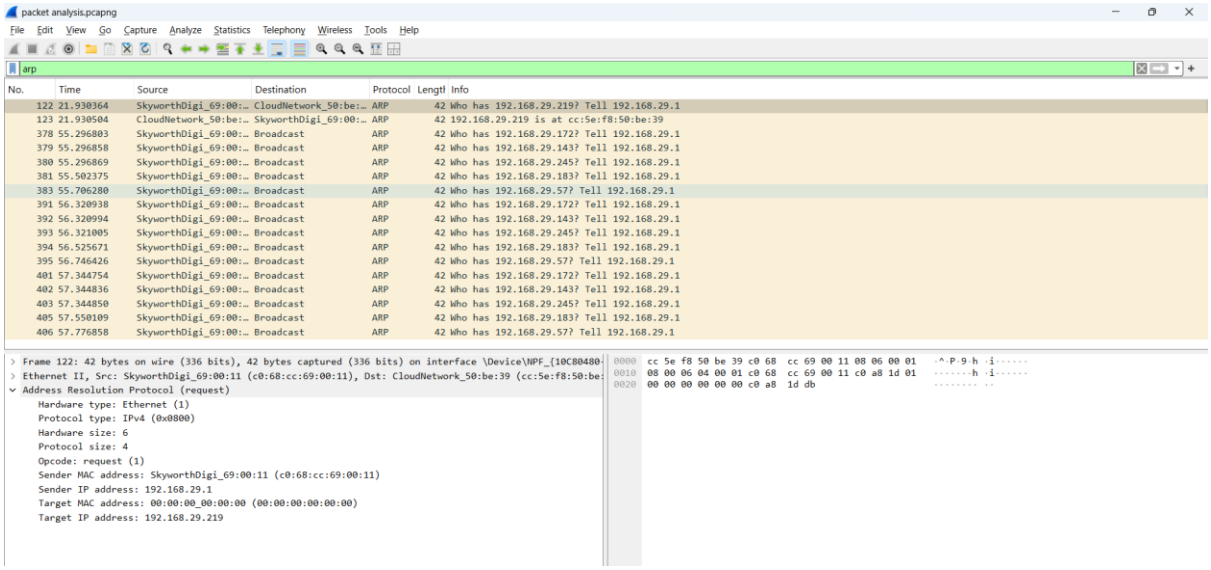


8. Let us try using the **UDP** protocol with port numbers **80** and **443**





9. In the filter below for **ARP**, we can see the broadcast request asking for the corresponding MAC address to the known IP address



I captured 433 packets in 1 minute. The top protocols observed were TCP, DNS, UDP.