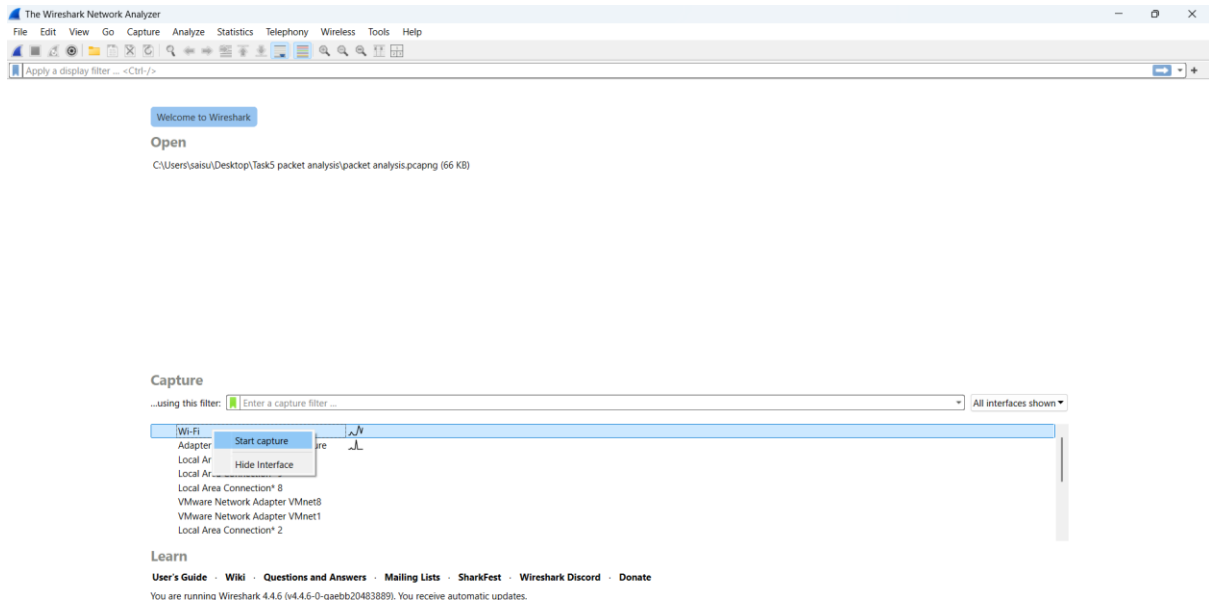


## TASK 5 - Packet Capture using Wireshark

### 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

No.	Time	Source	Destination	Protocol	Length	Info
2	0.115485	192.168.29.219	163.70.145.35	ICMP	98	Echo (ping) request id=0x2670, seq=793/6403, ttl=63 (reply in 4)
4	0.192758	163.70.145.35	192.168.29.219	ICMP	98	Echo (ping) reply id=0x2670, seq=793/6403, ttl=50 (request in 2)
9	1.116924	192.168.29.219	163.70.145.35	ICMP	98	Echo (ping) request id=0x2670, seq=794/6659, ttl=63 (reply in 10)
10	1.158286	163.70.145.35	192.168.29.219	ICMP	98	Echo (ping) reply id=0x2670, seq=794/6659, ttl=50 (request in 9)
13	2.118883	192.168.29.219	163.70.145.35	ICMP	98	Echo (ping) request id=0x2670, seq=795/6915, ttl=63 (reply in 14)
14	2.158643	163.70.145.35	192.168.29.219	ICMP	98	Echo (ping) reply id=0x2670, seq=795/6915, ttl=50 (request in 13)
20	3.121341	192.168.29.219	163.70.145.35	ICMP	98	Echo (ping) request id=0x2670, seq=796/7171, ttl=63 (reply in 21)
21	3.163335	163.70.145.35	192.168.29.219	ICMP	98	Echo (ping) reply id=0x2670, seq=796/7171, ttl=50 (request in 20)
23	4.124093	192.168.29.219	163.70.145.35	ICMP	98	Echo (ping) request id=0x2670, seq=797/7427, ttl=63 (reply in 26)
26	4.162519	163.70.145.35	192.168.29.219	ICMP	98	Echo (ping) reply id=0x2670, seq=797/7427, ttl=50 (request in 23)
29	5.128187	192.168.29.219	163.70.145.35	ICMP	98	Echo (ping) request id=0x2670, seq=798/7683, ttl=63 (reply in 30)
30	5.168018	163.70.145.35	192.168.29.219	ICMP	98	Echo (ping) reply id=0x2670, seq=798/7683, ttl=50 (request in 29)
34	6.130147	192.168.29.219	163.70.145.35	ICMP	98	Echo (ping) request id=0x2670, seq=799/7939, ttl=63 (reply in 36)
36	6.169747	163.70.145.35	192.168.29.219	ICMP	98	Echo (ping) reply id=0x2670, seq=799/7939, ttl=50 (request in 34)
40	7.196658	192.168.29.219	163.70.145.35	ICMP	98	Echo (ping) request id=0x2670, seq=800/8195, ttl=63 (reply in 41)
41	7.237051	163.70.145.35	192.168.29.219	ICMP	98	Echo (ping) reply id=0x2670, seq=800/8195, ttl=50 (request in 40)
44	8.134528	192.168.29.219	163.70.145.35	ICMP	98	Echo (ping) request id=0x2670, seq=801/8451, ttl=63 (reply in 45)
45	8.187240	163.70.145.35	192.168.29.219	ICMP	98	Echo (ping) reply id=0x2670, seq=801/8451, ttl=50 (request in 44)

> Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface \Device\NPF{18C80480-D0} Ethernet II, Src: CloudNetwork\_50:be:39 (cc:se:f8:50:be:39), Dst: SkyworthDigi\_69:00:11 (c0:68:ccc:69:00:11) Internet Protocol Version 4, Src: 192.168.29.219, Dst: 163.70.145.35 Internet Control Message Protocol

## 2. Filtered the packets with DNS protocol

No.	Time	Source	Destination	Protocol	Length	Info
137	25.103832	2405:201:c054:b012::	2405:201:c054:b012::	DNS	94	Standard query 0xa94d A www.google.com
138	25.125689	2405:201:c054:b012::	2405:201:c054:b012::	DNS	94	Standard query response 0xa94d A www.google.com A 142.250.182.196
139	25.125689	2405:201:c054:b012::	2405:201:c054:b012::	DNS	122	Standard query response 0xa94d AAAA www.google.com AAAA 2404:6800:4002:817::2004
250	39.779371	2405:201:c054:b012::	2405:201:c054:b012::	DNS	96	Standard query 0xc3dc A www.facebook.com
251	39.779513	2405:201:c054:b012::	2405:201:c054:b012::	DNS	96	Standard query response 0xc3dc A www.facebook.com
252	39.805685	2405:201:c054:b012::	2405:201:c054:b012::	DNS	141	Standard query response 0xc3dc CNAME star-mini.c10r.facebook.com A 163.70.145.35
253	39.805685	2405:201:c054:b012::	2405:201:c054:b012::	DNS	153	Standard query response 0xc3dc AAAA www.facebook.com CNAME star-mini.c10r.facebook.com AAAA 2a03:2880:f33d:1:face:b00c:0:25de
345	52.803128	2405:201:c054:b012::	2405:201:c054:b012::	DNS	94	Standard query 0x9d1d A www.amazon.com
346	52.803278	2405:201:c054:b012::	2405:201:c054:b012::	DNS	94	Standard query response 0x9d1d A www.amazon.com
347	52.848484	192.168.29.219	192.168.29.1	DNS	74	Standard query 0x3f5f AAAA www.amazon.com
348	52.848933	192.168.29.219	192.168.29.1	DNS	74	Standard query response 0x3f5f AAAA www.amazon.com
349	52.870728	2405:201:c054:b012::	2405:201:c054:b012::	DNS	194	Standard query response 0x9d1d A www.amazon.com CNAME tp.47cf2c8c9-frontier.amazon.com CNAME www.amazon.com.customer.fastly.net A 162...
350	52.870728	2405:201:c054:b012::	2405:201:c054:b012::	DNS	397	Standard query response 0x3f5f AAAA www.amazon.com CNAME tp.47cf2c8c9-frontier.amazon.com CNAME d3agdhukkh62yn.cloudfront.net AAAA 26...
351	52.870728	192.168.29.1	192.168.29.219	DNS	387	Standard query response 0x3f5f AAAA www.amazon.com CNAME tp.47cf2c8c9-frontier.amazon.com CNAME d3agdhukkh62yn.cloudfront.net AAAA 26...
353	52.890057	192.168.29.1	192.168.29.219	DNS	174	Standard query response 0x9d1d A www.amazon.com CNAME tp.47cf2c8c9-frontier.amazon.com CNAME www.amazon.com.customer.fastly.net A 162...

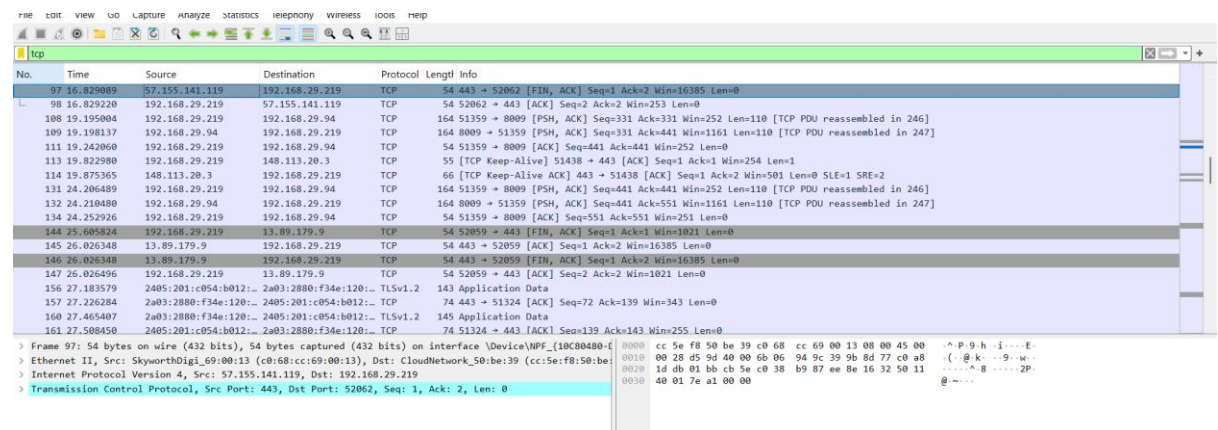
> Frame 136: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF{18C80480-D0} Ethernet II, Src: CloudNetwork\_50:be:39 (cc:se:f8:50:be:39), Dst: SkyworthDigi\_69:00:11 (c0:68:ccc:69:00:11) Internet Protocol Version 6, Src: 2405:201:c054:b012::49f6:2d7c:b7f6, Dst: 2405:201:c054:b012::c0a8 User Datagram Protocol, Src Port: 65153, Dst Port: 53 Domain Name System (query)

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

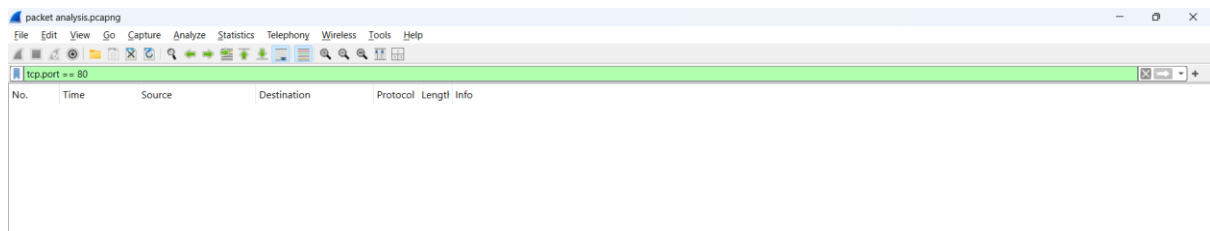
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.29.219	163.70.145.35	HTTP	100	GET / HTTP/1.1
2	0.000000	163.70.145.35	192.168.29.219	HTTP	100	200 OK
3	0.000000	192.168.29.219	163.70.145.35	HTTP	100	GET / HTTP/1.1
4	0.000000	163.70.145.35	192.168.29.219	HTTP	100	200 OK

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

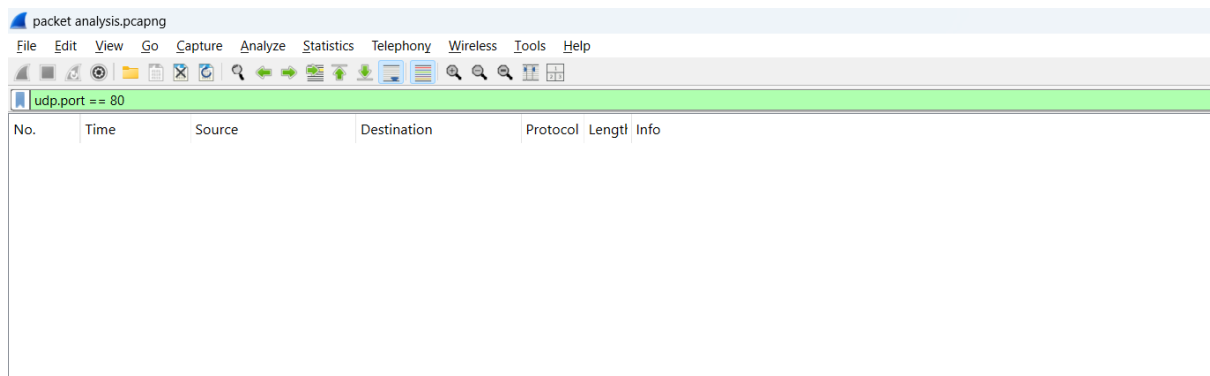


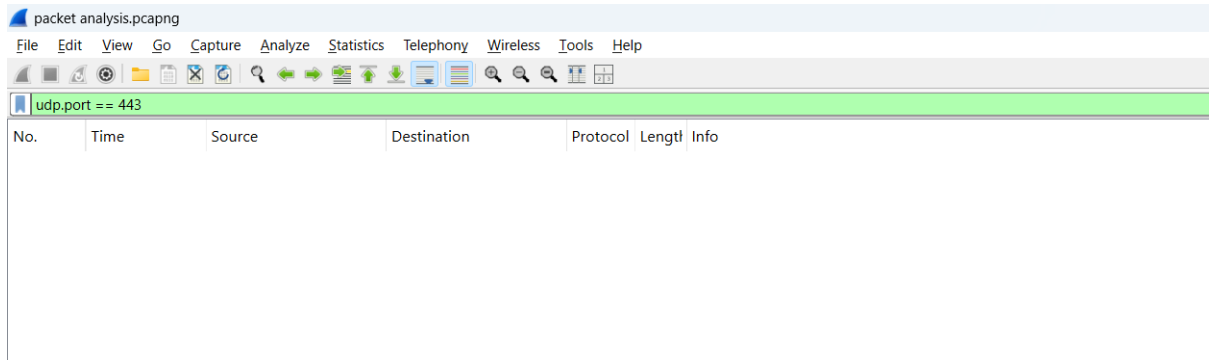
6. In this capture, we can also look at the port numbers associated with the protocol. Port number 443 indicates that it uses a secure communication method

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

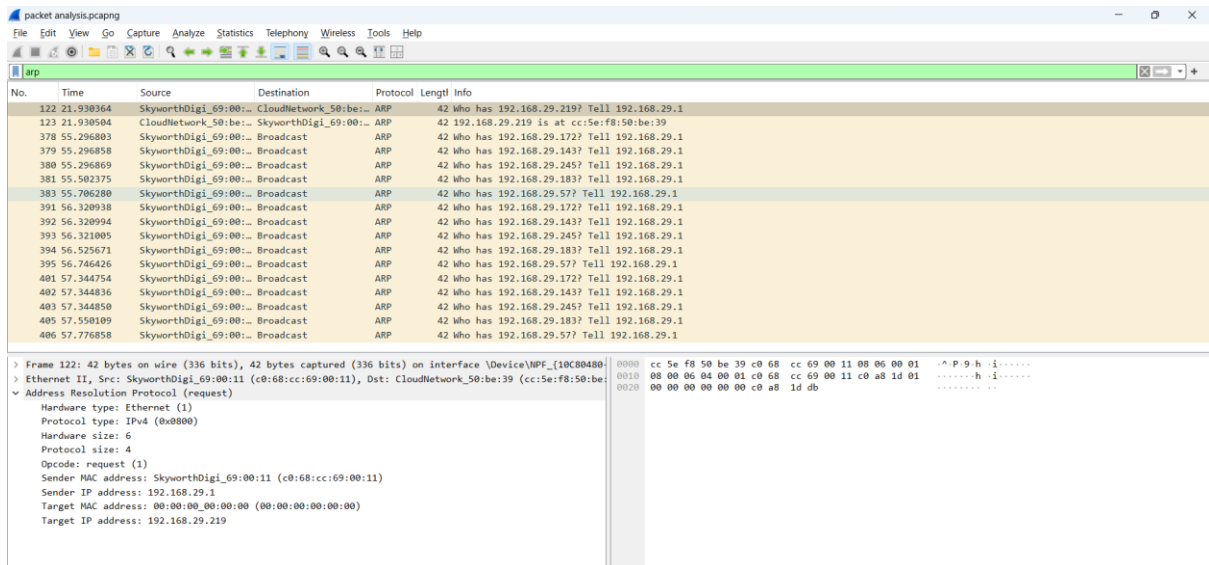


8. Let us try using the **UDP** protocol with port numbers **80** and **443**





- 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.