

Ex: No. 5

Aim: Experiments on packet capture tool: Wireshark.

Wireshark, a network analysis tool, captures packets in human-readable format. It includes filters, color coding and other features to dig deep into network traffic and dissect individual packets.

What we can do with wire shark

## Capture network traffic

Decode packet protocols using dissectors

Define fitters - capture and display

watch smart statistics

## Analyze problems

interactively ~~before~~ browse the traffic.

### Capturing packets:

Select the network interface under capture to start capturing packet on that interface. The interface could be Ethernet, wifi etc packets start to appear in real-time. Wireshark captures each packet sent to or from your system.

Run	Time	Source	Destination	Protocol	Length	Info
2070	10.230515	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.230515
2080	10.230600	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.230600
2090	10.230690	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.230690
2100	10.231000	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.231000
2110	10.231400	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.231400
2120	10.231500	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.231500
2130	10.231600	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.231600
2140	10.231700	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.231700
2150	10.231800	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.231800
2160	10.231900	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.231900
2170	10.232000	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.232000
2180	10.232100	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.232100
2190	10.232200	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.232200
2200	10.232300	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.232300
2210	10.232400	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.232400
2220	10.232500	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.232500
2230	10.232600	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.232600
2240	10.232700	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.232700
2250	10.232800	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.232800
2260	10.232900	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.232900
2270	10.233000	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.233000
2280	10.233100	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.233100
2290	10.233200	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.233200
2300	10.233300	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.233300
2310	10.233400	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.233400
2320	10.233500	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.233500
2330	10.233600	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.233600
2340	10.233700	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.233700
2350	10.233800	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.233800
2360	10.233900	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.233900
2370	10.234000	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.234000
2380	10.234100	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.234100
2390	10.234200	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.234200
2400	10.234300	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.234300
2410	10.234400	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.234400
2420	10.234500	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.234500
2430	10.234600	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.234600
2440	10.234700	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.234700
2450	10.234800	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.234800
2460	10.234900	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.234900
2470	10.235000	192.168.1.100	192.168.1.100	TCP	60	55 Syn/ack 10.235000
2480						

From 10.0.0.0 to 10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

Destination: 10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

Source: 10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

Info: 10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

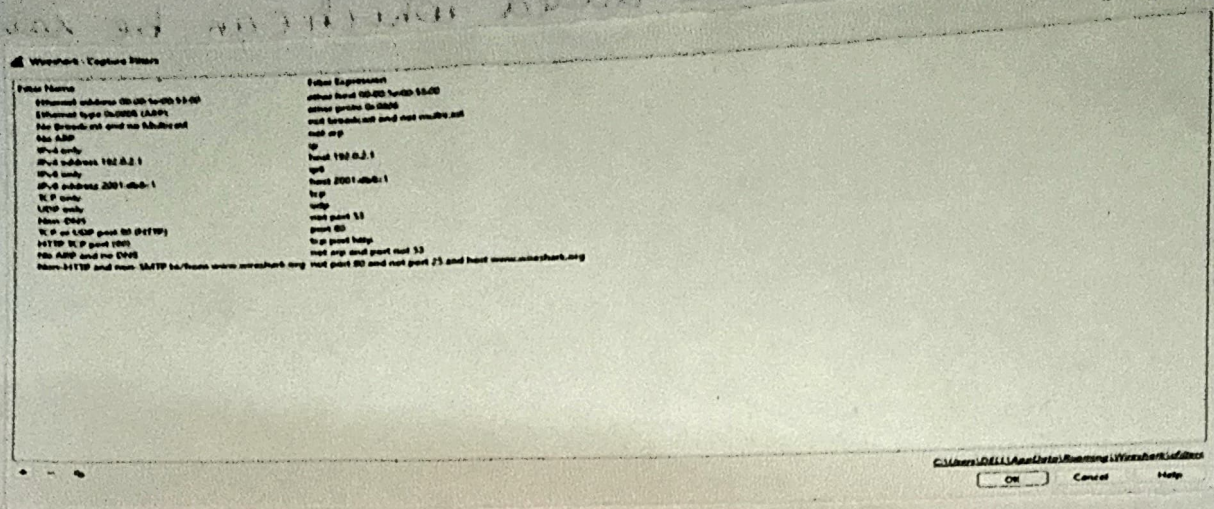
10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0.

10.0.0.0 (10.0.0.0 to 10.0.0.0). Both IP addresses are 10.0.0.0





~~CAP~~ The "Packet List" Pane

~~CAPP~~ The "Packet List" Pane  
The packet list pane display all the packets in the current capture file. Each line in the packet list corresponds to one packet in capture file. Selecting a line in this pane opens more details in the "Packets Details" and "Packet Bytes" panes.

## The "Packet Details" Pane

The "Packet Details" Pane  
The packet details pane shows the current selected packet in more detailed form. This pane shows the protocols and protocol field of packets selected in "Packet List" pane.

The "Packet Bytes" pane

The "Packet Bytes" pane shows the data of the current packets in a hexdump style.

Color coding:

color coding:  
wireshark uses colors to help you identify the types of traffic at glance - The colouring rules can also be customized and modified.

### Filtering Packets;

Filtering Packets;  
Wireshark's filters allow to narrow down the traffic to  
insert something specific. Basic way to apply filter is by  
typing it into the filter box. For example, type "tcp" and  
it will display only TCP packets.



Custom filter can also be added which can be saved for future life.

Time	Source	Destination
10.000000	Feder: 197.16.74.100	224.0.0.0
11.000000	Feder: 197.16.74.100	224.0.0.0
12.000000	Feder: 197.16.74.100	224.0.0.0
13.000000	Feder: 197.16.74.100	224.0.0.0
14.000000	Feder: 197.16.74.100	224.0.0.0
15.000000	Feder: 197.16.74.100	224.0.0.0
16.000000	Feder: 197.16.74.100	224.0.0.0
17.000000	Feder: 197.16.74.100	224.0.0.0
18.000000	Feder: 197.16.74.100	224.0.0.0
19.000000	Feder: 197.16.74.100	224.0.0.0
20.000000	Feder: 197.16.74.100	224.0.0.0
21.000000	Feder: 197.16.74.100	224.0.0.0
22.000000	Feder: 197.16.74.100	224.0.0.0
23.000000	Feder: 197.16.74.100	224.0.0.0
24.000000	Feder: 197.16.74.100	224.0.0.0
25.000000	Feder: 197.16.74.100	224.0.0.0
26.000000	Feder: 197.16.74.100	224.0.0.0
27.000000	Feder: 197.16.74.100	224.0.0.0
28.000000	Feder: 197.16.74.100	224.0.0.0
29.000000	Feder: 197.16.74.100	224.0.0.0
30.000000	Feder: 197.16.74.100	224.0.0.0
31.000000	Feder: 197.16.74.100	224.0.0.0
32.000000	Feder: 197.16.74.100	224.0.0.0
33.000000	Feder: 197.16.74.100	224.0.0.0
34.000000	Feder: 197.16.74.100	224.0.0.0
35.000000	Feder: 197.16.74.100	224.0.0.0
36.000000	Feder: 197.16.74.100	224.0.0.0
37.000000	Feder: 197.16.74.100	224.0.0.0
38.000000	Feder: 197.16.74.100	224.0.0.0
39.000000	Feder: 197.16.74.100	224.0.0.0
40.000000	Feder: 197.16.74.100	224.0.0.0
41.000000	Feder: 197.16.74.100	224.0.0.0
42.000000	Feder: 197.16.74.100	224.0.0.0
43.000000	Feder: 197.16.74.100	224.0.0.0
44.000000	Feder: 197.16.74.100	224.0.0.0
45.000000	Feder: 197.16.74.100	224.0.0.0
46.000000	Feder: 197.16.74.100	224.0.0.0
47.000000	Feder: 197.16.74.100	224.0.0.0
48.000000	Feder: 197.16.74.100	224.0.0.0
49.000000	Feder: 197.16.74.100	224.0.0.0
50.000000	Feder: 197.16.74.100	224.0.0.0

## CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL

Capture 100 packets from the wifi interface and save it

procedure:

Select WIF1 in wine shark

Go to Capture  $\rightarrow$  option

Select step capture automatically after 100 packets

Then, click start capture

Save the packets.

1. create a Filter to display only ~~the~~ TCP packets

procedure

too ~~to~~ capture  $\rightarrow$  option

Select stop capture automatically after 100 packets

Then click start capture

Search TCP packets in search bar

Save the packets

[illegible]



Time	172.16.75.110	23.202.229.23	150.171.31.254	Comment
0.000000	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
0.000000	30079	Application Data	443	TLSV1.2: Application Data
0.000101	30079	80878 → 443 [ACK] Seq=3461 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=3461 Win=1020 Len=0
0.000101	30079	80878 → 443 [ACK] Seq=3461 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=3461 Win=1020 Len=0
0.000101	30079	80878 → 443 [ACK] Seq=3461 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=3461 Win=1020 Len=0
0.000101	30079	80878 → 443 [ACK] Seq=3461 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=3461 Win=1020 Len=0
0.000166	30079	Application Data	443	TLSV1.2: Application Data
0.004433	30079	Application Data	443	TLSV1.2: Application Data
0.004433	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
0.004433	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
0.004433	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
0.049957	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
0.124626	30079	Application Data	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
0.124626	30079	Application Data	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
0.124714	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
2.953823	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
2.953967	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
2.953984	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
2.954069	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
2.960845	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
2.960845	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
5.815813	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
5.815737	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
5.817745	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
5.817745	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
12.560972	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0
12.560972	30079	80878 → 443 [ACK] Seq=1001 Win=1020 Len=0	443	TCP: 80878 → 443 [ACK] Seq=1001 Win=1020 Len=0

we can follow the same strategy for displaying and inspecting other packets like ARP, HTTP, IP/ICMP, DHCP etc.

1. What is promiscuous mode?

A node where it captures all packets on the network instead of only the ones addressed in the network adapter.

2. Does ARP packets has transport layer header? Explain?

No, ARP packets doesn't contain; ARP works at the data link layer.

3. Which transport layer protocol is used by DNS?

DNS primarily uses UDP test uses TCP for large queries

4. What is port number used by HTTP protocol?

HTTP uses port number 80.

5. What is a broadcast IP address

An IP address used to send data to all hosts in a network.

Result: Hence the wire share experiment was successful