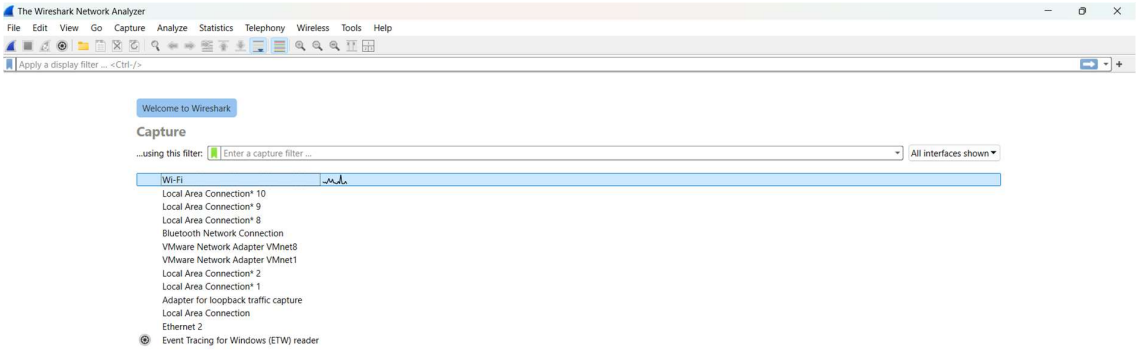
Reg.No.: 2116220701040

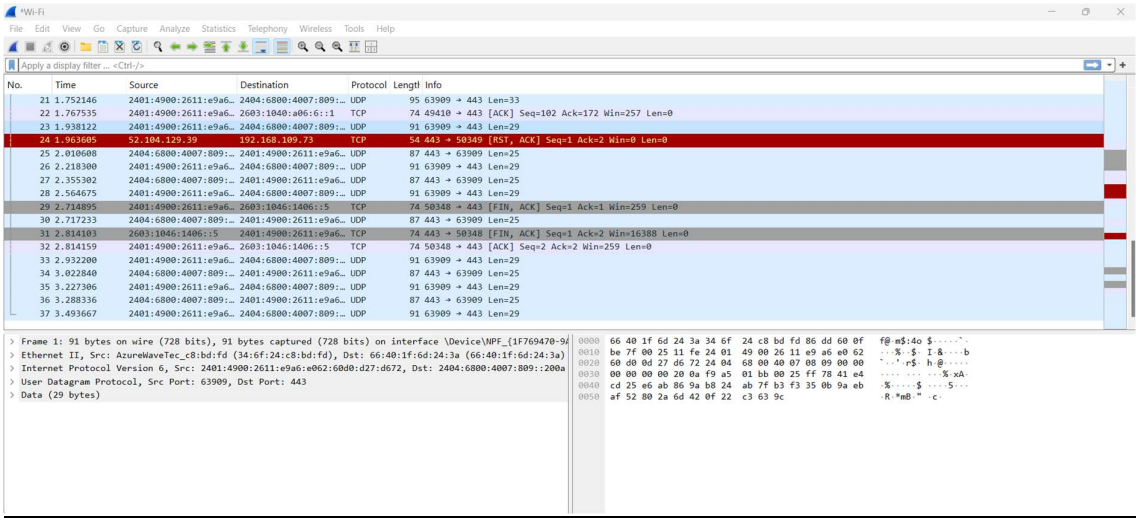
Practical 5

Aim:

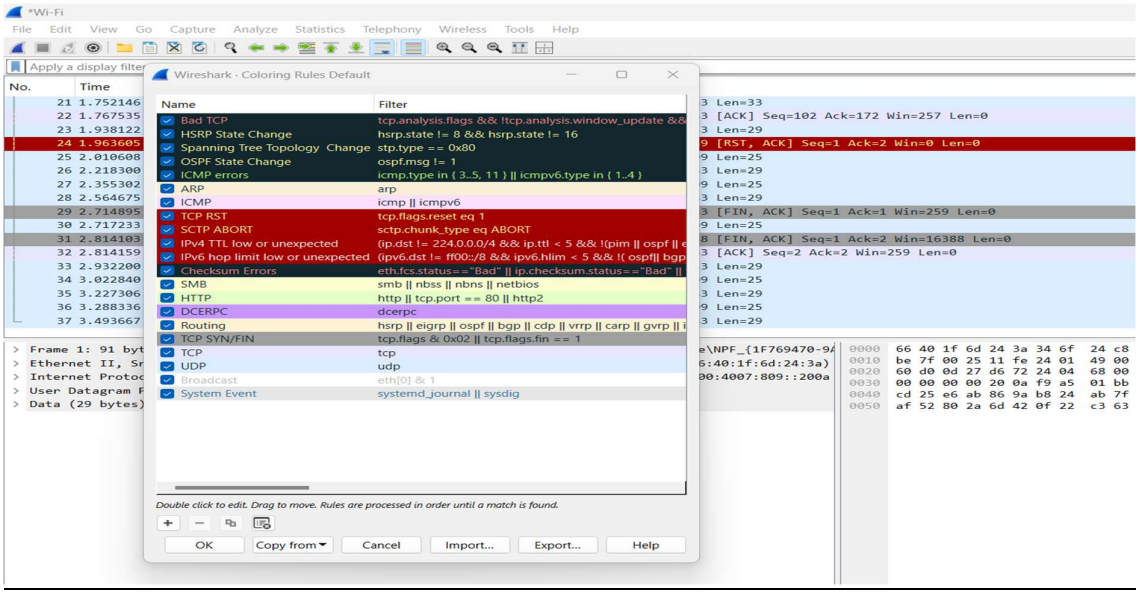
Experiments on Packet capture tool: Wireshark

Capturing Packets:

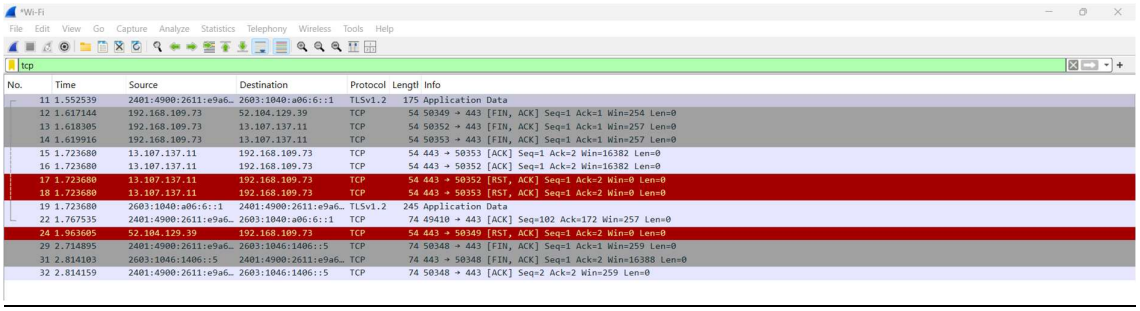




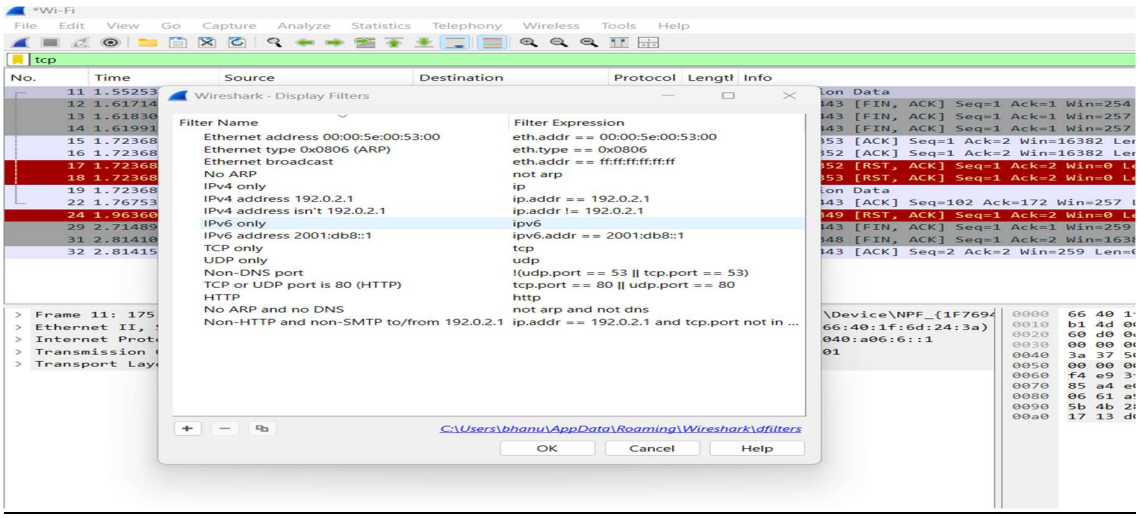
Color Coding:



Filtering Packets:

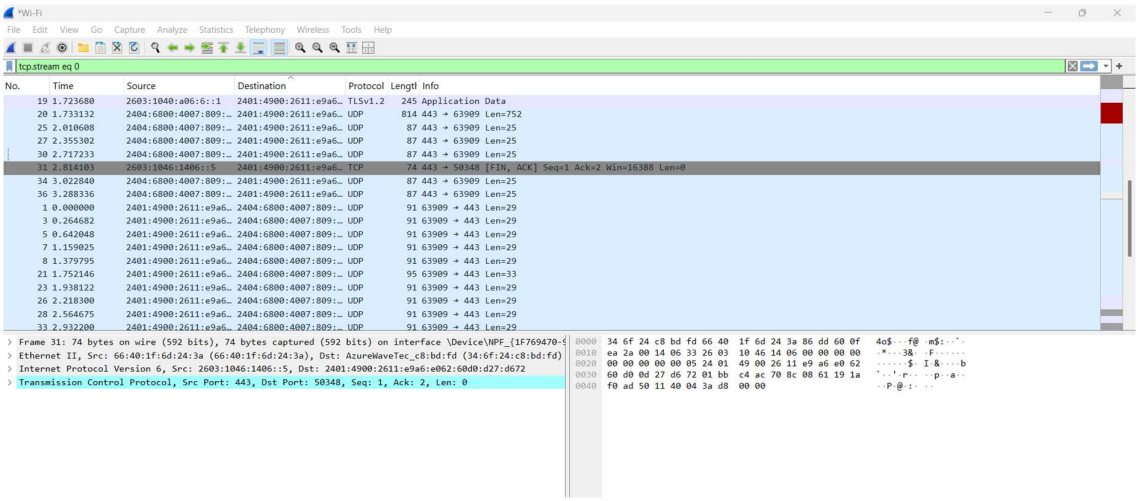


Display Filters:

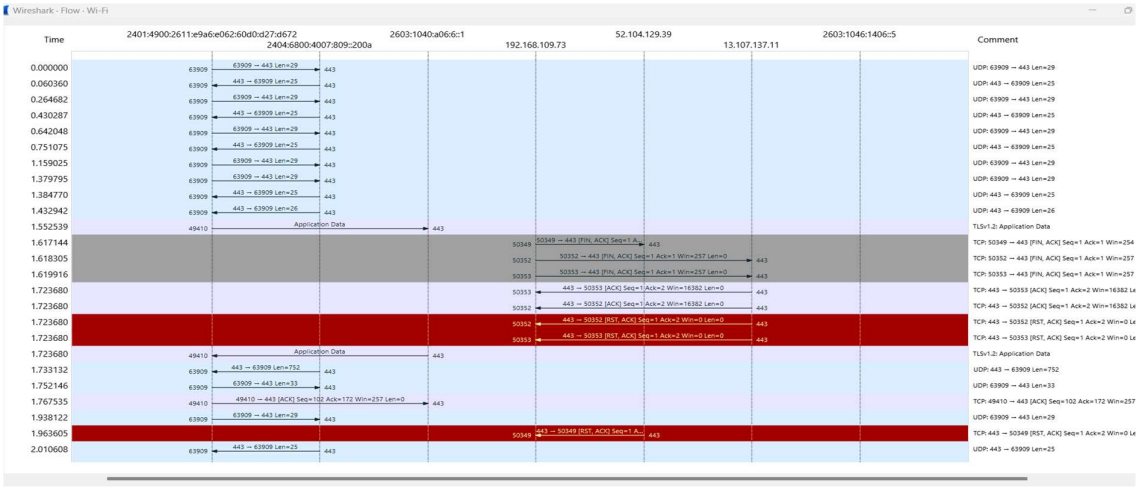


Tcp Stream:

Inspecting Packets:



Flow Graph:



1. Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph

Procedure

Select Local Area Connection in Wireshark.

Go to capture →option

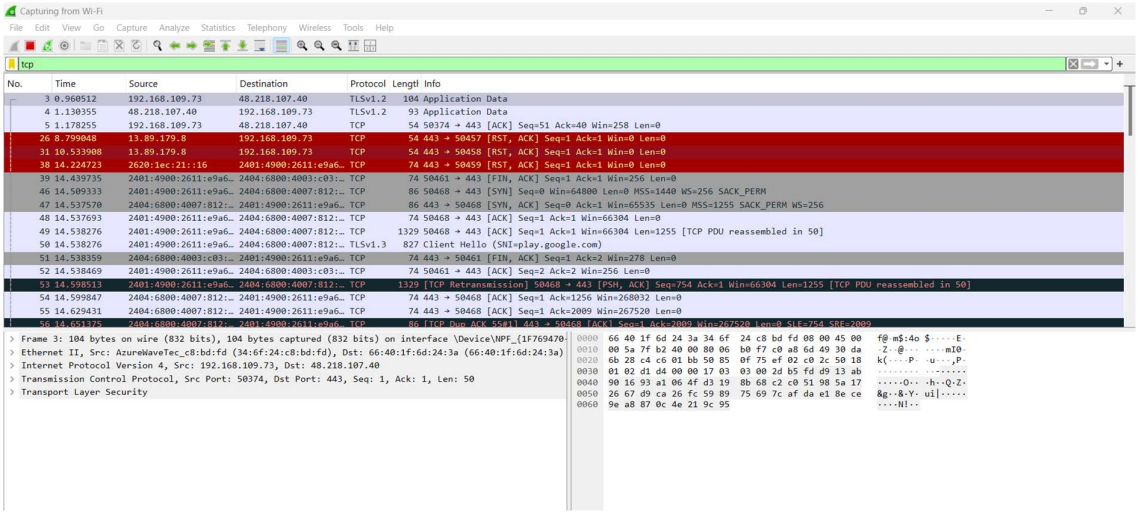
Select stop capture automatically after 100 packets.

Then click Start capture.

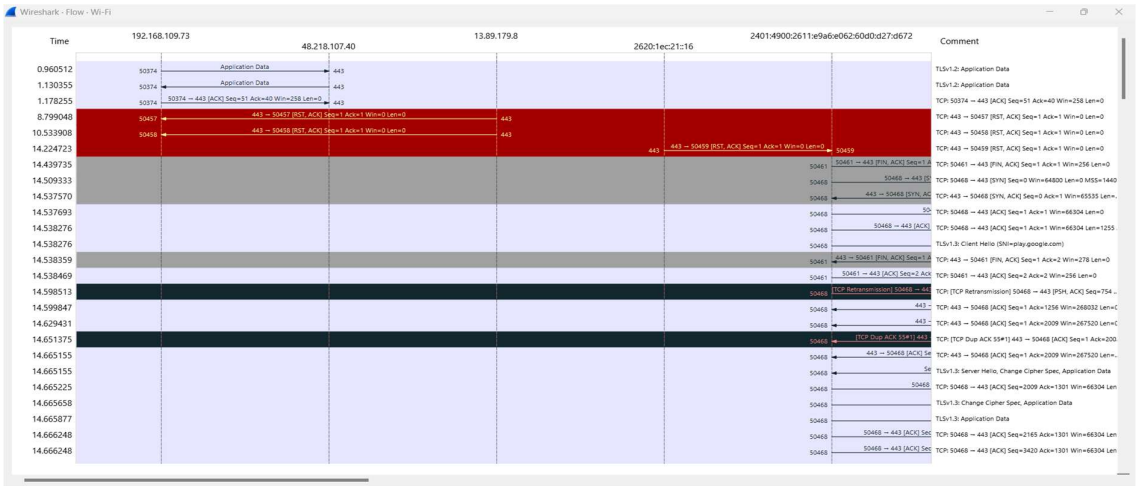
Search TCP packets in search bar.

To see flow graph click Statistics→Flow graph.

Save the packets.



Flowgraph:



2. Create a Filter to display only ARP packets and inspect the packets.

Procedure

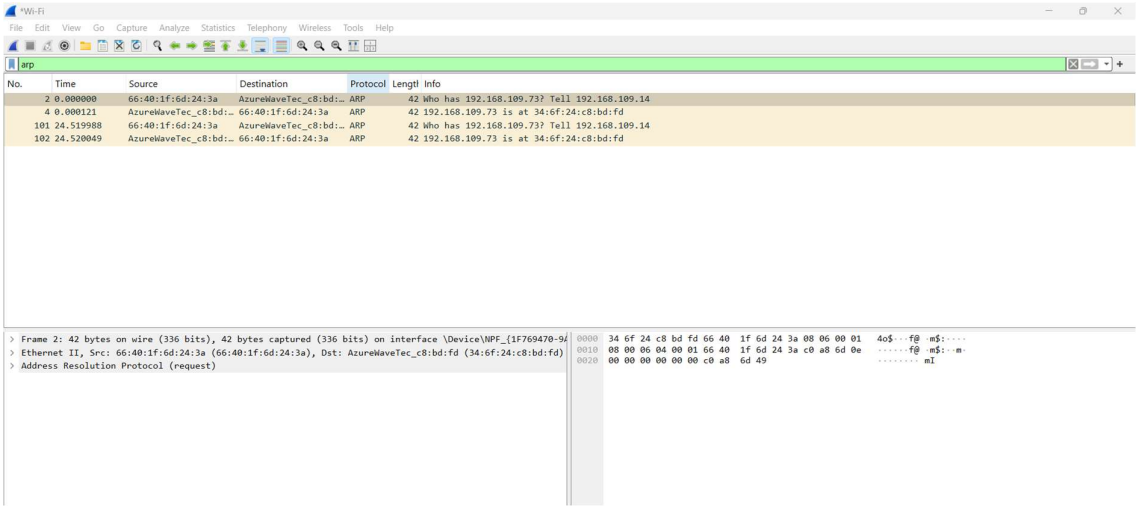
Go to capture →option

Select stop capture automatically after 100 packets.

Then click Start capture.

Search ARP packets in search bar.

Save the packets.



3. Create a Filter to display only DNS packets and provide the flow graph.

Procedure

Go to capture→option

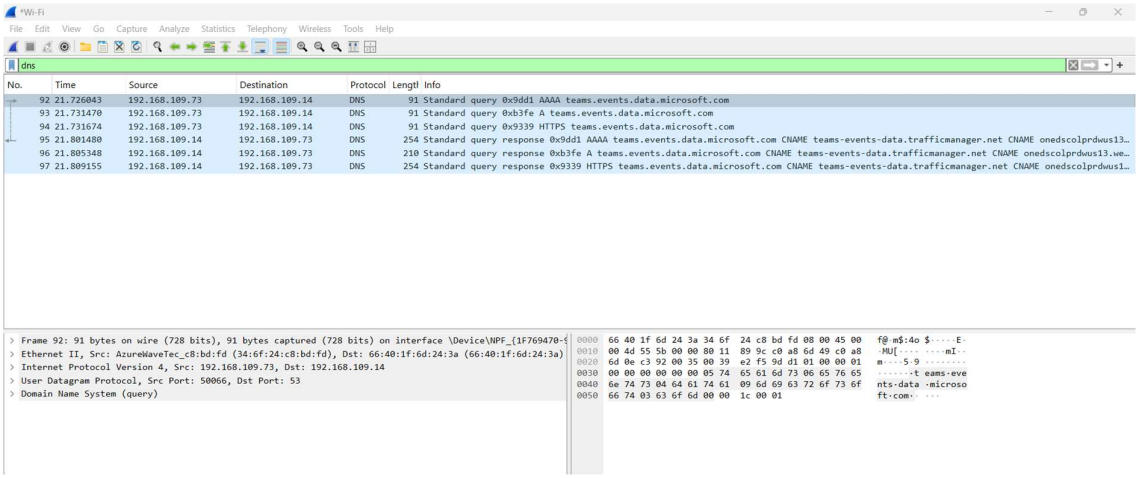
Select stop capture automatically after 100 packets.

Then click Start capture.

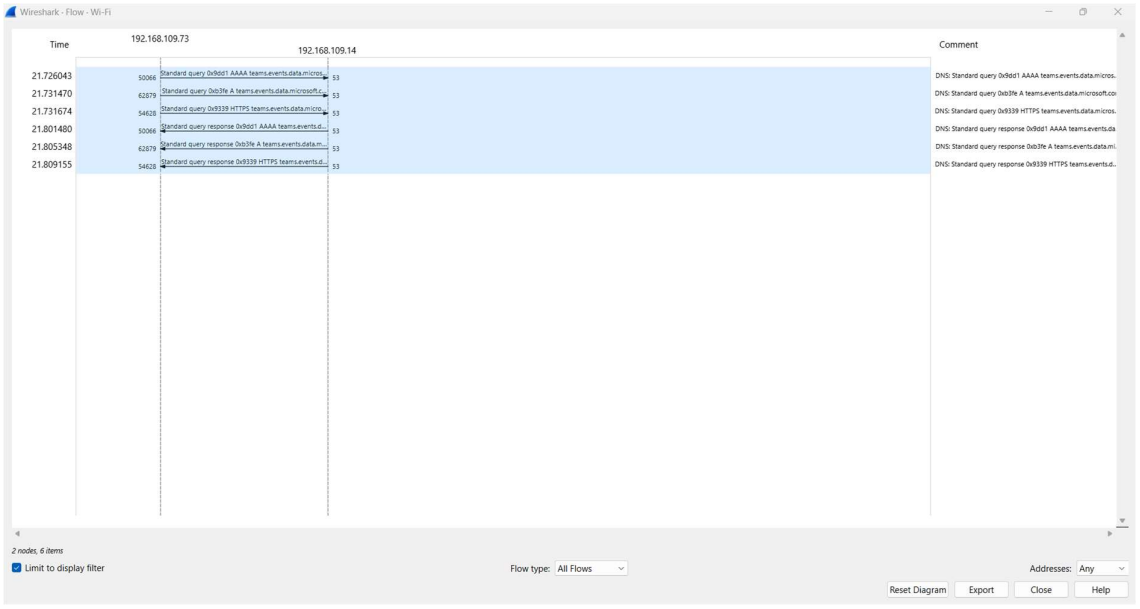
Search DNS packets in search bar.

To see flow graph click Statistics→Flow graph.

Save the packets.



Flowgraph:



4. Create a Filter to display only DHCP packets and inspect the packets.

Procedure

Select Local Area Connection in Wireshark.

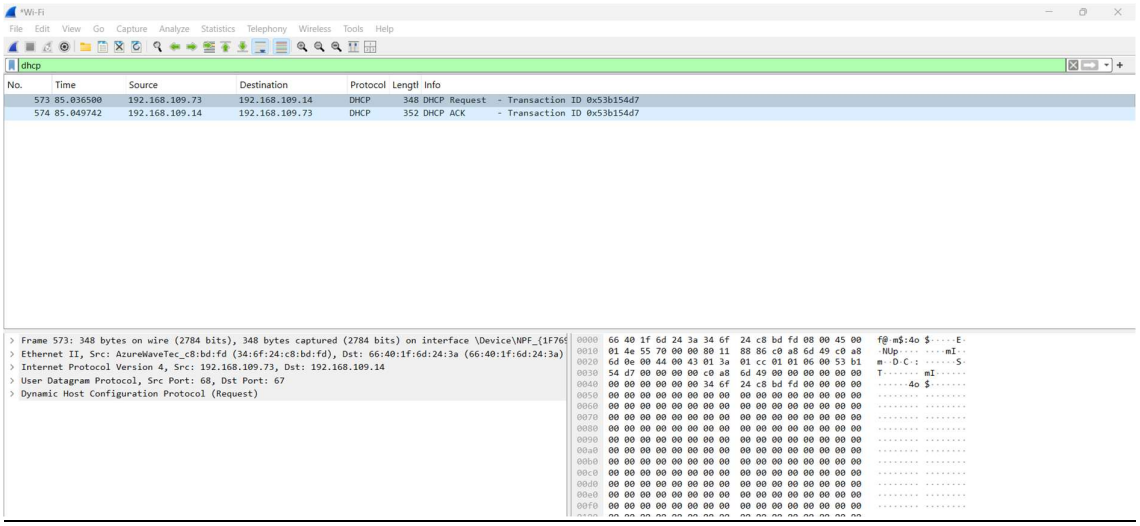
Go to capture →option

Select stop capture automatically after 100 packets.

Then click Start capture.

Search DHCP packets in search bar.

Save the packets


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp
No. Time Source Destination Protocol Lengtl Info
573 85.036500 192.168.109.73 192.168.109.14 DHCP 348 DHCP Request - Transaction ID 0x53b154d7
574 85.049742 192.168.109.14 192.168.109.73 DHCP 352 DHCP ACK - Transaction ID 0x53b154d7
Frame 573: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface \Device\NPF_{1F76
Ethernet II, Src: AzureWaveTec_c8:bd:fd (34:6f:24:c8:bd:fd), Dst: 66:40:1f:6d:24:3a (66:40:1f:6d:24:3a)
Internet Protocol Version 4, Src: 192.168.109.73, Dst: 192.168.109.14
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
0000 66 40 1f 6d 24 3a 34 6f 24 c8 bd fd 08 00 45 00 f@·m$:4o $·····E·
0010 01 4e 55 70 00 00 80 11 88 86 c0 a8 6d 49 c0 a8 ·NUp···· ····mI··
0020 6d 0e 00 44 00 43 01 3a 01 cc 01 01 06 00 53 b1 m··D·C·: ·····S·
0030 54 d7 00 00 00 00 c0 a8 6d 49 00 00 00 00 00 00 T····· mI····
0040 00 00 00 00 00 00 34 6f 24 c8 bd fd 00 00 00 00 ·····4o $·····