

Practical 5

Aim:

Experiments on Packet capture tool: Wireshark

Capturing Packets:

The screenshot displays the Wireshark Network Analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main window is divided into several panes. The top pane shows the 'Welcome to Wireshark' message. The 'Capture' pane below it lists available network interfaces for capturing packets, including Wi-Fi, Local Area Connections, Bluetooth, VMware Network Adapters, and Ethernet. The 'Packet List' pane shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The selected packet (No. 24) is highlighted in red. The bottom pane shows the details of the selected packet, including Ethernet II, Internet Protocol Version 6, and User Datagram Protocol fields.

Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

Welcome to Wireshark

Capture

...using this filter: [Enter a capture filter ...] All interfaces shown

Wi-Fi

Local Area Connection* 10

Local Area Connection* 9

Local Area Connection* 8

Bluetooth Network Connection

VMware Network Adapter VMnet8

VMware Network Adapter VMnet1

Local Area Connection* 2

Local Area Connection* 1

Adapter for loopback traffic capture

Local Area Connection

Ethernet 2

Event Tracing for Windows (ETW) reader

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|------------------------|------------------------|----------|--------|--|
| 21 | 1.752146 | 2401:4900:2611:e9a6... | 2404:6800:4007:809... | UDP | 95 | 63909 → 443 Len=33 |
| 22 | 1.767535 | 2401:4900:2611:e9a6... | 2603:1040:a06:6::1 | TCP | 74 | 49410 → 443 [ACK] Seq=102 Ack=172 Win=257 Len=0 |
| 23 | 1.938122 | 2401:4900:2611:e9a6... | 2404:6800:4007:809... | UDP | 91 | 63909 → 443 Len=29 |
| 24 | 1.963605 | 52.104.129.39 | 192.168.109.73 | TCP | 54 | 443 → 50349 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0 |
| 25 | 2.010608 | 2404:6800:4007:809... | 2401:4900:2611:e9a6... | UDP | 87 | 443 → 63909 Len=25 |
| 26 | 2.218300 | 2401:4900:2611:e9a6... | 2404:6800:4007:809... | UDP | 91 | 63909 → 443 Len=29 |
| 27 | 2.355362 | 2404:6800:4007:809... | 2401:4900:2611:e9a6... | UDP | 87 | 443 → 63909 Len=25 |
| 28 | 2.564675 | 2401:4900:2611:e9a6... | 2404:6800:4007:809... | UDP | 91 | 63909 → 443 Len=29 |
| 29 | 2.714895 | 2401:4900:2611:e9a6... | 2603:1046:1406::5 | TCP | 74 | 50348 → 443 [FIN, ACK] Seq=1 Ack=1 Win=259 Len=0 |
| 30 | 2.717233 | 2404:6800:4007:809... | 2401:4900:2611:e9a6... | UDP | 87 | 443 → 63909 Len=25 |
| 31 | 2.814103 | 2603:1046:1406::5 | 2401:4900:2611:e9a6... | TCP | 74 | 443 → 50348 [FIN, ACK] Seq=1 Ack=2 Win=16388 Len=0 |
| 32 | 2.814159 | 2401:4900:2611:e9a6... | 2603:1046:1406::5 | TCP | 74 | 50348 → 443 [ACK] Seq=2 Ack=2 Win=259 Len=0 |
| 33 | 2.932200 | 2401:4900:2611:e9a6... | 2404:6800:4007:809... | UDP | 91 | 63909 → 443 Len=29 |
| 34 | 3.022840 | 2404:6800:4007:809... | 2401:4900:2611:e9a6... | UDP | 87 | 443 → 63909 Len=25 |
| 35 | 3.227306 | 2401:4900:2611:e9a6... | 2404:6800:4007:809... | UDP | 91 | 63909 → 443 Len=29 |
| 36 | 3.288336 | 2404:6800:4007:809... | 2401:4900:2611:e9a6... | UDP | 87 | 443 → 63909 Len=25 |
| 37 | 3.493667 | 2401:4900:2611:e9a6... | 2404:6800:4007:809... | UDP | 91 | 63909 → 443 Len=29 |

> Frame 1: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF-{17709478-9} Ethernet II, Src: AzureWaveTec, c8:bd:fd (3a:6f:24:c8:bd:fd), Dst: 66:4b:1f:6d:24:3a (66:4b:1f:6d:24:3a)

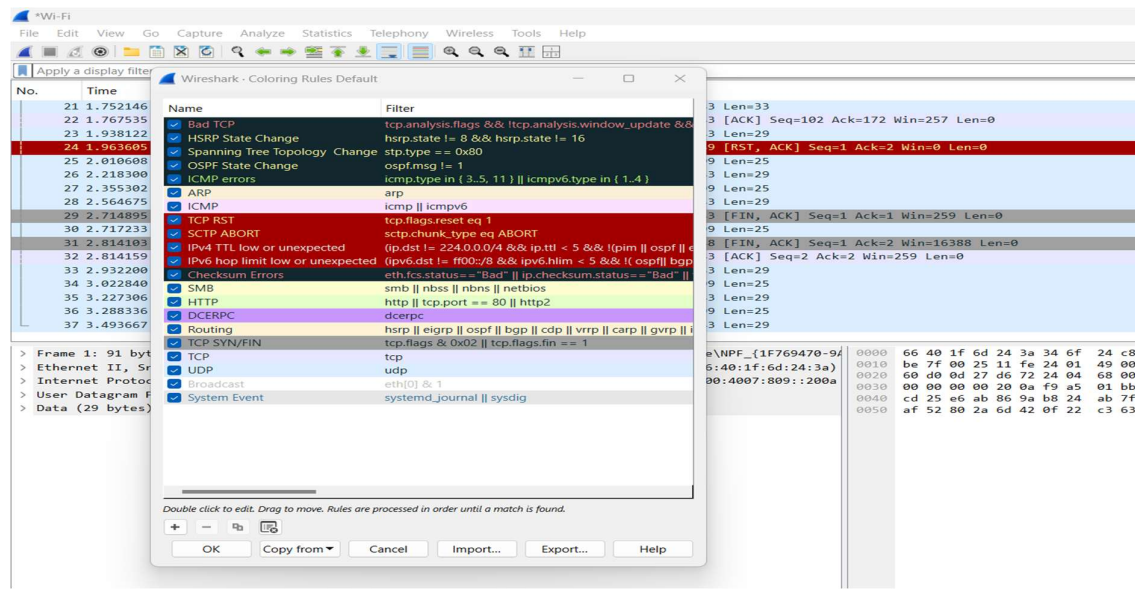
> Internet Protocol Version 6, Src: 2401:4900:2611:e9a6:e062:60d0:d27:d672, Dst: 2404:6800:4007:809:200a

> User Datagram Protocol, Src Port: 63909, Dst Port: 443

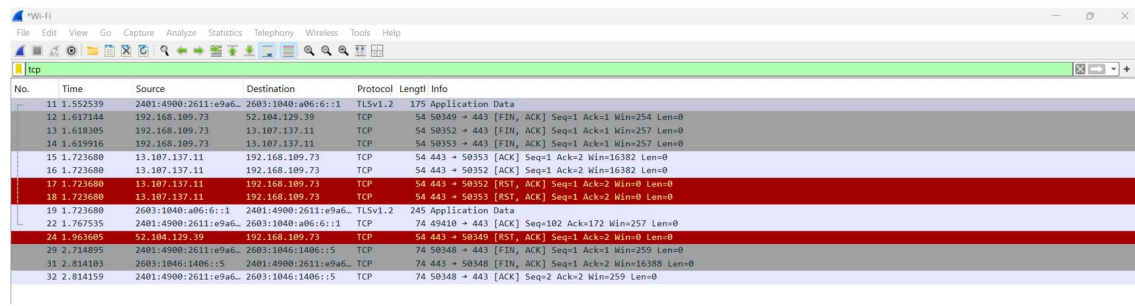
> Data (29 bytes)

0000 66 4b 1f 6d 24 3a 34 0f 24 c8 bd fd 86 dd 60 0f f8 a5 do \$
0010 be 7f 00 25 11 fe 24 01 49 00 26 11 e9 a6 e0 62 ..%\$ I&.....
0020 60 d0 0d 27 d6 72 24 04 68 00 40 07 08 09 00 00r\$.h@....
0030 00 00 00 00 20 0a f9 a5 01 bb 00 25 ff 78 41 e4\$...xA..
0040 cd 25 ed ab 86 9a bd 24 ab 7f b3 f3 35 06 9a eb\$...S...
0050 af 52 80 2a 6d 42 0f 22 c3 63 9cR.*B"....c.

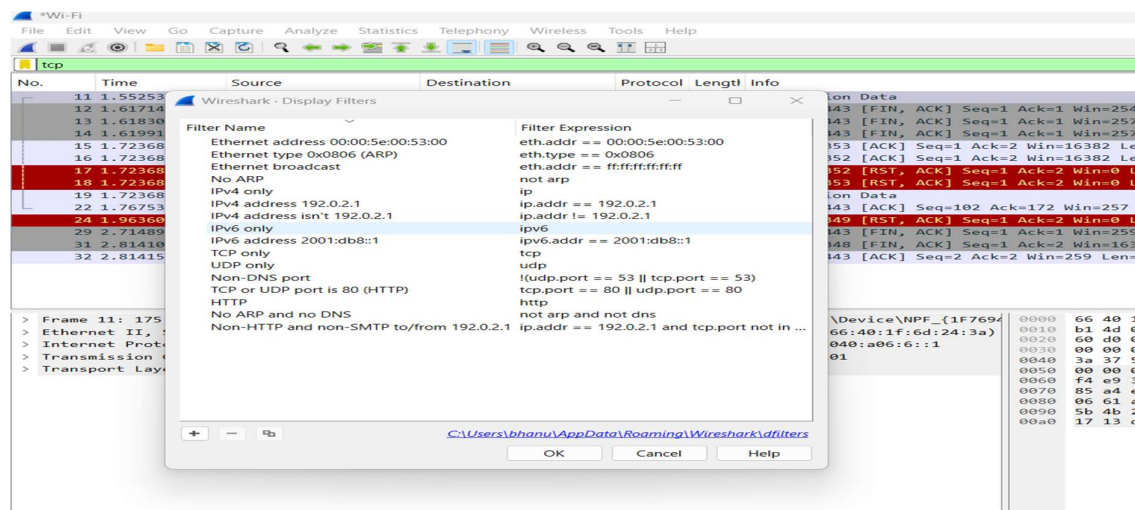
Color Coding:



Filtering Packets:



Display Filters:



```
.....+.mm.~.?.9.q.#....C.....x..l..*....a.E^#!;9o.....[K(.b.k#.++++.d-.b...
.....9.U.....i.`.....R.`6..2&M.....}.2nz....G||.....d...sy.2
C.5. 4..k...r...$.D....x...4.$@.3#.p..|.....,
.....k.+7F...H.C....._Q8V*.].|.j.....A~1
```

The image displays a Wireshark packet capture of a network traffic. The top bar shows the Wi-Fi icon and standard application menus (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help). Below the menu bar is a toolbar with various icons for packet capture and analysis. The main window is divided into three panes:

- Packet List:** Shows a list of captured packets. The first packet (No. 19) is selected, showing its details in the packet details pane.
- Packet Details:** Displays the hierarchical structure of the selected packet (No. 19). It includes:
 - Ethernet II:** Shows the source and destination MAC addresses (08:00:27:1d:1d:1d and 08:00:27:1d:1d:1d).
 - Internet Protocol Version 4:** Shows the source and destination IP addresses (192.168.1.100 and 192.168.1.1).
 - Transmission Control Protocol:** Shows the source and destination ports (443 and 80), the sequence number (30348), and the acknowledgment number (2).
- Packet Bytes:** Displays the raw packet data in hexadecimal and ASCII.

| Time | 2401:4900:2611:e9a6:e062:60d0:d27:d672 2404:6800:4007:809:200a | 2603:1040:a06:c1 | 192.168.109.73 | 52.104.129.39 | 13.107.137.11 | 2603:1046:1406:5 | Comment |
|----------|---|------------------|--|---------------|---------------|------------------|---|
| 0.000000 | 63909 → 443 Len=29 | 443 | | | | | UDP: 63909 → 443 Len=29 |
| 0.060360 | 443 → 63909 Len=29 | 443 | | | | | UDP: 443 → 63909 Len=29 |
| 0.264682 | 63909 → 443 Len=29 | 443 | | | | | UDP: 63909 → 443 Len=29 |
| 0.430287 | 443 → 63909 Len=25 | 443 | | | | | UDP: 443 → 63909 Len=25 |
| 0.642048 | 63909 → 443 Len=29 | 443 | | | | | UDP: 63909 → 443 Len=29 |
| 0.751075 | 443 → 63909 Len=25 | 443 | | | | | UDP: 443 → 63909 Len=25 |
| 1.159025 | 63909 → 443 Len=29 | 443 | | | | | UDP: 63909 → 443 Len=29 |
| 1.379795 | 63909 → 443 Len=29 | 443 | | | | | UDP: 63909 → 443 Len=29 |
| 1.384770 | 443 → 63909 Len=25 | 443 | | | | | UDP: 443 → 63909 Len=25 |
| 1.432942 | 63909 → 443 Len=26 | 443 | | | | | UDP: 443 → 63909 Len=26 |
| 1.552339 | 49410 Application Data | 443 | | | | | TLSv2 Application Data |
| 1.617144 | | | 50349 → 443 [FIN, ACK] Seq=1 Acs=1 Win=0 | 443 | | | TCP: 50349 → 443 [FIN, ACK] Seq=1 Acs=1 Win=0 |
| 1.618305 | | | 50352 → 443 [FIN, ACK] Seq=1 Acs=1 Win=257 Len=0 | 443 | | | TCP: 50352 → 443 [FIN, ACK] Seq=1 Acs=1 Win=257 |
| 1.619916 | | | 50353 → 443 [FIN, ACK] Seq=1 Acs=1 Win=257 Len=0 | 443 | | | TCP: 50353 → 443 [FIN, ACK] Seq=1 Acs=1 Win=257 |
| 1.723680 | | | 443 → 50353 [ACK] Seq=1 Acs=2 Win=10383 Len=0 | 443 | | | TCP: 443 → 50353 [ACK] Seq=1 Acs=2 Win=10383 |
| 1.723680 | | | 443 → 50353 [ACK] Seq=1 Acs=2 Win=10383 Len=0 | 443 | | | TCP: 443 → 50353 [ACK] Seq=1 Acs=2 Win=10383 |
| 1.723680 | | | 443 → 50353 [RST, ACK] Seq=1 Acs=0 Win=0 Len=0 | 443 | | | TCP: 443 → 50353 [RST, ACK] Seq=1 Acs=0 Win=0 |
| 1.723680 | | | 443 → 50353 [RST, ACK] Seq=1 Acs=0 Win=0 Len=0 | 443 | | | TCP: 443 → 50353 [RST, ACK] Seq=1 Acs=0 Win=0 |
| 1.733132 | 49410 Application Data | 443 | | | | | TLSv2 Application Data |
| 1.752146 | 443 → 63909 Len=752 | 443 | | | | | UDP: 443 → 63909 Len=752 |
| 1.767535 | 63909 → 443 Len=33 | 443 | | | | | UDP: 63909 → 443 Len=33 |
| 1.938122 | 49410 → 443 [ACK] Seq=102 Acs=172 Win=257 Len=0 | 443 | | | | | TCP: 49410 → 443 [ACK] Seq=102 Acs=172 Win=257 |
| 1.963605 | 63909 → 443 Len=29 | 443 | | | | | UDP: 63909 → 443 Len=29 |
| 2.010608 | 63909 → 443 Len=25 | 443 | 50349 → 443 [FIN, ACK] Seq=1 Acs=0 | 443 | | | TCP: 443 → 50349 [FIN, ACK] Seq=1 Acs=0 Win=0 |
| | 63909 → 443 Len=25 | 443 | | | | | UDP: 443 → 63909 Len=25 |

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

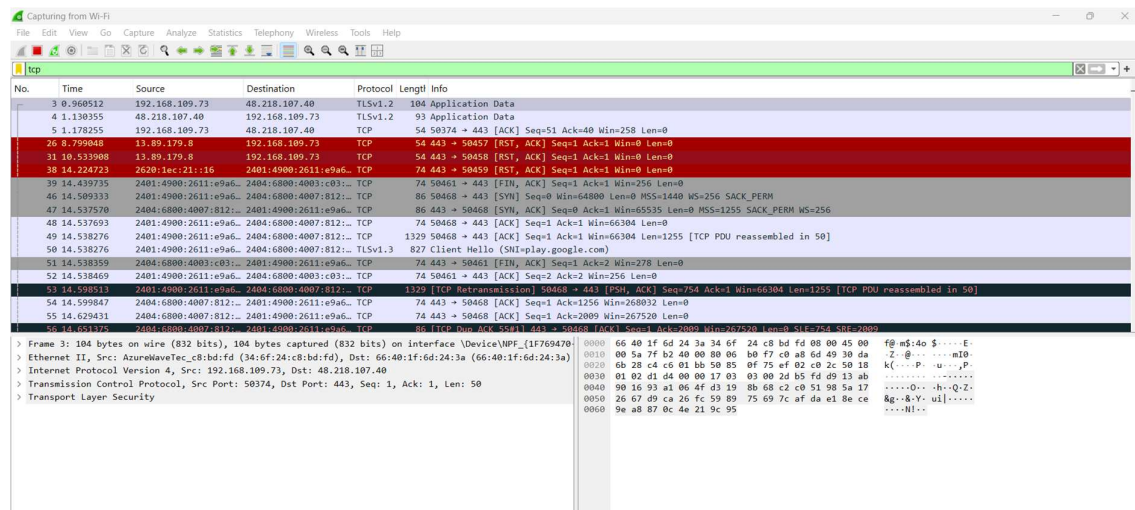
Select stop capture automatically after 100 packets.

Then click Start capture.

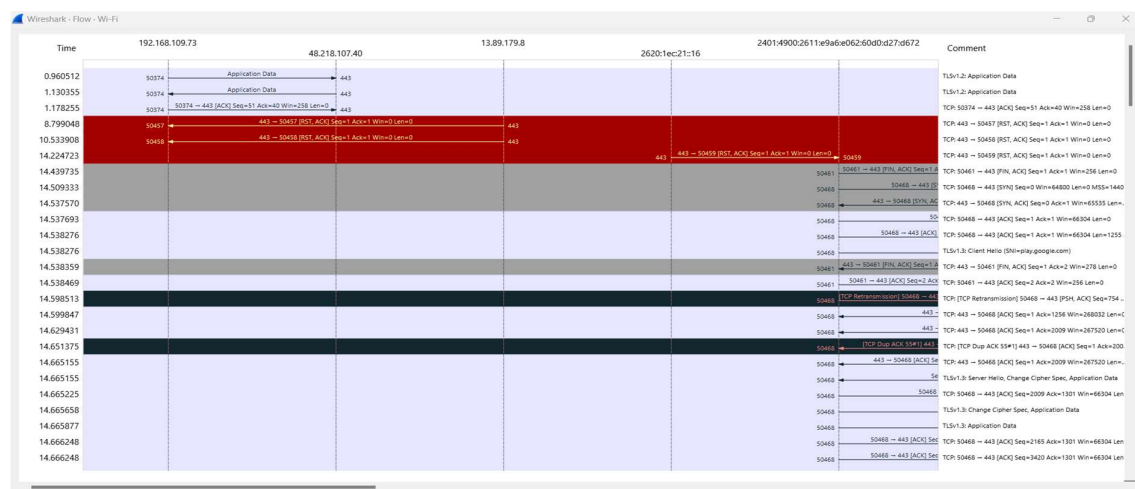
Search TCP packets in search bar.

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

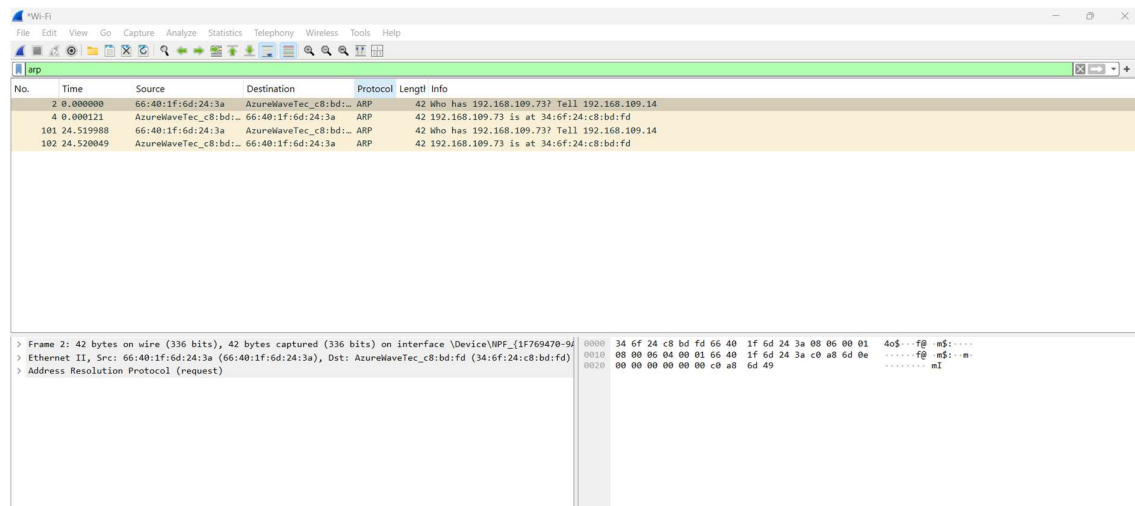
Go to capture → option

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

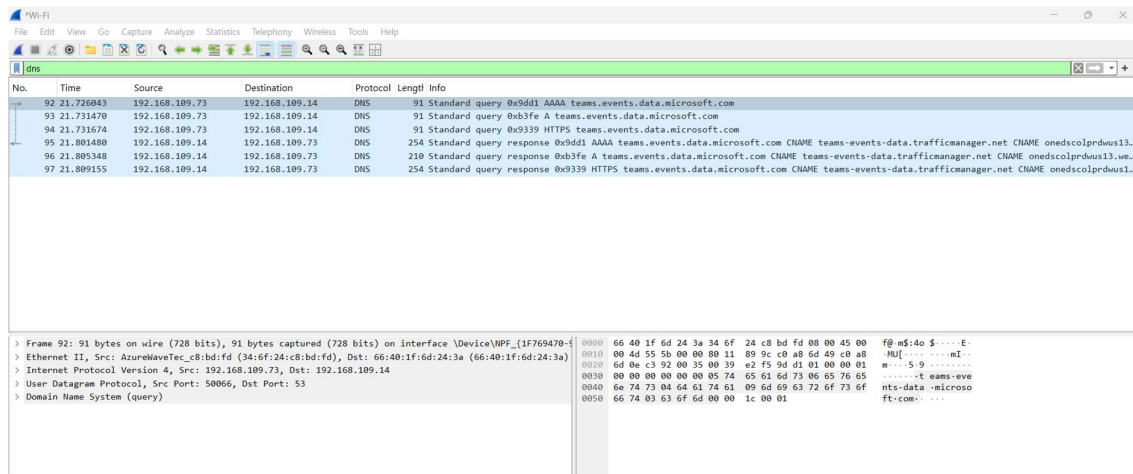
Select stop capture automatically after 100 packets.

Then click Start capture.

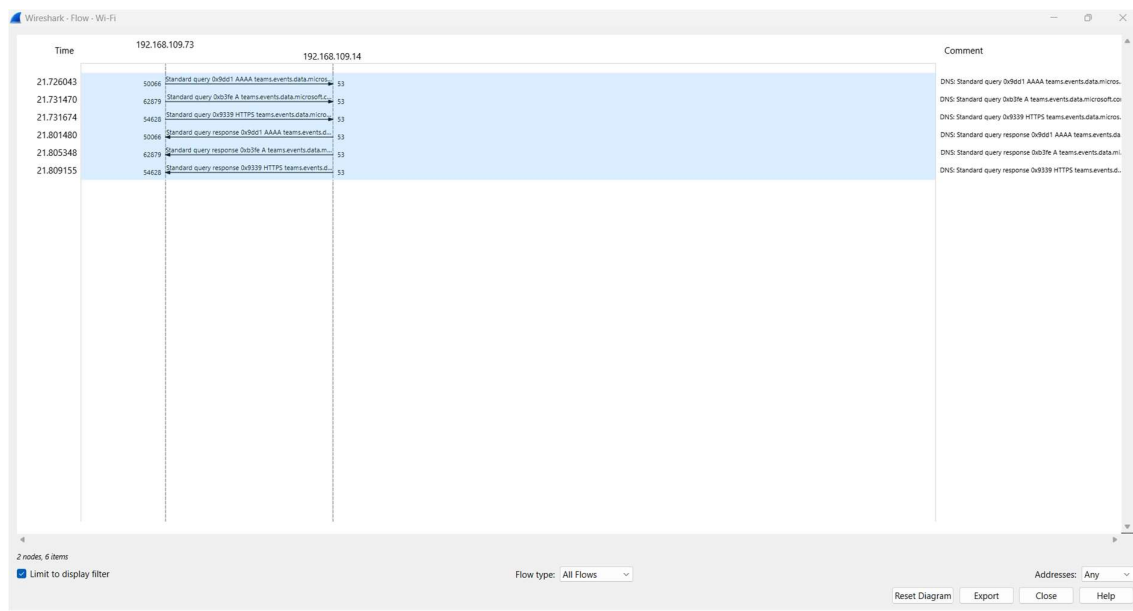
Search DNS packets in search bar.

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


```

Frame 573: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface \Device\NPF...{1F76E...}
Ethernet II, Src: AzureWiredTc8: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)

```