

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:

- Welcome to Wireshark**: A blue banner at the top of the main pane.
- Capture**: A section below the banner with a dropdown menu set to "using this filter" and a text input field for "Enter a capture filter...". To the right is a button labeled "All interfaces shown".
- Interface List**: A list of network interfaces available for capture. The "Wi-Fi" interface is selected and highlighted in blue. Other interfaces include Local Area Connection* 10, Local Area Connection* 9, Local Area Connection* 8, Bluetooth Network Connection, VMware Network Adapter VMnet3, VMware Network Adapter VMnet1, Local Area Connection* 2, Local Area Connection* 1, Adapter for loopback traffic capture, Local Area Connection, Ethernet 2, and Event Tracing for Windows (ETW) reader.
- Packet List**: A table showing captured packets. The columns are No., Time, Source, Destination, Protocol, Length, and Info. The table contains 29 entries, with the 29th entry (No. 29) selected.
- Packet Details**: A pane below the packet list showing the hierarchical structure of the selected packet (No. 29). It includes:
 - Frame 1: 91 bytes on wire (728 bits), 91 bytes captured (728 bits) on interface \Device\NPF>{1F709470-94...}
 - Ethernet II, Src: AzureWaveTec_081bd1fd (3a:0f:2a:c8:bd:fd), Dst: 66:40:3f:6d:24:3a (66:40:3f:6d:24:3a)
 - Internet Protocol Version 6, Src: 2404:4900:2611:e9a6:e062:0808:027:0672, Dst: 2404:6800:4007:809::200a
 - User Datagram Protocol, Src Port: 63909, Dst Port: 443
 - Data (29 bytes)
- Packet Bytes**: A pane at the bottom showing the raw bytes of the selected packet in hexadecimal and ASCII. The first few bytes are 0000 06 00 1f 6d 24 3a 0f 24 c8 bd fd 86 dd 80 0f, which correspond to the Ethernet II header.

Color Coding:

The image shows the Wireshark network protocol analyzer interface. The main window displays a list of captured packets, with the selected packet (No. 24) highlighted in red. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol, and User Datagram Protocol. The packet bytes pane shows the raw data of the selected packet. A dialog box titled 'Wireshark - Coloring Rules Default' is open, showing a list of rules with checkboxes and filter expressions. The rules are organized into a table with columns for Name, Filter, and a description. The rules are: Bad TCP, HSRP State Change, Spanning Tree Topology Change, OSPF State Change, ICMP errors, ARP, ICMP, TCP RST, SCTP ABORT, IPv4 TTL low or unexpected, IPv6 hop limit low or unexpected, Checksum Errors, SMB, HTTP, DCE/RPC, Routing, TCP SYN/FIN, UDP, Broadcast, and System Event. The dialog box also includes a 'Double click to edit. Drag to move. Rules are processed in order until a match is found.' message and buttons for OK, Copy from, Cancel, Import..., Export..., and Help.

Filtering Packets:

The image shows the Wireshark network protocol analyzer interface with a filter applied. The filter bar at the top contains the filter 'tcp'. The packet list pane shows only TCP packets, with the selected packet (No. 24) highlighted in red. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol, and User Datagram Protocol. The packet bytes pane shows the raw data of the selected packet.

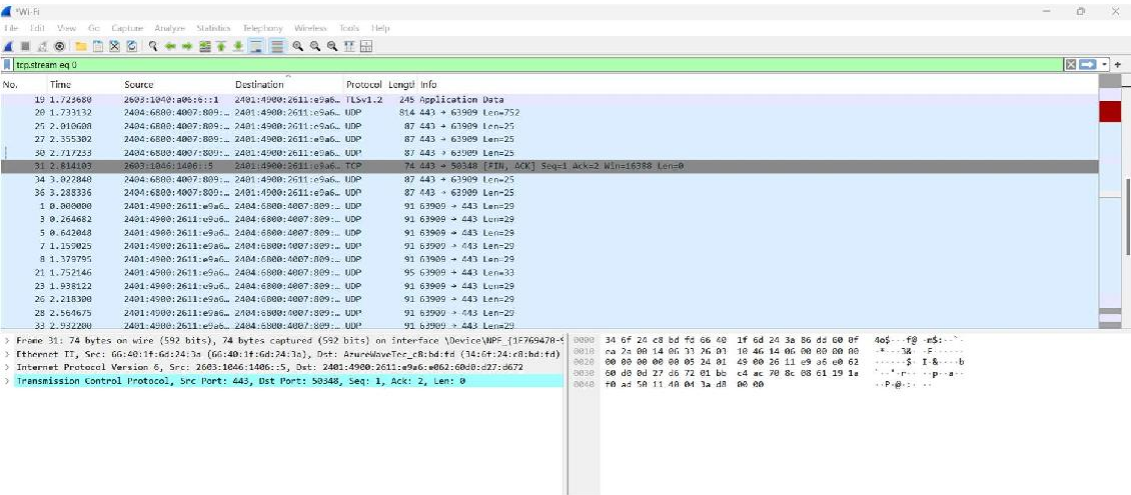
Display Filters:

The image shows the Wireshark network protocol analyzer interface with a filter applied. The filter bar at the top contains the filter 'tcp'. A dialog box titled 'Wireshark - Display Filters' is open, showing a list of filters with checkboxes and filter expressions. The filters are organized into a table with columns for Filter Name, Filter Expression, and a description. The filters are: Ethernet address 00:00:5e:00:03:00, Ethernet type 0x0806 (ARP), Ethernet broadcast, No ARP, IPv4 only, IPv4 address 192.0.2.1, IPv4 address isn't 192.0.2.1, IPv6 only, IPv6 address 2001:db8::1, TCP only, UDP only, Non-DNS port, TCP or UDP port is 80 (HTTP), HTTP, No ARP and no DNS, Non-HTTP and non-SMTP to/from 192.0.2.1, and ip.addr == 192.0.2.1 and tcp.port not in ... The dialog box also includes a 'Double click to edit. Drag to move. Rules are processed in order until a match is found.' message and buttons for OK, Cancel, and Help.

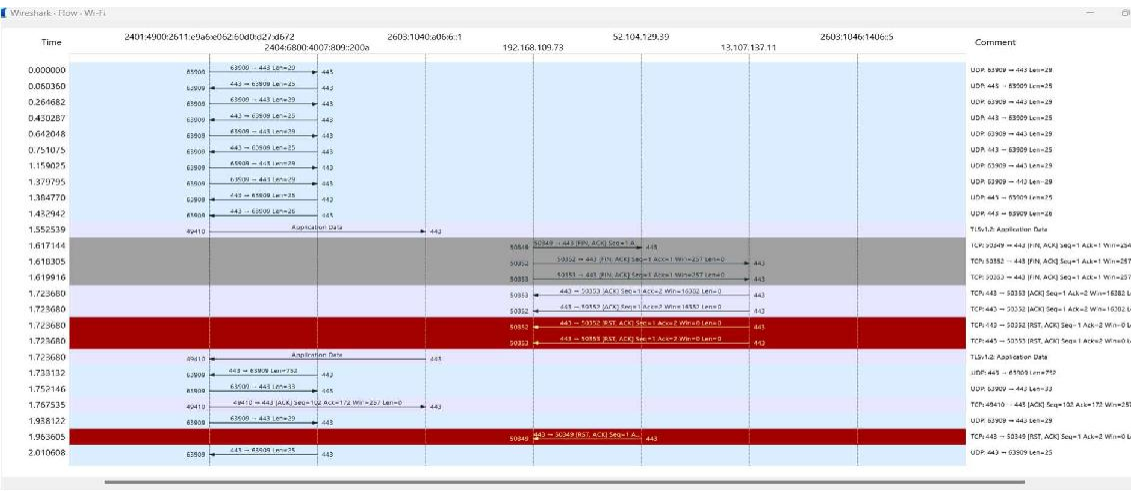
Tcp Stream:



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

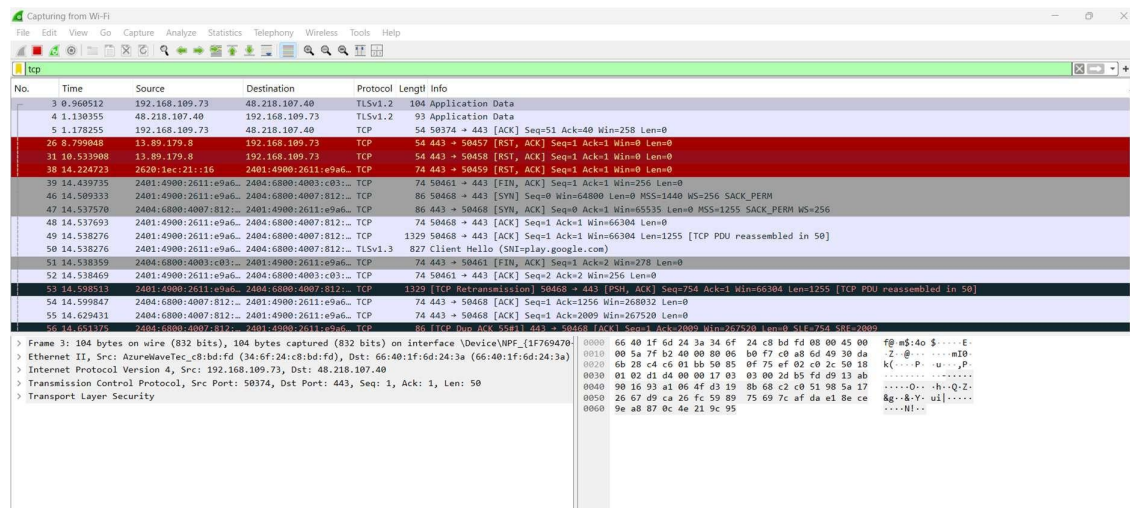
Select stop capture automatically after 100 packets.

Then click Start capture.

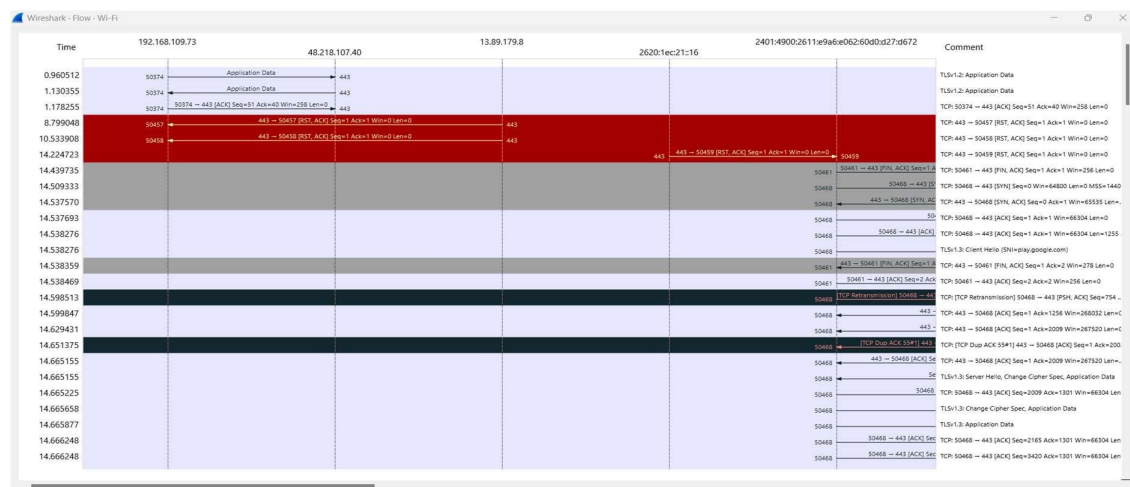
Search TCP packets in search bar.

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

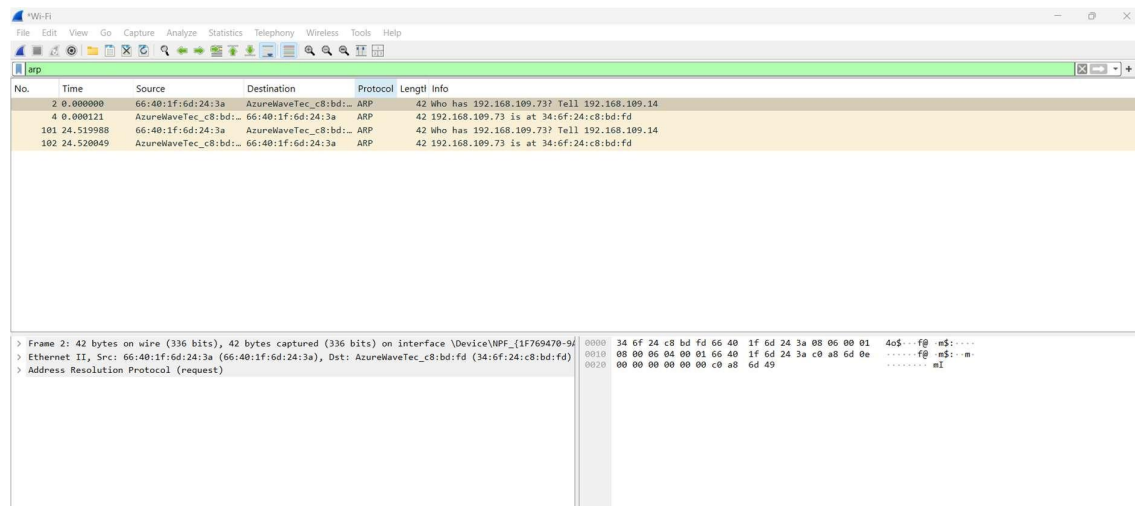
Go to capture → option

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

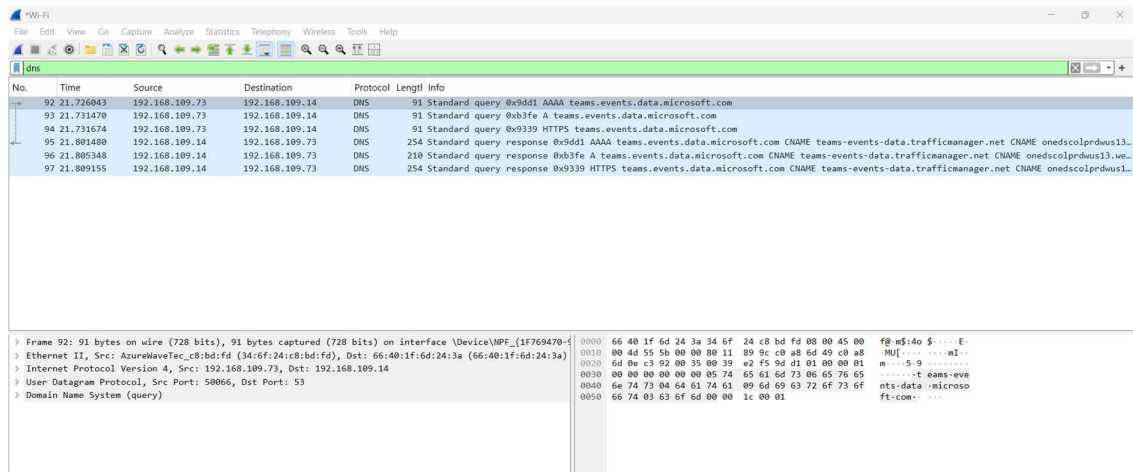
Select stop capture automatically after 100 packets.

Then click Start capture.

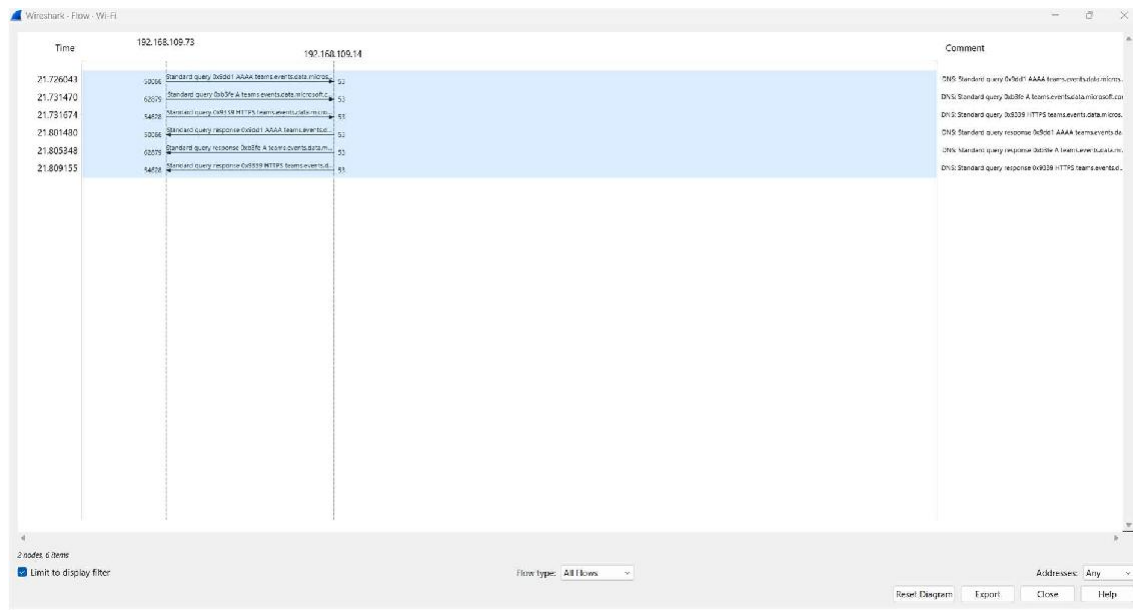
Search DNS packets in search bar.

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

[illegible]