



EXPERIMENT 07

Aim: Study of packet sniffer tools wireshark :-

1. Observer performance in promiscuous as well as non-promiscuous mode.
2. Show the packets can be traced based on different filters.

Theory:

What Is Wireshark?

Originally known as Ethereal, Wireshark displays data from hundreds of different protocols on all major network types. Data packets can be viewed in real-time or analyzed offline. Wireshark supports dozens of capture/trace file formats, including CAP and ERF. Integrated decryption tools display the encrypted packets for several common protocols, including WEP and WPA/WPA2.



How to Download and Install Wireshark

Wireshark can be downloaded at no cost from the Wireshark Foundation website for both macOS and Windows. You'll see the latest stable release and the current developmental release. Unless you're an advanced user, download the stable version.

During the Windows setup process, choose to install WinPcap or Npcap if prompted as these include libraries required for live data capture.

You must be logged in to the device as an administrator to use Wireshark. In Windows 10, search for Wireshark and select Run as administrator. In macOS, right-click the app icon and select Get Info. In the Sharing & Permissions settings, give the admin Read & Write privileges. The application is also available for Linux and other UNIX-like platforms including Red Hat, Solaris, and FreeBSD. The binaries required for these operating systems can be found toward the bottom of the Wireshark download page under the Third-Party Packages section.

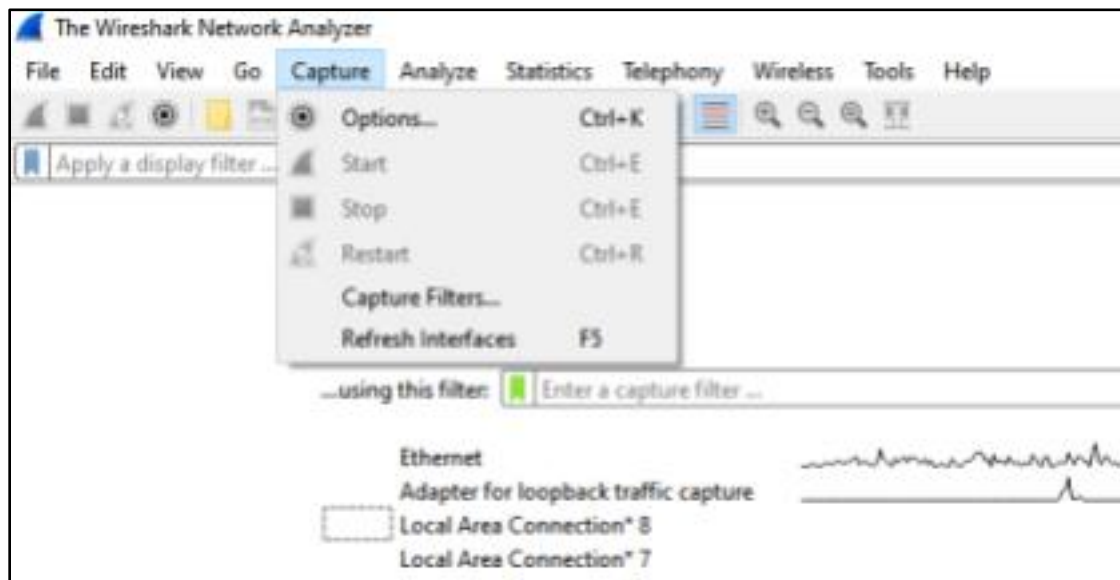


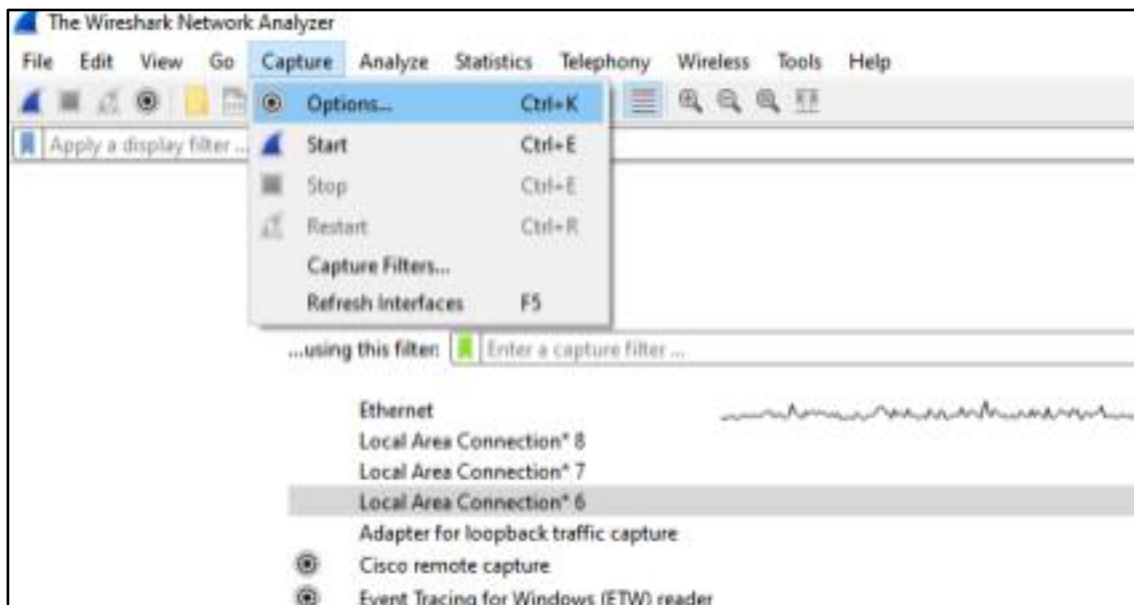
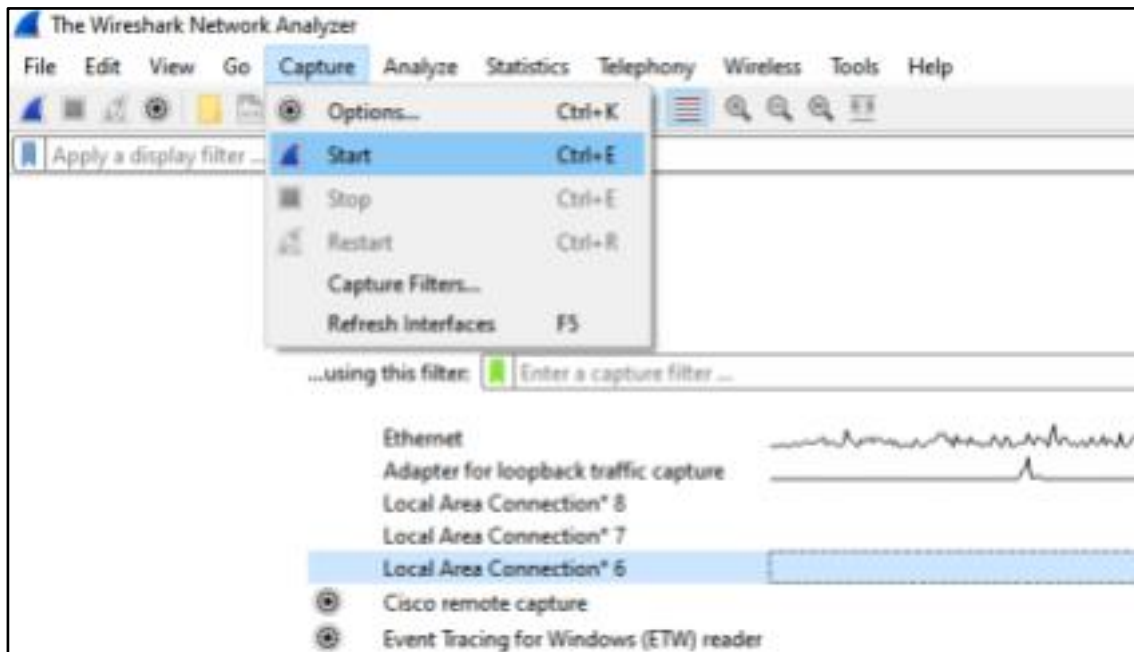
How to Capture Data Packets With Wireshark

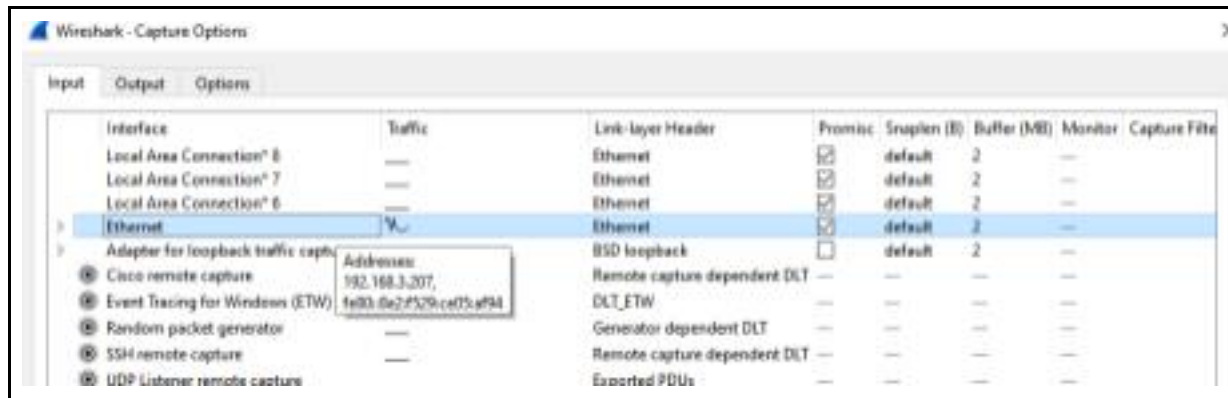
When you launch Wireshark, a welcome screen lists the available network connections on your current device. Displayed to the right of each is an EKG-style line graph that represents live traffic on that network.

To begin capturing packets with Wireshark:

1. Select one or more of the networks, go to the menu bar, then select Capture.
2. In the Wireshark Capture Interfaces window, select Start.
3. Select File > Save As or choose an Export option to record the capture.
4. To stop capturing, press Ctrl+E. Or, go to the Wireshark toolbar and select the red Stop button that's located next to the shark fin.







How to View and Analyze Packet Contents

The captured data interface contains three main sections:

The packet list pane (the top section)

The packet details pane (the middle section)

The packet bytes pane (the bottom section)

1. Packet List

The packet list pane, located at the top of the window, shows all packets found in the active capture file. Each packet has its own row and corresponding number assigned to it, along with each of these data points:

No: This field indicates which packets are part of the same conversation. It remains blank until you select a packet.

Time: The timestamp of when the packet was captured is displayed in this column. The default format is the number of seconds or partial seconds since this specific capture file was first created.

Source: This column contains the address (IP or other) where the packet originated.

Destination: This column contains the address that the packet is being sent to.

Protocol: The packet's protocol name, such as TCP, can be found in this column.

Length: The packet length, in bytes, is displayed in this column.

Info: Additional details about the packet are presented here. The contents of this column can vary greatly depending on packet contents.

To change the time format to something more useful (such as the actual time of day), select **View > Time Display Format**.

When a packet is selected in the top pane, you may notice one or more symbols appear in the No. column. Open or closed brackets and a straight horizontal line indicate whether a packet or group of packets are part of the same back-and-forth conversation on the network. A broken horizontal



Vidyavardhini's College of Engineering and Technology, Vasai

Department of Computer Science & Engineering (Data Science)

line signifies that a packet is not part of the conversation.

The image shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets. The middle pane shows the details of the selected packet (No. 5538), which is an Internet Protocol Version 4 packet. The bottom pane shows the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
5062	39.104617	Fe80::330d:86f6:854...	FF02::1::1	LLMNR	88	Standard query 0x4808 A WP1702274
5063	39.104595	192.168.1.200	224.0.0.252	LLMNR	68	Standard query 0x4808 AAAA WP1702274
5064	39.104595	192.168.1.200	224.0.0.252	LLMNR	68	Standard query 0x4808 A WP1702274
5065	39.215004	192.168.1.50	192.168.1.255	NDNS	92	Name query NB AVSERVER<00>
5066	39.220799	Fe80::330d:86f6:854...	FF02::1::1	NDNS	94	Standard query 0x0000 A AVSERVER.local, "Q1" question
5067	39.221827	Fe80::330d:86f6:854...	FF02::1::1	LLMNR	88	Standard query 0x2a08 A AVSERVER
5068	39.234892	192.168.1.50	192.168.1.255	NDNS	92	Name query NB AVSERVER<00>
5069	39.234200	192.168.1.50	224.0.0.251	NDNS	74	Standard query 0x0000 A AVSERVER.local, "Q1" question
5070	39.234258	192.168.1.50	224.0.0.252	LLMNR	68	Standard query 0x2a08 A AVSERVER
5071	39.238807	192.168.1.50	224.0.0.251	NDNS	74	Standard query 0x0000 A AVSERVER.local, "Q1" question
5072	39.238805	Fe80::330d:86f6:854...	FF02::1::1	NDNS	94	Standard query 0x0000 A AVSERVER.local, "Q1" question
5073	39.240534	Fe80::330d:86f6:854...	FF02::1::1	LLMNR	88	Standard query 0x521f A AVSERVER
5074	39.243240	192.168.1.50	224.0.0.252	LLMNR	68	Standard query 0x521f A AVSERVER
5075	39.261808	192.168.1.241	192.168.1.255	NDNS	92	Name query NB WP1702274<00>
5076	39.264849	192.168.1.213	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
5077	39.270043	192.168.1.213	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
5078	39.298200	192.168.1.50	192.168.1.255	NDNS	92	Name query NB AVSERVER<00>
5079	39.301836	LinkLocalNtfs 63:8b:c...	Broadcast	ARP	68	who has 192.168.1.1? Tell 192.168.1.34
5508	39.418527	Fe80::330d:86f6:854...	FF02::1::1	UDP	1304	63221 > 3702 [Len=1002]

Frame 5538: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface \\Device\\NPF_{469082C1-C9CF-4E86-A886-92D2311450F7}, id 0

Ethernet II, Src: Intel_33:fd:2e (3c:f8:62:33:fd:2e), Dst: 224.0.0.251

Internet Protocol Version 4, Src: 192.168.1.50, Dst: 224.0.0.251

User Datagram Protocol, Src Port: 5353, Dst Port: 5353

Link-local Multicast Name Resolution (query)

2. Packet Details

The details pane, found in the middle, presents the protocols and protocol fields of the selected packet in a collapsible format. In addition to expanding each selection, you can apply individual Wireshark filters based on specific details and follow streams of data based on protocol type by right-clicking the desired item.

The image shows the Wireshark packet details pane for a selected packet (Frame 10705). The details are organized into a tree structure, showing the hierarchy of the packet's components. The selected packet is a Multicast Domain Name System (query) packet.

Frame 10705: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \\Device\\NPF_{469082C1-C9CF-4E86-A886-92D2311450F7}, id 0

Ethernet II, Src: Intel_33:fd:2e (3c:f8:62:33:fd:2e), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)

Internet Protocol Version 4, Src: 192.168.1.50, Dst: 224.0.0.251

User Datagram Protocol, Src Port: 5353, Dst Port: 5353

Multicast Domain Name System (query)

0000 01 00 5e 00 00 fb 3c f8 62 33 fd 2e 00 00 45 00 ...-.-.-.-. b3 .-.-.-.-. E

0010 00 3c 20 62 00 00 01 11 e0 71 c0 ad 03 3a e0 00 ...-.-.-.-. q .-.-.-.-. .

0020 00 fb 34 a3 14 a3 00 28 ad e0 00 00 00 00 00 01 ...-.-.-.-. { .-.-.-.-. .

0030 00 00 00 00 00 00 00 41 56 53 45 52 56 45 52 05 ...-.-.-.-. A VSERVER

0040 0c 0f 83 01 8c 00 00 01 ...-.-.-.-. local .-.-.-.-. .



3. Packet Bytes

At the bottom is the packet bytes pane, which displays the raw data of the selected packet in a hexadecimal view. This hex dump contains 16 hexadecimal bytes and 16 ASCII bytes alongside the data offset.

Selecting a specific portion of this data automatically highlights its corresponding section in the packet details pane and vice versa. Any bytes that cannot be printed are represented by a period

To display this data in bit format as opposed to hexadecimal, right-click anywhere within the pane and select as bits.

How to Use Wireshark Filters

Capture filters instruct Wireshark to only record packets that meet specified criteria. Filters can also be applied to a capture file that has been created so that only certain packets are shown. These are referred to as display filters.

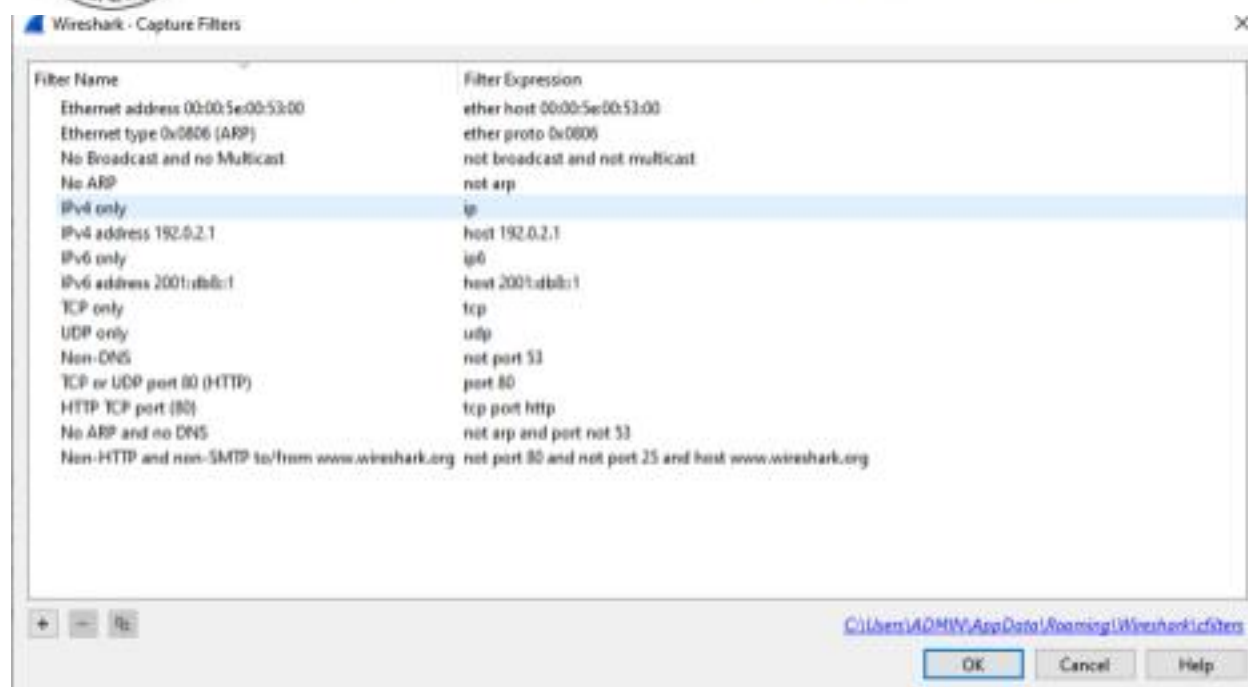
Wireshark provides a large number of predefined filters by default. To use one of these existing filters, enter its name in the Apply a display filter entry field located below the Wireshark toolbar or in the Enter a capture filter field located in the center of the welcome screen.

For example, if you want to display TCP packets, type tcp. The Wireshark autocomplete feature shows suggested names as you begin typing, making it easier to find the correct moniker for the filter you're seeking.

Another way to choose a filter is to select the bookmark on the left side of the entry field. Choose Manage Filter Expressions or Manage Display Filters to add, remove, or edit filters.

You can also access previously used filters by selecting the down arrow on the right side of the entry field to display a history drop-down list.

Capture filters are applied as soon as you begin recording network traffic. To apply a display filter, select the right arrow on the right side of the entry field.



Conclusion :