



Islamic University of Gaza
Faculty of Engineering
Computer Engineering Department
Fall 2025



Data Communications Lab

Lab 3

Wireshark



Eng. Abdullah Idris Ouda
Eng. Haneen Beram

Packet Sniffer

A packet sniffer is a piece of software that can capture and log the packets that travel over a network. They are also known as network analysers, protocol analysers or packet analysers.

These tools help to give network administrators insight into what is happening across their network, allow them to diagnose problems, and much more. While they have a range of legitimate uses, these programs can also be abused in the form of sniffing attacks.

An Example of packet sniffing software is **Wireshark**.

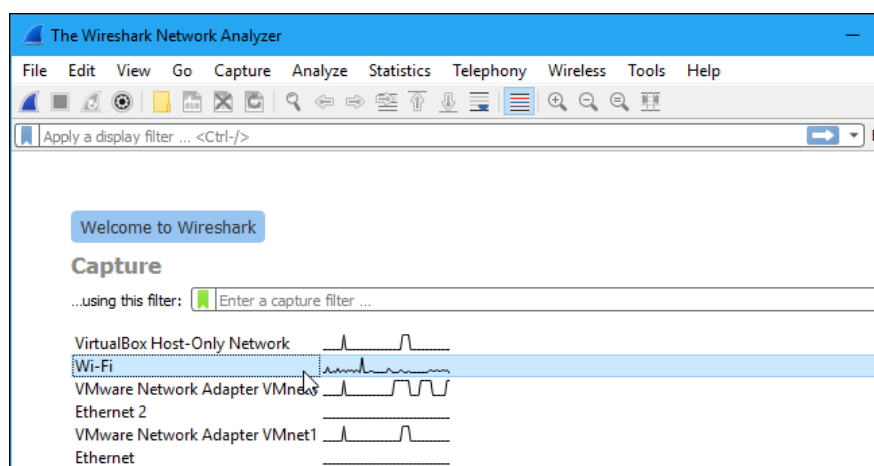
Wireshark

Wireshark is a software tool used to monitor the network traffic through a network interface. It captures network packets in real time and displays them in human-readable format. Wireshark is loved equally by system administrators, network engineers, network enthusiasts, network security professionals and black hat hackers.

Downloading and installing Wireshark is easy. Step one is to check the [official Wireshark download page](#) for the operating system you need. The installation is simple, and the basic version of Wireshark is free.

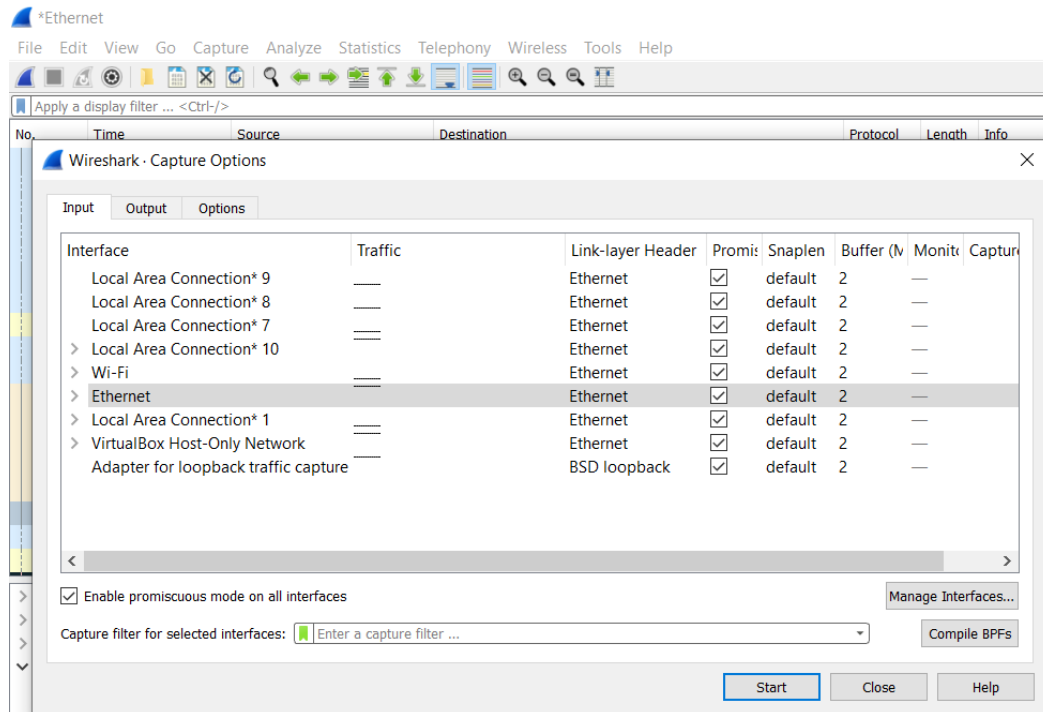
Capturing Packets

After downloading and installing Wireshark, you can launch it and double-click the name of a network interface under Capture to start capturing packets on that interface. For example, if you want to capture traffic on your wireless network, click your wireless interface. You can configure advanced features by clicking Capture > Options.

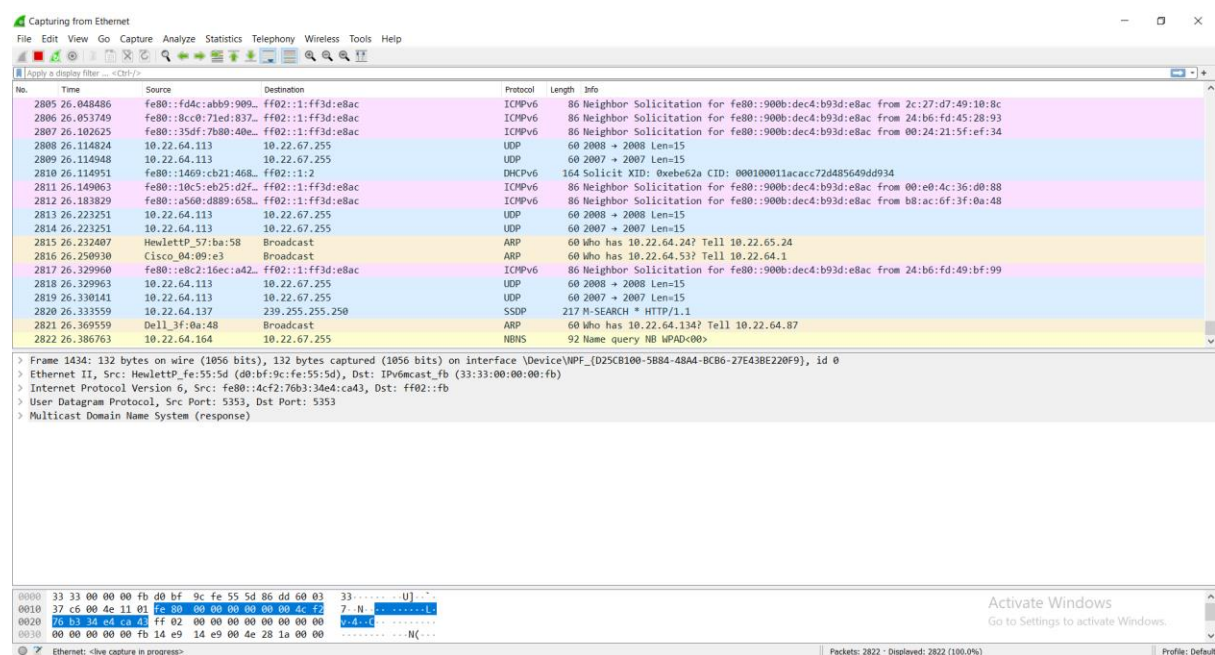


As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your computer system.

If you have **promiscuous mode** enabled—it's enabled by default—you'll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the “Enable promiscuous mode on all interfaces” checkbox is activated at the bottom of this window.



Main Display



- 1- **The menu:** is used to start actions.
- 2- **The main toolbar:** provides quick access to frequently used items from the menu.
- 3- **The filter toolbar:** provides a way to directly manipulate the currently used display filter.
- 4- **The packet list pane:** displays a summary of each packet captured. By clicking on packets in this pane, you control what is displayed in the other two panes.
- 5- **The packet details pane:** displays the packet selected in the packet list pane in more detail.
- 6- **The packet bytes pane:** displays the data from the packet selected in the packet list pane, and highlights the field selected in the packet details pane.
- 7- **The status bar:** shows some detailed information about the current program state and the captured data.

The “packet list” pane

The packet list pane displays all the packets in the current capture file.

No.	Time	Source	Destination	Protocol	Length	Info
318	2.497058	10.22.64.111	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
319	2.511542	10.22.64.36	10.22.67.255	NBNS	92	Name query NB WPAD<00>
320	2.535437	10.22.64.36	239.255.255.250	SSDP	212	M-SEARCH * HTTP/1.1
321	2.566127	10.22.64.111	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
322	2.600142	10.22.64.113	10.22.67.255	UDP	60	2008 → 2008 Len=15
323	2.600142	10.22.64.113	10.22.67.255	UDP	60	2007 → 2007 Len=15
324	2.601809	10.22.64.71	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
325	2.626423	10.22.65.7	239.255.255.250	SSDP	143	M-SEARCH * HTTP/1.1
326	2.628929	10.22.64.239	10.22.67.255	NBNS	110	Registration NB IUG<le>
327	2.633322	10.22.64.71	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
328	2.652845	10.22.65.80	10.22.67.255	NBNS	92	Name query NB WPAD<00>
329	2.678536	HewlettP_57:ba:58	Broadcast	ARP	60	who has 10.22.64.24? Tell 10.22.65.24
330	2.708081	10.22.64.113	10.22.67.255	UDP	60	2008 → 2008 Len=15
331	2.708250	10.22.64.113	10.22.67.255	UDP	60	2007 → 2007 Len=15
332	2.717605	IntelCor_c5:68:84	Broadcast	ARP	60	who has 10.22.65.88? Tell 10.22.64.201
333	2.759130	10.22.64.81	10.22.67.255	NBNS	92	Name query NB WPAD<00>
334	2.810308	10.22.64.47	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
335	2.816462	10.22.64.113	10.22.67.255	UDP	60	2008 → 2008 Len=15

The “packet details” pane

The packet details pane shows the current packet (selected in the “packet list” pane) in more detail form.

> Frame 10776: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{D25CB100-5B84-48A4-BCB6-27E43BE220F9}, id 0
> Ethernet II, Src: Micro-St_45:de:29 (44:8a:5b:45:de:29), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.22.64.113, Dst: 10.22.67.255
> User Datagram Protocol, Src Port: 2008, Dst Port: 2008
Source Port: 2008
Destination Port: 2008
Length: 23
Checksum: 0x8192 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
> [Timestamps]
UDP payload (15 bytes)
> Data (15 bytes)

The “packet bytes” pane

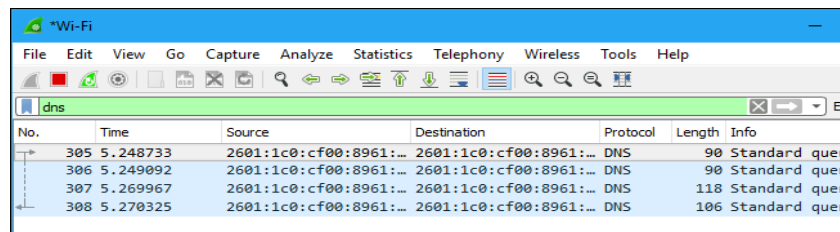
The packet bytes pane shows the data of the current packet (selected in the “packet list” pane) in hex dump style.

0000	ff ff ff ff ff ff 44 8a	5b 45 de 29 08 00 45 00	D- [E-)--E-
0010	00 2b 83 22 00 00 00 11	1f 04 0a 16 40 71 0a 16	..+.".....@q..
0020	43 ff 07 d8 07 d8 00 17	81 92 42 43 20 31 30 6d	C-----..BC 10m
0030	73 69 32 33 34 32 30 31	39 00 00 00	siz34201 9...

Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



Wireshark filters use key phrases, such as the following:

<code>ip.addr</code>	Specifies an IPv4 address
<code>ipv6.addr</code>	Specifies an IPv6 address
<code>src</code>	Source - where the packet came from
<code>dst</code>	Destination - where the packet is going

You can also use the following values:

<code>&&</code>	Means "and," as in, "Choose the IP address of 192.168.2.1 and 192.168.2.2"
<code>==</code>	Means "equals," as in "Choose only IP address 192.168.2.1"
<code>!</code>	Means "not," as in, do not show a particular IP address or source port

Example: let's say you want to see packets that have only the IP address of 18.224.161.65 somewhere inside. You would create the following command line, and put it into the Filter window: `ip.addr == 18.224.161.65`

Additional Filter Examples:

<code>tcp.port==8080</code>	Filters packets to show a port of your own choosing – in this case, port 8080
<code>!(ip.src == 162.248.16.53)</code>	Shows all packets except those originating from 162.248.16.53
<code>!(ipv6.dst == 2607:f8b0:400a:15::b)</code>	Shows all packets except those going to the IPv6 address of 2607:f8b0:400a:15::b
<code>ip.addr == 192.168.4.1 && ip.addr == 192.168.4.2</code>	Shows both 192.168.4.1 and 192.168.4.2
<code>http.request</code>	Shows only http requests – useful when troubleshooting or visualizing web traffic

Lab work

Part 1:

1. From PC setup Wireshark, from capture menu select interfaces then a list of network interfaces NIC will show, select the interface that connected to the network you want to sniff.
2. Click start to start sniffing (analyse the packets) , in this case sniffing tool will capture any packet and analyse it.

The analysis result of the sniffing tool depend on the packet that captured and the protocol that create the packet , as an example if we deal with ARP protocol then the data will only in the lower layer (Physical, Data link , Network) and no other data because the ARP protocol work over Network layer as shown in figure1 ; another example is DNS packet the data that will displayed is in all layers (Physical ,Data link , Network , Transport, and Application).

Part 2:

Access <http://www.techpanda.org/> then capture and analyze the login packets.

Example: Let us discuss an example of analysing a captured packet (DNS example) ; the result of the analysing will be displayed in the middle panel of the Wireshark :

1. The first layer displays the Physical layer data.
2. The second layer shows the MAC address for the sender and receiver if available otherwise it gives the MAC of the gateway for the sniffed machine.
3. Third layer shows the Network layer, the data in this layer is packet: it contains the source ip address and destination ip address, the internet protocol version i.e., IPv4 or IPv6, checksum and other related information to this layer.
4. Next layer displays the Transport layer (TCP or UDP), it displays source and destination ports and other related information.
5. The last thing is the upper layer protocols, this data in this layer depends on the protocols that initialize the packet, as in our example the data here is related to DNS (Domain Name Service), as shown in figures below.

