Network Analysis

Network analysis is a method used to

- study the relationships between entities in a network.
- analyze the connections, or links, between the entities.
- study a wide range of systems, including social networks, transportation networks.
- identify the most efficient routes between destinations.
- identify bottlenecks or other issues that may affect the performance of the network.

Why Network Analysis?

- Performance problems
- Analyze application behaviors
- Troubleshooting
- Locate and detect security breaches (الإختراقات الأمنية)

❖ use the network of **social media** users as an example. Analyzing this network helps in

- Identifying the most influent person/people in a group
- Defining characteristics of groups of users
- Prediction of suitable items for users

Network Analysis using Wireshark

Wireshark

- Is a powerful Network/packet analyzer tool or Network/packet sniffer tool
- Free and open source.
- allowing you to capture and analyze network traffic.
- break down packets of data being transferred across different networks. The user can search and filter for specific packets of data and analyze how they are transferred across their network.

Wireshark Core Features

- **Capture live packet data**
- **Import packets from text files**
- **View packet data and protocol information**
- **Save captured packet data**
- **Display packets**
- **Filter packets**
- **Search packets**
- **Colorize packets**
- **Generate Statistics**

When should Wireshark be used?

Wireshark helps:

- Network administrators troubleshoot problems across a network
- Security engineers examine security issues across a network
- QA engineers verify applications
- Developers debug protocol implementations
- Network users learn about a specific protocol

windows packet capture WinPcap / Npcap

- A software component added to the OS
- open-source library used to capture live network traffic; Without this component you will only be able to open saved capture files.

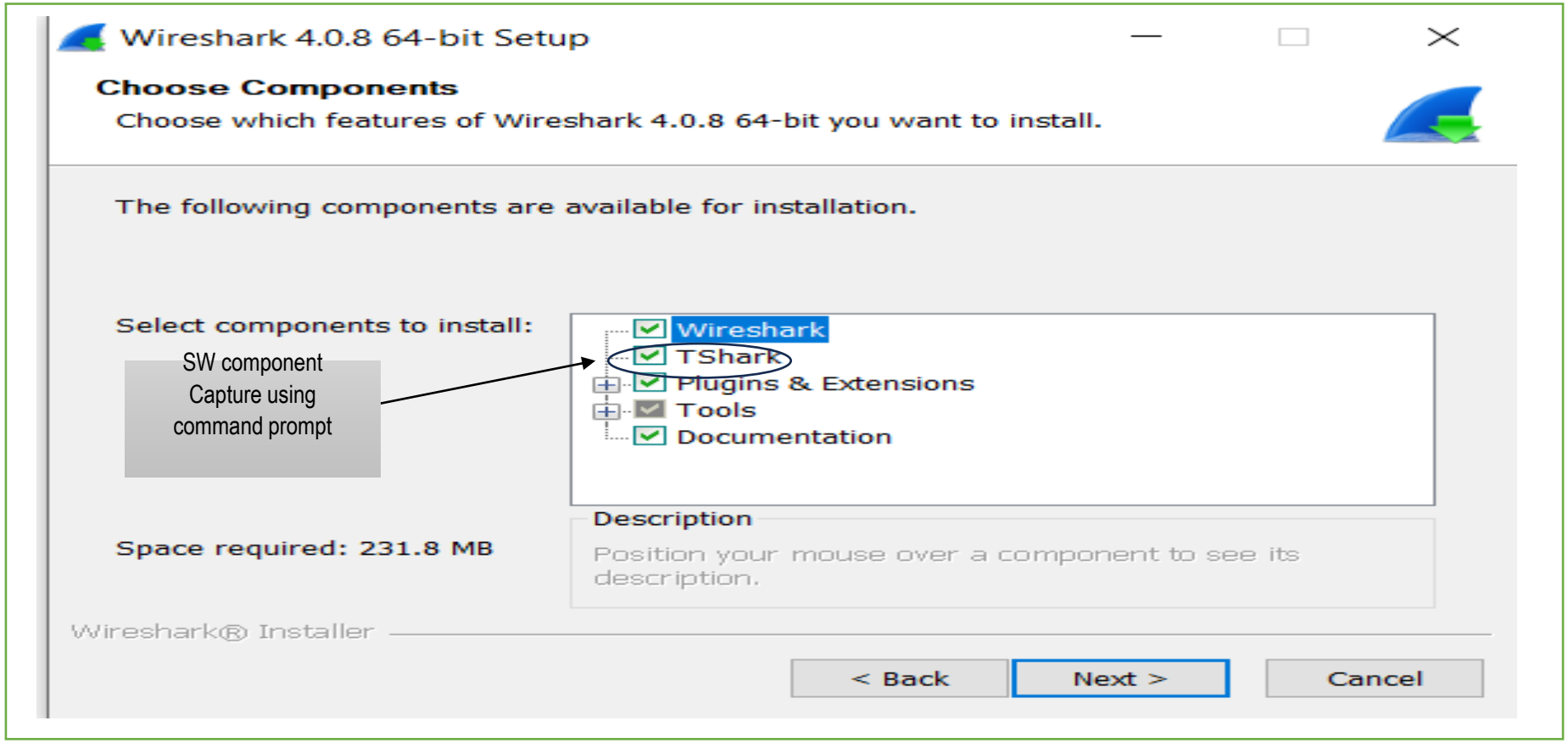
Software requirements: - Wireshark is a Cross platform

- support any version of Windows
- supports macOS
- runs on most Unix and Linux

Install Wireshark on Windows

- download and install WinPcap on your computer.

- download and install Wireshark on your computer.



SECTION 1

Capturing data packets on Wireshark

capture network traffic

1. start capture network traffic
2. how to capture dual/ two network interface
3. how to save network traffic
4. how to open saved traffic files

save network traffic

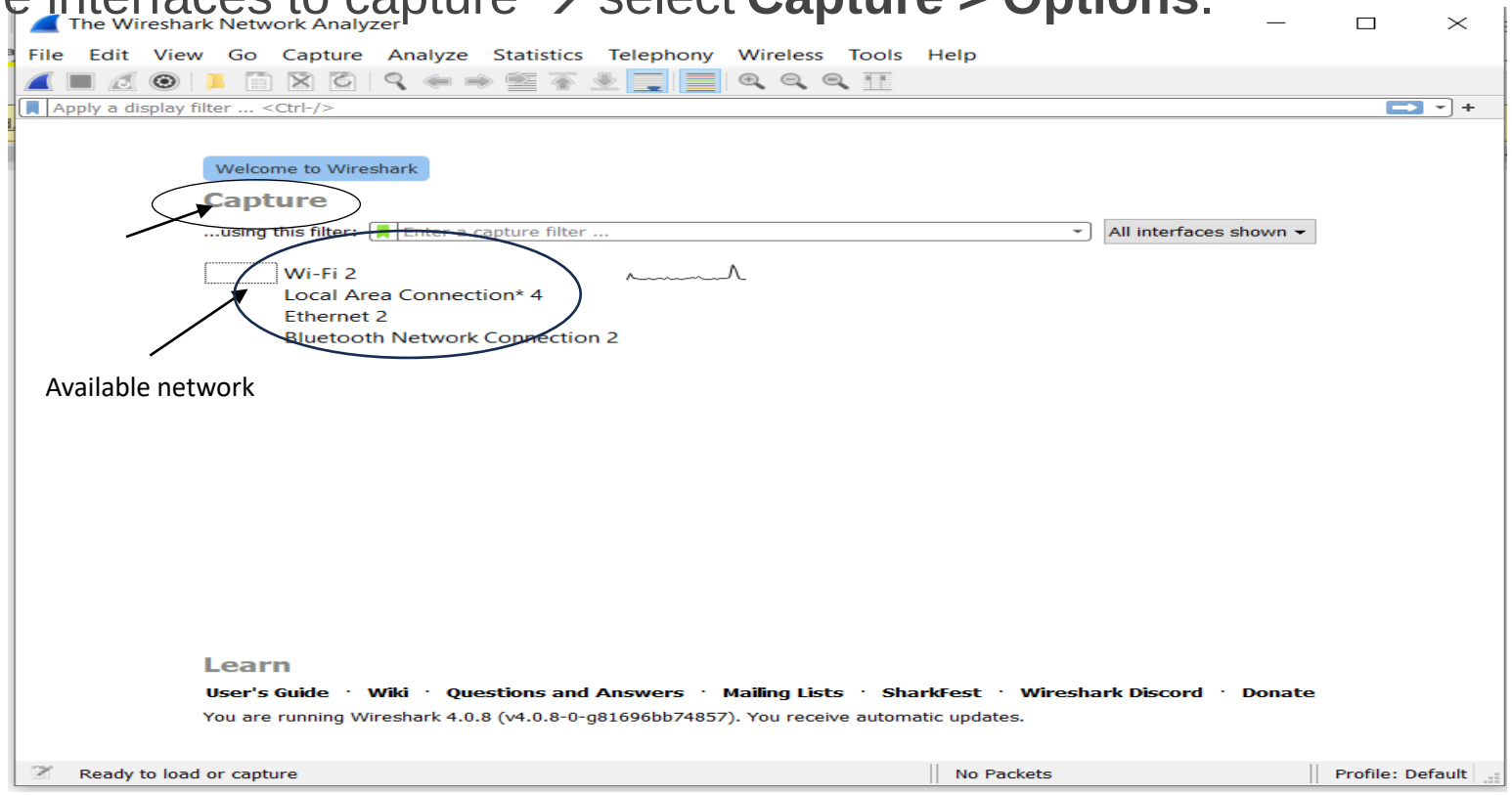
file → save as → name the file → extension of the file (.pcpng) → close the file.

pcpng→ packet capture next generation.

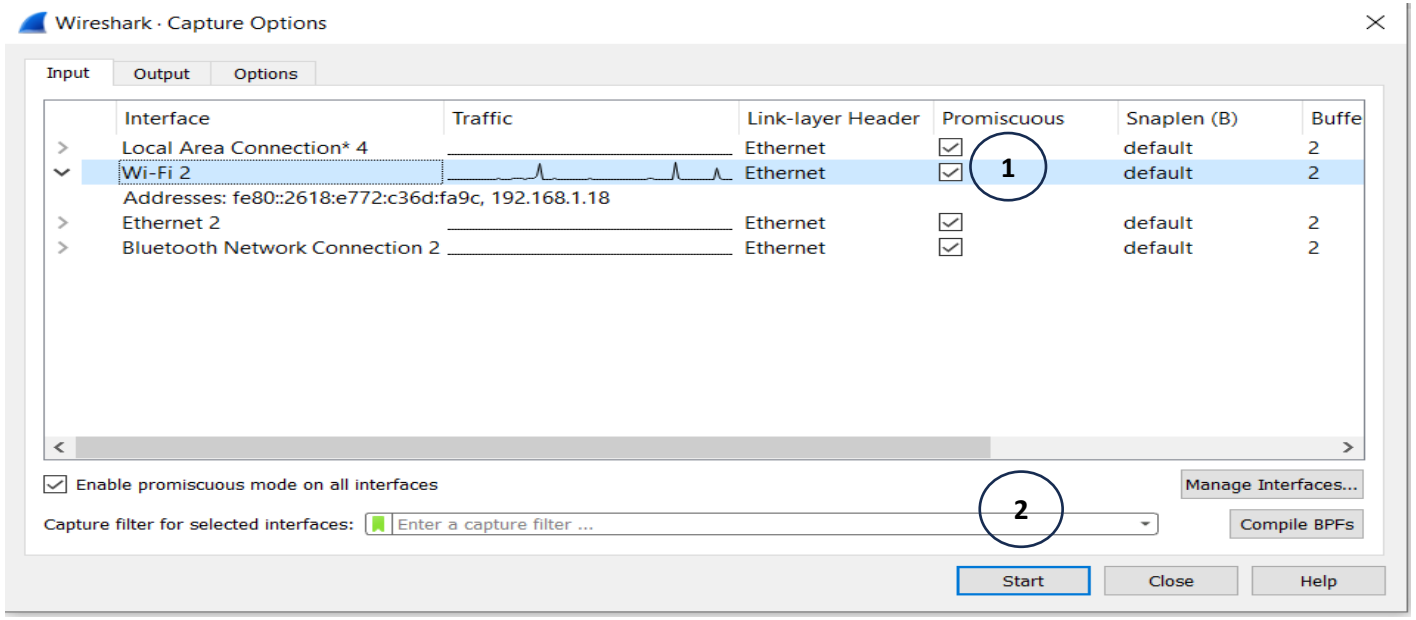
start capture network traffic

A. capture data from one source / multiple sources.

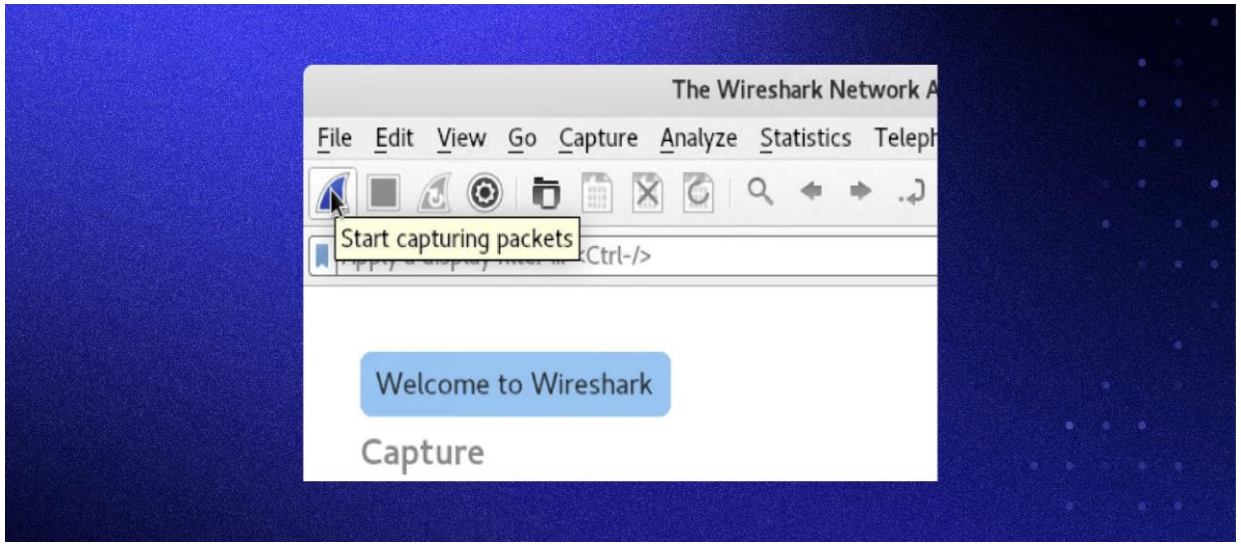
look available interfaces to capture → select **Capture > Options**.



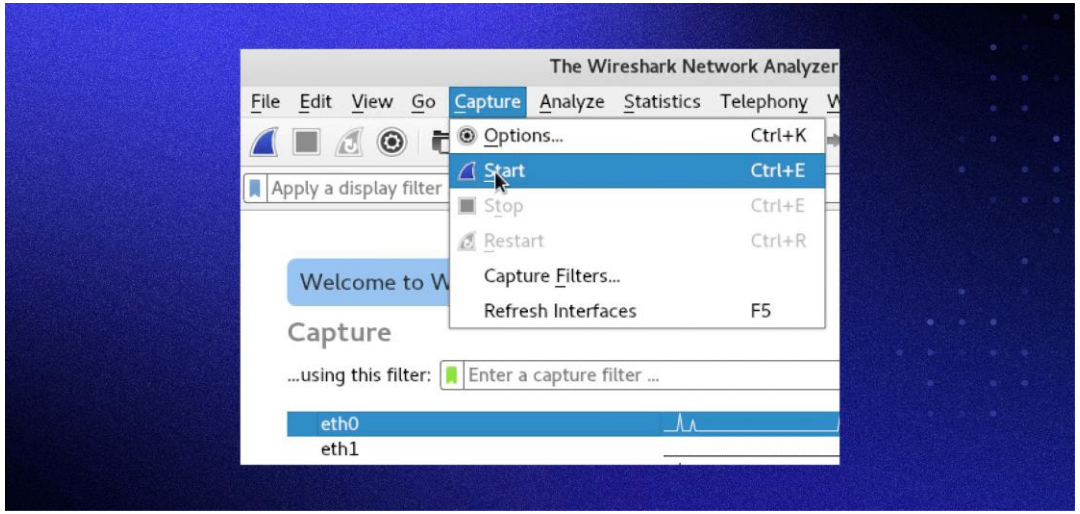
Check the box of the interface you want to capture and press the **Start** button to start

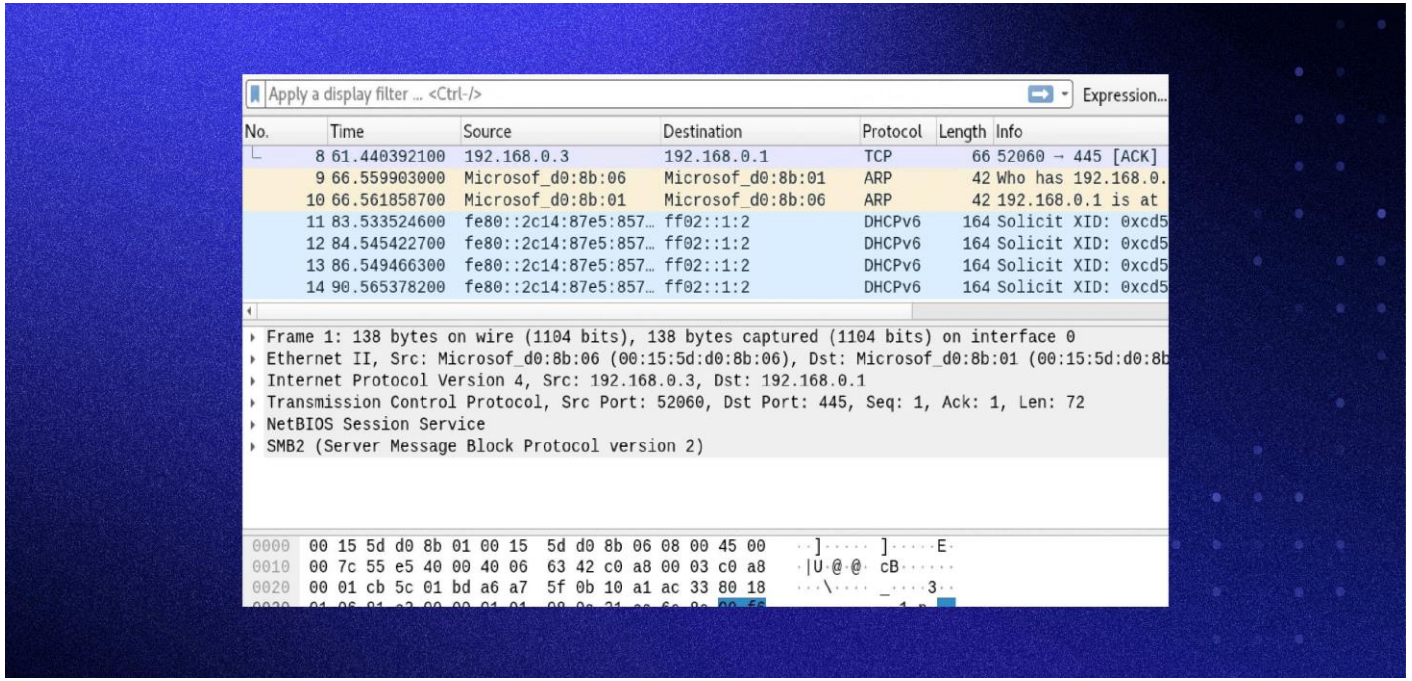


Click the first button on the toolbar, titled "Start capturing packets."



You can select the menu item Capture -> Start.





Analyzing data packets on Wireshark

No.: This is the number order of the packet captured. The bracket indicates that this packet is part of a conversation.

Time: This column shows how long after you started the capture this particular packet was captured. You can change this value in the Settings menu to display a different option.

Source: This is the address of the system that sent the packet.

Destination: This is the address of the packet destination.

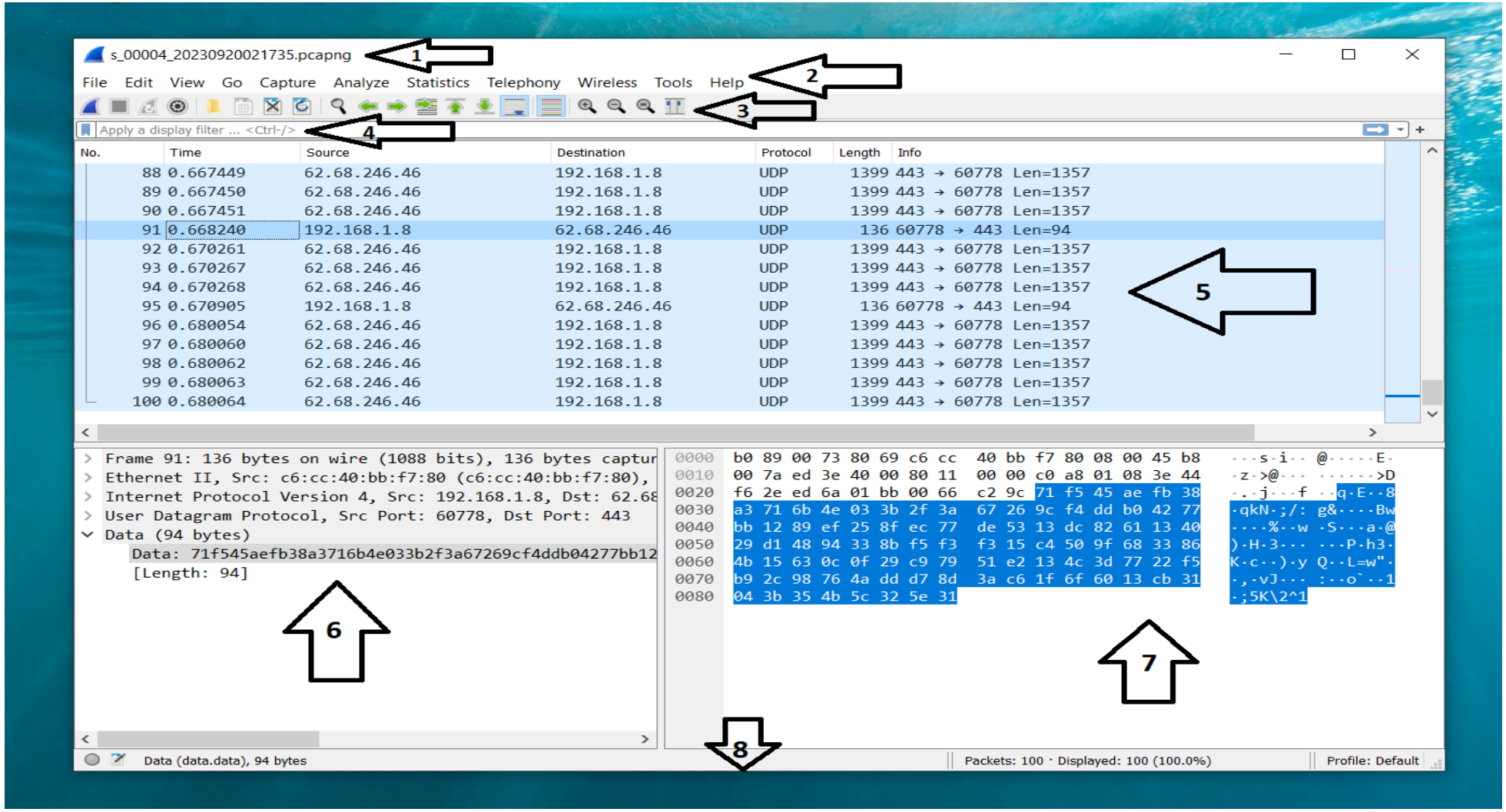
Protocol: This is the type of packet. For example: TCP, DNS, DHCPv6, or ARP.

Length: This column shows you the packet's length, measured in bytes.

Info: This column shows you more information about the packet contents, which will vary depending on the type of packet.

SECTION 2

Explain Wireshark interface



1. The Title

first capture.pcapng

2. The Main Menu

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

3. The "Main" Toolbar

4. The "Filter" Toolbar

A syntax check of your filter string is done while you are typing. The background will turn **red** if you enter an invalid string, and will become **green** when you enter a valid string.

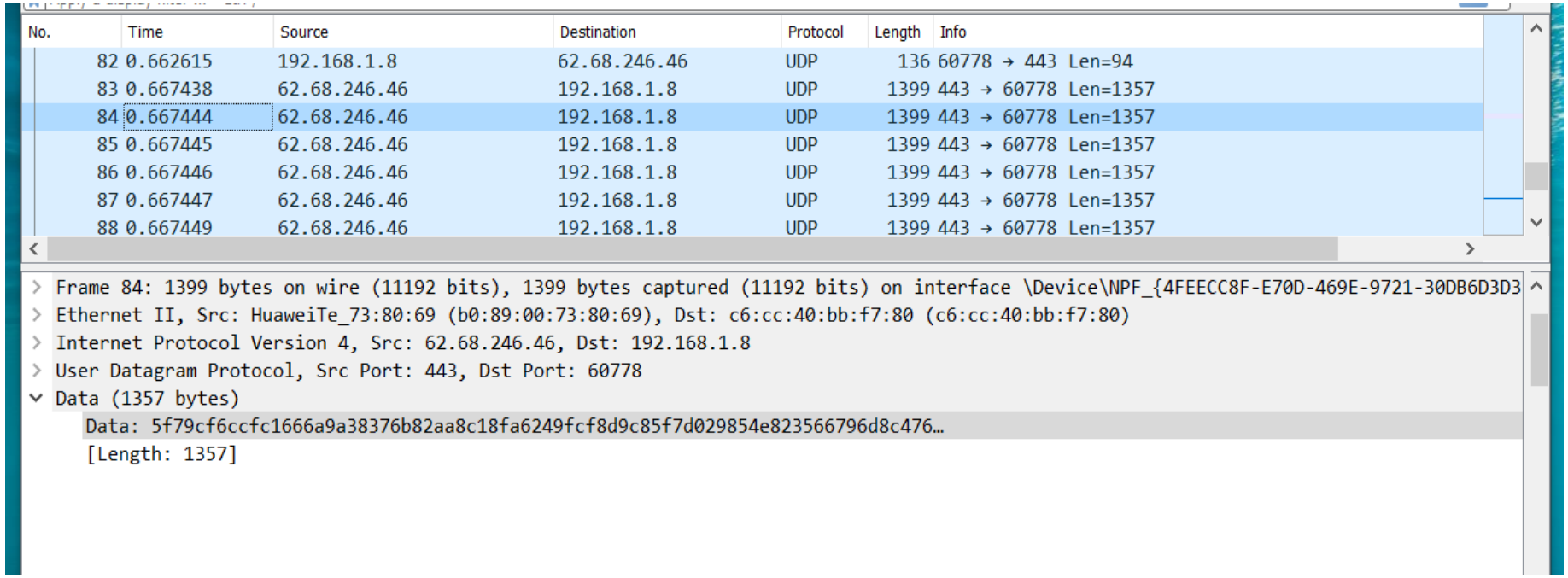
5. The “Packet List” Pane

No.	Time	Source	Destination	Protocol	Length	Info
88	0.667449	62.68.246.46	192.168.1.8	UDP	1399	443 → 60778 Len=1357
89	0.667450	62.68.246.46	192.168.1.8	UDP	1399	443 → 60778 Len=1357
90	0.667451	62.68.246.46	192.168.1.8	UDP	1399	443 → 60778 Len=1357
91	0.668240	192.168.1.8	62.68.246.46	UDP	136	60778 → 443 Len=94
92	0.670261	62.68.246.46	192.168.1.8	UDP	1399	443 → 60778 Len=1357
93	0.670267	62.68.246.46	192.168.1.8	UDP	1399	443 → 60778 Len=1357
94	0.670268	62.68.246.46	192.168.1.8	UDP	1399	443 → 60778 Len=1357
95	0.670905	192.168.1.8	62.68.246.46	UDP	136	60778 → 443 Len=94
96	0.680054	62.68.246.46	192.168.1.8	UDP	1399	443 → 60778 Len=1357
97	0.680060	62.68.246.46	192.168.1.8	UDP	1399	443 → 60778 Len=1357
98	0.680062	62.68.246.46	192.168.1.8	UDP	1399	443 → 60778 Len=1357
99	0.680063	62.68.246.46	192.168.1.8	UDP	1399	443 → 60778 Len=1357
100	0.680064	62.68.246.46	192.168.1.8	UDP	1399	443 → 60778 Len=1357

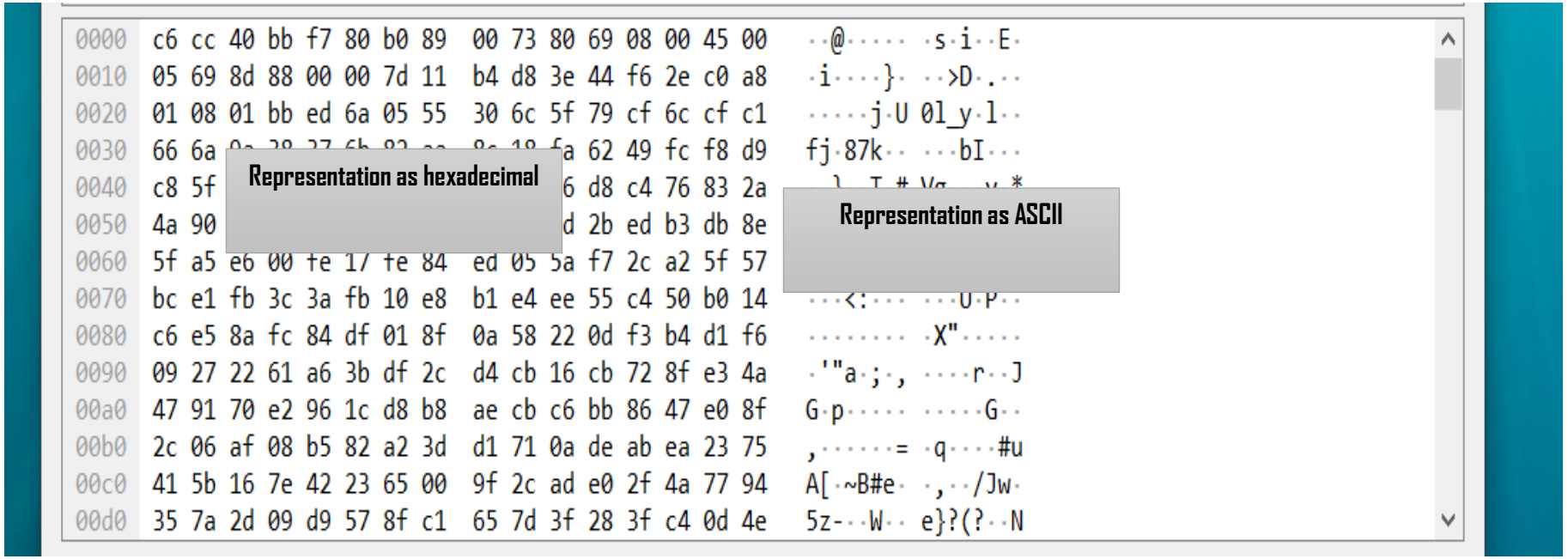
Each line in the packet list corresponds to one packet in the capture file. If you select a line in this pane, more details will be displayed in the “Packet Details” and “Packet Bytes” panes.

6. The “Packet Details” Pane

shows the current packet (selected in the “Packet List” pane) in a more detailed form.

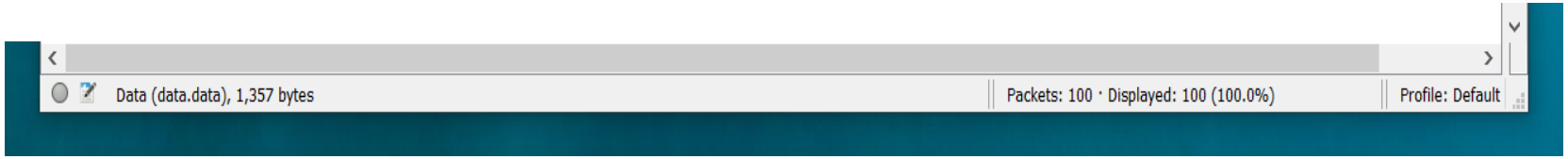


7. The “Packet Bytes” Pane



Each line contains the data offset, **sixteen hexadecimal** bytes, and **sixteen ASCII bytes**. Non-printable bytes are replaced with a period (“.”).

8. The Status bar



Packets: The number of captured packets.

Displayed: The number of packets currently displayed when using filter.

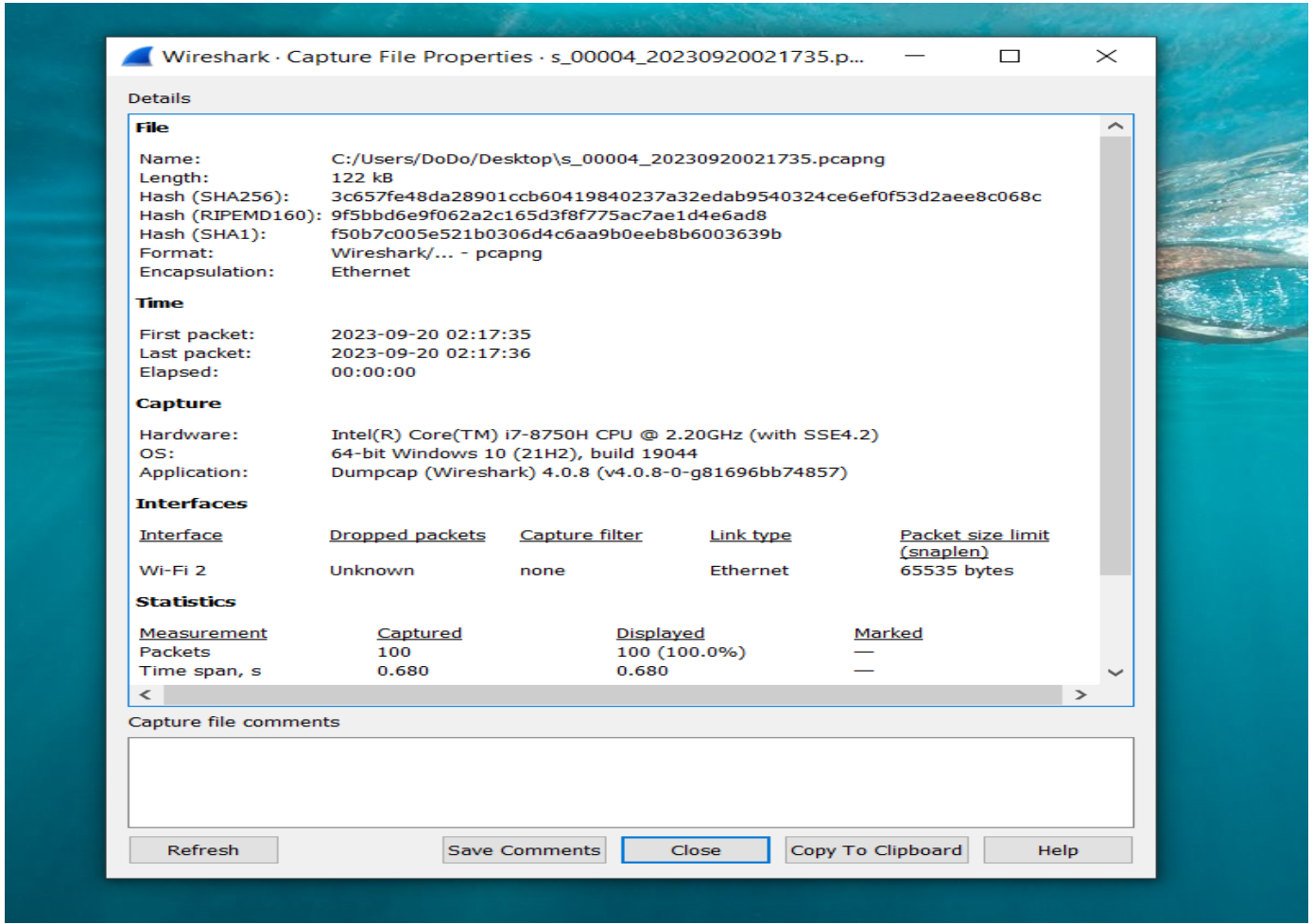
Profile: selecting from this list will change the configuration profile.

Capture File Properties

add a comment to the capture file , Show properties of capture file

Comment: Can be used to add a descriptive comment for the interface.

.pcapng → only support comment



SECTION 3

1) **Explain main toolbar**
2) **Save captured packets in more than one file**

Main toolbar items

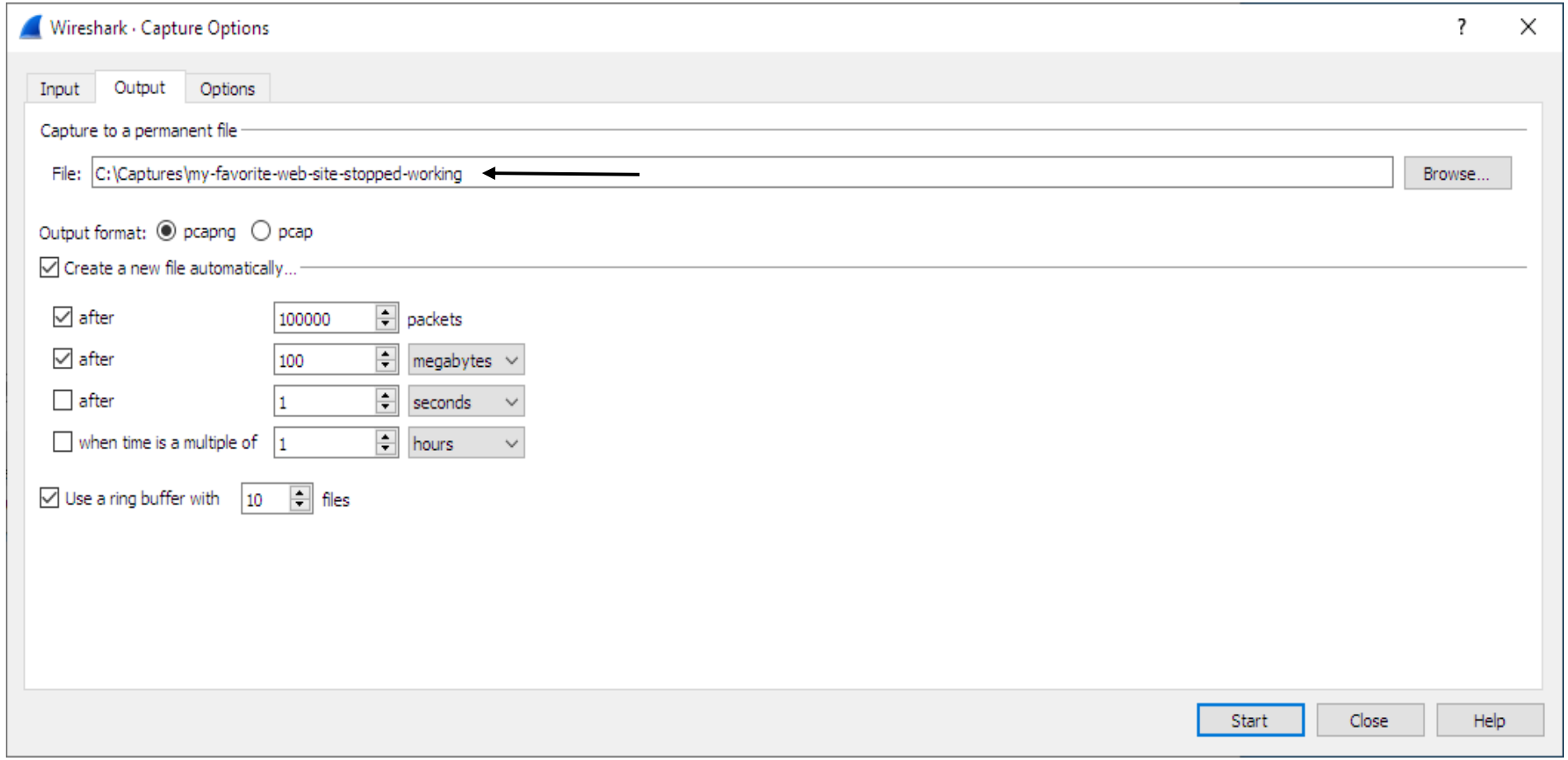
Toolbar Icon	Toolbar Item	Menu Item	Description
	Start	Capture → Start	Starts capturing packets
	Stop	Capture → Stop	Stops the currently running capture
	Restart	Capture → Restart	Restarts the current capture session.
	Options…	Capture → Options…	Opens the "Capture Options" dialog box.
	Open…	File → Open…	Opens the file open dialog box, which allows you to load a capture file for viewing.
	Save As…	File → Save As…	Save the current capture file to whatever file you would like.

Toolbar Icon	Toolbar Item	Menu Item	Description
	Open...	File → Open...	Opens the file open dialog box, which allows you to load a capture file for viewing.
	Save As...	File → Save As...	Save the current capture file to whatever file you would like.
	Close	File → Close	Closes the current capture. If you have not saved the capture, you will be asked to save it first.
	Reload	View → Reload	Reloads the current capture file.
	Find Packet...	Edit → Find Packet...	Find a packet based on different criteria.
	Go Back	Go → Go Back	Jump back in the packet history (previous packet)
	Go Forward	Go → Go Forward	Jump forward in the packet history (next packet)
	Go to Packet...	Go → Go to Packet...	Go to a specific packet.
	Go To First Packet	Go → First Packet	Jump to the first packet of the capture file.
	Go To Last Packet	Go → Last Packet	Jump to the last packet of the capture file.
	Auto Scroll in Live Capture	View → Auto Scroll in Live Capture	Auto scroll packet list while doing a live capture (or not).
	Colorize	View → Colorize	Colorize the packet list (or not).
	Zoom In	View → Zoom In	Zoom into the packet data (increase the font size).
	Zoom Out	View → Zoom Out	Zoom out of the packet data (decrease the font size).
	Normal Size	View → Normal Size	Set zoom level back to 100%.
	Resize Columns	View → Resize Columns	size columns, so **the** content fits into them.

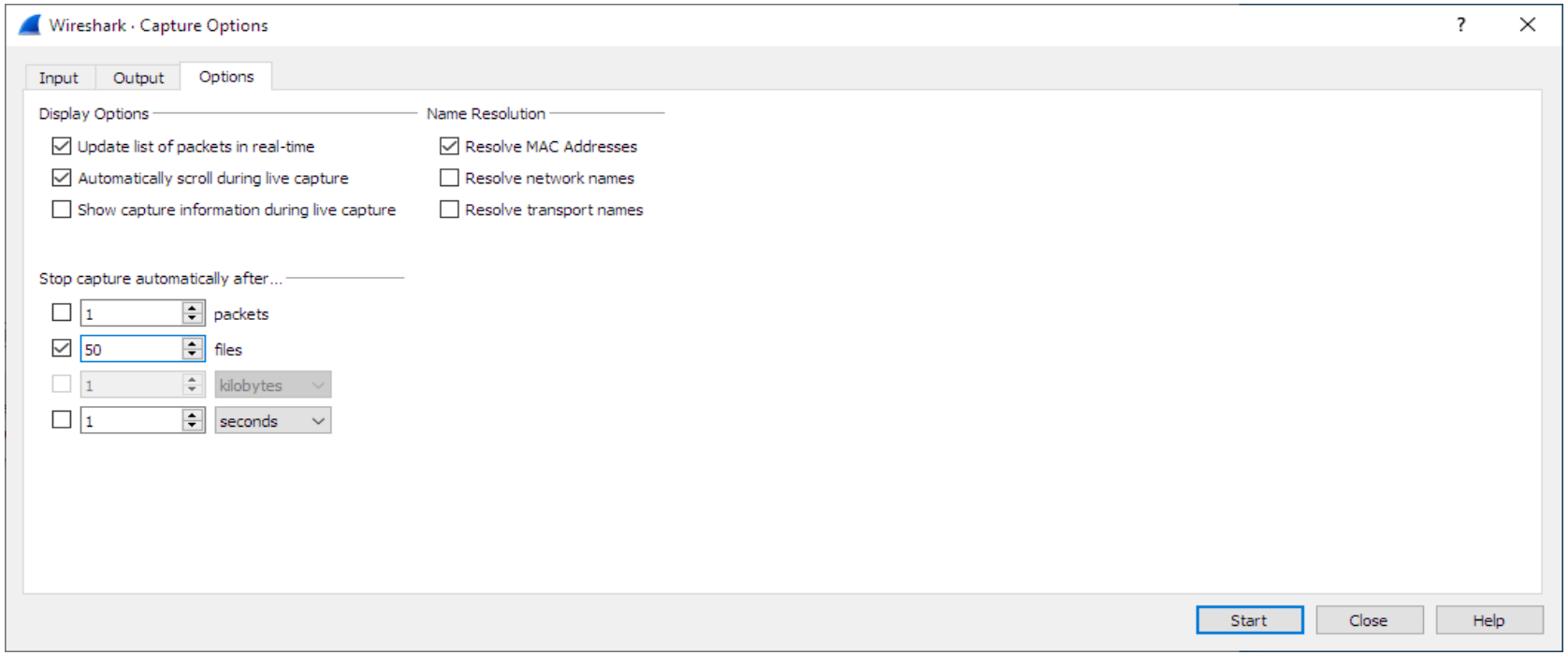
Save capture packet in more than one file

1.The “Capture Options” output tab

Set the format of the capture file**. pcapng** is the default

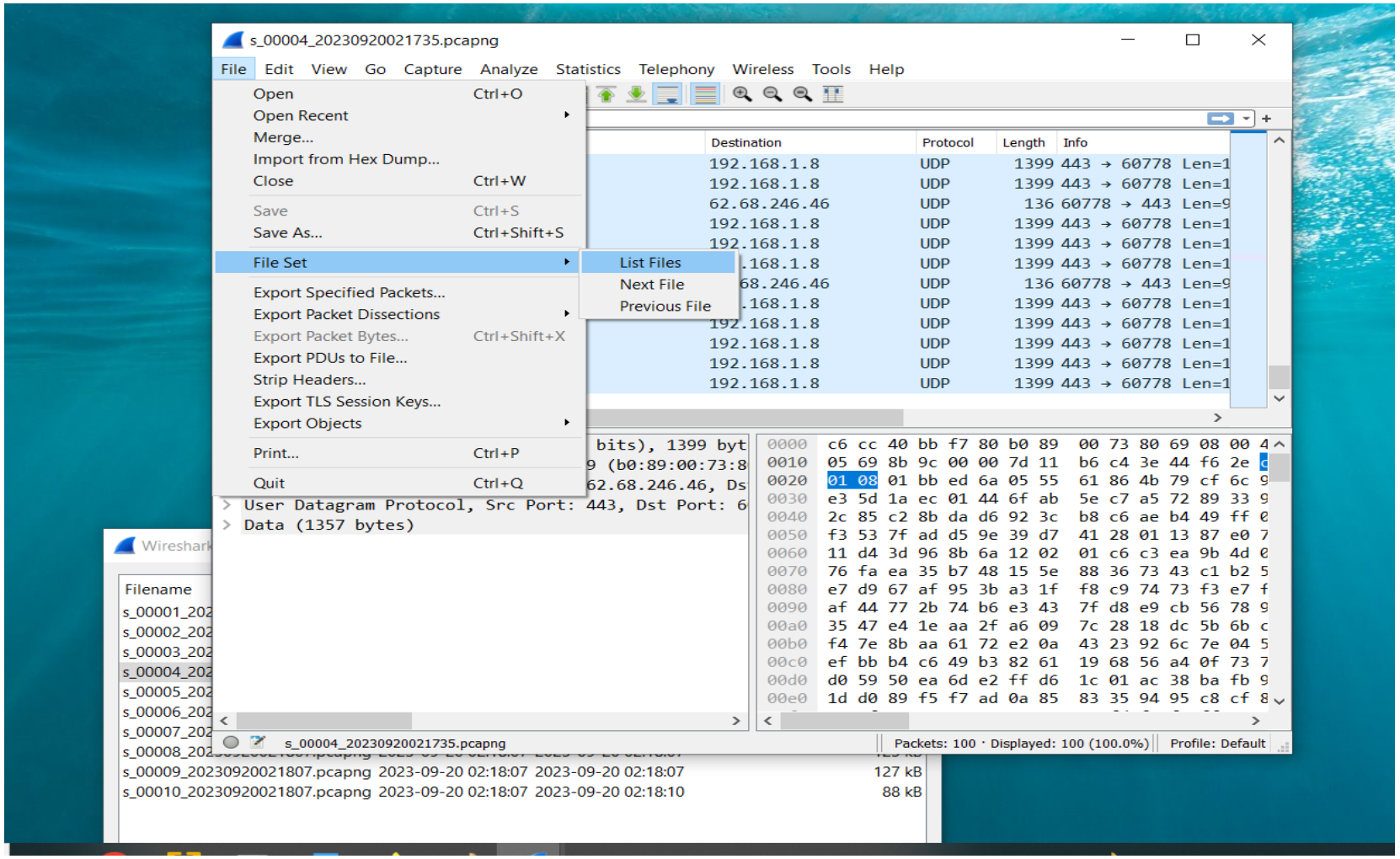


•The “Capture Options” options tab

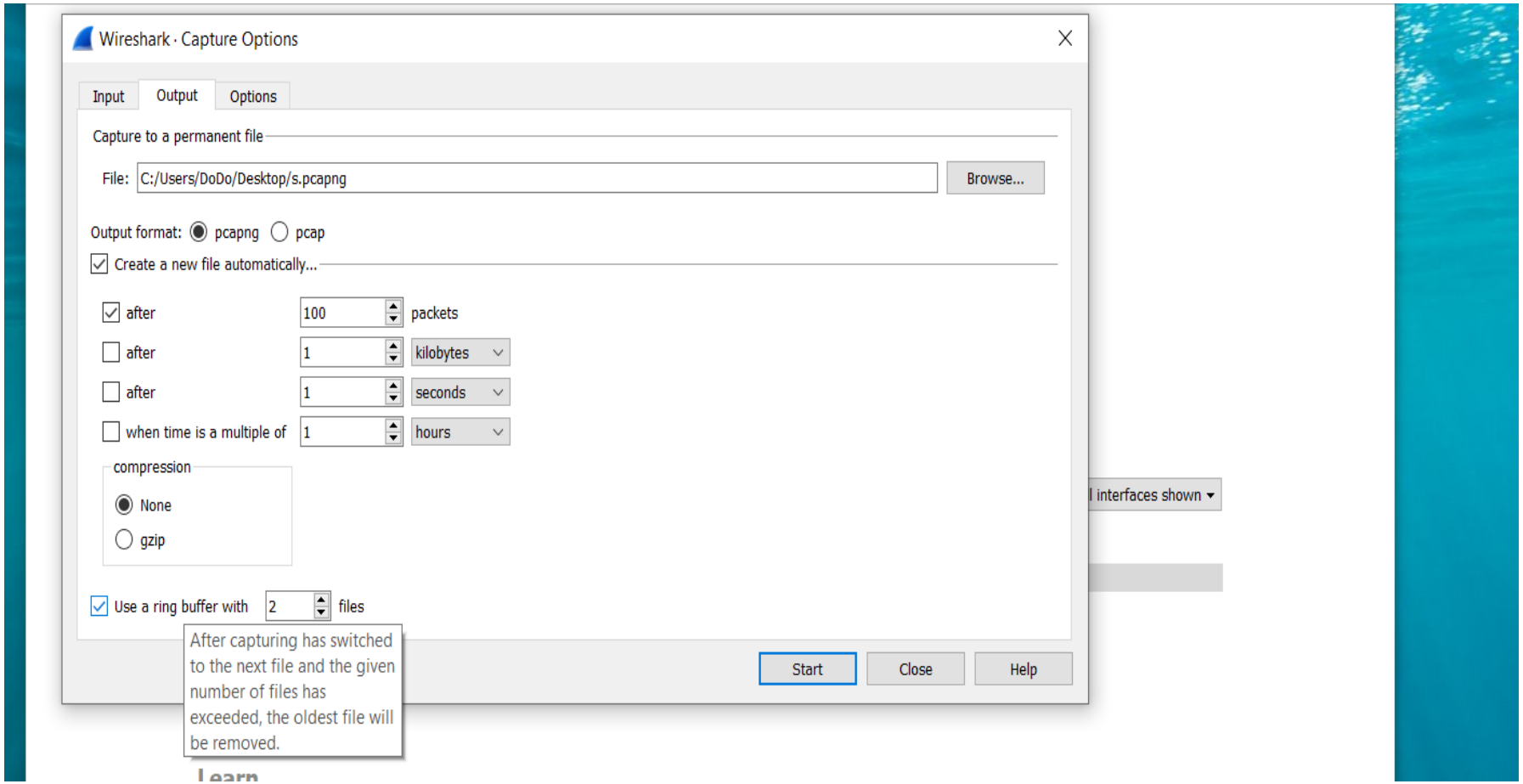


<u>Capturing can be stopped automatically based on the following conditions:</u>

- The number of packets in the capture file.
- The number of capture files.
- The capture file size.
- The capture file duration.



- **Show all created trace file after capturing.**



- **Multiple files, ring buffer**

  This will be a newly created file if value of “Ring buffer with n files” is not reached, otherwise it will replace the oldest of the formerly used files (thus forming a “ring”).

Remote Packet Capture Daemon

rpcapd → stands for **R**emote **P**acket **Cap**ture **D**aemon

used for capture packet remotely

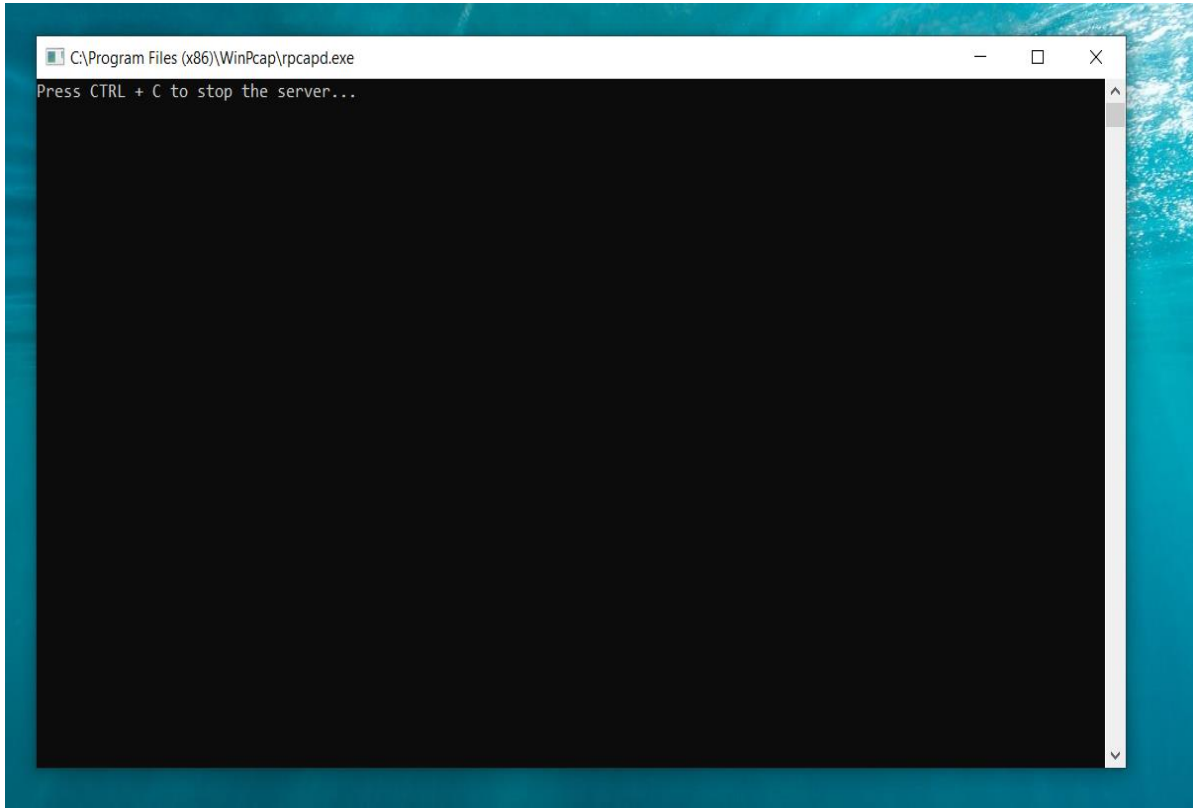
***rpcapd.exe* file** is a software component of *Remote Packet Capture Daemon*

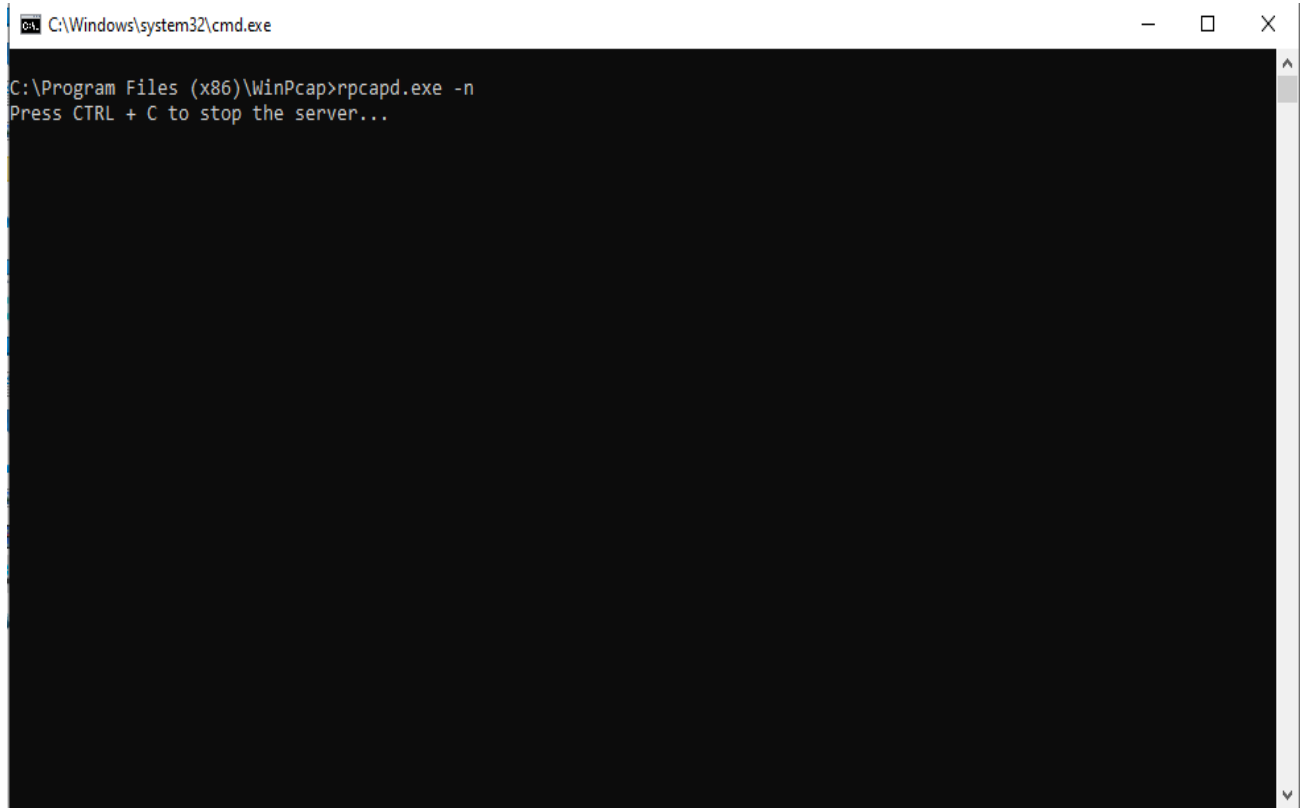
WinPcap is a packet sniffing tool that provides access to link-layer networks for Windows machines.

Rpcapd.exe is part of the WinPcap packet library.

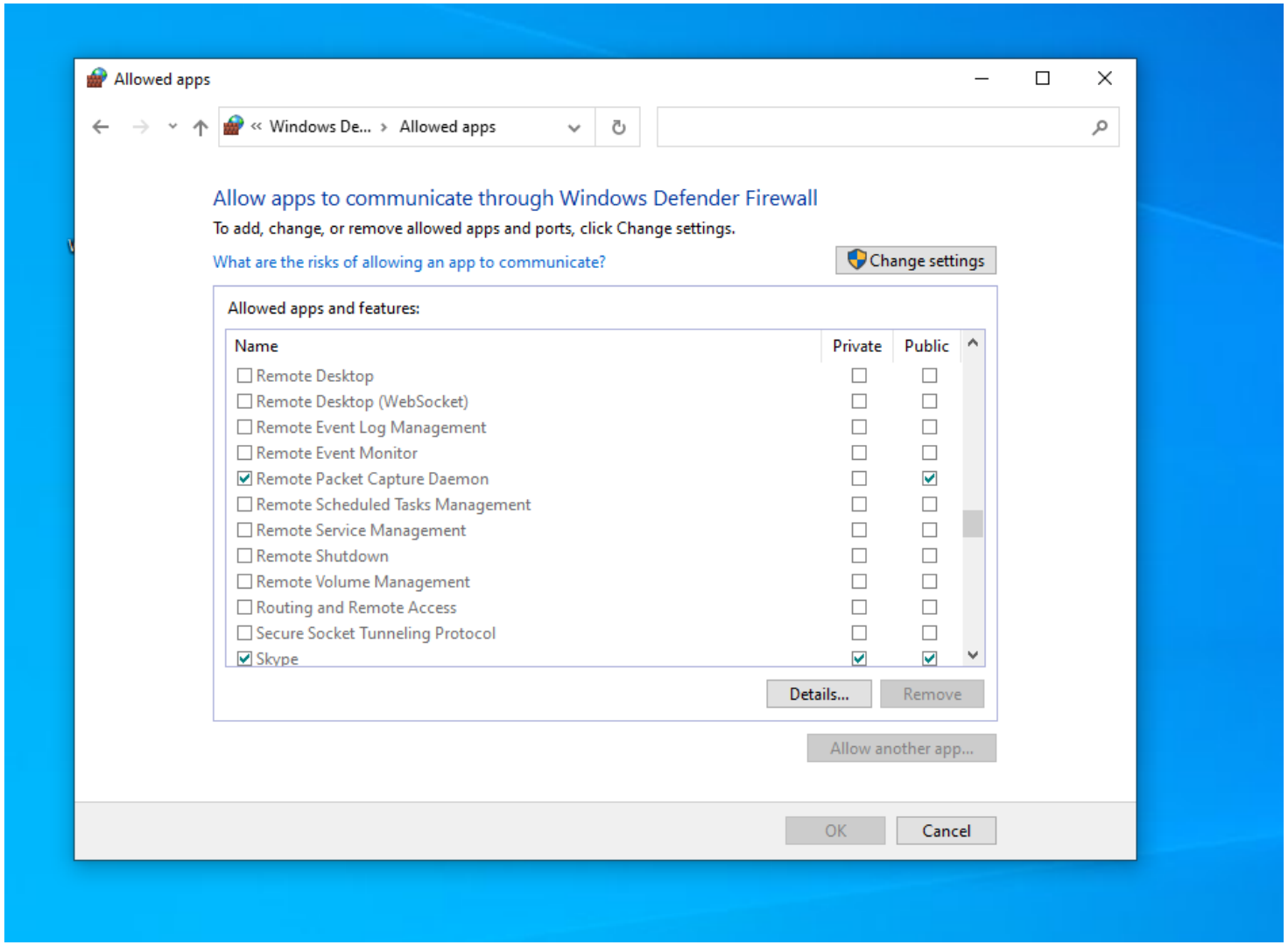
In the remote desktop

1. *Just install WinPcap to remote*
2. *C:\Program Files (x86)\WinPcap*
3. *Run rpcapd.exe.*
4. **Write this command in cmd to run null authentication and change the port→ rpcapd.exe -n –p 2004**



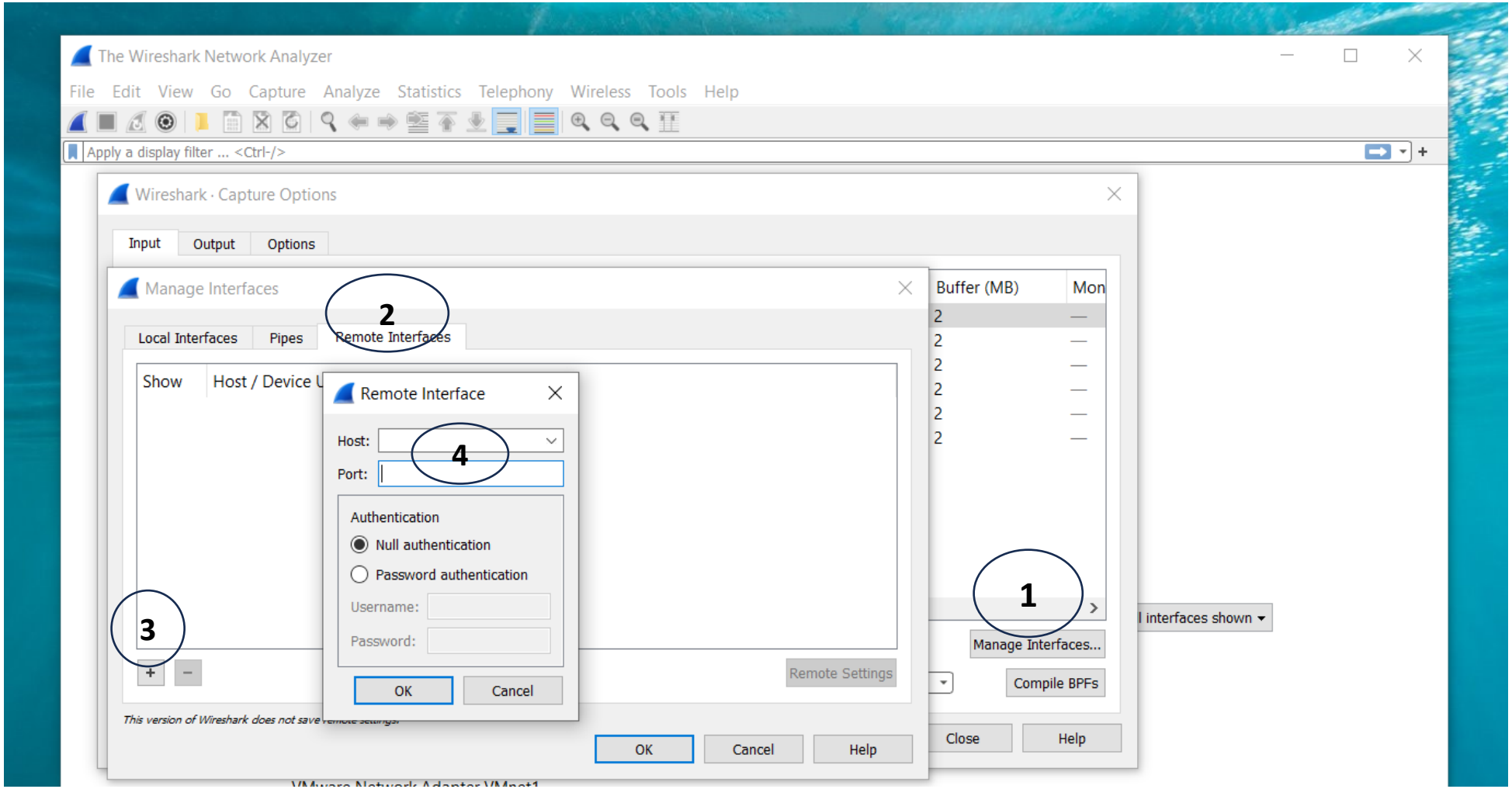


5. Goto Control Panel\All Control Panel Items\Windows Defender Firewall\Allowed apps → to allow daemon through firewall



In the captured desktop

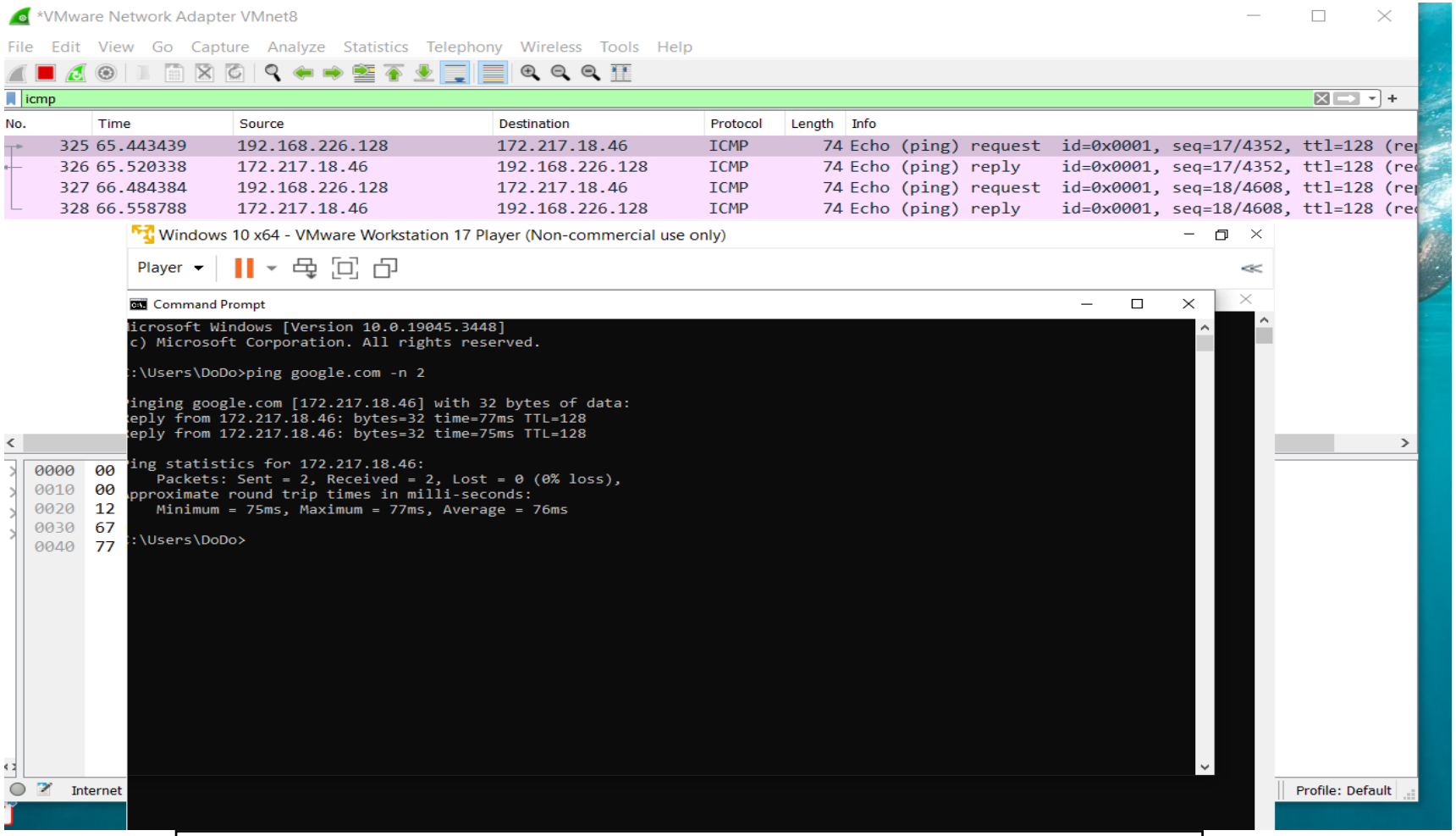
6. Open Wireshark to add the Ip address of remote desktop



7. In Wireshark Choose the remote desktop network and start capture

8. Open cmd in remote desktop and write ping google.com -n 2

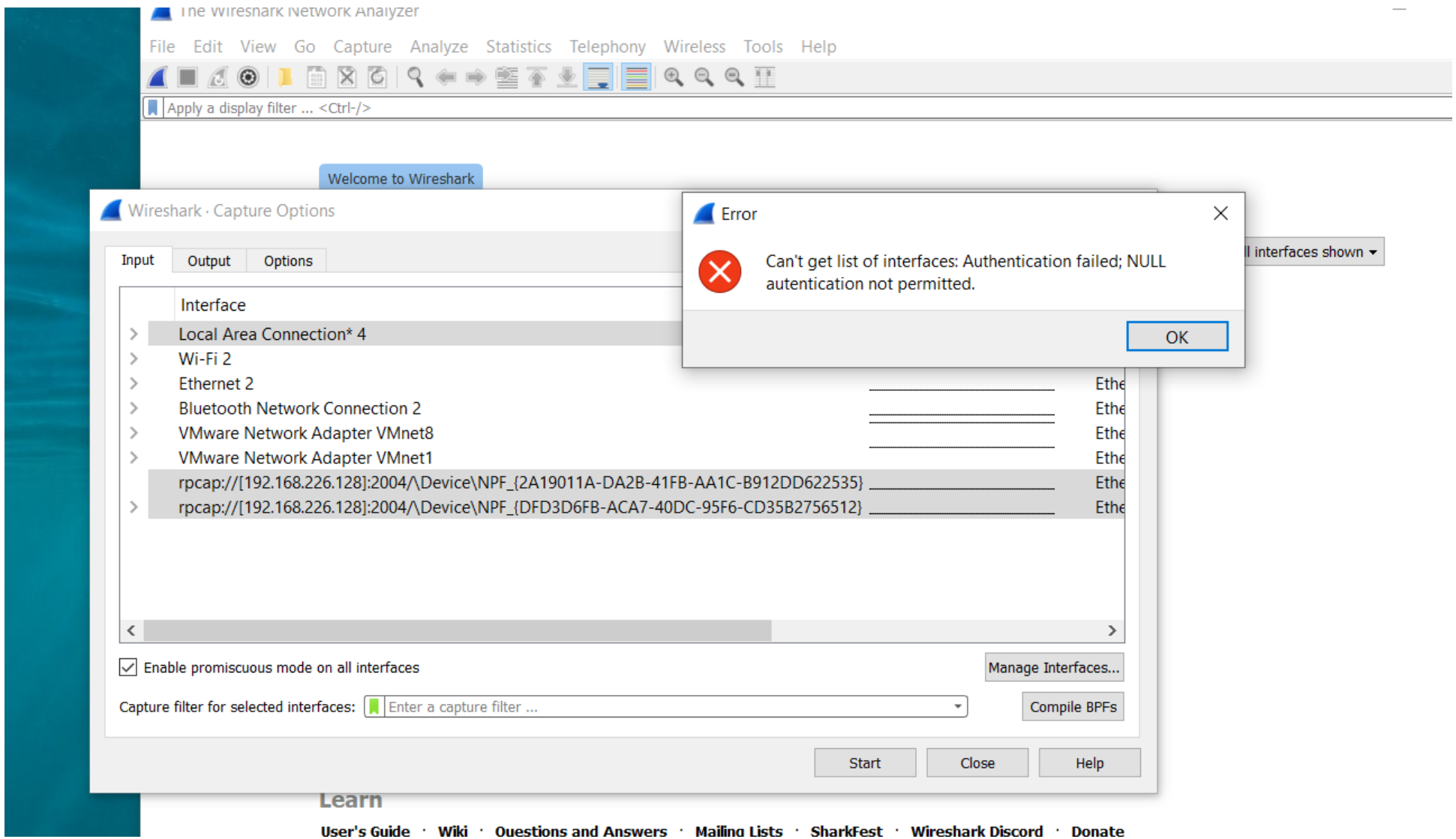
9. the Wireshark send two command pings of request and reply.



Icmp → ping protocol

Netstat.exe –n –p 2004 1 192.168.1.10,192.168.1.50,… → **determine Ip for remote connection**

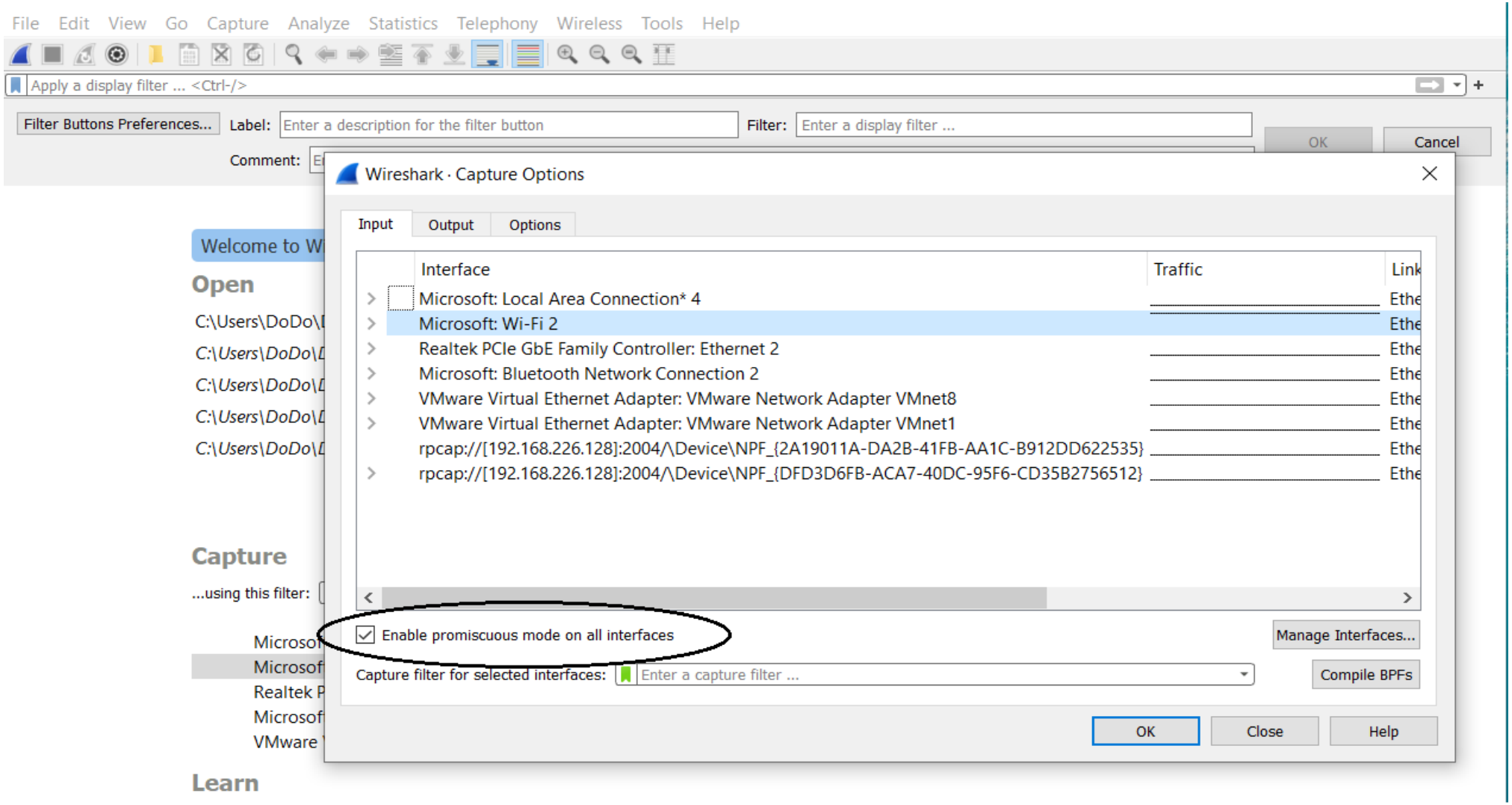
If not allowed for connection → return this message in Wireshark



What is promiscuous mode

Allows a network device to intercept and read each network packet

is a mode of operation in which every data packet transmitted can be received and read by a network adapter.



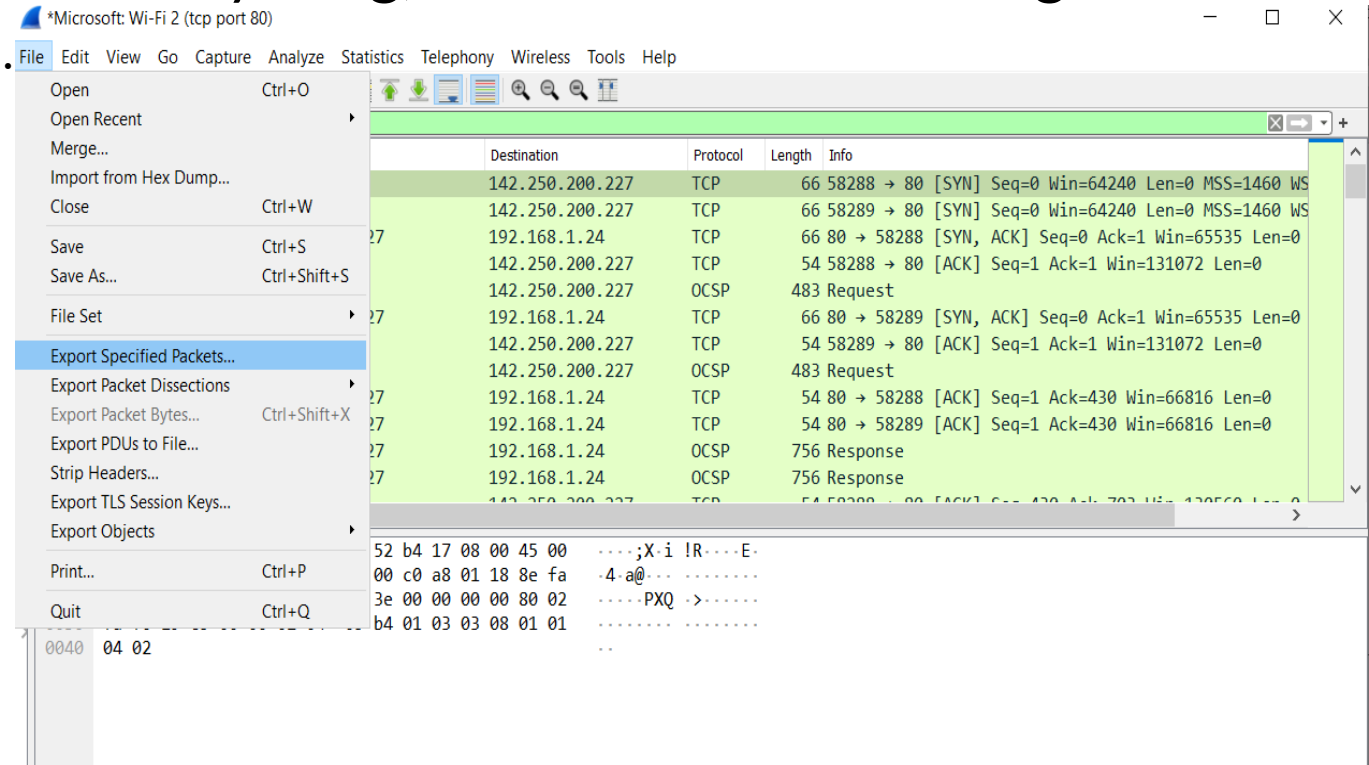
Filter in Wireshark

capture filters and display filters

Capture filters (like `tcp port 80`) are not to be confused with display filters (like `tcp.port = = 80`)

Capture filters :- only keep copies of packets that match the filter.

Display filters :- used when you've captured everything, but need to cut through the noise to analyze specific packets or flows.



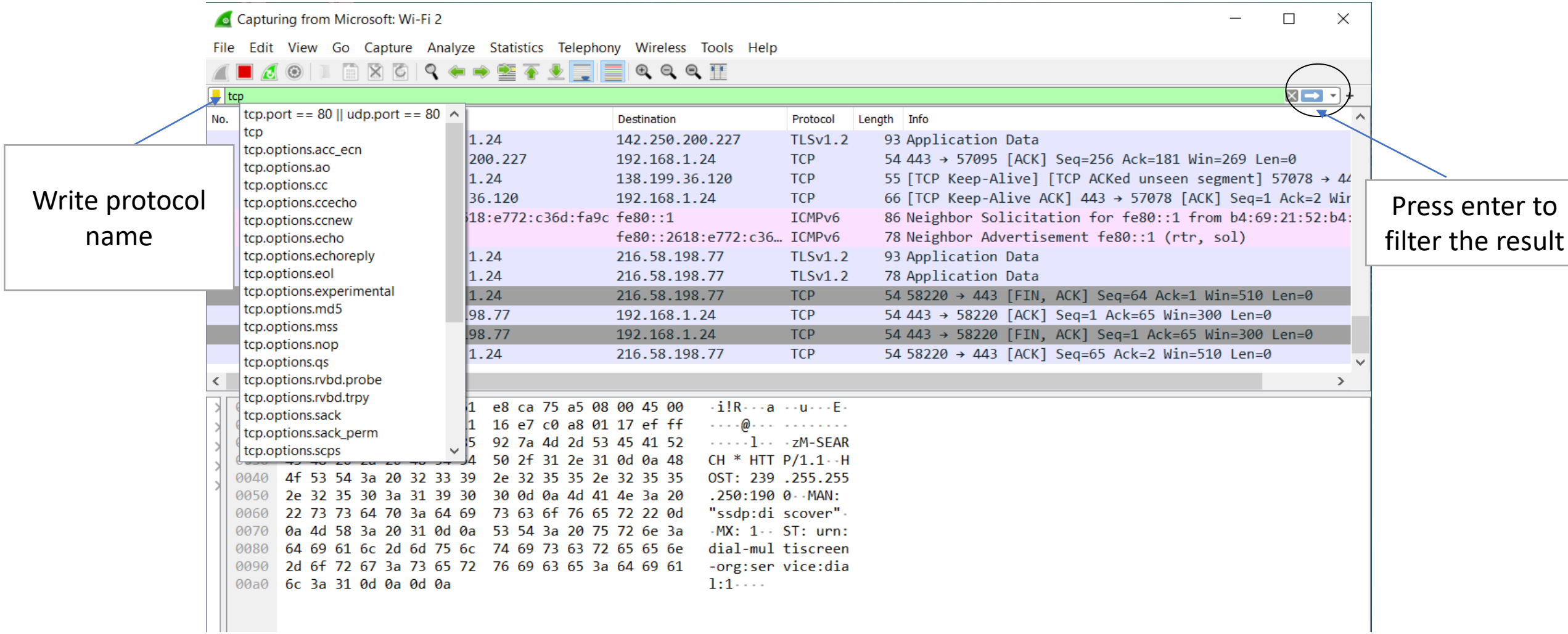
We can **save** the part of traffic when using filter

Stop filter → choose **file** menu **→ export specified packet → write the file name → save**

Display filters

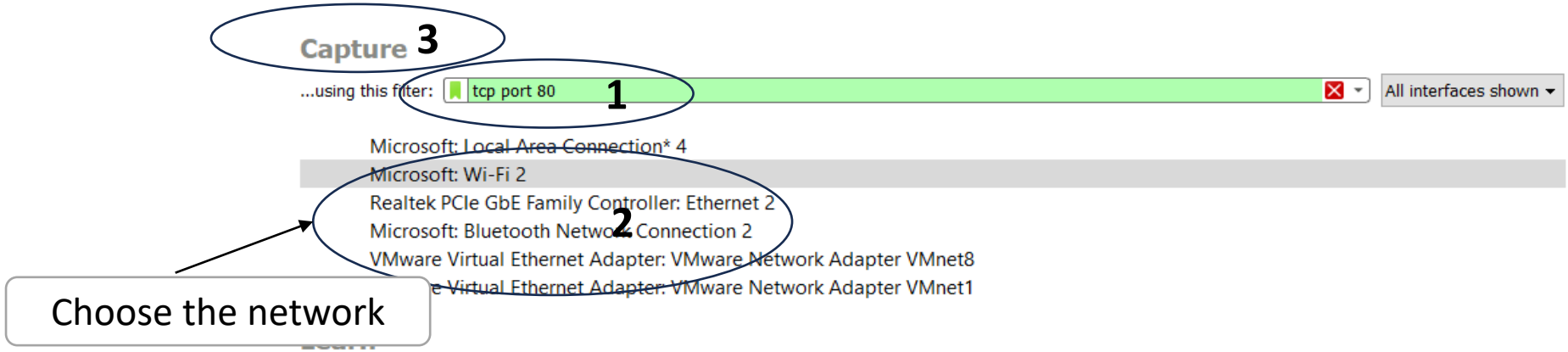
Capture then filter

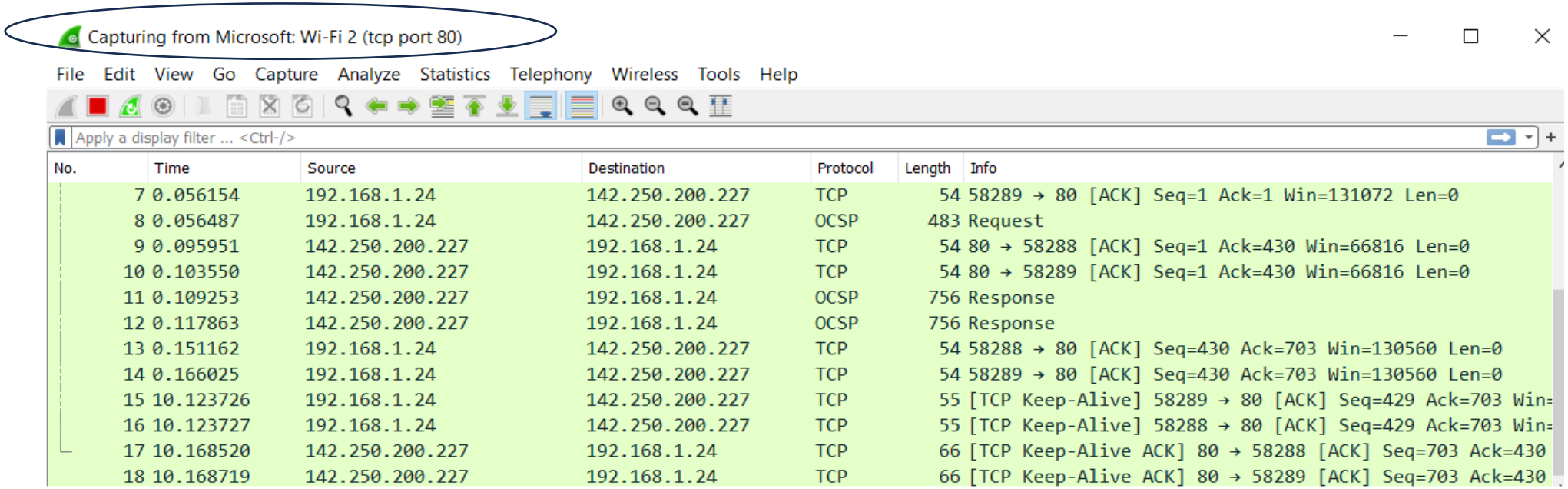
For example, to only display TCP packets, type tcp into Wireshark's display filter toolbar.



Capture filters

filter then Capture





No.	Time	Source	Destination	Protocol	Length	Info
7	0.056154	192.168.1.24	142.250.200.227	TCP	54	58289 → 80 [ACK] Seq=1 Ack=1 Win=131072 Len=0
8	0.056487	192.168.1.24	142.250.200.227	OCSP	483	Request
9	0.095951	142.250.200.227	192.168.1.24	TCP	54	80 → 58288 [ACK] Seq=1 Ack=430 Win=66816 Len=0
10	0.103550	142.250.200.227	192.168.1.24	TCP	54	80 → 58289 [ACK] Seq=1 Ack=430 Win=66816 Len=0
11	0.109253	142.250.200.227	192.168.1.24	OCSP	756	Response
12	0.117863	142.250.200.227	192.168.1.24	OCSP	756	Response
13	0.151162	192.168.1.24	142.250.200.227	TCP	54	58288 → 80 [ACK] Seq=430 Ack=703 Win=130560 Len=0
14	0.166025	192.168.1.24	142.250.200.227	TCP	54	58289 → 80 [ACK] Seq=430 Ack=703 Win=130560 Len=0
15	10.123726	192.168.1.24	142.250.200.227	TCP	55	[TCP Keep-Alive] 58289 → 80 [ACK] Seq=429 Ack=703 Win=
16	10.123727	192.168.1.24	142.250.200.227	TCP	55	[TCP Keep-Alive] 58288 → 80 [ACK] Seq=429 Ack=703 Win=
17	10.168520	142.250.200.227	192.168.1.24	TCP	66	[TCP Keep-Alive ACK] 80 → 58288 [ACK] Seq=703 Ack=430
18	10.168719	142.250.200.227	192.168.1.24	TCP	66	[TCP Keep-Alive ACK] 80 → 58289 [ACK] Seq=703 Ack=430