EXPERIMENT NO: 10

Note: Find the steps given in experiments to run the tools**.**

AIM: Wireshark

i. Packet Capture Using Wire shark
ii. Starting Wire shark
iii. Viewing Captured Traffic
iv. Analysis and Statistics & Filters.

Wireshark

What is Wireshark?

Wireshark is an open-source packet analyzer, which is used for **education, analysis, software development, communication protocol development, and network troubleshooting**.

It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a **sniffer, network protocol analyzer, and network analyzer**. It is also used by network security engineers to examine security problems.

Wireshark is a free to use application which is used to apprehend the data back and forth. It is often called as a free packet sniffer computer application. It puts the network card into an unselective mode, i.e., to accept all the packets which it receives.

Uses of Wireshark:

Wireshark can be used in the following ways:

1. It is used by network security engineers to examine security problems.
2. It allows the users to watch all the traffic being passed over the network.
3. It is used by network engineers to troubleshoot network issues.
4. It also helps to troubleshoot latency issues and malicious activities on your network.
5. It can also analyze dropped packets.

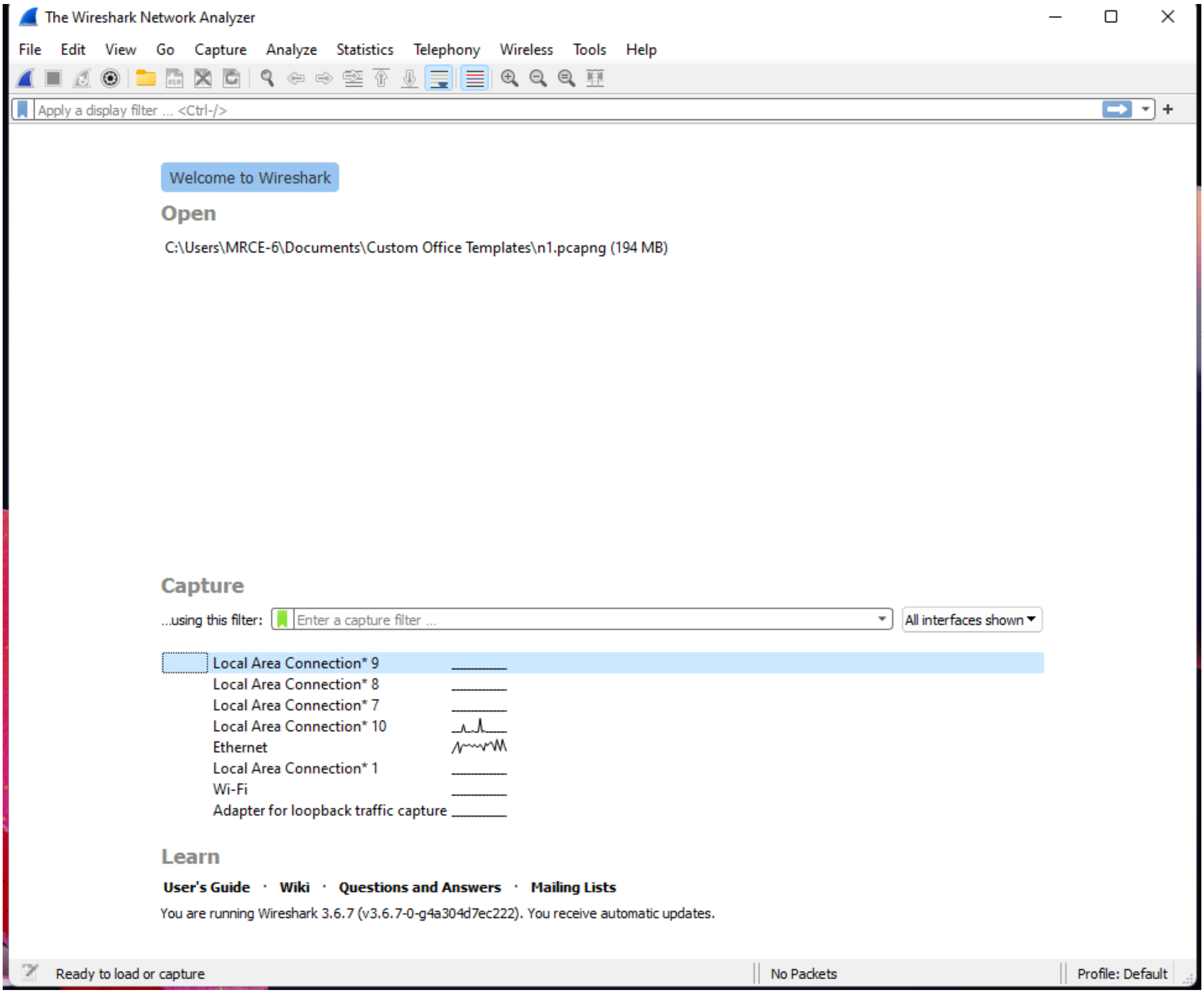
6. It helps us to know how all the devices like laptop, mobile phones, desktop, switch, routers, etc., communicate in a local network or the rest of the world.

What is a packet?

A packet is a unit of data which is transmitted over a network between the origin and the destination. Network packets are small, i.e., maximum **1.5 Kilobytes for Ethernet packets and 64 Kilobytes for IP packets**. The data packets in the Wireshark can be viewed online and can be analyzed offline.

i) Starting Wire shark

Step 1: Open the wire shark software



The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open

C:\Users\MRCE-6\Documents\Custom Office Templates\n1.pcapng (194 MB)

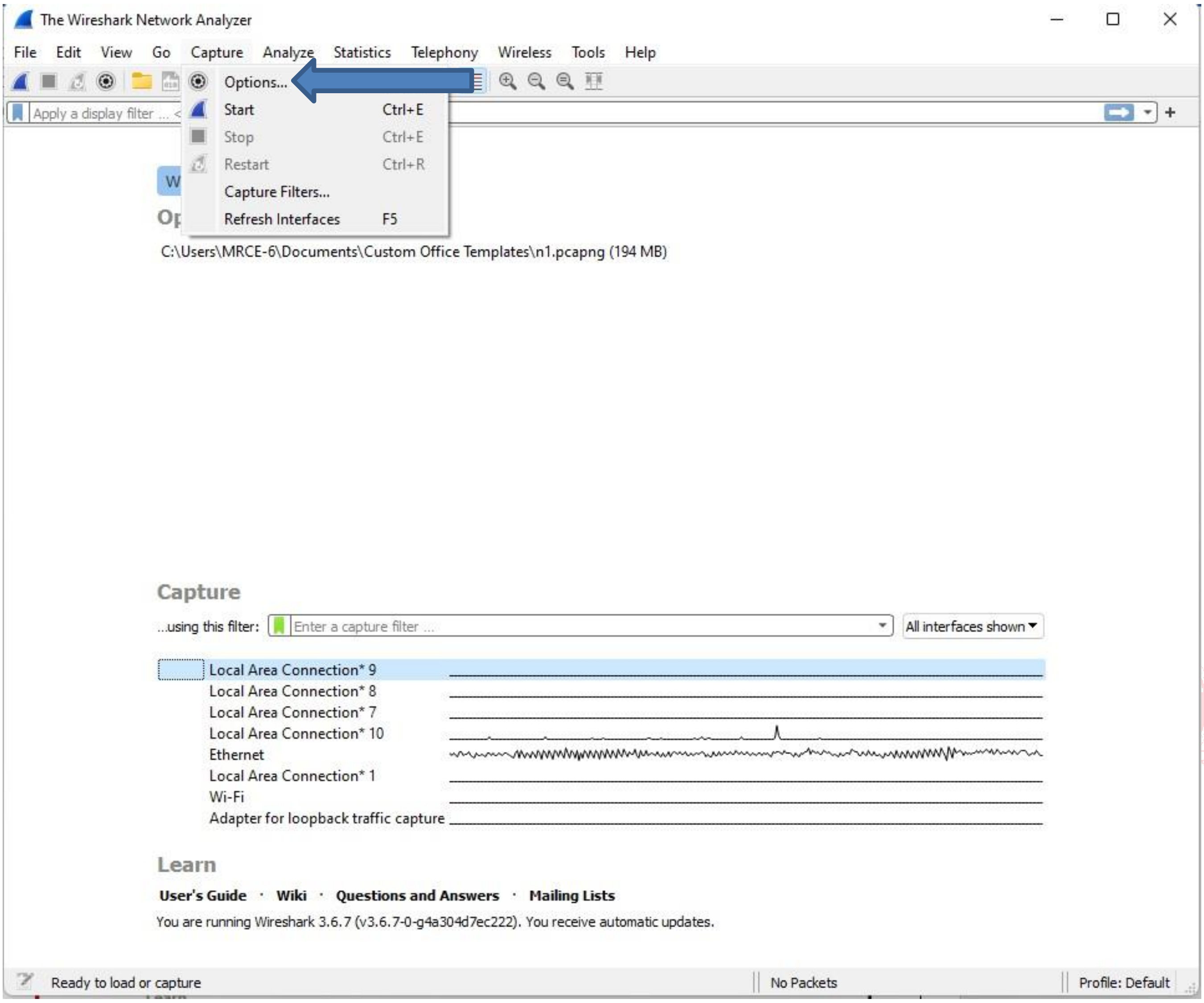
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 10
Ethernet
Local Area Connection* 1
Wi-Fi
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

You are running Wireshark 3.6.7 (v3.6.7-0-g4a304d7ec222). You receive automatic updates.

Ready to load or capture
No Packets
Profile: Default

ii) Packet Capture Using Wire shark

Step 1:



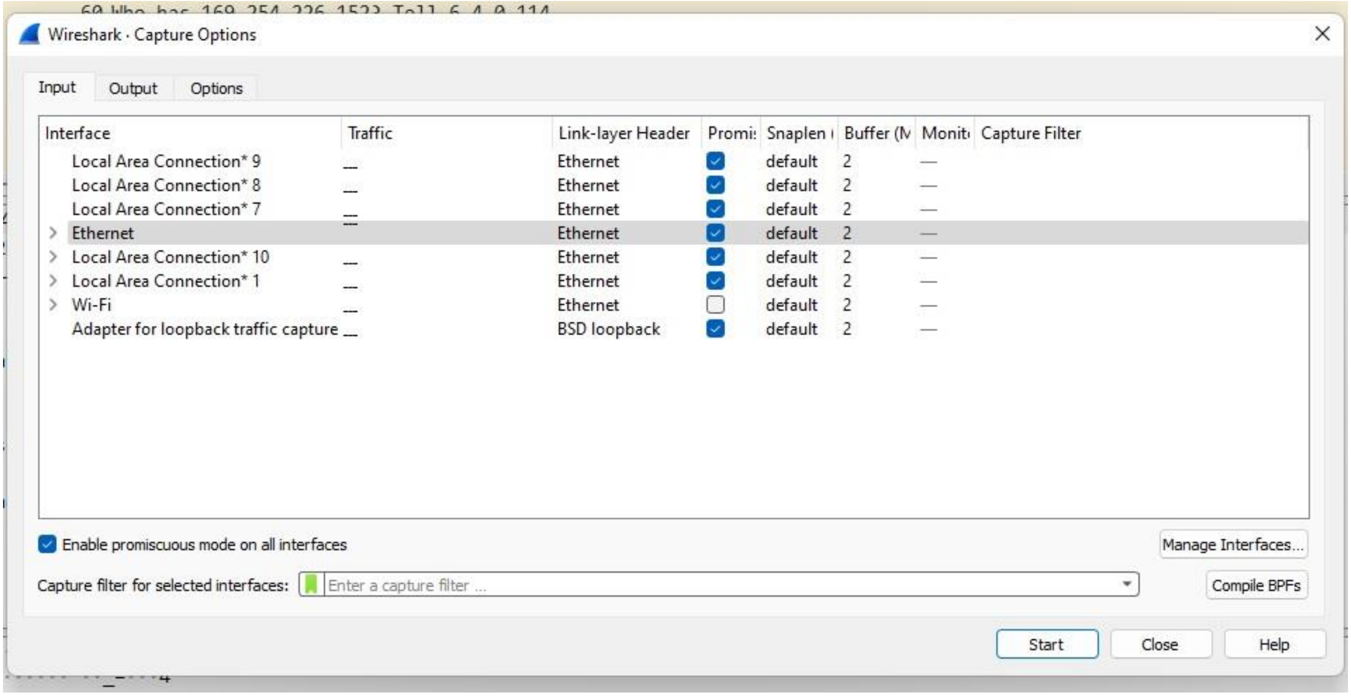
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Options...
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces F5
Apply a display filter ... <
W
Op
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Local Area Connection* 10
Ethernet
Local Area Connection* 1
Wi-Fi
Adapter for loopback traffic capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists

C:\Users\MRCE-6\Documents\Custom Office Templates\n1.pcapng (194 MB)

You are running Wireshark 3.6.7 (v3.6.7-0-g4a304d7ec222). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Step 2:



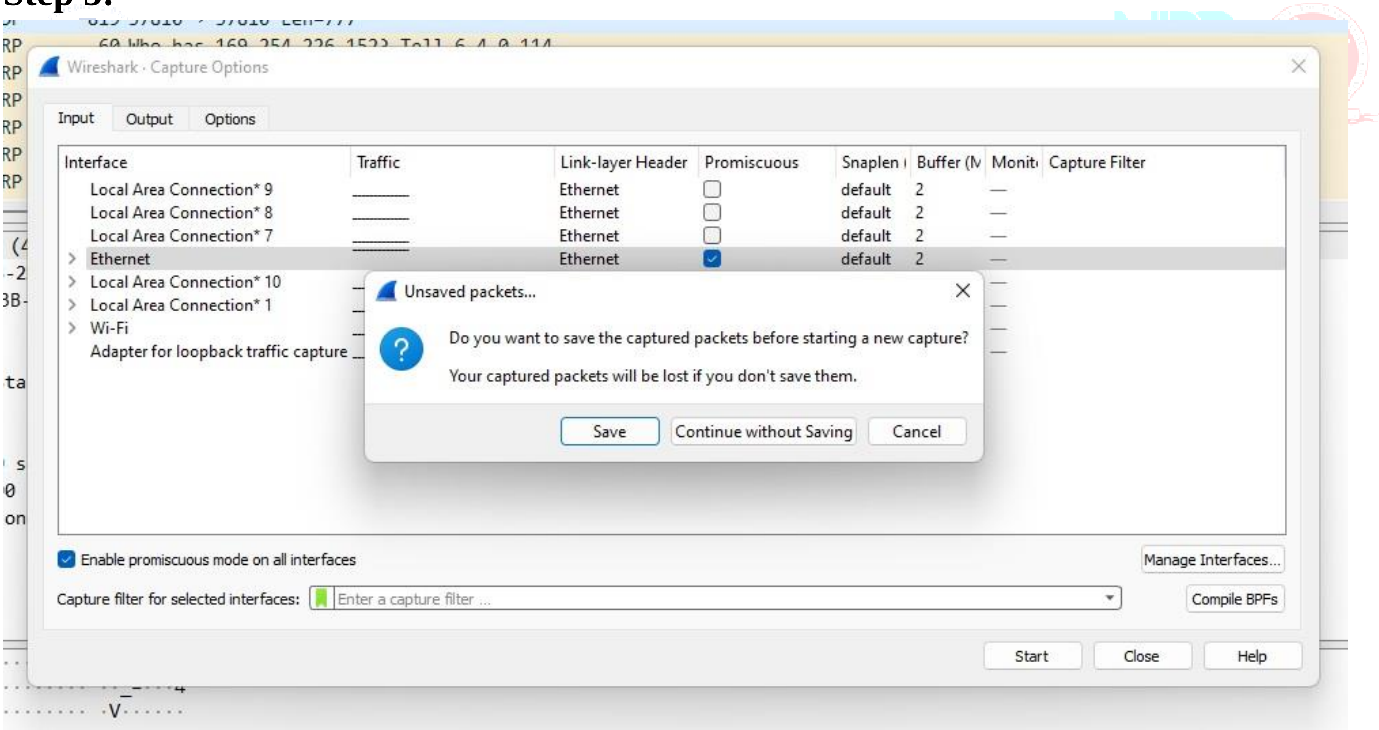
Wireshark · Capture Options

Interface	Traffic	Link-layer Header	Promi:	Snaplen (	Buffer (M	Monit	Capture Filter
Local Area Connection* 9	_	Ethernet	☑	default	2	—	
Local Area Connection* 8	_	Ethernet	☑	default	2	—	
Local Area Connection* 7	_	Ethernet	☑	default	2	—	
> Ethernet		Ethernet	☑	default	2	—	
> Local Area Connection* 10	_	Ethernet	☑	default	2	—	
> Local Area Connection* 1	_	Ethernet	☑	default	2	—	
> Wi-Fi	_	Ethernet	□	default	2	—	
Adapter for loopback traffic capture	_	BSD loopback	☑	default	2	—	

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

Step 3:



Wireshark · Capture Options

Interface	Traffic	Link-layer Header	Promiscuous	Snaplen (	Buffer (M	Monit	Capture Filter
Local Area Connection* 9		Ethernet	□	default	2	—	
Local Area Connection* 8		Ethernet	□	default	2	—	
Local Area Connection* 7		Ethernet	□	default	2	—	
> Ethernet		Ethernet	☑	default	2	—	
> Local Area Connection* 10						—	
> Local Area Connection* 1						—	
> Wi-Fi						—	
Adapter for loopback traffic capture						—	

Unsaved packets...

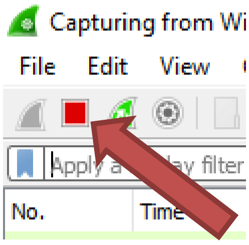
Do you want to save the captured packets before starting a new capture?

Your captured packets will be lost if you don't save them.

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

Step 4: Create a file to save captured packets



Step 5: Press red button to stop capturing packets

Step 6: Now open the captured packet file

iii) Viewing Captured Traffic

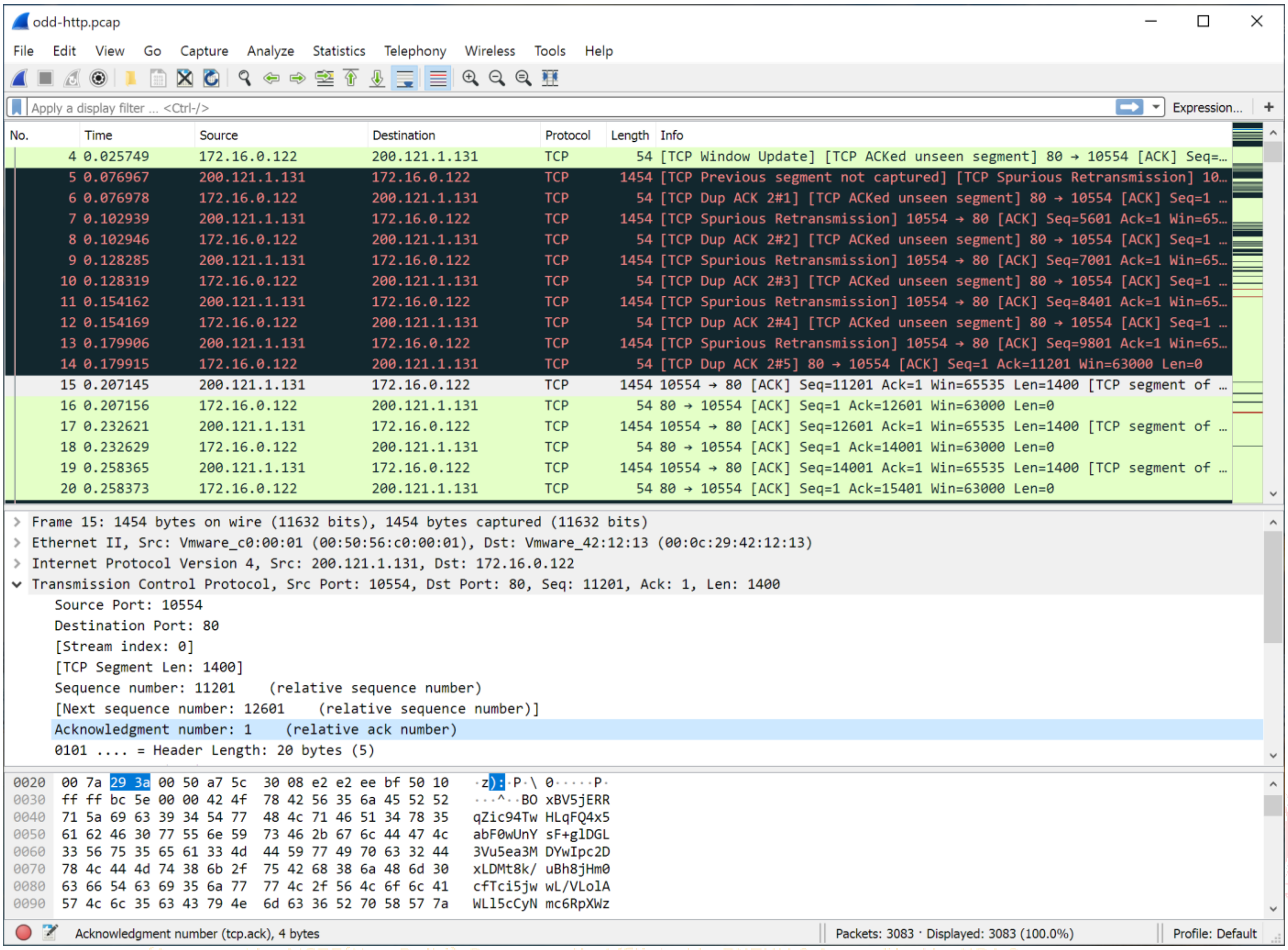
Step 1: Viewing Packets You Have Captured

Once you have captured some packets or you have opened a previously saved capture file, you can view the packets that are displayed in the packet list pane by simply clicking on a packet in the packet list pane, which will bring up the selected packet in the tree view and byte view panes.

You can then expand any part of the tree to view detailed information about each protocol in each packet. Clicking on an item in the tree will highlight the corresponding bytes in the byte view. An example with a TCP packet selected is shown in Figure 1, “Wireshark with a TCP packet selected for viewing”. It also has the Acknowledgment number in the TCP header selected, which shows up in the byte view as the selected bytes.

Fig 1. Wireshark with a TCP packet selected for viewing

Step 2:



odd-http.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.  Time      Source        Destination   Protocol Length Info
   4 0.025749  172.16.0.122  200.121.1.131 TCP        54 [TCP Window Update] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=…
   5 0.076967  200.121.1.131 172.16.0.122  TCP      1454 [TCP Previous segment not captured] [TCP Spurious Retransmission] 10…
   6 0.076978  172.16.0.122  200.121.1.131 TCP        54 [TCP Dup ACK 2#1] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
   7 0.102939  200.121.1.131 172.16.0.122  TCP      1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=5601 Ack=1 Win=65…
   8 0.102946  172.16.0.122  200.121.1.131 TCP        54 [TCP Dup ACK 2#2] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
   9 0.128285  200.121.1.131 172.16.0.122  TCP      1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=7001 Ack=1 Win=65…
  10 0.128319  172.16.0.122  200.121.1.131 TCP        54 [TCP Dup ACK 2#3] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
  11 0.154162  200.121.1.131 172.16.0.122  TCP      1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=8401 Ack=1 Win=65…
  12 0.154169  172.16.0.122  200.121.1.131 TCP        54 [TCP Dup ACK 2#4] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
  13 0.179906  200.121.1.131 172.16.0.122  TCP      1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=9801 Ack=1 Win=65…
  14 0.179915  172.16.0.122  200.121.1.131 TCP        54 [TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
  15 0.207145  200.121.1.131 172.16.0.122  TCP      1454 10554 → 80 [ACK] Seq=11201 Ack=1 Win=65535 Len=1400 [TCP segment of …
  16 0.207156  172.16.0.122  200.121.1.131 TCP        54 80 → 10554 [ACK] Seq=1 Ack=12601 Win=63000 Len=0
  17 0.232621  200.121.1.131 172.16.0.122  TCP      1454 10554 → 80 [ACK] Seq=12601 Ack=1 Win=65535 Len=1400 [TCP segment of …
  18 0.232629  172.16.0.122  200.121.1.131 TCP        54 80 → 10554 [ACK] Seq=1 Ack=14001 Win=63000 Len=0
  19 0.258365  200.121.1.131 172.16.0.122  TCP      1454 10554 → 80 [ACK] Seq=14001 Ack=1 Win=65535 Len=1400 [TCP segment of …
  20 0.258373  172.16.0.122  200.121.1.131 TCP        54 80 → 10554 [ACK] Seq=1 Ack=15401 Win=63000 Len=0
```

```
> Frame 15: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
> Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
> Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122
v Transmission Control Protocol, Src Port: 10554, Dst Port: 80, Seq: 11201, Ack: 1, Len: 1400
     Source Port: 10554
     Destination Port: 80
     [Stream index: 0]
     [TCP Segment Len: 1400]
     Sequence number: 11201    (relative sequence number)
     [Next sequence number: 12601    (relative sequence number)]
     Acknowledgment number: 1    (relative ack number)
     0101 .... = Header Length: 20 bytes (5)
```

```
0020  00 7a 29 3a 00 50 a7 5c  30 08 e2 e2 ee bf 50 10   ·z):·P·\ 0·····P·
0030  ff ff bc 5e 00 00 42 4f  78 42 56 35 6a 45 52 52   ···^··BO xBV5jERR
0040  71 5a 69 63 39 34 54 77  48 4c 71 46 51 34 78 35   qZic94Tw HLqFQ4x5
0050  61 62 46 30 77 55 6e 59  73 46 2b 67 6c 44 47 4c   abF0wUnY sF+glDGL
0060  33 56 75 35 65 61 33 4d  44 59 77 49 70 63 32 44   3Vu5ea3M DYwIpc2D
0070  78 4c 44 4d 74 38 6b 2f  75 42 68 38 6a 48 6d 30   xLDMt8k/ uBh8jHm0
0080  63 66 54 63 69 35 6a 77  77 4c 2f 56 4c 6f 6c 41   cfTci5jw wL/VLolA
0090  57 4c 6c 35 63 43 79 4e  6d 63 36 52 70 58 57 7a   WLl5cCyN mc6RpXWz
```

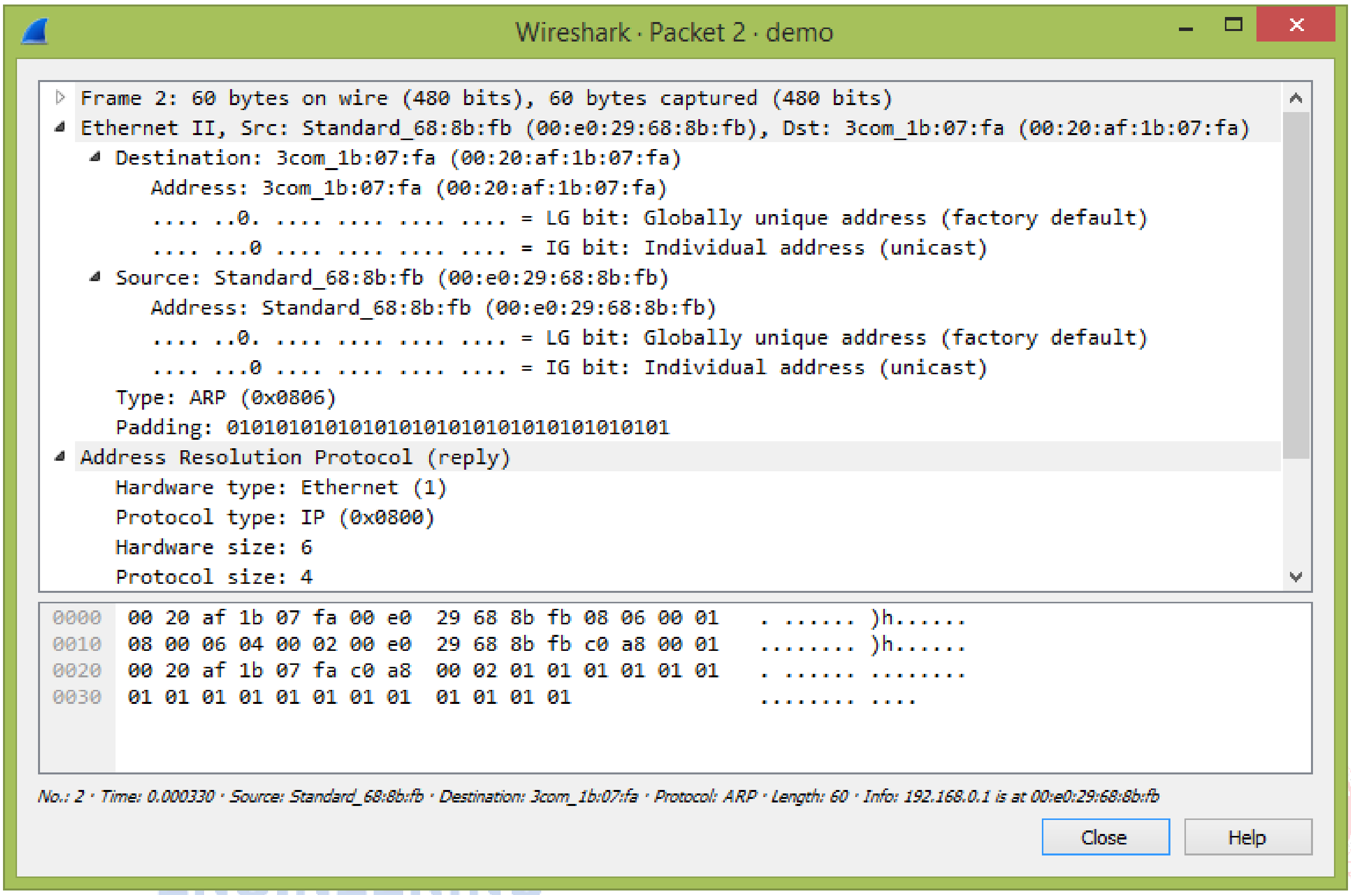
Acknowledgment number (tcp.ack), 4 bytes | Packets: 3083 · Displayed: 3083 (100.0%) | Profile: Default

You can also select and view packets the same way while Wireshark is capturing if you selected “Update list of packets in real time” in the “Capture Preferences” dialog box.

In addition you can view individual packets in a separate window as shown in Figure 2, “Viewing a packet in a separate window”. You can do this by double-clicking on an item in the packet list or by selecting the packet in which you are interested in the packet list pane and selecting

Step 3: View → Show Packet in New Window. This allows you to easily compare two or more packets, even across multiple files.

Figure 2. Viewing a packet in a separate window



```
▷ Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
◢ Ethernet II, Src: Standard_68:8b:fb (00:e0:29:68:8b:fb), Dst: 3com_1b:07:fa (00:20:af:1b:07:fa)
   ◢ Destination: 3com_1b:07:fa (00:20:af:1b:07:fa)
        Address: 3com_1b:07:fa (00:20:af:1b:07:fa)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   ◢ Source: Standard_68:8b:fb (00:e0:29:68:8b:fb)
        Address: Standard_68:8b:fb (00:e0:29:68:8b:fb)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
     Type: ARP (0x0806)
     Padding: 010101010101010101010101010101010101
◢ Address Resolution Protocol (reply)
     Hardware type: Ethernet (1)
     Protocol type: IP (0x0800)
     Hardware size: 6
     Protocol size: 4
```

```
0000  00 20 af 1b 07 fa 00 e0  29 68 8b fb 08 06 00 01   . ...... )h......
0010  08 00 06 04 00 02 00 e0  29 68 8b fb c0 a8 00 01   ........ )h......
0020  00 20 af 1b 07 fa c0 a8  00 02 01 01 01 01 01 01   . ...... ........
0030  01 01 01 01 01 01 01 01  01 01 01 01               ........ ....
```

No.: 2 · Time: 0.000330 · Source: Standard_68:8b:fb · Destination: 3com_1b:07:fa · Protocol: ARP · Length: 60 · Info: 192.168.0.1 is at 00:e0:29:68:8b:fb

iv) Analysis and Statistics & Filters.

Analyzing data packets on Wireshark

Wireshark shows you three different panes for inspecting packet data. The Packet List, the top pane, lists all the packets in the capture. When you click on a packet, the other two panes change to show you the details about the selected packet. You can also tell if the packet is part of a conversation. Here are details about each column in the top pane:

- **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.

Packet Details, the middle pane, shows you as much readable information about the packet as possible, depending on the packet type. You can right-click and create filters based on the highlighted text in this field.

The bottom pane, Packet Bytes, displays the packet exactly as it was captured in hexadecimal.

When looking at a packet that is part of a conversation, you can right-click the packet and select Follow to see only the packets that are part of that conversation.

Wireshark filters

Some of the best features of Wireshark are the capture filters and display filters. Filters allow you to view the capture the way you need to see it to troubleshoot the issues at hand. Below are several filters to get you started.

Wireshark capture filters

Capture filters limit the captured packets by the chosen filter. If the packets don’t match the filter, Wireshark won’t save them. Examples of capture filters include:

host IP-*address*: This filter limits the captured traffic to and from the IP address

net 192.168.0.0/24: This filter captures all traffic on the subnet

dst host IP-*address*: Capture packets sent to the specified host

port 53: Capture traffic on port 53 only

port not 53 and not arp: Capture all traffic except DNS and ARP traffic

Wireshark display filters

Wireshark display filters change the view of the capture during analysis. After you’ve stopped the packet capture, use display filters to narrow down the packets in the Packet List to troubleshoot your issue.

One of the most useful display filters is:

ip.src==*IP-address* and ip.dst==*IP-address*

This filter shows packets sent from one computer (ip.src) to another (ip.dst). You can also use ip.addr to show packets to and from that IP. Other filters include:

tcp.porteq 25: This filter will show you all traffic on port 25, which is usually SMTP traffic icmp: This filter will show you only ICMP traffic in the capture, most likely they are pings

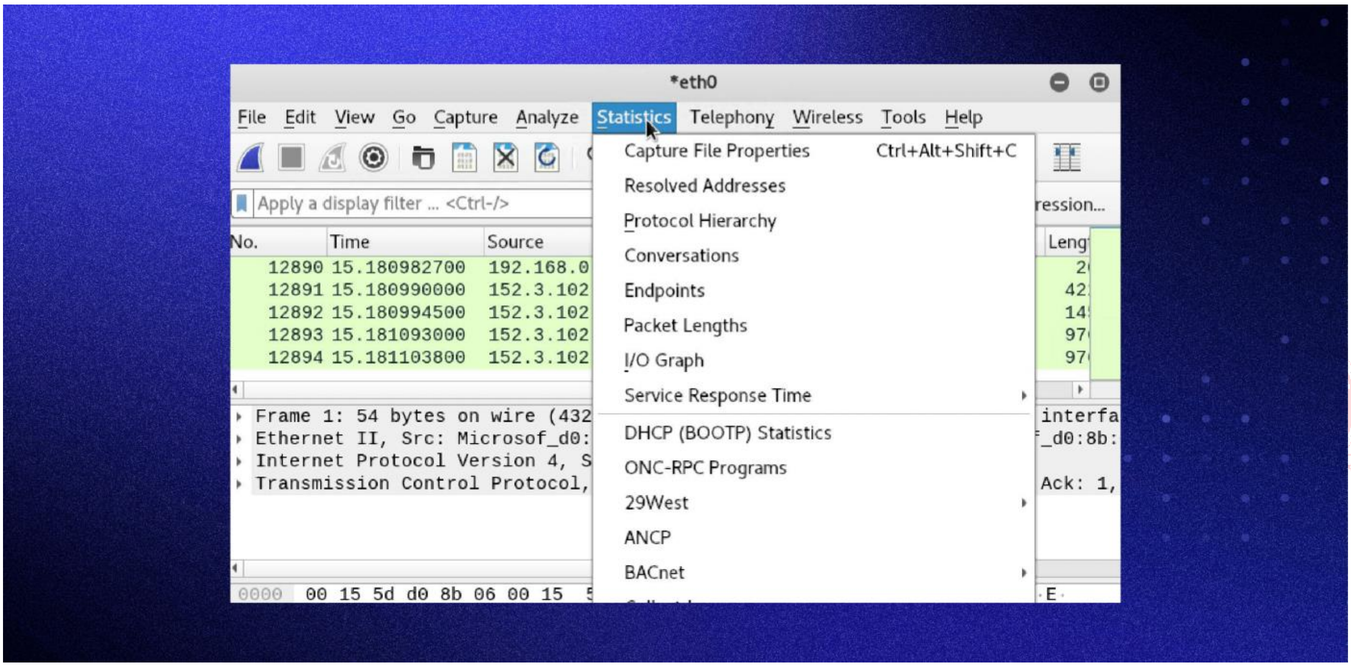
ip.addr != *IP_address*: This filter shows you all traffic except the traffic to or from the specified computer

Analysts even build filters to detect specific attacks, like this filter used to detect the Sasser worm:

ls_ads.opnum==0x09

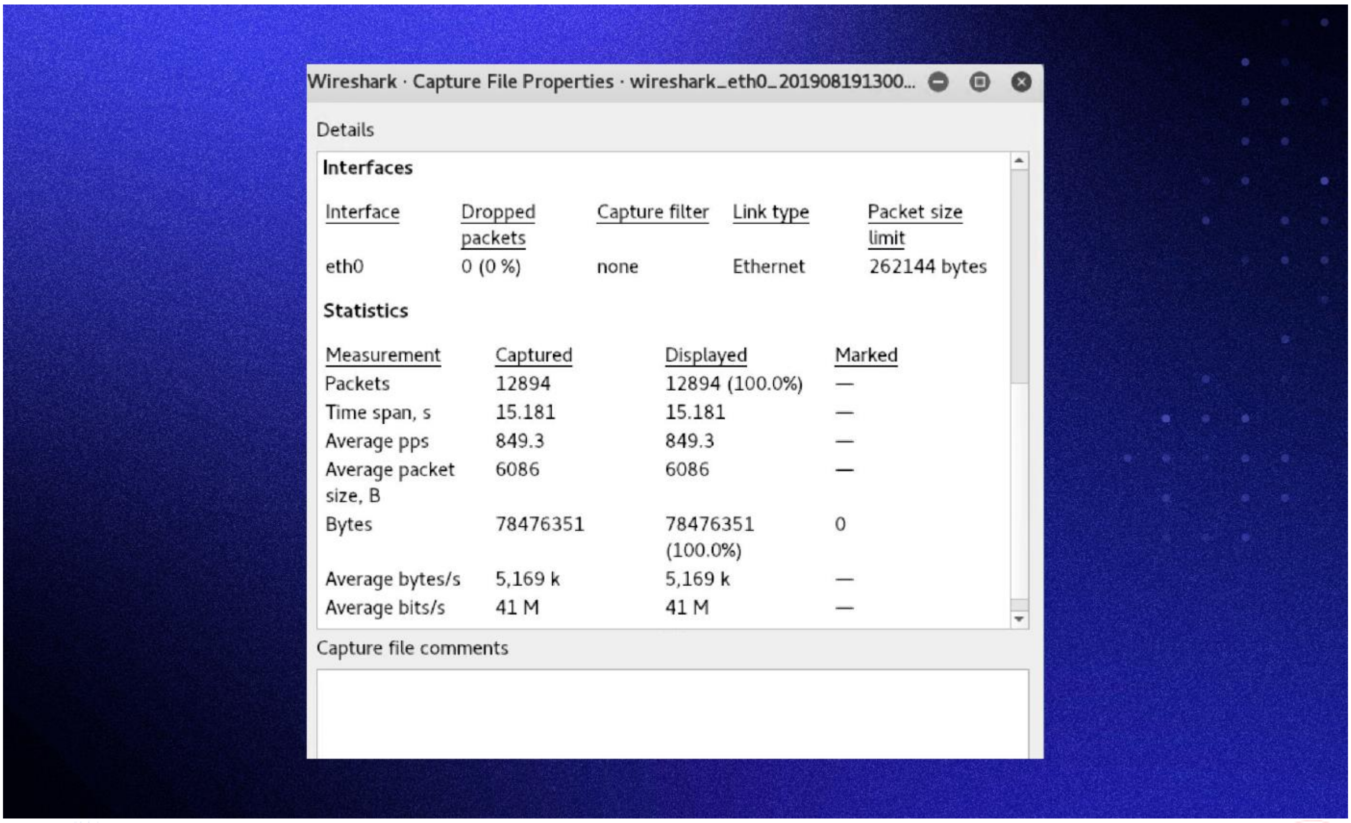
Step 4: Metrics and statistics

Under the Statistics menu, you'll find a plethora of options to view details about your capture.



```
No.     Time             Source          Leng
  12890 15.180982700  192.168.0          2
  12891 15.180990000  152.3.102          42
  12892 15.180994500  152.3.102          14
  12893 15.181093000  152.3.102          97
  12894 15.181103800  152.3.102          97

▸ Frame 1: 54 bytes on wire (432          interfa
▸ Ethernet II, Src: Microsof_d0:          _d0:8b:
▸ Internet Protocol Version 4, S
▸ Transmission Control Protocol,          Ack: 1,

0000  00 15 5d d0 8b 06 00 15 5           ·E·
```

Step 5: Capture File Properties:



Wireshark · Capture File Properties · wireshark_eth0_201908191300...

Details

Interfaces

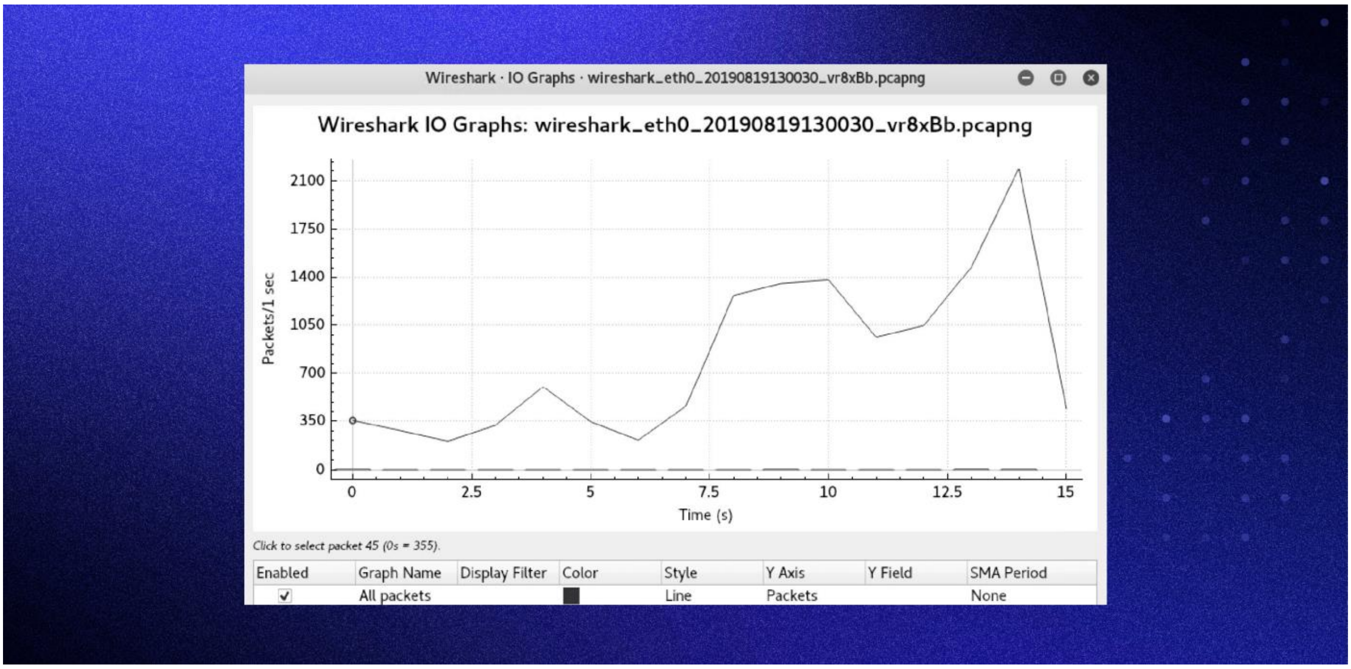
Interface	Dropped packets	Capture filter	Link type	Packet size limit
eth0	0 (0 %)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	12894	12894 (100.0%)	—
Time span, s	15.181	15.181	—
Average pps	849.3	849.3	—
Average packet size, B	6086	6086	—
Bytes	78476351	78476351 (100.0%)	0
Average bytes/s	5,169 k	5,169 k	—
Average bits/s	41 M	41 M	—

Capture file comments

Step 6: Wireshark I/O Graph:



Wireshark · IO Graphs · wireshark_eth0_20190819130030_vr8xBb.pcapng

Wireshark IO Graphs: wireshark_eth0_20190819130030_vr8xBb.pcapng

Click to select packet 45 (0s = 355).

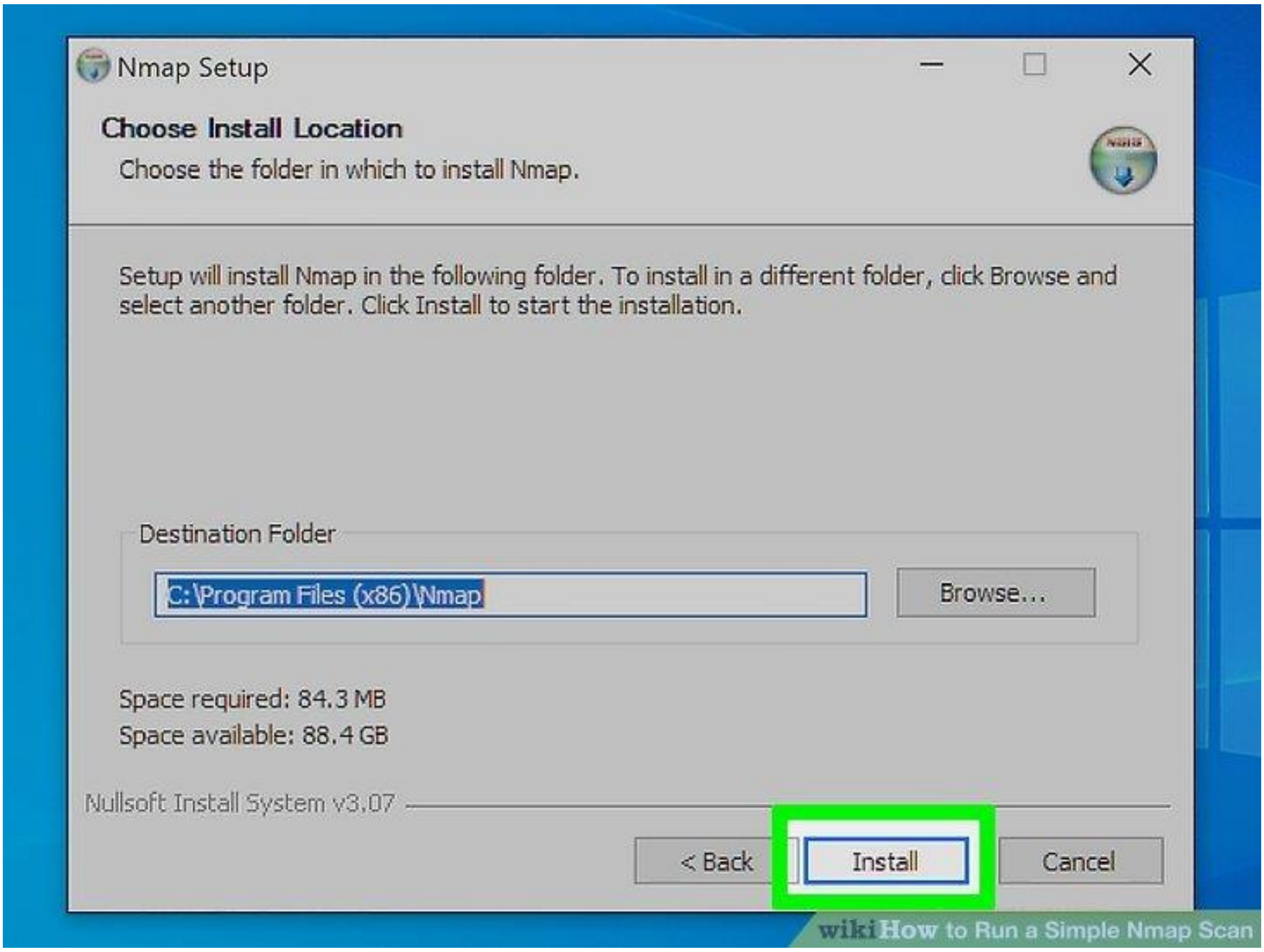
Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period
✓	All packets		■	Line	Packets		None

EXPERIMENT NO: 11

AIM: How to run Nmap scan

1. **Download the Nmap installer.** This can be found for free from the developer’s website. It is highly recommended that you download directly from the developer to avoid any potential viruses or fake files. Downloading the Nmap installer includes Zenmap, the graphical interface for Nmap which makes it easy for newcomers to perform scans without having to learn command lines.

   The Zenmap program is available for Windows, Linux, and Mac OS X. You can find the installation files for all operating systems on the Nmap website.



Nmap Setup

Choose Install Location

Choose the folder in which to install Nmap.

Setup will install Nmap in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\Program Files (x86)\Nmap

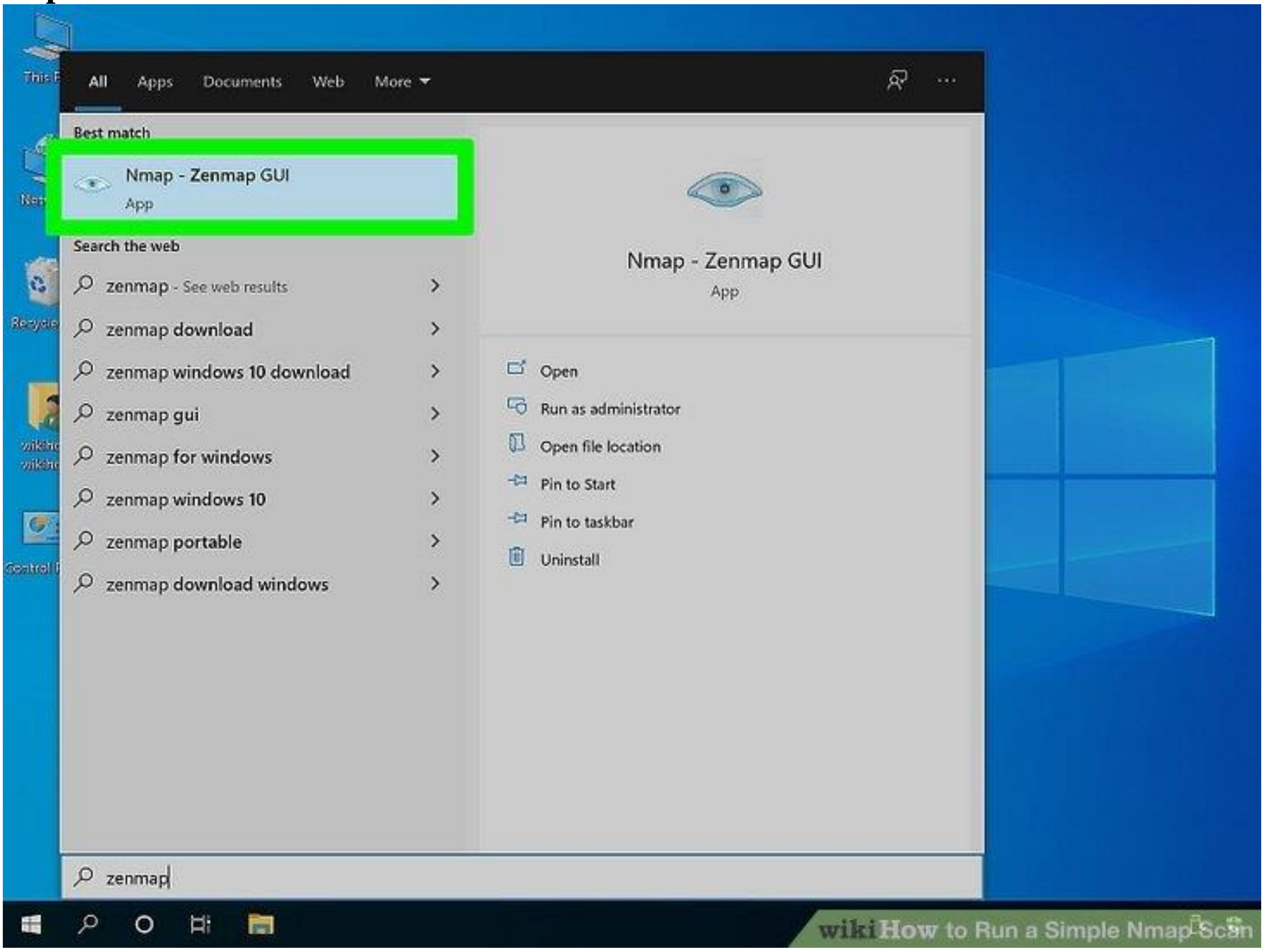
Space required: 84.3 MB

Space available: 88.4 GB

Nullsoft Install System v3.07

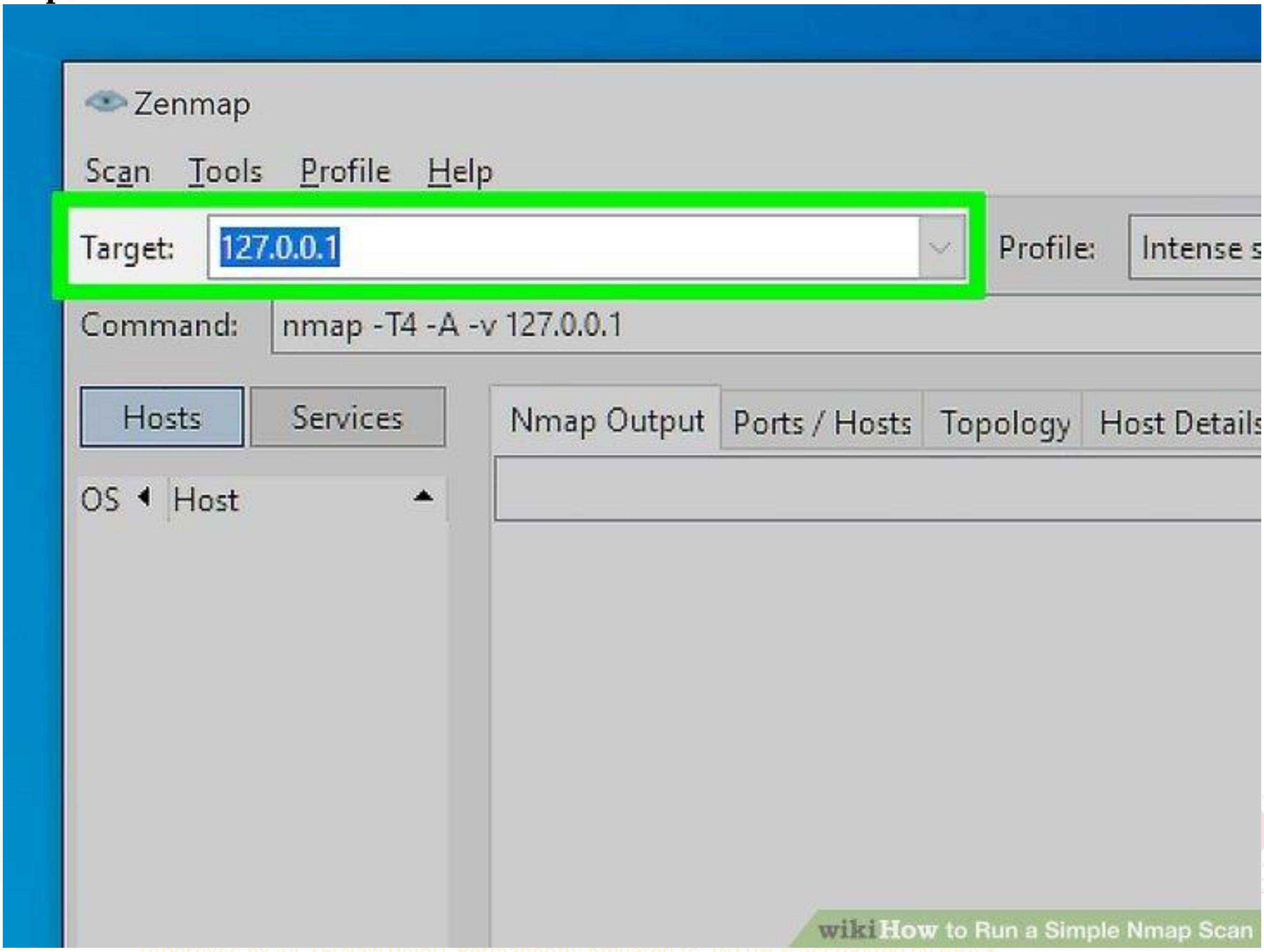
2. **Install Nmap.** Run the installer once it is finished downloading. You will be asked which components you would like to install. In order to get the full benefit of Nmap, keep all of these checked. Nmap will not install any adware or spyware.

Step 1:



3. **Run the "Nmap – Zenmap" GUI program.** If you left your settings at default during installation, you should be able to see an icon for it on your desktop. If not, look in your Start menu. Opening Zenmap will start the program.

Step 2:



Target: 127.0.0.1

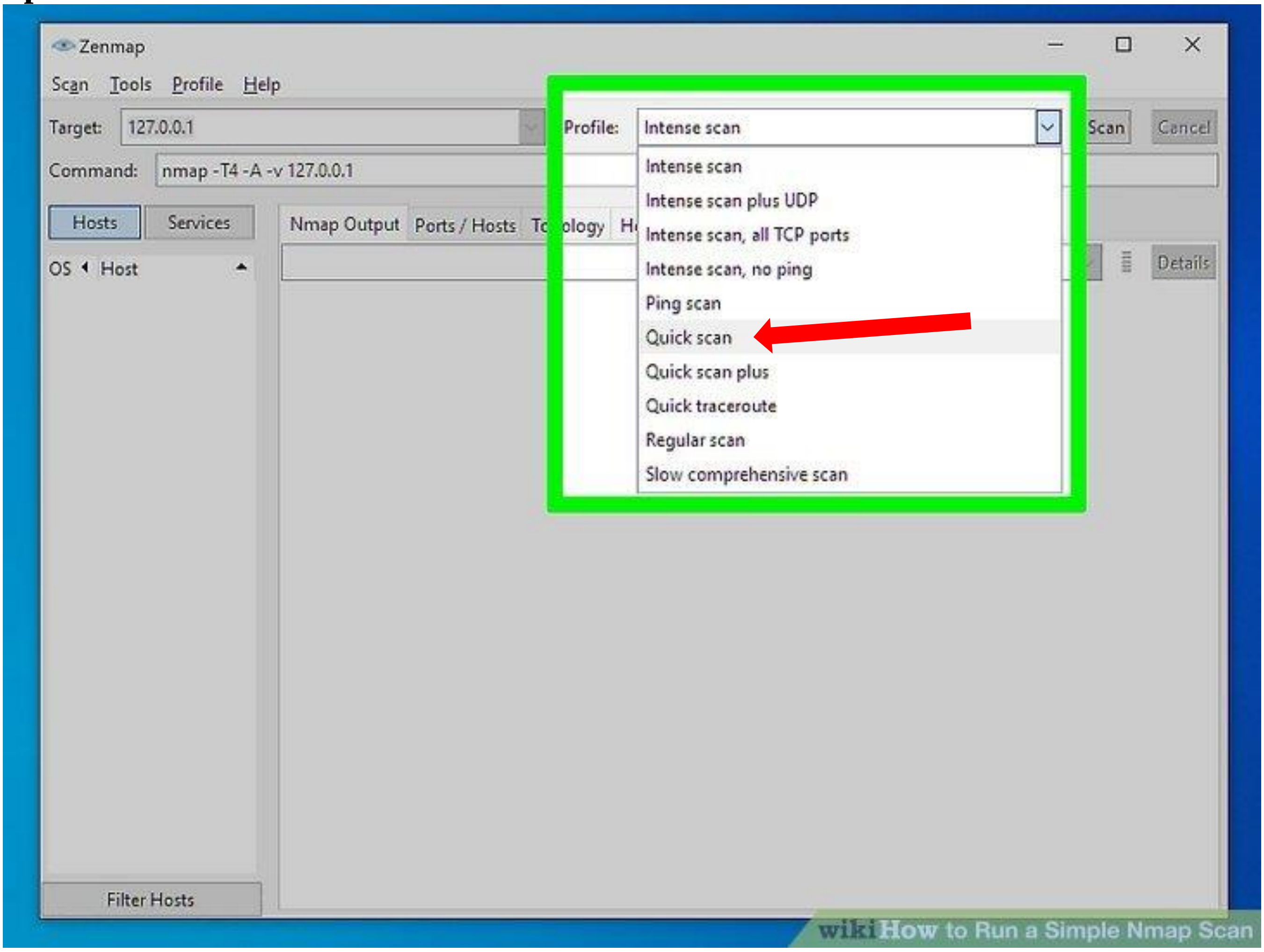
Profile: Intense s

Command: nmap -T4 -A -v 127.0.0.1

4. **Enter in the target for your scan.** The Zenmap program makes scanning a fairly simple process. The first step to running a scan is choosing your target. You can enter a domain (example.com), an IP address (127.0.0.1), a network (192.168.1.0/24), or a combination of those.

- Depending on the intensity and target of your scan, running an Nmap scan may be against the terms of your internet service provider, and may land you in hot water. Always check your local laws and your ISP contract before performing Nmap scans on targets other than your own network.

Step 3:



Target: 127.0.0.1

Command: nmap -T4 -A -v 127.0.0.1

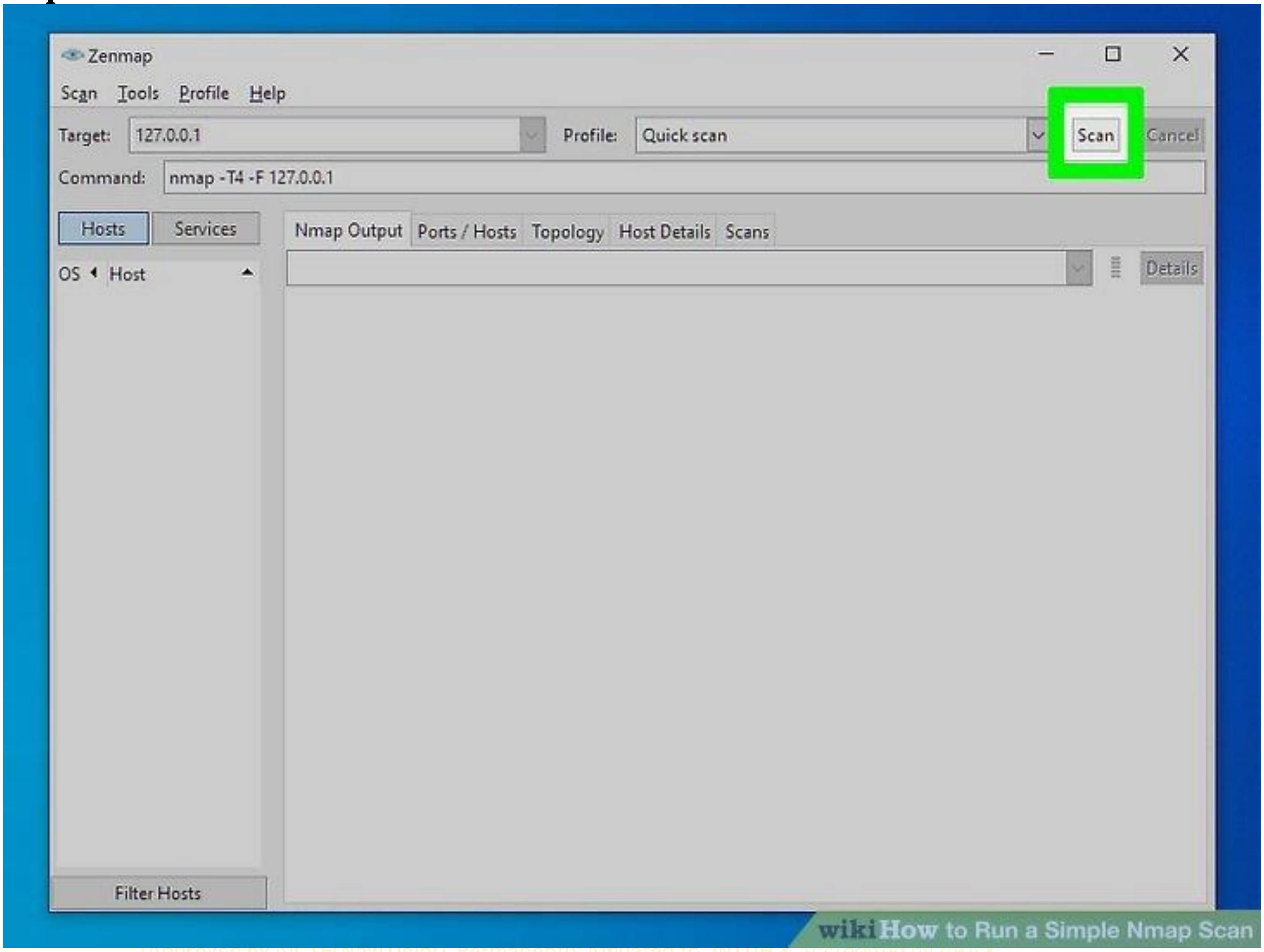
Profile: Intense scan

wikiHow to Run a Simple Nmap Scan

5. **Choose your Profile.** Profiles are preset groupings of modifiers that change what is scanned. The profiles allow you to quickly select different types of scans without having to type in the modifiers on the command line. Choose the profile that best fits your needs

- **Intense scan** - A comprehensive scan. Contains Operating System (OS) detection, version detection, script scanning, traceroute, and has aggressive scan timing. This is considered an intrusive scan.
- **Ping scan** - This scan simply detects if the targets are online, it does not scan any ports.
- **Quick scan** - This is quicker than a regular scan due to aggressive timing and only scanning select ports.
- **Regular scan** - This is the standard Nmap scan without any modifiers. It will return ping and return open ports on the target.

Step 4:



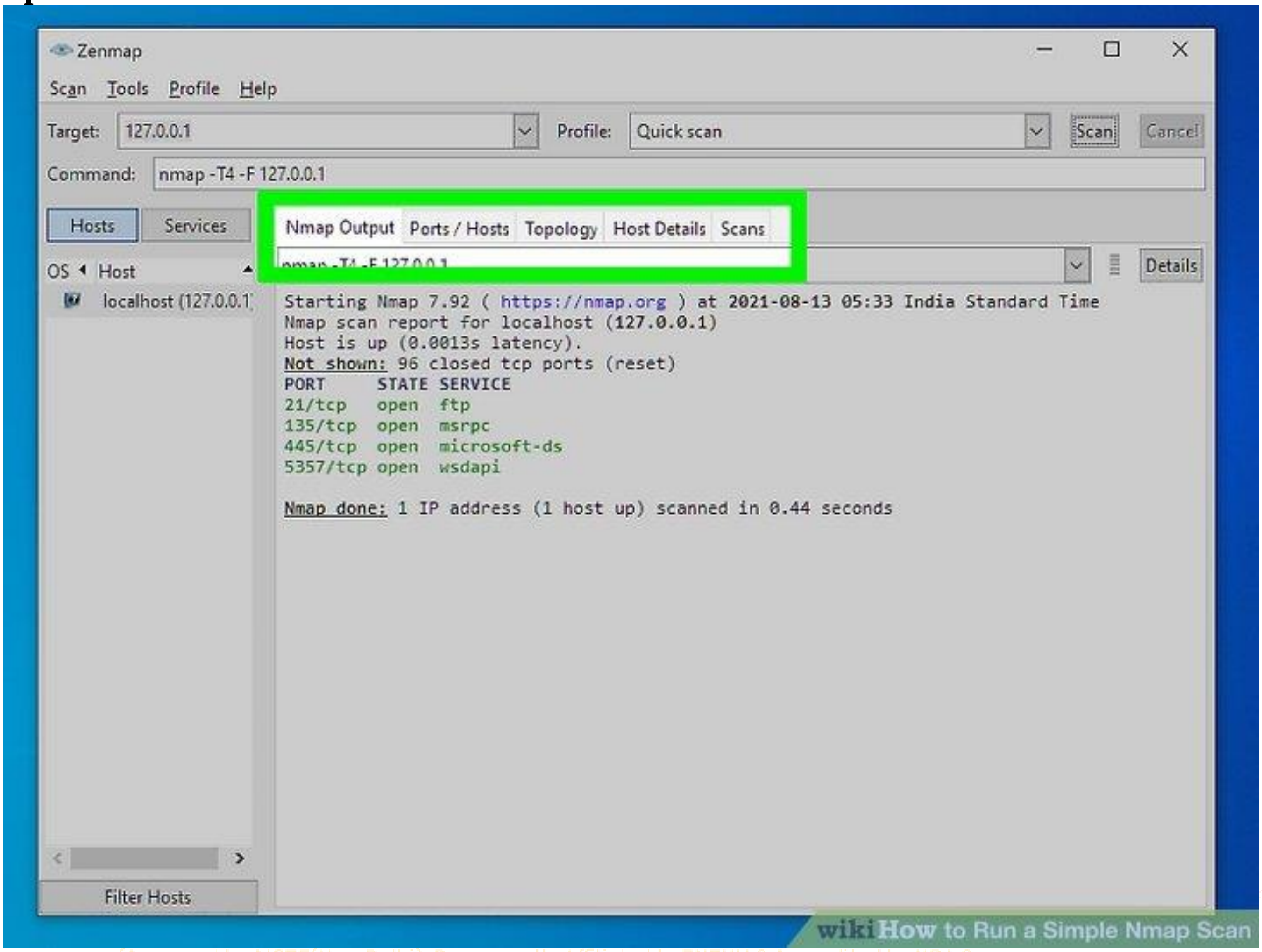
Target: 127.0.0.1

Profile: Quick scan

Command: nmap -T4 -F 127.0.0.1

6. **Click Scan to start scanning.** The active results of the scan will be displayed in the Nmap Output tab. The time the scan takes will depend on the scan profile you chose, the physical distance to the target, and the target’s network configuration.

Step 5:



Target: 127.0.0.1 Profile: Quick scan

Command: nmap -T4 -F 127.0.0.1

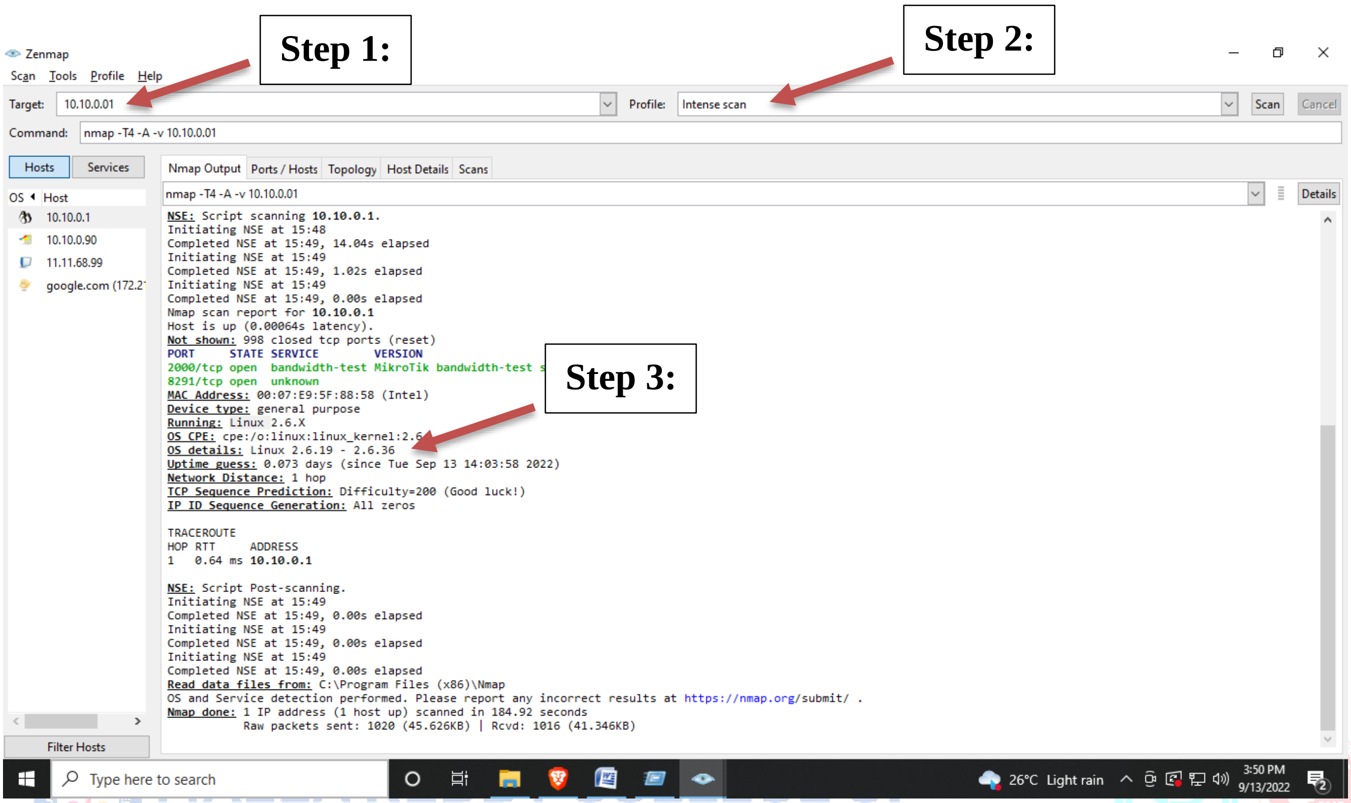
```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-08-13 05:33 India Standard Time
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0013s latency).
Not shown: 96 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds
```

7. **Read your results.** Once the scan is finished, you’ll see the message "Nmap done" at the bottom of the Nmap Output tab. You can now check your results, depending on the type of scan you performed. All of the results will be listed in the main Nmap Output tab, but you can use the other tabs to get a better look at specific data.[2]

- **Ports/Hosts** - This tab will show the results of your port scan, including the services for those ports.
- **Topology** - This shows the traceroute for the scan you performed. You can see how many hops your data goes through to reach the target.
- **Host Details** - This shows a summary of your target learned through scans, such as the number of ports, IP addresses, hostnames, operating systems, and more.
- **Scans** - This tab stores the commands of your previously-run scans. This allows you to quickly re-scan with a specific set of parameters.

EXPERIMENT NO: 12

AIM: Operating System Detection using Nmap



Step 1:

Step 2:

Step 3:

Target: 10.10.0.01

Profile: Intense scan

Command: nmap -T4 -A -v 10.10.0.01

```
nmap -T4 -A -v 10.10.0.01
NSE: Script scanning 10.10.0.1.
Initiating NSE at 15:48
Completed NSE at 15:49, 14.04s elapsed
Initiating NSE at 15:49
Completed NSE at 15:49, 1.02s elapsed
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
Nmap scan report for 10.10.0.1
Host is up (0.00064s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE        VERSION
2000/tcp open  bandwidth-test MikroTik bandwidth-test s
8291/tcp open  unknown
MAC Address: 00:07:E9:5F:88:58 (Intel)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.19 - 2.6.36
Uptime guess: 0.073 days (since Tue Sep 13 14:03:58 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=200 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT     ADDRESS
1   0.64 ms 10.10.0.1

NSE: Script Post-scanning.
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
Initiating NSE at 15:49
Completed NSE at 15:49, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 184.92 seconds
           Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.346KB)
```