Wireshark Installation and Use

Time required: 30 minutes

How to Create Screenshots: Please use the Windows Snip and Sketch Tool or the Snipping Tool. Paste a screenshot of just the program you are working on. If you are snipping a virtual machine, make sure your focus is outside the virtual machine before you snip.

1. Press and hold down the **Windows key** & **Shift**, then type **S.** This brings up the on-screen snipping tool.
2. Click and Drag your mouse around whatever you want to snip.
3. Release the mouse button. This places the snip into the Windows Clipboard.
4. Go into Word or wherever you want to paste the snip. Hold down **CTRL**, then type **V** to paste the snip.

Lab Description

Wireshark is a free, open source network protocol analyzer that can help demystify network messages and help make the OSI model a little more tangible.

Using Wireshark for the first time can be an epiphany experience. It allows you to study the OSI layers, all the information that is added to every message, and the messages that have to go back and forth just to bring up a Web page or even just to connect to the network.

It all becomes much more real when you see how many packets Wireshark collects during even a short capture.

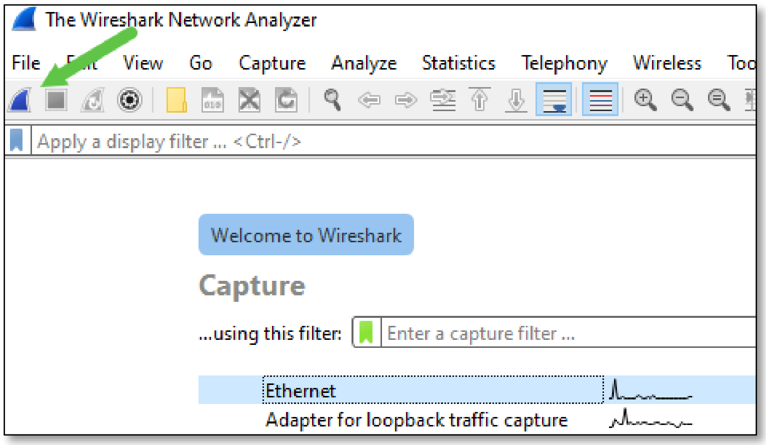
Install Wireshark

We'll install Wireshark in this project and take a first look at how it works. Later on, we'll dig deeper into Wireshark's capabilities.

1. Go to www.wireshark.org
2. Download and install the appropriate version for your OS.

Note: You may also need to install NPcap during the Wireshark installation process. NPcap is a Windows service that does not come standard in Windows and is required to capture live network data.

Capture Packets

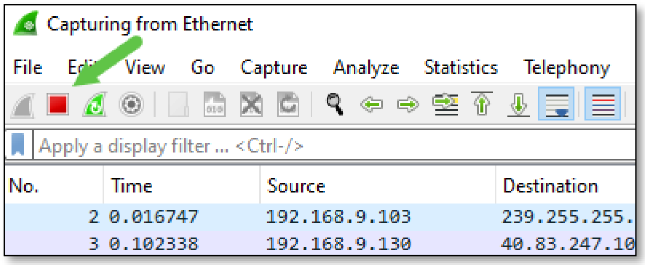

The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Too
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
Ethernet
Adapter for loopback traffic capture

1. To start our first capture, in the Wireshark Network Analyzer window, find the adapter that has activity. In the above screenshot, it is Ethernet. Yours may say WiFi.

2. Click the adapter that show activity.

3. Click the Sharkfin **Capture button**. Your capture will start.

4. While the capture is running, challenge your network a bit by opening your web browser and navigating to **google.com**.



No.	Time	Source	Destination
2	0.016747	192.168.9.103	239.255.255.
3	0.102338	192.168.9.130	40.83.247.10

5. Click the red box on the command ribbon to stop the capture.

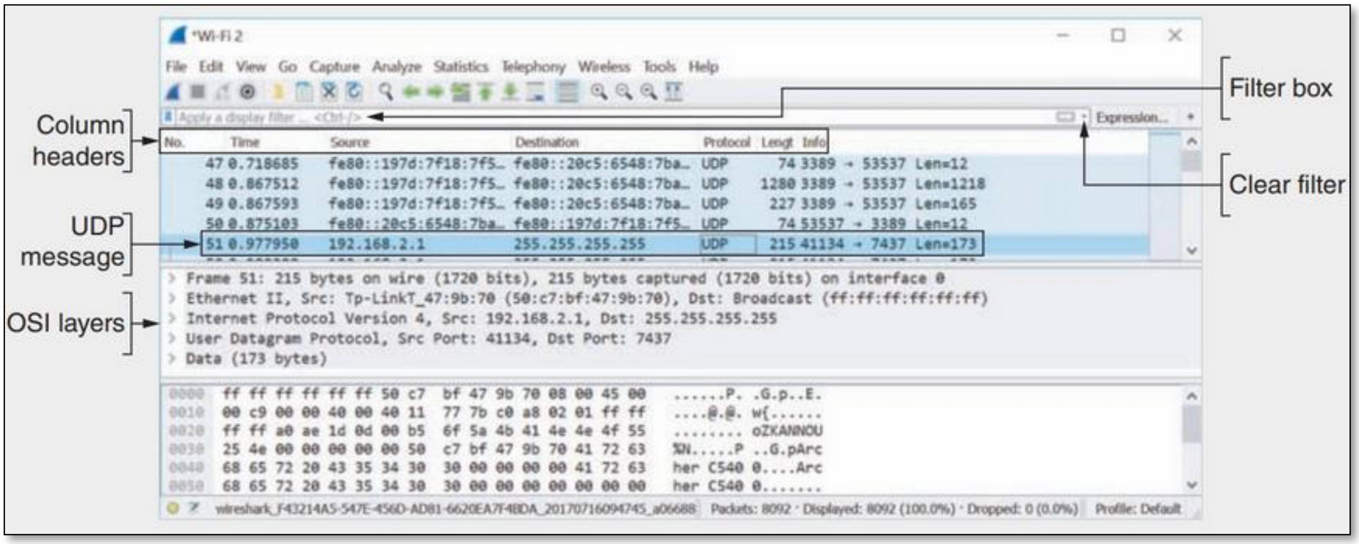
6. Take a look at some of the items you might have captured, and start to decode this blur of numbers and letters.

7. **Insert a screenshot:**

Click or tap here to enter text.

8. Notice the column headers along the top of the capture. Of particular interest are the Source and Destination columns, the Protocol column, and the Info column. Find a

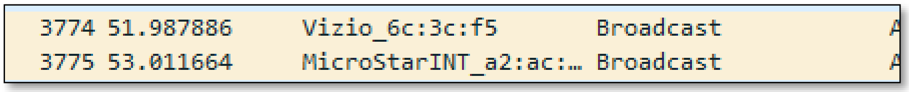
UDP message that has an IPv4 Source address and click on it. In the middle pane, click on each line to expand that layer's information.


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Column headers
UDP message
OSI layers
Filter box
Clear filter

```
No.  Time       Source                  Destination             Protocol Lengt Info
  47 0.718685   fe80::197d:7f18:7f5…    fe80::20c5:6548:7ba…    UDP        74 3389 → 53537 Len=12
  48 0.867512   fe80::197d:7f18:7f5…    fe80::20c5:6548:7ba…    UDP      1280 3389 → 53537 Len=1218
  49 0.867593   fe80::197d:7f18:7f5…    fe80::20c5:6548:7ba…    UDP       227 3389 → 53537 Len=165
  50 0.875103   fe80::20c5:6548:7ba…    fe80::197d:7f18:7f5…    UDP        74 53537 → 3389 Len=12
  51 0.977950   192.168.2.1             255.255.255.255         UDP       215 41134 → 7437 Len=173

> Frame 51: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_47:9b:70 (50:c7:bf:47:9b:70), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 192.168.2.1, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 41134, Dst Port: 7437
> Data (173 bytes)

0000  ff ff ff ff ff ff 50 c7  bf 47 9b 70 08 00 45 00   ......P. .G.p..E.
0010  00 c9 00 00 40 00 40 11  77 7b c0 a8 02 01 ff ff   ....@.@. w{......
0020  ff ff a0 ae 1d 0d 00 b5  6f 5a 4b 41 4e 4e 4f 55   ........ oZKANNOU
0030  25 4e 00 00 00 00 00 50  c7 bf 47 9b 70 41 72 63   %N.....P ..G.pArc
0040  68 65 72 20 43 35 34 30  30 00 00 00 00 41 72 63   her C540 0....Arc
0050  68 65 72 20 43 35 34 30  30 00 00 00 00 00 00 00   her C540 0.......

wireshark_F43214A5-547E-456D-AD81-6620EA7F48DA_20170716094745_a06688   Packets: 8092 · Displayed: 8092 (100.0%) · Dropped: 0 (0.0%)   Profile: Default
```

9. What pieces of information stand out to you?

Click or tap here to enter text.



```
3774 51.987886     Vizio_6c:3c:f5        Broadcast          A
3775 53.011664     MicroStarINT_a2:ac:… Broadcast          A
```

10. Which device on your network do you think sent this message, and which device(s) received it? In the capture above, my Vizio tv was picked up.

Click or tap here to enter text.

Color highlighting can help you easily spot different protocols. TCP messages are a light lavender color, ARP messages are a yellowish color, and DNS messages are a light bluish color. You can see the protocol names in the Protocol column.

11. To filter for a particular kind of packet, type the name of the protocol in the Filter box and press Enter. Try **TCP**. Try filtering for other protocols discussed earlier in this chapter and see how many different types you can find in your capture. Click Clear between searches to return to the complete capture data.

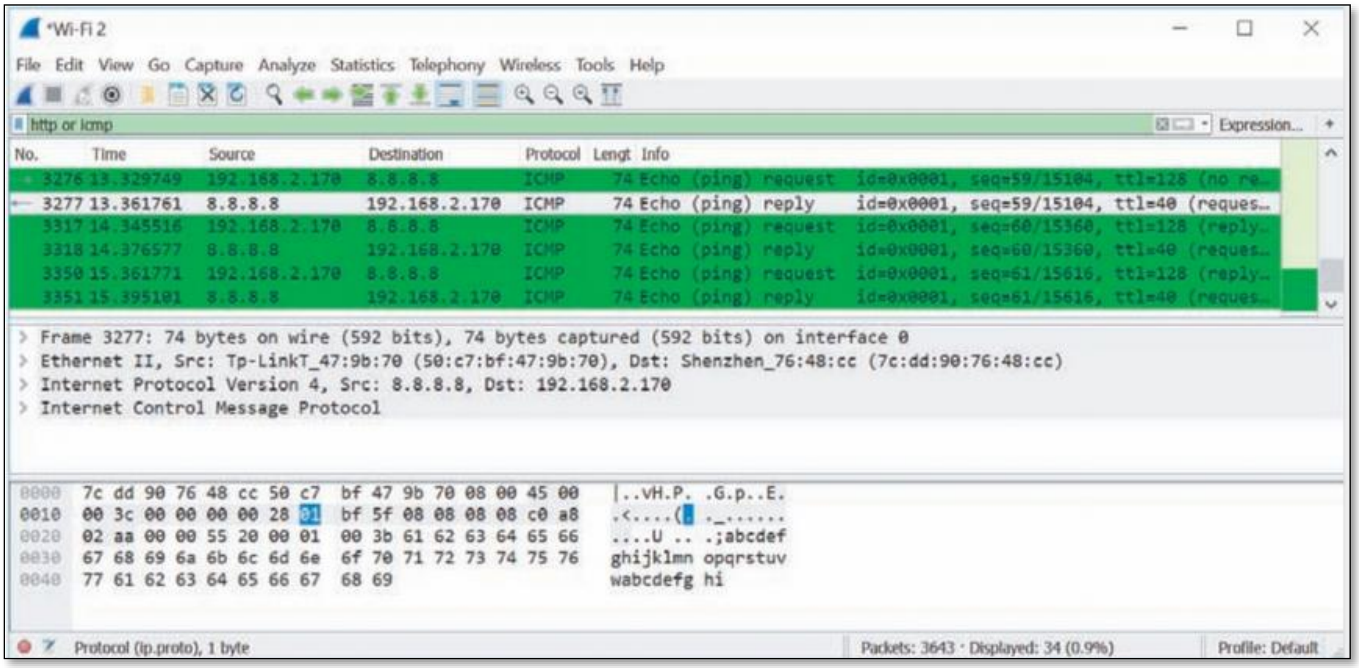
12. To compare OSI layers represented by each of these protocols, do another filter where you can see HTTP and TCP packets in the same search. Enter the following fields into the Filter box: **http or icmp**

13.Insert a screenshot:

Click or tap here to enter text.

14. Use the middle pane to dig into each layer's headers.

15. Click on an ICMP message and count the layers of information available in the middle pane. In Figure 4-32, there are four layers of information, which correspond to Layer 2 (Frame and Ethernet II) and Layer 3 (Internet Protocol Version 4 and Internet Control Message Protocol). 10. Examine an HTTP message. Figure 4-33 shows five layers of information in the middle pane. This time, Layer 7 (Hypertext Transfer Protocol) and Layer 4 (Transmission Control Protocol) are represented, in addition to Layer 3 (Internet Protocol Version 4) and Layer 2 (Ethernet II and Frame).


*Wi-Fi 2
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http or icmp
Expression...

No.	Time	Source	Destination	Protocol	Lengt	Info
3276	13.329749	192.168.2.170	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=59/15104, ttl=128 (no re…
3277	13.361761	8.8.8.8	192.168.2.170	ICMP	74	Echo (ping) reply id=0x0001, seq=59/15104, ttl=40 (reques…
3317	14.345516	192.168.2.170	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=60/15360, ttl=128 (reply…
3318	14.376577	8.8.8.8	192.168.2.170	ICMP	74	Echo (ping) reply id=0x0001, seq=60/15360, ttl=40 (reques…
3350	15.361771	192.168.2.170	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=61/15616, ttl=128 (reply…
3351	15.395101	8.8.8.8	192.168.2.170	ICMP	74	Echo (ping) reply id=0x0001, seq=61/15616, ttl=40 (reques…

```
> Frame 3277: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_47:9b:70 (50:c7:bf:47:9b:70), Dst: Shenzhen_76:48:cc (7c:dd:90:76:48:cc)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.2.170
> Internet Control Message Protocol
```

```
0000  7c dd 90 76 48 cc 50 c7  bf 47 9b 70 08 00 45 00   |..vH.P. .G.p..E.
0010  00 3c 00 00 00 00 28 01  bf 5f 08 08 08 08 c0 a8   .<....(. ._......
0020  02 aa 00 00 55 20 00 01  00 3b 61 62 63 64 65 66   ....U .. .;abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Protocol (ip.proto), 1 byte | Packets: 3643 · Displayed: 34 (0.9%) | Profile: Default

16.Is the packet using UDP or TCP?

Click or tap here to enter text.

17. Insert a screenshot of the selected packet.

Click or tap here to enter text.

TCP is a connection-oriented protocol. You can filter a capture to follow a TCP stream so you can see how these messages go back and forth for a single session.

18. In Wireshark → Find a **TCP** packet → **right-click** it →select **Follow** →click **TCP Stream**.

19. Click **Close** the Follow TCP Stream window and note that Wireshark has filtered the capture for this stream's packets.

20. In the Info column, you can see both SYN and ACK flags.

21. What is the purpose of these messages?

Click or tap here to enter text.

22. Select a TCP message from this filtered data, and explore the middle pane. Click to open each section in that pane.

23. Insert a screenshot:

Click or tap here to enter text.

24. Click on any message that includes a Source or Destination MAC address on the Ethernet II line of output in the middle pane.

25. Insert a screenshot.

Click or tap here to enter text.

26. Was Wireshark able to resolve the name of the manufacturer for this device? If so, what is it?

Click or tap here to enter text.

27. Close Wireshark. **Quit without Saving**.

Assignment Submission

Attach this completed document to the assignment in Blackboard.