**Using Wireshark to observe**

**Frames, Ethernet, and ARP**

In this lab, text that is in blue will be the stuff that you turn in for this lab.

# Getting Started

These instructions are meant for using the Windows operation system. The same thing can be done using Linux or Mac operating systems, but things may look a little different.

Make sure that you are connected to the Internet. Open a broswer and make sure you can get to some website (like Google).

## Get your MAC id and IP address

Start a command prompt window. To do this, type “cmd” in the search field at the bottom of the screen.



This will bring up a command prompt window like this:



Type in the command: **ipconfig /all**

You should see some output that looks similar to below. There will be more output than you need, so be sure to scroll up to get what you need. You are looking for the adaptor that has your IPv4 Address. You may have multiple adapters listed, and it won’t necessarily be the Wi-Fi adaptor.

|  |
| --- |
| C:\Users\mfern>ipconfig /all ...  Wireless LAN adapter Wi-Fi:  Connection-specific DNS Suffix . :  Description . . . . . . . . . . . : Realtek 8822CE Wireless LAN 802.11ac PCI-E NIC  Physical Address. . . . . . . . . : DC-E9-94-0B-6A-E9  DHCP Enabled. . . . . . . . . . . : Yes  Autoconfiguration Enabled . . . . : Yes  IPv6 Address. . . . . . . . . . . : fd47:b7c3:a405:5301:b199:a5ab:5744:5cee(Preferred)  Temporary IPv6 Address. . . . . . : fd47:b7c3:a405:5301:7055:64ec:feba:3c88(Deprecated)  Link-local IPv6 Address . . . . . : fe80::eda2:6784:6a68:2dd8%9(Preferred)  IPv4 Address. . . . . . . . . . . : 192.168.1.5(Preferred)  Subnet Mask . . . . . . . . . . . : 255.255.255.0  Lease Obtained. . . . . . . . . . : Thursday, September 21, 2023 3:01:34 PM  Lease Expires . . . . . . . . . . : Sunday, September 24, 2023 11:42:04 AM  Default Gateway . . . . . . . . . : 192.168.1.1  DHCP Server . . . . . . . . . . . : 192.168.1.1  DHCPv6 IAID . . . . . . . . . . . : 333244820  DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-8F-9E-38-1C-69-7A-4A-63-3A  DNS Servers . . . . . . . . . . . : 192.168.1.1 NetBIOS over Tcpip. . . . . . . . : Enabled ... |

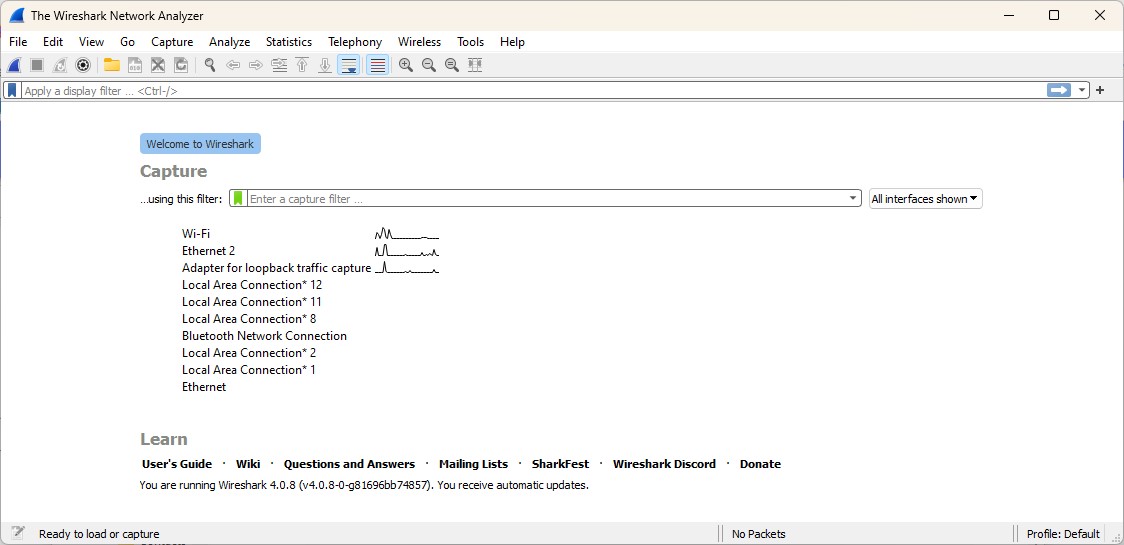
For example the IPv4 address of the machine that the above command was run on is 192.168.1.5. Make a note of this IP address.

Also find the MAC address, which should be listed as “Physical Address”. This is a series of 6 octets (2 hex digits). The MAC address, which is the address of your network card using by Ethernet, is 6 bytes. Since it takes 2 hex digits to represent 8 bits, each pair of hex digits is a single byte. For example 7C hex is 01111100 in

binary. The MAC address of the computer that I was using above is DC:E9:94:0B:6A:E9. Make a note of the MAC address.

## Start Wireshark

What you should see is something like below: start and



mini-meters

adaptors

stop capture

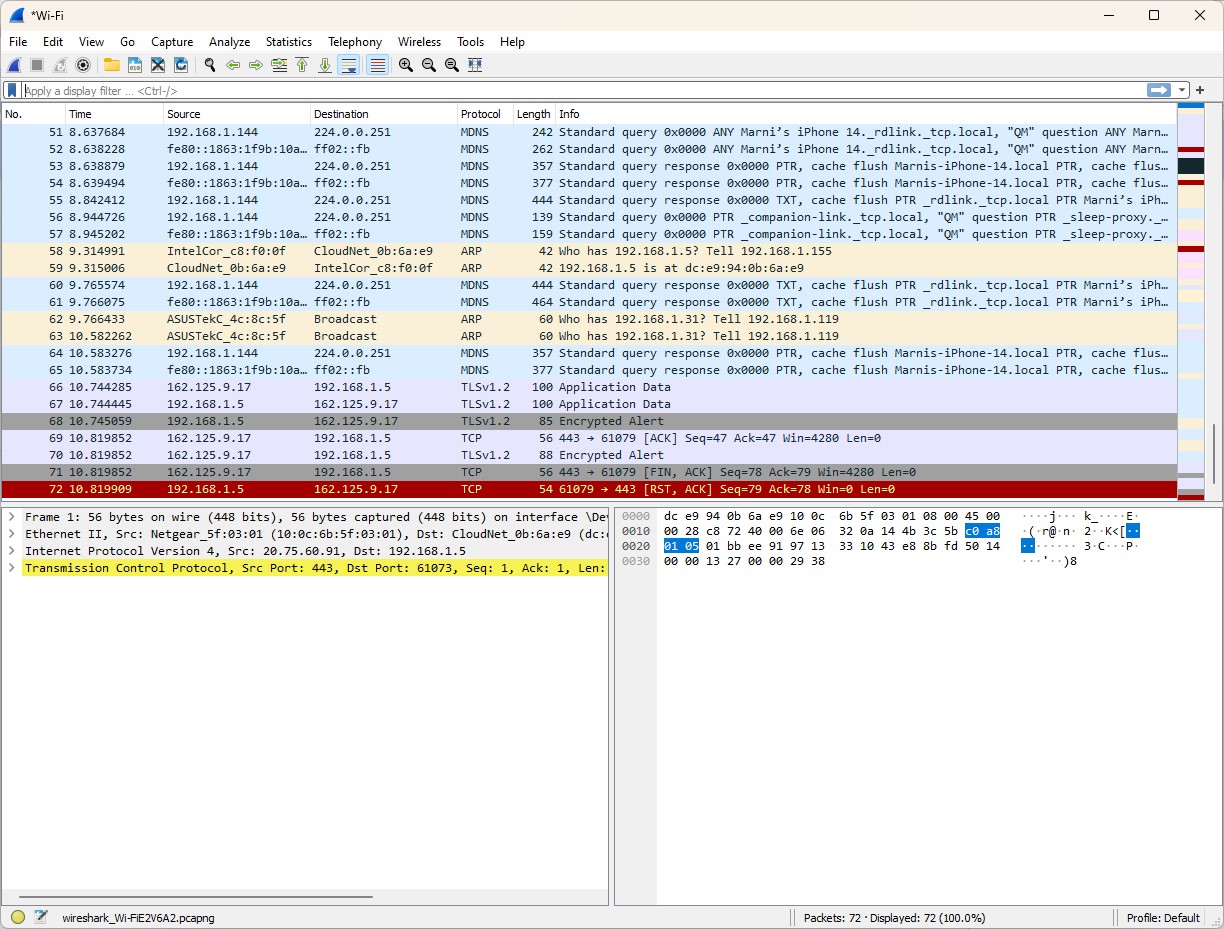
You should see the different adapters that are capable of sending and receiving traffic. To the right of those adapters, you will see a mini-meter, which looks like a bar with some peaks on it, showing the traffic on those adapters. Your active adapter may or may not be the Wi-Fi adapter.

In the top toolbar, just below the menu, on the left will be an icon that looks like a

shark fin and another that is a box (grayed out initially). The shark fin icon will start the capture. Once the capture is started, the box will turn red, and can be pressed to stop the capture. These are the most important buttons as you will need to start capturing packets/frames to inspect, but you also need to stop the capture before it becomes too much data to look at.

# Your first capture

Before you begin capturing data, you will need to make some traffic. You can do this by having a browser window open. Start the capture on Wireshark. Switch to the browser and go to a website (any website), such as google.com, cisco.com, amazon.com, uncw.edu, etc. Once the browser displays the webpage, go back to Wireshark and stop the capture. It is important to stop the capture, because there will be very many packets that will be captured in a very short amount of time. You should see something like this:



Filter bar

You should see a summary of the frames in the upper window. Look for your IP address for your machine in either the Source or Destination fields. In the bottom left window are the protocol layers. For example, you might see frame (Datalink layer), Ethernet (MAC sublayer), Internet Protocol (IP) (Network layer), Transmission Control Protocol (TCP) (Transport layer), etc. These layers are expandable and you can see more details. In the bottom right window is the hex code and text version (when the hex codes are within the ASCII range)of the data.

Type “tcp” in the filter bar and press enter to filter out all but the TCP packets. Look for a frame that has your computer’s IP address as either the Source or the Destination. Expand the frame information in the lower left window. Write down the following information:

1. Frame number

4

1. Frame length (in bytes)

186

1. Arrival time

11:26:14.175585000

Expande the Ethernet II information in the lower left window. Write down the following information:

1. Destination MAC Address

ac:91:a1:37:96:e7

1. Source MAC Address

6c:ab:b7:ad:1a

Expand the IP (Internet Protocol) information. Write down the following information:

1. Destination IP Address

172.20.10.27

1. Source IP Address

34.117.65.55

1. Header Checksum

0x9bb6

Expand the TCP (Transmission Control Protocol) information. Write down the following information:

1. Destination Port

50052

1. Source Port

443

1. Sequence Number (relative number)

1

1. Acknowledgment Number (relative)

1

1. Checksum

0x9322

# Address Resolution Protocol (ARP)

We will generator some ARP traffic and examine the frames. First, get a report of the ARP cache using the command-prompt window by typing the command: **arp -a**. The results will look something like this:

C:\Users\mfern>arp -a

Interface: 192.168.1.5 --- 0x9

Internet Address Physical Address Type

192.168.1.1 10-0c-6b-5f-03-01 dynamic

192.168.1.155 cc-2f-71-c8-f0-0f dynamic

192.168.1.255 ff-ff-ff-ff-ff-ff static

224.0.0.2 01-00-5e-00-00-02 static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.251 01-00-5e-00-00-fb static

224.0.0.252 01-00-5e-00-00-fc static

224.0.1.60 01-00-5e-00-01-3c static

239.0.0.1 01-00-5e-00-00-01 static

239.255.255.250 01-00-5e-7f-ff-fa static

255.255.255.255 ff-ff-ff-ff-ff-ff static

You may have more or less entries as well as the IP addresses may be different. What the data is telling you is what the physical address (the MAC address) is of the adapter that currently has a particular IP address. There is usually an entry for the gateway, which would be an IP address of something like ?.?.1.1. In the above case, it is 192.168.1.1. All traffic that needs to leave the local network has to go to the gateway.

We want to generate and ARP request for a particular IP address on your local network that is not your own machine. Choose an address that you know is on your local network.

*If the address is already in the cache, you might be able to remove it. You can remove any address from the ARP cache using the command* ***arp -d [IP address]****., although this may not work in the lab because you have to have elevated permissions to remove anything from the cache.*

Once you have determined what IP address to use and you have made sure it is no longer in the cache, then

1. Start a new capture (you not need to save the previous capture if you don’t want to)
2. Switch the the command-prompt window and type the command ping **[IP Address]**. You should see something like this:

C:\Users\mfern>ping 192.168.1.155

Pinging 192.168.1.155 with 32 bytes of data:

Reply from 192.168.1.155: bytes=32 time=58ms TTL=64

Reply from 192.168.1.155: bytes=32 time=70ms TTL=64

Reply from 192.168.1.155: bytes=32 time=95ms TTL=64

Reply from 192.168.1.155: bytes=32 time=96ms TTL=64

Ping statistics for 192.168.1.155:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds:

Minimum = 58ms, Maximum = 96ms, Average = 79ms

1. Stop the capture

The ping command sends a “ping” packet (and ICMP) packet to the computer with the IP address specified. A ping is nothing more than a message of “Hey … are you there?”. The response is nothing more than “Yes, I’m here.”.

Type “arp” in the filter bar and press enter to filter out all but the TCP packets. Look for a frame that has the IP address you used in the ping command above in the “Who as ...”. Expand the Ethernet II and ARP information in the lower left window. Write down the following information:

1. Destination Address (from the Ethernet II information)

ac:91:a1:36:e7:e9

1. Sender MAC address

E4:54:e8:73:75:4c

1. Sender IP address

172.20.10.24

1. Target MAC address

ac:91:a1:36:e7:e9

1. Target IP address

172.20.10.3

Look at the respond frame. Write down the following information:

1. Destination Address (from the Ethernet II information)

ac:91:a1:36:e7:e9

1. Sender MAC address

E4:54:e8:73:75:4c

1. Sender IP address

172.20.10.24

1. Target MAC address

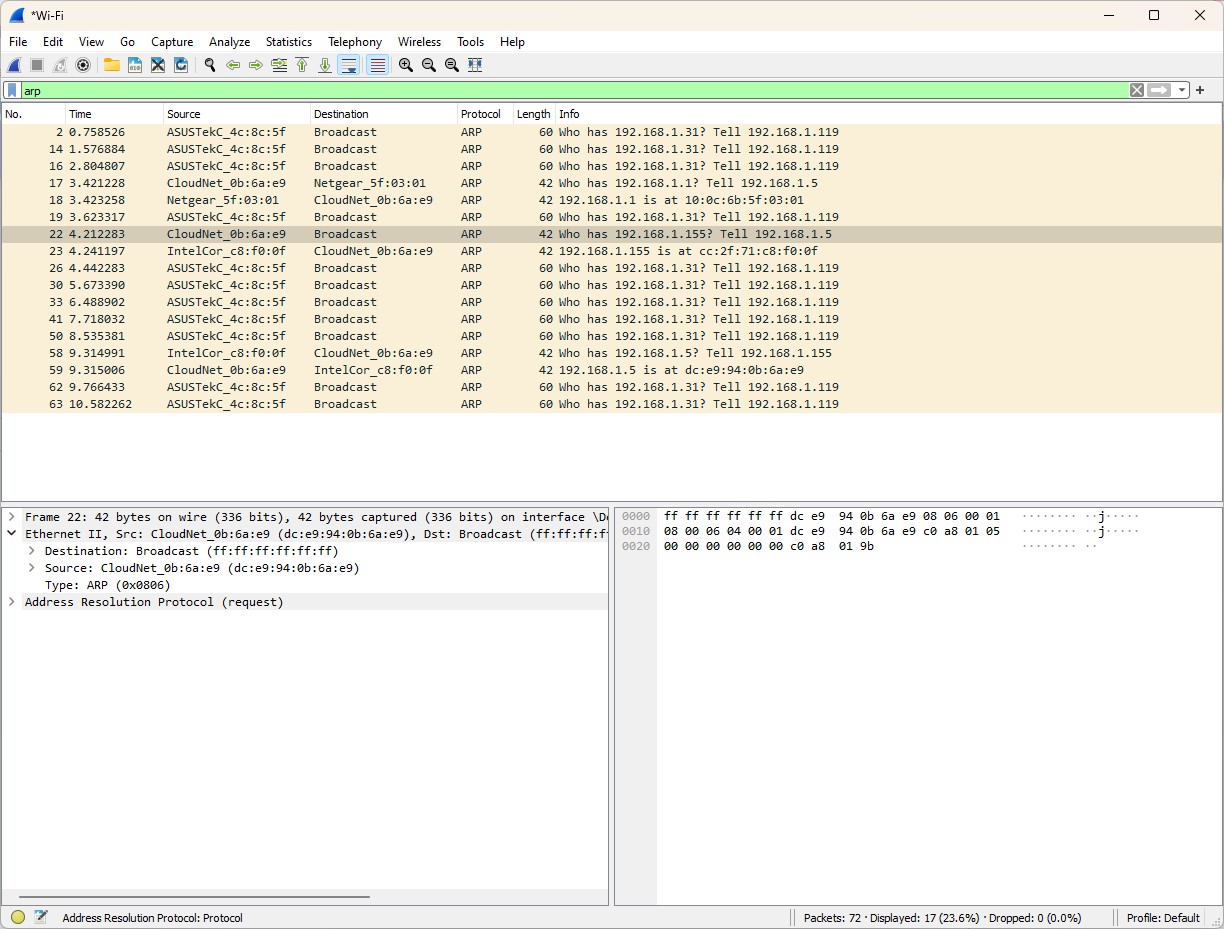
ac:91:a1:36:e7:e9

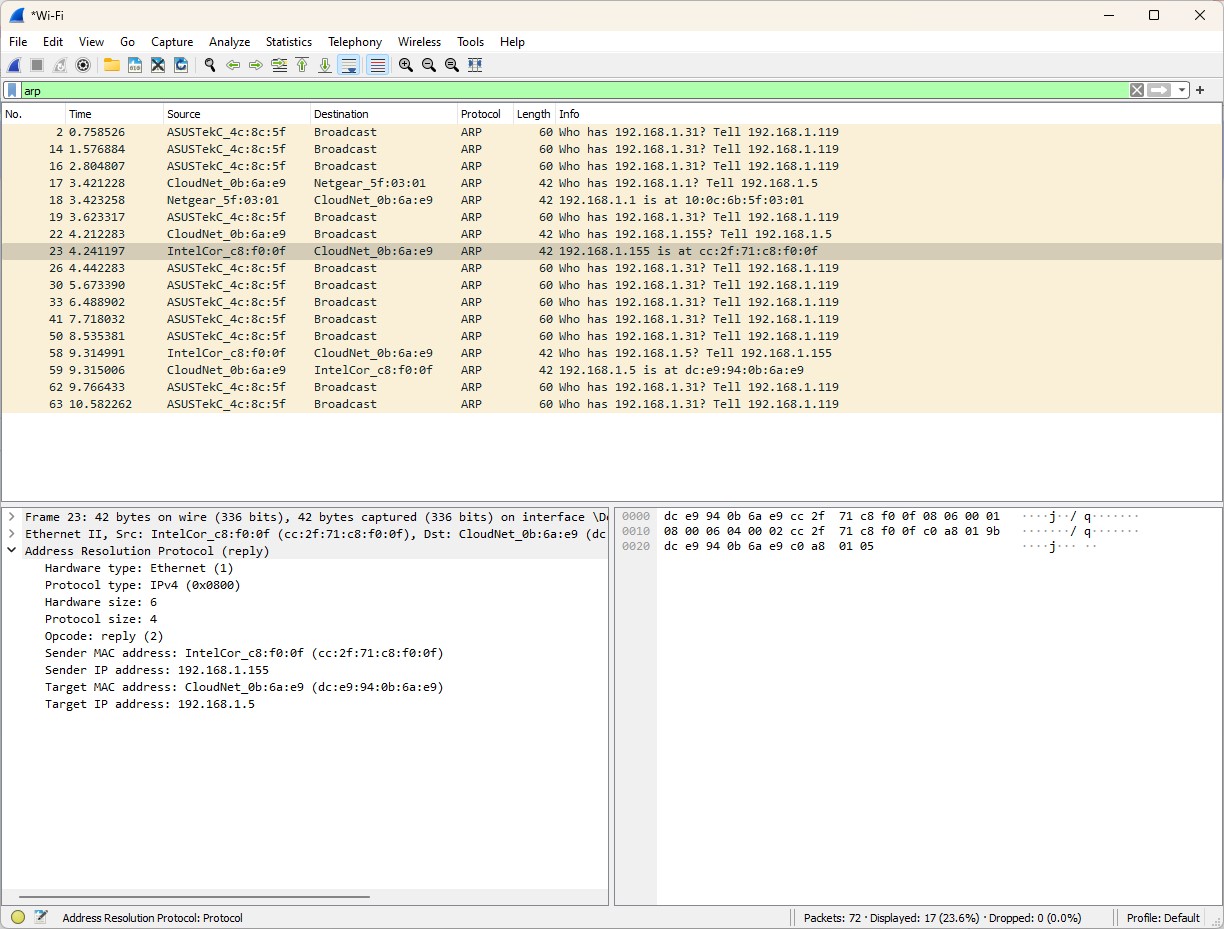
1. Target IP address

172.20.10.3

Look for at and ARP frame that is asking for the owner of an IP address that is not your machine. Do you see a response? Why is there not response?

No I do not see a response. Arp is not asking for ip addresses it asks for mac addresses





Type “icmp” in the filter bar and press enter to filter out all but the ICMP packets. These packets are the actual pings that your computer sent. What are the last two bytes if the data?

69 is the last hex data bytes