WAKE TECH
Building, Engineering, & Skilled Technologies

Wireshark- OSI- Physical & Data-link Layers

BAT-221: BAS Networking

This material is based upon work supported by the National Science Foundation Advanced Technical Education grant program, A New Technician Training Program for Advanced Building Technologies, DUE-2000190.

The opinions, findings, and conclusions or recommendations expressed are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Name: _____ Section: _____

Wireshark- OSI- Physical & Data-link Layers

SYNOPSIS

In this lab, we are going to use Wireshark to analyze the two lowest layers of the OSI model: Physical and Data-link layer.

OBJECTIVES

Upon completion of this activity the student will be able to:

- Capture and analyze network traffic using Wireshark.
- Analyze the OSI Physical layer in Wireshark.
- Understand the fields that make up a frame in the OSI Data-link layer.
- Analyze the OSI Data-link layer in Wireshark.

PARTS AND EQUIPMENT

- Networked laptop

SOFTWARE

- Wireshark [https://www.wireshark.org/]

REFERENCES

- What is a MAC Address: How to Find and Identify [https://whatismyipaddress.com/mac-address]
- OSI Model [http://www.practicalnetworking.net/series/packet-traveling/osi-model/]
- What is the Internet Control Message Protocol (ICMP)? [https://www.fortinet.com/resources/cyberglossary/internet-control-message-protocol-ICMP]

MANUALS

- Network Communications for Buildings [https://www.ccontrols.com/pdf/NCB2015.pdf]

BACKGROUND

The MAC address is a 48-bit (6 byte) network address. The MAC address is used to uniquely identify devices on a network.

A MAC address is hardcoded onto the network adaptor by the manufacturer. The manufacturer makes sure the address is unique.

The MAC address will appear be written using hexadecimal numbers and will usually appear in the following formats:

- A0-51-0B-29-C9-4E
- A0:51:0B:29:C9:4E

The MAC address is used for source and destination address at the Data-link layer.

PROCEDURES

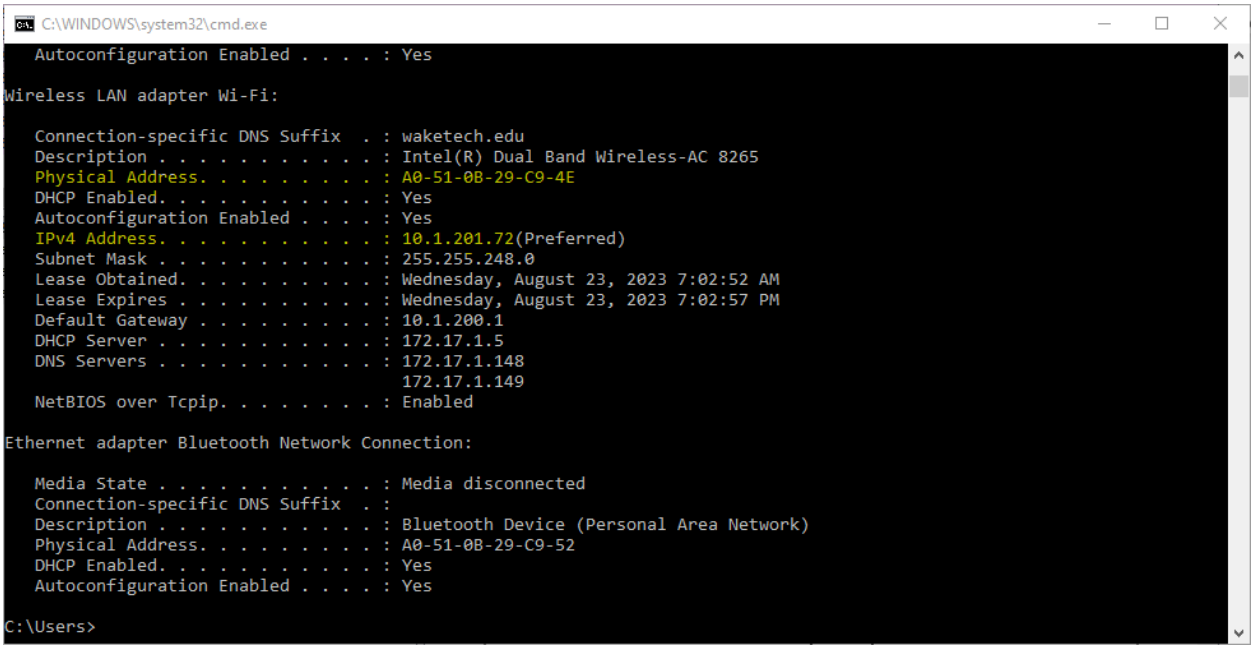
Part 1: Network configuration

We need to get the IPv4 address and MAC address of the network adaptor that we are going to be capturing traffic on.

1.1 - Laptop configuration

An ipconfig will give us the IPv4 address but we also want to know the MAC address on the network adaptor, so we are going to run it without the /all switch.

Run an "ipconfig /all" to get the IPv4 address and the MAC address:



What is the MAC (Physical) address of our network interface?_____

What is the IPv4 address of our network interface?_____

What is the IPv4 address of the Default Gateway?_____

1.2 - Default gateway

To reach outside out LAN, we go through the Default Gateway. While we have the IPv4 address of the Default Gateway, we need to get the MAC address of Default Gateway. We have already gotten the IPv4 address of the Default Gateway from our network interface.

ARP

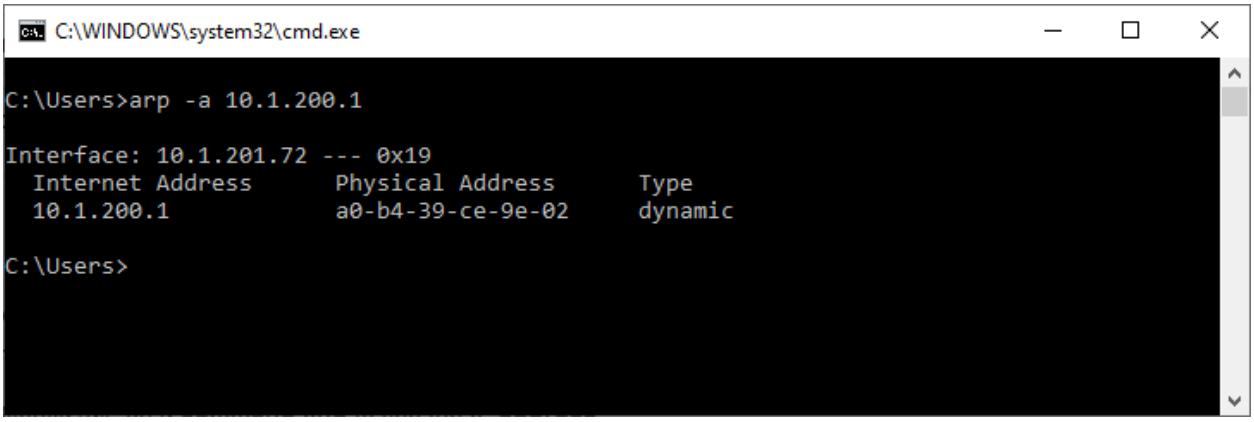
ARP is a protocol that maps an IP address to a MAC (Physical) address.

We can use the dos "arp" command to get the translation between the two.

Run the arp command with the -a switch with the IPv4 address of the Default Gateway.

What is the IPv4 address of the Default Gateway from our network interface?_____

_____



What is the MAC address of the Default Gateway?_____

1.3 - Summarize

Summarize the MAC and IPv4 address for our interface network as well as the Default Gateway.

Network Interface MAC address?_____

Network Interface IPv4 address?_____

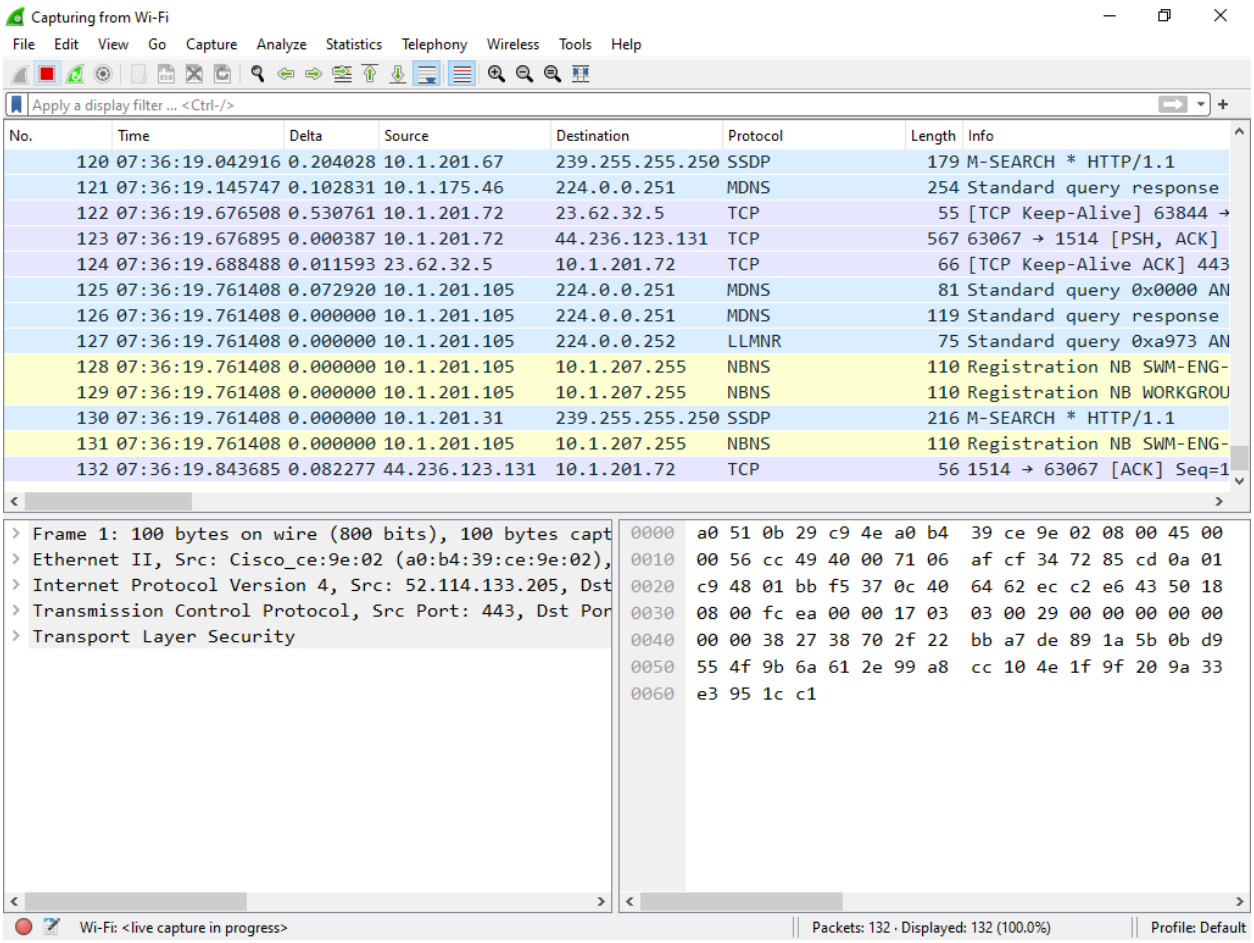
Default Gateway MAC address?_____

Default Gateway IPv4 address?_____

Part 2: Wireshark

2.1 - Wireshark Capture

Start Wireshark and it should start capturing network traffic once you have selected the network interface.

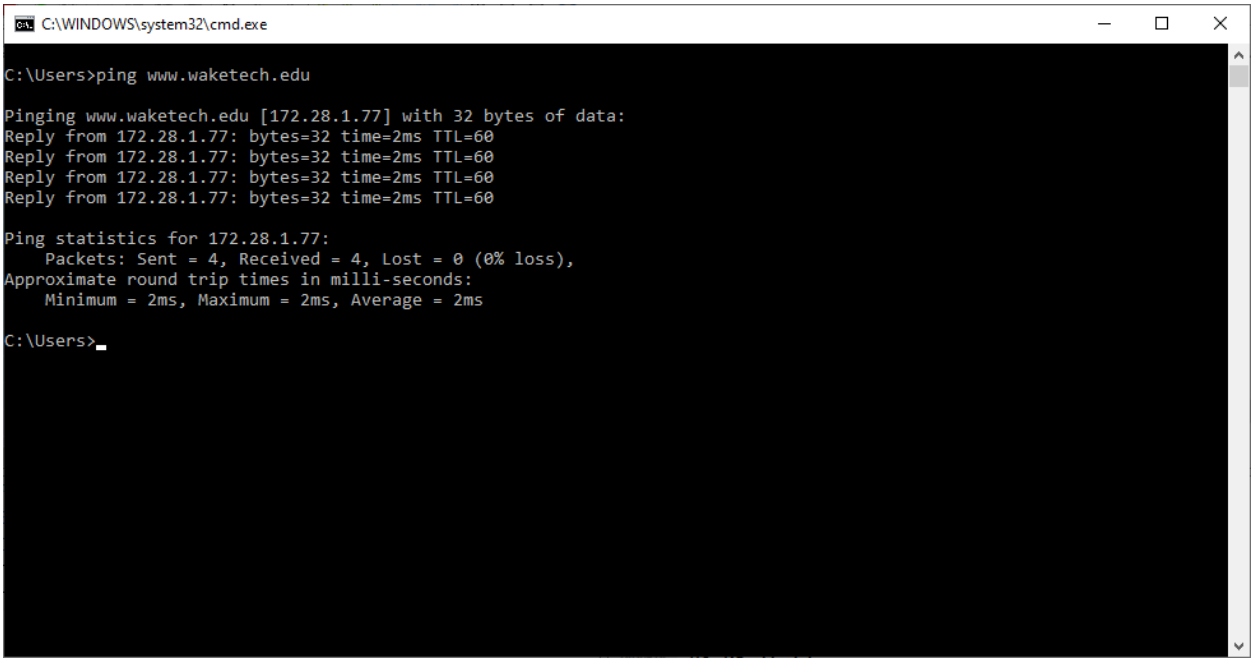


2.2 - Ping traffic

The network frames that we are going to be examining are ICMP packets. We are going to generate ICMP requests by using the dos “ping” command.

The dos “ping” command by default generates four ICMP requests.

Open a command prompt window and ping www.waketech.edu.

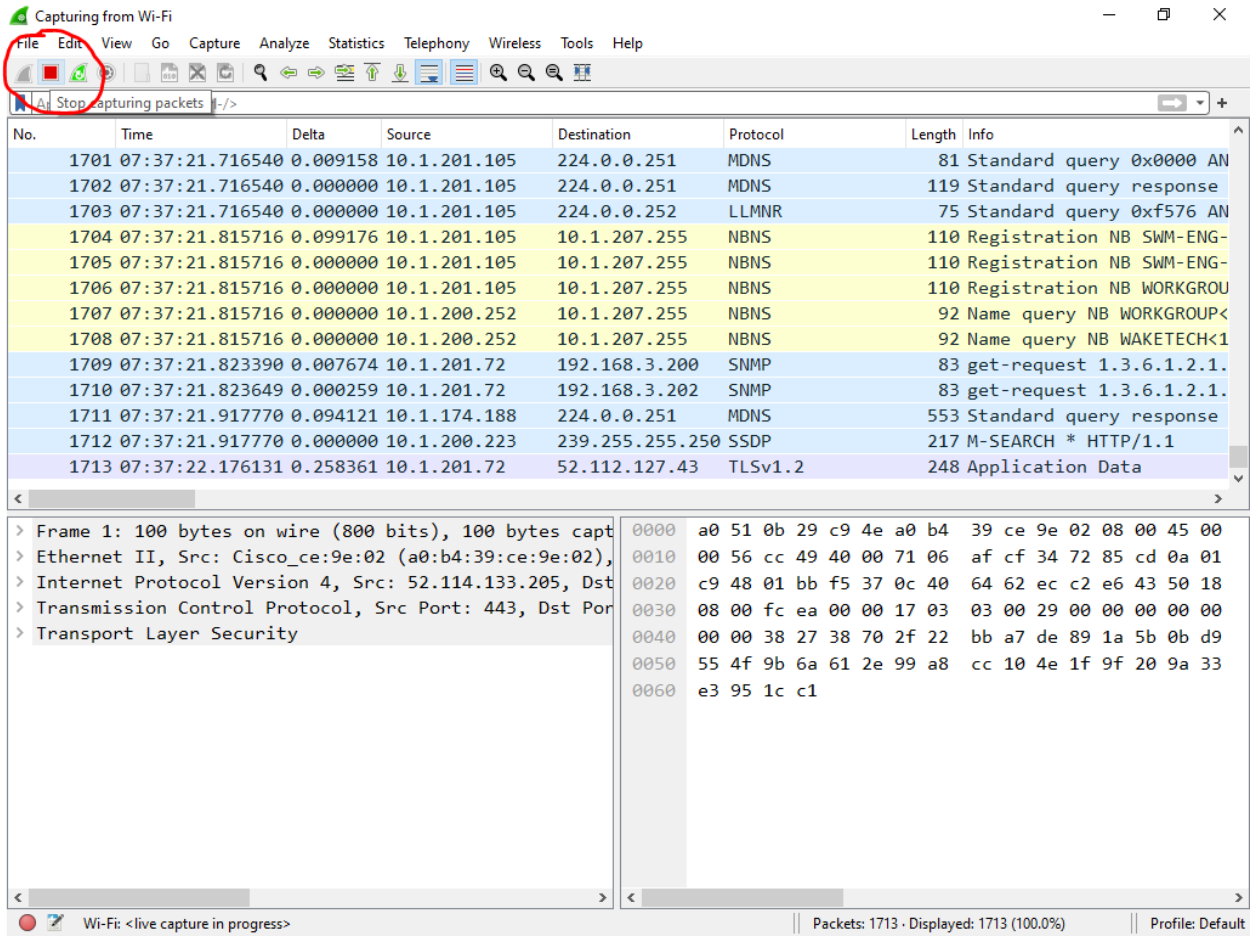


2.3 - Stop Capture

Wireshark should have captured the network traffic that we want to examine. There is no need for Wireshark to continue to capture packets.

You can stop capturing network traffic by one of the following ways:

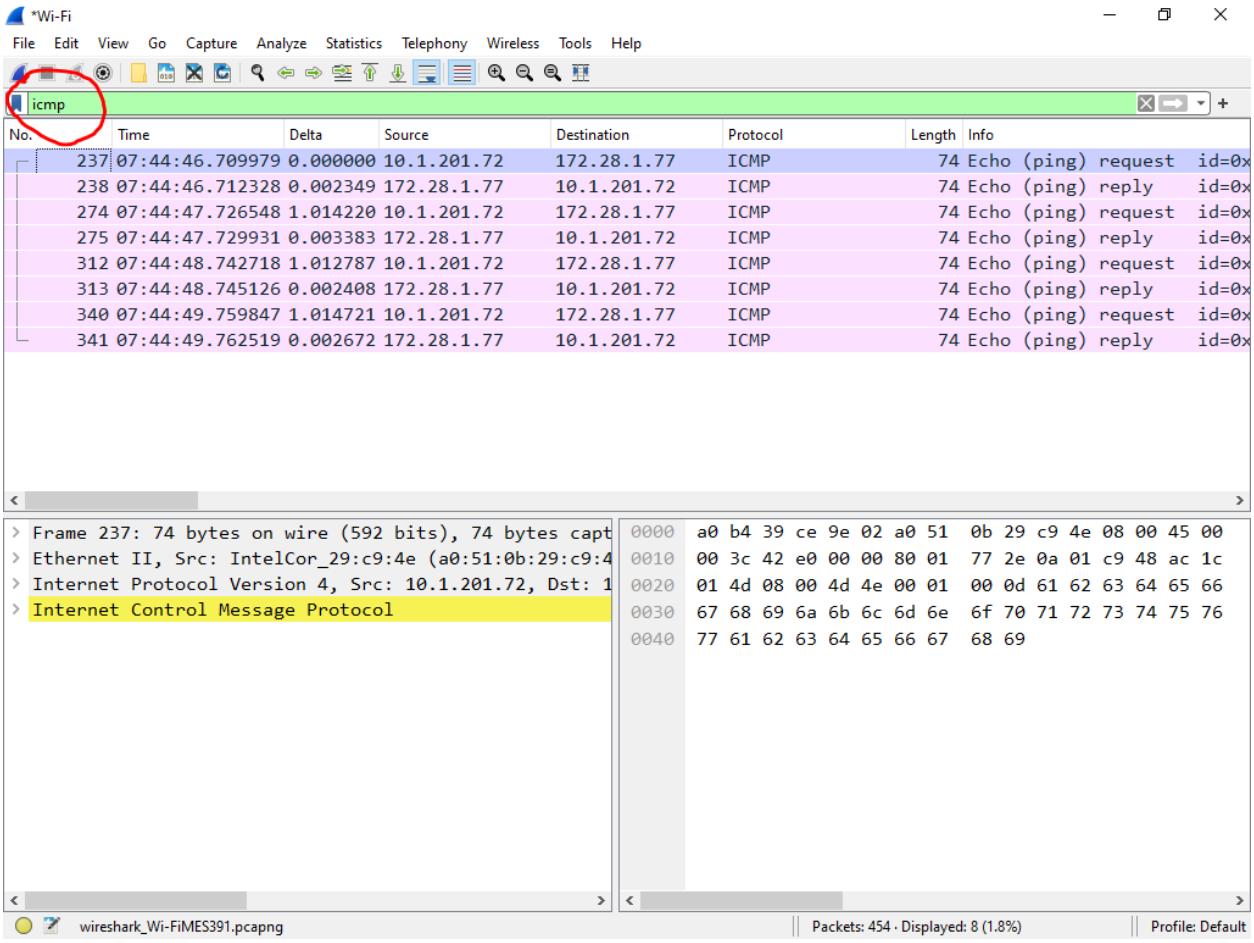
1. Toolbar: Click “Stop capturing packets” icon
2. Menu: Capture → Stop
3. Shortcut: CTRL+E



2.4 - Filter ICMP requests

Even though we were only capturing network traffic for a small period of time, Wireshark would have captured hundreds if not thousands of packets. We want to limit packets to just show the ICMP requests and replies.

1. In the filter window type “ICMP” and hit Enter.



You should see 8 packets in the Packet List pane. The 8 packets represent the 4 ICMP requests and a reply back for each request.

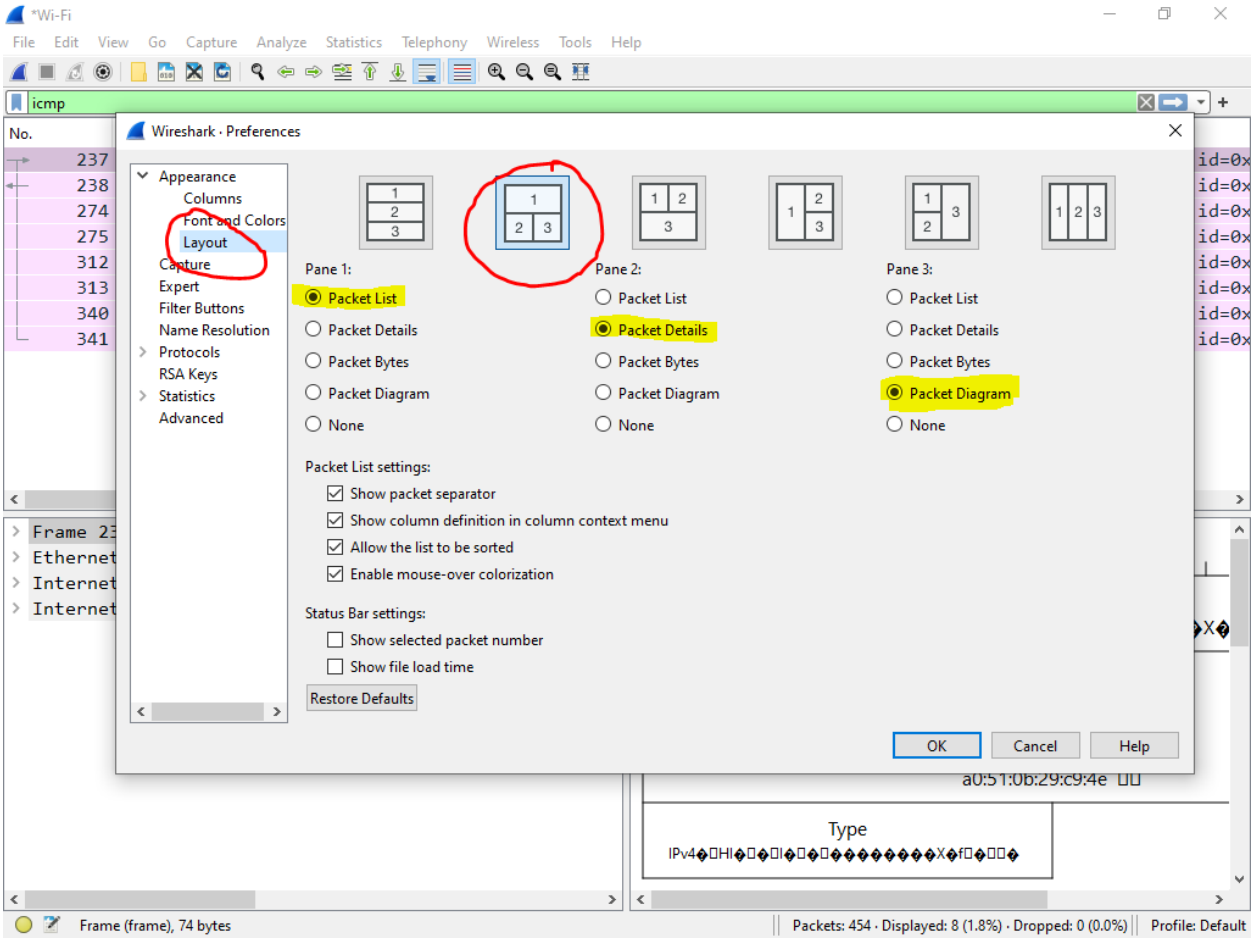
2.5 - Wireshark Configuration

We want to see the Packet Diagram in our view, so we need to set some preferences. The Packet Diagram shows a physical layout of the packet and makes looking at the frames easier.

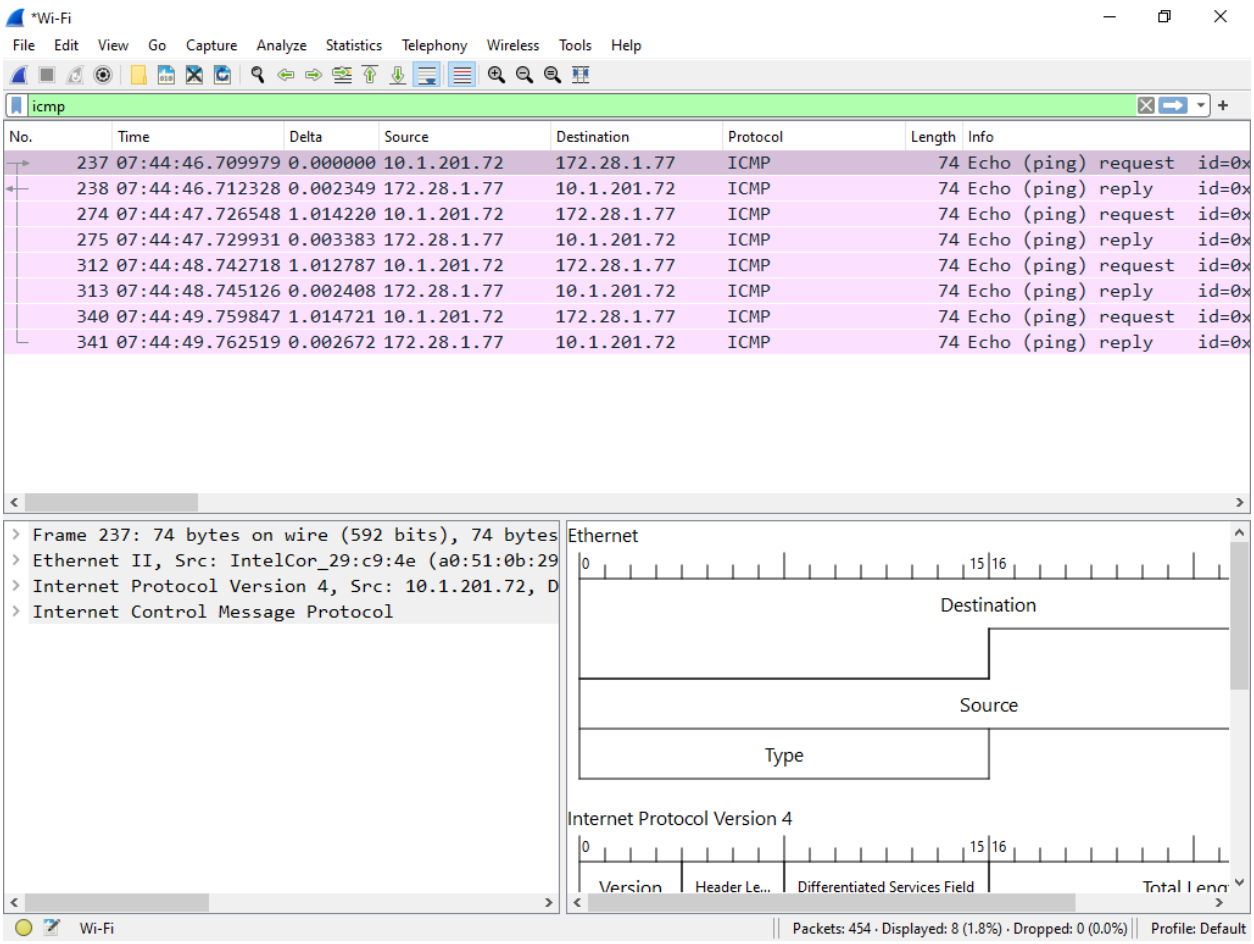
Open the preferences by one of the following means:

- Menu: Edit → Preferences…
- Shortcut: Ctrl+Shift+P

We want to change the layout of the Wireshark panes and we want to see the Packet Diagram in Pane 3. Make sure to save your preferences.



Your screen should look like this now:



Packet List

The top pane is the Packet List and shows all the packets that have been filtered. If you select a packet, then the panes below change to show that packet's information.

Packet Details

The bottom left pane is the Packet Details and shows the OSI model of the packet selected in the Packet List.

You can expand each level in the Packet Details to see more information.

Packet Diagram

The bottom right pane is the Packet Diagram and shows the frame in a physical diagram that makes looking at the data easier. It shows the packet selected in the Packet List.

Right-click the Packet Diagram and Select "Show Field Values" so the field values will be shown in the Packet Diagram pane.

Part 3: OSI – Physical layer

The Physical layer is the first layer of the OSI Model. It includes anything physically needed to send data from one location to another.

There are many possible mediums for the data to travel over and some examples are:

- Category cable
- Fiber
- Wireless

The network adapters of the Physical layer handles encoding the data into a format necessary to transfer the data based upon the medium. For Category cable, the data is encoded and transferred using voltages while fiber would utilize light. Radio waves are part of the Physical layer for Wireless.

The Physical layer includes but is not limited to:

- Network adaptors
- Medium
    - Copper and voltages for Category cables
    - Antennas and radio waves for Wi-Fi
- Hardware

Are the network adaptors considered part of the Physical layer?_____

For Category cables, how is the data represented over the wire?_____

Are radio waves considered part of the Physical layer?_____

If we are discussing speech from one person to another, name three items that would be considered part of the Physical layer?_____

_____

_____

_____

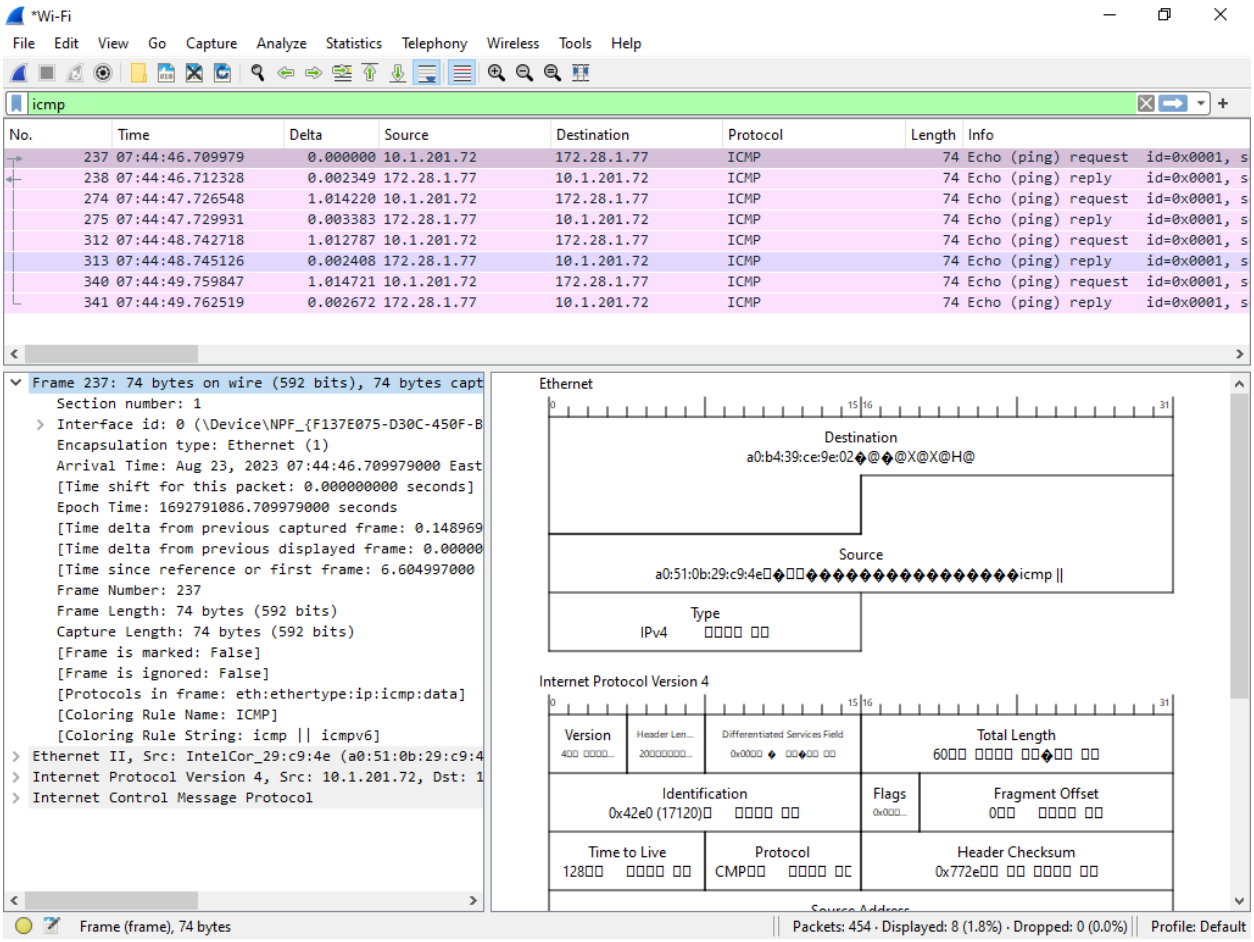
_____

Part 4: Wireshark – Physical layer

We are going to examine the Physical layer in Wireshark.

Select the first packet in the Packet List. The first item in the Packet Details window represents the Physical layer of the OSI model.

Expand the Physical layer.



The Packet Diagrams pane is the bottom right pane. The Physical layer is not represented in the Packet Diagram pane and the top entry here represents the Data-link layer.

How many bytes are in this frame?_____

How many bits are in this frame?_____

There are 8 bits per byte. Does the number of bytes correspond to the number of bits in this frame?_____

What date & time did this frame arrive at?_____

Expand the "Interface id" and what is the Interface description?_____

_____

Does the interface description match the network connection listed in "ncpa.cpl" that you are capturing traffic on for Wireshark?_____

In the Physical layer, do you see a MAC address field or an IPv4 address field?_____

In the Physical layer, why do you see or not see a MAC address field or an IPv4 address field?_____

_____

_____

_____

Part 5: OSI – Data Link layer

The Data-Link layer is the second layer in the OSI model. The Data-link layer is responsible for the node-to-node delivery. It delivers the data from a source node to the destination node and just moves data to the next hop.

The addressing for the Data-link layer is the MAC (media access control) or Physical address. While we may refer to devices by their IP address, the network utilizes the MAC address for its addressing at this layer.

The Data-link layer can only transmit to a node in the same LAN.

5.1 - MAC address

What is MAC an abbreviation for?_____

Is the MAC address the same as the Physical address?_____

How many bytes is a MAC address?_____

5.2 - Ethernet II DIX frame

Answer the questions in this Part with help from the Network Communications for Buildings manual.

Using the manual, look at the Ethernet Frames section under Shared Ethernet to answer the following questions.

Ethernet II fields

Looking at the Ethernet II DIX Frame, answer the following questions:

What field is the first 64 bits (8 bytes)?_____

What field is the next 48 bits (6 bytes)?_____

What field is the next 48 bits (6 bytes)?_____

What field is the next 16 bits (2 bytes)?_____

What field is the next field?_____

What field exists after the Data field?_____

Preamble field

When calculating the size of the frame is the Preamble field considered part of the Ethernet frame?_____

Destination field

Is the Destination field a MAC address or IPv4 address?_____

How many bits is the Destination field?_____

What is the purpose of the Destination field?_____

_____

_____

Does the Destination field represent the next hop or the final destination?_____

Is the Destination field a node in the same LAN?_____

Source field

Is the Source field a MAC address or IPv4 address?_____

How many bits is the Source field?_____

What is the purpose of the Source?_____

_____

_____

Data Type field

Does the Data-link layer guarantee delivery of data?_____

If delivery of data is guaranteed who would do that?_____

What is the purpose of the Type field?_____

_____

_____

Data field

What is the minimum size of the Data field?_____

What is the maximum size of the Data field?_____

What is a runt packet?_____

_____

_____

Frame Check Sequence field

The Frame Check Sequence is sometimes abbreviated to FCS.

What is the purpose of the FRC field?_____

How does the destination node utilize the FRC field?_____

What is considered a successful transmission according to the FRC field?_____

At this layer, if the destination calculates the FRC and the calculated FRC does not match the FRC field sent in the frame, is the source node informed?_____

Part 6: Wireshark – Data-link layer – ICMP request

We are going to look at an Ethernet frame in Wireshark.

Close the expanded Physical layer in the Packet Details pane to hide the Physical layer details.

The second item in the Packet Details represents the second layer of the OSI model. Expand the second item in the Packet Details list to show the frame in the Packet Diagram pane.

6.1 - ICMP request

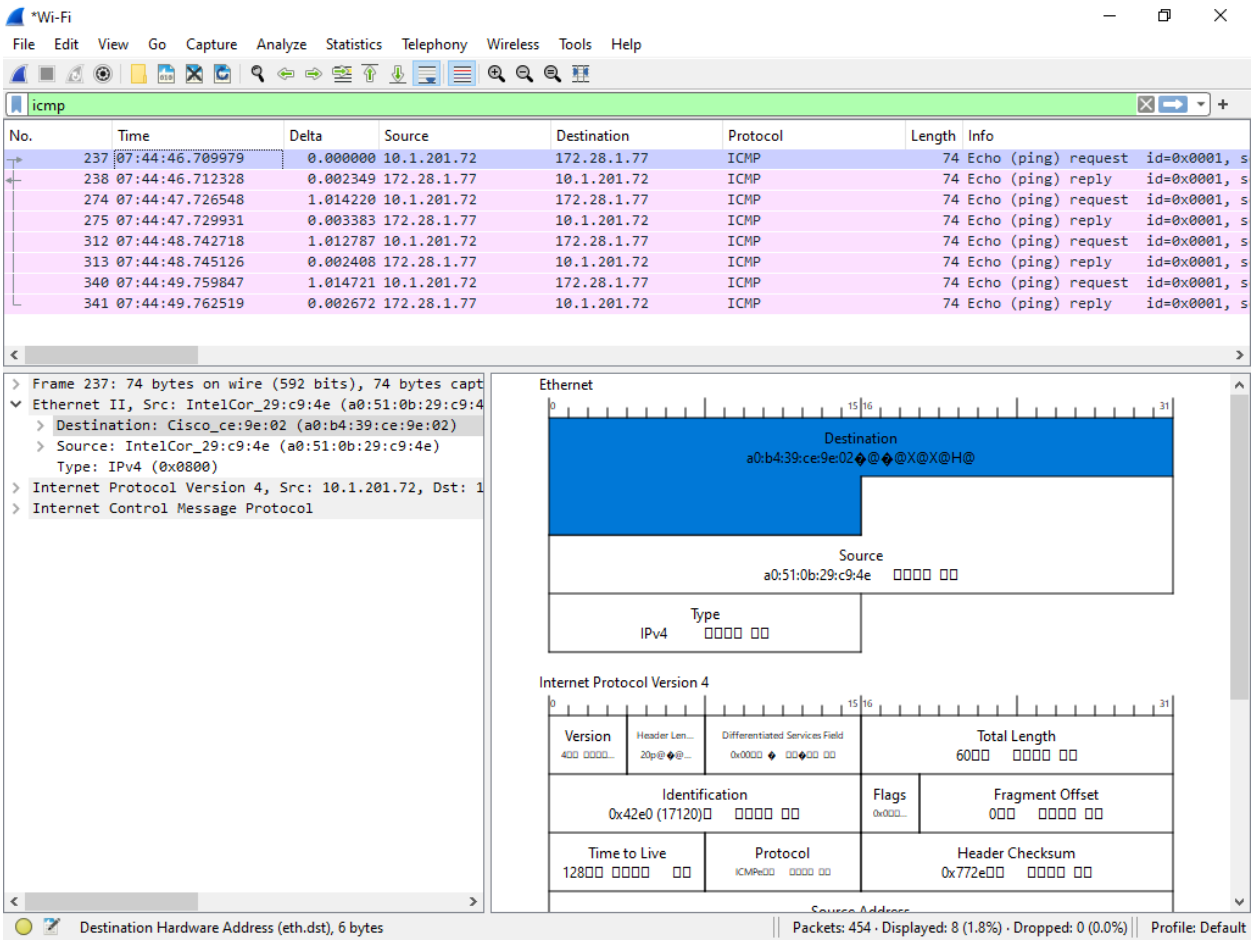
Make sure you are still looking at the first packet in the Packet List as this is an ICMP request. In an ICMP request, your laptop is sending a request to www.waketech.edu. With the request, your laptop is the source.

The Data-link layer just handles node-to-node traffic.

For any traffic to travel outside your LAN, the traffic will go through the Default Gateway, so the Default Gateway is where this ICMP request is going to. While there are many more hops before the packet gets to the final destination; we are only capturing the traffic to and from our network interface. With the ICMP request, the Default Gateway is the destination because the final destination is outside our LAN.

Destination field

Click on the Destination field in the Packet Details and you should see the Destination field will be highlighted in the Packet Diagram in the right pane.



What is the Destination (MAC address only) of the Ethernet frame?_____

What is the MAC address of your Default Gateway?_____

Is the Destination of the Ethernet frame the same as the Default Gateway?_____

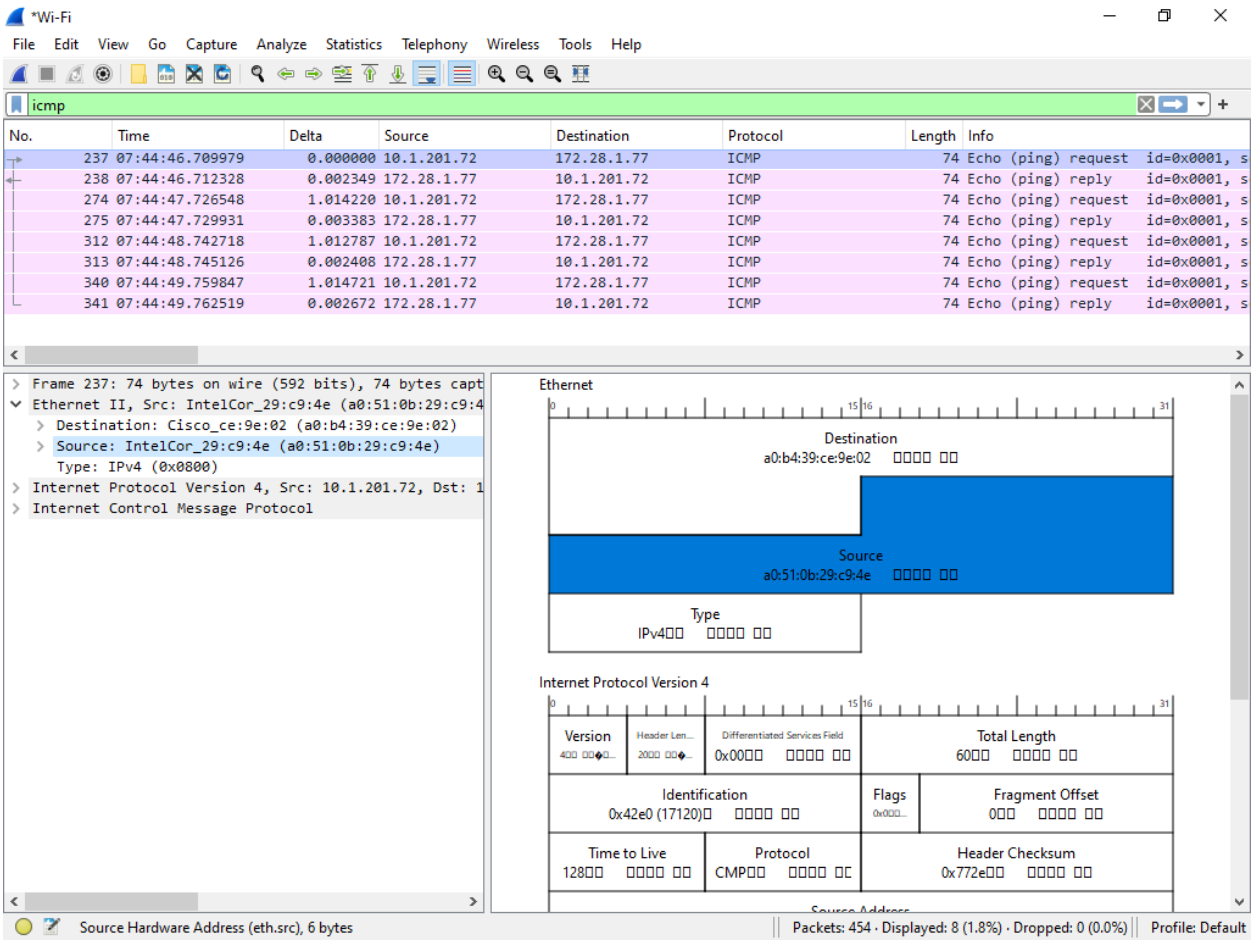
- If you answered No, troubleshoot the issue.

The Destination field is how many bytes?_____

The Destination address of the Ethernet frame should match the MAC address of the Default Gateway.

Source field

Click on the Source field in the Packet Details and you should see the Source field will be highlighted in the Packet Diagram in the right pane.



What is the Source (MAC address only) of the Ethernet frame?_____

What is MAC address of your network interface from Part 1?_____

Is the Source of the Ethernet frame the same as your network interface?_____

- If you answered No, troubleshoot the issue.

The Source field is how many bytes?_____

The Source address of the Ethernet frame should match the MAC address of your network interface. This shows that your network interface is sending the data.

Type field

What is the Type field of the Ethernet frame?_____

Preamble field

Do you see the Preamble field?_____

Why do you see or not see the Preamble field?_____

_____

_____

_____

FCS field

Do you see the FCS field?_____

Why do you see or not see the FCS field?_____

_____

_____

_____

IP Address

In the Data-link layer, is the IPv4 address referenced?_____

In the Data-link layer, why do you see or not see an IPv4 address?_____

_____

_____

_____

Part 7: Wireshark – Data-link layer – ICMP reply

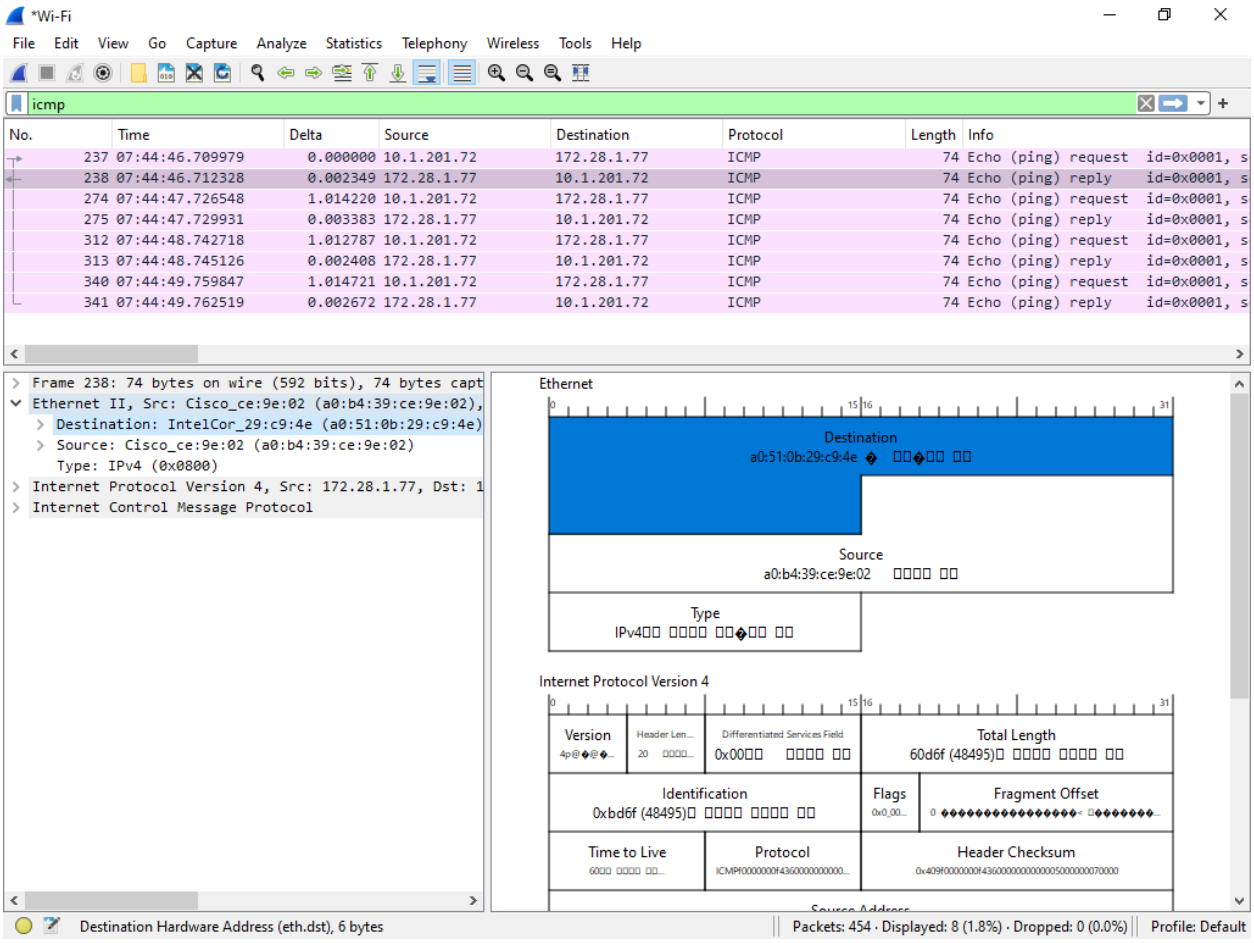
7.1 - ICMP reply

Select the second packet in the Packet List pane is the reply to the first packet which was a request.

We want to look at the ICMP reply which is the response to our request. Now this implies the packet is going to our laptop. With the ICMP request, our network interface was the source; however, with the ICMP reply out network interface is the destination.

Destination field

Click on the Destination field in the Packet Details.



What is the Destination (MAC address only) of the Ethernet frame?_____

What is MAC address of your network interface?_____

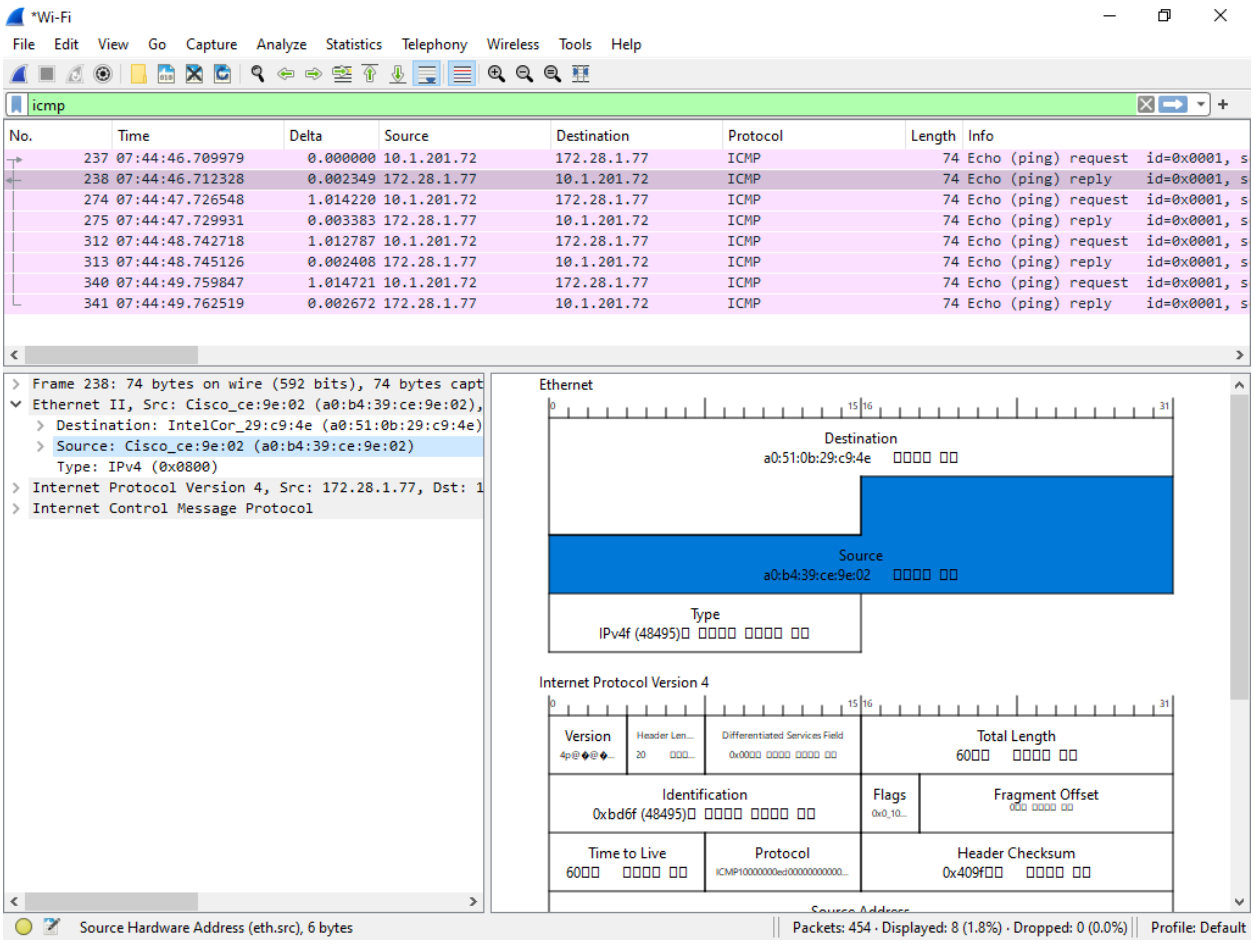
Is the Destination of the Ethernet frame the same as your network interface?_____

- If you answered No, troubleshoot the issue.

Since this is the ICMP reply, the Destination address of the Ethernet frame should match the MAC address of your network interface.

Source field

Click on the Source field in the Packet Details.



What is the Source (MAC address only) of the Ethernet frame?_____

What is MAC address of your network interface from Part 1?_____

Is the Source of the Ethernet frame the same as the Default Gateway?

- If you answered No, troubleshoot the issue.

Since this is an ICMP reply, the Source address of the Ethernet frame should match the MAC address of the Default Gateway. This shows that your network interface is sending the data.

Part 8: Summary

How many bits is a MAC address?_____

How many bytes is a MAC address?_____

Does the OSI Physical layer reference an address?_____

In the OSI Data-link layer, what types of addresses are used?_____

In detail, explain why the source address of the ICMP request is the destination of the ICMP reply?_____

In detail, explain why the destination address of the ICMP request is the source of the ICMP reply?_____