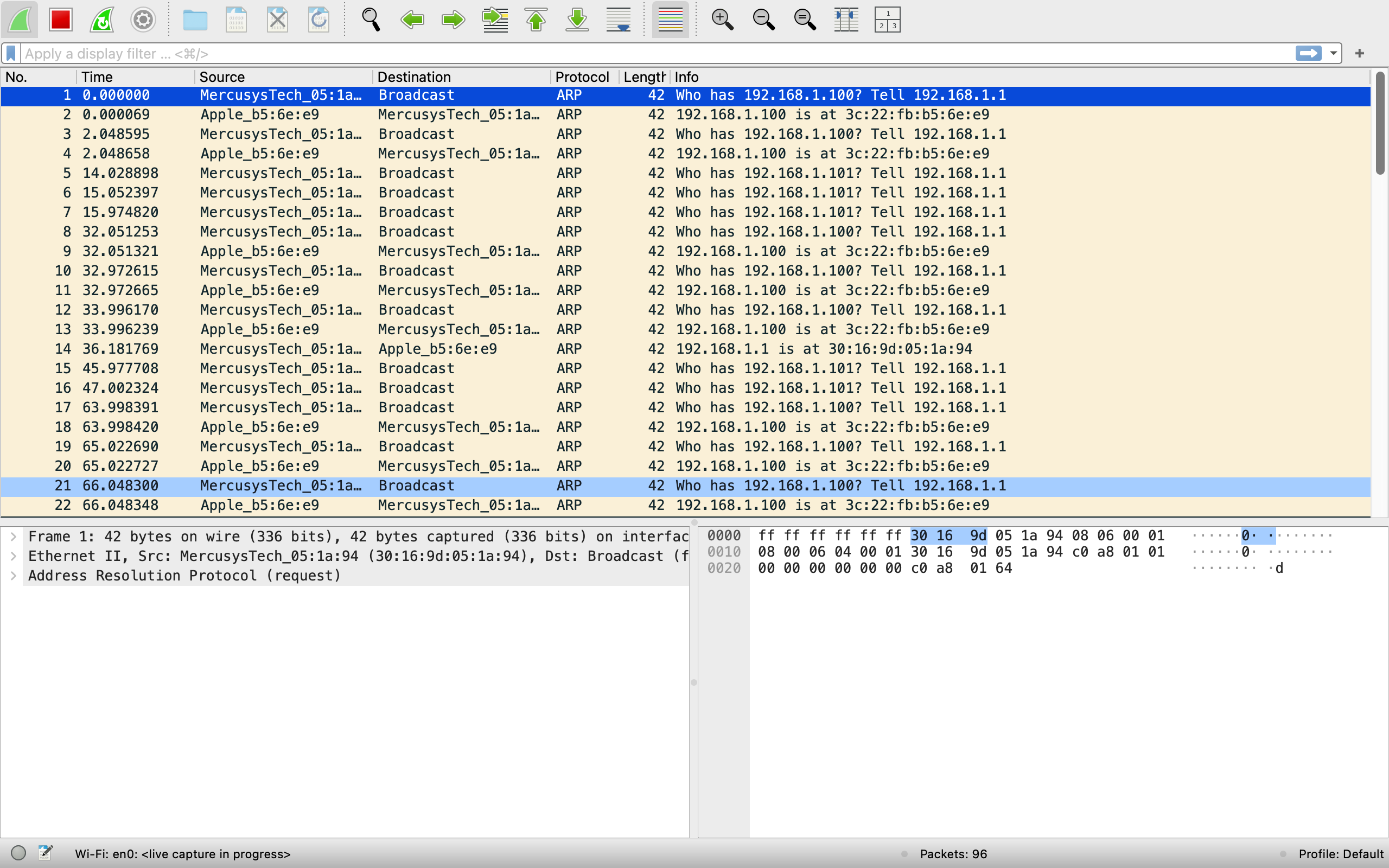
Lab - Using Wireshark to Examine Ethernet Frames

Part 1

Step 1-2



### **Part 1: Examine Ethernet II Header Contents of an ARP Request**

**Step 1-2**

**Step 3: Examine the Ethernet II Header Contents of an ARP Request**

1. **Why does the PC send out a broadcast ARP prior to sending the first ping request?**
2. The PC sends a broadcast ARP to discover the MAC address corresponding to the target IP address before it can send the ping request.
3. **What is the MAC address of the source in the first frame?**

The source MAC address is f4:8c:50:62:62:6d.

1. **What is the Vendor ID (OUI) of the Source’s NIC?**

The Vendor ID (OUI) is f4:8c:50.

1. **What portion of the MAC address is the OUI?**

The first 6 hexadecimal digits (f4:8c:50) are the OUI.

1. **What is the Source’s NIC serial number?**

The Source’s NIC serial number is 62:62:6d.

### **Part 2: Use Wireshark to Capture and Analyze Ethernet Frames**

In Part 2 of the lab, you will use Wireshark to capture and analyze Ethernet II frames in a controlled network environment. The goal is to examine how data is encapsulated in Ethernet frames and transmitted over a network.

Ethernet II frames consist of several key fields: Destination MAC Address, Source MAC Address, EtherType, Payload, and Frame Check Sequence (FCS). These frames are used to encapsulate higher-layer protocols like IP and TCP. By capturing these frames with Wireshark, you will be able to analyze their structure and gain a deeper understanding of data transmission at the Data Link Layer.

The lab begins by setting up a network using Mininet, which simulates a network of hosts and switches. After the setup, you will use Wireshark to monitor traffic from Host H3. Wireshark will allow you to filter and inspect the Ethernet frames in real-time, focusing on the header fields like the MAC addresses and EtherType.

This analysis is crucial for understanding how devices communicate over a network and for troubleshooting issues like network congestion or security threats. Overall, Part 2 enhances your knowledge of Ethernet frames and gives you practical experience with network analysis tools like Wireshark.

### **Part 3-4: Summary of Steps Performed in Part 2**

**Ping Command from Host H3:**

In the Host H3 terminal, I used the ping command to send 5 ICMP Echo Request packets to the default gateway 10.0.0.1.

**Command used:** ping -c 5 10.0.0.1

This command sent 5 ICMP Echo Request packets and waited for ICMP Echo Replies from the gateway, displaying the round-trip times for each packet.

**Wireshark Capture:**

While performing the ping operation, I had Wireshark running in the background, capturing the network traffic. The capture should have shown both the ICMP Echo Request and ICMP Echo Reply packets between Host H3 and the default gateway.

**Stopping Wireshark Capture:**

After completing the ping test and observing the captured packets, I stopped the Wireshark capture to prevent further unnecessary packet capture.

**Applying ICMP Filter in Wireshark:**

To focus on only the ICMP traffic, I applied a filter in Wireshark by using the filter icmp. This filter ensured that the displayed capture results only show ICMP Echo Requests and ICMP Echo Replies, eliminating other unrelated network traffic from the view.

### **Part 5: Examine the First Echo (Ping) Request in Wireshark**

**Examine the First Echo (Ping) Request in Wireshark:**

In Wireshark, I selected the first frame in the Packet List pane. This frame represented the Echo (ping) request. In the Packet Details pane, I reviewed various information, such as:

* Frame length and Ethernet II frame type: The source and destination MAC addresses were displayed, which helped identify the MAC address of the PC's NIC and the default gateway's MAC address.
* I clicked the arrow on the second line to expand and obtain more details about the Ethernet II frame.
* I also observed the source and destination IPv4 addresses in the data field of the frame. The source IP address and destination IP address were displayed.

**Examine the Echo Reply Frame:**

I selected the next frame, which was the Echo reply. I noticed that the source and destination MAC addresses had reversed because the reply came from the default gateway. I identified the device and MAC address displayed as the destination in the Echo reply frame.

**Start a New Capture in Wireshark:**

I started a new Wireshark capture after clicking the Start Capture icon and selected Continue without Saving for the previous capture. From the H3 terminal, I sent 5 ping requests to 172.16.0.40.

**Examine the New Data in Wireshark:**

I reviewed the first echo request frame in the Packet List pane. I checked the source and destination MAC addresses and source and destination IP addresses in the data field. Comparing these addresses with those from Step 5, I noted that the destination IP address had changed, while the destination MAC address remained the same.