M4 Lab: Data Link Layer

CITA 220: DATA COMM & NETWORK TECH

Gonzalez, Marco A.
SUNY CANTON | 34 CORNELL DRIVE, CANTON, NEW YORK 13617

TABLE OF CONTENTS

1 TABLE OF FIGURES

2 TABLE OF TABLES

3 WINDOWS

This section reviews some Windows data link layer commands. Use a Command Prompt.

3.1 MAC ADDRESS

A MAC address is a **locally significant** device identifier. There are two common methods to obtain the MAC addresses.

3.1.1 Method 1 (ipconfig)

Execute the following command. The MAC address is displayed as **Physical Address**. See Figure 1.

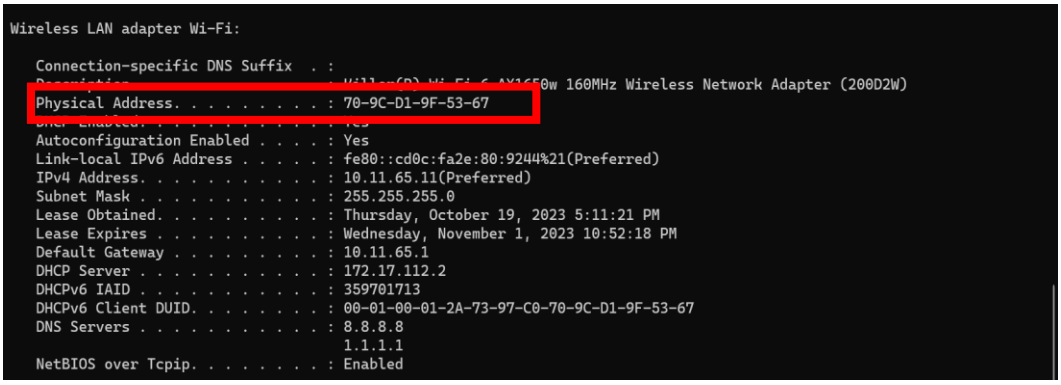

Figure 1. The ipconfig Command

Alternatively, the same information can be obtained by the following method. See Figure 2.

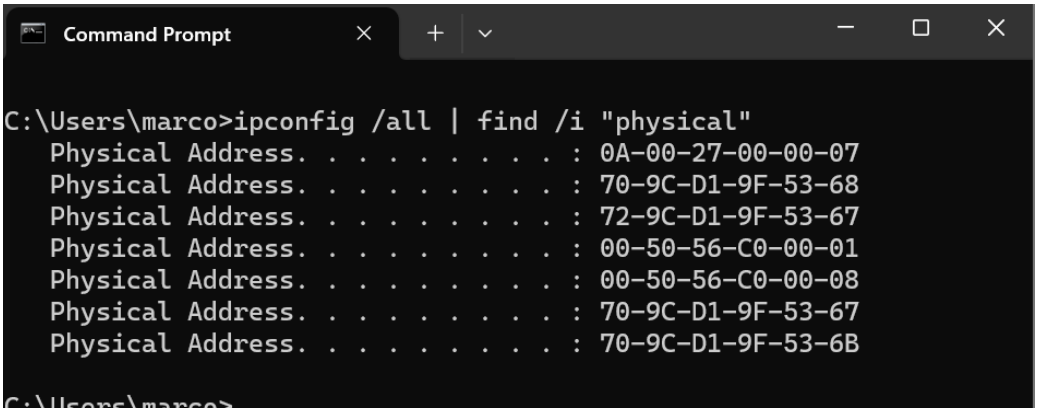

Figure 2. Alternate ipconfig Method

3.2 METHOD 2 (GETMAC)

Execute the following command. See Figure 3.

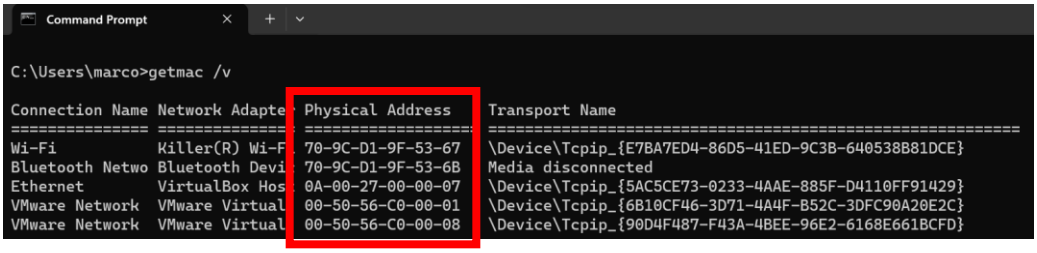

Figure 3. The getmac Command

3.3 ARP

ARP (Address Resolution Protocol) is used to query a MAC address from a given IP address. Queried MAC addresses are temporarily stored in a table in the RAM as **cached data**. This table is called an **ARP table**. To view the current contents of the ARP table, execute the **arp** command. See Figure 4.

```
C:\Users\marco>arp -a

Interface: 192.168.56.1 --- 0x7
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     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
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.29.1 --- 0xa
  Internet Address      Physical Address      Type
  192.168.29.254        00-50-56-e1-47-54     dynamic
  192.168.29.255        ff-ff-ff-ff-ff-ff     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
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figure 4. The arp Command

In this example, the device's MAC address at 192.168.29.254 (IPv4 address) is 00-50-56-e1-47-54. The type **dynamic** means that this entry was obtained via arp. You may sometimes see the type **static**. Static means that the entry was manually or automatically created by a system administrator or the operating system at boot time.

4 MAC Address Structure

Consider a MAC address E4-54-E8-A0-35-6B. See Table 1.

Table 1. MAC Address Structure

Part	OUI (Byte 1)	OUI (Byte 2)	OUI (Byte 3)	S/N (Byte 1)	S/N (Byte 2)	S/N (Byte 3)
MAC (Hex)	E4	54	E8	A0	35	6B
Decimal	228	84	232	160	53	107
Binary (Bits)	1110 0100	0101 0100	1110 1000	1010 0000	0011 0101	0110 1011
	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte	1 Byte
	1 Octet	1 Octet	1 Octet	1 Octet	1 Octet	1 Octet

Therefore, a MAC address consists of 48 bits, 6 bytes, or 6 octets. The first 24 bits (3 bytes or 3 octets) are called an OUI (organizationally unique identifier), which uniquely identifies the manufacturer of the network interface card (NIC). The second 24 bits (3 bytes or 3 octets) are used as the NIC serial number.

Note that a hexadecimal number can be converted into decimal, octal, and binary equivalent numbers using Windows Calculator in the Programmer mode. To switch to the Programmer mode, click the ≡ button and choose **Programmer**. See Figure 5.

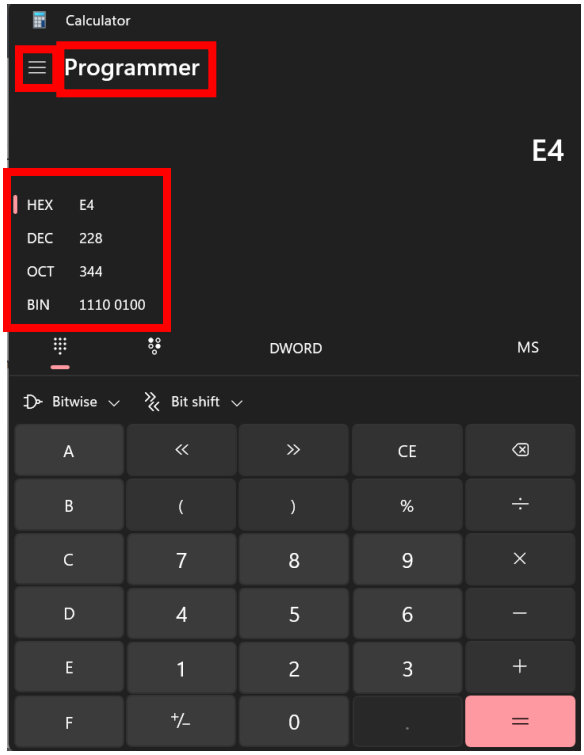

Figure 5. Windows Calculator in Programmer Mode

5 LINUX

This section reviews some Linux data link layer commands.

5.1 FRAME CHECK SEQUENCE

The data integrity of a frame is checked using a unique code in the frame trailer called a **frame check sequence** (FCS). This number is calculated using a mathematical formula called the **cyclic redundant check** (CRC). This formula calculates a unique number for the data. The following example shows how the CRC works.

Create a data file named **data.txt** that contains *Hello, World*. See Figure 6.

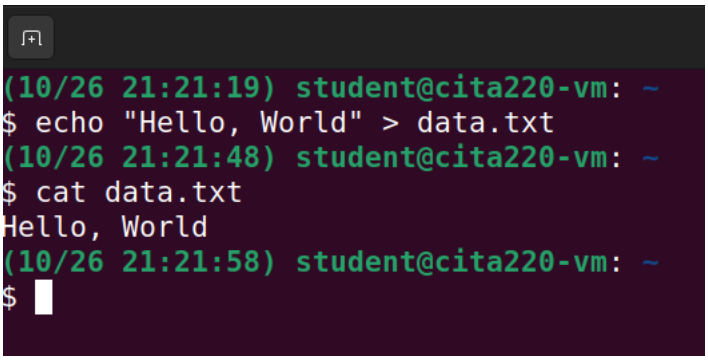

Figure 6. Creating a Data File

Run this data file through the CRC formula. Notice a hexadecimal number is returned. See Figure 7.

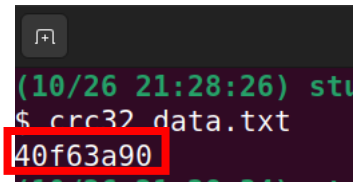

Figure 7. CRC Checksum

Next, change the contents of the data file. Notice the only difference is one letter, "w". A different number is displayed when this data file is run through the CRC formula, although the data difference is subtle. See Figure 8.

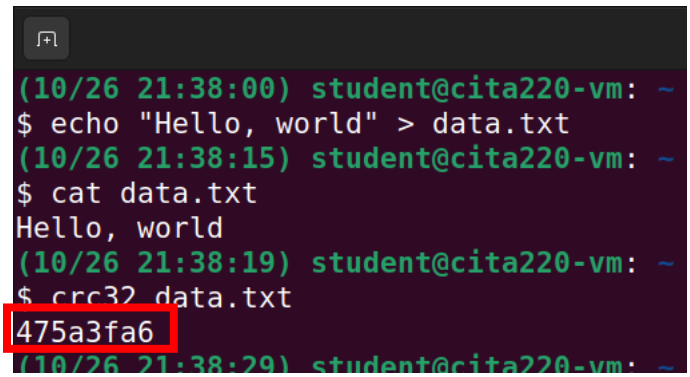

Figure 8. A Slight Different Data Changed the CRC Checksum

When the receiver receives a frame from the sender, it calculates the CRC checksum from the received data and compares it with the sender's calculated checksum (FCS) that came with the frame's data. If the checksums match, the receiver knows it has received the data intact.

5.2 MAC Address

There are two common methods to obtain IP addresses.

5.2.1 Method 1 (ifconfig)

The **ifconfig** command displays the MAC address as an **Ethernet** (ether) **address**. See Figure 9.

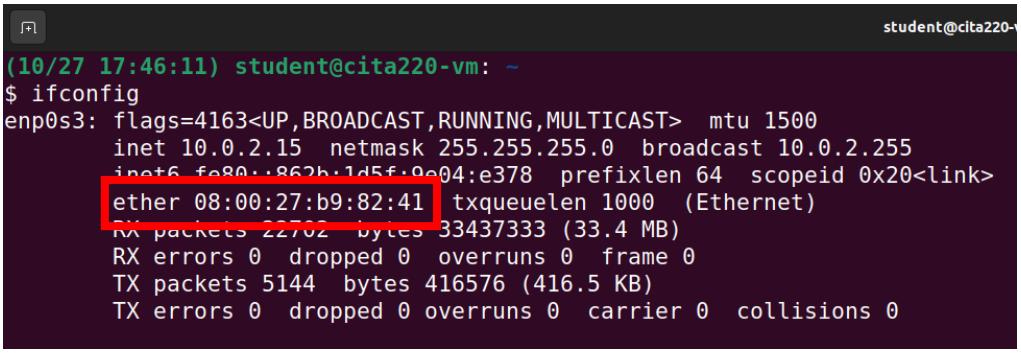

Figure 9. The ifconfig Command

5.2.2 Method 2 (ip)

The **ip** command used with the **link** subcommand displays the MAC address as a **link** (Ethernet address). See Figure 10.

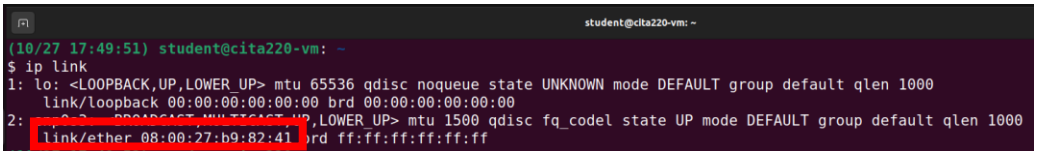

Figure 10. The ip link Command

5.3 ARP

There are two common methods to obtain the MAC address.

5.3.1 Method 1 (arp)

The arp command is typically used the **-n** option. See Figure 11.

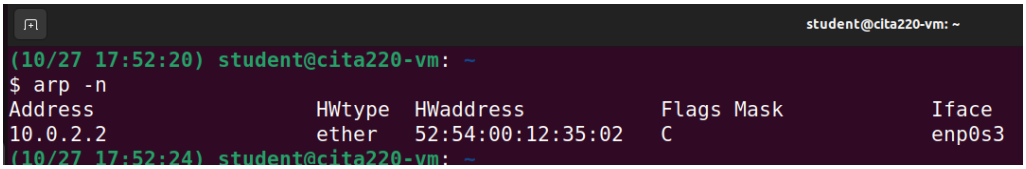

Figure 11. The arp Command

5.3.2 Method 2 (ip)

The **ip** command is used with a **neighbor** (n) subcommand. See Figure 12.

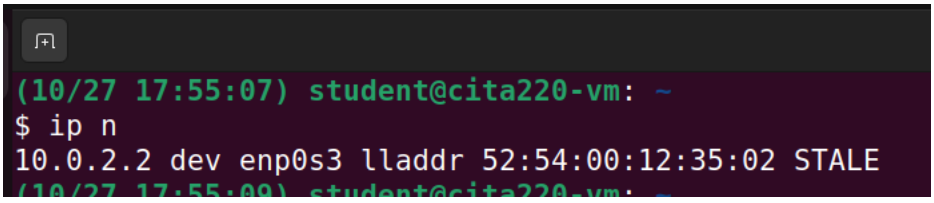

Figure 12. The ip neighbor Command

6 CAPTURING ARP BROADCASTS USING WIRESHARK

This section uses Wireshark to capture ARP broadcasts in the network. Wireshark is a well-known free, open-source software tool to capture frames that a network interface card (NIC) attached to the computer running Wireshark. It captures all frames regardless of where those frames are going. It then de-encapsulates those frames and displays the contents for analysis. Wireshark is classified as a **protocol analyzer** tool.

6.1 STARTING WIRESHARK

To start Wireshark, click the Wireshark icon. See Figure 13.

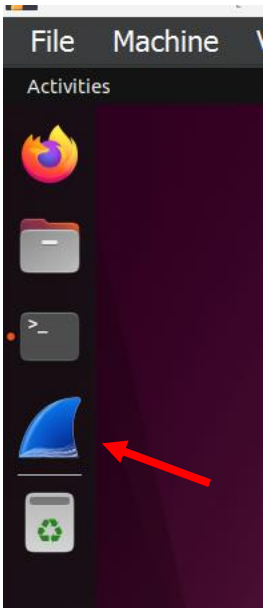

Figure 13. Starting Wireshark

6.2 CHANGING THE NETWORK SETTINGS

By default, the CITA220 resides in its private broadcast domain. Therefore, there are not many network frames to capture. More frames can be captured when placed on the same network the host operating system resides in. From the **Devices** menu, choose **Network > Network Settings…** . See Figure 14.

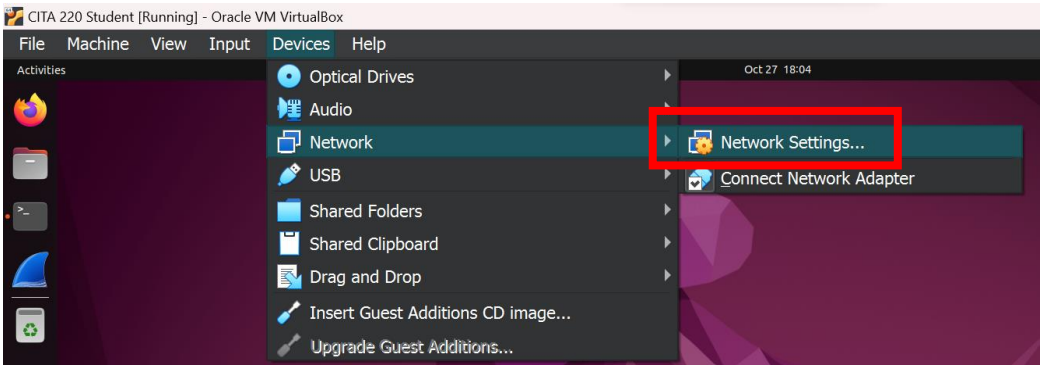

Figure 14. Changing the Network Settings

Change the **Attached** to from **NAT** to **Bridged Adapter** and click OK. Wait about 10 seconds. See Figure 15.

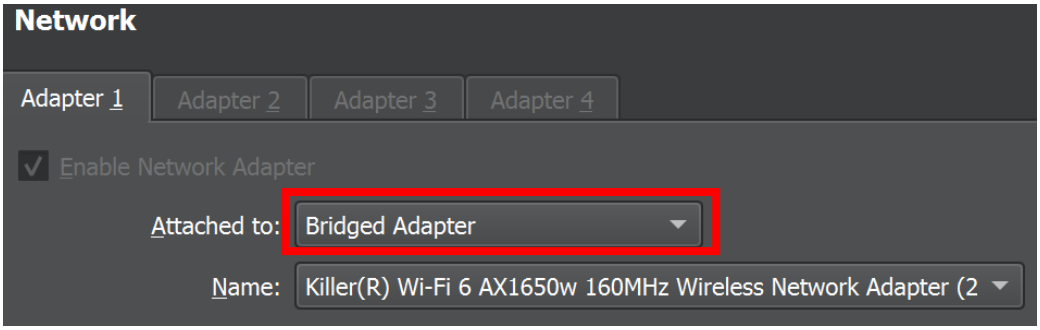

Figure 15. Changing to Bridged Adapter

6.3 Starting and Stopping to Capture Frames

Make sure the **enps03** interface is selected. Click the blue **Start capturing packets** button to start capturing frames. See Figure 16.

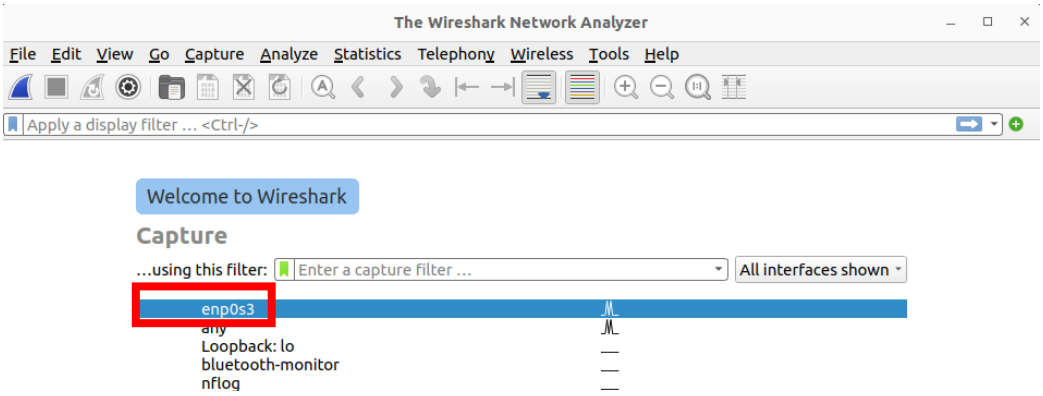

Figure 16. Starting to Capture Frames

The capturing starts immediately. Wait for 20 to 30 seconds. Then click the red **Stop capturing packets** button to stop capturing. See Figure 17.

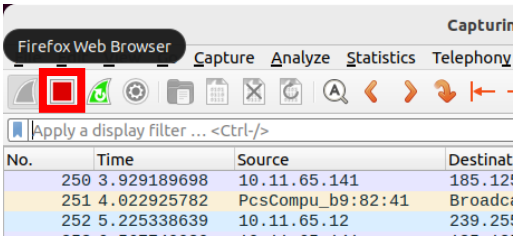

Figure 17. Stopping to Capture Frames

6.4 Examining ARP Frames

Note that a large number of frames are captured within a short period. Search for ARP frames is very difficult. Wireshark supports a powerful display filter command set that allows the user to search various captured frames' information. Type **arp** and press Enter in the display filter bar. As you type, the background color becomes red. It changes to green after the command syntax becomes correct. Only the ARP frames are displayed. Select one of them and expand the **Ethernet II** section.

Note that Wireshark automatically translated the OUIs of the MAC addresses to the manufacturers' names. The destination MAC address is **ff:ff:ff:ff:ff:ff**. It is a special MAC address for a broadcast. Wireshark automatically replaces the MAC address with the word **Broadcast**. Also, note the message under the **Info** column. The "*Who has (receiver IP address)? Tell (sender IP address).*" Is the ARP broadcast message. See Figure 18.

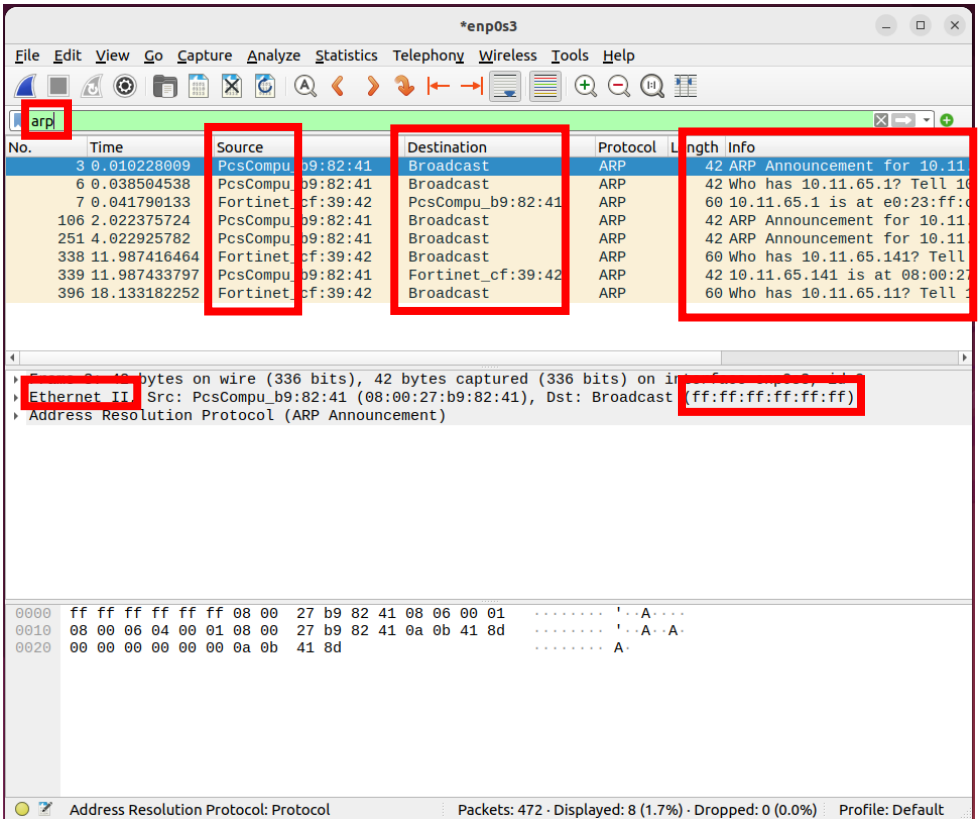

Figure 18. Captured ARP Frames