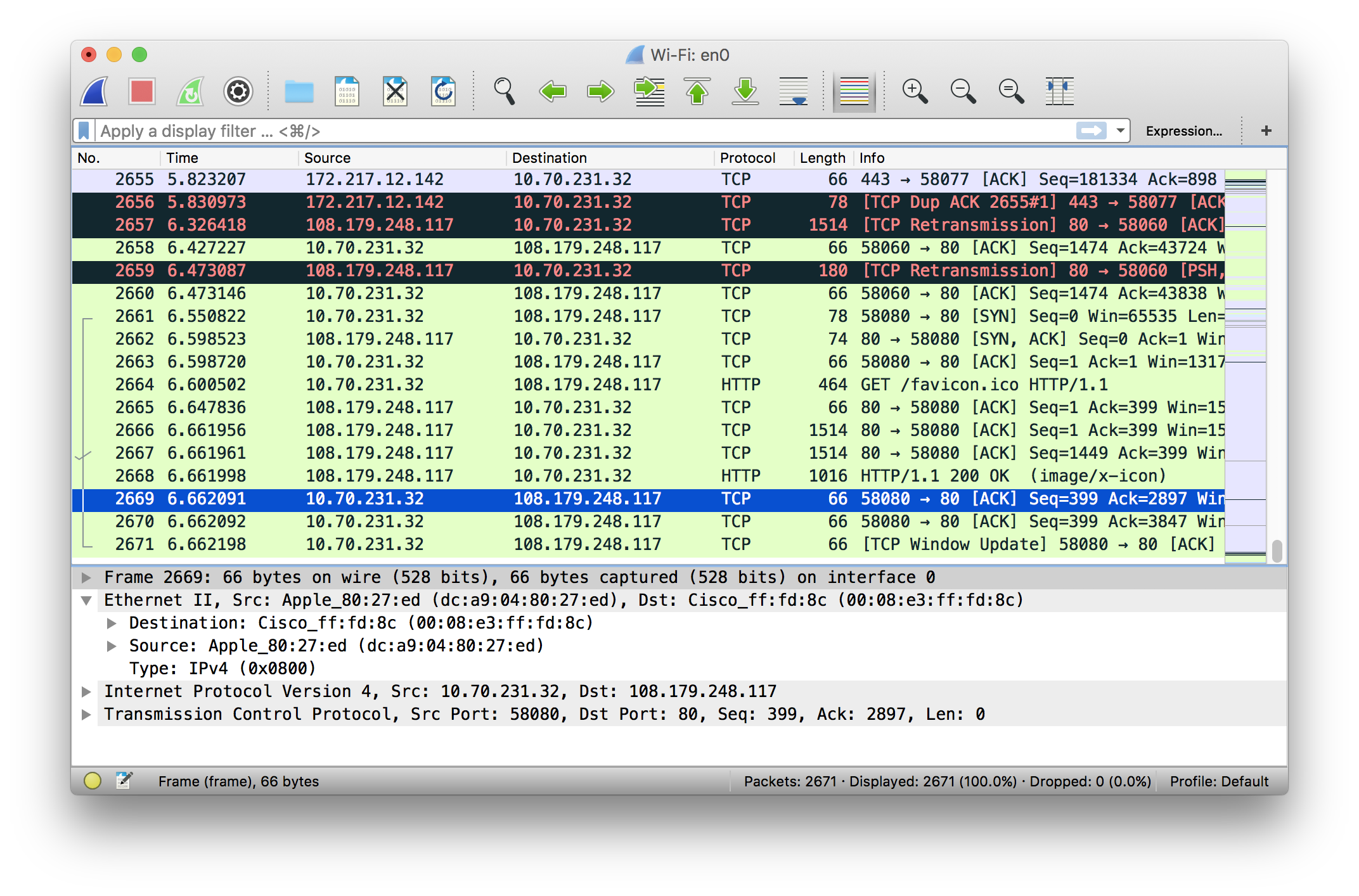
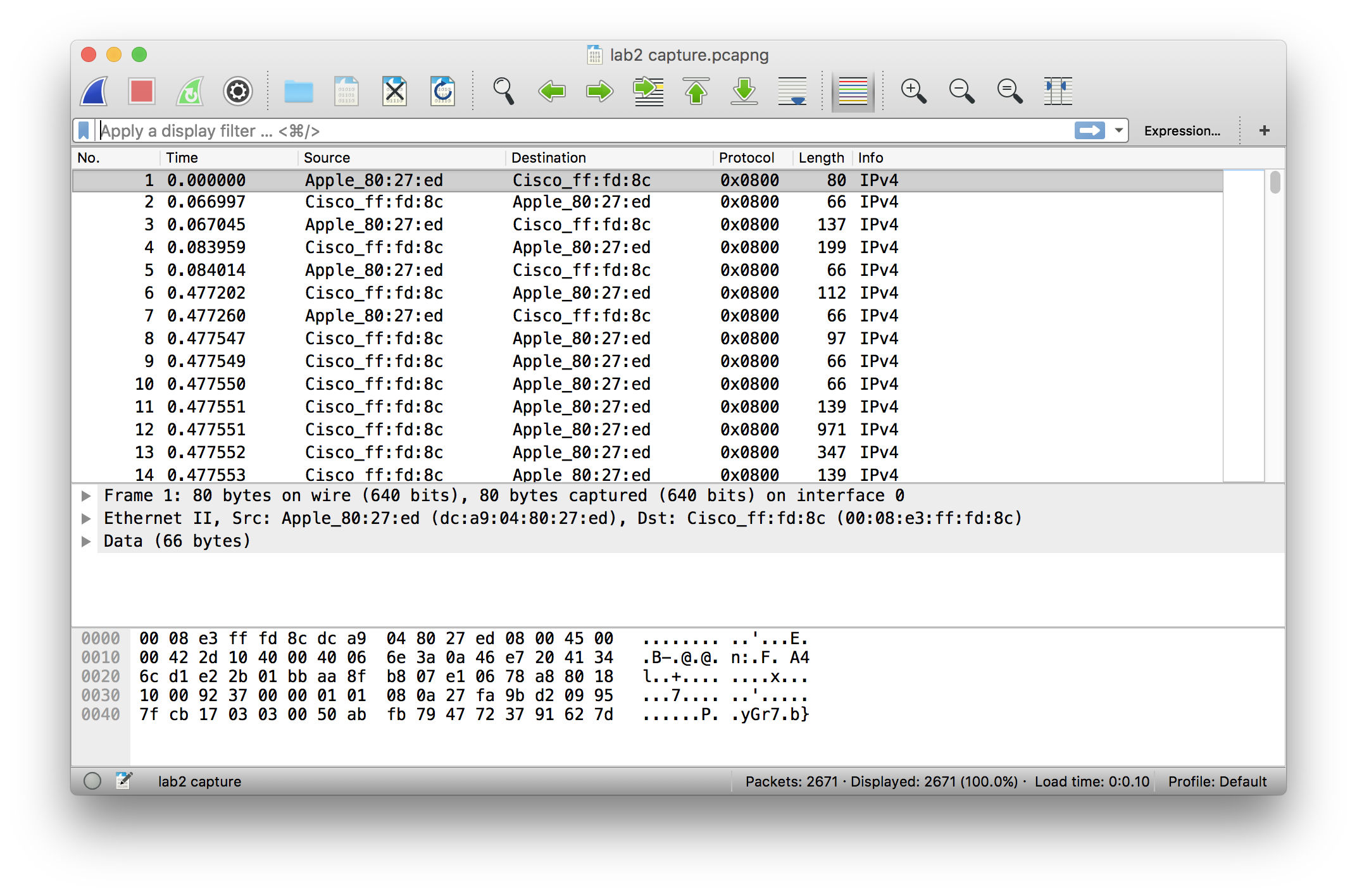
CSC 265 Lab Assignment 2

Due on 10/15/2017 11:59 pm

1. Capturing and analyzing Ethernet frames

Let’s begin by capturing a set of Ethernet frames to study. Do the following:

* First, make sure your browser’s cache is empty. To do this under Mozilla Firefox V3, select *Tools->Clear Recent History* and check the box for Cache. For Internet Explorer, select *Tools->Internet Options->Delete Files.* For Safari, *select History->clear history*.For Google Chrome, *Chrome-> Clear browsing data*. Start up the Wireshark packet sniffer
* Enter the following URL into your browser  
  <http://www.southernct.edu>
* Stop Wireshark packet capture. First, find the packet numbers (the leftmost column in the upper Wireshark window) of the HTTP GET message that was sent from your computer to www.southernct.edu, as well as the beginning of the HTTP response message sent to your computer by www.southernct.edu. You should see a screen that looks something like this (where packet 4 in the screen shot below contains the HTTP GET message)
* 
* Since this lab is about Ethernet and ARP, we’re not interested in IP or higher-layer protocols. So let’s change Wireshark’s “listing of captured packets” window so that it shows information only about protocols below IP. To have Wireshark do this, select *Analyze->Enabled Protocols.* Then uncheck the IP box and select *OK*. You should now see an Wireshark window that looks like:



In order to answer the following questions, you’ll need to look into the packet details and packet contents windows (the middle and lower display windows in Wireshark).

Select the Ethernet frame containing the HTTP GET message. Expand the Ethernet II information in the packet details window. Note that the contents of the Ethernet frame (header as well as payload) are displayed in the packet contents window.

Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message.

* What is the 48-bit Ethernet address of your computer?
  1. 14:94:6e:87:41:e2
* What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of www.southernct.edu? (Hint: the answer is *no*). What device has this as its Ethernet address?
  1. The 48-bit destination address is d0:a6:37:ec:8c:bd. No the Ethernet address of [www.southernct.edu](http://www.southernct.edu) is not. The device that the Ethernet address is connect thru the router that is connected.
* How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?
  1. 37.

Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

* What is the value of the Ethernet source address? Is this the address of your computer, or of www.southernct.edu (Hint: the answer is *no*). What device has this as its Ethernet address?
  1. The value of the Ethernet source
* What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?
* How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?

1. The Address Resolution Protocol

In this section, we’ll observe the ARP protocol in action.

**ARP Caching**

Recall that the ARP protocol typically maintains a cache of IP-to-Ethernet address translation pairs on your computer. The *arp* command (in both MSDOS and Linux/Unix) is used to view and manipulate the contents of this cache. Since the *arp* command and the ARP protocol have the same name, it’s understandably easy to confuse them. But keep in mind that they are different - the *arp* command is used to view and manipulate the ARP cache contents, while the ARP protocol defines the format and meaning of the messages sent and received, and defines the actions taken on message transmission and receipt.

Let’s take a look at the contents of the ARP cache on your computer:

* **MS-DOS.** The *arp* command is in c:\windows\system32, so type either “*arp*” or “*c:\windows\system32\arp*” in the MS-DOS command line (without quotation marks).
* **Linux/Unix/MacOS.** The executable for the *arp* command can be in various places. Popular locations are /sbin/arp (for linux) and /usr/etc/arp (for some Unix variants).

The Windows *arp* command with no arguments will display the contents of the ARP cache on your computer. Run the *arp* command.

1. Write down the contents of your computer’s ARP cache. What is the meaning of each column value?

|  |  |  |
| --- | --- | --- |
| Internet Address | Mac address | Type |
| 192.168.1.1 | 14:94:6e:87:41:e2 | ethernet |
| 192.168.1.7 | b8:78:2e:24:7e:2f | ethernet |
| 192.168.1.10 | 68:64:4b:1a:88:83 | ethernet |
| 192.168.1.12 | b8:a1:75:cb:c5:7b | ethernet |
| 192.168.1.15 | cc:95:d7:ec:2a:1e | ethernet |
| 192.168.1.255 | ff:ff:ff:ff:ff:ff | ethernet |
| 224.0.0.251 | 1:0:5e:0:0:fb | ethernet |
| 239.255.255.250 | 1:0:5e:7f:ff:fa | ethernet |
| 255.255.255.255 | ff:ff:ff:ff:ff:f | ethernet |

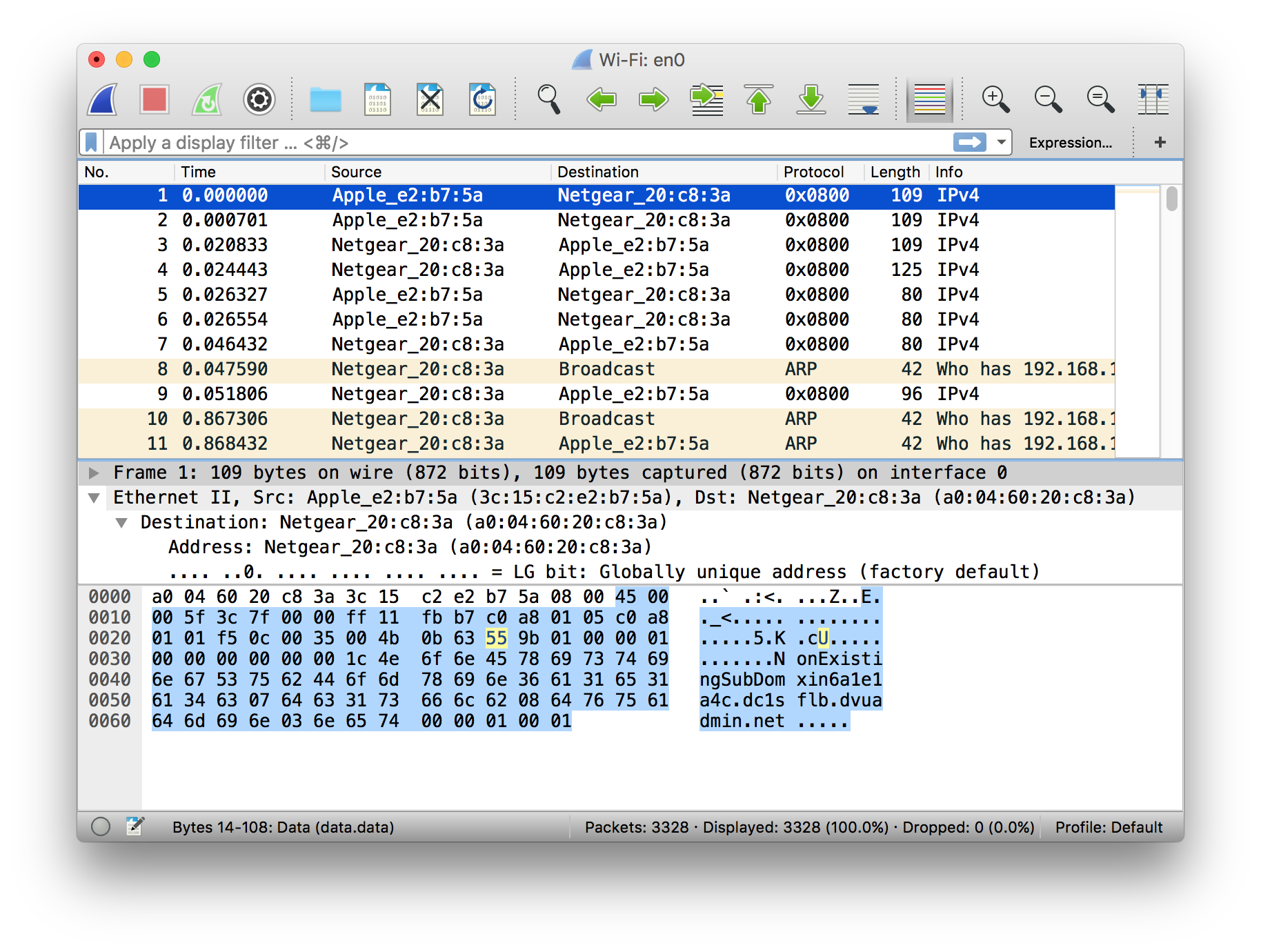
In order to observe your computer sending and receiving ARP messages, we’ll need to clear the ARP cache, since otherwise your computer is likely to find a needed IP-Ethernet address translation pair in its cache and consequently not need to send out an ARP message.

* **MS-DOS.** The MS-DOS *arp –d \** command will clear your ARP cache. The *–d* flag indicates a deletion operation, and the \* is the wildcard that says to delete all table entries.
* **Linux/Unix/MacOS.** The *arp –d \* (arp –d –a for mac os)* will clear your ARP cache. In order to run this command you’ll need root privileges. If you don’t have root privileges and can’t run Wireshark on a Windows machine.

**Observing ARP in action**

Do the following:

1. Clear your ARP cache, as described above.
2. Next, make sure your browser’s cache is empty. To do this under Mozilla Firefox V3, select *Tools->Clear Recent History* and check the box for Cache. For Internet Explorer, select *Tools->Internet Options->Delete Files.*
3. Start up the Wireshark packet sniffer
4. Enter the following URL into your browser  
   http://www.southernct.edu
5. Stop Wireshark packet capture. Again, we’re not interested in IP or higher-layer protocols, so change Wireshark’s “listing of captured packets” window so that it shows information only about protocols below IP. To have Wireshark do this, select *Analyze->Enabled Protocols.* Then uncheck the IP box and select *OK*. You should now see an Wireshark window that looks like:



In the example above, the 9th, 10th and 11th frames in the trace contain ARP messages.

Answer the following questions:

1. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
2. Download the ARP specification from

<ftp://ftp.rfc-editor.org/in-notes/std/std37.txt>. A readable, detailed discussion of ARP is also at <http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html>.

* 1. How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?
  2. What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?
  3. Does the ARP message contain the IP address of the sender?
  4. Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

1. Now find the ARP reply that was sent in response to the ARP request.
   1. How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?
   2. What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?
   3. Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?
2. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?