California State University,
Monterey Bay

# Week 8 – Lab 8
# Group 10

*Clarence Mitchell*

*CST311*

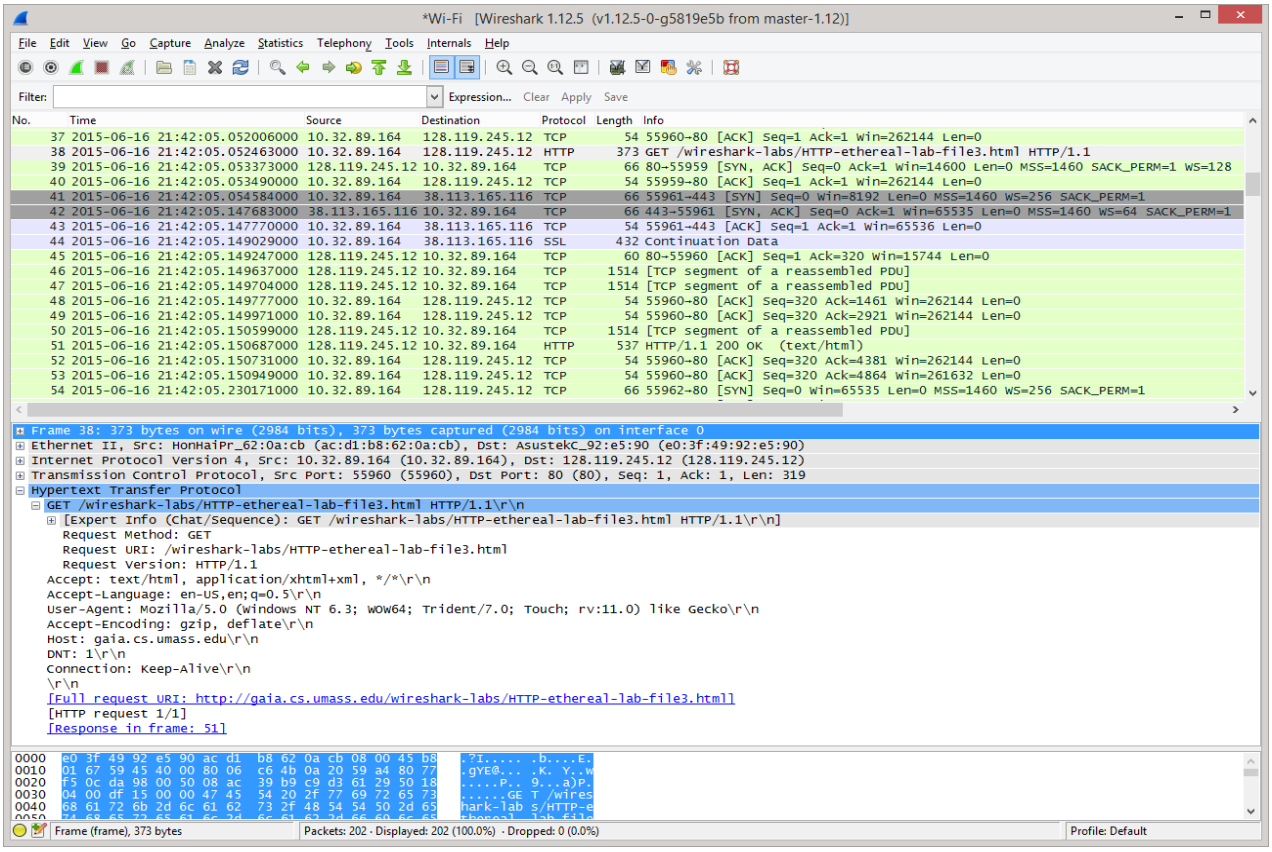
*Introduction to Computer Networks*

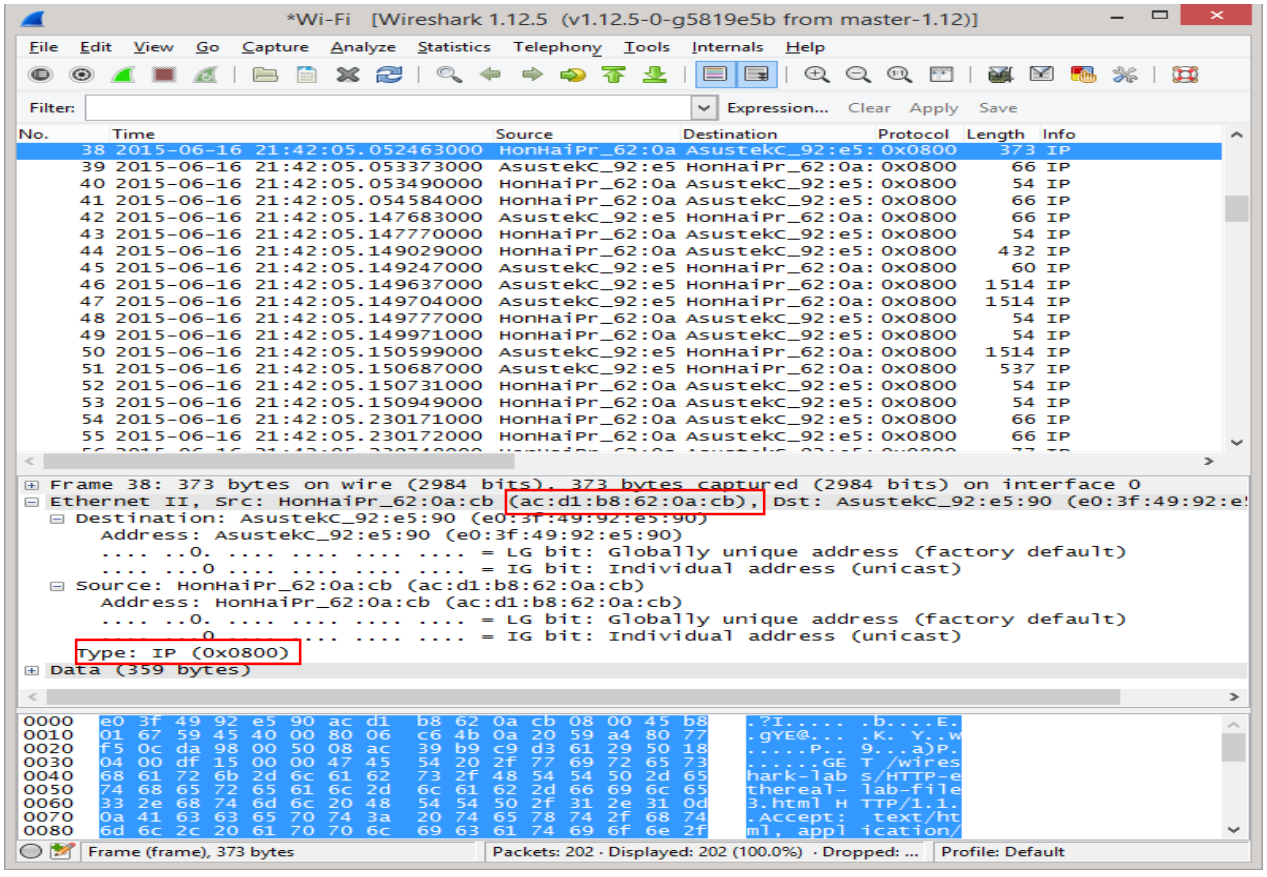
*SUMMER 2015*

*Instructor: Dr. Anand Seetharam*

## Questions and Answers

The following are the list of questions and related answers for this lab.



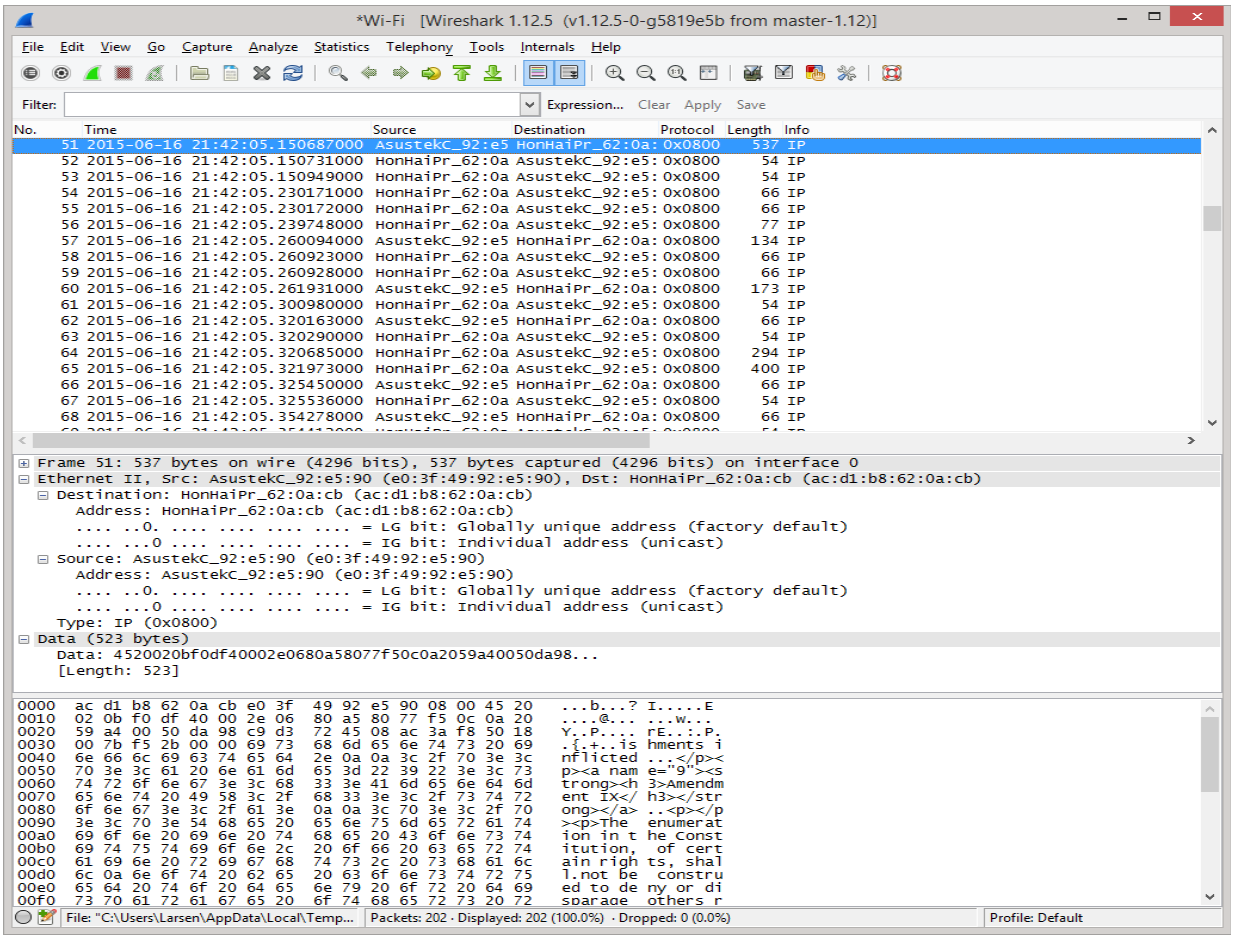
# 1. Capturing and analyzing Ethernet frames

1. What is the 48-bit Ethernet address of your computer?
   - I got the IP address ac:d1:b8:62:0a:cb

2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is *no*). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]
   - The destination address e0:3f:49:92:e5:90 is not the Ethernet address of gaia.cs.umass.edu. It is the address of my Asus router, which is the link used to get off the subnet.

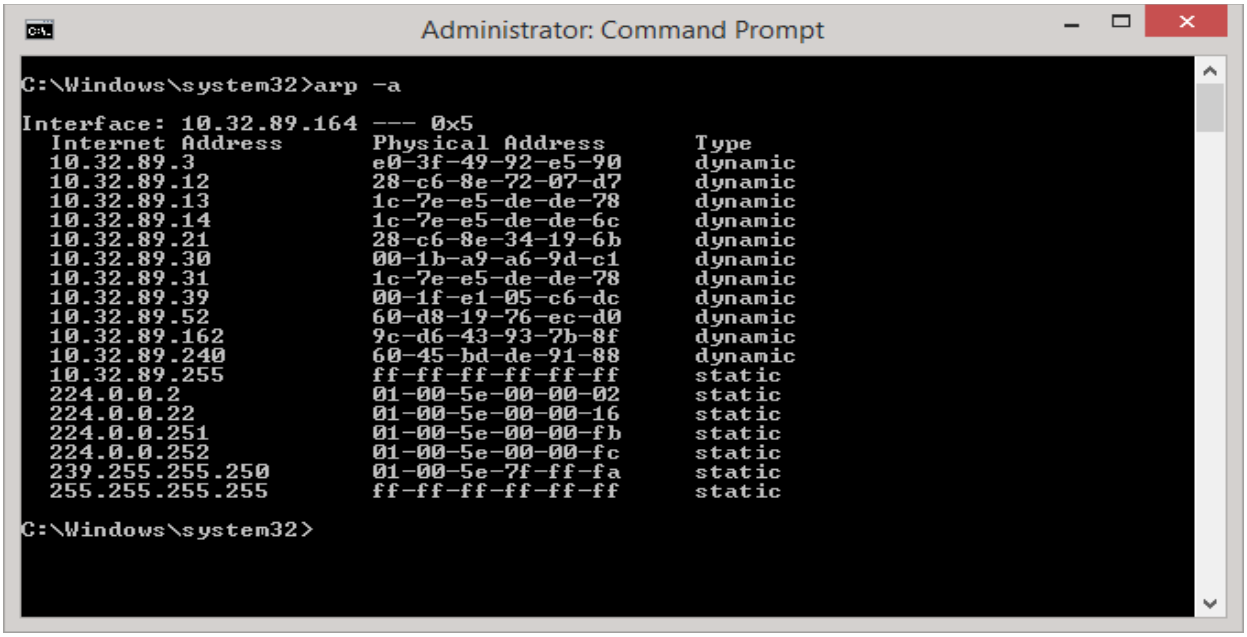
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
   - The hexidecimal value is 0x0800. This corresponds to the IP protocol.

4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?
   - It appears that the G in the GET appears 52 bits into the frame.

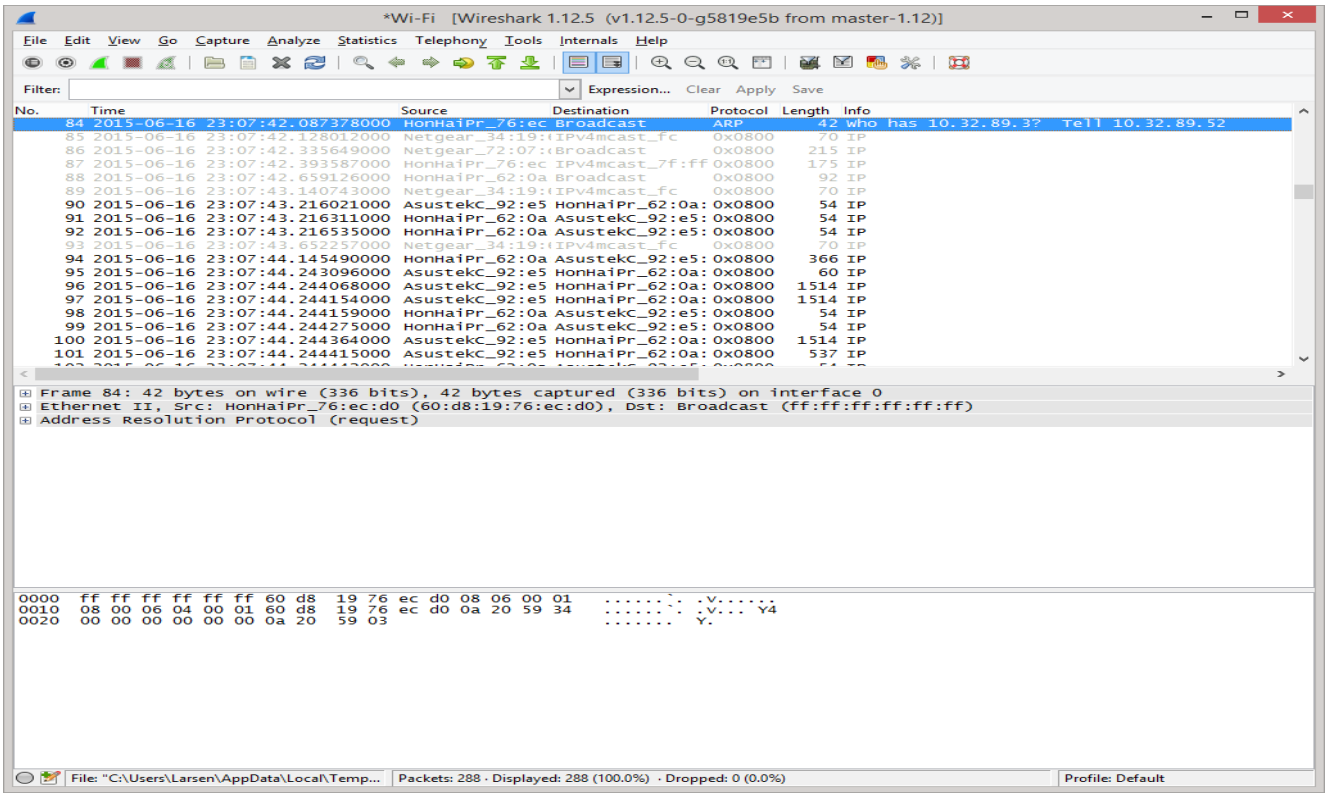


5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?
    - The source address e0:3f:49:92:e5:90 is neither the Ethernet address of gaia.cs.umass.edu nor the address of my computer. It is the address of my Asus router.
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?
    - The destination address ac:d1:b8:62:0a:cb is the address of computer.
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
    - The hex value for the Frame type field is 0x0800, which is IP.
8. 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?
    - The ASCII "O" appears to be 52 bytes from the start of the Ethernet frame..

## 2. The Address Resolution Protocol




9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?
    - This command is windows 8.1 requires the "-a" option.
    - The first column is the internet address of the computer then its physical address and finally what type it is and it is dynamic.




10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
    - The source address is (60:d8:19:76:ec:d0)
    - The Destination address is (ff:ff:ff:ff:ff:ff)

11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?
    - The hex value for the two byte Ethernet frame is ARP (0x0806), the corresponding upper layer protocol is ARP.

12. 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
    a) How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?
    - The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

    b) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?
    - The hex value for opcode field within the ARP-payload of the request is 0x0001, for request.

    c) Does the ARP message contain the IP address of the sender? Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?
    - Yes, the ARP message containg the IP address 10.32.89.164 for the sender. The field "Target MAC address" is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (10.32.89.3) is being queried.

13. Now find the ARP reply that was sent in response to the ARP request.
    a) How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

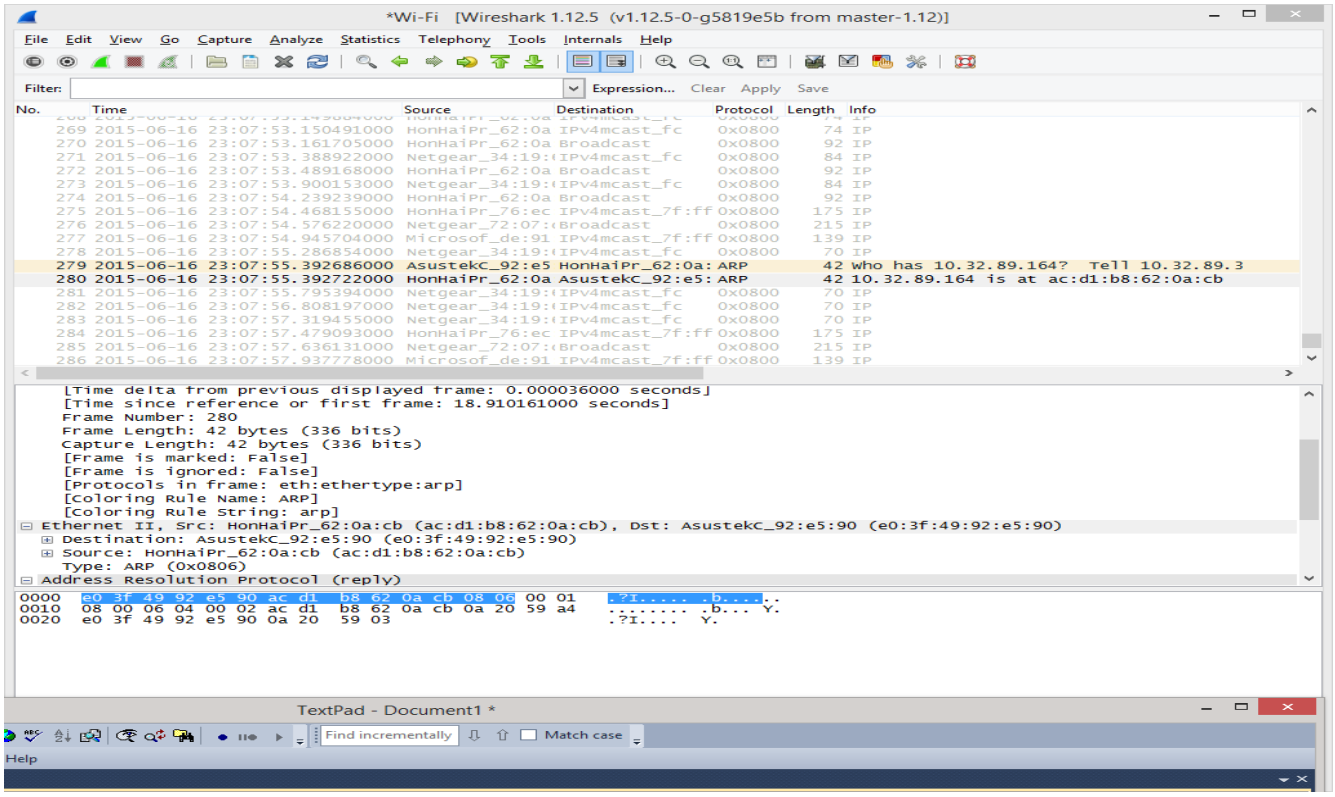
    - The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

    b) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

    - T The hex value for opcode field within the ARP-payload of the request is 0x0001, for request.

    c) 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?

    - ARP request appears in the"Sender MAC address" field, which contains the Ethernet address ac:d1:b8:62:0a:cb for the sender with IP address 10.32.89.3.




14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

    - The hex value for the source address is ac:d1:b8:62:0a:cb and for the destination is e0:3f:49:92:e5:90

15. Open the *ethernet-ethereal-trace-1* trace file in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?
    - There is no reply in this trace, that we can see because we are not the machine that sent the original request. We can see the reply to "our" ARP request because it is sent directly to us.