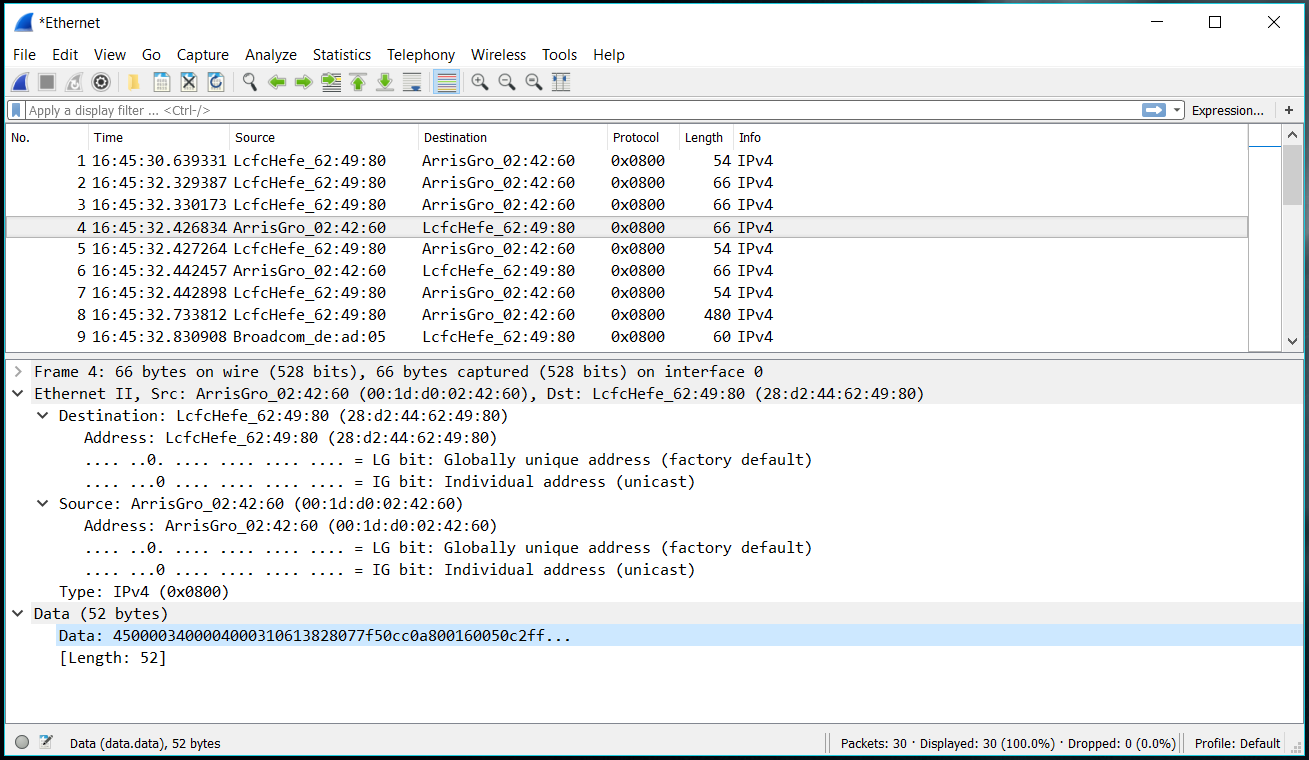
Broc Nickodemus

Lab5

1. What is the 48-bit Ethernet address of your computer?



The Ethernet address of my computer is 00:1d:d0:02:42:60

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 28:d2:44:62:49:80 is not the Ethernet address of gaia.cs.umass.edu. It is the address of LcfcHefe which is used to get the subnet.

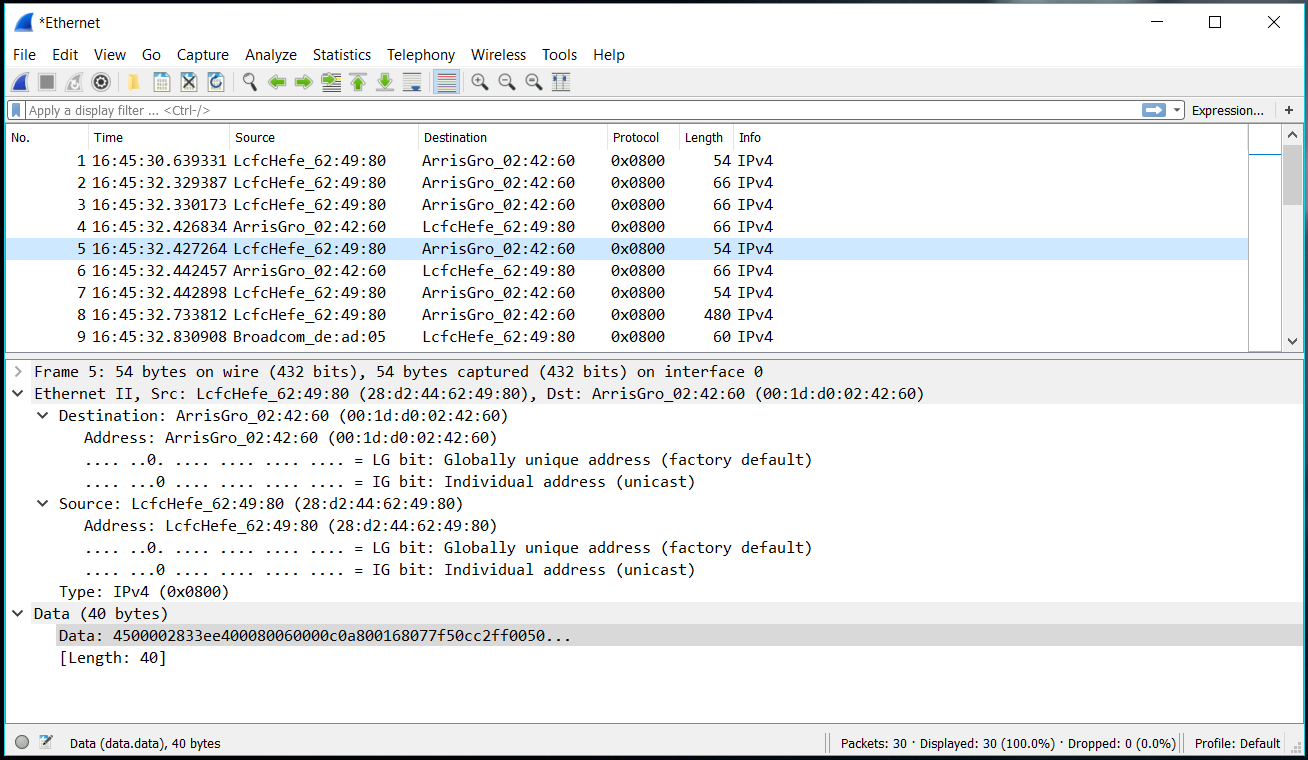
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

The type field is 0x0800

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 52 bytes from the start

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 28:d2:44:62:49:80 is not the Ethernet address ofgaia.cs.umass.edu or my computer. It is the address of LcfcHefe that gets the subnet.

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

The destination address 00:1d:d0:02:42:60 is the address of my computer.

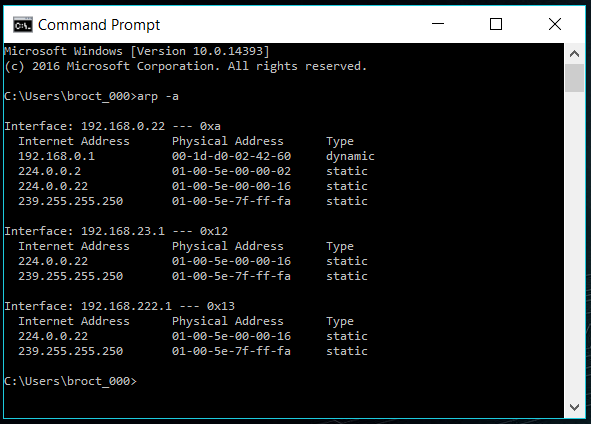
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

The hex value is 0x0800.

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?

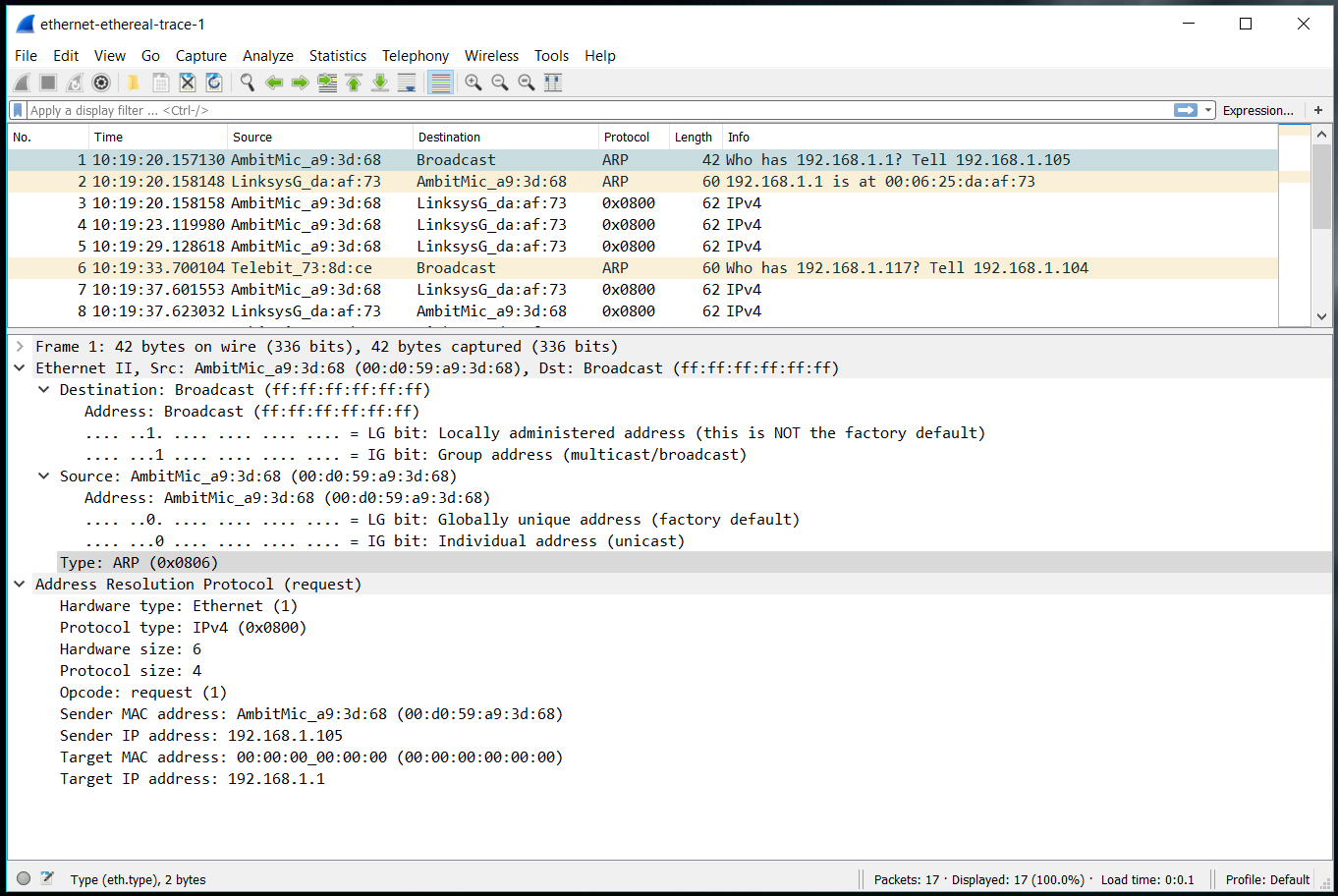
It appears 52 bytes from the start.

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



The interface contains the ip, the physical address contains the mac address, and the type indicates the protocol.

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



I couldn’t find the arp message so I used the wireshark example trace.

The hex value of the source address is00:80:ad:73:8d:ce. The hex value of the destination 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 is 0x0806, ARP is the upper layer it corresponds to.

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.

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?

ARP request has the value of 1

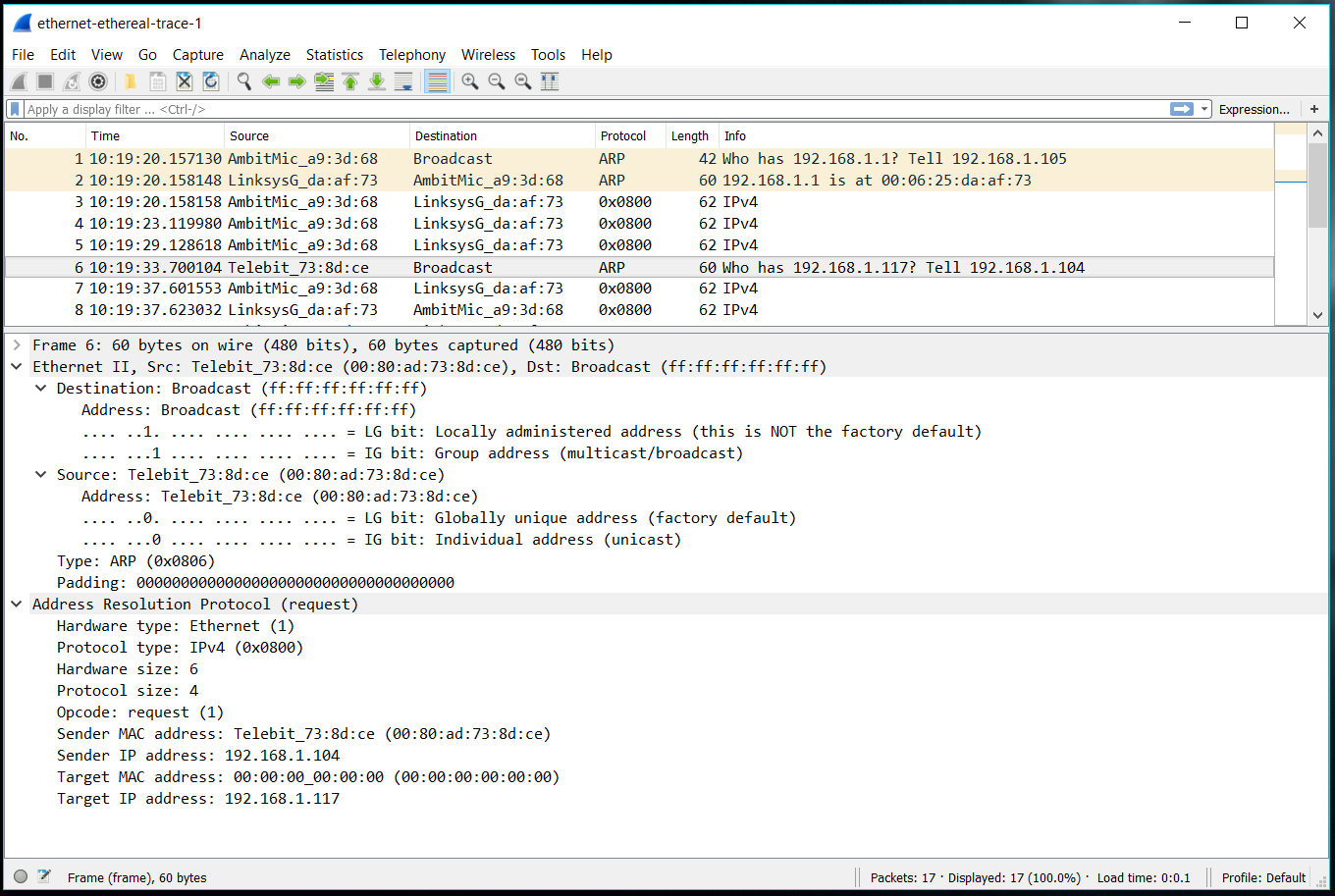
c) Does the ARP message contain the IP address of the sender?

Yes, the ARP message does.

d) Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

Target MAC address is set to 00:00:00:00:00:00 to question the machine.

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 op code begins 20 bytes from the beginning.

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?

It should have had 2 for reply but it failed so it returned 1 for another 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?

It appears in the Sender MAC address which contains 00:80:ad:73:8d:ce for the sender with an ip of 192.168.1.104.

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

The source address is 00:80:ad:73:8d:ce and the destination is 00:00:00:00:00:00

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 because our machine is not the machine that sent the request. The ARP reply is sent back to the sender’s Ethernet address.

**~~Extra Credit~~**

EX-1. The *arp* command:

*arp -s InetAddr EtherAddr*

allows you to manually add an entry to the ARP cache that resolves the IP address *InetAddr* to the physical address *EtherAddr*. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

EX-2. What is the default amount of time that an entry remains in your ARP cache before being removed. You can determine this empirically (by monitoring the cache contents) or by looking this up in your operation system documentation. Indicate how/where you determined this value.