Daniel McDonough (dmcdonough)
10/5/2018
Lab 3

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

My Ethernet address is Address: (00:d0:59:a9:3d:68)

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? (2 points)

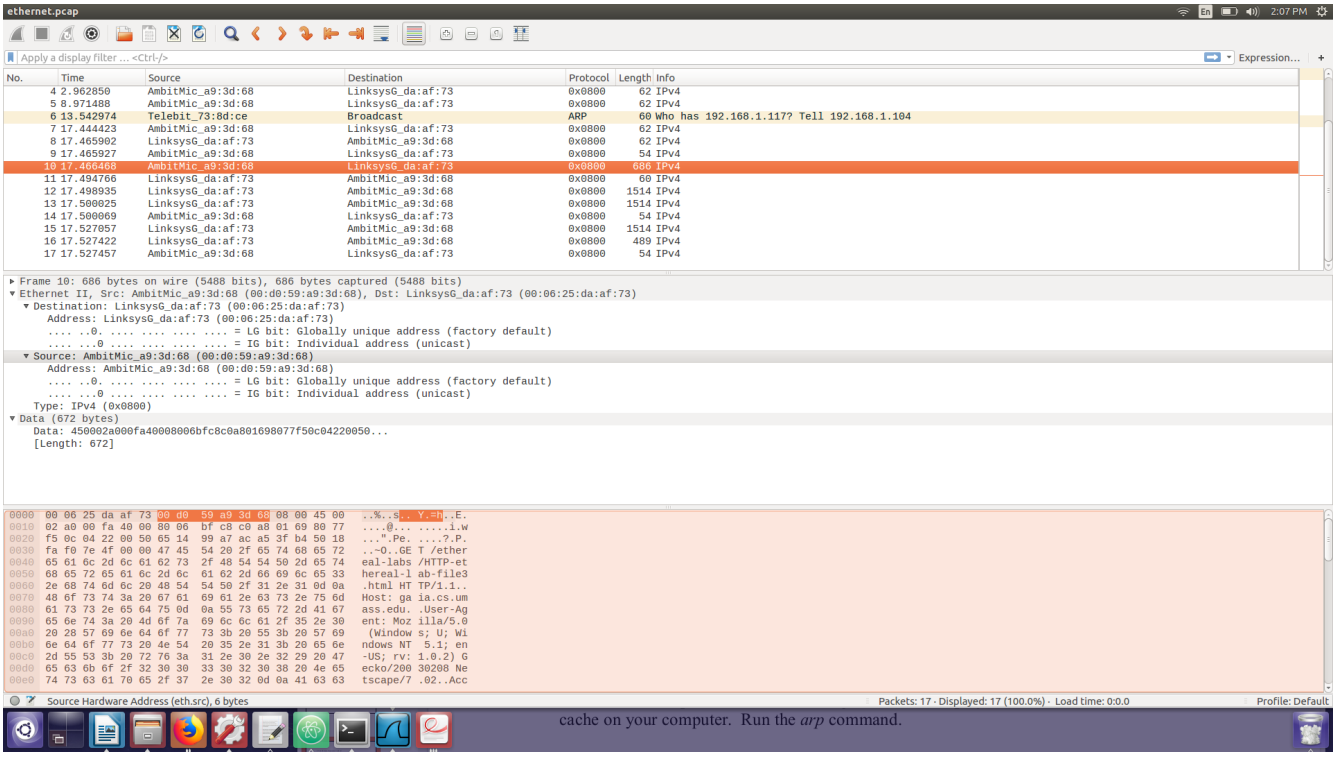
The destination address is 00:06:25:da:af:73. This is not the Ethernet address of gia.cs.umass.edu but rather the Ethernet address of the router we used to send the info.

3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to? (2 points)

0x0800 which is the IPv4 protocol

4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame? (1 point)

52 bytes before the G. 14 bytes for Ethernet header, 20bytes for each IP and TCP.



cache on your computer. Run the *arp* command.

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? (2 points)

The source is: 00:06:25:da:af:73 which is again the Ethernet address of the router used.

6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer? (2 points)

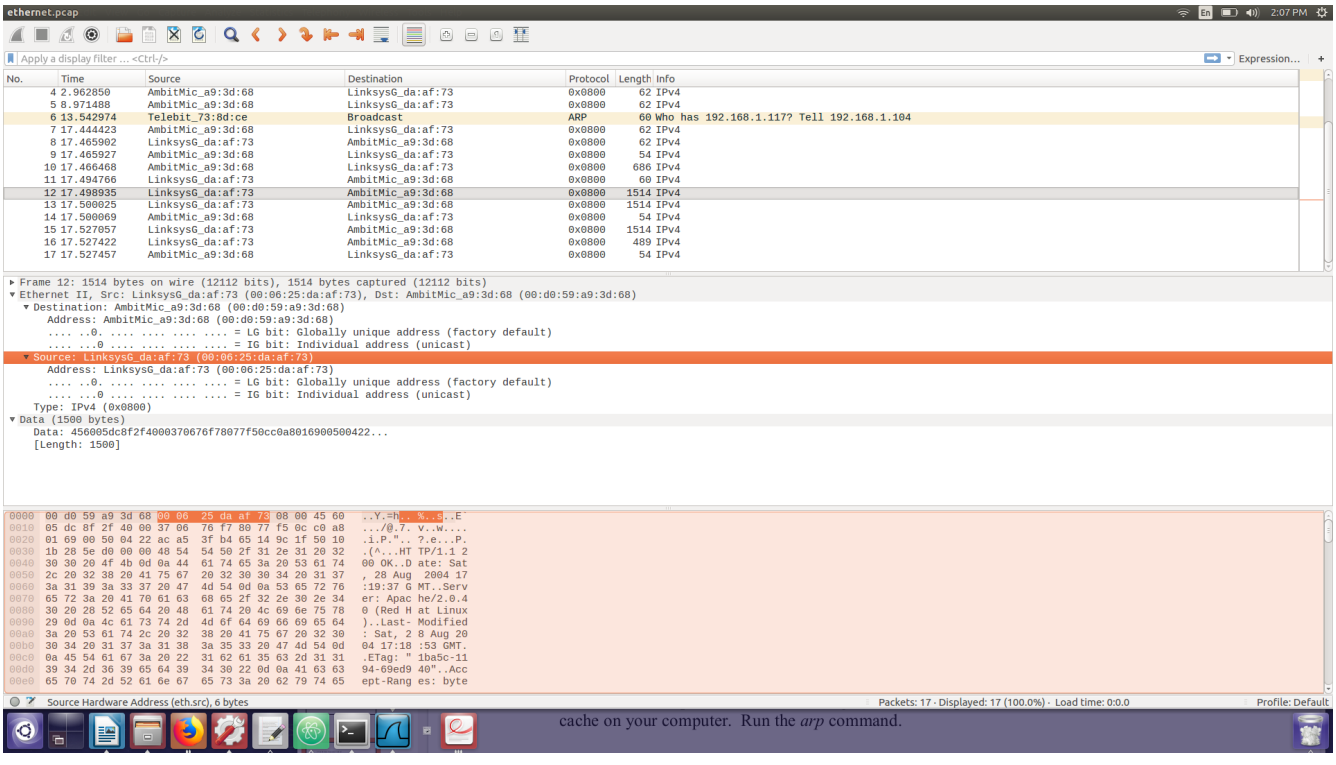
00:d0:59:a9:3d:68 is the destination and my Ethernet Address.

7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to? (2 points)

0x0800 which is the IPv4 protocol

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? (1 point)

54 bytes until the “O” .14 bytes for Ethernet header, 20bytes for each IP and TCP.



cache on your computer. Run the *arp* command.

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

Running "arp -a" on linux:

autoreg-704614.wifi.wpi.edu (130.215.120.243) at a4:5e:60:ca:7d:4b [ether] on wlp1s0
autoreg-166218.dyn.wpi.edu (130.215.123.157) at ac:bc:32:87:8a:99 [ether] on wlp1s0
autoreg-119838.dyn.wpi.edu (130.215.123.109) at 18:65:90:d3:b9:a5 [ether] on wlp1s0
? (130.215.122.175) at <incomplete> on wlp1s0
autoreg-174531.dyn.wpi.edu (130.215.123.240) at 2c:f0:ee:06:c6:e8 [ether] on wlp1s0
rtr-core-wireless120.inf.wpi.edu (130.215.120.1) at 00:00:5e:00:01:02 [ether] on wlp1s0
? (130.215.121.86) at ac:bc:32:bd:6c:91 [ether] on wlp1s0
autoreg-166699.dyn.wpi.edu (130.215.124.104) at c4:b3:01:99:69:7c [ether] on wlp1s0
autoreg-119337.dyn.wpi.edu (130.215.123.73) at 78:4f:43:81:87:40 [ether] on wlp1s0
autoreg-069184.dyn.wpi.edu (130.215.124.185) at c8:69:cd:91:7c:ec [ether] on wlp1s0
autoreg-170826.dyn.wpi.edu (130.215.122.123) at 8c:85:90:6c:6c:91 [ether] on wlp1s0
autoreg-121018.dyn.wpi.edu (130.215.126.96) at 8c:85:90:25:c8:fa [ether] on wlp1s0

This shows the IP address, the MAC address, and the Iface.

10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message? (1 point)

Source: (00:d0:59:a9:3d:68), Dst: (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? (2 points)

The Type value is 0x00000806 which 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? (1 point)

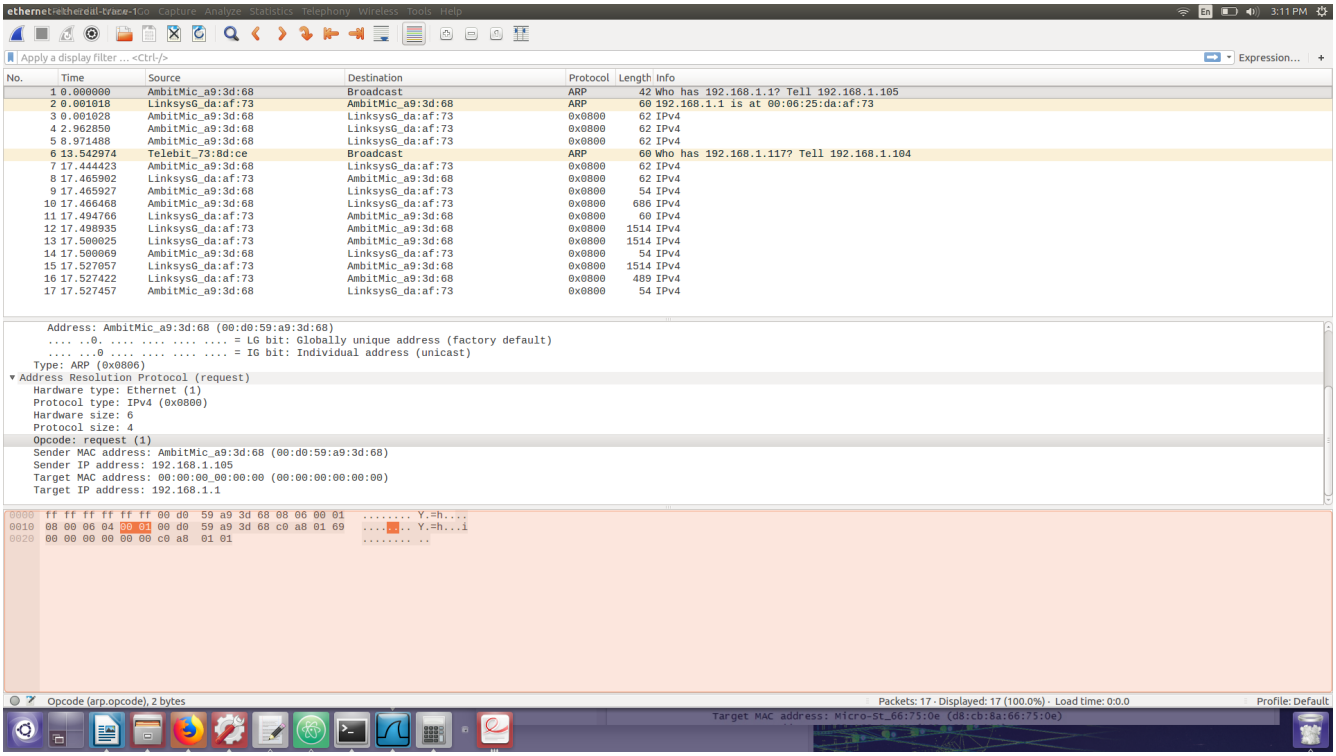
18 bytes prior to the opt code

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? (1 point)

0x0001 in the request 0x0002 in the response.

c) Does the ARP message contain the IP address of the sender? (1 point)

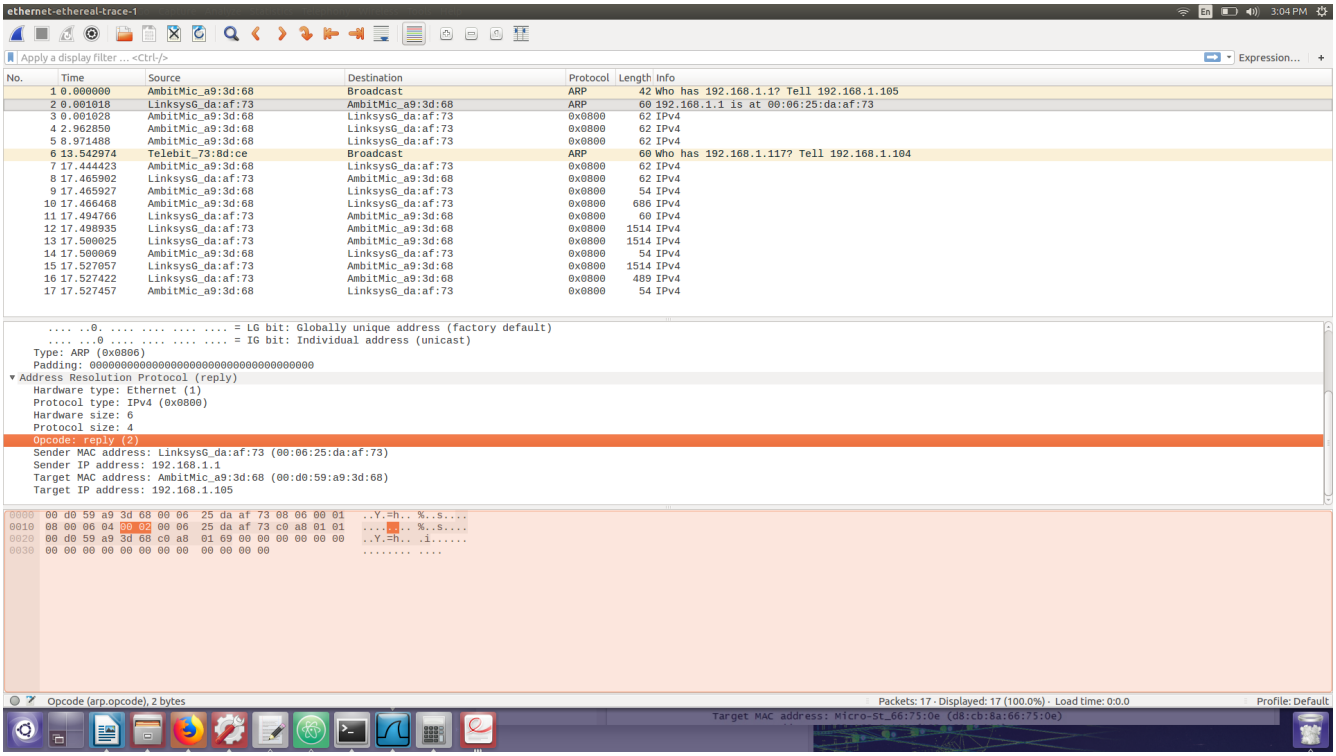
Yes, 192.168.1.105



d) Where in the ARP request does the “question” appear – the Ethernet (1 point) address of the machine whose corresponding IP address is being queried?

The question is in the target IP address as it is 192.168.1.1

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? (1 point)

18 bytes

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? (1 point)

0x0002

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? (1 point)

Sender IP Address: 192.168.1.1

14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message? (1 point)

Src: (00:06:25:da:af:73)
Dst: A(00:d0:59:a9:3d:68)

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?

The reply was sent from the router to that computer. The user's computer would not obtain the reply message from the router that was sent to a different IP. The only reason we see the request is because it is sent through the whole network in order to gain access to it.