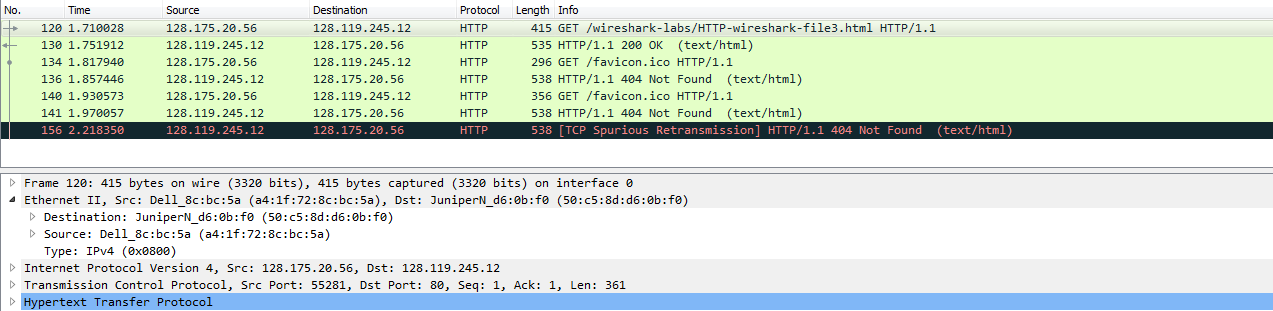
***What to hand in***

Answer the following questions, based on the contents of the Ethernet frame containing the HTTP **GET** message. Whenever possible, when answering a question you should hand in the saved packet(s) within the trace that you used to answer the question asked.



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

Source: a4:1f:72:8c:bc:5a

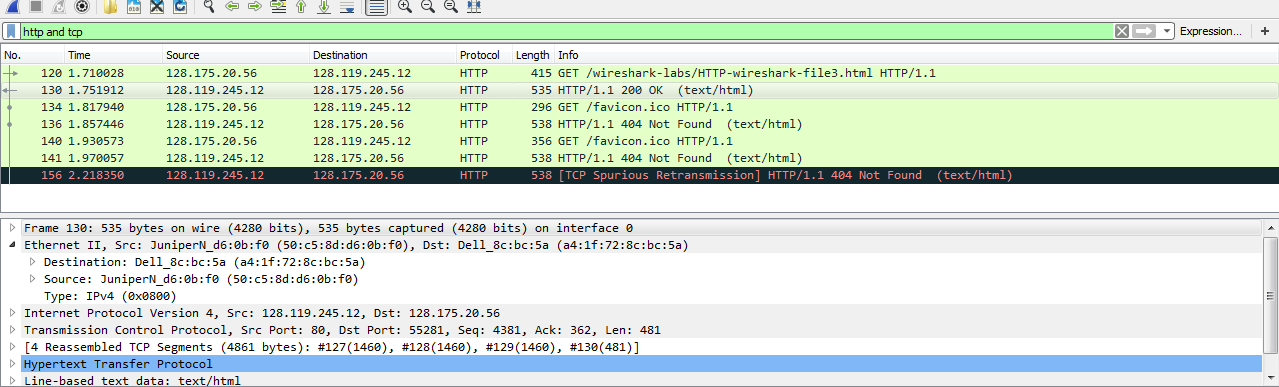
1. What is the 48-bit destination (MAC) address in the Ethernet frame? Is this the Ethernet (MAC) address of gaia.cs.umass.edu? What device has this as its Ethernet (MAC) address?

50:c5:8d:d6:0b:f0

No.

The router A which is the router of this network has this as its MAC address.

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



1. What is the value of the Ethernet (MAC) source address? Is this the address of your computer, or of gaia.cs.umass.edu? What device has this as its Ethernet (MAC) address?

50:c5:8d:d6:0b:f0

Neither. The router A which is the router of this network has this as its MAC address.

1. What is the destination (MAC) address in the Ethernet frame? Is this the Ethernet (MAC) address of your computer?

a4:1f:72:8c:bc:5a

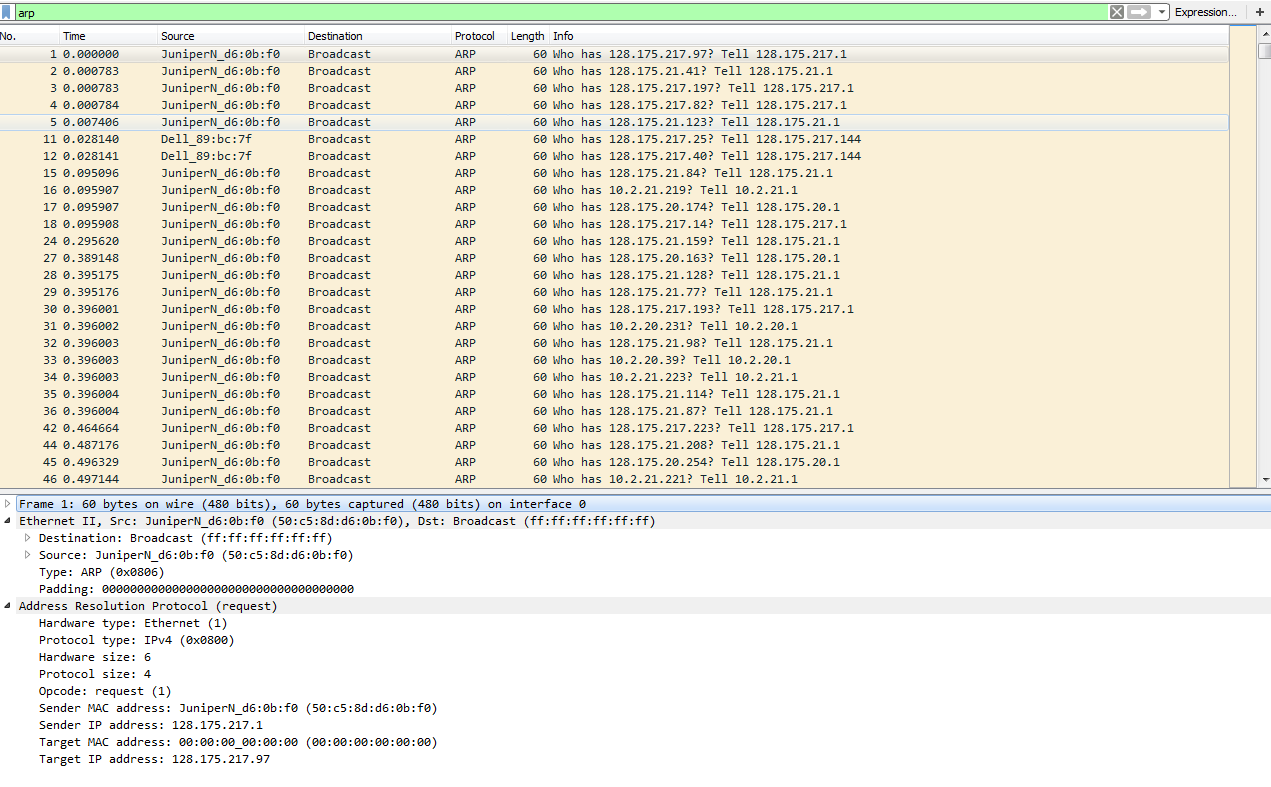
Yes

***What to hand in***

For this part of the lab, you should hand in a screenshot of the Command Prompt window. Whenever possible, when answering a question below, you should hand in the saved packet(s) within the trace that you used to answer the question asked.

Answer the following questions:

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

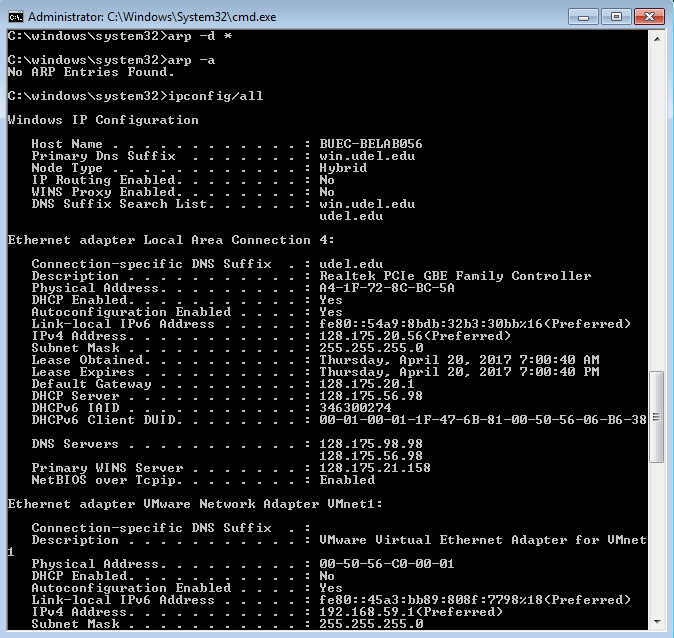


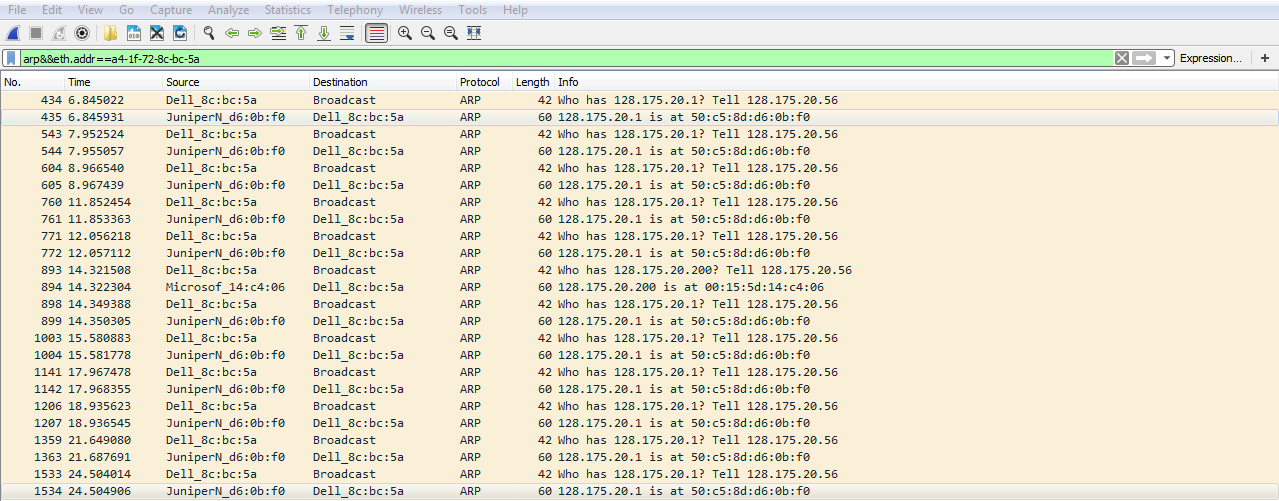
1. How many ARP messages do you capture? How do you determine which ARP messages are sent from and to your computer (**Hint**: You can use the command “**ipconfig /all**” to find your computer’s MAC address and then use “**ARP && eth.addr == your MAC address**” as the display filter)? Why can you see ARP messages sent to other computers?

1972 ARP messages

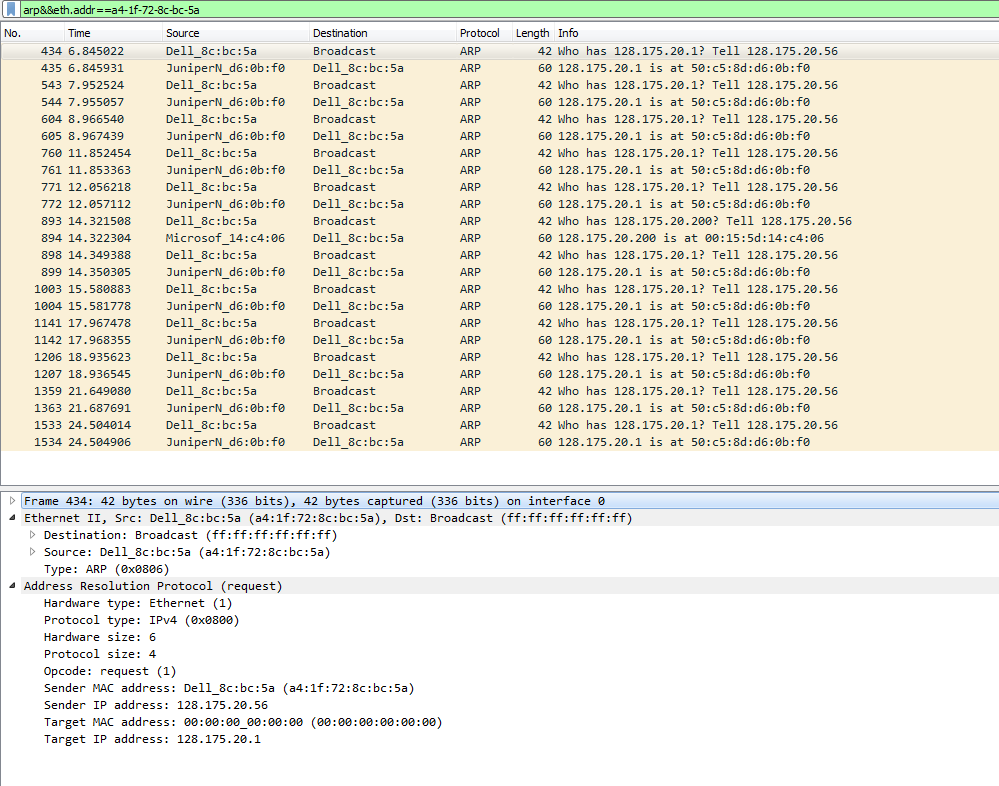
By using arp&&eth.addr==a4-1f-72-8c-bc-5a

Because when the MAC address is not in arp table, the request for MAC address will be broadcasted to the whole network, so since my computer is in this network, it will also receive arp messages sent to other computers.





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



Source: a4:1f:72:8c:bc:5a

Destination: ff:ff:ff:ff:ff:ff

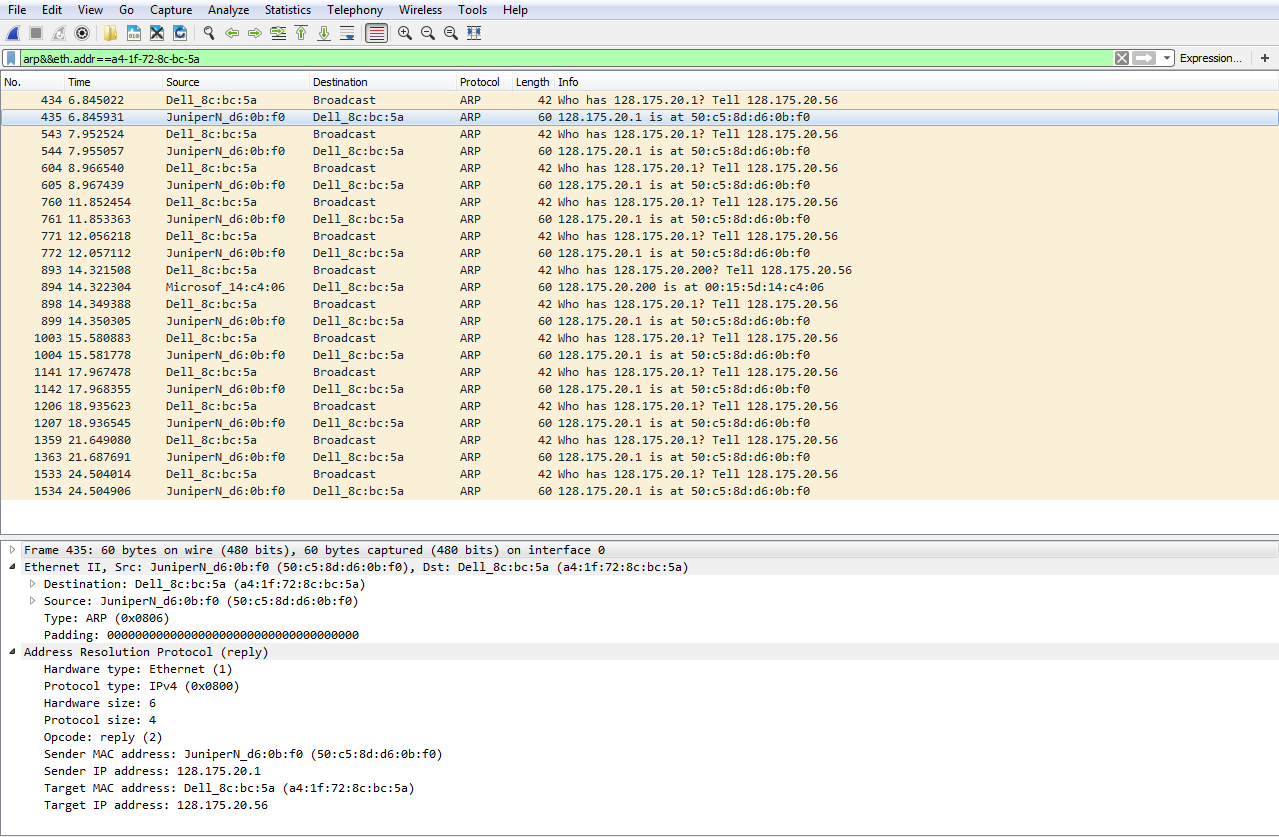
1. Does the ARP message contain the IP address of the sender?

Yes. Beyond the Address Resolution Protocol frame. It should be 128.175.20.56

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

Under the Address Resolution Protocol frame. It says target IP address:128.175.20.1

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



The destination address is a4:1f:72:8c:bc:5a

The source address is 50:c5:8d:d6:0b:f0

1. Where in the ARP message does the “answer” to the earlier ARP request appear – the Ethernet address of the machine having the IP address whose corresponding Ethernet address is being queried?

Under the ARP frame. It says sender MAC address: JuniperN\_d6:0b:f0 (50:c5:8d:d6:0b:f0)

1. 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?

Because it uses broadcasting to all the devices in the network to see if any of these has the target IP address. If there’s one device which has the target IP address, this device will return the MAC address of it to the requester. Other devices which don’t have the target IP address will just ignore and discard the message. That’s why we can see this require, but since we don’t have the MAC address, we will not respond to it. That’s why we can only see the request.