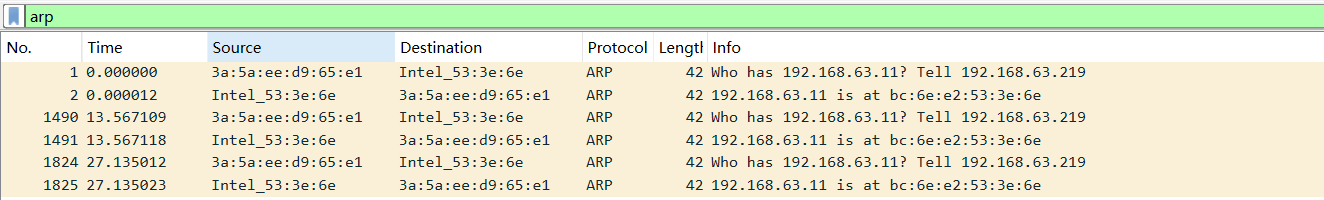
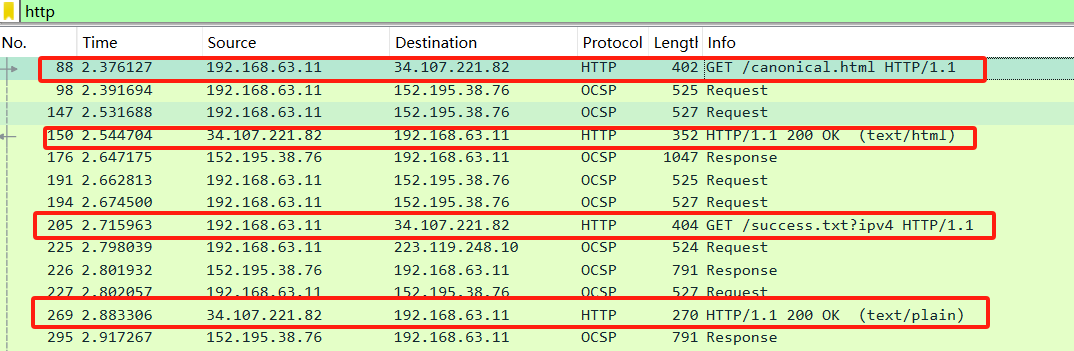
After packet capture is stopped, we filter the search and obtain the protocol Arp below:



Search http below:

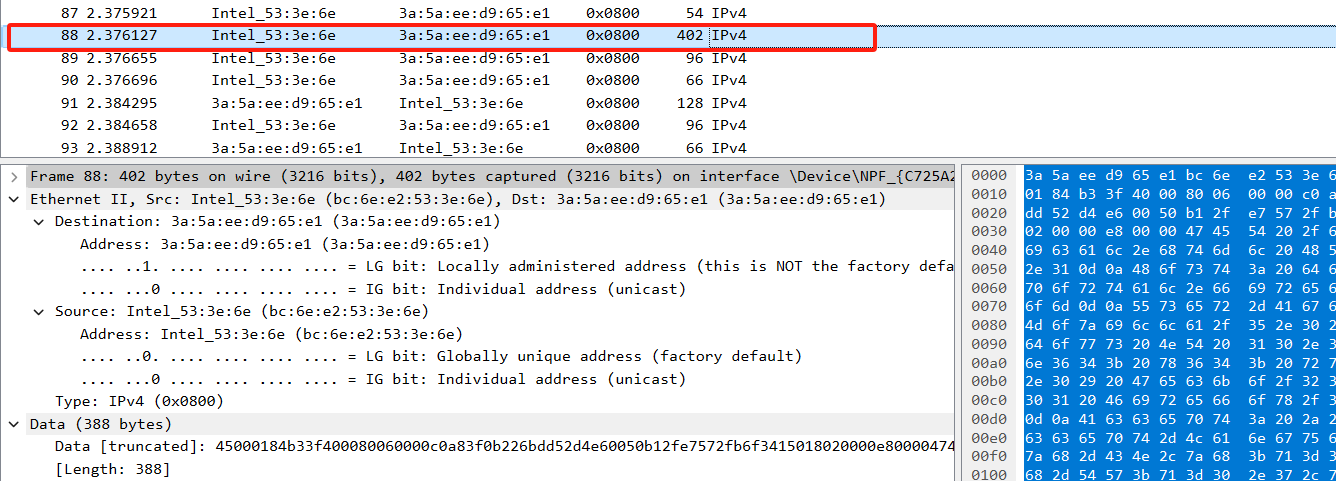


Select the Ethernet frame containing the HTTP GET message, whose time is 2.376127

Select the Ethernet frame containing the HTTP OK message, whose time is 2.544704

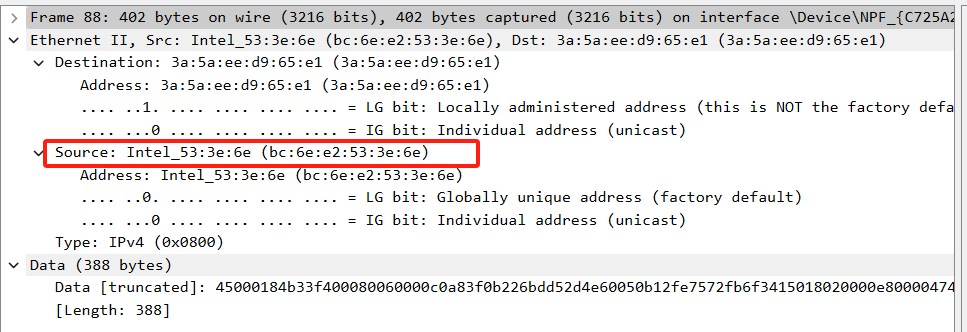
As you can see there are several of them, let's take the first message as an example.

After disabling the IPV4 protocol, We found the packet sent at the corresponding time, as follows:



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

My computer's MAC address is (bc:6e:e2:53:3e:6e)



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

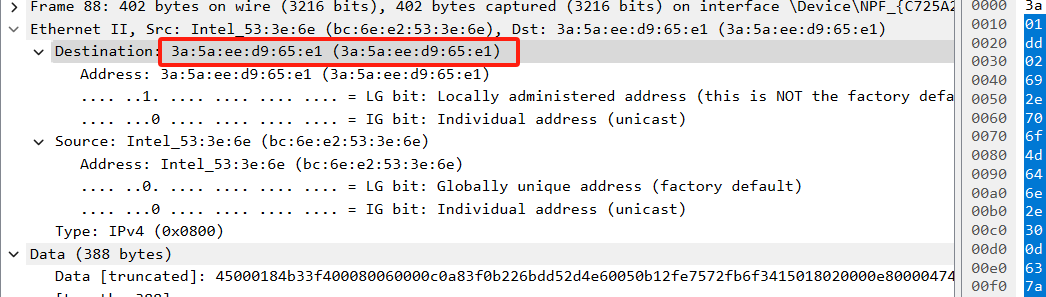
sometimes get wrong. Re-read pages 468-469 in the text and make sure you

understand the answer here.]

Destination: 3a:5a:ee:d9:65:e1

No, It's not the the Ethernet address of gaia.cs.umass.edu.

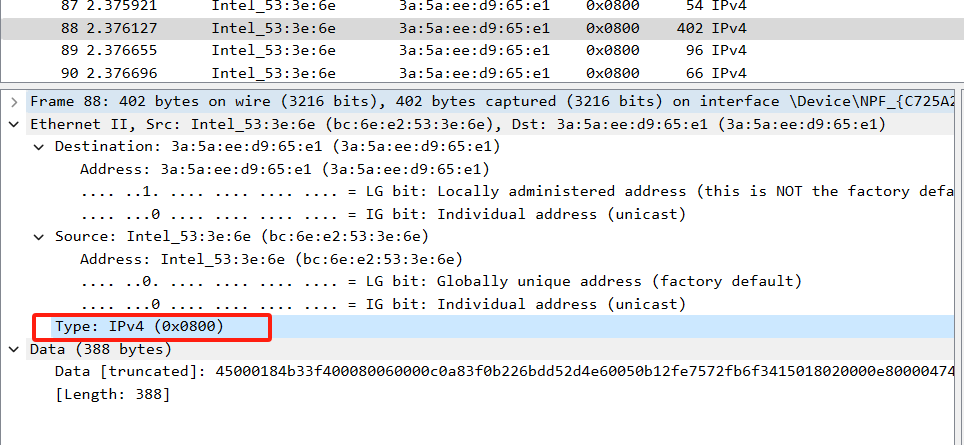
It is the address of the router, which is the link used to go out of the subnet, in here it is the virtual routing address of my phone(I use my phone to turn on the hot spot).



3. Give the hexadecimal value for the two-byte Frame type field. What upper layer

protocol does this correspond to?

The hexadecimal value for the two-byte Frame type field is 0x0800, it corresponds to IPv4 at the network layer.

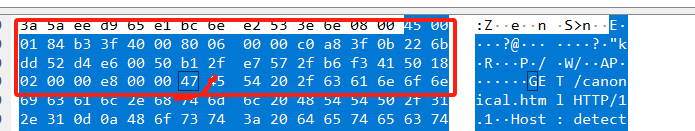


4.How many bytes from the very start of the Ethernet frame does the ASCII “G” in

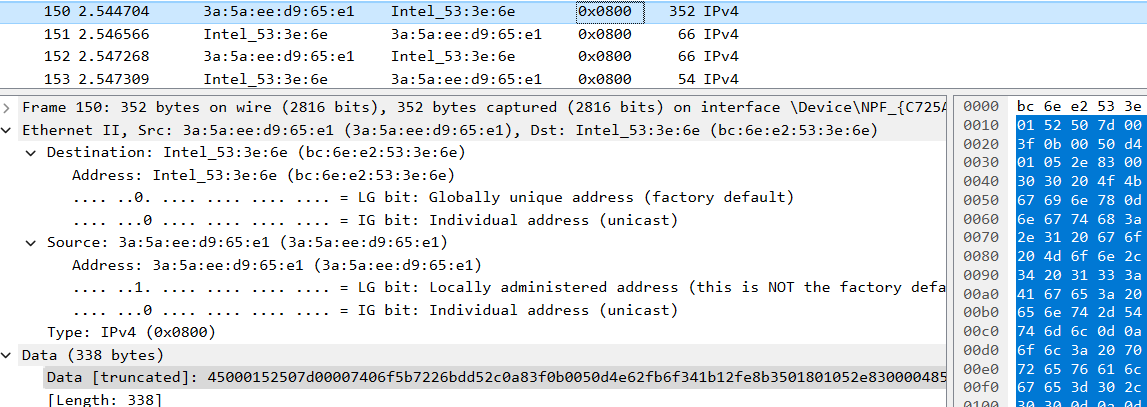
“GET” appear in the Ethernet frame?

The two hexadecimal numbers represent one byte, the first, second, and third lines are all 16 bytes, for a total of 48 bytes, and the fourth line through G has a total of 7 bytes, so a total of 55 bytes.

3\*16+7=55



Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message. Time is 2.544704



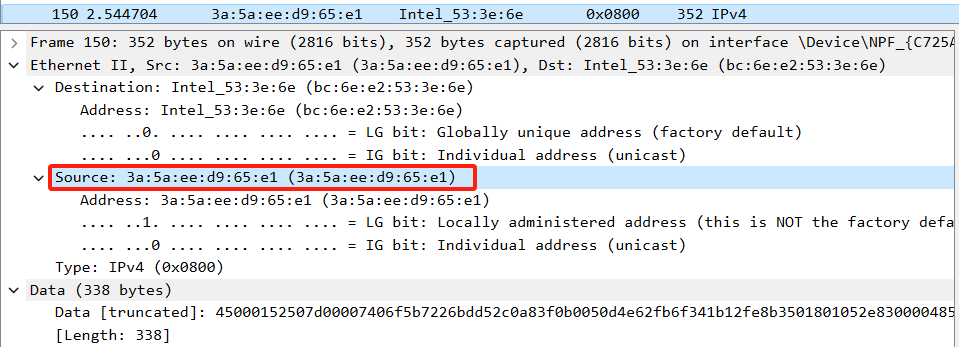
5. What is the value of the Ethernet source address? Is this the address of your

computer, or of gaia.cs.umass.edu (Hint: the answer is *no*). What device has this

as its Ethernet address?

Source: 3a:5a:ee:d9:65:e1

Neither one. As mentioned in the second question, this is the virtual routing address of my phone, and this is the link used to access my subnet.

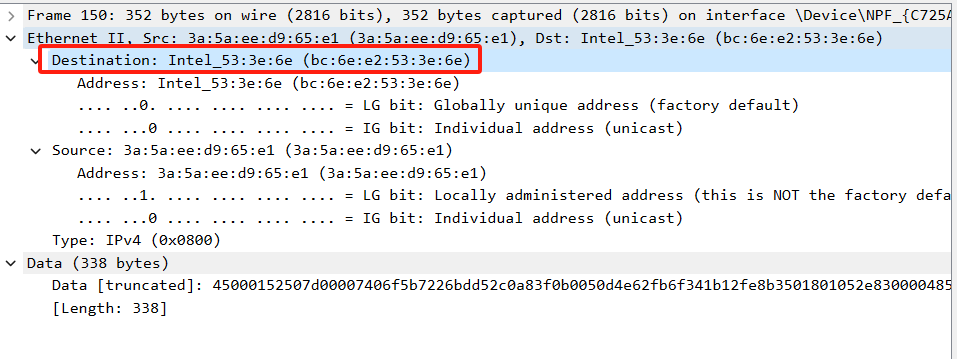


6. What is the destination address in the Ethernet frame? Is this the Ethernet address

of your computer?

Destination: bc:6e:e2:53:3e:6e

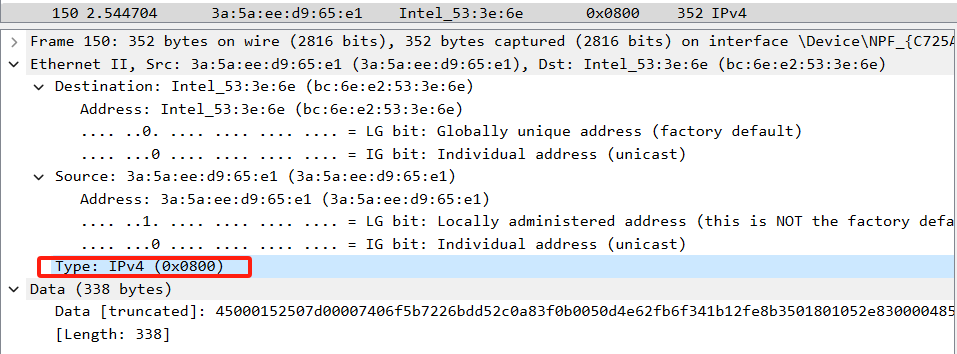
Yes, this is the Ethernet address of my computer.



7.Give the hexadecimal value for the two-byte Frame type field. What upper layer

protocol does this correspond to?

The hexadecimal value for the two-byte Frame type field is 0x0800, it corresponds to IPv4 at the network layer.

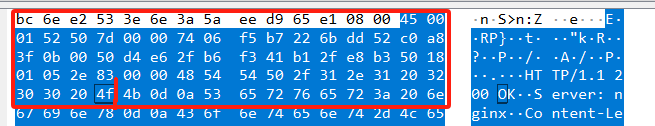


8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in

“OK” (i.e., the HTTP response code) appear in the Ethernet frame ?

68. The two hexadecimal numbers represent one byte, the first, second, third and the fourth lines are all 16 bytes, for a total of 64 bytes, and the fourth line through G has a total of 4 bytes, so a total of 68 bytes.

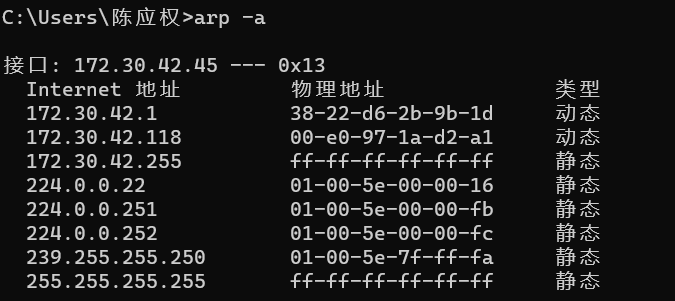
4\*16+4=68



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

each column value? (ps,这里做多了一道)

The Internet address column contains IP addresses, the physical address column contains MAC addresses, and the type indicates the protocol type(Dynamic: An entry is deleted if it is not used within a certain period of time. Static: an entry is stored permanently)

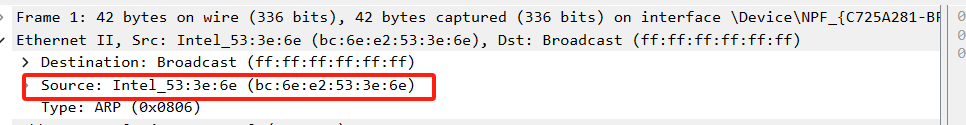


10. What are the hexadecimal values for the source and destination addresses in the

Ethernet frame containing the ARP request message?

Source: (bc:6e:e2:53:3e:6e)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

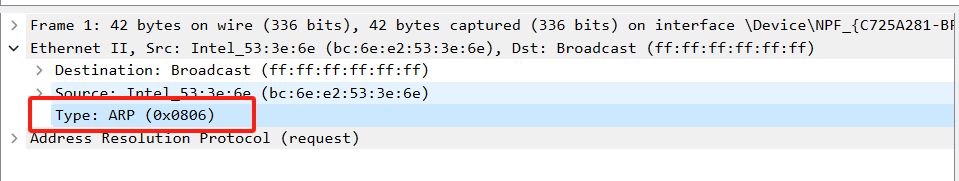


11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What

upper layer protocol does this correspond to?

the hexadecimal value for the two-byte Ethernet Frame type field is 0x0806.

It corresponds to ARP.

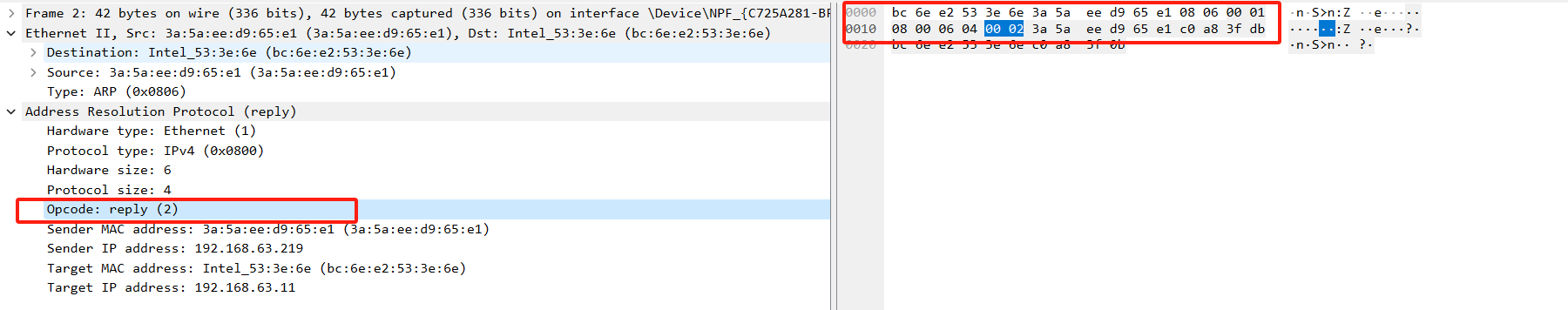


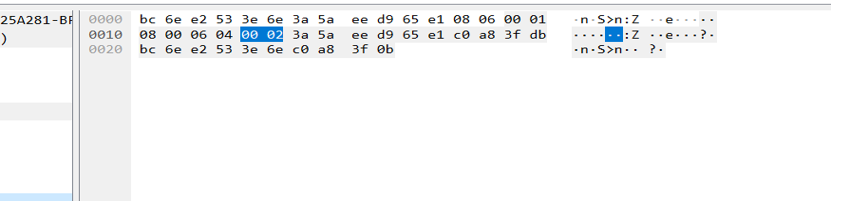
13. Now find the ARP reply that was sent in response to the ARP request.

a) How many bytes from the very beginning of the Ethernet frame does the

ARP opcode field begin?

16\*1+4=20. The first 20 bytes away from the Ethernet frame.

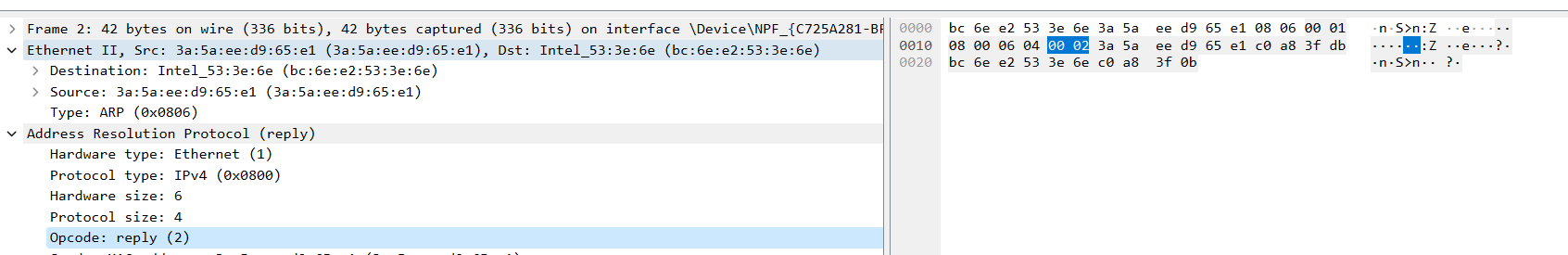




b) What is the value of the opcode field within the ARP-payload part of the

Ethernet frame in which an ARP response is made?

The value of the opcode in the ARP payload portion of the Ethernet frame making the ARP request is 0x0002



c) Where in the ARP message does the “answer” to the earlier ARP request

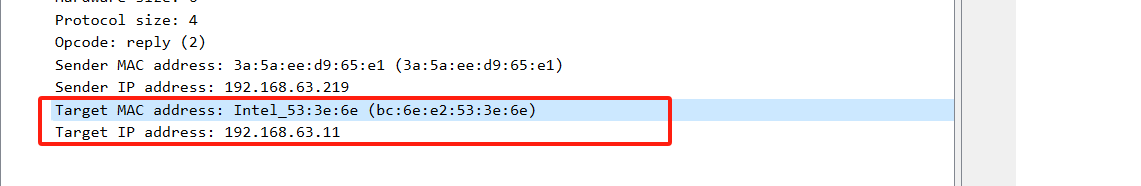
appear – the IP address of the machine having the Ethernet address whose

corresponding IP address is being queried?

Target MAC address: Intel\_53:3e:6e (bc:6e:e2:53:3e:6e)

Target IP address: 192.168.63.11

These two entries correspond to the previous ARP Sender MAC address, Sender IP address



14. What are the hexadecimal values for the source and destination addresses in the

Ethernet frame containing the ARP reply message?

Source: 3a:5a:ee:d9:65:e1 (3a:5a:ee:d9:65:e1)

Destination: Intel\_53:3e:6e (bc:6e:e2:53:3e:6e)

