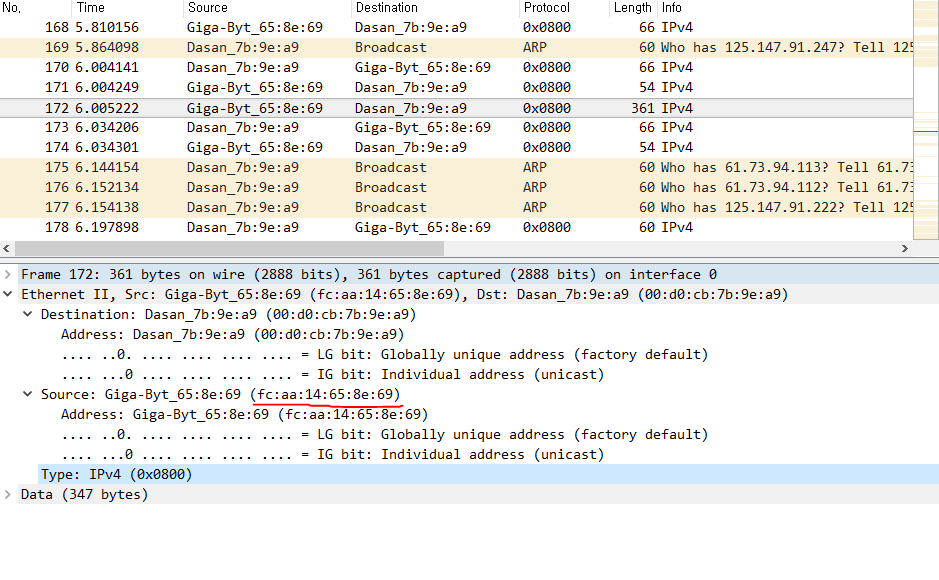
Wireshark

Ethernet & ARP

15146301 강신혁

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



**48-bit Ethernet address of my computer**

**- fc:aa:14:65:8e:69**

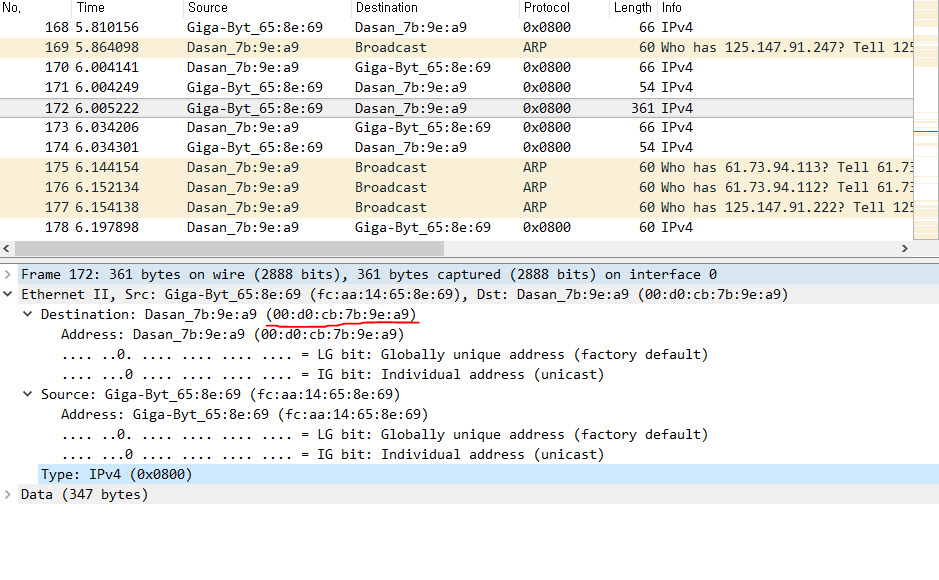
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet

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.]



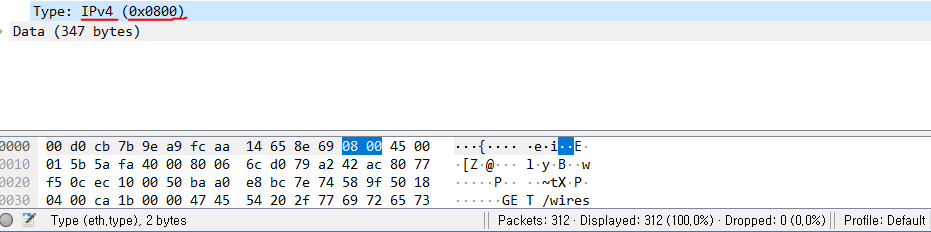
**48-bit destination address**

**- 00:d0:cb:7b:9e:a9**

**No. This MAC address is for first hop router of my computer.**

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

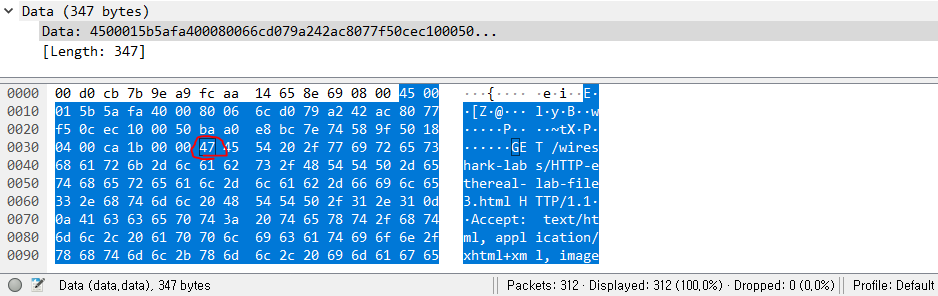
protocol does this correspond to?



**0x0800, correspond to IPv4**

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

“GET” appear in the Ethernet frame?



**After 54 bytes, G in ‘GET’ appears.**

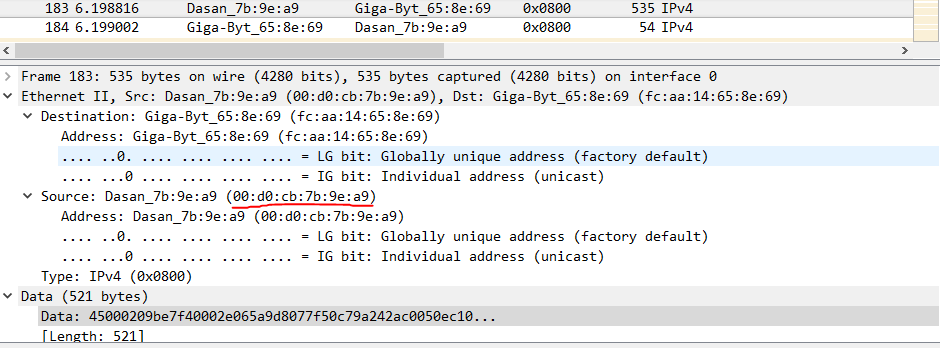
Next, answer the following questions, based on the contents of the Ethernet frame

containing the first byte of the HTTP response message.

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?

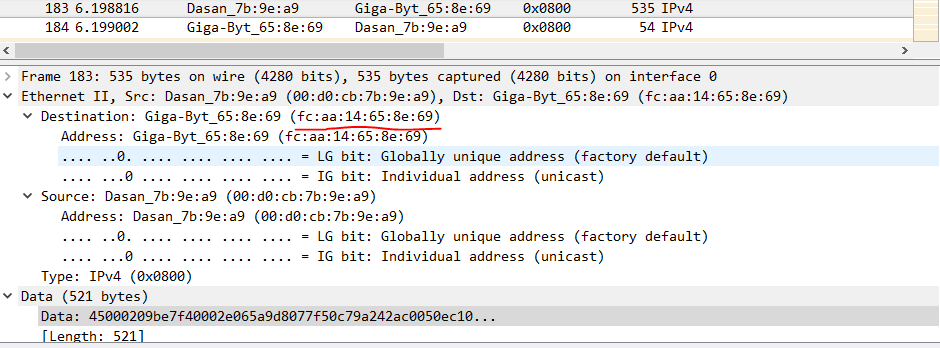


**Ethernet source address is 00:d0:cb:7b:9e:a9**

**This address if for first hop router of my computer.**

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

of your computer?

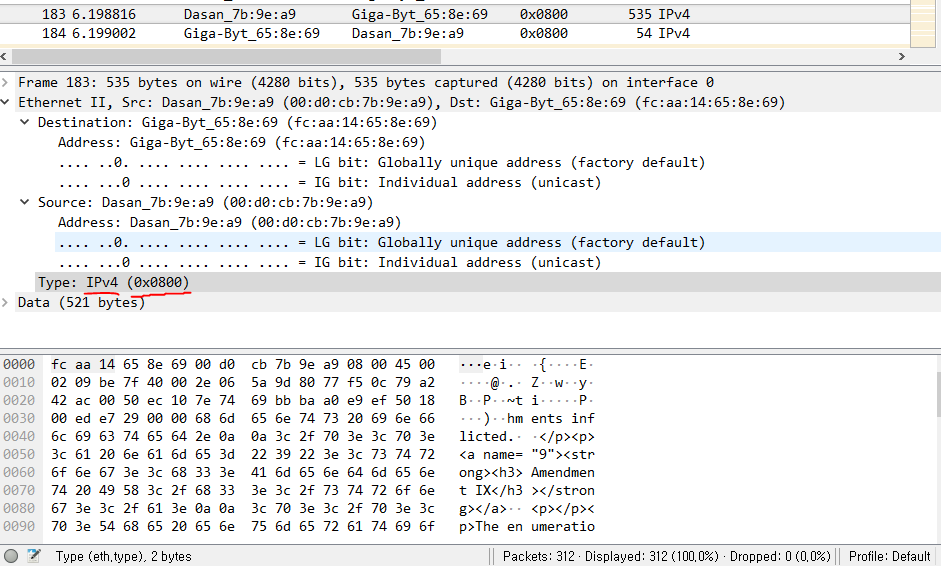


**Ethernet destination address is fc:aa:14:65:8e:69**

**Yes, this is the Ethernet address of my computer.**

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

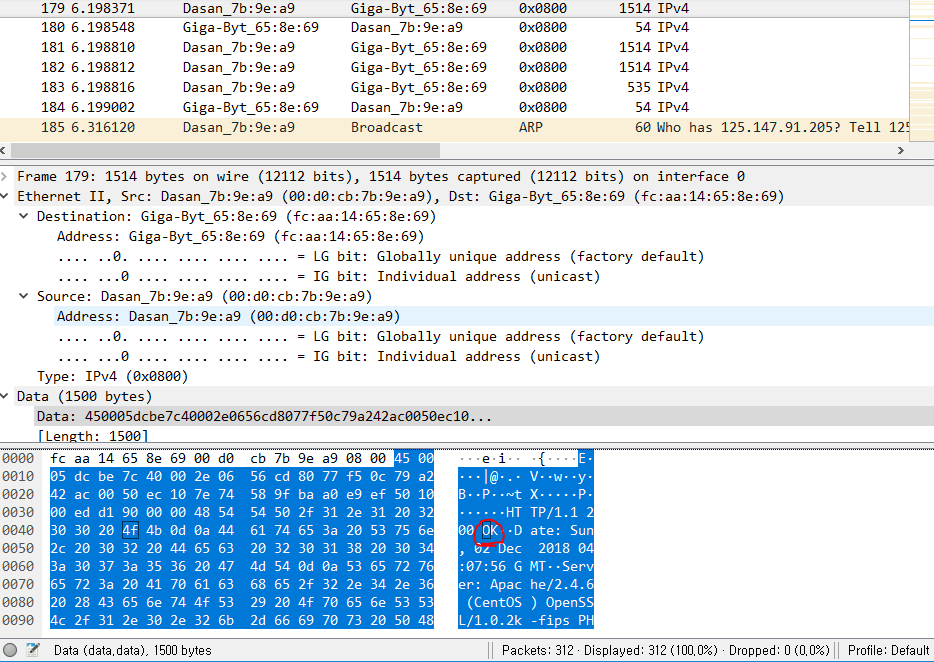
protocol does this correspond to?



**0x0800, correspond to IPv4**

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?



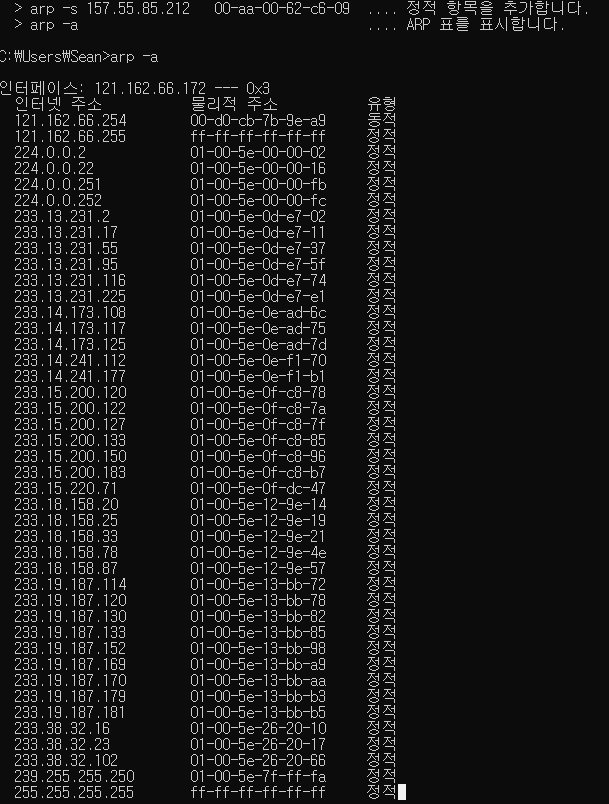
**After 67 bytes, ‘O’ in ‘OK’ appears.**

The Windows *arp* command with no arguments will display the contents of the ARP

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

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

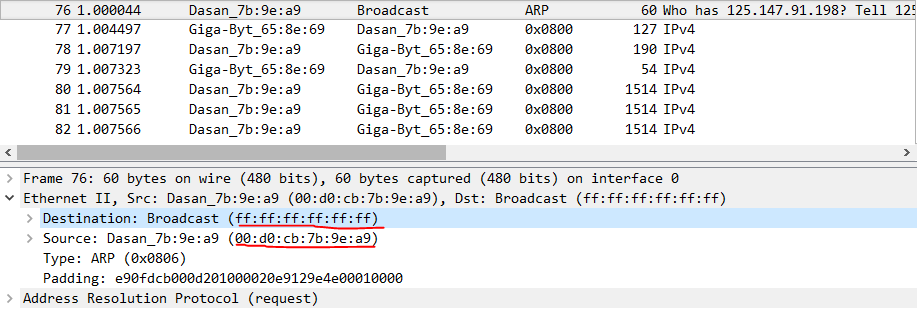
each column value?



**The first column represent the internet address and the second address represent MAC address. The third column shows whether the address is dynamic or static.**

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

Ethernet frame containing the ARP request message?

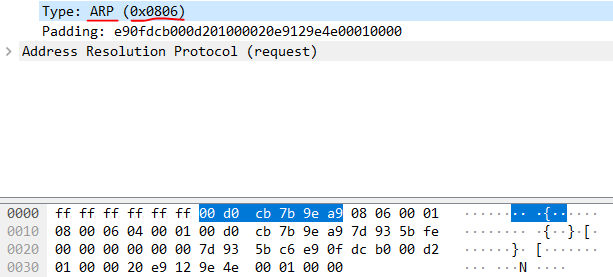


**Source address: 00:d0:cb:7b:9e:a9**

**Destination: 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?



**0x0806, corresponds to ARP**

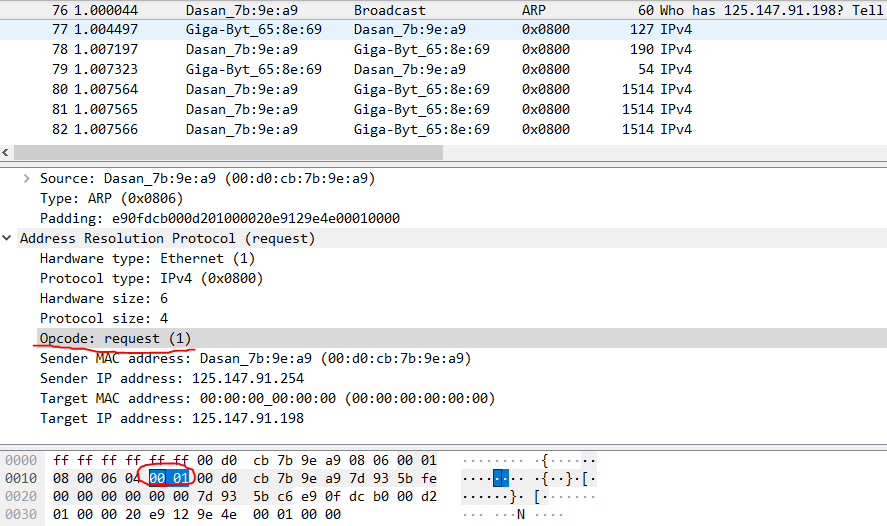
12. Download the ARP specification from

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?



**After 20 bytes, opcode field begin.**

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?

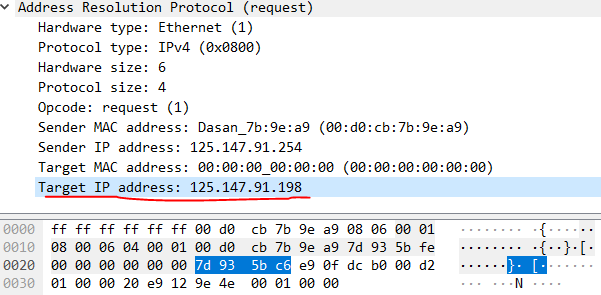
**0x0001, request(1)**

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

**Yes, Source address: 00:d0:cb:7b:9e:a9**

d) Where in the ARP request does the “question” appear – the Ethernet

address of the machine whose corresponding IP address is being queried?



**In the Target IP address field**

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?

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?

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?

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

Ethernet frame containing the ARP reply message?

**Could not find any ARP reply message even I tried twice.**

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

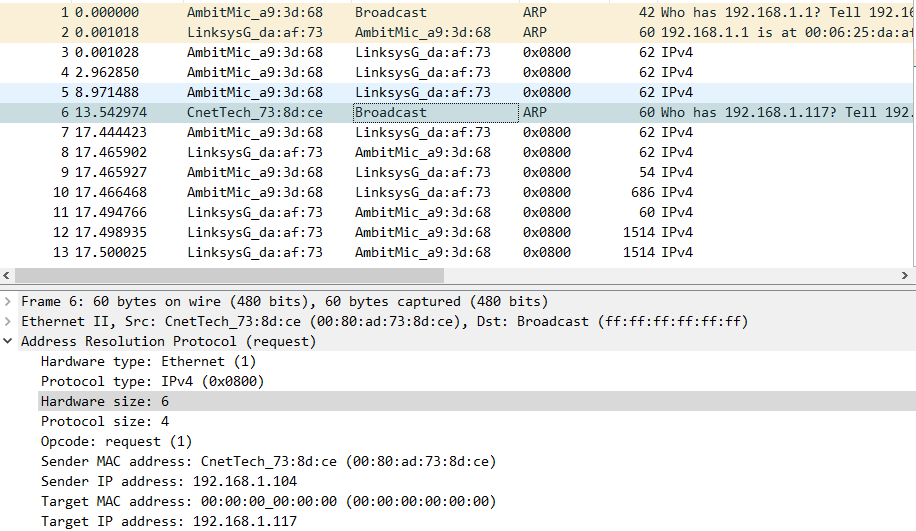
running Wireshark, and the ARP reply sent to the computer running Wireshark by

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?



**Although ARP request message is broadcast, ARP reply message is unicast which directly sent to the ARP request sender.**