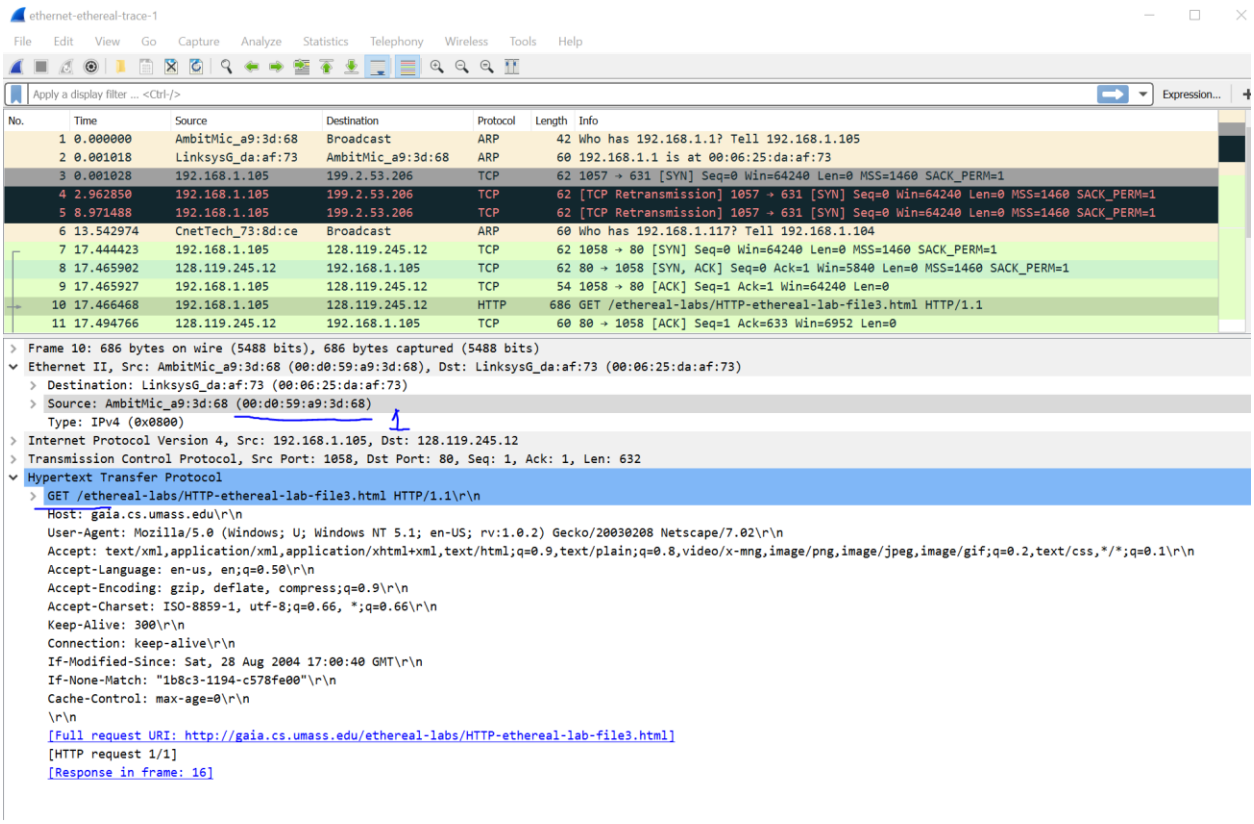
Lachlan Sinclair

Lab 5: CS 372

12/7/2019

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

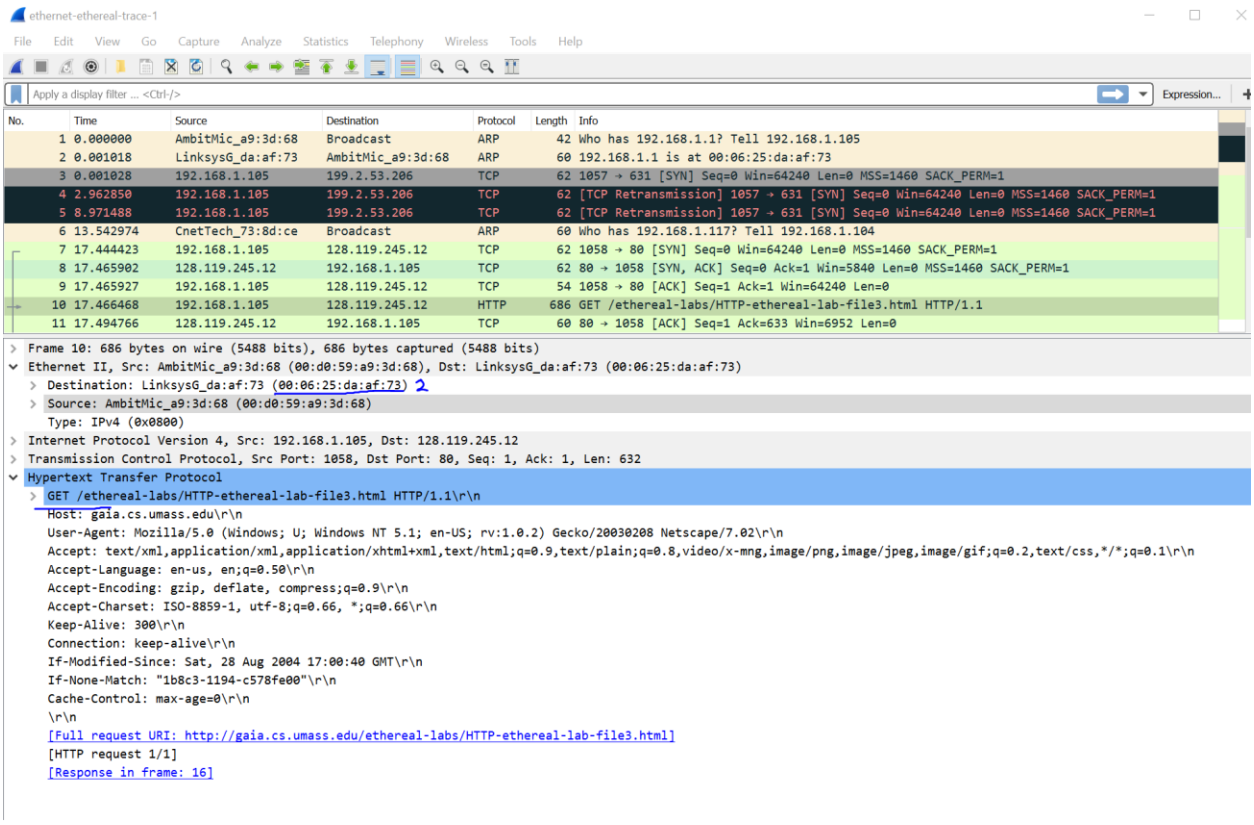
00:d0:59:a9:3d:68 is the 48 bit address of “my” computer.



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.]

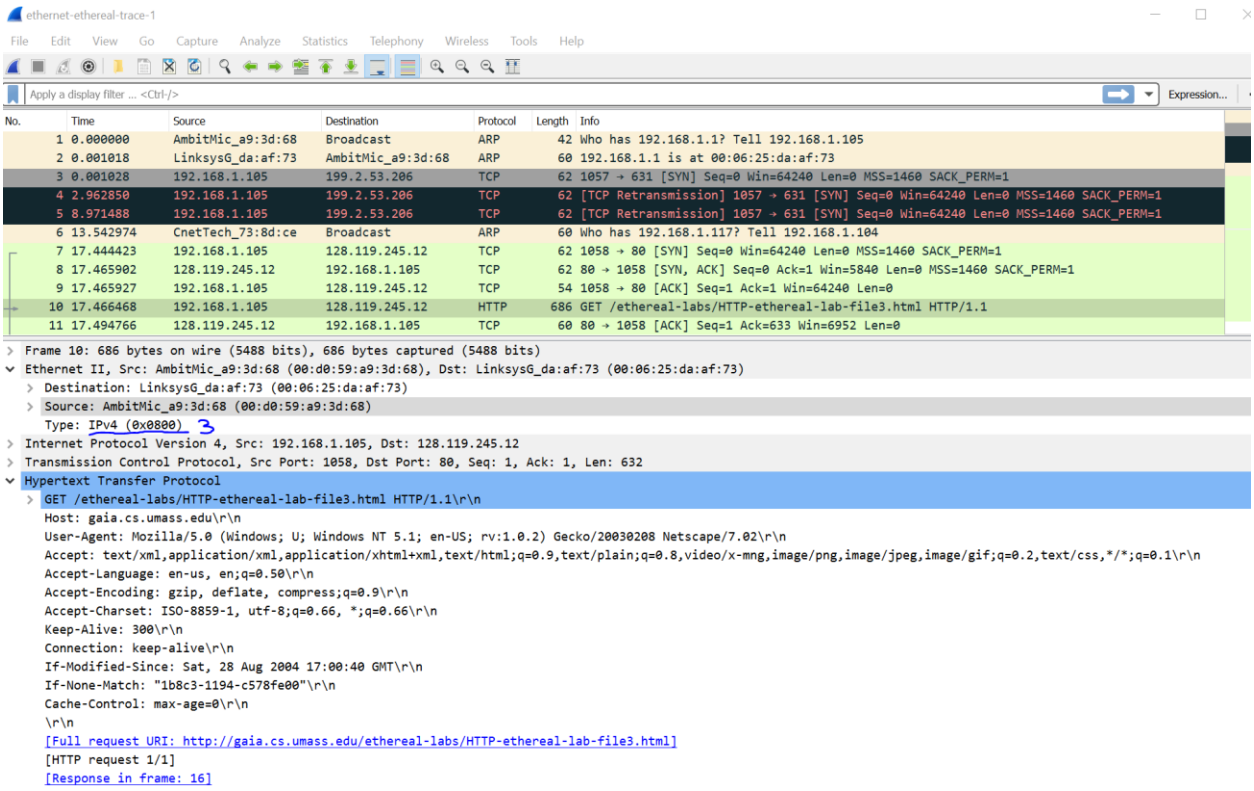
The 48-bit destination address is 00:06:25:da:af:73

This is the address of the router in the subnet that is being used by “my” computer to leave said subnet.



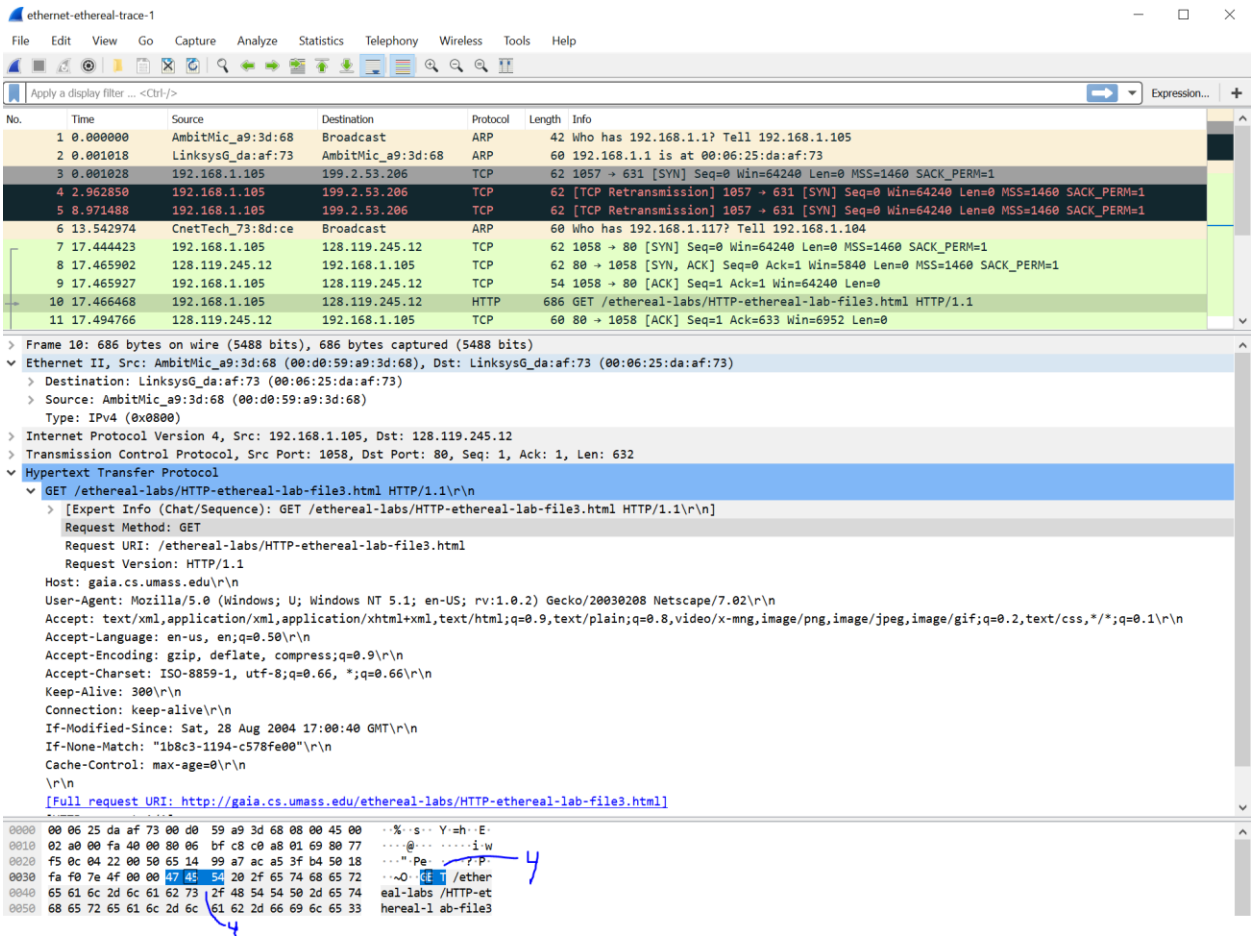
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

The hexadecimal for the two-byte frame type is 0x0800. This refers to 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?

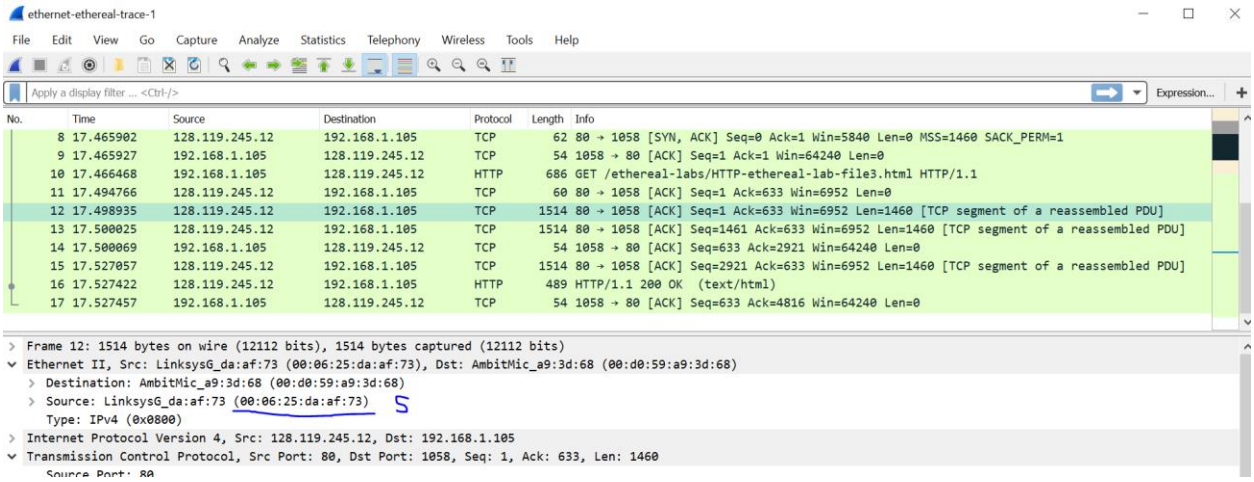
The G appears 54 bytes into the frame. When mousing over the byte, the visible byte count at the bottom of the window uses base 0 counting so that’s what I am going to use base 0 counting.



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?

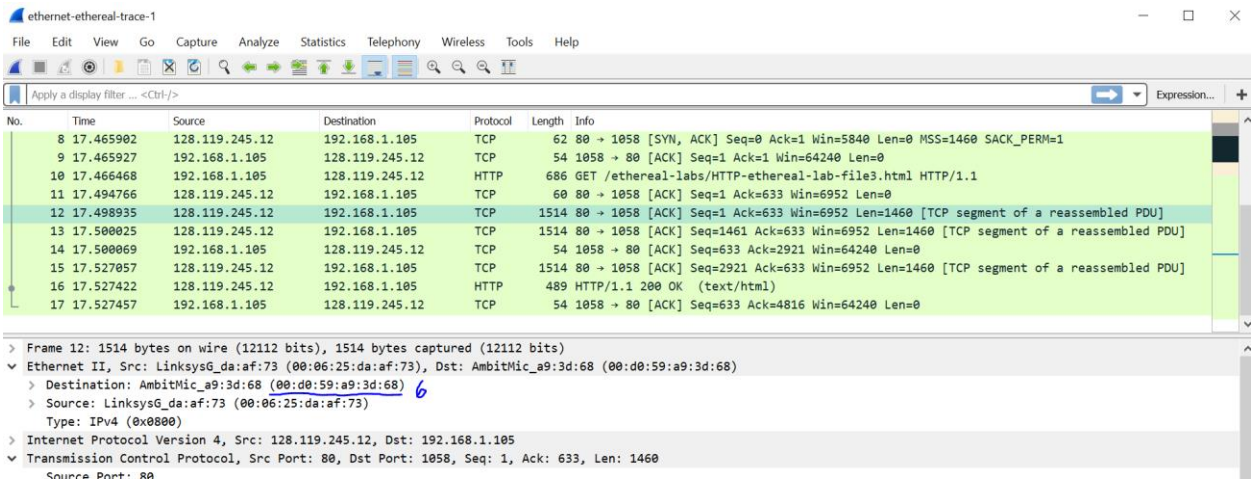
The source address is 00:06:25:da:af:73

As in question 2 this is the address of the external router used by “my” computer.



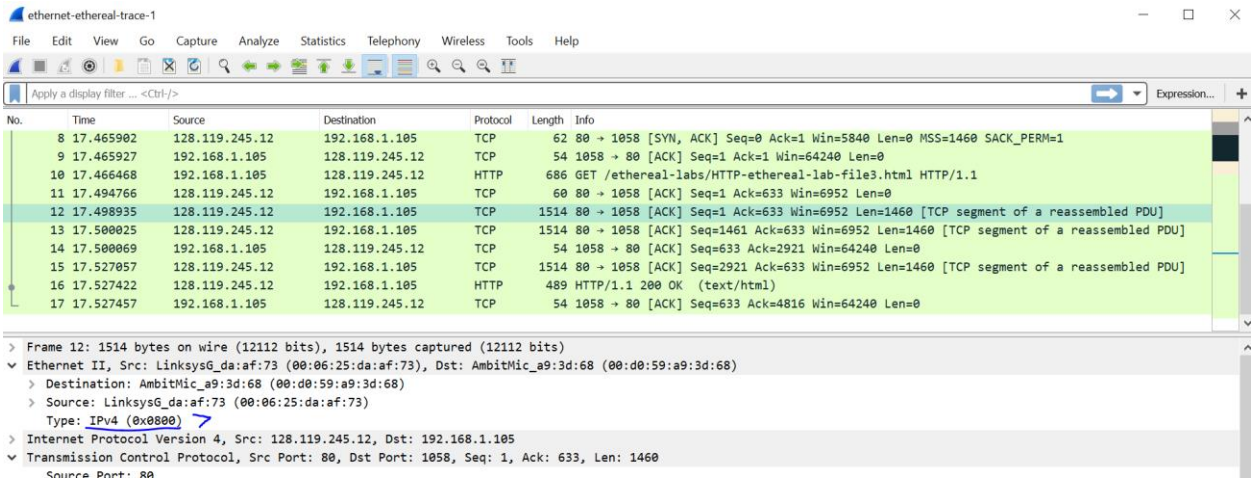
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

00:d0:59:a9:3d:68 which is the ethernet address of “my” computer.



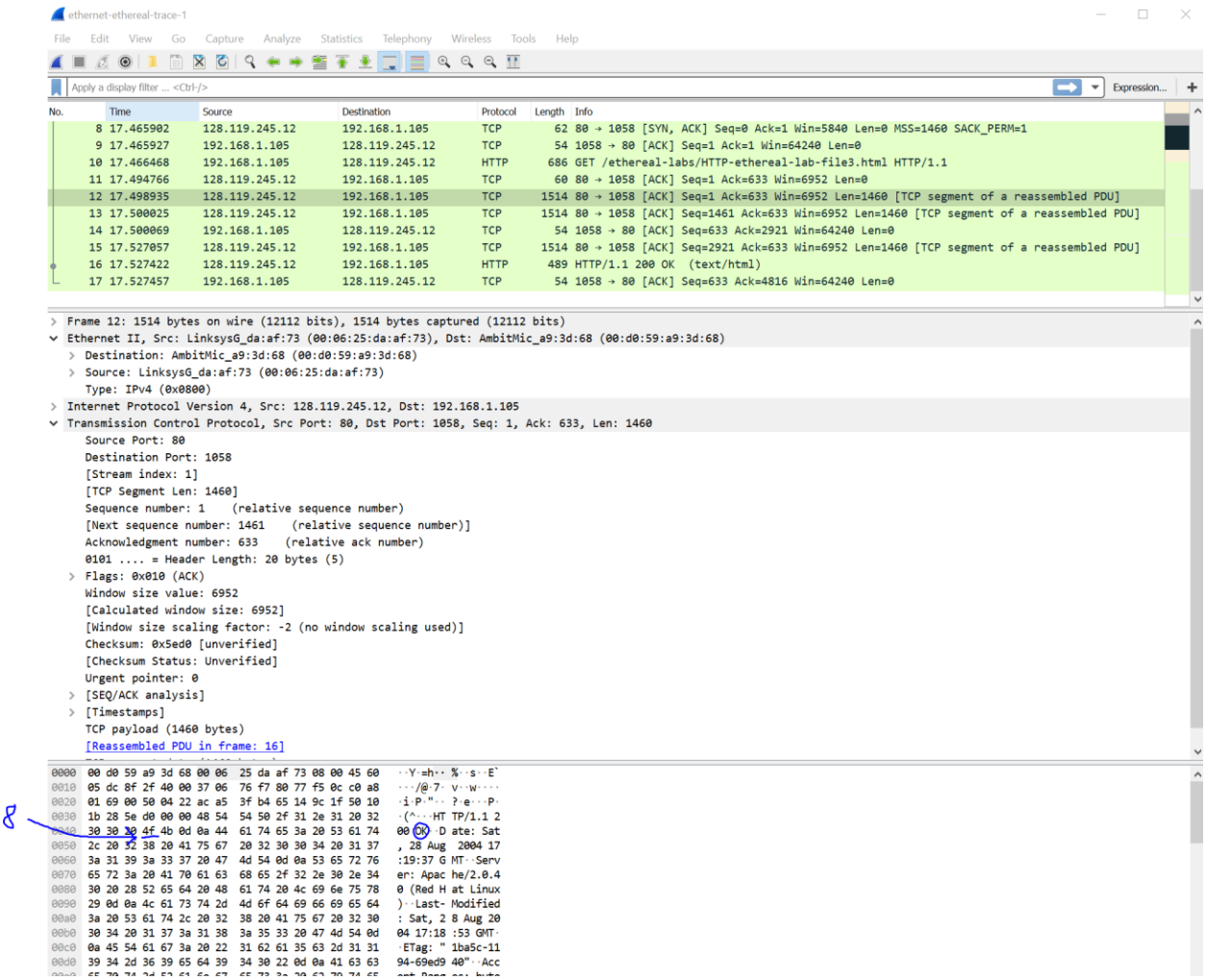
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

The hexadecimal for the two-byte frame type is 0x0800. This refers to 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?

The O appears 66 bytes in, using a base 0 counting system.



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

The internet address column lists the IP addresses.

The physical address column lists the MAC addresses.

The type column lists whether the entry is dynamic or static, static being the manually entered entries and dynamic being a entry that that is kept for a specific amount of time.

Internet Address	Physical Address	Type
192.168.0.1	dc-bf-e9-f6-64-61	dynamic
192.168.0.14	d8-31-34-32-2c-1f	dynamic
192.168.0.16	02-0f-b5-71-7d-d4	dynamic
192.168.0.23	02-0f-b5-9a-94-42	dynamic
192.168.0.27	02-0f-b5-e3-97-e4	dynamic

192.168.0.30 60-6d-3c-12-e1-47 dynamic

192.168.0.36 9c-5a-44-58-4a-00 dynamic

192.168.0.255 ff-ff-ff-ff-ff-ff static

224.0.0.22 01-00-5e-00-00-16 static

224.0.0.251 01-00-5e-00-00-fb static

224.0.0.252 01-00-5e-00-00-fc static

239.255.255.250 01-00-5e-7f-ff-fa static

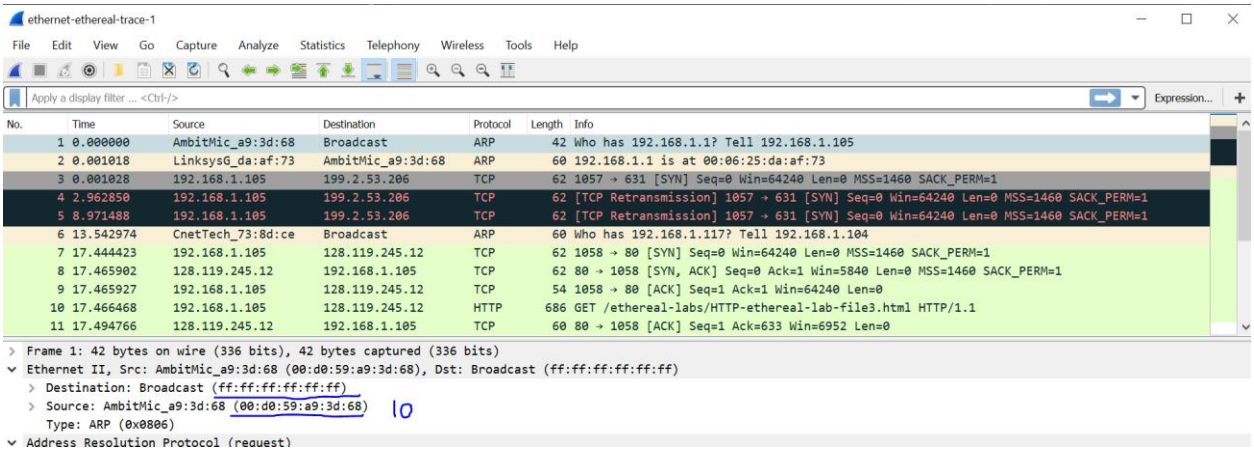
255.255.255.255 ff-ff-ff-ff-ff-ff static

```
c:\Windows\System32>arp -a -v

Interface: 127.0.0.1 --- 0x1
  Internet Address      Physical Address      Type
  224.0.0.0                                   static
  224.0.0.22                                  static
  224.0.0.251                                 static
  239.255.255.250                             static
  255.255.255.255                             static

Interface: 192.168.0.19 --- 0xe
  Internet Address      Physical Address      Type
  192.168.0.1           dc-bf-e9-f6-64-61     dynamic
  192.168.0.14          d8-31-34-32-2c-1f     dynamic
  192.168.0.16          02-0f-b5-71-7d-d4     dynamic
  192.168.0.23          02-0f-b5-9a-94-42     dynamic
  192.168.0.27          02-0f-b5-e3-97-e4     dynamic
  192.168.0.30          60-6d-3c-12-e1-47     dynamic
  192.168.0.36          9c-5a-44-58-4a-00     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

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

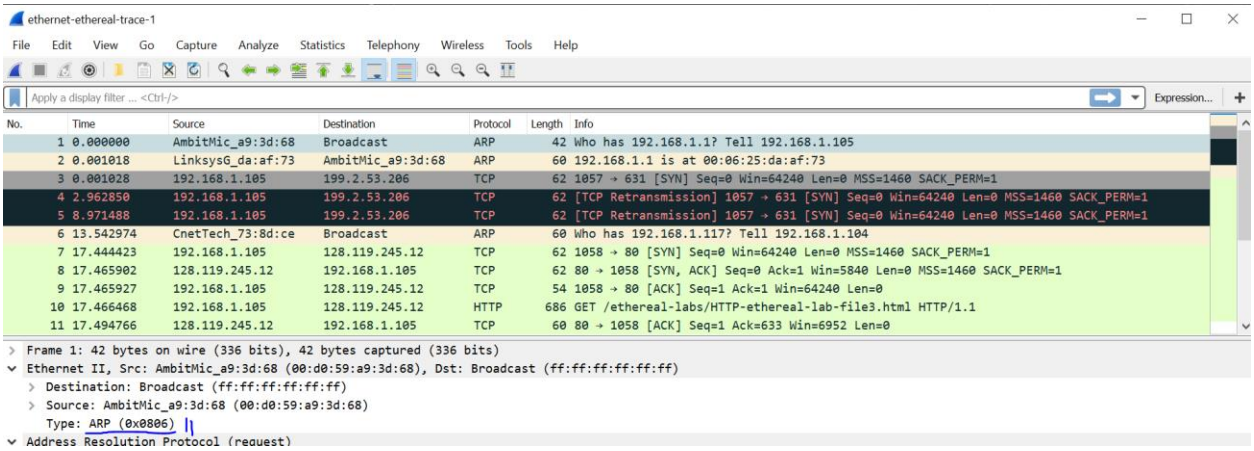
Destination Address: ff:ff:ff:ff:ff:ff

Source address: 00:d0:59:a9:3d:68



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

The two-byte the ethernet frame type field is 0x0806 which corresponds to the ARP protocol.



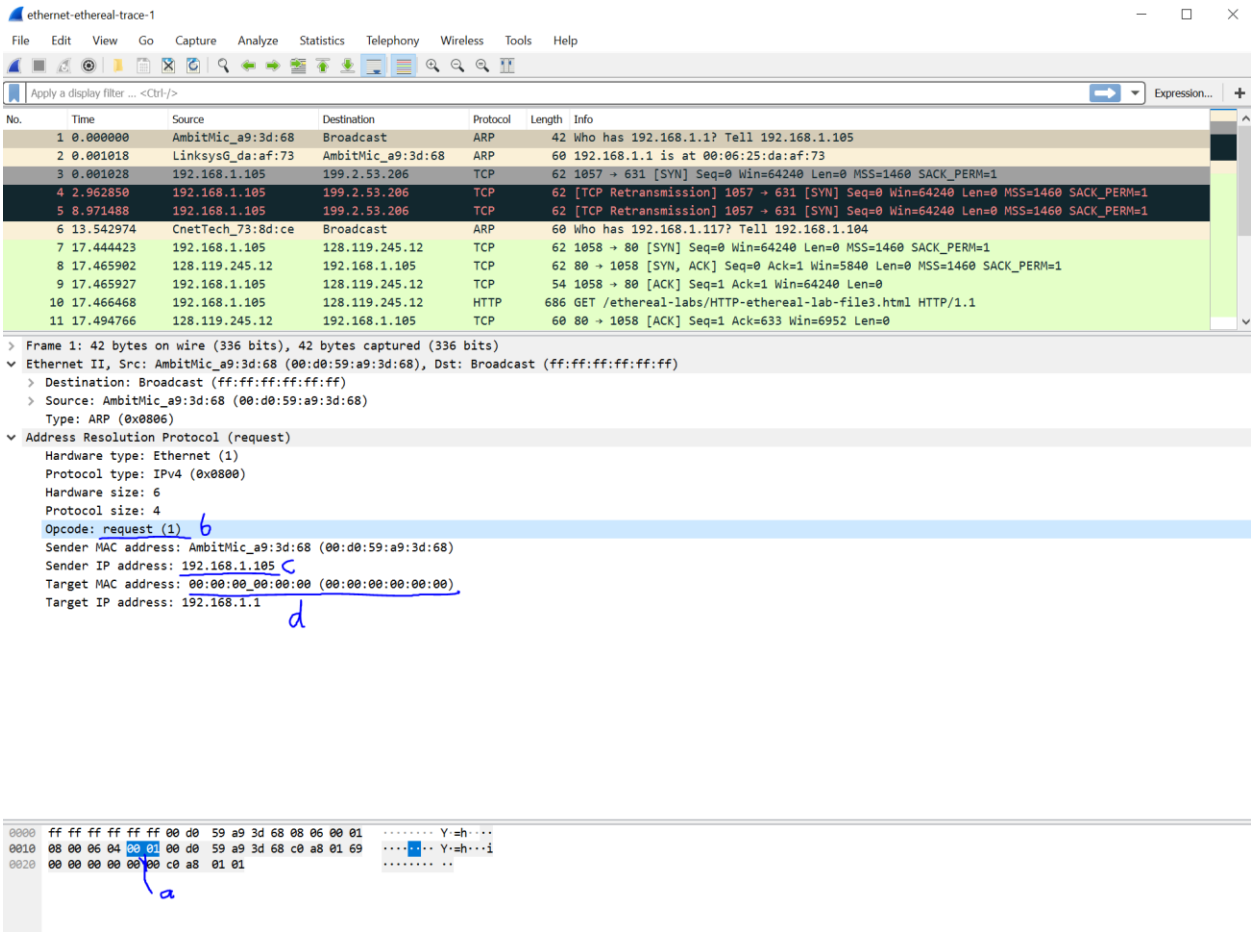
12. a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin? b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made? c) Does the ARP message contain the IP address of the sender? d) Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

a) The opcode field begins of byte 20, when using a base 0 counting system.

b) The opcode field value is 1, designating it as a request.

c) The message does contain the IP address of the sender. Its 192.168.1.105

d) You can see in the screenshot below where the request defines the target MAC (Ethernet) address which is the question. The target MAC address is 00:00:00:00:00:00 which signifies it is requesting the mac address from that machine with the IP 192.168.1.105

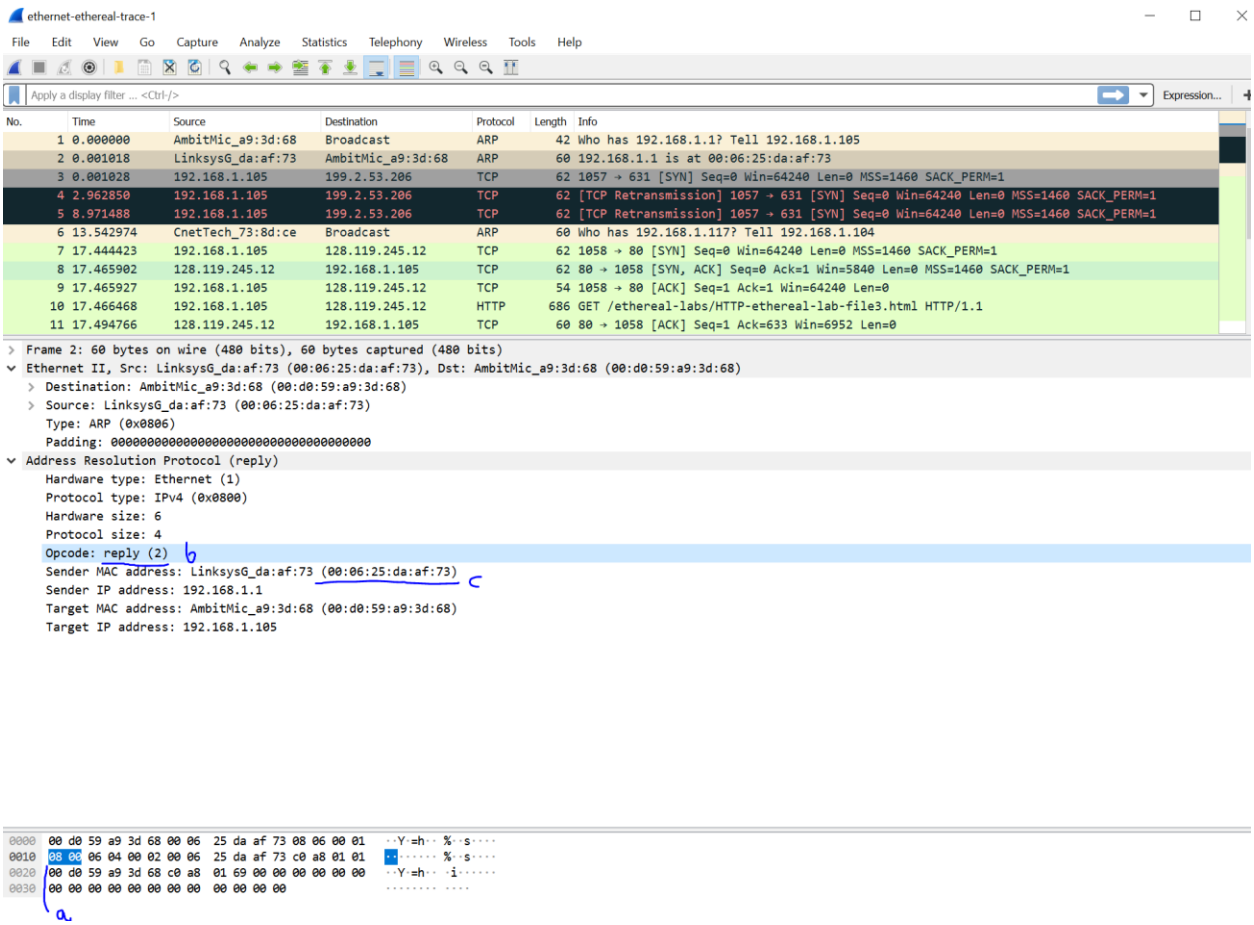


13. Now find the ARP reply that was sent in response to the ARP request. a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin? b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made? c) Where 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?

a) The opcode field begins on byte 20, when using a base 0 counting system.

b) The opcode field value is 2, designating it as a reply.

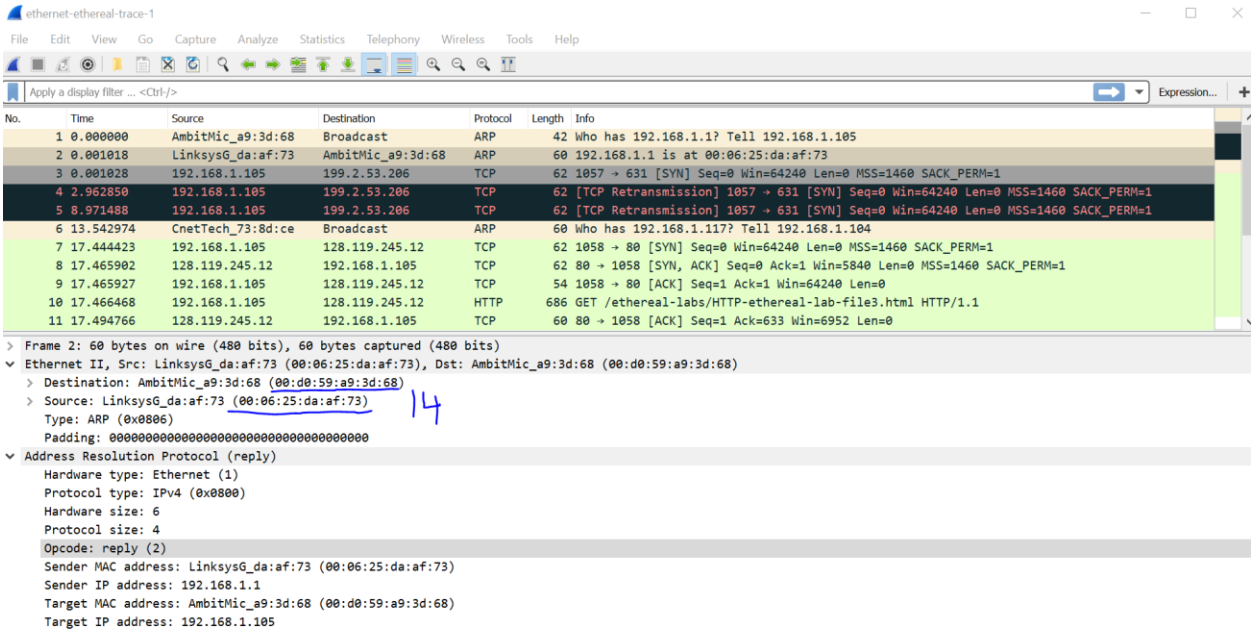
c) The message includes the answer in the sender MAC address section, so the answer is 00:06:25:da:af:73



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

Source address: 00:06:25:da:af:73

Destination address: 00:d0:59:a9:3d:68



15. 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 was not ARP reply sent because there isn't a computer in the subnet that has the Ethernet address requested in packet 6 (192.168.1.104).

EX-1: In theory I think it would cause problems any time that entry was used, until at some point it gets updated or removed by the ARP protocol. I tried testing this but was encountering permissions errors.

EX-2: My ARP cache uses a default reachable time of 4000ms as seen below in the screen shot.