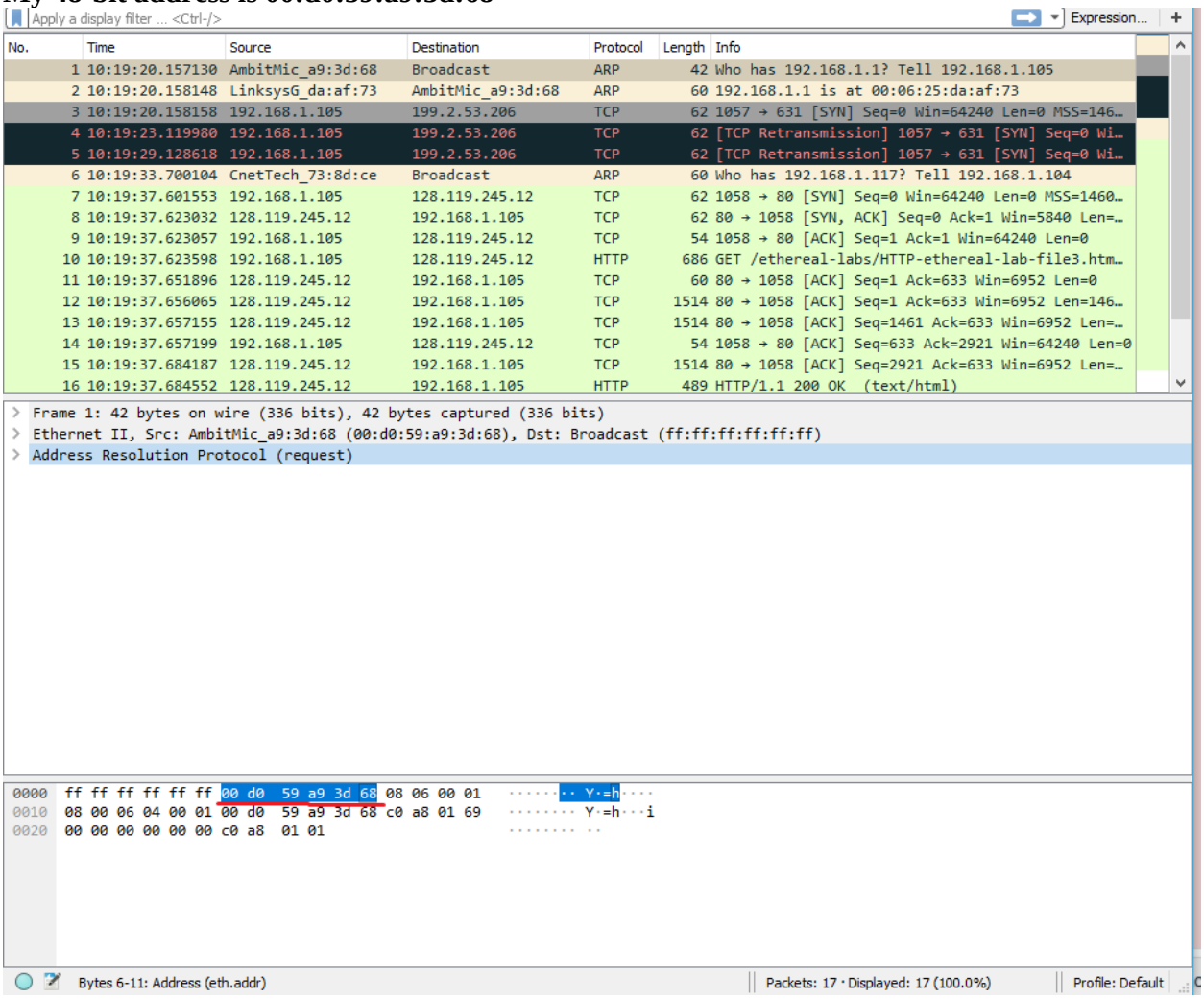
Hao (Jeff) Deng
ID: 932912420

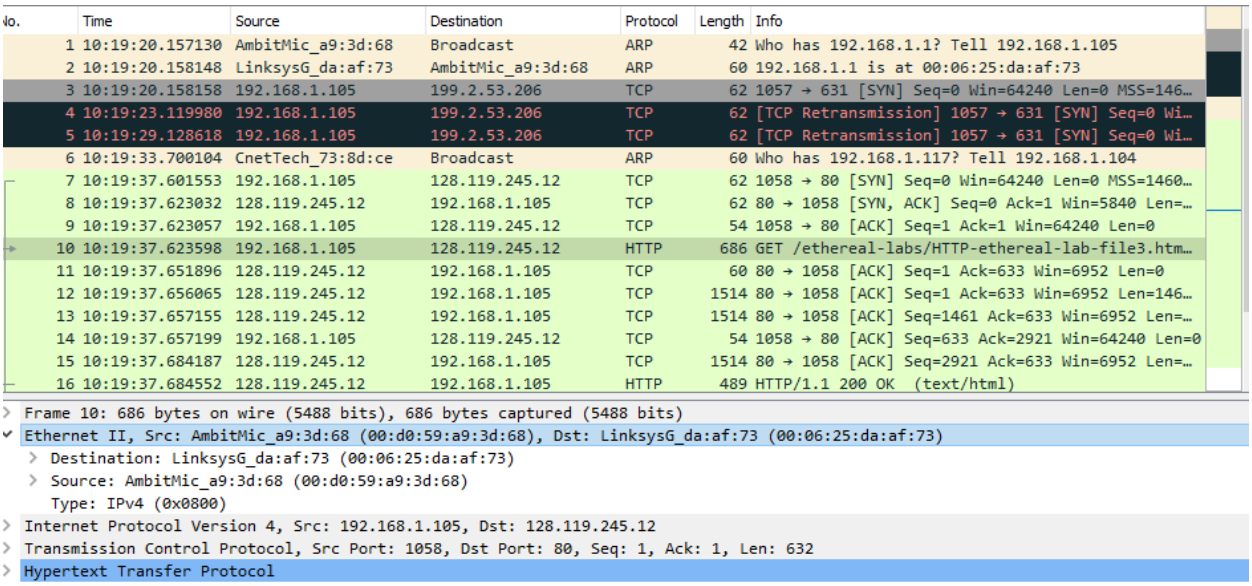
CS 372 – Lab 5

1. What is the 48-bit Ethernet address of your computer?
   My 48-bit address is 00:d0:59:a9:3d:68



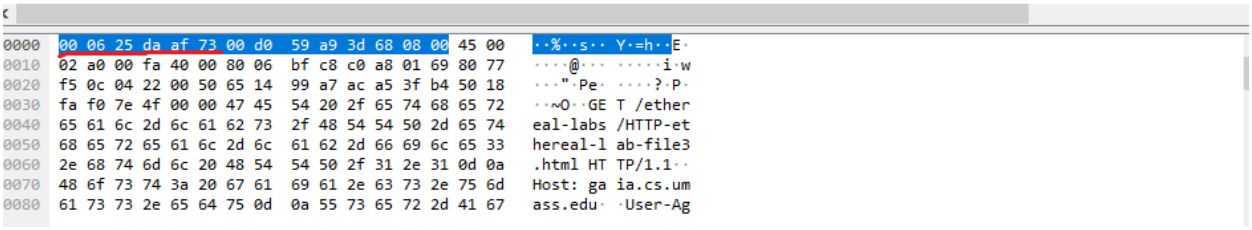
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is *no*). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]
   The 48-bit destination address is 00:06:25:da:af:73
   This is the first-hop router; the mac address for my router or internet gateway address.

Hao (Jeff) Deng
ID: 932912420



No.	Time	Source	Destination	Protocol	Length	Info
1	10:19:20.157130	AmbitMic_a9:3d:68	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	10:19:20.158148	LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
3	10:19:20.158158	192.168.1.105	199.2.53.206	TCP	62	1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=146…
4	10:19:23.119980	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Wi…
5	10:19:29.128618	192.168.1.105	199.2.53.206	TCP	62	[TCP Retransmission] 1057 → 631 [SYN] Seq=0 Wi…
6	10:19:33.700104	CnetTech_73:8d:ce	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104
7	10:19:37.601553	192.168.1.105	128.119.245.12	TCP	62	1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460…
8	10:19:37.623032	128.119.245.12	192.168.1.105	TCP	62	80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=…
9	10:19:37.623057	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
10	10:19:37.623598	192.168.1.105	128.119.245.12	HTTP	686	GET /ethereal-labs/HTTP-ethereal-lab-file3.htm…
11	10:19:37.651896	128.119.245.12	192.168.1.105	TCP	60	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
12	10:19:37.656065	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=146…
13	10:19:37.657155	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=…
14	10:19:37.657199	192.168.1.105	128.119.245.12	TCP	54	1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0
15	10:19:37.684187	128.119.245.12	192.168.1.105	TCP	1514	80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=…
16	10:19:37.684552	128.119.245.12	192.168.1.105	HTTP	489	HTTP/1.1 200 OK (text/html)

```
> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
v Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
    > Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
    > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 192.168.1.105, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 1058, Dst Port: 80, Seq: 1, Ack: 1, Len: 632
> Hypertext Transfer Protocol
```

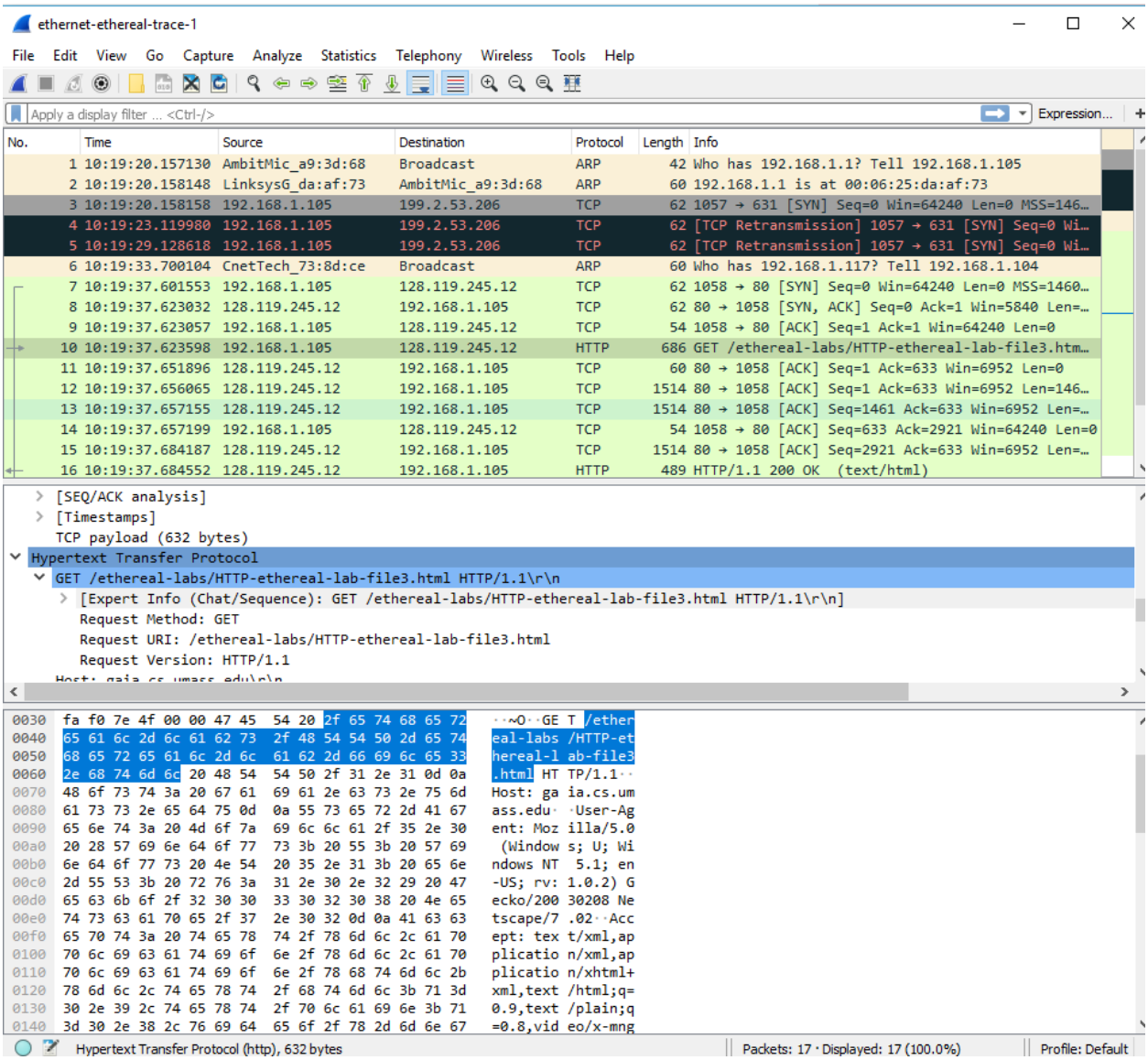


```
0000  00 06 25 da af 73 00 d0  59 a9 3d 68 08 00 45 00   ··%··s·· Y·=h··E·
0010  02 a0 00 fa 40 00 80 06  bf c8 c0 a8 01 69 80 77   ····@··· ·····i·w
0020  f5 0c 04 22 00 50 65 14  99 a7 ac a5 3f b4 50 18   ···"·Pe· ····?·P·
0030  fa f0 7e 4f 00 00 47 45  54 20 2f 65 74 68 65 72   ··~O··GE T /ether
0040  65 61 6c 2d 6c 61 62 73  2f 48 54 54 50 2d 65 74   eal-labs /HTTP-et
0050  68 65 72 65 61 6c 2d 6c  61 62 2d 66 69 6c 65 33   hereal-l ab-file3
0060  2e 68 74 6d 6c 20 48 54  54 50 2f 31 2e 31 0d 0a   .html HT TP/1.1··
0070  48 6f 73 74 3a 20 67 61  69 61 2e 63 73 2e 75 6d   Host: ga ia.cs.um
0080  61 73 73 2e 65 64 75 0d  0a 55 73 65 72 2d 41 67   ass.edu· ·User-Ag
```

3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
   The hex value for the Frame type field is 0x0800. This corresponds to the IP protocol.

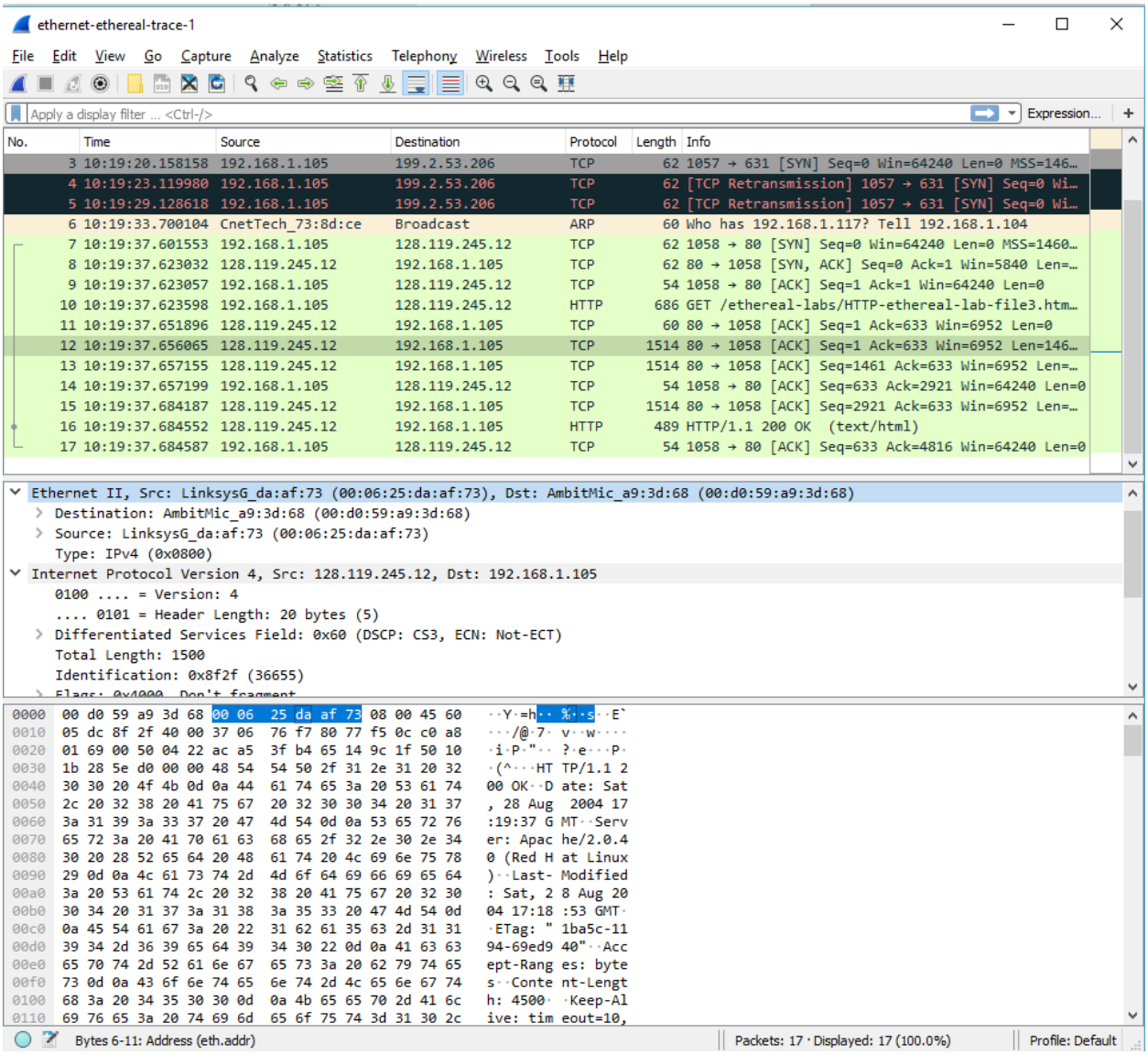
4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?
   After 432 bits or 54 bytes, the ‘G’ in get appears.

Hao (Jeff) Deng
ID: 932912420



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
This is again, the first hop router.

Hao (Jeff) Deng
ID: 932912420

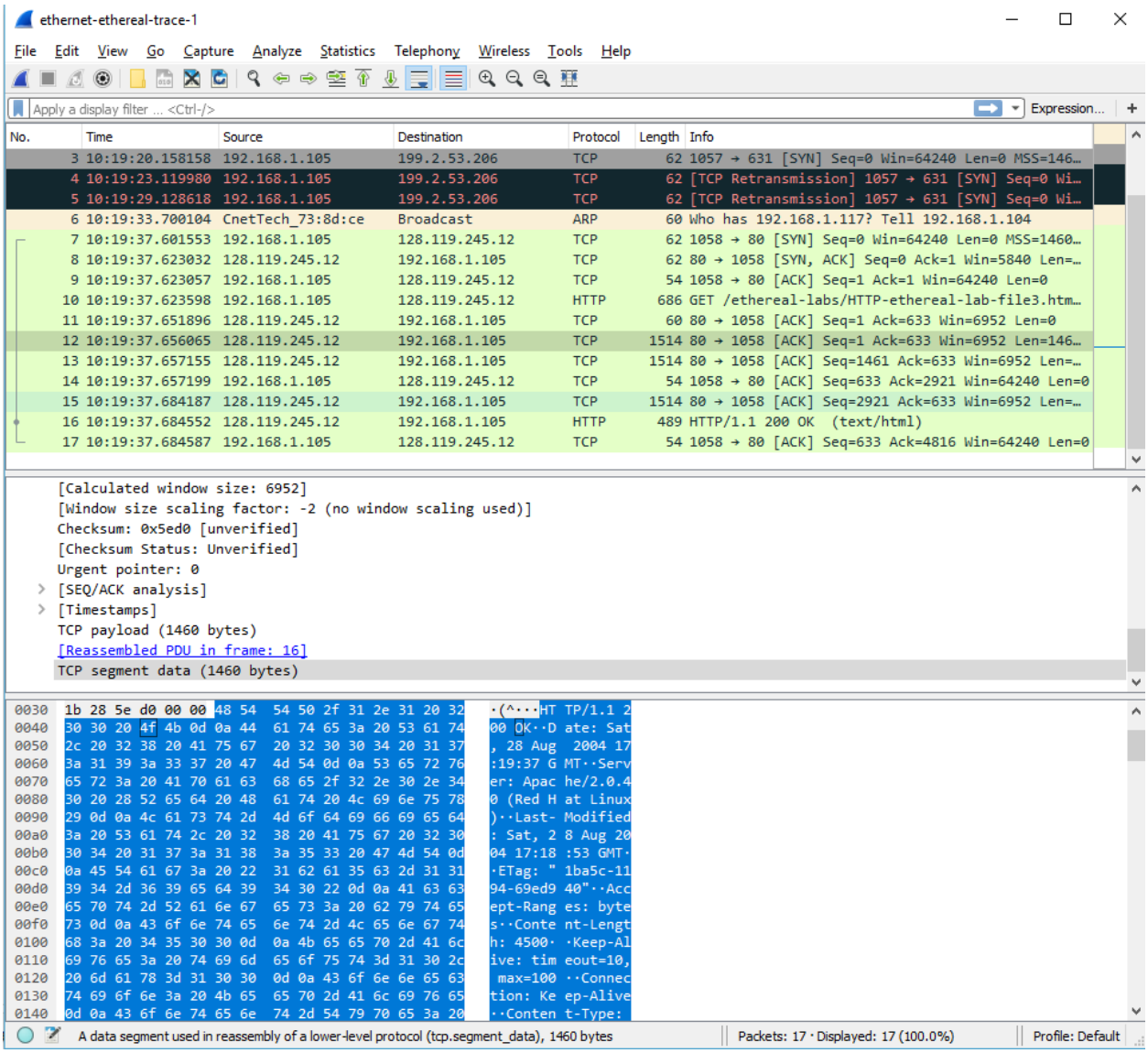


6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?
The destination address is 00:d0:59:a9:3d:68, and it is the Ethernet address of my computer.

7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
The hex value is 0x0800 and it corresponds to the IP protocol.

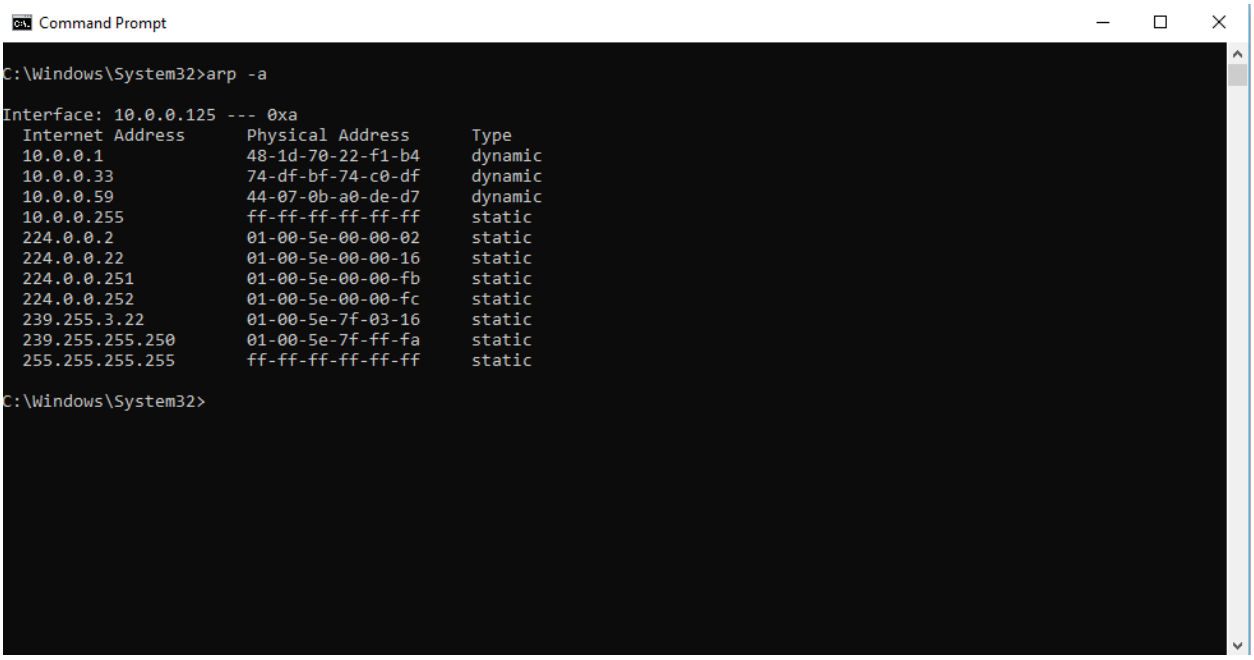
8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?
The “O” in “OK” appears from 64 bytes in.

Hao (Jeff) Deng
ID: 932912420



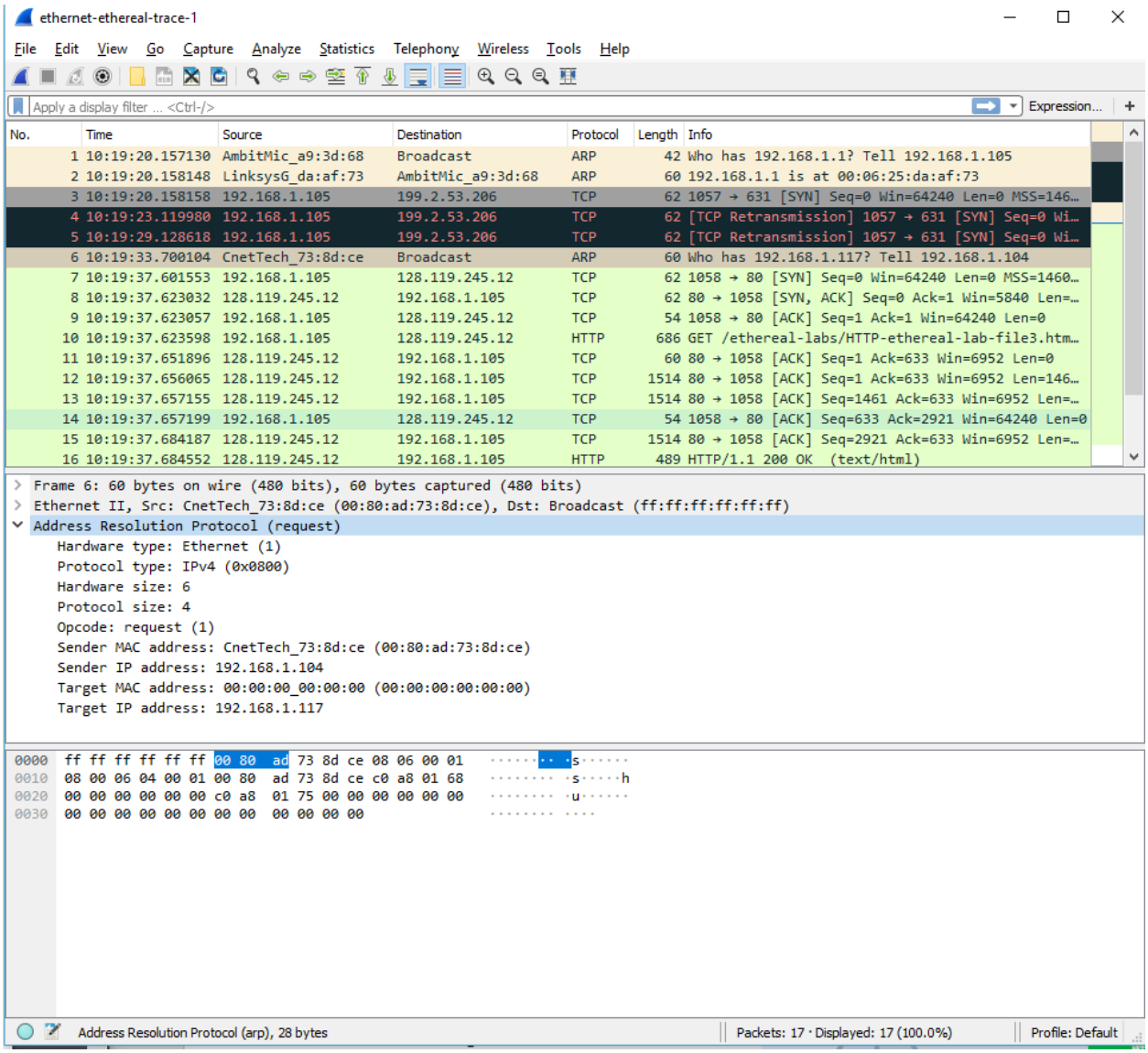
9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?
The internet address column contains the IP address, the physical address column contains the MAC address, and the type indicates the protocol type.

Hao (Jeff) Deng
ID: 932912420



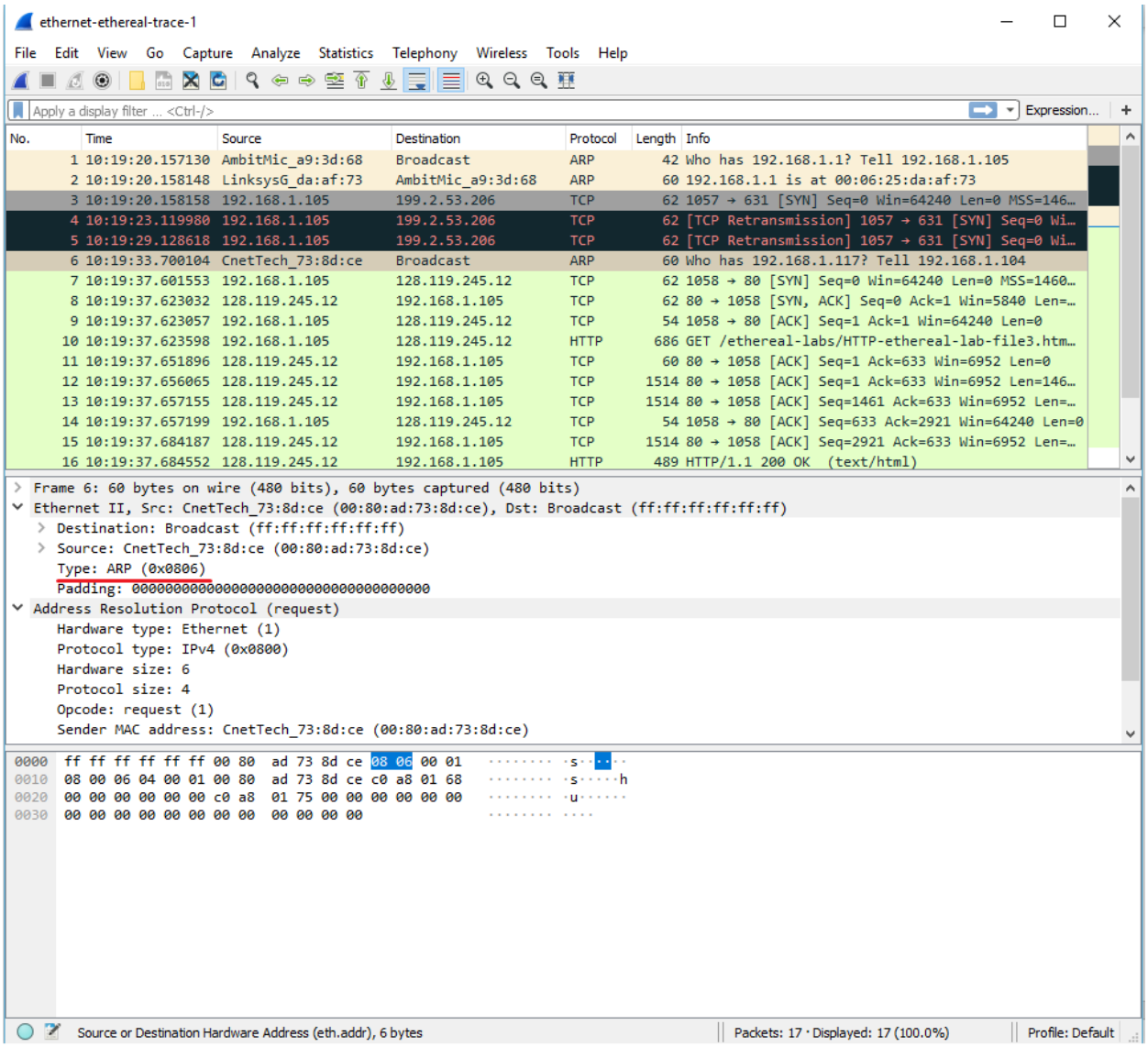
10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
The hex value for the source address is 00:80:ad:73:8d:ce. The hex value for the destination address is ff:ff:ff:ff:ff:ff, the broadcast address.

Hao (Jeff) Deng
ID: 932912420



11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?
The hex value for the Ethernet Frame type field is 0x0806, for ARP.

Hao (Jeff) Deng
ID: 932912420



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.

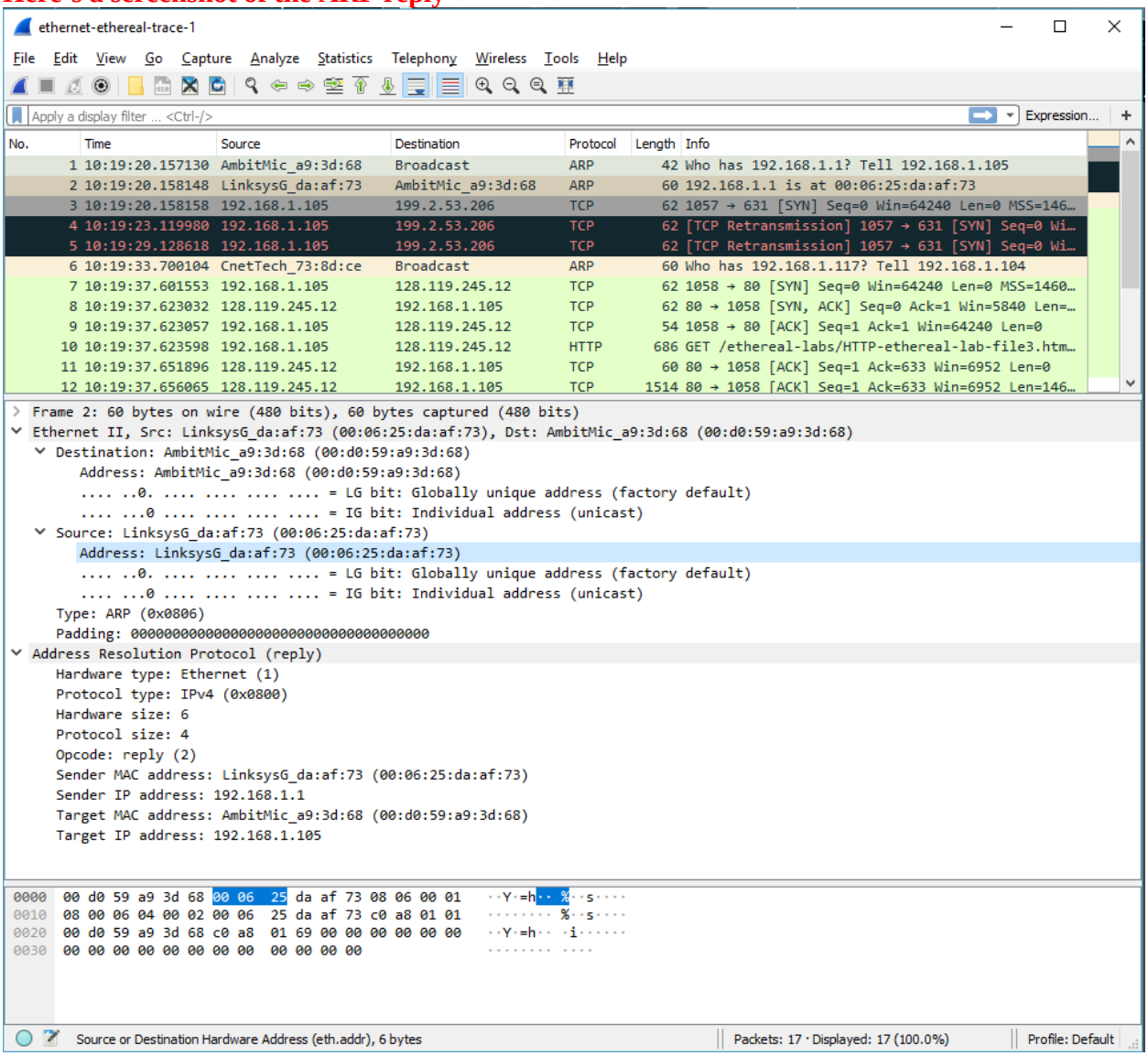
    a) How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?
    The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

    b) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?
    The hex value for opcode field within the ARP-payload of the request is 1 for the request.

    c) Does the ARP message contain the IP address of the sender?
    Yes, the ARP message containing the IP address 195.168.1.105 for 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?
In the "Target MAC address" field (destination) in the form of 00:00:00:00:00:00. Once the MAC address is resolved, this would be populated with the corresponding complete MAC address of the server or its relevant router.

13. Now find the ARP reply that was sent in response to the ARP request.
Here's a screenshot of the ARP reply



a) How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?
The ARP opcode field begins 20 bytes from the very beginning of the Ethernet frame.

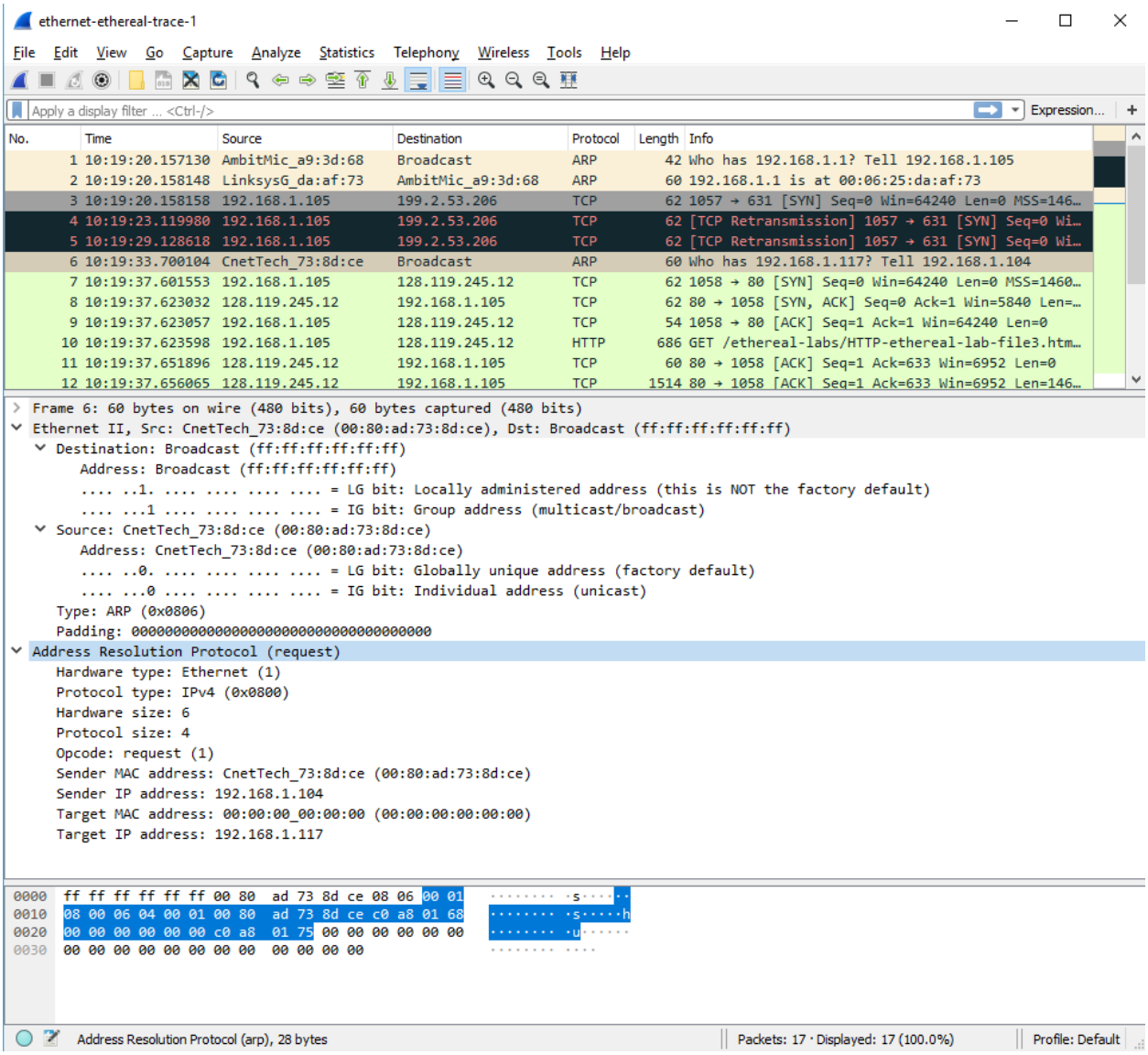
b) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?
The hex value for opcode field within the ARP-payload of the request is 2 for reply.

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?
The answer to the earlier ARP request appears in the "Sender MAC address" field, which contains the Ethernet address 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?
The hex value for the source address is 00:06:25:da:af:73 and for the destination is 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?
It is an IP address within the same subnet that the router has already mapped in its ARP table and does not need to be rediscovered and chronicled.

Hao (Jeff) Deng
ID: 932912420



Extra Credit

EX-1. The *arp* command:
arp -s InetAddr EtherAddr
allows you to manually add an entry to the ARP cache that resolves the IP address *InetAddr* to the physical address *EtherAddr*. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

The router/adapter would remove the IP address from the Ethernet frame and using ARP, once the router/adaptor received the destination IP address (even if we entered in the incorrect MAC address). It would get the correct MAC address of the destination.

Hao (Jeff) Deng
ID: 932912420

EX-2. What is the default amount of time that an entry remains in your ARP cache before being removed. You can determine this empirically (by monitoring the cache contents) or by looking this up in your operation system documentation. Indicate how/where you determined this value.

Since the default time to keep the ARP table entry is 20 minutes, the ARP table will refresh itself every 20 minutes. Though, the neighboring device can be out of the network so the ARP table should be updated according to the network states. When the table gets refreshed the content will get erased and when the chance comes to resolve the MAC address to the known IP address the ARP request will be sent in broadcast mode where the reply will be in Unicast mode.