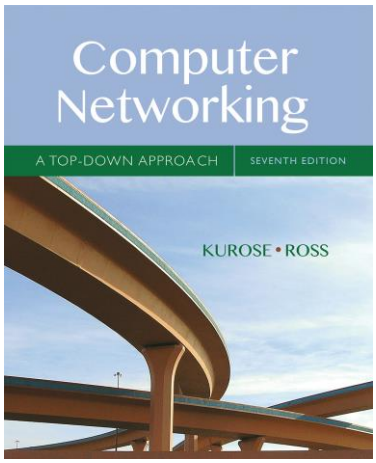
Name: Katie Schaumleffle

Wireshark Lab: Ethernet and ARP v7.0



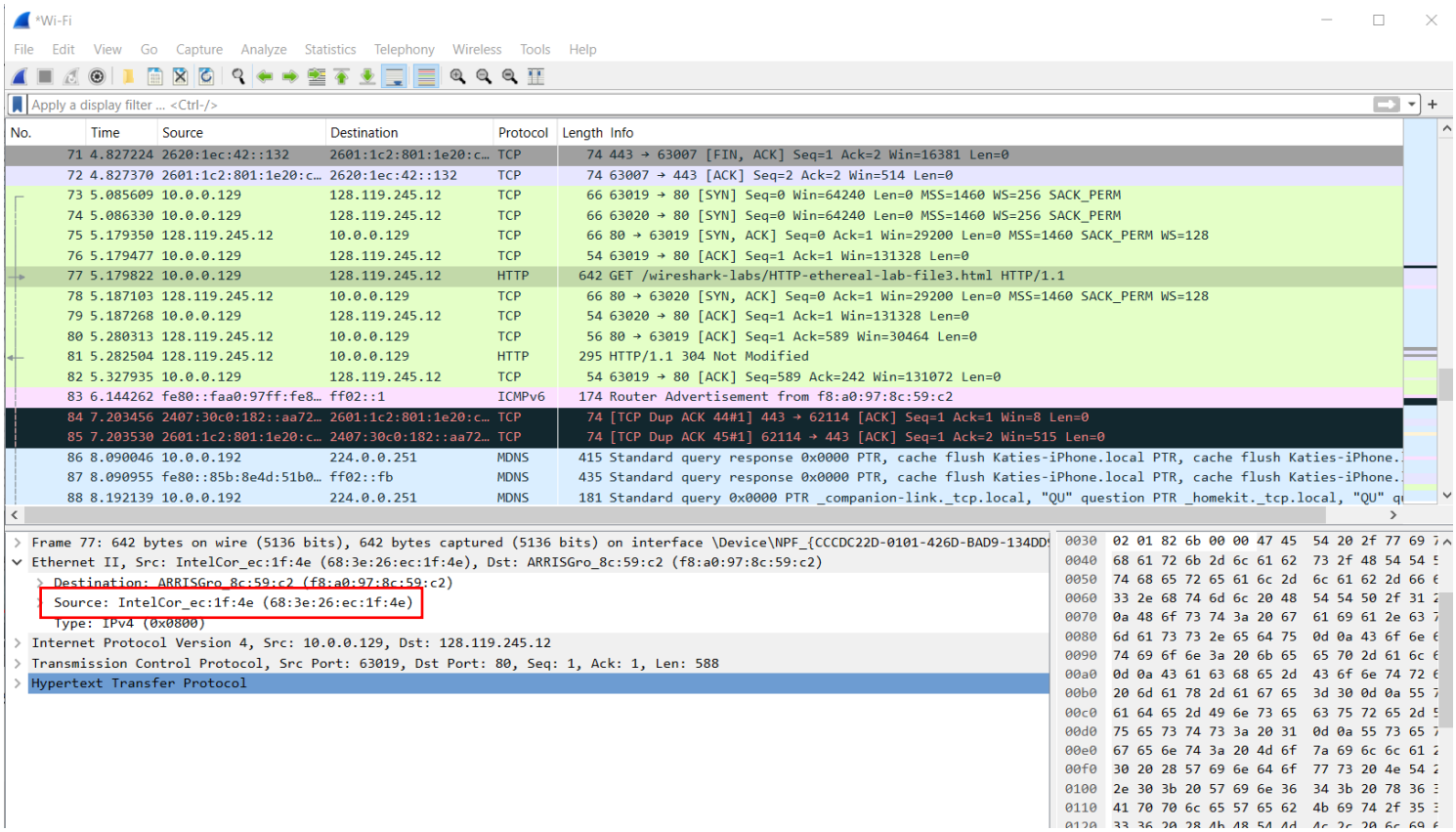
Supplement to *Computer Networking: A Top-Down Approach, 7th ed.*, J.F. Kurose and K.W. Ross

"Tell me and I forget. Show me and I remember. Involve me and I understand." Chinese proverb

---

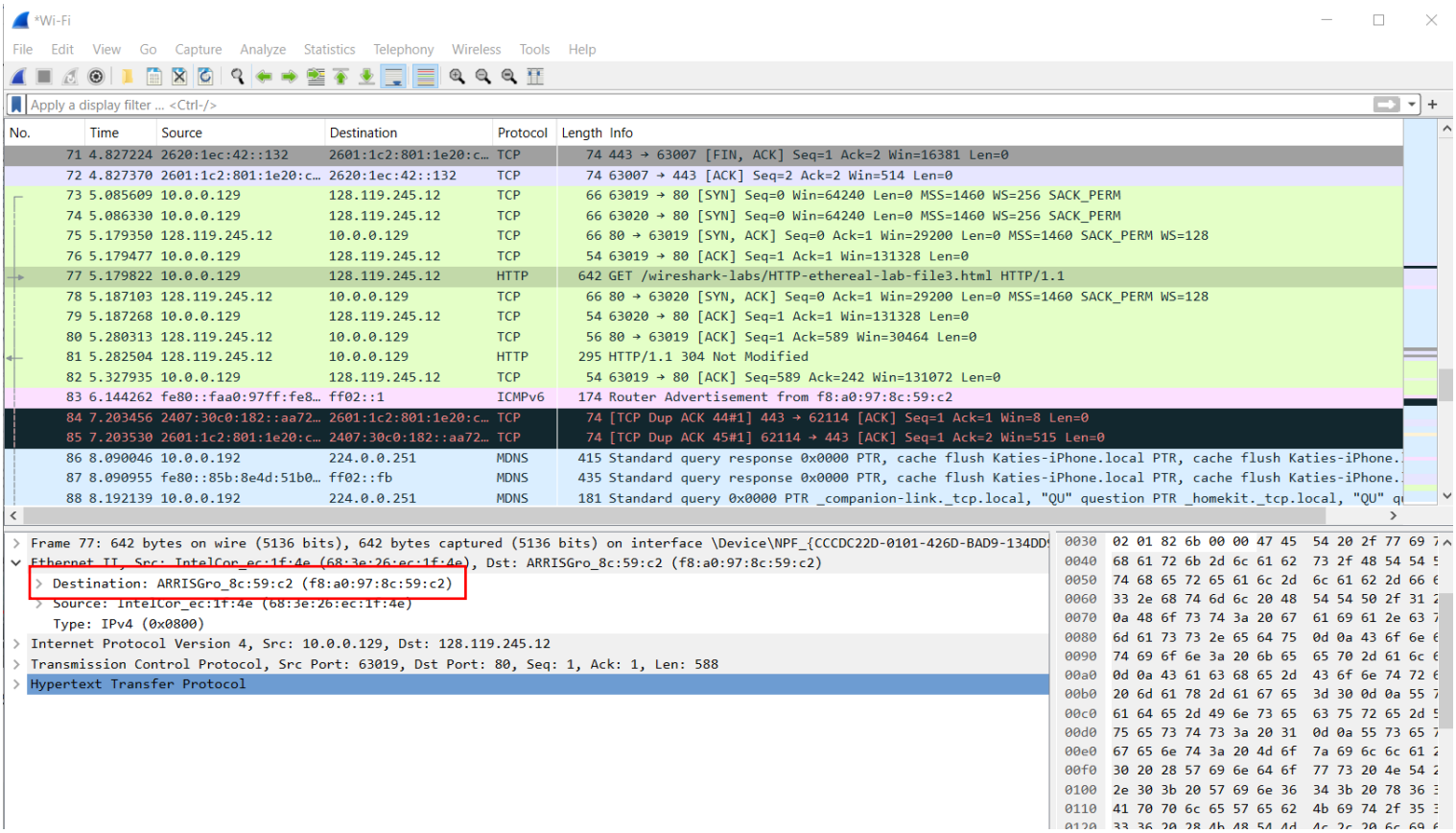
1. What is the 48-bit Ethernet address of your computer?

68:3e:26:ec:1f:4e

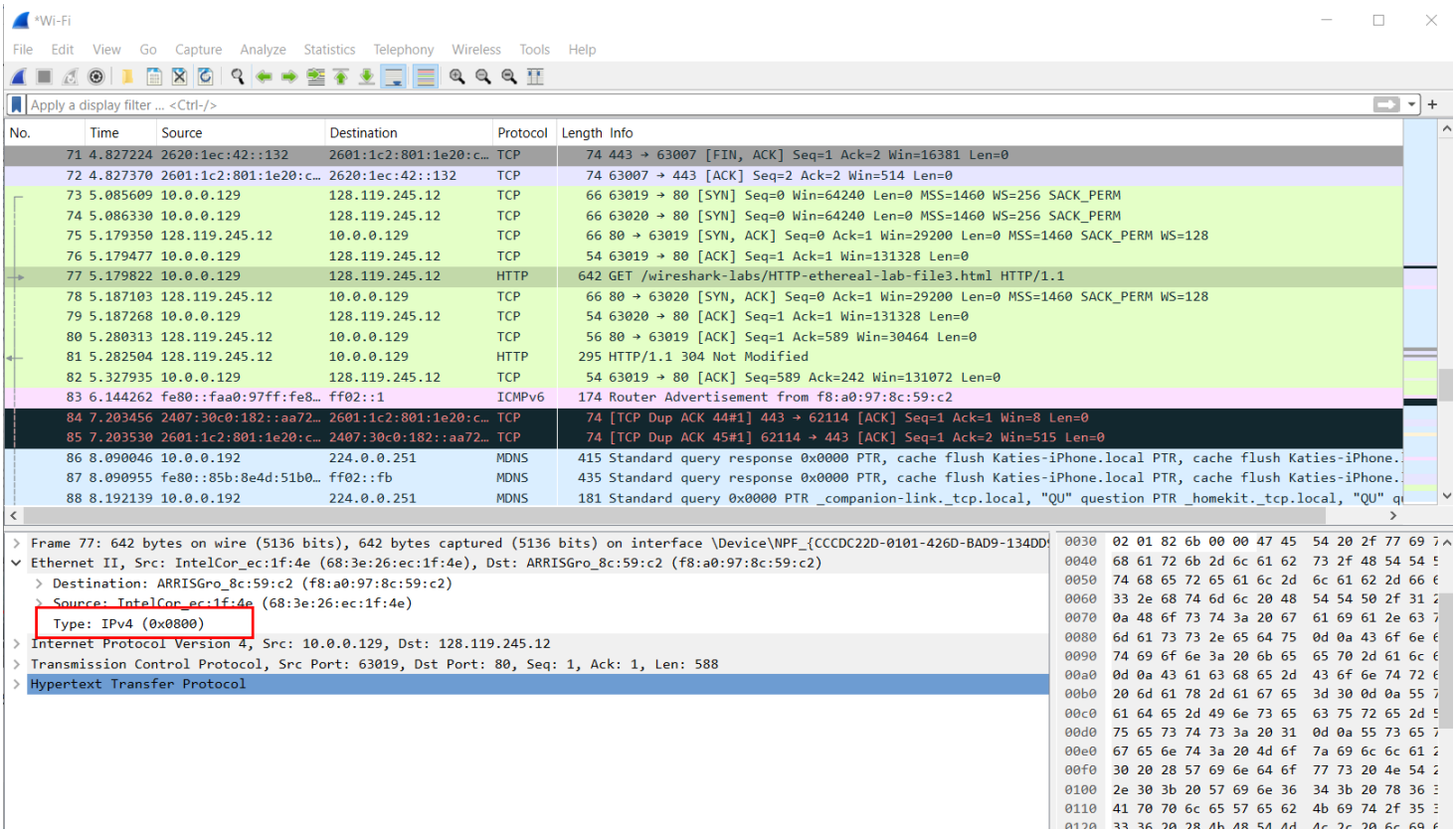


2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is *no*). What device has this as its

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: f8:a0:97:8c:59:c2
No, this is not the Ethernet address of gaia.cs.mass.edu. This is the address of my router at my house.

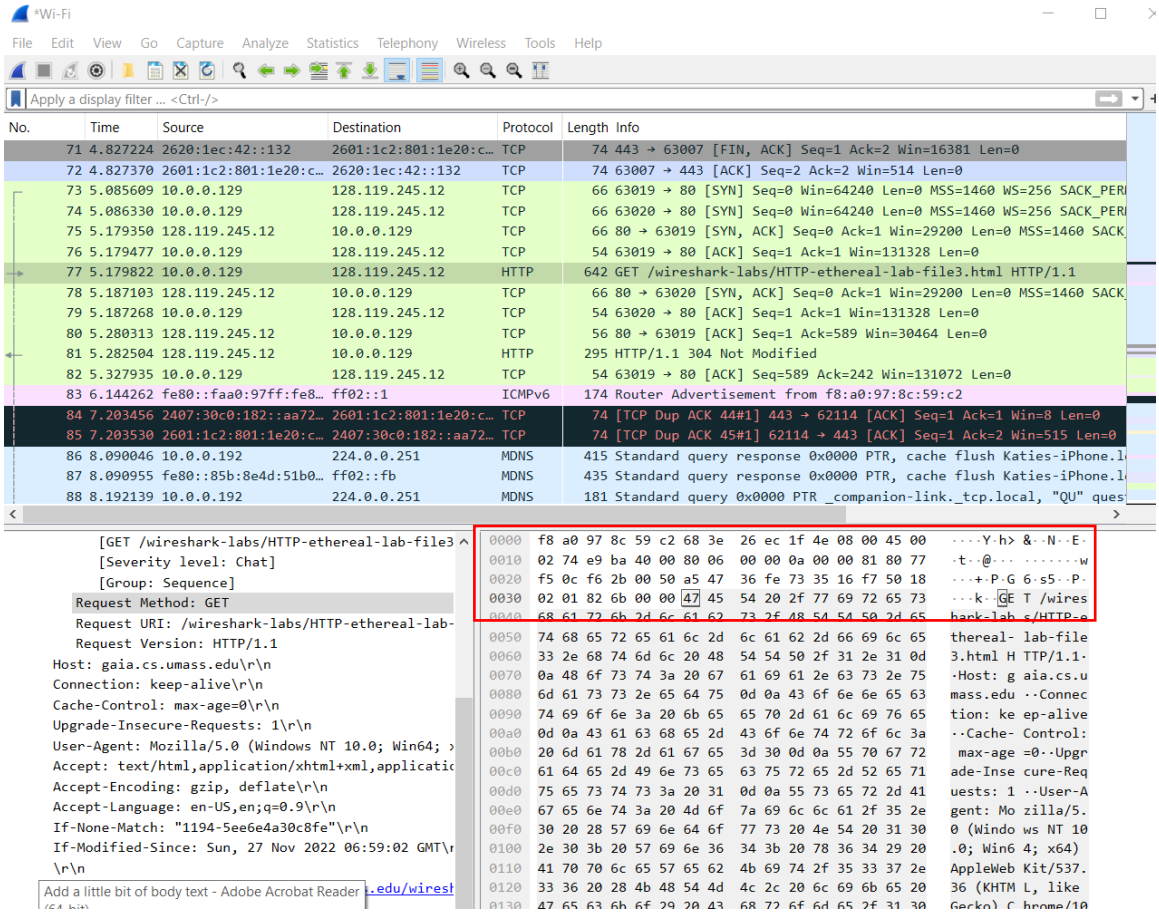


3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?
0x0800



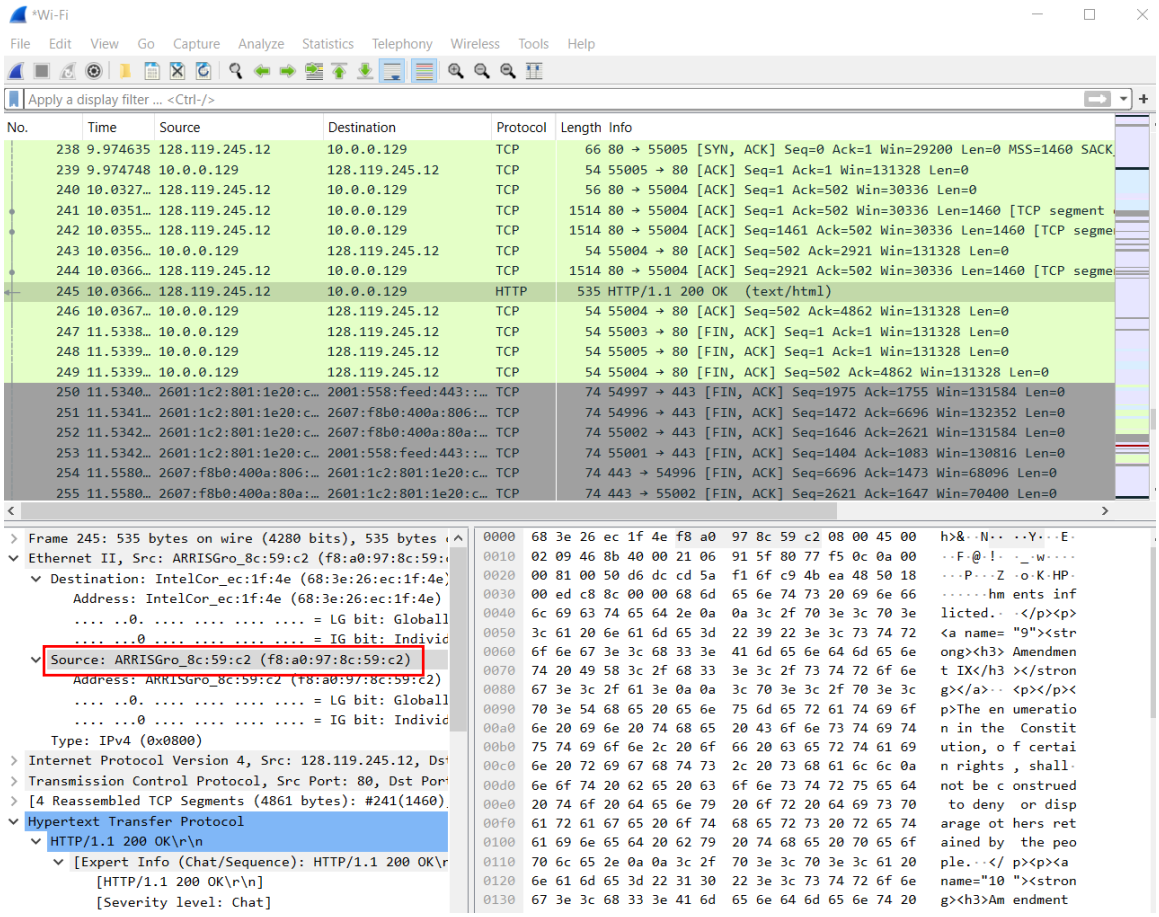
4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

The “G” in “GET” appears 54 bytes into the frame



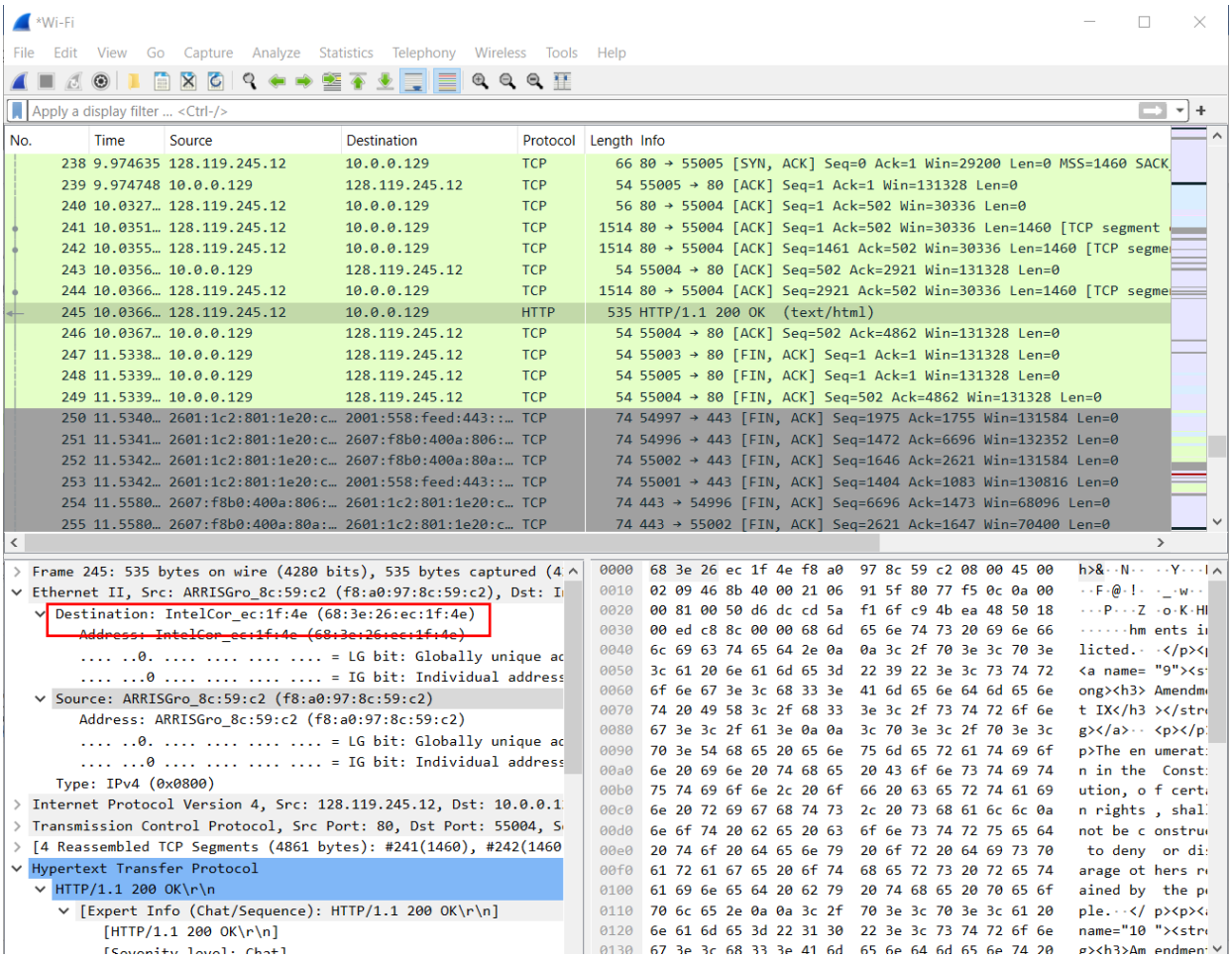
Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

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: f8:a0:97:8c:59:c2
   This is the address of my router and is coming back to my computer.



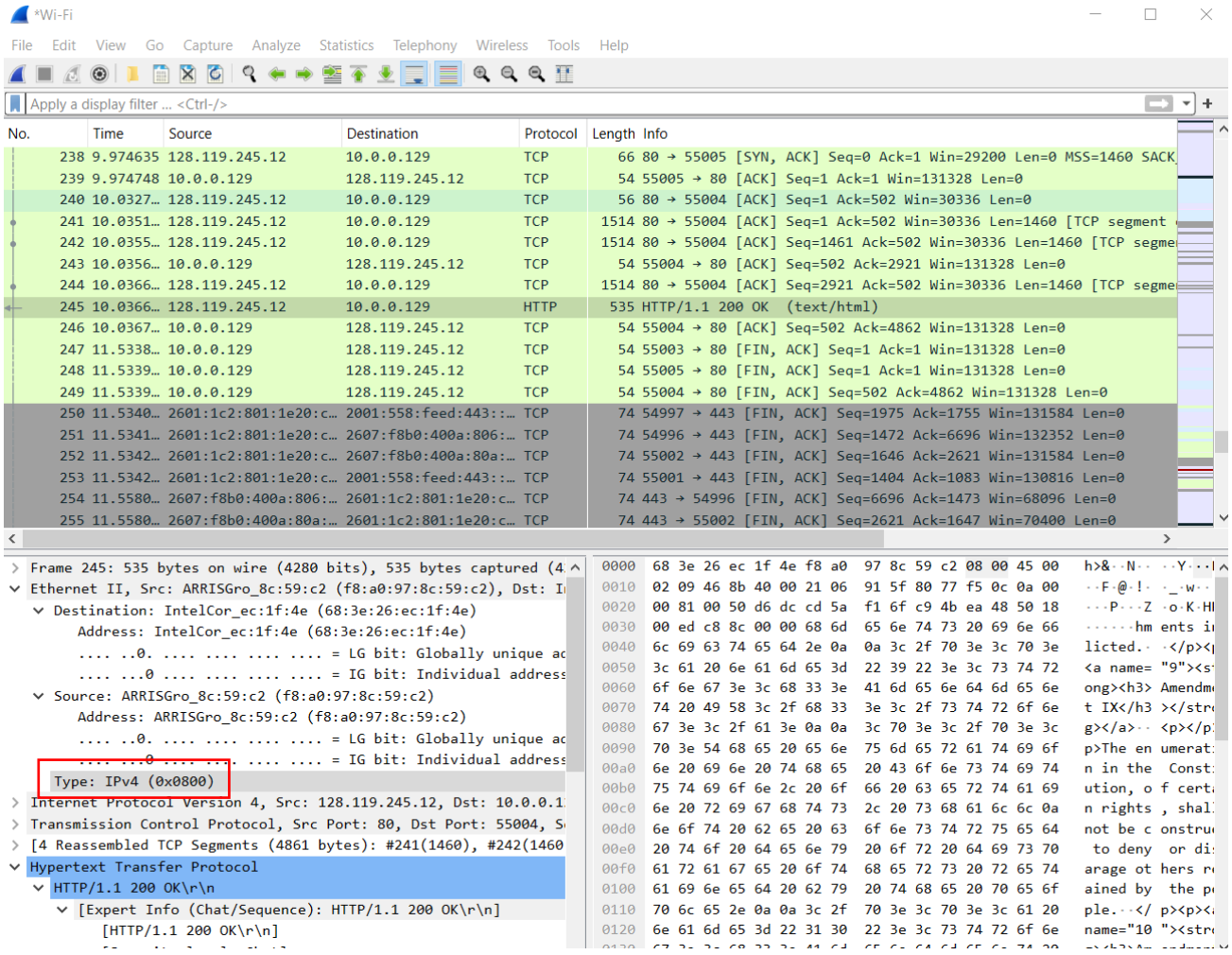
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

Yes, it's coming back to my computer. 68:3e:26:ec:1f:4e

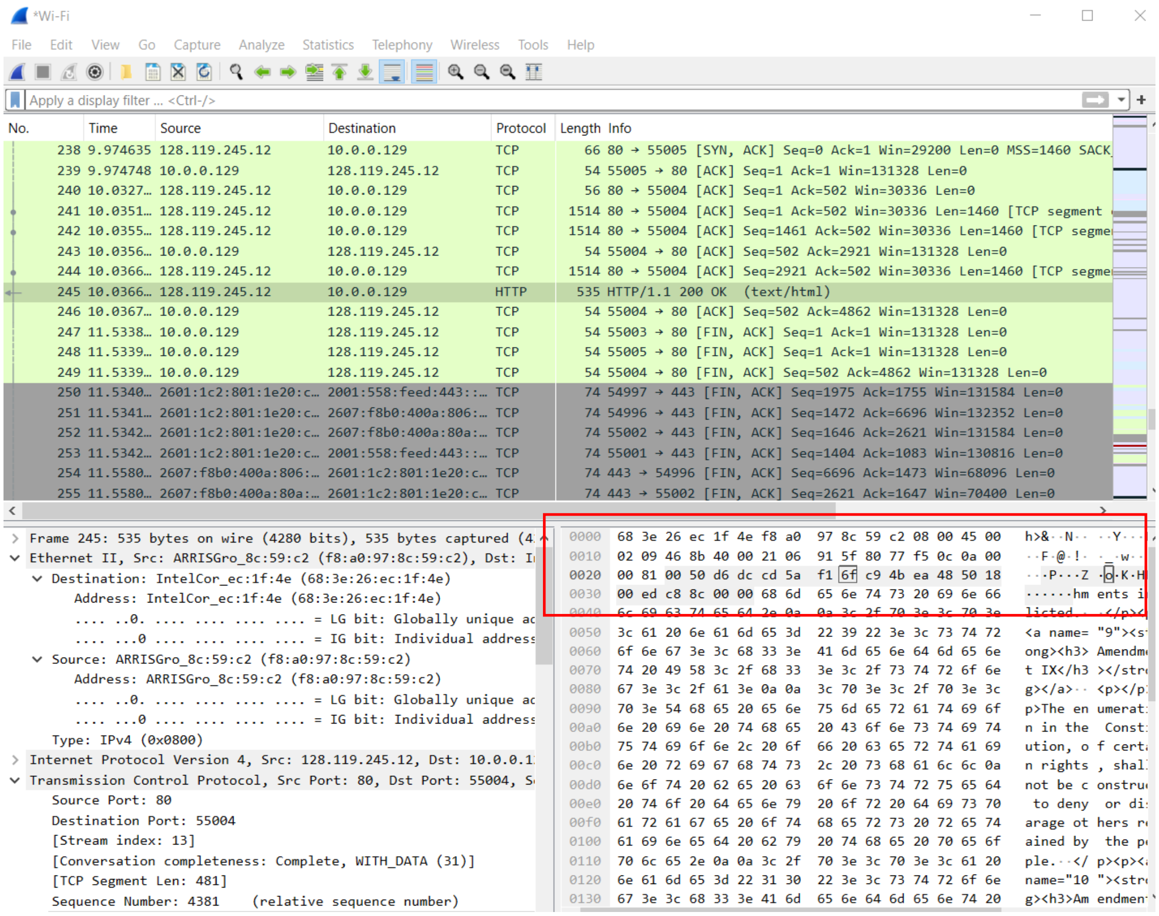


7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

   The Hex value is 0x0800, which 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?
42 bytes


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
238 9.974635 128.119.245.12 10.0.0.129 TCP 66 80 → 55005 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK
239 9.974748 10.0.0.129 128.119.245.12 TCP 54 55005 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
240 10.0327… 128.119.245.12 10.0.0.129 TCP 56 80 → 55004 [ACK] Seq=1 Ack=502 Win=30336 Len=0
241 10.0351… 128.119.245.12 10.0.0.129 TCP 1514 80 → 55004 [ACK] Seq=1 Ack=502 Win=30336 Len=1460 [TCP segment
242 10.0355… 128.119.245.12 10.0.0.129 TCP 1514 80 → 55004 [ACK] Seq=1461 Ack=502 Win=30336 Len=1460 [TCP segme
243 10.0356… 10.0.0.129 128.119.245.12 TCP 54 55004 → 80 [ACK] Seq=502 Ack=2921 Win=131328 Len=0
244 10.0366… 128.119.245.12 10.0.0.129 TCP 1514 80 → 55004 [ACK] Seq=2921 Ack=502 Win=30336 Len=1460 [TCP segme
245 10.0366… 128.119.245.12 10.0.0.129 HTTP 535 HTTP/1.1 200 OK (text/html)
246 10.0367… 10.0.0.129 128.119.245.12 TCP 54 55004 → 80 [ACK] Seq=502 Ack=4862 Win=131328 Len=0
247 11.5338… 10.0.0.129 128.119.245.12 TCP 54 55003 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
248 11.5339… 10.0.0.129 128.119.245.12 TCP 54 55005 → 80 [FIN, ACK] Seq=1 Ack=1 Win=131328 Len=0
249 11.5339… 10.0.0.129 128.119.245.12 TCP 54 55004 → 80 [FIN, ACK] Seq=502 Ack=4862 Win=131328 Len=0
250 11.5340… 2601:1c2:801:1e20:c… 2001:558:feed:443::… TCP 74 54997 → 443 [FIN, ACK] Seq=1975 Ack=1755 Win=131584 Len=0
251 11.5341… 2601:1c2:801:1e20:c… 2607:f8b0:400a:806:… TCP 74 54996 → 443 [FIN, ACK] Seq=1472 Ack=6696 Win=132352 Len=0
252 11.5342… 2601:1c2:801:1e20:c… 2607:f8b0:400a:80a:… TCP 74 55002 → 443 [FIN, ACK] Seq=1646 Ack=2621 Win=131584 Len=0
253 11.5342… 2601:1c2:801:1e20:c… 2001:558:feed:443::… TCP 74 55001 → 443 [FIN, ACK] Seq=1404 Ack=1083 Win=130816 Len=0
254 11.5580… 2607:f8b0:400a:806:… 2601:1c2:801:1e20:c… TCP 74 443 → 54996 [FIN, ACK] Seq=6696 Ack=1473 Win=68096 Len=0
255 11.5580… 2607:f8b0:400a:80a:… 2601:1c2:801:1e20:c… TCP 74 443 → 55002 [FIN, ACK] Seq=2621 Ack=1647 Win=70400 Len=0
Frame 245: 535 bytes on wire (4280 bits), 535 bytes captured (4
Ethernet II, Src: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2), Dst: I
Destination: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e)
Address: IntelCor_ec:1f:4e (68:3e:26:ec:1f:4e)
.... ..0. .... = LG bit: Globally unique ac
....0 .... = IG bit: Individual address
Source: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2)
Address: ARRISGro_8c:59:c2 (f8:a0:97:8c:59:c2)
.... ..0. .... = LG bit: Globally unique ac
....0 .... = IG bit: Individual address
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 10.0.0.1
Transmission Control Protocol, Src Port: 80, Dst Port: 55004, S
Source Port: 80
Destination Port: 55004
[Stream index: 13]
[Conversation completeness: Complete, WITH_DATA (31)]
[TCP Segment Len: 481]
Sequence Number: 4381 (relative sequence number)
0000 68 3e 26 ec 1f 4e f8 a0 97 8c 59 c2 08 00 45 00
0010 02 09 46 8b 40 00 21 06 91 5f 80 77 f5 0c 0a 00
0020 00 81 00 50 d6 dc cd 5a f1 6f c9 4b ea 48 50 18
0030 00 ed c8 8c 00 00 68 6d 65 6e 74 73 20 69 6e 66
0050 3c 61 20 6e 61 6d 65 3d 22 39 22 3e 3c 73 74 72
0060 6f 6e 67 3e 3c 68 33 3e 41 6d 65 6e 64 6d 65 6e
0070 74 20 49 58 3c 2f 68 33 3e 3c 2f 73 74 72 6f 6e
0080 67 3e 3c 2f 61 3e 0a 0a 3c 70 3e 3c 2f 70 3e 3c
0090 70 3e 54 68 65 20 65 6e 75 6d 65 72 61 74 69 6f
00a0 6e 20 69 6e 20 74 68 65 20 43 6f 6e 73 74 69 74
00b0 75 74 69 6f 6e 2c 20 6f 66 20 63 65 72 74 61 69
00c0 6e 20 72 69 67 68 74 73 2c 20 73 68 61 6c 6c 0a
00d0 6e 6f 74 20 62 65 20 63 6f 6e 73 74 72 75 65 64
00e0 20 74 6f 20 64 65 6e 79 20 6f 72 20 64 69 73 70
00f0 61 72 61 67 65 20 6f 74 68 65 72 73 20 72 65 74
0100 61 69 6e 65 64 20 62 79 20 74 68 65 20 70 65 6f
0110 70 6c 65 2e 0a 0a 3c 2f 70 3e 3c 70 3e 3c 61 20
0120 6e 61 6d 65 3d 22 31 30 22 3e 3c 73 74 72 6f 6e
0130 67 3e 3c 68 33 3e 41 6d 65 6e 64 6d 65 6e 74 20

2. The Address Resolution Protocol

9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?
   IP address; Physical (MAC) address; The type of ARP entry (dynamic or static)

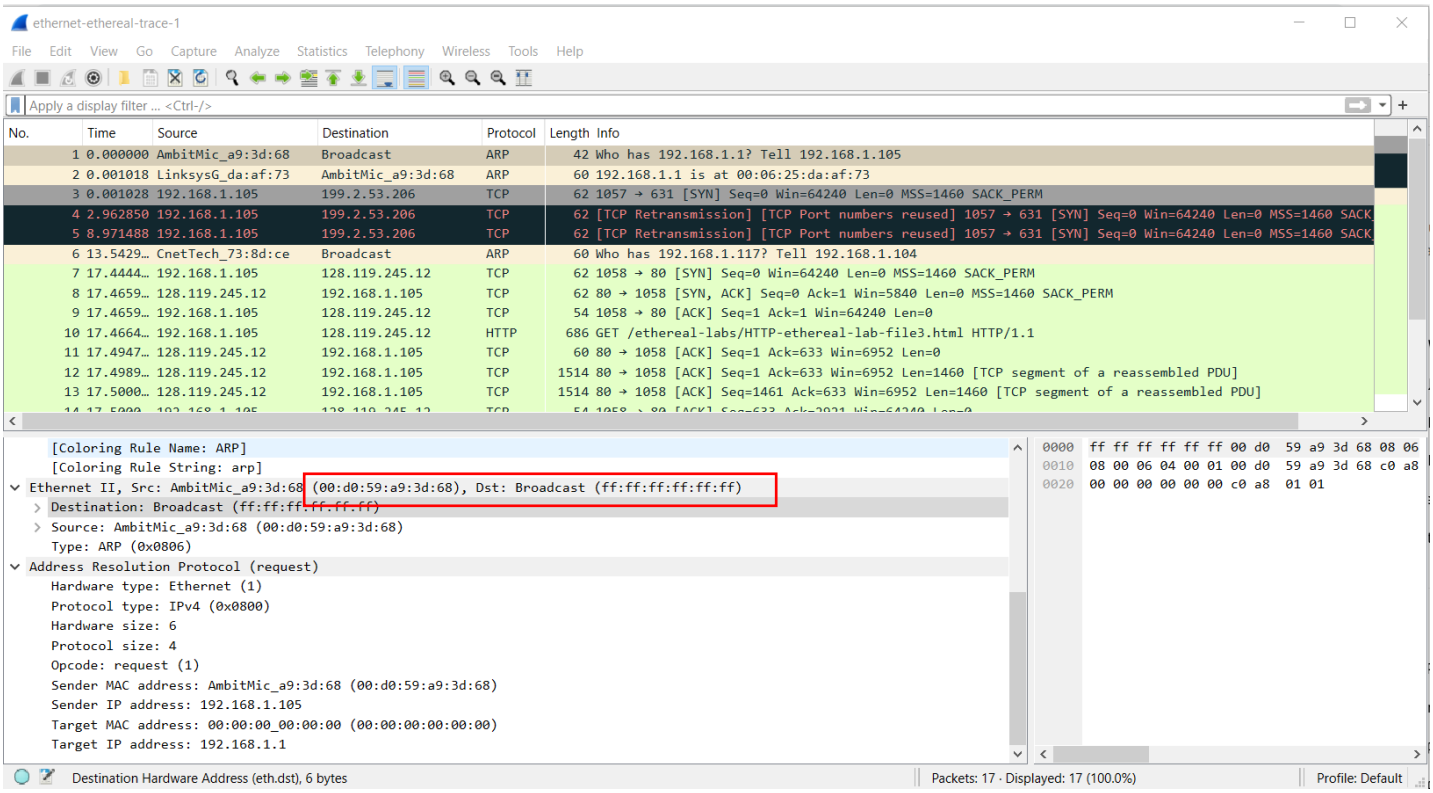
```
PS C:\windows\System32> .\arp -a

Interface: 10.0.0.129 --- 0xd
  Internet Address      Physical Address      Type
  10.0.0.1              f8-a0-97-8c-59-c2     dynamic
  10.0.0.225            f0-46-3b-13-72-27     dynamic
  10.0.0.255            ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     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

Interface: 172.21.192.1 --- 0x2f
  Internet Address      Physical Address      Type
  172.21.193.82         00-15-5d-b3-08-21     dynamic
  172.21.207.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
PS C:\windows\System32>
```

Observing ARP in action

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

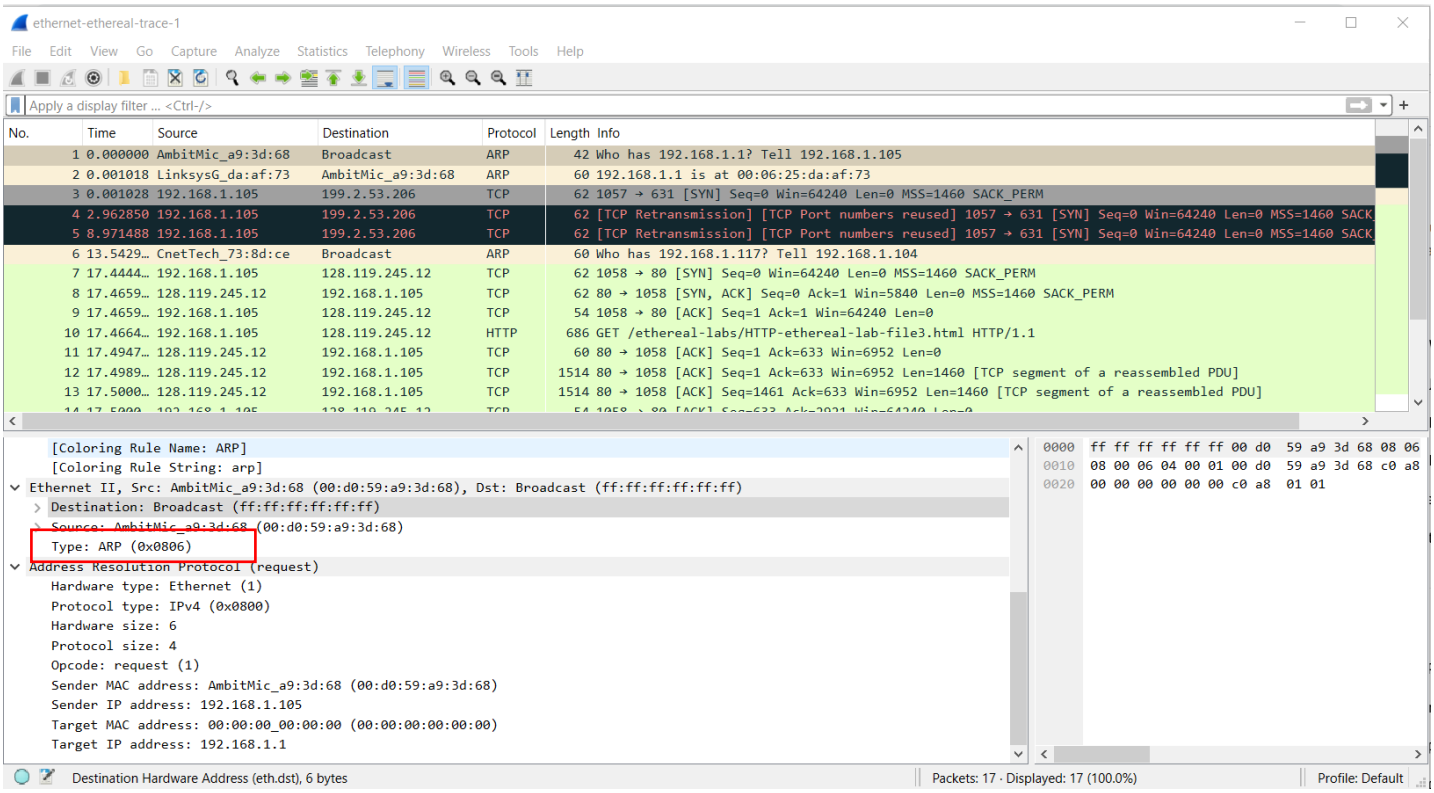
    Destination: ff:ff:ff:ff:ff:ff

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

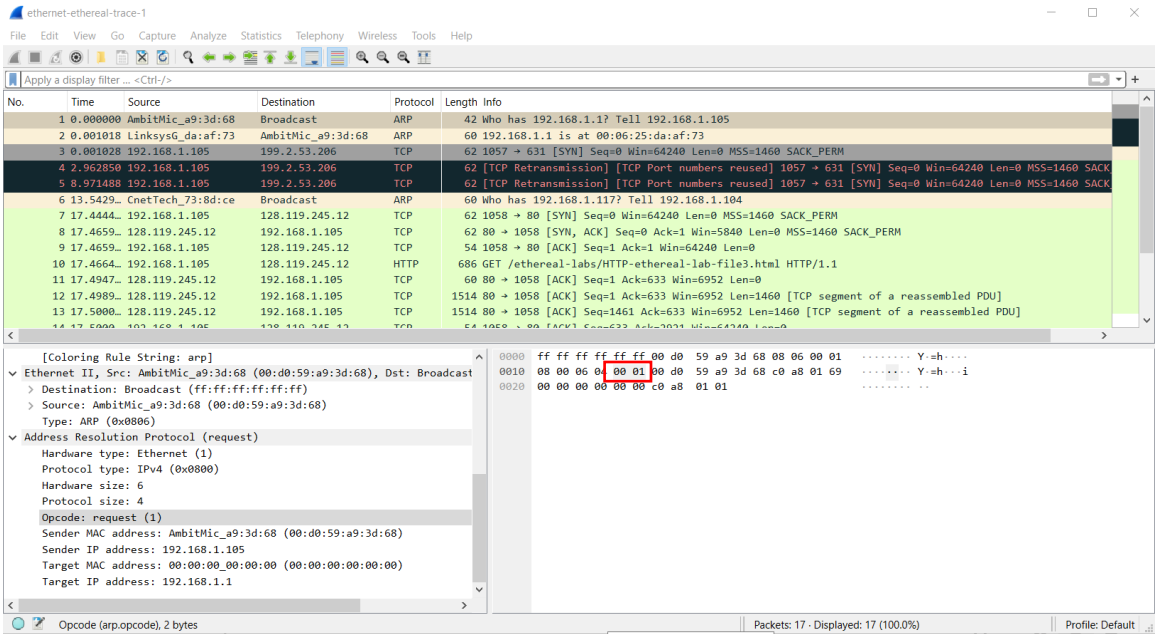


11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

0x0806. The upper layer protocol is ARP

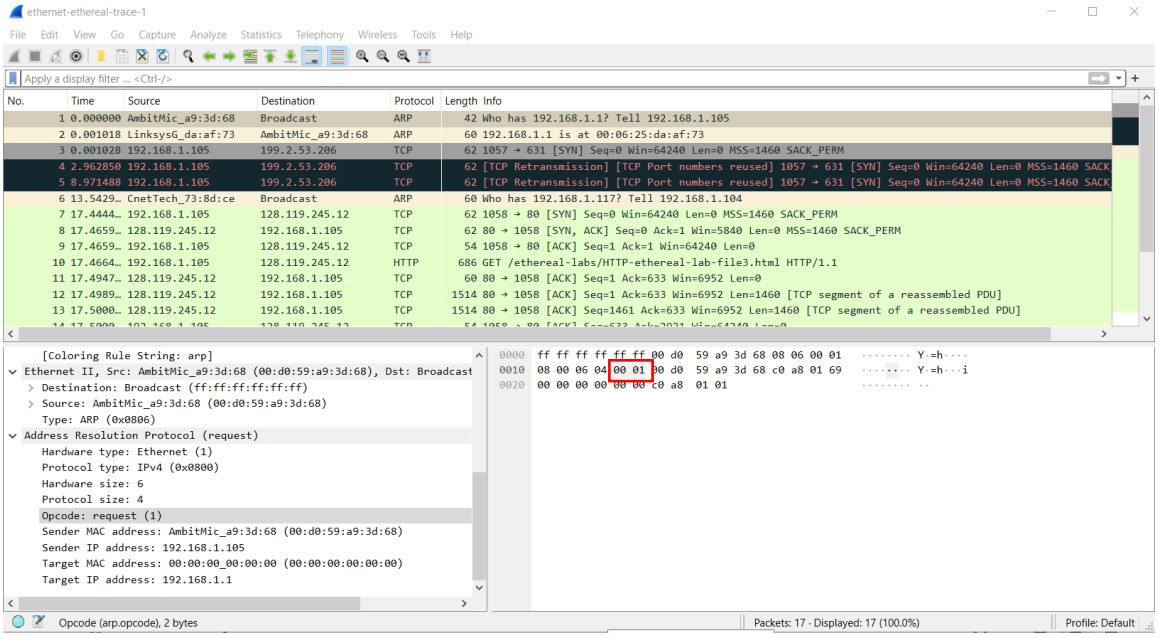


12. Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.
    a) How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?
    20 bytes



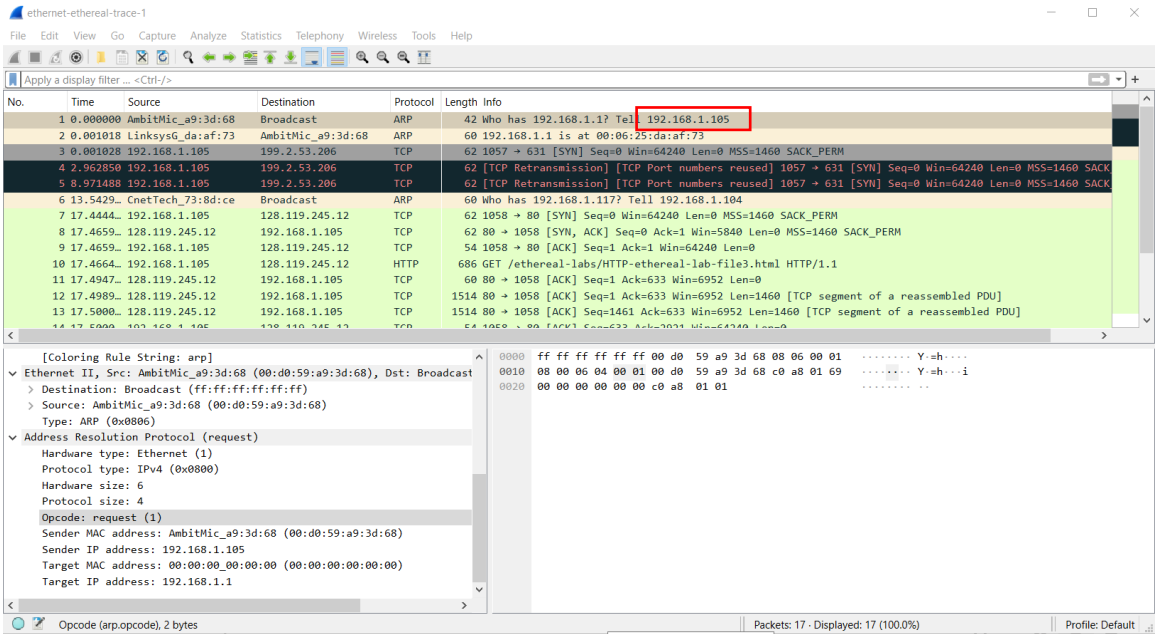
b) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

0x0001

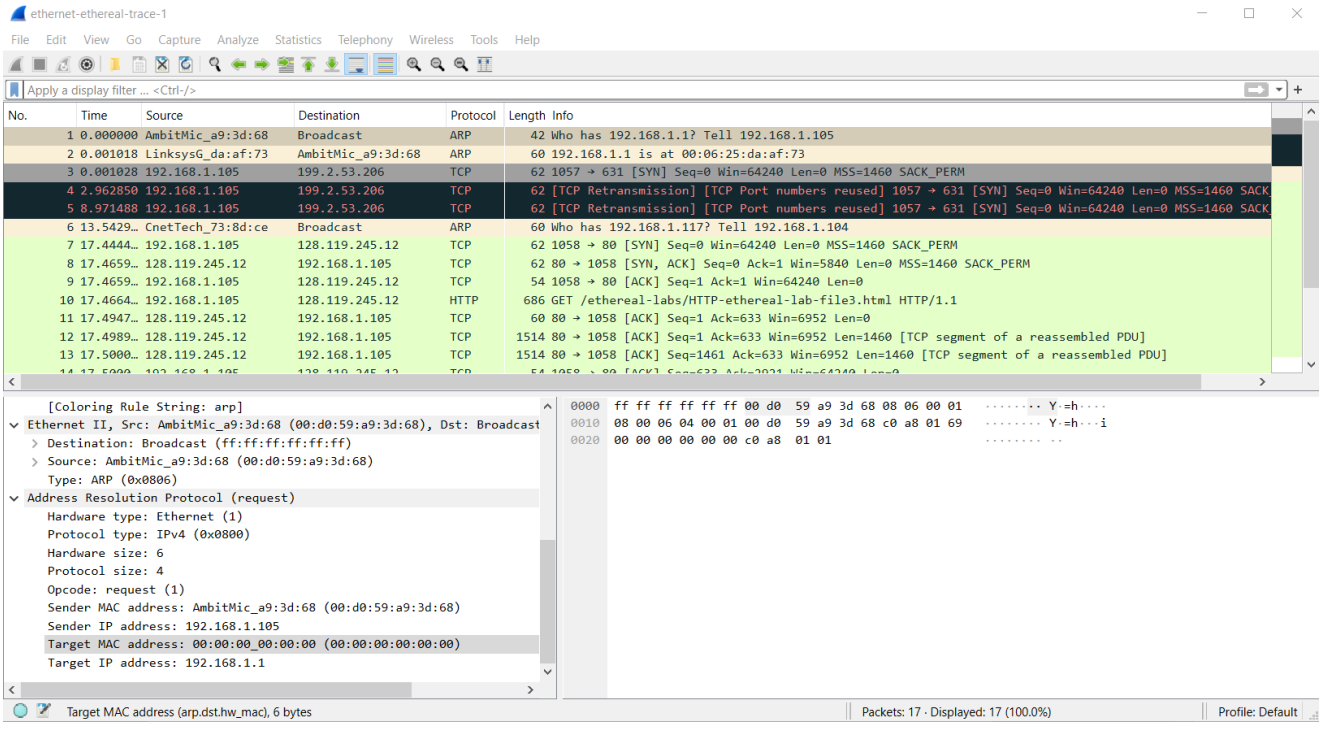


c) Does the ARP message contain the IP address of the sender?

Yes, it's 192.168.1.105



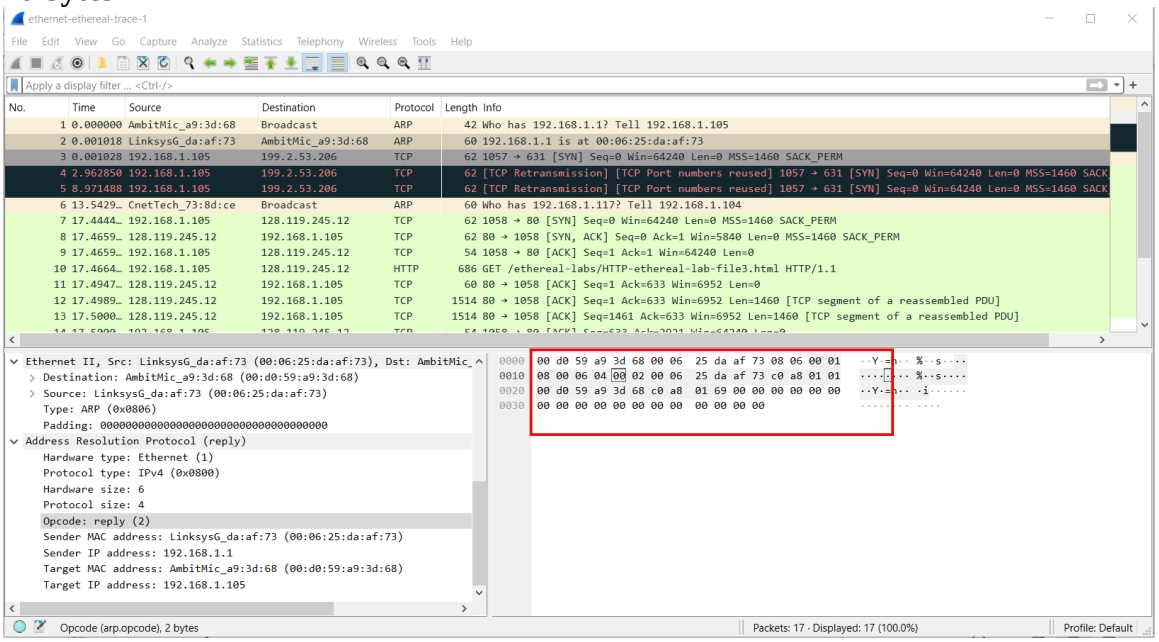
d) Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?
The target MAC address (00:00:00:00:00:00) queries the machine whose IP address is 192.168.1.105



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

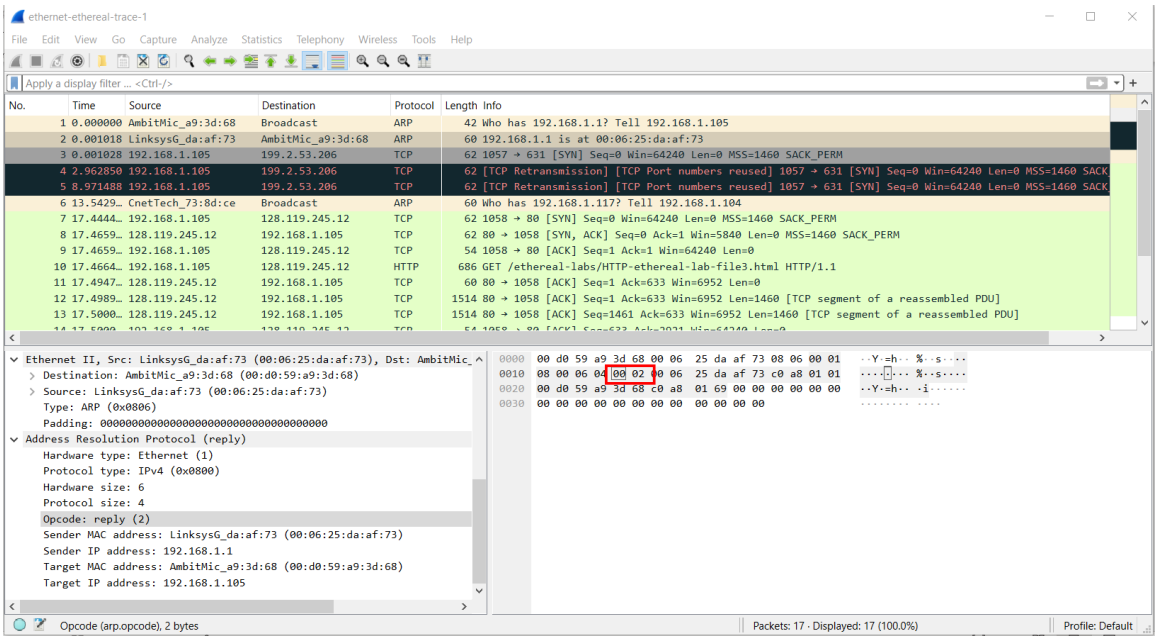
a) How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

20 bytes



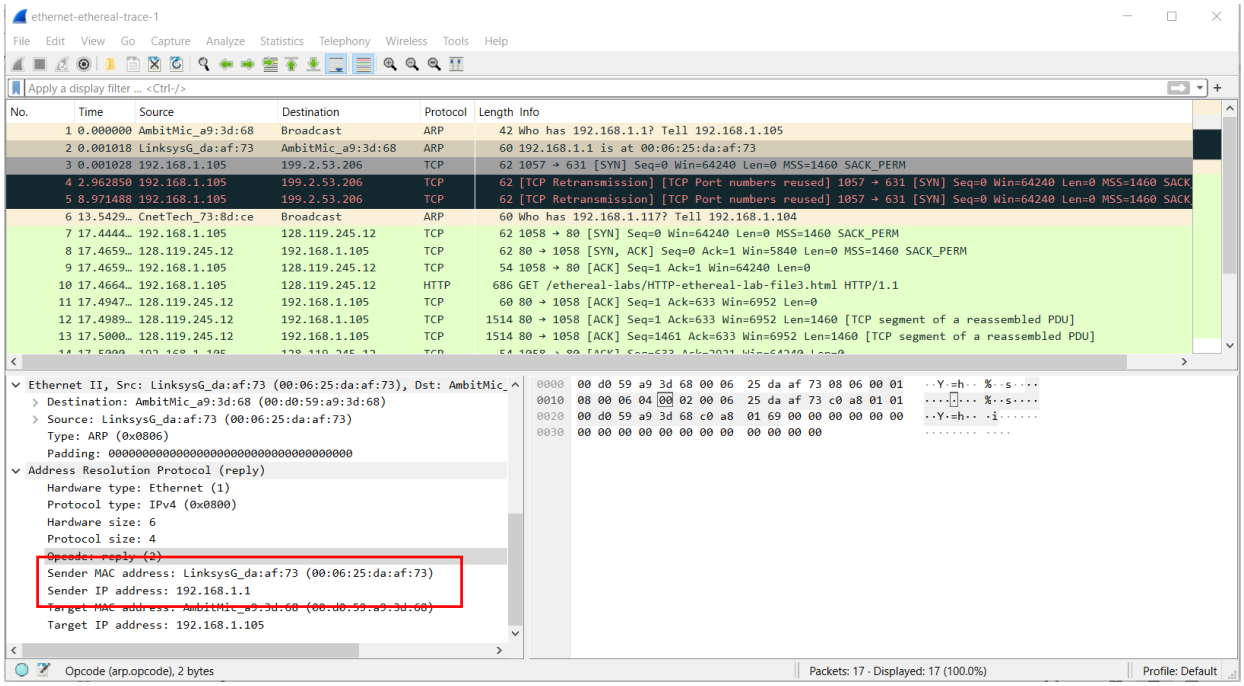
b) What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

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?

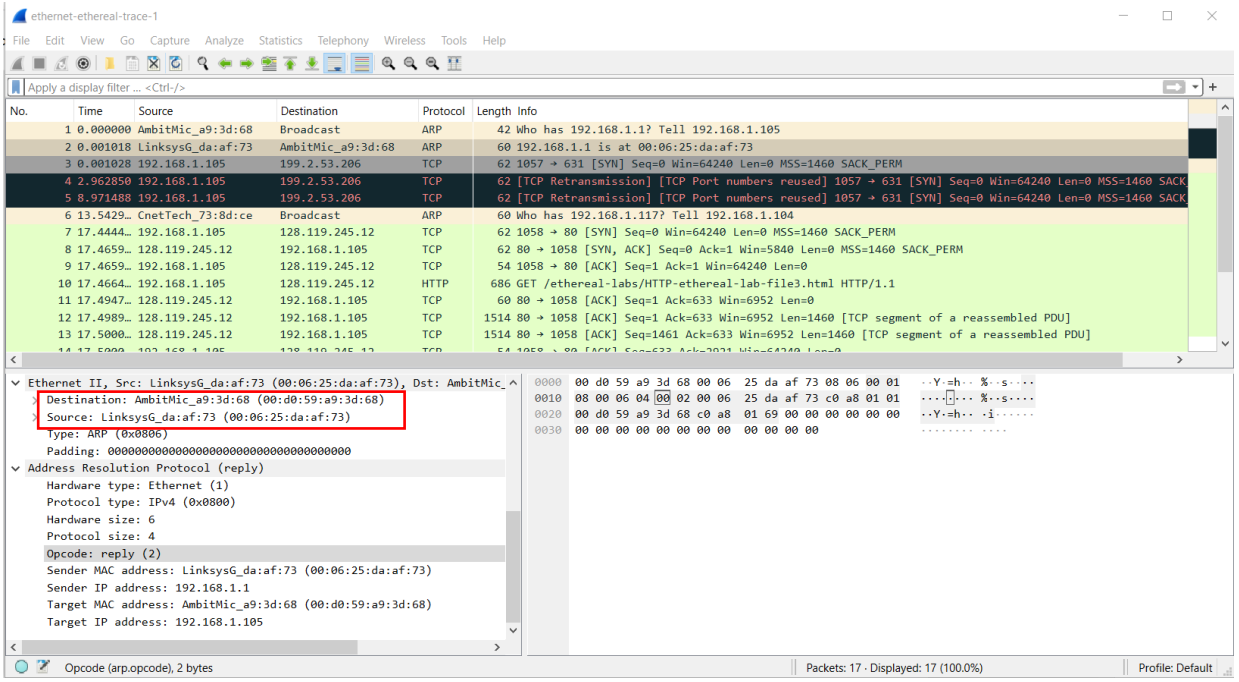
The sender IP address: 192.168.1.1 and Sender MAC address: 00:06:25:da:af:73 “answers” the earlier ARP request.



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

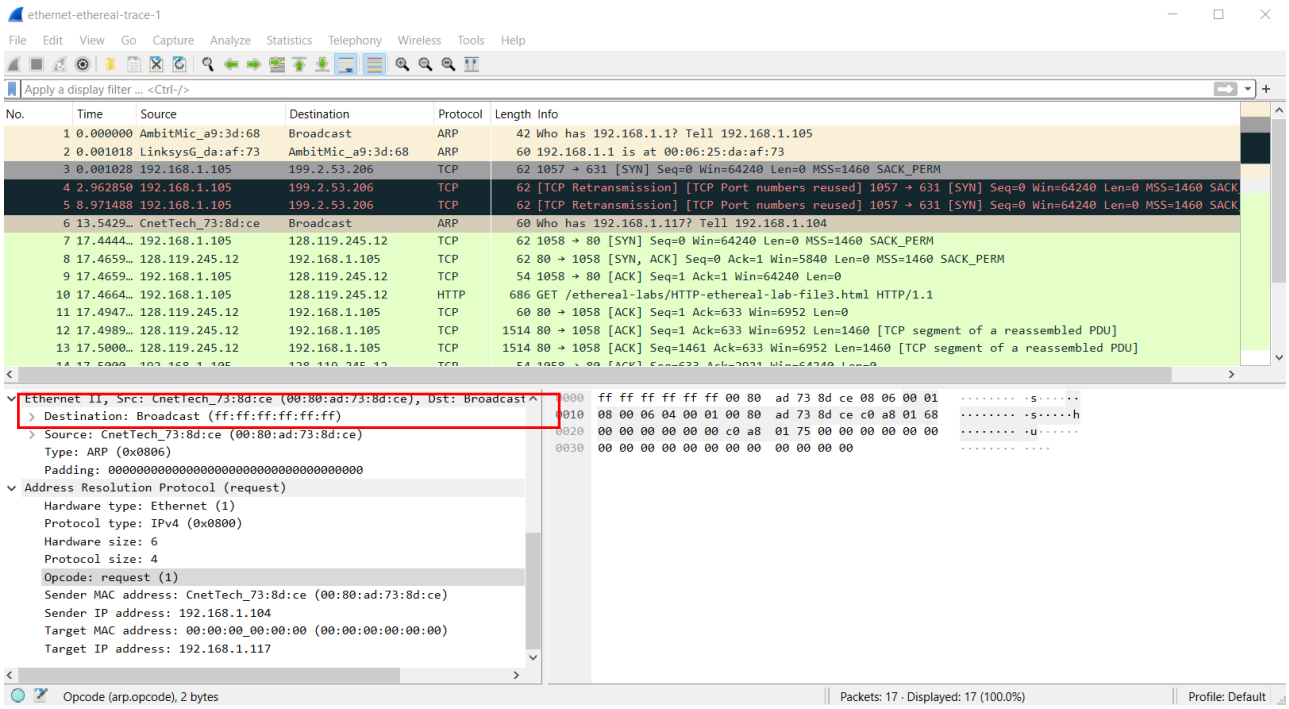
Source: 00:06:25:da:af:73

Destination: 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?

    There isn't an ARP reply in the packet trace because the ARP request is broadcast, and the ARP reply is not broadcast. The reply will be sent to the computer who made the request directly.



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?

It will actually be ok, because when it contacts the router, the router will use ARP which will get back the correct address.

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.

20,500 ms

I found this by going to my command line, and finding the system32 directory. Then typing ".\netsh interface ipv4 show interfaces" This showed that interface #13 was my wifi, so then I typed ".\netsh interface ipv4 show interface 13" which gave me the following information, including the "Reachable Time" which gives me the amount of time that an entry remains in my ARP cache.

```
PS C:\windows\System32> .\netsh interface ipv4 show interface 13

Interface Wi-Fi Parameters
----------------------------------------------
IfLuid                             : wireless_32768
IfIndex                            : 13
State                              : connected
Metric                             : 45
Link MTU                           : 1500 bytes
Reachable Time                     : 20500 ms
Base Reachable Time                : 30000 ms
Retransmission Interval            : 1000 ms
DAD Transmits                      : 3
Site Prefix Length                 : 64
Site Id                            : 1
Forwarding                         : disabled
Advertising                        : disabled
Neighbor Discovery                 : enabled
Neighbor Unreachability Detection  : enabled
Router Discovery                   : dhcp
Managed Address Configuration      : enabled
Other Stateful Configuration       : enabled
Weak Host Sends                    : disabled
Weak Host Receives                 : disabled
Use Automatic Metric               : enabled
Ignore Default Routes              : disabled
Advertised Router Lifetime         : 1800 seconds
Advertise Default Route            : disabled
Current Hop Limit                  : 0
Force ARPND Wake up patterns       : disabled
Directed MAC Wake up patterns      : disabled
ECN capability                     : application
```