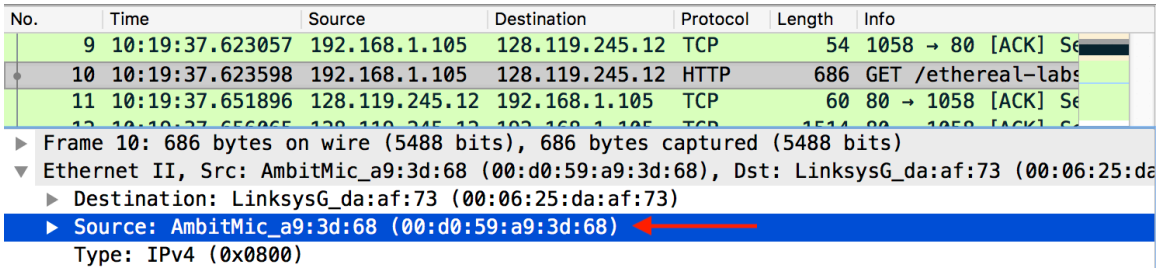
Class: CS-372
Term: Fall 2017
Author: Jon-Eric Cook
Date: December 3, 2017
Lab: #5

NOTE:
I was unable to run Wireshark live on my computer. Due to this, I downloaded the provided zip file and used the ***ethernet—etherreal-trace-1*** file to answer the questions of this lab.

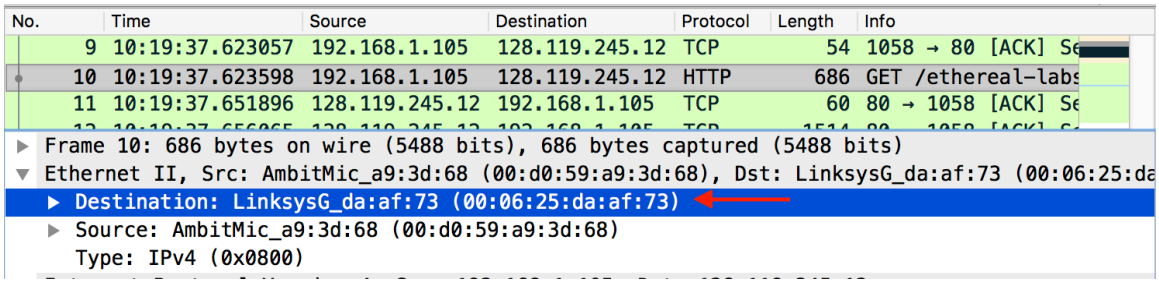
1) What is the 48-bit Ethernet address of your computer?

Answer:
00:d0:59:a9:3d:68
See screenshot below.



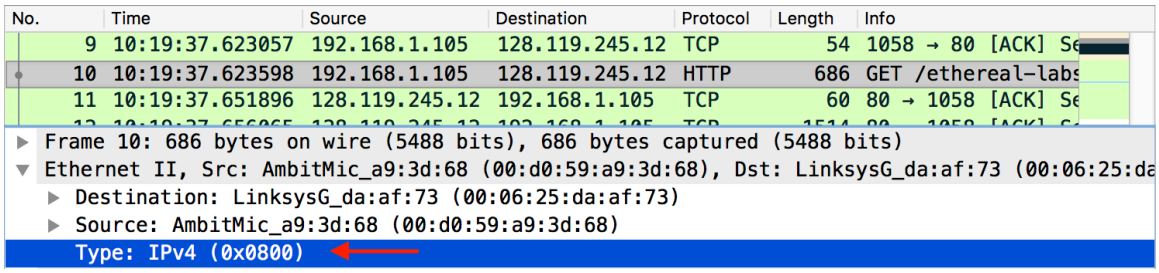
2) What is the 48-bit destination address in the Ethernet fame? Is this the Ethernet address of gaia.cs.umass.edu? What device has this as its Ethernet address?

Answer:
00:06:25:da:af:73
No
It is the Mac address for my router or internet gateway address.
See screenshot below.



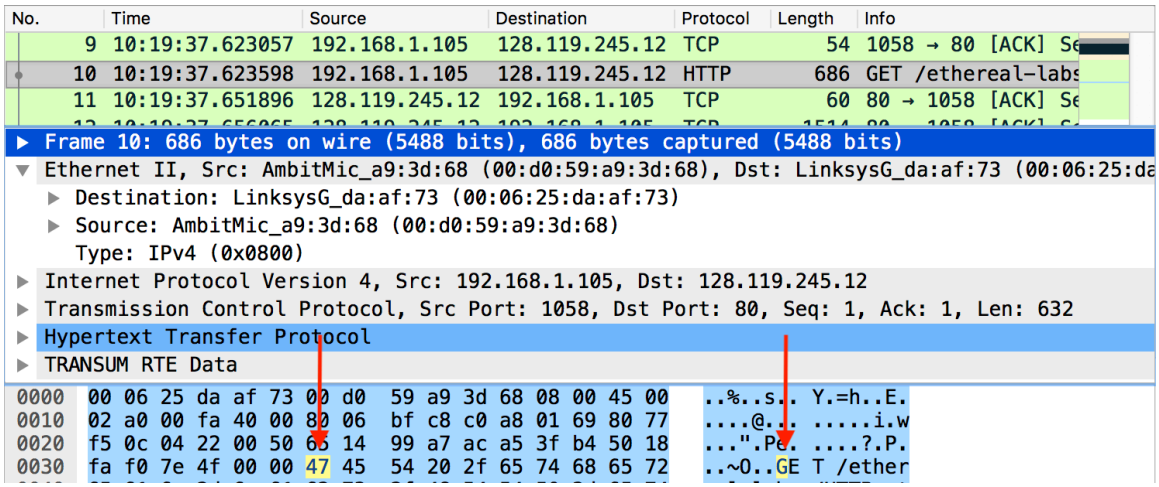
3) Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

Answer:
IPv4 (0x0800)
See screenshot below.



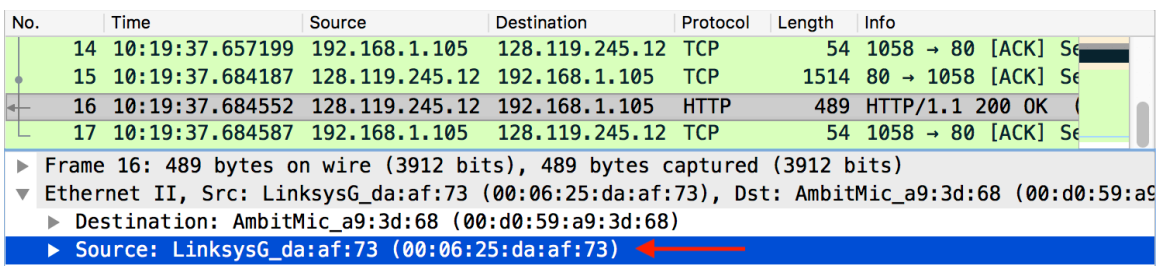
4) How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

Answer:
54 bytes
See screenshot below.



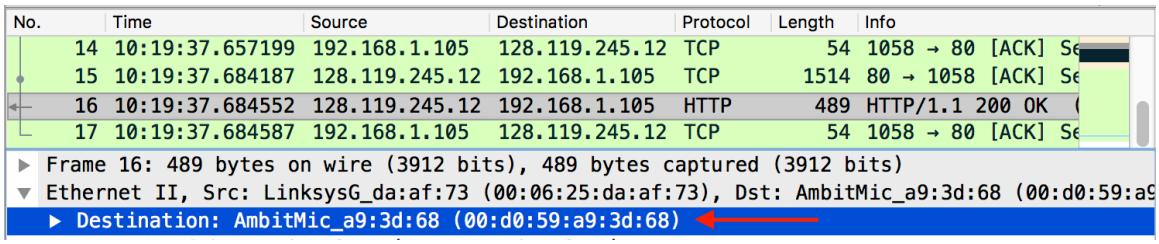
5) What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu? What device has this as its Ethernet address?

Answer:
00:06:25:da:af:73
Neither
My router has this as its Ethernet address.
See screenshot below.



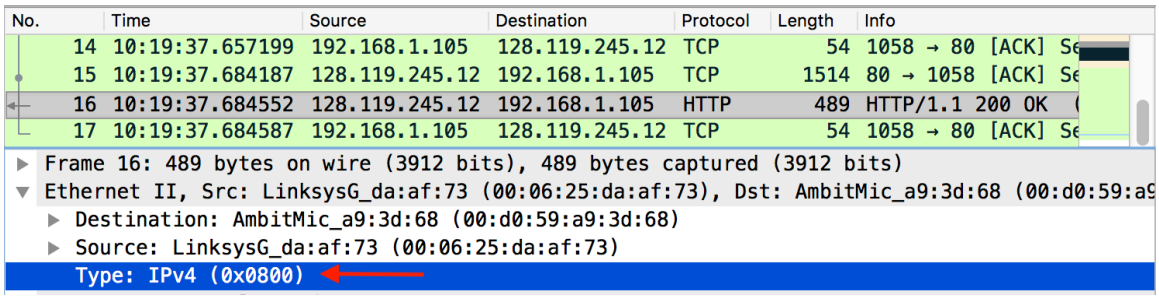
6) What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

Answer:
00:d0:59:a9:3d:68
Yes
See screenshot below.



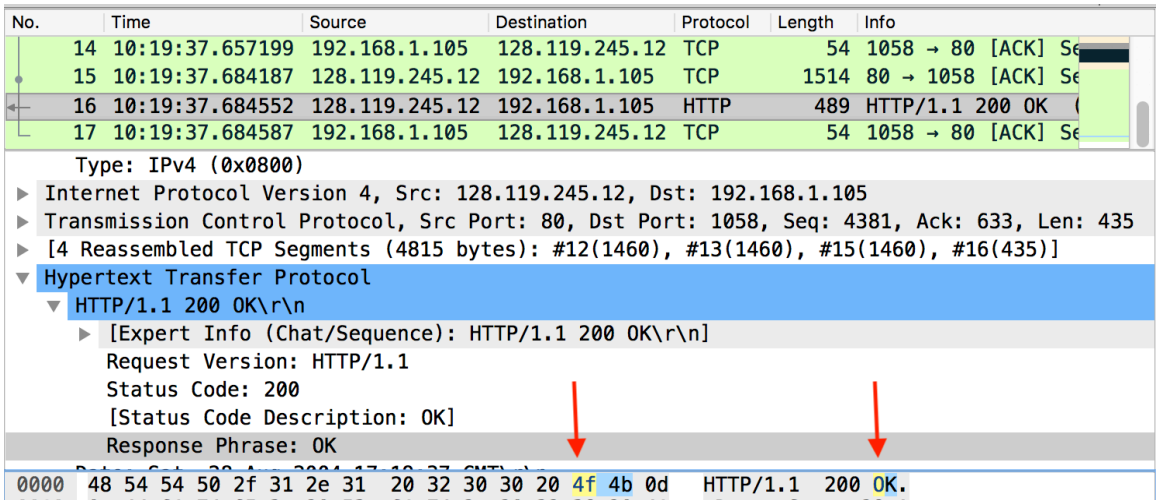
7) Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

Answer:
Type: IPv4 (0x0800)
See screenshot below.



8) How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” appear in the Ethernet frame?

Answer:
68
See screenshot below.



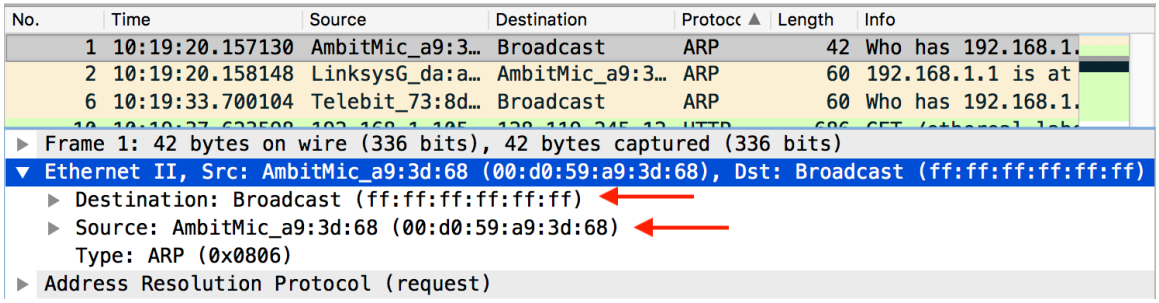
9) Write down the contents of your computer's ARP cache. What is the meaning of each column value?

Answer:
internet address = ip
physical adress = Mac
type = static/dynamic
See screenshot below.

```
? (192.168.1.1) at c4:4:15:23:3e:e on en0 ifscope [ethernet]
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
broadcasthost (255.255.255.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
```

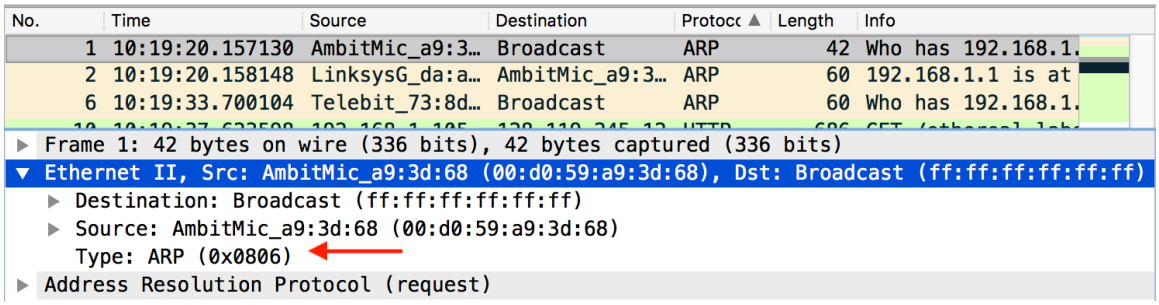
10) What are the hexadecimal values for the source and destination address in the Ethernet frame containing the ARP request message?

Answer:
Source: 00:d0:59:a9:3d:68
Destination: ff:ff:ff:ff:ff:ff
See screenshot below.



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

Answer:
Type: ARP (0x0806)
See screenshot below.



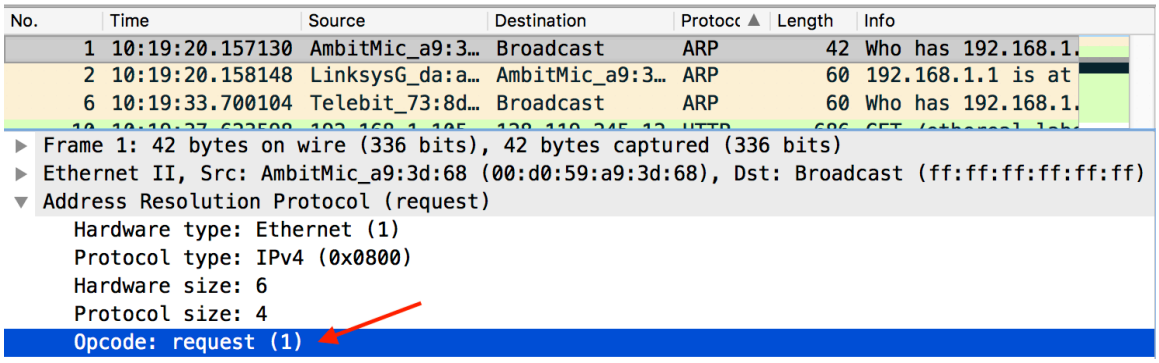
12)
A) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

Answer:
20 bytes
See screenshot below.

```
Ethernet transmission layer (not necessarily accessible to
      the user):
     48.bit: Ethernet address of destination    (6 bytes)
     48.bit: Ethernet address of sender         (6 bytes)
     16.bit: Protocol type = ether_type$ADDRESS_RESOLUTION (2 bytes)
 Ethernet packet data:
     16.bit: (ar$hrd) Hardware address space (e.g., Ethernet,
                      Packet Radio Net.) (2 bytes)
     16.bit: (ar$pro) Protocol address space.  For Ethernet
                      hardware, this is from the set of type
                      fields ether_typ$<protocol>. (2 bytes)
      8.bit: (ar$hln) byte length of each hardware address (1 byte)
      8.bit: (ar$pln) byte length of each protocol address (1 byte)
     16.bit: (ar$op)  opcode (ares_op$REQUEST | ares_op$REPLY) (2 bytes)
```

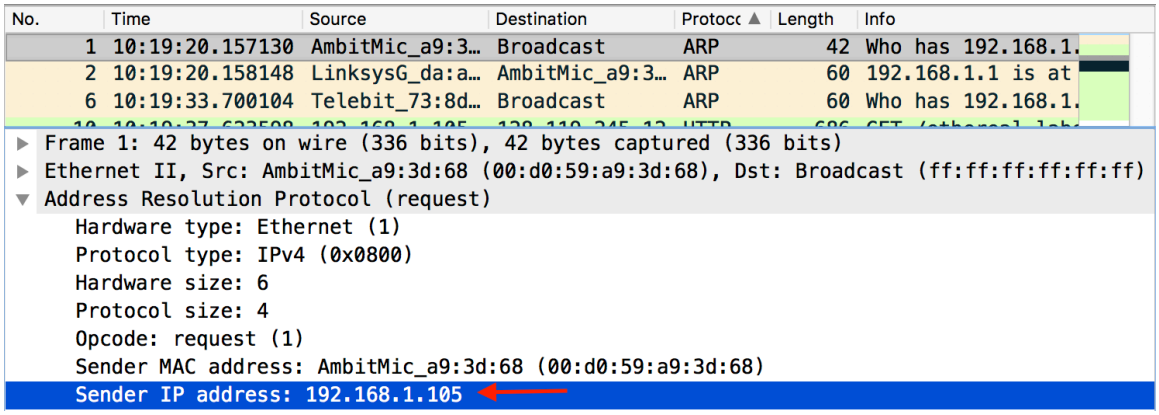
B) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

Answer:
Opcode: request (1)
See screenshot below.



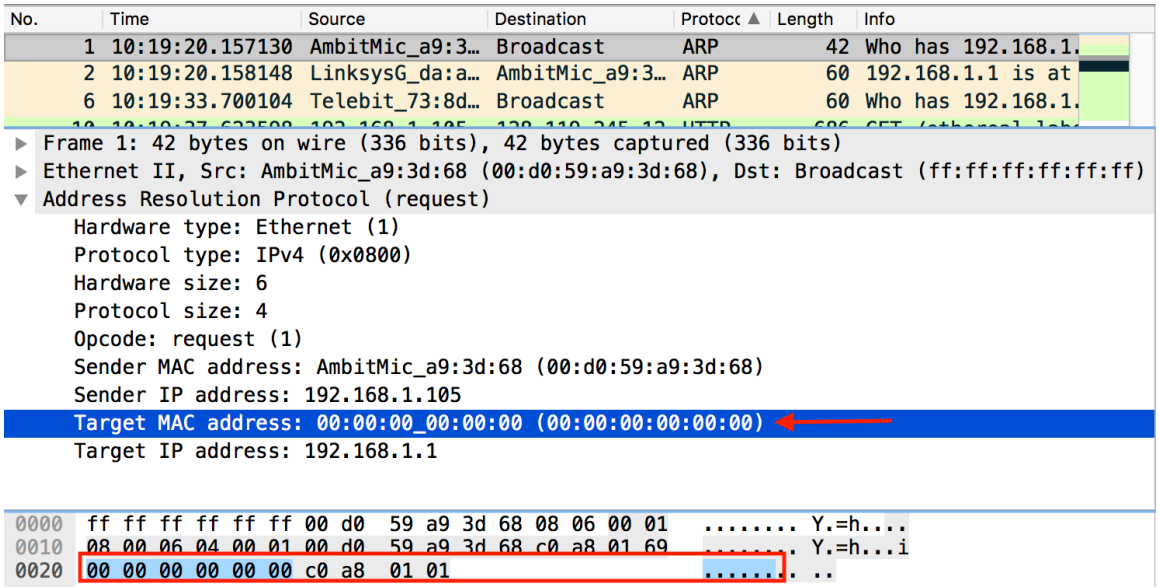
C) Does the ARP message contain the IP address of the sender?

Answer:
Yes - 192.168.1.105
See screenshot below.



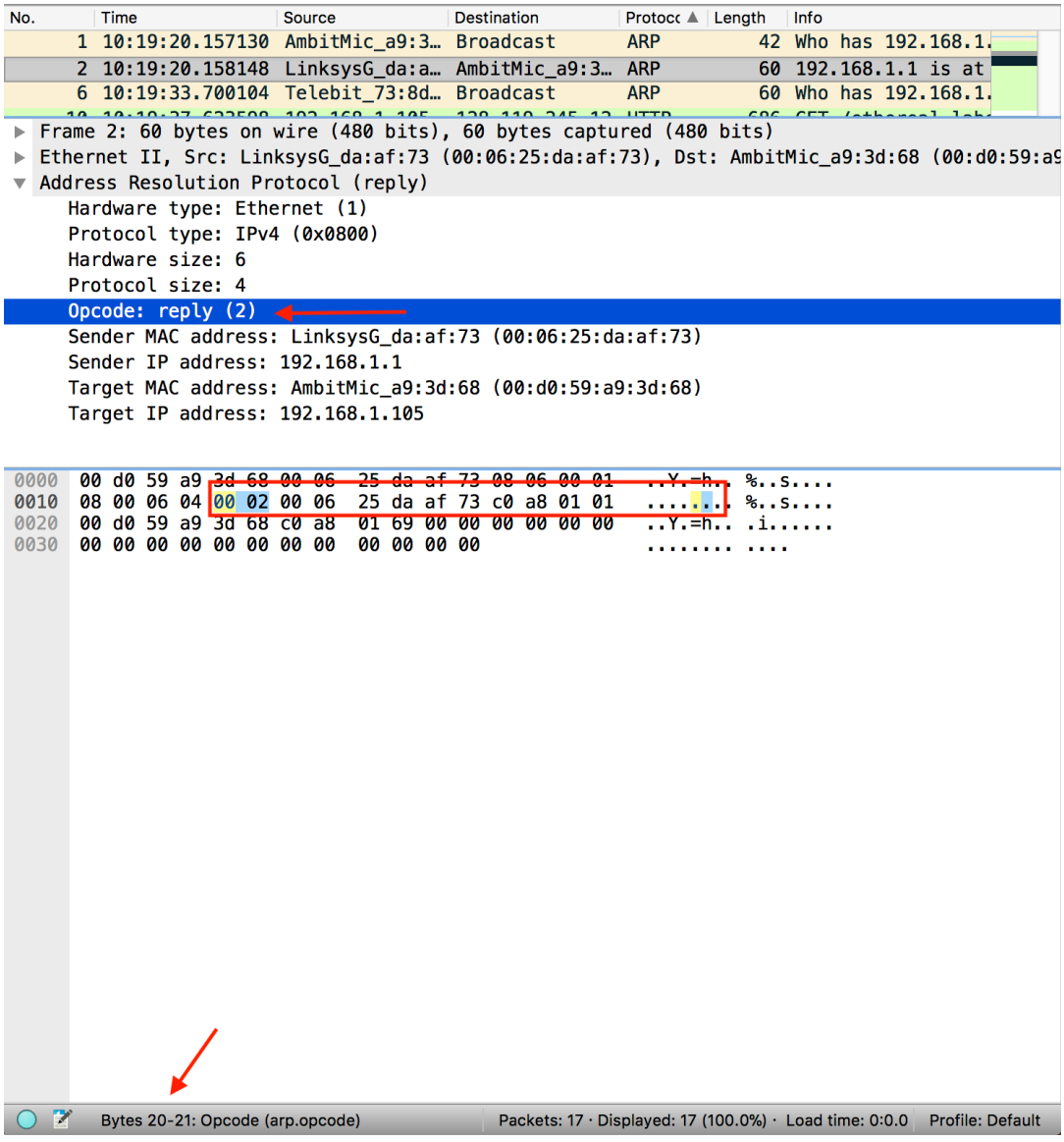
D) Where in the ARP request does the “question” appear - the Ethernet address of the machine whose corresponding IP address is being queried?

Answer:
In the Target MAC address field in the form of 00:00:00:00:00:00
See screenshot below.



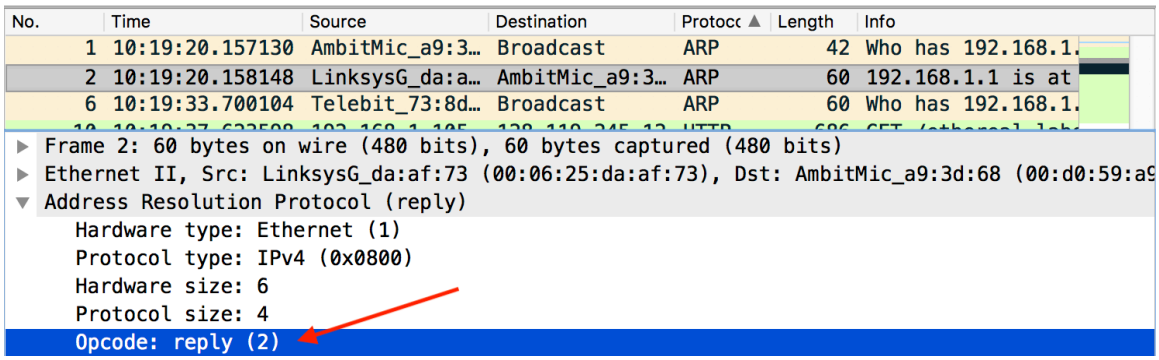
13) Now find the ARP reply that was sent in response to the ARP request.
A) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

Answer:
20 bytes
See screenshot below.



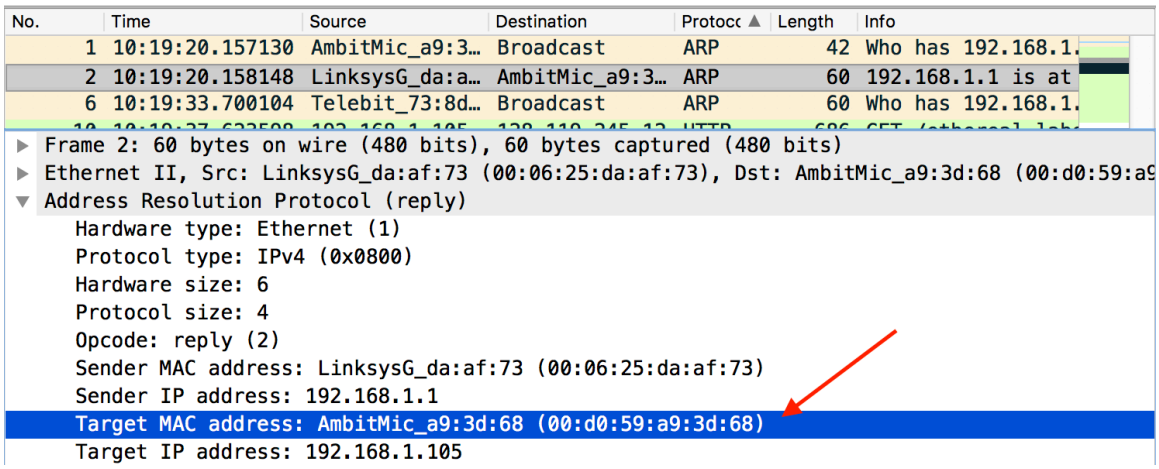
B) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

Answer:
Opcode: reply (2)
See screenshot below.



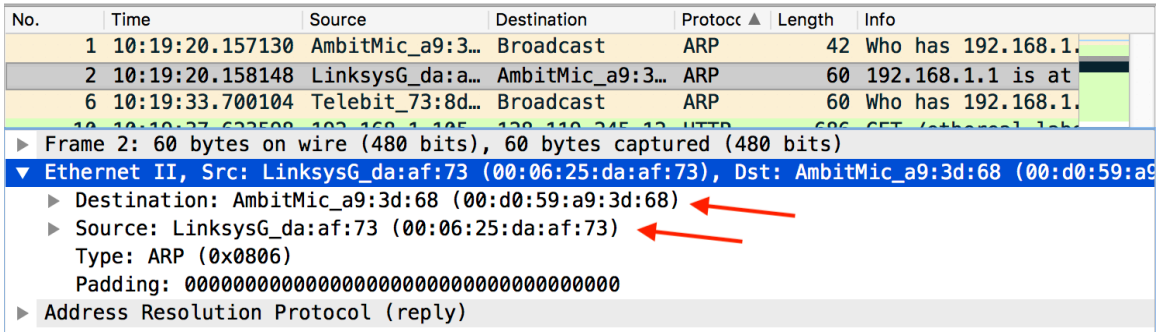
C) Where in the ARP message does the “answer” to the earlier ARP request appear - the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

Answer:
The Target MAC address was queried from 00:00:00:00:00:00 to 00:d0:59:a9:3d:68.
Also, the Target IP address changed from 192.168.1.1 to 192.168.1.105.
See screenshot below.



14) What is the hexadecimal values for the source and destination address in the Ethernet frame containing the ARP reply message?

Answer:
Source: 00:06:25:da:af:73
Destination: 00:d0:59:a9:3d:68
See screenshot below.



15) Why is there no ARP reply (sent in response to the ARP request in packet 6) in the packet trace?

Answer:
The target IP address is within the same subnet that the router has already mapped in its ARP table.
See screenshot below.