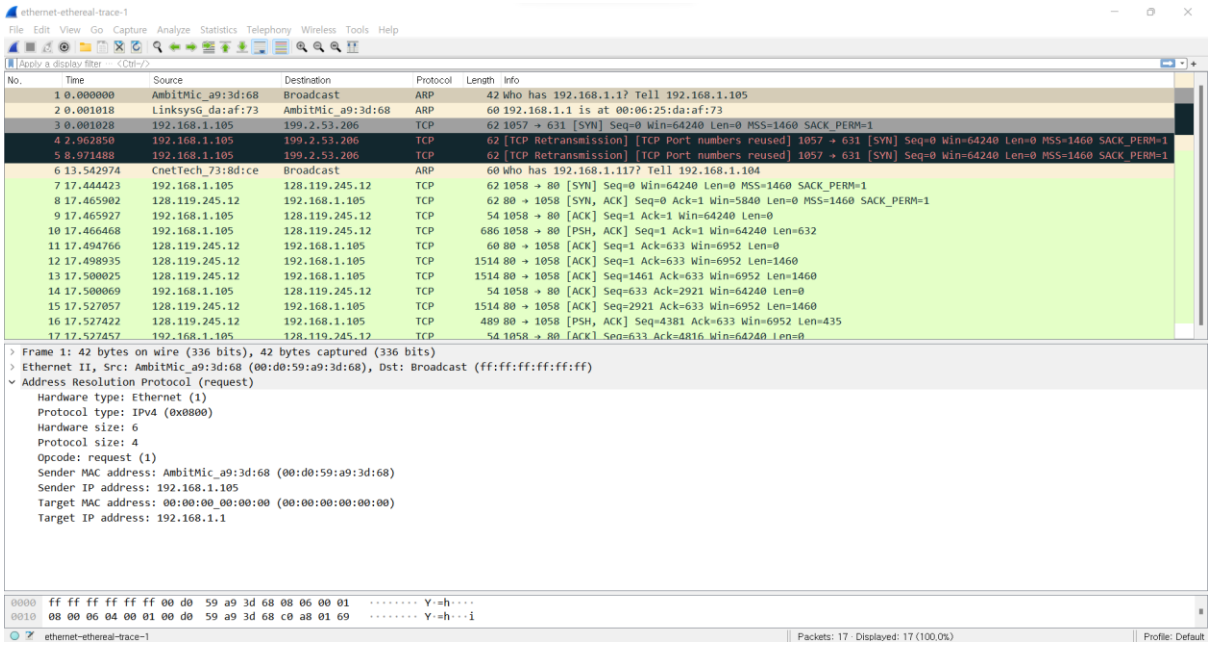
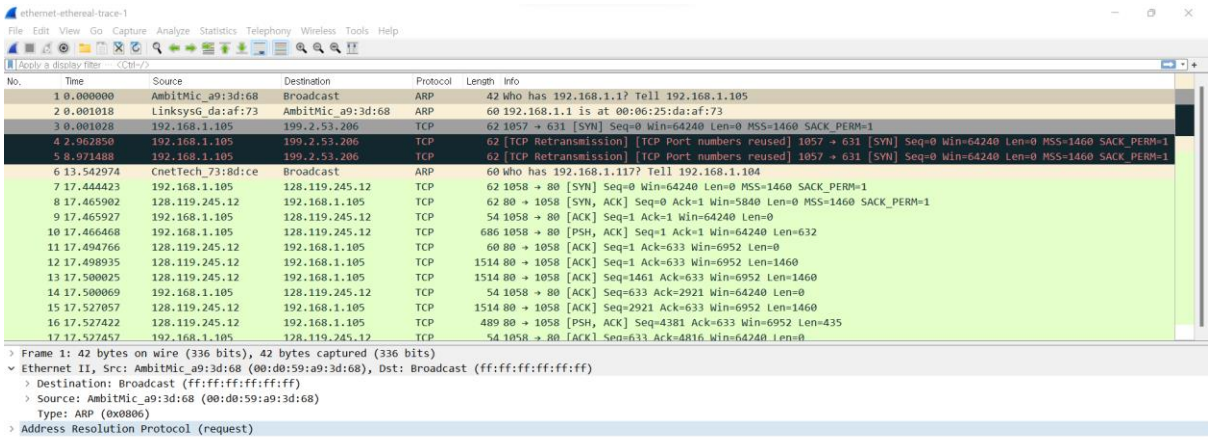
1. What is the 48-bit Ethernet address of your computer?

It 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.]

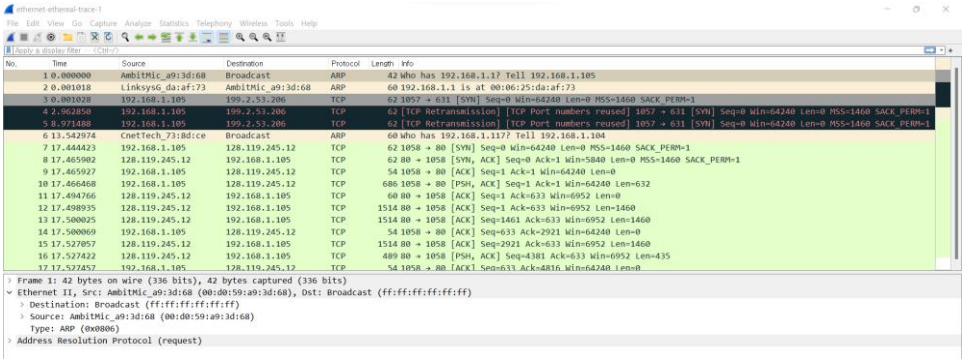
It is ff-ff-ff-ff-ff-ff.



No, it is not the Ethernet address of gaia.cs.umass.edu. The Ethernet address is indicating the broadcast all devices in the local area network.

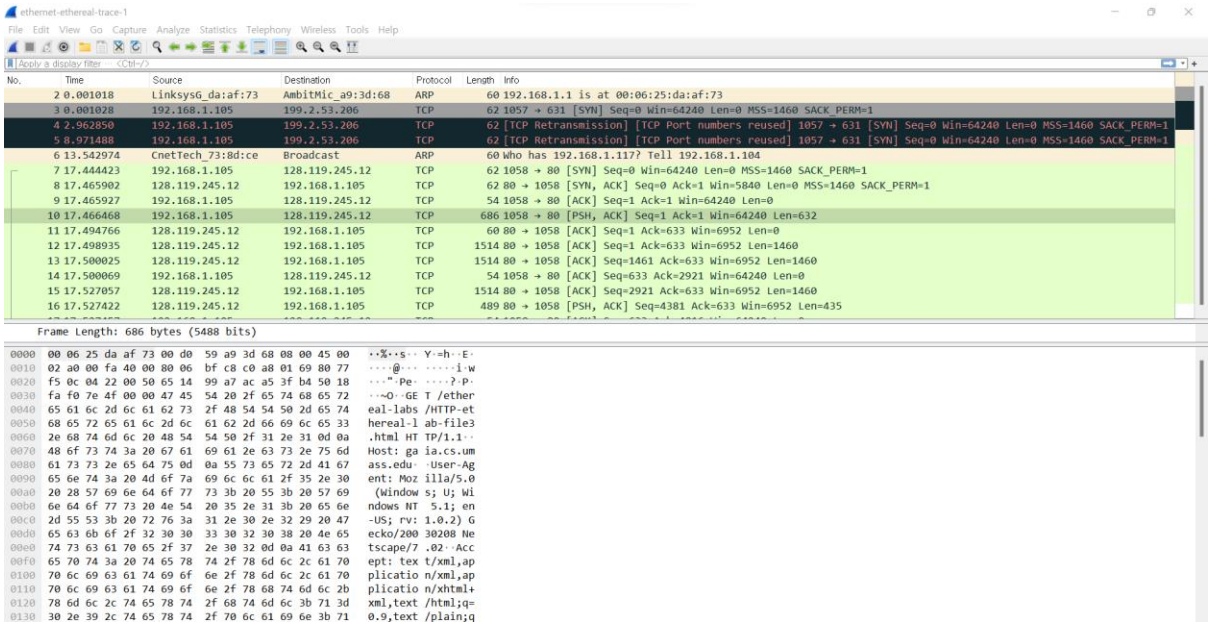
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

It is 0x0806. The corresponding upper layer protocol is ARP in data link layer.



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

54 bytes.

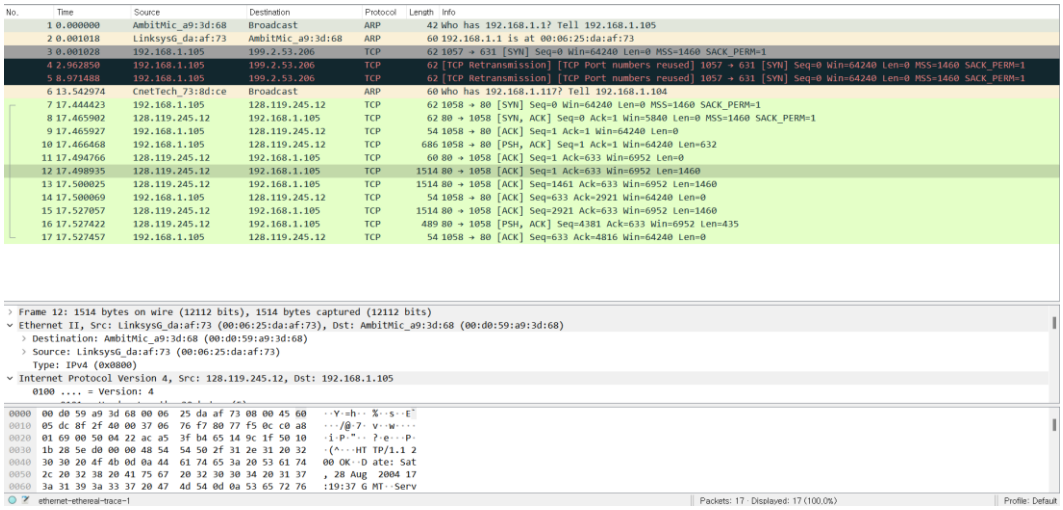


5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

The address is 00-06-25-da-af-73..

This address is not for both my computer and gaia.cs.umass.edu.

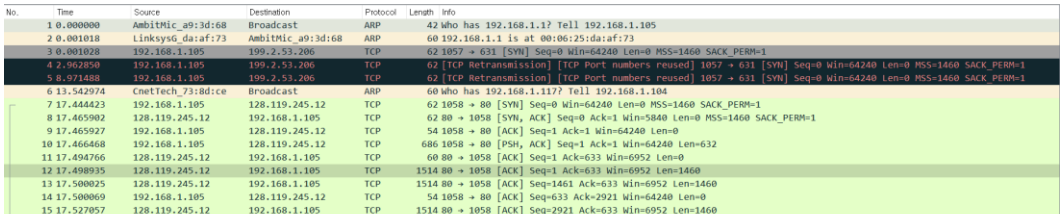
Router has this address.

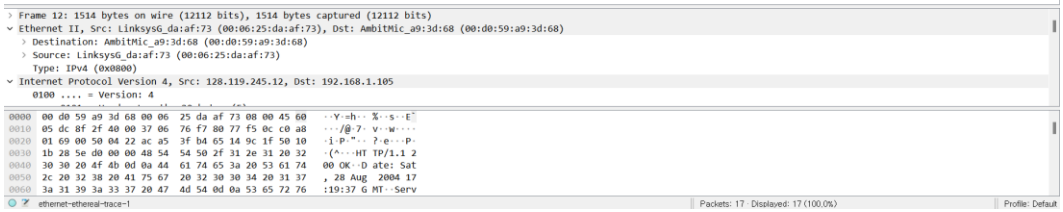


6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

00-d0-59-a9-3d-68.

This is the Ethernet address of my computer.

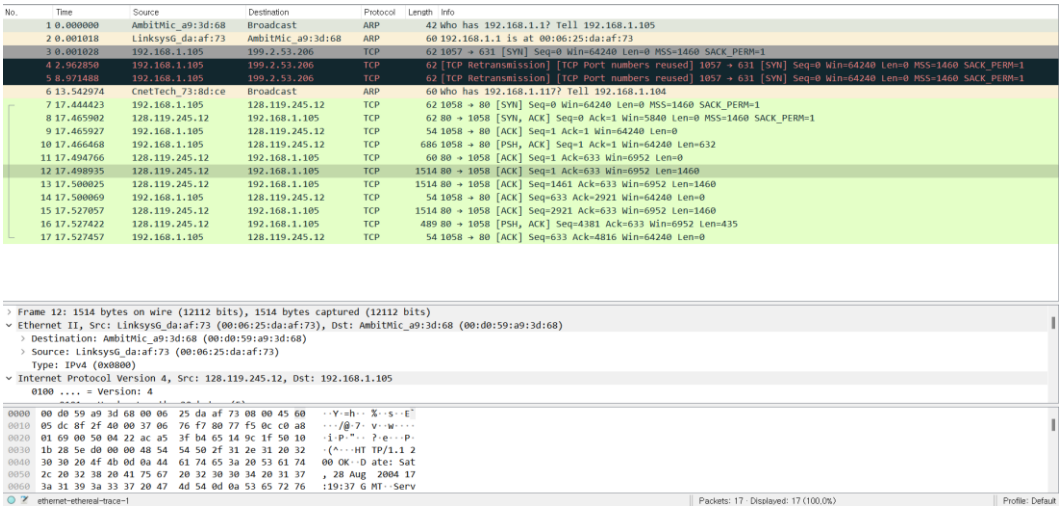




7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

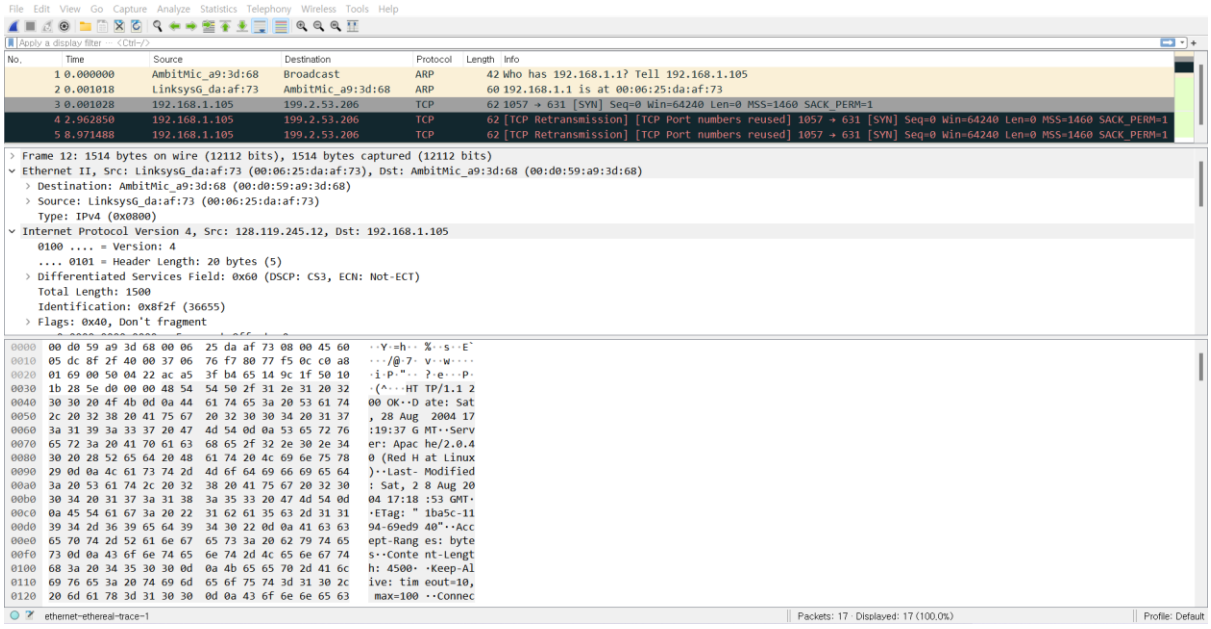
The hexadecimal value for the two-byte Frame type field is 0x0800.

This corresponds to 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?

66 bytes.



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

Each column means IP address, MAC address, and type of the address.

```
인터페이스: 10.248.188.217 --- 0x11
  인터넷 주소           물리적 주소           유형
  10.248.0.1            00-00-5e-00-01-01     동적
  10.249.255.255        ff-ff-ff-ff-ff-ff     정적
  224.0.0.22            01-00-5e-00-00-16     정적
  224.0.0.251           01-00-5e-00-00-fb     정적
  224.0.0.252           01-00-5e-00-00-fc     정적
  239.255.255.250       01-00-5e-7f-ff-fa     정적
  255.255.255.255       ff-ff-ff-ff-ff-ff     정적

인터페이스: 192.168.56.1 --- 0x1a
  인터넷 주소           물리적 주소           유형
  192.168.56.255        ff-ff-ff-ff-ff-ff     정적
  224.0.0.22            01-00-5e-00-00-16     정적
  224.0.0.251           01-00-5e-00-00-fb     정적
  224.0.0.252           01-00-5e-00-00-fc     정적
  239.255.255.250       01-00-5e-7f-ff-fa     정적
```

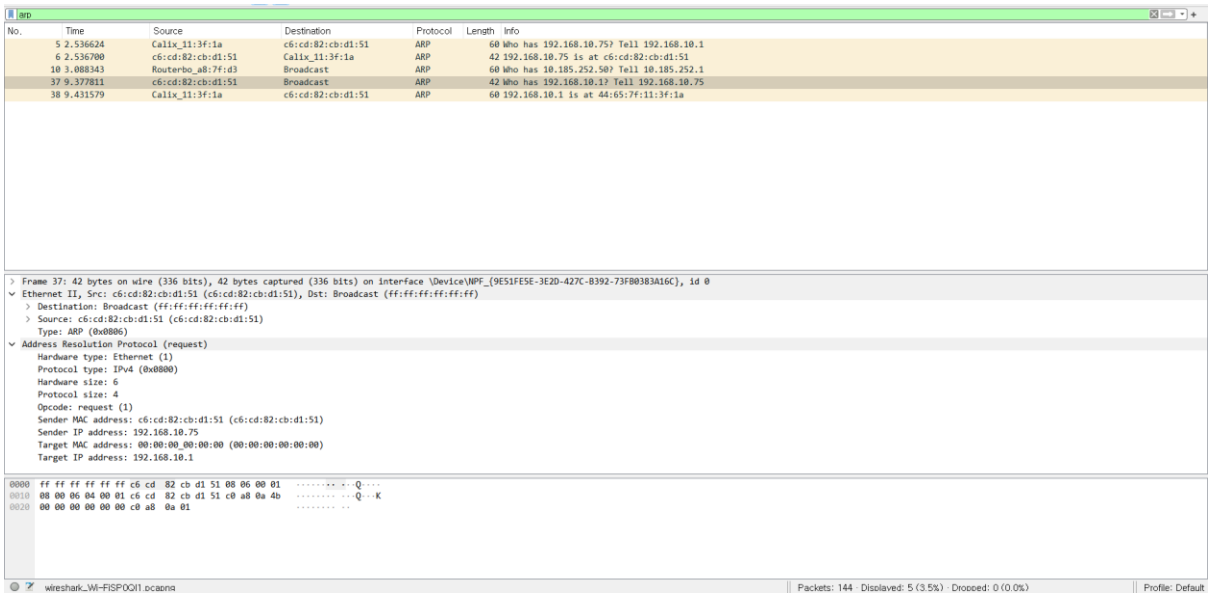
(Translation: "인터페이스" = interface, "인터넷 주소" = IP address, "물리적 주소" = Physical address

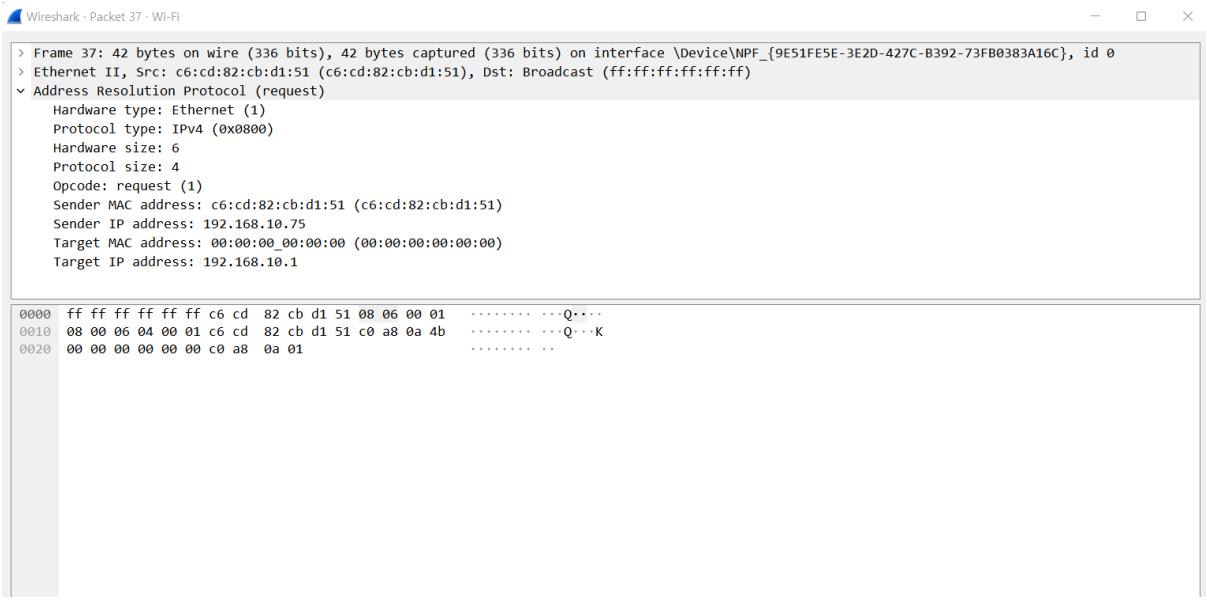
"유형" = type, "정적" = static, "동적" = dynamic)

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

Source Address: C6-CD-82-CB-D1-51

Destination Address: 00-00-00-00-00-00

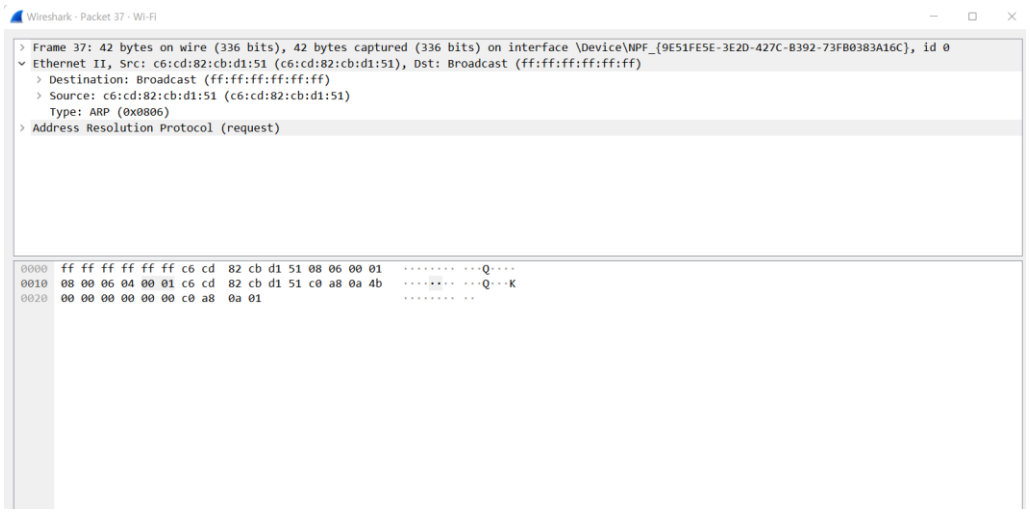




11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

The hexadecimal value is 0x0806.

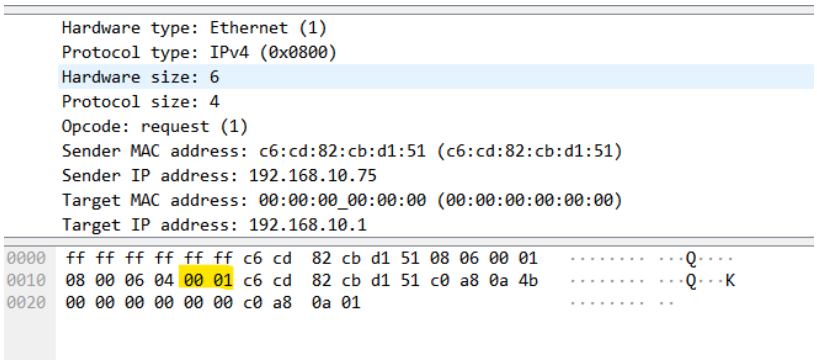
This corresponds to ARP protocol.



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.

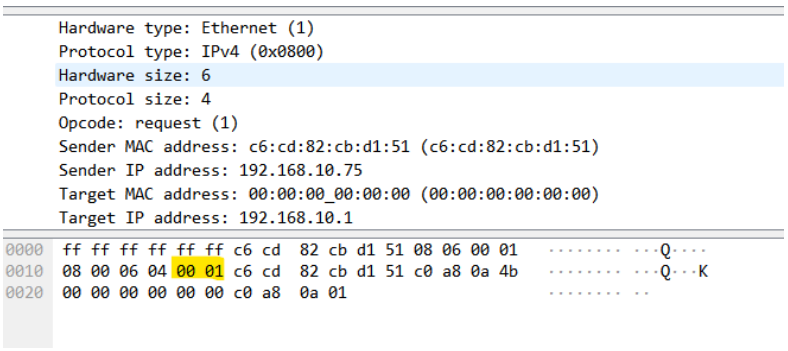
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

The ARP opcode field begins 20 bytes from the beginning of the Ethernet frame.



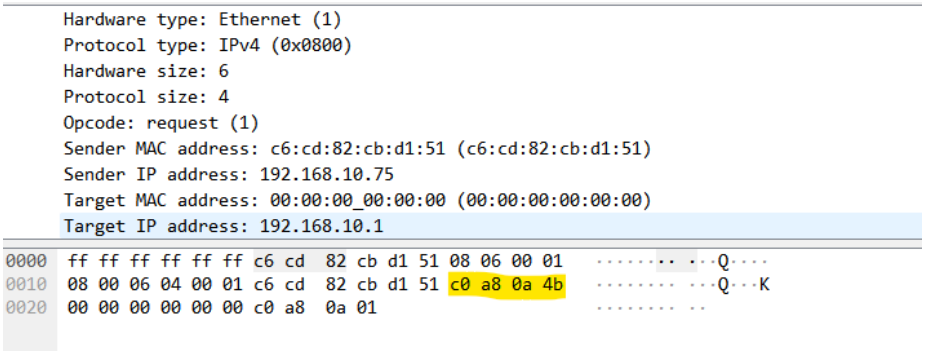
b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

The value of the opcode field is 0x0001.



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

The ARP message contains the IP address of the sender.

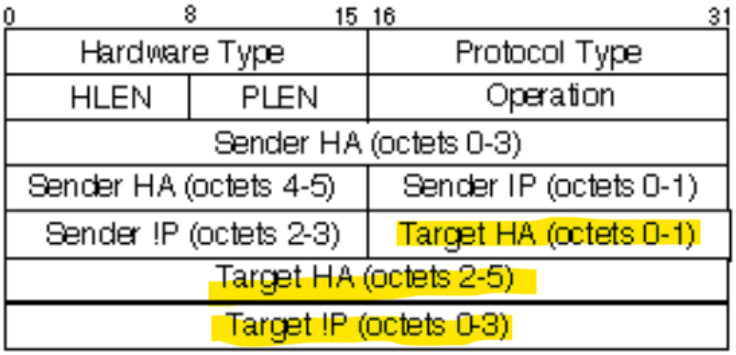


d) Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

The question appears in the 0x0020 line of the frame.

```
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51)
Sender IP address: 192.168.10.75
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.10.1
```

```
0000  ff ff ff ff ff ff c6 cd  82 cb d1 51 08 06 00 01   ........ ...Q....
0010  08 00 06 04 00 01 c6 cd  82 cb d1 51 c0 a8 0a 4b   ........ ...Q...K
0020  00 00 00 00 00 00 c0 a8  0a 01                     ........ ..
```



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?

The opcode field begins 20 bytes from the beginning of the Ethernet frame.

```
> Frame 38: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{9E51FE5E-3E2D-427C-B392-73FB0383A16C}, id 0
v Ethernet II, Src: Calix_11:3f:1a (44:65:7f:11:3f:1a), Dst: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51)
  > Destination: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51)
  > Source: Calix_11:3f:1a (44:65:7f:11:3f:1a)
    Type: ARP (0x0806)
    Padding: 00000000000000000000000000000000000000
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
```

```
0000  c6 cd 82 cb d1 51 44 65  7f 11 3f 1a 08 06 00 01   .....QDe ..?.....
0010  08 00 06 04 00 02 44 65  7f 11 3f 1a c0 a8 0a 01   ......De ..?.....
0020  c6 cd 82 cb d1 51 c0 a8  0a 4b 00 00 00 00 00 00   .....Q.. .K......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

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?

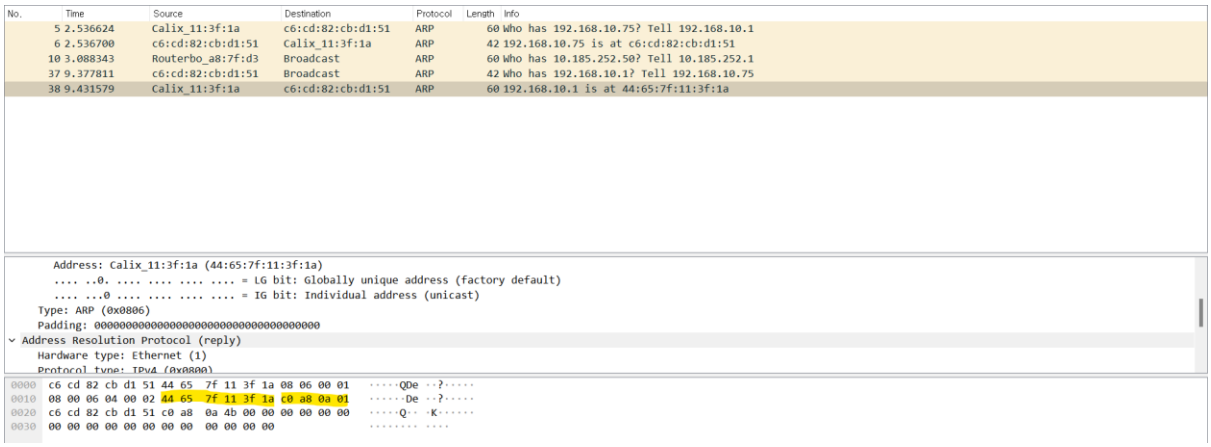
The value of the opcode field is 0x0002.

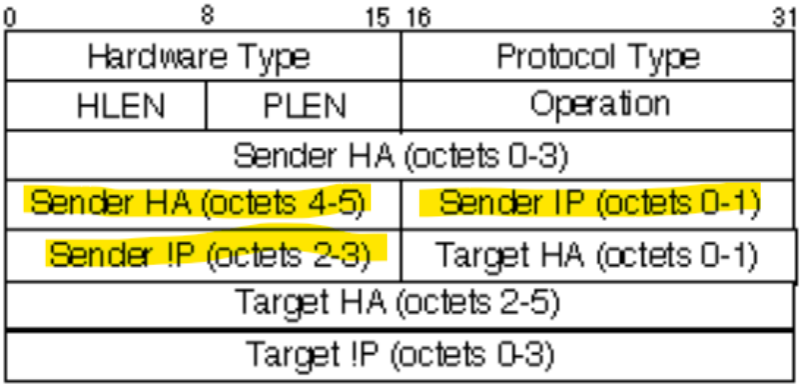
```
> Frame 38: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{9E51FE5E-3E2D-427C-B392-73FB0383A16C}, id 0
v Ethernet II, Src: Calix_11:3f:1a (44:65:7f:11:3f:1a), Dst: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51)
  > Destination: c6:cd:82:cb:d1:51 (c6:cd:82:cb:d1:51)
  > Source: Calix_11:3f:1a (44:65:7f:11:3f:1a)
    Type: ARP (0x0806)
    Padding: 00000000000000000000000000000000000000
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
```

```
0000  c6 cd 82 cb d1 51 44 65  7f 11 3f 1a 08 06 00 01   .....QDe ..?.....
0010  08 00 06 04 00 02 44 65  7f 11 3f 1a c0 a8 0a 01   ......De ..?.....
0020  c6 cd 82 cb d1 51 c0 a8  0a 4b 00 00 00 00 00 00   .....Q.. .K......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

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 is in the 0x0010 line of the frame.

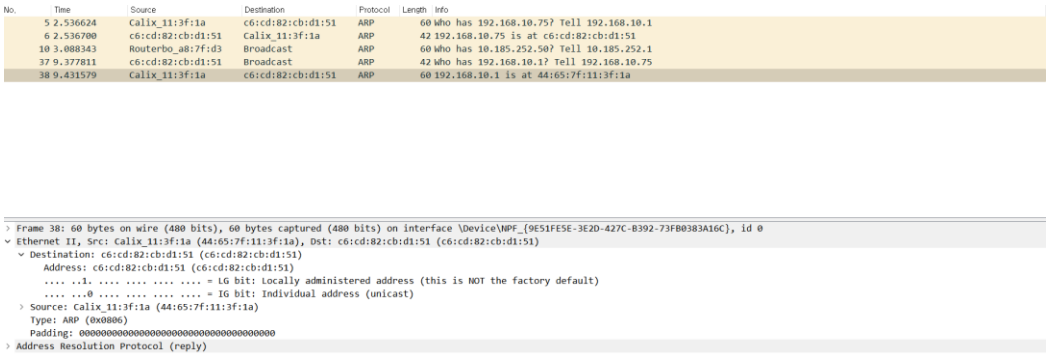




14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

Source Address: 44-65-7F-11-3F-1A

Destination Address: C6-CD-82-CB-D1-51



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 is no ARP request because the computer 192.168.1.105 is not the subject of the target address. The computer 192.168.1.104 broadcasts the request in the entire local area network, and the computer 192.168.1.117 replies to the request so that the computer 192.168.1.105 cannot see the ARP reply going to the computer 192.168.1.104.

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 packet frame will never reach the receiver if the Ethernet address is wrong while the IP address is correct. The sender sends the packet with MAC header and IP header to the receiver. Then, the LAN checks the MAC address and then sends it to correspond receiver. However, if the MAC address is wrong, then the LAN will reject that packet frame. Therefore, the packet from the sender will never arrive the receiver.

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.

There is no default amount of time that an entry remains in ARP cache before being removed in Windows operating system.

“In the new Windows Vista TCP/IP stack implementation, hosts create the neighbor cache entries when there is no matching entry in the neighbor cache. ARP cache entry for IPv4 is an example of a neighbor cache entry. After the entry is successfully created in the neighbor cache, the entry may change to the "Reachable" state if the entry meets certain conditions. If the entry is in the "Reachable" state, Windows Vista TCP/IP hosts do not send ARP requests to the network. Therefore, Windows Vista TCP/IP hosts use the information in the cache. If an entry is not used, and it stays in the "Reachable" state for longer than its "Reachable Time" value, the entry changes to the "Stale" state. If an entry is in the "Stale" state, the Windows Vista TCP/IP host must send an ARP request to reach that destination.”

“The "Reachable Time" value is calculated as follows:
Reachable Time = BaseReachable Time × (A random value between MIN_RANDOM_FACTOR and MAX_RANDOM_FACTOR)
RFC provides the following calculated results.”

BaseReachable Time	30,000 milliseconds (ms)
MIN_RANDOM_FACTOR	0.5
MAX_RANDOM_FACTOR	1.5

“Therefore, the "Reachable Time" value is somewhere between 15 seconds (30 × 0.5 seconds) and 45 seconds (30 × 1.5 seconds). If an entry is not used for a time between 15 to 45 seconds, it changes to the "Stale" state. Then, the host must send an ARP Request for IPV4 to the network when any IP datagram is sent to that destination.”

(Source from:

https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/address-resolution-protocol-arp-caching-behavior)