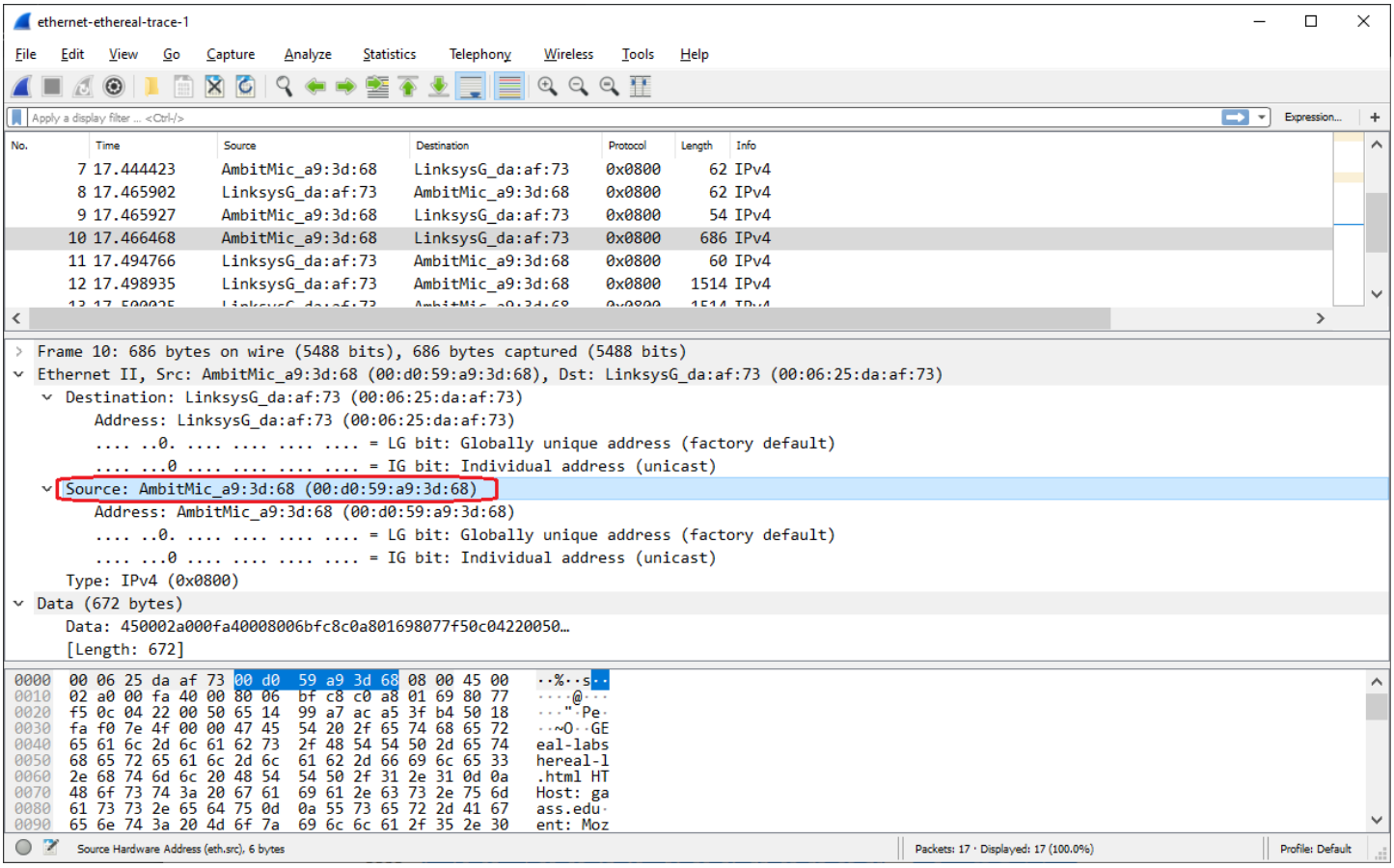
CS372-400
12/6/2019

Edmund Dea
ID# 933280343

Lab 5: Wireshark

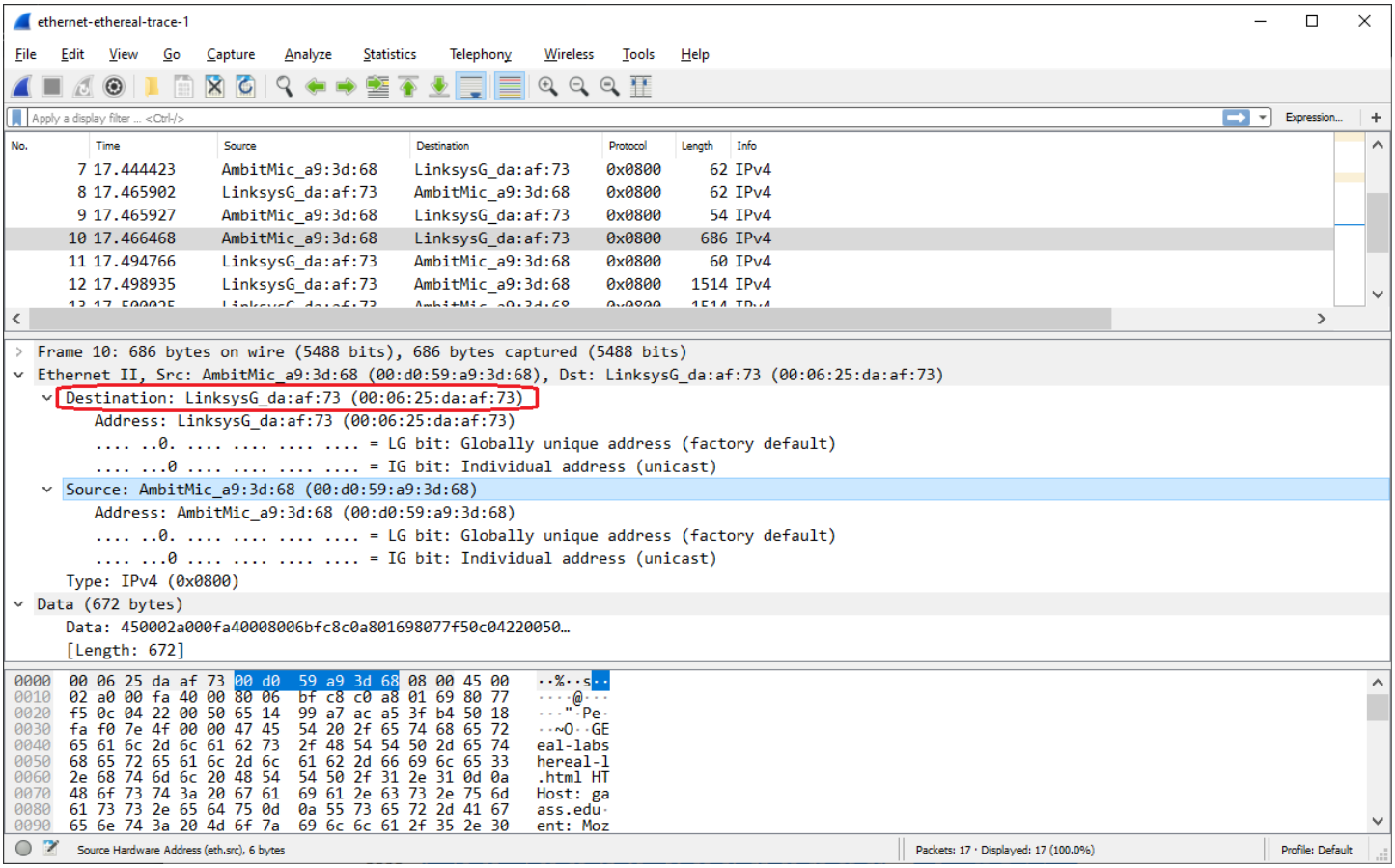
1) What is the 48-bit Ethernet address of your computer?

   The MAC address of my computer is 00:d0:59:a9:3d:68.



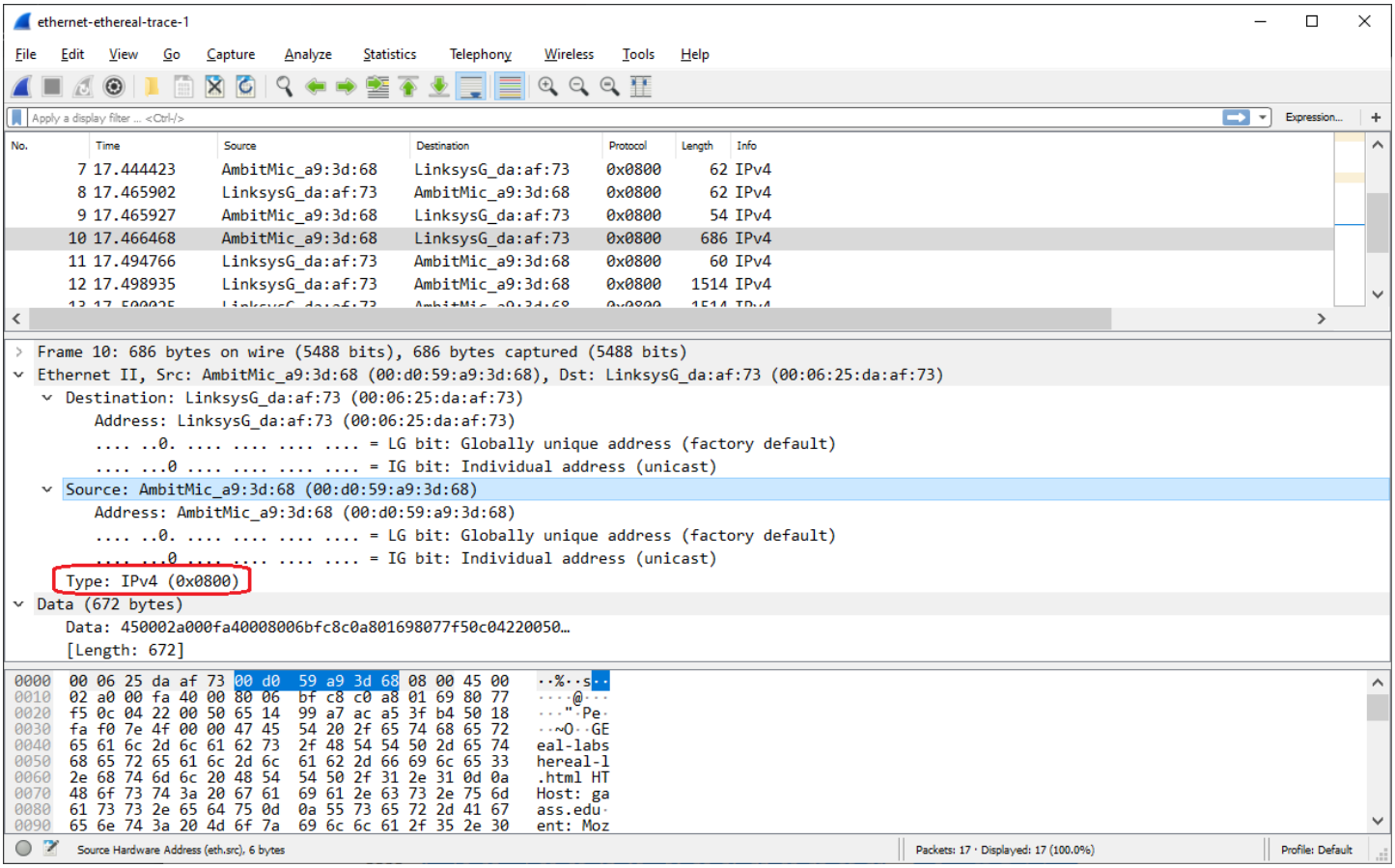
2) What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is *no*). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]

   The destination address in the Ethernet frame is 00:06:25:da:af:73. This is the ethernet address for the Linksys router, not the ethernet address for gaia.cs.umass.edu.



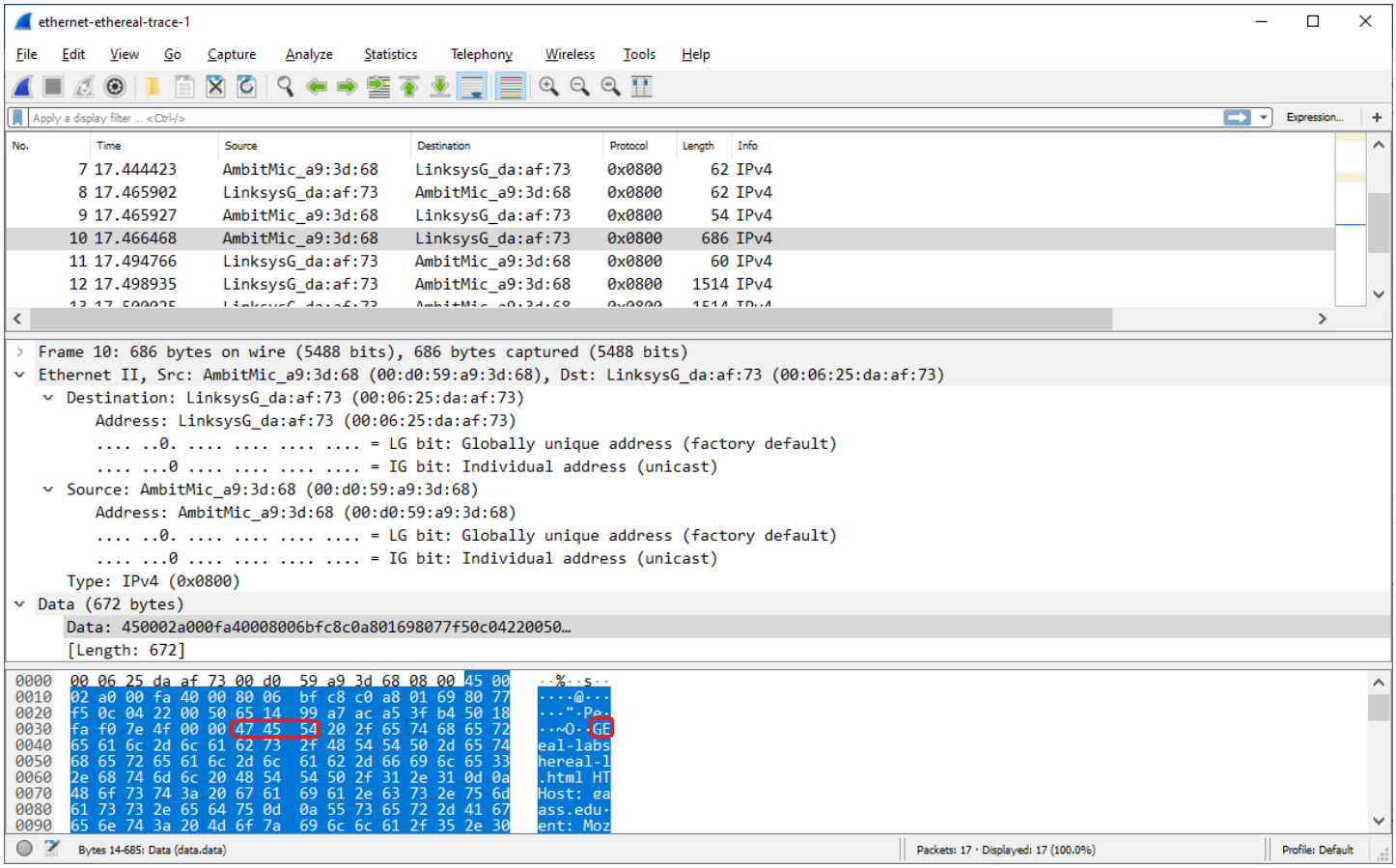
3) Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

The hex value for the two-byte Frame type field is 0x800. The value corresponds to the IPv4 upper layer protocol.



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

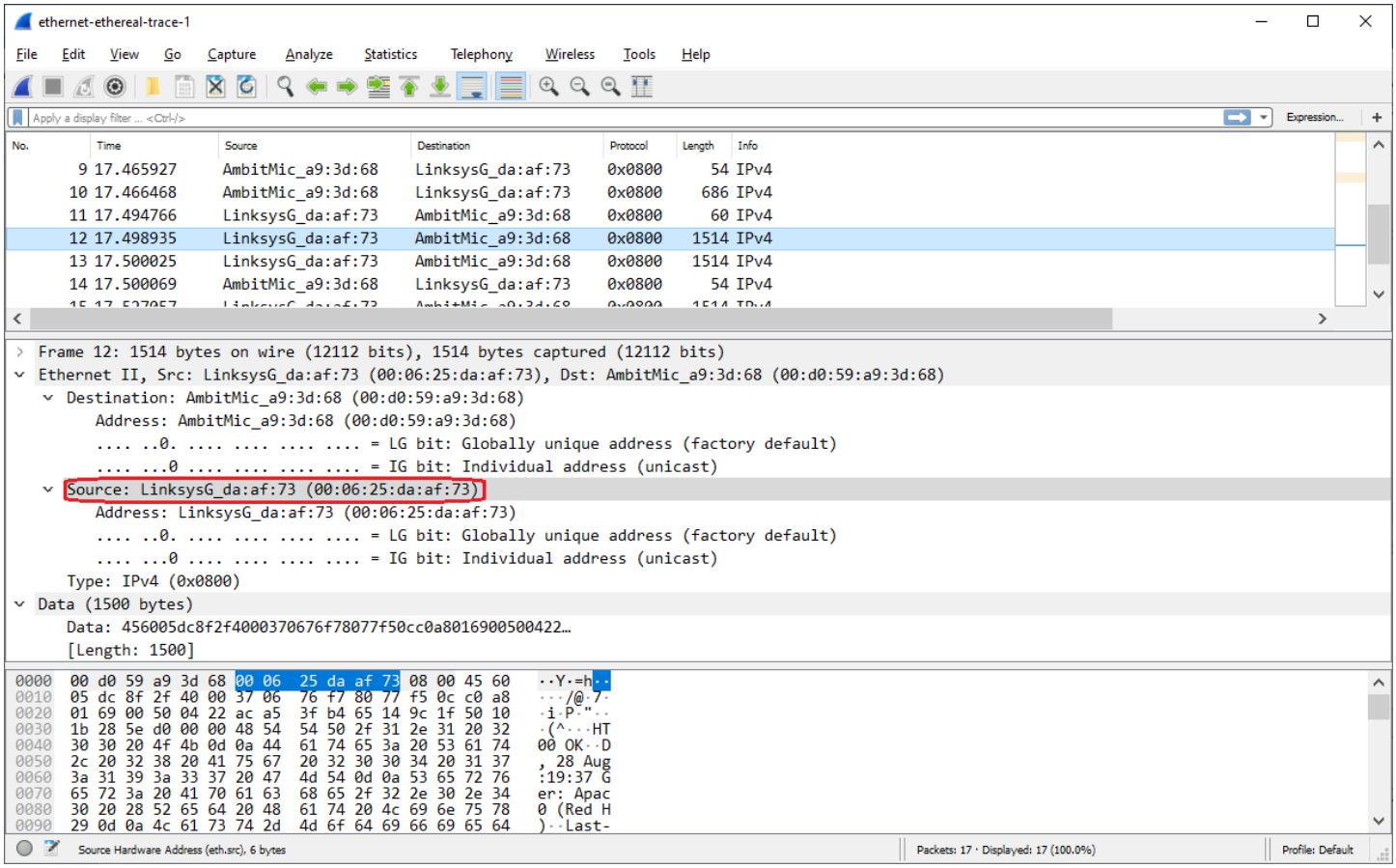
The ASCII ‘G’ in “GET” appears after 54 bytes from the very start of the ethernet frame.



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

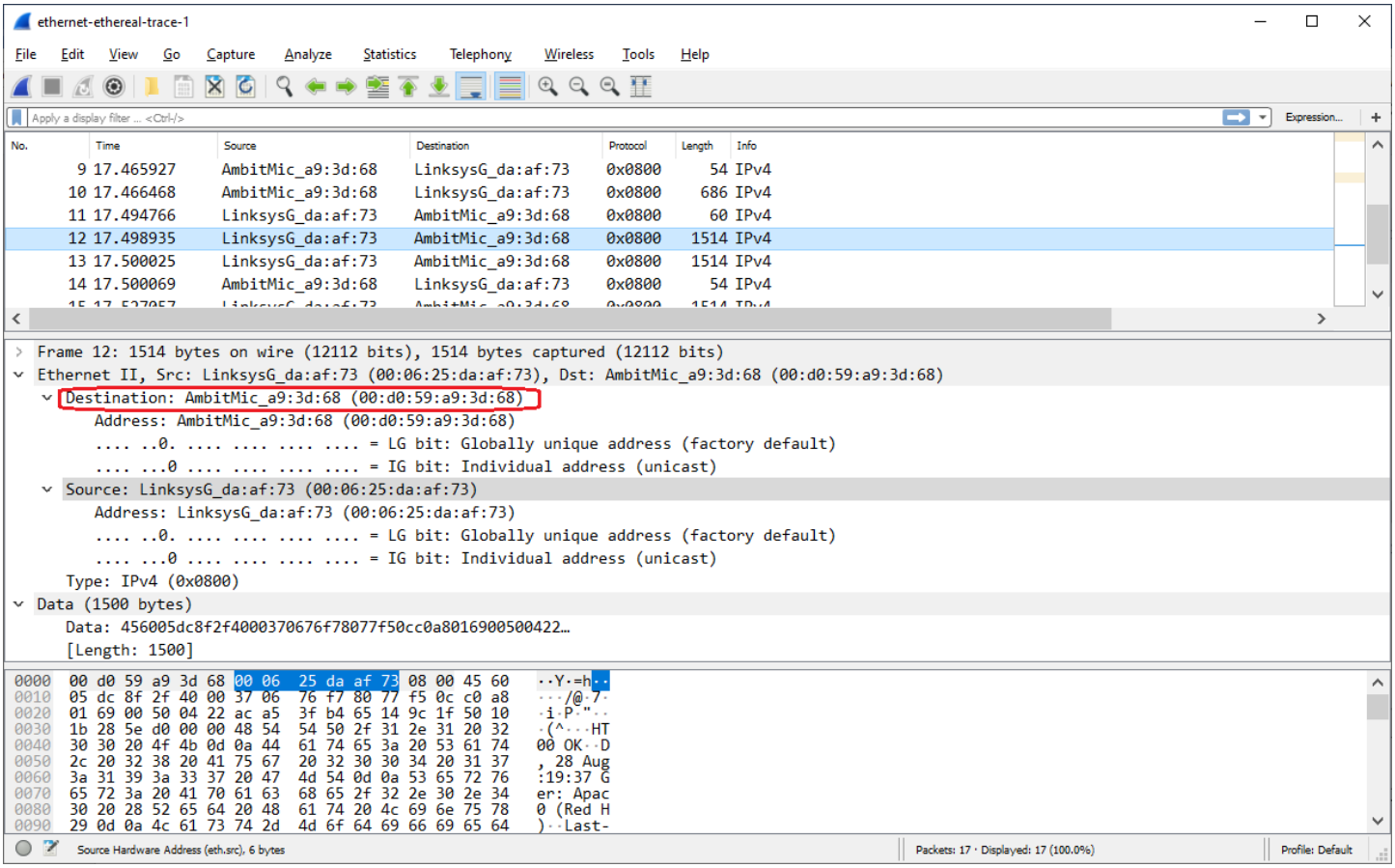
5) What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is *no*). What device has this as its Ethernet address?

   The value of the ethernet source address is 00:06:25:da:af:73. This is neither the address of my computer nor the address of gaia.cs.umass.edu. This is the ethernet address of the router.



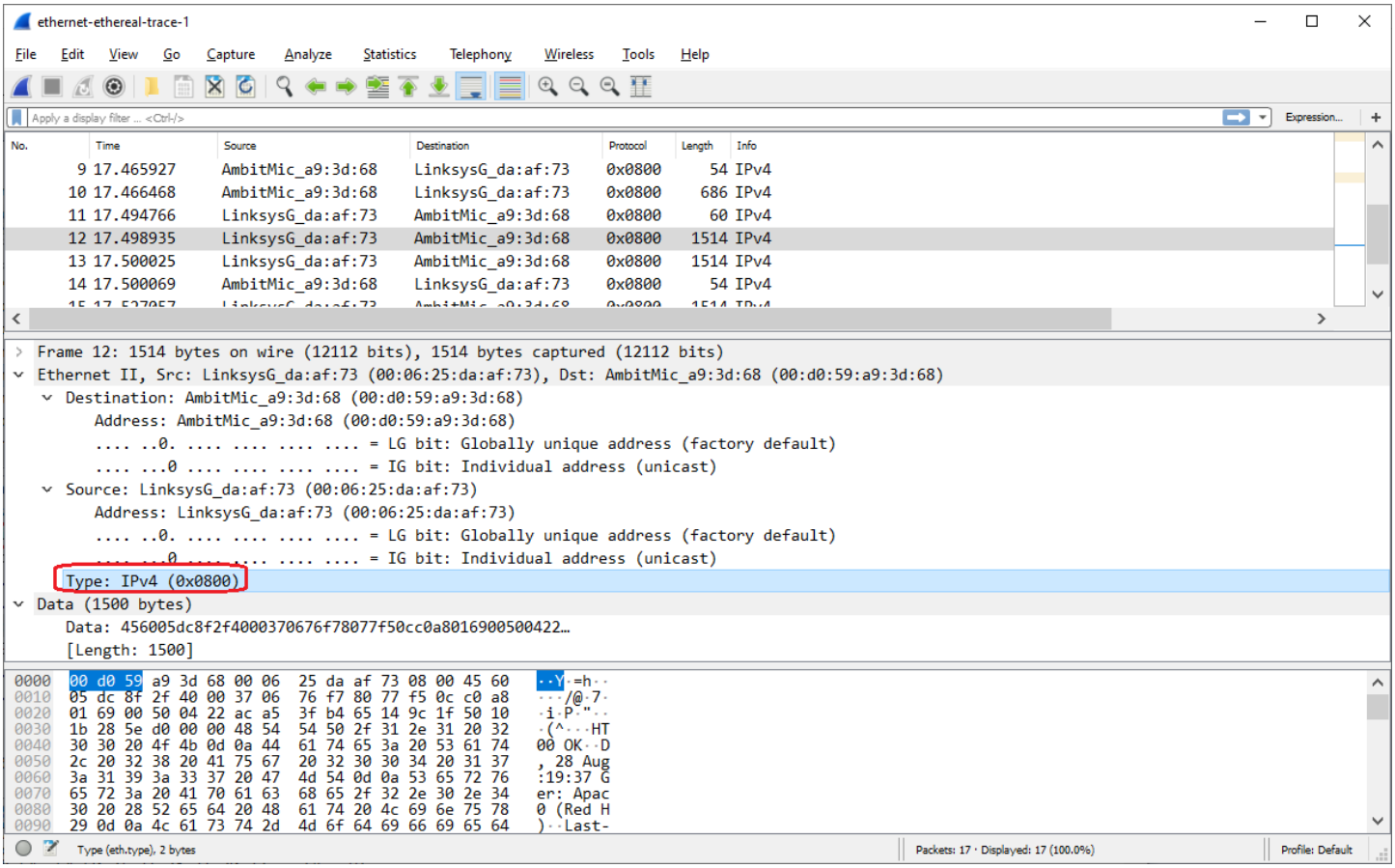
6) What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

The destination address in the ethernet frame is 00:d0:59:a9:3d:68. Yes, this is the address of my computer.



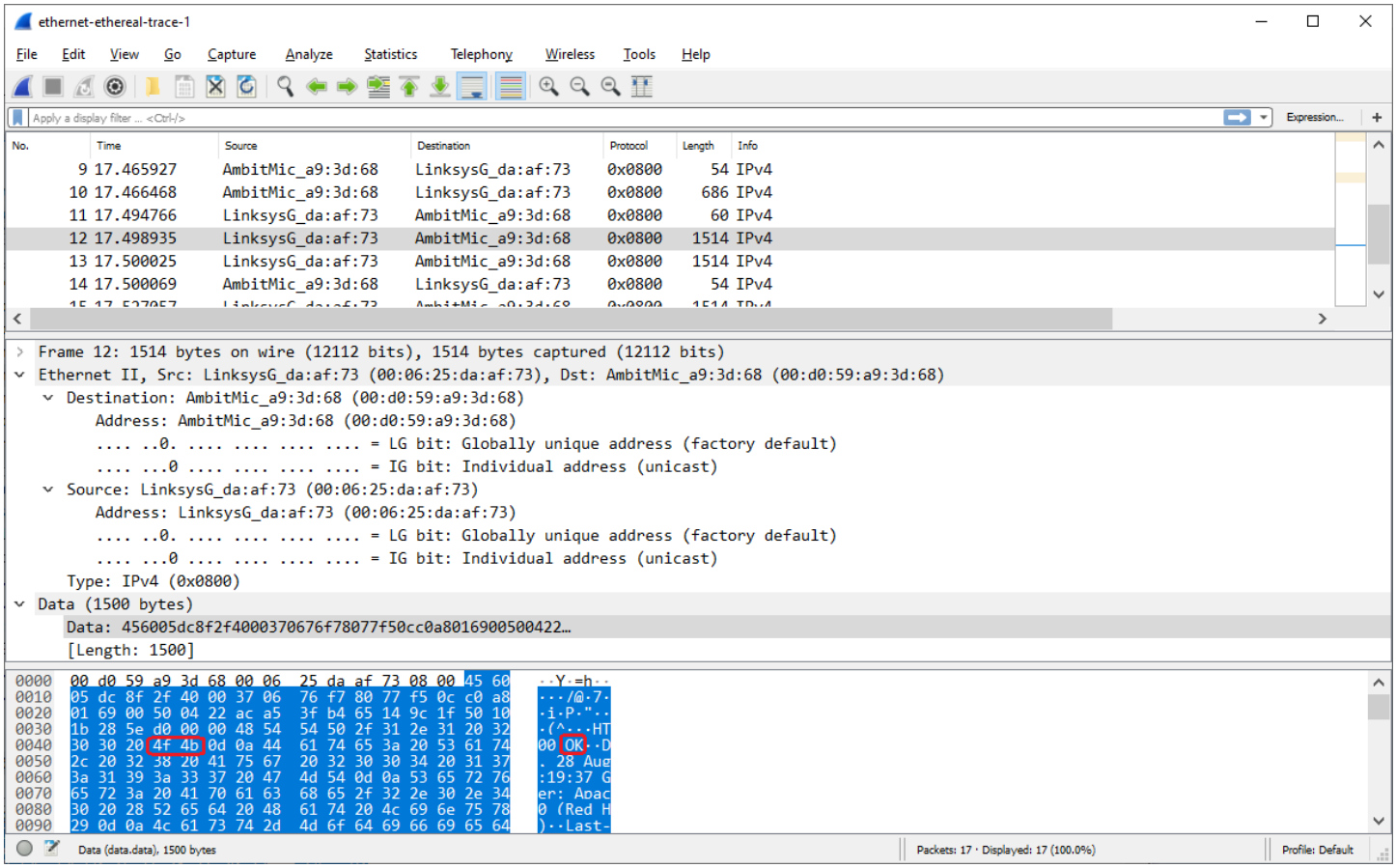
7) Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

   The hex value for the two-byte Frame type field is 0x800. This value corresponds with the IPv4 upper layer 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 ASCII “O” in “OK” occurs after 67 bytes from the very start of the ethernet frame.

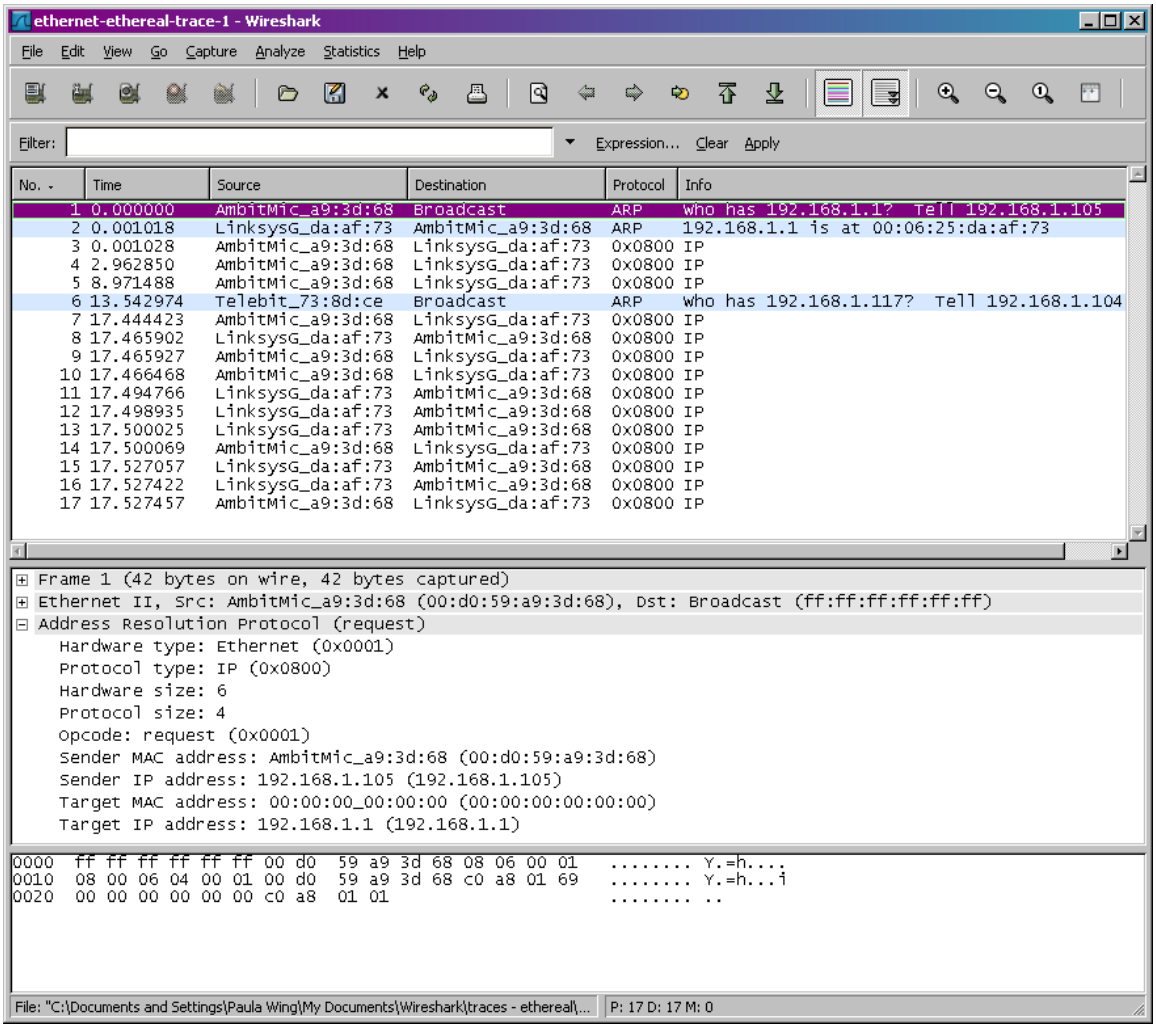


The Windows *arp* command with no arguments will display the contents of the ARP cache on your computer. Run the *arp* command.

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

The Internet Address column specifies the IP address used for address resolution. The Physical Address column specifies the MAC address used for address resolution. The Type column specifies the IP type used for address resolution, which can either be a static or dynamic IP address.

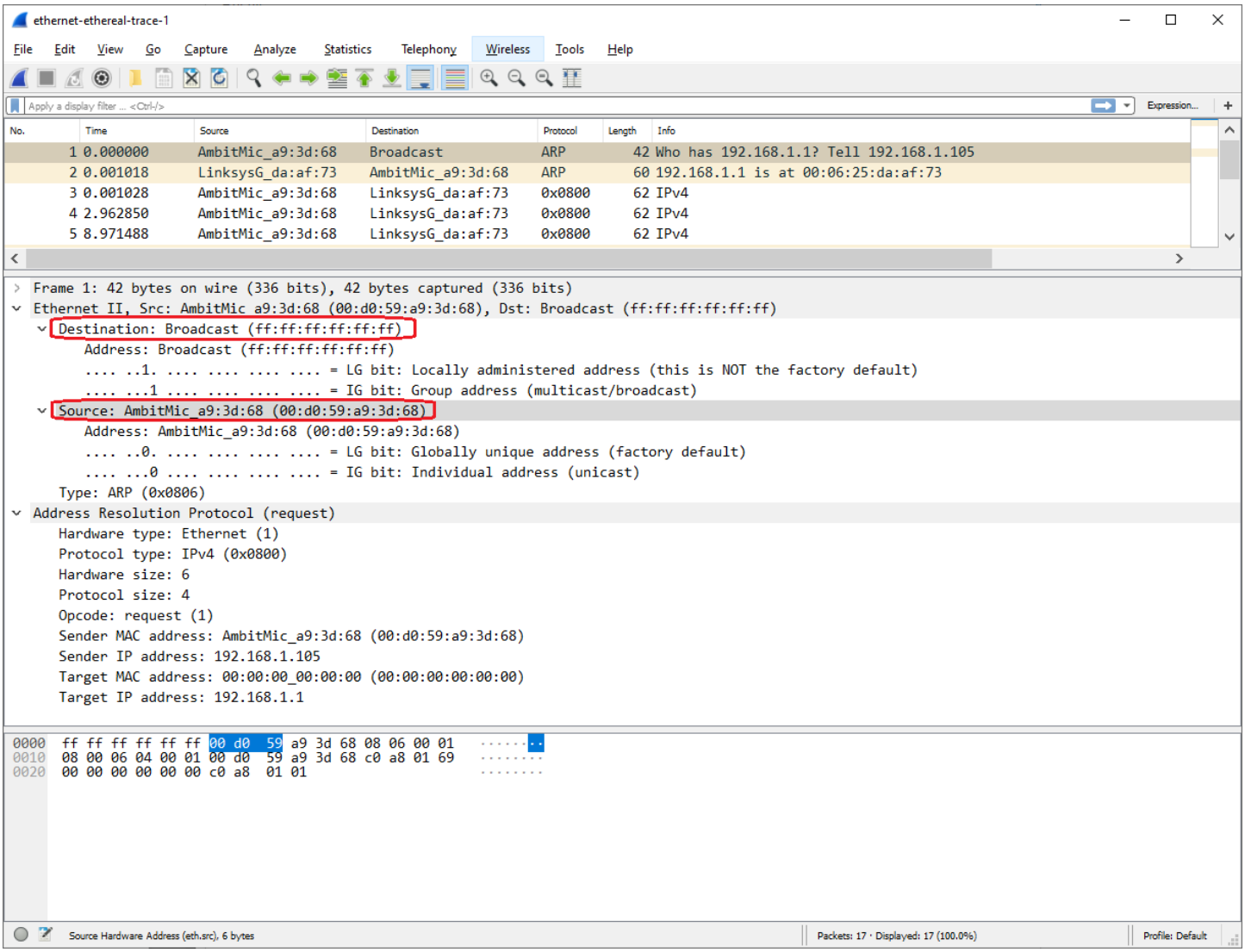
```
E:\Git\OSU\CS372>arp -a

Interface: 192.168.10.2 --- 0xc
  Internet Address      Physical Address      Type
  192.168.10.1          1c-b7-2c-c6-cb-08     dynamic
  192.168.10.189        00-16-6c-a3-12-90     dynamic
  192.168.10.255        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
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```



In the example above, the first two frames in the trace contain ARP messages (as does the 6th message). The screen shot above corresponds to the trace referenced in footnote 1. Answer the following questions:

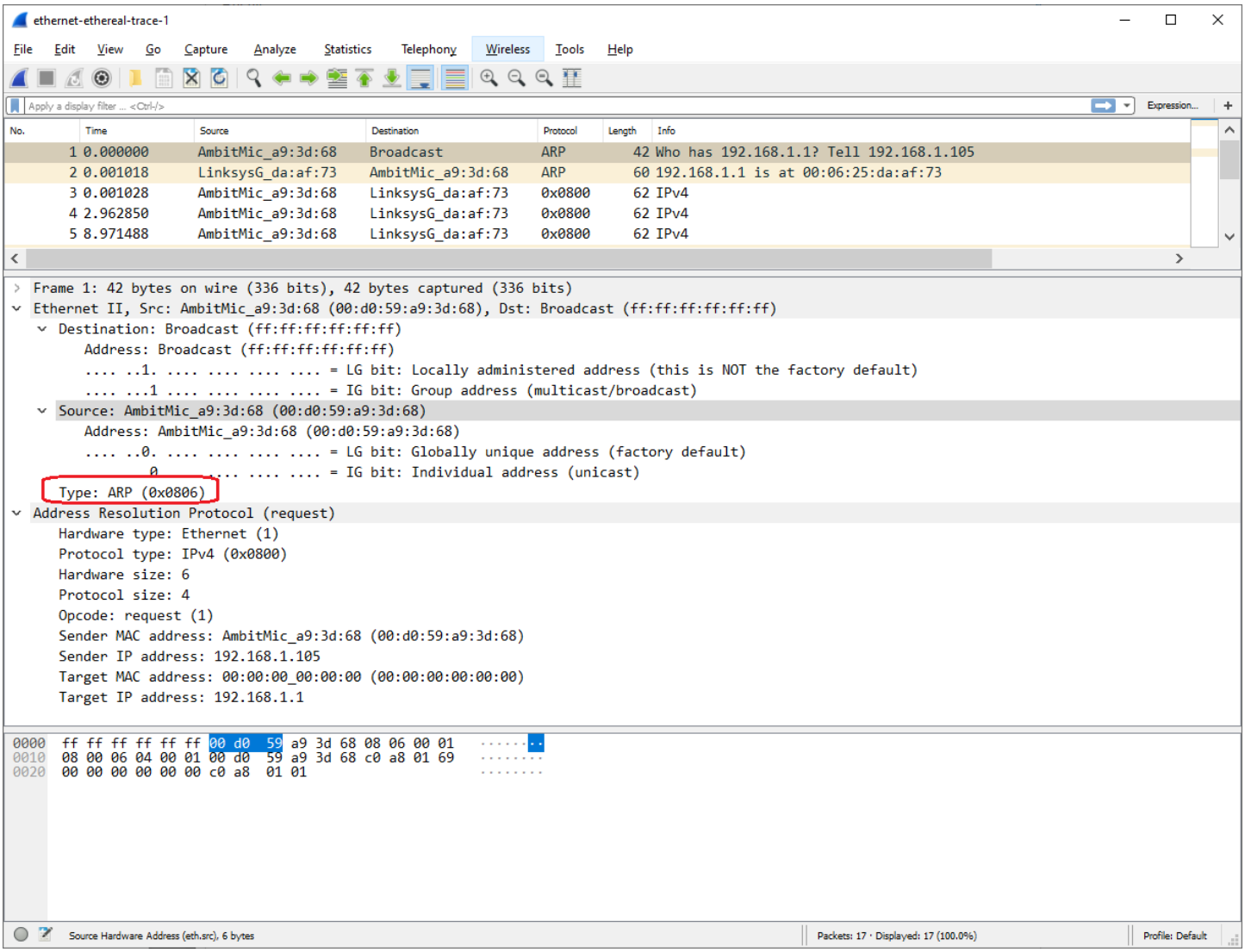
10) What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

The hex value for the source address containing the ethernet frame is 00:d0:59:a9:3d:68. The hex value for the destination address containing the ethernet frame is ff:ff:ff:ff:ff:ff.



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

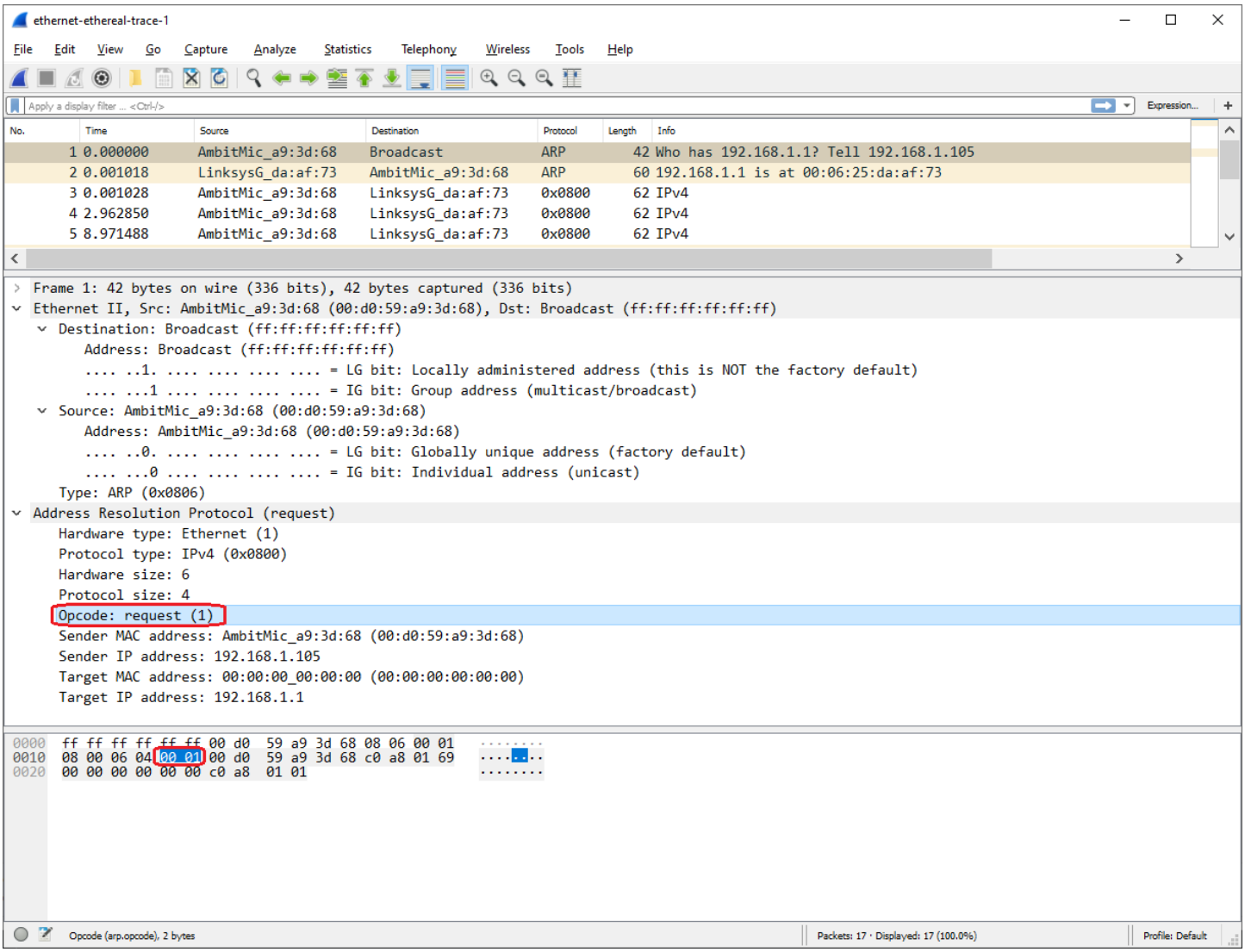
The hex value for the two-byte Ethernet Frame type field is 0x0806. This value corresponds with the ARP upper layer protocol.



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.

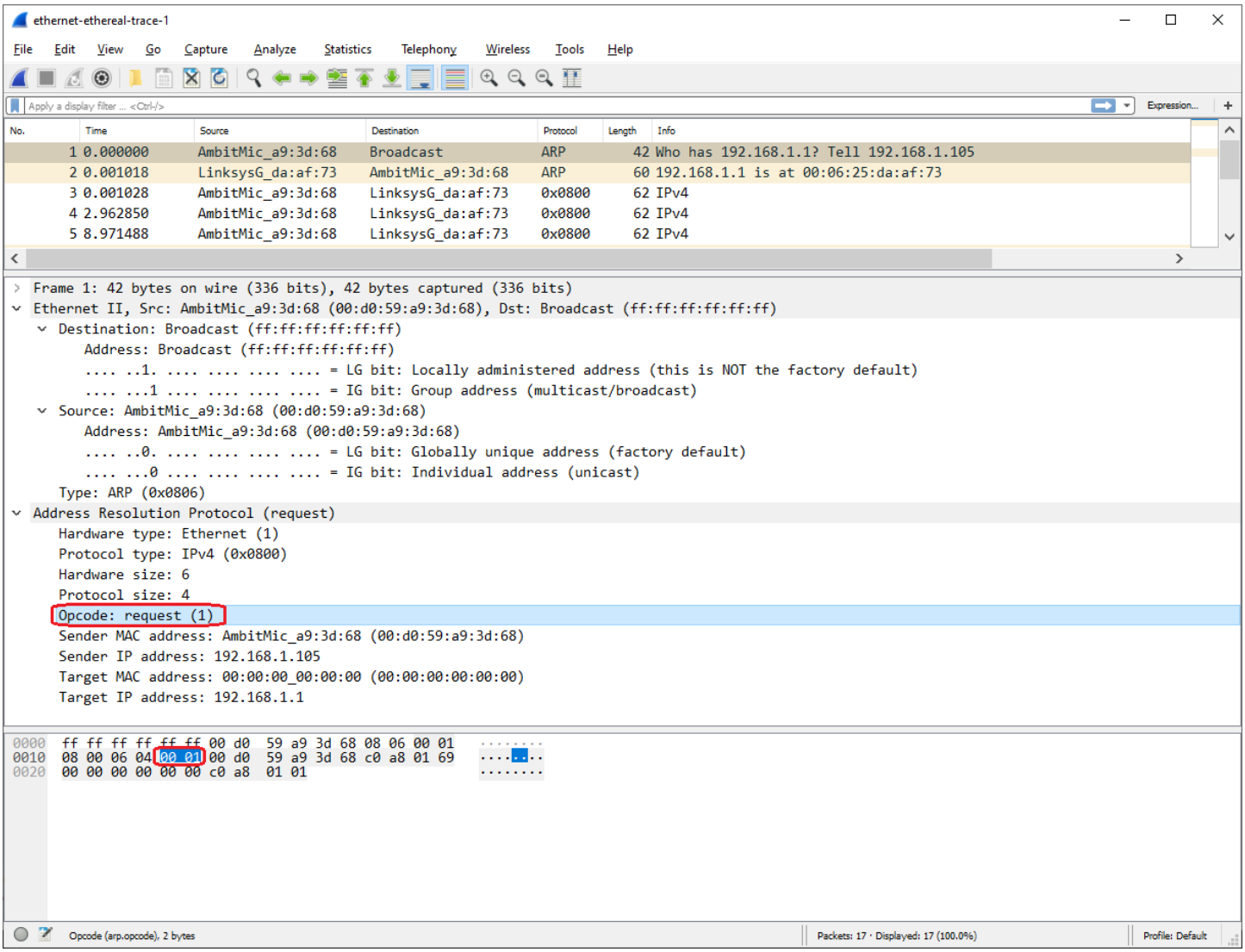
a. How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

The ARP opcode field begins after 20 bytes from the start of the ethernet frame.



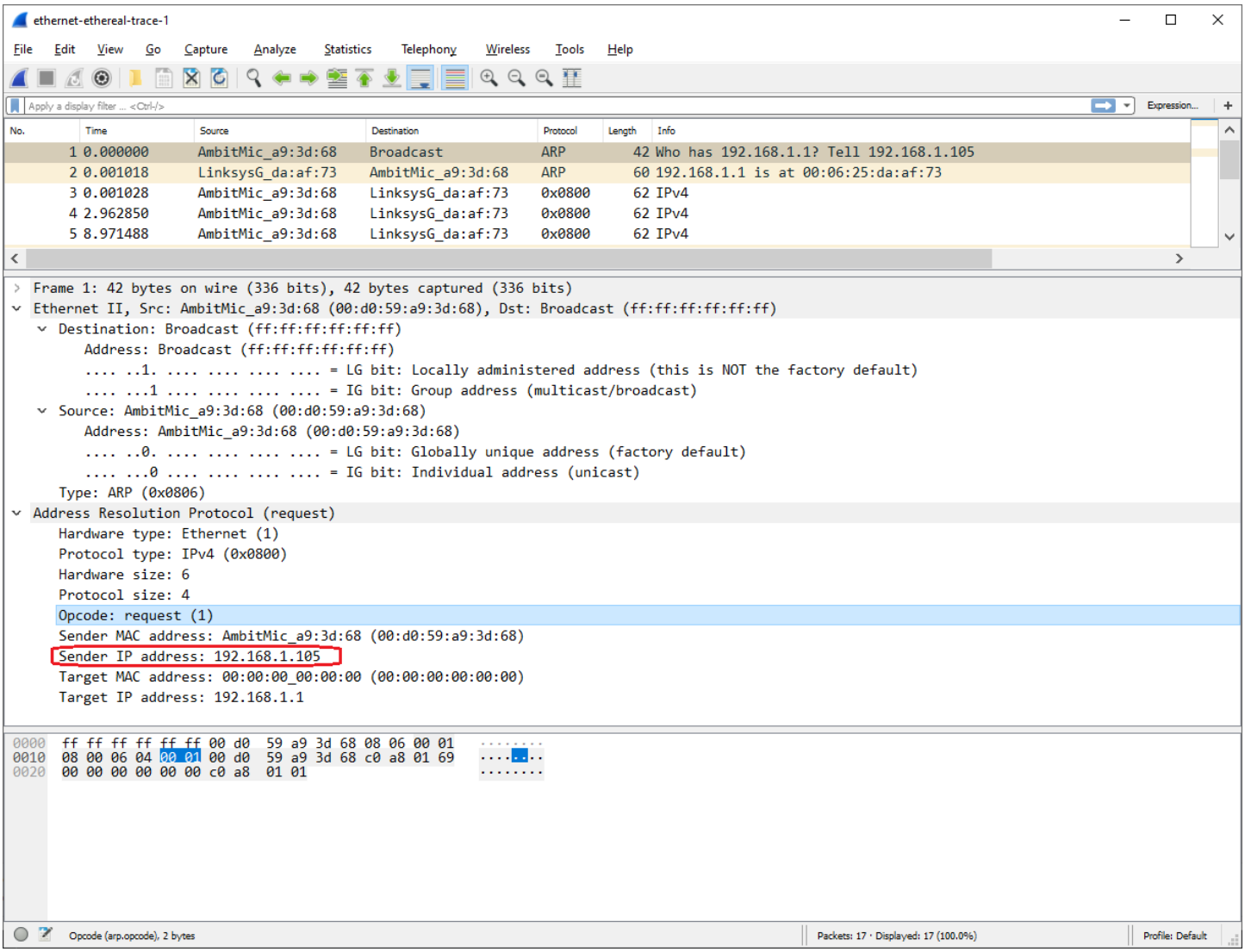
b. What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

The value of the ARP opcode field is 1.



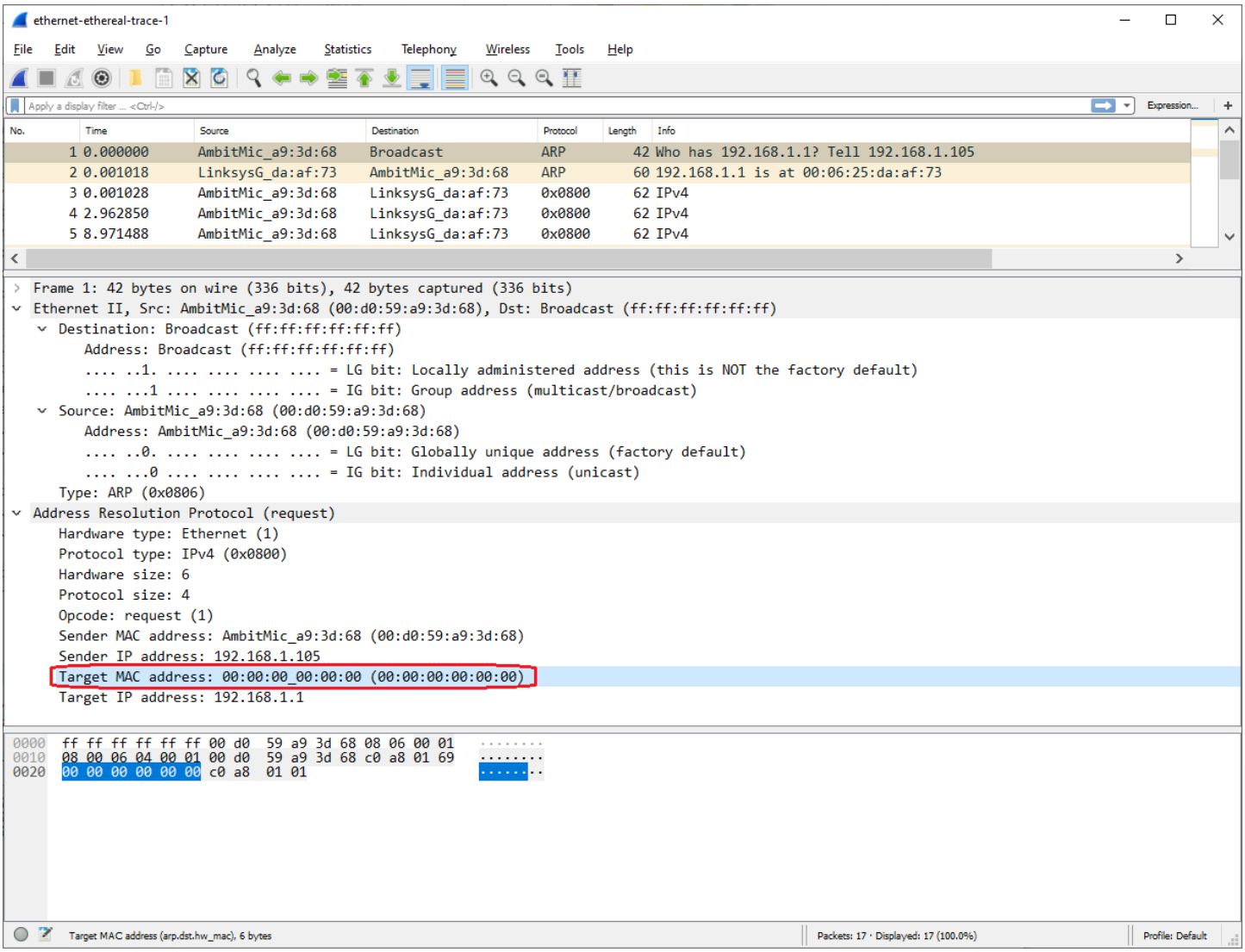
c. Does the ARP message contain the IP address of the sender?

Yes, the IP address of the sender is 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?

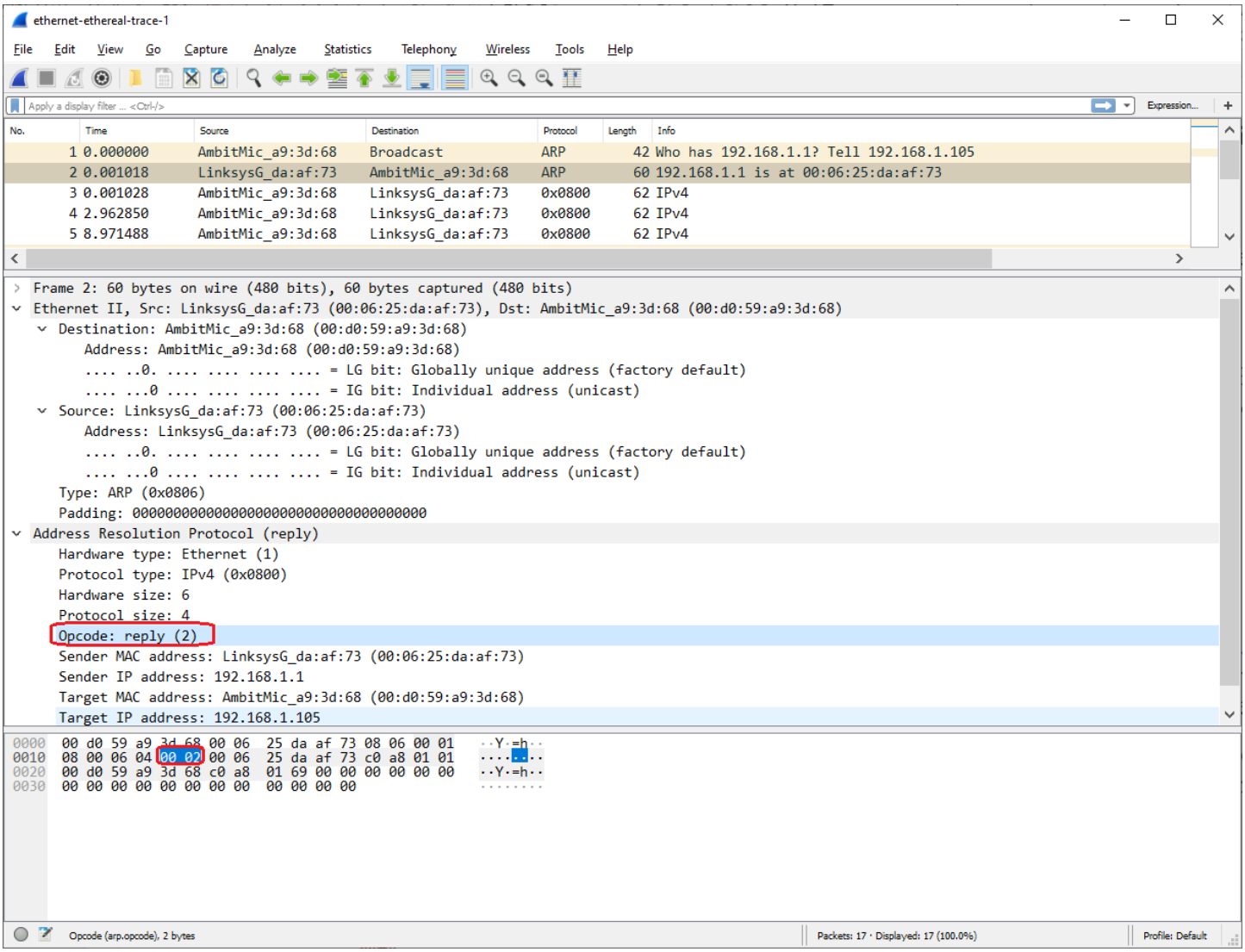
The Target MAC address field, which is set to 00:00:00:00:00:00, is the Ethernet address of the machine whose corresponding IP address is being queried.



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

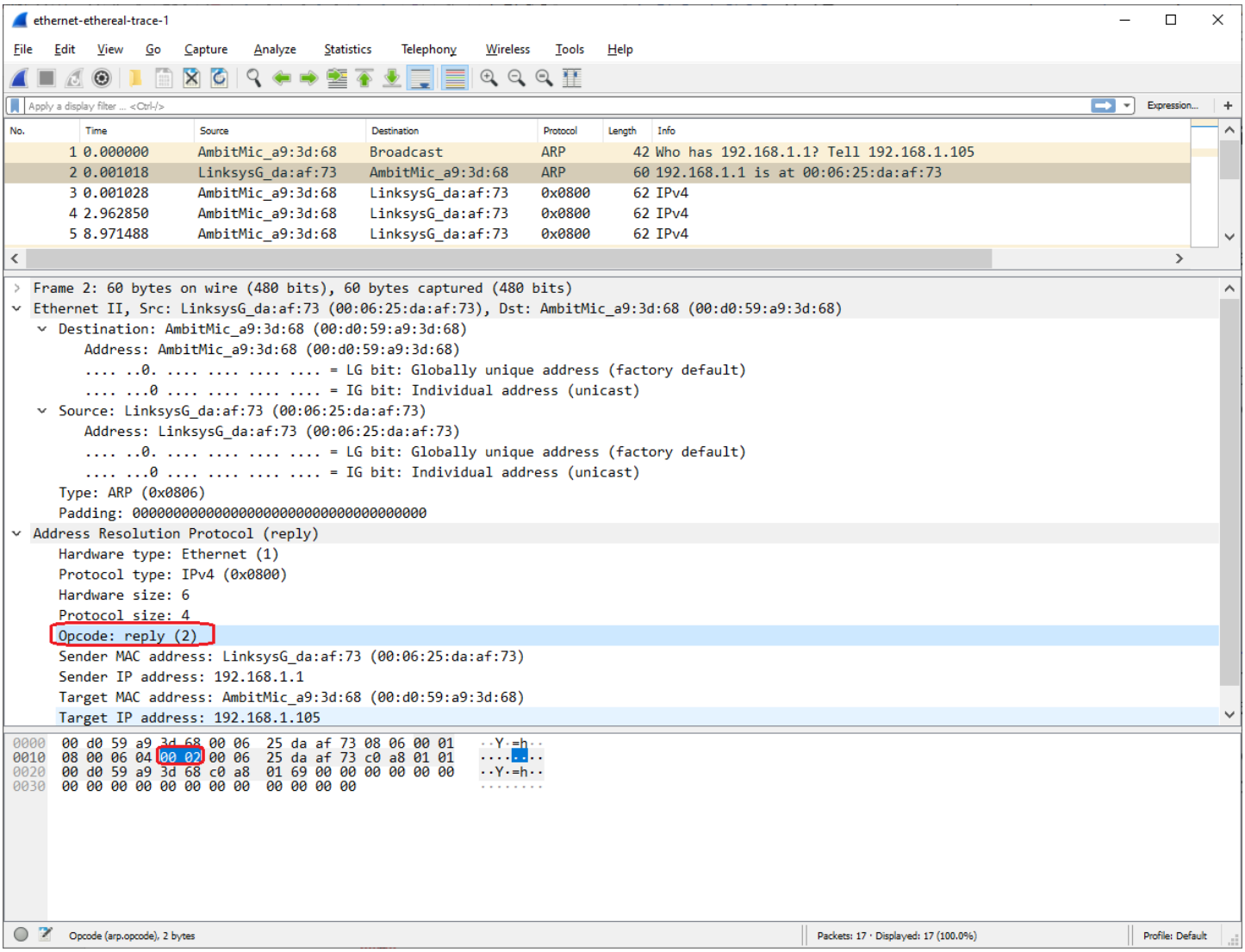
a. How many bytes from the very beginning of the Ethernet frame does the ARP *opcode* field begin?

The ARP reply's opcode occurs after 20 bytes from the start of the ethernet frame.



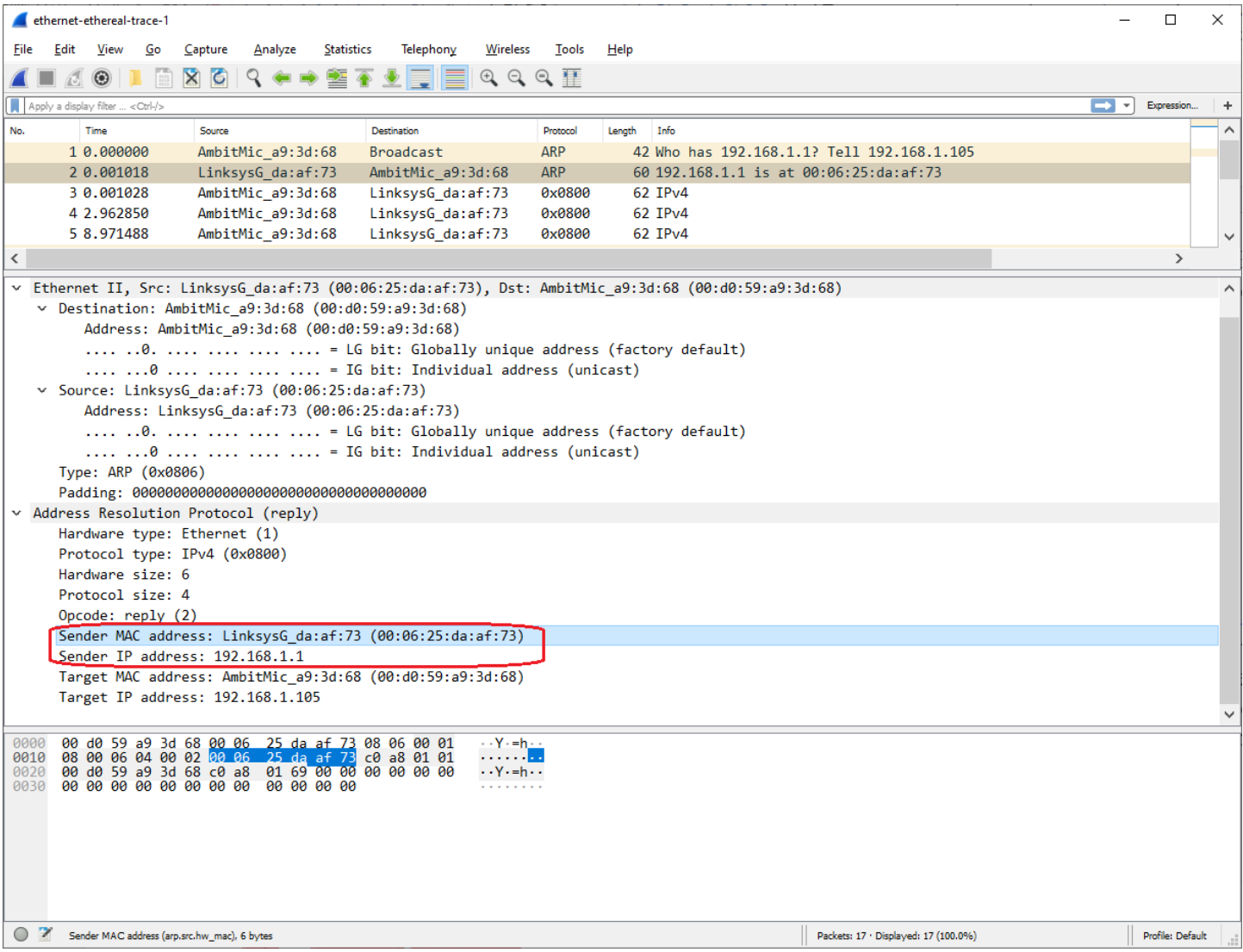
b. What is the value of the *opcode* field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

The value of the ARP opcode is 2, which corresponds with the “reply” opcode value.



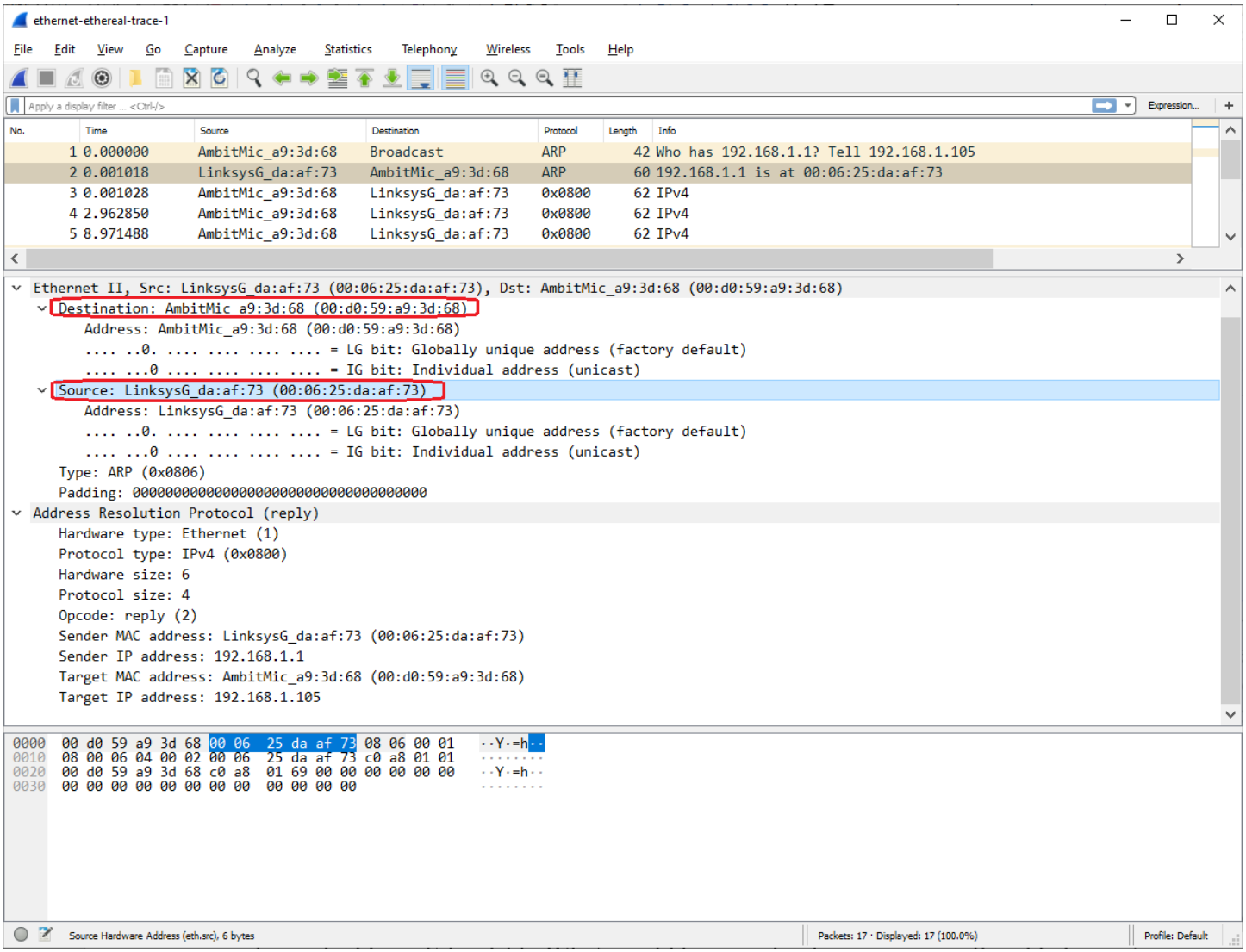
c. Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?

The Sender MAC address (00:06:25:da:af:73) and Sender IP address (192.168.1.1) is the "answer" to 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?

The source address is 00:06:25:da:af:73 and the destination address is 00:d0:59:a9:3d:68 in the ethernet frame containing the ARP reply message.



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 reply sent in response to the ARP request in packet 6 because the router will only send an ARP reply to the source ethernet address for an ARP request. In this case, the wireshark trace was collected 1st ARP request's sender at source address 00:d0:59:a9:3d:68, whereas the 2nd ARP request was sent from a second device at source address 00:80:ad:73:8d:ce. Since the router sent the ARP reply to the 2nd device, the 1st device did not receive the ARP reply for the 2nd device. However, the 1st device received the ARP request from the 2nd device because the 2nd device broadcasted an ARP request to all other devices on the same network.

16) 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?

If you manually added an entry with the correct address but wrong ethernet address, then once a frame reaches the router, the router will remove the IP address from the ethernet frame, use ARP to detect the correct destination MAC address based on the IP address, and proceed to forward the frame using the correct IP and MAC addresses.

17) 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.

The default amount of time that an entry remains in the ARP cache before being removed is 37.5 seconds for my Windows 10 system. This information is based on KB949589 (https://support.microsoft.com/en-us/help/949589/description-of-address-resolution-protocol-arp-caching-behavior-in-win). In KB949589, it says "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", which aligns with the definition of an ARP cache timeout value. The log from my Win10 system shows that the Reachable State is set to 37500 ms, which is equal to 37.5 seconds.

```
C:\Windows\system32>netsh interface ipv4 show interfaces

Idx     Met         MTU          State                Name
---  ----------  ----------  ------------  ---------------------------
  1          75  4294967295  connected     Loopback Pseudo-Interface 1
 12          35        1500  connected     Wi-Fi
  4          65        1500  disconnected  Bluetooth Network Connection
 11          25        1500  disconnected  Local Area Connection* 1
 17           5        1500  disconnected  Ethernet
  3          25        1500  disconnected  Local Area Connection* 2


C:\Windows\system32>netsh interface ipv4 show interface 12

Interface Wi-Fi Parameters
----------------------------------------------
IfLuid                             : wireless_32768
IfIndex                            : 12
State                              : connected
Metric                             : 35
Link MTU                           : 1500 bytes
Reachable Time                     : 37500 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
RA Based DNS Config (RFC 6106)     : disabled
DHCP/Static IP coexistence         : disabled
```