Họ tên : Lê Bảo Khánh

MSSV : 1911363

Lớp : L01

**LAB 6**

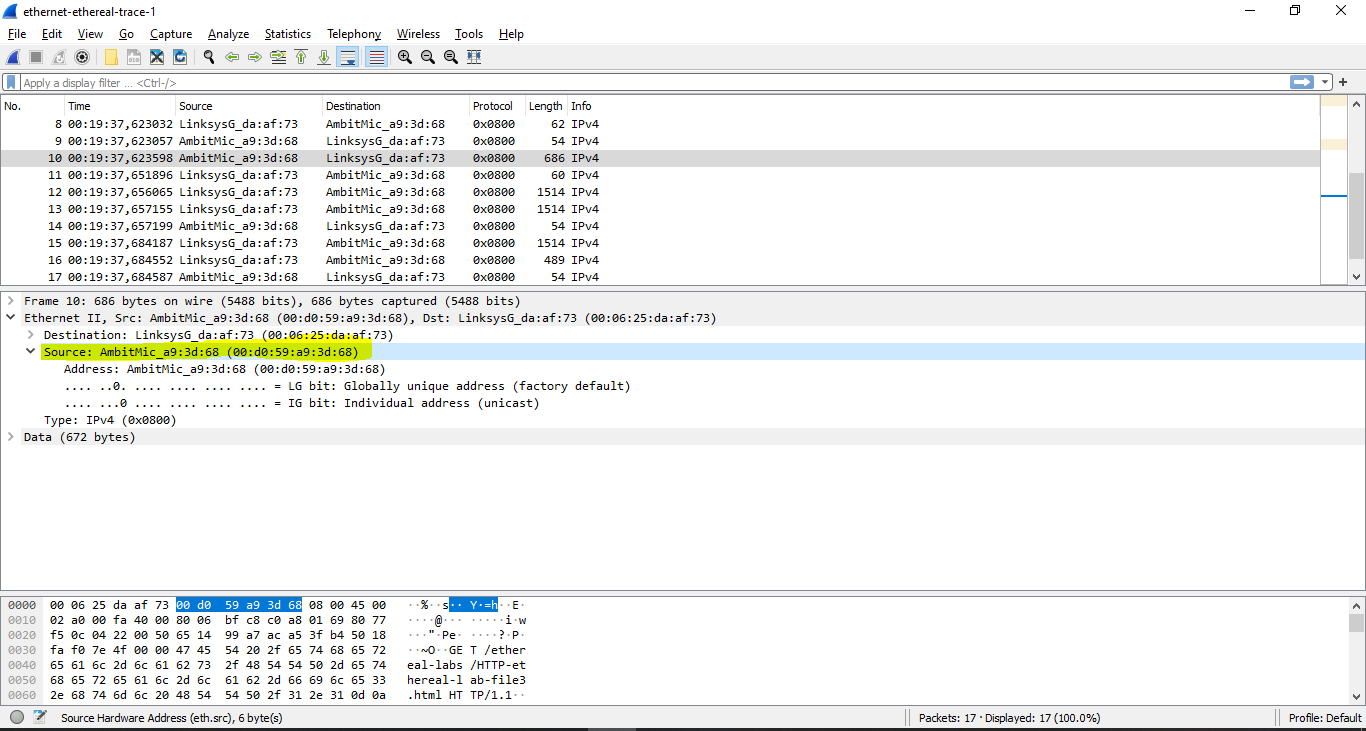
(Using the file ethernet--ethereal-trace-1)

**1. Capturing and analyzing Ethernet frames**

**Question 1**: What is the 48-bit Ethernet address of your computer?

**ANSWER:**

My 48-bit Ethernet address is 00:d0:59:a9:3d:68

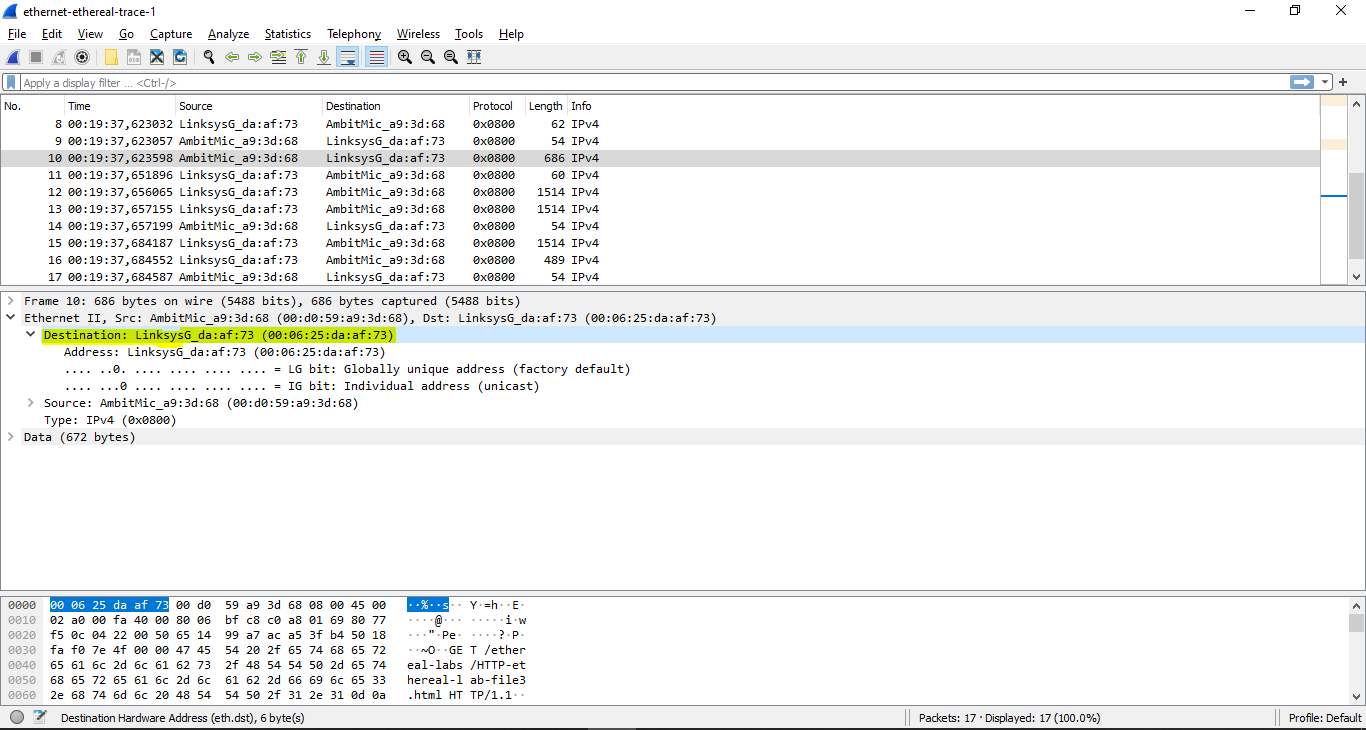


**Question 2:** What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address?

**ANSWER:**

The 48-bit destination address: 00:06:25:da:af:73  
(This is not the Ethernet address of gaia.cs.umass.edu)

It is the address of the router which the computer has to go through in order to reach the destination. (internet gateway address)

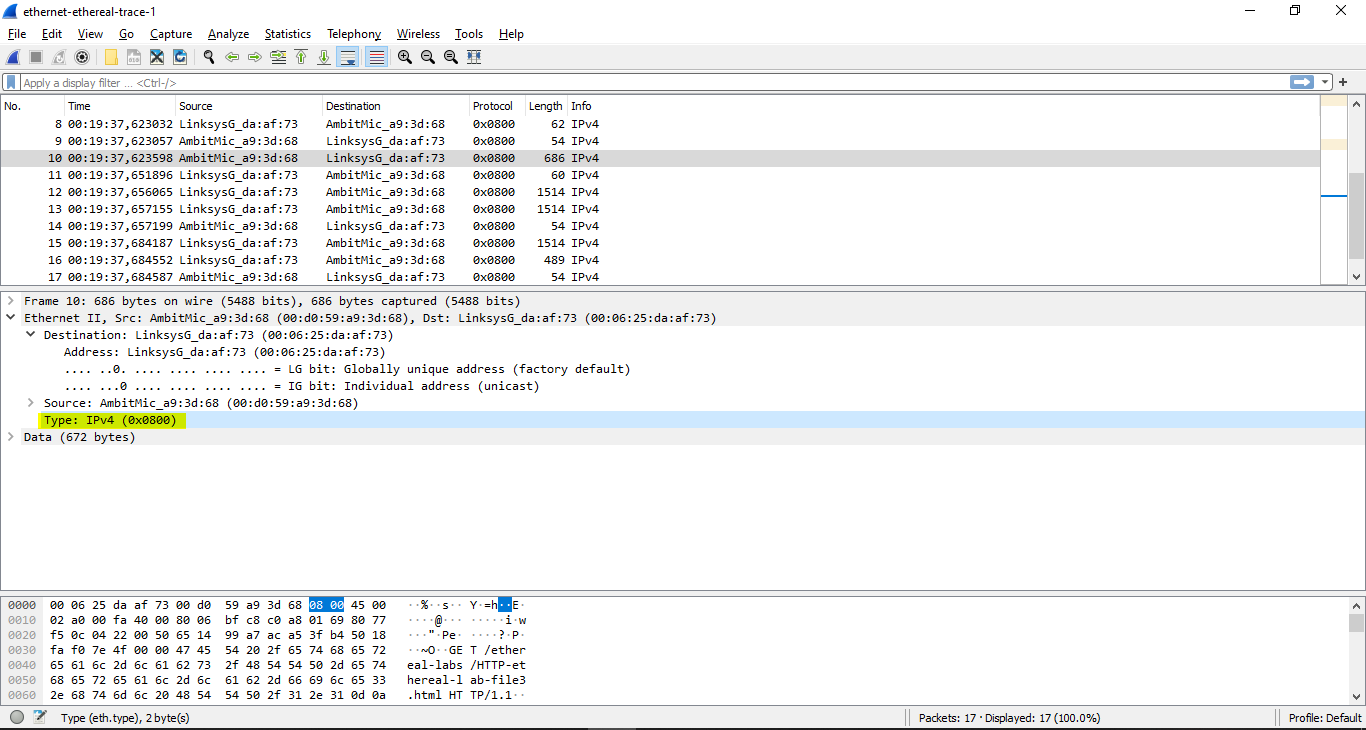


**Question 3:** Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

**ANSWER:**

The hexadecimal value for the two-byte Frame type field: 0x00000800

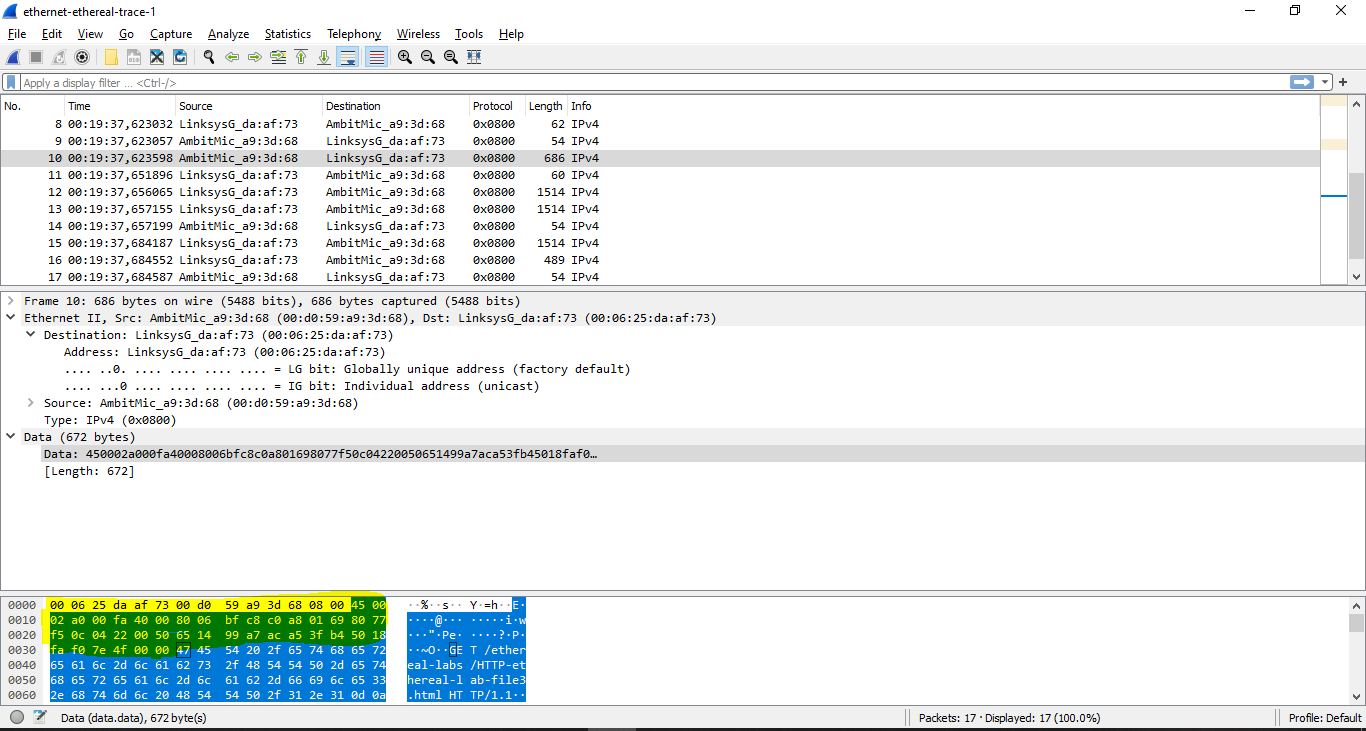
=> This is correspond to IP protocol



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

**ANSWER:**

After 54 bytes, the “G” in “GET” appears.



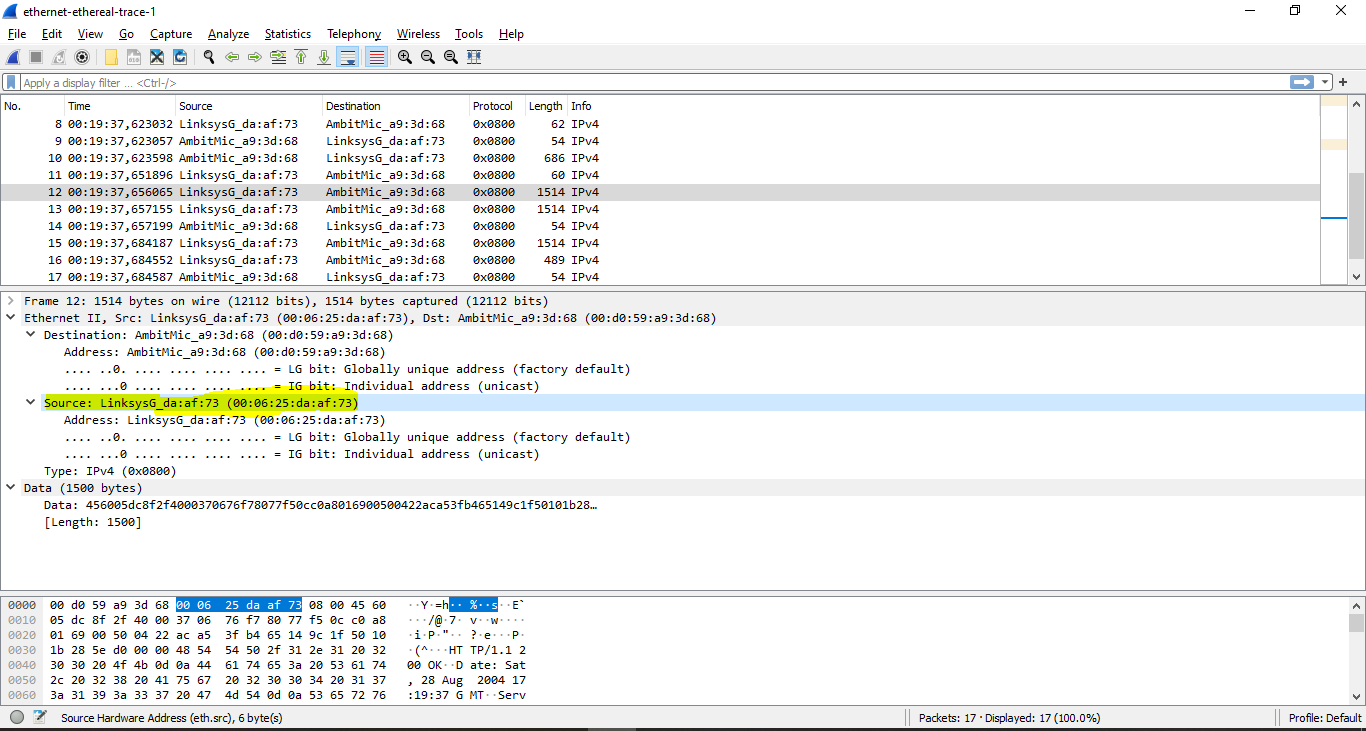
**Question 5**: What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?

**ANSWER:**

The value of the Ethernet source address: 00:06:25:da:af:73

This is not the address of the computer / of gaia.cs.umass.edu,

This is the address of the router

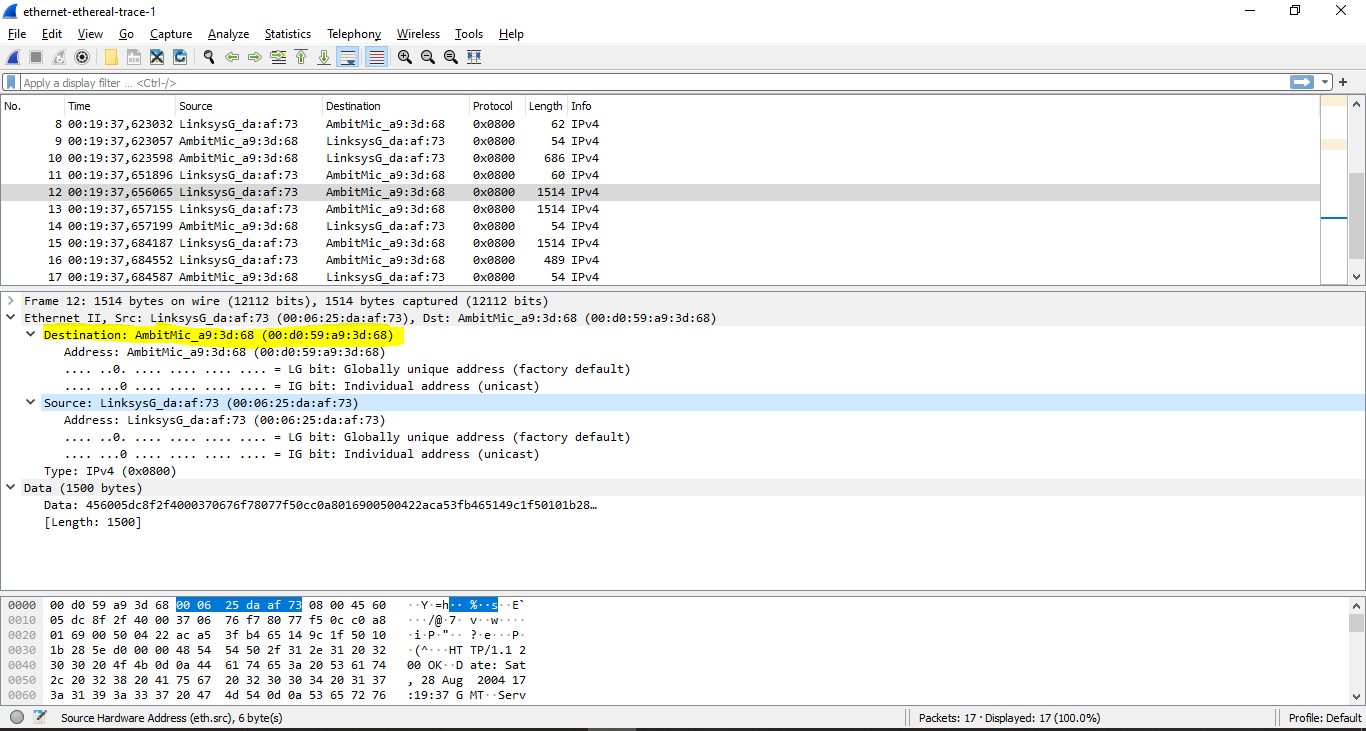


**Question 6:** What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

**ANSWER:**

The destination address in the Ethernet frame is 00:d0:59:a9:3d:68

This is the Ethernet address of the computer

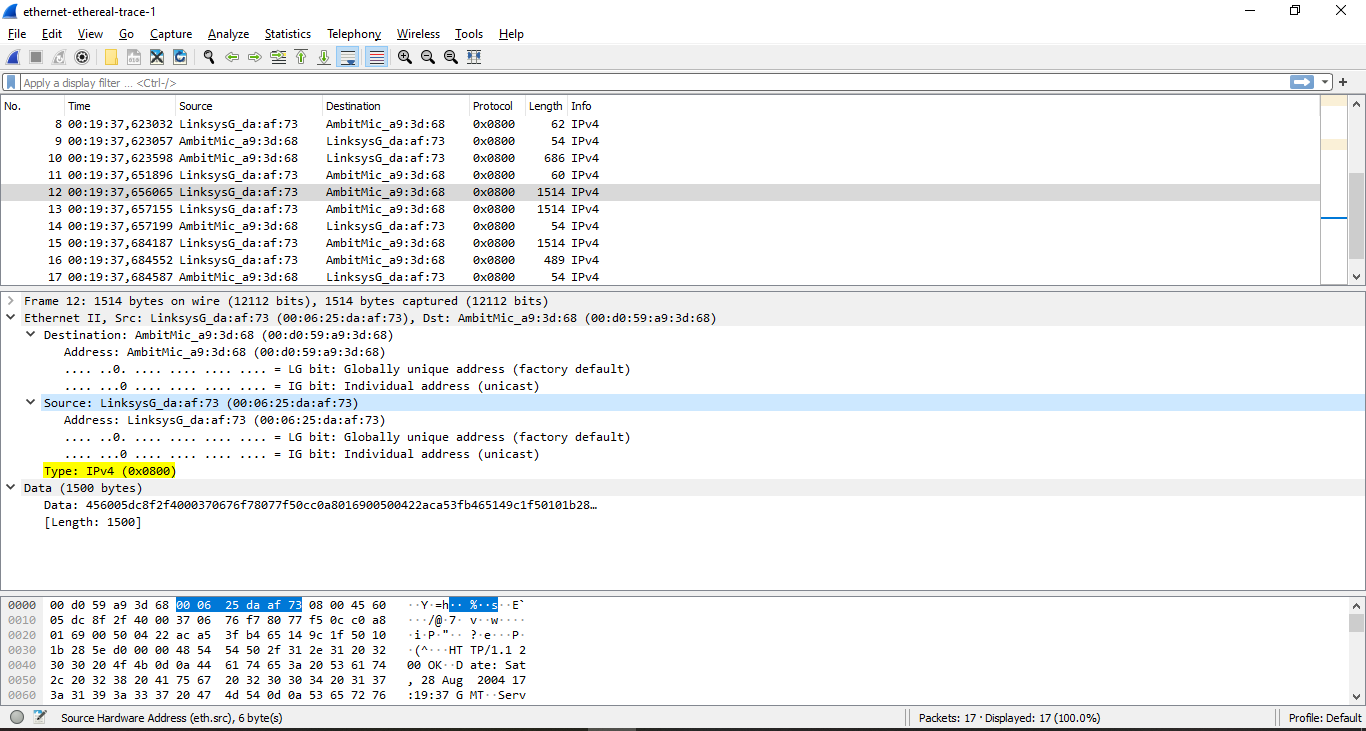


**Question 7:** Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

**ANSWER:**

The hexadecimal value for the two-byte Frame type field: 0x00000800

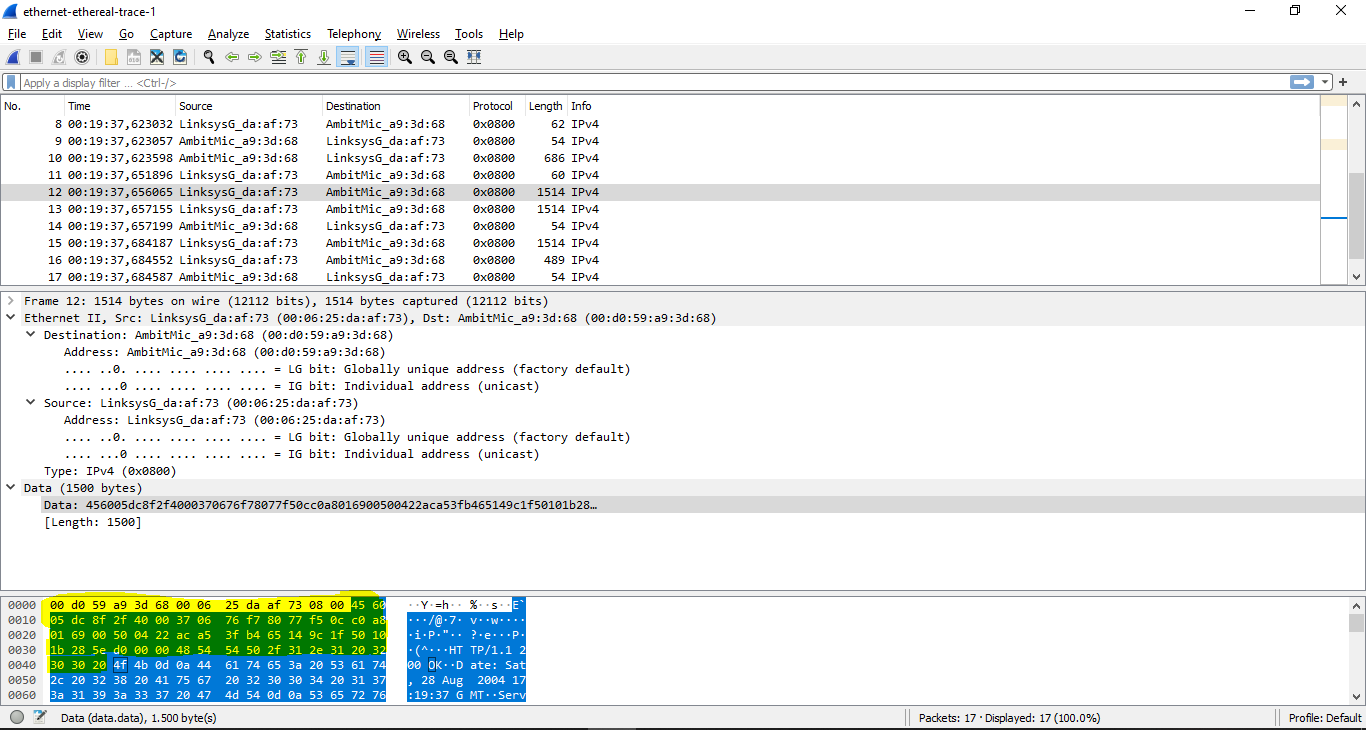
=> This is correspond to IP protocol



**Question 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?

**ANSWER:**

After 67 bytes, the “O” in “OK” appears.



**2. The Address Resolution Protocol**

**ARP Caching**

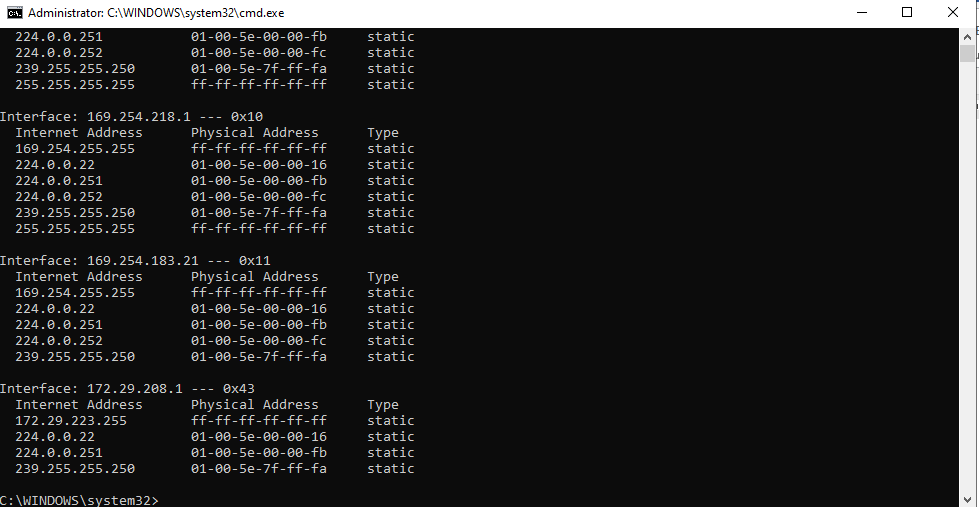
**Question 9:** Write down the contents of your computer’s ARP cache. What is the meaning of each column value?

**ANSWER:**

Internet Address column contains the IP address

Physical Address column contains the MAC address,

Type column indicates the protocol type.

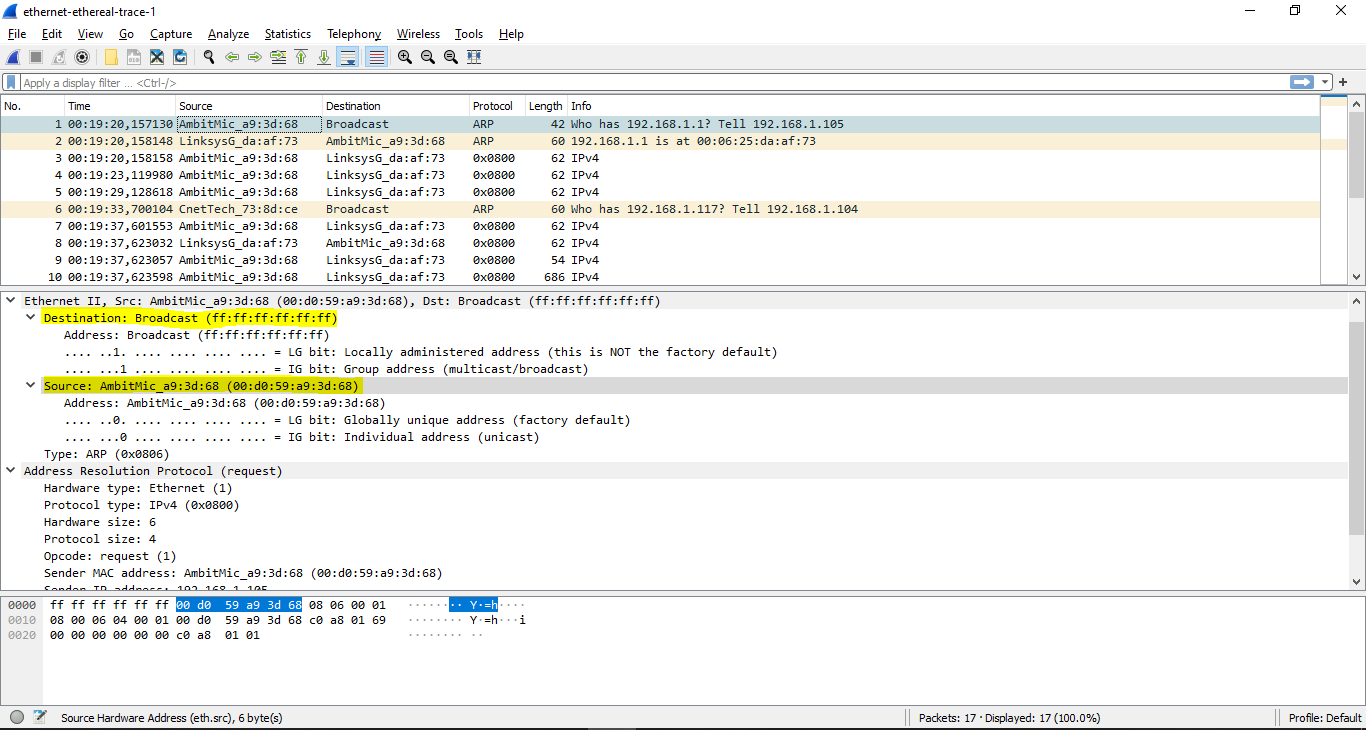


**Observing ARP in action**

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

**ANSWER:**

The Source address is 00:d0:59:a9:3d:68  
The Destination address is ff:ff:ff:ff:ff:ff

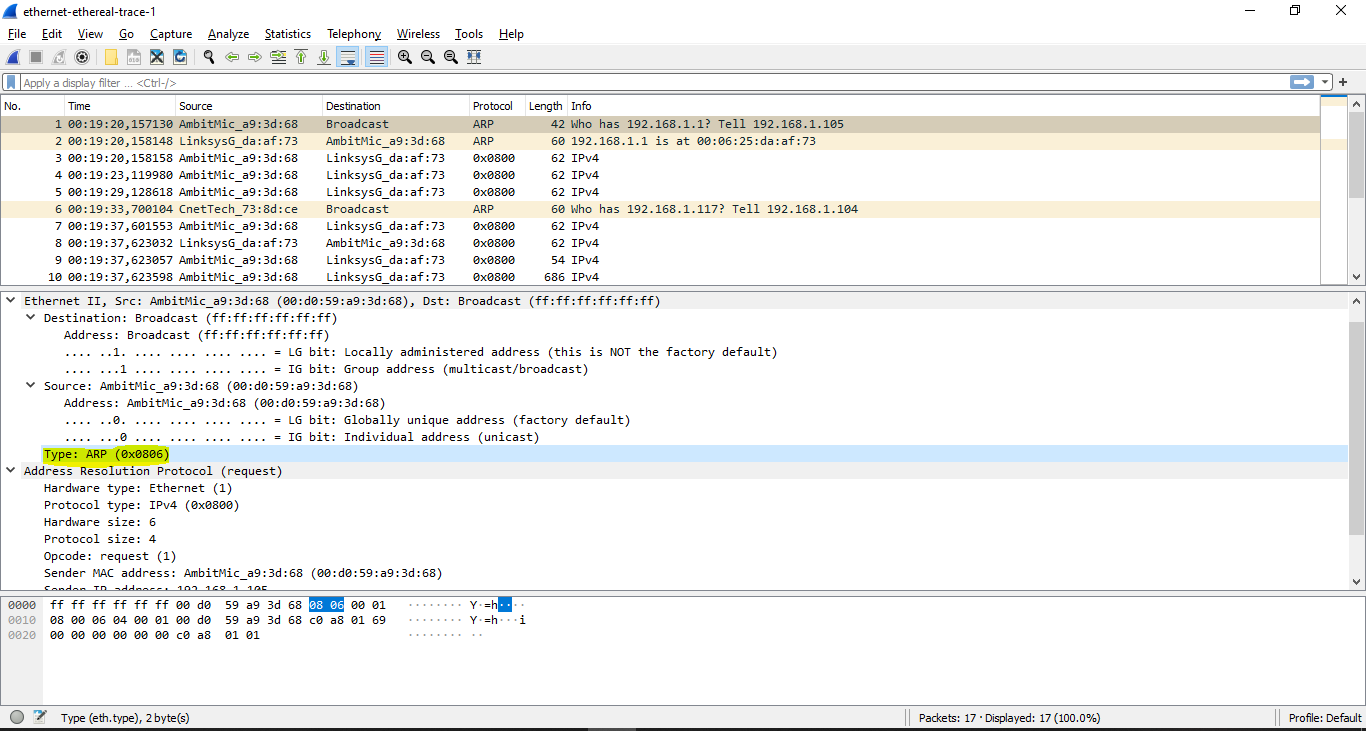


**Question 11:** Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

**ANSWER:**

The hex value for the two byte Ethernet frame is 0x00000806

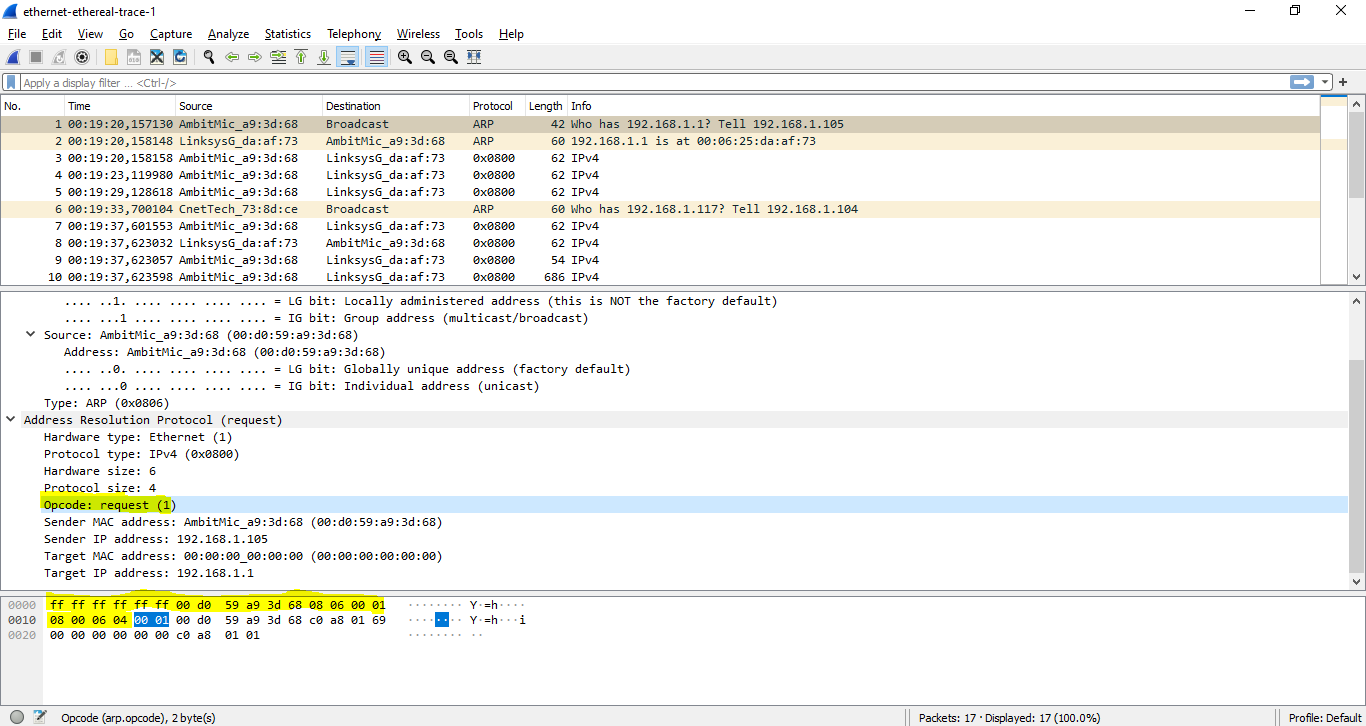
The corresponding upper layer protocol is ARP



**Question 12:**

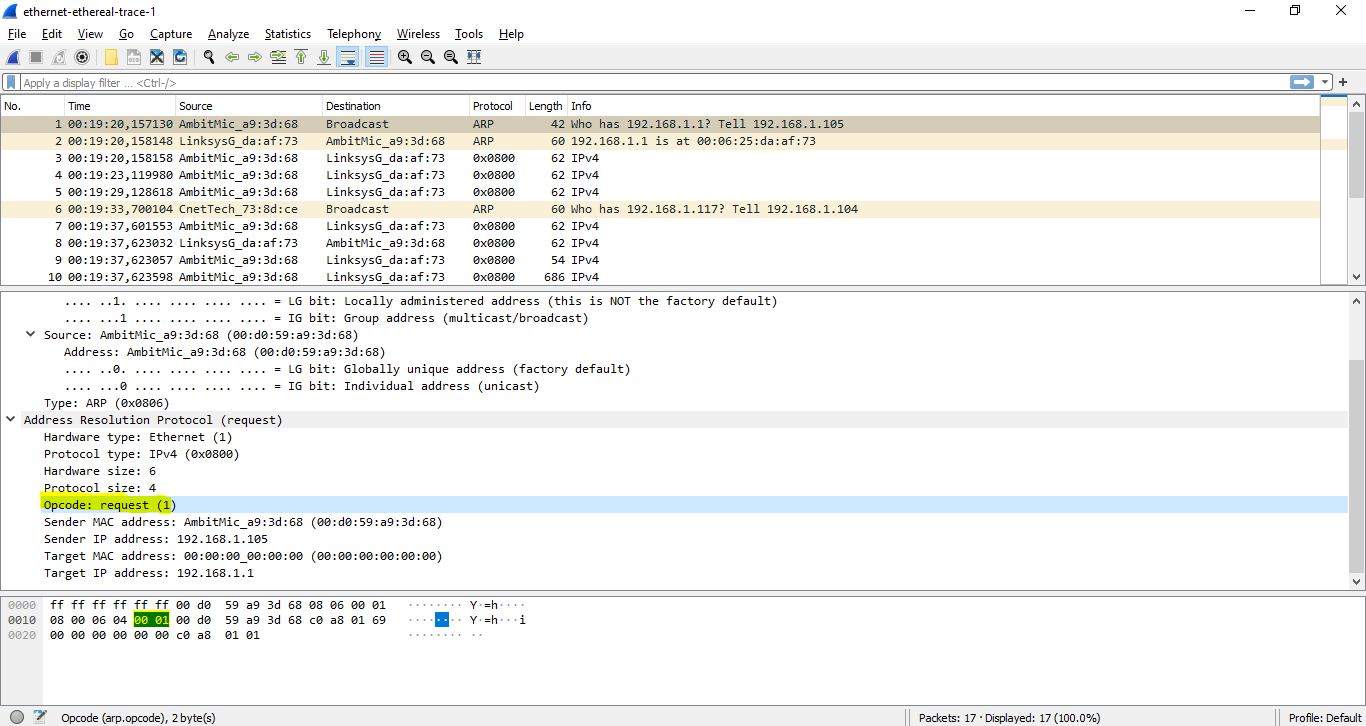
1. How many bytes from the very beginning of the Ethernet frame does the  
   ARP opcode field begin?

20 bytes



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

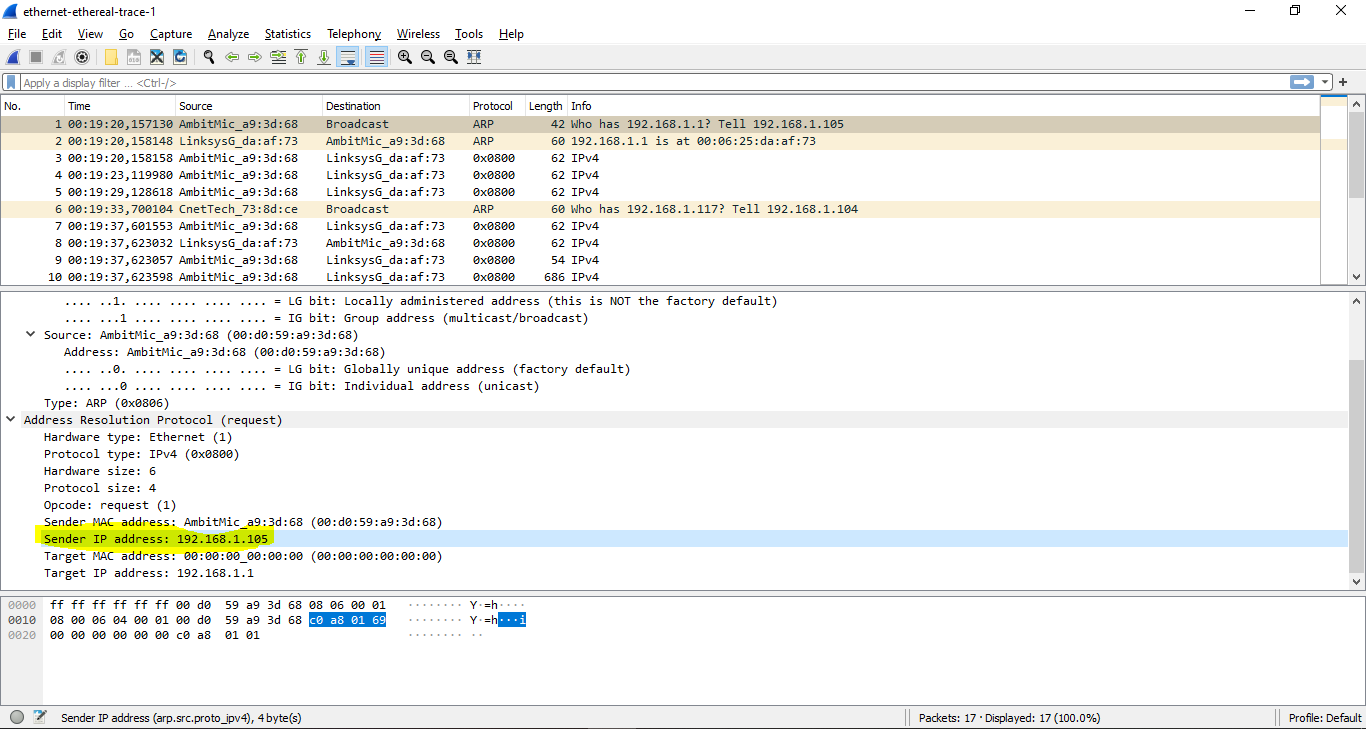
0x0001



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

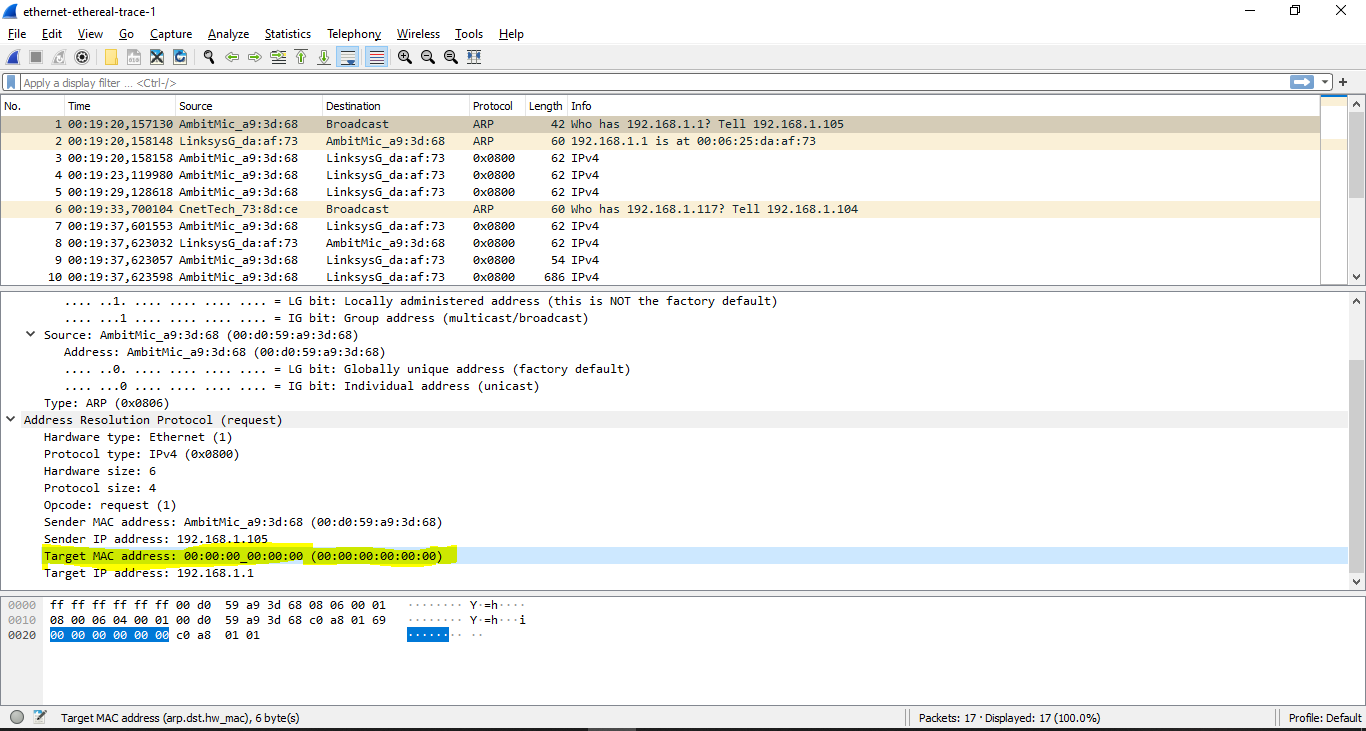
Yes

The ARP message contains the IP address 192.168.1.105



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

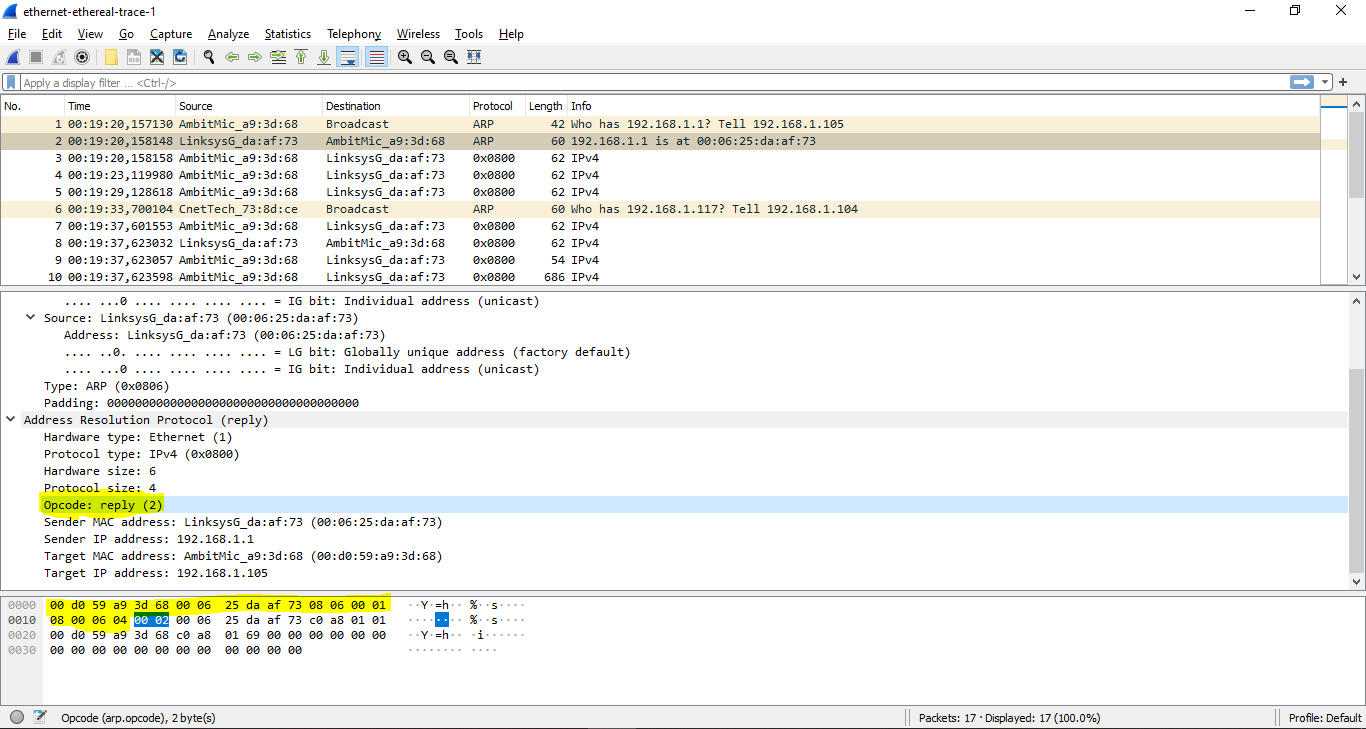
In the field Target MAC address 00:00:00:00:00:00



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

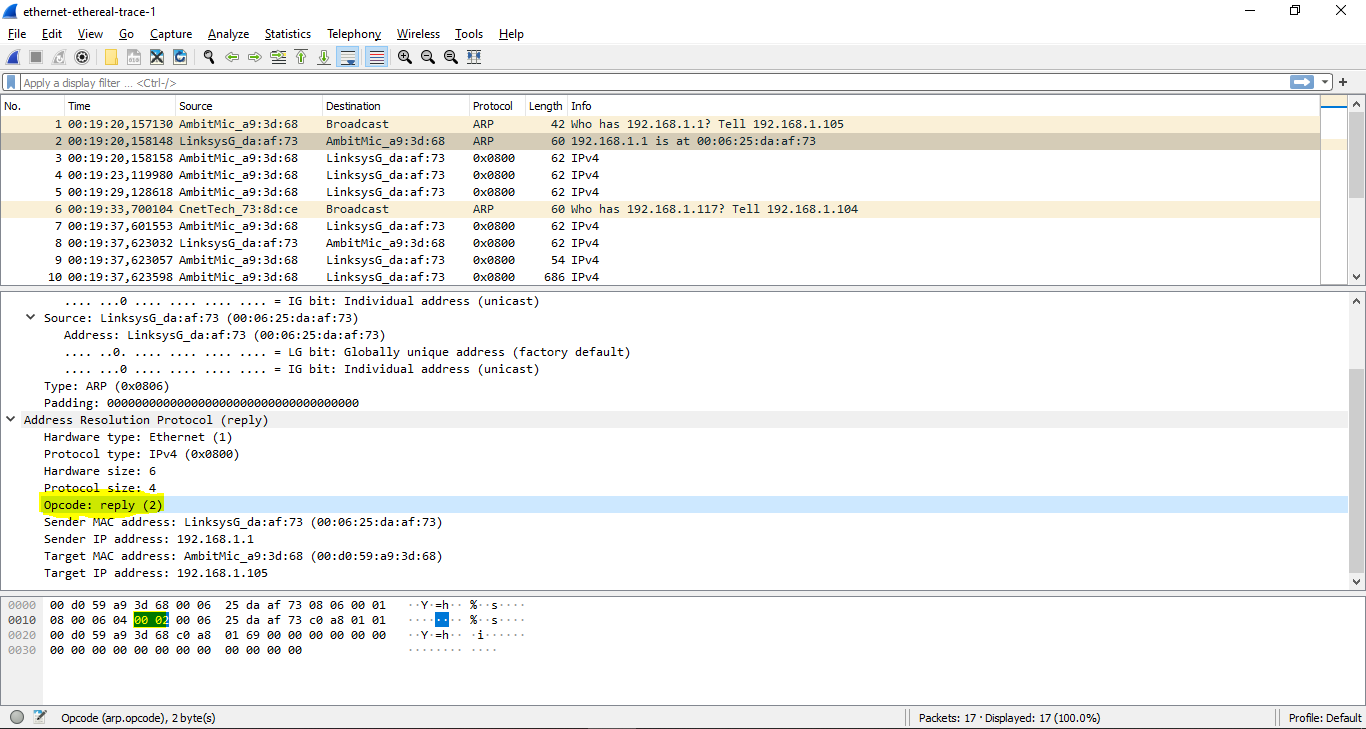
1. How many bytes from the very beginning of the Ethernet frame does the  
   ARP opcode field begin?

20 bytes



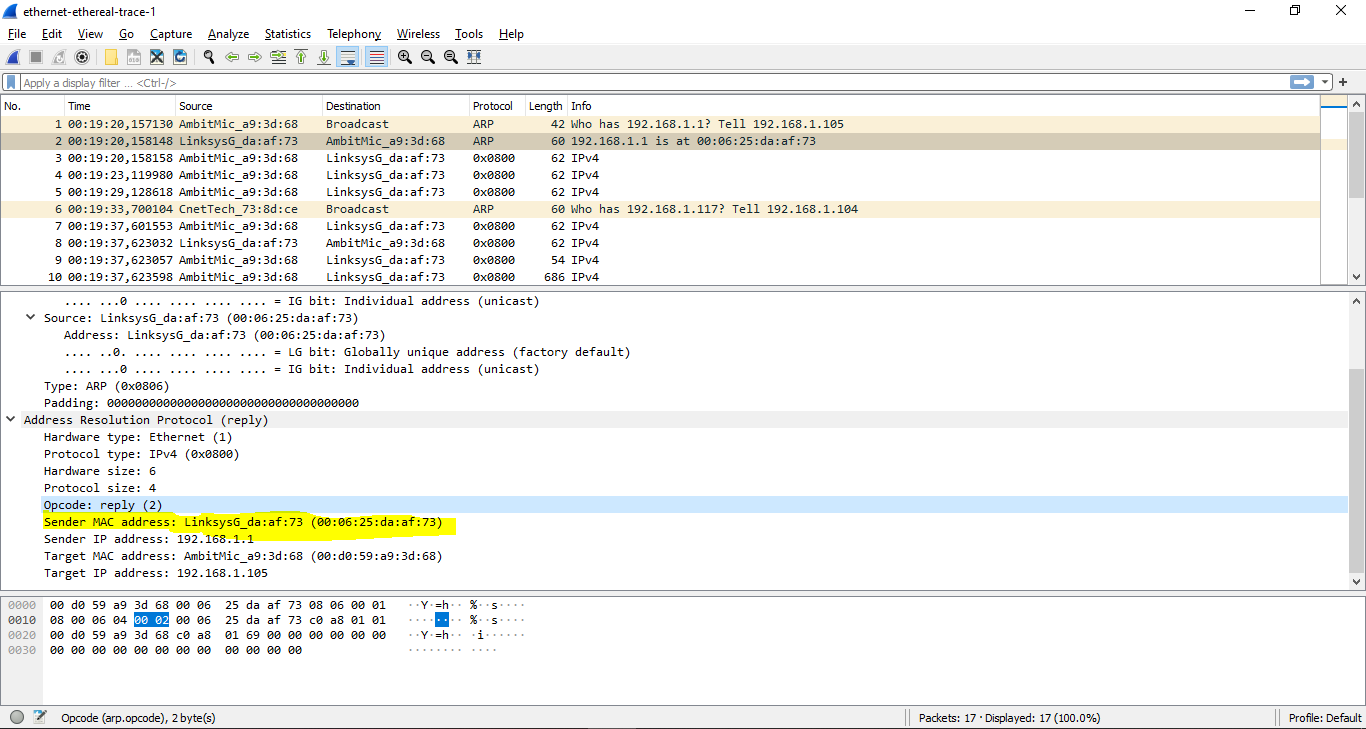
1. What is the value of the opcode field within the ARP-payload part of the  
   Ethernet frame in which an ARP response is made?

0x0002



1. 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?

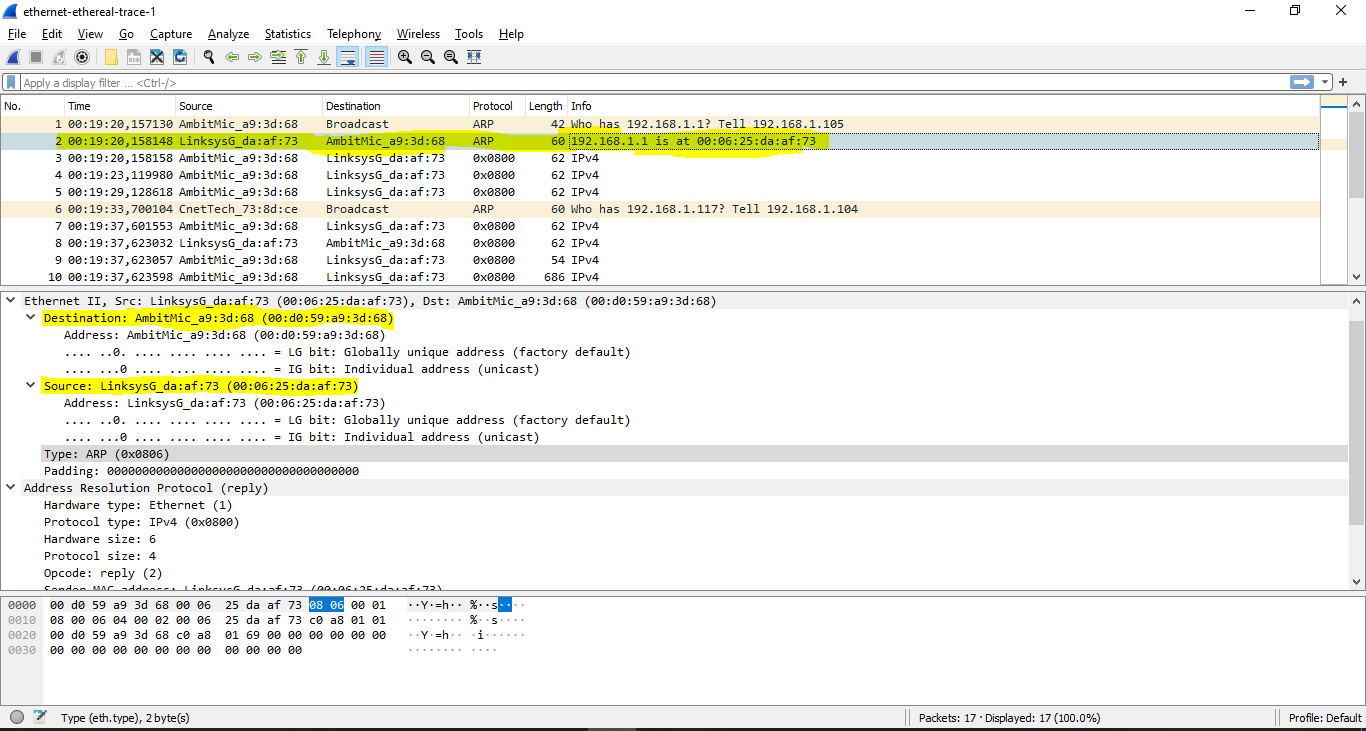
Sender MAC Address field



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

**ANSWER:**

The Source address is 00:06:25:da:af:73  
The Destination address is 00:d0:59:a9:3d:68



**Question 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?

**ANSWER:**

**Because we are not at the machine that sent the request.**

(The ARP request is broadcast, but **the ARP reply is not broadcast**. The reply will be sent directly to the computer who made the request directly => We can not see it)

**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?

**ANSWER:**

When the adapter/ router received the destination IP address, it would use the ARP to find the correct Ethernet address

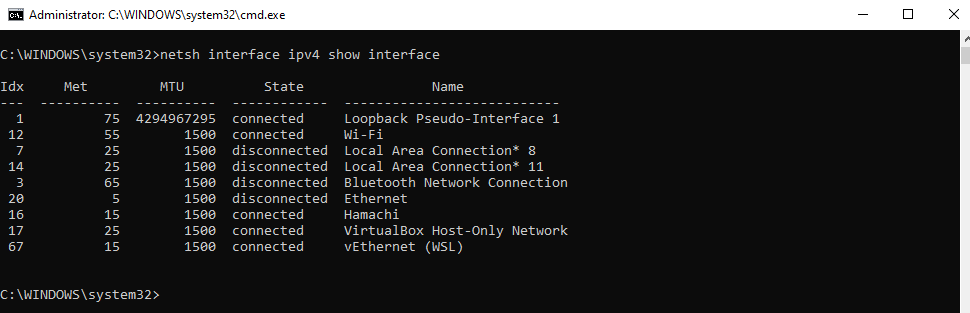
EX-2. What is the default amount of time that an entry remains in your ARP cache  
before being removed. You can determine this empirically (by monitoring the  
cache contents) or by looking this up in your operation system documentation.  
Indicate how/where you determined this value.

**ANSWER:**

I use cmd looking for this value:

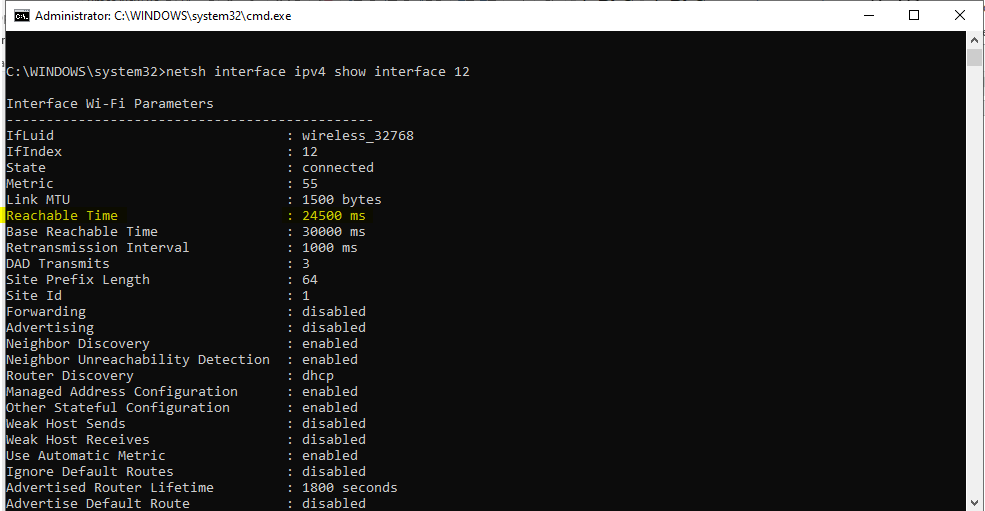
1st: “netsh interface ipv4 show interface”

-> Get the interface ID for the required interface (12)



2nd: “netsh interface ipv4 show interface 12”

-> See the "Reachable Time" in the output: **24500ms**



\*Addtion: (from docs.microsoft.com, *Description of Address Resolution Protocol (ARP) caching behavior in TCP/IP implementations)*

