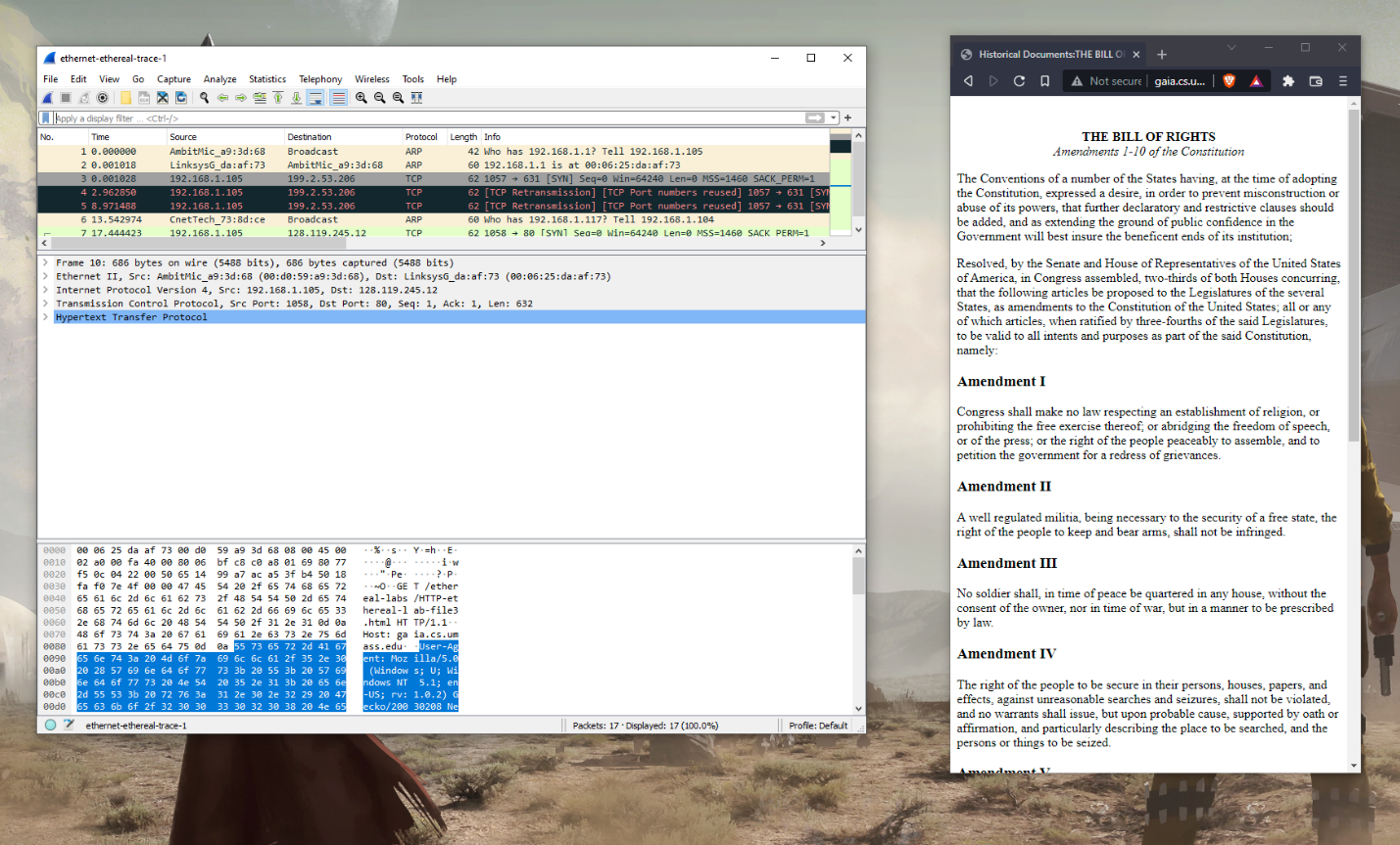
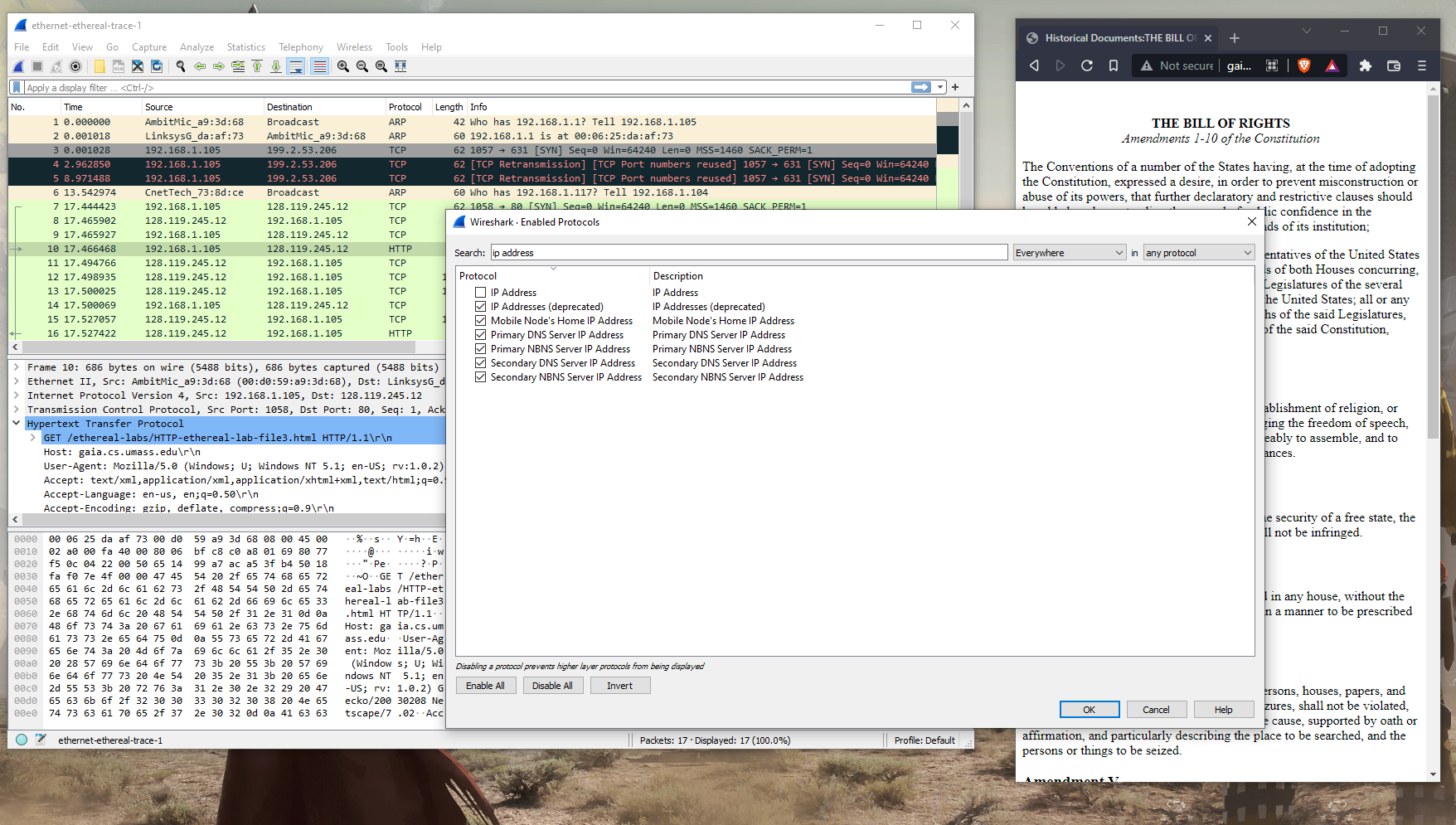
Dalton Murray

Lab 2

Part 1

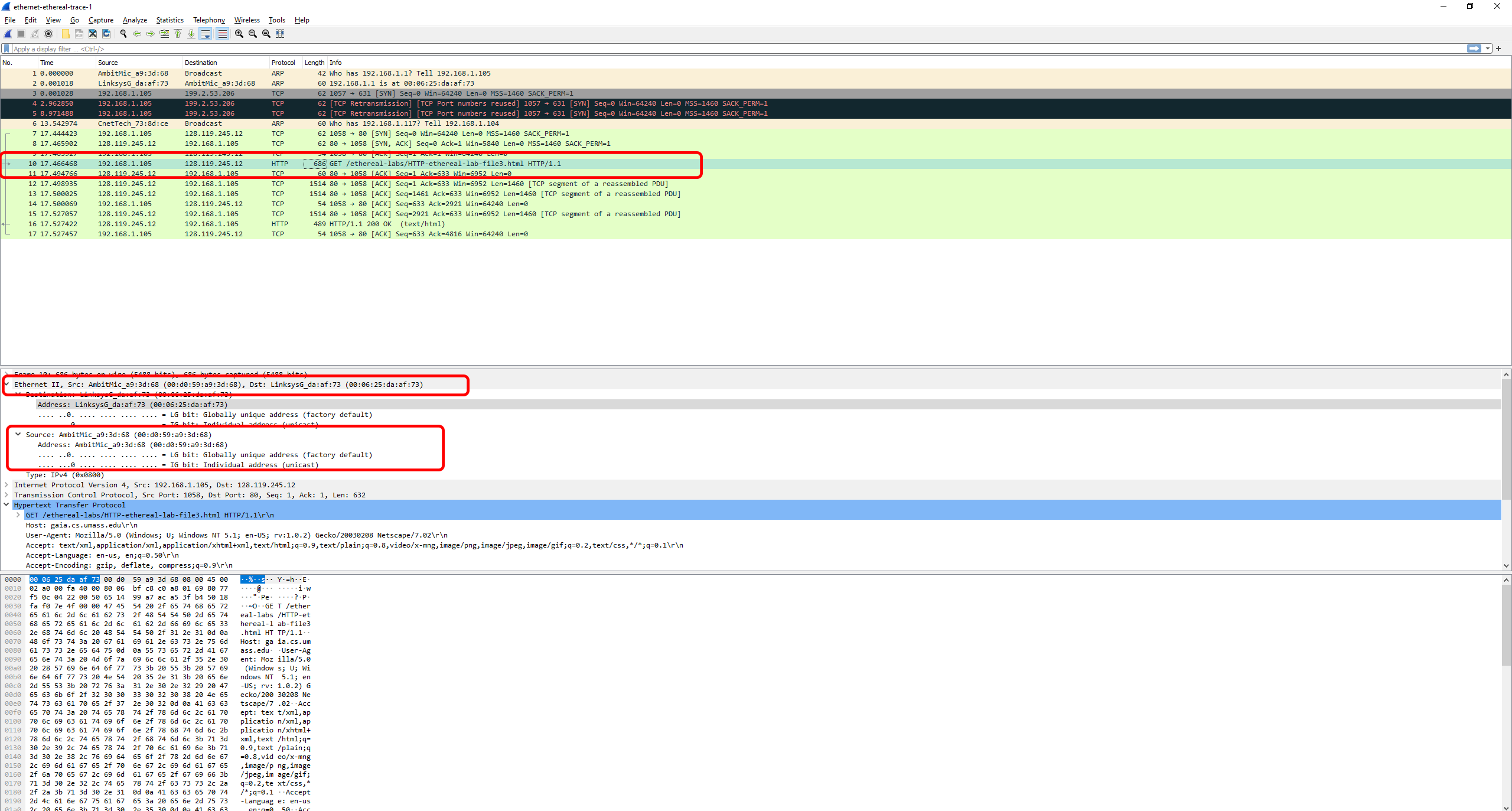
Capturing and analyzing Ethernet frames





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

The 48-bit Ethernet address of my computer is: Address: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

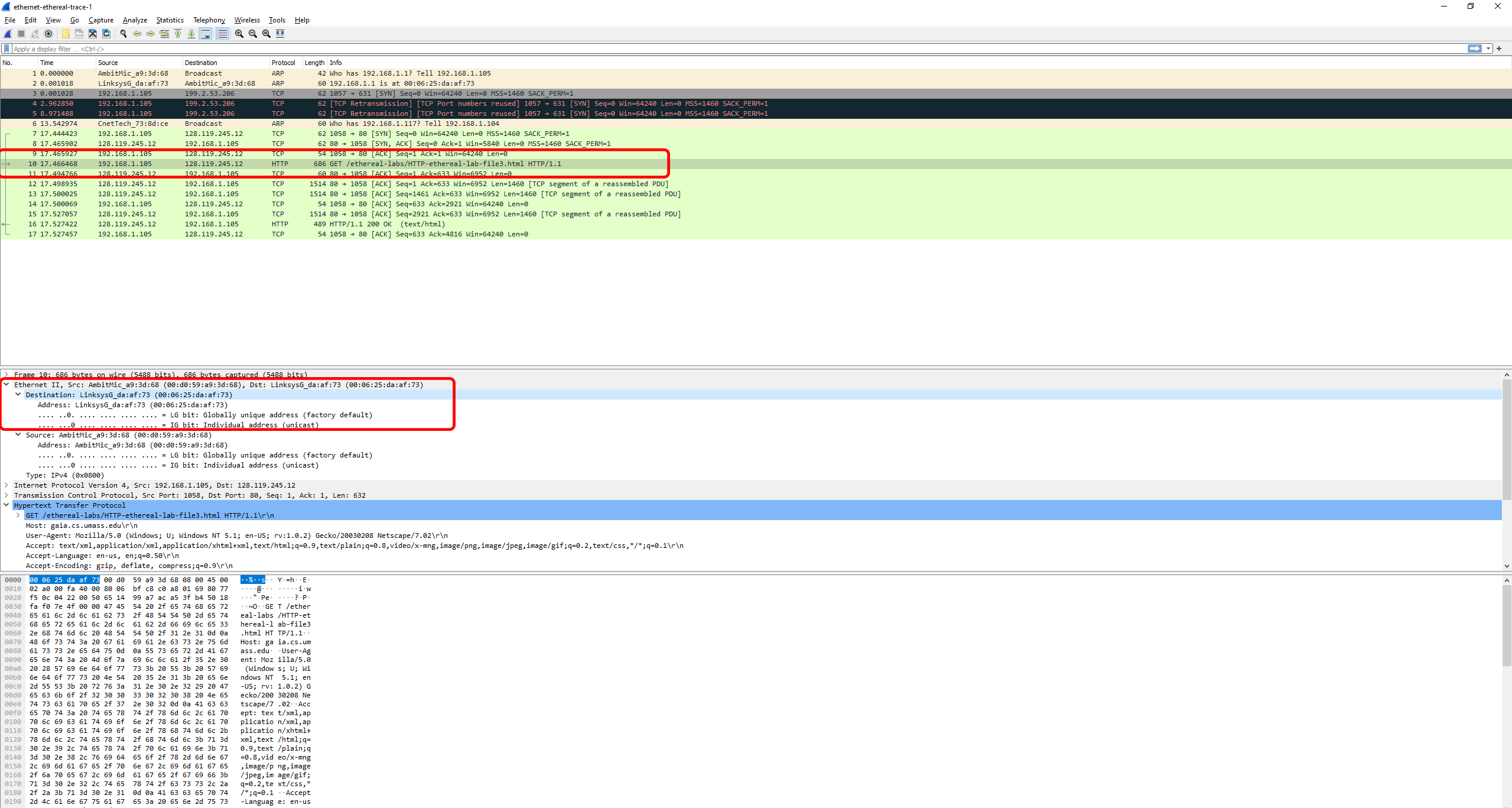


1. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? What device has this as its Ethernet address?

The 48-bit destination address in the Ethernet frame is: Address: LinksysG\_da:af:73 (00:06:25:da:af:73)

This is not the ethernet address of gaia.cs.umass.edu

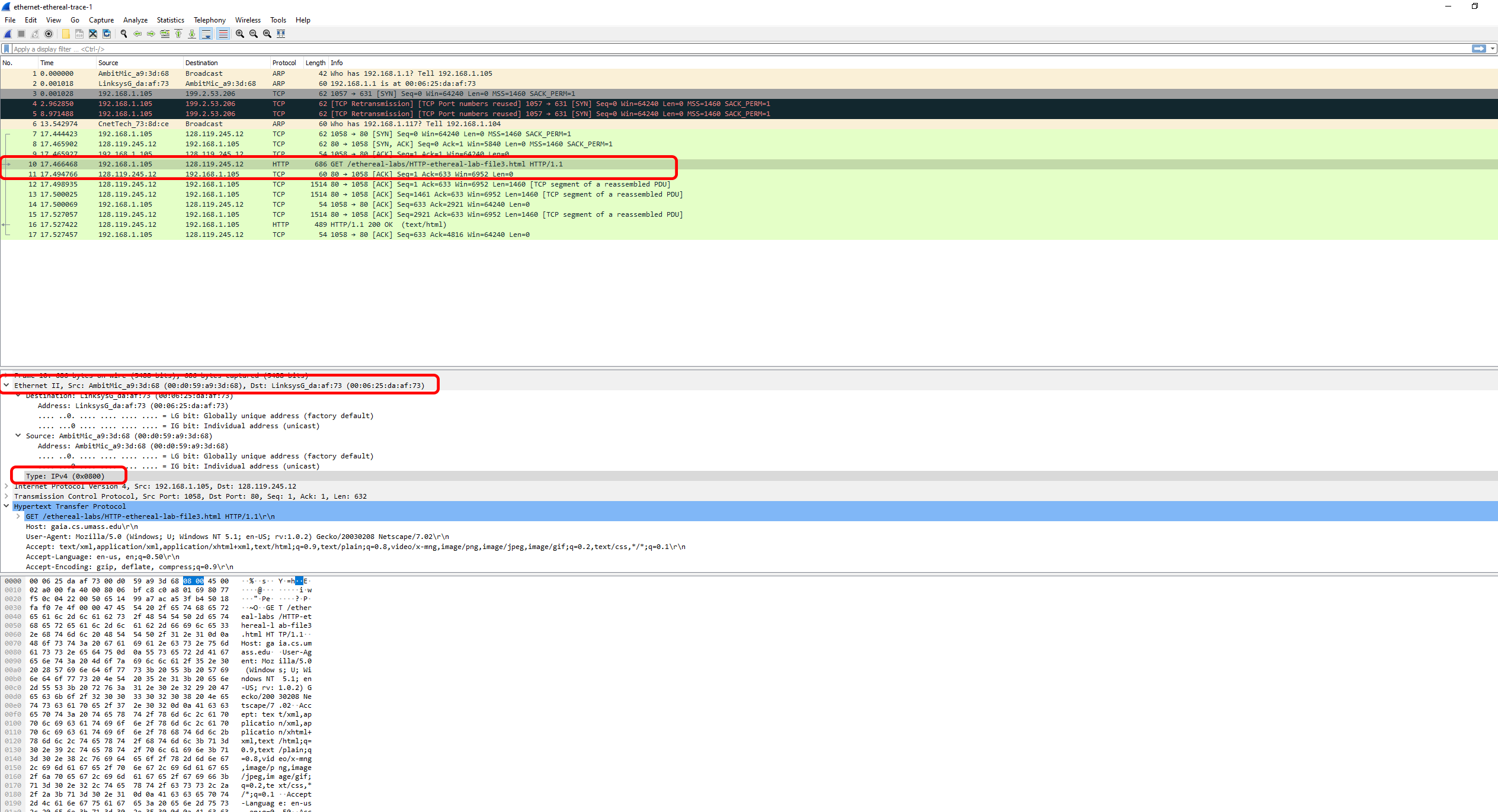
The device that has this as its ethernet address is my gateway



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

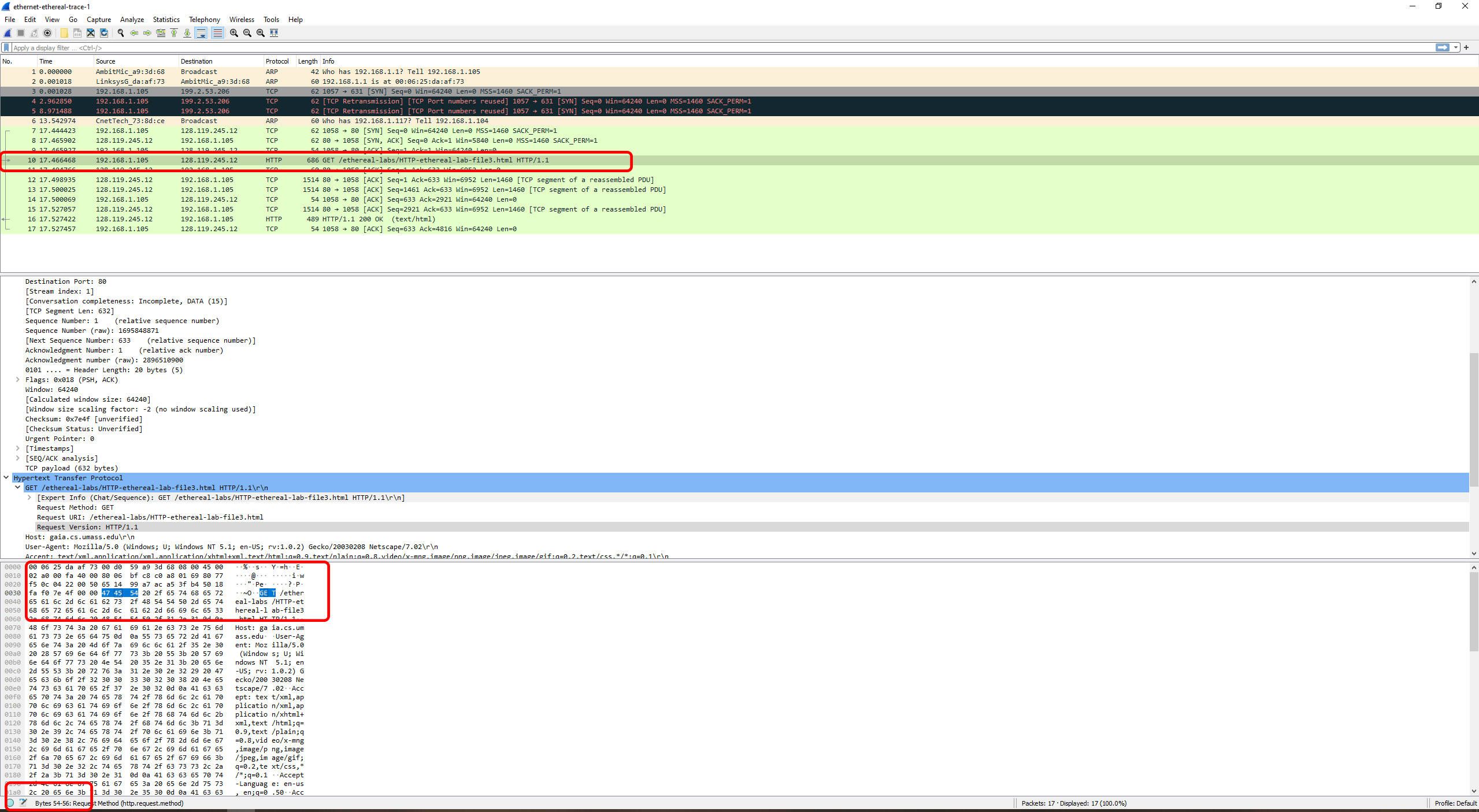
The hexadecimal value for the two-byte Frame type field is 0x0800.

This hexadecimal value corresponds to the upper layer protocol IP protocol.



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

The ASCII “G” in the “GET” appears 54 bytes after the very start of the Ethernet frame.

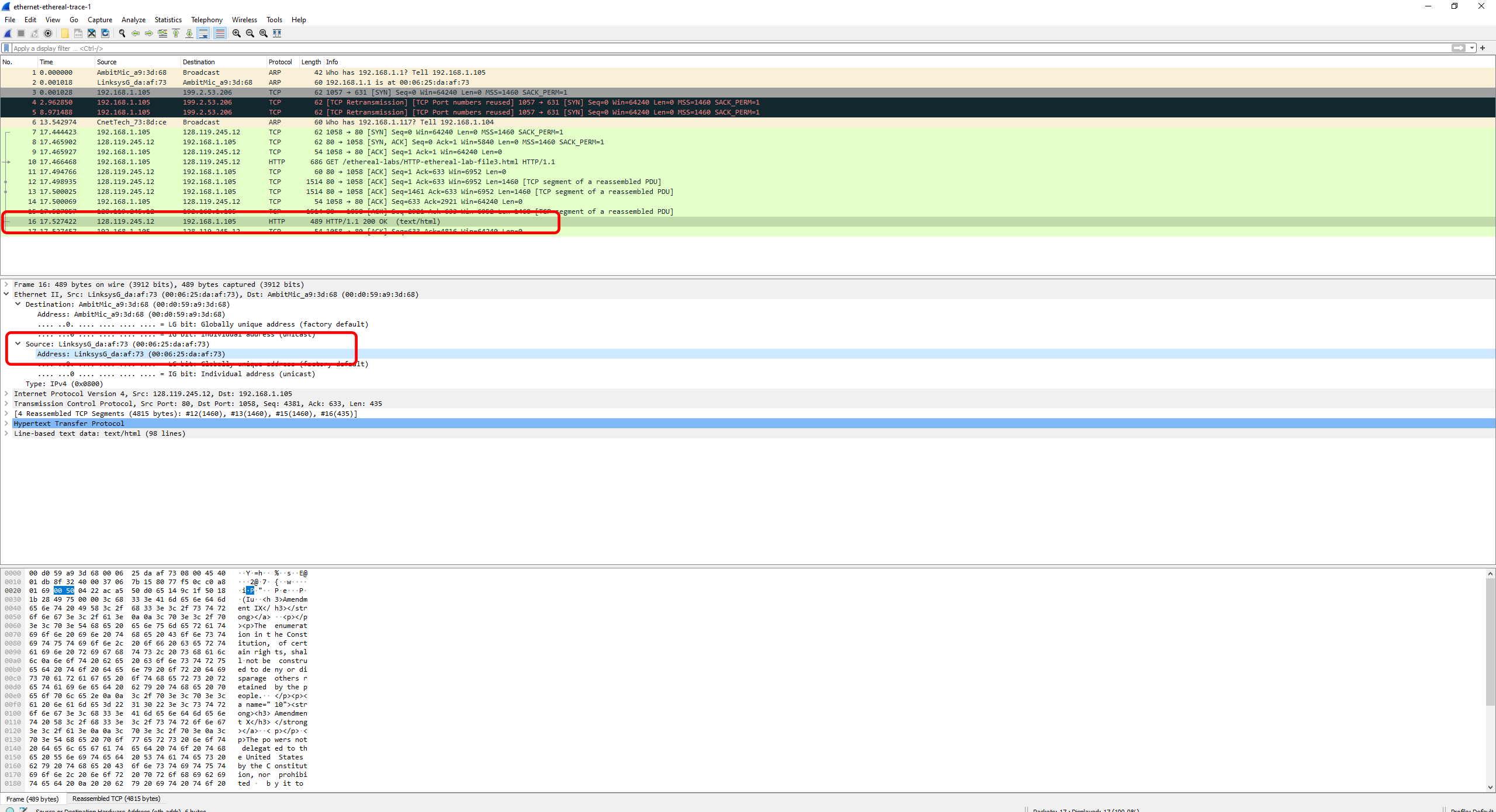


1. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu. What device has this as its Ethernet address?

The value of the Ethernet source address is LinksysG\_da:af:73 (00:06:25:da:af:73)

This is not the address of my computer or of gaia.cs.umass.edu.

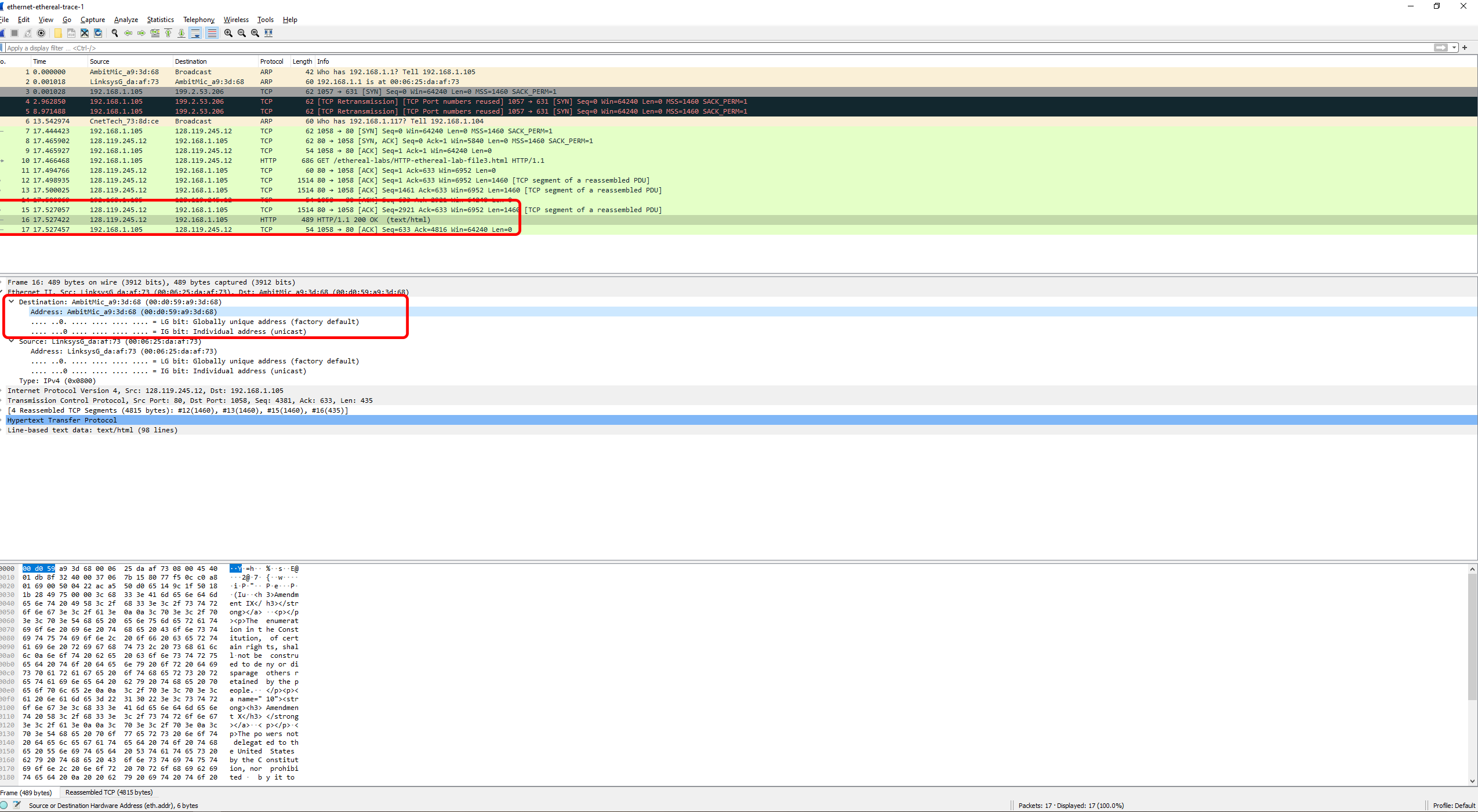
This is the address of my router/gateway.



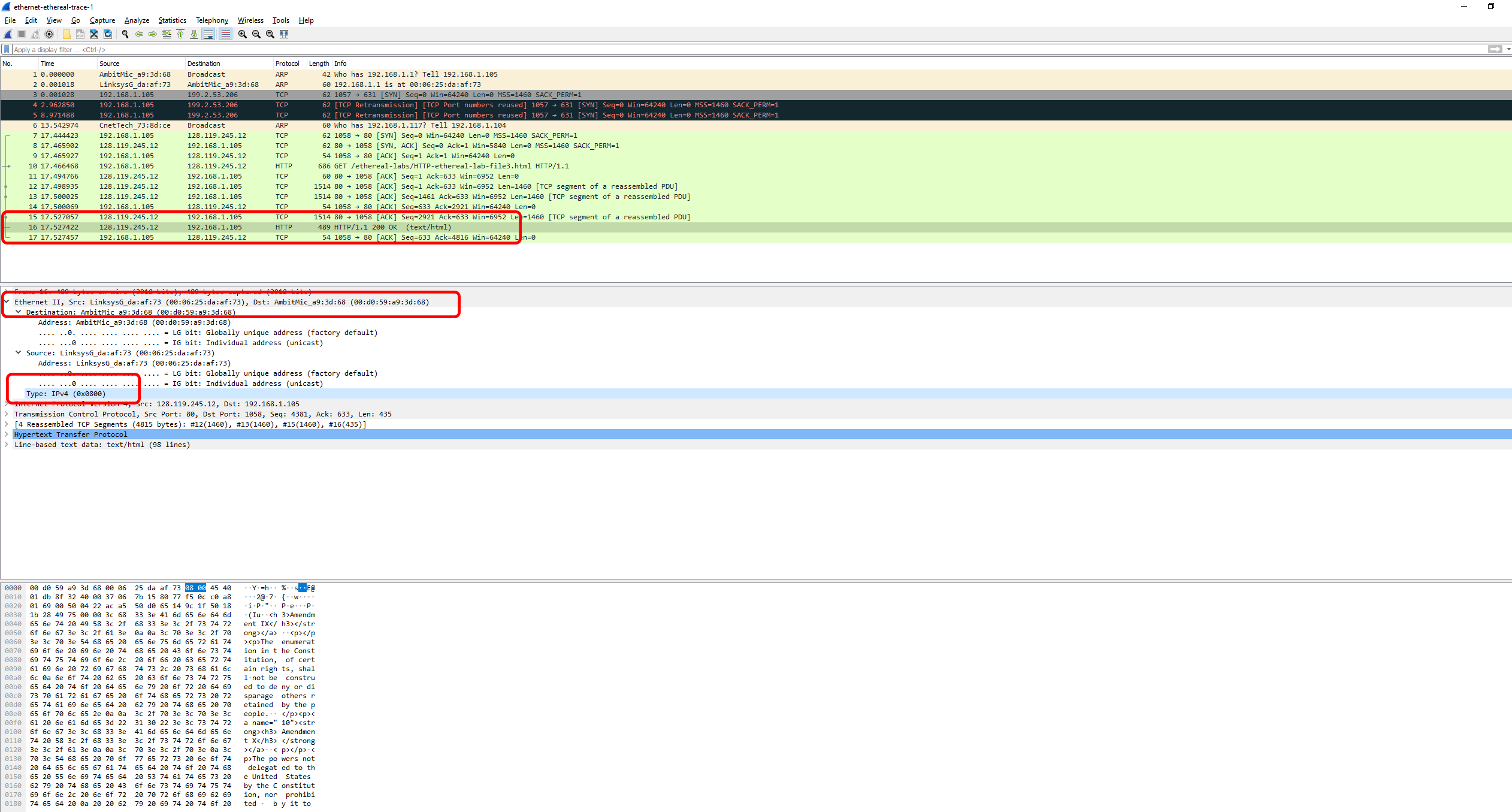
1. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

The destination address in the Ethernet frame is AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68).

This is the Ethernet address of my computer.



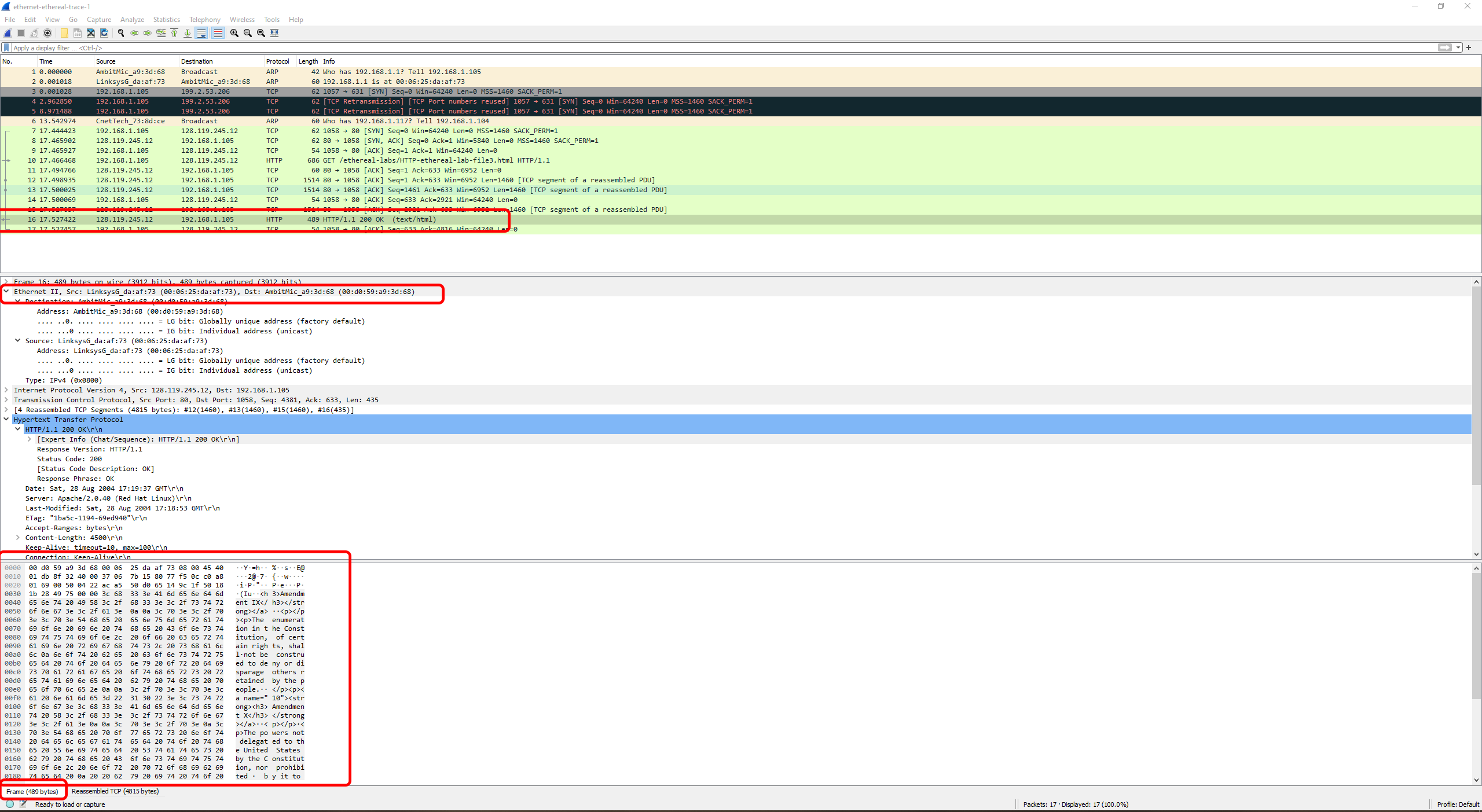
1. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

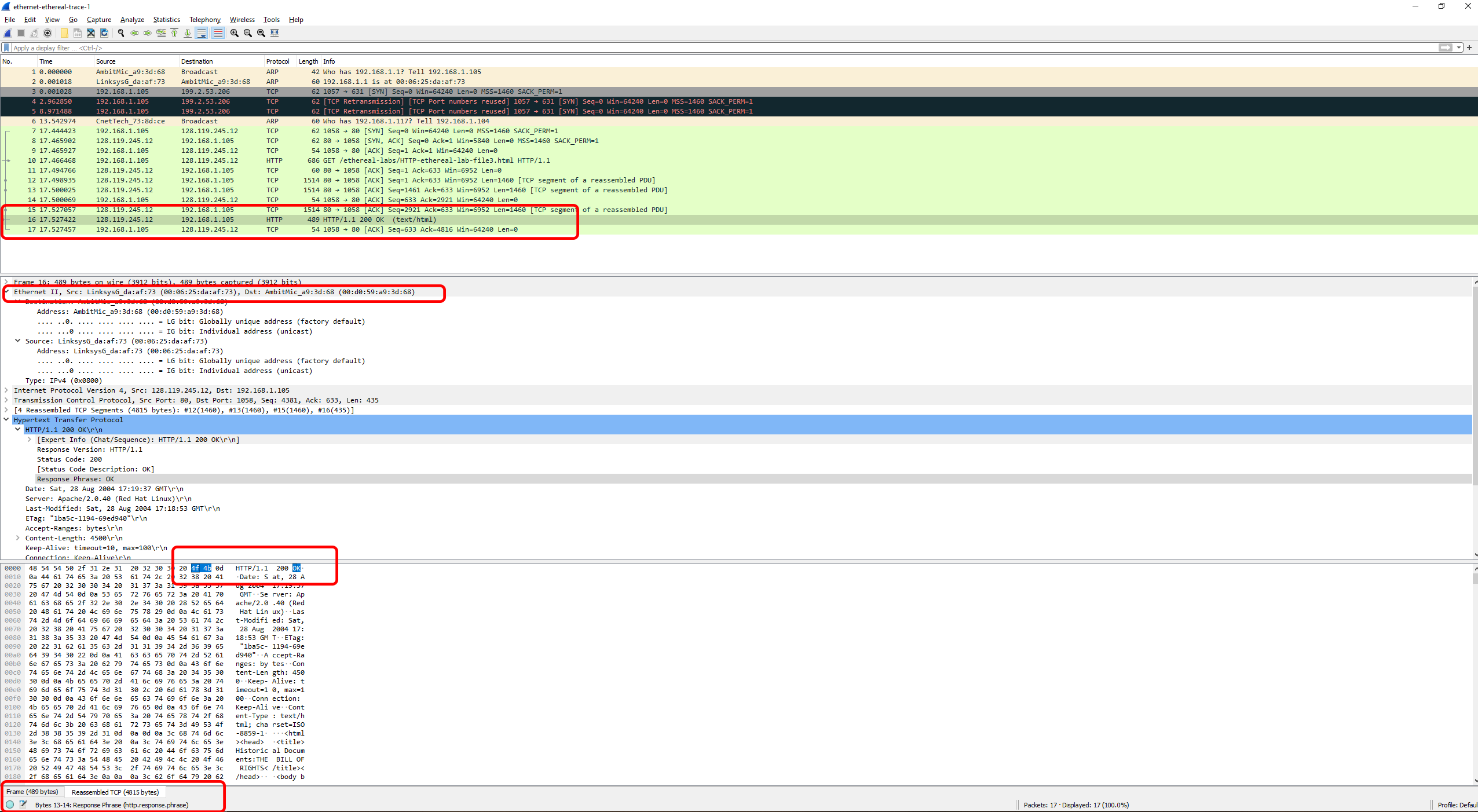
The hexadecimal value for the two-byte Frame type field is 0x0800  
This hexadecimal value corresponds to the upper layer protocol IP protocol  


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

The ASCII “OK” does not appear in the Frame (489 bytes) in the Ethernet II frame, however, it does appear in the Reassembled TCP (4815 bytes) section.

The ASCII “O” appears 13 Bytes away from the very start.

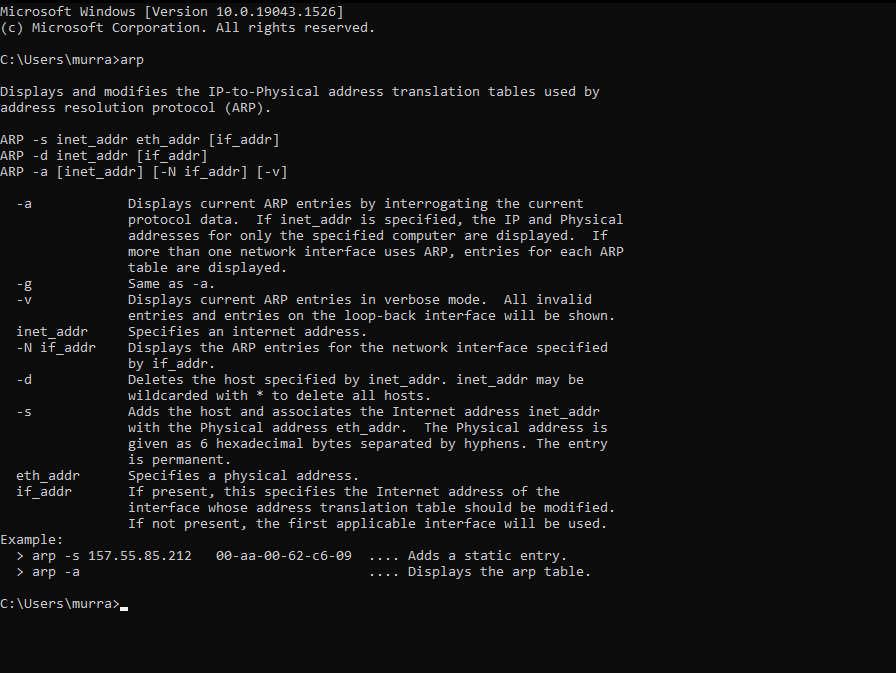




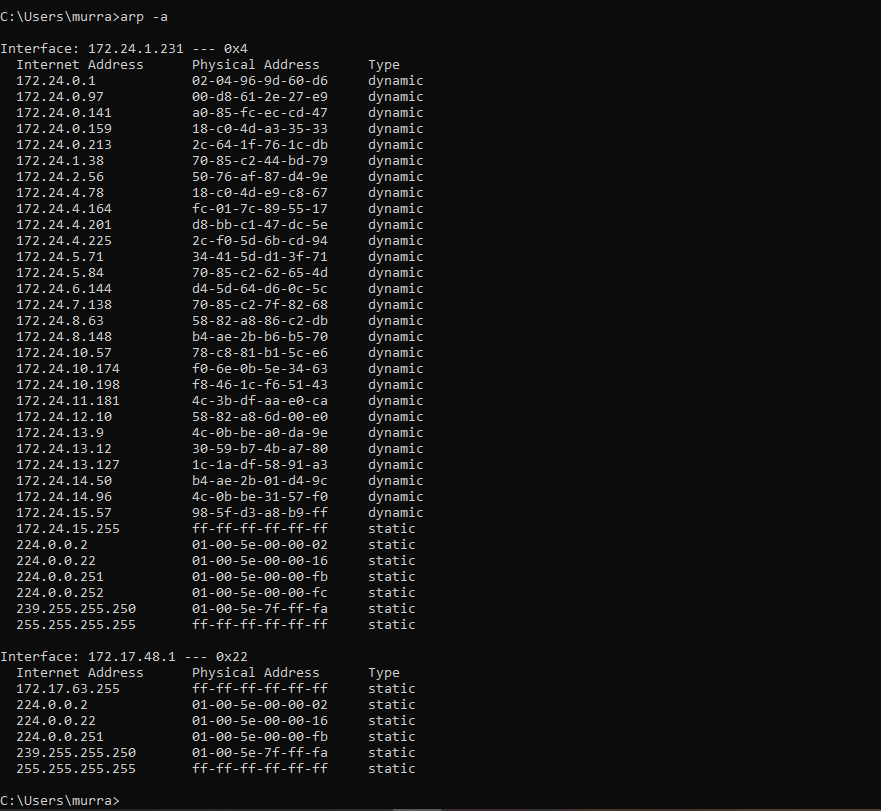
Part 2

The Address Resolution protocol

Arp



arp -a



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

The contents of my computer’s ARP cache is as follows:

Interface: 172.24.1.231 --- 0x4

Internet Address Physical Address Type

172.24.0.1 02-04-96-9d-60-d6 dynamic

172.24.0.97 00-d8-61-2e-27-e9 dynamic

172.24.0.141 a0-85-fc-ec-cd-47 dynamic

172.24.0.159 18-c0-4d-a3-35-33 dynamic

172.24.0.213 2c-64-1f-76-1c-db dynamic

172.24.1.38 70-85-c2-44-bd-79 dynamic

172.24.2.56 50-76-af-87-d4-9e dynamic

172.24.4.78 18-c0-4d-e9-c8-67 dynamic

172.24.4.164 fc-01-7c-89-55-17 dynamic

172.24.4.201 d8-bb-c1-47-dc-5e dynamic

172.24.4.225 2c-f0-5d-6b-cd-94 dynamic

172.24.5.71 34-41-5d-d1-3f-71 dynamic

172.24.5.84 70-85-c2-62-65-4d dynamic

172.24.5.148 94-a6-7e-ea-6d-5a dynamic

172.24.6.144 d4-5d-64-d6-0c-5c dynamic

172.24.7.138 70-85-c2-7f-82-68 dynamic

172.24.8.63 58-82-a8-86-c2-db dynamic

172.24.8.148 b4-ae-2b-b6-b5-70 dynamic

172.24.10.57 78-c8-81-b1-5c-e6 dynamic

172.24.10.174 f0-6e-0b-5e-34-63 dynamic

172.24.10.198 f8-46-1c-f6-51-43 dynamic

172.24.11.181 4c-3b-df-aa-e0-ca dynamic

172.24.12.10 58-82-a8-6d-00-e0 dynamic

172.24.13.9 4c-0b-be-a0-da-9e dynamic

172.24.13.12 30-59-b7-4b-a7-80 dynamic

172.24.13.127 1c-1a-df-58-91-a3 dynamic

172.24.14.50 b4-ae-2b-01-d4-9c dynamic

172.24.14.96 4c-0b-be-31-57-f0 dynamic

172.24.15.57 98-5f-d3-a8-b9-ff dynamic

172.24.15.255 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

239.255.255.250 01-00-5e-7f-ff-fa static

255.255.255.255 ff-ff-ff-ff-ff-ff static

Interface: 172.17.48.1 --- 0x22

Internet Address Physical Address Type

172.17.63.255 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

255.255.255.255 ff-ff-ff-ff-ff-ff static

The internet address is the IP address of what we are connected to.

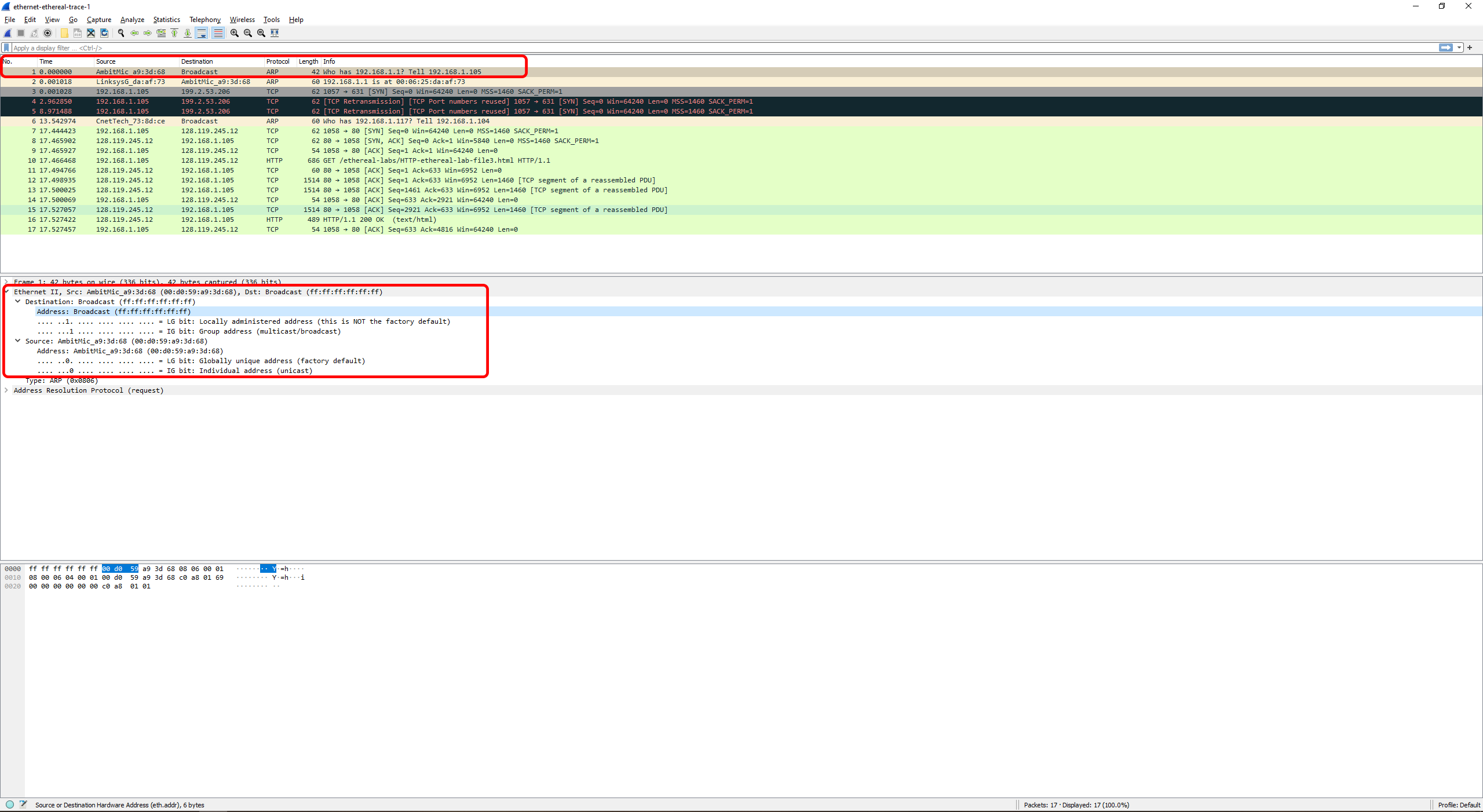
The physical address is the mac address of the device.

The type column is the protocol type.

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

The source address in the Ethernet frame is: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)

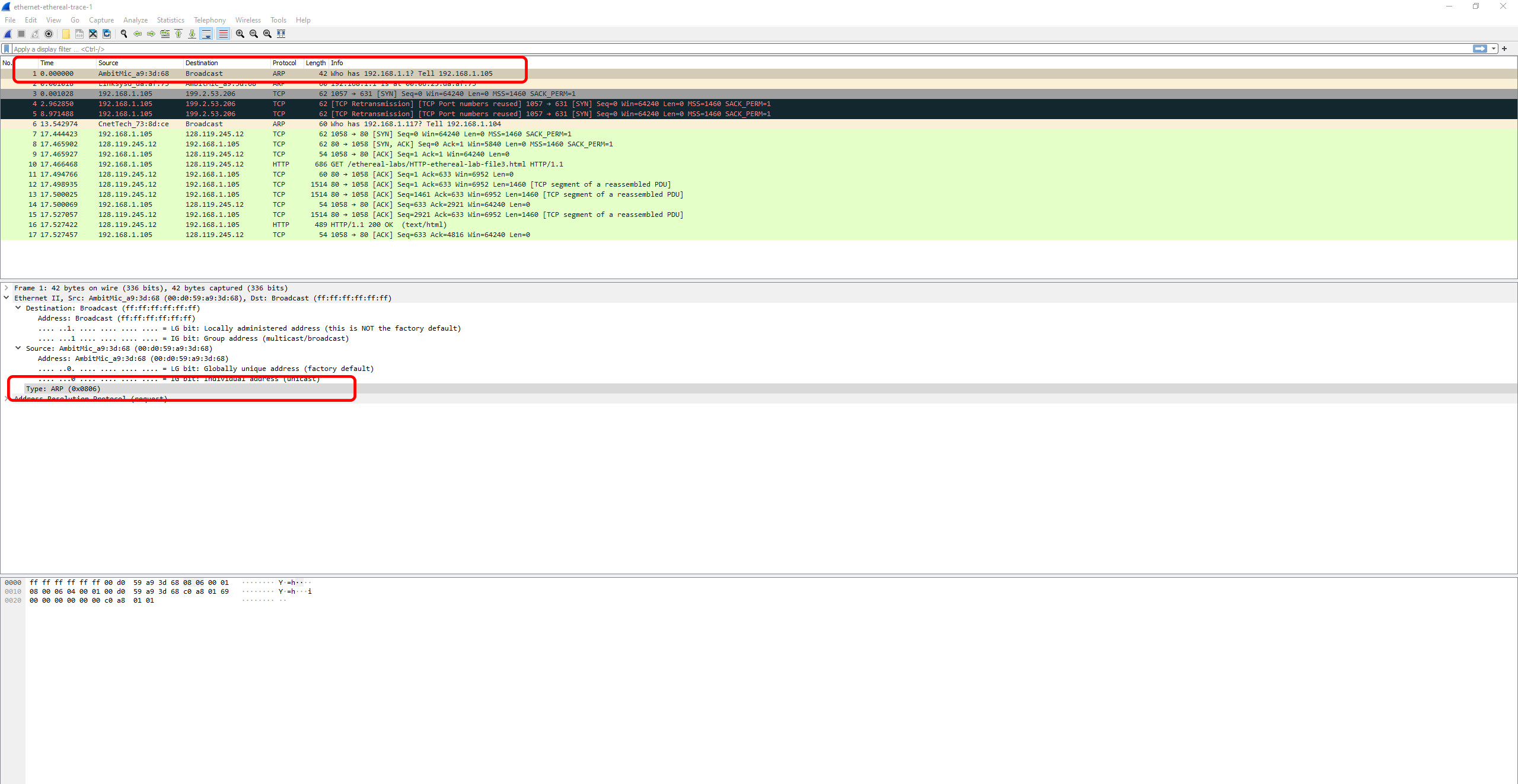
The destination address in the Ethernet frame is: Broadcast (ff:ff:ff:ff:ff:ff)



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

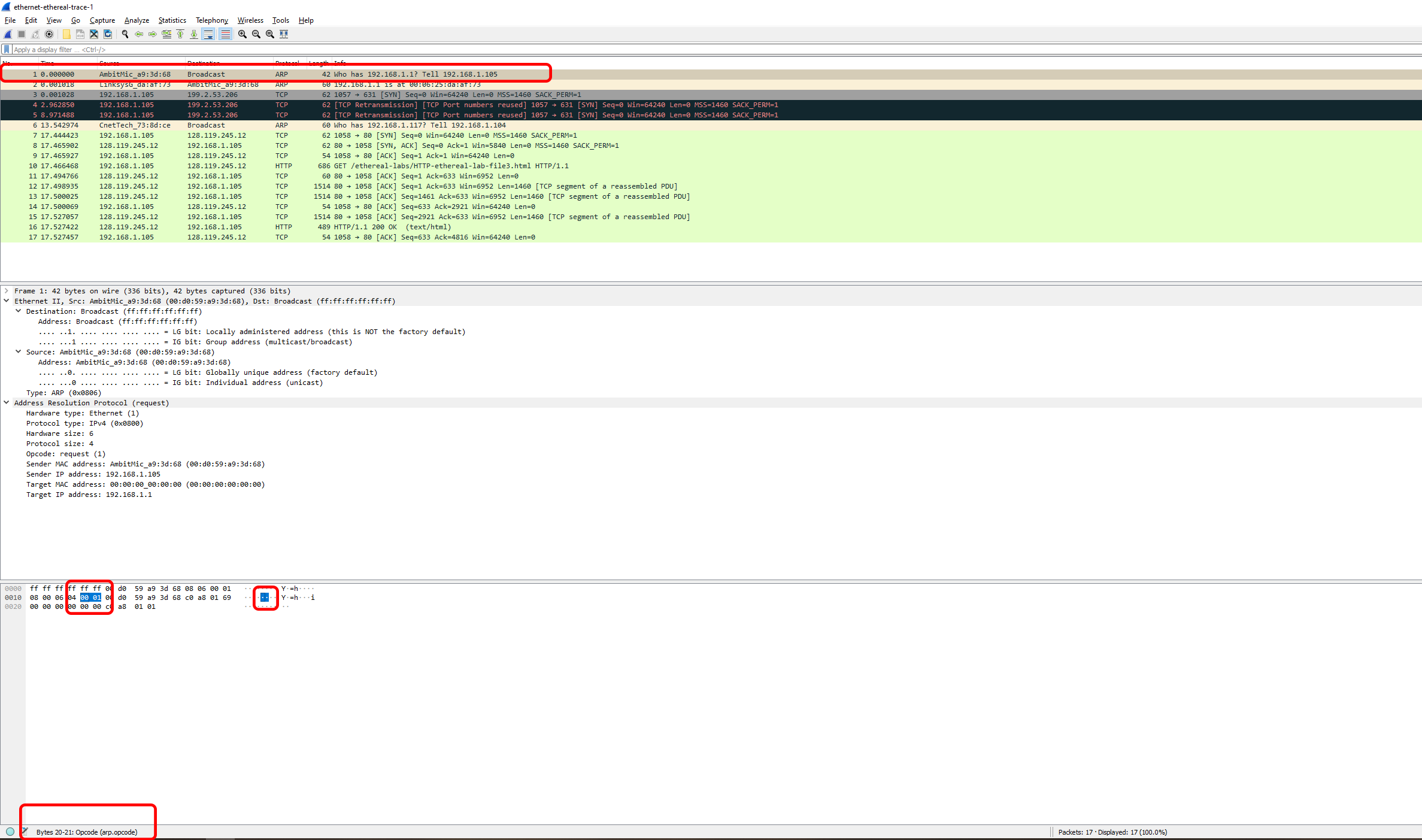
The hexadecimal value for the two-byte Ethernet Frame type field is 0x0806

This upper layer protocol corresponds to the ARP protocol



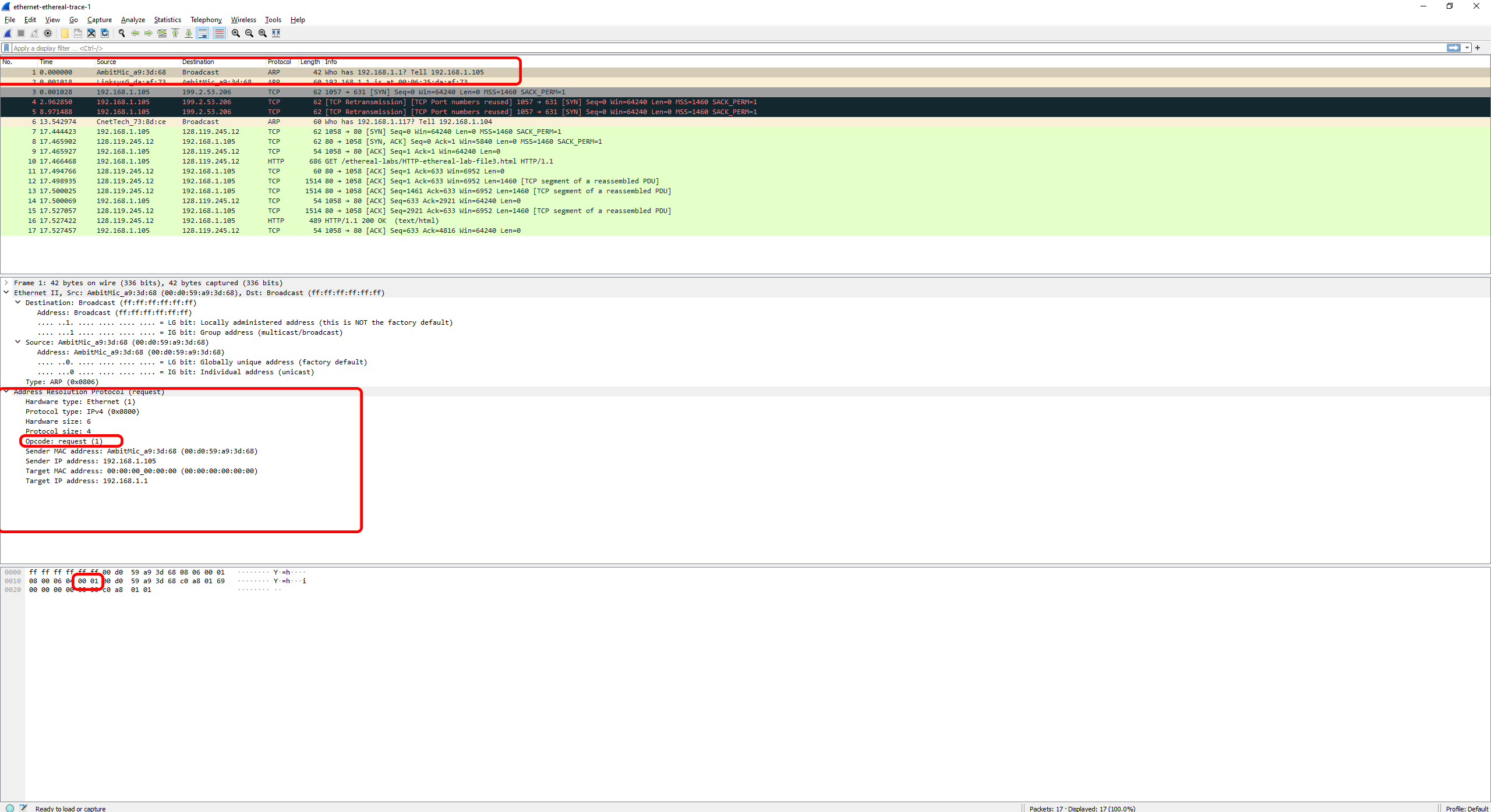
* 1. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

The start of the ARP opcode field begins at 20 Bytes away from the beginning



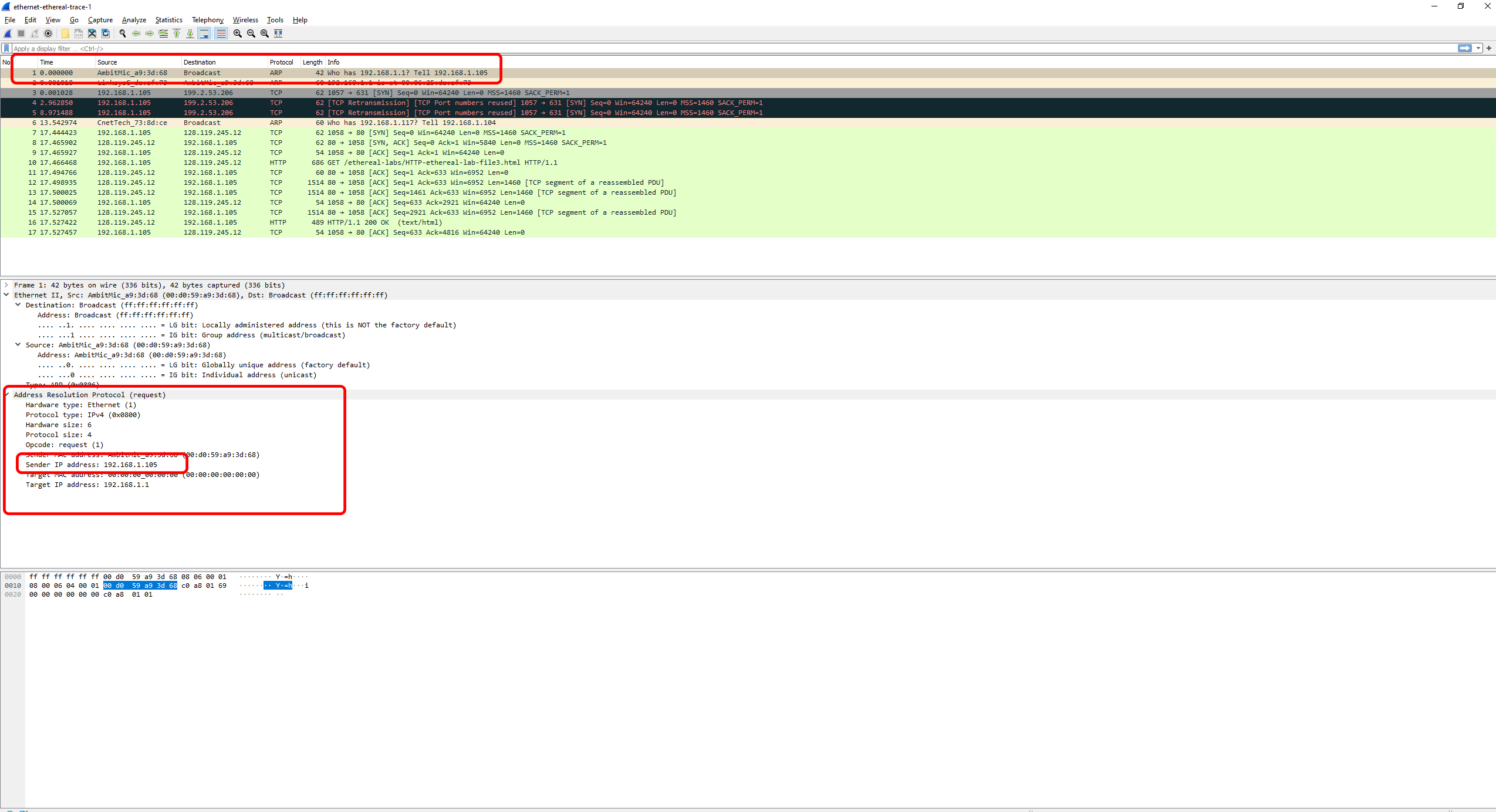
* 1. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

The value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made is 0x0001



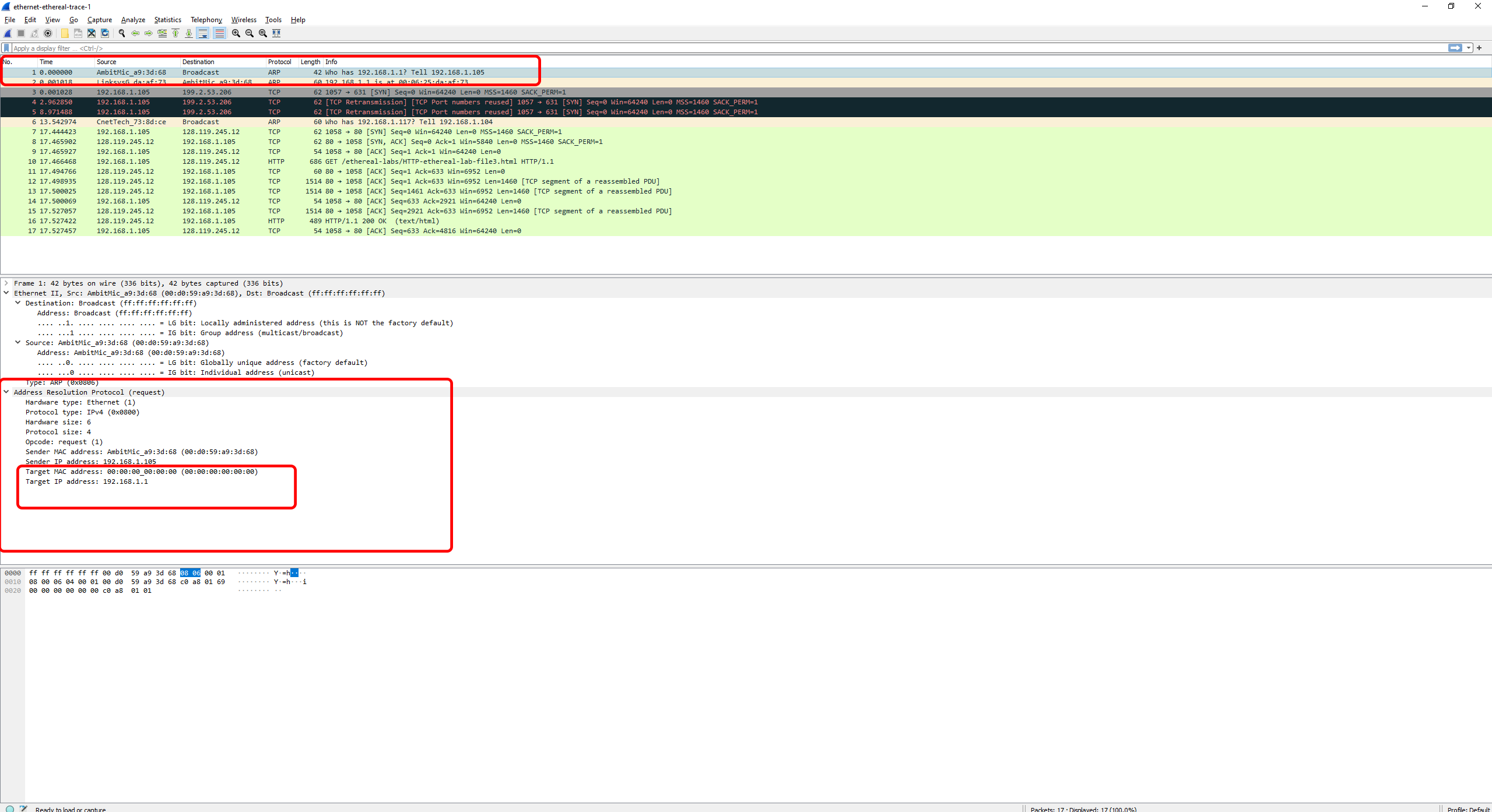
* 1. Does the ARP message contain the IP address of the sender?

Yes, the ARP message contains the IP address of the sender. It is shown to be 192.168.1.105



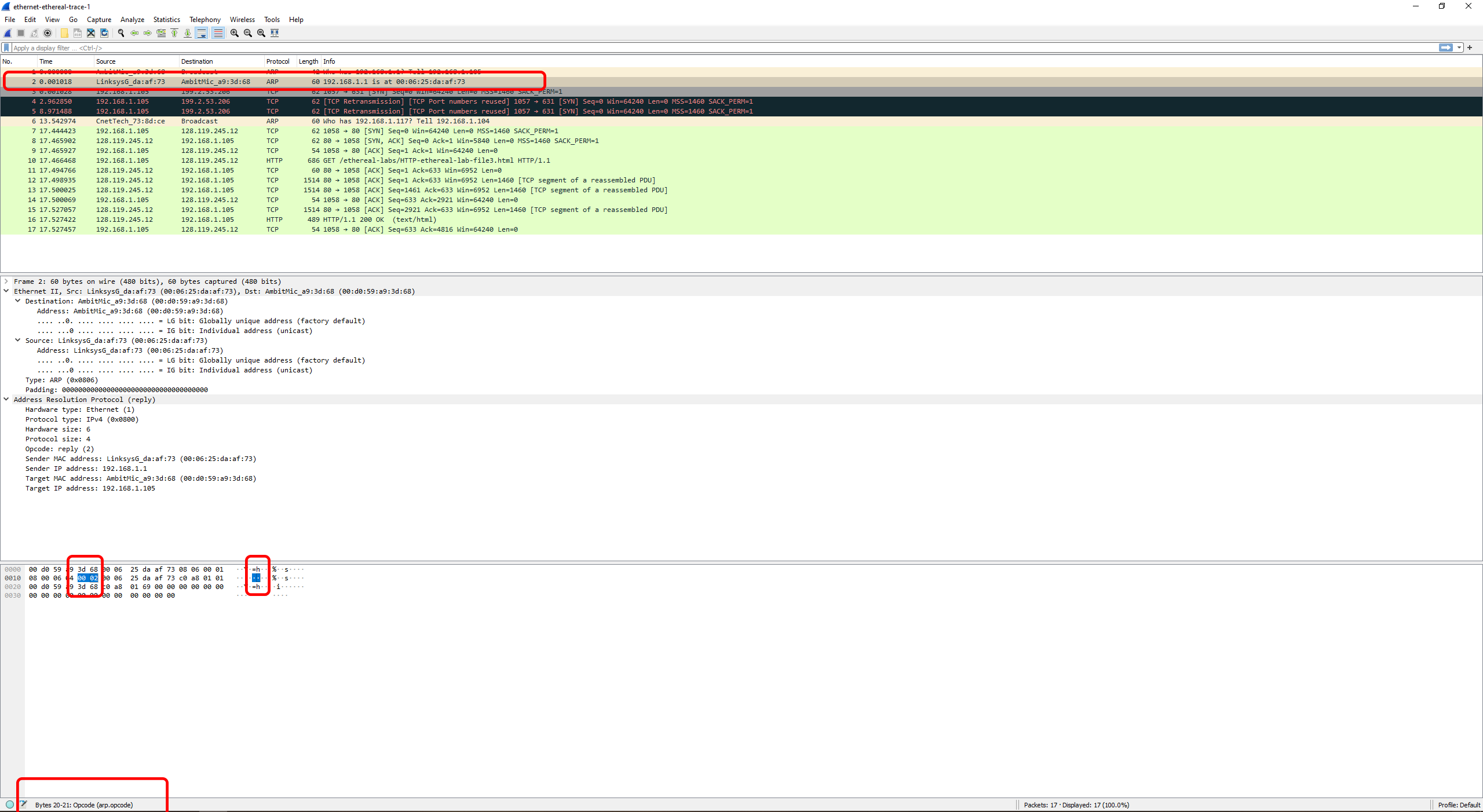
* 1. Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

The “question” or the machine’s IP which is being queried appears under the ARP request Target IP address. The target IP address is 192.168.1.1, and the MAC address is: 00:00:00\_00:00:00 (00:00:00:00:00:00)



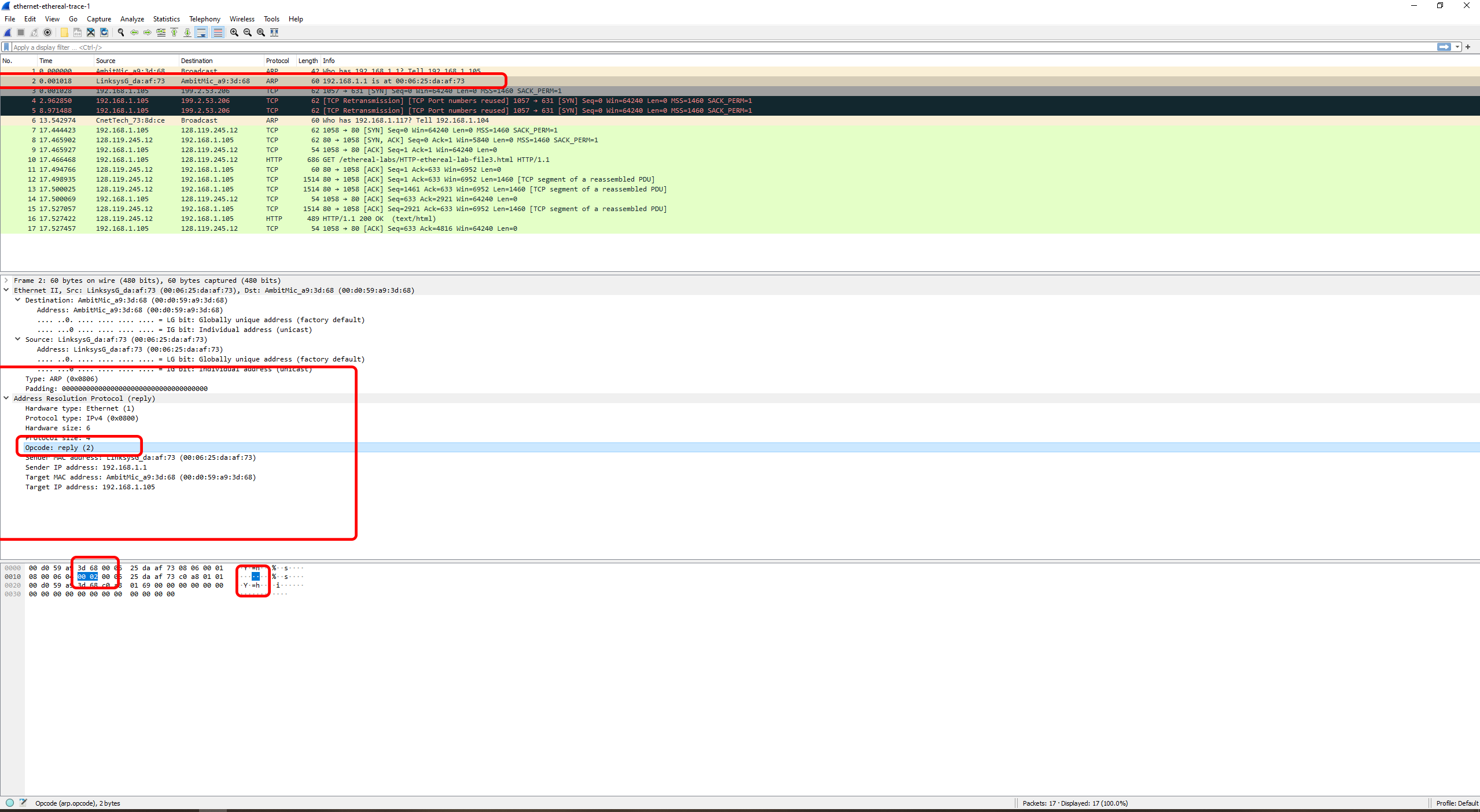
1. a. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

The ARP opcode field begins at byte 20 from the very beginning of the Ethernet frame.



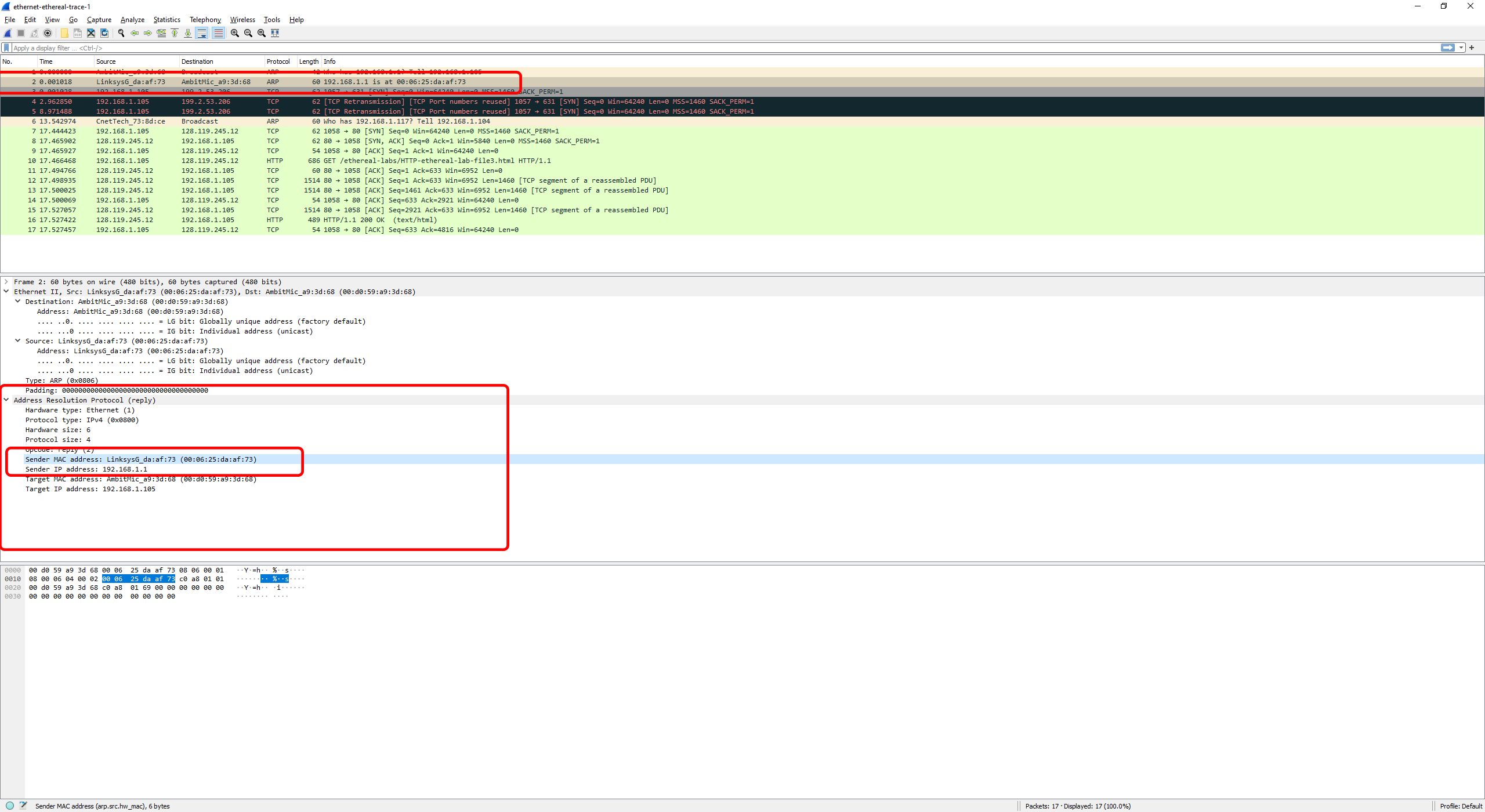
b. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

The value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made is 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 “answer” or the IP address of the machine having the Ethernet address whose corresponding IP address is being queried is in the ARP reply under the Sender IP address and Sender MAC address. The sender IP address is 192.168.1.1 and the MAC address is LinksysG\_da:af:73 (00:06:25:da:af:73).

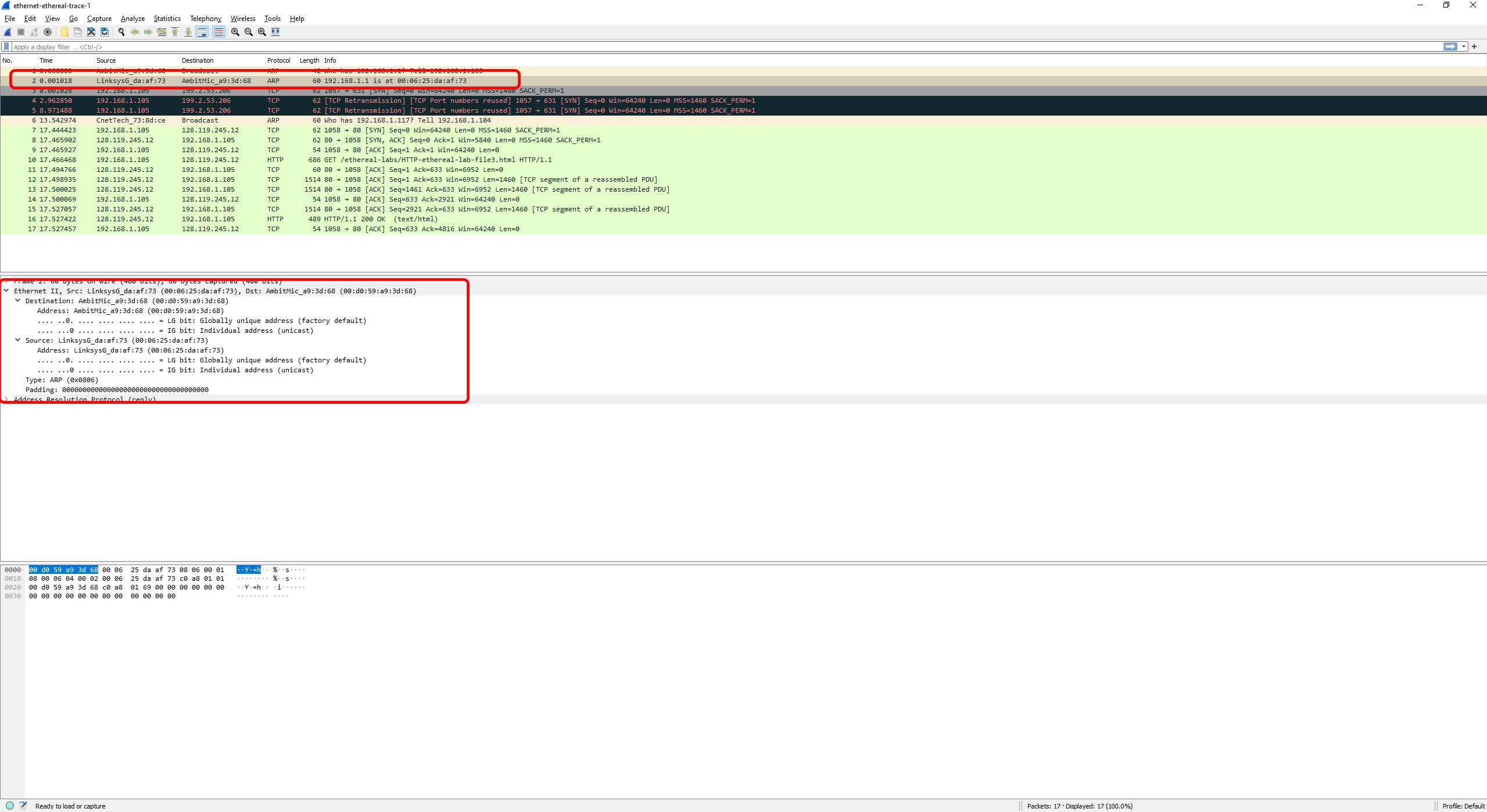


1. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

The hexadecimal values for the source and destination address in the Ethernet II frame containing the ARP reply message are as follows:

Source: LinksysG\_da:af:73 (00:06:25:da:af:73)

Destination: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)



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

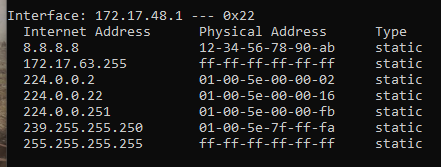
There is no ARP reply for packet 6 in the packet trace because of how ARP works. Packet 1 is us sending the ARP broadcast, and packet 2 is us receiving the reply from ARP. Packet 6 we are able to see the broadcast, however, we are not able to see the reply because it is being directly sent back to the sender who broadcasted.

**Extra credit**

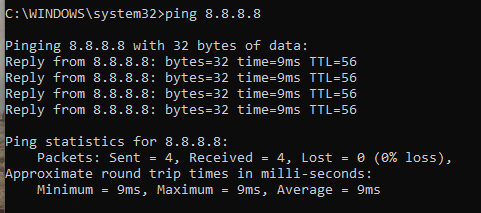
1. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface.

I have done a little bit of testing to see what would happen. Firstly, if attempting to add a correct IP address, 8.8.8.8 (Google) with a completely invalid Ethernet address (one that theoretically is impossible to exist (hf-ff-ff-ff-ff-ff) we get an error stating “ARP: bad argument: hf-ff-ff-ff-ff-ff. 

However, if we throw it back in with a valid Ethernet address, however, is wrong, it seems I can successfully add it to ARP.



When testing if I am able to access 8.8.8.8 I am able to successfully send and receive data.



1. What is the default amount of time that an entry remains in your ARP cache before being removed?

The default amount of time that an entry remains in your ARP cache before being removed is a little bit of a trick question. According to Microsoft, as of 09/24/2021 “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 it’s ‘Reachable Time’ value, the entry changes to the ‘Stale’ state.” However, they do not state a direct time it would take for an entry to remain in the ARP cache before it is automatically removed (Deland-Han).

After reviewing a lot of different places such as Juniper, Cisco, and Microsoft it seems that there is no default amount of time that an entry will remain in your ARP cache before it is automatically removed. However, according to Juniper, Cisco, and Microsoft there may be default timeouts set before it goes from ‘Reachable’ to ‘Stale’ or needs to be remapped. This, however, does not show that it will automatically be removed from your ARP cache.

References:

Deland-Han. (n.d.). Address resolution protocol caching behavior - windows server. Address Resolution Protocol caching behavior - Windows Server | Microsoft Docs <https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/address-resolution-protocol-arp-caching-behavior>

I pledge that on all academic work that I submit, I will neither give nor receive unauthorized aid, nor will I present another person's work as my own.

Dalton Murray