Justin Phillips

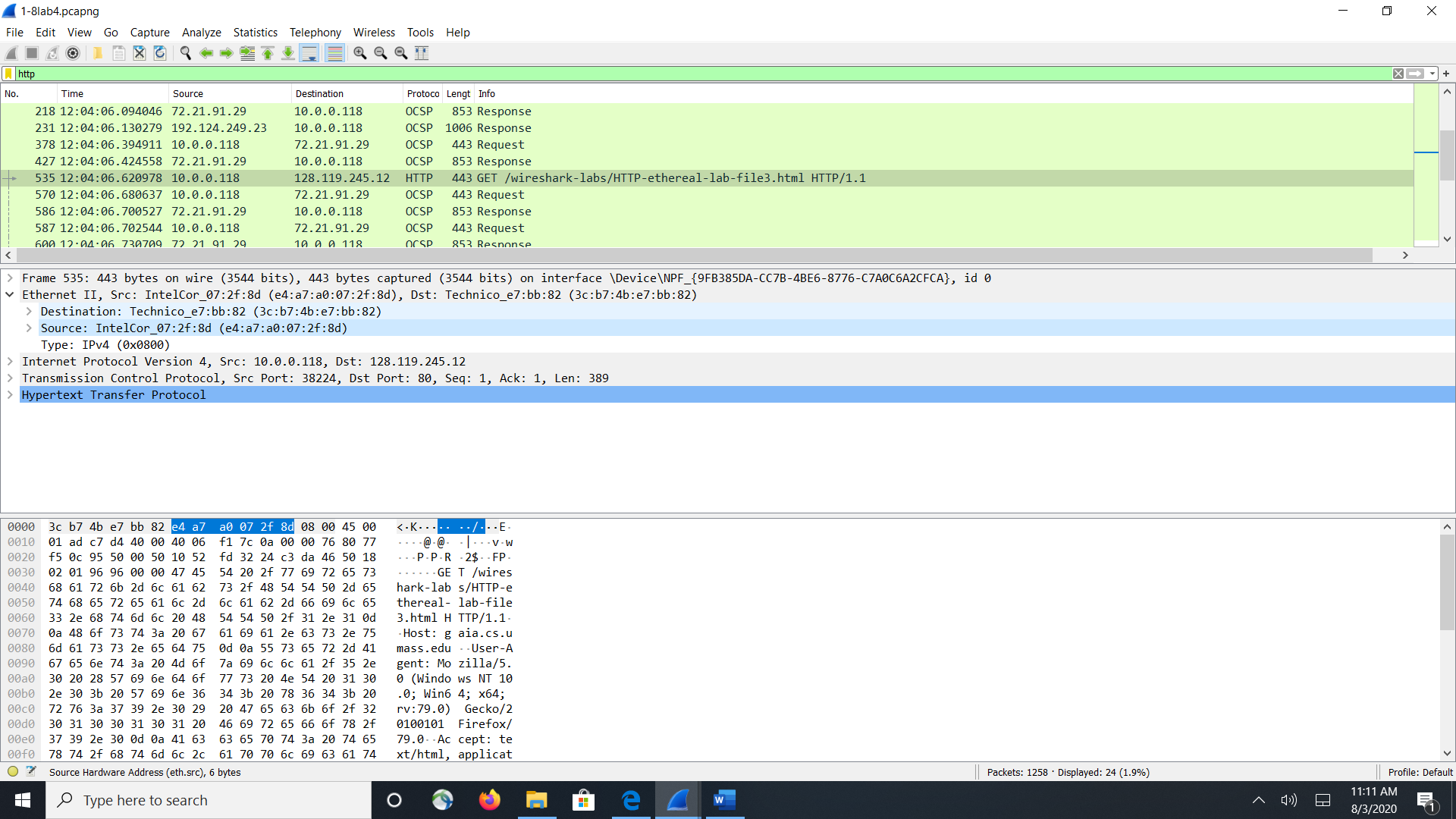
cs372 2020

lab5

Answer the following questions, based on the contents of the Ethernet frame containing the HTTP GET message. Whenever possible, when answering a question you should include a screenshot of the packet(s) within the trace that you used to answer the question asked. Make sure to include in the screenshot ALL and ONLY the minimum amount of packet detail that you need to answer the question.

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

Source: IntelCor\_07:2f:8d (e4:a7:a0:07:2f:8d)



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.]

Destination: Technico\_e7:bb:82 (3c:b7:4b:e7:bb:82)(screen shot is in 1)

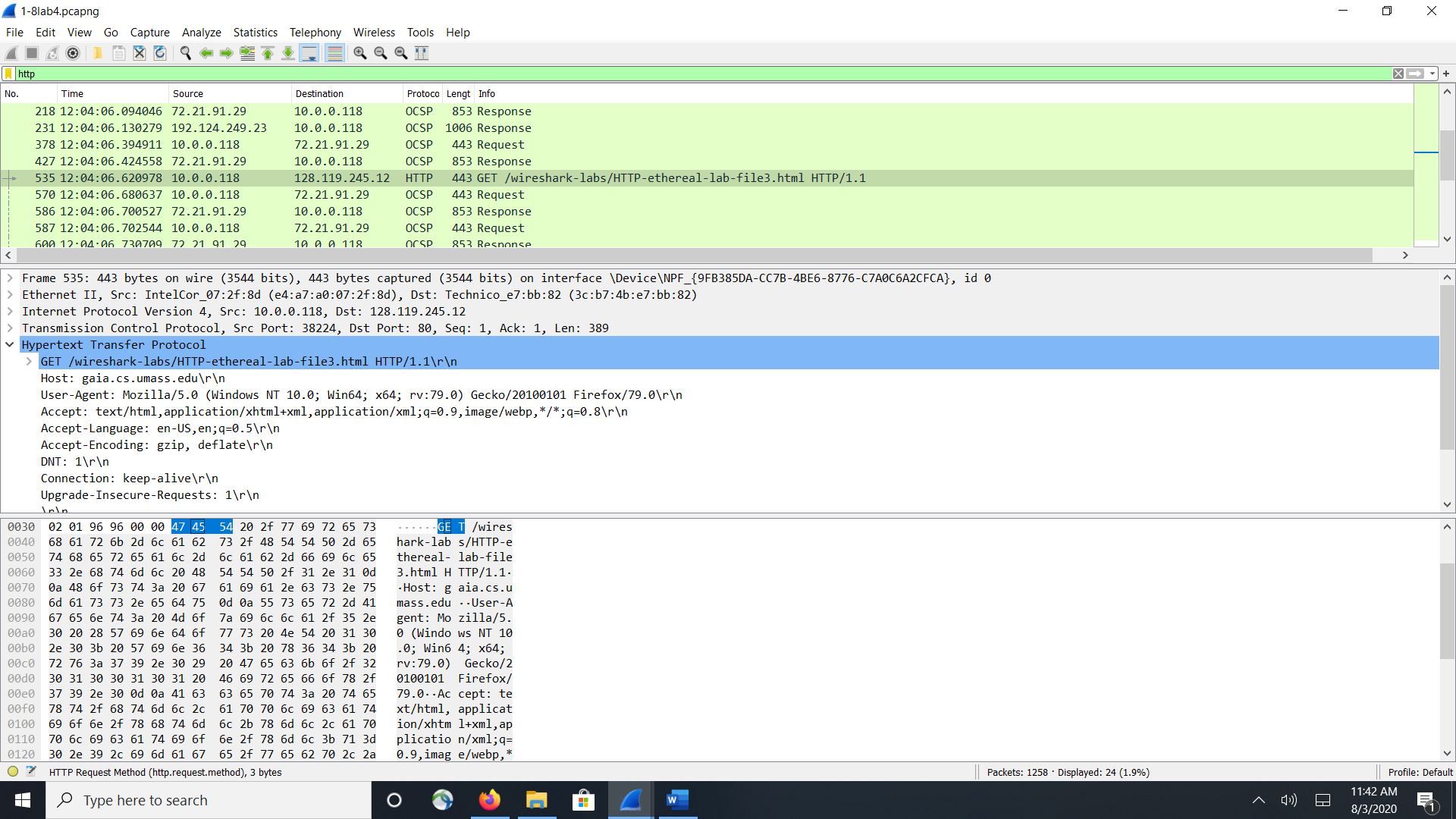
this is the address of my router

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

Type: IPv4 (0x0800)(as seen in 1) the upper layer protocol that this corresponds to is IP protocol as payload

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

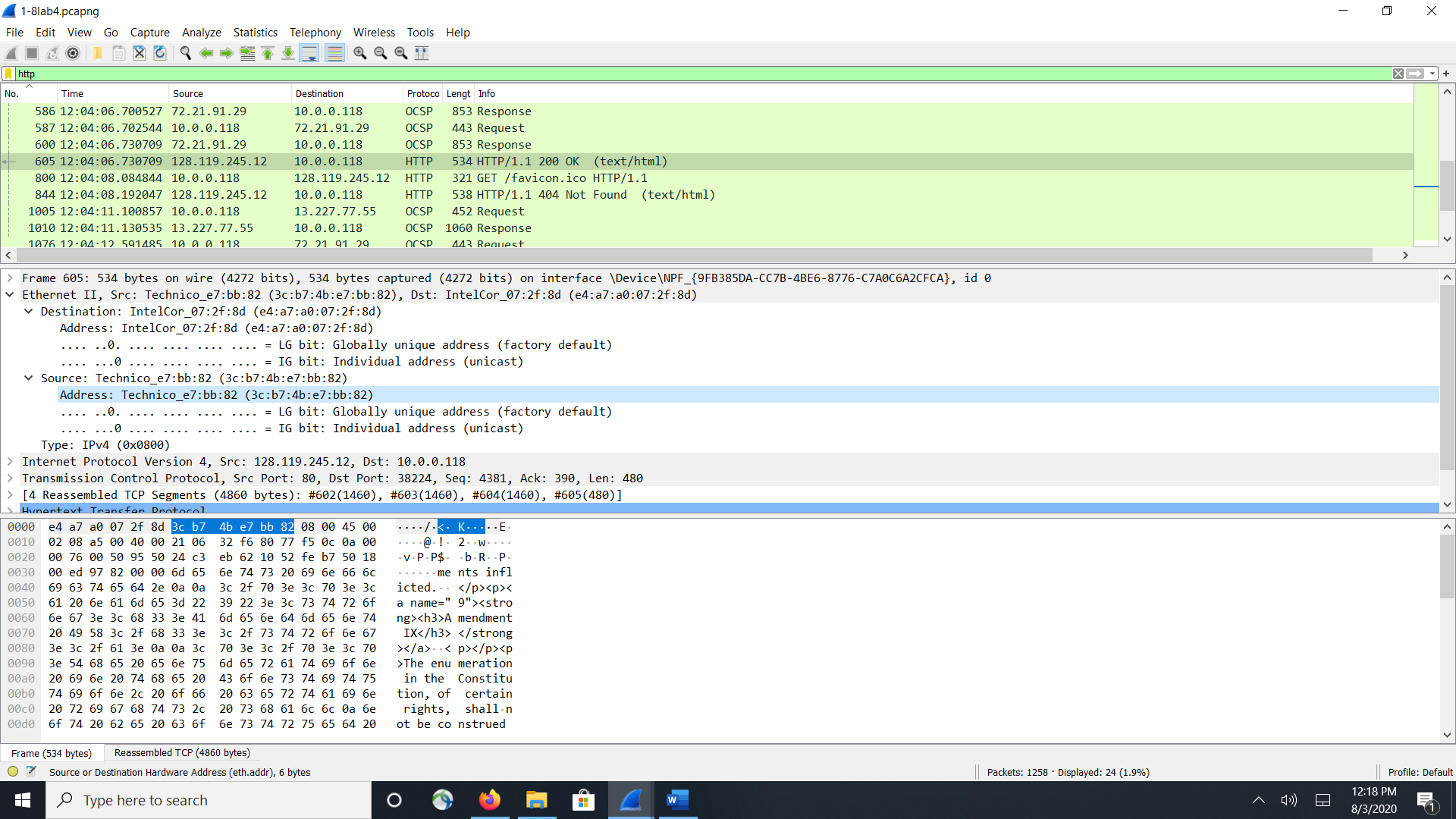
bytes 54-56 is the GET request, so 54 would be the G



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?

Address: Technico\_e7:bb:82 (3c:b7:4b:e7:bb:82), this is address of my router



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

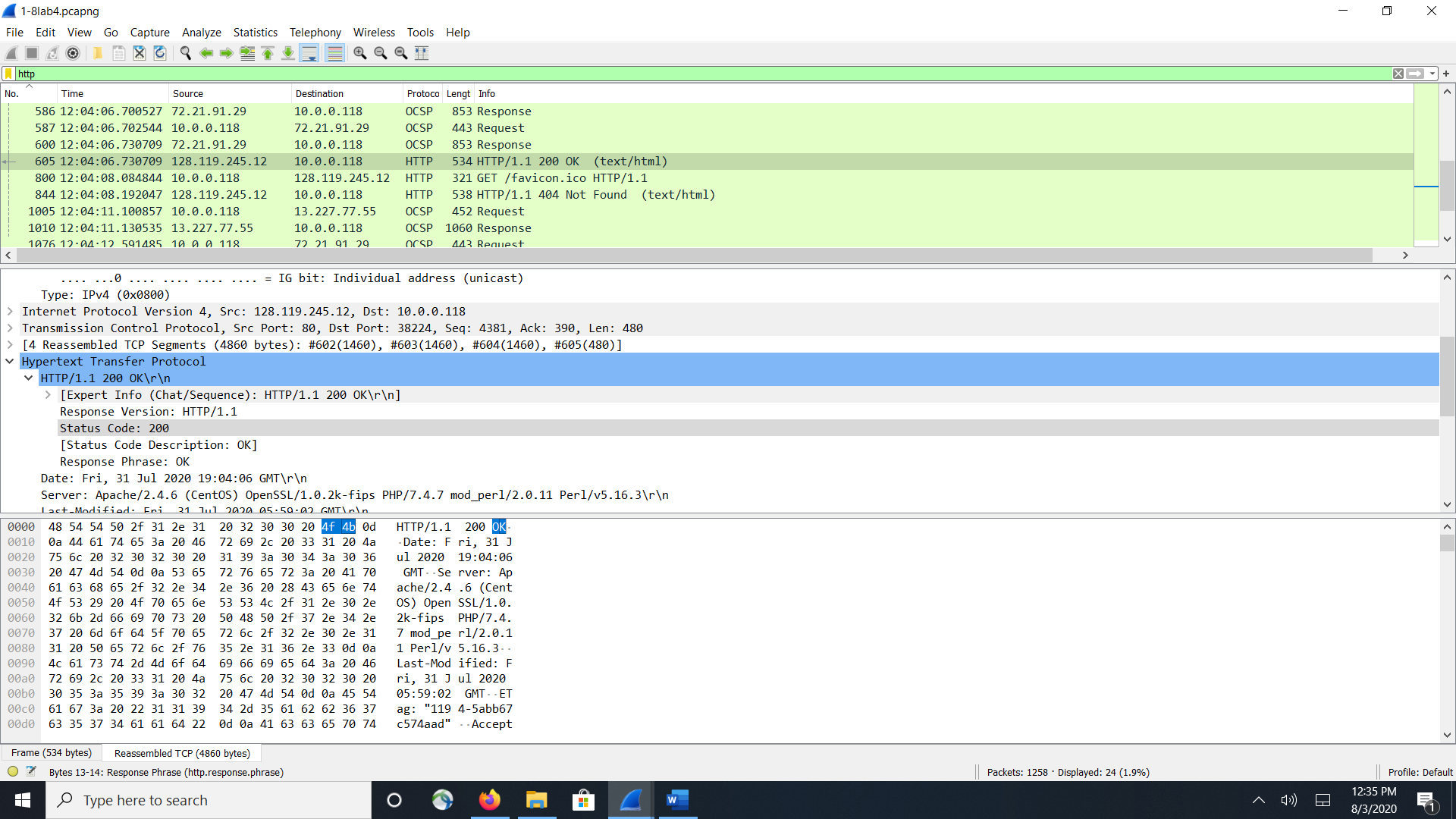
Destination: IntelCor\_07:2f:8d (e4:a7:a0:07:2f:8d)( from above) this is my pc

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

(0x0800) the upper layer protocol that this corresponds to is IP protocol(valie is in the screen shot above)

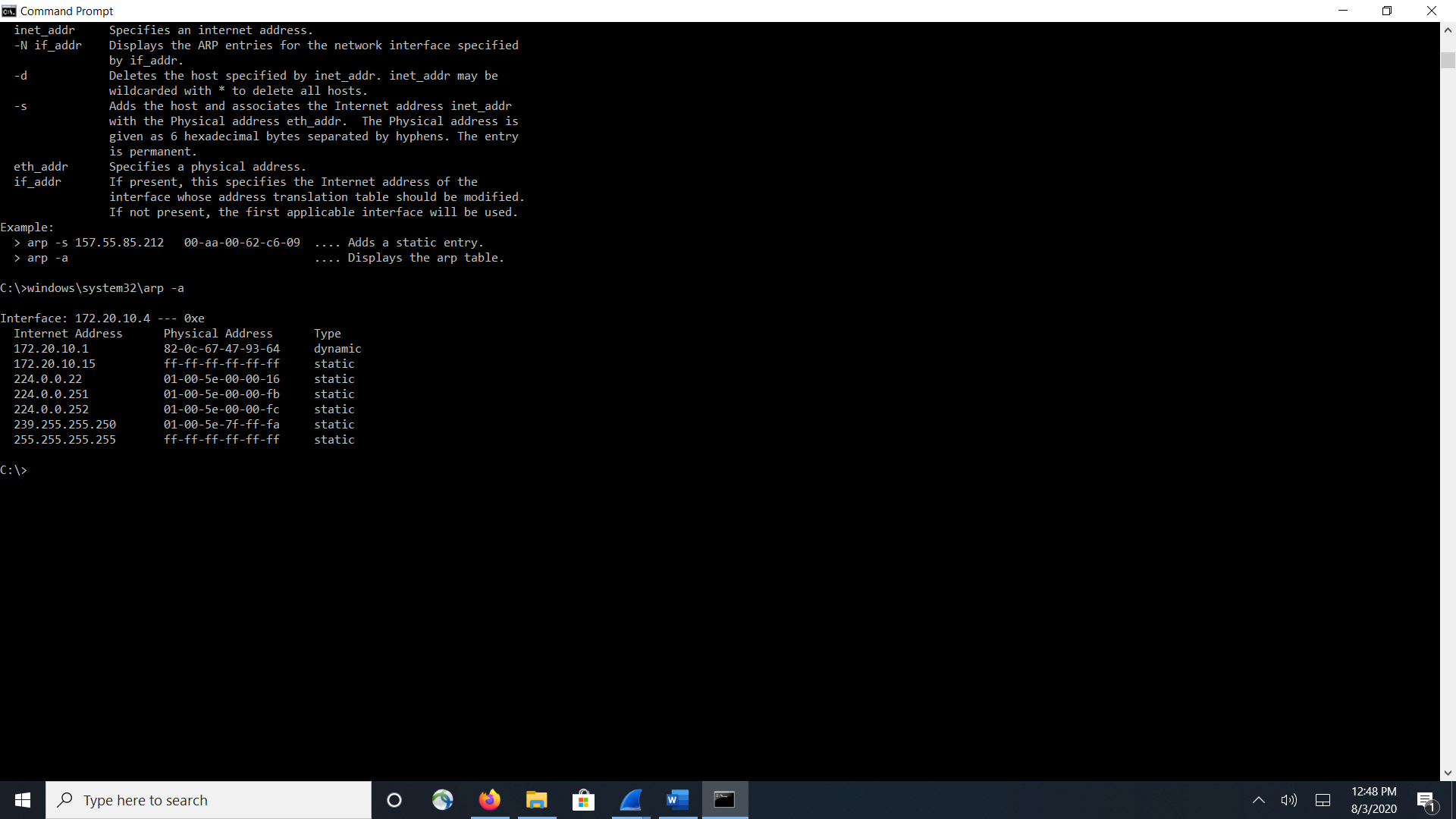
8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?

at the bottom of the screen shot it shows that after byte 13 the “O” appears in the frame



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

the value of each column is as follows the internet address is the address of Ip address of each device, The physical address is the MAC address of each device and the type is the protocol of each device



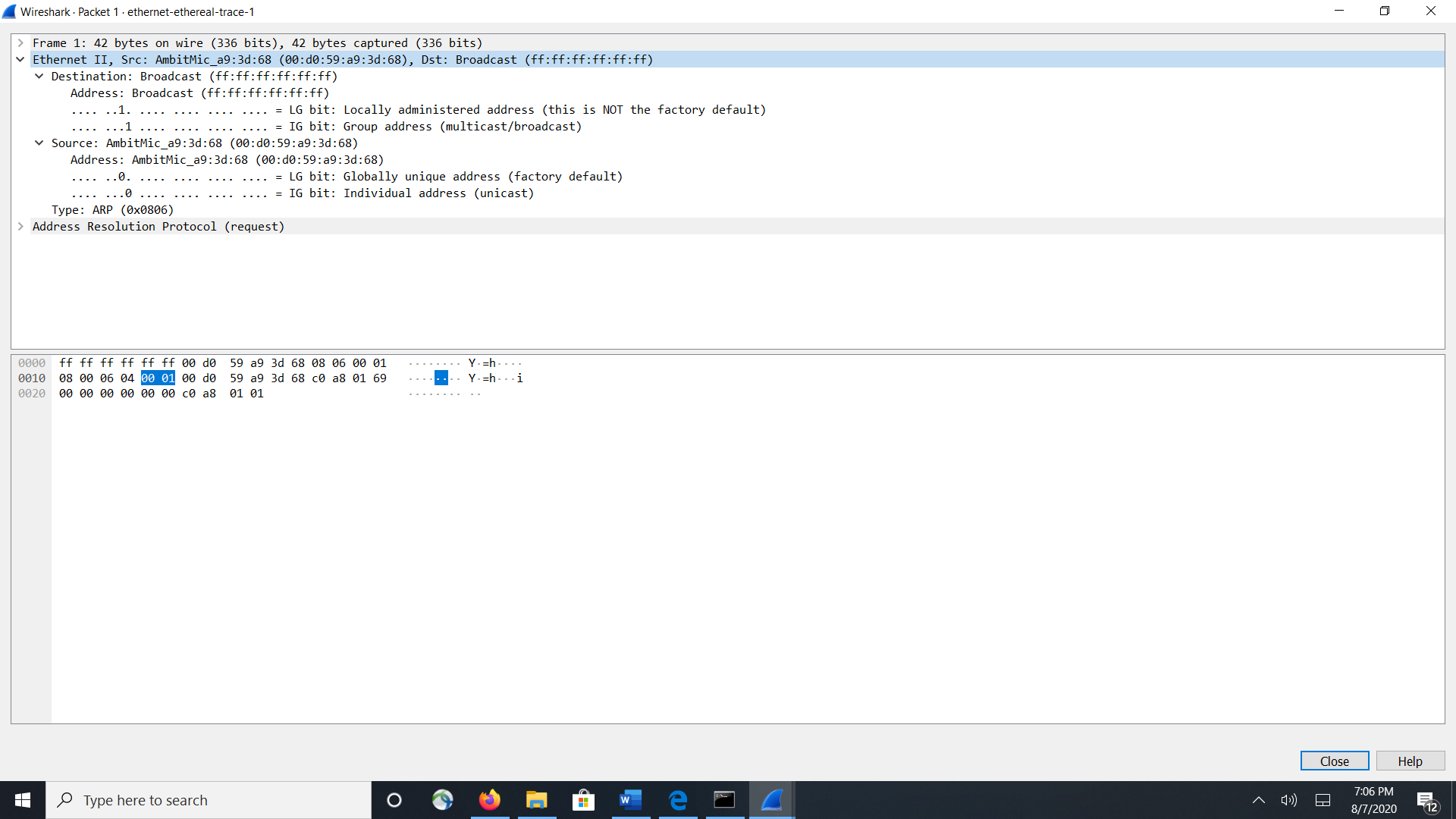
10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Address: Broadcast (ff:ff:ff:ff:ff:ff)

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

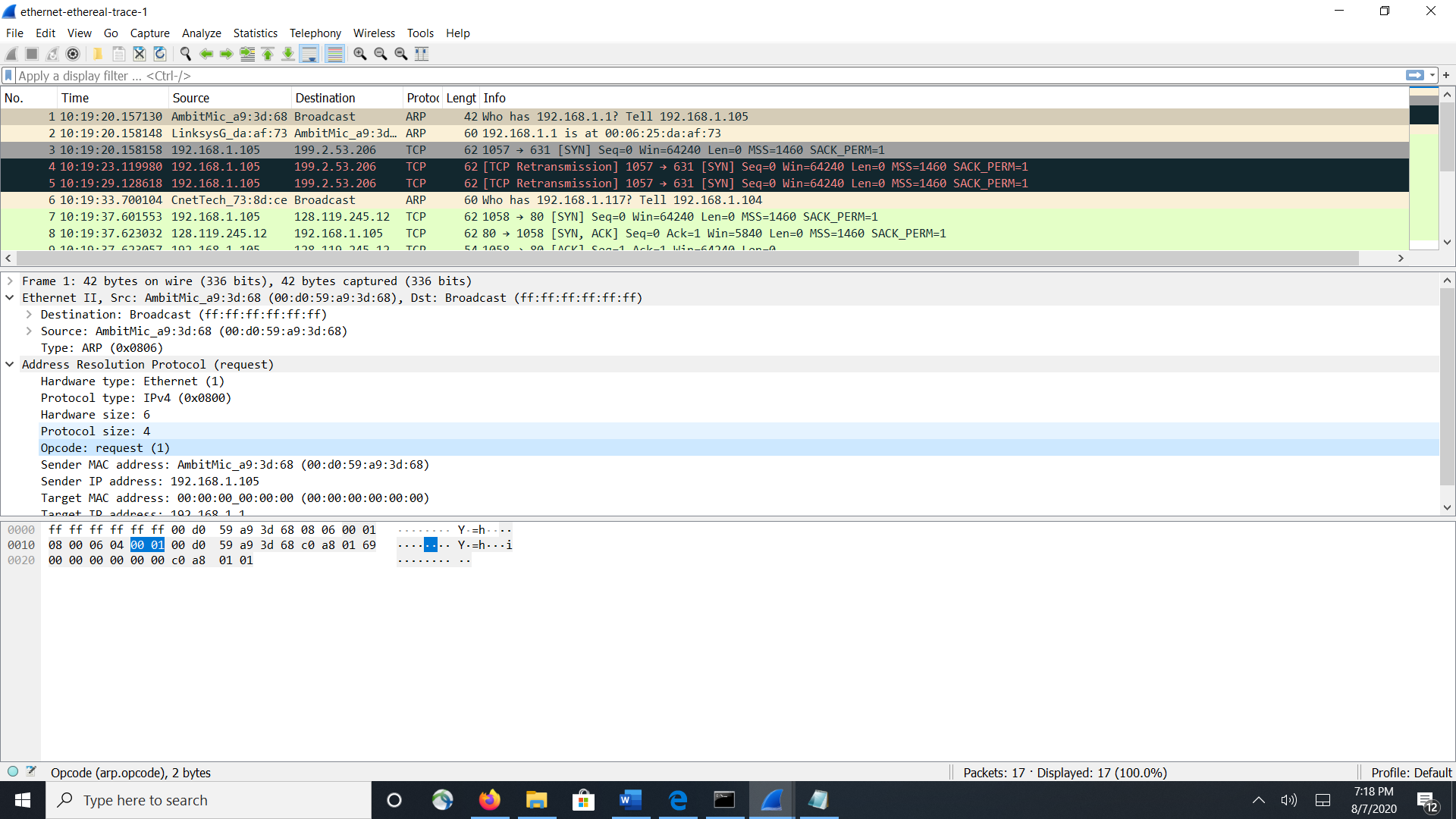
Address: AmbitMic\_a9:3d:68 (00:d0:59:a9:3d:68)



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

Type: ARP (0x0806)(in screen shot above), and the protocol is ARP

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? bytes 20-21

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?

0001

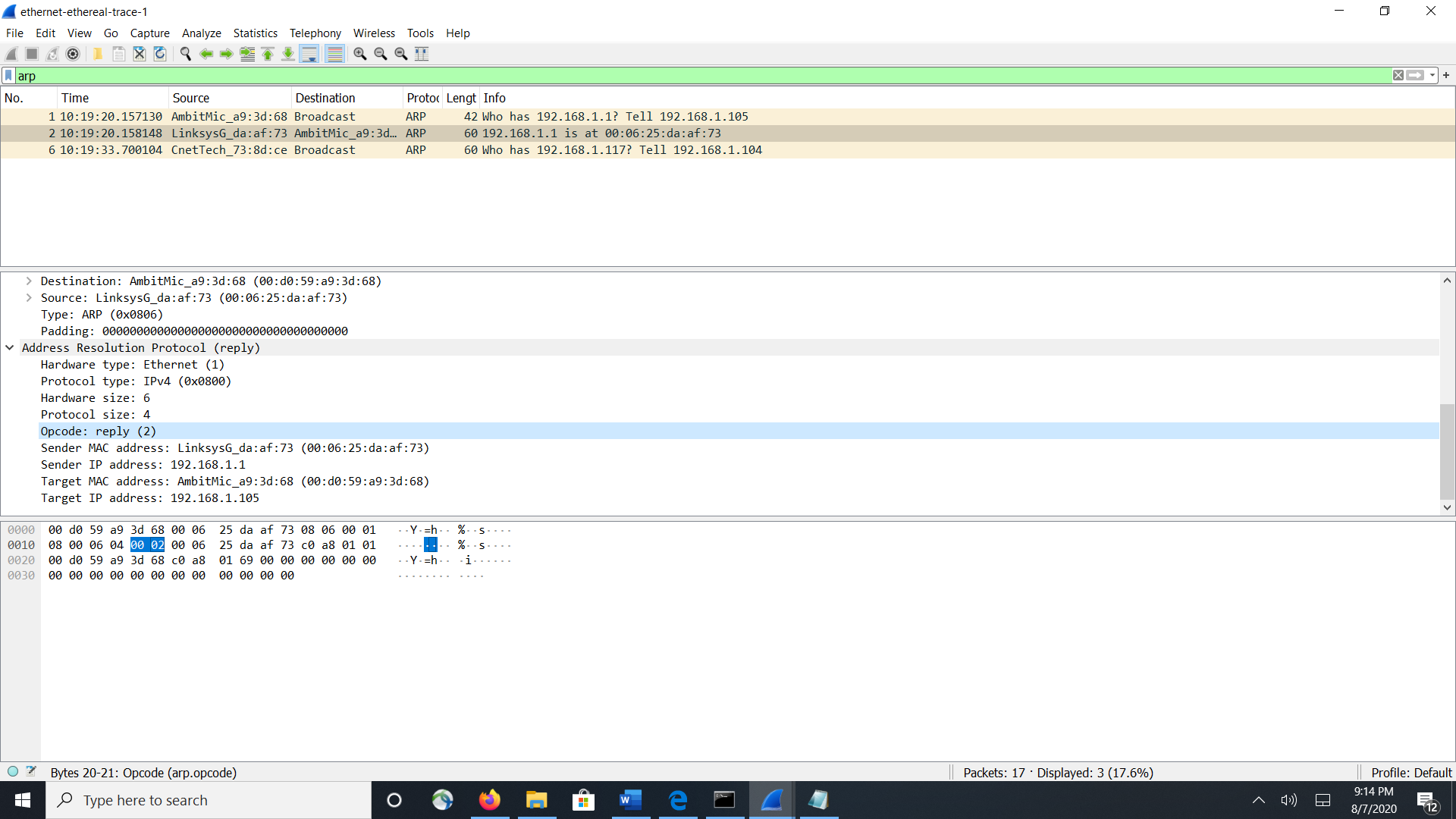
c) Does the ARP message contain the IP address of the sender?

Sender IP address: 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?

who has 192.168.1.1? it appears in the Target IP address: 192.168.1.1 which is the router

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?

20 bytes

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?

0002

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?

192.168.1.1 is at 00:06:25:da:af:73 appears in Sender MAC address: LinksysG\_da:af:73 (00:06:25:da:af:73) Sender IP address: 192.168.1.1 this is the router

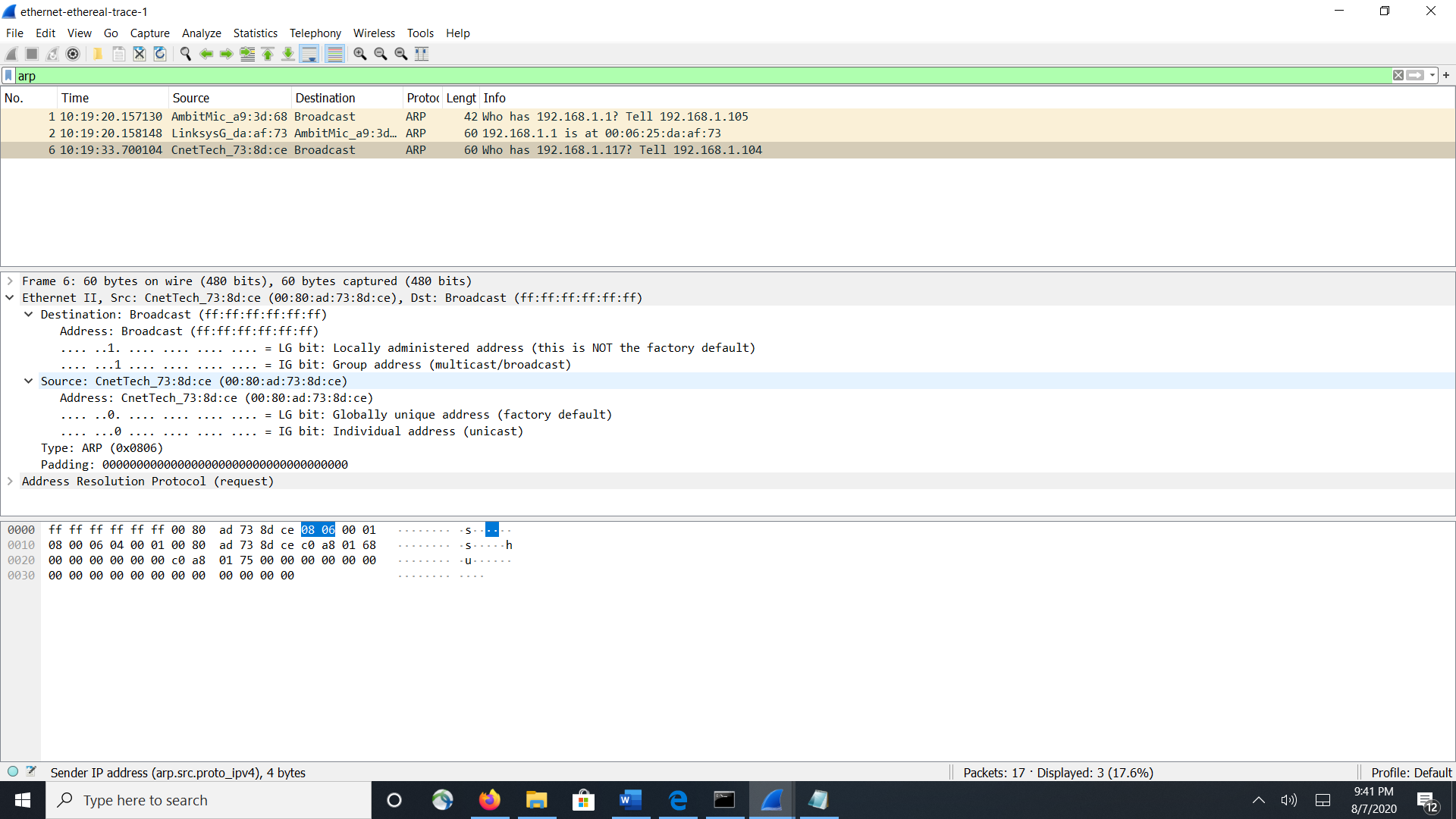
14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Address: Broadcast (ff:ff:ff:ff:ff:ff)

Source: CnetTech\_73:8d:ce (00:80:ad:73:8d:ce)

Address: CnetTech\_73:8d:ce (00:80:ad:73:8d:ce)



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?

We can only see the reply from our own pc because it was sent directly to the pc