Justin Phillips

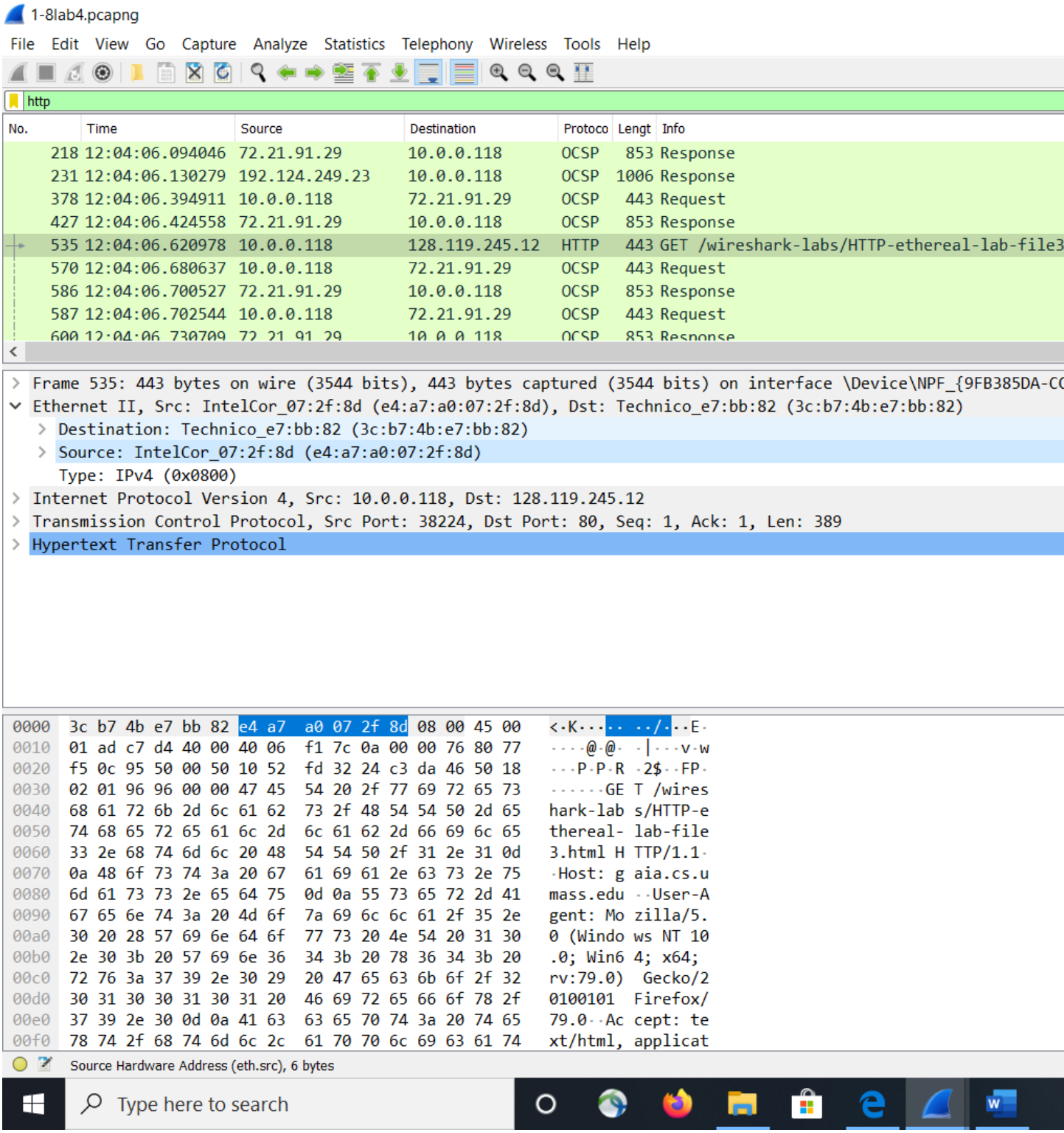
cs372 2020

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)

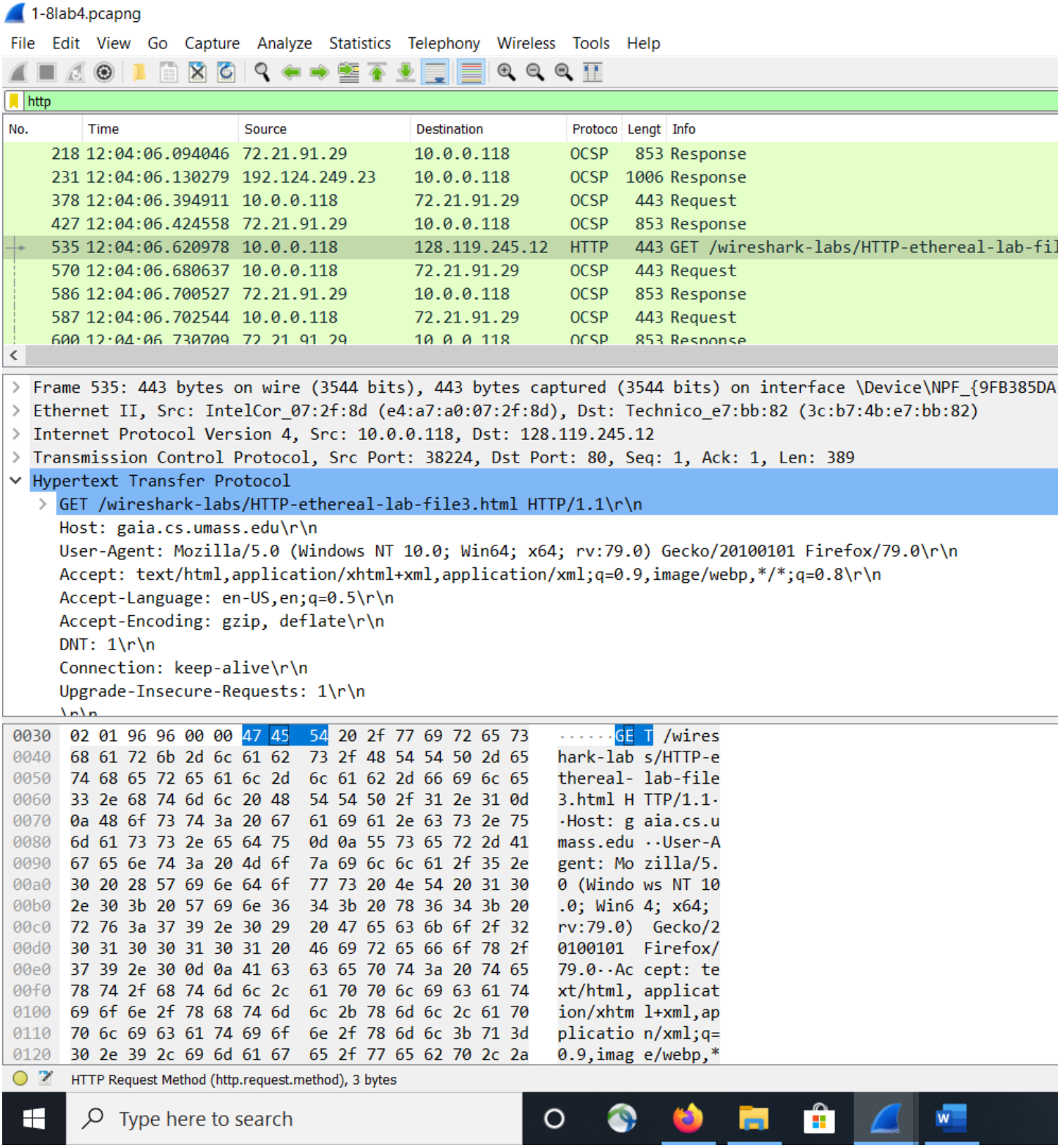
this is the address of my router

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?

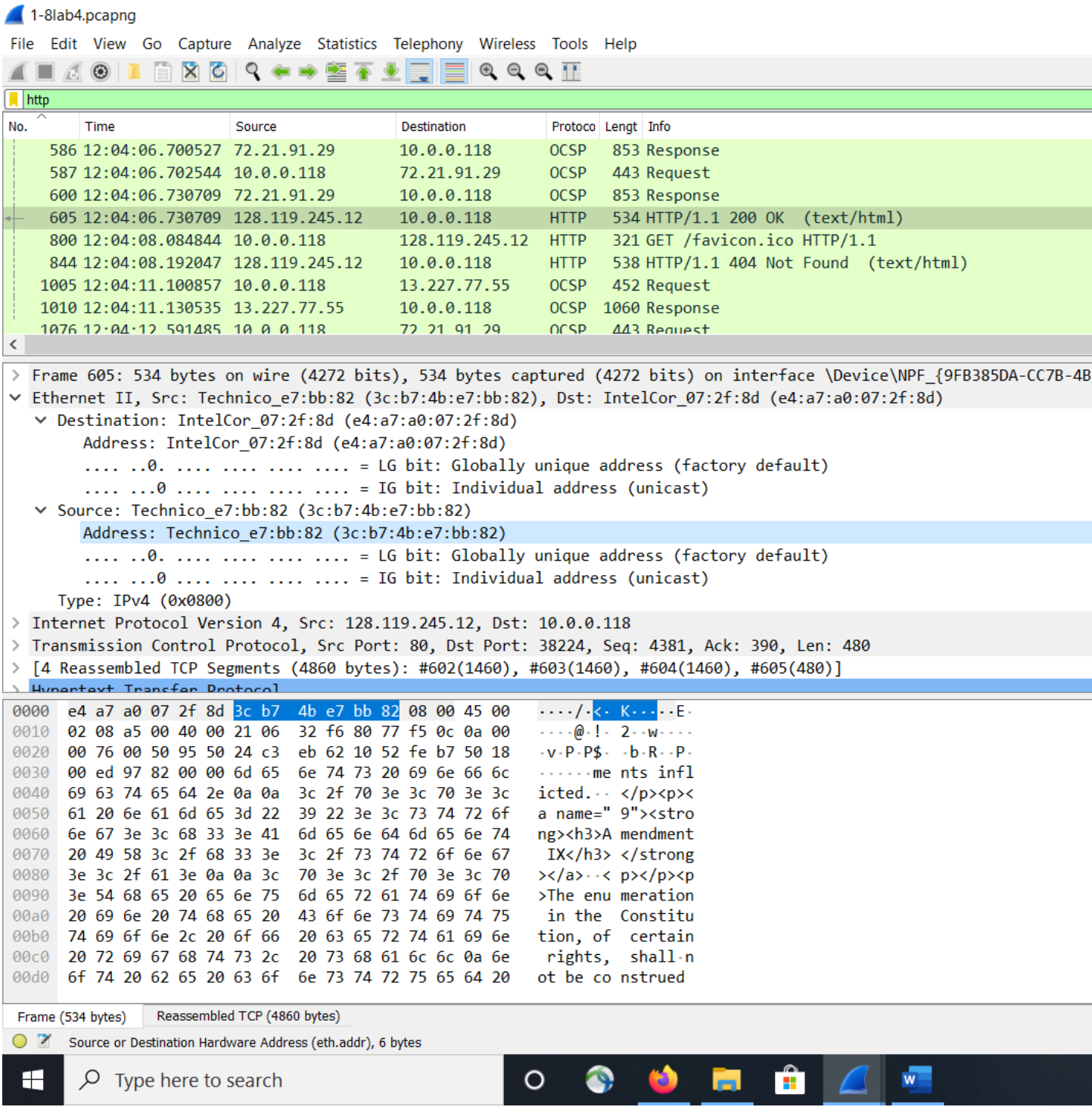
bytes 54-56 is the GET request, so 54 would be the G


1-8lab4.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
No. Time Source Destination Protoco Lengt Info
218 12:04:06.094046 72.21.91.29 10.0.0.118 OCSP 853 Response
231 12:04:06.130279 192.124.249.23 10.0.0.118 OCSP 1006 Response
378 12:04:06.394911 10.0.0.118 72.21.91.29 OCSP 443 Request
427 12:04:06.424558 72.21.91.29 10.0.0.118 OCSP 853 Response
535 12:04:06.620978 10.0.0.118 128.119.245.12 HTTP 443 GET /wireshark-labs/HTTP-ethereal-lab-fil
570 12:04:06.680637 10.0.0.118 72.21.91.29 OCSP 443 Request
586 12:04:06.700527 72.21.91.29 10.0.0.118 OCSP 853 Response
587 12:04:06.702544 10.0.0.118 72.21.91.29 OCSP 443 Request
600 12:04:06.730709 72.21.91.29 10.0.0.118 OCSP 853 Response
Frame 535: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface \Device\NPF_{9FB385DA
Ethernet II, Src: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d), Dst: Technico_e7:bb:82 (3c:b7:4b:e7:bb:82)
Internet Protocol Version 4, Src: 10.0.0.118, Dst: 128.119.245.12
Transmission Control Protocol, Src Port: 38224, Dst Port: 80, Seq: 1, Ack: 1, Len: 389
Hypertext Transfer Protocol
GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n
Host: gaia.cs.umass.edu\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
DNT: 1\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
0030 02 01 96 96 00 00 47 45 54 20 2f 77 69 72 65 73 ····· GE T /wires
0040 68 61 72 6b 2d 6c 61 62 73 2f 48 54 54 50 2d 65 hark-lab s/HTTP-e
0050 74 68 65 72 65 61 6c 2d 6c 61 62 2d 66 69 6c 65 thereal- lab-file
0060 33 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e 31 0d 3.html H TTP/1.1·
0070 0a 48 6f 73 74 3a 20 67 61 69 61 2e 63 73 2e 75 ·Host: g aia.cs.u
0080 6d 61 73 73 2e 65 64 75 0d 0a 55 73 65 72 2d 41 mass.edu ··User-A
0090 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e gent: Mo zilla/5.
00a0 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 0 (Windo ws NT 10
00b0 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 3b 20 .0; Win6 4; x64;
00c0 72 76 3a 37 39 2e 30 29 20 47 65 63 6b 6f 2f 32 rv:79.0) Gecko/2
00d0 30 31 30 30 31 30 31 20 46 69 72 65 66 6f 78 2f 0100101 Firefox/
00e0 37 39 2e 30 0d 0a 41 63 63 65 70 74 3a 20 74 65 79.0··Ac cept: te
00f0 78 74 2f 68 74 6d 6c 2c 61 70 70 6c 69 63 61 74 xt/html, applicat
0100 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d 6c 2c 61 70 ion/xhtm l+xml,ap
0110 70 6c 69 63 61 74 69 6f 6e 2f 78 6d 6c 3b 71 3d plicatio n/xml;q=
0120 30 2e 39 2c 69 6d 61 67 65 2f 77 65 62 70 2c 2a 0.9,imag e/webp,*
HTTP Request Method (http.request.method), 3 bytes
Type here to search

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?

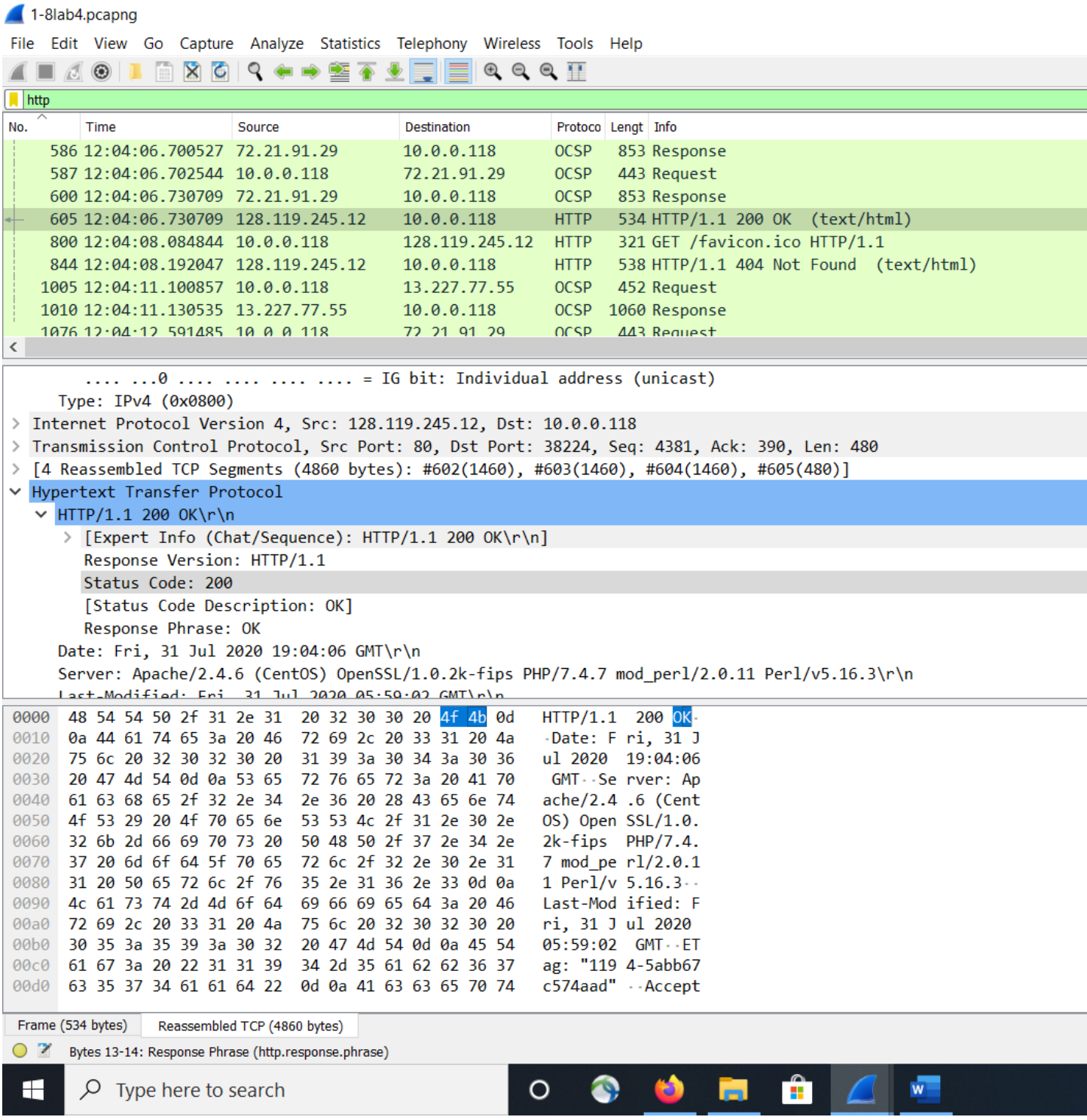
Destination: IntelCor_07:2f:8d (e4:a7:a0:07:2f:8d)(from above) this is my pc

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)

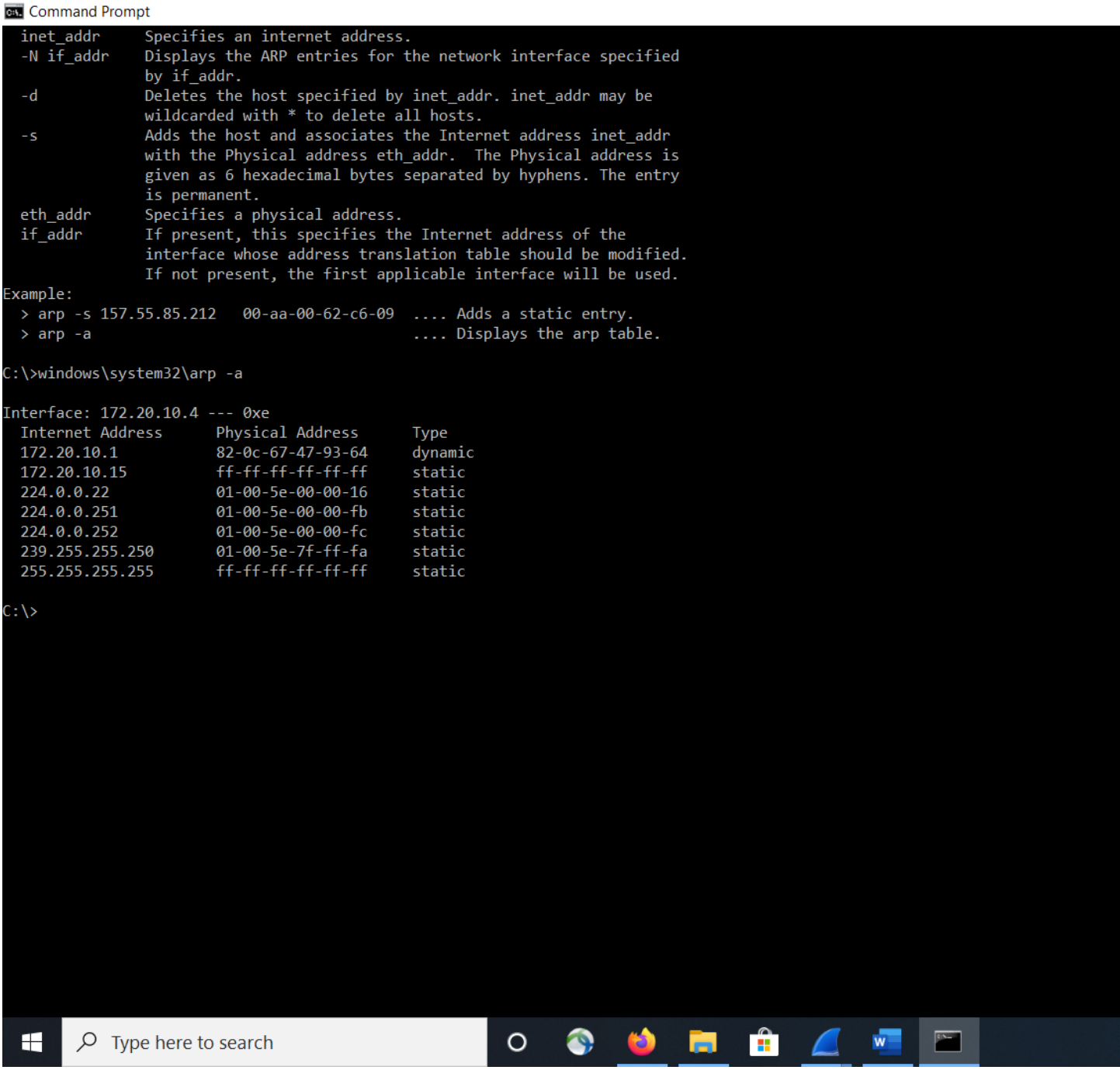
8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?

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



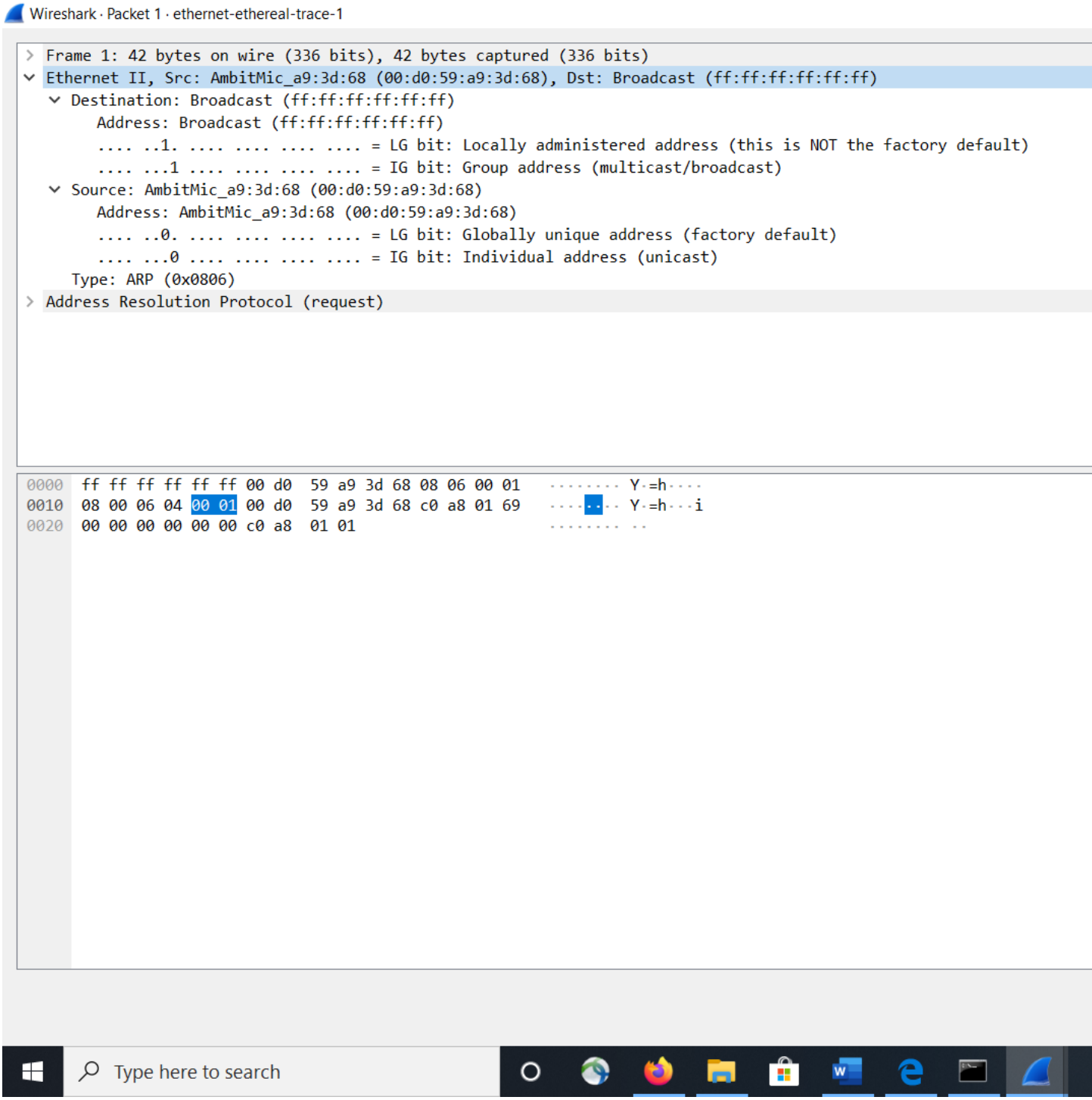
10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?

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)

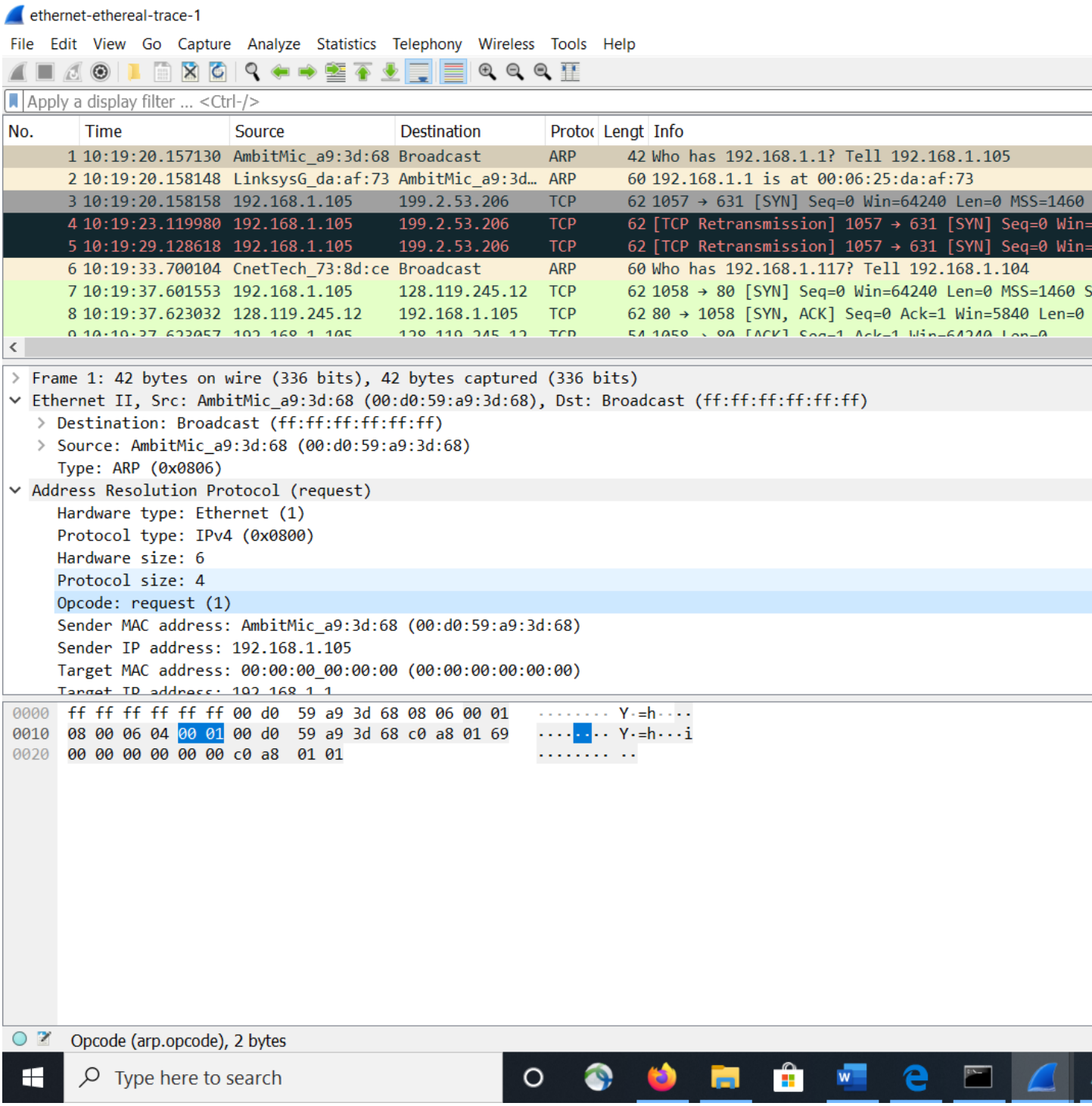
Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)



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

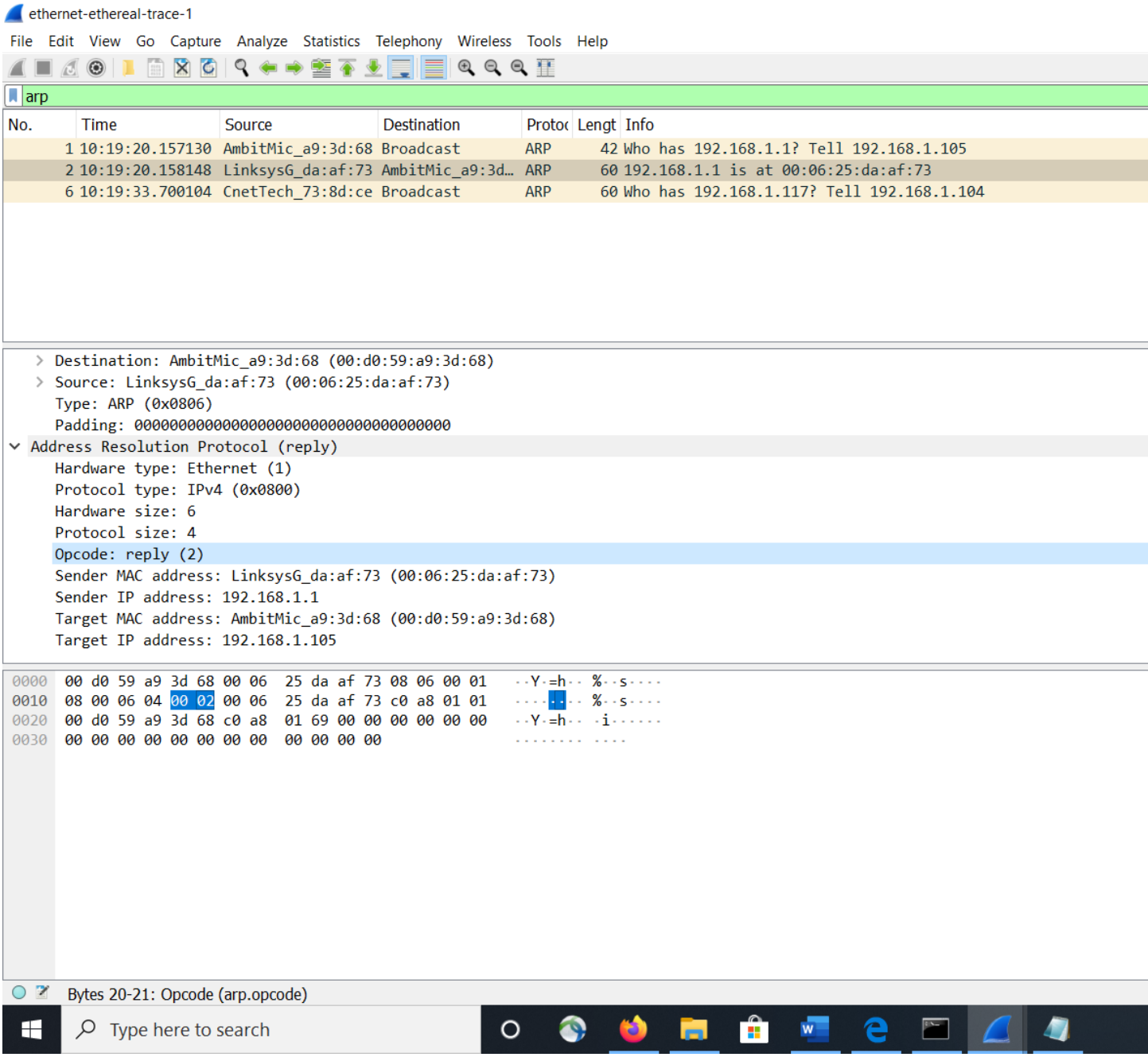
c) Does the ARP message contain the IP address of the sender?

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

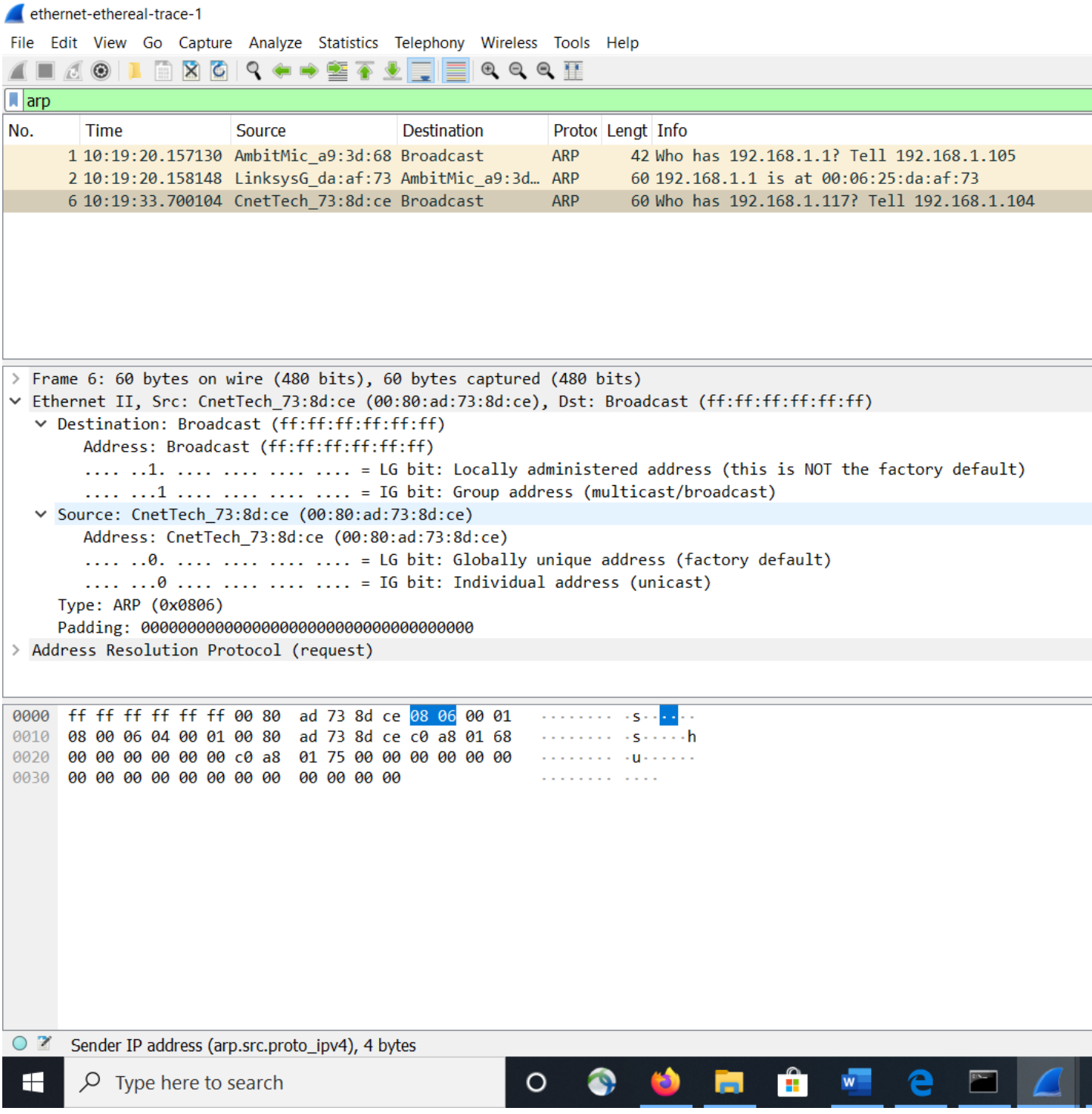
14. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

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