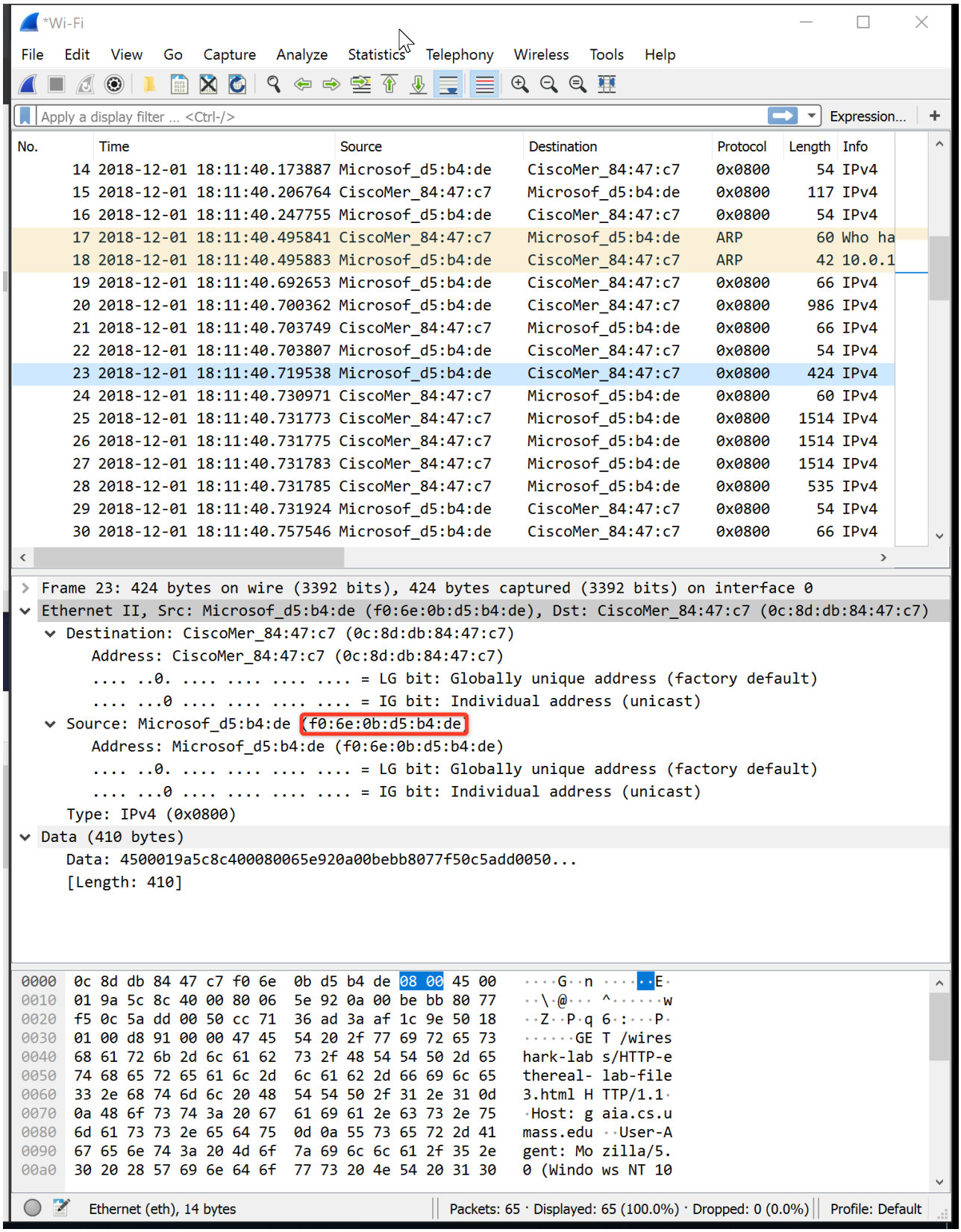
Joel Benjamin Castillo (jc5383)
CS6843 - Computer Networking
Prof. Rafail Portnoy

Wireshark Lab - Ethernet

Ethernet Frames

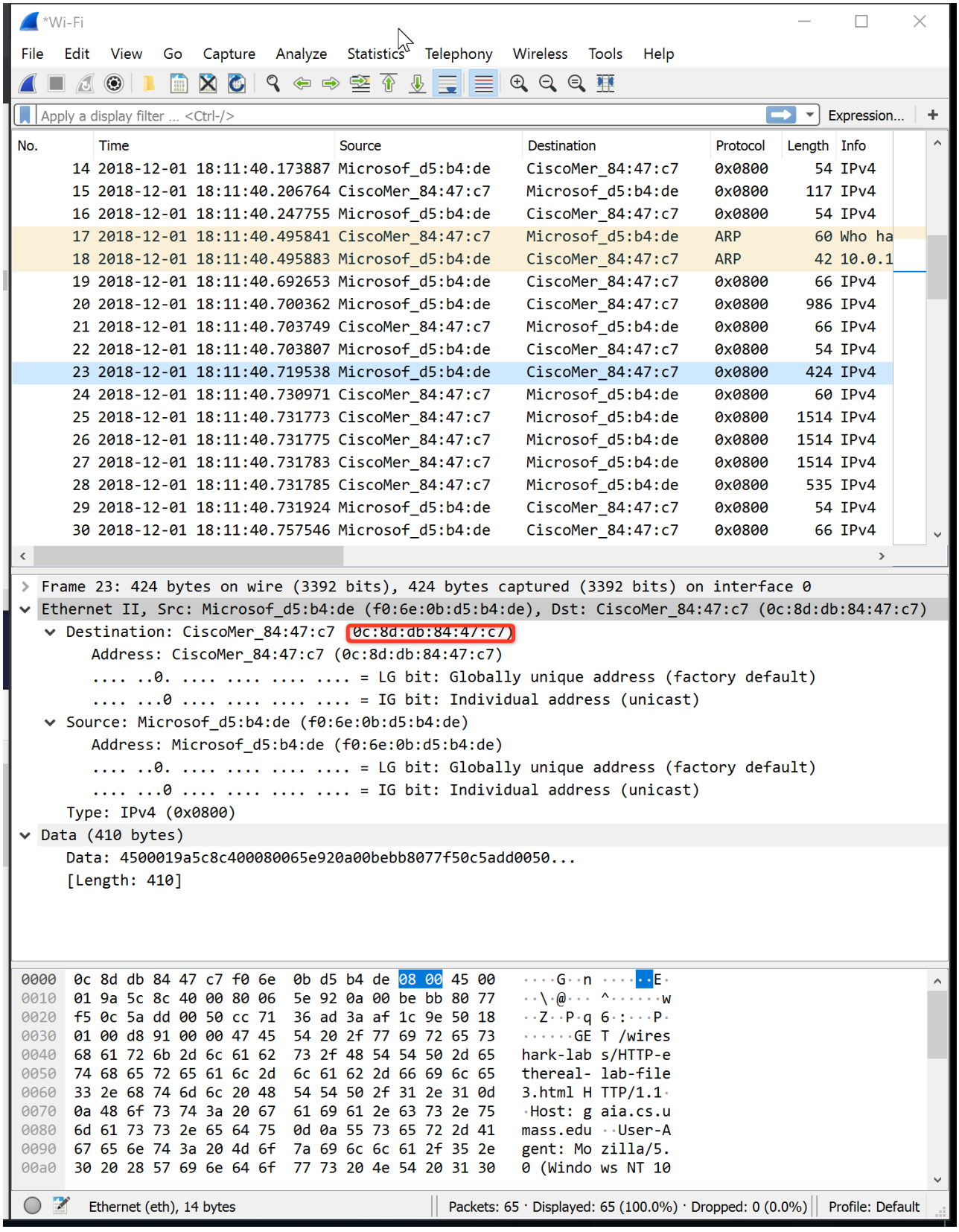
1. What is the 48-bit Ethernet address of your computer?
   `f0:6e:0b:d5:b4:de`



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.]

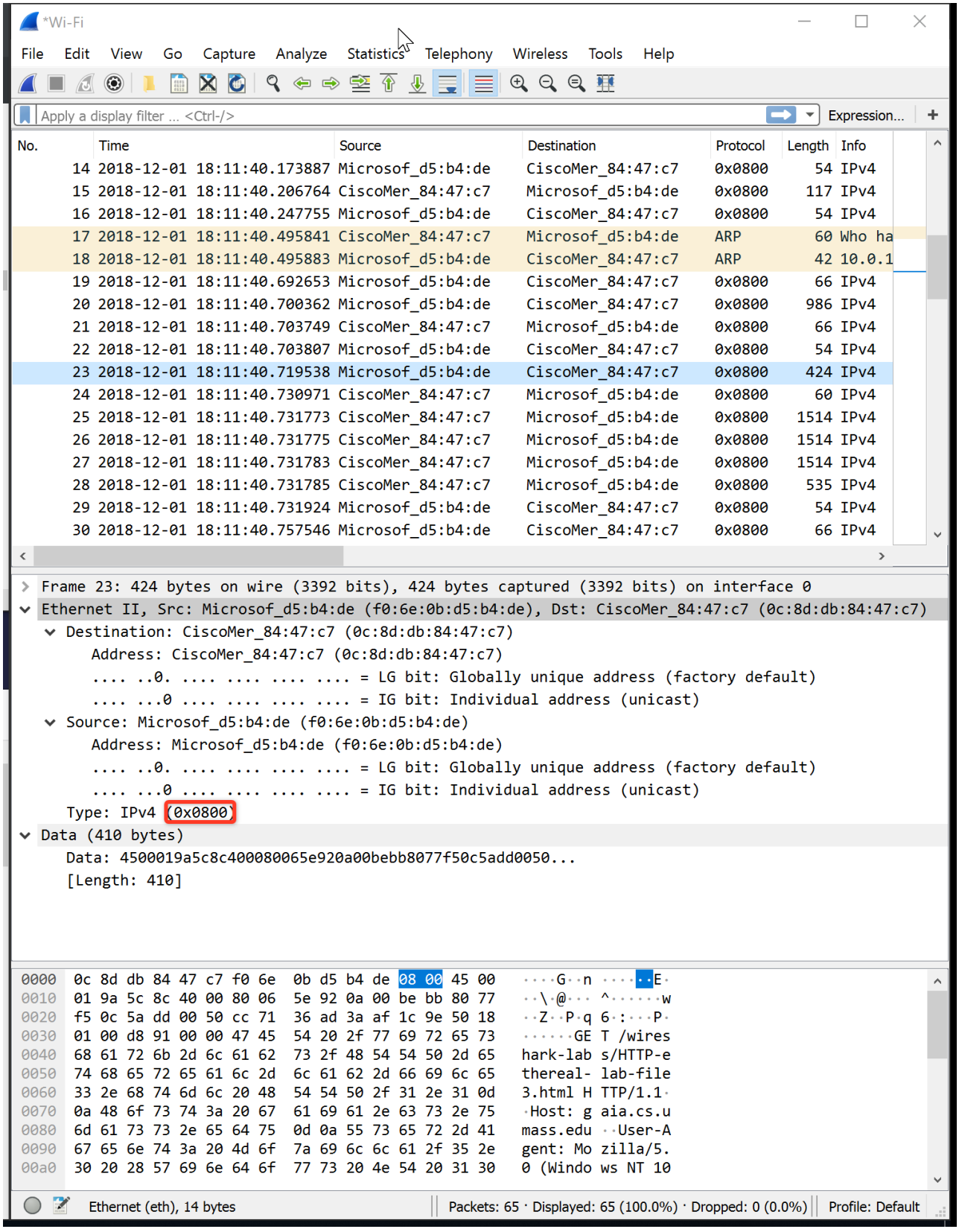
   `0c:8d:db:84:47:c7`

This is the Ethernet address of the router I am connected to.



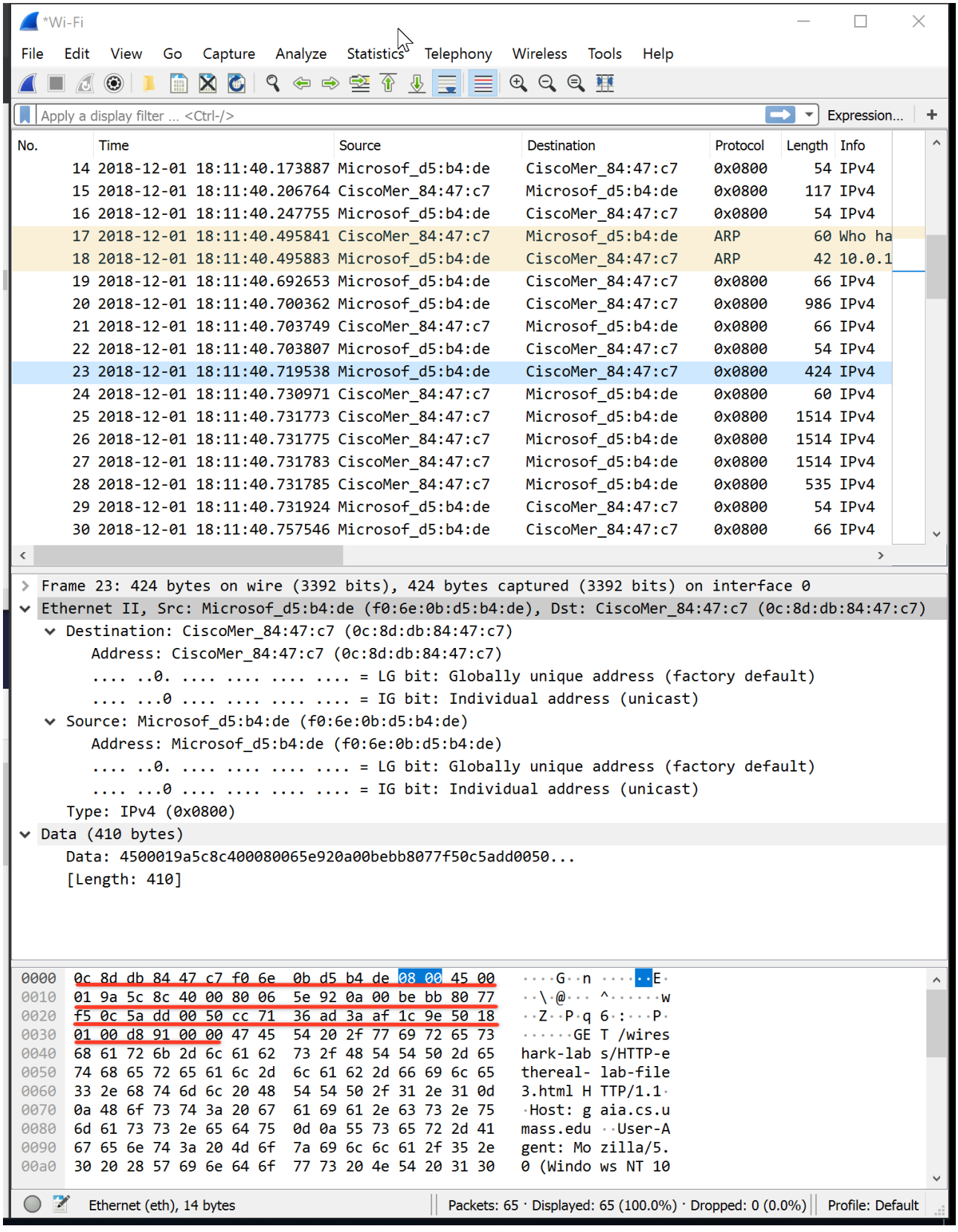
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

`0x0800` - IP



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

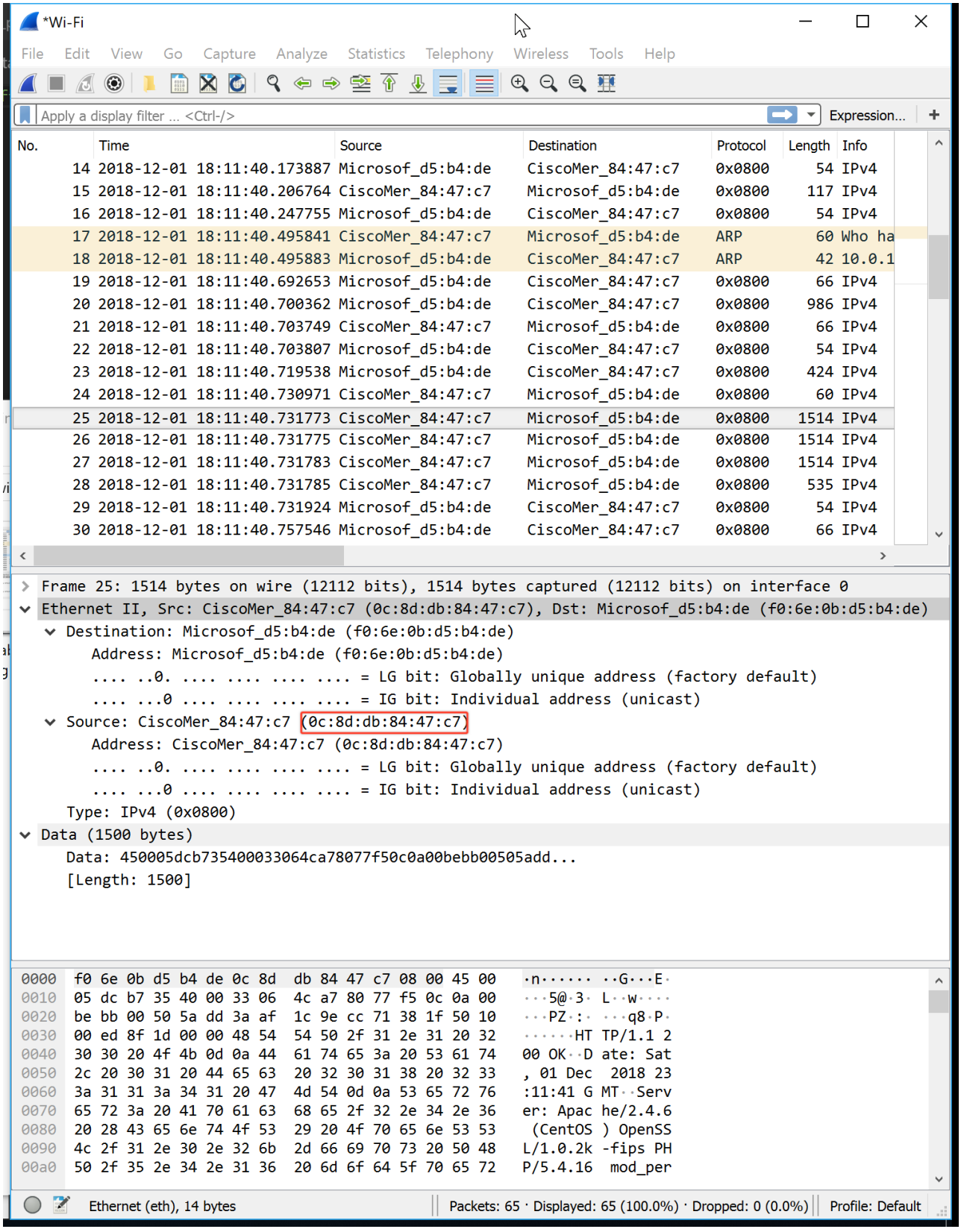
54 bytes



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?

   0c:8d:db:84:47:c7

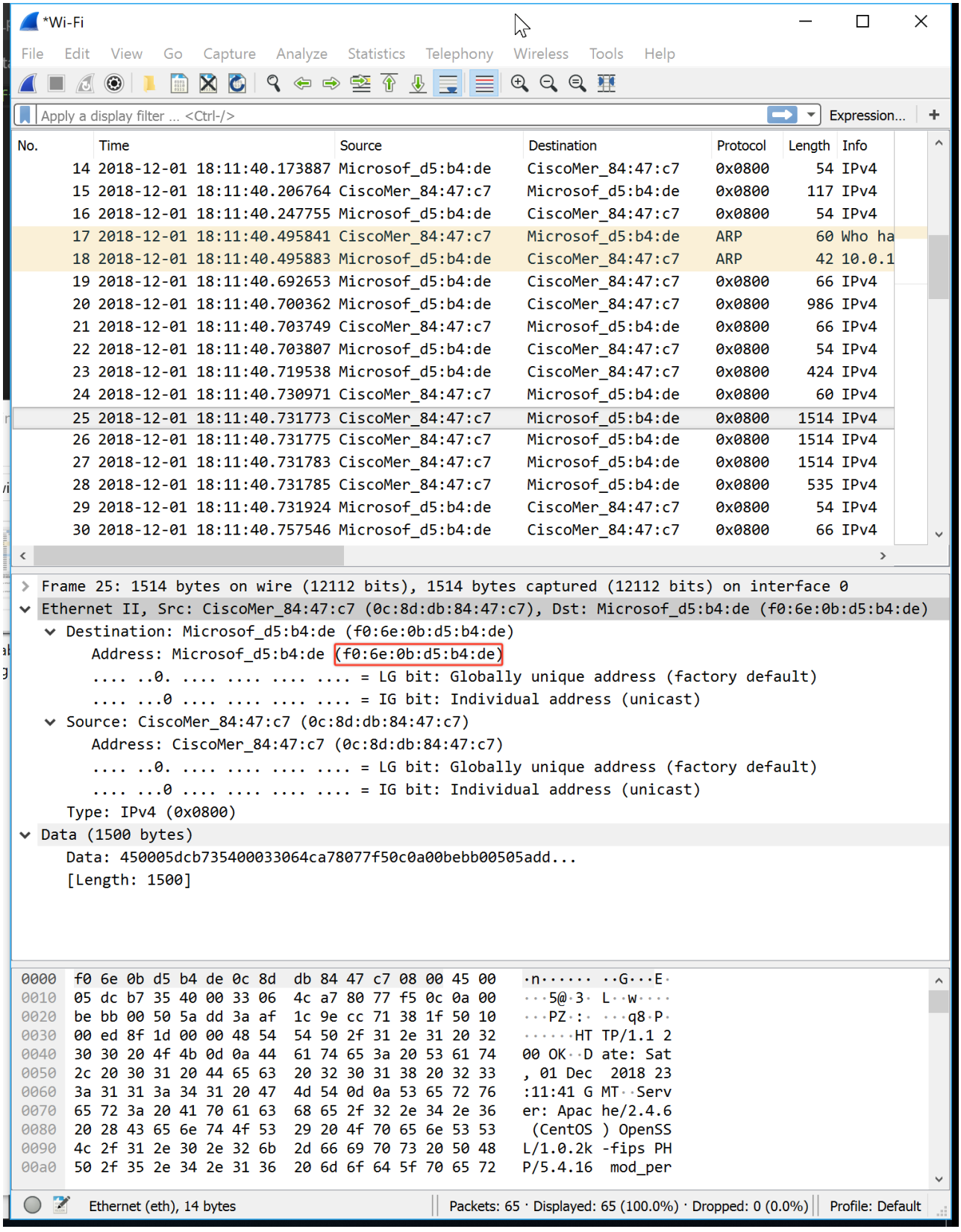
This is the Ethernet address of the router that I am connected to.



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

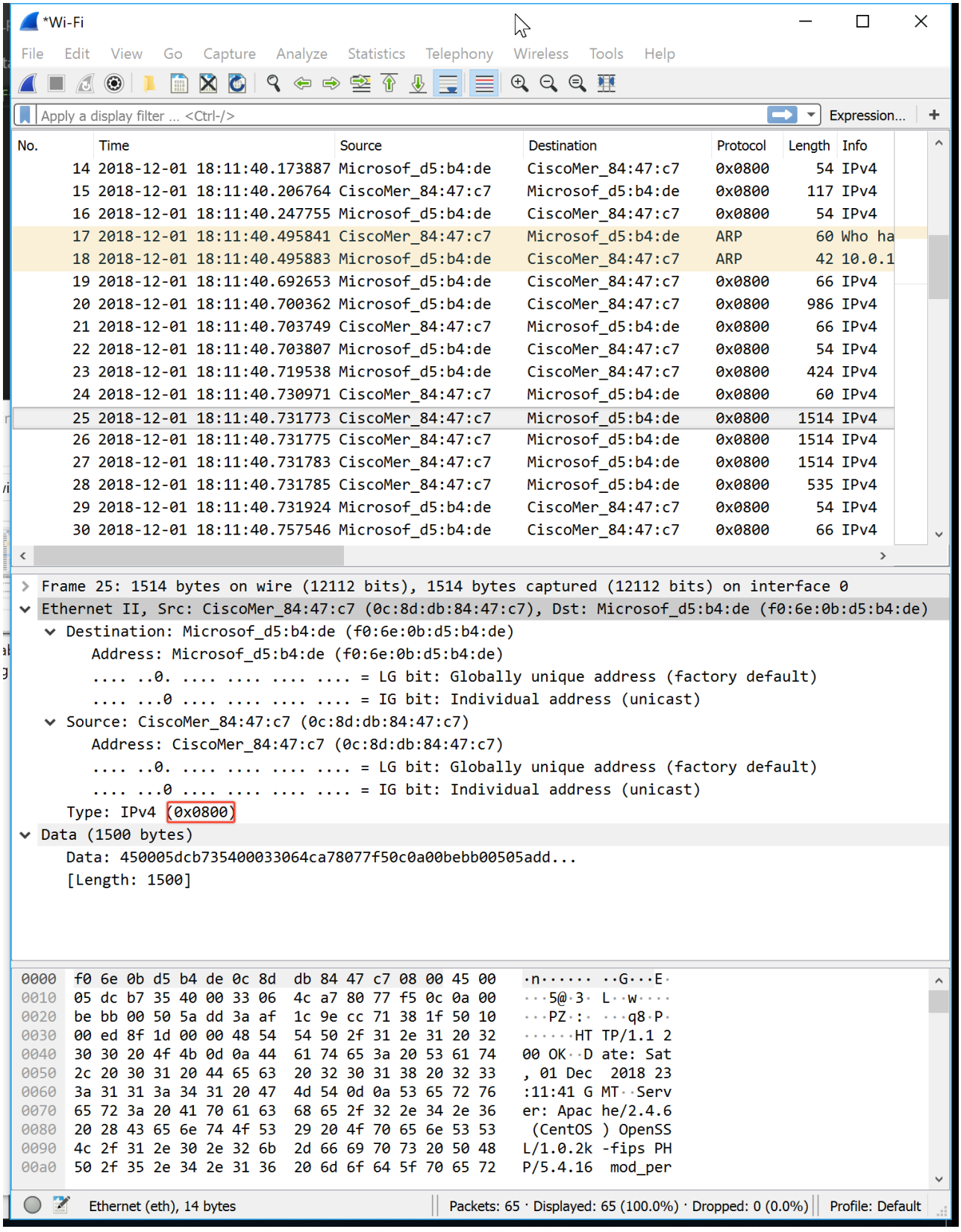
`f0:6e:0b:d5:b4:de`

Yes, this is the Ethernet address of my network adapter.



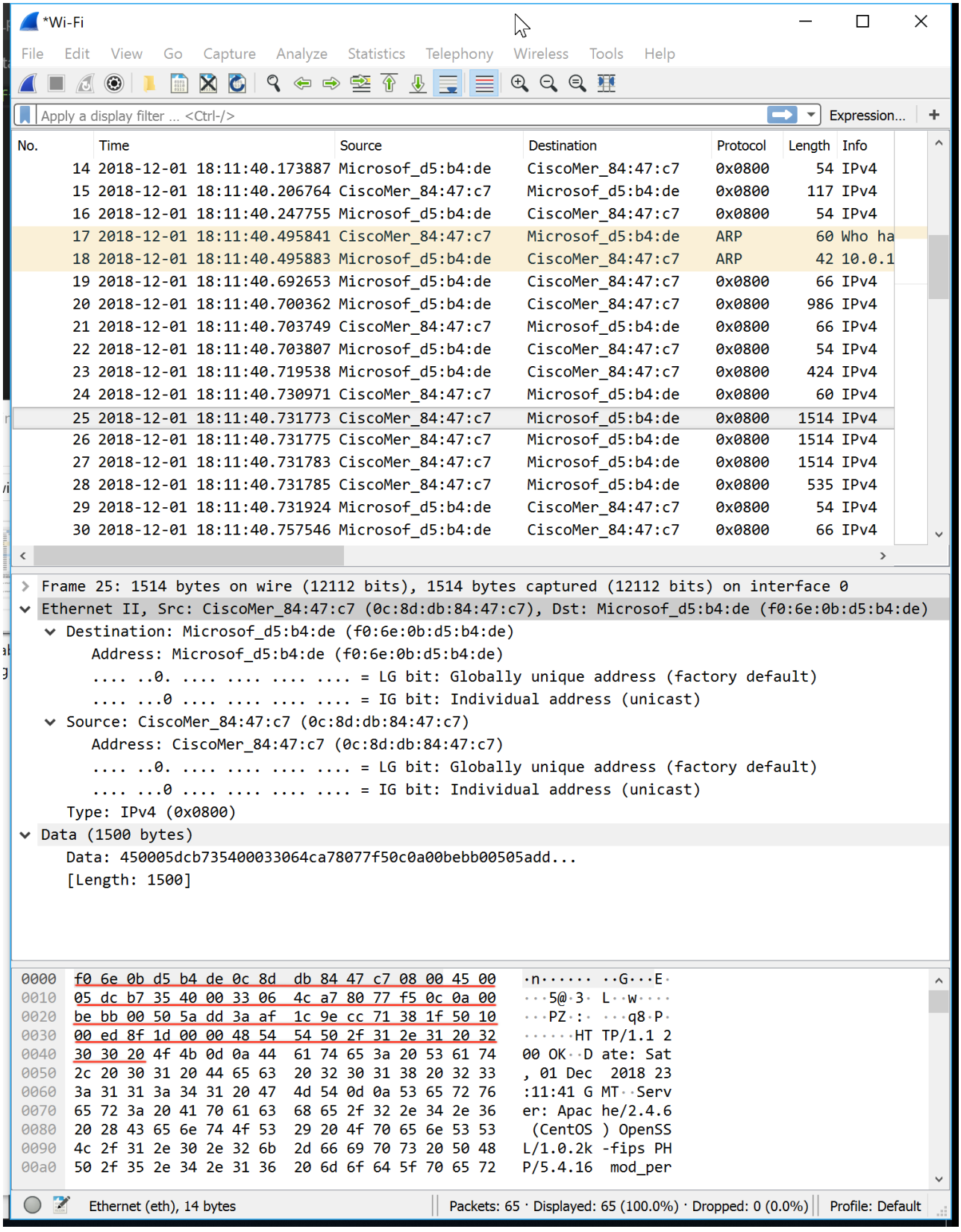
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

`0x0800` - IP



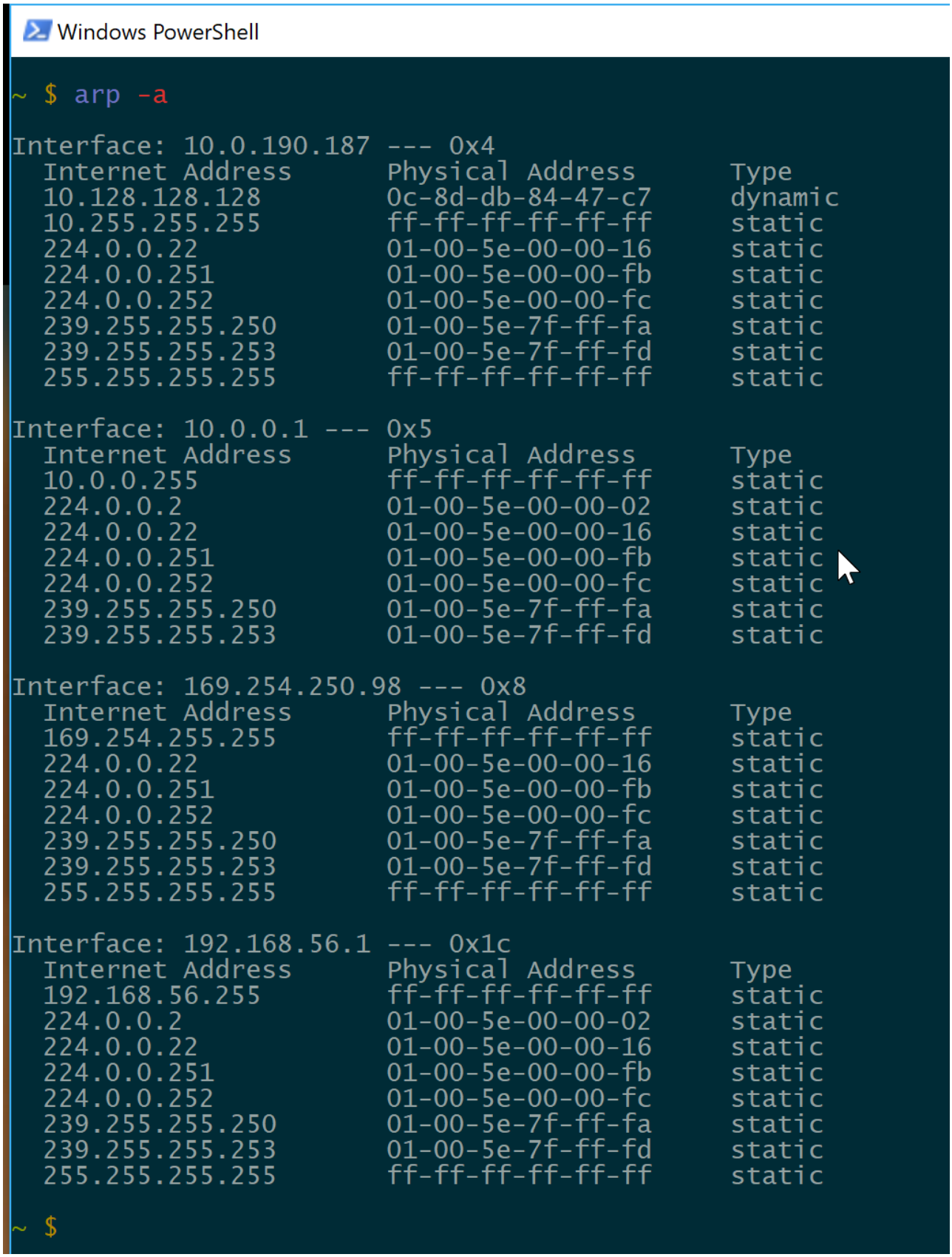
8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" (i.e., the HTTP response code) appear in the Ethernet frame?

67 bytes


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
14 2018-12-01 18:11:40.173887 Microsof_d5:b4:de CiscoMer_84:47:c7 0x0800 54 IPv4
15 2018-12-01 18:11:40.206764 CiscoMer_84:47:c7 Microsof_d5:b4:de 0x0800 117 IPv4
16 2018-12-01 18:11:40.247755 Microsof_d5:b4:de CiscoMer_84:47:c7 0x0800 54 IPv4
17 2018-12-01 18:11:40.495841 CiscoMer_84:47:c7 Microsof_d5:b4:de ARP 60 Who ha
18 2018-12-01 18:11:40.495883 Microsof_d5:b4:de CiscoMer_84:47:c7 ARP 42 10.0.1
19 2018-12-01 18:11:40.692653 Microsof_d5:b4:de CiscoMer_84:47:c7 0x0800 66 IPv4
20 2018-12-01 18:11:40.700362 Microsof_d5:b4:de CiscoMer_84:47:c7 0x0800 986 IPv4
21 2018-12-01 18:11:40.703749 CiscoMer_84:47:c7 Microsof_d5:b4:de 0x0800 66 IPv4
22 2018-12-01 18:11:40.703807 Microsof_d5:b4:de CiscoMer_84:47:c7 0x0800 54 IPv4
23 2018-12-01 18:11:40.719538 Microsof_d5:b4:de CiscoMer_84:47:c7 0x0800 424 IPv4
24 2018-12-01 18:11:40.730971 CiscoMer_84:47:c7 Microsof_d5:b4:de 0x0800 60 IPv4
25 2018-12-01 18:11:40.731773 CiscoMer_84:47:c7 Microsof_d5:b4:de 0x0800 1514 IPv4
26 2018-12-01 18:11:40.731775 CiscoMer_84:47:c7 Microsof_d5:b4:de 0x0800 1514 IPv4
27 2018-12-01 18:11:40.731783 CiscoMer_84:47:c7 Microsof_d5:b4:de 0x0800 1514 IPv4
28 2018-12-01 18:11:40.731785 CiscoMer_84:47:c7 Microsof_d5:b4:de 0x0800 535 IPv4
29 2018-12-01 18:11:40.731924 Microsof_d5:b4:de CiscoMer_84:47:c7 0x0800 54 IPv4
30 2018-12-01 18:11:40.757546 Microsof_d5:b4:de CiscoMer_84:47:c7 0x0800 66 IPv4
Frame 25: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Ethernet II, Src: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7), Dst: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
Destination: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
Address: Microsof_d5:b4:de (f0:6e:0b:d5:b4:de)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Source: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
Address: CiscoMer_84:47:c7 (0c:8d:db:84:47:c7)
.... ..0. .... = LG bit: Globally unique address (factory default)
....0 .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
Data (1500 bytes)
Data: 450005dcb735400033064ca78077f50c0a00bebb00505add...
[Length: 1500]
0000 f0 6e 0b d5 b4 de 0c 8d db 84 47 c7 08 00 45 00 ·n····· ··G···E·
0010 05 dc b7 35 40 00 33 06 4c a7 80 77 f5 0c 0a 00 ···5@·3· L··w····
0020 be bb 00 50 5a dd 3a af 1c 9e cc 71 38 1f 50 10 ···PZ·:· ···q8·P·
0030 00 ed 8f 1d 00 00 48 54 54 50 2f 31 2e 31 20 32 ·····HT TP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 53 61 74 00 OK··D ate: Sat
0050 2c 20 30 31 20 44 65 63 20 32 30 31 38 20 32 33 , 01 Dec 2018 23
0060 3a 31 31 3a 34 31 20 47 4d 54 0d 0a 53 65 72 76 :11:41 G MT··Serv
0070 65 72 3a 20 41 70 61 63 68 65 2f 32 2e 34 2e 36 er: Apac he/2.4.6
0080 20 28 43 65 6e 74 4f 53 29 20 4f 70 65 6e 53 53 (CentOS) OpenSS
0090 4c 2f 31 2e 30 2e 32 6b 2d 66 69 70 73 20 50 48 L/1.0.2k -fips PH
00a0 50 2f 35 2e 34 2e 31 36 20 6d 6f 64 5f 70 65 72 P/5.4.16 mod_per
Ethernet (eth), 14 bytes
Packets: 65 · Displayed: 65 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

ARP

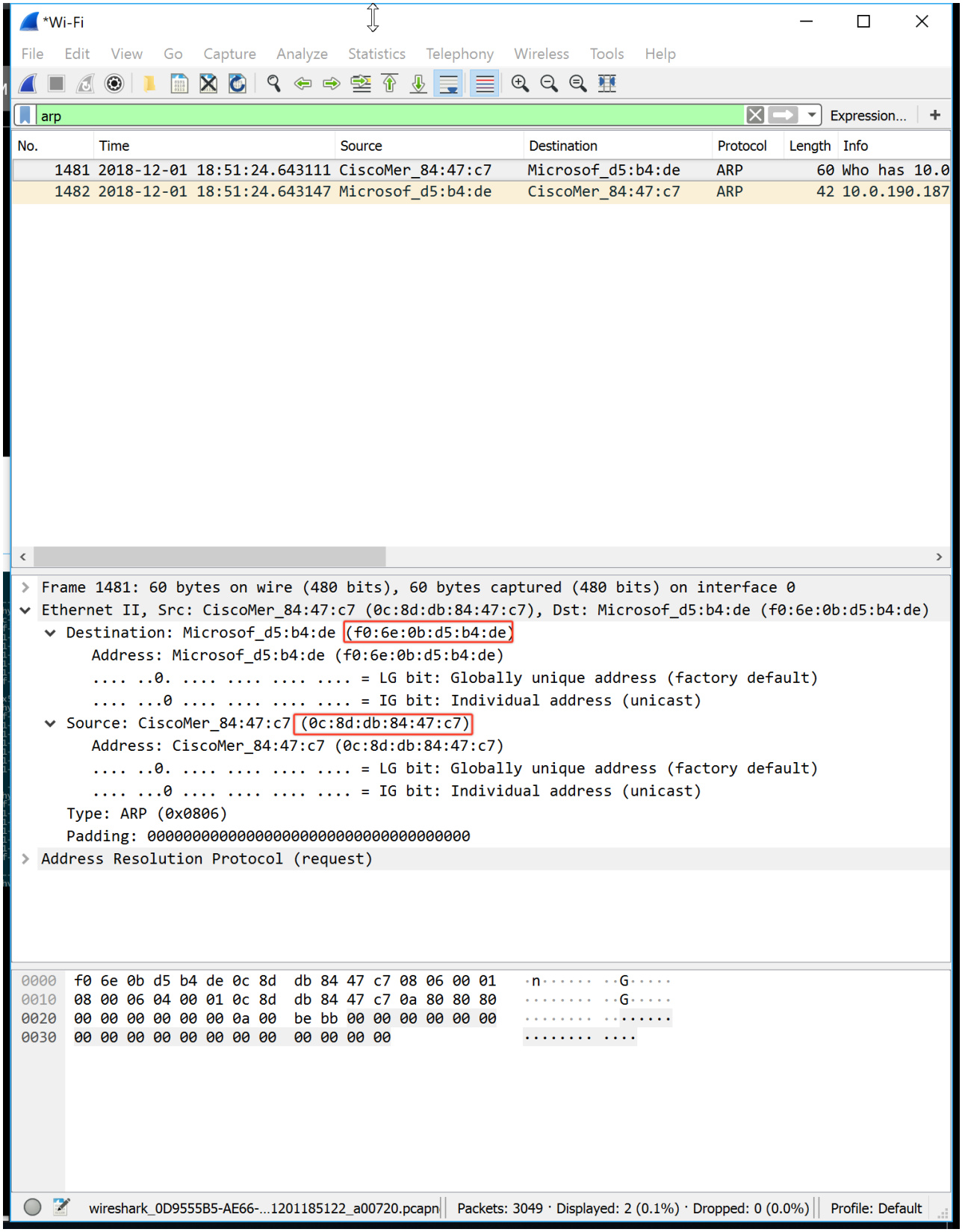
9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?



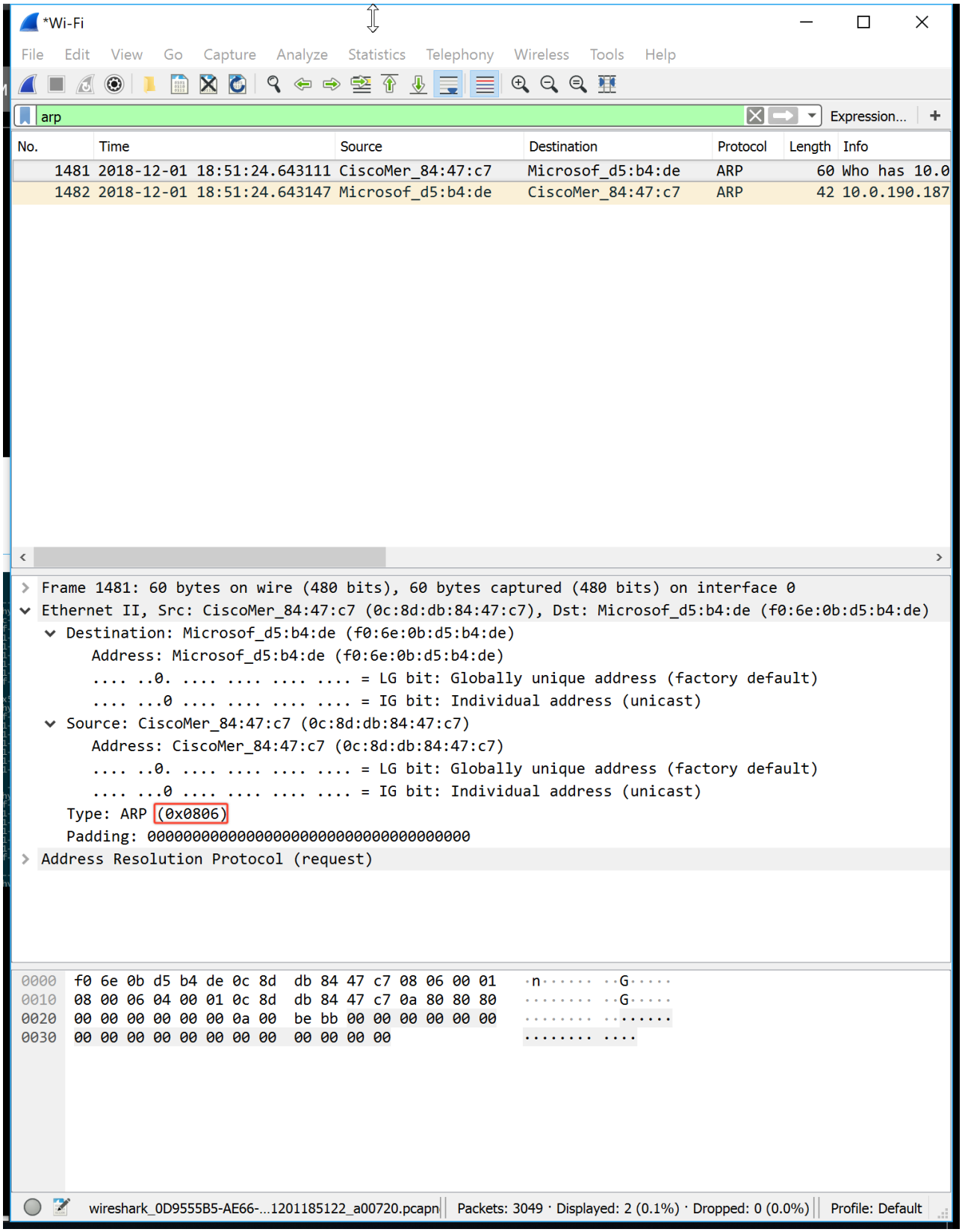
IP Address, MAC (Ethernet Address), ARP Entry Type - Static is manually configured and is permanent, Dynamic means the entry is created using the ARP protocol.

10. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?
Destination: `f0:6e:0b:d5:b4:de`

Source: 0c:8d:db:84:47:c7



11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to? 0x0806 - 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?

20 bytes from the beginning of the 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 hex value in the ARP-payload of the request is `0x0001`

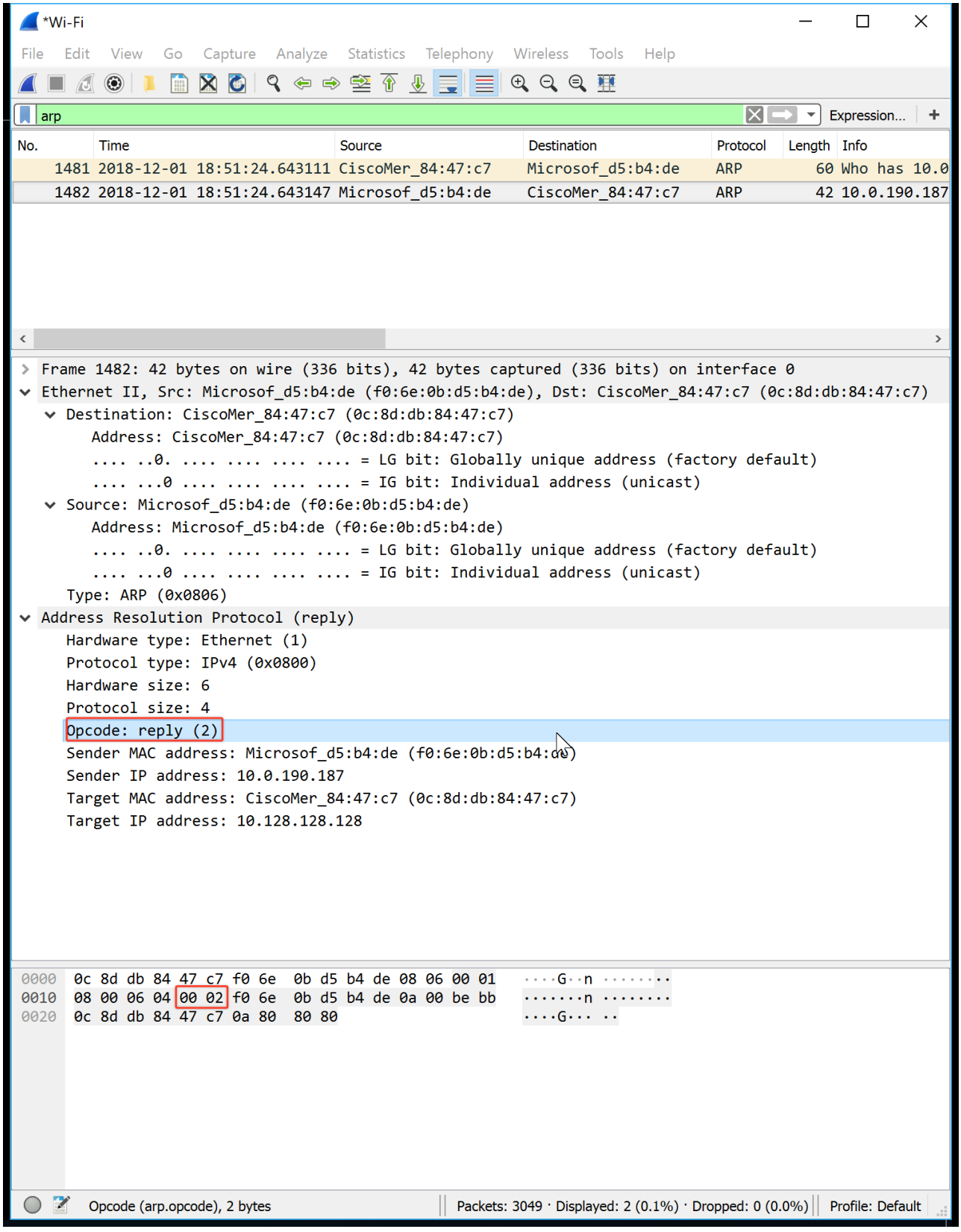
c) Does the ARP message contain the IP address of the sender?

Yes

d) Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?
The field `Target MAC Address` is set to `00:00:00:00:00:00` to query the machine whose 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?
20 byes from the beginning of the 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?

`0x0002` - 2



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 appears in the `Sender MAC Address` field. Value contains `f0:6e:0b:d5:b4:de`

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

Destination: `0c:8d:db:84:47:c7`

Source: `f0:6e:0b:d5:b4:de`

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 reply because this request came from a different host. It is a broadcast, but the reply will be sent to the sender's MAC address.