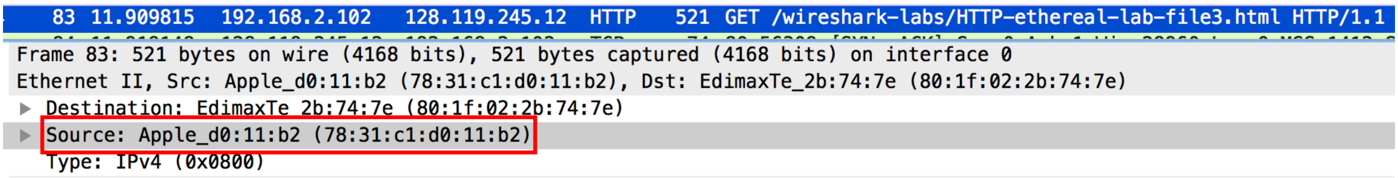
CS494 – Project 2 (Wireshark)

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

Wireshark Ethernet and ARP

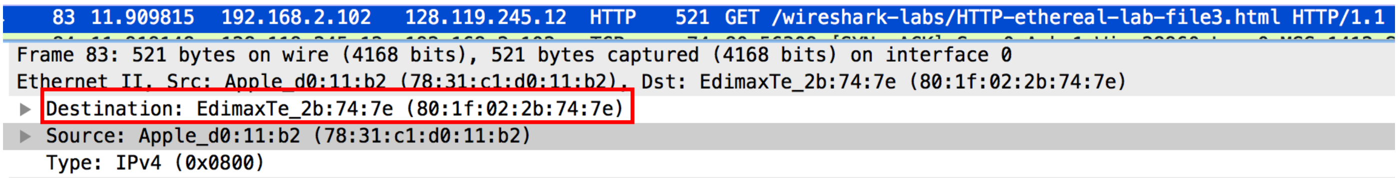
[1] What is the 48-bit Ethernet address of your computer?



```
83 11.909815  192.168.2.102   128.119.245.12  HTTP   521 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
Frame 83: 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface 0
Ethernet II, Src: Apple_d0:11:b2 (78:31:c1:d0:11:b2), Dst: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
▶ Destination: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
▶ Source: Apple_d0:11:b2 (78:31:c1:d0:11:b2)
  Type: IPv4 (0x0800)
```

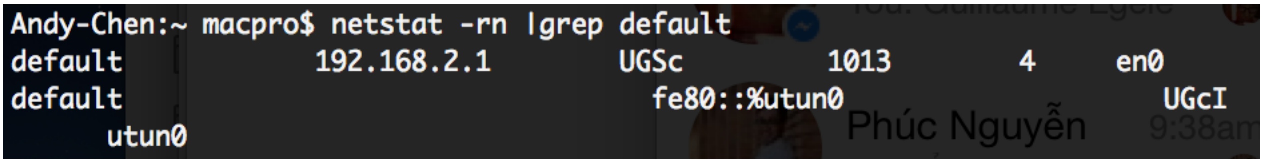
My computer MAC address: 78:31:c1:d0:11:b2

[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.]



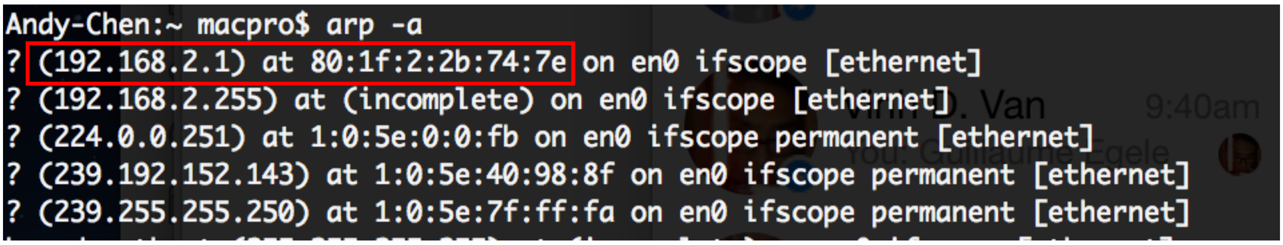
```
83 11.909815  192.168.2.102   128.119.245.12  HTTP   521 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
Frame 83: 521 bytes on wire (4168 bits), 521 bytes captured (4168 bits) on interface 0
Ethernet II, Src: Apple_d0:11:b2 (78:31:c1:d0:11:b2), Dst: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
▶ Destination: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
▶ Source: Apple_d0:11:b2 (78:31:c1:d0:11:b2)
  Type: IPv4 (0x0800)
```

The MAC address of the destination in the Ethernet frame: 80:1f:02:2b:74:7e



```
Andy-Chen:~ macpro$ netstat -rn |grep default
default            192.168.2.1        UGSc           1013        4      en0
default                                fe80::%utun0                   UGcI
     utun0
```

My connected router’s IP address is 192.168.2.1



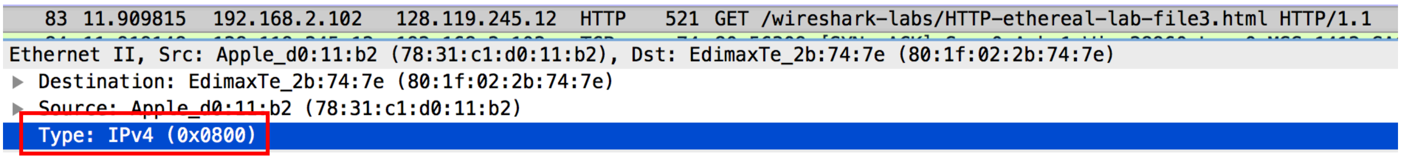
```
Andy-Chen:~ macpro$ arp -a
? (192.168.2.1) at 80:1f:2:2b:74:7e on en0 ifscope [ethernet]
? (192.168.2.255) at (incomplete) on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.192.152.143) at 1:0:5e:40:98:8f on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

The MAC address of my connected router (192.168.2.1) is 80:1f:2:2b:74:7e

- The MAC address of the destination in the Ethernet frame is also the MAC address of my connected router.

Trần Tinh Chí – 1351063
Lê Lưu Quỳnh Giao – 1351012
Nguyễn Đắc Phúc – 1351060

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

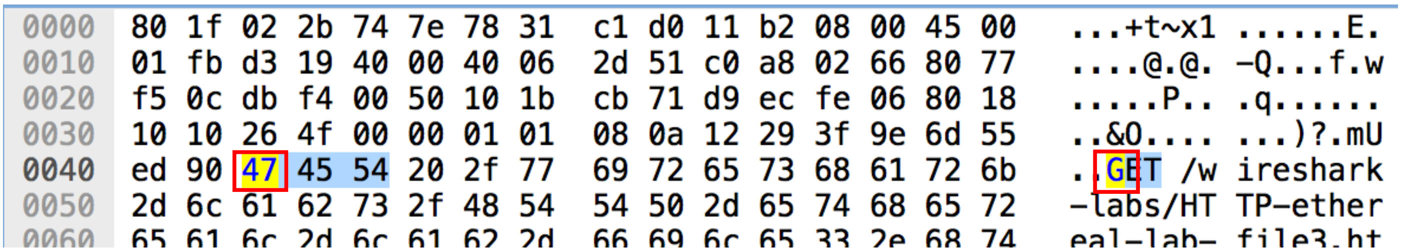


```
  83 11.909815  192.168.2.102   128.119.245.12  HTTP   521 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
Ethernet II, Src: Apple_d0:11:b2 (78:31:c1:d0:11:b2), Dst: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
▶ Destination: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
▶ Source: Apple_d0:11:b2 (78:31:c1:d0:11:b2)
  Type: IPv4 (0x0800)
```

The hexadecimal value for the 2-bytes Frame type field is 0x0800

The upper layer corresponded to IPv4

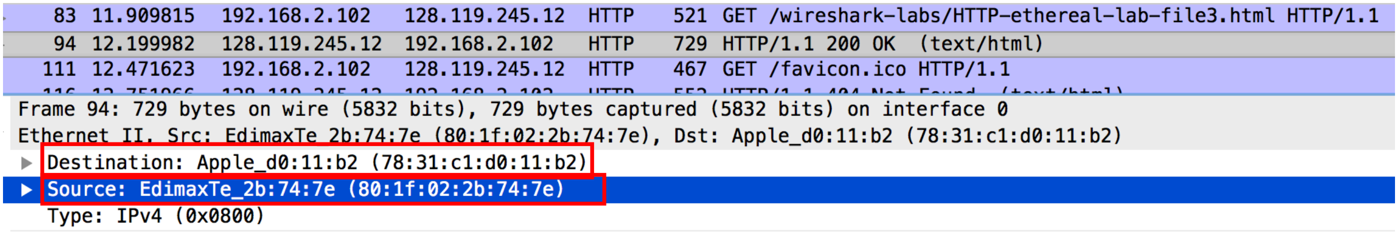
[4] How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?



```
0000  80 1f 02 2b 74 7e 78 31  c1 d0 11 b2 08 00 45 00   ...+t~x1 ......E.
0010  01 fb d3 19 40 00 40 06  2d 51 c0 a8 02 66 80 77   ....@.@. -Q...f.w
0020  f5 0c db f4 00 50 10 1b  cb 71 d9 ec fe 06 80 18   .....P.. .q......
0030  10 10 26 4f 00 00 01 01  08 0a 12 29 3f 9e 6d 55   ..&O.... ...)?.mU
0040  ed 90 47 45 54 20 2f 77  69 72 65 73 68 61 72 6b   ..GET /w ireshark
0050  2d 6c 61 62 73 2f 48 54  54 50 2d 65 74 68 65 72   -labs/HT TP-ether
0060  65 61 6c 2d 6c 61 62 2d  66 69 6c 65 33 2e 68 74   eal-lab- file3.ht
```

It appears at the byte 67th from the begining the the Ethernet frame.

[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?



```
  83 11.909815  192.168.2.102   128.119.245.12  HTTP   521 GET /wireshark-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
  94 12.199982  128.119.245.12  192.168.2.102   HTTP   729 HTTP/1.1 200 OK  (text/html)
 111 12.471623  192.168.2.102   128.119.245.12  HTTP   467 GET /favicon.ico HTTP/1.1
Frame 94: 729 bytes on wire (5832 bits), 729 bytes captured (5832 bits) on interface 0
Ethernet II, Src: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e), Dst: Apple_d0:11:b2 (78:31:c1:d0:11:b2)
▶ Destination: Apple_d0:11:b2 (78:31:c1:d0:11:b2)
▶ Source: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
  Type: IPv4 (0x0800)
```

The Ethernet source address: 80:1f:02:2b:74:7e

It is neither the MAC address of my laptop or gaia.cs.umass.edu. It is indeed the address of my connected router as shown in question 2.

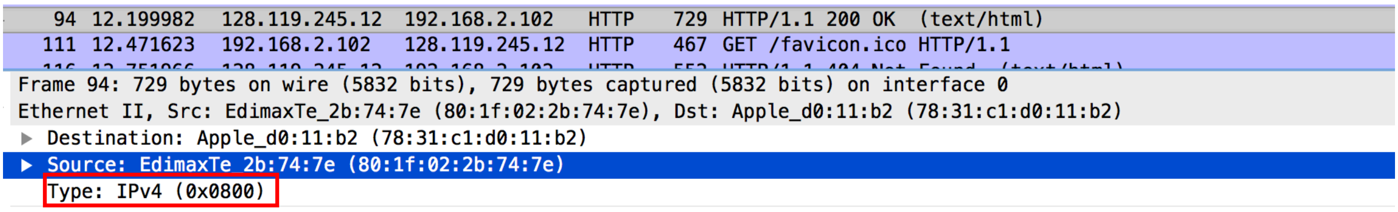
[6] What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?

The destination address in the Ethernet frame is 78:31:c1:d0:11:b2

My computer MAC address: 78:31:c1:d0:11:b2 as shown in question 1.

- It is exactly my laptop MAC address.

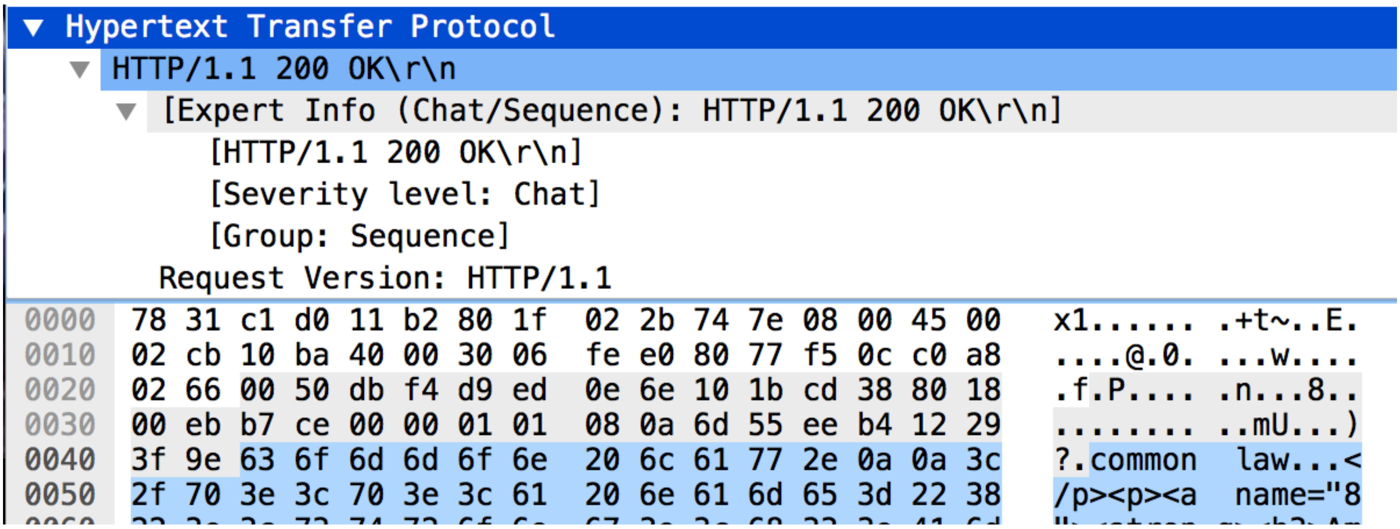
[7] Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?



```
   94 12.199982  128.119.245.12  192.168.2.102   HTTP    729 HTTP/1.1 200 OK  (text/html)
  111 12.471623  192.168.2.102   128.119.245.12  HTTP    467 GET /favicon.ico HTTP/1.1
 Frame 94: 729 bytes on wire (5832 bits), 729 bytes captured (5832 bits) on interface 0
 Ethernet II, Src: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e), Dst: Apple_d0:11:b2 (78:31:c1:d0:11:b2)
 ▶ Destination: Apple_d0:11:b2 (78:31:c1:d0:11:b2)
 ▶ Source: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
   Type: IPv4 (0x0800)
```

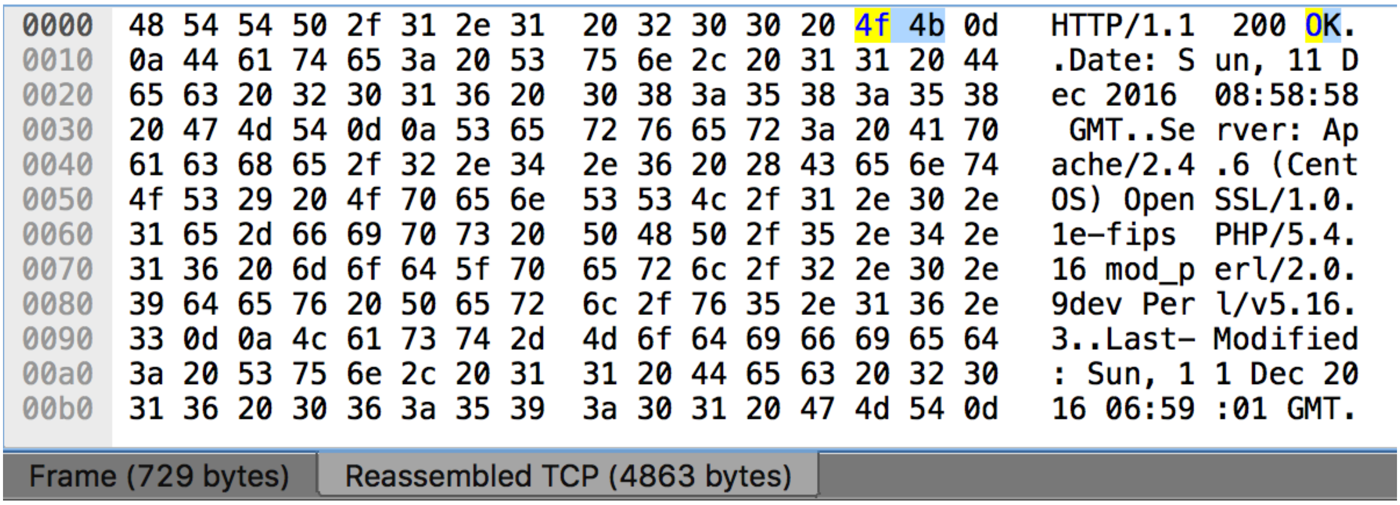
The hexadecimal value for the 2-bytes Frame type field is 0x0800
The upper layer corresponded to IPv4

[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?



```
▼ Hypertext Transfer Protocol
  ▼ HTTP/1.1 200 OK\r\n
    ▼ [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
        [HTTP/1.1 200 OK\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Version: HTTP/1.1
0000  78 31 c1 d0 11 b2 80 1f  02 2b 74 7e 08 00 45 00   x1...... .+t~..E.
0010  02 cb 10 ba 40 00 30 06  fe e0 80 77 f5 0c c0 a8   ....@.0. ...w....
0020  02 66 00 50 db f4 d9 ed  0e 6e 10 1b cd 38 80 18   .f.P.... .n...8..
0030  00 eb b7 ce 00 00 01 01  08 0a 6d 55 ee b4 12 29   ........ ..mU...)
0040  3f 9e 63 6f 6d 6d 6f 6e  20 6c 61 77 2e 0a 0a 3c   ?.common  law...<
0050  2f 70 3e 3c 70 3e 3c 61  20 6e 61 6d 65 3d 22 38   /p><p><a  name="8
```

We know that the HTTP response code begins at the byte 67th.
Then we reassemble the TCP, we have:

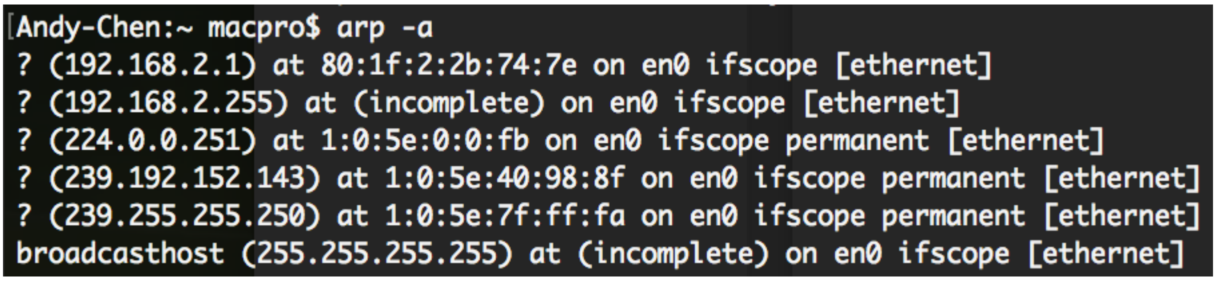


```
0000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d   HTTP/1.1  200 OK.
0010  0a 44 61 74 65 3a 20 53  75 6e 2c 20 31 31 20 44   .Date: S un, 11 D
0020  65 63 20 32 30 31 36 20  30 38 3a 35 38 3a 35 38   ec 2016  08:58:58
0030  20 47 4d 54 0d 0a 53 65  72 76 65 72 3a 20 41 70    GMT..Se rver: Ap
0040  61 63 68 65 2f 32 2e 34  2e 36 20 28 43 65 6e 74   ache/2.4 .6 (Cent
0050  4f 53 29 20 4f 70 65 6e  53 53 4c 2f 31 2e 30 2e   OS) Open SSL/1.0.
0060  31 65 2d 66 69 70 73 20  50 48 50 2f 35 2e 34 2e   1e-fips  PHP/5.4.
0070  31 36 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   16 mod_p erl/2.0.
0080  39 64 65 76 20 50 65 72  6c 2f 76 35 2e 31 36 2e   9dev Per l/v5.16.
0090  33 0d 0a 4c 61 73 74 2d  4d 6f 64 69 66 69 65 64   3..Last- Modified
00a0  3a 20 53 75 6e 2c 20 31  31 20 44 65 63 20 32 30   : Sun, 1 1 Dec 20
00b0  31 36 20 30 36 3a 35 39  3a 30 31 20 47 4d 54 0d   16 06:59 :01 GMT.
```

It means the character “O” of “OK” is at the 14th byte from the beginning of the HTTP response code.

- ➢ Thus, the “O” is at the **byte 80th** (which is 14 + 66) from the beginning of the Ethernet frame.

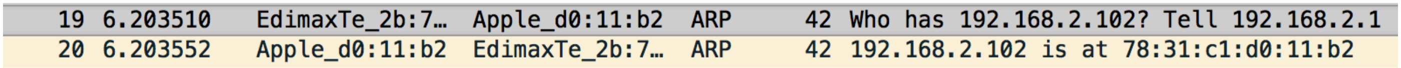
[9] Write down the contents of your computer’s ARP cache. What is the meaning of each column value?



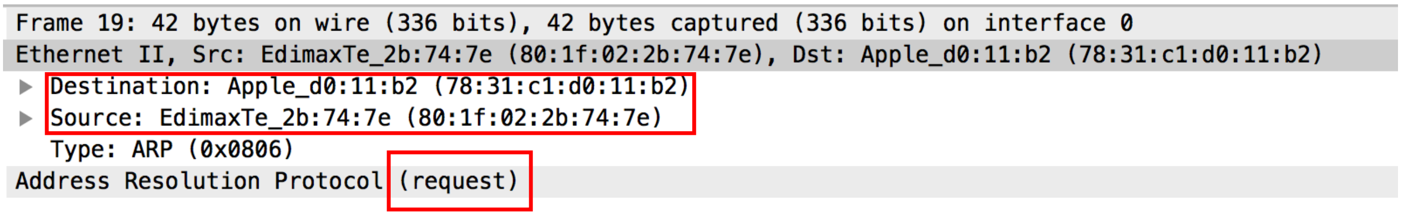
```
[Andy-Chen:~ macpro$ arp -a
? (192.168.2.1) at 80:1f:2:2b:74:7e on en0 ifscope [ethernet]
? (192.168.2.255) at (incomplete) on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
? (239.192.152.143) at 1:0:5e:40:98:8f on en0 ifscope permanent [ethernet]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
broadcasthost (255.255.255.255) at (incomplete) on en0 ifscope [ethernet]
```

It shows the IP address, MAC address and whether the protocol is permanent or not.

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



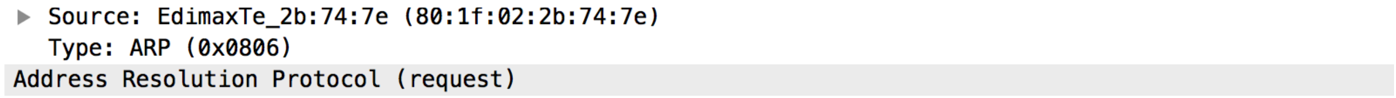
```
 19 6.203510   EdimaxTe_2b:7…  Apple_d0:11:b2  ARP      42  Who has 192.168.2.102? Tell 192.168.2.1
 20 6.203552   Apple_d0:11:b2  EdimaxTe_2b:7…  ARP      42  192.168.2.102 is at 78:31:c1:d0:11:b2
```



```
Frame 19: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
Ethernet II, Src: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e), Dst: Apple_d0:11:b2 (78:31:c1:d0:11:b2)
 ▶ Destination: Apple_d0:11:b2 (78:31:c1:d0:11:b2)
 ▶ Source: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
   Type: ARP (0x0806)
Address Resolution Protocol (request)
```

Source address: 80:1f:02:2b:74:7e
Destination address: 78:31:c1:d0:11:b2

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

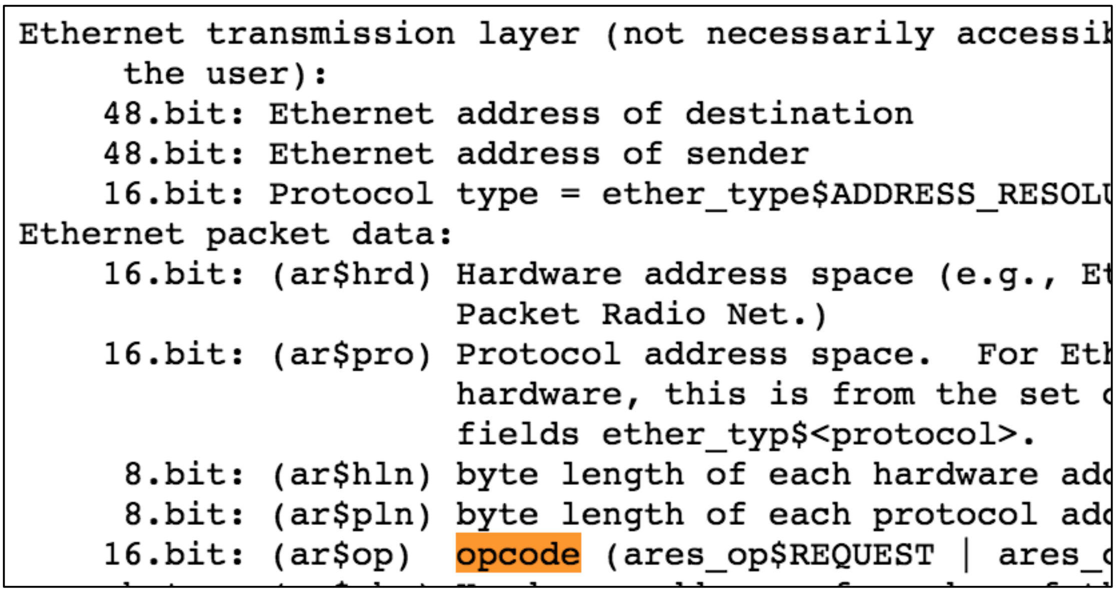


```
 ▶ Source: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
   Type: ARP (0x0806)
Address Resolution Protocol (request)
```

The hexadecimal value: 0x0806
It corresponds to ARP protocol

[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.

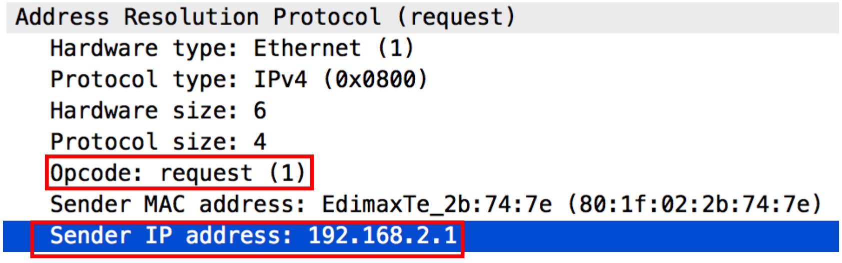
a. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?



```
Ethernet transmission layer (not necessarily accessi
     the user):
    48.bit: Ethernet address of destination
    48.bit: Ethernet address of sender
    16.bit: Protocol type = ether_type$ADDRESS_RESOLU
Ethernet packet data:
    16.bit: (ar$hrd) Hardware address space (e.g., Et
                     Packet Radio Net.)
    16.bit: (ar$pro) Protocol address space.  For Eth
                     hardware, this is from the set o
                     fields ether_typ$<protocol>.
     8.bit: (ar$hln) byte length of each hardware add
     8.bit: (ar$pln) byte length of each protocol add
    16.bit: (ar$op)  opcode (ares_op$REQUEST | ares_o
```

The ARP opcode field begins at byte 21th from the very beginning of the Ethernet frame (The photo is taken from the std37.txt file).

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?



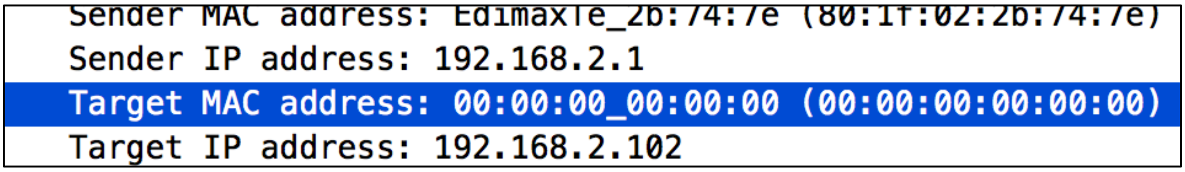
```
Address Resolution Protocol (request)
   Hardware type: Ethernet (1)
   Protocol type: IPv4 (0x0800)
   Hardware size: 6
   Protocol size: 4
   Opcode: request (1)
   Sender MAC address: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
   Sender IP address: 192.168.2.1
```

The value for opcode field within the ARP-payload of the request is 1, for request.

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

Yes, it does.

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

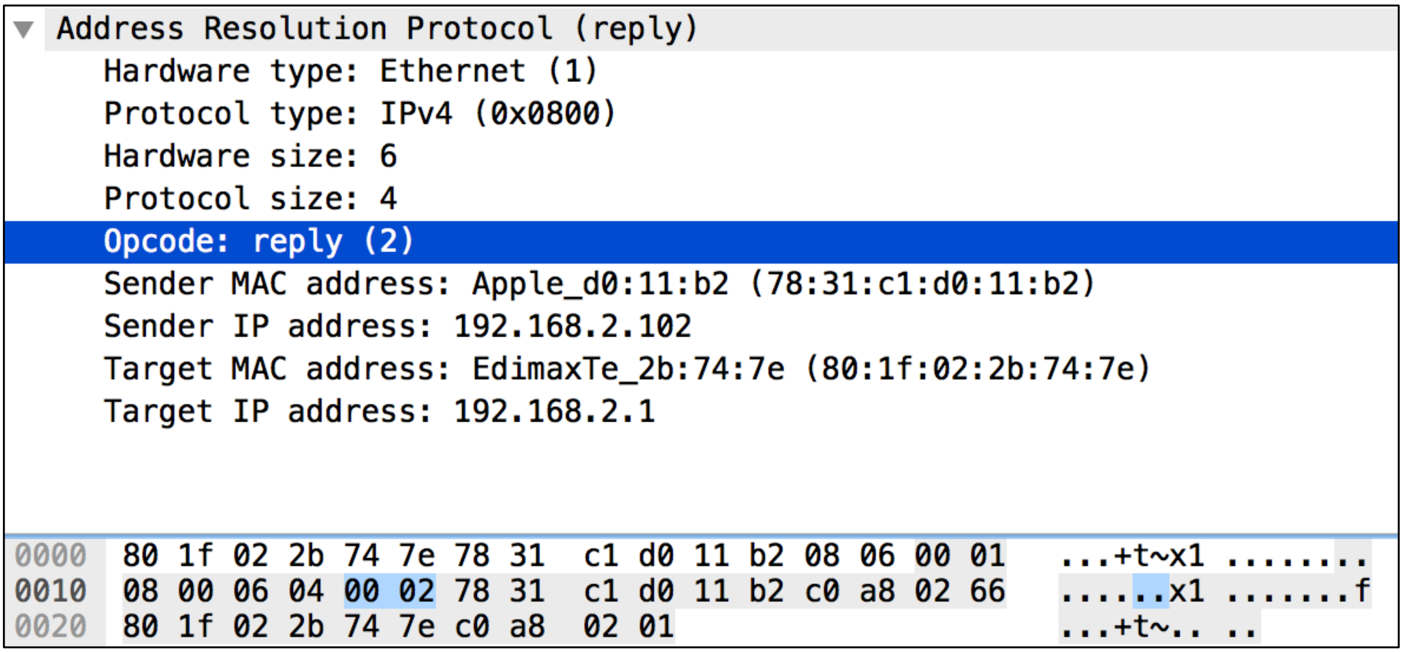


```
Sender MAC address: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
Sender IP address: 192.168.2.1
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.2.102
```

"Target MAC address" is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.2.102) 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?



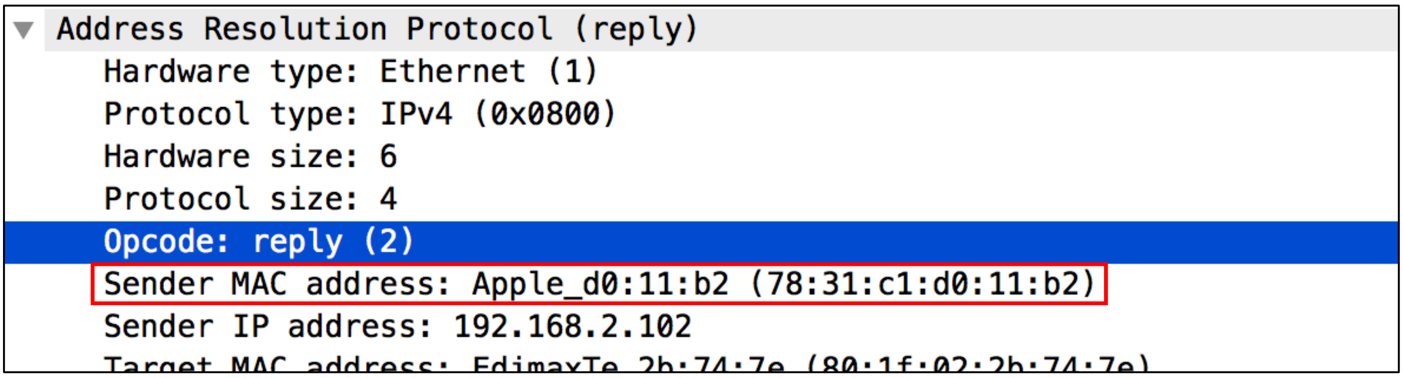
```
▼ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Apple_d0:11:b2 (78:31:c1:d0:11:b2)
    Sender IP address: 192.168.2.102
    Target MAC address: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
    Target IP address: 192.168.2.1

0000  80 1f 02 2b 74 7e 78 31  c1 d0 11 b2 08 06 00 01   ...+t~x1 ........
0010  08 00 06 04 00 02 78 31  c1 d0 11 b2 c0 a8 02 66   ......x1 .......f
0020  80 1f 02 2b 74 7e c0 a8  02 01                     ...+t~.. ..
```

The ARP opcode field begins at byte 21th 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 for opcode field within the ARP-payload part of Ethernet frame in which an ARP response is 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?

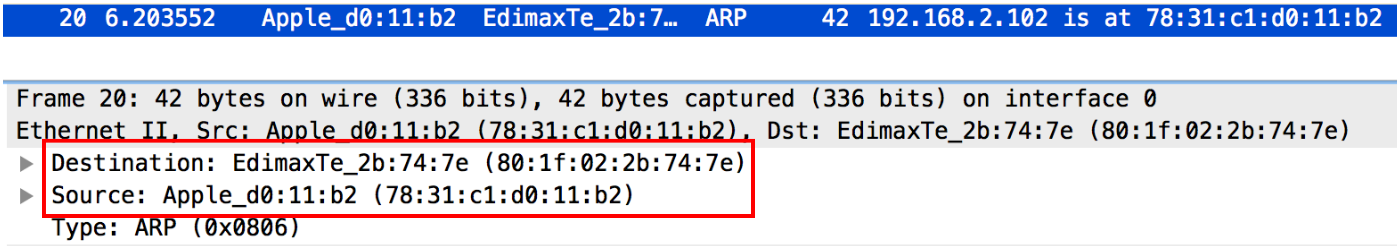


```
▼ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Apple_d0:11:b2 (78:31:c1:d0:11:b2)
    Sender IP address: 192.168.2.102
    Target MAC address: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
```

The request ARP questions the MAC address for IP address 192.168.2.102

- ➢ The "answer" is at the Sender MAC address.

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

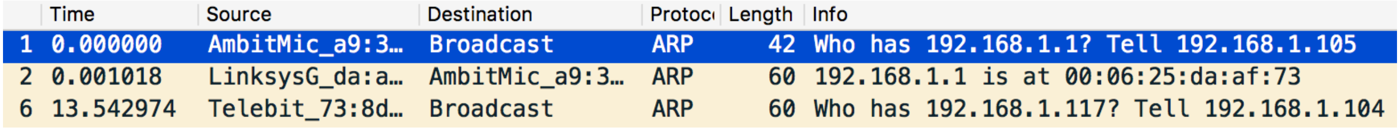


```
  20  6.203552    Apple_d0:11:b2  EdimaxTe_2b:7…  ARP      42  192.168.2.102 is at 78:31:c1:d0:11:b2

 Frame 20: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
 Ethernet II, Src: Apple_d0:11:b2 (78:31:c1:d0:11:b2), Dst: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
 ▶ Destination: EdimaxTe_2b:74:7e (80:1f:02:2b:74:7e)
 ▶ Source: Apple_d0:11:b2 (78:31:c1:d0:11:b2)
   Type: ARP (0x0806)
```

Source address: 78:31:c1:d0:11:b2
Destination address: 80:1f:02:2b:74:7e

[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?

Because the ARP request message is a Broadcast message, means every host in the same network can receive this message (it does not know which is the computer), thus we (the one in the same network) also receive it. However, the ARP response message is unicast to the one who sent the request message, thus we cannot see the response message for the ARP request message in line 6 (we are not this host).



	Time	Source	Destination	Protoc	Length	Info
1	0.000000	AmbitMic_a9:3…	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.105
2	0.001018	LinksysG_da:a…	AmbitMic_a9:3…	ARP	60	192.168.1.1 is at 00:06:25:da:af:73
6	13.542974	Telebit_73:8d…	Broadcast	ARP	60	Who has 192.168.1.117? Tell 192.168.1.104