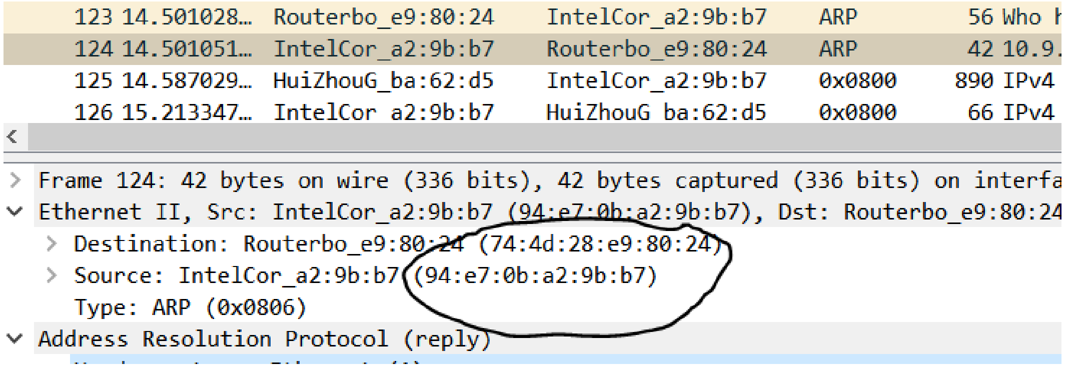
Gretel Rajamoney

Wireshark Lab #5

Ethernet and ARP

Note: Sharing a computer with a peer due to Wireshark issues, the TA stated that it was a Wireshark issue and told me I could utilize another laptop and leave a note for the grader.

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

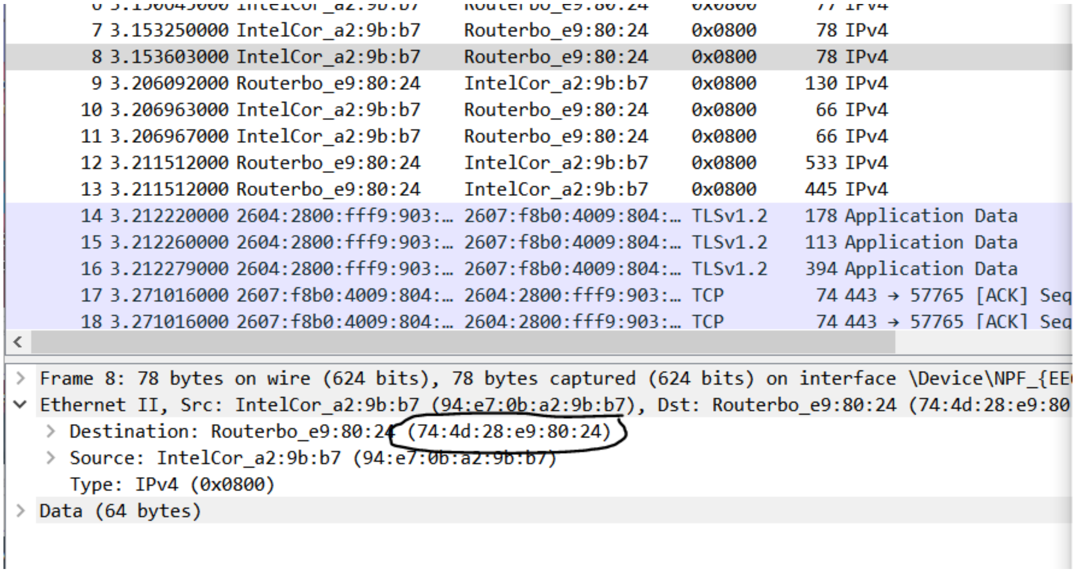


```
    123 14.501028…  Routerbo_e9:80:24   IntelCor_a2:9b:b7   ARP         56 Who h
    124 14.501051…  IntelCor_a2:9b:b7   Routerbo_e9:80:24   ARP         42 10.9.
    125 14.587029…  HuiZhouG_ba:62:d5   IntelCor_a2:9b:b7   0x0800     890 IPv4
    126 15.213347…  IntelCor_a2:9b:b7   HuiZhouG_ba:62:d5   0x0800      66 IPv4

> Frame 124: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interfa
v Ethernet II, Src: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7), Dst: Routerbo_e9:80:24
  > Destination: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
  > Source: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7)
    Type: ARP (0x0806)
v Address Resolution Protocol (reply)
```

The 48-bit Ethernet address of my computer is 94:e7:0b:a2:9b:b7

2. 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?

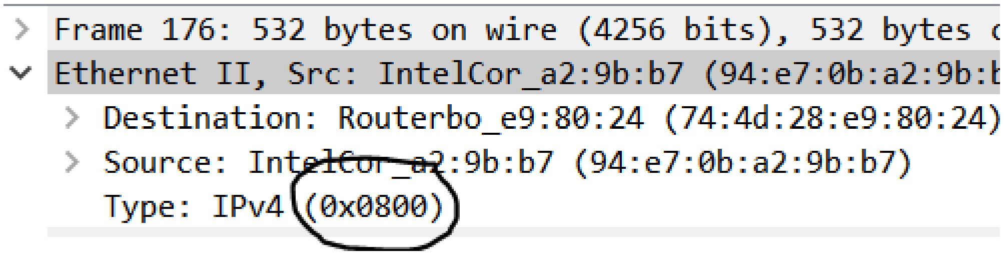


```
   7 3.153250000 IntelCor_a2:9b:b7      Routerbo_e9:80:24      0x0800    78 IPv4
   8 3.153603000 IntelCor_a2:9b:b7      Routerbo_e9:80:24      0x0800    78 IPv4
   9 3.206092000 Routerbo_e9:80:24      IntelCor_a2:9b:b7      0x0800   130 IPv4
  10 3.206963000 IntelCor_a2:9b:b7      Routerbo_e9:80:24      0x0800    66 IPv4
  11 3.206967000 IntelCor_a2:9b:b7      Routerbo_e9:80:24      0x0800    66 IPv4
  12 3.211512000 Routerbo_e9:80:24      IntelCor_a2:9b:b7      0x0800   533 IPv4
  13 3.211512000 Routerbo_e9:80:24      IntelCor_a2:9b:b7      0x0800   445 IPv4
  14 3.212220000 2604:2800:fff9:903:…   2607:f8b0:4009:804:…   TLSv1.2  178 Application Data
  15 3.212260000 2604:2800:fff9:903:…   2607:f8b0:4009:804:…   TLSv1.2  113 Application Data
  16 3.212279000 2604:2800:fff9:903:…   2607:f8b0:4009:804:…   TLSv1.2  394 Application Data
  17 3.271016000 2607:f8b0:4009:804:…   2604:2800:fff9:903:…   TCP       74 443 → 57765 [ACK] Seq
  18 3.271016000 2607:f8b0:4009:804:…   2604:2800:fff9:903:…   TCP       74 443 → 57765 [ACK] Seq

> Frame 8: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{EE
v Ethernet II, Src: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7), Dst: Routerbo_e9:80:24 (74:4d:28:e9:80
  > Destination: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
  > Source: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7)
    Type: IPv4 (0x0800)
> Data (64 bytes)
```

The 48-bit destination address is 74:4d:28:e9:80:24, this is not the Ethernet address of gaia.cs.umass.edu. The device that does have this as its Ethernet address is the internet gateway address.

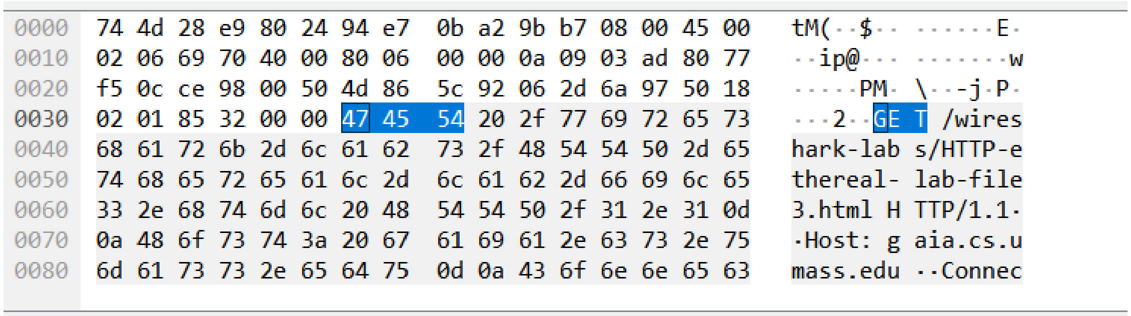
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?



```
> Frame 176: 532 bytes on wire (4256 bits), 532 bytes c
v Ethernet II, Src: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b
    > Destination: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
    > Source: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7)
      Type: IPv4 (0x0800)
```

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

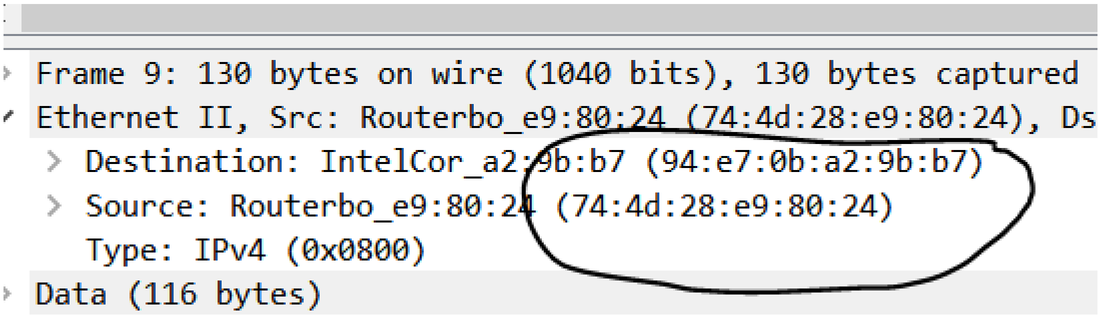
4. How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame?



```
0000  74 4d 28 e9 80 24 94 e7  0b a2 9b b7 08 00 45 00   tM(··$·· ······E·
0010  02 06 69 70 40 00 80 06  00 00 0a 09 03 ad 80 77   ··ip@··· ·······w
0020  f5 0c ce 98 00 50 4d 86  5c 92 06 2d 6a 97 50 18   ·····PM· \··-j·P·
0030  02 01 85 32 00 00 47 45  54 20 2f 77 69 72 65 73   ···2··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 43 6f 6e 6e 65 63   mass.edu ··Connec
```

The ASCII "G" in "GET" appears in the Ethernet frame 54 bytes from the very start of the Ethernet frame. It is not displayed within the screenshot since you must hover over it in order to see the byte count, but when hovered upon, the "GET" falls in the bytes of 54, 55, and 56, meaning that the "G" must be at the location of 54 bytes from the start.

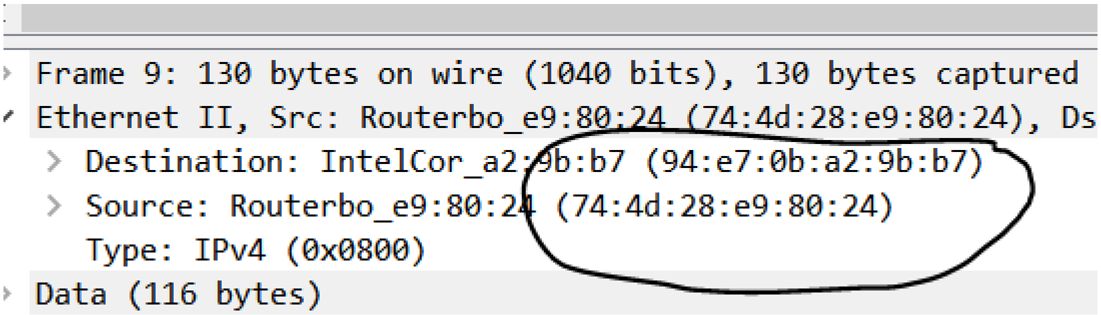
5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu. What device has this as its Ethernet address?



```
> Frame 9: 130 bytes on wire (1040 bits), 130 bytes captured
v Ethernet II, Src: Routerbo_e9:80:24 (74:4d:28:e9:80:24), Ds
    > Destination: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7)
    > Source: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
      Type: IPv4 (0x0800)
> Data (116 bytes)
```

The value of the Ethernet source address is 74:4d:28:e9:80:24. This is not the address of my computer or of gaia.cs.umass.edu, this is actually the Ethernet address of the internet gateway address.

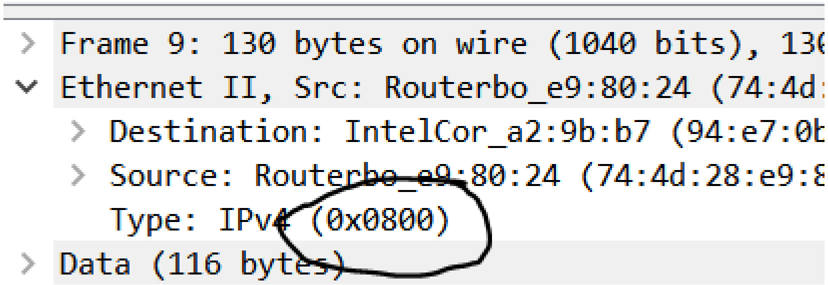
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?



```
› Frame 9: 130 bytes on wire (1040 bits), 130 bytes captured
⌄ Ethernet II, Src: Routerbo_e9:80:24 (74:4d:28:e9:80:24), Ds
  › Destination: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7)
  › Source: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
    Type: IPv4 (0x0800)
› Data (116 bytes)
```

The destination address in the Ethernet frame is 94:e7:0b:a2:9b:b7. Yes, this is the Ethernet address of my computer.

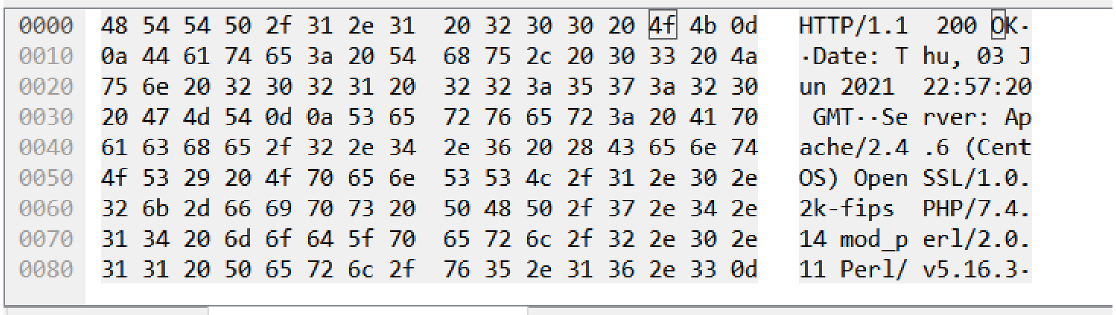
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?



```
› Frame 9: 130 bytes on wire (1040 bits), 13
⌄ Ethernet II, Src: Routerbo_e9:80:24 (74:4d
  › Destination: IntelCor_a2:9b:b7 (94:e7:0b
  › Source: Routerbo_e9:80:24 (74:4d:28:e9:8
    Type: IPv4 (0x0800)
› Data (116 bytes)
```

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

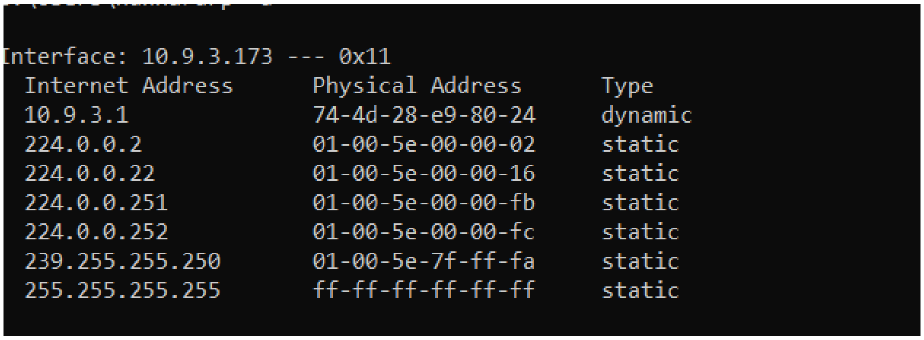
8. How many bytes from the very start of the Ethernet frame does the ASCII "O" in "OK" appear in the Ethernet frame?



```
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 54  68 75 2c 20 30 33 20 4a   ·Date: T hu, 03 J
0020  75 6e 20 32 30 32 31 20  32 32 3a 35 37 3a 32 30   un 2021  22:57:20
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  32 6b 2d 66 69 70 73 20  50 48 50 2f 37 2e 34 2e   2k-fips  PHP/7.4.
0070  31 34 20 6d 6f 64 5f 70  65 72 6c 2f 32 2e 30 2e   14 mod_p erl/2.0.
0080  31 31 20 50 65 72 6c 2f  76 35 2e 31 36 2e 33 0d   11 Perl/ v5.16.3·
```

The ASCII "O" in "OK" appears in the Ethernet frame 13 bytes from the very start of the Ethernet frame. It is not displayed within the screenshot since you must hover over it in order to see the byte count, but when hovered upon, the "OK" falls in the bytes of 13 and 14, meaning that the "O" must be at the location of 13 bytes from the start.

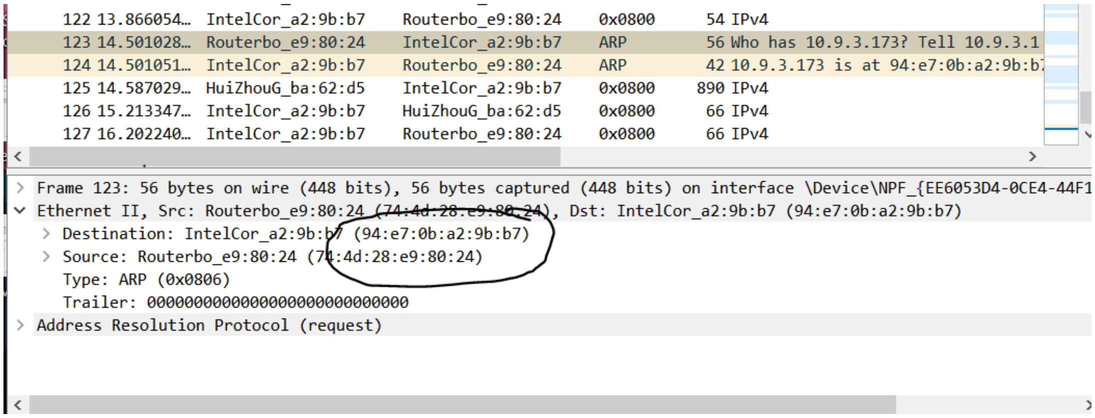
9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?



```
Interface: 10.9.3.173 --- 0x11
  Internet Address      Physical Address      Type
  10.9.3.1              74-4d-28-e9-80-24     dynamic
  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
```

The contents of my computer's ARP cache are screenshotted above. The first column of the ARP cache represents the internet address or IP address. The next column of the ARP cache represents the physical address or the MAC address. The last column of the ARP cache represents the protocol type.

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

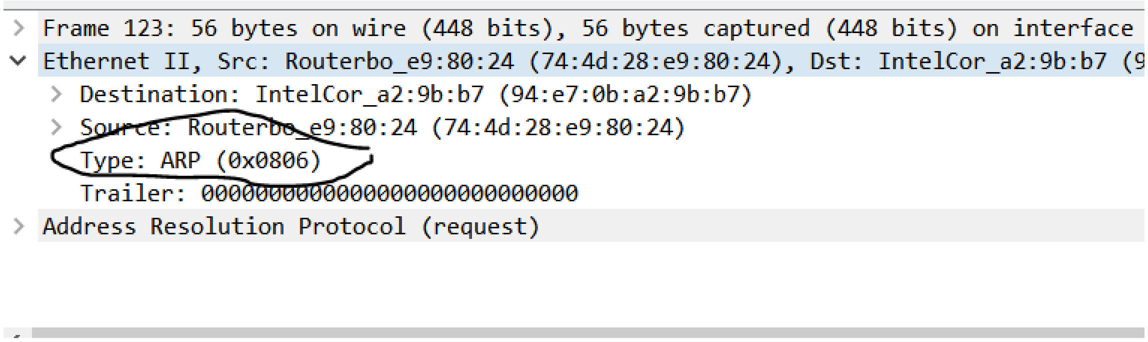


```
122 13.866054…  IntelCor_a2:9b:b7   Routerbo_e9:80:24   0x0800    54 IPv4
123 14.501028…  Routerbo_e9:80:24   IntelCor_a2:9b:b7   ARP       56 Who has 10.9.3.173? Tell 10.9.3.1
124 14.501051…  IntelCor_a2:9b:b7   Routerbo_e9:80:24   ARP       42 10.9.3.173 is at 94:e7:0b:a2:9b:b
125 14.587029…  HuiZhouG_ba:62:d5   IntelCor_a2:9b:b7   0x0800   890 IPv4
126 15.213347…  IntelCor_a2:9b:b7   HuiZhouG_ba:62:d5   0x0800    66 IPv4
127 16.202240…  IntelCor_a2:9b:b7   Routerbo_e9:80:24   0x0800    66 IPv4

> Frame 123: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{EE6053D4-0CE4-44F1
v Ethernet II, Src: Routerbo_e9:80:24 (74:4d:28:e9:80:24), Dst: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7)
  > Destination: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7)
  > Source: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
    Type: ARP (0x0806)
    Trailer: 0000000000000000000000000000
> Address Resolution Protocol (request)
```

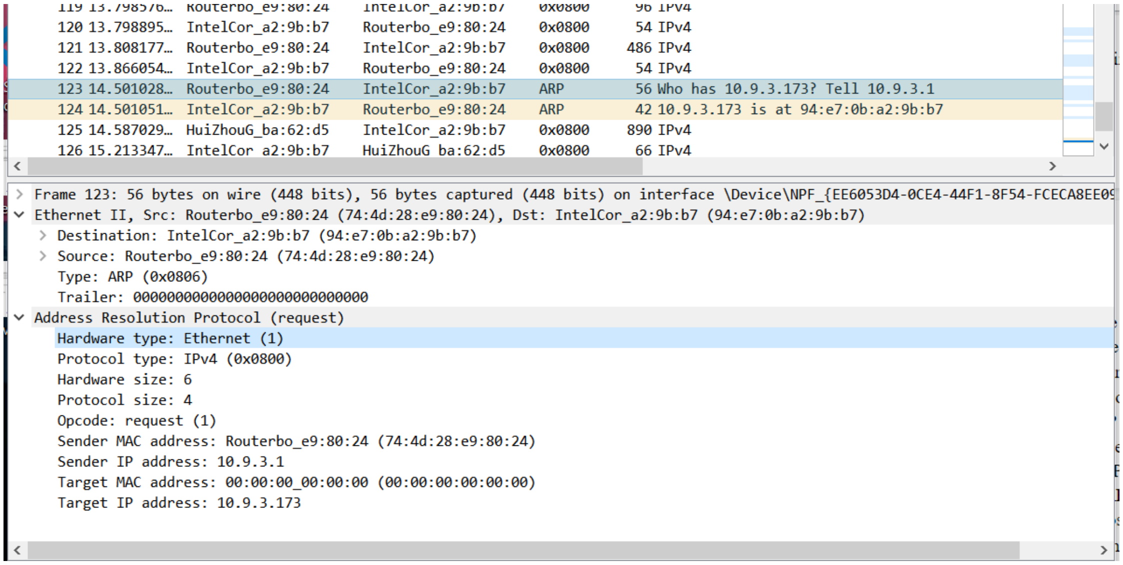
The hexadecimal value for the source address in the Ethernet frame containing the ARP request message is 74:4d:28:e9:80:24, and the hexadecimal value for the destination address in the Ethernet frame containing the ARP request message is 94:e7:0b:a2:9b:b7.

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



```
> Frame 123: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface
v Ethernet II, Src: Routerbo_e9:80:24 (74:4d:28:e9:80:24), Dst: IntelCor_a2:9b:b7 (9
  > Destination: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7)
  > Source: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
    Type: ARP (0x0806)
    Trailer: 0000000000000000000000000000
> Address Resolution Protocol (request)
```

The hexadecimal value for the two-byte Frame type field is 0x0806. The upper layer protocol that this corresponds to is the ARP.



```
119 13.798576… Routerbo_e9:80:24  IntelCor_a2:9b:b7  0x0800    96 IPv4
120 13.798895… IntelCor_a2:9b:b7  Routerbo_e9:80:24  0x0800    54 IPv4
121 13.808177… Routerbo_e9:80:24  IntelCor_a2:9b:b7  0x0800   486 IPv4
122 13.866054… IntelCor_a2:9b:b7  Routerbo_e9:80:24  0x0800    54 IPv4
123 14.501028… Routerbo_e9:80:24  IntelCor_a2:9b:b7  ARP       56 Who has 10.9.3.173? Tell 10.9.3.1
124 14.501051… IntelCor_a2:9b:b7  Routerbo_e9:80:24  ARP       42 10.9.3.173 is at 94:e7:0b:a2:9b:b7
125 14.587029… HuiZhouG_ba:62:d5  IntelCor_a2:9b:b7  0x0800   890 IPv4
126 15.213347… IntelCor_a2:9b:b7  HuiZhouG_ba:62:d5  0x0800    66 IPv4
```

```
> Frame 123: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF_{EE6053D4-0CE4-44F1-8F54-FCECA8EE0
v Ethernet II, Src: Routerbo_e9:80:24 (74:4d:28:e9:80:24), Dst: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7)
  > Destination: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7)
  > Source: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
    Type: ARP (0x0806)
    Trailer: 0000000000000000000000000000
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
    Sender IP address: 10.9.3.1
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.9.3.173
```

12.

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

The ARP opcode field begins 20 bytes 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 request is made?

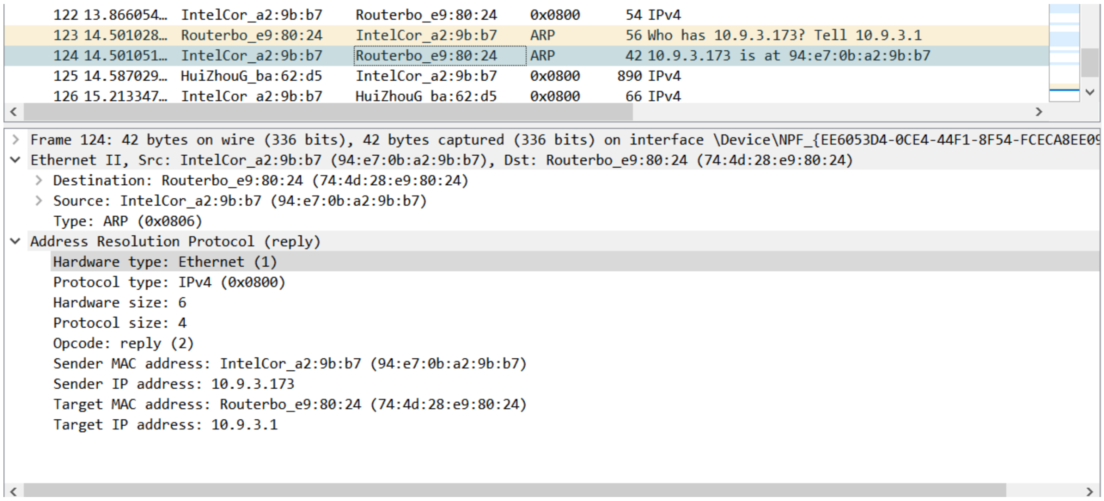
The value of the opcode field within the ARP-payload part of the Ethernet frame in which the ARP request is made is 0x0001.

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

The ARP message contains the ARP message containing the sender IP address of 10.9.3.1.

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

In the ARP request, the question appears in the Target MAC address which is 00:00:00:00:00:00, the Ethernet address of the machine whose corresponding IP address is being queried is 10.9.3.173.



```
122 13.866054… IntelCor_a2:9b:b7  Routerbo_e9:80:24  0x0800    54 IPv4
123 14.501028… Routerbo_e9:80:24  IntelCor_a2:9b:b7  ARP       56 Who has 10.9.3.173? Tell 10.9.3.1
124 14.501051… IntelCor_a2:9b:b7  Routerbo_e9:80:24  ARP       42 10.9.3.173 is at 94:e7:0b:a2:9b:b7
125 14.587029… HuiZhouG_ba:62:d5  IntelCor_a2:9b:b7  0x0800   890 IPv4
126 15.213347… IntelCor_a2:9b:b7  HuiZhouG_ba:62:d5  0x0800    66 IPv4
```

```
> Frame 124: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{EE6053D4-0CE4-44F1-8F54-FCECA8EE0
v Ethernet II, Src: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7), Dst: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
  > Destination: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
  > Source: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7)
    Type: ARP (0x0806)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7)
    Sender IP address: 10.9.3.173
    Target MAC address: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
    Target IP address: 10.9.3.1
```

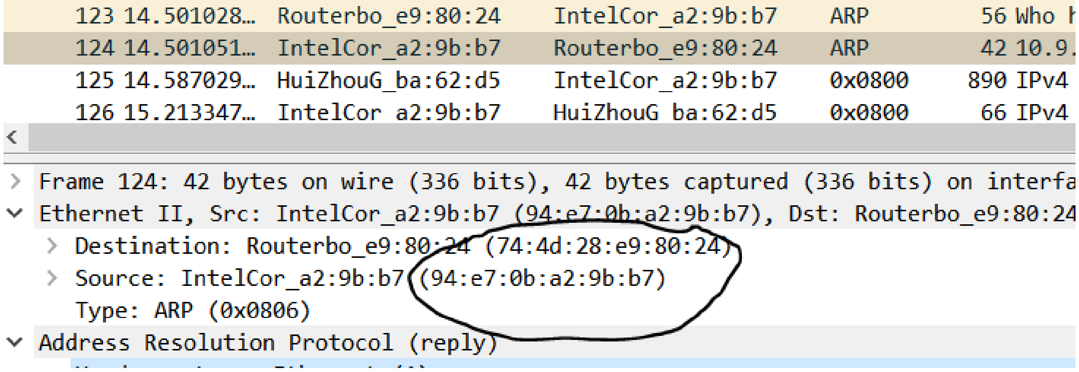
13.

a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?
The ARP opcode field begins 20 bytes 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 the ARP request 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?
In the ARP request, the answer appears in the Sender MAC address which is 94:e7:0b:a2:9b:b7, the Ethernet address of the machine whose corresponding IP address is being queried is 10.9.3.173.

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



```
    123 14.501028…  Routerbo_e9:80:24   IntelCor_a2:9b:b7   ARP        56 Who h
    124 14.501051…  IntelCor_a2:9b:b7   Routerbo_e9:80:24   ARP        42 10.9.
    125 14.587029…  HuiZhouG_ba:62:d5   IntelCor_a2:9b:b7   0x0800    890 IPv4
    126 15.213347…  IntelCor_a2:9b:b7   HuiZhouG_ba:62:d5   0x0800     66 IPv4

> Frame 124: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interfa
v Ethernet II, Src: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7), Dst: Routerbo_e9:80:24
  > Destination: Routerbo_e9:80:24 (74:4d:28:e9:80:24)
  > Source: IntelCor_a2:9b:b7 (94:e7:0b:a2:9b:b7)
    Type: ARP (0x0806)
v Address Resolution Protocol (reply)
```

The hexadecimal value for the source address is 94:e7:0b:a2:9b:b7. The hexadecimal value for the destination address if 74:4d:28:e9:80:24.

15. Why is there no ARP reply in the packet trace?
There is no ARP reply in the packet trace because we are not the one who sent out the request. The ARP request is broadcast, and the ARP reply is not broadcast.