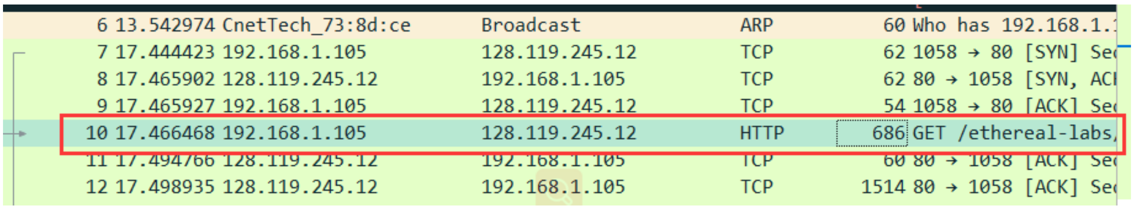
Lab9 Wireshark_ Ethernet and ARP

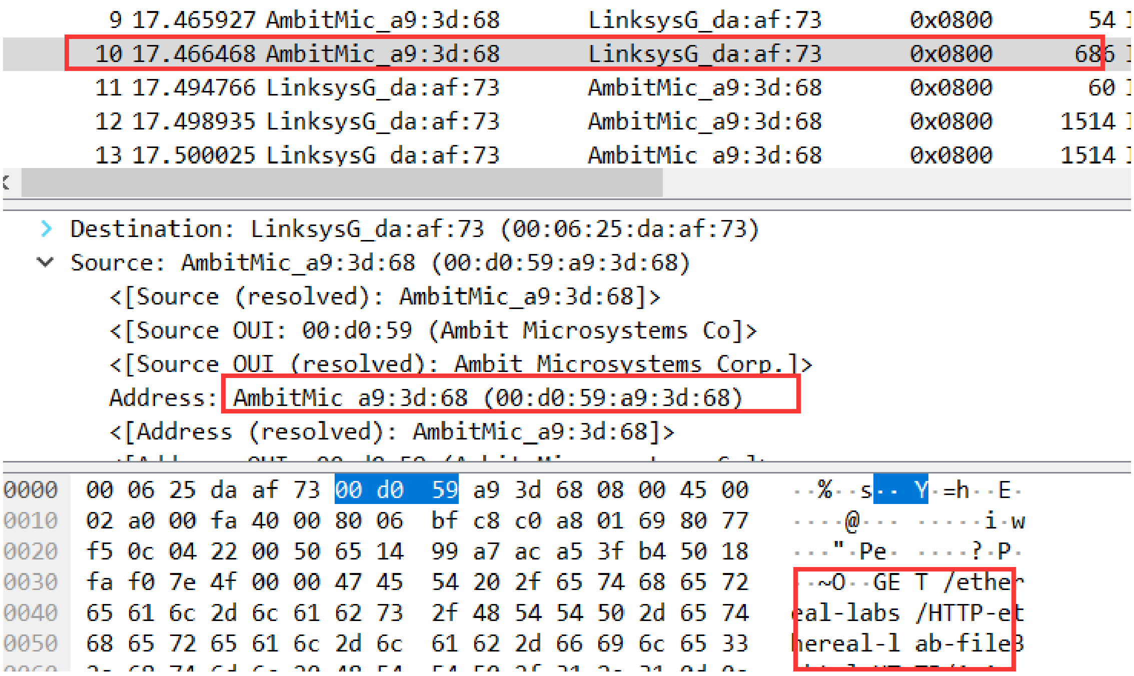
- 学号:1813075
- 姓名:刘茵

---

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



```
 6 13.542974 CnetTech_73:8d:ce   Broadcast        ARP     60 Who has 192.168.1.
 7 17.444423 192.168.1.105       128.119.245.12   TCP     62 1058 → 80 [SYN] Se
 8 17.465902 128.119.245.12      192.168.1.105    TCP     62 80 → 1058 [SYN, AC
 9 17.465927 192.168.1.105       128.119.245.12   TCP     54 1058 → 80 [ACK] Se
10 17.466468 192.168.1.105       128.119.245.12   HTTP   686 GET /ethereal-labs/
11 17.494766 128.119.245.12      192.168.1.105    TCP     60 80 → 1058 [ACK] Se
12 17.498935 128.119.245.12      192.168.1.105    TCP   1514 80 → 1058 [ACK] Se
```



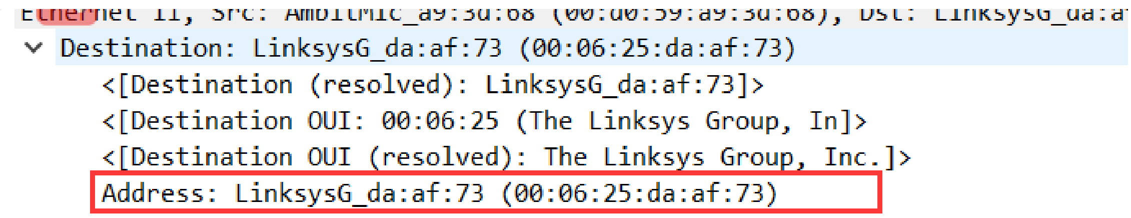
```
 9 17.465927 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800     54 I
10 17.466468 AmbitMic_a9:3d:68   LinksysG_da:af:73   0x0800    686 I
11 17.494766 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800     60 I
12 17.498935 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800   1514 I
13 17.500025 LinksysG_da:af:73   AmbitMic_a9:3d:68   0x0800   1514 I
```

```
  > Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
  v Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
        <[Source (resolved): AmbitMic_a9:3d:68]>
        <[Source OUI: 00:d0:59 (Ambit Microsystems Co]>
        <[Source OUI (resolved): Ambit Microsystems Corp.]>
        Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
        <[Address (resolved): AmbitMic_a9:3d:68]>
```

```
0000  00 06 25 da af 73 00 d0  59 a9 3d 68 08 00 45 00   ··%··s·· Y·=h··E·
0010  02 a0 00 fa 40 00 80 06  bf c8 c0 a8 01 69 80 77   ····@··· ·····i·w
0020  f5 0c 04 22 00 50 65 14  99 a7 ac a5 3f b4 50 18   ···"·Pe· ····?·P·
0030  fa f0 7e 4f 00 00 47 45  54 20 2f 65 74 68 65 72   ··~O··GE T /ether
0040  65 61 6c 2d 6c 61 62 73  2f 48 54 54 50 2d 65 74   eal-labs /HTTP-et
0050  68 65 72 65 61 6c 2d 6c  61 62 2d 66 69 6c 65 33   hereal-l ab-file3
```

答：地址为00:d0:59:a9:3d:68

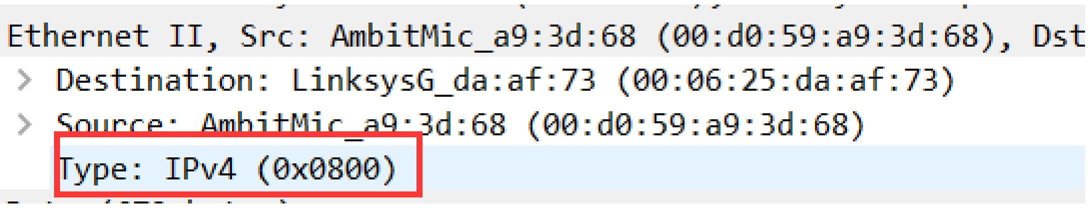
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]



```
  Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:a
  v Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
        <[Destination (resolved): LinksysG_da:af:73]>
        <[Destination OUI: 00:06:25 (The Linksys Group, In]>
        <[Destination OUI (resolved): The Linksys Group, Inc.]>
        Address: LinksysG_da:af:73 (00:06:25:da:af:73)
```

答：目的地址：00:06:25:da:af:73，不是gaia.cs.umass.edu的以太网地址。拥有这个以太网地址的设备是作者的路由器的地址。

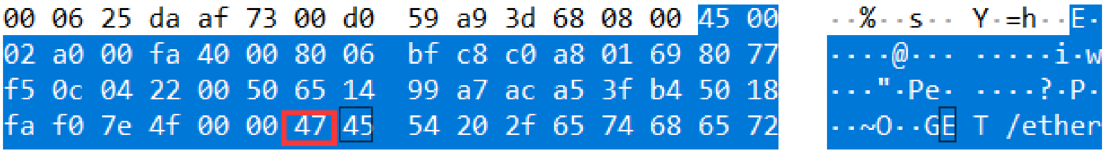
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?



```
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst
  > Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
  > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Type: IPv4 (0x0800)
```

答：十六进制数值：0x0800。代表上层协议是 IPV4

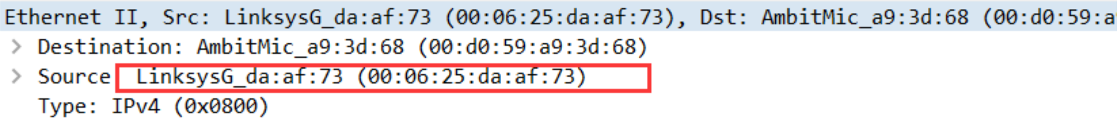
4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?



```
00 06 25 da af 73 00 d0  59 a9 3d 68 08 00 45 00   ··%··s·· Y·=h··E·
02 a0 00 fa 40 00 80 06  bf c8 c0 a8 01 69 80 77   ····@··· ·····i·w
f5 0c 04 22 00 50 65 14  99 a7 ac a5 3f b4 50 18   ···"·Pe· ····?·P·
fa f0 7e 4f 00 00 47 45  54 20 2f 65 74 68 65 72   ··~O··GE T /ether
```

答：有 16 × 3 + 7 = 55 Byte（包含G）

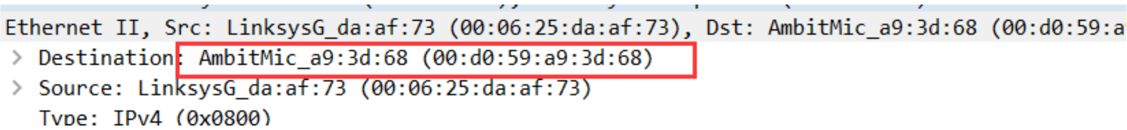
5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?



```
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a
  > Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  > Source: LinksysG_da:af:73 (00:06:25:da:af:73)
    Type: IPv4 (0x0800)
```

答：源地址：00:06:25:da:af:73，这个应该是作者的路由器的地址。

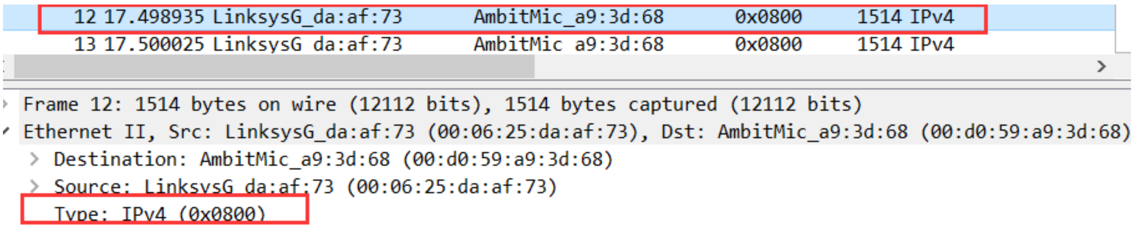
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?



```
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a
  > Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  > Source: LinksysG_da:af:73 (00:06:25:da:af:73)
    Type: IPv4 (0x0800)
```

答：目的地址：00:d0:59:a9:3d:68，这个是计算机的以太网地址。

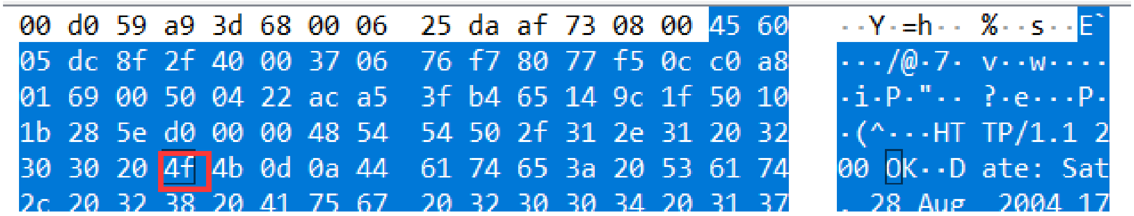
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?



```
   12 17.498935 LinksysG_da:af:73       AmbitMic_a9:3d:68       0x0800      1514 IPv4
   13 17.500025 LinksysG_da:af:73       AmbitMic_a9:3d:68       0x0800      1514 IPv4

> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
v Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  > Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  > Source: LinksysG_da:af:73 (00:06:25:da:af:73)
    Type: IPv4 (0x0800)
```

答：十六进制数值：0x0800。代表上层协议是 IPV4

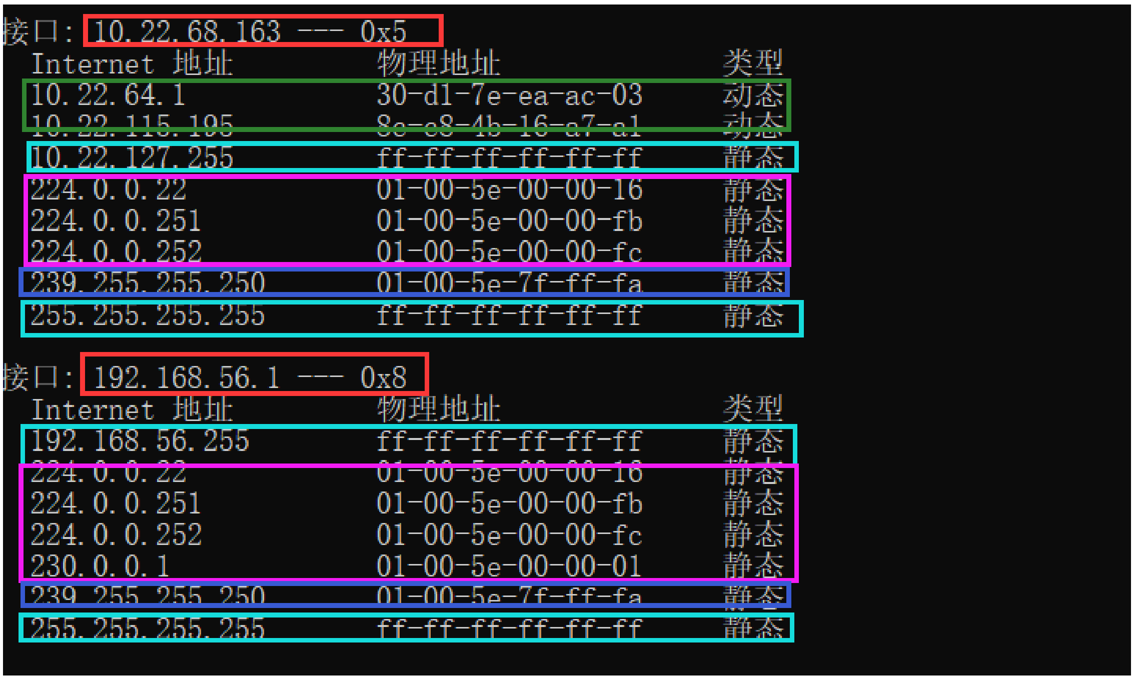
8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in “OK” (i.e., the HTTP response code) appear in the Ethernet frame?



```
00 d0 59 a9 3d 68 00 06  25 da af 73 08 00 45 60   ··Y·=h·· %··s··E`
05 dc 8f 2f 40 00 37 06  76 f7 80 77 f5 0c c0 a8   ···/@·7· v··w····
01 69 00 50 04 22 ac a5  3f b4 65 14 9c 1f 50 10   ·i·P·"·· ?·e···P·
1b 28 5e d0 00 00 48 54  54 50 2f 31 2e 31 20 32   ·(^···HT TP/1.1 2
30 30 20 4f 4b 0d 0a 44  61 74 65 3a 20 53 61 74   00 OK··D ate: Sat
2c 20 32 38 20 41 75 67  20 32 30 30 34 20 31 37   , 28 Aug  2004 17
```

答：有 16 × 4 + 4 = 68 Byte（包含O）

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



```
接口: 10.22.68.163 --- 0x5
  Internet 地址         物理地址              类型
  10.22.64.1            30-d1-7e-ea-ac-03     动态
  10.22.115.195         8c-c8-4b-16-a7-a1     动态
  10.22.127.255         ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态

接口: 192.168.56.1 --- 0x8
  Internet 地址         物理地址              类型
  192.168.56.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.251           01-00-5e-00-00-fb     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
  230.0.0.1             01-00-5e-00-00-01     静态
  239.255.255.250       01-00-5e-7f-ff-fa     静态
  255.255.255.255       ff-ff-ff-ff-ff-ff     静态
```

答：红色：网卡

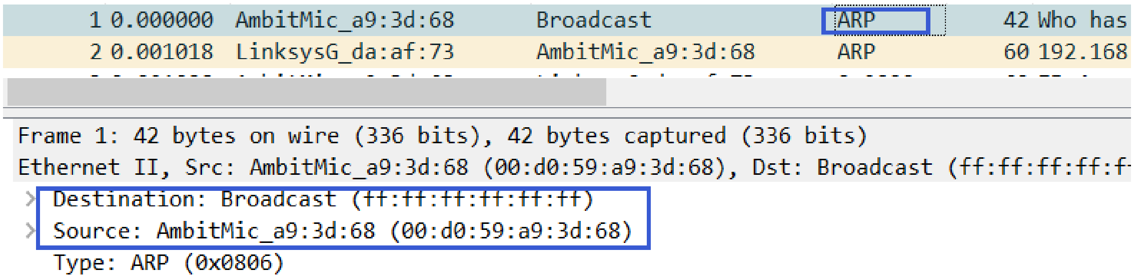
绿色：路由IP和MAC地址

浅蓝色：广播地址

紫色：组播地址（使用）

深蓝色：组播地址（管理）

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

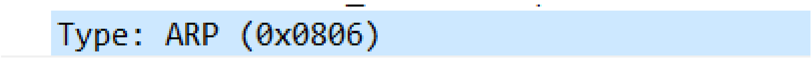


```
    1 0.000000  AmbitMic_a9:3d:68     Broadcast             ARP      42 Who has
    2 0.001018  LinksysG_da:af:73     AmbitMic_a9:3d:68     ARP      60 192.168

 Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
 Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:f
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Type: ARP (0x0806)
```

答：源地址：00:d0:59:a9:3d:68

目的地址：ff:ff:ff:ff:ff:ff

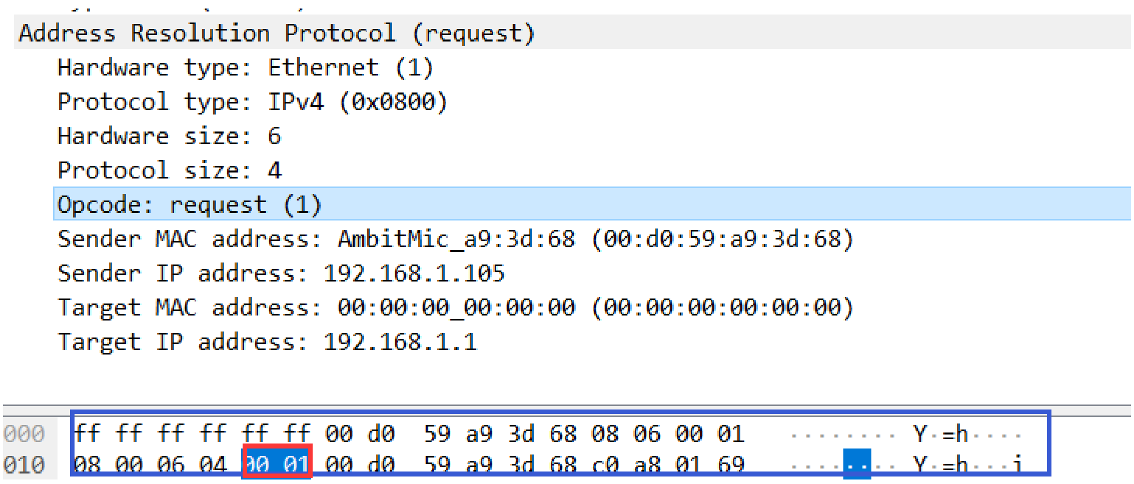
11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?



```
Type: ARP (0x0806)
```

答：0x0806，表示上层协议是 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?



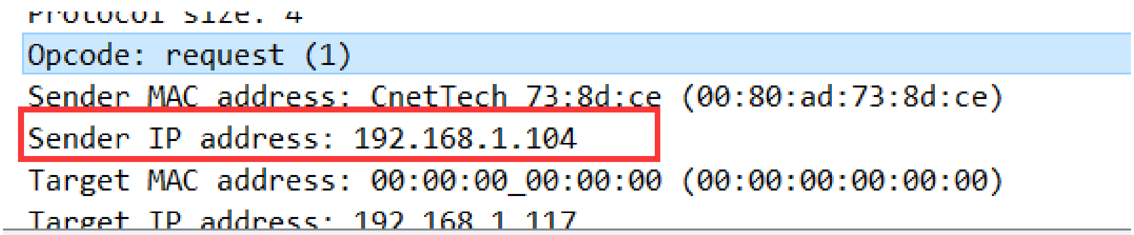
```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Sender IP address: 192.168.1.105
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1

000  ff ff ff ff ff ff 00 d0  59 a9 3d 68 08 06 00 01   ········ Y·=h····
010  08 00 06 04 00 01 00 d0  59 a9 3d 68 c0 a8 01 69   ········ Y·=h···i
```

答：20字节（不包含）21字节（包含第一个）

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?

答：操作码的值为 1。

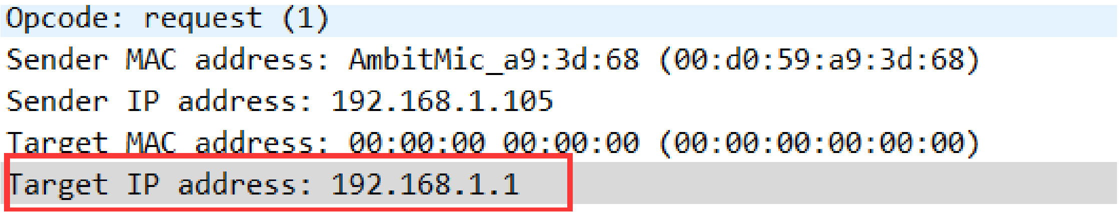
c) Does the ARP message contain the IP address of the sender?



```
Protocol size: 4
Opcode: request (1)
Sender MAC address: CnetTech_73:8d:ce (00:80:ad:73:8d:ce)
Sender IP address: 192.168.1.104
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.117
```

答：ARP 消息包含发送方的 IP 地址。

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

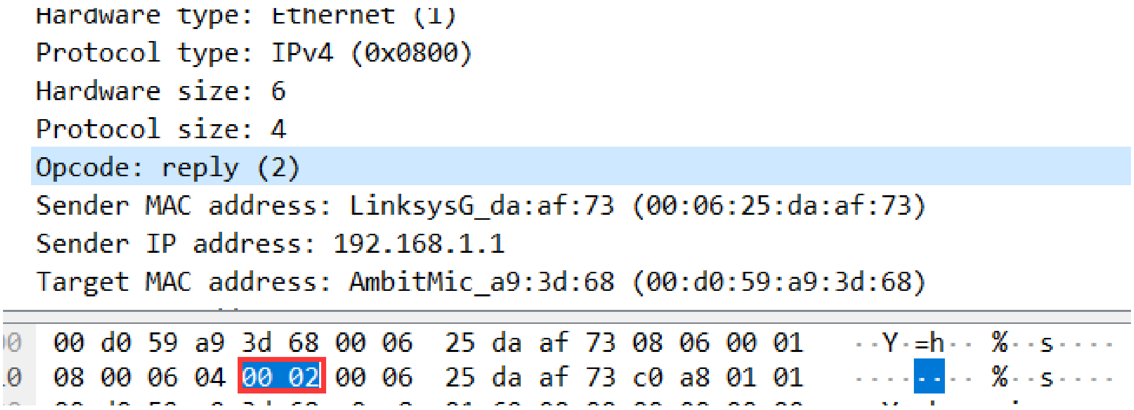


```
Opcode: request (1)
Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Sender IP address: 192.168.1.105
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.1
```

答：Target IP address

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?



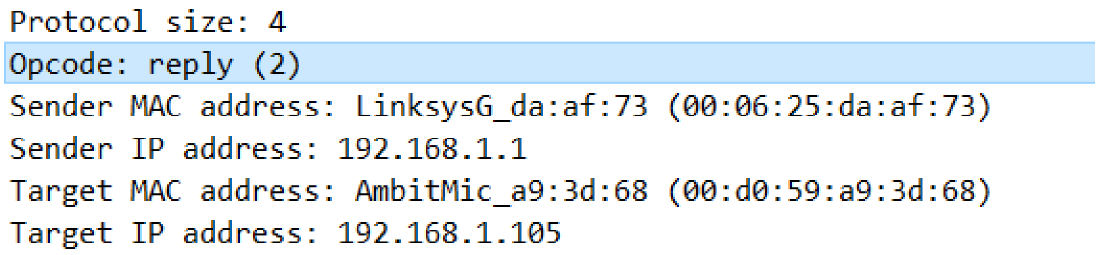
```
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
Sender IP address: 192.168.1.1
Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)

0  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01   ··Y·=h··  %··s····
0  08 00 06 04 00 02 00 06  25 da af 73 c0 a8 01 01   ········  %··s····
```

答：20字节（不包含）21字节（包含第一个）

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?

答：操作码的值为 2。

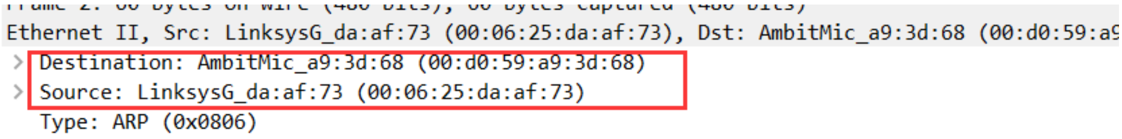
c) Where in the ARP message does the “answer” to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?



```
Protocol size: 4
Opcode: reply (2)
Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
Sender IP address: 192.168.1.1
Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Target IP address: 192.168.1.105
```

答：发送方IP地址和发送方MAC地址

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



```
Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9
  > Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  > Source: LinksysG_da:af:73 (00:06:25:da:af:73)
    Type: ARP (0x0806)
```

答：源地址：00:06:25:da:af:73

目的地址：00:d0:59:a9:3d:68

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?

答：因为 ARP 广播信息是广播的，所有该网段内所有的电脑均可收到，而 ARP 广播回 复是单播的，只有请求的那台电脑才能收到，因此抓不到另外一台电脑的 ARP 请求。