Ethernet and ARP 实验报告

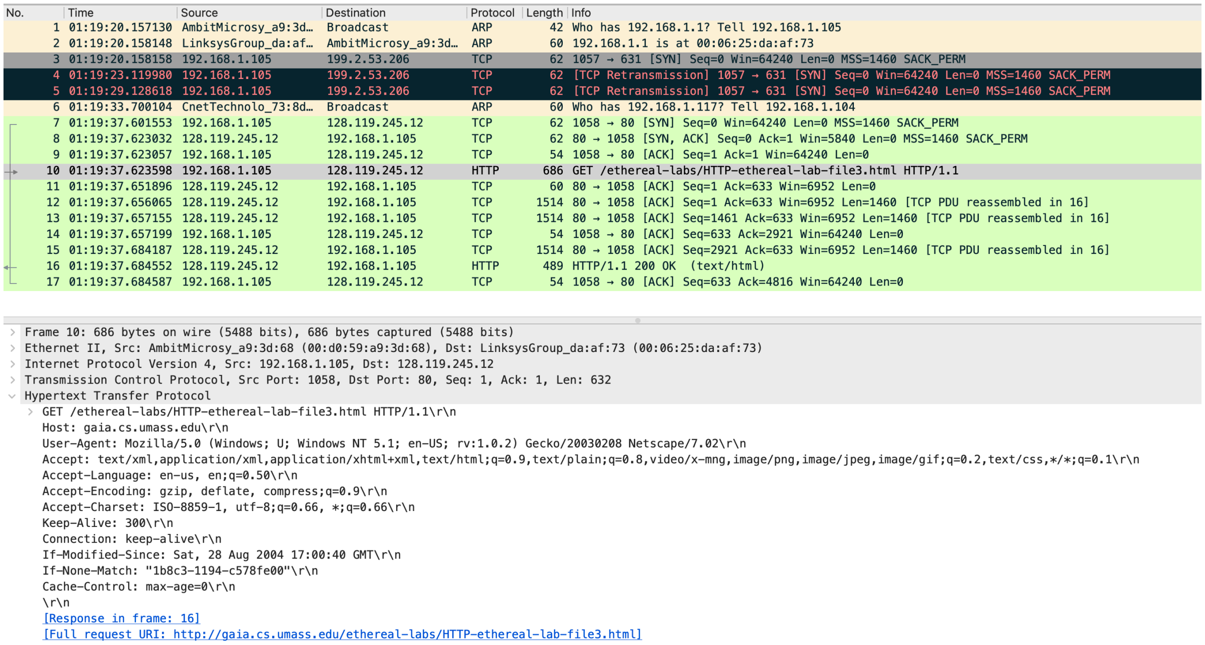
PB22050983 胡延伸

Capturing and analyzing Ethernet frames

- 首先，确保浏览器的缓存为空。开启 Wireshark 进行嗅探。

- 在浏览器中输入以下网址: http://gaia.cs.umass.edu/wireshark-labs/HTTP-ethereal-lab-file3.html

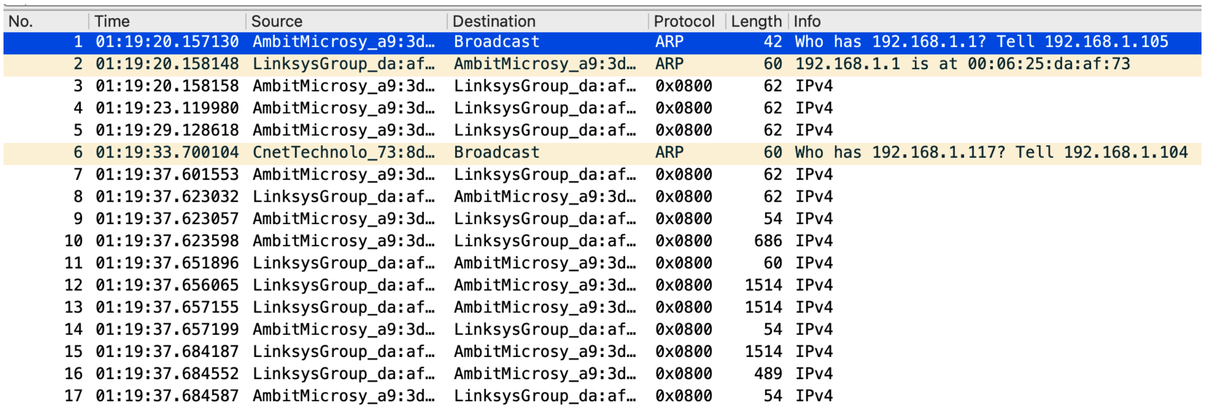
- 停止 Wireshark 数据包捕获。首先，找到从本地计算机发送到 gaia.cs.umass.edu 的 HTTP GET 消息的数据包编号（Wireshark 窗口上方最左侧的列），以及 gaia.cs.umass.edu 发送到本地计算机的 HTTP 响应消息的开头。如下图:



```
No.   Time             Source              Destination         Protocol Length Info
    1 01:19:20.157130  AmbitMicrosy_a9:3d… Broadcast           ARP        42 Who has 192.168.1.1? Tell 192.168.1.105
    2 01:19:20.158148  LinksysGroup_da:af… AmbitMicrosy_a9:3d… ARP        60 192.168.1.1 is at 00:06:25:da:af:73
    3 01:19:20.158158  192.168.1.105       199.2.53.206        TCP        62 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
    4 01:19:23.119980  192.168.1.105       199.2.53.206        TCP        62 [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
    5 01:19:29.128618  192.168.1.105       199.2.53.206        TCP        62 [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
    6 01:19:33.700104  CnetTechnolo_73:8d… Broadcast           ARP        60 Who has 192.168.1.117? Tell 192.168.1.104
    7 01:19:37.601553  192.168.1.105       128.119.245.12      TCP        62 1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
    8 01:19:37.623032  128.119.245.12      192.168.1.105       TCP        62 80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
    9 01:19:37.623057  192.168.1.105       128.119.245.12      TCP        54 1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   10 01:19:37.623598  192.168.1.105       128.119.245.12      HTTP      686 GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
   11 01:19:37.651896  128.119.245.12      192.168.1.105       TCP        60 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
   12 01:19:37.656065  128.119.245.12      192.168.1.105       TCP      1514 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [TCP PDU reassembled in 16]
   13 01:19:37.657155  128.119.245.12      192.168.1.105       TCP      1514 80 → 1058 [ACK] Seq=1461 Ack=633 Win=6952 Len=1460 [TCP PDU reassembled in 16]
   14 01:19:37.657199  192.168.1.105       128.119.245.12      TCP        54 1058 → 80 [ACK] Seq=633 Ack=2921 Win=64240 Len=0
   15 01:19:37.684187  128.119.245.12      192.168.1.105       TCP      1514 80 → 1058 [ACK] Seq=2921 Ack=633 Win=6952 Len=1460 [TCP PDU reassembled in 16]
   16 01:19:37.684552  128.119.245.12      192.168.1.105       HTTP      489 HTTP/1.1 200 OK  (text/html)
   17 01:19:37.684587  192.168.1.105       128.119.245.12      TCP        54 1058 → 80 [ACK] Seq=633 Ack=4816 Win=64240 Len=0
```

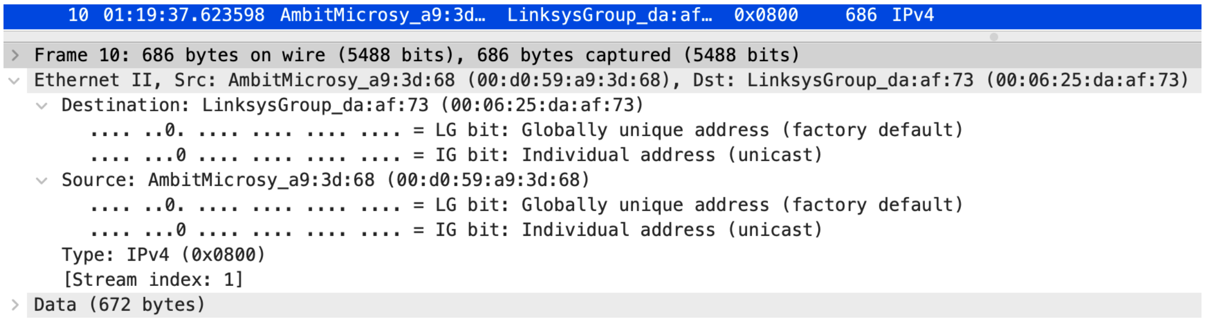
```
> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
> Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)
> Internet Protocol Version 4, Src: 192.168.1.105, Dst: 128.119.245.12
> Transmission Control Protocol, Src Port: 1058, Dst Port: 80, Seq: 1, Ack: 1, Len: 632
v Hypertext Transfer Protocol
  > GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n
    Host: gaia.cs.umass.edu\r\n
    User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.0.2) Gecko/20030208 Netscape/7.02\r\n
    Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,video/x-mng,image/png,image/jpeg,image/gif;q=0.2,text/css,*/*;q=0.1\r\n
    Accept-Language: en-us, en;q=0.50\r\n
    Accept-Encoding: gzip, deflate, compress;q=0.9\r\n
    Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66\r\n
    Keep-Alive: 300\r\n
    Connection: keep-alive\r\n
    If-Modified-Since: Sat, 28 Aug 2004 17:00:40 GMT\r\n
    If-None-Match: "1b8c3-1194-c578fe00"\r\n
    Cache-Control: max-age=0\r\n
    \r\n
    [Response in frame: 16]
    [Full request URI: http://gaia.cs.umass.edu/ethereal-labs/HTTP-ethereal-lab-file3.html]
```

- 更改 Wireshark 的“捕获数据包列表”窗口以便它仅显示有关 IP 下的协议的信息。如下图



```
No.  Time             Source               Destination          Protocol Length Info
   1 01:19:20.157130  AmbitMicrosy_a9:3d…  Broadcast            ARP        42 Who has 192.168.1.1? Tell 192.168.1.105
   2 01:19:20.158148  LinksysGroup_da:af…  AmbitMicrosy_a9:3d…  ARP        60 192.168.1.1 is at 00:06:25:da:af:73
   3 01:19:20.158158  AmbitMicrosy_a9:3d…  LinksysGroup_da:af…  0x0800     62 IPv4
   4 01:19:23.119980  AmbitMicrosy_a9:3d…  LinksysGroup_da:af…  0x0800     62 IPv4
   5 01:19:29.128618  AmbitMicrosy_a9:3d…  LinksysGroup_da:af…  0x0800     62 IPv4
   6 01:19:33.700104  CnetTechnolo_73:8d…  Broadcast            ARP        60 Who has 192.168.1.117? Tell 192.168.1.104
   7 01:19:37.601553  AmbitMicrosy_a9:3d…  LinksysGroup_da:af…  0x0800     62 IPv4
   8 01:19:37.623032  LinksysGroup_da:af…  AmbitMicrosy_a9:3d…  0x0800     62 IPv4
   9 01:19:37.623057  AmbitMicrosy_a9:3d…  LinksysGroup_da:af…  0x0800     54 IPv4
  10 01:19:37.623598  AmbitMicrosy_a9:3d…  LinksysGroup_da:af…  0x0800    686 IPv4
  11 01:19:37.651896  LinksysGroup_da:af…  AmbitMicrosy_a9:3d…  0x0800     60 IPv4
  12 01:19:37.656065  LinksysGroup_da:af…  AmbitMicrosy_a9:3d…  0x0800   1514 IPv4
  13 01:19:37.657155  LinksysGroup_da:af…  AmbitMicrosy_a9:3d…  0x0800   1514 IPv4
  14 01:19:37.657199  AmbitMicrosy_a9:3d…  LinksysGroup_da:af…  0x0800     54 IPv4
  15 01:19:37.684187  LinksysGroup_da:af…  AmbitMicrosy_a9:3d…  0x0800   1514 IPv4
  16 01:19:37.684552  LinksysGroup_da:af…  AmbitMicrosy_a9:3d…  0x0800    489 IPv4
  17 01:19:37.684587  AmbitMicrosy_a9:3d…  LinksysGroup_da:af…  0x0800     54 IPv4
```

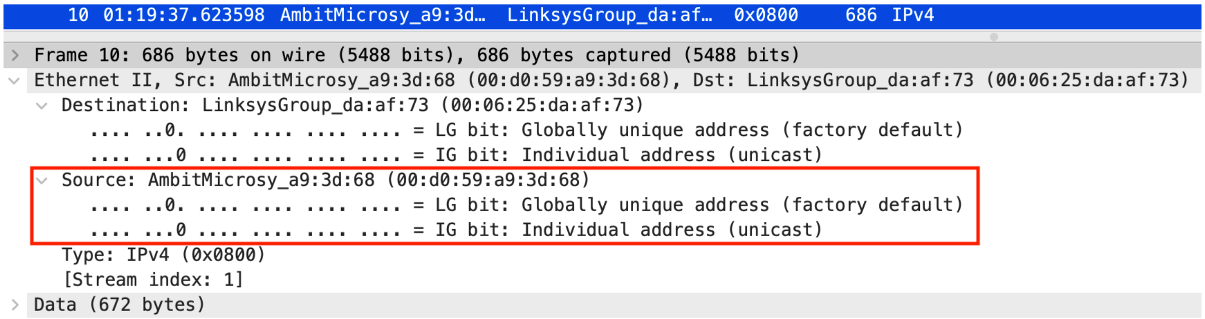
- 选择包含 HTTP GET 消息的以太网帧。在数据包详细信息窗口中展开以太网 II 信息。对比之前的捕捉窗口，找到包含 HTTP GET 的数据包如下:



```
  10 01:19:37.623598  AmbitMicrosy_a9:3d…  LinksysGroup_da:af…  0x0800    686  IPv4

> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
v Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)
  v Destination: LinksysGroup_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 1]
> Data (672 bytes)
```

Question

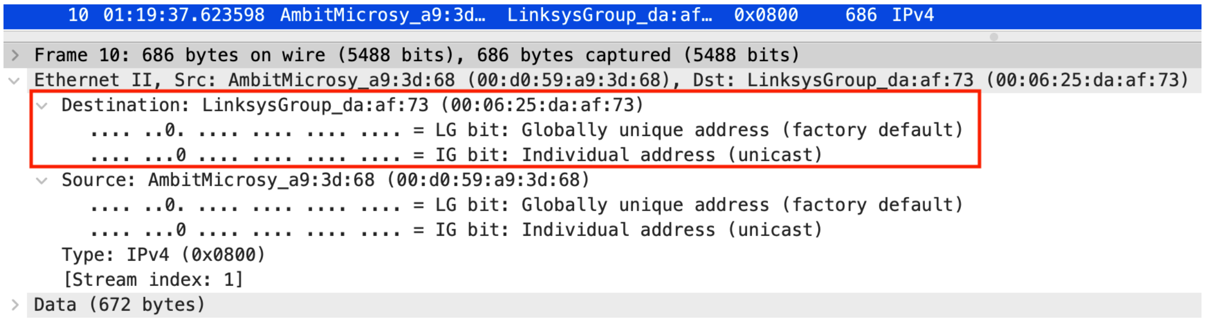
1. What is the 48-bit Ethernet address of your computer?



```
  10 01:19:37.623598  AmbitMicrosy_a9:3d…  LinksysGroup_da:af…  0x0800    686  IPv4

> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
v Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)
  v Destination: LinksysGroup_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 1]
> Data (672 bytes)
```

   AmbitMicrosy_a9:3d:68(00:06:25:da:af:73)

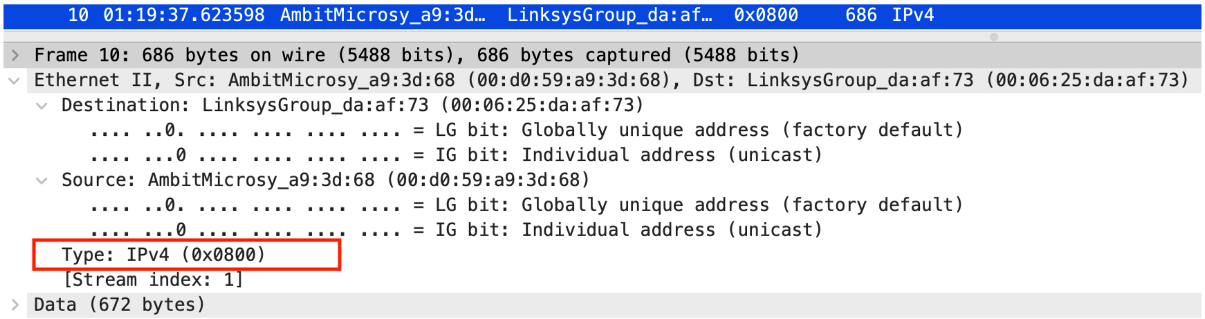
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address?



```
    10 01:19:37.623598  AmbitMicrosy_a9:3d…  LinksysGroup_da:af…  0x0800    686  IPv4
> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
v Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)
  v Destination: LinksysGroup_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 1]
> Data (672 bytes)
```

LinksysGroup_da:af:73 (00:06:25:da:af:73); 不是 gaia.cs.umass.edu 的以太网地址，是出子网的路由器的地址。

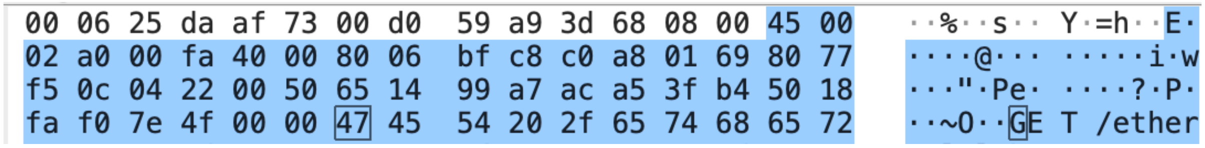
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?



```
    10 01:19:37.623598  AmbitMicrosy_a9:3d…  LinksysGroup_da:af…  0x0800    686  IPv4
> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
v Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysGroup_da:af:73 (00:06:25:da:af:73)
  v Destination: LinksysGroup_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 1]
> Data (672 bytes)
```

0x0800; IPv4

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

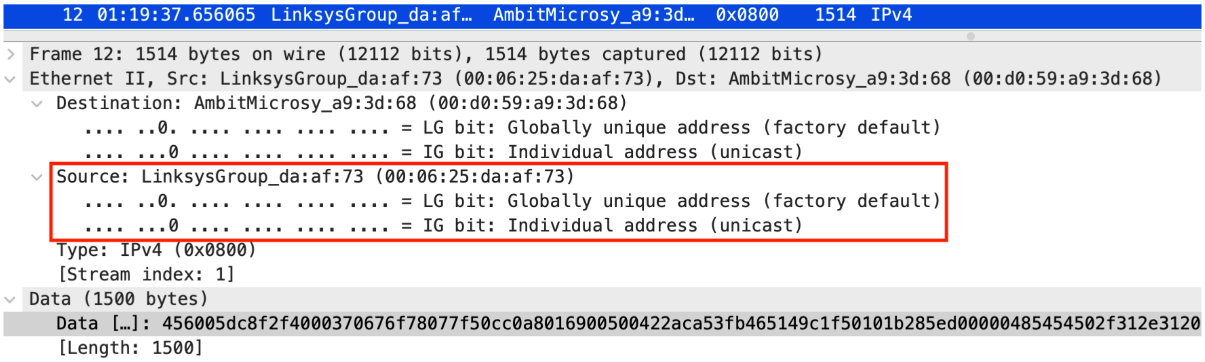


```
00 06 25 da af 73 00 d0  59 a9 3d 68 08 00 45 00   ··%··s·· Y·=h··E·
02 a0 00 fa 40 00 80 06  bf c8 c0 a8 01 69 80 77   ····@··· ·····i·w
f5 0c 04 22 00 50 65 14  99 a7 ac a5 3f b4 50 18   ···"·Pe· ····?·P·
fa f0 7e 4f 00 00 47 45  54 20 2f 65 74 68 65 72   ··~O··GE T /ether
```

16 × 3 + 7 = 55 bytes

接下来，根据包含 HTTP 响应消息的第一个字节的以太网帧的内容回答以下问题。

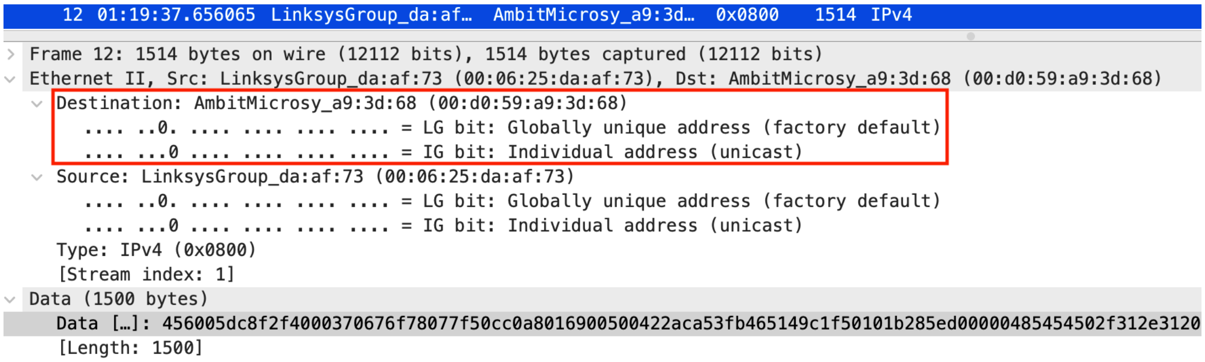
5. What is the value of the Ethernet source address? Is this the address of your computer, or of gaia.cs.umass.edu (Hint: the answer is no). What device has this as its Ethernet address?



```
    12 01:19:37.656065  LinksysGroup_da:af…  AmbitMicrosy_a9:3d…  0x0800   1514  IPv4
> Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
v Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
  v Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 1]
v Data (1500 bytes)
    Data […]: 456005dc8f2f4000370676f78077f50cc0a8016900500422aca53fb465149c1f50101b285ed00000485454502f312e3120
    [Length: 1500]
```

Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)；不是；应该是出子网的路由器的地址

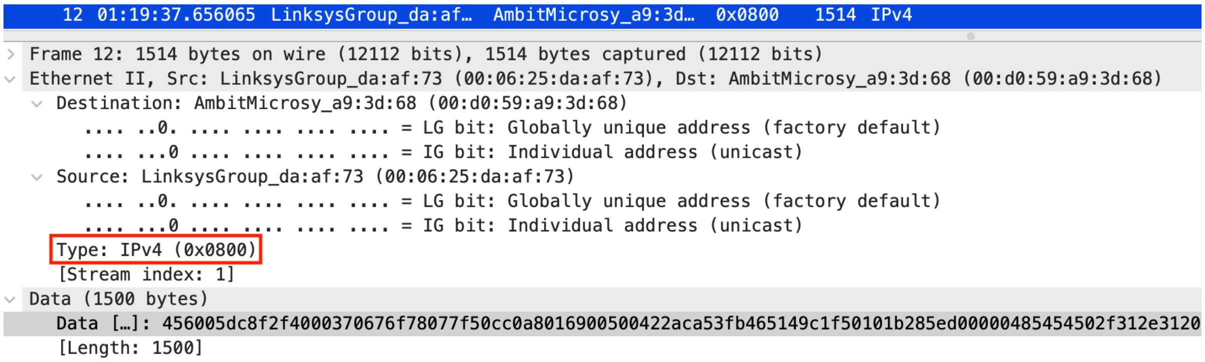
6. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?



```
     12 01:19:37.656065 LinksysGroup_da:af…  AmbitMicrosy_a9:3d…  0x0800    1514 IPv4

>  Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
v  Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
   v  Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
         .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
         .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   v  Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
         .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
         .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      Type: IPv4 (0x0800)
      [Stream index: 1]
v  Data (1500 bytes)
      Data […]: 456005dc8f2f4000370676f78077f50cc0a8016900500422aca53fb465149c1f50101b285ed00000485454502f312e3120
      [Length: 1500]
```

Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68); 是我的计算机以太网地址。

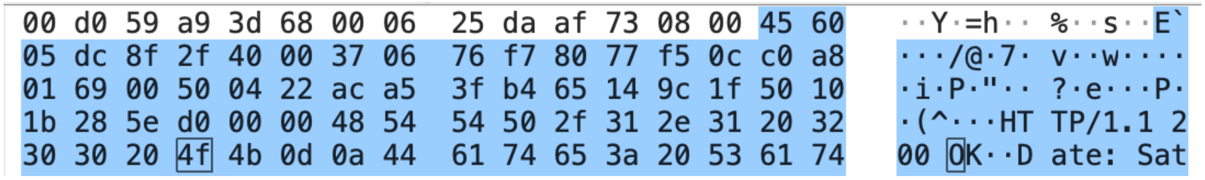
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?



```
     12 01:19:37.656065 LinksysGroup_da:af…  AmbitMicrosy_a9:3d…  0x0800    1514 IPv4

>  Frame 12: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
v  Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
   v  Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
         .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
         .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
   v  Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
         .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
         .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
      Type: IPv4 (0x0800)
      [Stream index: 1]
v  Data (1500 bytes)
      Data […]: 456005dc8f2f4000370676f78077f50cc0a8016900500422aca53fb465149c1f50101b285ed00000485454502f312e3120
      [Length: 1500]
```

0x0800;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?



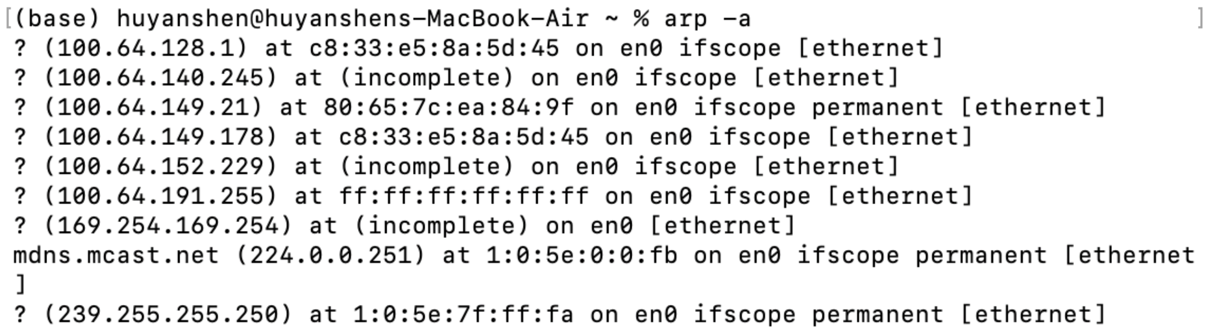
```
00 d0 59 a9 3d 68 00 06  25 da af 73 08 00 45 60   ··Y·=h·· %··s··E`
05 dc 8f 2f 40 00 37 06  76 f7 80 77 f5 0c c0 a8   ···/@·7· v··w····
01 69 00 50 04 22 ac a5  3f b4 65 14 9c 1f 50 10   ·i·P·"·· ?·e···P·
1b 28 5e d0 00 00 48 54  54 50 2f 31 2e 31 20 32   ·(^···HT TP/1.1 2
30 30 20 4f 4b 0d 0a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

16 × 4 + 4 = 68 bytes

The Address Resolution Protocol

Question

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

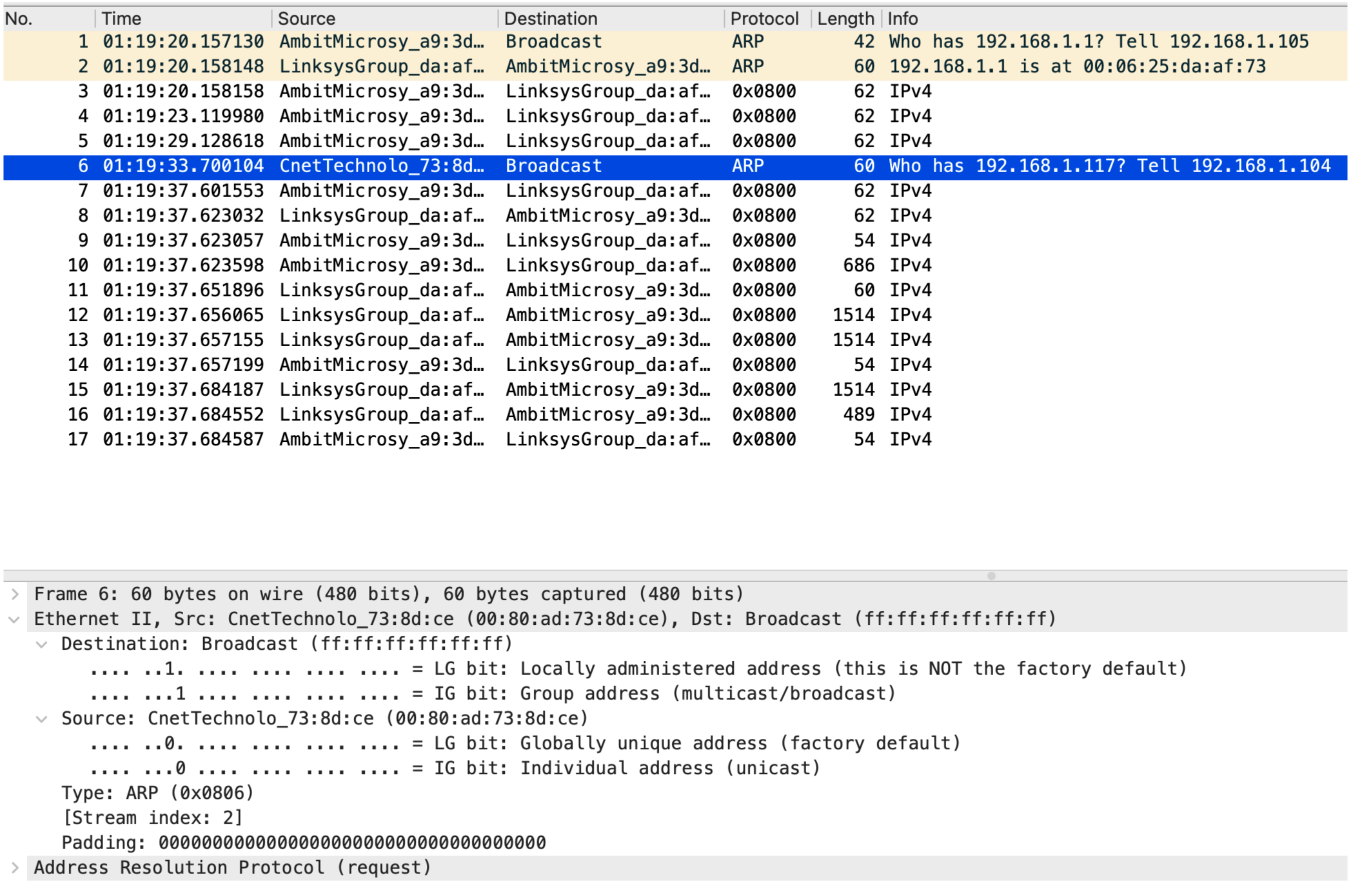


```
[(base) huyanshen@huyanshens-MacBook-Air ~ % arp -a
? (100.64.128.1) at c8:33:e5:8a:5d:45 on en0 ifscope [ethernet]
? (100.64.140.245) at (incomplete) on en0 ifscope [ethernet]
? (100.64.149.21) at 80:65:7c:ea:84:9f on en0 ifscope permanent [ethernet]
? (100.64.149.178) at c8:33:e5:8a:5d:45 on en0 ifscope [ethernet]
? (100.64.152.229) at (incomplete) on en0 ifscope [ethernet]
? (100.64.191.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (169.254.169.254) at (incomplete) on en0 [ethernet]
mdns.mcast.net (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet
]
? (239.255.255.250) at 1:0:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
```

其每一列的意义为: <hostname> (<IP address>) at <MAC address> on <interface>

接下来清除 ARP 缓存，以便电脑能发送 ARP 消息。

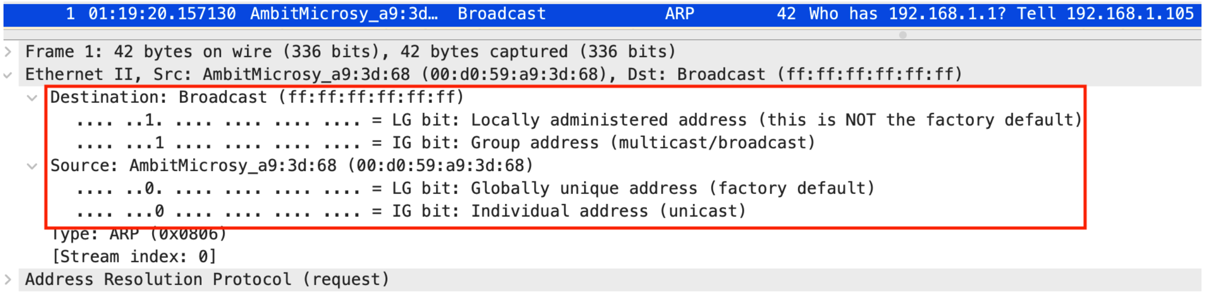
- 确保浏览器的缓存是空的,启动 Wireshark 数据包嗅探器.
- 在浏览器中输入以下网址 http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-lab-file3.html
- 停止 Wireshark 数据包捕获. 并且弃选 IP 及以上协议。得到如下界面。



```
No.  Time             Source                Destination           Protocol  Length  Info
  1  01:19:20.157130  AmbitMicrosy_a9:3d…   Broadcast             ARP           42  Who has 192.168.1.1? Tell 192.168.1.105
  2  01:19:20.158148  LinksysGroup_da:af…   AmbitMicrosy_a9:3d…   ARP           60  192.168.1.1 is at 00:06:25:da:af:73
  3  01:19:20.158158  AmbitMicrosy_a9:3d…   LinksysGroup_da:af…   0x0800        62  IPv4
  4  01:19:23.119980  AmbitMicrosy_a9:3d…   LinksysGroup_da:af…   0x0800        62  IPv4
  5  01:19:29.128618  AmbitMicrosy_a9:3d…   LinksysGroup_da:af…   0x0800        62  IPv4
  6  01:19:33.700104  CnetTechnolo_73:8d…   Broadcast             ARP           60  Who has 192.168.1.117? Tell 192.168.1.104
  7  01:19:37.601553  AmbitMicrosy_a9:3d…   LinksysGroup_da:af…   0x0800        62  IPv4
  8  01:19:37.623032  LinksysGroup_da:af…   AmbitMicrosy_a9:3d…   0x0800        62  IPv4
  9  01:19:37.623057  AmbitMicrosy_a9:3d…   LinksysGroup_da:af…   0x0800        54  IPv4
 10  01:19:37.623598  AmbitMicrosy_a9:3d…   LinksysGroup_da:af…   0x0800       686  IPv4
 11  01:19:37.651896  LinksysGroup_da:af…   AmbitMicrosy_a9:3d…   0x0800        60  IPv4
 12  01:19:37.656065  LinksysGroup_da:af…   AmbitMicrosy_a9:3d…   0x0800      1514  IPv4
 13  01:19:37.657155  LinksysGroup_da:af…   AmbitMicrosy_a9:3d…   0x0800      1514  IPv4
 14  01:19:37.657199  AmbitMicrosy_a9:3d…   LinksysGroup_da:af…   0x0800        54  IPv4
 15  01:19:37.684187  LinksysGroup_da:af…   AmbitMicrosy_a9:3d…   0x0800      1514  IPv4
 16  01:19:37.684552  LinksysGroup_da:af…   AmbitMicrosy_a9:3d…   0x0800       489  IPv4
 17  01:19:37.684587  AmbitMicrosy_a9:3d…   LinksysGroup_da:af…   0x0800        54  IPv4
```

```
> Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
v Ethernet II, Src: CnetTechnolo_73:8d:ce (00:80:ad:73:8d:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: CnetTechnolo_73:8d:ce (00:80:ad:73:8d:ce)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    [Stream index: 2]
    Padding: 000000000000000000000000000000000000
> Address Resolution Protocol (request)
```

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

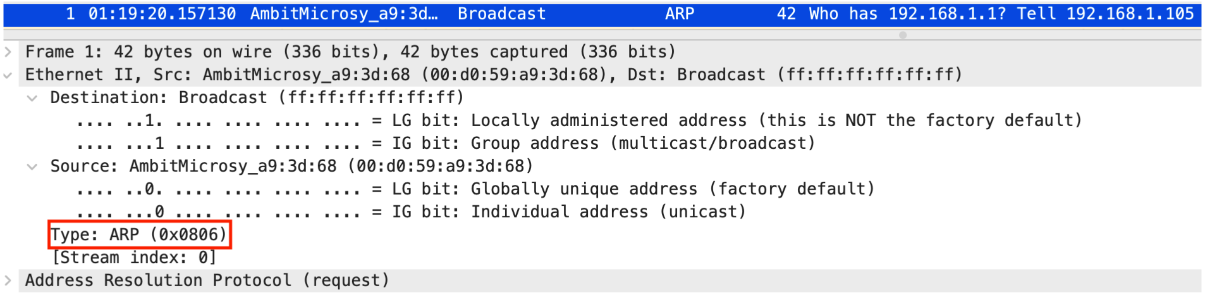


```
1 01:19:20.157130  AmbitMicrosy_a9:3d…  Broadcast            ARP        42  Who has 192.168.1.1? Tell 192.168.1.105

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
v Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    [Stream index: 0]
> Address Resolution Protocol (request)
```

Destination: Broadcast (ff:ff:ff:ff:ff:ff);

Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)

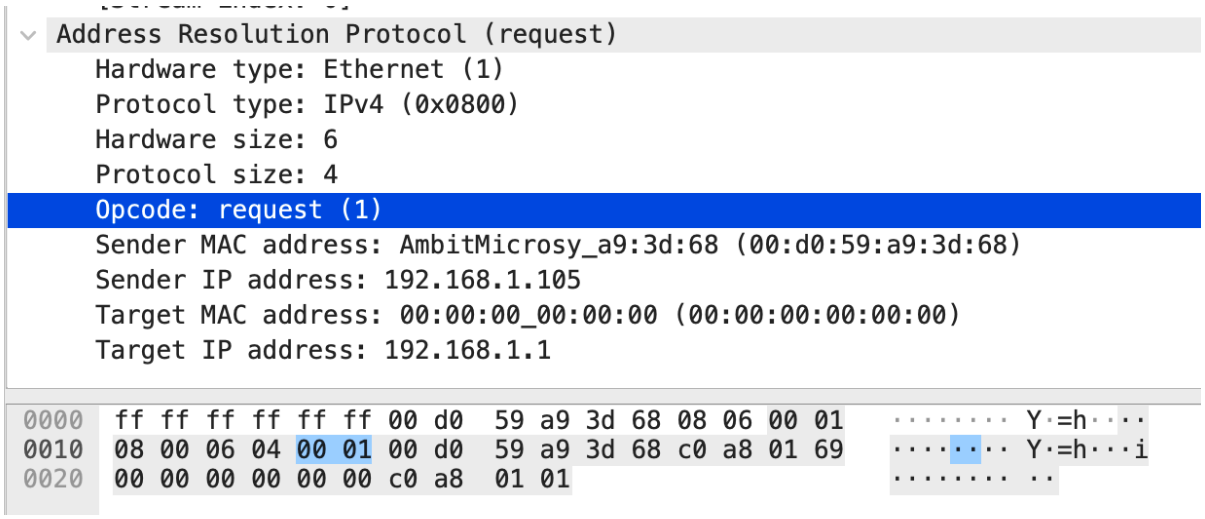
11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?



```
1 01:19:20.157130  AmbitMicrosy_a9:3d…  Broadcast            ARP        42  Who has 192.168.1.1? Tell 192.168.1.105

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
v Ethernet II, Src: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  v Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadcast)
  v Source: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    [Stream index: 0]
> Address Resolution Protocol (request)
```

0x0806; ARP

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



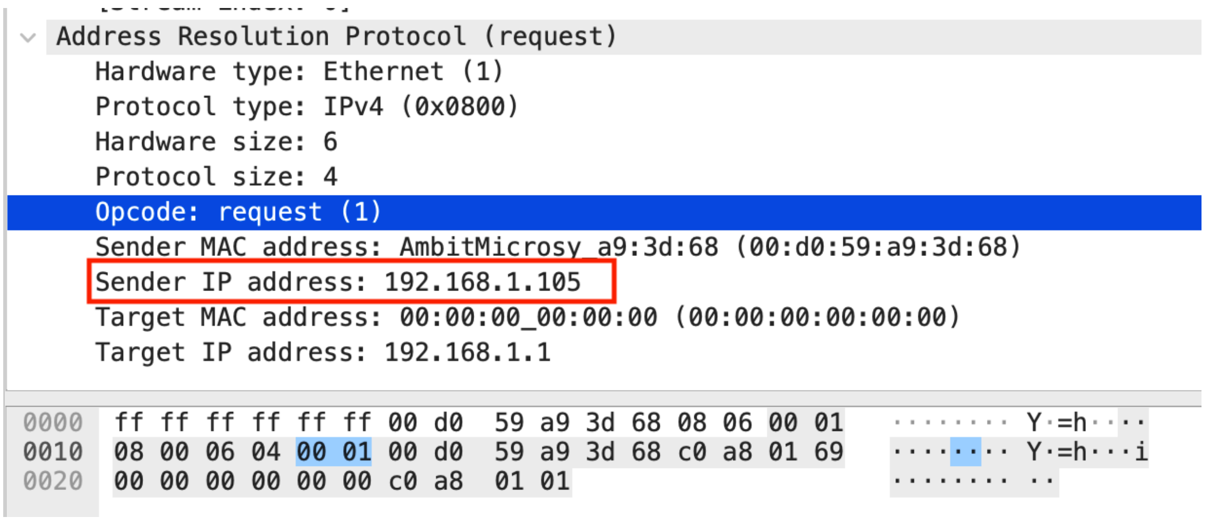
```
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
    Sender IP address: 192.168.1.105
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 192.168.1.1

0000  ff ff ff ff ff ff 00 d0  59 a9 3d 68 08 06 00 01   ········ Y·=h····
0010  08 00 06 04 00 01 00 d0  59 a9 3d 68 c0 a8 01 69   ········ Y·=h···i
0020  00 00 00 00 00 00 c0 a8  01 01                     ········ ··
```

16 + 5 = 21 bytes

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?

操作码值为1.

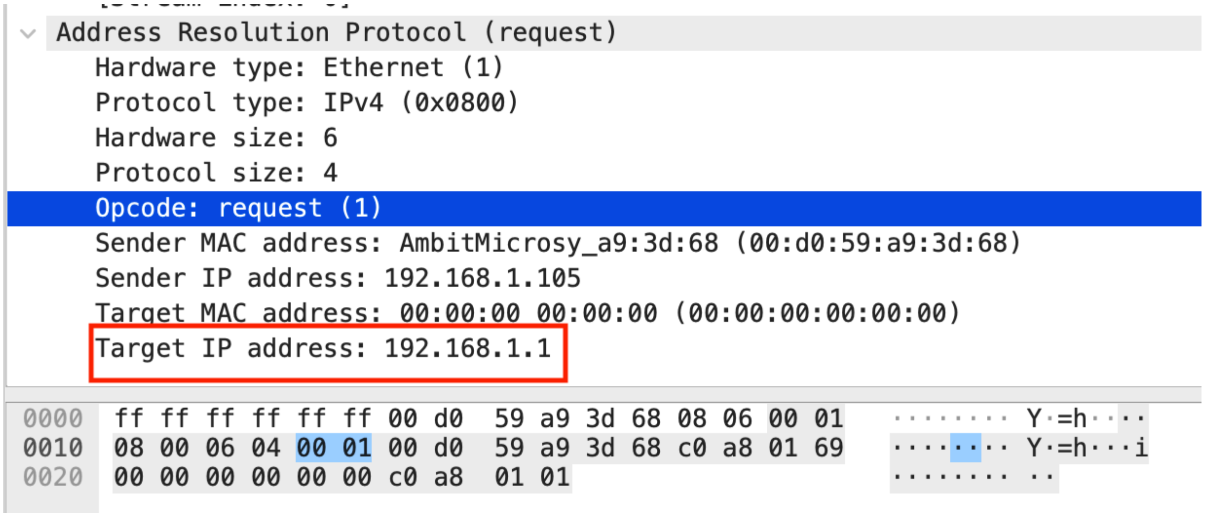
c)Does the ARP message contain the IP address of the sender?



```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AmbitMicrosy_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

0000  ff ff ff ff ff ff 00 d0  59 a9 3d 68 08 06 00 01   ········ Y·=h····
0010  08 00 06 04 00 01 00 d0  59 a9 3d 68 c0 a8 01 69   ········ Y·=h···i
0020  00 00 00 00 00 00 c0 a8  01 01                     ········ ··
```

包含

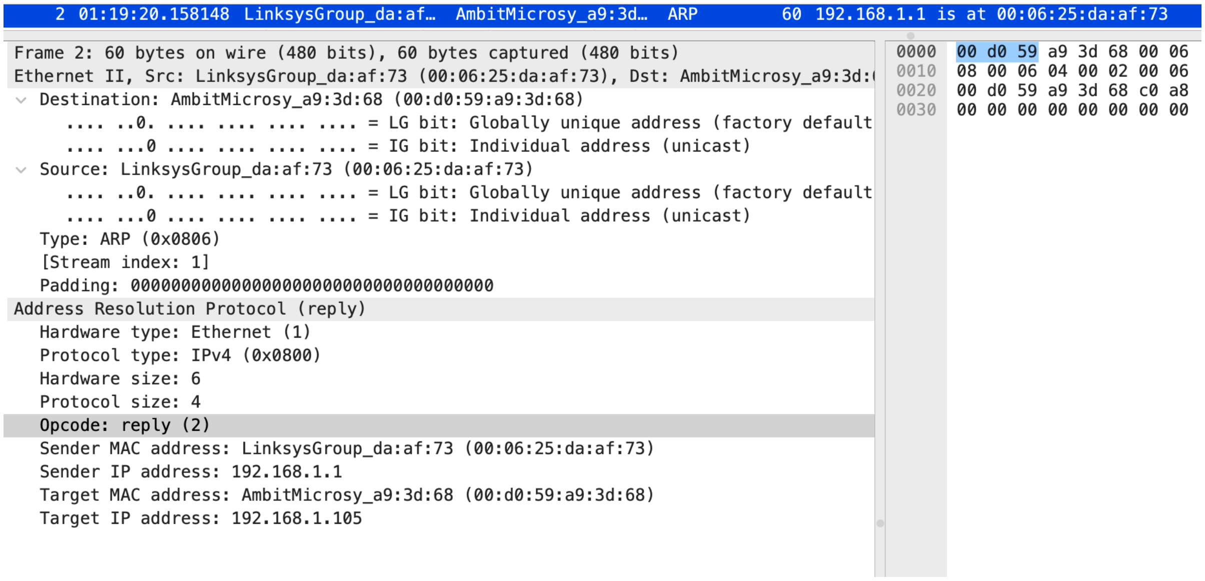
d)Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?



```
Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: AmbitMicrosy_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

0000  ff ff ff ff ff ff 00 d0  59 a9 3d 68 08 06 00 01   ········ Y·=h····
0010  08 00 06 04 00 01 00 d0  59 a9 3d 68 c0 a8 01 69   ········ Y·=h···i
0020  00 00 00 00 00 00 c0 a8  01 01                     ········ ··
```

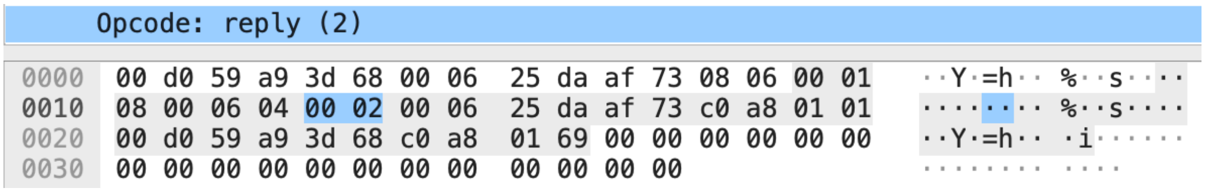
如上图，包含 Target IP address.

13. Now find the ARP reply that was sent in response to the ARP request.



```
  2 01:19:20.158148  LinksysGroup_da:af…  AmbitMicrosy_a9:3d…  ARP        60  192.168.1.1 is at 00:06:25:da:af:73

Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)          0000  00 d0 59 a9 3d 68 00 06
Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:(   0010  08 00 06 04 00 02 00 06
∨ Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)                   0020  00 d0 59 a9 3d 68 c0 a8
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default   0030  00 00 00 00 00 00 00 00
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
∨ Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  [Stream index: 1]
  Padding: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: LinksysGroup_da:af:73 (00:06:25:da:af:73)
  Sender IP address: 192.168.1.1
  Target MAC address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
  Target IP address: 192.168.1.105
```

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



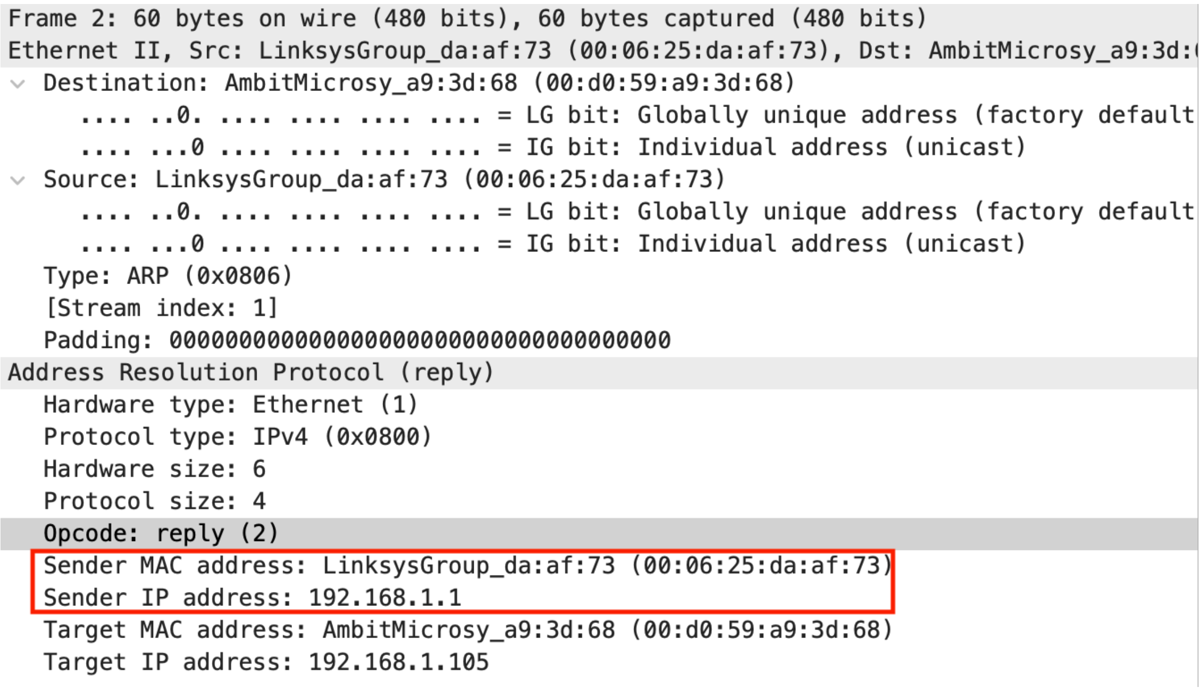
```
      Opcode: reply (2)

0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01   ··Y·=h·· %··s····
0010  08 00 06 04 00 02 00 06  25 da af 73 c0 a8 01 01   ········ %··s····
0020  00 d0 59 a9 3d 68 c0 a8  01 69 00 00 00 00 00 00   ··Y·=h·· ·i······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

16 + 5 = 21 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?

如上题图，Opcode 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?



```
Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
Ethernet II, Src: LinksysGroup_da:af:73 (00:06:25:da:af:73), Dst: AmbitMicrosy_a9:3d:(
  Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
     .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default
     .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)
     .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default
     .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  [Stream index: 1]
  Padding: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: LinksysGroup_da:af:73 (00:06:25:da:af:73)
  Sender IP address: 192.168.1.1
  Target MAC address: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)
  Target IP address: 192.168.1.105
```

在 Sender IP address 项中: 192.168.1.1。

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

Destination: AmbitMicrosy_a9:3d:68 (00:d0:59:a9:3d:68)

Source: LinksysGroup_da:af:73 (00:06:25:da:af:73)

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?

因为 ARP 查询分组是广播，而响应分组是单播。