Lab 7: NAT, Ethernet and ARP

Exercise 1：IP Addressing, NAT
Question 1:
Answer:

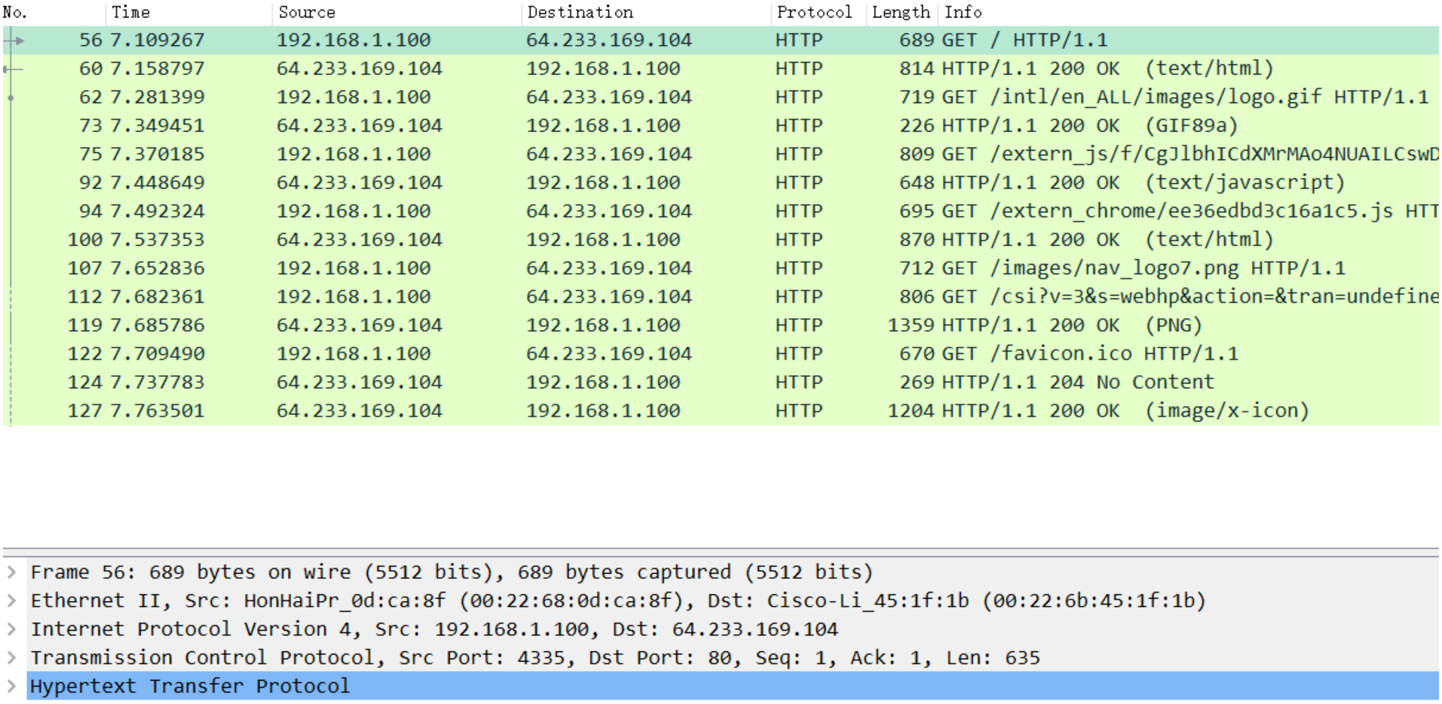
Subnet	Number	Netmask
Subnet 1	10.0.1.0	255.255.255.0
Subnet 2	10.0.2.0	255.255.255.0
Subnet 3	10.0.3.0	255.255.255.0

Interface	IP Address
H1	10.0.1.1
H2	10.0.1.2
H3	10.0.2.1
H4	10.0.2.2
R1a	10.0.1.3
R1b	10.0.3.1
R1c	10.0.2.3
NAT-i	10.0.3.2

Question 4:
Answer:
For example，FTP protocol would not work through this NAT because FTP is based on TCP protocol. It need to open a connection directly between server and client when it works. Any protocol that embeds IP or TCP-layer information in the application stream is likely to be broken by a basic NAT box.

Exercise 2: Understanding NAT using Wireshark
Question 2:
Answer:
source IP address:192.168.1.100
source port:4335
destination address:64.233.169.104

destination port:80



```
No.      Time        Source           Destination      Protocol  Length Info
     56 7.109267     192.168.1.100    64.233.169.104   HTTP       689 GET / HTTP/1.1
     60 7.158797     64.233.169.104   192.168.1.100    HTTP       814 HTTP/1.1 200 OK  (text/html)
     62 7.281399     192.168.1.100    64.233.169.104   HTTP       719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
     73 7.349451     64.233.169.104   192.168.1.100    HTTP       226 HTTP/1.1 200 OK  (GIF89a)
     75 7.370185     192.168.1.100    64.233.169.104   HTTP       809 GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswD
     92 7.448649     64.233.169.104   192.168.1.100    HTTP       648 HTTP/1.1 200 OK  (text/javascript)
     94 7.492324     192.168.1.100    64.233.169.104   HTTP       695 GET /extern_chrome/ee36edbd3c16a1c5.js HTT
    100 7.537353     64.233.169.104   192.168.1.100    HTTP       870 HTTP/1.1 200 OK  (text/html)
    107 7.652836     192.168.1.100    64.233.169.104   HTTP       712 GET /images/nav_logo7.png HTTP/1.1
    112 7.682361     192.168.1.100    64.233.169.104   HTTP       806 GET /csi?v=3&s=webhp&action=&tran=undefine
    119 7.685786     64.233.169.104   192.168.1.100    HTTP      1359 HTTP/1.1 200 OK  (PNG)
    122 7.709490     192.168.1.100    64.233.169.104   HTTP       670 GET /favicon.ico HTTP/1.1
    124 7.737783     64.233.169.104   192.168.1.100    HTTP       269 HTTP/1.1 204 No Content
    127 7.763501     64.233.169.104   192.168.1.100    HTTP      1204 HTTP/1.1 200 OK  (image/x-icon)

> Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
> Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b)
> Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
> Hypertext Transfer Protocol
```

Question 3:

Answer:

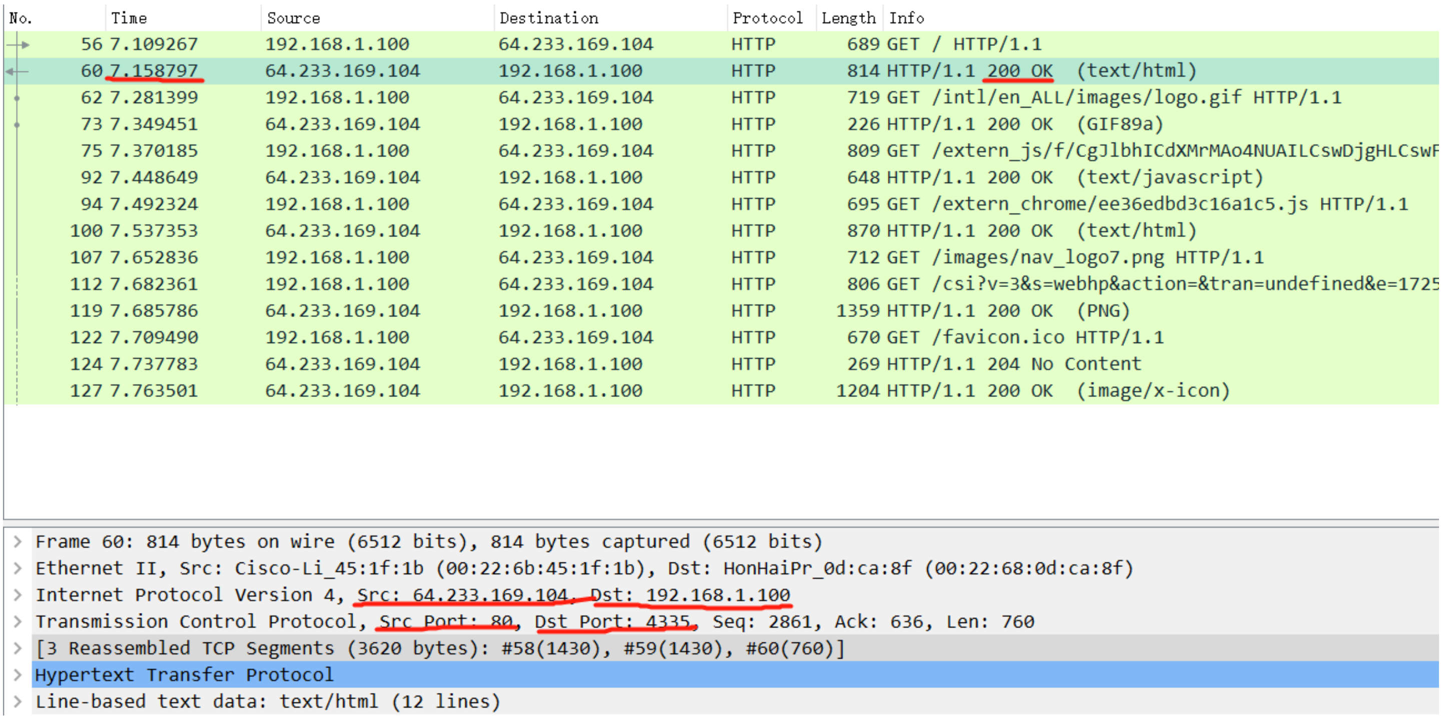
The time is 7.158797 seconds.

source IP address:64.233.169.104

source port:80

destination IP address:192.168.1.100

destination port:4335



```
No.      Time        Source           Destination      Protocol  Length Info
     56 7.109267     192.168.1.100    64.233.169.104   HTTP       689 GET / HTTP/1.1
     60 7.158797     64.233.169.104   192.168.1.100    HTTP       814 HTTP/1.1 200 OK  (text/html)
     62 7.281399     192.168.1.100    64.233.169.104   HTTP       719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
     73 7.349451     64.233.169.104   192.168.1.100    HTTP       226 HTTP/1.1 200 OK  (GIF89a)
     75 7.370185     192.168.1.100    64.233.169.104   HTTP       809 GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjgHLCswF
     92 7.448649     64.233.169.104   192.168.1.100    HTTP       648 HTTP/1.1 200 OK  (text/javascript)
     94 7.492324     192.168.1.100    64.233.169.104   HTTP       695 GET /extern_chrome/ee36edbd3c16a1c5.js HTTP/1.1
    100 7.537353     64.233.169.104   192.168.1.100    HTTP       870 HTTP/1.1 200 OK  (text/html)
    107 7.652836     192.168.1.100    64.233.169.104   HTTP       712 GET /images/nav_logo7.png HTTP/1.1
    112 7.682361     192.168.1.100    64.233.169.104   HTTP       806 GET /csi?v=3&s=webhp&action=&tran=undefined&e=1725
    119 7.685786     64.233.169.104   192.168.1.100    HTTP      1359 HTTP/1.1 200 OK  (PNG)
    122 7.709490     192.168.1.100    64.233.169.104   HTTP       670 GET /favicon.ico HTTP/1.1
    124 7.737783     64.233.169.104   192.168.1.100    HTTP       269 HTTP/1.1 204 No Content
    127 7.763501     64.233.169.104   192.168.1.100    HTTP      1204 HTTP/1.1 200 OK  (image/x-icon)

> Frame 60: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)
> Ethernet II, Src: Cisco-Li_45:1f:1b (00:22:6b:45:1f:1b), Dst: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f)
> Internet Protocol Version 4, Src: 64.233.169.104, Dst: 192.168.1.100
> Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760
> [3 Reassembled TCP Segments (3620 bytes): #58(1430), #59(1430), #60(760)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (12 lines)
```

Question 7:

Answer:

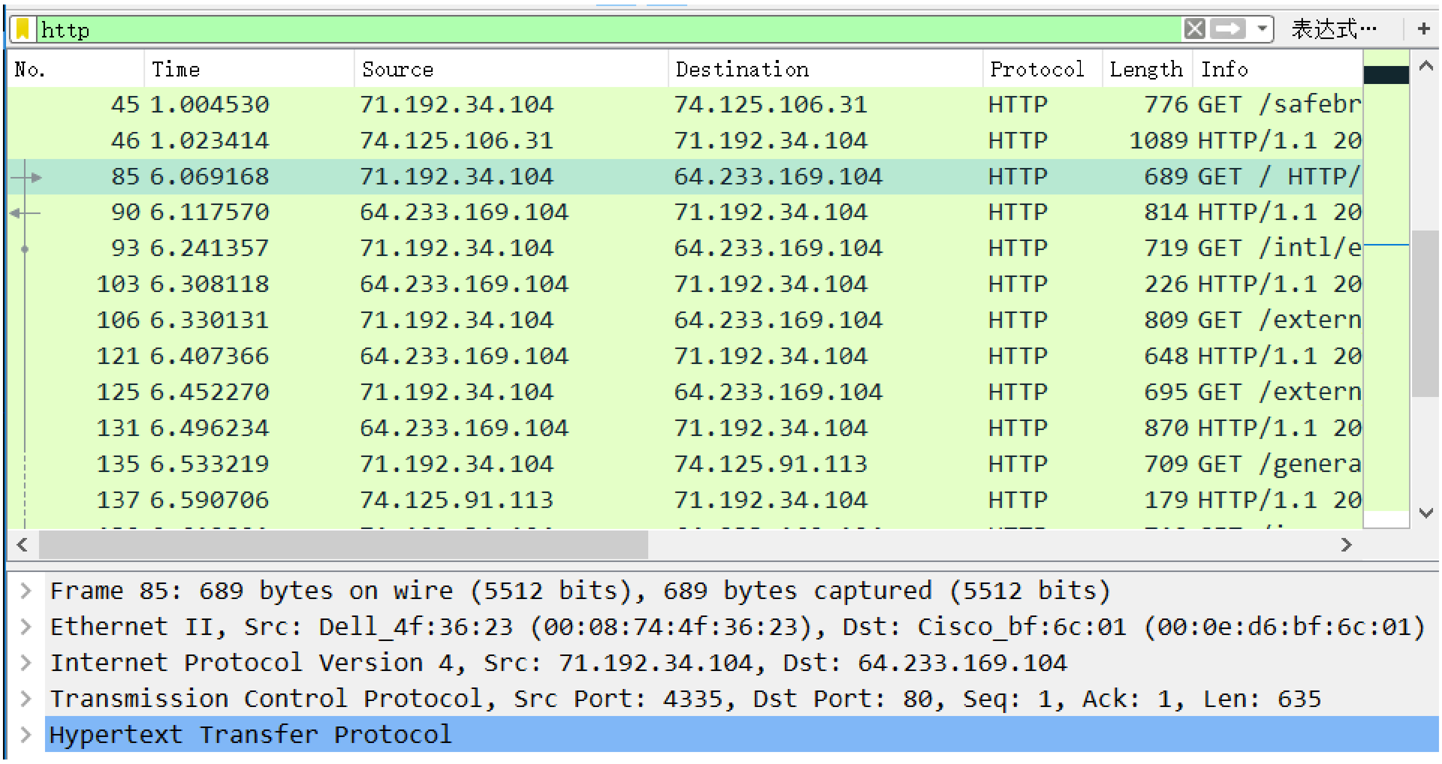
source IP: 71.192.34.104

source port: 4335

destination IP: 64.233.169.104

destination port: 80

compared with question 2， I find only source IP is different， other fields is the same.



```
http
No.   Time       Source           Destination      Protocol  Length  Info
   45 1.004530   71.192.34.104    74.125.106.31    HTTP         776 GET /safebr
   46 1.023414   74.125.106.31    71.192.34.104    HTTP        1089 HTTP/1.1 20
   85 6.069168   71.192.34.104    64.233.169.104   HTTP         689 GET / HTTP/
   90 6.117570   64.233.169.104   71.192.34.104    HTTP         814 HTTP/1.1 20
   93 6.241357   71.192.34.104    64.233.169.104   HTTP         719 GET /intl/e
  103 6.308118   64.233.169.104   71.192.34.104    HTTP         226 HTTP/1.1 20
  106 6.330131   71.192.34.104    64.233.169.104   HTTP         809 GET /extern
  121 6.407366   64.233.169.104   71.192.34.104    HTTP         648 HTTP/1.1 20
  125 6.452270   71.192.34.104    64.233.169.104   HTTP         695 GET /extern
  131 6.496234   64.233.169.104   71.192.34.104    HTTP         870 HTTP/1.1 20
  135 6.533219   71.192.34.104    74.125.91.113    HTTP         709 GET /genera
  137 6.590706   74.125.91.113    71.192.34.104    HTTP         179 HTTP/1.1 20

> Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
> Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
> Hypertext Transfer Protocol
```

Question 9:

Answer:

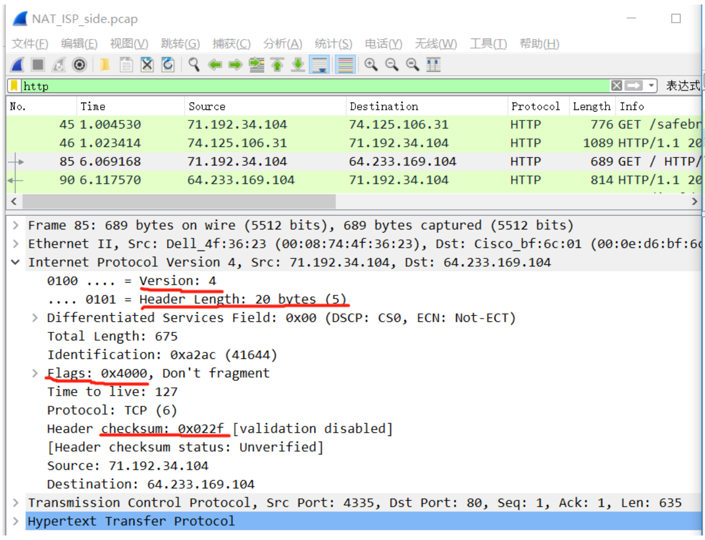
Version: Not changed

Header length: Not changed

Flags: Not changed

Checksum: changed

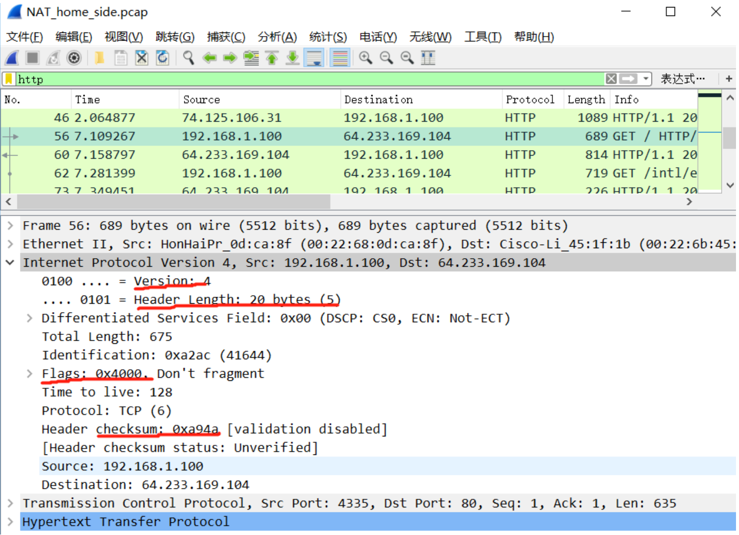
Because checksum of IP fragment is computed like that think of every two bytes of the header as a number, then summing these numbers with an inverse operation. Source IP address of IP fragment is changed， so checksum will be recomputed by NAT router. This is why checksum is changed.



NAT_ISP_side.pcap

```
http
No.   Time       Source           Destination      Protocol  Length  Info
   45 1.004530   71.192.34.104    74.125.106.31    HTTP         776 GET /safebr
   46 1.023414   74.125.106.31    71.192.34.104    HTTP        1089 HTTP/1.1 20
   85 6.069168   71.192.34.104    64.233.169.104   HTTP         689 GET / HTTP/
   90 6.117570   64.233.169.104   71.192.34.104    HTTP         814 HTTP/1.1 20

> Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c
v Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 675
    Identification: 0xa2ac (41644)
  > Flags: 0x4000, Don't fragment
    Time to live: 127
    Protocol: TCP (6)
    Header checksum: 0x022f [validation disabled]
    [Header checksum status: Unverified]
    Source: 71.192.34.104
    Destination: 64.233.169.104
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
> Hypertext Transfer Protocol
```

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式



NAT_home_side.pcap

```
http
No.   Time       Source           Destination      Protocol  Length  Info
   46 2.064877   74.125.106.31    192.168.1.100    HTTP        1089 HTTP/1.1 20
   56 7.109267   192.168.1.100    64.233.169.104   HTTP         689 GET / HTTP/
   60 7.158797   64.233.169.104   192.168.1.100    HTTP         814 HTTP/1.1 20
   62 7.281399   192.168.1.100    64.233.169.104   HTTP         719 GET /intl/e
   73 7.349451   64.233.169.104   192.168.1.100    HTTP         226 HTTP/1.1 20

> Frame 56: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
> Ethernet II, Src: HonHaiPr_0d:ca:8f (00:22:68:0d:ca:8f), Dst: Cisco-Li_45:1f:1b (00:22:6b:45:
v Internet Protocol Version 4, Src: 192.168.1.100, Dst: 64.233.169.104
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 675
    Identification: 0xa2ac (41644)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0xa94a [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.1.100
    Destination: 64.233.169.104
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 1, Ack: 1, Len: 635
> Hypertext Transfer Protocol
```

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…

Question 11:

Answer:

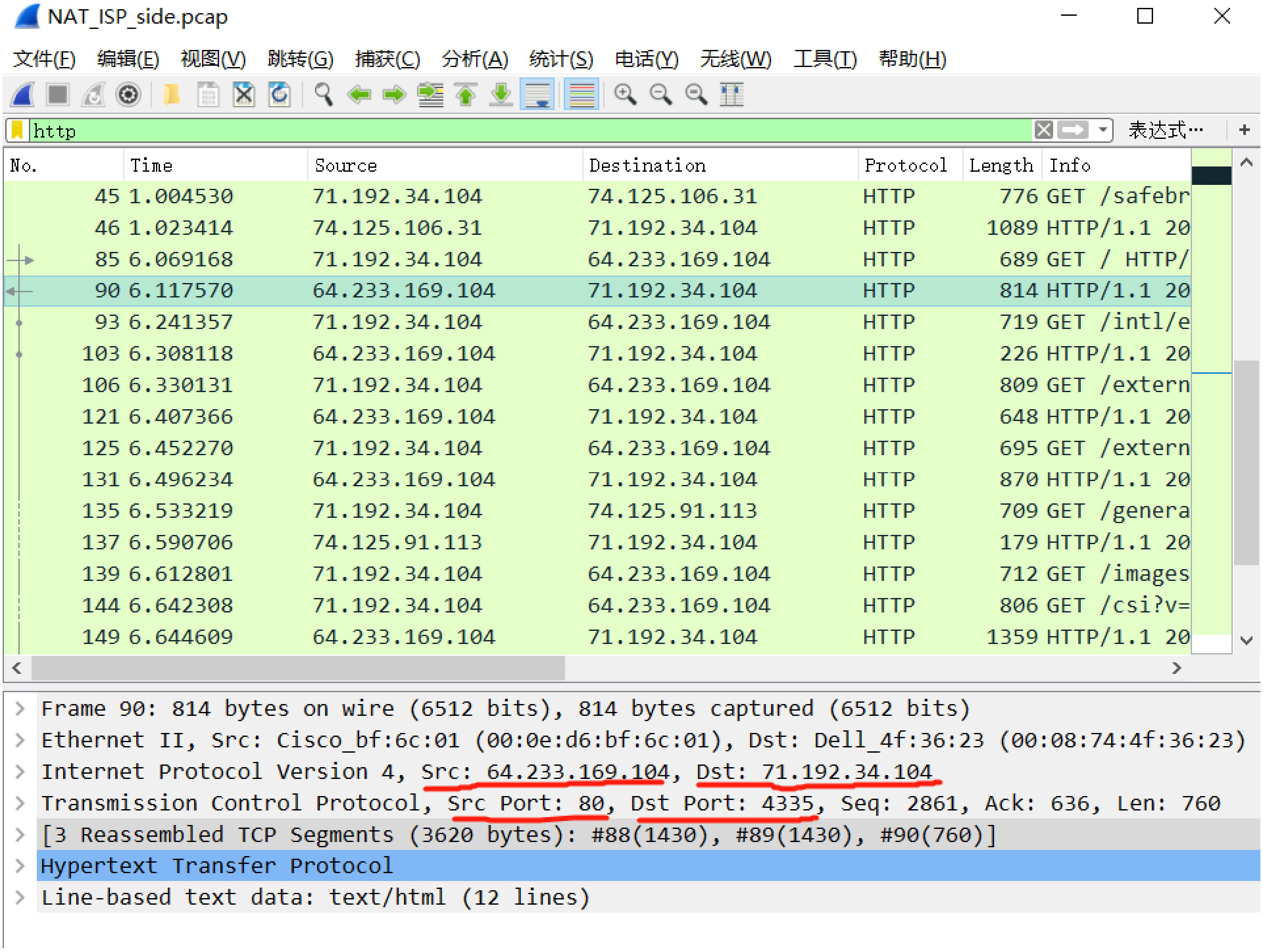
source IP address: 64.233.169.104

source port: 80

destination IP address: 71.192.34.104

destination port: 4335

Compared with question 3， I find only destination IP address is different， other fields is the same.


NAT_ISP_side.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
表达式…
+

http

```
No.    Time      Source          Destination      Protocol  Length Info
    45 1.004530  71.192.34.104   74.125.106.31    HTTP       776 GET /safebr
    46 1.023414  74.125.106.31   71.192.34.104    HTTP      1089 HTTP/1.1 20
    85 6.069168  71.192.34.104   64.233.169.104   HTTP       689 GET / HTTP/
    90 6.117570  64.233.169.104  71.192.34.104    HTTP       814 HTTP/1.1 20
    93 6.241357  71.192.34.104   64.233.169.104   HTTP       719 GET /intl/e
   103 6.308118  64.233.169.104  71.192.34.104    HTTP       226 HTTP/1.1 20
   106 6.330131  71.192.34.104   64.233.169.104   HTTP       809 GET /extern
   121 6.407366  64.233.169.104  71.192.34.104    HTTP       648 HTTP/1.1 20
   125 6.452270  71.192.34.104   64.233.169.104   HTTP       695 GET /extern
   131 6.496234  64.233.169.104  71.192.34.104    HTTP       870 HTTP/1.1 20
   135 6.533219  71.192.34.104   74.125.91.113    HTTP       709 GET /genera
   137 6.590706  74.125.91.113   71.192.34.104    HTTP       179 HTTP/1.1 20
   139 6.612801  71.192.34.104   64.233.169.104   HTTP       712 GET /images
   144 6.642308  71.192.34.104   64.233.169.104   HTTP       806 GET /csi?v=
   149 6.644609  64.233.169.104  71.192.34.104    HTTP      1359 HTTP/1.1 20
```

```
> Frame 90: 814 bytes on wire (6512 bits), 814 bytes captured (6512 bits)
> Ethernet II, Src: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01), Dst: Dell_4f:36:23 (00:08:74:4f:36:23)
> Internet Protocol Version 4, Src: 64.233.169.104, Dst: 71.192.34.104
> Transmission Control Protocol, Src Port: 80, Dst Port: 4335, Seq: 2861, Ack: 636, Len: 760
> [3 Reassembled TCP Segments (3620 bytes): #88(1430), #89(1430), #90(760)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (12 lines)
```

Question 13:

Anwer:

For TCP SYN:

source IP address: 71.192.34.104

source port: 4335

destination address: 64.233.169.104

destination port: 80

For TCP SYN/ACK:

source IP address: 64.233.169.104

source port: 80

destination address: 71.192.34.104

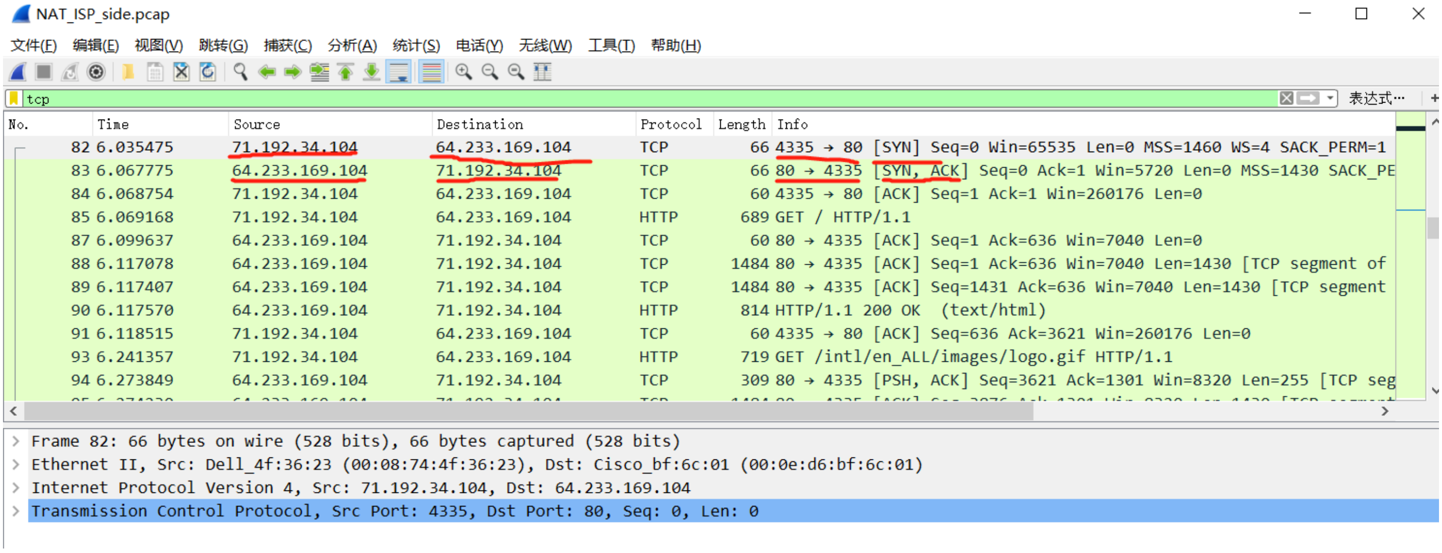
destination port: 4335

Difference:

For the SYN， source IP address is changed， and

For SYN/ACK， destination IP address is changed.

But the port numbers are unchanged.


NAT_ISP_side.pcap
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
tcp
表达式…

```
No.      Time      Source           Destination      Protocol  Length Info
      82 6.035475  71.192.34.104    64.233.169.104   TCP         66 4335 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 SACK_PERM=1
      83 6.067775  64.233.169.104   71.192.34.104    TCP         66 80 → 4335 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430 SACK_PE
      84 6.068754  71.192.34.104    64.233.169.104   TCP         60 4335 → 80 [ACK] Seq=1 Ack=1 Win=260176 Len=0
      85 6.069168  71.192.34.104    64.233.169.104   HTTP       689 GET / HTTP/1.1
      87 6.099637  64.233.169.104   71.192.34.104    TCP         60 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=0
      88 6.117078  64.233.169.104   71.192.34.104    TCP       1484 80 → 4335 [ACK] Seq=1 Ack=636 Win=7040 Len=1430 [TCP segment of
      89 6.117407  64.233.169.104   71.192.34.104    TCP       1484 80 → 4335 [ACK] Seq=1431 Ack=636 Win=7040 Len=1430 [TCP segment
      90 6.117570  64.233.169.104   71.192.34.104    HTTP       814 HTTP/1.1 200 OK  (text/html)
      91 6.118515  71.192.34.104    64.233.169.104   TCP         60 4335 → 80 [ACK] Seq=636 Ack=3621 Win=260176 Len=0
      93 6.241357  71.192.34.104    64.233.169.104   HTTP       719 GET /intl/en_ALL/images/logo.gif HTTP/1.1
      94 6.273849  64.233.169.104   71.192.34.104    TCP        309 80 → 4335 [PSH, ACK] Seq=3621 Ack=1301 Win=8320 Len=255 [TCP seg
```

```
> Frame 82: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
> Ethernet II, Src: Dell_4f:36:23 (00:08:74:4f:36:23), Dst: Cisco_bf:6c:01 (00:0e:d6:bf:6c:01)
> Internet Protocol Version 4, Src: 71.192.34.104, Dst: 64.233.169.104
> Transmission Control Protocol, Src Port: 4335, Dst Port: 80, Seq: 0, Len: 0
```

Question 14:

Answer:

NAT translation table is as below:

WAN side	LAN side
71.192.34.104， 4335	192.168.1.100， 4335

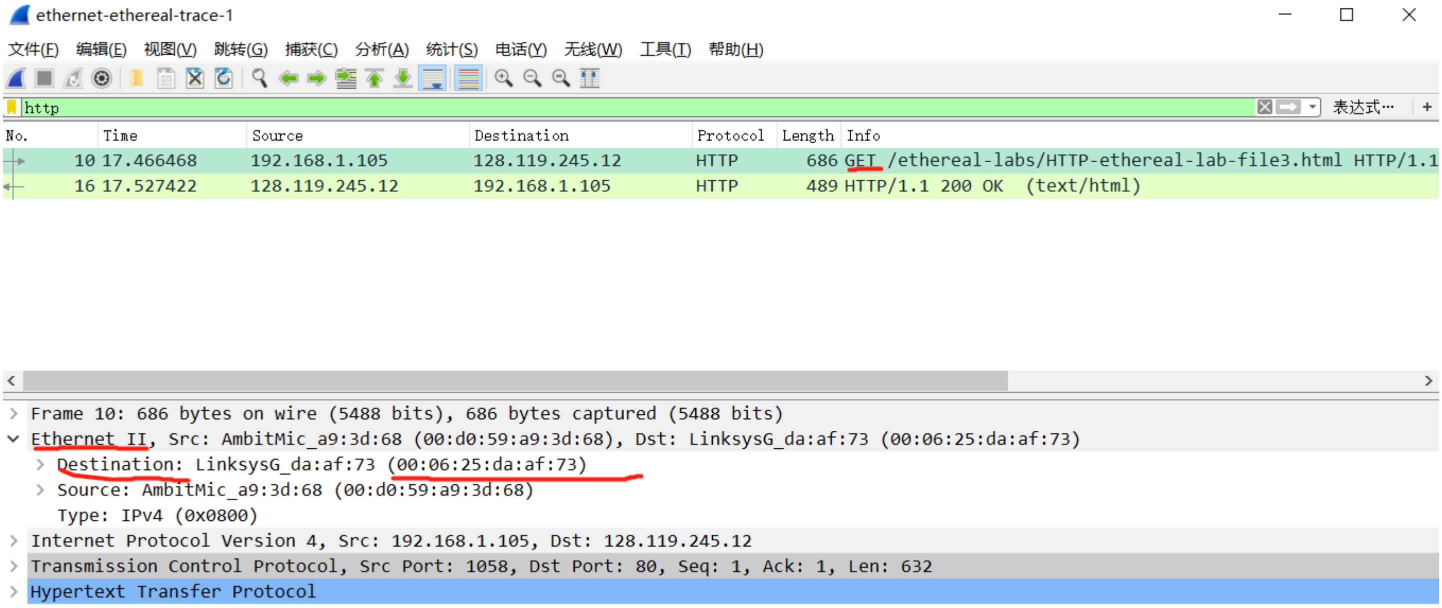
Exercise 3: Using Wireshark to understand Ethernet

Question 2:

Answer:

As the graph show below， the 48-bits destination address in the Ethernet frame is 00:06:25:da:af:73.

The source host and destination are not belong to same subnet， so the Ethernet address is not Ethernet address of gaia.cs.unmass.edu. It should be the MAC address of the first hop router on the source address to destination address path.


ethernet-ethereal-trace-1
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
http
表达式…

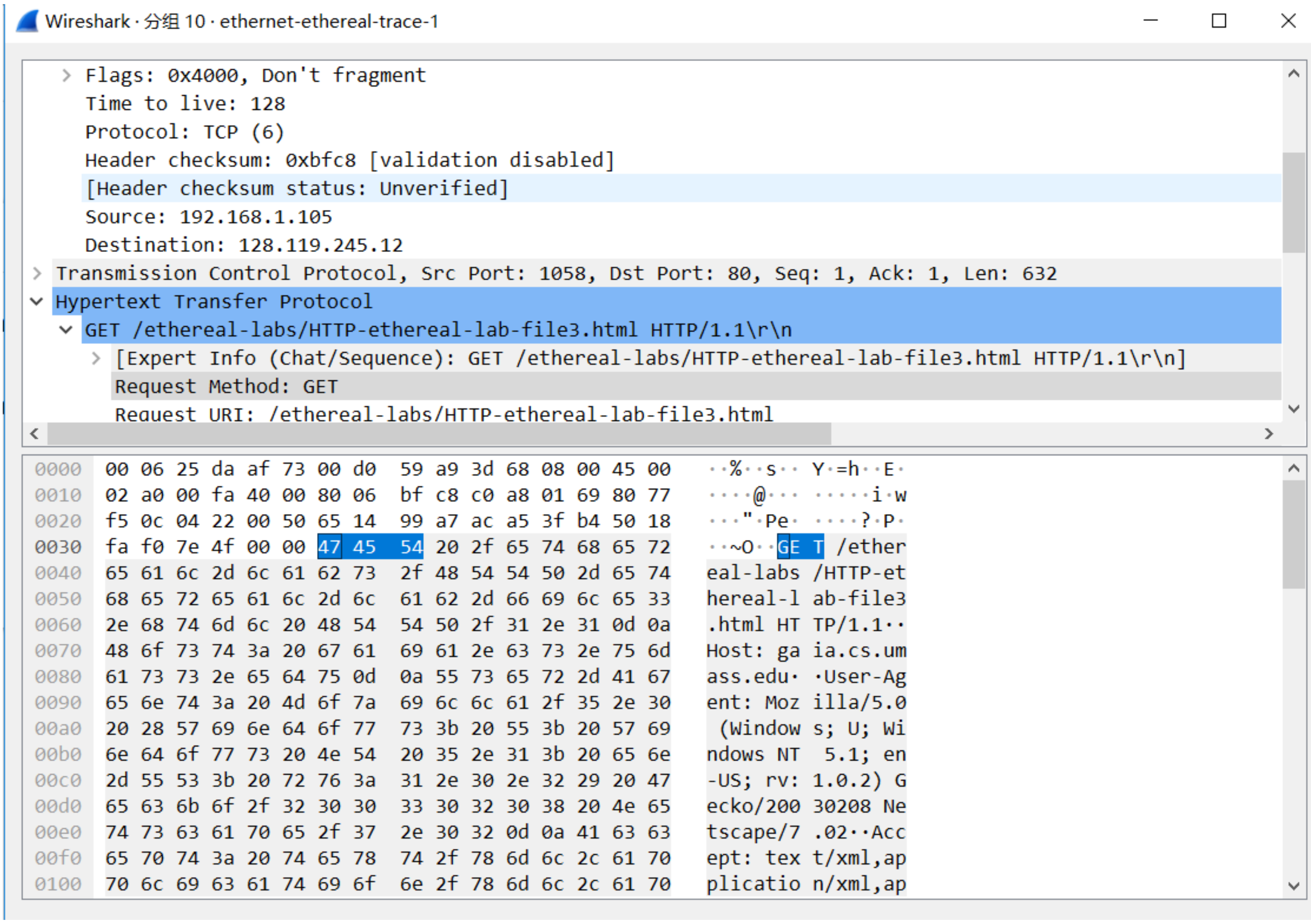
```
No.      Time       Source          Destination     Protocol  Length Info
      10 17.466468  192.168.1.105   128.119.245.12  HTTP        686 GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
      16 17.527422  128.119.245.12  192.168.1.105   HTTP        489 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
v Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
  > 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)
> 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
> Hypertext Transfer Protocol
```

Question 4:

Answer:

As the frame show below， G of GET appears at 54 bytes after the start of the frame. The preamble bytes are not captured by wireshark. The first 14 bytes represent the Ethernet frame header， and the next 20 bytes represent IP header. The 20 bytes following represent TCP header.



Wireshark · 分组 10 · ethernet-ethereal-trace-1

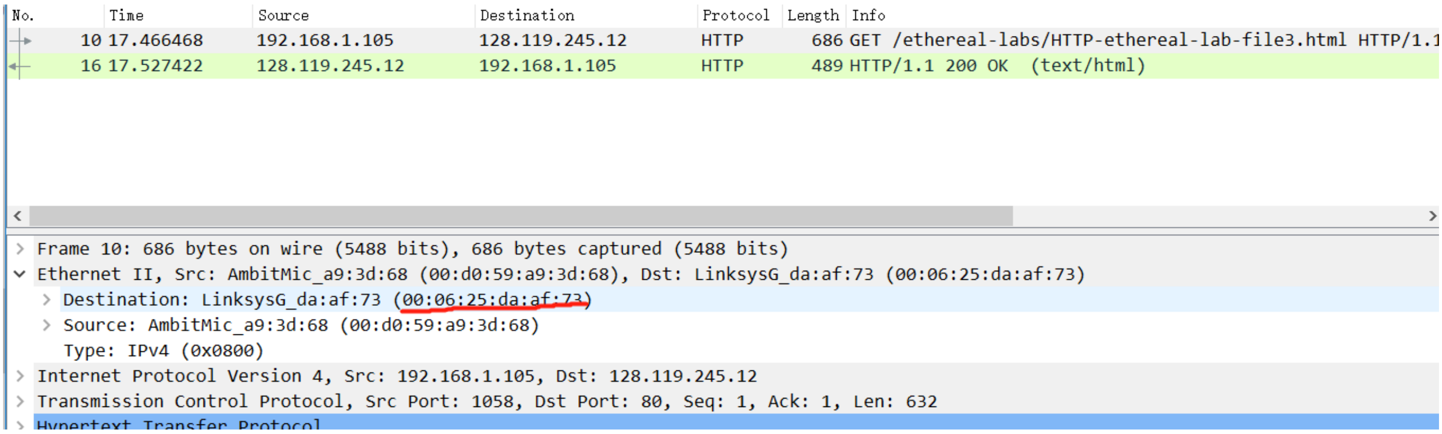
```
    > Flags: 0x4000, Don't fragment
      Time to live: 128
      Protocol: TCP (6)
      Header checksum: 0xbfc8 [validation disabled]
      [Header checksum status: Unverified]
      Source: 192.168.1.105
      Destination: 128.119.245.12
> Transmission Control Protocol, Src Port: 1058, Dst Port: 80, Seq: 1, Ack: 1, Len: 632
v Hypertext Transfer Protocol
  v GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n
    > [Expert Info (Chat/Sequence): GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1\r\n]
      Request Method: GET
      Request URI: /ethereal-labs/HTTP-ethereal-lab-file3.html
```

```
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
0060  2e 68 74 6d 6c 20 48 54  54 50 2f 31 2e 31 0d 0a   .html HT TP/1.1··
0070  48 6f 73 74 3a 20 67 61  69 61 2e 63 73 2e 75 6d   Host: ga ia.cs.um
0080  61 73 73 2e 65 64 75 0d  0a 55 73 65 72 2d 41 67   ass.edu· ·User-Ag
0090  65 6e 74 3a 20 4d 6f 7a  69 6c 6c 61 2f 35 2e 30   ent: Moz illa/5.0
00a0  20 28 57 69 6e 64 6f 77  73 3b 20 55 3b 20 57 69    (Window s; U; Wi
00b0  6e 64 6f 77 73 20 4e 54  20 35 2e 31 3b 20 65 6e   ndows NT  5.1; en
00c0  2d 55 53 3b 20 72 76 3a  31 2e 30 2e 32 29 20 47   -US; rv: 1.0.2) G
00d0  65 63 6b 6f 2f 32 30 30  33 30 32 30 38 20 4e 65   ecko/200 30208 Ne
00e0  74 73 63 61 70 65 2f 37  2e 30 32 0d 0a 41 63 63   tscape/7 .02··Acc
00f0  65 70 74 3a 20 74 65 78  74 2f 78 6d 6c 2c 61 70   ept: tex t/xml,ap
0100  70 6c 69 63 61 74 69 6f  6e 2f 78 6d 6c 2c 61 70   plicatio n/xml,ap
```

Question 5:

Answer:

As the graph show below， the source Ethernet address is 00:06:25:da:af:73. This address is neither the host that send the GET HTTP request， nor the gaia.cs.umass.edu. This address refers to the MAC address of the first-hop router on the path from source host to gaia.cs.umass.edu.



```
No.    Time         Source          Destination     Protocol Length Info
    10 17.466468    192.168.1.105   128.119.245.12  HTTP        686 GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
    16 17.527422    128.119.245.12  192.168.1.105   HTTP        489 HTTP/1.1 200 OK  (text/html)
```

```
> Frame 10: 686 bytes on wire (5488 bits), 686 bytes captured (5488 bits)
v Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
  > 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)
> 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
> Hypertext Transfer Protocol
```

Exercise 4: Using Wireshark to understand ARP

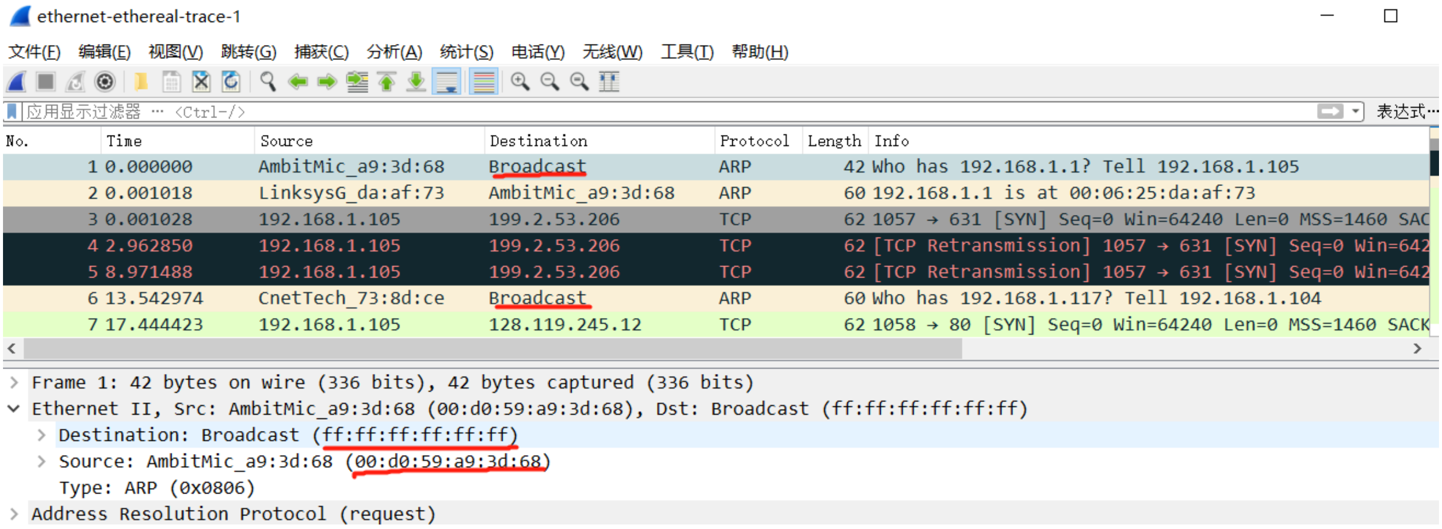
Question 1:

Answer:

source address: 00:d0:59:a9:3d:68

destination address: ff:ff:ff:ff:ff:ff

destiniation adress is used to broadcast， every host in this subnet will process this message.


ethernet-ethereal-trace-1
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
表达式…

```
No.   Time        Source              Destination         Protocol  Length  Info
  1 0.000000    AmbitMic_a9:3d:68   Broadcast           ARP       42 Who has 192.168.1.1? Tell 192.168.1.105
  2 0.001018    LinksysG_da:af:73   AmbitMic_a9:3d:68   ARP       60 192.168.1.1 is at 00:06:25:da:af:73
  3 0.001028    192.168.1.105       199.2.53.206        TCP       62 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SAC
  4 2.962850    192.168.1.105       199.2.53.206        TCP       62 [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=642
  5 8.971488    192.168.1.105       199.2.53.206        TCP       62 [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=642
  6 13.542974   CnetTech_73:8d:ce   Broadcast           ARP       60 Who has 192.168.1.117? Tell 192.168.1.104
  7 17.444423   192.168.1.105       128.119.245.12      TCP       62 1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK

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

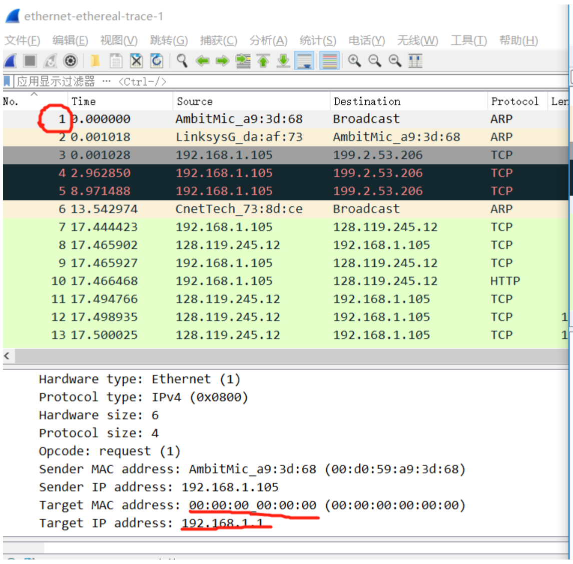
Question 6:

Answer:

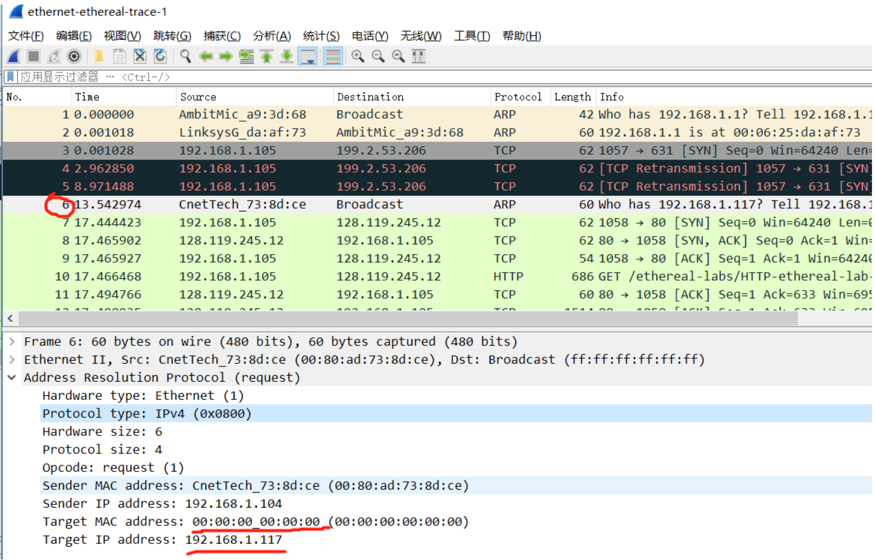
As the graph show below， there are two ARP requests.

we can see that IP address which want to request is fill in the target IP address，

and the MAC address is left blank(00:00:00:00:00:00).


ethernet-ethereal-trace-1
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.   Time        Source              Destination         Protocol  Len
  1 0.000000    AmbitMic_a9:3d:68   Broadcast           ARP
  2 0.001018    LinksysG_da:af:73   AmbitMic_a9:3d:68   ARP
  3 0.001028    192.168.1.105       199.2.53.206        TCP
  4 2.962850    192.168.1.105       199.2.53.206        TCP
  5 8.971488    192.168.1.105       199.2.53.206        TCP
  6 13.542974   CnetTech_73:8d:ce   Broadcast           ARP
  7 17.444423   192.168.1.105       128.119.245.12      TCP
  8 17.465902   128.119.245.12      192.168.1.105       TCP
  9 17.465927   192.168.1.105       128.119.245.12      TCP
 10 17.466468   192.168.1.105       128.119.245.12      HTTP
 11 17.494766   128.119.245.12      192.168.1.105       TCP
 12 17.498935   128.119.245.12      192.168.1.105       TCP       1
 13 17.500025   128.119.245.12      192.168.1.105       TCP       1

    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
```

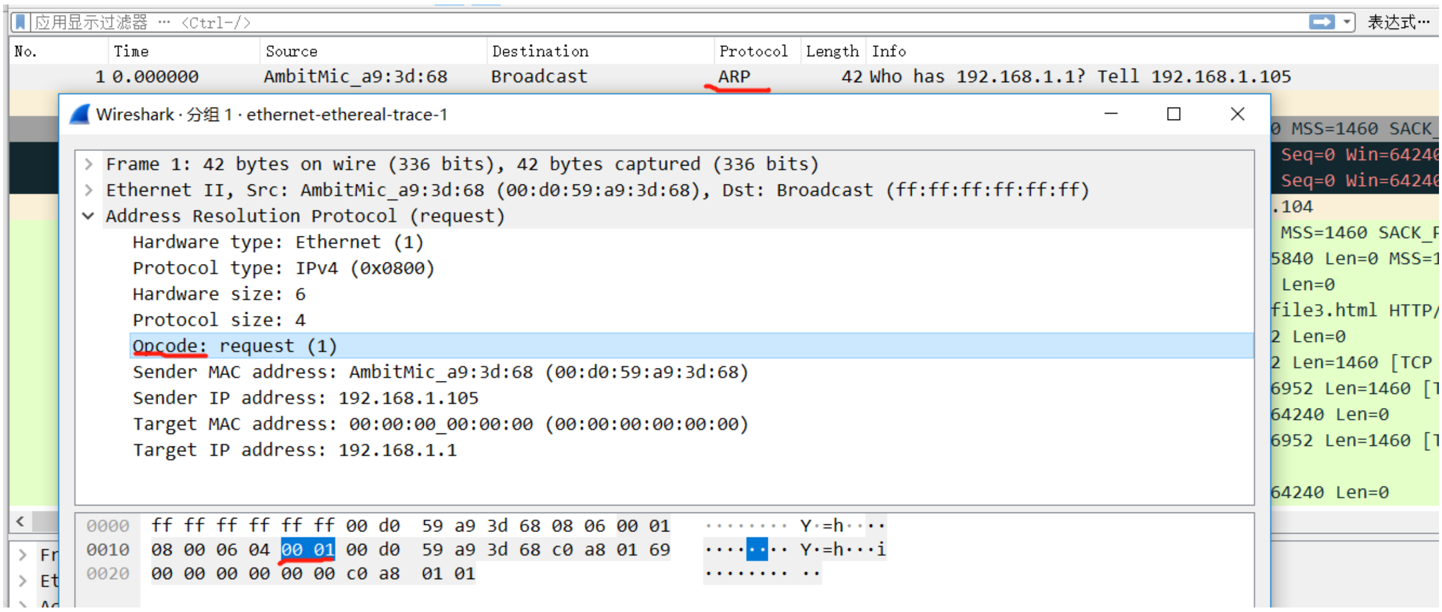

ethernet-ethereal-trace-1
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>

```
No.   Time        Source              Destination         Protocol  Length  Info
  1 0.000000    AmbitMic_a9:3d:68   Broadcast           ARP       42 Who has 192.168.1.1? Tell 192.168.1.1
  2 0.001018    LinksysG_da:af:73   AmbitMic_a9:3d:68   ARP       60 192.168.1.1 is at 00:06:25:da:af:73
  3 0.001028    192.168.1.105       199.2.53.206        TCP       62 1057 → 631 [SYN] Seq=0 Win=64240 Len=
  4 2.962850    192.168.1.105       199.2.53.206        TCP       62 [TCP Retransmission] 1057 → 631 [SYN]
  5 8.971488    192.168.1.105       199.2.53.206        TCP       62 [TCP Retransmission] 1057 → 631 [SYN]
  6 13.542974   CnetTech_73:8d:ce   Broadcast           ARP       60 Who has 192.168.1.117? Tell 192.168.1
  7 17.444423   192.168.1.105       128.119.245.12      TCP       62 1058 → 80 [SYN] Seq=0 Win=64240 Len=0
  8 17.465902   128.119.245.12      192.168.1.105       TCP       62 80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=
  9 17.465927   192.168.1.105       128.119.245.12      TCP       54 1058 → 80 [ACK] Seq=1 Ack=1 Win=64240
 10 17.466468   192.168.1.105       128.119.245.12      HTTP     686 GET /ethereal-labs/HTTP-ethereal-lab-
 11 17.494766   128.119.245.12      192.168.1.105       TCP       60 80 → 1058 [ACK] Seq=1 Ack=633 Win=695

> Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: CnetTech_73:8d:ce (00:80:ad:73:8d:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
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: 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
```

Question 7:

Answer:

20 bytes from the very beginning of the Ethernet frame does the ARP opcode field begin.



```
No.   Time        Source              Destination   Protocol Length Info
    1 0.000000    AmbitMic_a9:3d:68   Broadcast     ARP         42 Who has 192.168.1.1? Tell 192.168.1.105
```

Wireshark · 分组 1 · ethernet-ethereal-trace-1

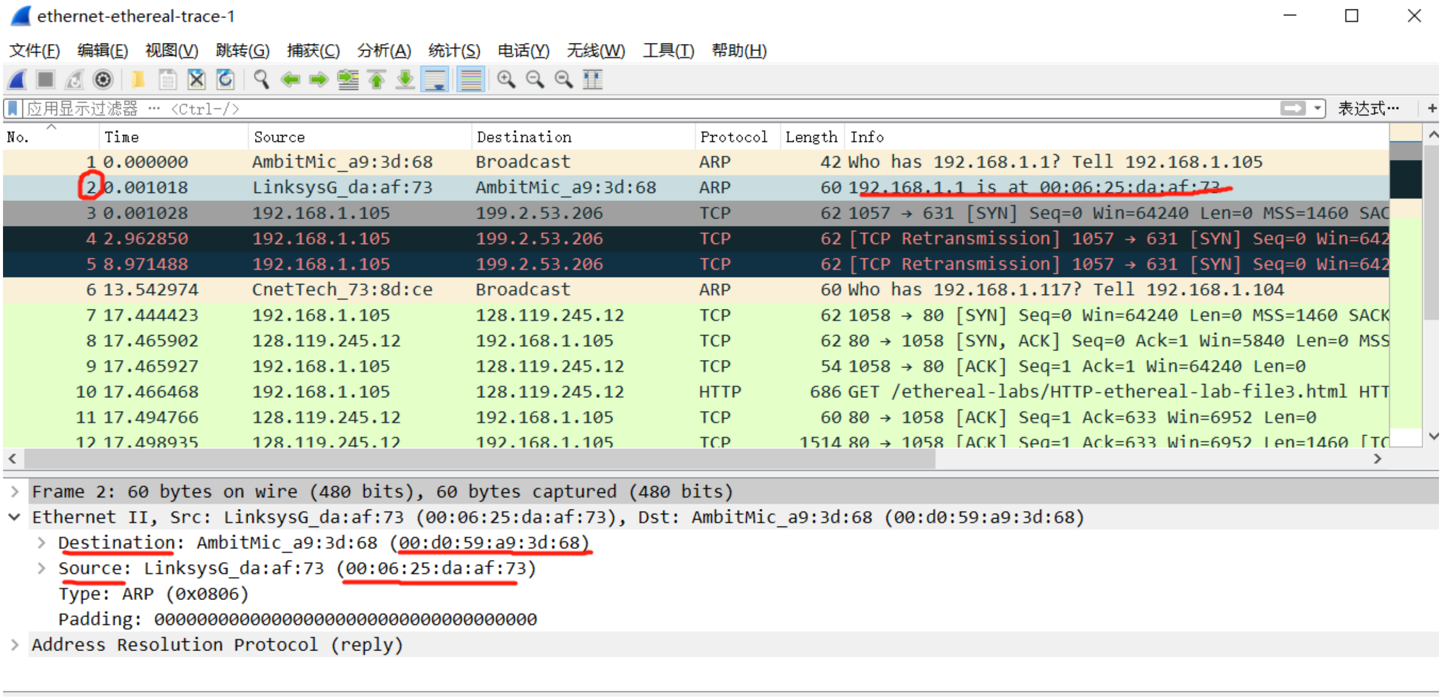
```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 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

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                     ········ ··
```

Question 10:

Answer:

As the graph below， the source address is 00:06:25:da:af:73，

the destination address is 00:d0:59:a9:3d:68.



ethernet-ethereal-trace-1

```
No.   Time        Source              Destination       Protocol Length Info
    1 0.000000    AmbitMic_a9:3d:68   Broadcast         ARP         42 Who has 192.168.1.1? Tell 192.168.1.105
    2 0.001018    LinksysG_da:af:73   AmbitMic_a9:3d:68 ARP         60 192.168.1.1 is at 00:06:25:da:af:73
    3 0.001028    192.168.1.105       199.2.53.206      TCP         62 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SAC
    4 2.962850    192.168.1.105       199.2.53.206      TCP         62 [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=642
    5 8.971488    192.168.1.105       199.2.53.206      TCP         62 [TCP Retransmission] 1057 → 631 [SYN] Seq=0 Win=642
    6 13.542974   CnetTech_73:8d:ce   Broadcast         ARP         60 Who has 192.168.1.117? Tell 192.168.1.104
    7 17.444423   192.168.1.105       128.119.245.12    TCP         62 1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
    8 17.465902   128.119.245.12      192.168.1.105     TCP         62 80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS
    9 17.465927   192.168.1.105       128.119.245.12    TCP         54 1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
   10 17.466468   192.168.1.105       128.119.245.12    HTTP       686 GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTT
   11 17.494766   128.119.245.12      192.168.1.105     TCP         60 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
   12 17.498935   128.119.245.12      192.168.1.105     TCP       1514 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [TC

> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 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: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
> Address Resolution Protocol (reply)
```