Lab 7

1. IP Addressing, NAT

1. **Your job is to help Elliot assign addresses to the subnets, routers and NAT box inside his house. Use addresses from the 10.x block. Complete the following tables:**

Subnet	Number	Netmask
Subnet 1	10.0.1.0	255.2555.255.0
Subnet 2	10.0.2.0	255.2555.255.0
Subnet 3	10.0.3.0	255.2555.255.0

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

The broadcast address (10.255.255.255) and the subnet address (10.0.0.0) are not assigned to interfaces.

Question 2. Assuming that the NAT box has no special support for any protocols, and merely translates TCP and IP ports and addresses, give an example of an application that would not work through this NAT, and very briefly explain why.

Any protocol using TCP/IP later information in the application stream would most likely be broken by a basic NAT.

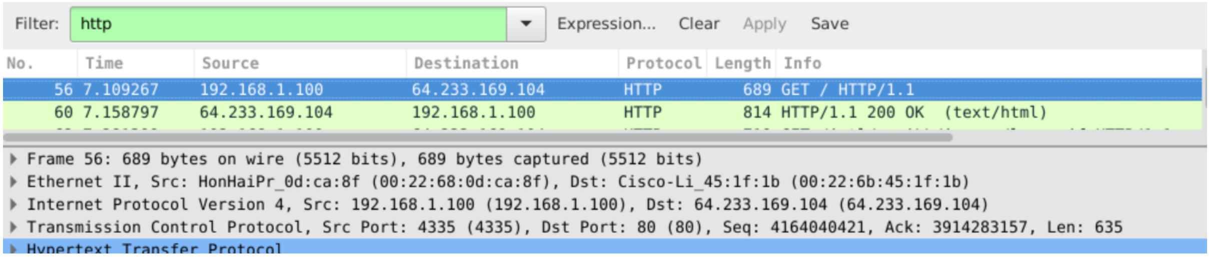
FTP would not work through the NAPT. This is because the server would need to open a connection back to the client.

However, this is not the case for passive mode FTP, as it has the client open the connection.

2. Understanding NAT using Wireshark

Question 1: Consider now the HTTP GET sent from the client to the Google server (whose IP address is IP address 64.233.169.104) at time 7.109267. What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET?

- Source IP: 192.168.1.100, Port = 4335
- Destination IP: 64.233.169.104, Port = 80



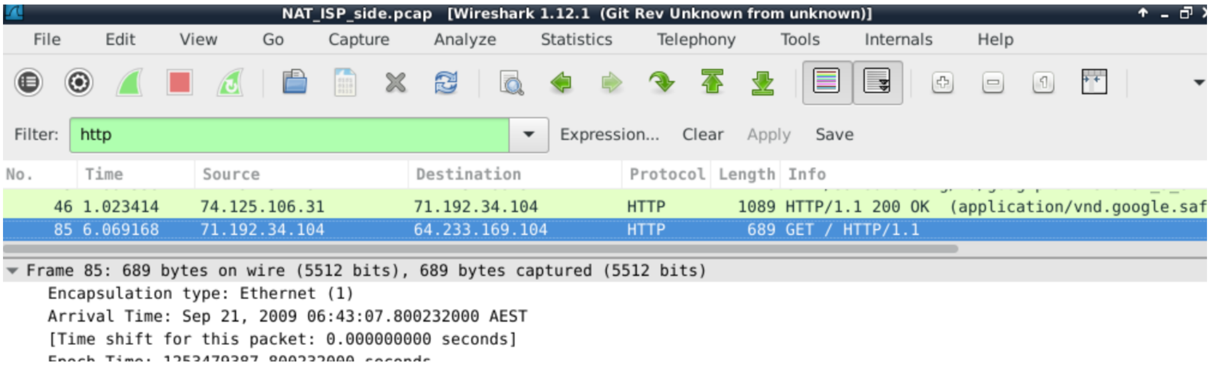
```
No.   Time        Source            Destination       Protocol Length Info
   56 7.109267    192.168.1.100     64.233.169.104    HTTP        689 GET / HTTP/1.1
   60 7.158797    64.233.169.104    192.168.1.100     HTTP        814 HTTP/1.1 200 OK  (text/html)

▸ 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 (192.168.1.100), Dst: 64.233.169.104 (64.233.169.104)
▸ Transmission Control Protocol, Src Port: 4335 (4335), Dst Port: 80 (80), Seq: 4164040421, Ack: 3914283157, Len: 635
▸ Hypertext Transfer Protocol
```

Question 2: At what time is the corresponding 200 OK HTTP message received from the Google server? What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message?

- Time: 7.158797
- Source IP: 64.233.169.104, Port = 80
- Destination IP: 192.168.1.100, Port = 4335

(As seen in the figure above)

Question 3: What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP GET message (as recorded in the NAT_ISP_side trace file)? Which of these fields are the same, and which are different, than in your answer to Question 2 above?



```
No.   Time        Source            Destination       Protocol Length Info
   46 1.023414    74.125.106.31     71.192.34.104     HTTP       1089 HTTP/1.1 200 OK  (application/vnd.google.saf
   85 6.069168    71.192.34.104     64.233.169.104    HTTP        689 GET / HTTP/1.1

▾ Frame 85: 689 bytes on wire (5512 bits), 689 bytes captured (5512 bits)
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 21, 2009 06:43:07.800232000 AEST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1253479387.800232000 seconds
```

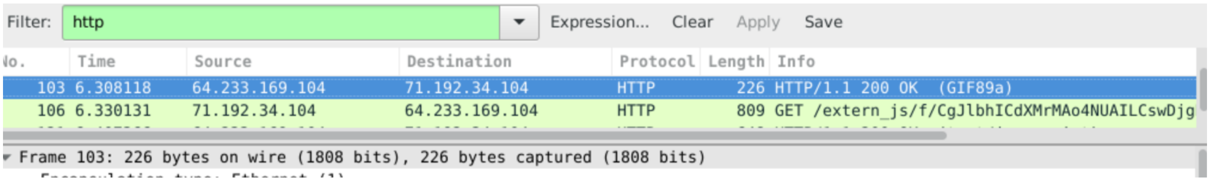
- Source IP: 71.192.34.104, Port = 4335
- Destination IP: 64.233.169.104, Port = 80

Source IP in Question 2 was 192.168.1.100, but it is now 71.192.34.104.

Question 4: Which of the following fields in the IP datagram carrying the HTTP GET are changed: Version, Header Length, Flags, Checksum. If any of these fields have changed, give a reason (in one sentence) stating why this field needed to change

- Version: NO
- Header Length: NO
- Flags: NO
- Checksum: Yes, changed from 0xa94a -> 0x4576
  The change in the IP address of the source IP address field will cause a change in the checksum, which is what has happened

Question 5: What are the source and destination IP addresses and TCP source and destination ports on the IP datagram carrying this HTTP 200 OK message? Which of these fields are the same, and which are different than your answer to Question 3 above?



```
No.  Time      Source          Destination     Protocol Length Info
 103 6.308118  64.233.169.104  71.192.34.104   HTTP        226 HTTP/1.1 200 OK  (GIF89a)
 106 6.330131  71.192.34.104   64.233.169.104  HTTP        809 GET /extern_js/f/CgJlbhICdXMrMAo4NUAILCswDjg
▾ Frame 103: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
```

- Source IP: 64.233.169.104,   Port = 80

- Destination IP: 71.192.34.104,   Port = 4335

- The source and destination IPs have swapped

Question 6: What are the source and destination IP addresses and source and destination ports for these two segments (TCP SYN and TCP SYN/ACK)? Which of these fields are the same, and which are different than your answer to Question 4 and 5 above?

- SYN Source IP =   71.192.34.104,   Port = 4335
- SYN Destination IP = 64.233.169.104   Port = 80
- ACK Source IP =   64.233.169.104   Port = 80
- ACK Destination IP = 71.192.34.104,   Port = 4335

For SYN: Source IP different

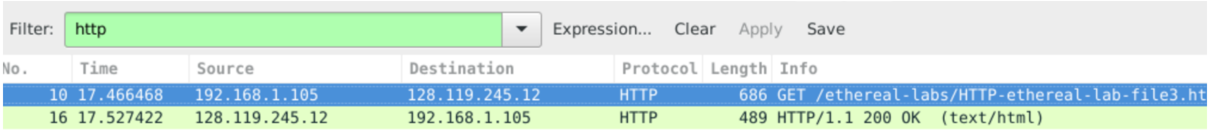
For ACK: Destination IP address different

Question 7: The discussion on NAT in the Week 8 lecture slides shows the NAT translation table used by a NAT router. Using your answers to the questions above, fill in the NAT translation table entries for the HTTP connection considered in the questions above.

WAN Side Address	LAN Side Address
71.192.34.104 | 4335	192.168.100 | 4335

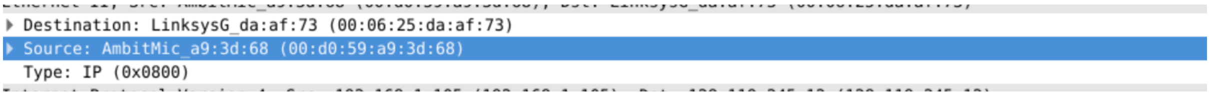
3. Using Wireshark to understand Ethernet

Question 1: What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? If not, then which device has this address? (Note: this is an important question, and one that students sometimes get wrong. You may want to refer back to relevant parts of the text and lecture notes and make sure you understand the answer here.)



Filter: http

```
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.ht
   16 17.527422  128.119.245.12  192.168.1.105   HTTP        489 HTTP/1.1 200 OK  (text/html)
```



```
▸ Destination: LinksysG_da:af:73 (00:06:25:da:af:73)
▸ Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  Type: IP (0x0800)
```

<u>The screenshot is given above for reference</u>

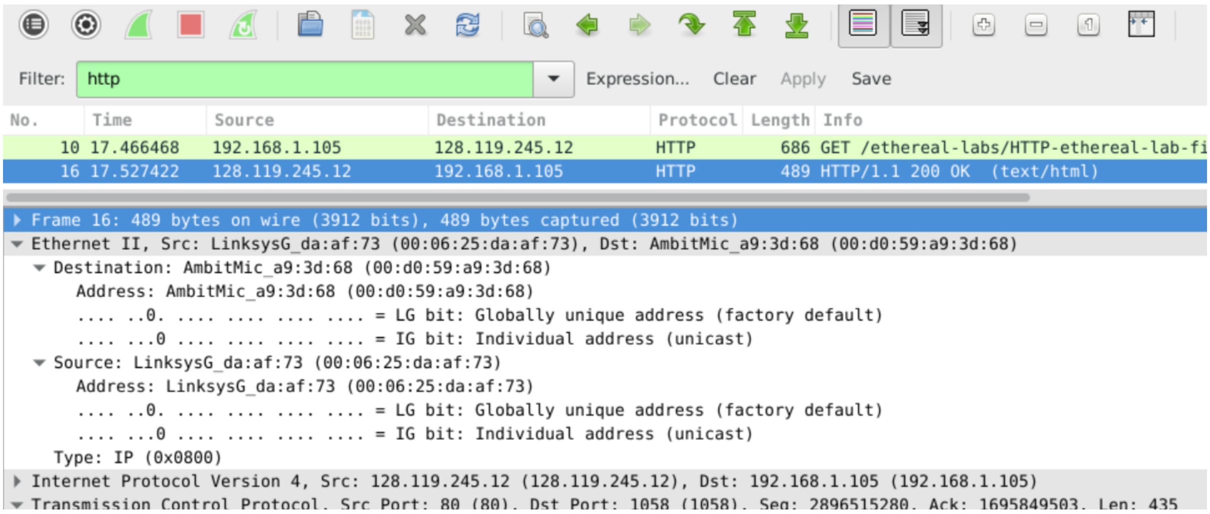
The destination address is 00:06:25:da:af:73 is not the Ethernet address of gaia.cs.umass.edu. It is the Ethernet address of a link called LinksysG, which is a router.

Question 3: How many bytes from the very start of the Ethernet frame does the ASCII "G" in "GET" appear in the Ethernet frame? Note that when you examine the Data portion of this frame, it actually consists of both the Ethernet frame headers as well as the payload (i.e. bottom window in Wireshark shows the entire 686 byte frame that is captured).

The ASCII "G" appears in the position 0x36. This is 54 bytes from the start of the Ethernet frame.

Of the bytes preceding the G, the first few bytes are the Ethernet frame header. Does this include the preamble bytes, or are those bytes omitted from the capture? Given this, how many bytes of frame header are present? What are the remainder of the bytes before the G?

- The Ethernet frame omits the preamble bytes from the capture
- Given this, there are a total of 14 bytes present in the Ethernet frame header.
- The remainder bytes before G are the IP and TCP layers with 20 bytes respectively. This makes a total of 20+20 bytes



Filter: http

```
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-fi
   16 17.527422  128.119.245.12  192.168.1.105   HTTP        489 HTTP/1.1 200 OK  (text/html)

▶ Frame 16: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
▼ 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)
      Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▼ Source: LinksysG_da:af:73 (00:06:25:da:af:73)
      Address: LinksysG_da:af:73 (00:06:25:da:af:73)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IP (0x0800)
▶ Internet Protocol Version 4, Src: 128.119.245.12 (128.119.245.12), Dst: 192.168.1.105 (192.168.1.105)
▼ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 1058 (1058), Seq: 2896515280, Ack: 1695849503, Len: 435
```

The screenshot is given as a reference

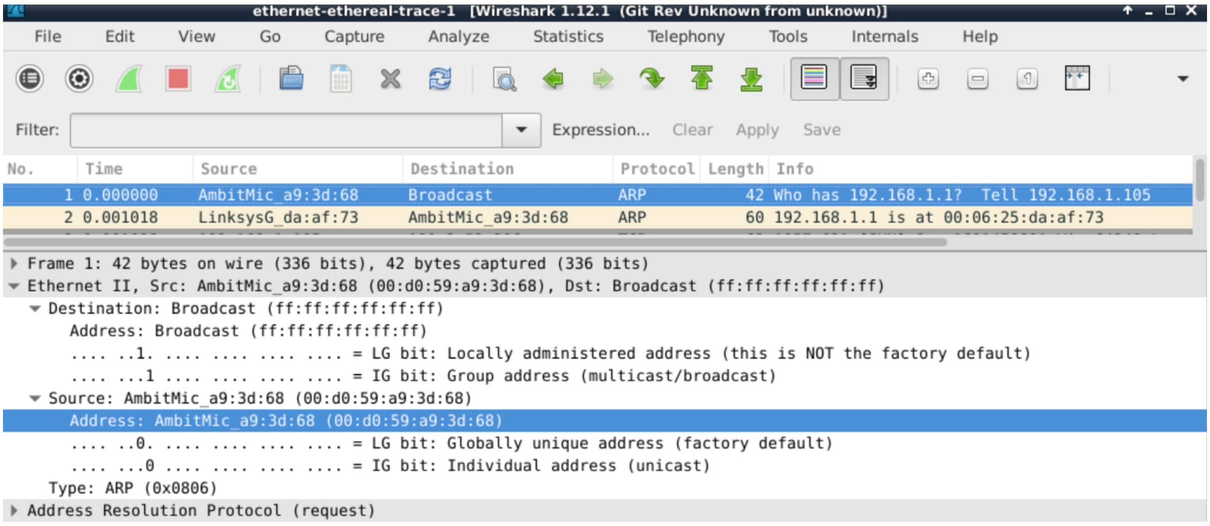
Question 3: What is the value of the Ethernet source address? Is this the address of the host that sent the GET HTTP request, or of gaia.cs.umass.edu? If not then which device has this address?

The source address 00:06:25:da:af:73 is neither the Ethernet address of gaia.cs.umass.edu nor the address of the host that sent the GET request.

It is the address of the Linksys router (LinksysG), which is the link used to get onto my subnet.

4. Using Wireshark to understand ARP

Question 1: What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message? Is there something special about the destination address?



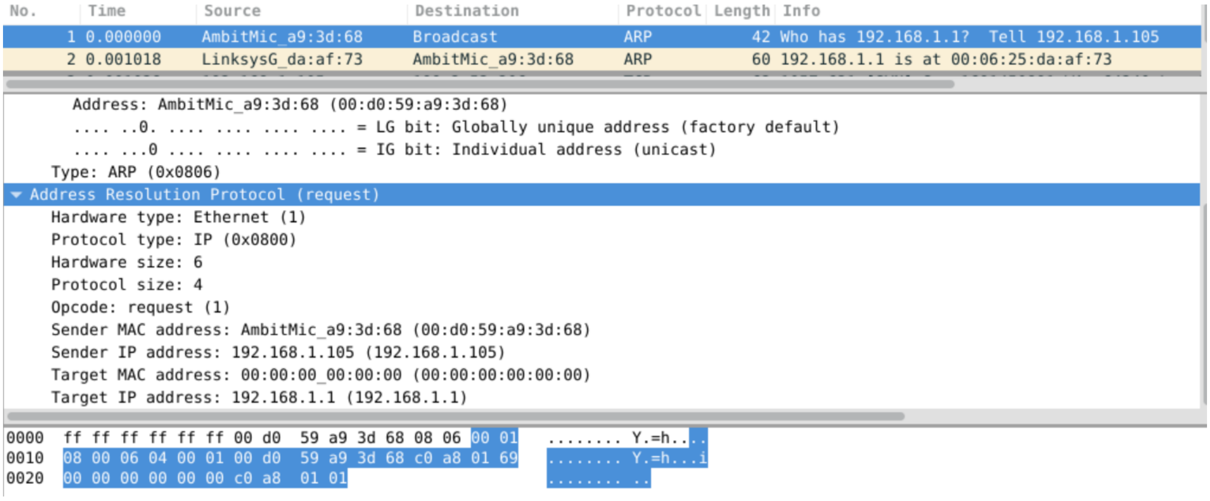
```
No.   Time       Source             Destination        Protocol Length Info
    1 0.000000   AmbitMic_a9:3d:68  Broadcast          ARP          42 Who has 192.168.1.1?  Tell 192.168.1.105
    2 0.001018   LinksysG_da:af:73  AmbitMic_a9:3d:68  ARP          60 192.168.1.1 is at 00:06:25:da:af:73

▸ 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)
  ▾ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
      Address: 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)
  ▾ Source: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
      Address: AmbitMic_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)
▸ Address Resolution Protocol (request)
```

<u>The screenshot is given as a reference</u>

The hex value for the source address is 00:d0:59:a9:3d:68.

The hex value for the destination address is ff:ff:ff:ff:ff:ff is the broadcast address, which is sent to all hosts on the given network.

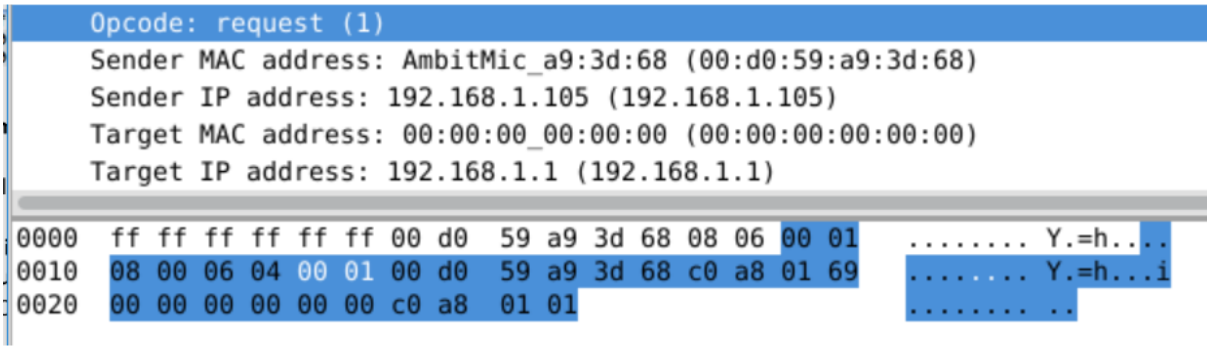
Question 2: Where in the ARP request does the “question” (IP address for which the mapping is being requested) appear?



```
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

      Address: AmbitMic_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)
▾ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (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 (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 (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                     ........ ..
```

The field “Target MAC address” is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.1.1) is being queried.

Question 3: How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?



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

The ARP opcode field begins after pos 0x0e = 14 bytes from the very beginning of the Ethernet frame.

Question 4: What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?

The hex value for the source address is 00:06:25:da:af:73

The destination is 00:d0:59:a9:3d:68.