21CY681– Internet Protocol lab

ASSIGNMENT -6

Name: B.Shebu

Register Number : CYS22005

Title: Understanding ARP using wireshark

Date of Assignment provided: 05/11/2022

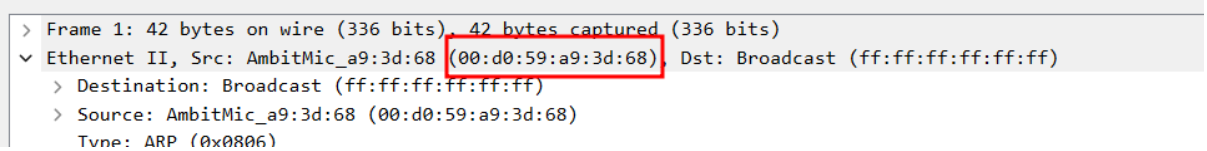
Aim: Analysing ARP request and response using wireshark.

PROCEDURE -

Use the provided pcap file (Arp) to answer the following questions.

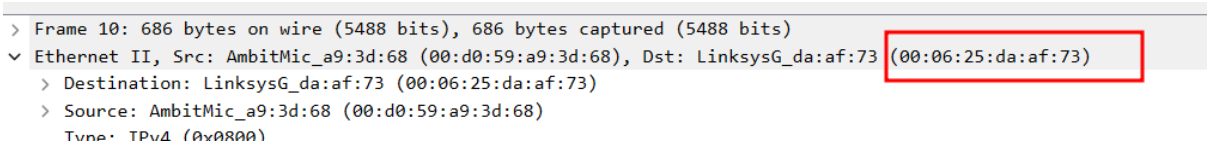
1. Answer the following questions based on the contents of the Ethernet frame containing the HTTP GET message.

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

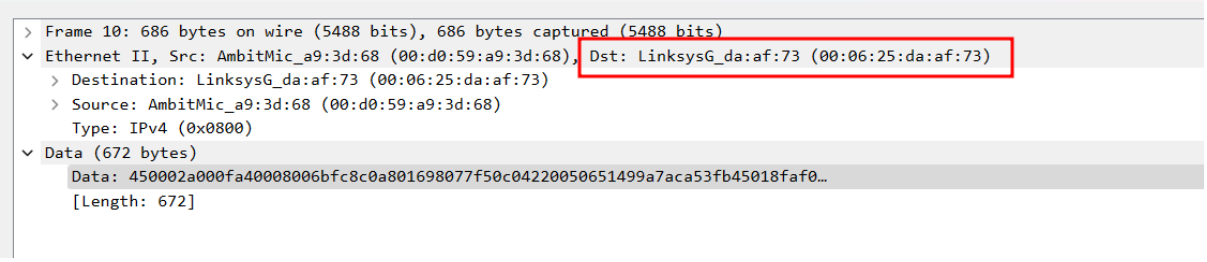


The 48 bit ethernet address of the source computer is 00:d0:59:a9:3d:68

b. 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?

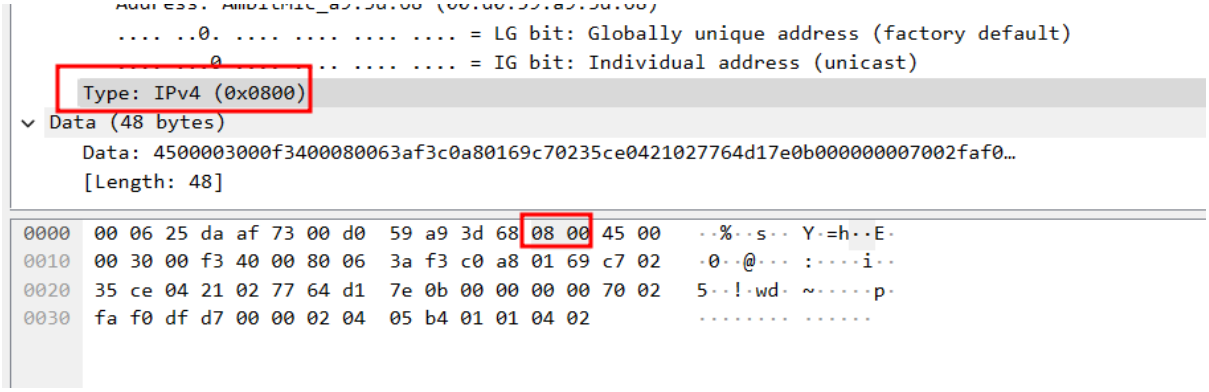


The 48 bit destination address in the Ethernet frame is 00:06:25:da:af:73 which is the address of the router/gateway



No this is the address of the router/gateway to which the source computer is sending the request.From there it gets transferred to the destination computer.

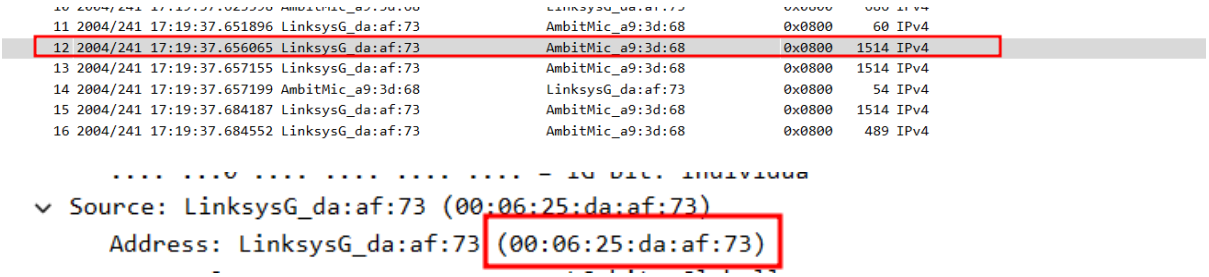
c. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to



The hex value of the 2 byte frame field is 0x0800 . It corresponds to IPV4 protocol.

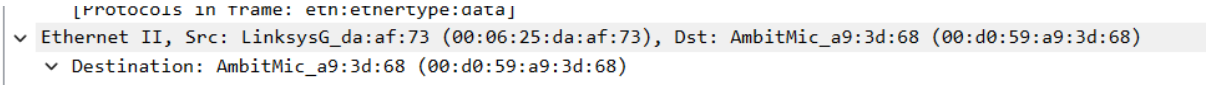
2. Answer the following questions based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

a. What is the value of the Ethernet source address?



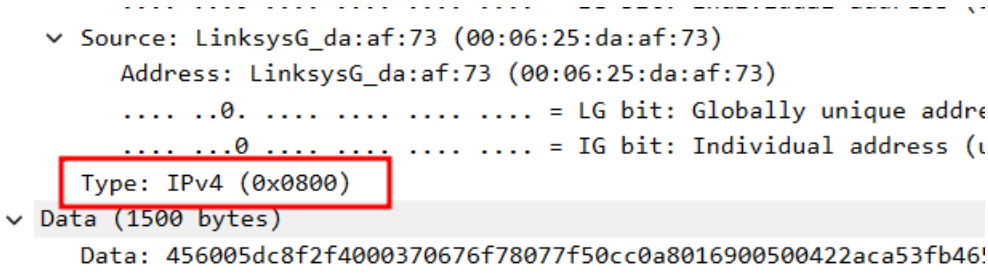
The value of ethernet source address in reply packet is 00:06:25:da:af:73

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



The Ethernet address of destination in reply packet is 00:d0:59;a9:ed:68

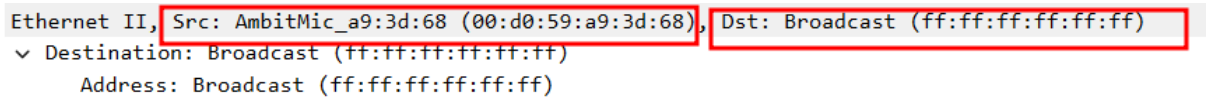
c. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?



The hex value of the two byte frame field is 0x0800. It corresponds to IPV4 layer.

3. Answer the following questions based on the contents of the ARP Request packets.

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

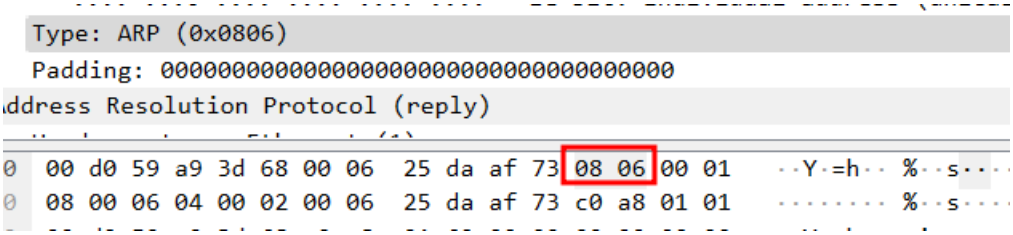


The address of

Source -> 00:d0:59:a9:3d:6d

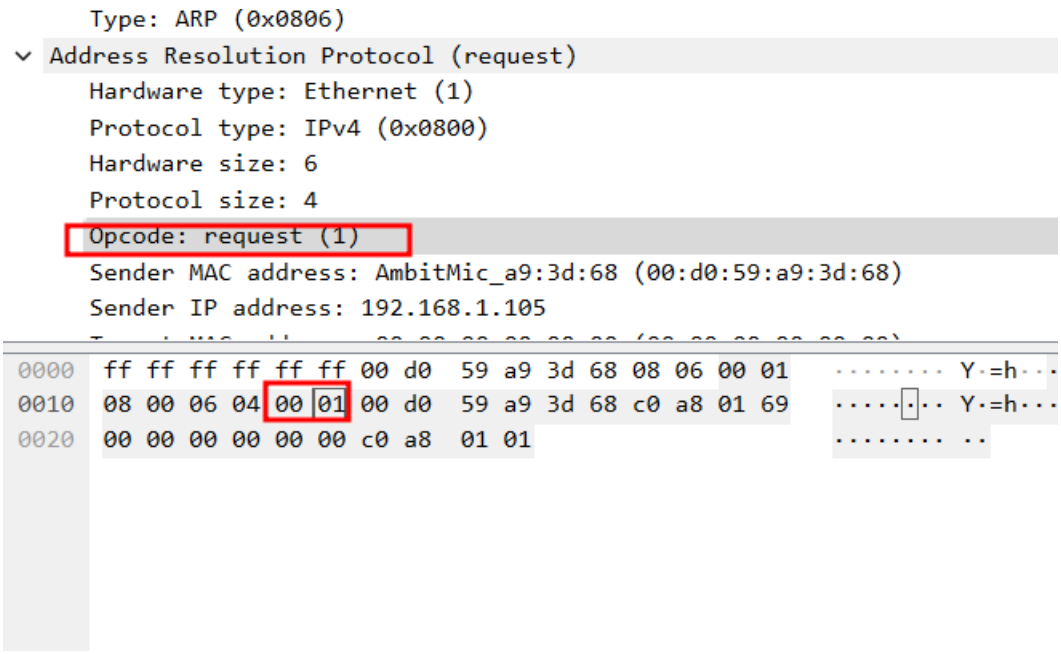
Destination -> ff:ff:ff:ff:ff:ff

b. Give the hexadecimal value for the two-byte Ethernet Frame type field.



The hex value of the two byte field is 0x0806

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



On clicking the OPCODE field we get to see the hex values 20-21. On clicking the hex values we see that the OPCODE field begins at 20 th field

d. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?

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

```
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···
0020  00 00 00 00 00 00 c0 a8  01 01                     ........ ··
```

e. Does the ARP message contain the IP address of the sender?

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

Yes it contains the sender IP address .

f. 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
```

From the above we can see that the request where the sender asks which system has the IP address 192.168.1.1

4. Answer the following questions based on the contents of the ARP Reply packets.

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

```
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)
Target IP address: 192.168.1.105
```

```
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               ········ ····
```

It begins at 20-21 st field

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?

```
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)
Target IP address: 192.168.1.105
```

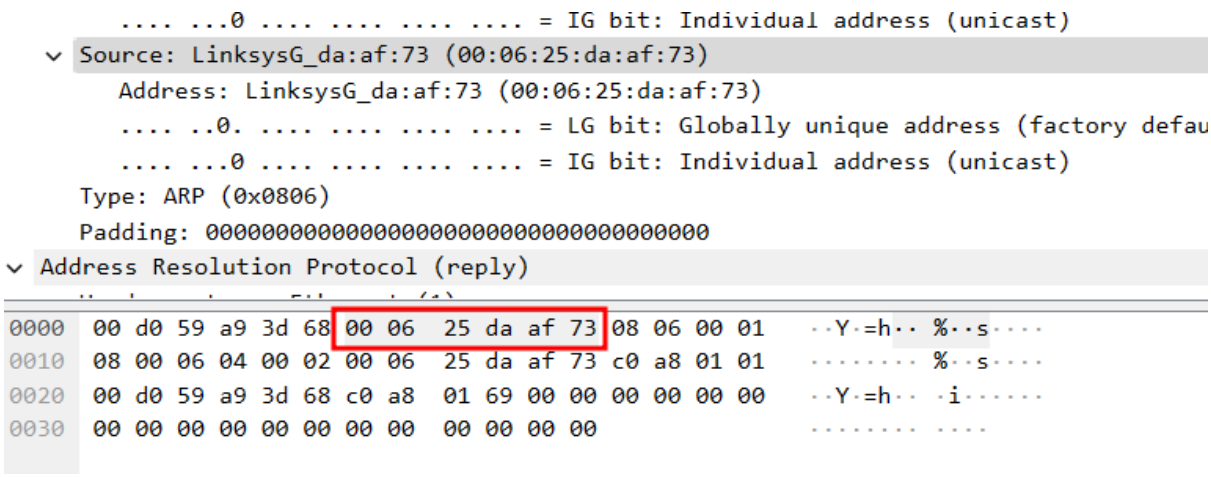
The value of the OPCODE field within the arp payload in response packet is 2.

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?

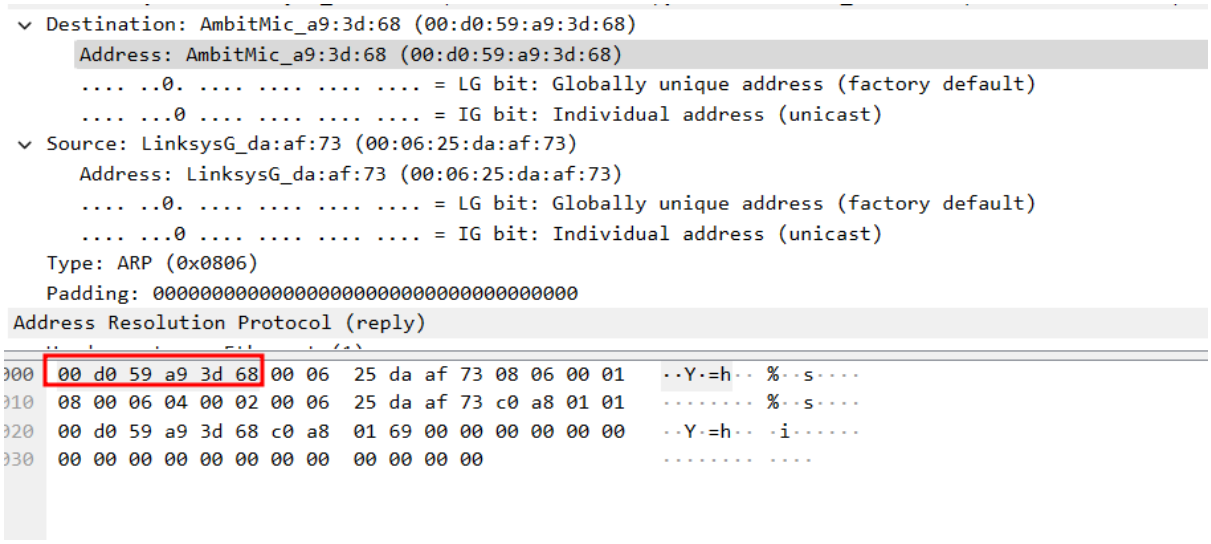
```
Opcode: reply (2)
Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
Sender IP address: 192.168.1.1
Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
Target IP address: 192.168.1.105
```

We can confirm that this packet contains the answer since it contains both the sender and reveiver’s MAC address along with their IP address.

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

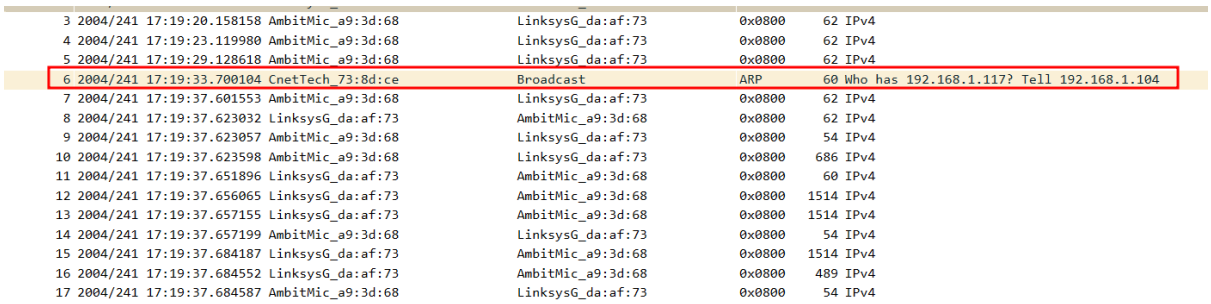


The hex value of the source address is 00 06 25 da af 73



The value of the destination address is 00 d0 59 a9 3d 68

e. 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



There is no response for the second ARP request packet because ARP request packet is a broadcast message and the arp response is unicast . So the computer which has the ip that is queried by the

server will send a unicast response packet back to the router. So since the traffic is captured from this computer which has the ip .105 we are not able to see the reply arp packet which is sent back.

RESULT –

Thus the experiment to understand ARP requests and responses have been done successfully.