INTERNET PROTOCOL LAB ASSIGNMENT -6

Name: Siriparapu Sparshika

Roll No: CYS22006

Date: 05-11-2022

TITLE: Analyzing ARP request and response using Wireshark

AIM:

To analyze ARP request and response using Wireshark.

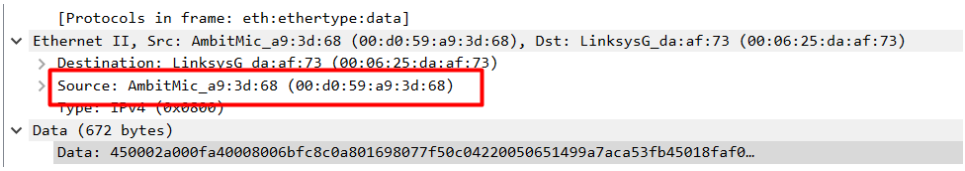
PROCEDURE:

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

HTTP GET message.

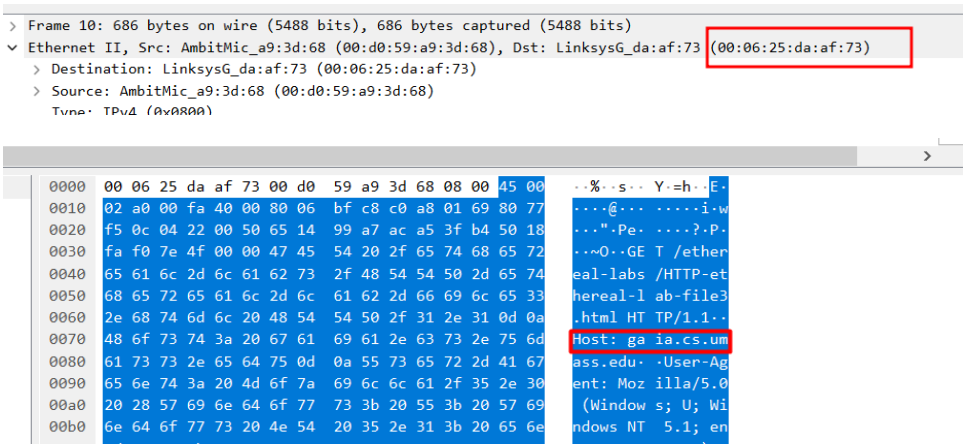
a. What is the 48-bit Ethernet address of your computer?

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?

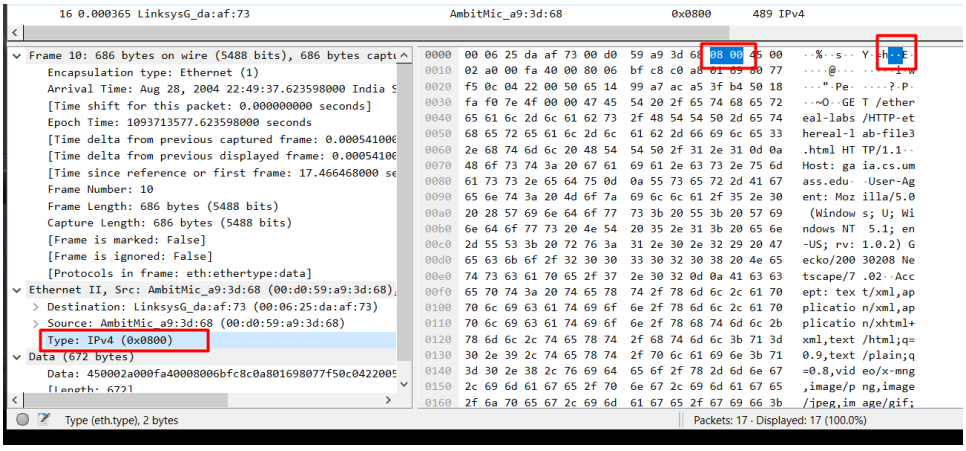


Router mac's address

c. Give the hexadecimal value for the two-byte Frame type field. What upper layer

protocol does this correspond to?

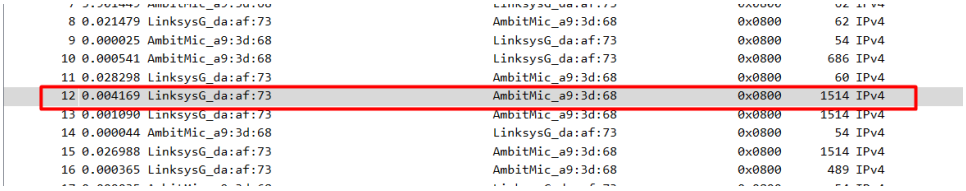
Ipv4 –0x0800 – ethernet frame –2 byte frame field



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?

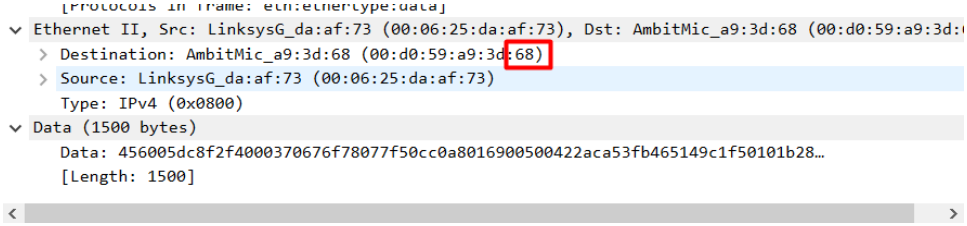


ethernet source address in reply packet is 00:06:25:da:af:73

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

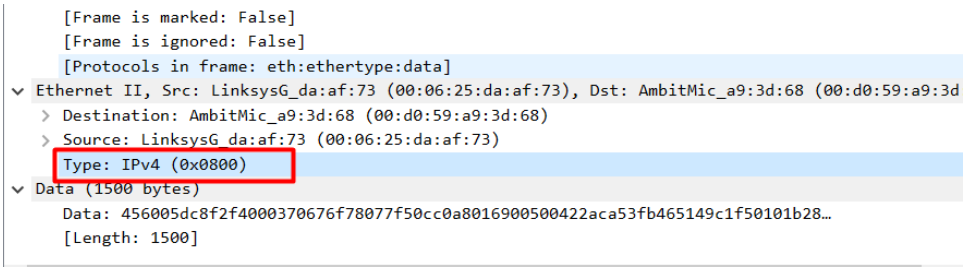
of your computer?

Yes, it's the ethernet address of my computer



c. Give the hexadecimal value for the two-byte Frame type field. What upper layer

protocol does this correspond to?



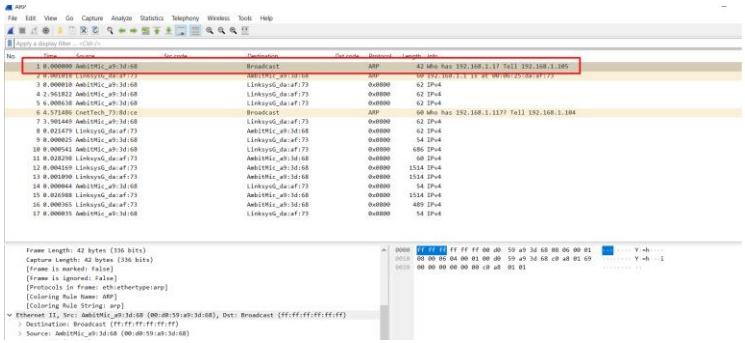
3. Answer the following questions based on the contents of the ARP Request packets.

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

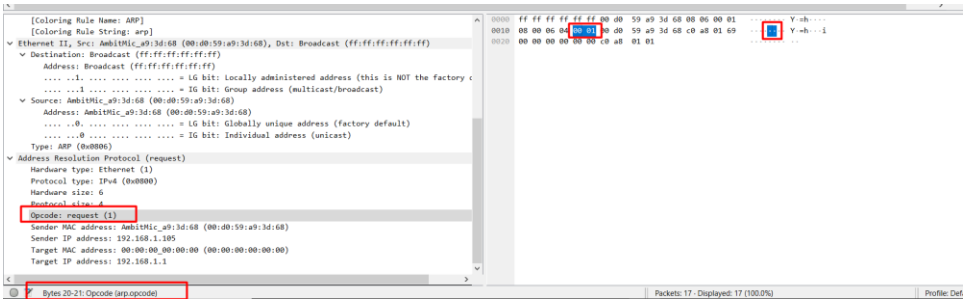
Destination -> ff:ff:ff:ff:ff:ff



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

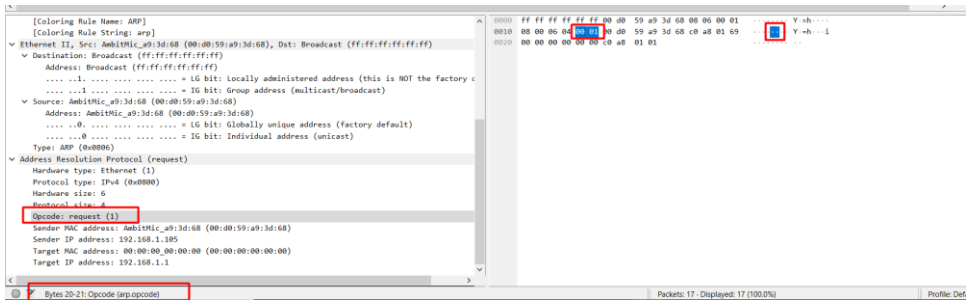
```
    [Protocols in frame: eth:ethertype:data]
▾ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  ▾ Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
```

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

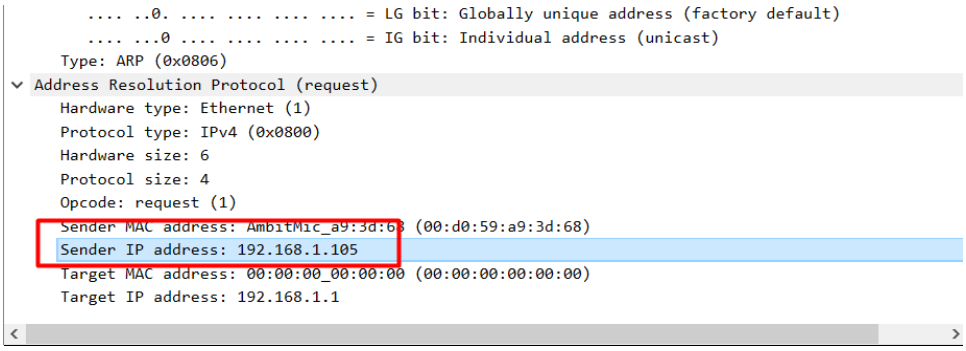


d. What is the value of the opcode field within the ARP-payload part of the Ethernet

frame in which an ARP request is made?

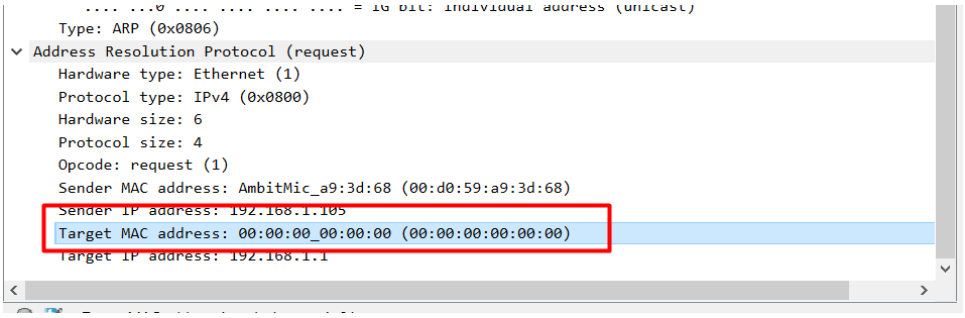


e. Does the ARP message contain the IP address of the sender?



f. Where in the ARP request does the “question” appear – the Ethernet address of the

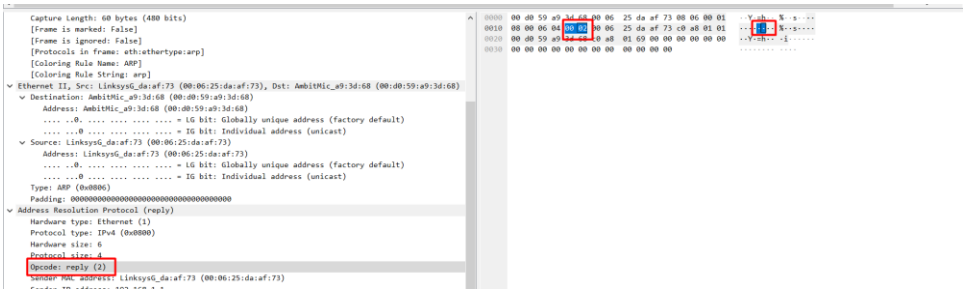
machine whose corresponding IP address is being queried?



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

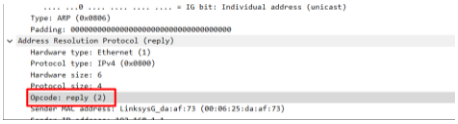
a. How many bytes from the very beginning of the Ethernet frame does the ARP

opcode field begin?



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?



By analyzing send mac address along with sender Ip address

c. Where in the ARP message does the “answer” to the earlier ARP request appear –

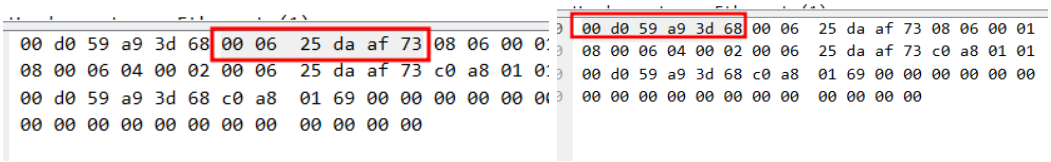
the IP address of the machine having the Ethernet address whose corresponding IP

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
```

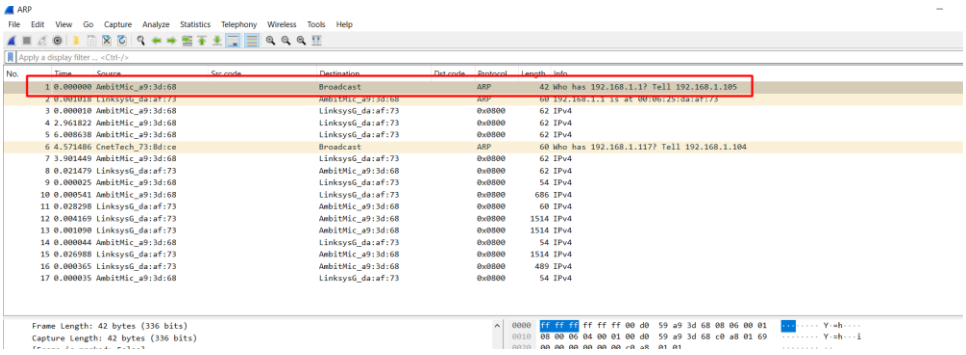
d. What are the hexadecimal values for the source and destination addresses in the

Ethernet frame containing the ARP reply message?.



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 - broadcast
message - arp response is unicast.
The computer which has the ip that is queried by the server will send a unicast response packet back to the router.

RESULT:

Thus, ARP requests and responses have been done observed successfully using Wireshark.