NAME: S.PRIYADHARSHINI

ROLL NO.: CB.EN.P2CYS22010

DATE: 3.11.2022

INTERNET PROTOCOL LAB – 6

ANALYSING ARP USING WIRESHARK

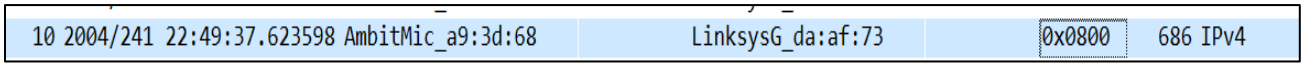
AIM:

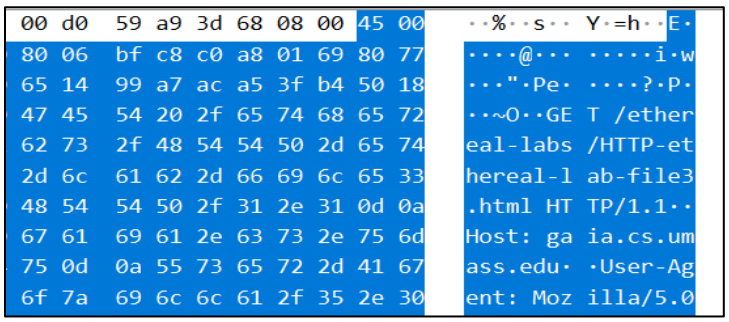
To analyze ARP (Address Resolution Protocol) using Wireshark.

PROCDURE:

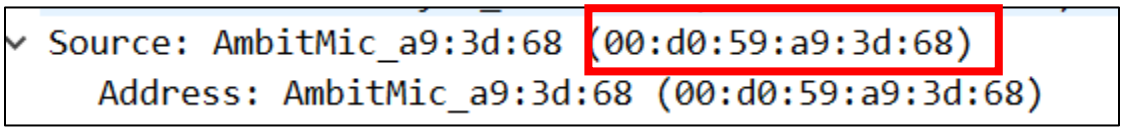
Analyze -> enabled protocols -> disable IPV4 protocols. (We have tuned the Wireshark to only read till link-layer (link-layer and physical layer)).

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

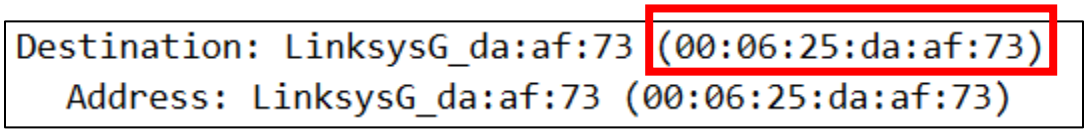




a.What is the 48-bit Ethernet address of your computer?



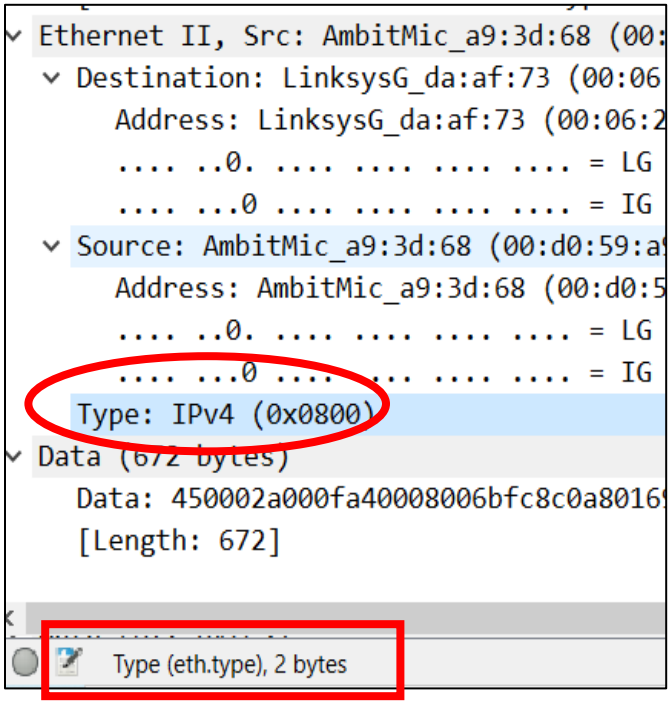
b. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? What device has this as its Ethernet address?



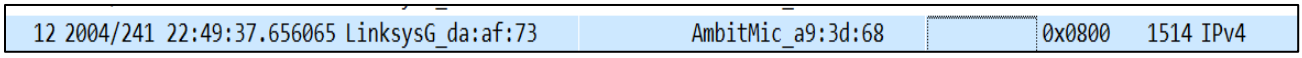
The source is sending the request to the router(00:06:25:da:af:73) from where it will reach the destination.

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

Hexadecimal value is 0x0800. This corresponds to IPV4 protocol.

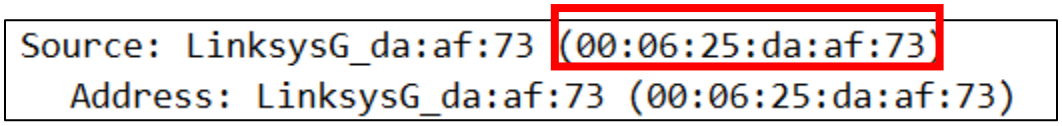


2. Answer the following questions based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

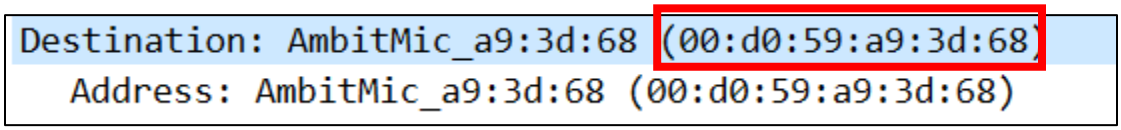


Packet number 12.

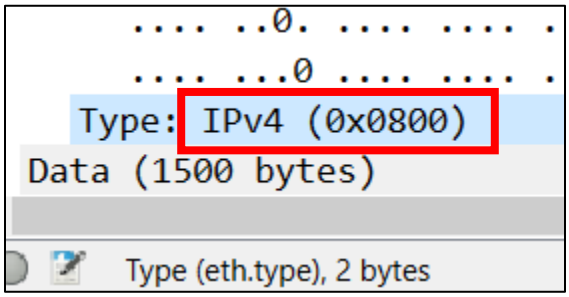
a.What is the value of the Ethernet source address?



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

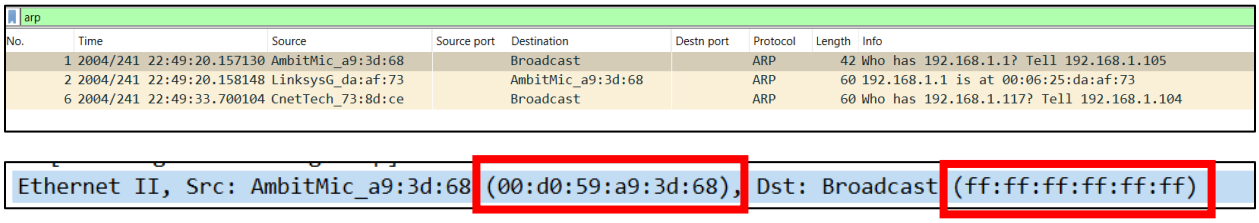


c. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

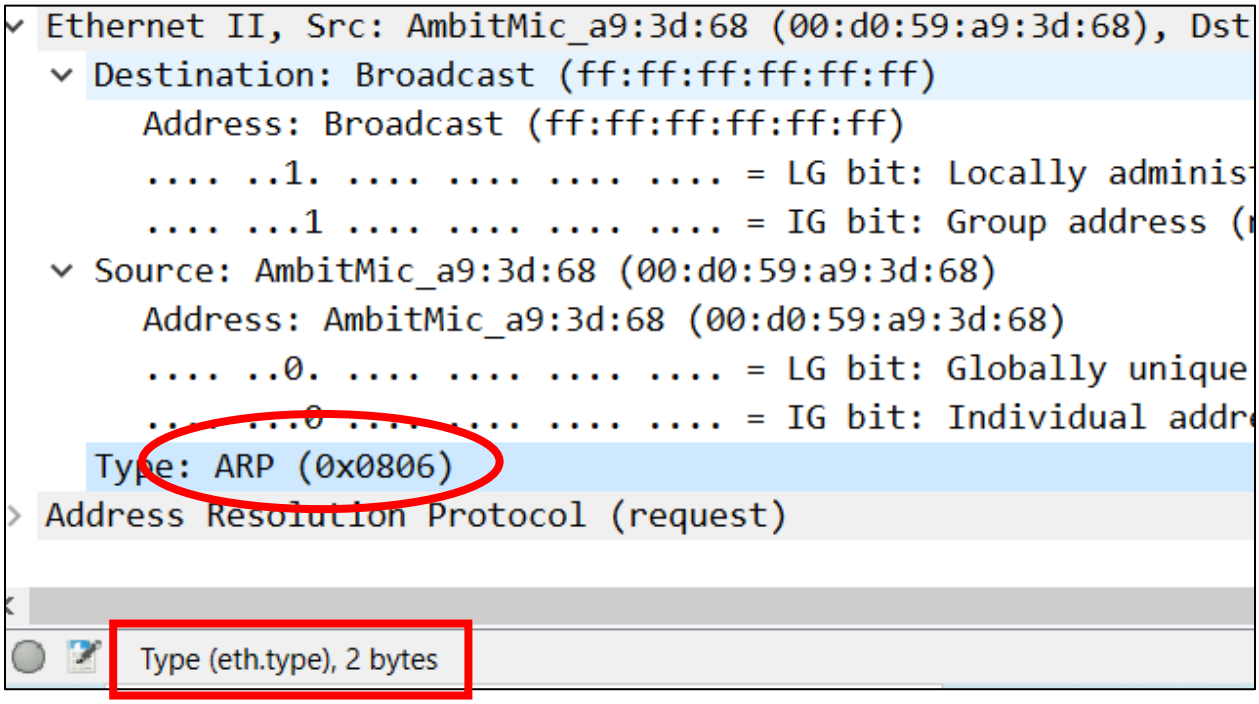


3. Answer the following questions based on the contents of the ARP Request packets.

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



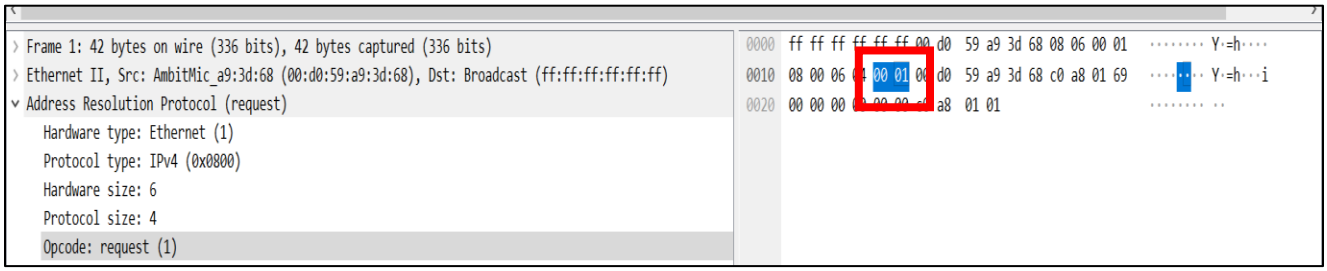
b. Give the hexadecimal value for the two-byte Ethernet Frame type field.



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

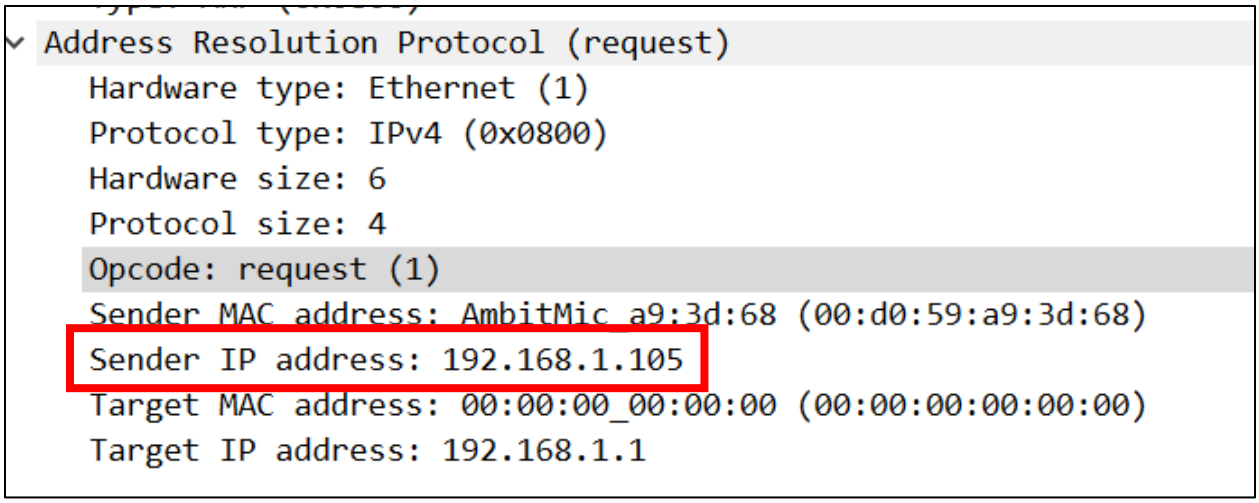
ARP opcode field begins from 20.

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?

Yes, it has the sender's IP address.



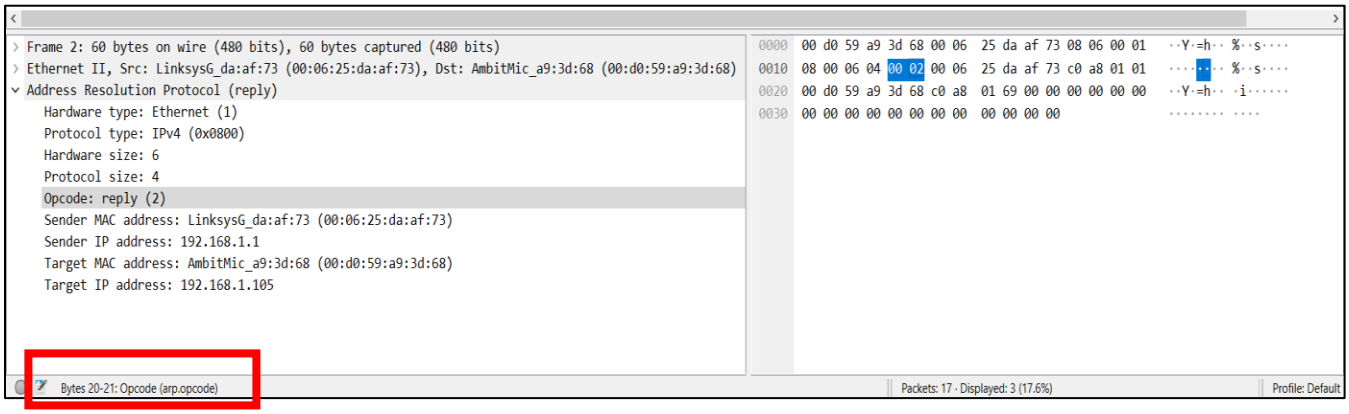
f. Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?

In the request message the target IP address is present. – 192.168.1.1. But target MAC address is not present(00:00:00:00:00:00)

```
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
```

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?

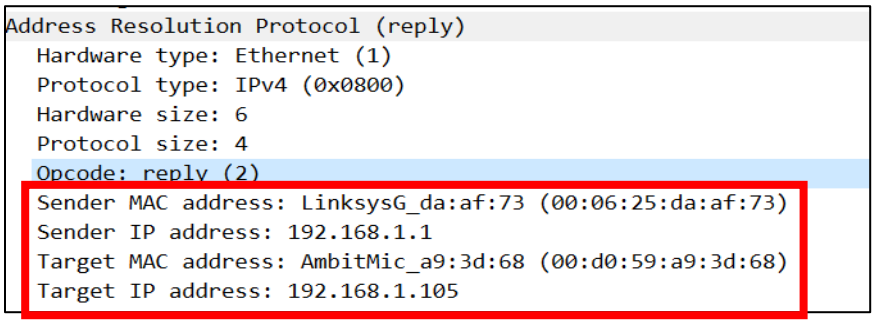


b. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

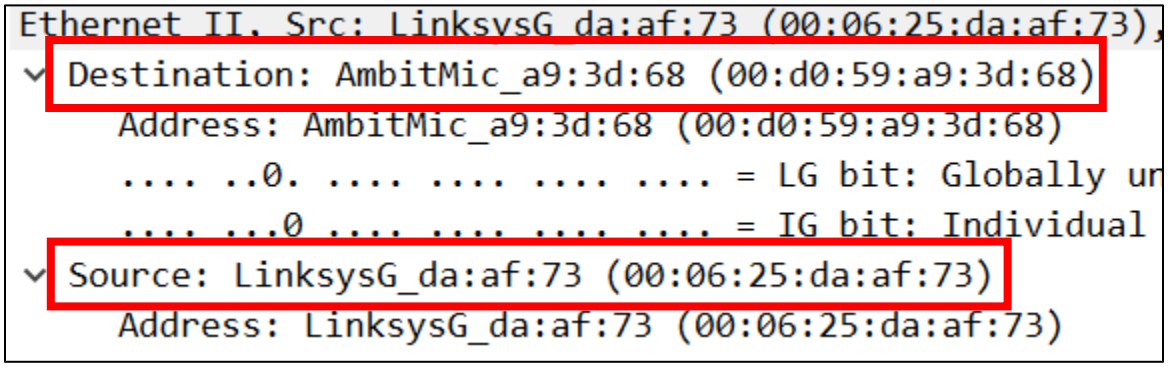
```
Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: LinksysG_da:af:73 (00:06:25:da:af:73)
  Sender IP address: 192.168.1.1
  Target MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  Target IP address: 192.168.1.105
```

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?

Both the source and destination MAC address is present. Therefore this can be considered as the answer to the previous request message.

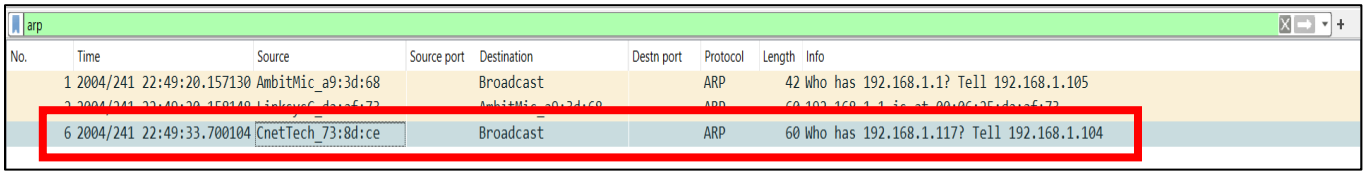


d. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP reply message?



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?

Here, there is another ARP request which is broadcast by the source(00:80:ad:73:8d:ce). The reply for this request will be unicast from the router to the source. Since, this capture is done from system with IP address 192.168.1.105 the unicast reply for the particular system cannot be seen.



RESULT:

Thus, ARP protocol has been successfully analyzed by Wireshark.