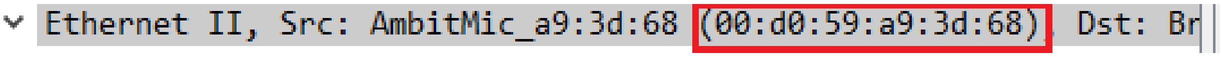
ASSIGNMENT
INTERNET PROTOCOL LAB

NAME: Rahul Raj
REG NO: CYS22011
DATE OF ASSIGNMENT PROVIDED: 5/11/2022
TITLE: Analyzing ARP request and response using Wireshark.

PROCEDURE –

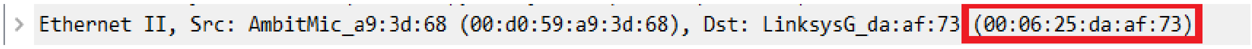
Use the provided pcap file (Arp) to answer the following questions
. 1. Answer the following questions based on the contents of the Ethernet frame containing the HTTP GET message.

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



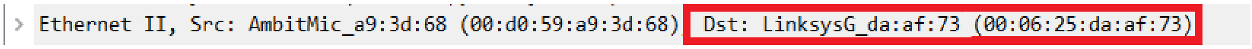
```
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) Dst: Br
```

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?



```
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
```

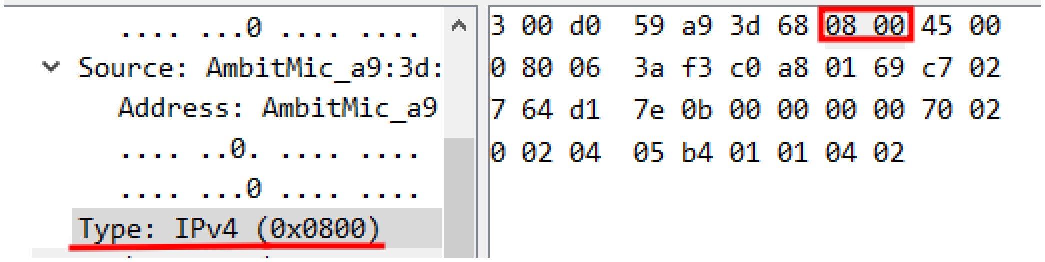
00:06:25:da:af:73 is the address of the router/router.



```
Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68) Dst: LinksysG_da:af:73 (00:06:25:da:af:73)
```

No, this is the address of the router/gateway.

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

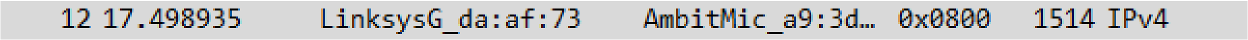


```
    .... ...0 .... ....        3 00 d0  59 a9 3d 68 08 00 45 00
  Source: AmbitMic_a9:3d:      0 80 06  3a f3 c0 a8 01 69 c7 02
    Address: AmbitMic_a9       7 64 d1  7e 0b 00 00 00 00 70 02
    .... ..0. .... ....        0 02 04  05 b4 01 01 04 02
    .... ...0 .... ....
  Type: IPv4 (0x0800)
```

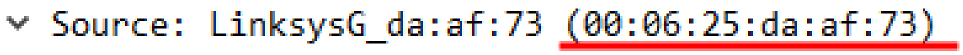
The Hexa decimal value of 2-byte frame field is 0x800, and it corresponds to IPV4.

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?



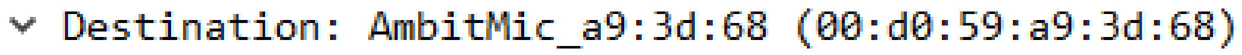
```
    12 17.498935      LinksysG_da:af:73     AmbitMic_a9:3d…  0x0800    1514 IPv4
```



```
 ⌄ Source: LinksysG_da:af:73 (00:06:25:da:af:73)
```

00:06:25:da:af:73 is the value of ethernet source address in replay packet.

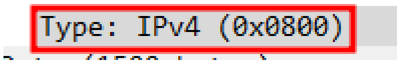
b. What is the destination address in the Ethernet frame? Is this the Ethernet address of your computer?



```
⌄ Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
```

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

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

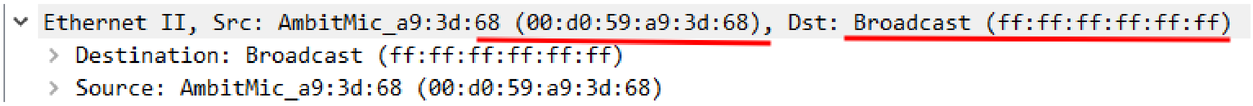


```
  Type: IPv4 (0x0800)
```

The Hexa decimal value of 2-byte frame field is 0x800, and it corresponds to IPV4.

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

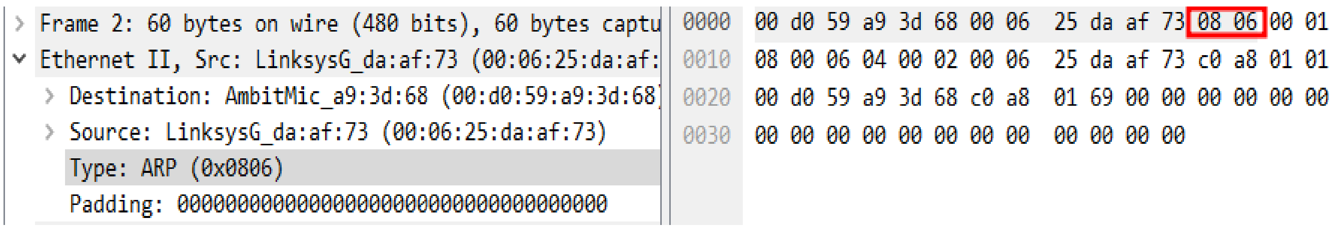
a. What are the hexadecimal values for the source and destination addresses in the Ethernet frame containing the ARP request message?



```
⌄ 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)
```

The address of Source is 00:d0:59:a9:3d:6 and Destination is ff:ff:ff:ff:ff:ff.

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

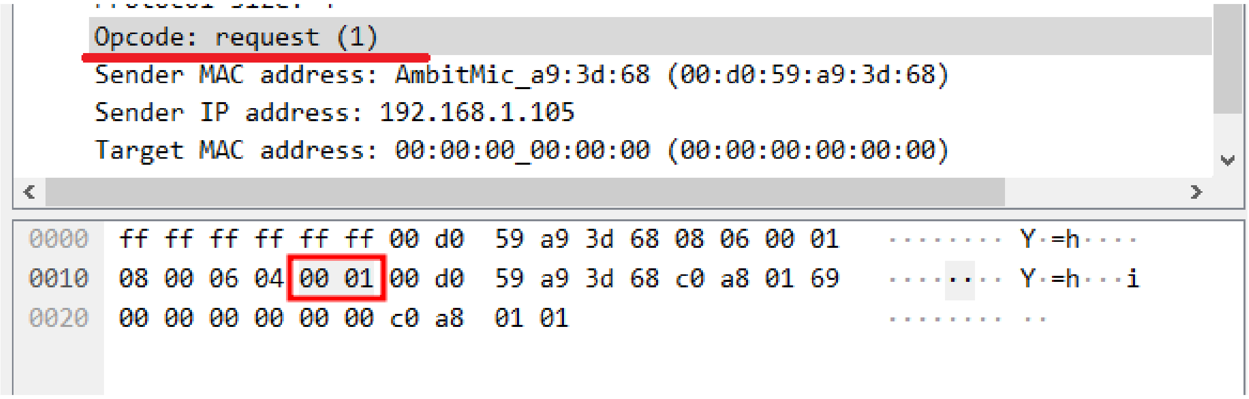


```
› Frame 2: 60 bytes on wire (480 bits), 60 bytes captu
⌄ Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:
  › Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
  › Source: LinksysG_da:af:73 (00:06:25:da:af:73)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
```

```
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01
0010  08 00 06 04 00 02 00 06  25 da af 73 c0 a8 01 01
0020  00 d0 59 a9 3d 68 c0 a8  01 69 00 00 00 00 00 00
0030  00 00 00 00 00 00 00 00  00 00 00 00
```

The hexadecimal of the 2byte field is 0x0806.

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

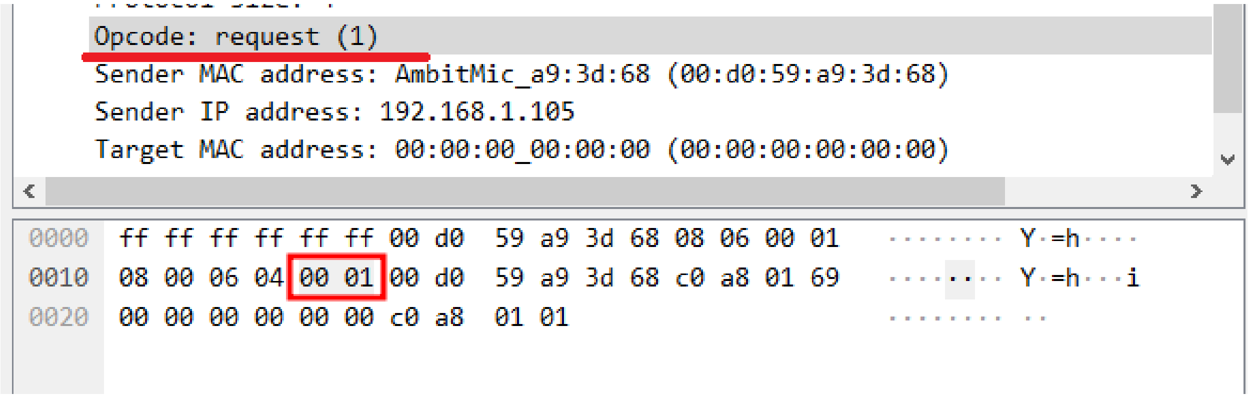


```
    Opcode: request (1)
    Sender MAC address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Sender IP address: 192.168.1.105
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
```

```
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                     ········ ··
```

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

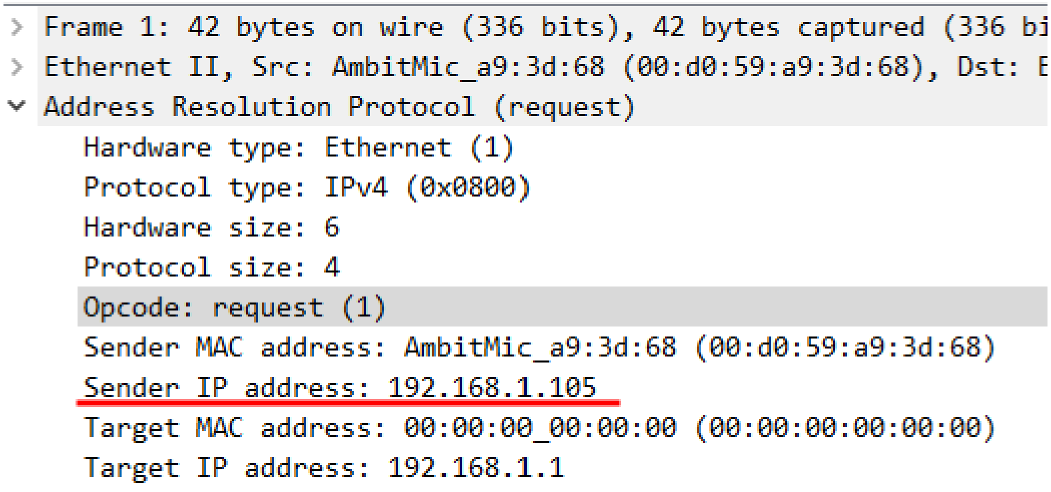
d. What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP request is made?



```
    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)
```

```
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                     ········ ··
```

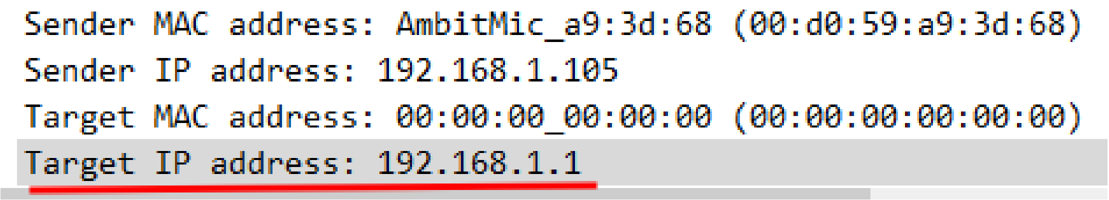
e. Does the ARP message contain the IP address of the sender?



```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bi
> Ethernet II, Src: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68), Dst: E
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
```

Yes, it contains the sender IP address.

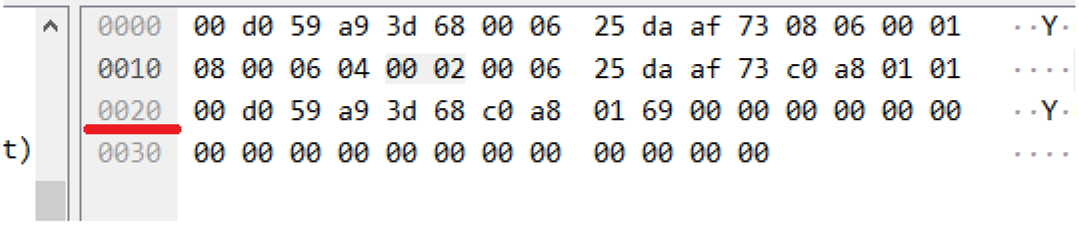
f. Where in the ARP request does the "question" appear – the Ethernet address of the machine whose corresponding IP address is being queried?



```
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.

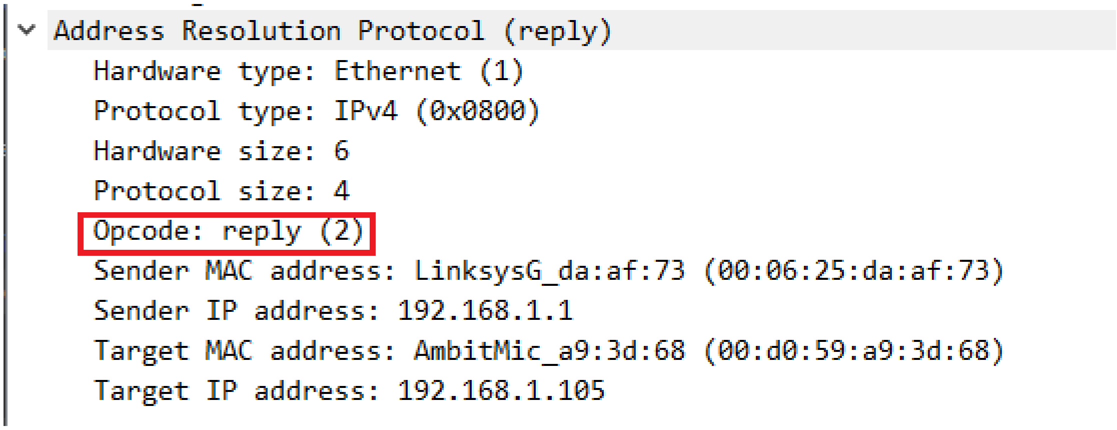
a. How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?



```
t)
0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01   ··Y·
0010  08 00 06 04 00 02 00 06  25 da af 73 c0 a8 01 01   ····
0020  00 d0 59 a9 3d 68 c0 a8  01 69 00 00 00 00 00 00   ··Y·
0030  00 00 00 00 00 00 00 00  00 00 00 00               ····
```

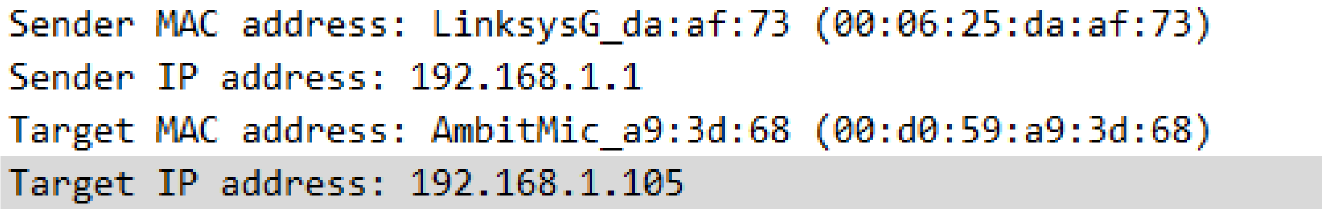
It begins at 20-21st field.

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?



```
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
```

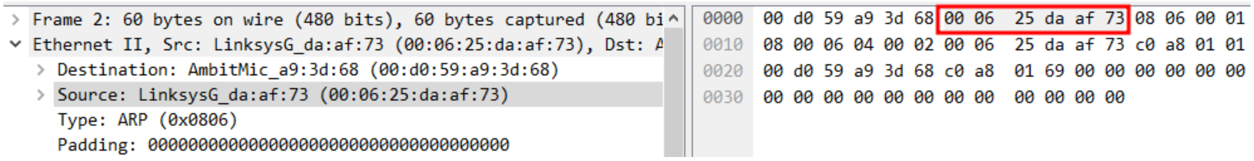
c. Where in the ARP message does the "answer" to the earlier ARP request appear – the IP address of the machine having the Ethernet address whose corresponding IP address is being queried?



```
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
```

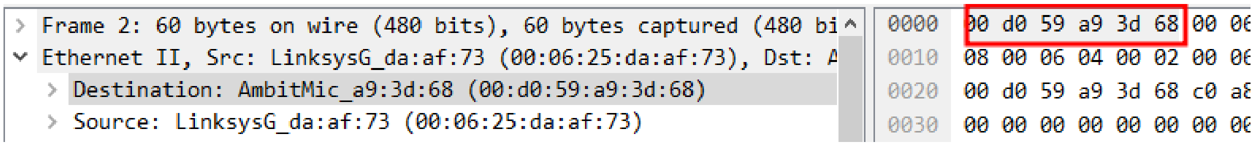
It confirms that this packet contains the answer since it contains both the sender and receiver's MAC address along with their IP address.

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



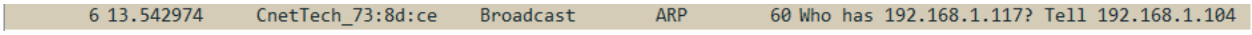
```
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bi      0000  00 d0 59 a9 3d 68 00 06  25 da af 73 08 06 00 01
v Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: A      0010  08 00 06 04 00 02 00 06  25 da af 73 c0 a8 01 01
  > Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)                 0020  00 d0 59 a9 3d 68 c0 a8  01 69 00 00 00 00 00 00
  > Source: LinksysG_da:af:73 (00:06:25:da:af:73)                      0030  00 00 00 00 00 00 00 00  00 00 00 00
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
```

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



```
> Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bi      0000  00 d0 59 a9 3d 68 00 06
v Ethernet II, Src: LinksysG_da:af:73 (00:06:25:da:af:73), Dst: A      0010  08 00 06 04 00 02 00 06
  > Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)                 0020  00 d0 59 a9 3d 68 c0 a8
  > Source: LinksysG_da:af:73 (00:06:25:da:af:73)                      0030  00 00 00 00 00 00 00 00
```

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.



```
6 13.542974    CnetTech_73:8d:ce    Broadcast    ARP    60 Who has 192.168.1.117? Tell 192.168.1.104
```

There is no response for the second ARP request packet because ARP request packet is a broadcast message and the arp response is unicas.

RESULT –

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