21CY681 - INTERNET PROTOCOL LAB - VI

Name: Surya S Nair

Register Number: CB.EN.P2CYS22007

Date: 5th November 2022

Assignment Topic: Analyzing ARP request and response using wireshark

AIM:Analyzing ARP request and response using wireshark

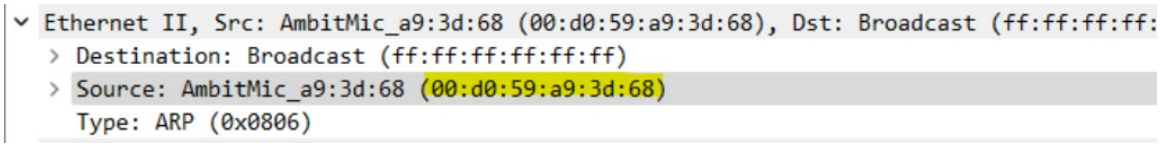
PROCEDURE:

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.

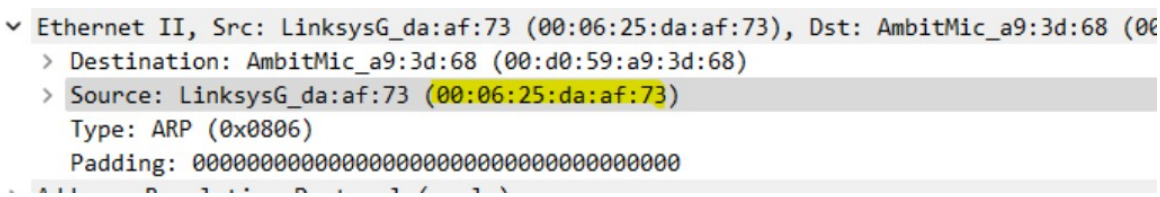
a. What is the 48-bit Ethernet address of your computer?

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



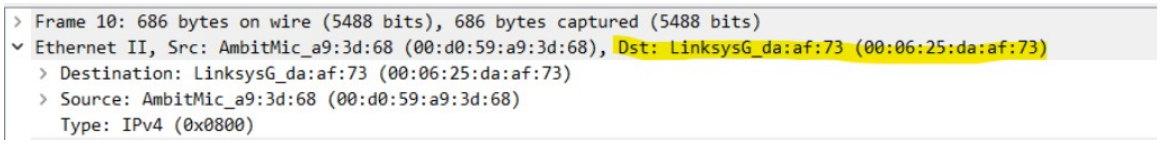
b. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? What device has this as its Ethernet address?

Ans:



48-bit destination address in the Ethernet frame is 00:06:25:da:af:73.It is the address

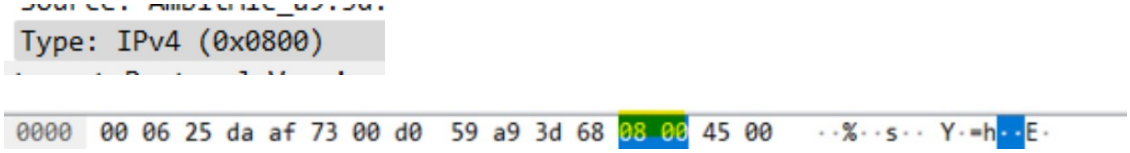
of router/gateway.



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?

Ans:

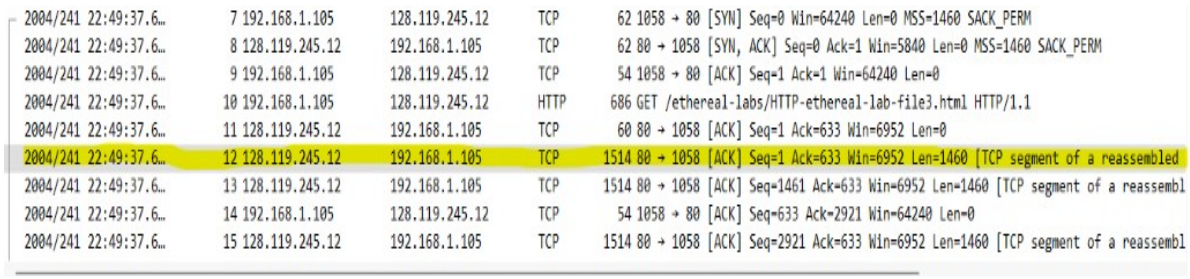


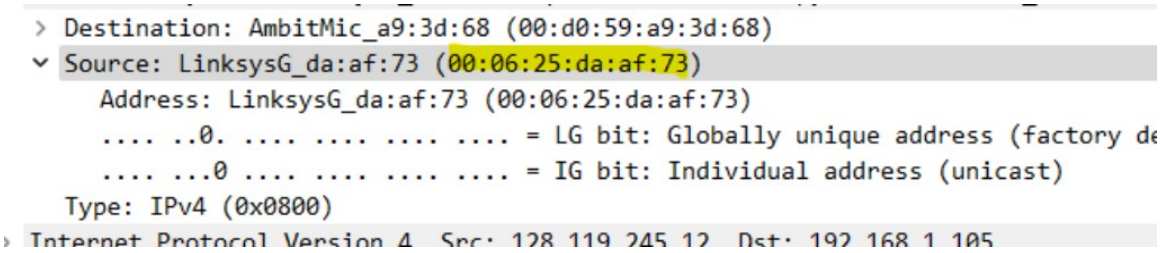
The hex value of the 2 byte frame field is 0x0800.It is corresponding to IPV4 protocol.

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?

Ans:

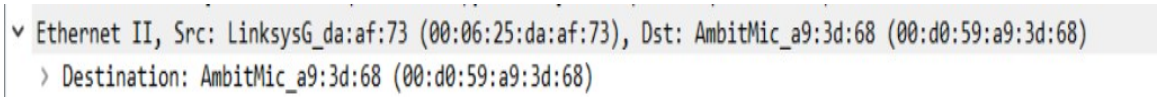




Value of the Ethernet source address in reply packet is 00:06:25:da:af:73

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

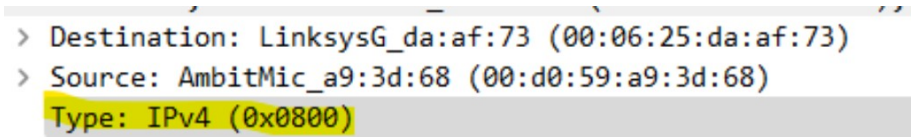
Ans:



The Ethernet address of destination in reply packet is 00:d0:59:a9:3d:68

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

Ans:

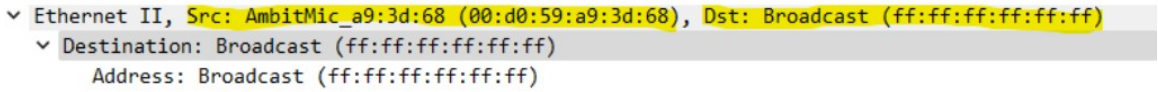


The hex value of the two byte frame field is 0x0800.It is corresponding to IPV4 layer.

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?

Ans:



The address of source --> 00:d0:59:a9:3d:68

The address of destination--> ff:ff:ff:ff:ff:ff

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

Ans:

```
.... ...0 .... .... .... .... = IG bit: Individual
Type: ARP (0x0806)
Padding: 00000000000000000000000000000000000000
```

```
0000  ff ff ff ff ff ff 00 80  ad 73 8d ce 08 06 00 01   ........ .s......
0010  08 00 06 04 00 01 00 80  ad 73 8d ce c0 a8 01 68   ........ .s.....h
0020  00 00 00 00 00 00 c0 a8  01 75 00 00 00 00 00 00   ........ .u......
0030  00 00 00 00 00 00 00 00  00 00 00 00              ........ ....
```

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?

Ans:

```
    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
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 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                     ........ ..
```

On clicking the OPCODE field we get to see the hex value 20-21.On clicking the hex value 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?

Ans:

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

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

Ans:

```
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?

Ans:

```
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
```

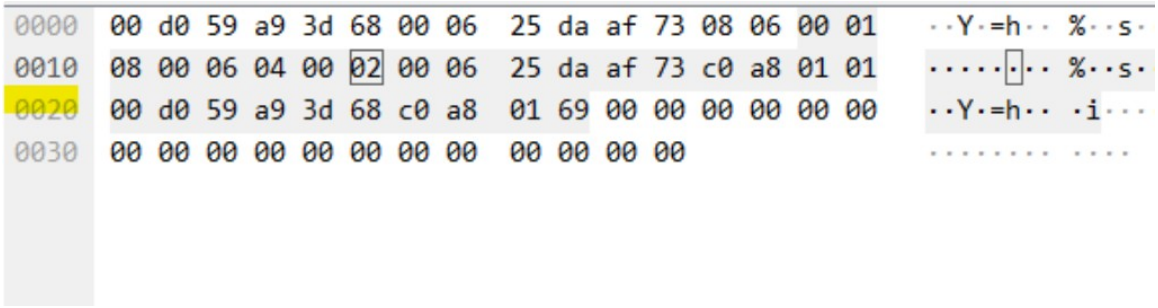
From the above we can see that the request where the sender asks which system has the IP address 192.168.1.1

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?

Ans:

```
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
```



It begins at 20-21 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?

Ans:

```
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 is 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?

Ans:

```
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 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?

Ans:

```
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: ARP (0x0806)
  Padding: 00000000000000000000000000000000
```

```
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               ········ ····
```

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

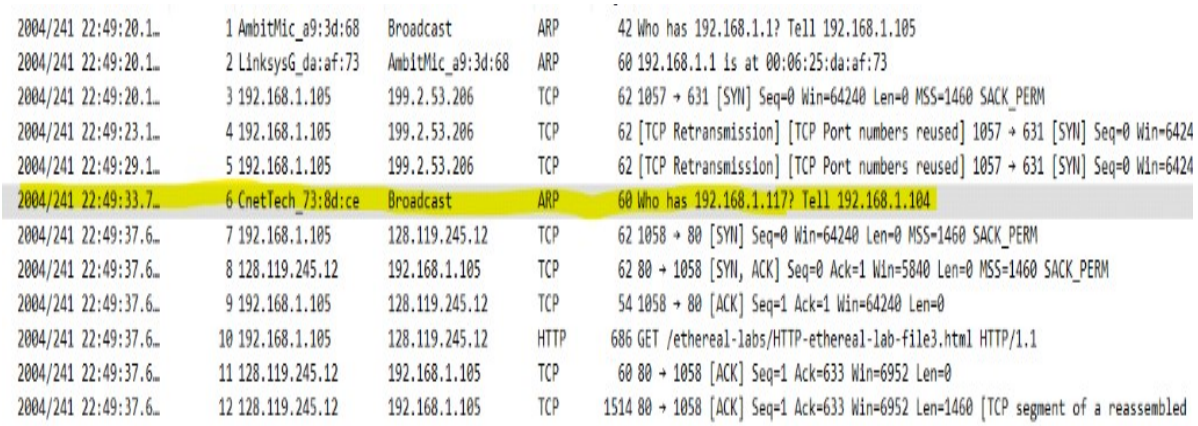
```
Destination: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    Address: AmbitMic_a9:3d:68 (00:d0:59:a9:3d:68)
    .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
Source: LinksysG_da:af:73 (00:06:25:da:af:73)
    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: ARP (0x0806)
  Padding: 00000000000000000000000000000000
```

```
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               ········ ····
```

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?

Ans:



2004/241 22:49:20.1…	1 AmbitMic_a9:3d:68	Broadcast	ARP	42 Who has 192.168.1.1? Tell 192.168.1.105
2004/241 22:49:20.1…	2 LinksysG_da:af:73	AmbitMic_a9:3d:68	ARP	60 192.168.1.1 is at 00:06:25:da:af:73
2004/241 22:49:20.1…	3 192.168.1.105	199.2.53.206	TCP	62 1057 → 631 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
2004/241 22:49:23.1…	4 192.168.1.105	199.2.53.206	TCP	62 [TCP Retransmission] [TCP Port numbers reused] 1057 → 631 [SYN] Seq=0 Win=6424
2004/241 22:49:29.1…	5 192.168.1.105	199.2.53.206	TCP	62 [TCP Retransmission] [TCP Port numbers reused] 1057 → 631 [SYN] Seq=0 Win=6424
2004/241 22:49:33.7…	6 CnetTech_73:8d:ce	Broadcast	ARP	60 Who has 192.168.1.117? Tell 192.168.1.104
2004/241 22:49:37.6…	7 192.168.1.105	128.119.245.12	TCP	62 1058 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM
2004/241 22:49:37.6…	8 128.119.245.12	192.168.1.105	TCP	62 80 → 1058 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM
2004/241 22:49:37.6…	9 192.168.1.105	128.119.245.12	TCP	54 1058 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2004/241 22:49:37.6…	10 192.168.1.105	128.119.245.12	HTTP	686 GET /ethereal-labs/HTTP-ethereal-lab-file3.html HTTP/1.1
2004/241 22:49:37.6…	11 128.119.245.12	192.168.1.105	TCP	60 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=0
2004/241 22:49:37.6…	12 128.119.245.12	192.168.1.105	TCP	1514 80 → 1058 [ACK] Seq=1 Ack=633 Win=6952 Len=1460 [TCP segment of a reassembled

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:Analyzed ARP request and response using wireshark