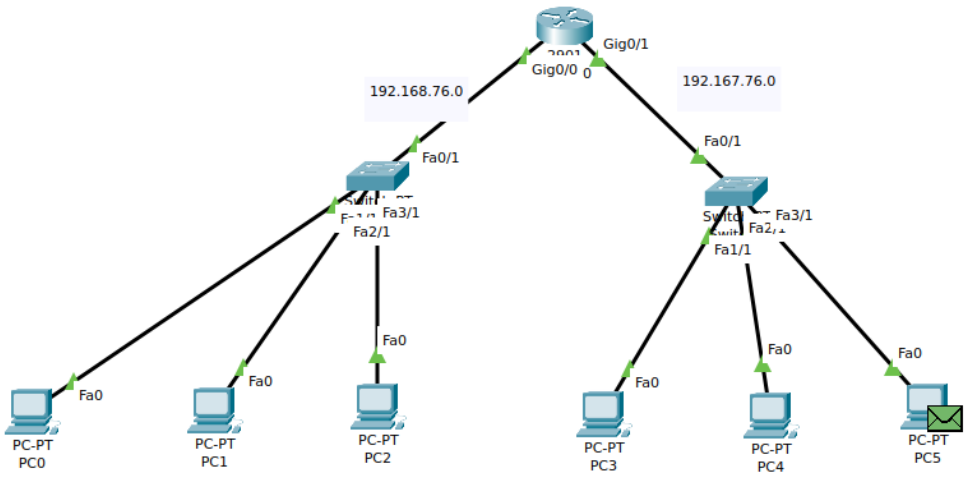
In_Class Problem & WireShark

21_AIE_211

ICN– SEM-IV
Professor – Ganga Gowri Mam

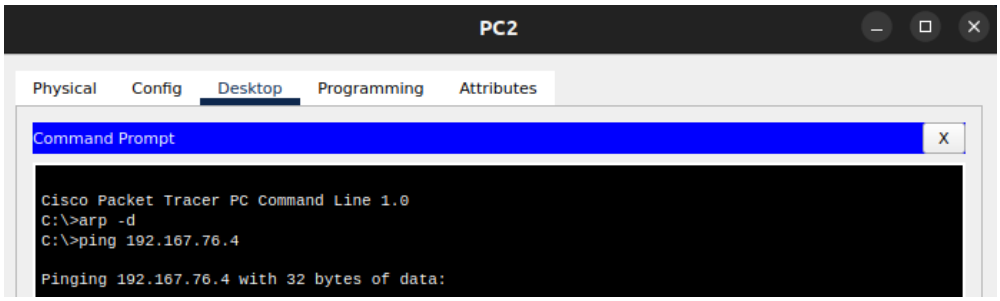
Submitted By: Vikhyat Bansal [CB.EN.U4AIE21076]

Network:

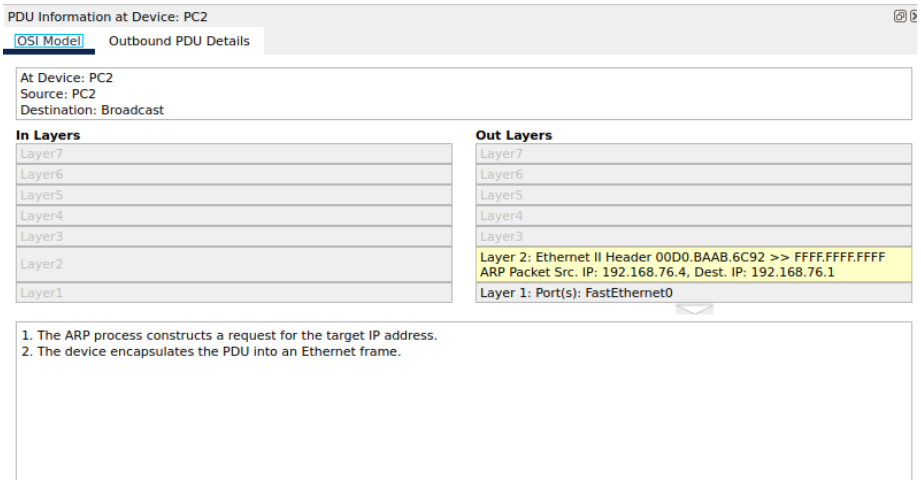


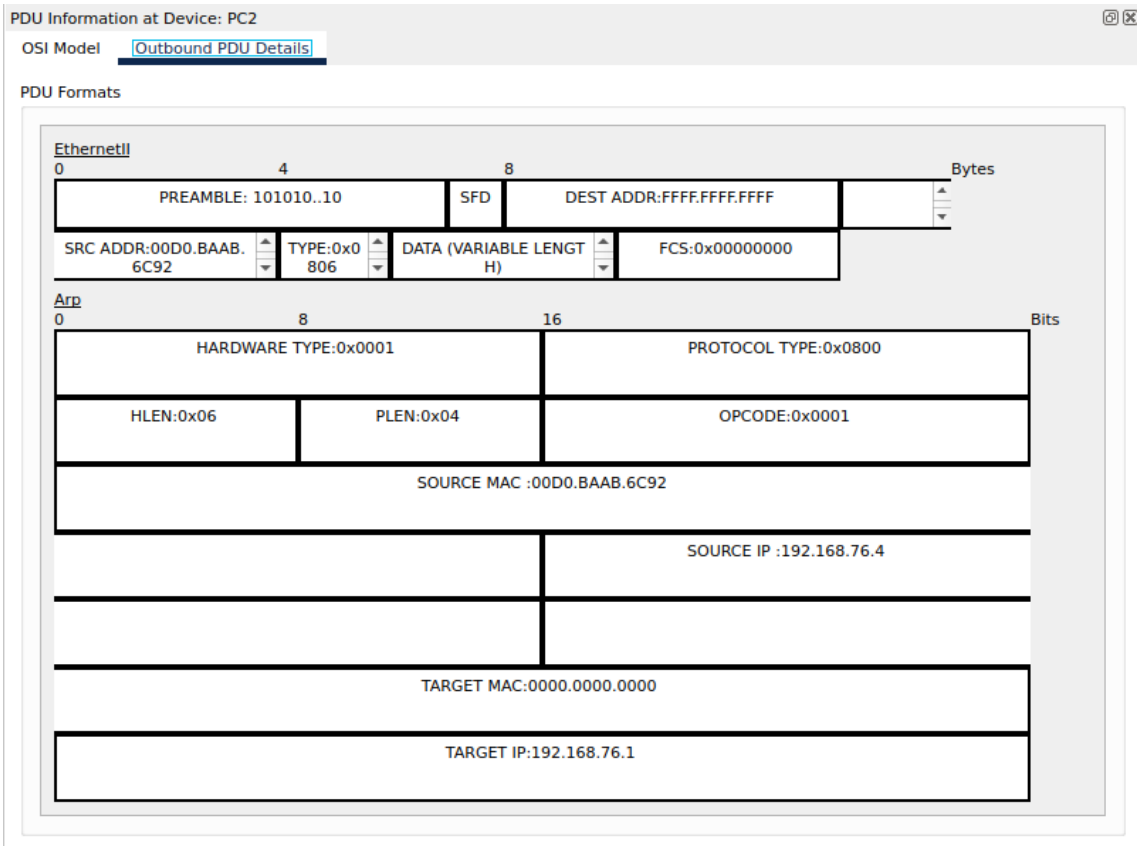
After creating the network, we will randomly take a PC and will try to ping a PC on the other subnet.

Pinging PC2 to PC5:



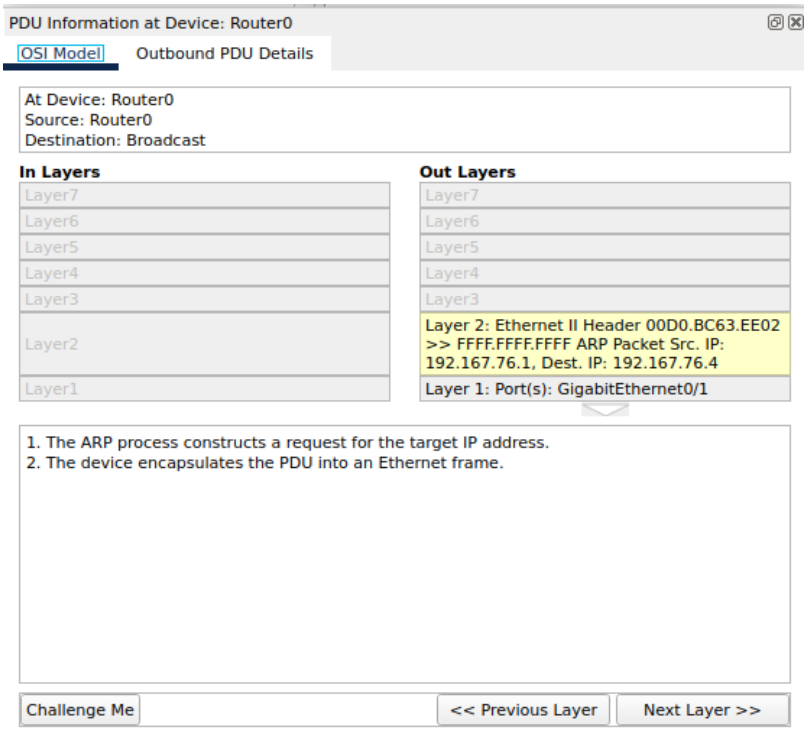
After running on the simulation, we will take a look at the PDU information of the PC.

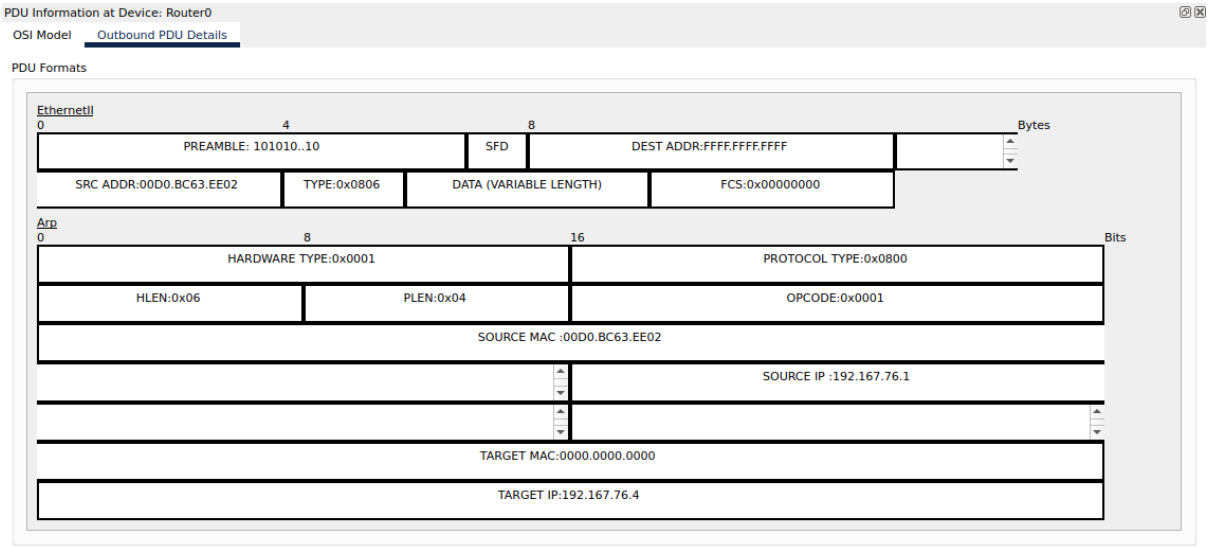




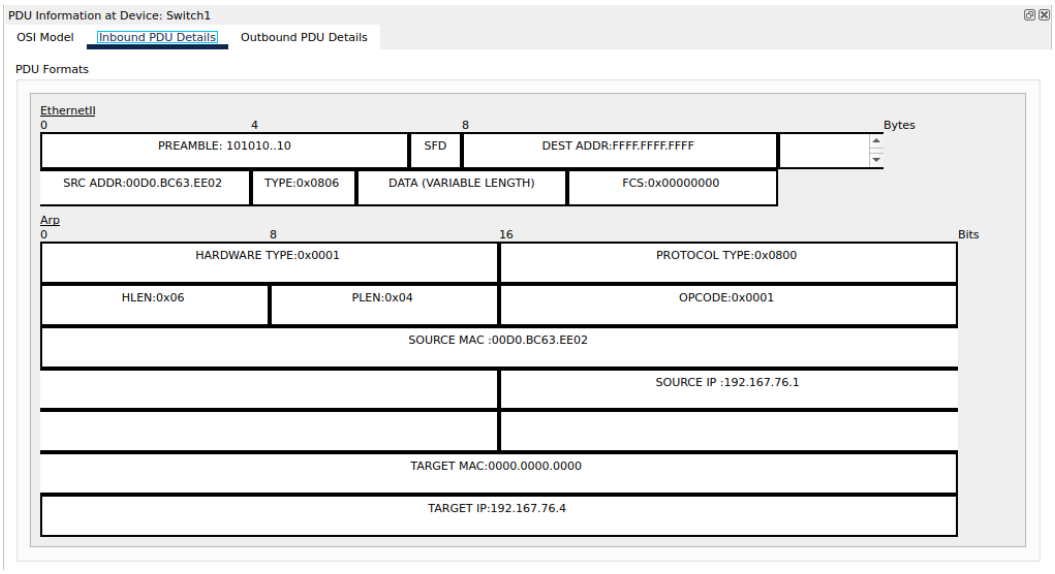
Query is being sent from PC 2 and from screenshot above it can be seen that destination MAC address is unknown. It is an ARP broadcast frame.

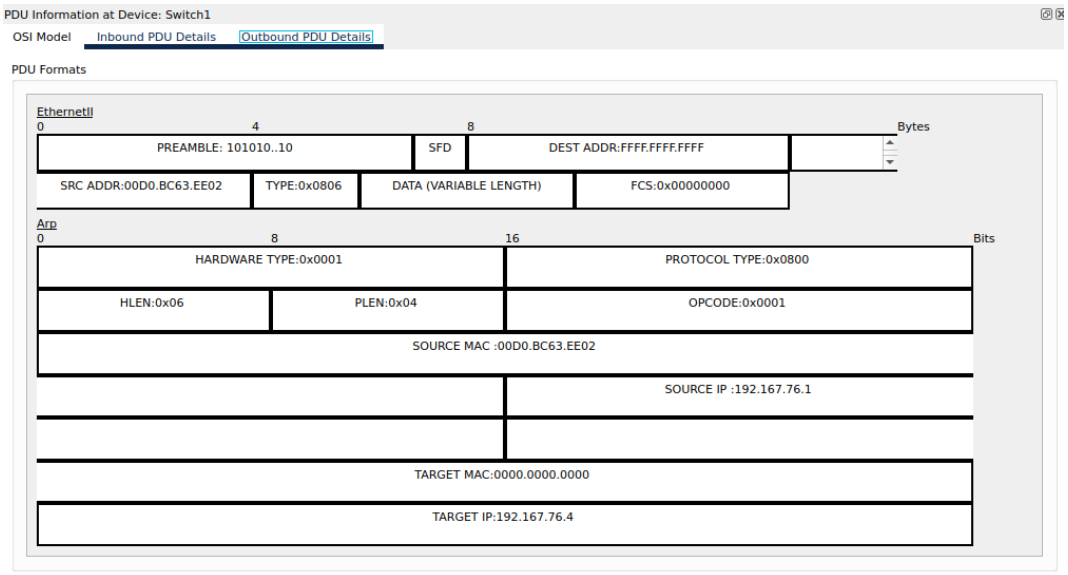
Query is being forwarded to PC5 from PC2 by router as seen from the screenshots below



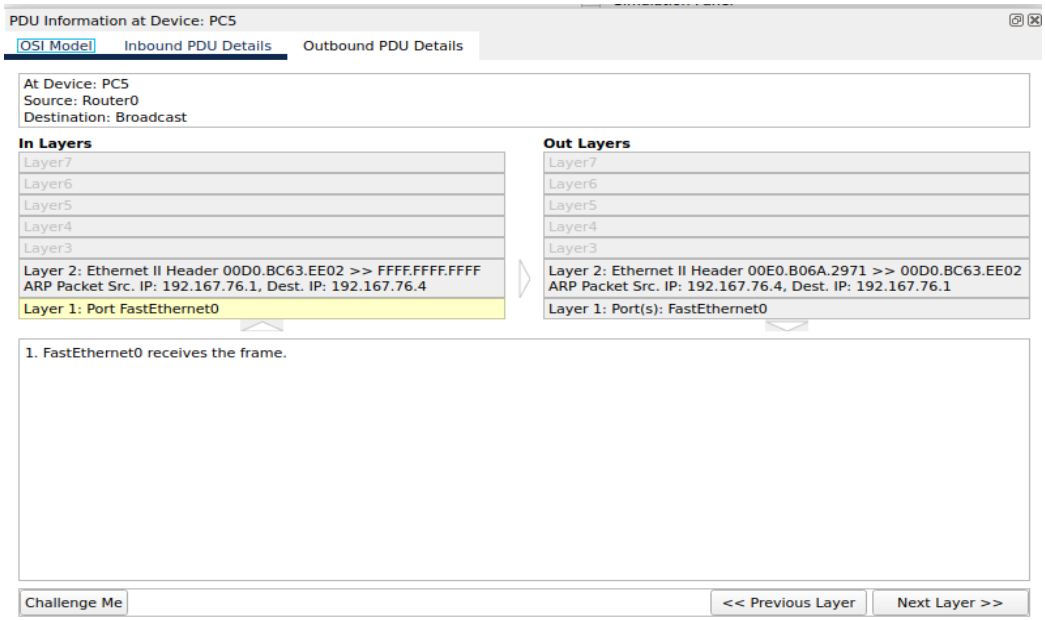


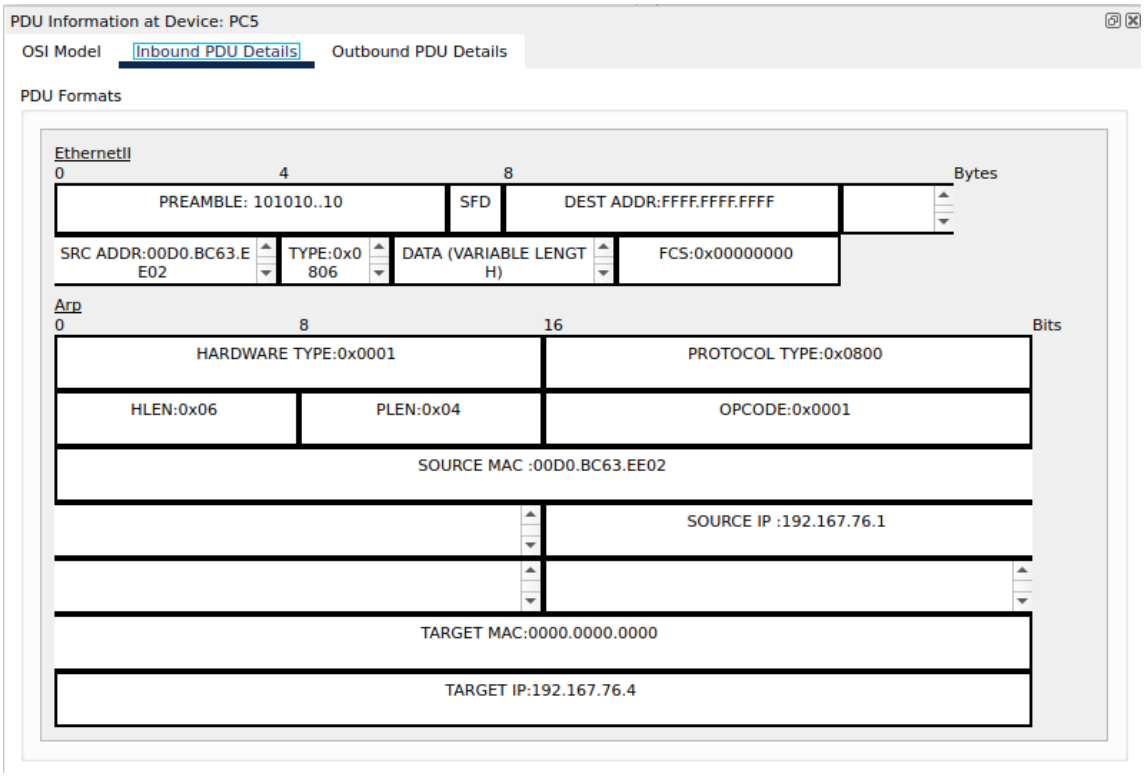
Request reaches the switch 1 where it will be given the destination MAC address

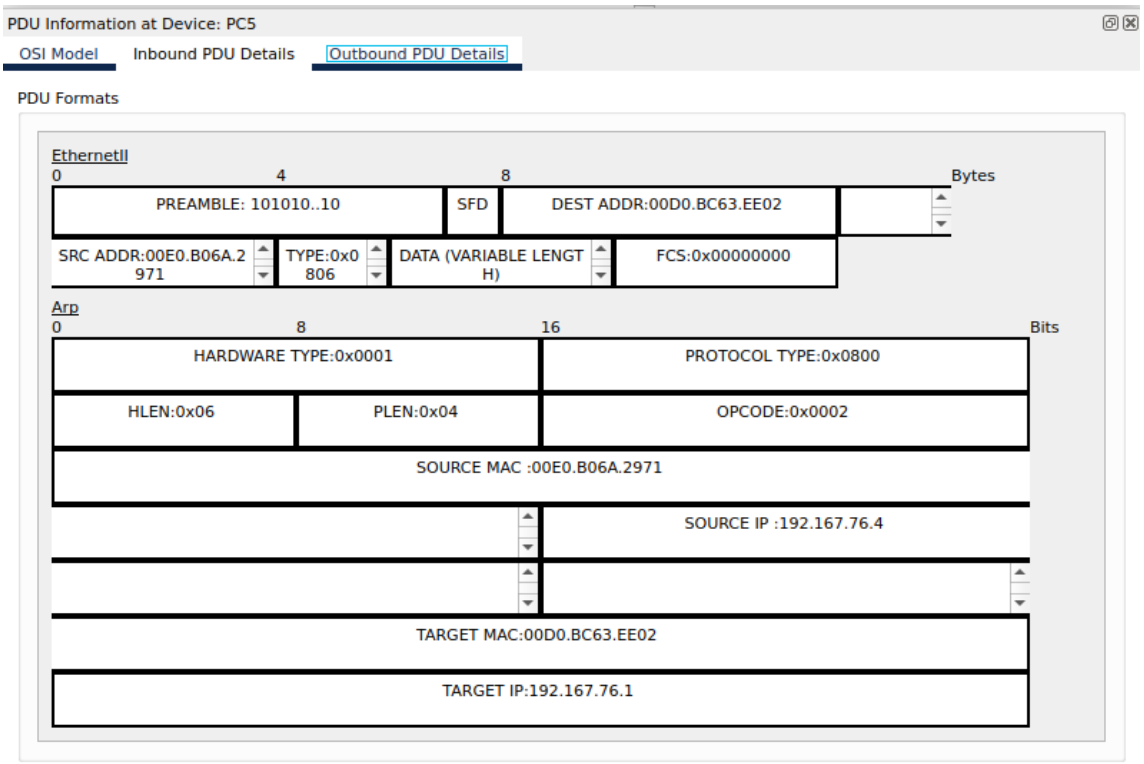




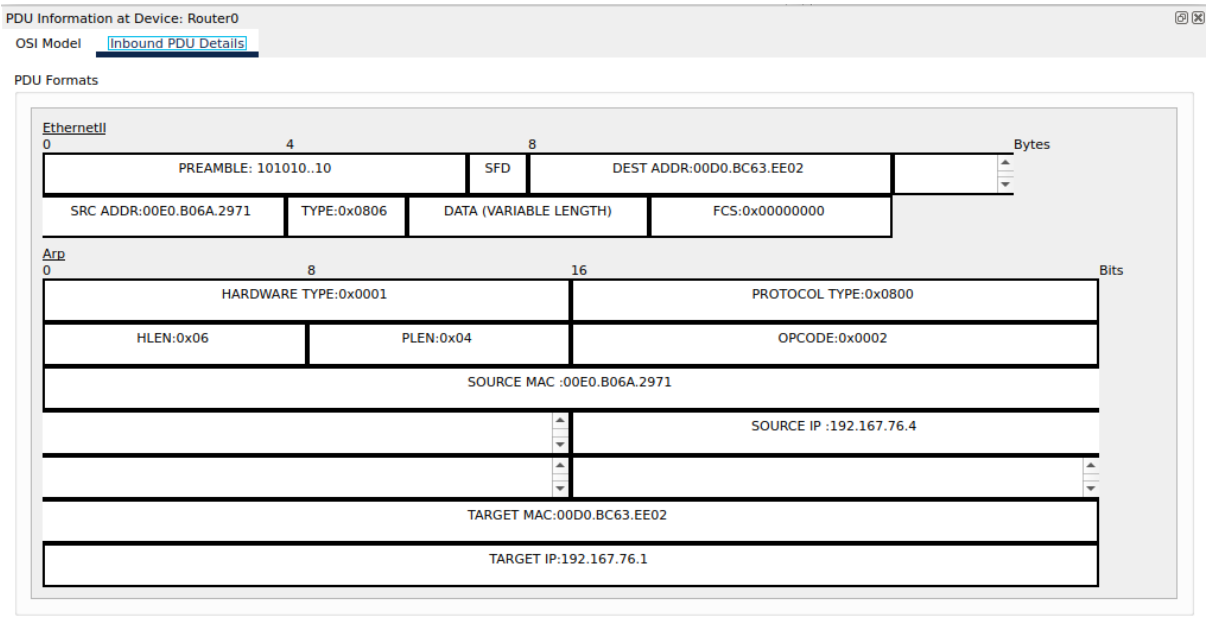
ARP reply is given by PC5 as shown below



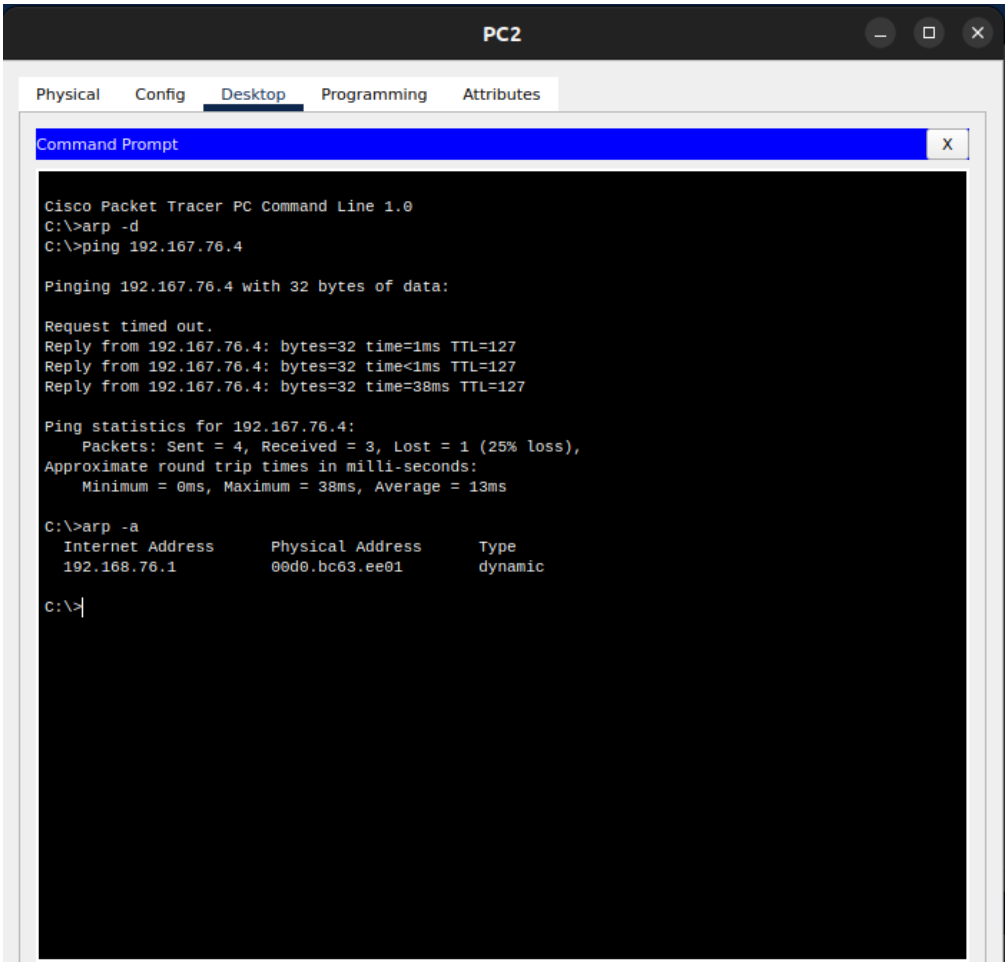




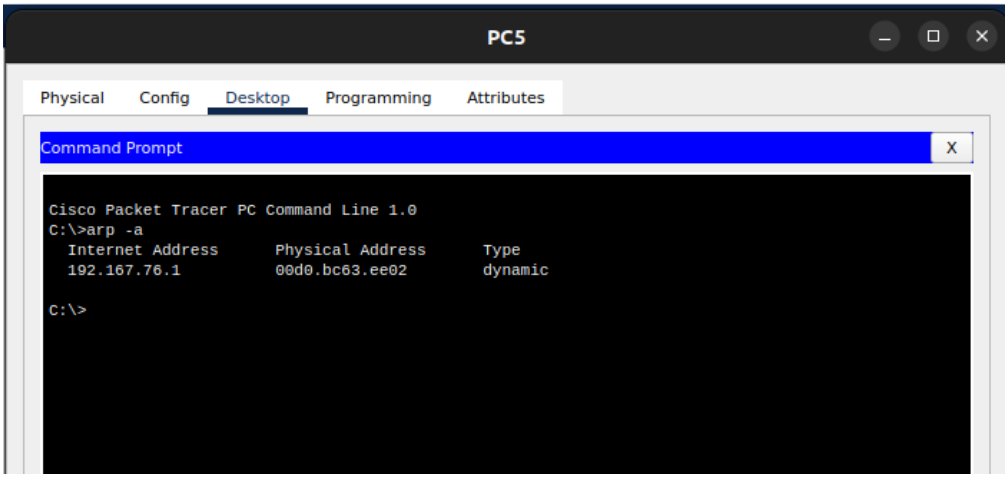
Finally, the reply will be received by router and then routing will take place as the destination MAC address will be mapped to source PC



ARP Table at the source device



ARP Table at the end device



For other end device ARP table does not exist as ARP is not used with them for pinging process.

ARP Table on the router

```
Router>enable
Router#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.167.76.1            -   00D0.BC63.EE02  ARPA   GigabitEthernet0/1
Internet  192.167.76.2            8   0060.2F51.5705  ARPA   GigabitEthernet0/1
Internet  192.167.76.4            7   00E0.B06A.2971  ARPA   GigabitEthernet0/1
Internet  192.168.76.1            -   00D0.BC63.EE01  ARPA   GigabitEthernet0/0
Internet  192.168.76.2            8   0040.0B19.D896  ARPA   GigabitEthernet0/0
Internet  192.168.76.4            7   00D0.BAAB.6C92  ARPA   GigabitEthernet0/0
Router#
```

Copy Paste

Mac – Address – Table – SWITCH_1

Switch1

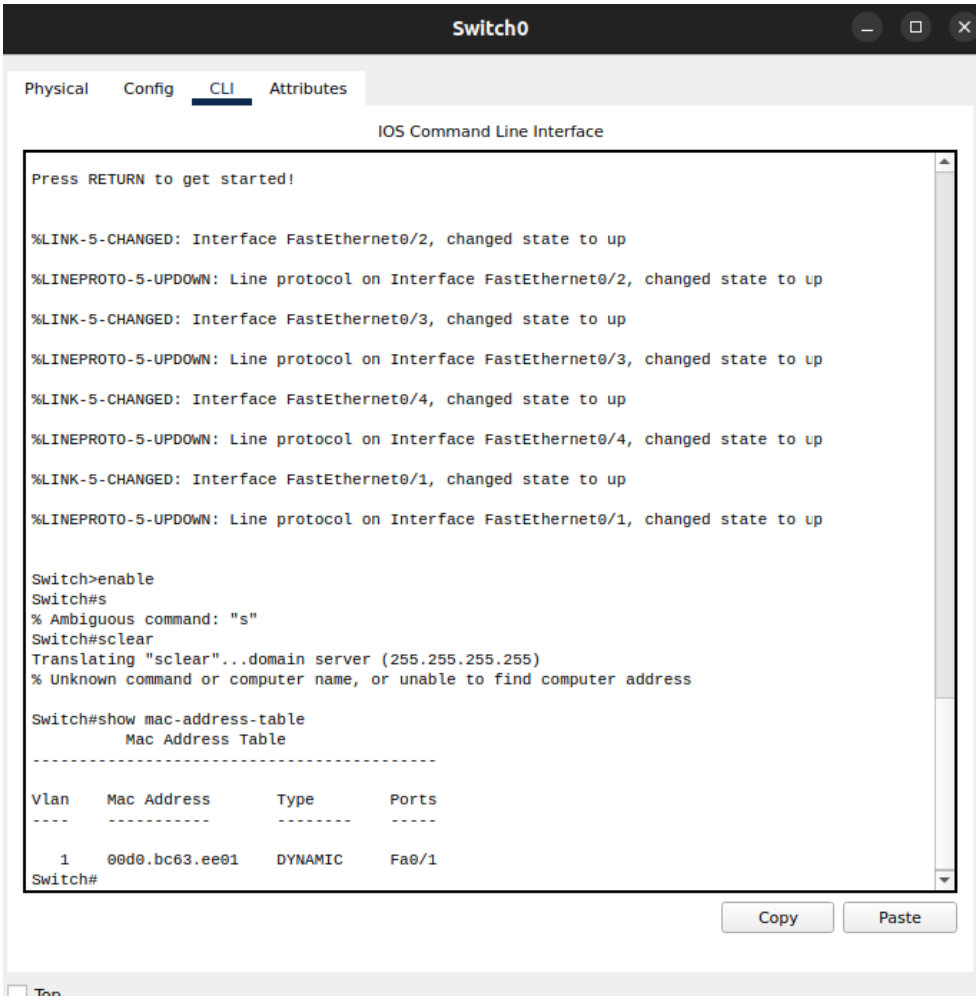
Physical Config CLI Attributes

IOS Command Line Interface

```
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by mnguyen



Press RETURN to get started!


%LINK-5-CHANGED: Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up


Switch>enable
Switch#show arp

Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    00d0.bc63.ee02    DYNAMIC     Fa0/1
Switch#
```

Copy Paste

Mac – Address – Table for SWITCH 0

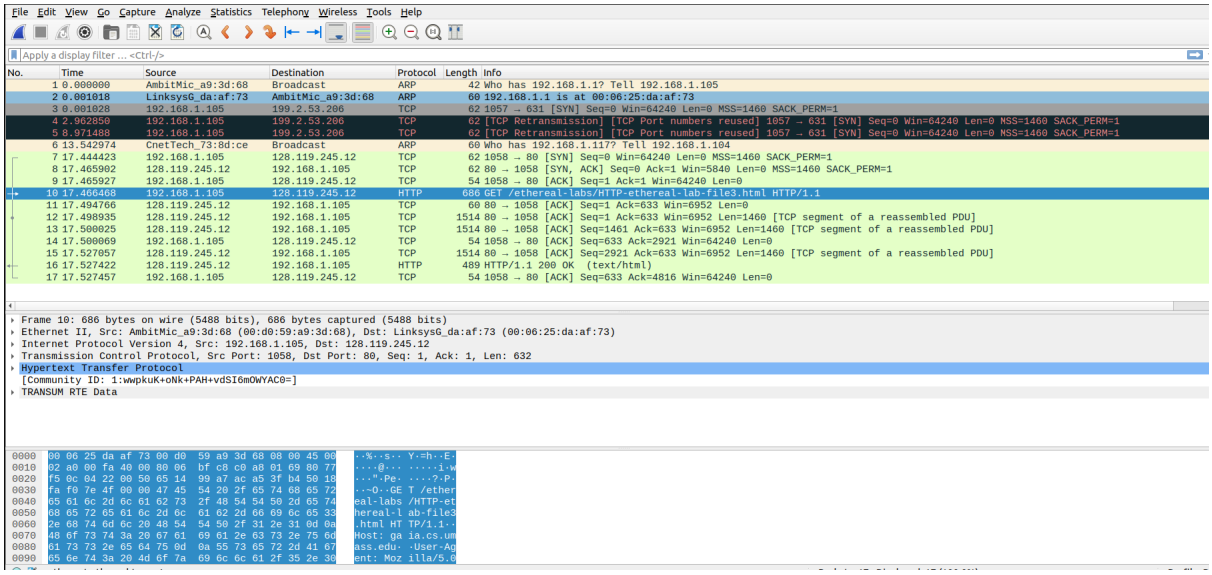


Link: [For CPT file]

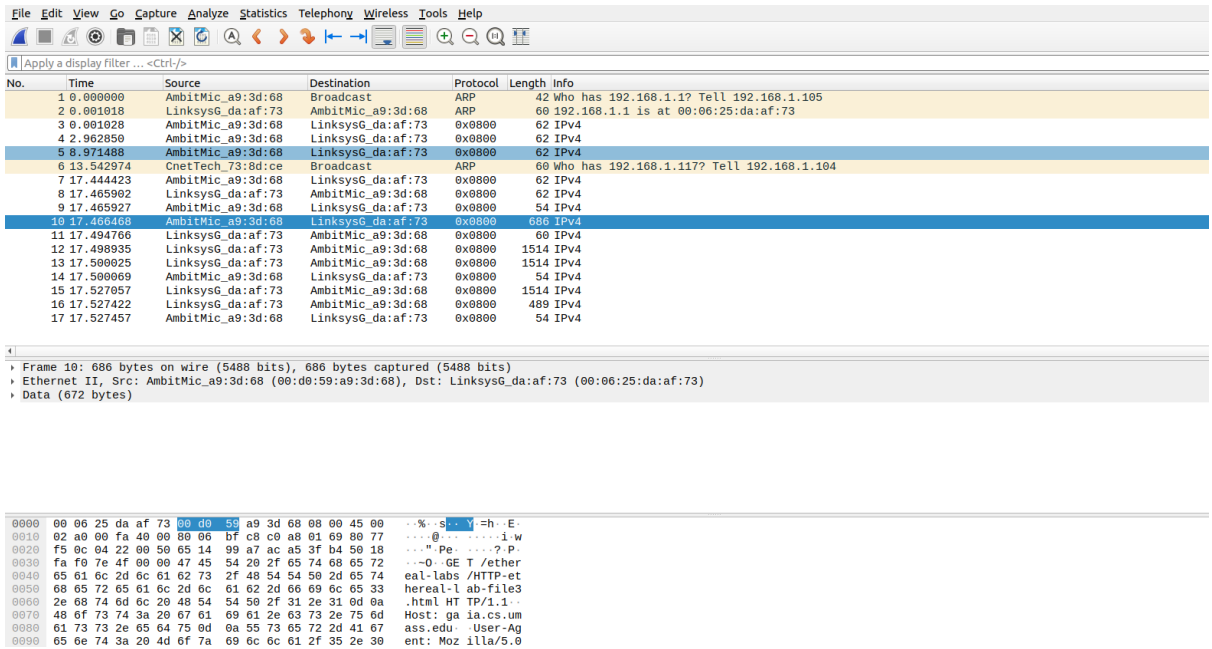
WireShark

For ETHERNET:

Capture Packet (Request):



Window with information below IP layer of the request:



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

Ans. (00:d0:59:a9:3d:68) is the address of the computer.

2. What is the 48-bit destination address in the Ethernet frame?

Ans. It is address of the router (LinkSysG) and the address is (00:06:25:da:af:73)

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

Ans. The hexadecimal frame type field in the ethernet header of this packet is 0x0800. It indicates that the upper layer protocol is Internet Protocol version 4 (IPv4).

4. How many bytes from the very start of the Ethernet frame does the ASCII “G” in “GET” appear in the Ethernet frame?

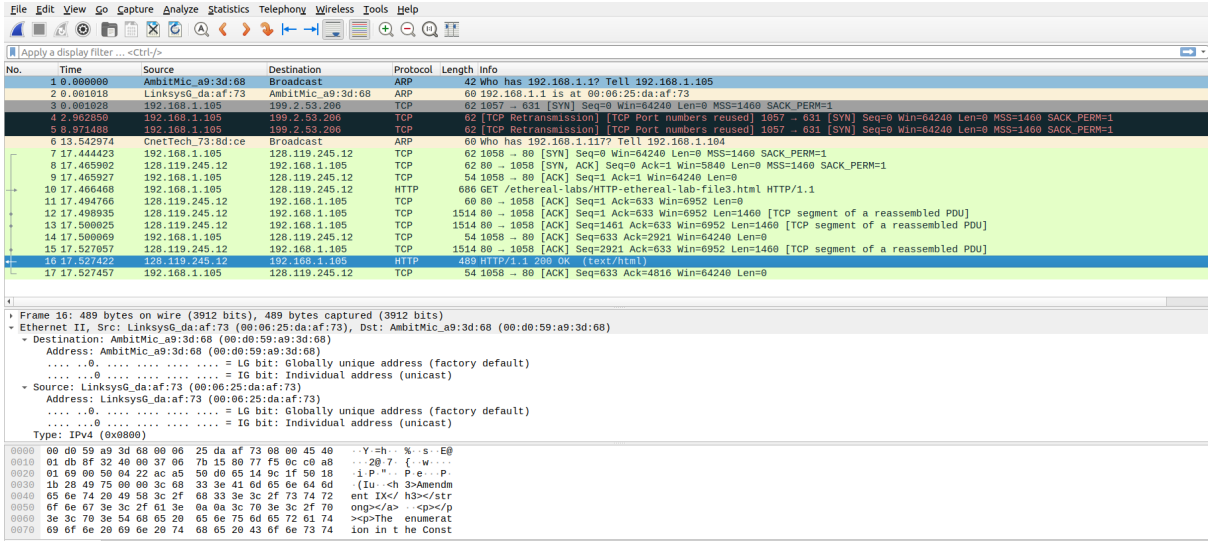
Ans. After 54 bytes from the very start of the ethernet frame the ASCII “G” appears,

The ethernet frame (first 14 bytes containing destination address, source address, and frame type)

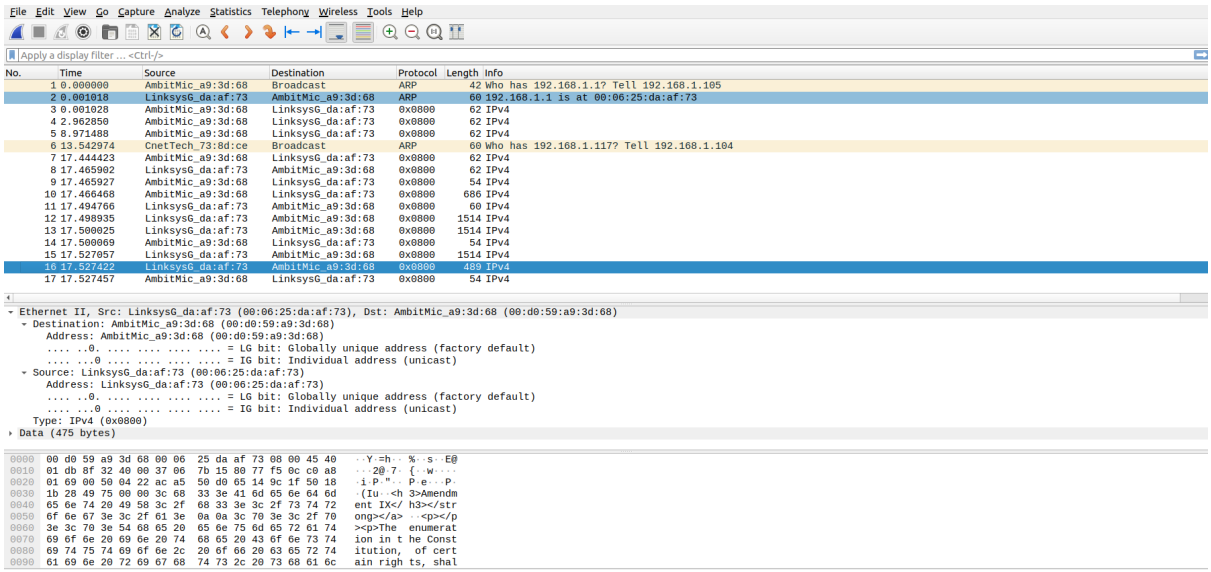
The IP header (20 bytes)

The TCP header (20 bytes) {Can be seen from the screenshot above}

Capture Packet (Response):



Window with information below IP layer of the response:



5. What is the value of the Ethernet source address? Is this the address of your computer, or of searched domain (Hint: the answer is no). What device has this as its Ethernet address?

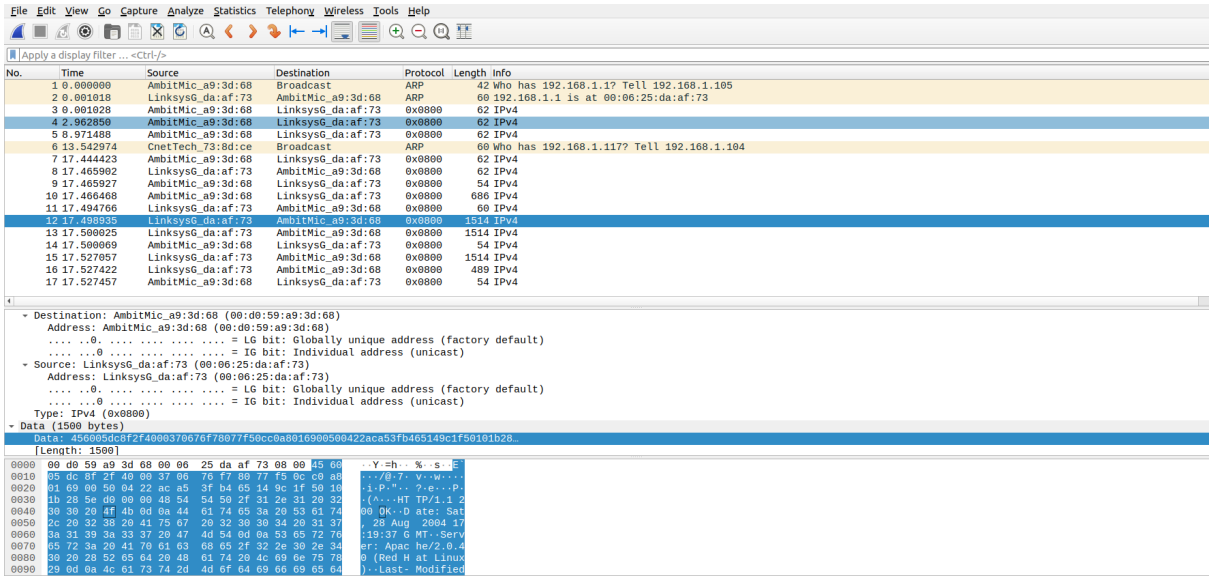
Ans. The source address of ethernet is (00:06:25:da:af:73) which is address of the router.

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

Ans. The destination address of ethernet is (00:d0:59:a9:3d:68). Yes, it the ethernet address of computer.

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

Ans. The hexadecimal frame type field in the ethernet header of this packet is 0x0800. It indicates that the upper layer protocol is Internet Protocol version 4 (IPv4).



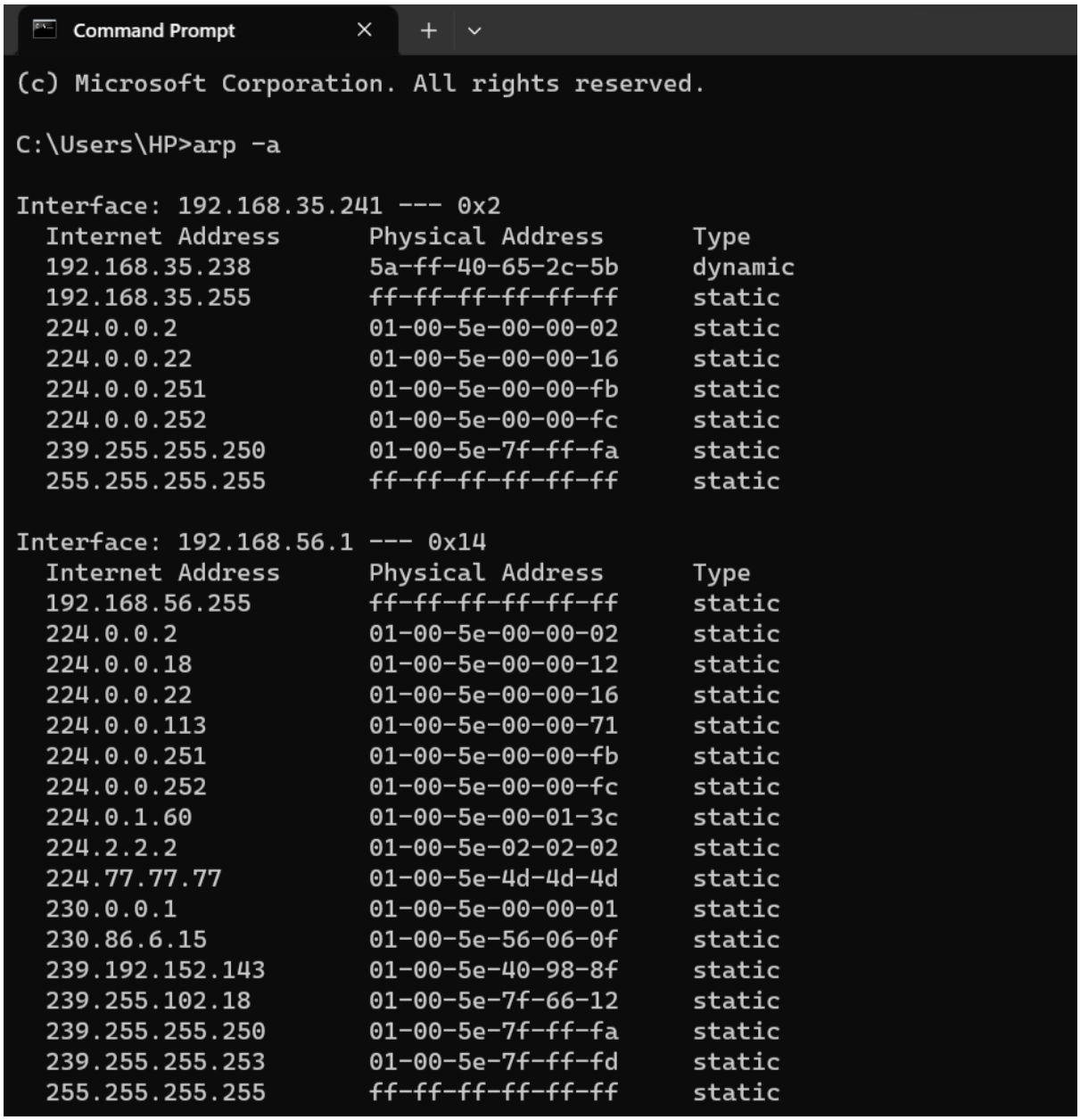
8. How many bytes from the very start of the Ethernet frame does the ASCII “O” in“OK” (i.e., the HTTP response code) appear in the Ethernet frame?

Ans. There are 65 bytes before the “O” (or “O” appears as the 66th byte). These bytes include the ethernet frame, the IP header, the TCP header, and some HTTP preamble text.

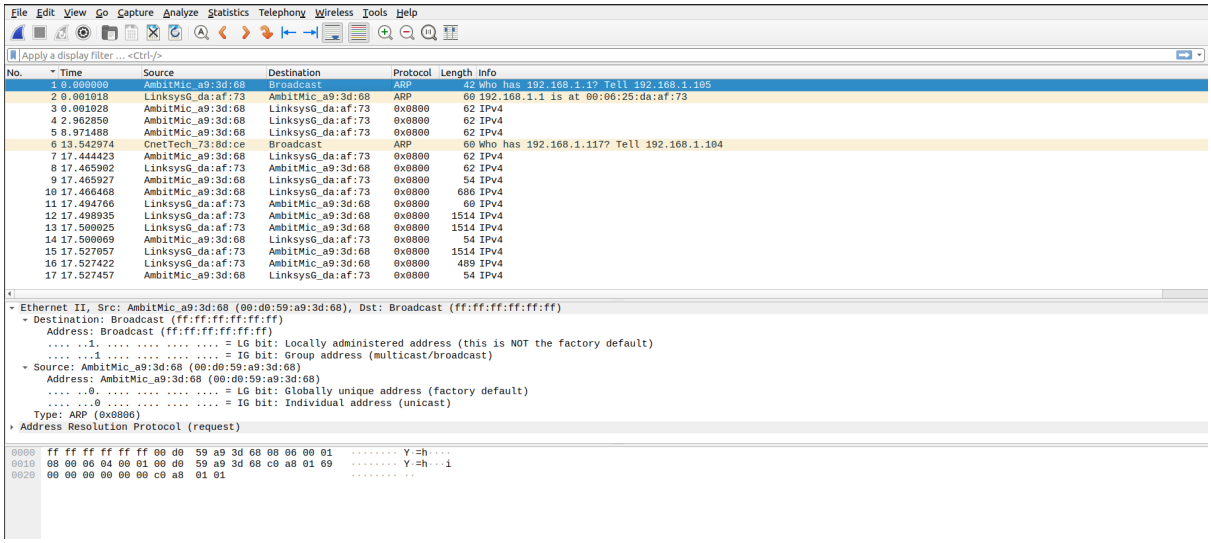
For ARP Protocol

9. Write down the contents of your computer's ARP cache. What is the meaning of each column value?

Ans.



The Internet Address column contains the IP address, the Physical Address column contains the MAC address, and the type indicates the IP protocol type.



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

Ans. The hex value for the source address is 00:d0:59:a9:3d:68. The hex value for the destination address is ff:ff:ff:ff:ff:ff, the broadcast address.

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

Ans. The hex value for the two byte Ethernet frame is ARP (0x0806), the corresponding upper layer protocol is ARP.

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

Ans. The ARP opcode field begins 6 bytes (48 bits) from the beginning of the ARP frame. Since the Ethernet frame (consisting of 6-byte source and 6-byte destination MAC addresses, as well as 2-byte Frame type) is 14 bytes long, the opcode appears 20 bytes from the start of the packet.

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

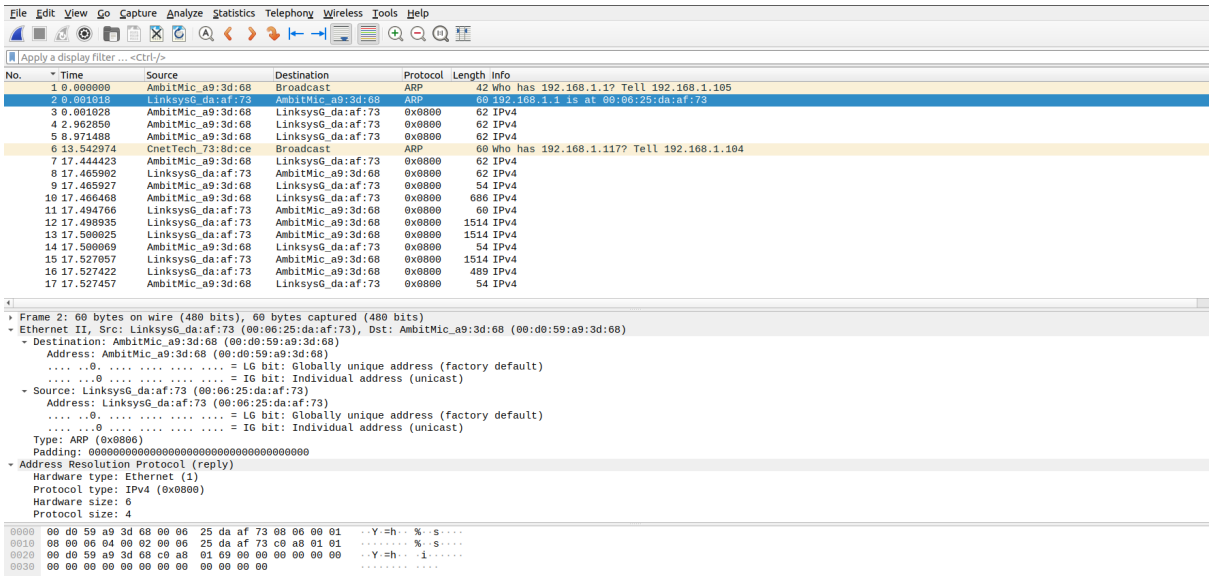
Ans. The hex value for opcode field withing the ARP-payload of the request is 0x0001, for request.

c) Does the ARP message contain the IP address of the sender?

Ans. Yes, according to above figure, the IP address of the sender is 192.168.1.105.

d) Where in the ARP request does the “question” appear – the Ethernet address of the machine whose corresponding IP address is being queried?

Ans. The field “Target MAC address” is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.1.105) is being queried.



13. Now find the ARP reply that was sent in response to the ARP request.

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

Ans. 20 Bytes

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. The hex value for opcode field withing the ARP-payload of the request is 0x0002, for reply.

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. The answer to the earlier ARP request appears in the “Sender MAC address” field, which contains the Ethernet address 00:06:25:da:af:73 for the sender with IP address 192.168.1.1.

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

Ans. The hex value for the source address is 00:06:25:da:af:73 and for the destination is 00:d0:59:a9:3d:68 .

15. The first and second ARP packets in this trace correspond to an ARP request sent by the computer running Wireshark, and the ARP reply sent to the computer running Wireshark by the computer with the ARP-requested Ethernet address. But there is yet another computer on this network, as indicated by packet 6 – another ARP request. Why is there no ARP reply?

Ans. There is no reply in this trace, because we are not at the machine that sent the request. The ARP request is broadcast, but the ARP reply is sent back directly to the sender’s Ethernet address.

Extra Credit

1. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

Ans. After entering wrong entry, one will not be able to ping the server IP and can not access the server through a web browser.
To get the connection back, one has to use arp -d command for clearing the manually added entry in arp cache table.

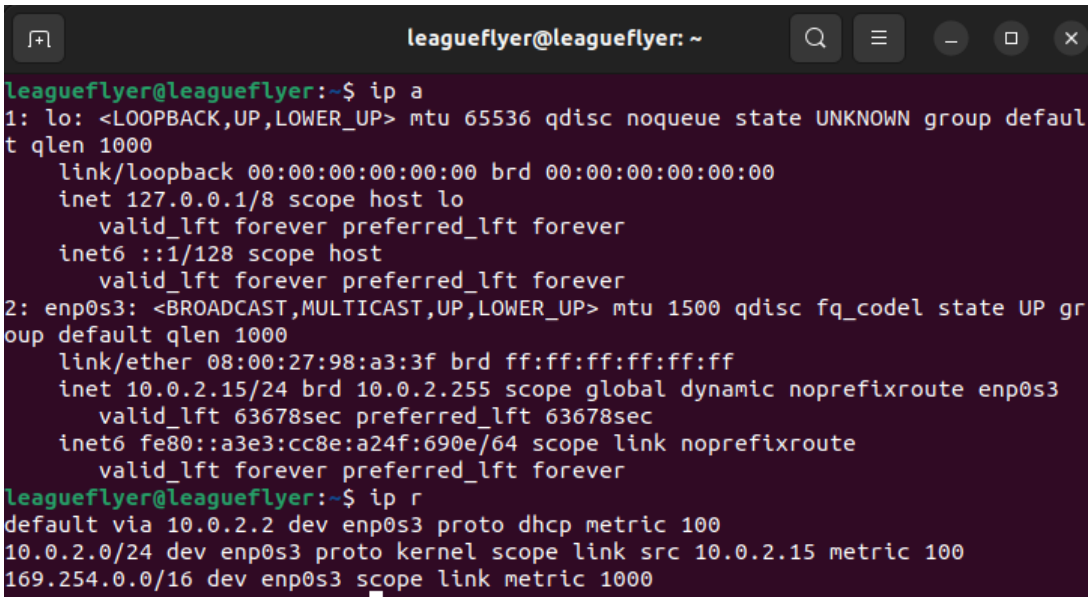
2. What is the default amount of time that an entry remains in your ARP cache before being removed. You can determine this empirically (by monitoring the cache contents) or by looking this up in your operation system documentation.

Ans. According to the document from Microsoft http://support.microsoft.com/kb/949589 , there is no default amount of time that an entry remains in the ARP cache now. In the new Windows Vista TCP/IP stack implementation, hosts create the neighbor cache entries when there is no matching entry in the neighbor cache. ARP cache entry for IPv4 is an example of a neighbor cache entry. After the entry is successfully created in the neighbor cache, the entry may change to the "Reachable" state if the entry meets certain conditions. If the entry is in the "Reachable" state, Windows Vista TCP/IP hosts do not send ARP requests to the network.

Therefore, Windows Vista TCP/IP hosts use the information in the cache. If an entry is not used, and it stays in the "Reachable" state for longer than its "Reachable Time" value, the entry changes to the "Stale" state. If an entry is in the "Stale" state, the Windows Vista TCP/IP host must send an ARP request to reach that destination

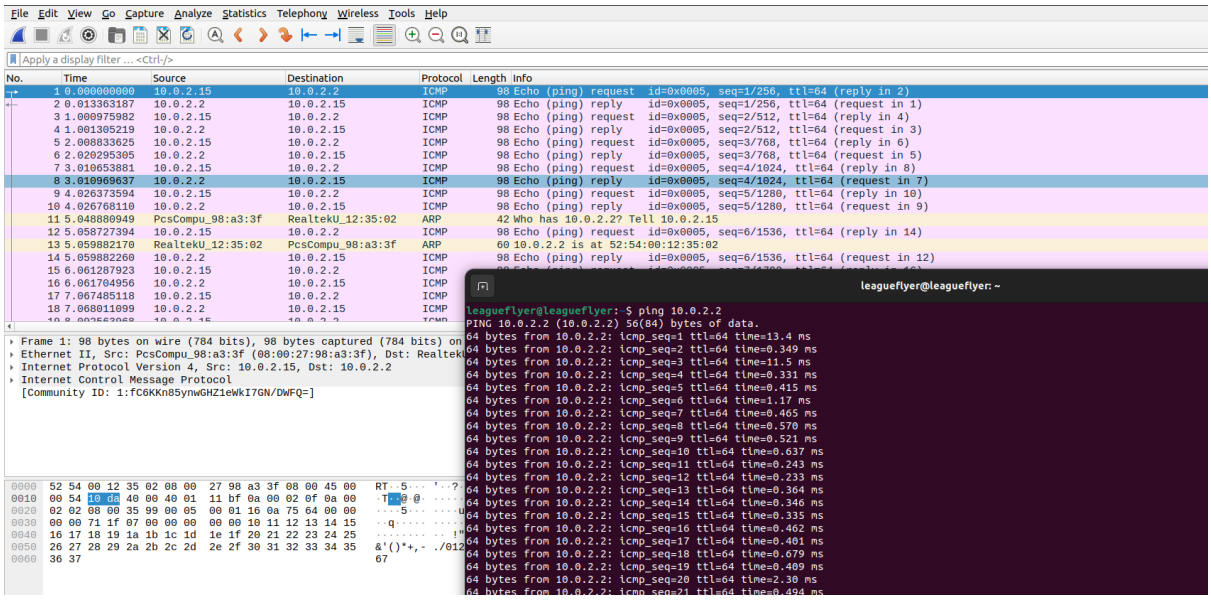
To do

IP address of the device



Pinging and Capturing packets for

a) Gateway Router



Header info in the layers

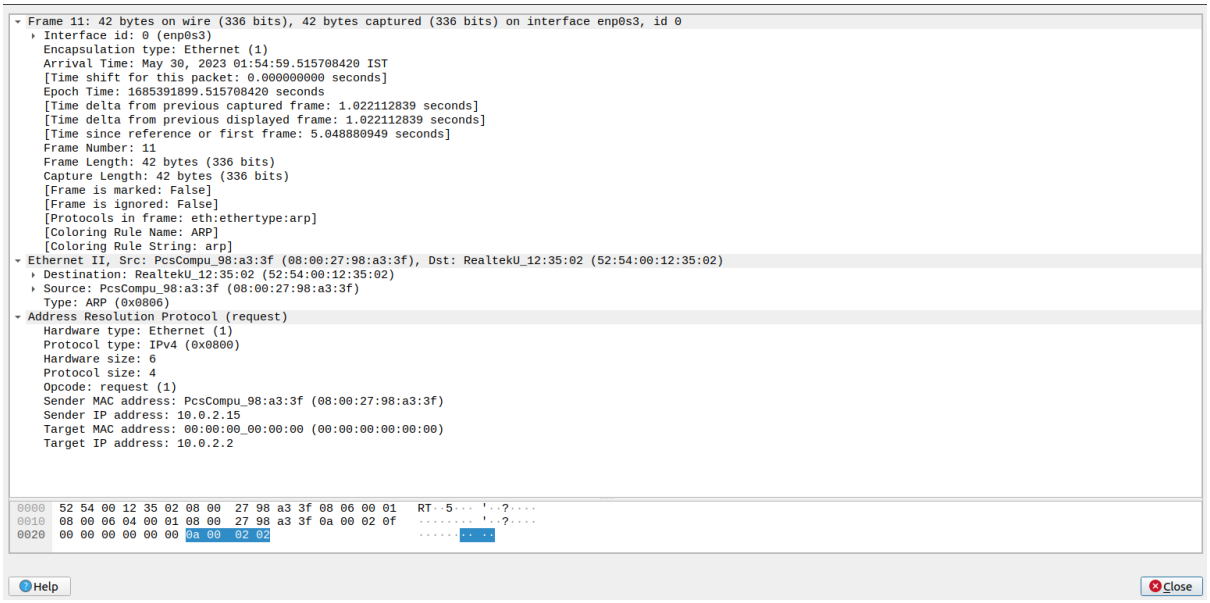
ICMP

```
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
  Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: May 30, 2023 01:54:54.466827471 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1685391894.466827471 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 98 bytes (784 bits)
    Capture Length: 98 bytes (784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: PcsCompu_98:a3:3f (08:00:27:98:a3:3f), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
  Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
  Source: PcsCompu_98:a3:3f (08:00:27:98:a3:3f)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x10da (4314)
  Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x11bf [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 10.0.2.2
0000  52 54 00 12 35 02 08 00  27 98 a3 3f 08 00 45 00   RT··5··· '··?··E·
0010  00 54 10 da 40 00 40 01  11 bf 0a 00 02 0f 0a 00   ·T··@·@· ········
```

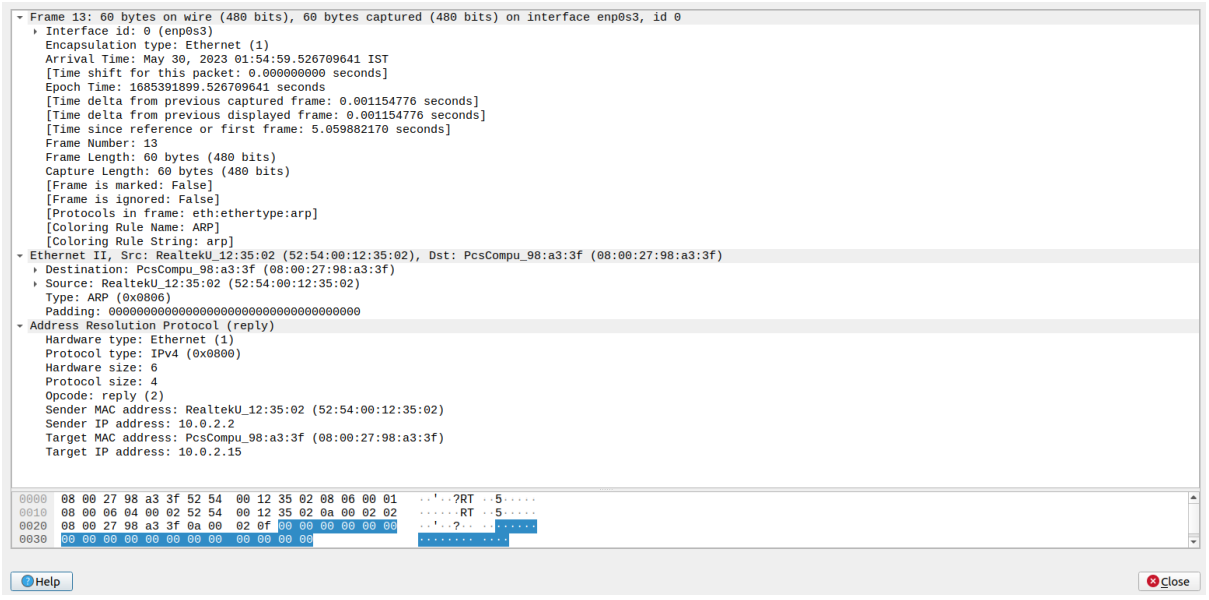
```
Frame 2: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
  Interface id: 0 (enp0s3)
    Encapsulation type: Ethernet (1)
    Arrival Time: May 30, 2023 01:54:54.480190658 IST
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1685391894.480190658 seconds
    [Time delta from previous captured frame: 0.013363187 seconds]
    [Time delta from previous displayed frame: 0.013363187 seconds]
    [Time since reference or first frame: 0.013363187 seconds]
    Frame Number: 2
    Frame Length: 98 bytes (784 bits)
    Capture Length: 98 bytes (784 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_98:a3:3f (08:00:27:98:a3:3f)
  Destination: PcsCompu_98:a3:3f (08:00:27:98:a3:3f)
  Source: RealtekU_12:35:02 (52:54:00:12:35:02)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.2, Dst: 10.0.2.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xacbf (44223)
  Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x75d9 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.2
    Destination Address: 10.0.2.15
0000  08 00 27 98 a3 3f 52 54  00 12 35 02 08 00 45 00   ··'··?RT ··5···E·
0010  00 54 ac bf 40 00 40 01  75 d9 0a 00 02 02 0a 00   ·T··@·@· u·······
0020  02 0f 00 00 3d 99 00 05  00 01 16 0a 75 64 00 00   ····=··· ····ud··
```

Help Close

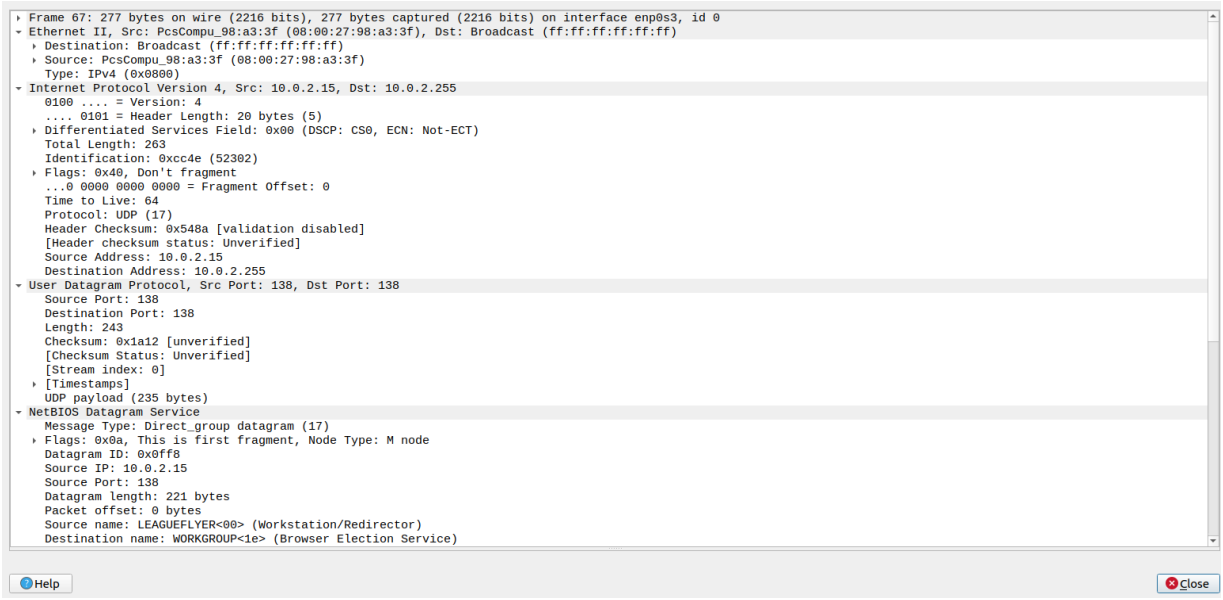
ARP (Request)

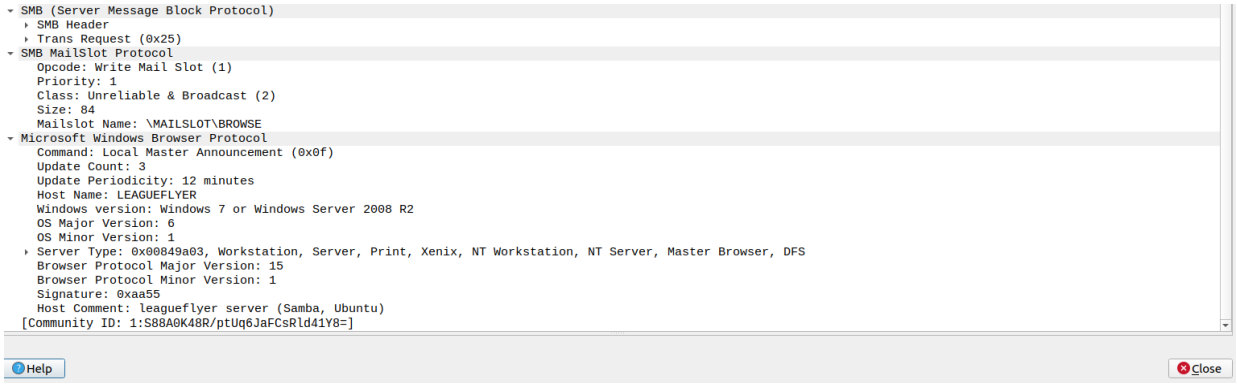


ARP (Reply)

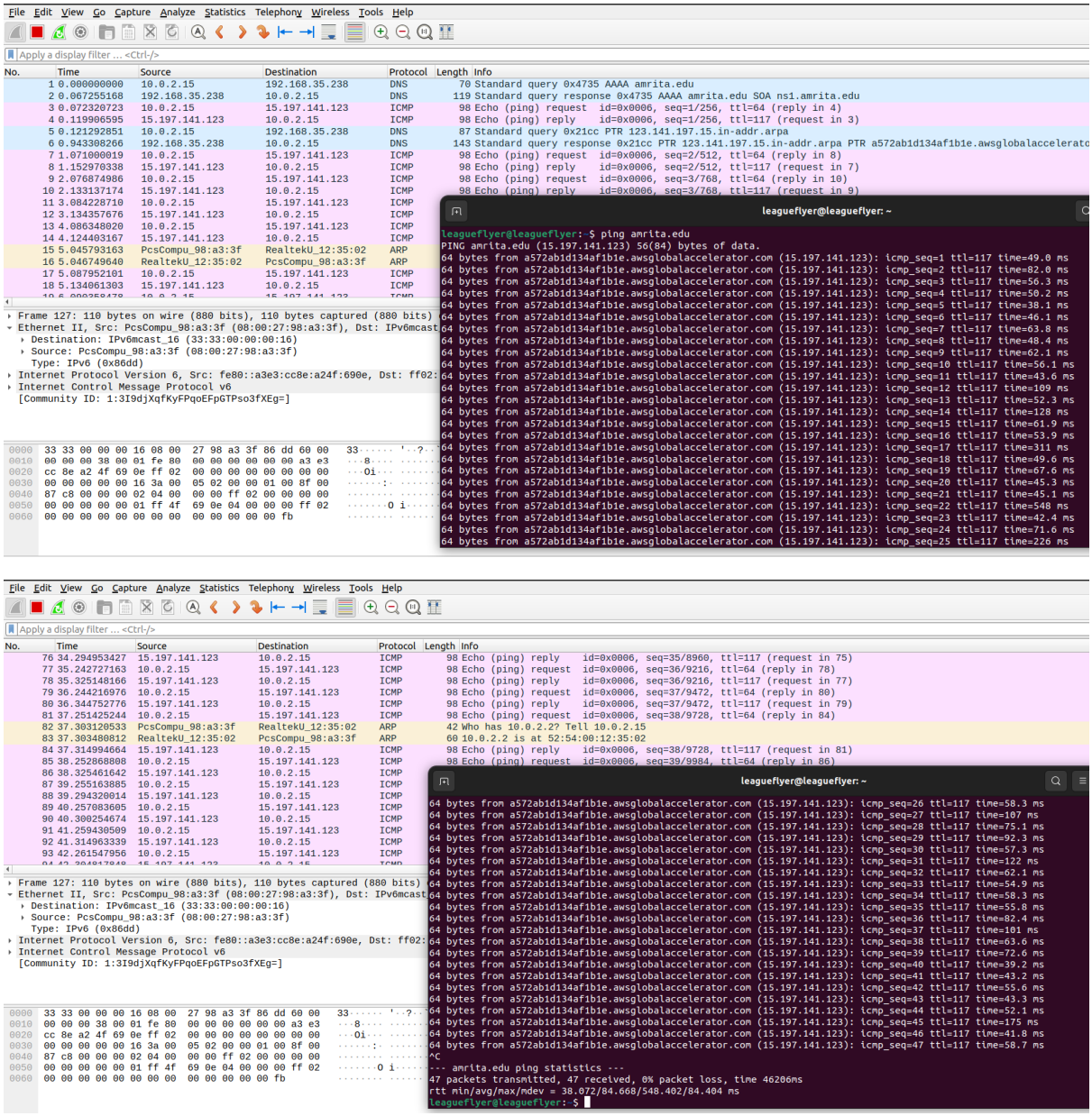


Browser


Frame 67: 277 bytes on wire (2216 bits), 277 bytes captured (2216 bits) on interface enp0s3, id 0
Ethernet II, Src: PcsCompu_98:a3:3f (08:00:27:98:a3:3f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: PcsCompu_98:a3:3f (08:00:27:98:a3:3f)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.255
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 263
Identification: 0xcc4e (52302)
Flags: 0x40, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: UDP (17)
Header Checksum: 0x548a [validation disabled]
[Header checksum status: Unverified]
Source Address: 10.0.2.15
Destination Address: 10.0.2.255
User Datagram Protocol, Src Port: 138, Dst Port: 138
Source Port: 138
Destination Port: 138
Length: 243
Checksum: 0x1a12 [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
[Timestamps]
UDP payload (235 bytes)
NetBIOS Datagram Service
Message Type: Direct_group datagram (17)
Flags: 0x0a, This is first fragment, Node Type: M node
Datagram ID: 0x0ff8
Source IP: 10.0.2.15
Source Port: 138
Datagram length: 221 bytes
Packet offset: 0 bytes
Source name: LEAGUEFLYER<00> (Workstation/Redirector)
Destination name: WORKGROUP<1e> (Browser Election Service)
Help
Close


SMB (Server Message Block Protocol)
SMB Header
Trans Request (0x25)
SMB MailSlot Protocol
Opcode: Write Mail Slot (1)
Priority: 1
Class: Unreliable & Broadcast (2)
Size: 84
Mailslot Name: \MAILSLOT\BROWSE
Microsoft Windows Browser Protocol
Command: Local Master Announcement (0x0f)
Update Count: 3
Update Periodicity: 12 minutes
Host Name: LEAGUEFLYER
Windows version: Windows 7 or Windows Server 2008 R2
OS Major Version: 6
OS Minor Version: 1
Server Type: 0x00849a03, Workstation, Server, Print, Xenix, NT Workstation, NT Server, Master Browser, DFS
Browser Protocol Major Version: 15
Browser Protocol Minor Version: 1
Signature: 0xaa55
Host Comment: leagueflyer server (Samba, Ubuntu)
[Community ID: 1:S88A0K48R/ptUq6JaFCsRld41Y8=]
Help
Close

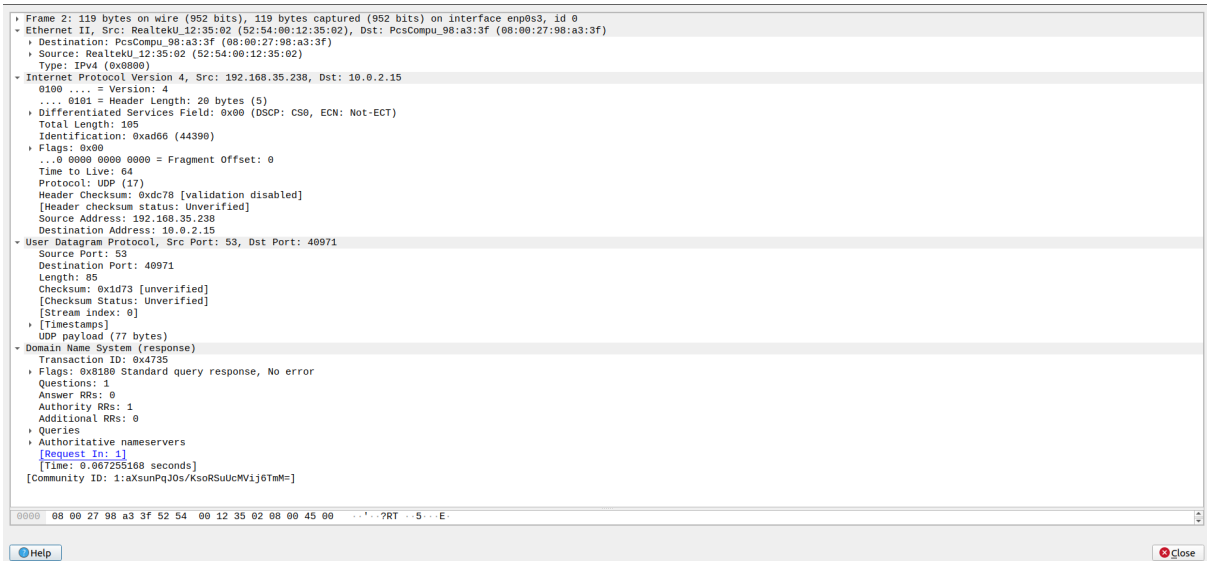
b) Amrita.edu


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 10.0.2.15 192.168.35.238 DNS 70 Standard query 0x4735 AAAA amrita.edu
2 0.067255168 192.168.35.238 10.0.2.15 DNS 119 Standard query response 0x4735 AAAA amrita.edu SOA ns1.amrita.edu
3 0.072320723 10.0.2.15 15.197.141.123 ICMP 98 Echo (ping) request id=0x0006, seq=1/256, ttl=64 (reply in 4)
4 0.119906595 15.197.141.123 10.0.2.15 ICMP 98 Echo (ping) reply id=0x0006, seq=1/256, ttl=117 (request in 3)
5 0.121292851 10.0.2.15 192.168.35.238 DNS 87 Standard query 0x21cc PTR 123.141.197.15.in-addr.arpa
6 0.943308266 192.168.35.238 10.0.2.15 DNS 143 Standard query response 0x21cc PTR 123.141.197.15.in-addr.arpa PTR a572ab1d134af1b1e.awsglobalaccelerato
7 1.071000019 10.0.2.15 15.197.141.123 ICMP 98 Echo (ping) request id=0x0006, seq=2/512, ttl=64 (reply in 8)
8 1.152970338 15.197.141.123 10.0.2.15 ICMP 98 Echo (ping) reply id=0x0006, seq=2/512, ttl=117 (request in 7)
9 2.076874986 10.0.2.15 15.197.141.123 ICMP 98 Echo (ping) request id=0x0006, seq=3/768, ttl=64 (reply in 10)
10 2.133137174 15.197.141.123 10.0.2.15 ICMP 98 Echo (ping) reply id=0x0006, seq=3/768, ttl=117 (request in 9)
11 3.084228710 10.0.2.15 15.197.141.123 ICMP
12 3.134357676 15.197.141.123 10.0.2.15 ICMP
13 4.086348020 10.0.2.15 15.197.141.123 ICMP
14 4.124403167 15.197.141.123 10.0.2.15 ICMP
15 5.045793163 PcsCompu_98:a3:3f RealtekU_12:35:02 ARP
16 5.046749640 RealtekU_12:35:02 PcsCompu_98:a3:3f ARP
17 5.087952101 10.0.2.15 15.197.141.123 ICMP
18 5.134061303 15.197.141.123 10.0.2.15 ICMP
Frame 127: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: PcsCompu_98:a3:3f (08:00:27:98:a3:3f), Dst: IPv6mcast
Destination: IPv6mcast_16 (33:33:00:00:00:16)
Source: PcsCompu_98:a3:3f (08:00:27:98:a3:3f)
Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: fe80::a3e3:cc8e:a24f:690e, Dst: ff02:
Internet Control Message Protocol v6
[Community ID: 1:3I9djXqfKyFPqoEFpGTPso3fXEg=]
0000 33 33 00 00 00 16 08 00 27 98 a3 3f 86 dd 60 00 33 ..... '..?..
0010 00 00 00 38 00 01 fe 80 00 00 00 00 00 00 a3 e3 ...8 .....
0020 cc 8e a2 4f 69 0e ff 02 00 00 00 00 00 00 00 00 ...Oi ...
0030 00 00 00 00 00 16 3a 00 05 02 00 00 01 00 8f 00 ..... :. .....
0040 87 c8 00 00 00 02 04 00 00 00 ff 02 00 00 00 00 ....
0050 00 00 00 00 00 01 ff 4f 69 0e 04 00 00 00 ff 02 ..... O i.....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 fb ....
leagueflyer@leagueflyer: ~
leagueflyer@leagueflyer:~$ ping amrita.edu
PING amrita.edu (15.197.141.123) 56(84) bytes of data.
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=1 ttl=117 time=49.0 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=2 ttl=117 time=82.0 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=3 ttl=117 time=56.3 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=4 ttl=117 time=50.2 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=5 ttl=117 time=38.1 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=6 ttl=117 time=46.1 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=7 ttl=117 time=63.8 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=8 ttl=117 time=48.4 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=9 ttl=117 time=62.1 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=10 ttl=117 time=56.1 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=11 ttl=117 time=43.6 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=12 ttl=117 time=109 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=13 ttl=117 time=52.3 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=14 ttl=117 time=128 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=15 ttl=117 time=61.9 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=16 ttl=117 time=53.9 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=17 ttl=117 time=311 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=18 ttl=117 time=49.6 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=19 ttl=117 time=67.6 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=20 ttl=117 time=45.3 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=21 ttl=117 time=45.1 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=22 ttl=117 time=548 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=23 ttl=117 time=42.4 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=24 ttl=117 time=71.6 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=25 ttl=117 time=226 ms
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
76 34.294953427 15.197.141.123 10.0.2.15 ICMP 98 Echo (ping) reply id=0x0006, seq=35/8960, ttl=117 (request in 75)
77 35.242727163 10.0.2.15 15.197.141.123 ICMP 98 Echo (ping) request id=0x0006, seq=36/9216, ttl=64 (reply in 78)
78 35.325148166 15.197.141.123 10.0.2.15 ICMP 98 Echo (ping) reply id=0x0006, seq=36/9216, ttl=117 (request in 77)
79 36.244216976 10.0.2.15 15.197.141.123 ICMP 98 Echo (ping) request id=0x0006, seq=37/9472, ttl=64 (reply in 80)
80 36.344752776 15.197.141.123 10.0.2.15 ICMP 98 Echo (ping) reply id=0x0006, seq=37/9472, ttl=117 (request in 79)
81 37.251425244 10.0.2.15 15.197.141.123 ICMP 98 Echo (ping) request id=0x0006, seq=38/9728, ttl=64 (reply in 84)
82 37.303120533 PcsCompu_98:a3:3f RealtekU_12:35:02 ARP 42 Who has 10.0.2.2? Tell 10.0.2.15
83 37.303480812 RealtekU_12:35:02 PcsCompu_98:a3:3f ARP 60 10.0.2.2 is at 52:54:00:12:35:02
84 37.314994664 15.197.141.123 10.0.2.15 ICMP 98 Echo (ping) reply id=0x0006, seq=38/9728, ttl=117 (request in 81)
85 38.252868808 10.0.2.15 15.197.141.123 ICMP 98 Echo (ping) request id=0x0006, seq=39/9984, ttl=64 (reply in 86)
86 38.325461642 15.197.141.123 10.0.2.15 ICMP
87 39.255163885 10.0.2.15 15.197.141.123 ICMP
88 39.294320014 15.197.141.123 10.0.2.15 ICMP
89 40.257083605 10.0.2.15 15.197.141.123 ICMP
90 40.300254674 15.197.141.123 10.0.2.15 ICMP
91 41.259430509 10.0.2.15 15.197.141.123 ICMP
92 41.314963339 15.197.141.123 10.0.2.15 ICMP
93 42.261547956 10.0.2.15 15.197.141.123 ICMP
Frame 127: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
Ethernet II, Src: PcsCompu_98:a3:3f (08:00:27:98:a3:3f), Dst: IPv6mcast
Destination: IPv6mcast_16 (33:33:00:00:00:16)
Source: PcsCompu_98:a3:3f (08:00:27:98:a3:3f)
Type: IPv6 (0x86dd)
Internet Protocol Version 6, Src: fe80::a3e3:cc8e:a24f:690e, Dst: ff02:
Internet Control Message Protocol v6
[Community ID: 1:3I9djXqfKyFPqoEFpGTPso3fXEg=]
0000 33 33 00 00 00 16 08 00 27 98 a3 3f 86 dd 60 00 33 ..... '..?..
0010 00 00 00 38 00 01 fe 80 00 00 00 00 00 00 a3 e3 ...8 .....
0020 cc 8e a2 4f 69 0e ff 02 00 00 00 00 00 00 00 00 ...Oi ...
0030 00 00 00 00 00 16 3a 00 05 02 00 00 01 00 8f 00 ..... :. .....
0040 87 c8 00 00 00 02 04 00 00 00 ff 02 00 00 00 00 ....
0050 00 00 00 00 00 01 ff 4f 69 0e 04 00 00 00 ff 02 ..... O i.....
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 fb ....
leagueflyer@leagueflyer: ~
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=26 ttl=117 time=58.3 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=27 ttl=117 time=107 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=28 ttl=117 time=75.1 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=29 ttl=117 time=92.3 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=30 ttl=117 time=57.3 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=31 ttl=117 time=122 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=32 ttl=117 time=62.1 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=33 ttl=117 time=54.9 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=34 ttl=117 time=58.3 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=35 ttl=117 time=55.8 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=36 ttl=117 time=82.4 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=37 ttl=117 time=101 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=38 ttl=117 time=63.6 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=39 ttl=117 time=72.6 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=40 ttl=117 time=39.2 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=41 ttl=117 time=43.2 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=42 ttl=117 time=55.6 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=43 ttl=117 time=43.3 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=44 ttl=117 time=52.1 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=45 ttl=117 time=175 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=46 ttl=117 time=41.8 ms
64 bytes from a572ab1d134af1b1e.awsglobalaccelerator.com (15.197.141.123): icmp_seq=47 ttl=117 time=58.7 ms
^C
--- amrita.edu ping statistics ---
47 packets transmitted, 47 received, 0% packet loss, time 46206ms
rtt min/avg/max/mdev = 38.072/84.668/548.402/84.404 ms
leagueflyer@leagueflyer:~$

Header info all the layers

DNS Query

DNS Reply

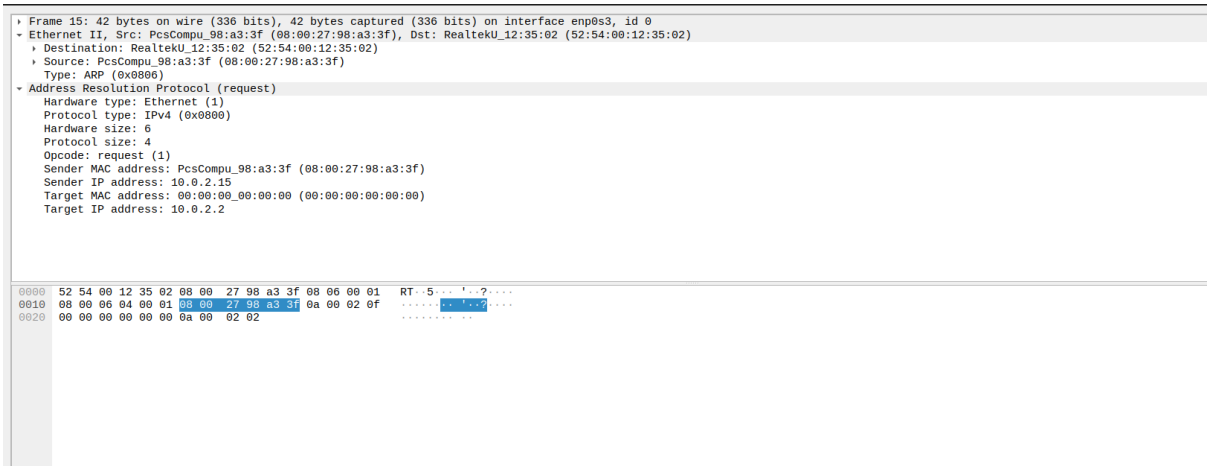


ICMP

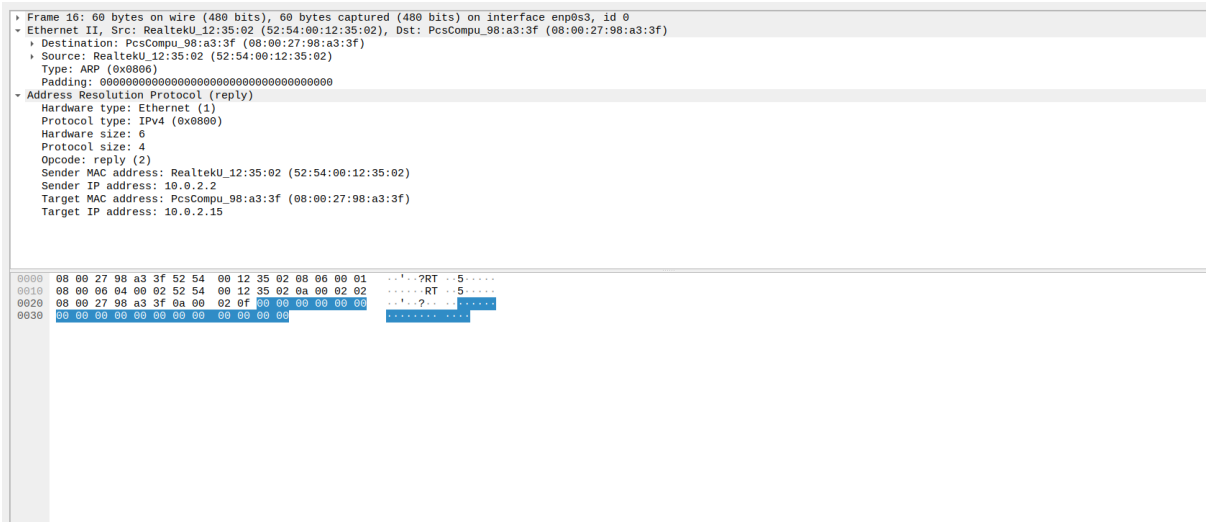
```
▸ Frame 3: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
▾ Ethernet II, Src: PcsCompu_98:a3:3f (08:00:27:98:a3:3f), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
  ▸ Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
  ▸ Source: PcsCompu_98:a3:3f (08:00:27:98:a3:3f)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 15.197.141.123
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0xbda1 (48545)
  ▸ Flags: 0x40, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0xd3b8 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.2.15
    Destination Address: 15.197.141.123
▾ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x63b9 [correct]
    [Checksum Status: Good]
    Identifier (BE): 6 (0x0006)
    Identifier (LE): 1536 (0x0600)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 4]
    Timestamp from icmp data: May 30, 2023 02:21:01.000000000 IST
    [Timestamp from icmp data (relative): 0.523648904 seconds]
  ▾ Data (48 bytes)
      Data: 23f807000000000010111213141516171819 1a1b1c1d1e1f202122232425262728292a2b…
      [Length: 48]
  [Community ID: 1:B3W1n9WZdK+Y9a6FzC03lOzK2Kg=]

0000  52 54 00 12 35 02 08 00  27 98 a3 3f 08 00 45 00   RT··5··· '··?··E·
0010  00 54 bd a1 40 00 40 01  d3 b8 0a 00 02 0f 0f c5   ·T··@·@· ········
```

```
▸ Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface enp0s3, id 0
▾ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_98:a3:3f (08:00:27:98:a3:3f)
  ▸ Destination: PcsCompu_98:a3:3f (08:00:27:98:a3:3f)
  ▸ Source: RealtekU_12:35:02 (52:54:00:12:35:02)
    Type: IPv4 (0x0800)
▾ Internet Protocol Version 4, Src: 15.197.141.123, Dst: 10.0.2.15
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x0a (DSCP: Unknown, ECN: ECT(0))
    Total Length: 84
    Identification: 0xad67 (44391)
  ▸ Flags: 0x00
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 117
    Protocol: ICMP (1)
    Header Checksum: 0xeee8 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 15.197.141.123
    Destination Address: 10.0.2.15
▾ Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x6bb9 [correct]
    [Checksum Status: Good]
    Identifier (BE): 6 (0x0006)
    Identifier (LE): 1536 (0x0600)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Request frame: 3]
    [Response time: 47.586 ms]
    Timestamp from icmp data: May 30, 2023 02:21:01.000000000 IST
    [Timestamp from icmp data (relative): 0.571234776 seconds]
  ▾ Data (48 bytes)
      Data: 23f807000000000010111213141516171819 1a1b1c1d1e1f202122232425262728292a2b…
      [Length: 48]
  [Community ID: 1:B3W1n9WZdK+Y9a6FzC03lOzK2Kg=]

0000  08 00 27 98 a3 3f 52 54  00 12 35 02 08 00 45 0a   ··'··?RT ··5···E·
0010  00 54 ad 67 00 00 75 01  ee e8 0f c5 8d 7b 0a 00   ·T·g··u· ·····{··
0020  02 0f 00 00 6b b9 00 06  00 01 35 10 75 64 00 00   ····k··· ··5·ud··
0030  00 00 23 f8 07 00 00 00  00 00 10 11 12 13 14 15   ··#····· ········

Help                                                    Close
```

ARP (Request)



ARP (Reply)



THANK YOU!!