In\_Class Problem & WireShark

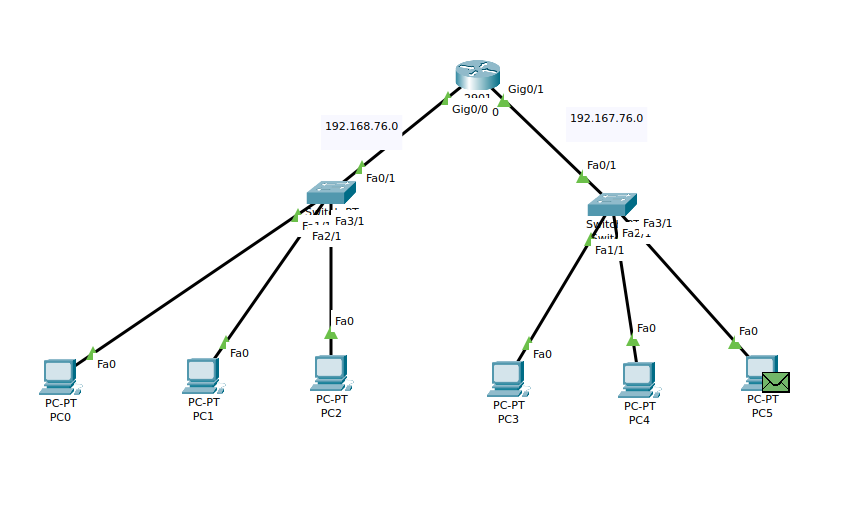
21\_AIE\_211

ICN– SEM-IV

Professor – Ganga Gowri Mam

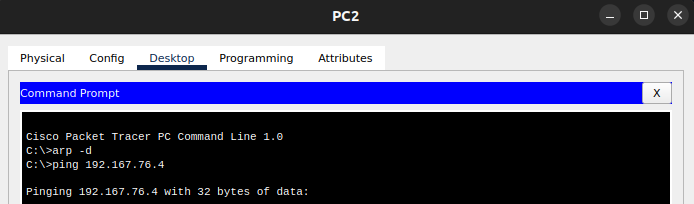
Submitted By: Vikhyat Bansal [CB.EN.U4AIE21076]



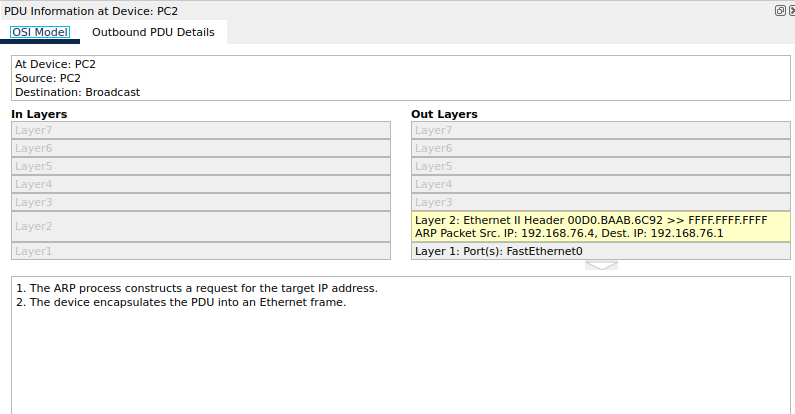
Network:

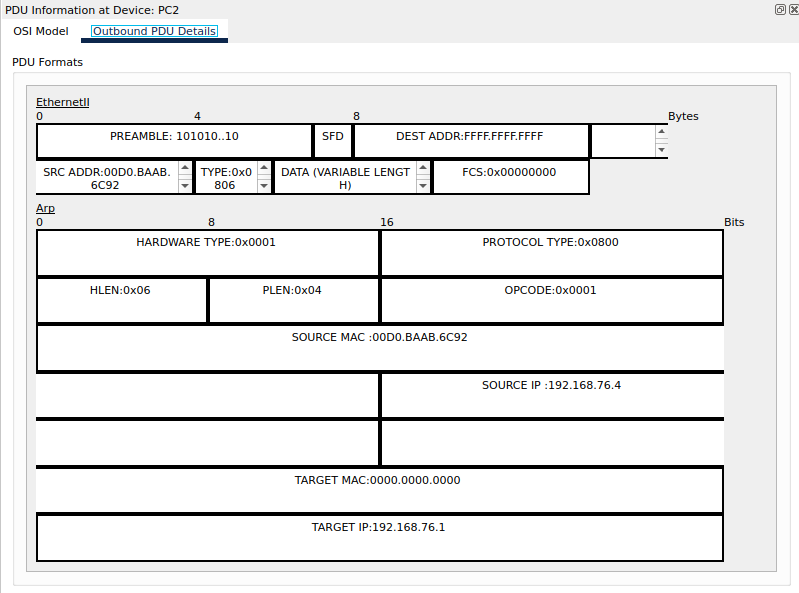
After creating the network, we will randomly take a PC and will try to ping a PC on the other subnet.

Pinging PC2 to PC5:



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

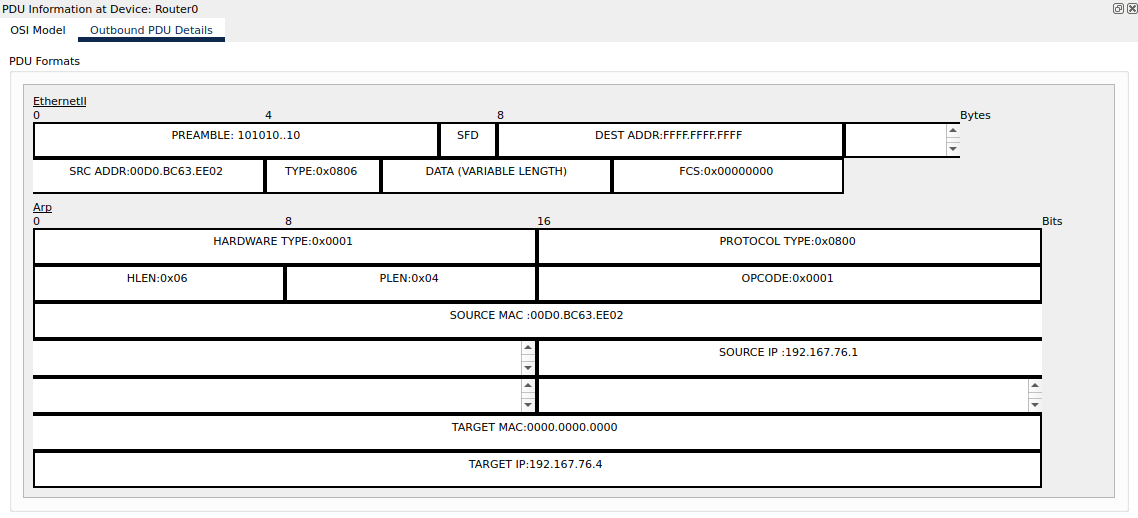




Query is being sent from PC 2 and from screenshot above it can be seen that destination MAC address is unknown. It is an ARP broadcast frame.

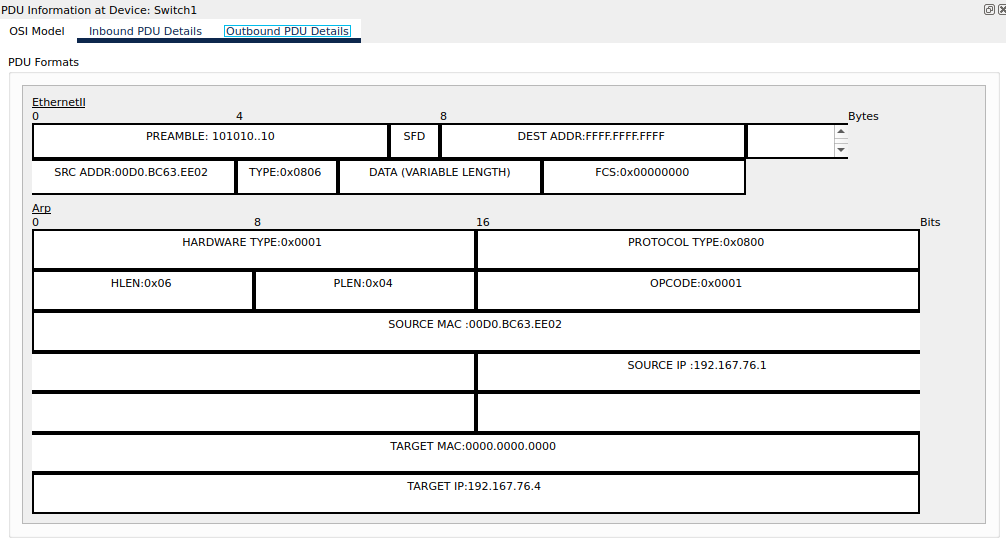
Query is being forwarded to PC5 from PC2 by router as seen from the screenshots below



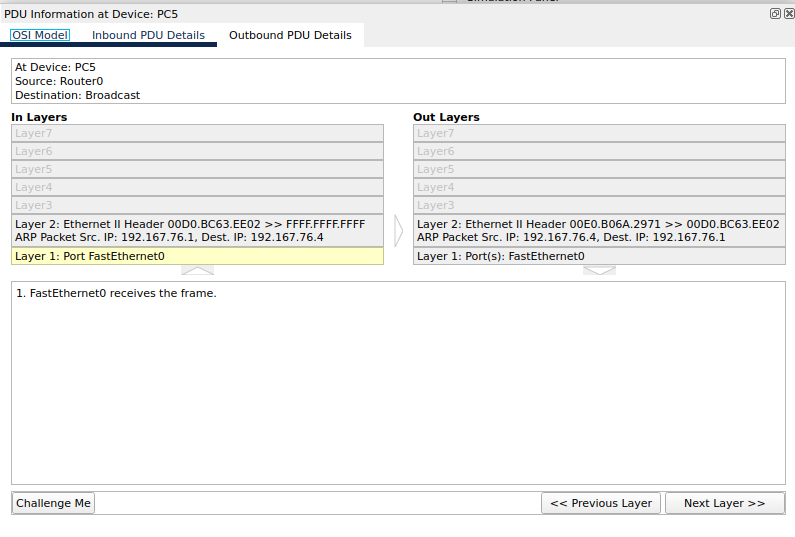


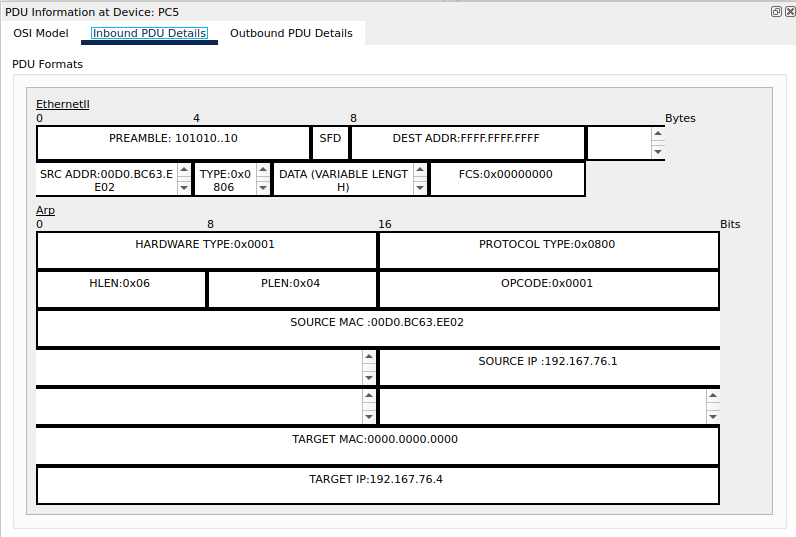
Request reaches the switch 1 where it will be given the destination MAC address

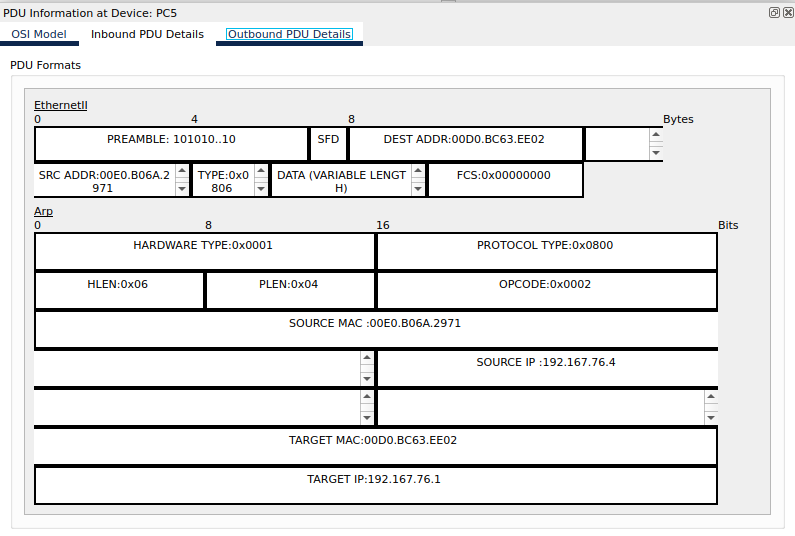


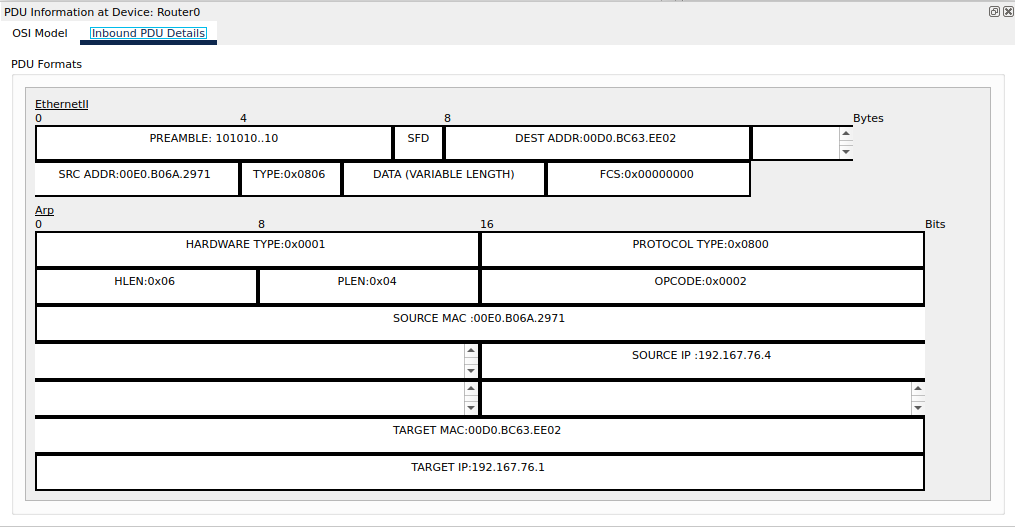


ARP reply is given by PC5 as shown below

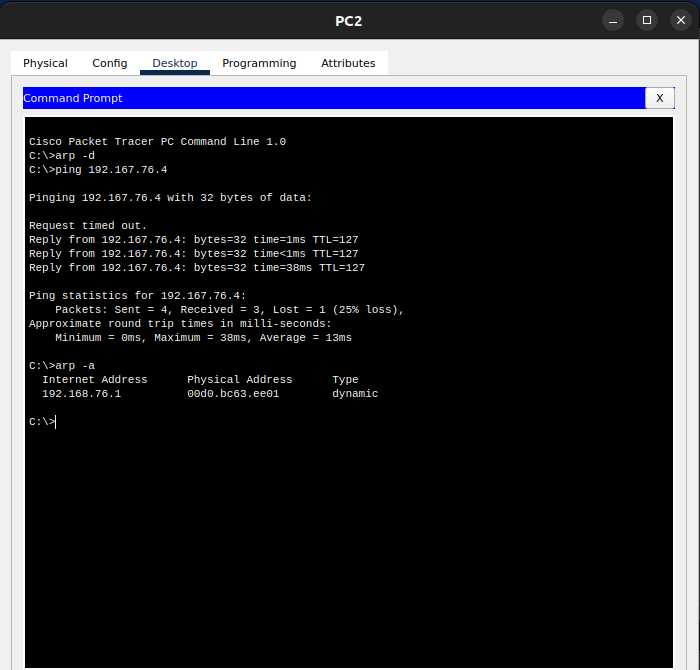




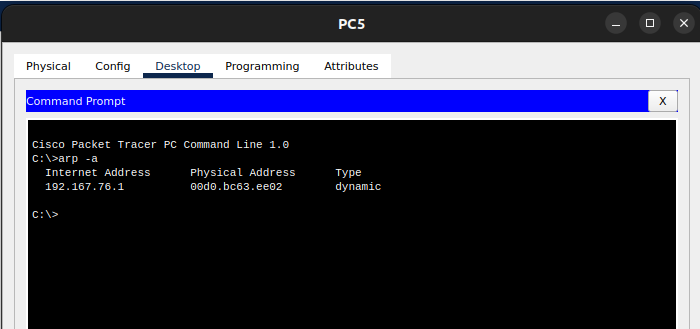


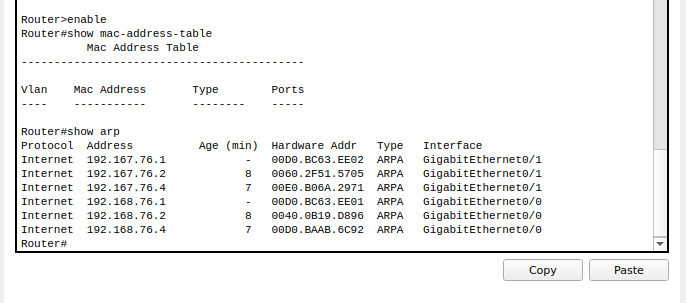
Finally, the reply will be received by router and then routing will take place as the destination MAC address will be mapped to source PC

ARP Table at the source device

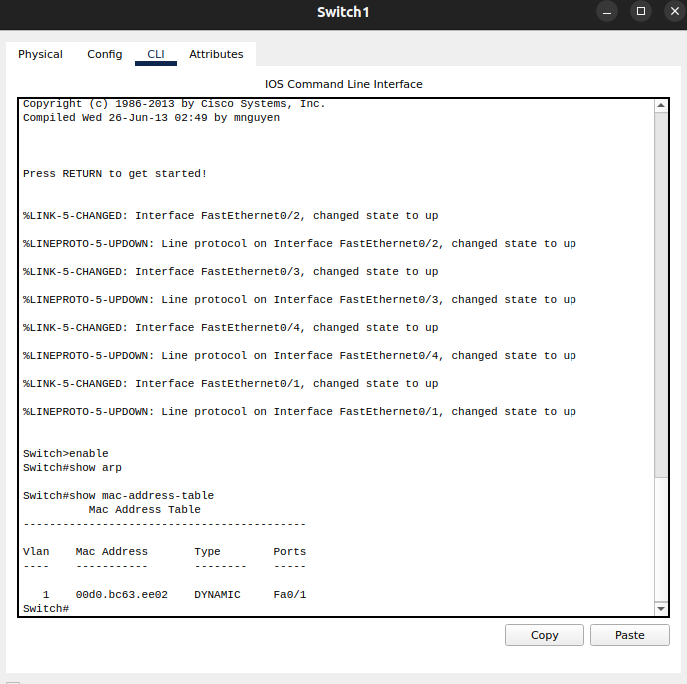


ARP Table at the end device



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

Mac – Address – Table – SWITCH\_1



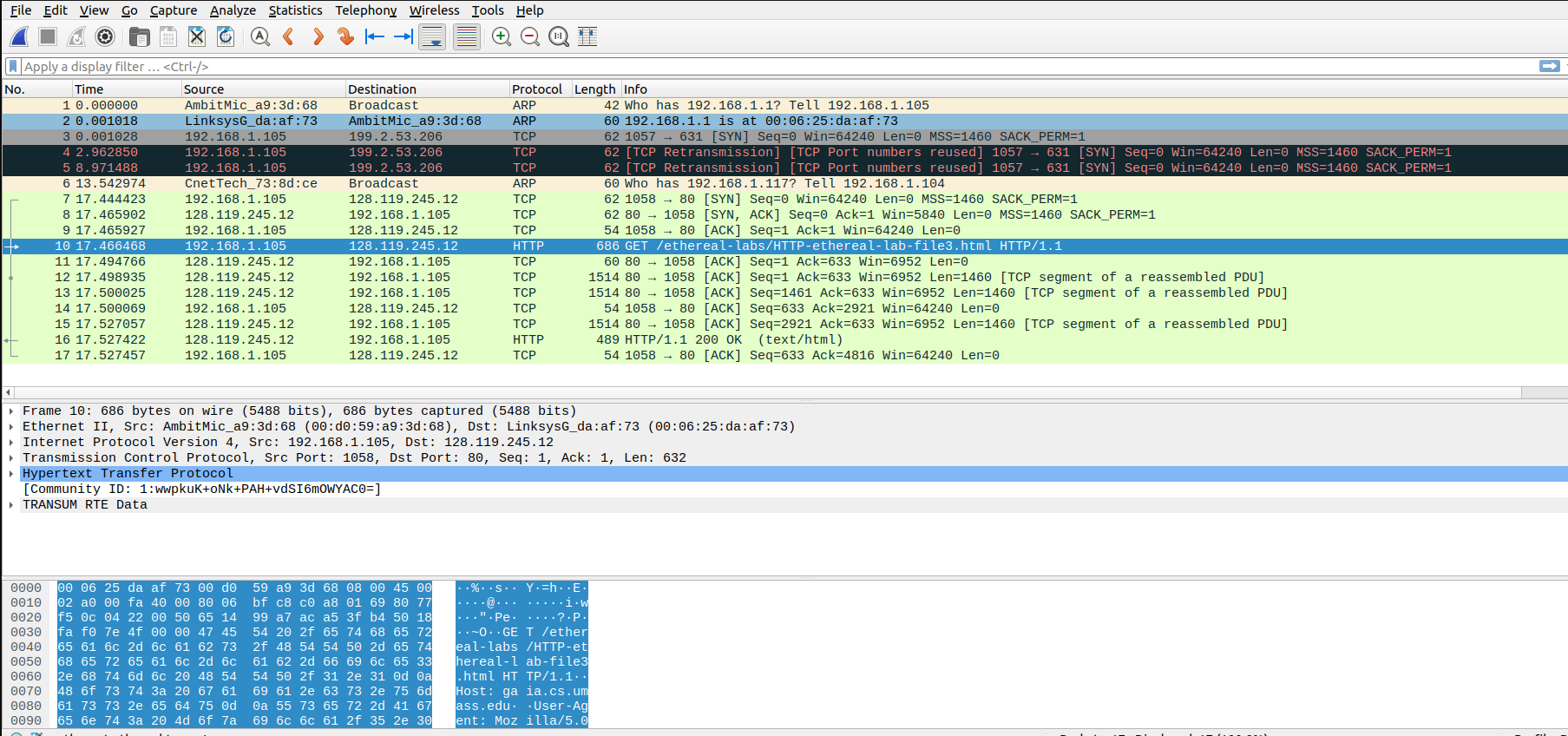
Mac – Address – Table for SWITCH 0



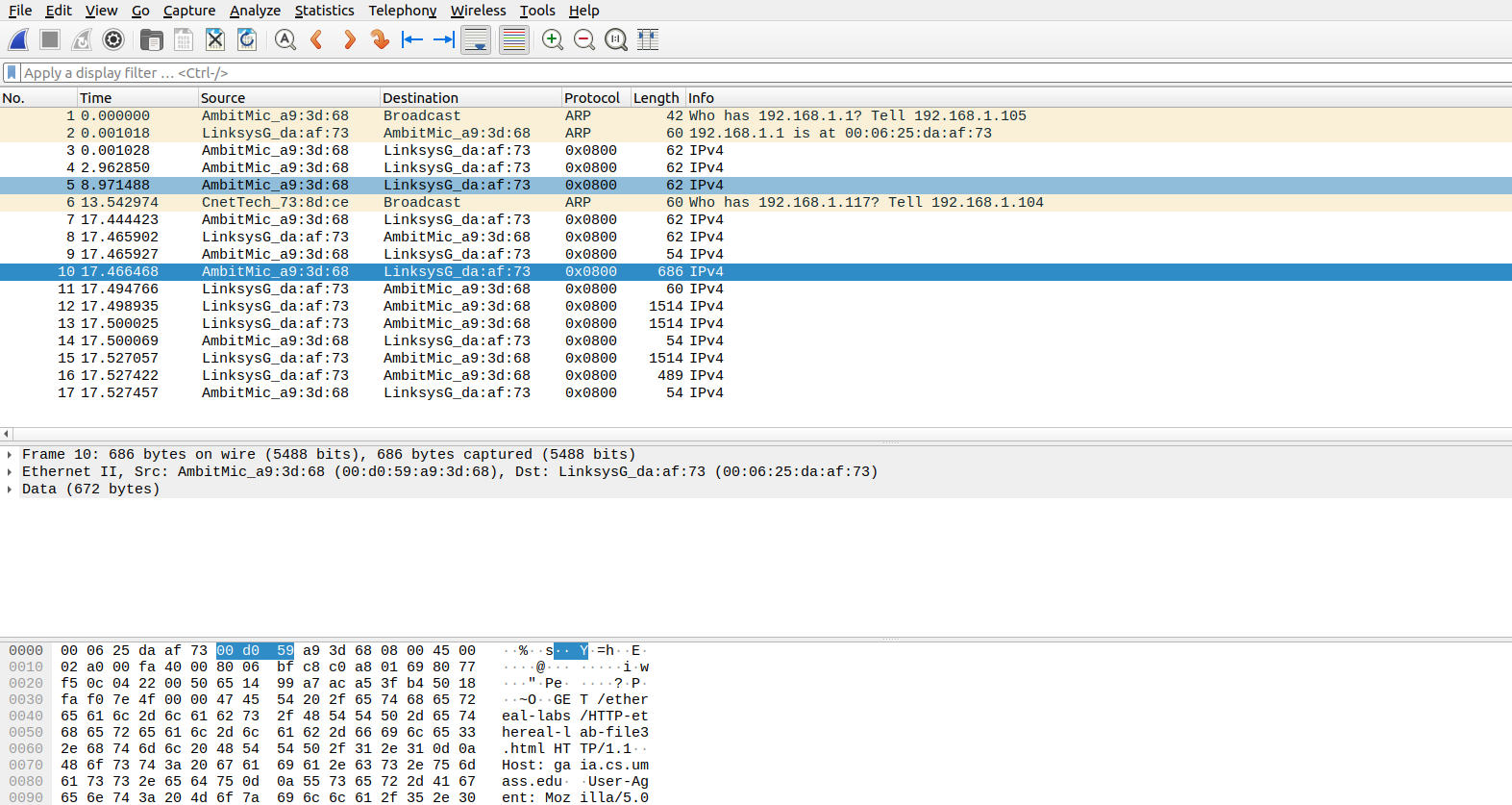
Link: [For CPT file](https://amritavishwavidyapeetham-my.sharepoint.com/:u:/g/personal/cb_en_u4aie21076_cb_students_amrita_edu/ESdQ9ICfHs1IvvssOzTajiEB8YsA7GXbCK8wDi_1-63sNw?e=JUY0HU)

**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?

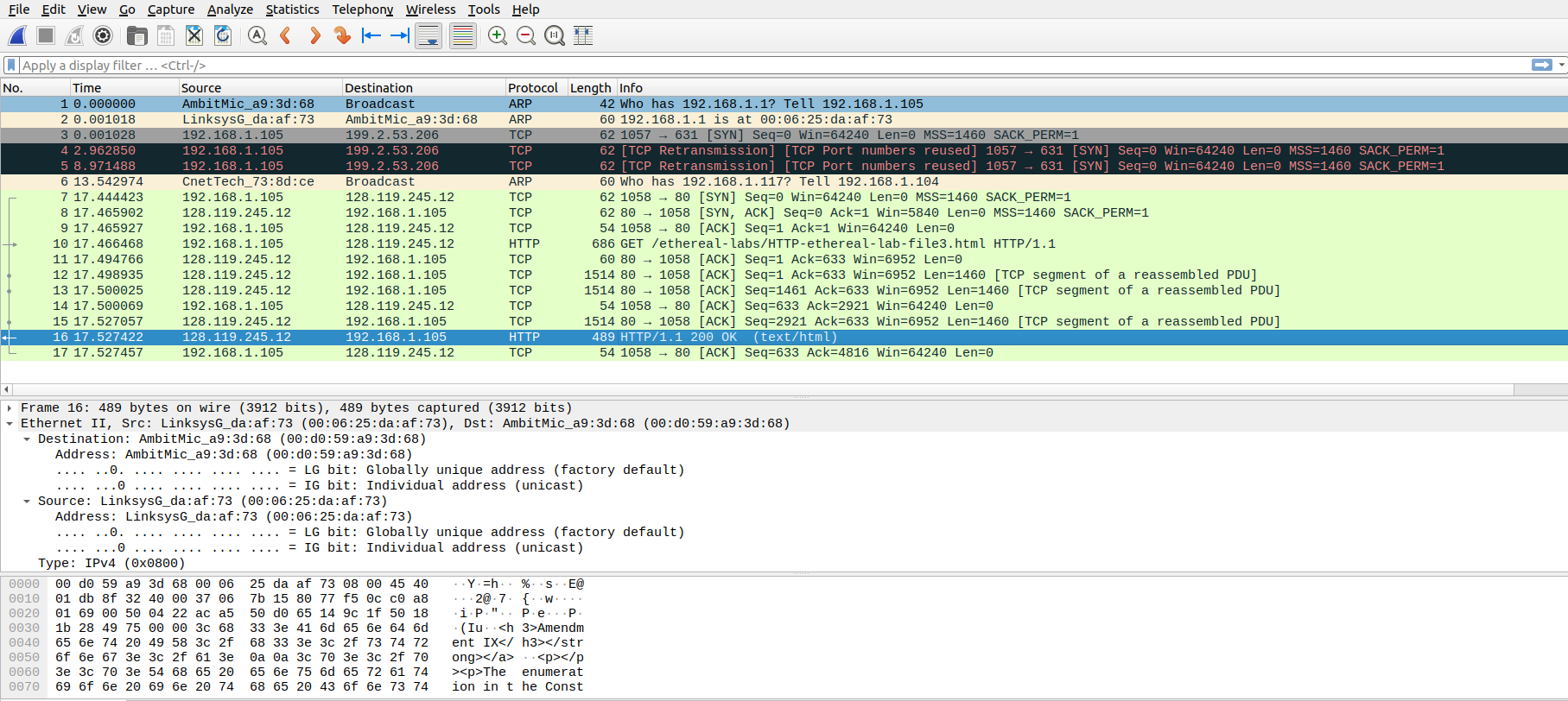
Ans. After 54 bytes from the very start of the ethernet frame the ASCII “G” appears,

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

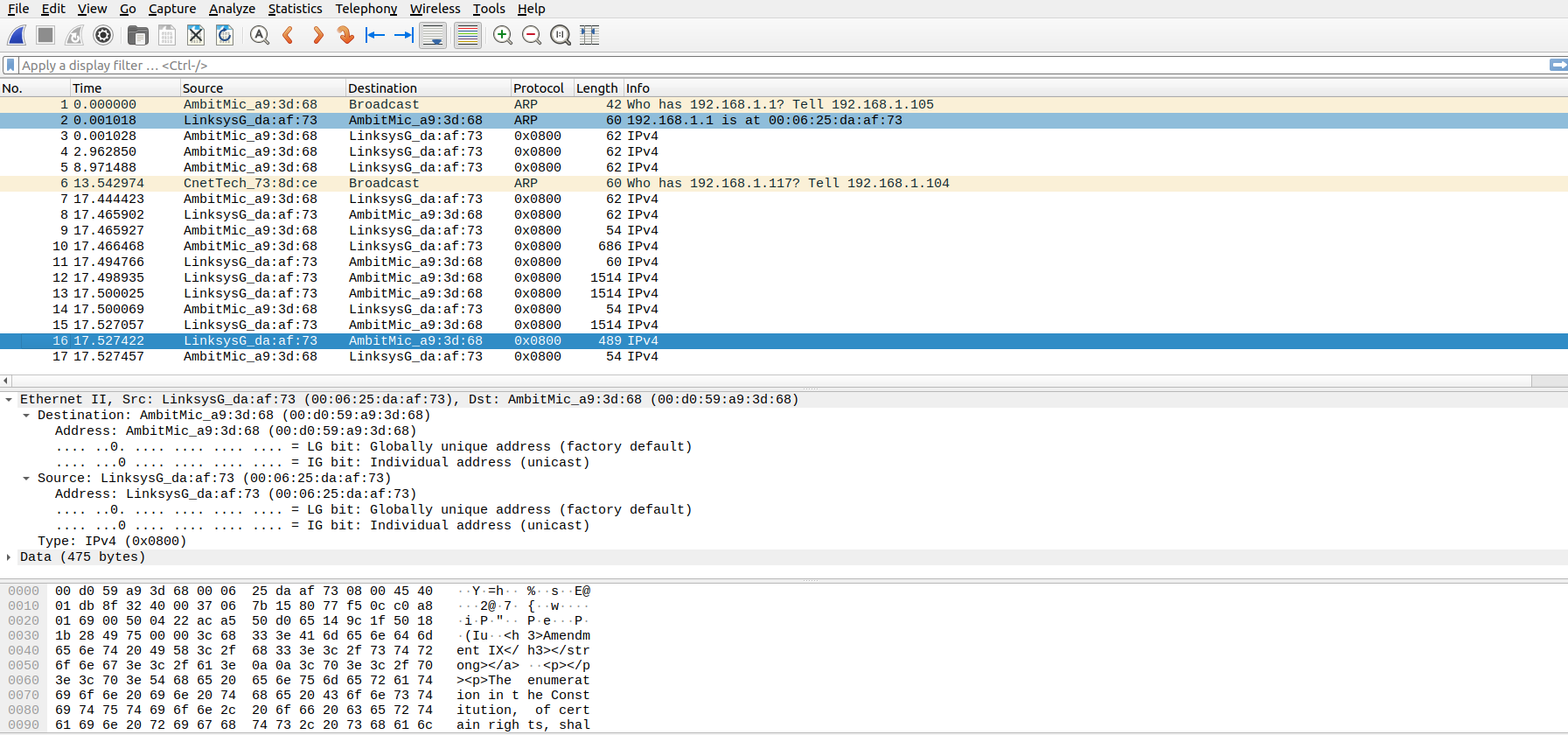
The IP header (20 bytes)

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

Capture Packet (Response):



Window with information below IP layer of the response:



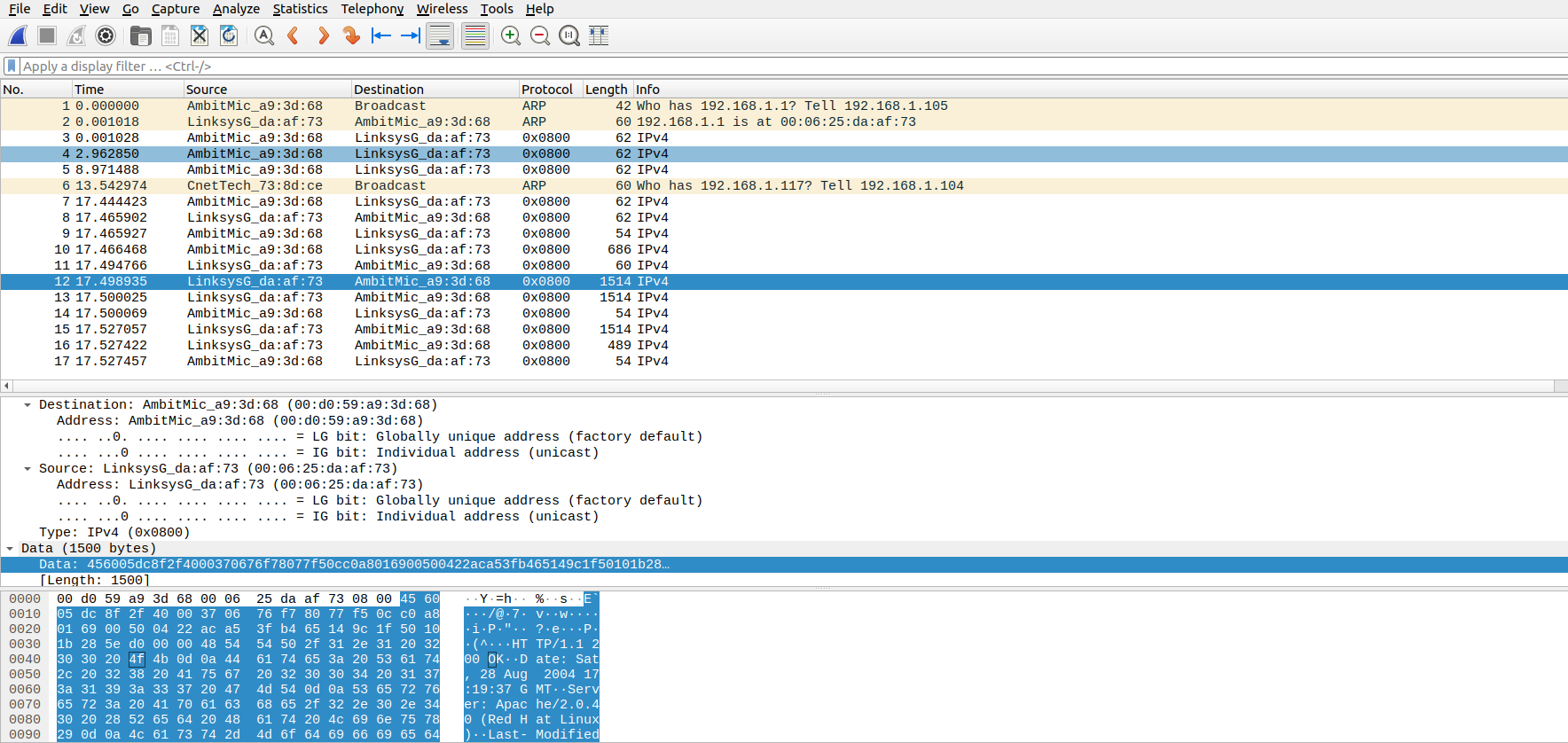
5. What is the value of the Ethernet source address? Is this the address of your computer, or of searched domain (Hint: the answer is no). What device has this as its Ethernet address?

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?

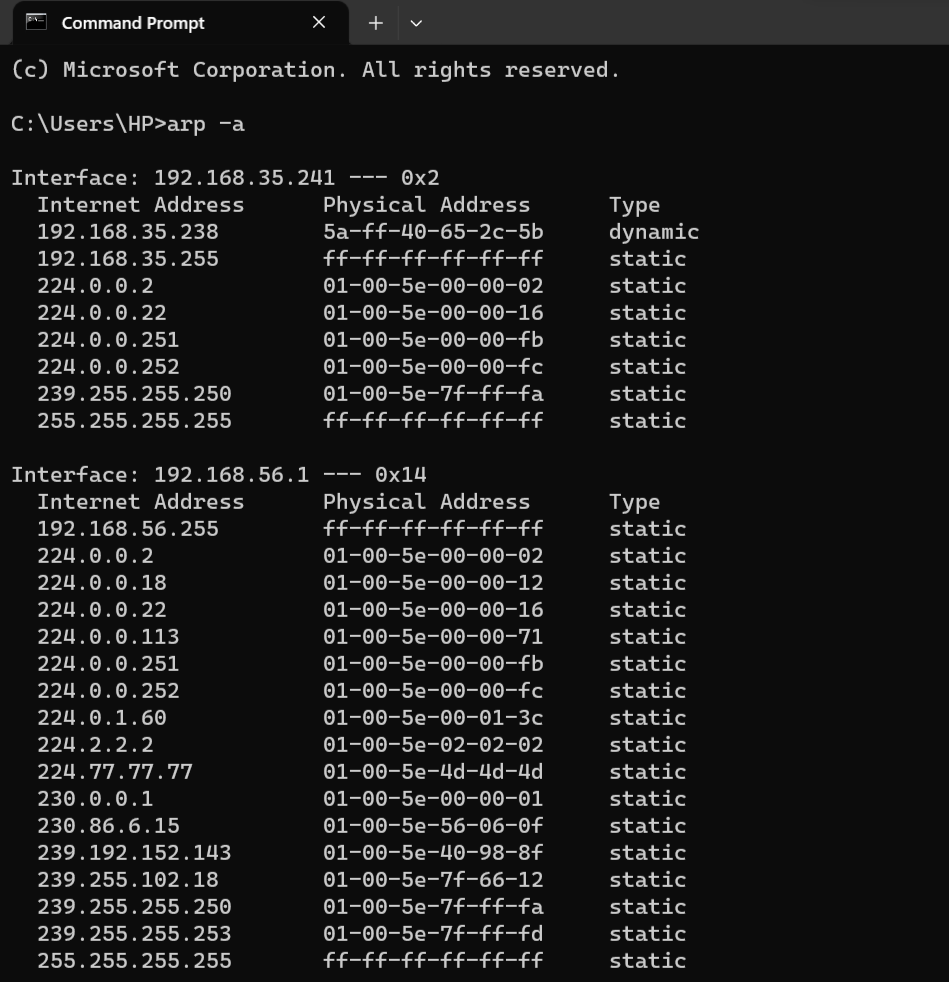
Ans. The hexadecimal frame type field in the ethernet header of this packet is 0x0800. It indicates that the upper layer protocol is Internet Protocol version 4 (IPv4).

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?

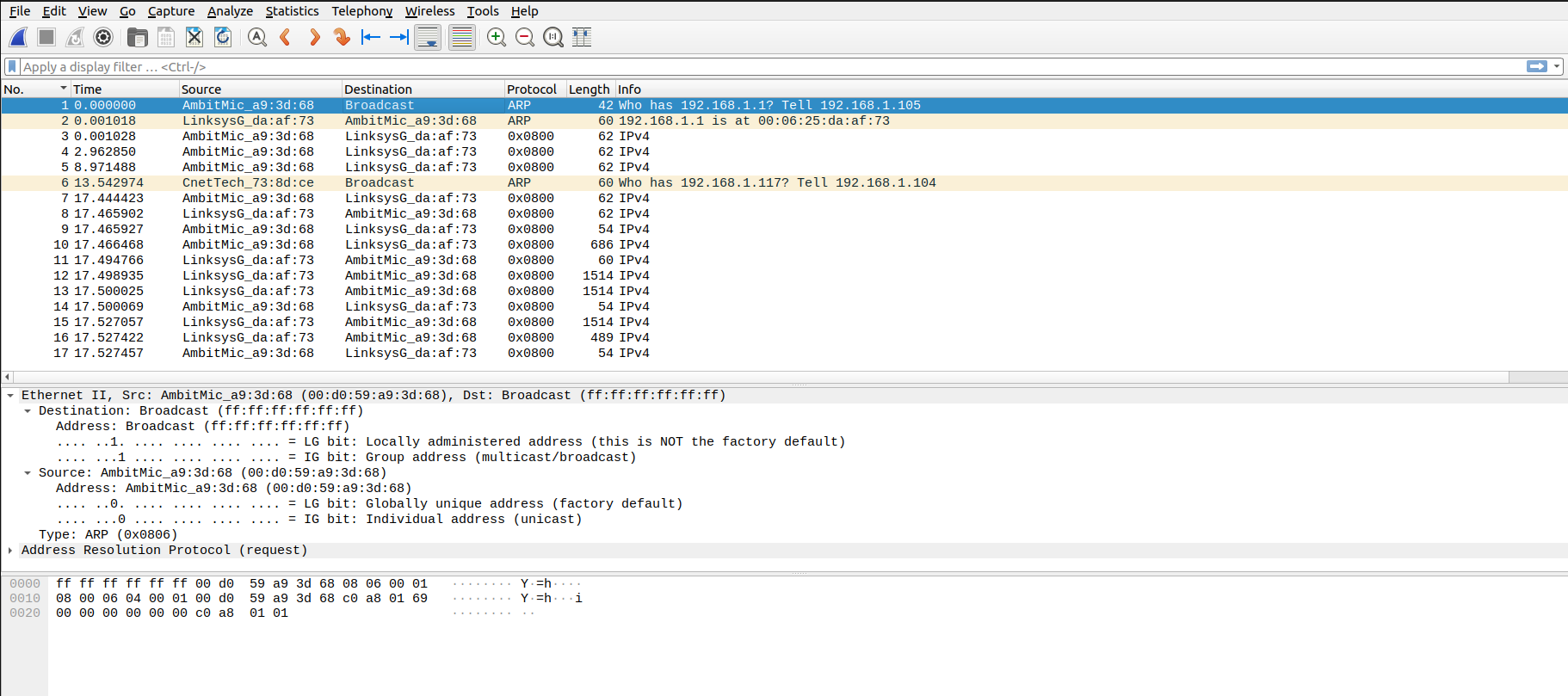
Ans. There are 65 bytes before the “O” (or “O” appears as the 66th byte). These bytes include the ethernet frame, the IP header, the TCP header, and some HTTP preamble text.

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?

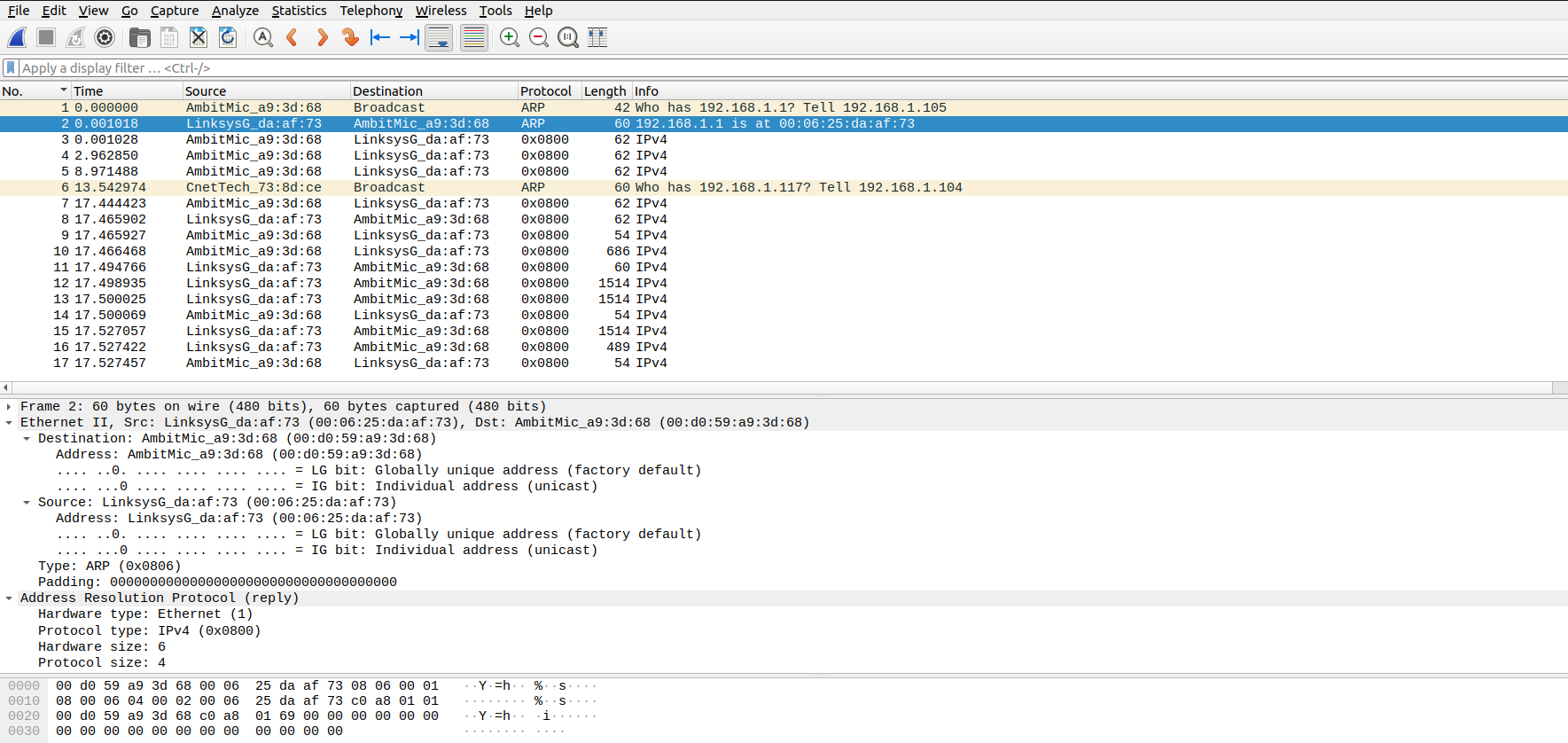
Ans. The hex value for opcode field withing the ARP-payload of the request is 0x0001, for request.

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?

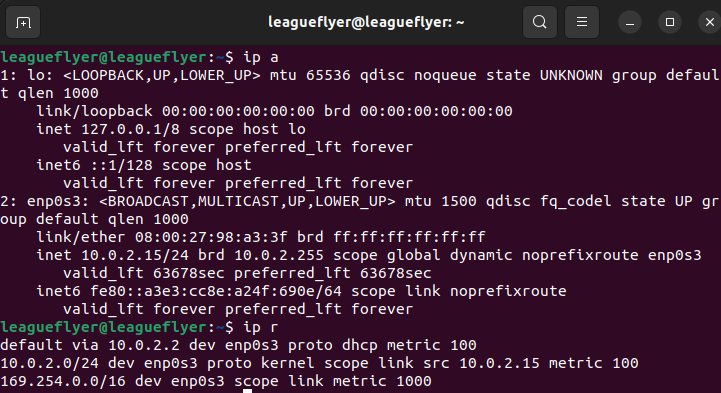
Ans. After entering wrong entry, one will not be able to ping the server IP and can not access the server through a web browser.  
To get the connection back, one has to use arp -d command for clearing the manually added entry in arp cache table.

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.

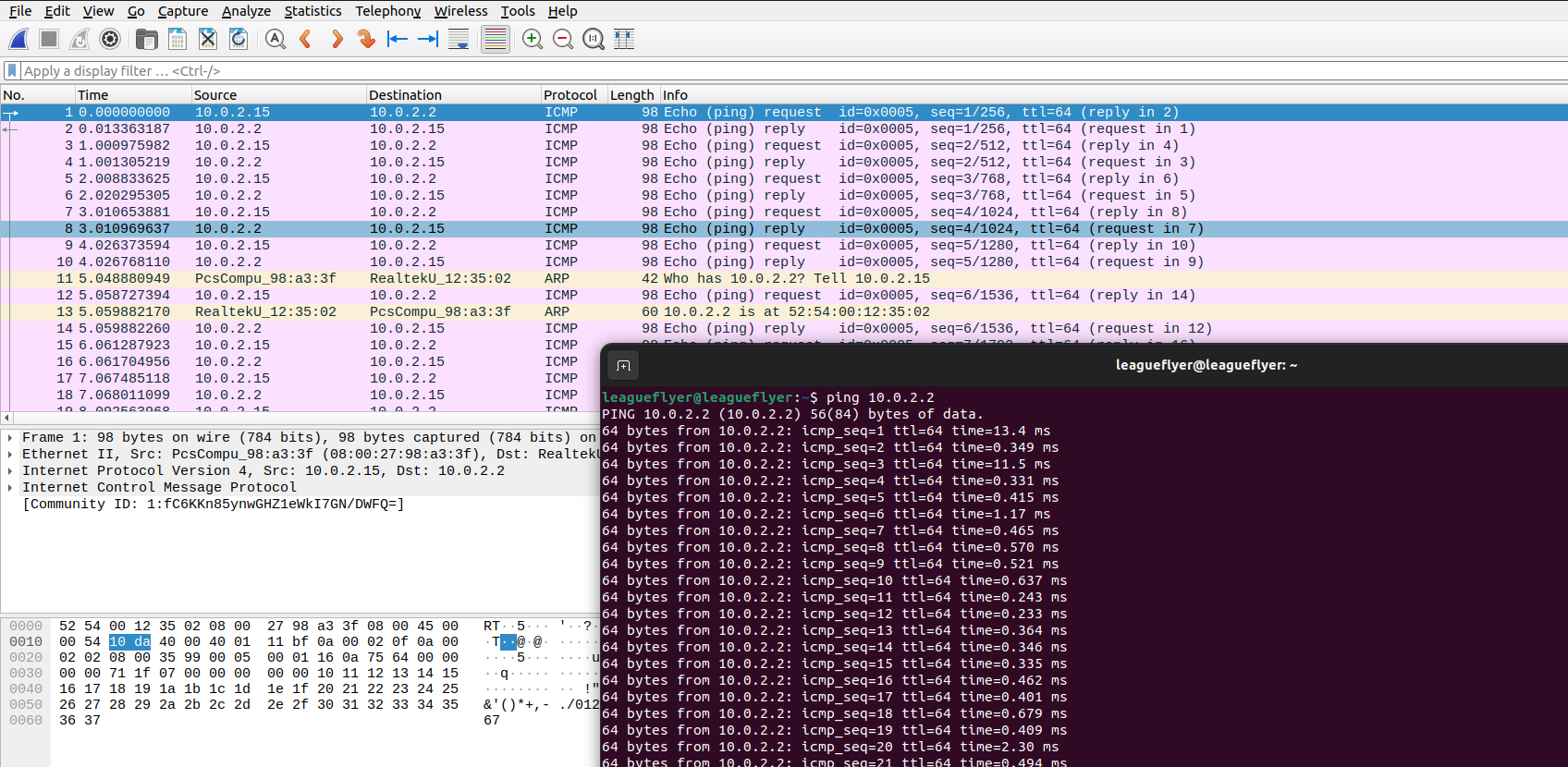
Therefore, Windows Vista TCP/IP hosts use the information in the cache. If an entry is not used, and it stays in the "Reachable" state for longer than its "Reachable Time" value, the entry changes to the "Stale" state. If an entry is in the "Stale" state, the Windows Vista TCP/IP host must send an ARP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

To do

IP address of the device

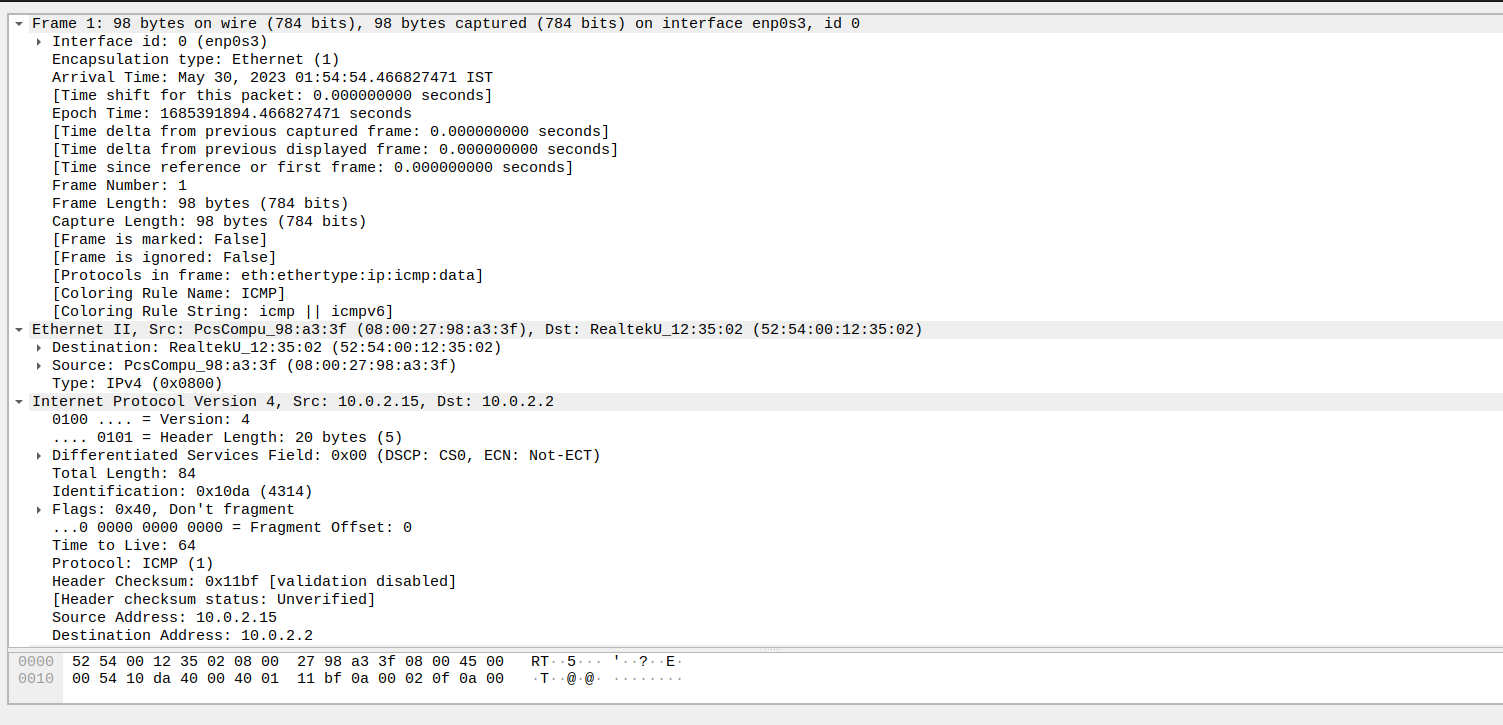
Pinging and Capturing packets for

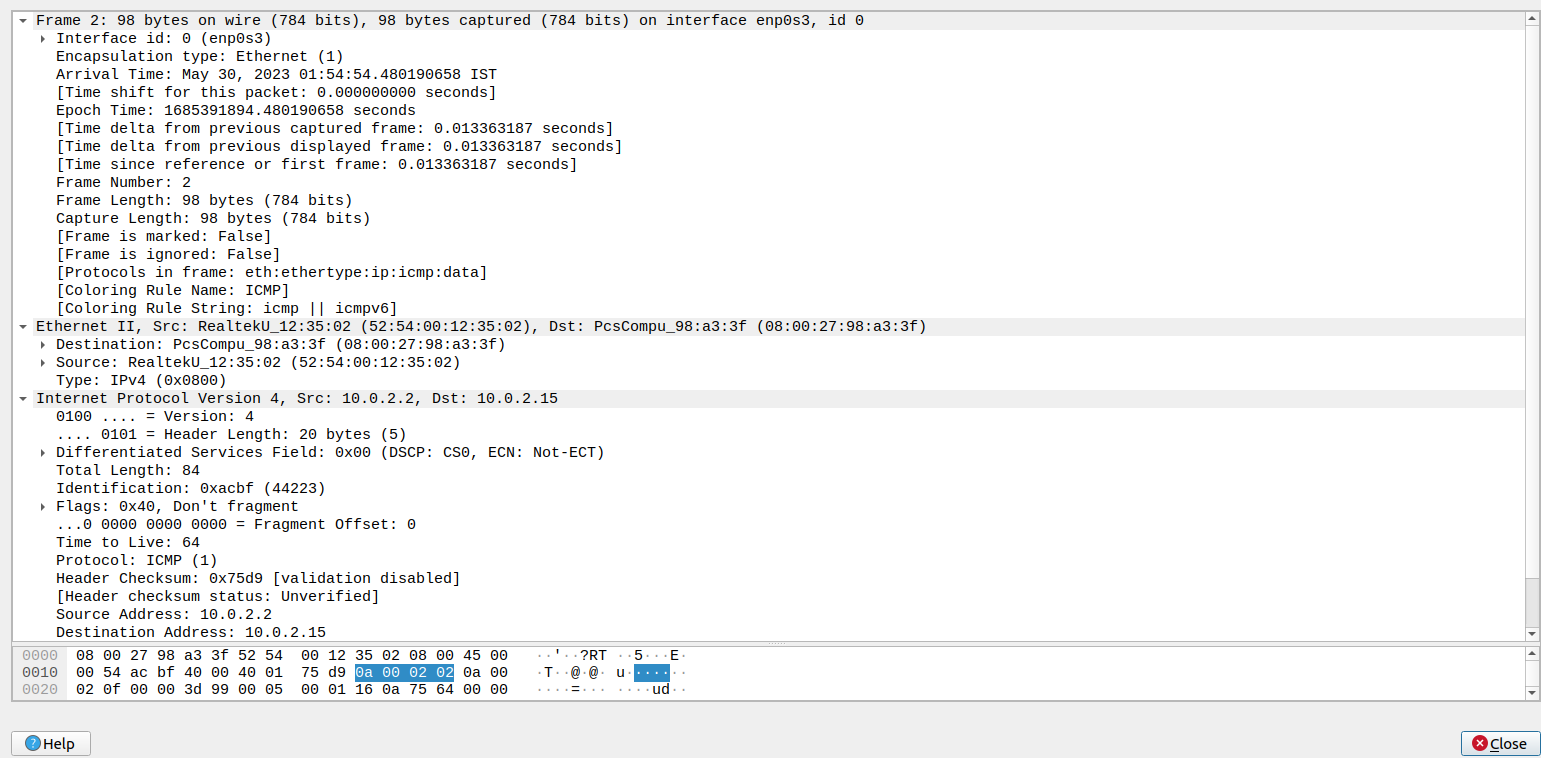
a) Gateway Router



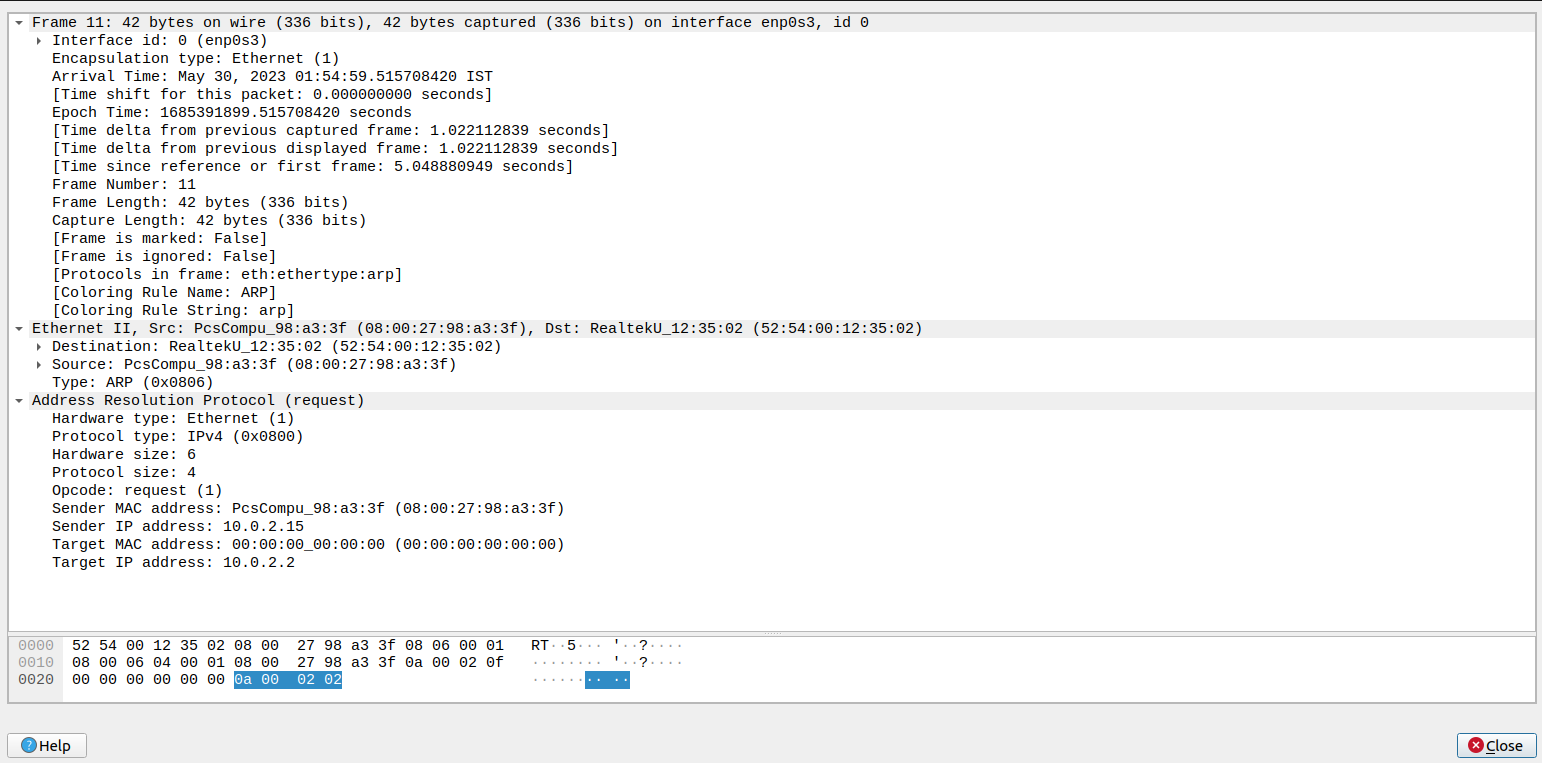
Header info in the layers

ICMP

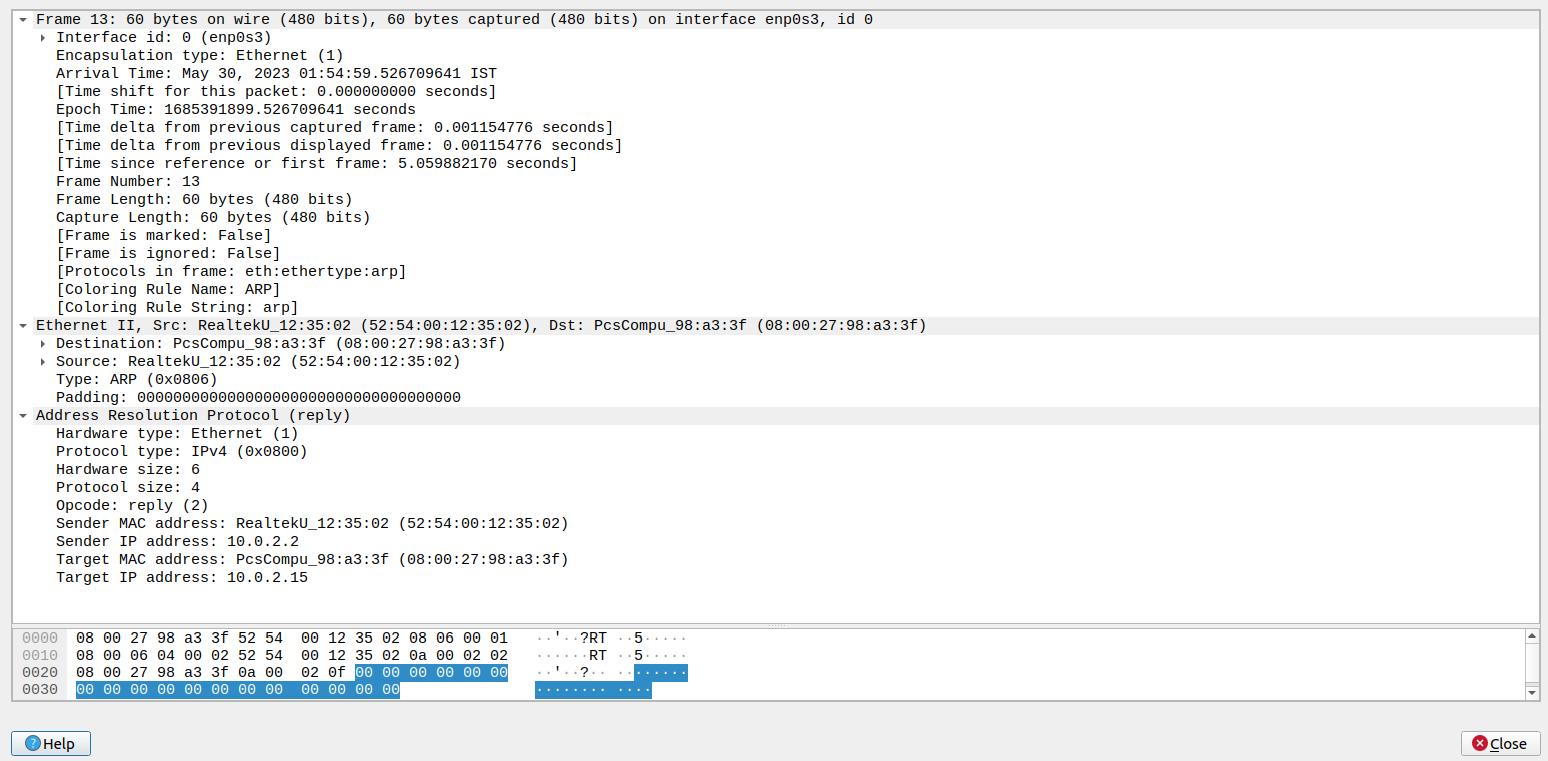




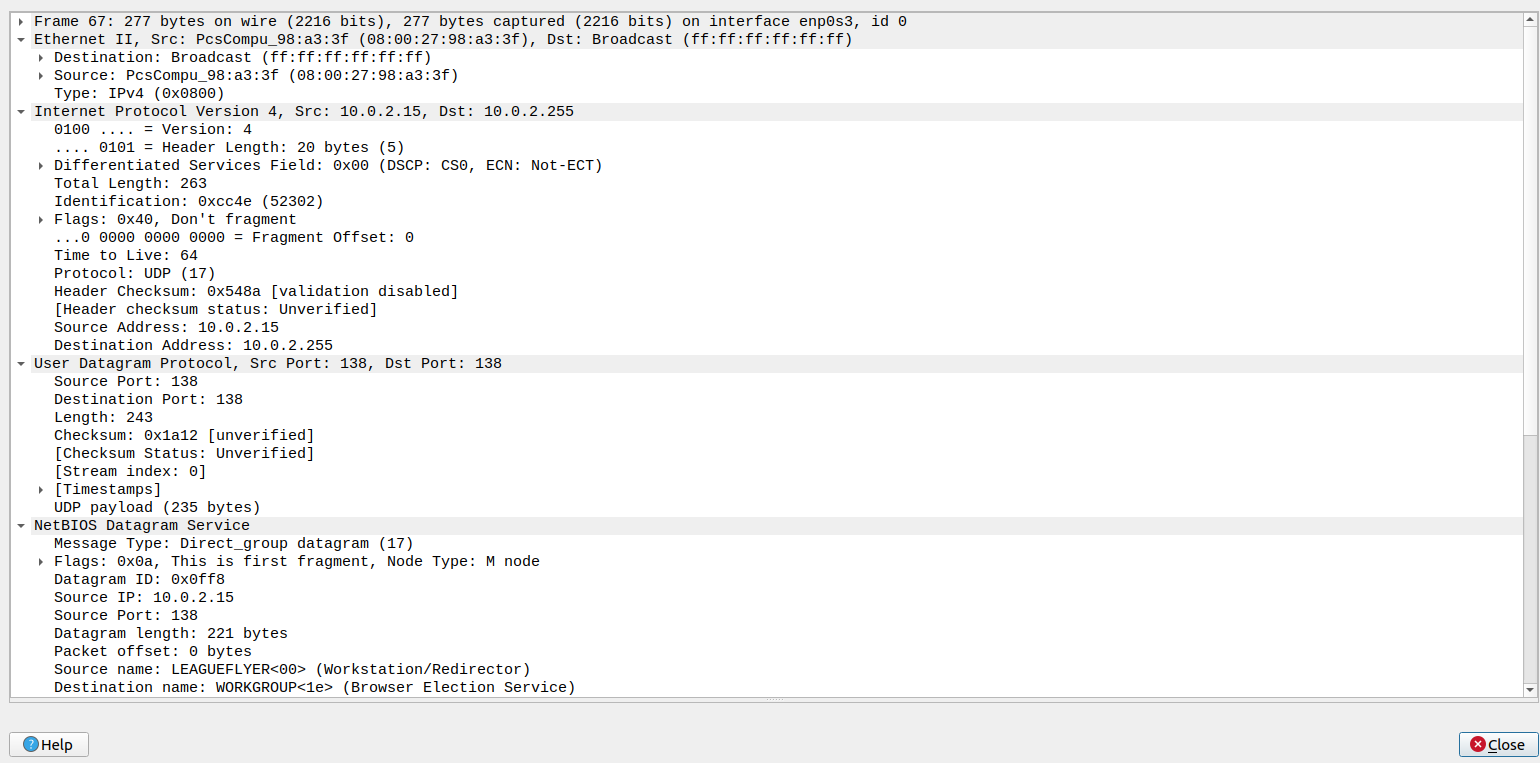
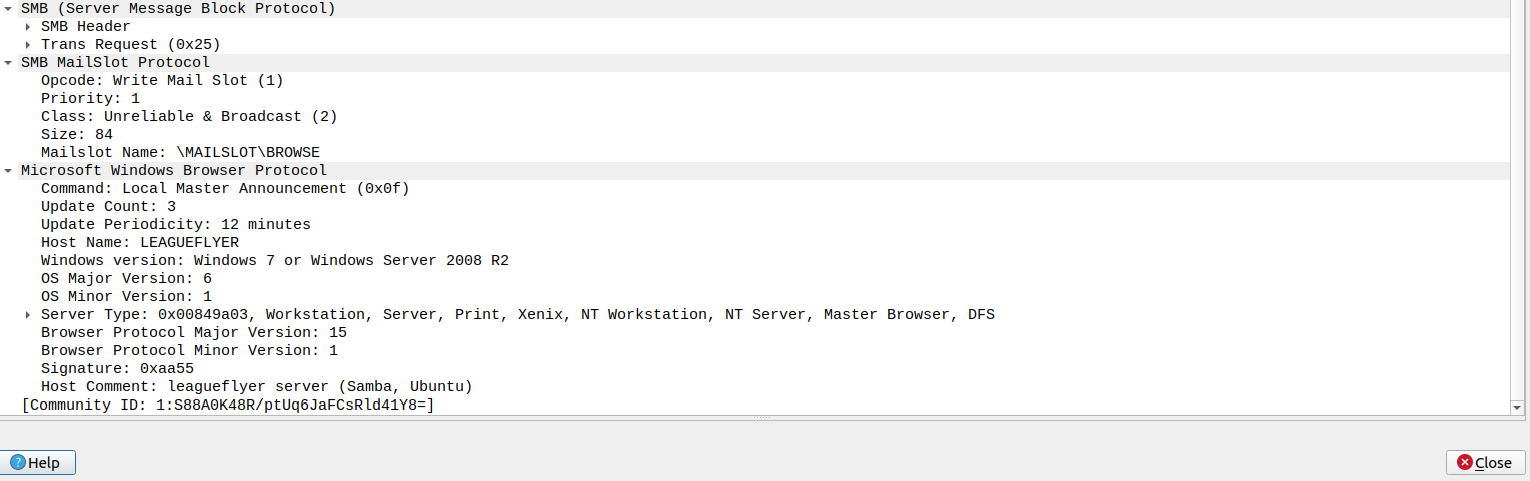
ARP (Request)



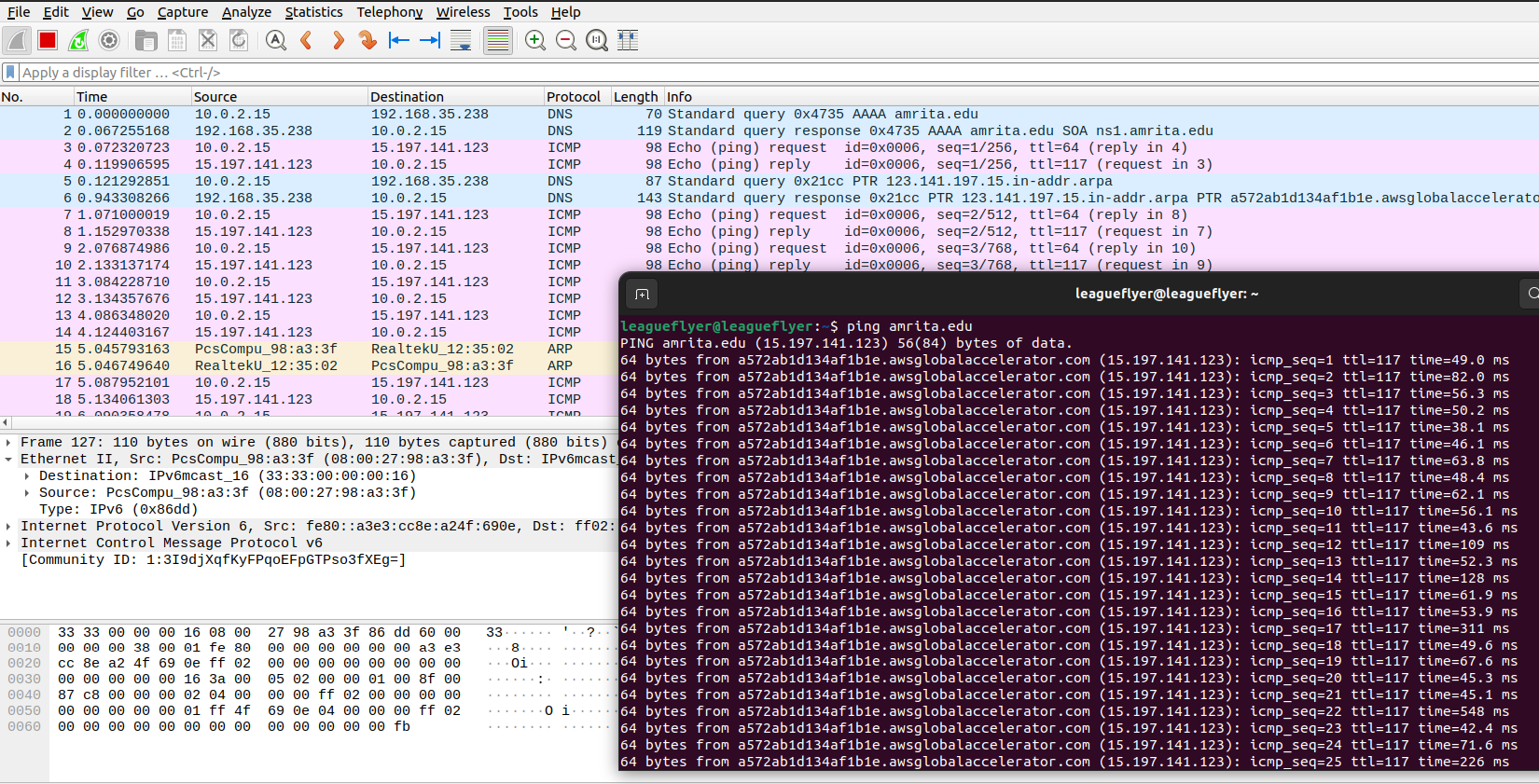
ARP (Reply)

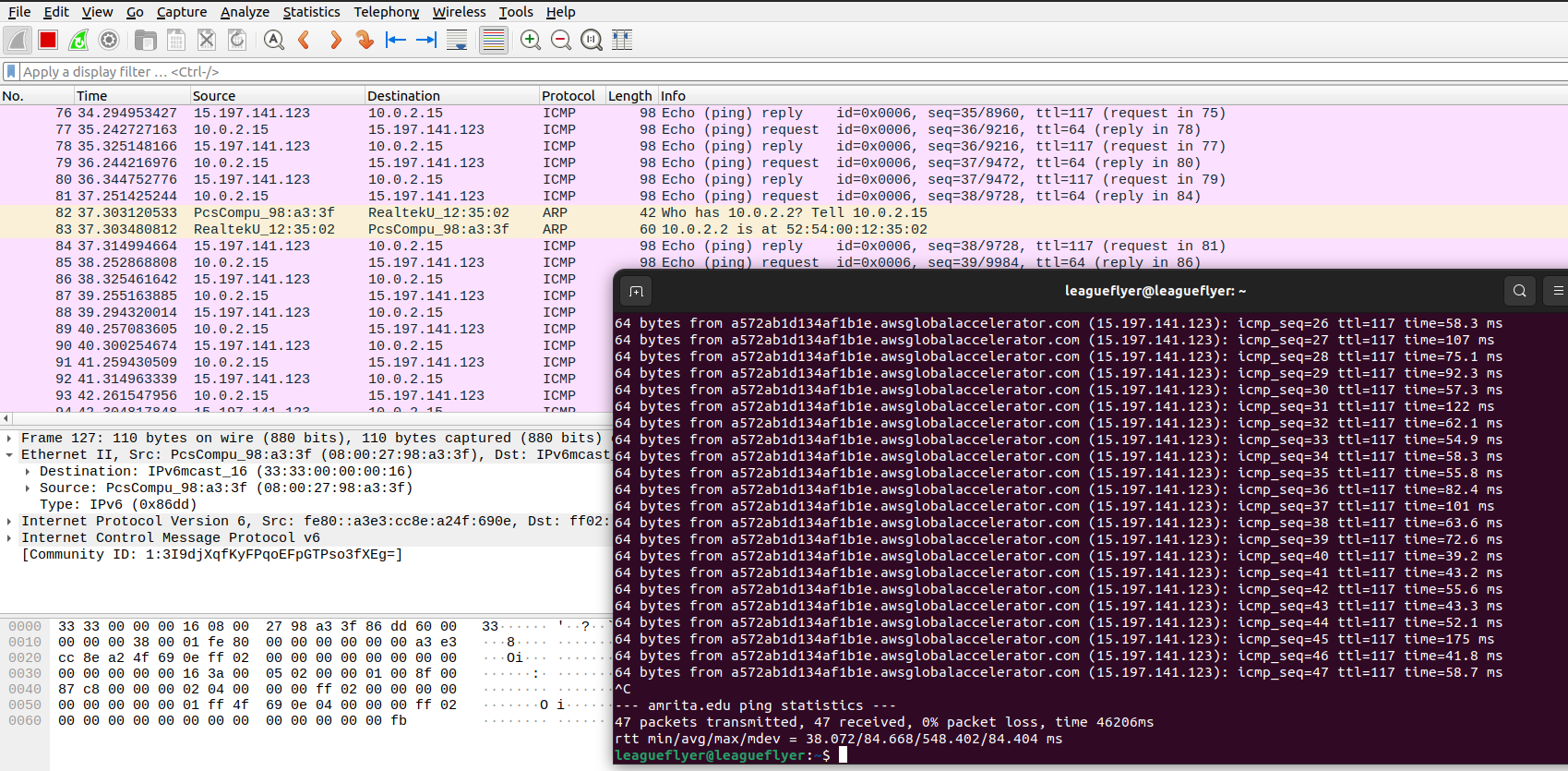


Browser



b) Amrita.edu



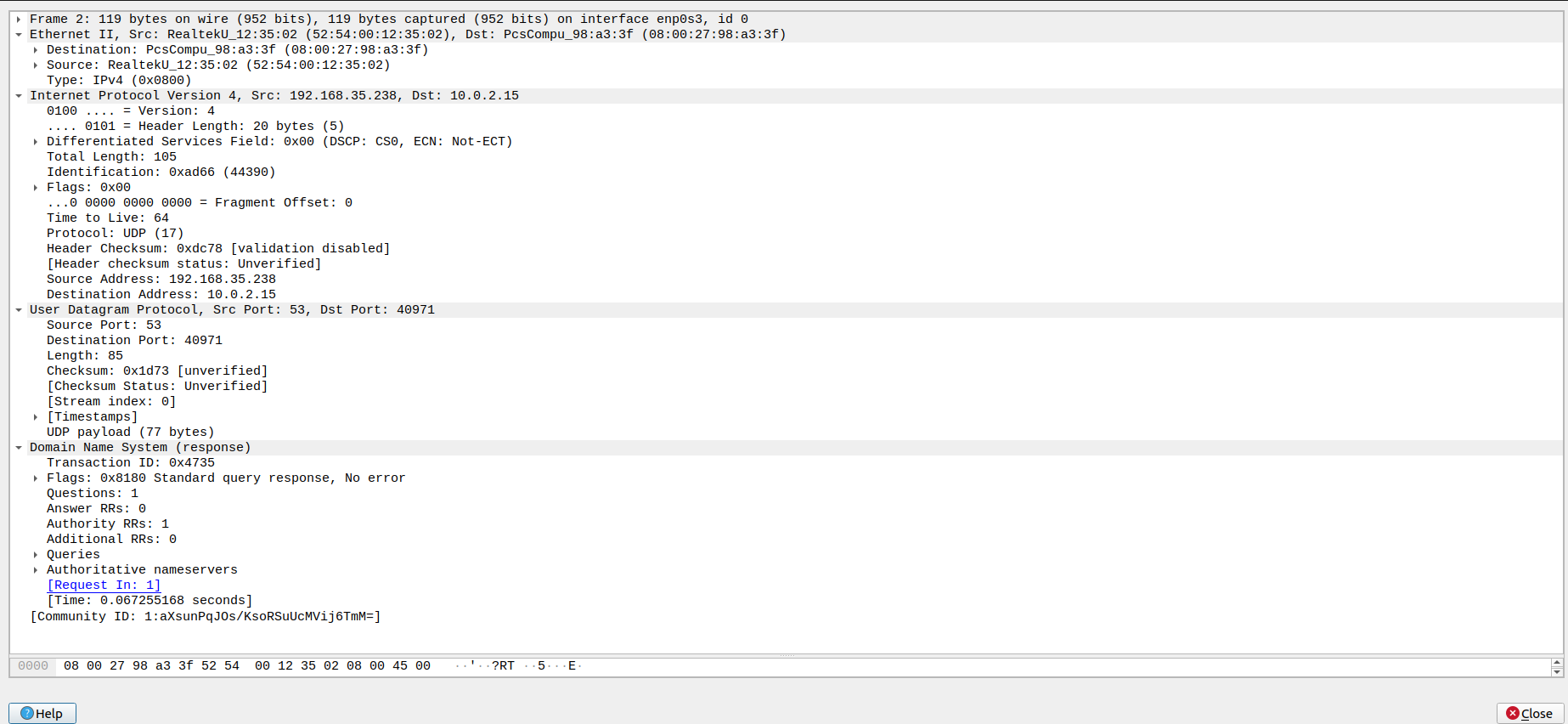


Header info all the layers

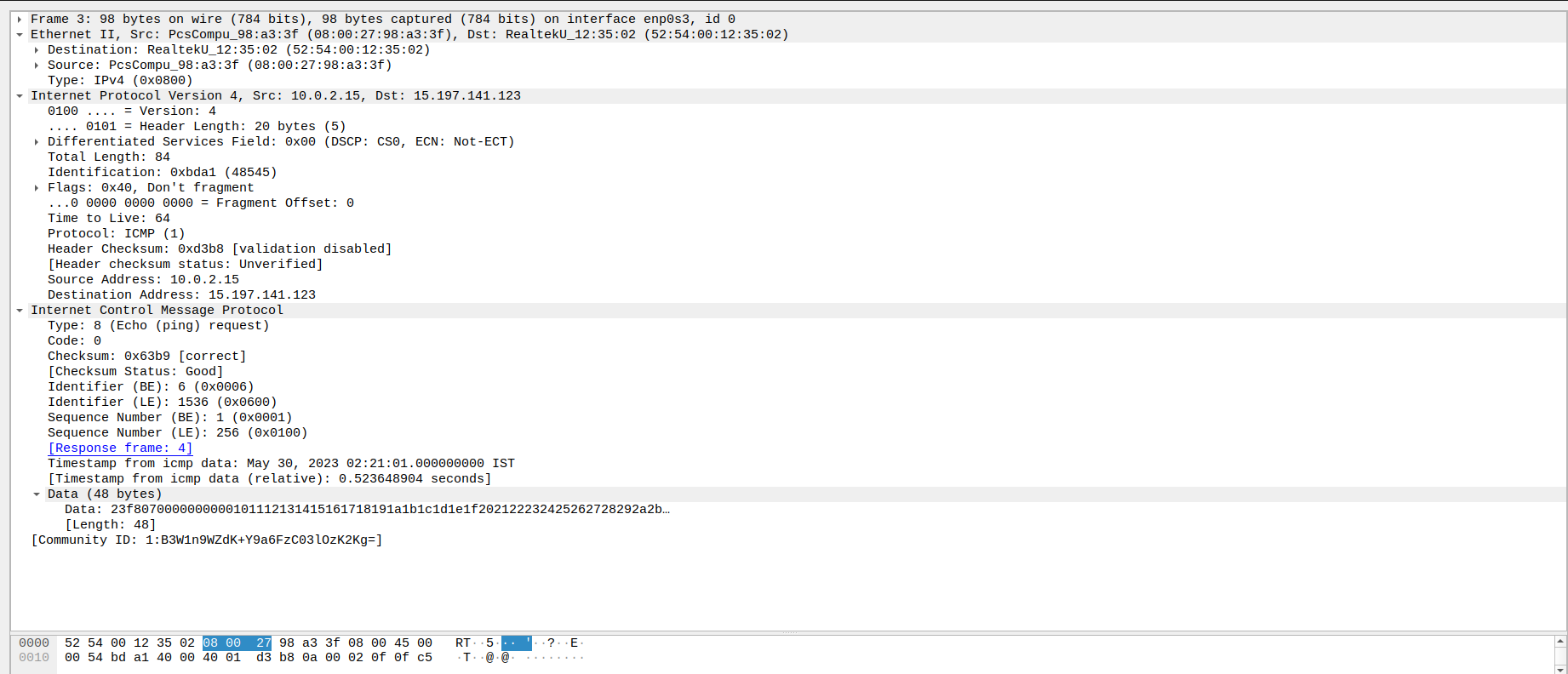
DNS Query

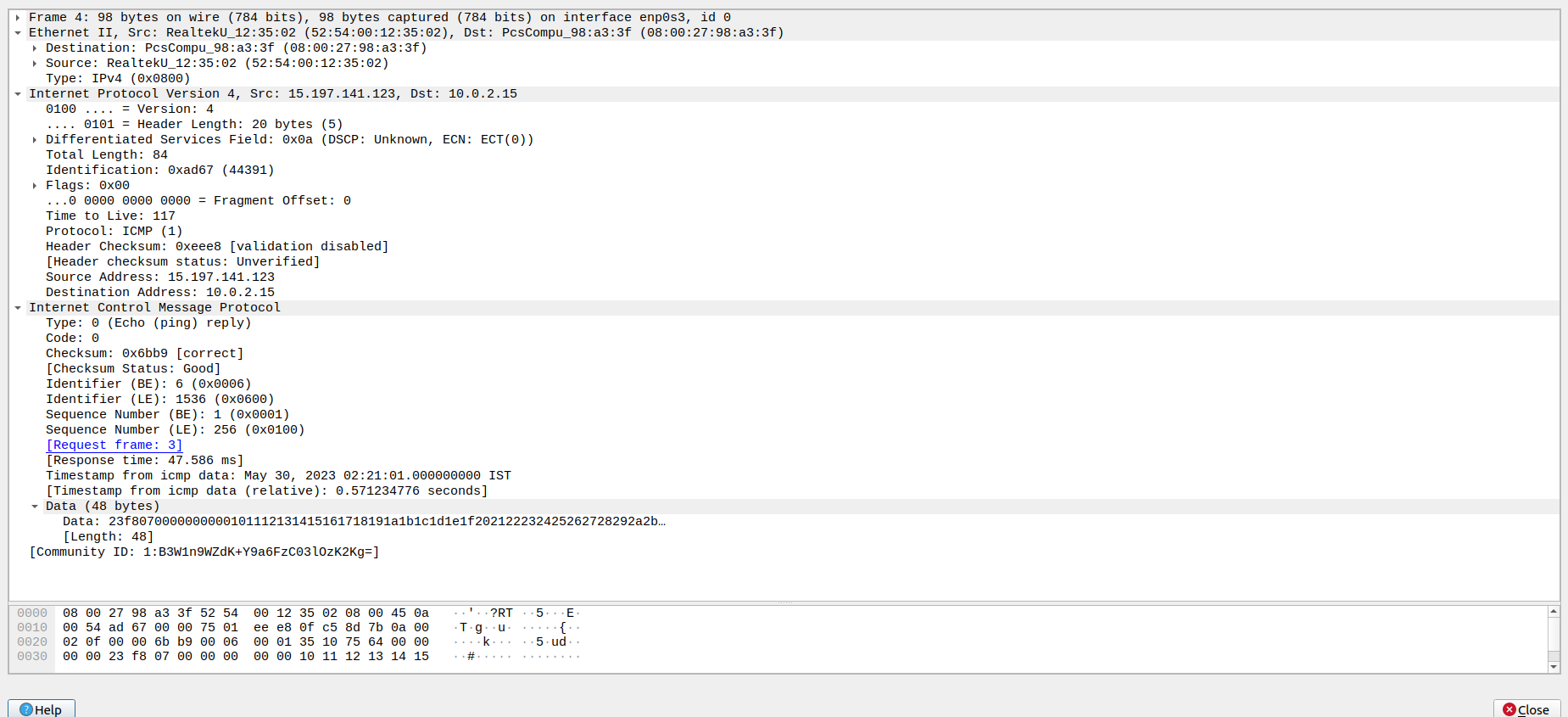


DNS Reply

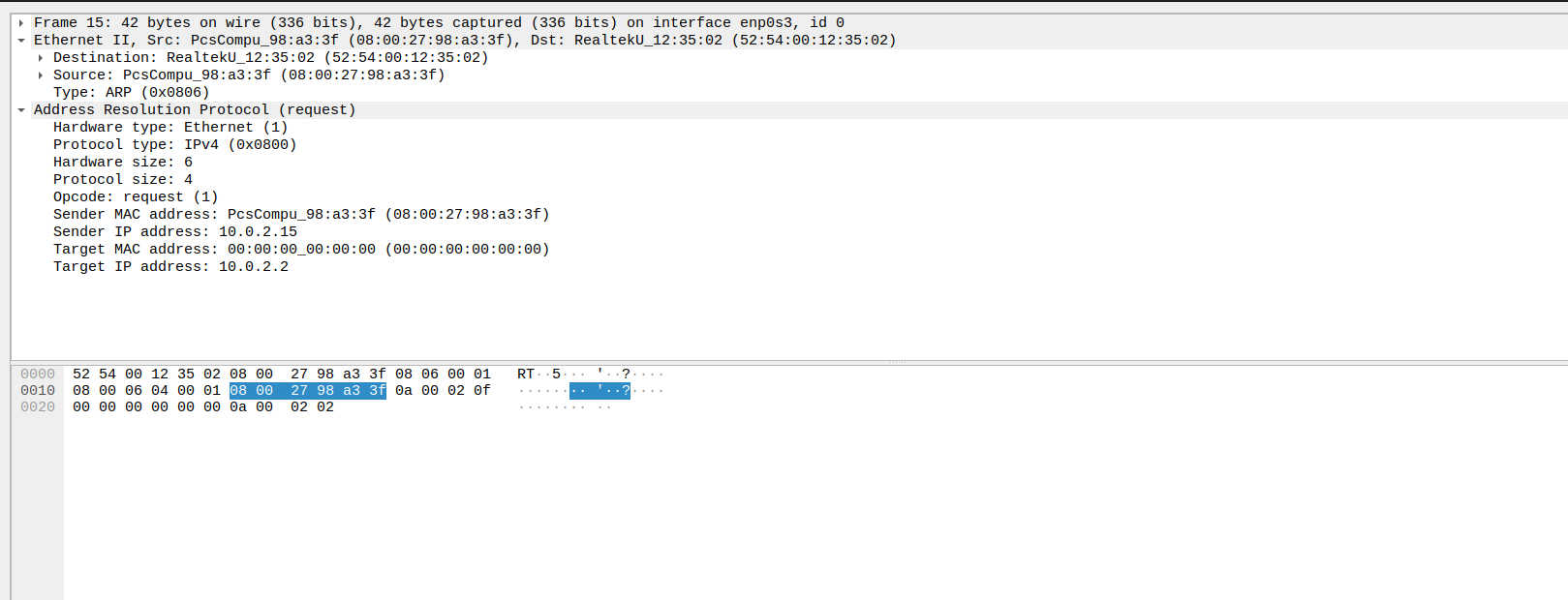


ICMP

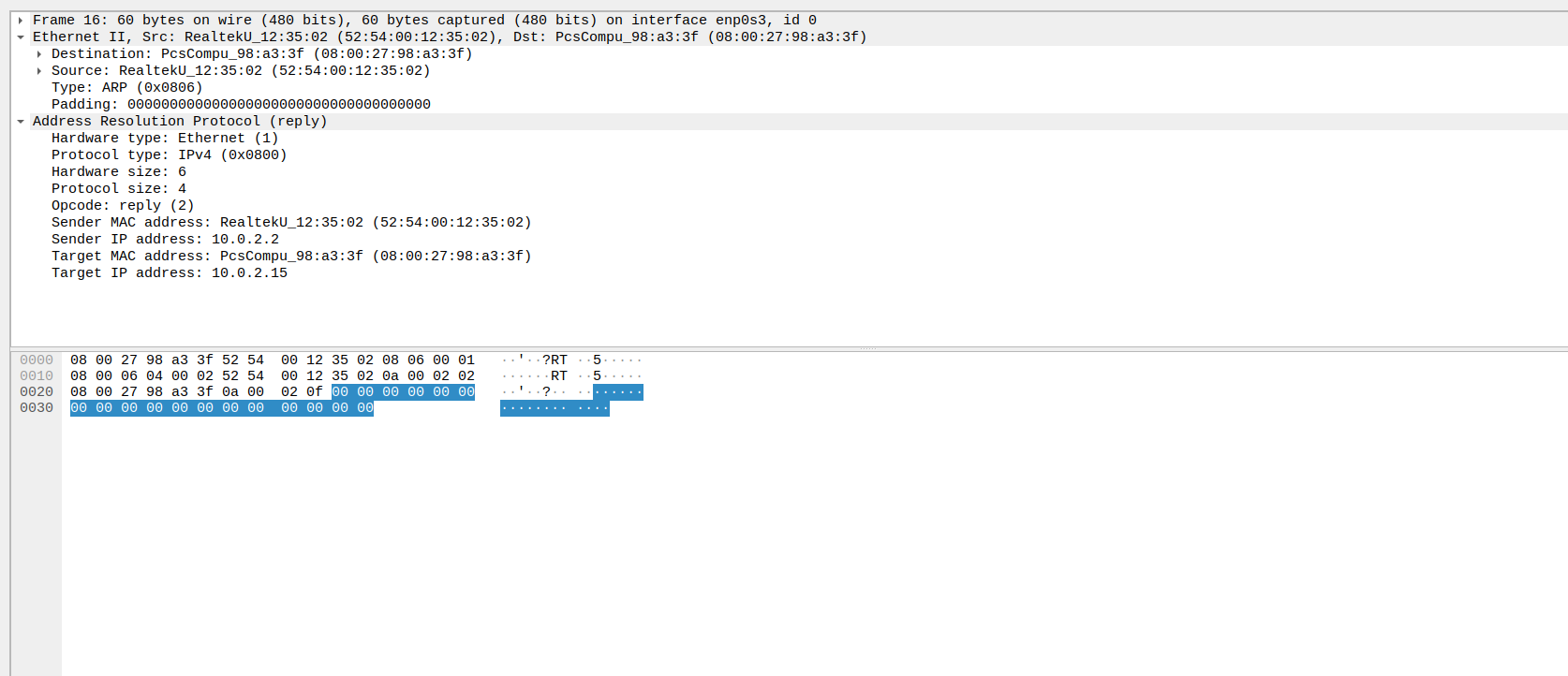




ARP (Request)



ARP (Reply)



THANK YOU!!