TRƯỜNG ĐẠI HỌC BÁCH KHOA

ĐẠI HỌC QUỐC GIA TP HỒ CHÍ MINH

HOMEWORK

MẠNG MÁY TÍNH (THỰC HÀNH) – LAB 6

Giảng viên hướng dẫn: Ths. Bùi Xuân Giang

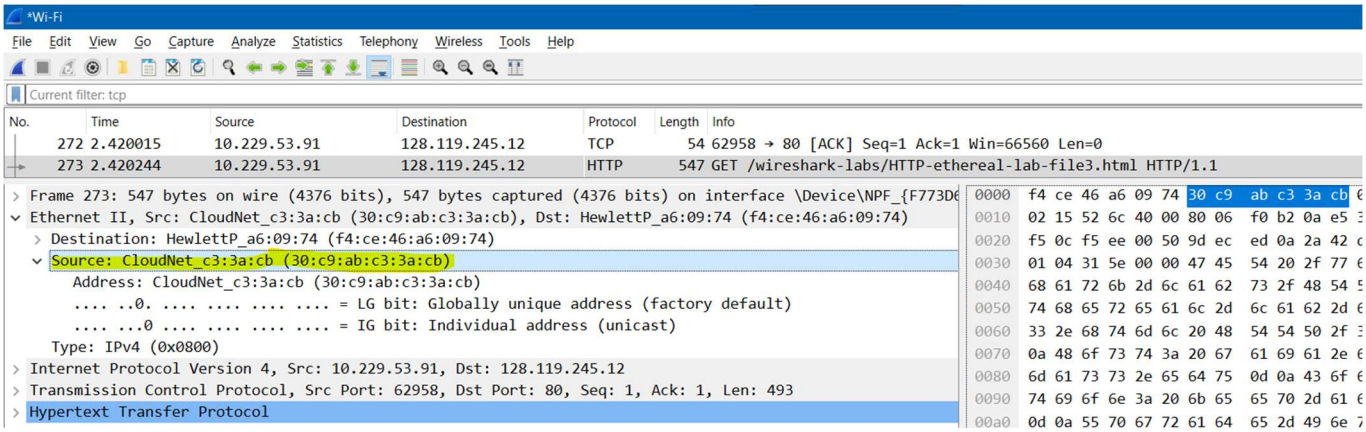
Sinh viên thực hiện: Trần Minh Tân

Mã số sinh viên: 2012018

Lớp: L10

Thành phố Hồ Chí Minh – 2022

Part 1:Capturing and analyzing Ethernet frames



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

The Ethernet address of my computer is 30:c9:ab:c3:3a:cb

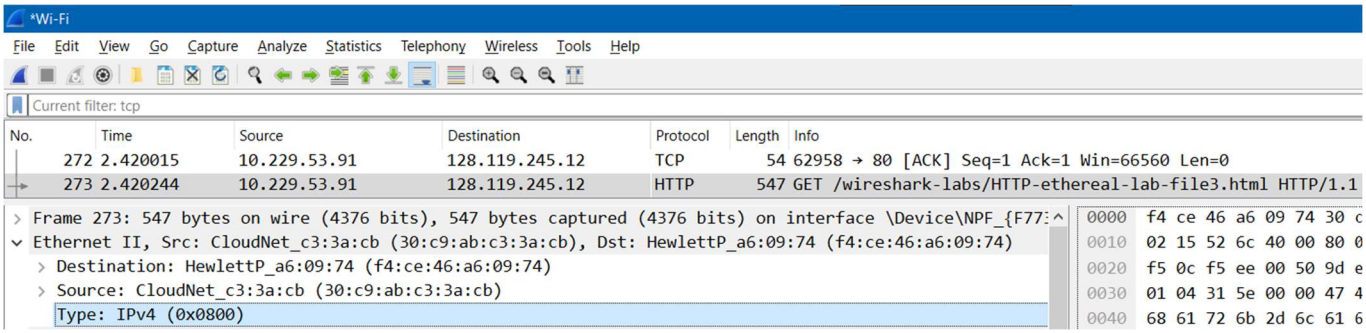
2. What is the 48-bit destination address in the Ethernet frame? Is this the Ethernet address of gaia.cs.umass.edu? (Hint: the answer is no). What device has this as its Ethernet address? [Note: this is an important question, and one that students sometimes get wrong. Re-read pages 468-469 in the text and make sure you understand the answer here.]

The 48-bit destination address in the Ethernet frame is f4:ce:46:a6:09:74

The device has this as its Ethernet address is my router (Hewlett Package)

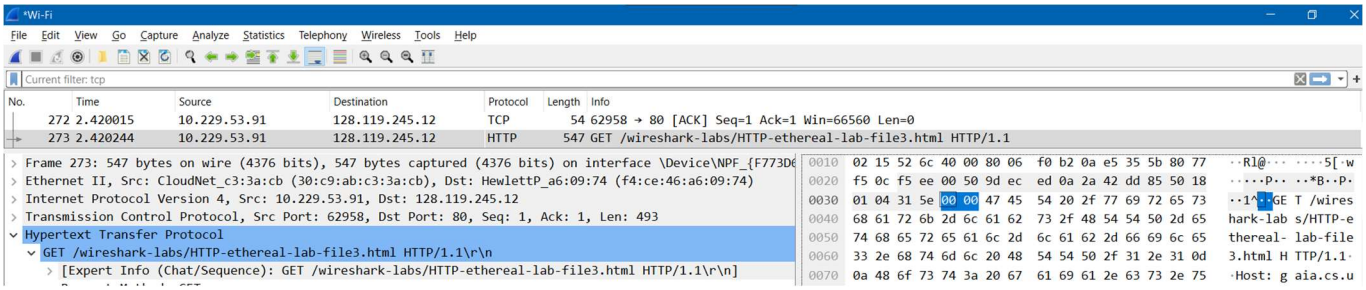
3. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?

The upper layer protocol this correspond to is IP protocol (0x0800).



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

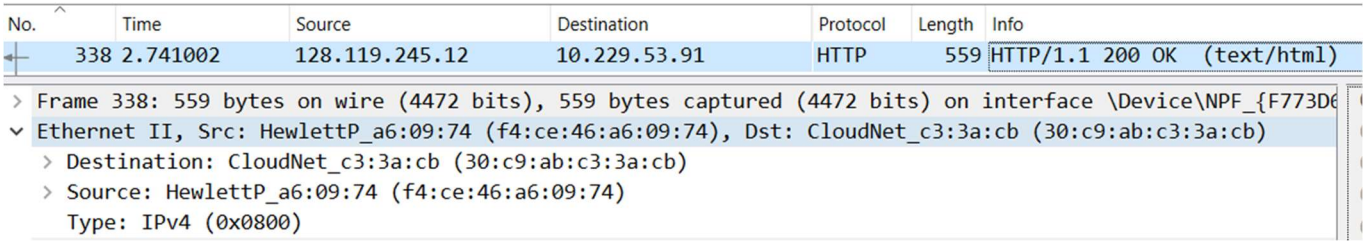
The length from the very start of the Ethernet frame to the ASCII “G” in “GET” appear is 52 bytes



Next, answer the following questions, based on the contents of the Ethernet frame containing the first byte of the HTTP response message.

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

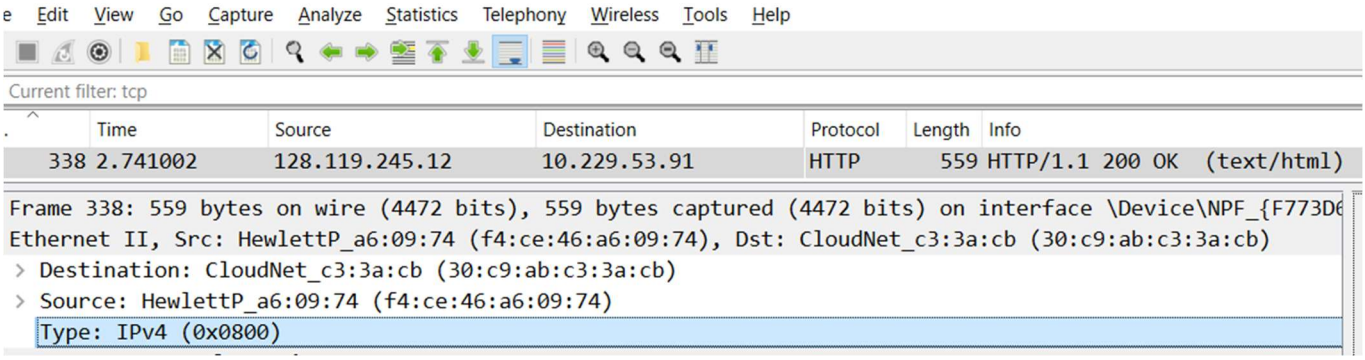
The value of the Ethernet source address is f4:ce:46:a6:09:74. This is the address of my router



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

According to the picture above, the destination address in the Ethernet frame is 30:c9:ab:c3:3a:cb. This is the Ethernet address of my computer.

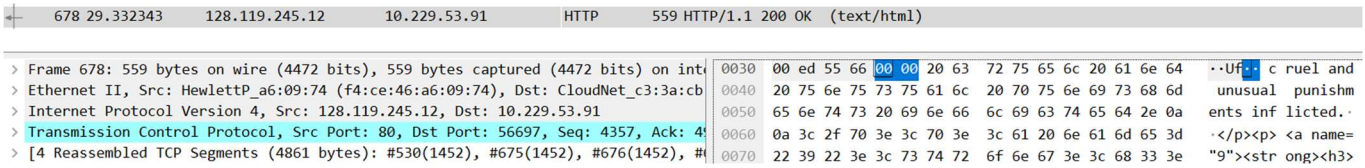
7. Give the hexadecimal value for the two-byte Frame type field. What upper layer protocol does this correspond to?



The upper layer protocol this correspond to is IP address.

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?

The length from the very start of the Ethernet frame to the ASCII “O” in “OK” appear is 52 bytes



PART 2 The Address Resolution Protocol

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

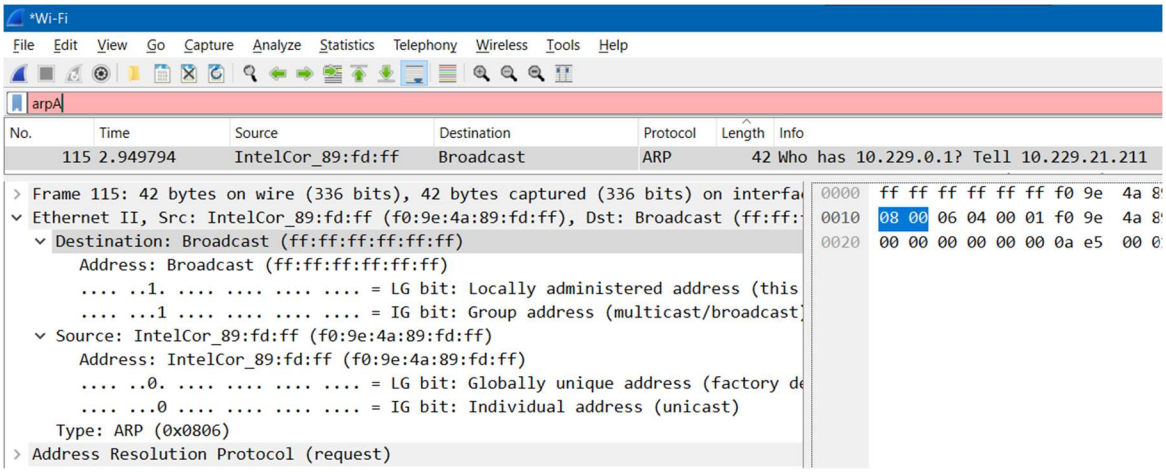
```
C:\Users\Admin>arp -a

Interface: 169.254.107.79 --- 0xc
  Internet Address      Physical Address      Type
  169.254.255.255       ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.192.152.143       01-00-5e-40-98-8f     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 10.230.160.91 --- 0x12
  Internet Address      Physical Address      Type
  10.230.0.1            f4-ce-46-a6-09-74     dynamic
  10.230.255.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\Admin>
```

Internet Address: IP address.

Physical Address: MAC address.

Type: the state of IP address (dynamic or static).

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



Destination address: ff:ff:ff:ff:ff:ff

Source address: f0:9e:3a:89:fd:ff

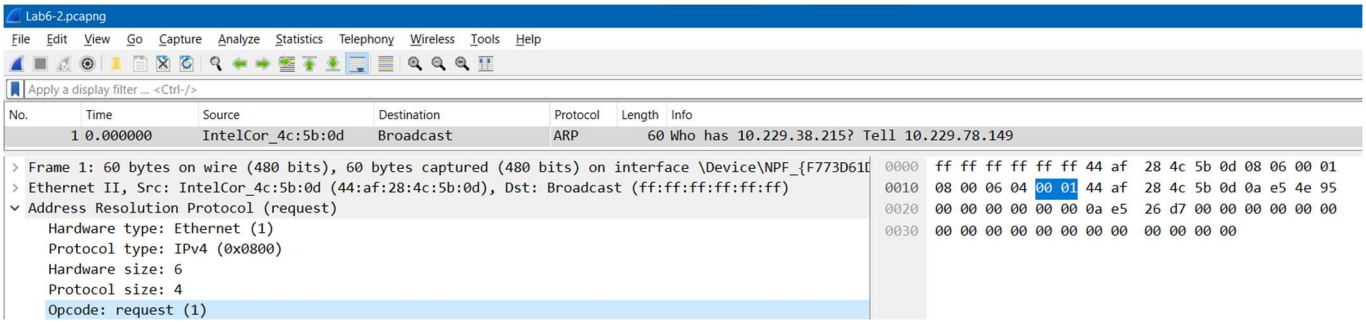
11. Give the hexadecimal value for the two-byte Ethernet Frame type field. What upper layer protocol does this correspond to?

The hexadecimal value for the two-byte Ethernet Frame is 0x0806. The upper layer protocol this correspond to is ARP.

12. Download the ARP specification from ftp://ftp.rfc-editor.org/in-notes/std/std37.txt. A readable, detailed discussion of ARP is also at http://www.erg.abdn.ac.uk/users/gorry/course/inet pages/arp.html.

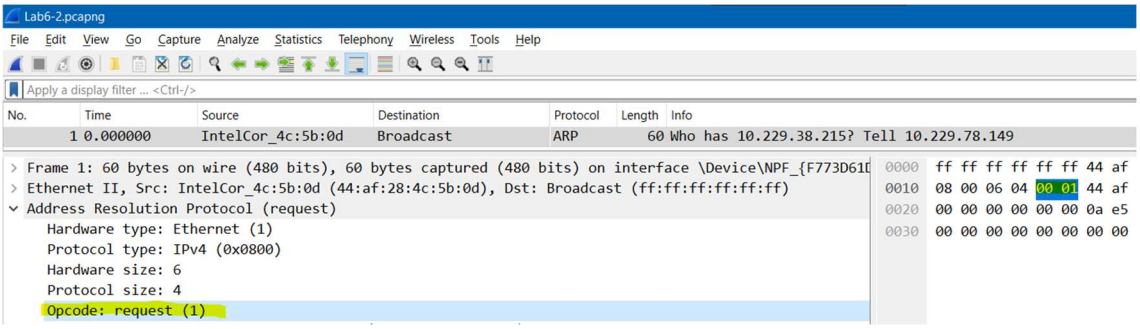
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

It begins 20 bytes from the very beginning of the Ethernet frame, as we can see in the screenshot below.



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?

The hex value for opcode field withing the ARP-payload of the request is 0x0001 as we can see in the screenshot below

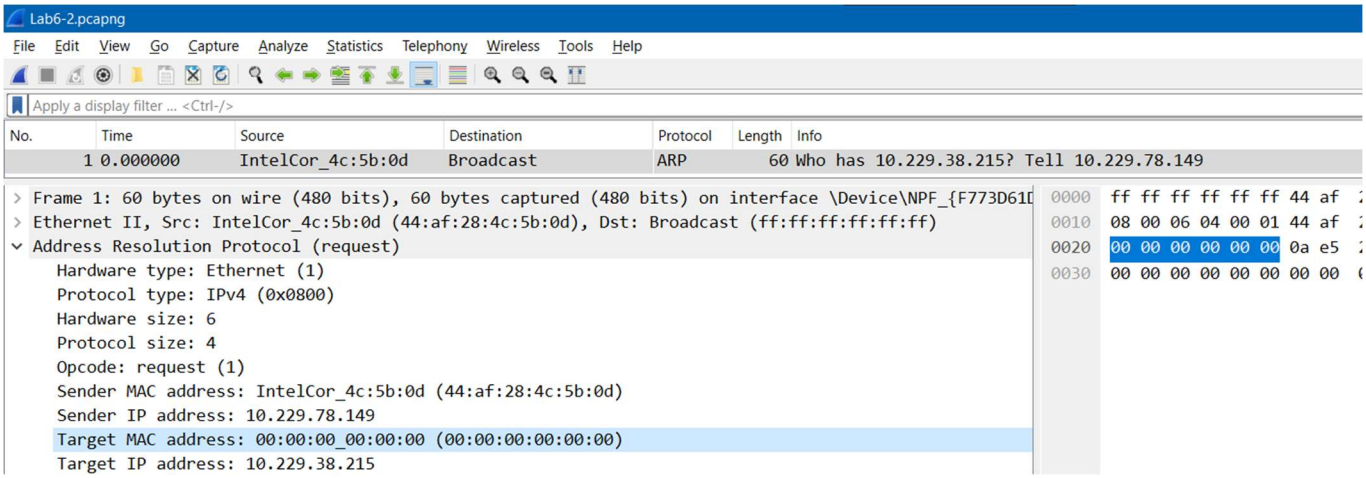


c) Does the ARP message contain the IP address of the sender?

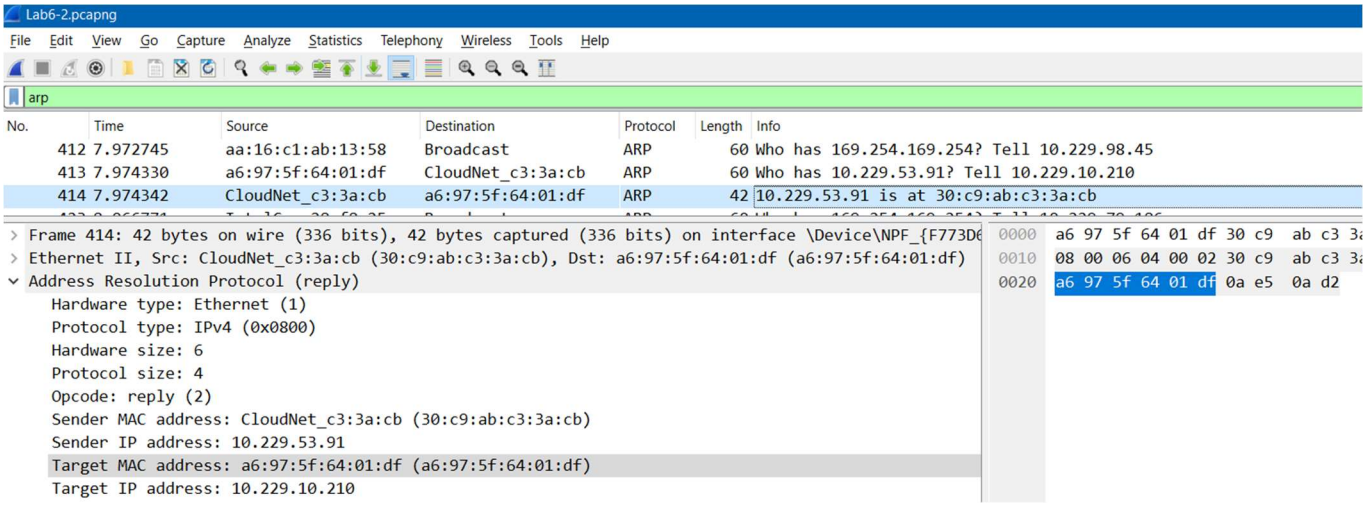
Yes, the ARP message containing the IP address 10.229.78.149 for the sender

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

The field "Target MAC address" is set to 00:00:00:00:00:00 to question the machine whose corresponding IP address (192.168.1.1) is being queried

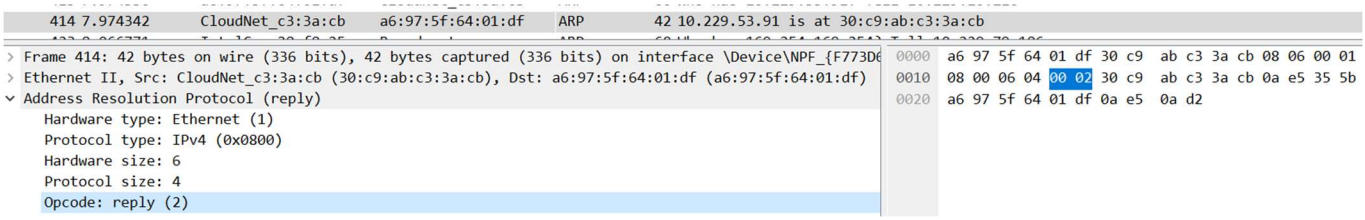


13. Now find the ARP reply that was sent in response to the ARP request.



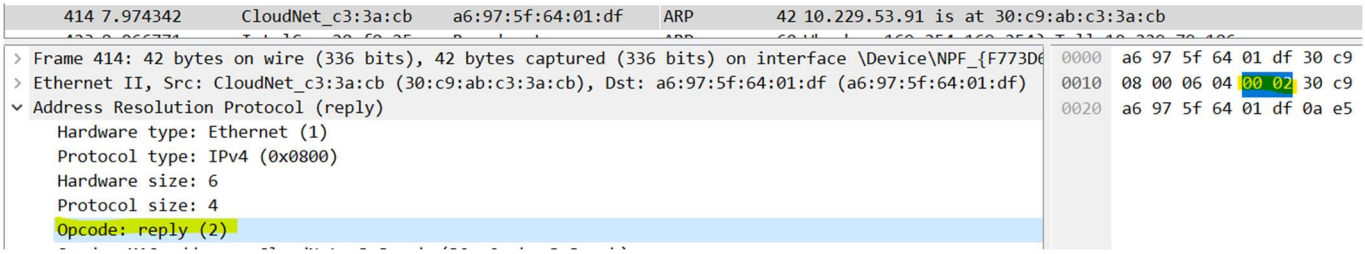
a) How many bytes from the very beginning of the Ethernet frame does the ARP opcode field begin?

There are 20 bytes from the very beginning of the Ethernet frame to the ARP opcode field.

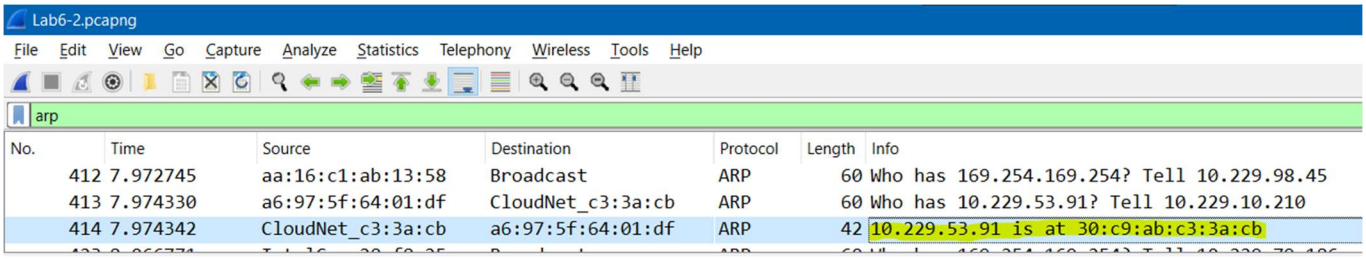


b) What is the value of the opcode field within the ARP-payload part of the Ethernet frame in which an ARP response is made?

The value of opcode fields within the ARP-payload part of the Ethernet frame in which an ARP is made is 0x002



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?

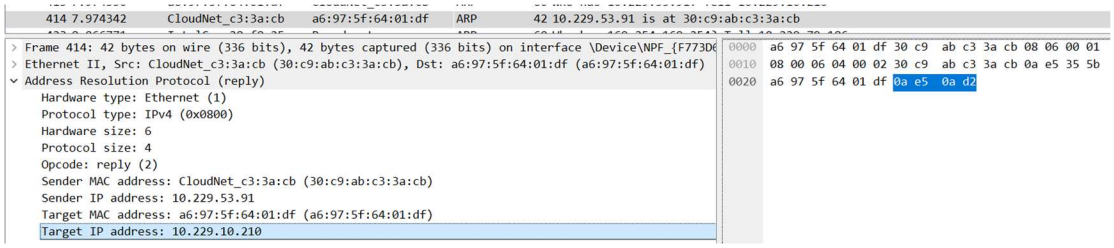


The answer in ARP reply message to the earlier ARP request appear in the "Info" fields – 10.229.53.91 is at 30:c9:ab:c3:3a:cb.

14. What are the hexadecimal values for the source and destination addresses in the

Ethernet frame containing the ARP reply message?

- Source address: 30:c9:ab:c3:3a:cb
- Destination address: a6:97:5f:64:01:df



15. Open the ethernet-ethereal-trace-1 trace file in http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip. 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 (sent in response to the ARP request in packet 6) in the packet trace?

There is no reply in this trace because we are not in the machine that sent the request.