

Computer Networks

Practice Session 1

Team members:

- ❖ Ahmad Ghalawinji
- ❖ Bashar Awada
- ❖ Nadine Zaatary

Network Interfaces:

Q1. Yes, a mobile phone has network interfaces, and many wireless interfaces such as WIFI, bluetooth, 4g..

Q2. According to ifconfig, our computer has 4 network interfaces: igb0, em0, lo0, usb0.

Q3. No, not all interfaces in the list correspond to a physical device because not all contain ethernet. They are both, wired and wireless, interfaces.

Q4. According to ifconfig, all interfaces are currently active. The interface must be “UP” for it to be active; we can see this using the ifconfig command.

Q5. IP address for em0 :147.171.108.67

IP address for lo0: 127.0.0.1

IPv6 for lo0 : inet6 ::1 prefixlen 128

inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3

(that is how they appeared in the terminal after using the ifconfig command)

A computer has several IP addresses since every interface has its own IP address.

Q6. IP addresses for the computer are unique only for ethernet interfaces, since we cannot change its IP address such as : igb0 and em0; and are not unique for other interfaces such as lo0 and usb0. Thus, the em0 interfaces are connected to the same network because they have the same first 24 bits that correspond to the network that we are connecting to.

Testing connectivity:

Q7. The “**ping 147.171.108.66**” command outputs:

1. The size of the sent packet which was 64 bytes
2. The destination IP address
3. The sequence number
4. The time to live
5. The time to return the packet (delay)

A copy form the terminal:

195 packets transmitted, 195 packets received, 0.0% packet loss

round-trip min/avg/max/stddev = 0.244/0.280/0.308/0.011 ms

- The minimum delay is: 0.244 ms.
- The average delay is: 0.280 ms.

Hence, we notice that the minimum and the average delay values are nearly the same.

Q8. The ping algorithm works by sending a packet (request) to the destination address and waiting for the other server to reply. The delay time is calculated from the time a request packet is sent to the server to the time the server responds.

Q9. --- universiteparis2019.fr ping statistics ---

A copy form the terminal:

12 packets transmitted, 12 packets received, 0.0% packet loss

- The average delay time from my PC is 13.819 ms.
- The average delay time from my neighbour's PC is 14.464 ms.

--- wwwr53.cc.columbia.edu ping statistics ---

A copy form the terminal:

12 packets transmitted, 12 packets received, 0.0% packet loss

- The average delay time from my PC is 85.397 ms.
- The average delay time from my neighbour's PC is 85.397.

Hence, we notice that the average delay values for both PCs (mine and my neighbour's) are very close, or the same.

Q10. Distance = Velocity * Time

Time= average delay / 2

- Distance from my PC to universiteparis2019 = 1381900 m
- Distance from neighbour's PC to universiteparis2019 = 1446400 m
- Distance from my PC to www.wwwr53.cc.columbia.edu = 8539700 m
- Distance from neighbour's PC to www.wwwr53.cc.columbia.edu = 8539700 m

Yes, the results seem consistent with the probable geographical location of the hosts.

Packet capture with Wireshark:

Q11. Each line in the interface of Wireshark represents a packet.

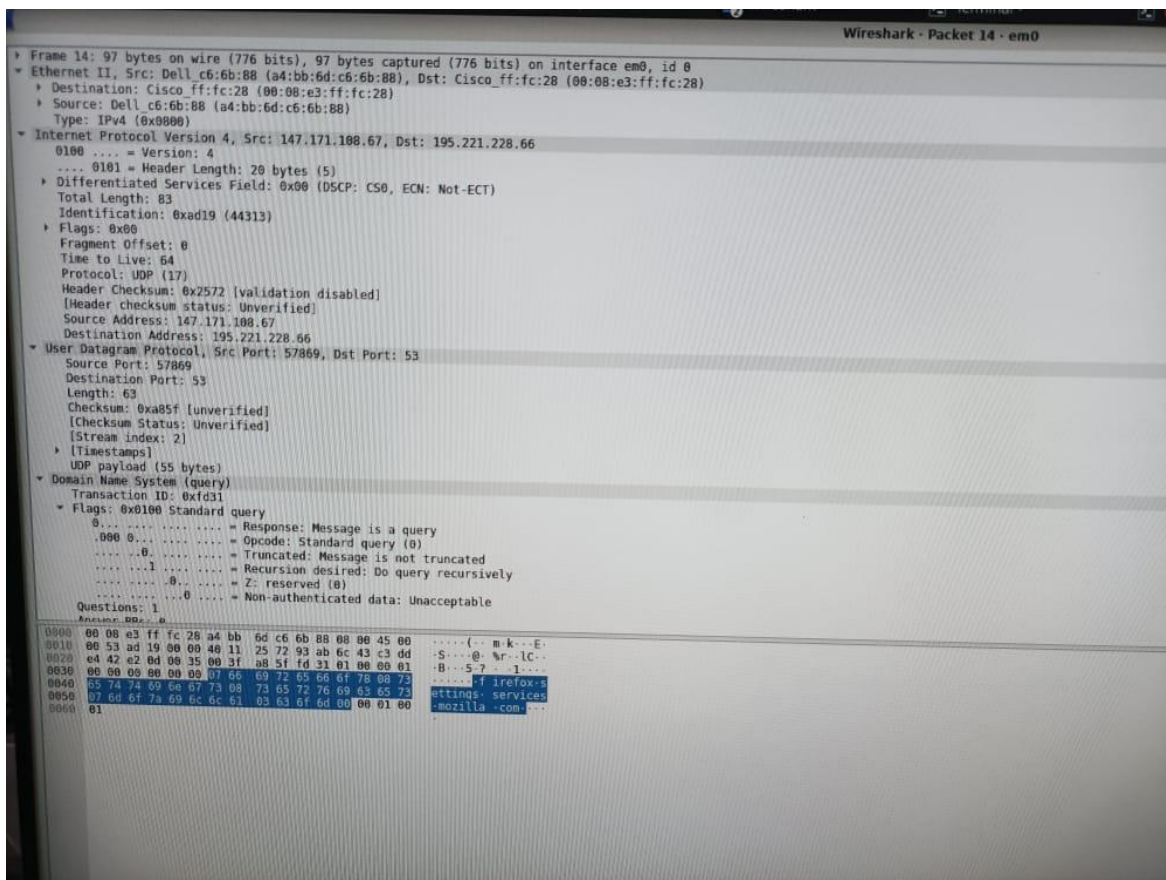
Q12. Protocols are: ARP, TCP, STP, DNS.

Yes, we recognize the Transmission Control Protocol (TCP), the Address Resolution Protocol (ARP), and the Domain Name System (DNS).

Q13. UDP protocol is also contained in the packet besides DNS protocol.

Q14. The Total length for the packet found by wireshark is 97 bytes.

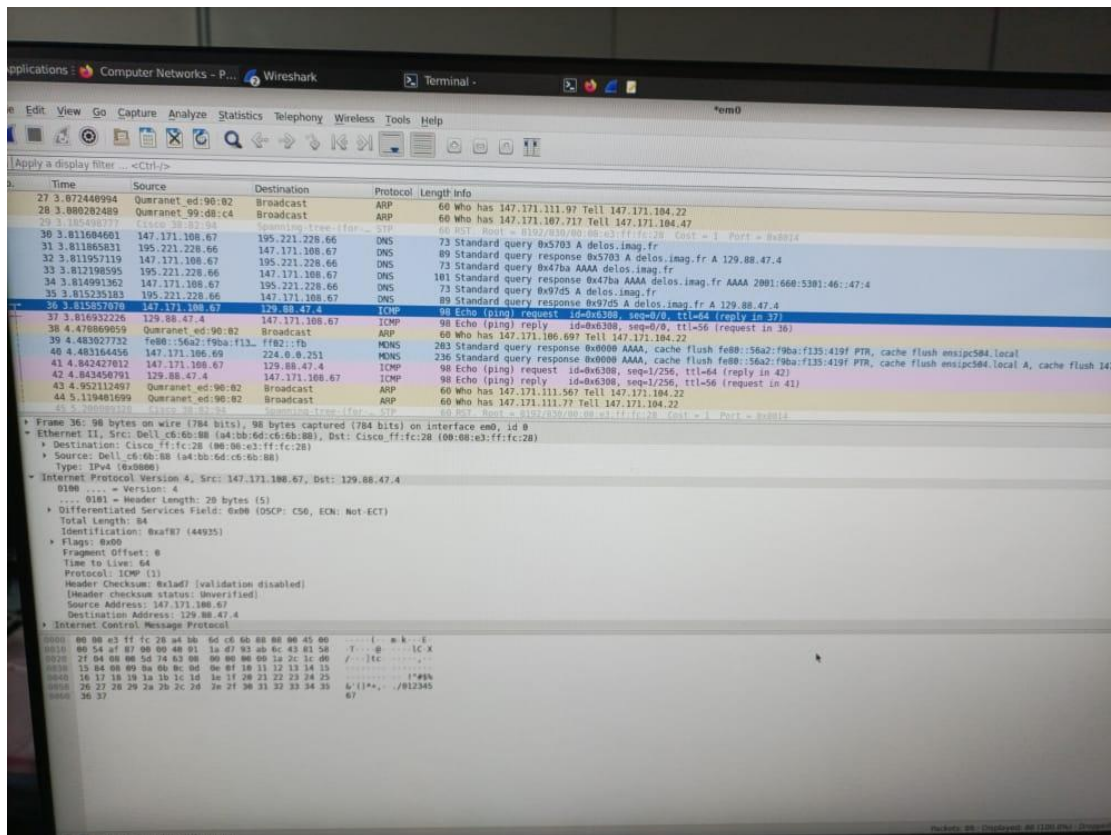
For the UDP protocol : the payload size is: 55 and the header size is 8 bytes.



Q15.

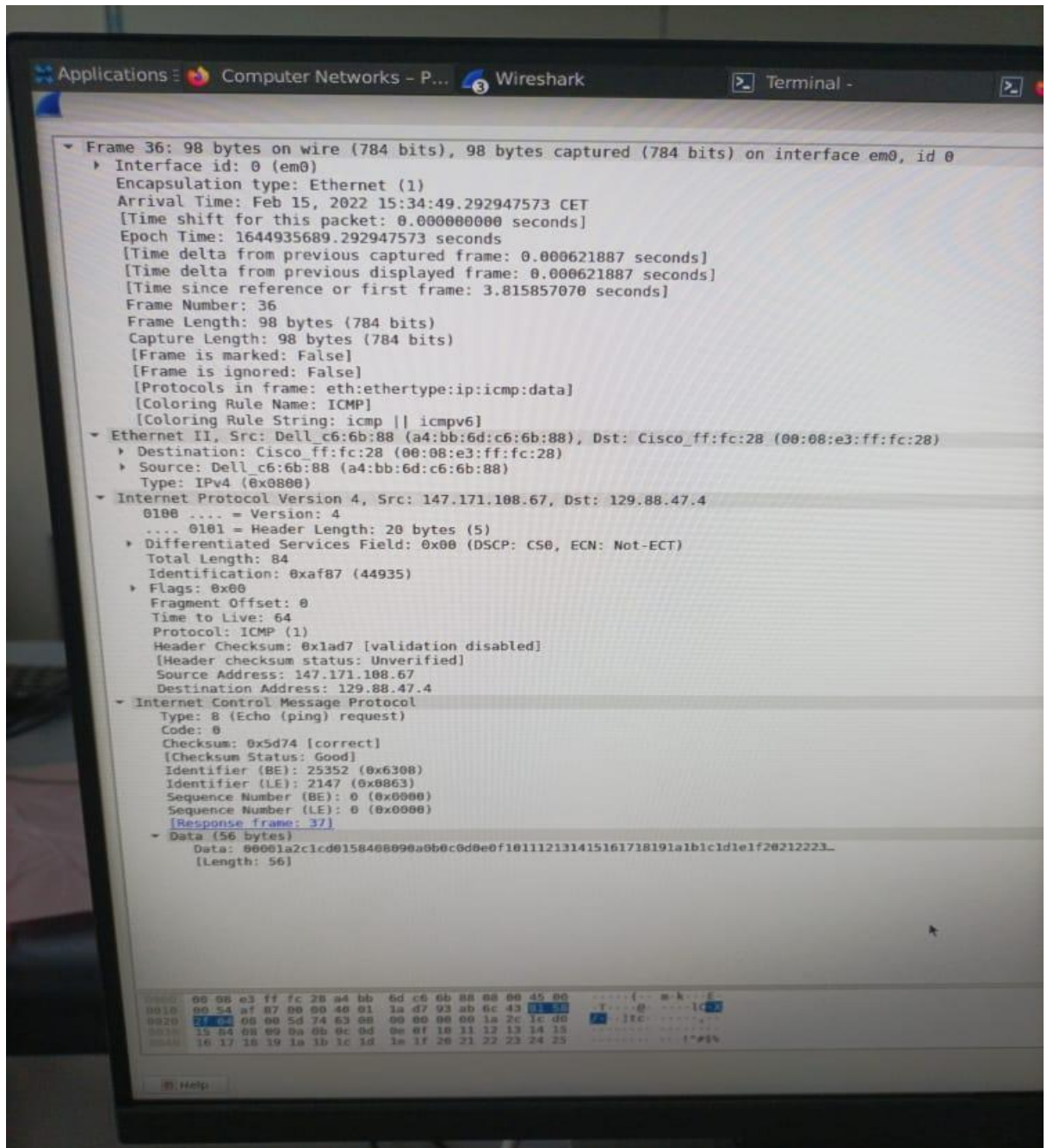
Packet size	IPv4 header	UDP header	UDP payload
97 bytes	20 bytes	8 bytes	55 bytes

Q16. The name of the protocol used by ping is ICMP protocol. It runs on the top of the IP address.



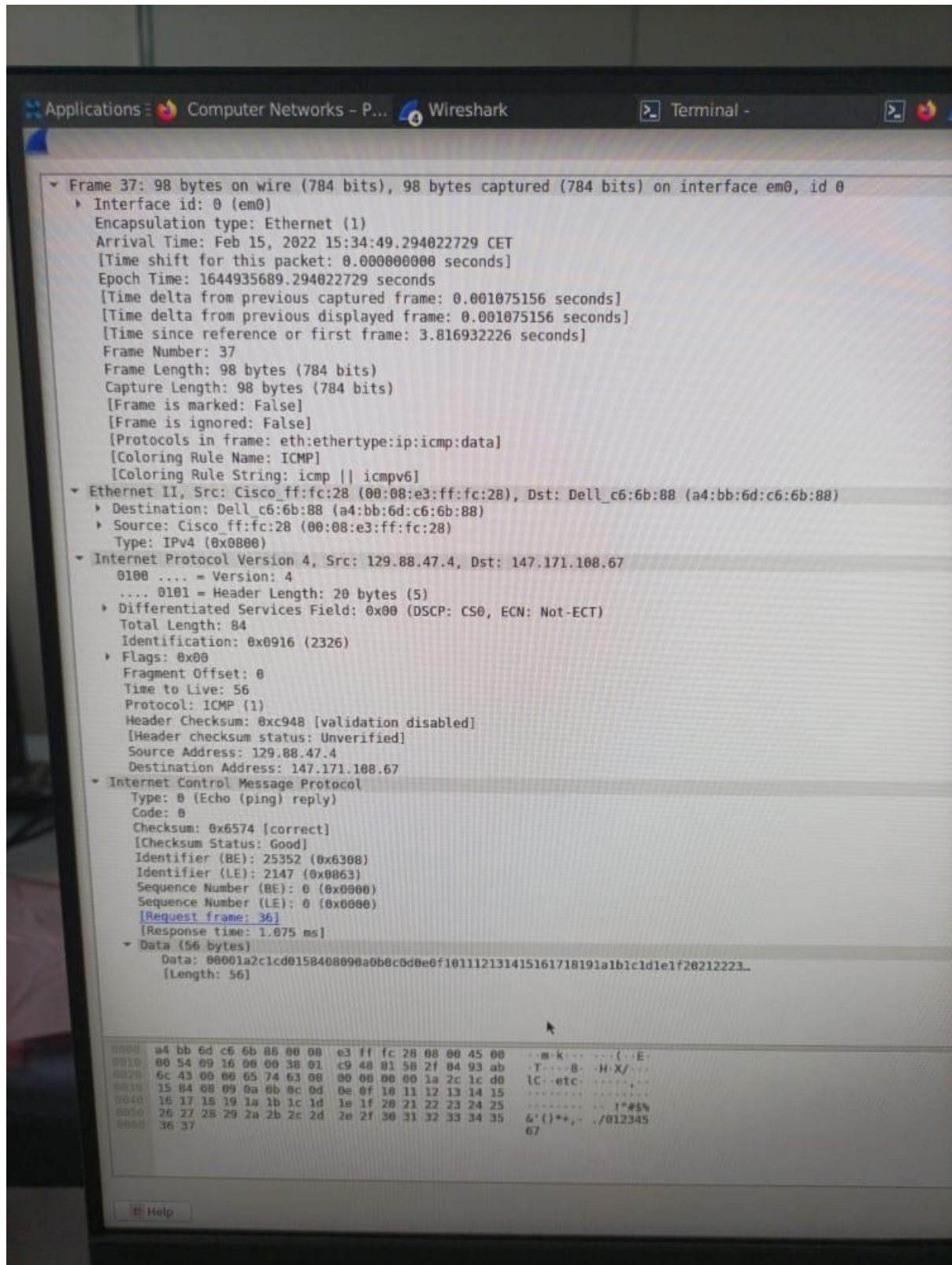
Q17. Packet at IP layer has:

- Source Address: 147.171.108.67
- Destination Address: 129.88.47.4



Q18. The value of the Type field is: 8 (Echo (ping) request)

The value of the Code field is: 0



- **Type Field:** The type or classification of the ICMP message, based on the RFC specification. The ICMP protocol has a field called type, which indicates what type the ICMP packet is. If the type field is 8, then the packet is an ICMP echo (ping) request, while if the type field is 0, then the packet is an ICMP echo (ping) reply. It is a one-byte field at the very beginning of the ICMP protocol header.
- **Code Field:** The subclassification of the ICMP message, based on the RFC specification.

Q19. The type field has changed from 8 in the request to 0 in the reply.

Q20. Delay time using Wireshark = $3.81693226 - 3.815857070 = 0.00107519 \text{ s} = 1.075 \text{ ms}$.

A copy from the terminal using the **ping** command:

64 bytes from 129.88.47.4: icmp_seq=1 ttl=56 time=1.075 ms

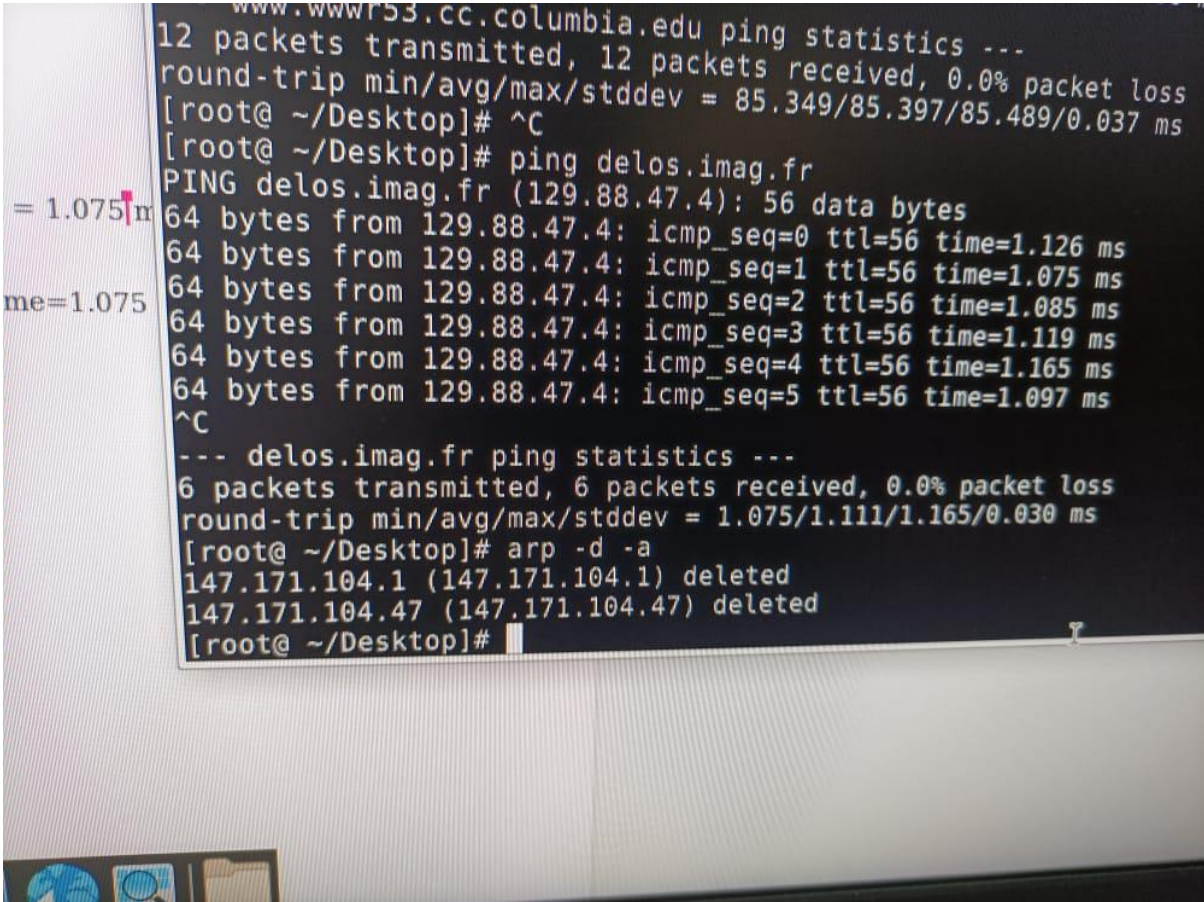
The delay reported using ping is: 1.075 ms.

```

File Edit View Terminal Tabs Help
64 bytes from 128.59.105.24: icmp_seq=6 ttl=241 time=85.365 ms
64 bytes from 128.59.105.24: icmp_seq=7 ttl=241 time=85.391 ms
64 bytes from 128.59.105.24: icmp_seq=8 ttl=241 time=85.349 ms
64 bytes from 128.59.105.24: icmp_seq=9 ttl=241 time=85.363 ms
64 bytes from 128.59.105.24: icmp_seq=10 ttl=241 time=85.401 ms
64 bytes from 128.59.105.24: icmp_seq=11 ttl=241 time=85.406 ms
^C
=1.075 --- www.wvr53.cc.columbia.edu ping statistics ---
12 packets transmitted, 12 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 85.349/85.397/85.489/0.037 ms
[root@ ~/Desktop]# ^C
[root@ ~/Desktop]# ping delos.imag.fr
PING delos.imag.fr (129.88.47.4): 56 data bytes
64 bytes from 129.88.47.4: icmp_seq=0 ttl=56 time=1.126 ms
64 bytes from 129.88.47.4: icmp_seq=1 ttl=56 time=1.075 ms
64 bytes from 129.88.47.4: icmp_seq=2 ttl=56 time=1.085 ms
64 bytes from 129.88.47.4: icmp_seq=3 ttl=56 time=1.119 ms
64 bytes from 129.88.47.4: icmp_seq=4 ttl=56 time=1.165 ms
64 bytes from 129.88.47.4: icmp_seq=5 ttl=56 time=1.097 ms
^C
--- delos.imag.fr ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.075/1.111/1.165/0.030 ms
[root@ ~/Desktop]#

```

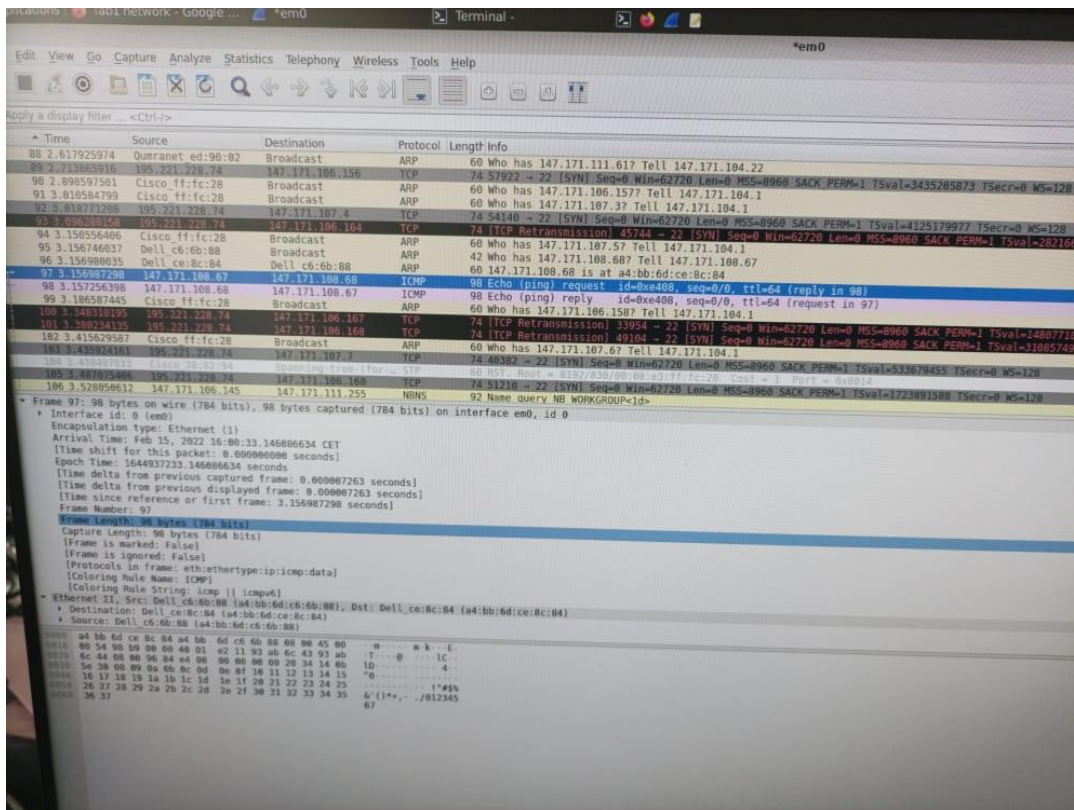

Understanding ARP :



```
www.wor53.cc.columbia.edu ping statistics ---
12 packets transmitted, 12 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 85.349/85.397/85.489/0.037 ms
[root@ ~/Desktop]# ^C
[root@ ~/Desktop]# ping delos.imag.fr
PING delos.imag.fr (129.88.47.4): 56 data bytes
64 bytes from 129.88.47.4: icmp_seq=0 ttl=56 time=1.126 ms
64 bytes from 129.88.47.4: icmp_seq=1 ttl=56 time=1.075 ms
64 bytes from 129.88.47.4: icmp_seq=2 ttl=56 time=1.085 ms
64 bytes from 129.88.47.4: icmp_seq=3 ttl=56 time=1.119 ms
64 bytes from 129.88.47.4: icmp_seq=4 ttl=56 time=1.165 ms
64 bytes from 129.88.47.4: icmp_seq=5 ttl=56 time=1.097 ms
^C
--- delos.imag.fr ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.075/1.111/1.165/0.030 ms
[root@ ~/Desktop]# arp -d -a
147.171.104.1 (147.171.104.1) deleted
147.171.104.47 (147.171.104.47) deleted
[root@ ~/Desktop]#
```

= 1.075
me=1.075

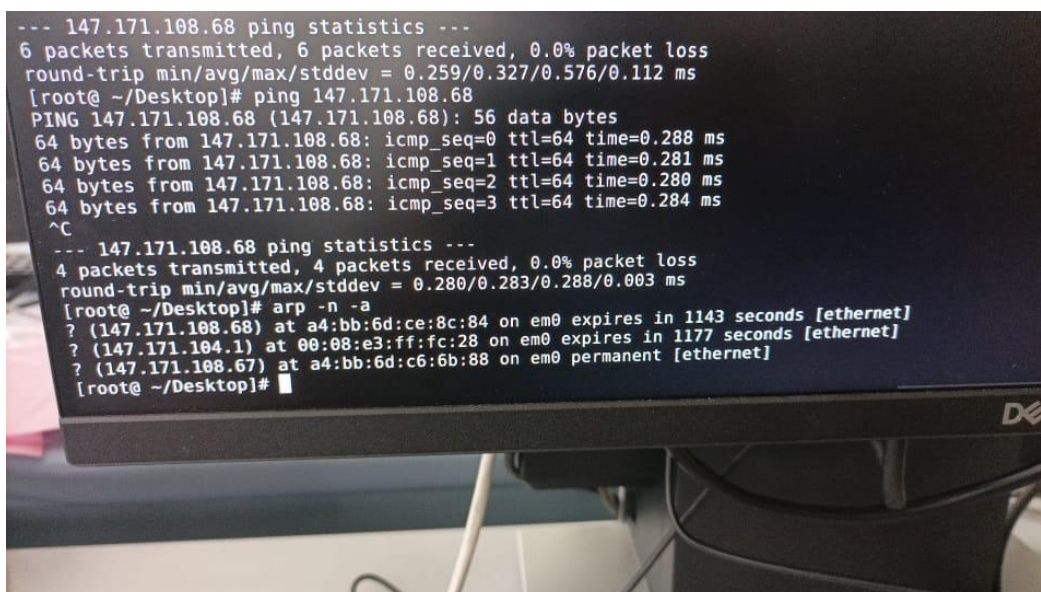
Q21. We see two kinds of ARP packets. The sender computer sends an ARP packet with request opcode and the target computer answers with icmp reply opcode and it's mac address. It occurs before the packets generated by ping.



Q22. There are no ARP packets because the MAC addresses and the belonging IP addresses are already in the ARP table.

Q23. ARP is what maps OSI Layer 2 addresses to Layer 3 addresses. In other words, ARP maps IP addresses to Ethernet MAC Addresses.

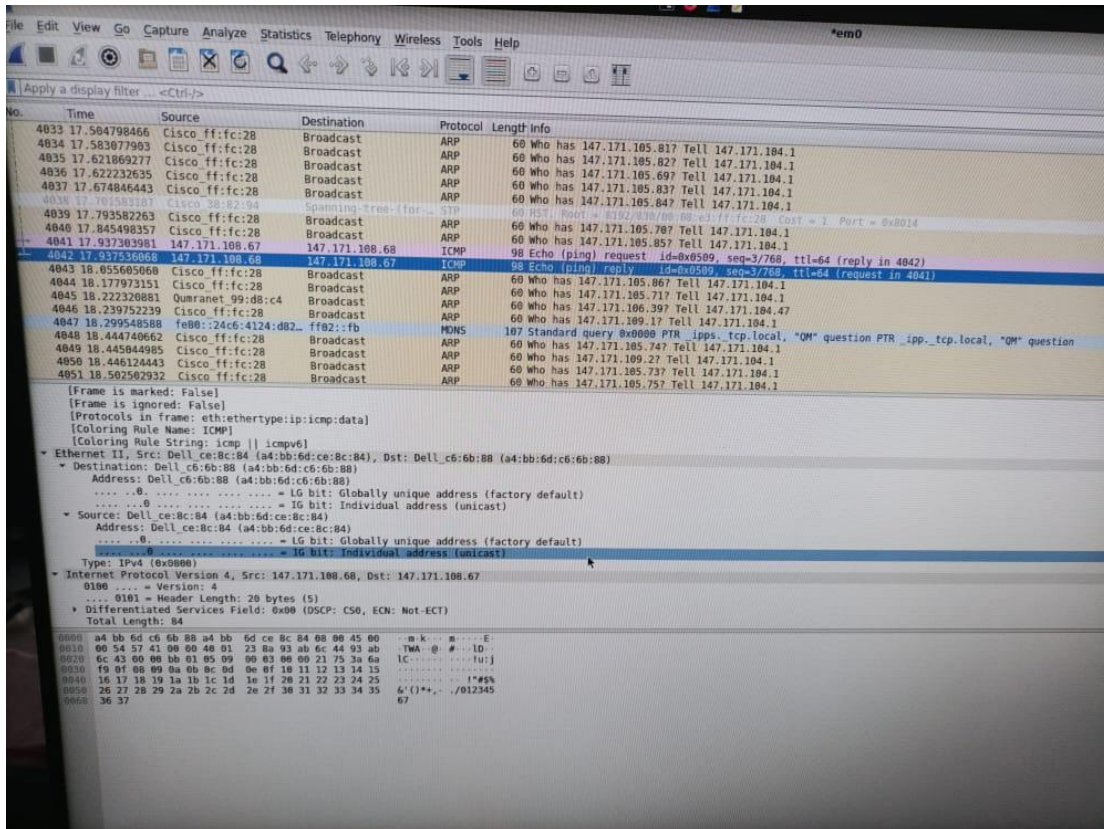
It can be also called an ARP cache because it stores the IP and the MAC in its own table.



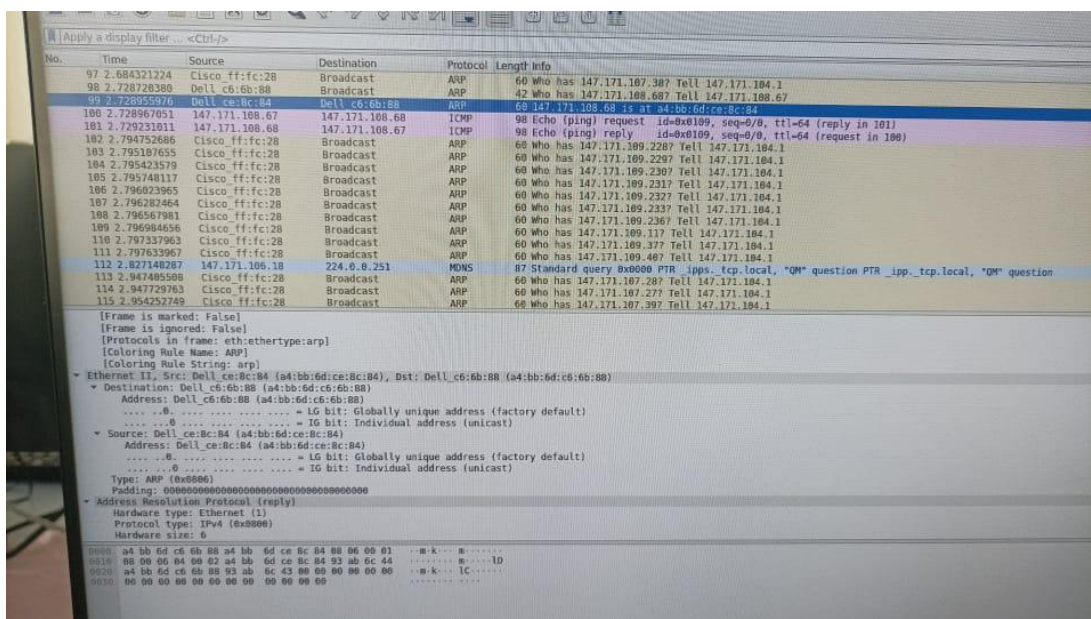
Local and remote networks:

Q24.

1. Captured by ICMP reply as shown in the picture below:

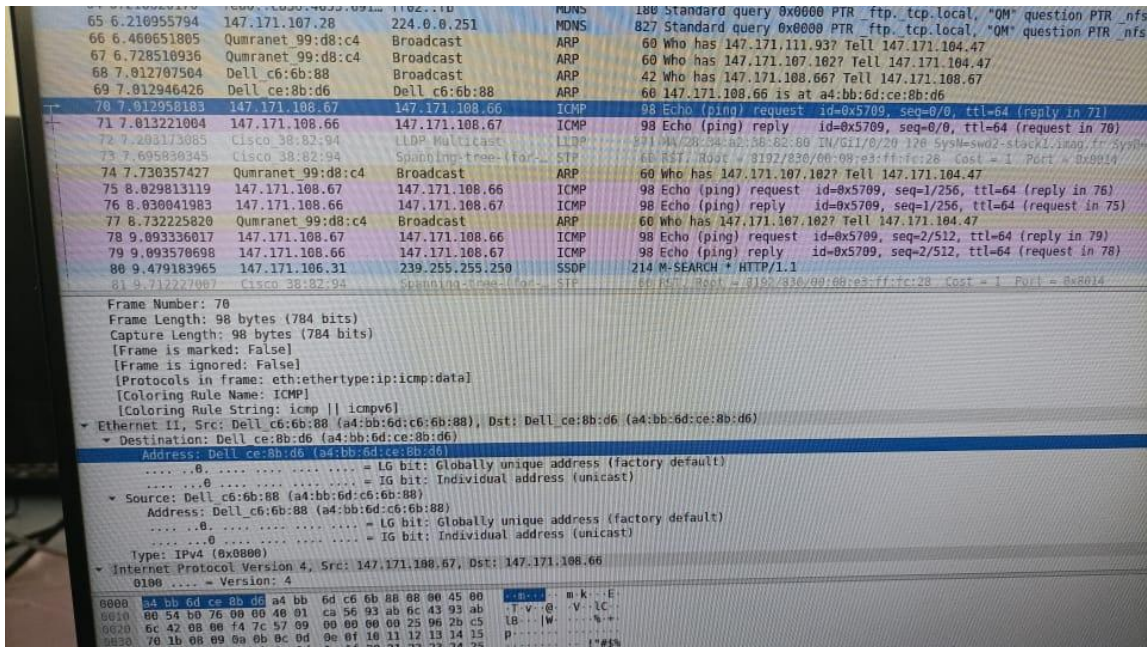


2. Captured by Arp request picture:



Address :Address: Dell_ce:8c:84 (a4:bb:6d:ce:8c:84).

Q25. Address of another neighbour: Address: Dell_ce:8b:d6 (a4:bb:6d:ce:8b:d6).

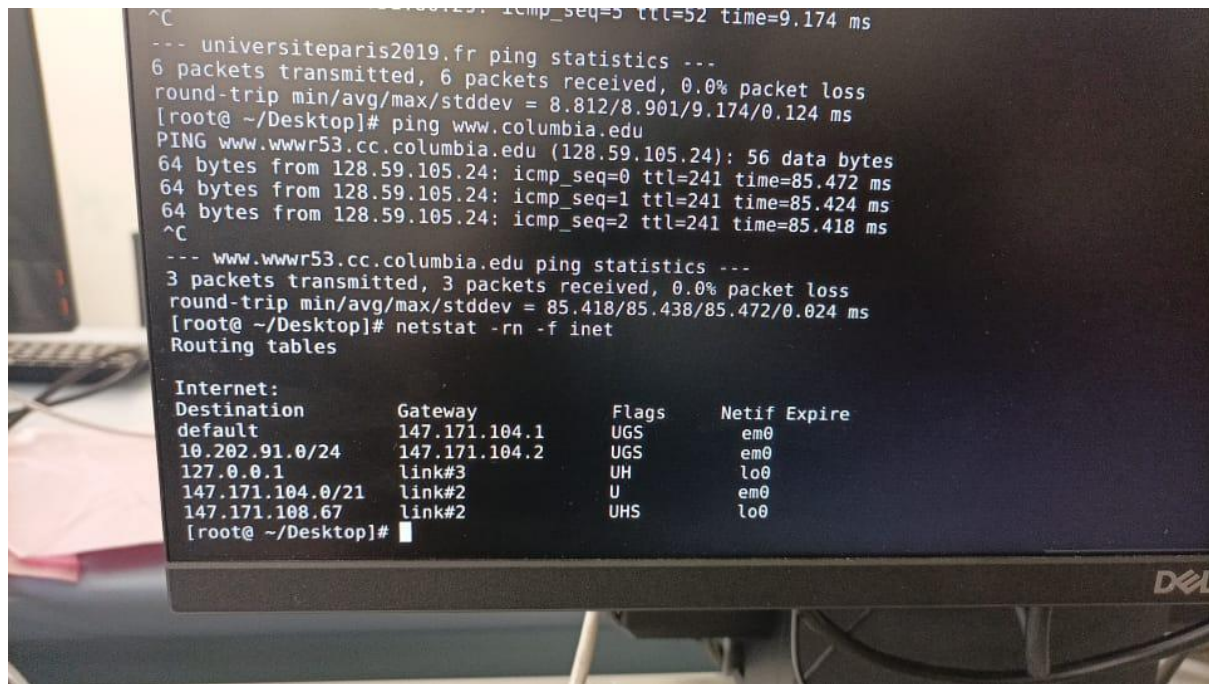


Q26. The Destination Ethernet address of the query packet is: Address: Cisco_ff:fc:28 (00:08:e3:ff:fc:28).

Q27. The destination Ethernet address of the query packet is: Cisco_ff:fc:28 (00:08:e3:ff:fc:28)

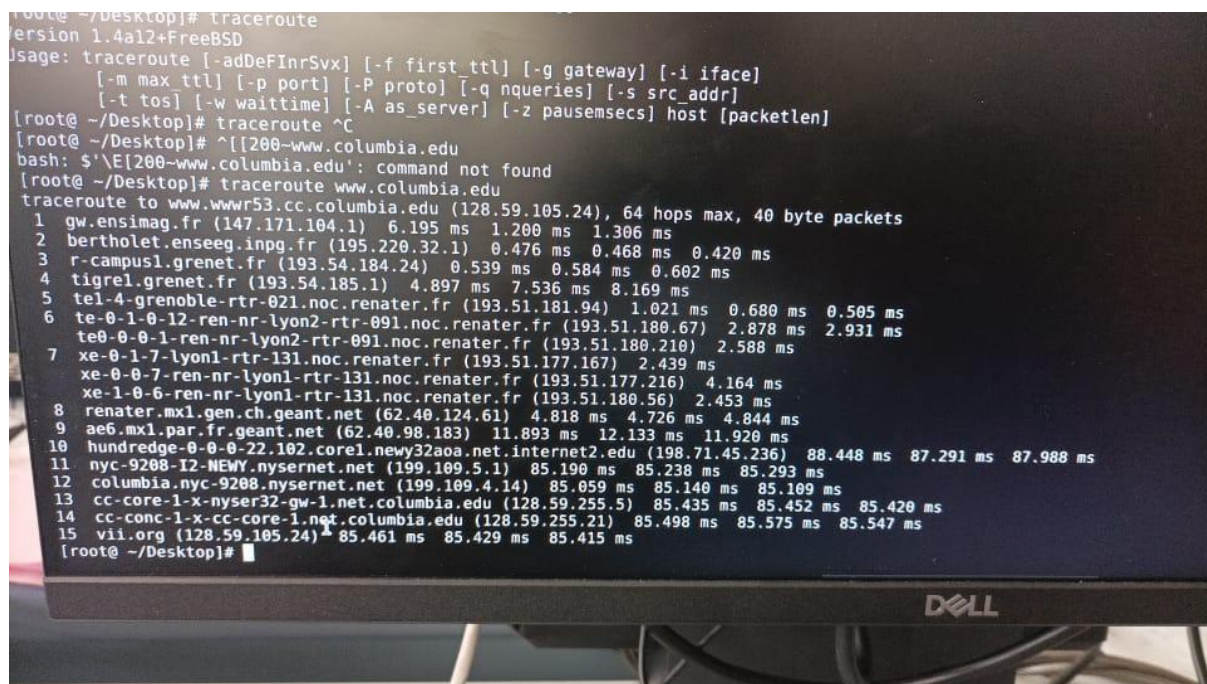
We obtained the same address in the DNS query because we are searching to the destination in the same gateway.

Q28. The two queries passed by the same gateway which is related to the em0 interface thus we have the same destination ethernet address.



Traceroute

Q29.



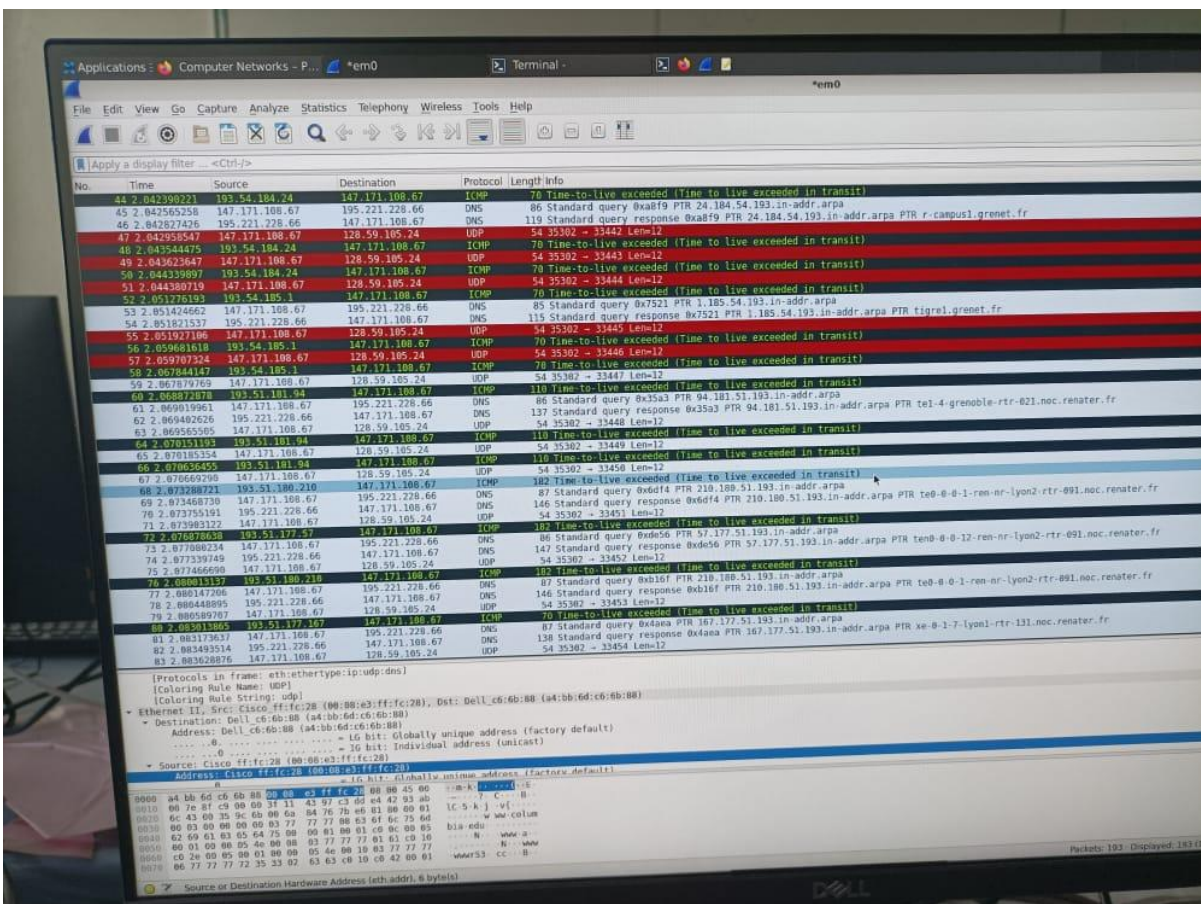
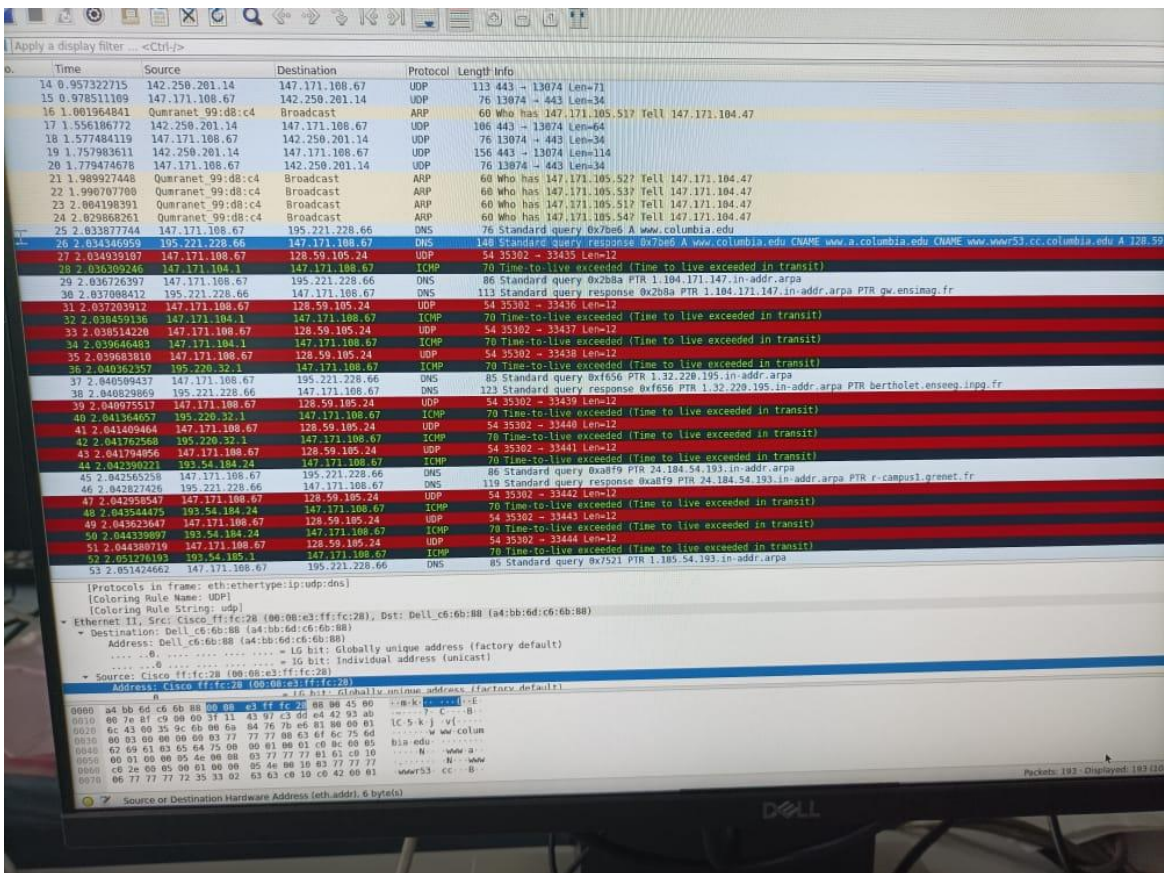

```

10 100.64.1.1.par.fr.geant.net (62.40.98.183) 11.893 ms 12.133 ms 11.920 ms
11 hundredge-0-0-0-22.102.corel.newy32aoa.net.internet2.edu (198.71.45.236) 88.448 ms 87.291 ms 87.988 ms
12 nyc-9208-I2-NEWY.nysernet.net (199.109.5.1) 85.190 ms 85.238 ms 85.293 ms
13 columbia.nyc-9208.nysernet.net (199.109.4.14) 85.059 ms 85.140 ms 85.109 ms
14 cc-core-1-x-nyser32-gw-1.net.columbia.edu (128.59.255.5) 85.435 ms 85.452 ms 85.420 ms
15 cc-conc-1-x-cc-core-1.net.columbia.edu (128.59.255.21) 85.498 ms 85.575 ms 85.547 ms
16 vii.org (128.59.105.24) 85.461 ms 85.429 ms 85.415 ms
[root@ ~/Desktop]# traceroute universiteparis2019.fr
traceroute to universiteparis2019.fr (193.51.86.29), 64 hops max, 40 byte packets
1 gw.ensimag.fr (147.171.104.1) 0.792 ms 0.631 ms 0.639 ms
2 bertholet.enseeg.inpg.fr (195.220.32.1) 0.547 ms 0.490 ms 0.439 ms
3 r-campus1.grenet.fr (193.54.184.24) 0.605 ms 0.552 ms 0.485 ms
4 tigre1.grenet.fr (193.54.185.1) 84.713 ms 5.622 ms 11.527 ms
5 tel-4-grenoble-rtr-021.noc.renater.fr (193.51.181.94) 0.844 ms 0.701 ms 0.970 ms
6 te-0-1-0-12-ren-nr-lyon2-rtr-091.noc.renater.fr (193.51.180.67) 8.727 ms 8.937 ms 8.734 ms
7 xe1-1-9-paris2-rtr-131.noc.renater.fr (193.51.177.42) 8.943 ms
8 xe0-1-9-paris2-rtr-131.noc.renater.fr (193.51.177.144) 8.879 ms
9 xe-0-0-1-paris2-rtr-131.noc.renater.fr (193.51.180.54) 9.160 ms
10 et-2-0-2-ren-nr-paris1-rtr-131.noc.renater.fr (193.55.204.192) 8.990 ms
11 et-3-1-1-ren-nr-paris1-rtr-131.noc.renater.fr (193.55.204.194) 9.230 ms
12 et-2-0-2-ren-nr-paris1-rtr-131.noc.renater.fr (193.55.204.192) 20.438 ms
13 te-0-0-0-11-ren-nr-odeon-rtr-091.noc.renater.fr (193.51.180.20) 8.927 ms
14 te-0-1-0-10-ren-nr-odeon-rtr-091.noc.renater.fr (193.55.204.6) 8.917 ms 9.257 ms
15 xe-0-3-0-odeon-rtr-111.noc.renater.fr (193.51.180.156) 8.468 ms 8.566 ms 8.563 ms
16 195.221.127.6 (195.221.127.6) 8.909 ms 8.546 ms 8.688 ms
17 * * *
18 * * *
19 up19.parisdescartes.fr (193.51.86.29) 9.228 ms 9.060 ms 8.919 ms
[root@ ~/Desktop]#

```

Q30. When passing from Lyon to columbia in line 9 to 10, we notice that the time difference increases a lot when the packet is transmitted between Lyon and columbia indicating that the 2 cities are far from each other.

Q31. By sending first a UDP request then getting a ICMP reply from every server and it is because we always want to trace the destination of the packet everytime is doing a roundtrip. We determine each hop when the destination is changed. The latency is measured by substituting the time of the icmp packet time and the udp packet time.



Q32. We always have a timeout.

If router does not respond within a timeout then traceroute prints an asterisk. Thus, if a packet is not acknowledged within the expected timeout, an asterisk is displayed.

To resolve the problem we can use -w parameter to set the number of seconds you want to wait before the timeout.

So here we can use "traceroute -w 10 www.jami.net"