Proyecto 1 - Wireshark

Wuke Zhang

1-ASIR

PARTE 1:

CMD como admin para poder borrar la cache ARP.

```
C:\windows\system32>arp -a
```

arp -d *: comando dado por chat gpt para borrar el cache.

VS

El comando que use para borrar la cache.

```
C:\windows\system32>netsh interface ip delete arpcache
Ok.
```

Ping a google

```
C:\windows\system32>ping www.google.es

Pinging www.google.es [2a00:1450:4003:80d::2003] with 32 bytes of data:
Reply from 2a00:1450:4003:80d::2003: time=31ms
Reply from 2a00:1450:4003:80d::2003: time=30ms
Reply from 2a00:1450:4003:80d::2003: time=31ms
Reply from 2a00:1450:4003:80d::2003: time=30ms

Ping statistics for 2a00:1450:4003:80d::2003:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 30ms, Maximum = 31ms, Average = 30ms

C:\windows\system32>
```

¿Entiendes todos los paquetes? Explica los paquetes capturados generados por la orden ping ejecutada.

ARP (Address Resolution Protocol):

ARP Request: Tu computadora pregunta "¿Quién tiene la IP asociada a www.google.es?".
ARP Reply: El dispositivo que tiene esa IP responde con su dirección MAC.
ICMP (Internet Control Message Protocol):

Echo Request: Tu computadora envía un paquete ICMP tipo Echo Request a la IP de www.google.es, básicamente diciendo "¿Estás ahí?".
Echo Reply: El servidor de Google responde con un paquete ICMP tipo Echo Reply, diciendo "Sí, aquí estoy".
DNS (Domain Name System):

DNS Query: Tu computadora pregunta a un servidor DNS "¿Cuál es la dirección IP de www.google.es?".
DNS Response: El servidor DNS responde con la dirección IP correspondiente a www.google.es.
Explicación de los paquetes generados por el comando ping:
Cuando ejecutas el comando ping www.google.es, ocurren los siguientes eventos que generan los paquetes capturados:

Resolución DNS:

Antes de enviar cualquier paquete ICMP, tu computadora necesita saber la dirección IP de www.google.es. Envía una consulta DNS y recibe una respuesta con la dirección IP correspondiente.

Resolución ARP:

Tu computadora necesita saber la dirección MAC de la puerta de enlace (router) para enviar los paquetes. Por eso, si no está en la caché ARP, envía una solicitud ARP y recibe una respuesta con la dirección MAC.
Ping (ICMP):

Una vez conocida la dirección IP de www.google.es, tu computadora envía paquetes ICMP tipo Echo Request a esa dirección IP.
El servidor de Google responde con paquetes ICMP tipo Echo Reply.
Ejemplo de un análisis de captura:
ARP Request y Reply:

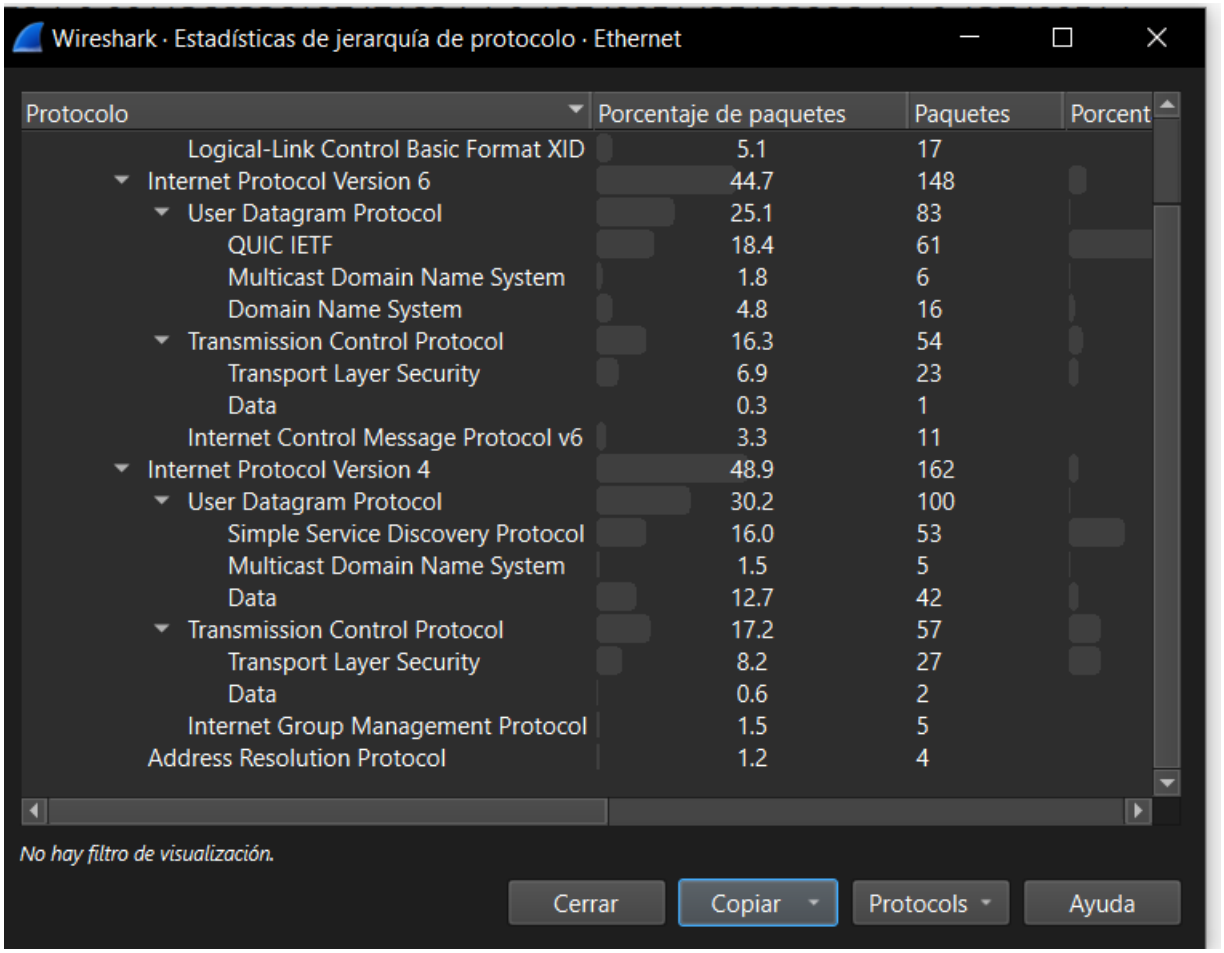
ARP Request: "¿Quién tiene la IP 192.168.1.1? Díselo a 192.168.1.2".
ARP Reply: "192.168.1.1 está en 00:11:22:33:44:55".
DNS Query y Response:

DNS Query: "¿Cuál es la IP de www.google.es?".
DNS Response: "La IP de www.google.es es 172.217.16.196".
ICMP Echo Request y Reply:

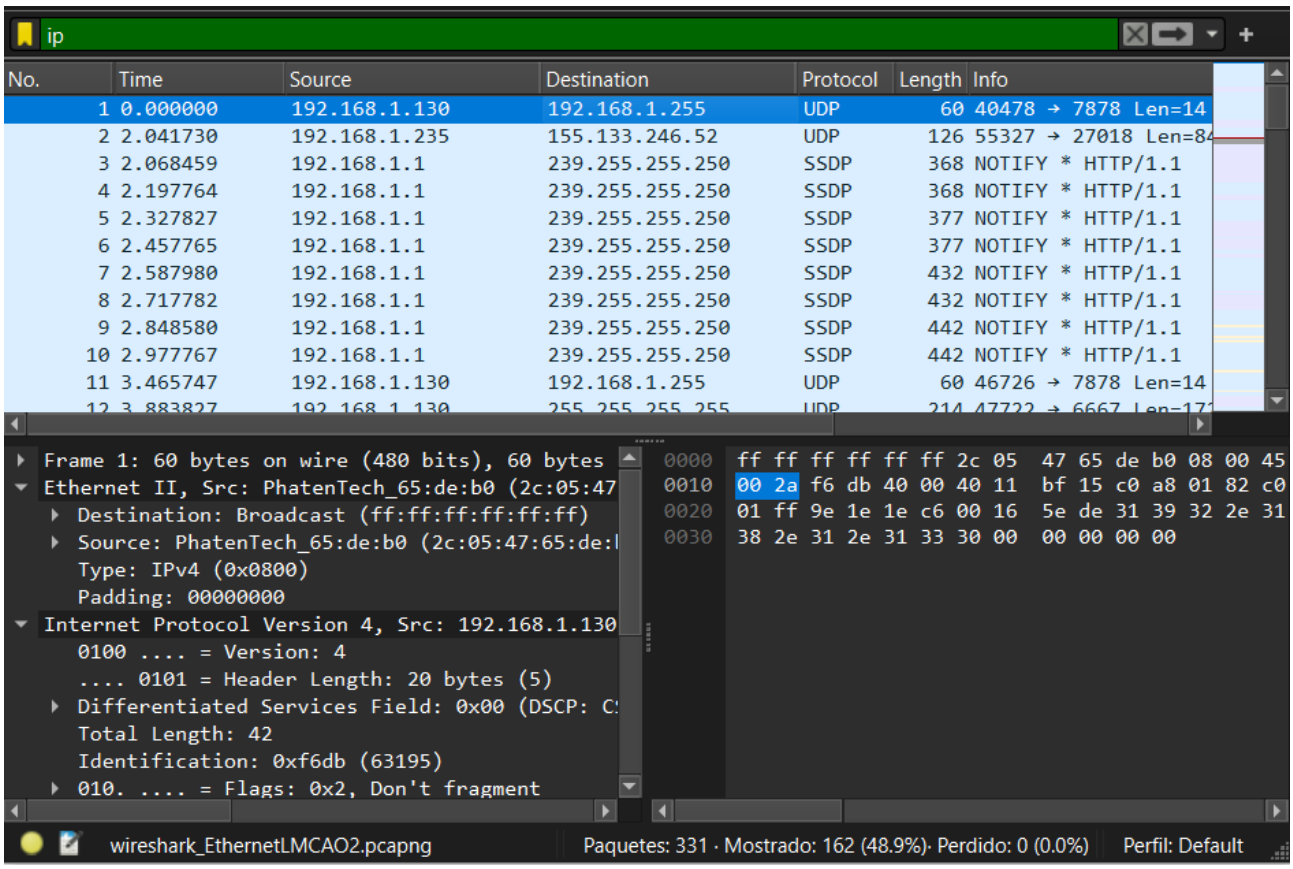
ICMP Echo Request: Un paquete ICMP desde tu IP hacia 172.217.16.196 con un mensaje tipo "ping".
ICMP Echo Reply: Un paquete ICMP desde 172.217.16.196 hacia tu IP con la respuesta "pong".

PARTE 2:

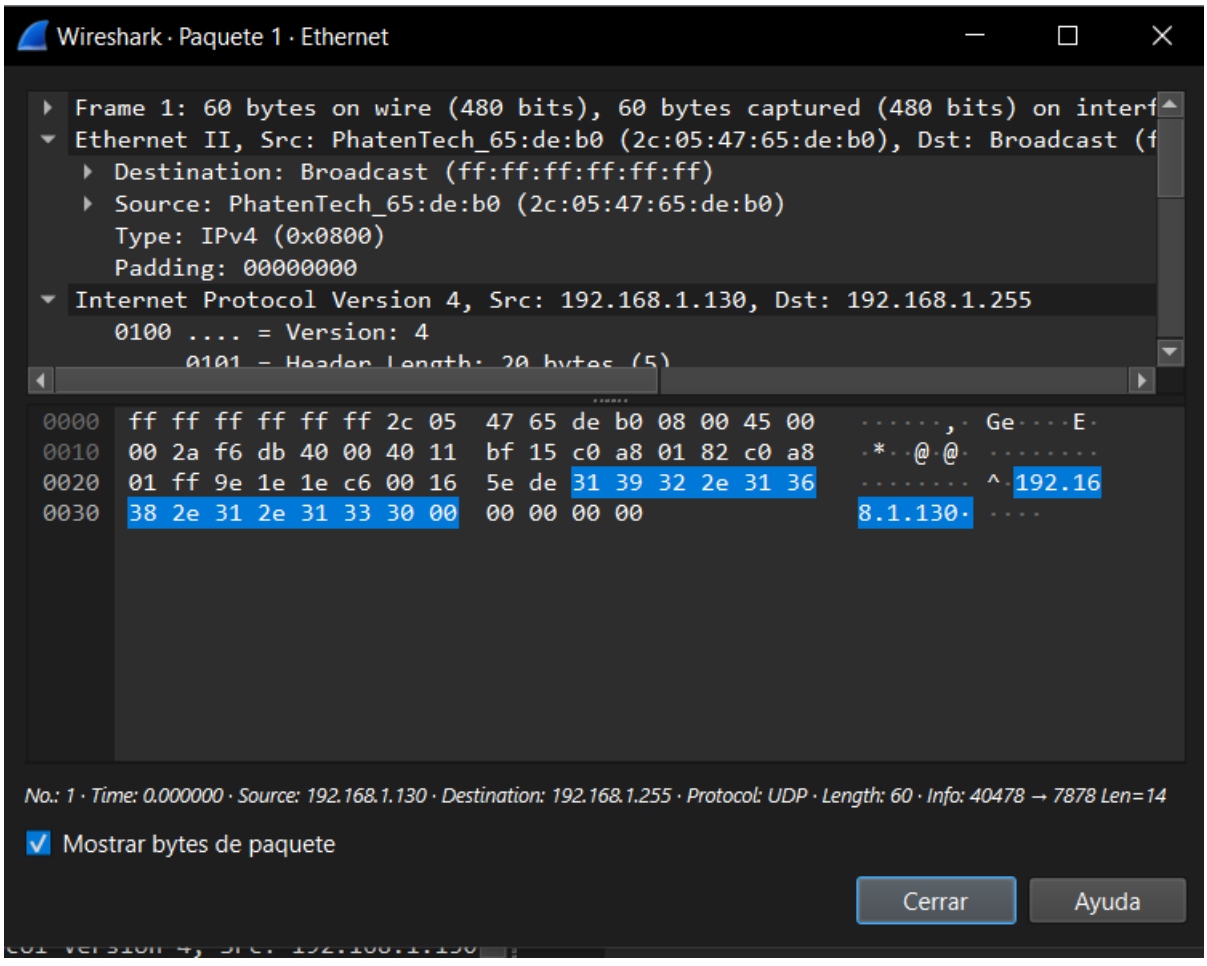
ARP: 4
IP: 148V6 162V4
ICMP: 11
TCP: 54
UDP: 83



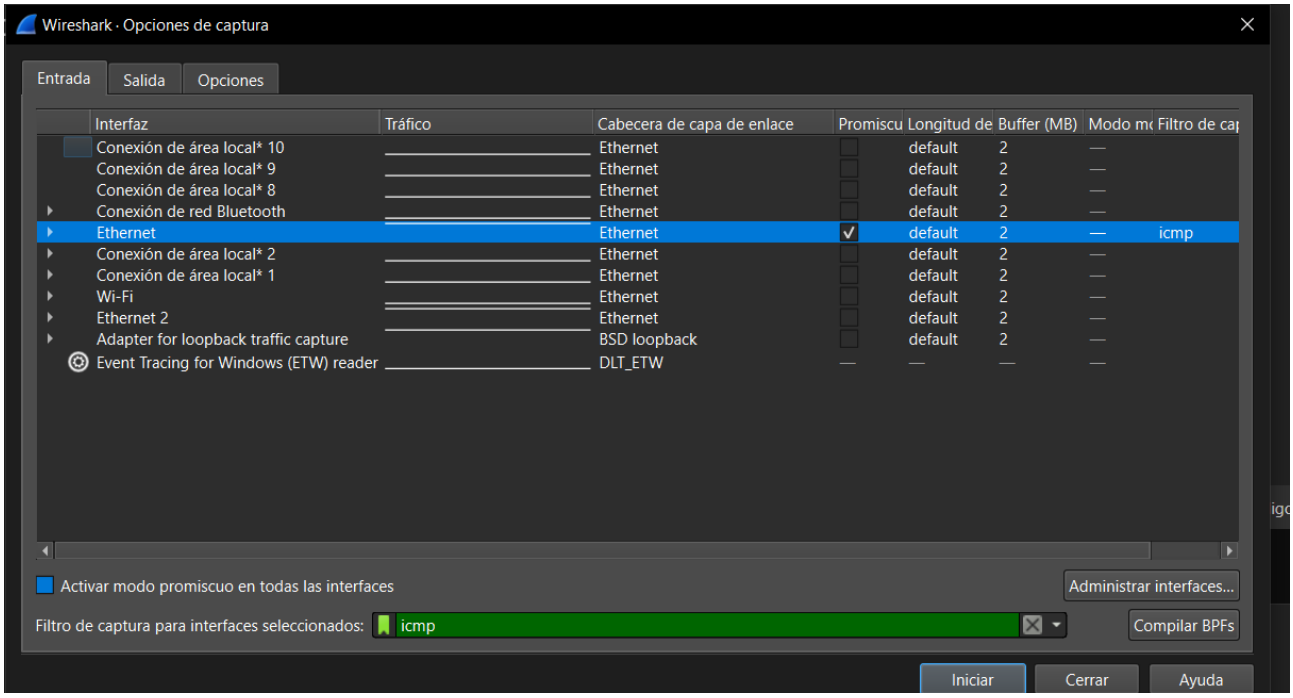
Dirección IP origen: 192.168.1.130
Dirección IP destino: 192.168.1.255
Protocolo: UDP
Tamaño: 42
TTL: 64
Identificador: Identification: 0xf6db (63195)



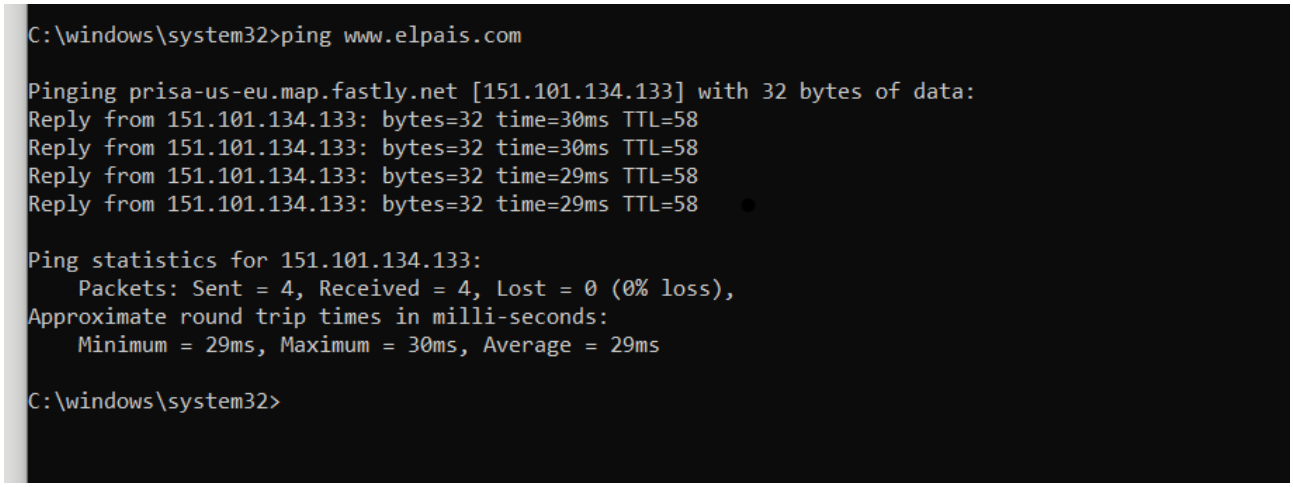
Aplique un filtro de IP.



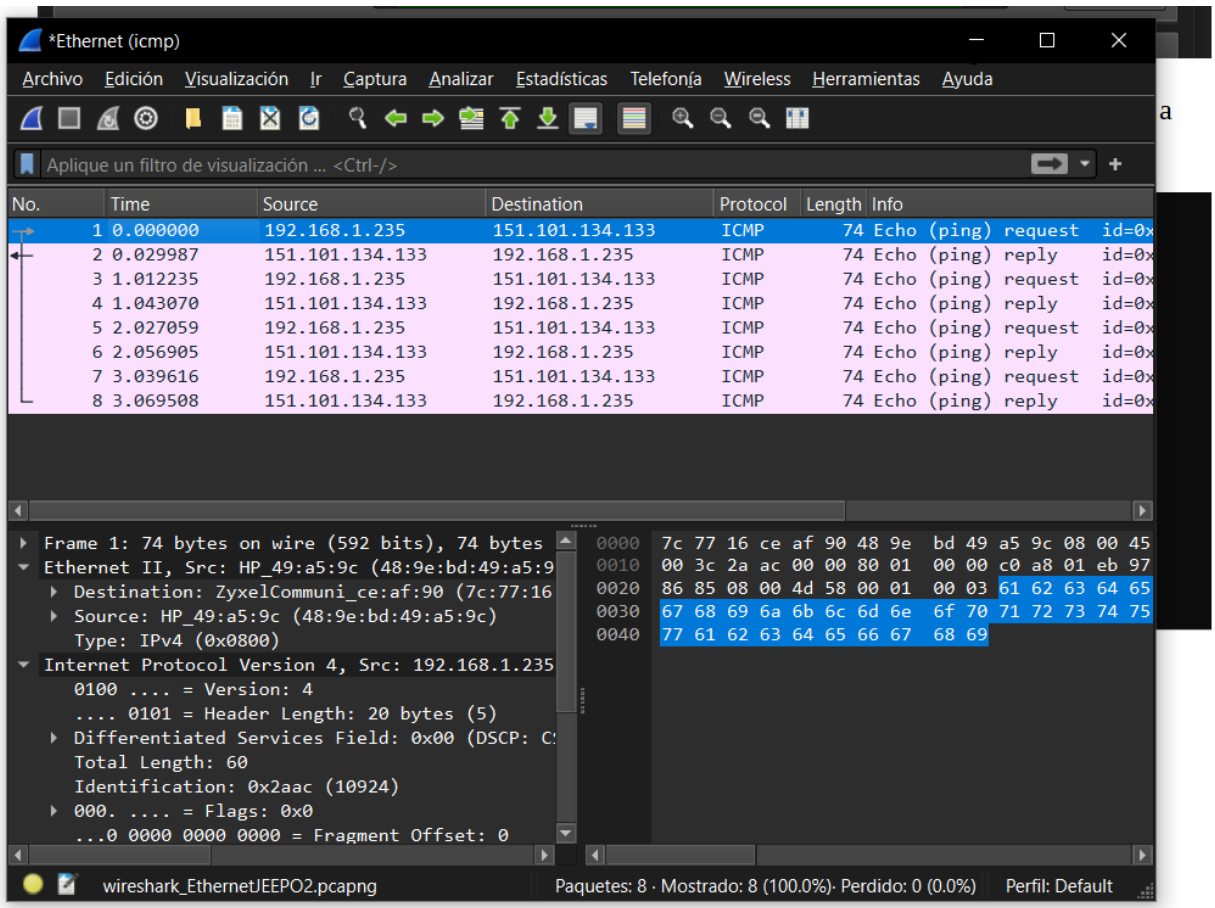
PARTE 3:



Desactivamos el modo promiscuo para que no coja todo el trafico de red y solo donde se vayan a realizar los paquetes es decir donde hay conexión y filtramos con icmp.



Ping a www.elpais.com.



Son 8 mensajes:

1-

Cabeceras ICMP

Tipo: 8

Codigo: 0

Bytes de Datos: 32 bytes

Cabeceras IP

Longitud de cabecera: 20 bytes (5)

Longitud total: 60

Bytes de datos = Longitud total del paquete - Longitud de cabecera IP
= 60 bytes - 20 bytes
= 40 bytes

2-

Cabeceras ICMP

Tipo: 0

Codigo: 0

Bytes de Datos: 32 bytes

Cabeceras IP

Longitud de cabecera: 20 bytes (5)

Longitud total: 60

Bytes de datos: 40

3-

Cabeceras ICMP

Tipo: 8

Codigo: 0

Bytes de Datos: 32 bytes

Cabeceras IP

Longitud de cabecera: 20 bytes (5)

Longitud total: 60

Bytes de datos: 40

4-

Cabeceras ICMP

Tipo: 0

Codigo: 0

Bytes de Datos: 32 bytes

Cabeceras IP

Longitud de cabecera: 20 bytes (5)

Longitud total: 60

Bytes de datos: 40

5-

Cabeceras ICMP

Tipo: 8

Codigo: 0

Bytes de Datos: 32 bytes

Cabeceras IP

Longitud de cabecera: 20 bytes (5)

Longitud total: 60

Bytes de datos: 40 bytes

6-

Cabeceras ICMP

Tipo: 0

Codigo: 0

Bytes de Datos: 32 bytes

Cabeceras IP

Longitud de cabecera: 20 bytes (5)

Longitud total: 60

Bytes de datos: 40 bytes

7-

Cabeceras ICMP

Tipo: 8

Codigo: 0

Bytes de Datos: 32 bytes

Cabeceras IP

Longitud de cabecera: 20 bytes (5)

Longitud total: 60

Bytes de datos: 40 bytes

8-

Cabeceras ICMP

Tipo: 0

Codigo: 0

Bytes de Datos: 32 bytes

Cabeceras IP

Longitud de cabecera: 20 bytes (5)

Longitud total: 60

Bytes de datos: 40 bytes