Tarea para ambos grupos, 1 y 2.

Con el fin de practicar con la herramienta Wireshark, vamos a ver cómo el tráfico de red circula por el interfaz de red de nuestro equipo. En particular, vamos a revisar el tráfico correspondiente al protocolo ICMP, utilizado por el comando ping para comprobar la conectividad con una IP. Los pasos a realizar son los siguientes:

1) Arrancar Wireshark y una vez iniciado, seleccionar el interfaz de red de nuestro equipo (puede ser Ethernet, si está conectado por cable, o Wi-Fi, si nuestra conexión es WiFi).

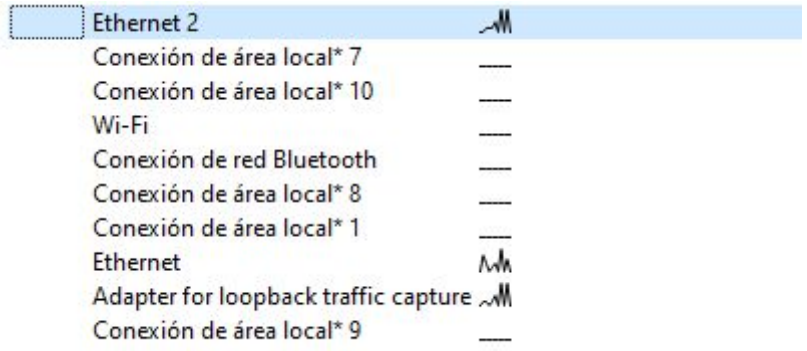
2) Una vez que comprobemos que el tráfico se está registrando, abrir un terminal Linux o una ventana de comandos Windows (cmd), y hacer un ping a www.google.com)

3) Ahora, volvemos a Wireshark y filtramos las entradas del protocolo "icmp".

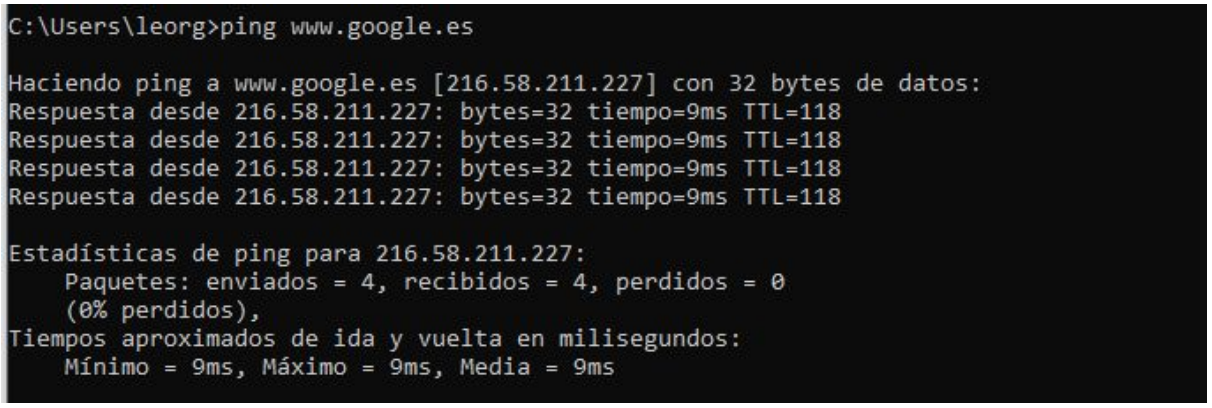
4) Hacemos clic en alguna de ellas y desplegamos, en la ventana del medio de Wireshark, la sección correspondiente a la capa de nivel físico (Ethernet II), con el fin de ver las direcciones MAC origen y destino. Luego, desplegamos la capa de nivel de red (Internet Protocol v4), para ver las direcciones IP origen y destino.

Toma algunos pantallazos e indica que paso del proceso corresponde a cada uno de ellos, adjuntando todo en un documento para anexar a esta tarea.

1.- En este caso tengo que usar la ethernet sin numero ya que voy por cable y la ethernet 2 no me deja buscar icmp



2.-



3.-

icmp

No.	Time	Source	Destination	Protocol	Length	Info
1681	1.422096	192.168.31.216	216.58.211.227	ICMP	74	Echo (ping) request
1682	1.431599	216.58.211.227	192.168.31.216	ICMP	74	Echo (ping) reply
1730	2.427038	192.168.31.216	216.58.211.227	ICMP	74	Echo (ping) request
1731	2.436307	216.58.211.227	192.168.31.216	ICMP	74	Echo (ping) reply
1745	3.433055	192.168.31.216	216.58.211.227	ICMP	74	Echo (ping) request
1746	3.442287	216.58.211.227	192.168.31.216	ICMP	74	Echo (ping) reply
1758	4.437763	192.168.31.216	216.58.211.227	ICMP	74	Echo (ping) request
1759	4.446807	216.58.211.227	192.168.31.216	ICMP	74	Echo (ping) reply

4

```
> Frame 1745: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{2F9D
> Ethernet II, Src: Pegatron_13:d9:c5 (54:b2:03:13:d9:c5), Dst: XIAOMIEl_1a:76:67 (50:64:2b:1a:76:67)
> Internet Protocol Version 4, Src: 192.168.31.216, Dst: 216.58.211.227
> Internet Control Message Protocol

v Ethernet II, Src: Pegatron_13:d9:c5 (54:b2:03:13:d9:c5), Dst: XIAOMIEl_1a:76:67 (50:64:2b:1a:76:67)
    > Destination: XIAOMIEl_1a:76:67 (50:64:2b:1a:76:67)
    > Source: Pegatron_13:d9:c5 (54:b2:03:13:d9:c5)
      Type: IPv4 (0x0800)

v Internet Protocol Version 4, Src: 192.168.31.216, Dst: 216.58.211.227
      0100 .... = Version: 4
      .... 0101 = Header Length: 20 bytes (5)
    > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      Total Length: 60
      Identification: 0xc6f5 (50933)
    > Flags: 0x0000
      Fragment offset: 0
      Time to live: 128
      Protocol: ICMP (1)
      Header checksum: 0x0000 [validation disabled]
      [Header checksum status: Unverified]
      Source: 192.168.31.216
```