USO DE WIRESHARK PARA VER EL TRÁFICO DE LA RED TOPOLOGÍA

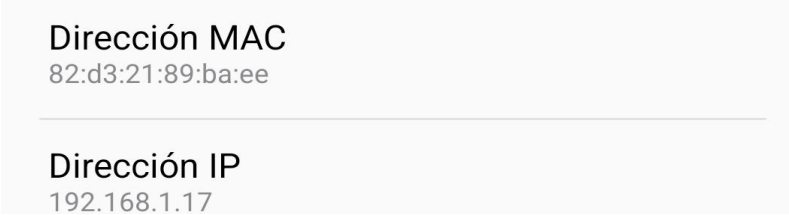
Paso 1: Recuperar las Direcciones de Interfaz

1. En la terminal, hay que poner el comando: **ipconfig /all**

2. Hay que sacar la dirección IP (dirección IPv4) y la dirección MAC (dirección física):

```
Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . : home
   Descripción . . . . . . . . . . . . . . . : MediaTek Wi-Fi 6 MT7921 Wireless LAN Card
   Dirección física. . . . . . . . . . . . . : C0-35-32-A0-5D-C1
   DHCP habilitado . . . . . . . . . . . . . : sí
   Configuración automática habilitada . . . : sí
   Vínculo: dirección IPv6 local . . . . . . : fe80::c056:9761:24cb:5521%10(Preferido)
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.1.19(Preferido)
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Concesión obtenida. . . . . . . . . . . . : jueves, 3 de abril de 2025 23:01:16
   La concesión expira . . . . . . . . . . . : sábado, 5 de abril de 2025 9:49:56
   Puerta de enlace predeterminada . . . . . : 192.168.1.1
   Servidor DHCP . . . . . . . . . . . . . . : 192.168.1.1
   IAID DHCPv6 . . . . . . . . . . . . . . . : 96482610
   DUID de cliente DHCPv6. . . . . . . . . . : 00-01-00-01-2D-D7-4C-41-40-C2-BA-F8-10-F4
   Servidores DNS. . . . . . . . . . . . . . : 192.168.1.1
   NetBIOS sobre TCP/IP. . . . . . . . . . . : habilitado
```

3. También hay que sacar la dirección IP y la dirección MAC en el otro dispositivo.



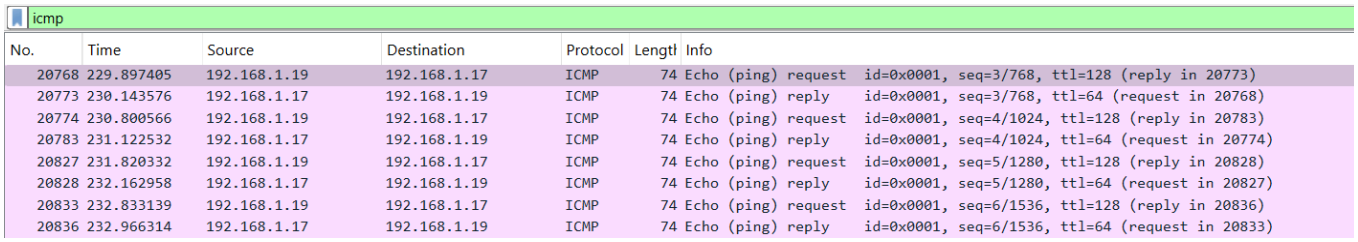
Paso 2: Inicia Wireshark y comienza a capturar

1. Una vez instalado Wireshark en el enlace: https://www.wireshark.org/download.html, hay que seleccionar la interfaz de red correcta

2. Inicia Wireshark para seleccionar la interfaz de red activa (Wi-Fi o Ethernet).

3. Iniciar Captura: hacer clic en la interfaz de red.

4. Filtrar solo los paquetes ICMP escribiendo **icmp** en la barra de filtros y presionar Enter.

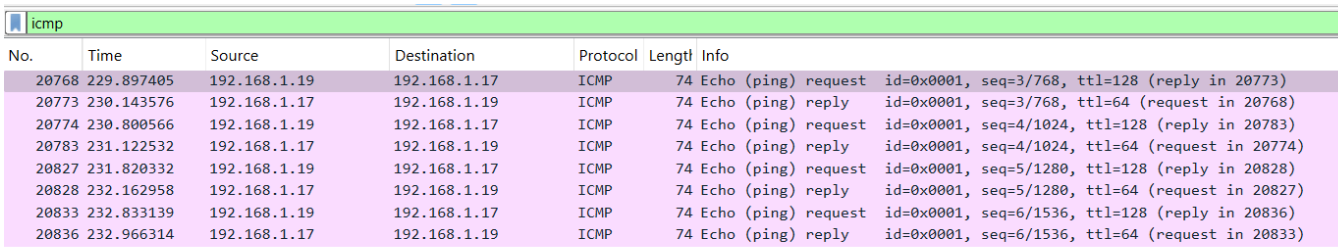


icmp

No.	Time	Source	Destination	Protocol	Lengtl	Info
20768	229.897405	192.168.1.19	192.168.1.17	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 20773)
20773	230.143576	192.168.1.17	192.168.1.19	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 20768)
20774	230.800566	192.168.1.19	192.168.1.17	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 20783)
20783	231.122532	192.168.1.17	192.168.1.19	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 20774)
20827	231.820332	192.168.1.19	192.168.1.17	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 20828)
20828	232.162958	192.168.1.17	192.168.1.19	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=64 (request in 20827)
20833	232.833139	192.168.1.19	192.168.1.17	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 20836)
20836	232.966314	192.168.1.17	192.168.1.19	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=64 (request in 20833)

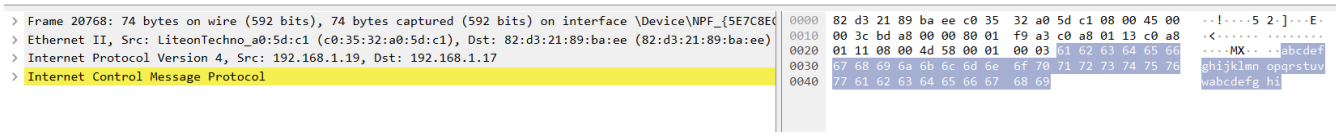
5. En la terminal, escribir: **ping [IP del otro dispositivo]** para hacer ping al otro dispositivo.

```
PS C:\Users\sofia> ping 192.168.1.17

Haciendo ping a 192.168.1.17 con 32 bytes de datos:
Respuesta desde 192.168.1.17: bytes=32 tiempo=364ms TTL=64
Respuesta desde 192.168.1.17: bytes=32 tiempo=322ms TTL=64
Respuesta desde 192.168.1.17: bytes=32 tiempo=342ms TTL=64
Respuesta desde 192.168.1.17: bytes=32 tiempo=133ms TTL=64

Estadísticas de ping para 192.168.1.17:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 133ms, Máximo = 364ms, Media = 290ms
PS C:\Users\sofia>
```



icmp

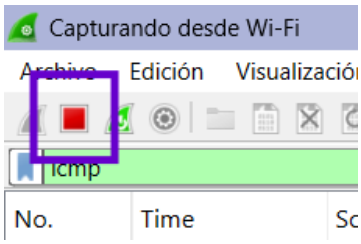
No.	Time	Source	Destination	Protocol	Lengtl	Info
20768	229.897405	192.168.1.19	192.168.1.17	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 20773)
20773	230.143576	192.168.1.17	192.168.1.19	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 20768)
20774	230.800566	192.168.1.19	192.168.1.17	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 20783)
20783	231.122532	192.168.1.17	192.168.1.19	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 20774)
20827	231.820332	192.168.1.19	192.168.1.17	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 20828)
20828	232.162958	192.168.1.17	192.168.1.19	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=64 (request in 20827)
20833	232.833139	192.168.1.19	192.168.1.17	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 20836)
20836	232.966314	192.168.1.17	192.168.1.19	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=64 (request in 20833)



```
> Frame 20768: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{5E7C8E(
> Ethernet II, Src: LiteonTechno_a0:5d:c1 (c0:35:32:a0:5d:c1), Dst: 82:d3:21:89:ba:ee (82:d3:21:89:ba:ee)
> Internet Protocol Version 4, Src: 192.168.1.19, Dst: 192.168.1.17
> Internet Control Message Protocol
```

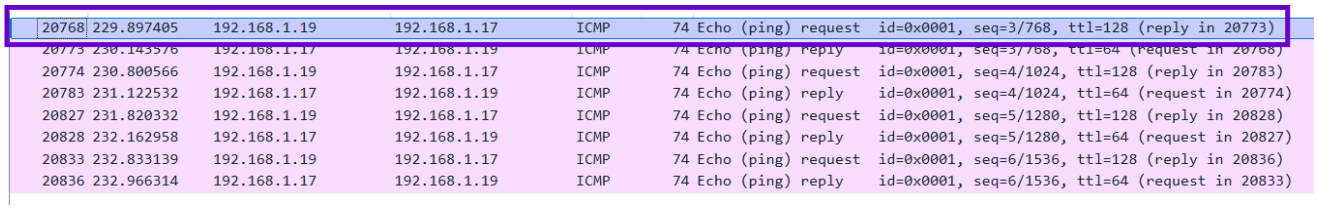
```
0000  82 d3 21 89 ba ee c0 35  32 a0 5d c1 08 00 45 00   ··!····5 2·]···E·
0010  00 3c bd a8 00 00 80 01  f9 a3 c0 a8 01 13 c0 a8   ·<·····  ········
0020  01 11 08 00 4d 58 00 01  00 03 61 62 63 64 65 66   ····MX·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                    wabcdefg hi
```

6. Detener la captura:



Paso 3: Análisis de los datos capturados

1. Hay que asegurarse de estar en un paquete "Echo (ping) request":

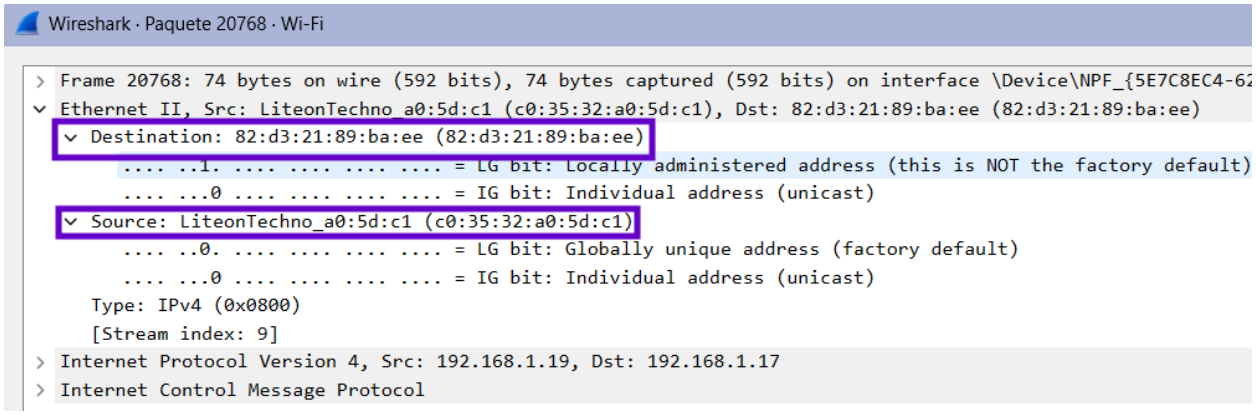


20768	229.897405	192.168.1.19	192.168.1.17	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 20773)
20773	230.143576	192.168.1.17	192.168.1.19	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 20768)
20774	230.800566	192.168.1.19	192.168.1.17	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 20783)
20783	231.122532	192.168.1.17	192.168.1.19	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 20774)
20827	231.820332	192.168.1.19	192.168.1.17	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 20828)
20828	232.162958	192.168.1.17	192.168.1.19	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=64 (request in 20827)
20833	232.833139	192.168.1.19	192.168.1.17	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 20836)
20836	232.966314	192.168.1.17	192.168.1.19	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=64 (request in 20833)

2. Abrir "Ethernet II"..

3. MAC de origen: Está después de Src: (Source). Es la dirección MAC del ordenador

4. MAC de destino: Está después de Dst: (Destination). Es la MAC del otro dispositivo:



5. Respondiendo a las preguntas:

5.1. ¿La MAC de origen es la de tu PC? Sí

5.2. ¿La MAC de destino es la del otro dispositivo? Sí

5.3. ¿Cómo obtiene tu PC la MAC del otro dispositivo?

Para que el ordenador obtenga la dirección MAC de otro dispositivo en la red, utiliza ARP (Address Resolution Protocol). Antes de enviar un ping, el ordenador necesita conocer la dirección MAC del dispositivo con la IP 192.168.1.17. Para hacerlo, envía un mensaje ARP preguntando “¿Quién tiene la IP 192.168.1.17?”. El dispositivo que tiene esa IP responde con su dirección MAC. Luego, el ordenador guarda esta dirección en su tabla ARP y la usa para enviar los paquetes ICMP correspondientes.

Paso 4: Capturar datos ICMP a sitios web

1. Volver a iniciar la captura.

2. En la terminal, escribir:

2.1. **ping www.cisco.com**

```
PS C:\Users\sofia> ping www.cisco.com

Haciendo ping a e2867.dsca.akamaiedge.net [2.17.153.67] con 32 bytes de dato
s:
Respuesta desde 2.17.153.67: bytes=32 tiempo=8ms TTL=56
Respuesta desde 2.17.153.67: bytes=32 tiempo=33ms TTL=56
Respuesta desde 2.17.153.67: bytes=32 tiempo=32ms TTL=56
Respuesta desde 2.17.153.67: bytes=32 tiempo=7ms TTL=56

Estadísticas de ping para 2.17.153.67:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 7ms, Máximo = 33ms, Media = 20ms
PS C:\Users\sofia>
```

Dirección IP: 2.17.153.67

2.2. **ping www.wikipedia.org**

```
PS C:\Users\sofia> ping www.wikipedia.org

Haciendo ping a dyna.wikimedia.org [185.15.58.224] con 32 bytes de datos:
Respuesta desde 185.15.58.224: bytes=32 tiempo=31ms TTL=55
Respuesta desde 185.15.58.224: bytes=32 tiempo=50ms TTL=55
Respuesta desde 185.15.58.224: bytes=32 tiempo=30ms TTL=55
Respuesta desde 185.15.58.224: bytes=32 tiempo=47ms TTL=55

Estadísticas de ping para 185.15.58.224:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 30ms, Máximo = 50ms, Media = 39ms
PS C:\Users\sofia>
```

Dirección IP: 185.15.58.224

2.3. **ping www.educa2.madrid.org**

```
PS C:\Users\sofia> ping www.educa2.madrid.org

Haciendo ping a www.educa2.madrid.org [193.146.123.83] con 32 bytes de datos
:
Respuesta desde 193.146.123.83: bytes=32 tiempo=9ms TTL=55
Respuesta desde 193.146.123.83: bytes=32 tiempo=8ms TTL=55
Respuesta desde 193.146.123.83: bytes=32 tiempo=9ms TTL=55
Respuesta desde 193.146.123.83: bytes=32 tiempo=10ms TTL=55

Estadísticas de ping para 193.146.123.83:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 8ms, Máximo = 10ms, Media = 9ms
PS C:\Users\sofia>
```

Dirección IP: 193.146.123.83

Paso 5: Análisis de los datos de los hosts remotos

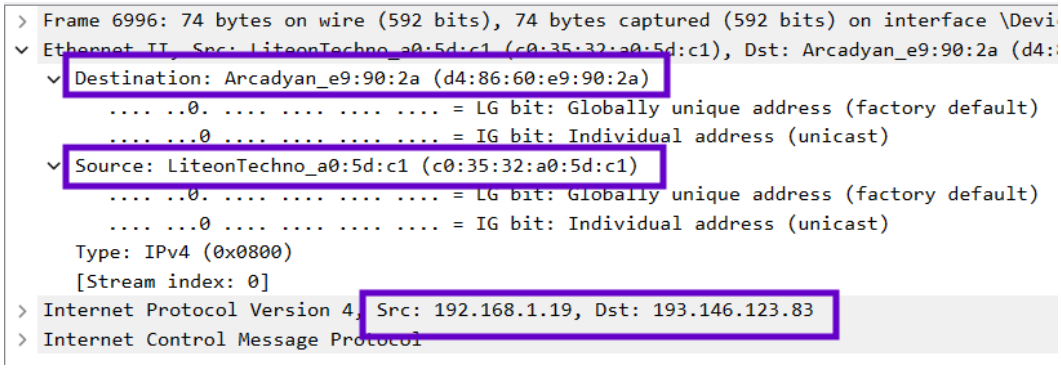
1. Echo (ping) request de IP: 2.17.153.67

```
> Frame 115: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\
v Ethernet II, Src: LiteonTechno_a0:5d:c1 (c0:35:32:a0:5d:c1), Dst: Arcadyan_e9:90:2a (d4:86
  v Destination: Arcadyan_e9:90:2a (d4:86:60:e9:90:2a)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: LiteonTechno_a0:5d:c1 (c0:35:32:a0:5d:c1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 192.168.1.19, Dst: 2.17.153.67
> Internet Control Message Protocol
```

2. Echo (ping) request de IP: 185.15.58.224

```
> Frame 5030: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Dev
v Ethernet II, Src: LiteonTechno_a0:5d:c1 (c0:35:32:a0:5d:c1), Dst: Arcadyan_e9:90:2a (d4
  v Destination: Arcadyan_e9:90:2a (d4:86:60:e9:90:2a)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  v Source: LiteonTechno_a0:5d:c1 (c0:35:32:a0:5d:c1)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
    [Stream index: 0]
> Internet Protocol Version 4, Src: 192.168.1.19, Dst: 185.15.58.224
> Internet Control Message Protocol
```

3. Echo (ping) request de IP: 193.146.123.83



¿Qué es lo curioso de estos datos?

Lo curioso en estos datos es que, aunque los paquetes se envían a diferentes direcciones IP en Internet, la dirección MAC de destino siempre es la del router de mi red local. Esto es porque las direcciones MAC solo son relevantes dentro de una misma red, y cuando el paquete sale hacia Internet, cada router por el que pasa cambia la dirección MAC de origen y destino según su propia red.

¿Por qué Wireshark muestra la MAC de los dispositivos locales pero no la de los remotos?

Wireshark solo captura los paquetes que pasan por tu interfaz de red. En una red local (LAN), las direcciones MAC se utilizan para la comunicación entre dispositivos dentro de la misma red. Sin embargo, cuando los paquetes viajan a través de Internet, solo se ve la dirección MAC del router de la red local, ya que los routers no transmiten direcciones MAC más allá de su propia red.

¿Qué diferencia hay entre el ping a la LAN y a Internet?

1. **Latencia**: Los pings dentro de la LAN tienen un tiempo de respuesta mucho menor que los pings a servidores en Internet.

2. **Direcciones MAC**: En la LAN se pueden ver direcciones MAC de origen y destino reales, pero en Internet solo se ve la MAC del router.

3. **TTL (Time to Live)**: El TTL de los pings a la LAN suele ser más alto (menos saltos), mientras que los pings a Internet muestran un TTL más bajo, ya que atraviesan varios routers.