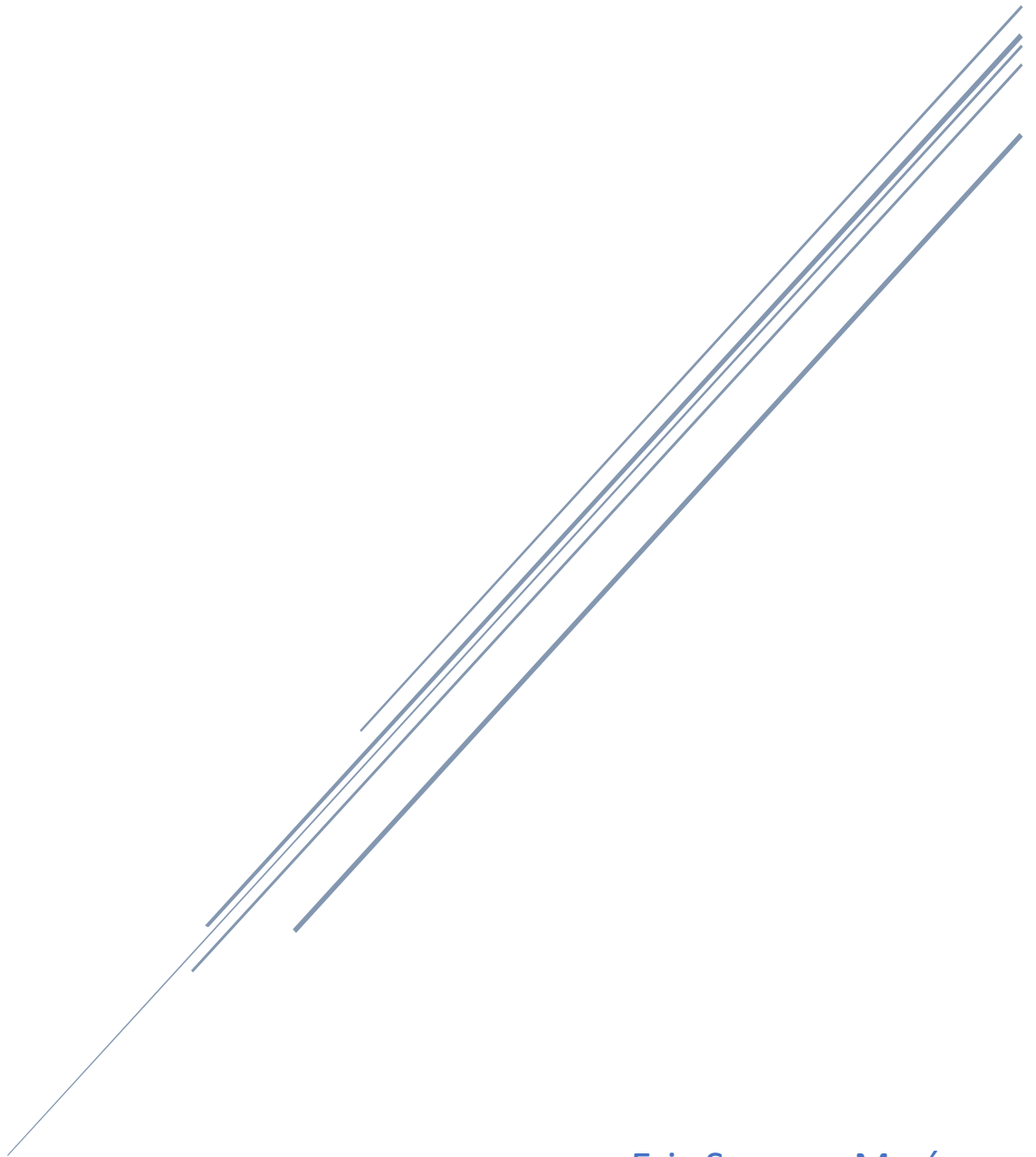


# PRÁCTICA 01: PROTOCOLO ARP

Redes Telemáticas



Eric Serrano Marín

27/09/2022

## CONTENIDO

Parte 1: Descargar e instalar Wireshark. ....	2
Paso 1: Descargar Wireshark .....	2
Paso 2: Instalación de Wireshark. ....	3
Paso 3: Desactivar Firewall.....	4
Parte 2: Capturar y analizar los datos ARP locales en Wireshark. ....	5
Paso 1: Recupere las direcciones de interfaz de la PC. ....	5
Paso 1.1: Ping a los diferentes grupos hechos en clase: .....	6
Paso 2: Inicie Wireshark y comience a capturar datos. ....	7
Paso 3: Examine los datos capturados. ....	7
Paso 4: Localice la trama de respuesta ARP que corresponde a la solicitud ARP que seleccionó. ....	9
Parte 3: Examine las entradas de la caché ARP en la PC. ....	10
Paso 1: Vea las entradas de la caché ARP en una PC con Windows. ....	10
Reflexión.....	10
1. ¿Cuál es el beneficio de mantener las entradas de la caché ARP en memoria de la computadora de origen? .....	10
2. Si la dirección IPv4 de destino no se encuentra en la misma red que el host de origen, ¿qué dirección MAC se usará como dirección MAC de destino de la trama? .....	10

## Objetivos

**Parte 1:** Descargar e instalar Wireshark

**Parte 2:** Capturar y analizar datos de ARP en Wireshark

- Iniciar y detener la captura de datos del tráfico de ping a los hosts remotos.
- Localizar la información de las direcciones IPv4 y MAC en las PDU capturadas.
- Analizar el contenido de los mensajes ARP intercambiados entre los dispositivos en la LAN.

**Parte 3:** Ver las entradas de caché ARP en la PC

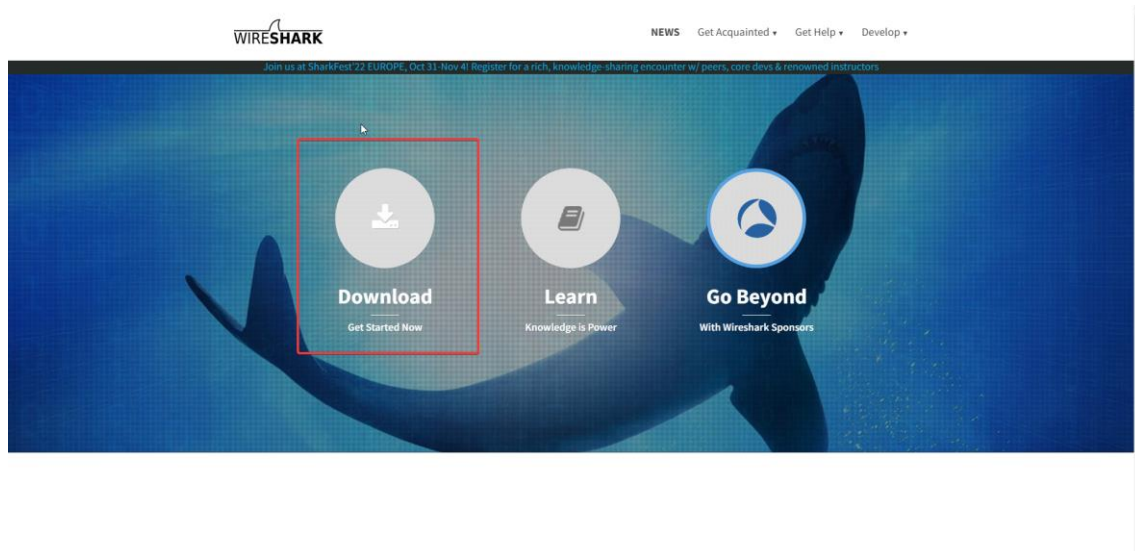
- Ingresar a la línea de comandos de Windows.
- Usar el comando arp de Windows para ver la caché de la tabla ARP local en la PC.

### PARTE 1: DESCARGAR E INSTALAR WIRESHARK.

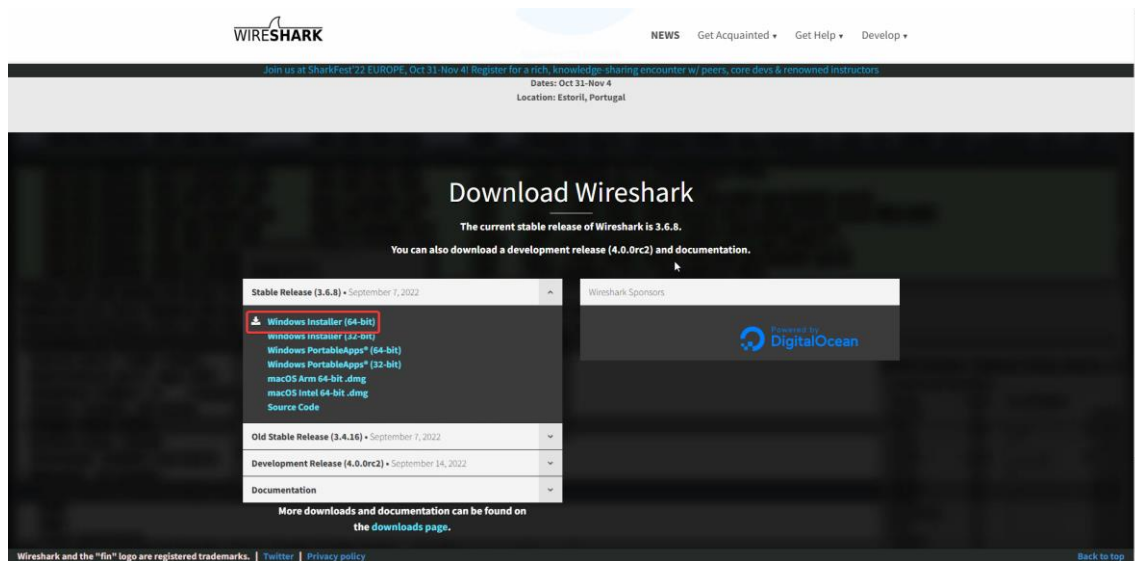
#### PASO 1: DESCARGAR WIRESHARK

Nos lo descargaremos en el siguiente enlace: [www.wireshark.org](http://www.wireshark.org).

Y haremos clic en Download.

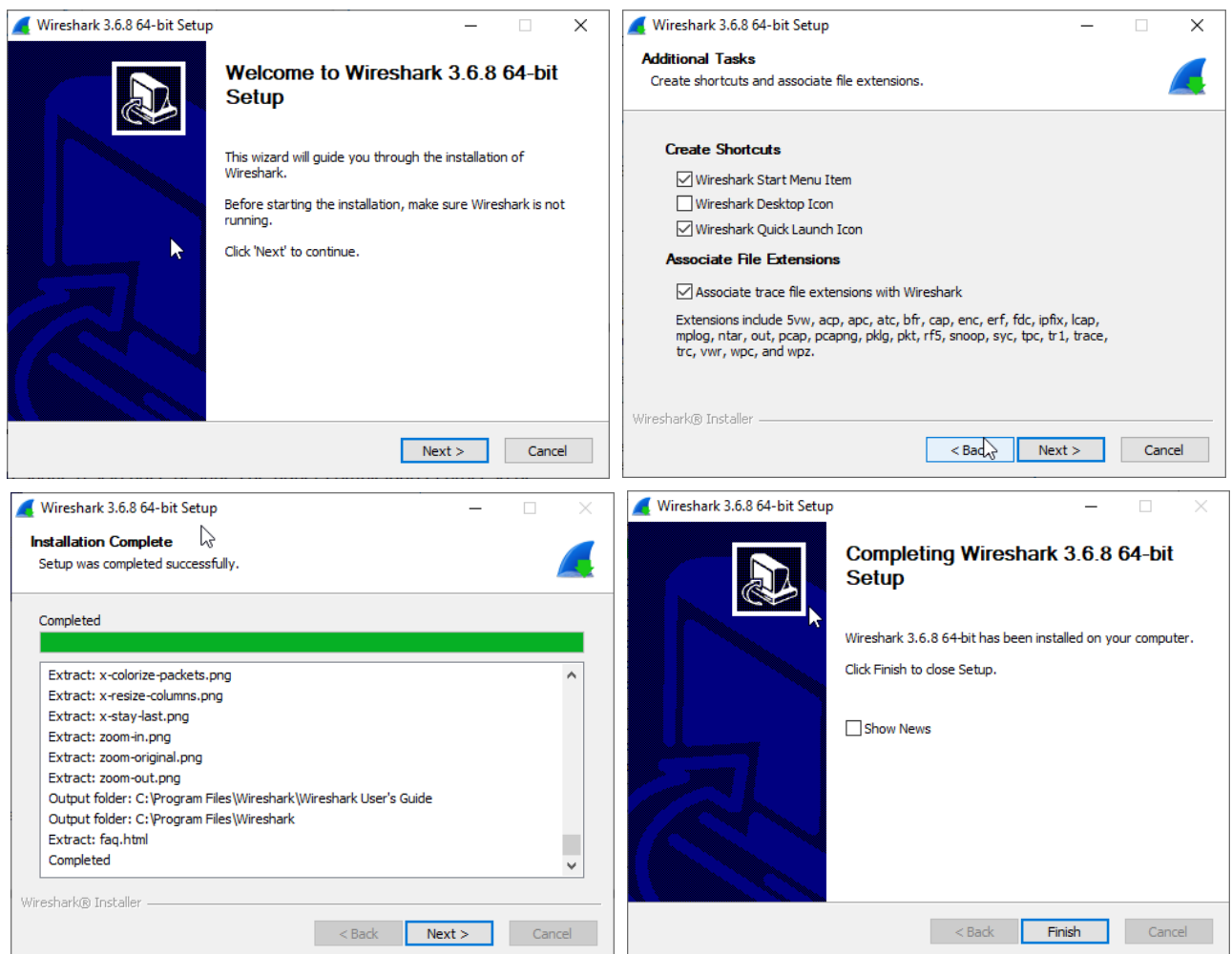


El siguiente paso será elegir sistema operativo y si tu sistema operativo es de 32 o 64bits.



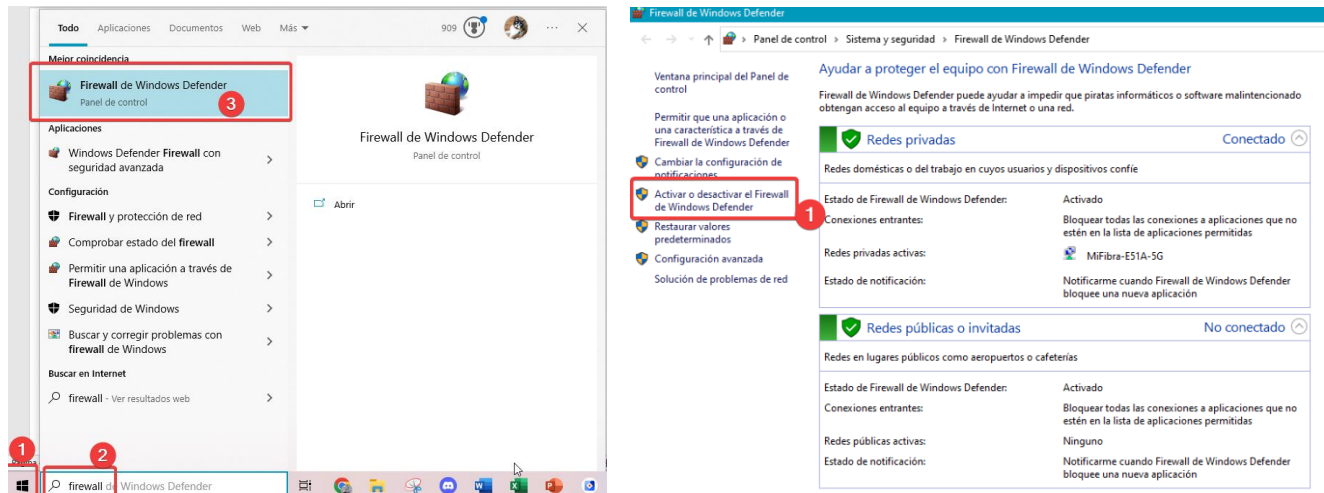
## PASO 2: INSTALACIÓN DE WIRESHARK.

Básicamente pulsaremos en las siguientes 3 capturas a next, teniendo que dar en la última a finish.



## PASO 3: DESACTIVAR FIREWALL.

Tecla inicio -> Escribimos firewall -> clic en Firewall de Windows Defender.



**PARTE 2: CAPTURAR Y ANALIZAR LOS DATOS ARP LOCALES EN WIRESHARK.****PASO 1: RECUPERE LAS DIRECCIONES DE INTERFAZ DE LA PC.**

IP y MAC del ordenador de mi grupo (grupo 1(PC Fran))

```
Símbolo del sistema
Configuración IP de Windows

Adaptador de LAN inalámbrica Conexión de área local* 1:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . : Home
    Vínculo: dirección IPv6 local. . . : fe80::19f1:21ab:6985:8122%5
    Dirección IPv4. . . . . : 172.26.0.71
    Máscara de subred. . . . . : 255.255.0.0
    Puerta de enlace predeterminada. . . . : 172.26.0.1

Adaptador de LAN inalámbrica Wi-Fi:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :

C:\Users\Raúl Campos>
```

```
Símbolo del sistema

Adaptador de Ethernet Ethernet:

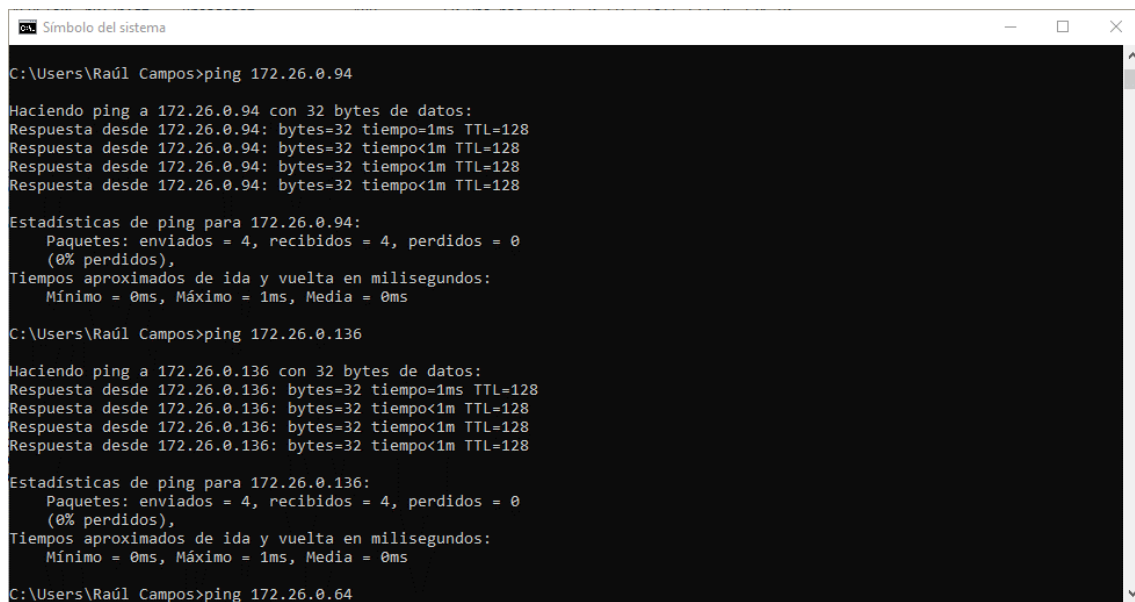
    Sufijo DNS específico para la conexión. . : Home
    Descripción. . . . . : Realtek PCIe GBE Family Controller
    Dirección física. . . . . : D8-9E-F3-7F-F4-80
    DHCP habilitado. . . . . : sí
    Configuración automática habilitada. . . : sí
    Vínculo: dirección IPv6 local. . . : fe80::19f1:21ab:6985:8122%5(Preferido)
    Dirección IPv4. . . . . : 172.26.0.71(Preferido)
    Máscara de subred. . . . . : 255.255.0.0
    Concesión obtenida. . . . . : lunes, 26 de septiembre de 2022 8:14:55
    La concesión expira. . . . . : martes, 27 de septiembre de 2022 8:14:55
    Puerta de enlace predeterminada. . . . : 172.26.0.1
    Servidor DHCP. . . . . : 172.26.0.1
    IAID DHCPv6. . . . . : 215523059
    DUID de cliente DHCPv6. . . . . : 00-01-00-01-29-89-63-A9-D8-9E-F3-7F-F4-80
    Servidores DNS. . . . . : 172.26.0.1
    NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de LAN inalámbrica Wi-Fi:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :
    Descripción. . . . . : Intel(R) Dual Band Wireless-AC 3165
    Dirección física. . . . . : D4-6D-6D-B9-F5-41
    DHCP habilitado. . . . . : sí
    Configuración automática habilitada. . . : sí

C:\Users\Raúl Campos>
```

## PASO 1.1: PING A LOS DIFERENTES GRUPOS HECHOS EN CLASE:



```
C:\Users\Raúl Campos>ping 172.26.0.94

Haciendo ping a 172.26.0.94 con 32 bytes de datos:
Respuesta desde 172.26.0.94: bytes=32 tiempo=1ms TTL=128
Respuesta desde 172.26.0.94: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.26.0.94: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.26.0.94: bytes=32 tiempo<1m TTL=128

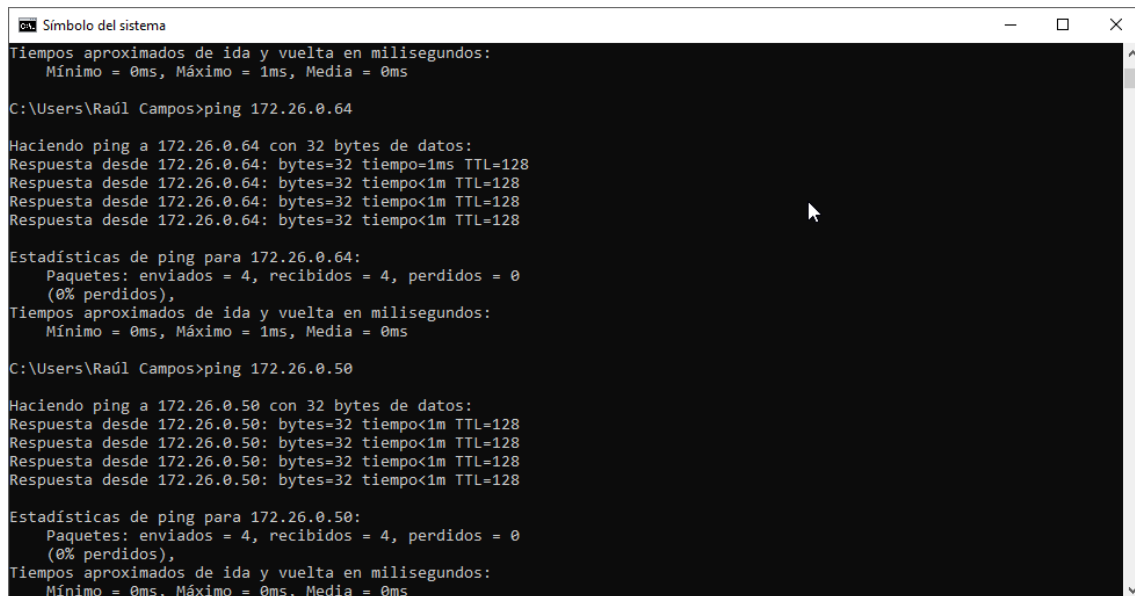
Estadísticas de ping para 172.26.0.94:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\Raúl Campos>ping 172.26.0.136

Haciendo ping a 172.26.0.136 con 32 bytes de datos:
Respuesta desde 172.26.0.136: bytes=32 tiempo=1ms TTL=128
Respuesta desde 172.26.0.136: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.26.0.136: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.26.0.136: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 172.26.0.136:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\Raúl Campos>ping 172.26.0.64
```



```
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\Raúl Campos>ping 172.26.0.64

Haciendo ping a 172.26.0.64 con 32 bytes de datos:
Respuesta desde 172.26.0.64: bytes=32 tiempo=1ms TTL=128
Respuesta desde 172.26.0.64: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.26.0.64: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.26.0.64: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 172.26.0.64:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

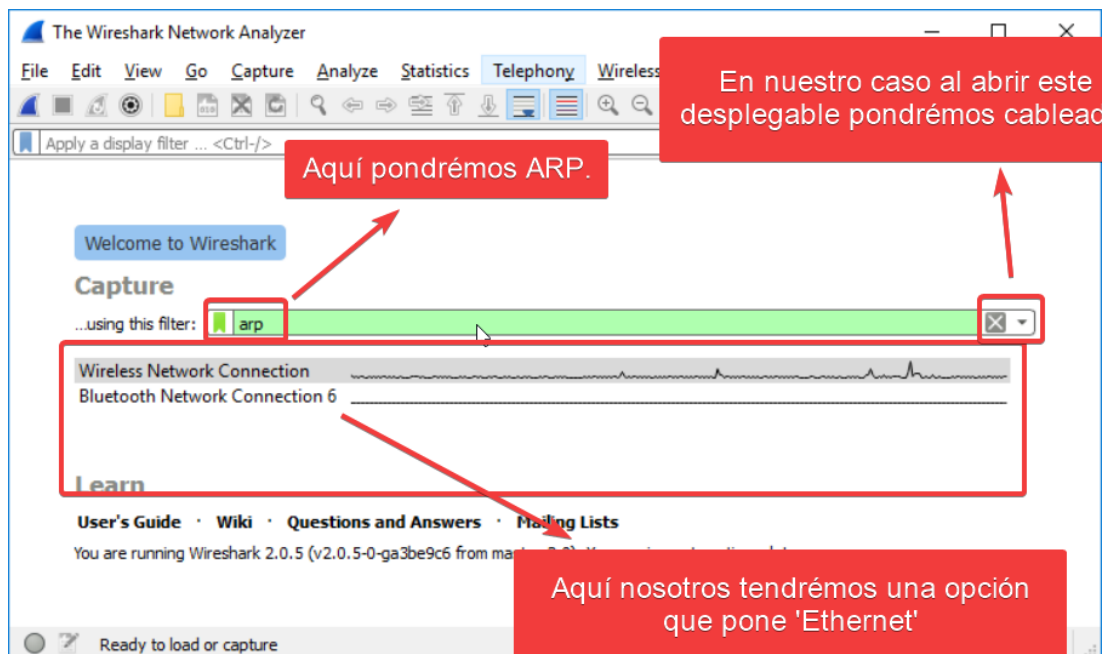
C:\Users\Raúl Campos>ping 172.26.0.50

Haciendo ping a 172.26.0.50 con 32 bytes de datos:
Respuesta desde 172.26.0.50: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.26.0.50: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.26.0.50: bytes=32 tiempo<1m TTL=128
Respuesta desde 172.26.0.50: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 172.26.0.50:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```



## PASO 2: INICIE WIRESHARK Y COMIENZE A CAPTURAR DATOS.



Cuando pulsemos enter nos empezarán a salir preguntas y respuestas de nuestra red. Nosotros vamos a distinguir la de los distintos grupos que hemos hecho en clase.

## PASO 3: EXAMINE LOS DATOS CAPTURADOS.

No.	Time	Source	Destination	Protocol	Length	Info
19	15.739146	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.53? Tell 172.26.124.10
20	15.739146	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.63? Tell 172.26.124.10
21	16.548170	Contrend_48:62:ea	Dell_7f:f4:80	ARP	60	Who has 172.26.0.71? Tell 172.26.0.1
22	16.548191	Dell_7f:f4:80	Contrend_48:62:ea	ARP	42	172.26.0.71 is at d8:9e:f3:7f:f4:80
23	16.740702	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.53? Tell 172.26.124.10
24	16.740702	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.63? Tell 172.26.124.10
25	16.820849	Contrend_48:62:ea	Dell_7f:f4:80	ARP	60	Who has 172.26.0.71? Tell 172.26.0.1
26	16.820864	Dell_7f:f4:80	Contrend_48:62:ea	ARP	42	172.26.0.71 is at d8:9e:f3:7f:f4:80
27	17.735222	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.49? Tell 172.26.124.10
28	17.735222	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.49? Tell 172.26.124.10

Pregunta y respuesta de nuestra IP (Grupo 1)

No.	Time	Source	Destination	Protocol	Length	Info
43	99.224690	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.49? Tell 172.26.124.10
44	99.282144	HP_cc:a3:de	Broadcast	ARP	60	Who has 172.26.0.71? Tell 172.26.0.94
45	99.282155	Dell_7f:f4:80	HP_cc:a3:de	ARP	42	172.26.0.71 is at d8:9e:f3:7f:f4:80
46	99.737690	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.49? Tell 172.26.124.10
47	100.728893	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.49? Tell 172.26.124.10
48	104.283089	Dell_7f:f4:80	HP_cc:a3:de	ARP	42	Who has 172.26.0.94? Tell 172.26.0.71
49	104.284471	HP_cc:a3:de	Dell_7f:f4:80	ARP	60	172.26.0.94 is at d8:9e:f3:cc:a3:de
50	109.022332	Giga-Byt_2e:57:64	Giga-Byt_2e:53:c2	ARP	60	Who has 172.26.0.49? Tell 172.26.0.127
51	110.030345	Giga-Byt_2e:57:64	Giga-Byt_2e:53:c2	ARP	60	Who has 172.26.0.49? Tell 172.26.0.127
52	111.032231	Giga-Byt_2e:57:64	Giga-Byt_2e:53:c2	ARP	60	Who has 172.26.0.49? Tell 172.26.0.127
53	112.883814	Dell_80:e3:79	Broadcast	ARP	60	Who has 172.26.0.71? Tell 172.26.0.136
54	112.883837	Dell_7f:f4:80	Dell_80:e3:79	ARP	42	172.26.0.71 is at d8:9e:f3:7f:f4:80
55	117.706693	Dell_7f:f4:80	Dell_80:e3:79	ARP	42	Who has 172.26.0.136? Tell 172.26.0.71
56	117.707353	Dell_80:e3:79	Dell_7f:f4:80	ARP	60	172.26.0.136 is at d8:9e:f3:80:e3:79
57	119.467359	Dell_80:fd:2b	Broadcast	ARP	60	Who has 172.26.0.71? Tell 172.26.0.64
58	119.467371	Dell_7f:f4:80	Dell_80:fd:2b	ARP	42	172.26.0.71 is at d8:9e:f3:7f:f4:80
59	120.730003	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.115? Tell 172.26.124.10
60	121.634840	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.71? Tell 172.26.0.50
61	121.634853	Dell_7f:f4:80	Dell_7f:db:44	ARP	42	172.26.0.71 is at d8:9e:f3:7f:f4:80
62	123.585324	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.115? Tell 172.26.124.10
63	124.198329	Dell_7f:f4:80	Dell_80:fd:2b	ARP	42	Who has 172.26.0.64? Tell 172.26.0.71
64	124.198992	Dell_80:fd:2b	Dell_7f:f4:80	ARP	60	172.26.0.64 is at d8:9e:f3:80:fd:2b
65	124.238872	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.115? Tell 172.26.124.10
66	125.239135	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.115? Tell 172.26.124.10
67	126.204956	Dell_7f:f4:80	Dell_7f:db:44	ARP	42	Who has 172.26.0.50? Tell 172.26.0.71
68	126.205305	Dell_7f:db:44	Dell_7f:f4:80	ARP	60	172.26.0.50 is at d8:9e:f3:7f:f4:80
69	127.592476	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.115? Tell 172.26.124.10
70	128.233026	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.115? Tell 172.26.124.10
71	129.228389	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.115? Tell 172.26.124.10
72	135.607772	ASUSTekC_b0:3b:df	Broadcast	ARP	60	Who has 172.26.0.115? Tell 172.26.124.10

Pregunta y Respuesta hacia la IP del grupo 3

Pregunta y respuesta realizada a la IP del grupo 4

Pregunta y respuesta para detectar la MAC del grupo 5

Pregunta y respuesta del grupo 2



Acto seguido comprobaremos la conectividad con la Gateway.

```

Símbolo del sistema
Microsoft Windows [Versión 10.0.19044.2006]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Raúl Campos>ping 172.26.0.1

Haciendo ping a 172.26.0.1 con 32 bytes de datos:
Respuesta desde 172.26.0.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.26.0.1: bytes=32 tiempo<1m TTL=64
Respuesta desde 172.26.0.1: bytes=32 tiempo=3ms TTL=64
Respuesta desde 172.26.0.1: bytes=32 tiempo<1m TTL=64

Estadísticas de ping para 172.26.0.1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
            (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 3ms, Media = 0ms

C:\Users\Raúl Campos>

```

Coincidencia de la MAC de origen con nuestra MAC:

Wireshark packet capture showing an ARP request. The packet list shows a request from Dell\_7f:f4:80 to Dell\_7f:f4:80. The packet details show the source MAC as d8:9e:f3:7f:f4:80, which is highlighted with a red box and a red arrow pointing to the text "Coincide nuestra dirección MAC". The packet bytes show the MAC address in hexadecimal.

No.	Time	Source	Destination	Protocol	Length	Info
10	64.168381	Dell_7f:f4:80	Contrend_48:62:ea	ARP	42	172.26.0.71 is at d8:9e:f3:7f:f4:80
11	71.849756	Dell_7f:f4:80	Dell_7f:f4:80	ARP	60	Who has 172.26.0.71? Tell 172.26.0.50
12	71.849784	Dell_7f:f4:80	Dell_7f:f4:80	ARP	42	172.26.0.71 is at d8:9e:f3:7f:f4:80
13	71.248453	Dell_7f:f4:80	Dell_7f:f4:80	ARP	42	Who has 172.26.0.50? Tell 172.26.0.71
14	71.249119	Dell_7f:f4:80	Dell_7f:f4:80	ARP	60	172.26.0.50 is at d8:9e:f3:7f:f4:80
15	83.738201	ASUSTekC_b0:3b:df	Broadcast	ARP		
16	84.968651	Contrend_48:62:ea	Dell_7f:f4:80	ARP		
17	84.968668	Dell_7f:f4:80	Contrend_48:62:ea	ARP		
18	85.078259	HP_cc:a3:de	Broadcast	ARP		
19	85.078259	HP_cc:a3:de	Broadcast	ARP		

Frame 13: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on Ethernet II, Src: Dell\_7f:f4:80 (d8:9e:f3:7f:f4:80), Dst: Dell\_7f:f4:80 (d8:9e:f3:7f:f4:80)

Ethernet II, Src: Dell\_7f:f4:80 (d8:9e:f3:7f:f4:80), Dst: Dell\_7f:f4:80 (d8:9e:f3:7f:f4:80)

Destination: Dell\_7f:f4:80 (d8:9e:f3:7f:f4:80)

Source: Dell\_7f:f4:80 (d8:9e:f3:7f:f4:80)

Type: ARP (0x0806)

Address Resolution Protocol (request)

Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . . : Home

Descripción. . . . . : Realtek PCIe GBE Family Controller

Dirección física. . . . . : D8-9E-F3-7F-F4-80

DHCP habilitado. . . . . : si

Configuración automática habilitada. . . . : si

Mac dirección IPv6 local. . . : fe80::19f1:21ab:6985:8122X5(Preferido)

Configuración automática habilitada. . . . : si

La concesión expira. . . . . : lunes, 26 de septiembre de 2022 8:14:55

La concesión predeterminada. . . . . : martes, 27 de septiembre de 2022 11:50:35

Puerta de enlace predeterminada. . . . : 172.26.0.1

Servidor DHCP. . . . . : 172.26.0.1

IAID DHCPv6. . . . . : 215523059

DUID de cliente DHCPv6. . . . . : 00-01-00-01-29-89-63-A9-D8-9E-F3-7F-F4-80

Servidores DNS. . . . . : 172.26.0.1

NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de LAN inalámbrica Wi-Fi:

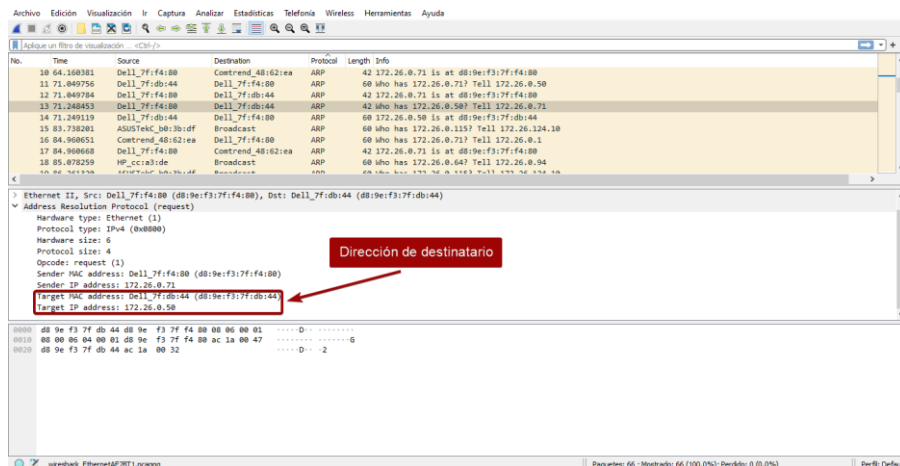
Estado de los medios. . . . . : medios desconectados

Sufijo DNS específico para la conexión. . . : Intel(R) Dual Band Wireless-AC 3165

Descripción. . . . . : Intel(R) Dual Band Wireless-AC 3165

Dirección física. . . . . : D4-60-60-09-F5-41

## Dirección destinatario:



## PASO 4: LOCALICE LA TRAMA DE RESPUESTA ARP QUE CORRESPONDE A LA SOLICITUD ARP QUE SELECCIONÓ.

- Con la dirección IPv4 de destino en la solicitud ARP, localice la trama de respuesta ARP en la sección superior de la pantalla de la captura de Wireshark.
  - ¿Cuál es la dirección IPv4 del dispositivo de destino de su solicitud ARP? 172.26.0.50.
- Selecione la trama de respuesta en la sección superior del resultado de Wireshark. Es posible que deba desplazarse por la ventana para encontrar la trama de respuesta que coincida con la dirección IPv4 de destino identificada en el paso anterior. Amplíe las filas Ethernet II y Protocolo de resolución de direcciones (respuesta) en la sección del medio de la pantalla.
  - ¿La trama de respuesta ARP es una trama de difusión? No, es unicast.
  - ¿Cuál es la dirección MAC de destino de la trama? D8:9e:f3:f4:80.
  - ¿Es la dirección MAC de su PC? Sí.
  - ¿Es la dirección MAC de su PC? D8:9e:f3:db:44.

### PARTE 3: EXAMINE LAS ENTRADAS DE LA CACHÉ ARP EN LA PC.

#### PASO 1: VEA LAS ENTRADAS DE LA CACHÉ ARP EN UNA PC CON WINDOWS.

Para ello abriremos la cmd y pondremos arp -a.

```

C:\Users\Raúl Campos>arp -a

Interfaz: 172.26.0.71 --- 0x5
Dirección de Internet      Dirección física      Tipo
172.26.0.1                 d8-b6-b7-48-62-ea    dinámico
172.26.0.50                d8-9e-f3-7f-db-44    dinámico
172.26.0.55                bc-5f-f4-df-a4-1f    dinámico
172.26.0.64                d8-9e-f3-80-fd-2b    dinámico
172.26.0.76                10-bf-48-7e-f6-21    dinámico
172.26.0.94                04-0e-3c-cc-a3-de    dinámico
172.26.0.129               54-a0-50-7d-ff-92    dinámico
172.26.255.255             ff-ff-ff-ff-ff-ff    estático
224.0.0.2                  01-00-5e-00-00-02    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.192.152.143            01-00-5e-40-98-8f    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático
  
```

¿Qué produce el arp -a en su PC?

- Produce las entradas que se encuentran en la caché de mi PC.

Arp /?

¿Qué opción elimina una entrada de la caché ARP? ARP -d inet addr.

¿Cuál sería el resultado del comando arp -d \*? En este caso borraría TODO el caché. (\* to delete all hosts.

### REFLEXIÓN

1. ¿CUÁL ES EL BENEFICIO DE MANTENER LAS ENTRADAS DE LA CACHÉ ARP EN MEMORIA DE LA COMPUTADORA DE ORIGEN?

Pues mantener las entradas de la caché permite que los hosts puedan tener la dirección hardware del remitente en la caché, lo que es una ventaja en caso de modificación de la dirección por cambio de tarjeta de red, por ejemplo.

2. SI LA DIRECCIÓN IPV4 DE DESTINO NO SE ENCUENTRA EN LA MISMA RED QUE EL HOST DE ORIGEN, ¿QUÉ DIRECCIÓN MAC SE USARÁ COMO DIRECCIÓN MAC DE DESTINO DE LA TRAMA?

Se usará la MAC del router como destino de la trama.