

## 1. ¿Qué es Wireshark?

- Es una herramienta que analiza el tráfico de red.
- Permite ver en detalle qué datos están entrando o saliendo de un dispositivo, incluyendo direcciones IP, protocolos, y puertos utilizados.
- Útil para verificar si las reglas de un firewall están bloqueando o permitiendo correctamente el tráfico hacia puertos específicos.

## 2. Instalación de Wireshark

### 2.1 Descargar e instalar Wireshark

1. Ve a la página oficial de Wireshark:  
<https://www.wireshark.org/download.html>
2. Descarga la versión para tu sistema operativo.
3. Sigue el instalador:
  - En Windows, permite instalar **Npcap** (necesario para capturar paquetes).
  - En Linux, instala Wireshark desde los repositorios:  
*sudo apt install wireshark # Para distribuciones basadas en Debian*  
*sudo yum install wireshark # Para distribuciones basadas en Red Hat*
4. Abre Wireshark para verificar que funciona correctamente.

## 3. Preparativos

### 3.1 Identificar la dirección IP de tu máquina

Necesitarás la dirección IP de tu máquina para enfocar el análisis en tu tráfico de red:

- En **Windows**:
  1. Abre una terminal (cmd) y escribe:  
*ipconfig*
  2. Busca el campo **IPv4 Address**.
    - Ejemplo: 192.168.1.10.
- En **Linux**:
  1. Escribe en la terminal:  
*ifconfig*
  2. Busca el campo **inet** asociado a tu interfaz de red.

### 3.2 Configurar el firewall

Antes de empezar, asegúrate de que el firewall está configurado para bloquear o permitir tráfico en puertos específicos. Por ejemplo:

- Bloquea puertos como **3389 (RDP)** y **80 (HTTP)** para probar si el firewall bloquea correctamente el tráfico.

## 4. Iniciando captura de tráfico en Wireshark

1. **Abre Wireshark.**
2. **Selecciona la interfaz de red activa:**
  - En la pantalla principal, verás una lista de interfaces (Wi-Fi, Ethernet, etc.).
  - Identifica cuál está en uso (generalmente muestra más actividad en tiempo real).
3. **Inicia la captura de tráfico:**
  - Haz clic en la interfaz para comenzar la captura.
  - Wireshark mostrará un flujo de paquetes capturados en tiempo real.

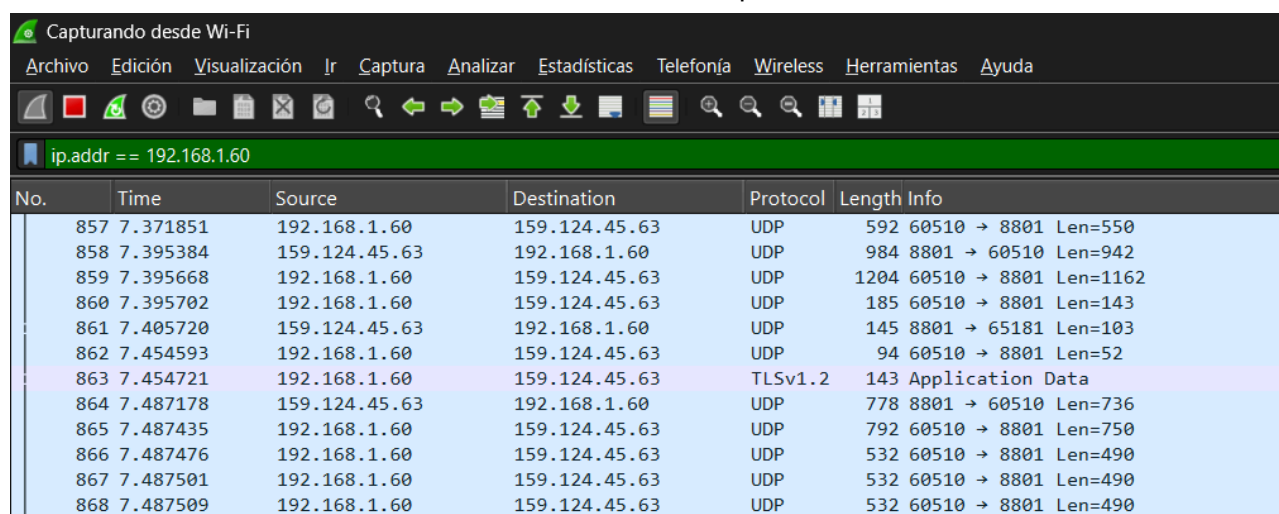
## 5. Filtro para ver tráfico relacionado con puertos

### 5.1 Aplicar un filtro básico

1. Detén la captura después de algunos segundos (botón cuadrado rojo).
2. En el campo de **filtros** (parte superior), escribe:
 

```
ip.addr == 192.168.1.10
```

  - Reemplaza 192.168.1.10 con la IP de tu máquina.
  - Esto filtra el tráfico relacionado con tu dispositivo.



Capturando desde Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ip.addr == 192.168.1.60

No.	Time	Source	Destination	Protocol	Length	Info
857	7.371851	192.168.1.60	159.124.45.63	UDP	592	60510 → 8801 Len=550
858	7.395384	159.124.45.63	192.168.1.60	UDP	984	8801 → 60510 Len=942
859	7.395668	192.168.1.60	159.124.45.63	UDP	1204	60510 → 8801 Len=1162
860	7.395702	192.168.1.60	159.124.45.63	UDP	185	60510 → 8801 Len=143
861	7.405720	159.124.45.63	192.168.1.60	UDP	145	8801 → 65181 Len=103
862	7.454593	192.168.1.60	159.124.45.63	UDP	94	60510 → 8801 Len=52
863	7.454721	192.168.1.60	159.124.45.63	TLSv1.2	143	Application Data
864	7.487178	159.124.45.63	192.168.1.60	UDP	778	8801 → 60510 Len=736
865	7.487435	192.168.1.60	159.124.45.63	UDP	792	60510 → 8801 Len=750
866	7.487476	192.168.1.60	159.124.45.63	UDP	532	60510 → 8801 Len=490
867	7.487501	192.168.1.60	159.124.45.63	UDP	532	60510 → 8801 Len=490
868	7.487509	192.168.1.60	159.124.45.63	UDP	532	60510 → 8801 Len=490

### 5.2 Verificar tráfico por puerto

1. Para analizar un puerto específico, escribe en el filtro:
 

```
tcp.port == 80 || udp.port == 80
```

  - Esto muestra solo tráfico relacionado con el puerto 80 (HTTP).

Capturando desde Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp.port == 80 || udp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
9586	81.413882	192.168.1.60	185.43.181.138	TCP	66	64263 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9588	81.427060	185.43.181.138	192.168.1.60	TCP	66	80 → 64263 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128
9589	81.427214	192.168.1.60	185.43.181.138	TCP	54	64263 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
9590	81.427539	192.168.1.60	185.43.181.138	HTTP	178	GET /ncsi.txt HTTP/1.1
9591	81.440625	185.43.181.138	192.168.1.60	TCP	60	80 → 64263 [ACK] Seq=1 Ack=125 Win=64128 Len=0
9592	81.440625	185.43.181.138	192.168.1.60	HTTP	233	HTTP/1.1 200 OK (text/plain)
9593	81.440625	185.43.181.138	192.168.1.60	TCP	60	80 → 64263 [FIN, ACK] Seq=180 Ack=125 Win=64128 Len=0
9594	81.440688	192.168.1.60	185.43.181.138	TCP	54	64263 → 80 [ACK] Seq=125 Ack=181 Win=65280 Len=0
9595	81.441058	192.168.1.60	185.43.181.138	TCP	54	64263 → 80 [FIN, ACK] Seq=125 Ack=181 Win=65280 Len=0
9596	81.454666	185.43.181.138	192.168.1.60	TCP	60	80 → 64263 [ACK] Seq=181 Ack=126 Win=64128 Len=0

2. Para analizar varios puertos, usa:

*tcp.port == 80 || tcp.port == 3389*

- Esto incluye tanto tráfico HTTP (80) como RDP (3389).

Capturando desde Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

tcp.port == 80 || tcp.port == 3389

No.	Time	Source	Destination	Protocol	Length	Info
9586	81.413882	192.168.1.60	185.43.181.138	TCP	66	64263 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
9588	81.427060	185.43.181.138	192.168.1.60	TCP	66	80 → 64263 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1452 SACK_PERM WS=128
9589	81.427214	192.168.1.60	185.43.181.138	TCP	54	64263 → 80 [ACK] Seq=1 Ack=1 Win=65280 Len=0
9590	81.427539	192.168.1.60	185.43.181.138	HTTP	178	GET /ncsi.txt HTTP/1.1
9591	81.440625	185.43.181.138	192.168.1.60	TCP	60	80 → 64263 [ACK] Seq=1 Ack=125 Win=64128 Len=0
9592	81.440625	185.43.181.138	192.168.1.60	HTTP	233	HTTP/1.1 200 OK (text/plain)
9593	81.440625	185.43.181.138	192.168.1.60	TCP	60	80 → 64263 [FIN, ACK] Seq=180 Ack=125 Win=64128 Len=0
9594	81.440688	192.168.1.60	185.43.181.138	TCP	54	64263 → 80 [ACK] Seq=125 Ack=181 Win=65280 Len=0
9595	81.441058	192.168.1.60	185.43.181.138	TCP	54	64263 → 80 [FIN, ACK] Seq=125 Ack=181 Win=65280 Len=0
9596	81.454666	185.43.181.138	192.168.1.60	TCP	60	80 → 64263 [ACK] Seq=181 Ack=126 Win=64128 Len=0

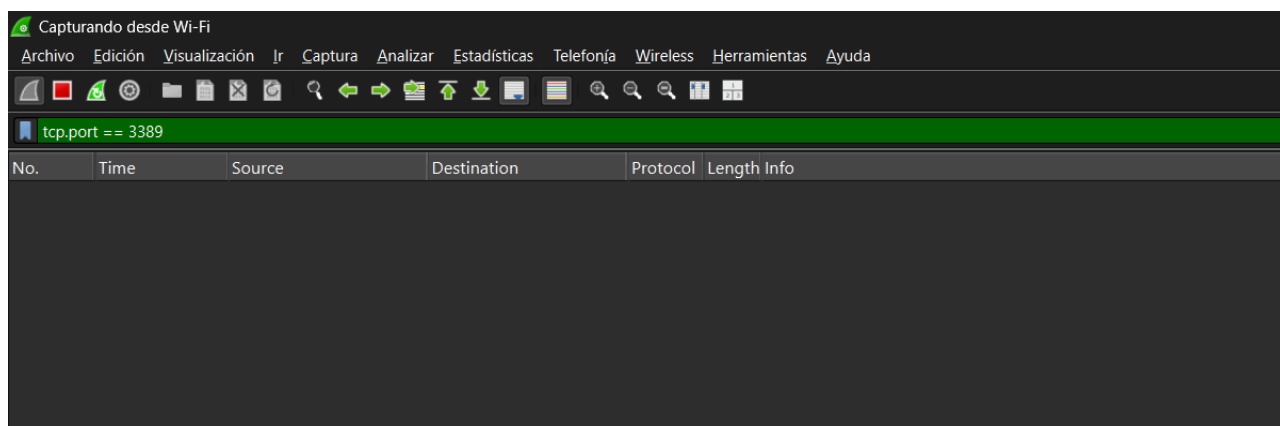
## 6. Interpretar los Resultados

### 6.1 Columnas importantes

- **Source (Fuente):** IP de origen del paquete.
- **Destination (Destino):** IP a la que se envió el paquete.
- **Protocol:** Tipo de protocolo (TCP, UDP, etc.).
- **Length:** Tamaño del paquete.
- **Info:** Información adicional, como número de puerto o detalles del protocolo.

### 6.2 Identificar tráfico hacia puertos específicos

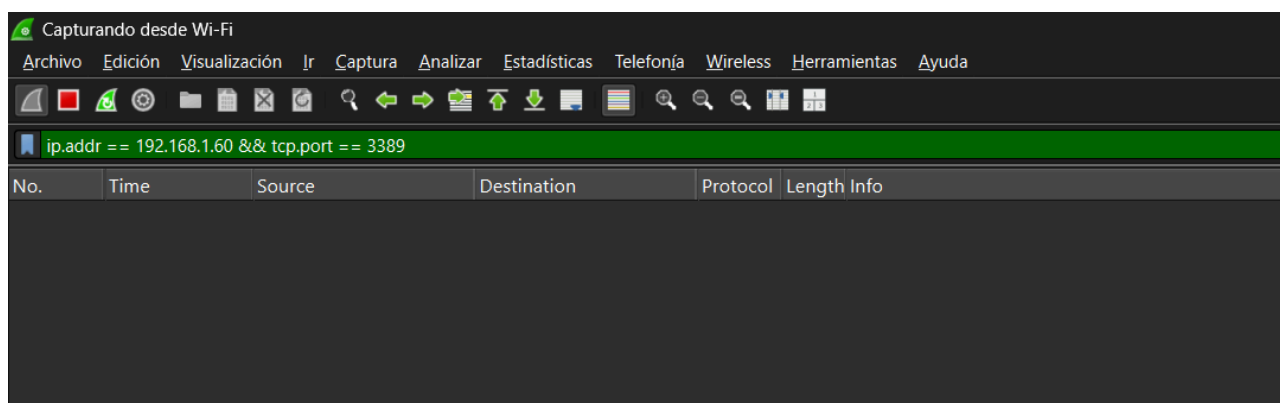
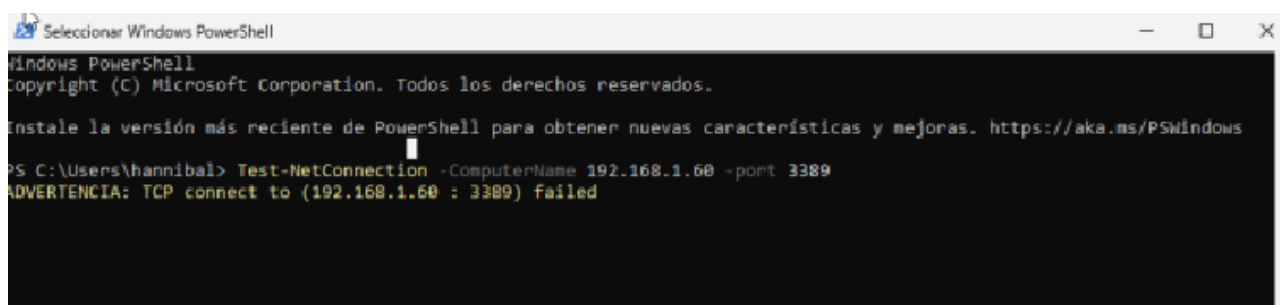
- Busca paquetes relacionados con los puertos abiertos o bloqueados.
  - Si el puerto está abierto, verás paquetes con **Destination Port** igual al número del puerto.
  - Si el firewall bloquea el puerto, no debería aparecer tráfico hacia él.



## 6.3 Ejemplo de análisis

- Si configuraste el firewall para bloquear el puerto **3389**:
  - Captura tráfico desde una máquina externa intentando conectarse a tu IP en ese puerto.
  - Si el firewall funciona correctamente, no verás paquetes hacia ese puerto.

### Desde VM



## 7. Generar tráfico para la prueba

Para probar la efectividad del firewall, puedes generar tráfico hacia tu máquina utilizando herramientas básicas:

### 7.1 Ping

En una terminal de otra máquina, usa el comando ping para generar tráfico ICMP:

ping 192.168.1.10

- Filtra en Wireshark:

*icmp*

```

Windows 11 VM [Corriendo] - Oracle VirtualBox

Símbolo del sistema

C:\Users\hannibal>ping 192.168.1.60

Pongiendo ping a 192.168.1.60 con 32 bytes de datos:
Respuesta desde 192.168.1.60: bytes=32 tiempo=1ms TTL=255
Respuesta desde 192.168.1.60: bytes=32 tiempo=2ms TTL=255
Respuesta desde 192.168.1.60: bytes=32 tiempo=6ms TTL=255
Respuesta desde 192.168.1.60: bytes=32 tiempo=5ms TTL=255

Estadísticas de ping para 192.168.1.60:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 6ms, Media = 3ms

C:\Users\hannibal>ping 192.168.1.60

Pongiendo ping a 192.168.1.60 con 32 bytes de datos:
Respuesta desde 192.168.1.60: bytes=32 tiempo=1ms TTL=255
Respuesta desde 192.168.1.60: bytes=32 tiempo=7ms TTL=255
Respuesta desde 192.168.1.60: bytes=32 tiempo=1ms TTL=255
Respuesta desde 192.168.1.60: bytes=32 tiempo<1m TTL=255

Estadísticas de ping para 192.168.1.60:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 7ms, Media = 2ms

C:\Users\hannibal>
    
```

Capturando desde Wi-Fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

icmp

No.	Time	Source	Destination	Protocol	Length	Info
27587	74.213694	192.168.1.1	192.168.1.60	ICMP	138	Destination unreachable (Port unreachable)
27777	75.898436	192.168.1.1	192.168.1.60	ICMP	138	Destination unreachable (Port unreachable)
27934	77.216511	192.168.1.1	192.168.1.60	ICMP	138	Destination unreachable (Port unreachable)
29295	83.216766	192.168.1.1	192.168.1.60	ICMP	138	Destination unreachable (Port unreachable)
29454	84.718167	192.168.1.1	192.168.1.60	ICMP	138	Destination unreachable (Port unreachable)

## 7.2 Conexión a puertos específicos

Usa **telnet** para intentar conectar a puertos específicos:

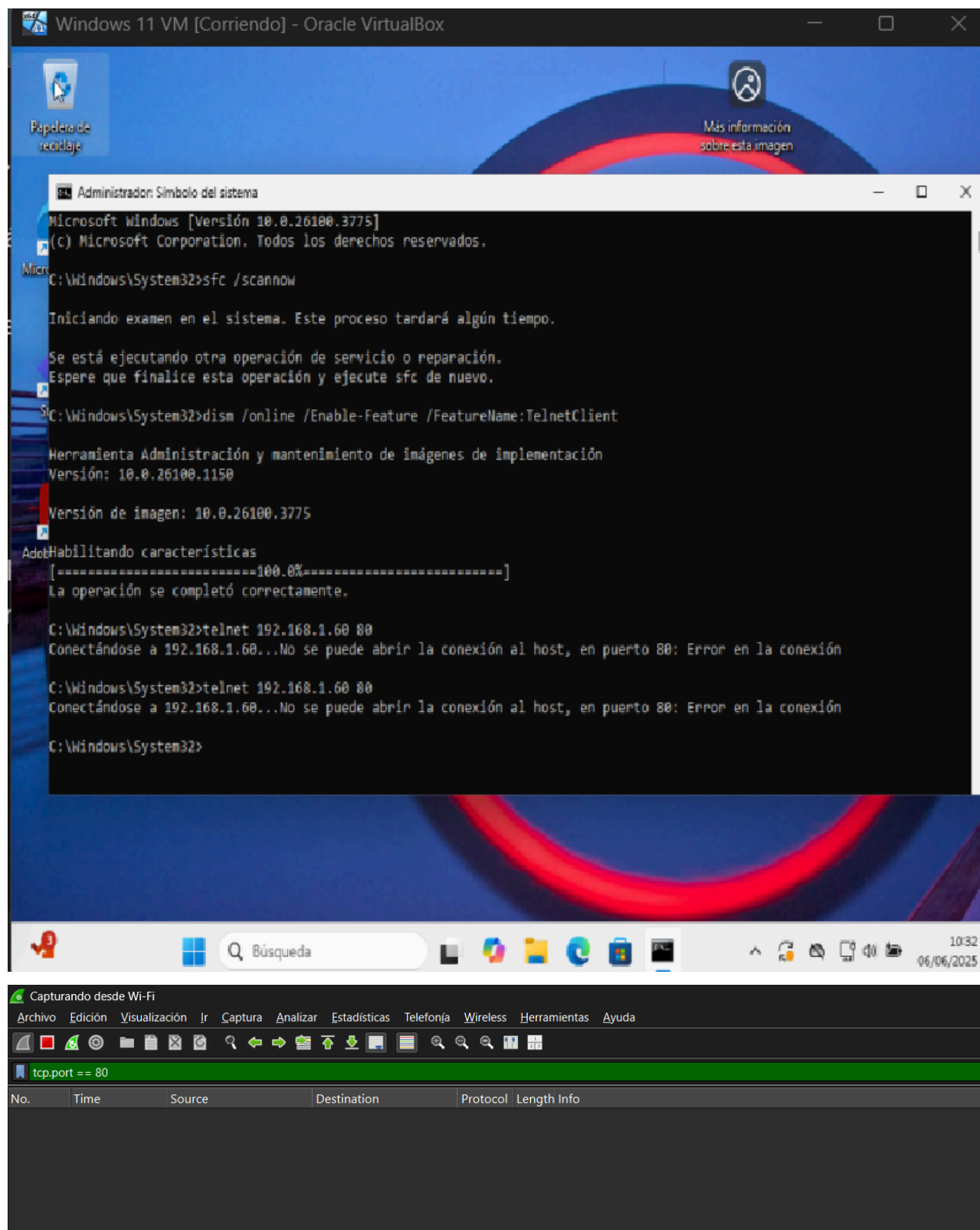
1. Desde otra máquina, escribe:

*telnet 192.168.1.10 80*

Esto intentará abrir una conexión con tu máquina en el puerto 80.

2. Filtra en Wireshark:

*tcp.port == 80*



## 8. Guardar y analizar resultados

1. Guarda la captura en un archivo para revisarla más tarde:
  - Ve a **File > Save As** y guarda con la extensión .pcapng.

2. Analiza el tráfico capturado:
  - Busca puertos abiertos que deberían estar cerrados.
  - Verifica que el tráfico no deseado esté bloqueado por el firewall.

## 9. Acciones correctivas

1. Bloquea puertos innecesarios desde el firewall.
2. Repite las pruebas para confirmar que los cambios en el firewall son efectivos.
3. Documenta tus hallazgos.