



**UNIVERSIDAD TECNOLÓGICA DE PUEBLA
DIVISIÓN DE TECNOLOGÍAS DE LA
INFORMACIÓN - INGENIERÍA EN DESARROLLO Y
GESTIÓN DE SOFTWARE**

**MATERIA:
Seguridad Desarrollo de Software**

Práctica 5 Uso de wireshark

**DOCENTE:
Luz María Pérez Sarmiento**

**ALUMNO:
Justino Juan Carlos Andrade Reyes**

8 ° A FECHA: 20/03/2025

ÍNDICE

<i>Discusión Guiada</i>	<i>3</i>
¿Qué es wireshark y para qué sirve?	3
<i>Ejercicio Práctico</i>	<i>3</i>
<i>Análisis y Reporte</i>	<i>4</i>
<i>Reflexión Final</i>	<i>8</i>

Discusión Guiada

¿Qué es Wireshark y para qué sirve?

Wireshark es una herramienta de análisis de protocolos de red ampliamente utilizada. Su función principal es capturar y analizar el tráfico de red en tiempo real, permitiendo a los usuarios inspeccionar los datos que fluyen a través de una red. Es especialmente útil para administradores de red, profesionales de seguridad y desarrolladores que necesitan diagnosticar problemas de red, analizar el rendimiento o investigar actividades sospechosas.

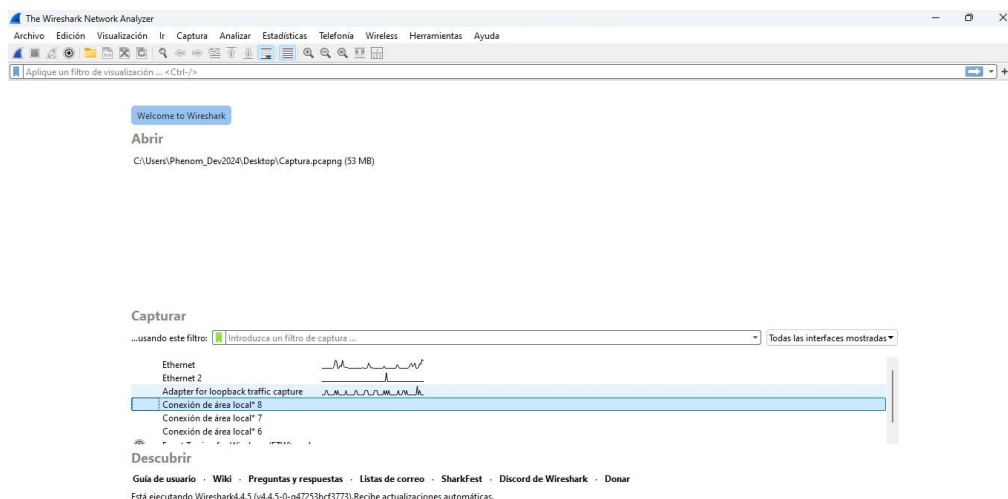
Características principales de Wireshark:

1. **Captura de paquetes:** Wireshark puede capturar paquetes de red en vivo desde una variedad de interfaces de red, como Ethernet, Wi-Fi, Bluetooth, entre otras.
2. **Análisis detallado:** Proporciona una vista detallada de cada paquete, desglosando los encabezados y datos de los protocolos de red (como TCP/IP, HTTP, DNS, etc.).
3. **Filtrado avanzado:** Permite filtrar el tráfico para centrarse en paquetes específicos, lo que facilita la identificación de problemas o patrones.
4. **Compatibilidad con múltiples protocolos:** Soporta una amplia gama de protocolos de red, lo que lo hace versátil para diferentes entornos.
5. **Herramientas de diagnóstico:** Incluye funcionalidades para detectar errores, latencias y otros problemas de red.

Usos comunes de Wireshark:

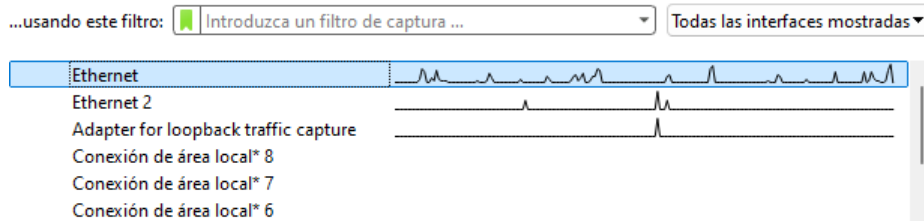
- **Diagnóstico de problemas de red:** Identificar cuellos de botella, paquetes perdidos o configuraciones incorrectas.
- **Seguridad de red:** Detectar tráfico malicioso, como escaneos de puertos, ataques de denegación de servicio (DoS) o intentos de intrusión.
- **Desarrollo y pruebas:** Verificar el correcto funcionamiento de aplicaciones y servicios de red.
- **Educación y aprendizaje:** Estudiar cómo funcionan los protocolos de red en la práctica.

Ejercicio Práctico



Para empezar el análisis de tráfico en la red elegimos la interfaz a utilizar en este caso usaremos Ethernet

Capturar

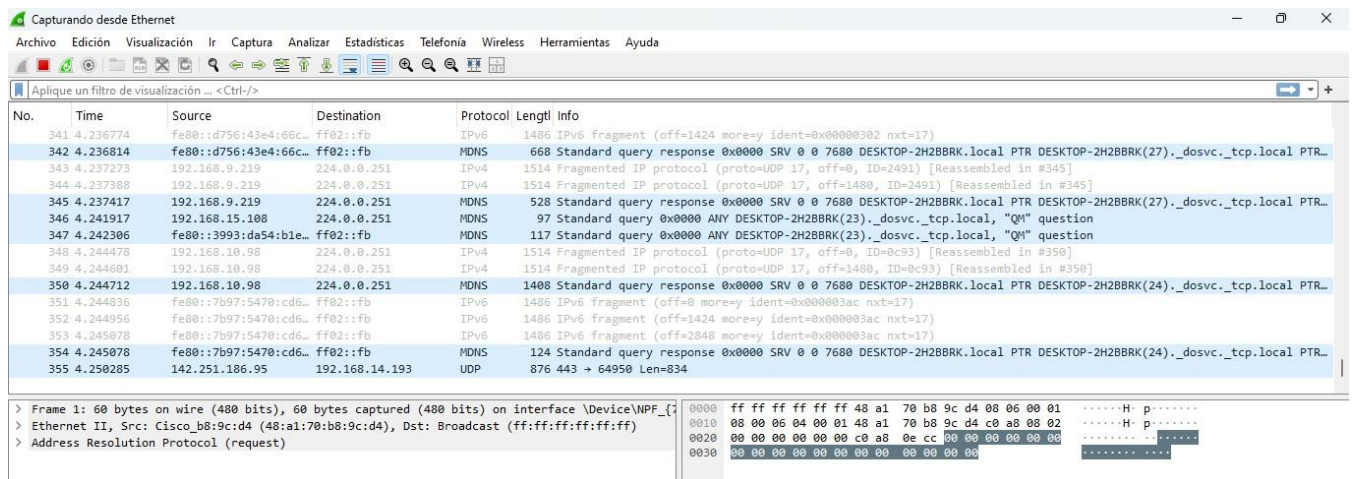


Descubrir

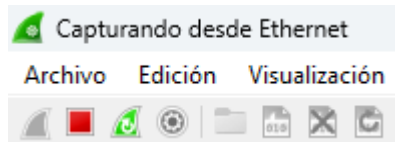
[Guía de usuario](#) · [Wiki](#) · [Preguntas y respuestas](#) · [Listas de correo](#) · [SharkFest](#) · [Discord de Wireshark](#) · [Donar](#)

Está ejecutando Wireshark 4.4.5 (v4.4.5-0-g47253bcf3773). Recibe actualizaciones automáticas.

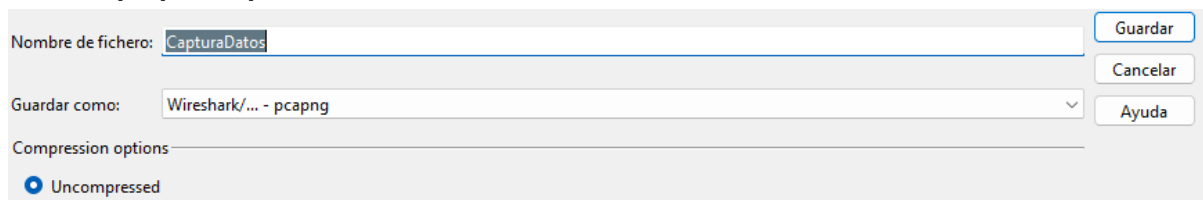
Una vez hecho esto empezara a mostrar toda la actividad de nuestra red



Después que tengamos paquetes capturados paramos el programa

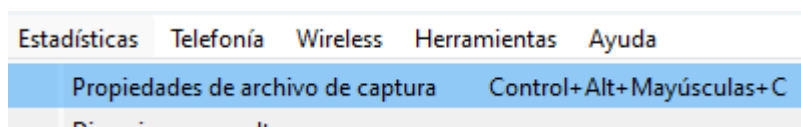


Se guardan los paquetes para analizar.



Análisis y Reporte

Propiedad de Archivo de Captura



Estadísticas > Propiedades de archivo de captura para obtener un resumen de la captura,

incluyendo cantidad de paquetes, duración y velocidad de captura.

Wireshark · Propiedades de archivo de captura · CapturaDatos.pcapng

Detalles

Archivo

Nombre:

C:\Users\Phenom_Dev2024\Desktop\CapturaDatos.pcapng

Longitud:

60 MB

Hash (SHA256):

d9ad6091a87f91aa9df961dd8ba58a095168ebe782a8825c40ad4d16f4879ab5

Hash (SHA1):

37ba1474338d20c9528d9b132f6dc183a534ec6c

Formato:

Wireshark/... - pcapng

Encapsulado:

Ethernet

Intervalo

Primer paquete:

2025-03-19 16:02:51

Último paquete:

2025-03-19 16:06:29

Transcurrido:

00:03:37

Captura

Hardware:

AMD Phenom(tm) II X2 B57 Processor

SO:

64-bit Windows 11 (23H2), build 22631

Aplicación:

Dumpcap (Wireshark) 4.4.5 (v4.4.5-0-g47253bcf3773)

Interfaces

Interfaz	Paquetes perdidos	Filtro de captura	Tipo de enlace	Packet size limit (snaplen)
Ethernet	0 (0.0%)	ninguno	Ethernet	262144 bytes

Estadísticas

Medida	Capturado	Mostrado	Marcado
Paquetes	70398	70398 (100.0%)	—
Espacio de tiempo, s	217.319	217.319	—
Promedio pps	323.9	323.9	—
Promedio de tamaño de paquete, B	831	831	—
Bytes	58474778	58474778 (100.0%)	0
Promedio de bytes/s	269 k	269 k	—
Promedio de bits/s	2152 k	2152 k	—

Jerarquía de Protocolo:

Estadísticas

Telefonía

Wireless

Herramientas

Ayuda

Propiedades de archivo de captura

Control+Alt+Mayúsculas+C

Direcciones resueltas

Jerarquía de protocolo

Estadísticas > Jerarquía de protocolo para ver un desglose de los protocolos utilizados en la captura.

Wireshark · Estadísticas de jerarquía de protocolo · CapturaDatos.pcapng

Protocolo	Porcentaje de paquetes	Paquetes	Porcentaje de bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s	PDUs
Frame	100.0	70398	100.0	58474778	2152 k	0	0	0	70398
Ethernet	100.0	70398	1.8	1034011	38 k	18	252	9	70398
Logical-Link Control	0.3	177	0.0	677	24	0	0	0	177
Spanning Tree Protocol	0.2	123	0.0	4305	158	123	4305	158	123
Datagram Delivery Protocol	0.0	11	0.0	143	5	0	0	0	11
Zone Information Protocol	0.0	11	0.0	88	3	11	88	3	11
Cisco Discovery Protocol	0.0	3	0.0	1371	50	3	1371	50	3
Internetwork Packet eXchange	0.1	52	0.0	1560	57	0	0	0	52
IPX Routing Information Protocol	0.1	52	0.0	520	19	12	120	4	52
Malformed Packet	0.1	40	0.0	0	0	40	0	0	40
Internet Protocol Version 6	37.9	26710	2.1	1208744	44 k	0	0	0	26710
User Datagram Protocol	17.3	12150	0.2	97200	3578	0	0	0	12150
Multicast Domain Name System	16.8	11847	39.2	22911673	843 k	11674	19505469	718 k	11847
Malformed Packet	0.2	173	0.0	0	0	173	0	0	173
Link-local Multicast Name Resolution	0.2	169	0.0	7001	257	169	7001	257	169
eXtensible Markup Language	0.0	20	0.0	20544	756	20	20544	756	20
Domain Name System	0.1	41	0.0	1608	59	41	1608	59	41
DHCPv6	0.1	52	0.0	3911	143	52	3911	143	52
Internet Control Message Protocol v6	1.0	680	0.0	21484	790	680	21484	790	680
Internet Protocol Version 4	58.1	40933	1.4	819000	30 k	0	0	0	40933
User Datagram Protocol	33.5	23563	0.3	188504	6939	0	0	0	23563
Simple Service Discovery Protocol	0.3	198	0.1	37559	1382	198	37559	1382	198
QUIC IETF	6.2	4393	4.2	2476259	91 k	4393	2468548	90 k	4416
NetBIOS Name Service	0.5	374	0.0	22228	818	374	22228	818	374
NetBIOS Datagram Service	0.0	35	0.0	2870	105	0	0	0	35

No hay filtro de visualización.

Cerrar

Copiar

Protocols

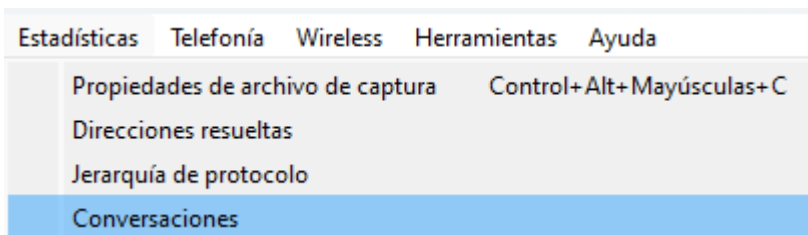
Ayuda

Este es el análisis de **Jerarquía de Protocolo** en Wireshark, que muestra los protocolos detectados en la captura de paquetes.

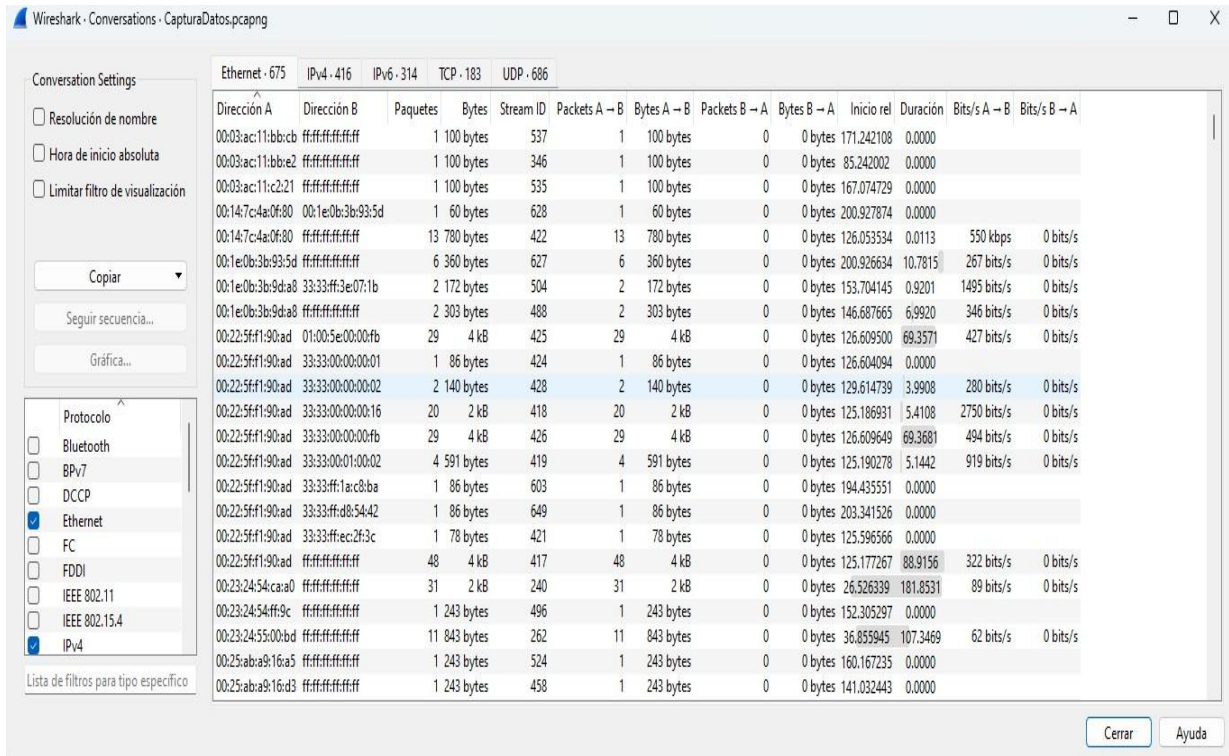
- **Ethernet (100%):** Todos los paquetes capturados están en la capa de enlace de datos.
- **IPv6 (37.9%) e IPv4 (58.1%):** La mayoría del tráfico usa estos protocolos de red.
- **UDP (17.3%) y TCP (33.5%):** Se observa más tráfico UDP que TCP, lo que indica uso de protocolos sin conexión.
- **DNS (0.1%):** Consultas/respuestas de nombres de dominio.
- **DHCPv6 (0.6%):** Asignación de direcciones IPv6.
- **Paquetes malformados:** Algunos paquetes están dañados y no se interpretan correctamente.

Esta vista ayuda a entender qué protocolos predominan en la red y su impacto en el tráfico.

Conversaciones:



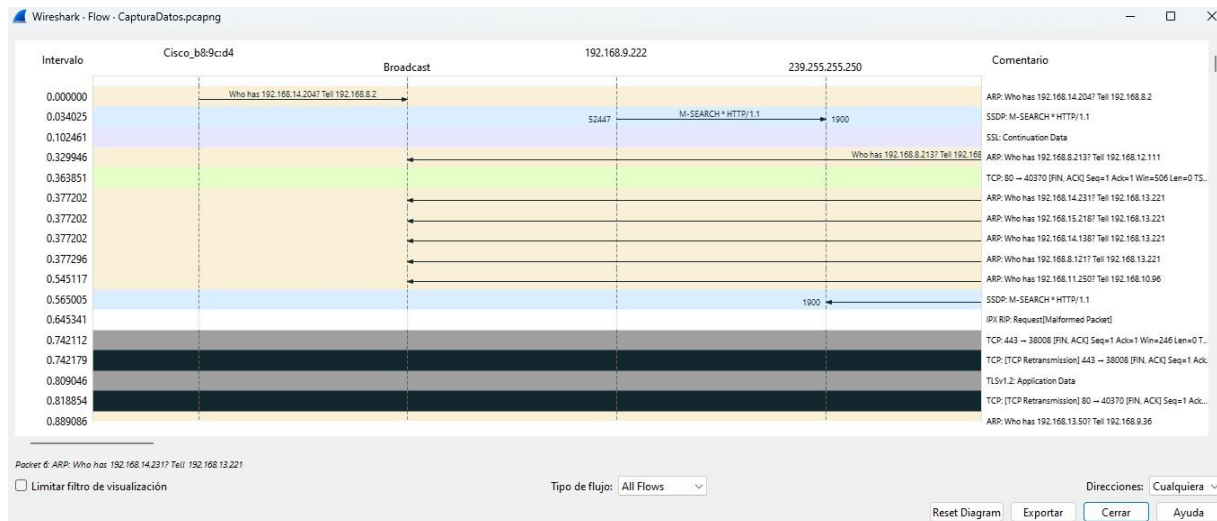
Estadísticas > Conversaciones para ver las conexiones entre direcciones IP y los protocolos utilizados.



"Conversaciones" en Wireshark, proporciona un resumen de las comunicaciones de red entre diferentes direcciones.

Conversations Settings

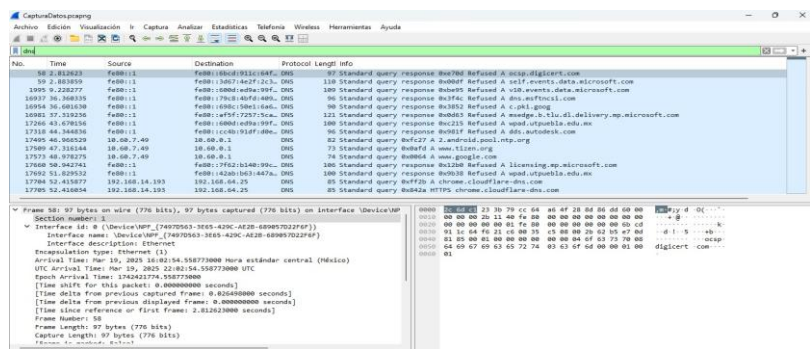
- Resolución de nombre: Si está activado, Wireshark intentará resolver las direcciones IP a nombres de dominio.
- Hora de inicio absoluta: Muestra el tiempo absoluto en lugar del relativo.
- Limitar filtro de visualización: Aplica el filtro actual a las conversaciones.



Estadísticas > Gráfica de flujo para visualizar el tráfico entre hosts de una manera más claro.

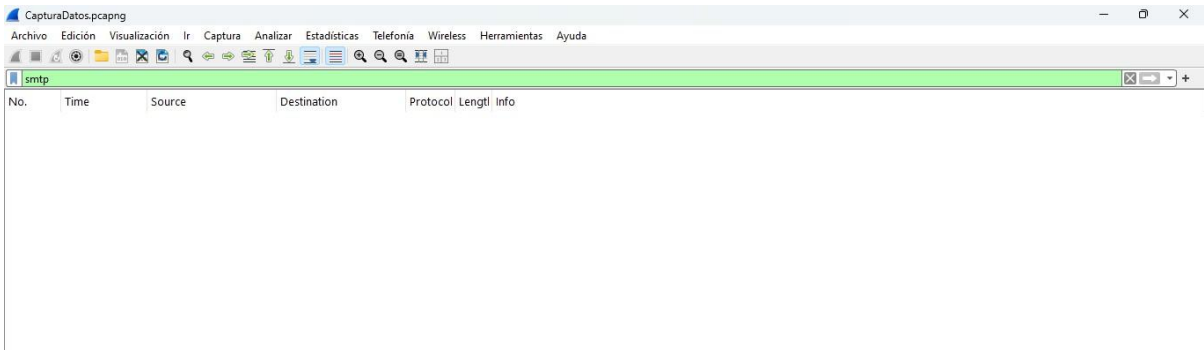
Filtro DNS

Aplicamos el filtro DNS en la barra de filtros



El **análisis del protocolo DNS** en Wireshark permite ver consultas y respuestas de nombres de dominio. Puedes identificar:

- **Consultas DNS:** Dispositivos pidiendo la IP de un dominio
 - **Respuestas DNS:** Servidores devolviendo la IP solicitada.
 - **Tiempo de respuesta:** Para detectar latencia en la resolución de nombres.
 - **Solicitudes fallidas:** Posibles problemas de conectividad o configuración.
- Filtro SMTP



Si el análisis del protocolo SMTP (correo electrónico) en Wireshark sale vacío, puede ser por:

- No hay tráfico SMTP capturado: Wireshark no registró correos enviados o recibidos.
- Cifrado (TLS/SSL): Muchos servidores usan cifrado, ocultando los datos de SMTP.
- Falta de filtro adecuado: Usa **smtp** en el filtro de Wireshark para ver solo paquetes SMTP.

Reflexión Final

Wireshark no es solo una herramienta técnica; es un aliado estratégico para cualquier organización o profesional que trabaje con redes. Su capacidad para proporcionar visibilidad, seguridad y eficiencia lo convierte en un recurso indispensable en un mundo donde las redes son el núcleo de la comunicación y la operación empresarial. Sin embargo, su uso responsable y ético es fundamental, ya que también puede ser empleado con fines malintencionados si cae en manos equivocadas. Por ello, su aplicación debe ir siempre acompañada de un sólido entendimiento ético y profesional.