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

ÍNDCE

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.

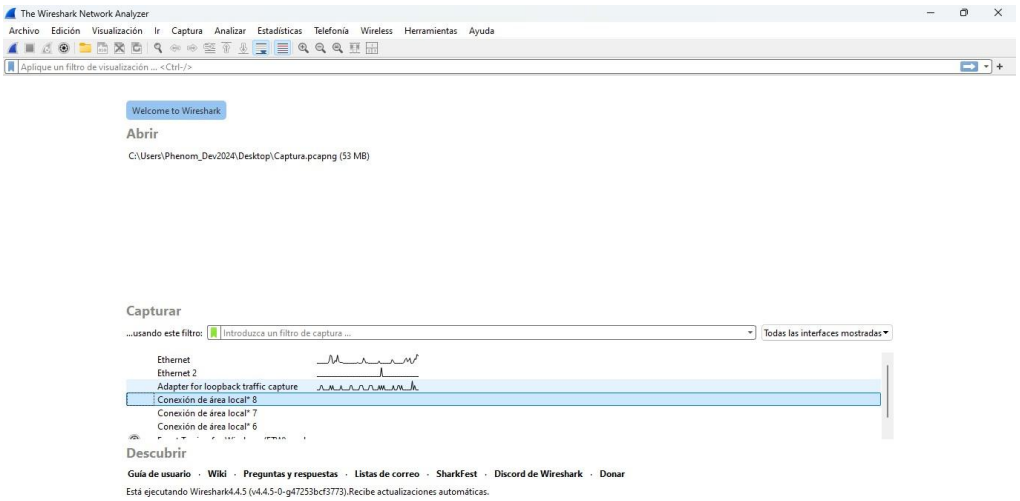
Características principales de Wireshark:

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.

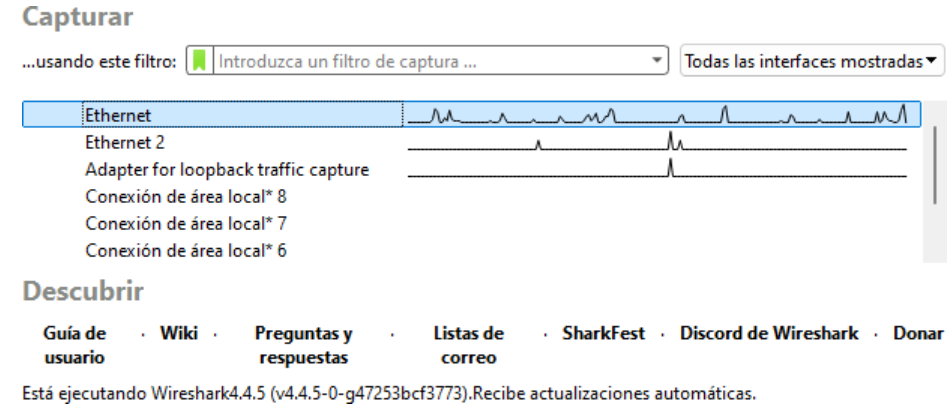
Usos comunes de Wireshark:

- **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.

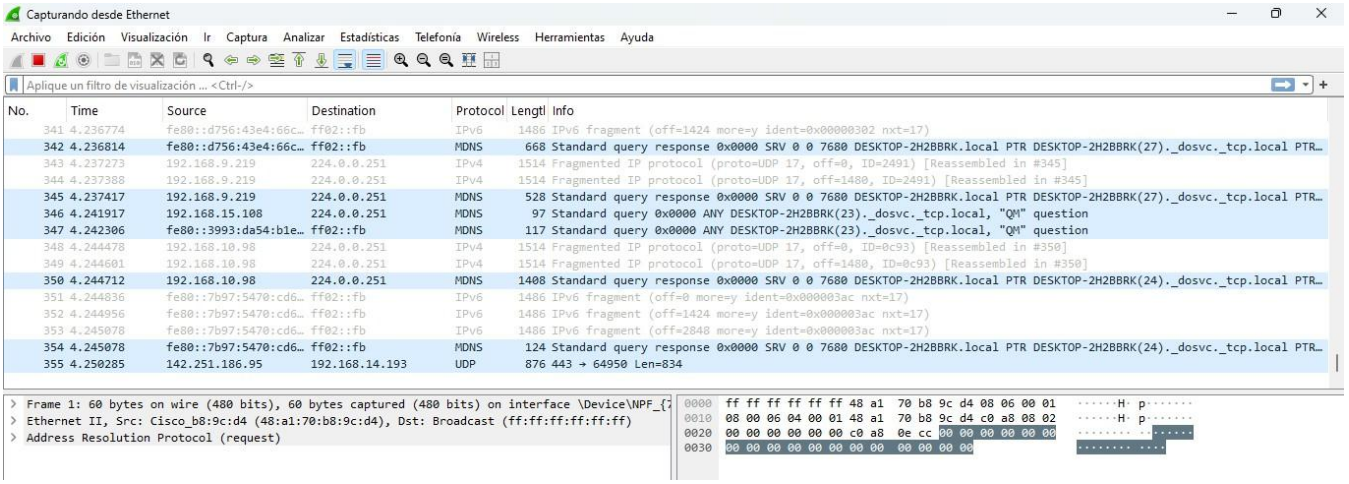
Ejercicio Práctico



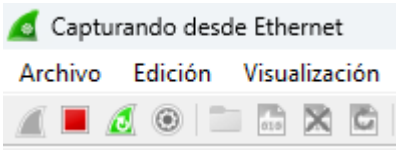
Para empezar el análisis de trafico en la red elegimos la interfaz a utilizar en este caso usaremos Ethernet



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

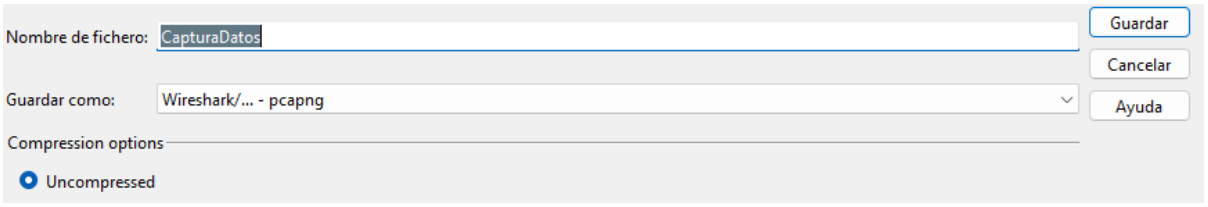


Después que tengamos paquetes capturados paramos el programa



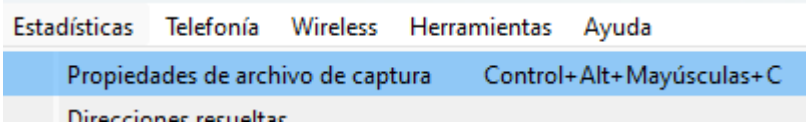
↗

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)

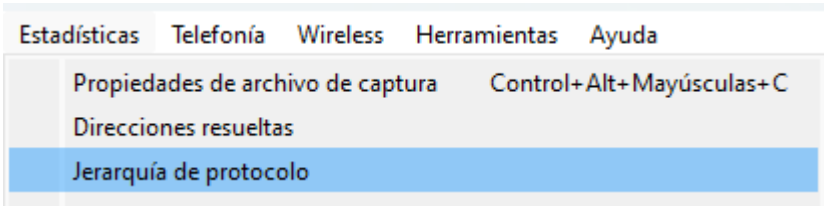
Interfaces

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

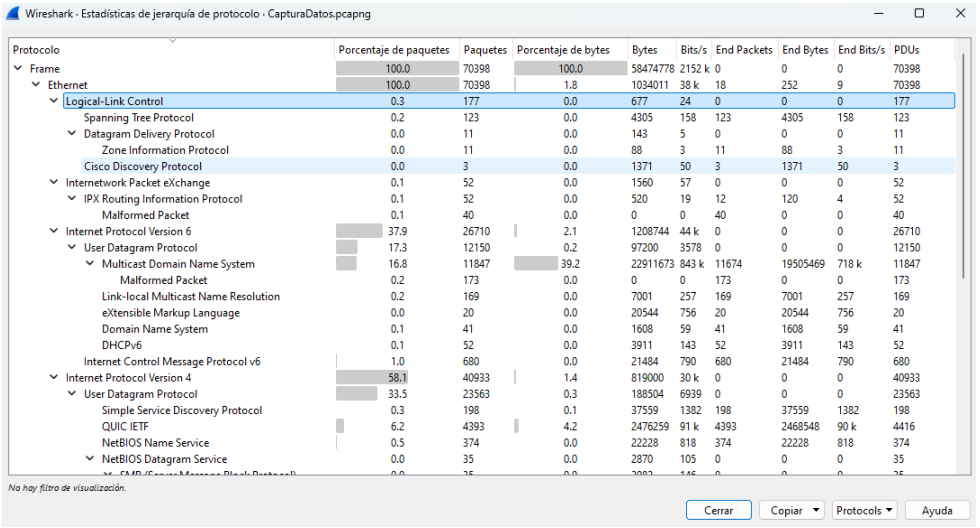
Estadísticas

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

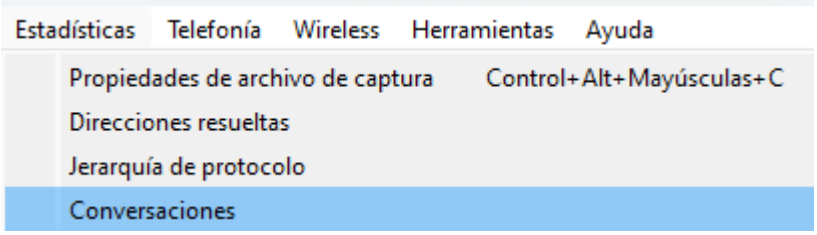


Este es el análisis de **Jerarquía de Protocolo** en Wireshark, que muestra los protocolos detectados en la captura de paquetes.

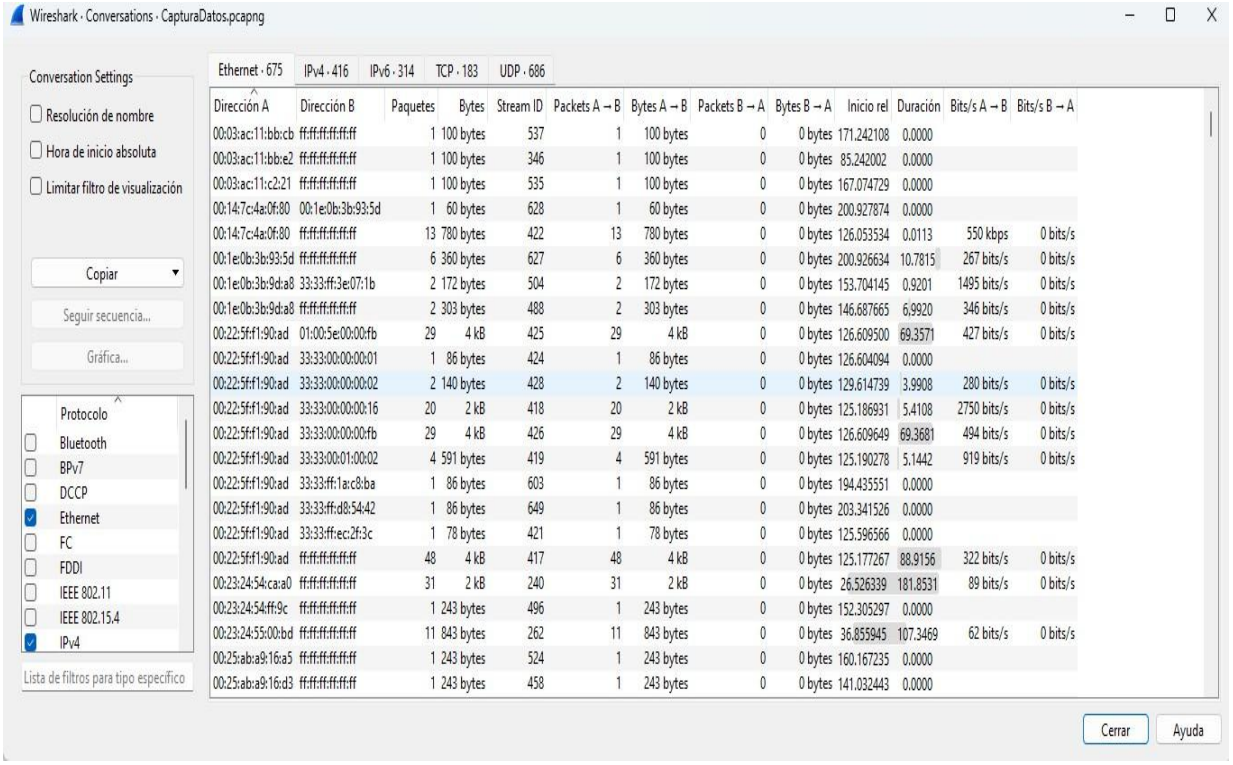
- **Ethernet (100%)**: Todos los paquetes capturados están en la capa de enlace de datos.
- **IPv6 (37.9%) e IPv4 (58.1%)**: La mayoría del tráfico usa estos protocolos de red.
- **UDP (17.3%) y TCP (33.5%)**: Se observa más tráfico UDP que TCP, lo que indica uso de protocolos sin conexión.
- **DNS (0.1%)**: 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:



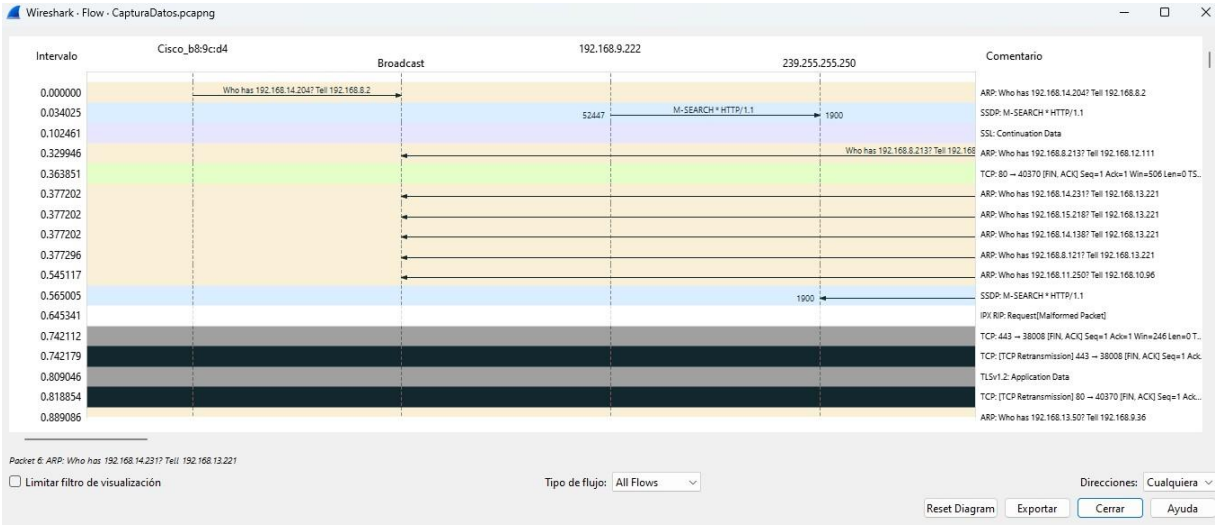
Estadísticas > Conversaciones para ver las conexiones entre direcciones IP y los protocolos utilizados.



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

Conversations Settings

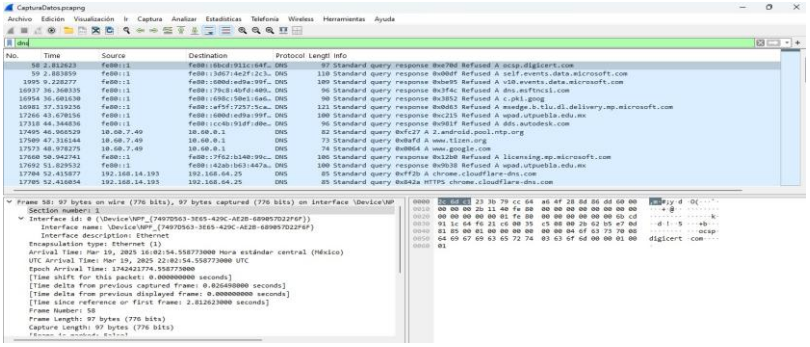
- Resolución de nombre: Si está activado, Wireshark intentará resolver las direcciones IP a nombres de dominio.
- Hora de inicio absoluta: Muestra el tiempo absoluto en lugar del relativo.
- Limitar filtro de visualización: Aplica el filtro actual a las conversaciones.



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

Filtro DNS

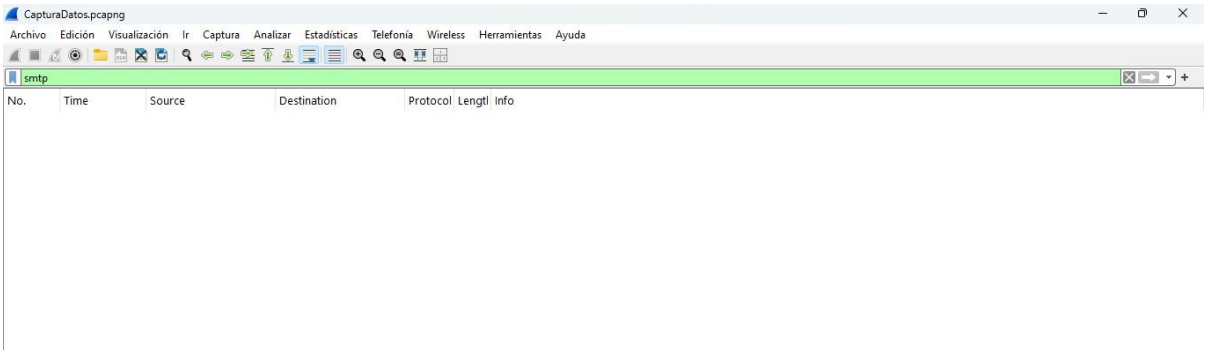
Aplicamos el filtro DNS en la barra de filtros



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.