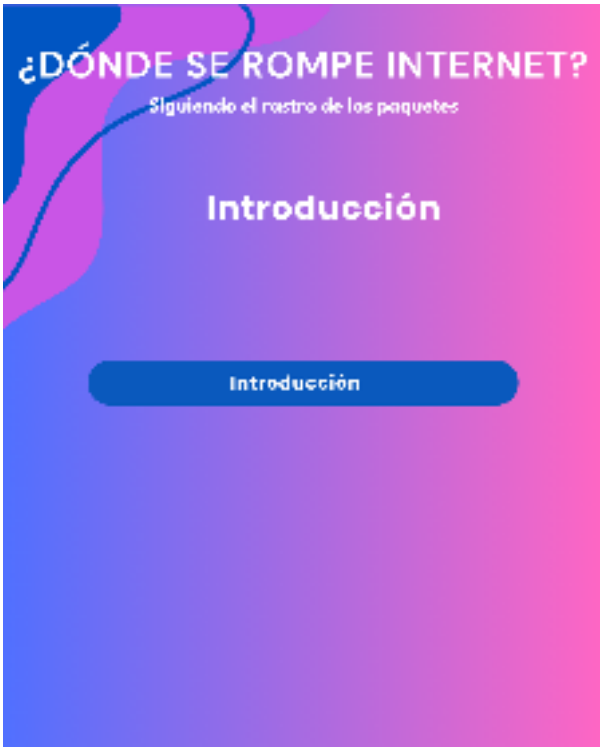


🟣 0 – Introducción

El funcionamiento de Internet suele percibirse como algo simple desde la experiencia del usuario, pero en la práctica involucra múltiples componentes y procesos. Cuando ocurre un problema de conectividad, es común recurrir a soluciones rápidas sin un análisis previo, como reiniciar dispositivos o repetir la acción.

Si bien estas acciones pueden resolver fallas puntuales, no permiten identificar el origen real del problema. Para realizar un diagnóstico adecuado, es necesario comprender cómo funciona una red y qué elementos intervienen en la comunicación.

En este contexto, herramientas como Wireshark permiten analizar el tráfico de red, aunque su uso resulta más efectivo cuando se cuenta con una base conceptual previa, por lo que vamos a iniciar con un pantallazo general sobre qué es una red y cómo funciona.”

🟣 1 – Redes e Internet / ¿Qué es una red?

Una red es un conjunto de dispositivos interconectados que intercambian información con distintos fines, como el acceso a recursos, la comunicación o la transferencia de datos.

Estos dispositivos (computadoras, celulares, impresoras, televisores, etc…) pueden conectarse mediante distintos medios, como cableado UTP, fibra óptica o conexiones inalámbricas. Además, intervienen equipos de red, como routers y switches, que permiten organizar y dirigir el tráfico.

La existencia de una red permite que los dispositivos amplíen sus capacidades al comunicarse entre sí, superando las limitaciones de un sistema aislado.

🟣 2 – ¿Qué es Internet?

Internet es una red de gran escala compuesta por múltiples redes interconectadas a nivel mundial. A diferencia de una red local, que suele estar limitada a un entorno específico, Internet permite la comunicación entre dispositivos ubicados en diferentes regiones del mundo.

Si bien es posible conectarse a otras redes sin acceso a Internet —por ejemplo, en entornos privados que requieren infraestructura propia—, el principio de funcionamiento sigue siendo similar, basado en la interconexión de dispositivos.

Una de las principales diferencias radica en los servicios disponibles, ya que en Internet se accede a plataformas, aplicaciones y contenidos mediante distintos protocolos, siendo la navegación web uno de los más comunes.

🟣 3 – ¿Cómo viaja la información?

La comunicación en una red no se realiza como un bloque único de datos, sino que la información se divide en unidades más pequeñas llamadas paquetes.

Cada paquete contiene tanto una porción del mensaje como información adicional *(que es capturada y usada por Wireshark)* necesaria para su envío, como direcciones de origen y destino . Estos paquetes viajan a través de la red pasando por distintos dispositivos intermedios, como routers, que se encargan de encaminarlos.

Este recorrido no es directo, sino que se realiza en múltiples saltos. Los paquetes pasan por distintos dispositivos de red, como routers, que se encargan de recibirlos y reenviarlos hacia el siguiente punto más adecuado. Estos dispositivos no conocen necesariamente todo el trayecto completo, pero sí saben cómo encaminar el paquete en cada paso, acercándolo a su destino final.


¿Cómo funciona?
• DNS
• conexión TCP
• transferencia HTTP


¿Qué pasa al entrar a una web?
• DNS
• conexión TCP
• transferencia HTTP

🟣 4 – ¿Qué pasa al entrar a una web?

- DNS
- TCP
- HTTP/HTTPS
Cuando un usuario ingresa una dirección web en el navegador, se inicia una serie de procesos que permiten establecer la comunicación con el servidor correspondiente y acceder al contenido solicitado.

Para que esto sea posible, previamente debe existir una configuración de red adecuada que permita la salida hacia Internet, incluyendo parámetros como la dirección IP, la puerta de enlace y los servidores DNS.

En primer lugar, se realiza una consulta al servidor DNS, cuya función es traducir el nombre de dominio ingresado a una dirección IP. Esto es necesario porque los dispositivos en la red se comunican utilizando direcciones numéricas.

Una vez obtenida la dirección IP, se establece una conexión mediante el protocolo TCP, que permite una comunicación confiable entre el cliente y el servidor, asegurando que los datos se transmitan correctamente.

Finalmente, con la conexión establecida, el navegador envía una solicitud al servidor utilizando el protocolo HTTP o HTTPS. El servidor responde con los datos de la página solicitada, y el navegador procesa esa información para mostrar el contenido al usuario.

🟣 5 – Cadena de red

– Dispositivo final (usuarios)
– Red local
– Dispositivos de red
– Internet (ISP y servicios)

El proceso de comunicación en una red involucra múltiples componentes que actúan de manera secuencial y coordinada. La información no viaja de forma directa, sino a través de una estructura amplia que introduce complejidad, pero que al mismo tiempo hace posible la comunicación entre dispositivos.

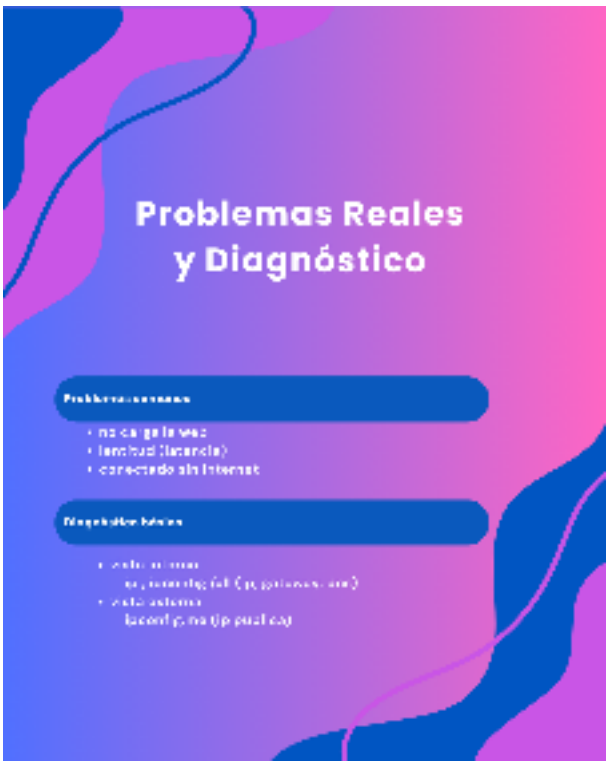
En primer lugar, se encuentra el dispositivo final, como una computadora o un teléfono, desde donde se origina la comunicación. Este depende tanto de su configuración como de su correcto funcionamiento a nivel de hardware y software.

A continuación, interviene la red local, entendida no solo como la conexión lógica entre dispositivos, sino también como la infraestructura física o edilicia que la soporta, incluyendo cableado, puntos de acceso y condiciones del entorno. Problemas en esta capa pueden estar relacionados con interferencias, fallas físicas o limitaciones en la instalación.

Luego participan los dispositivos de red, como routers y switches, que se encargan de dirigir y encaminar la información. Estos equipos pueden presentar fallas de configuración, saturación o limitaciones propias del hardware.

Finalmente, la comunicación alcanza Internet, que puede entenderse tanto como una red global de redes como el conjunto de servicios ofrecidos a través de un proveedor de acceso (ISP). En este nivel, los problemas pueden originarse en la infraestructura del proveedor o en los propios servicios a los que se intenta acceder.

Cada uno de estos componentes cumple un rol necesario dentro del proceso de comunicación, pero también representa un posible punto de falla. Por este motivo, cuando se percibe que “no funciona Internet”, es importante considerar que el problema puede encontrarse en cualquiera de estos niveles y no exclusivamente en el acceso externo.


Problemas Reales
y Diagnóstico


Problemas comunes
y Diagnóstico Básico
• vista interna
• vista externa

🟣 6 – Problemas comunes y Diagnóstico básico

Los problemas de conectividad pueden manifestarse de distintas formas, como la imposibilidad de acceder a una página web, tiempos de respuesta elevados o estados de conexión aparentemente activos pero sin acceso real a Internet. Sin embargo, estas situaciones no tienen una única causa.

Un mismo síntoma puede originarse en distintos puntos: en la red local del usuario, en la salida hacia Internet o incluso en el propio servicio al que se intenta acceder. Por este motivo, resulta fundamental distinguir dónde se encuentra el problema antes de intentar resolverlo.

El diagnóstico inicial puede abordarse a partir de dos perspectivas: una vista interna de la red y una vista externa.

Desde la **vista interna**, herramientas como **ipconfig /all** en Windows o **ip addr** en sistemas Linux permiten verificar la configuración de red del dispositivo. A través de ellas es posible obtener información como la *dirección IP privada*, la puerta de enlace (gateway) y los servidores DNS configurados. Estos datos permiten confirmar si el equipo está correctamente integrado a la red local.

Desde la **vista externa**, es posible utilizar servicios accesibles desde el navegador, como **ifconfig.me**, que permiten conocer la *dirección IP pública* con la que el dispositivo se presenta hacia Internet. Esta dirección no corresponde directamente al equipo, sino que es asignada por el proveedor de Internet y gestionada mediante mecanismos como *NAT*, que permiten que múltiples dispositivos compartan una misma IP pública.

Mientras que las herramientas de vista interna se utilizan directamente desde la computadora, la verificación externa puede realizarse también desde otros dispositivos, como teléfonos móviles. En estos casos, la dirección IP privada puede consultarse en la configuración de la red WiFi, mientras que la IP pública puede observarse mediante el navegador o, en conexiones móviles, a través de la información de estado del sistema.

Este conjunto de verificaciones permite determinar si el problema se encuentra dentro de la red local, en la salida hacia Internet o en un servicio externo, facilitando así un diagnóstico más preciso antes de recurrir a herramientas de análisis más avanzadas.

🟣 7 – Wireshark

Hasta este punto, el análisis se centró en la red desde una perspectiva interna y externa, pero no en la comunicación en sí. Para abordar este aspecto, se utiliza Wireshark.

Wireshark es una herramienta de software libre, ampliamente utilizada a nivel mundial, que permite capturar y analizar el tráfico de red. Es multiplataforma y cuenta con soporte para una gran variedad de protocolos, lo que la convierte en una herramienta versátil dentro del ámbito informático.

Su funcionamiento se basa en la captura de los paquetes que circulan por la red, su representación en un formato legible y la posibilidad de analizarlos en detalle. En este sentido, actúa como un analizador de protocolos de red, permitiendo observar cómo se comunican los dispositivos.

A partir de esta información, es posible interpretar el comportamiento de la red, identificar patrones de comunicación y detectar posibles anomalías o fallas. Debido a su nivel de detalle, Wireshark no solo se utiliza en redes, sino también en áreas como desarrollo, seguridad informática y diagnóstico de sistemas.

🟣 Uso real de Wireshark

Ancho de banda – Errores – Latencia – Malware

El análisis de tráfico mediante Wireshark permite abordar distintos escenarios reales dentro de una red, facilitando la detección y comprensión de problemas.

En el caso del análisis de **ancho de banda**, se captura el tráfico y se lo somete a un análisis estadístico, lo que genera una lista ordenada de las computadoras que más tráfico producen dentro de la muestra capturada.

Para la detección de **errores**, se realiza una captura desde la PC con problemas, se intenta replicar la situación y luego se analizan las cabeceras del tráfico capturado para identificar los paquetes que contienen mensajes de error de conexión.

En situaciones de **latencia**, ya sea en la red o en una PC en particular, se captura tráfico desde el equipo afectado y se analizan los TCP handshake del tráfico capturado. A partir de los tiempos de demora entre paquetes, es posible determinar la existencia de latencia y su origen.

En el caso de **malware** oculto en un nodo de la red, donde un antivirus no detecta actividad sospechosa, se realiza una captura prolongada del tráfico. Posteriormente, se analizan las direcciones IP y los puertos para identificar conexiones sospechosas, como comunicaciones con direcciones de mala reputación. Para este análisis pueden utilizarse herramientas externas como servicios de consulta **WHOIS**. (*https://www.whois.com/whois/*)

🟣 ¿Cuándo utilizar Wireshark?

Optimización – Solución de fallas – Seguridad – Evaluación

Wireshark puede aplicarse en distintos contextos dentro de la informática, dependiendo del objetivo del análisis.

En tareas de **optimización**, permite realizar análisis de causa y efecto para comprender cómo se comunica una aplicación y evaluar posibles mejoras, siendo útil *para desarrolladores y programadores*.

En la **solución de fallas**, se utiliza para identificar errores en servicios que no están funcionando correctamente, especialmente en entornos donde las tareas son críticas. En este caso, resulta una herramienta clave *para soporte técnico y administración de redes*.

En el ámbito de la **seguridad**, permite la detección de amenazas, la realización de pruebas de intrusión y el análisis forense del tráfico de red, siendo utilizada *por especialistas en seguridad informática*.

En procesos de **evaluación**, se emplea para verificar el funcionamiento de desarrollos propios, como aplicaciones o protocolos, asegurando que operen correctamente sobre la red. Esto resulta útil en etapas de *testing o desarrollo*.

Además, Wireshark cumple un **rol didáctic**o, ya que permite observar en detalle conceptos que en la teoría pueden resultar abstractos, como la estructura y composición de un paquete de red.

Como ven, no es solo una herramienta de redes, sirve para muchas áreas de la informática.

🟣***Los siguientes segmentos (conocer Wireshark, caso 1 tráfico típico de navegación web y caso 2 tipos de latencia) se muestran y explican usando el programa y compartiendo pantalla.***

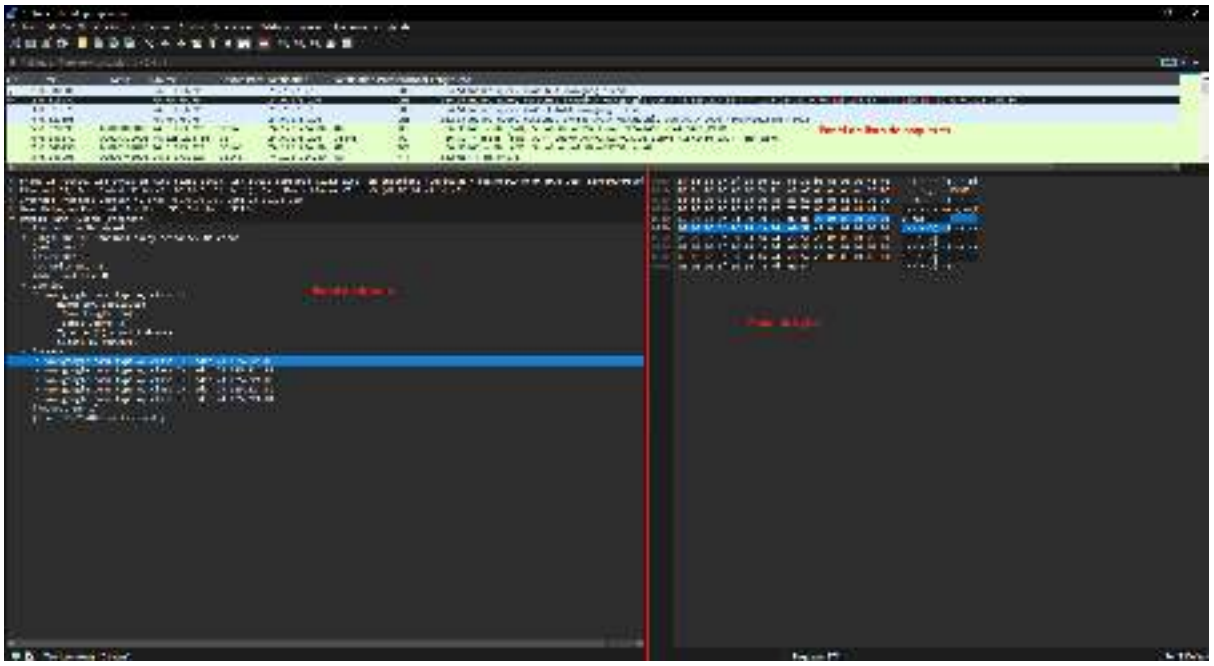
🟣Conocer Wireshark

Se nombran y explican los paneles, además de su personalización y el uso de columnas y filtros para búsqueda y visualización.
panel 1 → panel de lista de paquetes
panel 2 → panel de detalle → metadata (wireshark) e información de cabeceras TCP
panel 3 → panel de bytes → datos sin procesar en Hexadecimal y ASCII

Arrastrar campos a la barra de busqueda aplica filtros automáticos simples (como por ejemplo visualizar solo un tipo de protocolo o de ip destino)
La información que aparece en la cabecera se puede agregar en columnas (como es el caso de TCP Delta) mediante el uso de un menú contextual (click derecho)

🟣Caso 1: Tráfico típico de navegación Web

En la imagen además de estar marcados los paneles, se seleccionó un paquete de DNS, un query response, que responde con las IP de www.google.com (en formato IPv4)



Los primeros 4 paquetes de la captura corresponden al protocolo DNS.
El primero es una solicitud DNS con la IP de tipo IPv4 de la página de google. (un query)
El segundo paquete es la respuesta, un query response con cinco IP.
El tercer y cuarto paquete repiten pero para IPv6 (solo en caso de estar habilitado).
Los siguientes 3 paquetes son de protocolo TCP para establecer la conexión, se establece una comunicación en 3 pasos (3 Way Handshake).
En el quinto paquete se envía un SYN para establecer la conexión.
En el sexto paquete se recibe una respuesta SYN, ACK de confirmación.
El séptimo paquete se envía una confirmación que establece finalmente la comunicación.
Para finalizar tenemos el octavo paquete que es del protocolo de transferencia HTTP, el cual podemos ver que utiliza el puerto 80, y utiliza un GET para solicitar la información que posteriormente será cargada en el navegador.

🟣Caso 2: Tipos de latencia

La **latencia** puede definirse como el tiempo que tarda un dato en viajar desde el origen hasta el destino. En una comunicación de red, este valor puede estimarse midiendo el tiempo entre el envío de un paquete y la recepción de su respuesta dentro de una misma **TCP Stream**.

Un **TCP Stream** representa una comunicación específica entre dos dispositivos dentro del conjunto de todas las conexiones TCP posibles. Analizar estos flujos permite aislar y estudiar el comportamiento de una interacción puntual.

En Wireshark, es posible observar estos tiempos utilizando el campo **TCP Delta**, que se encuentra en los "*timestamps*" de la cabecera TCP. Este valor puede agregarse como columna y representa el tiempo transcurrido respecto del paquete anterior dentro del mismo **TCP Stream**. Para visualizarlo, se selecciona un paquete con protocolo TCP, se accede a la sección *Transmission Control Protocol*, se ubican los *timestamps* y se añade el campo correspondiente como columna.

Origen de Latencia

🔹 Latencia de la recorrido

Una de las formas de analizar la latencia es a través del **RTT (Round Trip Time)**, que representa el tiempo que tarda un paquete en ir desde el origen hasta el destino y recibir una respuesta.

Este valor puede observarse durante el establecimiento de la conexión TCP (three-way handshake), particularmente entre el paquete SYN enviado por el cliente y la respuesta SYN+ACK del servidor. La diferencia de tiempo entre ambos permite estimar el tiempo de recorrido dentro de la red.

En Wireshark, este análisis puede realizarse directamente observando el valor de TCP Delta en el paquete SYN+ACK, sin necesidad de cálculos adicionales.
*Podemos observar en el paquete 6 de la **captura 1***

🔹 Latencia del cliente

Durante una comunicación en curso, la latencia también puede originarse en el cliente (el dispositivo desde donde parte la conexión).

En este caso, el servidor envía datos y el cliente responde con un ACK de confirmación. El tiempo que transcurre entre ese ACK y el siguiente REQUEST puede interpretarse como latencia del cliente. Sin embargo, este retraso no siempre indica un problema técnico, ya que puede deberse al comportamiento del usuario, como el tiempo que tarda en interactuar con el contenido.

Para identificar estos casos en Wireshark, se puede ordenar la columna TCP Delta de mayor a menor y analizar los paquetes HTTP con mayor tiempo asociado.
*Podemos observar en los paquetes paquete 471, 470 y 458 de la **captura 2***

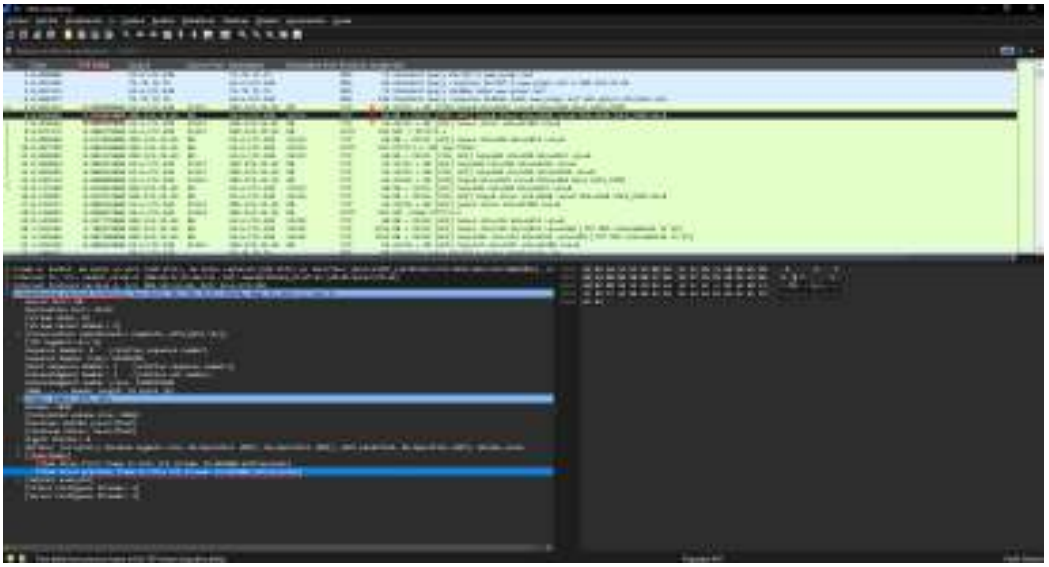
- **Latencia del servidor**

La latencia también puede originarse en el servidor. En este caso, el servidor recibe una solicitud (REQUEST), envía un ACK de confirmación y, luego de un intervalo de tiempo, responde con los datos solicitados.

Si el tiempo entre la confirmación y la respuesta es elevado, se puede inferir latencia del lado del servidor. Esto puede deberse a distintos factores, como alta carga, procesamiento interno o dependencias con otros sistemas.

En Wireshark, este comportamiento puede observarse ordenando los valores de TCP Delta y analizando los paquetes correspondientes a las respuestas del servidor.
*Podemos observar en los paquetes 432 y 20 de la **captura 2***

Captura 1



Captura 2