1. Cargar el PCAP y análisis general del tráfico

¿Cuántos paquetes contiene el PCAP?

6 paquetes

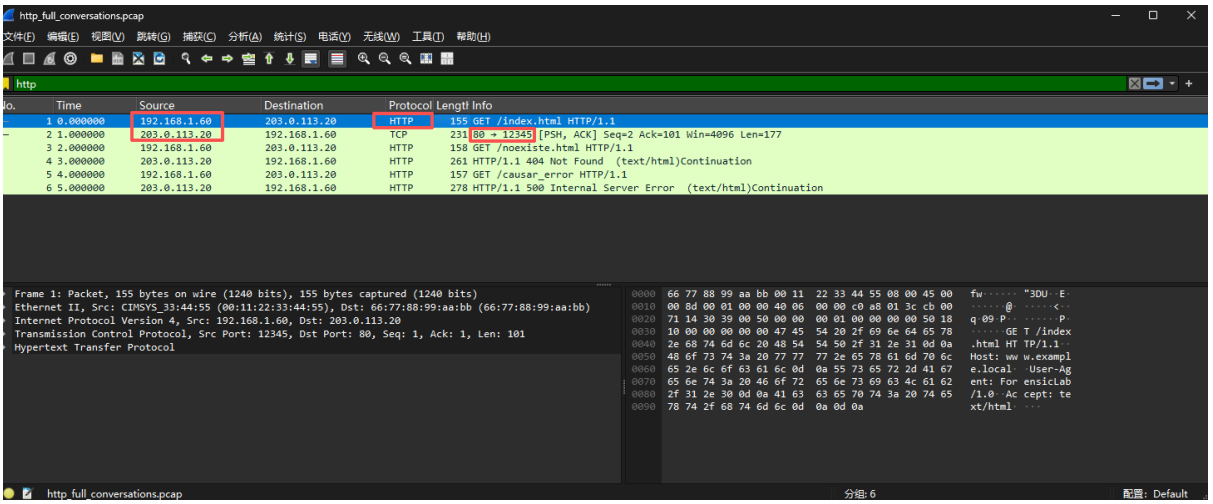
¿Entre qué direcciones IP se produce la comunicación?

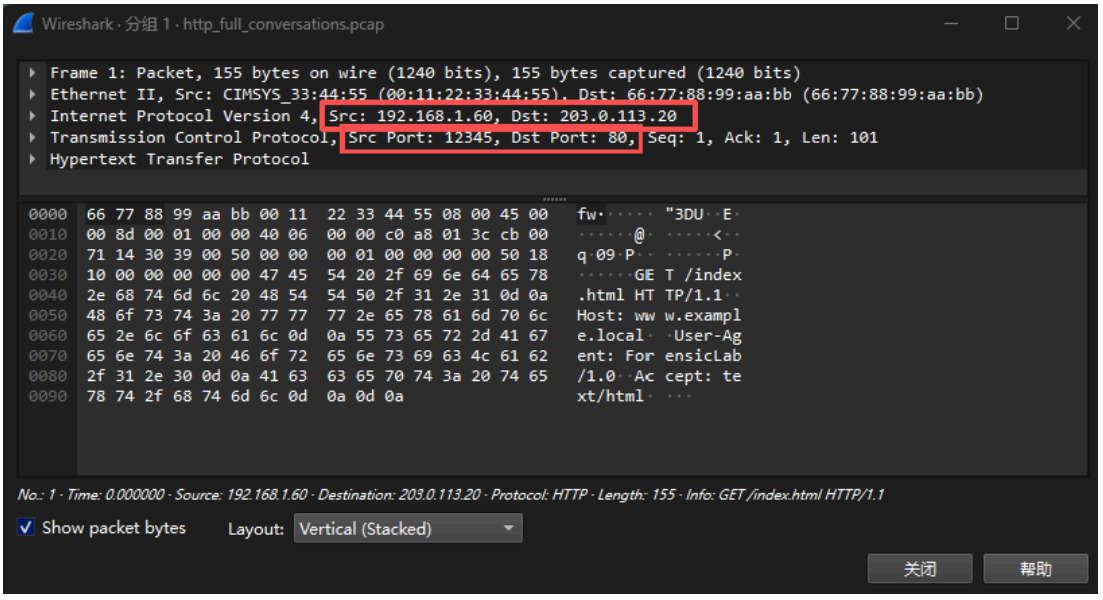
IP del cliente: 192.168.1.60

IP del servidor: 203.0.113.20

Indica también los puertos origen y destino utilizados.

El cliente utiliza el puerto temporal 12345, mientras que el servidor proporciona servicios HTTP a través del puerto 80.





2. Identificar las tres conversaciones HTTP
Indica qué puertos de origen (del cliente) corresponden a cada petición GET.

Las tres sesiones HTTP se originaron en el puerto de origen del cliente 12345.

Asocia cada puerto con el código de respuesta recibido (200, 404 y 500).

El servidor devolvió los siguientes códigos de estado respectivamente:

/index.html → 200 OK

/nonexist → 404 No encontrado

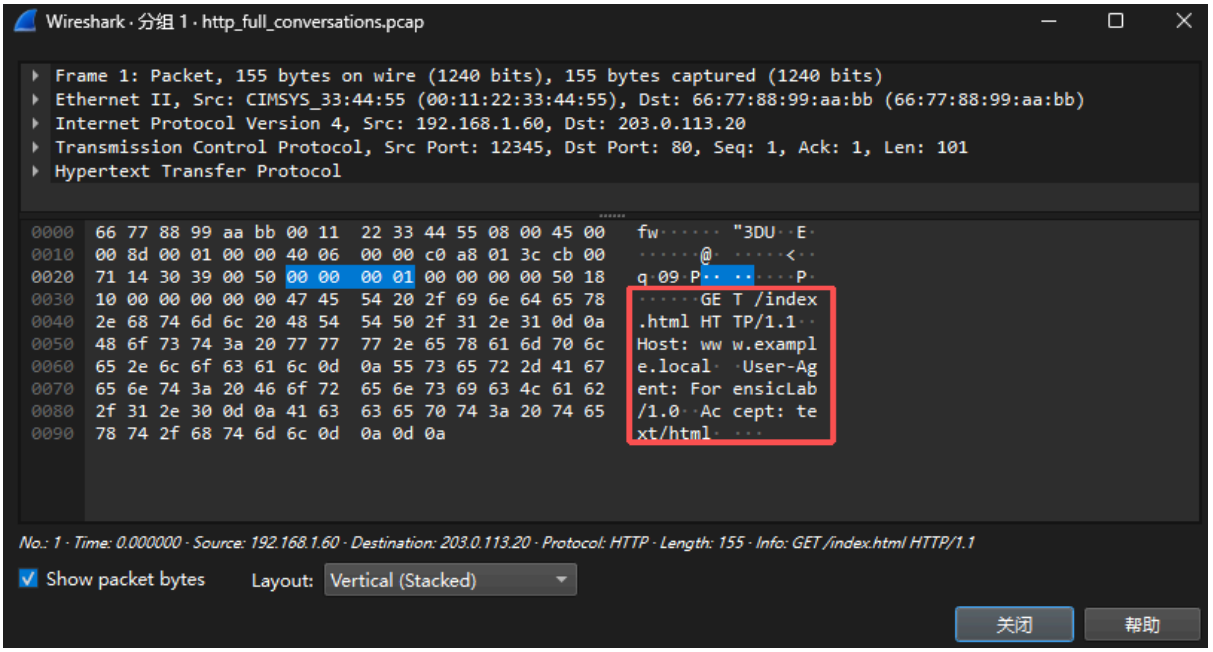
/causar_error → 500 Error interno del servidor

3. Conversación 1 – Respuesta 200 OK
Escribe la URL solicitada en la petición GET (ruta + host).

La URL solicitada por el cliente es: **http://www.example.com/index.html**

¿Qué tipo de contenido (`Content-Type`) devuelve el servidor? ¿El HTML devuelto es completo o parcial?

El servidor devuelve un tipo de contenido text/html, lo que indica que se está devolviendo una página HTML completa en lugar de contenido fragmentado.



4. Conversación 2 – Respuesta 404 Not Found

¿Qué recurso intentaba solicitar el cliente?

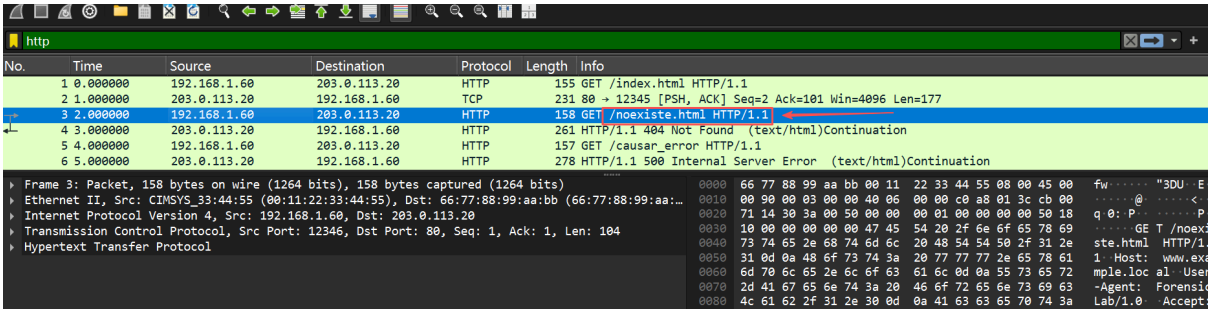
La ruta del recurso solicitada por el cliente es **/nonexist**

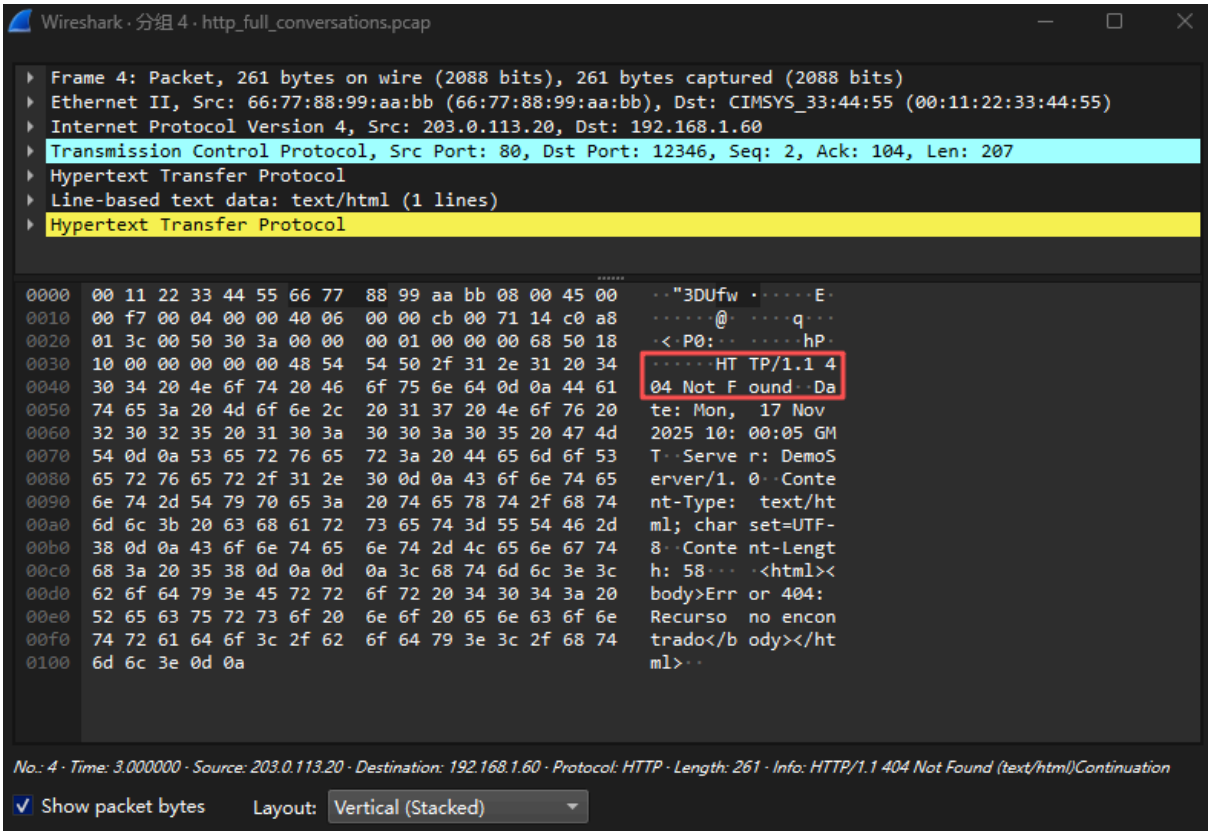
¿Qué mensaje proporciona el servidor al usuario en el cuerpo de la respuesta?

El servidor devuelve el mensaje “Not Found” en el cuerpo de la respuesta

Explica con tus palabras qué significa el código 404.

404 indica que la solicitud llegó al servidor, pero que el recurso solicitado no existe





5. Conversación 3 – Respuesta 500 Internal Server Error

¿Qué ruta intenta acceder el cliente?

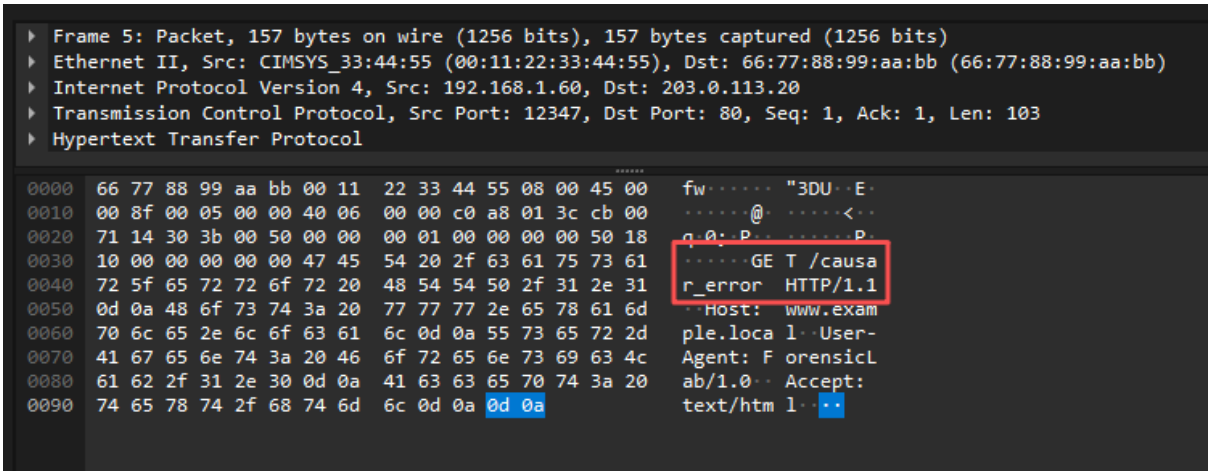
La ruta de acceso del cliente es **/causar_error**

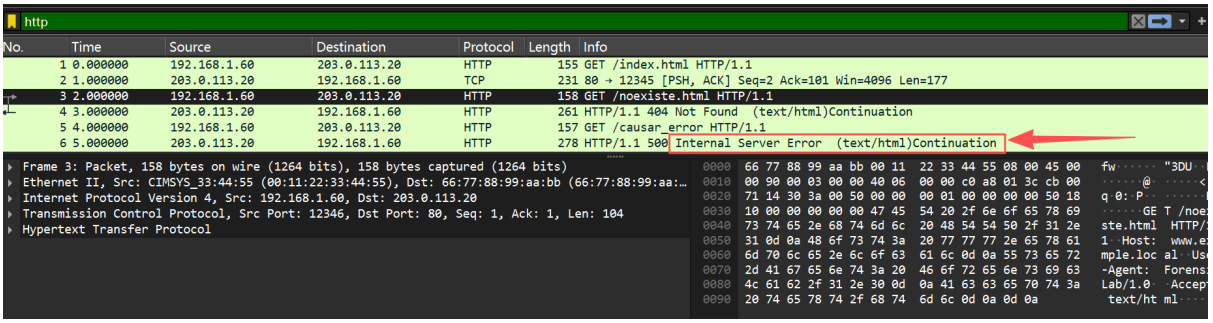
¿Cuál es la causa general de un error **500** en un servidor web?

Un error 500 indica que se ha producido un error interno del servidor durante el procesamiento de la solicitud, posiblemente causado por errores de script, fallos del programa o problemas de configuración del servidor.

Describe qué información se devuelve al cliente en esta respuesta.

El servidor devuelve una página de error que muestra “Internal Server Error”, sin revelar al cliente los detalles específicos del error interno.





6. Análisis técnico del comportamiento del servidor
Comparando las tres respuestas:

¿Cuáles son las diferencias más relevantes entre las cabeceras del servidor para los códigos 200, 404 y 500?
Analiza:

- `Content-Length`

    200 OK: longitud de contenido sustancial, devuelve la página HTML completa.

    404 / 500: longitud de contenido mínima, devuelve solo la página de error.

- `Content-Type`

    Las tres respuestas son text/html, pero la naturaleza del contenido difiere.

- `Date`

    Las tres respuestas incluyen la hora en que el servidor generó la respuesta.

- `Server`

    El campo Servidor es idéntico en las tres respuestas, lo que indica que la solicitud fue procesada por el mismo servidor web.

7. Reflexión final
Explica brevemente cómo puede usar un analista forense tráfico HTTP como este para:

a) Reconstruir la actividad de un usuario en la web.

    Al examinar las URL, la secuencia y las marcas de tiempo de las solicitudes HTTP, se puede reconstruir el comportamiento de navegación de un usuario en una página web

b) Determinar fallos de configuración en un servidor.

    Los errores recurrentes 404 o 500 pueden indicar problemas con la gestión de los recursos del servidor o con los programas de backend

c) Identificar rutas sensibles o errores inesperados.

    Las solicitudes a rutas inexistentes o anómalas (como las que provocan errores 500) pueden reflejar actividades de prueba, escaneo o posibles ataques.