

## 1. Cargar el PCAP y análisis general del tráfico

¿Cuántos paquetes contiene el PCAP?

6 paquetes

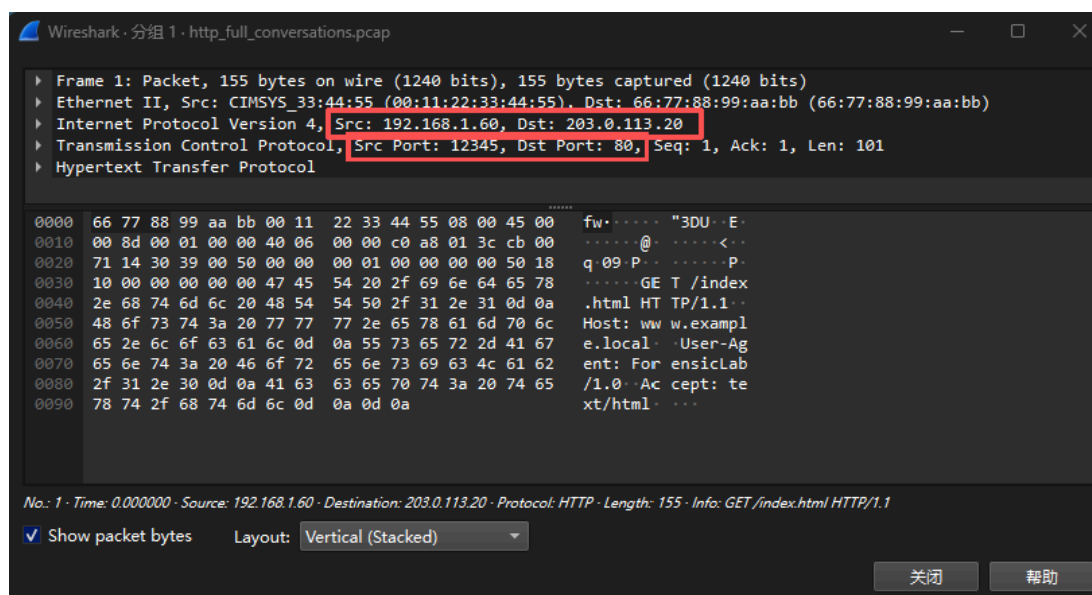
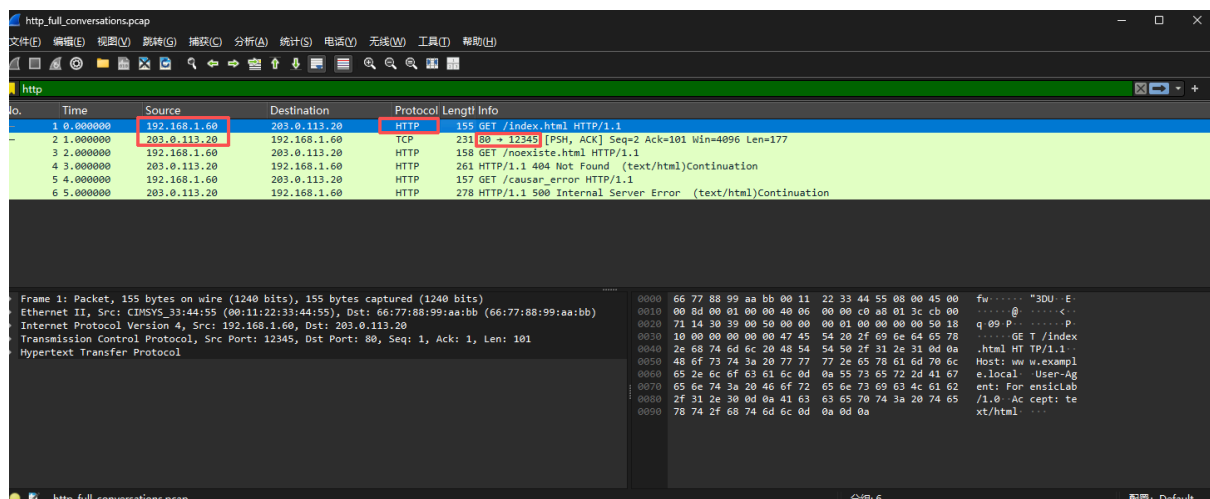
¿Entre qué direcciones IP se produce la comunicación?

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

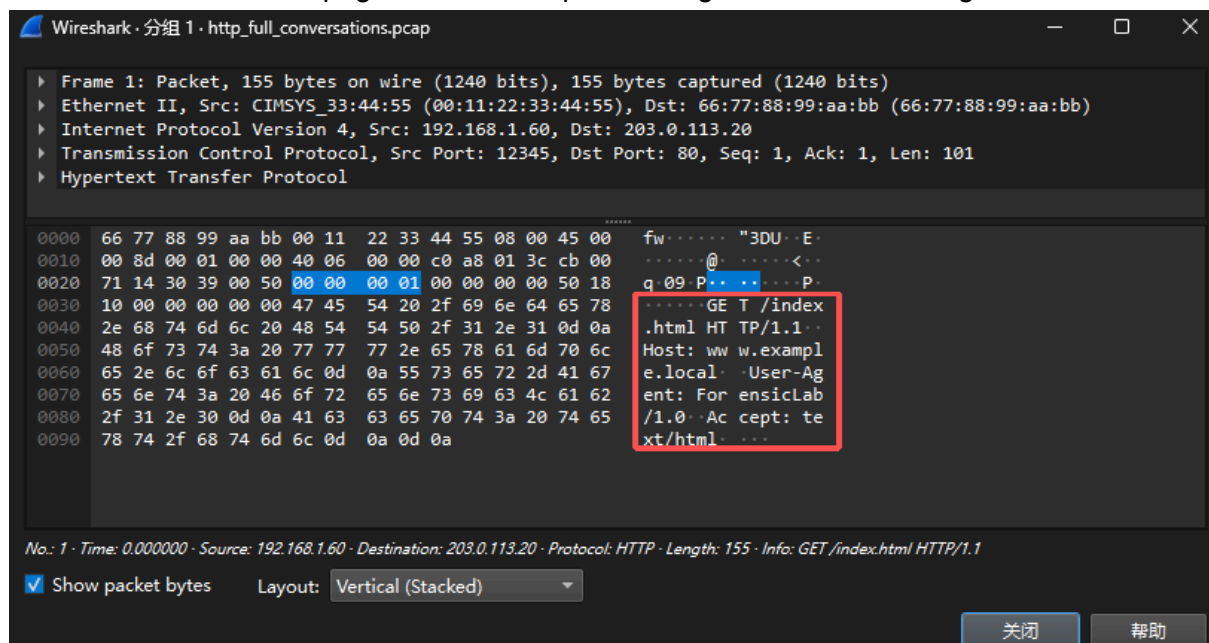
## 3. Conversación 1 – Respuesta 200 OK

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?

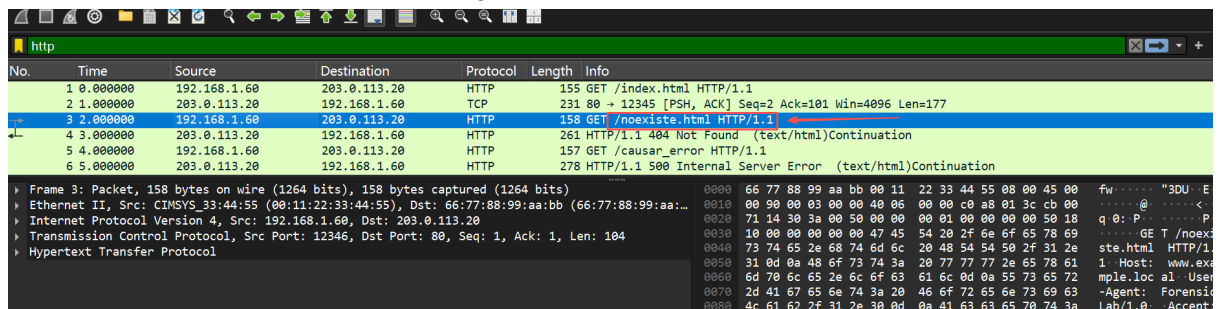
La ruta del recurso solicitada por el cliente es **/nonexist**

¿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

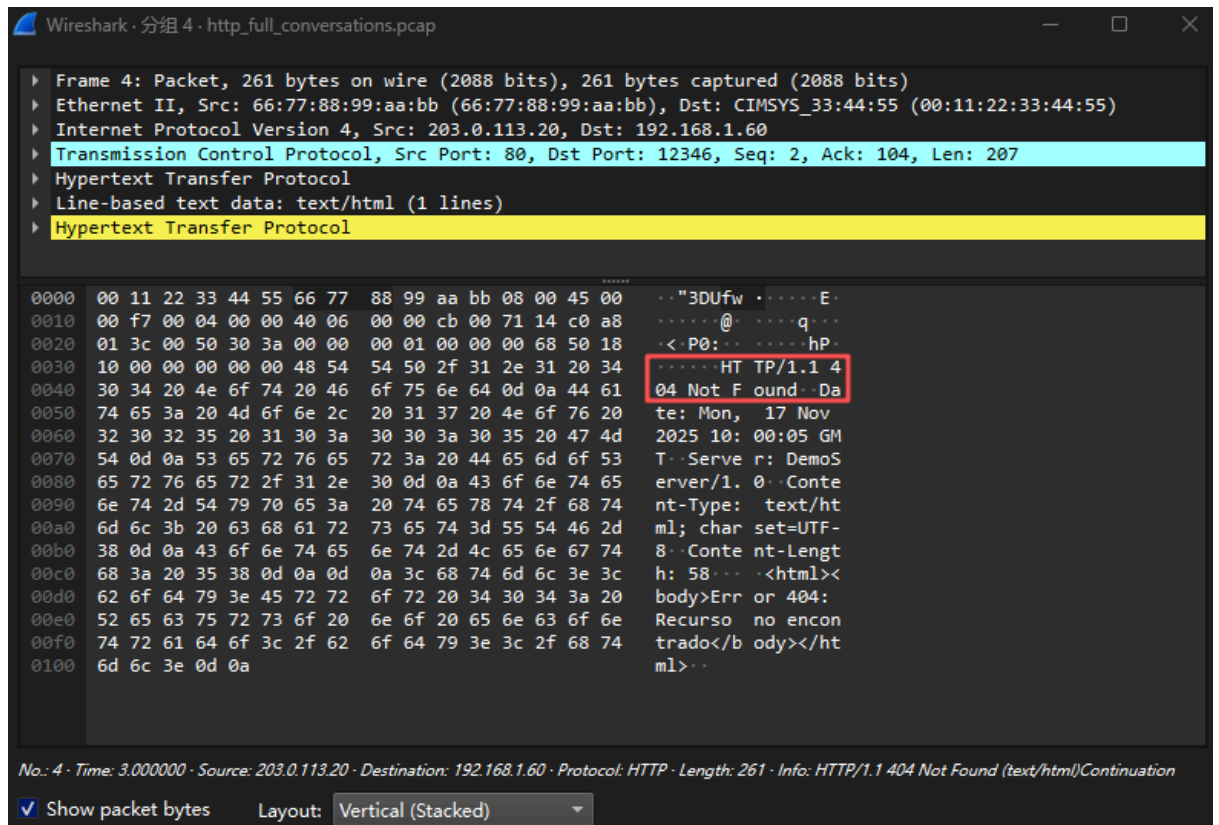
Explica con tus palabras qué significa el código 404.

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



The image shows a Wireshark packet capture of an HTTP conversation. The packet list on the left shows several packets, with packet 3 selected. The packet details pane on the right shows the structure of the selected packet, which is an HTTP GET request for /nonexist.html. The packet bytes pane at the bottom shows the raw data of the packet, including the HTTP status line: 404 Not Found.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.60	203.0.113.20	HTTP	155	GET /index.html HTTP/1.1
2	1.000000	203.0.113.20	192.168.1.60	TCP	231	80 → 12345 [PSH, ACK] Seq=2 Ack=101 Win=4096 Len=177
3	2.000000	192.168.1.60	203.0.113.20	HTTP	158	GET /nonexist.html HTTP/1.1
4	3.000000	203.0.113.20	192.168.1.60	HTTP	261	HTTP/1.1 404 Not Found (text/html)Continuation
5	4.000000	192.168.1.60	203.0.113.20	HTTP	157	GET /causar_error HTTP/1.1
6	5.000000	203.0.113.20	192.168.1.60	HTTP	278	HTTP/1.1 500 Internal Server Error (text/html)Continuation



The image shows a Wireshark packet capture of an HTTP conversation. The packet list on the left shows several packets, with packet 4 selected. The packet details pane on the right shows the structure of the selected packet, which is an HTTP 404 Not Found response. The packet bytes pane at the bottom shows the raw data of the packet, including the HTTP status line: 404 Not Found.

No.	Time	Source	Destination	Protocol	Length	Info
4	3.000000	203.0.113.20	192.168.1.60	HTTP	261	HTTP/1.1 404 Not Found (text/html)Continuation

## 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.

```
▶ Frame 5: Packet, 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits)
▶ Ethernet II, Src: CIMSYS_33:44:55 (00:11:22:33:44:55), Dst: 66:77:88:99:aa:bb (66:77:88:99:aa:bb)
▶ Internet Protocol Version 4, Src: 192.168.1.60, Dst: 203.0.113.20
▶ Transmission Control Protocol, Src Port: 12347, Dst Port: 80, Seq: 1, Ack: 1, Len: 103
▶ Hypertext Transfer Protocol

0000 66 77 88 99 aa bb 00 11 22 33 44 55 08 00 45 00  fw....."3DU..E.
0010 00 8f 00 05 00 00 40 06 00 00 c0 a8 01 3c cb 00  .....@.....<..
0020 71 14 30 3b 00 50 00 00 00 01 00 00 00 50 18  q 0: P.....P.
0030 10 00 00 00 00 00 47 45 54 20 2f 63 61 75 73 61  .....GE T /causa
0040 72 5f 65 72 72 6f 72 20 48 54 54 50 2f 31 2e 31  r_error HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 65 78 61 6d  ..Host: www.exam
0060 70 6c 65 2e 6c 6f 63 61 6c 0d 0a 55 73 65 72 2d  ple.local l..User-
0070 41 67 65 6e 74 3a 20 46 6f 72 65 6e 73 69 63 4c  Agent: F orensicl
0080 61 62 2f 31 2e 30 0d 0a 41 63 63 65 70 74 3a 20  ab/1.0 ..Accept:
0090 74 65 78 74 2f 68 74 6d 6c 0d 0a 0d 0a          text/htm l..
```

http						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.60	203.0.113.20	HTTP	155	GET /index.html HTTP/1.1
2	1.000000	203.0.113.20	192.168.1.60	TCP	231	80 → 12345 [PSH, ACK] Seq=2 Ack=101 Win=4096 Len=177
3	2.000000	192.168.1.60	203.0.113.20	HTTP	158	GET /noexiste.html HTTP/1.1
4	3.000000	203.0.113.20	192.168.1.60	HTTP	261	HTTP/1.1 404 Not Found (text/html)Continuation
5	4.000000	192.168.1.60	203.0.113.20	HTTP	157	GET /causar_error HTTP/1.1
6	5.000000	203.0.113.20	192.168.1.60	HTTP	278	HTTP/1.1 500 Internal Server Error (text/html)Continuation

```
▶ Frame 3: Packet, 158 bytes on wire (1264 bits), 158 bytes captured (1264 bits)
▶ Ethernet II, Src: CIMSYS_33:44:55 (00:11:22:33:44:55), Dst: 66:77:88:99:aa:bb (66:77:88:99:aa:bb)
▶ Internet Protocol Version 4, Src: 192.168.1.60, Dst: 203.0.113.20
▶ Transmission Control Protocol, Src Port: 12346, Dst Port: 80, Seq: 1, Ack: 1, Len: 104
▶ Hypertext Transfer Protocol

0000 66 77 88 99 aa bb 00 11 22 33 44 55 08 00 45 00  fw....."3DU..E.
0010 00 90 00 03 00 00 40 06 00 00 c0 a8 01 3c cb 00  .....@.....<..
0020 71 14 30 3a 00 50 00 00 00 01 00 00 00 50 18  q 0: P.....P.
0030 10 00 00 00 00 00 47 45 54 20 2f 6e 6f 65 78 69  .....GE T /noe
0040 73 74 65 2e 68 74 6d 6c 20 48 54 54 50 2f 31 2e  ste.html HTTP/
0050 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 65 78 61  1..Host: www.e
0060 6d 70 6c 65 2e 6c 6f 63 61 6c 0d 0a 55 73 65 72  mple.local l..Us
0070 2d 41 67 65 6e 74 3a 20 46 6f 72 65 6e 73 69 63  -Agent: Forns
0080 4c 61 62 2f 31 2e 30 0d 0a 41 63 63 65 70 74 3a  Lab/1.0 ..Accep
0090 20 74 65 78 74 2f 68 74 6d 6c 0d 0a 0d 0a          text/ht ml..
```

## 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.