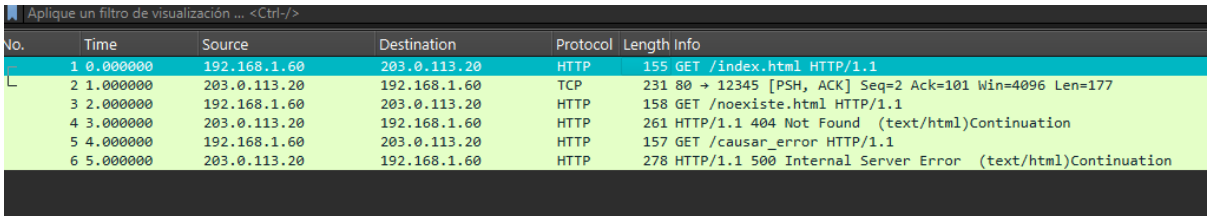
1 - [Análisis Forense] - TRÁFICO HTTP

En este ejercicio analizarás un archivo de captura de tráfico (PCAP) que contiene **tres conversaciones HTTP completas** entre un cliente y un servidor. Cada conversación incluye:

Archivo PCAP

http_full_conversations.pcapDownload http_full_conversations.pcap



- Una **petición GET** realizada por un cliente.
- Una **respuesta HTTP** enviada por el servidor, con tres códigos distintos:
- 200 OK**
- 404 Not Found*
- 500 Internal Server Error**

Tu objetivo es examinar cada conversación y comprender el flujo de petición/respuesta, el significado de los códigos de estado y la estructura de las cabeceras HTTP.

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

Abre el archivo `http_full_conversations.pcap` en Wireshark.

****Pregunta 1:****
¿Cuántos paquetes contiene el PCAP?

6 paquetes

¿Entre qué direcciones IP se produce la comunicación?

Entre la 192.168.1.60 y la 203.0.113.20

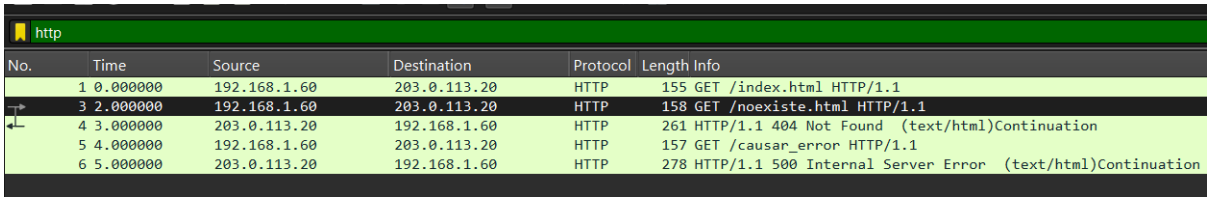
Indica también los puertos origen y destino utilizados.

--- **El puerto de origen es el source port y el de destino es el destination port.**

Son los puertos 80 y 12346 dependiendo si es la peticion o respuesta de un lado o de otro.

2. Identificar las tres conversaciones HTTP

Usa filtros en Wireshark para identificar cada conversación.



****Pregunta 2:****
Indica qué puertos de origen (del cliente) corresponden a cada petición GET.

Puertos 12347, 12346,12345

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

- **Conversación 1 (200 OK):**
  Petición GET: `/index.html`
  Puerto origen del cliente: `80 > 12345` (según la imagen)
  Código respuesta: `200 OK`
- **Conversación 2 (404 Not Found):**
  Petición GET: `/noexiste.html`
  Puerto origen del cliente: se mantiene el mismo ejemplo `80 > 12345` o un puerto efímero diferente según la captura real
  Código respuesta: `404 Not Found`
- **Conversación 3 (500 Internal Server Error):**
  Petición GET: `/causar_error`
  Puerto origen del cliente: de nuevo un puerto efímero
  Código respuesta: `500 Internal Server Error`

---

3. Conversación 1 – Respuesta 200 OK

Selecciona el paquete con la respuesta **HTTP/1.1 200 OK**.

Pregunta 3:
Escribe la URL solicitada en la petición GET (ruta + host).

……GET /index

.html HTTP/1.1..

Host: www.example.local..User-Agent: ForensicLab

/1.0..Accept: text/html….

¿Qué tipo de contenido (`Content-Type`) devuelve el servidor?

text/html

¿El HTML devuelto es completo o parcial?

es completo

---

4. Conversación 2 – Respuesta 404 Not Found

Analiza ahora la segunda petición y su respuesta.

Pregunta 4:
¿Qué recurso intentaba solicitar el cliente?

/noexiste.html

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

HTTP/1.1 404 Not Found\r\n

Line-based text data: text/html (1 lines)

Hypertext Transfer Protocol

Excess data after a body (not a new request/response), previous Content-Length bogus?

Explica con tus palabras qué significa el código 404.

El servidor no pudo encontrar el recurso solicitado. El cliente realizó la petición correctamente, pero el recurso no existe en el servidor.

---

5. Conversación 3 – Respuesta 500 Internal Server Error

Observa la tercera conversación.

****Pregunta 5:****
¿Qué ruta intenta acceder el cliente?

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

El servidor encontró un error interno al procesar la petición (problema en código, configuración o servicio interno).

Describe qué información se devuelve al cliente en esta respuesta.

HTTP/1.1 500 Internal Server Error\r\n

<html><body>Error 500: Falla interna del servidor</body></html>

---

6. Análisis técnico del comportamiento del servidor

Comparando las tres respuestas:

****Pregunta 6:****
¿Cuáles son las diferencias más relevantes entre las cabeceras del servidor para los códigos 200, 404 y 500?
Analiza:

- `Content-Length`

- `Content-Type`

- `Date`

- `Server`

Cabecera	200 OK	404 Not Found	500 Internal Server Error

Content-Length	177 (ejemplo en imagen)	261	278
Content-Type	text/html	text/html	text/html
Date	Fecha de la respuesta	Fecha de la respuesta	Fecha de la respuesta
Server	Nombre del servidor web	Nombre del servidor	Nombre del servidor

---

7. Reflexión final

****Pregunta 7:****
Explica brevemente cómo puede usar un analista forense tráfico HTTP como este para:

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

Viendo las URLs solicitadas, tiempos y patrones de navegación.

b) Determinar fallos de configuración en un servidor.

Identificando respuestas 404 o 500 y analizando cabeceras y rutas que generan errores.

c) Identificar rutas sensibles o errores inesperados.

Encontrando recursos que no deberían existir, errores internos o información filtrada por el servidor.