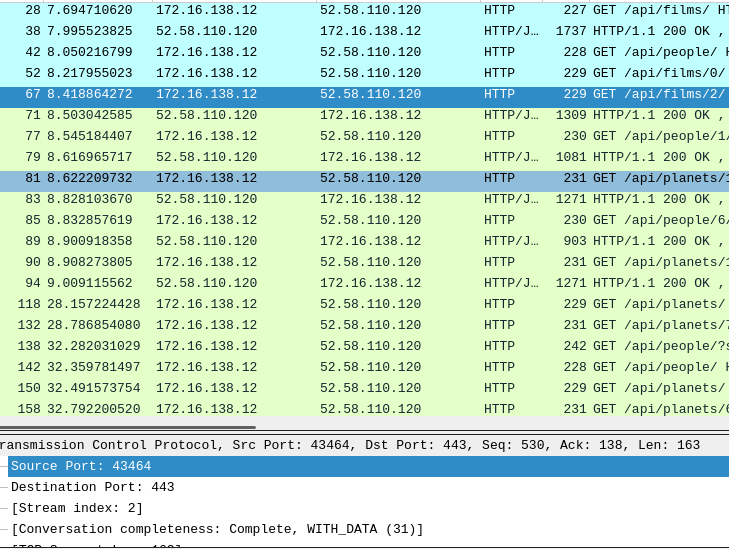
## Práctica Bloque III

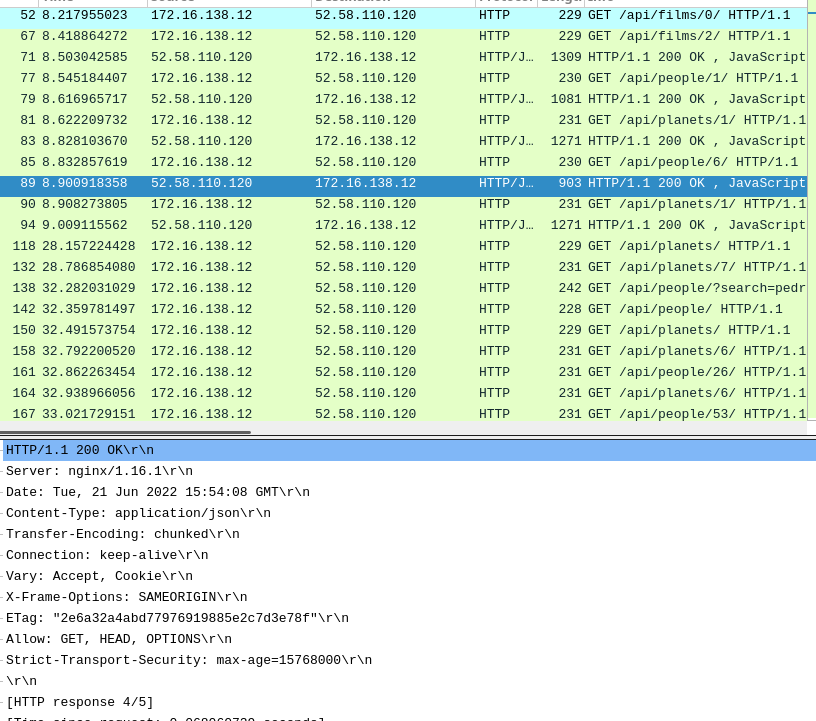
1. **Alumno 1:** Cano Moreno, Francisco Javier
2. **Titulación:** Grado de Ingeniería de Computadores
3. **PC de la práctica:** -
4. **Ejercicio 1.** ¿Cuál es el puerto utilizado por el servidor? ¿Es el normal de HTTP (80)? ¿Por qué?

* Tramas analizadas: 67.
* Utiliza el puerto número 443. En este caso, el puerto utilizado es el típico utilizado por HTTPS, no por HTTP.



1. **Ejercicio 2.** Observe el número de conexiones realizadas. ¿Cuántas hace? ¿Usa una conexión permanente (en la misma conexión hace varias peticiones) o no permanente (solo realiza una por conexión)? En caso de ser permanente, ¿qué cabecera de la petición indica que queremos que sea permanente?

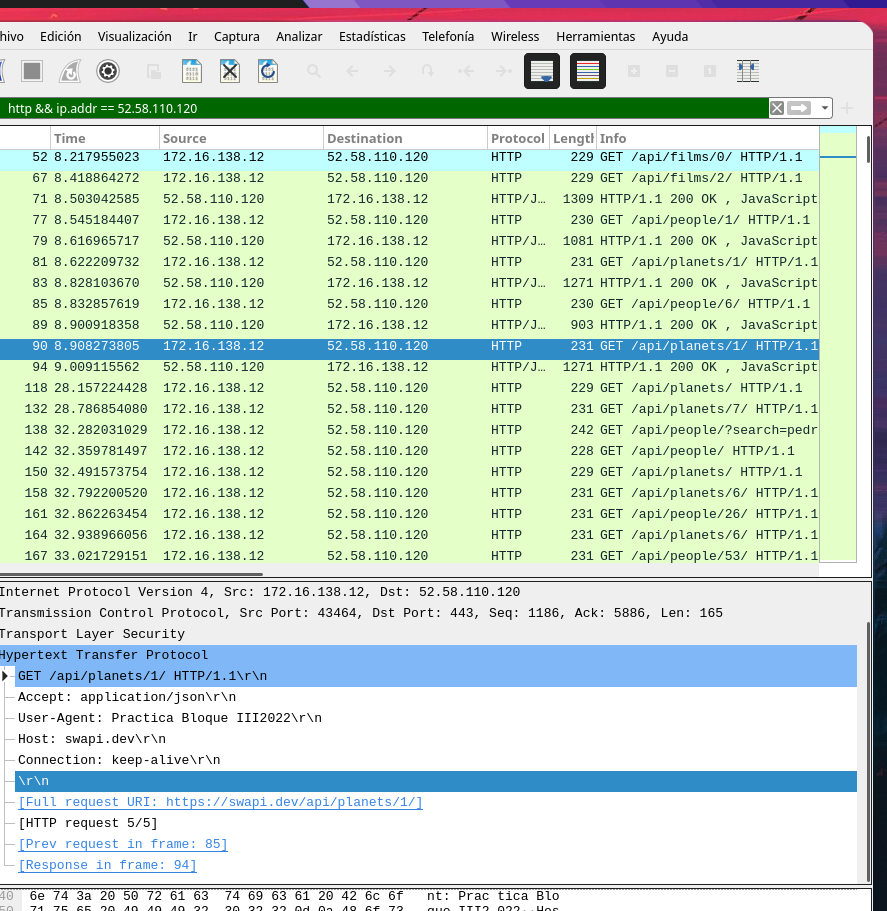
* Tramas analizadas: 83, 85, 89



* Se realiza una única conexión, la cual es permanente y viene indicada en el campo “Connection” dentro de HTTP: keep-alive\r\n.

1. **Ejercicio 3.** Observe una respuesta, ¿cómo se identifica dónde acaban las cabeceras HTTP y empieza el recurso?

* Tramas analizadas: 90
* La cabecera HTTP termina con \r\n.



1. **Ejercicio 4.** Describa el significado de las cabeceras de una petición y una respuesta (sin incluir las que empiecen por X-).

* Tramas analizadas: 118

-User-Agent: Envía los datos del cliente al servidor.

-Acept: Tipo de datos que se envía al cliente.

-Host: Aporta la información del servidor.

-Connection: Aporta información sobre la conexión entre cliente y servidor.

-Strict-Transport-Security: Se encarga de emplear HTTPS en la comunicación.

-Allow: Indica qué métodos HTTP son válidos.

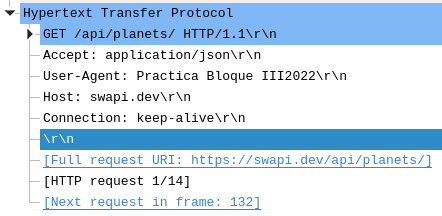
-Etag: identificador de la versión de un recurso de una URL.

-Vary: Indica cómo se emparejan las cabeceras de las siguientes peticiones.

-Transfer-Encoding: Codificación de transferencia.

-Content-type: Tipo del contenido.

* -Server y date nos dan información del servidor y de la fecha y hora del mensaje que se envía.



**————————————————————————————————————————————————**

**Ejercicio 5.** Filtre por el protocolo rtsp y use la opción **Follow TCP Stream** de Wireshark para observar el diálogo completo que han mantenido el cliente de correo y el servidor. Explique brevemente (una línea) el significado de cada comando enviado por el cliente (si algún comando se repite solo debe explicarlo una vez).

* Tramas analizadas:

**Ejercicio 6.** ¿Por qué se hacen dos comandos SETUP? ¿Cómo sabía que debía hacer dos comandos de ese estilo?

* Tramas analizadas:

**Ejercicio 7.** ¿Qué comandos ha provocado adelantar la reproducción del vídeo? ¿Cómo indica por donde debe seguir la reproducción tras el cambio?

* Tramas analizadas:

**Ejercicio 8.** Si observa los comandos y las respuestas son muy similares a las que usa HTTP. Indique dos cabeceras que use RTSP que también se usen en HTTP e indique (y explique) dos cabeceras de RTSP que no se usen en HTTP.

* Tramas analizadas:

**Ejercicio 9.** Ahora filtre por el protocolo rtp que se utiliza para transmitir el recurso multimedia tal cual. ¿Cómo se decidieron los puertos a utilizar en estas comunicaciones RTP? ¿Se confirman de alguna forma cada uno de los envíos RTP?

* Tramas analizadas:

**Ejercicio 10.** Finalmente filtre por el protocolo rtcp usado para controlar el estado de la conexión. Observe alguna trama que sea *Receiver Report*. Despliegue esa cabecera y marque (y explique) dos valores reportados que nos aporten información para poder ajustar la reproducción de acuerdo a las características de la comunicación.

* Tramas analizadas: