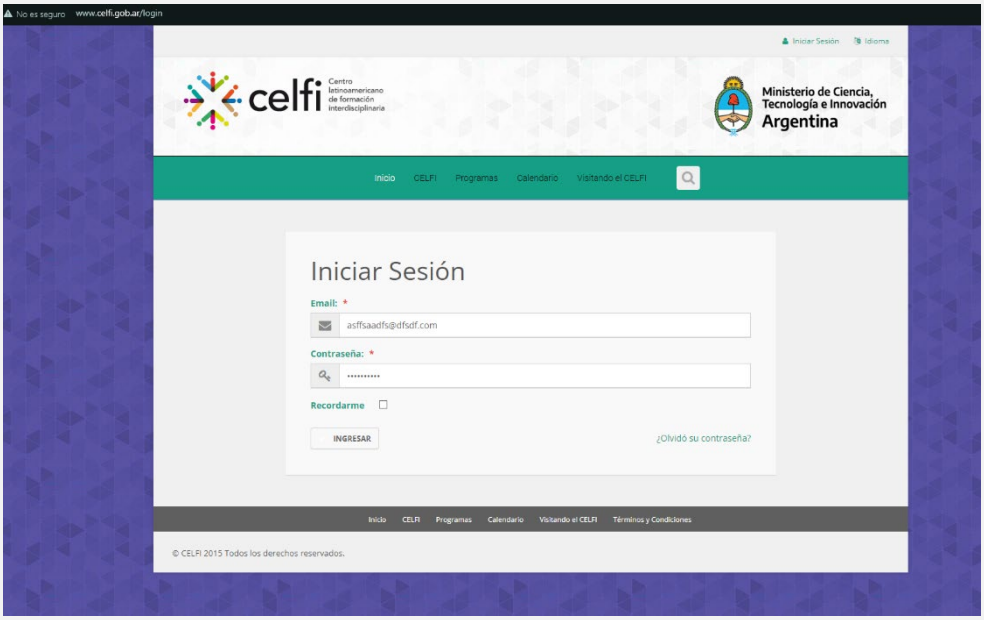
ANÁLISIS DE RED CON WIRESHARK Y NMAP

SEGURIDAD INFORMÁTICA

JUAN CARLOS NAVIDAD GARCÍA

1. Creación del paquete:

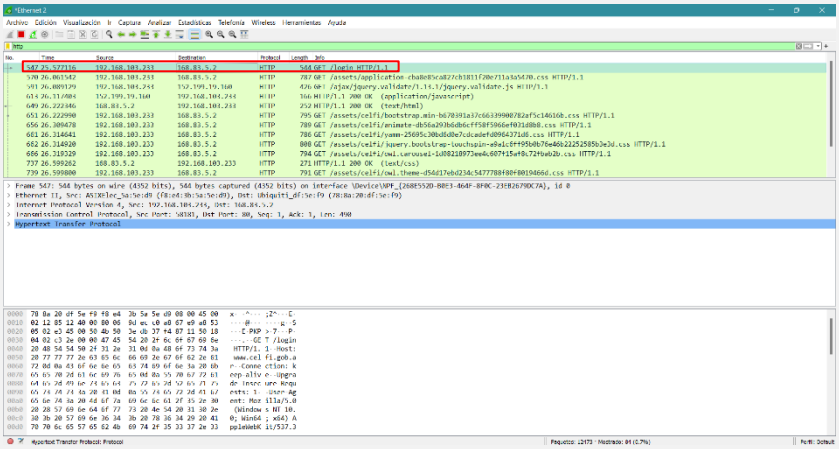
Lo primero que haremos será navegar por internet y realizar una solicitud de inicio de sesión sobre una página sin protección HTTP, de esta manera podremos ver toda la información del paquete que se crea en la red al intentar iniciar sesión en una página:



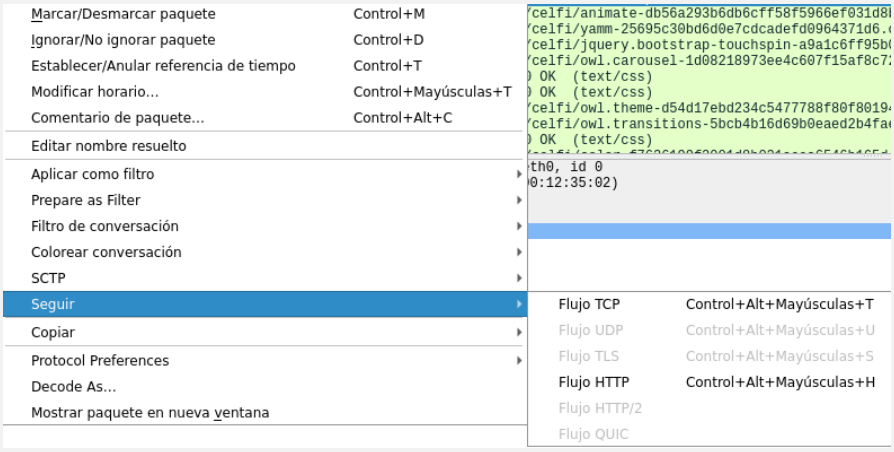
2. Comprobación con Wireshark:

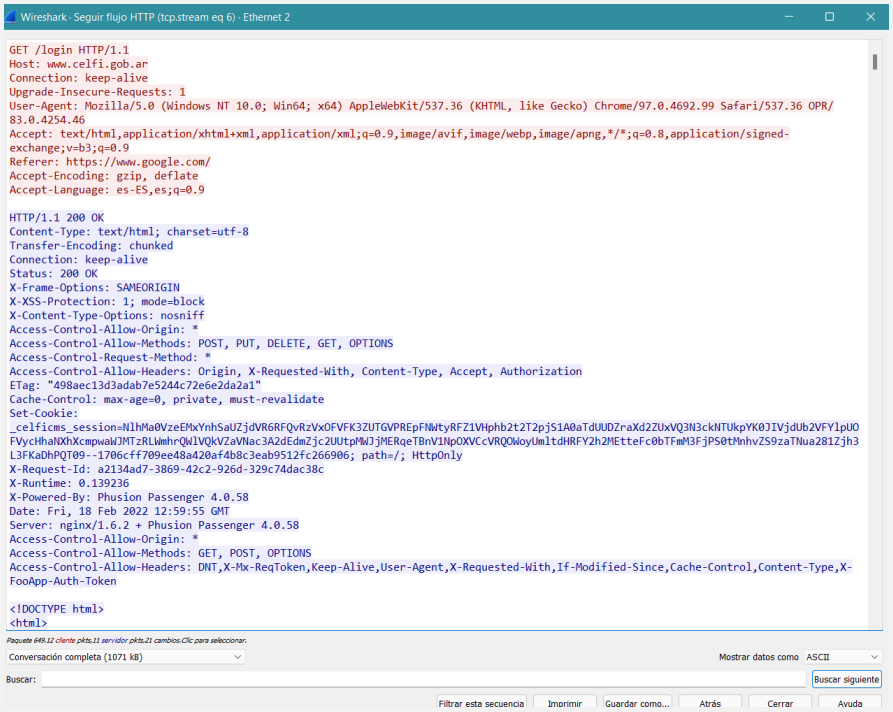
Ahora lo que haremos será abrir Wireshark para poder comprobar si se ha registrado el paquete. Para poder capturar el tráfico en la red, deberemos de iniciar Wireshark como administrador y seleccionar la tarjeta de red con la que estamos conectados.

Como el paquete que queremos ver es sobre una página HTTP, aplicaremos el primer filtro de búsqueda como HTTP:



Si queremos saber más acerca del paquete y de la web donde se ha iniciado sesión, haremos click derecho sobre el paquete → Seguir → Flujo HTTP:

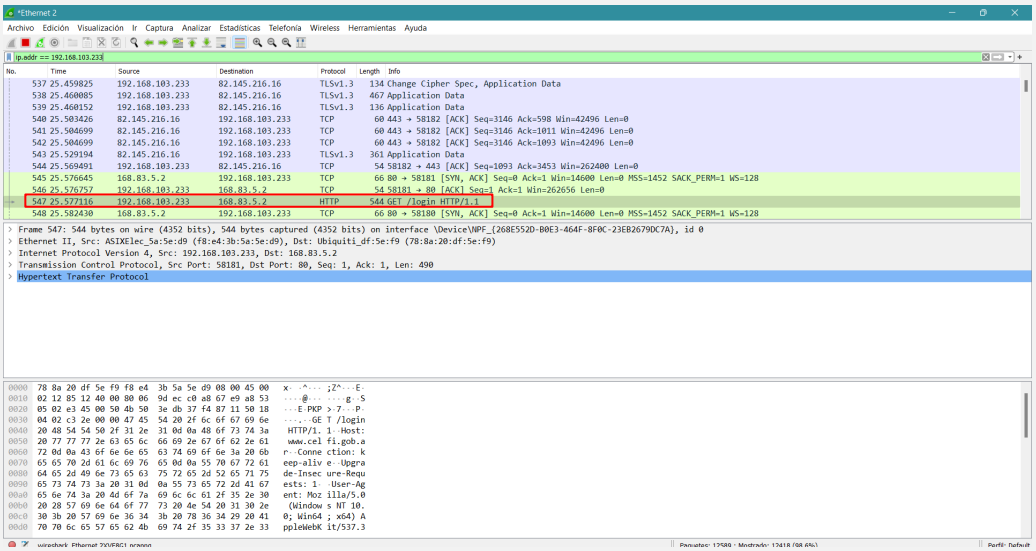




También podemos buscar por dirección IP, le aplicaremos el filtro de búsqueda:

- ip.addr == <IP>

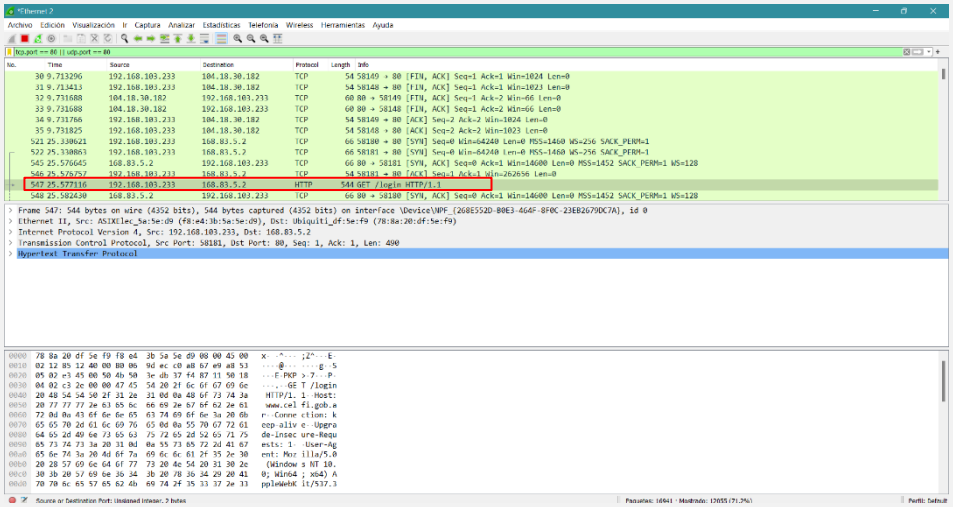
He buscado la misma IP con la que he realizado el inicio de sesión con la página HTTP, nos damos cuenta de que también aparece el paquete anterior:



Entre otros filtros de búsqueda, también podemos filtrar por puertos con:

- tcp/udp.port == <puerto>

En mi caso he filtrado el puerto 80 que es el puerto HTTP para volver a encontrar el paquete de inicio de sesión anterior:



3. Comprobación con Nmap:

Lo que vamos a hacer con Nmap es ver si una página está activa y los puertos que tiene abiertos y funcionando, para eso hay dos comandos:

- nmap -sV <dominio/ip>
- nmap -Pn <dominio/ip>

Primero lo comprobaré con la misma página de Los Cerros y después con la que hemos iniciado sesión anteriormente con el protocolo HTTP: