

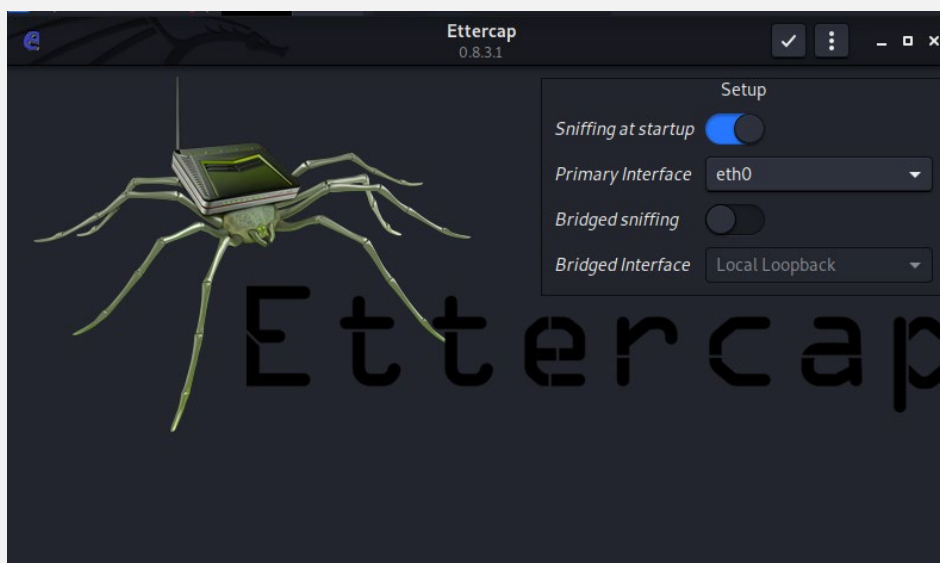
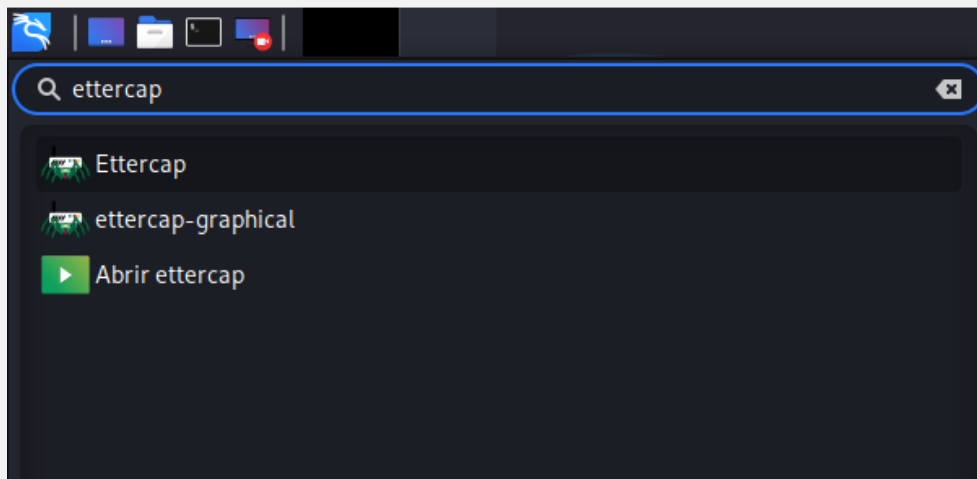
ATAQUE MAN IN THE MIDDLE MEDIANTE ARP



SEGURIDAD INFORMÁTICA
JUAN CARLOS NAVIDAD GARCÍA

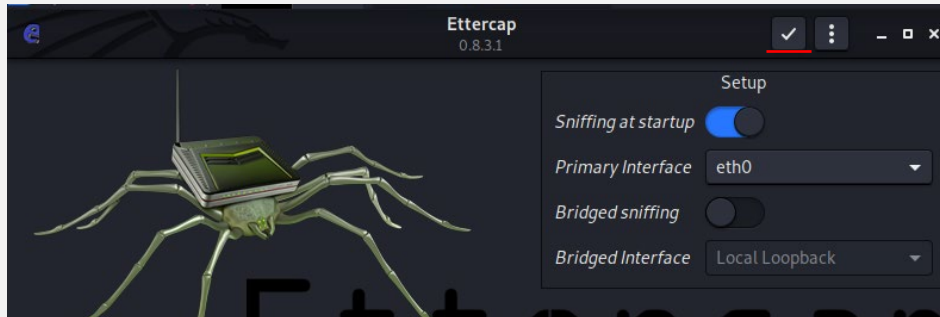
1. Abrir Ettercap:

Para abrir **Ettercap**, buscaremos desde el menú de Kali **Ettercap**:



2. Iniciar Ettercap:

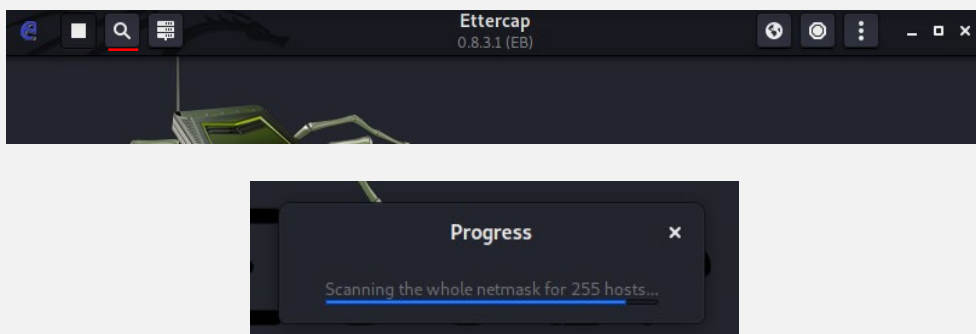
Para iniciar **Ettercap** le daremos al **tick** que aparece en la parte superior derecha:



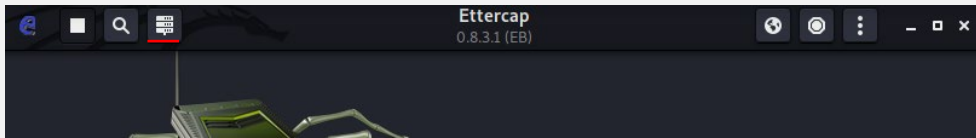
3. Buscar las direcciones en la red:

Necesitaremos **escanear la red** para seleccionar las **direcciones IP** de las que vamos a examinar el tráfico para sacar el **usuario** y **contraseña** de la página **HTTP**.

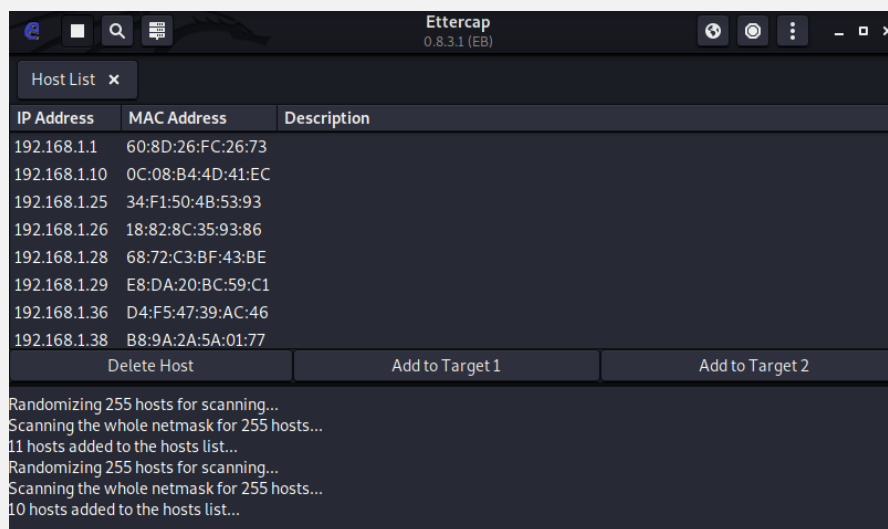
Le daremos a la **lupa** que hay en la parte superior izquierda para **escanear la red**:



Después le daremos al icono que hay justo al lado de la lupa para que nos liste los hosts encontrados:

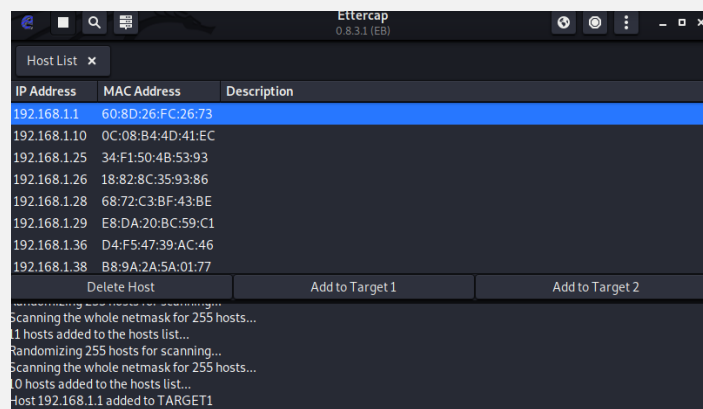


Ahora nos listará todos las **IPs** que hay en la red:

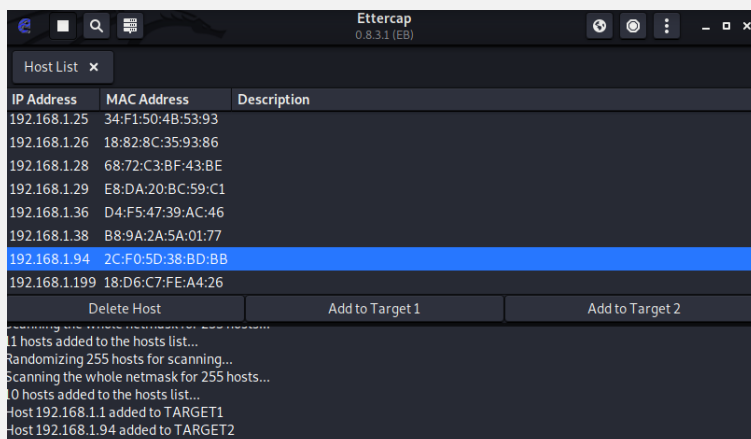


4. Seleccionar las direcciones que vamos a utilizar para examinar el tráfico:

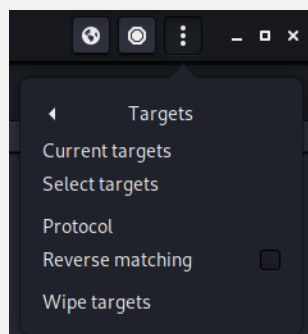
La **primera dirección** que escogeremos será la del **router (Puerta de enlace)**, la terminada en **.1** y le clicaremos sobre **Add Target 1**:



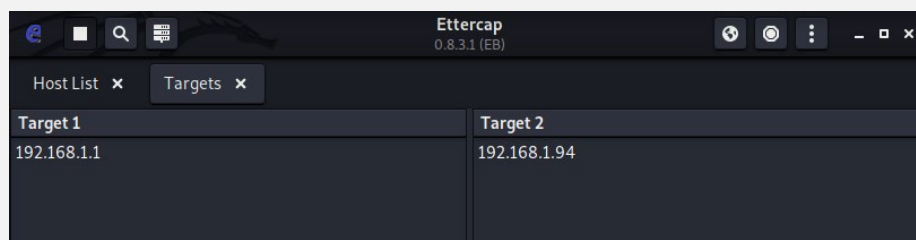
La **segunda dirección** que escogeremos será la del equipo con el que vamos a iniciar sesión en la **página HTTP** y le clicaremos sobre **Add Target 2**:



Podemos comprobar las direcciones seleccionadas pulsando sobre los **tres puntos** de la parte superior derecha y **Current targets**:

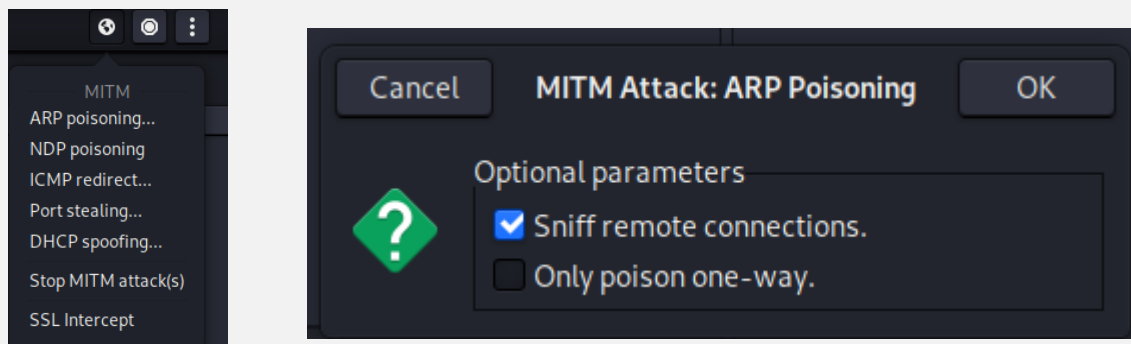


Nos aparecerán las **direcciones IPs** escogidas anteriormente:



5. Iniciaremos el envenenamiento o ataque por ARP:

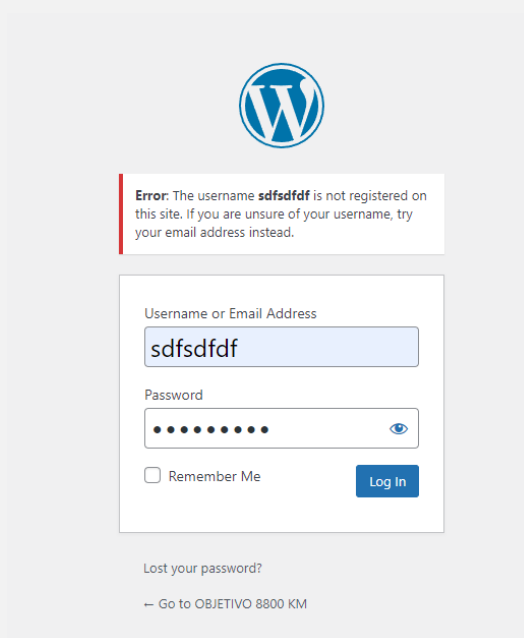
Para iniciar el **envenenamiento por ARP**, clicaremos sobre la **bola del mundo** que se encuentra en la parte superior derecha y **ARP poisoning...**:



Le daremos a **OK** para que empiece el envenenamiento.

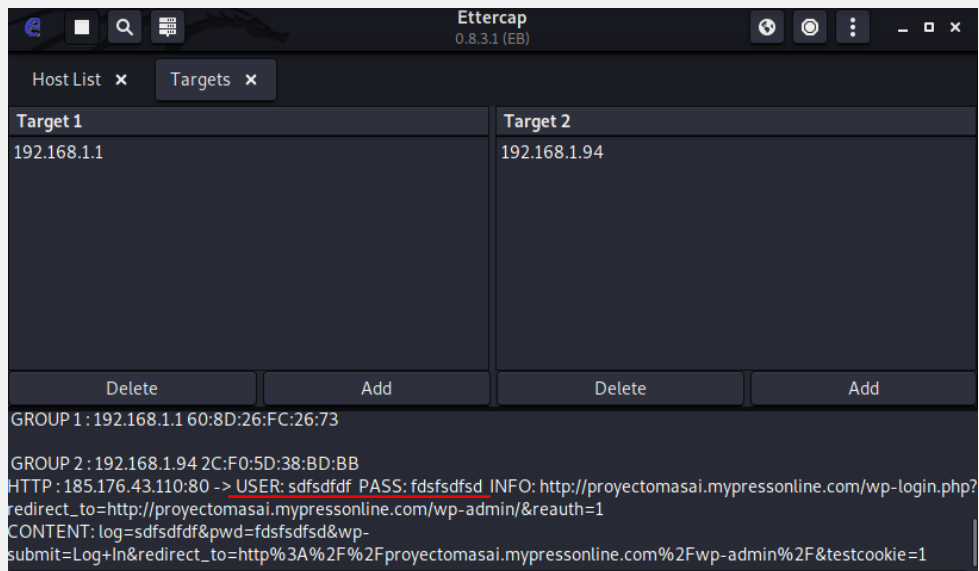
6. Iniciaremos sesión desde el Target 2 seleccionado:

Nos tenemos que ir a una página de inicio de sesión con **protocolo HTTP**:



7. Comprobaremos Ettercap para ver si nos aparece la información de inicio de sesión:

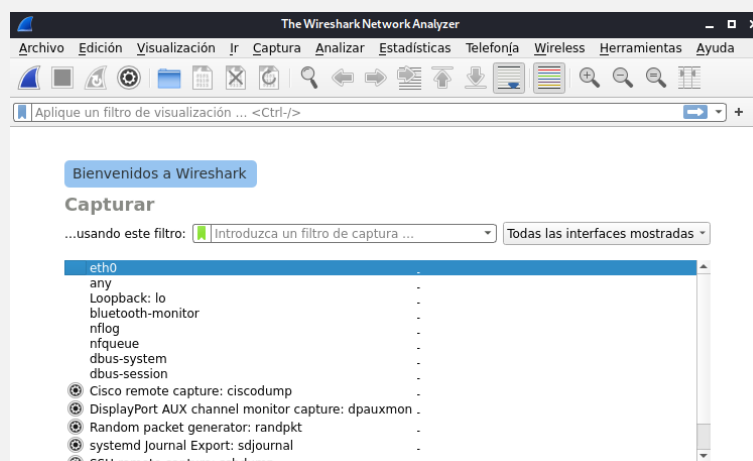
Como podremos observar, en la parte inferior de **Ettercap** nos aparecerá toda la **información de inicio de sesión**:



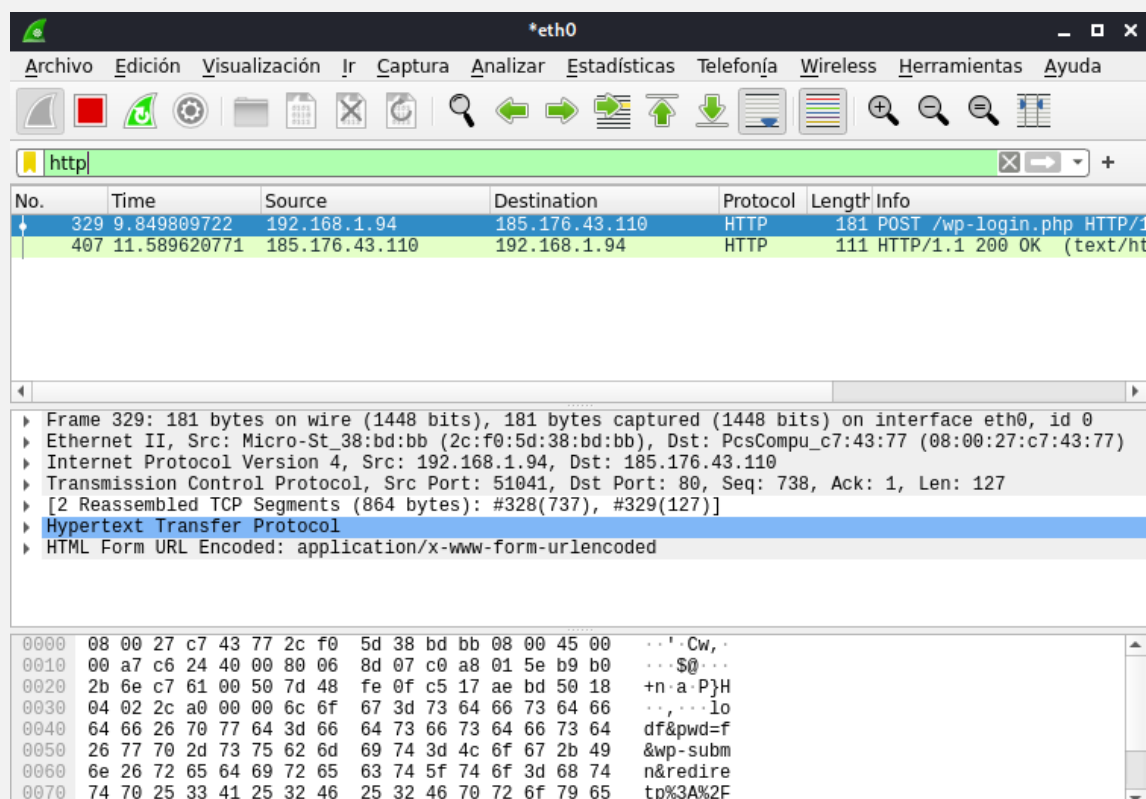
8. Comprobar la información de inicio de sesión desde Wireshark:

También podemos comprobar las credenciales de inicio de sesión desde **Wireshark** de la misma manera que con **Ettercap**.

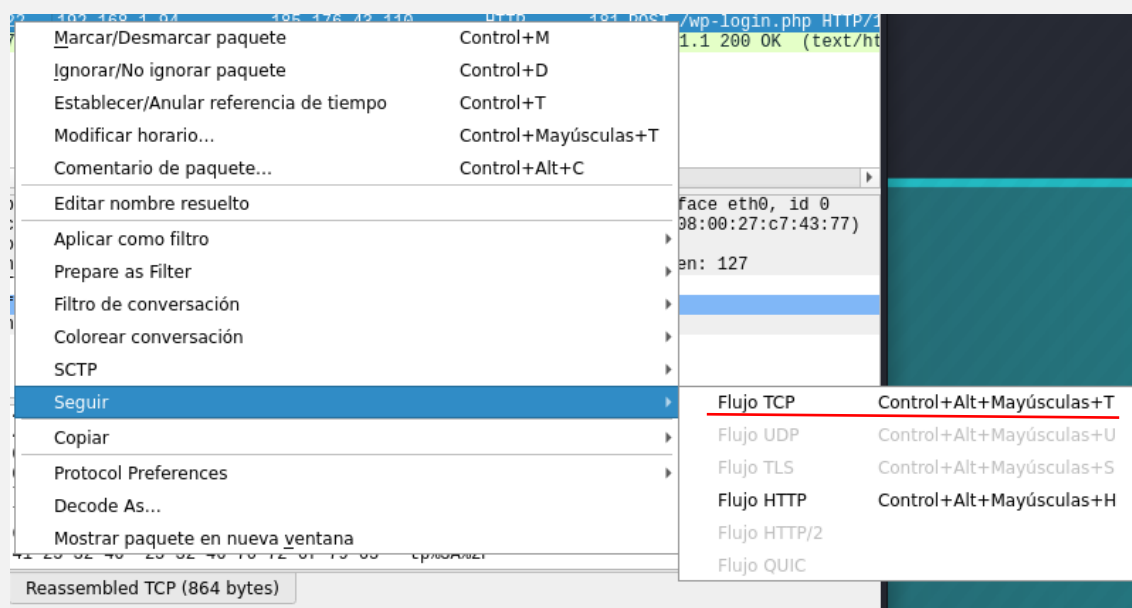
Para eso iniciaremos **Wireshark**, seleccionaremos nuestra **tarjeta de red** y aplicaremos el **filtro de búsqueda sobre http**:



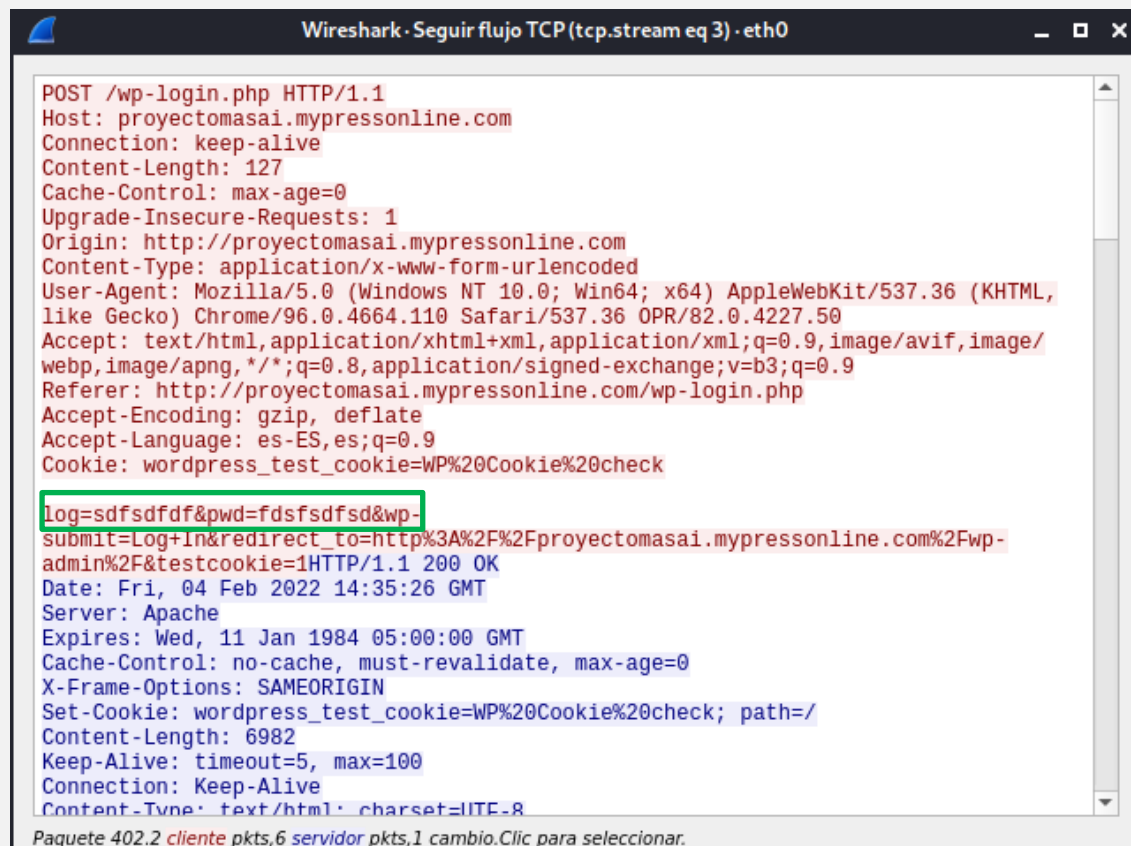
Podemos observar que, al aplicar el filtro, nos aparecerá un paquete proveniente del **target 2**:



Si hacemos click derecho sobre él, nos vamos a **seguir** y **flujo TCP**, nos aparecerá la misma información que en **Ettercap**:



Nos aparecerá la misma información que en **Ettercap**, para localizar las credenciales buscaremos **log** y **pwd**:



```
Wireshark · Seguir flujo TCP (tcp.stream eq 3) · eth0

POST /wp-login.php HTTP/1.1
Host: proyectomasai.mypresonline.com
Connection: keep-alive
Content-Length: 127
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://proyectomasai.mypresonline.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36 OPR/82.0.4227.50
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://proyectomasai.mypresonline.com/wp-login.php
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9
Cookie: wordpress_test_cookie=WP%20Cookie%20check

log=sdfsdfdf&pwd=fdsfsdfsd&wp-submit=Log+in&redirect_to=http%3A%2F%2Fproyectomasai.mypresonline.com%2Fwp-admin%2F&testcookie=1HTTP/1.1 200 OK
Date: Fri, 04 Feb 2022 14:35:26 GMT
Server: Apache
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
Set-Cookie: wordpress_test_cookie=WP%20Cookie%20check; path=/
Content-Length: 6982
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

Paquete 402.2 cliente pkts,6 servidor pkts,1 cambio.Clic para seleccionar.
```