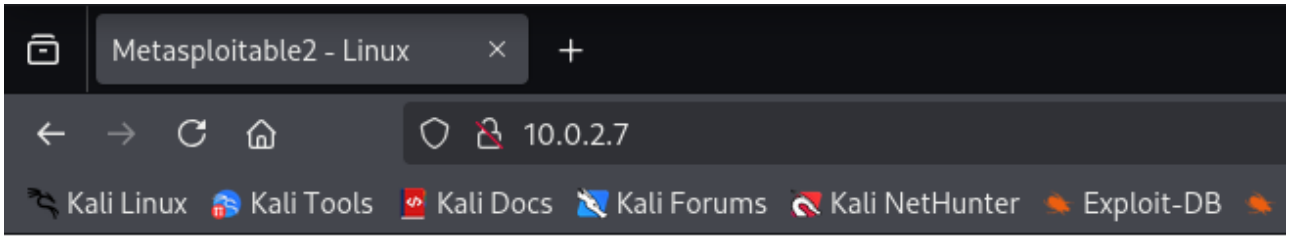
Wireshark análisis de tráfico

Tools

- Máquina Kali Linux (atacante)
- Debia (victima)
- Máquina Metasploitable (servidor)



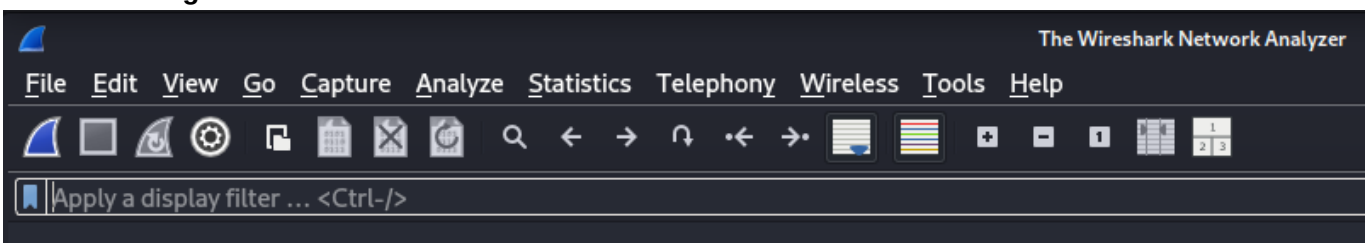
```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```

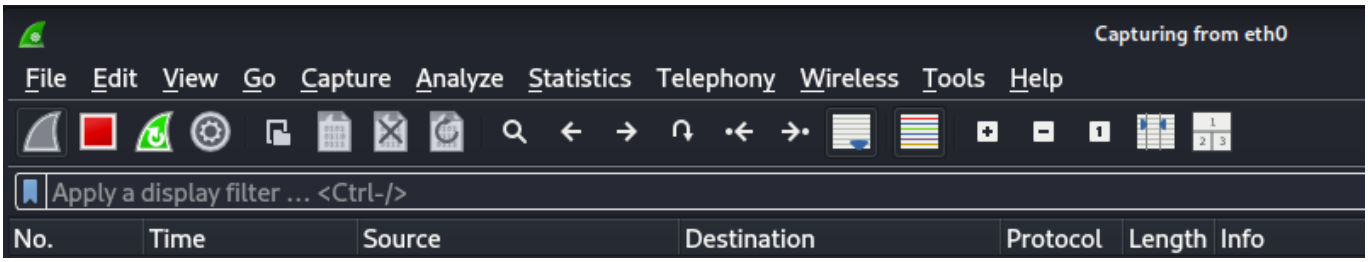
- TWiki
- phpMyAdmin
- Mutillidae
- DVWA
- WebDAV

Análisis de tráfico en Wireshark

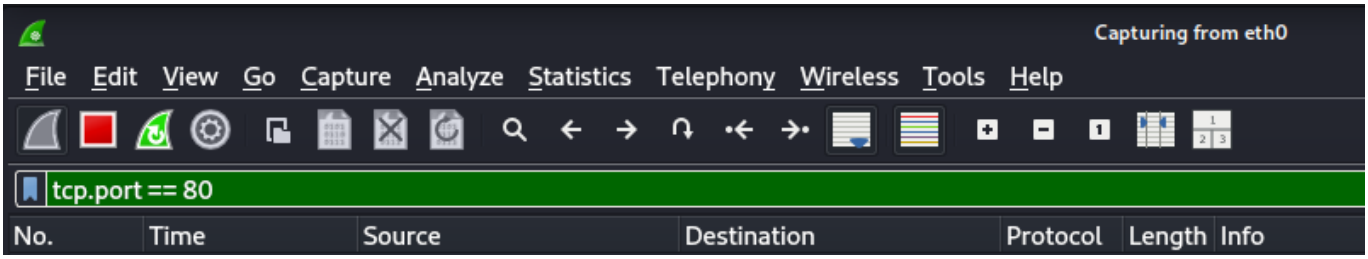
1 - Capturar y analizar el trafico HTTP

Paso 1: Configura Wireshark

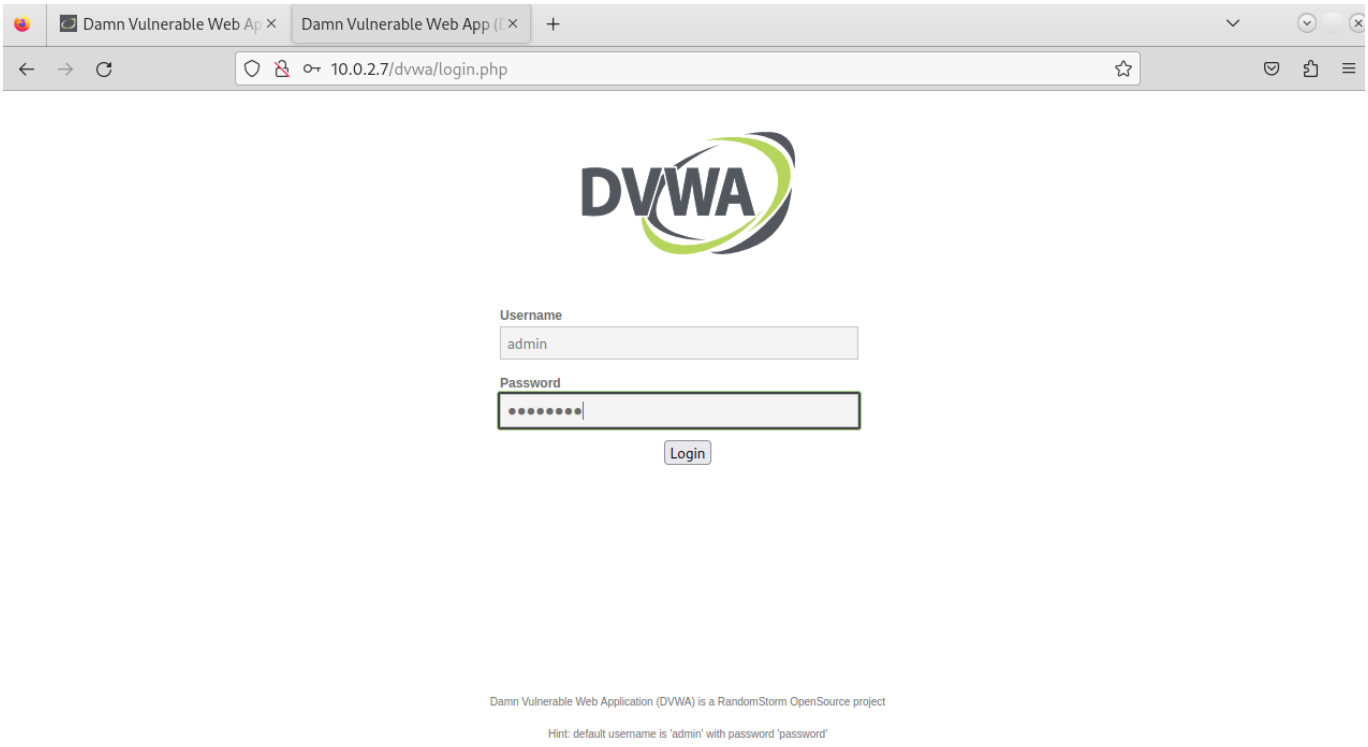


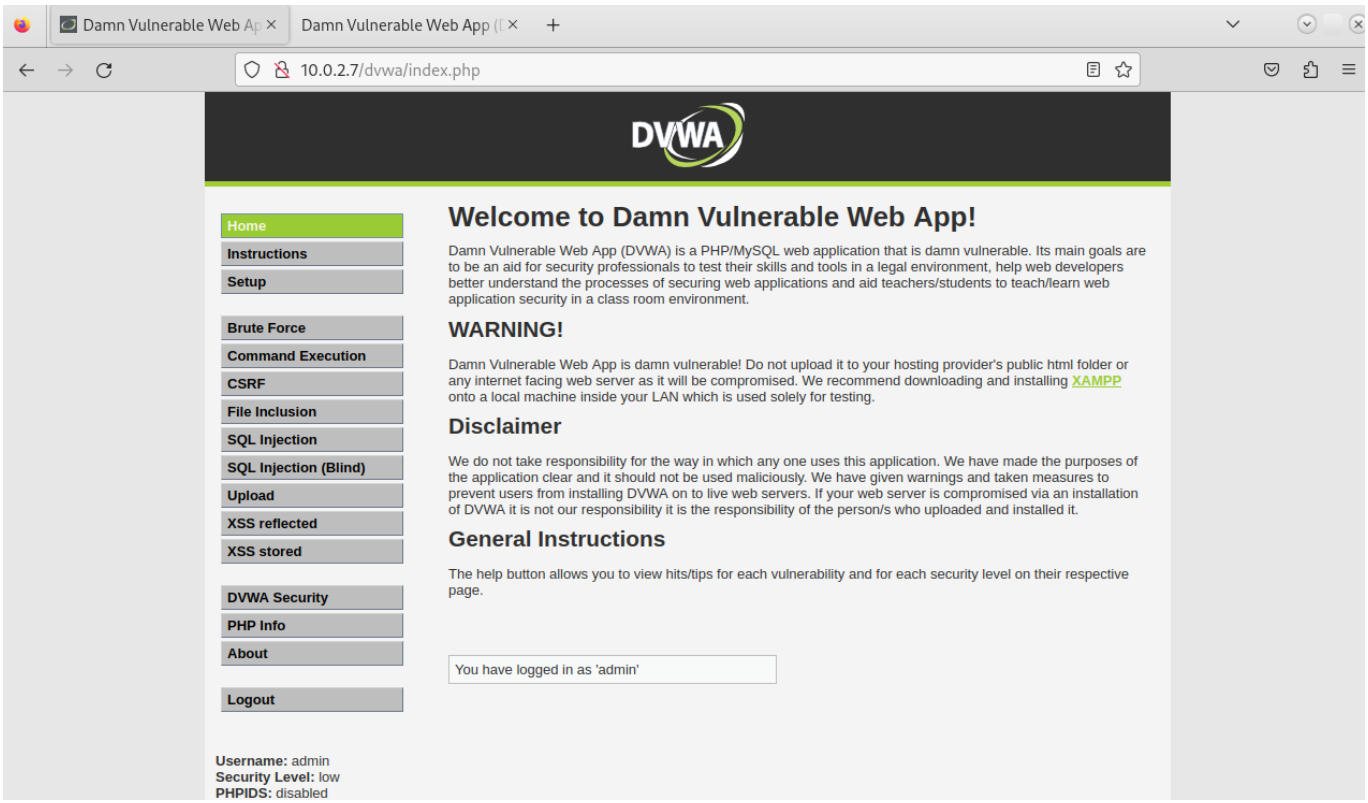


Paso 2: Aplicar filtro TCP para tráfico HTTP

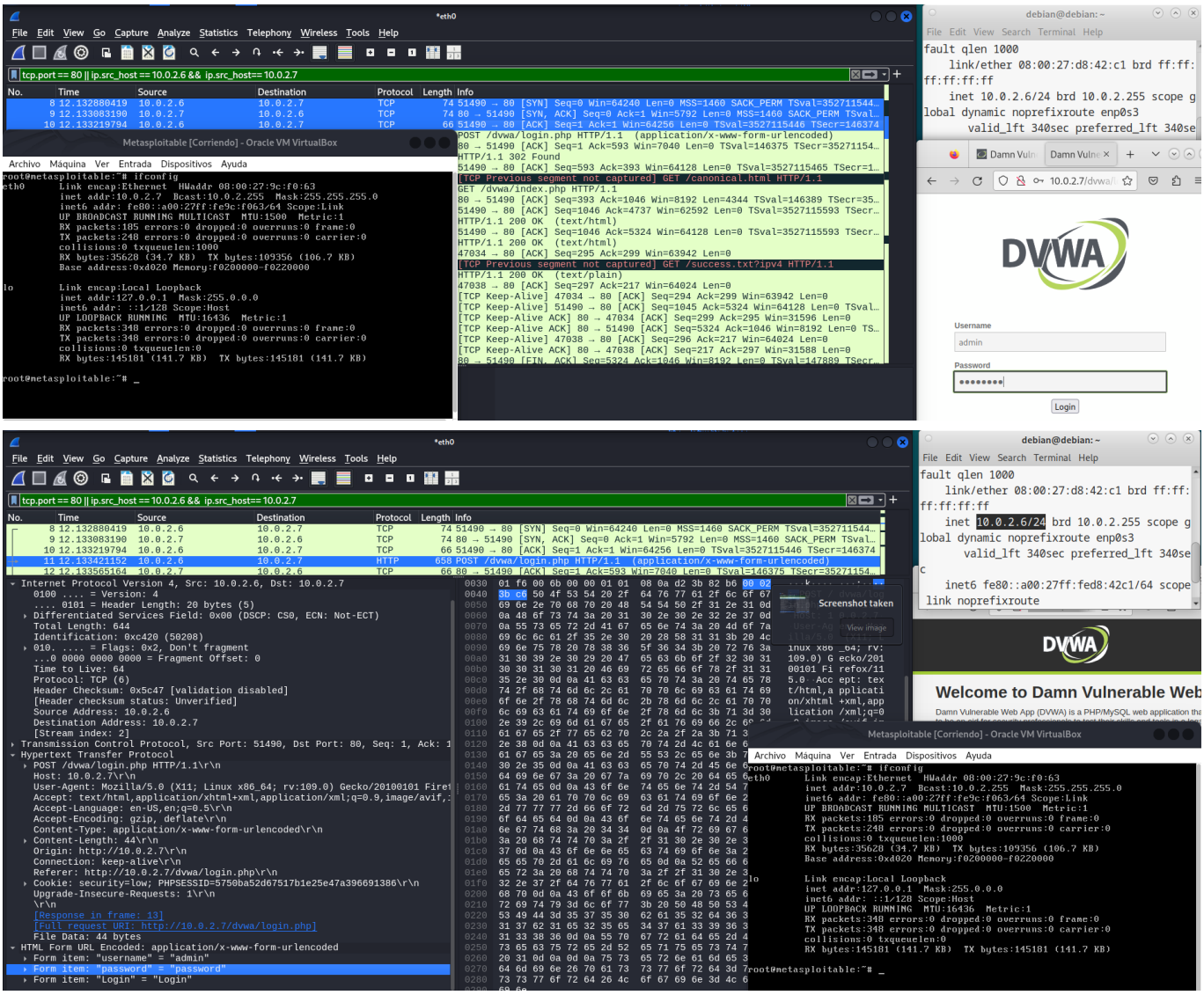


Paso 3: Realizar una solicitud HTTP en el navegador





Paso 4: Analizar los paquetes capturados

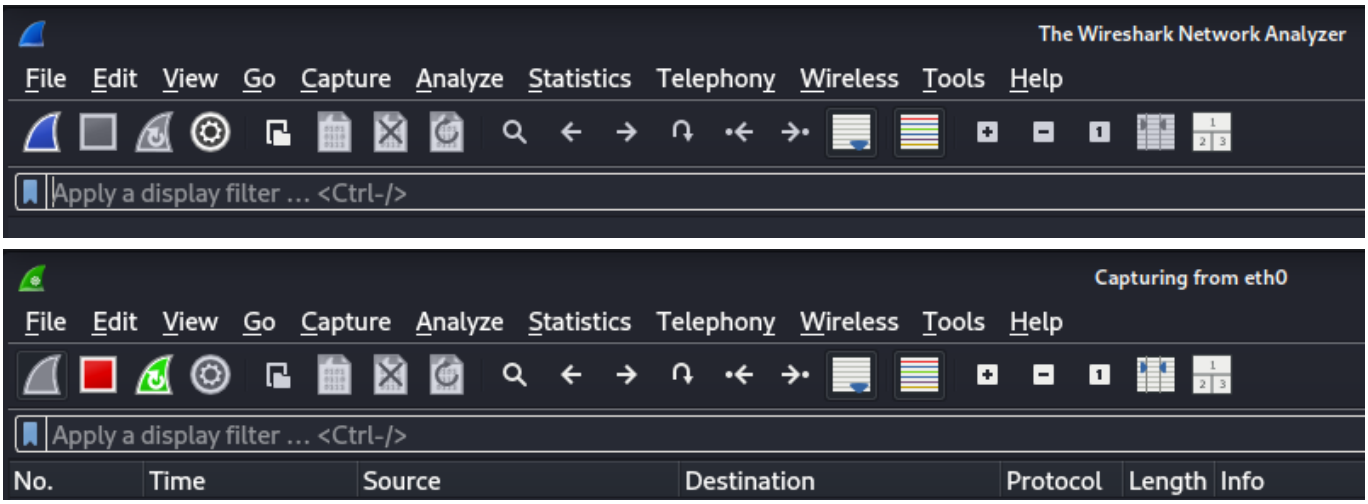


Explicación del resultado esperado:

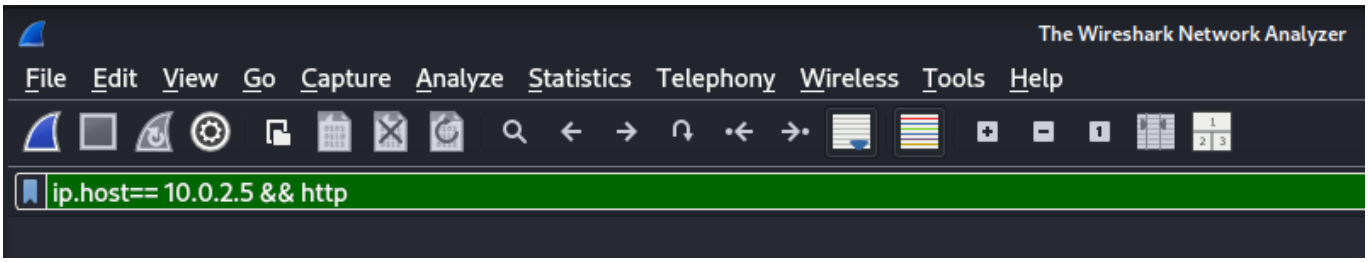
- La negociación TCP se ve como tres paquetes consecutivos con banderas y números de secuencia específicos. En la sección de solicitud HTTP, hay el nombre de usuario utilizado para autenticación "admin" junto con su contraseña correspondiente "password".

2 - Capturar y analizar ataque XSS

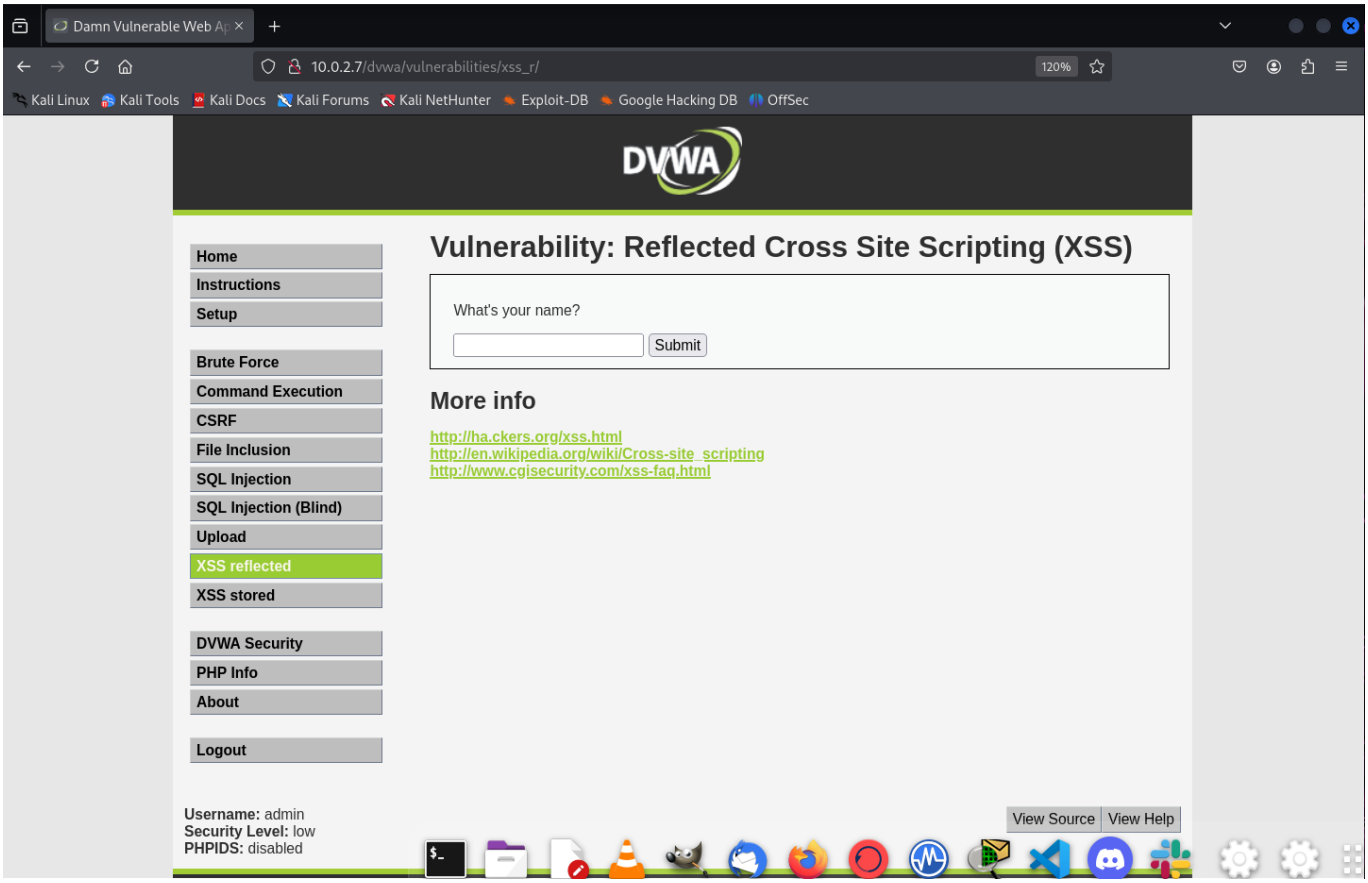
Paso 1: Configura Wireshark

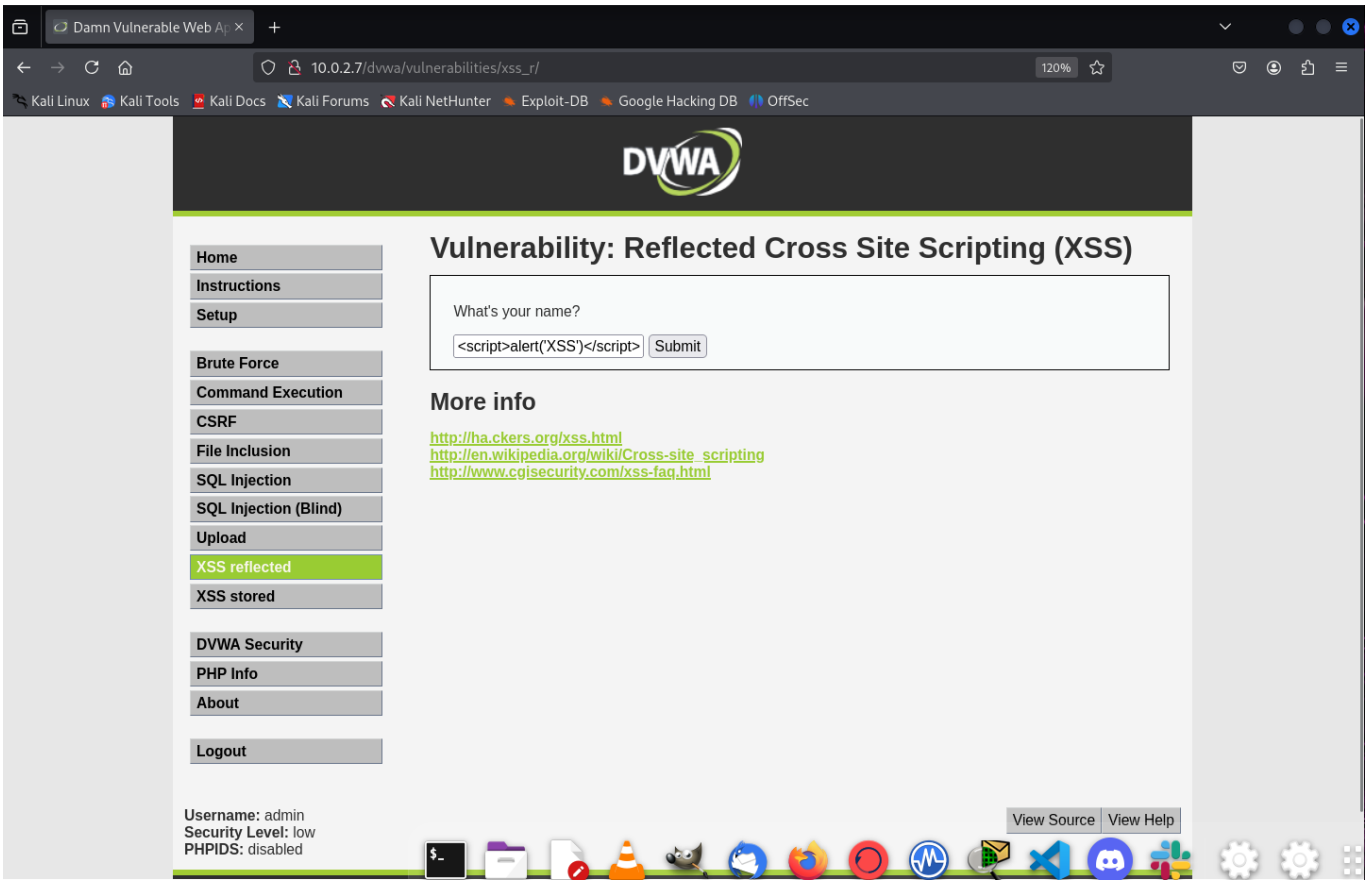


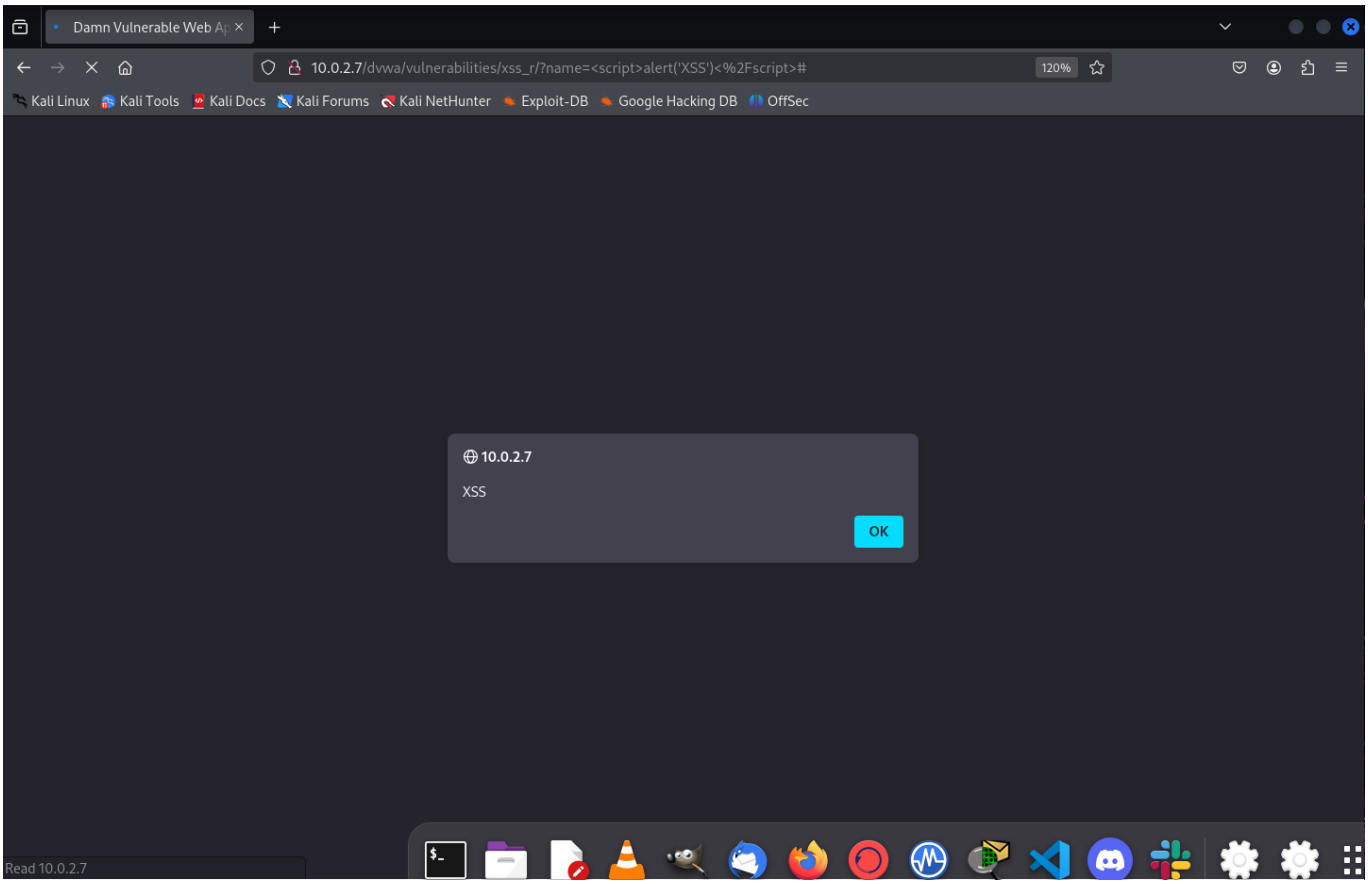
Paso 2: Aplicar filtro HTTP desde Kali Linux

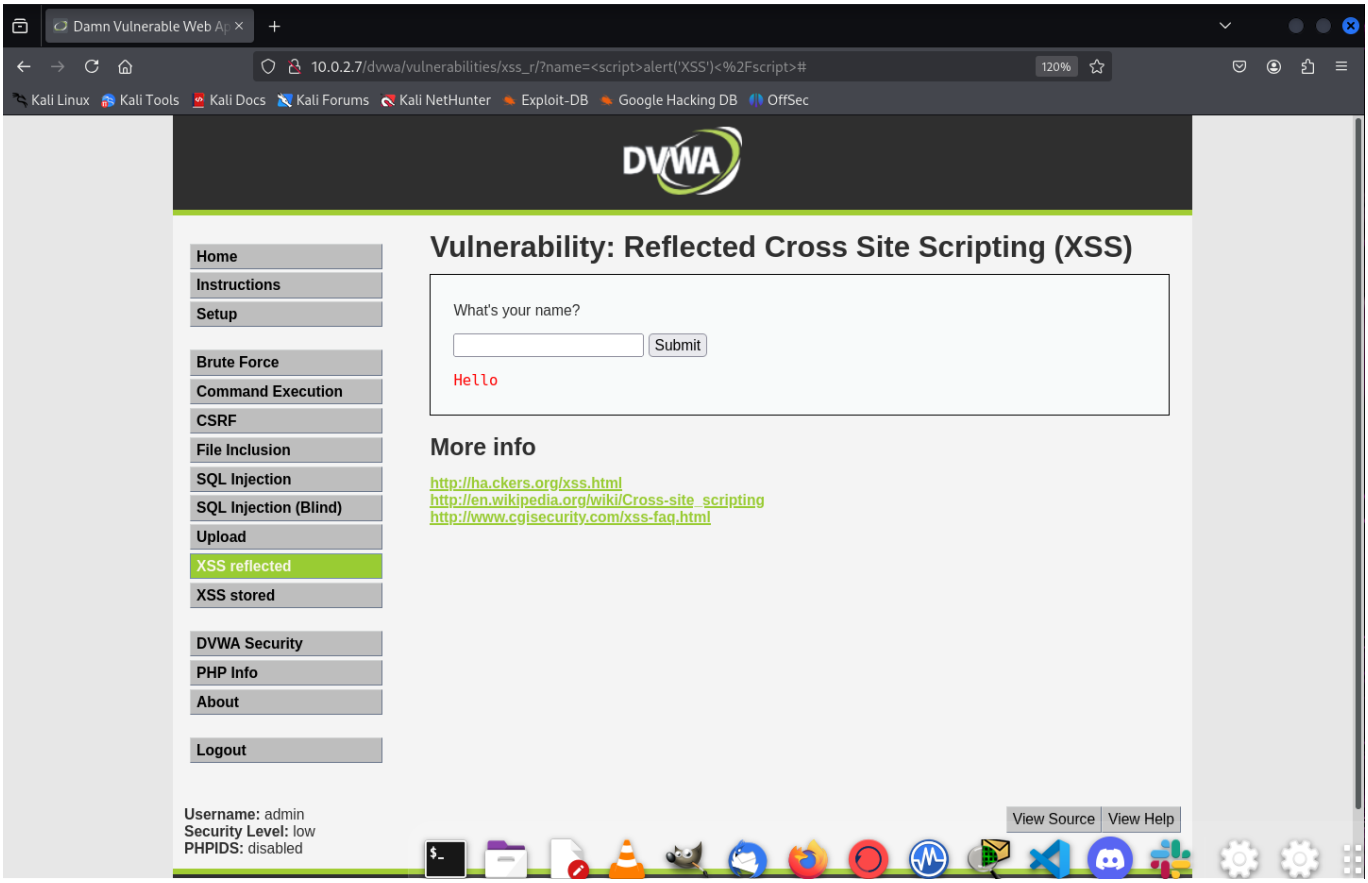


Paso 3: Realizar un ataque XSS en DVWA

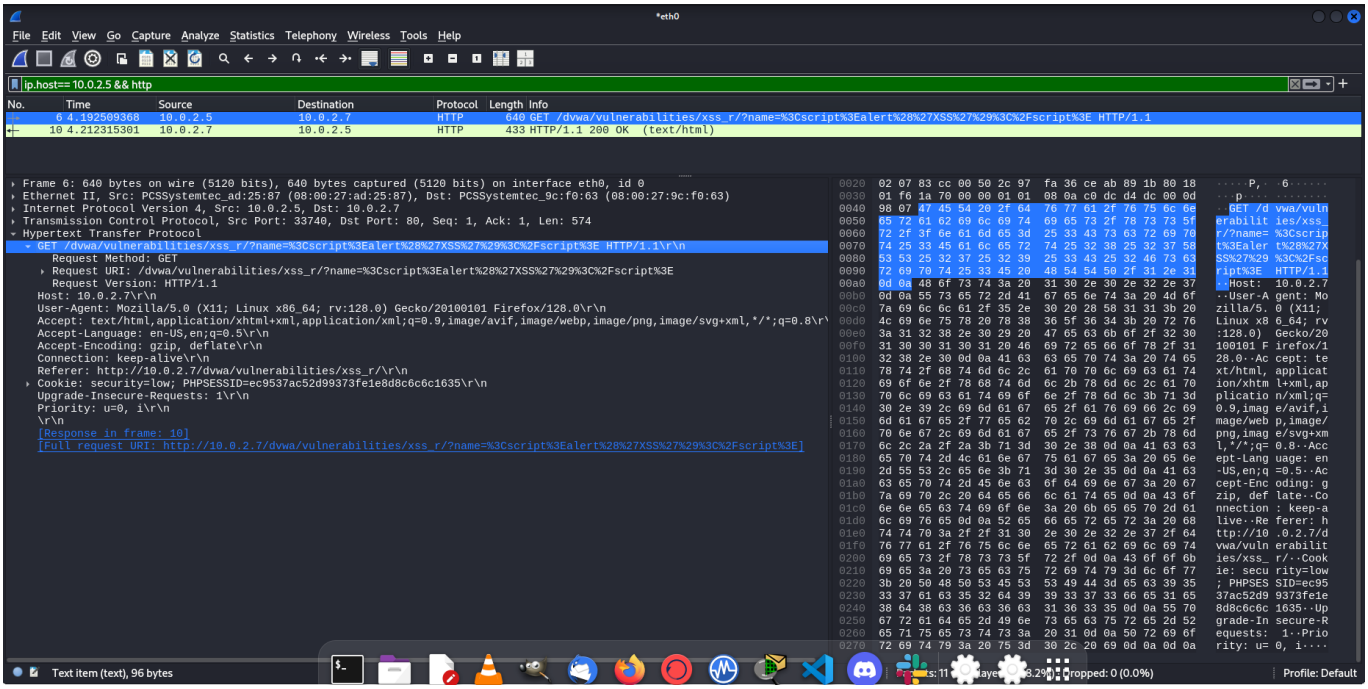


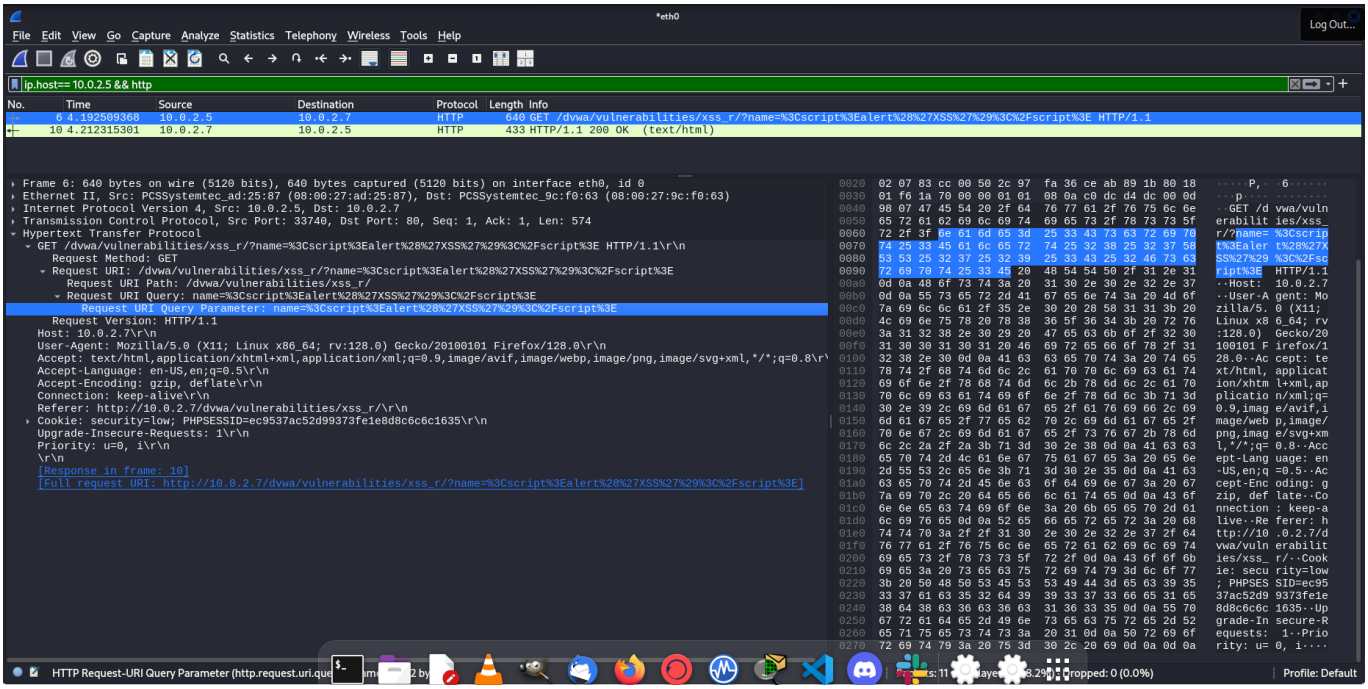



Damn Vulnerable Web A
10.0.2.7/dvwa/vulnerabilities/xss_r/?name=<script>alert('XSS')<%2Fscript>#
120%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
10.0.2.7
XSS
OK
Read 10.0.2.7


Damn Vulnerable Web A
10.0.2.7/dvwa/vulnerabilities/xss_r/?name=<script>alert('XSS')<%2Fscript>#
120%
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello
More info
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
Username: admin
Security Level: low
PHPIDS: disabled
View Source
View Help

Paso 4: Analizar los paquetes capturados





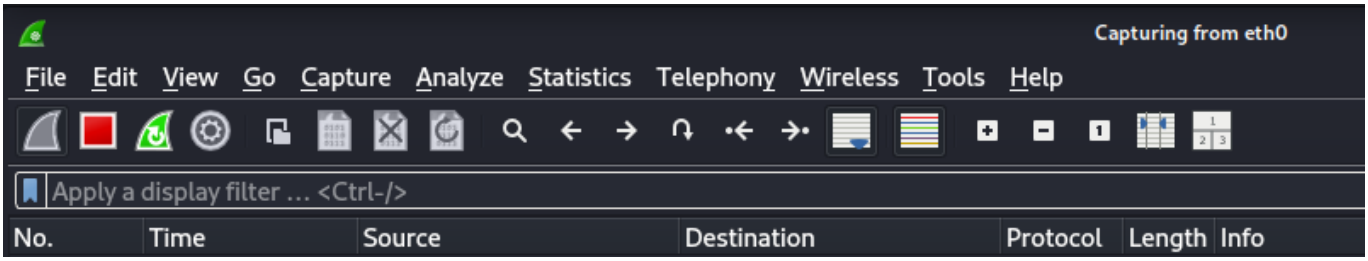
Explicación del resultado esperado:

- La solicitud HTTP contiene la carga útil de XSS en su sección de datos. Esta carga puede ser utilizada para ejecutar código JavaScript.

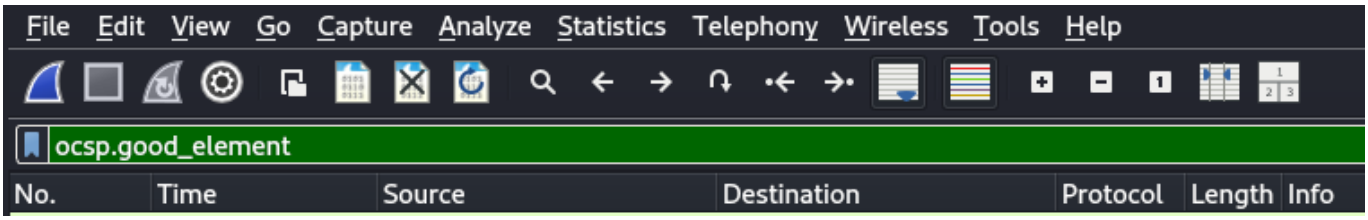
3 - Capturar y analizar la validación del certificado de Google

Instrucciones paso a paso:

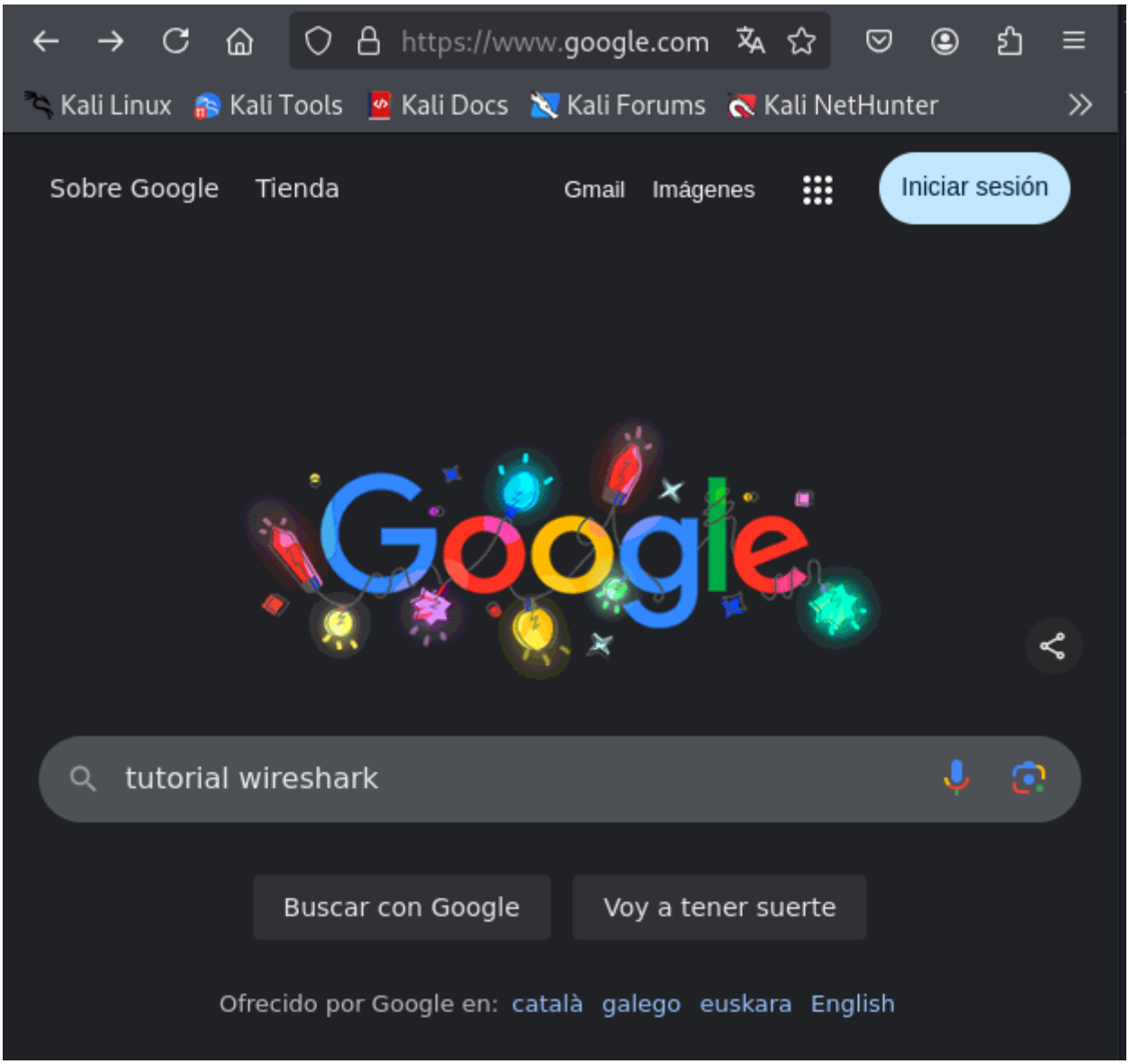
Paso 1: Configura Wireshark



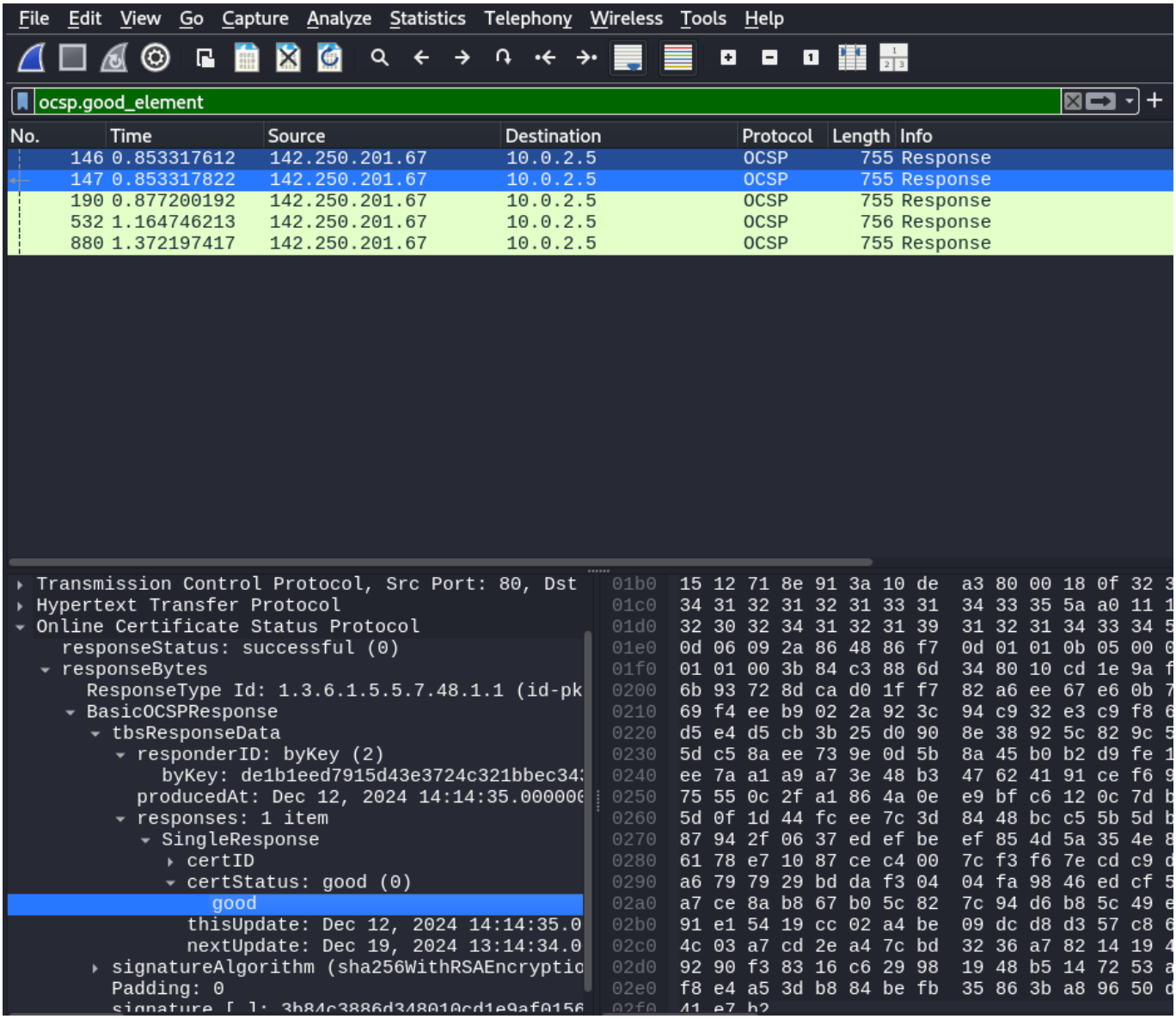
Paso 2: Aplicar filtro TLS desde Kali Linux



Paso 3: Realizar una búsqueda en Google



Paso 4: Analizar los paquetes capturados

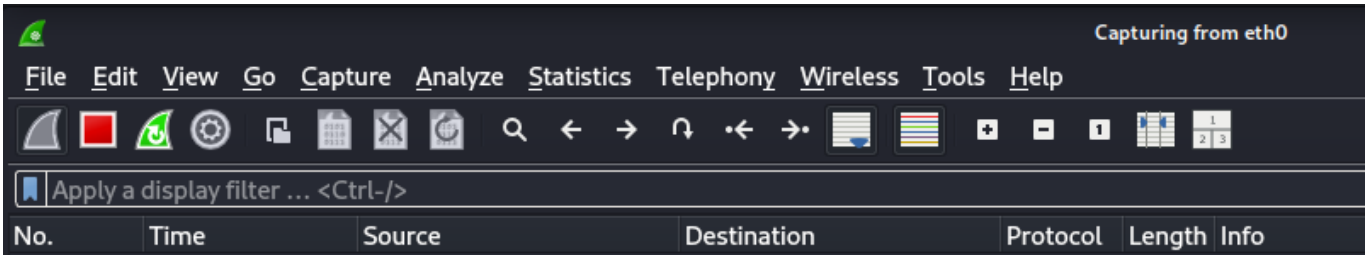


Explicación del resultado esperado:

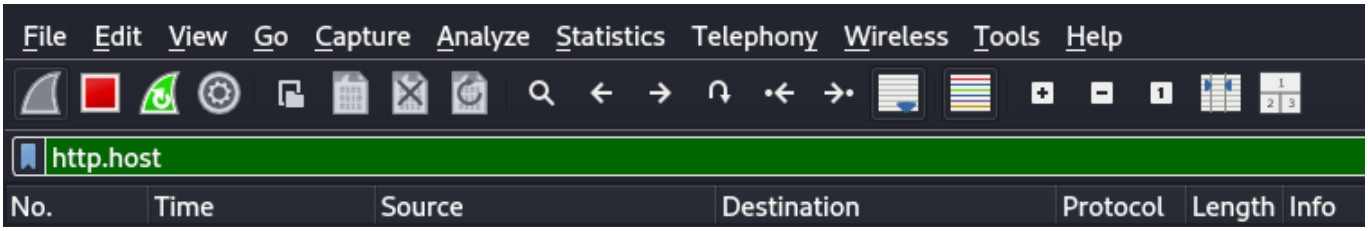
- El resultado mostra en la sección de negociación SSL/TLS, el certificado google válido con la confirmacion good, indincado a la vez informacion sobre las versiones y sus pssibles vulnerabilidades.

4 - Capturar y analizar solicitud a cocacola

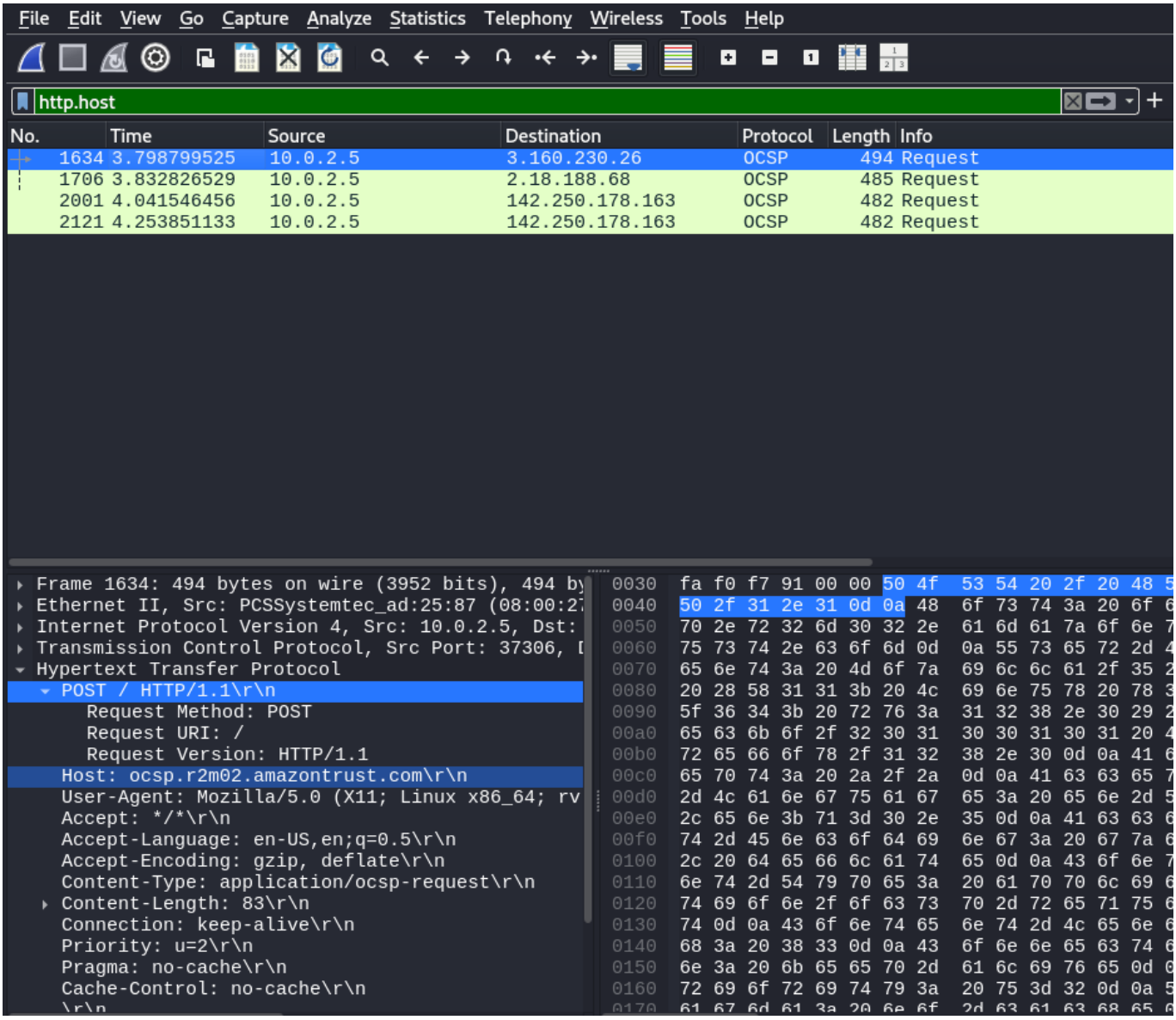
Paso 1: Configura Wireshark



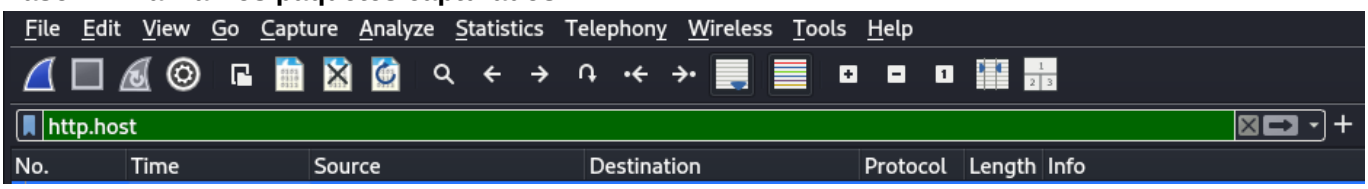
Paso 2: Aplicar filtro HTTP desde Kali Linux



Paso 3: Realizar una solicitud al sitio Cocacola



Paso 4: Analizar los paquetes capturados

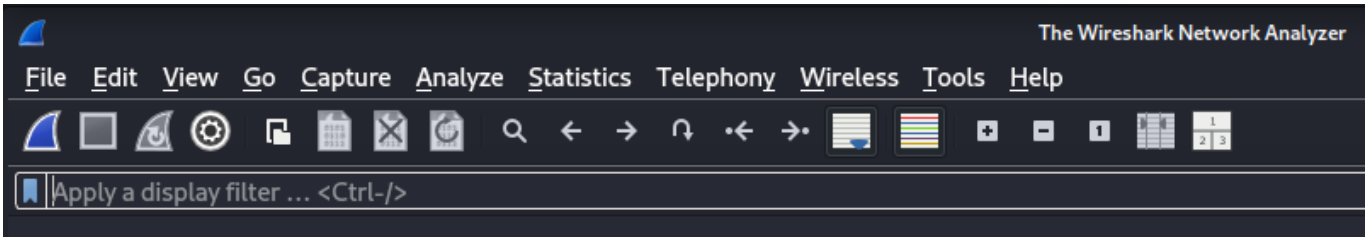


Explicación del resultado esperado:

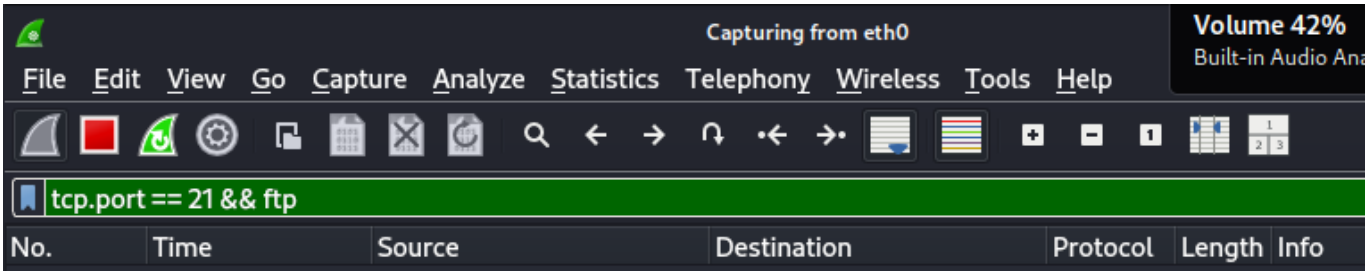
- La solicitud HTTP contiene la URL completa de la página, el methodo usado y la verson de HTTP, en este caso es "POST / HTTP/1.1" y tambien se aprecia informacion sobre el Host usado en este caso es "amazontrust.com"

5 - Capturar y analizar el archivo my.cnf a través de FTP al servidor Metasploitable desde la máquina Kali Linux

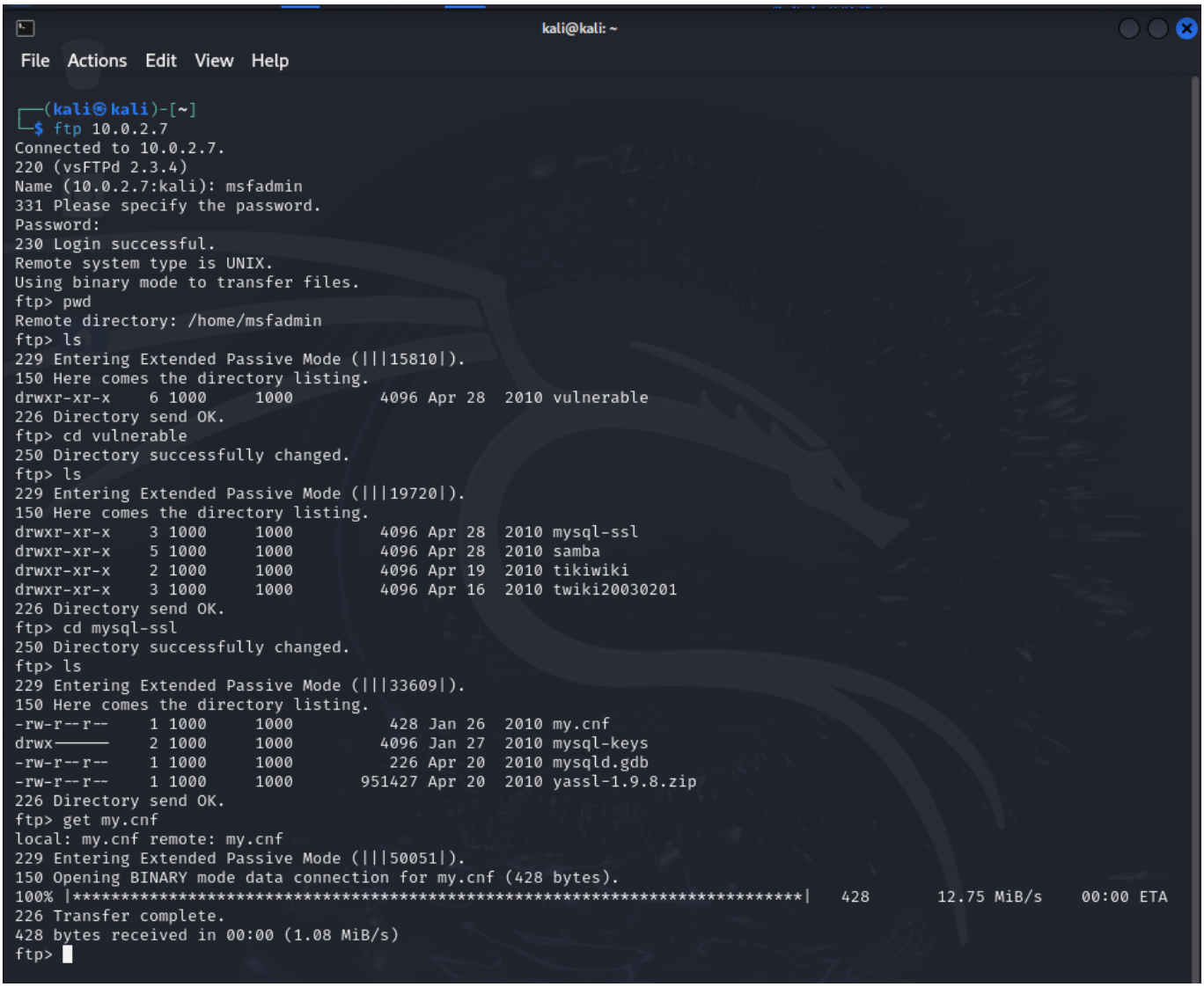
Paso 1: Configura Wireshark



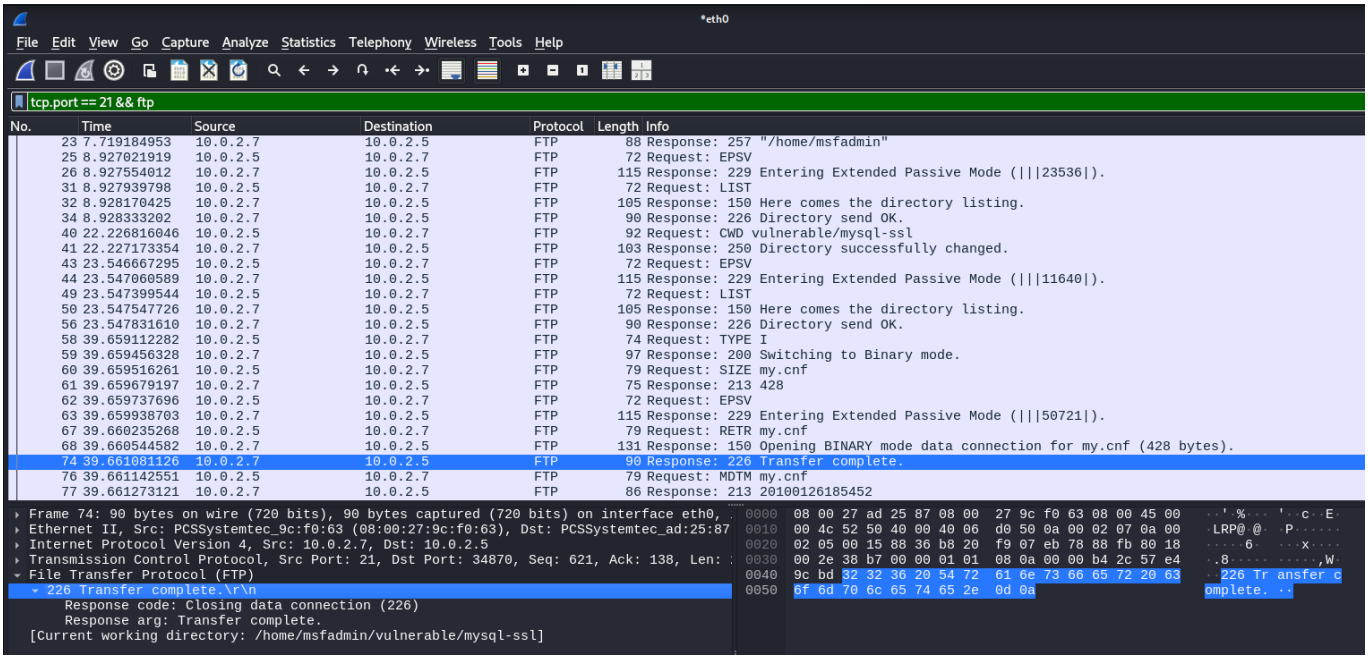
Paso 2: Aplicar filtro FTP



Paso 3: Conectar via FTP al servidor Metasploitable desde Kali Linux & Paso 4: Descargar el archivo my.cnf



Paso 5: Analizar los paquetes capturados



Explicación del resultado esperado:

- Los paquetes de datos contienen detalles sobre el archivo `my.cnf` descargado y mas contenido relacionado con las comunicaciones FTP realizadas.