# EJERCICIO ATAQUE MAN IN THE MIDDLE

## Prerrequisitos

- Kali Linux

- Damn Vulnerable Linux 1.5

- Metasploitable2

- Herramientas arrancadas: Wireshark, tshark

## Ejercicio 1

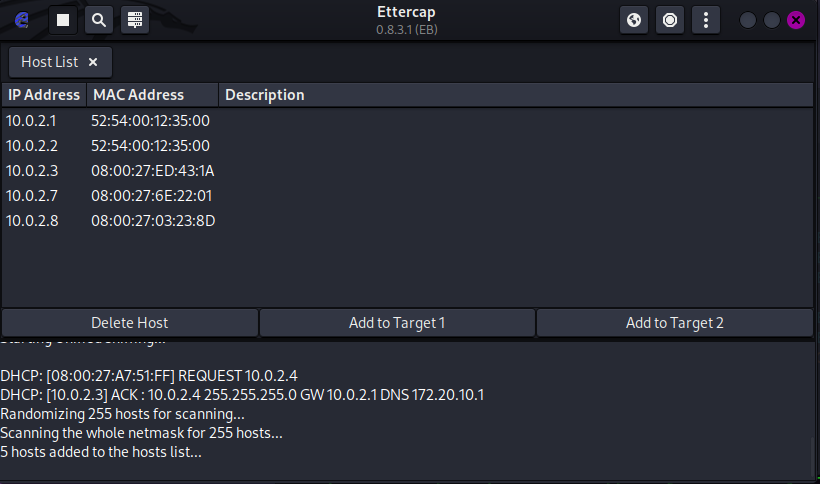
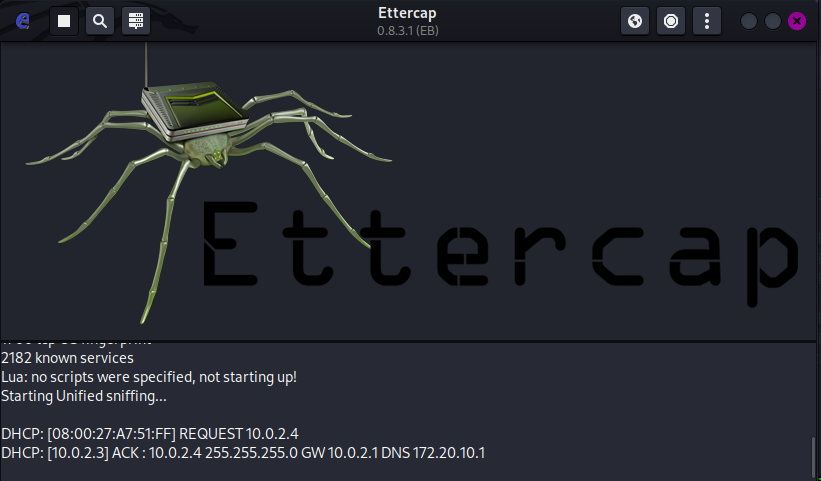
- Realizar un ataque MiTM desde Kali (que es la que tiene Wireshark) entre el cliente DVL y

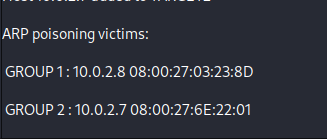
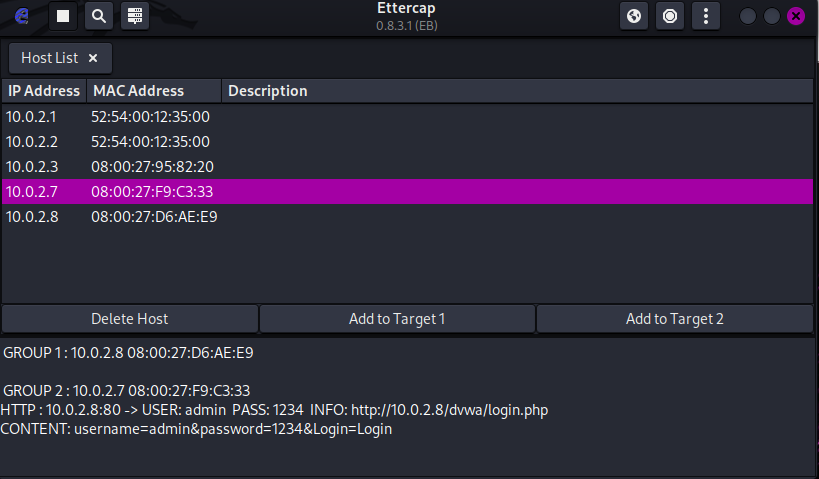
Metasploitable2 en el acceso al servicio web DVWA y capturar el usuario y contraseña en wireshark

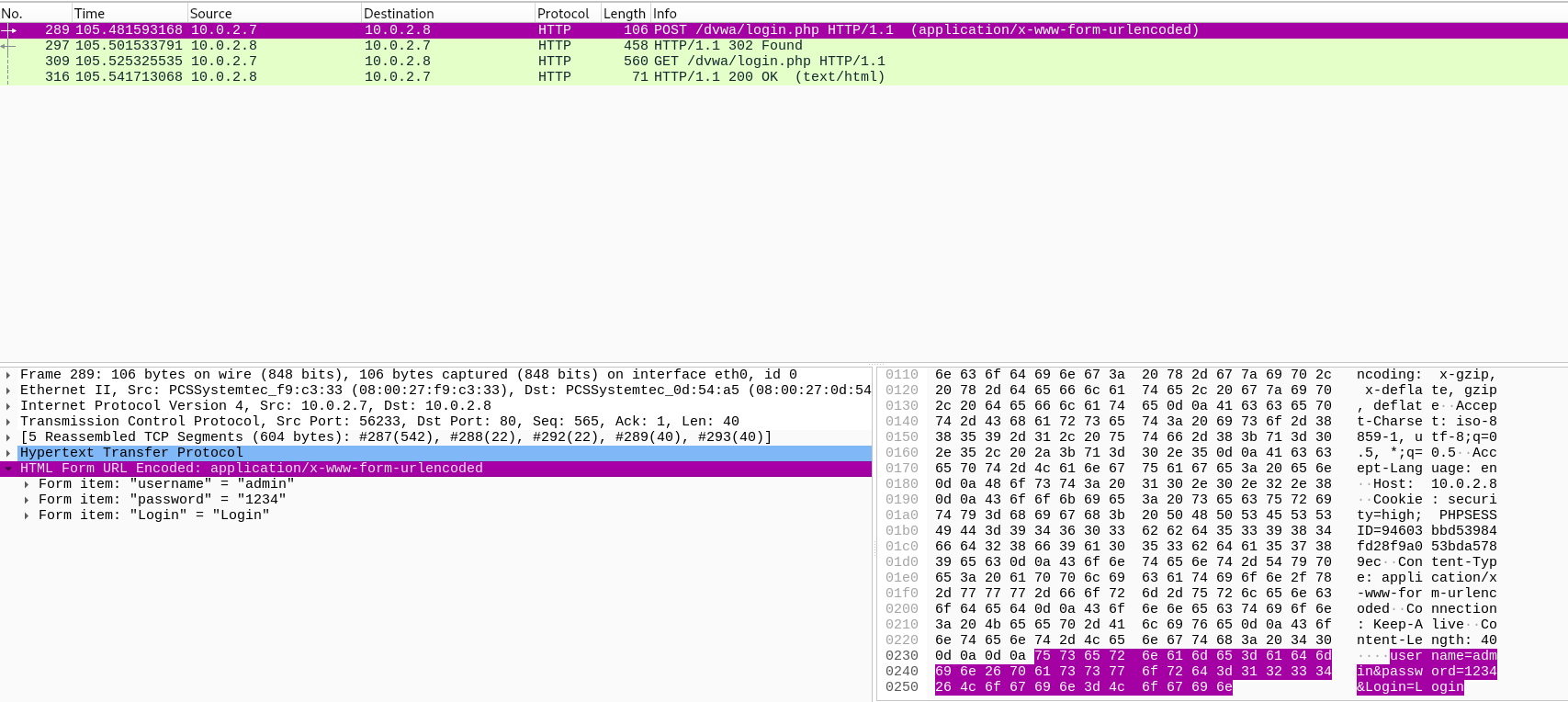
\* Metasploitable es la máquina víctima y DVL la máquina intermediaria

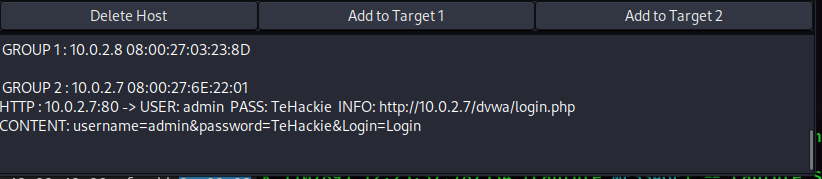
Desde Metasploitable a Kali (Apagamos DVL)

Investigar protocolos y filtros.

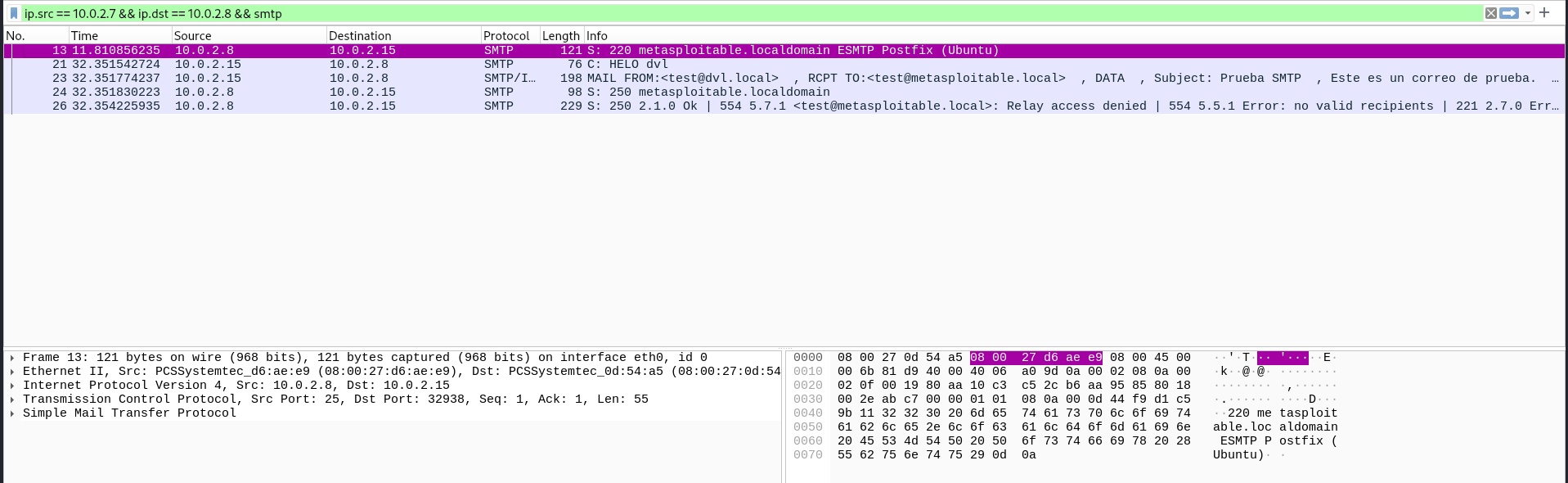
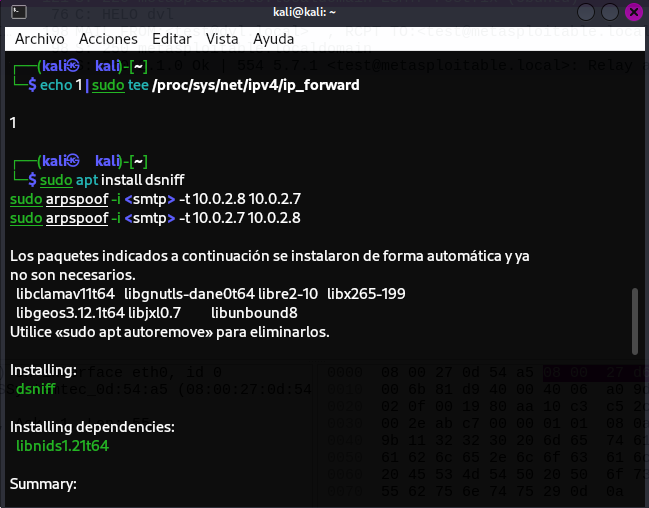
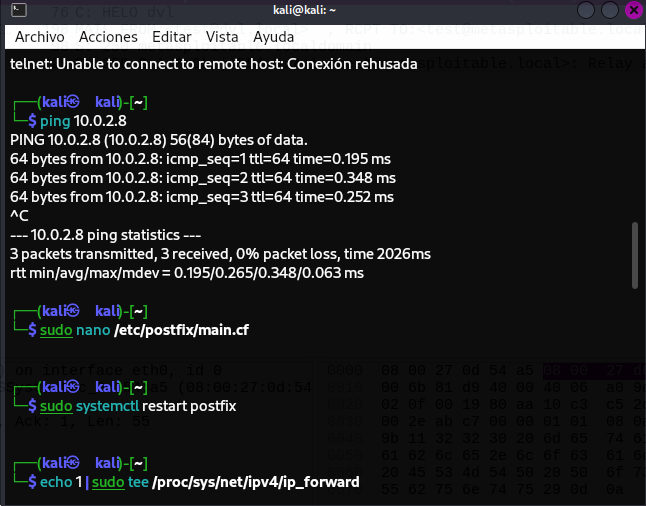
* 



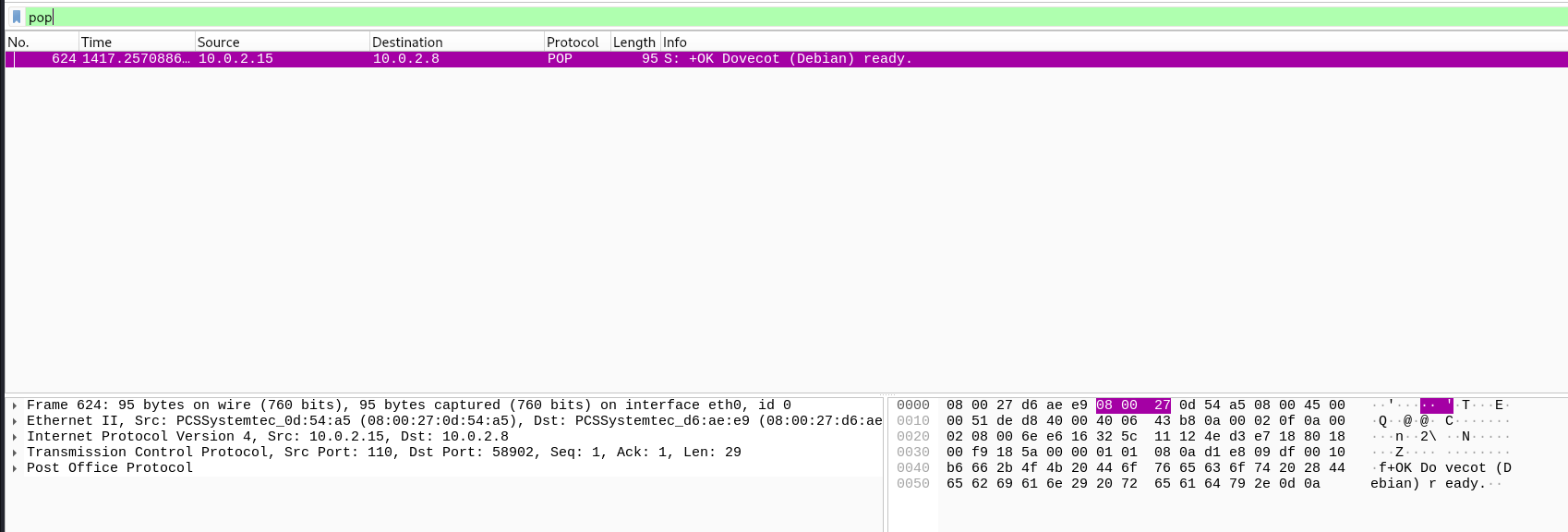
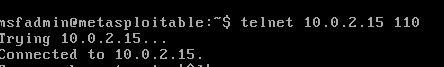
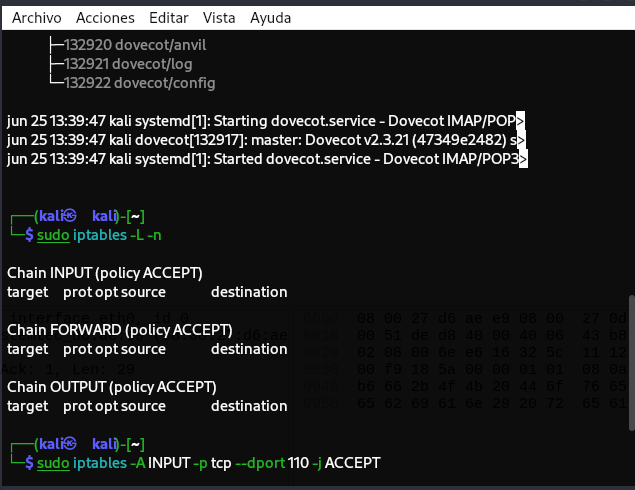
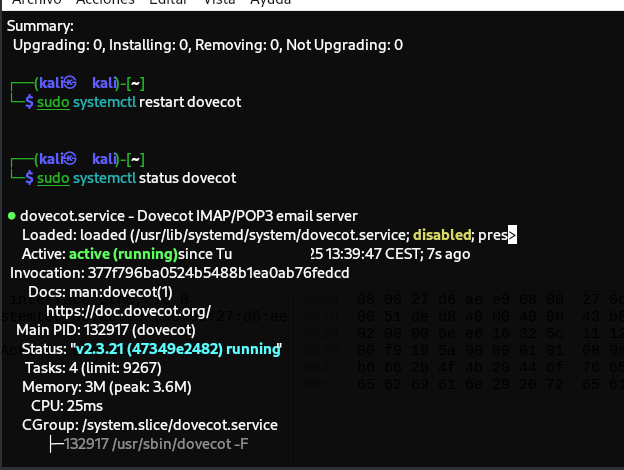
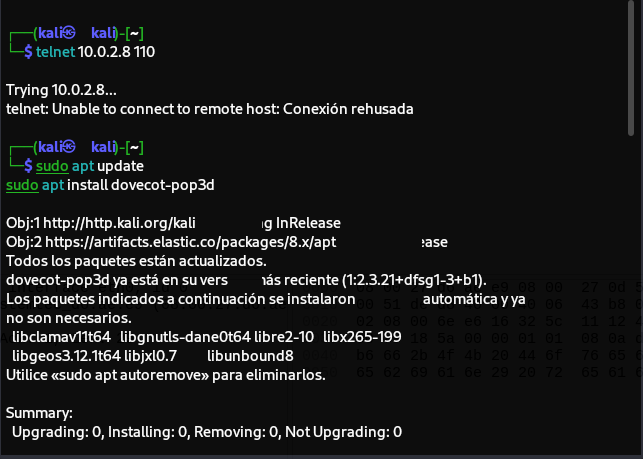


* 

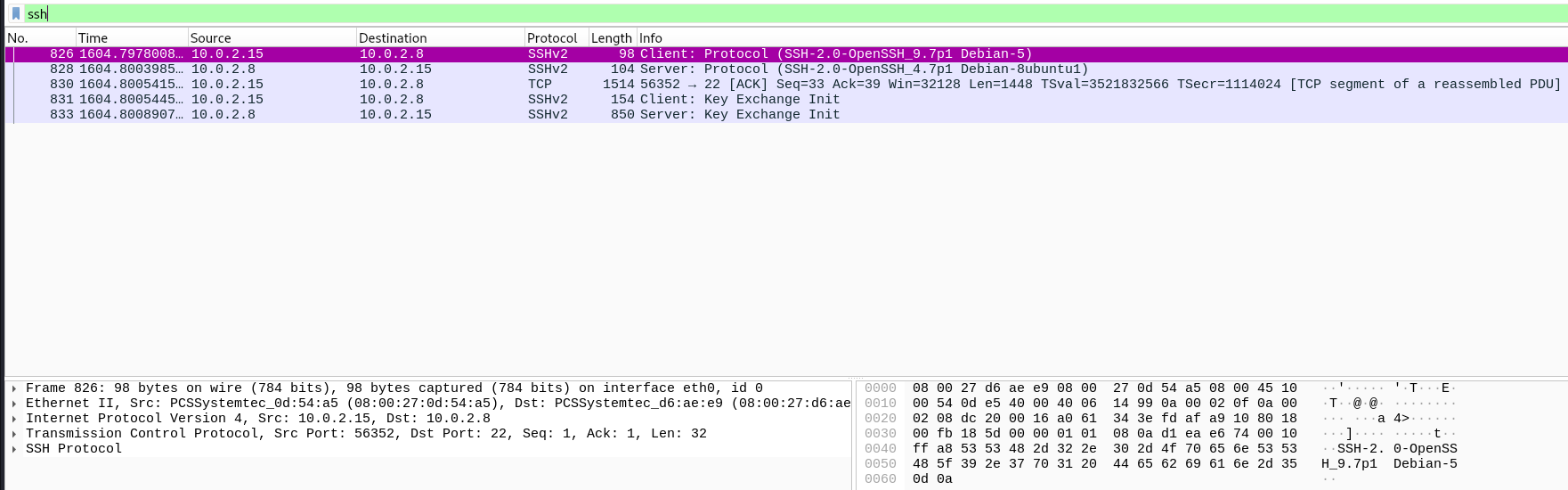
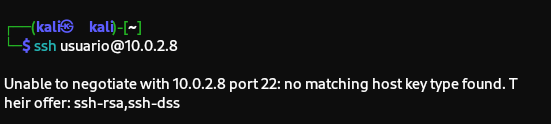
## Ejercicio 2

- Usar Wireshark para capturar tráfico SMTP (postfix)

## Ejercicio 3

- Lo mismo pero con pop 3 ( dovecot-pop3d) , ejecutando comando telnet

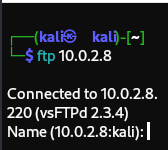
## Ejercicio 4

- Lo mismo con SSH

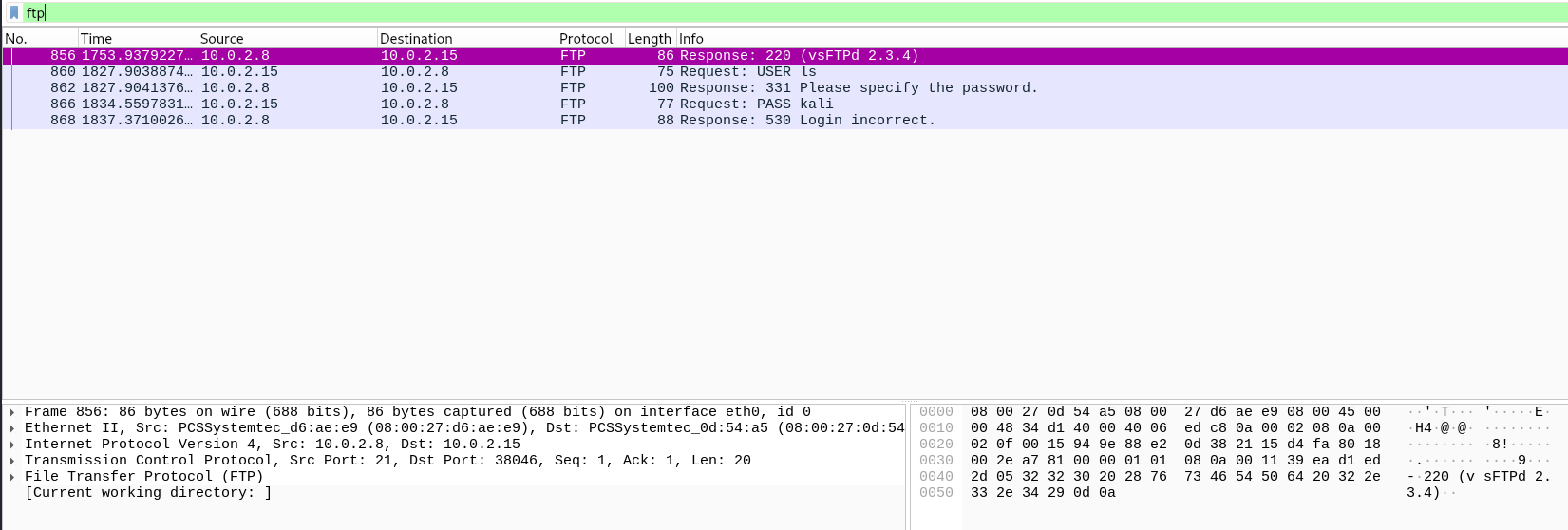
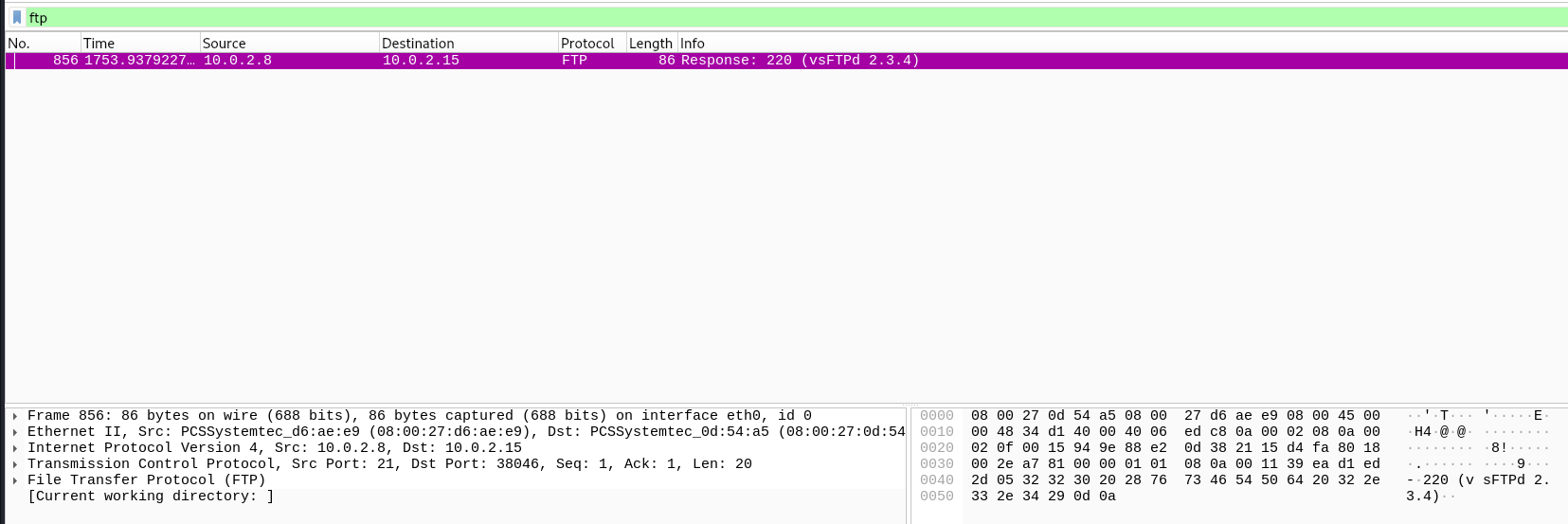
## Ejercicio 5

- Lo mismo con FTP (vsftpd)

Desde Kali a exterior (Apagamos Metasploitale)

**Desde Kali Linux, inicia una conexión FTP hacia el servidor externo:**

Utiliza el cliente FTP en la línea de comandos para conectarte a un servidor FTP externo. Por ejemplo:

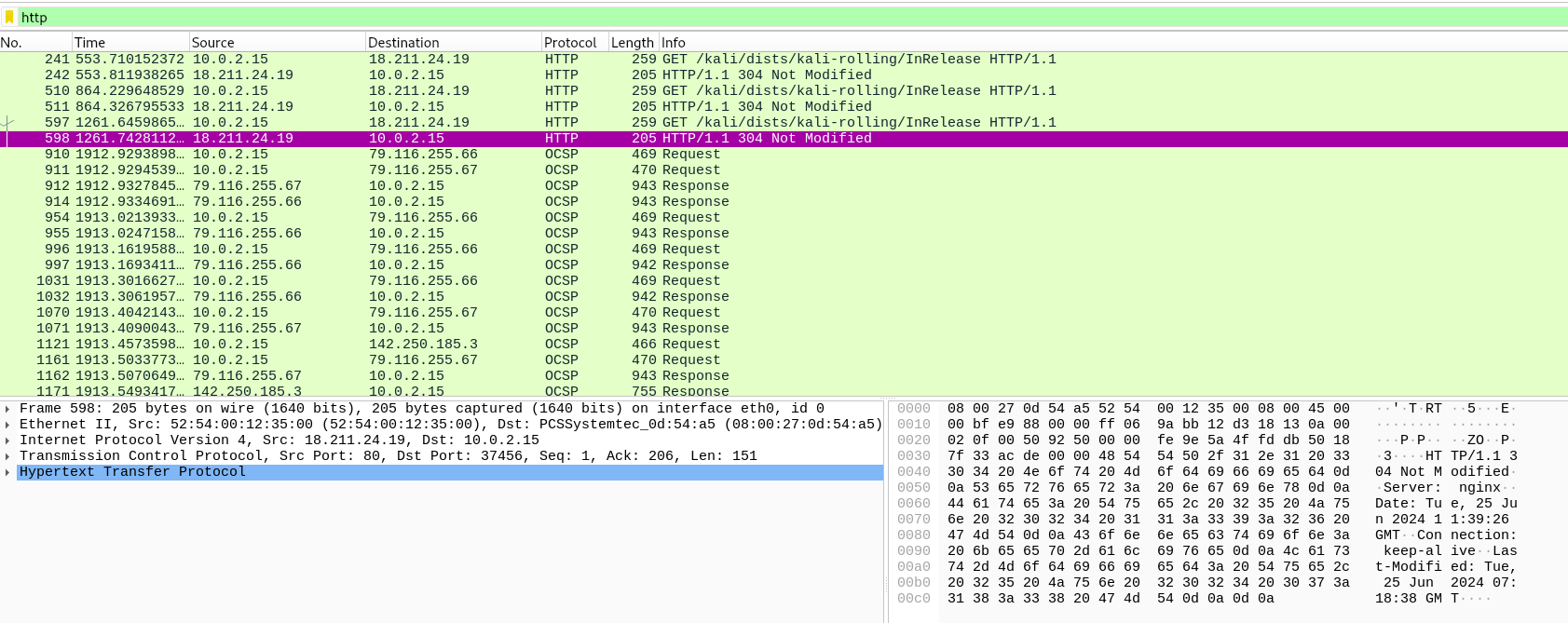


## Ejercicio 6

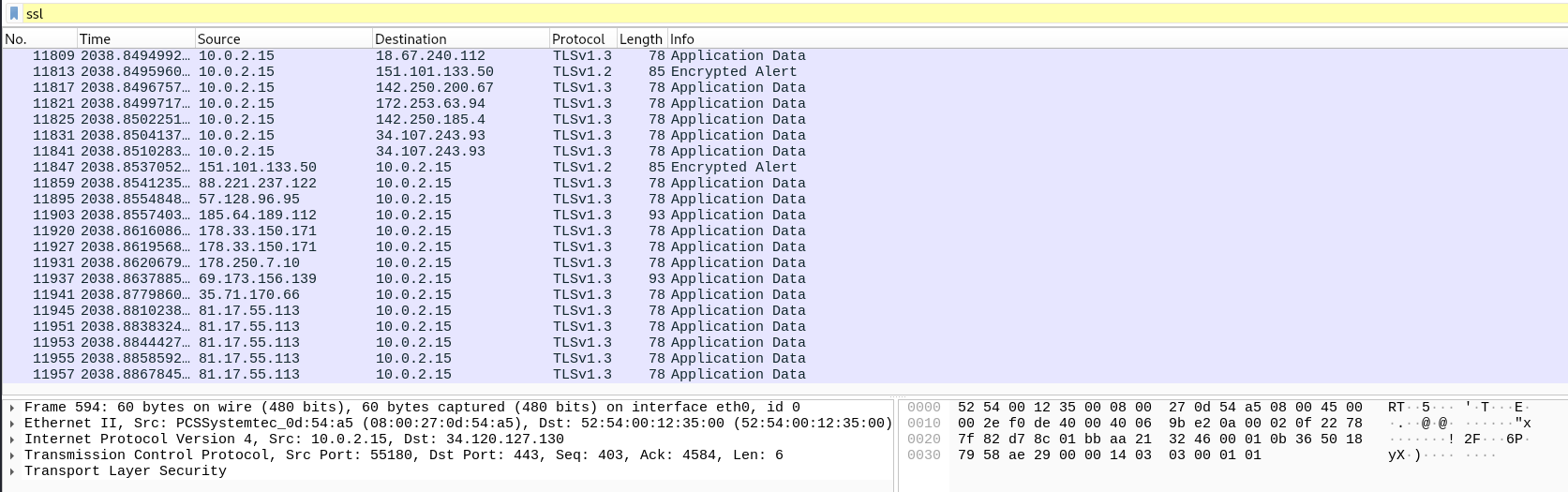
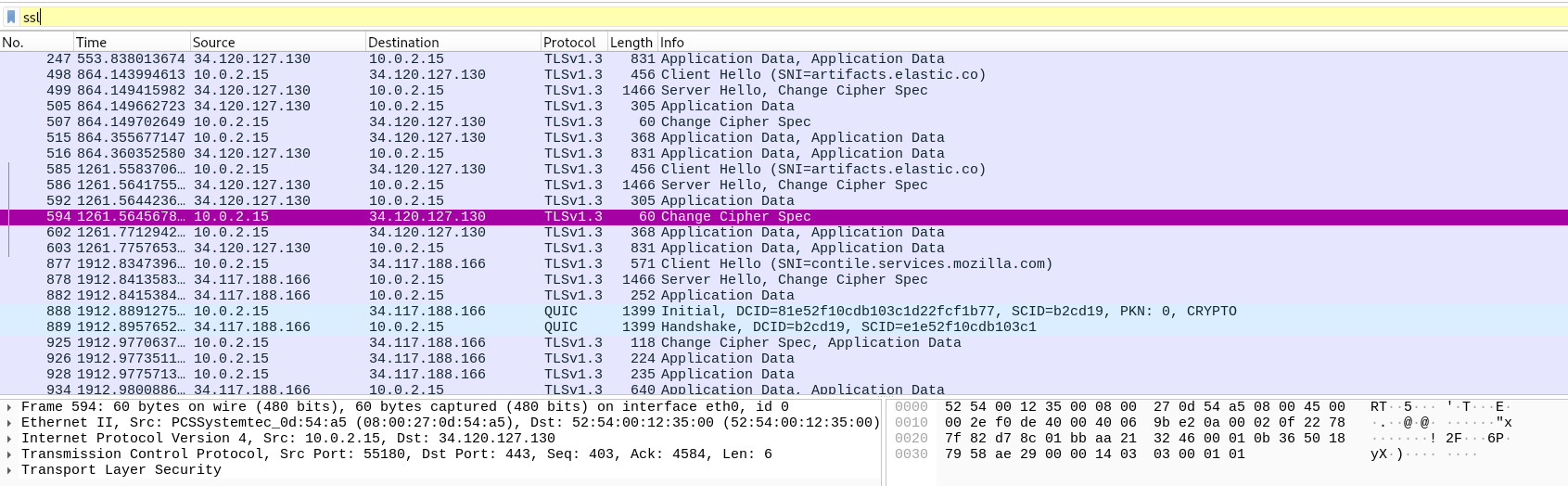
- Lo mismo http y https para páginas públicas, ¿qué se captura con Wireshark?, protocolos

cifrados y sin cifrar, mirar qué filtros de Wireshark son los apropiados a utilizar

**Navega hacia sitios web que utilicen HTTP en tu navegador desde Kali Linux.**



**Para capturar tráfico HTTPS, necesitarás configurar Wireshark para que pueda analizar el tráfico SSL/TLS. Escribe ssl en el campo de filtro**

****