github/truerandom

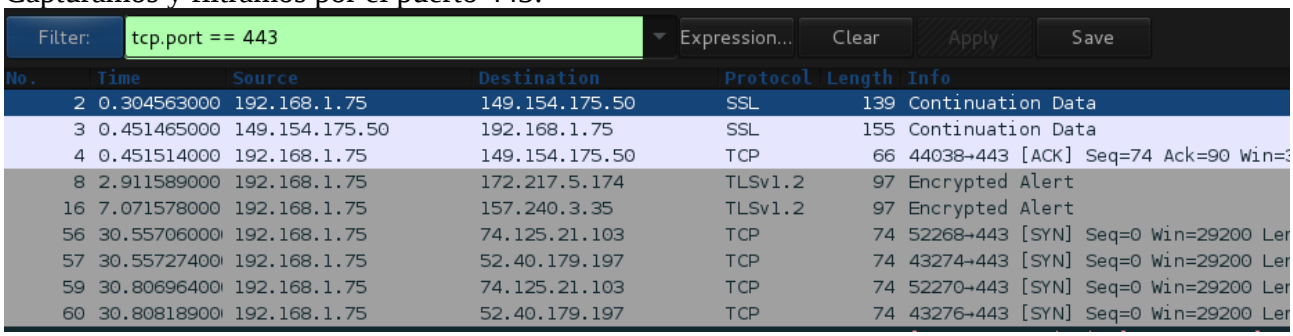
Definimos la variable de entorno, ella apunta al archivo donde se guardara el intercambio Diffie-Hellman

```
chaos@chaos:~/Criptografia/p7$ pwd
/home/chaos/Criptografia/p7
chaos@chaos:~/Criptografia/p7$ export SSLKEYLOGFILE='/home/chaos/Criptografia/p7/secrets.txt'
```

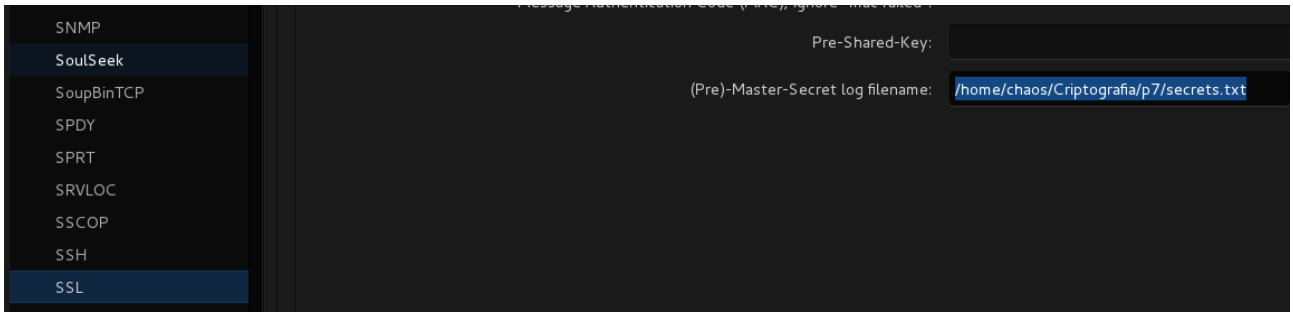
Ejecutamos wireshark:

```
chaos@chaos:~/Criptografia/p7$ pwd
/home/chaos/Criptografia/p7
chaos@chaos:~/Criptografia/p7$ export SSLKEYLOGFILE='/home/chaos/Criptografia/p7/secrets.txt'
```

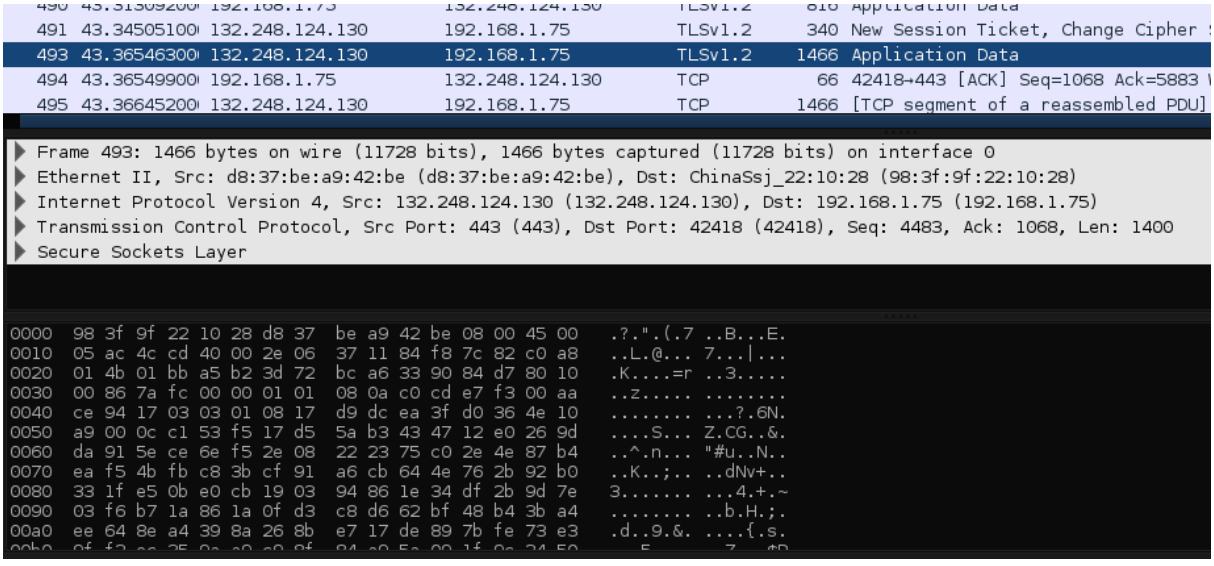
Capturamos y filtramos por el puerto 443:



En la terminal donde definimos la variable, iniciamos firefox y navegamos en la pagina analizar (en este caso fue seguridad.unam.mx):
Pasamos el archivo con la llave

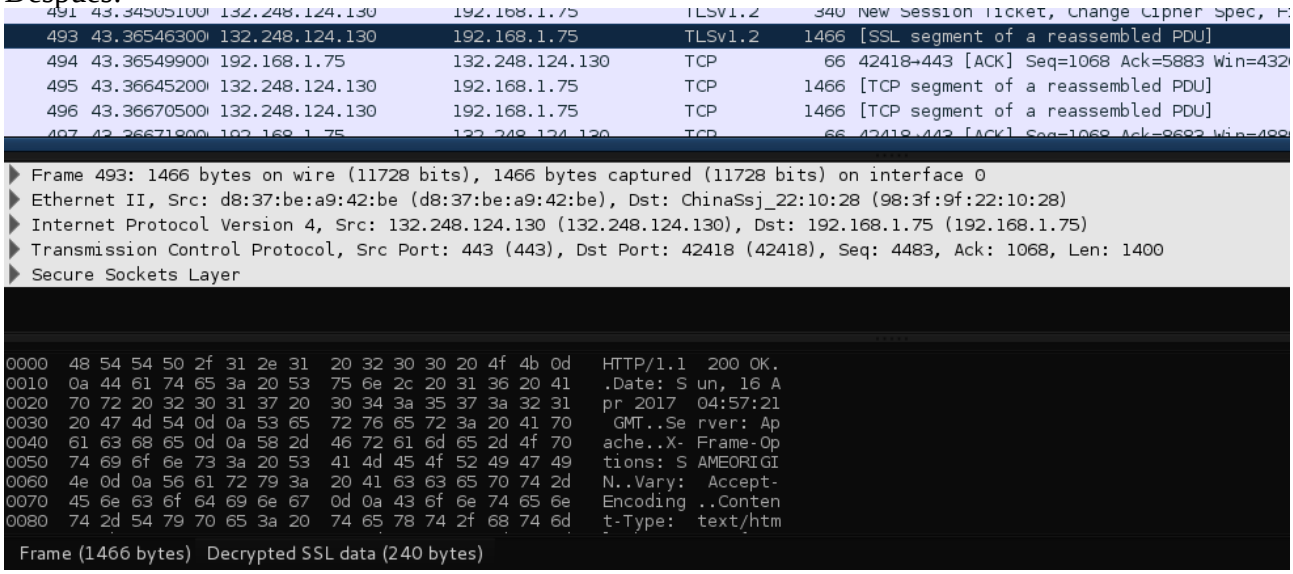


Comparacion de los paquetes antes y despues:
Antes:

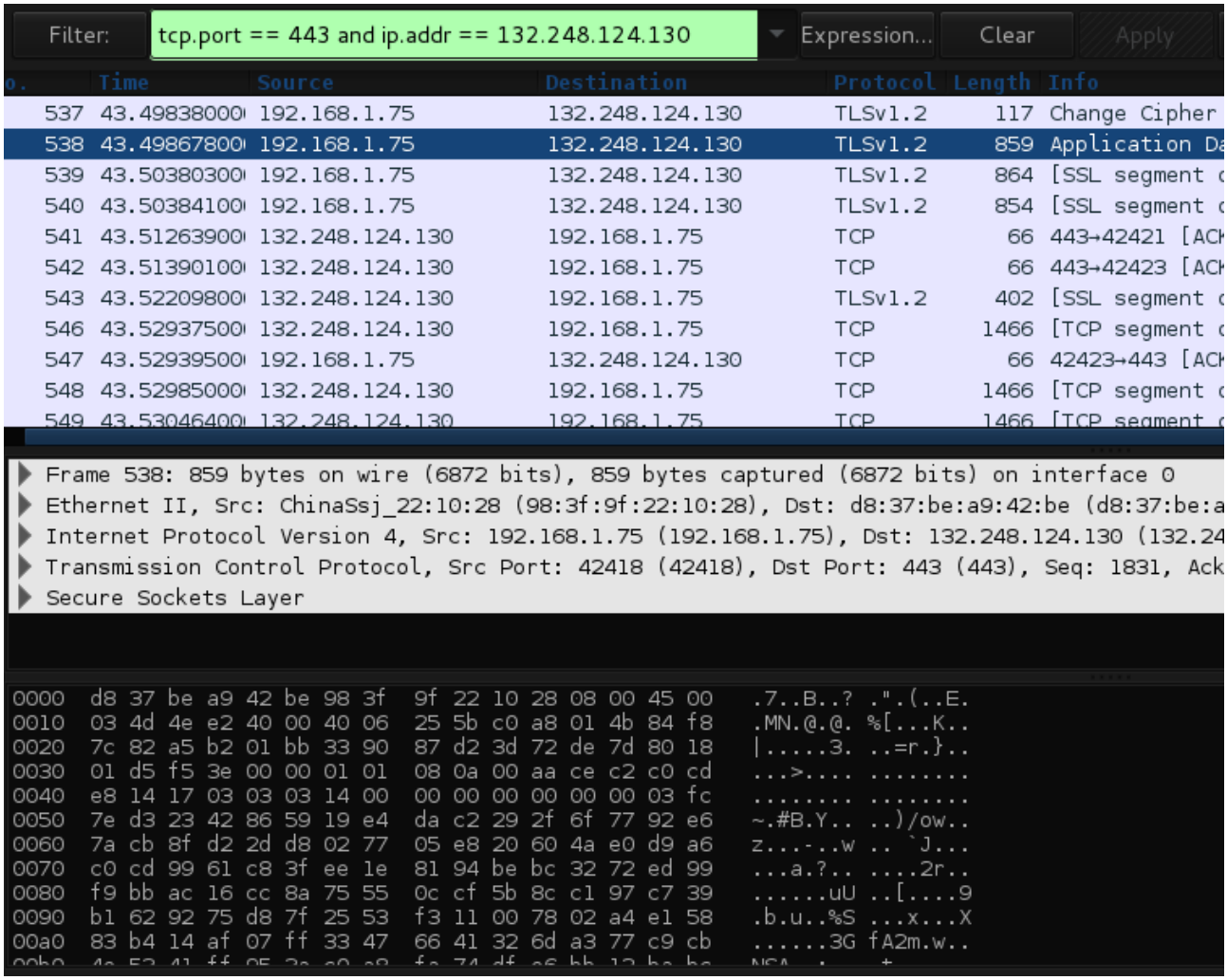


github/truerandom

Despues:



Antes:



github/truerandom

Despues: