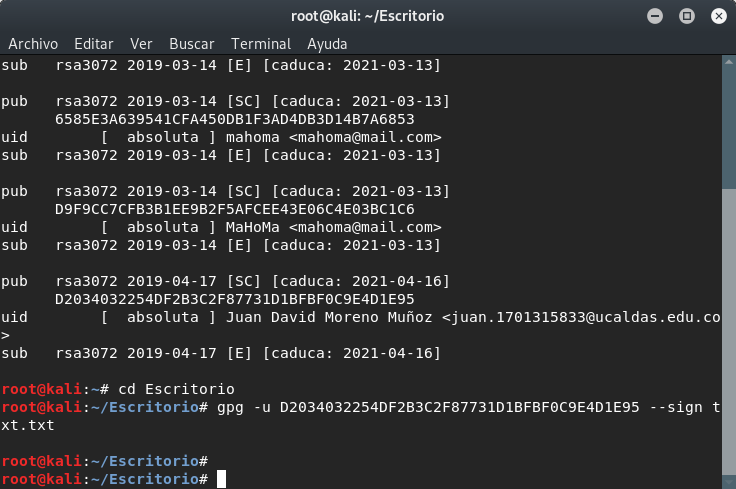
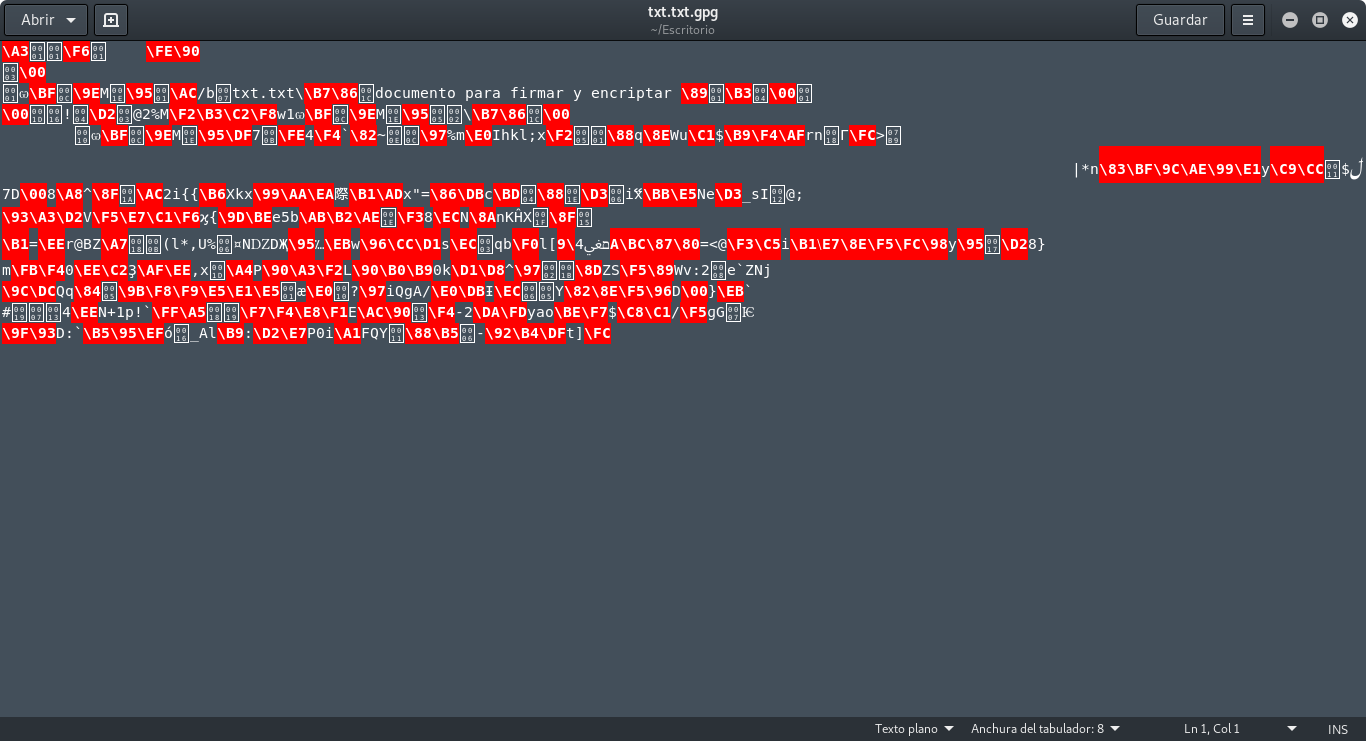
**GPG**

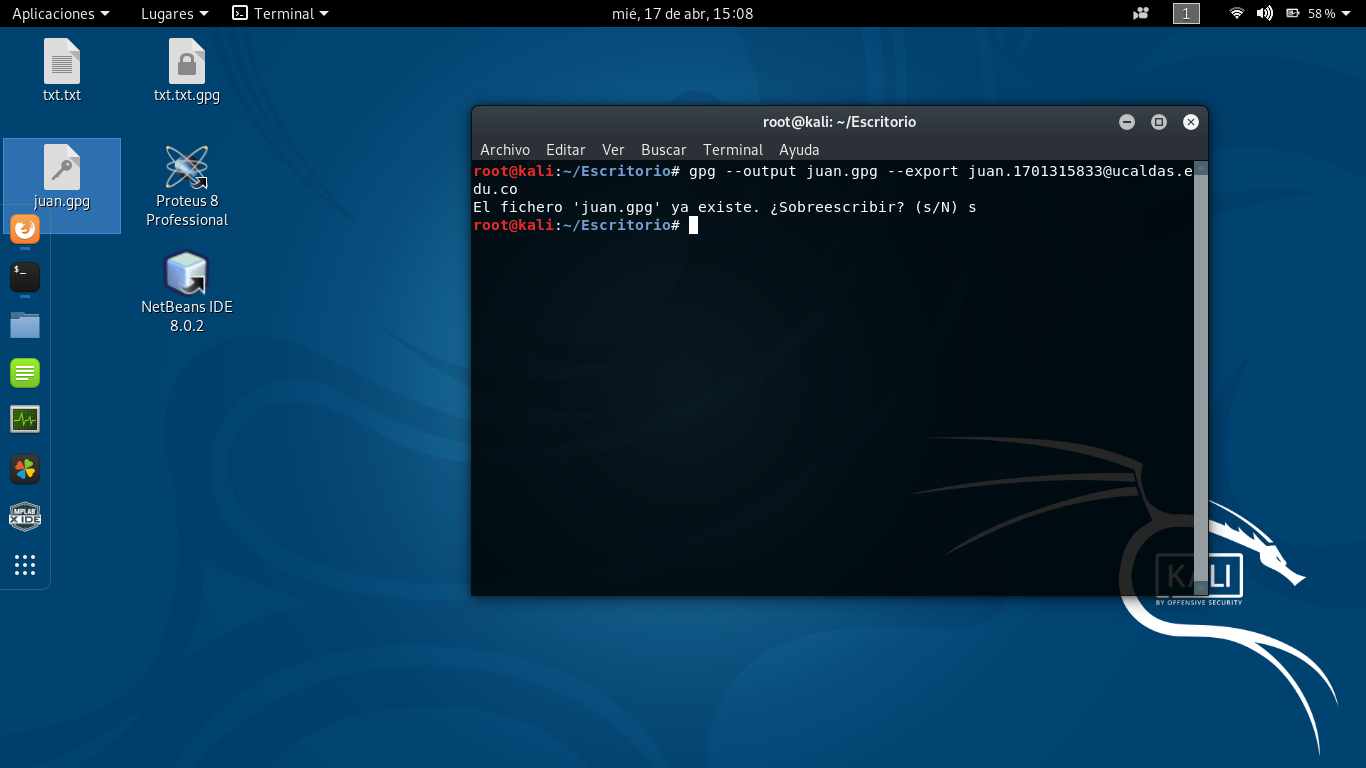
Teniendo nuestra llave procedemos a firmarla a traves de gpg.



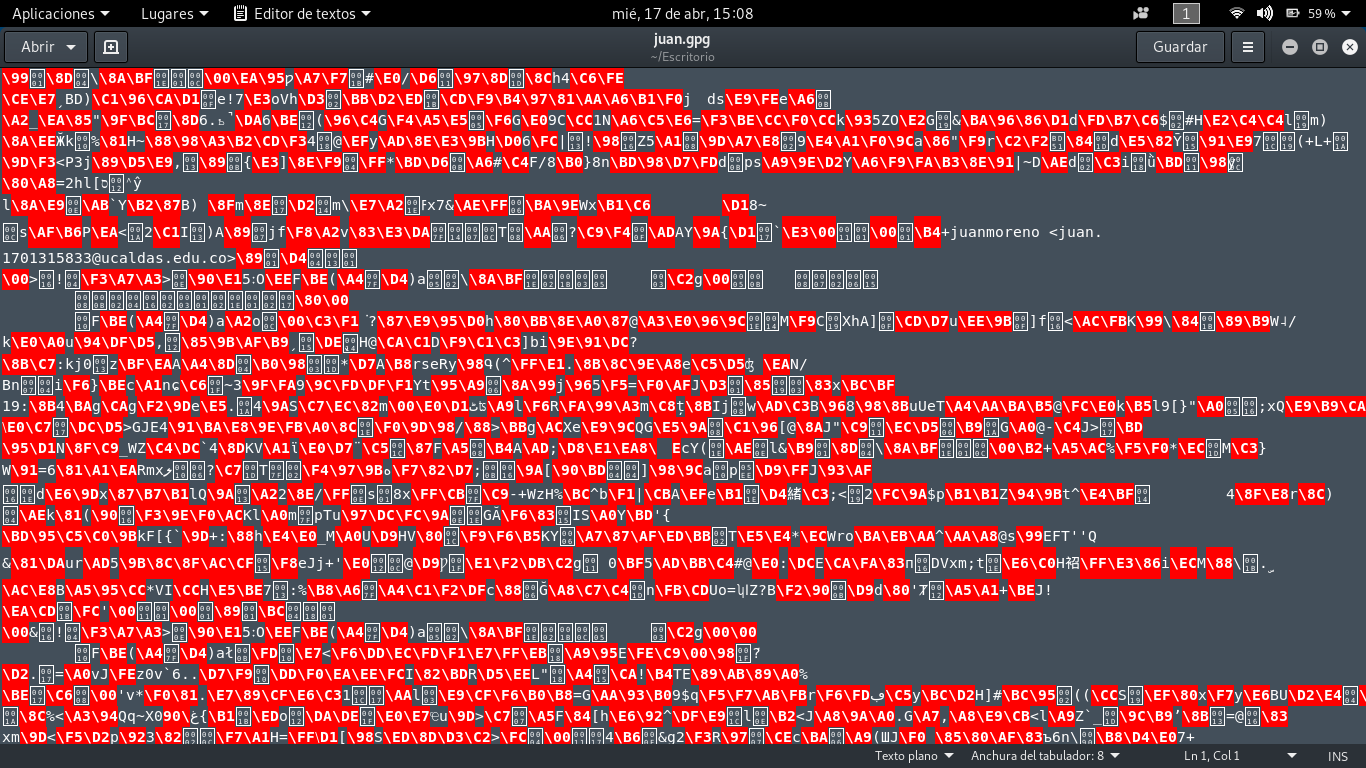
El comand o nos genera la firma de el archivo txt.txt que al abrirlo ya se ve de la siguiente forma.



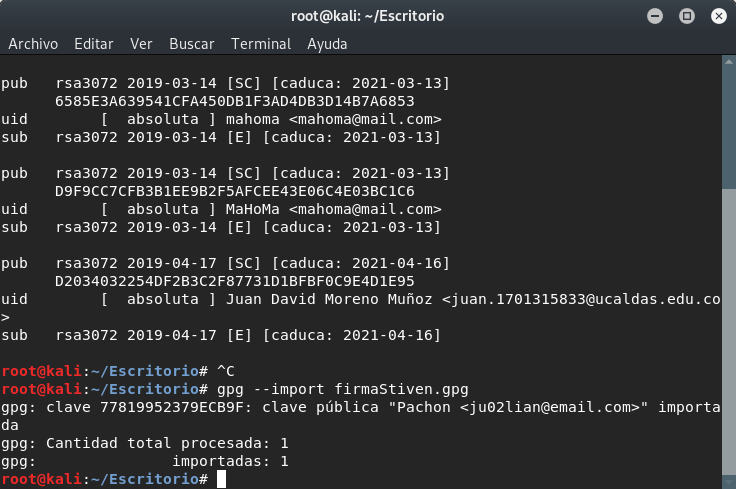
Teniendo el documento firmado procedemos a exportar la clave par aquel que quiera verificar la firma del archivo.



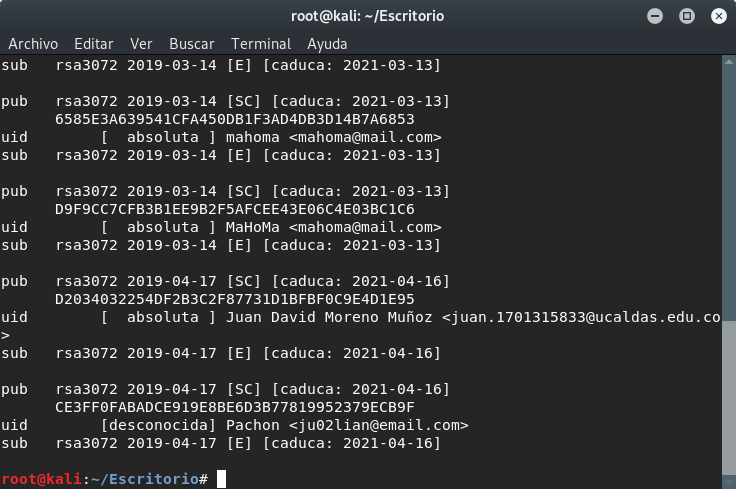
Nos entrega la firma y en el escritorio podemos preciar tambien el texto firmado en el fichero txt.txt.gpg. abrimos la firma y se ve de la siguiente manera.



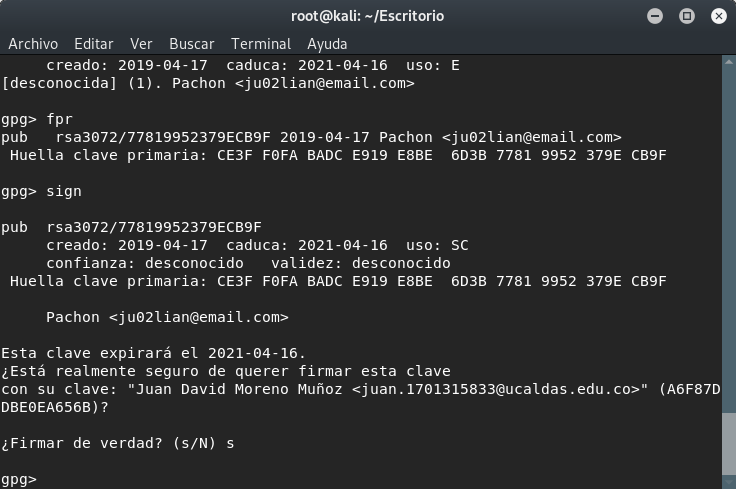
Ahora probaremos importando una llave para añadirla a nuestro llavero de confianza.

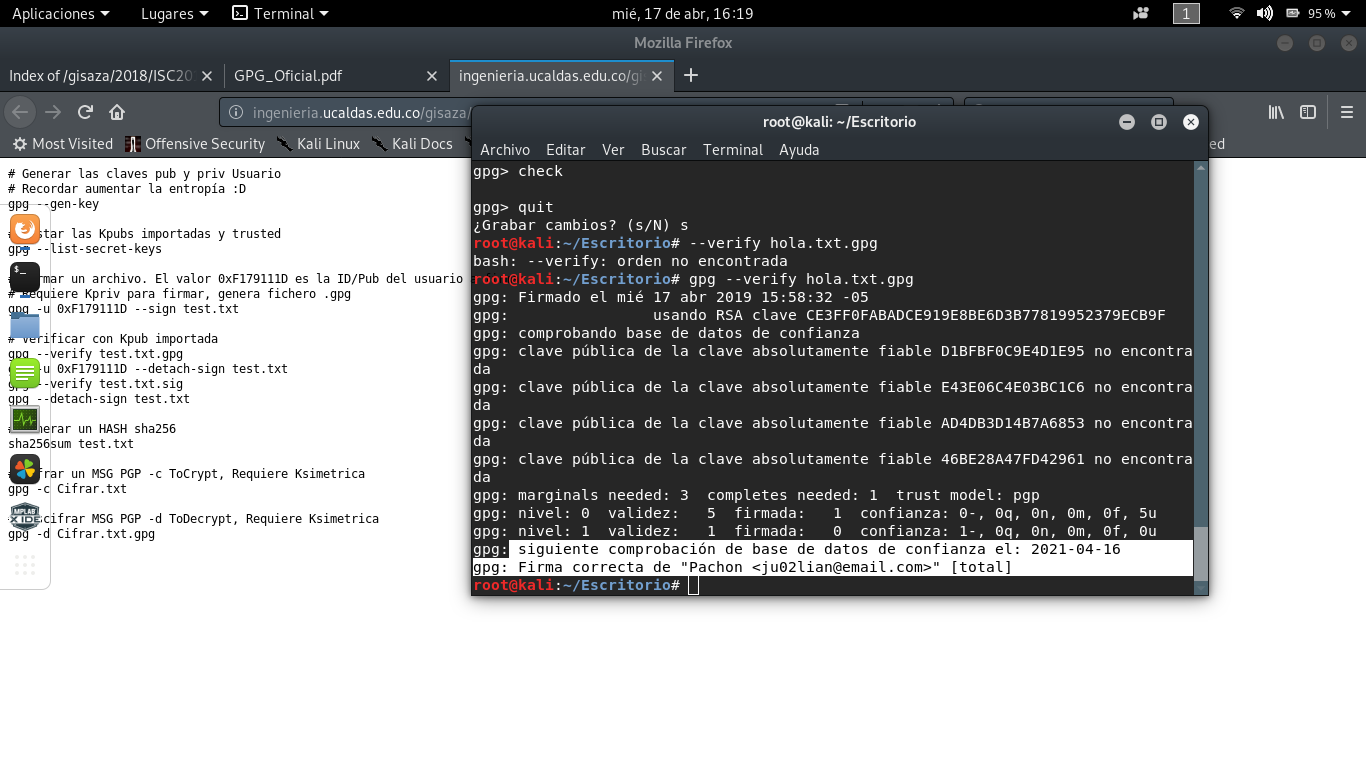


Con el comando gpg –list-keys verificamos que la firma haya sido importada a nuestro llavero.



Luego debemos hacer que gpg confie en esta llave y debemos firmarla con nuestra propia firma.

  
Posteriormente procedemos a verificar la firma del fichero y como resultado nos dira si es confiable o no lo es.

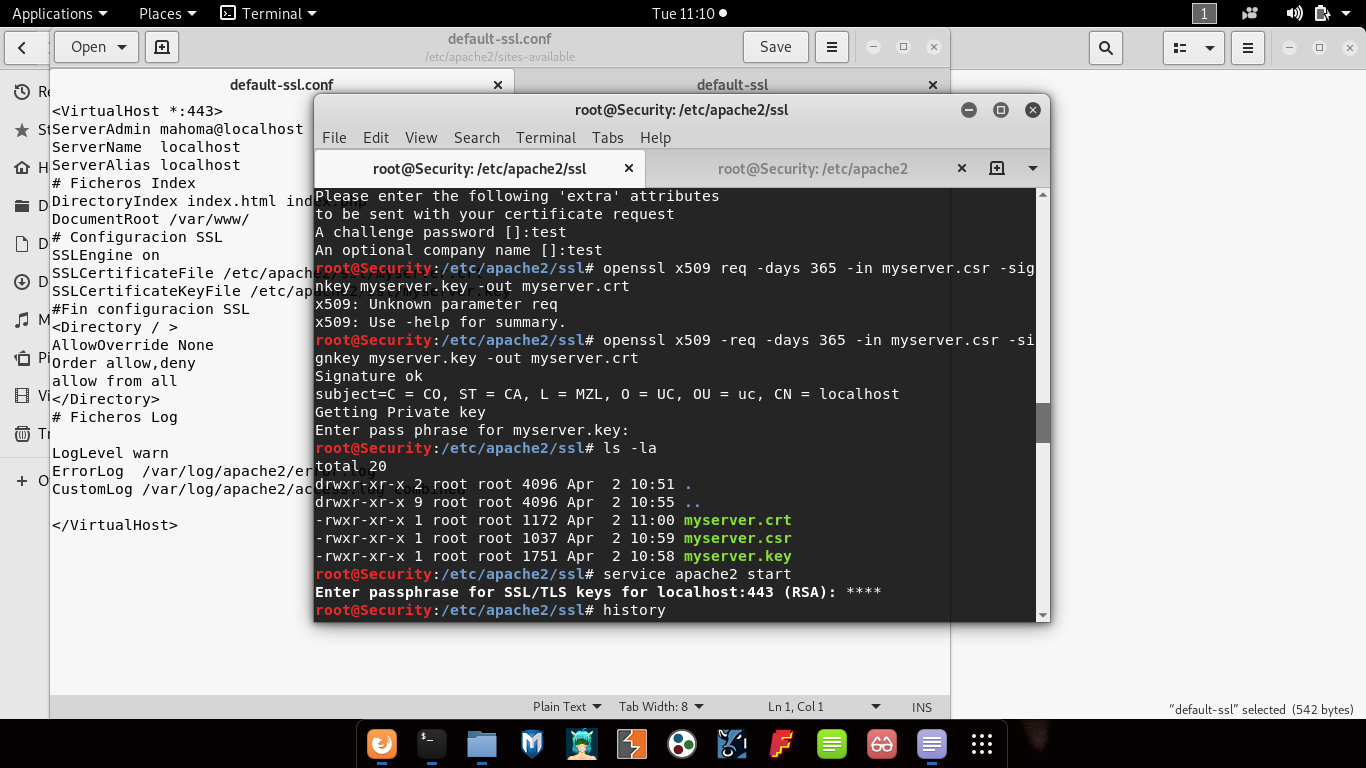


Como resultado nos arroja que la firma es confianble.

Open SSL

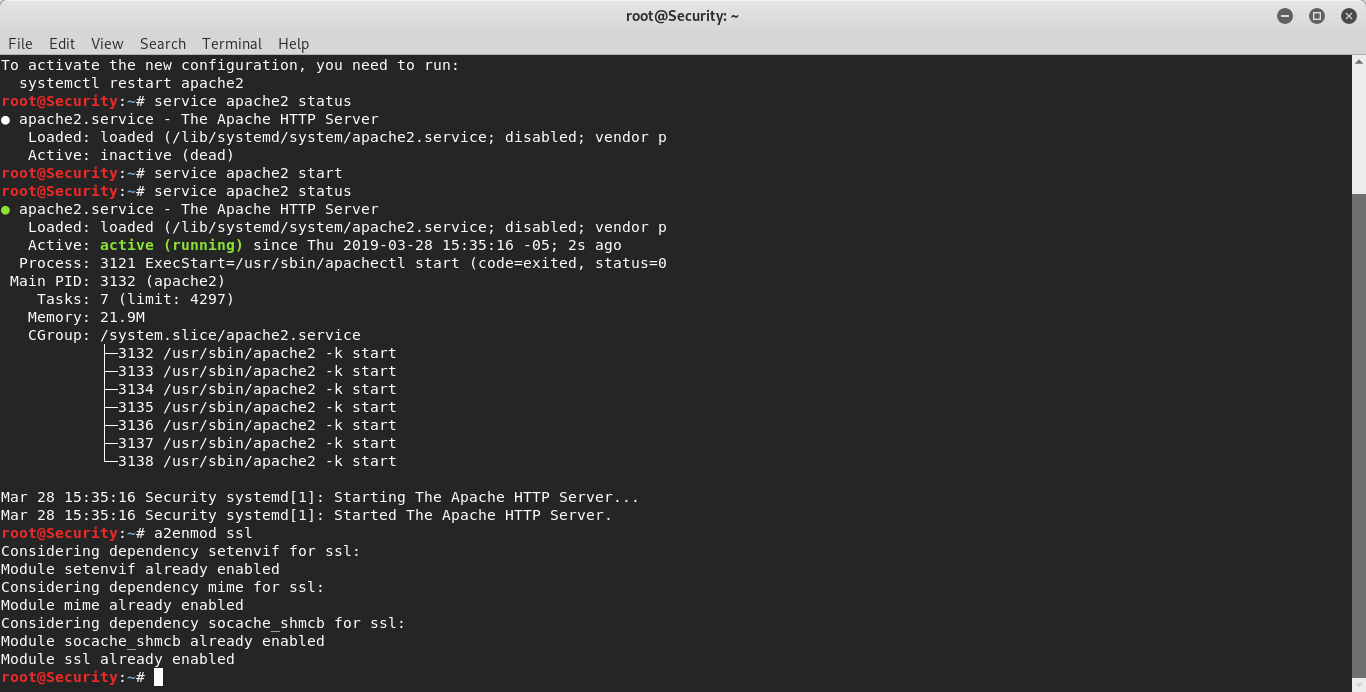
Lo primero que hacemos es general una clave para lo que sera nuestro server, la cual se generará a través de RSA.

  
Luego debemos configurar lo que serán los datos del certificado de autenticidad en la conexión al servidor.

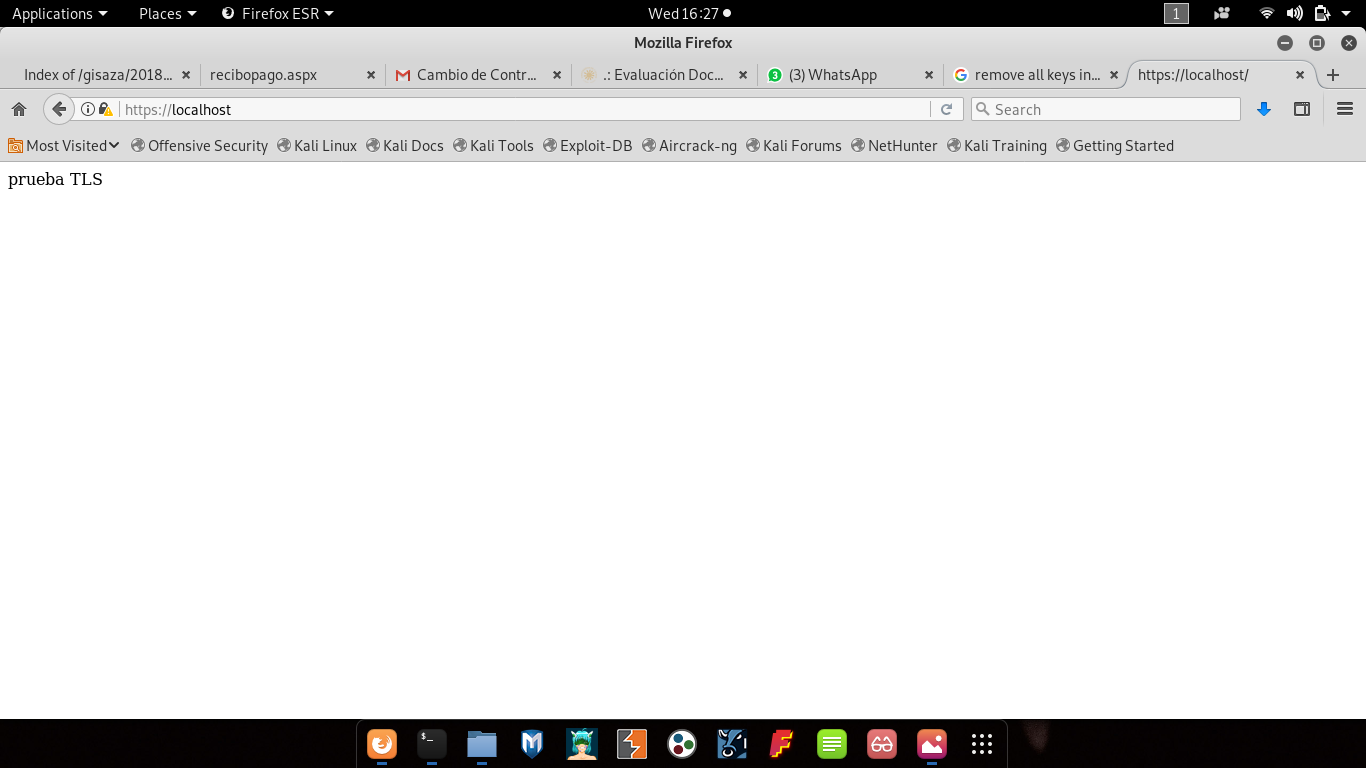


Podemos observar que ya se ha generado la clave y el certificado.

Luego ponemos en marcha nuestro servidor apache para probar la conexión.

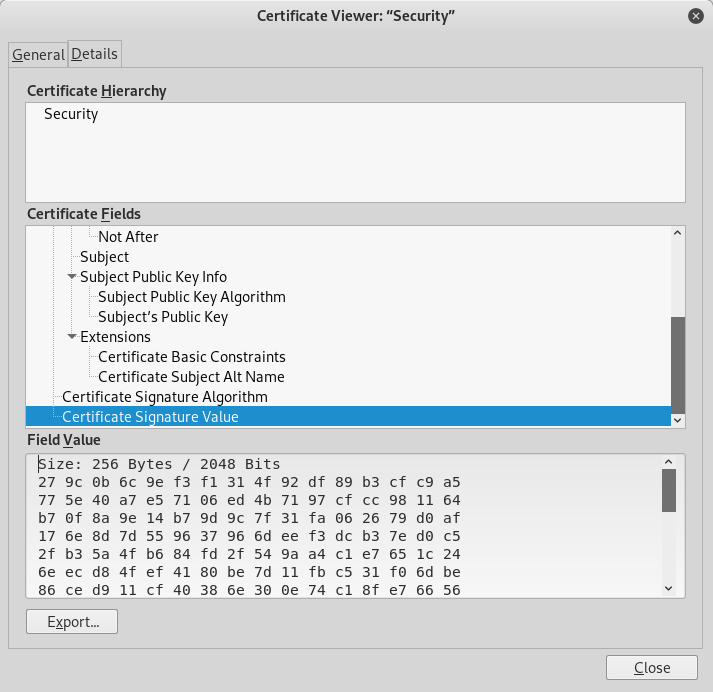


Ahora que el servicio estáen marcha verificamos que si haya conexión a nuestro index.

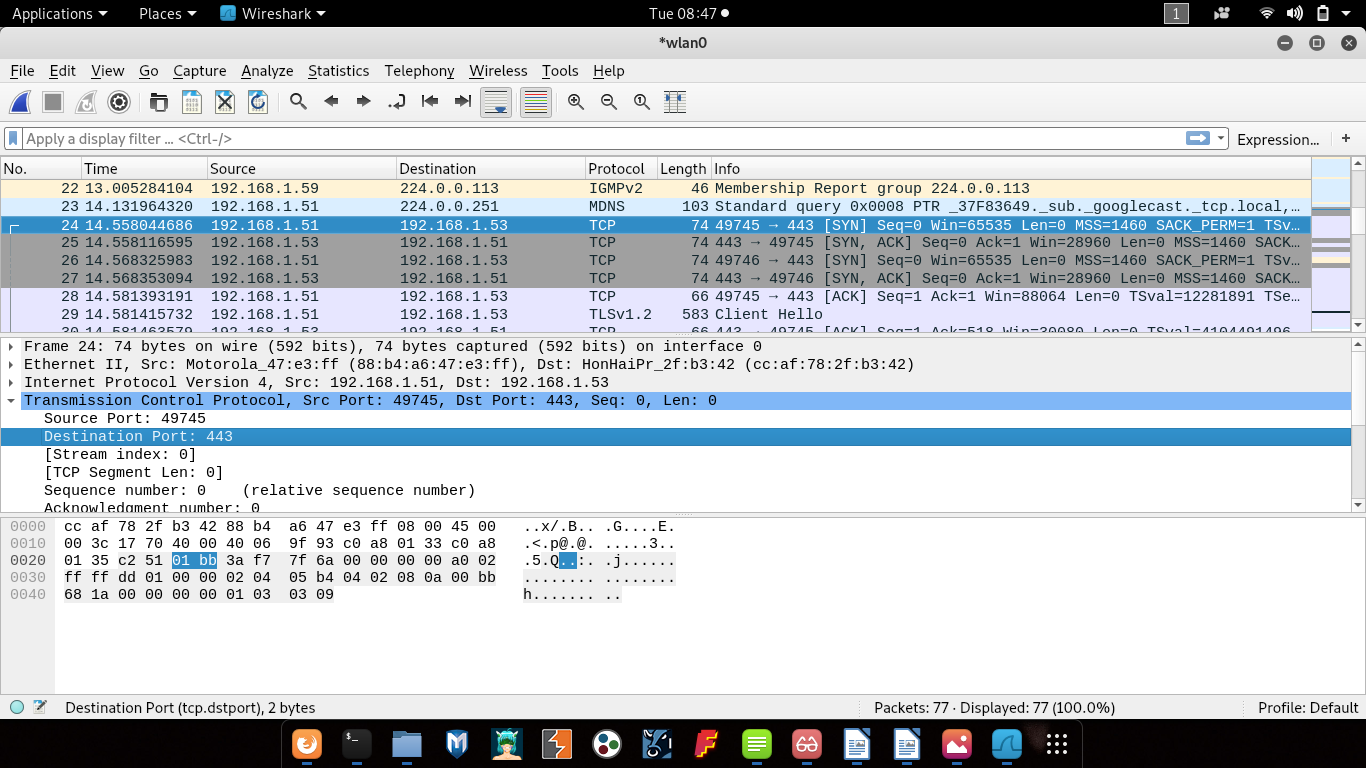


Efectivamente hay conexión y ahora tenemos que ir a verificar el certificado puesto que en primera instancia e buscador no confia en el sitio por que su certificado no ha sido generado por una CA externa.





Vemos que el certificado contiene nuestros datos y ahora el buscador confia en el sitio donde para asegurarnos que la informcion viaja de manera cifrada hacemos un pequeño sniffing en la red a través de wireshark.



UFW

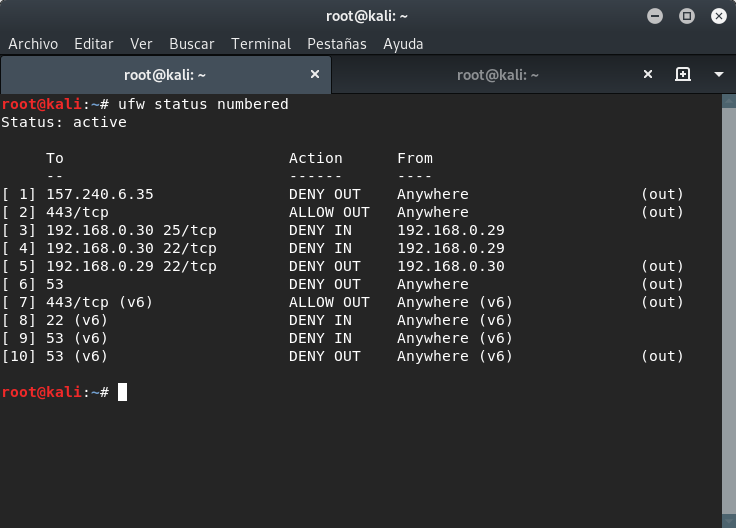
Para empezar ingresamos una serie de reglas para nuestro firewall donde epecificamos ciertas restricciones.

La regla 1 niega todo el tráfico saliente hacia la ip referenciada en la imagen que es la de Facebook.

La regla 2 acepta el tráfico saliente hacia cualquier destino https.

La regla 3,4,5 niega todo el tráfico tcp por los puertos 22 y 25 entre las iprelacionadas.

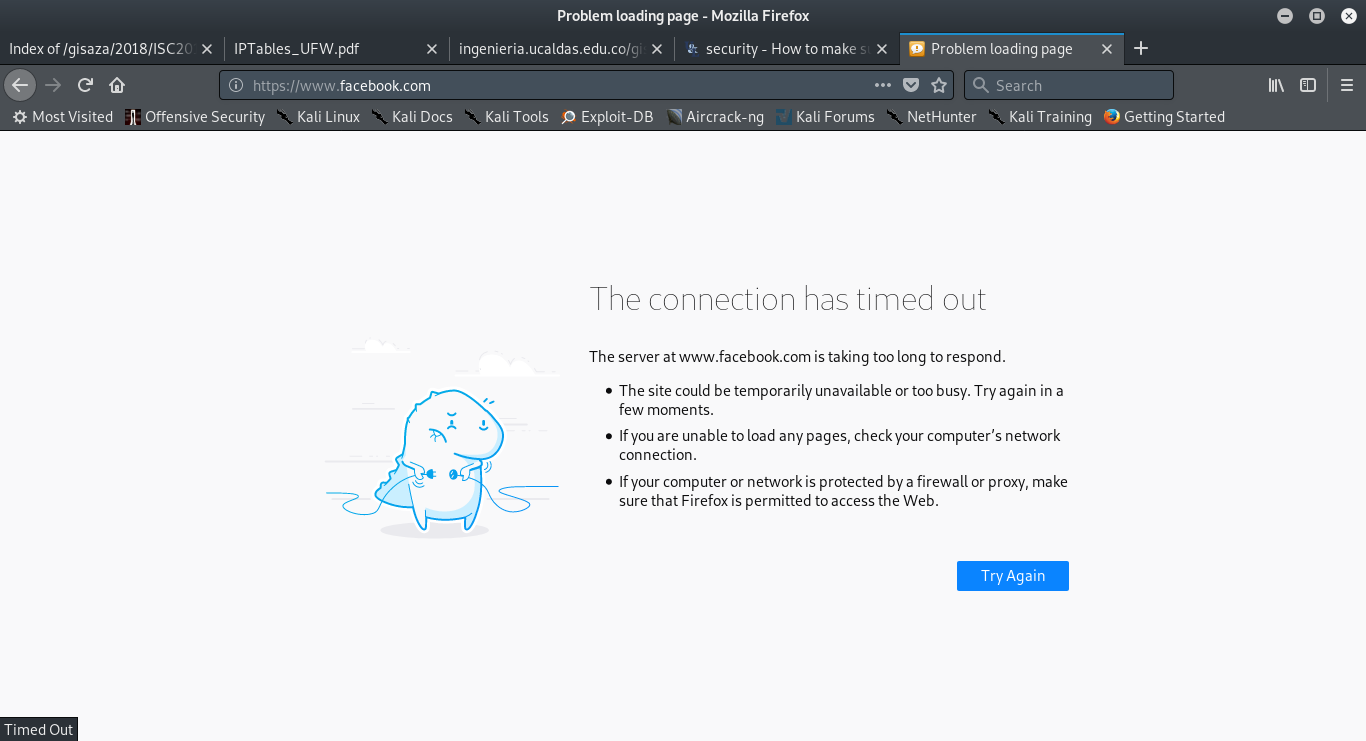
La regla 6 niega las peticiones a servicios dns.



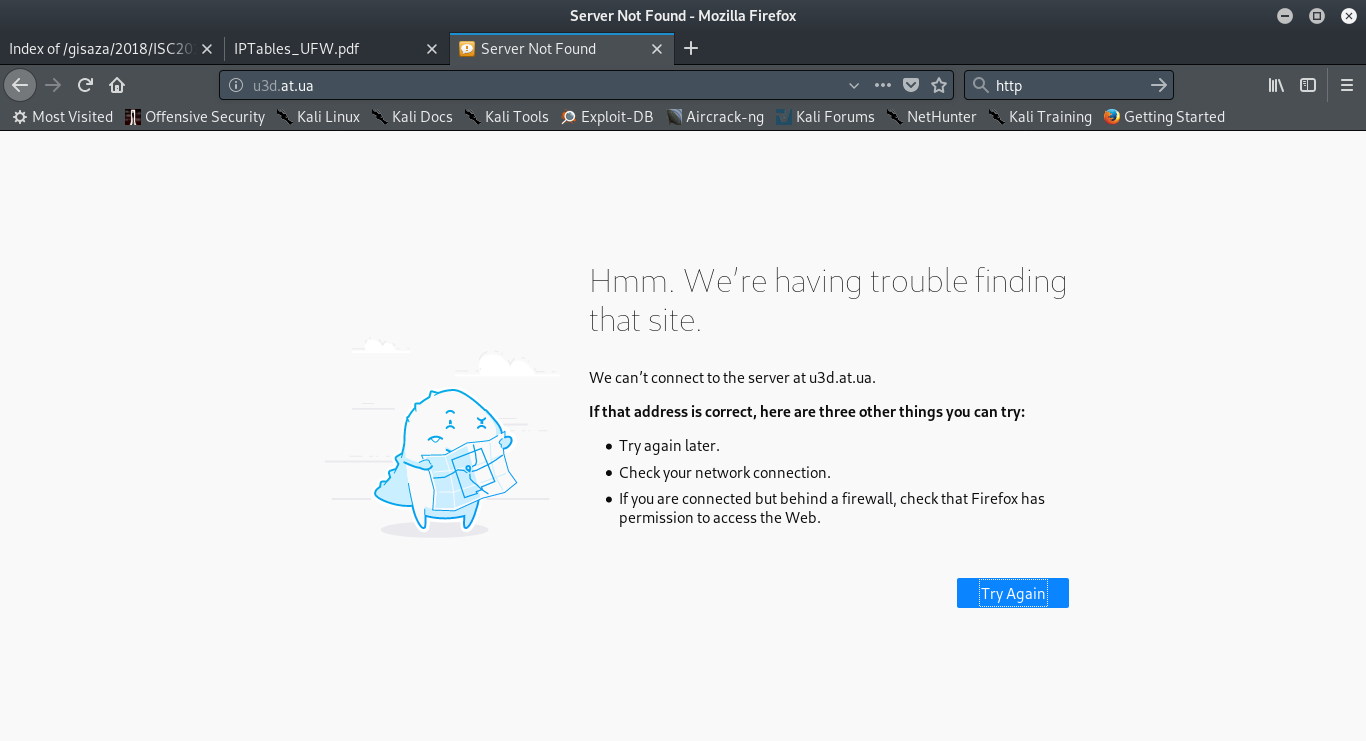
Vemos que ser permite la conexión https.



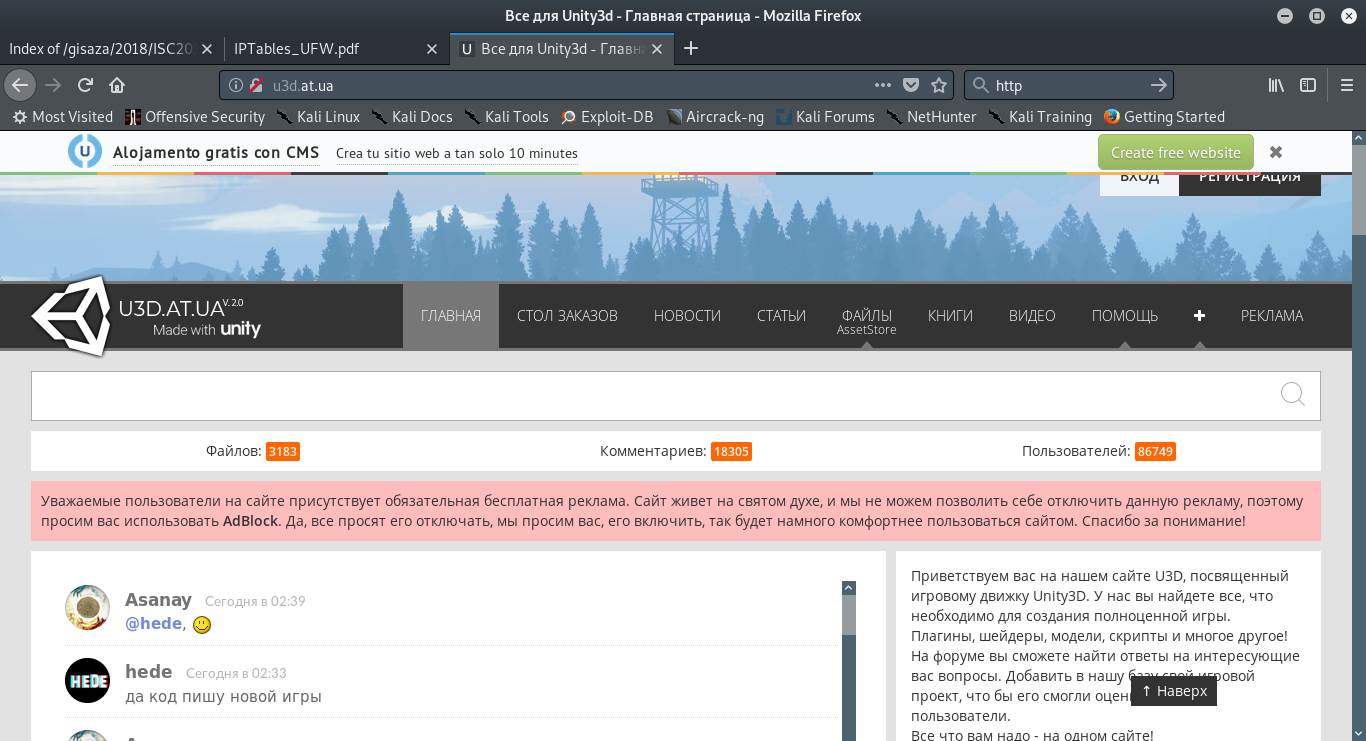
Pero vemos que no permite la conexión al sitio de Facebook.

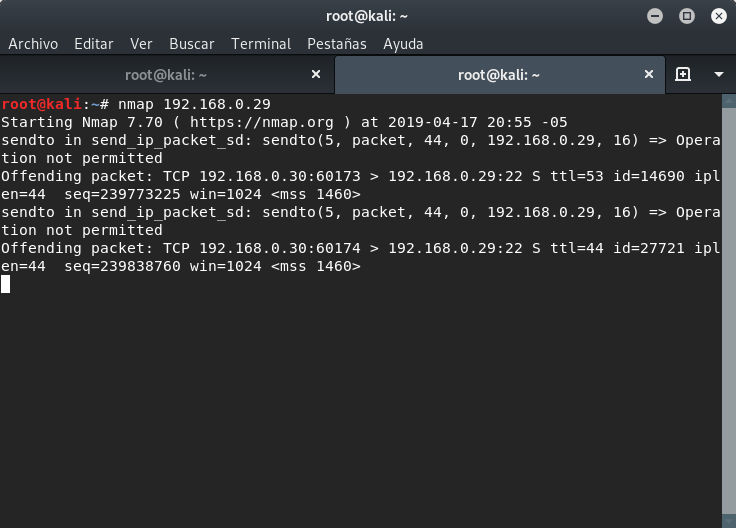


Luego accedemos a un sitio que no se ha accedido nunca y por lo tanto nuestro dns no lo conoce y vemos que esrechazado.

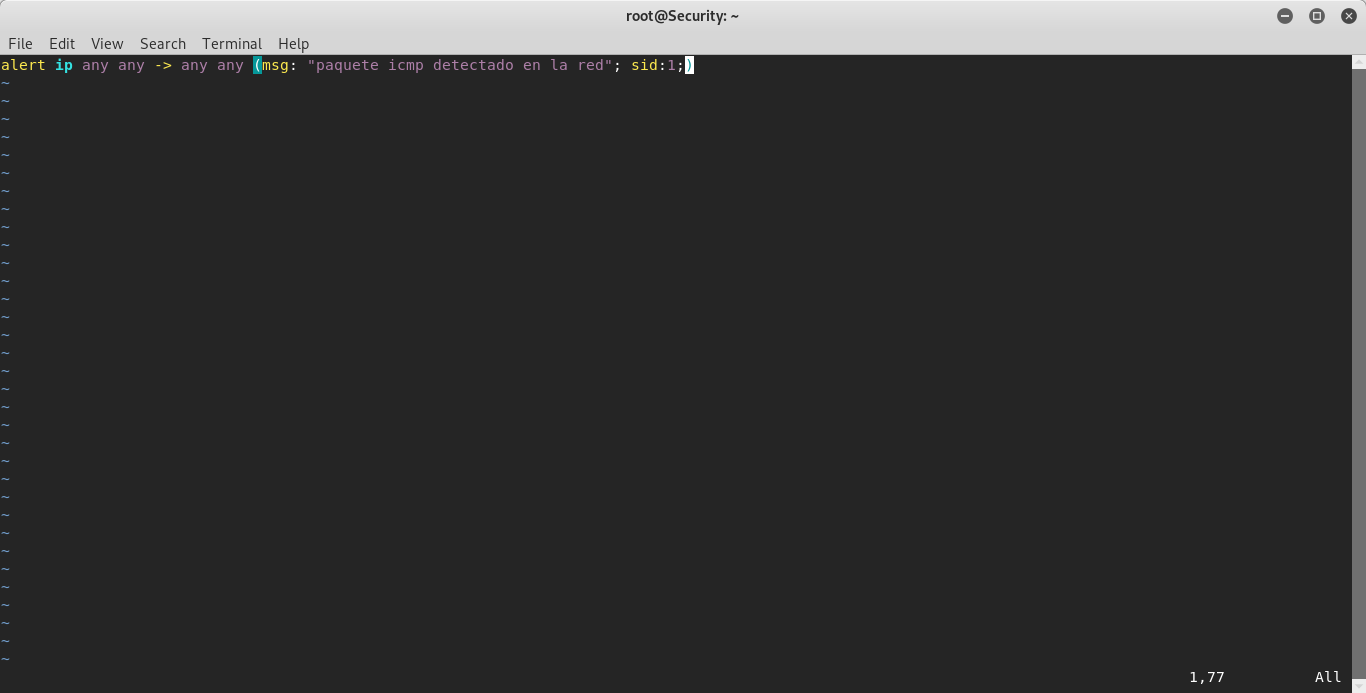


Eliminamos la regla para hacer la prueba y vemos que ahora si hay conexión.

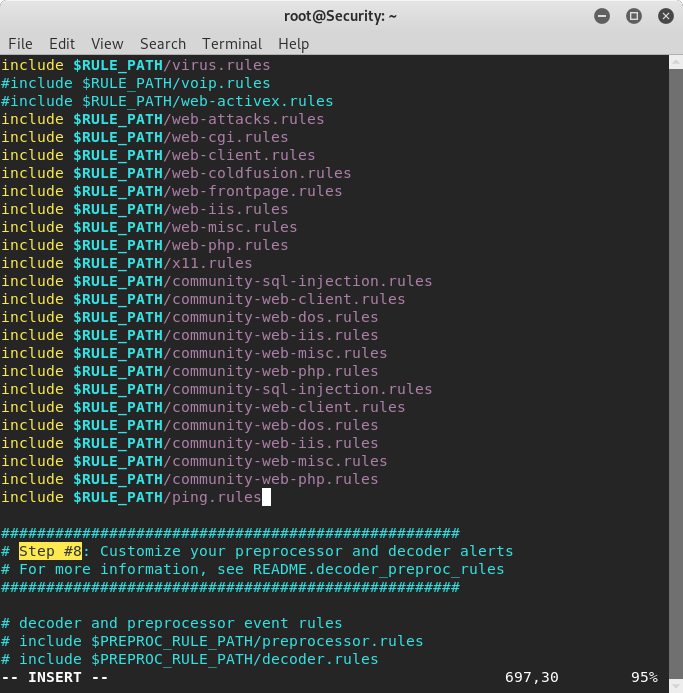
  
Con las otras reglas logramos que el pc sea no rastreable a través de un nmap lanzado a su ip.



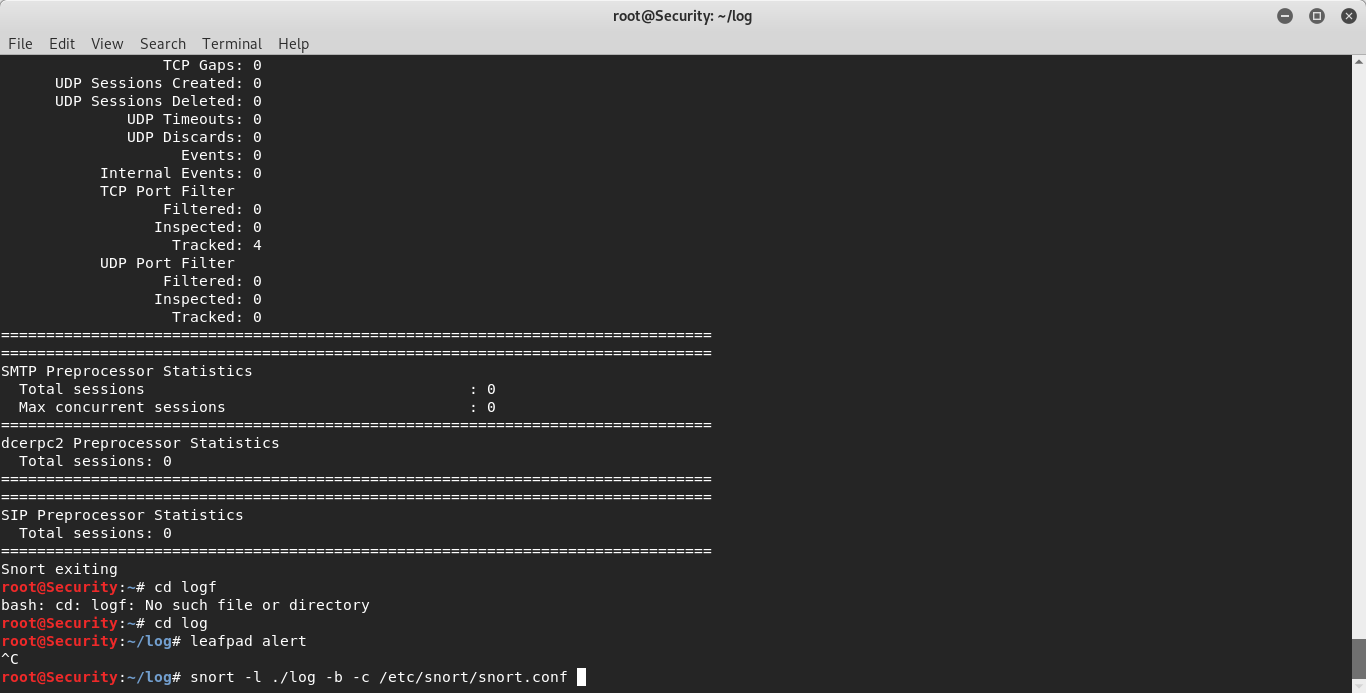
SNORT

Ceamos una regla que nos alerte sobre tráfico de paquetes ICMP en nuestra red. 

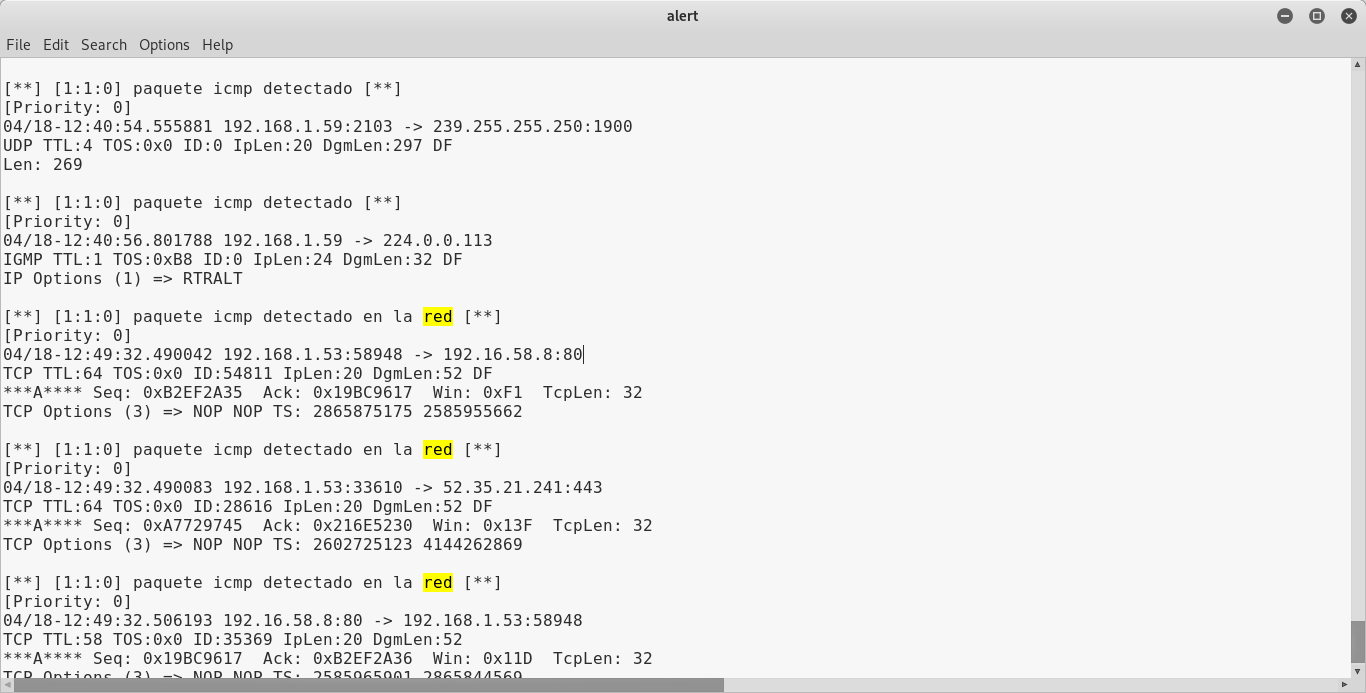
Lo guardamos en ping.rules



Abrimos nuestro archivo de log para ver si se ha lanzado alguna alerta.



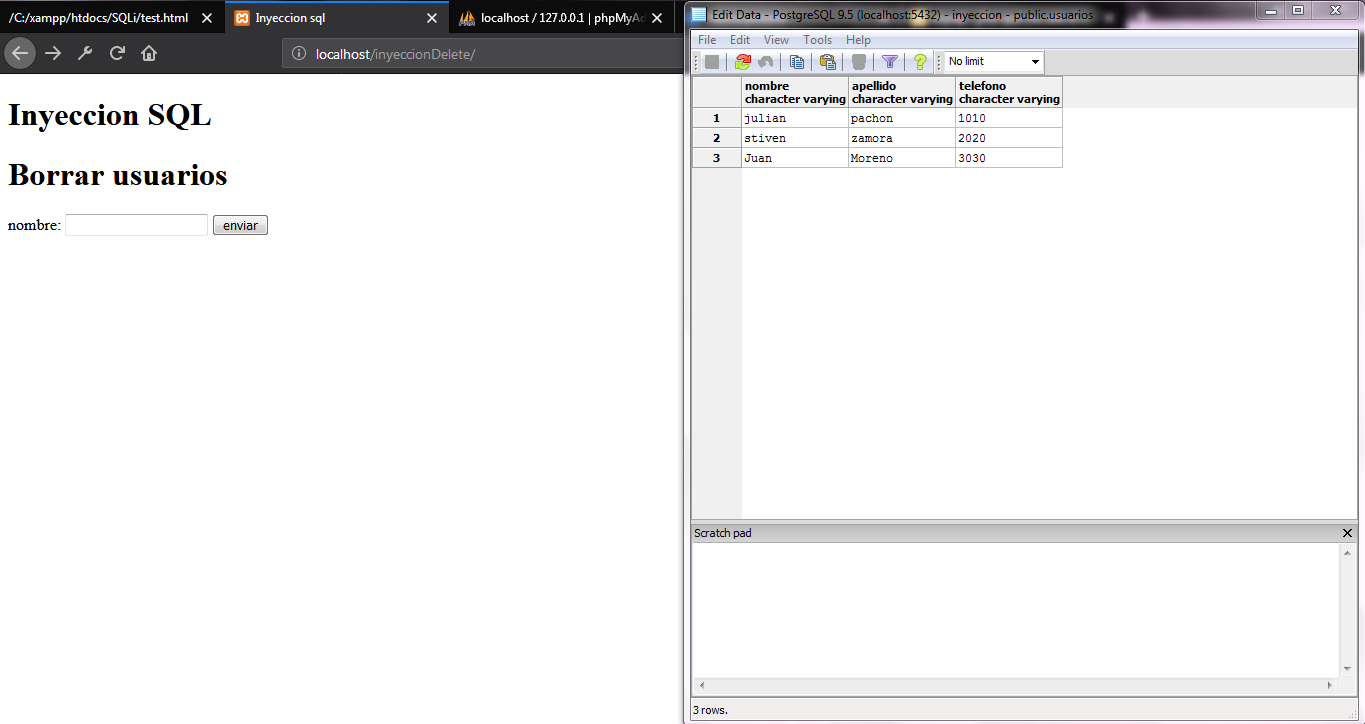
Y efectivamente vemos que ha detectado paquetes icmp en la red.



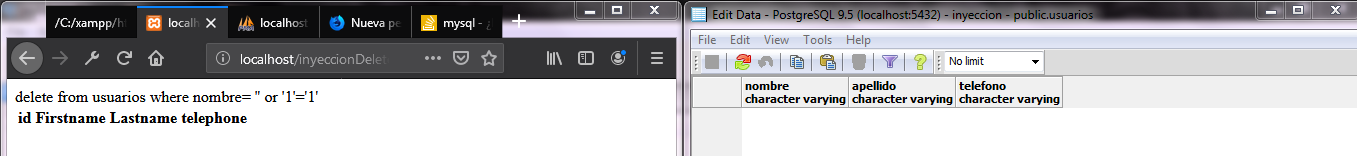
SQL INJECTION

Trabajamos en un entorno generado para la prueba compuesto de un javascript y una conexión a una base dedatos en postgresql que contiene 3 columnas con los datos de 3 personas.

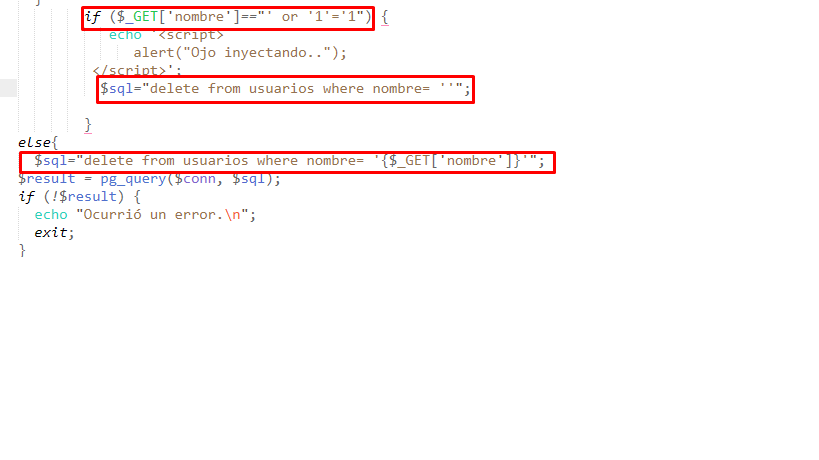
Accedemos al index que se modificó para borrar una columna donde se toma el nombre del textfield y el boton lanza el codigo sql para borrar el registro.

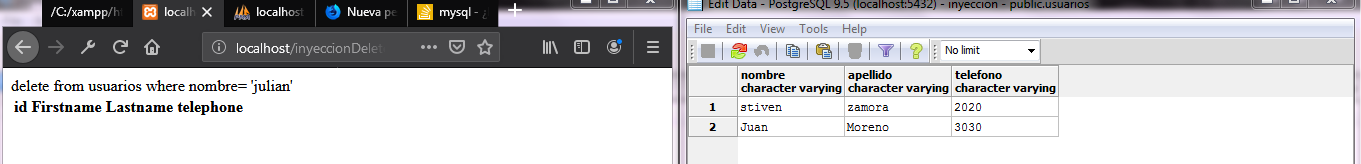


En el campo nombre ingresamos la sentencia ” or ‘1’=’1’ y como arroja verdadero borra todos los registros de la tabla.

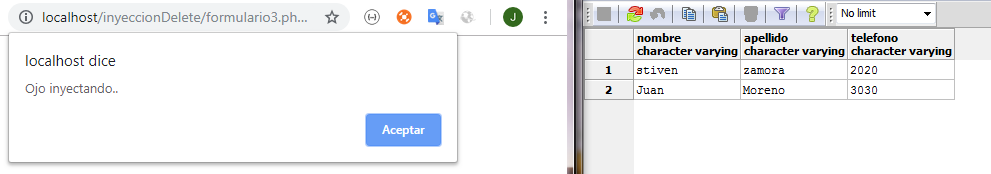


Para que no ser permitan ataques de este tipo se modifica el código de tl forma que reconozca la sentencia de inyección y envie una alerta, ademas de no permitir lanzar la sentencia y enviar una consulta vacia, de lo contrario tome el nombre y lo elimine.

Tratamos de eliminar por nombre y nos deja.

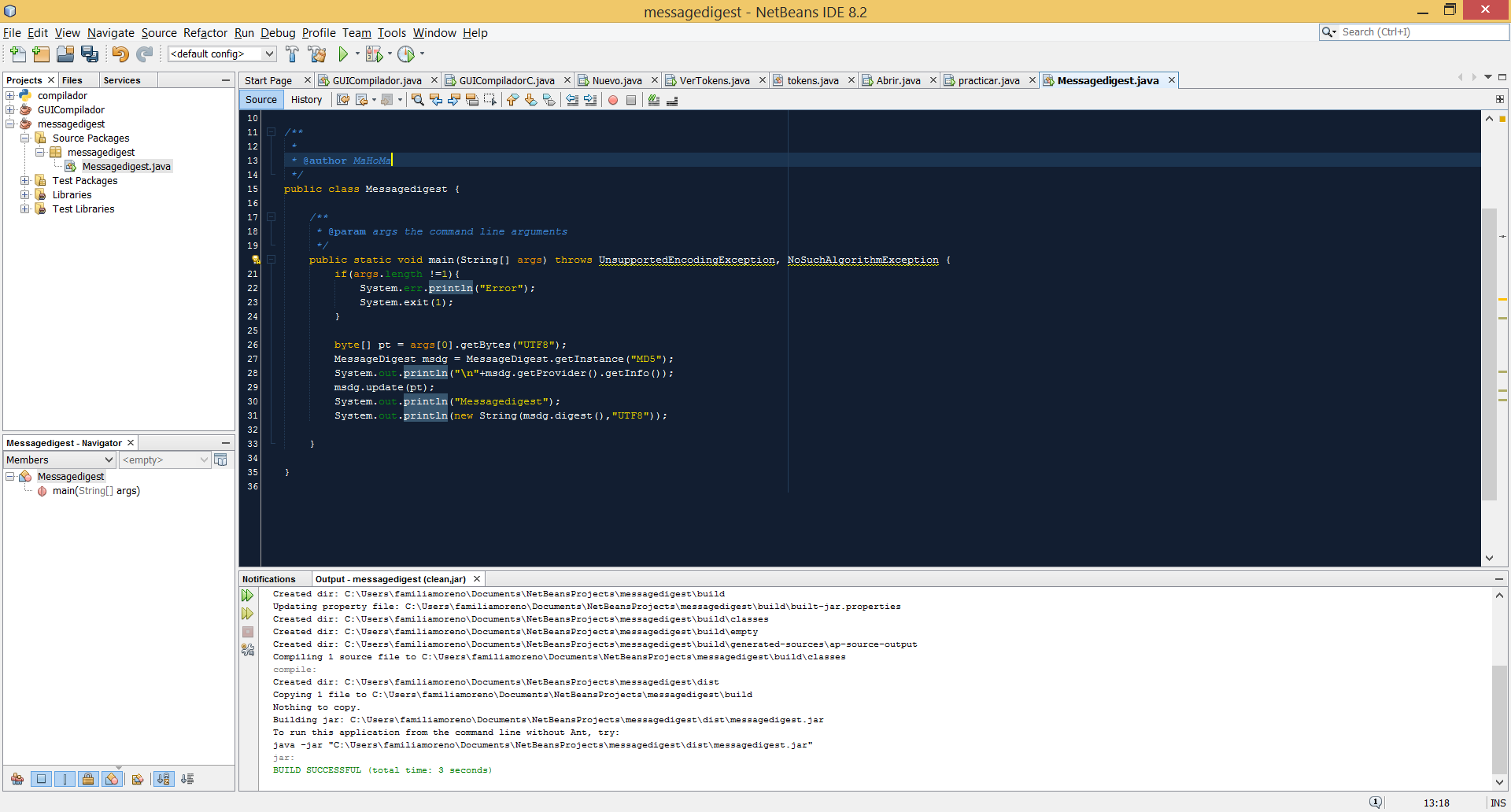


Observamos que lanza la alerta cuando no es un nombre lo que tenemos en el campo nombre.

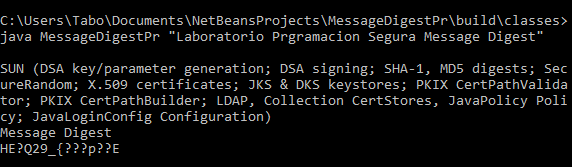


JAVA SECURITY

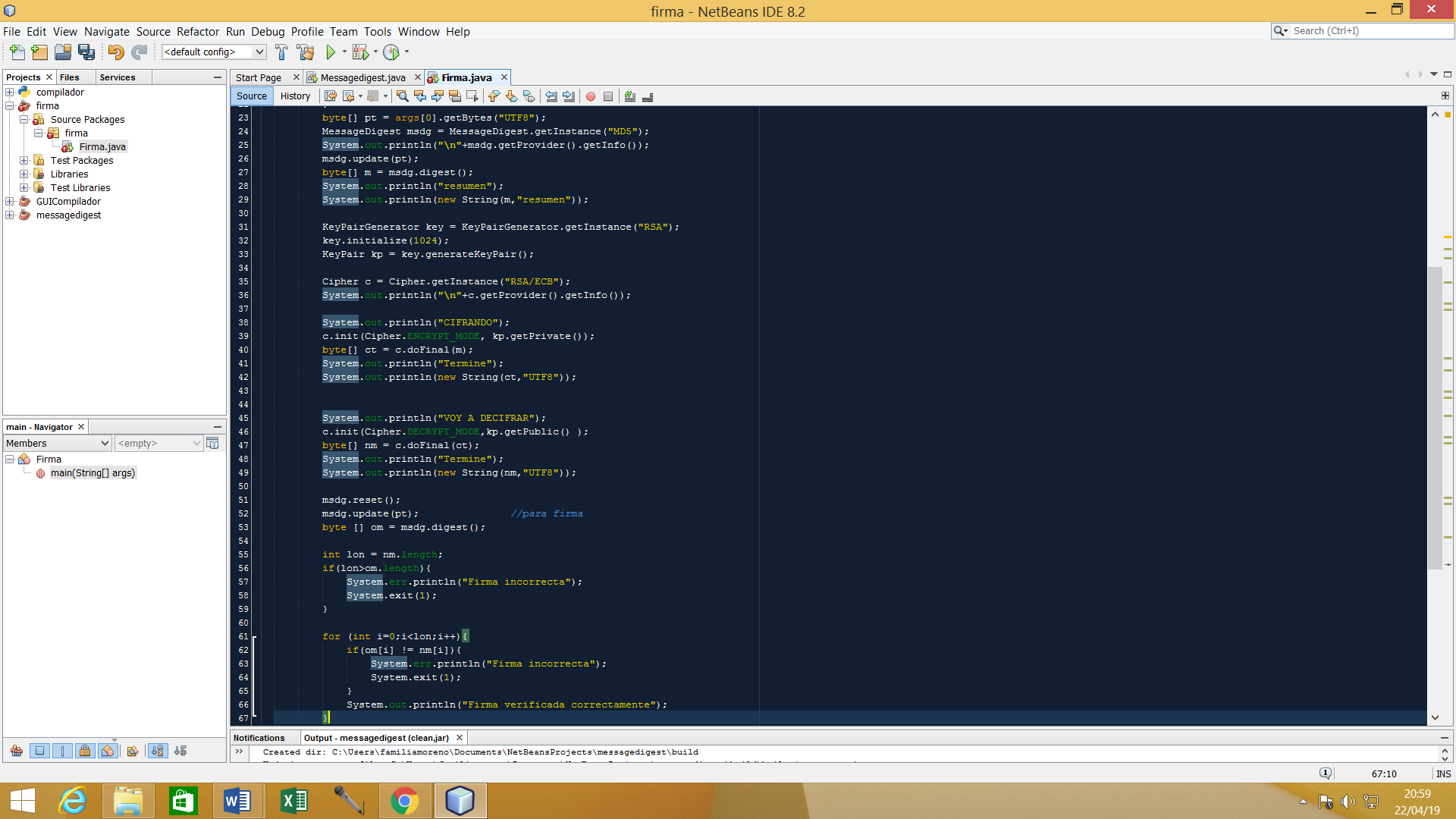
Resumiendo un mensaje



A través de la consola enviamos el argumento y nos arroja el resultado



Firmando y verificando



Compilamos y obtenemos el resultado

