

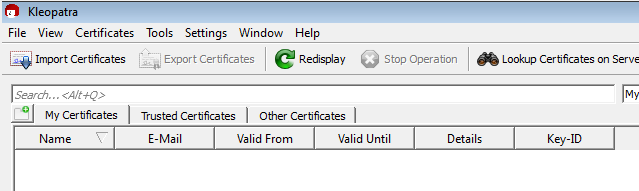
**Objetivo: realizar cifrado asimétrico con OpenGPG**

1.- Instale la aplicación GNUpg4win provista por su profesor:

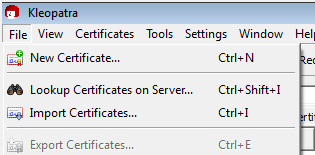
<http://www.gpg4win.org/>



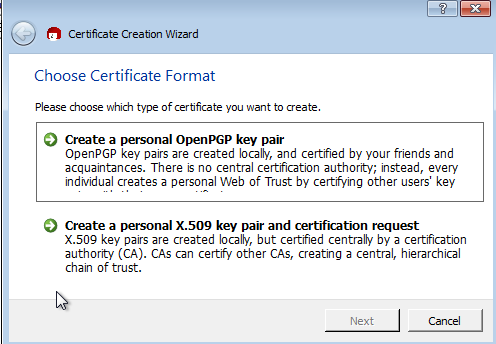
2.- Una vez instalada la aplicación, ejecute la interfaz de administración Kleopatra



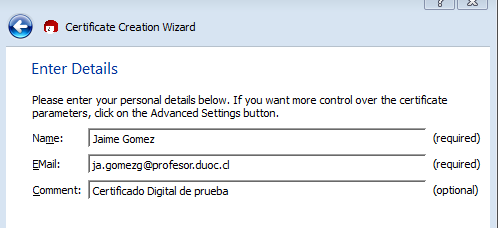
3.- Ejecute la opción “New Certificate” para crear su certificado digital



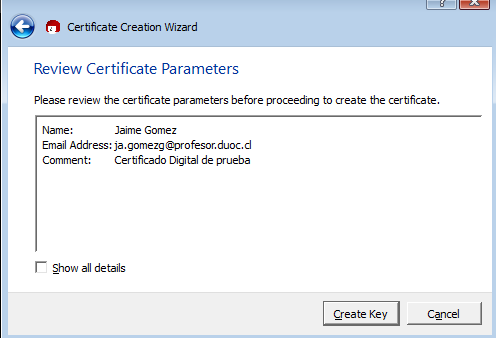
4.- Seleccione la opción “OpenPGP key pair”



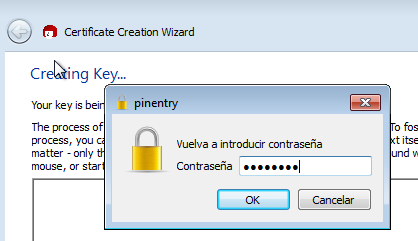
5.- A continuación complete los datos solicitados



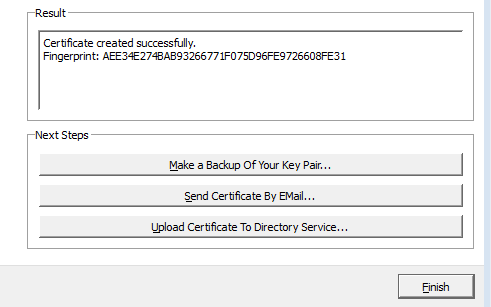
6.- Haga click en “Next” y confirme la creación del Certificado



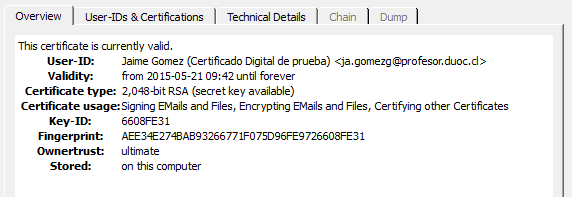
7.- Ingrese la contraseña de protección de su Certificado digital y su confirmación



8.- Haga click en “Finish” para finalizar la operación

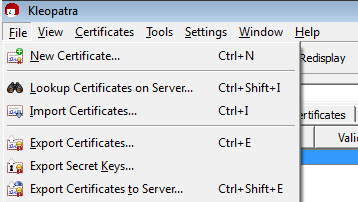


9.- Haga doble click en su certificado para visualizar sus principales parámetros y responda:

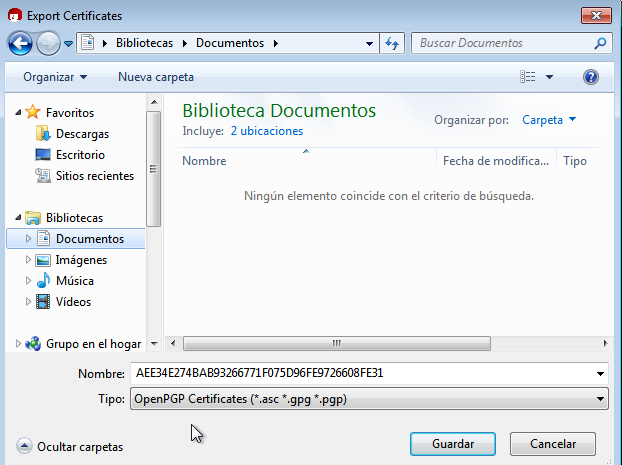


* Periodo de validez:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Algoritmo de cifrado:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Largo de la llave de cifrado:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

10.- Ejecute la opción de exportar su Certificado a un archivo

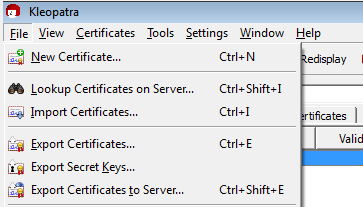


11.- Grabe el archivo de su certificado en su disco local

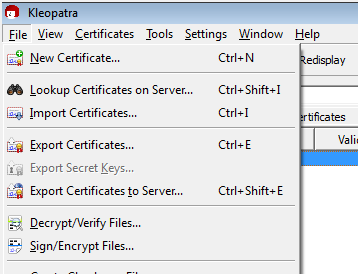


12.- Envíe el archivo de su certificado digital a algunos de sus compañeros por correo

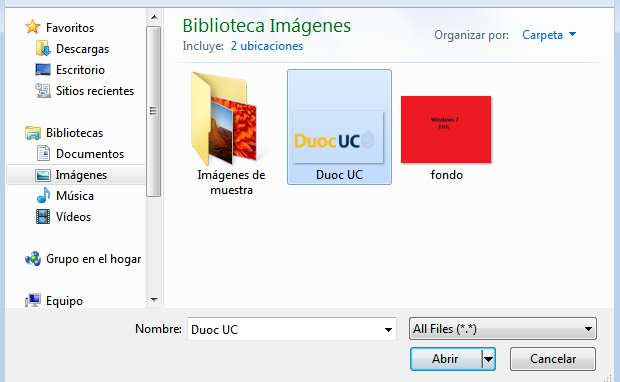
13.- Pida a su compañero que realice la importación del certificado digital recibido



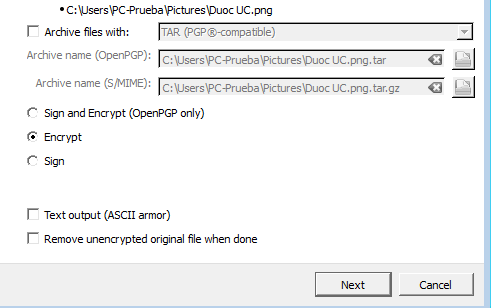
14.- A continuación ejecute la opción “Sign/Encrypt Files”



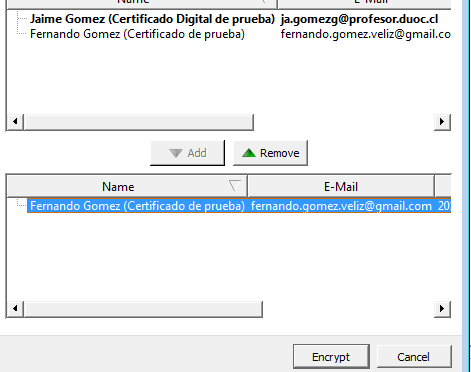
15.- Seleccione un archivo que será enviado cifrado a su compañero



16.- Seleccione la opción “Encrypt” y haga click en “Next”

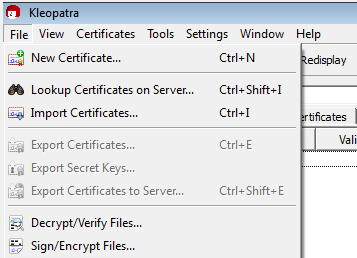


17.- Agregue el certificado digital de su compañero que será el destinatario del archivo

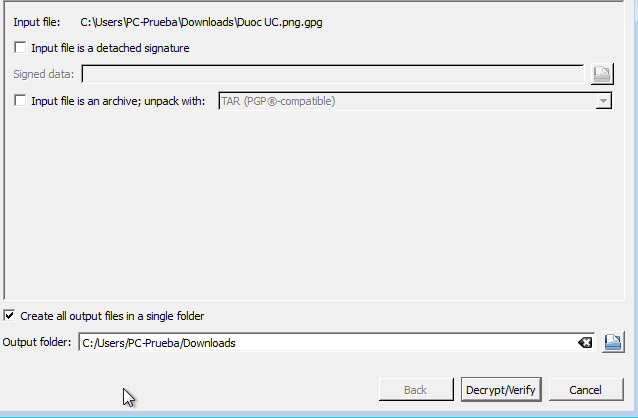


18.- Responda el correo de su compañero y adjunte el archivo cifrado

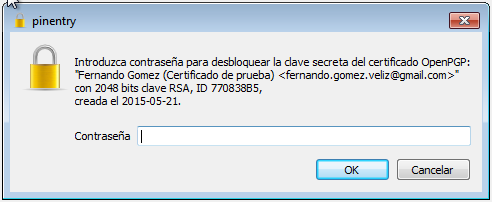
19.- Pida a su compañero que baje el archivo recibido y lo descifre con la opción “Decrypt/Verify Files”



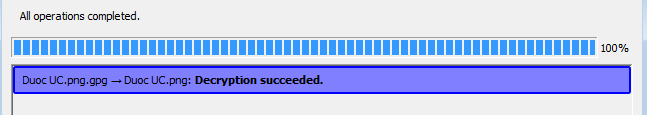
20.- Pida a su compañero que ejecute la opción Decrypt/Verify



21.- El sistema solicitara la clave de su llave privada, debe ingresarla para descifrar el archivo



22.- Una vez finalizada la operación, pida a su compañero que visualice el archivo descifrado



**Objetivo: Instalar y probar una aplicación de Esteganografía**

1.- Inicie su computador en Windows 7.

2.- Instale la aplicación “Invisible Secrets” versión 4 en modalidad trial, provista por su profesor.

3.- Ejecute la aplicación y vaya a su menú principal.

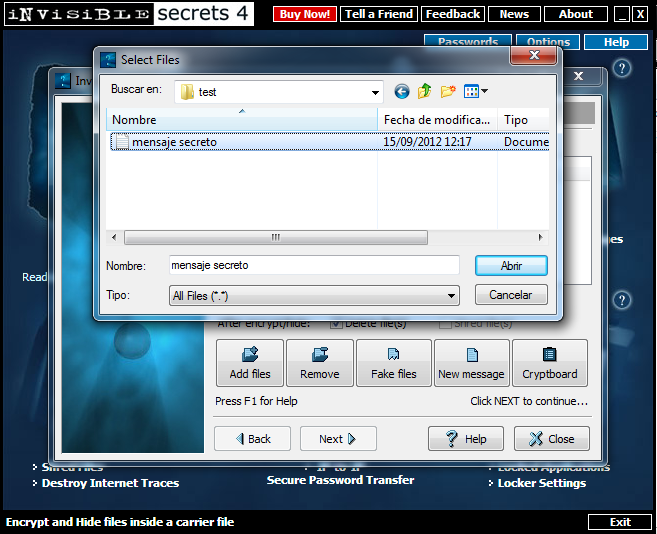


4.- Ingrese al sitio de google imágenes y baje alguna foto en formato .jpg

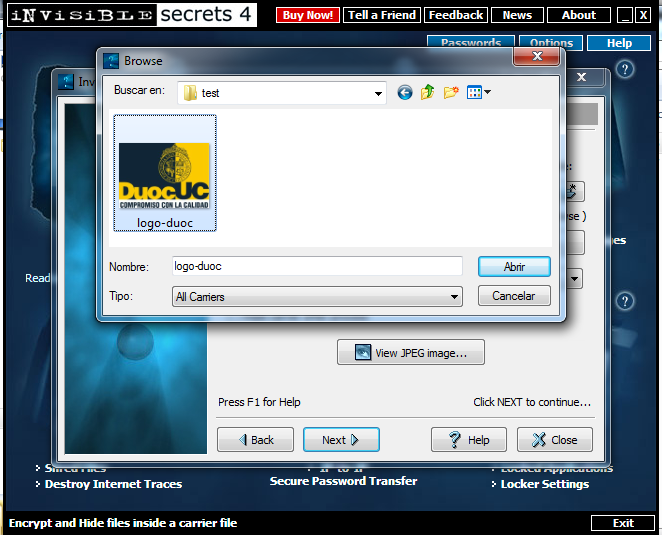
5.- Grave el archivo en un directorio temporal.

6.- Escriba en un archivo de “notepad” un mensaje para su compañero, sin que este lo vea.

7.- Ejecute la opción “Hide Files” y agregue el archivo de texto con el mensaje secreto.



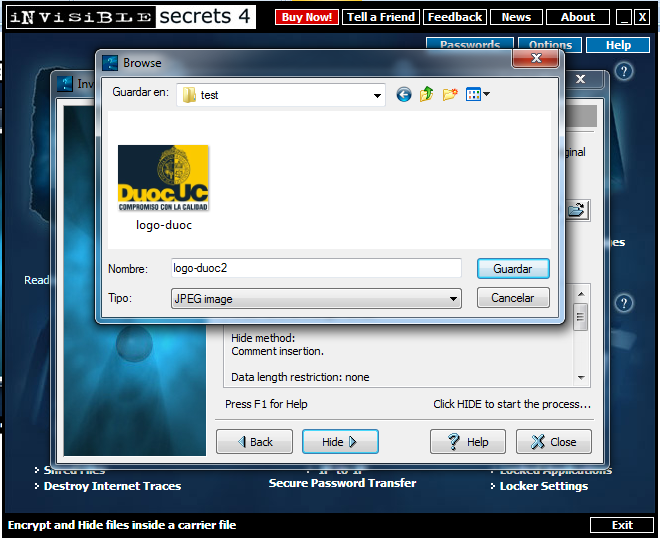
8.- Ejecute la opción Next y agregue el archivo imagen que acaba de bajar.



9.- Seleccione la opción Next y luego ingrese su clave secreta.



10.- Seleccione la opción Next y elija el nombre del archivo de salida.



11.- Presione Next para finalizar el proceso

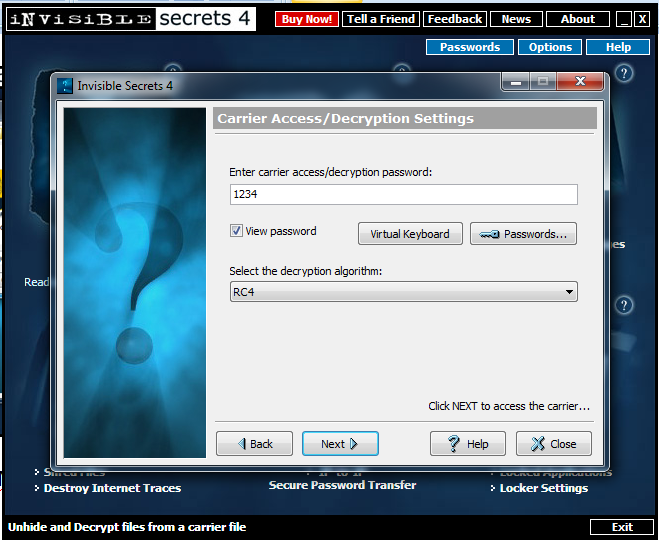
12.- Revise el archivo .jpg generado e intente buscar el mensaje dentro del archivo.

13.- Envíe el archivo generado por correo a su compañero junto con la password utilizada.

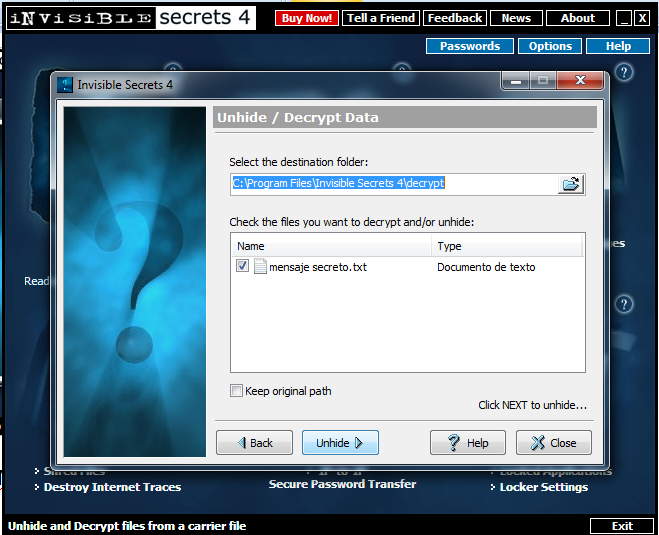
14.- Ejecute la opción “Unhide” utilizando el archivo recibido de su compañero.



15.- Presione Next e ingrese la password entregada por su compañero. (encriptación AES)



16.- Presione Next y luego la opción Unhide.



17.- Una vez finalizado el proceso revise el directorio “**C:\Program Files\Invisible Secrets 4\decrypt**” y abra el documento de texto encontrado.

18.- Compare el mensaje con el que tiene su compañero.

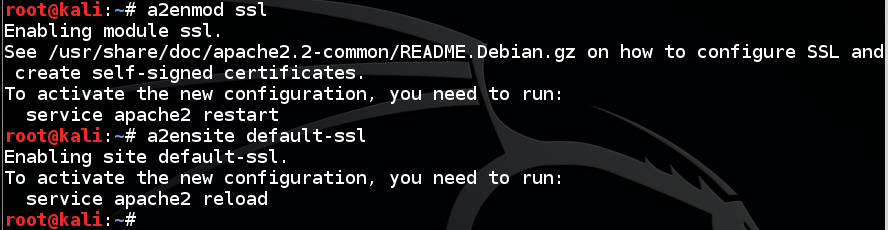
**Instalación de un certificado digital para SSL**

1.- Levante su máquina Kali con la interfaz de red en modo puente

2.- Habilite el servicio SSL con los siguientes comandos:

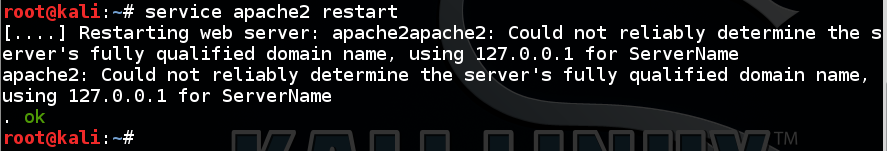
# a2enmod ssl

# a2ensite default-ssl



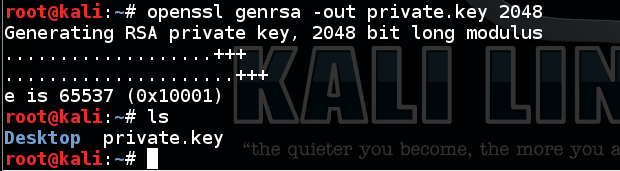
3.- Reinicie el servicio web de apache con el siguiente comando:

# service apache2 restart



4.- Genere la llave privada del certificado digital con el siguiente comando:

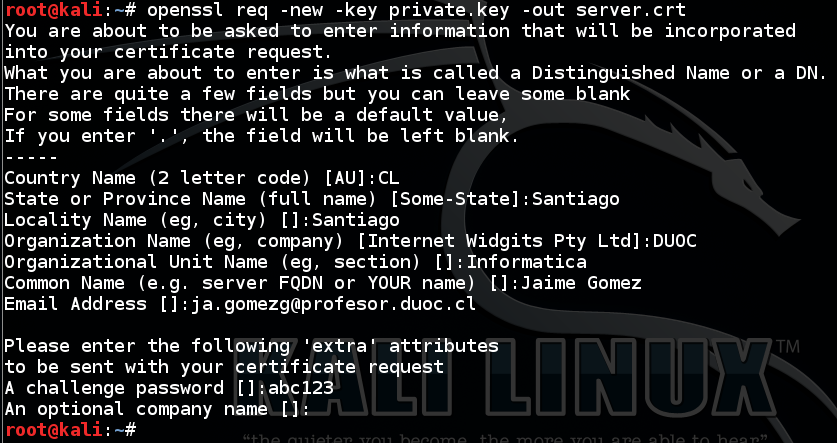
# openssl genrsa –out private.key 2048



5.- Realice la solicitud del certificado digital (CSR) con el siguiente comando:

# openssl req -new -key private.key -out server.csr

Solicitará algunos datos que debe ingresar, siga el ejemplo mostrado



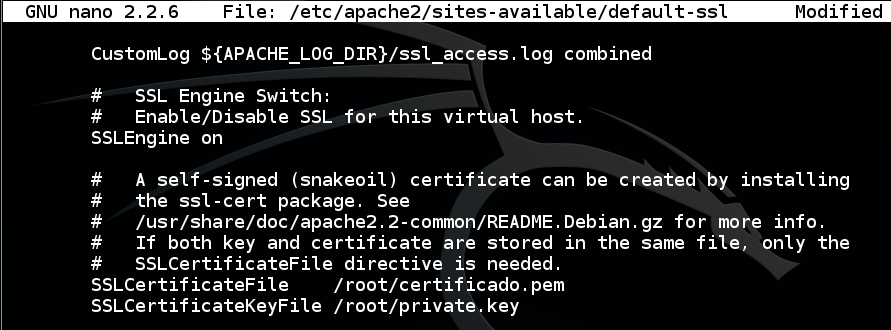
6.- Genere el certificado digital firmado con la llave privada con el siguiente comando:

# openssl x509 -req -days 365 -in server.csr -signkey private.key -out certificado.pem



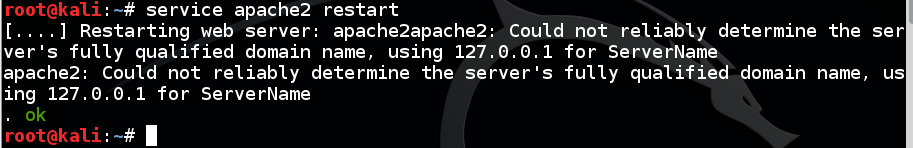
7.- A continuación modifique el archivo de configuración para que el servidor pueda acceder a la llave privada y certificado digital, con el siguiente comando:

# nano /etc/apache2/sites-available/default-ssl



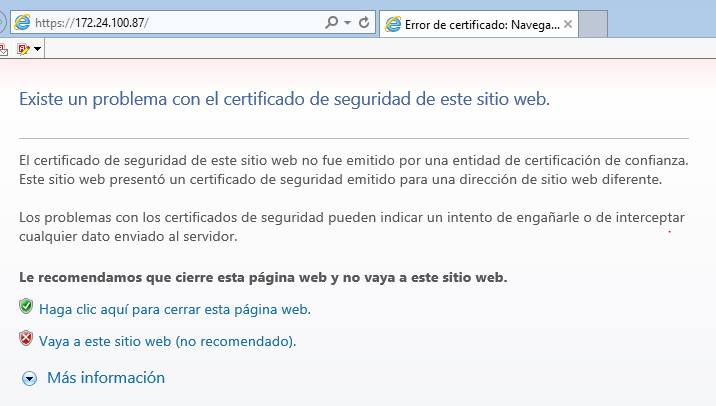
8.- Reinicie el servicio apache nuevamente con el comando:

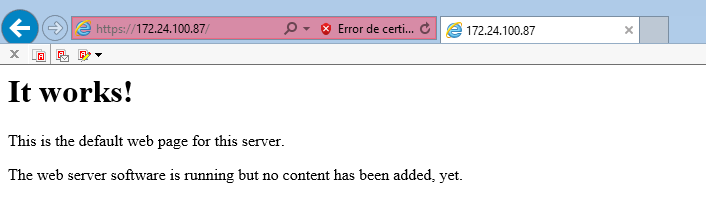
# service apache2 restart



9.- Conéctese con su browser al sitio web a la siguiente dirección

<https://ip_server>





10.- Visualice el certificado digital

