Práctica 4

Aspectos teóricos previos

- Para la realización de esta práctica hay que partir de la situación de la práctica 3, por lo que debes copiar la configuración de dicha práctica sobre el fichero de configuración vsftpd.conf.
- En el archivo de configuración puedes observar que aparecen las rutas al certificado y clave privada que usaría el servidor en los intentos de conexión usando SSL/TLS. Estos certificados son autofirmados y es importante cambiarlos por un certificado emitido por una CA reconocida o, en nuestro caso, al menos con un certificado autofirmado pero con el nombre del sitio adecuado, como hemos hecho en los sitios web.
- Recuerda que con respecto a la seguridad en el protocolo FTP podemos hacer las siguientes consideraciones:
    - Existe una versión de protocolo FTP denominado TFTP (Trivial) cuyo funcionamiento es similar a FTP aunque no requiere autenticación del usuario antes de la conexión, simplemente se lleva a cabo la transferencia de archivos (uso en WDS, por ejemplo).
    - Existe un protocolo de transferencia de ficheros que implementa la seguridad propia de SSH (SFTP), que es un protocolo independiente de FTP y diseñado también con independencia del protocolo original FTP.
    - Por último el protocolo FTP al que se le puede añadir una capa de seguridad SSL/TLS (como se hace con HTTP) para convertirlo en FTPS/FTPES . Serán estos últimos en los que nos detendremos, en primer lugar distinguiendo entre los modos explícito e implícito:
        - Implícito o FTPS (más antiguo): El cliente asume el modo seguro con TLS o SSL desde el inicio de la conexión, antes de transferir la información. Habitualmente se utiliza el puerto 990 (conexión) y 989 (datos) en lugar de los habituales. Se espera del cliente un mensaje “client hello” para comenzar.
        - Explícito o FTPES: El cliente se conecta al puerto habitual FTP (21) y explícitamente cambia a un modo seguro utilizando TLS o SSL para transferir la información.

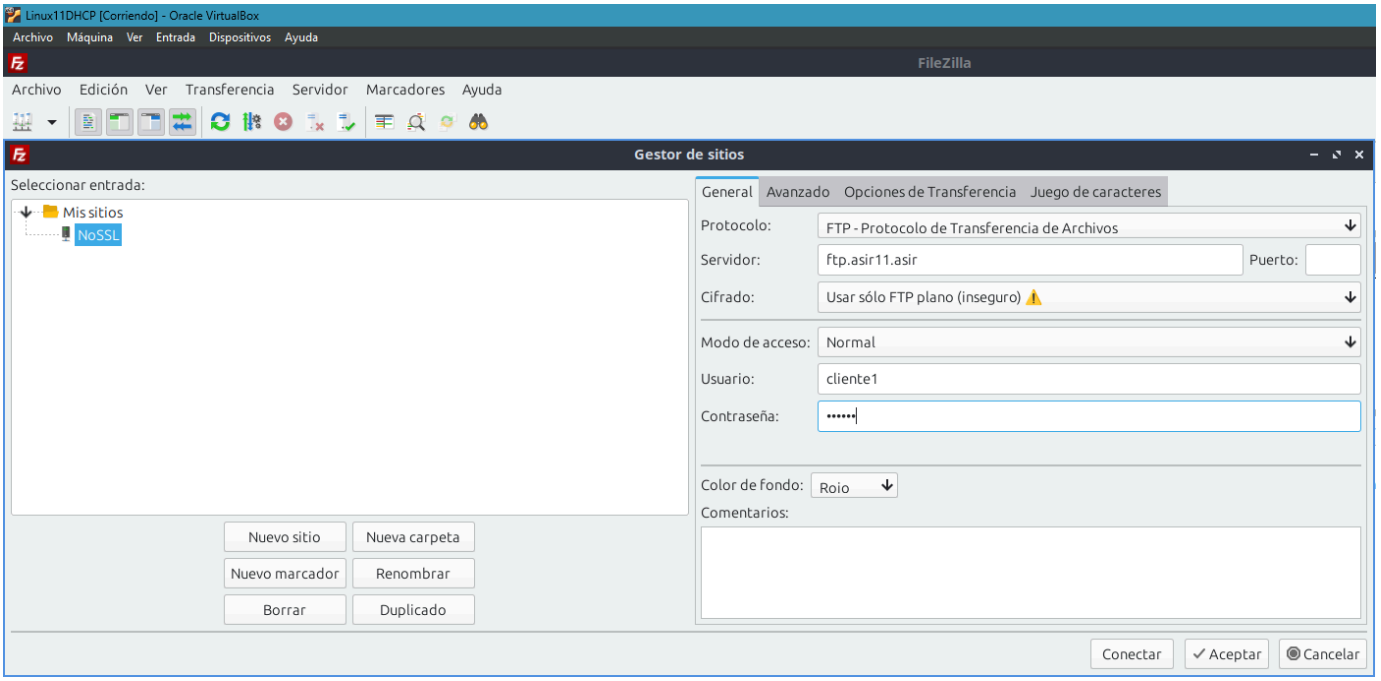
Consideraciones iniciales

- A lo largo de esta práctica se va a utilizar como cliente Filezilla. Si no lo tienes, instálalo en tu cliente LinuxXX
- Crea y almacena en Filezilla una conexión diferente por cada variante que hagas en dicha conexión y nómbralas adecuadamente para poder identificarlas con facilidad y poder volver a usarlas.

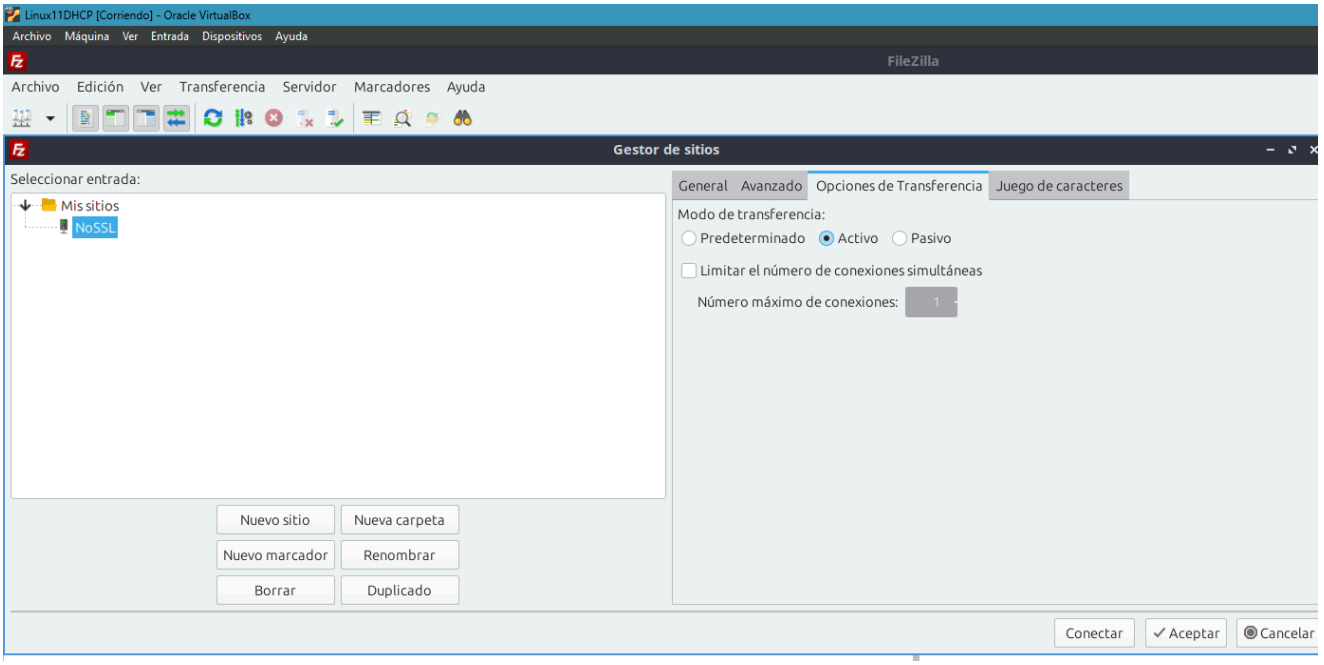
- Es importante que por cada intento de conexión solicitado hagas una captura de wireshark para poder observar los diálogos que se producen entre cliente y servidor.
- Utiliza como usuario de prueba 'cliente1'.
- Por cada cambio que realices en el servidor haz un reinicio del mismo.
- Ten especial cuidado y utiliza solamente minúsculas en los nombres de las directivas.

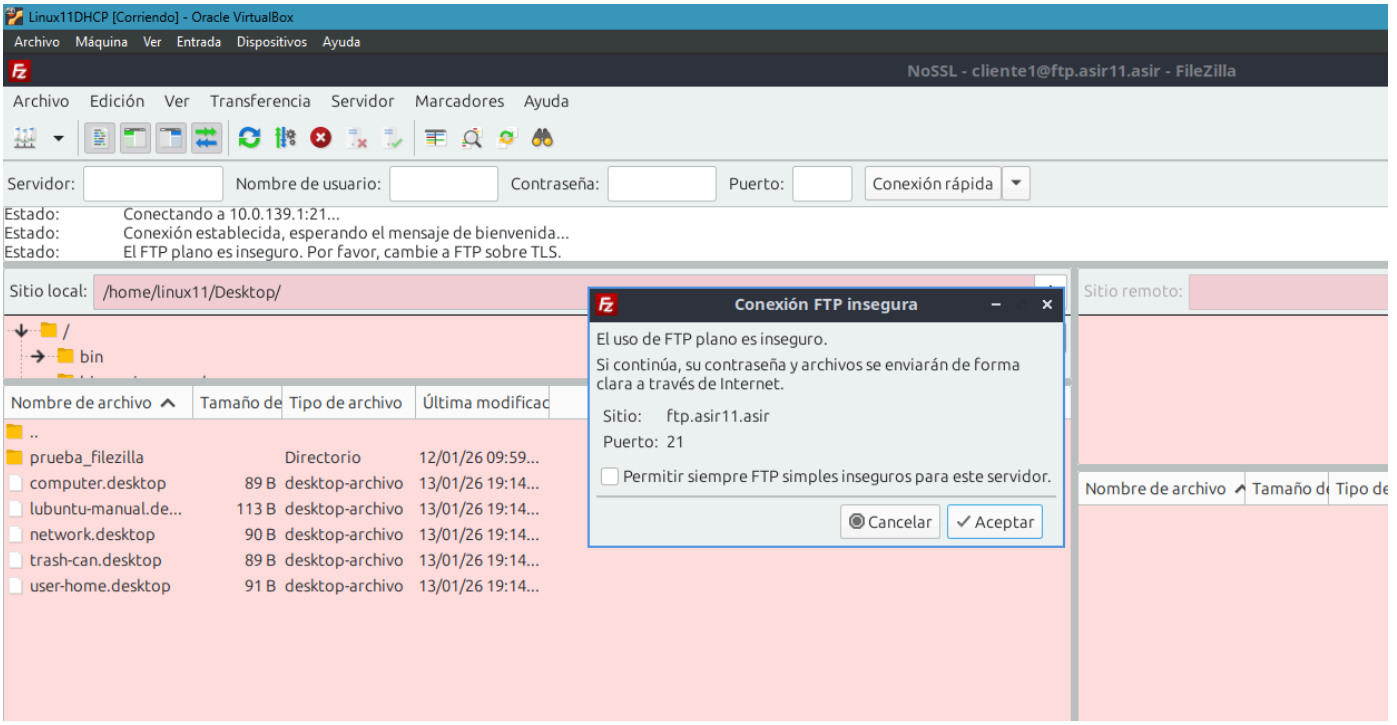
Desarrollo de la práctica

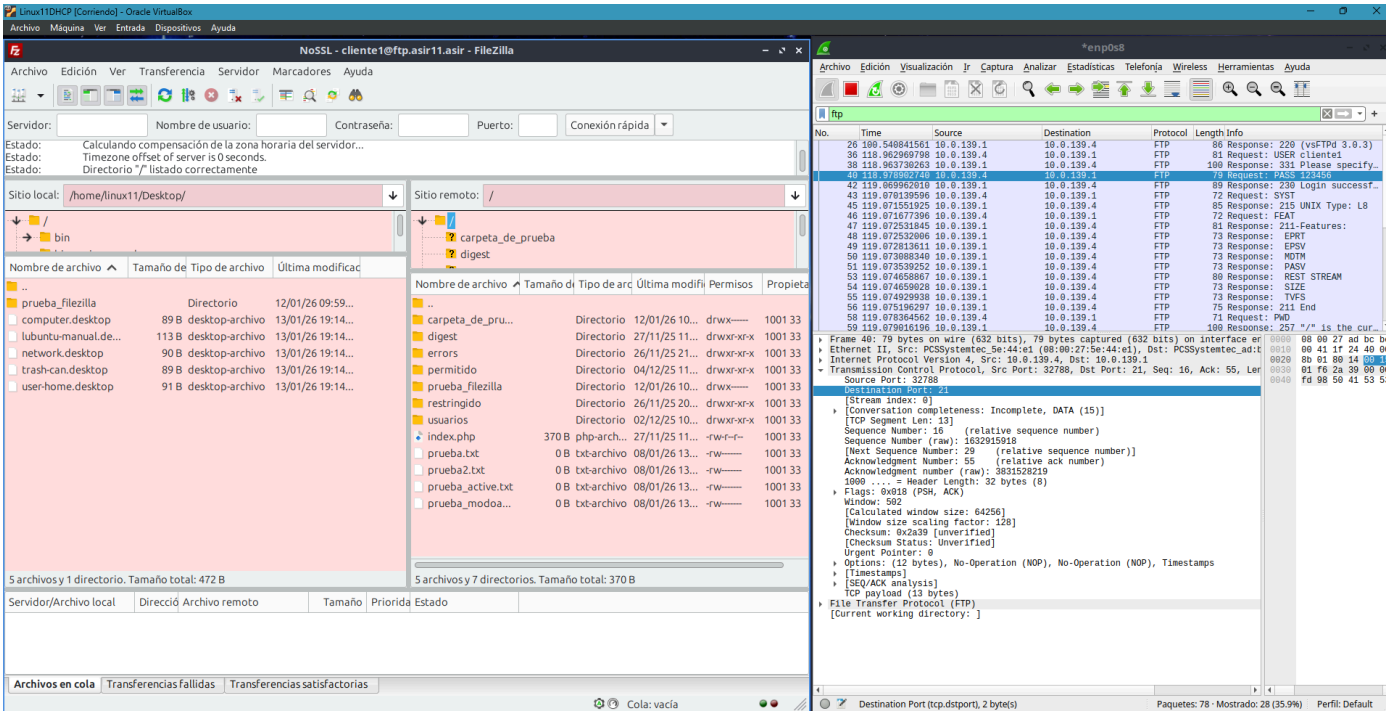
1. Crea en Filezilla un sitio denominado NoSSL (Only use plain FTP) y verifica que se produce la conexión, que la misma se hace sobre el puerto 21. ¿Qué modo de conexión para transferencia de archivos se utiliza? ¿Qué puertos se ven implicados? Desconéctate del servidor. Para hacerlo puedes seguir estos pasos:
    - En Archivos, gestor de sitios, crea un nuevo sitio con el nombre NoSSL
    - Configúralo en la primera pestaña: Nombre del servidor (ftp.asir.....), Only use plain FTP, usuario y contraseña (si bien es probable que no se pueda almacenar y se configure en modo 'preguntar por contraseña'). Pon como color de fondo el rojo.



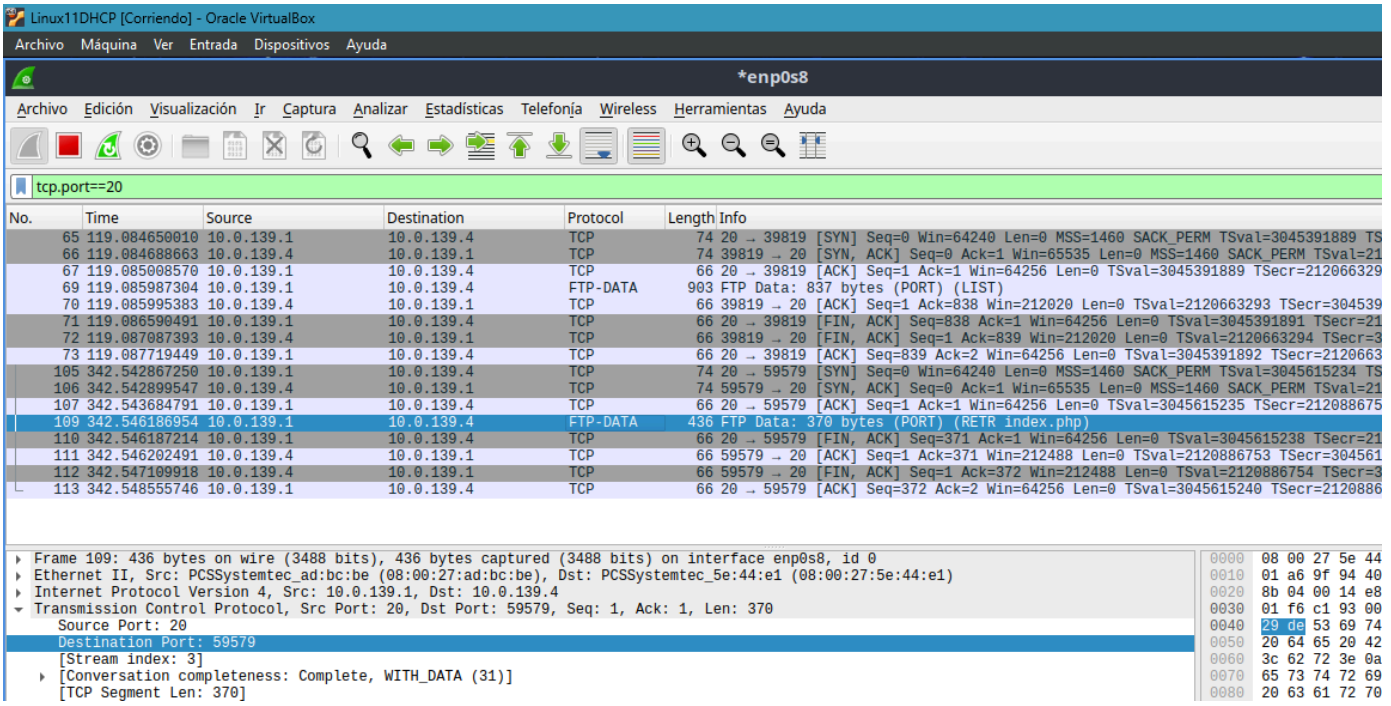
    - Configúralo en la tercera pestaña para forzar el modo 'activo'


Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
FileZilla
Archivo Edición Ver Transferencia Servidor Marcadores Ayuda
Gestor de sitios
Seleccionar entrada:
Mis sitios
NoSSL
General Avanzado Opciones de Transferencia Juego de caracteres
Modo de transferencia:
Predeterminado Activo Pasivo
Limitar el número de conexiones simultáneas
Número máximo de conexiones:
Nuevo sitio
Nueva carpeta
Nuevo marcador
Renombrar
Borrar
Duplicado
Conectar
Aceptar
Cancelar

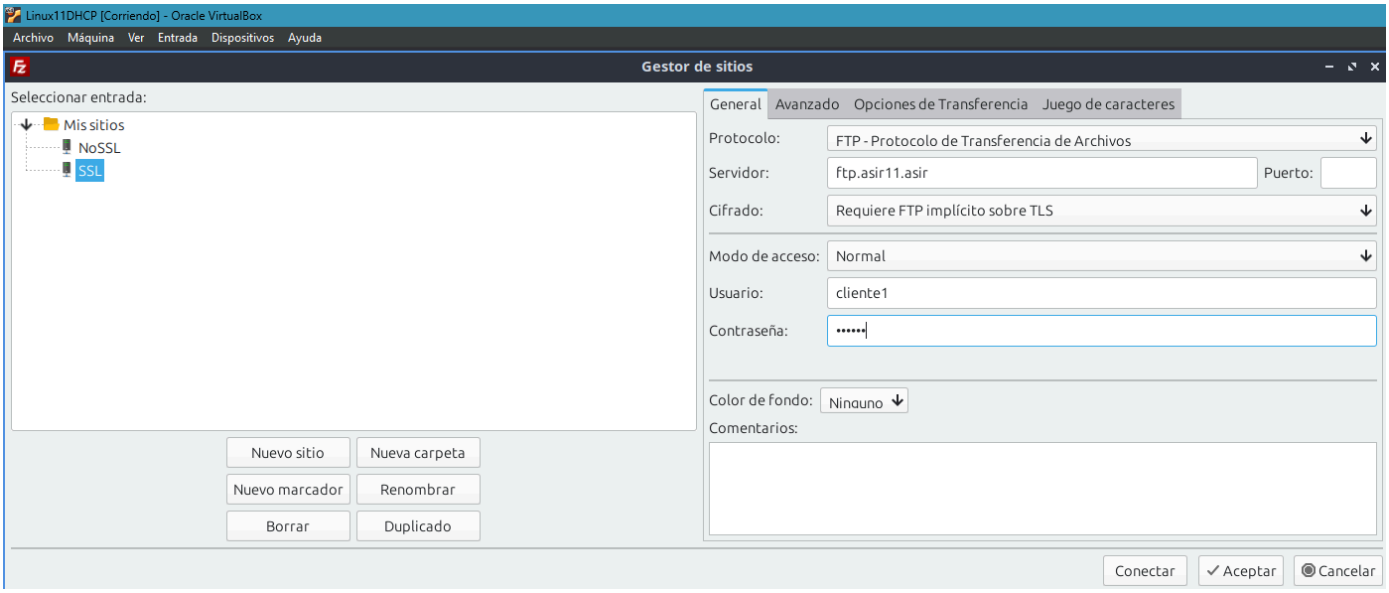

Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
NoSSL - cliente1@ftp.asir11.asir - FileZilla
Archivo Edición Ver Transferencia Servidor Marcadores Ayuda
Servidor:
Nombre de usuario:
Contraseña:
Puerto:
Conexión rápida
Estado: Conectando a 10.0.139.1:21...
Estado: Conexión establecida, esperando el mensaje de bienvenida...
Estado: El FTP plano es inseguro. Por favor, cambie a FTP sobre TLS.
Sitio local: /home/linux11/Desktop/
Sitio remoto:
/
bin
Nombre de archivo
Tamaño de
Tipo de archivo
Última modificac
..
prueba_filezilla Directorio 12/01/26 09:59...
computer.desktop 89 B desktop-archivo 13/01/26 19:14...
lubuntu-manual.de... 113 B desktop-archivo 13/01/26 19:14...
network.desktop 90 B desktop-archivo 13/01/26 19:14...
trash-can.desktop 89 B desktop-archivo 13/01/26 19:14...
user-home.desktop 91 B desktop-archivo 13/01/26 19:14...
Conexión FTP insegura
El uso de FTP plano es inseguro.
Si continúa, su contraseña y archivos se enviarán de forma clara a través de Internet.
Sitio: ftp.asir11.asir
Puerto: 21
Permitir siempre FTP simples inseguros para este servidor.
Cancelar
Aceptar



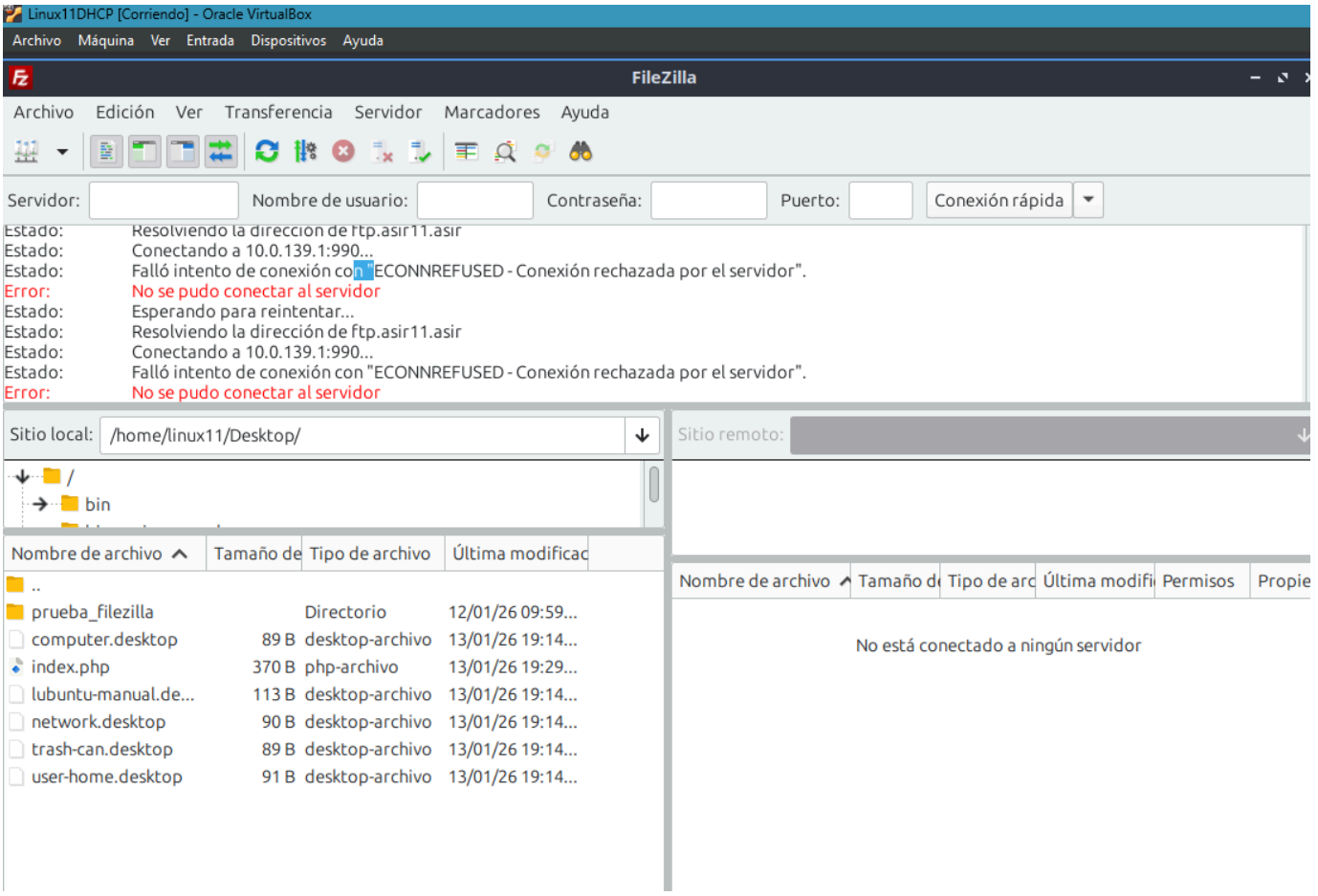
Al ser **activo** la transferencia de archivos se da por el **puerto 20** del servidor:

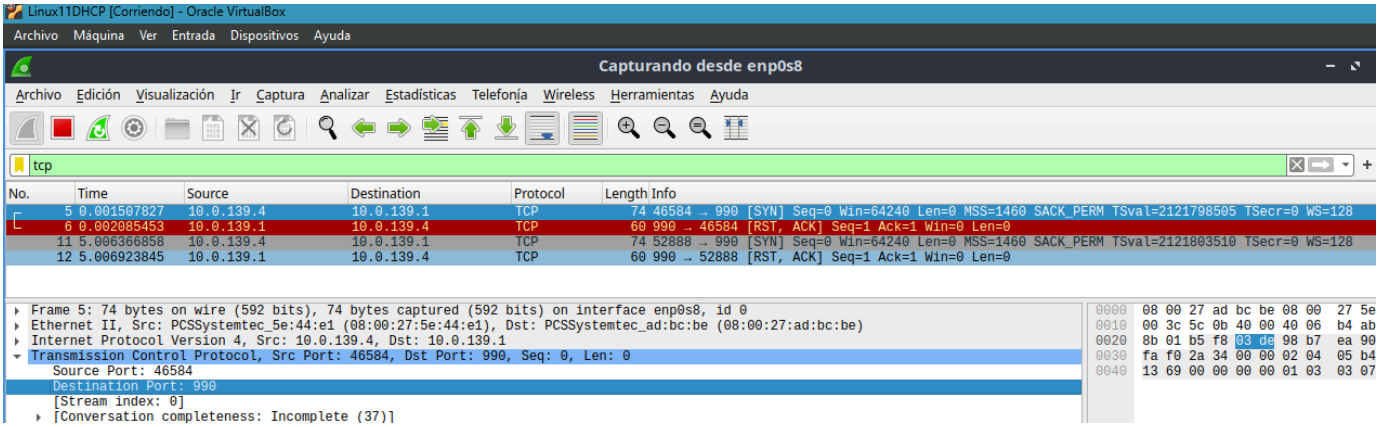


2. Crea un sitio igual que el anterior pero usando como cifrado 'FTP Implícito sobre TLS' (nómbralo como SSL). ¿Qué ocurre al intentar la conexión? ¿A qué nivel se produce la respuesta del servidor? ¿Qué puertos se ven implicados? ¿Es coherente lo que ocurre?



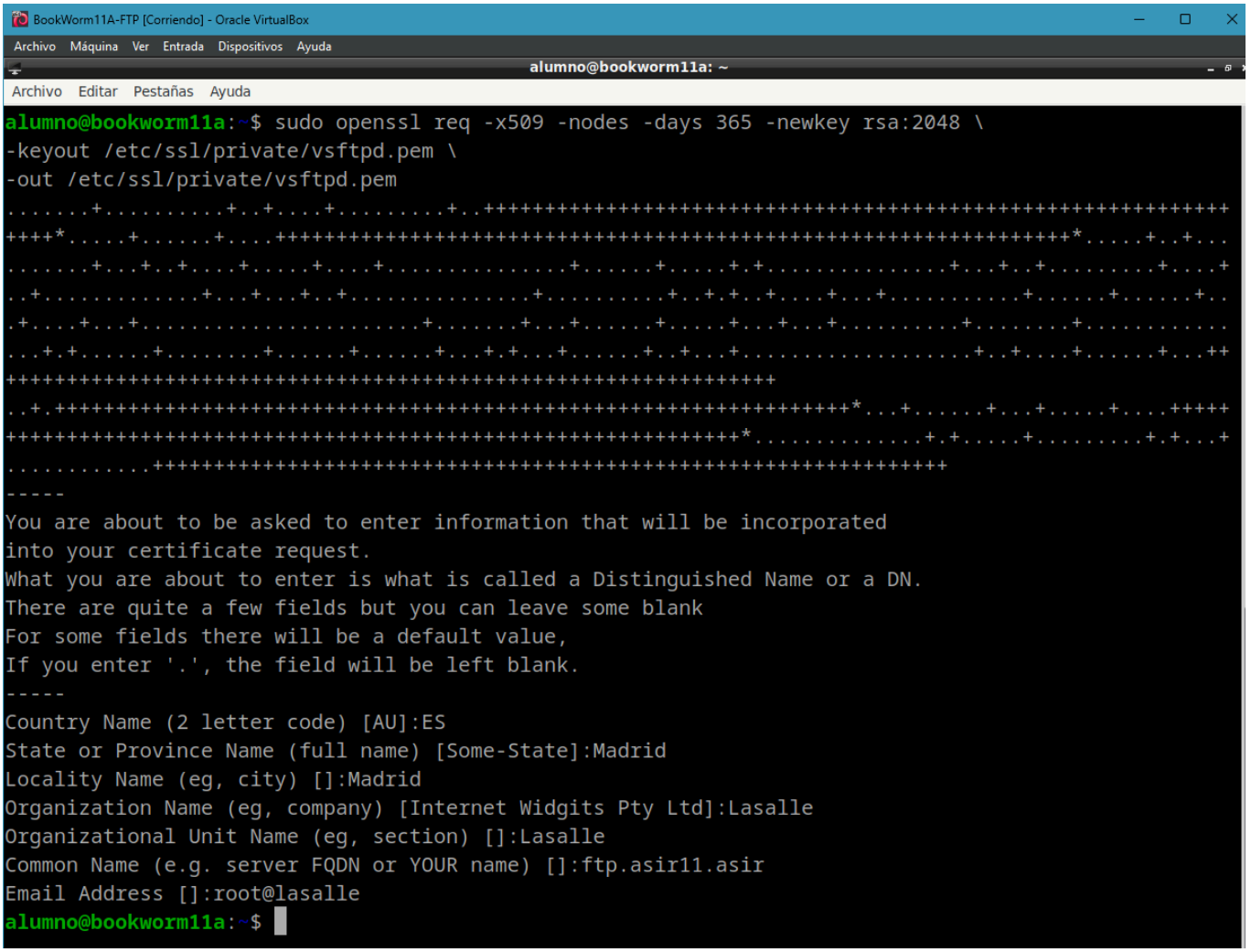
INTENTO DE CONEXIÓN CON EL SERVIDOR:

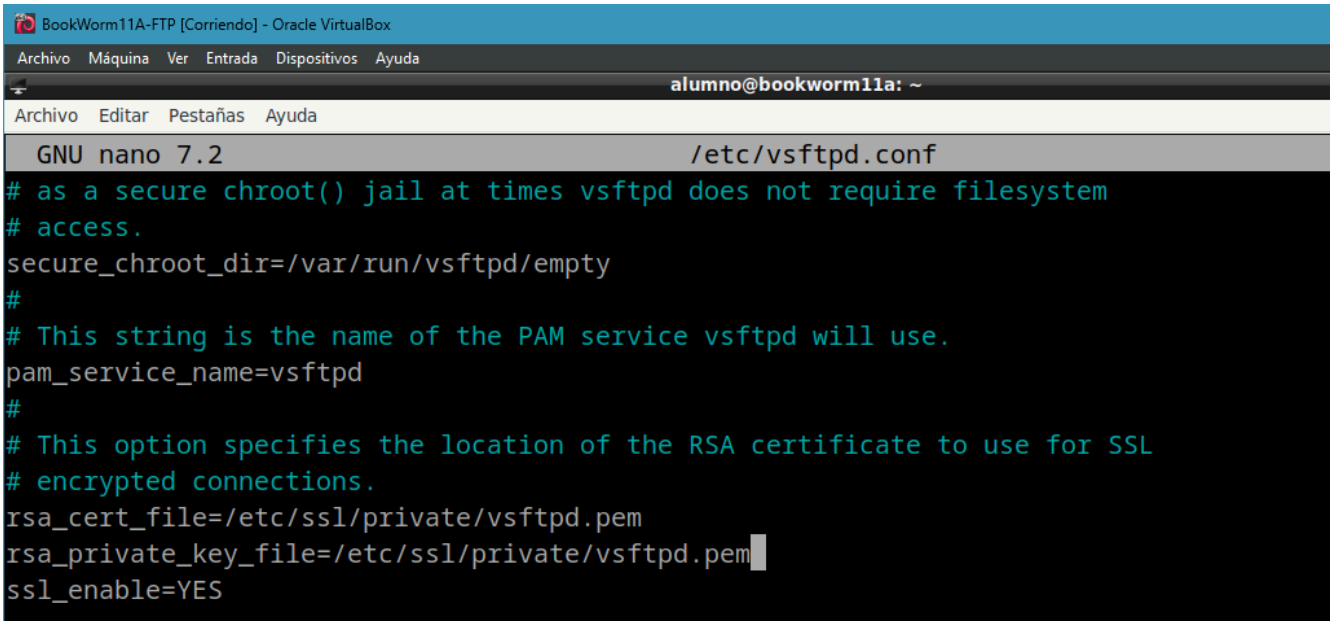




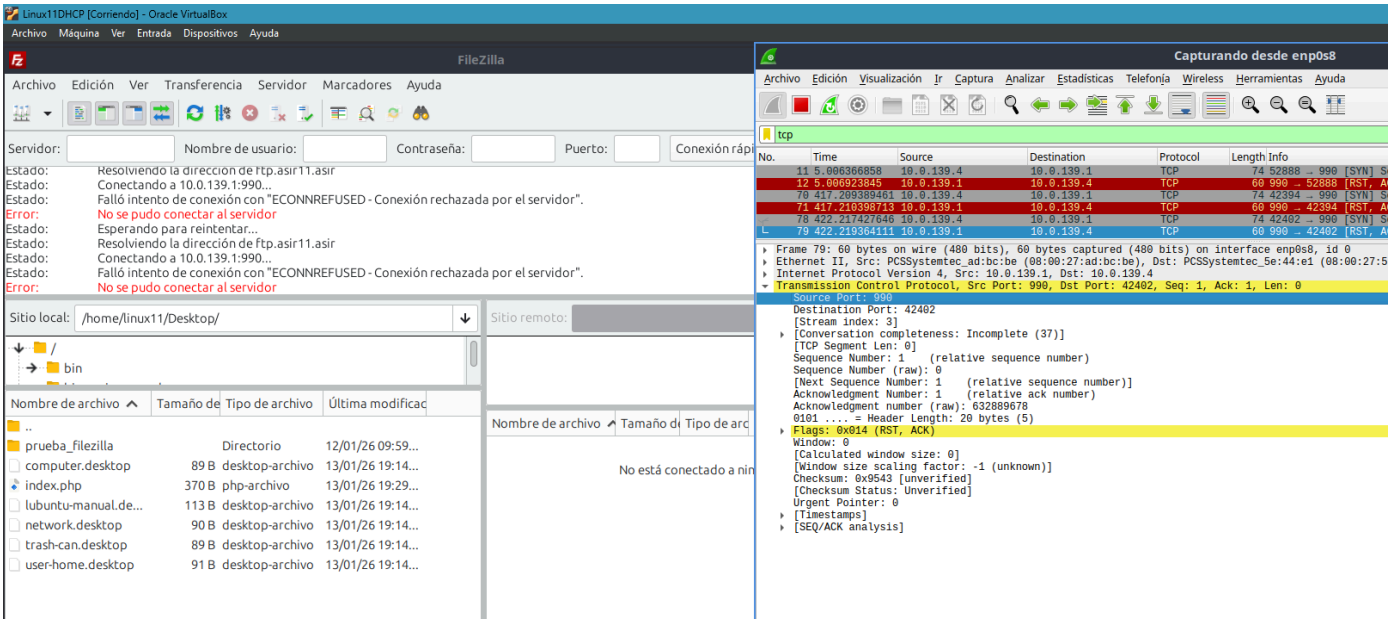
El modo **Implícito** espera conectarse al puerto **990** por defecto. Mi servidor ni siquiera está escuchando ahí, y aunque lo hiciera, no sabe hablar SSL todavía.

3. La configuración del servidor FTP para utilizar conexiones seguras comienza activando la directiva ssl_enable y, en nuestro caso, además, creando y usando un certificado propio para el servicio FTP (ftp.asirXX.asir). Créalo del mismo modo que lo creaste para el servicio web.



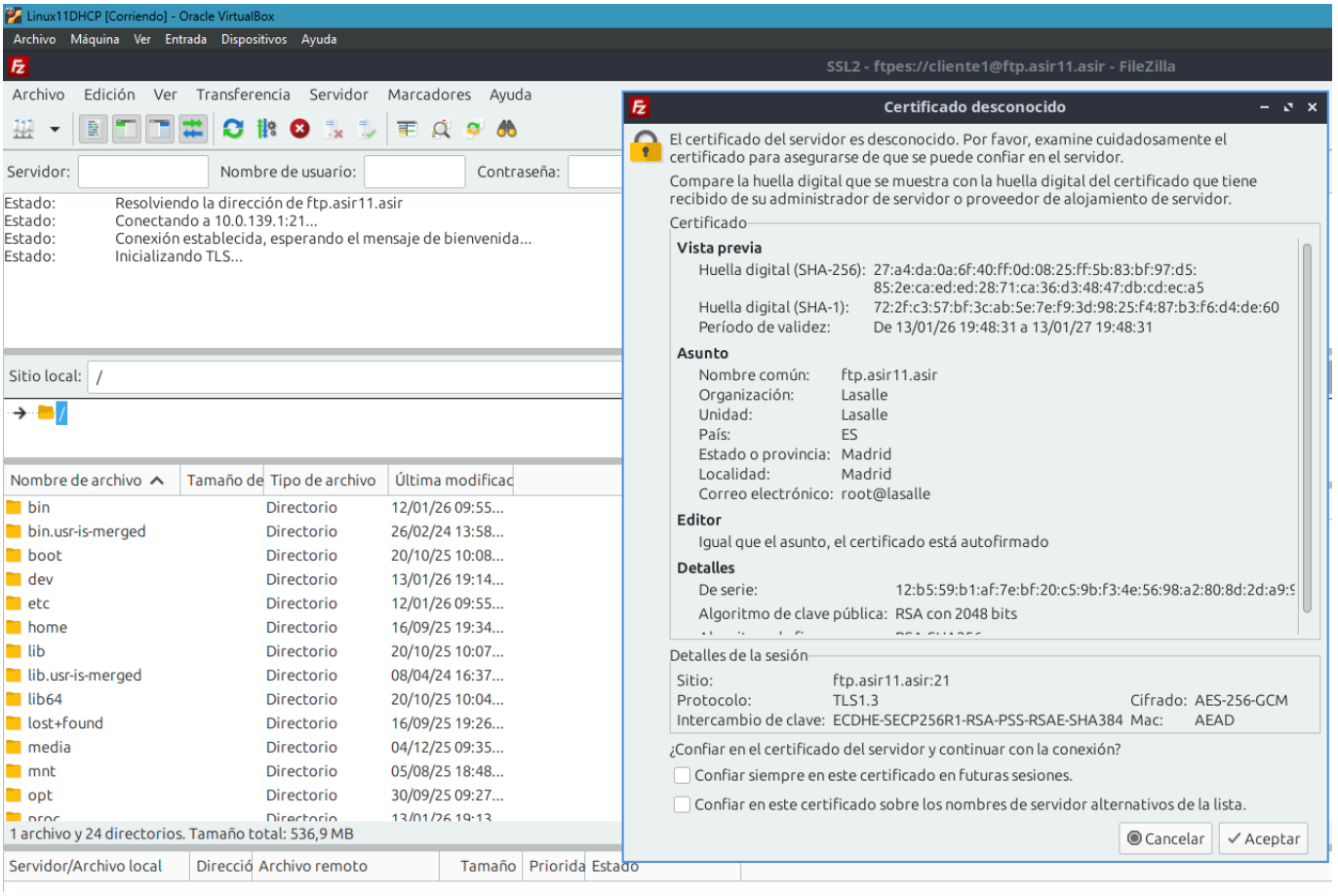


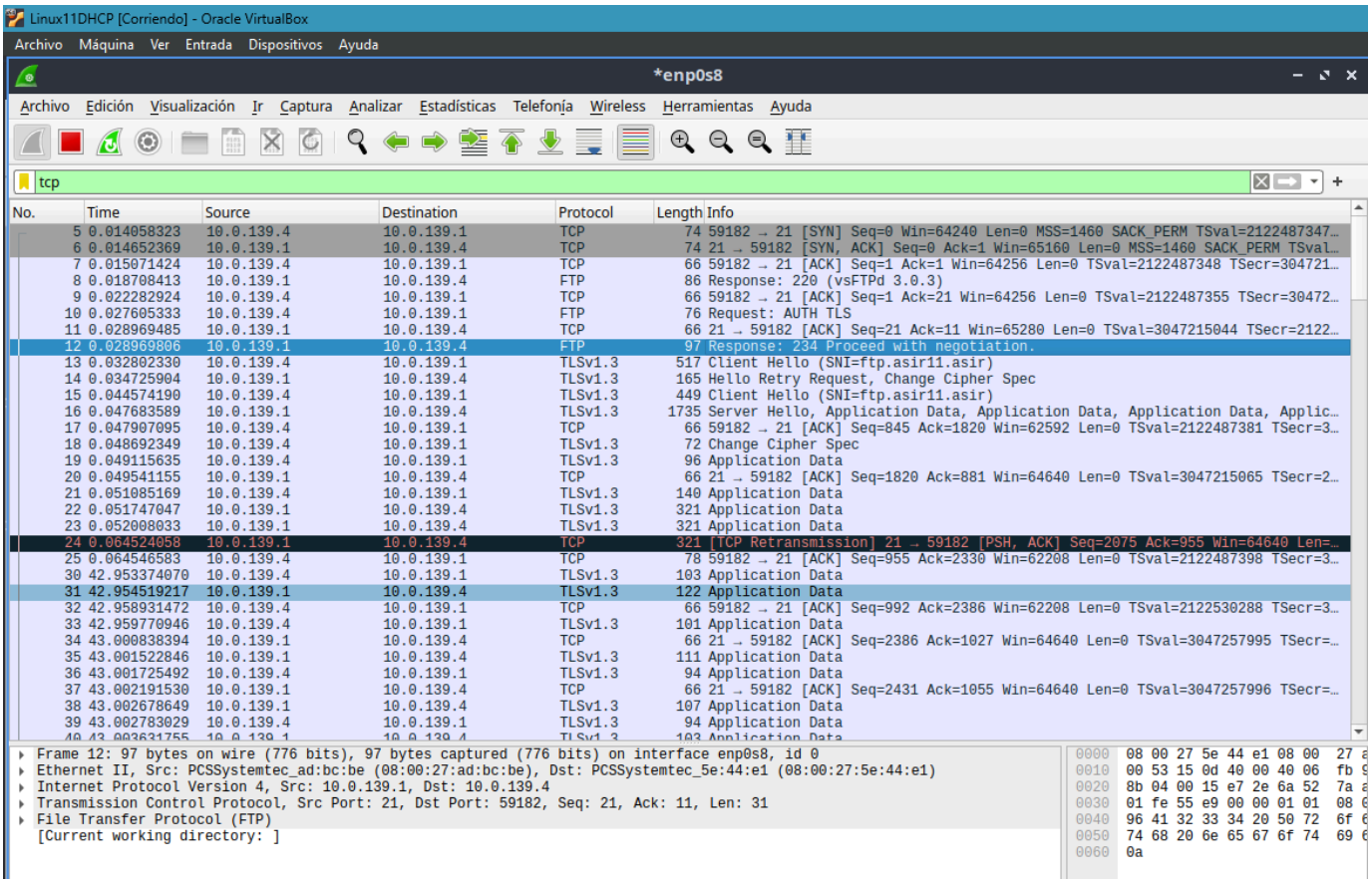
4. Vuelve a probar la conexión del punto 2 y matiza las respuestas que diste si fuera necesario, ¿Cambia alguna de dichas respuestas?

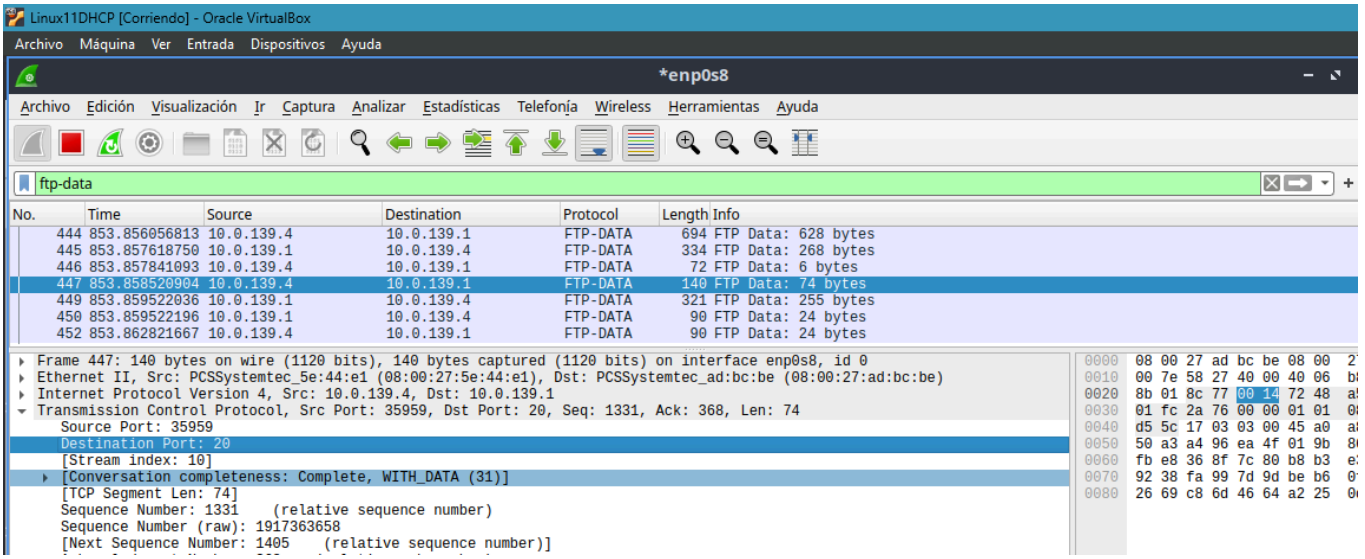


Sigue fallando ya que aunque tengamos activado el ssl no tengo activado el puerto 990 por el que se va realizar la conexión

5. Crea un sitio igual que SSL, denominado SSL2, en el que cambies de modo Implícito a modo 'Explícito sobre TLS'. Y responde a las siguientes preguntas:


Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
SSL2 - ftpes://cliente1@ftp.asir11.asir - FileZilla
Archivo Edición Ver Transferencia Servidor Marcadores Ayuda
Servidor: Nombre de usuario: Contraseña:
Estado: Resolviendo la dirección de ftp.asir11.asir
Estado: Conectando a 10.0.139.1:21...
Estado: Conexión establecida, esperando el mensaje de bienvenida...
Estado: Inicializando TLS...
Sitio local: /
Nombre de archivo Tamaño de Tipo de archivo Última modificac
bin Directorio 12/01/26 09:55...
bin.usr-is-merged Directorio 26/02/24 13:58...
boot Directorio 20/10/25 10:08...
dev Directorio 13/01/26 19:14...
etc Directorio 12/01/26 09:55...
home Directorio 16/09/25 19:34...
lib Directorio 20/10/25 10:07...
lib.usr-is-merged Directorio 08/04/24 16:37...
lib64 Directorio 20/10/25 10:04...
lost+found Directorio 16/09/25 19:26...
media Directorio 04/12/25 09:35...
mnt Directorio 05/08/25 18:48...
opt Directorio 30/09/25 09:27...
1 archivo y 24 directorios. Tamaño total: 536,9 MB
Servidor/Archivo local Dirección Archivo remoto Tamaño Prioridad Estado
Certificado desconocido
El certificado del servidor es desconocido. Por favor, examine cuidadosamente el certificado para asegurarse de que se puede confiar en el servidor.
Compare la huella digital que se muestra con la huella digital del certificado que tiene recibido de su administrador de servidor o proveedor de alojamiento de servidor.
Certificado
Vista previa
Huella digital (SHA-256): 27:a4:da:0a:6f:40:ff:0d:08:25:ff:5b:83:bf:97:d5:85:2e:ca:ed:ed:28:71:ca:36:d3:48:47:db:cd:ec:a5
Huella digital (SHA-1): 72:2f:c3:57:bf:3c:ab:5e:7e:f9:3d:98:25:f4:87:b3:f6:d4:de:60
Período de validez: De 13/01/26 19:48:31 a 13/01/27 19:48:31
Asunto
Nombre común: ftp.asir11.asir
Organización: Lasalle
Unidad: Lasalle
País: ES
Estado o provincia: Madrid
Localidad: Madrid
Correo electrónico: root@lasalle
Editor
Igual que el asunto, el certificado está autofirmado
Detalles
De serie: 12:b5:59:b1:af:7e:bf:20:c5:9b:f3:4e:56:98:a2:80:8d:2d:a9:
Algoritmo de clave pública: RSA con 2048 bits
Detalles de la sesión
Sitio: ftp.asir11.asir:21
Protocolo: TLS1.3 Cifrado: AES-256-GCM
Intercambio de clave: ECDHE-SECP256R1-RSA-PSS-RSAE-SHA384 Mac: AEAD
¿Confiar en el certificado del servidor y continuar con la conexión?
Confiar siempre en este certificado en futuras sesiones.
Confiar en este certificado sobre los nombres de servidor alternativos de la lista.
Cancelar
Aceptar


Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
*enp0s8
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
tcp
No. Time Source Destination Protocol Length Info
5 0.014058323 10.0.139.4 10.0.139.1 TCP 74 59182 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2122487347…
6 0.014652369 10.0.139.1 10.0.139.4 TCP 74 21 → 59182 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval…
7 0.015071424 10.0.139.4 10.0.139.1 TCP 66 59182 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2122487348 TSecr=304721…
8 0.018708413 10.0.139.1 10.0.139.4 FTP 86 Response: 220 (vsFTPd 3.0.3)
9 0.022282924 10.0.139.4 10.0.139.1 TCP 66 59182 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=2122487355 TSecr=30472…
10 0.027605333 10.0.139.4 10.0.139.1 FTP 76 Request: AUTH TLS
11 0.028969485 10.0.139.1 10.0.139.4 TCP 66 21 → 59182 [ACK] Seq=21 Ack=11 Win=65280 Len=0 TSval=3047215044 TSecr=2122…
12 0.028969806 10.0.139.1 10.0.139.4 FTP 97 Response: 234 Proceed with negotiation.
13 0.032802330 10.0.139.4 10.0.139.1 TLSv1.3 517 Client Hello (SNI=ftp.asir11.asir)
14 0.034725904 10.0.139.1 10.0.139.4 TLSv1.3 165 Hello Retry Request, Change Cipher Spec
15 0.044574190 10.0.139.4 10.0.139.1 TLSv1.3 449 Client Hello (SNI=ftp.asir11.asir)
16 0.047683589 10.0.139.1 10.0.139.4 TLSv1.3 1735 Server Hello, Application Data, Application Data, Application Data, Applic…
17 0.047907095 10.0.139.4 10.0.139.1 TCP 66 59182 → 21 [ACK] Seq=845 Ack=1820 Win=62592 Len=0 TSval=2122487381 TSecr=3…
18 0.048692349 10.0.139.4 10.0.139.1 TLSv1.3 72 Change Cipher Spec
19 0.049115635 10.0.139.4 10.0.139.1 TLSv1.3 96 Application Data
20 0.049541155 10.0.139.1 10.0.139.4 TCP 66 21 → 59182 [ACK] Seq=1820 Ack=881 Win=64640 Len=0 TSval=3047215065 TSecr=2…
21 0.051085169 10.0.139.4 10.0.139.1 TLSv1.3 140 Application Data
22 0.051747047 10.0.139.1 10.0.139.4 TLSv1.3 321 Application Data
23 0.052008033 10.0.139.1 10.0.139.4 TLSv1.3 321 Application Data
24 0.064524058 10.0.139.1 10.0.139.4 TCP 321 [TCP Retransmission] 21 → 59182 [PSH, ACK] Seq=2075 Ack=955 Win=64640 Len=…
25 0.064546583 10.0.139.4 10.0.139.1 TCP 78 59182 → 21 [ACK] Seq=955 Ack=2330 Win=62208 Len=0 TSval=2122487398 TSecr=3…
30 42.953374070 10.0.139.4 10.0.139.1 TLSv1.3 103 Application Data
31 42.954519217 10.0.139.1 10.0.139.4 TLSv1.3 122 Application Data
32 42.958931472 10.0.139.4 10.0.139.1 TCP 66 59182 → 21 [ACK] Seq=992 Ack=2386 Win=62208 Len=0 TSval=2122530288 TSecr=3…
33 42.959770946 10.0.139.4 10.0.139.1 TLSv1.3 101 Application Data
34 43.000838394 10.0.139.1 10.0.139.4 TCP 66 21 → 59182 [ACK] Seq=2386 Ack=1027 Win=64640 Len=0 TSval=3047257995 TSecr=…
35 43.001522846 10.0.139.1 10.0.139.4 TLSv1.3 111 Application Data
36 43.001725492 10.0.139.4 10.0.139.1 TLSv1.3 94 Application Data
37 43.002191530 10.0.139.1 10.0.139.4 TCP 66 21 → 59182 [ACK] Seq=2431 Ack=1055 Win=64640 Len=0 TSval=3047257996 TSecr=…
38 43.002678649 10.0.139.1 10.0.139.4 TLSv1.3 107 Application Data
39 43.002783029 10.0.139.4 10.0.139.1 TLSv1.3 94 Application Data
Frame 12: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface enp0s8, id 0
Ethernet II, Src: PCSSystemtec_ad:bc:be (08:00:27:ad:bc:be), Dst: PCSSystemtec_5e:44:e1 (08:00:27:5e:44:e1)
Internet Protocol Version 4, Src: 10.0.139.1, Dst: 10.0.139.4
Transmission Control Protocol, Src Port: 21, Dst Port: 59182, Seq: 21, Ack: 11, Len: 31
File Transfer Protocol (FTP)
[Current working directory:]
0000 08 00 27 5e 44 e1 08 00 27
0010 00 53 15 0d 40 00 40 06 fb
0020 8b 04 00 15 e7 2e 6a 52 7a
0030 01 fe 55 e9 00 00 01 01 08
0040 96 41 32 33 34 20 50 72 6f
0050 74 68 20 6e 65 67 6f 74 69
0060 0a



- ¿Sobre qué puerto se realiza la conexión? ¿Hay alguna diferencia con respecto al punto 4?

Por el puerto 21 del lado del **servidor**

- ¿Puedes ver el usuario y la contraseña? ¿Por qué?

No, ya que el tráfico se cifra con TLS

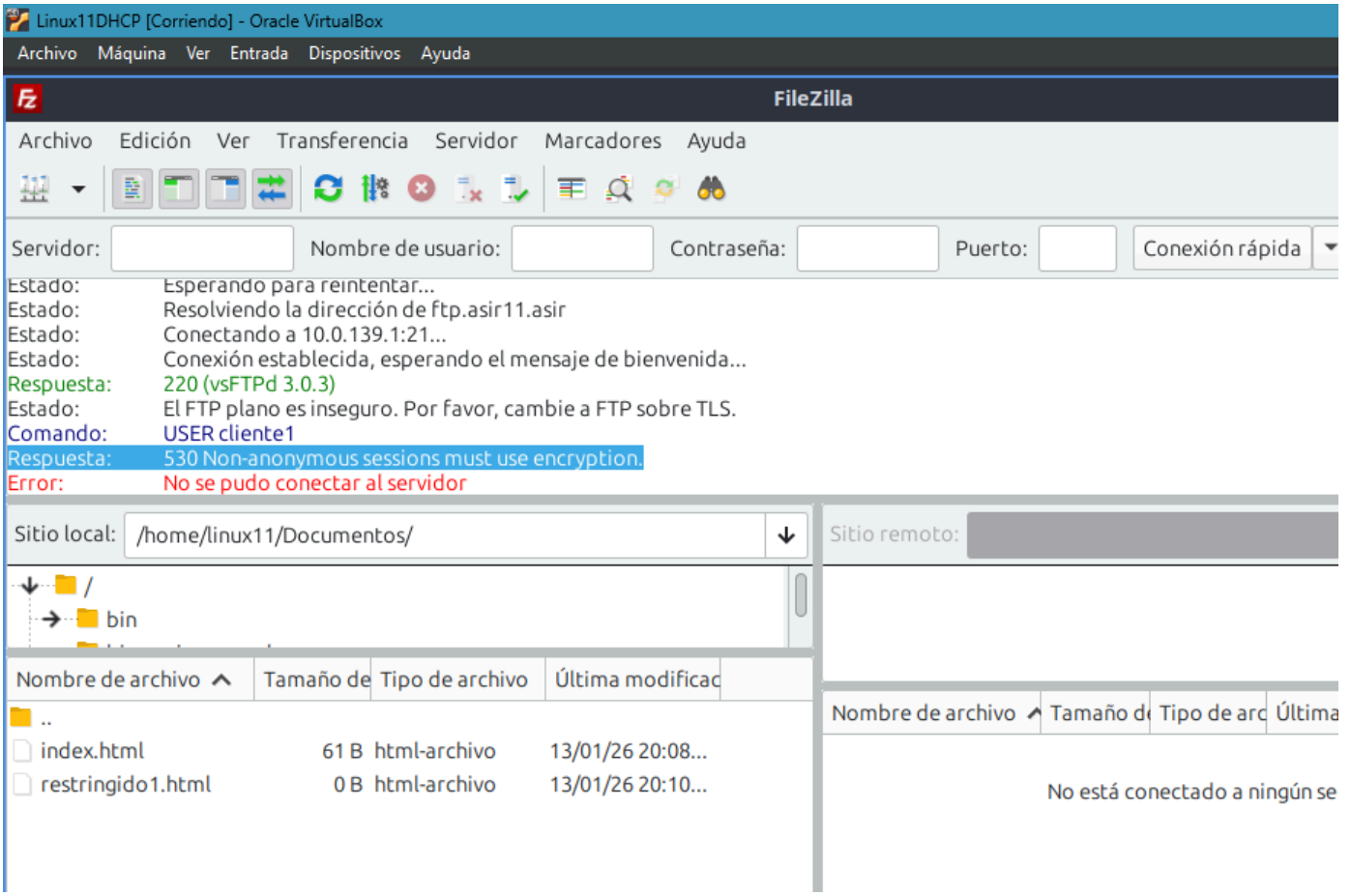
- ¿Qué puertos se utilizan? ¿Son coherentes?

El **puerto 21** para el control y el **puerto 20** para la transferencia de datos, Son coherentes porque el funcionamiento del **FTP Explícito (FTPES)** consiste precisamente en utilizar los puertos estándar del protocolo FTP original (21 para control y 20 para datos en modo activo). El cifrado encapsula el tráfico sin cambiar la arquitectura de puertos estándar del protocolo.

6. Consulta en la web de directivas para qué sirven y en qué se diferencian las directivas ssl_enable, ssl_sslv2, ssl_sslv3, ssl_tlsv1

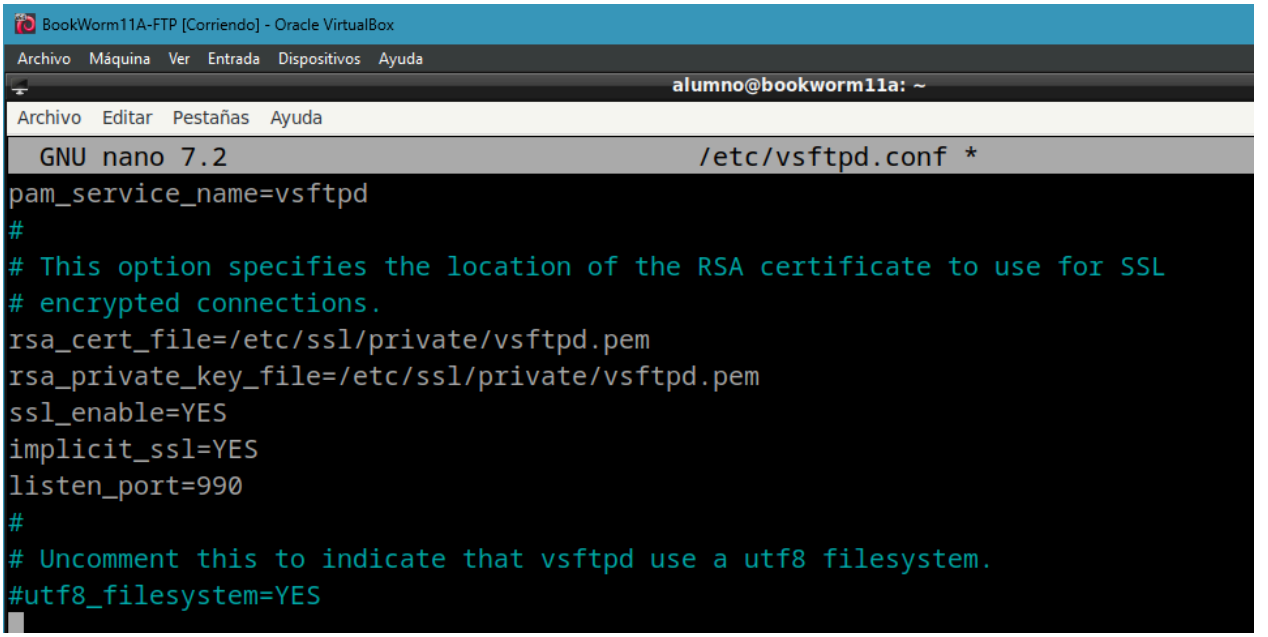
- `ssl_enable`: El interruptor general para habilitar ssl.
- `ssl_sslv2` y `ssl_sslv3`: Protocolos antiguos y rotos (inseguros)
- `ssl_tlsv1`: El estándar base actual (aunque idealmente se debe usar TLS 1.2 o 1.3).

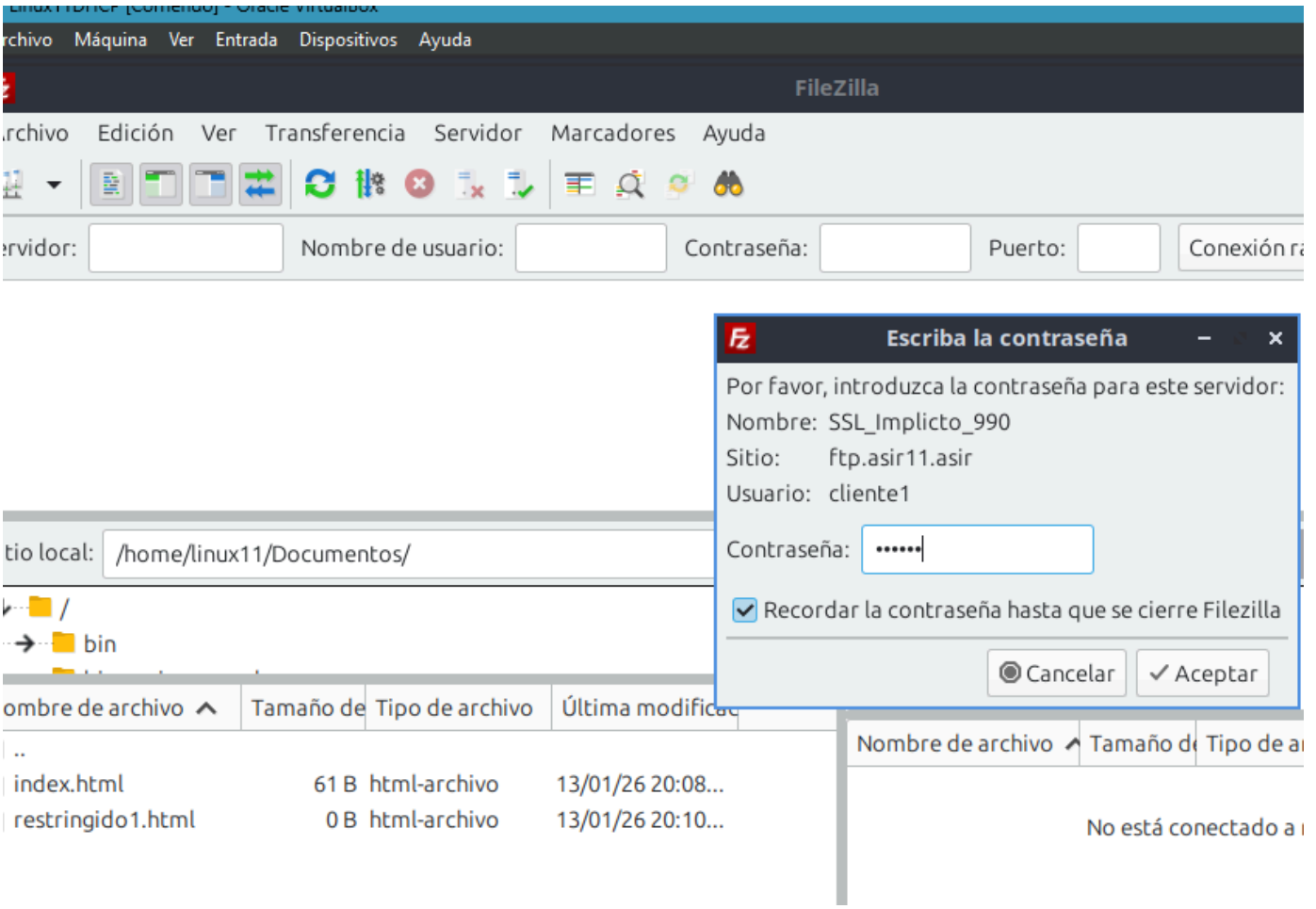
7. Ahora que tienes habilitada la directiva ssl_enable, vuelve a probar la conexión NoSSL y extrae conclusiones al respecto.

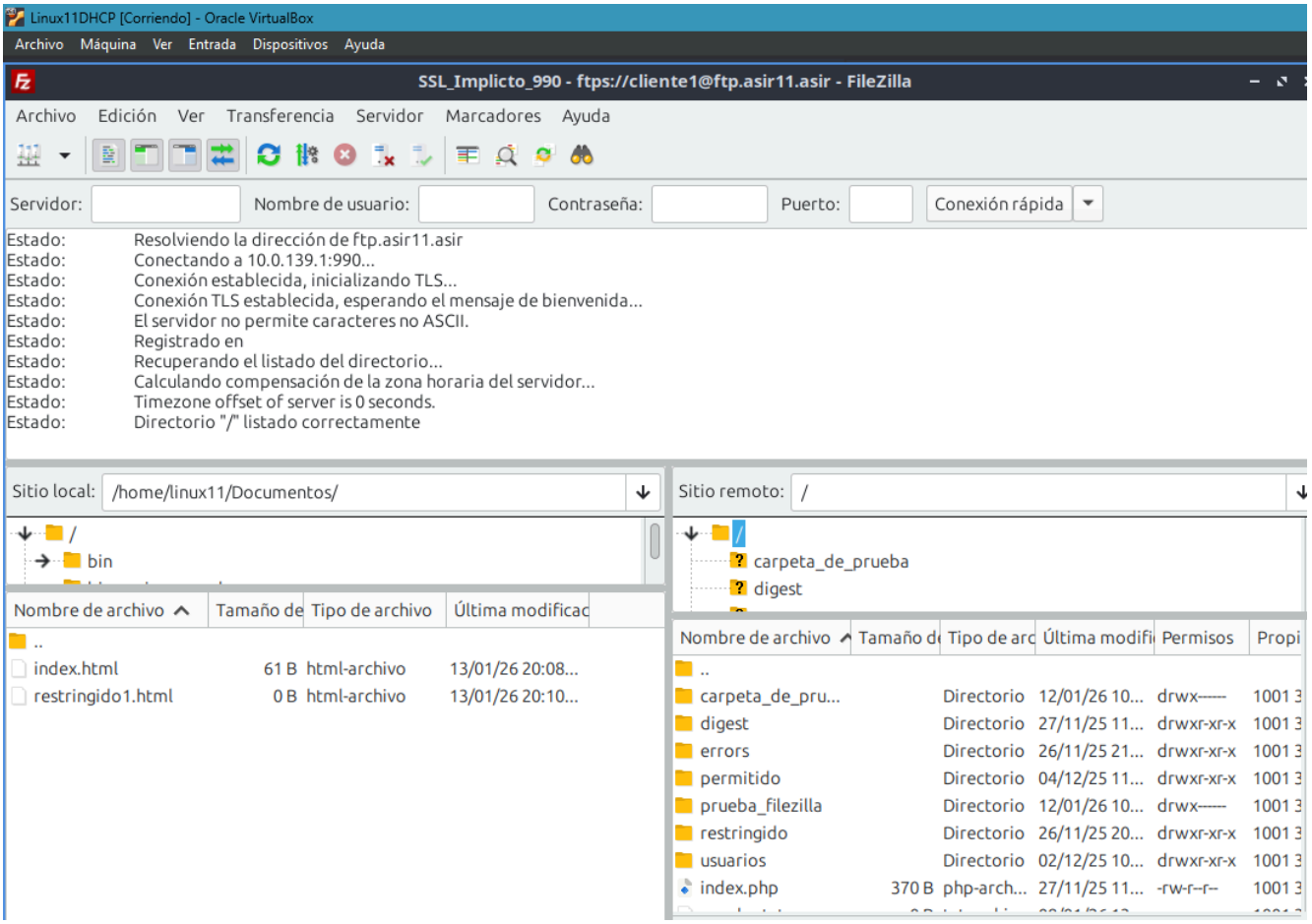


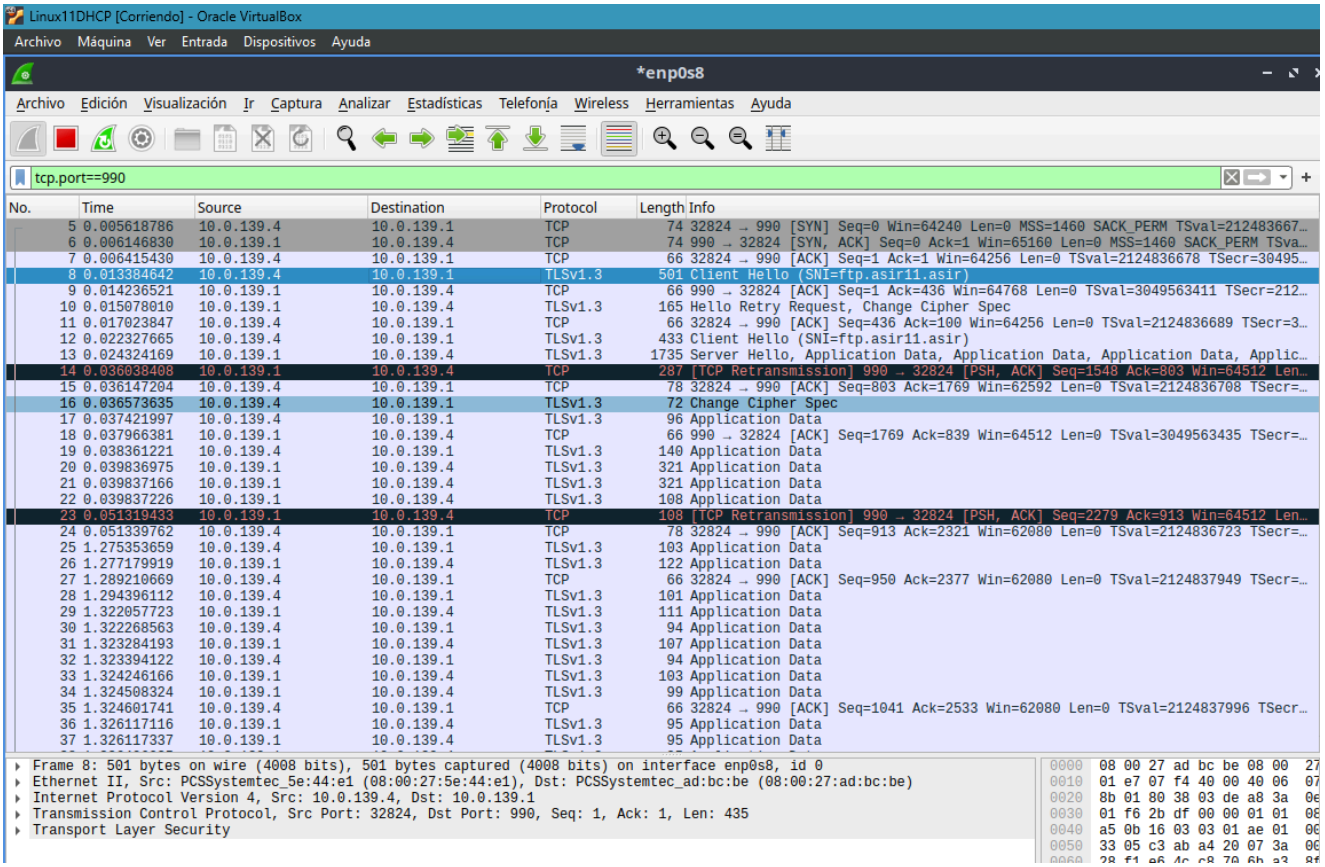
No permite la conexion NoSSL por defecto el servidor al tener habilitado al directiva ssl_enable, sin embargo, si quisieramos que funcionara el NoSSL deberiamos de añadir la directiva force_local_logins_ssl=NO aunque no es recomendable por la seguridad

8. Volvamos al modo 'FTP implícito sobre SSL',. Modifica la configuración del servidor para que pueda utilizarse este modo de conexión. Modifica las directivas que consideres necesarias para ello para conseguir la conexión y transferencia de archivos de dos formas
    - Atendiendo a los puertos bien conocidos definidos para el servicio FTP seguro en modo activo (para seleccionar de modo explícito el tipo de transferencia lo puedes hacer en la solapa 'Opciones de transferencia' del sitio que estés configurando.

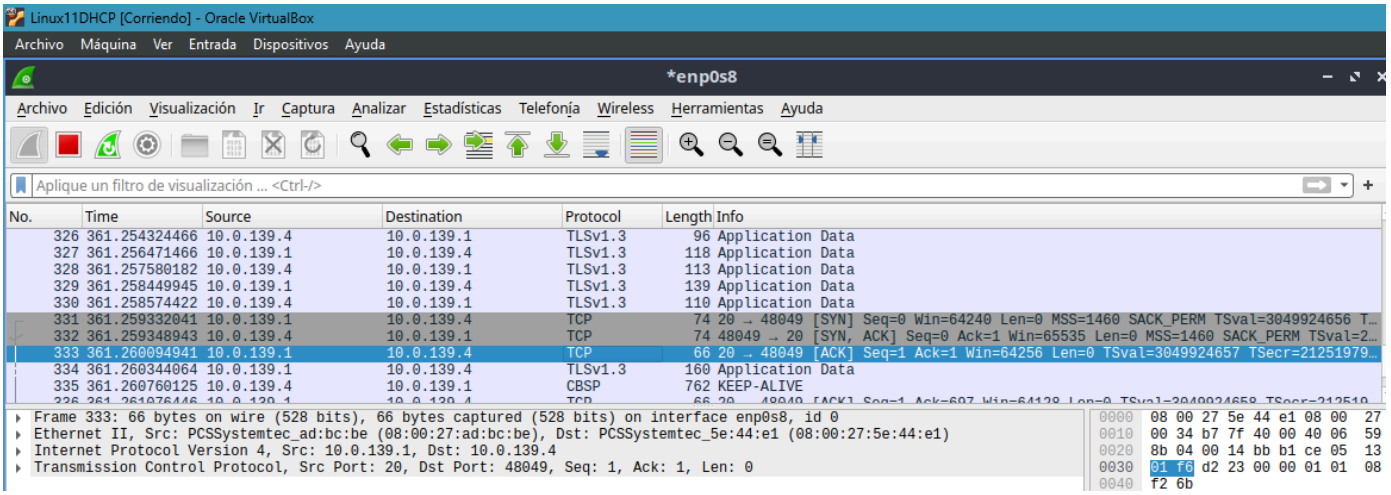

BookWorm11A-FTP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
alumno@bookworm11a: ~
Archivo Editar Pestañas Ayuda
GNU nano 7.2 /etc/vsftpd.conf *
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
implicit_ssl=YES
listen_port=990
#
Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES


FileZilla
Archivo Edición Ver Transferencia Servidor Marcadores Ayuda
Nombre de usuario:
Contraseña:
Puerto:
Escriba la contraseña
Por favor, introduzca la contraseña para este servidor:
Nombre: SSL_Implicto_990
Sitio: ftp.asir11.asir
Usuario: cliente1
Contraseña:
Recordar la contraseña hasta que se cierre Filezilla
Cancelar
Aceptar
/home/linux11/Documentos/
bin
Nombre de archivo
Tamaño de
Tipo de archivo
Última modificac
index.html 61 B html-archivo 13/01/26 20:08...
restringido1.html 0 B html-archivo 13/01/26 20:10...
No está conectado a


Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
SSL_Implicto_990 - ftps://cliente1@ftp.asir11.asir - FileZilla
Archivo Edición Ver Transferencia Servidor Marcadores Ayuda
Servidor: Nombre de usuario: Contraseña: Puerto: Conexión rápida
Estado: Resolviendo la dirección de ftp.asir11.asir
Estado: Conectando a 10.0.139.1:990...
Estado: Conexión establecida, inicializando TLS...
Estado: Conexión TLS establecida, esperando el mensaje de bienvenida...
Estado: El servidor no permite caracteres no ASCII.
Estado: Registrado en
Estado: Recuperando el listado del directorio...
Estado: Calculando compensación de la zona horaria del servidor...
Estado: Timezone offset of server is 0 seconds.
Estado: Directorio "/" listado correctamente
Sitio local: /home/linux11/Documentos/
/
bin
Nombre de archivo Tamaño de Tipo de archivo Última modificac
..
index.html 61 B html-archivo 13/01/26 20:08...
restringido1.html 0 B html-archivo 13/01/26 20:10...
Sitio remoto: /
/
carpeta_de_prueba
digest
Nombre de archivo Tamaño d Tipo de arc Última modifi Permisos Propi
..
carpeta_de_pru... Directorio 12/01/26 10... drwx------ 1001 3
digest Directorio 27/11/25 11... drwxr-xr-x 1001 3
errors Directorio 26/11/25 21... drwxr-xr-x 1001 3
permitido Directorio 04/12/25 11... drwxr-xr-x 1001 3
prueba_filezilla Directorio 12/01/26 10... drwx------ 1001 3
restringido Directorio 26/11/25 20... drwxr-xr-x 1001 3
usuarios Directorio 02/12/25 10... drwxr-xr-x 1001 3
index.php 370 B php-arch... 27/11/25 11... -rw-r--r-- 1001 3

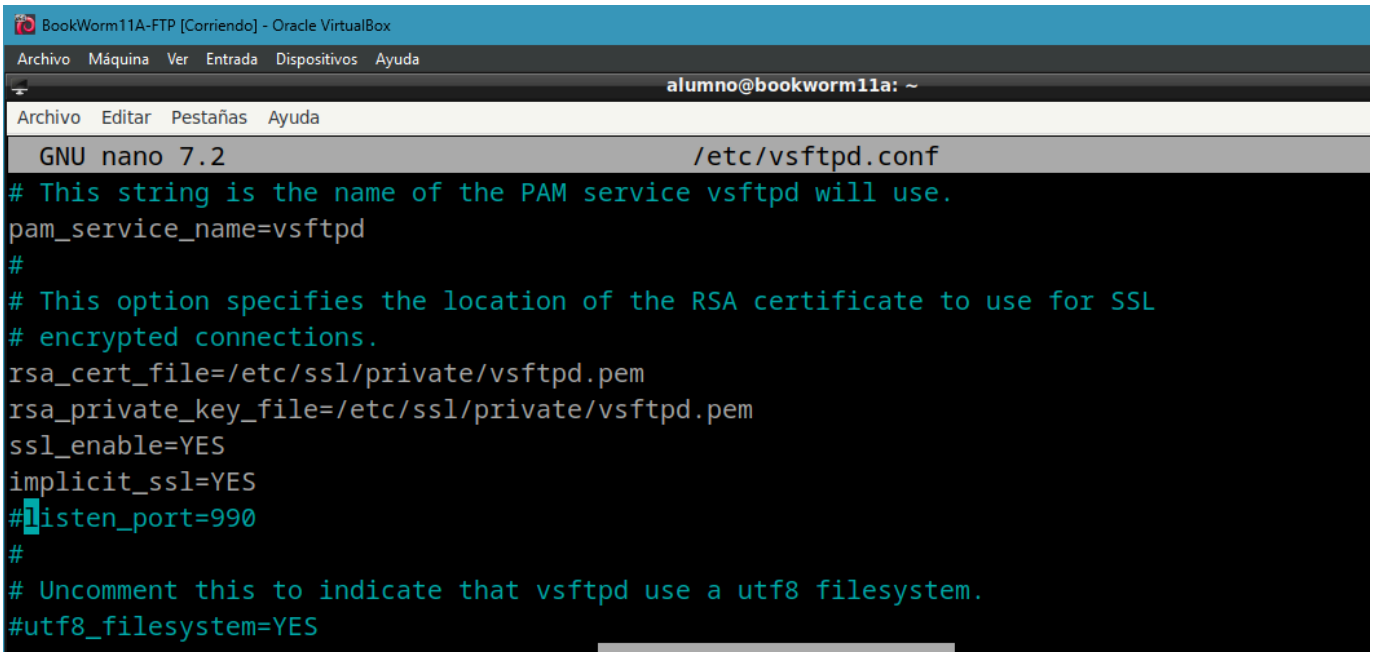

Linux11DHCP [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
*enp0s8
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
tcp.port==990
No. Time Source Destination Protocol Length Info
5 0.005618786 10.0.139.4 10.0.139.1 TCP 74 32824 → 990 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=212483667…
6 0.006146830 10.0.139.1 10.0.139.4 TCP 74 990 → 32824 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSva…
7 0.006415430 10.0.139.4 10.0.139.1 TCP 66 32824 → 990 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2124836678 TSecr=30495…
8 0.013384642 10.0.139.4 10.0.139.1 TLSv1.3 501 Client Hello (SNI=ftp.asir11.asir)
9 0.014236521 10.0.139.1 10.0.139.4 TCP 66 990 → 32824 [ACK] Seq=1 Ack=436 Win=64768 Len=0 TSval=3049563411 TSecr=212…
10 0.015078010 10.0.139.1 10.0.139.4 TLSv1.3 165 Hello Retry Request, Change Cipher Spec
11 0.017023847 10.0.139.4 10.0.139.1 TCP 66 32824 → 990 [ACK] Seq=436 Ack=100 Win=64256 Len=0 TSval=2124836689 TSecr=3…
12 0.022327665 10.0.139.4 10.0.139.1 TLSv1.3 433 Client Hello (SNI=ftp.asir11.asir)
13 0.024324169 10.0.139.1 10.0.139.4 TLSv1.3 1735 Server Hello, Application Data, Application Data, Applic…
14 0.036038408 10.0.139.1 10.0.139.4 TCP 287 [TCP Retransmission] 990 → 32824 [PSH, ACK] Seq=1548 Ack=803 Win=64512 Len…
15 0.036147204 10.0.139.4 10.0.139.1 TCP 78 32824 → 990 [ACK] Seq=803 Ack=1769 Win=62592 Len=0 TSval=2124836708 TSecr=…
16 0.036573635 10.0.139.4 10.0.139.1 TLSv1.3 72 Change Cipher Spec
17 0.037421997 10.0.139.4 10.0.139.1 TLSv1.3 96 Application Data
18 0.037966381 10.0.139.1 10.0.139.4 TCP 66 990 → 32824 [ACK] Seq=1769 Ack=839 Win=64512 Len=0 TSval=3049563435 TSecr=…
19 0.038361221 10.0.139.4 10.0.139.1 TLSv1.3 140 Application Data
20 0.039836975 10.0.139.1 10.0.139.4 TLSv1.3 321 Application Data
21 0.039837166 10.0.139.1 10.0.139.4 TLSv1.3 321 Application Data
22 0.039837226 10.0.139.1 10.0.139.4 TLSv1.3 108 Application Data
23 0.051319433 10.0.139.1 10.0.139.4 TCP 108 [TCP Retransmission] 990 → 32824 [PSH, ACK] Seq=2279 Ack=913 Win=64512 Len…
24 0.051339762 10.0.139.4 10.0.139.1 TCP 78 32824 → 990 [ACK] Seq=913 Ack=2321 Win=62080 Len=0 TSval=2124836723 TSecr=…
25 1.275353659 10.0.139.4 10.0.139.1 TLSv1.3 103 Application Data
26 1.277179919 10.0.139.1 10.0.139.4 TLSv1.3 122 Application Data
27 1.289210669 10.0.139.4 10.0.139.1 TCP 66 32824 → 990 [ACK] Seq=950 Ack=2377 Win=62080 Len=0 TSval=2124837949 TSecr=…
28 1.294396112 10.0.139.4 10.0.139.1 TLSv1.3 101 Application Data
29 1.322057723 10.0.139.1 10.0.139.4 TLSv1.3 111 Application Data
30 1.322268563 10.0.139.4 10.0.139.1 TLSv1.3 94 Application Data
31 1.323284193 10.0.139.1 10.0.139.4 TLSv1.3 107 Application Data
32 1.323394122 10.0.139.4 10.0.139.1 TLSv1.3 94 Application Data
33 1.324246166 10.0.139.1 10.0.139.4 TLSv1.3 103 Application Data
34 1.324508324 10.0.139.1 10.0.139.4 TLSv1.3 99 Application Data
35 1.324601741 10.0.139.4 10.0.139.1 TCP 66 32824 → 990 [ACK] Seq=1041 Ack=2533 Win=62080 Len=0 TSval=2124837996 TSecr…
36 1.326117116 10.0.139.1 10.0.139.4 TLSv1.3 95 Application Data
37 1.326117337 10.0.139.1 10.0.139.4 TLSv1.3 95 Application Data
Frame 8: 501 bytes on wire (4008 bits), 501 bytes captured (4008 bits) on interface enp0s8, id 0
Ethernet II, Src: PCSSystemtec_5e:44:e1 (08:00:27:5e:44:e1), Dst: PCSSystemtec_ad:bc:be (08:00:27:ad:bc:be)
Internet Protocol Version 4, Src: 10.0.139.4, Dst: 10.0.139.1
Transmission Control Protocol, Src Port: 32824, Dst Port: 990, Seq: 1, Ack: 1, Len: 435
Transport Layer Security
0000 08 00 27 ad bc be 08 00 27
0010 01 e7 07 f4 40 00 40 06 07
0020 8b 01 80 38 03 de a8 3a 0e
0030 01 f6 2b df 00 00 01 01 08
0040 a5 0b 16 03 03 01 ae 01 00
0050 33 05 c3 ab a4 20 07 3a 00

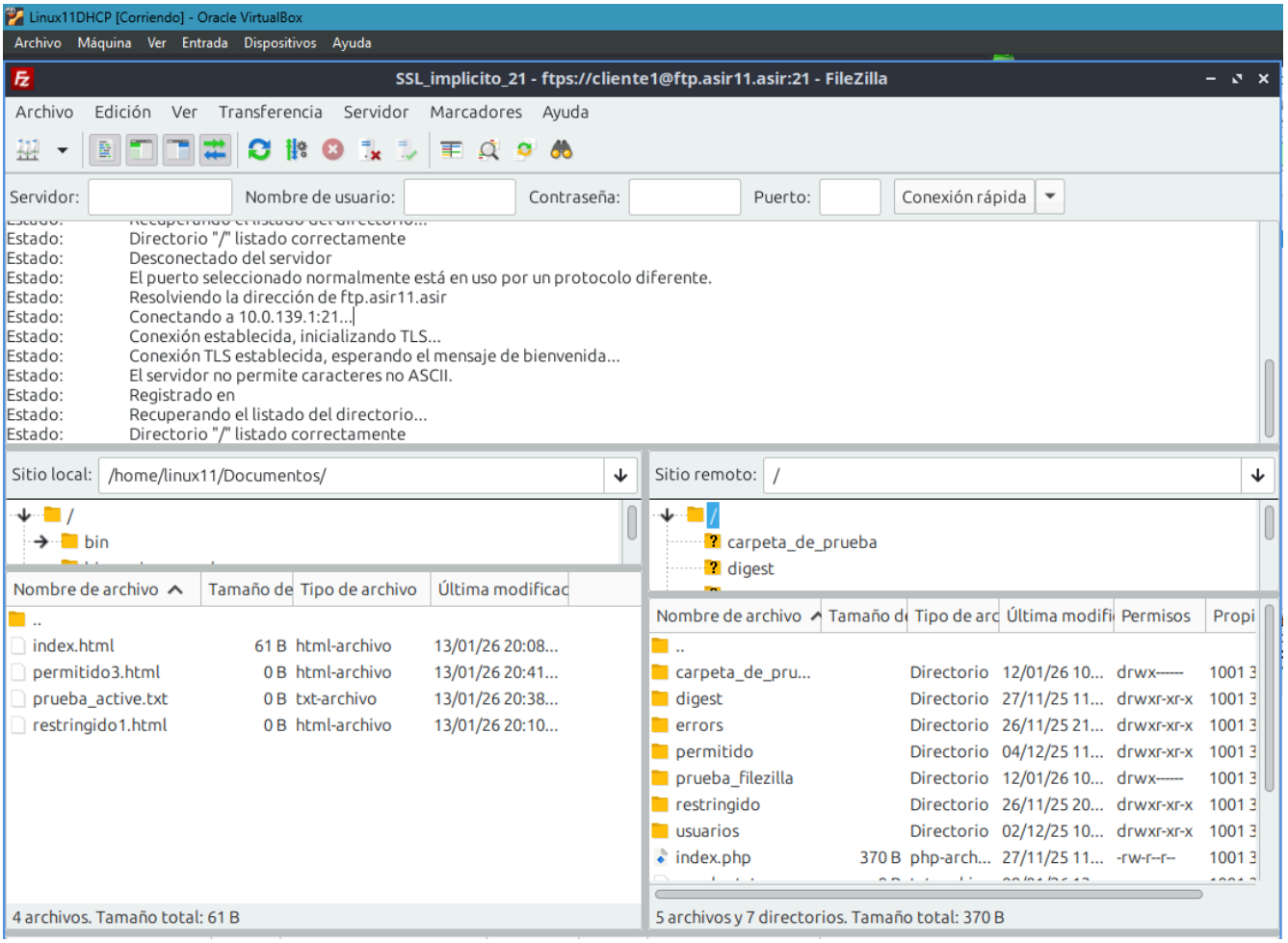
TRANSFERENCIA DE ARCHIVOS

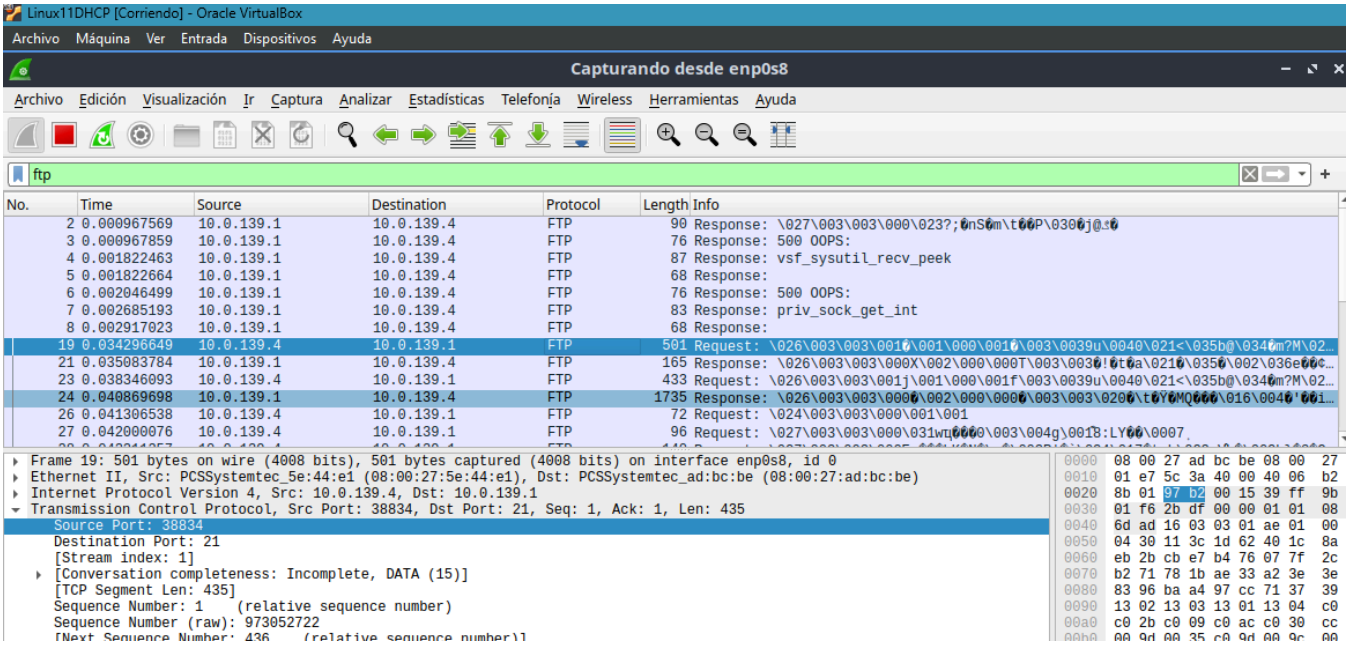


Aunque la teoría indica que el FTPS Implícito suele usar el puerto 989 para datos, mi servidor `vsftpd` está utilizando el puerto 20. Esto se debe a que la directiva `connect_from_port_20=YES` en la configuración fuerza el uso del puerto de datos FTP estándar, independientemente del cifrado SSL.

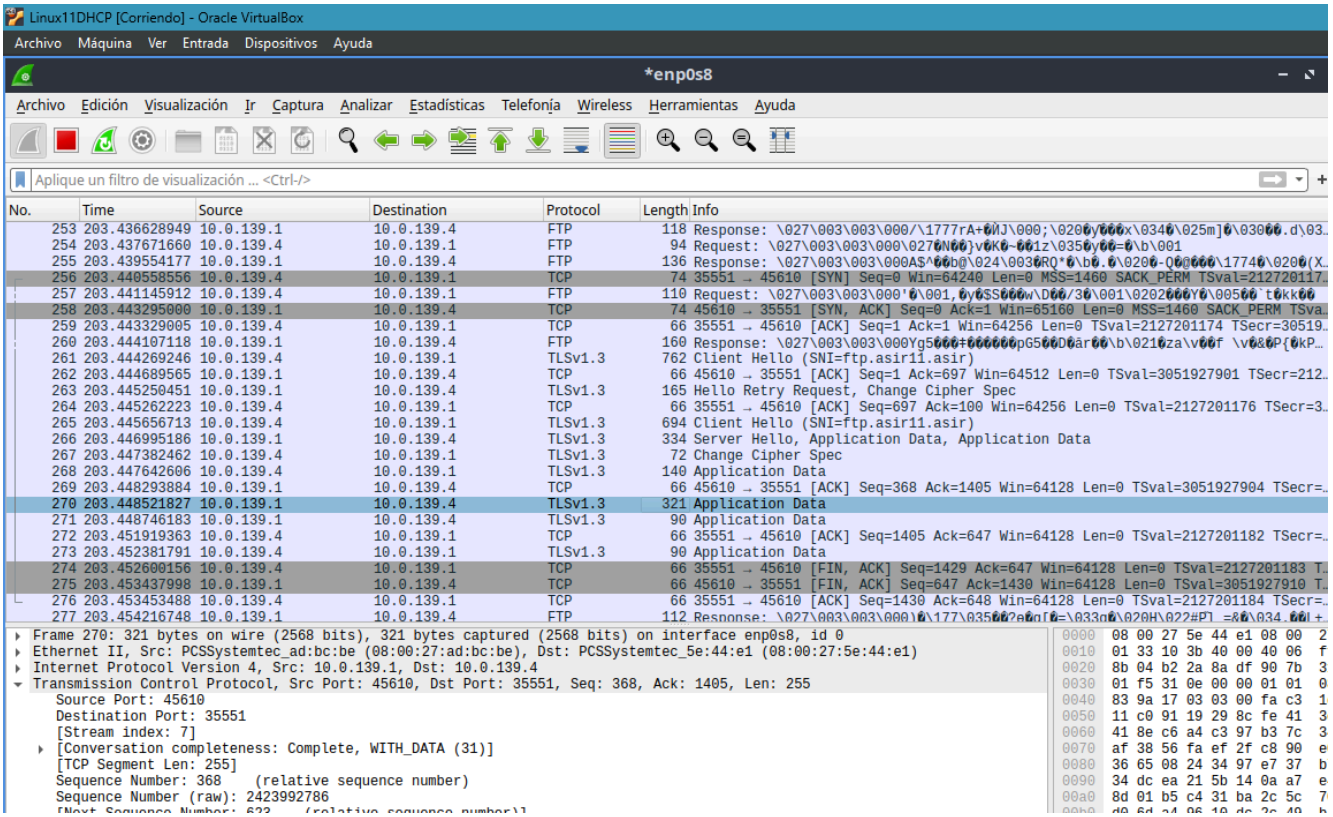
- Utilizando los puertos tradicionales de FTP para modo no seguro para el modo seguro. Prueba en este caso la conexión en modo pasivo







TRANSFERENCIA DE ARCHIVOS



Al transferir archivos en **Modo Pasivo** el cliente conecta a un puerto alto aleatorio del servidor en lugar del 989.

9. Con lo que has aprendido hasta ahora reflexiona sobre si es posible el funcionamiento SSL y no SSL simultáneo en el mismo servidor.

En modo Explícito (Puerto 21): SÍ. Depende de si fuerzas el SSL (`force_local_logins_ssl`). Si no lo fuerzas, el servidor acepta clientes seguros e inseguros por el mismo puerto.

10. Con lo que has aprendido hasta ahora reflexiona sobre si es posible el funcionamiento SSL explícito e implícito simultáneamente en el mismo servidor.

En el mismo servidor vsftpd: NO de forma nativa sencilla.

La directiva `implicit_ssl=YES` cambia el comportamiento de todo el socket de escucha. Si activas Implícito, el puerto espera SSL inmediato. Si usas Explícito, espera texto plano primero.Tendrías que ejecutar **dos instancias** de vsftpd con dos archivos `vsftpd.conf` distintos (uno escuchando en el 21 para Explícito y otro en el 990 para Implícito).

Recoge toda la información relevante así como las evidencias necesarias como capturas

Realiza una copia de seguridad de la configuración en otro archivo para no perderla de cara a las próximas prácticas (vsftpd.conf.practica4)