

# PRÁCTICA

## SERVICIOS TELEMÁTICOS

Jorge López Saura

Dni: 48745793-F

Correo electrónico: [jorge.lopez5@um.es](mailto:jorge.lopez5@um.es)

Curso: 3º

Subgrupo: 1.2

# ÍNDICE

<b>1.Introducción.....</b>	<b>3</b>
1.1 Descripción del escenario.....	3
1.2 Versiones de software.....	3
<b>2.Descripción de las configuraciones.....</b>	<b>4</b>
2.1 Configuración del servicio Apache HTTP/HTTPS.....	4
2.2 Configuración de un servidor de correo SMTP/POP.....	10
2.3 Configuración de DNS.....	13
2.4 Configuración de IPsec.....	17
<b>3.Descripción de la implementación del servicio Web.....</b>	<b>19</b>
<b>4.Trazas.....</b>	<b>22</b>
4.1 Trazas servicio web implementado.....	22
4.2 Trazas servicio web de Apache.....	25
4.3 Trazas servicio web seguro de Apache.....	30
4.4 Trazas SMTP/POP.....	39
4.5 Trazas IPsec.....	46
<b>5.Problemas encontrados en el desarrollo del escenario.....</b>	<b>48</b>
<b>6.Número de horas aproximadas empleadas en cada apartado y documentación.....</b>	<b>48</b>
<b>7. Conclusiones.....</b>	<b>48</b>

# 1.Introducción

## 1.1 Descripción del escenario

En esta práctica se va a desarrollar un escenario formado por un equipo servidor (servidor.sstt5793.org) el cual tendrá asociada la dirección IP 192.168.236.4 y un equipo cliente (cliente.sstt5793.org) al cual se le asignará la dirección IP 192.168.236.3, que realizará peticiones al servidor y se invocarán cada uno de los servicios configurados en dicho servidor.

En el equipo servidor se usarán los siguientes servicios:

- Un servidor web HTTP implementado en lenguaje c.
- Un servidor web de Apache HTTP/HTTPS.
- Un servidor de correo SMTP y un servidor POP para el acceso a correo.
- Un servidor DNS raíz que gestiona el dominio “sstt5793.org”.
- Una autoridad de certificación (CA) para la generación de certificados X.509
- Un protocolo de seguridad de Internet (IPsec) cuya función es asegurar las comunicaciones sobre el protocolo de internet (IP) autenticando y/o cifrando cada paquete IP, además de establecer claves de cifrado.

En el equipo cliente se usará:

- Un cliente SMTP/POP (Thunderbird)
- Un protocolo de seguridad de Internet (IPSec), al igual que en el servidor, para proporcionar seguridad sobre el protocolo IP.

## 1.2 Versiones de software

Las versiones de los servicios usados en la práctica son los siguientes:

- Servidor Apache: Apache2 versión 2.4.18
- SMTP/POP3 : Para SMTP exim4 versión 4.86\_2 y para POP3 dovecot versión 2.2.22 (fe789d2)
- Servidor DNS: Bind9 versión 9.10.3-P4-Ubuntu

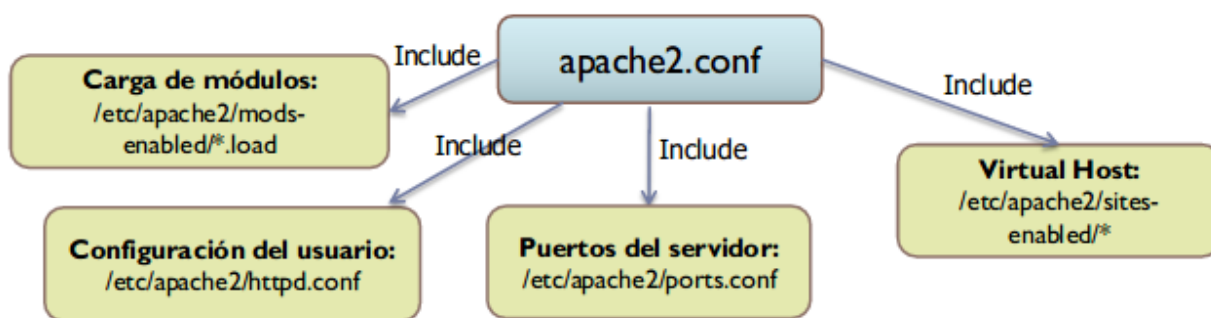
## 2.Descripción de las configuraciones

### 2.1 Configuración del servicio Apache HTTP/HTTPS

Para montar el servicio Apache, en primer lugar hay que ejecutar en una terminal el siguiente comando:

- sudo apt-get install apache2

Los archivos de configuración de apache2 se encuentran en la carpeta /etc/apache2 y son los mostrados a continuación:



donde “apache2.conf” es el fichero de configuración principal, e incluye a otros ficheros para modularizar y simplificar la configuración.

En primer lugar, para que la dirección del virtualHost sea resoluble, se crea una entrada [www.sstt5793.org](http://www.sstt5793.org) en el fichero “/etc/hosts” tanto del cliente como del servidor quedando el fichero de la siguiente manera:

```
jorge@ubuntuServer:/etc/apache2/sites-available$ cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      ubuntuServer
192.168.236.4  www.sstt5793.org
```

La entrada creada anteriormente se eliminará en ambos ficheros cuando se configure el servidor DNS, ya que este será el encargado de realizar la resolución de nombres.

El siguiente paso es crear el directorio donde estará el fichero “index.html” a devolver cada vez que se solicite la dirección [www.sstt5793.org](http://www.sstt5793.org) .En este caso el directorio será “/var/www/sstt5793”.

A continuación se crea un nuevo virtualHost en el directorio “/etc/apache2/sites-available”.En este caso se crea el fichero “sstt5793.conf” que queda de la siguiente manera:

```
<VirtualHost *:80>
    ServerAdmin usuario1@sstt5793.org
    ServerName www.sstt5793.org
    DocumentRoot /var/www/sstt5793
    <Directory /var/www/sstt5793>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>
</VirtualHost>

<VirtualHost *:443>
    ServerAdmin usuario1@sstt5793.org
    ServerName www.sstt5793.org
    DocumentRoot /var/www/sstt5793
    <Directory /var/www/sstt5793>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>
</VirtualHost>
```

Como se puede observar en la imagen anterior se han creado dos entradas, una de ellas que trata las peticiones realizadas en el puerto estándar para HTTP (puerto 80) y la otra que trata las peticiones realizadas en el puerto estándar para HTTPS (puerto 443), ambas entradas configuradas para el dominio sstt5793.org.

En “Directory” y en “DocumentRoot” se indica el directorio que se ha creado previamente donde se encuentran los ficheros html. En “serverName” se indica el nombre de host para el que se tendrá que atender la solicitud.

Una vez se ha creado el virtualHost, para activarlo se ejecuta el siguiente comando, en el directorio donde se encuentra el fichero .conf (“etc/apache2/sites-available”):

- sudo a2ensite sstt5793.conf

Tras ejecutar este comando aparece un enlace en “/etc/apache2/sites-enabled/”, para el fichero “sstt5793.conf” como se muestra a continuación:

```
jorge@ubuntuServer:/etc/apache2/sites-enabled$ ls -l
total 0
lrwxrwxrwx 1 root root 31 mar  9 16:51 ejemplo.conf -> ../sites-available/ejemplo.conf
lrwxrwxrwx 1 root root 32 mar 29 12:57 sstt5793.conf -> ../sites-available/sstt5793.conf
lrwxrwxrwx 1 root root 27 mar  9 18:16 st1.conf -> ../sites-available/st1.conf
lrwxrwxrwx 1 root root 27 mar  9 18:16 st2.conf -> ../sites-available/st2.conf
```

Tras configurarlo todo hay que arrancar el servidor, con el siguiente comando:

- /etc/init.d/apache2 start

Tras esto, el servidor apache ya estará en ejecución.

Para configurar el acceso via HTTPS (puerto 443) se va a crear una PKI (Public Key Infrastructure) para administrar los certificados necesarios para el resto de servicios. Para ello en primer lugar hay que definir una estructura de archivos para la **CA** (Autoridad de certificación) realizando los siguientes pasos:

1. Se crea la carpeta de trabajo para la CA en la carpeta de usuario, en este caso la carpeta de la CA se llama “ssttCA” y se crea con el comando “mkdir”

2. Se crea el archivo crlnumber con valor 00 mediante el siguiente comando:

```
echo 0 > crlnumber
```

3. Se crea un “index.txt” vacío con el comando “touch index.txt”

4. Se crea un fichero serial con valor 1 (número de serie de los certificados) con el comando:

```
echo 01 > serial
```

5. Se crean las carpetas “private”, “newcerts” y “certs” dentro de la carpeta de trabajo “ssttCA” con el comando “mkdir”.

El siguiente paso es configurar el fichero “/usr/lib/ssl/openssl.cnf” donde se realiza la configuración de la PKI. Para realizar la configuración de la CA en la sección “CA\_default” hay que poner los siguientes valores:

<b>dir</b>	= /home/jorge/ssttCA
<b>certs</b>	= \$dir/certs
<b>crl_dir</b>	= \$dir/crl
<b>database</b>	= \$dir/index.txt
<b>new_certs_dir</b>	= \$dir/newcerts
<b>certificate</b>	= \$dir/cacert.pem
<b>serial</b>	= \$dir/serial
<b>crlnumber</b>	= \$dir/crlnumber
<b>crl</b>	= \$dir/crl.pem
<b>private_key</b>	= \$dir/private/cakey.pem
<b>default_days</b>	= 365
<b>default_crl_days</b>	= 30

También hay que configurar las estructuras de nombres que se usarán para identificar a las entidades. Para ello hay que modificar el fichero “openssl.cnf” mencionado anteriormente, en concreto, la sección “req\_distinguished\_name” estableciendo los siguientes valores:

<b>countryName_default</b>	= ES
<b>stateOrProvinceName_default</b>	= Murcia
<b>0.organizationName_default</b>	= UMU
<b>organizationalUnitName_default</b>	= SSTT

El siguiente paso es generar el certificado de la CA, para ello, hay que ejecutar el siguiente comando en la carpeta de trabajo “ssttCA”:

```
openssl req -x509 -newkey rsa:2048 -keyout cakey.pem -out cacert.pem -days 3650
```

En el comando anterior se indica que la clave pública de la CA tiene una longitud de 2048 bits (-newkey rsa:2048), con el parámetro “days” se especifica la duración del certificado en días.

Durante la ejecución del comando, hay que indicar los valores para la identidad de la CA. Algunos valores solicitados ya se han introducido anteriormente (en la configuración de la estructura de nombres). Los nuevos valores a introducir son los

correspondientes al “**Common Name**” al cual se le asigna el valor “ca.sstt5793.org” y al “**Email address**”, el cual, se deja en blanco.

Tras la ejecución del comando anterior hay que mover el archivo con la clave privada de la CA (cakey.pem) a la carpeta “private” creada anteriormente.

El siguiente paso es generar un certificado para el servicio web “[www.sstt5793.org](http://www.sstt5793.org)”, para ello hay que ejecutar el siguiente comando:

```
openssl req -new -nodes -newkey rsa:2048 -keyout serverkey.pem -out servercsr.pem
```

donde se indica que la longitud de la clave pública para el servicio web es de 2048 bits.

Al ejecutar el comando, se solicitará introducir una serie de valores que deberán de coincidir con los valores ya introducidos para la CA, excepto para el campo “Common Name”, que en este caso se le asigna el valor “[www.sstt5793.org](http://www.sstt5793.org)”. El campo “Email Address”, se deja en blanco. Además en este caso tampoco se introduce una contraseña para proteger la clave privada.

Tras la ejecución del comando se generan los archivos “serverkey.pem” que contiene la clave privada RSA para el servicio web y el archivo “servercsr.pem” que contiene una solicitud de certificación. Una vez generada la solicitud hay que enviarla a la CA para que la firme digitalmente y genere el certificado X.509, para ello hay que ejecutar el siguiente comando:

```
openssl ca -keyfile private/cakey.pem -in servercsr.pem -out servercert.pem -days 400
```

Tras la ejecución del comando anterior se genera el certificado (servercert.pem).

Lo siguiente será importar el certificado de la CA (fichero cacert.pem) en el navegador para que éste conozca a la CA.

Por último hay que instalar el material criptográfico generado en el servidor web Apache, para ello en primer lugar hay que ejecutar el comando:

```
sudo a2enmod ssl
```



Ademas hay que añadir al fichero “/etc/apache2/sites-enabled/sstt5793.conf” las rutas a los ficheros “servercert.pem”, “serverkey.pem” y “cacert.pem” en la entrada correspondiente al puerto 443 quedando de la siguiente manera:

```
<VirtualHost *:443>
    ServerAdmin usuario1@sstt5793.org
    ServerName www.sstt5793.org
    DocumentRoot /var/www/sstt5793
    <Directory /var/www/sstt5793>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>
    SSLEngine on
    SSLCertificateFile /home/jorge/ssttCA/servercert.pem
    SSLCertificateKeyFile /home/jorge/ssttCA/serverkey.pem
    SSLCACertificateFile /home/jorge/ssttCA/cacert.pem
</VirtualHost>
```

Una vez generado el certificado del servicio web, lo siguiente que hay que hacer es generar un certificado para el cliente, para que pueda autenticarse frente a un servicio web. Para generar el certificado se ejecutan los siguientes comandos:

```
openssl req -new -nodes -newkey rsa:2048 -keyout clientkey.pem -out clientcsr.pem
```

Al ejecutar el comando, se solicitará introducir una serie de valores que deberán de coincidir con los valores ya introducidos para la CA, excepto para el campo “Common Name”, que en este caso se le asigna el valor “jorge48745793F”

Tras la ejecución de este comando se genera los archivos con la clave privada del cliente (clientkey.pem) y la solicitud de certificación (clientcsr.pem).

```
openssl ca -keyfile private/cakey.pem -in clientcsr.pem -out clientcert.pem -days 400
```

Tras ejecutar este comando se genera el certificado para el cliente (clientcert.pem)

Una vez generado el certificado, y la clave privada se genera un archivo en formato “pfx” a partir de estos valores, mediante el siguiente comando:

```
openssl pkcs12 -export -in clientcert.pem -certfile cacert.pem -inkey clientkey.pem -out clientcert.pfx
```

Tras generar el archivo anterior, éste se mueve al cliente y se importa en el navegador.

Para añadir la autenticación de cliente SSL a nuestra configuración de Apache hay que añadir un par de líneas en el fichero “/etc/apache2/sites-enabled/sstt5793.conf”, en concreto a la entrada asociada al puerto 443 quedando de la siguiente manera:

```
<VirtualHost *:443>
    ServerAdmin usuario1@sstt5793.org
    ServerName www.sstt5793.org
    DocumentRoot /var/www/sstt5793
    <Directory /var/www/sstt5793>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride None
        Order allow,deny
        allow from all
    </Directory>
    SSLEngine on
    SSLCertificateFile /home/jorge/ssttCA/servercert.pem
    SSLCertificateKeyFile /home/jorge/ssttCA/serverkey.pem
    SSLCACertificateFile /home/jorge/ssttCA/cacert.pem
    SSLVerifyClient require
    SSLVerifyDepth 10
</VirtualHost>
```

## 2.2 Configuración de un servidor de correo SMTP/POP

En primer lugar hay que añadir al fichero “/etc/hosts” tanto del cliente como del servidor las entradas “smtp.sstt5793.org” y “pop.sstt5793.org”

Quedando de la siguiente manera:

```
jorge@ubuntuServer:/etc/apache2$ cat /etc/hosts
127.0.0.1        localhost
127.0.1.1        ubuntuServer
192.168.236.4    www.sstt5793.org
192.168.236.4    web.sstt5793.org
192.168.236.4    smtp.sstt5793.org
192.168.236.4    pop.sstt5793.org
```

Las entradas creadas anteriormente se eliminarán cuando se configure el servidor DNS, ya que éste sera el encargado de la resolución de nombres.

Para montar el servicio de SMTP, vamos a hacer uso de “exim4”, para su instalación se ejecuta el siguiente comando:

- sudo apt-get install exim4

Una vez,este instalado hay que configurarlo con el siguiente comando:

-sudo dpkg-reconfigure exim4-config

Las **configuraciones** que hay que realizar son las siguientes:

**Tipo general de servidor:** Primera opción (Internet site)

**Nombre del sistema de correo:** sstt5793.org

**Direcciones IP en las que recibir conexiones SMTP:** (en blanco); Cualquier Ips

**Destinos de los que se acepta correo:** sstt5793.org

**Dominio para los que se puede reenviar correo:** (en blanco)

**Maquinas para las cuales reenviar correo:** (en blanco)

**Limitar consultas DNS:** NO

**Formato de buzón de correo:** Maildir

**Dividir ficheros de configuracion:** NO

Tras la configuración se reinicia exim4 con el siguiente comando:

- service exim4 restart

El siguiente paso, es la instalación del servidor POP, para ello, hay que ejecutar el siguiente comando:

- sudo apt-get install dovecot-pop3d

Tras la instalación hay que configurar los siguientes ficheros, con las siguientes opciones:

▶ */etc/dovecot/conf.d/10-auth.conf*

```
disable_plaintext_auth = no // (permitir autenticación débil basada en texto plano.  
                             POR DEFECTO a YES)  
auth_mechanisms = plain    // (activar autenticación débil basada en texto plano)
```

▶ */etc/dovecot/conf.d/10-mail.conf*

```
mail_location = maildir:~/Maildir // (especifica formato de los buzones de correo)
```

El siguiente paso es crear las cuentas de usuario en el sistema operativo, en este caso hay que crear los usuarios “nombre1\_5793” y “nombre2\_5793” en el servidor “servidor.sstt5793.org”, para ellos se ejecutan los siguientes comandos:

```
-sudo useradd nombre1_5793 -m  
-sudo passwd nombre1_5793
```

Los mismos comandos se han de usar para crear el usuario “nombre2\_5793”.

Tras esto habrá que reiniciar el servidor POP con el siguiente comando:

```
- service dovecot restart
```

Como ultimo paso, hay que configurar el cliente SMTP/POP, en este caso usaremos el cliente “Thunderbird” donde habrá que configurar las cuentas de correo de los usuarios creados anteriormente:

The screenshot shows the 'Configuración de la cuenta' (Account Configuration) window in Thunderbird. The left sidebar lists the account 'nombre1\_5793@sstt5793.org' and its settings, including 'Configuración del servidor', 'Copias y carpetas', 'Redacción y direcciones', 'Correo no deseado', 'Espacio en disco', 'Acuses de recibo', 'Seguridad', 'Carpetas locales', and 'Servidor de salida (SMTP)'. The main pane is titled 'Configuración de la cuenta - <nombre1\_5793@sstt5793.org>' and contains the following fields and options:

- Nombre de la cuenta:** nombre1\_5793@sstt5793.org
- Identidad predeterminada:** Cada cuenta tiene una identidad, que es la información que otras personas verán al leer sus mensajes.
- Su nombre:** nombre1\_5793
- Dirección de correo electrónico:** nombre1\_5793@sstt5793.org
- Dirección de respuesta:** Los destinatarios responderán a esta otra dirección
- Organización:** (empty field)
- Texto de la firma:** ☐ Usar HTML (p.e., <b>negrita</b>)
- ☐ Adjuntar la firma de un archivo (texto, HTML o imagen): (empty field)
- ☐ Adjuntar mi tarjeta en los mensajes
- Servidor de salida (SMTP):** nombre1\_5793 - smtp.sstt5793.org (Predeterminado)

At the bottom right, there are 'Cancelar' and 'Aceptar' buttons. At the bottom left, there is a button labeled 'Operaciones sobre la cuenta'.

En la configuración de la cuenta habrá que indicar el servidor SMTP y el servidor POP, que serán “smtp.sstt5793.org” y “pop.sstt5793.org” respectivamente. Además también hay que indicar el puerto (110 para POP y 25 para SMTP). Por último en el campo SSL (seguridad de la conexión) hay que poner “Ninguna” y en el método de identificación “contraseña normal”.

Configurar una dirección de correo existente

Su nombre:  Su nombre, tal y como se muestra a los demás

Dirección de correo:  Su dirección de correo existente

Contraseña:

☒ Recordar contraseña

Configuración encontrada intentando nombres habituales de servidor

	Nombre del servidor	Puerto	SSL	Identificación
Entrante: POP3	pop.sstt5793.org	110	Ninguno	Contraseña normal
Saliente: SMTP	smtp.sstt5793.org	25	Ninguno	Contraseña normal

Nombre de usuario: Entrante:  Saliente:

## 2.3 Configuración de DNS

Para la configuración de DNS, el primer paso es modificar el fichero “/etc/resolv.conf” tanto del cliente como del servidor, para añadir la entrada “nameserver 192.168.236.4”, donde la IP es la dirección del servidor DNS. Ambos ficheros quedarían de la siguiente manera:

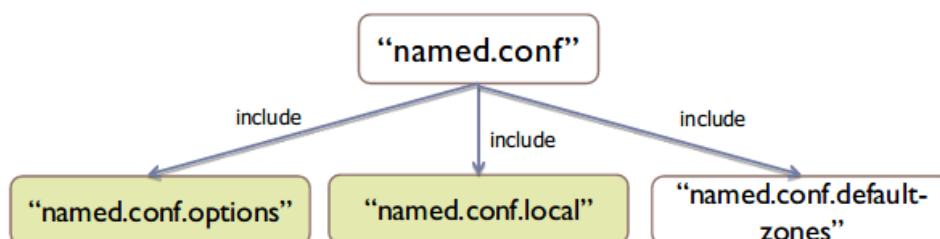
```
jorge@jorge-VirtualBox:~/Escritorio/SSTT$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.236.4
```

El siguiente paso, es eliminar las entradas creadas para el dominio “sstt5793.org” del fichero “/etc/hosts” tanto del cliente como del servidor. Ya que la resolución de nombres a partir de ahora sera realizada por nuestro servidor DNS.

Para montar el servicio DNS, hay que instalar “bind” mediante el siguiente comando:

- sudo apt-get install bind9

Tras la instalación se puede encontrar en el directorio “/etc/bind” los siguientes ficheros de configuración:



El primer fichero que hay que configurar es “named.conf.options” donde se indican las opciones de configuración globales del servidor.

Las opciones a configurar en este fichero son:

**directory:** Establece el directorio de trabajo, en el cual, se guarda la copia local de las resoluciones aprendidas. En este caso el directorio de trabajo es “/var/cache/bind”

**allow-query:** Indica los host que tienen permitido realizar consultas al servidor DNS. En este caso no se va a establecer ningún valor en esta opción ya que, por defecto, todos los hosts tienen permiso.

**Forwarders:** Indica direcciones IP de servidores DNS donde reenviar las peticiones, en caso de que este servidor no pueda resolverlas. En este caso hay que reenviar las peticiones al servidor DNS de la umu, por lo que en esta opción hay que poner la IP correspondiente a este servidor DNS.

Por lo tanto, el fichero “named.conf.options” quedaría de la siguiente manera:

```
jorge@ubuntuServer:/etc/bind$ cat named.conf.options
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        155.54.1.1;
    };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====
    dnssec-validation no;

    auth-nxdomain no;    # conform to RFC1035
    listen-on-v6 { any; };
};
```

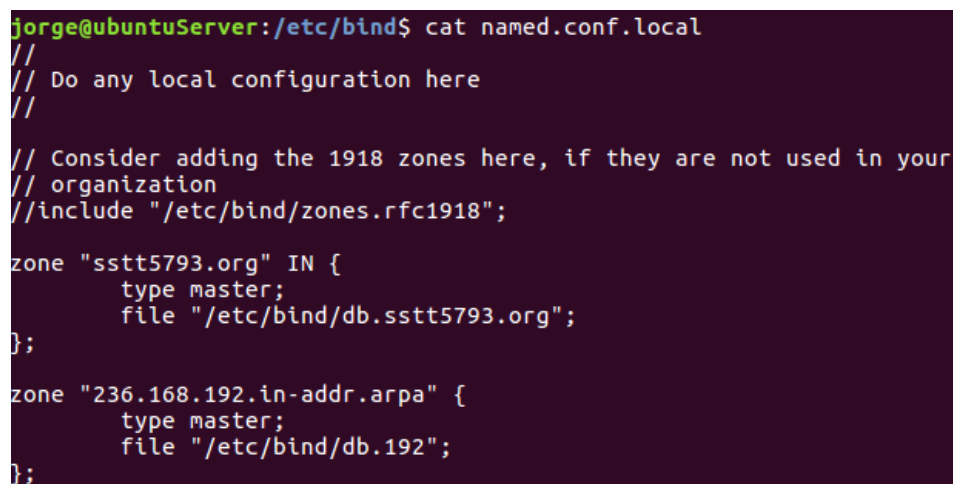
El siguiente fichero a configurar es “named.conf.local” donde se definen las zonas que gestionara el servidor DNS.

Las opciones a configurar en este fichero para cada una de las zonas creadas son las siguientes:

**Type:** Indica cual es el tipo de la zona. En este caso el tipo es “master”, que significa que el servidor tiene la autoridad para esta zona.

**File:** Nombre del archivo dentro del directorio de configuración, que contiene los datos de configuración de la zona.

Este fichero queda de la siguiente manera:

A terminal window with a dark purple background. The prompt is 'jorge@ubuntuServer:/etc/bind\$'. The command 'cat named.conf.local' has been executed, displaying the following configuration: //, // Do any local configuration here, //, // Consider adding the 1918 zones here, if they are not used in your organization, //include "/etc/bind/zones.rfc1918";, zone "sstt5793.org" IN {, type master;, file "/etc/bind/db.sstt5793.org";, }, zone "236.168.192.in-addr.arpa" {, type master;, file "/etc/bind/db.192";, };

```
jorge@ubuntuServer:/etc/bind$ cat named.conf.local
//
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "sstt5793.org" IN {
    type master;
    file "/etc/bind/db.sstt5793.org";
};

zone "236.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};
```

Como se puede observar se han creado dos zonas para el dominio “sstt5793.org”, la primera de ellas es para la resolución directa, la cual, es de tipo “Maestro” y el fichero con los datos de configuración de la zona es “/etc/bind/db.sstt5793.org”. La segunda zona es para la resolución inversa, la cual también es de tipo “Maestro” y el fichero con los datos de la zona es “/etc/bind/db.192”.

Por último hay que configurar los ficheros de cada zona. En primer lugar se configura el fichero “/etc/bind/db.sstt5793.org”, que queda de la siguiente manera:

```

$TTL 3600
@ IN SOA sstt5793.org. root.sstt5793.org. (
        1          ; Serial
        3600       ; Refresh
        1800       ; Retry
        604800    ; Expire
        3600      ) ; Negative Cache TTL
;
@ IN NS sstt5793.org.
@ IN A 192.168.236.4
www IN A 192.168.236.4
smtp IN A 192.168.236.4
pop  IN A 192.168.236.4
web  IN A 192.168.236.4
@ IN MX 10 smtp.sstt5793.org.

```

Como se puede observar en la imagen anterior se indica en primer lugar el valor del TTL (Time To Live) que indica el tiempo de vida de los registros de recursos (RR) definidos en la zona.

A continuación se define el registro “SOA” que indica el inicio de los datos para una zona y define parámetros que afectan a todos los registros de la zona.

Además se definen varios tipos de registros, en primer lugar se define un registro de tipo NS en el cual se establece el nombre de host del servidor DNS autoritativo que obtiene las direcciones IP de los hosts del dominio. En este caso el nombre del DNS autoritativo es “sstt5793.org”. Los siguientes registros definidos son los registros de tipo A, que asignan a cada host del dominio una dirección IP. En este caso se asignan direcciones IPs para los hosts ([www.sstt5793.org](http://www.sstt5793.org), [web.sstt5793.org](http://web.sstt5793.org), [smtp.sstt5793.org](http://smtp.sstt5793.org), [pop.sstt5793.org](http://pop.sstt5793.org), [servidor.sstt5793.org](http://servidor.sstt5793.org) y para [cliente.sstt5793.org](http://cliente.sstt5793.org)).

Por último se ha definido un registro de tipo “MX”, el cual, se utiliza para preguntar por la IP asociada a un servidor de correo.

Cuando un mensaje de correo electrónico es enviado a una dirección de correo, el agente de usuario, en este caso el Thunderbird, envía el mensaje al servidor de correo del cliente, y éste pregunta por el registro MX asociado al dominio de la dirección de destino al DNS local, el cual, mediante varias solicitudes DNS obtiene la dirección IP asociada al DNS local del destinatario. Una vez obtenida esta dirección IP el DNS local del emisor le pregunta al DNS local del destinatario por el registro MX asociado a su dominio, entonces el DNS local del destinatario le devuelve la IP asociada a su servidor de correo.



De esta forma el servidor SMTP del emisor puede conocer la IP del servidor SMTP del destinatario, al cual debe de enviar el mensaje.

Para esta práctica no es necesario definir un registro MX, ya que los mensajes no se mandan a direcciones de correo cuyo dominio sea distinto de “sstt5793.org”. Por tanto, en el caso de no definir un registro MX para nuestro dominio el DNS local puede obtener directamente la IP del servidor de correo en este caso “smtp.sstt5793.org”.

## 2.4 Configuración de IpSec

En primer lugar, hay que instalar la herramienta “Strongswan” tanto en el cliente como en el servidor, para ello se ejecuta el siguiente comando:

```
sudo apt-get install strongswan
```

El siguiente paso será configurar las características de la asociación de seguridad de Ipsec para ello hay que configurar el fichero “/etc/ipsec.conf”.

En el cliente el fichero “/etc/ipsec.conf” queda de la siguiente manera:

```
conn %default
    ikelifetime=60m
    keylife=20m
    rekeymargin=3m
    keyingtries=1
    mobike=no
    keyexchange=ikev2
    authby=pubkey

conn host-host
    left=192.168.236.3
    leftcert=/etc/ipsec.d/certs/clientcert.pem
    leftid="C=ES, ST=Murcia, O=UMU, OU=SSTT, CN=jorge48745793F"
    right=192.168.236.4
    rightid="C=ES, ST=Murcia, O=UMU, OU=SSTT, CN=www.sstt5793.org"
    type=tunnel
    auto=start
    esp=null-sha1_160
```

Como se puede observar en la imagen anterior se han establecido unas opciones de configuración para cualquier conexión (entrada conn %default) donde se indica por ejemplo, el tiempo de vida de una IKE SA (campo ikelifetime), el tiempo de vida de una asociación de seguridad ipsec (campo keylife), o como cliente y servidor se

autentican en la asociación de seguridad establecida (campo authby). En este caso al campo “authby” se le ha asignado el valor “pubkey”, que significa que la autenticación se realiza mediante la clave pública.

También se han establecido opciones de configuración para la conexión específica entre cliente y servidor (entrada conn host-host). En los campos “left” y “right” se indican las IPs asociadas a cliente y servidor respectivamente. En el campo “leftcert” se indica la ruta al certificado X.509 del cliente. En los campos “leftid” y “rightid” se indican los identificadores del certificado de cliente y servidor respectivamente. En el campo “type” se indica que se va a utilizar el modo túnel. Por último en el campo “esp” indicamos los algoritmos utilizados para cifrado y autenticación. En este caso no se asigna ningún algoritmo para el cifrado (valor null) y para la autenticación se usa el algoritmo “sha1\_160”.

En el servidor el fichero “/etc/ipsec.conf” quedaría de la siguiente manera:

```
conn %default
    ikelifetime=60m
    keylife=20m
    rekeymargin=3m
    keyingtries=1
    mobike=no
    keyexchange=ikev2
    authby=pubkey

conn host-host
    left=192.168.236.4
    leftcert=/etc/ipsec.d/certs/servercert.pem
    leftid="C=ES, ST=Murcia, O=UMU, OU=SSTT, CN=www.sstt5793.org"
    right=192.168.236.3
    rightid="C=ES, ST=Murcia, O=UMU, OU=SSTT, CN=jorge48745793F"
    type=tunnel
    auto=start
    esp=null-sha1_160
```

En este caso la configuración realizada para el campo “conn %default” es la misma que se realizó para el cliente.

Para la conexión específica entre cliente y servidor (entrada conn host-host), en este caso el campo “left” corresponde a la IP asociada al servidor y el campo “right” corresponde a la IP asociada al cliente. En el campo “leftcert” se indica la ruta al certificado X.509 del servidor y en los campos “leftid” y “rightid” se indican los identificadores de certificado de servidor y cliente respectivamente. El resto de campos se han definido igual que en el caso anterior.

El siguiente paso es configurar el fichero “/etc/ipsec.secrets” tanto en el cliente como en el servidor.

Este fichero quedaría de la siguiente forma en el cliente:

```
jorge@jorge-VirtualBox:~/Escritorio/SSTT$ sudo cat /etc/ipsec.secrets
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

192.168.236.3 192.168.236.4 : RSA /etc/ipsec.d/private/clientkey.pem
```

Como se puede observar en la imagen anterior se indican las Ips de cliente y servidor y la ruta a la clave privada RSA del cliente “clientkey.pem”.

El mismo fichero en el lado del servidor se define de la siguiente manera:

```
jorge@ubuntuServer:~$ sudo cat /etc/ipsec.secrets
[sudo] password for jorge:
# This file holds shared secrets or RSA private keys for authentication.

# RSA private key for this host, authenticating it to any other host
# which knows the public part.

192.168.236.3 192.168.236.4 : RSA /etc/ipsec.d/private/serverkey.pem
```

En este caso la única diferencia con respecto a la imagen anterior es que se indica la ruta a la clave privada RSA del servidor en lugar de la del cliente.

### 3.Descripción de la implementación del servicio web

En primer lugar tras recibir la petición HTTP se procede a leer los datos recibidos en el socket (mediante la función read).

El siguiente paso es parsear (mediante la función strtok) la petición HTTP y analizar cada una de las líneas que contiene .Se ha de tener en cuenta, el directorio que aparece en la línea de solicitud para saber cual es el recurso solicitado,el valor de la cabecera “Connection” para comprobar si la conexión a de ser persistente o no y el

valor de la cabecera “Cookie” para comprobar el número de accesos realizados al servidor.

Para comprobar que una petición HTTP es válida se comprueba que la línea de solicitud contenga el comando “GET” o “POST” , que la ruta introducida es válida (se comprueba mediante el uso de una expresión regular) ,que la versión de HTTP sea la 1.1 (HTTP/1.1) y que haya un espacio entre cada uno de estos tres componentes. Además se analizan cada una de las líneas de cabecera,y para cada línea se comprueba que la cabecera y el valor que contiene estén separados por un espacio en blanco. En el caso de que al menos una de las condiciones explicadas anteriormente sea falsa se devolverá como respuesta un “400 Bad Request” con un fichero HTML indicando que la petición no es válida.

Si la petición es válida se procede a buscar el recurso solicitado en el servidor.

En caso de que el directorio sea “/” se devuelve un mensaje de respuesta “200 OK” con el fichero “index.html”.

En el caso de que se quiera acceder a un directorio del servidor en el cual no se tengan permisos (para ello se comprueba si la ruta tiene la subcadena “..”) se devolverá un mensaje de respuesta “403 Forbidden” con un fichero HTML indicando que no se puede acceder al directorio solicitado.

En el caso de que no se encuentre el recurso solicitado se devolverá un mensaje de respuesta “404 Not Found” con un fichero HTML indicando que no se encuentra el recurso.

Por ultimo, en otro caso se comprobará en primer lugar que la extensión del recurso solicitado esta soportada y en ese caso se devolverá un mensaje de respuesta “200 OK” con el recurso solicitado. En el caso de que la extensión no este soportada se devolverá un mensaje de respuesta “404 Not Found”.

Los mensajes de respuesta HTTP “200 OK” se envían con las siguientes **cabeceras**:

**Date:** Fecha y hora actual.

**Server:** Nombre y versión del software del servidor.

**Content-length:** Longitud en bytes del cuerpo de la respuesta.

**Connection:** Indica el tipo de conexión.

**Content-Type:** Tipo MIME que identifica el tipo de dato de la respuesta.

**Set-Cookie:** Se establece el nuevo valor de la cookie. En este caso esta cabecera tiene tres atributos:

- counter: Indica el número de accesos al servidor
- Max-Age: Indica el tiempo de vida de la cookie en segundos.
- Path: Indica una url que debe existir en la url solicitada para mandar la cabecera de la cookie.

El envío del fichero solicitado se realiza en bloques de máximo 8 kb.

Los mensajes de respuesta “404 Not Found”, “403 Forbidden” y “400 Bad Request” tendrán las mismas cabeceras indicadas anteriormente menos la cabecera “Set-Cookie”.

En cuanto a la persistencia, como se ha mencionado anteriormente se comprueba la cabecera “connection ”de la petición HTTP. Si esta cabecera tiene el valor “keep-alive” la conexión será persistente, en caso de que tenga el valor “close” no será persistente.

La persistencia se ha implementado mediante el uso de la función “select” ,que comprueba si ha habido cambios en algún descriptor de fichero y añade a un conjunto FD\_SET los descriptors modificados. En este caso la función “select” solo comprueba un descriptor, el que se pasa como parámetro a la función “process\_web\_request”, ya que select se invoca dentro de esta función. Si este descriptor es modificado (la función “select” devuelve un valor mayor a cero) se procesará la petición, en caso contrario (la función “select” devuelve 0) debido a que se ha producido un timeout se cerrará la conexión.

En cuanto a las cookies, su valor se obtiene en la linea de cabecera “Cookie:” de la petición HTTP , mas concretamente en el atributo “counter” explicado anteriormente. Una cookie se crea tras realizar la primera petición al servidor, y también se crea en el caso de que la cookie anterior haya expirado. Cuando se crea se le asigna el valor 1 y se establece el tiempo de vida mediante el atributo “Max-Age”. Si el valor de la

cookie llega a 10 se devolverá un mensaje de respuesta “403 Forbidden” indicando que no se puede acceder al recurso.

## 4. Trazas

### 4.1 Trazas servicio web implementado

En esta sección vamos a comprobar como se comporta el servidor ante cada uno de los casos mencionados anteriormente, para ello se analizarán las trazas generadas por wireshark para cada uno de estos casos.

En primer lugar vamos a realizar una petición HTTP al servidor solicitando el recurso “index.html”:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.236.3	192.168.236.4	SSH	102	Client: Encrypted packet (len=36)
2	0.001387348	192.168.236.4	192.168.236.3	SSH	182	Server: Encrypted packet (len=116)
3	0.001411283	192.168.236.3	192.168.236.4	TCP	66	37498 → 22 [ACK] Seq=37 Ack=117 Win=1444 Len=0 TSval=1727174776
4	3.100473623	192.168.236.3	192.168.236.4	TCP	74	42334 → 8080 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1
5	3.100725851	192.168.236.4	192.168.236.3	TCP	74	8080 → 42334 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SA
6	3.100743661	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1727177876
7	3.100878066	192.168.236.3	192.168.236.4	HTTP	413	GET / HTTP/1.1
8	3.101400840	192.168.236.4	192.168.236.3	TCP	66	8080 → 42334 [ACK] Seq=1 Ack=348 Win=30080 Len=0 TSval=5122093
9	3.101412038	192.168.236.4	192.168.236.3	TCP	259	8080 → 42334 [PSH, ACK] Seq=1 Ack=348 Win=30080 Len=193 TSval=5
10	3.101416915	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=348 Ack=194 Win=30336 Len=0 TSval=172717
11	3.101513821	192.168.236.4	192.168.236.3	SSH	758	Server: Encrypted packet (len=692)
12	3.101523045	192.168.236.3	192.168.236.4	TCP	66	37498 → 22 [ACK] Seq=37 Ack=809 Win=1444 Len=0 TSval=1727177877
13	3.101532091	192.168.236.4	192.168.236.3	HTTP	581	HTTP/1.1 200 OK (text/html)
14	3.101537604	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=348 Ack=709 Win=31360 Len=0 TSval=172717
15	3.233605727	192.168.236.3	192.168.236.4	HTTP	413	GET /index_files/logo-um.jpg HTTP/1.1
16	3.234084954	192.168.236.4	192.168.236.3	TCP	260	8080 → 42334 [PSH, ACK] Seq=709 Ack=695 Win=31104 Len=194 TSval
17	3.234101842	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=695 Ack=903 Win=32512 Len=0 TSval=172717
18	3.234137046	192.168.236.4	192.168.236.3	TCP	8754	8080 → 42334 [ACK] Seq=903 Ack=695 Win=31104 Len=8688 TSval=512
19	3.234146160	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=695 Ack=9591 Win=49792 Len=0 TSval=17271
20	3.234234379	192.168.236.4	192.168.236.3	SSH	798	Server: Encrypted packet (len=732)
21	3.234241193	192.168.236.3	192.168.236.4	TCP	66	37498 → 22 [ACK] Seq=37 Ack=1541 Win=1444 Len=0 TSval=172717806
22	3.234251782	192.168.236.4	192.168.236.3	HTTP	936	HTTP/1.1 200 OK (JPEG JFIF image)
23	3.234256143	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=695 Ack=10461 Win=52736 Len=0 TSval=1727
24	13.235767295	192.168.236.3	192.168.236.4	TCP	66	[TCP Keep-Alive] 42334 → 8080 [ACK] Seq=694 Ack=10461 Win=52736
25	13.236300337	192.168.236.4	192.168.236.3	TCP	66	[TCP Keep-Alive ACK] 8080 → 42334 [ACK] Seq=10461 Ack=695 Win=3
26	13.244985055	192.168.236.4	192.168.236.3	TCP	66	8080 → 42334 [FIN, ACK] Seq=10461 Ack=695 Win=31104 Len=0 TSval
27	13.245010981	192.168.236.4	192.168.236.3	SSH	174	Server: Encrypted packet (len=108)
28	13.245021649	192.168.236.3	192.168.236.4	TCP	66	37498 → 22 [ACK] Seq=37 Ack=1649 Win=1444 Len=0 TSval=172718802

El significado de cada mensaje es el siguiente:

4-6: Establecimiento de la conexión TCP por parte del cliente.

7: Mensaje de solicitud HTTP del cliente al servidor.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.236.3	192.168.236.4	SSH	102	Client: Encrypted packet
2	0.001387348	192.168.236.4	192.168.236.3	SSH	182	Server: Encrypted packet
3	0.001411283	192.168.236.3	192.168.236.4	TCP	66	37498 → 22 [ACK] Seq=
4	3.100473623	192.168.236.3	192.168.236.4	TCP	74	42334 → 8080 [SYN] Seq=
5	3.100725851	192.168.236.4	192.168.236.3	TCP	74	8080 → 42334 [SYN, A
6	3.100743661	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] S
7	3.100878066	192.168.236.3	192.168.236.4	HTTP	413	GET / HTTP/1.1
8	3.101400840	192.168.236.4	192.168.236.3	TCP	66	8080 → 42334 [ACK] S
9	3.101412038	192.168.236.4	192.168.236.3	TCP	259	8080 → 42334 [PSH, A
10	3.101416915	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] S
11	3.101513821	192.168.236.4	192.168.236.3	SSH	758	Server: Encrypted packet
12	3.101523045	192.168.236.3	192.168.236.4	TCP	66	37498 → 22 [ACK] Seq=
13	3.101532091	192.168.236.4	192.168.236.3	HTTP	581	HTTP/1.1 200 OK (text/html)
14	3.101537604	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] S
▶ Frame 7: 413 bytes on wire (3304 bits), 413 bytes captured (3304 bits) on interface 0 ▶ Ethernet II, Src: PcsCompu_08:3c:9a (08:00:27:08:3c:9a), Dst: PcsCompu_34:de:c0 (08:00:27:34:de:c0) ▶ Internet Protocol Version 4, Src: 192.168.236.3, Dst: 192.168.236.4 ▶ Transmission Control Protocol, Src Port: 42334, Dst Port: 8080, Seq: 1, Ack: 1, Len: 347 ▼ Hypertext Transfer Protocol ▶ GET / HTTP/1.1\r\n Host: 192.168.236.4:8080\r\n User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:66.0) Gecko/20100101 Firefox/66.0\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3\r\n Accept-Encoding: gzip, deflate\r\n Connection: keep-alive\r\n Upgrade-Insecure-Requests: 1\r\n\r\n						

Los aspectos más importantes a destacar del mensaje de solicitud son los siguientes:

-En primer lugar en la línea de solicitud se usa el comando GET, el directorio solicitado es la carpeta raíz del servidor y se usa la versión de HTTP 1.1

-En la cabecera “Host” se ubican la dirección IP y puerto del servidor.

-La cabecera “Connection” tiene el valor Keep-Alive, es decir que la conexión será persistente (mientras no expire el timeout establecido).

No.	Time	Source	Destination	Protocol	Length	Info
7	3.100878066	192.168.236.3	192.168.236.4	HTTP	413	GET / HTTP/1.1
8	3.101400840	192.168.236.4	192.168.236.3	TCP	66	8080 → 42334 [ACK] Seq=1 Ack=3
9	3.101412038	192.168.236.4	192.168.236.3	TCP	259	8080 → 42334 [PSH, ACK] Seq=1
10	3.101416915	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=348 Ack=
11	3.101513821	192.168.236.4	192.168.236.3	SSH	758	Server: Encrypted packet (len=
12	3.101523045	192.168.236.3	192.168.236.4	TCP	66	37498 → 22 [ACK] Seq=37 Ack=80
13	3.101532091	192.168.236.4	192.168.236.3	HTTP	581	HTTP/1.1 200 OK (text/html)
14	3.101537604	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=348 Ack=
15	3.233605727	192.168.236.3	192.168.236.4	HTTP	413	GET /index_files/logo-um.jpg H
16	3.234084954	192.168.236.4	192.168.236.3	TCP	260	8080 → 42334 [PSH, ACK] Seq=70
17	3.234101842	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=695 Ack=
18	3.234137046	192.168.236.4	192.168.236.3	TCP	8754	8080 → 42334 [ACK] Seq=903 Ack=
19	3.234146160	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=695 Ack=
20	3.234224270	192.168.236.4	192.168.236.3	SSH	708	Server: Encrypted packet (len=
▶ Frame 13: 581 bytes on wire (4648 bits), 581 bytes captured (4648 bits) on interface 0 ▶ Ethernet II, Src: PcsCompu_34:de:c0 (08:00:27:34:de:c0), Dst: PcsCompu_08:3c:9a (08:00:27:08:3c:9a) ▶ Internet Protocol Version 4, Src: 192.168.236.4, Dst: 192.168.236.3 ▶ Transmission Control Protocol, Src Port: 8080, Dst Port: 42334, Seq: 194, Ack: 348, Len: 515 ▶ [2 Reassembled TCP Segments (708 bytes): #9(193), #13(515)] ▼ Hypertext Transfer Protocol ▶ HTTP/1.1 200 OK\r\n Date: Sun Mar 24 16:49:02 2019\r\n Server: UbuntuServer/16.04\r\n ▶ Content-Length: 515\r\n Connection: keep-alive\r\n Content-Type: text/html\r\n Set-Cookie: counter=1; Max-Age=120; Path=/\r\n\r\n						



El mensaje numero 13 es el mensaje de respuesta del servidor al cliente. En este caso es una respuesta 200 OK (la petición es válida y el recurso está disponible).

Como se puede observar se crea una cookie mediante la cabecera “Set-Cookie”, cuyo valor es 1 (counter=1) y su tiempo de vida máximo es de 2 minutos (Max-Age=120).

El siguiente mensaje (número 15) es otra petición del cliente al servidor, en este caso solicita la imagen contenida en el “index.html” solicitado en la anterior petición.

No.	Time	Source	Destination	Protocol	Length	Info
7	3.100878066	192.168.236.3	192.168.236.4	HTTP	413	GET / HTTP/1.1
8	3.101400840	192.168.236.4	192.168.236.3	TCP	66	8080 → 42334 [ACK] Seq=1 Ack=348 Win=30
9	3.101412038	192.168.236.4	192.168.236.3	TCP	259	8080 → 42334 [PSH, ACK] Seq=1 Ack=348 W:
10	3.101416915	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=348 Ack=194 Win=
11	3.101513821	192.168.236.4	192.168.236.3	SSH	758	Server: Encrypted packet (len=692)
12	3.101523045	192.168.236.3	192.168.236.4	TCP	66	37498 → 22 [ACK] Seq=37 Ack=809 Win=144
13	3.101532091	192.168.236.4	192.168.236.3	HTTP	581	HTTP/1.1 200 OK (text/html)
14	3.101537604	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=348 Ack=709 Win=
15	3.233605727	192.168.236.3	192.168.236.4	HTTP	413	GET /index_files/logo-um.jpg HTTP/1.1
16	3.234084954	192.168.236.4	192.168.236.3	TCP	260	8080 → 42334 [PSH, ACK] Seq=709 Ack=695
17	3.234101842	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=695 Ack=903 Win=
18	3.234137046	192.168.236.4	192.168.236.3	TCP	8754	8080 → 42334 [ACK] Seq=903 Ack=695 Win=
19	3.234146160	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=695 Ack=9591 Win=
20	3.234224270	192.168.236.4	192.168.236.3	SSH	708	Server: Encrypted packet (len=732)
▶ Frame 15: 413 bytes on wire (3304 bits), 413 bytes captured (3304 bits) on interface 0 ▶ Ethernet II, Src: PcsCompu_08:3c:9a (08:00:27:08:3c:9a), Dst: PcsCompu_34:de:c0 (08:00:27:34:de:c0) ▶ Internet Protocol Version 4, Src: 192.168.236.3, Dst: 192.168.236.4 ▶ Transmission Control Protocol, Src Port: 42334, Dst Port: 8080, Seq: 348, Ack: 709, Len: 347 ▼ Hypertext Transfer Protocol ▶ GET /index_files/logo-um.jpg HTTP/1.1\r\n Host: 192.168.236.4:8080\r\n User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:66.0) Gecko/20100101 Firefox/66.0\r\n Accept: image/webp,*/*\r\n Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3\r\n Accept-Encoding: gzip, deflate\r\n Referer: http://192.168.236.4:8080/\r\n Connection: keep-alive\r\n ▶ Cookie: counter=1\r\n \r\n						

Como se puede observar, en este caso, en la línea de solicitud el recurso solicitado es la imagen “logo-um.jpg”. Además el mensaje contiene otras cabeceras como “Referer” que contiene la url del documento desde el que se accedió al actual y la cabecera “Cookie” que contiene el valor de la cookie devuelta en el mensaje de respuesta anterior.

No.	Time	Source	Destination	Protocol	Length	Info
16	3.234084954	192.168.236.4	192.168.236.3	TCP	260	8080 → 42334 [PSH, ACK] Seq=709 Ack=695 Win=31104 Len=194
17	3.234101842	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=695 Ack=903 Win=32512 Len=0 TSval=
18	3.234137046	192.168.236.4	192.168.236.3	TCP	8754	8080 → 42334 [ACK] Seq=903 Ack=695 Win=31104 Len=8688 TSv
19	3.234146160	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=695 Ack=9591 Win=49792 Len=0 TSval
20	3.234234379	192.168.236.4	192.168.236.3	SSH	798	Server: Encrypted packet (len=732)
21	3.234241193	192.168.236.3	192.168.236.4	TCP	66	37498 → 22 [ACK] Seq=37 Ack=1541 Win=1444 Len=0 TSval=172
22	3.234251782	192.168.236.4	192.168.236.3	HTTP	936	HTTP/1.1 200 OK (JPEG JFIF image)
23	3.234256143	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=695 Ack=10461 Win=52736 Len=0 TSval
24	13.235767295	192.168.236.3	192.168.236.4	TCP	66	[TCP Keep-Alive] 42334 → 8080 [ACK] Seq=694 Ack=10461 Win=
25	13.236300337	192.168.236.4	192.168.236.3	TCP	66	[TCP Keep-Alive ACK] 8080 → 42334 [ACK] Seq=10461 Ack=695
26	13.244985055	192.168.236.4	192.168.236.3	TCP	66	8080 → 42334 [FIN, ACK] Seq=10461 Ack=695 Win=31104 Len=0
27	13.245010981	192.168.236.4	192.168.236.3	SSH	174	Server: Encrypted packet (len=108)
28	13.245021649	192.168.236.3	192.168.236.4	TCP	66	37498 → 22 [ACK] Seq=37 Ack=1649 Win=1444 Len=0 TSval=172
29	13.245274702	192.168.236.4	192.168.236.3	TCP	66	42334 → 8080 [FIN, ACK] Seq=695 Ack=10461 Win=52736 Len=0
▶ Frame 22: 936 bytes on wire (7488 bits), 936 bytes captured (7488 bits) on interface 0 ▶ Ethernet II, Src: PcsCompu_34:de:c0 (08:00:27:34:de:c0), Dst: PcsCompu_08:3c:9a (08:00:27:08:3c:9a) ▶ Internet Protocol Version 4, Src: 192.168.236.4, Dst: 192.168.236.3 ▶ Transmission Control Protocol, Src Port: 8080, Dst Port: 42334, Seq: 9591, Ack: 695, Len: 870 ▶ 3 Reassembled TCP Segments (9752 bytes): #16(194), #18(8688), #22(870)] ▼ Hypertext Transfer Protocol ▶ HTTP/1.1 200 OK\r\n Date: Sun Mar 24 16:49:02 2019\r\n Server: UbuntuServer/16.04\r\n Content-Length: 9558\r\n Connection: keep-alive\r\n Content-Type: image/jpg\r\n Set-Cookie: counter=2; Max-Age=120; Path=/\r\n \r\n						



La respuesta enviada por el servidor a la petición anterior es el mensaje número 22. En este caso la respuesta no identifica ningún error (respuesta 200 OK) y como se puede observar en este caso se establece una cookie con valor 2 (counter=2) ya que se han realizado 2 peticiones al servidor.

En los mensajes 24,25 se comprueba si la conexión entre cliente y servidor sigue activa.

No.	Time	Source	Destination	Protocol	Length	Info
21	3.234241193	192.168.236.3	192.168.236.4	TCP	66	37498 → 22 [ACK] Seq=37 Ack=1541 Win=1444 Len=0 TSval=1727178009 TS
22	3.234251782	192.168.236.4	192.168.236.3	HTTP	936	HTTP/1.1 200 OK (JPEG JFIF image)
23	3.234256143	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [ACK] Seq=695 Ack=10461 Win=52736 Len=0 TSval=17271780
24	13.235767295	192.168.236.3	192.168.236.4	TCP	66	[TCP Keep-Alive] 42334 → 8080 [ACK] Seq=694 Ack=10461 Win=52736 Len
25	13.236300337	192.168.236.4	192.168.236.3	TCP	66	[TCP Keep-Alive ACK] 8080 → 42334 [ACK] Seq=10461 Ack=695 Win=31104
26	13.244985055	192.168.236.4	192.168.236.3	TCP	66	8080 → 42334 [FIN, ACK] Seq=10461 Ack=695 Win=31104 Len=0 TSval=512
27	13.245010981	192.168.236.4	192.168.236.3	SSH	174	Server: Encrypted packet (len=108)
28	13.245021649	192.168.236.3	192.168.236.4	TCP	66	37498 → 22 [ACK] Seq=37 Ack=1649 Win=1444 Len=0 TSval=1727188020 TS
29	13.245274793	192.168.236.3	192.168.236.4	TCP	66	42334 → 8080 [FIN, ACK] Seq=695 Ack=10462 Win=52736 Len=0 TSval=172
30	13.245551653	192.168.236.4	192.168.236.3	TCP	66	8080 → 42334 [ACK] Seq=10462 Ack=696 Win=31104 Len=0 TSval=5124629
31	23.181872163	192.168.236.1	255.255.255.255	DB-LSP...	244	Dropbox LAN sync Discovery Protocol

En caso de que el timeout expire se cierra la conexión entre cliente y servidor (mensajes 26-30).

## 4.2 Trazas servicio web de Apache

En esta sección, se van a mostrar cada uno de los mensajes intercambiados al acceder al servicio web <http://www.sstt5793.org>.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x8135 A www.sstt5793.org
2	0.000083983	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x6751 AAAA www.sstt5793.org
3	0.000376232	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0x8135 A www.sstt5793.org A 192.168.23
4	0.000387136	192.168.236.4	192.168.236.3	DNS	117	Standard query response 0x6751 AAAA www.sstt5793.org SOA sstt5
5	0.001357864	192.168.236.3	192.168.236.4	DNS	76	Standard query 0xe0e7 A www.sstt5793.org
6	0.001650537	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0xe0e7 A www.sstt5793.org A 192.168.23
7	0.001772341	192.168.236.3	192.168.236.4	TCP	74	50750 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TS
8	0.001946393	192.168.236.4	192.168.236.3	TCP	74	80 → 50750 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SAC
9	0.001960054	192.168.236.3	192.168.236.4	TCP	66	50750 → 80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2495132525
10	0.002038970	192.168.236.3	192.168.236.4	HTTP	528	GET / HTTP/1.1
11	0.002162728	192.168.236.4	192.168.236.3	TCP	66	80 → 50750 [ACK] Seq=1 Ack=463 Win=30080 Len=0 TSval=133360 TS
12	0.002451024	192.168.236.4	192.168.236.3	HTTP	745	HTTP/1.1 200 OK (text/html)
13	0.002457716	192.168.236.3	192.168.236.4	TCP	66	50750 → 80 [ACK] Seq=463 Ack=680 Win=30592 Len=0 TSval=2495132
14	0.009090184	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x1499 A www.sstt5793.org
15	0.009470946	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x0b53 AAAA www.sstt5793.org
16	0.009432191	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0x1499 A www.sstt5793.org A 192.168.23
17	0.009443337	192.168.236.4	192.168.236.3	DNS	117	Standard query response 0x0b53 AAAA www.sstt5793.org SOA sstt5
18	0.071888795	192.168.236.3	192.168.236.4	HTTP	503	GET /index_files/logo-um.jpg HTTP/1.1
19	0.072218397	192.168.236.4	192.168.236.3	HTTP	247	HTTP/1.1 304 Not Modified
20	0.072234327	192.168.236.3	192.168.236.4	TCP	66	50750 → 80 [ACK] Seq=900 Ack=861 Win=32000 Len=0 TSval=2495132
21	0.079873172	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x62fd A www.sstt5793.org
22	0.079954925	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x5dae AAAA www.sstt5793.org
23	0.080213115	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0x62fd A www.sstt5793.org A 192.168.23
24	0.080224285	192.168.236.4	192.168.236.3	DNS	117	Standard query response 0x5dae AAAA www.sstt5793.org SOA sstt5
25	1.624824872	192.168.236.1	255.255.255.255	DB-LSP...	244	Dropbox LAN sync Discovery Protocol
26	1.629498458	192.168.236.1	255.255.255.255	DB-LSP...	244	Dropbox LAN sync Discovery Protocol
27	1.629541648	192.168.236.1	255.255.255.255	DB-LSP...	244	Dropbox LAN sync Discovery Protocol
28	1.629812703	192.168.236.1	255.255.255.255	DB-LSP...	244	Dropbox LAN sync Discovery Protocol
29	1.630593256	192.168.236.1	255.255.255.255	DB-LSP...	244	Dropbox LAN sync Discovery Protocol
30	1.630621755	192.168.236.1	255.255.255.255	DB-LSP...	244	Dropbox LAN sync Discovery Protocol
31	5.013159003	192.168.236.4	192.168.236.3	TCP	66	80 → 50750 [FIN, ACK] Seq=861 Ack=900 Win=31104 Len=0 TSval=13
32	5.013431947	192.168.236.3	192.168.236.4	TCP	66	50750 → 80 [FIN, ACK] Seq=900 Ack=862 Win=32000 Len=0 TSval=24
33	5.013917711	192.168.236.4	192.168.236.3	TCP	66	80 → 50750 [ACK] Seq=862 Ack=901 Win=31104 Len=0 TSval=134614

El significado de los mensajes mostrados en la imagen anterior es el siguiente:

1) **Solicitud DNS.** Se realiza una consulta DNS para obtener la dirección IP asociada al nombre de host “www.sstt5793.org”. Como se puede observar en el campo de “flags” se indica que el mensaje es una consulta. El id de la consulta es 0x8135 (indicado en el campo Transaction ID). Además en el campo “Queries” se indica que se quiere consultar el registro de tipo A asociado a “[www.sstt5793.org](http://www.sstt5793.org)”.

2) **Solicitud DNS** sobre el mismo nombre de host que la consulta anterior, pero en este caso para obtener la dirección IPv6 asociada al nombre (registro AAAA).

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x8135 A www.sstt5793.org
2	0.000083983	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x6751 AAAA www.sstt5793.org
3	0.000376232	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0x8135 A www.sstt5793.org
4	0.000387136	192.168.236.4	192.168.236.3	DNS	117	Standard query response 0x6751 AAAA www.sstt5793.org

▶ Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0  
▶ Ethernet II, Src: PcsCompu\_08:3c:9a (08:00:27:08:3c:9a), Dst: PcsCompu\_34:de:c0 (08:00:27:34:de:c0)  
▶ Internet Protocol Version 4, Src: 192.168.236.3, Dst: 192.168.236.4  
▶ User Datagram Protocol, Src Port: 41690, Dst Port: 53  
▼ Domain Name System (query)  
Transaction ID: 0x8135  
▼ Flags: 0x0100 Standard query  
0... .. = Response: Message is a query  
.000 0... .. = Opcode: Standard query (0)  
... ..0. .... = Truncated: Message is not truncated  
... ..1. .... = Recursion desired: Do query recursively  
... ..0. .... = Z: reserved (0)  
... ..0. .... = Non-authenticated data: Unacceptable  
Questions: 1  
Answer RRs: 0  
Authority RRs: 0  
Additional RRs: 0  
▼ Queries  
▼ www.sstt5793.org: type A, class IN  
Name: www.sstt5793.org  
[Name Length: 16]  
[Label Count: 3]  
Type: A (Host Address) (1)  
Class: IN (0x0001)  
[Response In: 3]

3) **Respuesta DNS** asociada a la solicitud anterior. Como se puede observar en el campo “flags” se indica el identificador de la respuesta (0x8135) que es el mismo que el de la consulta realizada anteriormente y que el servidor DNS, es un servidor autoritativo para el host solicitado.

Además en el mensaje de respuesta también se proporcionan los registros de recursos (RR) asociados al nombre que se ha consultado. En el campo “answers” se indica el registro de tipo A asociado a este nombre, donde también se indica su dirección IP. En el campo “Authoritative nameservers” se indican los servidores DNS autoritativos del dominio al que pertenece el host.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000376232	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0x8135 A v
4	0.000387136	192.168.236.4	192.168.236.3	DNS	117	Standard query response 0x6751 AA
5	0.001357864	192.168.236.3	192.168.236.4	DNS	76	Standard query 0xe0e7 A www.sstt57
6	0.001650537	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0xe0e7 A v

▶ Frame 3: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0  
 ▶ Ethernet II, Src: PcsCompu\_34:de:c0 (08:00:27:34:de:c0), Dst: PcsCompu\_08:3c:9a (08:00:27:08:3c:9a)  
 ▶ Internet Protocol Version 4, Src: 192.168.236.4, Dst: 192.168.236.3  
 ▶ User Datagram Protocol, Src Port: 53, Dst Port: 41690  
 ▼ Domain Name System (response)  
   Transaction ID: 0x8135  
   ▼ Flags: 0x8580 Standard query response, No error  
     1... .. = Response: Message is a response  
     .000 0... .. = Opcode: Standard query (0)  
     ... 1... .. = Authoritative: Server is an authority for domain  
     ... .0... .. = Truncated: Message is not truncated  
     ... ..1... .. = Recursion desired: Do query recursively  
     ... ..1... .. = Recursion available: Server can do recursive queries  
     ... ..0... .. = Z: reserved (0)  
     ... ..0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server  
     ... ..0... .. = Non-authenticated data: Unacceptable  
     ... ..0000 = Reply code: No error (0)  
   Questions: 1  
   Answer RRs: 1  
   Authority RRs: 1  
   Additional RRs: 1  
   ▶ Queries  
   ▼ Answers  
     ▶ www.sstt5793.org: type A, class IN, addr 192.168.236.4  
   ▼ Authoritative nameservers  
     ▶ sstt5793.org: type NS, class IN, ns sstt5793.org  
   ▼ Additional records  
     ▶ sstt5793.org: type A, class IN, addr 192.168.236.4  
   [Request In: 1]  
   [Time: 0.000376232 seconds]

4) Mensaje de respuesta a la consulta DNS de la linea 2.

7-9) Establecimiento de la conexión TCP entre cliente y servidor.

10) Solicitud HTTP del cliente al servidor.

Los aspectos mas importantes a destacar del mensaje de solicitud son los siguientes:

-En primer lugar en la linea de solicitud se usa el comando GET, el directorio solicitado es la carpeta raíz del servidor y se usa la versión de HTTP 1.1

-En la cabecera “Host” se indica el nombre de host solicitado.

-La cabecera “Connection” tiene el valor Keep-Alive.

No.	Time	Source	Destination	Protocol	Length	Info
10	0.002038970	192.168.236.3	192.168.236.4	HTTP	528	GET / HTTP/1.1
11	0.002162728	192.168.236.4	192.168.236.3	TCP	66	80 → 50750 [ACK] Seq=
12	0.002451024	192.168.236.4	192.168.236.3	HTTP	745	HTTP/1.1 200 OK (text/html)
13	0.002457716	192.168.236.3	192.168.236.4	TCP	66	50750 → 80 [ACK] Seq=
14	0.069090184	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x1499 A www.sstt5793.org
15	0.069170946	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x0b53 AAAA www.sstt5793.org

▶ Frame 10: 528 bytes on wire (4224 bits), 528 bytes captured (4224 bits) on interface 0  
 ▶ Ethernet II, Src: PcsCompu\_08:3c:9a (08:00:27:08:3c:9a), Dst: PcsCompu\_34:de:c0 (08:00:27:34:de:c0)  
 ▶ Internet Protocol Version 4, Src: 192.168.236.3, Dst: 192.168.236.4  
 ▶ Transmission Control Protocol, Src Port: 50750, Dst Port: 80, Seq: 1, Ack: 1, Len: 462

▼ Hypertext Transfer Protocol  
 ▶ GET / HTTP/1.1\r\n  
 Host: www.sstt5793.org\r\n  
 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:66.0) Gecko/20100101 Firefox/66.0\r\n  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8\r\n  
 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3\r\n  
 Accept-Encoding: gzip, deflate\r\n  
 Connection: keep-alive\r\n  
 Upgrade-Insecure-Requests: 1\r\n  
 If-Modified-Since: Fri, 29 Mar 2019 12:01:39 GMT\r\n  
 If-None-Match: "203-5853a6ef43c6a-gzip"\r\n  
 Cache-Control: max-age=0\r\n  
 \r\n  
 [Full request URI: http://www.sstt5793.org/]  
 [HTTP request 1/2]  
 [Response in frame: 12]  
 [Next request in frame: 18]

12) El mensaje número 12 es el mensaje de respuesta del servidor al cliente. En este caso es una respuesta 200 OK (la petición es válida y el recurso esta disponible). En el campo “Server” se indica el nombre del servidor, al cual se le ha enviado la petición, que en este caso es el nombre del servidor Apache.

No.	Time	Source	Destination	Protocol	Length	Info
12	0.002451024	192.168.236.4	192.168.236.3	HTTP	745	HTTP/1.1 200 OK (text/html)
13	0.002457716	192.168.236.3	192.168.236.4	TCP	66	50750 → 80 [ACK] Seq=463 Ack=680 Win=30592 Len=0
14	0.069090184	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x1499 A www.sstt5793.org
15	0.069170946	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x0b53 AAAA www.sstt5793.org

▶ Frame 12: 745 bytes on wire (5960 bits), 745 bytes captured (5960 bits) on interface 0  
 ▶ Ethernet II, Src: PcsCompu\_34:de:c0 (08:00:27:34:de:c0), Dst: PcsCompu\_08:3c:9a (08:00:27:08:3c:9a)  
 ▶ Internet Protocol Version 4, Src: 192.168.236.4, Dst: 192.168.236.3  
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50750, Seq: 1, Ack: 463, Len: 679

▼ Hypertext Transfer Protocol  
 ▶ HTTP/1.1 200 OK\r\n  
 Date: Sat, 25 May 2019 21:57:36 GMT\r\n  
 Server: Apache/2.4.18 (Ubuntu)\r\n  
 Last-Modified: Fri, 29 Mar 2019 12:01:39 GMT\r\n  
 ETag: "203-5853a6ef43c6a-gzip"\r\n  
 Accept-Ranges: bytes\r\n  
 Vary: Accept-Encoding\r\n  
 Content-Encoding: gzip\r\n  
 ▶ Content-Length: 342\r\n  
 Keep-Alive: timeout=5, max=100\r\n  
 Connection: Keep-Alive\r\n  
 Content-Type: text/html\r\n  
 \r\n  
 [HTTP response 1/2]  
 [Time since request: 0.000412054 seconds]  
 [Request in frame: 10]  
 [Next request in frame: 18]  
 [Next response in frame: 19]  
 Content-encoded entity body (gzip): 342 bytes -> 515 bytes  
 File Data: 515 bytes

▶ Line-based text data: text/html (18 lines)

18) En esta línea se envía una solicitud HTTP. En la línea de solicitud se emplea el comando GET, seguido del recurso solicitado, en este caso “/index\_files/logo-um.jpg” y se indica la versión de HTTP (HTTP/1.1). En este caso se está solicitando una imagen como se indica en la cabecera “Accept”. Además el mensaje contiene la cabecera “Referer” que contiene la url del documento desde el que se accedió al actual.

No.	Time	Source	Destination	Protocol	Length	Info
18	0.071888795	192.168.236.3	192.168.236.4	HTTP	503	GET /index_files/logo-um.jpg HTTP/1.1
19	0.072218397	192.168.236.4	192.168.236.3	HTTP	247	HTTP/1.1 304 Not Modified
20	0.072234327	192.168.236.3	192.168.236.4	TCP	66	50750 → 80 [ACK] Seq=900 Ack=861 Win=3
21	0.079873172	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x62fd A www.sstt5793.c

▶ Frame 18: 503 bytes on wire (4024 bits), 503 bytes captured (4024 bits) on interface 0  
 ▶ Ethernet II, Src: PcsCompu\_08:3c:9a (08:00:27:08:3c:9a), Dst: PcsCompu\_34:de:c0 (08:00:27:34:de:c0)  
 ▶ Internet Protocol Version 4, Src: 192.168.236.3, Dst: 192.168.236.4  
 ▶ Transmission Control Protocol, Src Port: 50750, Dst Port: 80, Seq: 463, Ack: 680, Len: 437

▼ Hypertext Transfer Protocol

▶ GET /index\_files/logo-um.jpg HTTP/1.1\r\n  
 Host: www.sstt5793.org\r\n  
 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:66.0) Gecko/20100101 Firefox/66.0\r\n  
 Accept: image/webp,\*/\*\r\n  
 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3\r\n  
 Accept-Encoding: gzip, deflate\r\n  
 Referer: http://www.sstt5793.org/\r\n  
 Connection: keep-alive\r\n  
 If-Modified-Since: Fri, 29 Mar 2019 12:12:06 GMT\r\n  
 If-None-Match: "2556-5853a94567b29"\r\n  
 Cache-Control: max-age=0\r\n  
 \r\n  
 [Full request URI: http://www.sstt5793.org/index\_files/logo-um.jpg]  
 [HTTP request 2/2]  
 [Prev request in frame: 10]  
 [Response in frame: 19]

19) Respuesta HTTP a la solicitud anterior.

No.	Time	Source	Destination	Protocol	Length	Info
19	0.072218397	192.168.236.4	192.168.236.3	HTTP	247	HTTP/1.1 304 Not Modified
20	0.072234327	192.168.236.3	192.168.236.4	TCP	66	50750 → 80 [ACK] Seq=900 A
21	0.079873172	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x62fd A ww
22	0.079954925	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x5dae AAAA

▶ Frame 19: 247 bytes on wire (1976 bits), 247 bytes captured (1976 bits) on interface 0  
 ▶ Ethernet II, Src: PcsCompu\_34:de:c0 (08:00:27:34:de:c0), Dst: PcsCompu\_08:3c:9a (08:00:27:08:3c:9a)  
 ▶ Internet Protocol Version 4, Src: 192.168.236.4, Dst: 192.168.236.3  
 ▶ Transmission Control Protocol, Src Port: 80, Dst Port: 50750, Seq: 680, Ack: 900, Len: 181

▼ Hypertext Transfer Protocol

▶ HTTP/1.1 304 Not Modified\r\n  
 Date: Sat, 25 May 2019 21:57:36 GMT\r\n  
 Server: Apache/2.4.18 (Ubuntu)\r\n  
 Connection: Keep-Alive\r\n  
 Keep-Alive: timeout=5, max=99\r\n  
 ETag: "2556-5853a94567b29"\r\n  
 \r\n  
 [HTTP response 2/2]  
 [Time since request: 0.000329602 seconds]  
 [Prev request in frame: 10]  
 [Prev response in frame: 12]  
 [Request in frame: 18]

31-33) Cierre de conexión entre cliente y servidor.



## 4.3 Trazas servicio web seguro de Apache

En esta sección, se van a mostrar cada uno de los mensajes intercambiados al acceder al servicio web seguro <https://www.sstt5793.org>.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.236.3	192.168.236.4	DNS	76	Standard query 0xf8e7 A www.sstt5793.org
2	0.000167	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x9e24 AAAA www.sstt5793.org
3	0.000606	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0xf8e7 A www.sstt5793.org A 192.168.236.4 NS
4	0.000817	192.168.236.4	192.168.236.3	DNS	117	Standard query response 0x9e24 AAAA www.sstt5793.org SOA sstt5793.o
5	0.000958	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x9935 A www.sstt5793.org
6	0.009587	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0x9935 A www.sstt5793.org A 192.168.236.4 NS
7	0.010098	192.168.236.3	192.168.236.4	TCP	74	48506 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=
8	0.010478	192.168.236.4	192.168.236.3	TCP	74	443 → 48506 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK PE
9	0.010521	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3623314584 TSecr
10	0.013560	192.168.236.3	192.168.236.4	TLSv1.2	583	Client Hello
11	0.013932	192.168.236.4	192.168.236.3	TCP	66	443 → 48506 [ACK] Seq=1 Ack=518 Win=30080 Len=0 TSval=2695793 TSecr
12	0.017663	192.168.236.4	192.168.236.3	TLSv1.2	2477	Server Hello, Certificate, Server Key Exchange, Certificate Request
13	0.017699	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [ACK] Seq=518 Ack=2412 Win=34048 Len=0 TSval=3623314591
14	0.060237	192.168.236.3	192.168.236.4	TLSv1.2	1397	Certificate, Client Key Exchange, Certificate Verify, Change Cipher
15	0.060994	192.168.236.3	192.168.236.4	TLSv1.2	561	Application Data
16	0.061599	192.168.236.4	192.168.236.3	TCP	66	443 → 48506 [ACK] Seq=2412 Ack=2344 Win=35712 Len=0 TSval=2695806 TS
17	0.061789	192.168.236.4	192.168.236.3	TLSv1.2	1284	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
18	0.061804	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [ACK] Seq=2344 Ack=3630 Win=36992 Len=0 TSval=3623314636
19	0.062270	192.168.236.4	192.168.236.3	TLSv1.2	832	Application Data, Application Data, Application Data
20	0.062285	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [ACK] Seq=2344 Ack=4396 Win=39936 Len=0 TSval=3623314636
21	0.156643	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x8f16 A www.sstt5793.org
22	0.156748	192.168.236.3	192.168.236.4	DNS	76	Standard query 0xa726 AAAA www.sstt5793.org
23	0.157075	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0x8f16 A www.sstt5793.org A 192.168.236.4 NS
24	0.157093	192.168.236.4	192.168.236.3	DNS	117	Standard query response 0xa726 AAAA www.sstt5793.org SOA sstt5793.or
25	0.158744	192.168.236.3	192.168.236.4	TLSv1.2	537	Application Data
26	0.159168	192.168.236.4	192.168.236.3	TLSv1.2	276	Application Data
27	0.159204	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [ACK] Seq=2815 Ack=4606 Win=42752 Len=0 TSval=3623314733
28	0.166701	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x71e3 A www.sstt5793.org
29	0.166808	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x12b0 AAAA www.sstt5793.org
30	0.167048	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0x71e3 A www.sstt5793.org A 192.168.236.4 NS
31	0.167151	192.168.236.4	192.168.236.3	DNS	117	Standard query response 0x12b0 AAAA www.sstt5793.org SOA sstt5793.or
32	1.425176	192.168.236.1	255.255.255.255	DB-LSP-DI	244	Dropbox LAN sync Discovery Protocol
33	1.427978	192.168.236.1	255.255.255.255	DB-LSP-DI	244	Dropbox LAN sync Discovery Protocol
34	1.427992	192.168.236.1	255.255.255.255	DB-LSP-DI	244	Dropbox LAN sync Discovery Protocol
35	1.427996	192.168.236.1	255.255.255.255	DB-LSP-DI	244	Dropbox LAN sync Discovery Protocol
36	1.428391	192.168.236.1	255.255.255.255	DB-LSP-DI	244	Dropbox LAN sync Discovery Protocol
37	1.428866	192.168.236.1	255.255.255.255	DB-LSP-DI	244	Dropbox LAN sync Discovery Protocol
38	4.772199	192.168.236.4	192.168.236.3	TLSv1.2	97	Encrypted Alert
39	4.772256	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [ACK] Seq=2815 Ack=4637 Win=42752 Len=0 TSval=3623319346
40	4.772291	192.168.236.4	192.168.236.3	TCP	66	443 → 48506 [FIN, ACK] Seq=4637 Ack=2815 Win=38272 Len=0 TSval=26970
41	4.772853	192.168.236.3	192.168.236.4	TLSv1.2	97	Encrypted Alert
42	4.773046	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [FIN, ACK] Seq=2846 Ack=4638 Win=42752 Len=0 TSval=36233
43	4.773179	192.168.236.4	192.168.236.3	TCP	66	443 → 48506 [ACK] Seq=4638 Ack=2847 Win=38272 Len=0 TSval=2697065 TS

El significado de cada uno de los mensajes mostrados en la imagen anterior es el siguiente:

1) Solicitud DNS. Se realiza una consulta DNS para obtener la dirección IP asociada al nombre de host “www.sstt5793.org”. Como se puede observar en el campo de “flags” se indica que el mensaje es una consulta. El id de la consulta es 0xf8e7 (indicado en el campo Transaction ID). Además en el campo “Queries” se indica que se quiere consultar el registro de tipo A del nombre “[www.sstt5793.org](https://www.sstt5793.org)”

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.236.3	192.168.236.4	DNS	76	Standard query 0xf8e7 A www.sstt5793.org
2	0.000167	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x9e24 AAAA www.sstt5793.org
3	0.000606	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0xf8e7 A www.sstt5793.org

▶ Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)  
 ▶ Ethernet II, Src: PcsCompu\_08:3c:9a (08:00:27:08:3c:9a), Dst: PcsCompu\_34:de:c0 (08:00:27:34:de:c0)  
 ▶ Internet Protocol Version 4, Src: 192.168.236.3, Dst: 192.168.236.4  
 ▶ User Datagram Protocol, Src Port: 55067, Dst Port: 53  
 ▼ Domain Name System (query)  
   Transaction ID: 0xf8e7  
   Flags: 0x0100 Standard query  
     0... .. = Response: Message is a query  
     .000 0... .. = Opcode: Standard query (0)  
     ... ..0. = Truncated: Message is not truncated  
     ... ..1. = Recursion desired: Do query recursively  
     ... ..0. = Z: reserved (0)  
     ... ..0. = Non-authenticated data: Unacceptable  
   Questions: 1  
   Answer RRs: 0  
   Authority RRs: 0  
   Additional RRs: 0  
   Queries  
     ▶ www.sstt5793.org: type A, class IN  
     [Response In: 3]

2) Consulta DNS sobre el mismo nombre de host que la consulta anterior, pero en este caso para obtener la dirección IPv6 asociada al nombre (registro AAAA)

3) Respuesta DNS asociada a la solicitud anterior. Como se puede observar en el campo “flags” se indica el identificador de la respuesta (0xf8e7) que es el mismo que el de la consulta realizada anteriormente, también se indica que el servidor DNS, es un servidor autoritativo para el host solicitado.

Además en el mensaje de respuesta también se proporcionan los registros de recursos (RR) asociados al nombre que se ha consultado. En el campo “answers” se indica el registro de tipo A asociado a este nombre, donde también se indica su dirección IP. En el campo “Authoritative nameservers” se indican los servidores DNS autoritativos del dominio al que pertenece el host.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.000606	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0xf8e7
4	0.000817	192.168.236.4	192.168.236.3	DNS	117	Standard query response 0x9e24

▼ Domain Name System (response)  
   Transaction ID: 0xf8e7  
   Flags: 0x0500 Standard query response, No error  
     1... .. = Response: Message is a response  
     .000 0... .. = Opcode: Standard query (0)  
     ... ..1. = Authoritative: Server is an authority for domain  
     ... ..0. = Truncated: Message is not truncated  
     ... ..1. = Recursion desired: Do query recursively  
     ... ..1. = Recursion available: Server can do recursive queries  
     ... ..0. = Z: reserved (0)  
     ... ..0. = Answer authenticated: Answer/authority portion was not authenticated by the server  
     ... ..0. = Non-authenticated data: Unacceptable  
     ... ..0000 = Reply code: No error (0)  
   Questions: 1  
   Answer RRs: 1  
   Authority RRs: 1  
   Additional RRs: 1  
   Queries  
     ▶ www.sstt5793.org: type A, class IN  
   Answers  
     ▶ www.sstt5793.org: type A, class IN, addr 192.168.236.4  
   Authoritative nameservers  
     ▶ sstt5793.org: type NS, class IN, ns sstt5793.org  
   Additional records

4) Mensaje de respuesta a la consulta DNS de la linea 2.

7-9) Establecimiento de la conexión TCP entre cliente y servidor

10) Mensaje client\_hello enviado por el cliente. En este mensaje se especifica información como el identificador de sesión (campo Session ID), una suite de cifrado (campo Cipher Suites) que es una lista que contiene las combinaciones de algoritmos criptográficos admitidos por el cliente, y una lista de métodos de compresión admitidos por el cliente(campo Compression methods), que este caso es null.

No.	Time	Source	Destination	Protocol	Length	Info
9	0.010521	192.168.236.3	192.168.236.4	TCP	60	48500 → 443 [ACK]
10	0.013560	192.168.236.3	192.168.236.4	TLSv1.2	583	Client Hello
11	0.013888	192.168.236.4	192.168.236.3	TCP	60	443 → 48500 [ACK]

▶ Frame 10: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits)
▶ Ethernet II, Src: PcsCompu_08:3c:9a (08:00:27:08:3c:9a), Dst: PcsCompu_34:de:c0 (08:00:27:34:de:c0)
▶ Internet Protocol Version 4, Src: 192.168.236.3, Dst: 192.168.236.4
▶ Transmission Control Protocol, Src Port: 48506, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
▼ Secure Sockets Layer
- TLSv1.2 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 512
▼ Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 508
Version: TLS 1.2 (0x0303)
▶ Random: 25ae934f3280810eb514ddcc3478aec10a9df691f8d04673...
Session ID Length: 32
Session ID: da2a15e07bacbc0ef6ae4beaaff41a83532f28755a653c1c...
Cipher Suites Length: 36
▶ Cipher Suites (18 suites)
Compression Methods Length: 1
▼ Compression Methods (1 method)
Compression Method: null (0)
Extensions Length: 399

12) Esta linea incluye los mensajes “server\_hello”, “certificate”, “server\_key\_exchange”, “certificate\_request”, y “server\_hello\_done” emitidos por el servidor.

El mensaje “server\_hello” contiene los mismos campos que el mensaje anterior. En este caso se muestra el id de sesión, la suite de cifrado (campo Cipher Suites) que en este caso contiene una única suite de cifrado seleccionada por el servidor de entre las propuestas por el cliente. La suite de cifrado seleccionada es “TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256” en la cual se indica en primer lugar el método de intercambio de claves (ECDHE), en este caso el método es Diffie-Hellman de curva elíptica efímero, el cual se usa para crear claves secretas



compartidas efímeras (temporales o de un solo uso).

En segundo lugar se indica que las firmas digitales se realizarán mediante RSA. Por último se indica el algoritmo de cifrado (AES) y el algoritmo de hash (SHA256).

En este caso no se utiliza ningún método de compresión (campo “compression method” es nulo).

No.	Time	Source	Destination	Protocol	Length	Info
11	0.013932	192.168.236.4	192.168.236.3	TCP	66	443 → 48506
12	0.017663	192.168.236.4	192.168.236.3	TLSv1.2	2477	Server Hello
13	0.017699	192.168.236.3	192.168.236.4	TCP	66	48506 → 443

▶ Frame 12: 2477 bytes on wire (19816 bits), 2477 bytes captured (19816 bits)

▶ Ethernet II, Src: PcsCompu\_34:de:c0 (08:00:27:34:de:c0), Dst: PcsCompu\_08:3c:9a (08:00:27:3c:9a:08)

▶ Internet Protocol Version 4, Src: 192.168.236.4, Dst: 192.168.236.3

▶ Transmission Control Protocol, Src Port: 443, Dst Port: 48506, Seq: 1, Ack: 518, Len: 2411

▼ Secure Sockets Layer

• TLSv1.2 Record Layer: Handshake Protocol: Server Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 80

▼ Handshake Protocol: Server Hello

Handshake Type: Server Hello (2)

Length: 76

Version: TLS 1.2 (0x0303)

▶ Random: 54f32240885fe718832256bd5ff776682c7f1e7399b64289...

Session ID Length: 0

Cipher Suite: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 (0xc02f)

Compression Method: null (0)

Extensions Length: 36

▶ Extension: server\_name (len=0)

▶ Extension: renegotiation\_info (len=1)

▶ Extension: ec\_point\_formats (len=4)

▶ Extension: SessionTicket TLS (len=0)

▶ Extension: application\_layer\_protocol\_negotiation (len=11)

El siguiente mensaje mostrado es “certificate” en el cual el servidor se autentica enviando su certificado X.509. Los certificados enviados se muestran en el campo “certificates”. La información asociada a cada certificado enviado se muestra en el campo “certificate”. En primer lugar se muestra el identificador del certificado, en el cual el campo “commonName” tiene el valor [www.sstt5793.org](http://www.sstt5793.org), por lo que es el certificado del servidor. Además se envía el certificado de la CA (commonName es “ca.sstt5793.org”). Para cada certificado enviado en el campo “signedCertificate” se muestra información asociada al certificado, como por ejemplo, su periodo de validez (campo validity), información de su clave pública (campo subjectPublicKeyInfo) o el algoritmo empleado para realizar el cifrado (campo “algorithmIdentifier”).

No.	Time	Source	Destination	Protocol	Length	Info
12	0.017663	192.168.236.4	192.168.236.3	TLSv1.2	2477	Server Hello, Certificate, Server Key Exchange, C
13	0.017699	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [ACK] Seq=518 Ack=2412 Win=34048 Len=
14	0.060237	192.168.236.3	192.168.236.4	TLSv1.2	1397	Certificate, Client Key Exchange, Certificate Ver
15	0.060994	192.168.236.3	192.168.236.4	TLSv1.2	561	Application Data
<b>TLSv1.2 Record Layer: Handshake Protocol: Certificate</b> Content Type: Handshake (22) Version: TLS 1.2 (0x0303) Length: 1843 ▼ Handshake Protocol: Certificate Handshake Type: Certificate (11) Length: 1839 Certificates Length: 1836 ▼ Certificates (1836 bytes) Certificate Length: 933 ▶ Certificate: 308203a130820289a003020102020101300d06092a864886... (id-at-commonName=www.sstt5793.org,id-at-organizationalUnitN Certificate Length: 897 ▶ Certificate: 3082037d30820265a0030201020209009b7c9fb56faab7ce... (id-at-commonName=ca.sstt5793.org,id-at-organizationalUnitN						

No.	Time	Source	Destination	Protocol	Length	Info
12	0.017663	192.168.236.4	192.168.236.3	TLSv1.2	2477	Server Hello, Certificate
▼ Certificate: 308203a130820289a003020102020101300d06092a864886... (id-at-commonName=www.sstt5793.org, ▼ signedCertificate version: v3 (2) serialNumber: 1 ▼ signature (sha256WithRSAEncryption) Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption) ▶ issuer: rdnSequence (0) ▼ validity ▶ notBefore: utcTime (0) ▶ notAfter: utcTime (0) ▶ subject: rdnSequence (0) ▼ subjectPublicKeyInfo ▼ algorithm (rsaEncryption) Algorithm Id: 1.2.840.113549.1.1.1 (rsaEncryption) ▼ subjectPublicKey: 3082010a02820101009df1f19562eef342dad915541570cc... modulus: 0x009df1f19562eef342dad915541570cca095c672d04088ab... publicExponent: 65537 ▶ extensions: 4 items ▼ algorithmIdentifier (sha256WithRSAEncryption) Algorithm Id: 1.2.840.113549.1.1.11 (sha256WithRSAEncryption) Padding: 0 encrypted: 12a1ab13a175dba680b62485eefcf8ba9aa249c90b8234e54... Certificate Length: 897						

El siguiente mensaje enviado es “server\_key\_exchange” en el cual el servidor solicita un intercambio de clave. En el campo “EC Diffie-Hellman Server Params” se indica la clave pública de Diffie-Hellman a intercambiar (campo Pubkey) y en el campo “signature Algorithm” se indica el algoritmo empleado para hacer la firma digital (Signature Hash Algorithm Signature) que es RSA (la clave pública Diffie-Hellman se envía firmada con la clave privada RSA del emisor).

No.	Time	Source	Destination	Protocol	Length	Info
12	0.017663	192.168.236.4	192.168.236.3	TLSv1.2	2477	Server Hello, Ce
13	0.017699	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [ACK]
- TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange						
Content Type: Handshake (22)						
Version: TLS 1.2 (0x0303)						
Length: 333						
▼ Handshake Protocol: Server Key Exchange						
Handshake Type: Server Key Exchange (12)						
Length: 329						
▼ EC Diffie-Hellman Server Params						
Curve Type: named_curve (0x03)						
Named Curve: secp256r1 (0x0017)						
Pubkey Length: 65						
Pubkey: 0485a61cb8dc5f2f04998d86414a903cac04e6046727edab...						
▼ Signature Algorithm: rsa_pkcs1_sha256 (0x0401)						
Signature Hash Algorithm Hash: SHA256 (4)						
Signature Hash Algorithm Signature: RSA (1)						
Signature Length: 256						
Signature: 93a3d2d9c86a2334c4ff6ec32f190681f770b1015e56e510...						
▼ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages						
Content Type: Handshake (22)						
Version: TLS 1.2 (0x0303)						
Length: 135						

El siguiente mensaje mostrado es “certificate\_request” en el cual se solicita un certificado al cliente.

No.	Time	Source	Destination	Protocol	Length	Info
12	0.017663	192.168.236.4	192.168.236.3	TLSv1.2	2477	Server Hello, Certif
13	0.017699	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [ACK] Se
▶ Handshake Protocol: Server Hello						
▶ TLSv1.2 Record Layer: Handshake Protocol: Certificate						
▶ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange						
▼ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages						
Content Type: Handshake (22)						
Version: TLS 1.2 (0x0303)						
Length: 135						
- Handshake Protocol: Certificate Request						
Handshake Type: Certificate Request (13)						
Length: 127						
Certificate types count: 3						
▼ Certificate types (3 types)						
Certificate type: RSA Sign (1)						
Certificate type: DSS Sign (2)						
Certificate type: ECDSA Sign (64)						
Signature Hash Algorithms Length: 30						
▶ Signature Hash Algorithms (15 algorithms)						
Distinguished Names Length: 89						
▼ Distinguished Names (89 bytes)						
Distinguished Name Length: 87						
▶ Distinguished Name: (id-at-commonName=ca.sstt5793.org,id-at-organizationalUnitName=SSTT,id-at-or						

Este mensaje incluye dos parámetros:

-El tipo de certificado que indica el algoritmo de clave pública y su uso, que en este caso el algoritmo empleado es RSA y se utiliza solo para firmas digitales (campo “certificate types”)

-Una lista de los diferentes nombres de autoridades de certificación aceptables, que en este caso la lista solo contiene nuestra CA creada (commonName=ca.sstt5793.org) esta información se indica en el campo “Distinguished Names”.

El último mensaje mostrado es “Server Hello Done” , enviado por el servidor para indicar el final del mensaje “hello” y los demás mensajes relacionados. Este mensaje no tiene parámetros.

No.	Time	Source	Destination	Protocol	Length	Info
12	0.017663	192.168.236.4	192.168.236.3	TLSv1.2	2477	Server Hello, Certif
13	0.017699	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [ACK] Se

▶ Frame 12: 2477 bytes on wire (19816 bits), 2477 bytes captured (19816 bits)
▶ Ethernet II, Src: PcsCompu_34:de:c0 (08:00:27:34:de:c0), Dst: PcsCompu_08:3c:9a (08:00:27:08:3c:9a)
▶ Internet Protocol Version 4, Src: 192.168.236.4, Dst: 192.168.236.3
▶ Transmission Control Protocol, Src Port: 443, Dst Port: 48506, Seq: 1, Ack: 518, Len: 2411
▼ Secure Sockets Layer
▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 80
▶ Handshake Protocol: Server Hello
▶ TLSv1.2 Record Layer: Handshake Protocol: Certificate
▶ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange
▼ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
Content Type: Handshake (22)
Version: TLS 1.2 (0x0303)
Length: 135
▶ Handshake Protocol: Certificate Request
▶ Handshake Protocol: Server Hello Done
Handshake Type: Server Hello Done (14)
Length: 0

14) Esta línea incluye los mensajes “certificate”, “client\_key\_exchange” y “change\_cipher\_spec”.

En el mensaje “certificate” el cliente envía su certificado como respuesta al mensaje “certificate\_request” del servidor.

El significado de los campos de este mensaje es el mismo que el explicado anteriormente para el mensaje “certificate” enviado por el servidor. En este caso el campo “certificate” muestra el identificador del certificado del cliente cuyo “CN” es “jorge48745793F”.

No.	Time	Source	Destination	Protocol	Length	Info
11	0.013932	192.168.236.4	192.168.236.3	TCP	66	443 → 48506 [ACK] Seq=1 ACK=518 W
12	0.017663	192.168.236.4	192.168.236.3	TLSv1.2	2477	Server Hello, Certificate, Server
13	0.017699	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [ACK] Seq=518 Ack=241
14	0.060237	192.168.236.3	192.168.236.4	TLSv1.2	1397	Certificate, Client Key Exchange,
15	0.060994	192.168.236.3	192.168.236.4	TLSv1.2	561	Application Data
16	0.061509	192.168.236.4	192.168.236.3	TCP	66	443 → 48506 [ACK] Seq=2412 Ack=23
17	0.061789	192.168.236.4	192.168.236.3	TLSv1.2	1284	New Session Ticket, Change Cipher
18	0.061804	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [ACK] Seq=2412 Ack=26

▶ Frame 14: 1397 bytes on wire (11176 bits), 1397 bytes captured (11176 bits)  
 ▶ Ethernet II, Src: PcsCompu\_08:3c:9a (08:00:27:08:3c:9a), Dst: PcsCompu\_34:de:c0 (08:00:27:34:de:c0)  
 ▶ Internet Protocol Version 4, Src: 192.168.236.3, Dst: 192.168.236.4  
 ▶ Transmission Control Protocol, Src Port: 48506, Dst Port: 443, Seq: 518, Ack: 2412, Len: 1331  
 ▼ Secure Sockets Layer  
   ▼ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages  
     Content Type: Handshake (22)  
     Version: TLS 1.2 (0x0303)  
     Length: 1275  
   ▶ Handshake Protocol: Certificate  
     Handshake Type: Certificate (11)  
     Length: 937  
     Certificates Length: 934  
     ▼ Certificates (934 bytes)  
       Certificate Length: 931  
       ▶ Certificate: 3082039f30820287a003020102020102300d06092a864886... (id-at-commonName=jorge48745793F,id-at-organ

El siguiente mensaje es “client\_key\_exchange” en el cual el cliente envía su clave pública de Diffie-Hellman (campo Pubkey).

No.	Time	Source	Destination	Protocol	Length	Info
11	0.013932	192.168.236.4	192.168.236.3	TCP	66	443 → 48506 [ACK] Seq=1 ACK=518 W
12	0.017663	192.168.236.4	192.168.236.3	TLSv1.2	2477	Server Hello, Certificate, Server
13	0.017699	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [ACK] Seq=518 Ack=2412
14	0.060237	192.168.236.3	192.168.236.4	TLSv1.2	1397	Certificate, Client Key Exchange,
15	0.060994	192.168.236.3	192.168.236.4	TLSv1.2	561	Application Data

▶ Frame 14: 1397 bytes on wire (11176 bits), 1397 bytes captured (11176 bits)  
 ▶ Ethernet II, Src: PcsCompu\_08:3c:9a (08:00:27:08:3c:9a), Dst: PcsCompu\_34:de:c0 (08:00:27:34:de:c0)  
 ▶ Internet Protocol Version 4, Src: 192.168.236.3, Dst: 192.168.236.4  
 ▶ Transmission Control Protocol, Src Port: 48506, Dst Port: 443, Seq: 518, Ack: 2412, Len: 1331  
 ▼ Secure Sockets Layer  
   ▼ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages  
     Content Type: Handshake (22)  
     Version: TLS 1.2 (0x0303)  
     Length: 1275  
   ▶ Handshake Protocol: Certificate  
     Handshake Type: Certificate (11)  
     Length: 937  
     Certificates Length: 934  
     ▼ Certificates (934 bytes)  
       Certificate Length: 931  
       ▶ Certificate: 3082039f30820287a003020102020102300d06092a864886... (id-at-commonName=jorge48745793F,id-at-organ

▶ Handshake Protocol: Client Key Exchange
Handshake Type: Client Key Exchange (16)
Length: 66
▼ EC Diffie-Hellman Client Params
Pubkey Length: 65
Pubkey: 044883043389c58779457cf7d5f90b443b9ac94e66789466...

El siguiente mensaje es “certificate\_verify”, en el cual se proporciona verificación explícita del certificado de cliente.



No.	Time	Source	Destination	Protocol	Length	Info
11	0.013932	192.168.236.4	192.168.236.3	TCP	66	443 → 48506 [ACK] Seq=2477
12	0.017663	192.168.236.4	192.168.236.3	TLSv1.2	2477	Server Hello, Certificate, Client Key Exchange
13	0.017699	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [ACK] Seq=518
14	0.060237	192.168.236.3	192.168.236.4	TLSv1.2	1397	Certificate, Client Key Exchange
15	0.060994	192.168.236.3	192.168.236.4	TLSv1.2	561	Application Data

▶ Frame 14: 1397 bytes on wire (11176 bits), 1397 bytes captured (11176 bits)  
 ▶ Ethernet II, Src: PcsCompu\_08:3c:9a (08:00:27:08:3c:9a), Dst: PcsCompu\_34:de:c0 (08:00:27:34:de:c0)  
 ▶ Internet Protocol Version 4, Src: 192.168.236.3, Dst: 192.168.236.4  
 ▶ Transmission Control Protocol, Src Port: 48506, Dst Port: 443, Seq: 518, Ack: 2412, Len: 1331  
 ▼ Secure Sockets Layer  
   ▼ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages  
     Content Type: Handshake (22)  
     Version: TLS 1.2 (0x0303)  
     Length: 1275  
     ▶ Handshake Protocol: Certificate  
     ▶ Handshake Protocol: Client Key Exchange  
     - Handshake Protocol: Certificate Verify  
       Handshake Type: Certificate Verify (15)  
       Length: 260  
       ▼ Signature Algorithm: rsa\_pkcs1\_sha256 (0x0401)  
         Signature Hash Algorithm Hash: SHA256 (4)  
         Signature Hash Algorithm Signature: RSA (1)  
         Signature length: 256  
         Signature: 00c7fb215425bea5f53a4b7123c380335d87ff75e1af2be8...

En el mensaje “change\_cipher\_spec” se copia la especificación de cifrado pendiente en la especificación de cifrado operativa. El mensaje se muestra de la siguiente manera:

No.	Time	Source	Destination	Protocol	Length	Info
12	0.017663	192.168.236.4	192.168.236.3	TLSv1.2	2477	Server Hello, Certificate, Client Key Exchange
13	0.017699	192.168.236.3	192.168.236.4	TCP	66	48506 → 443 [ACK] Seq=518
14	0.060237	192.168.236.3	192.168.236.4	TLSv1.2	1397	Certificate, Client Key Exchange
15	0.060994	192.168.236.3	192.168.236.4	TLSv1.2	561	Application Data
16	0.061509	192.168.236.4	192.168.236.3	TCP	66	443 → 48506 [ACK] Seq=2412
17	0.061509	192.168.236.4	192.168.236.3	TLSv1.2	1397	Change Cipher Spec, Finished

▶ Frame 14: 1397 bytes on wire (11176 bits), 1397 bytes captured (11176 bits)  
 ▶ Ethernet II, Src: PcsCompu\_08:3c:9a (08:00:27:08:3c:9a), Dst: PcsCompu\_34:de:c0 (08:00:27:34:de:c0)  
 ▶ Internet Protocol Version 4, Src: 192.168.236.3, Dst: 192.168.236.4  
 ▶ Transmission Control Protocol, Src Port: 48506, Dst Port: 443, Seq: 518, Ack: 2412, Len: 1331  
 ▼ Secure Sockets Layer  
   ▼ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages  
     Content Type: Handshake (22)  
     Version: TLS 1.2 (0x0303)  
     Length: 1275  
     ▶ Handshake Protocol: Certificate  
     ▶ Handshake Protocol: Client Key Exchange  
     ▶ Handshake Protocol: Certificate Verify  
     - TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec  
       Content Type: Change Cipher Spec (20)  
       Version: TLS 1.2 (0x0303)  
       Length: 1  
       Change Cipher Spec Message

El servidor envía otro mensaje “change\_cipher\_spec” para actualizar especificación de cifrado (línea 17)

Por último los mensajes 39-40-42-43 son para cerrar la conexión TCP entre cliente y servidor.

Tras realizarse todo el intercambio de mensajes anteriores, los siguientes mensajes transmitidos entre cliente y servidor irán cifrados.

## 4.4 Trazas SMTP/POP

En esta sección, se van a mostrar cada uno de los mensajes DNS, SMTP y POP intercambiados al realizar el envío de un mensaje desde una dirección de correo origen a un dirección de correo destino a través del “Thunderbird”.

No.	Time	Source	Destination	Protocol	Length	Info
13	42.537502562	192.168.236.3	192.168.236.4	DNS	77	Standard query 0x3313 A smtp.sstt5793.org
14	42.537607218	192.168.236.3	192.168.236.4	DNS	77	Standard query 0x14a6 AAAA smtp.sstt5793.org
15	42.537913559	192.168.236.4	192.168.236.3	DNS	123	Standard query response 0x3313 A smtp.sstt5793.org A 192.168.236.4 NS sstt5793.org A 1
16	42.537925787	192.168.236.4	192.168.236.3	DNS	118	Standard query response 0x14a6 AAAA smtp.sstt5793.org SOA sstt5793.org
17	42.538045761	192.168.236.3	192.168.236.4	TCP	74	45070 → 25 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1601277095 TSecr=0 W
18	42.538267724	192.168.236.4	192.168.236.3	TCP	74	25 → 45070 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=4383327 T
19	42.538284264	192.168.236.3	192.168.236.4	TCP	66	45070 → 25 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1601277095 TSecr=4383327
20	42.698010851	192.168.236.4	192.168.236.3	SMTP	141	S: 220 ubuntuServer ESMTP Exim 4.86.2 Ubuntu Fri, 03 May 2019 16:08:17 +0200
21	42.698073468	192.168.236.3	192.168.236.4	TCP	66	45070 → 25 [ACK] Seq=1 Ack=76 Win=29312 Len=0 TSval=1601277255 TSecr=4383367
22	42.759587892	192.168.236.3	192.168.236.4	SMTP	88	C: EHLO [192.168.236.3]
23	42.759889093	192.168.236.4	192.168.236.3	TCP	66	25 → 45070 [ACK] Seq=76 Ack=23 Win=29056 Len=0 TSval=4383382 TSecr=1601277316
24	42.760075147	192.168.236.4	192.168.236.3	SMTP	191	S: 250-ubuntuServer Hello [192.168.236.3] [192.168.236.3]   250-SIZE 52428800   250-8B
25	42.760084793	192.168.236.3	192.168.236.4	TCP	66	45070 → 25 [ACK] Seq=23 Ack=201 Win=29312 Len=0 TSval=1601277317 TSecr=4383382
26	42.775147978	192.168.236.3	192.168.236.4	SMTP	128	C: MAIL FROM:<nombre1_5793@sstt5793.org> BODY=8BITMIME SIZE=474
27	42.775513719	192.168.236.4	192.168.236.3	SMTP	74	S: 250 OK
28	42.775959931	192.168.236.3	192.168.236.4	SMTP	103	C: RCPT TO:<nombre2_5793@sstt5793.org>
29	42.776281803	192.168.236.4	192.168.236.3	SMTP	80	S: 250 Accepted
30	42.776490676	192.168.236.3	192.168.236.4	SMTP	72	C: DATA
31	42.776738174	192.168.236.4	192.168.236.3	SMTP	122	S: 354 Enter message, ending with "." on a line by itself
32	42.777352101	192.168.236.3	192.168.236.4	SMTP	540	C: DATA fragment, 474 bytes
33	42.777483540	192.168.236.3	192.168.236.4	SMTP I...	69	from: nombre1_5793 <nombre1_5793@sstt5793.org>, subject: Nuevo mensaje, (text/plain)
34	42.777731383	192.168.236.4	192.168.236.3	TCP	66	25 → 45070 [ACK] Seq=279 Ack=605 Win=30080 Len=0 TSval=4383387 TSecr=1601277334
35	42.883801582	192.168.236.4	192.168.236.3	SMTP	94	S: 250 OK id=1hMYrJ-000001-DK
36	42.927956311	192.168.236.3	192.168.236.4	TCP	66	45070 → 25 [ACK] Seq=605 Ack=307 Win=29312 Len=0 TSval=1601277485 TSecr=4383413
37	43.147376098	192.168.236.3	192.168.236.4	SMTP	72	C: QUIT
38	43.148145335	192.168.236.4	192.168.236.3	SMTP	103	S: 221 ubuntuServer closing connection
39	43.148247258	192.168.236.3	192.168.236.4	TCP	66	45070 → 25 [ACK] Seq=611 Ack=344 Win=29312 Len=0 TSval=1601277705 TSecr=4383479
40	43.148331481	192.168.236.4	192.168.236.3	TCP	66	25 → 45070 [FIN, ACK] Seq=344 Ack=611 Win=30080 Len=0 TSval=4383479 TSecr=1601277704
41	43.191617239	192.168.236.3	192.168.236.4	TCP	66	45070 → 25 [ACK] Seq=611 Ack=345 Win=29312 Len=0 TSval=1601277748 TSecr=4383479
42	43.274569288	192.168.236.3	192.168.236.4	TCP	66	45070 → 25 [FIN, ACK] Seq=611 Ack=345 Win=29312 Len=0 TSval=1601277831 TSecr=4383479
43	43.274772149	192.168.236.4	192.168.236.3	TCP	66	25 → 45070 [ACK] Seq=345 Ack=612 Win=30080 Len=0 TSval=4383511 TSecr=1601277831

El significado de cada mensaje mostrado en la imagen anterior es el siguiente:

13) Consulta DNS. Se realiza una consulta DNS para obtener la dirección IP asociada al nombre de host “smtp.sstt5793.org”. Como se puede observar en el campo de “flags” se indica que el mensaje es una consulta. El id de la consulta es 0x3313 (indicado en el campo Transaction ID). Además en el campo “Queries” se indica que se quiere consultar el registro de tipo A del nombre “smtp.sstt5793.org”.

No.	Time	Source	Destination	Protocol	Length	Info
13	42.537502562	192.168.236.3	192.168.236.4	DNS	77	Standard query 0x3313 A smtp.sstt5793.org
14	42.537607218	192.168.236.3	192.168.236.4	DNS	77	Standard query 0x14a6 AAAA smtp.sstt5793.org
15	42.537913559	192.168.236.4	192.168.236.3	DNS	123	Standard query response 0x3313 A smtp.sstt5793.org A 192.168.236.4 NS sstt5793.org A 1
16	42.537925787	192.168.236.4	192.168.236.3	DNS	118	Standard query response 0x14a6 AAAA smtp.sstt5793.org SOA sstt5793.org
17	42.538045761	192.168.236.3	192.168.236.4	TCP	74	45070 → 25 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1601277095 TSecr=0 W
18	42.538267724	192.168.236.4	192.168.236.3	TCP	74	25 → 45070 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=4383327 T
19	42.538284264	192.168.236.3	192.168.236.4	TCP	66	45070 → 25 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1601277095 TSecr=4383327
20	42.698010851	192.168.236.4	192.168.236.3	SMTP	141	S: 220 ubuntuServer ESMTP Exim 4.86.2 Ubuntu Fri, 03 May 2019 16:08:17 +0200
21	42.698073468	192.168.236.3	192.168.236.4	TCP	66	45070 → 25 [ACK] Seq=1 Ack=76 Win=29312 Len=0 TSval=1601277255 TSecr=4383367
22	42.759587892	192.168.236.3	192.168.236.4	SMTP	88	C: EHLO [192.168.236.3]
23	42.759889093	192.168.236.4	192.168.236.3	TCP	66	25 → 45070 [ACK] Seq=76 Ack=23 Win=29056 Len=0 TSval=4383382 TSecr=1601277316
24	42.760075147	192.168.236.4	192.168.236.3	SMTP	191	S: 250-ubuntuServer Hello [192.168.236.3] [192.168.236.3]   250-SIZE 52428800   250-8B
25	42.760084793	192.168.236.3	192.168.236.4	TCP	66	45070 → 25 [ACK] Seq=23 Ack=201 Win=29312 Len=0 TSval=1601277317 TSecr=4383382
26	42.775147978	192.168.236.3	192.168.236.4	SMTP	128	C: MAIL FROM:<nombre1_5793@sstt5793.org> BODY=8BITMIME SIZE=474
27	42.775513719	192.168.236.4	192.168.236.3	SMTP	74	S: 250 OK
28	42.775959931	192.168.236.3	192.168.236.4	SMTP	103	C: RCPT TO:<nombre2_5793@sstt5793.org>
29	42.776281803	192.168.236.4	192.168.236.3	SMTP	80	S: 250 Accepted
30	42.776490676	192.168.236.3	192.168.236.4	SMTP	72	C: DATA
31	42.776738174	192.168.236.4	192.168.236.3	SMTP	122	S: 354 Enter message, ending with "." on a line by itself
32	42.777352101	192.168.236.3	192.168.236.4	SMTP	540	C: DATA fragment, 474 bytes
33	42.777483540	192.168.236.3	192.168.236.4	SMTP I...	69	from: nombre1_5793 <nombre1_5793@sstt5793.org>, subject: Nuevo mensaje, (text/plain)
34	42.777731383	192.168.236.4	192.168.236.3	TCP	66	25 → 45070 [ACK] Seq=279 Ack=605 Win=30080 Len=0 TSval=4383387 TSecr=1601277334
35	42.883801582	192.168.236.4	192.168.236.3	SMTP	94	S: 250 OK id=1hMYrJ-000001-DK
36	42.927956311	192.168.236.3	192.168.236.4	TCP	66	45070 → 25 [ACK] Seq=605 Ack=307 Win=29312 Len=0 TSval=1601277485 TSecr=4383413
37	43.147376098	192.168.236.3	192.168.236.4	SMTP	72	C: QUIT
38	43.148145335	192.168.236.4	192.168.236.3	SMTP	103	S: 221 ubuntuServer closing connection
39	43.148247258	192.168.236.3	192.168.236.4	TCP	66	45070 → 25 [ACK] Seq=611 Ack=344 Win=29312 Len=0 TSval=1601277705 TSecr=4383479
40	43.148331481	192.168.236.4	192.168.236.3	TCP	66	25 → 45070 [FIN, ACK] Seq=344 Ack=611 Win=30080 Len=0 TSval=4383479 TSecr=1601277704
41	43.191617239	192.168.236.3	192.168.236.4	TCP	66	45070 → 25 [ACK] Seq=611 Ack=345 Win=29312 Len=0 TSval=1601277748 TSecr=4383479
42	43.274569288	192.168.236.3	192.168.236.4	TCP	66	45070 → 25 [FIN, ACK] Seq=611 Ack=345 Win=29312 Len=0 TSval=1601277831 TSecr=4383479
43	43.274772149	192.168.236.4	192.168.236.3	TCP	66	25 → 45070 [ACK] Seq=345 Ack=612 Win=30080 Len=0 TSval=4383511 TSecr=1601277831

▶ Frame 13: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0

▶ Ethernet II, Src: PcsCompu\_08:3c:9a (08:00:27:08:3c:9a), Dst: PcsCompu\_34:de:c0 (08:00:27:34:de:c0)

▶ Internet Protocol Version 4, Src: 192.168.236.3, Dst: 192.168.236.4

▶ User Datagram Protocol, Src Port: 44332, Dst Port: 53

▼ Domain Name System (query)

Transaction ID: 0x3313

Flags: 0x0100 Standard query

9... .. = Response: Message is a query

.000 0... .. = Opcode: Standard query (0)

... .. = Truncated: Message is not truncated

... ..1 ... = Recursion desired: Do query recursively

... ..0... .. = Z: reserved (0)

... ..0 ... = Non-authenticated data: Unacceptable

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

▼ Queries

smtp.sstt5793.org: type A, class IN

Name: smtp.sstt5793.org

[Name Length: 17]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

[Response In: 15]

14) Consulta DNS sobre el mismo nombre de host que la consulta anterior, pero en este caso para obtener la dirección IPv6 asociada al nombre (registro AAAA)

15) Respuesta DNS asociada a la solicitud anterior. Como se puede observar en el campo “flags” se indica el identificador de la respuesta (0x3313) que es el mismo que el de la consulta realizada anteriormente, también se indica que es un mensaje de respuesta y que el servidor DNS, es un servidor autoritativo para el host solicitado.

Además en el mensaje de respuesta también se proporcionan los registros de recursos (RR) asociados al nombre que se ha consultado. En el campo “answers” se indica el registro de tipo A asociado a este nombre, donde también se indica su dirección IP. En el campo “Authoritative nameservers” se indican los servidores DNS autoritativos del dominio al que pertenece el host.

No.	Time	Source	Destination	Protocol	Length	Info
15	42.537913559	192.168.236.4	192.168.236.3	DNS	123	Standard query response 0x3313 A smtp.sstt5793.org
16	42.537925787	192.168.236.4	192.168.236.3	DNS	118	Standard query response 0x14a6 AAAA smtp.sstt5793.org
17	42.538045761	192.168.236.3	192.168.236.4	TCP	74	45070 -> 25 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SA=192.168.236.3 Dst=192.168.236.4
18	42.538267724	192.168.236.4	192.168.236.3	TCP	74	25 -> 45070 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0

▶ Ethernet II, Src: PcsCompu\_34:de:c0 (08:00:27:34:de:c0), Dst: PcsCompu\_08:3c:9a (08:00:27:08:3c:9a)

▶ Internet Protocol Version 4, Src: 192.168.236.4, Dst: 192.168.236.3

▶ User Datagram Protocol, Src Port: 53, Dst Port: 44332

▼ Domain Name System (response)

Transaction ID: 0x3313

▼ Flags: 0x8580 Standard query response, No error

1... .. = Response: Message is a response

... .. = Opcode: Standard query (0)

... ..1... .. = Authoritative: Server is an authority for domain

... ..0... .. = Truncated: Message is not truncated

... ..1... .. = Recursion desired: Do query recursively

... ..1... .. = Recursion available: Server can do recursive queries

... ..0... .. = Z: reserved (0)

... ..0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server

... ..0... .. = Non-authenticated data: Unacceptable

... ..0000 = Reply code: No error (0)

Questions: 1

Answer RRs: 1

Authority RRs: 1

Additional RRs: 1

▼ Queries

▶ smtp.sstt5793.org: type A, class IN

▼ Answers

▶ smtp.sstt5793.org: type A, class IN, addr 192.168.236.4

▼ Authoritative nameservers

▶ sstt5793.org: type NS, class IN, ns sstt5793.org

▼ Additional records

▶ sstt5793.org: type A, class IN, addr 192.168.236.4

[Request In: 13]

[Time: 0.000410997 seconds]

16) Mensaje de respuesta a la consulta DNS de la línea 14.

17-19) Establecimiento de la conexión TCP por parte del cliente.

20) Respuesta 220 del servidor tras establecer la conexión.

22) El cliente manda un mensaje con el comando “HELO” para abrir una sesión con el servidor

24) El servidor manda un mensaje de respuesta al mensaje “HELO” del cliente.



- 26) El cliente manda un mensaje con el comando “MAIL FROM” indicando la dirección de correo del emisor.
- 27) Mensaje de respuesta del servidor al mensaje anterior.
- 28) El cliente manda un mensaje con el comando “RCPT TO” indicando la dirección de correo del receptor.
- 29) Mensaje de respuesta del servidor al mensaje anterior.
- 30) El cliente manda un mensaje DATA indicando que se va a introducir el contenido del mensaje.
- 31) Mensaje de respuesta del servidor al mensaje anterior.
- 32) En este mensaje se indica todo lo relativo al mensaje de correo enviado.

No.	Time	Source	Destination	Protocol	Length	Info
21	0.404942102	192.168.236.3	192.168.236.4	SMTP	534	C: DATA fragment, 468 bytes
22	0.405085908	192.168.236.3	192.168.236.4	SMTP	69	from: nombre1_5793 <nombre1_5793@sstt5793.org>
23	0.417990292	192.168.236.3	192.168.236.4	TCP	69	[TCP Retransmission] 44636 → 44636
24	0.418260446	192.168.236.4	192.168.236.3	TCP	78	25 → 44636 [ACK] Seq=279 Ack=44636
25	0.457094290	192.168.236.4	192.168.236.3	SMTP	94	S: 250 OK id=1hMUfs-0000Wy-8:1
26	0.457682461	192.168.236.3	192.168.236.4	SMTP	72	C: QUIT

▶ Frame 21: 534 bytes on wire (4272 bits), 534 bytes captured (4272 bits) on interface 0  
 ▶ Ethernet II, Src: PcsCompu\_08:3c:9a (08:00:27:08:3c:9a), Dst: PcsCompu\_34:de:c0 (08:00:27:34:de:c0)  
 ▶ Internet Protocol Version 4, Src: 192.168.236.3, Dst: 192.168.236.4  
 ▶ Transmission Control Protocol, Src Port: 44636, Dst Port: 25, Seq: 128, Ack: 279, Len: 468  
 ▼ Simple Mail Transfer Protocol  
   ▼ Line-based text data (14 lines)  
     To: nombre2\_5793@sstt5793.org\r\n  
     From: nombre1\_5793 <nombre1\_5793@sstt5793.org>\r\n  
     Subject: Nuevo mensaje\r\n  
     Message-ID: <3cb87a61-998b-3c05-54e3-f9a63678af17@sstt5793.org>\r\n  
     Date: Fri, 3 May 2019 11:40:11 +0200\r\n  
     User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:60.0) Gecko/20100101 Thunderbird/60.6.1\r\n  
     MIME-Version: 1.0\r\n  
     Content-Type: text/plain; charset=utf-8; format=flowed\r\n  
     Content-Transfer-Encoding: 7bit\r\n  
     Content-Language: en-US\r\n  
     \r\n  
     Hola este es un mensaje de prueba\r\n  
     \r\n  
     Reassembled DATA in frame: 22

Como se puede observar en la imagen anterior en el campo “To” se indica el correo del destinatario, en el campo “From” se indica el correo del emisor, en el campo “Message-ID” se indica el id del mensaje, en el campo “Subject” se indica el asunto del mensaje y en el campo “Content-Language” se indica el contenido del mensaje.

- 33) En este mensaje se indica el final del mensaje para el servidor. Este mensaje consta unicamente del carácter “.”

35) Mensaje de respuesta del servidor al mensaje anterior.

37) Mensaje “QUIT” enviado por el cliente para cerrar la sesión con el servidor.

38) Mensaje de respuesta del servidor , al mensaje anterior , indicando que se cierra la sesión.

40-43) Cierre de la conexión TCP entre cliente y servidor.

No.	Time	Source	Destination	Protocol	Length	Info
44	46.889108459	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x0f0a A pop.sstt5793.org
45	46.889203108	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x1178 AAAA pop.sstt5793.org
46	46.889498300	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0x0f0a A pop.sstt5793.org A 192.168.236.4 NS sstt5793
47	46.889510860	192.168.236.4	192.168.236.3	DNS	117	Standard query response 0x1178 AAAA pop.sstt5793.org SOA sstt5793.org
48	46.889649278	192.168.236.3	192.168.236.4	TCP	74	45922 → 110 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1601281446
49	46.889842228	192.168.236.4	192.168.236.3	TCP	74	110 → 45922 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=
50	46.889858468	192.168.236.3	192.168.236.4	TCP	66	45922 → 110 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1601281447 TSecr=4384415
51	46.900534820	192.168.236.4	192.168.236.3	POP	86	S: +OK Dovecot ready.
52	46.900561278	192.168.236.3	192.168.236.4	TCP	66	45922 → 110 [ACK] Seq=1 Ack=21 Win=29312 Len=0 TSval=1601281457 TSecr=4384417
53	46.912254514	192.168.236.3	192.168.236.4	POP	72	C: CAPA
54	46.912509134	192.168.236.4	192.168.236.3	TCP	66	110 → 45922 [ACK] Seq=21 Ack=7 Win=29056 Len=0 TSval=4384420 TSecr=1601281469
55	46.912605450	192.168.236.4	192.168.236.3	POP	149	S: +OK
56	46.922504655	192.168.236.3	192.168.236.4	POP	78	C: AUTH PLAIN
57	46.922945135	192.168.236.4	192.168.236.3	POP	70	+
58	46.940346835	192.168.236.3	192.168.236.4	POP	96	C: AG5vbWJyZTJfNTc5MmBub21icmUy
59	46.959944608	192.168.236.4	192.168.236.3	POP	82	S: +OK Logged in.
60	46.960146996	192.168.236.3	192.168.236.4	POP	72	C: STAT
61	46.970082580	192.168.236.4	192.168.236.3	POP	78	S: +OK 2 1618
62	46.974227534	192.168.236.3	192.168.236.4	POP	72	C: LIST
63	46.974547206	192.168.236.4	192.168.236.3	POP	100	S: +OK 2 messages:
64	46.985016842	192.168.236.3	192.168.236.4	POP	72	C: UIDL
65	46.985222831	192.168.236.4	192.168.236.3	POP	114	S: +OK
66	46.985761137	192.168.236.3	192.168.236.4	POP	74	C: RETR 2
67	46.986207673	192.168.236.4	192.168.236.3	POP	897	S: +OK 812 octets
68	47.027961780	192.168.236.3	192.168.236.4	TCP	66	45922 → 110 [ACK] Seq=75 Ack=1049 Win=30976 Len=0 TSval=1601281585 TSecr=4384
69	47.035609640	192.168.236.3	192.168.236.4	POP	72	C: QUIT
70	47.040312509	192.168.236.4	192.168.236.3	POP	84	S: +OK Logging out.
71	47.063906968	192.168.236.3	192.168.236.4	TCP	66	45922 → 110 [ACK] Seq=81 Ack=1068 Win=30976 Len=0 TSval=1601281641 TSecr=4384
72	47.107084259	192.168.236.3	192.168.236.4	TCP	66	45922 → 110 [FIN, ACK] Seq=81 Ack=1068 Win=30976 Len=0 TSval=1601281664 TSecr=
73	47.107427454	192.168.236.4	192.168.236.3	TCP	66	110 → 45922 [ACK] Seq=1068 Ack=82 Win=29056 Len=0 TSval=4384469 TSecr=1601281

El significado de los mensajes de la imagen anterior es el siguiente:

44) Consulta DNS. Se realiza una consulta DNS para obtener la dirección IP asociada al nombre de host “pop.sstt5793.org”. Como se puede observar en el campo de “flags” se indica que el mensaje es una consulta. El id de la consulta es 0x0f0a (indicado en el campo Transaction ID). Además en el campo “Queries” se indica que se quiere consultar el registro de tipo A del nombre “pop.sstt5793.org”.

No.	Time	Source	Destination	Protocol	Length	Info
44	46.889108459	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x0f0a A pop.sstt5793.org
45	46.889203108	192.168.236.3	192.168.236.4	DNS	76	Standard query 0x1178 AAAA pop.sstt5793.org
46	46.889498300	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0x0f0a A pop.sstt5793
47	46.889510860	192.168.236.4	192.168.236.3	DNS	117	Standard query response 0x1178 AAAA pop.sstt
▶ Frame 44: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0						
▶ Ethernet II, Src: PcsCompu_08:3c:9a (08:00:27:08:3c:9a), Dst: PcsCompu_34:de:c0 (08:00:27:34:de:c0)						
▶ Internet Protocol Version 4, Src: 192.168.236.3, Dst: 192.168.236.4						
▶ User Datagram Protocol, Src Port: 39206, Dst Port: 53						
▼ Domain Name System (query)						
Transaction ID: 0x0f0a						
▼ Flags: 0x0100 Standard query						
0... .. = Response: Message is a query						
.000 0... .. = Opcode: Standard query (0)						
... ..0... .. = Truncated: Message is not truncated						
... ..1... .. = Recursion desired: Do query recursively						
... ..0... .. = Z: reserved (0)						
... ..0... .. = Non-authenticated data: Unacceptable						
Questions: 1						
Answer RRs: 0						
Authority RRs: 0						
Additional RRs: 0						
▼ Queries						
▼ pop.sstt5793.org: type A, class IN						
Name: pop.sstt5793.org						
[Name Length: 16]						
[Label Count: 3]						
Type: A (Host Address) (1)						
Class: IN (0x0001)						
[Response In: 46]						

46) Respuesta DNS asociada a la solicitud anterior. Como se puede observar en el campo “flags” se indica el identificador de la respuesta (0x0f0a) que es el mismo que el de la consulta realizada anteriormente, también se indica que es un mensaje de respuesta y que el servidor DNS, es un servidor autoritativo para el host solicitado. Además en el mensaje de respuesta también se proporcionan los registros de recursos (RR) asociados al nombre que se ha consultado. En el campo “answers” se indica el registro de tipo A asociado a este nombre, donde también se indica su dirección IP. En el campo “Authoritative nameservers” se indican los servidores DNS autoritativos del dominio al que pertenece el host.

No.	Time	Source	Destination	Protocol	Length	Info
46	46.889498300	192.168.236.4	192.168.236.3	DNS	122	Standard query response 0x0f0a A pop.sstt5793.org
47	46.889510860	192.168.236.4	192.168.236.3	DNS	117	Standard query response 0x1178 AAAA pop.sstt5793.org
48	46.889649278	192.168.236.3	192.168.236.4	TCP	74	45922 → 110 [SYN] Seq=0 Win=29200 Len=0 MSS=1460
49	46.889842228	192.168.236.4	192.168.236.3	TCP	74	110 → 45922 [ACK] Seq=0 Ack=1 Win=28960 Len=0

```

▶ Frame 46: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
▶ Ethernet II, Src: PcsCompu_34:de:c0 (08:00:27:34:de:c0), Dst: PcsCompu_08:3c:9a (08:00:27:08:3c:9a)
▶ Internet Protocol Version 4, Src: 192.168.236.4, Dst: 192.168.236.3
▶ User Datagram Protocol, Src Port: 53, Dst Port: 39206
▼ Domain Name System (response)
  Transaction ID: 0x0f0a
  ▼ Flags: 0x8580 Standard query response, No error
    1... .. = Response: Message is a response
    .000 0... .. = Opcode: Standard query (0)
    .... 1... .. = Authoritative: Server is an authority for domain
    .... 0... .. = Truncated: Message is not truncated
    .... 1... .. = Recursion desired: Do query recursively
    .... 1... .. = Recursion available: Server can do recursive queries
    .... 0... .. = Z: reserved (0)
    .... 0... .. = Answer authenticated: Answer/authority portion was not authenticated by the server
    .... 0... .. = Non-authenticated data: Unacceptable
    .... 0000 = Reply code: No error (0)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 1
  Additional RRs: 1
  ▼ Queries
    ▶ pop.sstt5793.org: type A, class IN
  ▼ Answers
    ▶ pop.sstt5793.org: type A, class IN, addr 192.168.236.4
  ▼ Authoritative nameservers
    ▶ sstt5793.org: type NS, class IN, ns sstt5793.org
  ▼ Additional records
    ▶ sstt5793.org: type A, class IN, addr 192.168.236.4
  [Request In: 44]

```

48-50) Establecimiento de la conexión TCP por parte del cliente.

51) Respuesta del servidor tras establecer la conexión.

53) Mensaje del cliente con el comando “CAPA” que pregunta las capacidades del servidor POP

55) Mensaje de respuesta del servidor al mensaje anterior conteniendo lo siguiente:

No.	Time	Source	Destination	Protocol	Length	Info
51	46.900534820	192.168.236.4	192.168.236.3	POP	86	S: +OK Dovecot ready.
52	46.900561278	192.168.236.3	192.168.236.4	TCP	66	45922 → 110 [ACK] Seq=1 Ac
53	46.912254514	192.168.236.3	192.168.236.4	POP	72	C: CAPA
54	46.912509134	192.168.236.4	192.168.236.3	TCP	66	110 → 45922 [ACK] Seq=21 A
55	46.912605450	192.168.236.4	192.168.236.3	POP	149	S: +OK
56	46.922504655	192.168.236.3	192.168.236.4	POP	78	C: AUTH PLAIN
57	46.922945135	192.168.236.4	192.168.236.3	POP IMF	70	+
58	46.940346835	192.168.236.3	192.168.236.4	POP	96	C: AG5vbWJyZTJfNTc5MwBub2
59	46.959944608	192.168.236.4	192.168.236.3	POP	82	S: +OK Logged in.
60	46.960146996	192.168.236.3	192.168.236.4	POP	72	C: STAT
61	46.970082580	192.168.236.4	192.168.236.3	POP	78	S: +OK 2 1618
62	46.974227534	192.168.236.3	192.168.236.4	POP	72	C: LIST
63	46.974547206	192.168.236.4	192.168.236.3	POP	100	S: +OK 2 messages:
64	46.985016842	192.168.236.3	192.168.236.4	POP	72	C: UIDL

▶ Frame 55: 149 bytes on wire (1192 bits), 149 bytes captured (1192 bits) on interface 0  
 ▶ Ethernet II, Src: PcsCompu\_34:de:c0 (08:00:27:34:de:c0), Dst: PcsCompu\_08:3c:9a (08:00:27:08:3c:9a)  
 ▶ Internet Protocol Version 4, Src: 192.168.236.4, Dst: 192.168.236.3  
 ▶ Transmission Control Protocol, Src Port: 110, Dst Port: 45922, Seq: 21, Ack: 7, Len: 83  
 ▼ Post Office Protocol  
   ▼ +OK\r\n  
     Response indicator: +OK  
     CAPA\r\n  
     TOP\r\n  
     UIDL\r\n  
     RESP-CODES\r\n  
     PIPELINING\r\n  
     AUTH-RESP-CODE\r\n  
     USER\r\n  
     SASL PLAIN\r\n  
     .\r\n

56) Mensaje del cliente con el comando “AUTH”.Este comando indica al servidor un mecanismo de autenticación. Si el servidor lo soporta se produce un intercambio entre cliente y servidor a través de un protocolo de autenticación para “autenticar e identificar al usuario”

58) En este mensaje el cliente indica su nombre de usuario y contraseña cifrado en base 64.

59) Mensaje del servidor que indica que la autenticación se ha realizado correctamente.

60) Mensaje del cliente con el comando “STAT”

61) Mensaje de respuesta del servidor al mensaje anterior. El servidor responde al comando “STAT” indicando la cantidad total de mensajes y la cantidad total de octetos de todos los mensajes.

No.	Time	Source	Destination	Protocol	Length	Info
60	46.960146996	192.168.236.3	192.168.236.4	POP	72	C: STAT
61	46.970082580	192.168.236.4	192.168.236.3	POP	78	S: +OK 2 1618
62	46.974227534	192.168.236.3	192.168.236.4	POP	72	C: LIST
63	46.974547206	192.168.236.4	192.168.236.3	POP	100	S: +OK 2 messages:
▶ Frame 61: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0 ▶ Ethernet II, Src: PcsCompu_34:de:c0 (08:00:27:34:de:c0), Dst: PcsCompu_08:3c:9a (08:00:27:08:3c:9a) ▶ Internet Protocol Version 4, Src: 192.168.236.4, Dst: 192.168.236.3 ▶ Transmission Control Protocol, Src Port: 110, Dst Port: 45922, Seq: 124, Ack: 55, Len: 12 ▼ Post Office Protocol ▼ +OK 2 1618\r\n Response indicator: +OK Response description: 2 1618						

Como se muestra en la imagen anterior solo hay dos mensaje que ocupan un total de 1618 octetos entre los dos.

62) Mensaje del cliente con el comando “LIST” que solicita el listado de los mensajes.

63) Mensaje de respuesta del servidor al mensaje anterior.

No.	Time	Source	Destination	Protocol	Length	Info
60	46.960146996	192.168.236.3	192.168.236.4	POP	72	C: STAT
61	46.970082580	192.168.236.4	192.168.236.3	POP	78	S: +OK 2 1618
62	46.974227534	192.168.236.3	192.168.236.4	POP	72	C: LIST
63	46.974547206	192.168.236.4	192.168.236.3	POP	100	S: +OK 2 messages:
64	46.985016842	192.168.236.3	192.168.236.4	POP	72	C: UIDL
65	46.985222831	192.168.236.4	192.168.236.3	POP	114	S: +OK
▶ Frame 63: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0 ▶ Ethernet II, Src: PcsCompu_34:de:c0 (08:00:27:34:de:c0), Dst: PcsCompu_08:3c:9a (08:00:27:08:3c:9a) ▶ Internet Protocol Version 4, Src: 192.168.236.4, Dst: 192.168.236.3 ▶ Transmission Control Protocol, Src Port: 110, Dst Port: 45922, Seq: 136, Ack: 61, Len: 34 ▼ Post Office Protocol ▼ +OK 2 messages:\r\n Response indicator: +OK Response description: 2 messages: 1 806\r\n 2 812\r\n .\r\n						

Como se puede observar en la imagen anterior en la respuesta para cada mensaje se muestra un número que lo identifica y el número de octetos que ocupa.

66) Mensaje del cliente con el comando “RETR” en el que se indica que se quiere obtener el mensaje con el número 2

67) Respuesta del servidor al mensaje anterior, en el cual, se especifica información del mensaje solicitado.

No.	Time	Source	Destination	Protocol	Length	Info
67	46.986207673	192.168.236.4	192.168.236.3	POP	897	S: +OK 812 octets
68	47.027961780	192.168.236.3	192.168.236.4	TCP	66	45922 → 110 [ACK] Seq=75 Ac
69	47.035609640	192.168.236.3	192.168.236.4	POP	72	C: QUIT
70	47.040312569	192.168.236.4	192.168.236.3	POP	84	S: +OK Logging out.
71	47.083906968	192.168.236.3	192.168.236.4	TCP	66	45922 → 110 [ACK] Seq=81 Ac
▶ Transmission Control Protocol, Src Port: 110, Dst Port: 45922, Seq: 218, Ack: 75, Len: 831						
▼ Post Office Protocol						
▼ +OK 812 octets\r\n						
Response indicator: +OK						
Response description: 812 octets						
Return-path: <nombre1_5793@sstt5793.org>\r\n						
Envelope-to: nombre2_5793@sstt5793.org\r\n						
Delivery-date: Fri, 03 May 2019 16:08:17 +0200\r\n						
Received: from [192.168.236.3]\r\n						
\tbody ubuntuServer with esmtp (Exim 4.86_2)\r\n						
\t(envelope-from <nombre1_5793@sstt5793.org>)\r\n						
\tid 1hMYrJ-0000it-DK\r\n						
\tfor nombre2_5793@sstt5793.org; Fri, 03 May 2019 16:08:17 +0200\r\n						
To: nombre2_5793@sstt5793.org\r\n						
From: nombre1_5793 <nombre1_5793@sstt5793.org>\r\n						
Subject: Nuevo mensaje\r\n						
Message-ID: <3394560a-d603-cb55-7faa-b5f456123f56@sstt5793.org>\r\n						
Date: Fri, 3 May 2019 16:08:17 +0200\r\n						
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101\r\n						
Thunderbird/60.6.1\r\n						
MIME-Version: 1.0\r\n						
Content-Type: text/plain; charset=utf-8; format=flowed\r\n						
Content-Transfer-Encoding: 7bit\r\n						
Content-Language: en-US\r\n						
\r\n						
Hola esto es un nuevo mensaje de prueba\r\n						
\r\n						
.\r\n						

Como se puede observar se especifica el correo del emisor, el correo del destinatario, el asunto del mensaje, el id del mensaje, el agente de usuario (Thunderbird) y el contenido del mensaje.

69) Mensaje del cliente para cerrar la sesión establecida con el servidor.

70) Mensaje de respuesta del servidor al mensaje anterior.

72-73) Cierre de la conexión TCP entre cliente y servidor.

## 4.5 Trazas IPsec

A continuación se muestra el intercambio de paquetes realizado con IPsec al realizar un ping desde el cliente al servidor. En la secuencia de mensajes se puede ver el intercambio de mensajes IKEv2 para el establecimiento de la IPsec SA y las cabeceras ESP con el contenido de los paquetes IP autenticados.



No.	Time	Source	Destination	Protocol	Length	Info
22	13.088290288	192.168.236.3	192.168.236.4	ISAKMP	118	INFORMATIONAL MID=00 Responder Request
23	13.088973843	192.168.236.4	192.168.236.3	ISAKMP	118	INFORMATIONAL MID=00 Initiator Response
24	15.342126371	192.168.236.3	192.168.236.4	ISAKMP	1166	IKE_SA_INIT MID=00 Initiator Request
25	15.349848851	192.168.236.4	192.168.236.3	ISAKMP	523	IKE_SA_INIT MID=00 Responder Response
26	15.360411402	192.168.236.3	192.168.236.4	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=f952) [Reassembled in #27]
27	15.360487645	192.168.236.3	192.168.236.4	ISAKMP	270	IKE_AUTH MID=01 Initiator Request
28	15.365843827	192.168.236.4	192.168.236.3	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=1809) [Reassembled in #29]
29	15.365851054	192.168.236.4	192.168.236.3	ISAKMP	60	IKE_AUTH MID=01 Responder Response
30	16.982977531	192.168.236.3	192.168.236.4	ESP	150	ESP (SPI=0xca1a43fa)
31	16.983238497	192.168.236.4	192.168.236.3	ESP	150	ESP (SPI=0xc2d28a41)
32	16.983238497	192.168.236.4	192.168.236.3	ICMP	98	Echo (ping) reply id=0x1612, seq=1/256, ttl=64
33	18.002942611	192.168.236.3	192.168.236.4	ESP	150	ESP (SPI=0xca1a43fa)
34	18.003442639	192.168.236.4	192.168.236.3	ESP	150	ESP (SPI=0xc2d28a41)
35	18.003442639	192.168.236.4	192.168.236.3	ICMP	98	Echo (ping) reply id=0x1612, seq=2/512, ttl=64
36	19.026833783	192.168.236.3	192.168.236.4	ESP	150	ESP (SPI=0xca1a43fa)
37	19.027242577	192.168.236.4	192.168.236.3	ESP	150	ESP (SPI=0xc2d28a41)
38	19.027242577	192.168.236.4	192.168.236.3	ICMP	98	Echo (ping) reply id=0x1612, seq=3/768, ttl=64
39	20.051899054	192.168.236.3	192.168.236.4	ESP	150	ESP (SPI=0xca1a43fa)
40	20.052220922	192.168.236.4	192.168.236.3	ESP	150	ESP (SPI=0xc2d28a41)
41	20.052220922	192.168.236.4	192.168.236.3	ICMP	98	Echo (ping) reply id=0x1612, seq=4/1024, ttl=64
42	20.358301101	PcsCompu_34:de:c0	PcsCompu_08:3c:9a	ARP	60	Who has 192.168.236.3? Tell 192.168.236.4
43	20.358345000	PcsCompu_08:3c:9a	PcsCompu_34:de:c0	ARP	42	192.168.236.3 is at 08:00:27:08:3c:9a
44	20.819881964	192.168.236.1	255.255.255.255	DB-LSP...	243	Dropbox LAN sync Discovery Protocol
45	20.822080086	192.168.236.1	255.255.255.255	DB-LSP...	243	Dropbox LAN sync Discovery Protocol
46	20.822102601	192.168.236.1	255.255.255.255	DB-LSP...	243	Dropbox LAN sync Discovery Protocol
47	20.822264613	192.168.236.1	255.255.255.255	DB-LSP...	243	Dropbox LAN sync Discovery Protocol
48	20.822848432	192.168.236.1	255.255.255.255	DB-LSP...	243	Dropbox LAN sync Discovery Protocol
49	20.822871136	192.168.236.1	255.255.255.255	DB-LSP...	243	Dropbox LAN sync Discovery Protocol
50	21.077228976	192.168.236.3	192.168.236.4	ESP	150	ESP (SPI=0xca1a43fa)
51	21.077618885	192.168.236.4	192.168.236.3	ESP	150	ESP (SPI=0xc2d28a41)
52	21.077618885	192.168.236.4	192.168.236.3	ICMP	98	Echo (ping) reply id=0x1612, seq=5/1280, ttl=64
53	50.846589600	192.168.236.1	255.255.255.255	DB-LSP...	243	Dropbox LAN sync Discovery Protocol
54	50.849546361	192.168.236.1	255.255.255.255	DB-LSP...	243	Dropbox LAN sync Discovery Protocol
55	50.849564275	192.168.236.1	255.255.255.255	DB-LSP...	243	Dropbox LAN sync Discovery Protocol

24-25) Mensajes IKE\_SA\_INIT. En este par de mensajes cliente y servidor intercambian información sobre algoritmos criptográficos, otros parámetros de seguridad y valores de Diffie-Hellman. Tras este intercambio se establece una asociación de seguridad especial llamada IKE SA. Esta SA define parámetros para un canal seguro entre cliente y servidor, sobre el cual se realizara todo el intercambio de mensajes IKE.

27 y 29) Mensajes IKE\_AUTH. En este par de mensajes cliente y servidor se autentican y se establece una asociación seguridad Ipsec que se utiliza para proteger mensajes ordinarios

30) En esta linea el cliente envía al servidor un paquete protegido con la cabecera ESP. En esta cabecera se transporta el SPI de la asociación de seguridad elegido por el receptor de la SA. En este caso el SPI es “0xca1a43fa”

31) En esta linea el servidor envía un “ping reply” al cliente como respuesta al mensaje anterior. Este mensaje al igual que el anterior va protegido con una cabecera ESP, donde se transporta el SPI de la SA elegido por el receptor de la SA. En este caso el SPI es “0xc2d28a41”.

32) Cuando el mensaje anterior llega al cliente, estando en el nivel 3, el kernel lo descifra y encuentra un ICMP. Wireshark muestra este ICMP descifrado.



Los mensajes correspondientes a los siguientes paquetes transmitidos muestran la misma información explicada anteriormente.

## **5. Problemas encontrados en el desarrollo del escenario**

Los principales problemas que tuve durante la realización de la práctica fueron en la implementación del servidor web en c, ya que en muchas ocasiones no sabía exactamente que tenía que implementar, lo cual me llevo a estancarme varias veces.

## **6. Número de horas aproximadas empleadas en cada apartado y en la documentación**

El número aproximando de horas empleado en cada una de los apartados realizados es el siguiente:

2.1 Programación Web-SSTT HTTP server: 25 horas

2.2 Desplegar servicio DNS: 6 horas

2.3 Desplegar servicio SMTP/POP: 2 horas

2.4 Desplegar servicio HTTP/HTTPS: 3 horas

2.5 IPsec: 2 horas

Documentación: 40 horas

## **7. Conclusiones**

Como conclusión la práctica me ha parecido bastante didáctica en cuanto al funcionamiento de cada uno de los servicios implementados. Además la realización de esta memoria y el análisis de las trazas de wireshark para cada uno de los servicios ayuda a asentar muchos conceptos.