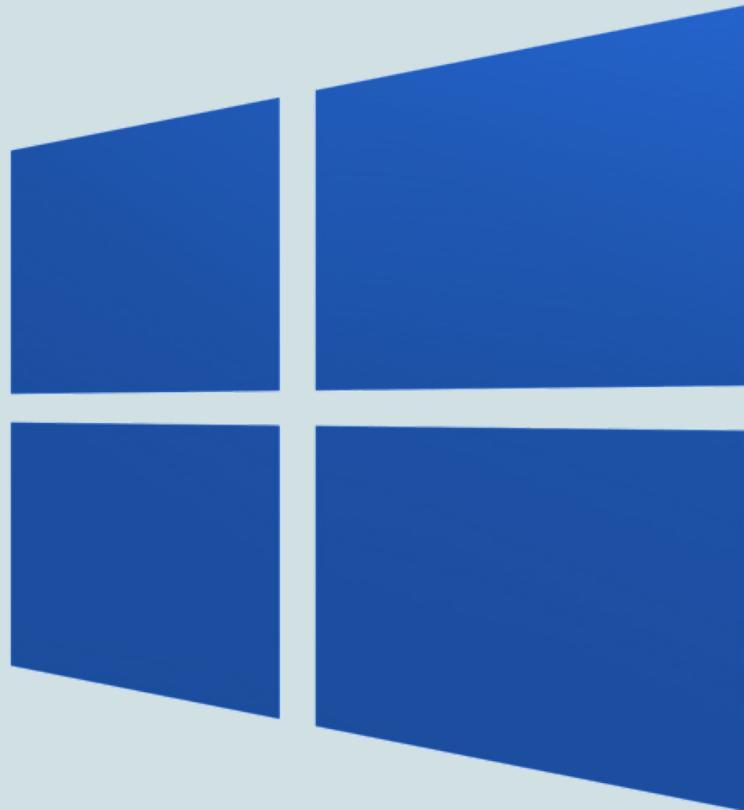


# **TÍTULO: Administración de redes en Windows 10 en una máquina virtual**

**UNIDAD: 6**

**CICLO FORMATIVO Y MÓDULO: DAW Sistemas Informáticos**



<u>DESCRIPCIÓN DE LA TAREA</u>	<u>3</u>
<u>ACTIVIDAD 1</u>	<u>4</u>
<u>ACTIVIDAD 2</u>	<u>7</u>
<u>ACTIVIDAD 3</u>	<u>9</u>
<u>ACTIVIDAD 4</u>	<u>11</u>
<u>ACTIVIDAD 5</u>	<u>16</u>
<u>ACTIVIDAD 6</u>	<u>18</u>
<u>ACTIVIDAD 7</u>	<u>21</u>
<u>ACTIVIDAD 8</u>	<u>27</u>

## **DESCRIPCIÓN DE LA TAREA**

### **Caso práctico**

*María y Juan ya han terminado de administrar el sistema operativo instalado de los equipos del Auditorio pero les falta configurarlos para que estén conectados a la red. Como siempre, Ada será la que les dé el visto bueno.*

### **¿Qué te pedimos que hagas?**

*Realiza las siguientes actividades en tu equipo o máquina virtual utilizando Windows 10 u 11. El equipo o máquina virtual debe contener dos adaptadores de red: uno de tipo Ethernet y el otro inalámbrico para conexiones a redes WIFI.*

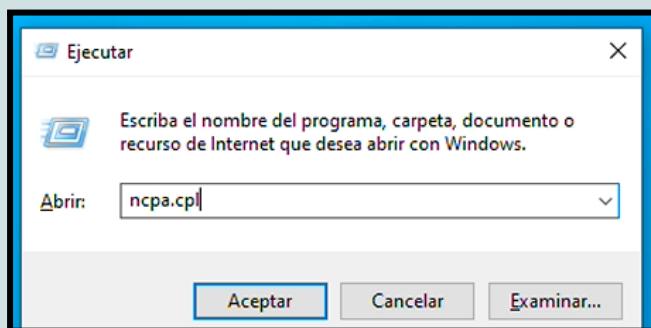
---

## ACTIVIDAD 1

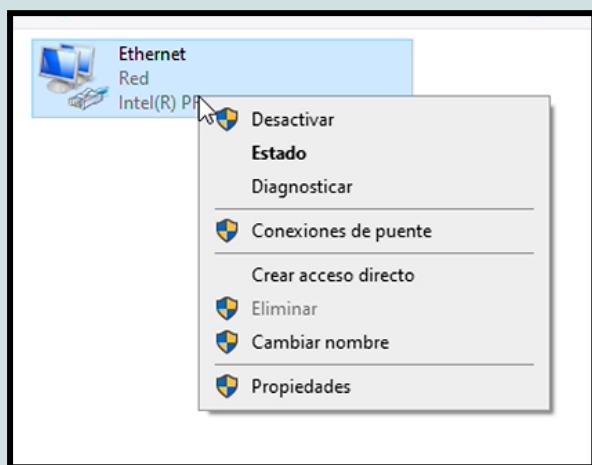
Configura la conexión de la tarjeta de red Ethernet con los siguientes datos:

- Dirección IP: 192.168.18.20
- Máscara de red: 255.255.255.0
- Puerta de enlace: 192.168.18.1
- DNS: 8.8.8.8
- DNS: 8.8.4.4

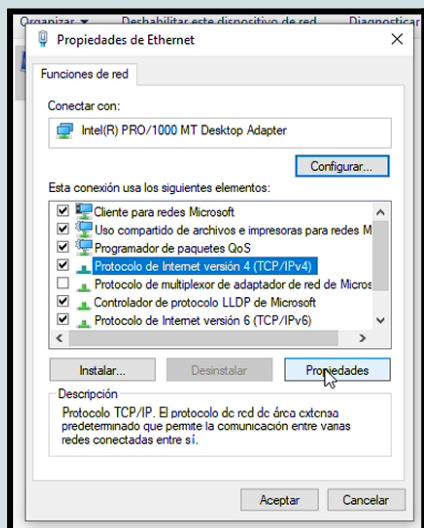
Para empezar, desde el inicio pulsamos **Windows+R** para abrir el “**Símbolo del Sistema**” y escribiremos el comando “**ncpa.cpl**”.



Con esto se nos abre la ventana de **Conexiones de Red**, en el ícono del **Ethernet** haremos clic derecho sobre ella y seleccionaremos **Propiedades**.



*En las propiedades de Ethernet seleccionamos **Protocolo de Internet versión 4 (TCP/IPv4)** y damos a **Propiedades**.*



Aquí deberemos introducir las siguientes direcciones en el orden siguiente:

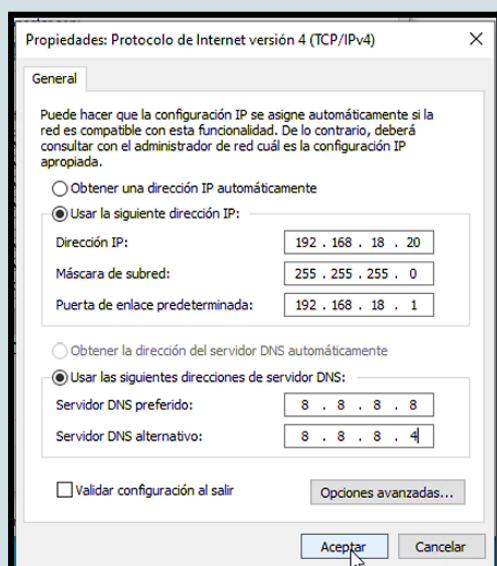
**Usar la siguiente dirección IP:**

1. **Dirección IP:** 192.168.18.20
2. **Máscara de subred:** 255.255.255.0 (esta se completa sola)
3. **Puerta de enlace predeterminada:** 192.168.18.1

**Usar las siguientes direcciones de servidor DNS:**

1. **Servidor DNS preferido:** 8.8.8.8
2. **Servidor DNS alternativo:** 8.8.4.4

Luego guardamos y aplicamos los cambios, debe quedar así:



\*Yo por si acaso le dí a validar la configuración al salir pero hice la captura de antes. Una vez hecho esto abrimos el cmd para verificar que se han guardado los cambios. Para ello usaremos el comando **ipconfig /all**.

Como se puede ver se han aplicado bien los cambios. Pero para el siguiente ejercicio es mejor devolverlo a como estaba ya que la IP proporcionada no existe, así que volvemos a la configuración de Ethernet y seleccionamos la opción de obtener las direcciones automáticamente.

## ACTIVIDAD 2

Configura la conexión inalámbrica para conectarse a la red con SSID "TAREA\_6", que da los valores de conexión por servidor DHCP y cuya clave de acceso WPA o WPA2 es "SistemasInformaticos". En ocasiones el servidor DHCP no funciona adecuadamente y tenemos que utilizar los siguientes valores de configuración alternativos, pero sólo cuando el servidor DHCP no funcione correctamente:

- Dirección IP: 192.168.18.220
- Máscara de red: 255.255.255.0
- Puerta de enlace: 192.168.18.1
- DNS: 8.8.8.8

Para este ejercicio he tenido que crear la red WiFi en mi host para que la máquina virtual lo detecte y pueda conectarse, para ello vamos a las **configuraciones del host** y de ahí a la opción **Red e Internet**.

Donde dice **zona de cobertura inalámbrica** editamos el **nombre** y la **contraseña** de la red como pide la actividad quedando así:



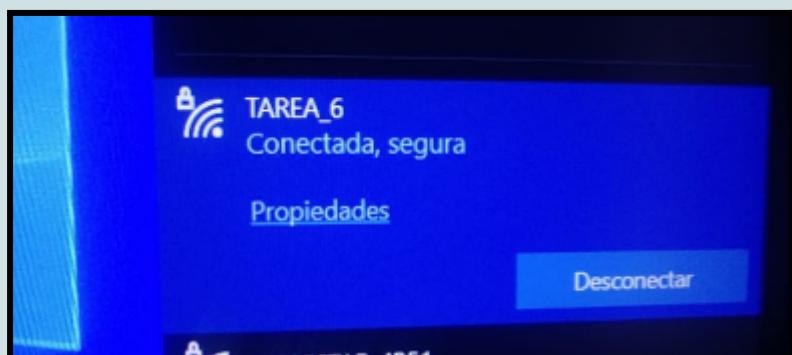
Ahora vamos a la máquina virtual y antes de abrirla vamos a **Configuración ⇒ Redes** para asegurarnos de que detecte la red **TAREA\_6**.



*En caso de que no funcionase el servidor **DHCP** podríamos hacerlo utilizando los siguientes valores en la cmd. A mí me funcionó pero de todos modos lo comprobé:*

```
VINCULOS. DIRECCION IPv4 LOCAL: . . . . . 192.168.18.220(PREFERIDA)
Dirección IPv4. . . . . : 192.168.18.220(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . : 192.168.18.1
IAID DHCPv6 . . . . . : 412633127
DUID de cliente DHCPv6. . . . . : 00-01-00-01-27-E2-AD-71-F
Servidores DNS. . . . . : 8.8.8.8
                                         8.8.4.4
NetBIOS sobre TCP/IP. . . . . : habilitado
```

*\*Como me dejó de funcionar la opción de capturar pantalla por algún motivo que no entiendo le hice una foto con mi móvil a la red no sea que se fuese en algún momento y luego no la cogiese otra vez.*



## ACTIVIDAD 3

**Ejecuta e interpreta la salida de la ejecución de los siguientes comandos:**

- Hostname
  - Ipconfig
  - nslookup <nombre\_dominio>
  - ping <dirección\_ip>
  - tracert <dirección\_ip>

Donde <dirección\_ip> debe ser la misma en los apartados D y E, y <nombre\_dominio> en C debe ser un nombre de dominio cualquiera de un sitio web.

Para esta actividad de nuevo accederemos al **cmd** y ejecutaremos uno por uno los siguientes comandos:

1. **hostname** ⇒ muestra el nombre del equipo

```
C:\Users\VMRidaoChaves>hostname  
DESKTOP-0LEE0QQ
```

2. ***Ipcconfig*** ⇒ muestra la configuración de red del equipo

3. ***nslookup*** ⇒ traduce un dominio a una dirección IP (yo lo hice con la página [XtraLife](#))

```
C:\Users\VMRidaooChaves>nslookup xtralife.com
Servidor: 254.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.254

Respuesta no autoritativa:
Nombre: xtralife.com
Addresses: 3.160.231.18
            3.160.231.7
            3.160.231.44
            3.160.231.103
```

4. ***ping*** ⇒ verifica la conectividad con una IP (de nuevo usando la misma página)

```
C:\Users\VMRidaooChaves>ping xtralife.com

Haciendo ping a xtralife.com [3.160.231.7] con 32 bytes de datos:
Respuesta desde 3.160.231.7: bytes=32 tiempo=11ms TTL=247
Respuesta desde 3.160.231.7: bytes=32 tiempo=14ms TTL=247
Respuesta desde 3.160.231.7: bytes=32 tiempo=12ms TTL=247
Respuesta desde 3.160.231.7: bytes=32 tiempo=48ms TTL=247

Estadísticas de ping para 3.160.231.7:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 11ms, Máximo = 48ms, Media = 21ms
```

5. ***tracert*** ⇒ muestra la ruta que siguen los paquetes hasta llegar a la IP

```
C:\Users\VMRidaooChaves>tracert xtralife.com

Traza a la dirección xtralife.com [3.160.231.7]
sobre un máximo de 30 saltos:

 1  3 ms    3 ms    2 ms  192.168.1.1
 2  5 ms    5 ms    8 ms  192.168.144.1
 3  7 ms    8 ms    5 ms  189.red-81-41-225.staticip.rima-tde.net [81.41.225.189]
 4  15 ms   17 ms   13 ms  22.red-81-41-226.staticip.rima-tde.net [81.41.226.22]
 5  12 ms   13 ms   13 ms  189.red-80-58-106.staticip.rima-tde.net [80.58.106.189]
 6  16 ms   14 ms   12 ms  be1-400-grtmadre2.net.telefonicaglobalsolutions.com [216.184.113.184]
 7  *        *        *      Tiempo de espera agotado para esta solicitud.
 8  *        *        *      Tiempo de espera agotado para esta solicitud.
```

## ACTIVIDAD 4

Instala y configura un servidor FTP con el servicio de FTP que suministra Windows (con autenticación básica y permitiendo SSL).

Para el cliente utiliza el programa "Filezilla". El nombre del sitio FTP será "Auditorio\_< inicial de tu nombre y primer apellido >".

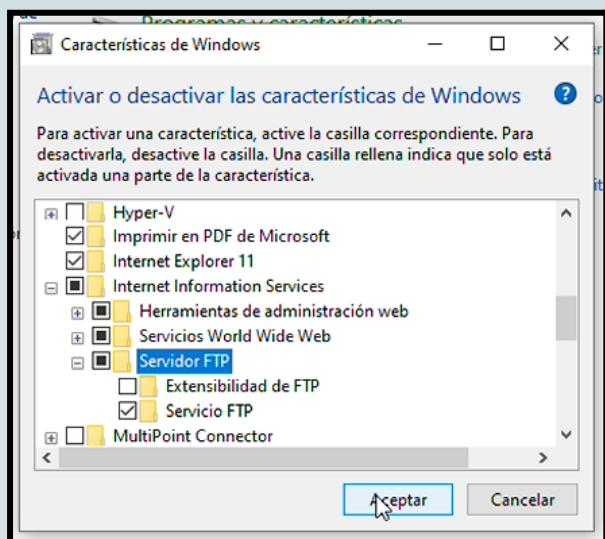
Por ejemplo, para un alumno llamado Pablo Rodríguez Campos, el nombre de su sitio FTP será "Auditorio\_prodriguez".

Debes entregar una captura de pantalla del administrador del servicio FTP donde se vea claramente el nombre de tu sitio FTP y otra captura de una conexión de un cliente (utilizando, por ejemplo, la herramienta Filezilla) en la que haya existido transferencia de archivos (en ambos sentidos, cliente-servidor y servidor-cliente).

Para habilitar los **FTP** pulsamos **Windows + R** y escribimos **optionalfeatures**.

Esto nos llevará a la ventana de “**Características de Windows**” y marcaremos las siguientes opciones:

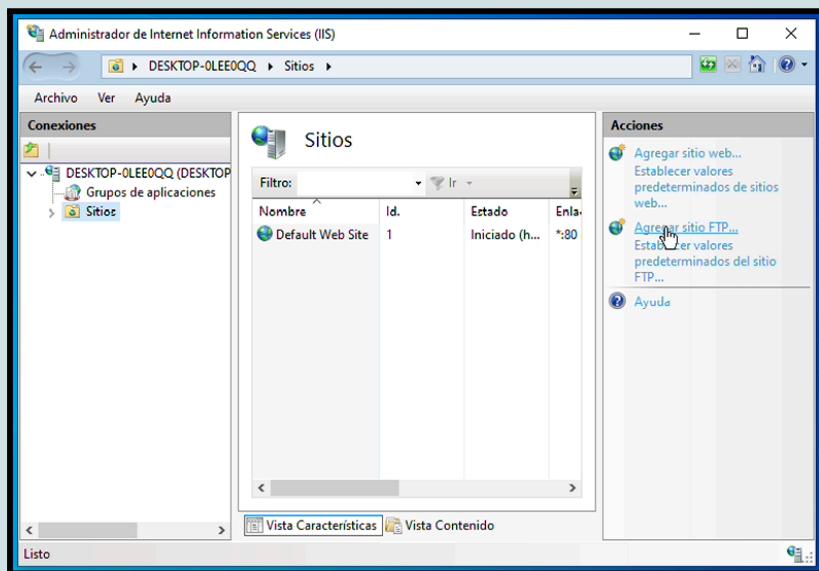
- **Servidor FTP**
- **Extensibilidad de FTP**
- **Herramientas de administración web**



Una vez seleccionados aceptamos y esperamos a que se instalen.

Cuando esté listo configuraremos el servidor FTP.

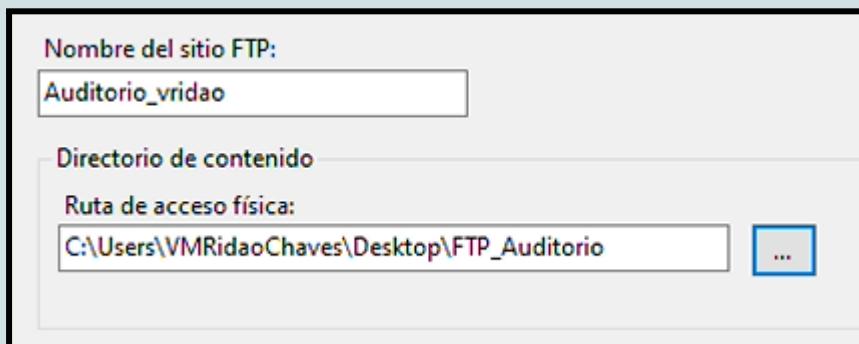
Para ello abriremos el **Administrador de Internet Information Services (IIS)**.



Hacemos clic en la carpeta **Sitios** y a la derecha en **Acciones** le damos a **Agregar sitio FTP**.

Nos pedirá que le demos un nombre de dominio que será: **Auditorio\_vridao**.

En la ruta de acceso física creé la carpeta **FTP\_Auditorio** en el escritorio para tenerla a la vista.

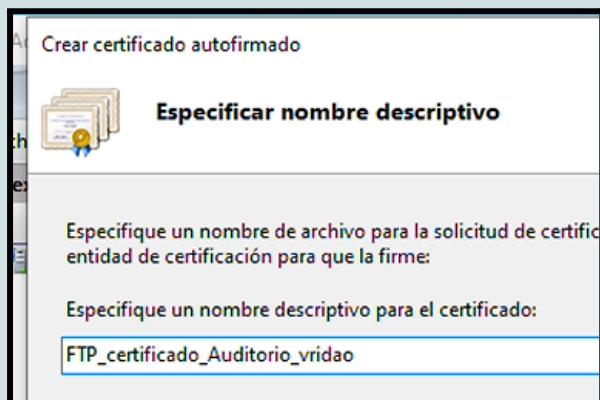


Ahora para configurar la conexión puse la siguiente dirección y puerto de mi FTP.

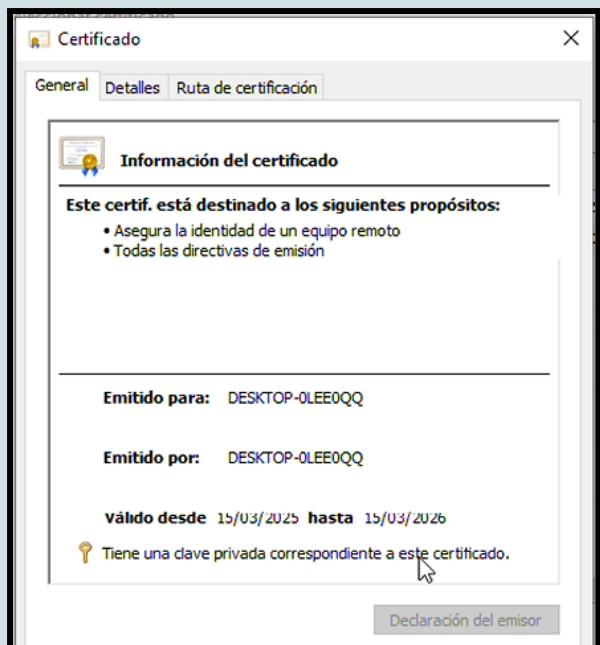
Tipo	Nombre de host	Puerto	Dirección IP	Información de ...
ftp		21	192.168.1.80	

Ya por último para habilitar el **SSL básico** cree un **certificado autofirmado** para la actividad.

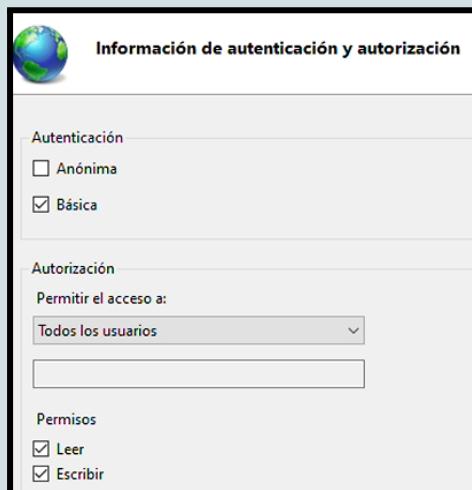
Este certificado se puede sacar en la misma pestaña y te sirve durante un año.



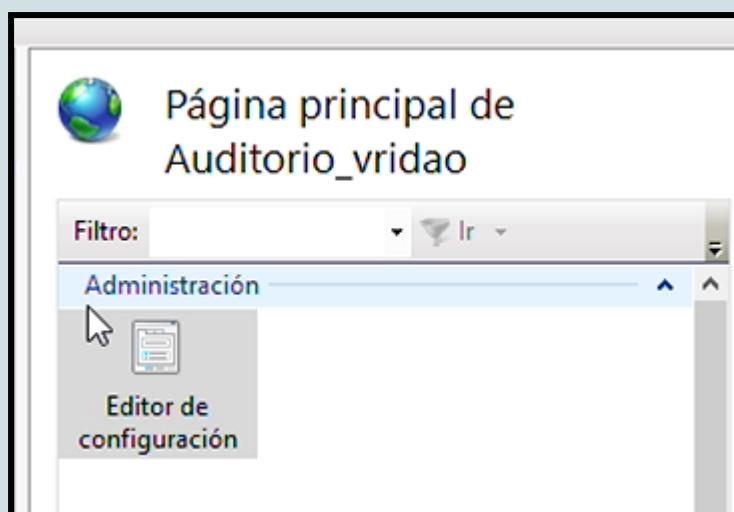
Así aparecería al final.



Por último en las **reglas de autorización FTP** en Permitir Usuarios específicos yo puse todos los usuarios y en los permisos lo dejé en Lectura y Escritura.

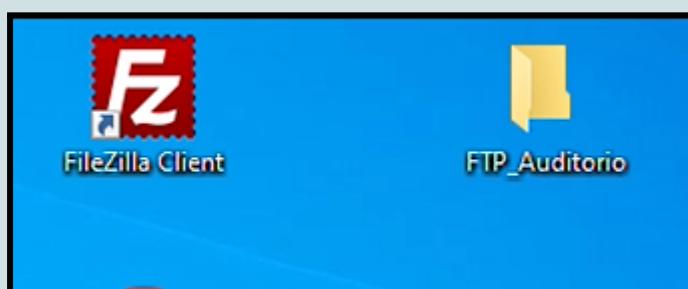


Así aparecería una vez hecho todo:

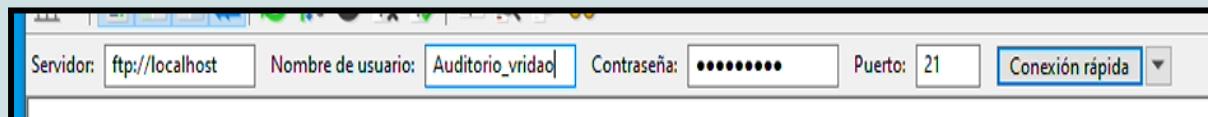


Ahora descargamos el programa **FileZilla Client** para poder realizar una conexión.

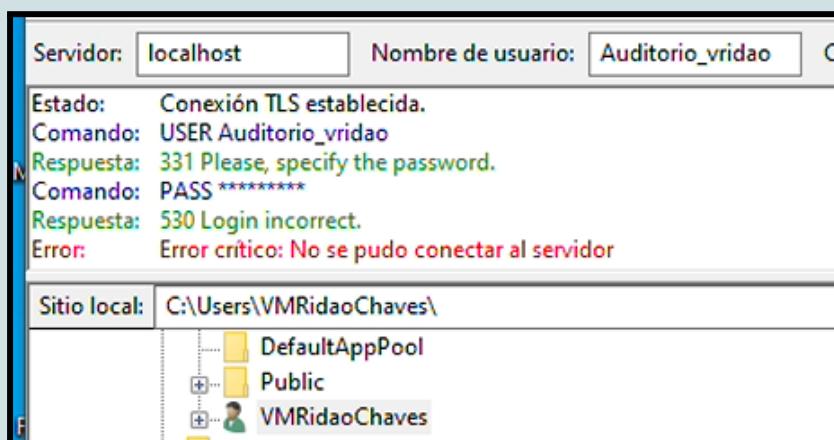
Me ahorraré la explicación para no saturar el documento y adjuntaré una captura con el ícono del programa.



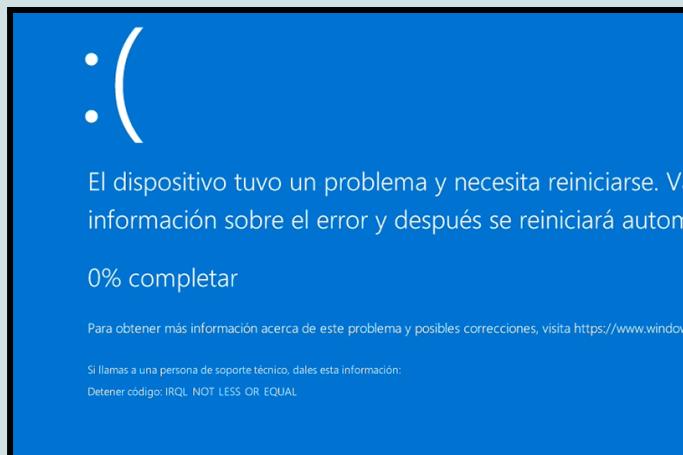
Abrimos FileZilla y en la parte superior rellenamos los campos con los siguientes datos:



A partir de aquí o no me salía nada o me decía que la contraseña era incorrecta.



Lo seguí intentando varias veces pero a la cuarta vez bueno...



Me pasó una vez más y preferí dejarlo así que hasta aquí llegué.

## ACTIVIDAD 5

Instala y configura un servidor web en tu equipo con XAMPP. Una vez activados los servicios, en la carpeta pública del servidor Apache, guarda un archivo llamado mipagina.html con el siguiente código:

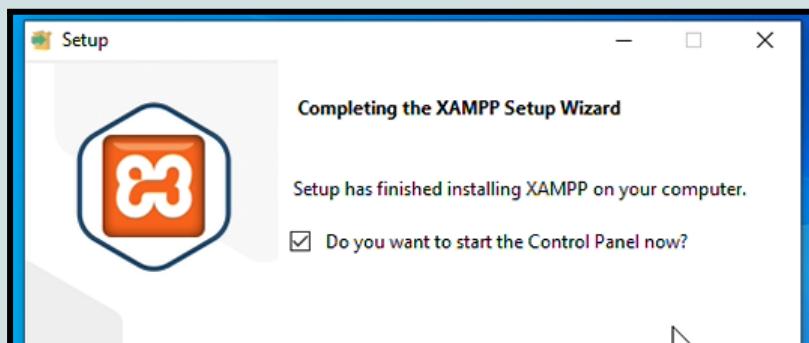
```
<html>
    <head>
        <title>Sistemas Informáticos DAM/DAW – Tarea 6</title>
    </head>
    <body>
        <h1>Esto es una página de prueba en código html</h1>
        Realizado por – Tu Nombre y Apellidos -
        Creado el día - dd mmm aaaa -
        
        <h1> Curso 20xx/xx </h1>
    </body>
</html>
```

Para ello, abre un editor simple de texto, copia las líneas de html personalizándolo con tu nombre y referenciando la imagen correctamente, Por último guarda el archivo como "mipagina.html" y añade a la carpeta pública del servidor una foto tuya de tamaño carnet para que se visualice al abrir la página.

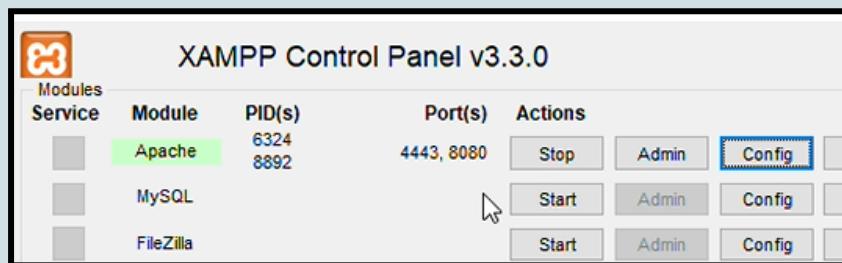
A continuación, realiza una captura de pantalla del navegador accediendo a esta

URL: "<http://localhost/mipagina.html>"

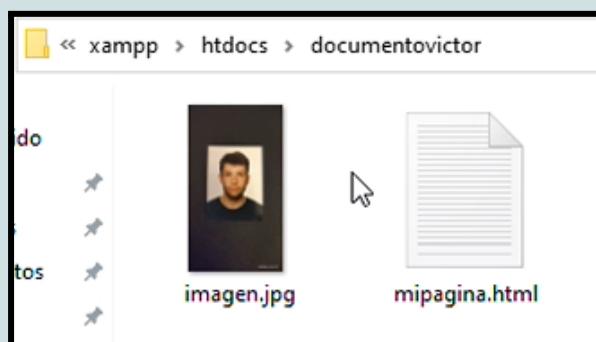
Para este ejercicio comenzaremos descargando el programa **XAMPP** de su página oficial.



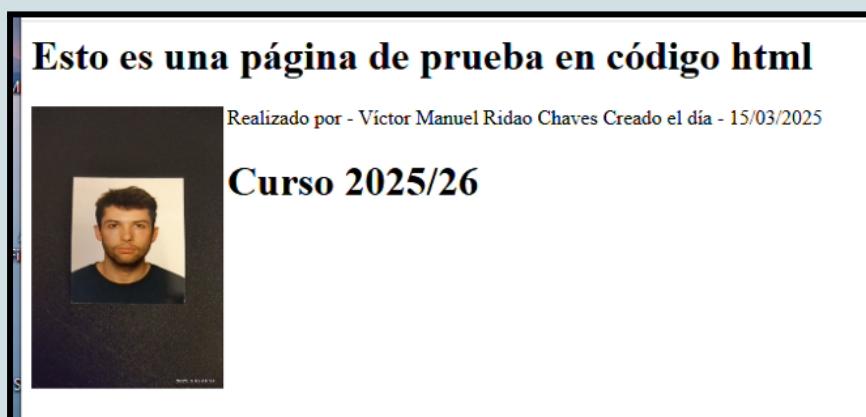
Una vez abierto, en el panel de control le damos a **Start** a la derecha de **Apache** para que se inicie el servidor web. Tiene que ponerse en verde indicando que el servidor está en funcionamiento.



Ahora en la carpeta de **XAMPP** en el disco C: buscamos la carpeta **htdocs** donde guardaremos el archivo **html** junto con la foto.



Ahora que ya está dentro de la carpeta iremos al buscador y abriremos el documento de modo que aparezca así:

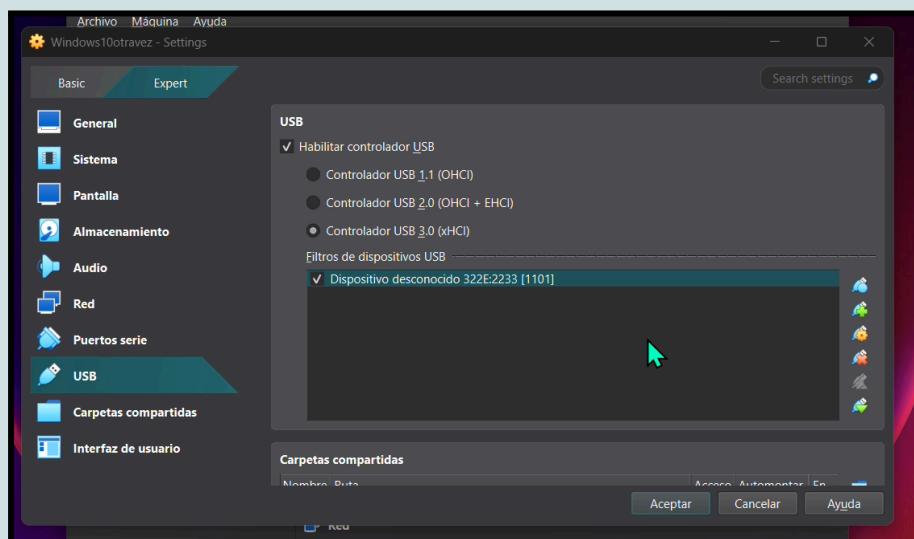


## ACTIVIDAD 6

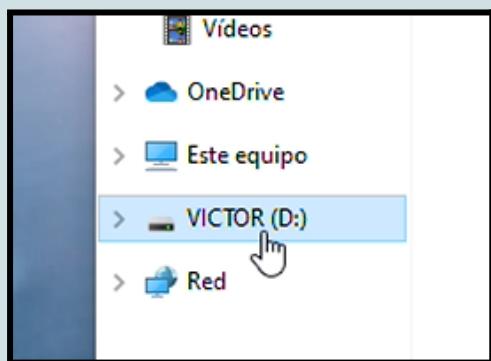
Utilizando un antivirus, realiza lo siguiente:

- Analiza una unidad extraíble que tengas conectada al ordenador y muestra una captura de pantalla del proceso y otra del resultado del análisis. ¿Se ha detectado alguna amenaza? En caso afirmativo, ¿de qué tipo? ¿Qué acciones has tomado (eliminar, ignorar alerta, poner en cuarentena el archivo)? Razona tu respuesta.

Para empezar, la máquina virtual no detectará el USB a menos que se cambie desde las configuraciones en la parte de USB, hay que señalar qué dispositivo queremos que detecte. Una vez hecho eso ya podemos continuar.

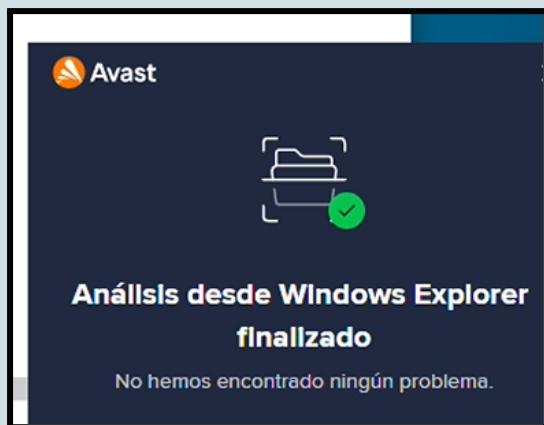


Ahora lo detectará.



Para realizar el análisis hay que **hacer clic derecho** sobre el **USB** y en el desplegable ir donde dice “**analizar los elementos seleccionados**”, esto hará que Avast lo analice y nos diga si ha encontrado algún problema.

En mi caso no fue así.

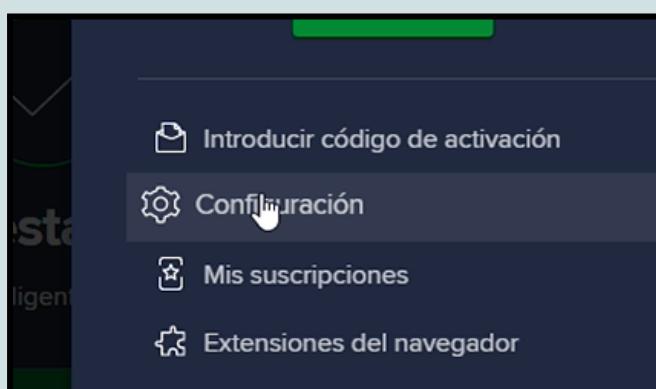


Por defecto tenemos Windows Defender pero por si acaso descargué Avast porque es el que tengo en mi ordenador personal y me va bien.

Es verdad que aunque no detectó ninguna amenaza, en caso de haber encontrado un **WispRider** que son los virus que suelen pasar a través de USBs, lo habría intentado solucionar o si acaso borrar todos los archivos de la unidad y hacer una limpieza total. Si ni eso fuera suficiente supongo que lo desecharía y compraría otra, qué remedio.

**b) Configura un análisis programado para que se ejecute semanalmente a las 6:00 horas y revise todas las unidades de disco y la memoria. Nombra la tarea como 'ANÁLISIS SEMANAL - <tu nombre completo y apellidos>'. Muestra una captura de pantalla de la configuración de la programación.**

Para realizar esta parte, de nuevo abrimos el antivirus y nos desplazamos al menú de la parte derecha y en el desplegable le damos a **Configuración**.

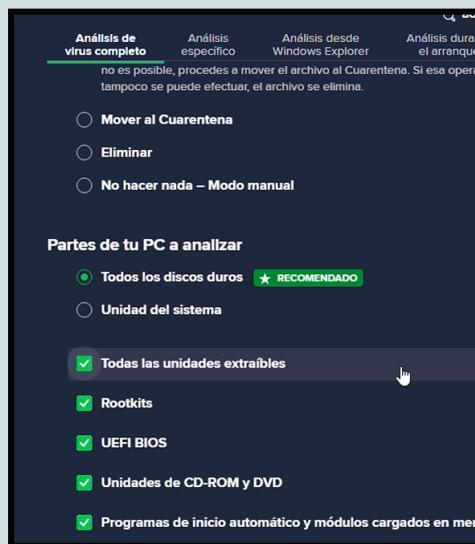


Ahí, en la parte de **Protección** ⇒ **Análisis Inteligente** podemos establecer un horario para analizar el equipo.



Quedará establecido con frecuencia semanal, los domingos y que se inicie a las 06:00 horas.

Ya por último podemos establecer que realice un análisis completo de todos los archivos y discos duros del sistema, pero deberemos declararlo nosotros de forma manual.



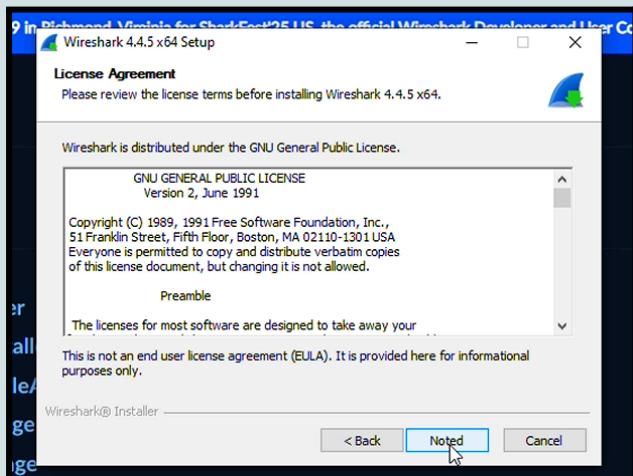
Intenté buscar dónde se podía nombrar la tarea pero parece que Avast no permite personalizar a ese nivel, igualmente queda declarado con las imágenes que se ha establecido el análisis.

## ACTIVIDAD 7

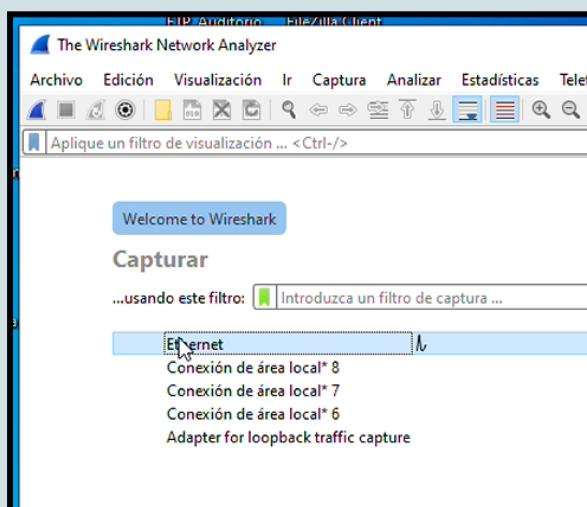
- **Captura de tráfico DNS**

1. Instala e inicia Wireshark y comienza una captura de tráfico en tu red.

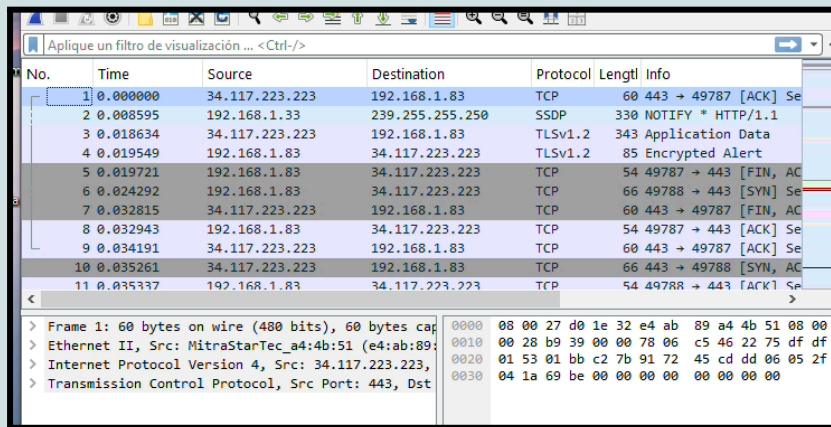
Para empezar descargamos **Wireshark** de la página:



Una vez descargado accedemos a su **panel de control**, nos aparecerán diferentes interfaces de red, tanto WiFi como Ethernet, la idea es señalar que sea la de **Ethernet**:



*Esto es la línea de tráfico de la red Ethernet que aparece a la derecha:*



## 2. Abre una terminal (CMD o PowerShell) y ejecuta el siguiente comando: [nslookup www.google.com](http://www.google.com)

Ahora nos dirigimos al **cmd** y escribimos el comando [nslookup www.google.com](http://www.google.com).

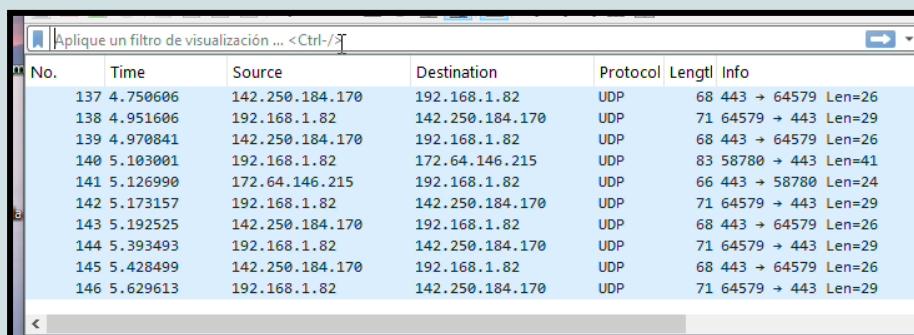
```
C:\Users\VMRidaoChaves>nslookup www.google.com
Servidor: 254.red-80-58-61.staticip.rima-tde.net
Address: 80.58.61.254

Respueta no autoritativa:
Nombre: www.google.com
Addresses: 2a00:1450:4003:80a::2004
           172.217.17.4

InC:\Users\VMRidaoChaves>
```

## 3. Detén la captura y utiliza el filtro dns en Wireshark.

**Sin filtro DNS:**



**Con filtro DNS:**

No.	Time	Source	Destination	Protocol	Length	Info
40	2.419885	192.168.1.82	80.58.61.254	DNS	75	Standard query 0x9fe0
41	2.420191	192.168.1.82	80.58.61.254	DNS	75	Standard query 0x3587
50	2.475072	192.168.1.83	80.58.61.254	DNS	86	Standard query 0x4047
51	2.566250	80.58.61.254	192.168.1.83	DNS	319	Standard query response
61	2.584216	192.168.1.82	80.58.61.250	DNS	75	Standard query 0x11e3
62	2.584478	192.168.1.82	80.58.61.250	DNS	75	Standard query 0x1339
64	2.595573	80.58.61.250	192.168.1.82	DNS	317	Standard query response
66	2.598759	80.58.61.250	192.168.1.82	DNS	476	Standard query response

#### 4. Identifica la consulta DNS enviada y la respuesta recibida.

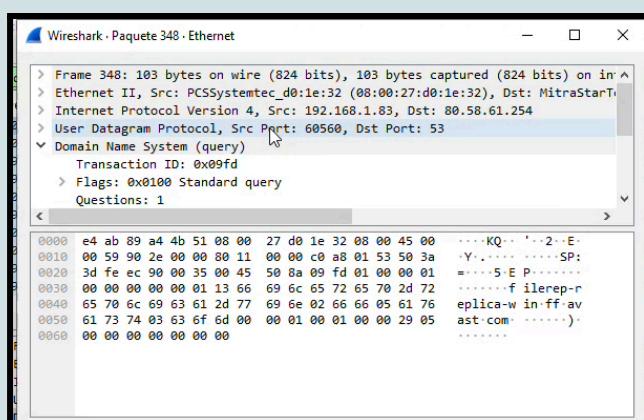
**Consulta DNS:**

80.58.61.254	DNS	103 Standard query 0x7d7
80.58.61.254	DNS	103 Standard query 0x2b5
192.168.1.83	DNS	161 Standard query response
192.168.1.83	DNS	210 Standard query response

**Respuesta recibida:**

```
> Internet Protocol Version 4, Src: 192.168.1.82, Dst: 80.58.61.254
> User Datagram Protocol, Src Port: 62490, Dst Port: 53
> Domain Name System (query)
```

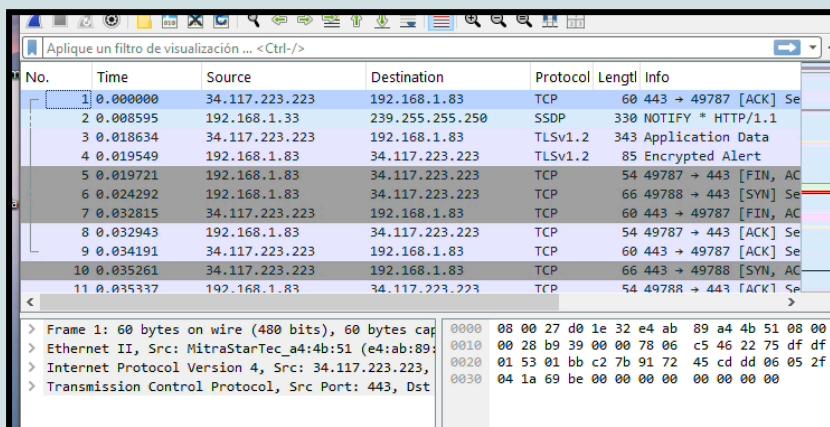
#### 5. Captura una imagen del paquete DNS y explica su contenido.



Este paquete tiene información como el tipo de consulta, el nombre del dominio solicitado y la dirección IP.

- Comparación de tráfico HTTP vs. HTTPS
1. Repite el proceso de captura en Wireshark.

*Reiniciamos Wireshark y comenzamos el proceso de captura:*



2. Accede a un sitio web sin cifrado (como <http://neverssl.com>) y luego a un sitio cifrado (como <https://www.google.com>).

#### SITIO WEB SIN CIFRADO:

**What?**  
This website is for when you try to open Facebook, Google, Amazon, etc on a wifi network, and nothing happens. Type "http://neverssl.com" into your browser's url bar, and you'll be able to log on.

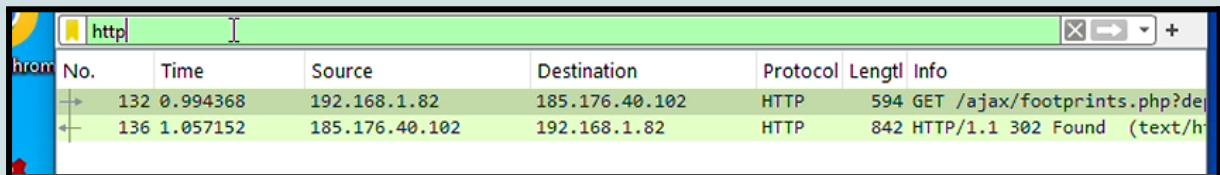
**How?**  
neverssl.com will never use SSL (also known as TLS). No encryption, no strong authenticator, no HSTS, no HTTP/2.0, just plain old unencrypted HTTP and forever stuck in the dark ages of internet security.

**Why?**  
Normally, that's a bad idea. You should always use SSL and secure encryption when possible. In fact, it's such a bad idea that most websites are now using https by default.  
neverssl.com's great selling point is that it's a public service that makes it impossible for those WiFi networks to be hacked online. Secure servers and websites use https make it impossible for those WiFi networks to send you to a login or payment page. Basically, those networks can't tap into your connection just like attackers can't. Modern browsers are so good that they can remember when a website supports encryption and even if you type in the website name, they'll use https.  
And if the network never redirects you to this page, well as you can see, you're not missing much.

#### SITIO WEB CON CIFRADO:

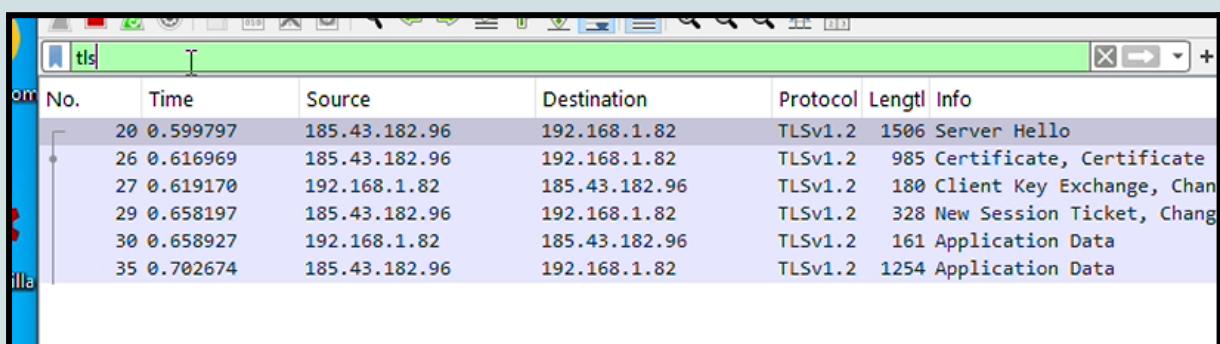
### 3. Detén la captura y filtra por “http” y “tls” en Wireshark.

**FILTRO http:**



No.	Time	Source	Destination	Protocol	Length	Info
132	0.994368	192.168.1.82	185.176.40.102	HTTP	594	GET /ajax/footprints.php?de
136	1.057152	185.176.40.102	192.168.1.82	HTTP	842	HTTP/1.1 302 Found (text/html)

**FILTRO tls:**



No.	Time	Source	Destination	Protocol	Length	Info
20	0.599797	185.43.182.96	192.168.1.82	TLSv1.2	1506	Server Hello
26	0.616969	185.43.182.96	192.168.1.82	TLSv1.2	985	Certificate, Certificate
27	0.619170	192.168.1.82	185.43.182.96	TLSv1.2	180	Client Key Exchange, Chan
29	0.658197	185.43.182.96	192.168.1.82	TLSv1.2	328	New Session Ticket, Chang
30	0.658927	192.168.1.82	185.43.182.96	TLSv1.2	161	Application Data
35	0.702674	185.43.182.96	192.168.1.82	TLSv1.2	1254	Application Data

### 4. Explica las diferencias entre los paquetes capturados en HTTP y HTTPS.

- Los paquetes capturados en *http* son **no cifrados**, lo que significa que todo se envía en texto claro.
- Los paquetes capturados en *https* están **cifrados**, con cabeceras privadas y los datos serán ilegibles.

## Análisis de cabeceras HTTPS

1. Encuentra un paquete HTTP GET en Wireshark y analiza las cabeceras que envían un texto claro.

Cogeremos la primera opción que aparece:

Protocol	Length	Info
HTTP	594	GET /ajax/foo
HTTP	842	HTTP/1.1 302
HTTP	594	GET /ajax/foo
HTTP	841	HTTP/1.1 302

Al hacer clic sobre ella nos aparece la siguiente información:

```
> GET /ajax/footprints.php?deptid=0&r=hphps%3
Host: livechat2.supportindeed.com\r\n
Connection: keep-alive\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
Accept: image/avif,image/webp,image/apng,image/*,*/*;q=0.9
Referer: http://pagina-web.com/
Accept-Encoding: gzip, deflate\r\n
Accept-Language: es-ES,es;q=0.9\r\n
<
0000 e4 ab 89 a4 4b 51 08 00 27 d0 1e 32 08 00
```

- **User-Agent:** informa sobre el navegador (Mozilla)
- **Referer:** la página de donde proviene la solicitud.
- **Cookies:** datos que contienen la información del usuario.

2. Explica cómo estas cabeceras pueden exponer información y como HTTPS protege contra ello.

- Las cabeceras HTTP al no estar cifradas permiten que se exponga todo tipo de información sensible de los usuarios, además de que es visible en textos claros lo cual permite a los atacantes actuar con mayor facilidad.
- Por el contrario las HTTPS como sí cifran todo el tráfico incluidas las cabeceras no le será fácil para los atacantes robar datos de los usuarios.

## ACTIVIDAD 8

**Accede a un punto de acceso o router inalámbrico y muestra con capturas de pantalla cómo se realizarán las siguientes operaciones:**

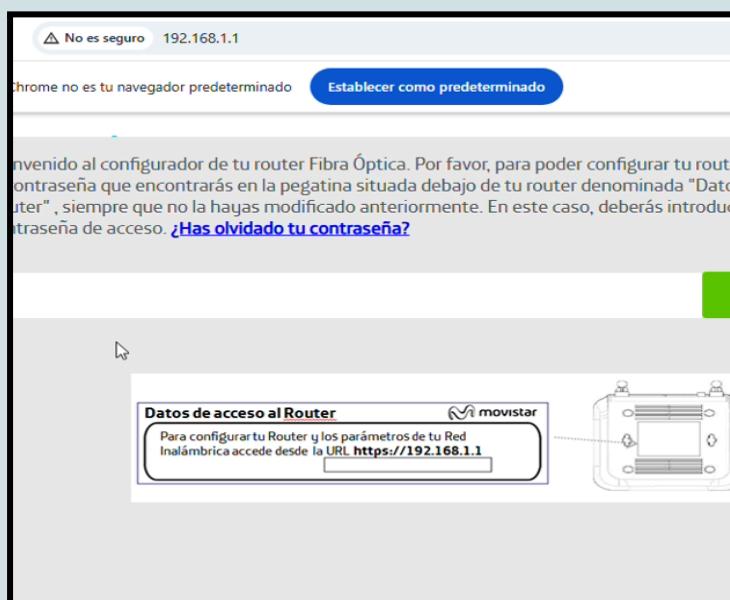
## **1. Configuración de la clave del router.**

Para ello deberemos conocer la dirección IP del router. En caso de no saberla podemos irnos al **cmd** y escribir el comando **ipconfig** y nos aparecerá la información.

*En este caso sería: **192.168.1.1***

**2. Configuración de la clave de red. Si aún no dispones de clave, establecela.**

*Para hacer esto nos dirigimos al buscador y ponemos la clave de **Puerta de enlace**.*



Para acceder necesitaremos la contraseña del router, se encuentra en la parte inferior del router justo encima del código de barras por lo menos en mi caso. Con esta clave ya podremos acceder a la configuración.

The screenshot shows a 'WiFi' configuration interface. It includes fields for the network name ('Nombre WiFi') set to 'MOVISTAR\_4B51', visibility ('Ocultar nombre WiFi') set to 'No', and a password field ('Clave WiFi') containing several dots. There is also a note about entering letters, numbers, and characters.

### 3. Configuración del tipo de cifrado. Cambia el cifrado a WPA2 si no lo tienes así.

The screenshot shows a dropdown menu for 'Tipo de cifrado' (Encryption type) with 'WPA2-PSK' selected.

Se encontraba así por defecto.

### 4. Activa el cifrado MAC para los equipos de tu red, averiguando sus direcciones MAC y añade además esta MAC ficticia: "DC:0A:B3:1B:7E:C0". Acompaña las capturas con los comentarios descriptivos necesarios.

Esto último no me dejó hacerlo, no parecía darme opción a hacerlo desde la máquina me decía que lo hiciese desde el móvil.

The screenshot shows a 'Filtrado MAC' (MAC Filtering) configuration page. It includes a note about a mobile app for filtering, and a large 'Aplicar cambios' (Apply changes) button.

Y con esto último quedaría el trabajo terminado.

