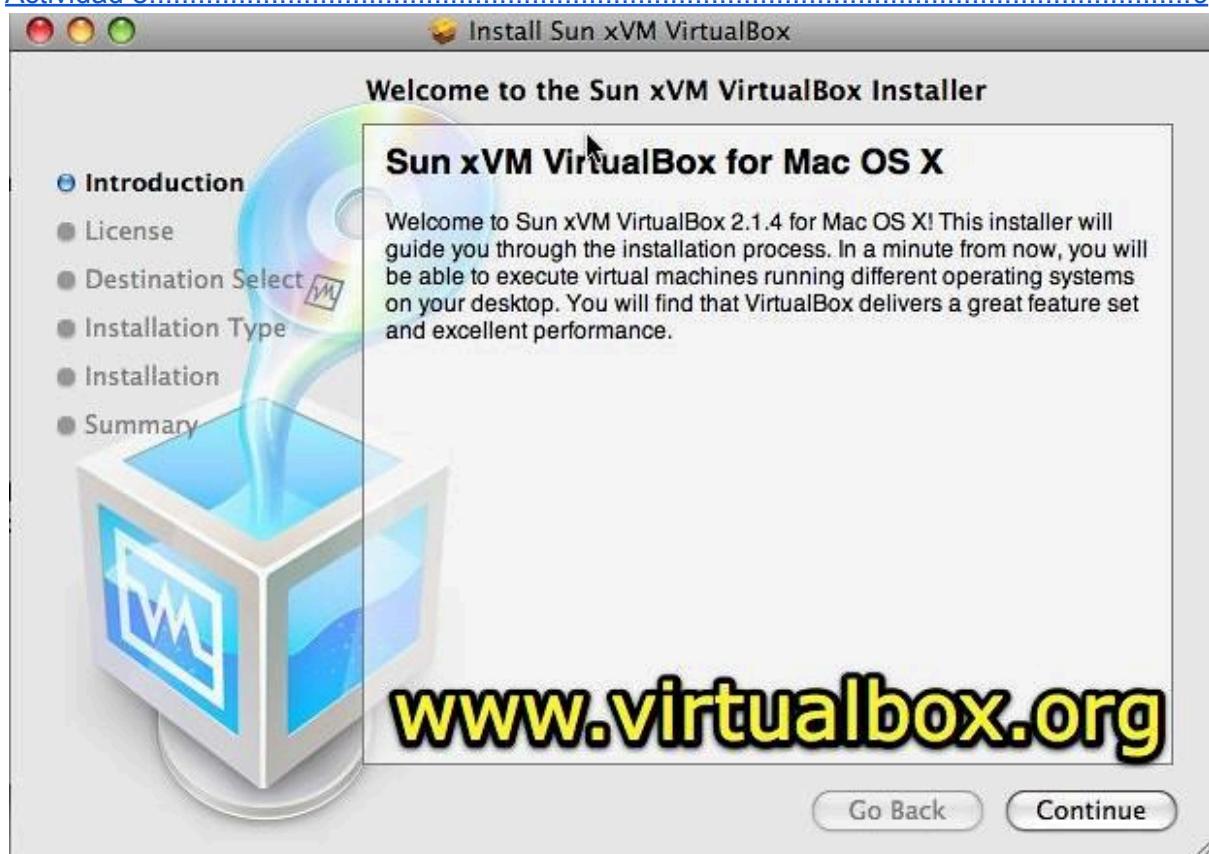


# Sistemas Informáticos – Tarea 06

---

<a href="#">Actividad 1</a>	2
<a href="#">Actividad 2</a>	3
<a href="#">Actividad 3</a>	4
<a href="#">Actividad 4</a>	5
<a href="#">Actividad 5</a>	6
<a href="#">Actividad 6</a>	7
<a href="#">Actividad 7</a>	8
<a href="#">Actividad 8</a>	9



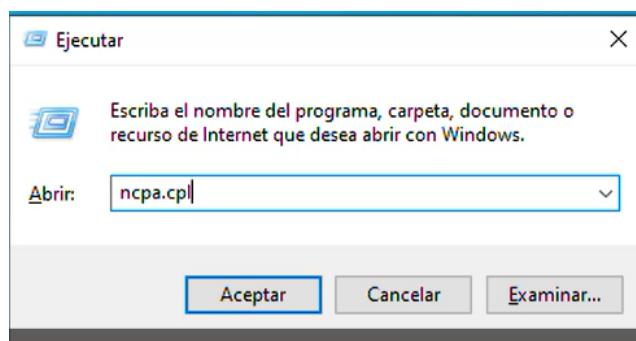
# Actividad 1.

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

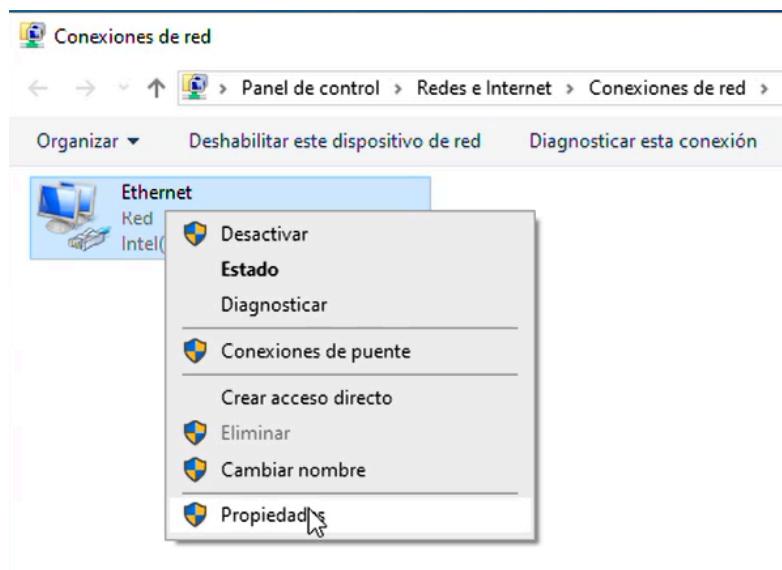
- Dirección IP: 192.168.18.20
- Máscara de red: 255.255.255.0
- Puerta de enlace: 192.168.18.1
- DNS: 8.8.8.8
- DNS: 8.8.4.4

## 1. Abrir la configuración de red

Pulsa **Win + R**, escribe **ncpa.cpl** y presiona **Enter**.

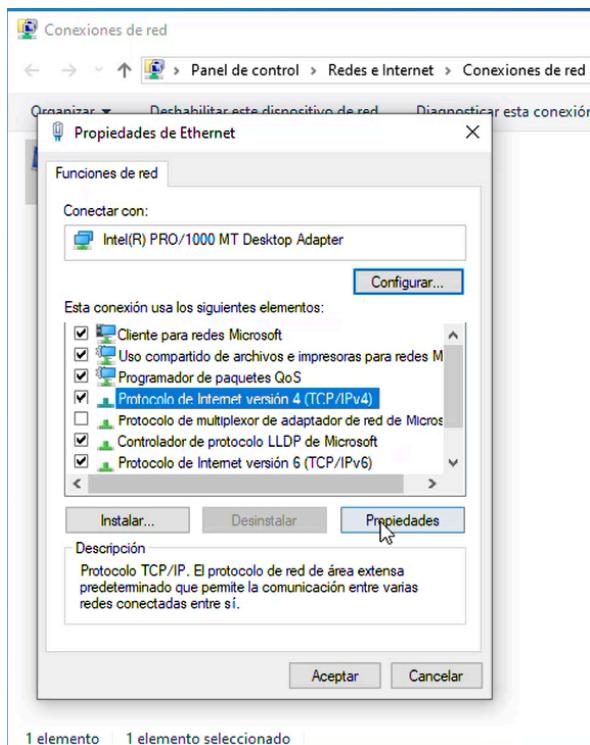


Esto abrirá la ventana de "Conexiones de red". Busca tu conexión de red Ethernet, haz clic derecho sobre ella y selecciona "**Propiedades**".



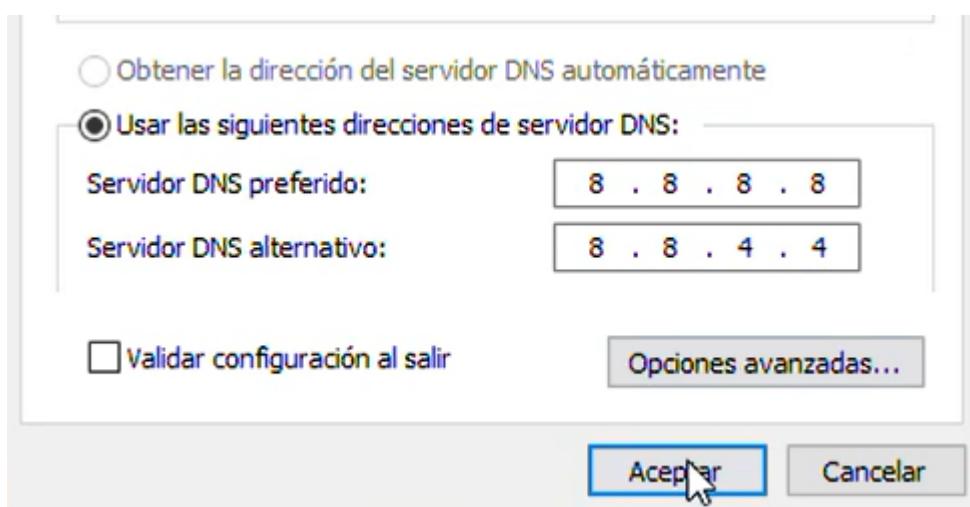
## 2. Configurar la dirección IP

En la lista, selecciona "**Protocolo de Internet versión 4 (TCP/IPv4)**" y haz clic en "**Propiedades**".



## 3. Configurar los servidores DNS

Marca "**Usar las siguientes direcciones de servidor DNS**" e introduce: **Servidor DNS preferido: 8.8.8.8** y **Servidor DNS alternativo: 8.8.4.4**



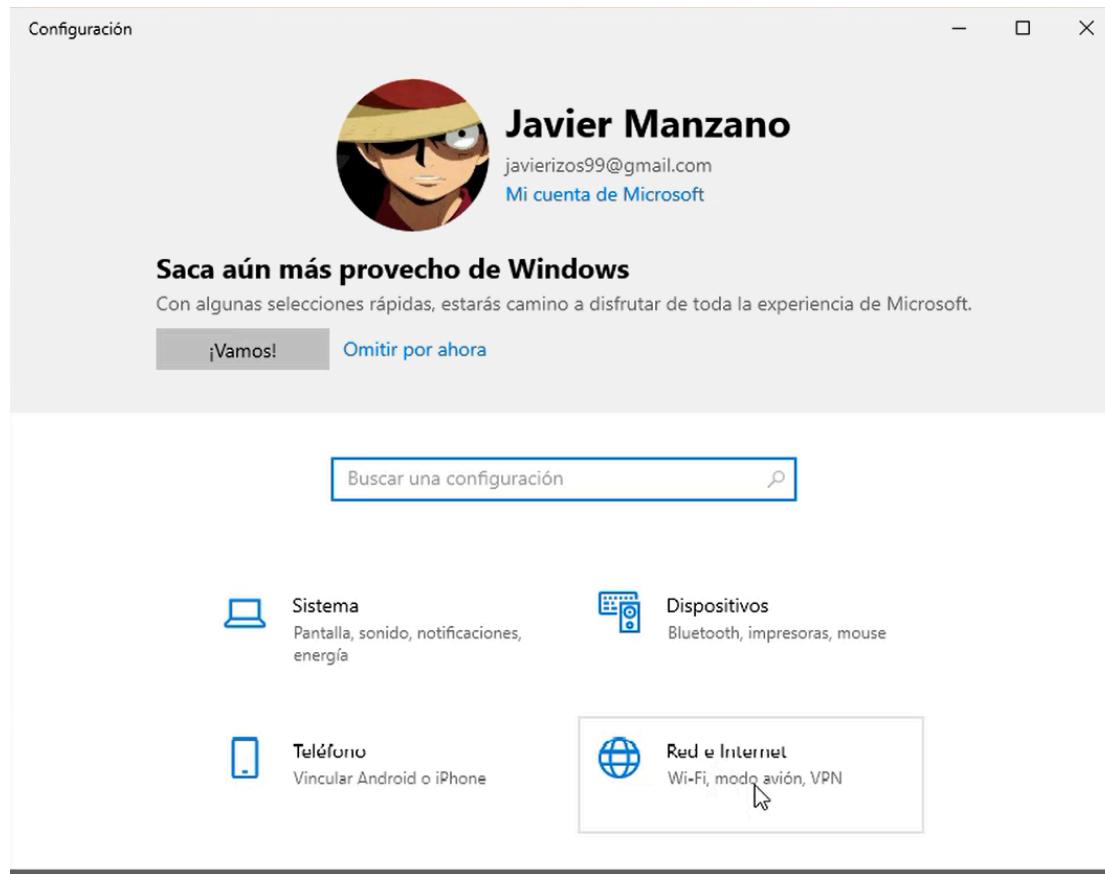
## Actividad 2.

**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:**

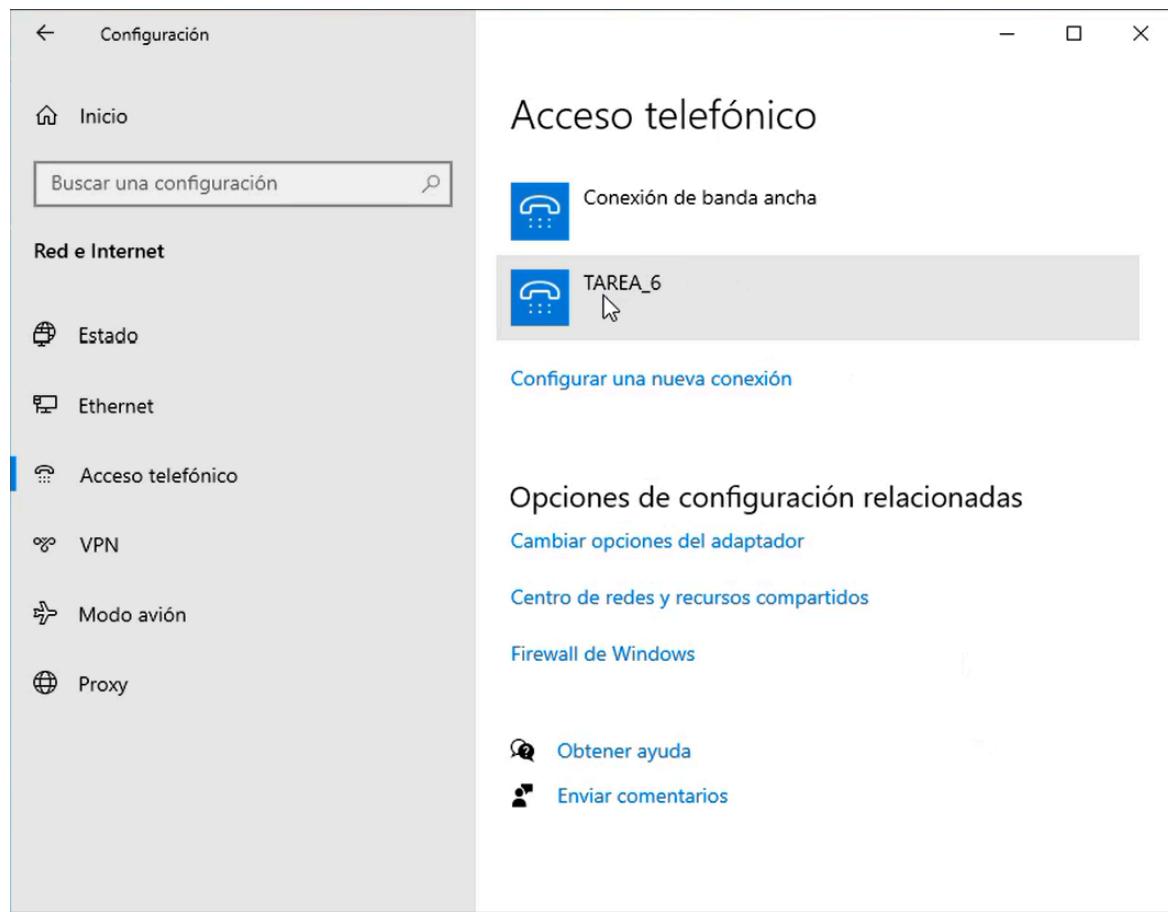
- Dirección IP: 192.168.18.220
- Máscara de red: 255.255.255.0
- Puerta de enlace: 192.168.18.1
- DNS: 8.8.8.8

### 1. Conectarse a la red Wi-Fi

Abre Configuración (**Win + I**) y ve a "Red e Internet".



Selecciona "Wi-Fi" en el menú de la izquierda. Haz clic en "**Mostrar redes disponibles**", selecciona la red "**TAREA\_6**" y pulsa "**Conectarse**".



# 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.

---

## 1. Abrir la terminal

Pulsa **Win + R**, escribe **cmd** y presiona **Enter**. Luego, ejecuta los siguientes comandos uno por uno y revisa la salida.

## 2. Ejecutar y analizar los comandos

### A) hostname

Este comando muestra el **nombre del equipo** en la red.

```
□ Símbolo del sistema
Microsoft Windows [Versión 10.0.19045.3803]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\javie>hostname
DESKTOP-VBGR567

C:\Users\javie>
```

**Interpretación:** Indica el nombre del equipo dentro de la red.

B) ipconfig

Muestra la configuración de red del equipo.

## **Interpretación:**

- **Dirección IPv4:** IP asignada al dispositivo.
  - **Máscara de subred:** Define el rango de IPs dentro de la misma red.
  - **Puerta de enlace:** Dirección del router o servidor de salida.

C) nslookup <nombre\_dominio>

Consulta los servidores DNS para obtener la IP de un dominio.

```
C:\Users\javie>nslookup google.com
Servidor:  dns.google
Address:  8.8.8.8

Respuesta no autoritativa:
Nombre:  google.com
Addresses:  2a00:1450:4003:803::200e
                        216.58.215.142
```

## **Interpretación:**

- **Servidor:** Indica el servidor DNS utilizado (en este caso, Google DNS 8.8.8.8).
  - **Addresses:** Muestra la IP del dominio [google.com](http://google.com).

#### D) `ping <dirección_ip>`

Envía paquetes de prueba a una IP para comprobar si responde.

```
C:\Users\javie>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=12ms TTL=255
Respuesta desde 8.8.8.8: bytes=32 tiempo=9ms TTL=255
Respuesta desde 8.8.8.8: bytes=32 tiempo=11ms TTL=255
Respuesta desde 8.8.8.8: bytes=32 tiempo=10ms TTL=255

Estadísticas de ping para 8.8.8.8:
  Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos).
Tiempos aproximados de ida y vuelta en milisegundos:
  Mínimo = 9ms, Máximo = 12ms, Media = 10ms

C:\Users\javie>_
```

Interpretación:

- **Si responde:** La IP es accesible y el tiempo indica la latencia en milisegundos.
- **Si falla:** Puede indicar que la IP no es accesible o que el firewall la bloquea.

#### E) `tracert <dirección_ip>`

Muestra la ruta que siguen los paquetes hasta la IP destino.

```
C:\Users\javie>tracert 8.8.8.8

Traza a la dirección dns.google [8.8.8.8]
sobre un máximo de 30 saltos:

 1      9 ms      9 ms     15 ms  dns.google [8.8.8.8]

Traza completa.
```

Interpretación:

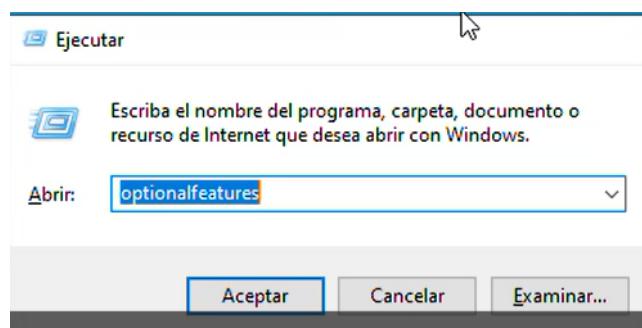
- Cada línea representa un "salto" entre servidores hasta llegar al destino.
- **Primer salto:** Router local (192.168.18.1).
- **Último salto:** Destino alcanzado (8.8.8.8).
- **Si hay un asterisco \* en la salida:** Puede indicar pérdida de paquetes o firewall bloqueando el tráfico.

# 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).**

## 1. Instalar el servidor FTP en Windows

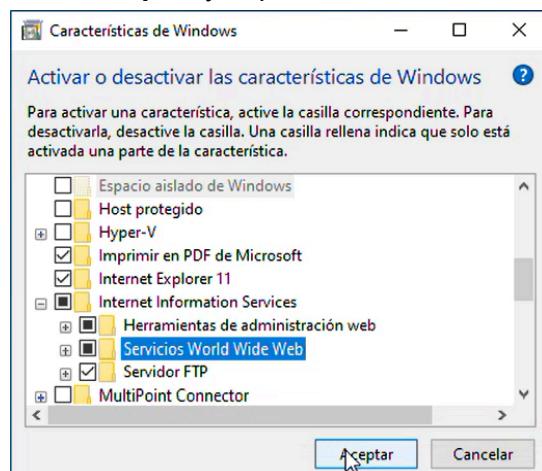
Abrir "Activar o desactivar características de Windows". Pulsa **Win + R**, escribe **optionalfeatures** y presiona **Enter**.



Busca "**Servicios de Internet Information Services (IIS)**" y expande la lista.  
Activa las siguientes opciones:

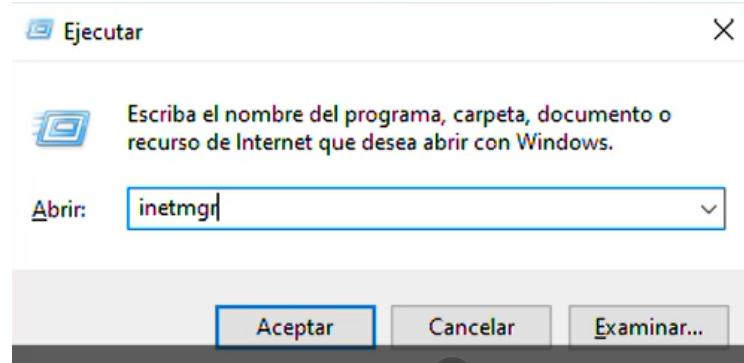
- Servidor FTP
- Extensibilidad de FTP
- Servicio de FTP

Pulsa **Aceptar** y espera la instalación.

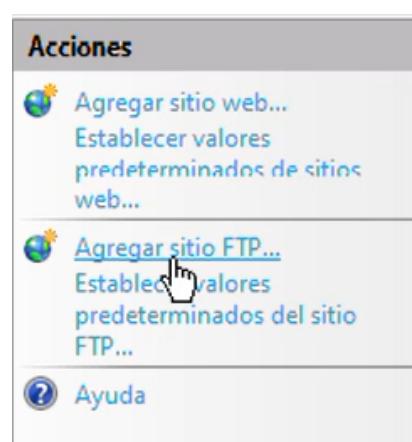
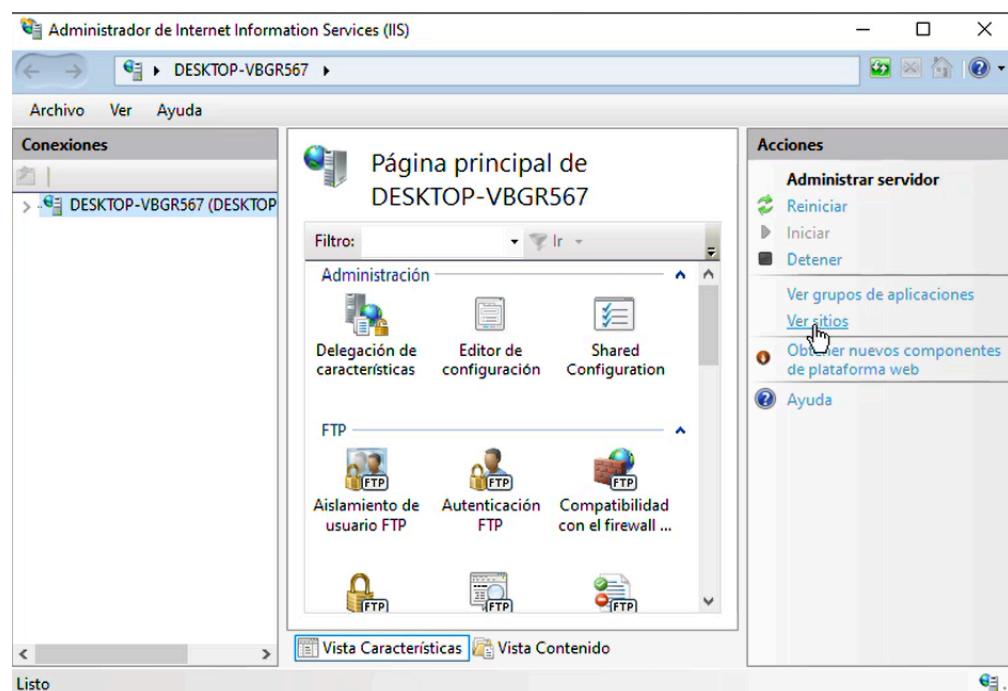


## 2. Crear y configurar el sitio FTP

Abrir el Administrador de IIS. Pulsa **Win + R**, escribe **inetmgr** y presiona **Enter**.

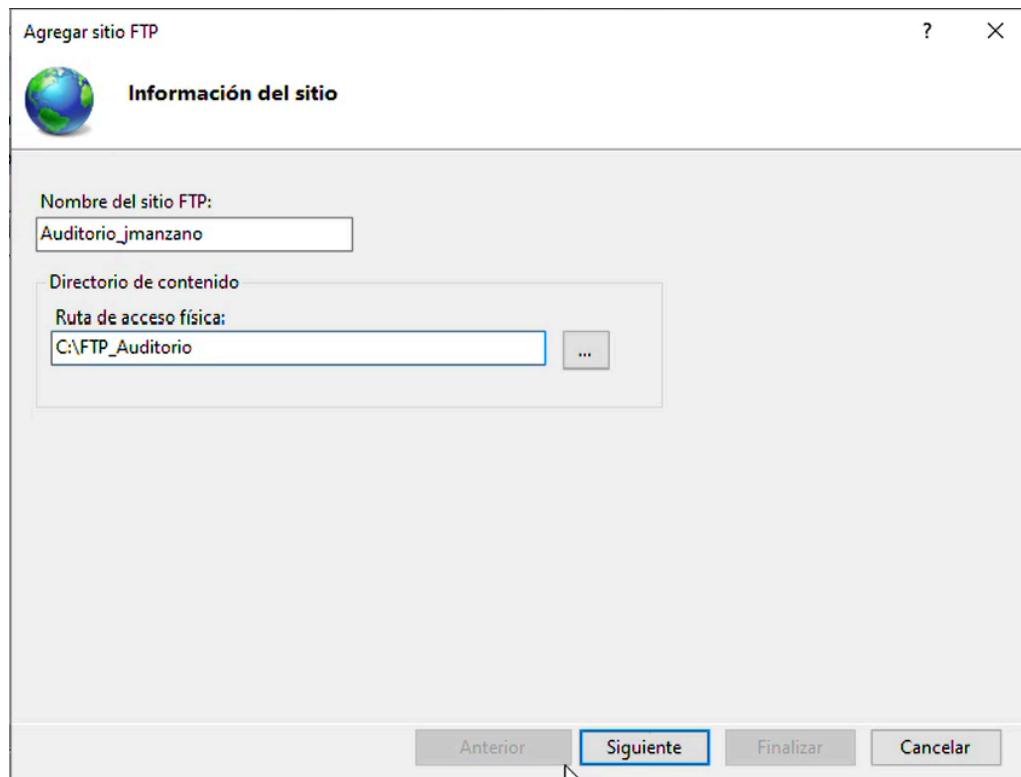


En el panel derecho, haz clic derecho en "**Sitios**" → "**Agregar sitio FTP...**".



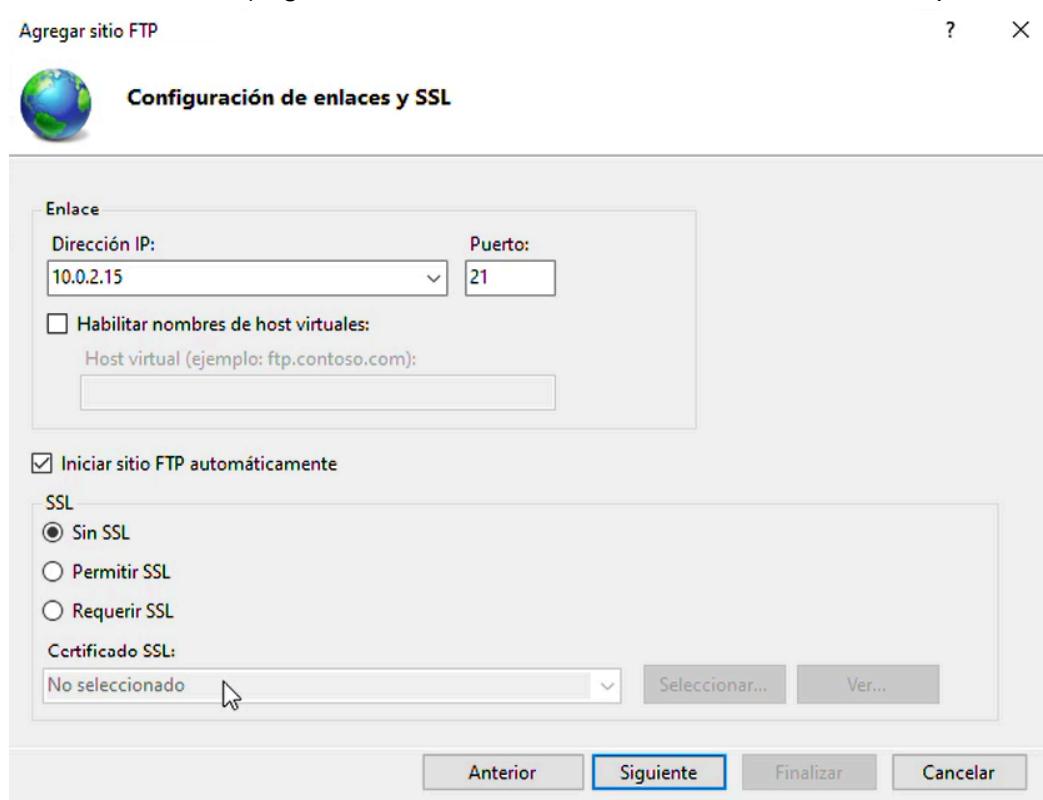
**Configura los datos del sitio: Nombre del sitio FTP: Auditorio\_jmanzano**

**Ruta física:** Crea una carpeta en **C:\FTP\_Auditorio** y selecciona esta ubicación.



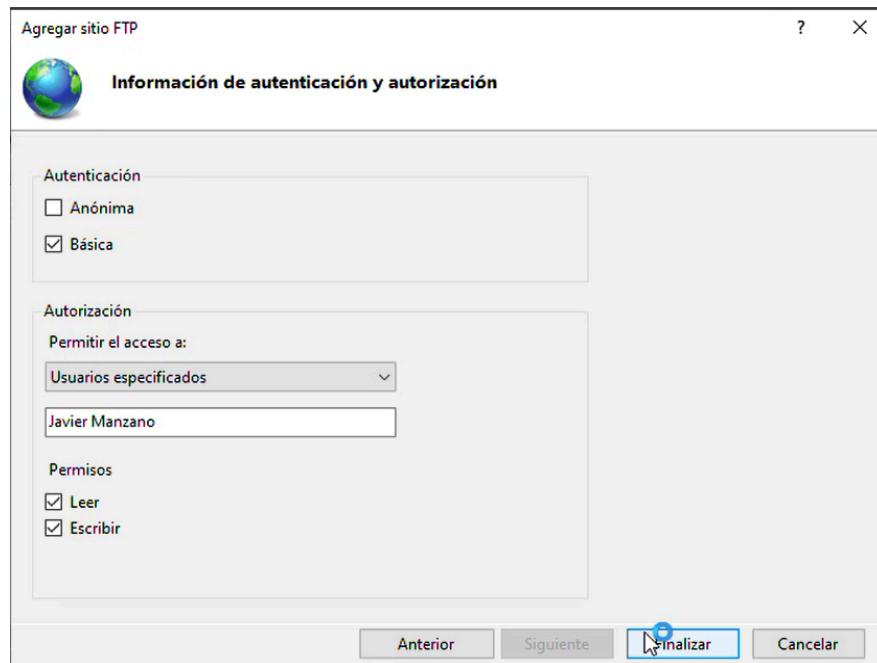
**IP:** **192.168.18.20** (o la IP de tu máquina).

**Habilitar SSL:**  (elige un certificado si tienes, o selecciona "Sin SSL" por ahora).



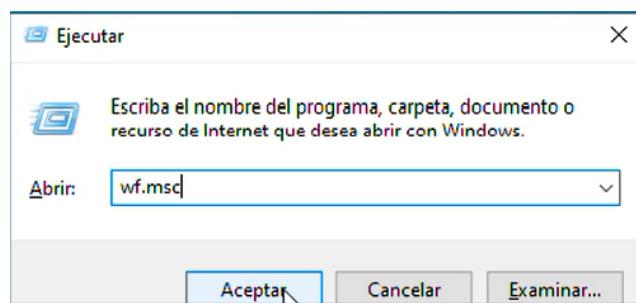
## Autenticación: Básica

**Autorización:** Selecciona "Usuarios específicos" e ingresa tu usuario de Windows. Activa permisos de **Lectura y Escritura**.

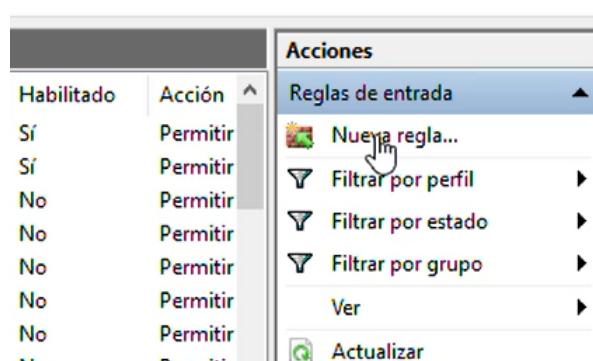
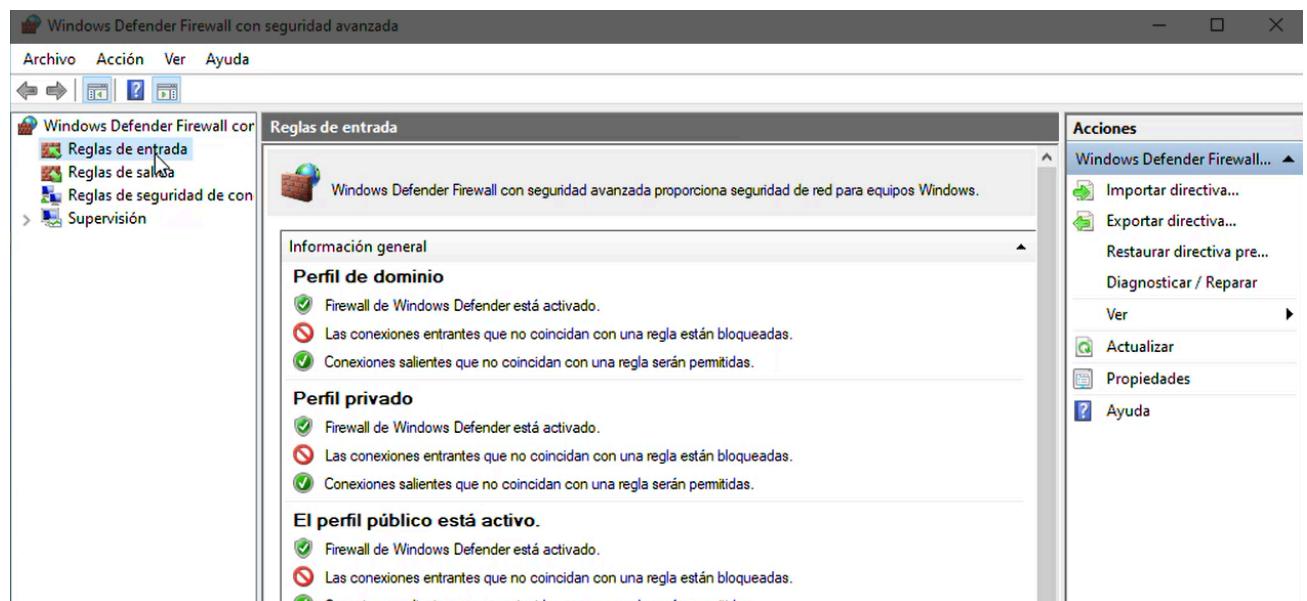


## 3. Configurar el Firewall para permitir conexiones FTP

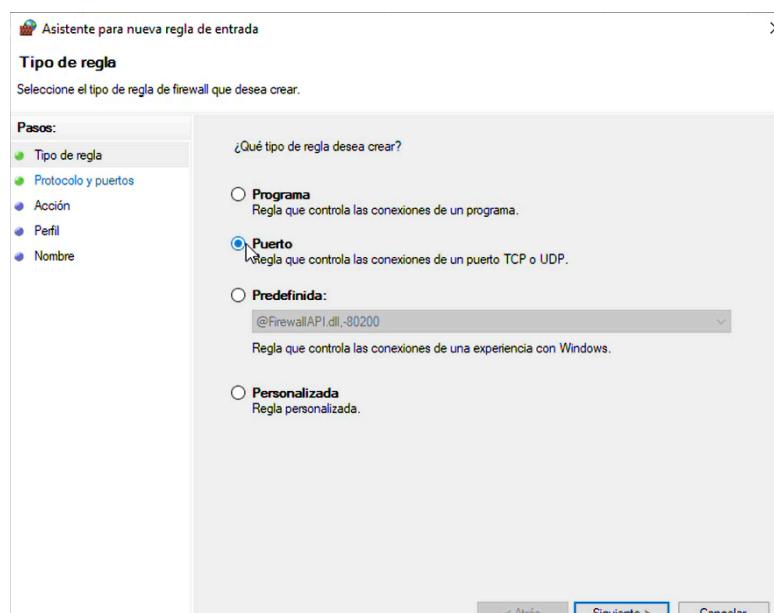
Pulsa **Win + R**, escribe **wf.msc** y presiona **Enter**.



En el panel izquierdo, selecciona **Reglas de entrada** → **Nueva regla**.



Selecciona **Puerto** → **TCP** e ingresa 21.



## Asistente para nueva regla de entrada

X

### Protocolo y puertos

Especifique los puertos y protocolos a los que se aplica esta regla.

#### Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

¿Se aplica esta regla a TCP o UDP?

- TCP  
 UDP

¿Se aplica esta regla a todos los puertos locales o a unos puertos locales específicos?

- Todos los puertos locales  
 Puertos locales específicos:

21

Ejemplo: 80, 443, 5000-5010

< Atrás

Siguiente >

Cancelar

## Asistente para nueva regla de entrada

X

### Nombre

Especifique el nombre y la descripción de esta regla.

#### Pasos:

- Tipo de regla
- Protocolo y puertos
- Acción
- Perfil
- Nombre

Nombre:

FTP\_Javier

Descripción (opcional):

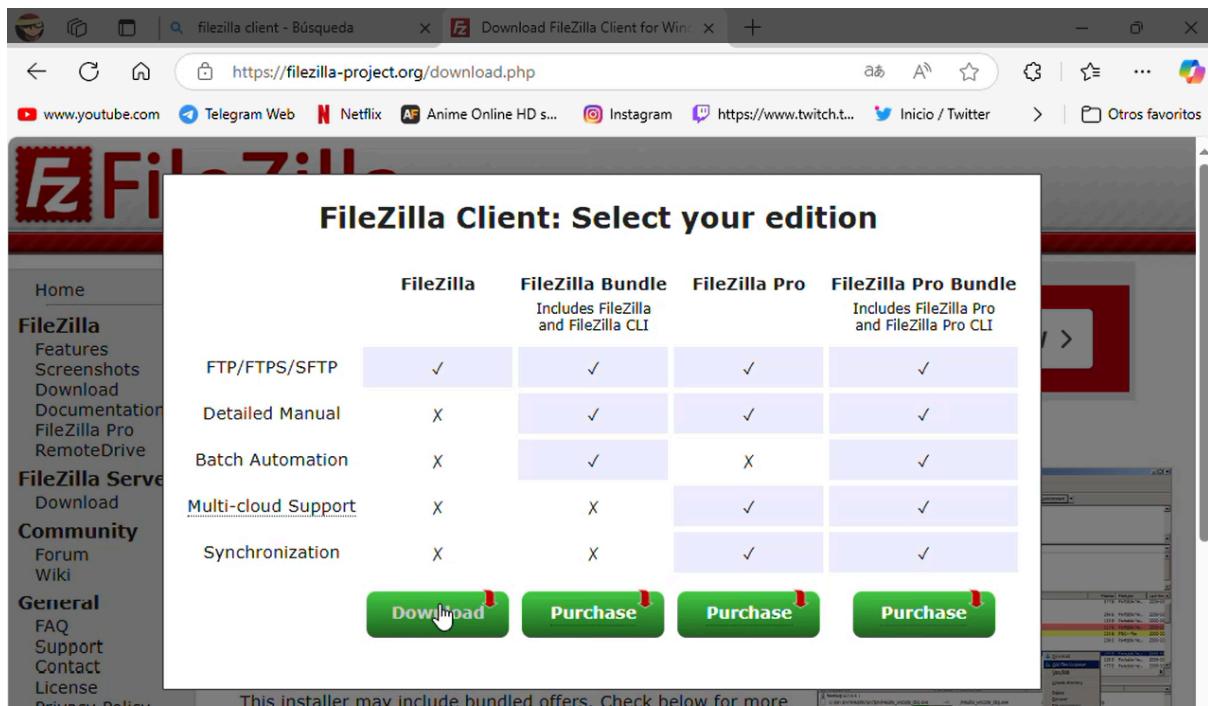
< Atrás

Finalizar

Cancelar

## 4. Conectar con FileZilla (Cliente FTP)

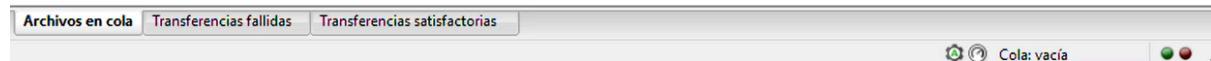
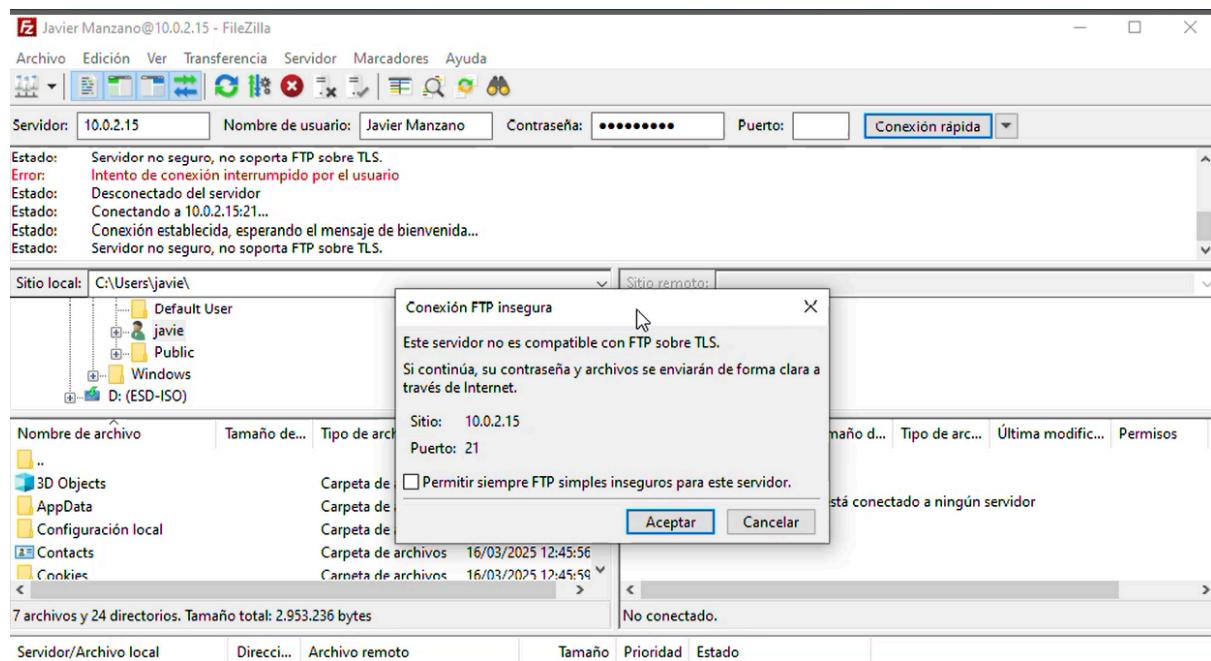
Descarga e instala [FileZilla Client](#).



Abre FileZilla y en la barra superior ingresa:

- **Servidor:** `ftp://192.168.18.20`
- **Usuario:** Tu usuario de Windows
- **Contraseña:** Tu contraseña de Windows
- **Puerto:** `21`

Pulsa **Conexión rápida**.



## 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>
```

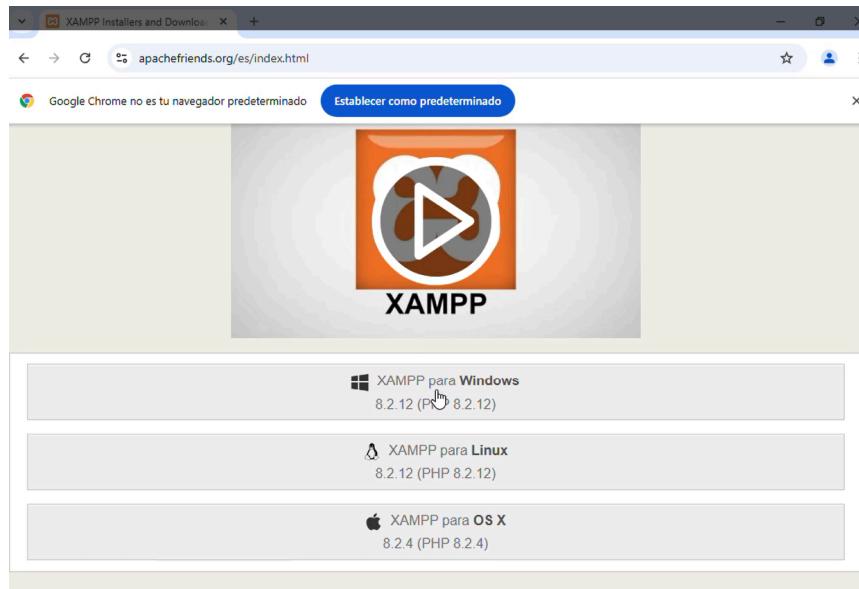
Para ello, abre un editor simple de texto, copia las líneas de html personalizándolo con tu nombre y referenciando la imagen correctamente, Por último guarda el archivo como "mipagina.html" y añade a la carpeta pública del servidor una foto tuya de tamaño carné para que se visualice al abrir la página.

A continuación, realiza una captura de pantalla del navegador accediendo a esta URL: "<http://localhost/mipagina.html>"

---

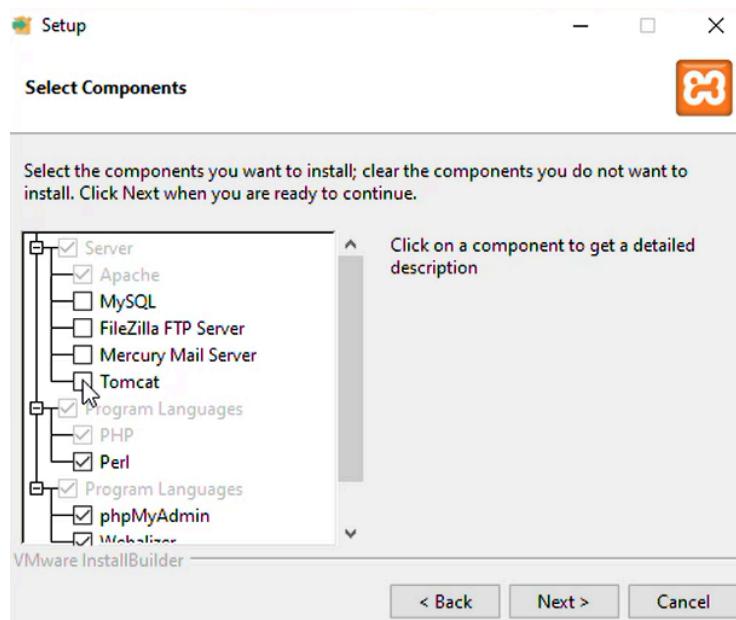
### 1. Instalar XAMPP

Descarga XAMPP desde la página oficial: <https://www.apachefriends.org/es/index.html>

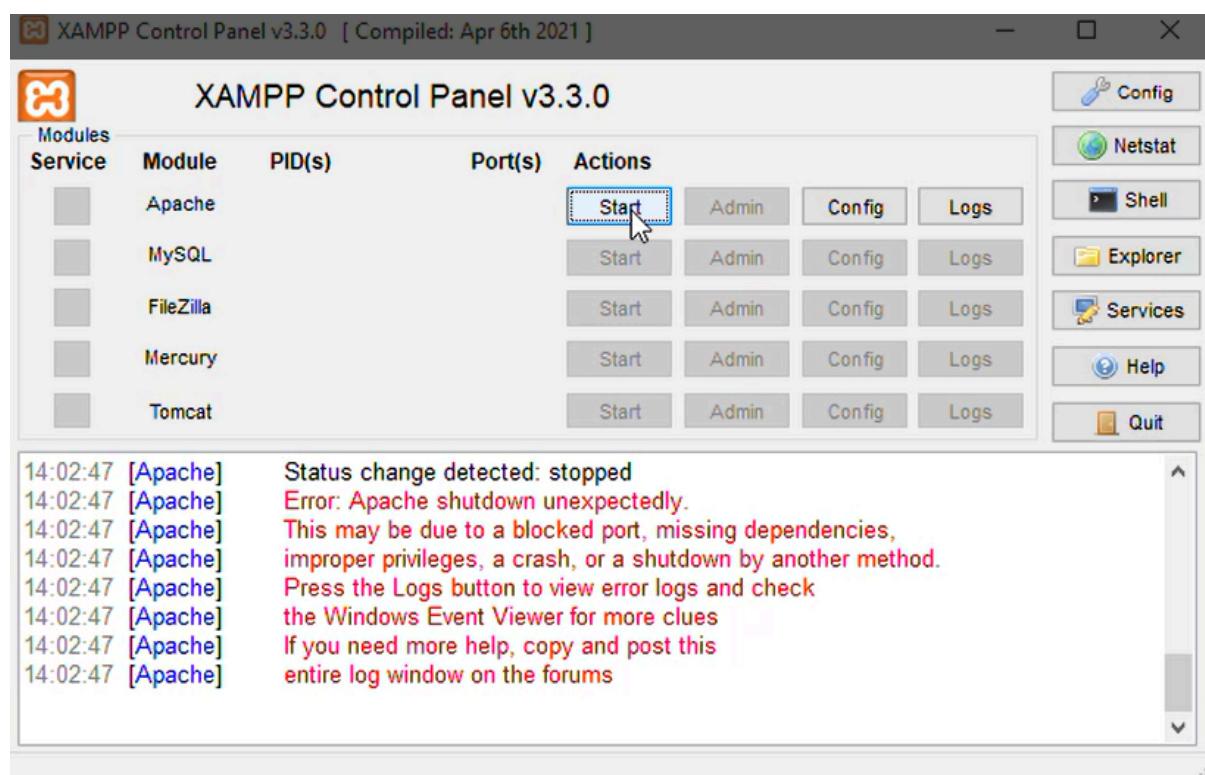


Ejecuta el instalador y selecciona los siguientes módulos:

- **Apache** (servidor web)
- **PHP** (opcional, pero útil para futuras prácticas)



Completa la instalación y abre **XAMPP Control Panel**.



Inicia el servicio **Apache** pulsando el botón "**Start**".

No me funciona, he buscado que hacer pero no se como hacerlo y la máquina me va fatal.

# Actividad 6.

**Utilizando un antivirus, realiza lo siguiente:**

a) 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.

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 hacer esta actividad necesitas tener instalado un programa antivirus. Lo más probable es que lo tengas, pero si no es así, estos son algunos gratuitos que puedes instalar:

- Avast! Free Antivirus.
  - Avira Antivir Personal-Free.
  - AVG Anti-virus Free Edition.
- 

## 1. Elegir un antivirus

Si ya tienes instalado un antivirus como **Windows Defender**, **Avast**, **Avira**, o **AVG**, úsallo.

Si no tienes ninguno, puedes descargar **Windows Defender** (integrado en Windows 10) o uno de los gratuitos mencionados.

Yo tengo el **Windows Defender**.

## 2. Realizar el análisis de una unidad extraíble

Conectar la unidad USB o disco externo al PC.

Abrir el antivirus:

- Si usas **Windows Defender**, ve a:  
Configuración de Windows → Actualización y seguridad → Seguridad de Windows → Protección antivirus y contra amenazas
- Si usas **Avast**, **Avira** o **AVG**, abre su panel de control.

← Configuración

Inicio

Buscar una configuración

Actualización y seguridad

- Windows Update
- Optimización de distribución
- Seguridad de Windows**
- Copia de seguridad de archivos
- Solucionar problemas
- Recuperación
- Activación
- Encontrar mi dispositivo
- Para programadores

## Seguridad de Windows

El servicio Seguridad de Windows es el lugar de inicio para ver y administrar la seguridad y el estado de tu dispositivo.

Abrir Seguridad de Windows

### Áreas de protección

- Protección contra virus y amenazas  
No se requieren acciones.
- Protección de cuentas  
No se requieren acciones.
- Firewall y protección de red  
No se requieren acciones.
- Control de aplicaciones y exploradores  
No se requieren acciones.
- Seguridad del dispositivo  
No se requieren acciones.
- Rendimiento y estado del dispositivo  
Informa sobre el estado del dispositivo.
- Opciones de familia

← Configuración

Inicio

Buscar una configuración

Actualización y seguridad

- Windows Update
- Optimización de distribución
- Seguridad de Windows**
- Copia de seguridad de archivos
- Solucionar problemas
- Recuperación
- Activación
- Encontrar mi dispositivo
- Para programadores

## Seguridad de Windows

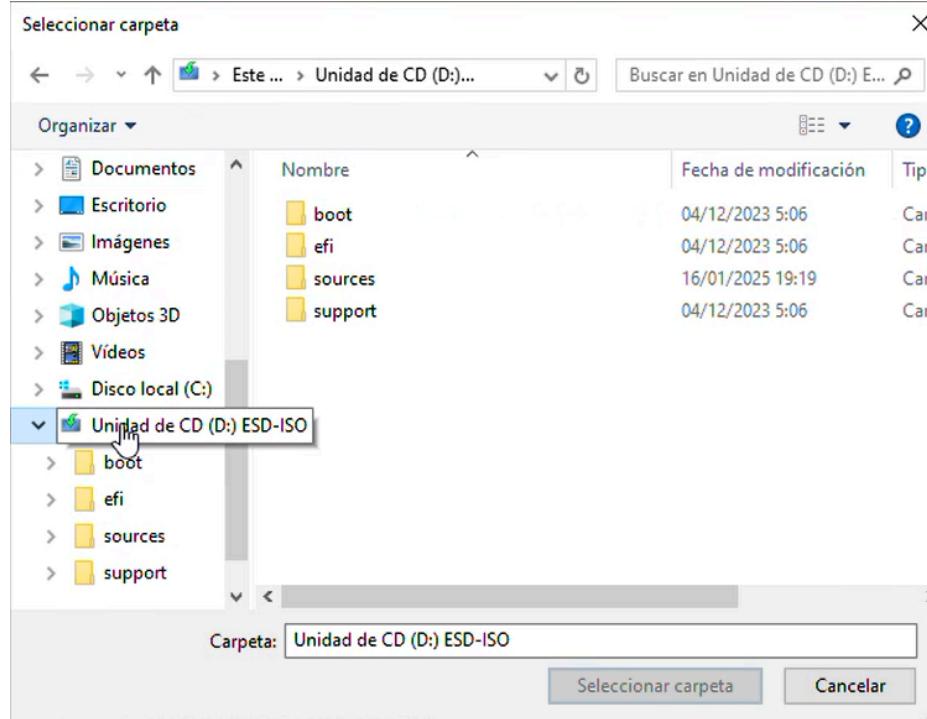
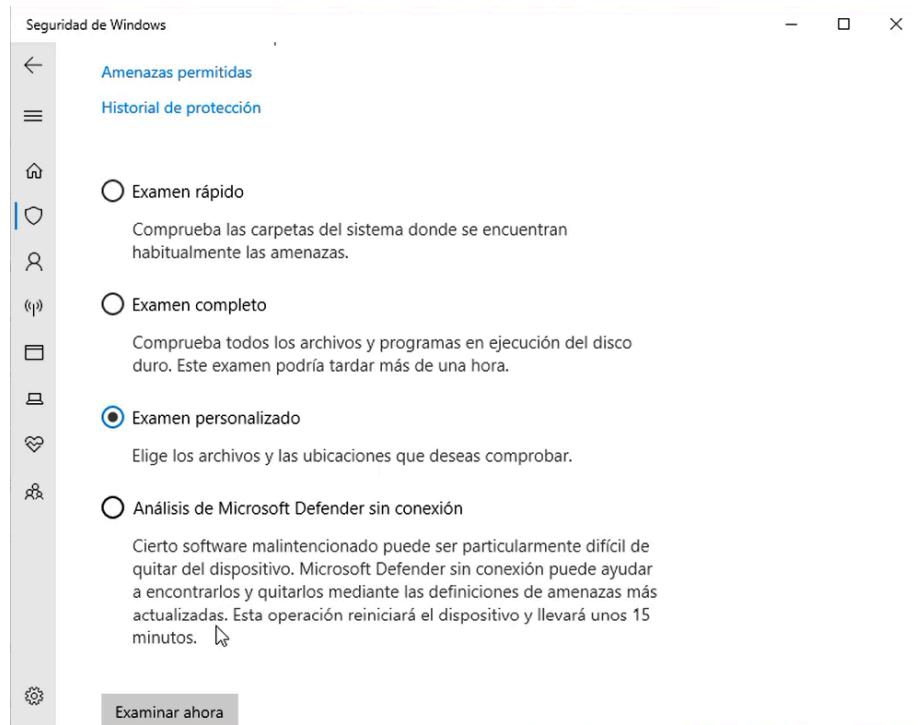
El servicio Seguridad de Windows es el lugar de inicio para ver y administrar la seguridad y el estado de tu dispositivo.

Abrir Seguridad de Windows

### Áreas de protección

- Protección contra virus y amenazas  
No se requieren acciones.
- Protección de cuentas  
No se requieren acciones.
- Firewall y protección de red  
No se requieren acciones.
- Control de aplicaciones y exploradores  
No se requieren acciones.
- Seguridad del dispositivo  
No se requieren acciones.
- Rendimiento y estado del dispositivo  
Informa sobre el estado del dispositivo.
- Opciones de familia

**Seleccionar "Análisis personalizado" o "Escaneo de unidad específica".**  
**Elegir la unidad USB y comenzar el análisis.**





## Opciones de examen

Ejecuta un análisis rápido, completo, personalizado o de Microsoft Defender sin conexión.

Ejecutando examen personalizado...

Tiempo restante estimado: 00:00:01

1990 archivos examinados

[Cancelar](#)

Puedes seguir trabajando mientras examinamos tu dispositivo.

[Historial de protección](#)



¿Tienes alguna pregunta?

[Obtener ayuda](#)

Ayuda a mejorar el servicio

Seguridad de Windows

[Envíanos tus comentarios](#)



## Actividad 7.

### • Captura de tráfico DNS

1. Instala e inicia Wireshark y comienza una captura de tráfico en tu red.
2. Abre una terminal (CMD o PowerShell) y ejecuta el siguiente comando:  
nslookup www.google.com
3. Detén la captura y utiliza el filtro dns en Wireshark.
4. Identifica la consulta DNS enviada y la respuesta recibida.
5. Captura una imagen del paquete DNS y explica su contenido.

### • Comparación de tráfico HTTP vs. HTTPS

1. Repite el proceso de captura en Wireshark.
2. Accede a un sitio web sin cifrado (como http://neverssl.com) y luego a un sitio con cifrado (como https://www.google.com).
3. Detén la captura y filtra por http y tls en Wireshark.
4. Explica las diferencias entre los paquetes capturados en HTTP y HTTPS.

### Análisis de cabeceras HTTP

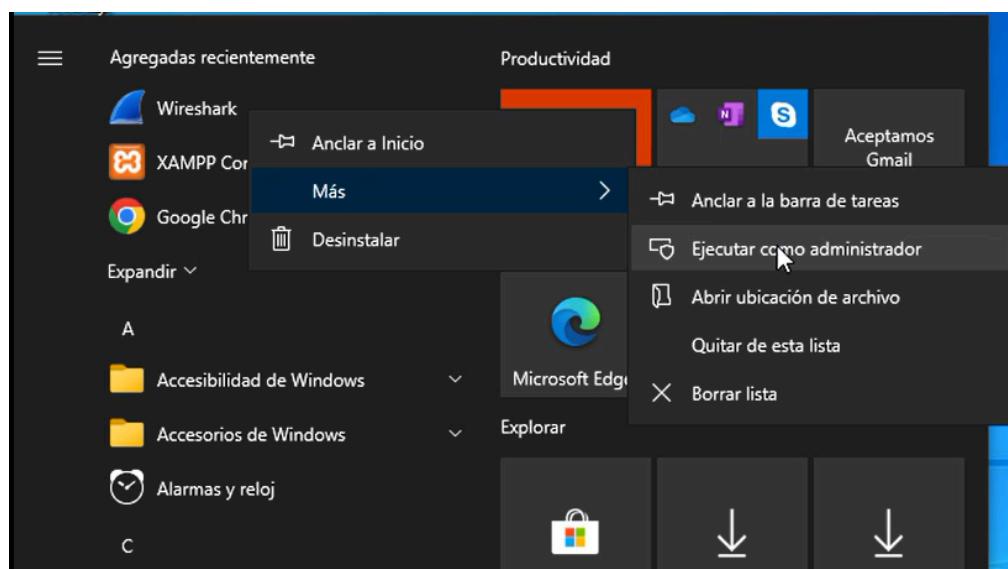
1. Encuentra un paquete HTTP GET en Wireshark y analiza las cabeceras que se envían en texto claro.
2. Explica cómo estas cabeceras pueden exponer información y cómo HTTPS protege contra ello.

## ◆ Parte 1: Captura de Tráfico DNS

### 1. Instalar y Configurar Wireshark

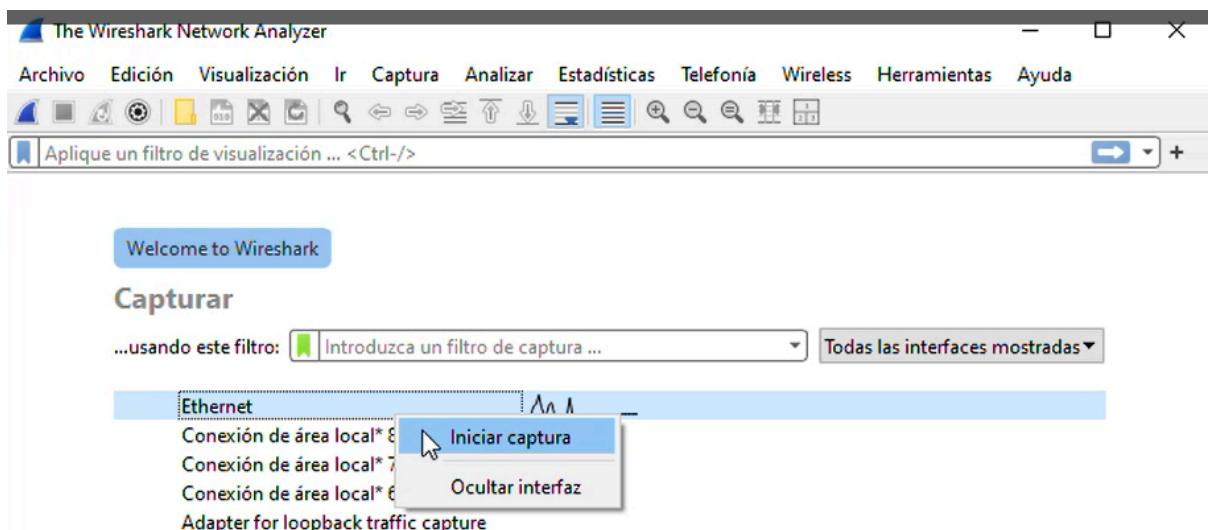
Descarga e instala Wireshark desde: <https://www.wireshark.org/download.html>

Ejecuta Wireshark como Administrador.



En la lista de interfaces, selecciona tu **tarjeta de red activa** (Wi-Fi o Ethernet).

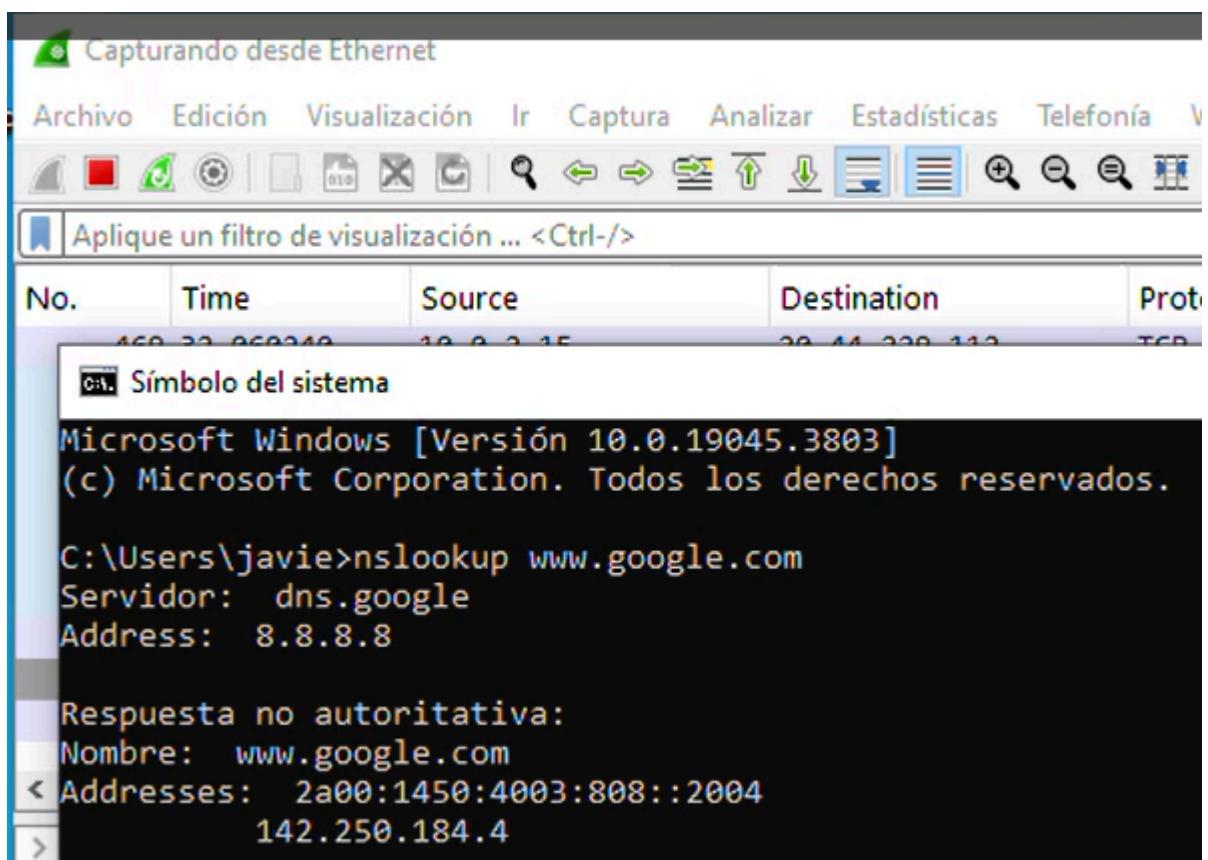
Pulsa "**Start**" para comenzar la captura.



## 2. Generar una Consulta DNS

Abre **CMD o PowerShell**.

Escribe y ejecuta: `nslookup www.google.com`



Esto generará tráfico DNS en Wireshark.

### 3. Filtrar y Analizar Paquetes DNS

En Wireshark, detén la captura (**Stop**).

En la barra de filtro, escribe: **dns**

Busca los paquetes "**Standard query**" y "**Standard query response**".

**Explicación del paquete DNS:**

- **Query:** El cliente pregunta por la IP de [www.google.com](http://www.google.com).
- **Response:** El servidor responde con la dirección IP asociada.

The screenshot shows the Wireshark interface with the following details:

- Toolbar:** Includes icons for file operations (File, Edit, View, Capture, Analyze, Statistics, Phone, Wireless, Tools, Help), search (Search, Find Next, Find Previous, Find in Captured Packets, Find in Displayed Packets, Find in Hex Editor, Find in All Columns), and selection (Select, Select All, Deselect, Deselect All, Select by Address, Select by Content, Select by Bytes, Select by Hex, Select by Dec, Select by Hex/Dec, Select by Hex/Dec/Hex).
- Filter Bar:** Shows the filter **dns**.
- Packet List:** Displays a list of DNS packets. The columns are Destination, Protocol, Length, and Info. Key entries include:
  - 8.8.8.8 DNS 77 Standard query 0x585b A p-ring.msedge.net
  - 8.8.8.8 DNS 77 Standard query 0x34b8 AAAA p-ring.msedge.net
  - 10.0.2.15 DNS 179 Standard query response 0x585b A p-ring.msedge.net CNAME p-ri...
  - 10.0.2.15 DNS 203 Standard query response 0x34b8 AAAA p-ring.msedge.net CNAME p...
  - 8.8.8.8 DNS 88 Standard query 0x26f6 A arc-ring-fallback.msedge.net
  - 8.8.8.8 DNS 88 Standard query 0x2fbb AAAA arc-ring-fallback.msedge.net
  - 10.0.2.15 DNS 180 Standard query response 0x26f6 A arc-ring-fallback.msedge.net...
  - 8.8.4.4 DNS 88 Standard query 0x2fbb AAAA arc-ring-fallback.msedge.net
  - 10.0.2.15 DNS 204 Standard query response 0x2fbb AAAA arc-ring-fallback.msedge...
  - 10.0.2.15 DNS 204 Standard query response 0x2fbb AAAA arc-ring-fallback.msedge...
  - 8.8.8.8 DNS 113 Standard query 0x6965 A 243chfe0474938d7cd149hfdc2heh4f0.azr...
- Details Panel:** Shows the details of the selected packet (Frame 110).
  - Frame 110: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface Ethernet II, Src: PCSSystemtec\_33:a0:fc (08:00:27:33:a0:fc), Dst: Google DNS (8.8.8.8) (00:0c:29:10:7d:91)
  - Ethernet II, Src: PCSSystemtec\_33:a0:fc (08:00:27:33:a0:fc), Dst: Google DNS (8.8.8.8) (00:0c:29:10:7d:91)
  - Internet Protocol Version 4, Src: 10.0.2.15, Dst: 8.8.8.8
  - User Datagram Protocol, Src Port: 55669, Dst Port: 53
  - Domain Name System (query)
- Hex Editor:** Shows the hex dump of the selected packet.
- Bottom Status Bar:** Shows the number of packets (504), displayed (24), lost (0), and profile (Default).

## ◆ Parte 2: Comparación de Tráfico HTTP vs HTTPS

### 1. Iniciar Captura en Wireshark

Reinicia Wireshark y empieza una nueva captura.

### 2. Acceder a Páginas HTTP y HTTPS

**HTTP:**

Abre un navegador y ve a: <http://neverssl.com>

**HTTPS:**

Luego accede a: <https://www.google.com>

Detén la captura.

The screenshot shows a Google search results page for the query "neverssl". The top result is a link to "NeverSSL - helping you get online" with the URL <http://neverssl.com>. Below the link, there is a snippet of text: "This website is when you try to open Facebook, Google, Amazon, etc on a wifi network, and nothing happens. Type "http://neverssl.com" into your browser's ...". The page has a standard Google layout with navigation links like "Todo", "Imágenes", "Vídeos", etc., and a "Herramientas" menu.

Más preguntas :

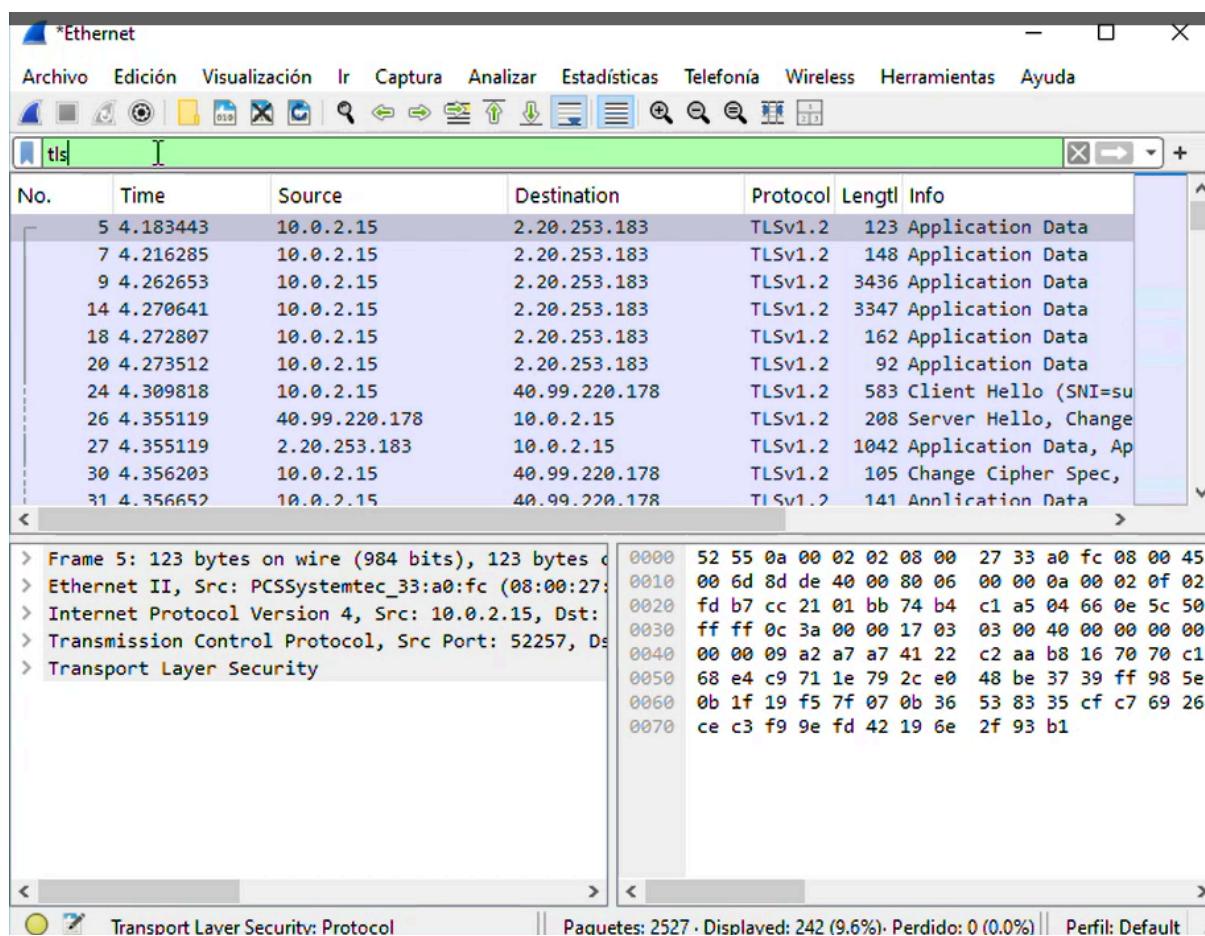
The screenshot shows a Google search results page for the query "NeverSSL - helping you get online". The top result is a link to "NeverSSL - helping you get online" with the URL <http://neverssl.com>. Below the link, there is a snippet of text: "This website is when you try to open Facebook, Google, Amazon, etc on a wifi network, and nothing happens. Type "http://neverssl.com" into your browser's ...". The page has a standard Google layout with navigation links like "Sobre Google", "Tienda", "Gmail", "Imágenes", etc., and a "Herramientas" menu.

### 3. Filtrar por HTTP y HTTPS

Filtrar HTTP: `http`



Filtrar HTTPS (TLS): `tls`



Diferencias observadas:

- HTTP muestra contenido en **texto claro**.
- HTTPS usa **cifrado TLS**, y el contenido no es visible en Wireshark.

## ◆ Parte 3: Análisis de Cabeceras HTTP

### 1. Encontrar un Paquete HTTP GET

Filtrar por HTTP en Wireshark: `http.request.method == "GET"`

1. Selecciona un paquete y analiza las **cabeceras** en **texto claro**.

### 2. Explicación de Seguridad

HTTP expone información como:

- URLs
- Cookies
- User-Agent (navegador y sistema operativo)

No me salía nada tampoco.

# Actividad 8.

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

- 1. Configuración de la clave del router.**
  - 2. Configuración de la clave de red. Si aún no dispones de clave, establécela.**
  - 3. Configuración del tipo de cifrado. Cambia el cifrado a WPA2 si no lo tienes así.**
  - 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.**
- 

No puedo hacerlo porque estoy en casa de mi novia y hay 4 personas más viviendo y les voy a molestar. Pero esto es algo que ya he hecho muchas otras veces. Siempre lo hago en mi casa cada vez que hemos cambiado en internet.

Te dejo los pasos a seguir, espero que valga para algo al menos.

## 1. Acceder al Router

1. Conéctate a la red Wi-Fi del router o usa un cable Ethernet.
2. Abre un navegador e ingresa la dirección IP del router (suele ser una de estas):
  - **192.168.1.1**
  - **192.168.0.1**
  - **192.168.18.1**
3. Introduce **usuario y contraseña** (normalmente están en la parte trasera del router).
  - Si no los conoces, revisa el manual del router o pregunta al administrador de la red.

## 2. Cambiar la Clave de Acceso del Router

1. Ve a **Configuración Avanzada → Administración → Cambiar contraseña**.
2. Introduce una nueva clave segura para acceder al router.
3. **Captura de pantalla de la configuración antes y después del cambio.**

## 3. Configurar la Clave de la Red Wi-Fi

1. En el menú, busca "**Configuración Inalámbrica**" o "**Wireless Settings**".
2. Ubica la opción "**Clave de red**" o "**Contraseña Wi-Fi**".
3. Si no hay clave, actívala y establece una segura.
4. **Captura de pantalla del cambio de clave.**

#### **4. Cambiar el Tipo de Cifrado a WPA2**

1. En el mismo menú de "**Configuración Inalámbrica**", busca la opción de **Seguridad**.
2. Si el cifrado no es **WPA2**, cambia a:
  - **WPA2-PSK (AES)** para mayor seguridad.
3. **Captura de pantalla mostrando el cifrado seleccionado.**

#### **5. Filtrar Dispositivos por Dirección MAC**

1. Encuentra la opción "**Filtro de Direcciones MAC**" o "**MAC Filtering**".
2. Actívalo y selecciona "**Permitir solo estas MAC**".
3. **Añade las direcciones MAC de los dispositivos en tu red.**

Puedes verlas ejecutando en CMD: `ipconfig /all`

- O en el router en la sección "**Dispositivos Conectados**".
4. **Añade la MAC ficticia:** `DC:0A:B3:1B:7E:C0`.
  5. **Captura de pantalla con las direcciones MAC configuradas.**