

Sistemas Informáticos

Tarea N° 6



Manuel Pacheco Sánchez

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?

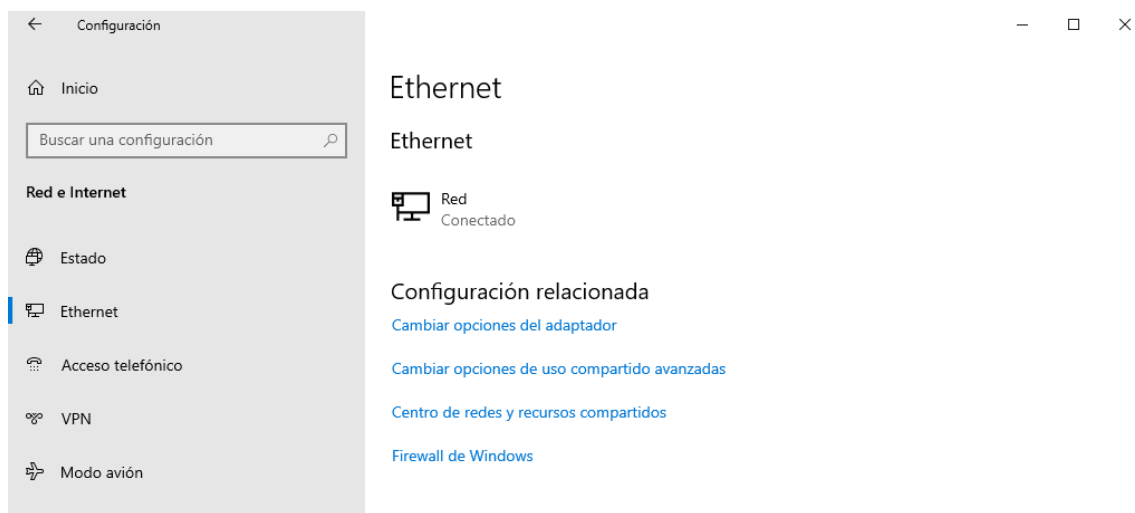
Realiza las siguientes actividades en tu equipo o máquina virtual utilizando Windows 10. El equipo o máquina virtual debe contener dos adaptadores de red: uno de tipo Ethernet y el otro inalámbrico para conexiones a redes WIFI.

Actividad 1.

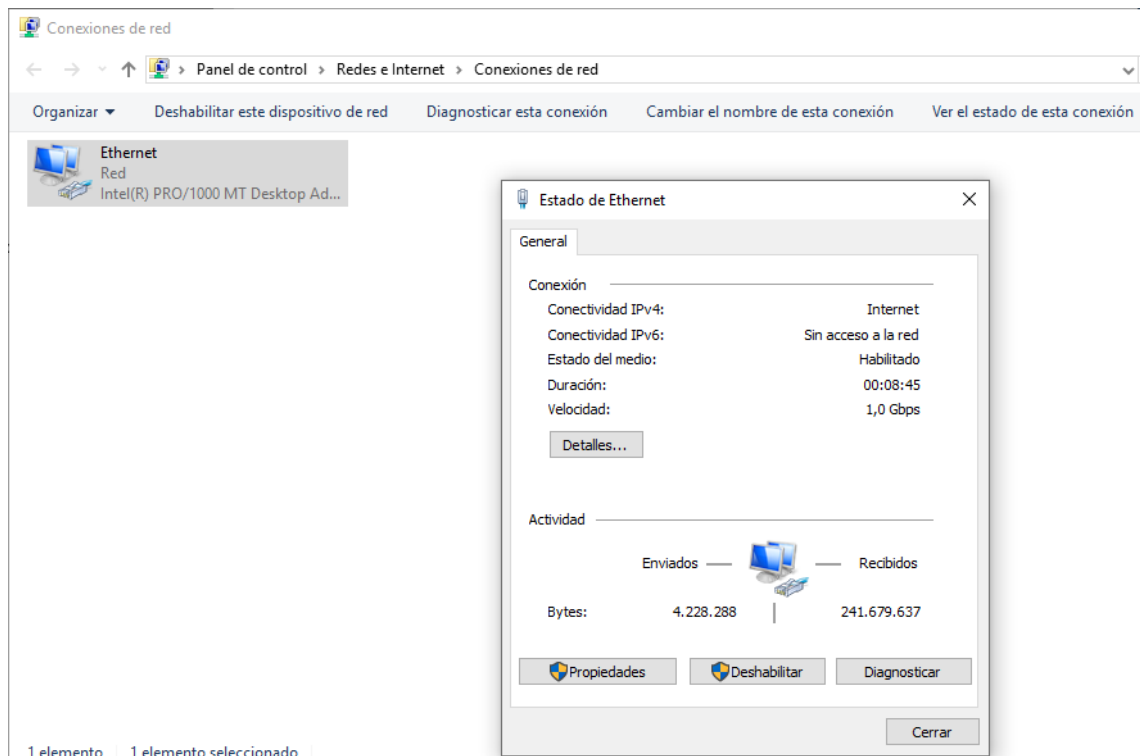
Configura la conexión de la tarjeta de red Ethernet con los siguientes datos:

- **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**

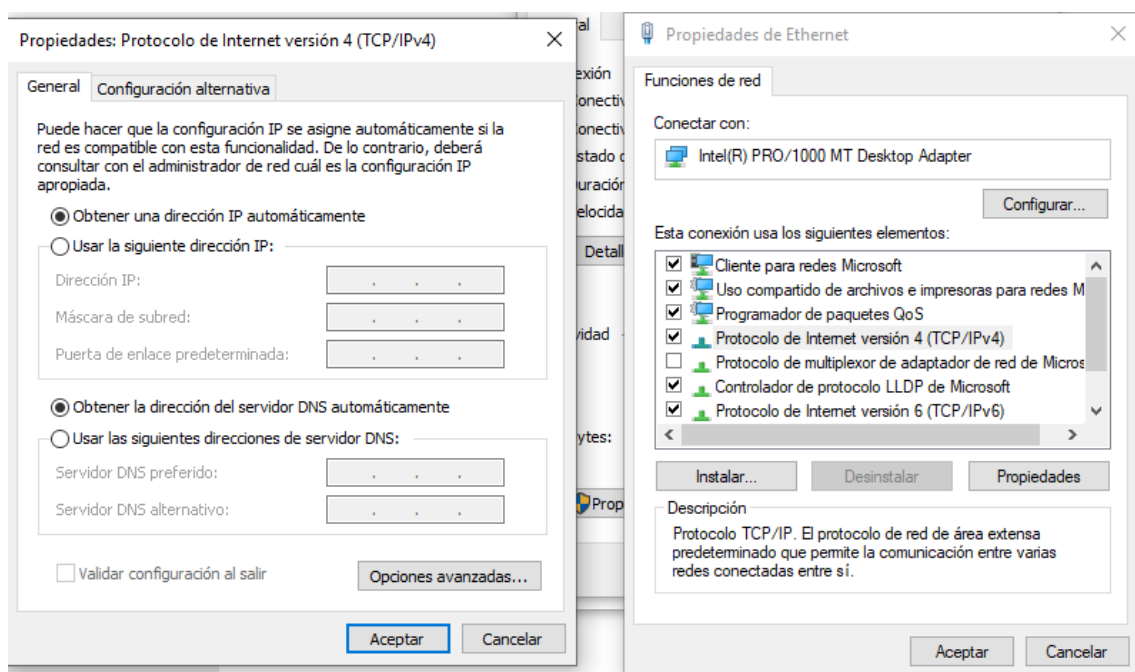
Para cambiar la configuración de la tarjeta de red Ethernet, en la barra de tareas accedemos al apartado de red. Damos click derecho y “Abrir Configuración de Red e Internet”. Dentro de la configuración, vamos a “Cambiar opciones del adaptador”.



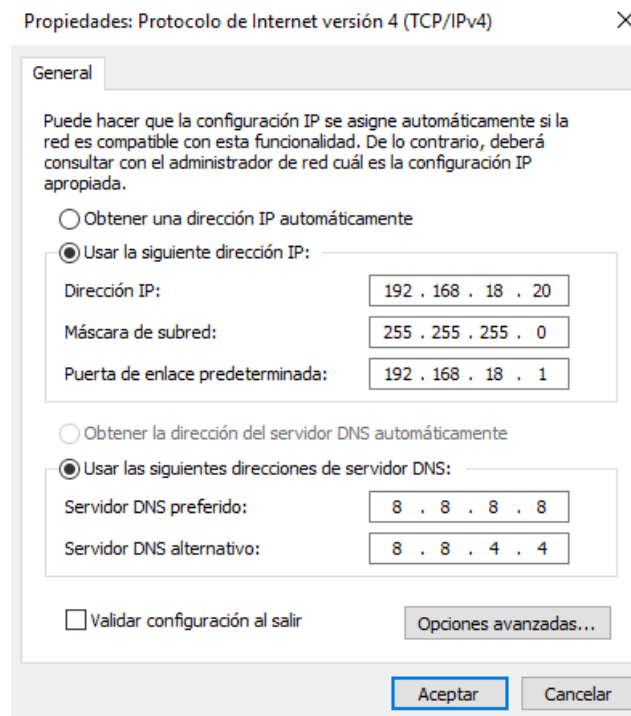
Seleccionamos la pestaña de Ethernet, y dentro vamos a “Propiedades”.



Dentro de las propiedades, buscamos “Protocolo de internet versión 4 (IPv4)”. Damos doble click y nos aparecerá el menú de configuración.



Vamos a introducir los parámetros que se nos han dado para la tarjeta de red.



Actividad 2.

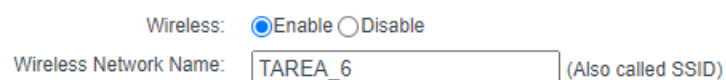
Configura la conexión inalámbrica para conectarse a la red con SSID "TAREA_6" que da los valores de conexión por servidor DHCP y cuya clave de acceso WPA o WPA2 es "SistemasInformaticos". En ocasiones el servidor DHCP no funciona adecuadamente y tenemos que utilizar los siguientes valores de configuración 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 emular la configuración de la conexión inalámbrica vamos a acceder a un simulador de routers, por ejemplo el simulador de TP-LINK.

Escogemos un router cualquiera, y accedemos a su configuración.

Como nombre de red, asignamos "TAREA_6".



Establecemos la seguridad de la red como WPA y ponemos como contraseña “SistemasInformaticos”.

☒ WPA/WPA2 - Personal(Recommended)

Authentication Type:

Encryption:

Wireless Password:

Group Key Update Period:

Activamos también la asignación de direcciones mediante DHCP.

DHCP Server: ☐ Disable ☒ Enable

Start IP Address:

End IP Address:

Lease Time: minutes (1~2880 minutes, the default value is 120)

Default Gateway: (optional)

Default Domain: (optional)

DNS Server: (optional)

Secondary DNS Server: (optional)

Y vamos a reservar una dirección para cuando el servidor DHCP no funcione correctamente.

Connection Type:

IP Address:

Subnet Mask:

Gateway:

Primary DNS Server:

Secondary DNS Server: (optional)

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.

```
C:\Users\Manuel Pacheco>hostname  
Manuel
```

Hostname devuelve el nombre del host en la red, es el nombre con el que se identifica nuestro equipo en una red.

```
C:\Users\Manuel Pacheco>ipconfig  
  
Configuración IP de Windows  
  
Adaptador de Ethernet Ethernet 2:  
    Sufijo DNS específico para la conexión. . . :  
    Vínculo: dirección IPv6 local. . . : fe80::6935:486:527d:ee67%5  
    Dirección IPv4. . . . . : 192.168.56.1  
    Máscara de subred. . . . . : 255.255.255.0  
    Puerta de enlace predeterminada. . . . . :  
  
Adaptador de LAN inalámbrica Conexión de área local* 1:  
    Estado de los medios. . . . . : medios desconectados  
    Sufijo DNS específico para la conexión. . . :  
  
Adaptador de LAN inalámbrica Conexión de área local* 10:  
    Estado de los medios. . . . . : medios desconectados  
    Sufijo DNS específico para la conexión. . . :  
  
Adaptador de LAN inalámbrica Wi-Fi:  
    Sufijo DNS específico para la conexión. . . :  
    Vínculo: dirección IPv6 local. . . : fe80::4c22:6383:cae6:64a0%17  
    Dirección IPv4. . . . . : 10.200.33.167  
    Máscara de subred. . . . . : 255.255.255.0  
    Puerta de enlace predeterminada. . . . . : 10.200.33.1  
  
Adaptador de Ethernet Conexión de red Bluetooth:  
    Estado de los medios. . . . . : medios desconectados  
    Sufijo DNS específico para la conexión. . . :  
  
C:\Users\Manuel Pacheco>
```

Ipconfig nos devuelve la configuración de nuestro adaptador de red.

```
C:\Users\Manuel Pacheco>nslookup google.com  
Servidor:  UnKnown  
Address:  10.200.8.1  
  
Respuesta no autoritativa:  
Nombre:  google.com  
Addresses:  2a00:1450:4003:806::200e  
           142.250.201.78
```

Nslookup nos devuelve la “conversión” que realiza el servidor DNS, es decir, la dirección ip a la que accedemos y la traducción que realiza con la URL.

```

C:\Users\Manuel Pacheco>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=9ms TTL=115
Respuesta desde 8.8.8.8: bytes=32 tiempo=9ms TTL=115
Respuesta desde 8.8.8.8: bytes=32 tiempo=10ms TTL=115
Respuesta desde 8.8.8.8: bytes=32 tiempo=9ms TTL=115

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 = 10ms, Media = 9ms

```

El comando ping envía paquetes a un servidor y nos devuelve el tiempo que han tardado en llegar y si han llegado o no.

```

C:\Users\Manuel Pacheco>tracert 8.8.8.8

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

 1    4 ms    1 ms    2 ms    10.200.33.1
 2    4 ms    3 ms    4 ms    192.168.144.1
 3    4 ms    3 ms    4 ms    185.red-81-41-225.staticip.rima-tde.net [81.41.225.185]
 4    *        *        *        Tiempo de espera agotado para esta solicitud.
 5    *        *        *        Tiempo de espera agotado para esta solicitud.
 6   14 ms   11 ms   11 ms   176.52.253.97
 7   10 ms    9 ms    9 ms   72.14.211.154
 8    9 ms   10 ms    9 ms   172.253.50.37
 9   10 ms    9 ms    9 ms   142.251.51.141
10    9 ms   10 ms    8 ms   dns.google [8.8.8.8]

Traza completa.

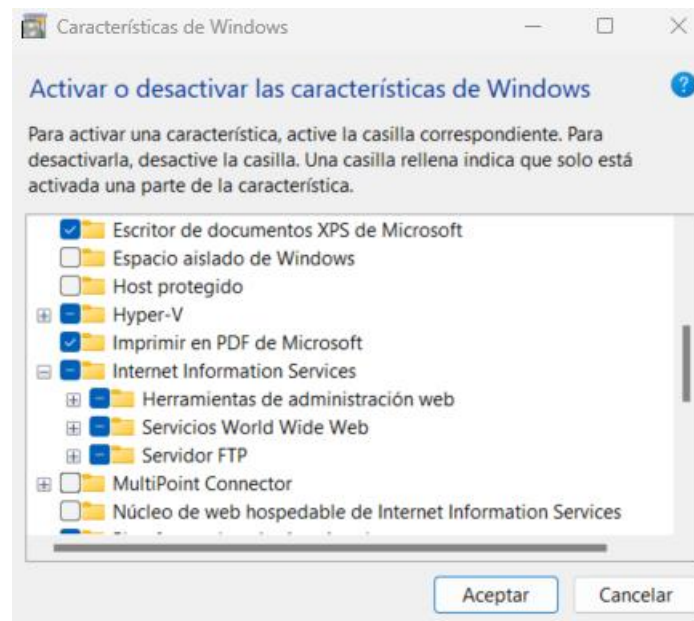
```

El comando tracert sigue los paquetes que recibimos de la dirección IP que especificamos, y nos devuelve el tiempo que tardan en llegar.

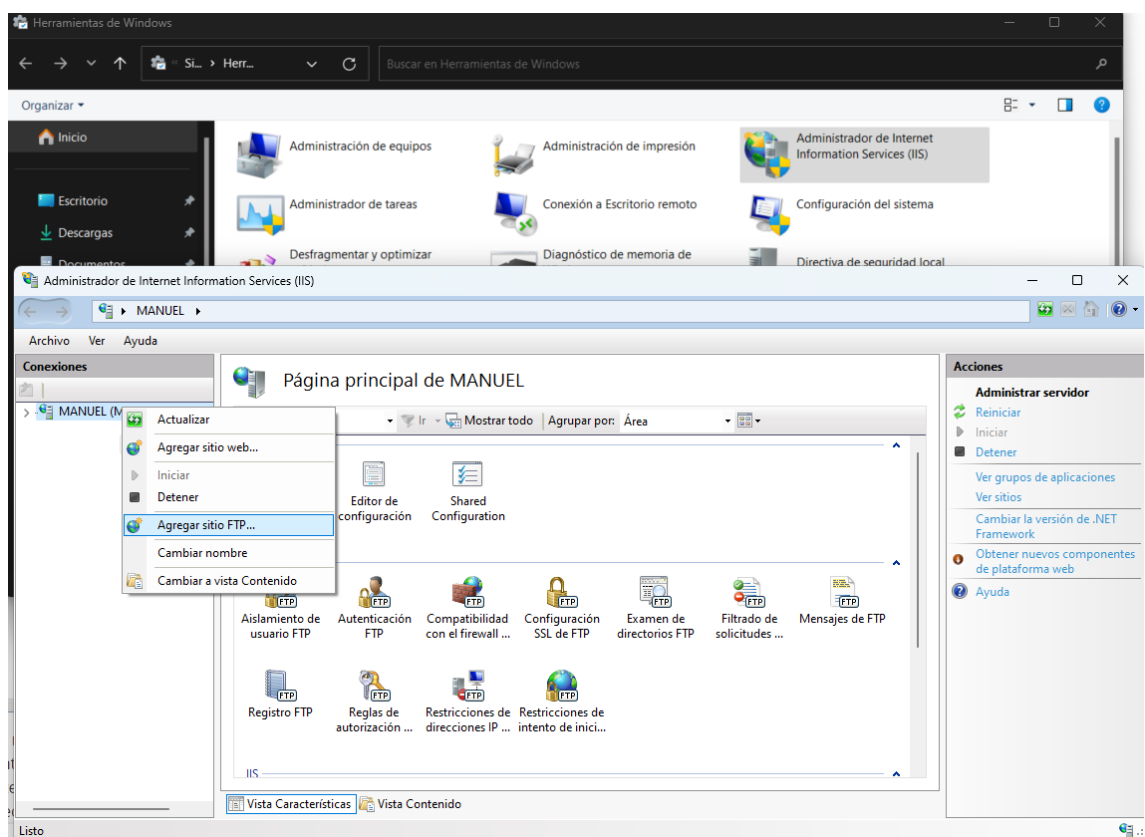
Actividad 4.

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).


Vamos a activar la característica de Windows de servidor FTP. Para ello, vamos a panel de control, programas, activar o desactivar características de Windows y buscamos "Internet Information Services", y desglosando la pestaña, activamos "Servidor FTP".



Para crear un nuevo servidor FTP, vamos a herramientas de Windows, damos doble click sobre “Administrador de Internet Information Services” y en la barra izquierda, damos click derecho y pulsamos sobre “Agregar sitio FTP”.



Inicializamos nuestro sitio con el nombre especificado en el ejercicio y señalamos el directorio sobre el que vamos a montar el servidor. Seguidamente, indicamos la dirección IP para conectarnos con el servidor y el puerto, el cual por defecto es el 21.




Configuración de enlaces y SSL

Enlace
Dirección IP: Puerto:
☐ Habilitar nombres de host virtuales:
Host virtual (ejemplo: ftp.contoso.com):

☒ Iniciar sitio FTP automáticamente

SSL
☒ Sin SSL
☐ Permitir SSL
☐ Requerir SSL
Certificado SSL:

Establecemos la autenticación básica.



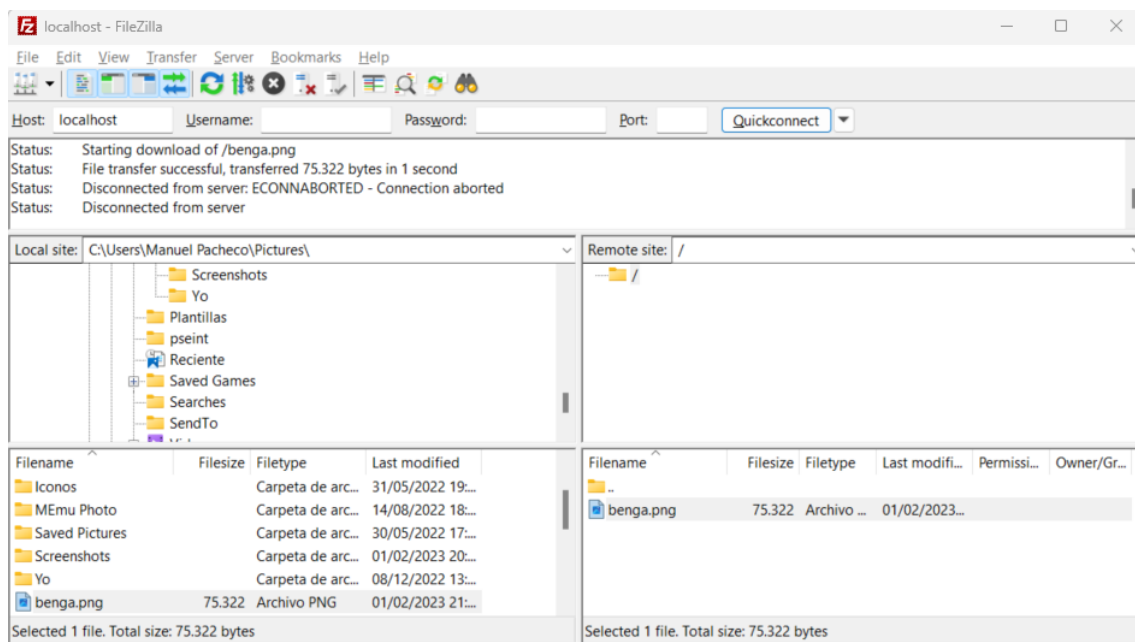
Información de autenticación y autorización

Autenticación
☐ Anónima
☒ Básica

Autorización
Permitir el acceso a:

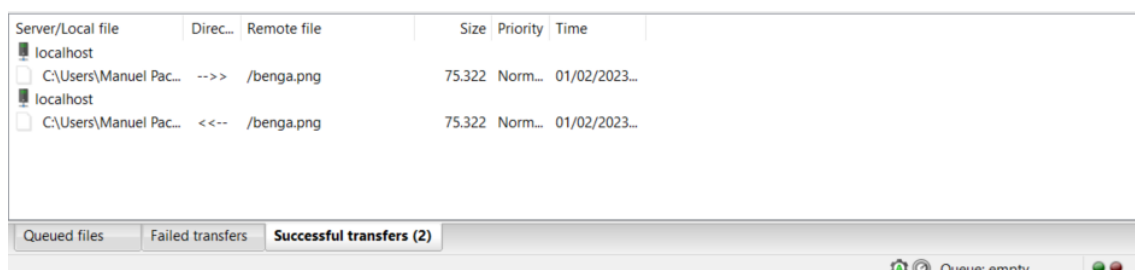
Permisos
☐ Leer
☐ Escribir

Una vez tenemos creado el servidor, vamos a descargar el cliente de Filezilla para comprobar que funciona correctamente.



Para conectarnos a nuestro sitio, como lo tenemos creado sobre nuestro mismo equipo, en host especificamos "localhost", y como la autenticación es anónima, solo tenemos que indicar el puerto, que como vemos en las capturas anteriores es el 21.

Una vez dentro de nuestro servidor FTP, vamos a probar que podemos leer y escribir sobre el servidor. Vamos a coger una imagen cualquiera y montarla y posteriormente descargarla de nuestro servidor.



Como vemos, ambas transferencias se han realizado correctamente.

Actividad 5.

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

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.

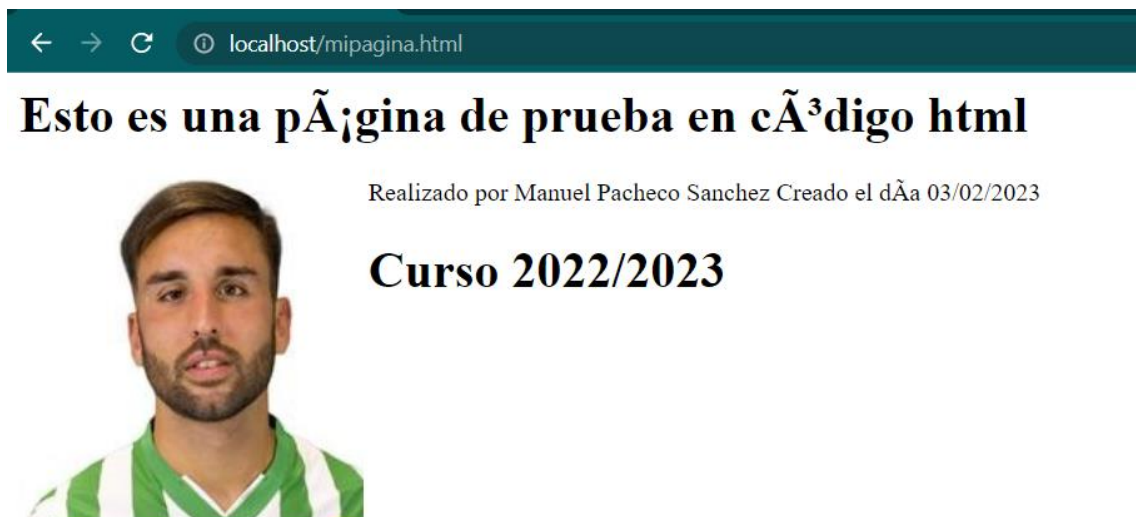
A continuación, realiza una captura de pantalla del navegador accediendo a esta URL:
"http:\\localhost\\mipagina.html"

Para hacer esta actividad, vamos a crear un archivo HTML donde vamos a copiar el código que se nos proporciona.

```
File Edit Selection View Go Run Terminal Help
C:\xampp\htdocs> mipagina.html
1 <html>
2
3 <head>
4   <title>Sistemas Informaticos DAM/DAM Tarea 6</title>
5 </head>
6
7 <body>
8   <!--Esto es una página de prueba en código html-->
9   Realizado por Manuel Pacheco Sanchez
10  Creado el día 03/02/2023
11  
12  <!-- curso 2022/2023 -->
13 </body>
14
15 </html>
```

Vamos a guardar esta página en la ruta donde tengamos instalado Xampp, y en su interior en la carpeta htdocs.

Al arrancar el servidor Apache y navegar hacia localhost/mipagina.html, este es el resultado que obtenemos:



Actividad 6

Utilizando un antivirus realiza lo siguiente:

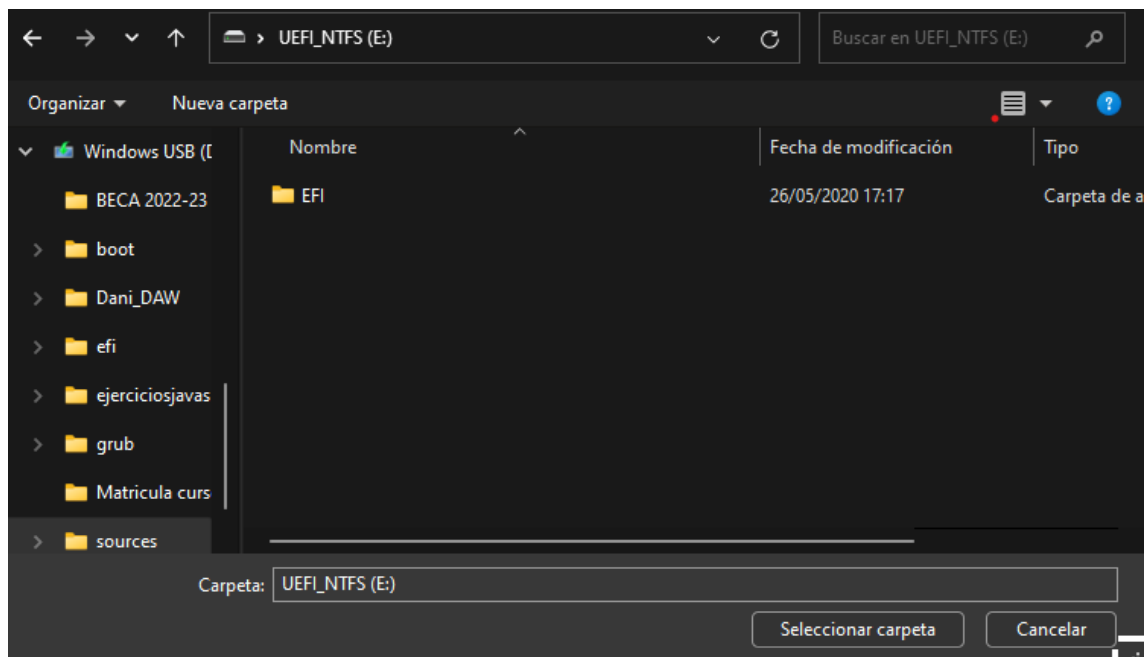
- Analiza una unidad extraíble que tengas conectada al ordenador y muestra una captura de pantalla del proceso y otra del resultado del análisis. ¿Se ha detectado alguna amenaza? En caso afirmativo, ¿de qué tipo? ¿qué acciones has tomado (eliminar, ignorar alerta, poner en cuarentena el archivo)? Razona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

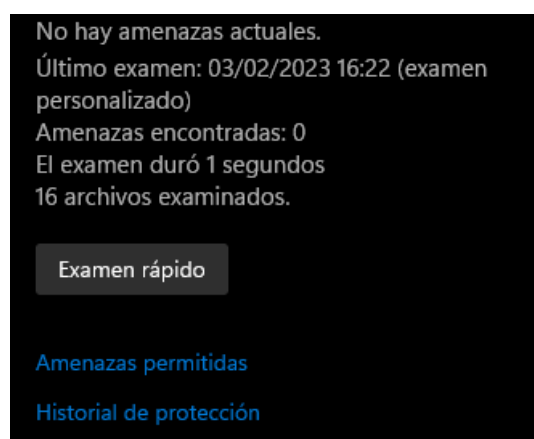
- **Avast! Free Antivirus.**
- **Avira Antivir Personal-Free.**
- **AVG Anti-virus Free Edition.**

Para realizar el examen sobre una unidad externa, vamos a ir a Windows Defender, seleccionamos “Protección contra virus y amenazas” y seleccionamos examen personalizado.

Al empezar el examen, nos va a pedir seleccionar la ubicación que queremos examinar:



Seleccionamos la ubicación y empezamos el examen:



Como vemos, nuestra unidad óptica no tiene amenazas, por lo que no tendremos que tomar medidas.

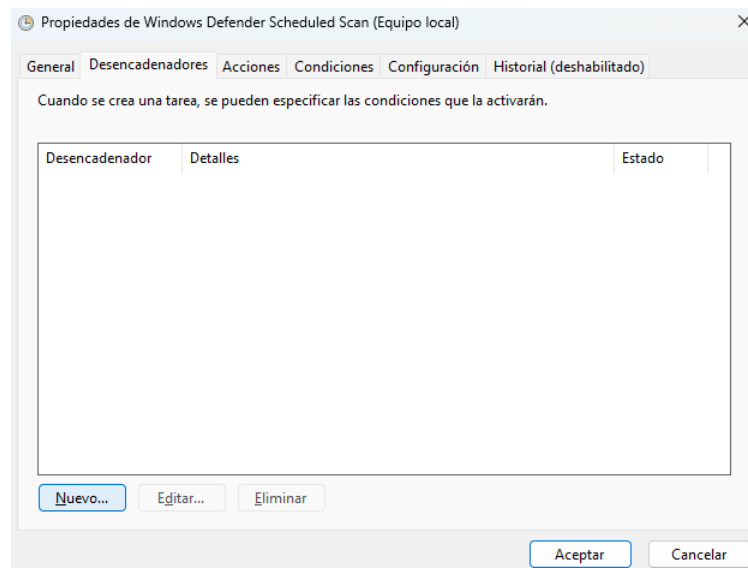
Ahora, vamos a programar Windows Defender para que haga un análisis de forma periódica.

Vamos a acceder al programador de tareas, y dentro vamos a Biblioteca del programador de tareas > Microsoft > Windows > Windows Defender.

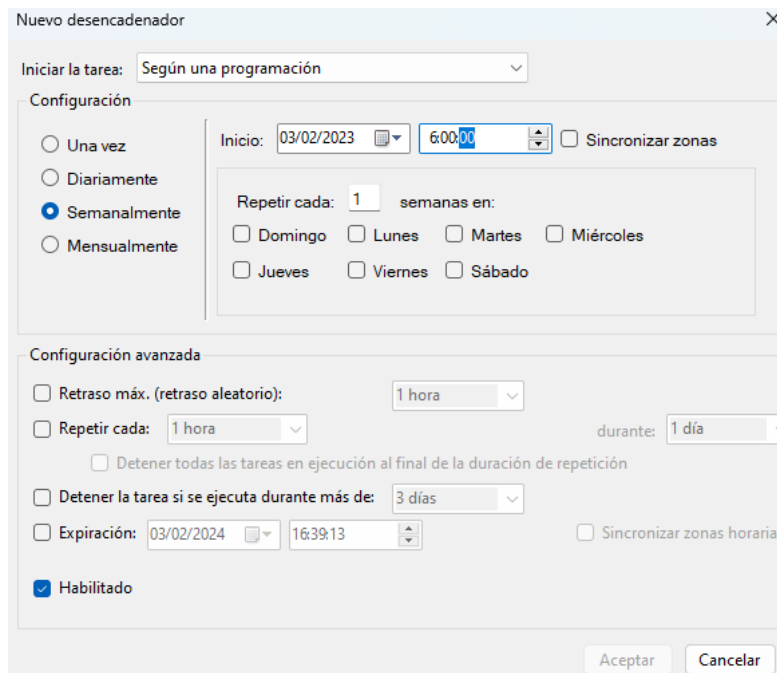
Ahora vamos a seleccionar “Análisis programado de Windows Defender”.

Nombre	E	Desencade...	Hora próxima ej...	Hora última ej...	Resultado de última ejecución	C.
Windows Defender Verification	Listo			03/02/2023 15:36:53	La operación se completó correctamente. (0x0)	
Windows Defender Scheduled Scan	Listo			01/02/2023 19:30:27	El proceso ha terminado de forma inesperada. (0x8007042B)	
Windows Defender Cleanup	Listo			01/02/2023 18:25:03	La operación se completó correctamente. (0x0)	
Windows Defender Cache Maintenance	Listo			01/02/2023 21:06:22	La operación se completó correctamente. (0x0)	

Damos doble click y vamos a “Desencadenadores”.



Y creamos un desencadenador con los parámetros que se nos indican.



Actividad 7.

Descarga e instala el analizador de protocolos de red gratuito "Wireshark". A continuación, inicia una captura en Wireshark, conéctate a una web que no use una conexión cifrada, como por ejemplo www.dgt.es y a otra web que sí la use, como por ejemplo www.juntadeandalucia.es y por último detén la captura de Wireshark.

Realiza los siguientes apartados:

1. Utilizando la herramienta de búsqueda de paquetes ("find packet") busca paquetes que contengan el texto "dgt.es" (marcando la opción "string") dentro de los "packet bytes".
Ejemplo:

Busca un paquete con protocolo HTTP con el mensaje HTTP GET, que corresponde a la petición de la página web www.dgt.es.

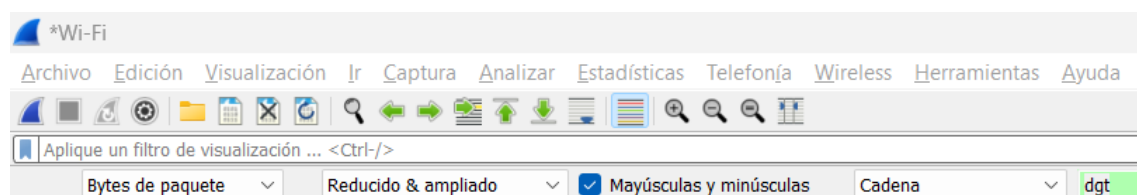
Cuando lo encuentres, haz clic derecho sobre dicho paquete y marca un filtro de conversación ("conversation filter") de tipo IPv4. Esto filtrará toda la conversación entre la máquina virtual y el servidor web de www.dgt.es mostrando todos los paquetes que se intercambiaron mientras se cargaba la web. Realiza una captura de pantalla en la que se muestre el inicio de esta conversación.

2. Realiza el mismo proceso del apartado anterior para filtrar la conversación mantenida con el servidor web que usa cifrado, www.juntadeandalucia.es. Para ello tendrás que eliminar el filtro anterior antes de realizar una nueva búsqueda y aplicar un nuevo filtro.

3. Analiza y compara las conversiones filtradas en los apartados 1 y 2. Para ello muestra una captura de pantalla en la que aparezca la principal diferencia entre ambas conversaciones y explica dicha diferencia.

Antes que nada, debemos descargar e instalar Wireshark.

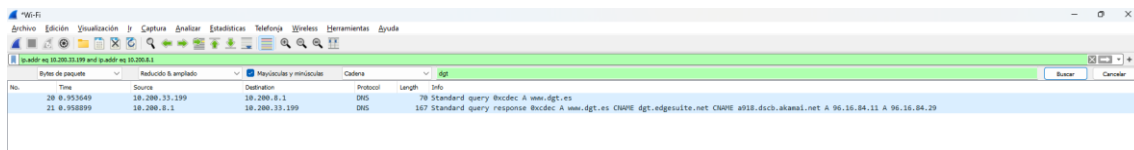
Vamos a configurar los parámetros que nos indica la actividad para que el filtrado de paquetes se realice correctamente.



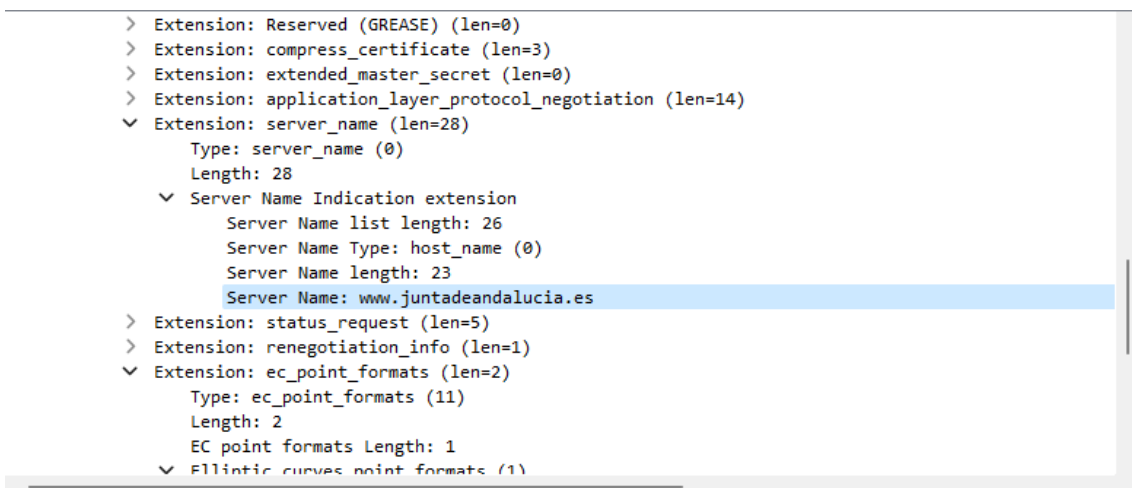
Vamos a entrar en la web de la dgt mientras trackeamos los paquetes que recibe nuestro equipo, y vamos a buscar los que incluyan el nombre de la dgt.



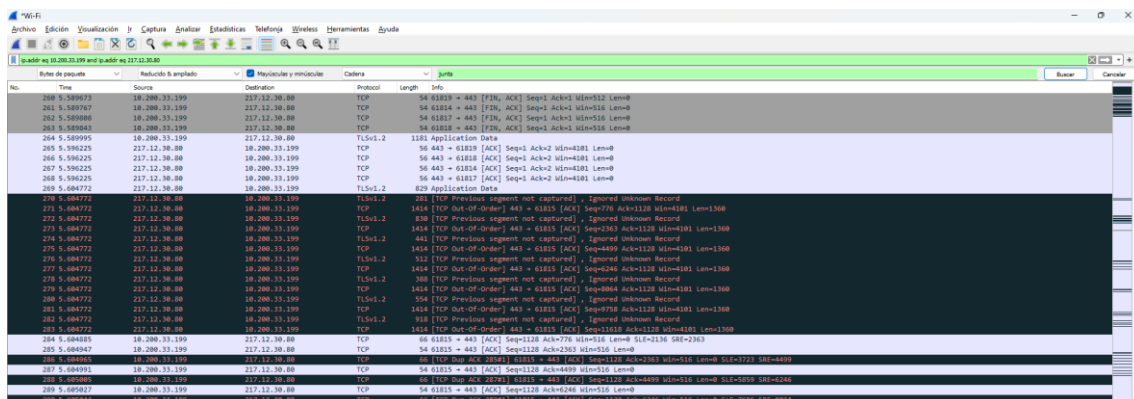
Al aplicar sobre este paquete el filtrado de conexiones IPV4, nos aparecen todos los paquetes que se han intercambiado mientras estábamos trackeando.



Ahora vamos a filtrar paquetes mientras nos conectamos a la web de la junta de andalucia.



Y vamos a filtrar para que nos aparezcan solo los paquetes enviados entre nuestra conexión con la web de la junta.



El propósito de comparar el resultado de ambas conexiones era diferenciar la conexión cifrada HTTPS con la no cifrada HTTP, pero la web de la DGT ahora también usa conexión HTTPS 😞.

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.

Antes que nada, vamos a configurar la clave del router. Por defecto venia 1234 tanto para username como para la contraseña, y vamos a cambiarlas por root.

Account Management ?

Old Username:

1234

✓

Old Password:

....

✓

New Username:

root

New Password:

....

Low Middle High

Confirm New Password:

....

✓

Save

Ahora vamos a configurar la clave de red de nuestro router, y casualmente en la misma interfaz tenemos para cambiar el tipo de cifrado, el cual vamos a poner como WPA2.

2.4GHz | 5GHz

Save

Por último, vamos a activar el cifrado por MAC.

Binding List

 Add Delete

En esta lista encontramos la MAC de los equipos a los que permitimos acceder a nuestra red, seguido de la IP que le asignamos.

Vamos a añadir nuestra MAC ficticia.

--	--	--	--	--	--	--
----	----	----	----	----	----	----

MAC Address:

DC-0A-B3-1B-7E-C0

IP Address:

192.168.0.107

Description:

Direccion ficticia

(Optional)

☒ Enable This Entry

Cancel

OK

Con esta entrada, el equipo con dicha MAC tiene permitido el acceso a nuestra red.