CENTRE ESPECÍFIC
D´EDUCACIÓ A DISTÀNCIA DE
LA COMUNITAT VALENCIANA

ACTIVIDAD EVALUABLE

SEGURIDAD Y ALTA DISPONIBILIDAD

UD4. Sniffing (pág 2) y DOH (pág 10)

Autor: Manuel Fernández

Sniffing: captura de trazas TCP con Wireshark

Se trata de un software gratuito que permite analizar el tráfico red en tiempo real, es un sniffer de red. La herramienta intercepta el tráfico y lo convierte en un formato legible para las personas. Esto hace que sea más fácil identificar qué tráfico está cruzando la red, con qué frecuencia y la latencia que hay entre ciertos saltos.

Instala Wireshark **en Windows** si no lo tienes: https://www.wireshark.org/#download

Se utilizará Wireshark para capturar y examinar **paquetes que se generan entre el navegador de nuestro PC** mediante el protocolo de transferencia de hipertexto (HTTP**) y un servidor Web**, como www.google.com.

Cuando una aplicación, como HTTP se inicia en un host (nuestro PC), se utiliza TCP para establecer una sesión confiable entre los dos hosts (tu PC y el servidor Web). Una PC puede tener varias sesiones TCP simultáneas activas con diversos sitios Web.

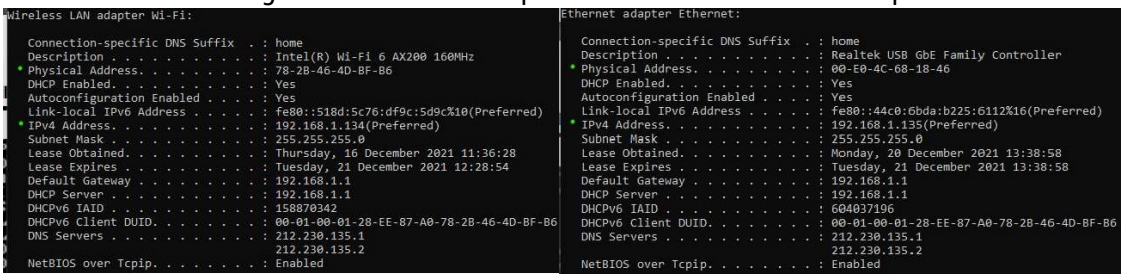
Parte 1: Preparar Wireshark para capturar paquetes

Paso 1: Recuperar las direcciones de tu PC

Para esta práctica deberás buscar la **dirección IP** de tu PC y la dirección física de la tarjeta de interfaz de red (NIC), que también se conoce como **dirección MAC**.

a. Abre una terminal o ventana del símbolo del sistema (escribiendo en el buscador de Windows “CMD”) y escribe “ipconfig /all”, pulsa ENTER.

Si está conectado a internet vía Wi-Fi debes fijarte en el apartado “Wireless LAN adapter Wi-Fi”, si está conectado a internet a través de cable debes fijarte en el apartado “Ethernet adapter Ethernet”.



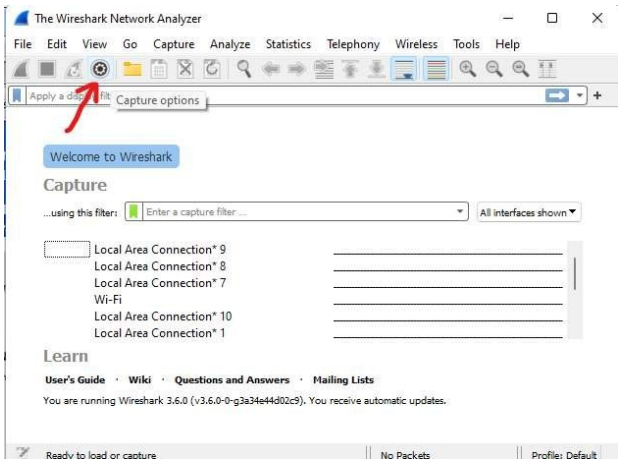
b. Apunta la dirección IP (IPv4 Address) y la MAC (Physical Address)

Dirección IP de tu PC: 192.168.1.16

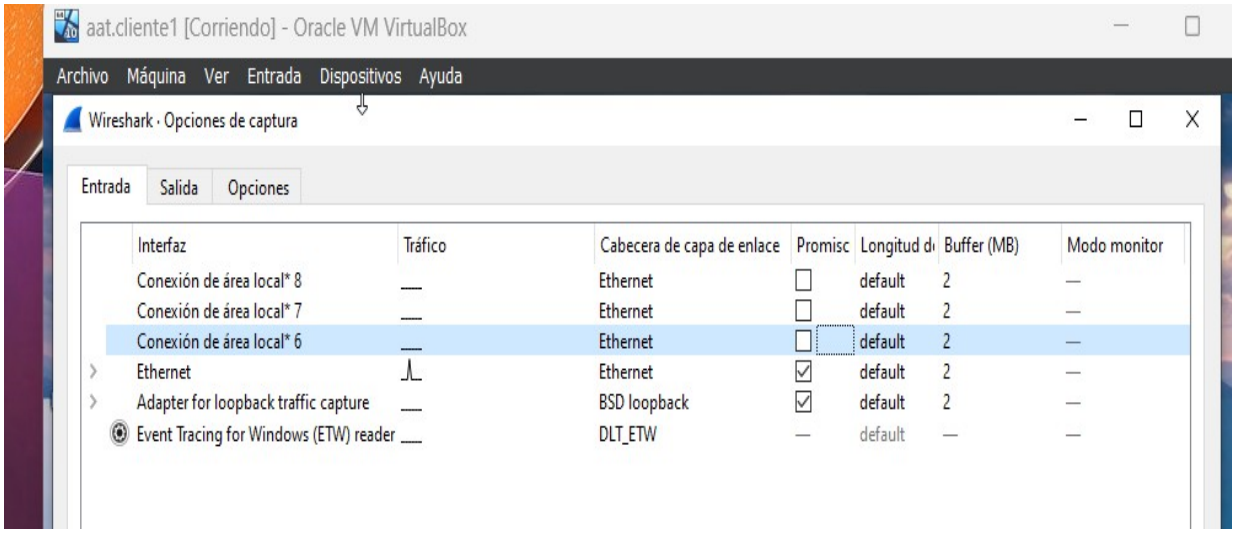
Dirección MAC de tu PC: 08-00-27-40-9B-43

Paso 2: Iniciar Wireshark y seleccionar la interfaz apropiada

a. Inicia Wireshark y pulsa el botón de opciones de captura:



b. Existen varias interfaces en las que capturar tráfico, solo nos interesa la interfaz de Wi-Fi y de Ethernet. Por lo tanto ponemos únicamente en modo promiscuo (captura de tráfico) dichas interfaces:

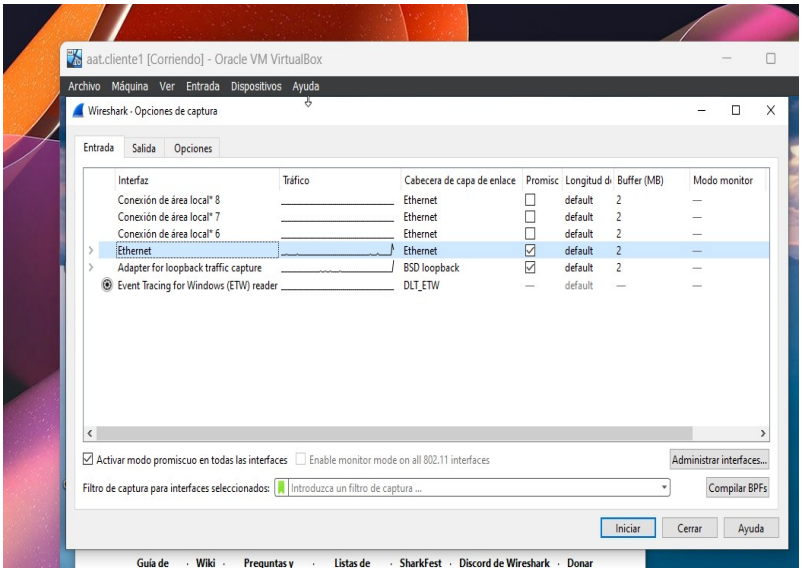


Parte 2: Capturar, localizar y examinar paquetes

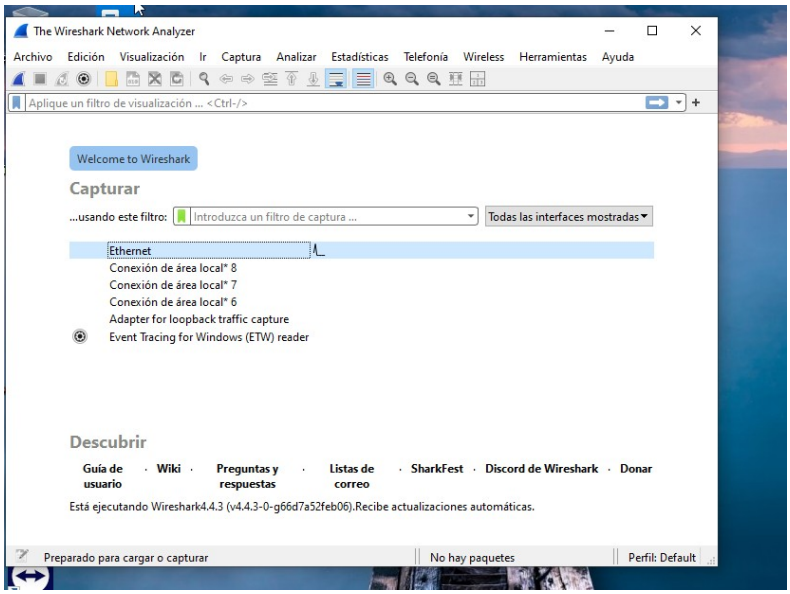
Paso 1: Empezar a capturar datos

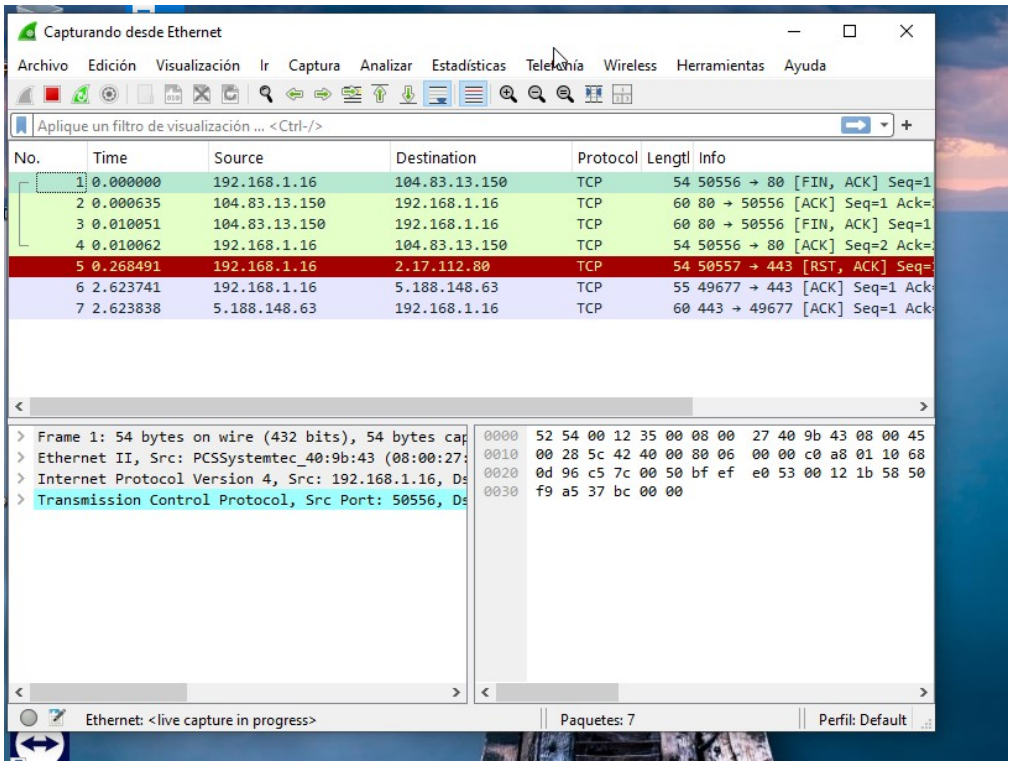
a. Abre el navegador de internet. En esta práctica es importante que no tengas abierta ninguna pestaña de tu navegador ni ningún navegador. Cuantos menos programas con acceso a internet tengas abiertos, mejor

b. Vuelve a Wireshark. La primera vez que capturas datos debes hacerlo desde la ventana de opciones de captura. Selecciona la interfaz que te interesa haciendo clik (Wi-Fi si estás conectado a internet a través de Wi-Fi o Ethernet si estás conectado a través de cable) y pulsa el botón Start.

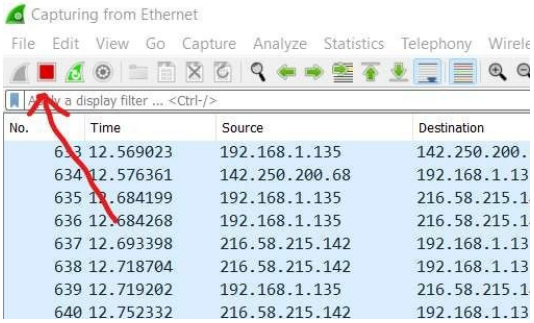


Cierra la ventana. Las próximas veces empezaras a capturar desde el botón de la aleta azul pues elige la misma opción que acabas de realizar:



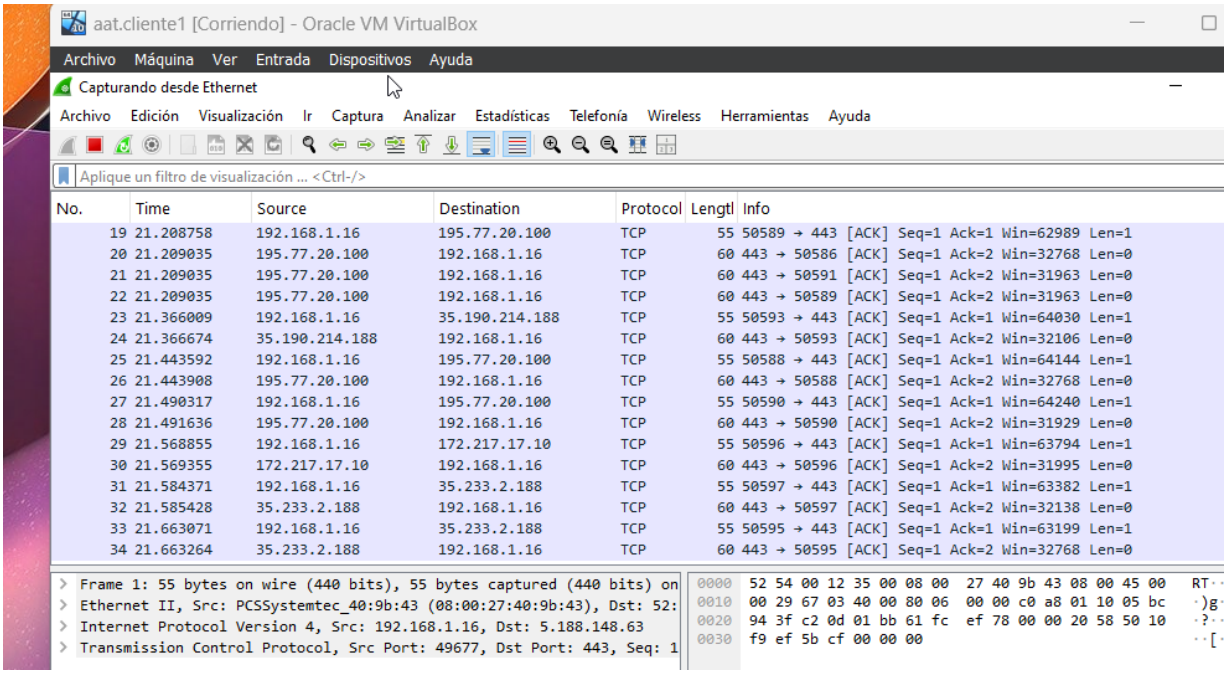


c. Abre el navegador y accede a https://portal.edu.gva.es/ceedcv/es/inicio/ (es importante que escribas tú la URL en el navegador para acceder). Minimice la ventana de Google y vuelva a Wireshark. Detén la captura de datos dándole al botón rojo cuadrado al lado de la aleta azul.

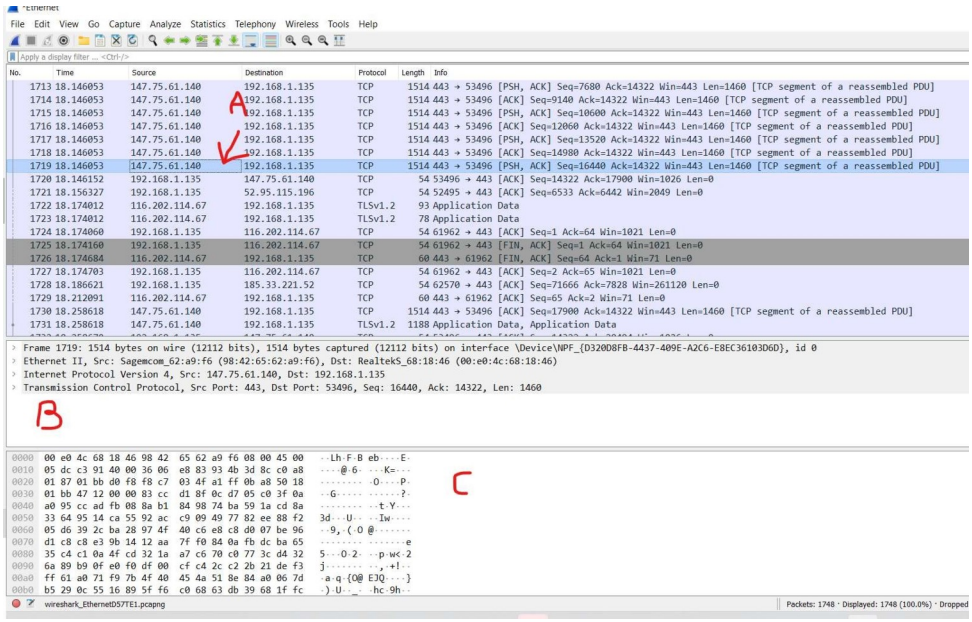


d.

e. Hemos capturado todo el trafico que ha pasado a través de tu interfaz Wi-Fi o Ethernet, dependiendo de tu caso. En la ventana principal de WireShark podemos ver los paquetes capturados.



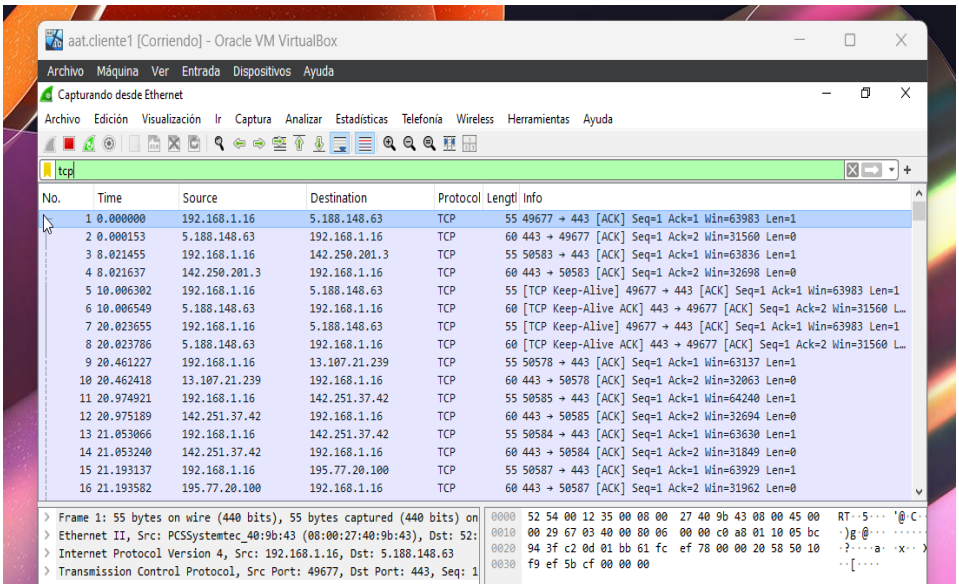
Puedes hacer click en cualquier paquete para ver si información. Por ejemplo, en la siguiente imagen, hemos hecho click en un paquete cualquiera (A). Podemos ver información sobre el paquete en el apartado marcado con el número B y podemos ver la información en bruto del paquete dentro del apartado C en el lado izquierdo en hexadecimal. Wireshark intenta mostrarte la información procesada en el lado derecho del apartado C pero al tratarse de información encriptada solo vemos caracteres sin sentido.



Paso 2: Localizar paquetes

Es muy probable que además de los paquetes transmitidos para acceder a la página web aparezcan muchos otros paquetes. Por lo tanto, vamos a filtrar para encontrar los paquetes que nos interesan.

a. En primer lugar vamos a filtrar por el tipo de paquete. Indicaremos que solo queremos los paquetes TCP escribiendo en el filtro superior la palabra “tcp”.



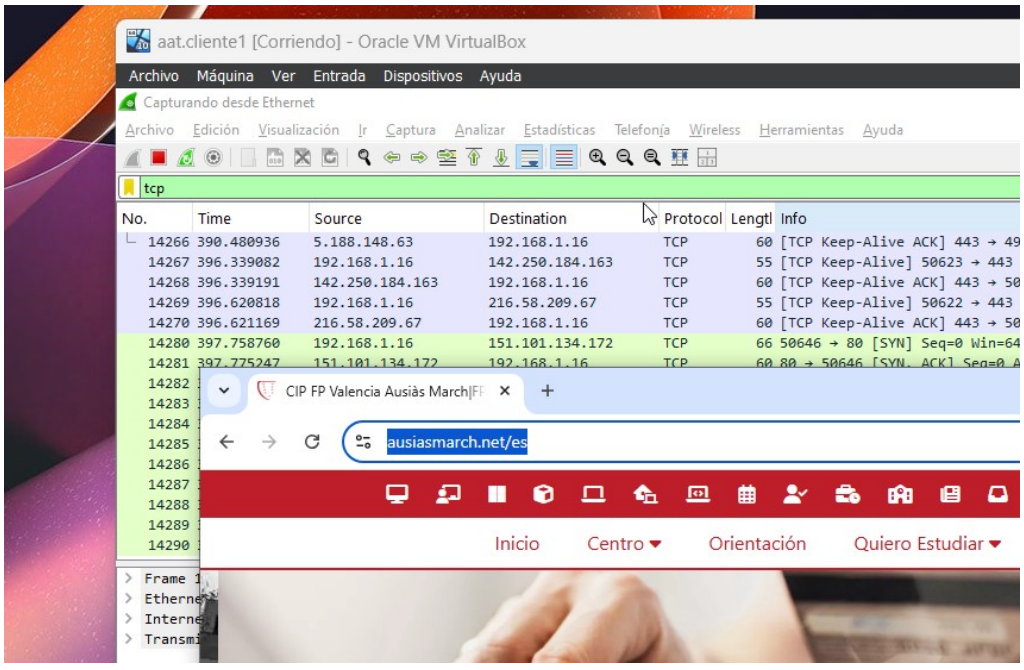
b. Lo normal es que siga habiendo bastantes paquetes, pero menos que antes. Para quedarnos solo con los paquetes que queremos vamos a buscar cuál es la IP de la página web del CEEDCV https://portal.edu.gva.es/ceedcv/es/inicio/. Para ello abrimos la terminal CMD de nuevo y escribimos el siguiente comando el cual pregunta al servidor DNS cual es la IP de ese dominio, en este caso sobre otra web:

```
C:\Program Files (x86)\VMware\VMware Workstation\bin>nslookup www.portal.edu.gva.es/ceedcv/es/inicio/
Servidor:  UnKnown
Address:  2a0c:5a80:0:2::1

*** UnKnown no encuentra www.portal.edu.gva.es/ceedcv/es/inicio/: Non-existent domain
```

nslookup www.ausiasmarch.net Cambio a este nslookup:

```
C:\Program Files (x86)\VMware\VMware W
Servidor:  UnKnown
Address:  2a0c:5a80:0:2::1

Respuesta no autoritativa:
Nombre:  www.ausiasmarch.net
Address:  178.33.158.168
```

Es importante que lo hagas tú también pues es posible que a ti te salga otra IP diferente pues puede haber cambiado. En este caso la IP es 178.33.158.168.

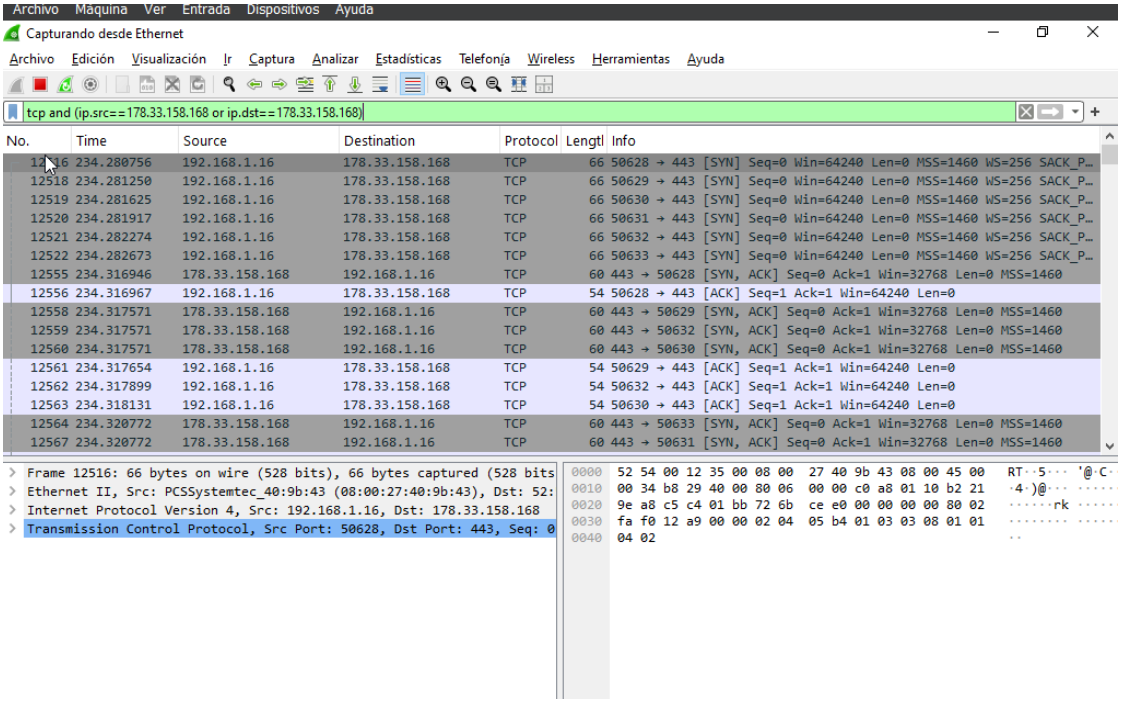


c. Ahora que ya tenemos la ip, vamos a filtrar nuestros paquetes para que además de ser con el protocolo TCP tengan como IP de destino o IP de fuente la IP 178.33.158.168. Para ello pondremos en el filtro la siguiente línea:

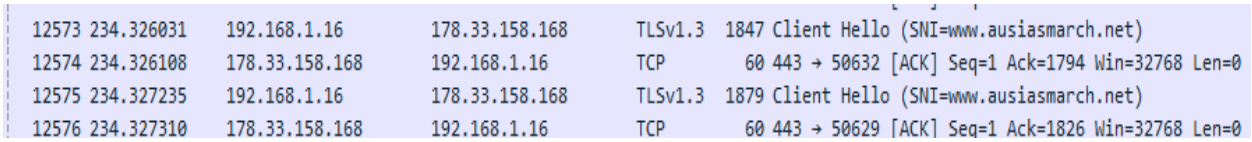
```
tcp and (ip.src==178.33.158.168 or ip.dst==178.33.158.168)
```

Recuerda poner la IP que te ha salido a ti.

El resultado será algo así:

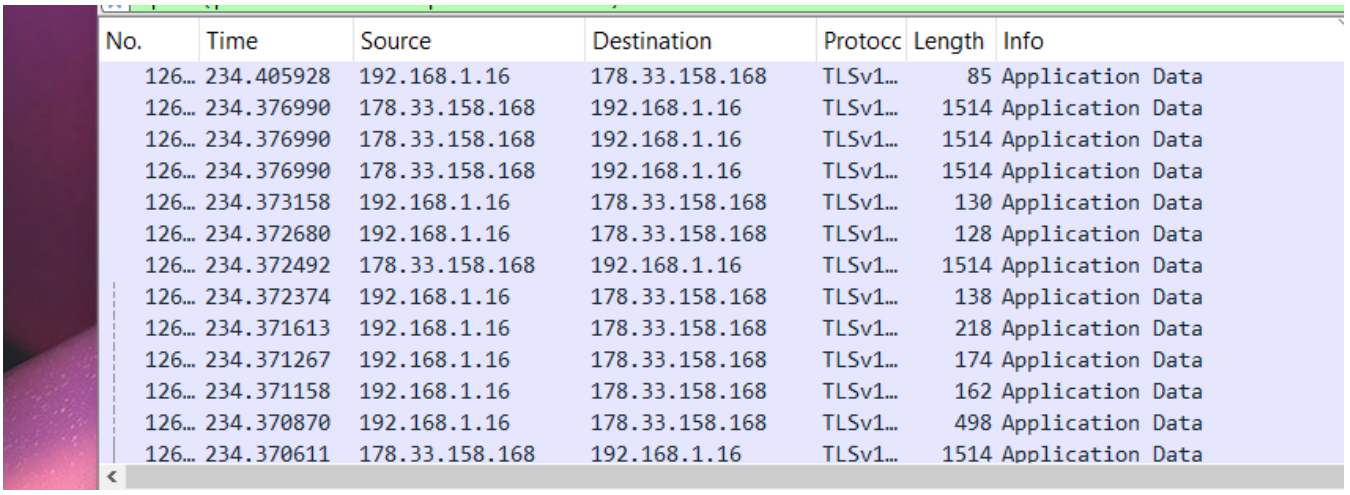


Como podrás comprobar, por ejemplo, en el siguiente paquete:

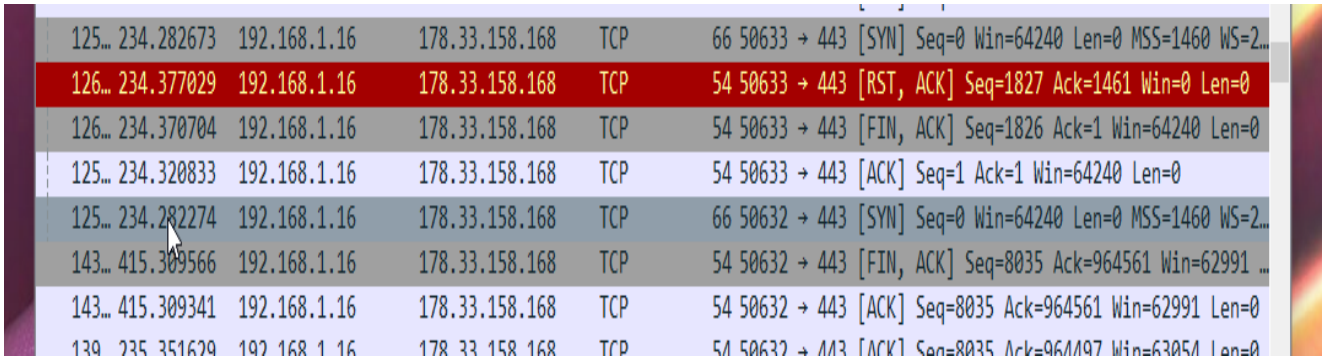


La IP destino es la IP del servidor web donde se aloja la página web y la IP fuente (Source) es la IPv4 de nuestro equipo la cual hemos guardado al principio de la práctica. A ti te aparecerá tu IP en vez de la que aparece en la captura.

d. Si observamos el resto de los paquetes podemos observar la comunicación que ha habido entre nuestro PC y el servidor web para cargar la página en el navegador. Los paquetes en los cuales en el apartado Info pone “Aplication Data” contienen la información que se ha enviado entre los dos hosts. Los paquetes en los cuales pone “[ACK]” son paquetes típicos de una comunicación TCP que utilizan para conseguir una conexión en la cual se aseguran de que la información no se pierde por el camino.



No.	Time	Source	Destination	Protocc	Length	Info
126…	234.405928	192.168.1.16	178.33.158.168	TLSv1…	85	Application Data
126…	234.376990	178.33.158.168	192.168.1.16	TLSv1…	1514	Application Data
126…	234.376990	178.33.158.168	192.168.1.16	TLSv1…	1514	Application Data
126…	234.376990	178.33.158.168	192.168.1.16	TLSv1…	1514	Application Data
126…	234.373158	192.168.1.16	178.33.158.168	TLSv1…	130	Application Data
126…	234.372680	192.168.1.16	178.33.158.168	TLSv1…	128	Application Data
126…	234.372492	178.33.158.168	192.168.1.16	TLSv1…	1514	Application Data
126…	234.372374	192.168.1.16	178.33.158.168	TLSv1…	138	Application Data
126…	234.371613	192.168.1.16	178.33.158.168	TLSv1…	218	Application Data
126…	234.371267	192.168.1.16	178.33.158.168	TLSv1…	174	Application Data
126…	234.371158	192.168.1.16	178.33.158.168	TLSv1…	162	Application Data
126…	234.370870	192.168.1.16	178.33.158.168	TLSv1…	498	Application Data
126…	234.370611	178.33.158.168	192.168.1.16	TLSv1…	1514	Application Data



125…	234.282673	192.168.1.16	178.33.158.168	TCP	66 50633 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2…
126…	234.377029	192.168.1.16	178.33.158.168	TCP	54 50633 → 443 [RST, ACK] Seq=1827 Ack=1461 Win=0 Len=0
126…	234.370704	192.168.1.16	178.33.158.168	TCP	54 50633 → 443 [FIN, ACK] Seq=1826 Ack=1 Win=64240 Len=0
125…	234.320833	192.168.1.16	178.33.158.168	TCP	54 50633 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
125…	234.282274	192.168.1.16	178.33.158.168	TCP	66 50632 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2…
143…	415.309566	192.168.1.16	178.33.158.168	TCP	54 50632 → 443 [FIN, ACK] Seq=8035 Ack=964561 Win=62991 …
143…	415.309341	192.168.1.16	178.33.158.168	TCP	54 50632 → 443 [ACK] Seq=8035 Ack=964561 Win=62991 Len=0
139…	235.351629	192.168.1.16	178.33.158.168	TCP	54 50632 → 443 [ACK] Seq=8035 Ack=964497 Win=63054 Len=0

DNS over HTTPS

Parte 1: ¿Qué es DoH?

Explica qué es y las ventajas y desventajas de usar DNS sobre HTTPS en lugar de DNS únicamente según hemos visto en clase:

- Ventajas:

1. Mejora la integridad ya que gracias al https garantiza que las respuestas dns se modifiquen por servidores intermedios

2. Las redes que bloqueen el trafico o lo alteren utilizando el dns convencional, con el doh no pasa ya que utiliza el puerto 443 el mismo que el trafico normal por https

3. Ganamos privacidad ya que el envio ya no viaja en texto plano sino que lo hace cifrado mediante una conexión https cifrada.

4. Seguridad ante ataques “man-in-the-middle” al estar cifradas es mucho mas difícil que las descifren y modifiquen pero no imposible.

-Desventajas:

1. Dependemos de un servidor externo, confías por ejemplo en CloudFlare o Google para que este maneje satisfactoriamente tus consultas dns y si este guarda registros ya estarían invadiendo la privacidad.

2. No todos los dispositivos, redes o aplicaciones soportan DoH. Algunos Firewall o sistemas de filtrado pueden no permitir o reconocer trafico Doh, depende mucho de las Políticas de seguridad de la red.

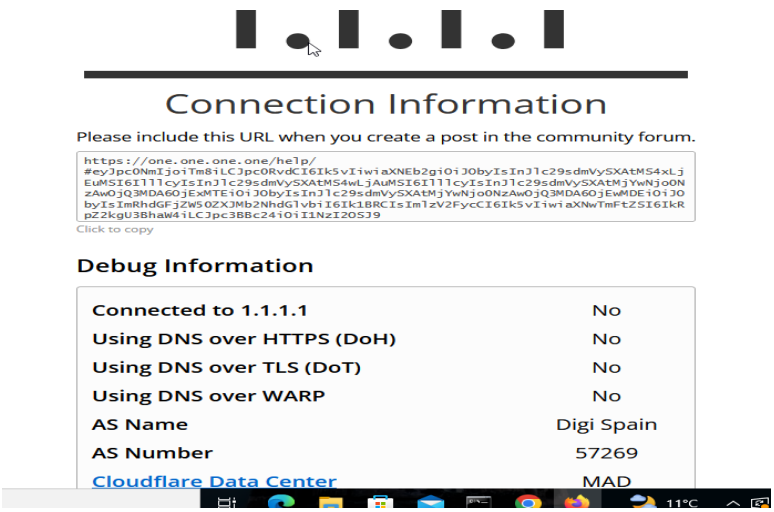
3. Dificultad para monitorizar y controlar el trafico DNS, ya que estas dejaran de ser visibles en su forma original.

4. Disminución del rendimiento debido a la necesidad de establecer conexiones https y su cifrado correspondiente en comparación al dns tradicional, aunque cabe destacar que en muy pocos casos de uso diario se notaria la diferencia.

Parte 2: Activar el uso de DoH en un navegador.

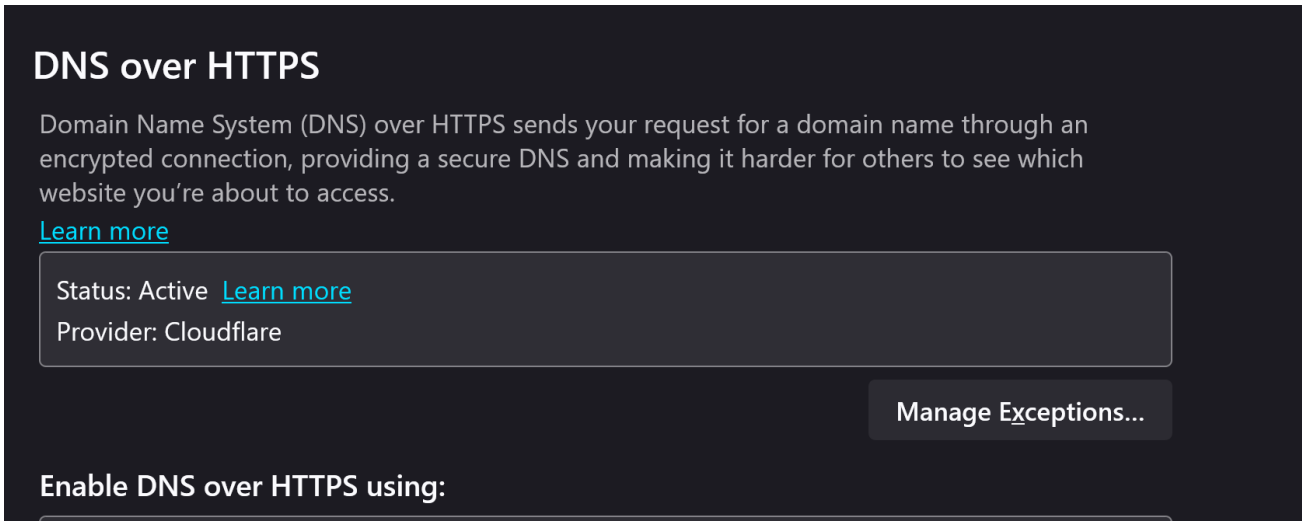
En esta práctica deberás tener instalado el navegador Firefox en tu ordenador Windows. No funciona igual en Chrome

a. Abre Firefox y entra en la página https://1.1.1.1/help y comprueba que no estamos usando el servicio DoH (en este caso de CloudFlare).

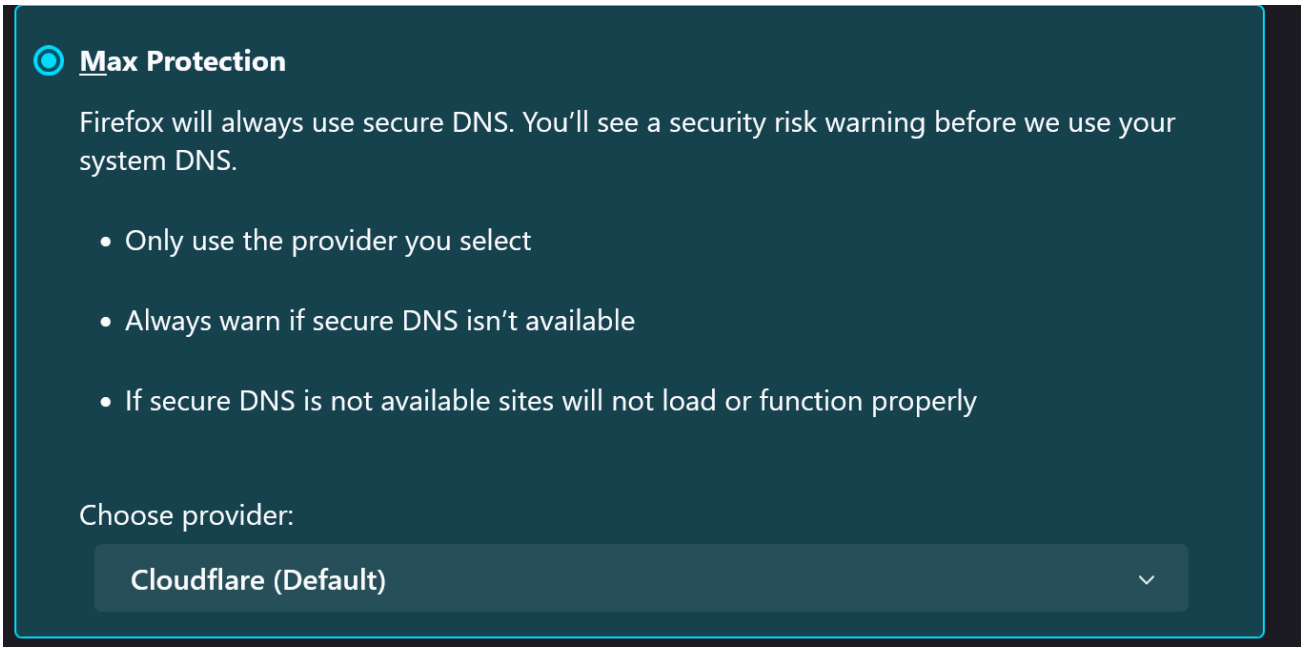


b. Por otro lado y sin cerrar la pestaña que hemos abierto, abre los ajustes de Firefox.

c. Tendremos que buscar el apartado de seguridad y privacidad, bajar hasta abajo del todo y activar la opción max protection debajo de:



d. Nos saldrá por defecto la opción de CloudFlare:



e. Ahora, vuelve a la otra pestaña, refréscala y comprueba de nuevo si tienes activado el uso de DoH. Deberá aparecer como “yes”.

Debug Information

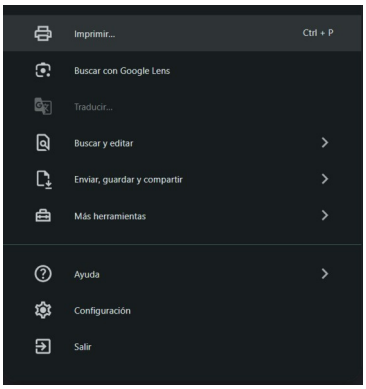
Connected to 1.1.1.1	Yes
Using DNS over HTTPS (DoH)	Yes
Using DNS over TLS (DoT)	No
Using DNS over WARP	No
AS Name	Cloudflare
AS Number	13335
Cloudflare Data Center	MAD

f. **Ahora, comprueba si el DoH esta activo en Chrome**

Debug Information

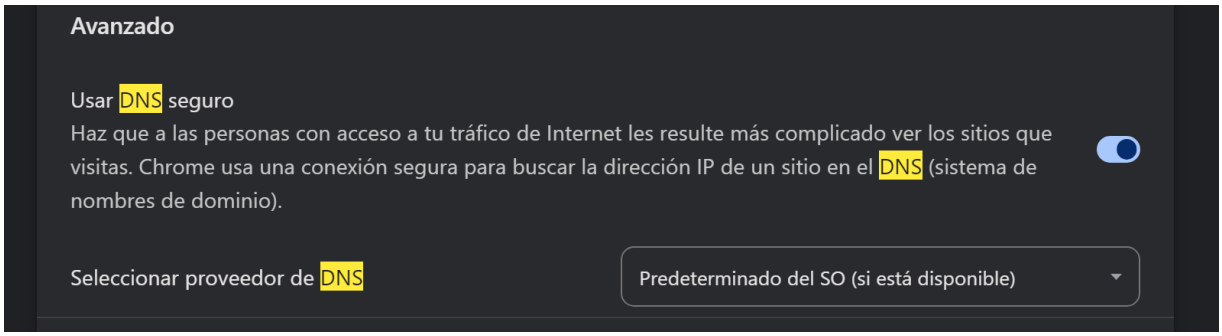
Connected to 1.1.1.1	No
Using DNS over HTTPS (DoH)	No
Using DNS over TLS (DoT)	No
Using DNS over WARP	No
AS Name	Digi Spain
AS Number	57269
Cloudflare Data Center	MAD

Para activarlo nos iremos a la configuración de Google:

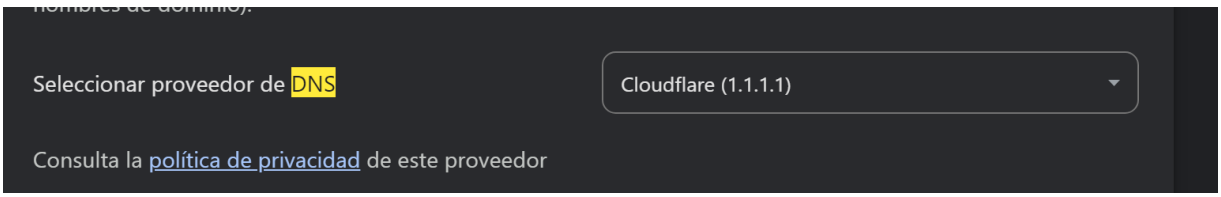


Aparecerá el menú y en el buscador pondremos dns:

Clicaremos en seguridad y bajaremos hasta dns:



Donde pone seleccionar proveedor pondremos CloudFlare:



Ahora comprobaremos que funciona el DOH en Chrome: