

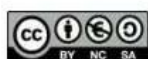
ACTIVIDAD EVALUABLE

SEGURIDAD Y ALTA DISPONIBILIDAD

UD4. Sniffing (pág 2) y DOH (pág 10)

Autor: Manuel Fernández

Licencia Creative Commons



Reconocimiento – NoComercial – CompartirIgual (by-nc-sa): No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.

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.

- 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".

```
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : home
Description . . . . . : Intel(R) Wi-Fi 6 AX200 160MHz
Physical Address. . . . . : 78-2B-46-4D-BF-B6
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::518d:5c76:df9c:5d9c%10(Preferred)
IPv4 Address. . . . . : 192.168.1.134(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, 16 December 2021 11:36:28
Lease Expires . . . . . : Tuesday, 21 December 2021 12:20:54
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 158870342
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-EE-87-A0-78-2B-46-4D-BF-B6
DNS Servers . . . . . : 212.230.135.1
                        212.230.135.2
NetBIOS over Tcpip. . . . . : Enabled

Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : home
Description . . . . . : Realtek USB GbE Family Controller
Physical Address. . . . . : 00-E0-4C-08-18-46
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::44c0:6bda:b225:6112%16(Preferred)
IPv4 Address. . . . . : 192.168.1.135(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, 20 December 2021 13:30:58
Lease Expires . . . . . : Tuesday, 21 December 2021 13:30:58
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 604037196
DHCPv6 Client DUID. . . . . : 00-01-00-01-28-EE-87-A0-78-2B-46-4D-BF-B6
DNS Servers . . . . . : 212.230.135.1
                        212.230.135.2
NetBIOS over Tcpip. . . . . : Enabled
```

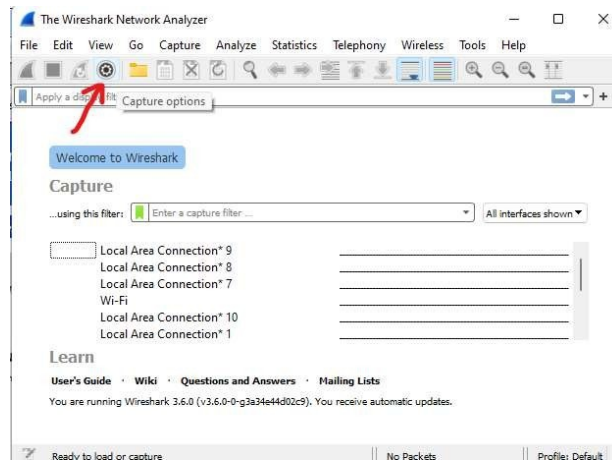
b. Apunta la dirección IP (IPv4 Address) y la MAC (Physical Address)

Dirección IP de tu PC: 192.168.1.16

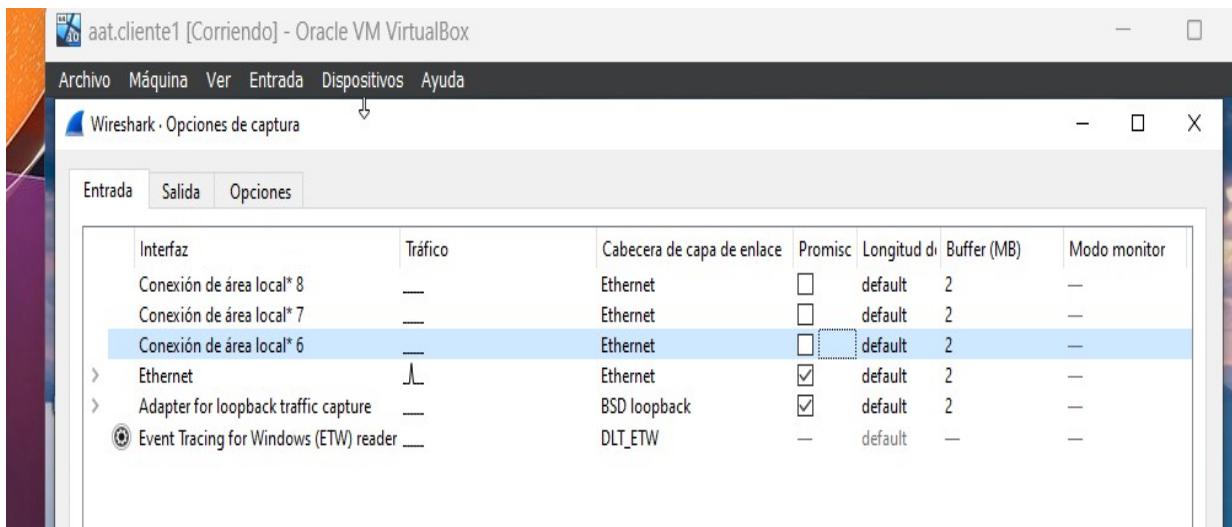
Dirección MAC de tu PC: 08-00-27-40-9B-43

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:



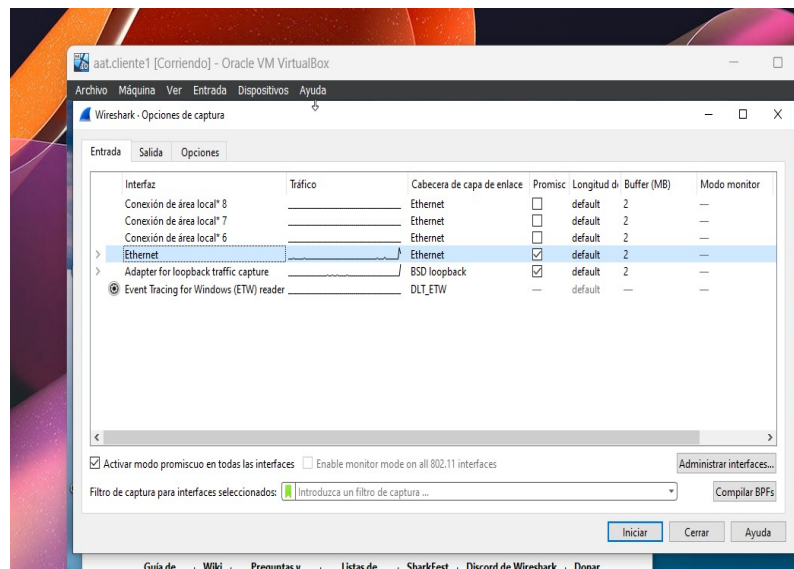
Parte 2: Capturar, localizar y examinar paquetes

Paso 1: Empezar a capturar datos

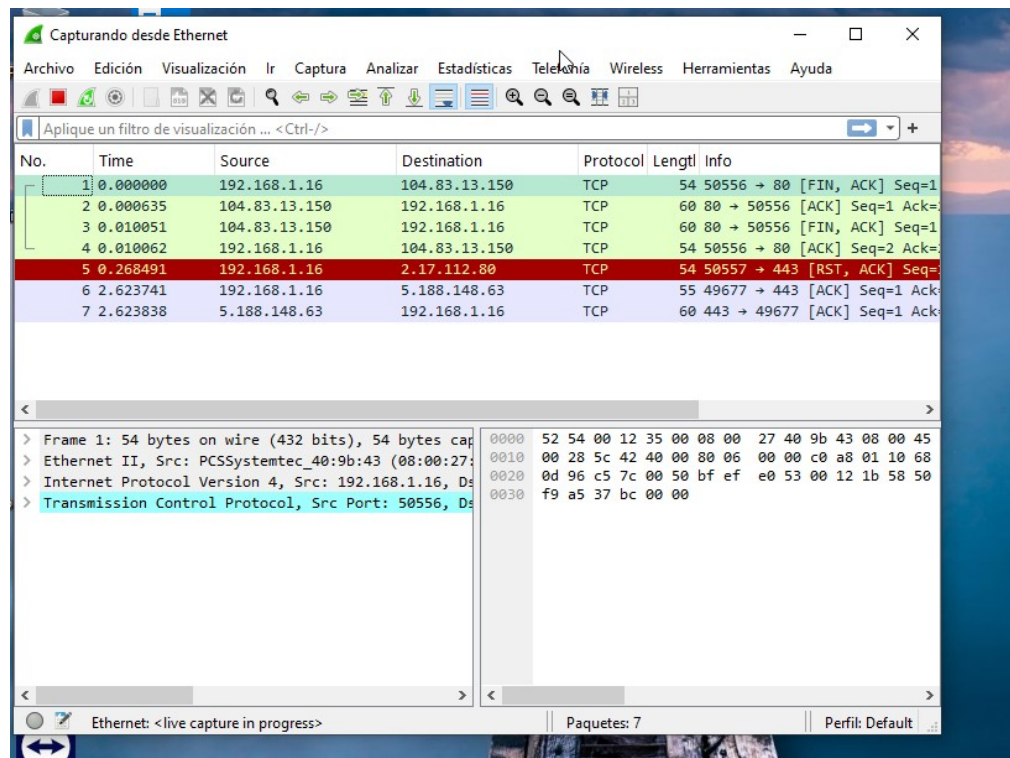
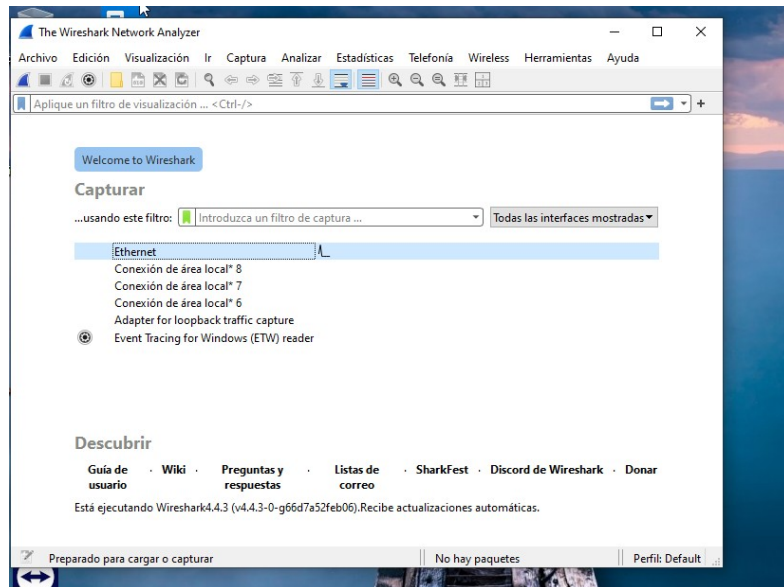
- a. Abre el navegador de internet. En esta práctica es importante que no tengas abierta ninguna pestaña de tu navegador ni ningún navegador. Cuantos menos programas con acceso a internet tengas abiertos, mejor



- 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 clic (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.



Capturing from Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wirel

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination
633	12.569023	192.168.1.135	142.250.200.
634	12.576361	142.250.200.68	192.168.1.13
635	12.684199	192.168.1.135	216.58.215.1
636	12.684268	192.168.1.135	216.58.215.1
637	12.693398	216.58.215.142	192.168.1.13
638	12.718704	216.58.215.142	192.168.1.13
639	12.719202	192.168.1.135	216.58.215.1
640	12.752332	216.58.215.142	192.168.1.13

- 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.

aat.ciente1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Capturando desde Ethernet

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplice un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
19	21.208758	192.168.1.16	195.77.20.100	TCP	55	50589 → 443 [ACK] Seq=1 Ack=1 Win=62989 Len=1
20	21.209035	195.77.20.100	192.168.1.16	TCP	60	443 → 50586 [ACK] Seq=1 Ack=2 Win=32768 Len=0
21	21.209035	195.77.20.100	192.168.1.16	TCP	60	443 → 50591 [ACK] Seq=1 Ack=2 Win=31963 Len=0
22	21.209035	195.77.20.100	192.168.1.16	TCP	60	443 → 50589 [ACK] Seq=1 Ack=2 Win=31963 Len=0
23	21.366009	192.168.1.16	35.190.214.188	TCP	55	50593 → 443 [ACK] Seq=1 Ack=1 Win=64030 Len=1
24	21.366674	35.190.214.188	192.168.1.16	TCP	60	443 → 50593 [ACK] Seq=1 Ack=2 Win=32106 Len=0
25	21.443592	192.168.1.16	195.77.20.100	TCP	55	50588 → 443 [ACK] Seq=1 Ack=1 Win=64144 Len=1
26	21.443908	195.77.20.100	192.168.1.16	TCP	60	443 → 50588 [ACK] Seq=1 Ack=2 Win=32768 Len=0
27	21.490317	192.168.1.16	195.77.20.100	TCP	55	50590 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=1
28	21.491636	195.77.20.100	192.168.1.16	TCP	60	443 → 50590 [ACK] Seq=1 Ack=2 Win=31929 Len=0
29	21.568855	192.168.1.16	172.217.17.10	TCP	55	50596 → 443 [ACK] Seq=1 Ack=1 Win=63794 Len=1
30	21.569355	172.217.17.10	192.168.1.16	TCP	60	443 → 50596 [ACK] Seq=1 Ack=2 Win=31995 Len=0
31	21.584371	192.168.1.16	35.233.2.188	TCP	55	50597 → 443 [ACK] Seq=1 Ack=1 Win=63382 Len=1
32	21.585428	35.233.2.188	192.168.1.16	TCP	60	443 → 50597 [ACK] Seq=1 Ack=2 Win=32138 Len=0
33	21.663071	192.168.1.16	35.233.2.188	TCP	55	50595 → 443 [ACK] Seq=1 Ack=1 Win=63199 Len=1
34	21.663264	35.233.2.188	192.168.1.16	TCP	60	443 → 50595 [ACK] Seq=1 Ack=2 Win=32768 Len=0

> Frame 1: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on
 > Ethernet II, Src: PCSSystemtec_40:9b:43 (08:00:27:40:9b:43), Dst: 52:
 > Internet Protocol Version 4, Src: 192.168.1.16, Dst: 5.188.148.63
 > Transmission Control Protocol, Src Port: 49677, Dst Port: 443, Seq: 1

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.

Wireshark packet capture showing a list of network packets. A red arrow points to packet 1719, which is a TCP segment. Below the packet list, the packet details pane shows the structure of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. A red 'B' is written next to the packet list, and a red 'C' is written next to the packet details pane.

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.

- 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”.

Wireshark packet capture showing a list of network packets. The filter bar at the top shows 'tcp'. The packet list shows a list of TCP segments. The packet details pane shows the structure of the packet, including the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header. A red 'B' is written next to the packet list, and a red 'C' is written next to the packet details pane.

- 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

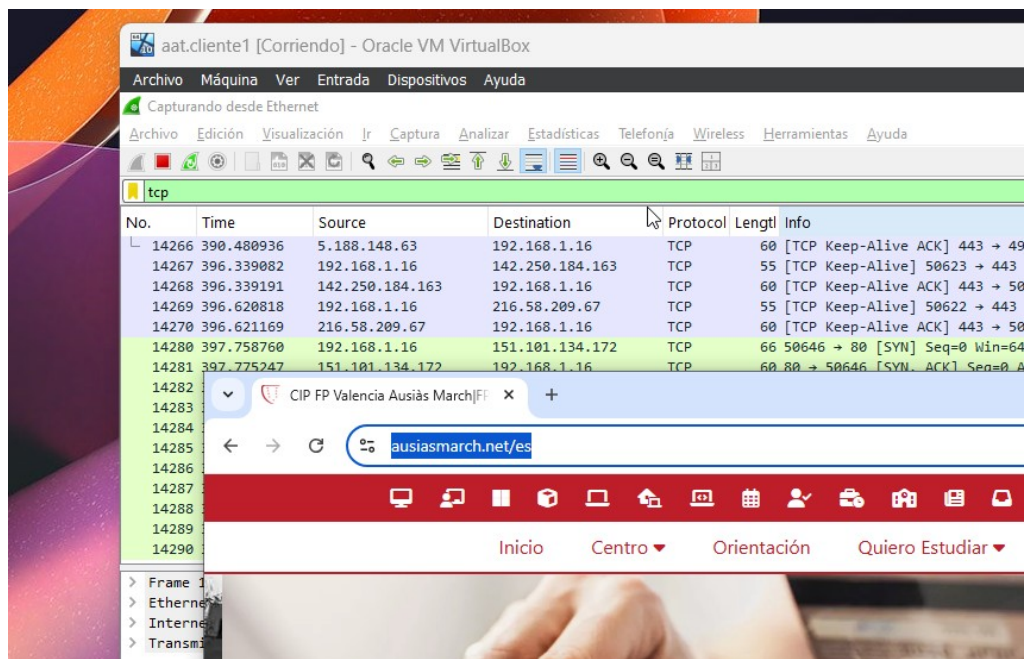
*** UnKnown no encuentra www.portal.edu.gva.es/ceedcv/es/inicio/: Non-existent domain
```

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:

The screenshot shows the Wireshark interface with the packet capture filter `tcp and (ip.src==178.33.158.168 or ip.dst==178.33.158.168)` applied. The packet list shows several TCP packets between 192.168.1.16 and 178.33.158.168. The selected packet 12516 is expanded, showing the Ethernet II header, Internet Protocol Version 4 header, and Transmission Control Protocol header.

No.	Time	Source	Destination	Protocol	Length	Info
12516	234.280756	192.168.1.16	178.33.158.168	TCP	66	50628 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
12518	234.281250	192.168.1.16	178.33.158.168	TCP	66	50629 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
12519	234.281625	192.168.1.16	178.33.158.168	TCP	66	50630 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
12520	234.281917	192.168.1.16	178.33.158.168	TCP	66	50631 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
12521	234.282274	192.168.1.16	178.33.158.168	TCP	66	50632 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
12522	234.282673	192.168.1.16	178.33.158.168	TCP	66	50633 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_P...
12555	234.316946	178.33.158.168	192.168.1.16	TCP	60	443 → 50628 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
12556	234.316967	192.168.1.16	178.33.158.168	TCP	54	50628 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
12558	234.317571	178.33.158.168	192.168.1.16	TCP	60	443 → 50629 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
12559	234.317571	178.33.158.168	192.168.1.16	TCP	60	443 → 50632 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
12560	234.317571	178.33.158.168	192.168.1.16	TCP	60	443 → 50630 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
12561	234.317654	192.168.1.16	178.33.158.168	TCP	54	50629 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
12562	234.317899	192.168.1.16	178.33.158.168	TCP	54	50632 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
12563	234.318131	192.168.1.16	178.33.158.168	TCP	54	50630 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
12564	234.320772	178.33.158.168	192.168.1.16	TCP	60	443 → 50633 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460
12567	234.320772	178.33.158.168	192.168.1.16	TCP	60	443 → 50631 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MSS=1460

Frame 12516: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: PCSSystemtec_40:9b:43 (08:00:27:40:9b:43), Dst: 52:54:00:12:35:00
Internet Protocol Version 4, Src: 192.168.1.16, Dst: 178.33.158.168
Transmission Control Protocol, Src Port: 50628, Dst Port: 443, Seq: 0

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

12573	234.326031	192.168.1.16	178.33.158.168	TLSv1.3	1847	Client Hello (SNI=www.ausiasmarch.net)
12574	234.326108	178.33.158.168	192.168.1.16	TCP	60	443 → 50632 [ACK] Seq=1 Ack=1794 Win=32768 Len=0
12575	234.327235	192.168.1.16	178.33.158.168	TLSv1.3	1879	Client Hello (SNI=www.ausiasmarch.net)
12576	234.327310	178.33.158.168	192.168.1.16	TCP	60	443 → 50629 [ACK] Seq=1 Ack=1826 Win=32768 Len=0

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 “Application 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	Protoc	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...	235.351620	192.168.1.16	178.33.158.168	TCP	54	50632 → 443 [ACK] Seq=8035 Ack=964561 Win=62991 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).



```
https://one.one.one.one/help/
#eyJpc0NoIjoiTm81Cjpc0RvdGI6Iks1v1wiIiwiaXNBJ2giOiJ0byIsInJlCj29sdmVYXATM54xlj.
EUMS16T117cyIsInJlCj29sdmVYXATM54xljAUMS16T117cyIsInJlCj29sdmVYXATM54xljWjYn0o
zAw0Q3MDA60jcxMTE0oiJ0byIsInJlCj29sdmVYXATM54xljWjYn0oZAw0Q3MDA60jcxMTE0oiJ0
byIsInJlCj29sdmVYXATM54xljWjYn0oZAw0Q3MDA60jcxMTE0oiJ0byIsInJlCj29sdmVYXATM54xlj
pZ2kgU3RhbmR4IjL3Cj3B6C24y0iIiIN2120S9J
```

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

- 
- Sincronizar y guardar datos Iniciar sesión
- Nueva pestaña Ctrl+T
 - Nueva ventana Ctrl+N
 - Nueva ventana privada Ctrl+Mayús.+P
 - Marcadores >
 - Historial >
 - Descargas Ctrl+J
 - Contraseñas
 - Complementos y temas Ctrl+Mayús.+A
 - Imprimir... Ctrl+P
 - Guardar como... Ctrl+S
 - Buscar en la página... Ctrl+F
 - Tamaño - 100% + ↗
 - Ajustes** ←
 - Más herramientas >
 - Ayuda >
 - Salir Ctrl+Mayús.+Q

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

DNS over HTTPS

Domain Name System (DNS) over HTTPS sends your request for a domain name through an encrypted connection, providing a secure DNS and making it harder for others to see which website you're about to access.

[Learn more](#)

Status: Active [Learn more](#)

Provider: Cloudflare

Manage Exceptions...

Enable DNS over HTTPS using:

- d. Nos saldrá por defecto la opción de CloudFlare:

☒ **Max Protection**

Firefox will always use secure DNS. You'll see a security risk warning before we use your system DNS.

- Only use the provider you select
- Always warn if secure DNS isn't available
- If secure DNS is not available sites will not load or function properly

Choose provider:

Cloudflare (Default)



- 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

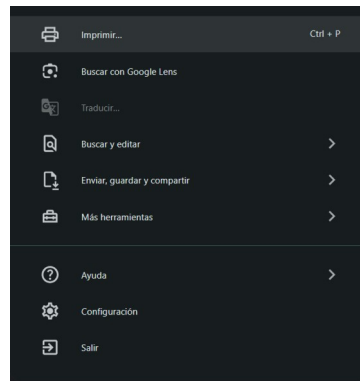
Connected to 1.1.1.1	Yes
Using DNS over HTTPS (DoH)	Yes
Using DNS over TLS (DoT)	No
Using DNS over WARP	No
AS Name	Cloudflare
AS Number	13335
Cloudflare Data Center	MAD

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

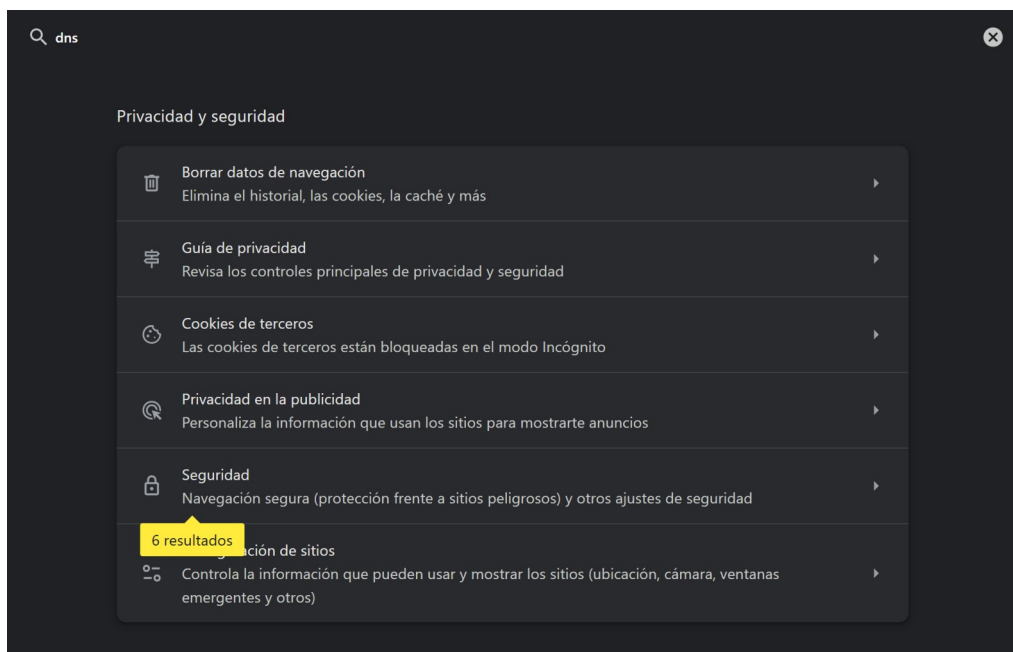
Debug Information

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

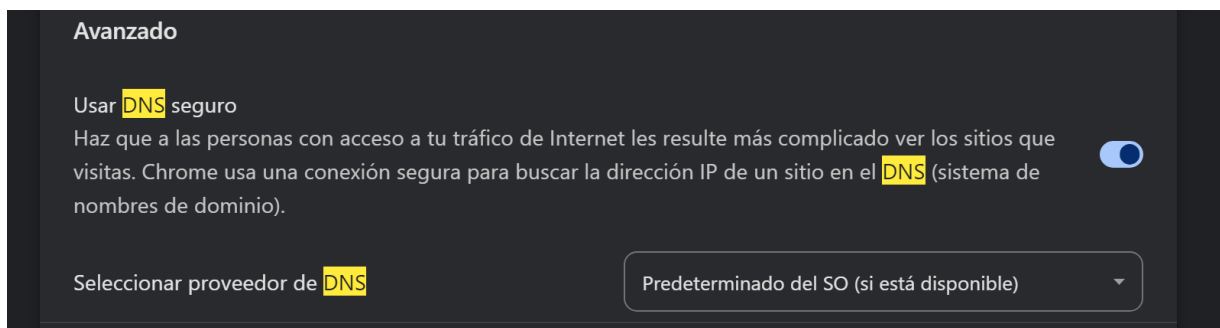
Para activarlo nos iremos a la configuración de Google:



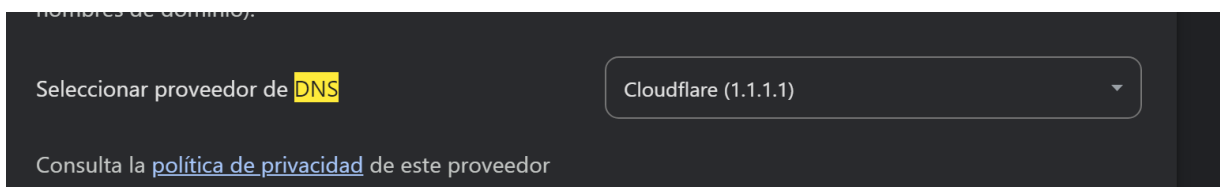
Aparecerá el menú y en el buscador pondremos dns:



Clicaremos en seguridad y bajaremos hasta dns:



Donde pone seleccionar proveedor pondremos CloudFlare:



Ahora comprobaremos que funciona el DOH en Chrome:

