

SEMINARIO 2: HAZLO TÚ MISMO – 2

Analicemos herramientas para entender y medir las transmisiones que hacen nuestras aplicaciones y sitios web.

Utiliza Google Chrome para realizar este ejercicio.

APARTADO 1

Este ejercicio tiene como objetivo que los estudiantes comprendan el funcionamiento de *DNS over HTTPS* (DoH), realizando consultas reales y aprendiendo a interpretar las respuestas en formato JSON. Para ello, se hace necesario:

1. Comprender qué es *DNS over HTTPS* (DoH) y por qué se usa.
2. Realizar consultas DNS usando el servicio público de Google DoH.
3. Interpretar las respuestas JSON: estado, flags, preguntas, respuestas, TTL.
4. Diferenciar distintos tipos de registros DNS (A, AAAA, MX, TXT).

Para realizar este ejercicio se utilizará la API de DNS de Google, Endpoint:

<https://dns.google/resolve>

Comencemos por lo más básico. Abre en tu navegador

<https://dns.google/resolve?name=www.cloudflare.com&type=A>

Cuando utilizamos “type=A”, estamos solicitando su dirección IPv4. Por tanto, ¿cuál es la dirección IPv4 de www.cloudflare.com? Identifica el campo Status; observa el array “Answer” y observa específicamente el TTL.

- Analiza el array “Answer”.
- Observa el campo TTL.

Además, al inicio verás una serie de datos y flags:

- Status: 0 → Indica que no hay error
- TC (*Truncated*): false → la respuesta no fue truncada.
- RD (*Recursion Desired*): true → el cliente pidió resolución recursiva.
- RA (*Recursion Available*): true → el servidor (Google DNS) sí ofrece resolución recursiva.
- AD (*Authenticated Data*): true → la respuesta está validada con DNSSEC, es decir, es auténtica y está no manipulada.
- CD (*Checking Disabled*): false → la validación DNSSEC no está desactivada.

Ahora, realiza la misma consulta con la web de la Universidad de Córdoba (uco.es). ¿Cambia algo? ¿Hay algún dato de respuesta que motive tu interés?

Comprobemos si Cloudflare.com tiene IPv6. Para eso debes utilizar “type=AAAA”.

<https://dns.google/resolve?name=www.cloudflare.com&type=AAAA>

Pregunta: ¿Tiene el servidor de la Universidad de Córdoba una IPv6? ¿Y el de la Universidad de Málaga?

Puedes intentar averiguar la información de registro de un dominio con los tipos “MX” para los servidores de correo electrónico, y “TXT” para registros de texto.

APARTADO 2

Comprobemos qué protocolo HTTP está utilizando un determinado sitio. Hay dos formas de hacerlo. La más sencilla es mediante las herramientas de desarrollador del navegador. Para ello, activa las “herramientas de desarrollador” (F12 o clic derecho → “Inspeccionar”).

Ve a la pestaña **Red (Network)** y activa la columna **Protocolo** (clic derecho en cabecera de la tabla).

Abre primero la URL: <https://es.wikipedia.org>

En la ventana de búsqueda de la Wikipedia, escribe la cadena de búsqueda “CURL”. Se deberá abrir automáticamente la URL: <https://es.wikipedia.org/wiki/CURL>

Analizando las herramientas de desarrollador, responde a las siguientes preguntas:

- ¿Qué protocolo utiliza Wikipedia en su respuesta a nuestra solicitud?
- ¿Qué información están dando el gráfico y el resto de las columnas de información?

Esto mismo se puede hacer utilizando la herramienta de línea de comando “curl”, que resulta mucho más completa para analizar y trabajar con solicitudes HTTP. **Opcionalmente**, puedes intentar instalarla y probarla. En caso de que así lo hagas, cuenta tu experiencia (incluyendo alguna captura) e, incluso, puedes presentar algún tipo de asistencia al resto de compañeros sobre la herramienta (cómo descargarla, cómo invocarla desde la CLI, etc.)

APARTADO 3

1. Abre el vídeo de “The Mother of All Demos, presented by Douglas Engelbart” en YouTube (video presentación de aproximadamente 1 hora y 40 minutos).
2. Ve a la pestaña **Red (Network)** y marca estas opciones:
 - Activar columna **Protocolo** (clic derecho en cabecera de la tabla).
 - Activar columna **ID de conexión**.
 - Marca la casilla **Inhabilitar caché** para ver peticiones reales.
3. Espera y reproduce el vídeo durante al menos 30 segundos.
4. Observa:
 - Qué protocolo aparece en la columna (**h2**, **h3**...).
 - Qué tipo de recursos ves (videoplayback, watchtime, qoe).
 - Cómo se repiten los fragmentos de vídeo/audio.
 - Si varios fragmentos comparten la misma **ID de conexión**.

Comprobarás que aparecen rutas como “videoplayback?...” Son fragmentos de vídeo/audio que YouTube va descargando dinámicamente. Por su parte, “watchtime?...” y “qoe?...” son peticiones de telemetría, esto es, el cliente informa a YouTube de métricas como el estado de reproducción, la calidad del servicio, o eventos de usuario. Con estos datos, Youtube es capaz, por ejemplo, de reducir la calidad de un video para que no se penalice la experiencia de usuario.

Realiza un análisis de las tramas que se reciben y qué se deben, el estado, qué protocolo se está utilizando, qué script es el iniciador, el peso de la trama descargada, la latencia y el id de conexión.

Analiza la situación y responde a las siguientes preguntas:

- ¿Por qué hay distintos IDs de conexión para el mismo video?
- ¿Por qué las tramas tienen tamaños pequeños si es un video largo?
- ¿Por qué hay tramas de estado 204 (No content)?
- ¿Cómo pueden conseguirse estas latencias bajas?