Práctica 2.1: Protocolo HTTP

Objetivo:

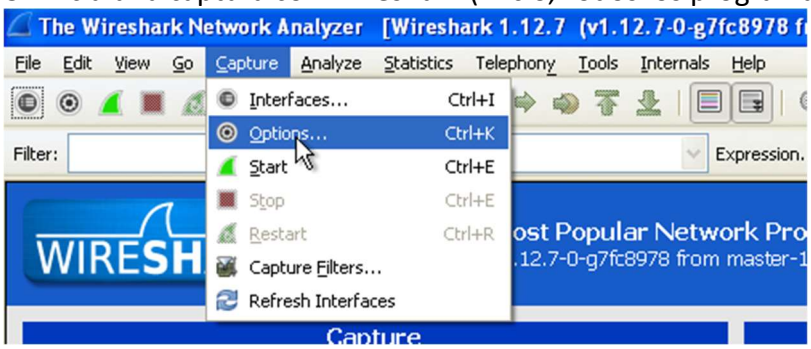
En esta práctica se analiza la información de los mensajes de petición y respuesta del protocolo HTTP.

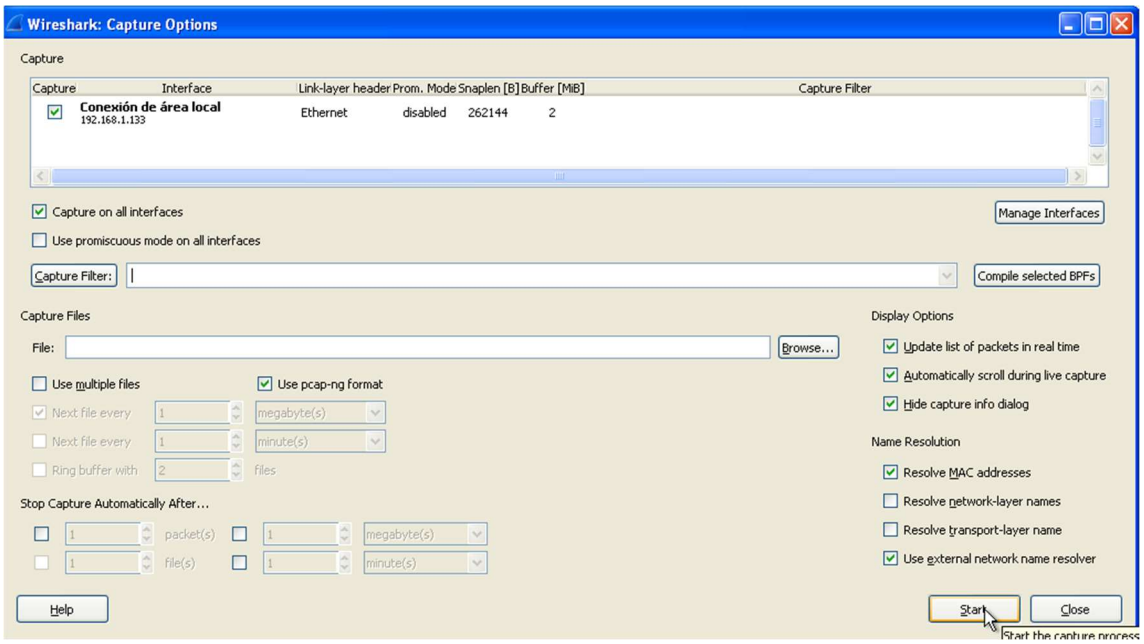
Pasos Previos:
Instalar el programa wireshark, cuyo ejecutable está en FTP.

1. Inicia sesión en Windows.

2. Abre el navegador que tengas en tu equipo.

3. Inicia una captura con Wireshark (Inicio, Todos los programas, Wireshark)





Nota: Desactivar el modo promiscuous

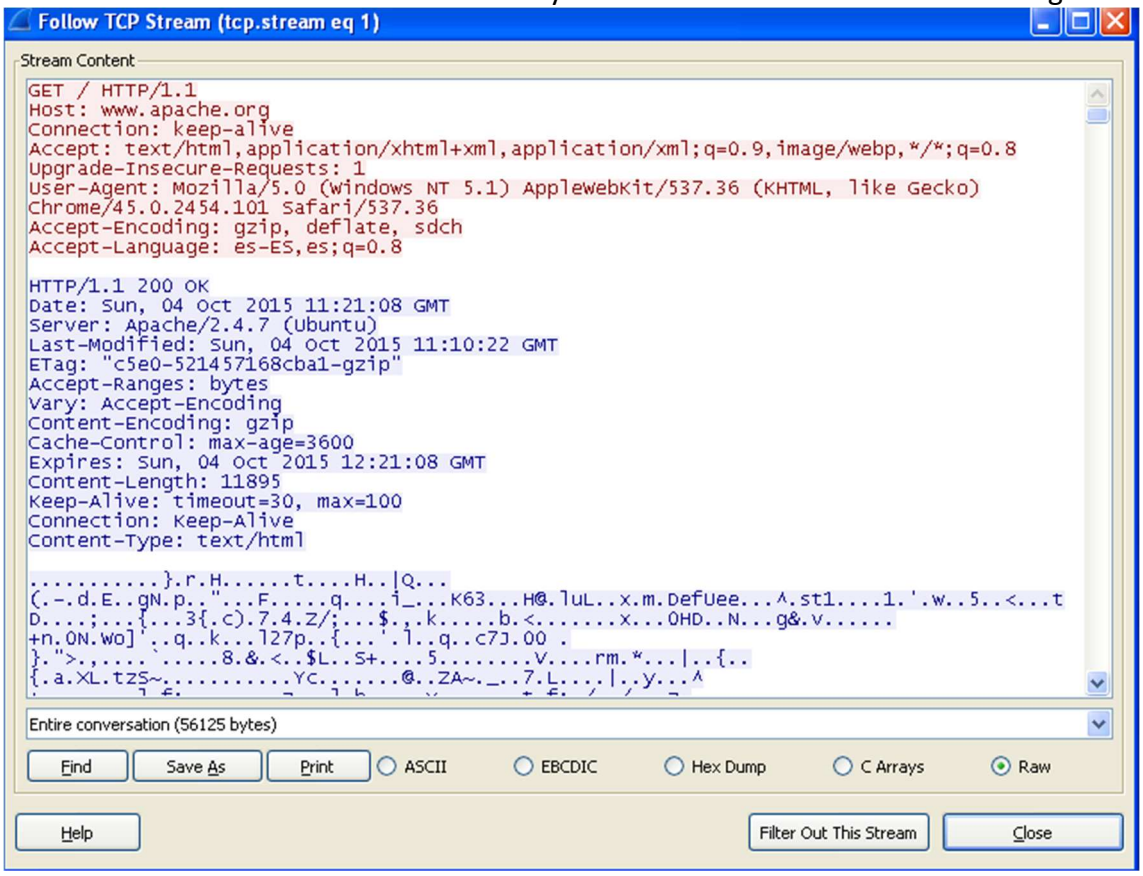
Capture=> Interfaces=> **Start**.

4. Desde el navegador establece una conexión a **http://www.apache.org/**.

5. Vuelve a Wireshark y para la captura (Capture, **Stop**).

6. Buscar una trama HTTP en donde la petición sea **GET / HTTP/1.1**, e incluye el pantallazo en la práctica.

7. Haz clic con el botón derecho del ratón y selecciona **Follow TCP Stream**. Ver Figura



Incluye en la práctica tu pantallazo

8. Responde a las siguientes preguntas:

8.1. ¿Cuál es la IP de la máquina donde se ejecuta el servidor Web?

8.2. ¿Qué versión de HTTP se utiliza?

8.3. ¿Qué método de petición se utiliza?

8.4. ¿Qué recurso se solicita al servidor?

8.5. ¿Qué valor tiene la cabecera Host?

8.6. ¿Se envían cookies en la petición HTTP?

8.7. ¿Qué lenguaje utiliza el navegador?

8.8. ¿Qué código de estado tiene la respuesta HTTP?

8.9. ¿Qué servidor Web y versión se utiliza?

8.10. ¿De qué tipo MIME es el recurso recibido?

8.11. ¿Se han utilizado conexiones persistentes, es decir, en la misma conexión TCP hay varias peticiones y respuestas HTTP? ¿Qué significa Keep alive?

8.12. ¿Existen peticiones y respuestas de imágenes? Obtener pantallazo

8.13.- Lanza de nuevo una captura de red con wireshark. ¿Qué observas al hacer una petición a www.google.es? ¿Qué protocolo se está utilizando a nivel de aplicación? ¿Qué diferencias observas con la petición anterior?

9.- CONCLUSIONES: Se trata de realizar el seguimiento de las tramas que pertenecen a una determinada petición HTTP, introduciendo una URL determinada desde el navegador y haciendo el seguimiento de todos los protocolos implicados que posibilitan esa "conversación" (conjunto de peticiones/respuestas) entre los equipos origen y destino, en concreto el envío de mensaje de petición HTTP del navegador al servidor y la respuesta de éste al cliente que inició la comunicación.

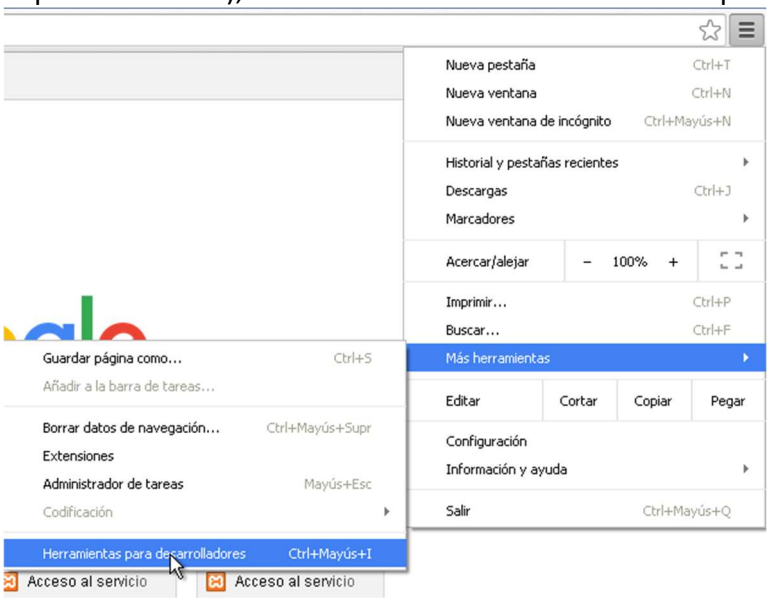
Se pide:

Iniciar el analizador de red (wireshark) y lanzar una determinada petición http, esperar a que la página se haya cargado, parar la captura, guardar la captura y a continuación, explicar el proceso seguido y los protocolos intervinientes. Si no obtenemos lo esperado, utilizad los comandos apropiados para borrar de la caché las direcciones MAC asociadas a IPs, así como las IPs asociadas a los nombres de dominio correspondientes (URL).

9.1.- CONCLUSIONES:

9.2.- Comandos:

10. Accede a las opciones de configuración de Google Chrome (cuadrado en la parte superior derecha), Más Herramientas => Herramientas para desarrolladores.



Accede a http://tomcat.apache.org/ y analiza las peticiones y respuestas HTTP, qué métodos usan, los códigos de respuesta, los recursos que envía el servidor. Obtén el pantallazo.

11. Accede a las opciones de configuración de Google Chrome (cuadrado en la parte superior derecha), Configuración => Mostrar Configuración Avanzada => Configuración de contenido => Todas las cookies y los datos de sitios.
Observa las cookies que tiene almacenadas el navegador. Obtén Pantallazo.
Elimina todas las cookies.