Práctica 2.1: Protocolo HTTP

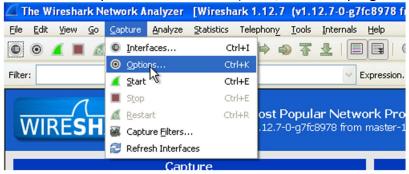
Objetivo:

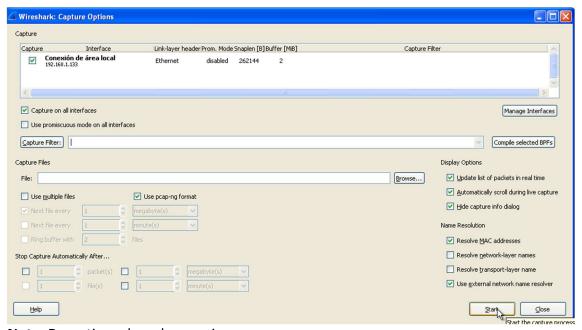
En esta práctica se analiza la información de los mensajes de petición y respuesta del protocolo HTTP.

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 🛚 Follow TCP Stream (tcp.stream eq 1) Stream Content GET / HTTP/1.1
Host: www.apache.org
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (windows NT 5.1) ApplewebKit/537.36 (KHTML, like Gecko)
Chrome/45.0.2454.101 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: es-ES,es;q=0.8 HTTP/1.1 200 OK Date: Sun, 04 Oct 2015 11:21:08 GMT Server: Apache/2.4.7 (Ubuntu) Last-Modified: Sun, 04 Oct 2015 11:10:22 GMT ETag: "c5e0-521457168cba1-gzip" ETag: "c5e0-521457168cba1-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Cache-Control: max-age=3600
Expires: Sun, 04 Oct 2015 12:21:08 GMT
Content-Length: 11895
Keep-Alive: timeout=30, max=100
Connection: Keep-Alive
Content-Type: text/html Entire conversation (56125 bytes) O ASCII ○ EBCDIC O Hex Dump Raw Find Save As Print C Arrays Help Filter Out This Stream

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).

4 CONCLUCIONES	
.1 CONCLUSIONES:	
.2 Comandos:	
•	e configuración de Google Chrome (cuadrado en la pa
iperior derecha), Más Herra	amientas => Herramientas para desarrolladores.
	☆ 🗏
	Nueva pestaña Ctrl+T Nueva ventana Ctrl+N
	Nueva ventana de incógnito Ctrl+Mayús+N
	Historial y pestañas recientes ▶
	Descargas Ctrl+J
	Marcadores >
	Acercar/alejar – 100% + []
	Imprimir Ctrl+P
	Buscar Ctrl+F
Guardar página como Ctrl+5 Añadir a la barra de tareas	Más herramientas
	Editar Cortar Copiar Pegar
Borrar datos de navegación Ctrl+Mayús+Supr Extensiones	Configuración
Administrador de tareas Mayús+Esc	Información y ayuda
Codificación	Salir Ctrl+Mayús+Q
Herramientas para desarrolladores Ctrl+Mayús+I	
Acceso al servicio 🔀 Acceso al servicio	
sada a http://tamaat.ana.	cho era/ v analiza los naticiones v respuestos UTTD a
	che.org/ y analiza las peticiones y respuestas HTTP, q
•	de respuesta, los recursos que envía el servidor. Obtén
intallazo.	
	e configuración de Google Chrome (cuadrado en la pa
perior derecha), Configura	ción => Mostrar Configuración Avanzada => Configuraci
e contenido => Todas las co	okies y los datos de sitios.
oserva las cookies que tiene	e almacenadas el navegador. Obtén Pantallazo.
imina todas las cookies.	