Tarea N° 1

"Dime y lo olvido, muéstrame y lo recuerdo, **involúcrame y lo aprendo**." Proverbio Chino.

Nuestro aprendizaje de los protocolos de red se enriquece al ver los protocolos en acción observando los mensajes intercambiados entre procesos remotos y a través de la constatación de nuestro entendimiento vía la experimentación. Es así como en esta tarea usted observará el comportamiento del protocolo HTTP y podrá constatar qué uso hace de éste su browser y servidores WEBs del Departamento de Electrónica.

Preparación previa: Revise la ayuda básica para la instalación y uso de Wireshark disponible en:

http://profesores.elo.utfsm.cl/~agv/elo322/1s19/Assignments/Wireshark_Intro_v7.0.pdf

¿Cómo se aprende con estas tareas?: Si bien la tarea es para un grupo de estudiantes, se desea que cada uno la resuelva primero individualmente. Luego comparan sus observaciones y respuestas para generar la solución grupal. Esto vale para todas las tarea de esta asignatura.

1. Ejecute Wireshark y luego acceda a la siguiente página usando un browser.

   http://profesores.elo.utfsm.cl/~agv/elo322/HTTP/httpTest.html

   En Wireshark Use http como filtro de paquetes para ver solo esta interacción.

   a) ¿Qué versión de HTTP corre su browser? ¿Qué versión de HTTP corre el servidor profesores.elo.utfsm.cl? ¿Qué versión de HTTP corre el servidor alumnos.elo.utfsm.cl?

   b) ¿Cuál es la IP de su computador y el puerto asignado al socket de su browser (equivale a puerto asignado a la aplicación browser)?

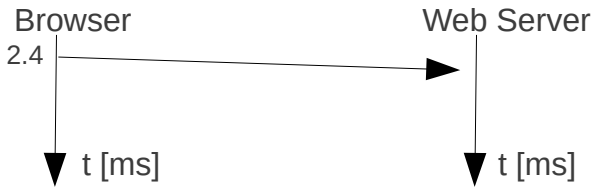
   c) ¿Cuáles son las IPs de los computadores donde corren el servidor web profesores y el servidor web alumnos, y cuál es el puerto de cada servidor web?

   d) ¿Cuándo fue modificado el archivo HTML httpTest.html?

   e) ¿Cuántos bytes son pasados al proceso browser, es decir la aplicación, en respuesta a su requerimiento del archivo HTML? Explique cómo obtuvo ese resultado.

   f) ¿Cuántos bytes son recibos por la capa de red (IP) de su computador en la respuesta que incluye el archivo HTML?

   g) Flexibilice el filtro para mostrar además los paquetes TCP donde su browser sea el origen o el destino de los paquetes. Haga un diagrama temporal como el mostrado partiendo desde el momento en que su browser inicia el establecimiento de conexión con el servidor web hasta que termina de recibir la primera imagen. Según este diagrama ¿diría usted que su navegador es persistente o no-persistente?



   h) Estime el tiempo desde que usted presionó la tecla "intro" (enter o return según su computador) luego de ingresar su URL hasta la llegada de la última imagen. (Nota: Cuando se pide estimar, se espera un valor aproximado, es decir, una o a lo más dos cifras significativas.)

   i) ¿Cuántas conexiones TCP son efectuadas para bajar toda la página; es decir, el html más cada objeto referenciado en ella? Una conexión TCP se inicia con mensajes para establecer la conexión (handshake) y termina con mensaje FIN de TCP. ¿Cuántos servidores webs intervinieron para bajar todo el contenido de la página?

2. Limpie el cache se su browser y mientras wireshark está capturando, **baje dos veces** el archivo indicado a continuación:

   http://profesores.elo.utfsm.cl/~agv/elo322/HTTP/prueba.html

   a) Diga si usted identifica la línea “IF-MODIFIED-SINCE” en la primera captura GET del archivo html. Muestre los campos del encabezado enviado por el browser.

   b) ¿Identifica usted la línea “IF-MODIFIED-SINCE” en la segunda captura GET del html? Muestre los campos del encabezado enviado por el browser en este segundo caso.

   c) ¿Cuál es el código de estatus HTTP y frase descriptiva retornada desde el servidor en la segunda respuesta a GET del html? Incluya el encabezado enviado por el servidor. ¿Llegó desde el servidor el contenido solicitado por el browser? Explique su respuesta.

3. Conéctese a aragorn usando ssh. Ocupando una consola o terminal para acceder a aragorn, corra telnet para enviar un requerimiento GET con solo una línea de encabezado para bajar la página ubicada en:

   http://profesores.elo.utfsm.cl/~agv/elo322/HTTP/prueba.html

   Espere hasta que la conexión sea cerrada desde el servidor. Ponga en su tarea toda la interacción que usted observa en pantalla desde antes de ejecutar telnet, hasta que la conexión es cerrada.

   Ayuda: Previo a ejecutar el comando telnet, ejecute el comando script. Este comando permite generar un registro de todo lo que usted verá por pantalla. Este registro queda en archivo con nombre typescript (vea man script si desea conocer variantes).

4. Conectado a aragorn vía ssh, ejecute el comando script y luego ejecute

   $ traceroute gaia.cs.umass.edu

   Complete el cuadro al estilo de:

Salida de traceroute a gaia.cs.umass.edu	Nombre del institución responsable de la IP	País y ciudad (o solo país) en que (probablemente) se encuentra el equipo
1 elo-gw (200.1.17.1) 15.599 ms	UTFSM	Valparaíso, Chile
:	:	:

   Usando Google Maps capture una imagen que incluya todos los lugares por donde pasaron los paquetes, marque los lugares y haga una línea que muestre el recorrido seguido. Incluya en su respuesta la imagen final.

5. **Extra-créditos**: si responde correctamente esta parte, su grupo puede obtener 10 puntos adicionales . En todo caso su nota de tarea se satura en 100%.

   Autenticación HTTP: Borre el cache de su browser y ciérrelo. Vuelva a ejecutarlo y corra wireshark. Ingrese al URL: http://profesores.elo.utfsm.cl/~agv/elo322/readings/

   Ingrese el usuario y password dados en clases. Detenga la captura de wireshark.

   a) ¿Cuál es la respuesta del servidor en respuesta al mensaje HTTP GET inicial?

   b) ¿Qué campos son incluidos en el mensaje HTTP GET en el segundo mensaje GET enviado por su browser?

   Borre el cache nuevamente y cierre el browser. Vuelva a ejecutarlo y corra wireshark. Ingrese al URL: http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

   ocupe user wireshark-students y password network. Detenga la captura de wireshark. Responda a y b para este caso.

   Aún cuando esta segunda forma de ingresar una password pareciera segura, no lo es. Los datos enviados por la red son codificados en formato Base64 el cual es simple de decodificar. Puede leer más sobre esto en: http://frontier.userland.com/stories/storyReader$2159