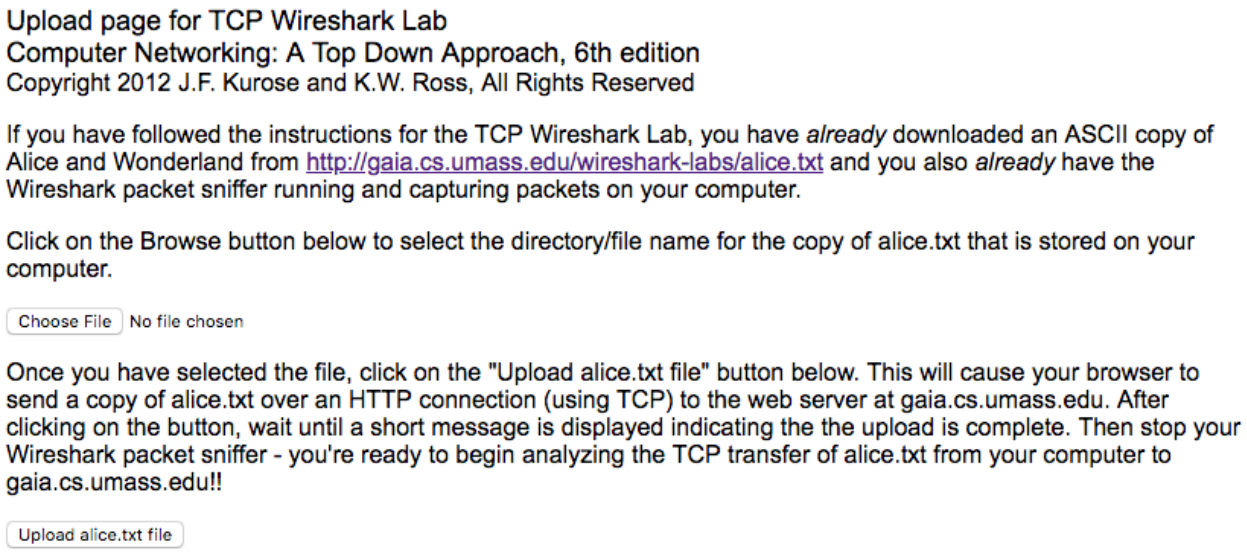
LABORATORIO WIRESHARK – TCP

En este laboratorio estudiaremos diferentes aspectos del protocolo TCP, ya vistos en la teoría, mediante el análisis de una captura hecha con Wireshark. Haremos entonces la captura de la transferencia de un archivo hacia un sitio web.

Para hacer la captura:

- Inicie su navegador web. Vaya al enlace http://gaia.cs.umass.edu/wireshark-labs/alice.txt . En pantalla aparecerá el texto completo de "Alicia en el país de las maravillas". Guarde este archivo de texto en el disco duro de su computador.
- Luego, navegue a http://gaia.cs.umass.edu/wireshark-labs/TCP-wireshark-file1.html . La pantalla se verá similar a ésta:


Upload page for TCP Wireshark Lab
Computer Networking: A Top Down Approach, 6th edition
Copyright 2012 J.F. Kurose and K.W. Ross, All Rights Reserved

If you have followed the instructions for the TCP Wireshark Lab, you have *already* downloaded an ASCII copy of Alice and Wonderland from http://gaia.cs.umass.edu/wireshark-labs/alice.txt and you also *already* have the Wireshark packet sniffer running and capturing packets on your computer.

Click on the Browse button below to select the directory/file name for the copy of alice.txt that is stored on your computer.

Choose File No file chosen

Once you have selected the file, click on the "Upload alice.txt file" button below. This will cause your browser to send a copy of alice.txt over an HTTP connection (using TCP) to the web server at gaia.cs.umass.edu. After clicking on the button, wait until a short message is displayed indicating the the upload is complete. Then stop your Wireshark packet sniffer - you're ready to begin analyzing the TCP transfer of alice.txt from your computer to gaia.cs.umass.edu!!

Upload alice.txt file

- Presione el botón "Choose File" y navegue hasta el archivo `alice.txt` que grabó en el primer paso de la práctica.
- Inicie la captura de paquetes en Wireshark.
- Presione el botón "Upload alice.txt file" para subir el archivo al sitio remoto. Espere a que aparezca un mensaje de confirmación.
- Detenga la captura en Wireshark.
- Filtre en Wireshark por la dirección IP de `gaia.cs.umass.edu`, mediante el filtro `ip.addr==128.119.245.12` .
- Seleccione el primer paquete de la conexión, y fíltrela presionando el botón derecho del ratón, y escogiendo `Follow -> TCP Stream`.

Conteste las siguientes preguntas, empleando capturas de pantalla o tablas para sustentar cada respuesta:

Guide Modified By: Juan Felipe Gómez Manzanares. M. Sc.
Telematic Engineer.

1. ¿Cuáles son la dirección IP y el puerto TCP empleados por el computador cliente que está transfiriendo el archivo a `gaia.cs.umass.edu`?
2. ¿Cuáles es la dirección IP de `gaia.cs.umass.edu`? ¿Qué puerto TCP está empleando el servidor para enviar y recibir los segmentos de esta conexión?
3. ¿Cuál es el número de secuencia del segmento TCP SYN que abre la conexión entre el cliente y el servidor? ¿Qué identifica a este segmento como un segmento SYN?
4. ¿Cuál es el número de secuencia del segmento SYN-ACK enviado por el servidor como respuesta al SYN del cliente? ¿Cuál es el valor del campo de acknowledgement de este segmento SYN-ACK? ¿Cómo determinó el servidor dicho valor? ¿Qué identifica a este segmento como un segmento SYN-ACK?
5. ¿Cuál es el número de secuencia del segmento TCP que contiene la solicitud HTTP POST? Para poder hallar el comando POST, debe observar el contenido del segmento en la parte inferior de la ventana de Wireshark; el comando aparecerá en el payload del segmento.
6. Considere el segmento TCP que contiene el POST como el primer segmento de la conexión. ¿Cuáles son los números de secuencia de los seis primeros segmentos que van del cliente al servidor (incluyendo el del POST)? ¿En qué tiempo se envió cada uno de estos segmentos? ¿En qué tiempo se recibió el ACK correspondiente? Calcule el RTT para cada uno de los seis segmentos, como la diferencia entre el tiempo de envío de cada segmento, y el de llegada de su respectivo ACK. ¿Cuál es el valor del EstimatedRTT para cada segmento? Para el primer segmento, asuma que el EstimatedRTT es igual al RTT medido; para el segundo y posteriores, emplee la fórmula del capítulo 3 del libro. Calcule también el valor del timeout para cada uno de los segmentos.
7. ¿Cuál es la longitud de cada uno de los primeros seis segmentos TCP?
8. ¿Cuál es la mínima cantidad de buffer disponible anunciada por el servidor durante toda la conexión? ¿El cliente debe parar en algún momento el envío de datos debido a falta de espacio de buffer?
9. ¿Hay segmentos retransmitidos en la captura? ¿Qué buscó en la captura para contestar esta pregunta?
10. ¿Cuántos bytes reconoce típicamente el servidor en un ACK? ¿Puede identificar algún caso en el que el servidor esté reconociendo más de un segmento a la vez?
11. ¿Cuál es el throughput de la conexión TCP en bytes/segundo? Explique cómo calculó este valor.

Guide Modified By: Juan Felipe Gómez Manzanares. M. Sc.
Telematic Engineer.