|  |  |  |
| --- | --- | --- |
| **GRUPO 9** | | |
| Iván González | 2973523-9 | ivan.gonzalezlo@alumnos.usm.cl |
| Guillermo Baeza | 2973600-6 | guillermo.baeza@alumnos.usm.cl |

Introducción

En esta segunda versión de la exitosa aplicación creada anteriormente, se establece comunicación entre los distintos usuarios de Avioncito de Papel II, los que pueden ser gestionados a través del sistema creado en la tarea 1.

La comunicación entre usuarios se logra sobre la base de un entorno distribuido cliente-servidor, en el que tenemos, por un lado, una aplicación servidor tipo TCP en donde los distintos usuarios se conectan para lograr comunicarse a través del chat, y otra aplicación cliente correspondiente a la aplicación creada en la tarea 1, con su propio cliente (navegador web mostrando interfaz creada) y servidor local HTTP que envía los mensajes al servidor TCP, que finalmente devuelve al servidor HTTP para actualizar la interfaz.

En el presente documento se explica el funcionamiento de la aplicación desarrollada en el marco de la segunda tarea de Redes de Computadores, año 2014. Además, se evidencia la correcta ejecución de la aplicación a través de pantallazos y captura de paquetes con *Wireshark*.

Se deberá elaborar un informe en formato PDF, el cual debe contener evidencia del funcionamiento de la aplicación (pantallazos) con el siguiente procedimiento, explicado paso a paso por ustedes con sus propias palabras:

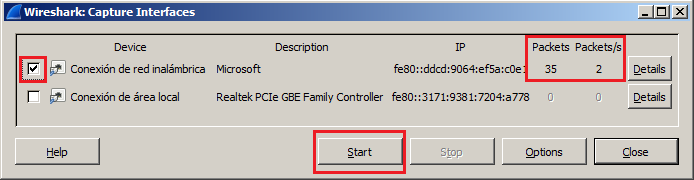
1. Iniciar dos clientes y un servidor de Avioncito de Papel.

2. Conectar ambos clientes (agregarse como contactos, intercambiar direcciones IP y puertos)

3. Iniciar la captura de paquetes con Wireshark

Wireshark es un analizador de protocolos de red, que permite visualizar el tráfico (paquetes) que pasan a través de la interfaz de red seleccionada. Tiene una *interfaz gráfica* *amigable* que permite al usuario seleccionar aquellos paquetes de interés y estudiarlos. Esto será revisado en el punto 6 y 9 de este informe.

Para iniciar la captura de paquetes con Wireshark, primero debe seleccionarse la interfaz de red desde la cual se quiera filtrar los paquetes. Para ellos, nos vamos al menú *Capture -> Interfaces*, (o bien, Ctrl + I). La manera de identificar la intefaz de red activa, es sencillamente viendo la que tenga paquetes (columna *packets*). Luego de seleccionarla, se da click sobre *Start* para empezar a capturar paquetes.

***Captura 1: Selección de interfaz de red correcta, y comienzo de monitoreo.***

Los paquetes de interés pueden filtrarse de la lista escribiendo un filtro adecuado, como por ejemplo “tcp” en *filter* y luego apretar sobre *apply*.

Para terminar la captura de paquetes, basta ir a *Capture -> Stop* (Ctrl + E).

4. Enviar un mensaje (Cliente 1 envía mensaje a Cliente 2)

5. Enviar una respuesta (Cliente 2 envía mensaje a Cliente 1)

6. Mostrar en *Wireshark* los mensajes que se enviaron, destacando direcciones IP y puertos de origen y destino. Comparar ACK y números de secuencia de acuerdo al protocolo escogido.

7. Enviar un archivo (Cliente 1 envía un archivo de al menos 1 MB a Cliente 1)

8. Recibir archivo (Cliente 2 recibe el archivo y lo abre)

9. Mostrar en *Wireshark* el envío del archivo, destacando direcciones IP y puertos de origen y destino. Comparar ACK y números de secuencia de acuerdo al protocolo escogido.

10. El informe deberá contener dos diagramas similares a este (aparece en las diapositivas), con los números correctos de IP y puertos para cada caso (puntos 6 y 9).