Laboratorio

Wireshark

Ciencias de la Computación VIII

Instrucciones:

Este laboratorio tiene como objetivo reforzar conocimiento del comportamiento del protocolo **TCP**, **UDP** e **ICMP**. Para ello se hará uso de su **primer laboratorio** para analizar **TCP** y **UDP**.

Instalación en Windows o Mac

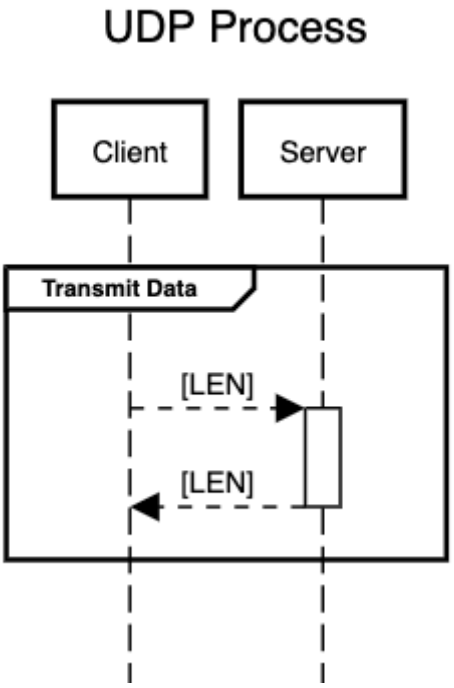
https://www.wireshark.org/#download

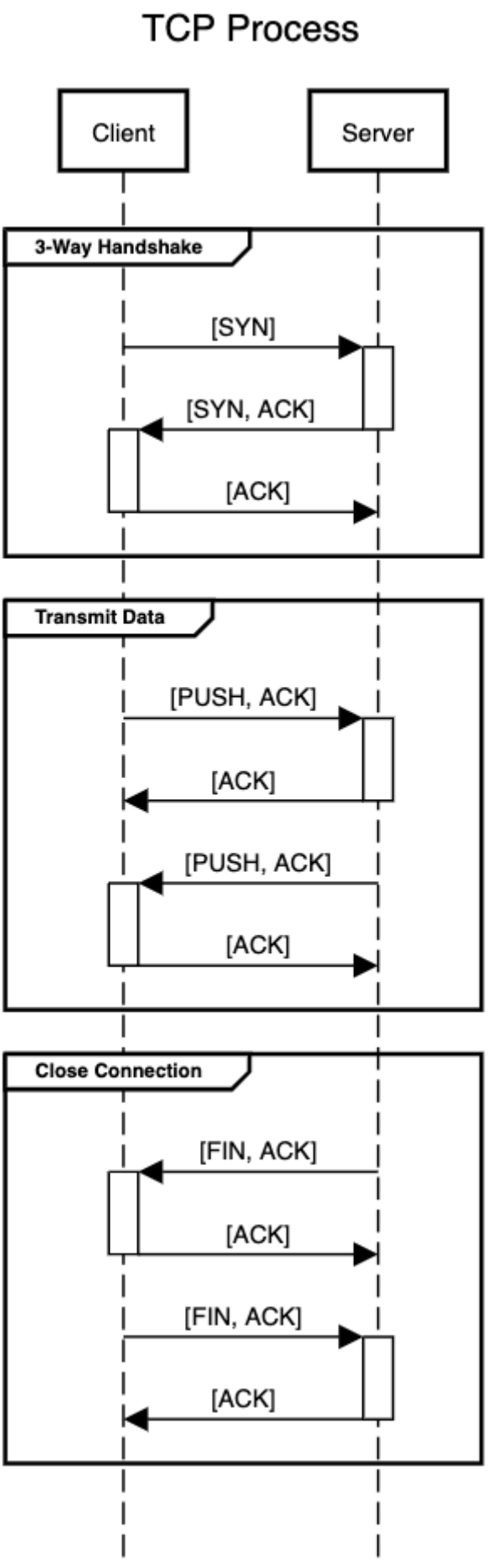
Instalación de Wireshark en Linux

```
sudo apt-get install aptitude
sudo aptitude install wireshark
sudo wireshark &
```

Documentación

IP https://en.wikipedia.org/wiki/Internet_Protocol
TCP https://en.wikipedia.org/wiki/Transmission_Control_Protocol
UDP https://en.wikipedia.org/wiki/User_Datagram_Protocol
ICMP https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol




TCP Process
Client
Server
3-Way Handshake
[SYN]
[SYN, ACK]
[ACK]
Transmit Data
[PUSH, ACK]
[ACK]
[PUSH, ACK]
[ACK]
Close Connection
[FIN, ACK]
[ACK]
[FIN, ACK]
[ACK]

Capturar:
Para facilitar su trabajo, antes de iniciar la Wireshark asegúrese de no tener abierta ninguna aplicación que tenga conexiones abiertas, para facilitar la identificación.

1. Para la prueba escoja un Puerto "vistoso" para luego hacer búsqueda del mismo, por ejemplo: **tcp** o **udp.port==XX**
2. Inicie WireShark y comience la captura de paquetes, es recomendable que para cada caso limpie las capturas de paquetes.
3. Ahora proceda a ejecutar su servidor TCP y el cliente, envíe el mensaje **lorem ipsum** y luego cierre su conexión correctamente enviando el mensaje **EXIT**.
4. Haga el mismo procedimiento de TCP pero ahora con **UDP**.
5. Utilice su **Cliente UDP** para generar los ICMP: **host** y **port unreachable**, colocando un **PORT incorrecto**, otro con una **IP incorrecta** y otro con **ambos incorrectos**.
6. Utilice **TraceRoute** (Tracert en Windows) para generar el **Time Exceeded**, hágalo hacia Google.com.
7. Utilice Ping para generar **Echo** y **Echo Reply**, hágalo hacia Google.com.

Actividad:
Coloque sus respuestas e imágenes en un **archivo EXCEL.**

TCP

1. Tome un Screenshot de toda la secuencia de paquetes capturados en Wireshark de TCP
2. Desglose por columnas todos los campos del encabezado TCP/IP capturados.
3. ¿Cuál es el Sequence Number inicial y final de la conexión, hace sentido que sean esa cantidad, por qué?
4. ¿Se enviaron 4 mensajes, por lo cual solo deben de existir 4 paquetes con DATA, es eso correcto o existen más paquetes?
5. Según la captura, realice un diagrama secuencial del proceso, indicando los SYN, SEQ, ACK, DATA y FIN.

UDP

1. Tome un Screenshot de toda la secuencia de paquetes capturados en Wireshark de UDP
2. Desglose por columnas todos los campos del encabezado UDP/IP capturados.
3. ¿Se generó algún ICMP durante la transmisión, se podría general alguno?
4. Según la captura ¿Los paquetes tenían el mismo length, si no, cuál piensa que sea el motivo?

ICMP

1. Tome un Screenshot de cada par de paquetes capturados en Wireshark de UDP/IP e ICMP/IP, host y port unreachable, Time Exceeded, Echo y Echo Reply.
2. Desglose por columnas todos los campos del encabezado por cada par de UDP/IP e ICMP/IP, solo tome un par de cada tipo.
3. ¿Los ICMP/IP host y port unreachable, cómo se pueden diferenciar?, ¿Cuál es la respuesta de enviar un UDP/IP con IP y PORT incorrectos y por qué?, ¿Se puede conseguir?
4. ¿Qué es lo que contiene el ICMP Time Exceeded en su data o viene vacío?
5. ¿Cuál es la particularidad de Echo y Echo Reply?

Entrega:
El laboratorio debe ser entregado por medio del GES, con todos los archivos en un ZIP, las **siete capturas** de pantalla que realizó en WireShark en pantalla completa y el documento **respuestas.xls** con lo siguiente:

1. **Un Tab TCP/IP**
    a. Todo el proceso TCP/IP desglosa su secuencia numérica y mensajes en las celdas y por cada paquete por fila. Idealmente tiene que tener **15 paquetes**, de ser necesario corrija su laboratorio para facilitar este el desglose.

2. **Un Tab UDP/IP**
    a. Los **4 paquetes** que se intercambian en el proceso.

3. **Un Tab ICMP/IP**
    a. Para todos los Paquetes **ICMP/IP** debe colocar el **UDP/IP** que lo provocó
    b. **Echo**
    c. **Echo Reply**
    d. **Time Exceeded**
    e. **Port unreachable**
    f. **Host unreachable**

El laboratorio puede tener una calificación parcial o cero si: no se entrega completo o -100 si se detecta plagio.