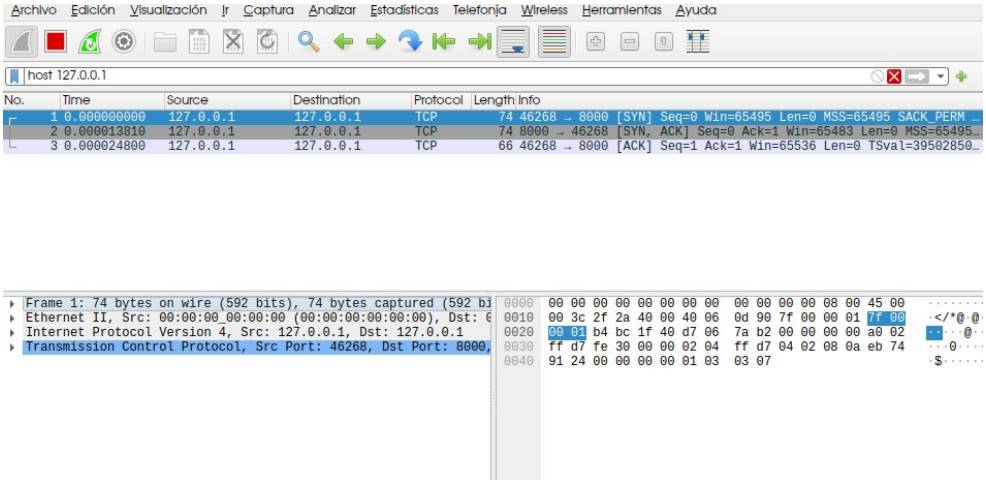
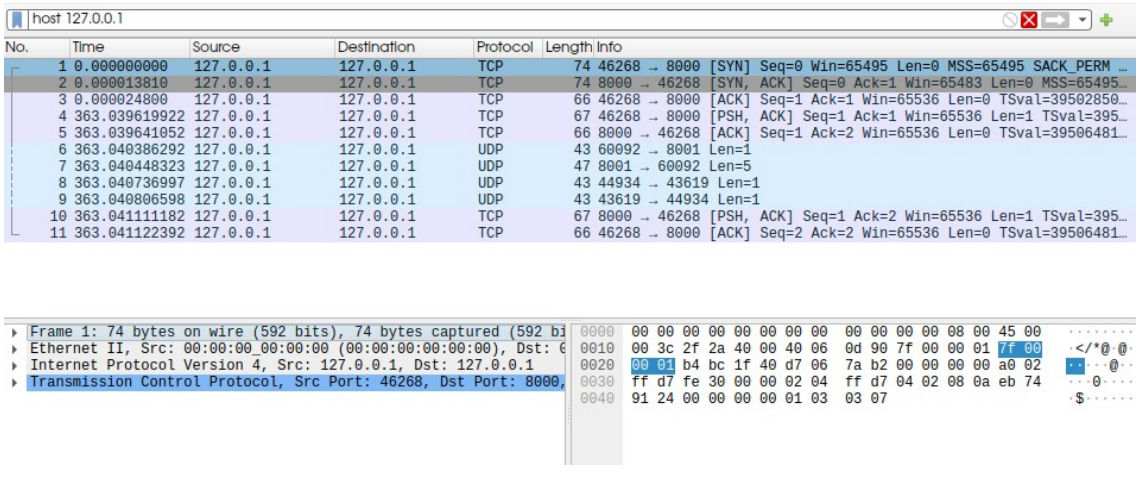
Análisis de Tráfico

1. Si se analiza el número de los mensajes enviados dentro de la aplicación. ¿Cuántos son los que logra detectar Wireshark?. Y comparando en base al código, ¿Es la misma cantidad? Si no lo es, ¿A qué se debería?

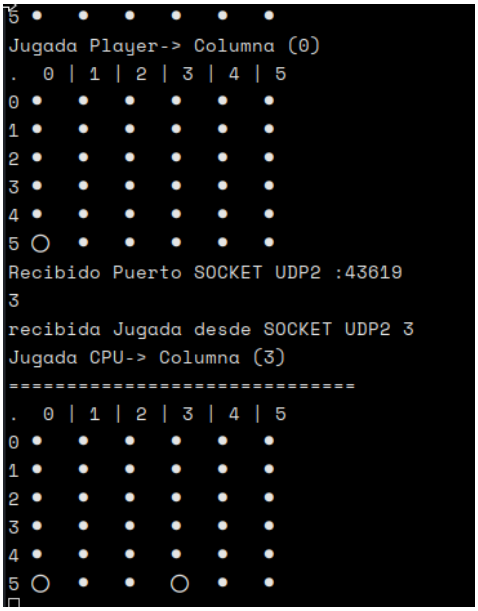
Al correr los tres ejecutables por primera vez (server.py, conecta4.go, client.py), vemos que Wireshark detecta tres conecciones mediante puertos TCP. Podemos notar que primero el puerto 46268 se comunica con el puerto 8000, este último le responde y finalmente el 46268 le envia un último mensaje:



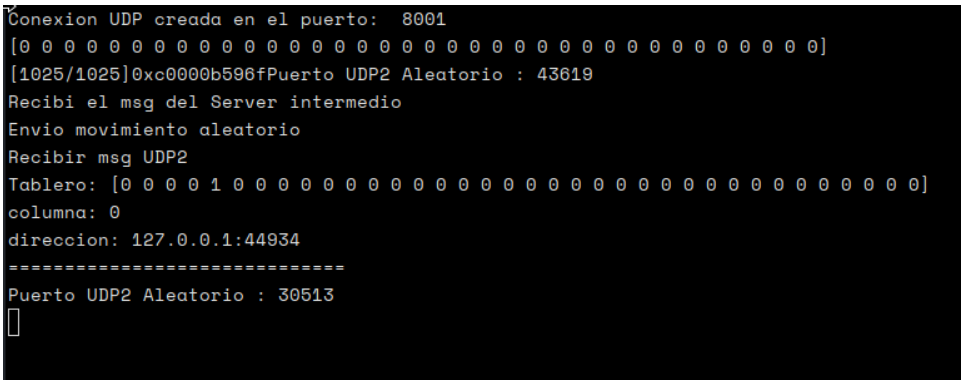
La jugada posterior muestra las siguientes conexiones en Wireshark. En donde las primeras conexiones TCP van desde y hacia el puerto 8000 y 46268. En relacion a las UDP, vemos que van desde y hacia el puerto 8001, 60092, 44934 y 43619:



Podemos notar que es consistente con lo que los programas reportan:



La consola anterior reporta lo que muestra el servidor intermediario por pantalla, podemos notar que es consistente con lo que Wireshark lee.



Esta consola reporta lo que muestra el BOT de conecta4, la cual tambien calza con lo visto en Wireshark. Asi que es correcto afirmar que la cantidad de mensajes reportados es igual a la que se leen.

2. ¿Cuál es el protocolo que se debiese ver a la hora de revisar el intercambio de mensajes en Wireshark? ¿Y cuáles encontró?

TCP y UDP. Lo cual es consistente en base a lo que vimos en Wireshark.

3. ¿El contenido de los mensajes dentro de Wireshark son legibles?, ¿Por Qué si? o ¿Por Qué no?

El contenido de los mensajes no es directamente legible, ya que se codificaron en formato binario, esto se debe al protocolo que se adopto para la tarea (TCP y UDP).