1. **Introducción**

En esta práctica hemos realizado una monitorización de red. Para ello se nos ha proporcionado un archivo *.pcap* que hemos tenido que analizar utilizando la herramienta *tshark*. Para simplificar la ejecución de la práctica, hemos ido introduciendo todos los comandos en una serie de ejecutables *.sh* que recogen todos los requisitos del enunciado.

1. **Requisitos**

A continuación, vamos a analizar los puntos requeridos en el enunciado:

**2.1 Porcentajes**

Para estudiar los porcentajes de paquetes IP hemos utilizado los siguientes filtros de tshark:

***tshark -r traza.pcap -T fields -e frame.len*** (así obtenemos todos los paquetes y los podemos contar con un *wc* para poder obtener los porcentajes)

***tshark -r traza.pcap -T fields -e ip.dst -e ip.src -e udp.dstport -e udp.srcport -e tcp.dstport -e tcp.srcport -e frame.len -Y ‘eth.type eq 0x00000800 or vlan.etype eq 0x00000800’*** (así obtenemos TODOS los paquetes IP, TCP y UDP y luego analizamos el resultado obtenido mediante *awk*, obteniendo los datos necesarios)

El resultado obtenido es el siguiente:

(imagen)

Como se puede apreciar en la imagen, el 99.01% de los paquetes son IP, lo que indica que la inmensa mayoría del tráfico de red capturado utiliza dicho protocolo en sus comunicaciones.

Por otro lado, el 89.59% del tráfico IP capturado emplea el protocolo de transporte IP-TCP, que garantiza la entrega sin errores de los datos, en el mismo orden que se transmitieron. Claramente, es el protocolo de transporte IP más utilizado (posiblemente gracias a las características descritas), frente al 9.02% del UDP y el 1.29% de otros protocolos.

Podemos sacar ciertas conclusiones acerca de este último punto, como descartar la posibilidad de estar realizando o recibiendo un *streaming,* debido al escaso tráfico UDP. El protocolo TCP estándar se emplea, por ejemplo, en páginas web comunes (es decir, protocolo HTTP), por lo que podemos suponer que los usuarios de la red se dedican a este tipo de navegación.

**2.2 TOPS 10**

Para obtener los tops 10 que nos solicitan, hemos utilizado el resultado obtenido de la consulta *tshark* anterior y, empleando las herramientas *awk* (para quedarnos con las columnas que nos interesan y darles formato)*, sort* (para ordenar los resultados)*, sed* (para borrar líneas vacías)*, uniq* (para agrupar los datos iguales y contabilizar su cantidad) *y head* (para imprimir los 10 primeros)*.*

El resultado obtenido es el siguiente:

(imagen ip destino)

Podemos ver que la mayoría de los paquetes se dirigen a la IP 29.181.234.168