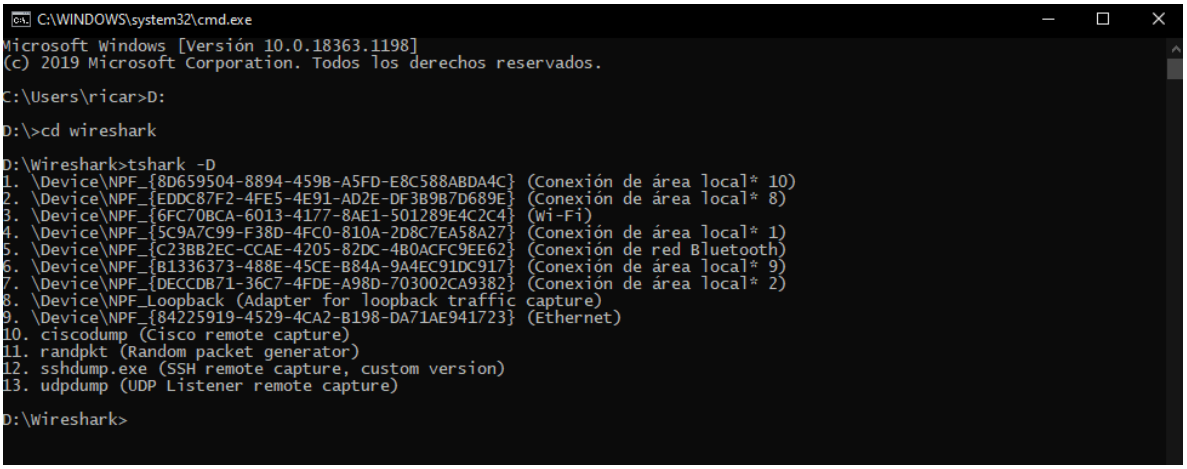
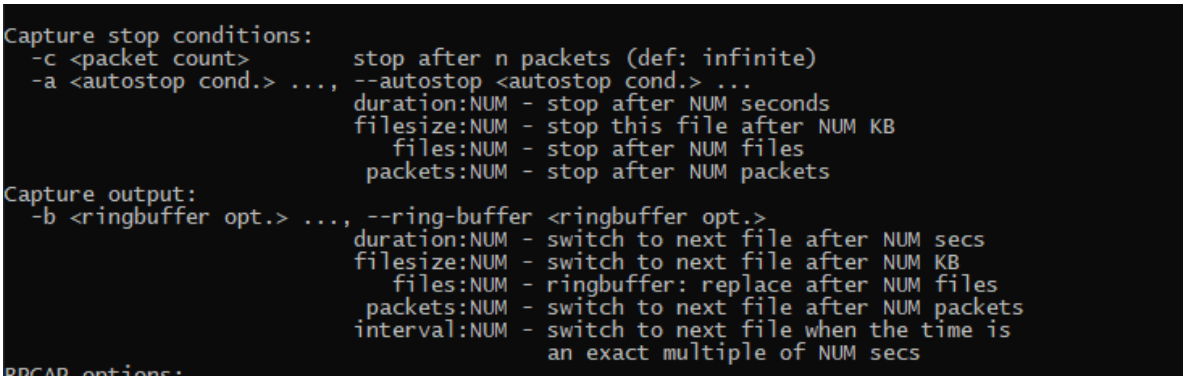
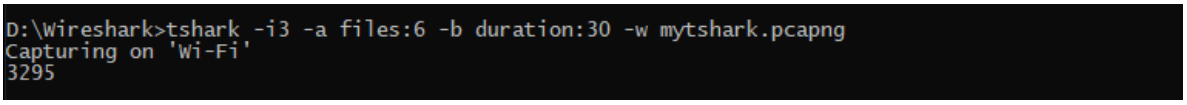
Lab 44

Abriremos nuestro cmd y escribiremos tshark -D para ver la lista de interfaces disponibles, después escribiremos tshark -h para ver los parámetros disponibles para guardar en varios archivos y establecer una condición de parada automática





Después escribiremos el comando tshark -i3 -a files:6 -b duration:30 -w mytshark.pcapng mientras navegamos por la web de www.wireshark.org y esperaremos a que se capturen los paquetes



Una vez terminado escribiremos dir mytshark*.* para ver los archivos y se podrá observar que la marca de tiempo coincide con la configuración para cambiar al siguiente archivo, es decir, 30 segundos.