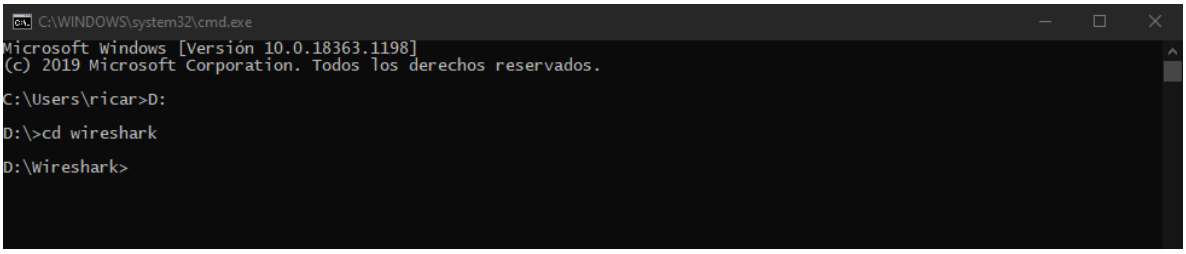
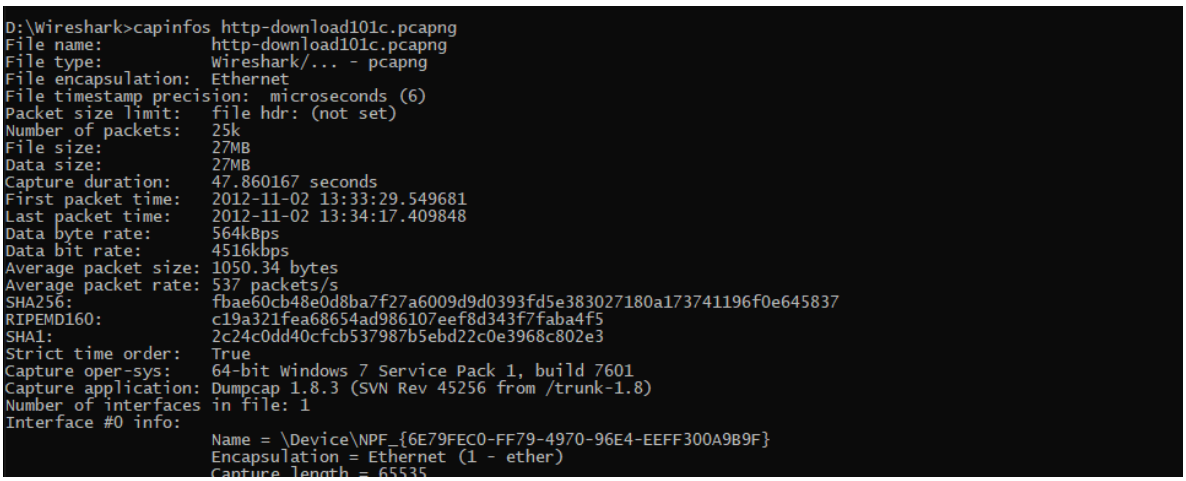
Lab 42

Primero abriremos un símbolo de sistema o cmd de Windows y nos dirigiremos a la carpeta donde se encuentran nuestros archivos de wireshark

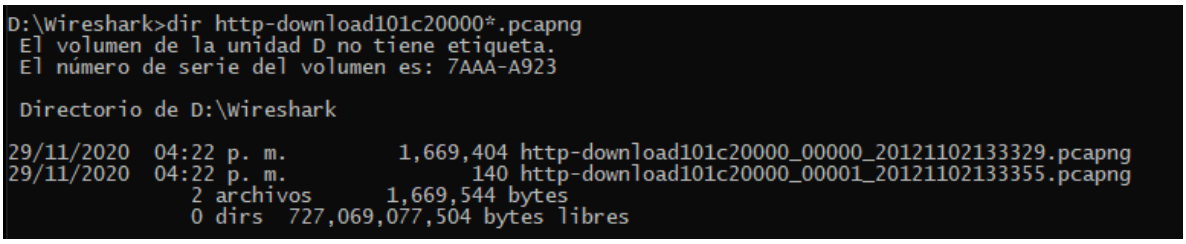


Una ves dentro de la raíz de la carpeta escribiremos el comando capinfos http-download101c.pcapng para observar de manera mas detallada la información, y el total de datos que contiene el paquete

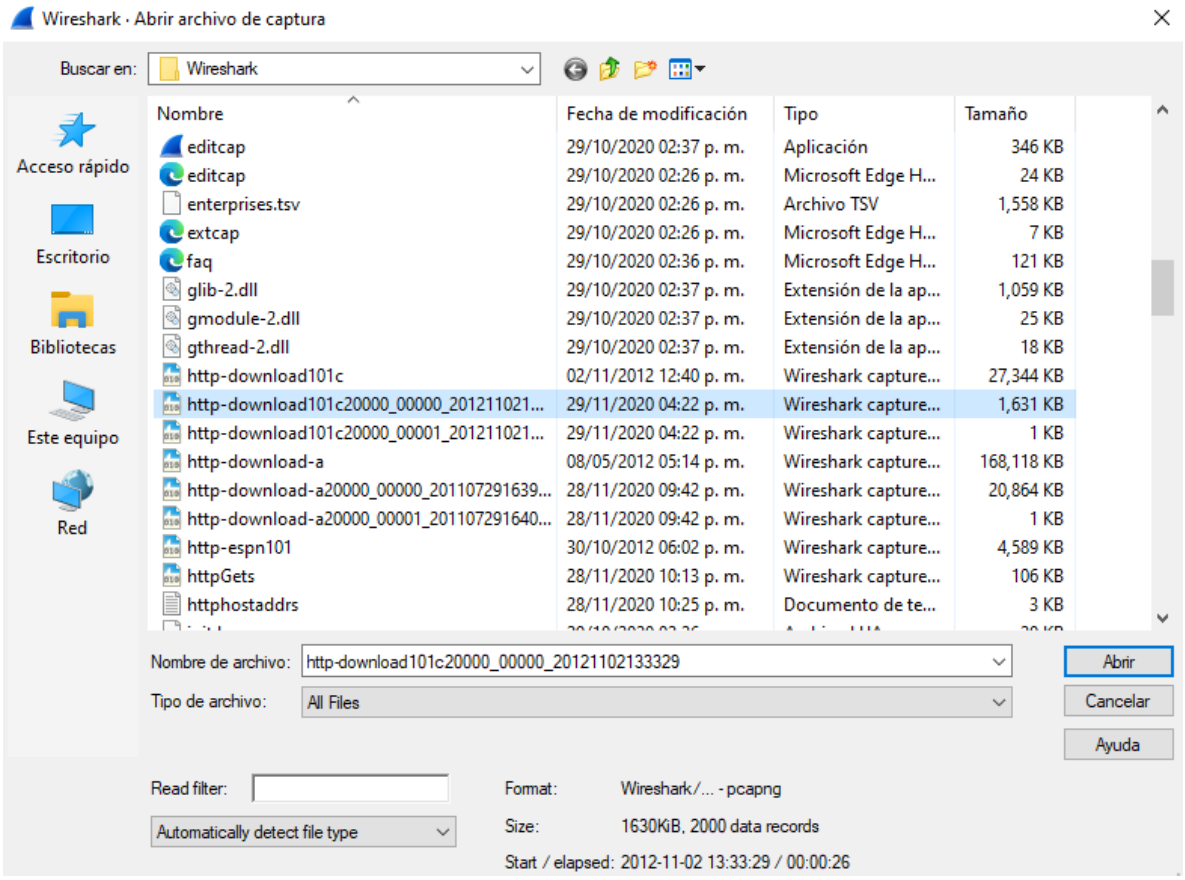


Una vez terminando de ver toda la información procederemos a escribir el comando editcap -c 2000 http-download101c.pcapng http-download101c20000.pcapng

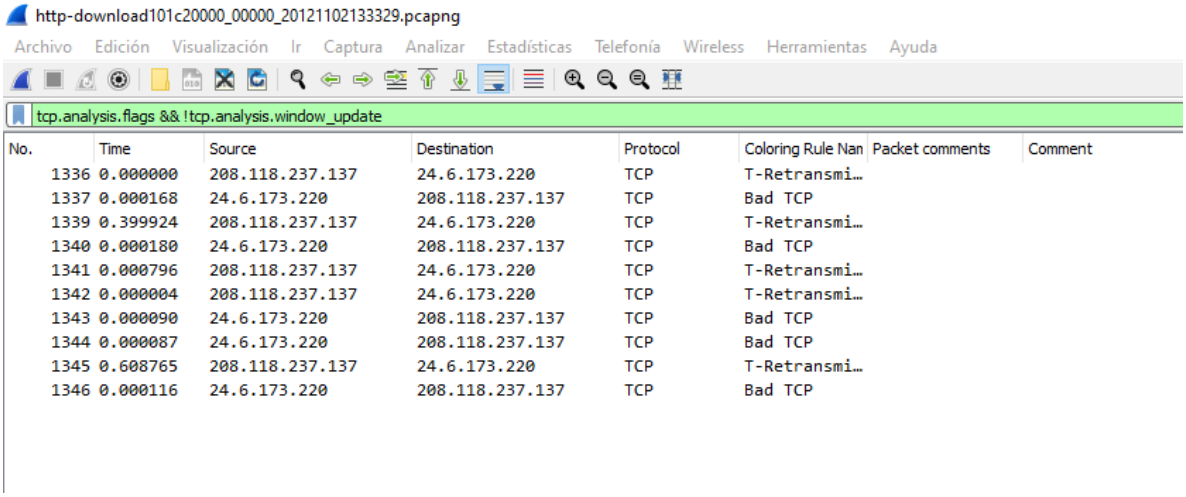
Y después el comando dir http-download101c20000*.pcapng



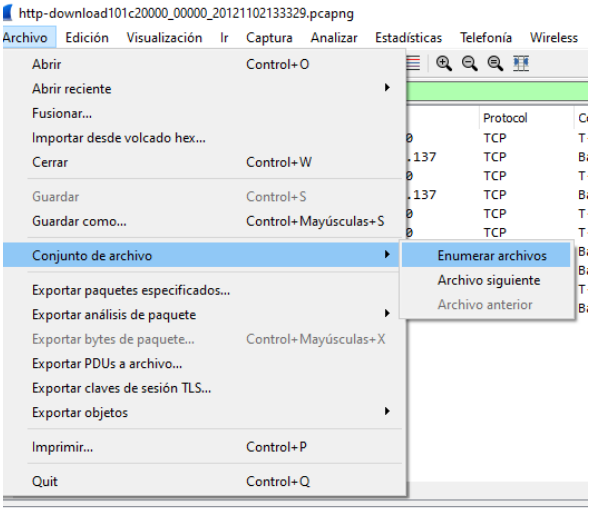
Abriremos el wireshark y buscaremos el archivo que creamos anteriormente

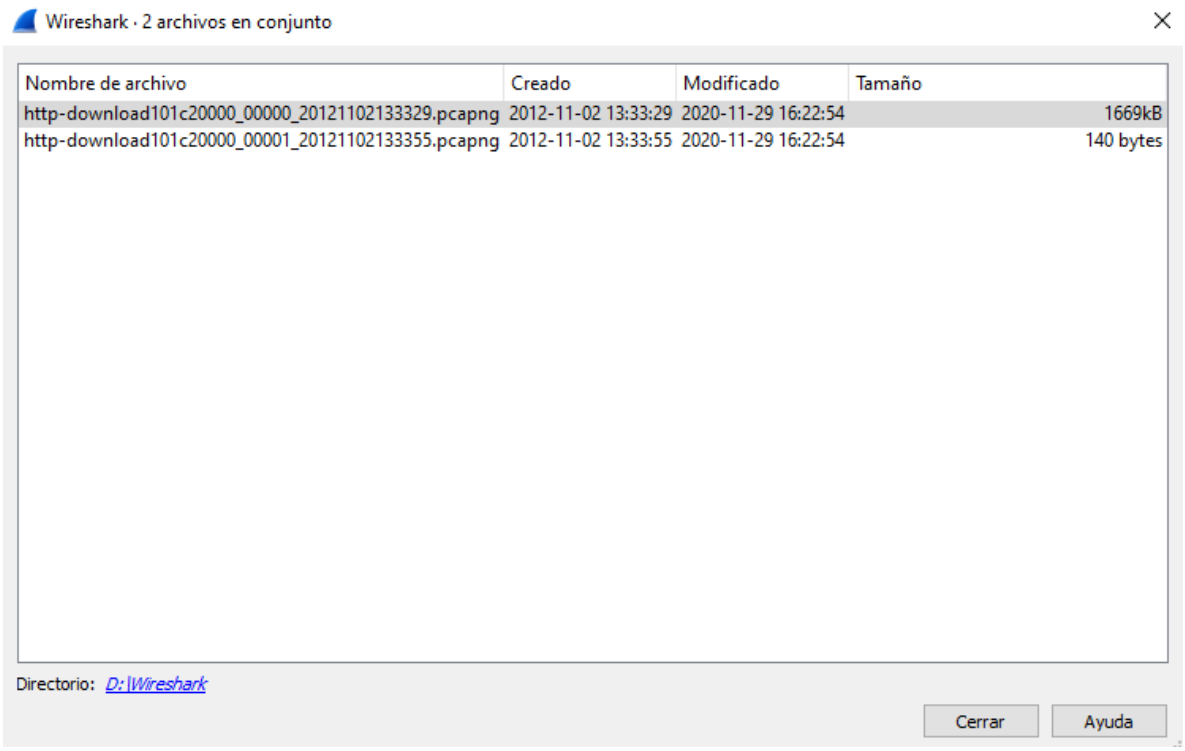


Una ves abierto en el apartado de filtros escribiremos tcp.analysis.flags && !tcp.analysis.window_update



Después le daremos clic al botón de Archivo, conjunto de archivo y enumerar archivos, daremos un clic sobre el nombre de cada archivo para poder examinarlos de manera correcta





El programa wireshark aplica el filtro de visualización para todos los archivos, mientras se abren los distintos archivos se pude observar la barra de estados para verificar cuantos paquetes coincidieron con el filtro en cada uno de los archivos de seguimiento.