

## 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

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Versión 10.0.18363.1198]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.
C:\Users\ricar>D:
D:\>cd wireshark
D:\Wireshark>
```

Una vez 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

```
D:\Wireshark>capinfos http-download101c.pcapng
File name:      http-download101c.pcapng
File type:      Wireshark/... - pcapng
File encapsulation: Ethernet
File timestamp precision: microseconds (6)
Packet size limit: file hdr: (not set)
Number of packets: 25k
File size:      27MB
Data size:      27MB
Capture duration: 47.860167 seconds
First packet time: 2012-11-02 13:33:29.549681
Last packet time: 2012-11-02 13:34:17.409848
Data byte rate: 564kBps
Data bit rate: 4516kbps
Average packet size: 1050.34 bytes
Average packet rate: 537 packets/s
SHA256:         fbae60cb48e0d8ba7f27a6009d9d0393fd5e383027180a173741196f0e645837
RIPEMD160:      c19a321fea68654ad986107eef8d343f7faba4f5
SHA1:           2c24c0dd40cfcb537987b5ebd22c0e3968c802e3
Strict time order: True
Capture oper-sys: 64-bit Windows 7 Service Pack 1, build 7601
Capture application: Dumpcap 1.8.3 (SVN Rev 45256 from /trunk-1.8)
Number of interfaces in file: 1
Interface #0 info:
  Name = \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}
  Encapsulation = Ethernet (1 - ether)
  Capture length = 65535
```

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

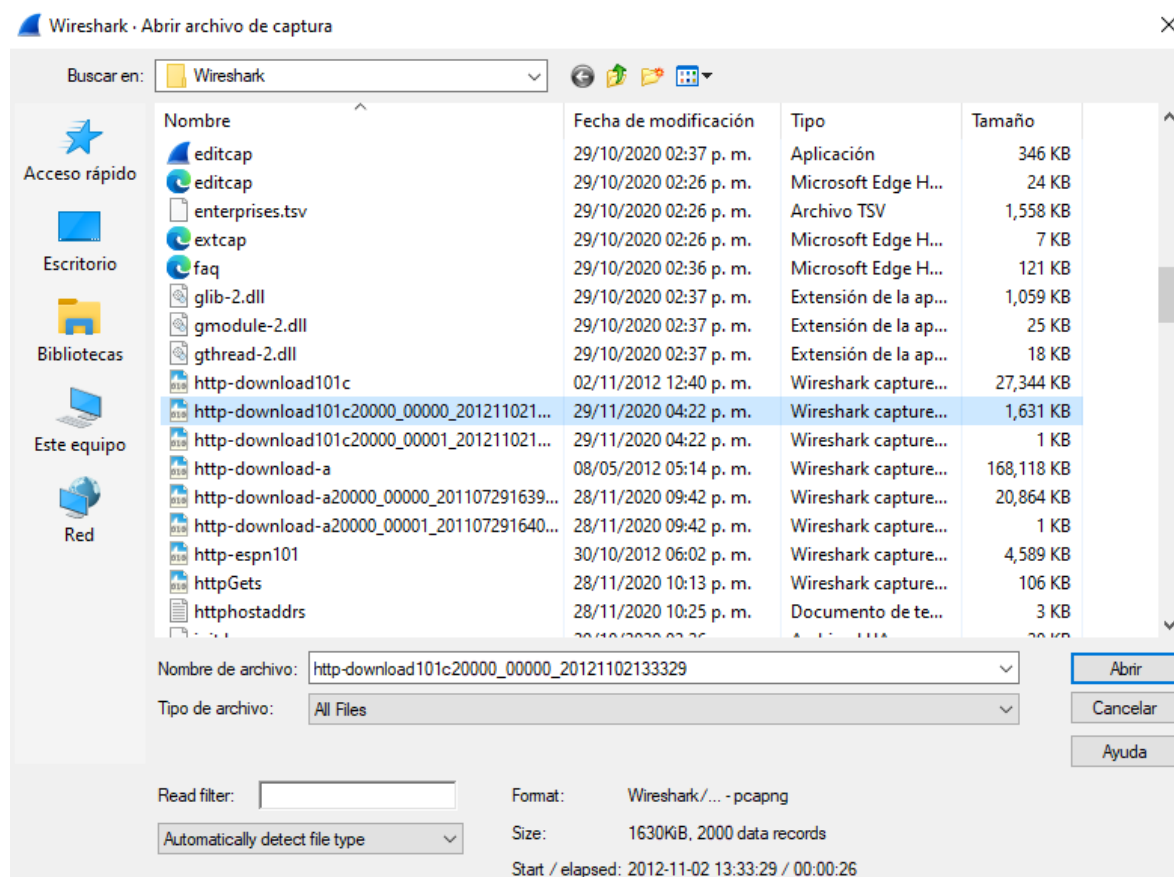
Y después el comando dir http-download101c20000\*.pcapng

```
D:\Wireshark>dir http-download101c20000*.pcapng
El volumen de la unidad D no tiene etiqueta.
El número de serie del volumen es: 7AAA-A923

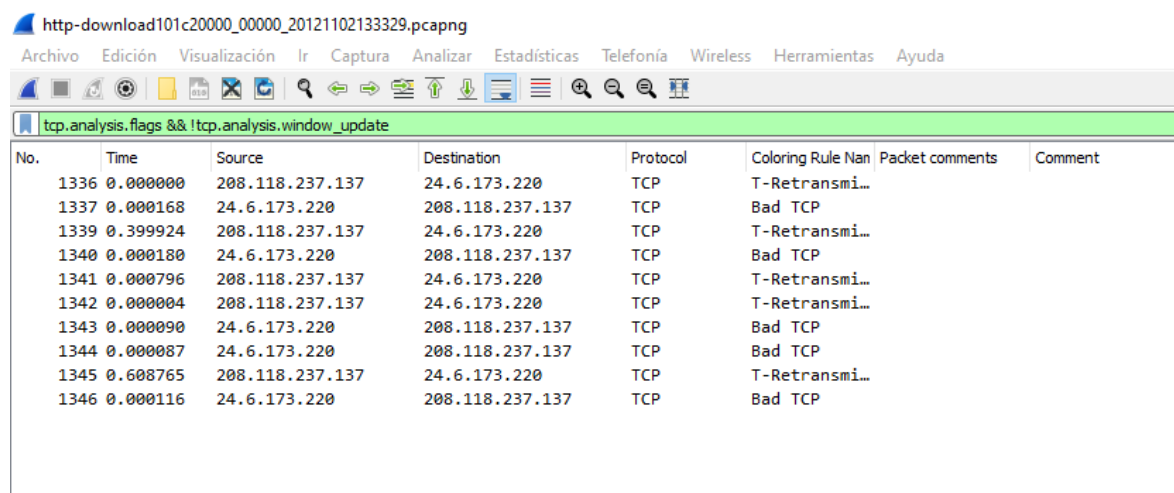
Directorio de D:\Wireshark

29/11/2020  04:22 p. m.          1,669,404 http-download101c20000_00000_20121102133329.pcapng
29/11/2020  04:22 p. m.          140 http-download101c20000_00001_20121102133355.pcapng
          2 archivos          1,669,544 bytes
          0 dirs 727,069,077,504 bytes libres
```

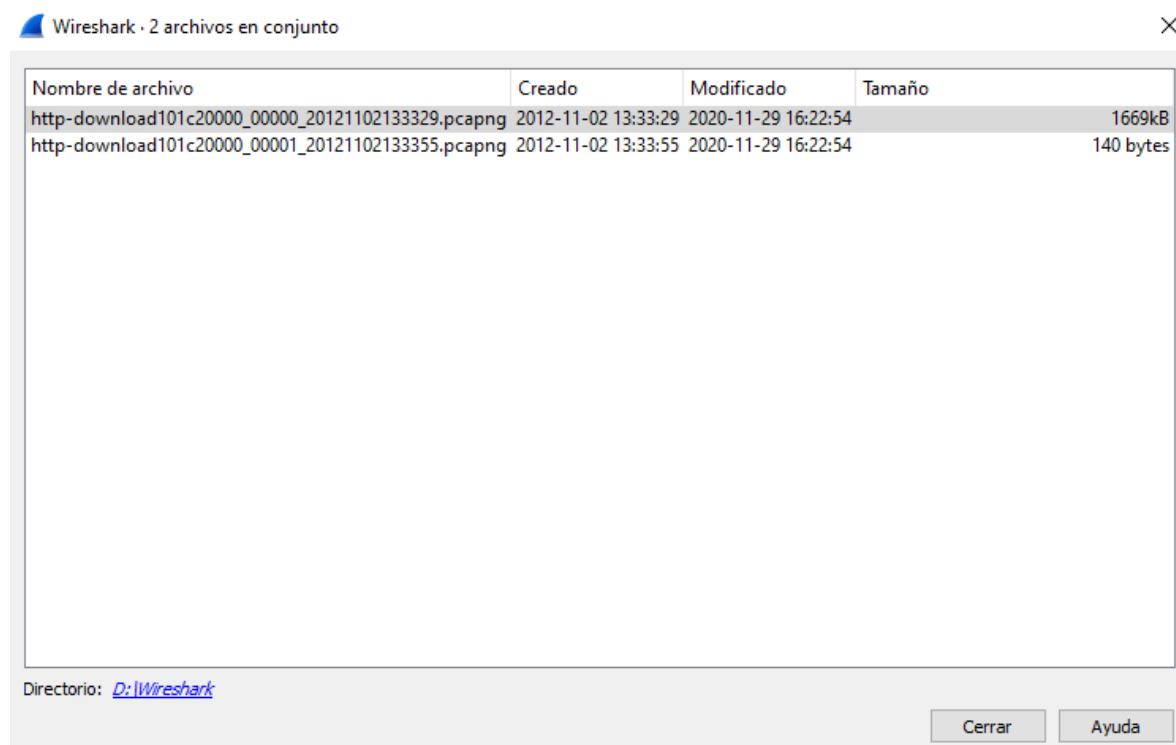
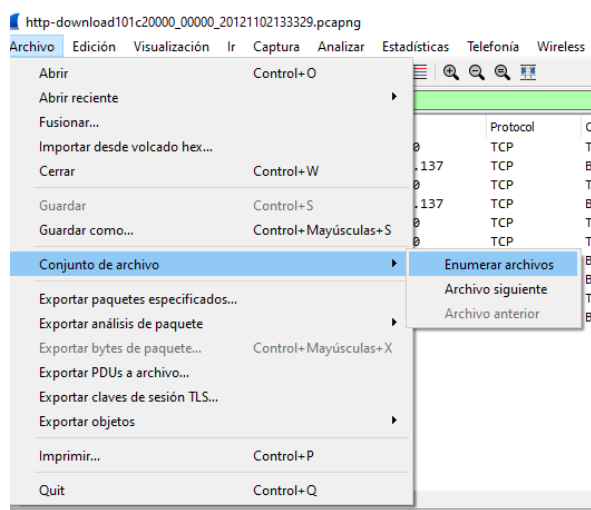
Abriremos el wireshark y buscaremos el archivo que creamos anteriormente



Una vez 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 puede observar la barra de estados para verificar cuantos paquetes coincidieron con el filtro en cada uno de los archivos de seguimiento.