Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

Lab42 - Split a File and Work with Filtered File Sets

Docente: Ing. Ismael Jiménez Sánchez

Alumno: Uc Uc César Enrique

Lab42 - Split a File and Work with Filtered File Sets

Antes de iniciar, debemos de abrir el archivo htt-download101c.pcapng en Wireshark

1 Abrimos el cmd o powershell

2 Nos dirigimos donde esta nuestra carpeta de descargas de los archivos de Wireshark

```
C:\Users\ameri\Videos\wireshark101v2files>
```

3 Escribimos el siguiente comando capinfos http-download101c.pcapng y le damos enter

Como podemos observar contiene 25000 paquetes

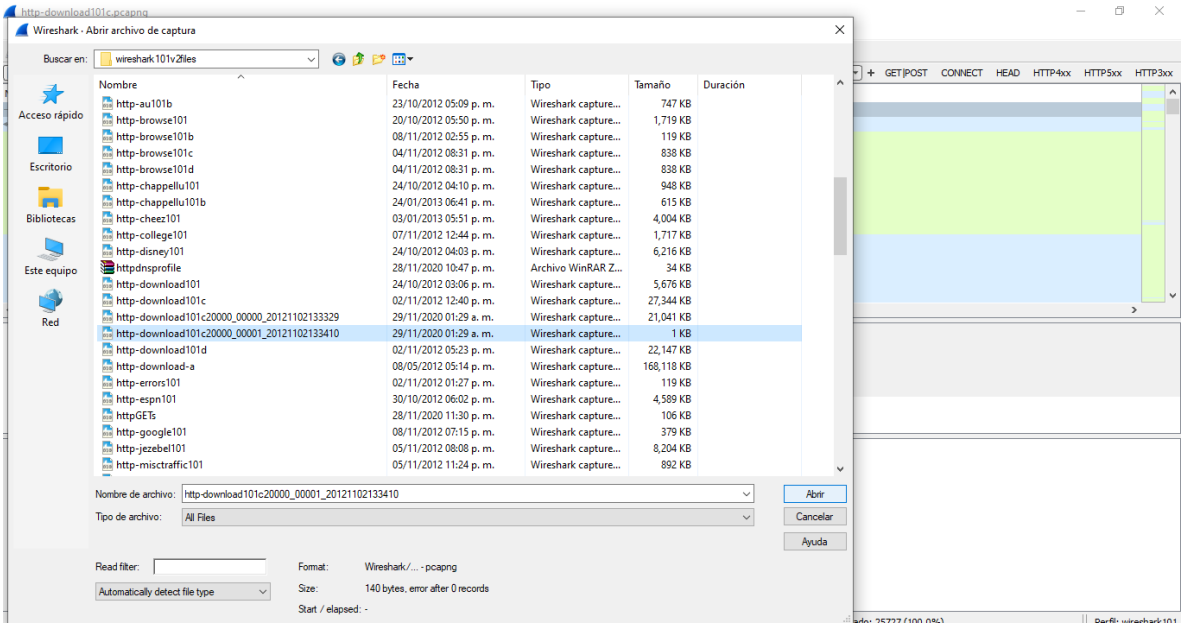
```
C:\Users\ameri\Videos\wireshark101v2files>capinfos http-download101c.pcapng
File name:           http-download101c.pcapng
File type:           Wireshark/... - pcapng
File encapsulation:  Ethernet
File timestamp precision:  microseconds (6)
Packet size limit:   file hdr: (not set)
Number of packets:   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
                     Time precision = microseconds (6)
                     Time ticks per second = 1000000
                     Time resolution = 0x06
                     Operating system = 64-bit Windows 7 Service Pack 1, build 7601
                     Number of stat entries = 1
                     Number of packets = 25727
Number of resolved IPv4 addresses in file: 2892
```

4 Escribimos el siguiente comando editcap –c 2000 http-download101c.pcapng http-download101c20000.pcapng y le damos enter

Luego escribimos el comando dir http-download101c20000*.pcapng

```
C:\Users\ameri\Videos\wireshark101v2files>editcap -c 20000 http-download101c.pcapng http-download101c20000.pcapng
editcap: An internal error occurred while writing record 20001 of file "http-download101c.pcapng" to the file "http-download101c20000_00001_20121102133410.pcapng".
(pcapng: epb.interface_id (0) >= wdh->interface_data->len (0))

C:\Users\ameri\Videos\wireshark101v2files>dir http-download101c20000*.pcapng
 El volumen de la unidad C es Windows
 El número de serie del volumen es: 88D3-E838

 Directorio de C:\Users\ameri\Videos\wireshark101v2files

29/11/2020  01:29 a. m.        21,545,508 http-download101c20000_00000_20121102133329.pcapng
29/11/2020  01:29 a. m.               140 http-download101c20000_00001_20121102133410.pcapng
               2 archivos     21,545,648 bytes
               0 dirs  628,871,753,728 bytes libres

C:\Users\ameri\Videos\wireshark101v2files>
```

5 Entramos a Wireshark y abrimos el archivo creado en el paso anterior



6. Escribimos en filtros tcp.analysis.flags && !tcp.analysis.window_update

7 Seleccionamos File>File Set>List Files y seleccionamos el archivo que abrimos anteriormente