

## 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

```
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>tshark -D
1. \Device\NPF_{8D659504-8894-459B-A5FD-E8C588ABDA4C} (Conexión de área local* 10)
2. \Device\NPF_{EDDC87F2-4FE5-4E91-AD2E-DF3B9B7D689E} (Conexión de área local* 8)
3. \Device\NPF_{6FC70BCA-6013-4177-8AE1-501289E4C2C4} (Wi-Fi)
4. \Device\NPF_{5C9A7C99-F38D-4FC0-810A-2D8C7EA58A27} (Conexión de área local* 1)
5. \Device\NPF_{C23BB2EC-CCAE-4205-82DC-4B0ACFC9EE62} (Conexión de red Bluetooth)
6. \Device\NPF_{B1336373-488E-45CE-B84A-9A4EC91DC917} (Conexión de área local* 9)
7. \Device\NPF_{DECCDB71-36C7-4FDE-A98D-703002CA9382} (Conexión de área local* 2)
8. \Device\NPF_{Loopback (Adapter for loopback traffic capture)} (Ethernet)
9. \Device\NPF_{84225919-4529-4CA2-B198-DA71AE941723} (Ethernet)
10. ciscodump (Cisco remote capture)
11. randpkt (Random packet generator)
12. sshdump.exe (SSH remote capture, custom version)
13. udpdump (UDP Listener remote capture)

D:\wireshark>
```

```
Capture stop conditions:
-c <packet count> stop after n packets (def: infinite)
-a <autostop cond.> ..., --autostop <autostop cond.> ...
    duration:NUM - stop after NUM seconds
    filesize:NUM - stop this file after NUM KB
    files:NUM - stop after NUM files
    packets:NUM - stop after NUM packets

Capture output:
-b <ringbuffer opt.> ..., --ring-buffer <ringbuffer opt.>
    duration:NUM - switch to next file after NUM secs
    filesize:NUM - switch to next file after NUM KB
    files:NUM - ringbuffer: replace after NUM files
    packets:NUM - switch to next file after NUM packets
    interval:NUM - switch to next file when the time is
                    an exact multiple of NUM secs

PCAP options:
```

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

```
D:\Wireshark>tshark -i3 -a files:6 -b duration:30 -w mytshark.pcapng
Capturing on 'Wi-Fi'
3295
```

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.

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

Directorio de D:\Wireshark

28/11/2020  10:02 p. m.          481,960 mytshark_00001_20201128220200.pcapng
28/11/2020  10:03 p. m.          352,544 mytshark_00002_20201128220230.pcapng
28/11/2020  10:03 p. m.          608,744 mytshark_00003_20201128220300.pcapng
28/11/2020  10:04 p. m.          401,668 mytshark_00004_20201128220331.pcapng
28/11/2020  10:04 p. m.           43,048 mytshark_00005_20201128220401.pcapng
28/11/2020  10:05 p. m.           27,056 mytshark_00006_20201128220432.pcapng
               6 archivos          1,915,020 bytes
               0 dirs  727,071,092,736 bytes libres

D:\Wireshark>
```