Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

Lab44 - Use Tshark to Capture to File Sets with an Autostop Condition

Docente: Ing. Ismael Jiménez Sánchez

Alumno: Uc Uc César Enrique

Lab44 - Use Tshark to Capture to File Sets with an Autostop Condition

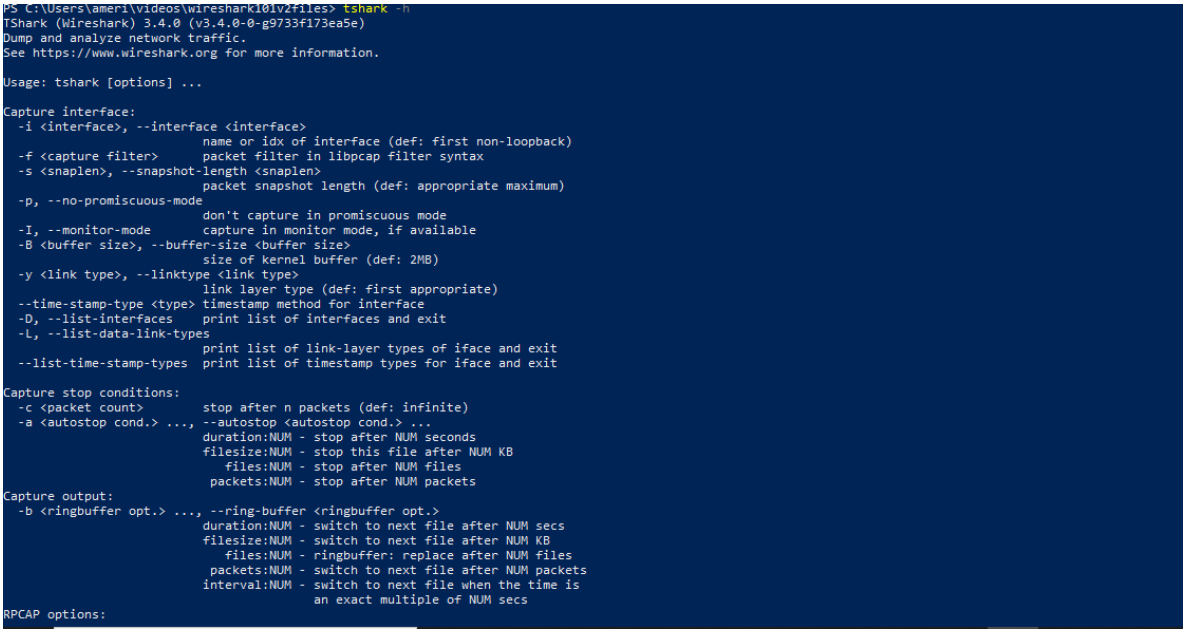
1 Abrimos el cmd o powershell

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

```
PS C:\Users\ameri\videos> cd wireshark101v2files
```

3 Ponemos el comando de tshark –h, observamos la sección de Capture stop conditions y Capture output

```
PS C:\Users\ameri\videos\wireshark101v2files> tshark -h
```



```
PS C:\Users\ameri\videos\wireshark101v2files> tshark -h
TShark (Wireshark) 3.4.0 (v3.4.0-0-g9733f173ea5e)
Dump and analyze network traffic.
See https://www.wireshark.org for more information.

Usage: tshark [options] ...

Capture interface:
  -i <interface>, --interface <interface>
                           name or idx of interface (def: first non-loopback)
  -f <capture filter>      packet filter in libpcap filter syntax
  -s <snaplen>, --snapshot-length <snaplen>
                           packet snapshot length (def: appropriate maximum)
  -p, --no-promiscuous-mode
                           don't capture in promiscuous mode
  -I, --monitor-mode       capture in monitor mode, if available
  -B <buffer size>, --buffer-size <buffer size>
                           size of kernel buffer (def: 2MB)
  -y <link type>, --linktype <link type>
                           link layer type (def: first appropriate)
  --time-stamp-type <type> timestamp method for interface
  -D, --list-interfaces    print list of interfaces and exit
  -L, --list-data-link-types
                           print list of link-layer types of iface and exit
  --list-time-stamp-types  print list of timestamp types for iface and exit

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

RPCAP options:
```

4 Ingresamos el comando de tshark –i 3 –a files:6 –b durarion:30 –w myshark.pcapng

```
PS C:\Users\ameri\videos\wireshark101v2files> tshark -i 3 -a files:6 -b duration:30 -w mytshark.pcapng
Capturing on 'Wi-Fi'
4579
```

5 Ingresamos ahora el comando dir mytshark*.*