



“Secretaría De La Educación Superior”
“Instituto Tecnológico de Cancún”

Ingeniería en Sistemas Computacionales

Materia: Fundamentos de Telecomunicaciones

Tema: Laboratorio N#44 Wireshark

Alumno: Vargas Rodríguez Javier Jesús

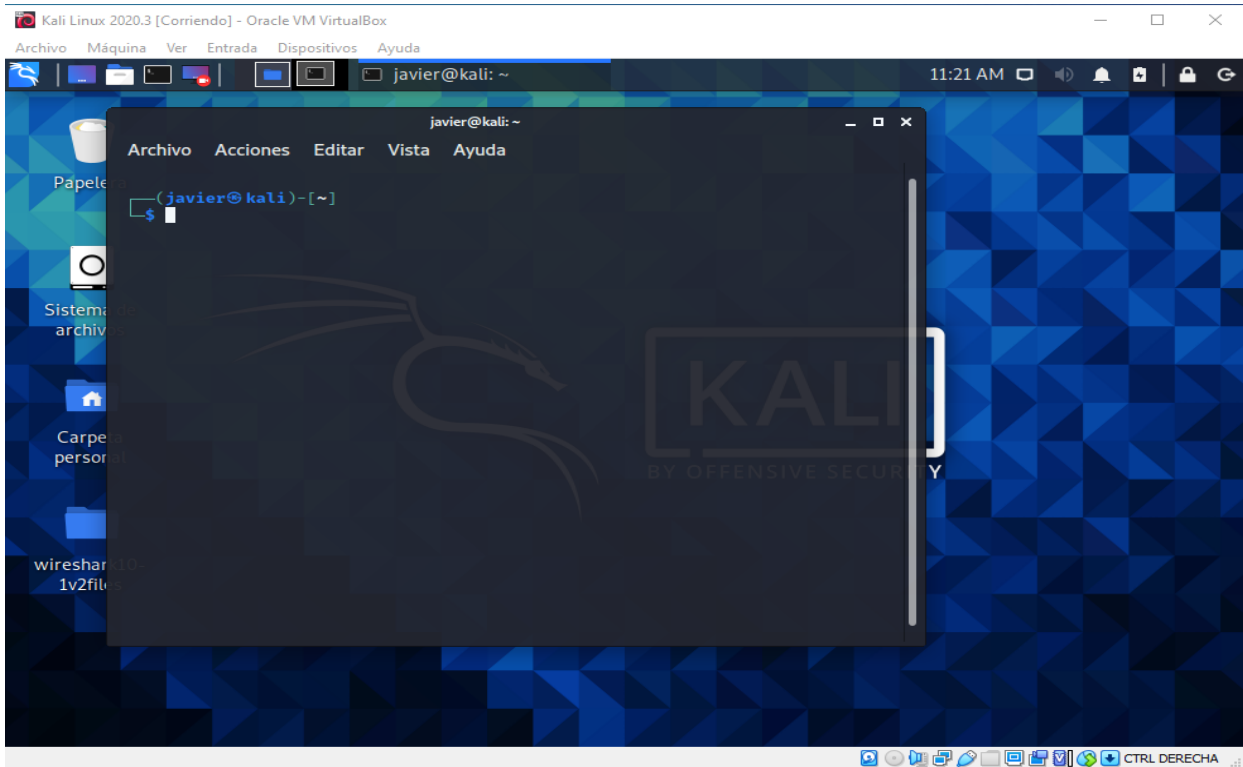
Maestro: Ismael Jiménez Sánchez

Fecha De Entrega: 8/Diciembre/2020

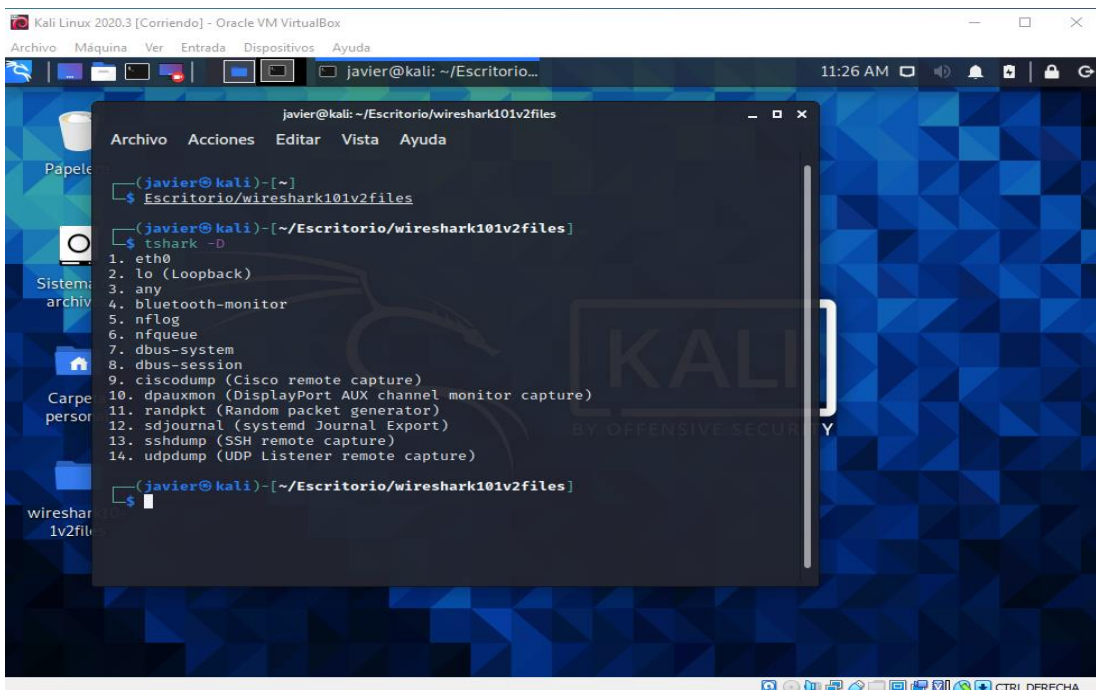
Horario: 5:00 pm – 6:00 pm

Laboratio N#44 – Use Tshark para capturar en conjunto de archivos con una condicion de detencion automatica.

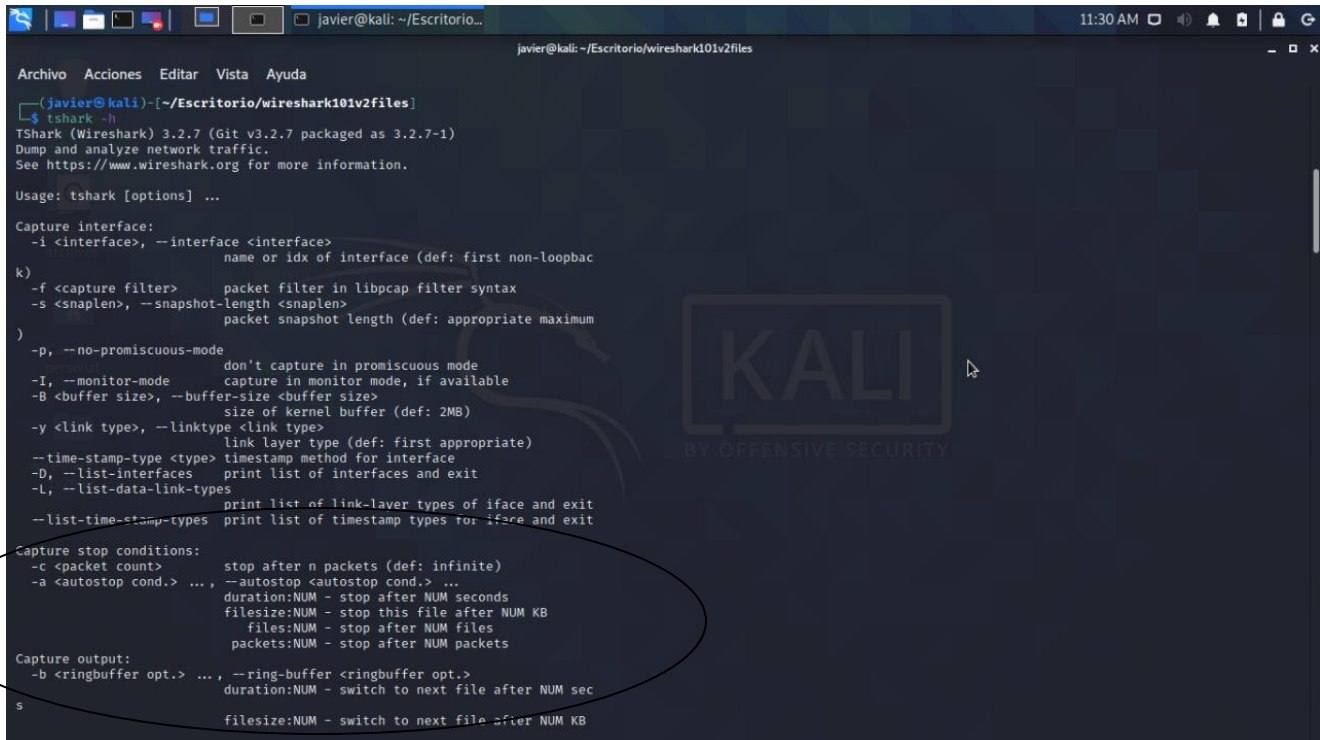
Paso 1 – Abrimos el símbolo del sistema.



Paso 2 – Navegamos hasta el directorio del archivo de seguimiento y escribimos Tshark -D



Paso 3 – Una vez que haya determinado que interfaz utilizar, vamos a escribir `tshark -h` para ver los parámetros para guardar en varios archivos.



```
javier@kali: ~/Escritorio...
javier@kali: ~/Escritorio/wireshark101v2files

(javier@kali)-[~/Escritorio/wireshark101v2files]
$ tshark -h
TShark (Wireshark) 3.2.7 (Git v3.2.7 packaged as 3.2.7-1)
Dump and analyze network traffic.
See https://www.wireshark.org for more information.

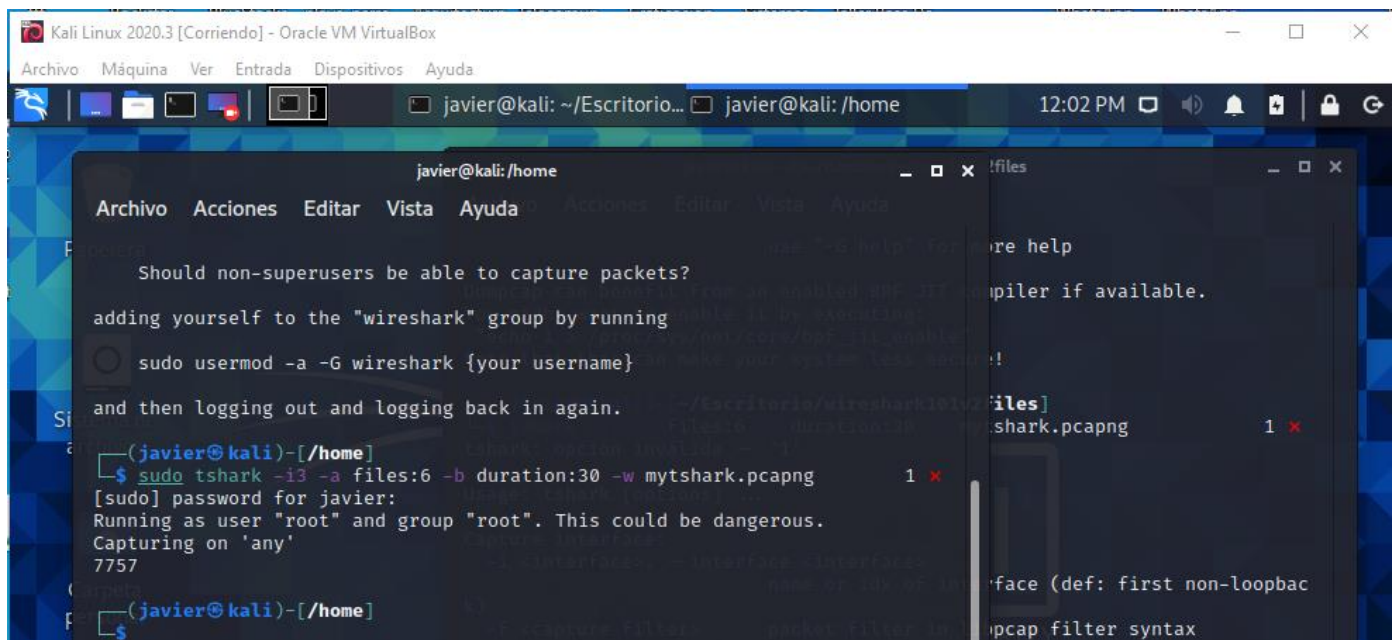
Usage: tshark [options] ...

Capture interface:
  -i <interface>, --interface <interface>
                                name or idx of interface (def: first non-loopbac
k)
  -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 sec
s
                                filesize:NUM - switch to next file after NUM KB
```

Paso 4 – Usaremos el siguiente comando y nos tenemos que quedar 3 minutos esperando en la página de Wireshark.org para que capture los datos.



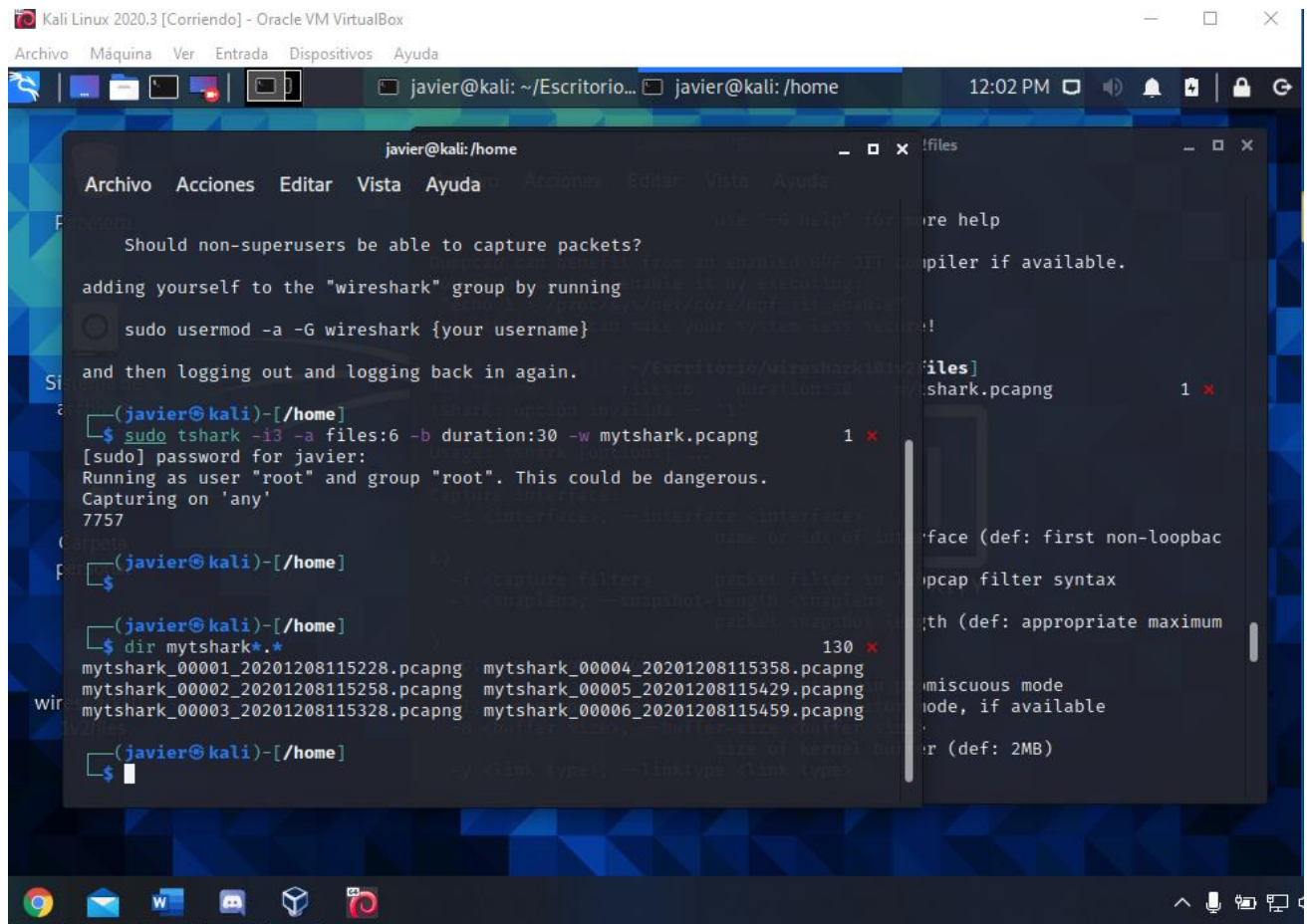
```
Kali Linux 2020.3 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
javier@kali: ~/Escritorio... javier@kali: /home
12:02 PM

javier@kali: /home
Archivo Acciones Editar Vista Ayuda
Should non-superusers be able to capture packets?
adding yourself to the "wireshark" group by running
sudo usermod -a -G wireshark {your username}
and then logging out and logging back in again.

(javier@kali)-[/home]
$ sudo tshark -i3 -a files:6 -b duration:30 -w mytshark.pcapng
[sudo] password for javier:
Running as user "root" and group "root". This could be dangerous.
Capturing on 'any'
7757

(javier@kali)-[/home]
$
```

Paso 5 – Ahora usamos el dir mytshark*. * y nos debe mostrar lo siguiente:



```
Kali Linux 2020.3 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
javier@kali: ~/Escritorio... javier@kali: /home 12:02 PM

javier@kali: /home
Archivo Acciones Editar Vista Ayuda
Should non-superusers be able to capture packets?
adding yourself to the "wireshark" group by running
sudo usermod -a -G wireshark {your username}
and then logging out and logging back in again.

(javier@kali)-[/home]
$ sudo tshark -i3 -a files:6 -b duration:30 -w mytshark.pcapng
[sudo] password for javier:
Running as user "root" and group "root". This could be dangerous.
Capturing on 'any'
7757

(javier@kali)-[/home]
$
$ dir mytshark*.*
130
mytshark_00001_20201208115228.pcapng mytshark_00004_20201208115358.pcapng
mytshark_00002_20201208115258.pcapng mytshark_00005_20201208115429.pcapng
mytshark_00003_20201208115328.pcapng mytshark_00006_20201208115459.pcapng

(javier@kali)-[/home]
$
```