



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

Ingeniería en Sistemas Computacionales

Materia: Fundamentos de Telecomunicaciones

Tema: Laboratorio N#42 Wireshark

Alumno: Vargas Rodríguez Javier Jesús

Maestro: Ismael Jiménez Sánchez

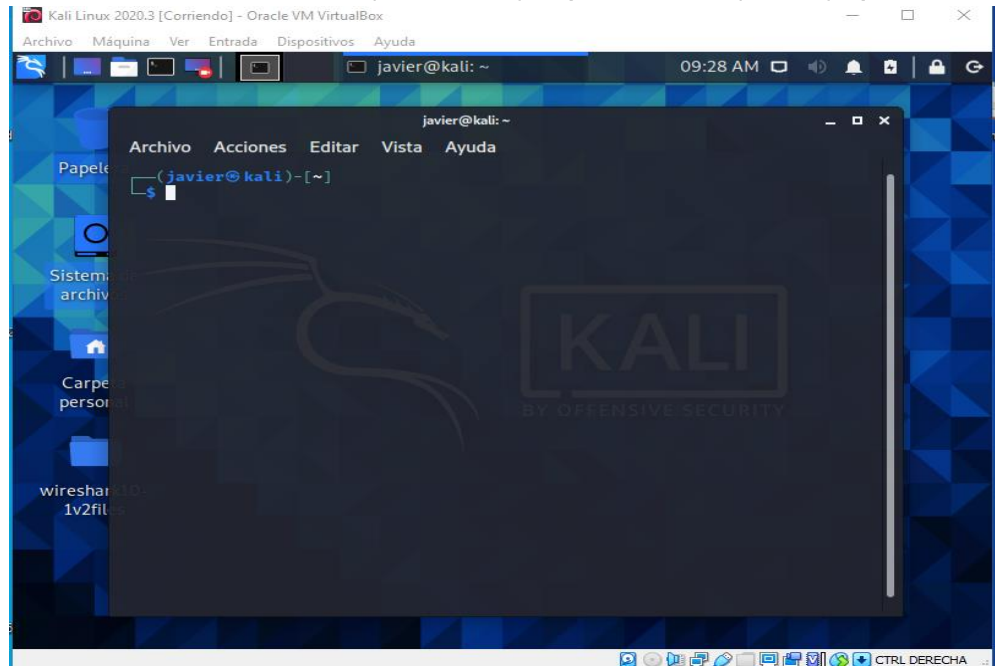
Fecha De Entrega: 6/Diciembre/2020

Horario: 5:00 pm – 6:00 pm

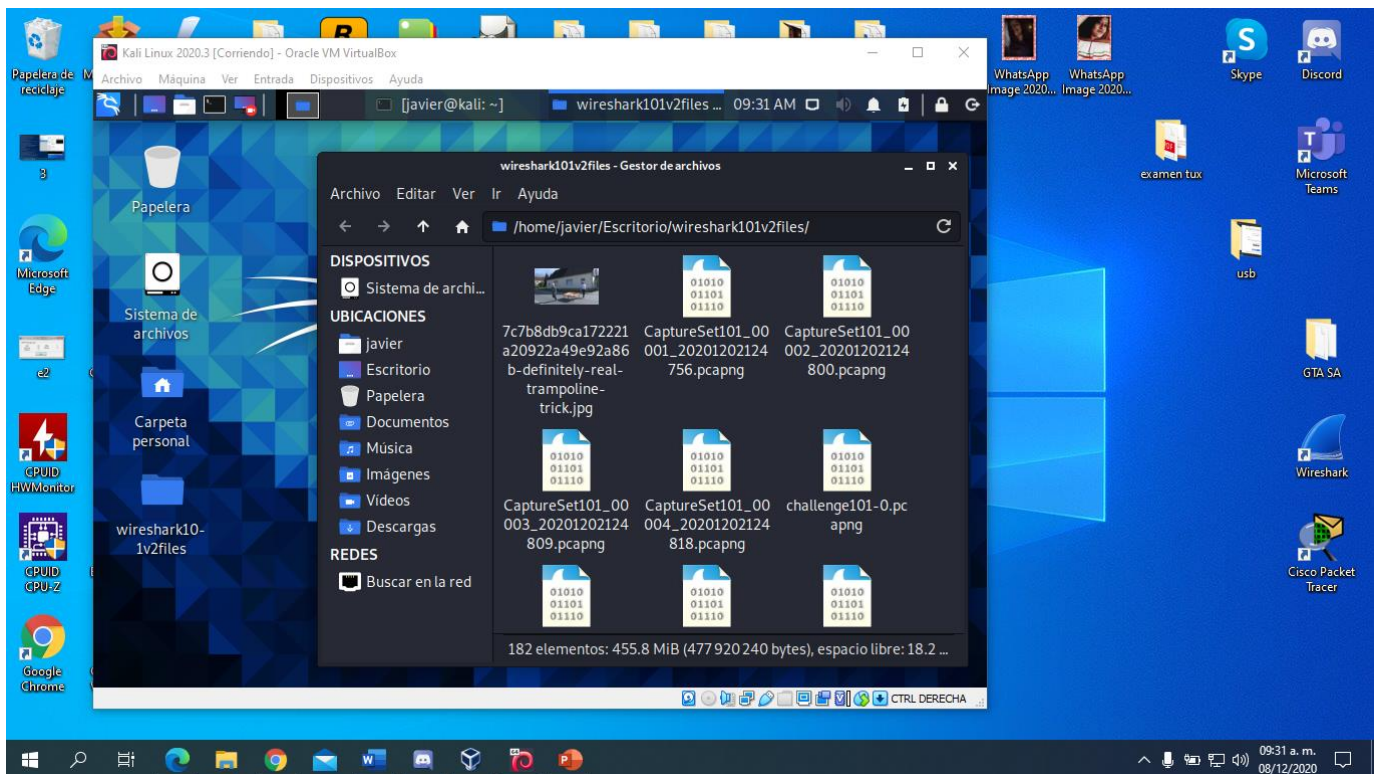
Laboratio N#42 – Dividir un archivo y trabajar con conjuntos filtrados de archivos.

Vamos a trabajar con el archivo http-download-c.pcapng en este laboratorio.

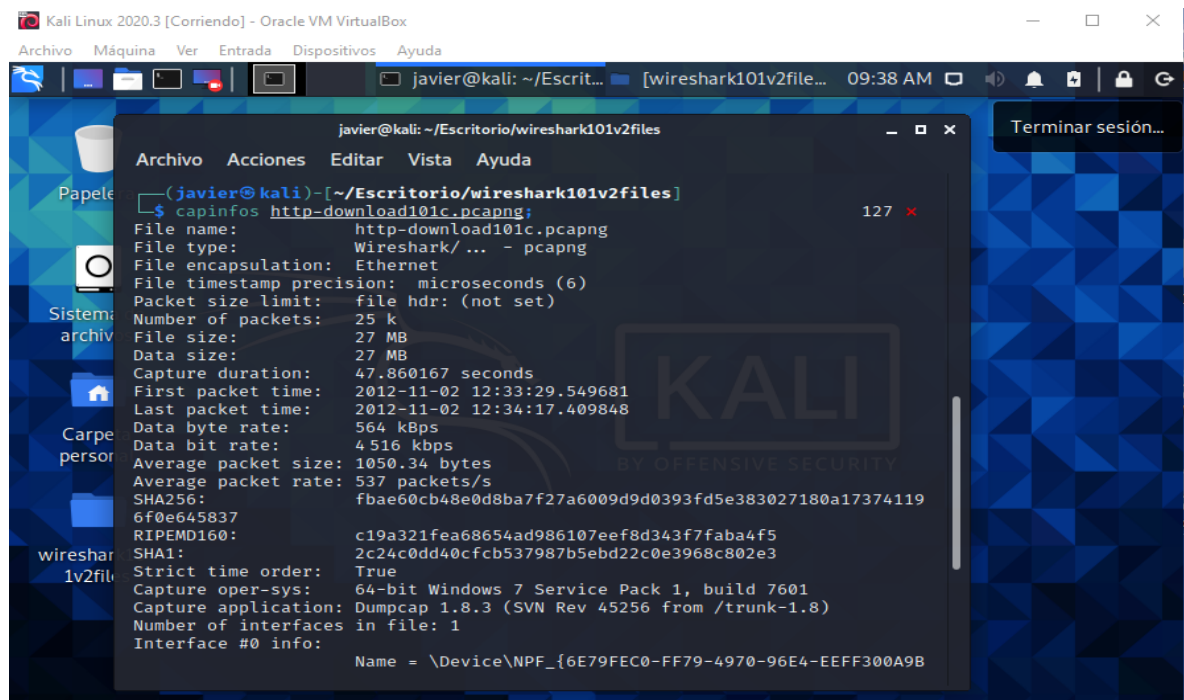
Paso 1 – Abrimos el símbolo del sistema (Windows) o puede ser (Linux) que es mi caso.



Paso 2 – Navegamos en el directorio de archivos de seguimiento.

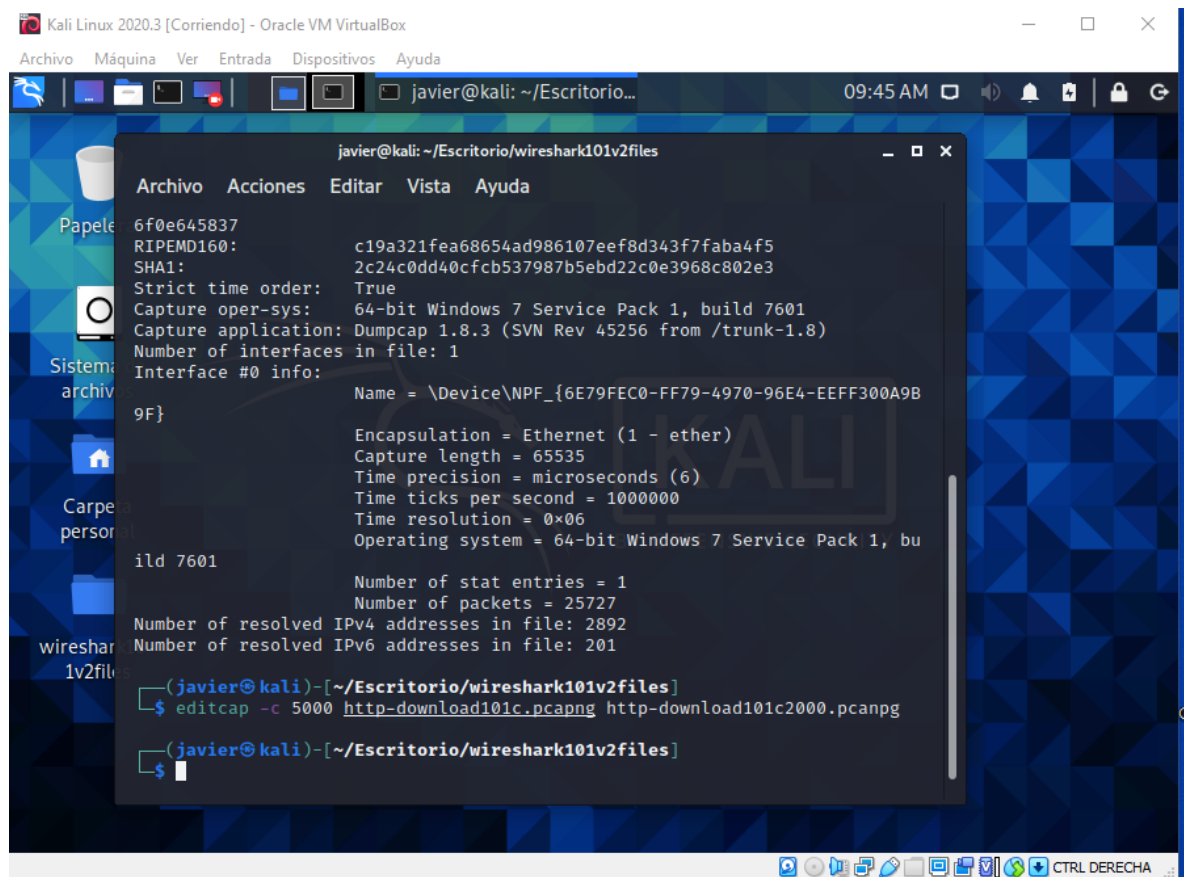


Paso 3 – Se va a dividir este archivo según el recuento de paquetes, vamos a escribir en la consola; capinfos “http-download101c.pcapng



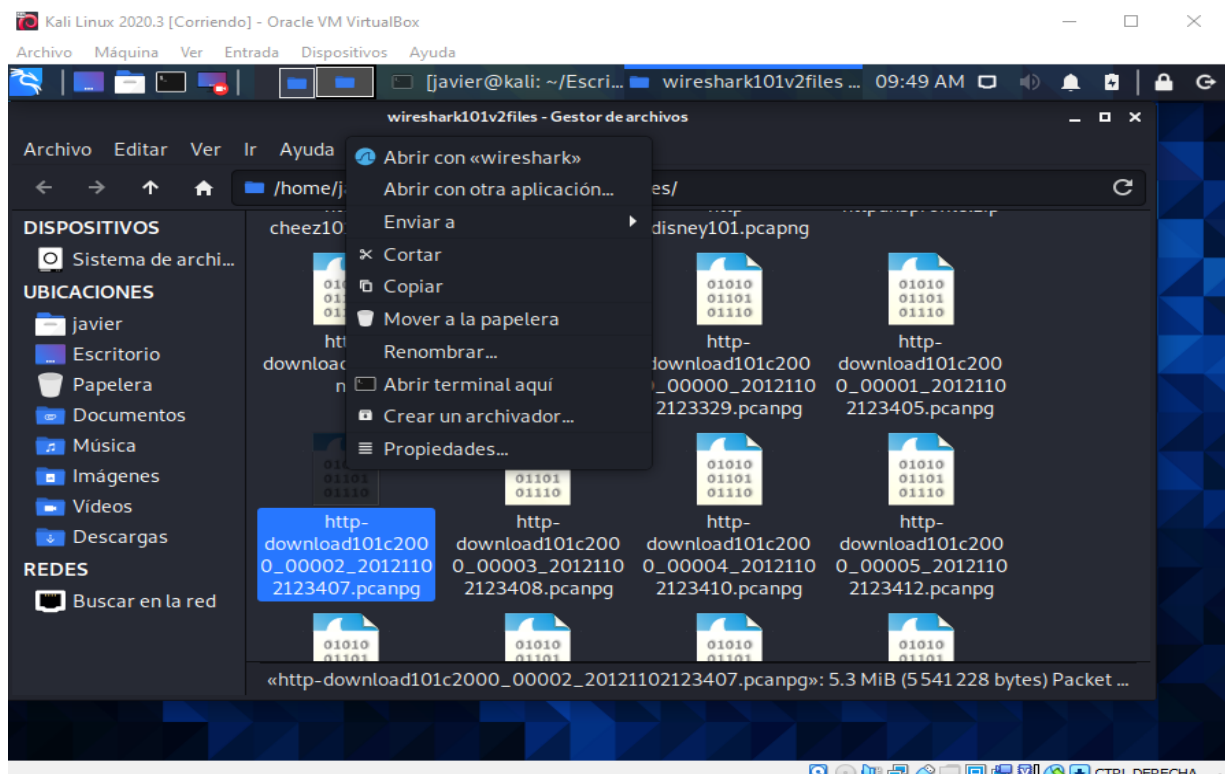
```
javier@kali: ~/Escritorio/wireshark101v2files
Archivo Acciones Editar Vista Ayuda
(javier@kali)-[~/Escritorio/wireshark101v2files]
$ capinfos http-download101c.pcapng
File name: http-download101c.pcapng
File type: Wireshark/... - pcapng
File encapsulation: Ethernet
File timestamp precision: microseconds (6)
Packet size limit: file hdr: (not set)
Number of packets: 25 k
File size: 27 MB
Data size: 27 MB
Capture duration: 47.860167 seconds
First packet time: 2012-11-02 12:33:29.549681
Last packet time: 2012-11-02 12:34:17.409848
Data byte rate: 564 kBps
Data bit rate: 4 516 kbps
Average packet size: 1050.34 bytes
Average packet rate: 537 packets/s
SHA256: fbae60cb48e0d8ba7f27a6009d9d0393fd5e383027180a17374119
6f0e645837
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-EEFF300A9B
9F}
```

Paso 4 – Escribimos los comandos;

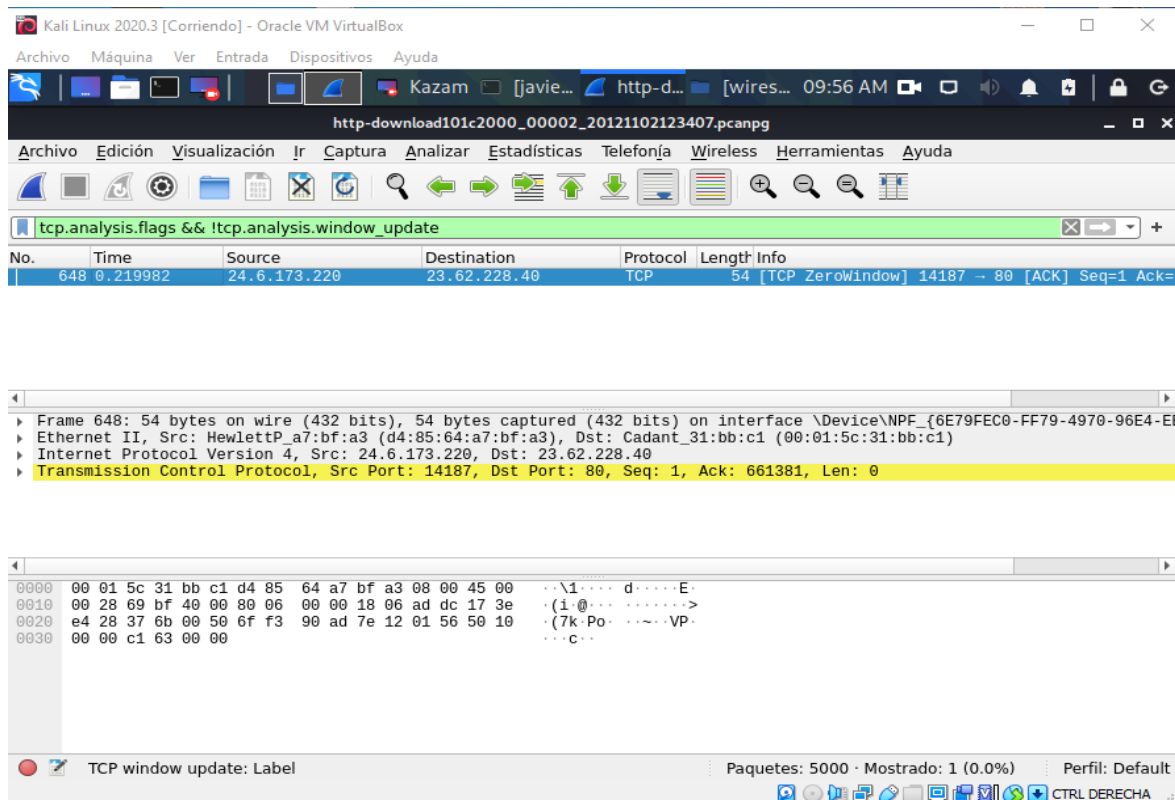


```
javier@kali: ~/Escritorio/wireshark101v2files
Archivo Acciones Editar Vista Ayuda
6f0e645837
RIPEMD160: c19a321fea68654ad986107eef8d343f7faba4f5
SHA1: 2c24c0dd40cfcb537987b5ebd22c0e3968c802e3
Strict time order: True
Capture oper-sys: 64-bit Windows 7 Service Pack 1, build 7601
Capture application: 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-EEFF300A9B
9F}
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, bu
ild 7601
Number of stat entries = 1
Number of packets = 25727
Number of resolved IPv4 addresses in file: 2892
Number of resolved IPv6 addresses in file: 201
(javier@kali)-[~/Escritorio/wireshark101v2files]
$ editcap -c 5000 http-download101c.pcapng http-download101c2000.pcanpg
(javier@kali)-[~/Escritorio/wireshark101v2files]
$
```

Paso 5 – Iniciamos Wireshark y seleccionamos Archivo | y seleccionamos el archivo numerado _00002 que se creo en el paso 4.



Paso 6 – Ahora escribimos tcp.analysis.flags && !tcp.analysis.window_update:



Paso 7 – Seleccionamos Archivos | Conjunto de archivos y hacer clic para mostrar los archivos.

