INSTITUTO TECNOLOGICO DE CANCUN

Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 42

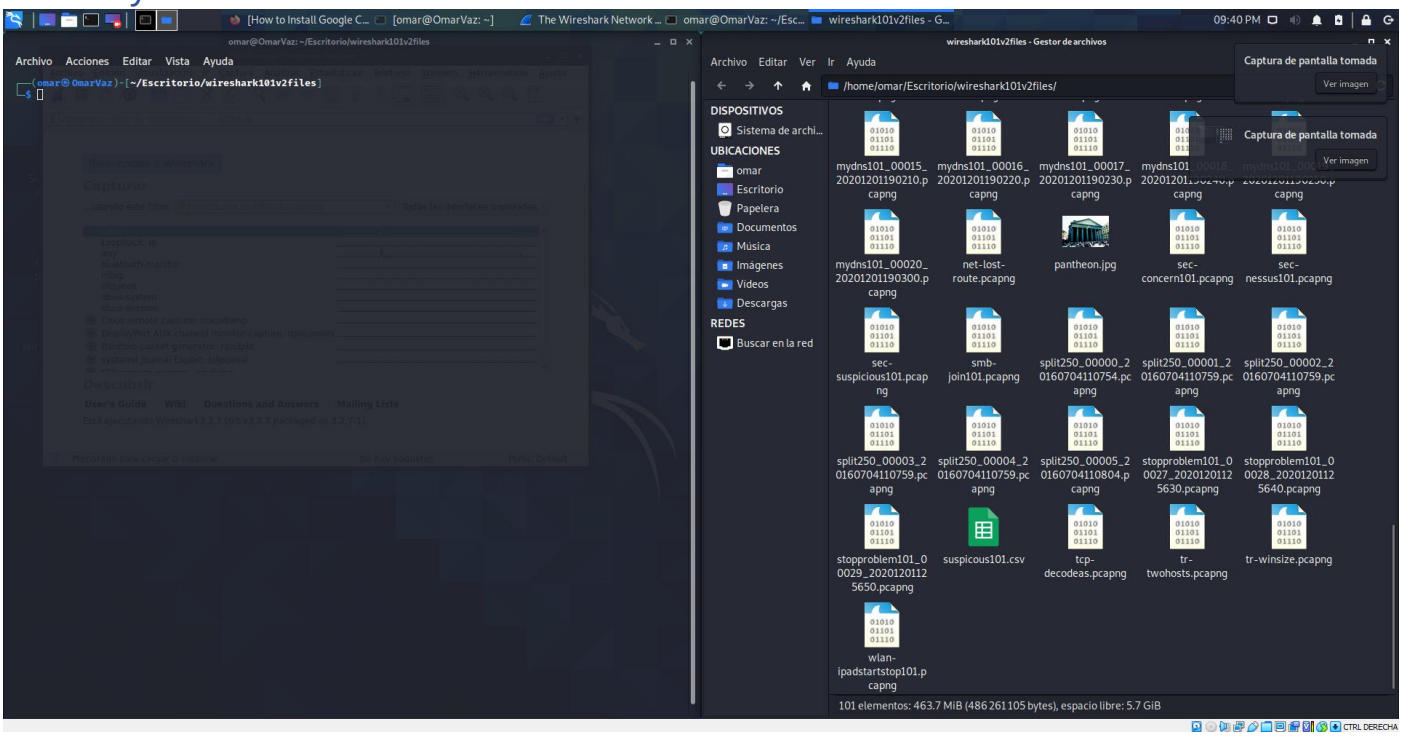
Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

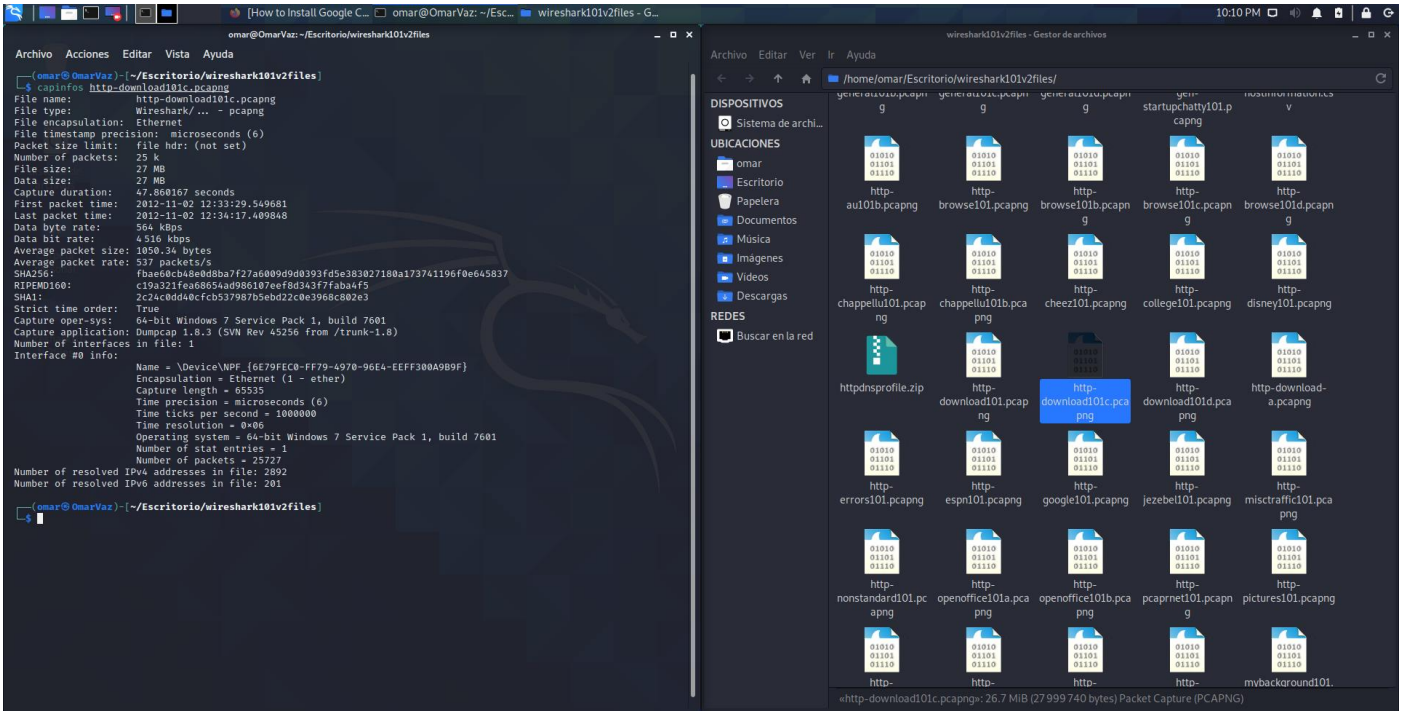
Lab42- Split a File and Work with Filtered File Sets

Este laboratorio tuve que hacerlo en Kali Linux ya que powershell y cmd no me detectaba los comandos asi que use Kali Linux para hacer este laboratorio lamento las molestias

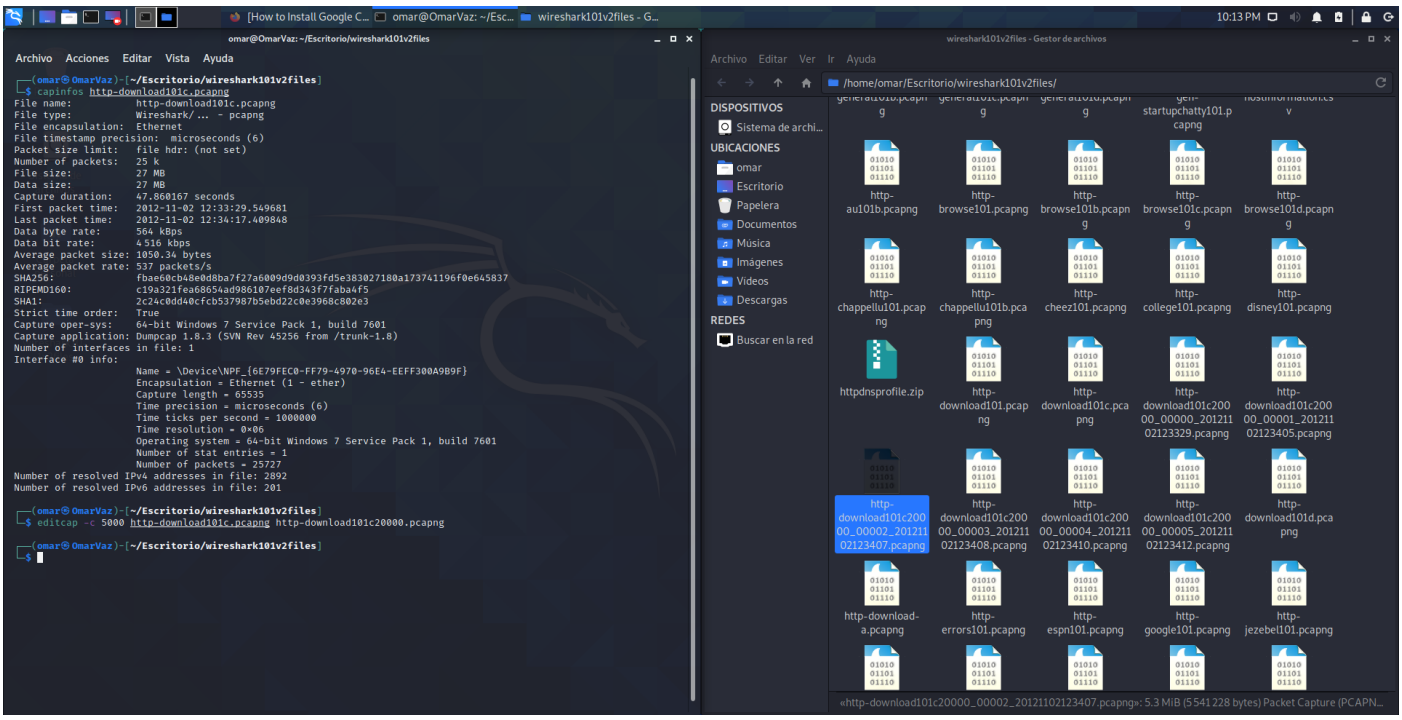
Paso 1 y 2:



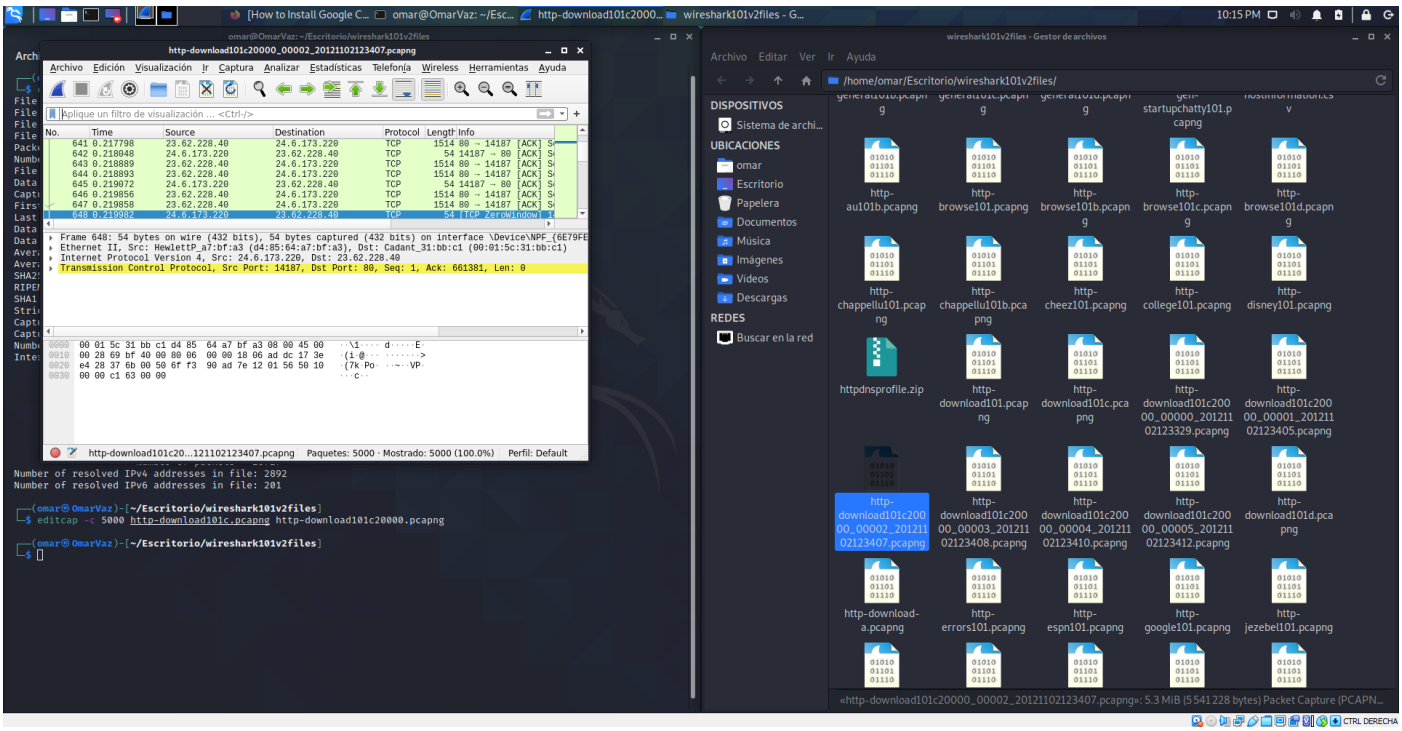
Paso 3



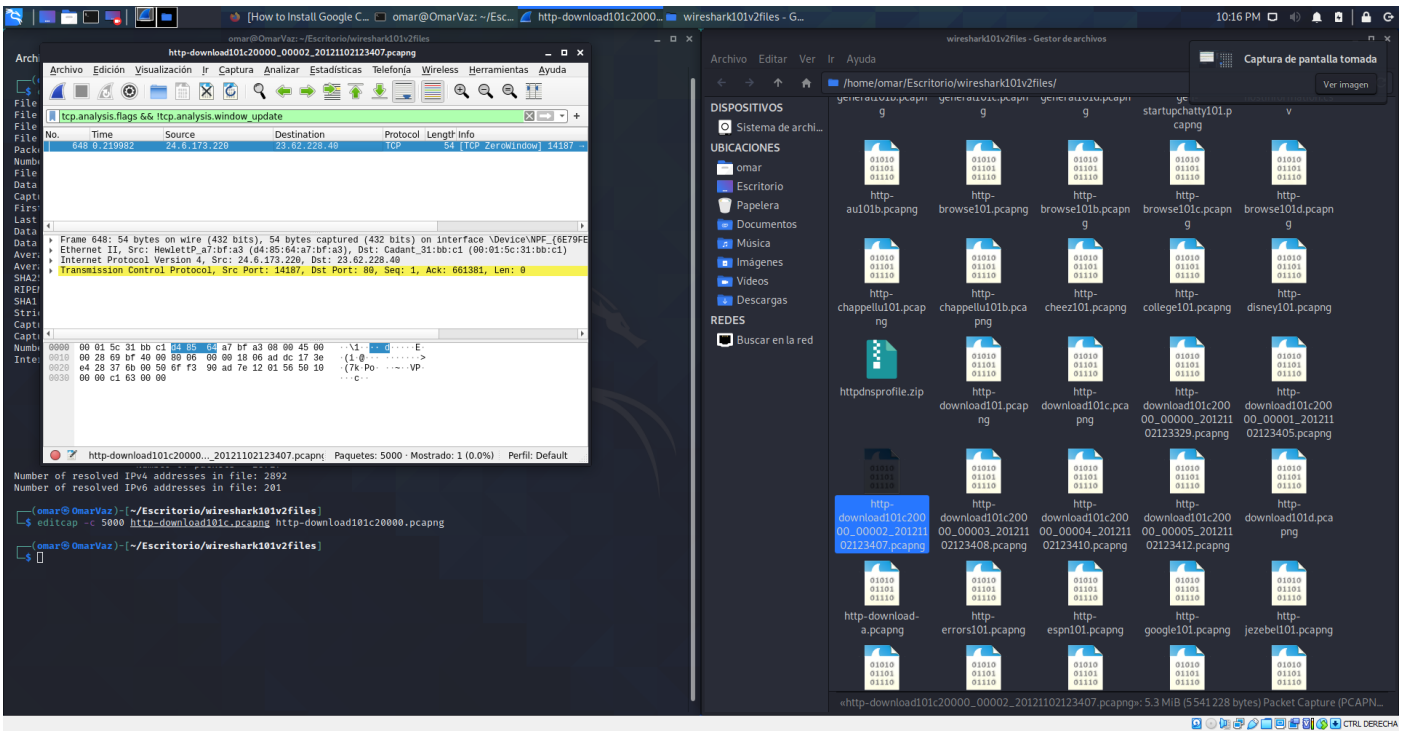
Paso 4:


omar@OmarVaz: ~/Escritorio/wireshark101v2files
Archivo Acciones Editar Vista Ayuda
(omar㉿OmarVaz)-[~/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: 4516 kbps
Average packet size: 1050.34 bytes
Average packet rate: 537 packets/s
SHA256: fbae60cb48e0d8ba7f27a6009d9d0393fd5e383027180a173741196f0e645837
RIPEMD160: c19a321fea68654ad986107eef8d343f7faba4f5
SHA1: 2c24c0dd40cfcb537987b5eb22c0e3968c802e3
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
Number of resolved IPv6 addresses in file: 201
(omar㉿OmarVaz)-[~/Escritorio/wireshark101v2files]
$ editcap -c 5000 http-download101c.pcapng http-download101c20000.pcapng
(omar㉿OmarVaz)-[~/Escritorio/wireshark101v2files]
$
wireshark101v2files - Gestor de archivos
/home/omar/Escritorio/wireshark101v2files/
DISPOSITIVOS
UBICACIONES
REDES
http-au101b.pcapng
http-browse101.pcapng
http-browse101b.pcapng
http-browse101c.pcapng
http-browse101d.pcapng
http-chappellu101.pcapng
http-chappellu101b.pcapng
http-cheez101.pcapng
http-college101.pcapng
http-disney101.pcapng
httpdnsprofile.zip
http-download101.pcapng
http-download101c.pcapng
http-download101c20000_00000_20121102123329.pcapng
http-download101c20000_00001_20121102123405.pcapng
http-download101c20000_00002_20121102123407.pcapng
http-download101c20000_00003_20121102123408.pcapng
http-download101c20000_00004_20121102123410.pcapng
http-download101c20000_00005_20121102123412.pcapng
http-download101d.pcapng
http-download-a.pcapng
http-errors101.pcapng
http-espn101.pcapng
http-google101.pcapng
http-jezebel101.pcapng
«http-download101c20000_00002_20121102123407.pcapng»: 5.3 MiB (5 541 228 bytes) Packet Capture (PCAPN...

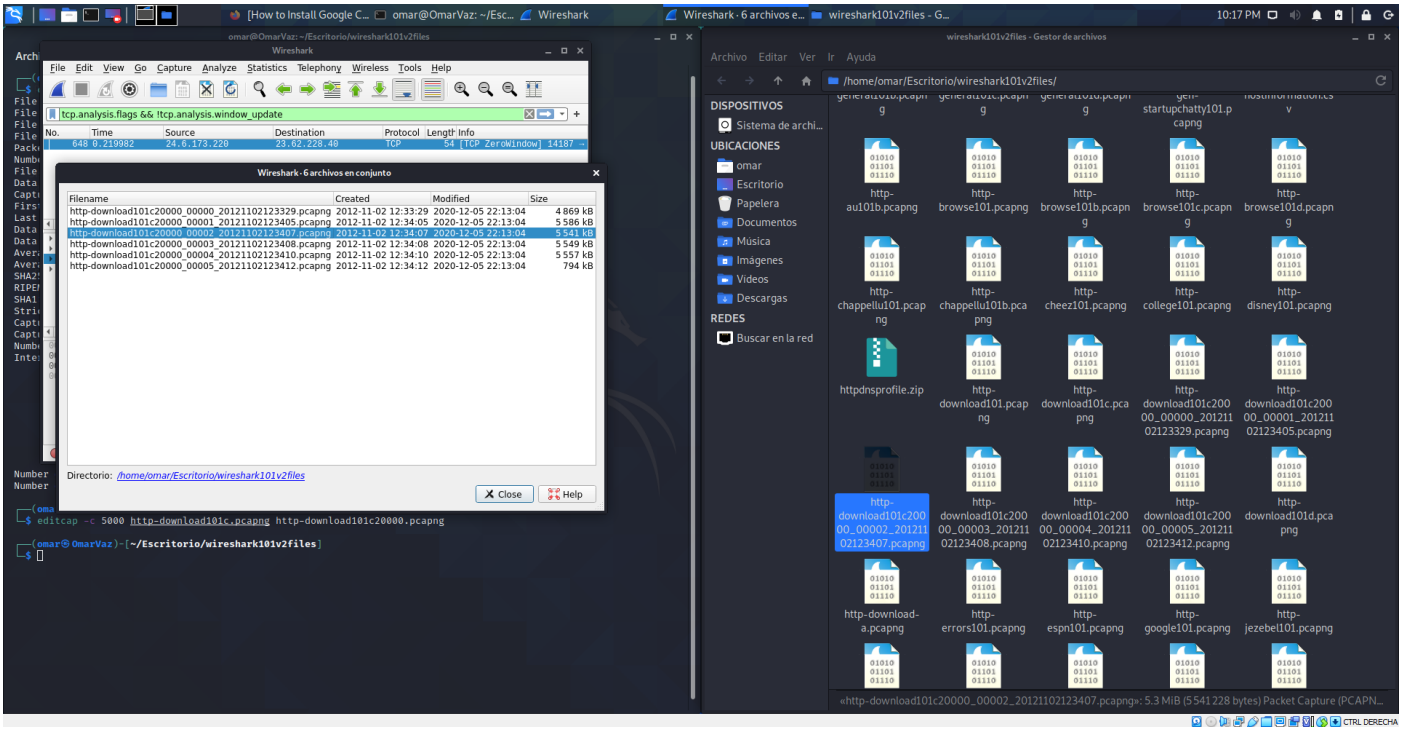
Paso 5:


http-download101c20000_00002_20121102123407.pcapng
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
641 0.217798 23.62.228.40 24.6.173.220 TCP 1514 80 → 14187 [ACK] Seq=
642 0.218048 24.6.173.220 23.62.228.40 TCP 54 14187 → 80 [ACK] Seq=
643 0.218889 23.62.228.40 24.6.173.220 TCP 1514 80 → 14187 [ACK] Seq=
644 0.218893 23.62.228.40 24.6.173.220 TCP 1514 80 → 14187 [ACK] Seq=
645 0.219072 24.6.173.220 23.62.228.40 TCP 54 14187 → 80 [ACK] Seq=
646 0.219856 23.62.228.40 24.6.173.220 TCP 1514 80 → 14187 [ACK] Seq=
647 0.219858 23.62.228.40 24.6.173.220 TCP 1514 80 → 14187 [ACK] Seq=
648 0.219982 24.6.173.220 23.62.228.40 TCP 54 [TCP ZeroWindow]
Frame 648: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{6E79FE
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 23.62.228.40
Transmission Control Protocol, Src Port: 14187, Dst Port: 80, Seq: 1, Ack: 661381, Len: 0
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 00 28 69 bf 40 00 80 06 00 00 18 06 ad dc 17 3e
0020 e4 28 37 6b 00 50 6f f3 90 ad 7e 12 01 56 50 10
0030 00 00 c1 63 00 00
http-download101c20...121102123407.pcapng Paquetes: 5000 · Mostrado: 5000 (100.0%) Perfil: Default
Number of resolved IPv4 addresses in file: 2892
Number of resolved IPv6 addresses in file: 201
(omar㉿OmarVaz)-[~/Escritorio/wireshark101v2files]
$ editcap -c 5000 http-download101c.pcapng http-download101c20000.pcapng
(omar㉿OmarVaz)-[~/Escritorio/wireshark101v2files]
$
wireshark101v2files - Gestor de archivos
/home/omar/Escritorio/wireshark101v2files/
DISPOSITIVOS
UBICACIONES
REDES
«http-download101c20000_00002_20121102123407.pcapng»: 5.3 MiB (5 541 228 bytes) Packet Capture (PCAPN...

Paso 6:


http-download101c20000_00002_20121102123407.pcapng
tcp.analysis.flags && !tcp.analysis.window_update
No. Time Source Destination Protocol Length Info
648 0.219982 24.6.173.220 23.62.228.40 TCP 54 [TCP ZeroWindow] 14187
Frame 648: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{6E79FE
Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 23.62.228.40
Transmission Control Protocol, Src Port: 14187, Dst Port: 80, Seq: 1, Ack: 661381, Len: 0
Number of resolved IPv4 addresses in file: 2892
Number of resolved IPv6 addresses in file: 201
editcap -c 5000 http-download101c.pcapng http-download101c20000.pcapng
Captura de pantalla tomada
Ver imagen
/home/omar/Escritorio/wireshark101v2files/
DISPOSITIVOS
UBICACIONES
REDES
http-download101c20000_00002_20121102123407.pcapng
«http-download101c20000_00002_20121102123407.pcapng»: 5.3 MiB (5 541 228 bytes) Packet Capture (PCAPN...

Paso 7


Wireshark · 6 archivos en conjunto
Filename Created Modified Size
http-download101c20000_00000_20121102123329.pcapng 2012-11-02 12:33:29 2020-12-05 22:13:04 4 869 kB
http-download101c20000_00001_20121102123405.pcapng 2012-11-02 12:34:05 2020-12-05 22:13:04 5 586 kB
http-download101c20000_00002_20121102123407.pcapng 2012-11-02 12:34:07 2020-12-05 22:13:04 5 541 kB
http-download101c20000_00003_20121102123408.pcapng 2012-11-02 12:34:08 2020-12-05 22:13:04 5 549 kB
http-download101c20000_00004_20121102123410.pcapng 2012-11-02 12:34:10 2020-12-05 22:13:04 5 557 kB
http-download101c20000_00005_20121102123412.pcapng 2012-11-02 12:34:12 2020-12-05 22:13:04 794 kB
Directorio: /home/omar/Escritorio/wireshark101v2files
Close
Help
editcap -c 5000 http-download101c.pcapng http-download101c20000.pcapng
/home/omar/Escritorio/wireshark101v2files/
DISPOSITIVOS
UBICACIONES
REDES
http-download101c20000_00002_20121102123407.pcapng
«http-download101c20000_00002_20121102123407.pcapng»: 5.3 MiB (5 541 228 bytes) Packet Capture (PCAPN...