

## **Ingeniería en Sistemas Computacionales**

**Materia:** Fundamentos de Telecomunicaciones

**Tema:** Laboratorio N#19 Wireshark

**Alumno:** Vargas Rodríguez Javier Jesús

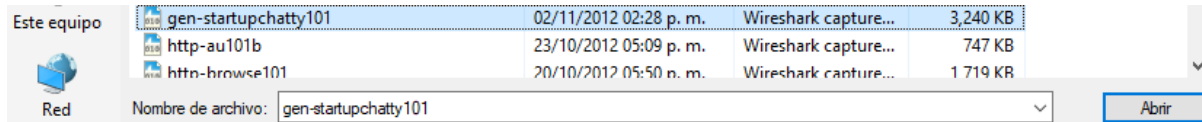
**Maestro:** Ismael Jiménez Sánchez

***Fecha De Entrega: 4/Diciembre/2020***

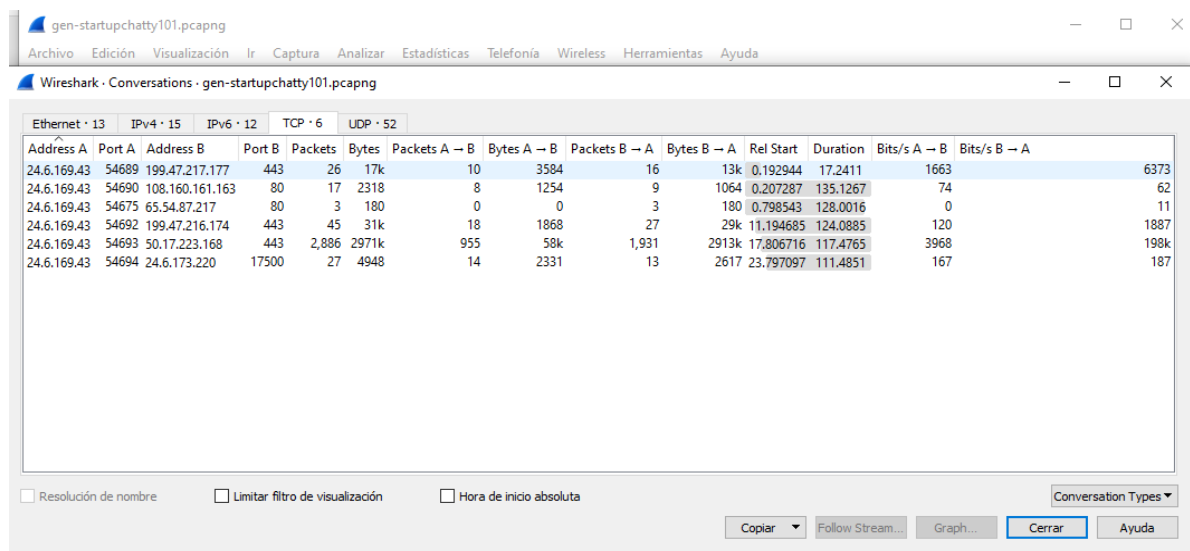
Horario: 5:00 pm – 6:00 pm

## Laboratio N#19 – Deteccion de transferencias de archivos en segundo plano al iniciar.

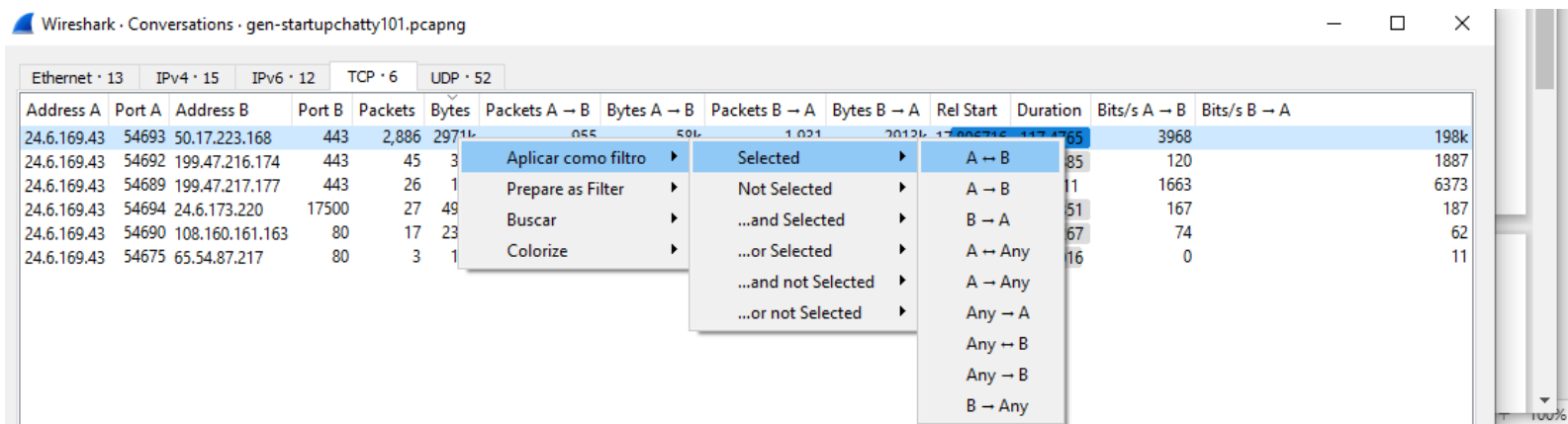
Paso 1 – Abrimos el archivo gen-startupchatty101.pcapng



Paso 2 – Seleccionamos estadísticas | conversaciones | TCP y ordenamos las columnas Bytes de mayor a menor para localizar la Conversación TCP más activa.



Paso 3 – Hacemos clic derecho en la conversación más activa y seleccionamos aplicar como filtro | seleccionado | a <> b. En la barra de estado debe indicar que 2.886 paquetes coinciden con su filtro.



Paso 4 – El frame 311 debe ser el primer paquete en la conversación. Hacemos clic para borrar el filtro y buscamos un proceso de resolución antes del 311.

gen-startupchatty101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ip.addr==24.6.169.43 && tcp.port==54693 && ip.addr==50.17.223.168 && tcp.port==443

No.	Info	Source	Destination	Protocol
311	54693 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1	24.6.169.43	50.17.223.168	TCP
313	443 → 54693 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128	50.17.223.168	24.6.169.43	TCP
314	54693 → 443 [ACK] Seq=1 Ack=1 Win=65700 Len=0	24.6.169.43	50.17.223.168	TCP

Paso 5 – Hacemos clic en borrar para eliminar esos filtros de visualización no deseados.

gen-startupchatty101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplicar un filtro de visualización ... <Ctrl-/>

No.	Info	Source	Destination	Protocol
302	443 → 54692 [ACK] Seq=23047 Ack=801 Win=17920 Len=1460 [TCP segment of a reassembled data segment]	199.47.216.174	24.6.169.43	TCP
303	443 → 54692 [ACK] Seq=24507 Ack=801 Win=17920 Len=1460 [TCP segment of a reassembled data segment]	199.47.216.174	24.6.169.43	TCP
304	54692 → 443 [ACK] Seq=801 Ack=24507 Win=65700 Len=0	24.6.169.43	199.47.216.174	TCP
305	443 → 54692 [ACK] Seq=25967 Ack=801 Win=17920 Len=1460 [TCP segment of a reassembled data segment]	199.47.216.174	24.6.169.43	TCP
306	Application Data	199.47.216.174	24.6.169.43	TLSv1
307	54692 → 443 [ACK] Seq=801 Ack=27741 Win=65700 Len=0	24.6.169.43	199.47.216.174	TCP
308	GET /en-us/...&... HTTP/1.1	24.6.169.43	199.169.161.163	HTTP

> Frame 311: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0

> Ethernet II, Src: ASUSTekC\_19:9e:19 (c8:60:00:19:9e:19), Dst: Cadant\_31:bb:c1 (00:01:5c:31:bb:c1)

> Internet Protocol Version 4, Src: 24.6.169.43, Dst: 50.17.223.168

> Transmission Control Protocol, Src Port: 54693, Dst Port: 443, Seq: 0, Len: 0

0000 00 01 5c 31 bb c1 c8 60 00 19 9e 19 08 00 45 00 ..1...E

0010 00 34 01 ff 40 00 00 06 25 da 18 06 a9 2b 32 11 4...%+2

0020 df a8 d5 a5 01 bb 4a 40 19 a2 00 00 00 00 00 02 .....j.....

0030 20 00 40 e8 00 00 02 04 05 b4 01 03 03 02 01 01 ..@.....

0040 04 02 ..

gen-startupchatty101.pcapng Paquetes: 3290 - Mostrado: 3290 (100.0%) Perfil: wireshark101