

Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

**Lab19 - Detect Background File
Transfers on Startup**

Docente: Ing. Ismael Jiménez Sánchez

Alumno: Uc Uc César Enrique

Lab19 - Detect Background File Transfers on Startup

1 Abrimos el archivo gen-startupchatty101.pcapng

2 Seleccionamos estadísticas>conversaciones>TCP>Bytes

gen-startupchatty101.pcapng

ArchivoEdiciónVisualizaciónIrCapturaAnalizarEstadísticasFoníaWirelessHerramientasAyuda

3 En Bytes le damos click derecho seleccionamos Apply as Filter>Select>AB

Lab19.pdf - Adobe Acrobat Reader DC

ArchivoEdiciónVerFirmarVentanaAyuda

InicioHerramientasLab19.pdf

?

Inicio sesión

Wireshark - Conversations - gen-startupchatty101.pcapng

Ethernet · 13IPv4 · 15IPv6 · 12TCP · 6UDP · 52

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
24.6.169.43	54693	50.17.223.168	443	2,886	2971k	955	58k	1,931	2913k	17.806716	117.4765	3968	198k
24.6.169.43	54692	199.47.216.174	443	45	31k	18	1868	27	29k	11.194685	124.0885	120	1887
24.6.169.43	54689	199.47.217.177	443	26	17k	10	3584	16	13k	0.192944	17.2411	1663	6373
24.6.169.43	54694	24.6.173.220	17500	27	4948	14	2331	13	2617	23.797097	111.4851	167	187
24.6.169.43	54690	108.160.161.163	80	17	2318	8	1254	9	1064	0.207287	135.1267	74	62
24.6.169.43	54675	65.54.87.217	80	3	180	0	0	3	180	0.798543	128.0016	0	11

Aplicar como filtro

Prepare as Filter

Buscar

Colorize

Selected

Not Selected

...and Selected

...or Selected

...and not Selected

...or not Selected

A → B

A → B

B → A

A → Any

A → Any

Any → A

Any → B

B → Any

☐ Resolución de nombre☐ Limitar filtro de visualización☐ Hora de inicio absoluta

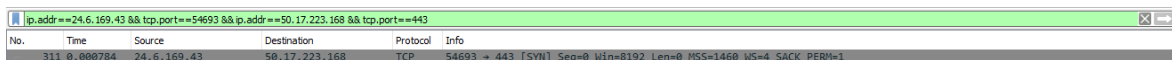
Conversation Types ▼

CopiarFollow Stream...Graph...CerrarAyuda

Deberá mostrar 2886 paquetes

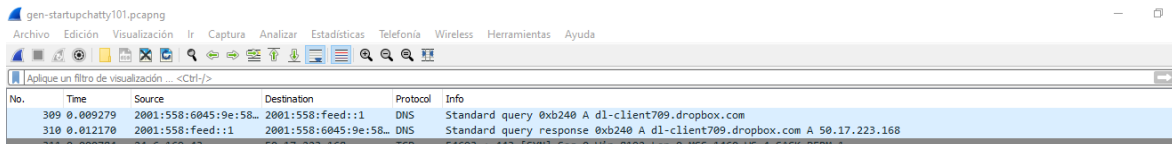
Paquetes: 3290 · Mostrado: 2886 (87.7%)

4. El primer paquete que aparece es el 311



No.	Time	Source	Destination	Protocol	Info
311	0.000784	24.6.169.43	50.17.223.168	TCP	54693 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

Quitamos el filtro y podemos observar que en los paquetes 309 y 310 aparece un server de Dropbox. El cliente pudo haber checado y descargado desde un folder de Dropbox



No.	Time	Source	Destination	Protocol	Info
309	0.009279	2001:558:6045:9e:58...	2001:558:feed::1	DNS	Standard query 0xb240 A dl-client709.dropbox.com
310	0.012170	2001:558:feed::1	2001:558:6045:9e:58...	DNS	Standard query response 0xb240 A dl-client709.dropbox.com A 50.17.223.168
311	0.000784	24.6.169.43	50.17.223.168	TCP	54693 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1