

**Instituto Tecnológico de Cancún**

**Fundamentos de Telecomunicaciones**

**Lab31 - Filter on the Most Active  
TCP Conversation**

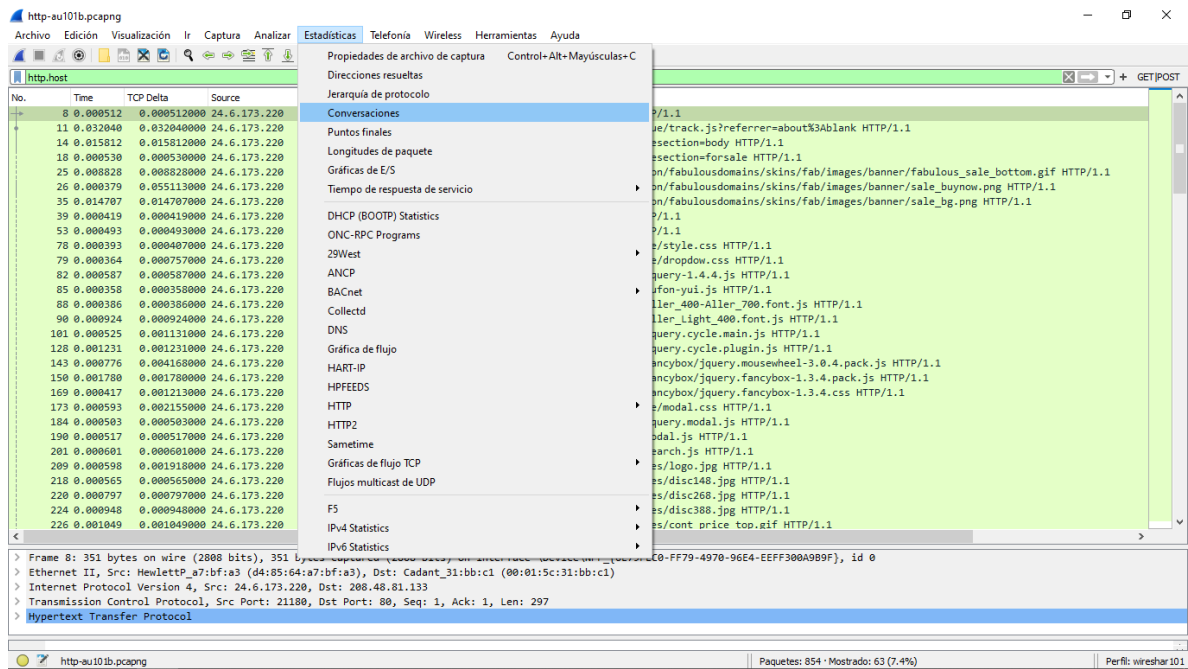
**Prof. Ismael Jiménez Sánchez**

**Alumno(a). Laury del Rosario Mex  
Martin**

**Ciclo 2020-B**

En este lab se mostrara otra forma de aplicar filtros de display.

## Seleccionamos Estadísticas| Conversaciones



The screenshot shows the Wireshark interface with the 'Estadísticas' (Statistics) pane open. The 'Conversaciones' (Conversations) tab is selected, displaying a list of network flows. The left pane shows a list of flows with columns for No., Time, TCP Delta, and Source. The right pane shows the details of the selected flow, including HTTP headers and body content.

Frame 8: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface 0, 1 packet from 24.6.173.220 to 208.48.81.133

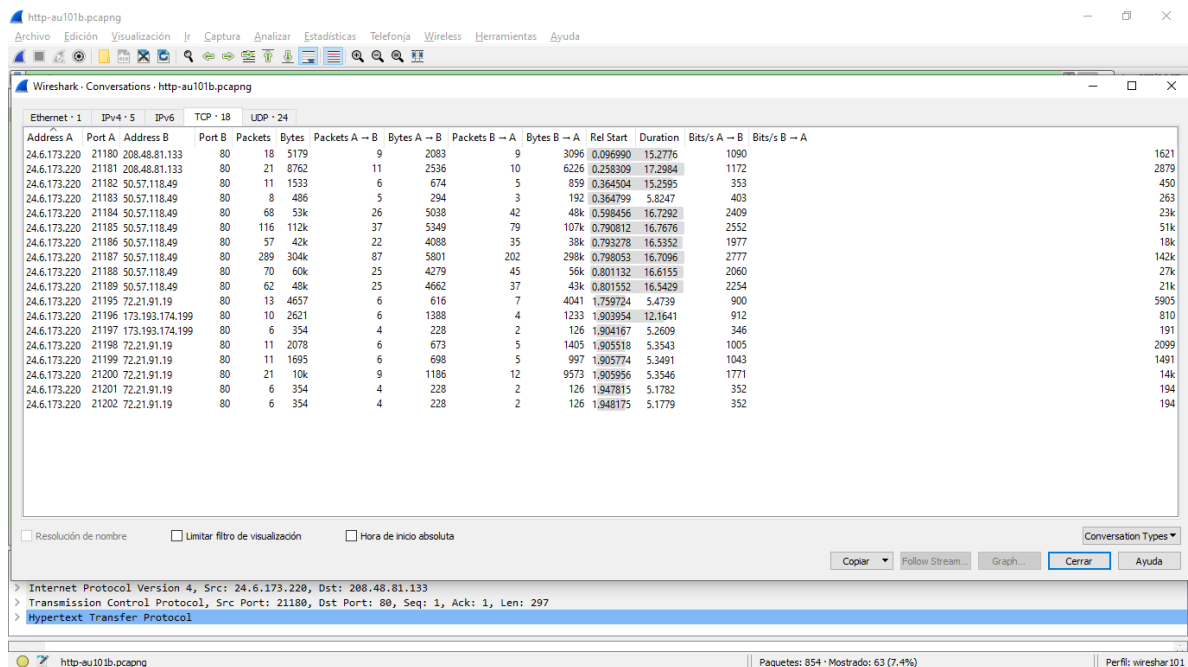
Ethernet II, Src: HewlettP\_87:bfa3 (d4:85:64:a7:bfa3), Dst: Cadant\_31:bb:c1 (00:01:5c:31:bb:c1)

Internet Protocol Version 4, Src: 24.6.173.220, Dst: 208.48.81.133

Transmission Control Protocol, Src Port: 21180, Dst Port: 80, Seq: 1, Ack: 1, Len: 297

Hypertext Transfer Protocol

Y nos saldrá una ventana



The screenshot shows the Wireshark interface with the 'Conversations' pane open. The 'Conversations' tab is selected, displaying a list of network flows. The left pane shows a list of flows with columns for Address A, Port A, Address B, Port B, Packets, Bytes, and Rel Start. The right pane shows the details of the selected flow, including HTTP headers and body content.

Internet Protocol Version 4, Src: 24.6.173.220, Dst: 208.48.81.133

Transmission Control Protocol, Src Port: 21180, Dst Port: 80, Seq: 1, Ack: 1, Len: 297

Hypertext Transfer Protocol

En la pestaña IPv4 solo vemos 2 conversaciones y vemos una conversación muy activa que es la 24.6.181.160 con la 107.6.133.250

Wireshark - Conversations - http-misctraffic101.pcapng

Ethernet - 1IPv4 - 2IPv6TCP - 7UDP

Address A	Address 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
24.6.181.160	208.118.237.137	207	177k	71	9483	136	168k	0.000000	1.3153	57k	1024k
24.6.181.160	107.6.133.250	475	533k	126	8261	349	525k	5.720527	1.9523	33k	2153k

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

CopiarFollow StreamGraphCerrarAyuda

Conversation Types

En la pestaña TCP ordenaremos la columna de bytes y seleccionamos la conversación

Wireshark - Conversations - http-misctraffic101.pcapng

Ethernet · 1IPv4 · 2IPv6TCP · 7UDP

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
24.6.181.160	1266	107.6.133.250	80	475	533k	126	8261	349	525k	5.720527	1.9523	33k	
24.6.181.160	1260	208.118.237.137	80	127	133k	37	3086	90	130k	0.000000	1.3153	18k	
24.6.181.160	1264	208.118.237.137	80	40	36k	14	1705	26	34k	0.294237	0.7301	18k	
24.6.181.160	1261	208.118.237.137	80	10	2141	5	1174	5	967	0.000756	0.3405	27k	
24.6.181.160	1263	208.118.237.137	80	10	2012	5	1175	5	837	0.172622	0.3237	29k	
24.6.181.160	1262	208.118.237.137	80	10	2011	5	1174	5	837	0.067684	0.3449	27k	
24.6.181.160	1265	208.118.237.137	80	10	1821	5	1169	5	652	0.348607	0.3110	30k	

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

CopiarFollow Stream...Graph...CerrarAyuda

Wireshark - Conversations - http-misctraffic101

Damos clic derecho apply as filter| selected | A ↔ B

Wireshark · Conversations · http-misctraffic101.pcapng

Ethernet · 1IPv4 · 2IPv6TCP · 7UDP

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
24.6.181.160	1266	107.6.133.250	80	475	533k	126	8261	349	525k	5.720527	1.9523	33k	
24.6.181.160	1260	208.118.237.137	80	127	133k	37	3086	90	130k	0.000000	1.3153	18k	
24.6.181.160	1264	208.118.237.137	80	40	36k	14	1705	26	34k	0.294237	0.7301	18k	
24.6.181.160	1261	208.118.237.137	80	10	2141	5	1174	5	967	0.000756	0.3405	27k	
24.6.181.160	1263	208.118.237.137	80	10	2012	5	1175	5	837	0.172622	0.3237	29k	
24.6.181.160	1262	208.118.237.137	80	10	2011	5	1174	5	837	0.067684	0.3449	27k	
24.6.181.160	1265	208.118.237.137	80	10	1821	5	1169	5	652	0.348607	0.3110	30k	

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

Any → B

B → Any

<div>

>

☐ Resolución de nombre

☐ Limitar filtro de visualización

☐ Hora de inicio absoluta

Conversation Types ▼

Copiar ▼

Follow Stream...

Graph...

Cerrar

Ayuda

Cerramos la ventana y ya estará aplicado el filtro.

http-misctraffic101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

`p.addr==24.6.181.160 && tcp.port==1266 && p.addr==107.6.133.250 && tcp.port==80` GET/POST

No.	Time	TCP Delta	Source	Destination	Protocol	Host	Info
200	4.495202	0.000000000	24.6.181.160	107.6.133.250	TCP		1266 → 80 [SYN] Seq=0 Win=6192 Len=0 MSS=1460 WS=4 SACK_PERM=1
209	0.003000	0.002000000	107.6.133.250	24.6.181.160	TCP		80 → 1266 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=128
210	0.000755	0.000755000	24.6.181.160	107.6.133.250	TCP		1266 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
211	0.014505	0.014505000	24.6.181.160	107.6.133.250	HTTP	downloads.metasploit.c...	GET /data/releases/metasploit-latest-windows-installer.exe HTTP/1.1
212	0.004223	0.004223000	107.6.133.250	24.6.181.160	TCP		80 → 1266 [ACK] Seq=1 Ack=702 Win=7296 Len=0
213	0.001248	0.001248000	107.6.133.250	24.6.181.160	HTTP		HTTP/1.1 200 OK (application/x-msdos-program)
214	0.000799	0.000799000	107.6.133.250	24.6.181.160	HTTP		Continuation
215	0.001509	0.001509000	107.6.133.250	24.6.181.160	HTTP		Continuation
216	0.000004	0.000004000	24.6.181.160	107.6.133.250	TCP		1266 → 80 [ACK] Seq=702 Ack=4381 Win=65700 Len=0
217	0.001719	0.001719000	107.6.133.250	24.6.181.160	HTTP		Continuation
218	0.000003	0.000003000	107.6.133.250	24.6.181.160	HTTP		Continuation
219	0.000003	0.000003000	107.6.133.250	24.6.181.160	HTTP		Continuation
220	0.000700	0.000700000	107.6.133.250	24.6.181.160	HTTP		Continuation
221	0.004715	0.004715000	24.6.181.160	107.6.133.250	TCP		1266 → 80 [ACK] Seq=702 Ack=10221 Win=65700 Len=0
222	0.002874	0.002874000	107.6.133.250	24.6.181.160	HTTP		Continuation
223	0.000775	0.000775000	107.6.133.250	24.6.181.160	HTTP		Continuation
224	0.000003	0.000003000	107.6.133.250	24.6.181.160	HTTP		Continuation
225	0.000792	0.000792000	107.6.133.250	24.6.181.160	HTTP		Continuation
226	0.000005	0.000005000	107.6.133.250	24.6.181.160	HTTP		Continuation
227	0.003568	0.003568000	24.6.181.160	107.6.133.250	TCP		1266 → 80 [ACK] Seq=702 Ack=17521 Win=65700 Len=0
228	0.003496	0.003496000	107.6.133.250	24.6.181.160	HTTP		Continuation
229	0.000807	0.000807000	107.6.133.250	24.6.181.160	HTTP		Continuation
230	0.000012	0.000012000	107.6.133.250	24.6.181.160	HTTP		Continuation
231	0.000792	0.000792000	24.6.181.160	107.6.133.250	TCP		1266 → 80 [ACK] Seq=702 Ack=20441 Win=64240 Len=0
232	0.000003	0.000003000	107.6.133.250	24.6.181.160	HTTP		Continuation
233	0.001659	0.001659000	107.6.133.250	24.6.181.160	HTTP		Continuation
234	0.000005	0.000005000	24.6.181.160	107.6.133.250	TCP		1266 → 80 [ACK] Seq=702 Ack=23361 Win=61320 Len=0
235	0.000001	0.000001000	107.6.133.250	24.6.181.160	HTTP		Continuation
236	0.000897	0.000897000	24.6.181.160	107.6.133.250	TCP		1266 → 80 [ACK] Seq=702 Ack=26281 Win=58400 Len=0

< Frame 200: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface unknown, id 0  
> Ethernet II, Src: Flextron\_40:d6:91 (00:21:cc:40:d6:91), Dst: Cadant\_31:bb:c1 (00:01:5c:31:bb:c1)  
> Internet Protocol Version 4, Src: 24.6.181.160, Dst: 107.6.133.250  
> Transmission Control Protocol, Src Port: 1266, Dst Port: 80, Seq: 0, Len: 0

http-misctraffic101.pcapng Paquetes: 682 · Mostrado: 475 (69.6%) Perfil: wireshark101