

Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

**Lab25 - Add a Column to Display
Coloring Rules in Use**

Docente: Ing. Ismael Jiménez Sánchez

Alumno: Uc Uc César Enrique

Lab25 - Add a Column to Display Coloring Rules in Use

1 Abrimos el archivo http-sfgate101.pcapng

2. Buscamos el paquete 475 y podemos observar que son 3 colores diferentes.

http-sfgate101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

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

No.	Time	Source	Destination	Protocol	Info
470	0.015007	66.109.241.50	24.6.173.220	TCP	80 → 10623 [ACK] Seq=6901 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
471	0.000928	66.109.241.50	24.6.173.220	TCP	80 → 10623 [ACK] Seq=8281 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
472	0.000004	66.109.241.50	24.6.173.220	TCP	80 → 10623 [ACK] Seq=9661 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
473	0.000176	24.6.173.220	66.109.241.50	TCP	10623 → 80 [ACK] Seq=316 Ack=11041 Win=66240 Len=0
474	0.000778	66.109.241.50	24.6.173.220	TCP	80 → 10623 [ACK] Seq=11041 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
475	0.008319	66.109.241.50	24.6.173.220	TCP	[TCP Dup ACK 410#1] 80 → 10623 [ACK] Seq=12421 Ack=316 Win=65220 Len=0
476	0.027249	24.6.173.220	75.75.75.75	DNS	Standard query 0x7394 A partner.googleadservices.com
477	0.008586	24.6.173.220	107.22.233.219	TCP	10635 → 80 [ACK] Seq=380 Ack=308 Win=65392 Len=0
478	0.004329	75.75.75.75	24.6.173.220	DNS	Standard query response 0x7394 A partner.googleadservices.com CNAME partnerad.l.doubleclick.net A 74.125.224.45 A 74...
479	0.000774	24.6.173.220	75.75.75.75	DNS	Standard query 0x6d20 AAAA partner.googleadservices.com
480	0.013337	75.75.75.75	24.6.173.220	DNS	Standard query response 0x6d20 AAAA partner.googleadservices.com CNAME partnerad.l.doubleclick.net SOA ns1.google.com
481	0.038338	66.109.241.50	24.6.173.220	TCP	80 → 10623 [ACK] Seq=12421 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
482	0.002347	24.6.173.220	66.109.241.50	TCP	10623 → 80 [ACK] Seq=316 Ack=13801 Win=66240 Len=0
483	0.000792	66.109.241.50	24.6.173.220	TCP	80 → 10623 [ACK] Seq=13801 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
484	0.000004	66.109.241.50	24.6.173.220	TCP	80 → 10623 [ACK] Seq=15181 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]

> Frame 472: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface \Device\NPF_{6E79FEC0-F779-4970-96E4-EEFF300A989F}, id 0

> Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)

> Internet Protocol Version 4, Src: 66.109.241.50, Dst: 24.6.173.220

> Transmission Control Protocol, Src Port: 80, Dst Port: 10623, Seq: 9661, Ack: 316, Len: 1380

3 y 4. En el mismo paquete 475 expandimos el HTTP y encontramos Coloring Rule: Name lo aplicamos como columna

http-sfgate101.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

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

No.	Time	Source	Destination	Protocol	Coloring Rule Name	Info
470	0.015007	66.109.241.50	24.6.173.220	TCP	HTTP	80 → 10623 [ACK] Seq=6901 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
471	0.000928	66.109.241.50	24.6.173.220	TCP	HTTP	80 → 10623 [ACK] Seq=8281 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
472	0.000004	66.109.241.50	24.6.173.220	TCP	HTTP	80 → 10623 [ACK] Seq=9661 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
473	0.000176	24.6.173.220	66.109.241.50	TCP	HTTP	10623 → 80 [ACK] Seq=316 Ack=11041 Win=66240 Len=0
474	0.000778	66.109.241.50	24.6.173.220	TCP	HTTP	80 → 10623 [ACK] Seq=11041 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
475	0.008319	66.109.241.50	24.6.173.220	TCP	Bad TCP	[TCP Dup ACK 410#1] 80 → 10623 [ACK] Seq=12421 Ack=316 Win=65220 Len=0
476	0.027249	24.6.173.220	75.75.75.75	DNS	UDP	Standard query 0x7394 A partner.googleadservices.com
477	0.008586	24.6.173.220	107.22.233.219	TCP	HTTP	10635 → 80 [ACK] Seq=380 Ack=308 Win=65392 Len=0
478	0.004329	75.75.75.75	24.6.173.220	DNS	UDP	Standard query response 0x7394 A partner.googleadservices.com CNAME partnerad.l.doubleclick.net A 74.125.224.45 A 74...
479	0.000774	24.6.173.220	75.75.75.75	DNS	UDP	Standard query 0x6d20 AAAA partner.googleadservices.com
480	0.013337	75.75.75.75	24.6.173.220	DNS	UDP	Standard query response 0x6d20 AAAA partner.googleadservices.com CNAME partnerad.l.doubleclick.net SOA ns1.google.com
481	0.038338	66.109.241.50	24.6.173.220	TCP	HTTP	80 → 10623 [ACK] Seq=12421 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
482	0.002347	24.6.173.220	66.109.241.50	TCP	HTTP	10623 → 80 [ACK] Seq=316 Ack=13801 Win=66240 Len=0
483	0.000792	66.109.241.50	24.6.173.220	TCP	HTTP	80 → 10623 [ACK] Seq=13801 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]
484	0.000004	66.109.241.50	24.6.173.220	TCP	HTTP	80 → 10623 [ACK] Seq=15181 Ack=316 Win=65220 Len=1380 [TCP segment of a reassembled PDU]

[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp]
[Coloring Rule Name: Bad TCP]
[Coloring Rule String: tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack]
> Ethernet II, Src: Cadant_31:bb:c1 (00:01:5c:31:bb:c1), Dst: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3)
> Internet Protocol Version 4, Src: 66.109.241.50, Dst: 24.6.173.220