



**TECNOLÓGICO
NACIONAL DE MÉXICO**



INSTITUTO TECNOLÓGICO DE CANCÚN

SISTEMAS COMPUTACIONALES

MATERIA: Fundamentos de Telecomunicaciones

PROFESOR: ING. ISMAEL JIMÉNEZ SÁNCHEZ

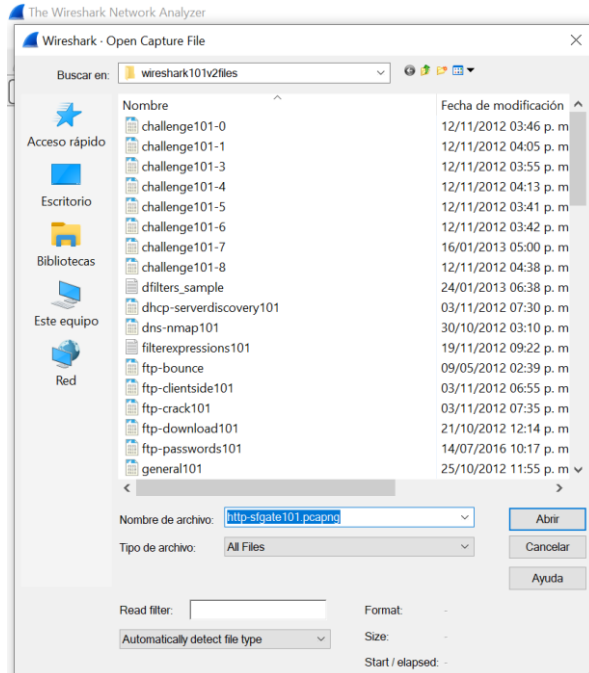
LABORATORIO: 25

Alumno:

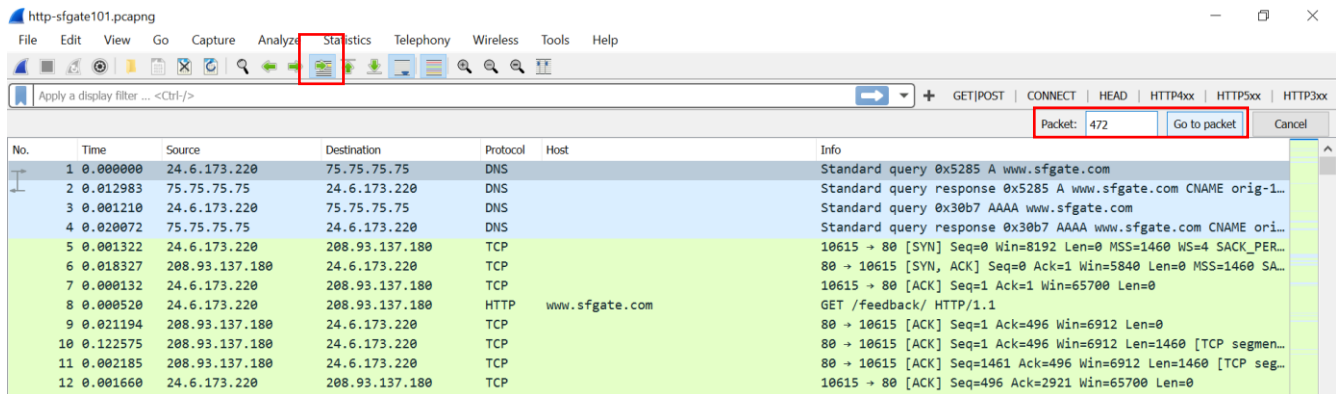
SARRAGOT PASTRANA WILIAM ADRIEN

LAB 25: ADD A COLUMN TO DISPLAY COLORING RULES IN USE

Abriremos el archivo ***http-sfgate101.pcapng***



En la flechita que se encuentra en la parte superior daremos click y buscaremos el paquete 472



Dentro de la sección 472 buscaremos coloring rule name, daremos clic derecho y lo aplicaremos como columna

The screenshot shows the Wireshark interface with packet 472 selected. A right-click context menu is open over the packet list, with 'Apply as Column' highlighted. The packet details pane shows the HTTP layer selected. The packet list shows the following data:

No.	Time	Source	Destination	Protocol	Host
458	0.003027	24.6.173.2	208.93.137.180	HTTP	aps.hearstnp.com
459	0.000366	24.6.173.220	75.75.75.75	DNS	
460	0.015504	75.75.75.75	24.6.173.220	DNS	
461	0.001408	24.6.173.220	75.75.75.75	DNS	
462	0.002884	208.93.137.180	24.6.173.220	TCP	
463	0.000806	208.93.137.180	24.6.173.220	HTTP	
464	0.001715	184.73.197.77	24.6.173.220	TCP	
465	0.001730	184.73.197.77	24.6.173.220	HTTP	
466	0.000904	24.6.173.220	184.73.197.77	TCP	
467	0.005980	24.6.173.220	208.93.137.180	TCP	
468	0.001222	75.75.75.75	24.6.173.220	DNS	
469	0.018754	24.6.173.220	66.109.241.50	TCP	
470	0.015007	66.109.241.50	24.6.173.220	TCP	
471	0.000928	66.109.241.50	24.6.173.220	TCP	
472	0.000004	66.109.241.50	24.6.173.220	TCP	
473	0.000176	24.6.173.220	66.109.241.50	TCP	

The packet details pane shows the following data:

Frame 472: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0

Interface id: 0 (\Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F})

Encapsulation type: Ethernet (1)

Arrival Time: Nov 2, 2012 10:50:36.731493000 Hora estándar del Este (México)

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1351871436.731493000 seconds

[Time delta from previous captured frame: 0.000004000 seconds]

[Time delta from previous displayed frame: 0.000004000 seconds]

[Time since reference or first frame: 0.696044000 seconds]

Frame Number: 472

Una vez aplicada la columna esta se utilizará cuando se desee enumerar rápidamente la regla de coloración aplicada a cada marco

The screenshot shows the Wireshark interface with packet 472 selected. The 'Coloring Rule Name' column is visible in the packet list, and the packet details pane shows the HTTP layer selected. The packet list shows the following data:

No.	Time	Source	Destination	Protocol	Host	Coloring Rule Name	Info
458	0.003027	24.6.173.220	208.93.137.180	HTTP	aps.hearstnp.com	HTTP	GET /Scripts/initDefineAds.js HTTP/1.1
459	0.000366	24.6.173.220	75.75.75.75	DNS		UDP	Standard query 0xb657 A www.googletagservices.
460	0.015504	75.75.75.75	24.6.173.220	DNS		UDP	Standard query response 0xb657 A www.googletag
461	0.001408	24.6.173.220	75.75.75.75	DNS		UDP	Standard query 0xbb69 AAAA www.googletagservic
462	0.002884	208.93.137.180	24.6.173.220	TCP		HTTP	80 → 10625 [ACK] Seq=7112 Ack=1190 Win=10240 L
463	0.000806	208.93.137.180	24.6.173.220	HTTP		HTTP	HTTP/1.1 200 OK (application/x-javascript)
464	0.001715	184.73.197.77	24.6.173.220	TCP		HTTP	80 → 10642 [ACK] Seq=4381 Ack=308 Win=6912 Len
465	0.001730	184.73.197.77	24.6.173.220	HTTP		HTTP	HTTP/1.1 200 OK (text/javascript)
466	0.000904	24.6.173.220	184.73.197.77	TCP		HTTP	10642 → 80 [ACK] Seq=308 Ack=6271 Win=65700 Le
467	0.005980	24.6.173.220	208.93.137.180	TCP		HTTP	10618 → 80 [ACK] Seq=1275 Ack=40046 Win=65700 L
468	0.001222	75.75.75.75	24.6.173.220	DNS		UDP	Standard query response 0xbb69 AAAA www.google
469	0.018754	24.6.173.220	66.109.241.50	TCP		HTTP	10622 → 80 [ACK] Seq=320 Ack=450 Win=65788 Len
470	0.015007	66.109.241.50	24.6.173.220	TCP		HTTP	80 → 10623 [ACK] Seq=6901 Ack=316 Win=65220 Le
471	0.000928	66.109.241.50	24.6.173.220	TCP		HTTP	80 → 10623 [ACK] Seq=8281 Ack=316 Win=65220 Le
472	0.000004	66.109.241.50	24.6.173.220	TCP		HTTP	80 → 10623 [ACK] Seq=9661 Ack=316 Win=65220 Le
473	0.000176	24.6.173.220	66.109.241.50	TCP		HTTP	10623 → 80 [ACK] Seq=316 Ack=11041 Win=66240 L

The packet details pane shows the following data:

Frame 472: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F}, id 0

Interface id: 0 (\Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF300A9B9F})

Encapsulation type: Ethernet (1)

Arrival Time: Nov 2, 2012 10:50:36.731493000 Hora estándar del Este (México)

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1351871436.731493000 seconds

[Time delta from previous captured frame: 0.000004000 seconds]

[Time delta from previous displayed frame: 0.000004000 seconds]

[Time since reference or first frame: 0.696044000 seconds]

Frame Number: 472

Para desactivar esta columna haremos clic derecho en el encabezado de la columna y desmarcar la opción coloring rule name

