

Instituto Tecnológico de Cancún

Fundamentos de Telecomunicaciones

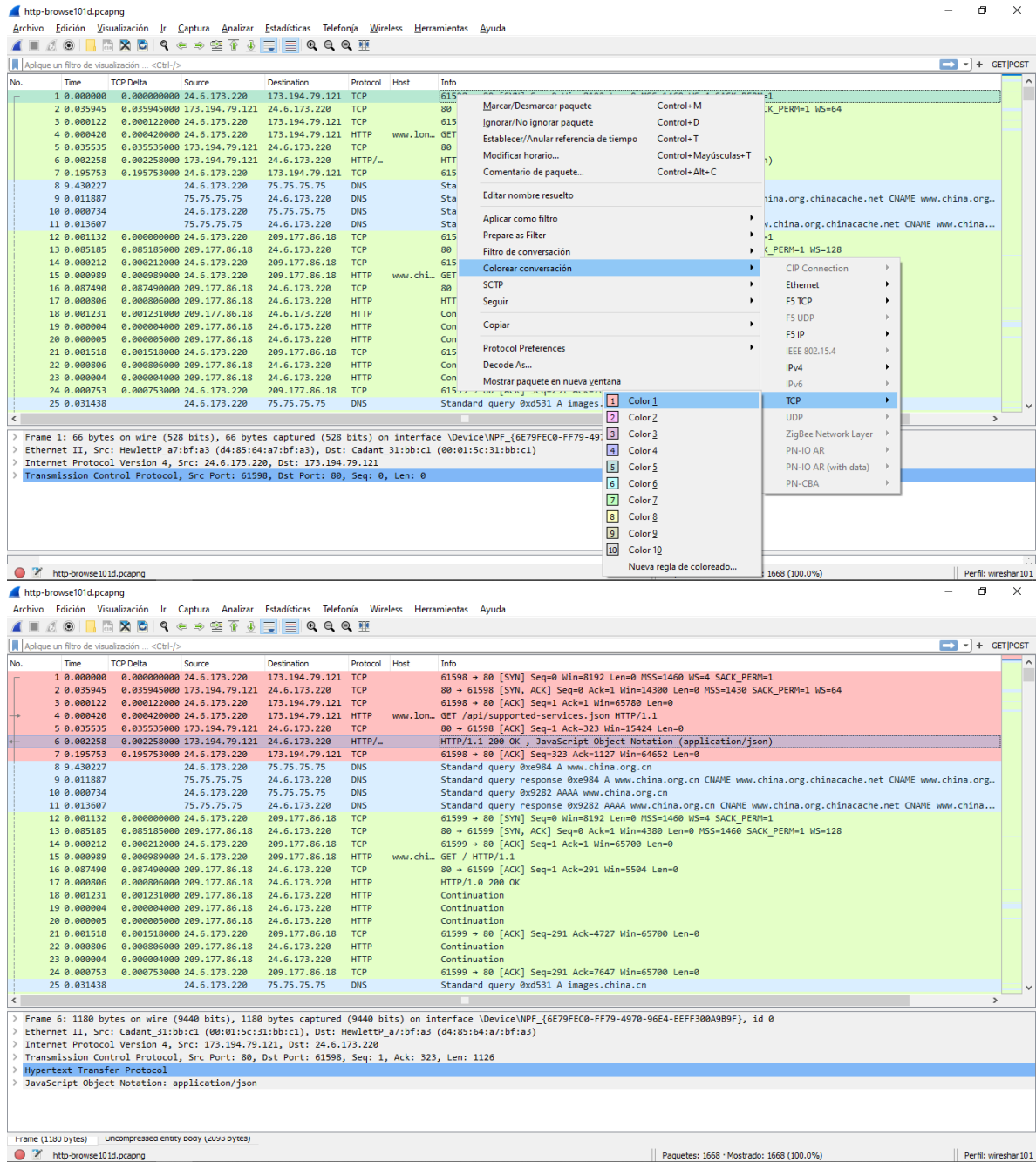
**Lab27 - Create Temporary
Conversation Coloring Rules**

Prof. Ismael Jiménez Sánchez

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

Ciclo 2020-B

En el frame 1 es un TCP handshake packet (SYN) lo vamos a seleccionar y aplicaremos un color de conversación que será el color 1



The image shows the Wireshark network protocol analyzer interface. The top menu bar includes Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Telefonía, Wireless, Herramientas, and Ayuda. The toolbar contains various icons for file operations, search, and analysis. The main window is divided into three panes: Packet List, Packet Details, and Packet Bytes.

Packet List: Shows a list of captured packets. The first packet (No. 1) is selected, which is a TCP SYN packet from 24.6.173.220 to 173.194.79.121. The packet is highlighted in green.

Packet Details: Shows the structure of the selected packet. It includes Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (SYN). The packet length is 66 bytes.

Color Conversation: A context menu is open over the first packet, showing a list of color conversations. 'Color 1' is selected, which is the color assigned to the SYN packet.

Packet Bytes: Shows the raw data of the selected packet in hexadecimal and ASCII format.

Vamos al frame 12 que es el siguiente SYN y le aplicaremos el color 4.

The image shows a Wireshark packet capture of 'http-browse101d.pcapng'. The packet list on the left shows frame 12 selected, which is a TCP SYN packet from 209.177.86.18 to 24.6.173.220. The packet details pane on the right shows the frame structure: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw data. The packet list table is as follows:

No.	Time	TCP Delta	Source	Destination	Protocol	Host	Info
1	0.000000	0.000000000	24.6.173.220	173.194.79.121	TCP		61598 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.035945	0.035945000	173.194.79.121	24.6.173.220	TCP		80 → 61598 [SYN, ACK] Seq=0 Ack=1 Win=14300 Len=0 MSS=1430 SACK_PERM=1 WS=64
3	0.000122	0.000122000	24.6.173.220	173.194.79.121	TCP		61598 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
4	0.000420	0.000420000	24.6.173.220	173.194.79.121	HTTP	www.lon.	GET /api/supported-services.json HTTP/1.1
5	0.035535	0.035535000	173.194.79.121	24.6.173.220	TCP		80 → 61598 [ACK] Seq=1 Ack=323 Win=15424 Len=0
6	0.002258	0.002258000	173.194.79.121	24.6.173.220	HTTP	...	HTTP/1.1 200 OK , JavaScript Object Notation (application/json)
7	0.195753	0.195753000	24.6.173.220	173.194.79.121	TCP		61598 → 80 [ACK] Seq=323 Ack=1127 Win=64652 Len=0
8	9.430227		24.6.173.220	75.75.75.75	DNS		Standard query 0xe984 A www.china.org.cn
9	0.011887		75.75.75.75	24.6.173.220	DNS		Standard query response 0xe984 A www.china.org.cn CNAME www.china.org.chinacache.net CNAME www.china.org...
10	0.000734		24.6.173.220	75.75.75.75	DNS		Standard query 0x9282 AAAA www.china.org.cn
11	0.013607		75.75.75.75	24.6.173.220	DNS		Standard query response 0x9282 AAAA www.china.org.cn CNAME www.china.org.chinacache.net CNAME www.china...
12	0.001132	0.000000000	24.6.173.220	209.177.86.18	TCP		61599 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
13	0.005105	0.005105000	209.177.86.18	24.6.173.220	TCP		80 → 61599 [SYN, ACK] Seq=0 Ack=1 Win=4300 Len=0 MSS=1460 SACK_PERM=1 WS=128
14	0.000212	0.000212000	24.6.173.220	209.177.86.18	TCP		61599 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
15	0.000989	0.000989000	24.6.173.220	209.177.86.18	HTTP	www.chi.	GET / HTTP/1.1
16	0.007490	0.007490000	209.177.86.18	24.6.173.220	TCP		80 → 61599 [ACK] Seq=1 Ack=291 Win=5504 Len=0
17	0.000006	0.000006000	209.177.86.18	24.6.173.220	HTTP		HTTP/1.0 200 OK
18	0.001231	0.001231000	209.177.86.18	24.6.173.220	HTTP		Continuation
19	0.000004	0.000004000	209.177.86.18	24.6.173.220	HTTP		Continuation
20	0.000005	0.000005000	209.177.86.18	24.6.173.220	HTTP		Continuation
21	0.001518	0.001518000	24.6.173.220	209.177.86.18	TCP		61599 → 80 [ACK] Seq=291 Ack=4727 Win=65700 Len=0
22	0.000806	0.000806000	209.177.86.18	24.6.173.220	HTTP		Continuation
23	0.000004	0.000004000	209.177.86.18	24.6.173.220	HTTP		Continuation
24	0.000753	0.000753000	24.6.173.220	209.177.86.18	TCP		61599 → 80 [ACK] Seq=291 Ack=7647 Win=65700 Len=0
25	0.031438		24.6.173.220	75.75.75.75	DNS		Standard query 0xd531 A images.china.cn

Y el ultimo en el frame 61 que es el ultimo SYN y le aplicamos el color 8

The image shows a Wireshark packet capture of 'http-browse101d.pcapng'. The packet list on the left shows frame 61 selected, which is a TCP SYN packet from 210.72.21.11 to 24.6.173.220. The packet details pane on the right shows the frame structure: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw data. The packet list table is as follows:

No.	Time	TCP Delta	Source	Destination	Protocol	Host	Info
44	0.000006	0.000006000	209.177.86.18	24.6.173.220	HTTP		Continuation
45	0.000007	0.000007000	209.177.86.18	24.6.173.220	HTTP		Continuation
46	0.001212	0.001212000	24.6.173.220	209.177.86.18	TCP		61599 → 80 [ACK] Seq=291 Ack=31007 Win=65700 Len=0
47	0.001896		24.6.173.220	75.75.75.75	DNS		Standard query 0x56c9 A pagead2.googleadsyndication.com
48	0.014451		75.75.75.75	24.6.173.220	DNS		Standard query response 0x56c9 A pagead2.googleadsyndication.com CNAME pagead46.1.doubleclick.net A 74.125...
49	0.001656		24.6.173.220	75.75.75.75	DNS		Standard query 0x5155 AAAA pagead2.googleadsyndication.com
50	0.012504		75.75.75.75	24.6.173.220	DNS		Standard query response 0x5155 AAAA pagead2.googleadsyndication.com CNAME pagead46.1.doubleclick.net AAAA ...
51	0.048502	0.079000000	209.177.86.18	24.6.173.220	HTTP		Continuation
52	0.001157	0.001157000	209.177.86.18	24.6.173.220	HTTP		Continuation
53	0.000007	0.000007000	209.177.86.18	24.6.173.220	HTTP		Continuation
54	0.000006	0.000006000	209.177.86.18	24.6.173.220	HTTP		Continuation
55	0.001146	0.001146000	24.6.173.220	209.177.86.18	TCP		61599 → 80 [ACK] Seq=291 Ack=36847 Win=65700 Len=0
56	0.000008	0.000008000	209.177.86.18	24.6.173.220	HTTP		Continuation
57	0.000004	0.000004000	209.177.86.18	24.6.173.220	HTTP		Continuation
58	0.000006	0.000006000	209.177.86.18	24.6.173.220	HTTP		Continuation
59	0.000003	0.000003000	209.177.86.18	24.6.173.220	HTTP		Continuation
60	0.001921	0.001921000	24.6.173.220	209.177.86.18	TCP		61599 → 80 [ACK] Seq=291 Ack=41250 Win=65700 Len=0
61	0.000186	0.000000000	24.6.173.220	210.72.21.11	TCP		61601 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
62	0.253123		24.6.173.220	75.75.75.75	DNS		Standard query 0x6a8e A log.china.cn
63	0.013626		75.75.75.75	24.6.173.220	DNS		Standard query response 0x6a8e A log.china.cn A 210.72.21.11
64	0.001725	0.000000000	24.6.173.220	210.72.21.11	TCP		61602 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
65	0.001844	0.270319000	210.72.21.11	24.6.173.220	TCP		80 → 61601 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=32
66	0.000187	0.000187000	24.6.173.220	210.72.21.11	TCP		61601 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
67	0.000855	0.000855000	24.6.173.220	210.72.21.11	HTTP	log.chi.	GET /log.js HTTP/1.1
68	0.266296	0.269182000	210.72.21.11	24.6.173.220	TCP		80 → 61602 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=32

Y con esto podemos ver el seguimiento de conversacion de cada uno y diferenciarlos por colores

Para quitar los colores vamos en visualizacion| colorear conversacion | restablecer coloreado

http-browse101d.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Barra de herramientas principal
Barra de herramientas de filtro
Barra de estado

Aplicar un filtro de visualización

No. Time

44 0.000 Pantalla completa F11
45 0.000
46 0.001 Listado de paquetes
47 0.001 Detalles de paquete
48 0.014 Bytes de paquete
49 0.001 Packet Diagram
50 0.012
51 0.048
52 0.001 Formato de visualización de hora
53 0.000 Resolución de nombre
54 0.000
55 0.001 Zoom
56 0.000 Expandir subárboles Mayúsculas+Derecha
57 0.000 Contraer subárboles Mayúsculas+Izquierda
58 0.000 Expandir todo Control+Derecha
59 0.000 Contraer todo Control+Izquierda
60 0.001
61 0.006
62 0.252
63 0.013 Colorear listado de paquetes
64 0.001 Reglas de coloreado...
65 0.001 Colorear conversación
66 0.000
67 0.000 Restablecer diseño Control+Mayúsculas+W
68 0.266 Cambiar tamaño de columnas Control+Mayúsculas+R

Internas

Mostrar paquete en nueva ventana
Volver a cargar como formato/captura de archivo Control+Mayúsculas+F
Volver a cargar Control+R

Continuation
Continuation
599 → 80 [ACK] Seq=291 Ack=31007 Win=65700 Len=0
Standard query 0x56c9 A pagead2.google syndication.com
Standard query response 0x56c9 A pagead2.google syndication.com CNAME pagead46.1.doubleclick.net A 74.125...
Standard query 0x5155 AAAA pagead2.google syndication.com
Standard query response 0x5155 AAAA pagead2.google syndication.com CNAME pagead46.1.doubleclick.net AAAA ...
Continuation
Continuation
Continuation
599 → 80 [ACK] Seq=291 Ack=36847 Win=65700 Len=0
Continuation
Continuation
Continuation
599 → 80 [ACK] Seq=291 Ack=41250 Win=65700 Len=0
601 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
Standard query 0x6a8e A log.china.cn
Standard query response 0x6a8e A log.china.cn A 210.72.21.11
602 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
1 Color 1 Control+1
2 Color 2 Control+2
3 Color 3 Control+3
4 Color 4 Control+4
5 Color 5 Control+5
6 Color 6 Control+6
7 Color 7 Control+7
8 Color 8 Control+8
9 Color 9 Control+9
10 Color 10 Control+10
Restablecer coloreado Control+Espacio
Nueva regla de coloreado...

Frame 60: 54
Ethernet II, Src: HewlettP_7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 209.177.86.18
Transmission Control Protocol, Src Port: 61599, Dst Port: 80, Seq: 291, Ack: 41250, Len: 0

Paquetes: 1668 · Mostrado: 1668 (100.0%) Perfi: wireshark 101

http-browse101d.pcapng

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

Aplicar un filtro de visualización <Ctrl+>

No. Time TCP Delta Source Destination Protocol Host Info

44 0.000006 0.000006000 209.177.86.18 24.6.173.220 HTTP Continuation
45 0.000007 0.000007000 209.177.86.18 24.6.173.220 HTTP Continuation
46 0.001212 0.001212000 24.6.173.220 209.177.86.18 TCP 61599 → 80 [ACK] Seq=291 Ack=31007 Win=65700 Len=0
47 0.001896 24.6.173.220 75.75.75.75 DNS Standard query 0x56c9 A pagead2.google syndication.com
48 0.014451 75.75.75.75 24.6.173.220 DNS Standard query response 0x56c9 A pagead2.google syndication.com CNAME pagead46.1.doubleclick.net A 74.125...
49 0.001656 24.6.173.220 75.75.75.75 DNS Standard query 0x5155 AAAA pagead2.google syndication.com
50 0.012504 75.75.75.75 24.6.173.220 DNS Standard query response 0x5155 AAAA pagead2.google syndication.com CNAME pagead46.1.doubleclick.net AAAA ...
51 0.045502 0.079009000 209.177.86.18 24.6.173.220 HTTP Continuation
52 0.001157 0.001157000 209.177.86.18 24.6.173.220 HTTP Continuation
53 0.000007 0.000007000 209.177.86.18 24.6.173.220 HTTP Continuation
54 0.000006 0.000006000 209.177.86.18 24.6.173.220 HTTP Continuation
55 0.001146 0.001146000 24.6.173.220 209.177.86.18 TCP 61599 → 80 [ACK] Seq=291 Ack=36847 Win=65700 Len=0
56 0.000008 0.000008000 209.177.86.18 24.6.173.220 HTTP Continuation
57 0.000004 0.000004000 209.177.86.18 24.6.173.220 HTTP Continuation
58 0.000006 0.000006000 209.177.86.18 24.6.173.220 HTTP Continuation
59 0.000003 0.000003000 209.177.86.18 24.6.173.220 HTTP Continuation
60 0.001921 0.001921000 24.6.173.220 209.177.86.18 TCP 61599 → 80 [ACK] Seq=291 Ack=41250 Win=65700 Len=0
61 0.006106 0.000000000 24.6.173.220 210.72.21.11 TCP 61601 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
62 0.253123 24.6.173.220 75.75.75.75 DNS Standard query 0x6a8e A log.china.cn
63 0.013626 75.75.75.75 24.6.173.220 DNS Standard query response 0x6a8e A log.china.cn A 210.72.21.11
64 0.001726 0.000000000 24.6.173.220 210.72.21.11 TCP 61602 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
65 0.001844 0.270319000 210.72.21.11 24.6.173.220 TCP 80 → 61601 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=32
66 0.000187 0.000187000 24.6.173.220 210.72.21.11 TCP 61601 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
67 0.000855 0.000855000 24.6.173.220 210.72.21.11 HTTP log.chi GET /log.js HTTP/1.1
68 0.266296 0.269182000 210.72.21.11 24.6.173.220 TCP 80 → 61602 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=32

Frame 60: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EFF300A9B9F}, id 0
Ethernet II, Src: HewlettP_7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:31:bb:c1)
Internet Protocol Version 4, Src: 24.6.173.220, Dst: 209.177.86.18
Transmission Control Protocol, Src Port: 61599, Dst Port: 80, Seq: 291, Ack: 41250, Len: 0

Paquetes: 1668 · Mostrado: 1668 (100.0%) Perfi: wireshark 101