

INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

Lab27- Create Temporary Conversation Coloring Rules

Paso 1:

The screenshot shows the Wireshark 'Open Capture File' dialog box. The file list contains various .pcapng files. The file 'http-browse101d.pcapng' is selected, and a tooltip shows its details: 'Tipo: Wireshark capture file', 'Tamaño: 837 KB', and 'Fecha de modificación: 04/11/2012 20:31'. The 'Nombre de archivo' field is set to 'http-browse101d.pcapng' and 'Tipo de archivo' is set to 'All Files'. The 'Read filter' is empty, and the 'Format' is 'Wireshark/... - pcapng'. The 'Size' is '837KB, 1668 data records' and the 'Start / elapsed' time is '2012-11-04 21:28:20 / 00:00:48'. The 'Abrir' button is highlighted.

Below the dialog, the packet capture data is displayed in hexadecimal and ASCII format. The data shows a sequence of bytes, including a null byte (00) and a sequence of bytes (01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00) followed by a sequence of bytes (00 34 1a f2 40 00 80 06 00 00 18 06 ad dc ad c2) and a sequence of bytes (4f 79 f0 9e 00 50 24 6b 15 b2 00 00 00 00 80 02) followed by a sequence of bytes (20 00 c3 44 00 00 02 04 05 b4 01 03 03 02 01 01) and a sequence of bytes (04 02).

The bottom status bar shows 'http-browse101d.pcapng', 'Packets: 1668 · Displayed: 1668 (100.0%)', and 'Profile: wireshark101'.

The screenshot shows the Wireshark network protocol analyzer interface. The main pane displays a list of captured packets. The packet list has columns for No., Time, TCP Delta, Source, Destination, Protocol, and Info. The selected packet is packet 1, which is a TCP SYN packet from 24.6.173.220 to 173.194.79.121. A context menu is open over the packet list, showing options like 'Mark/Unmark Packet', 'Ignore/Unignore Packet', 'Set/Unset Time Reference', 'Time Shift...', 'Packet Comment...', 'Edit Resolved Name', 'Apply as Filter', 'Prepare as Filter', 'Conversation Filter', 'Colorize Conversation', 'SCTP', 'Follow', 'Copy', 'Protocol Preferences', 'Decode As...', and 'Show Packet in New Window'. The 'Colorize Conversation' option is highlighted, and a submenu is open showing a list of coloring rules. The submenu includes 'CIP Connection', 'Ethernet', 'F5 TCP', 'F5 UDP', 'F5 IP', 'IEEE 802.15.4', 'IPv4', 'IPv6', 'TCP', 'UDP', 'ZigBee Network Layer', 'PN-IO AR', 'PN-IO AR (with data)', and 'PN-CBA'. The 'TCP' rule is selected, and a further submenu is open showing a list of colors: 'Color 1' (red), 'Color 2' (orange), 'Color 3' (yellow), 'Color 4' (green), 'Color 5' (light green), 'Color 6' (blue), 'Color 7' (dark blue), 'Color 8' (purple), 'Color 9' (brown), 'Color 10' (pink), and 'New Coloring Rule...'. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane shows the raw data in hexadecimal and ASCII.

Paso 3:

The screenshot shows the Wireshark network protocol analyzer interface. The main pane displays a list of captured packets. The packet list has columns for No., Time, TCP Delta, Source, Destination, Protocol, and Info. The packets are color-coded: red for SYN/ACK, blue for DNS, and green for HTTP. A context menu is open over packet 12, showing options like 'Mark/Unmark Packet', 'Ignore/Unignore Packet', 'Set/Unset Time Reference', 'Time Shift...', 'Packet Comment...', 'Edit Resolved Name', 'Apply as Filter', 'Prepare as Filter', 'Conversation Filter', 'Colorize Conversation', 'SCTP', 'Follow', 'Copy', 'Protocol Preferences', 'Decode As...', and 'Show Packet in New Window'. The 'Colorize Conversation' option is selected, opening a submenu with a list of colors (Color 1 to Color 10) and a 'New Coloring Rule...' option. The 'Color 4' option is highlighted in the submenu. The bottom status bar shows 'Packets: 1668 · Displayed: 1668 (100.0%)' and 'Profile: wireshark101'.

No.	Time	TCP Delta	Source	Destination	Protocol	Info
1	0.000000	0.000000...	24.6.173.220	173.194.79.121	TCP	61598 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
2	0.035945	0.035945...	173.194.79.121	24.6.173.220	TCP	80 → 61598 [SYN, ACK] Seq=0 Ack=1 Win=14300 Len=0
3	0.000122	0.000122...	24.6.173.220	173.194.79.121	TCP	61598 → 80 [ACK] Seq=1 Ack=1 Win=65780 Len=0
4	0.000420	0.000420...	24.6.173.220	173.194.79.121	HTTP	GET /api/supported-services.json HTTP/1.1
5	0.035535	0.035535...	173.194.79.121	24.6.173.220	TCP	80 → 61598 [ACK] Seq=1 Ack=323 Win=15424 Len=0
6	0.002258	0.002258...	173.194.79.121	24.6.173.220	HTTP/JSON	HTTP/1.1 200 OK, JavaScript Object Notation (
7	0.195753	0.195753...	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
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.
12	0.001122	0.000000...	24.6.173.220	209.177.86.18	TCP	61599 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
13	0.000000		24.6.173.220	209.177.86.18	TCP	80 → 61599 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0
14	0.000000		209.177.86.18	24.6.173.220	TCP	61599 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
15	0.000000		209.177.86.18	24.6.173.220	HTTP	GET / HTTP/1.1
16	0.000000		24.6.173.220	24.6.173.220	TCP	80 → 61599 [ACK] Seq=1 Ack=291 Win=5504 Len=0
17	0.000000		24.6.173.220	24.6.173.220	HTTP	HTTP/1.0 200 OK
18	0.000000		24.6.173.220	24.6.173.220	HTTP	Continuation

Paso 4:

The image shows the Wireshark network protocol analyzer interface. The main pane displays a list of captured packets. Packet 62 is selected, and a context menu is open over it. The menu options include: Mark/Unmark Packet (Ctrl+M), Ignore/Unignore Packet (Ctrl+D), Set/Unset Time Reference (Ctrl+T), Time Shift... (Ctrl+Shift+T), Packet Comment... (Ctrl+Alt+C), Edit Resolved Name, Apply as Filter, Prepare as Filter, Conversation Filter, Colorize Conversation, SCTP, Follow, Copy, Protocol Preferences, Decode As..., and Show Packet in New Window. The 'Colorize Conversation' option is highlighted, and a sub-menu is open showing color selection options: Color 1 through Color 10, and a 'New Coloring Rule...' option. The 'Color 8' option is selected. The packet list shows various protocols including HTTP, TCP, DNS, and Ethernet. The packet details pane shows the selected packet's structure, and the packet bytes pane shows the raw data.

No.	Time	TCP Delta	Source	Destination	Protocol	Info
52	0.001157	0.001157...	209.177.86.18	24.6.173.220	HTTP	Continuation
53	0.000007	0.000007...	209.177.86.18	24.6.173.220	HTTP	Continuation
54	0.000006	0.000006...	209.177.86.18	24.6.173.220	HTTP	Continuation
55	0.001146	0.001146...	24.6.173.220	209.177.86.18	TCP	61599 → 80 [ACK] Seq=291 Ack=36847 Win=65700 L
56	0.000808	0.000808...	209.177.86.18	24.6.173.220	HTTP	Continuation
57	0.000004	0.000004...	209.177.86.18	24.6.173.220	HTTP	Continuation
58	0.000006	0.000006...	209.177.86.18	24.6.173.220	HTTP	Continuation
59	0.000003	0.000003...	209.177.86.18	24.6.173.220	HTTP	Continuation
60	0.001921	0.001921...	24.6.173.220	209.177.86.18	TCP	61599 → 80 [ACK] Seq=291 Ack=41250 Win=65700 L
61	0.006165	0.006165...	210.72.21.11	24.6.173.220	TCP	61601 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
62	0.006165	0.006165...	210.72.21.11	24.6.173.220	DNS	Standard query 0x6a8e A log.china.cn
63	0.006165	0.006165...	24.6.173.220	210.72.21.11	DNS	Standard query response 0x6a8e A log.china.cn
64	0.006165	0.006165...	210.72.21.11	24.6.173.220	TCP	61602 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
65	0.006165	0.006165...	24.6.173.220	210.72.21.11	TCP	80 → 61601 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
66	0.006165	0.006165...	210.72.21.11	24.6.173.220	TCP	61601 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
67	0.006165	0.006165...	210.72.21.11	24.6.173.220	HTTP	GET /log.js HTTP/1.1
68	0.006165	0.006165...	24.6.173.220	210.72.21.11	TCP	80 → 61602 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
69	0.006165	0.006165...	210.72.21.11	24.6.173.220	TCP	61602 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0

Colorize Conversation sub-menu options:

- 1 Color 1
- 2 Color 2
- 3 Color 3
- 4 Color 4
- 5 Color 5
- 6 Color 6
- 7 Color 7
- 8 Color 8
- 9 Color 9
- 10 Color 10
- New Coloring Rule...

Paso 5:

The image shows the Wireshark network protocol analyzer interface. The main pane displays a list of captured packets. A context menu is open over packet 61, showing options for packet manipulation and coloring. The 'Colorize Conversation' option is selected, which has opened a sub-menu for selecting a color from a list of 10 colors. The bottom status bar indicates 1668 packets displayed (100.0%) and the profile is 'wireshark101'.

No.	Time	TCP Delta	Source	Destination	Protocol	Info
52	0.001157	0.001157...	209.177.86.18	24.6.173.220	HTTP	Continuation
53	0.000007	0.000007...	209.177.86.18	24.6.173.220	HTTP	Continuation
54	0.000006	0.000006...	209.177.86.18	24.6.173.220	HTTP	Continuation
55	0.001146	0.001146...	24.6.173.220	209.177.86.18	TCP	61599 → 80 [ACK] Seq=291 Ack=36847 Win=65700 L
56	0.000808	0.000808...	209.177.86.18	24.6.173.220	HTTP	Continuation
57	0.000004	0.000004...	209.177.86.18	24.6.173.220	HTTP	Continuation
58	0.000006	0.000006...	209.177.86.18	24.6.173.220	HTTP	Continuation
59	0.000003	0.000003...	209.177.86.18	24.6.173.220	HTTP	Continuation
60	0.001921	0.001921...	24.6.173.220	209.177.86.18	TCP	61599 → 80 [ACK] Seq=291 Ack=41250 Win=65700 L
61	0.005165	0.005165...	210.72.21.11	24.6.173.220	TCP	61601 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
62	0.005165	0.005165...	75.75.75.75	24.6.173.220	DNS	Standard query 0x6a8e A log.china.cn
63	0.005165	0.005165...	24.6.173.220	210.72.21.11	DNS	Standard query response 0x6a8e A log.china.cn
64	0.005165	0.005165...	210.72.21.11	24.6.173.220	TCP	61602 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
65	0.005165	0.005165...	24.6.173.220	210.72.21.11	TCP	80 → 61601 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
66	0.005165	0.005165...	210.72.21.11	24.6.173.220	TCP	61601 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
67	0.005165	0.005165...	210.72.21.11	24.6.173.220	HTTP	GET /log.js HTTP/1.1
68	0.005165	0.005165...	24.6.173.220	210.72.21.11	TCP	80 → 61602 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0
69	0.005165	0.005165...	210.72.21.11	24.6.173.220	TCP	61602 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0

Context Menu Options:

- Mark/Unmark Packet (Ctrl+M)
- Ignore/Unignore Packet (Ctrl+D)
- Set/Unset Time Reference (Ctrl+T)
- Time Shift... (Ctrl+Shift+T)
- Packet Comment... (Ctrl+Alt+C)
- Edit Resolved Name
- Apply as Filter
- Prepare as Filter
- Conversation Filter
- Colorize Conversation**
 - CIP Connection
 - Ethernet
 - F5 TCP
 - F5 UDP
 - F5 IP
 - IEEE 802.15.4
 - IPv4
 - IPv6
 - TCP**
 - 1 Color 1
 - 2 Color 2
 - 3 Color 3
 - 4 Color 4
 - 5 Color 5
 - 6 Color 6
 - 7 Color 7
 - 8 Color 8**
 - 9 Color 9
 - 10 Color 10
 - New Coloring Rule...
 - UDP
 - ZigBee Network Layer
 - PN-IO AR
 - PN-IO AR (with data)
 - PN-CBA
- Protocol Preferences
- Decode As...
- Show Packet in New Window