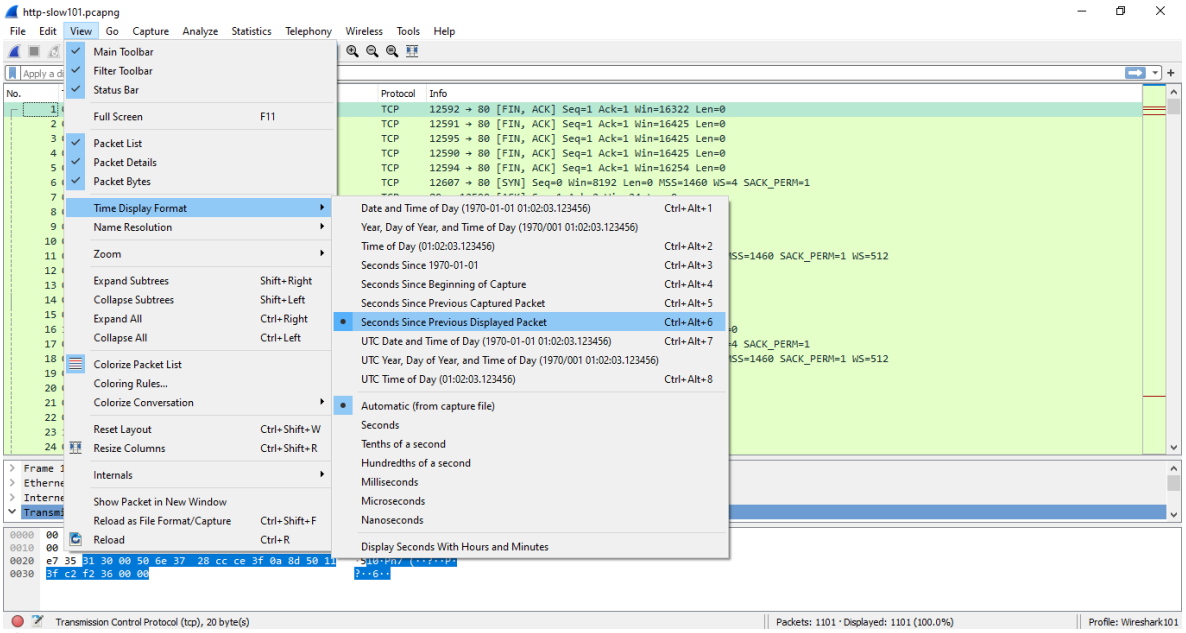
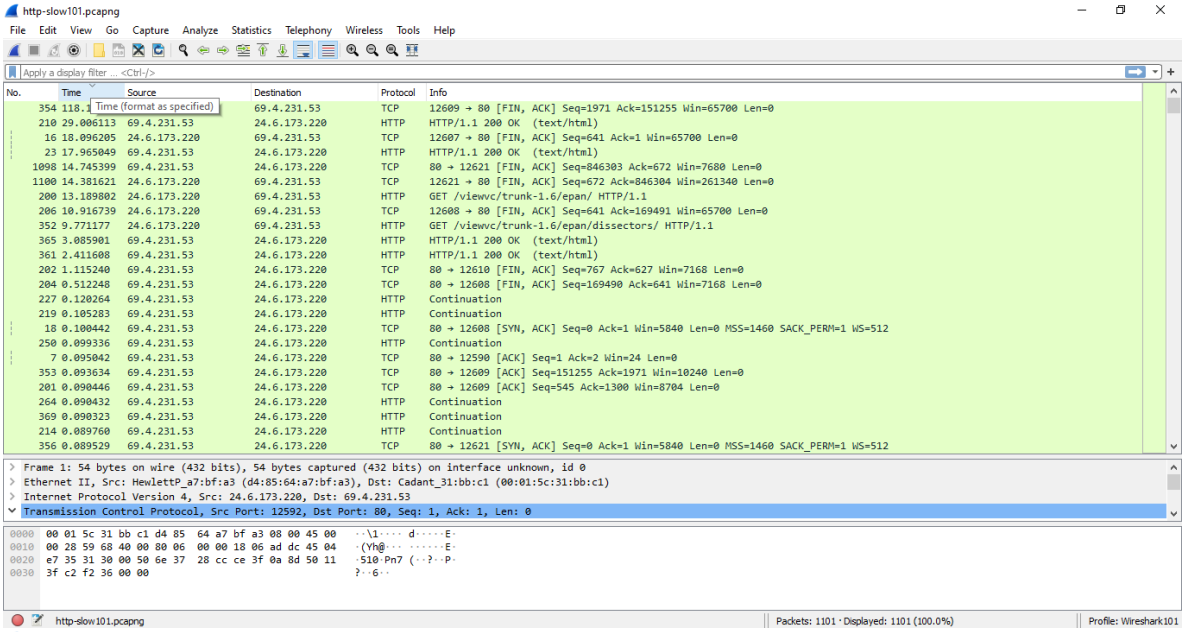
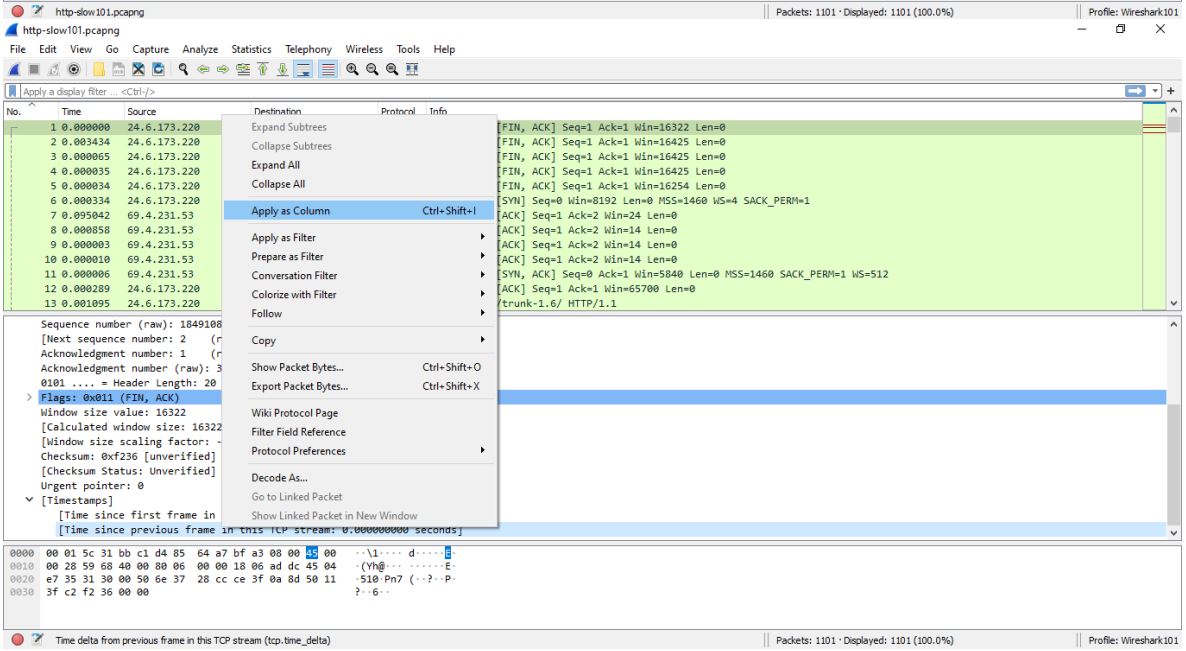
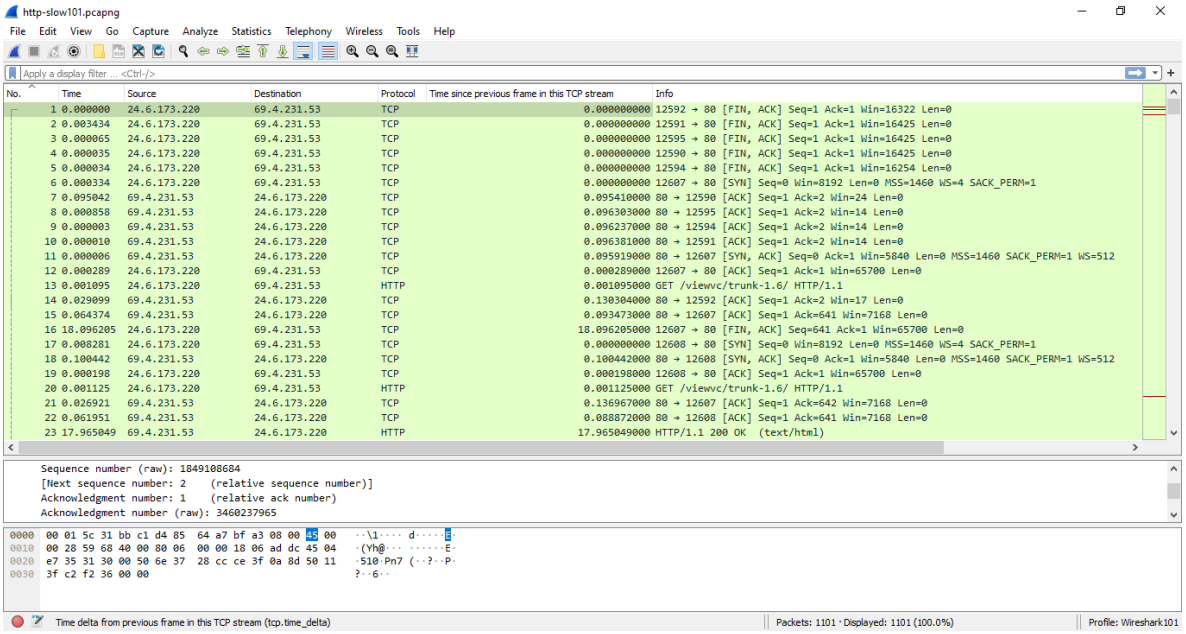
Laboratorio 8
Wireshark

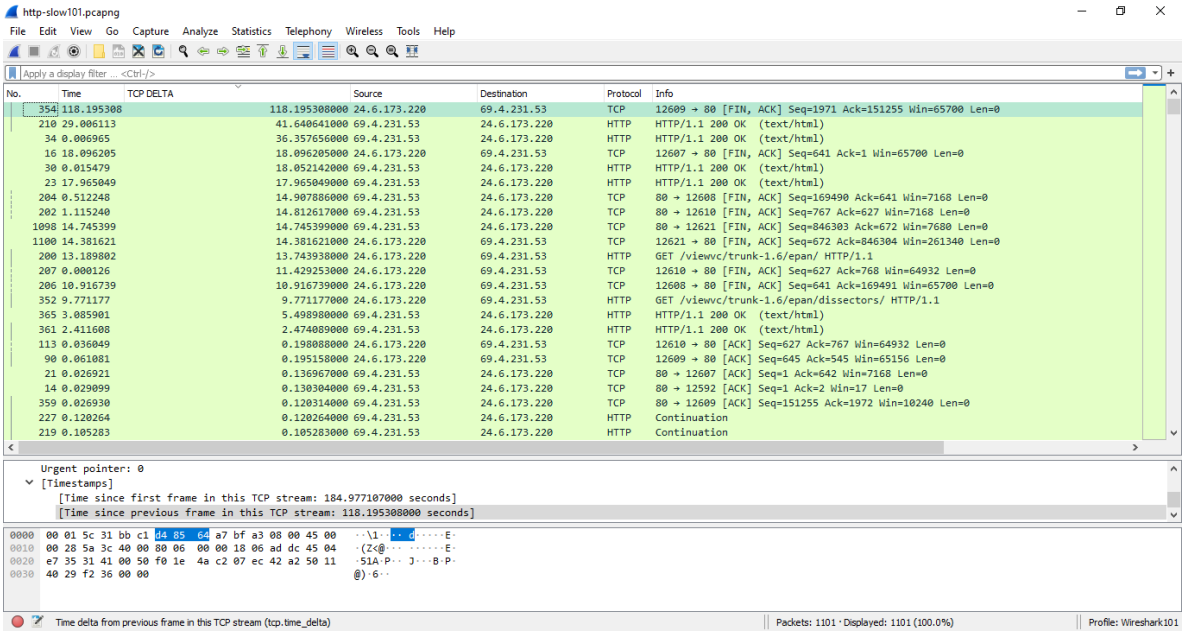
Wilmer Rodríguez Jiménez
Fundamentos de telecomunicaciones
Prof: Ismael Jimenez Sanchez
Periodo Ago – Dic


http-slow101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Main Toolbar
Filter Toolbar
Status Bar
Full Screen F11
Packet List
Packet Details
Packet Bytes
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout Ctrl+Shift+W
Resize Columns Ctrl+Shift+R
Internals
Show Packet in New Window
Reload as File Format/Capture Ctrl+Shift+F
Reload Ctrl+R
Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+1
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
Time of Day (01:02:03.123456) Ctrl+Alt+2
Seconds Since 1970-01-01 Ctrl+Alt+3
Seconds Since Beginning of Capture Ctrl+Alt+4
Seconds Since Previous Captured Packet Ctrl+Alt+5
Seconds Since Previous Displayed Packet Ctrl+Alt+6
UTC Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+7
UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
UTC Time of Day (01:02:03.123456) Ctrl+Alt+8
Automatic (from capture file)
Seconds
Tenths of a second
Hundredths of a second
Milliseconds
Microseconds
Nanoseconds
Display Seconds With Hours and Minutes
Protocol Info
TCP 12592 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16322 Len=0
TCP 12591 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
TCP 12595 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
TCP 12590 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
TCP 12594 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16254 Len=0
TCP 12607 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
Transmission Control Protocol (tcp), 20 byte(s)
Packets: 1101 · Displayed: 1101 (100.0%)
Profile: Wireshark101


http-slow101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Info
Time (format as specified)
354 118.1 69.4.231.53 TCP 12609 → 80 [FIN, ACK] Seq=1971 Ack=151255 Win=65700 Len=0
210 29.006113 69.4.231.53 24.6.173.220 HTTP HTTP/1.1 200 OK (text/html)
16 18.096205 24.6.173.220 69.4.231.53 TCP 12607 → 80 [FIN, ACK] Seq=641 Ack=1 Win=65700 Len=0
23 17.965049 69.4.231.53 24.6.173.220 HTTP HTTP/1.1 200 OK (text/html)
1098 14.745399 69.4.231.53 24.6.173.220 TCP 80 → 12621 [FIN, ACK] Seq=846303 Ack=672 Win=7680 Len=0
1100 14.381621 24.6.173.220 69.4.231.53 TCP 12621 → 80 [FIN, ACK] Seq=672 Ack=846304 Win=261340 Len=0
200 13.189802 24.6.173.220 69.4.231.53 HTTP GET /viewvc/trunk-1.6/epan/ HTTP/1.1
206 10.916739 24.6.173.220 69.4.231.53 TCP 12608 → 80 [FIN, ACK] Seq=641 Ack=169491 Win=65700 Len=0
352 9.771177 24.6.173.220 69.4.231.53 HTTP GET /viewvc/trunk-1.6/epan/dissectors/ HTTP/1.1
365 3.085901 69.4.231.53 24.6.173.220 HTTP HTTP/1.1 200 OK (text/html)
361 2.411608 69.4.231.53 24.6.173.220 HTTP HTTP/1.1 200 OK (text/html)
202 1.115240 69.4.231.53 24.6.173.220 TCP 80 → 12610 [FIN, ACK] Seq=767 Ack=627 Win=7168 Len=0
204 0.512248 69.4.231.53 24.6.173.220 TCP 80 → 12608 [FIN, ACK] Seq=169490 Ack=641 Win=7168 Len=0
227 0.120264 69.4.231.53 24.6.173.220 HTTP Continuation
219 0.105283 69.4.231.53 24.6.173.220 HTTP Continuation
18 0.100442 69.4.231.53 24.6.173.220 TCP 80 → 12608 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=512
250 0.099336 69.4.231.53 24.6.173.220 HTTP Continuation
7 0.095042 69.4.231.53 24.6.173.220 TCP 80 → 12590 [ACK] Seq=1 Ack=2 Win=24 Len=0
353 0.093634 69.4.231.53 24.6.173.220 TCP 80 → 12609 [ACK] Seq=151255 Ack=1971 Win=10240 Len=0
201 0.090446 69.4.231.53 24.6.173.220 TCP 80 → 12609 [ACK] Seq=545 Ack=1300 Win=8704 Len=0
264 0.090432 69.4.231.53 24.6.173.220 HTTP Continuation
369 0.090323 69.4.231.53 24.6.173.220 HTTP Continuation
214 0.089760 69.4.231.53 24.6.173.220 HTTP Continuation
356 0.089529 69.4.231.53 24.6.173.220 TCP 80 → 12621 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=512
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface unknown, id 0
Ethernet II, Src: HewlettP_a7: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: 69.4.231.53
Transmission Control Protocol, Src Port: 12592, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 00 28 59 68 40 00 80 06 00 00 18 06 ad dc 45 04
0020 e7 35 31 30 00 50 6e 37 28 cc ce 3f 0a 8d 50 11
0030 3f c2 f2 36 00 00
http-slow101.pcapng
Packets: 1101 · Displayed: 1101 (100.0%)
Profile: Wireshark101


http-slow101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Info
1 0.000000 24.6.173.220
2 0.003434 24.6.173.220
3 0.000065 24.6.173.220
4 0.000035 24.6.173.220
5 0.000034 24.6.173.220
6 0.000334 24.6.173.220
7 0.095042 69.4.231.53
8 0.000858 69.4.231.53
9 0.000003 69.4.231.53
10 0.000010 69.4.231.53
11 0.000006 69.4.231.53
12 0.000289 24.6.173.220
13 0.001095 24.6.173.220
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Sequence number (raw): 1849108
[Next sequence number: 2
Acknowledgment number: 1
Acknowledgment number (raw): 3
0101 .... = Header Length: 20
Flags: 0x011 (FIN, ACK)
Window size value: 16322
[Calculated window size: 16322
[Window size scaling factor: -
Checksum: 0xf236 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[Timestamps]
[Time since first frame in
[Time since previous frame in this TCP stream: 0.000000000 seconds]
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 00 28 59 68 40 00 80 06 00 00 18 06 ad dc 45 04
0020 e7 35 31 30 00 50 6e 37 28 cc ce 3f 0a 8d 50 11
0030 3f c2 f2 36 00 00
Time delta from previous frame in this TCP stream (tcp.time_delta)
Packets: 1101 · Displayed: 1101 (100.0%)
Profile: Wireshark101


http-slow101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Time since previous frame in this TCP stream Info
1 0.000000 24.6.173.220 69.4.231.53 TCP 0.000000000 12592 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16322 Len=0
2 0.003434 24.6.173.220 69.4.231.53 TCP 0.000000000 12591 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
3 0.000065 24.6.173.220 69.4.231.53 TCP 0.000000000 12595 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
4 0.000035 24.6.173.220 69.4.231.53 TCP 0.000000000 12590 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16425 Len=0
5 0.000034 24.6.173.220 69.4.231.53 TCP 0.000000000 12594 → 80 [FIN, ACK] Seq=1 Ack=1 Win=16254 Len=0
6 0.000334 24.6.173.220 69.4.231.53 TCP 0.000000000 12607 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
7 0.095042 69.4.231.53 24.6.173.220 TCP 0.095410000 80 → 12590 [ACK] Seq=1 Ack=2 Win=24 Len=0
8 0.000858 69.4.231.53 24.6.173.220 TCP 0.096303000 80 → 12595 [ACK] Seq=1 Ack=2 Win=14 Len=0
9 0.000003 69.4.231.53 24.6.173.220 TCP 0.096237000 80 → 12594 [ACK] Seq=1 Ack=2 Win=14 Len=0
10 0.000010 69.4.231.53 24.6.173.220 TCP 0.096381000 80 → 12591 [ACK] Seq=1 Ack=2 Win=14 Len=0
11 0.000006 69.4.231.53 24.6.173.220 TCP 0.095919000 80 → 12607 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=512
12 0.000289 24.6.173.220 69.4.231.53 TCP 0.000289000 12607 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
13 0.001095 24.6.173.220 69.4.231.53 HTTP 0.001095000 GET /viewvc/trunk-1.6/ HTTP/1.1
14 0.029099 69.4.231.53 24.6.173.220 TCP 0.130304000 80 → 12592 [ACK] Seq=1 Ack=2 Win=17 Len=0
15 0.064374 69.4.231.53 24.6.173.220 TCP 0.093473000 80 → 12607 [ACK] Seq=1 Ack=641 Win=7168 Len=0
16 18.096205 24.6.173.220 69.4.231.53 TCP 18.096205000 12607 → 80 [FIN, ACK] Seq=641 Ack=1 Win=65700 Len=0
17 0.008281 24.6.173.220 69.4.231.53 TCP 0.000000000 12608 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
18 0.100442 69.4.231.53 24.6.173.220 TCP 0.100442000 80 → 12608 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SACK_PERM=1 WS=512
19 0.000198 24.6.173.220 69.4.231.53 TCP 0.000198000 12608 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
20 0.001125 24.6.173.220 69.4.231.53 HTTP 0.001125000 GET /viewvc/trunk-1.6/ HTTP/1.1
21 0.026921 69.4.231.53 24.6.173.220 TCP 0.136967000 80 → 12607 [ACK] Seq=1 Ack=642 Win=7168 Len=0
22 0.061951 69.4.231.53 24.6.173.220 TCP 0.088872000 80 → 12608 [ACK] Seq=1 Ack=641 Win=7168 Len=0
23 17.965049 69.4.231.53 24.6.173.220 HTTP 17.965049000 HTTP/1.1 200 OK (text/html)
Sequence number (raw): 1849108684
[Next sequence number: 2 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Acknowledgment number (raw): 3460237965
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 00 28 59 68 40 00 80 06 00 00 18 06 ad dc 45 04
0020 e7 35 31 30 00 50 6e 37 28 cc ce 3f 0a 8d 50 11
0030 3f c2 f2 36 00 00
Time delta from previous frame in this TCP stream (tcp.time_delta)
Packets: 1101 · Displayed: 1101 (100.0%)
Profile: Wireshark101


http-slow101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time TCP DELTA Source Destination Protocol Info
354 118.195308 118.195308000 24.6.173.220 69.4.231.53 TCP 12609 → 80 [FIN, ACK] Seq=1971 Ack=151255 Win=65700 Len=0
210 29.006113 41.640641000 69.4.231.53 24.6.173.220 HTTP HTTP/1.1 200 OK (text/html)
34 0.006965 36.357656000 69.4.231.53 24.6.173.220 HTTP HTTP/1.1 200 OK (text/html)
16 18.096205 18.096205000 24.6.173.220 69.4.231.53 TCP 12607 → 80 [FIN, ACK] Seq=641 Ack=1 Win=65700 Len=0
30 0.015479 18.052142000 69.4.231.53 24.6.173.220 HTTP HTTP/1.1 200 OK (text/html)
23 17.965049 17.965049000 69.4.231.53 24.6.173.220 HTTP HTTP/1.1 200 OK (text/html)
204 0.512248 14.907886000 69.4.231.53 24.6.173.220 TCP 80 → 12608 [FIN, ACK] Seq=169490 Ack=641 Win=7168 Len=0
202 1.115240 14.812617000 69.4.231.53 24.6.173.220 TCP 80 → 12610 [FIN, ACK] Seq=767 Ack=627 Win=7168 Len=0
1098 14.745399 14.745399000 69.4.231.53 24.6.173.220 TCP 80 → 12621 [FIN, ACK] Seq=846303 Ack=672 Win=7680 Len=0
1100 14.381621 14.381621000 24.6.173.220 69.4.231.53 TCP 12621 → 80 [FIN, ACK] Seq=672 Ack=846304 Win=261340 Len=0
200 13.189802 13.743938000 24.6.173.220 69.4.231.53 HTTP GET /viewvc/trunk-1.6/epan/ HTTP/1.1
207 0.000126 11.429253000 24.6.173.220 69.4.231.53 TCP 12610 → 80 [FIN, ACK] Seq=627 Ack=768 Win=64932 Len=0
206 10.916739 10.916739000 24.6.173.220 69.4.231.53 TCP 12608 → 80 [FIN, ACK] Seq=641 Ack=169491 Win=65700 Len=0
352 9.771177 9.771177000 24.6.173.220 69.4.231.53 HTTP GET /viewvc/trunk-1.6/epan/dissectors/ HTTP/1.1
365 3.085901 5.498980000 69.4.231.53 24.6.173.220 HTTP HTTP/1.1 200 OK (text/html)
361 2.411608 2.474089000 69.4.231.53 24.6.173.220 HTTP HTTP/1.1 200 OK (text/html)
113 0.036049 0.198088000 24.6.173.220 69.4.231.53 TCP 12610 → 80 [ACK] Seq=627 Ack=767 Win=64932 Len=0
90 0.061081 0.195158000 24.6.173.220 69.4.231.53 TCP 12609 → 80 [ACK] Seq=645 Ack=545 Win=65156 Len=0
21 0.026921 0.136967000 69.4.231.53 24.6.173.220 TCP 80 → 12607 [ACK] Seq=1 Ack=642 Win=7168 Len=0
14 0.029099 0.130304000 69.4.231.53 24.6.173.220 TCP 80 → 12592 [ACK] Seq=1 Ack=2 Win=17 Len=0
359 0.026930 0.120314000 69.4.231.53 24.6.173.220 TCP 80 → 12609 [ACK] Seq=151255 Ack=1972 Win=10240 Len=0
227 0.120264 0.120264000 69.4.231.53 24.6.173.220 HTTP Continuation
219 0.105283 0.105283000 69.4.231.53 24.6.173.220 HTTP Continuation
Urgent pointer: 0
[Timestamps]
[Time since first frame in this TCP stream: 184.977107000 seconds]
[Time since previous frame in this TCP stream: 118.195308000 seconds]
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00
0010 00 28 5a 3c 40 00 80 06 00 00 18 06 ad dc 45 04
0020 e7 35 31 41 00 50 f0 1e 4a c2 07 ec 42 a2 50 11
0030 40 29 f2 36 00 00
Time delta from previous frame in this TCP stream (tcp.time_delta)
Packets: 1101 · Displayed: 1101 (100.0%)
Profile: Wireshark101