INSTITUTO TECNOLOGICO DE CANCUN

Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

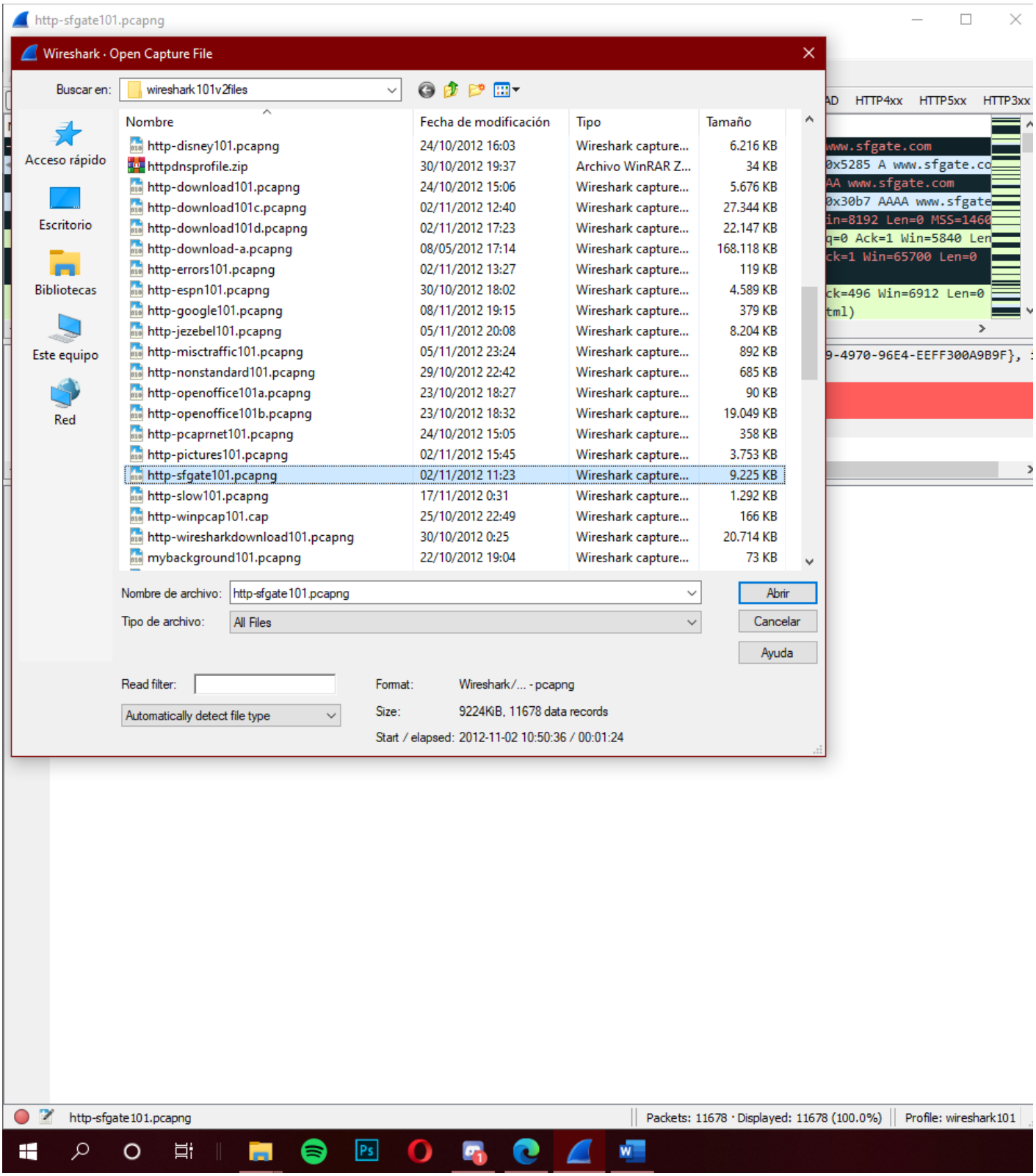
N.º De Actividad: Laboratorio

Nombre Del Alumno: Vazquez Canto Andres Omar

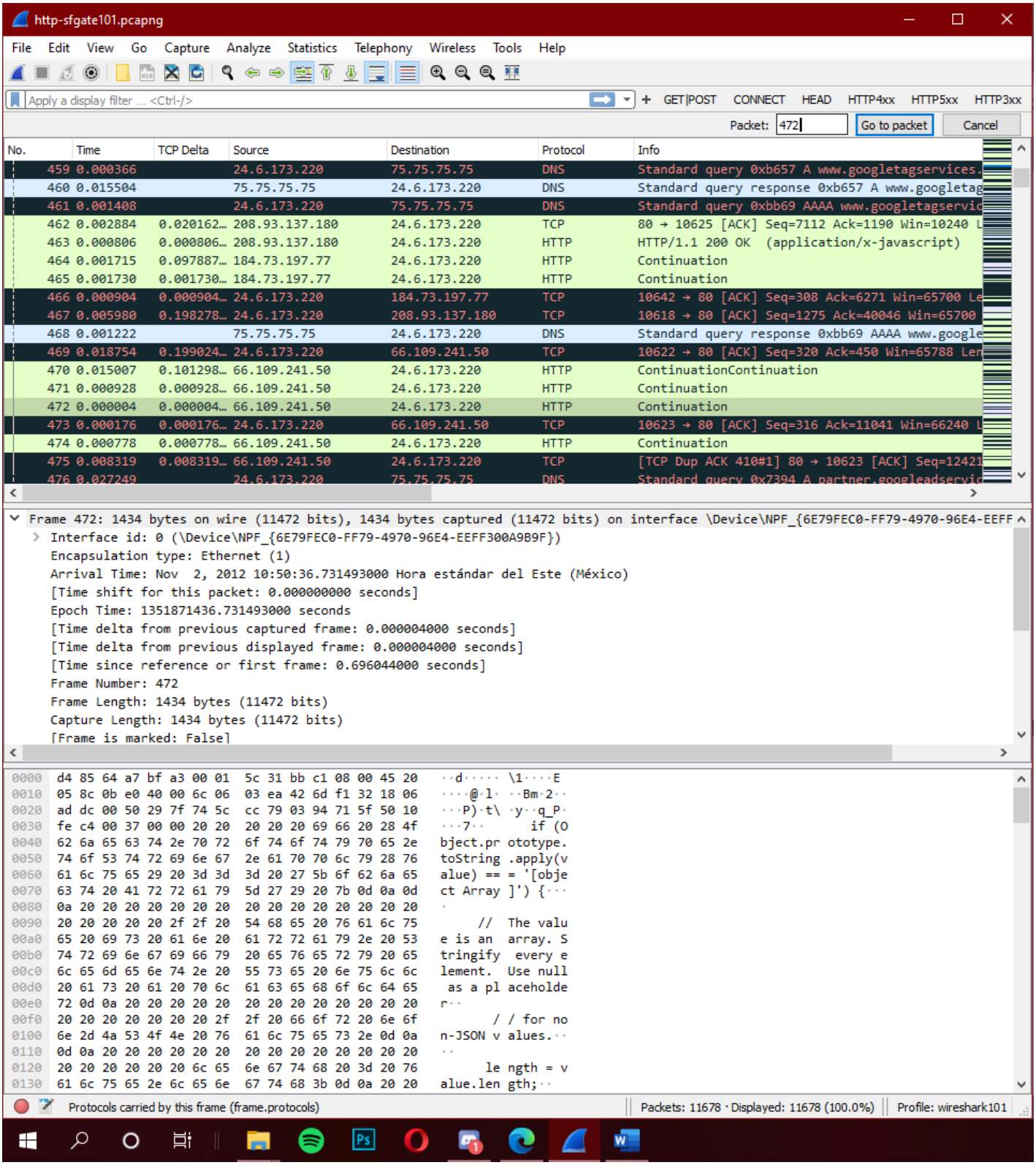
N.º De Control: 17530439

Lab25- Add a Column to Display Coloring Rules in Use

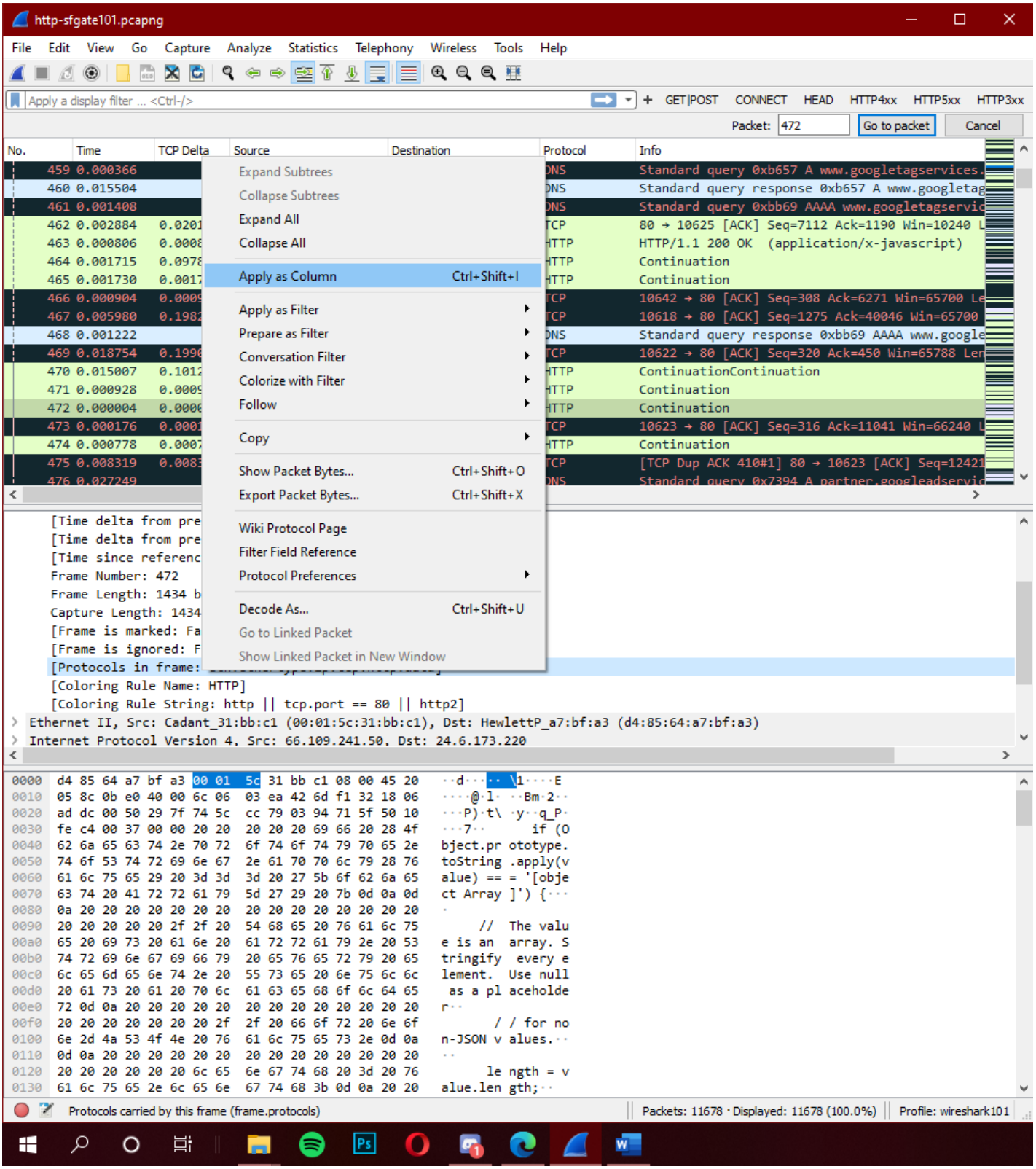
Paso 1:

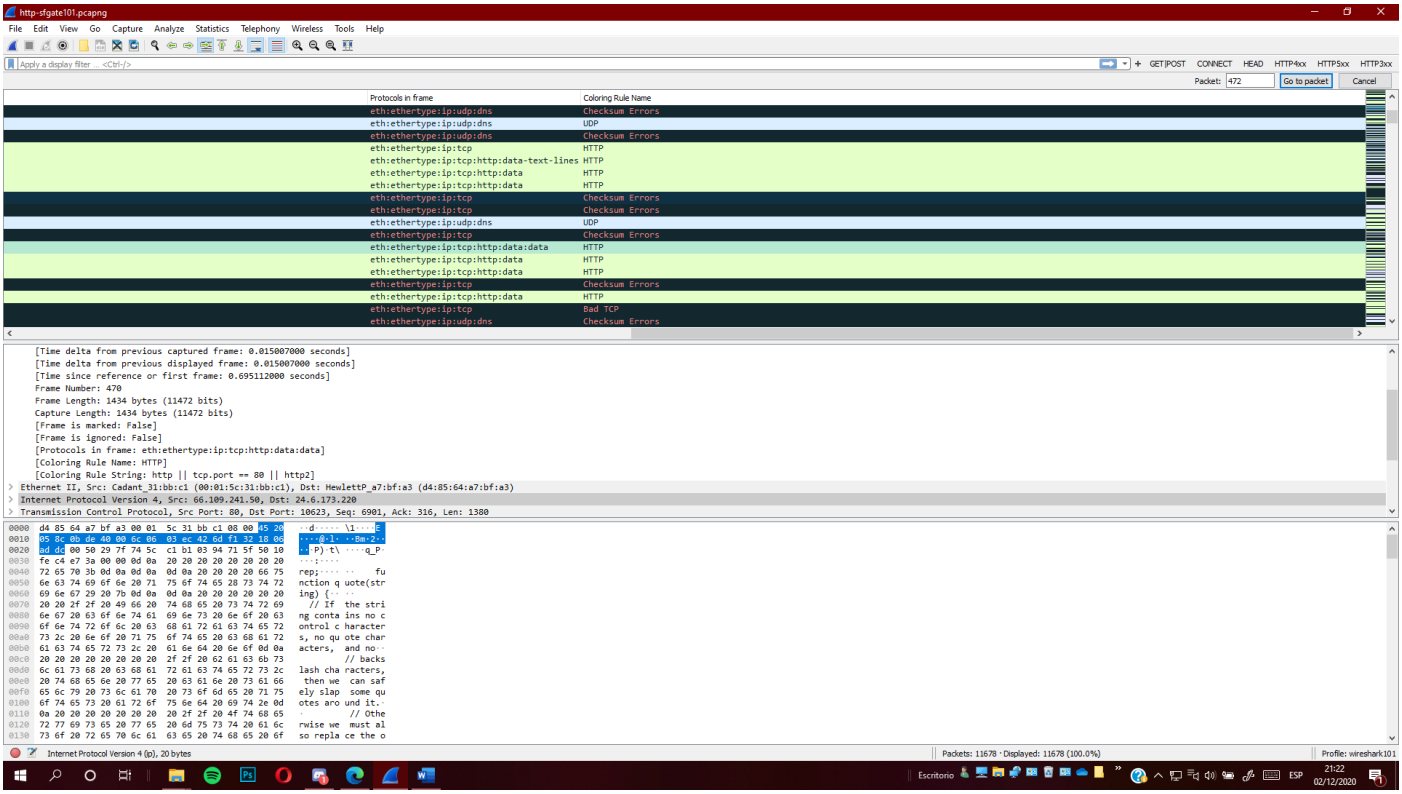


Paso 2:


http-sfgate101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
GET|POST CONNECT HEAD HTTP4xx HTTP5xx HTTP3xx
Packet: 472
Go to packet
Cancel
No. Time TCP Delta Source Destination Protocol Info
459 0.000366 24.6.173.220 75.75.75.75 DNS Standard query 0xb657 A www.googletagservices.
460 0.015504 75.75.75.75 24.6.173.220 DNS Standard query response 0xb657 A www.googletag
461 0.001408 24.6.173.220 75.75.75.75 DNS Standard query 0xbb69 AAAA www.googletagservic
462 0.002884 0.020162... 208.93.137.180 24.6.173.220 TCP 80 → 10625 [ACK] Seq=7112 Ack=1190 Win=10240 L
463 0.000806 0.000806... 208.93.137.180 24.6.173.220 HTTP HTTP/1.1 200 OK (application/x-javascript)
464 0.001715 0.097887... 184.73.197.77 24.6.173.220 HTTP Continuation
465 0.001730 0.001730... 184.73.197.77 24.6.173.220 HTTP Continuation
466 0.000904 0.000904... 24.6.173.220 184.73.197.77 TCP 10642 → 80 [ACK] Seq=308 Ack=6271 Win=65700 Le
467 0.005980 0.198278... 24.6.173.220 208.93.137.180 TCP 10618 → 80 [ACK] Seq=1275 Ack=40046 Win=65700
468 0.001222 75.75.75.75 24.6.173.220 DNS Standard query response 0xbb69 AAAA www.google
469 0.018754 0.199024... 24.6.173.220 66.109.241.50 TCP 10622 → 80 [ACK] Seq=320 Ack=450 Win=65788 Len
470 0.015007 0.101298... 66.109.241.50 24.6.173.220 HTTP ContinuationContinuation
471 0.000928 0.000928... 66.109.241.50 24.6.173.220 HTTP Continuation
472 0.000004 0.000004... 66.109.241.50 24.6.173.220 HTTP Continuation
473 0.000176 0.000176... 24.6.173.220 66.109.241.50 TCP 10623 → 80 [ACK] Seq=316 Ack=11041 Win=66240 L
474 0.000778 0.000778... 66.109.241.50 24.6.173.220 HTTP Continuation
475 0.008319 0.008319... 66.109.241.50 24.6.173.220 TCP [TCP Dup ACK 410#1] 80 → 10623 [ACK] Seq=12421
476 0.027249 24.6.173.220 75.75.75.75 DNS Standard query 0x7394 A partner.googleadservic
Frame 472: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface \Device\NPF_{6E79FEC0-FF79-4970-96E4-EEFF
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
Frame Length: 1434 bytes (11472 bits)
Capture Length: 1434 bytes (11472 bits)
[Frame is marked: False]
0000 d4 85 64 a7 bf a3 00 01 5c 31 bb c1 08 00 45 20 ··d····· \1····E
0010 05 8c 0b e0 40 00 6c 06 03 ea 42 6d f1 32 18 06 ····@·l· ··Bm·2··
0020 ad dc 00 50 29 7f 74 5c cc 79 03 94 71 5f 50 10 ···P)·t\ ·y··q_P·
0030 fe c4 00 37 00 00 20 20 20 20 20 69 66 20 28 4f ···7·· if (O
0040 62 6a 65 63 74 2e 70 72 6f 74 6f 74 79 70 65 2e bject.pr ototype.
0050 74 6f 53 74 72 69 6e 67 2e 61 70 70 6c 79 28 76 toString .apply(v
0060 61 6c 75 65 29 20 3d 3d 3d 20 27 5b 6f 62 6a 65 alue) == = '[obje
0070 63 74 20 41 72 72 61 79 5d 27 29 20 7b 0d 0a 0d ct Array]') {···
0080 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ·
0090 20 20 20 20 20 2f 2f 20 54 68 65 20 76 61 6c 75 // The valu
00a0 65 20 69 73 20 61 6e 20 61 72 72 61 79 2e 20 53 e is an array. S
00b0 74 72 69 6e 67 69 66 79 20 65 76 65 72 79 20 65 tringify every e
00c0 6c 65 6d 65 6e 74 2e 20 55 73 65 20 6e 75 6c 6c lement. Use null
00d0 20 61 73 20 61 20 70 6c 61 63 65 68 6f 6c 64 65 as a pl aceholde
00e0 72 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 r··
00f0 20 20 20 20 20 20 20 2f 2f 20 66 6f 72 20 6e 6f / / for no
0100 6e 2d 4a 53 4f 4e 20 76 61 6c 75 65 73 2e 0d 0a n-JSON v alues.··
0110 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 ··
0120 20 20 20 20 20 20 6c 65 6e 67 74 68 20 3d 20 76 le ngth = v
0130 61 6c 75 65 2e 6c 65 6e 67 74 68 3b 0d 0a 20 20 alue.len gth;··
Protocols carried by this frame (frame.protocols)
Packets: 11678 · Displayed: 11678 (100.0%)
Profile: wireshark101

Paso 3 y 4:


http-sfgate101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
GET|POST CONNECT HEAD HTTP4xx HTTP5xx HTTP3xx
Packet: 472
Go to packet
Cancel
No. Time TCP Delta Source Destination Protocol Info
459 0.000366
460 0.015504
461 0.001408
462 0.002884 0.0201
463 0.000806 0.0008
464 0.001715 0.0978
465 0.001730 0.0017
466 0.000904 0.0009
467 0.005980 0.1982
468 0.001222
469 0.018754 0.1990
470 0.015007 0.1012
471 0.000928 0.0009
472 0.000004 0.0006
473 0.000176 0.0001
474 0.000778 0.0007
475 0.008319 0.0083
476 0.027249
Standard query 0xb657 A www.googletagservices.
Standard query response 0xb657 A www.googletag
Standard query 0xbb69 AAAA www.googletagservic
80 → 10625 [ACK] Seq=7112 Ack=1190 Win=10240
HTTP/1.1 200 OK (application/x-javascript)
Continuation
Continuation
10642 → 80 [ACK] Seq=308 Ack=6271 Win=65700
10618 → 80 [ACK] Seq=1275 Ack=40046 Win=65700
Standard query response 0xbb69 AAAA www.google
10622 → 80 [ACK] Seq=320 Ack=450 Win=65788
ContinuationContinuation
Continuation
Continuation
10623 → 80 [ACK] Seq=316 Ack=11041 Win=66240
Continuation
[TCP Dup ACK 410#1] 80 → 10623 [ACK] Seq=12421
Standard query 0x7394 A partner.googleadservic
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... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window
[Time delta from pre
[Time delta from pre
[Time since referenc
Frame Number: 472
Frame Length: 1434 b
Capture Length: 1434
[Frame is marked: Fa
[Frame is ignored: F
[Protocols in frame:
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
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
0000 d4 85 64 a7 bf a3 00 01 5c 31 bb c1 08 00 45 20
0010 05 8c 0b e0 40 00 6c 06 03 ea 42 6d f1 32 18 06
0020 ad dc 00 50 29 7f 74 5c cc 79 03 94 71 5f 50 10
0030 fe c4 00 37 00 00 20 20 20 20 20 69 66 20 28 4f
0040 62 6a 65 63 74 2e 70 72 6f 74 6f 74 79 70 65 2e
0050 74 6f 53 74 72 69 6e 67 2e 61 70 70 6c 79 28 76
0060 61 6c 75 65 29 20 3d 3d 3d 20 27 5b 6f 62 6a 65
0070 63 74 20 41 72 72 61 79 5d 27 29 20 7b 0d 0a 0d
0080 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0090 20 20 20 20 20 2f 2f 20 54 68 65 20 76 61 6c 75
00a0 65 20 69 73 20 61 6e 20 61 72 72 61 79 2e 20 53
00b0 74 72 69 6e 67 69 66 79 20 65 76 65 72 79 20 65
00c0 6c 65 6d 65 6e 74 2e 20 55 73 65 20 6e 75 6c 6c
00d0 20 61 73 20 61 20 70 6c 61 63 65 68 6f 6c 64 65
00e0 72 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20
00f0 20 20 20 20 20 20 20 2f 2f 20 66 6f 72 20 6e 6f
0100 6e 2d 4a 53 4f 4e 20 76 61 6c 75 65 73 2e 0d 0a
0110 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0120 20 20 20 20 20 20 6c 65 6e 67 74 68 20 3d 20 76
0130 61 6c 75 65 2e 6c 65 6e 67 74 68 3b 0d 0a 20 20
Protocols carried by this frame (frame.protocols)
Packets: 11678 · Displayed: 11678 (100.0%)
Profile: wireshark101


http-sfgate101.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
GET|POST CONNECT HEAD HTTP4xx HTTP5xx HTTP3xx
Packet: 472 Go to packet Cancel
Protocols in frame
Coloring Rule Name
eth:ethertype:ip:udp:dns Checksum Errors
eth:ethertype:ip:udp:dns UDP
eth:ethertype:ip:udp:dns Checksum Errors
eth:ethertype:ip:tcp HTTP
eth:ethertype:ip:tcp:http:data-text-lines HTTP
eth:ethertype:ip:tcp:http:data HTTP
eth:ethertype:ip:tcp:http:data HTTP
eth:ethertype:ip:tcp Checksum Errors
eth:ethertype:ip:tcp Checksum Errors
eth:ethertype:ip:udp:dns UDP
eth:ethertype:ip:tcp Checksum Errors
eth:ethertype:ip:tcp:http:data:data HTTP
eth:ethertype:ip:tcp:http:data HTTP
eth:ethertype:ip:tcp:http:data HTTP
eth:ethertype:ip:tcp Checksum Errors
eth:ethertype:ip:tcp:http:data HTTP
eth:ethertype:ip:tcp Bad TCP
eth:ethertype:ip:udp:dns Checksum Errors
[Time delta from previous captured frame: 0.015007000 seconds]
[Time delta from previous displayed frame: 0.015007000 seconds]
[Time since reference or first frame: 0.695112000 seconds]
Frame Number: 470
Frame Length: 1434 bytes (11472 bits)
Capture Length: 1434 bytes (11472 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:data:data]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
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: 6901, Ack: 316, Len: 1380
0000 d4 85 64 a7 bf a3 00 01 5c 31 bb c1 08 00 45 20
0010 05 8c 0b de 40 00 6c 06 03 ec 42 6d f1 32 18 06
0020 bd d8 00 50 29 7f 74 5c c1 b1 03 94 71 5f 50 10
0030 fe e7 3a 00 00 0d 0a 20 20 20 20 20 20 20 20
0040 72 65 70 3b 0d 0a 0d 0a 0d 0a 20 20 20 20 66 75
0050 6e 63 74 69 6f 6e 20 71 75 6f 74 65 28 73 74 72
0060 69 6e 67 29 20 7b 0d 0a 0d 0a 20 20 20 20 20 20
0070 20 20 2f 2f 20 49 66 20 74 68 65 20 73 74 72 69
0080 6e 67 20 63 6f 6e 74 61 69 6e 73 20 6e 6f 20 63
0090 6f 6e 74 72 6f 6c 20 63 68 61 72 61 63 74 65 72
00a0 73 2c 20 6e 6f 20 71 75 6f 74 65 20 63 68 61 72
00b0 61 63 74 65 72 73 2c 20 61 6e 64 20 6e 6f 0d 0a
00c0 20 20 20 20 20 20 20 20 2f 2f 20 62 61 63 6b 73
00d0 6c 61 73 68 20 63 68 61 72 61 63 74 65 72 73 2c
00e0 20 74 68 65 6e 20 77 65 20 63 61 6e 20 73 61 66
00f0 65 6c 79 20 73 6c 61 70 20 73 6f 6d 65 20 71 75
0100 6f 74 65 73 20 61 72 6f 75 6e 64 20 69 74 2e 0d
0110 0a 20 20 20 20 20 20 20 20 2f 2f 20 4f 74 68 65
0120 72 77 69 73 65 20 77 65 20 6d 75 73 74 20 61 6c
0130 73 6f 20 72 65 70 6c 61 63 65 20 74 68 65 20 6f
Internet Protocol Version 4 (ip), 20 bytes
Packets: 11678 · Displayed: 11678 (100.0%)
Profile: wireshark101
Escritorio
ESP
21:22
02/12/2020