INSTITUTO TECNOLOGICO DE CANCUN

Nombre De La Materia: Fundamentos De Telecomunicaciones

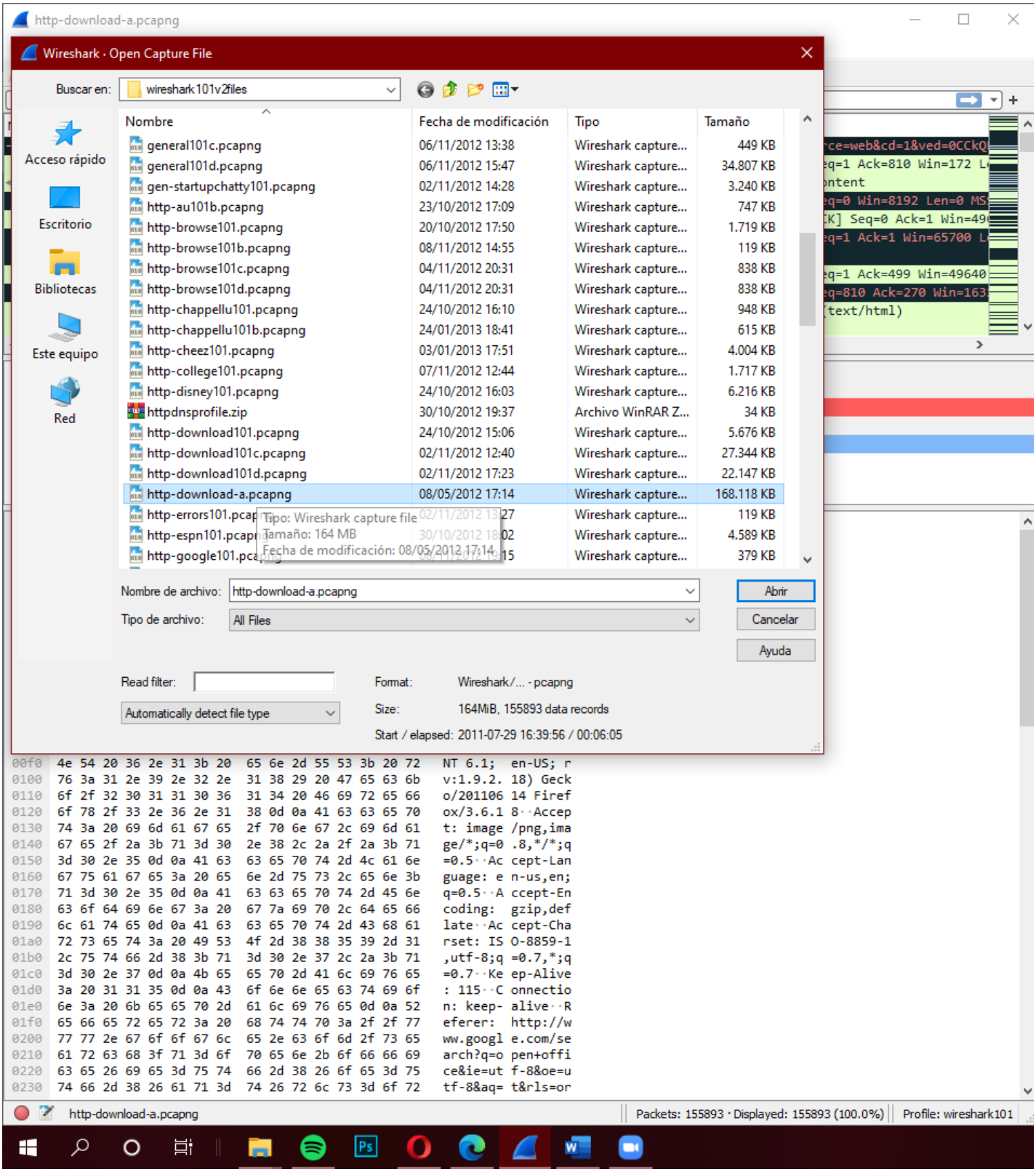
Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 24

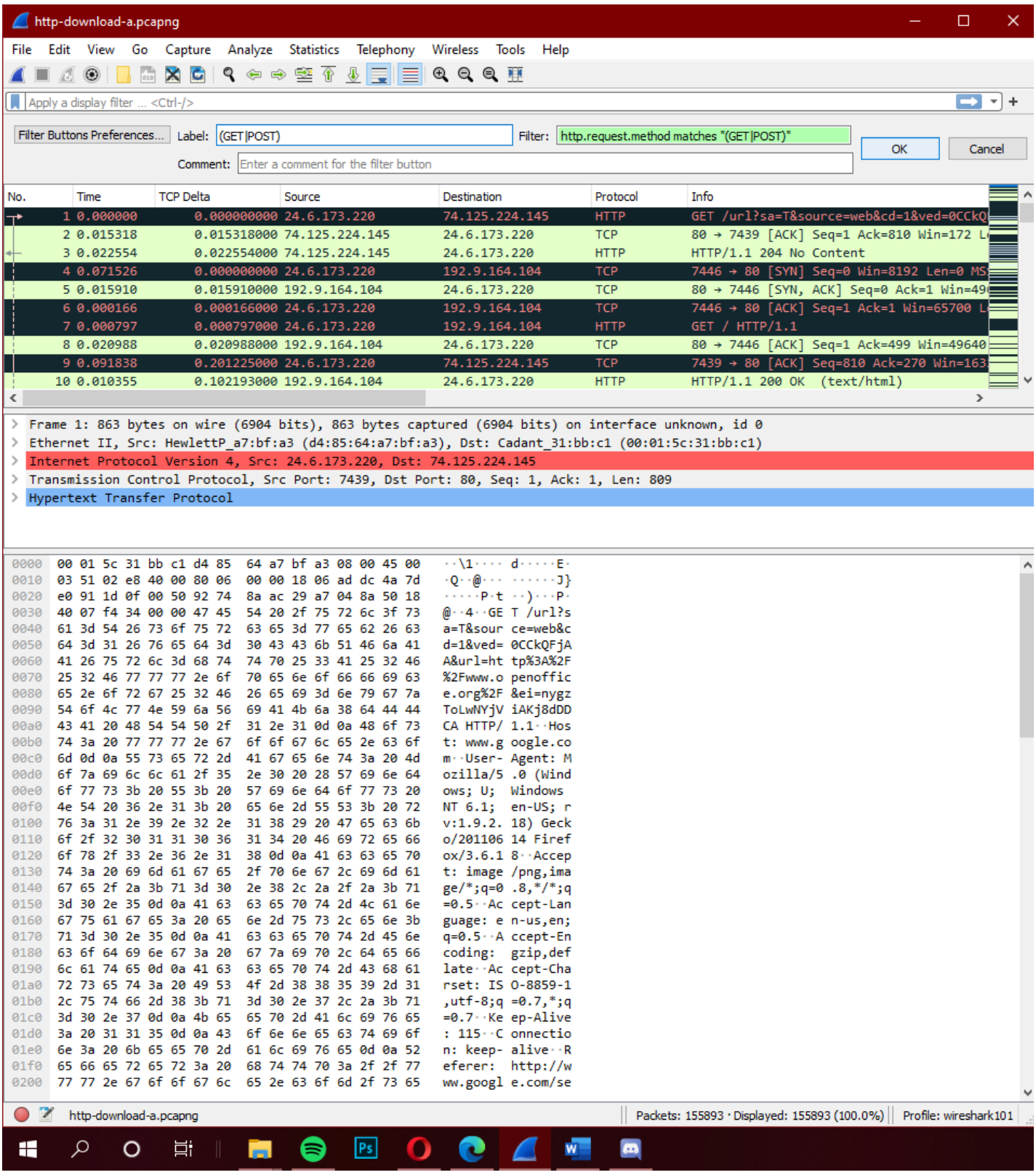
Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

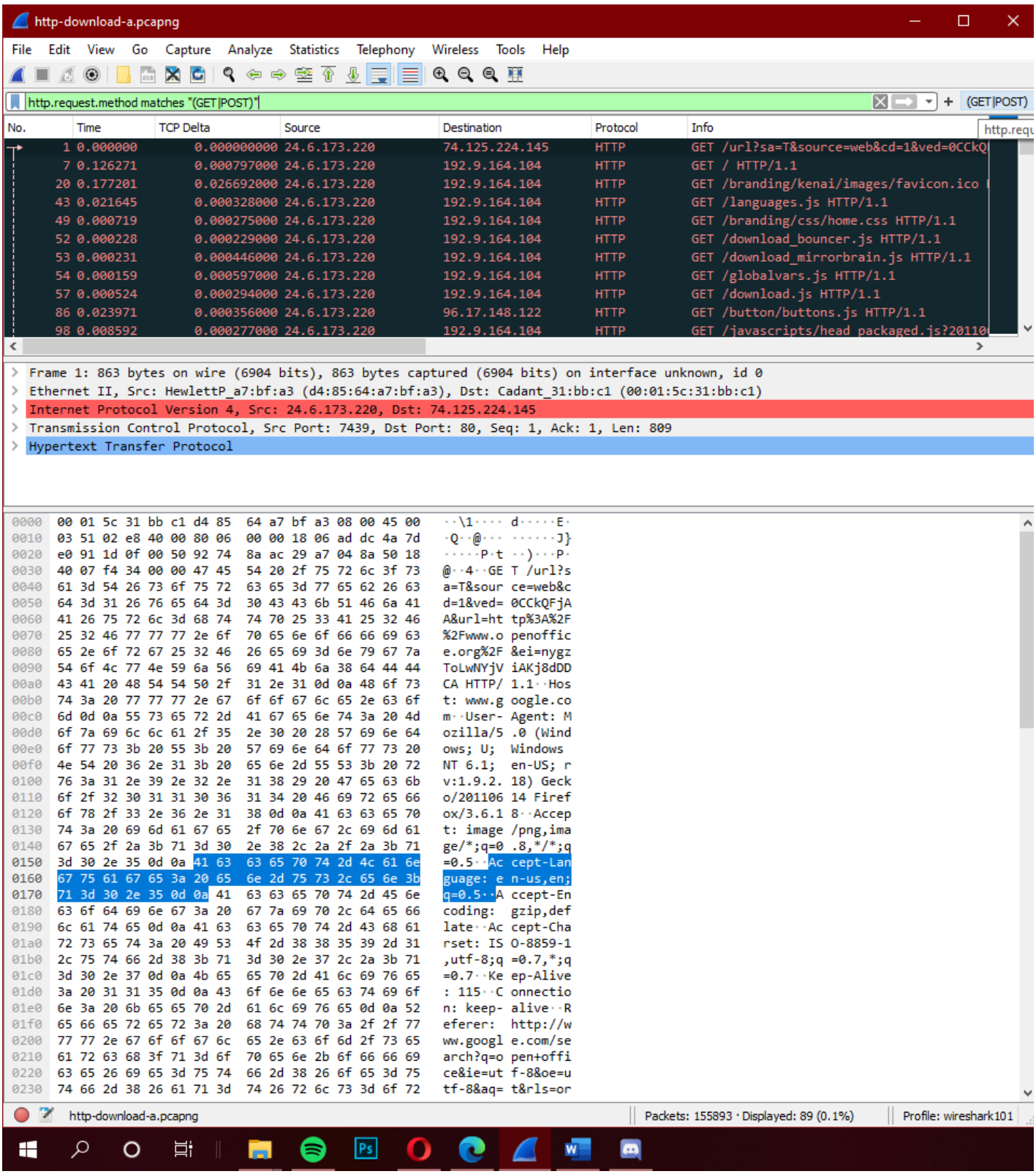
Lab24- Create and Import HTTP Filter Expression Buttons



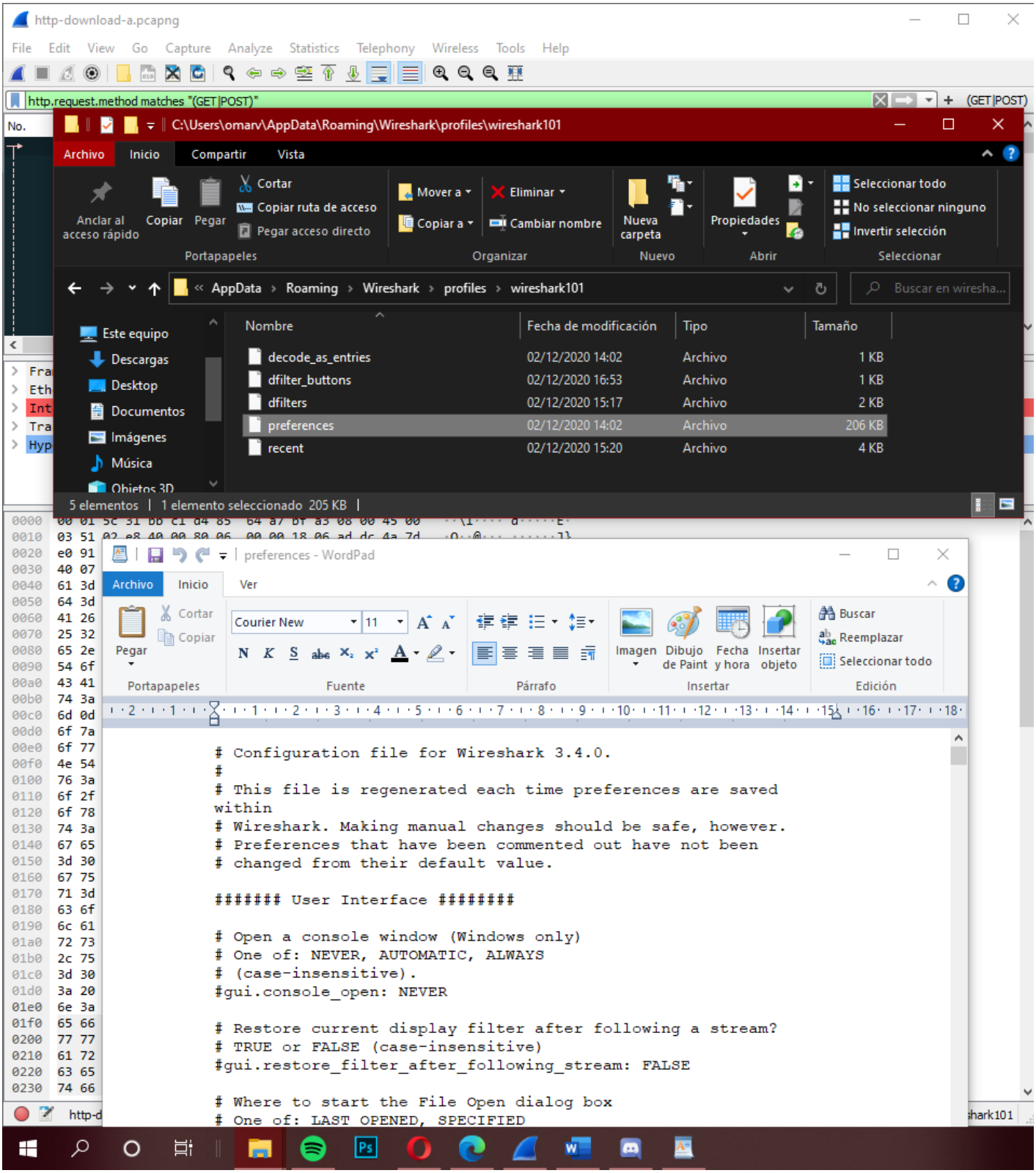
PASO 2:


http-download-a.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Filter Buttons Preferences...
Label: (GET|POST)
Filter: http.request.method matches "(GET|POST)"
OK
Cancel
Comment: Enter a comment for the filter button
No. Time TCP Delta Source Destination Protocol Info
1 0.000000 0.000000000 24.6.173.220 74.125.224.145 HTTP GET /url?sa=T&source=web&cd=1&ved=0CCkQ
2 0.015318 0.015318000 74.125.224.145 24.6.173.220 TCP 80 → 7439 [ACK] Seq=1 Ack=810 Win=172
3 0.022554 0.022554000 74.125.224.145 24.6.173.220 HTTP HTTP/1.1 204 No Content
4 0.071526 0.000000000 24.6.173.220 192.9.164.104 TCP 7446 → 80 [SYN] Seq=0 Win=8192 Len=0 MS
5 0.015910 0.015910000 192.9.164.104 24.6.173.220 TCP 80 → 7446 [SYN, ACK] Seq=0 Ack=1 Win=49
6 0.000166 0.000166000 24.6.173.220 192.9.164.104 TCP 7446 → 80 [ACK] Seq=1 Ack=1 Win=65700
7 0.000797 0.000797000 24.6.173.220 192.9.164.104 HTTP GET / HTTP/1.1
8 0.020988 0.020988000 192.9.164.104 24.6.173.220 TCP 80 → 7446 [ACK] Seq=1 Ack=499 Win=49640
9 0.091838 0.201225000 24.6.173.220 74.125.224.145 TCP 7439 → 80 [ACK] Seq=810 Ack=270 Win=163
10 0.010355 0.102193000 192.9.164.104 24.6.173.220 HTTP HTTP/1.1 200 OK (text/html)
Frame 1: 863 bytes on wire (6904 bits), 863 bytes captured (6904 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: 74.125.224.145
Transmission Control Protocol, Src Port: 7439, Dst Port: 80, Seq: 1, Ack: 1, Len: 809
Hypertext Transfer Protocol
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ··\1···· d·····E·
0010 03 51 02 e8 40 00 80 06 00 00 18 06 ad dc 4a 7d ·Q··@··· ·····J}
0020 e0 91 1d 0f 00 50 92 74 8a ac 29 a7 04 8a 50 18 ·····P·t ··)···P·
0030 40 07 f4 34 00 00 47 45 54 20 2f 75 72 6c 3f 73 @··4··GE T /url?s
0040 61 3d 54 26 73 6f 75 72 63 65 3d 77 65 62 26 63 a=T&sour ce=web&c
0050 64 3d 31 26 76 65 64 3d 30 43 43 6b 51 46 6a 41 d=1&ved= 0CCkQFjA
0060 41 26 75 72 6c 3d 68 74 74 70 25 33 41 25 32 46 A&url=ht tp%3A%2F
0070 25 32 46 77 77 77 2e 6f 70 65 6e 6f 66 66 69 63 %2Fwww.o penoffic
0080 65 2e 6f 72 67 25 32 46 26 65 69 3d 6e 79 67 7a e.org%2F &ei=nygz
0090 54 6f 4c 77 4e 59 6a 56 69 41 4b 6a 38 64 44 44 ToLwNYjV iAKj8dDD
00a0 43 41 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 CA HTTP/ 1.1··Hos
00b0 74 3a 20 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f t: www.g oogle.co
00c0 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d m··User- Agent: M
00d0 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 ozilla/5 .0 (Wind
00e0 6f 77 73 3b 20 55 3b 20 57 69 6e 64 6f 77 73 20 ows; U; Windows
00f0 4e 54 20 36 2e 31 3b 20 65 6e 2d 55 53 3b 20 72 NT 6.1; en-US; r
0100 76 3a 31 2e 39 2e 32 2e 31 38 29 20 47 65 63 6b v:1.9.2. 18) Geck
0110 6f 2f 32 30 31 31 30 36 31 34 20 46 69 72 65 66 o/201106 14 Firef
0120 6f 78 2f 33 2e 36 2e 31 38 0d 0a 41 63 63 65 70 ox/3.6.1 8··Accep
0130 74 3a 20 69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 t: image /png,ima
0140 67 65 2f 2a 3b 71 3d 30 2e 38 2c 2a 2f 2a 3b 71 ge/*;q=0 .8,*/*;q
0150 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 4c 61 6e =0.5··Ac cept-Lan
0160 67 75 61 67 65 3a 20 65 6e 2d 75 73 2c 65 6e 3b guage: e n-us,en;
0170 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e q=0.5··A ccept-En
0180 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 64 65 66 coding: gzip,def
0190 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d 43 68 61 late··Ac cept-Cha
01a0 72 73 65 74 3a 20 49 53 4f 2d 38 38 35 39 2d 31 rset: IS O-8859-1
01b0 2c 75 74 66 2d 38 3b 71 3d 30 2e 37 2c 2a 3b 71 ,utf-8;q =0.7,*;q
01c0 3d 30 2e 37 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 =0.7··Ke ep-Alive
01d0 3a 20 31 31 35 0d 0a 43 6f 6e 6e 65 63 74 69 6f : 115··C onnectio
01e0 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 52 n: keep- alive··R
01f0 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 77 eferer: http://w
0200 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 73 65 ww.googl e.com/se
http-download-a.pcapng
Packets: 155893 · Displayed: 155893 (100.0%)
Profile: wireshark101

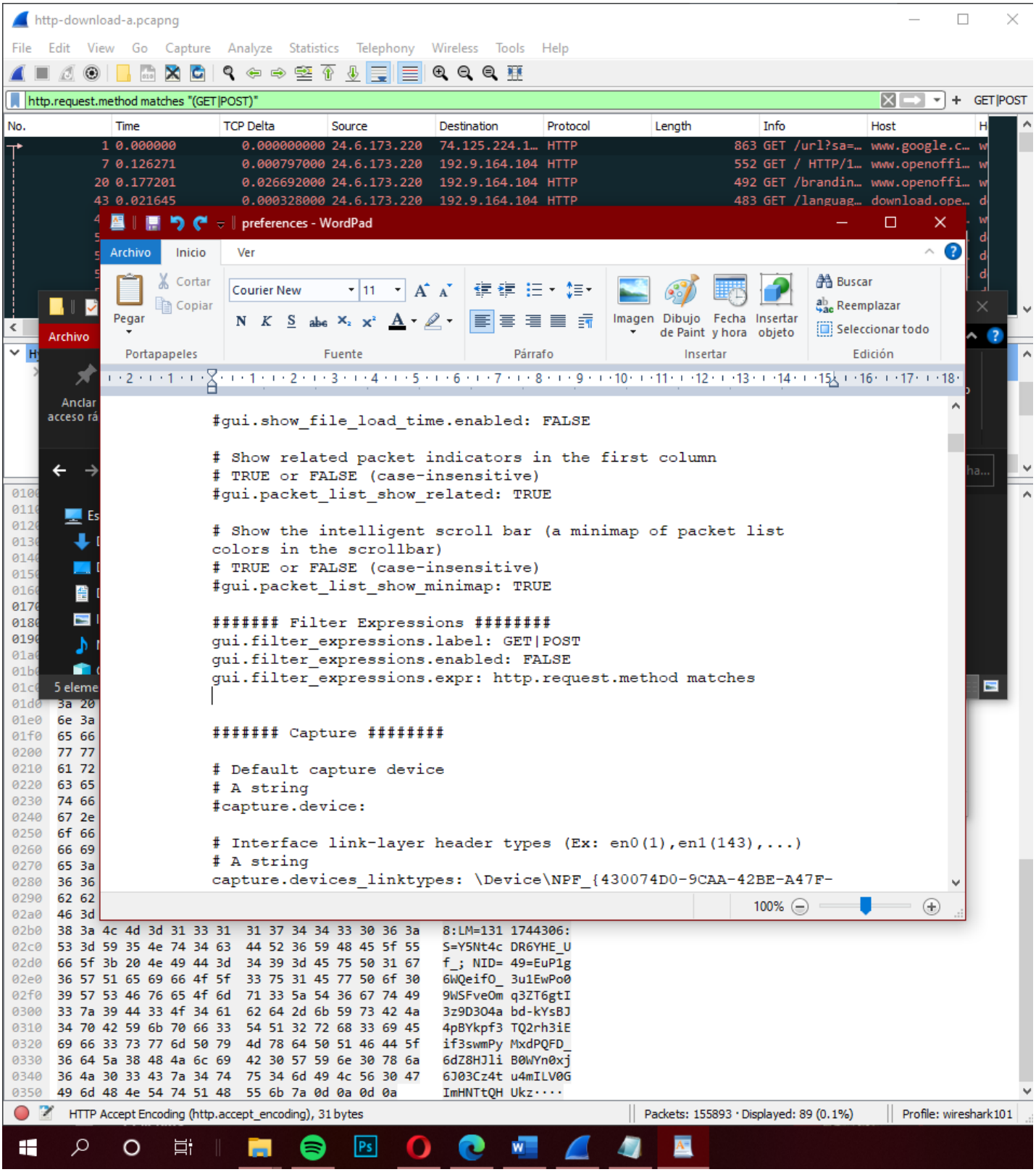
Paso 3:


http-download-a.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method matches "(GET|POST)"
(GET|POST)
No. Time TCP Delta Source Destination Protocol Info
1 0.000000 0.000000000 24.6.173.220 74.125.224.145 HTTP GET /url?sa=T&source=web&cd=1&ved=0CCkQ
7 0.126271 0.000797000 24.6.173.220 192.9.164.104 HTTP GET / HTTP/1.1
20 0.177201 0.026692000 24.6.173.220 192.9.164.104 HTTP GET /branding/kenai/images/favicon.ico
43 0.021645 0.000328000 24.6.173.220 192.9.164.104 HTTP GET /languages.js HTTP/1.1
49 0.000719 0.000275000 24.6.173.220 192.9.164.104 HTTP GET /branding/css/home.css HTTP/1.1
52 0.000228 0.000229000 24.6.173.220 192.9.164.104 HTTP GET /download_bouncer.js HTTP/1.1
53 0.000231 0.000446000 24.6.173.220 192.9.164.104 HTTP GET /download_mirrorbrain.js HTTP/1.1
54 0.000159 0.000597000 24.6.173.220 192.9.164.104 HTTP GET /globalvars.js HTTP/1.1
57 0.000524 0.000294000 24.6.173.220 192.9.164.104 HTTP GET /download.js HTTP/1.1
86 0.023971 0.000356000 24.6.173.220 96.17.148.122 HTTP GET /button/buttons.js HTTP/1.1
98 0.008592 0.000277000 24.6.173.220 192.9.164.104 HTTP GET /javascripts/head_packaged.js?20110
Frame 1: 863 bytes on wire (6904 bits), 863 bytes captured (6904 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: 74.125.224.145
Transmission Control Protocol, Src Port: 7439, Dst Port: 80, Seq: 1, Ack: 1, Len: 809
Hypertext Transfer Protocol
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00 ··\1···· d·····E·
0010 03 51 02 e8 40 00 80 06 00 00 18 06 ad dc 4a 7d ·Q··@··· ·····J}
0020 e0 91 1d 0f 00 50 92 74 8a ac 29 a7 04 8a 50 18 ·····P·t ··)···P·
0030 40 07 f4 34 00 00 47 45 54 20 2f 75 72 6c 3f 73 @··4··GE T /url?s
0040 61 3d 54 26 73 6f 75 72 63 65 3d 77 65 62 26 63 a=T&sour ce=web&c
0050 64 3d 31 26 76 65 64 3d 30 43 43 6b 51 46 6a 41 d=1&ved= 0CCkQFjA
0060 41 26 75 72 6c 3d 68 74 74 70 25 33 41 25 32 46 A&url=ht tp%3A%2F
0070 25 32 46 77 77 77 2e 6f 70 65 6e 6f 66 66 69 63 %2Fwww.o penoffic
0080 65 2e 6f 72 67 25 32 46 26 65 69 3d 6e 79 67 7a e.org%2F &ei=nygz
0090 54 6f 4c 77 4e 59 6a 56 69 41 4b 6a 38 64 44 44 ToLwNYjV iAKj8dDD
00a0 43 41 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 CA HTTP/ 1.1··Hos
00b0 74 3a 20 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f t: www.g oogle.co
00c0 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d m··User- Agent: M
00d0 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 ozilla/5 .0 (Wind
00e0 6f 77 73 3b 20 55 3b 20 57 69 6e 64 6f 77 73 20 ows; U; Windows
00f0 4e 54 20 36 2e 31 3b 20 65 6e 2d 55 53 3b 20 72 NT 6.1; en-US; r
0100 76 3a 31 2e 39 2e 32 2e 31 38 29 20 47 65 63 6b v:1.9.2. 18) Geck
0110 6f 2f 32 30 31 31 30 36 31 34 20 46 69 72 65 66 o/201106 14 Firef
0120 6f 78 2f 33 2e 36 2e 31 38 0d 0a 41 63 63 65 70 ox/3.6.1 8··Accep
0130 74 3a 20 69 6d 61 67 65 2f 70 6e 67 2c 69 6d 61 t: image /png,ima
0140 67 65 2f 2a 3b 71 3d 30 2e 38 2c 2a 2f 2a 3b 71 ge/*;q=0 .8,*/*;q
0150 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 4c 61 6e =0.5··Ac cept-Lan
0160 67 75 61 67 65 3a 20 65 6e 2d 75 73 2c 65 6e 3b guage: e n-us,en;
0170 71 3d 30 2e 35 0d 0a 41 63 63 65 70 74 2d 45 6e q=0.5··A ccept-En
0180 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c 64 65 66 coding: gzip,def
0190 6c 61 74 65 0d 0a 41 63 63 65 70 74 2d 43 68 61 late··Ac cept-Cha
01a0 72 73 65 74 3a 20 49 53 4f 2d 38 38 35 39 2d 31 rset: IS O-8859-1
01b0 2c 75 74 66 2d 38 3b 71 3d 30 2e 37 2c 2a 3b 71 ,utf-8;q =0.7,*;q
01c0 3d 30 2e 37 0d 0a 4b 65 65 70 2d 41 6c 69 76 65 =0.7··Ke ep-Alive
01d0 3a 20 31 31 35 0d 0a 43 6f 6e 6e 65 63 74 69 6f : 115··C onnectio
01e0 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 52 n: keep- alive··R
01f0 65 66 65 72 65 72 3a 20 68 74 74 70 3a 2f 2f 77 eferer: http://w
0200 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 73 65 ww.googl e.com/se
0210 61 72 63 68 3f 71 3d 6f 70 65 6e 2b 6f 66 66 69 arch?q=o pen+offi
0220 63 65 26 69 65 3d 75 74 66 2d 38 26 6f 65 3d 75 ce&ie=ut f-8&oe=u
0230 74 66 2d 38 26 61 71 3d 74 26 72 6c 73 3d 6f 72 tf-8&aq= t&rls=or
http-download-a.pcapng
Packets: 155893 · Displayed: 89 (0.1%)
Profile: wireshark101

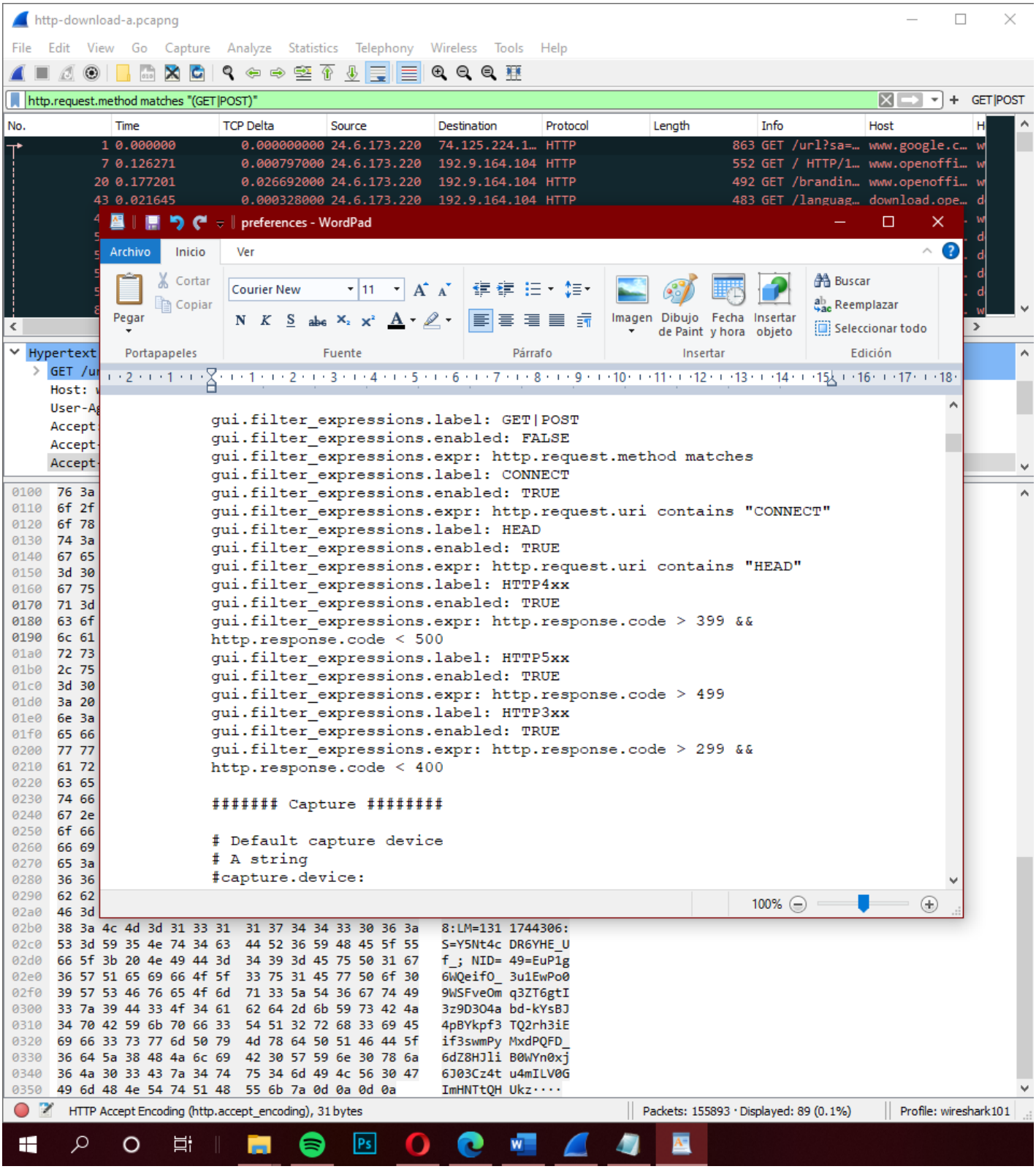
Paso 4:


http-download-a.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method matches "(GET|POST)"
C:\Users\omarv\AppData\Roaming\Wireshark\profiles\wireshark101
Archivo Inicio Compartir Vista
AppData › Roaming › Wireshark › profiles › wireshark101
Nombre Fecha de modificación Tipo Tamaño
decode_as_entries 02/12/2020 14:02 Archivo 1 KB
dfilter_buttons 02/12/2020 16:53 Archivo 1 KB
dfilters 02/12/2020 15:17 Archivo 2 KB
preferences 02/12/2020 14:02 Archivo 206 KB
recent 02/12/2020 15:20 Archivo 4 KB
5 elementos | 1 elemento seleccionado 205 KB
preferences - WordPad
Configuration file for Wireshark 3.4.0.
#
This file is regenerated each time preferences are saved within
Wireshark. Making manual changes should be safe, however.
Preferences that have been commented out have not been
changed from their default value.
####### User Interface ########
Open a console window (Windows only)
One of: NEVER, AUTOMATIC, ALWAYS
(case-insensitive).
#gui.console_open: NEVER
Restore current display filter after following a stream?
TRUE or FALSE (case-insensitive)
#gui.restore_filter_after_following_stream: FALSE
Where to start the File Open dialog box
One of: LAST_OPENED, SPECIFIED

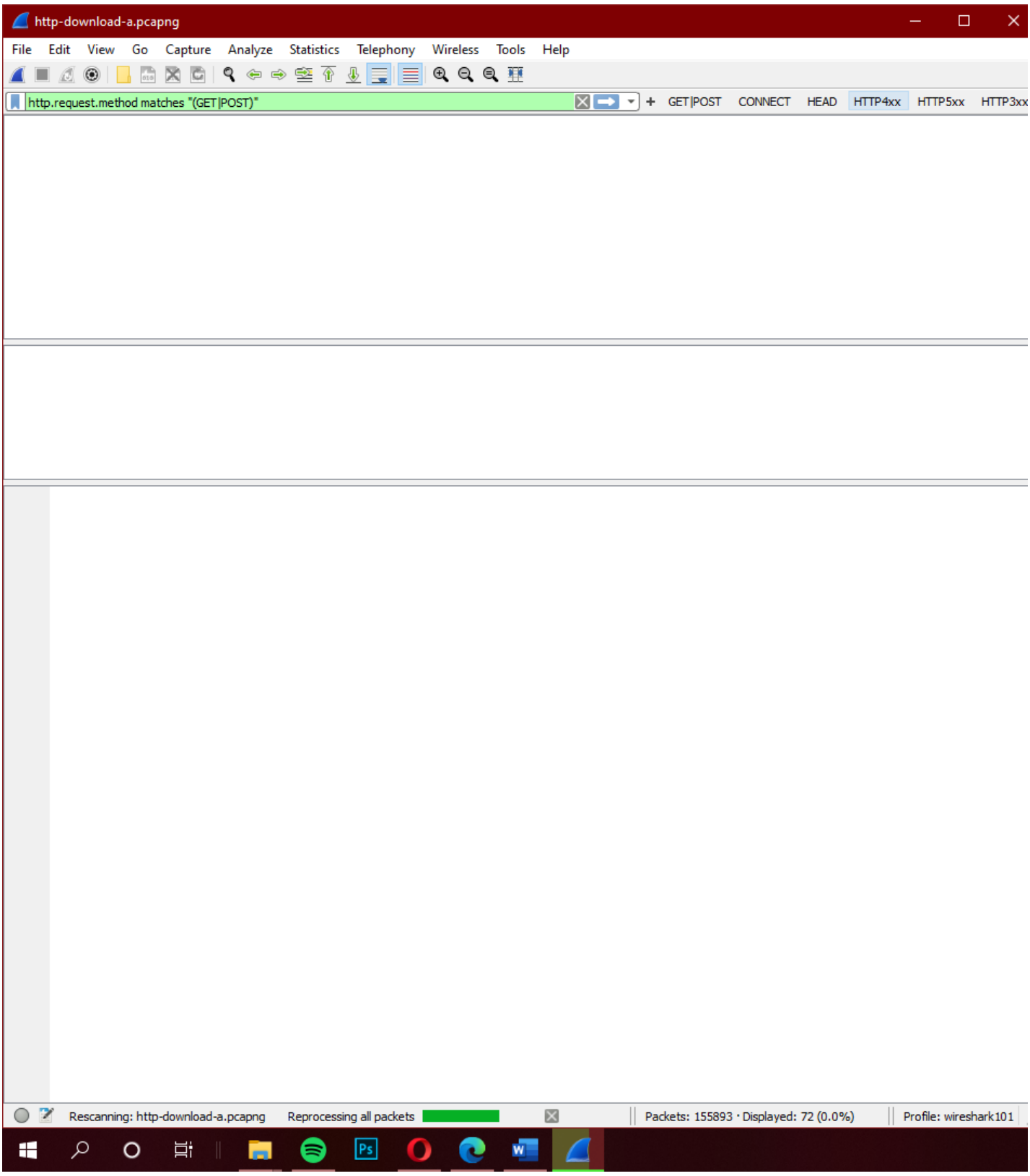
Paso 5:


http-download-a.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method matches "(GET|POST)"
GET|POST
No. Time TCP Delta Source Destination Protocol Length Info Host
1 0.000000 0.000000000 24.6.173.220 74.125.224.1… HTTP 863 GET /url?sa=… www.google.c…
7 0.126271 0.000797000 24.6.173.220 192.9.164.104 HTTP 552 GET / HTTP/1… www.openoffi…
20 0.177201 0.026692000 24.6.173.220 192.9.164.104 HTTP 492 GET /brandin… www.openoffi…
43 0.021645 0.000328000 24.6.173.220 192.9.164.104 HTTP 483 GET /languag… download.ope…
preferences - WordPad
Archivo Inicio Ver
Pegar Cortar Copiar
Courier New 11
Portapapeles Fuente Párrafo Insertar Edición
Imagen Dibujo de Paint Fecha y hora Insertar objeto
Buscar Reemplazar Seleccionar todo
#gui.show_file_load_time.enabled: FALSE
Show related packet indicators in the first column
TRUE or FALSE (case-insensitive)
#gui.packet_list_show_related: TRUE
Show the intelligent scroll bar (a minimap of packet list
colors in the scrollbar)
TRUE or FALSE (case-insensitive)
#gui.packet_list_show_minimap: TRUE
####### Filter Expressions ########
gui.filter_expressions.label: GET|POST
gui.filter_expressions.enabled: FALSE
gui.filter_expressions.expr: http.request.method matches
####### Capture ########
Default capture device
A string
#capture.device:
Interface link-layer header types (Ex: en0(1),en1(143),...)
A string
capture.devices_linktypes: \Device\NPF_{430074D0-9CAA-42BE-A47F-
100%
02b0 38 3a 4c 4d 3d 31 33 31 31 37 34 34 33 30 36 3a 8:LM=131 1744306:
02c0 53 3d 59 35 4e 74 34 63 44 52 36 59 48 45 5f 55 S=Y5Nt4c DR6YHE_U
02d0 66 5f 3b 20 4e 49 44 3d 34 39 3d 45 75 50 31 67 f_; NID= 49=EuP1g
02e0 36 57 51 65 69 66 4f 5f 33 75 31 45 77 50 6f 30 6WQeifO_ 3u1EwPo0
02f0 39 57 53 46 76 65 4f 6d 71 33 5a 54 36 67 74 49 9WSFveOm q3ZT6gtI
0300 33 7a 39 44 33 4f 34 61 62 64 2d 6b 59 73 42 4a 3z9D3O4a bd-kYsBJ
0310 34 70 42 59 6b 70 66 33 54 51 32 72 68 33 69 45 4pBYkpf3 TQ2rh3iE
0320 69 66 33 73 77 6d 50 79 4d 78 64 50 51 46 44 5f if3swmPy MxdPQFD_
0330 36 64 5a 38 48 4a 6c 69 42 30 57 59 6e 30 78 6a 6dZ8HJli B0WYn0xj
0340 36 4a 30 33 43 7a 34 74 75 34 6d 49 4c 56 30 47 6J03Cz4t u4mILV0G
0350 49 6d 48 4e 54 74 51 48 55 6b 7a 0d 0a 0d 0a ImHNTtQH Ukz····
HTTP Accept Encoding (http.accept_encoding), 31 bytes
Packets: 155893 · Displayed: 89 (0.1%)
Profile: wireshark101

Paso 6:


http-download-a.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method matches "(GET|POST)"
GET|POST
No. Time TCP Delta Source Destination Protocol Length Info Host
1 0.000000 0.000000000 24.6.173.220 74.125.224.1… HTTP 863 GET /url?sa=… www.google.c…
7 0.126271 0.000797000 24.6.173.220 192.9.164.104 HTTP 552 GET / HTTP/1… www.openoffi…
20 0.177201 0.026692000 24.6.173.220 192.9.164.104 HTTP 492 GET /brandin… www.openoffi…
43 0.021645 0.000328000 24.6.173.220 192.9.164.104 HTTP 483 GET /languag… download.ope…
preferences - WordPad
Archivo Inicio Ver
Pegar Cortar Copiar
Courier New 11
Portapapeles Fuente Párrafo Insertar Edición
Imagen Dibujo de Paint Fecha y hora Insertar objeto
Buscar Reemplazar Seleccionar todo
gui.filter_expressions.label: GET|POST
gui.filter_expressions.enabled: FALSE
gui.filter_expressions.expr: http.request.method matches
gui.filter_expressions.label: CONNECT
gui.filter_expressions.enabled: TRUE
gui.filter_expressions.expr: http.request.uri contains "CONNECT"
gui.filter_expressions.label: HEAD
gui.filter_expressions.enabled: TRUE
gui.filter_expressions.expr: http.request.uri contains "HEAD"
gui.filter_expressions.label: HTTP4xx
gui.filter_expressions.enabled: TRUE
gui.filter_expressions.expr: http.response.code > 399 &&
http.response.code < 500
gui.filter_expressions.label: HTTP5xx
gui.filter_expressions.enabled: TRUE
gui.filter_expressions.expr: http.response.code > 499
gui.filter_expressions.label: HTTP3xx
gui.filter_expressions.enabled: TRUE
gui.filter_expressions.expr: http.response.code > 299 &&
http.response.code < 400
####### Capture ########
Default capture device
A string
#capture.device:
100%
HTTP Accept Encoding (http.accept_encoding), 31 bytes
Packets: 155893 · Displayed: 89 (0.1%)
Profile: wireshark101

Paso 7:


http-download-a.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method matches "(GET|POST)"
GET|POST CONNECT HEAD HTTP4xx HTTP5xx HTTP3xx
Rescanning: http-download-a.pcapng
Reprocessing all packets
Packets: 155893 · Displayed: 72 (0.0%)
Profile: wireshark101