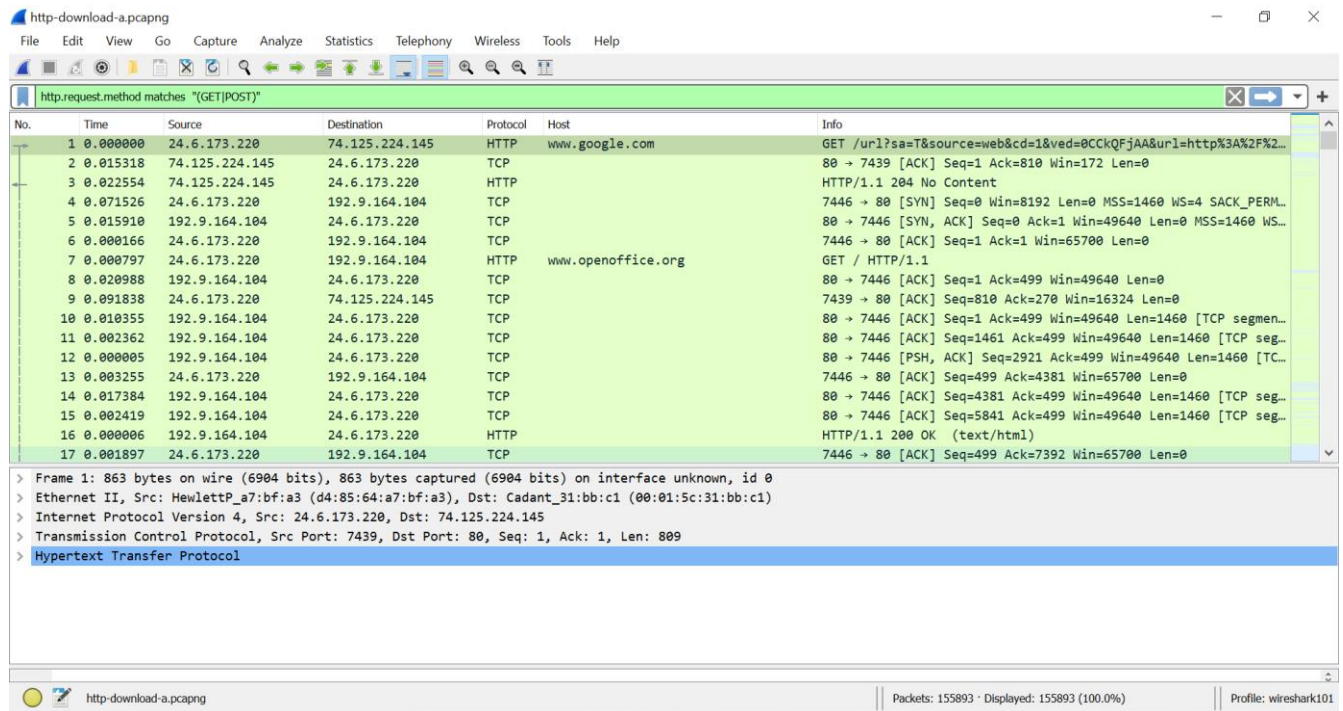


## Lab 24

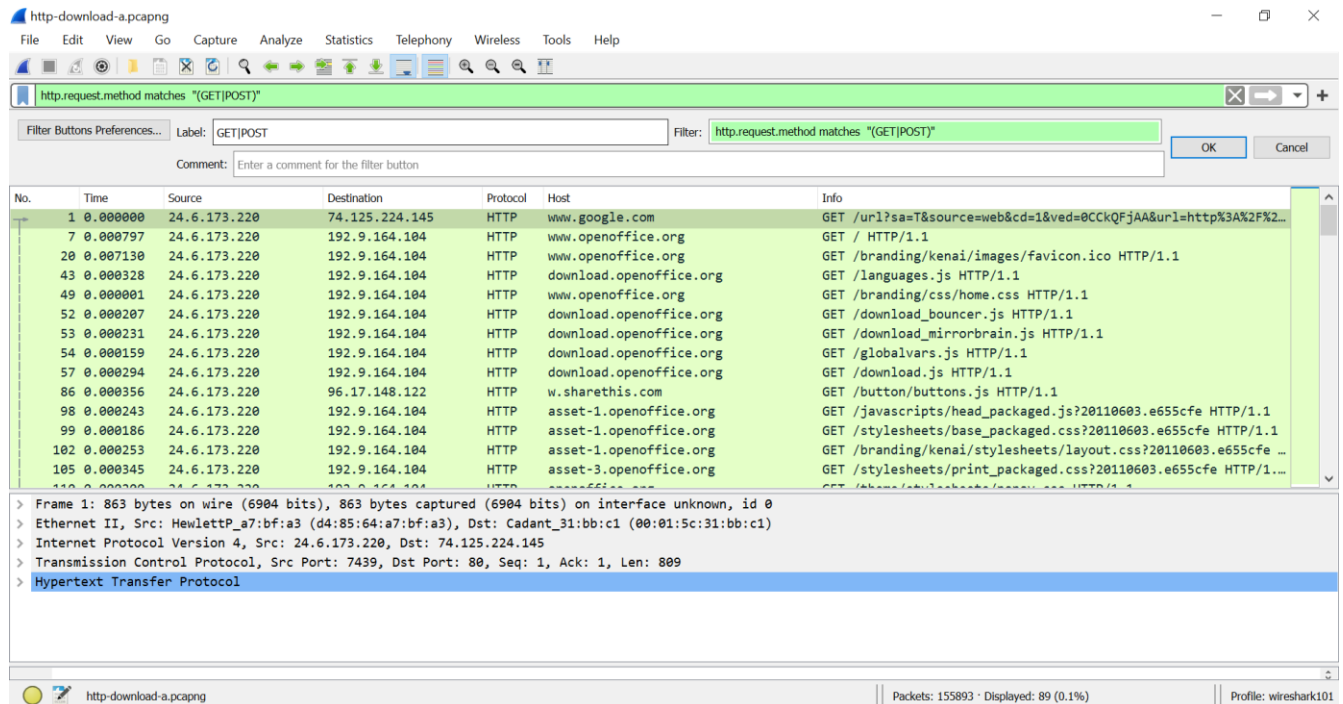
Abriremos el archivo `http-download-a.pcapng` y aplicaremos el filtro `http.request.method matches "(GET|POST)"`



The screenshot shows the Wireshark interface with the file `http-download-a.pcapng` open. The filter bar at the top displays `http.request.method matches "(GET|POST)"`. The packet list shows 17 packets, all of which are HTTP requests (GET or POST) to `www.google.com` and `www.openoffice.org`. The packet details pane shows the selected packet (No. 1) with its structure: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

No.	Time	Source	Destination	Protocol	Host	Info
1	0.000000	24.6.173.220	74.125.224.145	HTTP	www.google.com	GET /url?sa=T&source=web&cd=1&ved=0CCKQFjAA&url=http%3A%2F%2F...
2	0.015318	74.125.224.145	24.6.173.220	TCP		80 → 7439 [ACK] Seq=1 Ack=810 Win=172 Len=0
3	0.022554	74.125.224.145	24.6.173.220	HTTP		HTTP/1.1 204 No Content
4	0.071526	24.6.173.220	192.9.164.104	TCP		7446 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM...
5	0.015910	192.9.164.104	24.6.173.220	TCP		80 → 7446 [SYN, ACK] Seq=0 Ack=1 Win=49640 Len=0 MSS=1460 WS...
6	0.000166	24.6.173.220	192.9.164.104	TCP		7446 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
7	0.000797	24.6.173.220	192.9.164.104	HTTP	www.openoffice.org	GET / HTTP/1.1
8	0.020988	192.9.164.104	24.6.173.220	TCP		80 → 7446 [ACK] Seq=1 Ack=499 Win=49640 Len=0
9	0.091838	24.6.173.220	74.125.224.145	TCP		7439 → 80 [ACK] Seq=810 Ack=270 Win=16324 Len=0
10	0.010355	192.9.164.104	24.6.173.220	TCP		80 → 7446 [ACK] Seq=1 Ack=499 Win=49640 Len=1460 [TCP segmen...
11	0.002362	192.9.164.104	24.6.173.220	TCP		80 → 7446 [ACK] Seq=1461 Ack=499 Win=49640 Len=1460 [TCP seg...
12	0.000005	192.9.164.104	24.6.173.220	TCP		80 → 7446 [PSH, ACK] Seq=2921 Ack=499 Win=49640 Len=1460 [TC...
13	0.003255	24.6.173.220	192.9.164.104	TCP		7446 → 80 [ACK] Seq=499 Ack=4381 Win=65700 Len=0
14	0.017384	192.9.164.104	24.6.173.220	TCP		80 → 7446 [ACK] Seq=4381 Ack=499 Win=49640 Len=1460 [TCP seg...
15	0.002419	192.9.164.104	24.6.173.220	TCP		80 → 7446 [ACK] Seq=5841 Ack=499 Win=49640 Len=1460 [TCP seg...
16	0.000006	192.9.164.104	24.6.173.220	HTTP		HTTP/1.1 200 OK (text/html)
17	0.001897	24.6.173.220	192.9.164.104	TCP		7446 → 80 [ACK] Seq=499 Ack=7392 Win=65700 Len=0

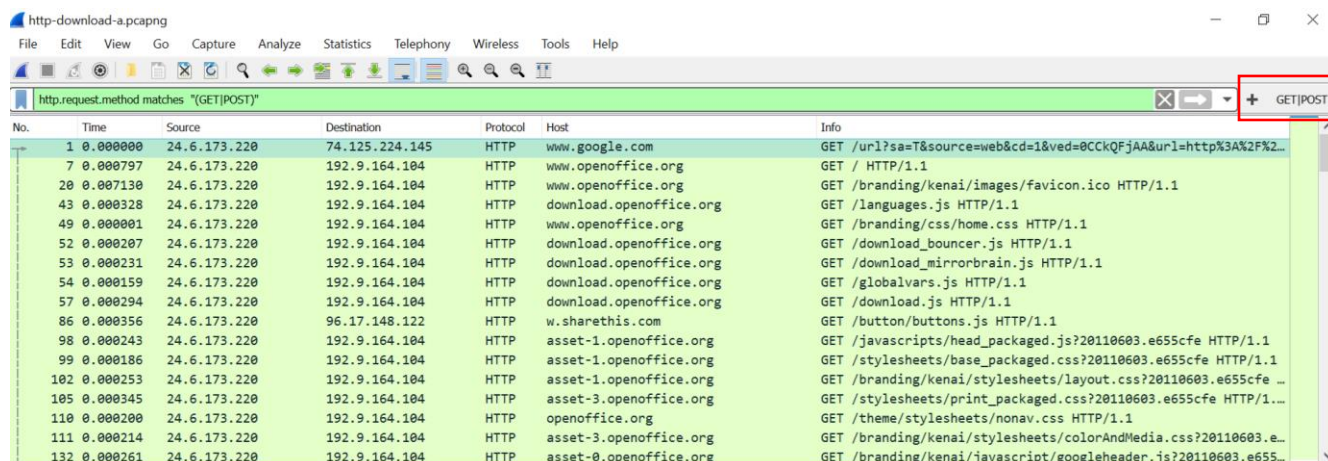
Dándole clic en el botón de + agregaremos una etiqueta llamada GET|POST



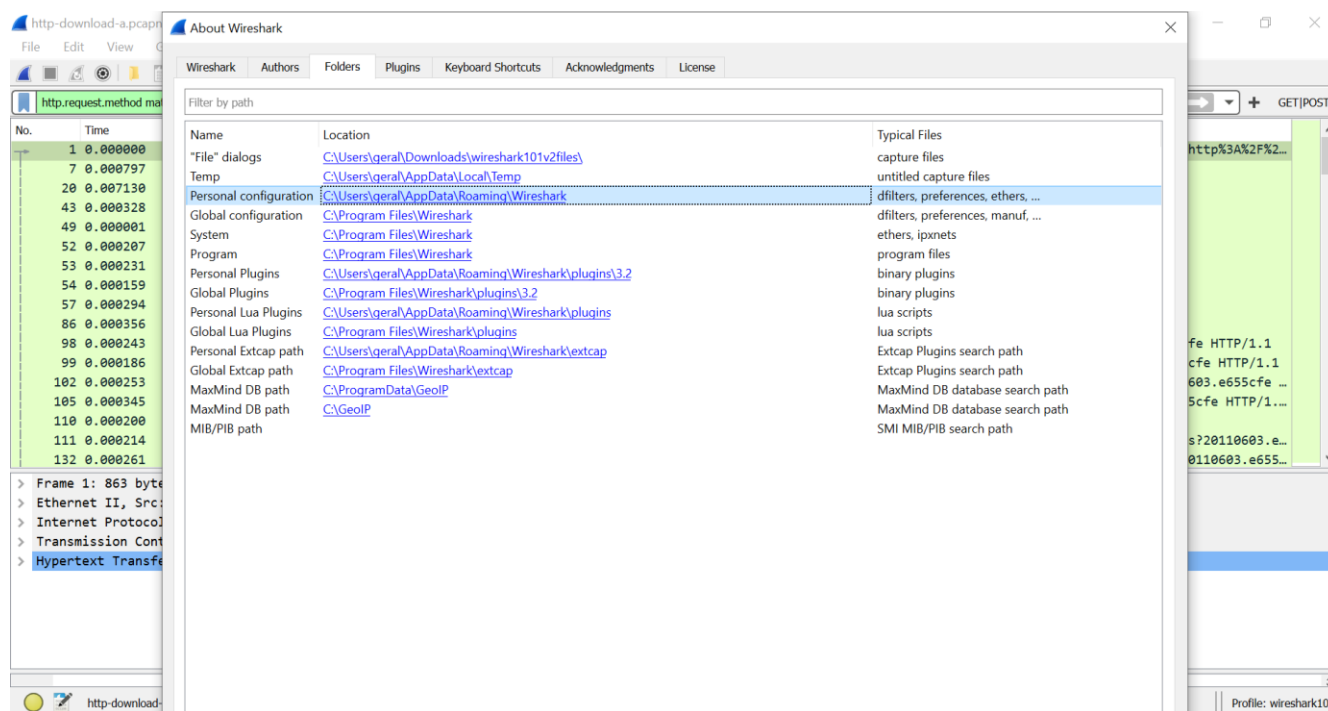
The screenshot shows the Wireshark interface with the file `http-download-a.pcapng` open. The filter bar at the top displays `http.request.method matches "(GET|POST)"`. A new filter button labeled `GET|POST` has been added to the filter bar. The packet list shows 105 packets, all of which are HTTP requests (GET or POST) to `www.google.com` and `www.openoffice.org`. The packet details pane shows the selected packet (No. 1) with its structure: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.

No.	Time	Source	Destination	Protocol	Host	Info
1	0.000000	24.6.173.220	74.125.224.145	HTTP	www.google.com	GET /url?sa=T&source=web&cd=1&ved=0CCKQFjAA&url=http%3A%2F%2F...
7	0.000797	24.6.173.220	192.9.164.104	HTTP	www.openoffice.org	GET / HTTP/1.1
20	0.007130	24.6.173.220	192.9.164.104	HTTP	www.openoffice.org	GET /branding/kenai/images/favicon.ico HTTP/1.1
43	0.000328	24.6.173.220	192.9.164.104	HTTP	download.openoffice.org	GET /languages.js HTTP/1.1
49	0.000001	24.6.173.220	192.9.164.104	HTTP	www.openoffice.org	GET /branding/css/home.css HTTP/1.1
52	0.000207	24.6.173.220	192.9.164.104	HTTP	download.openoffice.org	GET /download_bouncer.js HTTP/1.1
53	0.000231	24.6.173.220	192.9.164.104	HTTP	download.openoffice.org	GET /download_mirrorbrain.js HTTP/1.1
54	0.000159	24.6.173.220	192.9.164.104	HTTP	download.openoffice.org	GET /globalvars.js HTTP/1.1
57	0.000294	24.6.173.220	192.9.164.104	HTTP	download.openoffice.org	GET /download.js HTTP/1.1
86	0.000356	24.6.173.220	96.17.148.122	HTTP	w.sharethis.com	GET /button/buttons.js HTTP/1.1
98	0.000243	24.6.173.220	192.9.164.104	HTTP	asset-1.openoffice.org	GET /javascripts/head_packaged.js?20110603.e655cfe HTTP/1.1
99	0.000186	24.6.173.220	192.9.164.104	HTTP	asset-1.openoffice.org	GET /stylesheets/base_packaged.css?20110603.e655cfe HTTP/1.1
102	0.000253	24.6.173.220	192.9.164.104	HTTP	asset-1.openoffice.org	GET /branding/kenai/stylesheets/layout.css?20110603.e655cfe ...
105	0.000345	24.6.173.220	192.9.164.104	HTTP	asset-3.openoffice.org	GET /stylesheets/print_packaged.css?20110603.e655cfe HTTP/1.1

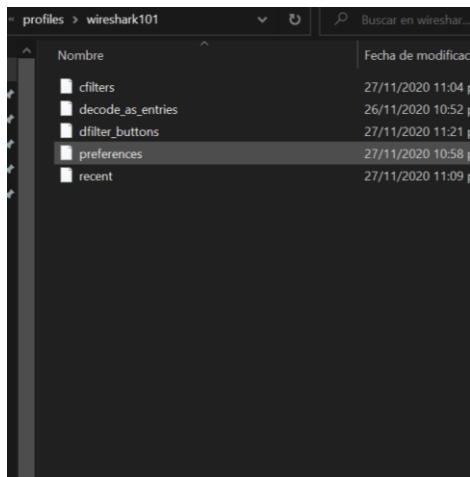
Nos aparecerá de la siguiente manera y daremos clic en ese mismo



Iremos a Help > Folders y dos clics para abrir personal configuration



Dentro del explorador de archivos en la carpeta de wireshark101 abriremos con bloc de notas “preferences”



```
preferences: Bloc de notas
Archivo Edici3n Formato Ver Ayuda
# Configuration file for Wireshark 3.2.4.
#
# 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
# (case-insensitive).
#gui.fileopen.style: LAST_OPENED
# The max. number of items in the open recent files list
# A decimal number
gui.recent_files_count.max: 30
# The max. number of entries in the display filter list
# A decimal number
gui.recent_display_filter_entries.max: 30
# Directory to start in when opening File Open dialog.
# A path to a directory
#gui.fileopen_dir: C:\Users\user\OneDrive\Documents
```

Bajamos hasta esta sección

```
*preferences: Bloc de notas
Archivo Edición Formato Ver Ayuda
#gui.packet_header_column_definition.enabled: TRUE

# Show selected packet in the Status Bar
# TRUE or FALSE (case-insensitive)
#gui.show_selected_packet.enabled: FALSE

# Show file load time in the Status Bar
# TRUE or FALSE (case-insensitive)
#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 scrollbar (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
"(GET|POST)"

##### 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_{A0EB9880-DE32-44D9-AFD3-B0827BF3E77E}(0),\Device\NPF
```

Buscaremos el archivo ***filterexpressions101.txt*** que se descargó de la pagina de [www.wiresharkbook.com](http://www.wiresharkbook.com) y copiaremos el contenido y lo pegaremos debajo de la sección encontrada previamente, guardamos el archivo y cerramos.

```
*preferences: Bloc de notas
Archivo Edición Formato Ver Ayuda
# TRUE or FALSE (case-insensitive)
#gui.packet_list_show_minimap: TRUE

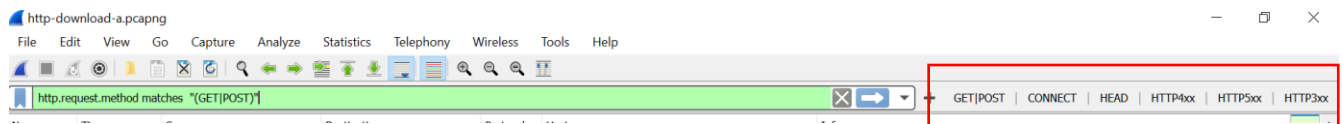
##### Filter Expressions #####
gui.filter_expressions.label: GET|POST
gui.filter_expressions.enabled: False
gui.filter_expressions.expr: http.request.method matches
"(GET|POST)"
gui.filter_expressions.label: CONNECT
gui.filter_expressions.enabled: TRUE
gui.filter_expressions.expr: http.request.uri contains "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 #####
```

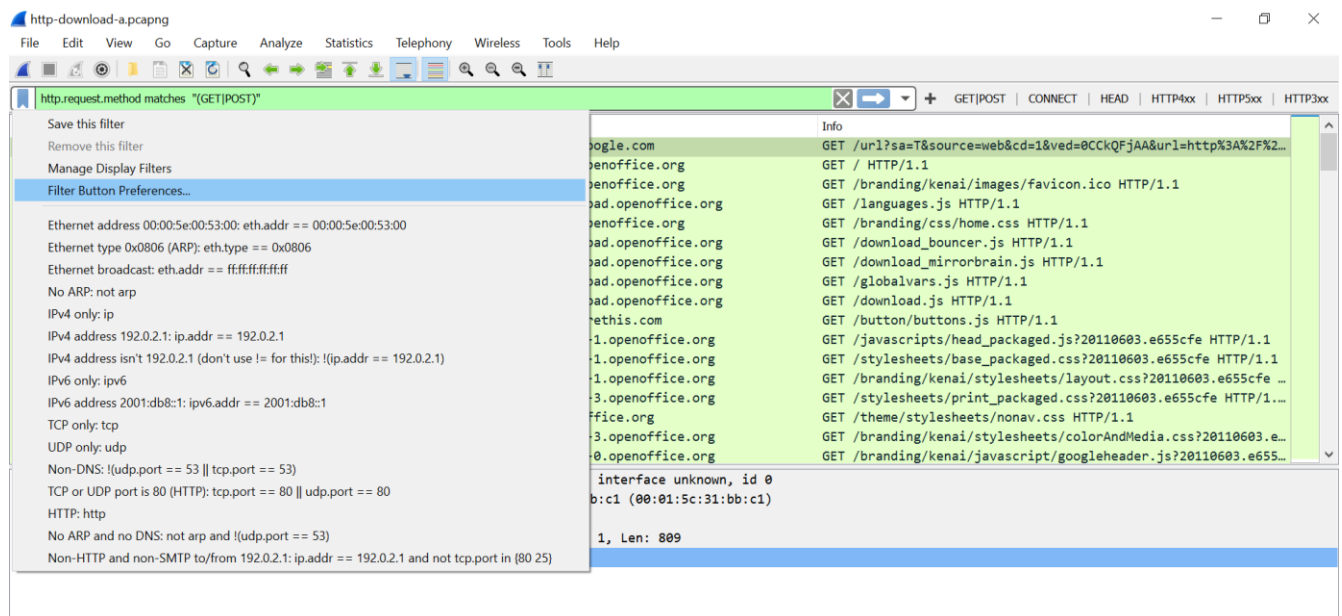
Dentro de wireshark cambiaremos el perfil a default, después cambiaremos nuevamente al perfil wireshark101, esto para que carguen las nuevas configuraciones, una vez cargadas podremos visualizar los nuevos botones en la parte superior

Profile: Default

Profile: wireshark101



Para deshabilitar las nuevas expresiones de filtros hacer clic en la bandera azul que se encuentra del lado izquierdo> filter button preferences



Y en esta ventana podemos deshabilitar los botones

