



“Secretaría De La Educación Superior”
“Instituto Tecnológico de Cancún”

Ingeniería en Sistemas Computacionales

Materia: Fundamentos de Telecomunicaciones

Tema: Laboratorio N#24 Wireshark

Alumno: Vargas Rodríguez Javier Jesús

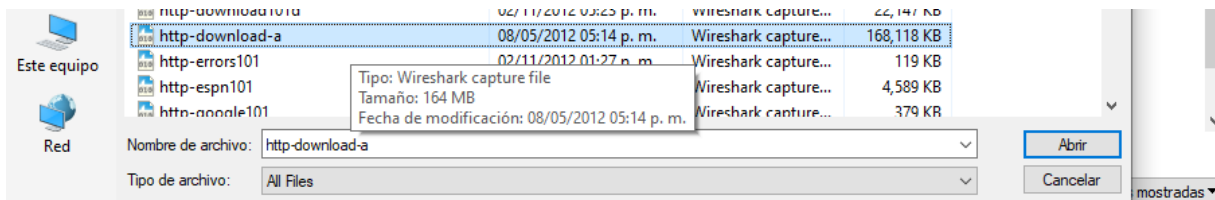
Maestro: Ismael Jiménez Sánchez

Fecha De Entrega: 4/Diciembre/2020

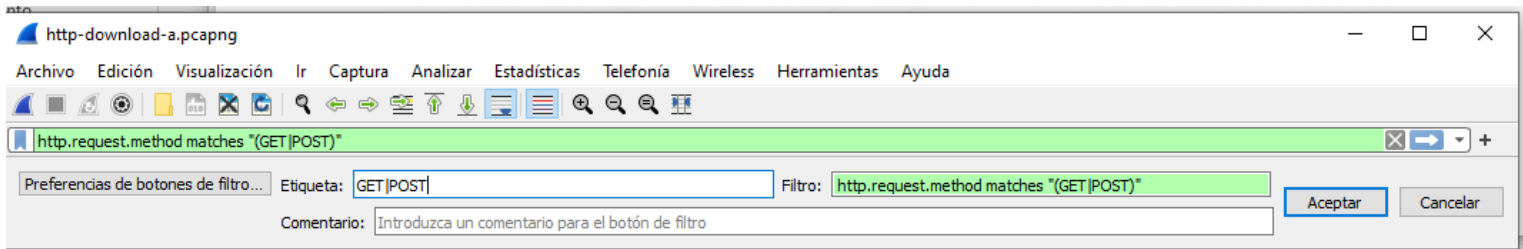
Horario: 5:00 pm – 6:00 pm

Laboratio N#24 – Crear e importar botones de expresion de filtro HTTP.

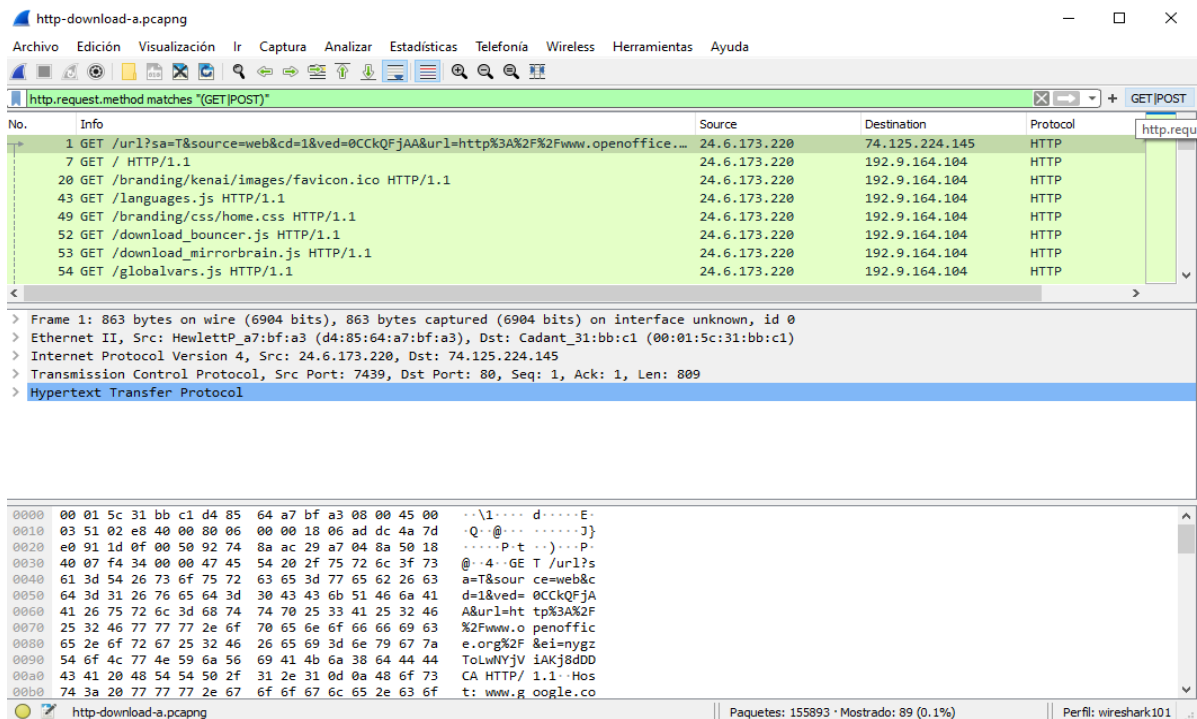
Paso 1 – Abrir el archivo http-download-a.pcapng



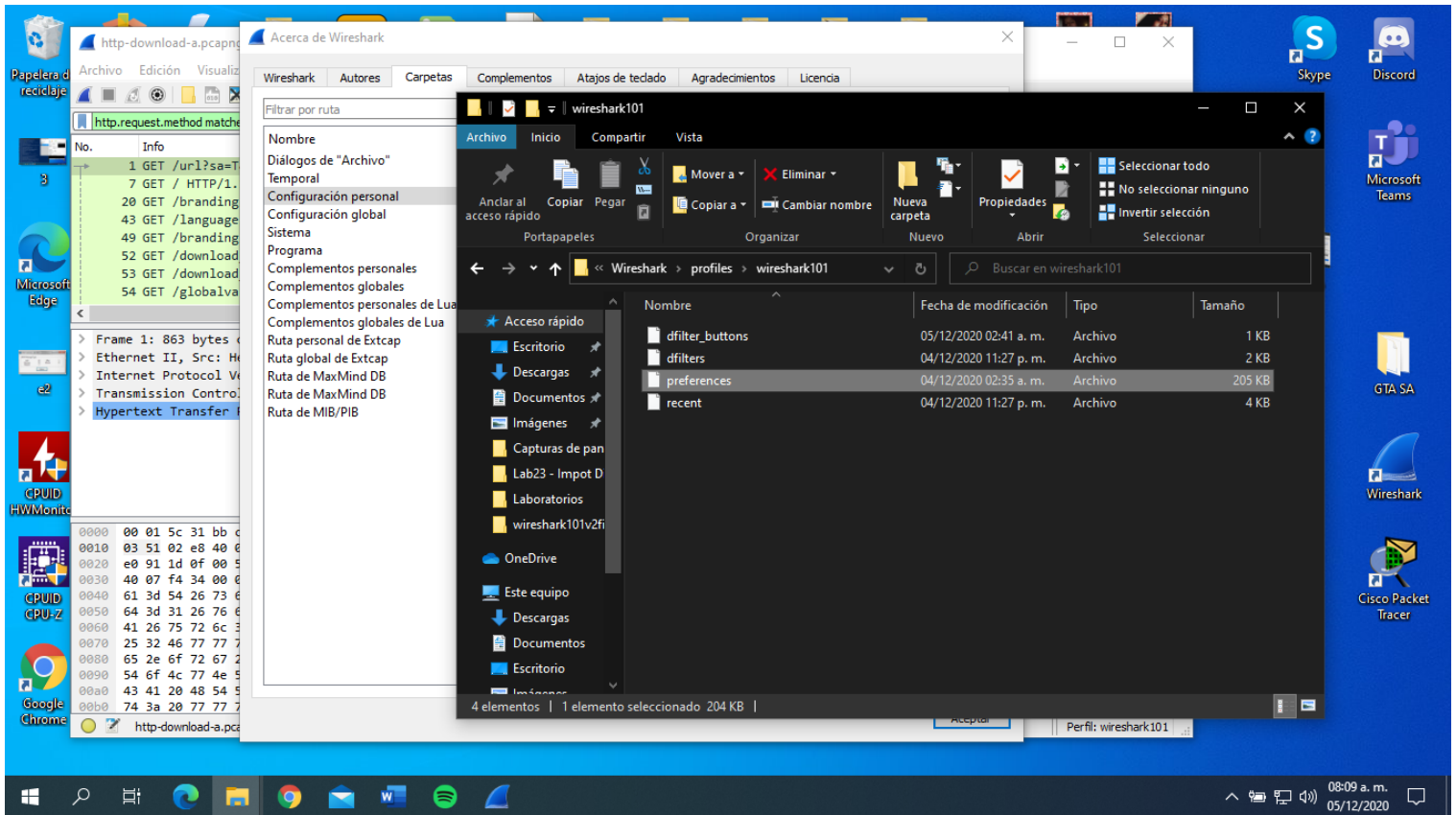
Paso 2 – Checamos que http.request.method matches “(GET|POST)” En el área de filtro. Hacemos clic en agregar la expresión del filtro que se encuentra.



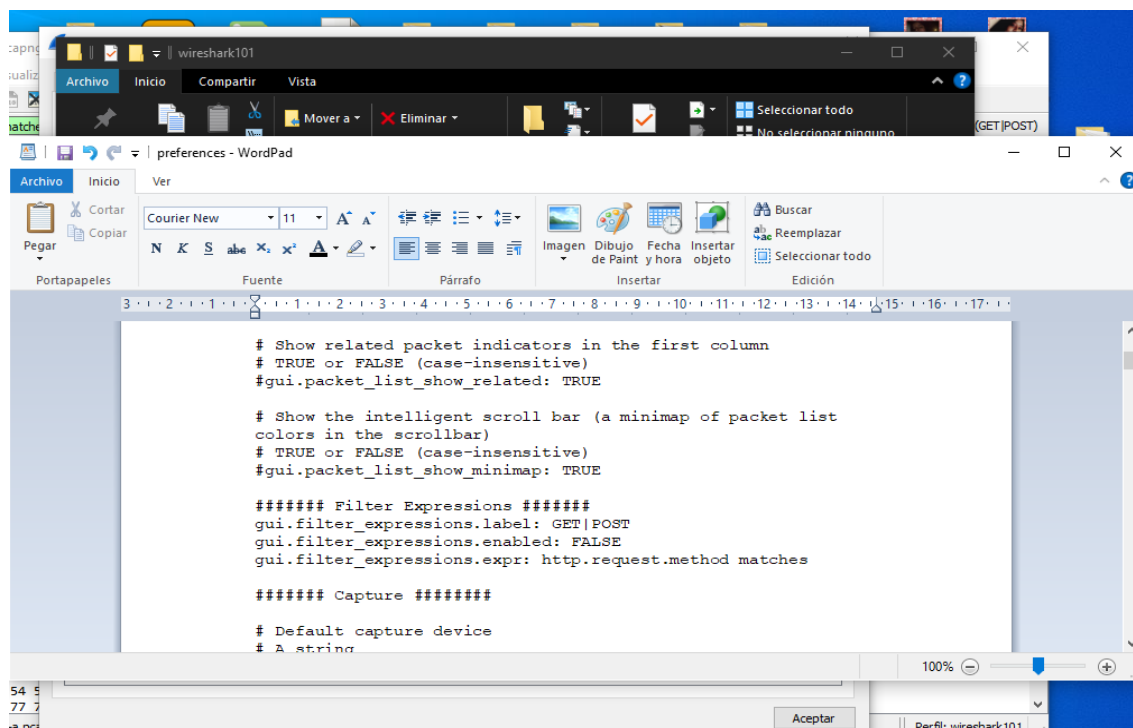
Paso 3 – Le damos clic en GET | POST para ver los paquetes que coinciden con el filtro que pusimos.



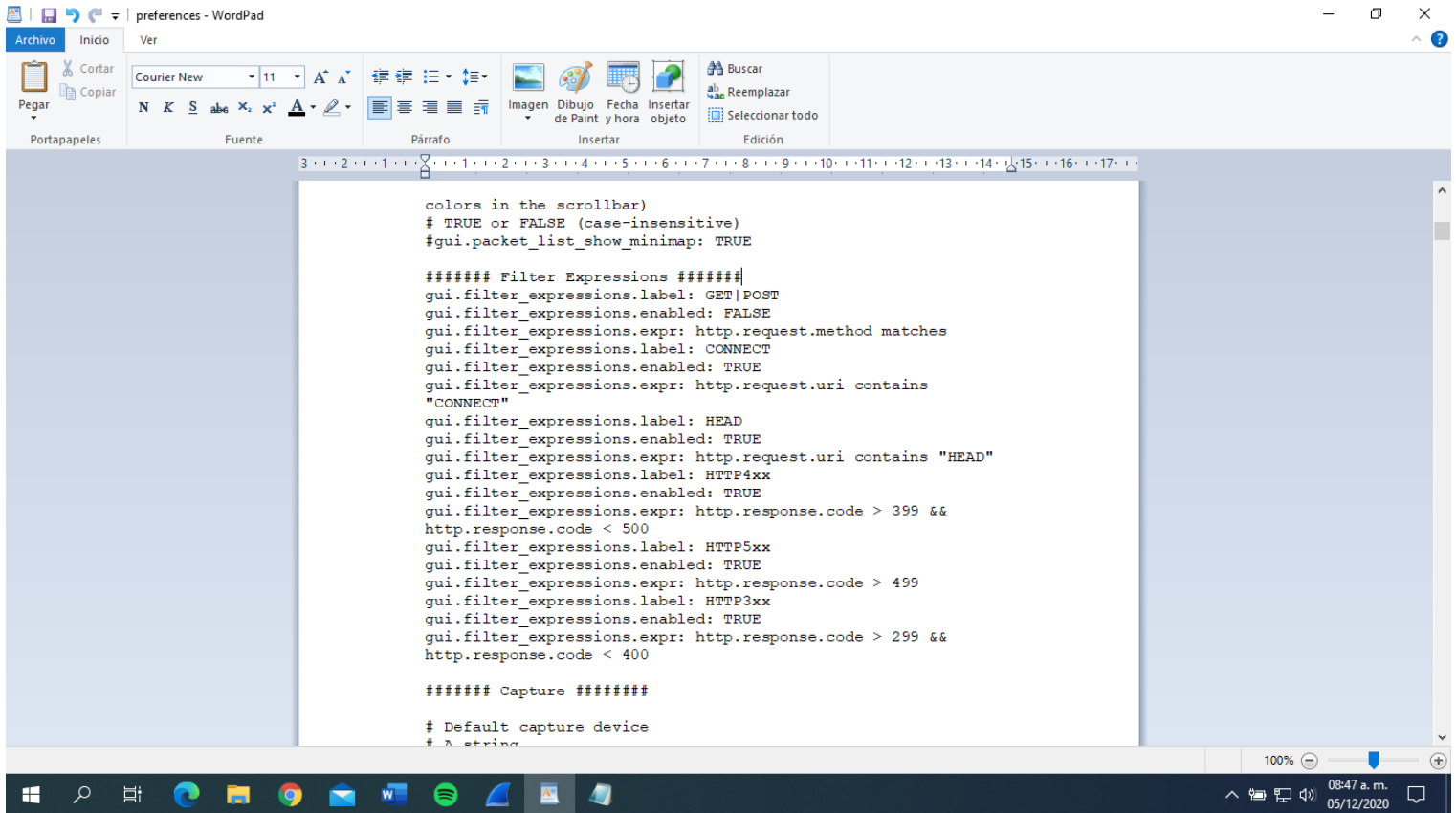
Paso 4 – Utilizando un editor de texto como WordPad abrimos el archivo PREFERENCES que se encuentra en la carpeta Wireshark | Profies.



Paso 5 – Utilizamos la función Buscas en el editor de texto para buscar expresiones en el filtro. Veremos que debe hacer un botón GET | POST como se muestra.



Paso 6 – Extraiga las expresiones filterexpressions101.txt del archivo wireshark101filespart2.



```
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
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
```

Paso 7 – Debemos de recargar wireshark para ver los cambios realizados.

The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Telefonía, Wireless, Herramientas, and Ayuda. The toolbar contains icons for file operations, capture, analysis, and display. The main window is titled 'http-download-a.pcapng' and displays a list of captured packets. The filter bar shows 'http.request.method matches "(GET|POST)"'. The packet list shows several GET requests to various resources. The packet details pane on the right shows the selected packet (No. 1) with its structure: Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Info	Source	Destination	Protocol
1	GET /url?sa=T&source=web&cd=1&ved=0CCKQFjAA&url=http%3A%2F%2Fwww.openoffice...	24.6.173.220	74.125.224.145	HTTP
7	GET / HTTP/1.1	24.6.173.220	192.9.164.104	HTTP
20	GET /branding/kenai/images/favicon.ico HTTP/1.1	24.6.173.220	192.9.164.104	HTTP
43	GET /languages.js HTTP/1.1	24.6.173.220	192.9.164.104	HTTP
49	GET /branding/css/home.css HTTP/1.1	24.6.173.220	192.9.164.104	HTTP
52	GET /download_bouncer.js HTTP/1.1	24.6.173.220	192.9.164.104	HTTP
53	GET /download_mirrorbrain.js HTTP/1.1	24.6.173.220	192.9.164.104	HTTP
54	GET /globalvars.js HTTP/1.1	24.6.173.220	192.9.164.104	HTTP

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 ..\.... d....E
0010 03 51 02 e8 40 00 00 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 18P.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&source=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 50 2f 31 2e 31 0d 0a 48 6f 73 CA HTTP/ 1.1..Hos
00b0 74 3a 20 77 77 77 2e 6f 6f 6f 67 6c 65 2e 63 6f t: www.g oogle.co