

Instituto Tecnológico de Cancún

Fundamentos de Telecomunicaciones

**Lab23 - Impot Display Filters into a
Profile**

Prof. Ismael Jiménez Sánchez

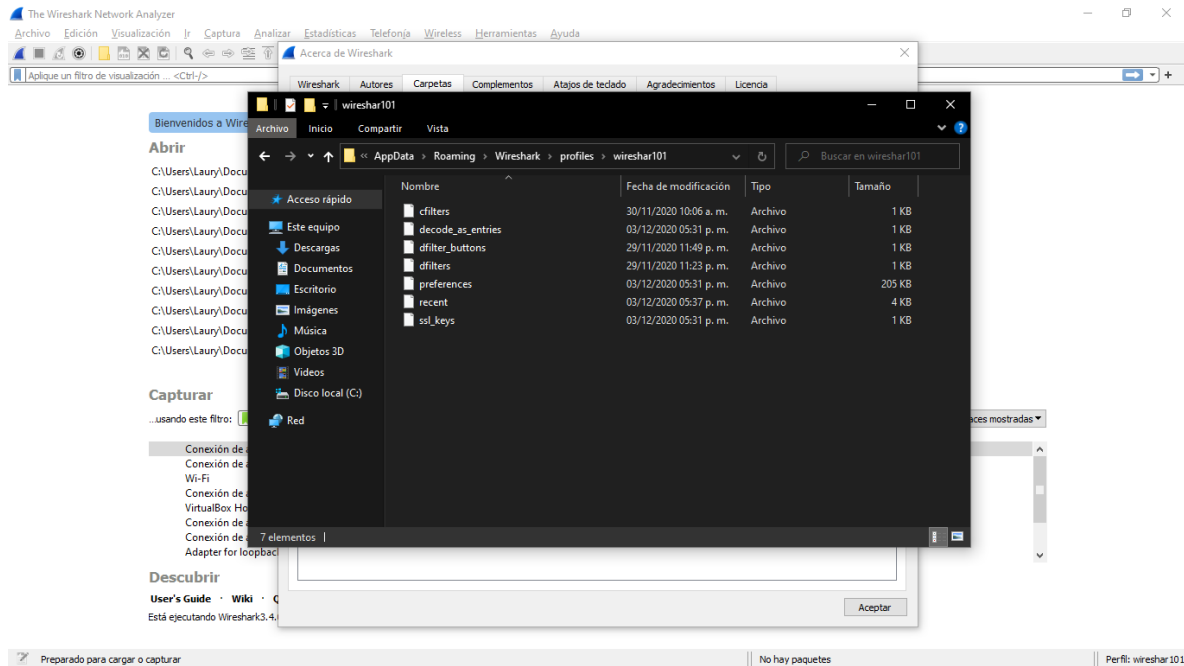
**Alumno(a). Laury del Rosario Mex
Martin**

Ciclo 2020-B

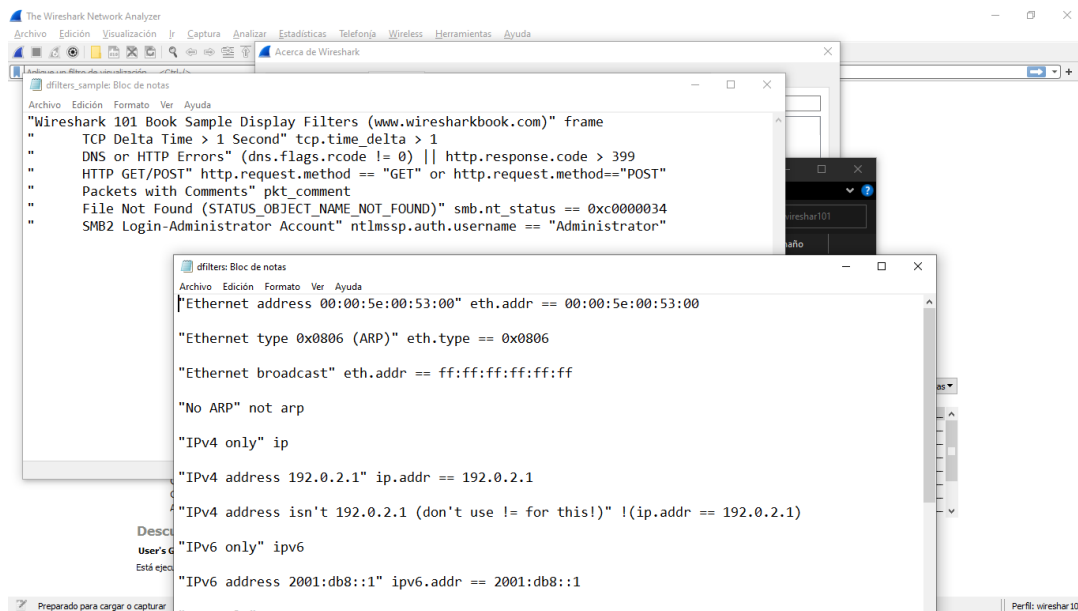
En este lab se va importar filtros de display de un perfil.

Paso 1:

Entramos en la carpeta del perfil que creamos en el Lab 6, debemos de crear antes el filtro My IP Address del Lab 15.



Paso 2: Descargamos primero el archivo dfilter_sample.txt, copiamos el contenido y en el archivo dfilters de la carpeta de wireshar101 pegamos el contenido al final.



Guardamos el archivo

```
*dfilters: Bloc de notas
Archivo Edición Formato Ver Ayuda

"IPv4 address 192.0.2.1" ip.addr == 192.0.2.1

"IPv4 address isn't 192.0.2.1 (don't use != for this!)" !(ip.addr == 192.0.2.1)

"IPv6 only" ipv6

"IPv6 address 2001:db8::1" ipv6.addr == 2001:db8::1

"TCP only" tcp

"UDP only" udp

"Non-DNS" !(udp.port == 53 || tcp.port == 53)

"TCP or UDP port is 80 (HTTP)" tcp.port == 80 || udp.port == 80

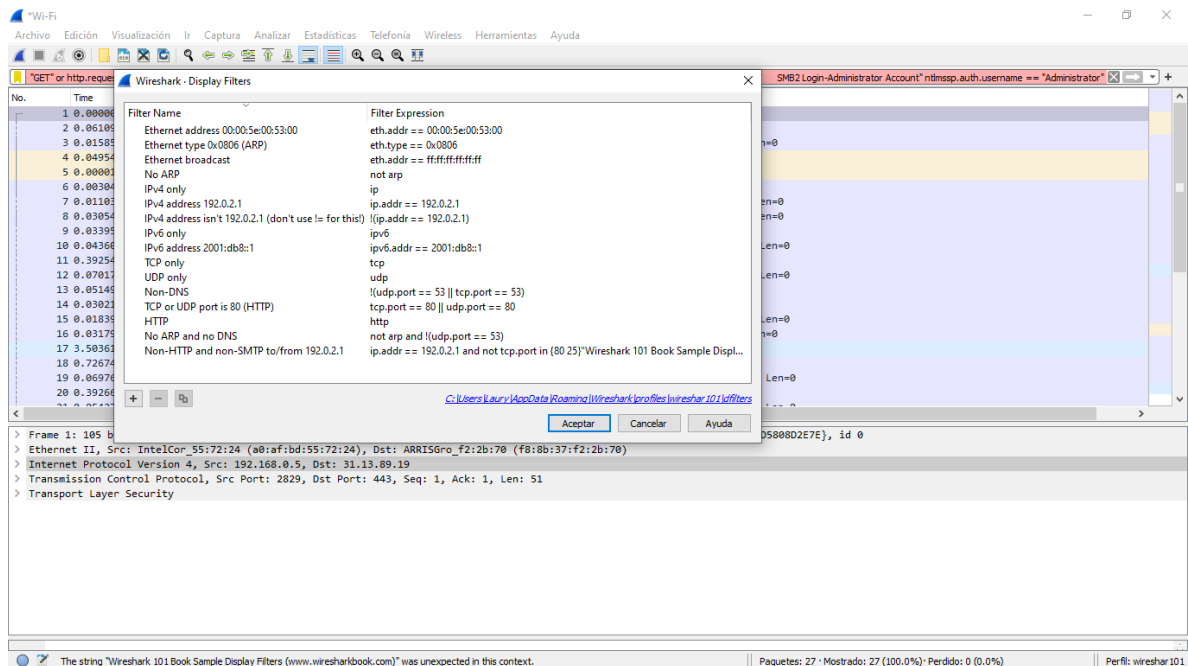
"HTTP" http

"No ARP and no DNS" not arp and !(udp.port == 53)

"Non-HTTP and non-SMTP to/from 192.0.2.1" ip.addr == 192.0.2.1 and not tcp.port in {80 25}

"Wireshark 101 Book Sample Display Filters (www.wiresharkbook.com)" frame
"    TCP Delta Time > 1 Second" tcp.time_delta > 1
"    DNS or HTTP Errors" (dns.flags.rcode != 0) || http.response.code > 399
"    HTTP GET/POST" http.request.method == "GET" or http.request.method=="POST"
"    Packets with Comments" pkt.comment
"    File Not Found (STATUS_OBJECT_NAME_NOT_FOUND)" smb.nt_status == 0xc0000034
"    SMB2 Login-Administrator Account" ntlmssp.auth.username == "Administrator"
|
```

Paso 3: En el wireshark cambiamos el perfil para poder visualizar lo que se hizo con anterioridad, dando click en el administrador de filtros, pero a mi me salió un error.



Esto mismo puede hacerse con el filtro de captura.