

# INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 23

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

# Lab23- Import Display Filters into a Profile

## Paso 1:

The screenshot shows the Wireshark Network Analyzer interface. The top menu bar includes Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Telefonía, Wireless, Herramientas, and Ayuda. Below the menu is a toolbar with various icons. The main window is divided into several sections:

- Bienvenidos a Wireshark**: A welcome message.
- Abrir**: A list of files to open, including various .pcapng files from the desktop.
- Capturar**: The capture section, showing a list of network interfaces. The first interface, "Conexión de área local\* 2", is selected. Below the list are several network traffic capture waveforms.
- Descubrir**: A section for discovering network devices, with links to User's Guide, Wiki, Questions and Answers, and Mailing Lists.

At the bottom of the interface, there is a status bar showing "Preparado para cargar o capturar" and "No hay paquetes". On the right side, a dropdown menu is open, showing a list of display filters: Default, Bluetooth, Classic, HTTP-DNS\_Errors, No Reassembly, and wireshark101 (which is highlighted).

## Paso 2:

The screenshot illustrates the second step of the Wireshark installation process. It features three overlapping windows:

- About Wireshark:** A dialog box with tabs for 'Wireshark', 'Authors', 'Folders', 'Plugins', 'Keyboard Shortcuts', 'Acknowledgments', and 'License'. The 'Folders' tab is active, displaying a table of file locations.
- File Explorer:** A window showing the directory `C:\Users\omav\AppData\Roaming\Wireshark\profiles\wireshark101`. It contains a table of files:

Nombre	Fecha de modificación	Tipo	Tamaño
decode_as_entries	02/12/2020 14:02	Archivo	1 KB
dfilters	02/12/2020 14:06	Archivo	1 KB
preferences	02/12/2020 14:02	Archivo	206 KB
recent	02/12/2020 14:02	Archivo	4 KB

Below the File Explorer, the 'Network Interface Selection' screen is visible, listing available network adapters for capture:

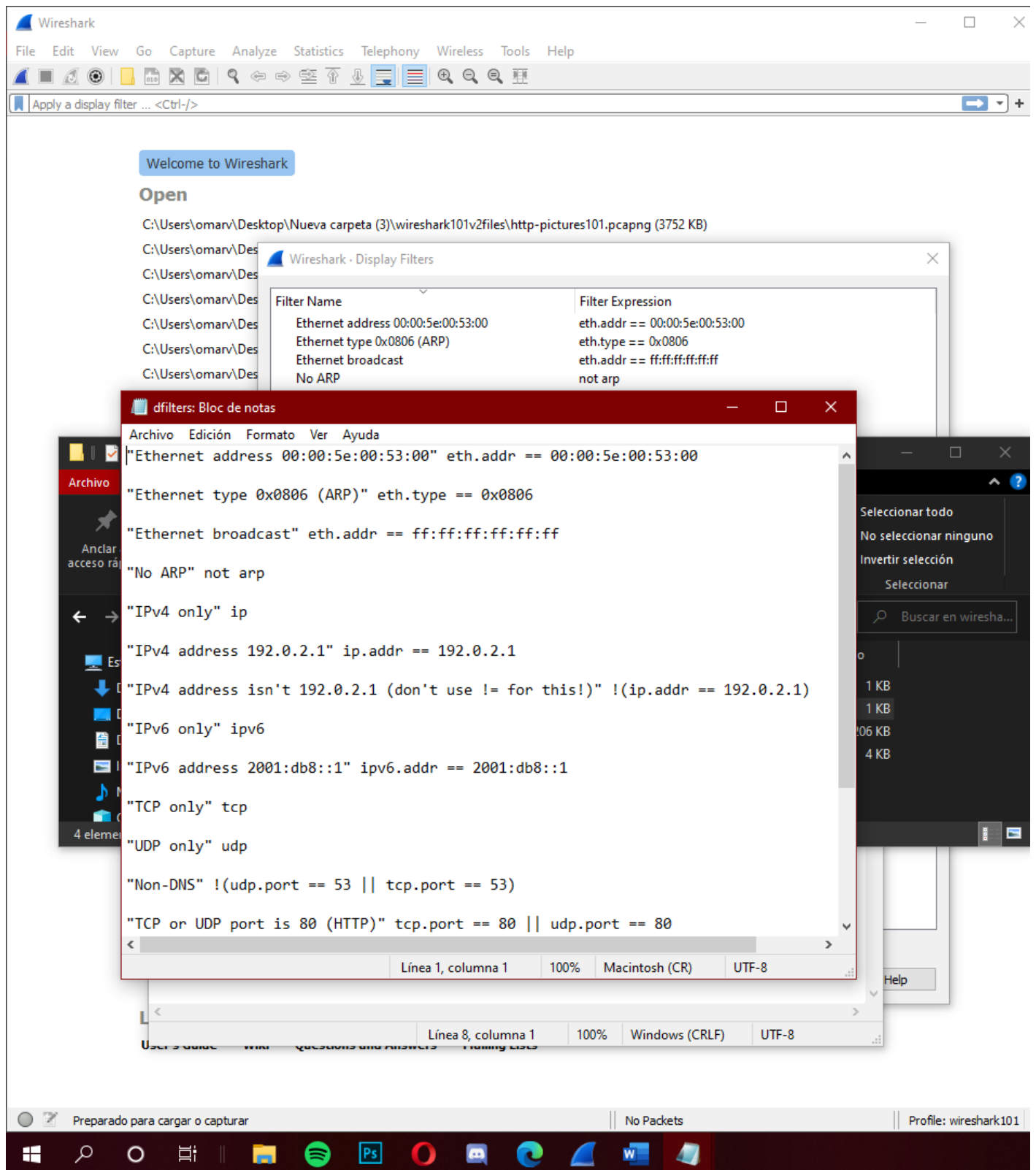
- Conexión de área local\* 8
- Conexión de área local\* 10
- Ethernet
- Conexión de área local\* 9
- VirtualBox Host-Only Network
- Adapter for loopback traffic capture

At the bottom, the Wireshark main window shows the status bar with 'Preparado para cargar o capturar', 'No Packets', and 'Profile: wireshark101'.

**Learn**

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

### Paso 3:



## PASO 4:

The screenshot shows the Wireshark network protocol analyzer interface. The main window displays a list of files to open, including a PCAPng file. Overlaid on this is the 'Wireshark · Display Filters' dialog box, which lists various filter names and their corresponding expressions. In the foreground, a 'Bloc de notas' (Notepad) window is open, displaying a list of sample display filters from the Wireshark book. The bottom status bar indicates 'No Packets' are currently loaded.

**Wireshark · Display Filters**

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp

**dfilters\_sample.txt: Bloc de notas**

```
Archivo Edición Formato Ver Ayuda
"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"
```

**Learn**

[User's Guide](#) · [Wiki](#) · [Questions and Answers](#) · [Mailing Lists](#)

Preparado para cargar o capturar | No Packets | Profile: wireshark101

## Paso 5:

The screenshot shows the Wireshark network protocol analyzer interface. The main window displays a list of files to open, including a file named 'http-pictures101.pcapng (3752 KB)'. Overlaid on this is a 'Wireshark - Display Filters' dialog box, which contains a table of filter names and their corresponding expressions:

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp

Below the dialog box, a Notepad window titled '\*dfilters: Bloc de notas' is open, displaying a list of display filters:

```
"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
"My IP address" ip.addr == 192.168.0.15
"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"
```

The bottom status bar of Wireshark shows 'Preparado para cargar o capturar', 'No Packets', and 'Profile: wireshark101'.

## Paso 6:

The screenshot shows the Wireshark application window with the 'Welcome to Wireshark' dialog and the 'Open' section. A file named 'http-pictures101.pcapng' (3752 KB) is listed. A 'Wireshark - Display Filters' dialog box is open, showing a list of filter names and their corresponding expressions. Below this, a Windows File Explorer window is open, showing the directory 'C:\Users\omarov\AppData\Roaming\Wireshark\profiles\wireshark101'. The 'dfilters' file is selected. A text box at the bottom of the screen contains the following display filters:

```
"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
"My IP adress" ip.addr == 192.168.0.15
```

The Windows taskbar at the bottom shows the Start button and several application icons, including File Explorer, Spotify, Photoshop, and Microsoft Word.

## Paso 7 y 8

The screenshot shows the Wireshark Network Analyzer interface. The main window is titled "The Wireshark Network Analyzer" and has a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. Below the toolbar is a status bar that says "Apply a display filter ... <Ctrl-/>".

A "Wireshark - Display Filters" dialog box is open, showing a list of filter names and their corresponding filter expressions. The dialog box has a title bar with a close button (X). The list is as follows:

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	eth.type == 0x0806
Ethernet broadcast	eth.addr == ff:ff:ff:ff:ff:ff
No ARP	not arp
IPv4 only	ip
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}
My IP address	ip.addr == 192.168.0.15
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"

At the bottom of the dialog box, there are three buttons: "+", "-", and "Reset". To the right of these buttons is a URL: <C:\Users\lomarv\AppData\Roaming\Wireshark\profiles\wireshark101\filters>. At the bottom right of the dialog box are three buttons: "OK", "Cancel", and "Help".

Below the dialog box, the text "Adapter for loopback traffic capture \_M..." is visible.

**Learn**

**User's Guide · Wiki · Questions and Answers · Mailing Lists**

You are running Wireshark 3.4.0 (v3.4.0-0-g9733f173ea5e). You receive automatic updates.

The bottom of the screenshot shows the Windows taskbar with various application icons (Windows, Search, File Explorer, Spotify, Photoshop, Firefox, Telegram, Edge, Word, Wireshark) and the system tray showing "Ready to load or capture", "No Packets", and "Profile: wireshark101".