

INSTITUTO TECNOLÓGICO DE CANCUN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 13

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

LAB 13 Create, Save and Apply a DNS Capture Filter

Paso 1:

The screenshot displays the Wireshark Network Analyzer interface. The 'Capture' menu is open, showing options: Start (Ctrl+E), Stop (Ctrl+E), Restart (Ctrl+R), Capture Filters... (F5), and Refresh Interfaces (F5). Below the menu, a list of capture files is shown, including stopproblem101_00029_20201201125650.pcapng (516 KB) and http-winpcap101.cap (165 KB).

Capture

...using this filter: All interfaces shown ▼

Interface	Packet Count
Conexión de área local* 2	0
Conexión de área local* 1	0
Wi-Fi	0
Radmin VPN	0
Conexión de área local* 8	0
Conexión de área local* 10	0
Ethernet	0
Conexión de área local* 9	0
VirtualBox Host-Only Network	0
Adapter for loopback traffic capture	0
Conexión de red Bluetooth	0

Learn

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

You are running Wireshark 3.2.4 (v3.2.4-0-g893b5a5e1e3e). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Paso 2:

The Wireshark Network Analyzer

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Welcome to Wireshark

Open

C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00029_20201201125650.pcapng (516 KB)

Wireshark · Capture Interfaces

Input Output Options

Interface	Traffic	Link-layer Header	Promisc	Snapshot	Buffer (B)	Monitor	Capture Filter
> Conexión de área local* 2	—	Ethernet	<input checked="" type="checkbox"/>	default	2	—	
> Conexión de área local* 1	—	Ethernet	<input checked="" type="checkbox"/>	default	2	—	
> Wi-Fi	—	Ethernet	<input checked="" type="checkbox"/>	default	2	—	
> Radmin VPN	—	Ethernet	<input checked="" type="checkbox"/>	default	2	—	
Conexión de área local* 8	—	Ethernet	<input checked="" type="checkbox"/>	default	2	—	
Conexión de área local* 10	—	Ethernet	<input checked="" type="checkbox"/>	default	2	—	
> Ethernet	—	Ethernet	<input checked="" type="checkbox"/>	default	2	—	
Conexión de área local* 9	—	Ethernet	<input checked="" type="checkbox"/>	default	2	—	
> VirtualBox Host-Only Network	—	Ethernet	<input checked="" type="checkbox"/>	default	2	—	
Adapter for loopback traffic capture	—	BSD loopback	<input checked="" type="checkbox"/>	default	2	—	
> Conexión de red Bluetooth	—	Ethernet	<input checked="" type="checkbox"/>	default	2	—	

☒ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces:

Manage Interfaces... Compile BPFs

Start Close Help

Conexión de área local* 2
Conexión de área local* 1
Wi-Fi
Radmin VPN
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
Conexión de red Bluetooth

Learn

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

You are running Wireshark 3.2.4 (v3.2.4-0-g893b5a5e1e3e). You receive automatic updates.

Ready to load or capture No Packets Profile: Default

Paso 3:

The Wireshark Network Analyzer interface is shown. The 'Capture Interfaces' dialog box is open, displaying a list of network interfaces. The 'Ethernet' interface is selected, and the capture filter 'port 53' is applied. The 'Start' button is highlighted.

Welcome to Wireshark

Open

C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00029_20201201125650.pcapng (516 KB)

Wireshark - Capture Interfaces

Input Output Options

Interface	Traffic	Link-layer Header	Promisc	Snapshot	Buffer (B)	Monitor	Capture Filter
> Conexión de área local* 2		Ethernet	<input checked="" type="checkbox"/>	default	2	—	
> Conexión de área local* 1		Ethernet	<input checked="" type="checkbox"/>	default	2	—	
> Wi-Fi		Ethernet	<input checked="" type="checkbox"/>	default	2	—	
> Radmin VPN		Ethernet	<input checked="" type="checkbox"/>	default	2	—	
Conexión de área local* 8		Ethernet	<input checked="" type="checkbox"/>	default	2	—	
Conexión de área local* 10		Ethernet	<input checked="" type="checkbox"/>	default	2	—	
> Ethernet		Ethernet	<input checked="" type="checkbox"/>	default	2	—	port 53
Conexión de área local* 9		Ethernet	<input checked="" type="checkbox"/>	default	2	—	
> VirtualBox Host-Only Network		Ethernet	<input checked="" type="checkbox"/>	default	2	—	
Adapter for loopback traffic capture		BSD loopback	<input checked="" type="checkbox"/>	default	2	—	
> Conexión de red Bluetooth		Ethernet	<input checked="" type="checkbox"/>	default	2	—	

☒ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces:

Manage Interfaces... Compile BPFs

Start Close Help

Conexión de área local* 2
Conexión de área local* 1
Wi-Fi
Radmin VPN
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
Conexión de red Bluetooth

Learn

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

You are running Wireshark 3.2.4 (v3.2.4-0-g893b5a5e1e3e). You receive automatic updates.

Ready to load or capture | No Packets | Profile: Default

Paso 4:

The image 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-/>".

On the left side, there is a sidebar with sections: "Welcome to Wireshark", "Open" (listing various file locations), "Capture" (listing network interfaces), and "Learn" (with links to User's Guide, Wiki, Questions and Answers, and Mailing Lists). The "Capture" section is currently selected, showing a list of network interfaces including "Ethernet", "VirtualE", and "Adapte".

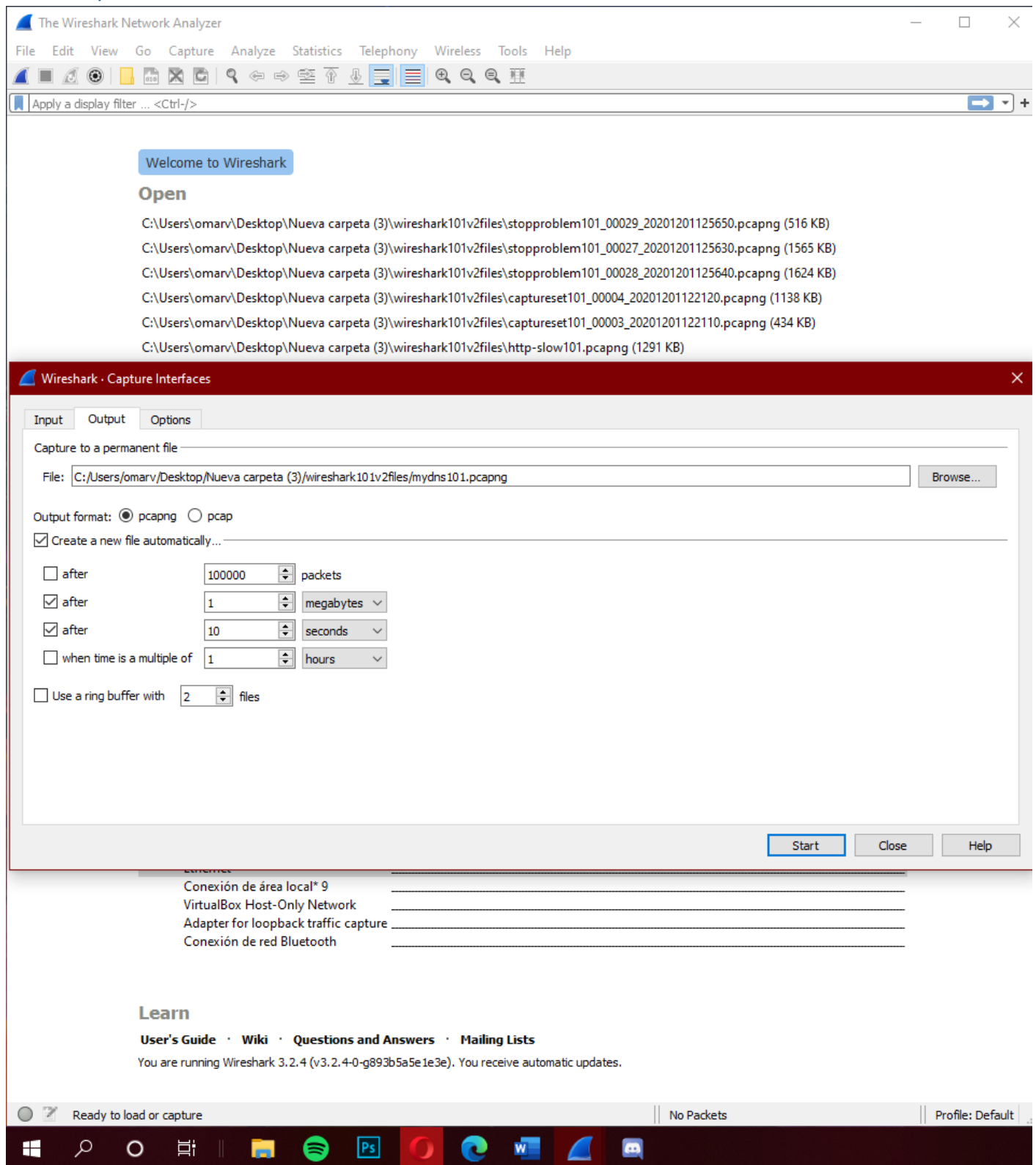
A "Wireshark - Capture Filters" dialog box is open in the center. It has a table with two columns: "Filter Name" and "Filter Expression". The "DNS" filter is selected and highlighted in blue.

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	not port 53
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org
NotMyMac	not ether host C4-65-16-BF-8D-83
DNS	ip host host.example.com

At the bottom of the dialog box, there are "OK", "Cancel", and "Help" buttons. A link to the filters file is also present: <C:\Users\omary\AppData\Roaming\Wireshark\filters>.

The bottom status bar of the main window shows "Ready to load or capture", "No Packets", and "Profile: Default".

Paso 5 y 6:



Paso 8: Damos clic stop capture Button;

Paso 9

The image shows a dual-screen setup. The left screen displays a Wireshark network capture of a DNS query. The right screen shows a web browser displaying the Beatles website.

Wireshark Capture (Left Screen):

- Filter:** mydns101_00001_20201201190340.pcapng
- Packet List:** Shows a series of DNS queries and responses. The selected packet is a Standard query response from 192.168.0.15 to 192.168.0.15.
- Packet Details:** Shows the structure of the DNS response, including Ethernet II, Internet Protocol Version 6, User Datagram Protocol, and Domain Name System (query).
- Packet Bytes:** Shows the raw hex and ASCII data of the selected packet.

Web Browser (Right Screen):

- Address Bar:** www.thebeatles.com
- Page Title:** THE BEATLES
- Content:** A large image of George Harrison sitting on a bench in a park, holding an umbrella. The text "GEORGE HARRISON" and "ALL THINGS MUST PASS" is overlaid on the image.
- Footer:** A green banner with the text "We use cookies on this site to enhance your user experience. By clicking the Accept button, you agree to us doing so. No, give me more info." and buttons for "OK, I AGREE" and "NO, THANKS".