

INSTITUTO TECNOLÓGICO DE CANCUN



TECNOLÓGICO

INSTITUTO

DE CANCÚN



Nombre De La Materia: Fundamentos De Telecomunicaciones

Nombre De La Unidad: Sistemas de comunicación

N.º De Actividad: Laboratorio 11

Nombre Del Alumno: Vazquez Canto Andres Omar

N.º De Control: 17530439

Lab11- Capture Only Traffic to or from Your IP Address

Paso 1:

The screenshot shows the Wireshark Network Analyzer interface. The main window displays a list of files to open, with the following paths and sizes:

- C:\Users\omarr\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00029_20201201125650.pcapng (516 KB)
- C:\Users\omarr\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00027_20201201125630.pcapng (1565 KB)
- C:\Users\omarr\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00028_20201201125640.pcapng (1624 KB)
- C:\Users\omarr\Desktop\Nueva carpeta (3)\wireshark101v2files\captureset101_00004_20201201122120.pcapng (1138 KB)
- C:\Users\omarr\Desktop\Nueva carpeta (3)\wireshark101v2files\captureset101_00003_20201201122110.pcapng (434 KB)
- C:\Users\omarr\Desktop\Nueva carpeta (3)\wireshark101v2files\http-slow101.pcapng (1291 KB)
- C:\Users\omarr\Desktop\Nueva carpeta (3)\wireshark101v2files\http-pcapnet101.pcapng (357 KB)
- C:\Users\omarr\Desktop\Nueva carpeta (3)\wireshark101v2files\http-disney101.pcapng (6215 KB)
- C:\Users\omarr\Desktop\Nueva carpeta (3)\wireshark101v2files\challenge101-0.pcapng (220 KB)
- C:\Users\omarr\Desktop\Nueva carpeta (3)\wireshark101v2files\http-wincap101.cap (165 KB)

The 'Wireshark - Capture Interfaces' window is open, showing a list of interfaces and their capture filters. The 'Input' tab is selected, and the 'Conexión de área local* 2' interface is highlighted. The 'Capture Filter' column shows 'Ethernet' for all interfaces. The 'Promiscuous' column is checked for all interfaces. The 'Snaplen' column is set to 'default' for all interfaces. The 'Buffer (B)' column is set to '2' for all interfaces. The 'Monitor' column is set to '—' for all interfaces. The 'Capture Filter' column is set to 'Ethernet' for all interfaces.

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

Below the table, there is a checkbox for 'Enable promiscuous mode on all interfaces' which is checked. To the right of this checkbox is a 'Manage Interfaces...' button. Below the checkbox is a text field for 'Capture filter for selected interfaces:' with a dropdown menu showing 'Enter a capture filter ...'. To the right of this text field is a 'Compile BPFs' button. At the bottom of the window are three buttons: 'Start', 'Close', and 'Help'.

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 image shows the Wireshark Network Analyzer interface. The main window displays a list of files to open, with the following paths and sizes:

- C:\Users\omar\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00029_20201201125650.pcapng (516 KB)
- C:\Users\omar\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00027_20201201125630.pcapng (1565 KB)
- C:\Users\omar\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00028_20201201125640.pcapng (1624 KB)
- C:\Users\omar\Desktop\Nueva carpeta (3)\wireshark101v2files\captureset101_00004_20201201122120.pcapng (1138 KB)
- C:\Users\omar\Desktop\Nueva carpeta (3)\wireshark101v2files\captureset101_00003_20201201122110.pcapng (434 KB)
- C:\Users\omar\Desktop\Nueva carpeta (3)\wireshark101v2files\http-slow101.pcapng (1291 KB)
- C:\Users\omar\Desktop\Nueva carpeta (3)\wireshark101v2files\http-pcapnet101.pcapng (357 KB)
- C:\Users\omar\Desktop\Nueva carpeta (3)\wireshark101v2files\http-disney101.pcapng (6215 KB)
- C:\Users\omar\Desktop\Nueva carpeta (3)\wireshark101v2files\challenge101-0.pcapng (220 KB)
- C:\Users\omar\Desktop\Nueva carpeta (3)\wireshark101v2files\http-wincap101.cap (165 KB)

The 'Open' dialog is also visible, showing the 'Input' tab with a list of interfaces and their capture filters. The 'Wi-Fi' interface is selected, and the 'Capture filter for selected interfaces' is set to 'Enter a capture filter ...'.

Wireshark - Capture Interfaces

Interface	Traffic	Link-layer Header	Promi:	Snaptlen	Buffer (v	Monit	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	—	Addresses: fe80::d0ea35e:7110:2392, 192.168.0.2
> 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	—	
> 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	—	
> Ethernet		Ethernet	<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:

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 screenshot shows the Wireshark Network Analyzer interface. The main window displays a list of files to open, with the file `C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\captureset101_00003_20201201122110.pcapng (434 KB)` selected. Below this, the **Wireshark · Capture Interfaces** dialog is open, showing a table of available network interfaces. The **Wi-Fi** interface is selected, and the **Capture filter for selected interfaces** is set to `host 192.168.0.2`. The **Start** button is highlighted.

Welcome to Wireshark

Open

C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00029_20201201125650.pcapng (516 KB)
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00027_20201201125630.pcapng (1565 KB)
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00028_20201201125640.pcapng (1624 KB)
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\captureset101_00004_20201201122120.pcapng (1138 KB)
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\captureset101_00003_20201201122110.pcapng (434 KB)
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\http-slow101.pcapng (1291 KB)
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\http-pcapnet101.pcapng (357 KB)
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\http-disney101.pcapng (6215 KB)
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\challenge101-0.pcapng (220 KB)
C:\Users\omarv\Desktop\Nueva carpeta (3)\wireshark101v2files\http-winpcap101.cap (165 KB)

Wireshark · Capture Interfaces

Input Output Options

Interface	Traffic	Link-layer Header	Promi:	Snappen	Buffer (N	Monit	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	—	host 192.168.0.2
Addresses: fe80::d0e35e:7110:2392, 192.168.0.2							
> 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	—	
> 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	—	
> Ethernet		Ethernet	<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

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 screenshot shows the Wireshark Network Analyzer interface. The main window displays a list of capture files under the 'Open' section. The file `C:\Users\omarov\Desktop\Nueva carpeta (3)\wireshark101v2files\captureset101_00003_20201201122110.pcapng (434 KB)` is selected. Below this, the 'Wireshark - Capture Interfaces' dialog is open, showing the 'Input' tab. The dialog is configured to capture to a permanent file, with the output format set to 'pcapng'. The 'Create a new file automatically...' checkbox is checked, and the 'after' checkbox is selected with a value of 100000 packets. The 'Use a ring buffer with' checkbox is also checked, with a value of 2 files. The 'Start' button is highlighted.

Welcome to Wireshark

Open

- C:\Users\omarov\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00029_20201201125650.pcapng (516 KB)
- C:\Users\omarov\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00027_20201201125630.pcapng (1565 KB)
- C:\Users\omarov\Desktop\Nueva carpeta (3)\wireshark101v2files\stopproblem101_00028_20201201125640.pcapng (1624 KB)
- C:\Users\omarov\Desktop\Nueva carpeta (3)\wireshark101v2files\captureset101_00004_20201201122120.pcapng (1138 KB)
- C:\Users\omarov\Desktop\Nueva carpeta (3)\wireshark101v2files\captureset101_00003_20201201122110.pcapng (434 KB)
- C:\Users\omarov\Desktop\Nueva carpeta (3)\wireshark101v2files\http-slow101.pcapng (1291 KB)
- C:\Users\omarov\Desktop\Nueva carpeta (3)\wireshark101v2files\http-pcapnet101.pcapng (357 KB)
- C:\Users\omarov\Desktop\Nueva carpeta (3)\wireshark101v2files\http-disney101.pcapng (6215 KB)
- C:\Users\omarov\Desktop\Nueva carpeta (3)\wireshark101v2files\challenge101-0.pcapng (220 KB)
- C:\Users\omarov\Desktop\Nueva carpeta (3)\wireshark101v2files\http-wincap101.cap (165 KB)

Wireshark - Capture Interfaces

Input Output Options

Capture to a permanent file

File: Leave blank to use a temporary file Browse...

Output format: ☒ pcapng ☐ pcap

☐ Create a new file automatically...

☐ after 100000 packets

☐ after 1 kilobytes

☐ after 1 seconds

☐ when time is a multiple of 1 hours

☐ Use a ring buffer with 2 files

Start Close Help

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 5:

Capturing from Wi-Fi (host 192.168.0.2)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
484	0.001346	109.207.80.96	192.168.0.2	UDP	60	59927 → 62254 Len=14
485	0.000570	192.168.0.2	181.137.121.215	UDP	54	51033 → 61850 Len=12
486	0.000003	192.168.0.2	46.159.240.240	UDP	54	54170 → 59721 Len=12
487	0.001438	168.194.103.37	192.168.0.2	UDP	60	53467 → 62138 Len=12
488	0.000142	192.168.0.2	168.194.103.37	UDP	56	62138 → 53467 Len=14
489	0.003961	201.141.218.126	192.168.0.2	UDP	60	59024 → 59960 Len=14
490	0.002768	181.169.139.68	192.168.0.2	UDP	60	63038 → 54359 Len=14
491	0.004717	186.61.53.77	192.168.0.2	UDP	60	49833 → 52338 Len=12
492	0.000175	192.168.0.2	186.61.53.77	UDP	56	52338 → 49833 Len=14
493	0.000634	138.128.138.231	192.168.0.2	UDP	250	50003 → 57977 Len=208
494	0.001197	192.168.0.2	109.129.48.33	UDP	54	60504 → 51581 Len=12
495	0.000509	192.168.0.2	138.128.138.231	UDP	253	57977 → 50003 Len=211
496	0.015550	138.128.138.231	192.168.0.2	UDP	202	50003 → 57977 Len=160
497	0.005824	192.168.0.2	138.128.138.231	UDP	243	57977 → 50003 Len=201
498	0.000473	212.5.194.245	192.168.0.2	UDP	392	61220 → 56509 Len=350
499	0.000194	192.168.0.2	212.5.194.245	UDP	56	56509 → 61220 Len=14
500	0.000957	168.194.103.37	192.168.0.2	UDP	60	53467 → 62138 Len=14
501	0.003942	192.168.0.2	187.187.224.120	UDP	54	59530 → 53940 Len=12
502	0.000003	192.168.0.2	109.248.81.6	UDP	54	54190 → 64685 Len=12

Símbolo del sistema

```

-k host-list      Ruta de origen estricta para lista-host (solo IPv4).
-w timeout       Tiempo de espera en milisegundos para cada respuesta.
-R              Usar encabezado de enrutamiento para probar también
                la ruta inversa (solo IPv6).
                Por RFC 5095 el uso de este encabezado de enrutamiento ha
                quedado en desuso. Es posible que algunos sistemas anulen
                solicitudes de eco si usa este encabezado.
-S srcaddr       Dirección de origen que se desea usar.
-c compartment   Enrutamiento del identificador del compartimiento.
-p              Hacer ping a la dirección del proveedor de Virtualización
                de red de Hyper-V.
-4              Forzar el uso de IPv4.
-6              Forzar el uso de IPv6.

C:\Users\omarv>ping www.chappellu.com

Haciendo ping a td-balancer-sv5-61-211.wixdns.net [185.230.61.211] con 32 bytes de datos:
Respuesta desde 185.230.61.211: bytes=32 tiempo=105ms TTL=238
Respuesta desde 185.230.61.211: bytes=32 tiempo=103ms TTL=238
Respuesta desde 185.230.61.211: bytes=32 tiempo=106ms TTL=238
Respuesta desde 185.230.61.211: bytes=32 tiempo=112ms TTL=238

Estadísticas de ping para 185.230.61.211:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
        (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 103ms, Máximo = 112ms, Media = 106ms

000
001 C:\Users\omarv>
002 00 02 d0 ed e6 7d 00 14 45 f9 1f 05 d9 04 80 00 .....E.....
003 63 33 85 ff 01 37 00 00 00 00 00 00 .....c3...7...

```

Wi-Fi: <live capture in progress>

Packets: 12671 · Displayed: 12671 (100.0%) | Profile: Default

Paso 6:

Wi-Fi (host 192.168.0.2)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
2012	0.006623	109.129.48.33	192.168.0.2	UDP	184	51581 → 60504 Len=142
2021	0.001896	109.129.48.33	192.168.0.2	UDP	168	51581 → 60504 Len=126
2025	0.000885	109.129.48.33	192.168.0.2	UDP	152	51581 → 60504 Len=110
2029	0.003168	109.129.48.33	192.168.0.2	UDP	168	51581 → 60504 Len=126
2033	0.002466	109.129.48.33	192.168.0.2	UDP	152	51581 → 60504 Len=110
2041	0.000001	109.129.48.33	192.168.0.2	UDP	168	51581 → 60504 Len=126
2043	0.022643	109.129.48.33	192.168.0.2	UDP	184	51581 → 60504 Len=142
2047	0.000001	109.129.48.33	192.168.0.2	UDP	168	51581 → 60504 Len=126
2053	0.004715	109.129.48.33	192.168.0.2	UDP	184	51581 → 60504 Len=142
2058	0.001368	109.129.48.33	192.168.0.2	UDP	60	51581 → 60504 Len=14
2101	0.003487	109.129.48.33	192.168.0.2	UDP	184	51581 → 60504 Len=142
2106	0.000001	109.129.48.33	192.168.0.2	UDP	490	51581 → 60504 Len=448
2109	0.003183	109.129.48.33	192.168.0.2	UDP	302	51581 → 60504 Len=260
2118	0.000123	109.129.48.33	192.168.0.2	UDP	302	51581 → 60504 Len=260
2122	0.000759	109.129.48.33	192.168.0.2	UDP	60	51581 → 60504 Len=14
2218	0.000001	109.129.48.33	192.168.0.2	UDP	168	51581 → 60504 Len=126
2223	0.000002	109.129.48.33	192.168.0.2	UDP	152	51581 → 60504 Len=110
2227	0.002880	109.129.48.33	192.168.0.2	UDP	168	51581 → 60504 Len=126
2232	0.000001	109.129.48.33	192.168.0.2	UDP	152	51581 → 60504 Len=110
2426	0.002142	109.129.48.33	192.168.0.2	UDP	168	51581 → 60504 Len=126
2577	0.000120	109.129.48.33	192.168.0.2	UDP	168	51581 → 60504 Len=126
2587	0.001308	109.129.48.33	192.168.0.2	UDP	184	51581 → 60504 Len=142
2589	0.008185	109.129.48.33	192.168.0.2	UDP	168	51581 → 60504 Len=126

> Frame 2118: 302 bytes on wire (2416 bits), 302 bytes captured (2416 bits) on interface \Device\NPF_{EDA43C56-28F1-4510-83C1-5F2A647264} Ethernet II, Src: ARRISGro_11:22:33 (00:00:ca:11:22:33), Dst: MegaWell_6a:e9:85 (a4:fc:77:6a:e9:85)
 > Internet Protocol Version 4, Src: 109.129.48.33, Dst: 192.168.0.2
 > User Datagram Protocol, Src Port: 51581, Dst Port: 60504
 > Data (260 bytes)

```

0000  a4 fc 77 6a e9 85 00 00  ca 11 22 33 08 00 45 00  ..wj.... 3..E.
0010  01 20 f1 b7 00 00 ec 11  7d c8 6d 81 30 21 c0 a8  .m.0!..
0020  00 02 c9 7d ec 58 01 0c  ce ad 92 82 f9 4d 80 00  .X. .M.
0030  81 64 86 00 45 7d 00 80  a1 d4 ad 45 48 dd 11 02  -d..E}...EH...
0040  35 37 11 c9 4f 3f 52 b9  db 4b f1 92 48 4b cf 9a  57..O?R..K..HK..
0050  1f 84 44 74 01 84 55 09  9a 63 38 10 1d 8a 08 1e  ..Dt..U..c8....
  
```

wireshark_Wi-Fi_20201201152342_a13056.pcapng | Packets: 33542 · Displayed: 33542 (100.0%) · Dropped: 0 (0.0%) | Profile: Default