

Lab 1

Microsoft Windows [Versión 10.0.19045.4046]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\Henry_Guevara>

Uso de dns interno y externo para determinar ip_publica de url. En el ejemplo es privada

```
C:\Users\Henry_Guevara>nslookup
```

```
> www.una.ac.cr
```

```
Servidor: UnKnown
```

```
Address: 172.17.8.5
```

```
Nombre: www.una.ac.cr
```

```
Address: 10.0.96.57
```

```
>
```

Ejemplo de ip publica

```
Respuesta no autoritativa:  
Nombre: e2581.dscx.akamaiedge.net  
Addresses: 2600:1419:5600:385::a15  
            2600:1419:5600:38c::a15  
            23.205.157.123  
Aliases: www.oracle.com  
          ds-www.oracle.com.edgekey.net
```

```
>
```

Rutas default y persistentes

```
=====
Rutas activas:
Destino de red      Máscara de red      Puerta de enlace      Interfaz      Métrica
0.0.0.0             0.0.0.0             10.251.32.1           10.251.34.160 35
10.251.32.0         255.255.252.0       En vínculo            10.251.34.160 291
10.251.34.160       255.255.255.255     En vínculo            10.251.34.160 291
10.251.35.255       255.255.255.255     En vínculo            10.251.34.160 291
127.0.0.0           255.0.0.0           En vínculo            127.0.0.1     331
127.0.0.1           255.255.255.255     En vínculo            127.0.0.1     331
127.255.255.255     255.255.255.255     En vínculo            127.0.0.1     331
224.0.0.0           240.0.0.0           En vínculo            127.0.0.1     331
224.0.0.0           240.0.0.0           En vínculo            10.251.34.160 291
255.255.255.255     255.255.255.255     En vínculo            127.0.0.1     331
255.255.255.255     255.255.255.255     En vínculo            10.251.34.160 291
=====
Rutas persistentes:
Dirección de red    Máscara de red    Dirección de puerta de enlace    Métrica
201.220.29.11      255.255.255.255   192.168.1.1                  1
10.1.0.0            255.255.0.0       10.1.1.1                     1
=====
```

Ver dirección ip

```
C:\Users\Henry_Guevara>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 1:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Conexión de área local* 2:

    Estado de los medios. . . . . : medios desconectados
    Sufixo DNS específico para la conexión. . :

Adaptador de LAN inalámbrica Wi-Fi:

    Sufixo DNS específico para la conexión. . : eduroam.una.cr
    Vínculo: dirección IPv6 local. . . : fe80::de2:d1bb:6b04:c0c3%3
    Dirección IPv4. . . . . : 10.251.34.160
    Máscara de subred . . . . . : 255.255.252.0
    Puerta de enlace predeterminada . . . . : 10.251.32.1

C:\Users\Henry_Guevara>
```

Mac address e ip address y DNS

Adaptador de LAN inalámbrica Wi-Fi:

```
Sufijo DNS específico para la conexión. . : eduroam.una.cr
Descripción . . . . . : Intel(R) Wireless-AC 9560 160MHz
Dirección física. . . . . : 80-32-53-63-2A-45
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::de2:d1bb:6b04:c0c3%3(Preferido)
Dirección IPv4. . . . . : 10.251.34.160(Preferido)
Máscara de subred . . . . . : 255.255.252.0
Concesión obtenida. . . . . : miércoles, 28 de febrero de 2024 17:41:03
La concesión expira . . . . . : miércoles, 28 de febrero de 2024 18:40:01
Puerta de enlace predeterminada . . . . . : 10.251.32.1
Servidor DHCP . . . . . : 10.251.32.1
IAID DHCPv6 . . . . . : 58733139
DUID de cliente DHCPv6. . . . . : 00-01-00-01-27-BB-0B-8A-F8-75-A4-A6
Servidores DNS. . . . . : 172.17.8.5
                          172.17.8.4
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Agrega ruta

```
C:\Users\Henry_Guevara>route add -p 10.0.0.4 mask 255.255.255.255 10.1.4.1  
La operación solicitada requiere elevación.
```

```
C:\Users\Henry_Guevara>
```

```
C:\Windows\system32>route add -p 10.0.0.4 mask 255.255.255.255 10.1.4.1  
Correcto
```

```
C:\Windows\system32>
```


Ver si tenemos un url en nuestras conexiones

se debe buscar las ip address en `netstat -na | findstr 23.221.214.163`

```
> www.bncr.fi.cr
Servidor: UnKnown
Address: 172.17.8.5


Respuesta no autoritativa:
Nombre: e38474.dscx.akamaiedge.net
Addresses: 2600:1419:5600:7::5c7a:9d95
           2600:1419:5600:7::5c7a:9d94
           23.221.214.163
           23.221.214.153
Aliases:  www.bncr.fi.cr
           oce.bncr.fi.cr.edgekey.net
```

Abrir wireshark, elije la interface con movimiento

Bienvenidos a Wireshark

Capturar

...usando este filtro:

<input checked="" type="checkbox"/>	Conexión de área local* 8	—
<input type="checkbox"/>	Conexión de área local* 10	—
<input type="checkbox"/>	Conexión de área local* 9	—
<input type="checkbox"/>	Conexión de área local* 2	—
<input type="checkbox"/>	Wi-Fi	
<input type="checkbox"/>	Conexión de área local* 1	—
<input type="checkbox"/>	Adapter for loopback traffic capture	—
<input type="checkbox"/>	Ethernet	—

Descubrir

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

Está ejecutando Wireshark3.4.3 (v3.4.3-0-g6ae6cd335aa9). Recibe actualizaciones automáticas.

Escribe la dirección del destino analizado

Capturing from wi-fi

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ip.addr == 23.221.214.153

No.	Time	Source	Destination	Protocol	Length	Info
550	17:55:58,429073	10.251.34.176	239.255.255.2...	SSDP	217	M-SEARCH * HTTP/1.1
551	17:55:58,476136	10.251.34.176	239.255.255.2...	SSDP	212	M-SEARCH * HTTP/1.1
552	17:55:58,571295	f4:a4:75:4e:e2:51	IntelCor_63:2...	ARP	42	Who has 10.251.35.181? Tell 10.2
553	17:55:58,688003	10.251.33.133	239.255.255.2...	SSDP	216	M-SEARCH * HTTP/1.1
554	17:55:58,695398	10.251.34.169	mdns.mcast.net	MDNS	78	Standard query 0x0000 PTR _rdlir
555	17:55:58,695746	fe80::14:f944:22...	ff02::fb	MDNS	98	Standard query 0x0000 PTR _rdlir
556	17:55:58,793734	iPhone-de-Alejan...	mdns.mcast.net	MDNS	380	Standard query response 0x0000 F

<

- > Frame 1: 5894 bytes on wire (47152 bits), 5894 bytes captured (47152 bits)
- > Ethernet II, Src: Cisco_1a:67:bf (84:b8:02:1a:67:bf), Dst: IntelCor_63:2a:45 (80:32:53:63:2a:45)
- > Internet Protocol Version 4, Src: 52.167.17.97 (52.167.17.97), Dst: 10.251.34.160 (10.251.34.160)
- > Transmission Control Protocol, Src Port: https (443), Dst Port: 57285 (57285), Seq: 1, Ack: 1, Len: 5840

✕ ➡ ▼ +

Length	Info
5894	Ignored Unknown Record
54	57285 → https(443) [ACK] Seq=1 Ac
2974	Ignored Unknown Record
427	Ignored Unknown Record
54	57285 → https(443) [ACK] Seq=1 Ac
1414	Application Data
4434	https(443) → 57285 [ACK] Seq=9134

- ```
:2a:45)
.34.160)
k: 1, Len: 5840
```

# Análisis de tcp

The image shows the Wireshark network protocol analyzer interface. The main window displays a packet capture from the file 'wireshark\_Wi-FiSKZSJ2.pcap'. The filter bar at the top shows 'ip.addr == 10.251.34.160'. The packet list on the left shows several frames, with frame 1 selected. The packet details pane on the right shows the structure of the selected frame, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The 'Analyze' menu is open, showing options like 'Mostrar filtros...', 'Mostrar macros de filtro...', 'Mostrar expresión de filtro...', 'Aplicar como columna', 'Aplicar como filtro', 'Prepare as Filter', 'Filtro de conversación', 'Protocolos activados...', 'Decodificar como...', 'Volver a cargar complementos Lua', 'SCTP', 'Seguir', 'Mostrar bytes de paquete...', and 'Información especializada'. The 'Seguir' option is highlighted, and a submenu is open showing options like 'Flujo TCP', 'Flujo UDP', 'Flujo TLS', 'Flujo HTTP', 'Flujo HTTP/2', and 'Flujo QUIC'. The status bar at the bottom shows 'Paquetes: 69842 · Mostrado: 63661 (91.2%)' and 'Perfil: Default'.

Wireshark interface showing a packet capture analysis of a TCP connection. The 'Analyze' menu is open, highlighting the 'Seguir' (Follow) option. The packet list shows a sequence of frames, and the packet details pane shows the structure of a TCP segment.

Packet List:

| No. | Time         |
|-----|--------------|
| 1   | 17:55:36,205 |
| 2   | 17:55:36,205 |
| 3   | 17:55:36,207 |
| 4   | 17:55:36,207 |
| 5   | 17:55:36,208 |
| 6   | 17:55:36,211 |
| 10  | 17:55:36,320 |

Packet Details (Frame 1):

- Frame 1: 5894 bytes on wire (47152 bytes captured)
- Ethernet II, Src: Cisco\_1a:67:bf (84:51:37:1a:67:bf), Dst: 08:00:45:00:00:00
- Internet Protocol Version 4, Src: 10.251.34.160, Dst: 10.251.34.160
- Transmission Control Protocol, Src Port: 57285, Dst Port: 443
- Transport Layer Security

Packet Bytes:

```
0000 80 32 53 63 2a 45 84 b8 02 1a 67 bf 08 00 45 00 -ZSC*E...g...E-
0010 16 f8 7e ea 40 00 6b 06 06 73 34 a7 11 61 0a fb -...@.k..s4..a..
0020 22 a0 01 bb df c5 5a f2 1f 5d 37 62 df ac 50 18 -.....Z..]7b..P-
0030 3f fb 00 00 00 00 99 d5 0a 16 e6 30 5e 38 79 07 -?.....^8y..
0040 df e5 4e 83 4e 2b 11 09 42 8c 91 99 90 9a e2 25 -..N.N+..B.....%
0050 9c 5b 2b c6 2d 9f f9 01 18 fc 53 95 10 b4 54 b3 -.[+... ..S...T-
0060 14 f5 9e ee 93 7f 75 60 99 6c f9 3e df fd 3b 32 -.....u`..1.>..;2
0070 1a 0b b8 6e 29 95 c7 fb 4e 49 3f f6 bf e9 8f 7d -...n)...NI?...}
```

Status Bar: Paquetes: 69842 · Mostrado: 63661 (91.2%) | Perfil: Default

# Ver conversaciones

