

Práctica de laboratorio: Explorar tráfico DNS Alan lozano

Objetivos

Parte 1: Capturar tráfico DNS

Parte 2: Explorar tráfico de consultas DNS

Parte 3: Explorar tráfico de respuestas DNS

Antecedentes / Escenario

Wireshark es una herramienta de captura y análisis de paquetes de código abierto. Wireshark proporciona un desglose detallado de la pila de protocolos de red. Wireshark les permite filtrar tráfico para solucionar problemas de red, investigar problemas de seguridad y analizar protocolos de red. Como Wireshark permite ver los detalles de los paquetes, un atacante también puede utilizarla como herramienta de reconocimiento.

En esta práctica de laboratorio instalaremos y utilizaremos Wireshark para filtrar paquetes DNS y ver los detalles de los paquetes de consultas y respuestas DNS.

Recursos necesarios

- Una computadora personal con acceso a internet y Wireshark instalado

Instrucciones

NOTA: RESPONDER CADA PREGUNTA CON CAPTURAS DE PANTALLA COMPLETAS DONDE SE VEAN LAS SIGLAS DE SU NOMBRE AL LADO DEL RELOJ. EN LUGAR DE COLOCAR UN TEXTO DEBE DE SELECCIONAR EL TEXTO INVESTIGADO EN UNA PÁGINA WEB Y HACERLE CAPTURA DE PANTALLA COMPLETA, PARA LUEGO COLOCARLA AQUÍ. SI SON VARIAS PREGUNTAS, DEBE COLOCAR VARIAS CAPTURAS DE PANTALLAS COMPLETAS. NO COLOCAR INFORMACIÓN ENCONTRADA EN NETACAD, COLOCAR INFORMACIÓN INVESTIGADA EN OTRAS PÁGINAS WEB.

Parte 1: Capturar tráfico DNS

Paso 1: Descargar e instalar Wireshark

- a. Descargue la última versión estable de Wireshark desde la siguiente dirección web: www.wireshark.org. Elija la versión de software que necesita según la arquitectura y el sistema operativo de la computadora personal.
- b. Siga las instrucciones que aparecen en la pantalla para instalar Wireshark. Si le aparece un cuadro solicitando que instale USBPcap, **NO** debe instalar USBPcap para la captura de tráfico normal. USBPcap es experimental, y podría causar problemas en los dispositivos USB de su computadora personal.

Paso 2: Capturar tráfico DNS

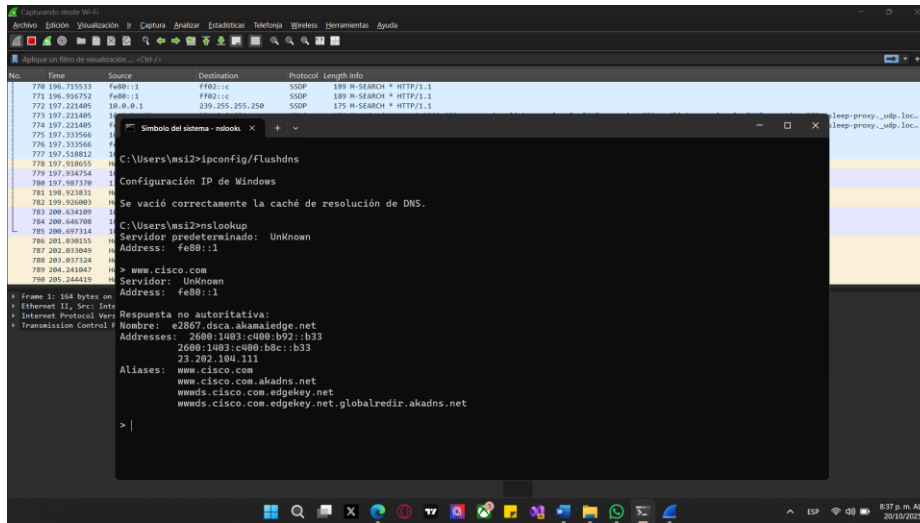
- a. Inicie Wireshark. Seleccione una interfaz activa con tráfico para la captura de paquetes.
- b. Limpie la caché DNS
 - 1) En el Símbolo del sistema de Windows (Command Prompt), escriba **ipconfig /flushdns**.
 - 2) Para la mayoría de las distribuciones de Linux, se utiliza una de las siguientes utilidades para el almacenamiento caché DNS: Systemd-Resolved, DNSMasq y NSCD. Si la distribución Linux que está usando no utiliza ninguna de las utilidades mencionadas, busque en internet la herramienta para vaciar caché DNS para esa distribución Linux.

Identifique la herramienta utilizada en una distribución Linux, comprobando el estado (status):

 1. Systemd-Resolved: **systemctl status systemd-resolved.service**
 2. DNSMasq: **systemctl status dnsmasq.service**
 3. NSCD: **systemctl status nscd.service**

Si está utilizando systemd-Resolved, debe escribir **systemd-resolve --flush-caches** para vaciar la caché de Systemd-Resolved antes de reiniciar el servicio. Los siguientes comandos reinician el servicio asociado mediante privilegios elevados:

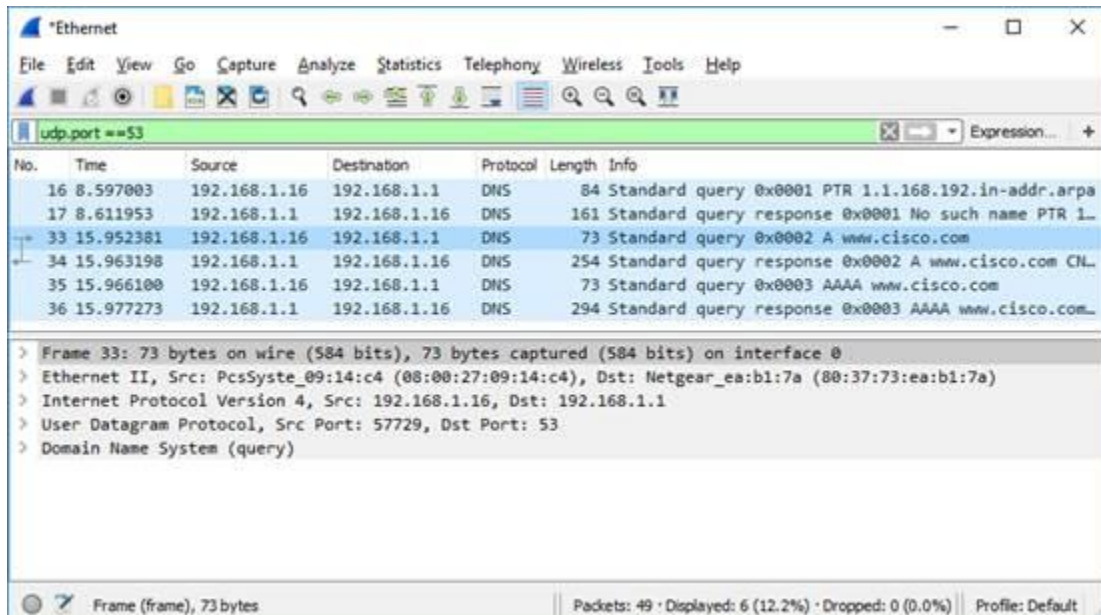
 4. Systemd-Resolved: **sudo systemctl restart systemd-resolved.service**
 5. DNSMasq: **sudo systemctl restart dnsmasq.service**
 6. NSCD: **sudo systemctl restart nscd.service**
 - 3) Para macOS, escriba **sudo killall -HUP mDNSResponder** para limpiar la caché DNS en la consola Terminal. Busque en internet cuales son los comandos que se usan para limpiar la caché DNS de una versión pasada del sistema operativo
- c. En el Símbolo del sistema o terminal, escriba **nslookup** para entrar en el modo interactivo.
- d. Introduzcan el nombre de dominio del sitio web. En este ejemplo se utiliza el nombre de dominio www.cisco.com.

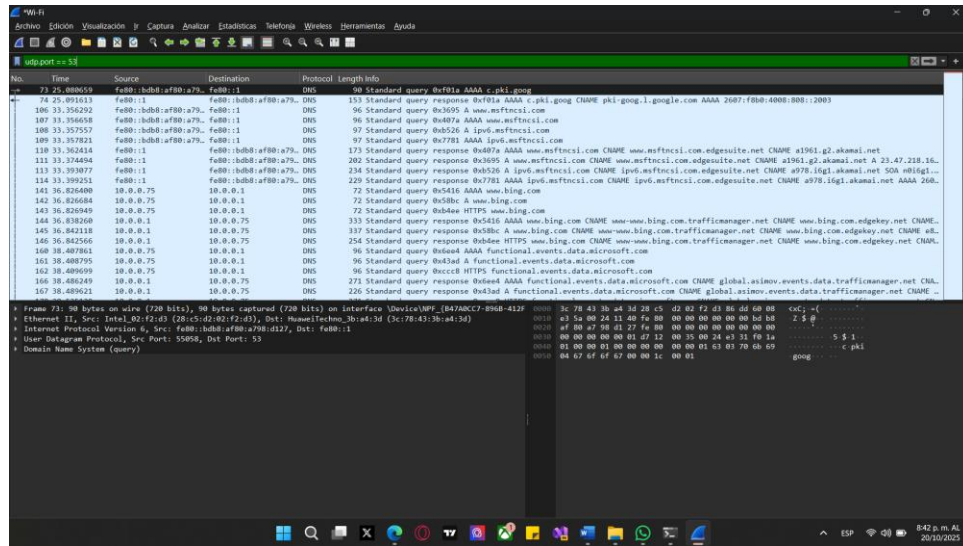


- e. Escriban **exit** cuando hayan terminado. Cierren el símbolo del sistema.
- f. Hagan clic en **Stop capturing packets** (Dejar de capturar paquetes) para detener la captura de Wireshark.

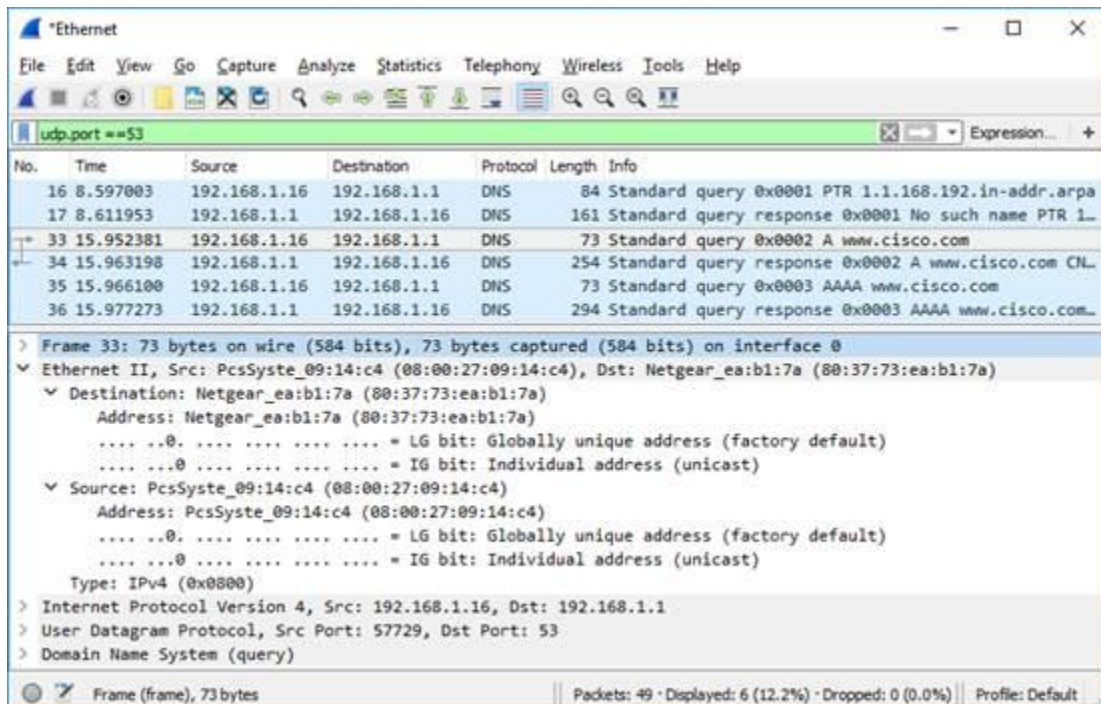
Parte 2: Explorar tráfico de consultas DNS

- a. Observen el tráfico capturado en el panel Packet List (Lista de paquetes) de Wireshark. Introduzcan **udp.port == 53** en el cuadro de filtros y hagan clic en la flecha (o presionen Intro) para mostrar solamente paquetes DNS. **Nota:** Las capturas de pantalla proporcionadas son solo ejemplos. La salida que obtenga puede ser ligeramente diferente a la mostrada.

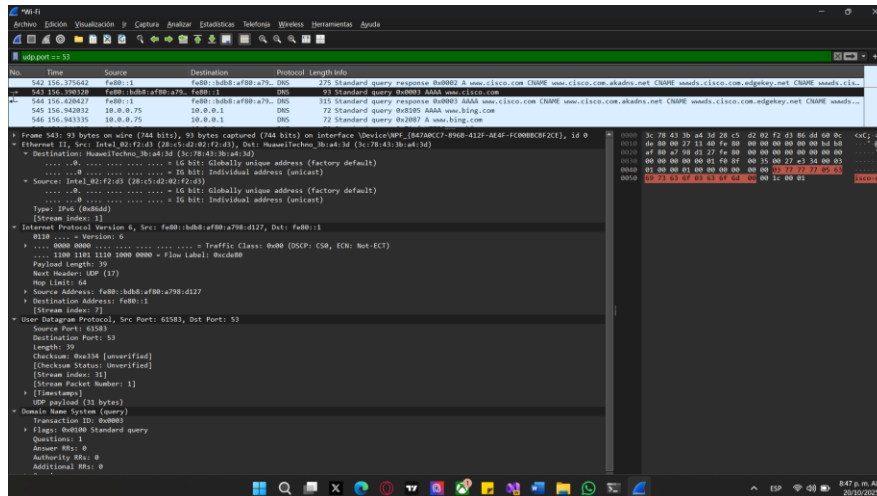




- Selecione el paquete DNS que contiene la **Standard query (Consulta estándar)** y **A www.cisco.com** en la columna Información.
- En el panel Packet Details (Detalles del paquete), observen que este paquete tiene Ethernet II, Internet Protocol Version 4, User Datagram Protocol y Domain Name System (query).
- Expandan **Ethernet II** para ver los detalles. Observen los campos de origen y de destino.

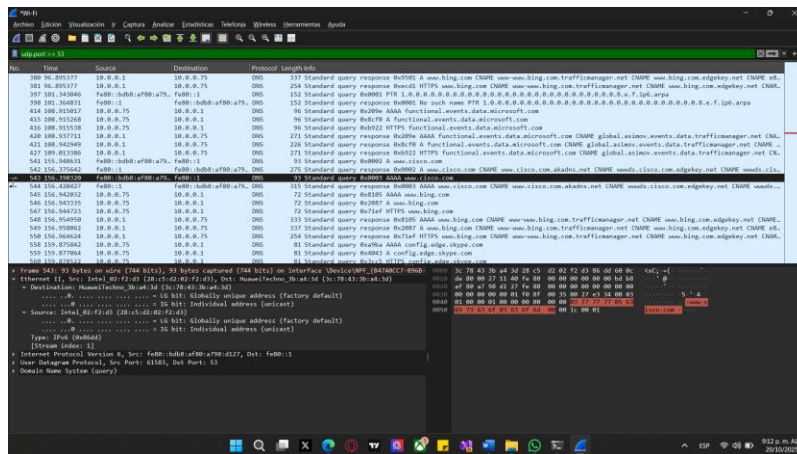


Práctica de laboratorio: Explorar tráfico DNS

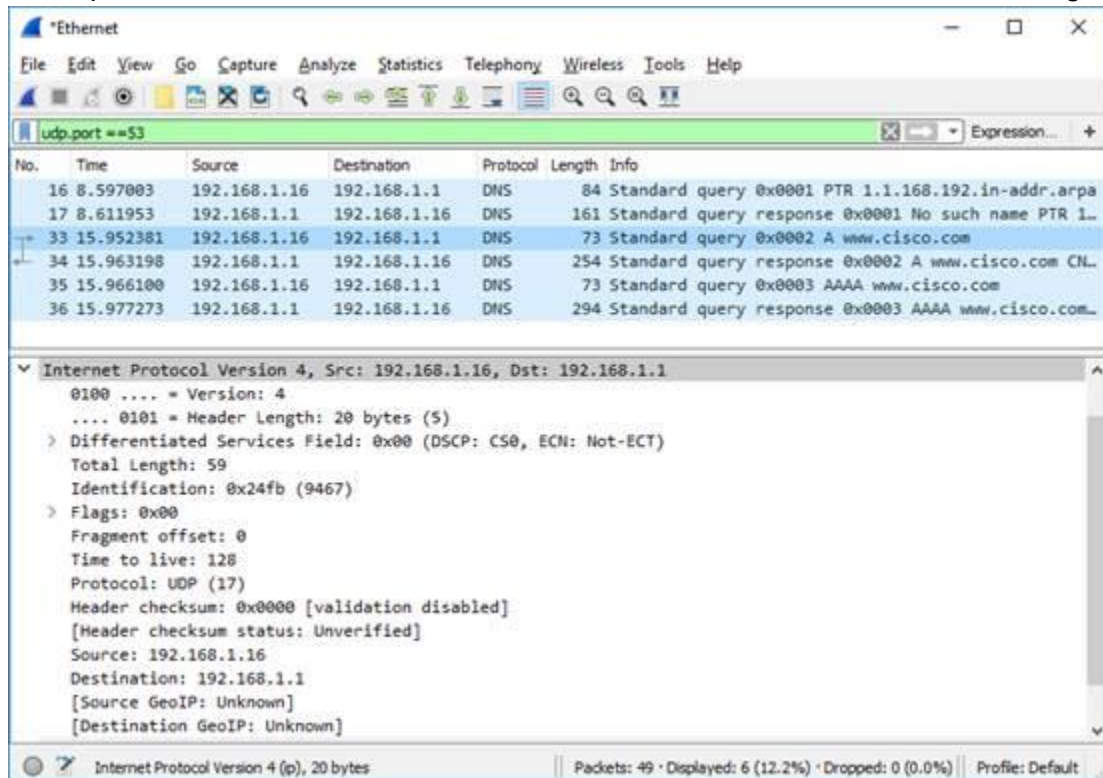


¿Qué sucedió con las direcciones MAC de origen y de destino? ¿Con qué interfaces de red están asociadas estas direcciones MAC?

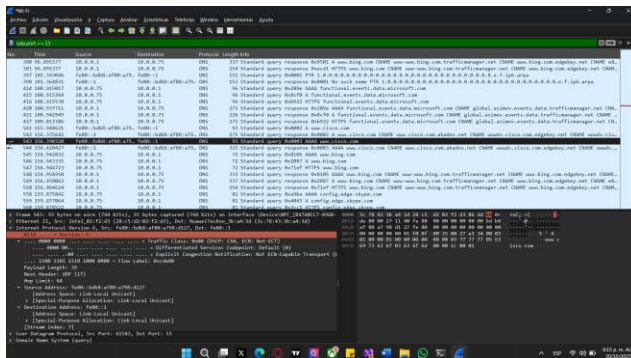
Las direcciones MAC corresponden a la comunicación **local** entre tu computadora y el router Wi-Fi. El paquete aún no ha salido a Internet; una vez que el router lo reenvía, las direcciones MAC cambian, porque cada salto de red tiene sus propias direcciones físicas.



e. Expandan **Internet Protocol Version 4**. Observen las direcciones IPv4 de origen y de destino.



¿Cuáles son las direcciones IP de origen y destino? ¿Con qué interfaces de red están asociadas estas direcciones IP?

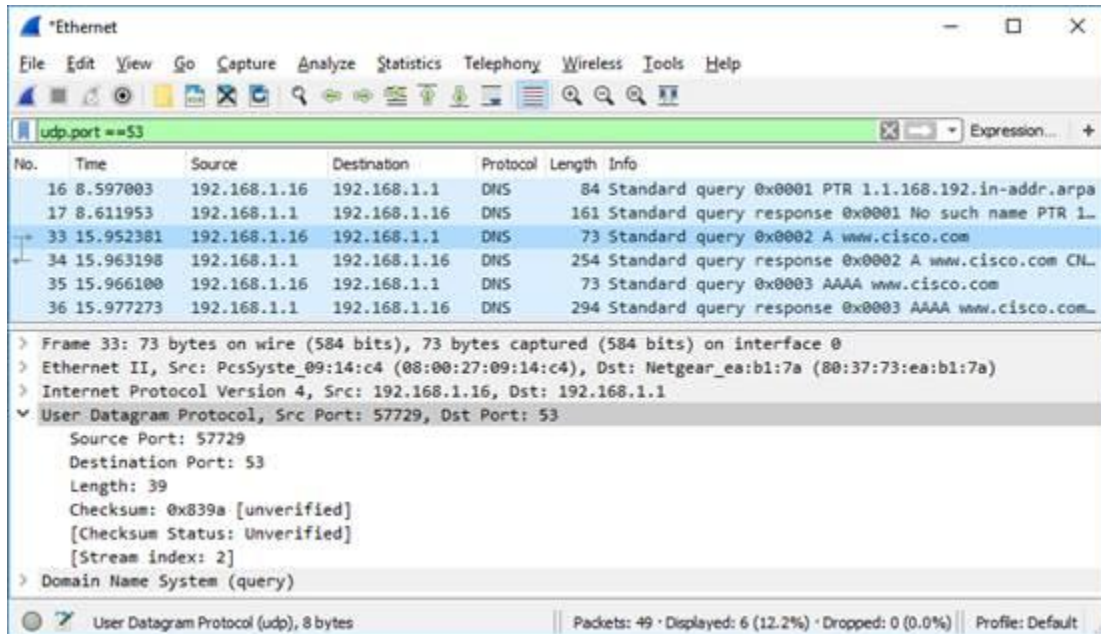


IP origen: fe80::bdb8:af80:a798:d127 → tu computadora (Wi-Fi Intel).

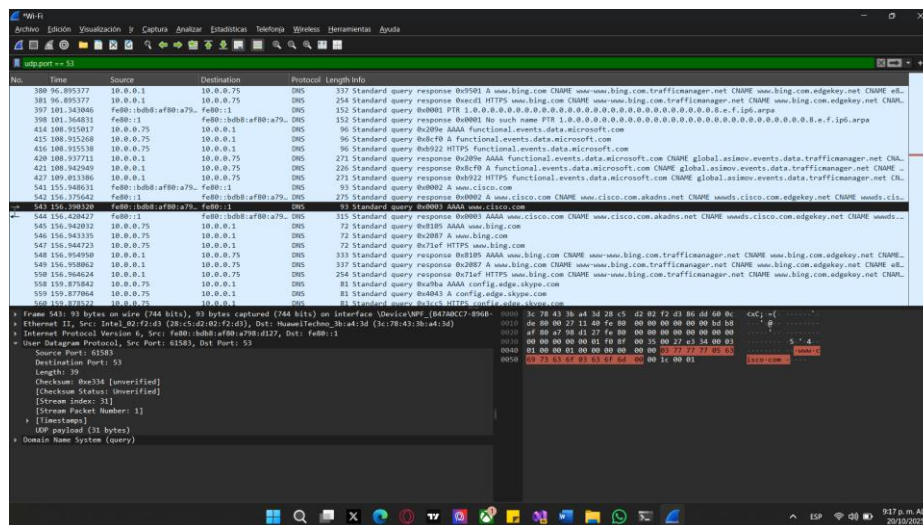
IP destino: fe80::1 → tu router Huawei.

Es una comunicación local entre tu PC y el router dentro de la red.

f. Expandan **User Datagram Protocol**. Observen los puertos de origen y de destino.



¿Cuáles son los puertos de origen y de destino? ¿Cuál es el número de puerto de DNS predeterminado?



Puerto de origen: 61583

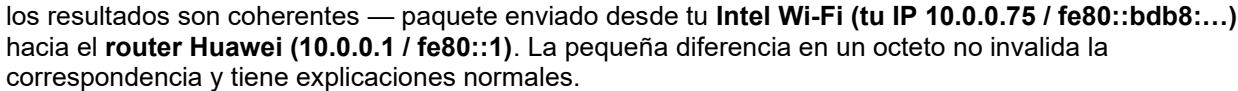
Puerto de destino: 53

Puerto DNS predeterminado: 53

g. Determine las direcciones IP y MAC de la computadora personal.

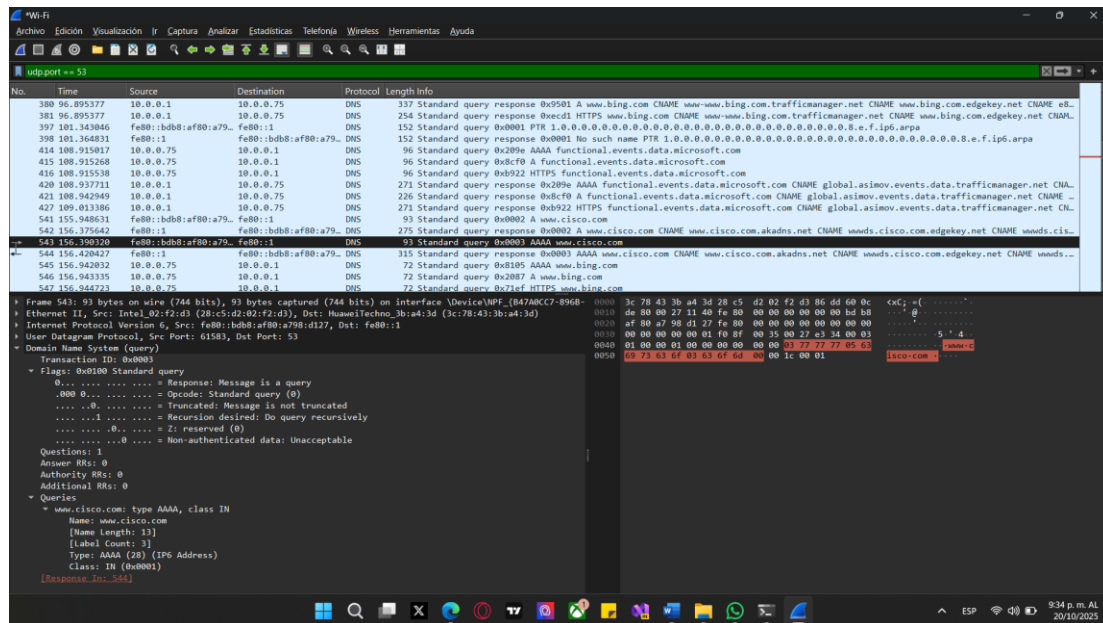
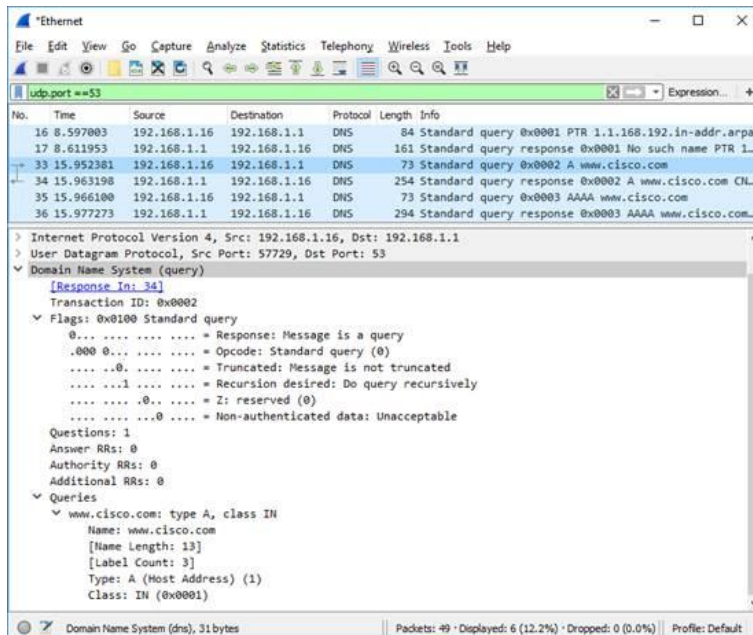
- 1) En el Símbolo de sistema de Windows, introduzca **arp -a** y **ipconfig /all** para registrar las direcciones MAC y las direcciones IP de la computadora personal.
- 2) Para Linux y macOS, introduzca **ifconfig** o **ip address** en la consola terminal.

Compare las direcciones MAC y las direcciones IP presentes en los resultados de Wireshark con los resultados obtenidos del símbolo del sistema o terminal. ¿Cuál es su opinión?



Práctica de laboratorio: Explorar tráfico DNS

- i. Observen los resultados. El marcador está definido para realizar la consulta recursivamente y así consultar la dirección IP en www.cisco.com.



Parte 3: Explorar tráfico de respuestas DNS

- a. Seleccione el paquete que contiene la **Standard query response (respuesta de consulta estándar)** y **A www.cisco.com** en la columna "Info" (Información).

The image shows a Wireshark packet capture analysis. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for packet capture and analysis. The filter bar shows the expression 'udp.port == 53'. The packet list pane displays six packets, all of which are DNS-related. The packet details pane shows the structure of the selected packet (Frame 34), including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (response). The packet bytes pane shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
16	8.597003	192.168.1.16	192.168.1.1	DNS	84	Standard query 0x0001 PTR 1.1.168.192.in-addr.arpa
17	8.611953	192.168.1.1	192.168.1.16	DNS	161	Standard query response 0x0001 No such name PTR 1.
33	15.952381	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0002 A www.cisco.com
34	15.963198	192.168.1.1	192.168.1.16	DNS	254	Standard query response 0x0002 A www.cisco.com CN.
35	15.966100	192.168.1.16	192.168.1.1	DNS	73	Standard query 0x0003 AAAA www.cisco.com
36	15.977273	192.168.1.1	192.168.1.16	DNS	294	Standard query response 0x0003 AAAA www.cisco.com

Frame 34: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface 0

- Ethernet II, Src: Netgear_ea:b1:7a (80:37:73:ea:b1:7a), Dst: PcsSyste_09:14:c4 (08:00:27:09:14:c4)
- Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.16
- User Datagram Protocol, Src Port: 53, Dst Port: 57729
- Domain Name System (response)

Frame (frame), 254 bytes

Packets: 49 · Displayed: 6 (12.2%) · Dropped: 0 (0.0%) Profile: Default

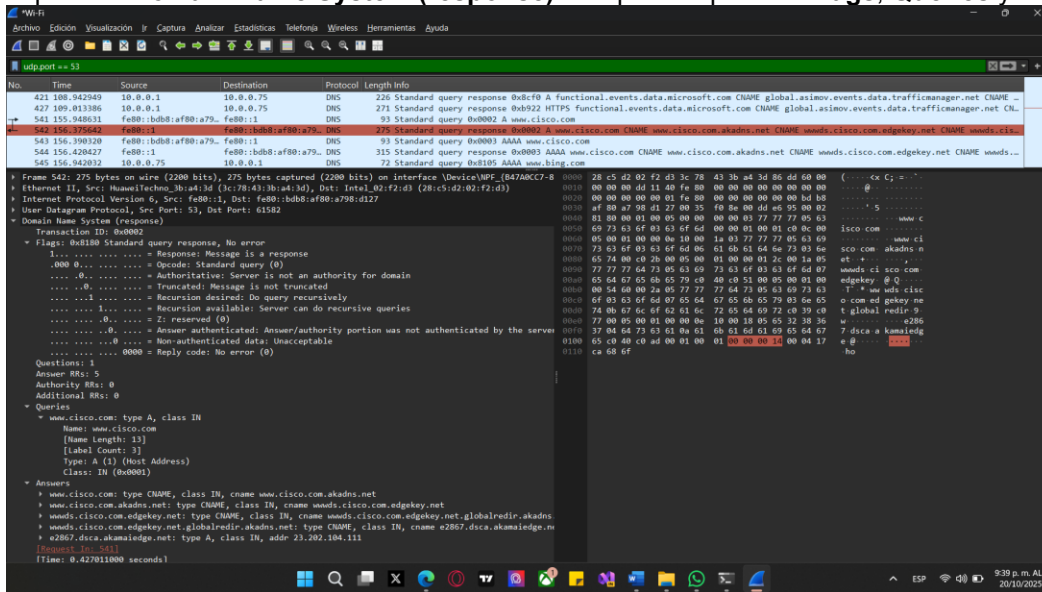
¿Cuáles son las direcciones MAC e IP y los números de puerto de origen y de destino? ¿Que similitudes y diferencias tienen con las direcciones presentes en los paquetes de consultas DNS?

[illegible]

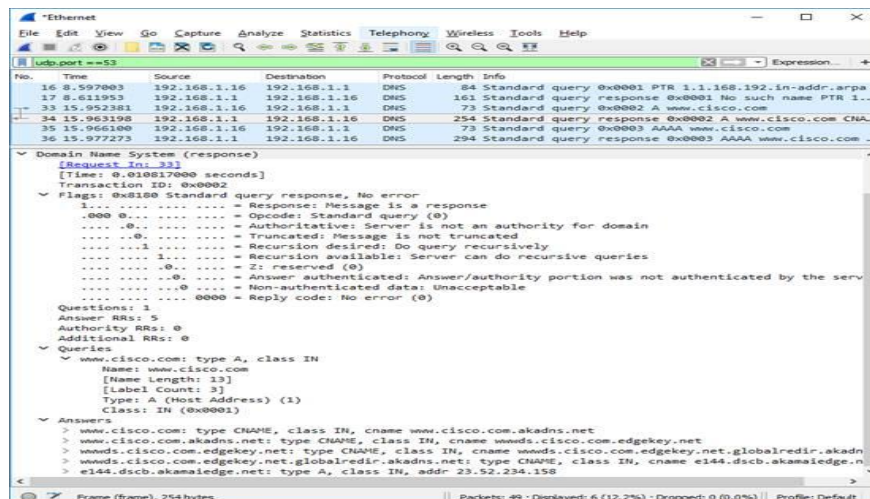
En la respuesta DNS, las direcciones MAC, IP y los puertos están invertidos respecto a la consulta: el router (fe80::1, MAC 3c:78:43:3b:a4:3d) responde a tu PC (fe80::bdb8:af80:a798:d127, MAC 28:c5:d2:02:f2:d3) usando el puerto 53.

Práctica de laboratorio: Explorar tráfico DNS

- b. Expandan Domain Name System (response). Después expandan **Flags**, **Queries** y **Answers**



- c. Observen los resultados.
¿El servidor DNS puede realizar consultas recursivas?
Sí, el servidor DNS **puede realizar consultas recursivas.**



- d. Observen los registros CNAME y A en los detalles de las Respuestas.

¿Qué similitudes y diferencias tienen con los resultados de nslookup?

Tanto en **Wireshark** como en **nslookup** aparecen los mismos registros **CNAME** y **A**, que muestran los alias del dominio (`www.cisco.com` → `wwwds.cisco.com.edgekey.net` → `e2867.dsca.akamaiedge.net`) y la **IP final (A)** que corresponde al servidor.

Reflexión

1. A partir de los resultados de Wireshark. ¿qué más pueden averiguar sobre la red cuando quitan el filtro?
Quitando el filtro ves todo el tráfico: hosts y sus IP/MAC, servicios y puertos activos, volúmenes de tráfico, dispositivos (routers/VMs) y posibles anomalías o tráfico no cifrado.
2. ¿De qué manera un atacante puede utilizar Wireshark para poner en riesgo la seguridad de sus redes?
Un atacante puede usar Wireshark para espiar credenciales, mapear la red, robar sesiones o, combinado con ARP spoofing, hacer MITM; mitígalo con cifrado (HTTPS/TLS/SSH/VPN), Wi-Fi segura (WPA2/3), segmentación, y medidas en switches (ARP/DHCP inspection, 802.1X) y detección de intrusos