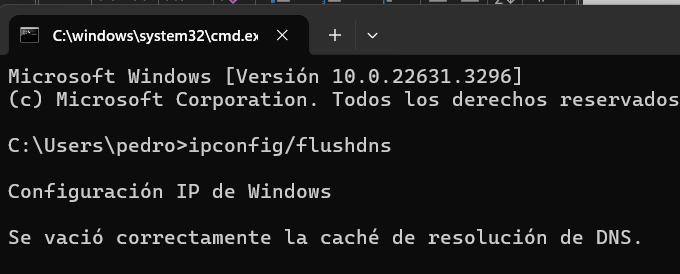
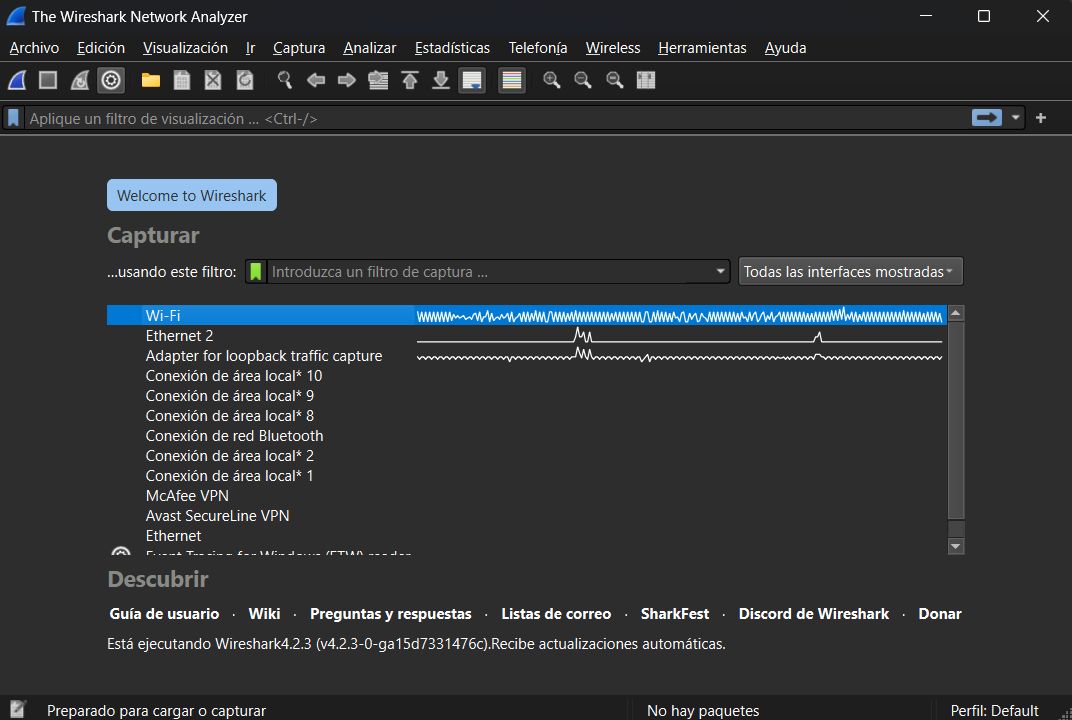
**Bitácora: Explorar tráfico DNS**

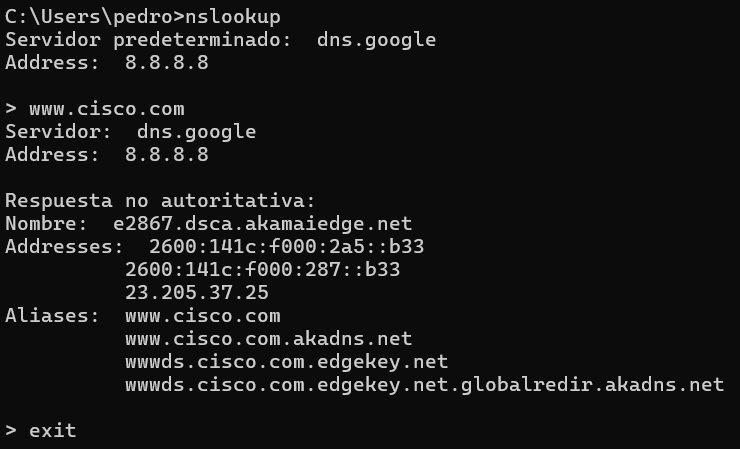
1. Teniendo instalado la aplicación de Wireshark, se abre cmd y se ejecuta el comando **ipconfig/flushdns**para borrar el caché del equipo.



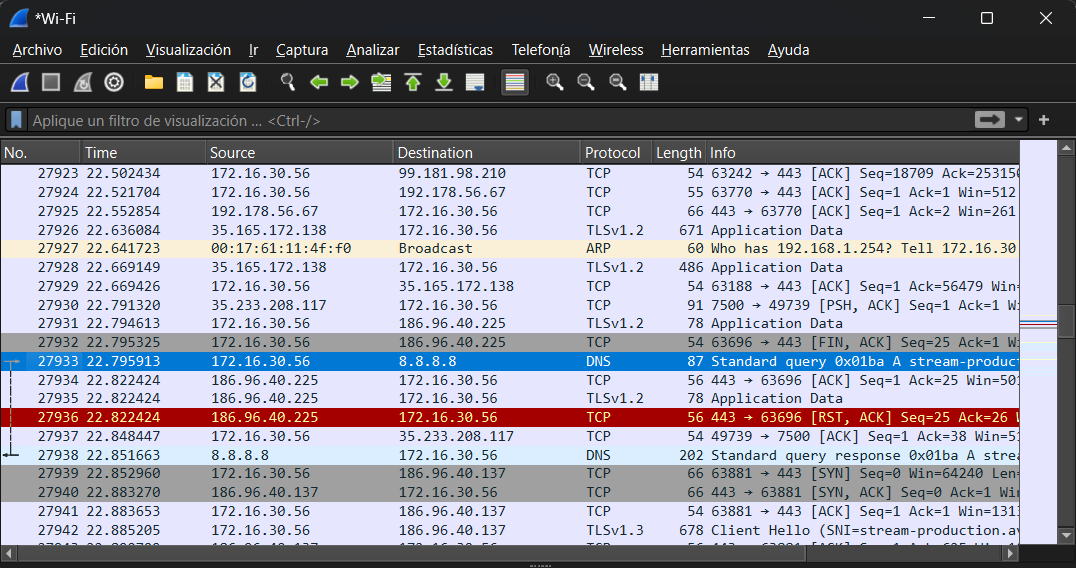
1. Abres Wireshark y das doble clic en la red para que empiece a capturar el trafico de las consultas.



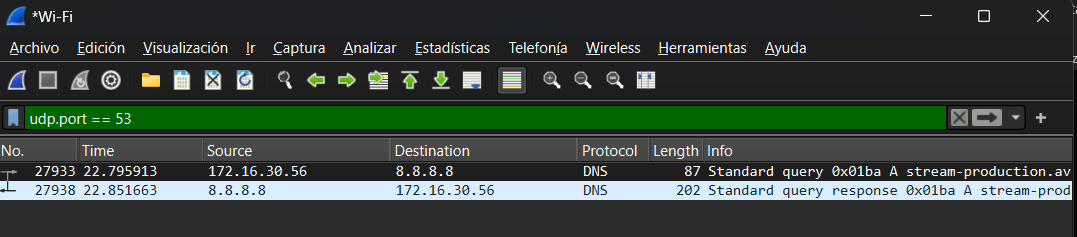
1. Vuelves al cmd y ejecutas el comando **nslookup** para capturar la los nombres y las IPs de los dominios y después das el comando **exit** para salir del modo.



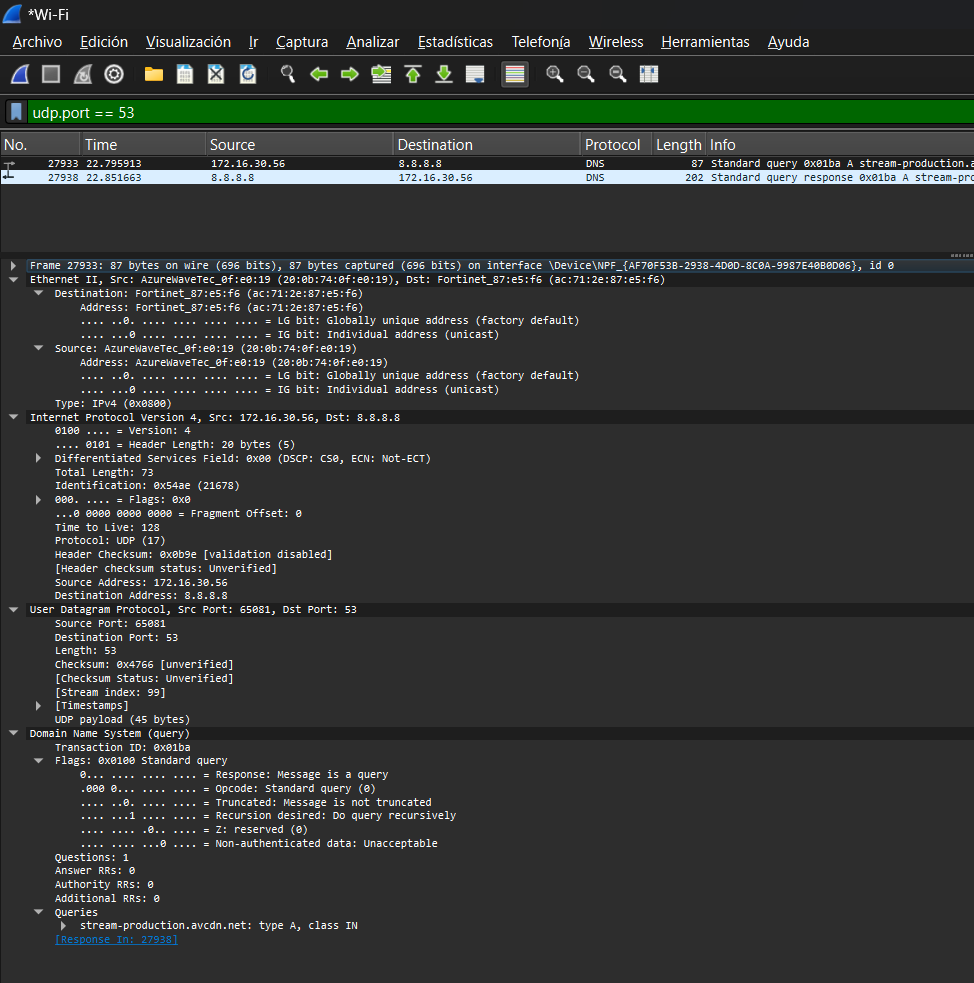
1. Regresas a la aplicación y detienes la captura de paquetes.



1. Ejecutas en el buscador (que aplica como filtro) lo siguiente **udp.port == 53** para mostrar únicamente los paquetes DNS.



1. Al hacer doble clic en **Estándar query 0x0002 A www.cisco.com**, se visualiza todos los detalles del paquete.



1. Regresamos al cmd e introducimos los comandos **arp -a** e **ipconfig/all** para hacer el registro de las direcciones MAC e IP del equipo.
2. Este puede observar el tráfico de la red y puede obtener información confidencial en los detalles del
3. paquete si el tráfico no está encriptado



1. Preguntas que responder.
   1. ¿Qué sucedió con las direcciones MAC de origen y de destino? ¿Con qué interfaces de red están asociadas estas direcciones MAC?  
      *La dirección MAC de destino está asociada con el Gateway determinado; Si existe un servidor DNS local, la dirección MAC seria la dirección DNS local.*
   2. ¿Cuáles son las direcciones IP de origen y destino? ¿Con qué interfaces de red están asociadas estas direcciones IP?  
      *La dirección IP de origen está asociada con la NIC de la PC y la dirección IP de destino está asociada con el servidor DNS.*
   3. ¿Cuáles son los puertos de origen y de destino? ¿Cuál es el número de puerto de DNS predeterminado?  
      *El número de puerto de origen es 58461 y el puerto de destino es 53, el cual es número de puesto de DNS predeterminado.*
   4. ¿Cuáles son las direcciones MAC e IP y los números de puerto de origen y de destino? ¿Qué similitudes y diferencias tienen con las direcciones presentes en los paquetes de consultas DNS?  
      *La IP de origen, la dirección MAC y el número de puerto del paquete de consulta son ahora direcciones de destino. La IP de destino, la dirección MAC y el número de puerto en el paquete de consulta ahora son direcciones de origen.*
   5. ¿El servidor DNS puede realizar consultas recursivas?  
      *Si*
   6. ¿Qué similitudes y diferencias tienen con los resultados de nslookup?  
      *De que los resultados deben ser los mismos.*
   7. A partir de los resultados de Wireshark. ¿qué más pueden averiguar sobre la red cuando quitan el filtro?  
      *Se puede obtener información de otros dispositivos y LAN.*
   8. ¿De qué manera un atacante puede utilizar Wireshark para poner en riesgo la seguridad de sus redes?  
      *Este puede observar el tráfico de la red y puede obtener información confidencial en los detalles del paquete si el tráfico no está encriptado*