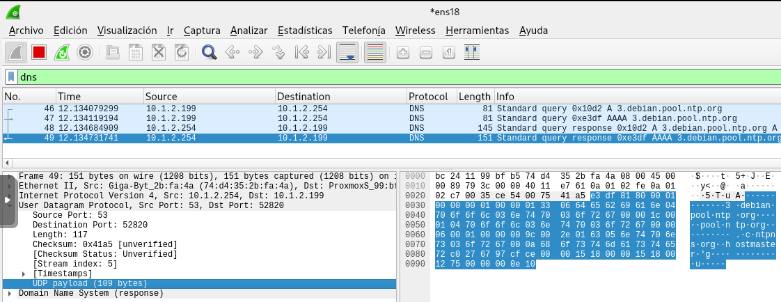
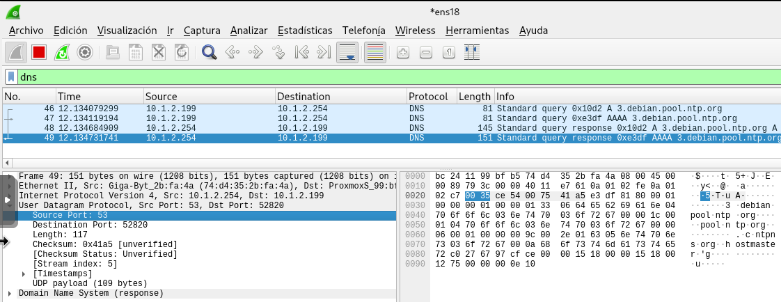
1. **Locate the DNS query and response messages. Are then sent over UDP or TCP?**

En Wireshark, en los detalles del paquete, puedes ver el campo Protocol y debería indicar si es UDP o TCP. En la mayoría de las consultas DNS, será UDP.



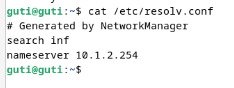
1. **What is the destination port for the DNS query message? What is the source port of DNS response messages?**

En Wireshark, cuando examinas el paquete de la consulta DNS, el puerto de destino será el puerto 53, ya que es el puerto estándar para las consultas DNS

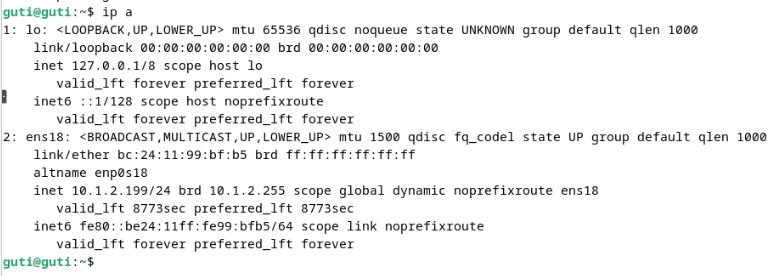


1. **To what IP address is the DNS query message sent? Use ipconfig to determine the IP address of your local DNS server. Are these two IP addresses the same?**

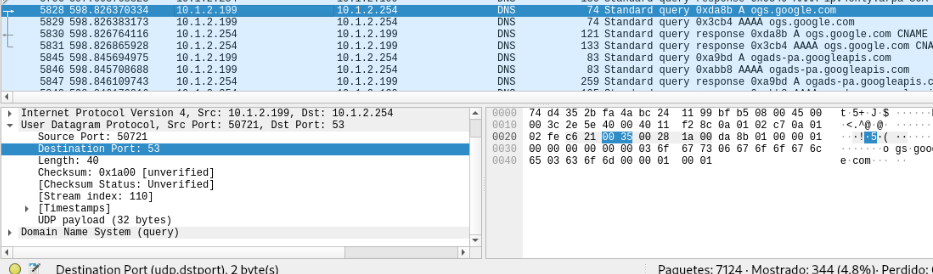
Para conocer la IP de tu servidor DNS local, en Debian puedes utilizar el comando cat /etc/resolv.conf:



Esto te dará la IP de tu servidor DNS. En Wireshark, podrás ver que la consulta DNS se dirige a esa misma dirección IP.

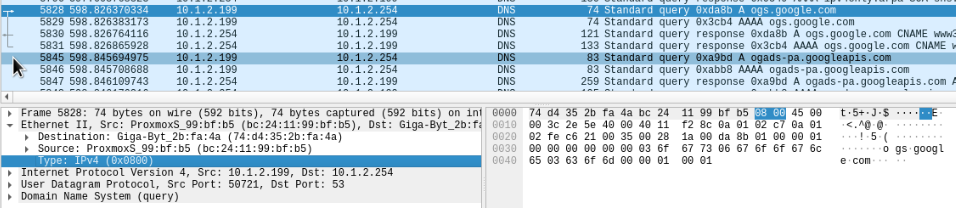


Por último comprobaremos desde Wireshark el puerto correspondiente, que como podemos ver es el 53



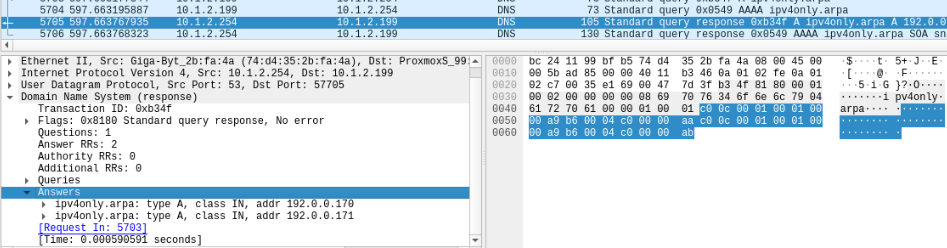
1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

Es una consulta de tipo IPv4. No, las respuestas generalmente no están presentes en la consulta, ya que es un mensaje que solicita una resolución

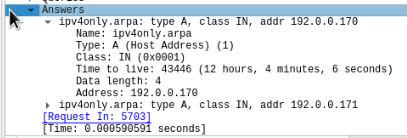


1. **Examine the DNS response message. How many “answers” are provided? What do each of these answers contain?**

Como podemos ver el mensaje contiene dos respuestas

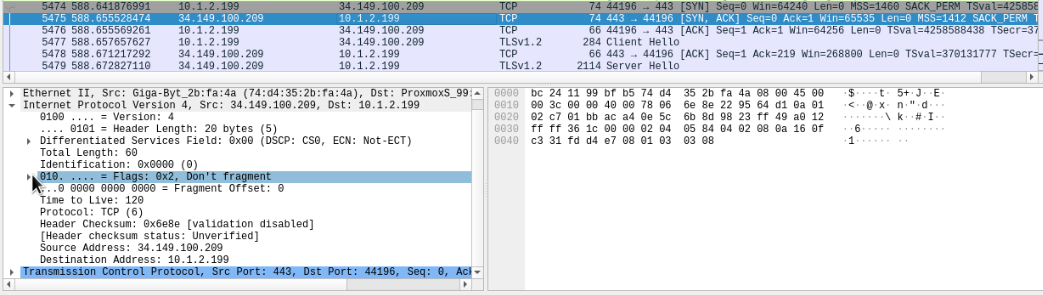


Estas, listan las respuestas que el servidor DNS proporciona. Pueden ser direcciones IP (en tipo A) o alias de dominio.



1. **Consider the subsequent TCP SYN packet sent by your host. Does the destination IP address of the SYN packet correspond to any of the IP addresses provided in the DNS response message?**

Como podemos ver el paquete SYN contiene la correspondiente dirección IP de la máquina destino (10.1.2.199).

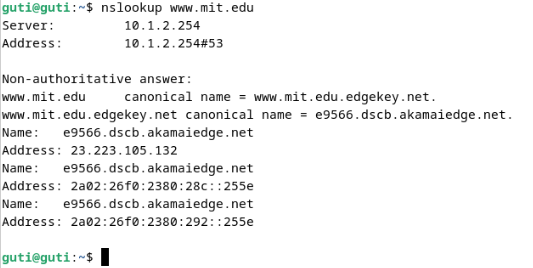


1. **This web page contains images. Before retrieving each image, does your host issue new DNS queries?**

* *Start packet capture.*
* *Do an nslookup on* [*www.mit.edu*](http://www.mit.edu)
* *Stop packet capture.*

Para realizar esta actividad comenzaremos iniciando una captura en wireshark.

A continuación abriremos una terminal y ejecutaremos el comando: nslookup [www.mit.edu](http://www.mit.edu)



Este comando hará una consulta DNS para obtener la dirección IP de www.mit.edu. Al mismo tiempo, podrás ver cómo Wireshark captura el paquete de consulta y la respuesta DNS.

Por último, una vez que hayas completado la consulta DNS y se haya capturado suficiente información, haz clic en "Detener captura" en Wireshark

1. **What is the destination port for the DNS query message? What is the source port of DNS response message?**

El puerto de destino para las consultas DNS siempre es el puerto 53, que es el puerto estándar utilizado por el protocolo DNS.

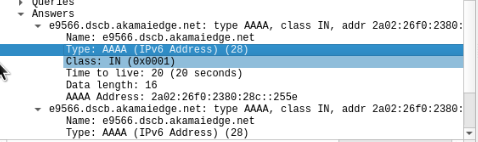
En el caso de la respuesta DNS, el puerto de origen puede ser 53, que es el puerto estándar en el servidor DNS que está respondiendo a la consulta.

1. **To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?**

La dirección es 10.1.2.199. Si, la dirección IP corresponde con el servidor local

1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

Las consultas DNS para la resolución de nombres de dominio son de tipo A o AAAA.

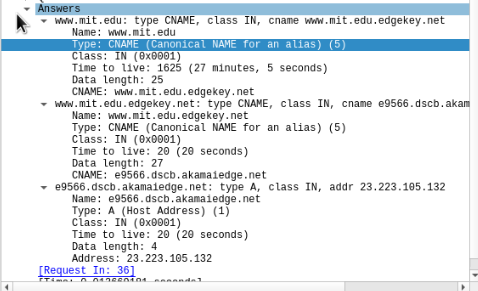


El mensaje de consulta no contiene respuestas, ya que solo solicita una respuesta al servidor DNS.

1. **Examine the DNS response message. How many “answers” are provided? Whatvdo each of these answers contain?**

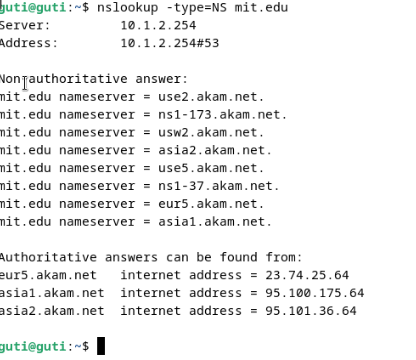
La cantidad de respuestas depende del mensaje, en el caso del mensaje donde hemos hecho la solicitud a mit.edu podemos ver que la respuesta contiene 3 respuestas.

1. **Provide a screenshot.**



**Now repeat the previous experiment, but instead issue the command:**

**nslookup –type=NS mit.edu**



1. **To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server?**

Se envía hacia la dirección: 10.1.2.254 a través del puerto UDP (17). Si, si lo es.

1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

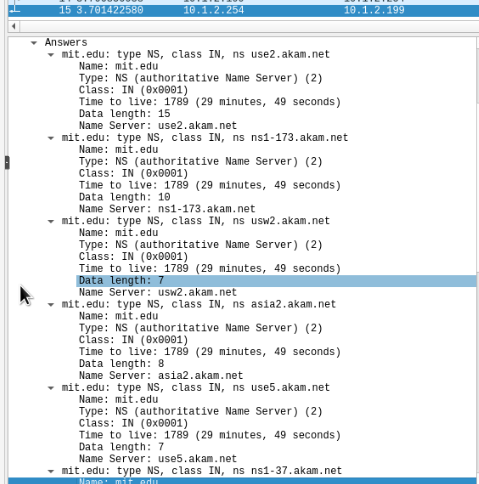
El tipo de mensaje es NS (authoritative Name Server).

1. **Examine the DNS response message. What MIT nameservers does the response message provide? Does this response message also provide the IP addresses of the MIT namesers?**

Al realizar una consulta para mit.edu usando nslookup, la respuesta debe incluir registros NS (servidores de nombres) para el dominio.

También revisa si se proporcionan las direcciones IP de esos servidores de nombres.

1. **Provide a screenshot.**



1. **To what IP address is the DNS query message sent? Is this the IP address of your default local DNS server? If not, what does the IP address correspond to?**

En el caso de consultas a servidores externos, si el servidor DNS local no es utilizado, la IP puede pertenecer a un servicio público de DNS como Google DNS o Cloudflare.

1. **Examine the DNS query message. What “Type” of DNS query is it? Does the query message contain any “answers”?**

La consulta es de tipo A para la dirección IPv4

1. **Examine the DNS response message. How many “answers” are provided? What does each of these answers contain?**

Como se mencionó antes, la respuesta debe contener registros como A (para direcciones IP) y puede haber múltiples respuestas.

1. **Provide a screenshot.**

