**SEGURIDAD INFORMÁTICA**

**PRÁCTICA 1 (PARTE II)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Alumno** | **Apellidos** | **Nombre** | **Curso** |
| **1** | **Garrido Cobo** | **Javier** | **4** |
| **2** | **Viñals Lage** | **Diego** | **4** |
| **3** |  |  |  |

Los objetivos de esta segunda parte de la práctica 1 son los siguientes:

**I. SERVICIO DNS**

1. Estudiar el servicio DNS:
   1. Proceso de resolución de nombres mediante el wireshark
   2. Archivo de zona
   3. Registros de recursos
2. Instalación y configuración en Linux del servidor DNS (BIND9)
3. Configuración del cliente DNS.
4. Instalación de un servidor Web en Linux
5. Conexión del cliente para acceder a la página web

Para ello instalaremos el servicio BIND9 y un servidor http en Linux (Apache o Nginx)

1. Investigar sobre los ataques que pueden sufrir este tipo de servidores

**ACTIVIDADES**

1. **Instalar un servidor DNS en Linux y creación de una zona con el siguiente nombre:** Nombre de la zona DNS: “los primeros apellidos de cada uno de los miembros del grupo separados por guion”.com.

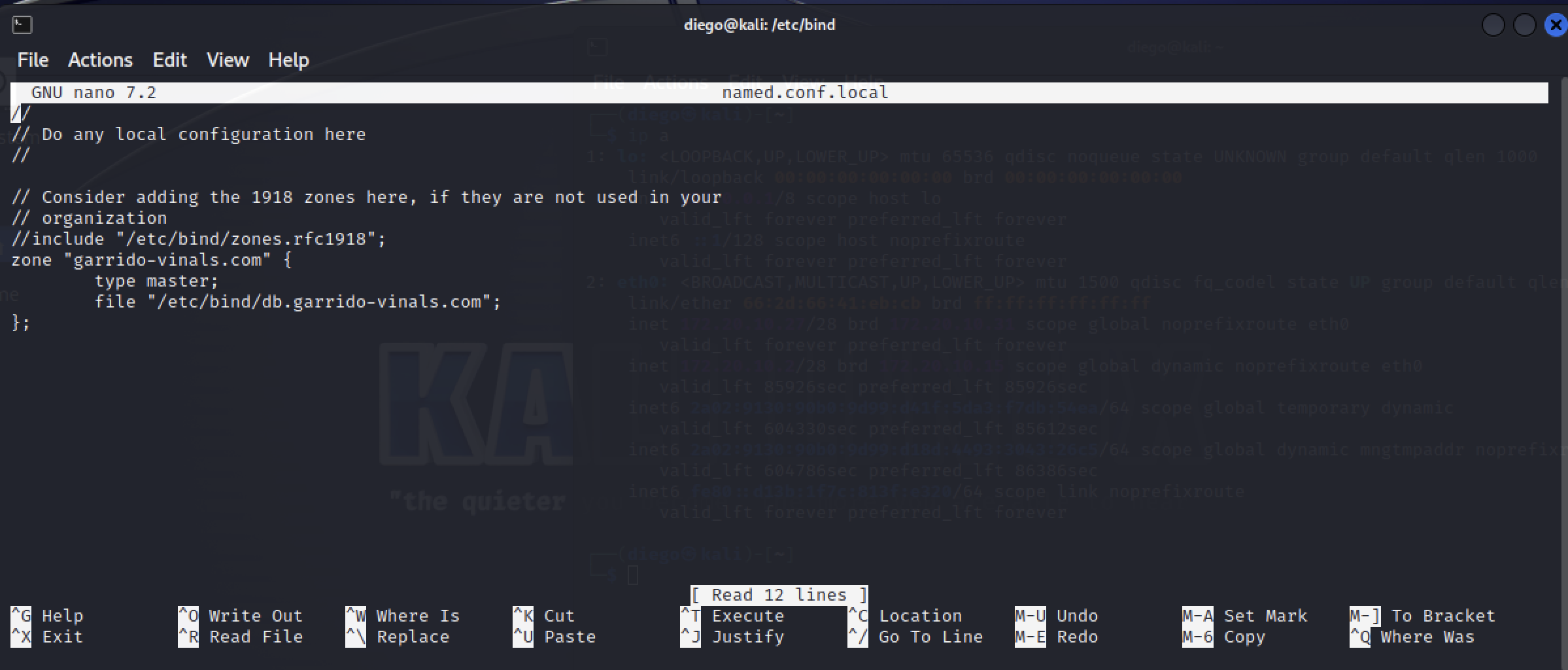
**Ejemplo: si fuese mi apellido (Malagón) junto con alguien cuyo apellido fuese García el dominio sería: malagon-garcia.com**

* 1. ¿Cómo se instala y configura el servicio DNS?
     1. Se instala mediante la orden **sudo apt-get install bind9**
     2. Configuración del archivo de zona

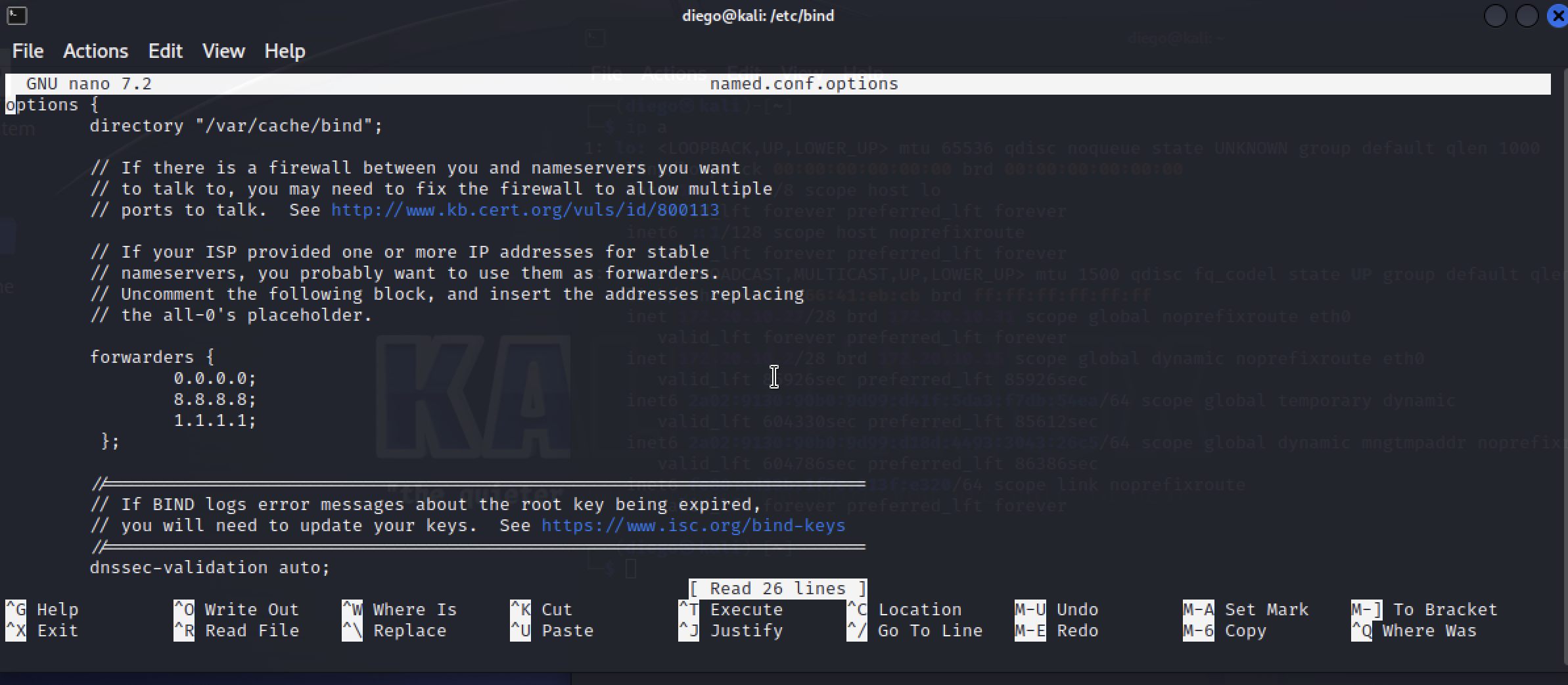
Interfaz de usuario gráfica

Descripción generada automáticamente

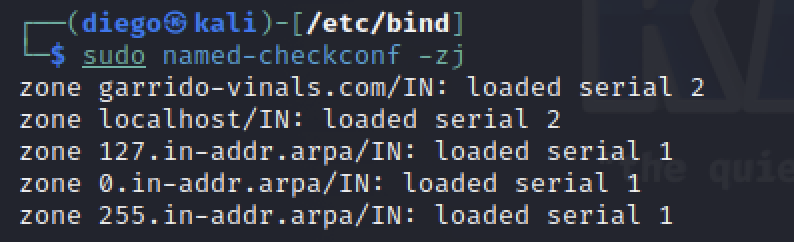
* + 1. Se declara la zona en el fichero **named.conf.local**
    2. Declaración de la zona y del fichero de zona



* + 1. Se declaran los servidores DNS a los que se les pueden reenviar las peticiones (llamados forwarders).Para ello habrá que configurar nuestro servidor DNS para que reenvíe esta petición a cualquier otro servidor DNS (8.8.8.8 de Google o mejor el 1.1.1.1 de Cloudfare)



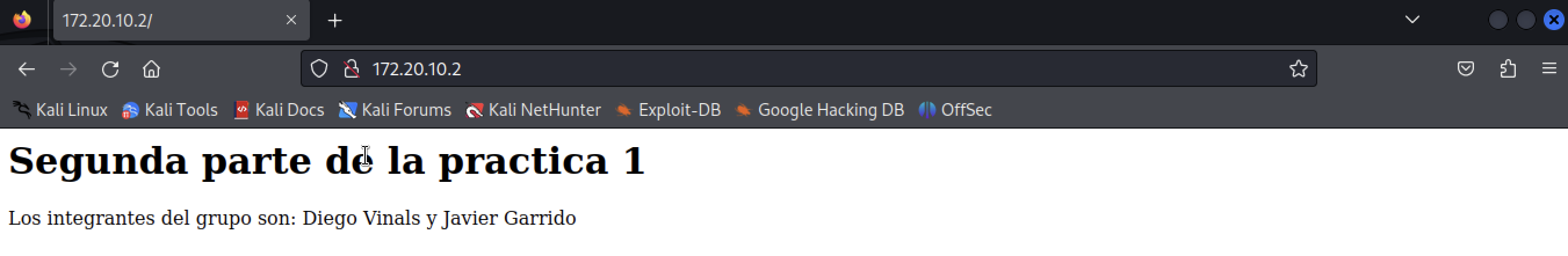
* + 1. Se reinicia el demonio con la orden **sudo service named restart**
    2. Mediante la orden named-checkconf -zj comprueba que tu fichero de zona está bien definido.



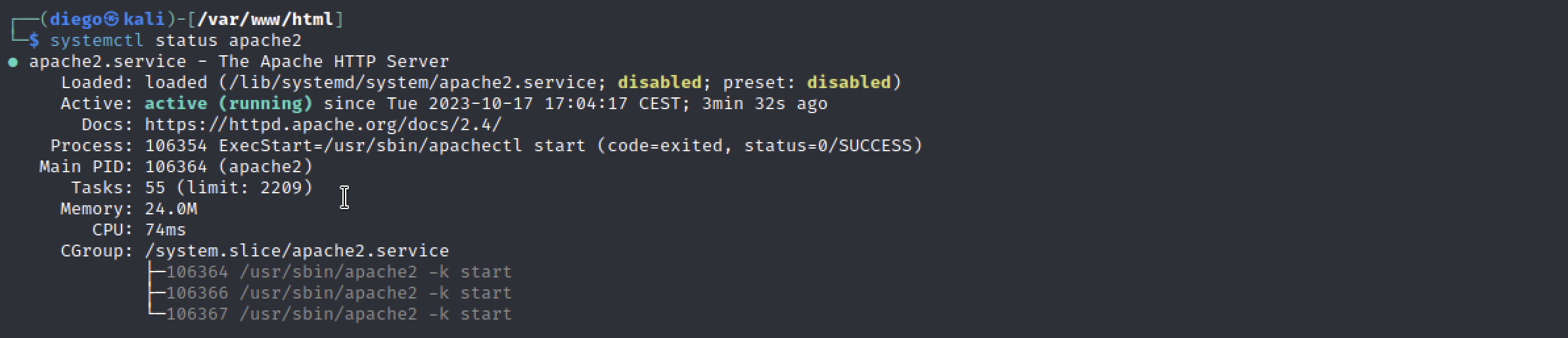
1. **Instalar un servidor Web en Linux (Nginx, Apache o cualquier otro) y publicar una página web de prueba en la que aparezca como mínimo el texto “Segunda parte de la práctica 1 y los nombres de los componentes del grupo”.**

**NOTA IMPORTANTE: En esta práctica el servidor DNS y el servidor web van a coincidir en el mismo equipo, pero en general esto no es así y el servidor DNS y el servidor web son equipos diferentes.**

* 1. ¿Cómo funciona y cómo se instala?
     1. Se instala mediante la orden **sudo apt-get install apache2**
     2. Configuro mi sitio web y la página index en el directorio **/var/www/html/**
  2. Demuestra que el servidor apache está operativo
     1. Puedo comprobar que funciona desde mi propio Linux accediendo desde el navegador a la dirección IP 127.0.0.1



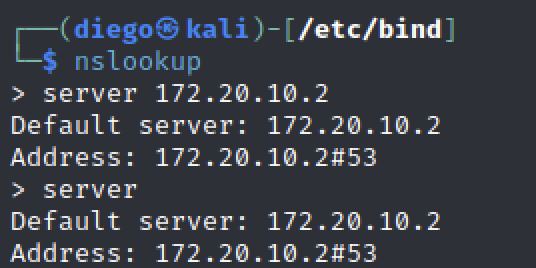
* + 1. Mostrando evidencias de que el demonio está arrancado



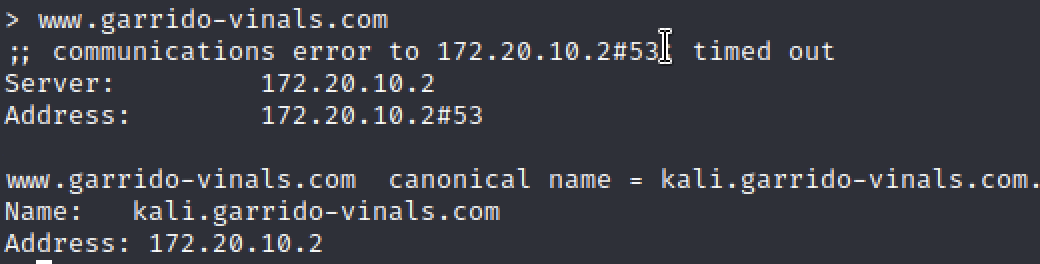
* + 1. Mediante los comandos y las evidencias que el puerto del servicio HTTP está escuchando



1. **Comprobación del servidor DNS con nslookup**
   1. Mediante la orden nslookup obtener la IP del servidor DNS predeterminado (escribiendo server). Esta IP debería ser la IP de nuestro Linux, que es el servidor DNS.



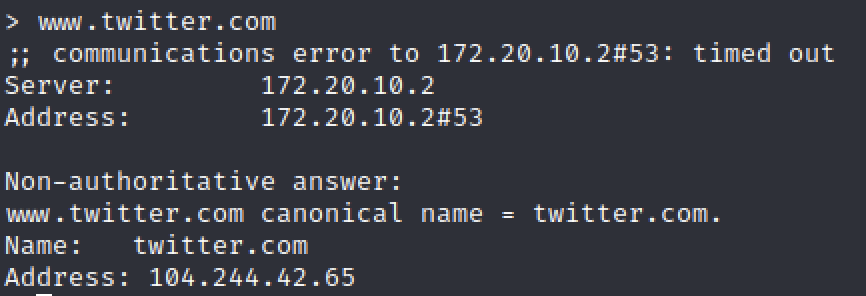
* 1. Preguntar por [www.malagon-garcia.com](http://www.malagon-garcia.com) (en mi caso) y comprobar que nos devuelve la IP del servidor web (que en este caso es la misma que la del servidor DNS puesto que los dos servicios coinciden en el mismo equipo, pero como hemos dicho, no es lo habitual).



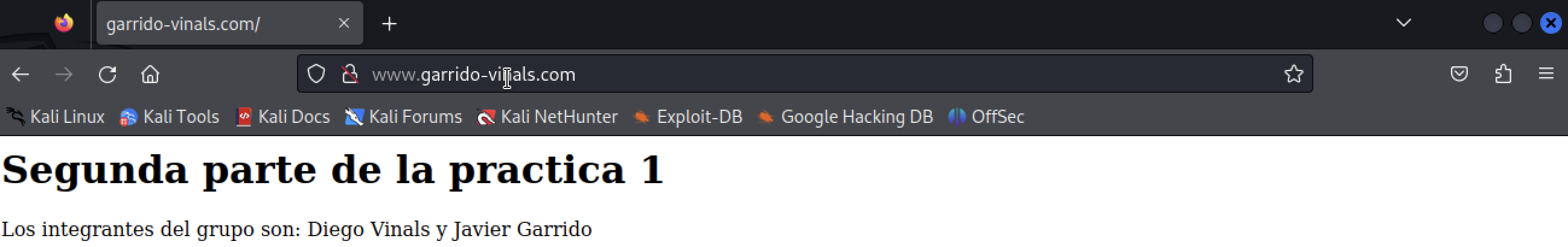
* 1. Siempre que carga la página WEB mediante la URL, ¿Se hace una consulta al DNS?

**Si, cuando abres tu navegador y escribes una dirección web (como "www.ejemplo.com"), tu navegador no sabe automáticamente a qué servidor conectarse. Así que, para averiguarlo, hace una llamada a un directorio llamado DNS. Este directorio contiene todas las direcciones de sitios web y sus nombres fáciles de recordar, como "ejemplo.com." cada vez que visitas una página web, el navegador hace una llamada rápida al DNS para averiguar dónde debe ir.**

* 1. **Resolución de una URL externa**: preguntar por [www.twitter.com](http://www.twitter.com) y comprobar que nos devuelve la IP del servidor web de Twitter.



1. **Conexión del cliente a un servidor web mediante la dirección:** [**http://www.malagon-garcia.com**](http://www.malagon-garcia.com) **(ejemplo del nombre que he escrito antes; cada uno que ponga el suyo)** 
   1. Muestre el navegador del cliente con su URL donde se vea la página web con la URL donde aparezca el nombre del dominio creado.



* 1. ¿Qué diferencia hay entre poner la URL o poner la IP del servidor WEB en el navegador?

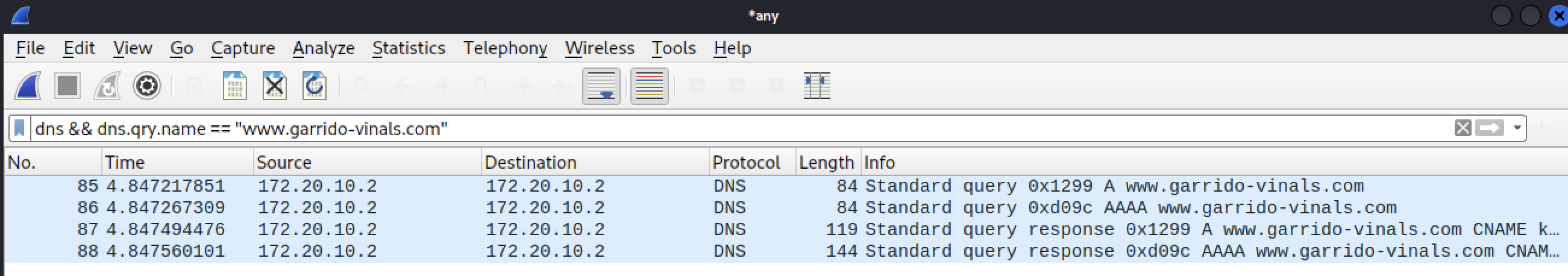
**Usar una URL en lugar de una dirección IP en el navegador es más fácil para las personas, ya que las URLs son nombres de sitios web que recordamos fácilmente. Cuando usamos una URL, el navegador realiza una búsqueda para encontrar la dirección IP correspondiente al sitio web. Por otro lado, ingresar directamente una dirección IP es más técnico y menos amigable para los usuarios, ya que las direcciones IP son secuencias numéricas difíciles de recordar. Además, si cambias la dirección IP del servidor, los usuarios deben conocer la nueva IP, mientras que con una URL, los cambios pueden hacerse de manera más flexible y transparente para los usuarios.**

* 1. Si en el fichero de zona define la URL ftp. midominio.com (en su caso malagon-garcia.com, pero incluyendo la palabra ftp al principio) y lo asocia a la IP del servidor WEB, ¿qué sucede cuando escribe la URL ftp.midominio.com en el navegador?

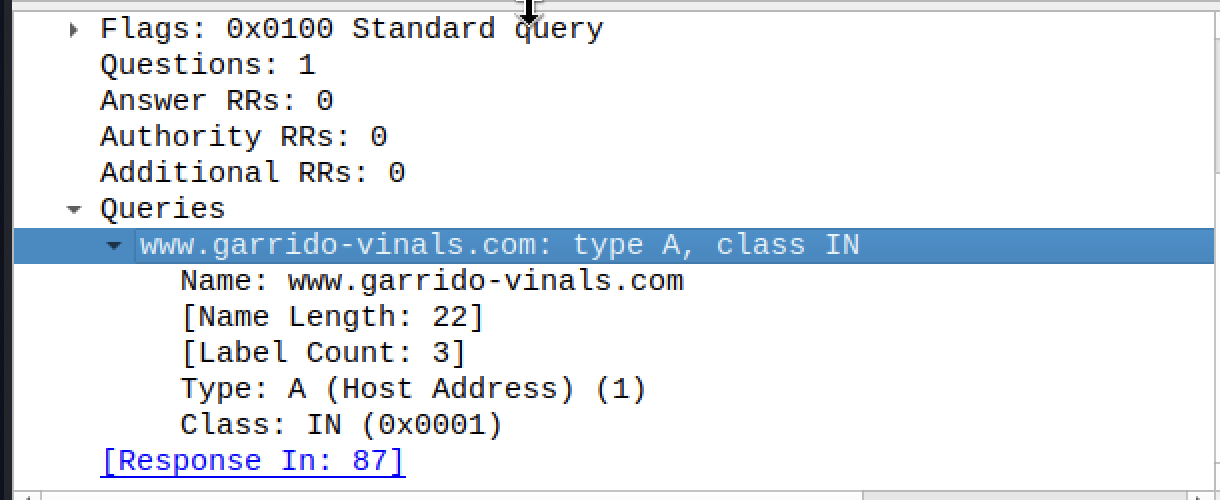
**Cuando defines en un archivo de zona la URL "ftp.midominio.com" y la asocia a la IP del servidor web, al escribir la URL "ftp.midominio.com" en el navegador, lo que sucede es que el navegador intentará acceder al servidor web utilizando el subdominio "ftp" como parte de la dirección. Esto significa que el navegador buscará la dirección IP del servidor web asociada con "ftp.midominio.com" y cargará el sitio web correspondiente.**

**En otras palabras, la URL "ftp.midominio.com" dirige el navegador a buscar el servidor web al que está asociado el subdominio "ftp" dentro del dominio "midominio.com". Si la configuración DNS y del servidor web se ha realizado correctamente, se cargará el sitio web relacionado con "ftp.midominio.com" en el navegador. Esto permite tener múltiples subdominios en un dominio principal, cada uno apuntando a contenido o servicios específicos en el servidor web.**

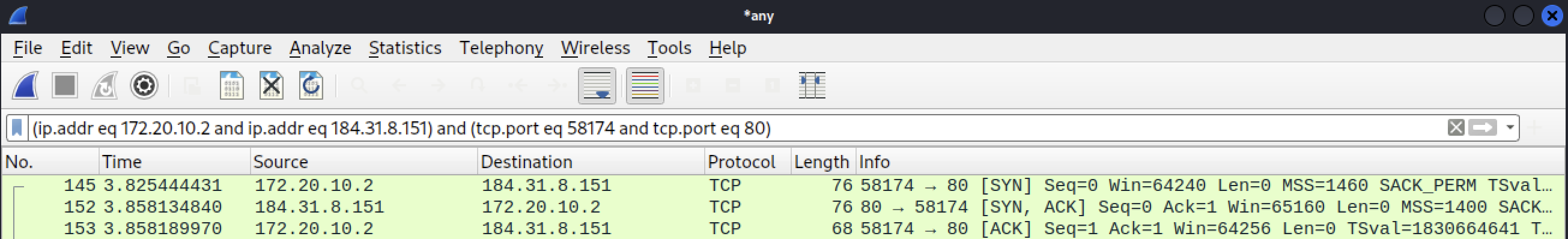
1. **Uso de un sniffer como el Wireshark para:**
   1. Identificar los paquetes que intervienen en la resolución de nombres entre el cliente y el servidor DNS mediante un ejemplo



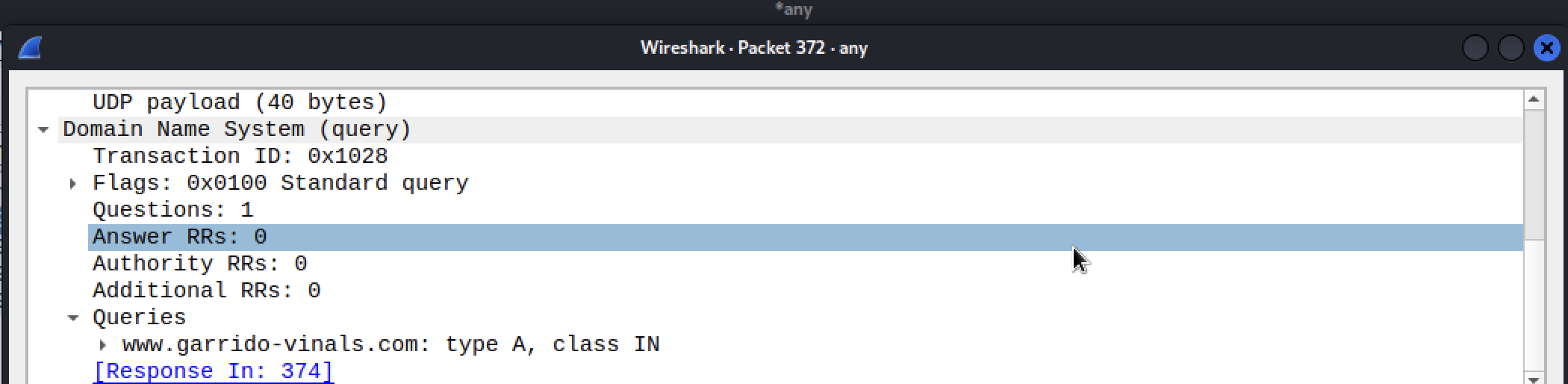
* 1. ¿Qué protocolo se utiliza en esta resolución? **UPD con puerto 53**
  2. ¿Qué tipo de registro es www? **Type A**



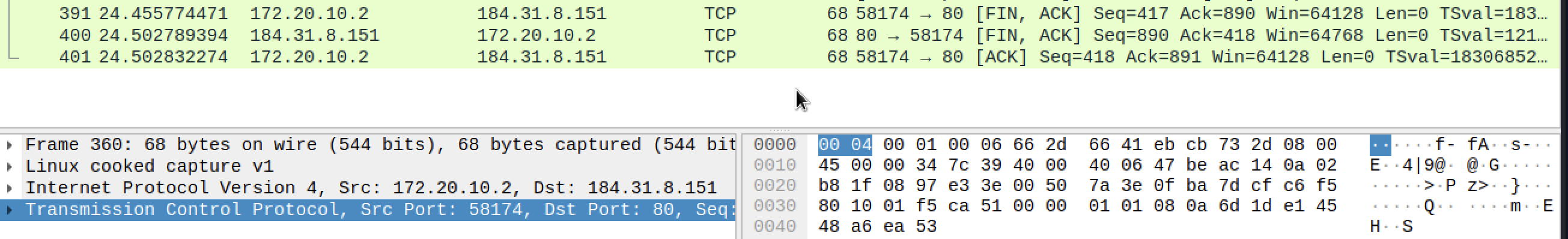
* 1. Identificar los paquetes que intervienen en la conexión cliente-servidor web:
     1. Three-way handshake



* + 1. Obtención de la página web



* + 1. Fin de conexión



1. **Parte de investigación** 
   1. Investigar y contar brevemente en qué consisten los principales ataques que puede sufrir un servidor DNS. Explicar uno de ellos y buscar un ejemplo real de ataque sufrido por un servidor DNS junto con sus consecuencias

**Existen varios tipos de ataque que puede sufrir un servidor DNS, el que vamos a explicar es el ataque de denegación de servicio.**

**Los atacantes llenan el servidor DNS con mucho volumen de tráfico falso, lo que sobrecarga el servidor y hace que no pueda responder a solicitudes reales.**

**En octubre de 2016, ocurrió un incidente real en el que un ataque DDoS masivo impactó al proveedor de servicios DNS llamado Dyn. Este ataque tuvo graves consecuencias, ya que provocó la caída de varios sitios web populares, entre ellos Twitter, Reddit, Spotify y Airbnb. Lo que hicieron los atacantes fue aprovechar una red de dispositivos de Internet de las cosas (IoT) que habían sido comprometidos previamente. Estos dispositivos, como cámaras de seguridad y enrutadores, se utilizaron para enviar una gran cantidad de tráfico de datos falso hacia los servidores DNS de Dyn. Esta avalancha de tráfico abrumador congestionó los servidores, lo que resultó en la interrupción del servicio para un gran número de usuarios de Internet. Este incidente ilustra la importancia de proteger los servidores DNS y estar preparados para defenderse contra ataques DDoS para garantizar el funcionamiento ininterrumpido de los servicios en línea.** [1]

**IMPORTANTE: Si se detecta que esta parte ha sido copiada la práctica será calificada con un 0.**

# Bibliografía

|  |  |
| --- | --- |
| [1] | G. González, «Genbeta,» 27 Octubre 2016. [En línea]. Available: https://www.genbeta.com/actualidad/el-ataque-contra-dyn-dns-que-sacudio-internet-fue-probablemente-obra-de-hackers-amateurs. [Último acceso: 19 Octubre 2023]. |

# INSTRUCCIONES

* Entrega:
  + Un archivo PDF a partir de este documento de Word con las respuestas (las que están señaladas en rojo) y los pantallazos pedidos.
* Los ejercicios **SÓLO** podrán realizarse en grupos de dos alumnos como máximo. Si hay un grupo de tres se debe escribir un correo al profesor para notificárselo (no hace falta volver a hacerlo si ya se ha hecho para la primera parte de la práctica). **No se permiten entregas de prácticas por grupos de tres o más alumnos que no hayan sido notificadas en fecha al profesor.**

* El nombre del fichero entregado serán los apellidos de los alumnos separados por guion.
* Se deberán usar al menos dos equipos diferentes (cliente y servidor) o realizarlo mediante máquinas virtuales.
* **La fecha límite de entrega será el lunes 23 de octubre a las 23 horas.**
* No se recogerán memorias entregadas fuera de fecha o por otro medio distinto de los indicados (como por ejemplo el mail). Debe entregarse en el apartado correspondiente en el campus virtual.