Práctica 4:

Requisitos:

- Haber hecho la práctica 3.
- Durante todo el proceso de la práctica deberán hacerse capturas de imagen de cada uno de los pasos dados así como capturas y almacenaje de los paquetes de wireshark. Algunos de ellos serán solicitados por el profesor una vez concluida la práctica.

Otra forma de conseguir que el cliente LinuxXX funcione con systemd-resolved

Puedes mantener systemd-resolved activado y decirle qué servidor DNS quieres que se utilice y que no use el DNS STUB. Para ello, en el archivo /etc/systemd/resolved.conf tienes que añadir las líneas:

```
DNS=10.0.128+XX.2

DNSStubListener=no
```

Antes de empezar:

- Recuerda que tienes a tu disposición la documentación de Zytrax donde puedes consultar sobre conceptos y sintaxis.
- Sustituye el valor 'XX' por tu número de puesto asignado que venimos utilizando
- Toma nota de todo lo que vayas haciendo, incluyendo errores y soluciones sobre los mismos, así como capturas
- Debes utilizar el cliente LinuxXX para hacer todas las consultas DNS de prueba
- Recuerda que cada vez que actualices un fichero de zona tienes que incrementar el número de serie del SOA
- Para poder trabajar mejor es necesario instalar wireshark en el cliente LinuxXX

Prueba:

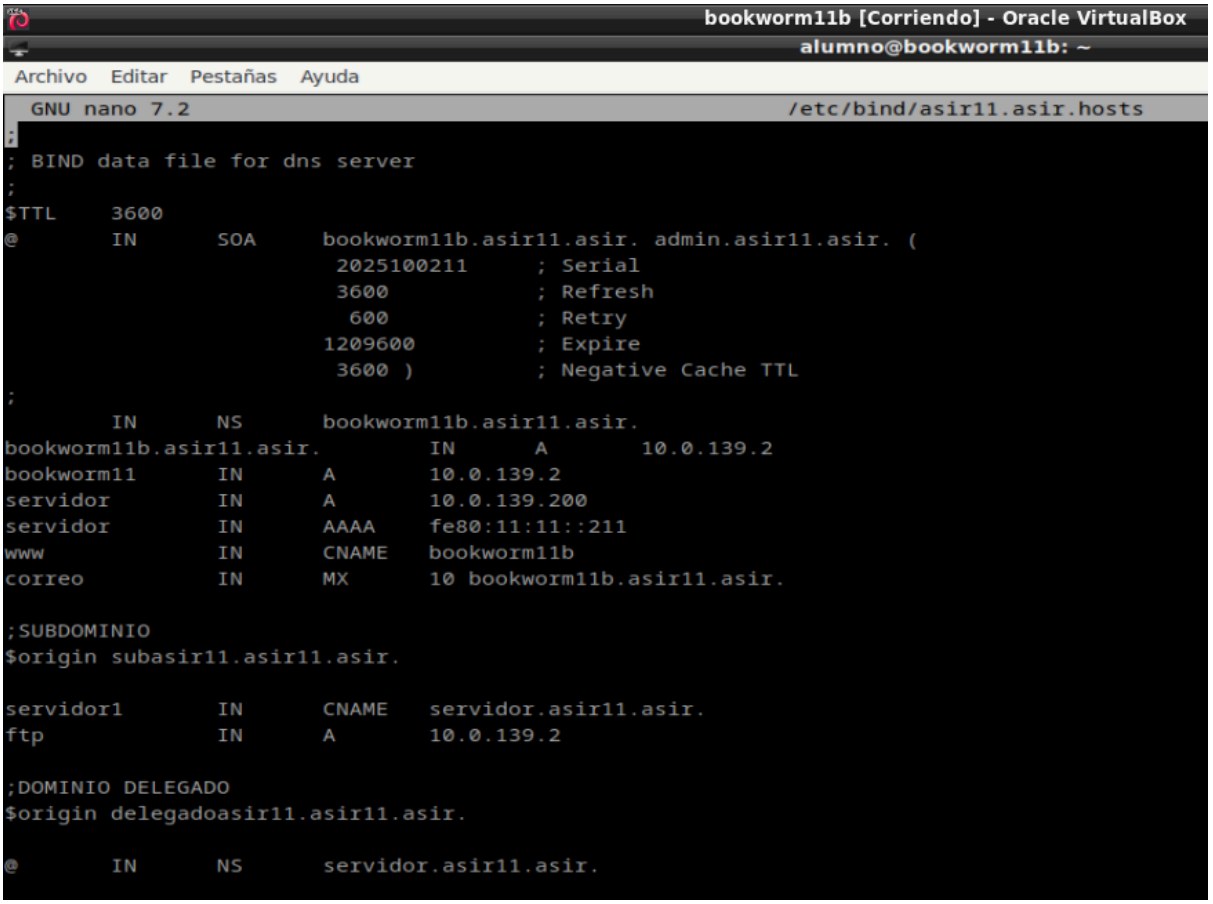
- Hay que utilizar el comando 'dig' para todas la pruebas
- Dispones además de comandos de comprobación de sintaxis para el BIND9:
    - Podemos comprobar un archivo de configuración con, por ejemplo: named-checkconf /path/to/named.conf
    - Podemos comprobar una zona con, por ejemplo: named-checkzone example.net /etc/bind/example.net

Pasos:

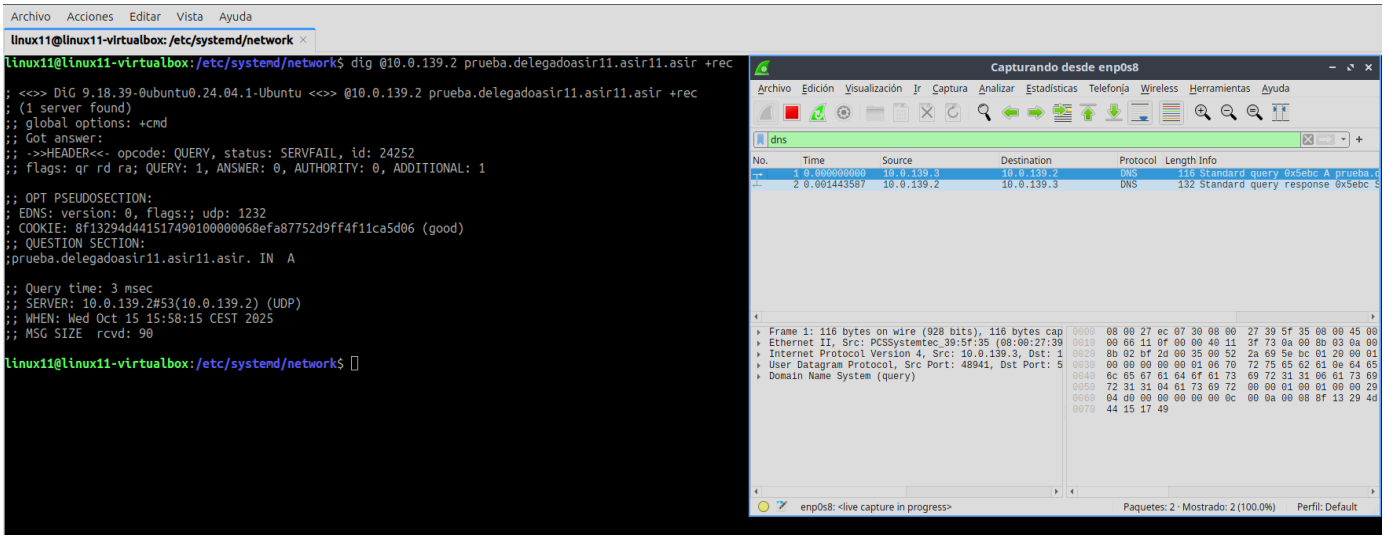
1. En la zona 'asirXX.asir' crea un nuevo un subdominio denominado "delegadoasirXX.asirXX.asir" del mismo modo que en la práctica anterior. Utiliza para ello la directiva $origin.
2. Asigna a ese subdominio como registro NS el DNS servidor.asirXX.asir (se trata de un DNS ficticio, que no existe) y vuelve a cargar la zona. Para ello

tendrás que habilitar un registro NS específico para 'delegadoasirXX.asirX.asir'. Para ello, después de la directiva $origin, usa la sintaxis:

- @ IN NS servidor.asirXX.asir.
- No añadimos ningún registro más

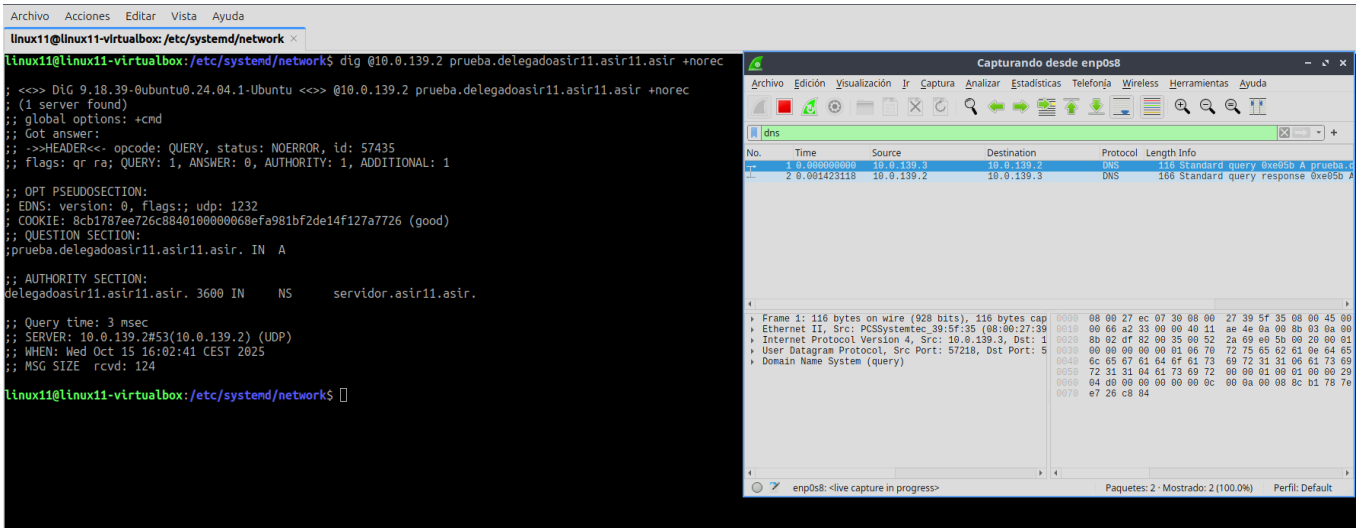


3. Vamos a consultar desde nuestro cliente Linux el nombre "prueba.delegadoasirXX.asirXX.asir" usando el comando dig. Si no indicamos nada de forma expresa, la pregunta recursiva. Observa qué ocurre. Observa la respuesta que se da. Observa la captura de paquetes que se produce en la interfaz de la red interna del cliente LinuxXX y extrae conclusiones. Recuerda por filtrar por DNS para que sea más sencillo.



Sale SERVFAIL ya que al ser recursiva mi dns ve que el encargado de ese dominio es el server ficticio creado al que le pregunta y como no existe ese servidor da servfail

4. Pregunta por "prueba.delegadoasirX.asirXX.asir" usando el comando dig, pero haciendo que la pregunta sea NO recursiva. Observa qué ocurre y la respuesta que se da. Observa la captura de paquetes que se produce en la interfaz de la red interna del cliente LinuxXX y extrae conclusiones. Recuerda por filtrar por DNS para que sea más sencillo.



Aquí al ser no recursiva mi servidor dns puede darme una referencia de quien es el encargado de ese dominio y me da a servidor.asir11.asir.

5. Extrae conclusiones sobre el concepto de delegación

La delegación DNS permite asignar la autoridad de un subdominio a otro servidor.

En una consulta recursiva, el servidor intenta resolver el nombre completo y falla si no puede contactar con el DNS delegado.

En una no recursiva, sólo informa qué servidor es responsable del subdominio sin resolverlo.