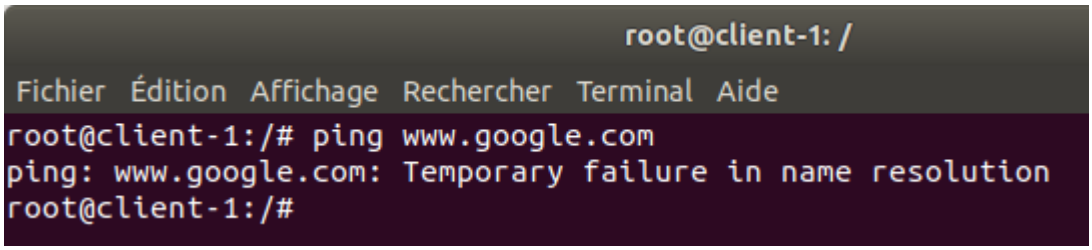
Troubleshooting DNS

Situation 1

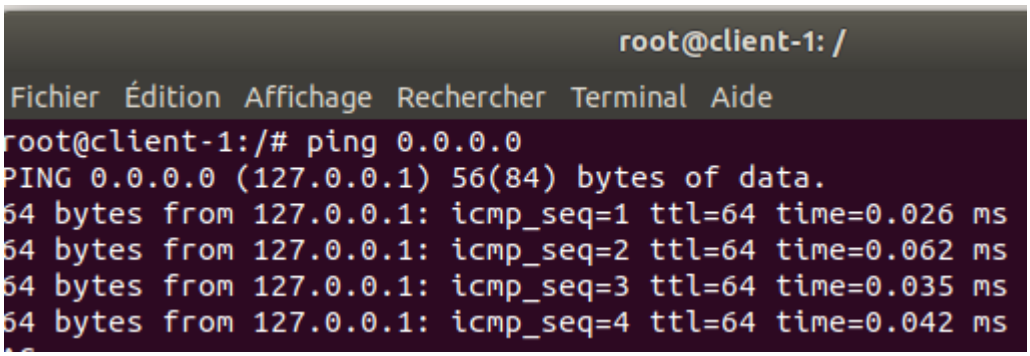
Collecte des symptômes :

Commande que j'utilise sur le client et l'output sont :

- ping www.google.com



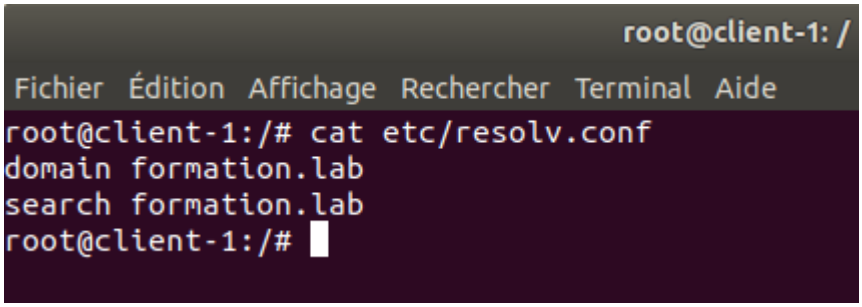
- ping 0.0.0.0



Le client peut accéder à l'internet mais ne peut pas accéder aux liens par noms.

J'ai fait une trace sur wireshark, mais il n'y a pas une trace que je peux voir quand je fais un ping à google.com, alors je regarde si le client a l'adresse IP du résolveur.

- cat etc/resolv.conf



Je regarde dans le fichier resolve.conf dans le client et je voie que le client n'a pas l'adresse IP du résolveur.

Description du problème :

Le client n'est pas connecté avec le résolveur, alors il n'est pas possible de résoudre le nom du lien.

Proposition de solution :

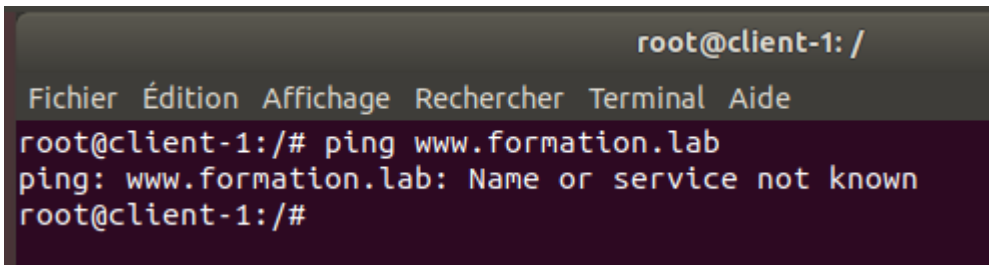
Une solution est d'ajouter une option dans le fichier /etc/dhcp/dhcpd.conf avec l'adresse IP du résolveur et redémarrer les serveurs. La ligne qu'il doit être ajouter est : « option domain-name-servers 192.168.0.1; »

Situation 2

Collecte des symptômes :

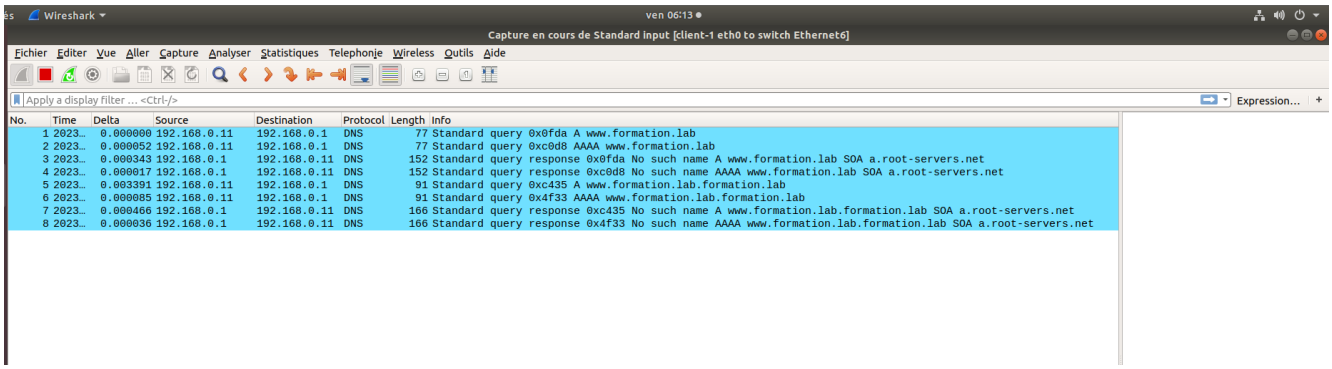
Commande que j'utilise sur le client et l'output :

- ping www.formation.lab

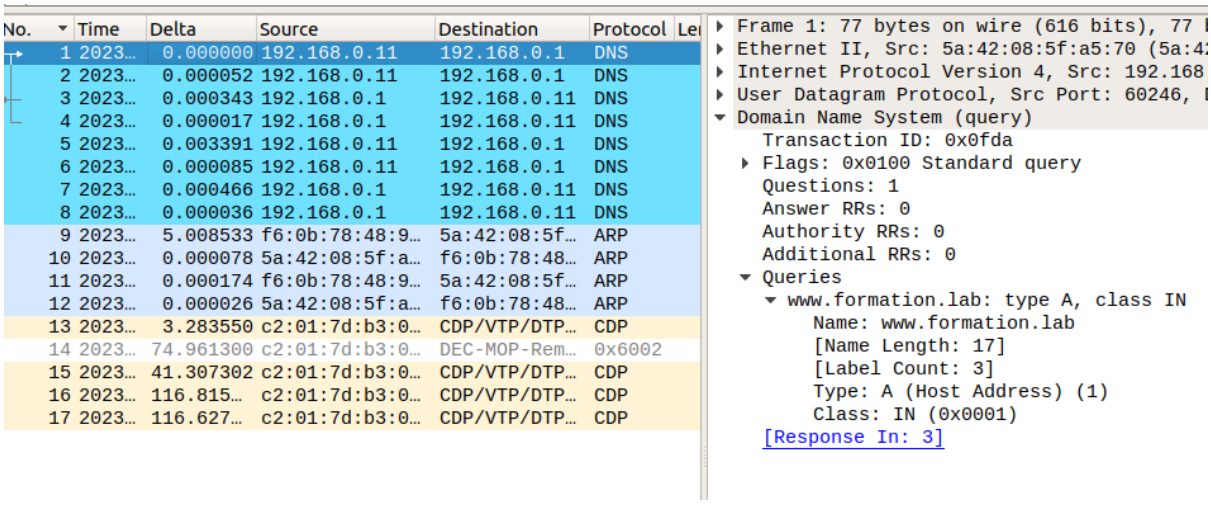


Ici on peut voir que le ping ne s'effectue pas correctement et rend une erreur.

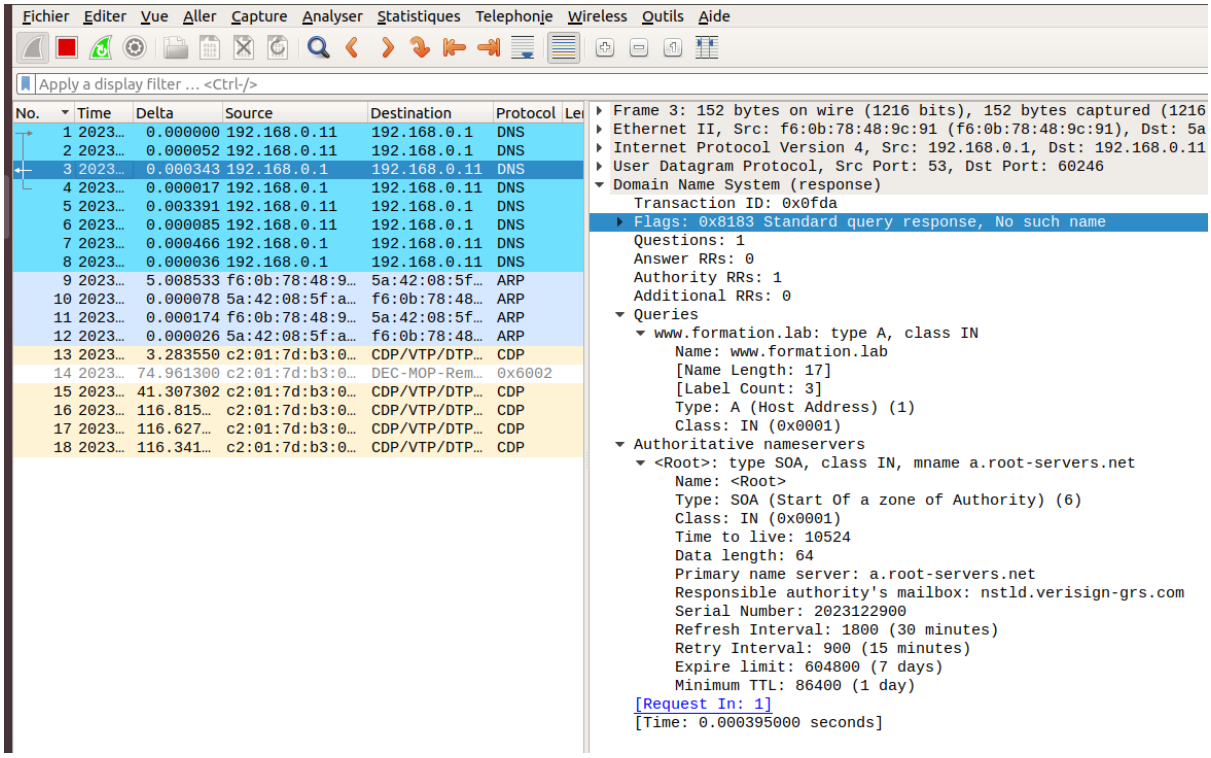
- Trace wireshark du ping www.formation.lab sur le client :



Ici on peut voir la trace wireshark du ping www.formation.lab.



Sur la trace numéro 1 le client envoye une demande DNS au resolveur. La demande est une demande de trouver l'adresse IP du lien www.formation.lab.



Sur la trace numéro 3, qui est la réponse du résolveur au client, on peut voir qu'il cherche au root de trouver l'adresse IP pour ce lien mais ne trouve rien et envoie une erreur.

Description du problème :

Le résolveur envoie une requête au root server et ne fait pas un forward au SOA, qui contient l'adresse IP de l'intranet.

Proposition de solution :

Il faut ajouter une zone forward de l'intranet dans le fichier /etc/bind/named.conf dans le résolveur pour résoudre ce problème.

Dans ce cas ça doit être :

```
zone "formation.lab." IN {
        type forward;
        forwarders { 192.168.0.2; };
        forward only;
    };
```

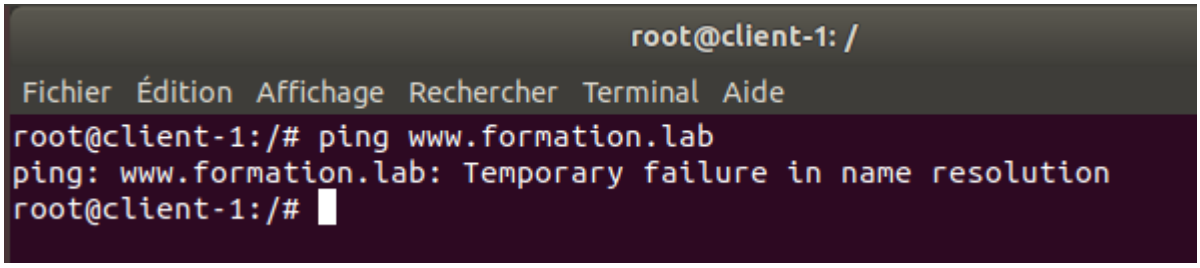
```
root@client-1:/# ping www.formation.lab
PING www.formation.lab (192.168.0.4) 56(84) bytes of data.
64 bytes from 192.168.0.4 (192.168.0.4): icmp_seq=1 ttl=64 time=0.390 ms
64 bytes from 192.168.0.4 (192.168.0.4): icmp_seq=2 ttl=64 time=0.709 ms
64 bytes from 192.168.0.4 (192.168.0.4): icmp_seq=3 ttl=64 time=0.366 ms
64 bytes from 192.168.0.4 (192.168.0.4): icmp_seq=4 ttl=64 time=0.237 ms
64 bytes from 192.168.0.4 (192.168.0.4): icmp_seq=5 ttl=64 time=0.191 ms
```

Situation 3

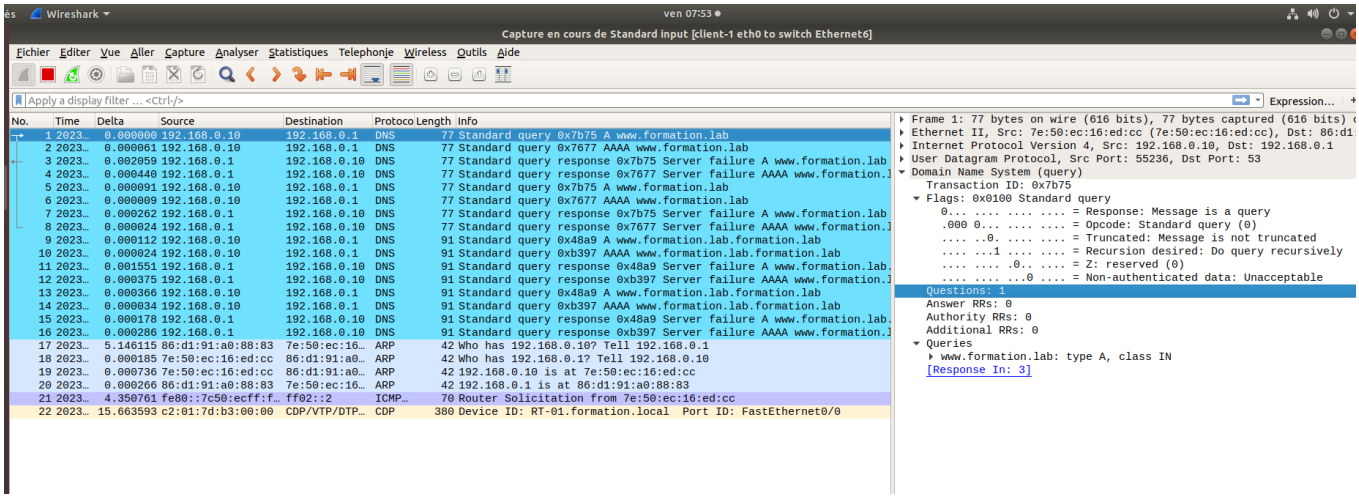
Collecte des symptômes :

Commande que j'utilise cette commande sur le client et l'output est :

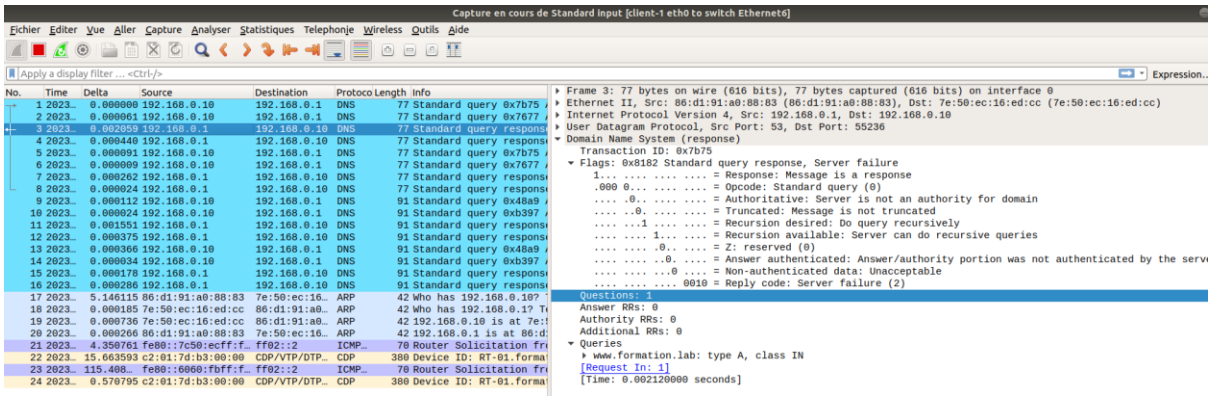
- dig www.formation.lab



- trace wireshark du client après le ping sur www.formation.lab :

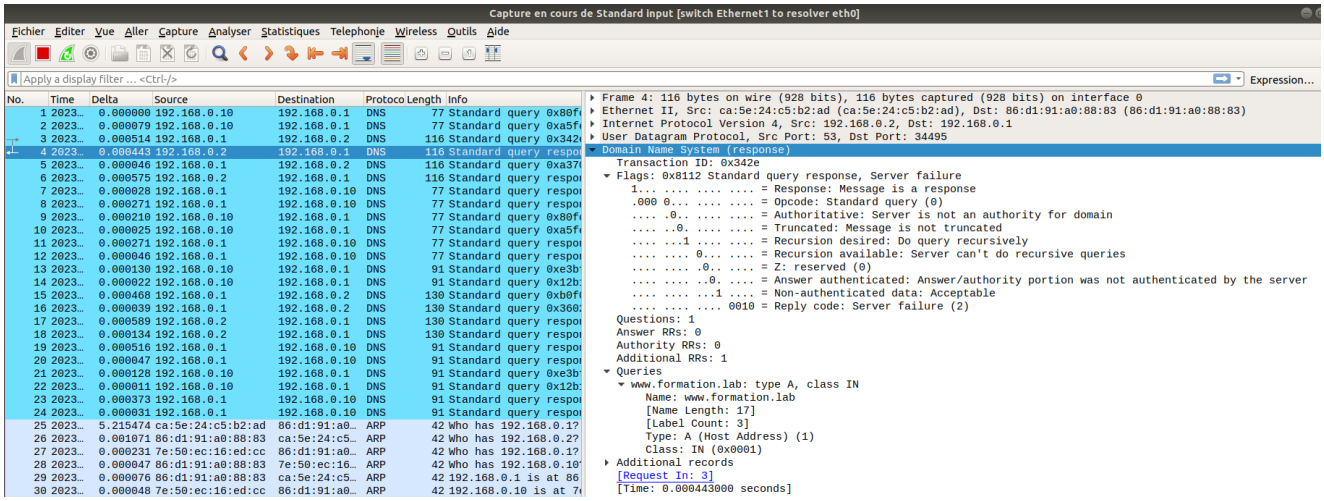


La trace numéro 1 on peut voir que le client envoie une demande DNS au resolveur et demande l'adresse IP de www.formation.lab.



La trace numéro 3 on peut voir que il y a un serveur failure, le résolveur dit que le nom n'est pas dans la liste qu'il contien.

- Trace wireshark sur le résolveur après un ping sur www.formation.lab :



Sur la trace 3 et 4 on peut voir que le résolveur envoie une requête au SOA, mais le SOA dit qu'il ne contient pas ce nom au résolveur.

- nano /etc/bind/formation.lab sur le SOA

```
  GNU nano 4.8                                                    formation.lab
$ORIGIN formation.lab.
$TTL 1d

@       IN      SOA     soa.formation.lab       vvds.ephec.be. (
                2001062501 ; serial
                21600      ; refresh after 6 hours
                3600       ; retry after 1 hour
                604800     ; expire after 1 week
                86400 )    ; minimum TTL of 1 day
;

@       IN      NS      soa.formation.lab
@       IN      MX      10      mail

soa     IN      A       192.168.0.2
resolver IN     A       192.168.0.1
dhcpd   IN      A       192.168.0.3
www     IN      A       192.168.0.4
mail    IN      A       192.168.0.5
```

Ici on peut voir que la syntaxe du fichier formation.lab n'est pas correcte. Sur la ligne 4 il manque un point pour faire référence au root. Sur la ligne 12 le nameserveur c'est seulement « soa » et pas « soa.formation.lab », car il fait référence de la ligne 15.

Description du problème :

Le SOA ne contient pas le nom correct ou syntaxe correct dans les fichiers. Le client peut accéder au internet et envoyer une requête au résolveur. Le résolveur peut aussi envoyer une requête au SOA, mais le SOA n'arrive pas à donner une solution au résolveur. Alors on doit regarder dans les fichiers du SOA. Dans le fichier /etc/etc/formation.lab on peut voir qu'il y a des problèmes syntaxe.

Proposition de solution :

Simplement appliquer les changements dans les lignes 12 et 15 dans le fichier /etc/bind/formation.lab sur le serveur SOA, que j'ai indiqué avant.

```
root@client-1:/# ping www.formation.lab
PING www.formation.lab (192.168.0.4) 56(84) bytes of data.
64 bytes from www.formation.lab (192.168.0.4): icmp_seq=1 ttl=64 time=1.22 ms
64 bytes from www.formation.lab (192.168.0.4): icmp_seq=2 ttl=64 time=0.687 ms
64 bytes from www.formation.lab (192.168.0.4): icmp_seq=3 ttl=64 time=0.483 ms
64 bytes from www.formation.lab (192.168.0.4): icmp_seq=4 ttl=64 time=0.275 ms
```