Mayala-Luneko Loyde 17/12/2024

Classe : 2L1

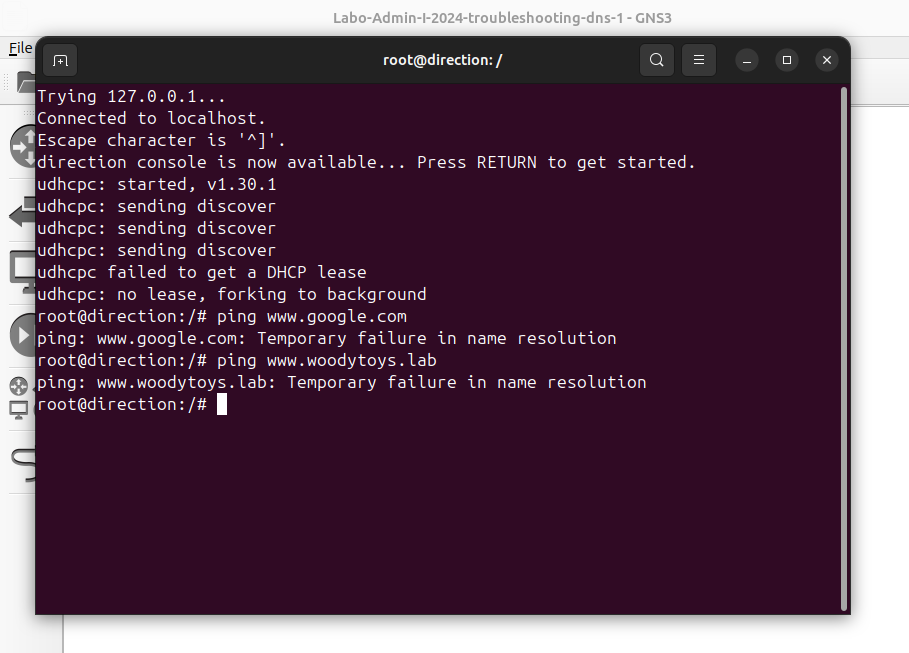
Rapport de troubleshooting DNS

## Situation  1 :

Identification du problème :

1. Echec de connectivité vers un domaine publique et privé :

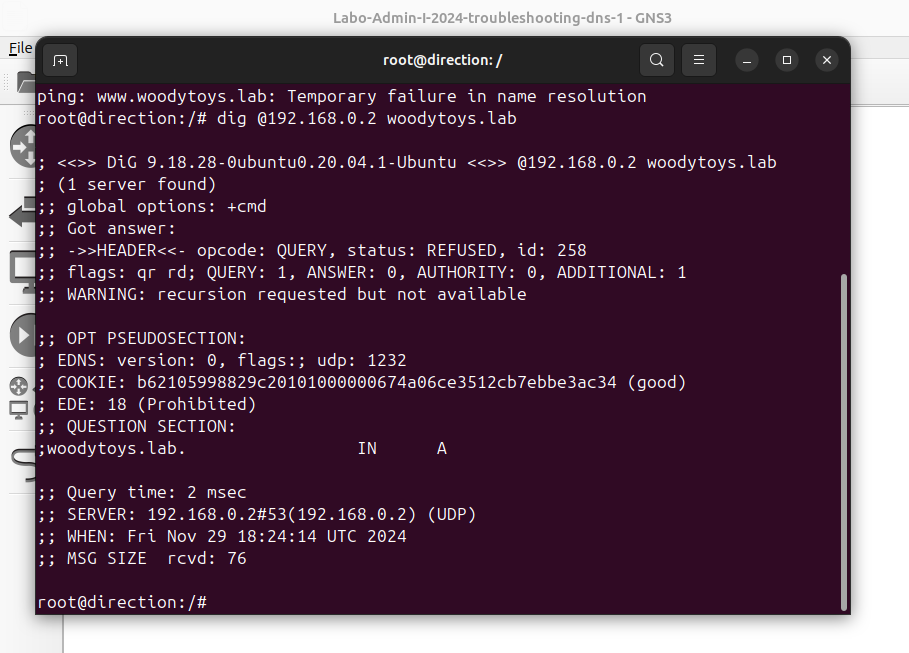
Les pings vers l’adresse [www.google.com](http://www.google.com) et [www.woodytoys.lab](http://www.woodytoys.lab) à partir du client de direction ont échoué, ceux-ci affiche une erreur :

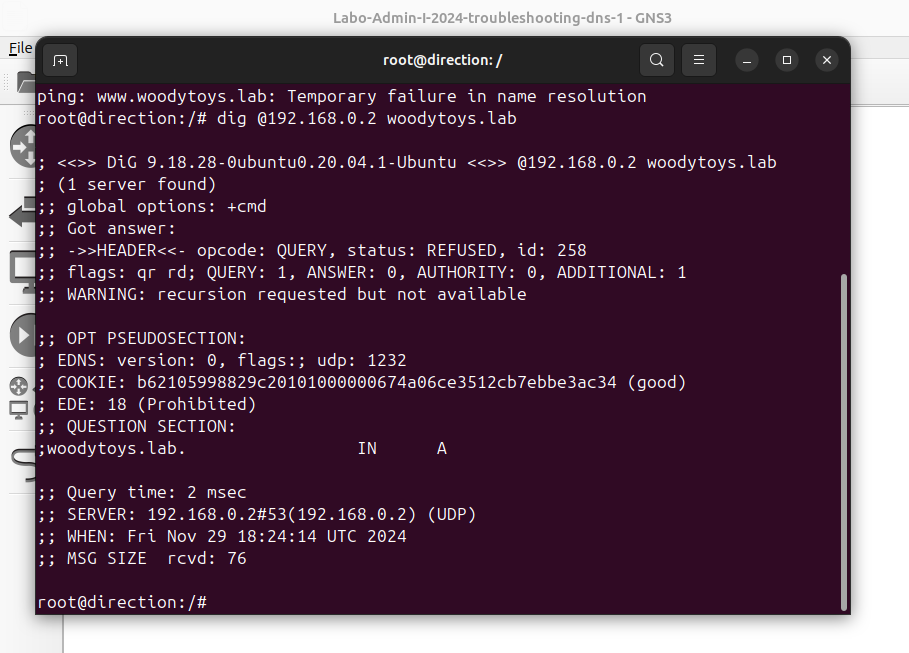


Collecte des symptômes

1. Erreur lors des requêtes DNS avec dig :

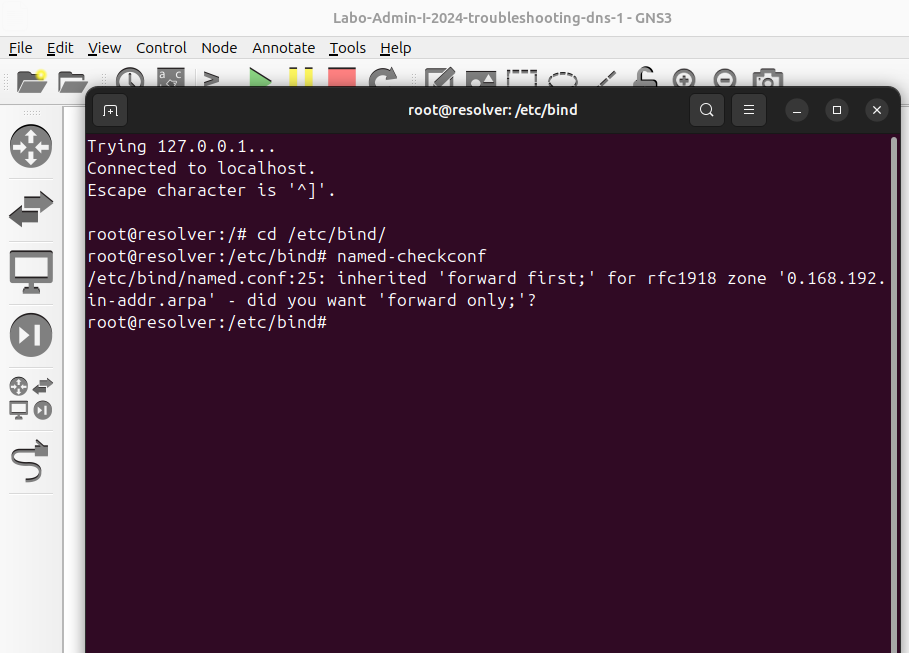
Une requêtes via **dig** à partir du client de direction vers une adresse pour obtenir les informations sur le domaine [www.woodytoys.lab](http://www.woodytoys.lab) échoue





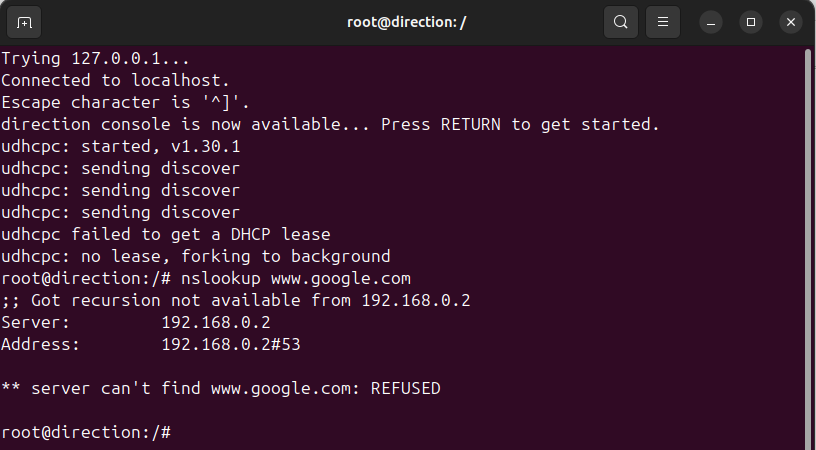
1. Une erreur lors de la configuration aperçu via la commande named-checkconf

Lors de la commande du **named-checkconf** effectué dans le résolveur affiche qu’il y a un manque le **« forward only »** dans le fichier de configuration du résolveur



1. Résolution DNS échoué avec nslookup :

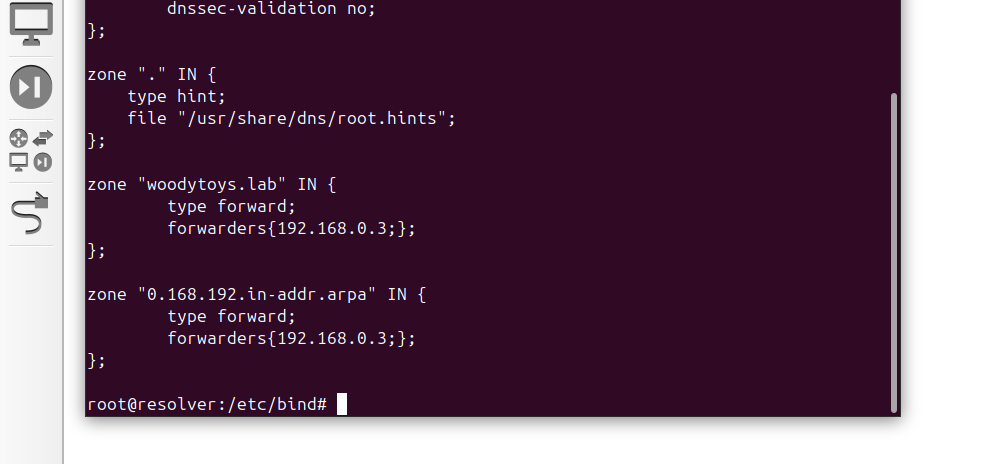
L’exécution de la requêtes nslookup vers Google « génère une erreur » (REFUSED) :



Description du problème

1. Problème dû au manque du forward only

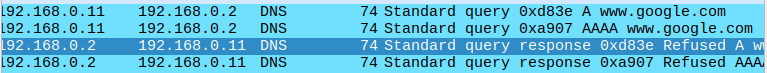
Si la directive "forward only" est absente, le résolveur DNS tente de résoudre les requêtes de manière récursive, c'est-à-dire qu'il interroge d'abord les serveurs racines DNS, et s'il ne trouve pas la réponse, il tente d'autres méthodes locales de résolution. Ce comportement empêche le résolveur de simplement relayer la requête vers le serveur de noms autoritaire (SOA) pour une résolution directe



1. Problème dû au récursion non valide :

Analyse des trames WireShark :

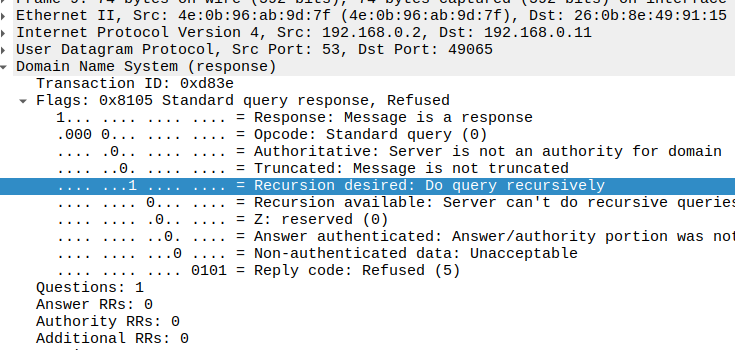
Le message « REFUSED » dans une réponse DNS indique que le serveur DNS refuse de traiter la requêtes



Lorsque l’on regarde de plus prêt, on comprend qu’il y a un souci de récursion. L’indication **Recursion Desired: Do query recursively (1)** indique si le client (votre machine) souhaite que le serveur DNS résolve la requête de manière récursive. (le flag est de 1)

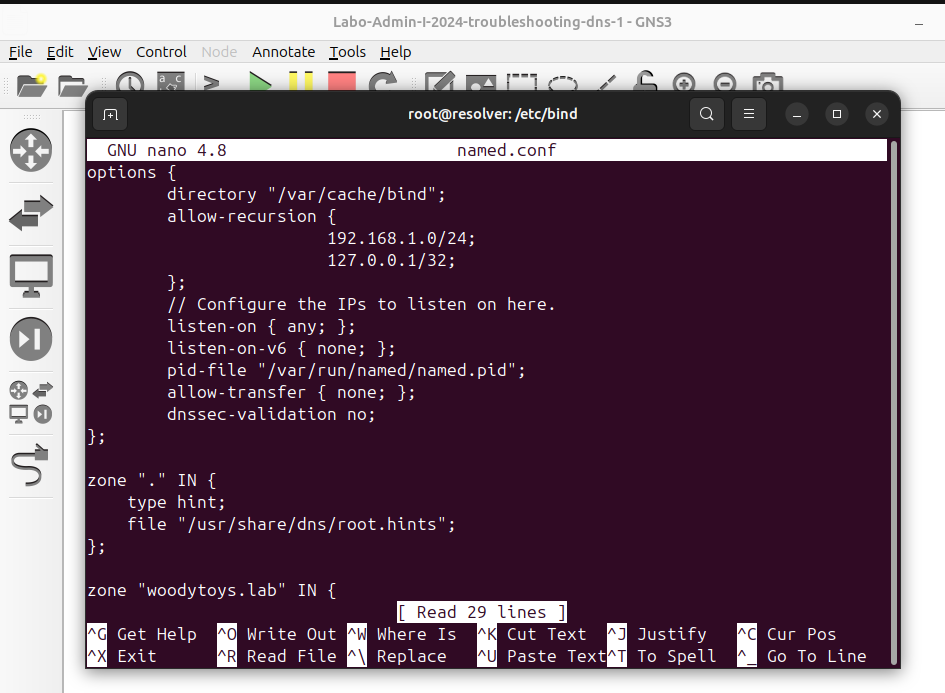
Cela dit, on remarque que le flag est à O près de l’indication : **Recursion available : Server can’t do recursive queries .** En effet, les requêtes récursive ne sont pas activée et donc le résolveur ne traite pas la requêtes comme demandé .

De plus, l’indication pour la réponse est à 0 ( **Answer RRs : 0**), cela signifie qu’il n’y a pas de réponse valide dans la section "Answer" de la réponse DNS et que le résolveur n'a pas renvoyé de Resource Record) correspondant à la requête.



Les raisons de ce problème :

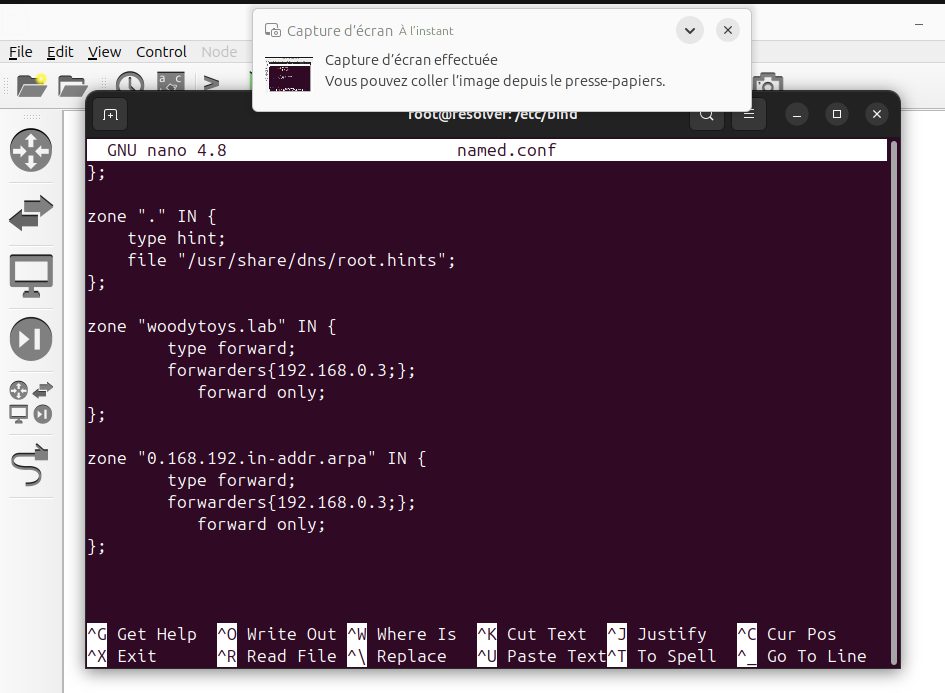
Le résolveur ne fait pas des requêtes récursives pas sur la bonne adresse de sous réseaux ce qui mène à ce que les requêtes qui veinent de l’autre adresse sous-réseaux (192.168.0.0) ne sont pas traités



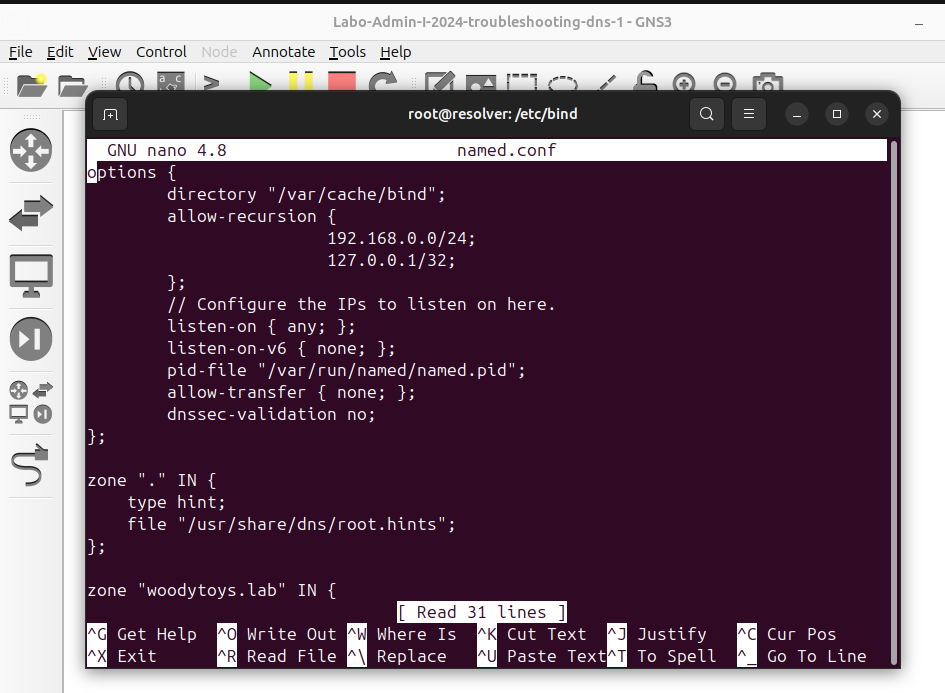
Proposition de solution

1. SOLUTION  :

La première chose, serait de rajouter les forward-only dans le résolveur afin que celui-ci puissent déléguer les requêtes au SOA

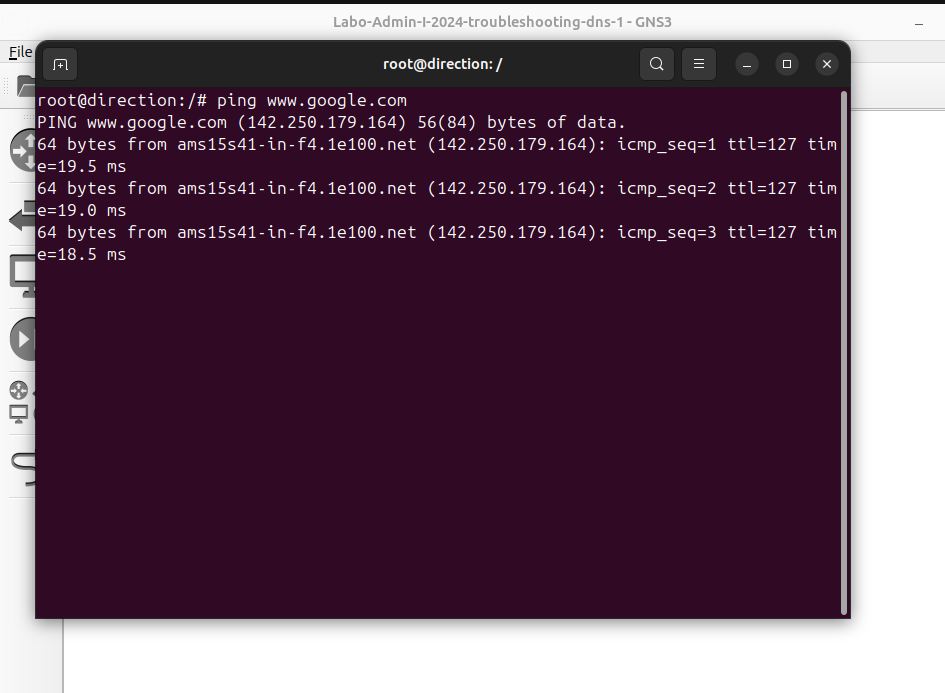


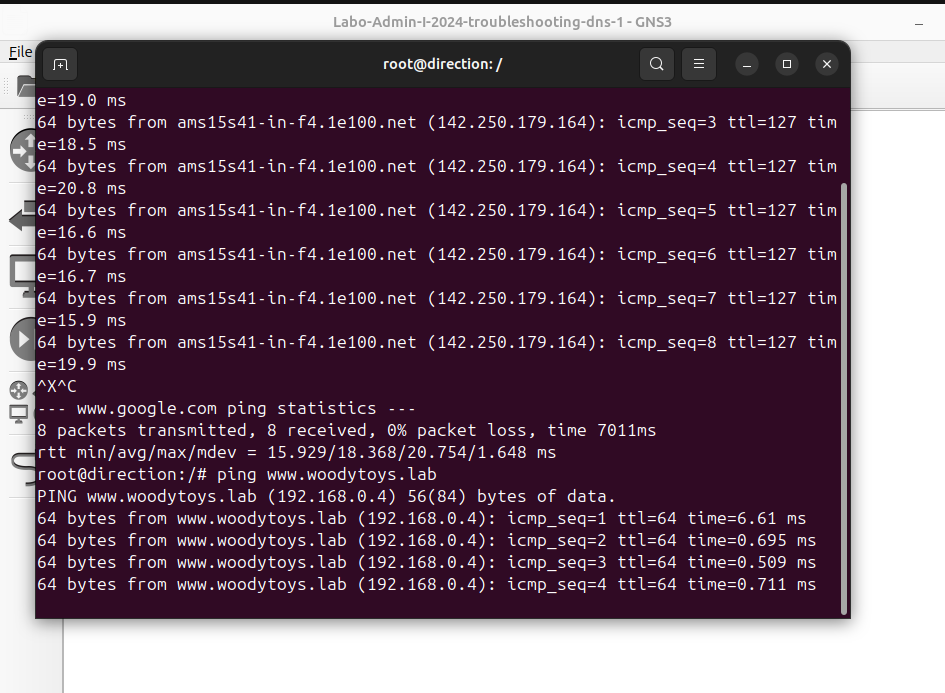
La deuxième serait de modifier le sous réseaux dans lequel le résolveur acceptent les requêtes et donc mettre le bon sous réseaux



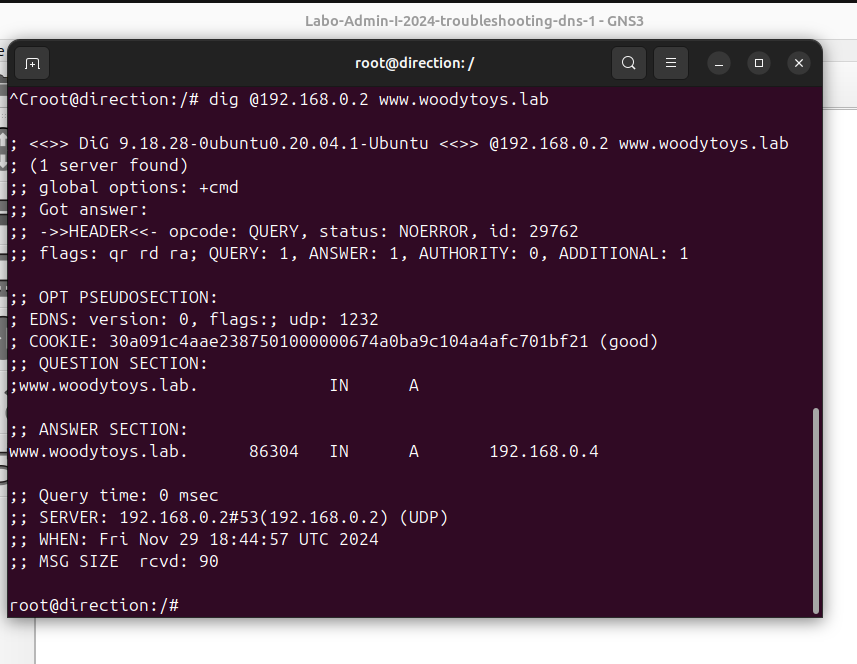
1. RESOLUTION DU PROBLEME :

Le ping à partir du client de direction vers [www.google.com](http://www.google.com) et [www.woodytoys.lab](http://www.woodytoys.lab) fonctionnent





Le dig à partir du client de direction vers une adresse obtenir les informations sur le domaine [www.woodytoys.lab](http://www.woodytoys.lab) a enfin réussit



Lorsque l’on refait une capture WireShark, on remarque que le résolveur répond à la récursion et traite la requête comme demandé :

