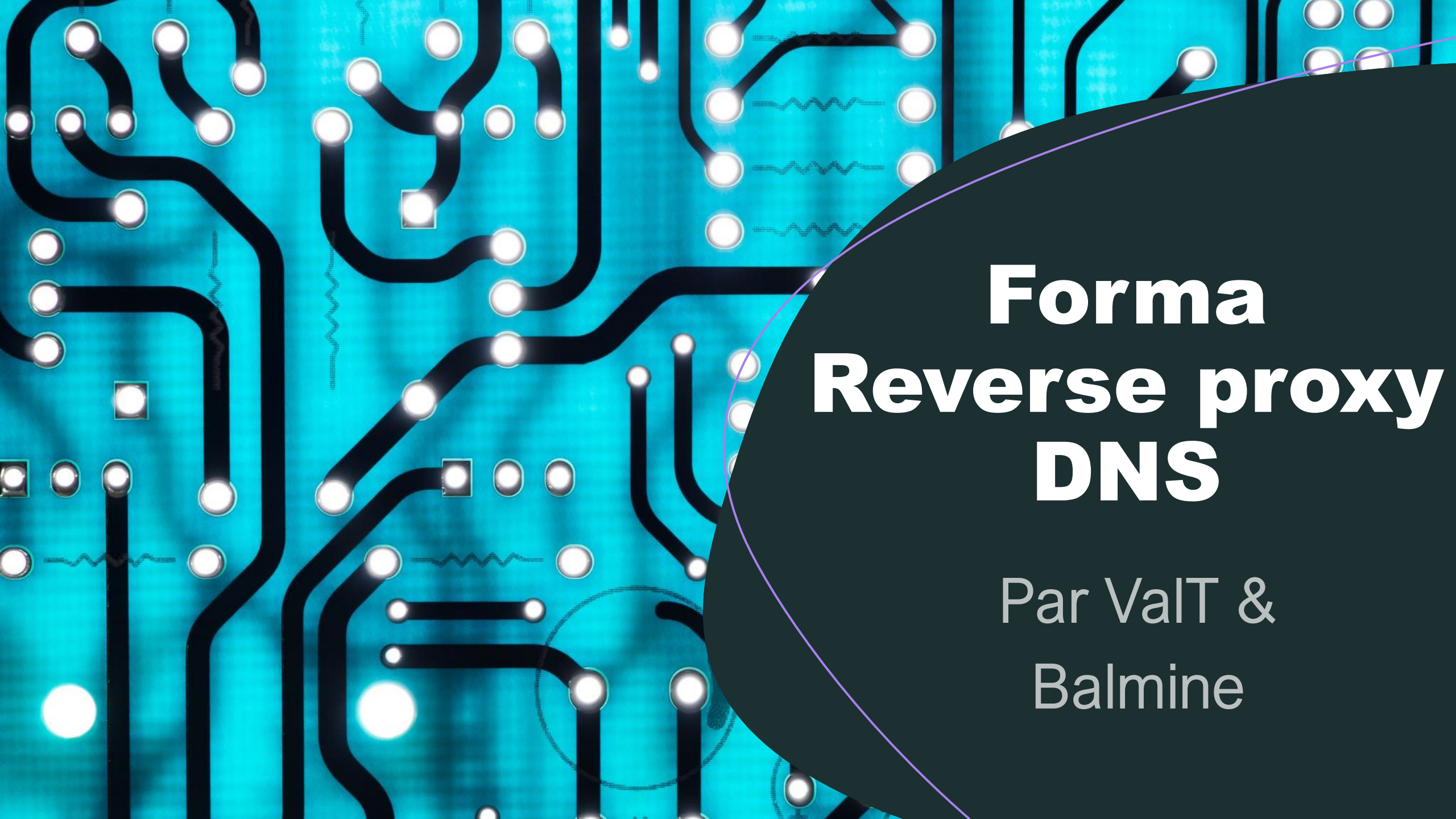
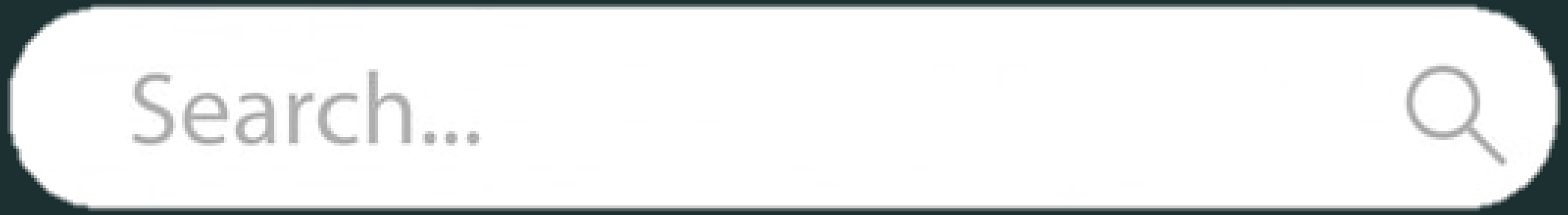


Forma
Reverse proxy
DNS

Par ValIT &
Balmine

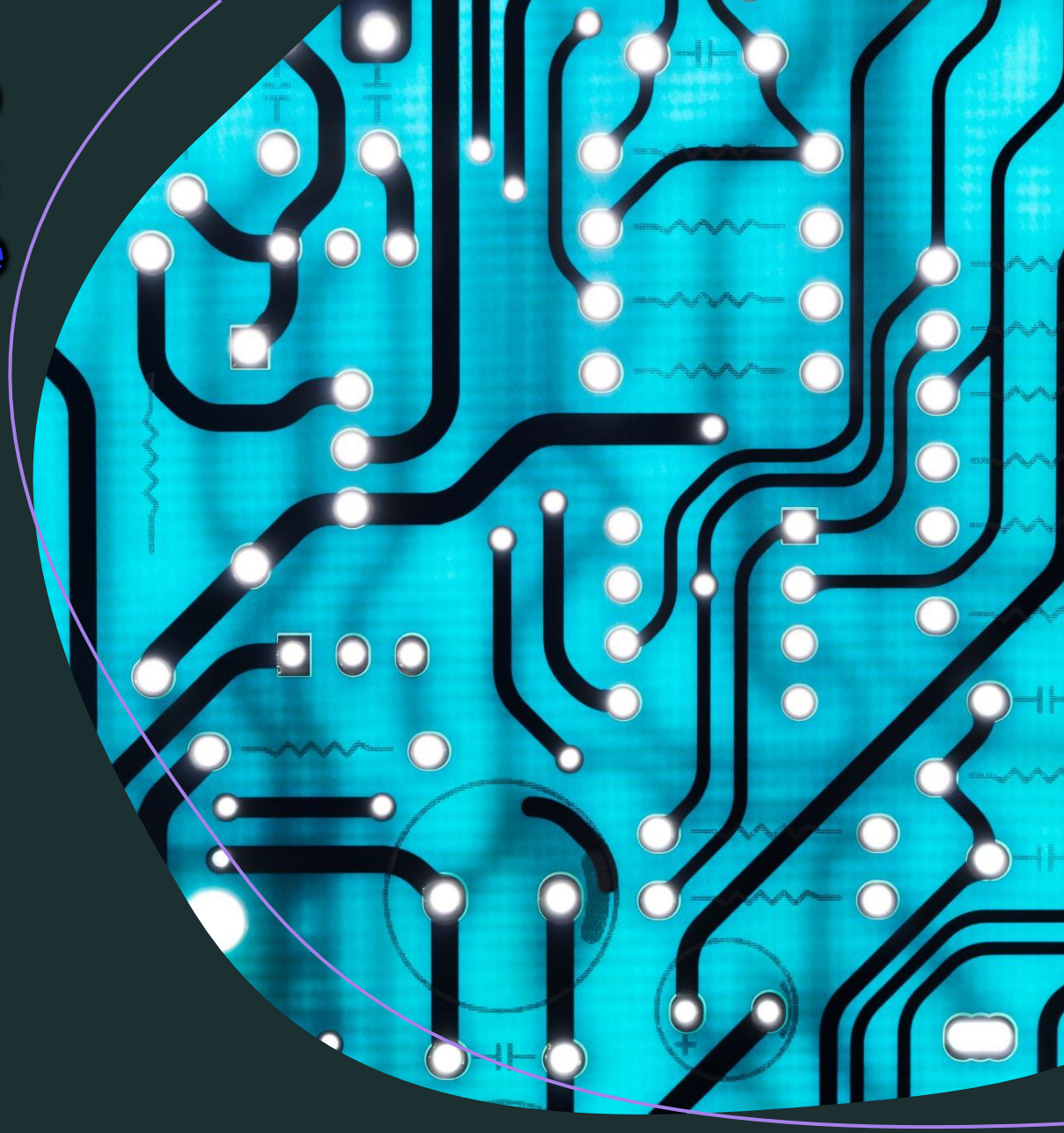
D’un point de vue utilisateur, Internet peut se résumer à une barre de recherche



Je tape le nom d’un site, ça me renvoie sur ce site

Pour aller sur google.com, il me faut l'adresse IP correspondant à la machine qui héberge le site

.
.
.
google.com<>172.217.20.206
.
.
.
discord.gg<>162.159.135.234
.
.
.
facebook.com<>157.240.202.35
.
.
.



Et me donner une IP c'est le boulot du DNS

Un DNS, c’est un serveur avec un programme pour le transformer en DNS dessus

Serveur DNS

.
.
.
google.com<>172.217.20.206
.
.
.
discord.gg<>162.159.135.234
.
.
.
facebook.com<>157.240.202.35
.
.
.

Vous pouvez transformer votre machine en dns si vous voulez :

$ sudo apt install bind9

Dans un DNS, il y a notamment un fichier avec 2 colonnes : nom de domaine, et l’adresse IP correspondante

$ sudo nano /etc/bind/named.conf

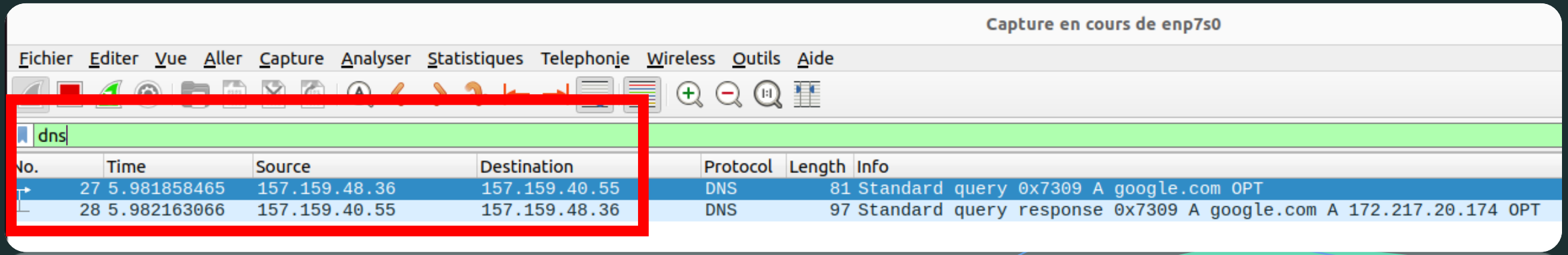
Expérience DNS avec Wireshark (apt install wireshark)

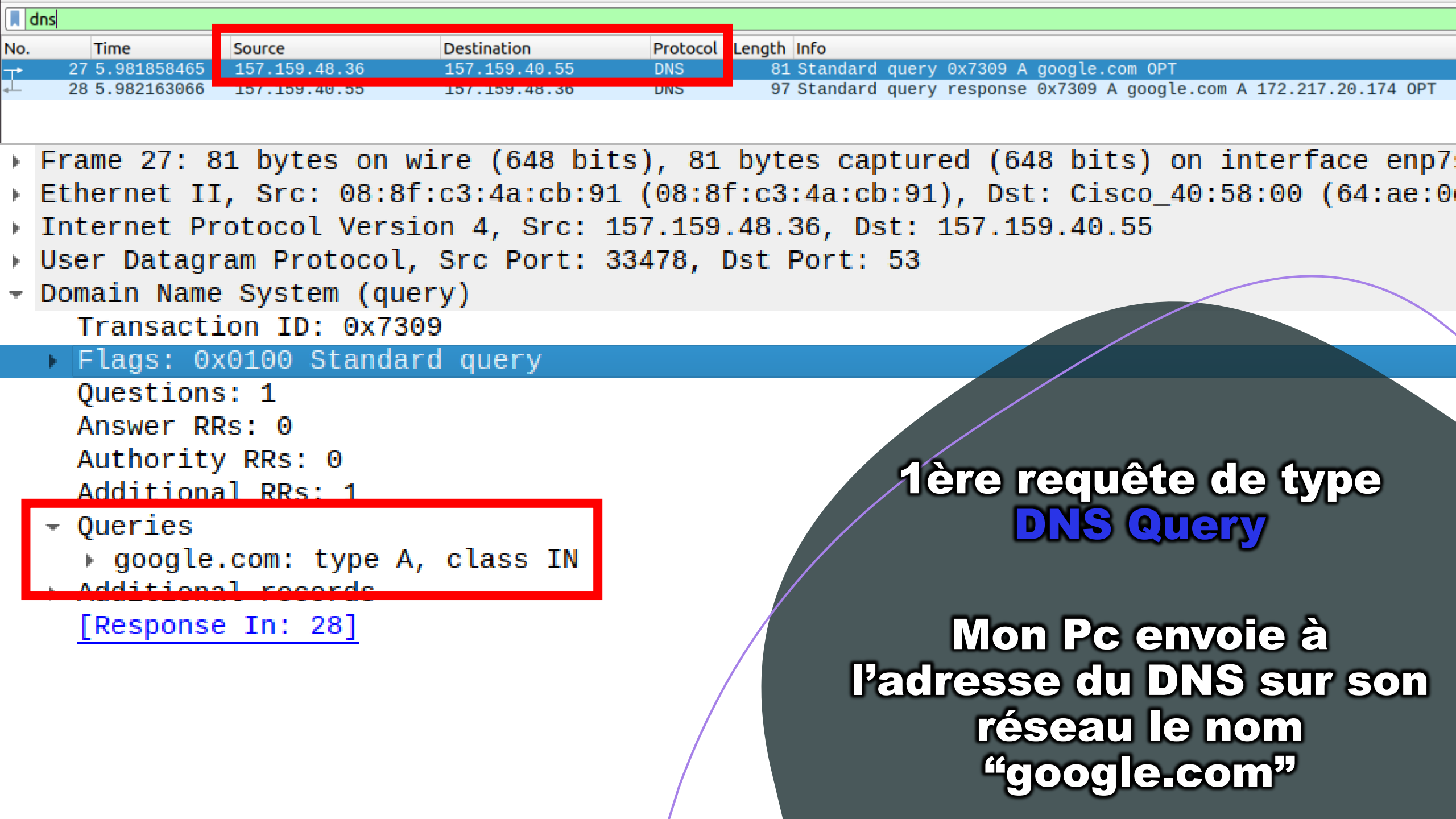
1) On lance une capture wireshark

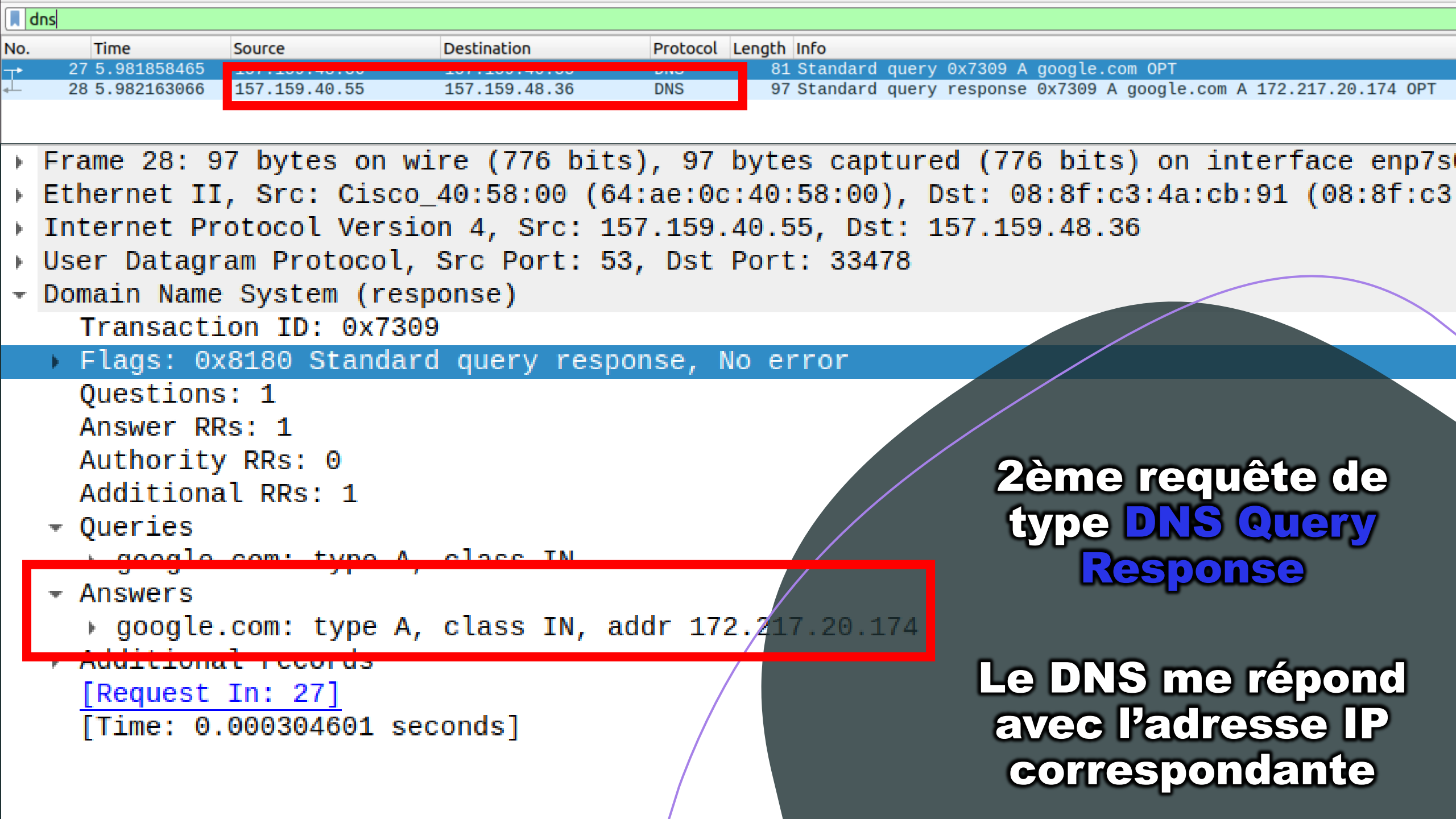
2) On ping google.com (y'a son ip)

```
valt@Valt:~$ ping google.com
PING google.com (172.217.20.174) 56(84) bytes of data.
64 bytes from waw02s07-in-f174.1e100.net (172.217.20.174): icmp_seq=1 ttl=119 time=1.17 ms
64 bytes from waw02s07-in-f174.1e100.net (172.217.20.174): icmp_seq=2 ttl=119 time=1.28 ms
```

3) On remarque 2 requêtes

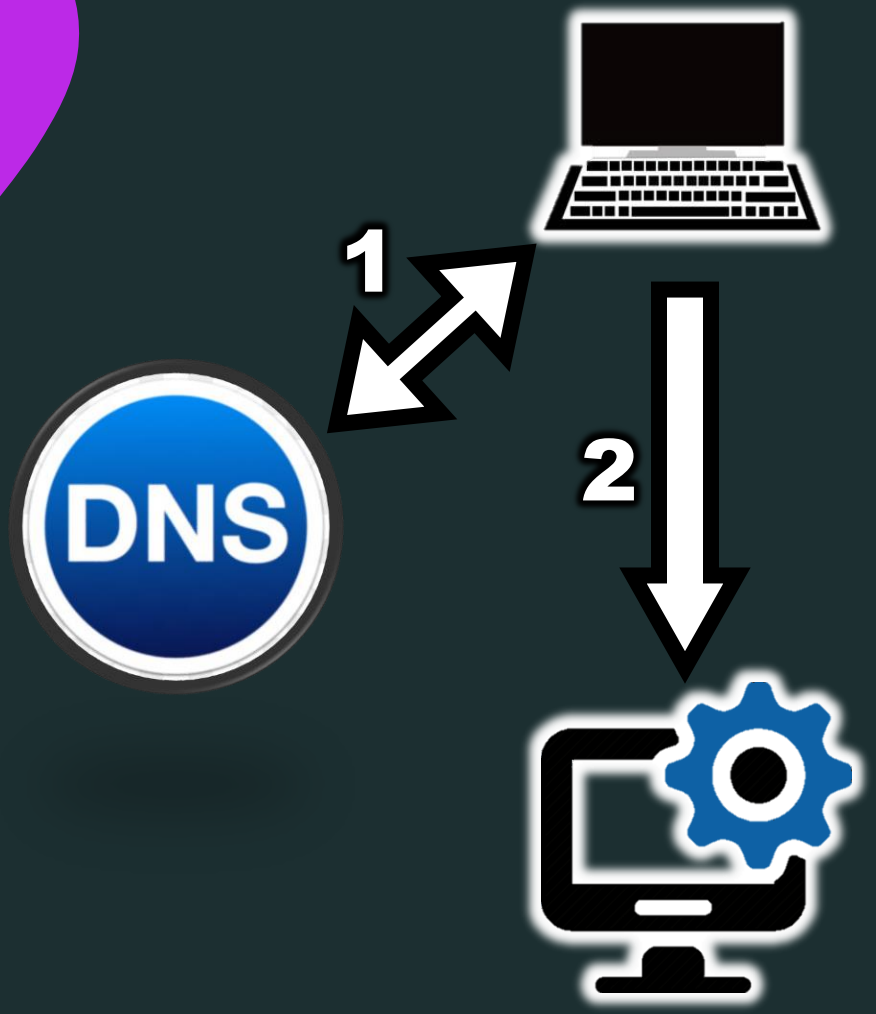



dns
No. Time Source Destination Protocol Length Info
27 5.981858465 157.159.48.36 157.159.40.55 DNS 81 Standard query 0x7309 A google.com OPT
28 5.982163066 157.159.40.55 157.159.48.36 DNS 97 Standard query response 0x7309 A google.com A 172.217.20.174 OPT
Frame 27: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface enp7
Ethernet II, Src: 08:8f:c3:4a:cb:91 (08:8f:c3:4a:cb:91), Dst: Cisco_40:58:00 (64:ae:0
Internet Protocol Version 4, Src: 157.159.48.36, Dst: 157.159.40.55
User Datagram Protocol, Src Port: 33478, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x7309
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
google.com: type A, class IN
Additional records
[Response In: 28]
1ère requête de type
DNS Query
Mon Pc envoie à
l'adresse du DNS sur son
réseau le nom
"google.com"


dns
No. Time Source Destination Protocol Length Info
27 5.981858465 81 Standard query 0x7309 A google.com OPT
28 5.982163066 157.159.40.55 157.159.48.36 DNS 97 Standard query response 0x7309 A google.com A 172.217.20.174 OPT
Frame 28: 97 bytes on wire (776 bits), 97 bytes captured (776 bits) on interface enp7s
Ethernet II, Src: Cisco_40:58:00 (64:ae:0c:40:58:00), Dst: 08:8f:c3:4a:cb:91 (08:8f:c3
Internet Protocol Version 4, Src: 157.159.40.55, Dst: 157.159.48.36
User Datagram Protocol, Src Port: 53, Dst Port: 33478
Domain Name System (response)
Transaction ID: 0x7309
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 1
Queries
Answers
google.com: type A, class IN, addr 172.217.20.174
[Request In: 27]
[Time: 0.000304601 seconds]
2ème requête de type DNS Query Response
Le DNS me répond avec l'adresse IP correspondante

Comment ça se passe si mon DNS ne connait pas un site ?

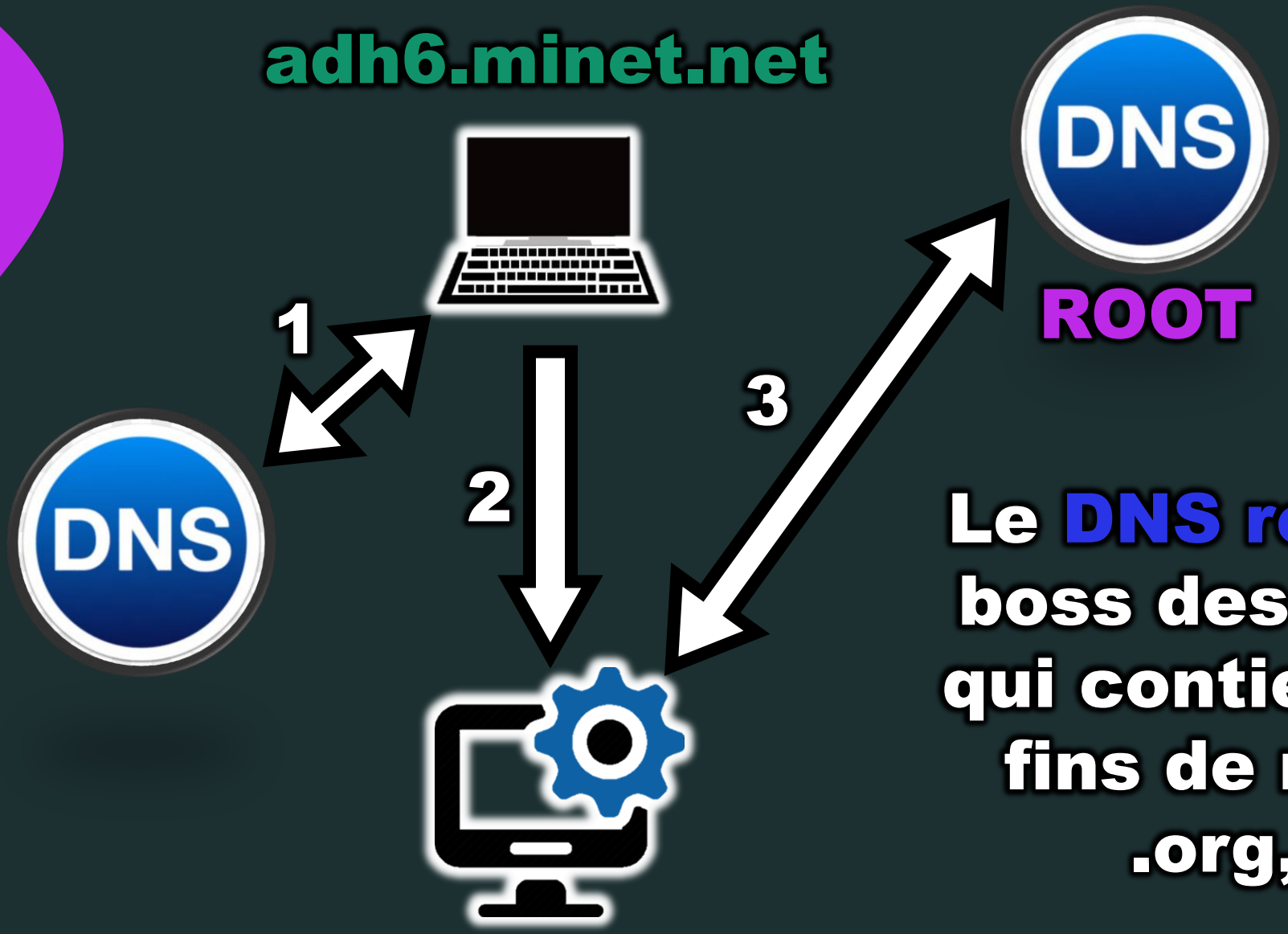
adh6.minet.net



Si mon DNS ne connait pas un site, mon pc l'envoie à un **DNS resolver** (souvent c'est un logiciel intégré à votre machine)

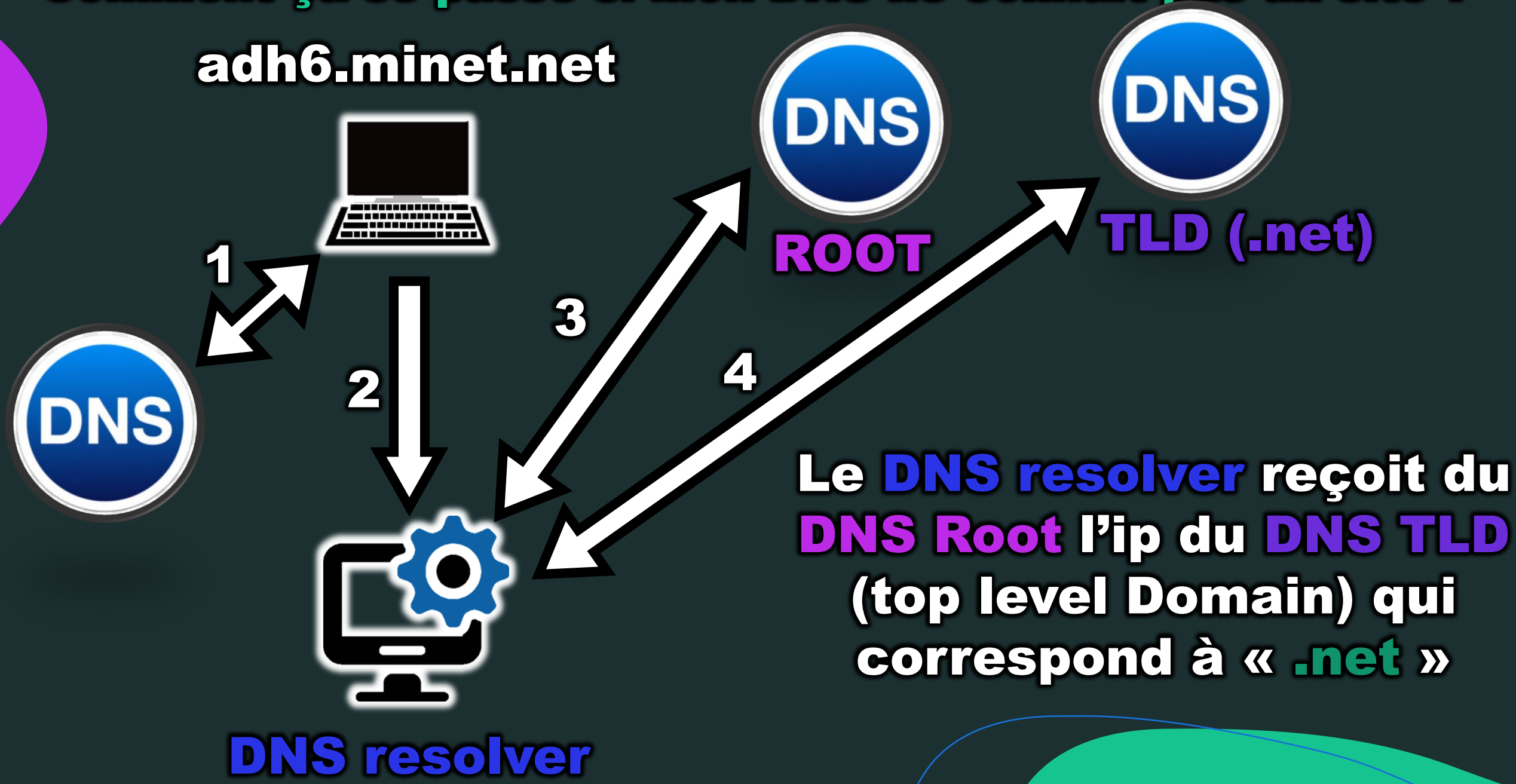
Comment ça se passe si mon DNS ne connait pas un site ?

adh6.minet.net



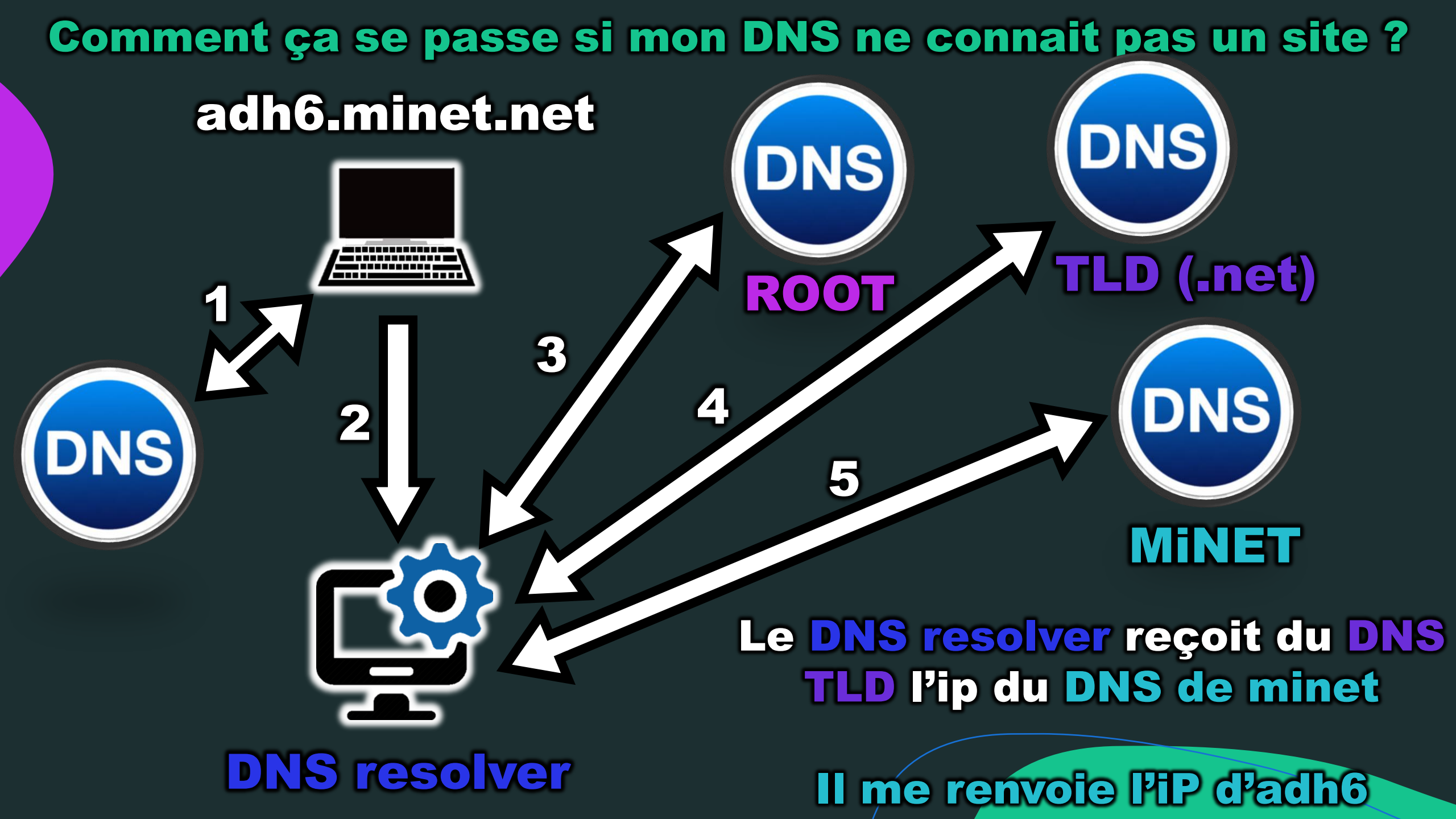
Le DNS resolver contacte le boss des DNS : le DNS Root qui contient les infos sur les fins de nom de domaine : .org, .com, .fr, .net

Comment ça se passe si mon DNS ne connait pas un site ?



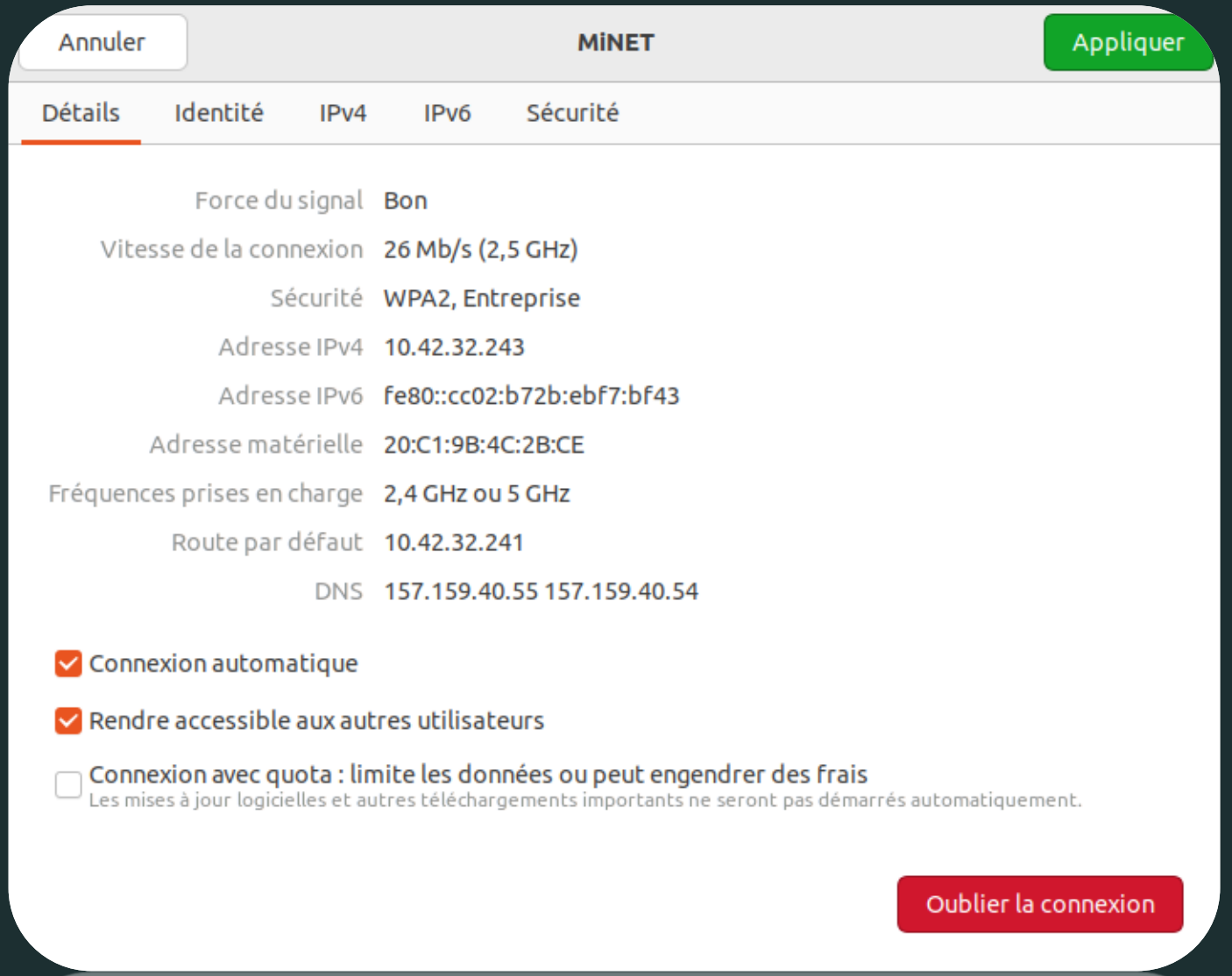
Le DNS resolver reçoit du DNS Root l'ip du DNS TLD (top level Domain) qui correspond à « .net »

Comment ça se passe si mon DNS ne connait pas un site ?



Dans les paramètres su Wifi auquel vous êtes connecté, y'a l'IP de votre DNS

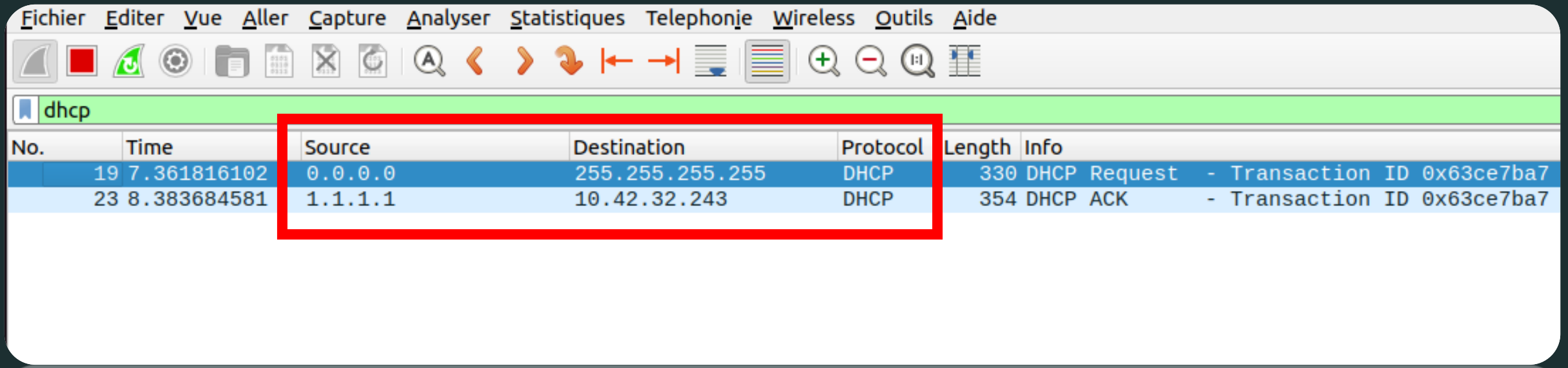
Mais comment j'ai reçu l'IP de mes DNS ?



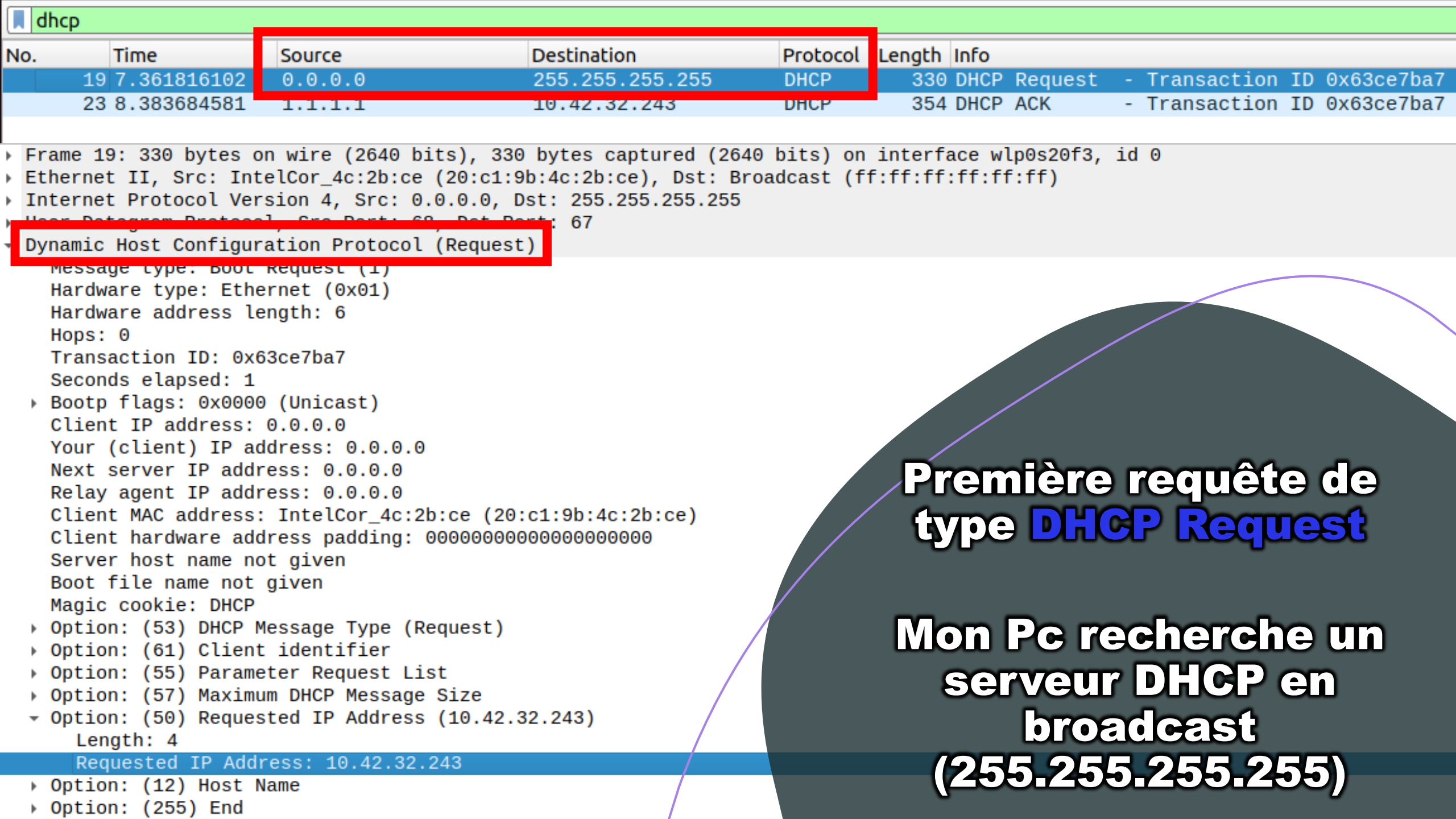
Expérience DHCP avec Wireshark (apt install wireshark)

1) On lance une capture Wireshark

2) On se déconnecte/reconnecte



3) On filtre les requêtes DHCP


dhcp
No. Time Source Destination Protocol Length Info
19 7.361816102 0.0.0.0 255.255.255.255 DHCP 330 DHCP Request - Transaction ID 0x63ce7ba7
23 8.383684581 1.1.1.1 10.42.32.243 DHCP 354 DHCP ACK - Transaction ID 0x63ce7ba7
Frame 19: 330 bytes on wire (2640 bits), 330 bytes captured (2640 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: IntelCor_4c:2b:ce (20:c1:9b:4c:2b:ce), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
67
Dynamic Host Configuration Protocol (Request)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x63ce7ba7
Seconds elapsed: 1
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: IntelCor_4c:2b:ce (20:c1:9b:4c:2b:ce)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Request)
Option: (61) Client identifier
Option: (55) Parameter Request List
Option: (57) Maximum DHCP Message Size
Option: (50) Requested IP Address (10.42.32.243)
Length: 4
Requested IP Address: 10.42.32.243
Option: (12) Host Name
Option: (255) End
Première requête de type DHCP Request
Mon Pc recherche un serveur DHCP en broadcast (255.255.255.255)

dhcp

No.	Time	Source	Destination	Protocol	Length	Info
19	7.361816102	[illegible]	[illegible]	[illegible]	330	DHCP Request - Transaction ID 0x63ce7ba7
23	8.383684581	1.1.1.1	10.42.32.243	DHCP	354	DHCP ACK - Transaction ID 0x63ce7ba7

```
Frame 7: 354 bytes on wire (2832 bits), 354 bytes captured (2832 bits) on interface wlp0s20f3, id 0
Ethernet II, Src: Cisco_a7:d4:90 (b4:e9:b0:a7:d4:90), Dst: IntelCor_4c:2b:ce (20:c1:9b:4c:2b:ce)
Internet Protocol Version 4, Src: 1.1.1.1, Dst: 10.42.32.243
User Datagram Protocol, Src Port: 67, Dst Port: 68
Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0x4939aabb
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.42.32.243
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: IntelCor_4c:2b:ce (20:c1:9b:4c:2b:ce)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (ACK)
  > Option: (1) Subnet Mask (255.255.255.240)
  > Option: (3) Router
  v Option: (6) Domain Name Server
      Length: 8
      Domain Name Server: 157.159.40.55
      Domain Name Server: 157.159.40.54
  > Option: (12) Host Name
  v Option: (15) Domain Name
      Length: 14
```

Première requête de type DHCP ACK

Le DHCP m’envoie une IP et les 2 DNS de mon reseau (ici ceux de minet)

Comment marche le DHCP ?

Je viens d’arriver sur un réseau : pas d’IP, de DNS, rien

DHCP request en Broadcast en espérant qu’un DHCP m’écoute

Comment marche le DHCP ?

Le serv DHCP du réseau entend la DHCP request

LET'S GO

Il me renvoie une IP, celle des DNS, ma gateway, la durée du bail de l'adresse...

Expérience traceroute vers les sites de MiNET

1) Faite $ traceroute minet.net
Quelle IP ça renvoie ?

2) Pareil avec adh6.minet.net
Puis formation.minet.net

3) Pourquoi on obtient toujours la même IP ?
Chaque site doit avoir sa propre IP pourtant...

Fonctionnement du RevProxy

Le revproxy est un serveur qui se place entre l'internet public et un réseau local privé

Fonctionnement du RevProxy

Tous les sites de minet ont une adresse IP privée (192.168.102.xx)
Et dans nos DNS, on met l'adresse publique de notre RevProxy pour chacun de nos sites

Fonctionnement du RevProxy

.
.
.
Adh6-api<>192.168.102.146
.
.
.
Minet.net<>192.168.102.40
.
.
.
Adh6-frontend<>192.168.102.147
.
.
.

Un Revproxy c'est une machine avec un WebServer installé dessus (nginx ou apache par exemple)

APACHE

NGINX

Et comme un DNS, y'a un fichier avec 2 colonnes : nom de site web et son adresse IP

Fonctionnement du RevProxy

Le Revproxy sait quelle machine contacter et renvoie sa réponse à la personne qui l'a demandé

C'est utile pour :

1) Economiser des IP publiques (une IP pour plein de sites)

2) Sécuriser un réseau (De l'extérieur, on ne sait pas ce qu'il y a derrière le RevProxy)

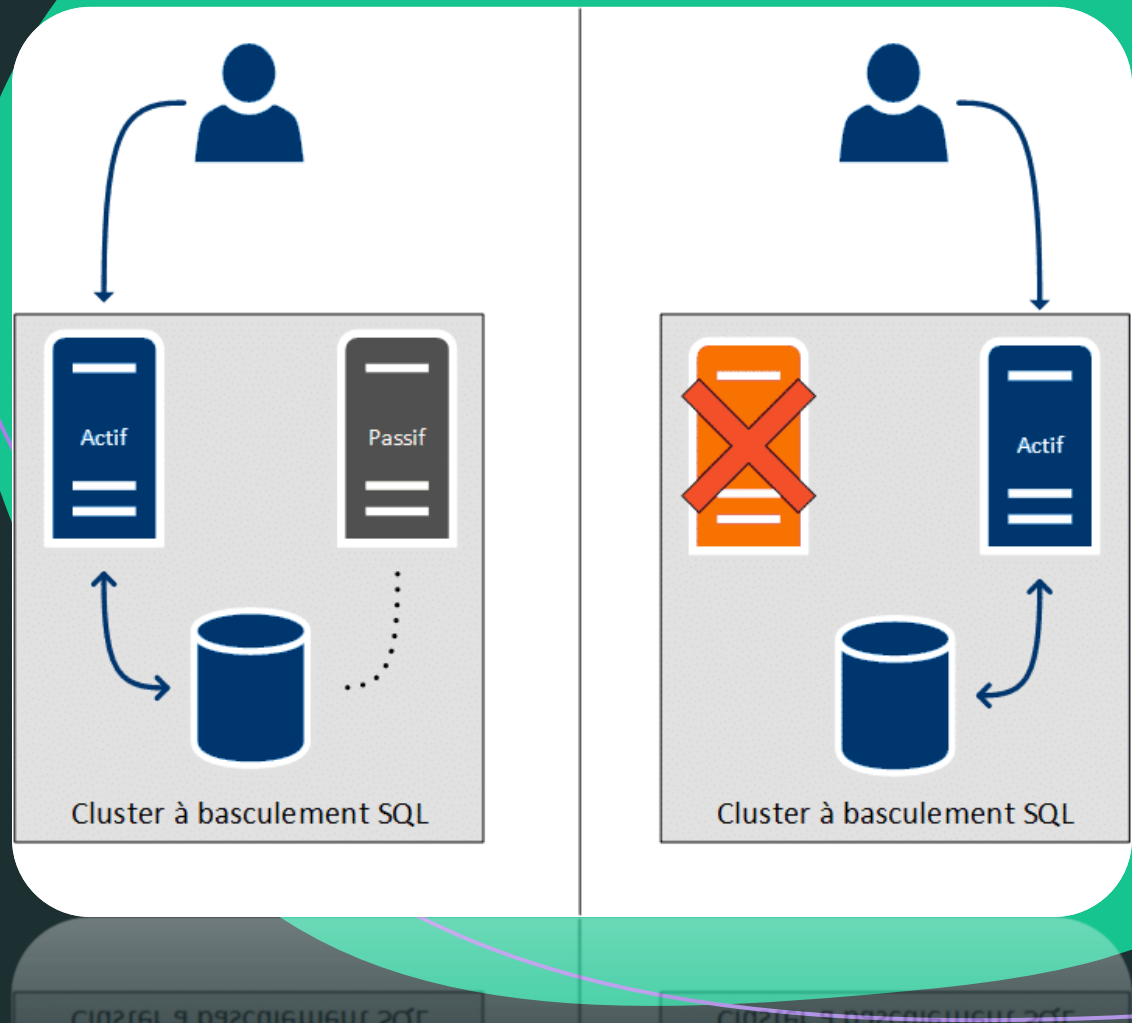
3) Faire du Load Balancing (Avoir plusieurs fois le même site web, et rediriger les gens sur l'un ou sur l'autre)

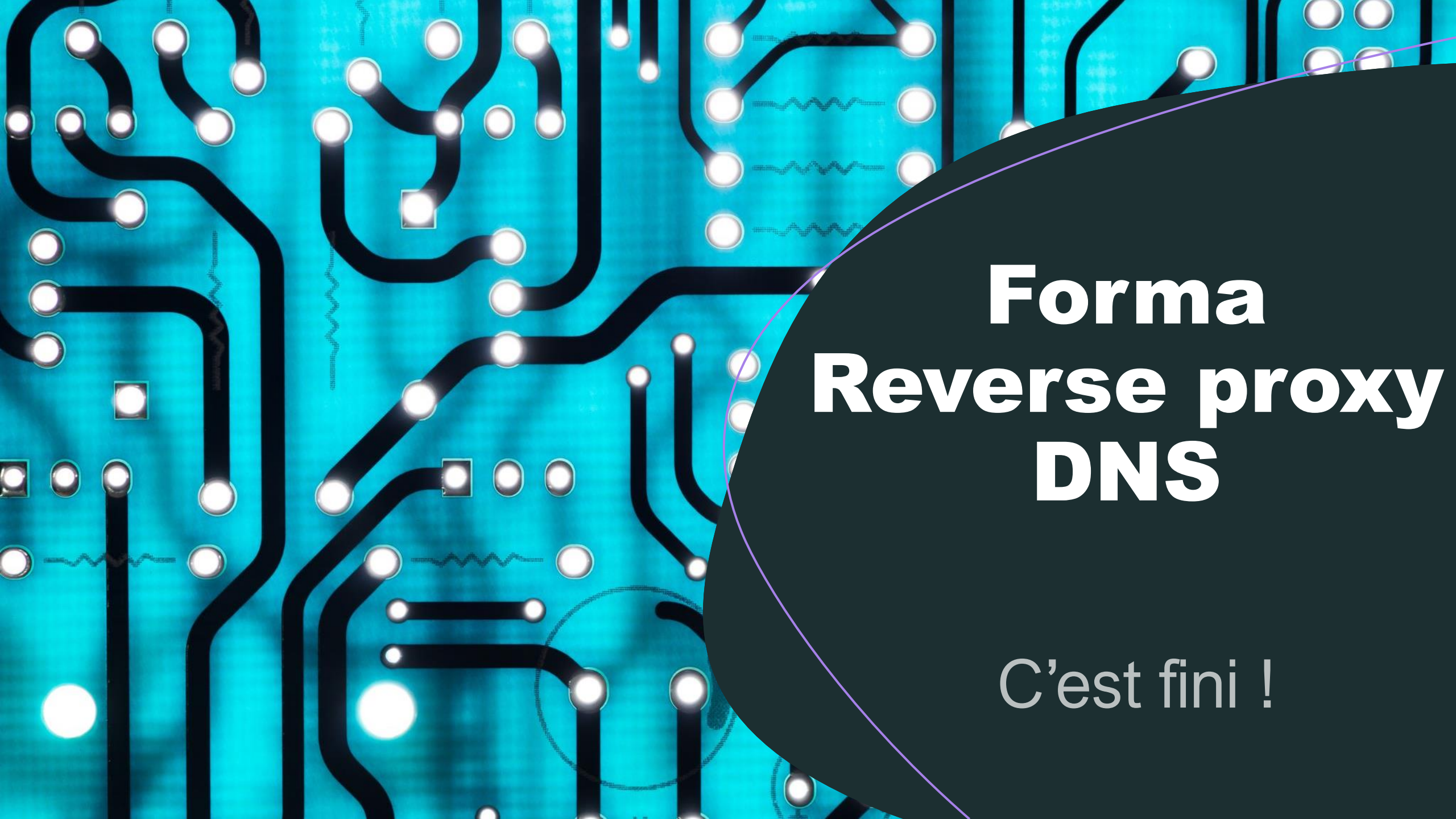
C’est quoi la HA ? (Haute Disponibilité)

On a 2 dns, 2 dhcp et 2 revproxy à minet

Chaque paire partage une IP commune et se répartie les requêtes en 2

Le but : si le premier casse, l’autre assure le travail le temps qu’il se remette à fonctionner





Forma
Reverse proxy
DNS

C’est fini !