Au sujet du DNS...

Bernard Szelag[1] et Julien Soula[1]

[1]Université de Lille

Min2Rien, novembre 2019

Université de Lille

Origine

- base de communication Internet = IP
- confort: attribution de noms à la place des IP

  $\hookrightarrow$ un fichier unique HOSTS.TXT
- mis à jour puis echangé entre les institutions

  $\hookrightarrow$ problème de taille et de synchronisation

nécessité d'une gestion répartie

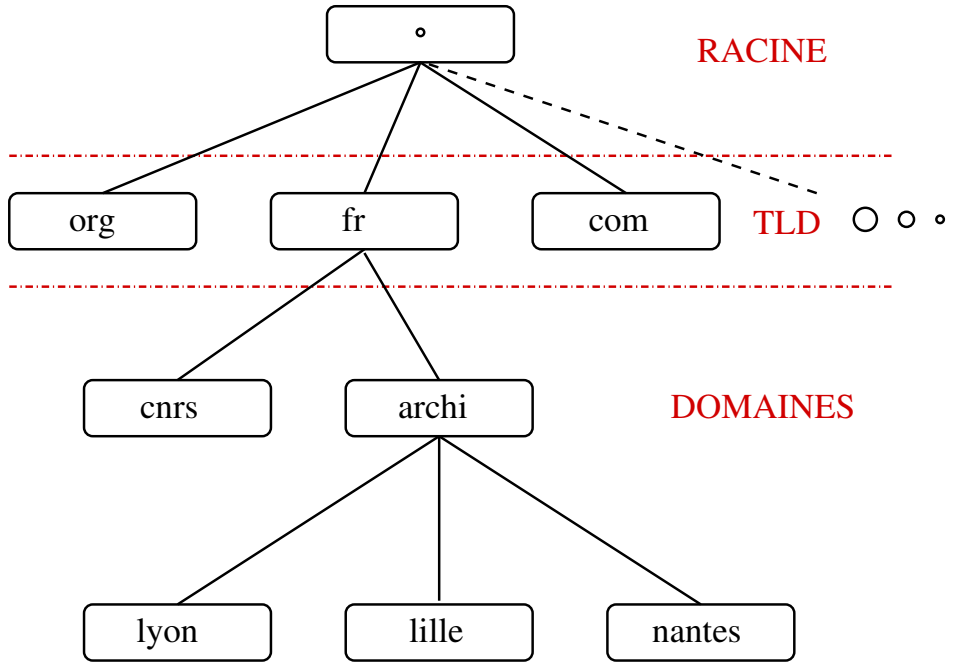
Université de Lille

domaine et hierarchie ($\sim$ 1984)

- attribution de domaines par entité géographique ou administrative (x.fr, y.com ..)

  $\hookrightarrow$ un domaine annonce un service de nom (DNS)

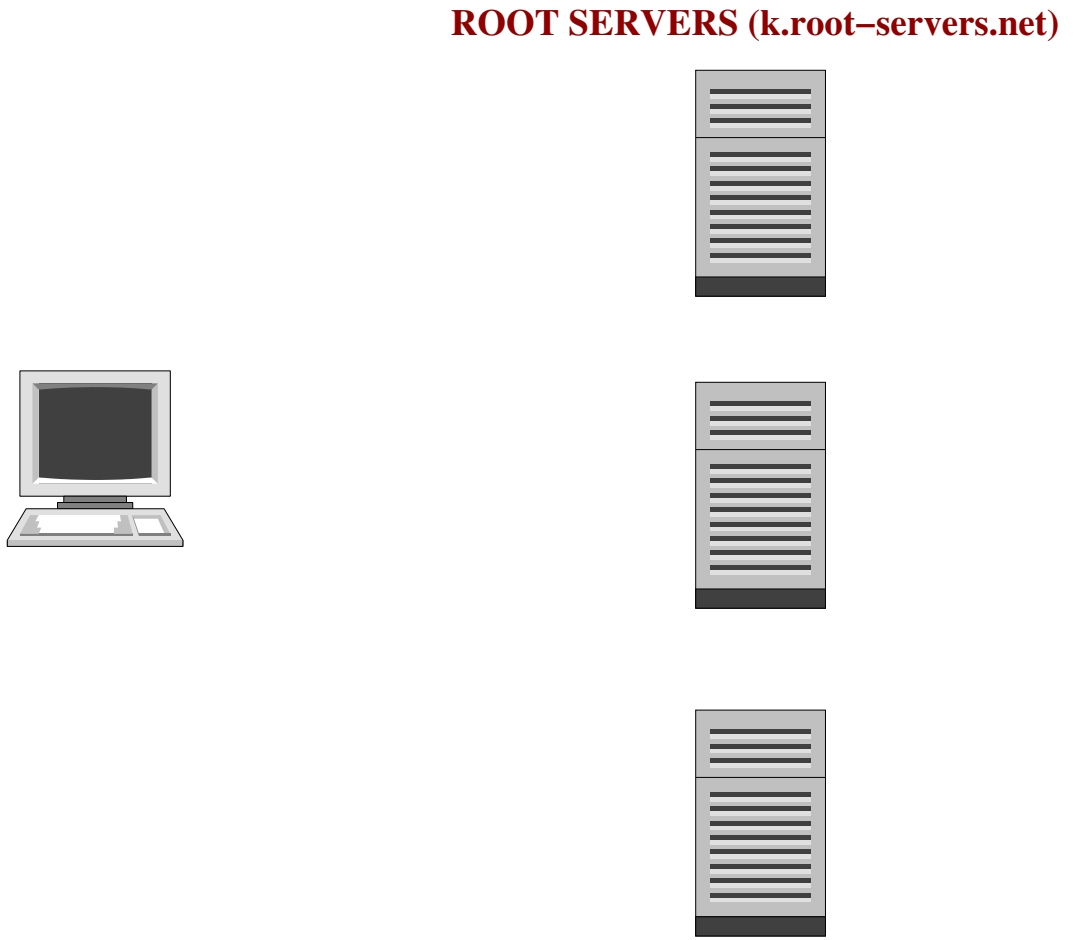
  $\hookrightarrow$ l'entité est SEULE responsable de sa mise à jour
- arborescence des domaines
- interrogation DNS: UDP/53 en clair



Université de Lille

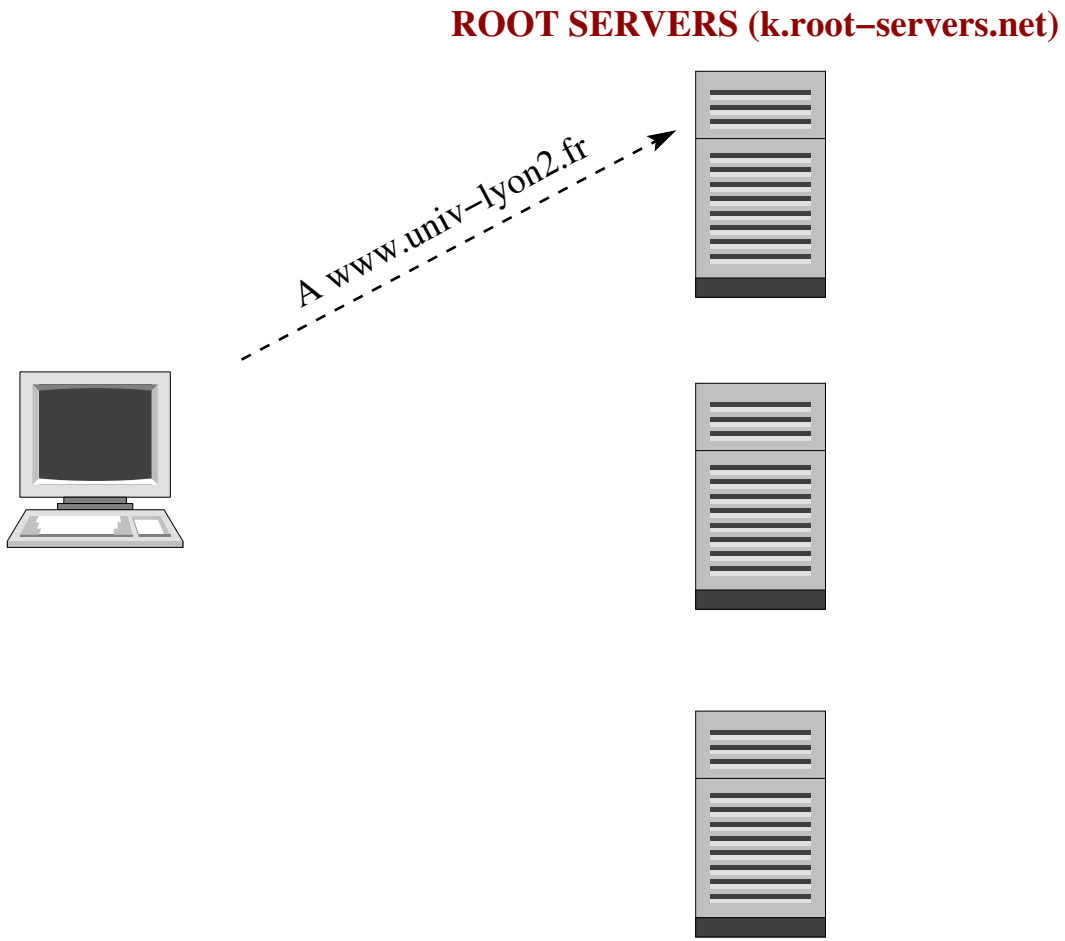
Comment ça marche ?

- point de départ: bootstrap: liste pré-établie des DNS de la Racine .



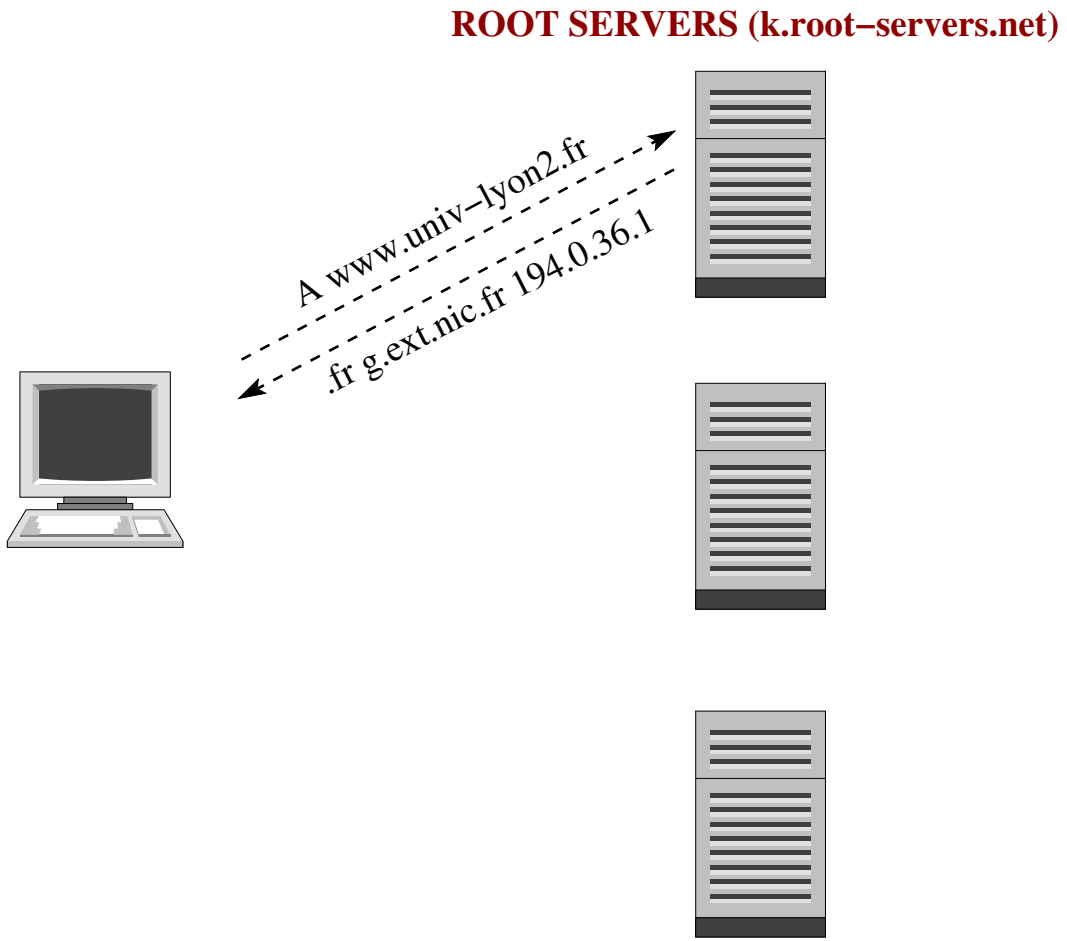
Comment ça marche ?

- point de départ: bootstrap: liste pré-établie des DNS de la Racine .



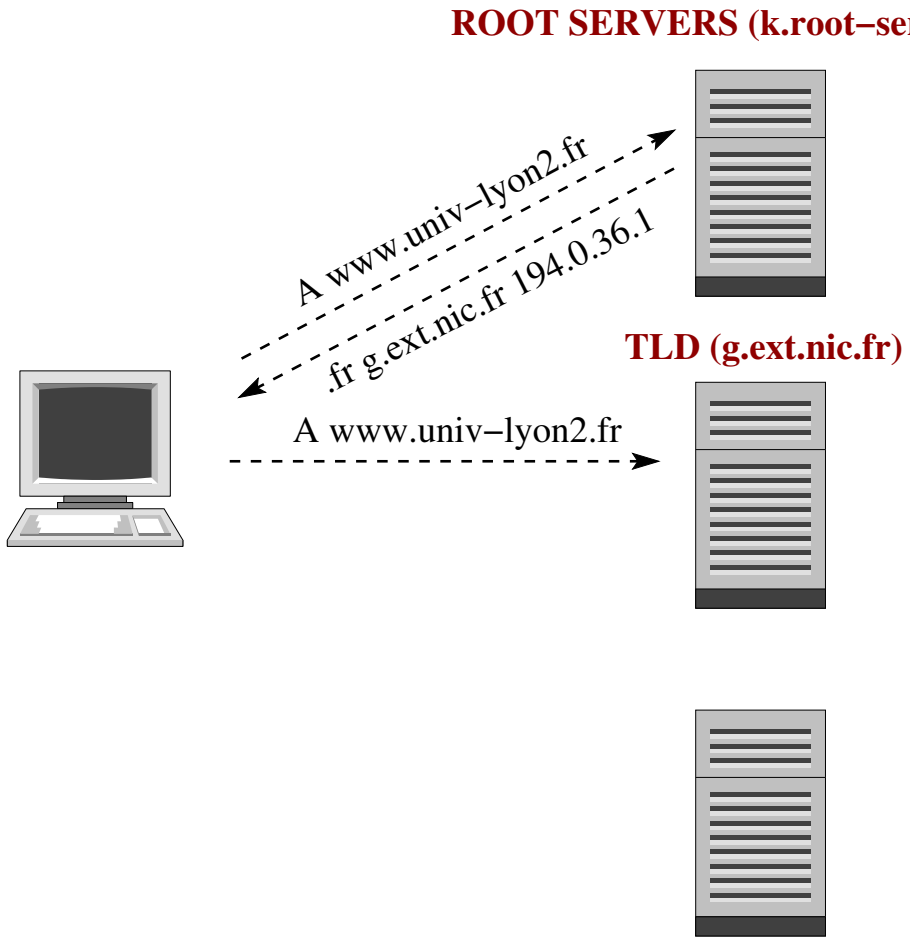
Comment ça marche ?

- point de départ: bootstrap: liste pré-établie des DNS de la Racine .



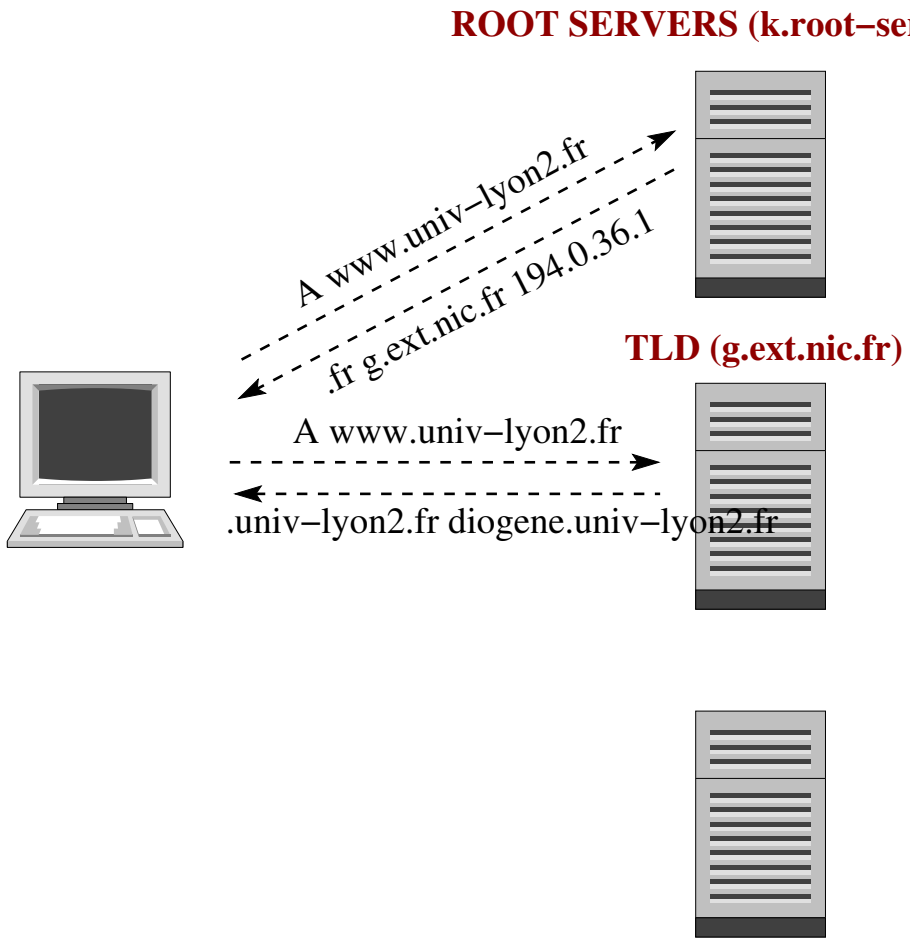
Comment ça marche ?

- point de départ: bootstrap: liste pré-établie des DNS de la Racine .



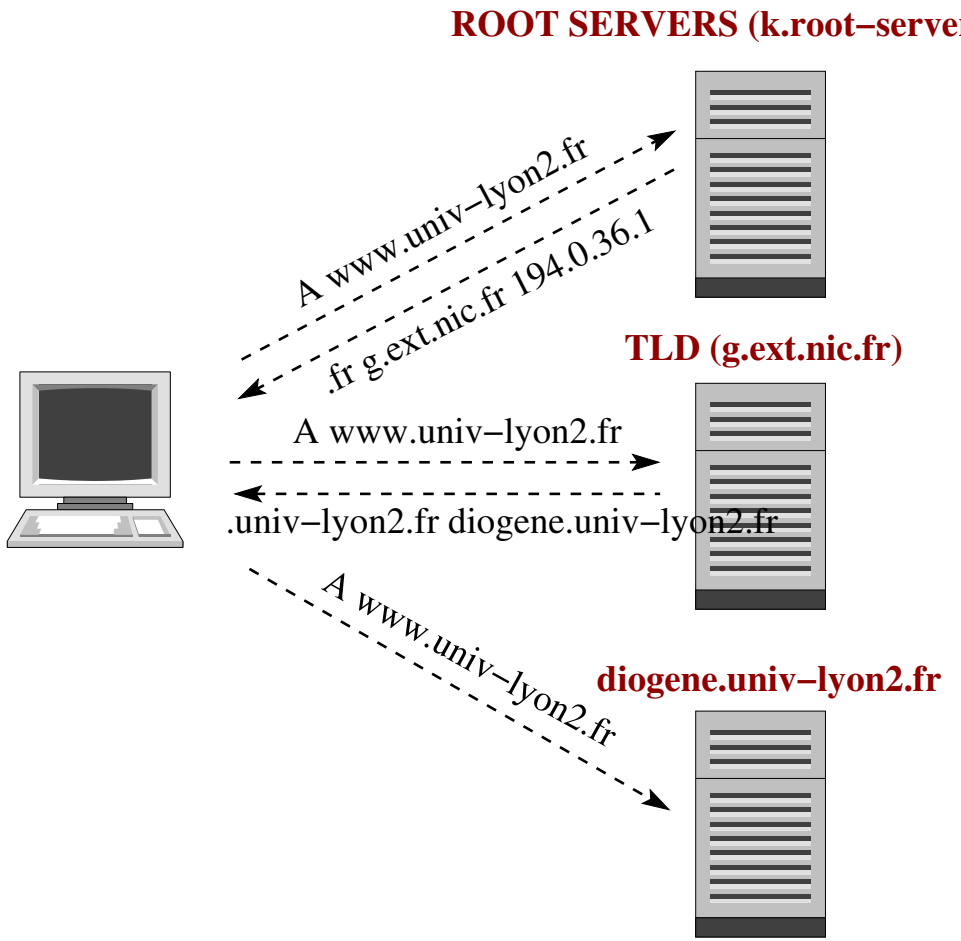
Comment ça marche ?

- point de départ: bootstrap: liste pré-établie des DNS de la Racine .



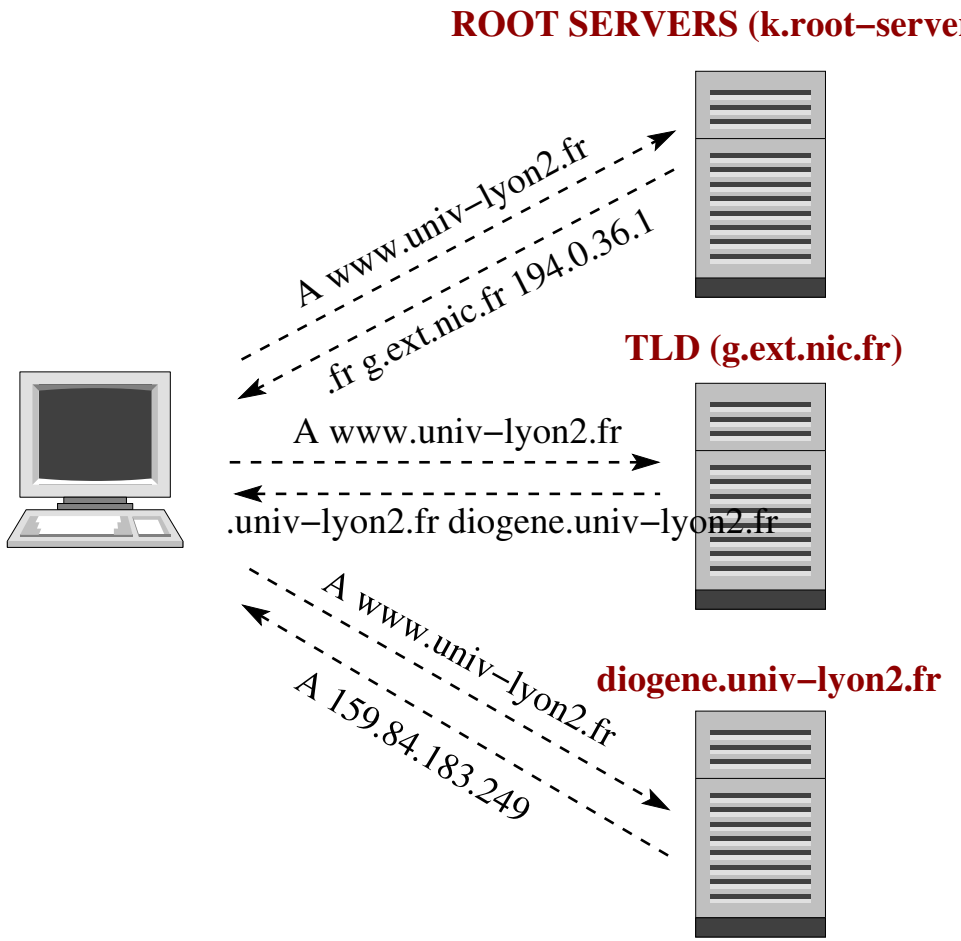
Comment ça marche ?

- point de départ: bootstrap: liste pré-établie des DNS de la Racine .



Comment ça marche ?

- point de départ: bootstrap: liste pré-établie des DNS de la Racine .



Université de Lille

quelles informations ?

- résolution IP, messagerie, services, sécurité
- Les requêtes DNS sont typées
  - A(ipv4), AAAA(ipv6), PTR(inverse)

```
mx01                          IN      A       193.49.225.81
ldap1                         IN      CNAME   anubis.univ-lille1.fr.
15.225.49.193.in-addr.arpa    IN      PTR     reserv1.univ-lille1.fr.
```

quelles informations ?

- résolution IP, messagerie, services, sécurité
- Les requêtes DNS sont typées
  - A(ipv4), AAAA(ipv6), PTR(inverse)
  - NS, MX(mail), SRV(services), TXT

```
mx01                          IN      A       193.49.225.81
ldap1                         IN      CNAME   anubis.univ-lille1.fr.
15.225.49.193.in-addr.arpa    IN      PTR     reserv1.univ-lille1.fr.

mx01                          IN      AAAA    2001:660:4401:100::81
_imaps._tcp                   IN      SRV     0 1 993 imap.univ-lille.fr.
univ-lille.fr.                IN      TXT     "v=spf1 mx ip4:193.49.225.4..."
```

quelles informations ?

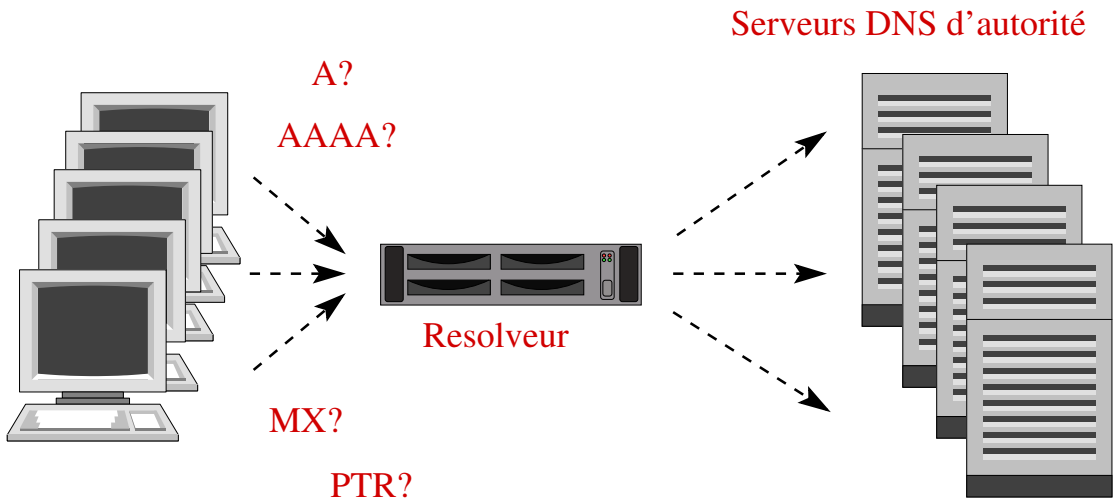
- résolution IP, messagerie, services, sécurité
- Les requêtes DNS sont typées
  - A(ipv4), AAAA(ipv6), PTR(inverse)
  - NS, MX(mail), SRV(services), TXT
  - TLSA(dane), RRSIG(dnssec)

```
mx01                          IN      A       193.49.225.81
ldap1                         IN      CNAME   anubis.univ-lille1.fr.
15.225.49.193.in-addr.arpa    IN      PTR     reserv1.univ-lille1.fr.

mx01                          IN      AAAA    2001:660:4401:100::81
_imaps._tcp                   IN      SRV     0 1 993 imap.univ-lille.fr.
univ-lille.fr.                IN      TXT     "v=spf1 mx ip4:193.49.225.4..."


 _443._tcp.www.freebsd.org.  3600 IN      TLSA    3 1 1 31EF2A4D6E285CC29A6DA8CC8 1187482A..
wfe0.nyi.freebsd.org.        3335     IN      RRSIG   A 8 4 3600 20191017 201911144..freebsd.org.
```

Le Résolveur

- Efficience/rationnalisation/contrôle

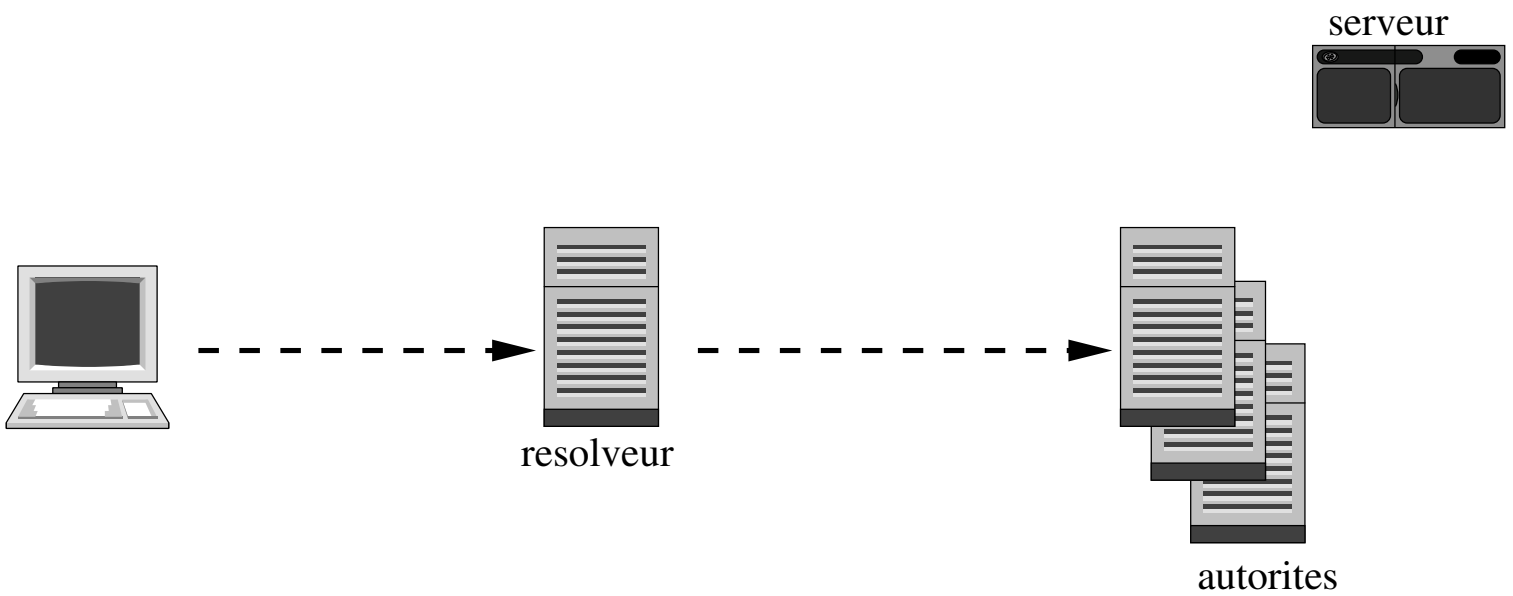
  ↪ Le résolveur: serveur DNS de résolution (proxy DNS)
  - utilisateur → resolveur → serveurs DNS d'autorité
- resolveur:
  - au sein d'une société, d'un FAI
  - public : 8.8.8.8 (google), 1.1.1.1 (cloudfare)
- distribué par DHCP → pour la plupart ceux de l'entité



Université de Lille

Enjeux

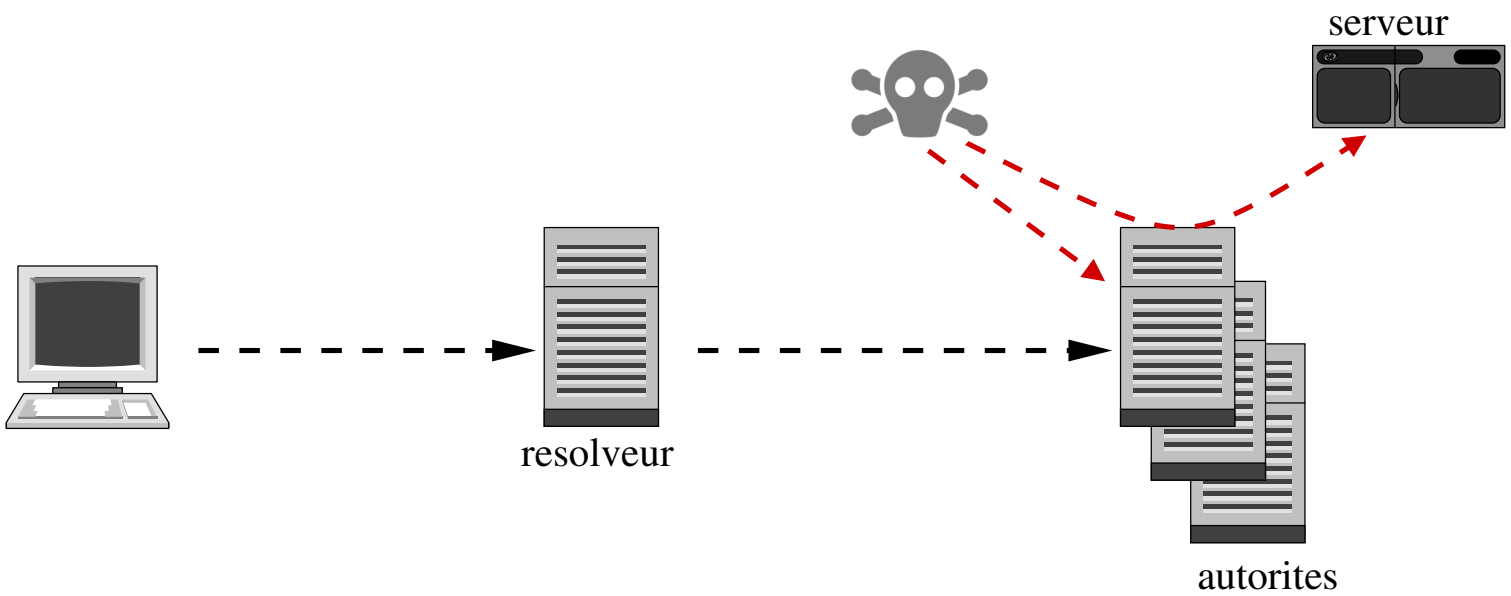
- fiabilité:
  - pas de résolution = pas d'Internet !!!
  - UDP en clair
    ↪ service crucial = cible d'attaque (DDOS, corruption, amplification réflexive ...)
- confidentialité (vie privée)
- neutralité/integrité (DNS menteur)



Université de Lille

Enjeux

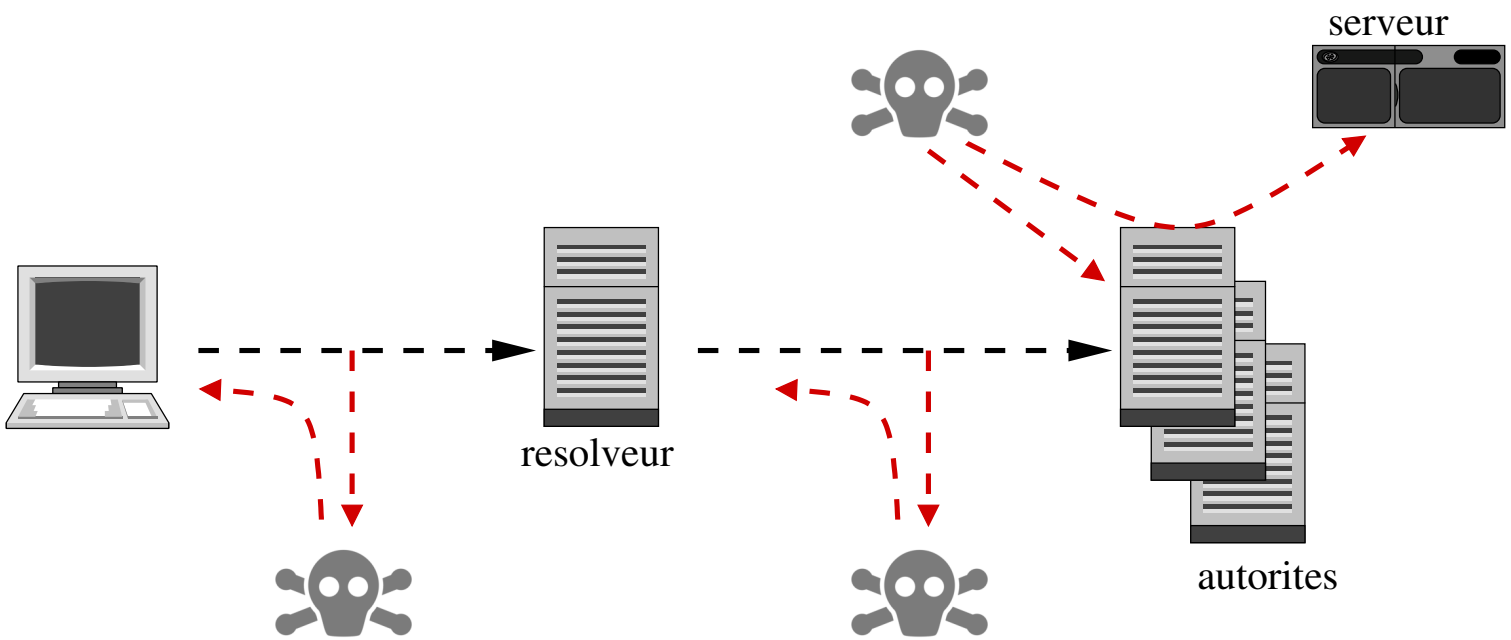
- fiabilité:
  - pas de résolution = pas d'Internet !!!
  - UDP en clair
    ↪ service crucial = cible d'attaque (DDOS, corruption, amplification réflexive ...)
- confidentialité (vie privée)
- neutralité/integrité (DNS menteur)



Université de Lille

Enjeux

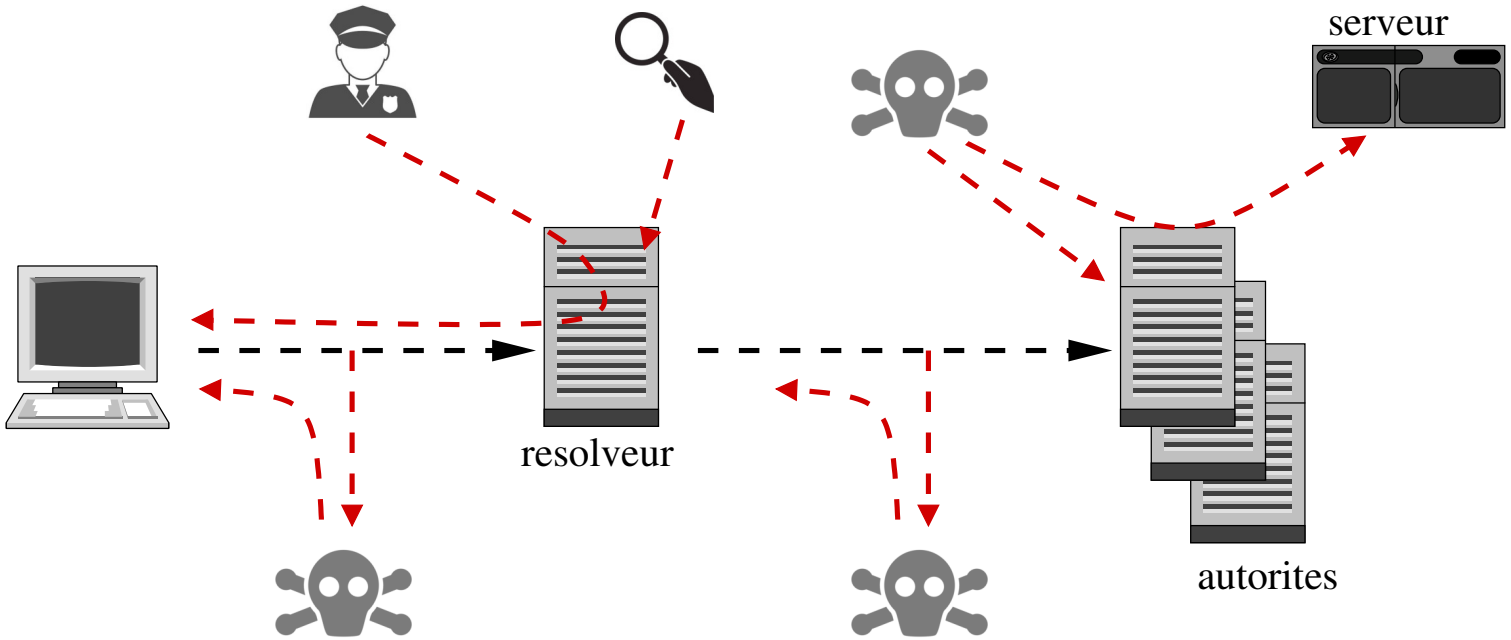
- fiabilité:
  - pas de résolution = pas d'Internet !!!
  - UDP en clair
    ↪ service crucial = cible d'attaque (DDOS, corruption, amplification réflexive ...)
- confidentialité (vie privée)
- neutralité/integrité (DNS menteur)



Université de Lille

Enjeux

- fiabilité:
  - pas de résolution = pas d'Internet !!!
  - UDP en clair
    ↪ service crucial = cible d'attaque (DDOS, corruption, amplification réflexive ...)
- confidentialité (vie privée)
- neutralité/integrité (DNS menteur)



Université de Lille

Vers plus de sécurité

- DNSSEC
- DNS over TLS (DoT)
- DNS over HTTPS (DoH)
- DNSCurve, DNSCrypt, CONFIDENTIAL-DNS...

Université de Lille

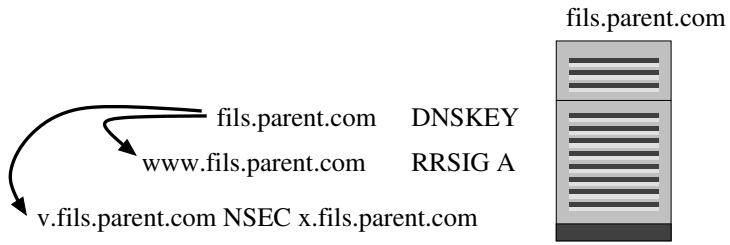
DNSSEC

- DNSSEC : signature des réponses
  - début travaux $\sim$ 2000
  - mature $\sim$ 2005
  - déploiement $\sim$ 2010
- complétement intégré au protocole DNS
- certification hiérarchique (DS/DNSKEY)

Université de Lille

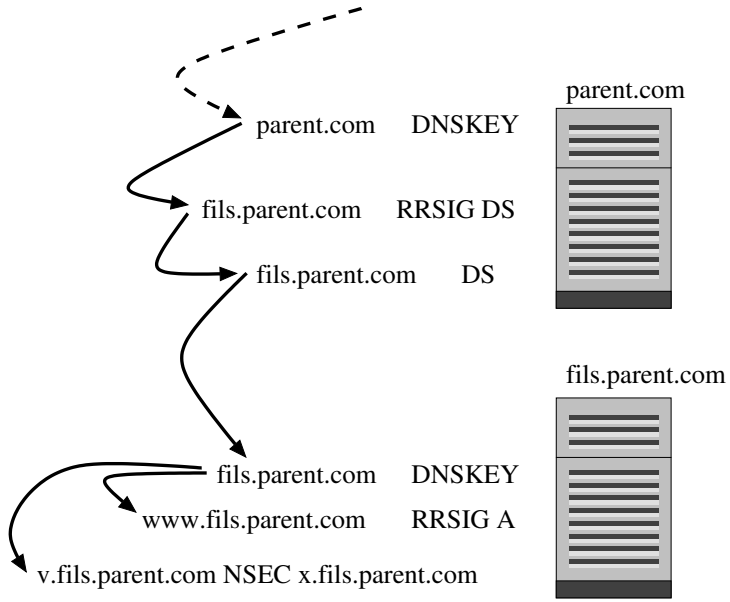
DNSSEC (fonctionnement)

```
wfe0.nyi.freebsd.org.    3600 IN RRSIG A 8 4 3600 (
                 20191127210714 20191114050314 10641 freebsd.org.
                 WlXzJvHyriwTJDWFyS9JN1Vujb6/2s81rY1oxEukNifp
                 uKFygKfMSE53uCJbI5ztorm1Ws50DjV2kXc/mOAt2acN
                 Tpuyeyec19C8QaPmbVbWi3ypHA4zhPzR152fEmYzp2c5
                 zepjZn2lMOdrmCwlmsdV8yYDoo7nI6v5tYTbLhYwB2gw
                 0rMF6FcJn01YyrNNROXeIY0RPC5sdwqcG3Vi6+xAzPfT
                 dgNpAVQgDP2zG7TiofmFOKXrDh0T2Dau2797bIggTakd
                 FfRSRQaANFWEu341hLeEuxxkFxxE1ZQd3ofJq6IR0mFI
                 hZvbtxTIn4PAJSOU3Mn+E7cQug6RDVTIJA== )
freebsd.org.         3600 IN DNSKEY 256 3 8 (
                 AwEAAcaXpHEUD71pzgttHWf97fiAfFWEek1dH1cVrtR3
                 n8YP3sZxI8QZo2HUWzJSJeIEDIpbTzUOEcMQU/MQtGZJ
                 udUdkowZ1uosoBID/PCjQkia/pOHSYSEItPSNvhQIVju
                 JIWEGnzjcjfGFDSt8W5QOAbjThqYnKoPwMduddp1JXIp
                 ZG2aBXEa3WBKBp/gaTLUEc0TyKS46r36AhHRsd6eV8Gk
                 bT+TLJyqg2ymmjJMkDECSSbHisdfTWfI2v1VsX0blibJ
                 CF5osB9cQQvpTIAg4jHtEAxk8W7hrFHydyR0a1Ja51ao
                 o/e69uqxRJN/M9Y3CTas+TukjKWFKbN1veL1Pr8=
                 ) ; ZSK; alg = RSASHA256 ; key id = 42019
.../...
freebsd.org.         86400 IN DS 32359 8 2 (
                 8A3535DDE847BE0B7AB7BFA6F8C917FE6E1E32DF96C3
                 76C1804F41F2E862F46A )
```



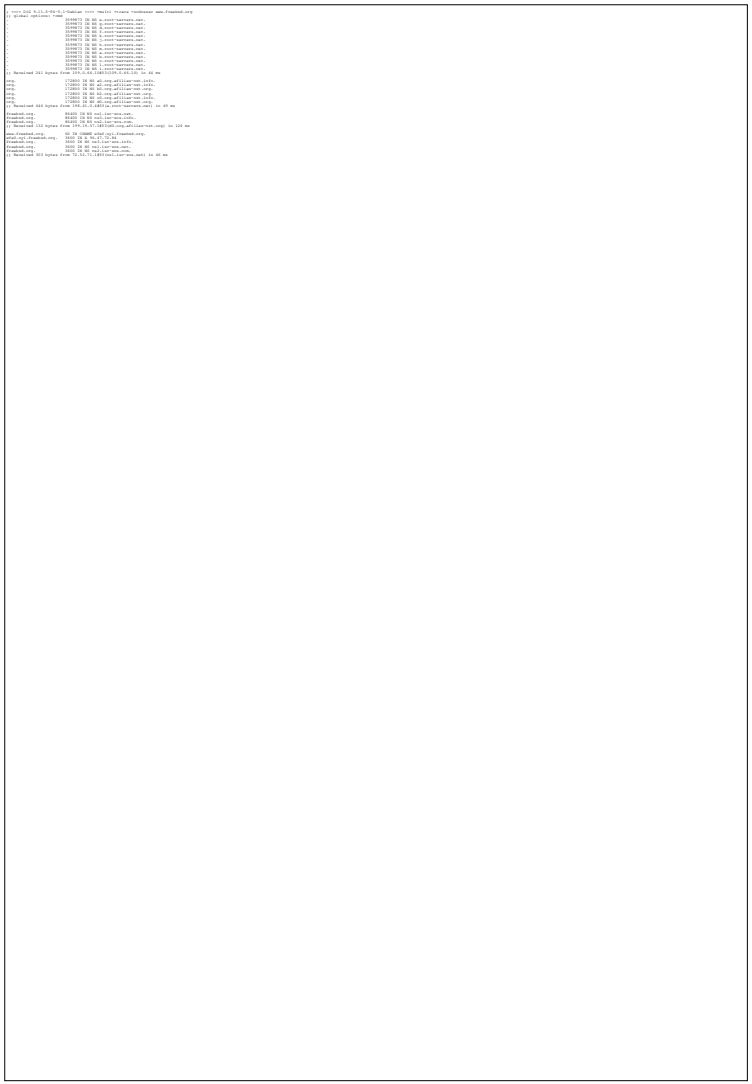
DNSSEC (fonctionnement)

```
wfe0.nyi.freebsd.org.    3600 IN RRSIG A 8 4 3600 (
                  20191127210714 20191114050314 10641 freebsd.org.
                  WlXzJvHyriwTJDWFyS9JN1Vujb6/2s81rY1oxEukNifp
                  uKFygKfMSE53uCJbI5ztorm1Ws50DjV2kXc/mOAt2acN
                  Tpuyeyec19C8QaPmbVbWi3ypHA4zhPzR152fEmYzp2c5
                  zepjZn2lMOdrmCwlmsdV8yYDoo7nI6v5tYTbLhYwB2gw
                  0rMF6FcJn01YyrNNROXeIY0RPC5sdwqcG3Vi6+xAzPfT
                  dgNpAVQgDP2zG7TiofmFOKXrDh0T2Dau2797bIggTakd
                  FfRSRQaANFWEu341hLeEuxxkFxxE1ZQd3ofJq6IR0mFI
                  hZvbtxTIn4PAJSOU3Mn+E7cQug6RDVTIJA== )
freebsd.org.          3600 IN DNSKEY 256 3 8 (
                  AwEAAcaXpHEUD71pzgttHWf97fiAfFWEek1dH1cVrtR3
                  n8YP3sZxI8QZo2HUWzJSJeIEDIpbTzUOEcMQU/MQtGZJ
                  udUdkowZ1uosoBID/PCjQkia/pOHSYSEItPSNvhQIVju
                  JIWEGnzjcjfGFDSt8W5QOAbjThqYnKoPwMduddp1JXIp
                  ZG2aBXEa3WBKBp/gaTLUEc0TyKS46r36AhHRsd6eV8Gk
                  bT+TLJyqg2ymmjJMkDECSSbHisdfTWfI2v1VsX0blibJ
                  CF5osB9cQQvpTIAg4jHtEAxk8W7hrFHydyR0a1Ja51ao
                  o/e69uqxRJN/M9Y3CTas+TukjKWFKbN1veL1Pr8=
                  ) ; ZSK; alg = RSASHA256 ; key id = 42019
.../...
freebsd.org.          86400 IN DS 32359 8 2 (
                  8A3535DDE847BE0B7AB7BFA6F8C917FE6E1E32DF96C3
                  76C1804F41F2E862F46A )
```

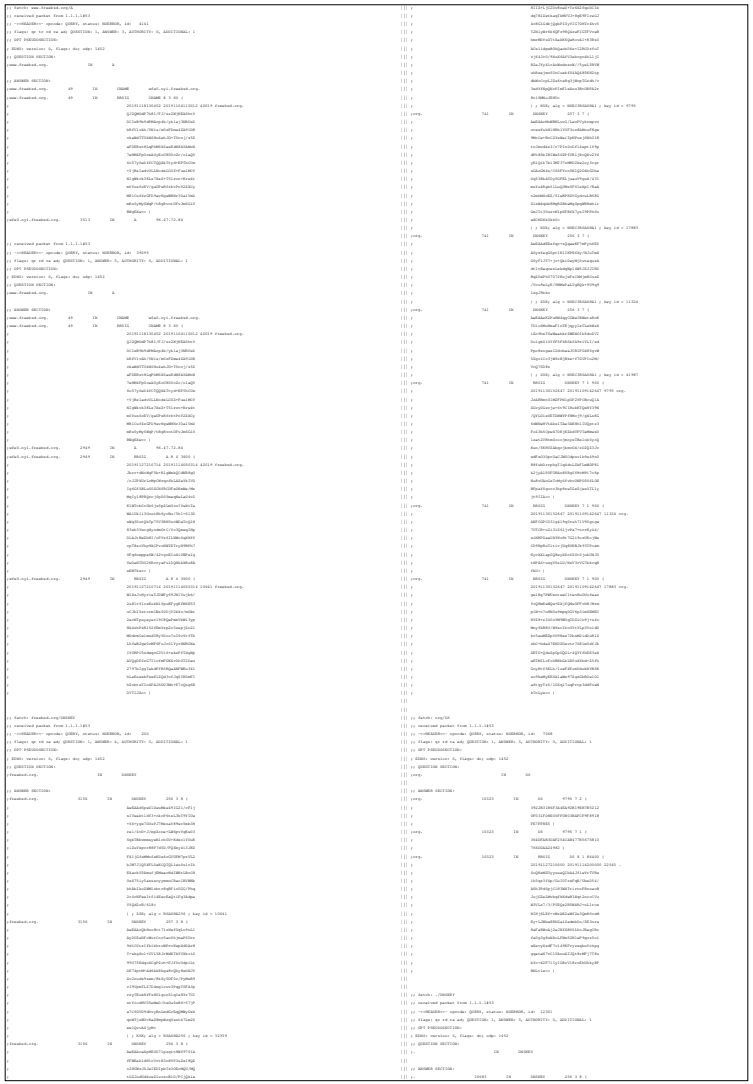


DNSSEC (exemple)

Sans DNSSEC



Avec DNSSEC



DNSSEC (deploiement)

- la plupart des serveurs/résolveurs le supportent
- client: se fie au résolveur (flag `AD`)
- zones signés: majoritaire en haut, peu en bas ($< 1\%$ en `.com`)

Université de Lille

DoT

- DNS over TLS (DoT) :
  - simple couche TLS mais protocole inchangé
  - RFC7858 $\sim$ 2016
  - TCP/853
  - entre le client et le résolveur
- Deploiement mitigé
  - serveur: résolveurs publiques OK, qqs applications (`unbound`), possibilité de stunnel
  - client: option dans systemd

Université de Lille

DoH

- DNS over HTTPS (DoH) :
  - RFC oct 2018
  - paquet DNS dans une requête HTTPS
  - TLS déjà présent
  - enfoui dans le traffic web

www.example.com $\rightarrow$ *93.184.216.34*

```
https://cloudflare-dns.com
POST /dns-query
Length:  33 [application/dns-message]
00 00 01 00 00 01 00 00 00 00 00 00 03 77 77 77
07 65 78 61 6d 70 6c 65 03 63 6f 6d 00 00 01 00
01

HTTP/1.1 200 OK
Length:  128 [application/dns-message]
00 00 81 A0 00 01 00 01 00 00 00 01 03 77 77 77
07 65 78 61 6D 70 6C 65 03 63 6F 6D 00 00 01 00
01 C0 0C 00 01 00 01 00 00 24 5C 00 04 5D B8 D8
22 00 00 29 05 AC 00 00 00 00 00 44 00 0C 00 40
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Université de Lille

DoH et Mozilla

- Annonce d'origine (septembre 2019)
  - introduire la résolution DoH dans les navigateurs → ignore le résolveur systeme
  - désactivation trés difficile (about:config)
  - pré-configuré par défaut vers CloudFare
  - accord Mozilla/CloudFare : confidentialité
- Raisons
  - défiance vis a vis des résolveurs "officiels"
  - CloudFare: CDN de beaucoup de sites → non filtrable

Université de Lille

DoH et Mozilla (suite)

- problématique
  - filtrage : contrôle parental, sites dangereux ...
  - split DNS : vue intérieure / vue extérieure
  - sincérité de CloudFare

Université de Lille

DoH et Mozilla (suite)

- problématique
  - filtrage : contrôle parental, sites dangereux ...
  - split DNS : vue intérieure / vue extérieure
  - sincérité de CloudFare
- Corrections
  - possibilité de désactivation et de changement d'URL
  - mécanismes intelligents de désactivation si nécessaire (non définis)
    $\hookrightarrow$ domaine *canary* (temporaire) : `use-application-dns.net.`

Université de Lille

DoH (deploiement)

- navigateurs
  - chrome
    - ★ *opt out*
    - ★ résolveur Google
    - ★ serveur dedié donc filtrable
  - Safari/IE/Opera : non implementé pour l'instant
- serveurs : CloudFare, Google, OpenDNS... `www.bortzmeyer.org`
- applicatif : front-end DoH (cloudfared, facebook, PowerDNS ...)

Université de Lille

Conclusion

- au cours du temps $\rightarrow$ fonctionalités et criticités accrues
- pique de fievre : mail, http... et maintenant le DNS (maillon faible)
- prise de conscience récente du besoin de sécurité et de confidentialité

  $\hookrightarrow$ des solutions sans remettre en cause le protocole de base