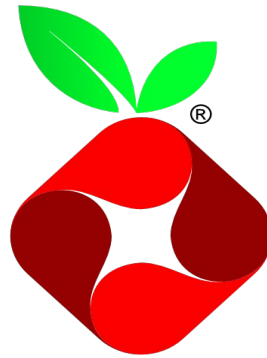


« Pi-hole, un bloqueur de pubs pour ta box»



@Benzo, 13.03.21

Root66.net



Internet & vie privée :

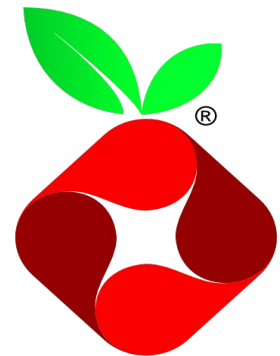
- ✓ Le traçage de nos activités numériques : Qui ? Comment ?
- ✓ Quelques rappels sur le Dns , ce grand bavard !
- ✓ Les bloqueurs de pubs existants

Pihole : (une) solution pour filtrer comme un chef !

- ✓ Principe – avantages - inconvénients
- ✓ Installation & configuration (Démon)
- ✓ Ya quoi sous le capot ?

Pihole : pour aller plus loin

- ✓ Contrôle parental
- ✓ Unbound , wireguard, doh, https ihm admin ...
- ✓ Les alternatives



La surveillance numérique

Un certain nombre d'**acteurs surveillent et tracent** nos actions, nos comportements en ligne à des fins :

- économiques (pub) : gafam ; régies publicitaires
- politiques (censure, surveillance, espionnage...)
- motifs privés (proches indiscrets)

intérêts divergents

Quelques techniques de tracking



- le **cookie** (first-party – tiers – pixel invisible)
- le fingerprinting (empreinte numérique)

Exemple de tracking

Page d'accueil du site de BFMTV consultée avec Firefox :

31 requêtes bloquées !!

The screenshot shows the BFMTV website in a Firefox browser. The uBlock Origin extension is active, displaying a list of blocked domains and statistics. The website content includes a main article about European elections and a 'News 24/7' sidebar.

uBlock Origin 1.19.4

Domain	Action
facebook.net	++
01net.com	-
accengage.net	+
adleadvent.com	-
brightcove.com	+
chartbeat.com	-
elasticad.net	-
estat.com	-
ew3.lo	-
facebook.net	-
google-analytics.com	-
google.com	+
hubvisor.io	-
medlarithmics.com	-
nuggad.net	-
outbrain.com	-

Requêtes bloquées

sur cette page :
31, soit 31%

depuis toujours :
111, soit 20%

Domaines connectés

4 sur un total de 21

BFMTV

EUROPÉENNES 2019 VIDÉOS POLITIQUE POLICE-JUSTICE INTERNATIONAL SOCIÉTÉ ÉCONOMIE TECH AUTO SANTÉ SPORT PEOPLES

Européennes: Édouard Philippe paiera-t-il les pots cassés d'une défaite de LaREM?

News 24/7

- 06:54 Chili : six touristes brésiliens meurent intoxiqués dans une location Airbnb
- 06:31 Un indépendantiste élu à la tête du Congrès de Nouvelle-Calédonie
- 00:11 Européennes: Macron interviewé par le youtubeur Hugo Travers pour convaincre les jeunes d'aller voter
- 23/05 Haute-Savoie: trente ans de réclusion pour un infanticide par vengeance

DIRECT

Les traces : ya pas que le web !

Même sans navigateur sur internet, la surveillance s'opère aussi à partir :

- De l'OS :
 - **windows 10**
 - **Android** et son écosystème google
 - télémétrie, pubs, géolocalisation etc...**
- Des applications
 - => trackers embarqués ds les applis
 - (smartphone – TV – montres...)

La TV : exemple de requêtes DNS

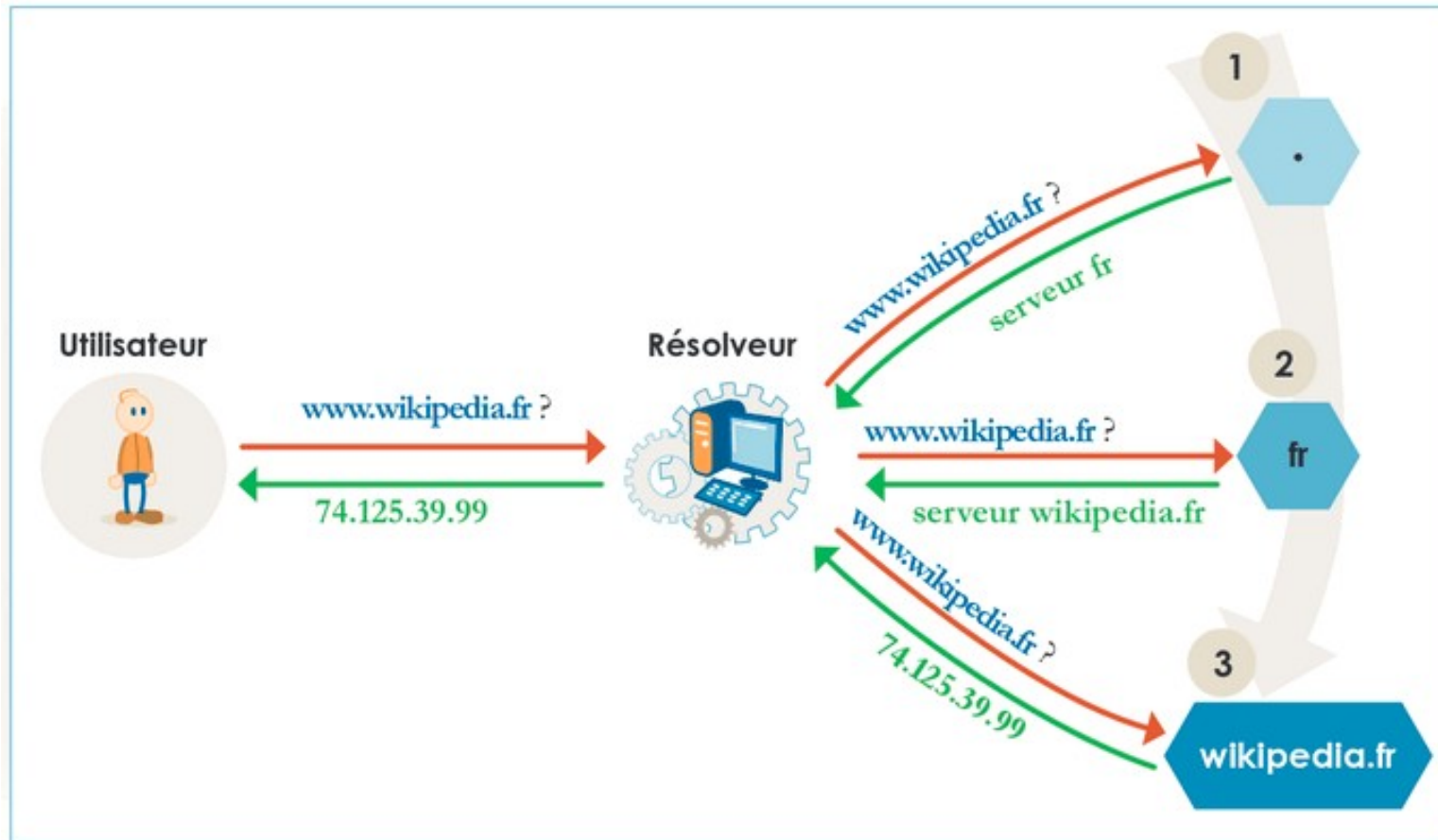
Time	Type	Domain	Client	Status	Reply	Action
2019-05-19 17:50:14	A	fr.lgtvsdp.com	192.168.0.35	OK (cached)	CNAME (0.7ms)	 Blacklist
2019-05-19 17:50:13	A	fr.lgtvsdp.com	192.168.0.35	OK (forwarded)	N/A	 Blacklist
2019-05-19 17:50:09	A	fr.ad.lgsmartad.com	192.168.0.35	OK (forwarded)	N/A	 Blacklist
2019-05-19 17:50:06	A	ichnaea.netflix.com	192.168.0.35	OK (forwarded)	CNAME (5.9ms)	 Blacklist
2019-05-19 17:49:54	A	api-global.netflix.com	192.168.0.35	OK (forwarded)	CNAME (5.3ms)	 Blacklist
2019-05-19 17:49:30	A	rdvs.alljoyn.org	192.168.0.35	OK (forwarded)	NXDOMAIN (5.8ms)	 Blacklist
2019-05-19 17:49:30	A	rdvs.alljoyn.org	192.168.0.35	OK (cached)	NXDOMAIN (0.6ms)	 Blacklist
2019-05-19 17:49:28	A	nrdp.nccp.netflix.com	192.168.0.35	OK (forwarded)	CNAME (16.4ms)	 Blacklist

Point commun à toutes ses techniques de traçage numérique

Le traçage numérique commence toujours par ...

une requête DNS

Résolution DNS



Source image: skyminds.net

Et le réseau à la maison ?

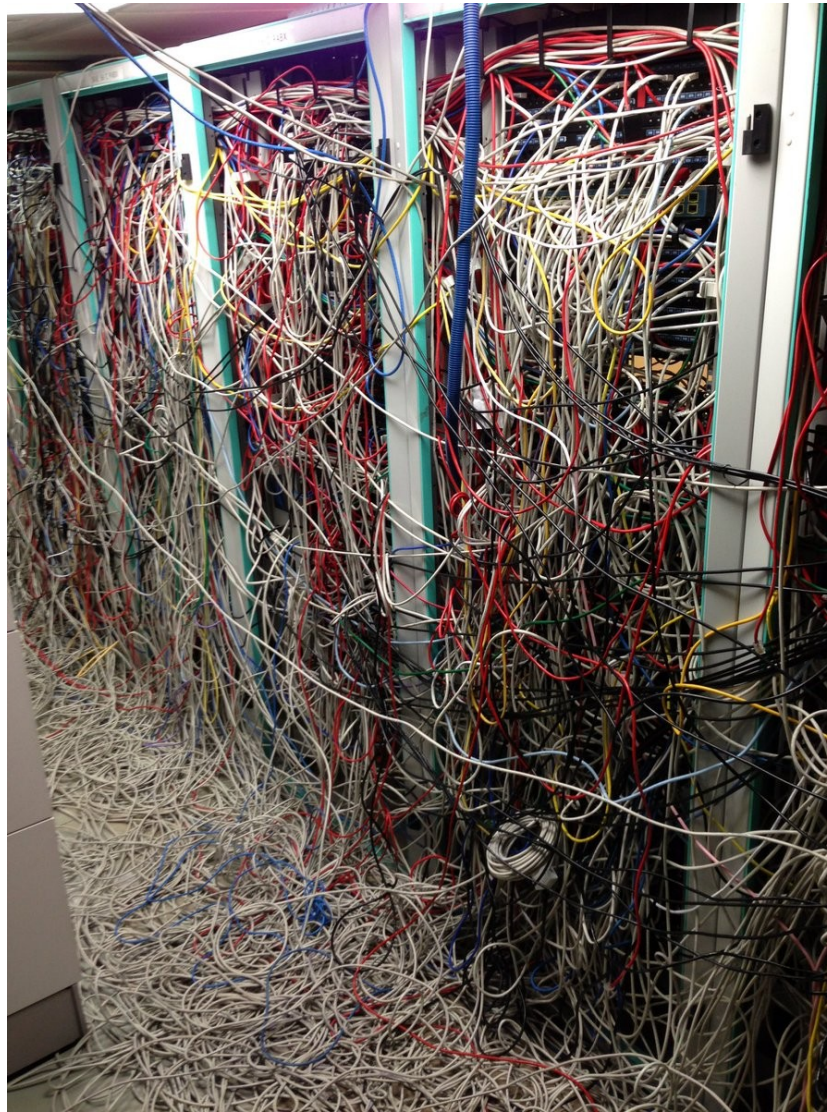
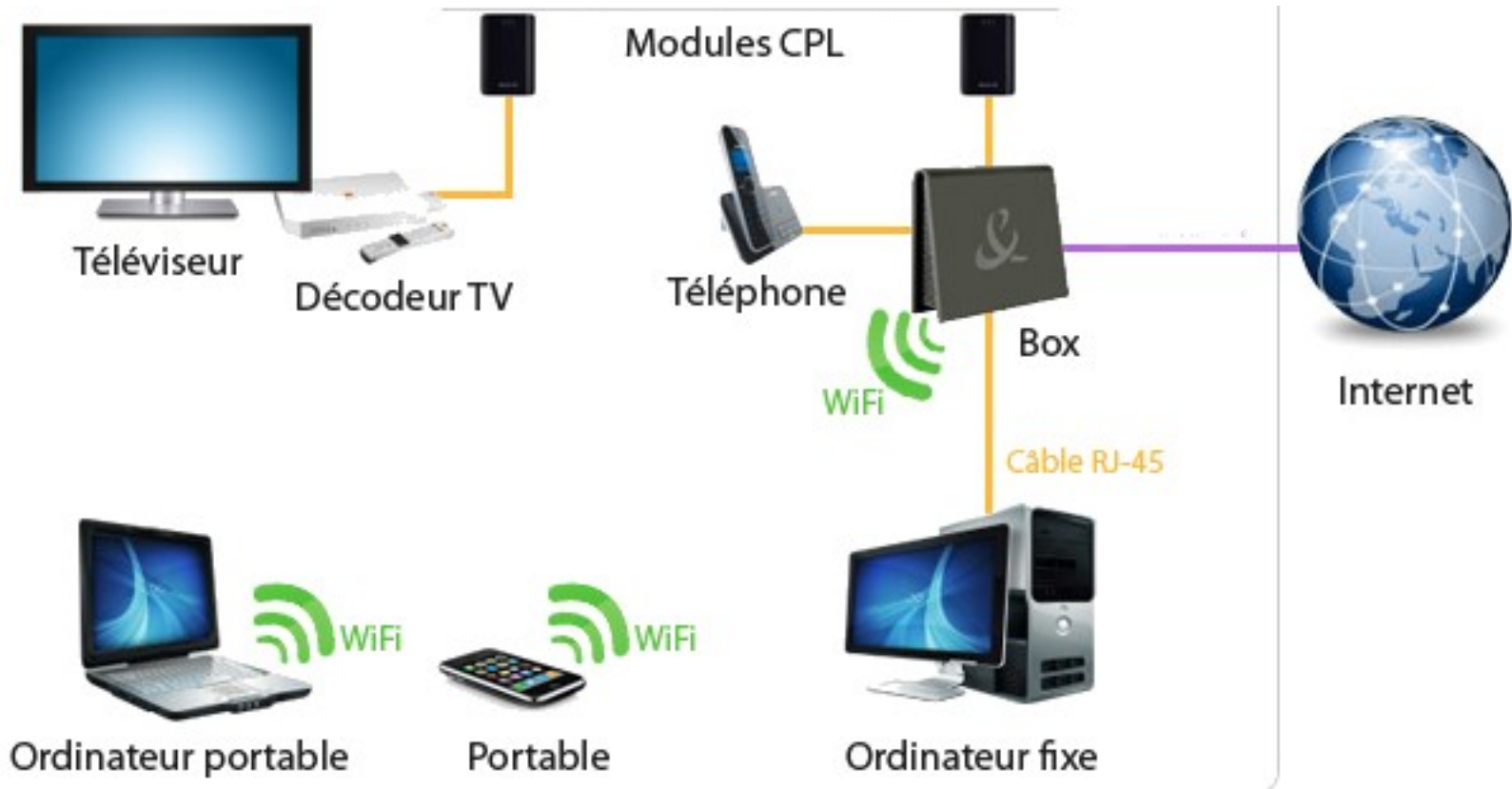


Schéma réseau maison



Le monde se divise en 2 catégories...
de serveur DNS



Vocabulaire serveur DNS

→ 2 types de serveurs DNS :

- **Serveur faisant autorité :**
connaissent infos sur le **contenu des domaines**.
Ex: serveurs de l'AFNIC connaissent contenu de FR.
- **Résolveur (ou récursif):**
 - Situé entre le client et le serveur faisant autorité. Au démarrage il ne sait rien mis à part les adresses de la **racine**.
 - Il **mémore les réponses (système de cache)**
 - Chez M.Lambda, résolveur = **box**

Les différents résolveurs 1/3

Résolveurs DNS
fournis par
nos **FAI**

=

Embarqué dans la box
Distribués via DHCP

- Lents
- Vie privée = BOF !
- DNS menteurs
- impossible à changer
(orange ?)

Liste des serveurs DNS des principaux opérateurs

DNS Bouygues

 194.158.122.10
194.158.122.15

DNS Free

 212.27.40.240
212.27.40.241

DNS de SFR

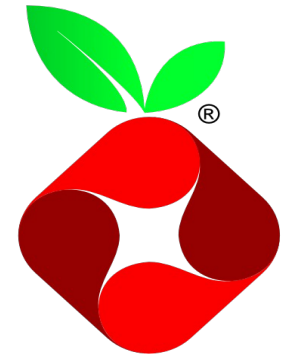
 109.0.66.10
109.0.66.20

DNS Orange

 80.10.246.2
80.10.246.129

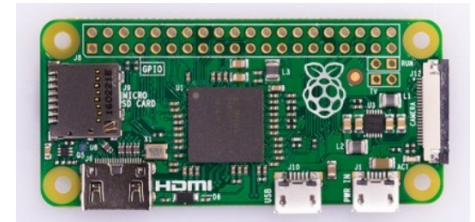
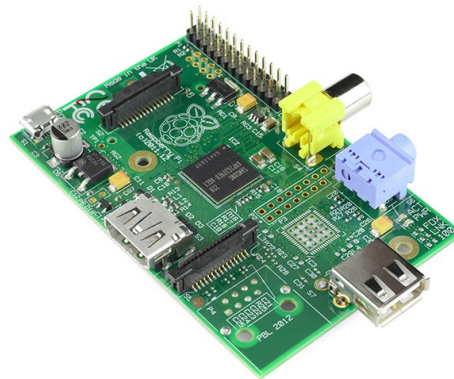
Pihole : présentation

- **bloqueur de pubs**
- d'une manière générale filtre les requêtes dns indésirables sur tout un réseau
- agit comme un dns menteur

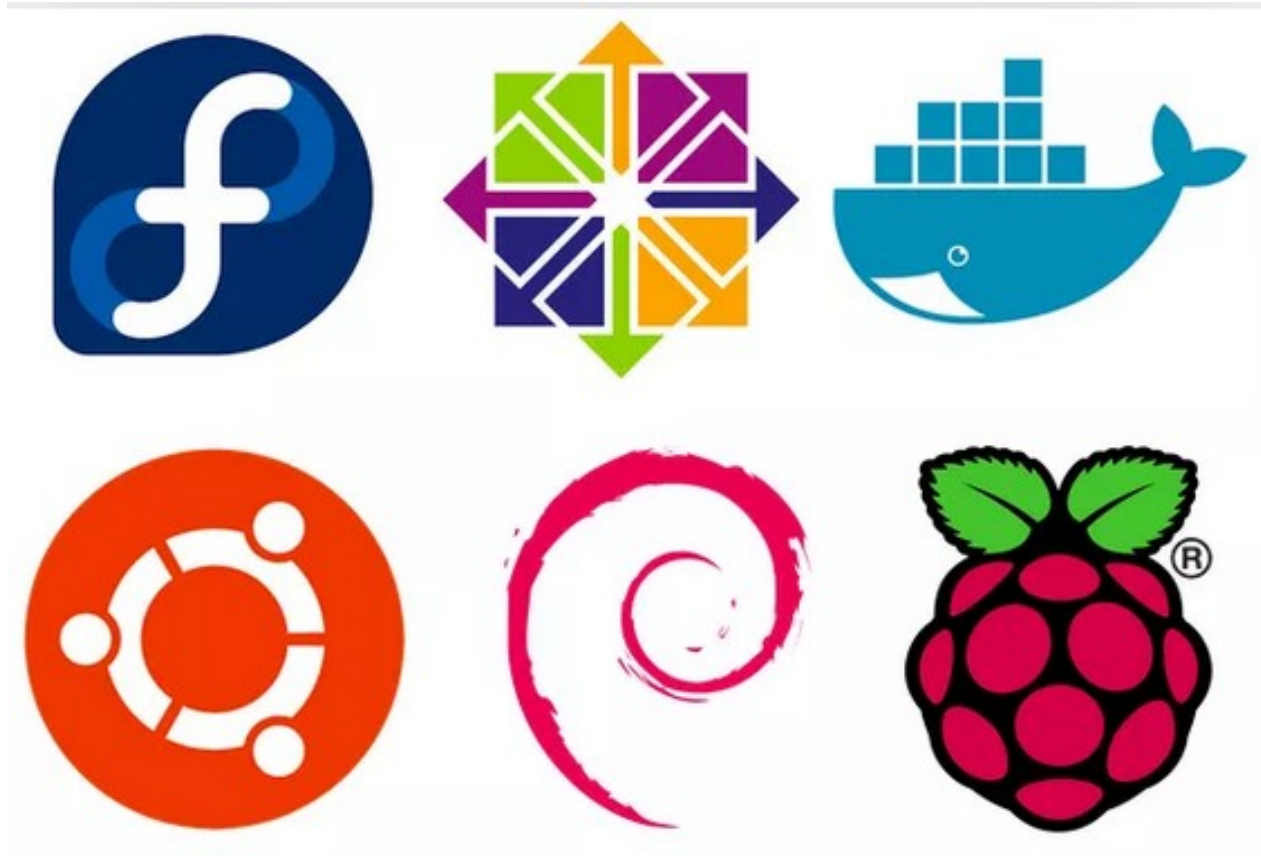


Installation : physique

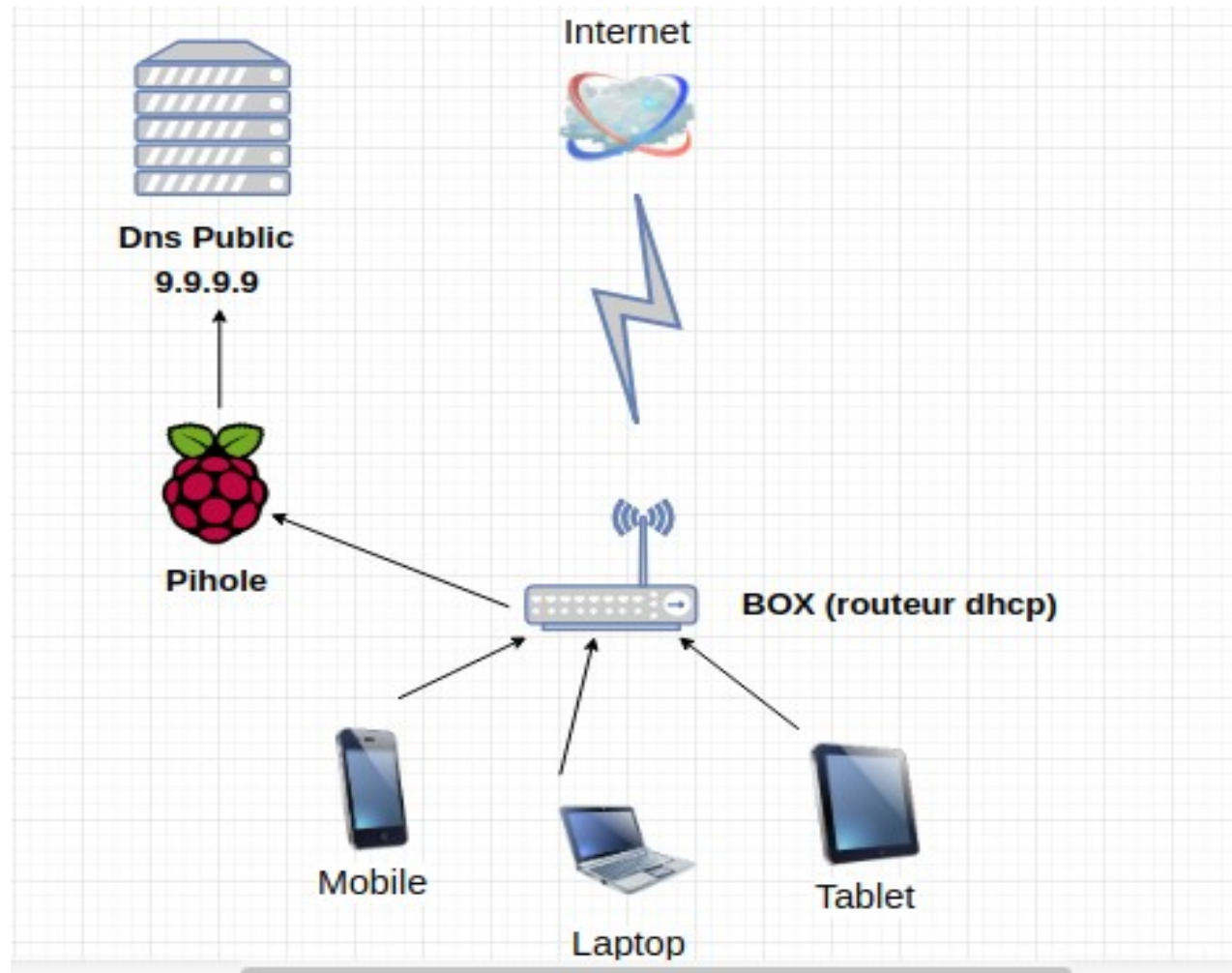
- Sur **raspberry** (le + économique)
- Sur un vieux pc , sur un Nas, sur son laptop ...
- Environnement virtualisé possible
- => Image docker
- => Machine Virtuelle



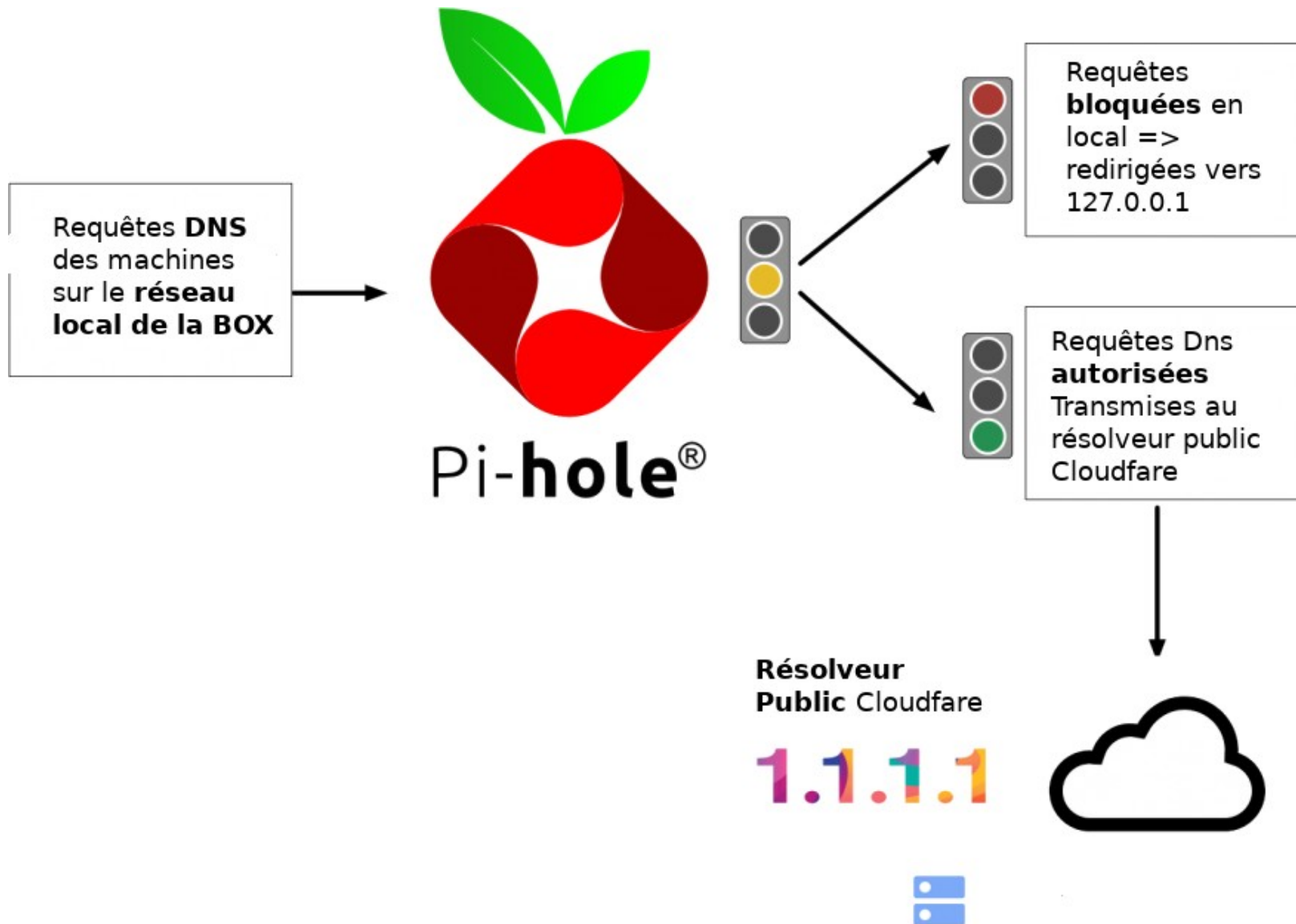
Installation : quel OS ?



Le pihole dans tout ça ?



Le pihole dans tout ça ?



Pihole : son action

1. Le pc client demande au pihole :
« Quelle est l'@IP de fr.wikipedia.org ? »
2. *Le pihole regarde dans son cache si la réponse est déjà connue.*
3. *Le pihole vérifie sa liste si le domaine est « blacklisté »*
4. Si pas connu du cache et non blacklisté , le pihole **transmet la requête au résolveur public** . Ex : Cloudfare
5. Le pihole reçoit la réponse et la transmet au pc client
6. Le pihole garde **en cache la réponse**
=> ce qui lui permettra de répondre beaucoup plus vite la prochaine fois!!!

Avantages du Pi-hole

- Filtre au niveau du réseau **toutes les requêtes DNS** de **tous les appareils connectés** à la box
- application légère , libre , multiplateforme, « autohébergeable »
- Améliore la vie privée (antipubs, trackers, malwares...)
- Améliore la bande passante (cache et moins de trafic DNS)
- Administration centralisée et facile , simple à installer
- Fonctionnalités supplémentaires intéressantes
(DHCP, contrôle parental, service de nommage interne des machines, DNSSEC ...)



Démonstration



Pihole : ya quoi sous le capot ?



Pihole : installation logicielle

- 1) En une seule ligne de commande
- 2) (méthode non sécurisée, à vos risques)



`curl -sSL https://install.pi-hole.net | sudo bash`



Pihole : installation logicielle

Méthode conseillée



1) Clône du dépôt distant

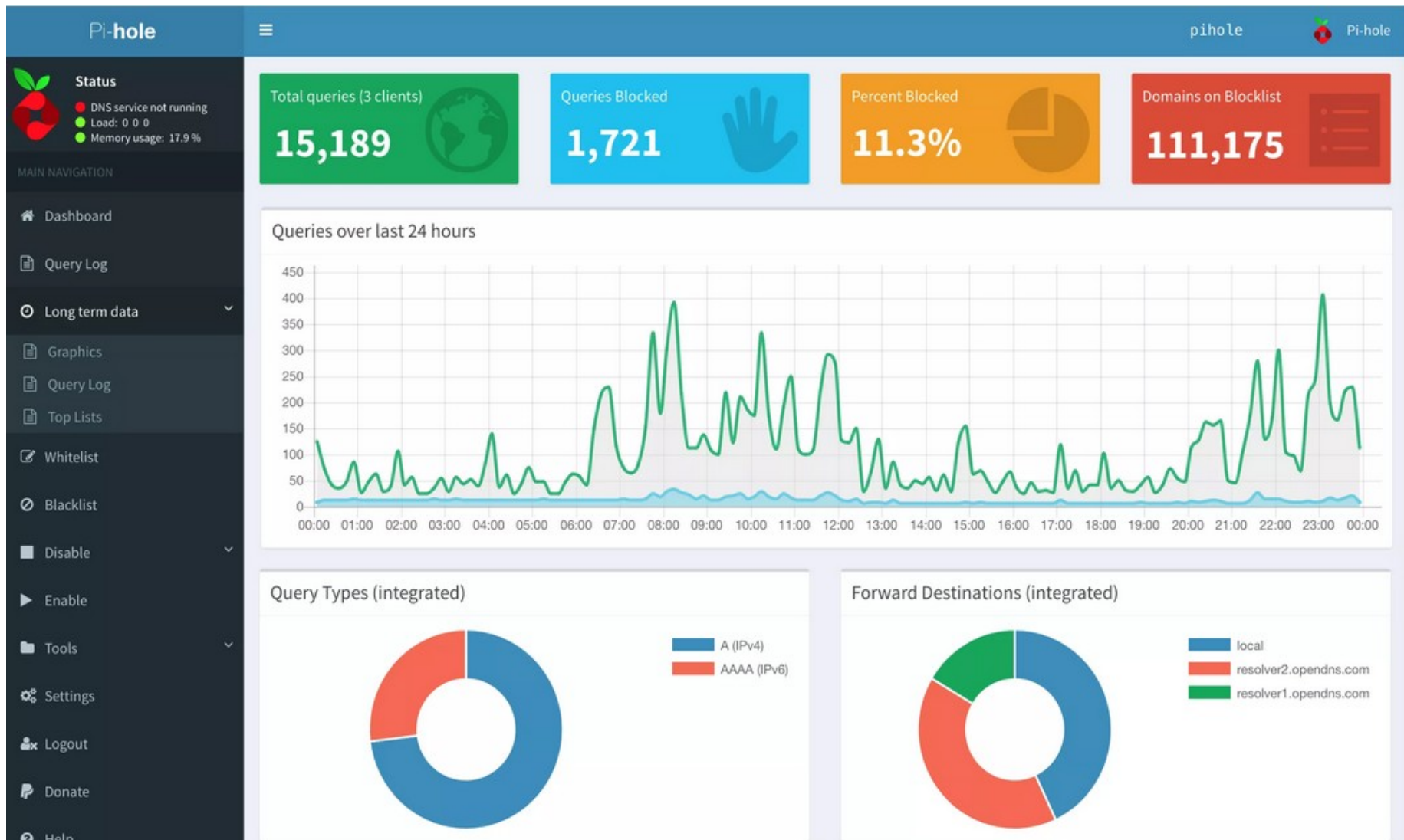
```
git clone --depth 1 https://github.com/pi-hole/pi-hole.git Pi-hole
```

2) Exécution du script d'installation (on aura bien sûr lu tout le code avant :-)

```
cd "Pi-hole/automated install/"
```

```
sudo bash basic-install.sh
```

Pihole : l'interface d'administration

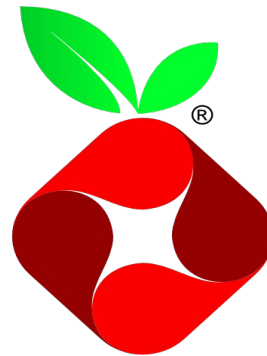


Limites du Pi-hole



- Ne gère pas nativement le chiffrement (**DOH etc.**)
- Solution facilement contournable pour un geek : changement @ip du resolveur facile sur pc
- Le pi-hole tombe en panne : plus d'internet à la maison (SPOF)
- Limité pour certains services - La TV sur certaines BOX avec pi-hole peut en pâtir (Orange)
- Efficacité sur nouvelles techniques de traçage ? (privacy sandbox, idconnect verizon)

Pihole pour aller plus loin



Customiser son pi-hole

- Enrichir les **listes de blocage** (blacklist) »
ex: <https://firebog.net/> ou <https://blocklist.site>
- **Contrôle parental** - Planifier des interdictions de domaine que certaines plages horaires
- Activer **DNSSEC**
- Mettre en place noms de domaines interne
- Mettre son propre résolveur type « **unbound** » devant son pi-hole

DNSSEC

- 1) Extension du DNS (!= nouveau protocole)
- 2) Signature cryptographique des enregistrements
- 3) **Authentication + intégrité** des données
=> réponse sûre
- 4) Ne prémunit pas contre l'espionnage
- 5) Activé sur la plupart des DNS publics
- 6) Mesure efficace contre le DNS poisoning

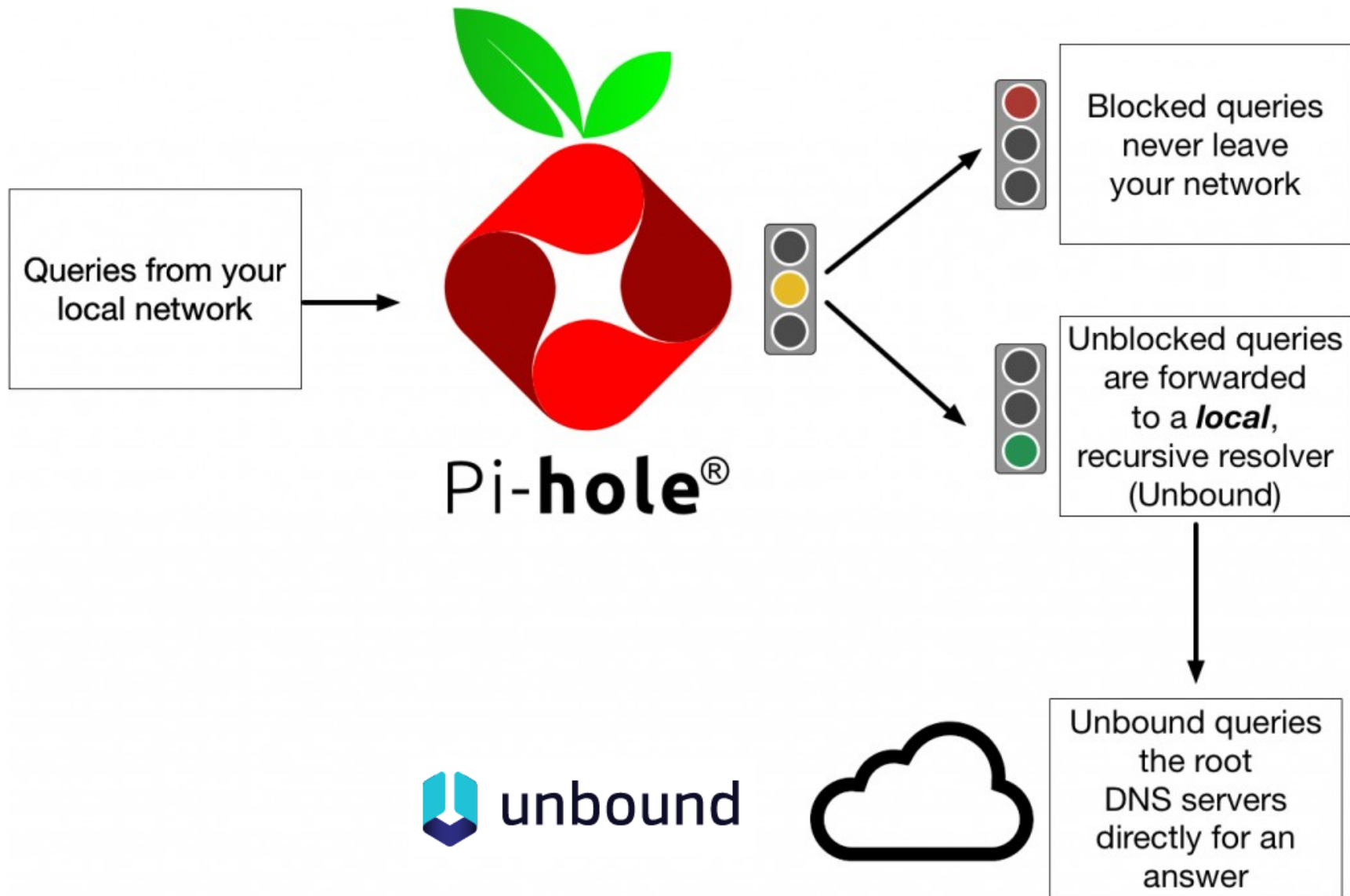
Contrôle parental

Dans la crontab :

- 1 ligne de commande pour activer la censure (pihole --wild)
- 1 ligne de commande pour la désactiver (pihle --wild -d)

```
# m h dom mon dow    command
30 21 * * * /usr/local/bin/pihole --wild facebook.com tiktok.com s
napchat.com whatsapp.com instagram.com googlevideo.com youtube.com
&& /usr/local/bin/pihole updateGravity
07 09 * * * /usr/local/bin/pihole --wild -d facebook.com snapchat.
com tiktok.com whatsapp.com instagram.com googlevideo.com youtube.
com && /usr/local/bin/pihole updateGravity
```

Pihole avec son propre résolveur



Avantages

Unbound :

- Permet de limiter l'envoi des données aux autres acteurs (**Qname Minimisation**)
- **DNSSEC** activé par défaut
- Possibilité de faire du DOH (dns over https)
- Cache chaud (au début lent, phase d'apprentissage mais super rapide par la suite)
- Améliore la vie privée en amont

Contribuer au projet Pi-hole

1) Produit libre

2) Faire un don

=> couvrir frais liés au coût du développement

et/ou

3) Contribuer en :

=> participant au code (« pull request » sur github)

=> traduisant la documentation dans d'autres langues

=> participant au forum (modération etc.)

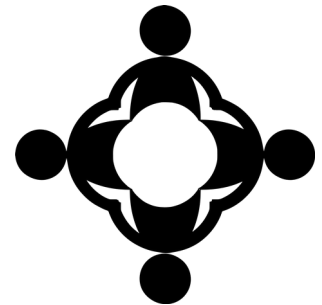
=> en promouvant son utilisation (faire sa pub quoi :-)

...



Documentation

- Sur votre dashboard :
<http://pihole/admin/help.php>
- Documentation officielle
<https://docs.pi-hole.net>
- Forum :
<https://discourse.pi-hole.net>
- Les tutos de blogs nombreux (pas tous valables)



sources

- C'est quoi un résolveur :
- Comment installer pihole ?
- Contourner l'accès restreint aux options du routeur
- Pihole : installer unbound son propre résolveur ?

sources

- Tester l'empreinte de son navigateur :
- comprendre le « fingerprinting » :.
- détecter & analyser les cookies traceurs
- Résoudre pb pi-hole et box orange TV