

DNS Resolver

“ To really and fully utilize your SSL environment you need a local DNS resolver that knows your home network...

There are various ways to successfully implement this technology (DNS), even with "in-house knowledge".

1. hosts File

You can define your devices in a hosts file and, for example, distribute this manually to all hosts files of the affected devices. However, this can quickly turn into time-consuming work and is prone to errors! Furthermore, there are devices (e.g. IOT, network devices, TVs) that do not offer manual hosts management at all.

2. Resolver

The standard tools such as bind9, dnsmasq could be considered here. However, availability is questionable depending on the operating system. In addition, "failure" is usually pre-programmed, as the technology and tools should be, let's say, semi-professional.

3. Hybrid Applications

The best-known tools here are PI-Hole and AdGuard. Please keep in mind that these tools were created for a different reason: Ad Blocker!!!!!! Due to the concept (foundation, structure), it is becoming increasingly difficult for the tools to follow modern DNS concepts, i.e. to implement the technologies (e.g. DNSSEC) with all possible methods (e.g. DNS-over-HTTPS or DNS-over-QUIC).

A currently less well-known but all the more remarkable application is [Technitium](#). It combines all the "home computer scientist" requirements of a modern, customizable, sustainable DNS resolver solution. It can provide ad blocking with flexibility and customizability, a really easy to set up and maintain resolver implementation and, if desired, an extensive analysis and reporting environment. Hm, the only disadvantage could be the application language: English. However, this is very technical and English is always better than any botched German translations. The [linked](#) video is also very helpful!!!!!!

Dashboard

Last Hour

Last Day

Last Week

Last Month

Last Year

Custom

2,848

100%

Total Queries

1,504

52.81%

No Error

0

0.00%

Server Failure

1,344

47.19%

NX Domain

0

0.00%

Refused

12

0.42%

Authoritative

850

29.85%

Recursive

732

25.70%

Cached

1,254

44.03%

Blocked

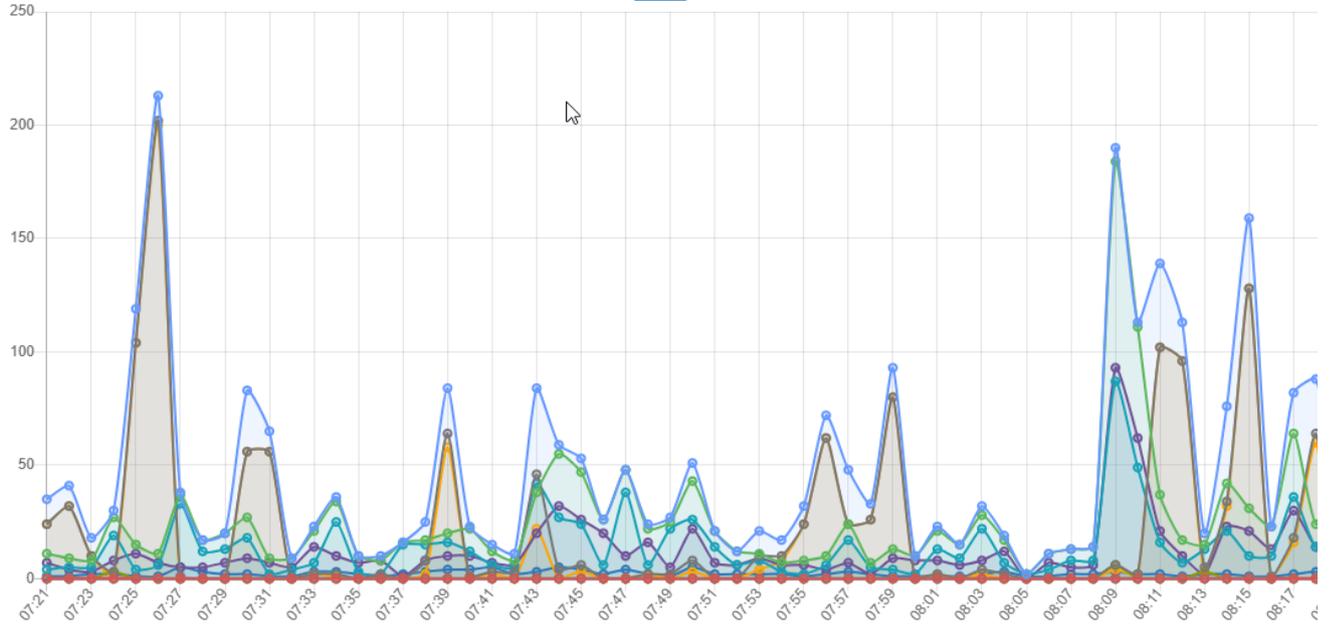
0

0.00%

Dropped

9

Clients



6

Zones

6,568

Cache

0

Allowed

0

Blocked

0

Allow List

214,03

Block L

DNS Resolver

← Back

hopto.home 

Primary Enabled

Add Record Disable Zone Delete Zone Options Permissions DNS

Name Type Page Number Records Per Page

1-6 (6) of 6 records (page 1 of 1)

#	Name	Type	TTL	Data	
1	@	NS	3600 (1h)	Name Server: netfactory Last Used: 0001-01-01 00:00:00 (never) Last Modified: 2025-06-15 08:55:21 (3 days ago)	Edit Disable Delete
2	@	SOA	900 (15m)	Primary Name Server: netfactory Responsible Person: hostadmin@hopto.home Serial: 5 Refresh: 900 (15m) Retry: 300 (5m) Expire: 604800 (1w) Minimum: 900 (15m) Use Serial Date Scheme: false Last Used: 2025-06-18 08:12:44 (10 minutes ago) Last Modified: 2025-06-15 08:55:21 (3 days ago)	Edit Disable Delete
3	netfactory	A	3600 (1h)	192.168.158.10 Last Used: 2025-06-18 08:12:44 (10 minutes ago)	Edit Disable Delete

Ad Blocking

Blocking Answer TTL seconds (default 30)

The TTL value in seconds that must be used for the records in a blocking response. This is the TTL value that the client will use to cache the blocking response.

Allow / Block List URLs

```
https://raw.githubusercontent.com/StevenBlack/hosts/master/alternates/fakenews-gambling-social/hosts
```

Quick Add

- None
- Default
- Steven Black [adware + malware]
- Steven Black [adware + malware + fakenews]
- Steven Black [adware + malware + gambling]
- Steven Black [adware + malware + porn]
- Steven Black [adware + malware + social]
- Steven Black [adware + malware + fakenews + gambling]
- Steven Black [adware + malware + fakenews + porn]
- Steven Black [adware + malware + fakenews + social]
- Steven Black [adware + malware + gambling + porn]
- Steven Black [adware + malware + gambling + social]
- Steven Black [adware + malware + porn + social]
- Steven Black [adware + malware + fakenews + gambling + porn]
- Steven Black [adware + malware + fakenews + gambling + social]
- Steven Black [adware + malware + fakenews + porn + social]
- Steven Black [adware + malware + gambling + porn + social]
- Steven Black [adware + malware + fakenews + gambling + porn + social]
- OISD Big [Adblock Plus]

Block List Update Interval

Block List Next Update On

Notel DNS Server will use the data returned to it from the file containing list of domains to block, wildcard domains are not be used with allow lists

[Help: Blocking Internet Ads Using DNS Sinkhole](#)

to add known block list
path. For example, on Linux should look like
and update of the block lists.
format is standard `hosts` file format, plain

[Save Settings](#) [Flush Cache](#) [Backup Settings](#) [Restore Settings](#)

“my recommendation: Technitium

Revision #3

Created 18 June 2025 08:55:42 by tomek

Updated 18 June 2025 09:57:33 by tomek