Messaging, Malware and Mobile Anti-Abuse Working Group

M^{3}AAWG Tutorial on Third Party Recursive Resolvers and Encrypting DNS Stub Resolver-to-Recursive Resolver Traffic

Version 1.0
September 2019

The direct URL to this paper is: www.m3aawg.org/dns-crypto-tutorial

Document 1 of 2: This document is intended to be accompanied by the paper "M^{3}AAWG Companion Document: Recipes for Encrypting DNS Stub Resolver-to-Recursive Resolver Traffic (www.m3aawg.org/dns-crypto-recipes)," which provides detailed instructions and processes.

This document was produced by the M^{3}AAWG Data and Identity Protection Committee.

Table of Content

List of Figures

Executive Summary

The Domain Name System (DNS) is key to making the internet work: virtually everything you do online begins with a DNS lookup. DNS lookups are automatically performed for users via recursive resolvers. Recursive resolver service has historically been offered by a user's Internet Service Provider (ISP) or other connectivity provider, such as an employer, a student's school, etc.

Of late, third parties have been offering free alternative recursive resolver services, for example, Google's 8.8.8.8 or Cloudflare's 1.1.1.1. These services, and others like them, have been touted as an alternative to default recursive resolver services that may have been "slow," "unreliable," "filtered," or "intrusively monitored."

More recently still, third party recursive resolver operators have begun offering encryption of DNS recursive resolver traffic between the stub resolver (running on the user's system or device) and the third party recursive resolver. Multiple competing encryption standards have emerged for that purpose, including DNSCrypt, DNS over TLS, and DNS over HTTPS.

This paper provides the basic information to evaluate the benefits and potential issues with encrypting DNS traffic. It is written for both end-users who want to implement encrypted DNS on their personal devices or home broadband networks and for ISPs and enterprise administrators who are considering it as an additional layer of security on their corporate networks. This paper also includes specific recommendations on how M^{3}AAWG members and the online anti-abuse eco-system can apply this technology.

A separate supplemental document, "M^{3}AAWG Companion Document: Recipes for Encrypting DNS Stub Resolver-to-Recursive Resolver Traffic" outlines the specific steps to install and configure a third party encrypted DNS service on popular end-user hardware and mobile devices. It is available at www.m3aawg.org/dns-crypto-recipes and in the Best Practices section of the M^{3}AAWG website.

Introduction

The Motivation for Using an Encrypted Third Party DNS Service

Why would a user change from their default provider DNS provider to a third party service? There are numerous reasons:

The Domain Name System (DNS) – often called the "internet's phone book" – plays a critical role in internet operations, so it needs to be both reliable and fast. DNS is a mission-critical and fundamental service. If the recursive resolver service is broken or the DNS settings on a user's system are misconfigured, "the internet" will be perceived as being "down" by end users. Slow DNS resolution also has the potential to make page loads lag, causing frustrated end-users to think that the internet is "slow." Users may switch to a third party service because they believe using alternative DNS providers will fix these reliability problems or improve internet performance. In fact, many alternative DNS providers stress the "speed" of their services as a core marketing message.

ISPs (Internet Service Providers) or governments may attempt to manipulate the DNS to block user access to some types of content. DNS represents a natural potential network choke point for filtering content because what a user can access online depends in part on what they can resolve in DNS. DNS-based filtering can be a double-edged sword: it can benefit users (for example, a DNS provider might block user access to phishing, malware and online scam sites), or it can interfere with the user's ability to access popular internet resources (for example, some governments may block access to specific search engines, social media providers or Wikipedia). Ironically, users may seek either alternative DNS providers that filter content they want to avoid or alternative DNS providers that are unfiltered.

Stub resolver-to-recursive resolver DNS traffic can disclose sensitive metadata (PII, personally identifiable information) about how a user browses the internet. Because virtually everything a user does online begins with DNS, stub resolver-to-recursive resolver traffic has the potential to faithfully chronicle the sites a user visits online. This record of where a user goes online may be of substantial interest to those engaged in "pervasive monitoring," whether that is an internal police agency or online marketers. Users may not always be able to pick their DNS provider, but when they can, some use an alternative DNS provider to hinder such tracking.

From their point of view, end users considering an alternative DNS provider face six options that can be categorized into six choices:

1) "Should I just continue to use the default recursive resolvers provider by my ISP or should I try an alternative recursive resolver service provided by a third party?" Most users will likely never even ask this question and will simply continue to use whatever DNS servers they are given by default.

2) "If I do use a third party DNS service, should I encrypt that traffic or should I just leave it unencrypted?" If their unencrypted DNS services appear to work satisfactory, many nontechnical users will probably leave their DNS traffic unencrypted. The process of encrypting DNS traffic, while not technically daunting, may still be too arcane to be of interest to average users.

3) "If I am going to encrypt my DNS traffic, should I do it device-by-device, to protect me wherever I use that device, or on my home broadband router, to protect all the devices using that gateway router but only at that one location?"

4) "What encryption software product should I use?" Since most systems do not ship with built-in support for encrypting DNS traffic, users will need to install software to perform this task. But which product to use? Some users may have a choice of several encryption products, while others may only have one option (although more options will likely emerge over time). Choice of one encryption product over another may also be impacted by the type of adversary the user is trying to defend against.

5) "The encryption software I have found supports more than one encryption protocol. Which encryption protocol should I use?" There are three main competing protocols (DNS over TLS, DNS over HTTPS and DNSCrypt) and most users will not be aware of their respective technical advantages and disadvantages, nor will they care. What users choose to install may be a function of what is enabled by default or what they can make work.

   There is an another opportunity for confusion because some users may think they are getting DNS encryption if they use a DNS service that simply offers DNSSEC. "DNSSEC" certainly sounds "secure," even though it provides no protection from eavesdropping whatsoever. While DNSSEC leverages cryptography for DNS integrity protection, and that is good, it is of no consequence when it comes to protecting the confidentiality of user recursive resolver traffic.

   Users also may have to choose between encrypted DNS or an encrypted VPN service because they often cannot do both. A user choosing DoT, DoH or DNSCrypt might have to forgo use of an encrypted VPN service since these technologies are often implemented as pseudo-VPN services. Thus, while implementing DNS encryption may help protect a user's *DNS traffic* from monitoring, forgoing use of an encrypted VPN service may increase a user's exposure to *other, non-DNS-focused* traffic monitoring.

6) "Which third party encrypted recursive resolver service provider should I use?" The encryption software the user installs and the encryption protocols that software supports may excessively-constrain the user's choice of a third party recursive resolver service provider. Lacking the detailed information to make a better choice, a nontechnical user might "select" whatever is configured as a default.

   Other issues can result from an insufficient understanding of selection criteria. For example, the list of providers available for potential use may be filterable by factors such as IPv6 accessibility, support for DNSSEC, filtering (or lack thereof), and query logging (or lack thereof). Once those options have been set, the filtering software may then choose the matching provider that has the lowest latency. Unfortunately, mechanical provider-selection process like this fail to recognize that important differences may still exist between providers with the same IPv6/DNSSEC/filtering/logging profile, such as:

   - WHO is offering the service? (Is it a company? a non-commercial organization? an individual? a nation-state?)

   - WHY is the provider offering the encrypted DNS service? (What is their motivation and business model?)

- WHERE is the service based? (The geographical location of the encrypted recursive resolver service's servers impacts both the service's performance and the privacy policies the service may be able to sustain.)

- WHAT data does the provider collect and what do they do with the data once it is collected?

- Does the service provider pass along "hints" about the user's IP address via the EDNS0 Client Subnet Extension? (Doing so may help accelerate CDN-delivered content but at some potential cost to the privacy of the DNS queries the user makes.)

- Does the service provider use QNAME minimization, limiting user query leakage upstream to authoritative servers?

From the above discussion, it is evident that the choice of a recursive resolver provider may have a major impact on the privacy, security, performance and reliability of DNS services.

As noted, this tutorial outlines the benefits and potential issues with encrypting DNS traffic. It also includes recommendations for M^{3}AAWG and its various audiences.

Recipes for Installing DNS Encryption on Computers, Smart Phones and Home Broadband Routers

Since what is available for DNS encryption support on a given platform often effectively dictates choices three through six above, a separate stand-alone supplemental document, "M^{3}AAWG Companion Document: Recipes for Encrypting DNS Stub Resolver-to-Recursive Resolver Traffic" shows users how to install and configure a third party encrypted DNS service on Mac OS X, MS Windows, iPhone, Android and a standalone Raspberry Pi (the Pi would be integrated by connecting it to the user's home broadband router).

Recommendations for M^{3}AAWG and Its Audiences

1. M^{3}AAWG, as an organization focused on anti-abuse, should:
   - Offer training on encrypted DNS prior to M^{3}AAWG member meetings.

   - Follow its own best practices and offer encrypted recursive resolver service at its meeting.

   - Educate its members on motivations for offering or using encrypted third party recursive resolver services.

2. M^{3}AAWG ISP members should:
   - Continue to permit user access to trustworthy third party DNS service providers, reducing or eliminating the need for block-evasive DNS encryption protocols.

   - Offer their own encrypted recursive resolver service to reduce or eliminate the need for third-party recursive resolver services.

   - Offer encrypted recursive resolver services which should support all leading stub resolver-to-recursive resolver encryption options. (Users may have an imperfect ability to use a single option that might otherwise be selected.)

3. Third party recursive resolver operators should:

   Operate transparently, offering their services on well-known IPs via standardized ports to facilitate whitelisting and avoiding tactical maneuvers aimed at circumventing network management efforts.

   Third party recursive resolver operator choices in areas such as encryption support, privacy practices, applicable jurisdiction, and other features and capabilities (such as Qname minimization, EDNS0 Client Subnet Extension use and DNS Padding practices), should also be clearly and publicly described. They should also be provided in a standardized, to-be-developed machine-readable format, anticipating the need for automated assessment and assistance in the selection of compatible third party resolvers.

   Third parties must obtain the user's explicit and informed consent before changing the user's default resolver.

4. M^{3}AAWG operating system and application software vendor members and M^{3}AAWG participants active in the open source software community should endeavor to provide support for DNS encryption in relevant software products.

   M^{3}AAWG hardware vendor members should likewise consider providing native support for encryption of DNS traffic in appropriate network hardware devices, such as home broadband routers, DNS recursive resolver appliances, etc.

5. Users should be advised of the potential benefits and potential costs of using encrypted recursive resolver services. In particular, users should be helped to understand:

    - The importance of ensuring that any third party software they install comes from a trustworthy source, has not been tampered with (e.g., checksums are correct), is securely configured, and that the software must be kept up-to-date with the latest security patches.

    - The importance of choosing a trustworthy and reliable recursive resolver provider.

    - The fact that, even if they successfully encrypt the traffic to and from a recursive resolver, they will not necessarily be communicating with total privacy because they may still be vulnerable to other types of pervasive monitoring.

6. Researchers should be encouraged to investigate the uptake of encrypted recursive resolver services by internet users over time, broken out by the ASN of the user, the country of the user, the encryption technology employed, and the encrypted DNS service provider used (if these metrics can be ascertained). Usage should be reported both in terms of the percentage of total unique users and the percentage of total DNS traffic seen.

I. Is the Use of Alternative Third Party Recursive Resolvers and Encryption of Stub Resolver-To-Recursive Resolver Traffic “In-Scope" for M^{3}AAWG Remit?

1. DNS is an Operationally Critical Core Internet Protocol

DNS is often described as the "internet's phone book."[1] DNS maps easy-to-remember domain names to the numeric IP addresses that computers need to connect to the internet. While DNS is a tremendous convenience for users, it also delivers numerous objective technical benefits, including enabling efficient use of limited IPv4 addresses via name-based virtual hosting.[2]

Because DNS normally seems to just "magically" work, many internet users take it for granted, but it would be inconceivable to try to use the internet without DNS. DNS is truly one of the internet's most-critical core protocols. DNS rarely fails, but when for whatever reason it does, the internet is widely perceived as being "down" (even if all the other components except the DNS continues to operate).[3]

Debugging, identifying and correcting user-misconfigured DNS also has the potential to be troublesome and expensive for service provider support staff, and it can be particularly problematic for lower-tier support staff who may not know to double check the user's DNS configuration as part of their fault isolation and remediation process.

Bottom line? Users and ISPs alike need the DNS to work reliably and efficiently.

2. DNS and Messaging/Anti-Abuse Work

We also note that DNS plays a particularly crucial role for messaging and anti-abuse work since:

- DNS "MX" records[4] route incoming mail and help users access Web mail interfaces, as well as POP,[5] IMAP[6] and SMTP.[7]

- Domain-based and IP-based blocklists,[8] plus RPZ (Response Policy Zones),[9] are pivotal to suppressing spam, phishing and other unwanted traffic.

[1] https://en.wikipedia.org/wiki/Domain_Name_System

[2] https://httpd.apache.org/docs/2.4/vhosts/name-based.html

[3] https://gizmodo.com/this-is-probably-why-half-the-internet-shut-down-today-1788062835; and http://blog.catchpoint.com/2018/06/14/analyzing-impact-public-dns-resolver-outage/

[4] https://en.wikipedia.org/wiki/MX_record

[5] https://en.wikipedia.org/wiki/Post_Office_Protocol

[6] https://en.wikipedia.org/wiki/Internet_Message_Access_Protocol

[7] https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

[8] https://en.wikipedia.org/wiki/Blacklist_(computing)

[9] https://dnsrpz.info/

- DNS is the substrate for key messaging identity related protocols such as SPF (Sender Policy Framework),[10] DKIM (DomainKeys Identified Mail)[11] and DMARC (Domain Messaging Authentication Reporting and Conformance)[12].

- Permissively-configured and poorly monitored open recursive resolvers are a prime tool for launching DDoS (Distributed Denial of Service) attacks[13].

Not surprisingly, messaging and anti-abuse professionals tend to care deeply about DNS. That is one reason why M^{3}AAWG has a DNS Abuse Special Interest Group (SIG).

3. User Privacy and Opposition to Pervasive Monitoring

M^{3}AAWG also has a well-established history of opposing pervasive monitoring and advocating for effective user privacy on the internet, including having had an active and highly productive anti-pervasive monitoring SIG dating from the time of Edward Snowden's initial revelations.[14] The M^{3}AAWG position on this matter is consistent with the IETF's anti-pervasive monitoring perspective ("Pervasive Monitoring Is an Attack") guidance.[15]

4. M^{3}AAWG Membership – Many M^{3}AAWG Members Have a Keen Interest in This Topic

M^{3}AAWG is also unique because its membership[16] includes:

- The world's leading ISPs
- The world's leading operating system and application software vendors
- The world's leading hardware vendors
- Virtually all the organizations involved with fielding public third party recursive resolvers
- Virtually all the entities working on encryption between stub resolvers and recursive resolvers
- Participants/liaisons from standards organizations such as the IETF
- Participants/liaisons from privacy-focused non-governmental organizations
- Guest participants from federal and international government, law enforcement and military organizations.

This breadth of organizational representation potentially complicates treatment of third party recursive resolvers and encryption of stub-to-recursive traffic issues, but we believe that M^{3}AAWG can, and must, take the lead to discuss this important issue fairly and objectively.

Ultimately the choice of what to actively champion, deploy, allow, discourage, or block outright will be, just as it always has been, a matter for each individual participant organization – or each individual end user. Our goal in this paper is not to try to sway your opinion one way or the other; our goal is to help clarify the issues and options so the participant can make a fully informed and technically rational choice.

[10] https://www.getmailbird.com/what-spf-resources-are-available-now-that-openspf-org-is-gone

[11] http://www.dkim.org/l

[12] https://dmarc.org/

[13] https://www.us-cert.gov/ncas/alerts/TA13-088A

[14] The work of the anti-Pervasive Monitoring SIG is now part of the broader M^{3}AAWG Data and Identity Protection Committee's remit.

[15] https://tools.ietf.org/html/rfc7258

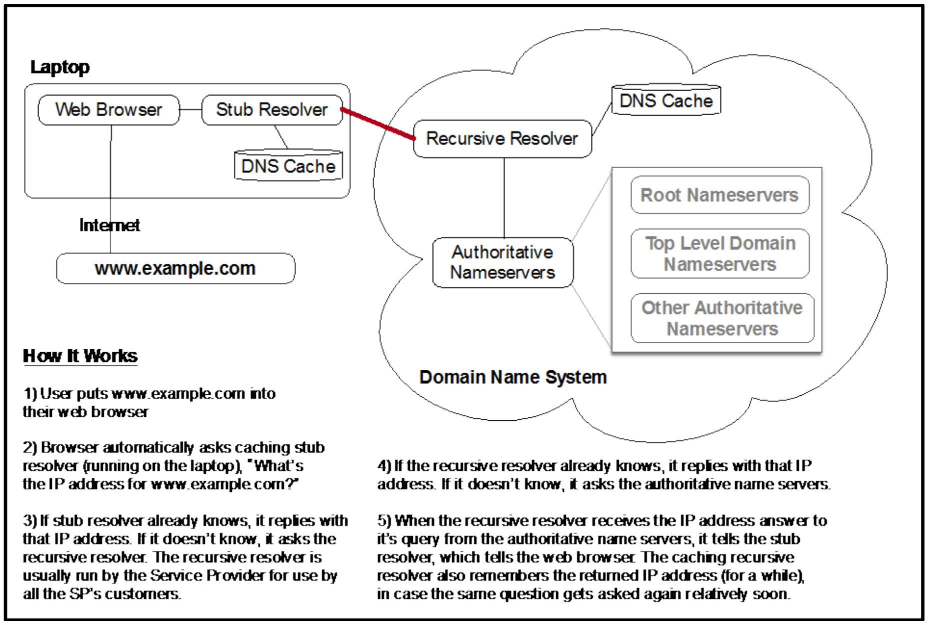
[16] https://www.m3aawg.org/about/roster

II. Recursive Resolvers (Default ISP, Third Party Alternatives and Dedicated Personal Recursive Resolvers)

This section provides background information explaining the relationship between the ISP's default recursive resolvers and third party recursive resolvers.

5. How Do Recursive Resolvers Normally Work in an ISP Environment Today?

Traditionally, ISPs have provided recursive resolvers for use by their customers.[17] Customer systems normally get told about those name servers automatically when the customer's system requests an IP address via DHCP.[18] A notional depiction of how those servers operate can be seen in Figure 1:



How It Works

1) User puts www.example.com into their web browser

2) Browser automatically asks caching stub resolver (running on the laptop), "What's the IP address for www.example.com?"

3) If stub resolver already knows, it replies with that IP address. If it doesn't know, it asks the recursive resolver. The recursive resolver is usually run by the Service Provider for use by all the SP's customers.

4) If the recursive resolver already knows, it replies with that IP address. If it doesn't know, it asks the authoritative name servers.

5) When the recursive resolver receives the IP address answer to it's query from the authoritative name servers, it tells the stub resolver, which tells the web browser. The caching recursive resolver also remembers the returned IP address (for a while), in case the same question gets asked again relatively soon.

Figure 1. The Notional Normal DNS Resolution Process

The link denoted in red in the above conceptual diagram is our special focus. That is where encryption of stub resolver-to-recursive resolver traffic (discussed in more detail later in this document) would occur.

Where the user is connecting from, the type of link the user has, the encryption the user has installed (or is not using), and the path the traffic takes between the stub resolver and the recursive resolver being used, all can impact who is potentially able to filter, capture and inspect, or modify the user's DNS traffic.

For the sake of this discussion, we assume that the user's own computer and his or her home network[19] are secure. If the user's computer and home network are not secure (for example, if the user's system or home networking equipment is misconfigured or unpatched, is infected with malware, or has a hardware sniffer surreptitiously installed), it will be impossible for the user to use the internet securely. While all ISPs naturally

[17] The enterprise case is comparable: corporations traditionally have provided recursive resolver service for their employee "users."

[18] See for example "option domain-name-servers" at https://kb.isc.org/docs/isc-dhcp-41-manual-pages-dhcp-options

[19] We define that network system(s) and network devices up to and including the CPE demarc device (e.g., "the cable modem" or "DSL modem").

want their users to have a secure computer and home network environment, ultimately it is the user's responsibility to correct insecurities downstream of the CPE (customer premise equipment) demarc point (e.g., on the customer premises).

Upstream of the CPE demarc device, there are two main areas of potential concern, as shown on Figure 2 below:

- If the wide-area link (between the user's CPE demarc device and the ISP's infrastructure) is vulnerable to being monitored by an adversary, any unencrypted traffic on that wide-area link (including, but not limited to, DNS traffic) is potentially subject to interception or modification. See the upper red arrow in Figure 2.

- Unencrypted DNS traffic from the user to the recursive resolver over infrastructural links within the ISP's data center may also be specifically targeted for interception and eavesdropping. See the lower red arrow in Figure 2.

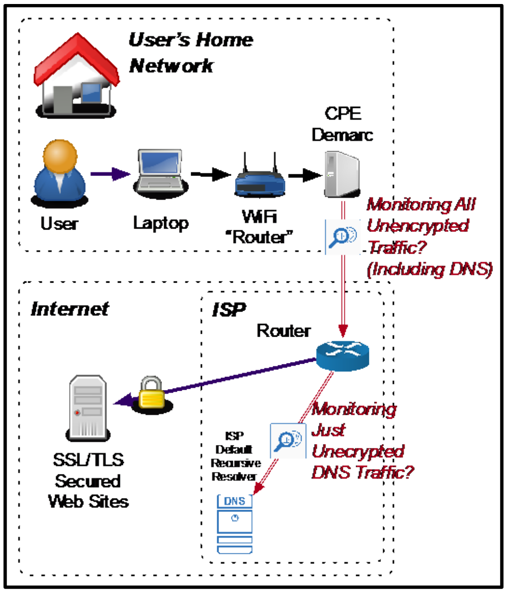

User's Home Network
CPE Demarc
User
Laptop
WiFi "Router"
Monitoring All Unencrypted Traffic? (Including DNS)
Internet
ISP
Router
SSL/TLS Secured Web Sites
ISP Default Recursive Resolver
DNS
Monitoring Just Unecrypted DNS Traffic?

Figure 2. Prime Areas for Potential Monitoring

6. A Typical Day in a Typical User's Life Online: Many Different Internet Service Providers, Many Different Recursive Resolvers

While in Section II.5 we showed a user connecting from a single home laptop to a single ISP, in fact, most people connect through a variety of different ISPs over the course of a typical day:

- You might use your normal broadband provider when you first wake up and check your email.
- En route to work, you might use a mobile service.
- Once you get to work, you will probably use your employer's network.
- Lunchtime? When you go out for a sandwich, you may use the restaurant's internet service while waiting for your order.

- After work, you may go out for drinks with friends, to the gym for a workout, to the store for a little shopping, or maybe it is time to ferry the kids to soccer or music lessons or some other after-school activity. Again, all too often you will be using still other "public" internet connectivity providers.
- If you are traveling for work, away from home on vacation, etc., you will often use still more providers (airport/airline WiFi, hotel WiFi, guest networks at other companies, etc.).

Each of those network providers will likely give users different recursive resolvers to use.

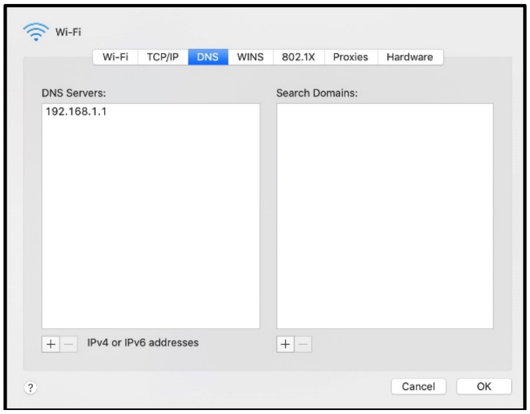
And of course, most of us also use multiple devices during a day – perhaps a desktop workstation, a laptop, a tablet, one or more smart phones, an e-reader, etc. Additionally, there are all the "Internet of Things" (IoT) devices such as our "smart" televisions, "smart" thermostats, etc. All these devices connect to the internet, and all these devices use DNS.

Bottom line: a "typical" user's "simple" connectivity -- and the recursive resolver services that come with that connectivity -- may be anything but simple. That means if any of their ISPs or any of the recursive resolvers they are given by default are being monitored, snoopers may be able to trace the user's internet activity for the duration of time the insecure connection is used.

7. How Can I Even Tell What Name Servers I Am Actually Using Right Now?"

It can sometimes be a little difficult to tell exactly what name servers your system may be using, at least if a "DNS forwarder" is in play. DNS forwarders are often part of the default setup provided by at least some home wireless broadband routers. Those forwarders transparently "proxy" or "relay" local user DNS queries to upstream recursive resolvers.

When a DNS forwarder is being used, often the only thing you will see is the "local" (RFC1918[20]) IP address of a home broadband router in a list of DNS servers reported by an end-user device. For example, on a typical Mac laptop's setting you might see:



DNS Servers:
192.168.1.1

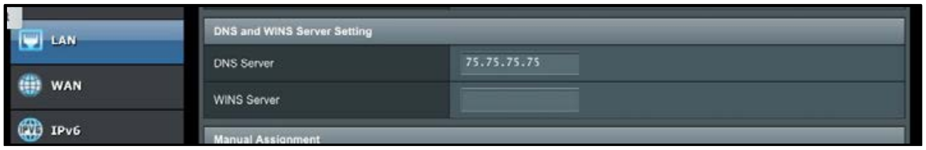
Search Domains:

Figure 3. Example of a Mac Configured to Use a Forwarding Name Server Running on a Home Broadband Router

[20] https://en.wikipedia.org/wiki/Private_network

In that case, to determine the name servers you are using, you would need to check the home broadband router itself.

For example, on one popular device of this type the actual DNS server setting being used can be seen via the LAN --> DHCP tab --> DNS Server setting in the home router's admin interface:



DNS and WINS Server Setting

DNS Server 75.75.75.75

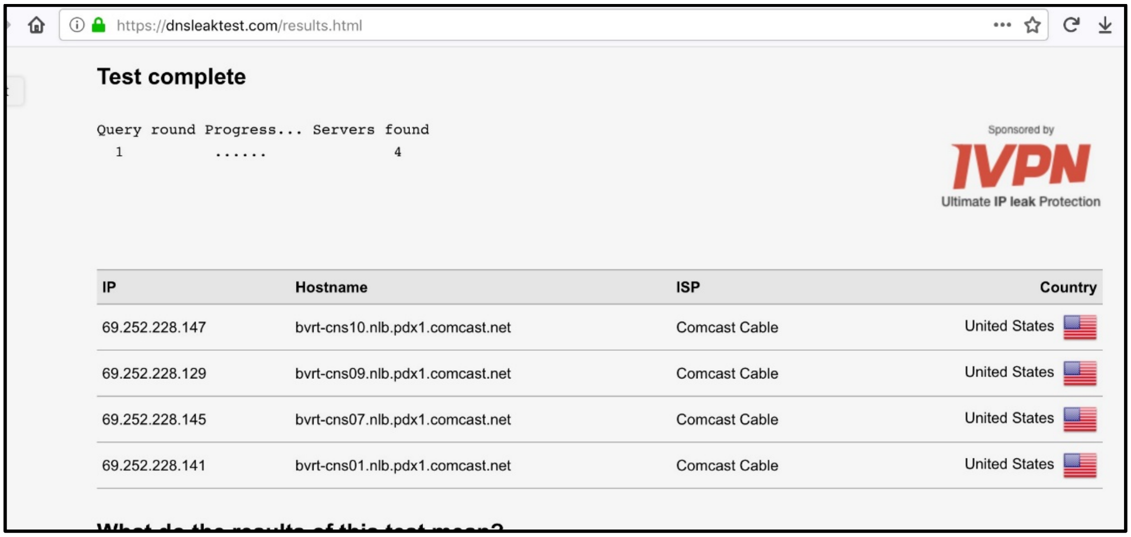
WINS Server

Manual Assignment

Figure 4. Example of a DNS Server that has been Configured on a Home Broadband Router

If you do not have access to the admin interface running on a home broadband router, you might want to try visiting https://dnsleaktest.com/ instead. That site does a nice job of providing a report about the recursive resolvers you are actually using. For any curious readers, that site works by showing you a webpage with some unique-to-you image URLs, and then checking its own nameservers' logs to see where those URLs are resolved, a clever way of finding the recursive resolvers you are actually using.

In the case of some anycast[21] recursive resolvers (such as Comcast's 75.75.75.75, as shown above), dnsleaktest.com will show you specific individual name server host IPs (e.g., the specific IP addresses of individual specific servers that are part of a multi-server anycast instance) rather than 75.75.75.75 (or whatever the overarching anycast address may be). For example, from a system that was downstream of the home router that was using "75.75.75.75," dnsleaktest.com reported:


https://dnsleaktest.com/results.html
Sponsored by
IVPN
Ultimate IP leak Protection

Test complete

```
Query round Progress... Servers found
  1          ......             4
```

IP	Hostname	ISP	Country
69.252.228.147	bvrt-cns10.nlb.pdx1.comcast.net	Comcast Cable	United States
69.252.228.129	bvrt-cns09.nlb.pdx1.comcast.net	Comcast Cable	United States
69.252.228.145	bvrt-cns07.nlb.pdx1.comcast.net	Comcast Cable	United States
69.252.228.141	bvrt-cns01.nlb.pdx1.comcast.net	Comcast Cable	United States

What do the results of this test mean?

Figure 5. Reported Results From https://dnsleaktest.com/ for one test

[21] https://en.wikipedia.org/wiki/Anycast

8. Intentionally Configuring an Alternative Third Party Recursive Resolver

Most users generally use the recursive resolvers that are automatically suggested by their provider of the moment, but (at least in most cases) users can opt to use an alternative third party recursive resolver instead.[22] But why would some users want to do that?

Avoiding Censorship

An ISP may be required by local authorities to filter some content. That filter may be implemented via the ISP's recursive resolvers.

While one might imagine that the sites being blocked are quite reprehensible (for example, perhaps sites encouraging terroristic violence or sites related to online child exploitation), at least in some cases, the sites being blocked are some of the most mainstream, popular, and useful sites on the internet. In Turkey, one site blocked via ISP operated recursive resolvers was Twitter:

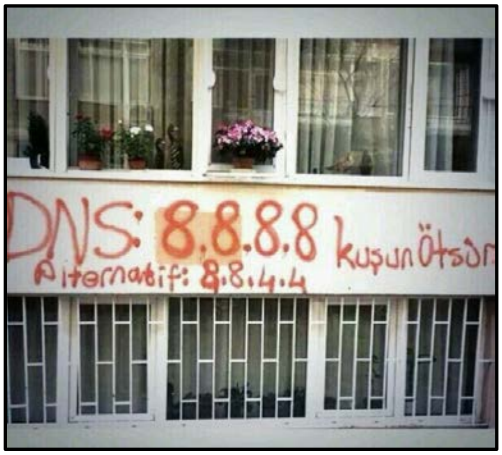
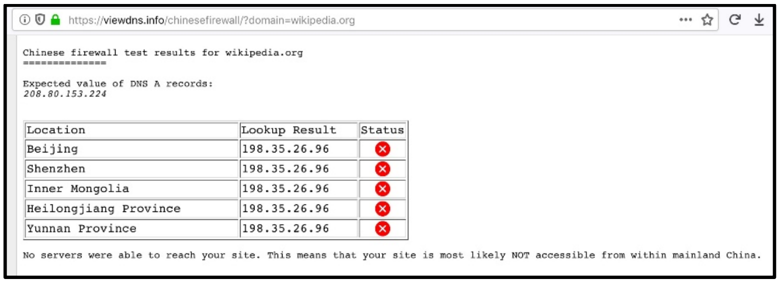


Figure 6. "Turkish graffiti spreads the IP addresses of Google's DNS servers, useful for getting around the government's ban on Twitter. The tag reads "let the bird sing." Image via @FindikKahve/Twitter." [23]

As another example, in China DNS-based censorship may interfere with user access to Wikipedia:



```
Chinese firewall test results for wikipedia.org
==============

Expected value of DNS A records:
208.80.153.224
```

Location	Lookup Result	Status
Beijing	198.35.26.96	✗
Shenzhen	198.35.26.96	✗
Inner Mongolia	198.35.26.96	✗
Heilongjiang Province	198.35.26.96	✗
Yunnan Province	198.35.26.96	✗

```
No servers were able to reach your site. This means that your site is most likely NOT accessible from within mainland China.
```

Figure 7. Wikipedia, Reportedly Inaccessible Due to DNS-Based Censorship in China

[22] Not all users will have the option of changing their name servers. For example, in a centrally-managed enterprise environment, choice of DNS servers may be something central IT determines and enforces, either via device policies or via network policies.

[23] https://gawker.com/turkish-graffiti-spreads-the-ip-addresses-of-googles-d-1548946312

On the other hand, some users may want filtered DNS in order to voluntarily block unwanted content, such as malware or content unsuitable for minors. For example, Nykolas Z commented in a Medium.com blog post:[24]

> "I was at a Marriot hotel last week with my family and I noticed that they were doing DNS hijacking and redirecting all my DNS requests to their own servers. It would not be a big deal, if wasn't for the fact that I had OpenDNS Family Filter setup on the laptop that the kids were using—and it wasn't working due to the DNS hijacking."

Improved Speed or Availability

Other times an ISP customer may be unhappy with the default recursive resolver service provided by their service provider, believing the default recursive resolver service to be "slow" or "unreliable." (Whether that is objectively true or not is a different matter; the user's perception may be what ultimately matters).

Wanting DNSSEC or – Conversely – Wanting to be DNSSEC-Free

Another group of third party recursive resolvers customers consists of users who may understand the importance of a DNSSEC-protected recursive resolver service (even if their ISP does not currently perform DNSSEC validation). The opposite situation also exists: there are some users who have ISPs that do perform DNSSEC validation but they want a DNSSEC-free recursive resolver option.

Avoiding NXDOMAIN Monetization

Another complaint sometimes heard from users is that they may dislike how their ISP's recursive resolver service displays ads in their Web browser when the user accidentally makes a typo or unintentionally accesses a webpage. There are some third party alternative recursive resolver services that pledge to never do that sort of thing.

Resistance to Ongoing Encroachments on End User Privacy

Other users may object to their ISP logging their DNS traffic. Their objection may not be associated with anything nefarious; it may simply be a matter of the customer being tired of having marketers (or "Big Brother") always "looking over their shoulder" online.

9. Well-Known Third Party Recursive Resolver Providers

While a user can select from many different well-known third party recursive resolver services, nine of the better-known free third-party public recursive resolver services are shown here in alphabetical order by the provider name:

1) Cisco OpenDNS Service at 208.67.222.222 and 208.67.220.220 (see https://www.opendns.com/home-internet-security/)

2) Cleanbrowsing DNS at 185.228.168.9 and185.228.169.9 (see https://cleanbrowsing.org/)

3) Cloudflare Recursive Resolver Service at 1.1.1.1 and 1.0.0.1 (see https://blog.cloudflare.com/dns-resolver-1-1-1-1/)

[24] "Ending DNS Hijacking with DNSCrypt,"https://medium.com/@nykolas.z/ending-dns-hijacking-with-dnscrypt-1679e78b2c92

4) Comodo Secure DNS at 8.26.56.26 and 8.20.247.20 (see https://www.comodo.com/secure-dns/)

5) Google Public DNS Service at 8.8.8.8 and 8.8.4.4 (see https://developers.google.com/speed/public-dns/)

6) IBM/PCH/GCA Quad 9 Service at 9.9.9.9 and 149.112.112.112 (see https://www.quad9.net/)

7) Neustar Free Recursive DNS Service at 156.154.70.5, 156.154.71.5 (see https://www.security.neustar/digital-performance/dns-services/recursive-dns)

8) Oracle/Dyn Internet Guide Service at 216.146.35.35 and 216.146.36.36 (see https://help.dyn.com/internet-guide-setup/)

9) Verisign Public DNS Service at 64.6.64.6 and 64.6.65.6 9 (see https://www.verisign.com/en_US/security-services/public-dns/index.xhtml)

To use one of these providers, the user simply enters the relevant IP addresses into the configuration of their broadband home router or the DNS configuration panel on their laptop, smartphone, or other device.

10. Picking the *Right* Third Party Recursive Resolver Service

You can find numerous lists of third party recursive resolvers on the internet. Do not assume that simply because a site is included on one or more such lists that it must be operated by someone who has "pure intentions," is technically careful, or is privacy-minded and trustworthy. For example, have you ever see any lists of third party recursive resolvers that have been reviewed and deemed to be ***un***trustworthy?

It is up to you to do your own due diligence when picking a recursive resolver operator. For example:

- If your primary DNS concerns are performance, resilience and long term stability, perhaps you should avoid a hypothetical third party recursive resolver service that is operated from a single location or run by one or two people on a shoestring budget.

- If your worry is that a large fraction of all your internet traffic is already being processed by a relatively small number of huge providers, such as some search engine providers or some CDNs (Content Delivery Networks), you might not want to send more of your traffic to those same outfits. Then again, you might assume they already know a good deal about you and decide that maybe it is better to send all your DNS query traffic to them, rather than spreading your information out still further.

- If your DNS-related privacy concerns are associated with worries about marketers "snooping on what you do online," perhaps avoid using a hypothetical recursive resolver service that is being run by an online marketing or advertising firm.

- Similarly, if you worry about hackers or crackers snooping on your traffic, perhaps you should avoid DNS services hosted on "anything-goes" providers who may be (in)famous for tolerating or being infested with dubious customers.

Making an informed choice means that you need to understand:

- Who is offering the service you are considering using? And why are they offering that service to the general public?

- Does the service have a formal privacy policy? Is their compliance with that policy formally audited by a third party?

- How does offering a recursive resolver fits into an organization's overall business model or the organization's mission?

THE RUMORS ARE TRUE. GOOGLE WILL BE SHUTTING DOWN PLUS—ALONG WITH HANGOUTS, PHOTOS, VOICE, DOCS, DRIVE, MAPS, GMAIL, CHROME, ANDROID, AND SEARCH—TO FOCUS ON OUR CORE PROJECT: THE 8.8.8.8 DNS SERVER.
Google

Figure 8. The Primacy of Third Party Recursive Resolver Service to Google from the Subtly-Nuanced Point of View of XKCD [25]

Speaking of business models, it is often said that "on the internet, if a service is free, you are the product that is being monetized." That may be true but sometimes that "monetization" may be acceptable. For example, sometimes a "free" internet service is offered to build a company's market share, to undercut a competitor, or to boost a company's potential valuation for merger-and-acquisition-related purposes. (However, such strategies may ultimately hurt internet users by reducing competition).

11. Technical Considerations Associated with Picking a Third party Recursive Resolver Service

There are several issues to considered when selecting a third party recursive resolver service:

- Performance: Using an in-country/low-latency third party recursive resolver service may dramatically improve a user's DNS experience. Some third party recursive resolvers may be located quite far away. You may want to check a recent report of third party recursive resolver performance to see which service is performing the best overall.[26] If you would like to benchmark third-party recursive resolvers from your location, a useful tool is dnsperftest.[27]

[25] https://xkcd.com/1361/ and https://www.explainxkcd.com/wiki/index.php/1361:_Google_Announcement

[26] https://blog.thousandeyes.com/ranking-performance-public-dns-providers-2018/

[27] https://github.com/cleanbrowsing/dnsperftest

- Government Policy-Related Implications: The location of a recursive resolver might also influence:
    - The ease with which intelligence agencies can broadly monitor a recursive resolver's traffic
    - The process required when law enforcement wants to intercept a particular user's traffic
    - The overarching protections potentially provided by privacy frameworks such as the GDPR (the European Union's General Data Protection Regulation)[28]

- Reliability: Because a recursive resolver service is critical to being able to access the internet, a good third-party recursive resolver service will typically field multiple redundant recursive resolvers, all announced via anycast. When using this type of service, you will automatically go to the closest working recursive resolver and should rarely (if ever) see any down time.

  Other times, a recursive resolver service may be offered by a "public-spirited" hobbyist via a single virtual hosting node. When circumstances make offering the service difficult or expensive, that free service may understandably end up being withdrawn. Some clients may automatically notice that the name server has gone out-of-service and automatically reconfigure; other clients may simply fail and require debugging and manual attention.

- Does the provider filter? Some providers take pride in running a completely unfiltered service, offering totally "clean" (i.e., "untampered-with") results. Other providers may attempt to differentiate their services by intentionally blocking scam, phishing or malware-related domains that they have identified or by intentionally blocking online content that may be disturbing for children or distracting for some adults.

- Does the provider support DNSSEC? Use (or non-use) of DNSSEC is another dimension to evaluate when picking a third-party resolver service. Some users may find it hard to imagine not being protected by DNSSEC; another group of users may find it frustrating to have to "put up with" DNSSEC and may want a service that does not use it. Non-technical users may simply not care.

- What about IPv6 connectivity? While there are only IPv4 addresses shown for the third-party services mentioned in Section II.9, most of those providers also offer servers accessible over IPv6. Dual homing is important to IPv6 addresses eventually becoming fully on-par with IPv4 on the global internet.

- Are user queries getting logged? If so, for how long and for what purpose? Some third-party providers log user queries for debugging, abuse prevention, to support research, or for summary statistical purposes. Others do not. Some users may be bothered by this logging, others may not.

- EDNS0 Client Subnet Extension (ECS)? Some third-party recursive resolver service providers may provide "clues" or "hints" about your IP address (and thus your geographic location) via an extension known as the "EDNS0 Client Subnet Extension," or "ECS."[29] This is a very subtle technical feature that can help improve performance, but which can also undercut user privacy (this is a very important feature for you to understand if you are serious about DNS privacy). See Appendix 3.

[28] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

[29] https://tools.ietf.org/html/rfc7871 and http://www.afasterinternet.com/

- Qname Minimization? Many recursive resolvers "leak" complete queries to root servers and TLD servers. Qname minimization – if used – can reduce this. See Appendix 4 for more information on who is and who is not doing this.

- Alternate Roots? Virtually all internet sites use domain names that are rooted in IANA (Internet Assigned Names Authority)-listed TLDs.[30] There are some parties, however, who attempt to use or promote the use of non-IANA-listed TLDs, typically referred to as "alt root domains."[31] Consistent with the analysis presented in "IAB Technical Comment on the Unique DNS Root,"[32] we discourage use of third party recursive resolvers that choose to support non-IANA-listed TLDs.

- Encryption? If a user is planning to use DNS encryption, the third party recursive resolver service they pick will also obviously need to support the encryption protocol of interest. This topic is treated in more detail in Section IV of this document.

12. "Inadvertently Public" Recursive Resolvers

There are undoubtedly numerous other "publicly-accessible" recursive resolvers besides the ones listed in Section II.9. Some of those services may be totally on par with the examples mentioned in Section II.9 – it is difficult to be aware of them all and we do not have room to list them all in this document.

That said, some recursive resolvers may inadvertently be available to the entire internet due to bugs or misconfiguration. Inadvertently open recursive resolvers are a serious problem and typically are readily abusable.[33] To avoid problems and potential abuse, do not use someone else's recursive resolver unless it is being intentionally made available for your use.

See the "Open Resolver Project"[34] for more information about the open recursive resolver problem in general. We should also note that the founder of the "Open Resolver Project" received the M^{3}AAWG JD Falk Award[35] for his work in helping to tackle millions of inadvertently available open recursive resolvers.

13. Untrustworthy/Intentionally Malicious Recursive Resolvers

Some cyber criminals are known to run totally untrustworthy malicious recursive resolvers that may intentionally attempt to misroute users to fake bank sites, fake credit card sites, etc. Obviously, no user should be using these resolvers. For one example of this sort of malicious resolver issue, see the DNS Changer Working Group at http://www.dcwg.org/.

We mention these malicious resolvers here because some ISPs may intentionally filter or redirect all DNS traffic destined for third party recursive resolvers to ensure that customers are not unintentionally using untrustworthy recursive resolvers. Other ISPs may block most DNS traffic that is not directed to their own recursive resolvers but allow limited exceptions for well-known and trusted alternative DNS providers, such as the sites mentioned in Section II.9.

[30] https://www.iana.org/domains/root/db

[31] https://en.wikipedia.org/wiki/Alternative_DNS_root

[32] https://tools.ietf.org/html/rfc2826

[33] https://www.security.neustar/blog/recursive-dns-what-it-is-and-why-you-should-care

[34] http://web.archive.org/web/20190102040312/http://openresolverproject.org/

[35] https://www.m3aawg.org/news/open-resolver-project-founder-jared-mauch-receives-m3aawg-jd-falk-award-for-identifying-systems

14. What About Users Running Their Own Personal Dedicated Recursive Resolver?

At least some technically inclined users may also choose to run their own dedicated personal recursive resolver service. Doing so in a fully professional way involves a number of considerations:

- To avoid flaunting routine "no server" terms of service for residential services, most consumer users will need to upgrade their current internet service plan to one allowing the user to operate a server. Alternatively, the user can purchase hosting from a third party Web hosting company for their resolver.

- The user may also need to purchase a static IP from their ISP at additional cost.

- The user will need to register a domain and arrange for authoritative name service for the domain or run an authoritative server of their own.

- The user will need to purchase and correctly configure an SSL/TLS certificate from a commercial service provider, or perhaps, use the free Let's Encrypt certificate service.

- The user needs to appropriately limit access to their server so that others can use it while also ensuring that it is not vulnerable to abuse by third parties (e.g., prevent the server from being unintentionally "open").

Contrast the above to-do list with the work involved when "I've got to install an app on my phone." The difference in technical effort and knowledge is noteworthy.

There is also the reality that running your own personal dedicated recursive resolver means that you potentially lose the ability to "hide in the crowd." The fact that you are running your own personal dedicated recursive resolver means that the stream of queries seen in conjunction with that resolver will all correlate 1:1 to you and you alone, or to you and whomever else you allow to use your dedicated recursive resolver such as your family members. One potential redeeming factor is that running your own dedicated personal recursive resolver may be so uncommon that few, if any, would even think to look for that traffic and monitor it. It may also be worth noting that if you are using a third party recursive resolver that sends EDNS Client Subnext extension (or uses other EDNS0 options to increase attributability), your ability to "hide in the crowd" may also be limited. See Appendix 3.

III. Which Encryption Technology Should I Pick?

A great deal of attention has been devoted to the question of which DNS encryption technology users should employ. This section is meant to explain the encryption options available and why, ultimately, the protocols supported in various products may be the ultimate overriding consideration – users can only implement what is available for their device(s).

15. In-Scope Encryption Technologies

There are three primary options that we will consider (in alphabetical order):

- DNS over HTTPS (DoH)[36]
- DNS over TLS (DoT)[37]
- DNSCrypt[38]

16. Encryption Options Out-of-Scope for This Report

We will not be considering a number of other potential DNS encryption solutions, including:

- Confidential DNS[39]
- DNS Over Datagram Transport Layer Security[40]
- DNS Over QUIC[41]
- DNS Over SSH[42]
- Oblivious DNS[43]
- Tor-Based Resolvers Accessed Via Alt-Svc[44]

17. Does It Really Matter If a User Chooses to Use DoH, Instead of DoT, Instead of DNSCrypt?

One individual who has been highly involved with the effort to field an encrypted DNS solution, Patrick McManus, has stated that:

> "DoH builds on the great foundation of DoT. The most important part of each protocol is that they provide encrypted and authenticated communication between clients and arbitrary DNS resolvers . . . What DoH and DoT have in common is far more important than their differences and for some use cases they will work equally well."[45]

[36] https://tools.ietf.org/html/rfc8484

[37] https://tools.ietf.org/html/rfc7858

[38] https://DNSCrypt.info/

[39] https://tools.ietf.org/html/draft-wijngaards-dnsop-confidentialdns-03

[40] https://tools.ietf.org/html/rfc8094

[41] https://datatracker.ietf.org/doc/draft-huitema-quic-dnsoquic/

[42] See for example https://github.com/apenwarr/sshuttle - readme

[43] https://odns.cs.princeton.edu/

[44] https://blog.cloudflare.com/welcome-hidden-resolver/

[45] "The Benefits of HTTPS for DNS," https://bitsup.blogspot.com/2018/05/the-benefits-of-https-for-dns.html

Cloudflare's new "1.1.1.1" app for iPhones and Android offers both DoH and DoT. Their in-app FAQ tackles the choice of DoH versus DoT with the following text:

> "What is the difference between using DNS over TLS and using DNS over HTTPS?
>
> Both DNS over TLS and DNS over HTTPS encrypt plain DNS queries from the phone.
>
> DNS over HTTPS uses port 443 and DNS over TLS uses port 853. In some networks, one of these ports may be blocked. If port 443 is blocked you should use DNS over TLS. If port 853 is blocked, you should use DNS over HTTPS. In some cases, DNS over TLS may be faster than DNS over HTTPS or the other way around."

That said, there are technical differences.

- **One of the best "green light/red light" "thumbs up/thumbs down" comparisons can be seen at** https://dnscrypt.info/faq

  That comparison looks at DNS over SSH, DNS-over-TLS, DNS over HTTPS, DNS over DTLS, and DNS over QUIC. It is worth noting that the last part of that comparison reads: "Practical considerations: All the solutions above offer the same practical security level. Compatibility with existing tools and infrastructure is what makes an actual difference."

- **A critical reality: client support may vary**

  Before you roll out a service at scale or endorse any encrypted DNS protocol for your family, friends, or customers, try it yourself. Try it not just on the operating system you normally use, but on all the popular operating systems your friends, family or customers probably use. (This includes MS Windows 10 and Mac OS X, iOS and Android, broadband routers, etc.). Try it at various locations, too, just as users would – hotels, restaurants and coffee shops, schools, etc.

- **Another critical reality: provider support may vary**

  Who (e.g., what encrypted recursive resolver service provider) do you plan to connect to when using encrypted DNS? What protocols do they support? If they offer DNS over TLS, and DNS over HTTPS, and DNSCrypt, that is great -- when that is true, what they support will not be a gating factor. But if they do not support "everything," beware.

- **DNSCrypt is not an IETF-standardized protocol but it is very widely deployed**

  The main DNSCrypt site[46] states "DNSCrypt is an open specification, with free and open source reference implementations, and it is not affiliated with any company nor organization, however it widely used." The same site claims that DNSCrypt "is probably the most deployed encrypted DNS protocol to date."

[46] https://dnscrypt.info/

- **Proponents of DNS over HTTPS most often tout the fact that DNS over HTTPS uses the "regular" https port, e.g., 443/TCP.**
  From their point of view, this may make it harder for network managers or national network authorities to identify and block DoH traffic, even if they can easily find and block DoT traffic due to its use of a well-known and officially assigned port, 853/TCP. Naturally, port numbers are not the only element that can be used to block unwanted traffic – there are still only a tiny number of services offering any encrypted DNS protocol. If blocking by port number becomes difficult or impossible, assume that network operators will enumerate and begin blocking DoH servers by domain name and/or IP address.

- **Control plane traffic moving into the data plane in DNS over HTTPS**[47]
  Paul Vixie, one of the architects of the DNS, reckoned it is nothing short of a disaster. In October 2018, he tweeted: "RFC 8484 is a cluster duck for internet security. Sorry to rain on your parade. The inmates have taken over the asylum."

  Dr. Vixie has said that DoH is incompatible with the basic architecture of DNS because it moves control plane (signaling) messages to the data plane (message forwarding), and that is a major problem. Network admins, he argued on Twitter also in October 2018, need to be able to see and analyze DNS activity and DoH prevents that. "DoH is an over the top bypass of enterprise and other private networks. But DNS is part of the control plane, and network operators must be able to monitor and filter it. Use DoT, never DoH."

18. How Do the Various DNS Encryption Options Relate to Encrypted VPNs?

Encrypted VPNs often are described as a good "belt and suspenders" option. For example, Bill Woodcock of PCH and the Quad9 project says:[48]

> "[...] it makes sense as a matter of operational security to use both a VPN and a good DNS recursor, and to keep those separate. Not related parties. And make sure that you're cryptographically authenticating your recursive nameserver, so you know if someone tries to redirect you to a MITM [Man-in-the Middle attack]. Also, Tor's good in principle, but it's worth keeping in mind that the moment one party controls any significant number of entry and exit nodes, or any significant number of exit nodes, deanonymization starts to get relatively easy. Intelligence services know this, and have plenty of budget. So, don't trust your VPN operator any more than you have to. Just as you shouldn't trust your DNS operator any more than you have to. Cache locally, QNAME minimize, and read privacy policies."

Unfortunately, at least some encrypted DNS solutions are implemented via VPN profiles, which means that if you elect to encrypt your DNS traffic separately, you may not be able to also run a VPN. In those cases, you may be forced to choose one or the other, not both.

[47] https://www.theregister.co.uk/2018/10/23/paul_vixie_slaps_doh_as_dns_privacy_feature_becomes_a_standard/

[48] https://www.reddit.com/r/privacy/comments/89pr15/dnsoverhttps_vs_dns_overtls_vs_DNSCrypt/

IV. The Mechanics of Encrypting Stub Resolver-to-Recursive Resolver Traffic

19. Options for Encrypting Stub-to-Recursive Resolver Traffic

Using cryptography to protect stub resolver-to-recursive resolver traffic requires more effort than simply entering the IP addresses of an alternative recursive resolver. Why? Most out-of-the-box consumer broadband home routers (and most out-of-the-box consumer computers, tablets and smart phones) currently do not know how to encrypt stub resolver-to-recursive resolver traffic.

To date, the most common approach to encrypting that traffic has been based around installing a DNS proxy on the local system. Once that has been done, the user can then configure the local system to point at the locally-installed DNS proxy, which in turn passes the DNS traffic along to a full recursive resolver over the encrypted connection.

The exact process for doing this varies by platform and by DNS proxy product. To keep those instructions from interrupting the flow of the main body of this paper, the "recipes" for the various platforms are included in a separate document, "M^{3}AAWG Companion Document: Recipes for Encrypting DNS Stub Resolver-to-Recursive Resolver Traffic."

20. How Hard Is It to Set Up Encryption?

The complexity of the installation process will vary from platform-to-platform and from one software solution to another. Some are quick and easy while others may take hours to install, configure and debug.

Technically-inclined users (and even some technophobes) will likely find the process straightforward. Non-technical users may find the process more challenging and may want to ensure they have a technically-inclined friend or relative available to help, or they may want to gain confidence and experience by starting with easy platforms first.

21. Can I Run Multiple DNS Encryption Solutions at the Same Time?

The software solutions described in "M^{3}AAWG Companion Document: Recipes for Encrypting DNS Stub Resolver-to-Recursive Resolver Traffic" generally bind to 127.0.0.1 port 53/TCP, so you will normally only be able to run one DNS encryption solution at a time. That is why the Recipes paper typically shows a test installation process, first. Then, if you decide you like how a particular solution works and want to routinely continue to use it going forward, you can see the instructions explaining how to make your test installation persistent.

Also note that often you can do encryption of a stub resolver-to-recursive resolver or use an encrypted VPN product, but not both on the same platform.

22. “I Just Cannot Seem to Do Encrypted DNS!"

Sometimes you may just need to keep working at it – do not get discouraged and quit just as you may be about to succeed. Other times, you should know that some ISPs, enterprises, and governmental authorities may block attempts to use encrypted alternative DNS servers. The process of identifying and overcoming those filters is explicitly out of scope for this document.

V. Potential Benefits Associated with Using Third Party Encrypted Recursive Resolver Services

In this section, we will discuss some of the benefits potentially accruing to end users choosing to encrypt stub resolver-to-recursive resolver traffic.

23. Using Encrypted Recursive Resolver Services May Help Preserve Access to Content

Some users connect to the internet from heavily-controlled network environments, such as:

- Private homes
- Private businesses
- Totalitarian states
- Military sites/government agencies
- Financial institutions
- Prisons, jails, psychiatric hospitals, juvenile correctional centers and other custodial facilities
- Hospitals and other health care facilities
- Elementary and secondary schools

Network policy in those environments may strictly limit what users can access via the network, including blocking both specific categories of content (such as adult sites, drug-related sites, hate-speech sites, etc.), as well as sites that might enable a determined user to evade network-based filtering. (This latter category often includes virtual private network sites and well-known alternative third party recursive resolvers.)[49] If a user's network traffic is encrypted, it may be somewhat harder for the provider to detect and block third party DNS traffic, depending on the protocols employed.

24. Preventing Eavesdropping ("Passive Monitoring") of Stub-to-Recursive Resolver Traffic

DNS query/response traffic between the stub and recursive resolvers (as represented by the red line in Figure 1 and the red arrows in Figure 2) will normally not be protected against eavesdropping. This means that an adversary who is able to access that unencrypted traffic may be able to discover the sites a user is accessing, including potentially highly privacy-sensitive destinations, such as:

- Financial sites (banks, stockbrokerages, online payment sites, cryptocurrency sites), etc. Even if a hacker or a cracker cannot eavesdrop on the content that is exchanged with those sites, simply knowing the services a user interacts with may help the attacker construct a more-credible, narrowly-tailored phishing message.

- Health-related sites discussing sexually-transmitted diseases, cancer, Alzheimer's, Parkinson's, genetic conditions, etc.

[49] The network operator may use "deep packet inspection" devices (or simple access control lists on appropriate ports or destinations IPs) to block unencrypted access to well-known alternative third party recursive resolvers.

- Sites pertaining to potentially trust-impacting or potential blackmailable conditions, including sites pertaining to treatment for problem gambling, alcoholism, or illicit substance abuse; sites related to sexual practices and proclivities; alternative political or religious sites; etc.

- Sites that may potentially impact a visitor's employment status, such as labor union-related websites, headhunting websites, whistleblower websites, attorney offices known for representing disgruntled employees, investigative journalists, etc.

- Peaceful political sites, religious-protest sites (at least when accessed from repressive countries), etc.

Using a DNS service that encrypts your DNS queries and responses can potentially help[50] to protect you from this sort of eavesdropping -- at least if the attacker is targeting stub-to-recursive traffic. Stub-to-recursive traffic is normally the most sensitive stream of DNS traffic since those queries can be directly associated with a downstream customer.

Be sure to also see Section VII for other considerations to review if privacy protection is an important motivation for moving to encrypted stub resolver-to-recursive resolver protocols.

25. Preventing Spoofing and Impersonation (Active Attacks)

Even if your DNS stub resolver rigorously checks to ensure that you are talking to the recursive resolver you want to talk to, and not some other service that is "masquerading" as the server you wanted to reach, encryption can help protect you against DNS server spoofing and impersonation attacks. Some encrypted DNS solutions may provide that sort of protection while others may not, even though that can leave the users of that service vulnerable to server spoofing and impersonation. The process of verifying a server's "real" identity can sometimes be unexpectedly tricky or can open side channels for leakage of private information, as in cases where a third party certificate authority needs to be contacted to validate an SSL/TLS certificate.

Consider always using a service that supports DNSSEC, regardless of what other crypto may also be used.

26. From the Point of View of the Network Operator, Capex and Opex Formerly Devoted to Fielding a Local Recursive Resolver Service Can Be Devoted to Something Else

Operating a recursive resolver is normally viewed as an ongoing operational responsibility; e.g., a cost center rather than a profit center or point of competitive differentiation. If an ISP can offload running the recursive resolver service to a third party, the cost of the service provider's operating its own recursive resolver service can be avoided and the resulting savings may result in improved profitability, lower user costs, more money for other needs, etc. This can be very seductive, just like outsourcing end-user email service.

[50] Even if you use an encrypted recursive resolver, and the web site is protected with TLS, too, you may still be exposed because of SNI protocols being unencrypted, just to mention one potential bleed-through point. See Appendix 1 for more.

VI. Potential Costs Associated with Using Third Party Encrypted Recursive Resolver Services

A. End-User Issues

27. Performance: DNS Response Time (Latency) May Potentially Increase

Properly designed and operated on-net "local" recursive resolvers will normally have very low-latency – on the order of just a few milliseconds. Low latency is important given that everything a typical user does online begins with DNS and accessing even a single webpage may result in dozens (if not hundreds) of DNS lookups. If those lookups are slow (or timeout altogether), users may become frustrated and perceive their entire connection as "slow" even if the performance issue is only with the DNS service.

28. DNS Availability May Worsen

On-net "local" recursive resolvers with appropriate redundancy will normally have very high availability/very low downtime. High availability and low downtime are important because if the recursive resolver service is down, users perceive the entire internet as being "down."

Some encrypted third party recursive resolvers may be less than carrier grade and may have periodic outages, particularly if they are not on multihomed connectivity. If the encrypted DNS client is configured to overcome any outages, the user may never notice them, but some configurations may be less robust, perhaps allowing only for the configuration of a single server rather than multiple redundant servers. In that case, outages may happen more often and DNS uptime, as perceived by the end user, may go down.

29. Bootstrapping or Deadlock Issues, Including Issues with Time Synchronization and Captive Portals May Arise

There can also be bootstrapping issues when using third party encrypted recursive resolver services. As described by the person who implemented the Firefox TRR (Trusted Recursive Resolver) code:[51]

> "You specify the DOH service as a full URI with a name that needs to be resolved, and in a cold start Firefox won't know the IP address of that name and thus needs to resolve it first or use the provided address you can set with network.trr.bootstrapAddress. Firefox will then use the native resolver for that, until TRR has proven itself to work by resolving the network.trr.confirmationNS test domain. Firefox will also by default wait for the captive portal check to signal "OK" before it uses TRR, unless you tell it otherwise. As a result of this bootstrap procedure, and if you're not in TRRonly mode, you might still get a few native name resolves done at initial Firefox startups. Just telling you this so you don't panic if you see a few show up."

[51] https://daniel.haxx.se/blog/2018/06/03/inside-firefoxs-doh-engine/

Another example of a potential deadlock bootstrap issue was highlighted in conjunction with DNSCrypt. As recounted by one author:[52]

> "The author of DNSCrypt now has provided a tool (hostip) for resolving DNS before DNSCrypt can become active. This is useful for resolving NTP servers, and eliminates the chicken/egg scenario of DNScrypt needing the Time to work, and the Time needing functional DNS to set itself."

30. Long-Running Persistent Encrypted Stub Resolver-to-Recursive Resolver Connections May Be Down-Prioritized by Some Quality of Service (QoS) Traffic Management Rules or by Power Management Schemes on Mobile Devices

Another potential issue involves long-running persistent TCP connections (as used for DNSCrypt) and Quality of Service (QoS) traffic management.[53] When these issues are noticed and understood, they can be worked around -- but that may not always happen.

> "Unlike traditional DNS, DNSCrypt keeps one connection open for all DNS queries, instead of opening multiple smaller connections per query. If you are using Toastman QOS rules, this will result in your queries being sent to the crawl category. To fix this, remove the "KB Transferred" portion of the DNS rule."

Another example of a potential issue associated with long-running encrypted DNS processes, the Cloudflare "1.1.1.1" app's FAQ mentions that:

> **"I kept the app enabled but I noticed it turned off after a while. What happened?**
>
> Your phone is trying to manage the battery by disabling the app. For example, most Huawei devices are known for their aggressive memory and power management. You can fix this by following the steps below:
>
> - Go to the 'Settings' on your phone.
> - Select 'Advanced'
> - Visit 'Battery Manager'
> - Open 'Protect Apps'
> - You can select 'Allow apps to keep running after the screen is turned off' for the 1.1.1.1 app."

31. End-User Defensive Security (and ISP Infection Detection Mechanisms) Can Be Bypassed or Undercut When Provider-Supplied Customer-Protective Filtering Is Avoided

Some providers may use their role as operator of the customer's default recursive resolver service to protect their users from:

- Unknowingly visiting phishing or scam sites
- Being infected with malware
- Inadvertently being exposed to online child abuse or disturbing terrorism-related materials
- Being directed to untrustworthy DNS or Web search services operated by cyber criminals

[52] http://www.linksysinfo.org/index.php?threads/dnscrypt-preview.37031/

[53] ibid

If a user elects to use a third party recursive resolver service instead, that third party service may not offer the same protection as the ISP's recursive resolver service. (Then again, some third party DNS services may offer better protection via their filtered DNS offerings; it all depends on the third party recursive resolver service).[54] If nothing else, if a third party recursive resolver is used, the ISP may have a harder time noticing DNS-based network IOC (indicators of compromise) associated with compromised customer systems.

32. Online Activity May Become Easier to Track Via Encrypted DNS Channels If TCP and/or Cookies are Used

Currently the DNS traffic of thousands of downstream users typically gets comingled and combined behind an ISP's recursive resolvers. If the recursive resolver does not have the information needed to answer a query from its local cache, it will request the needed information with no indication of which specific user is ultimately making that request (e.g., the query source gets "washed," with it appearing as if the ISP's recursive resolver is itself doing the asking). This mixing and interleaving of query traffic from diverse users provides significant protection against tracking of individual users, particularly if long TTLs result in infrequent upstream queries. That helpful mixing and interleaving is lost when encrypted recursive resolvers are used. Suddenly, because of persistent connections, it becomes very easy to isolate and correlated a user's stream of queries, either by exploiting the fact that persistent TCP connections are in use, or by potentially tracking users via cookies.[55]

33. Simply Having Encrypted DNS Traffic (and Having "Missing" or "Limited" Regular DNS Traffic or Both) May Draw Unwanted Attention

Experienced traffic analysts know what normal consumer broadband traffic generally looks like and may often be on the lookout for traffic that seems anomalous or different. One example of an anomaly might be a user that tries to hide all his or her DNS traffic by encrypting it. Another example of an anomaly might be having no discernible regular DNS traffic at all (DNS over HTTPS hides DNS traffic inside regular secure Web traffic). Most regular (uninteresting) users will have discernible, unencrypted DNS traffic. If you are trying to "fly under the radar" and not be noticed, you probably do not want to do things that are likely to make you stand out.

Figure 9. Being Anomalous Can Draw Attention

[54] One head-to-head bake off can be seen at "DNS Security Filters Compared: Quad9 x OpenDNS x Comodo Secure x Norton ConnectSafe x Yandex Safe," https://medium.com/@nykolas.z/dns-security-filters-compared-quad9-x-opendns-x-comodo-secure-x-norton-connectsafe-x-yandex-safe-a00ace3bf21f

[55] See the discussion in RFC 8484 section 8.2 (https://tools.ietf.org/html/rfc8484).

B. Provider (ISP or Enterprise) Issues

34. The DNS Split Horizon Issue in the Enterprise Case

Many enterprises make extensive use of private address space (RFC1918 address space) for non-public "Intranets." When the enterprise runs its own local recursive resolvers for the enterprise users, local users can be given appropriate DNS information. If third party recursive resolvers are used in that sort of split horizon environment, correctly handling Split Horizon DNS deployments can require some care.

In the case of DNS over HTTPS support in the Firefox browser,[56] an effort was made to address this issue by offering "option 2" aka "TRR first" for Firefox's Trusted Recursive Resolver, e.g.:

> “All preferences (go to "about:config") for this functionality are located under the "network.trr" prefix.
> network.trr.mode - set which resolver mode you want.

0	“Off (default). Use standard native resolving only (don't use TRR at all)”
1	“Race native against TRR. Do them both in parallel and go with the one that returns a result first.”
2	**“TRR first. Use TRR first, and only if the name resolve fails use the native resolver as a fallback**
3	“TRR only. Only use TRR. Never use the native (after the initial setup).”
4	“Shadow mode. Runs the TRR resolves in parallel with the native for timing and measurements but uses only the native resolver results.”
5	“Explicitly off. Also, off, but selected off by choice and not default.”

TRR first is more explicitly explained in that article as including:

> “[...] a system that detects if a name can't be resolved at all with TRR and can then fall back and try again with just the native resolver (the so called TRR-first mode). Ending up in this scenario is of course slower and leaks the name over clear-text UDP but this safety mechanism exists to avoid users risking ending up in a black hole where certain sites can't be accessed. Names that causes such TRR failures are then put in an internal dynamic blacklist so that subsequent uses of that name automatically avoids using DNS-over-HTTPS for a while (see the blacklist-duration pref to control that period). Of course this fall-back is not in use if TRR-only mode is selected.
>
> In addition, if a host's address is retrieved via TRR and Firefox subsequently fails to connect to that host, it will redo the resolve without DOH and retry the connect again just to make sure that it wasn't a split-horizon situation that caused the problem.
>
> When a host name is added to the TRR blacklist, its domain also gets checked in the background to see if that whole domain perhaps should be blacklisted to ensure a smoother ride going forward.
>
> Additionally, "localhost" and all names in the ".local" TLD are sort of hard-coded as blacklisted and will never be resolved with TRR. (Unless you run TRR-only...)”

See also "Configuring Networks to Disable DNS over HTTPS" at https://support.mozilla.org/en-US/kb/configuring-networks-disable-dns-over-https

[56] https://daniel.haxx.se/blog/2018/06/03/inside-firefoxs-doh-engine/

35. DNS Debugging Becomes More Complex If Some Applications Use Application-Specific Encrypted Channels While Other Applications Do Not; This May Increase ISP Support Calls/Costs

At least some models for deploying encrypted third party recursive resolver services have focused on deployment via the Web browser, with other applications left to typically continue using the ISP's conventional recursive resolvers. This model, if followed, has the potential to substantially complicate debugging of customer connectivity issues:

- "I can reach the site in my Web browser, but my instant messaging application does not seem to work..."
- "Mail works fine, but my Web browser is broken and can not seem to find the same site..."

Ideally, all applications should use a single consistent source of DNS truth.

36. Irrecoverable Loss of Local DNS Expertise May Occur

Most enterprises, ISPs, and other sites operating recursive resolvers, have staff members with substantial expertise in DNS. If recursive resolver services are outsourced, even as a temporary "experiment," local DNS operational expertise may be lost as part of cost cutting and reorganization measures. It may be hard or impossible to regain that same level of DNS expertise if a third party recursive resolver service "experiment" ultimately proves to be a failure.

37. Load On Name Servers May Increase

Normally the traffic between a stub resolver and an ISP's recursive resolver runs over UDP. Will an environment where encrypted stub resolver-to-recursive resolver traffic runs exclusively over persistent TCP connections crush the ISP's recursive resolver? See a full discussion of this environment in "Is large-scale DNS over TCP practical?"[57]

ISP recursive resolvers also normally heavily-leverage caching: common DNS requests get asked and answered once, with those results being shared across users for further queries until relevant TTLs cook down and expire. In an encrypted recursive resolver environment, if encryption is done without caching, load on servers and the bandwidth consumed by edge links may increase.

38. DNS Traffic May Become Increasingly Centralized Internet-Wide and Prone to a Loss of Diversity and Common-Mode Failures

Currently many different DNS recursive resolvers are deployed at diverse locations (e.g., at ISPs, corporations, colleges and universities, government agencies, etc.), just as on-site email services were once deployed by diverse providers. Those servers also used many different recursive resolver software products.

When recursive resolver services get centralized onto just a relatively small number of providers, "shared failure modes" may develop in DNS, just as they have in messaging, cloud computing, etc. Failures may not happen often in that highly specialized environment, but when they do, perhaps because of distributed denial of service attacks, they will be major.

[57] https://ripe76.ripe.net/presentations/95-jonglez-dns-tcp-ripe76.pdf

39. Subtle but Widely-Relied-Upon DNS Resource Records May Get Interpreted Differently by Some Encrypted Recursive Resolvers

For example, again quoting from the article that summarizes how Firefox's TRR service works:[58]

> "CNAME
>
> The code is aware of CNAME records and will "chase" them down and use the final A/AAAA entry with its TTL as if there were no CNAMEs present and store that in the in-memory DNS cache. This initial approach, at least, does not cache the intermediate CNAMEs nor does it care about the CNAME TTL values.
>
> Firefox currently allows no more than 64(!) levels of CNAME redirections."

This difference in how some names will be resolved may result in subtle and difficult to diagnose anomalous behavior.

[58] https://daniel.haxx.se/blog/2018/06/03/inside-firefoxs-doh-engine/

VII. Even If You are Encrypting Stub-to-Recursive Traffic, Your Online Privacy Will Still Be Imperfect

40. Recursive-to-Authoritative Traffic Will Still Be Unencrypted

As you would expect from its name, "stub resolver-to-recursive resolver" encryption does not deliver “end-to-end” encryption for all the traffic related to a user's DNS queries. It only encrypts DNS queries and responses from the stub resolver running on the user's local system to whatever recursive resolver may be handling those queries. If the recursive resolver has not already cached the name the user needs, unencrypted queries will still end up getting made, albeit now from the recursive resolver to authoritative servers.

The IETF DPRIVE (DNS PRIVate Exchange) Working Group has indicated that they hope to work on the recursive to authoritative issue shortly. See https://datatracker.ietf.org/doc/charter-ietf-dprive/ (last updated 2019-03-27)

41. Recursive-to-Authoritative Traffic Will Still (Often) Not Be Qname Minimized

Unless the recursive resolver operator has taken special care to implement Qname minimization[59] recursive-to-authoritative queries will show the full domain name of interest, not just the minimum information required to proceed. For example, assume a user is interested in resolving www.example.com and their resolver does not have that information already cached. As a first step, if the resolver does not know how to find the com server, all that needs to be sent to the root is the very simple query: "What servers can tell me about dot com?"

Normally, however, that is not what is sent to the root. Instead the root is sent the full hostname of interest, www.example.com. This is more information than it needs and an obvious example of DNS query leakage. Recursive resolver operators should consider deploying Qname minimization to help fix this. See "DNS Query Name Minimisation to Improve Privacy."[60] NLNetLabs also has an excellent discussion of Qname minimization considerations and implications that is well worth reading.[61]

When it comes to individual free or open source recursive resolver products, their Qname minimization status is as follows:

- **BIND**: BIND does Qname minimization as of BIND 9.14[62]
- **Knot:** Knot does Qname minimization[63]
- **Unbound:** For Unbound, Qname minimization has been the default for Unbound since 7 May 2018 per https://nlnetlabs.nl/svn/unbound/tags/release-1.8.1/doc/Changelog

[59] A big thank you to Verisign for licensing their patent relating to Qname minimization (see https://blog.verisign.com/security/minimum-disclosure-what-information-does-a-name-server-need-to-do-its-job/)

[60] https://www.rfc-editor.org/rfc/rfc7816.txt

[61] https://nlnetlabs.nl/downloads/presentations/unbound_qnamemin_oarc24.pdf

[62] See https://kb.isc.org/docs/aa-01310 and https://gitlab.isc.org/isc-projects/bind9/blob/master/HISTORY.md

[63] See for example slide 2 of https://ripe75.ripe.net/presentations/84-knot_resolver.pdf

Reports regarding the Qname minimization status of other free or open source recursive resolver products can be submitted for future updates to this paper by using the Contact Us form on the M^{3}AAWG website.

See Appendix 4 for empirical test data for the recursive resolvers from Section II.9

42. SNI Leakage: SSL/TLS May Still Be "Leaking" The Names of the Sites You Visit

If your goal is to improve your privacy by keeping your Web traffic from being tracked, you should know that even if you encrypt your stub-to-recursive resolver traffic and visit only SSL/TLS-enabled https websites, there is still a good chance that your Web traffic may be exposing more than you may expect or desire. This could be the case if the sites you visit have not yet implemented TLS 1.3 with ESNI support (TLS 1.2 and before leak the server identity via the certificate).[64] (See Appendix 1)

43. EDNS0 Options: The Client Subnet Extension (and Other EDNS0 Options) May Undercut Your Privacy

The good news is that the identity of a user is not normally associated with a query they make – the query appears to be coming from the recursive resolver itself. However, as recursive resolvers begin handling traffic for wider and wider segments of the world, they have grown to need "hints" or "clues" about where the actual querier lives. This is provided by some providers via EDNS0 CSE (Client Subnet Extension). See Appendix 3 for more on that issue. There are also other EDNS0 options that may provide additional specific identifiers.[65]

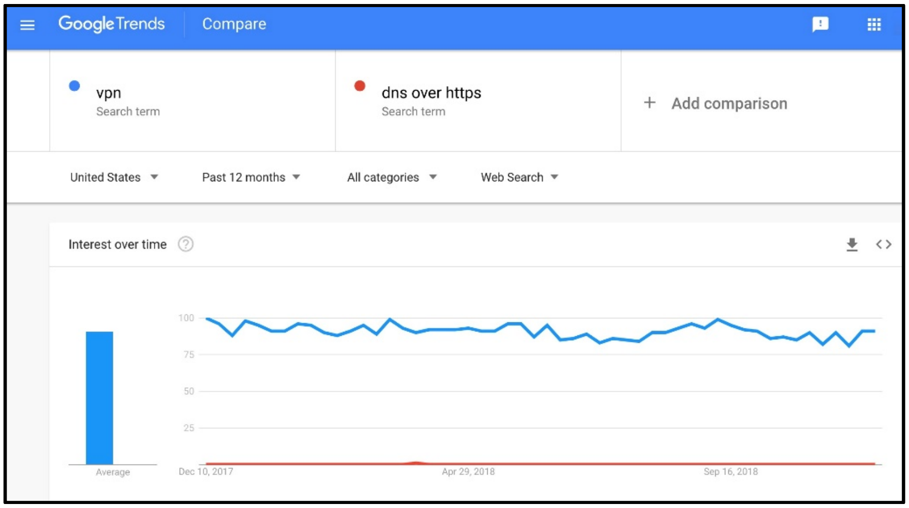
[64] See https://blog.cloudflare.com/encrypted-sni/ and https://encryptedsni.com/

[65] See for example https://docs.umbrella.com/umbrella-api/docs/identifying-dns-traffic2/ and slides 28-29 of https://media.defcon.org/DEF CON 25/DEF CON 25 presentations/DEFCON-25-Jim-Nitterauer-DNS-Devious-Name-Services-Destroying-Privacy-Anonymity-Without-Your-Consent.pdf

VIII. Encrypted Recursive Resolver Connections vs. Encrypted Virtual Private Networks (VPNs)

44. The VPN Alternative to DNS Over HTTPS, DNS Over TLS, or DNSCrypt

While DNS encryption with DNS Over HTTPS, DNS Over TLS, and DNSCrypt have all received a lot of attention in some circles lately, the level of popular interest in Virtual Private Networks (VPNs) consistently dwarfs interest in DNS over HTTPS and related terms, at least as measured by Google Trends:



vpn
Search term

dns over https
Search term

+ Add comparison

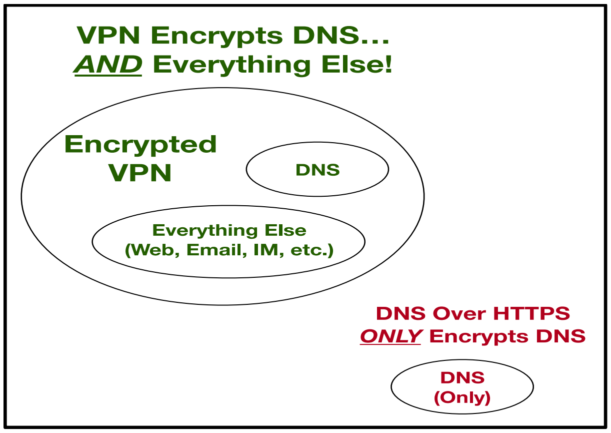
United States ▾ Past 12 months ▾ All categories ▾ Web Search ▾

Interest over time

Figure 10. Google Trends Graph Showing Relative Level of Searches for "vpn" vs. "dns over https"

The dominance of VPNs over DNS over HTTPS, DNS over TLS, and DNSCrypt is understandable when you note two critical facts:

- On many platforms, such as iOS and Android, you can use encrypted DNS or a VPN, but not both simultaneously. (This is because the DNS encryption solutions on mobile devices gets implemented as a "VPN" profile, even though, in fact, they only encrypt DNS traffic.)
- VPNs encrypt all of a user's internet traffic, including, but not limited to, DNS traffic. DNS encryption only encrypts a user's DNS traffic, as show in Figure 11.



VPN Encrypts DNS…
AND Everything Else!

DNS Over HTTPS
ONLY Encrypts DNS

Figure 11. The VPN vs. Encrypted DNS: Differences in Encryption Coverage

45. VPN Trust, Privacy and Online Threat Profile-Related Considerations

Choosing to use a true VPN, rather than just using encrypted DNS, can potentially increase the privacy of your internet traffic but it can also change your online experience in a variety of subtle, and some not so subtle, ways:

- You are probably drawing attention to yourself and losing any ability to blend into the crowd. The fact that you are using a VPN and trying to "hide" what you are doing online may make you stand out and may increase interest in you (and whatever it is that you are presumably trying to avoid having monitored).

- You may be shifting who you trust. No matter where you send your traffic over an encrypted VPN tunnel – that traffic will eventually leave the encrypted tunnel and go onto the regular internet. At that point it becomes monitorable. Previously you trusted your local ISP not to monitor your traffic, now you will be trusting a VPN operator and their ISP(s), instead.

- You may be changing who can identify the source of your traffic. Your ISP has always known your identity since you are their customer and they have provided service to your home or office. They can always tie your traffic to your identity. However, if you use a VPN, the VPN operator becomes the one who will know who you are and what your traffic stream contains.

- You will pay, one way or the other: VPN providers are like any other business: they need to cover their costs. Some simply charge a straight-forward subscription fee. Others may offer a limited "free" trial VPN service and hope that you will get "hooked" and eventually upgrade to their paid "premium" VPN service. A third group will cover their costs by showing you advertising. A fourth group may simply be after market share, hoping to cash in via lucrative venture capital funding or an eventual merger or acquisition. You will want to understand the VPN provider's business model so you can determine if it will work for you. For example, if you are using a VPN to try to avoid being profiled by marketers, a "free" VPN that is supported by advertising may not be a good match for your needs.

- The governmental pervasive monitoring environment may change: The ease with which national intelligence agencies can monitor your traffic may change when you use a VPN and it may potentially become easier for an intelligence agency to monitor you, rather than harder.

  Note that the legal consideration protecting domestic traffic from warrantless pervasive monitoring by U.S. intelligence agencies[66] becomes presumptively "inapplicable" if your traffic exits internationally. Once you route your internet traffic through a third country, that traffic will look as if it is "from" citizens of whatever country your VPN endpoint may be using (Panama, the Netherlands, Iceland, Switzerland, etc.). At that point your traffic may become fair game for U.S. intelligence agencies, for the intelligence agencies of the nation hosting the VPN endpoint, and for any potentially-interested third party intelligence agencies.

[66] https://www.cia.gov/news-information/featured-story-archive/2018-featured-story-archive/top-10-cia-myths.html

- You may suddenly show up on the "radar" of cyber miscreants: The likelihood that you will come to the attention of the hacker or cracker community may change when you use some VPN services. Many potential cyber adversaries are VPN customers themselves, using VPNs to hide their identities and avoid being held accountable for their criminal activities. As a side effect of their defensive "situational awareness" online, they may notice you and your VPN traffic alongside their own. That detection may end up being of no consequence or it may result in an uptick in scans, probes, malicious traffic, scams/spam/phishing, etc.

- VPNs are generally legal but some countries may not allow them. Other countries (e.g. those subject to regime sanctions) may be denied access to VPN software: At the time this document was prepared, countries where VPN use may be unlawful, potentially unlawful, or subject to government restrictions include Belarus, China, Cuba, Democratic Republic of the Congo, Hong Kong, Iran, Iraq, Lebanon, Libya, North Korea, Oman, Pakistan, Qatar, Russia, Saudi Arabia, Somalia, Sudan, Syria, Turkey, Turkmenistan, Ukraine, UAE, Yemen, and Zimbabwe.

  Individuals on the US Department of Commerce Denied Persons List[67] are also barred from using VPN encryption.

  If you have any concerns, consult your attorney for more information before you decide to use a VPN.

46. Usability and User Experience

VPNs also may pose some usability issuess, depending on the product you pick and how you use the internet.

- Providers often will use IP geolocation to figure out where you are located and to infer what language would likely work best when communicating with you. For example, if the VPN you are using had an exit node in Rome, you might routinely see content that had been localized for Italian users or advertising for restaurants or shops in Rome. When you use a VPN with international exit nodes, be prepared to manually toggle your choice of language at remote sites back to your preferred language, such as English.

  When using a VPN, access to some content may also worsen or improve due to geolocation artifacts. For example, some online video services may not work if it looks like you are trying to connect to them from abroad.

- Traffic from some particularly heavily abused VPN exit nodes may be blocked entirely by some providers, or purchases attempted via those nodes may be declined by some online merchants.

[67] See https://www.bis.doc.gov/index.php/regulationsear/740.pdf

- When using a VPN, your traffic may be routed indirectly (like flying from San Francisco to Los Angeles via Honolulu). When your traffic takes an indirect route, its "time-in-flight," or "latency," will increase:

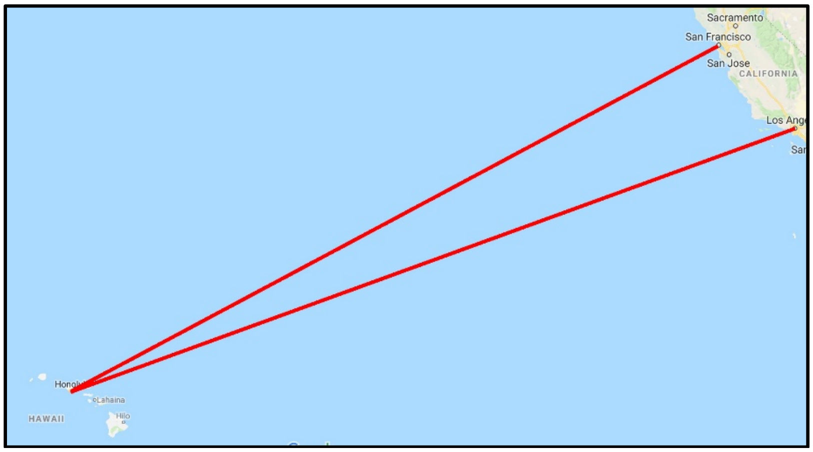


Figure 12. Indirect Routings Add Latency

This latency may be noticeable, depending on how you use the internet:

- Increased latency may make using an editor in an interactive SSH terminal session frustrating.
- Increased latency may make bulk TCP file transfers go slower (due to bandwidth-delay products)
- Increased latency may make VoIP phone calls unsatisfactory. The delay makes it harder to avoid "interrupting" or "stepping on" the party you are calling, unless you agree to adopt "CB radio" style "flow control" and say "over" at the end of each remark, which can be tiresome.
- Increased latency may make online gaming difficult. (That extra latency may result in your character routinely getting zapped by players who have lower latency connections).

47. Ultimately, You are the Only One Who Can Decide if a VPN is the Right Privacy Solution for You

You may decide that it is, or you may decide that it is not. If you decide that you want to use a VPN, how can you determine which one to use? There are many different options (with some of those options even leveraging aggressive "affiliate programs" for marketing!) and it is easy to end up making a suboptimal choice. So, which one should you pick?

48. The Role of M^{3}AAWG in Evaluating Specific VPN Options

M^{3}AAWG does not pick technology "winners" or "losers" but it can provide illustrative lists of major products within defined categories and provide pointers to what third party evaluators have independently and objectively determined. M^{3}AAWG does not endorse or recommend any provider or resource and the educational information listed below is presented as a service to the industry. These products are not affiliated with the Messaging, Malware and Mobile Anti-Abuse Working Group and M^{3}AAWG has no control over their content. The links and information are provided here "as is" without any responsibility for the material and solely for the user's convenience.

49. Internet Security ("Anti-Virus") Companies May Be One Avenue to Finding Easy-to-Trust VPN Providers

A prime objective in selecting a VPN provider (or an encrypted DNS service provider) is finding one you can trust. Unless you are deeply embedded in the cybersecurity industry, you may lack the information needed to do this. Fortunately, many traditional "internet security" or "anti-virus" companies have broadened their offerings to include consumer VPN services. These providers have previously established solid reputations for trustworthiness and discretion. In general, if they ever failed to act in a trustworthy or discrete way, they would quickly be out of business.

The partial list of VPN products shown here all support at least Windows, Mac, iPhone and Android, and some may also support other environments, such as Chrome:

• Avast SecureLine VPN:	https://www.avast.com/en-us/secureline-vpn
• Avira Phantom VPN:	https://www.avira.com/en/avira-phantom-vpn
• F Secure Freedome VPN:	https://www.f-secure.com/en_US/web/home_us/freedome
• Kaspersky Secure Connection:	https://www.kaspersky.com/secure-connection
• McAfee Safe Connect:	https://safeconnect.mcafee.com/
• Norton Secure VPN:	https://us.norton.com/wifi-privacy

We welcome reports via the M^{3}AAWG Contact Us form of other traditional "internet security" or "anti-virus" companies that offer VPN products supporting all of Windows, Mac, iPhone and Android platforms.

50. VPN Service Providers Beyond Traditional Internet Security Companies or Anti-virus Vendors

Besides the providers listed above, there are many VPN service providers that are not associated with internet security companies or anti-virus vendors that can be researched online. Among the articles available online covering VPN:

- "AnchorFree, Maker of a Top Online Privacy App, Raises $295 Million," https://www.nytimes.com/2018/09/05/technology/anchorfree-vpn-hotspot-shield.html

  "[...] AnchorFree, the maker of Hotspot Shield, one of the oldest VPN apps, said Wednesday that it had raised $295 million. The round brings AnchorFree's total funding to $358 million, far outpacing any of its competitors. [...] Hotspot Shield has been downloaded 650 million times. Lately, it has averaged 250,000 downloads a day. For most of the summer [2018], it has been the top-grossing app in its category in the Apple App Store, and in the top 50 over all, according to the app-ranking site

> App Annie. AnchorFree's other apps, Betternet and HexaTech, ranked high on the App Store charts this week, as well as competing VPN apps owned by Norton, McAfee and a variety of obscure companies. [...] Many of AnchorFree's competitors license its technology, including Bitdefender, Dashlane, Kaspersky and McAfee. AnchorFree's tech is also prevalent in smartphones and the products of telecommunications companies. Samsung Galaxy phones come loaded with AnchorFree's VPN software; Verizon and Telefónica license it as well. [article continues]"

See also:

- "The Best VPN Services of 2019," August 23rd, 2019
  https://www.pcmag.com/roundup/296955/the-best-vpn-services

- "Which VPN Services Keep You Anonymous in 2019?" (March 24th, 2019)
  https://torrentfreak.com/which-vpn-services-keep-you-anonymous-in-2019/

IX. Enterprise and ISP Considerations

51. Should an Enterprise or ISP Block – or Attempt to Block – Encrypted DNS Traffic to Third Party Recursive Resolvers?

Generally speaking, no, encrypted DNS traffic to third party recursive resolvers should not be blocked. The development of DNS over HTTPS was motivated at least in part by a desire to help circumvent blocking of DNS over TLS's readily spotted traffic on port 853.

While it is unquestionably true that many, if not all, enterprises and ISPs have the expertise, the technology and the determination required to block encrypted DNS traffic of all types (typically by taking advantage of non-port-based characteristics), attempting to block encrypted user traffic to third party recursive resolver providers would likely:

- Divert network and security staff resources from other projects
- Introduce network management complexity and fragility, potentially with collateral damage to innocent traffic
- Increase user calls for support
- Stimulate more-aggressive encrypted DNS developer efforts aimed at avoiding filtering
- Result in negative publicity and potentially increase customer churn for ISPs or, in enterprises, encourage an unhealthy adversarial relationship between users and enterprise networking and security staff

More generally, is attempting to filter encrypted DNS traffic worth the consequential drain on resources and operations that it would likely cause? Probably not. Instead, we recommend an alternative "harm reduction" strategy,[68] where the enterprise or ISP offers its own free encrypted recursive resolver service with a feature set that is fully (or at least largely) on-par with those of the alternative third party providers. If an ISP or enterprise has successfully fielded their own encrypted recursive DNS service, there should be little reason for users to turn to a third party recursive resolver service provider as an alternative.

In some cases, ISP or enterprise customers may need to ask for encrypted recursive DNS support to be added to the commercial recursive resolver product or products they use.

At the same time, we believe it is incumbent upon operators of third party recursive resolvers to honor local network management decisions by not attempting to evade local network management choices. This means operating transparently, with well-documented IP addresses and port numbers. Operators of third party recursive resolvers should also work to develop a common "code of conduct," including timely sharing of abstracted attack data with relevant providers.

[68] An example of a non-DNS-related harm-reduction can be seen in highway speed limit policies: if statewide speed limits are raised to as-engineered-standards on well-maintained highways in rural areas, police can shift their attention to drivers going truly unsafe speeds; drunk, stoned, and sleepy drivers; speeders in construction zones & school crossing zones; drivers who text while behind the wheel; reckless driving in bad weather conditions; etc.

52. What Encrypted Protocols Should Be Offered on the Enterprise or ISP Encrypted Resolvers?

We recommend offering all three of the leading protocols for encrypting stub resolver-to-encrypted resolver traffic: DNSCrypt, DNS over TLS, and DNS over HTTPS. While enterprises and ISPs might prefer to select just one or two of those protocols, the unfortunate reality is that software client support is still very uneven, and supporting all three will maximize the likelihood that local users will be able to successfully take advantage of the local service rather than having to turn to a third party encrypted DNS service provider.

We realize this recommendation may increase the ISP's responsibilities and associated costs, including potentially complicating support and increasing attack surfaces. When such circumstances drive deployment decisions, some providers may decide that concentrating on offering a single encrypted DNS service, such as DNS over TLS, may be the most pragmatic choice.

53. Offering Enterprise or ISP-Encrypted VPN Services

At the same time the enterprise or ISP enables encrypted stub resolver-to-recursive resolver service, we also encourage these providers to consider offering encrypted VPN service. If users or customers are worried about the security of their network traffic and are exploring encrypted DNS services, they likely are sufficiently worried about eavesdropping and would be candidates for an encrypted VPN service if they could obtain one from a trusted source.

By offering such a service, an ISP can ensure that their traffic will be protected both on its network edge, and while users may be roaming. Service providers would likely prefer that their users or customers do not tunnel their traffic to or from random or sketchy international locations.

54. What About Criminals Abusing Encrypted DNS for Data Exfiltration and Botnet Command and Control-Related Purposes?

This is already being discussed.[69] It will likely be difficult to prevent unless you use ubiquitous SSL/TLS interception and inspection (SSL/TLS "stripping"), and that raises significant issues of its own, particularly in an ISP rather than enterprise or agency environment.[70]

X. Conclusion

DNS is a mission-critical core internet protocol, and normally consumer recursive resolver service is provided for ISP customers by the ISP itself. DNS is a complex protocol and one that is easy to accidentally mis-implement due to the many subtleties involved. To ensure stability, availability, security and interoperability, DNS changes need to be made deliberately and with much testing. Unfortunately, DNS performance concerns, filtering downtime and other considerations may motivate some users to seek recursive resolver services from alternatives parties.

DNS traffic normally travels unencrypted between the stub resolver running on an end-user's device and a recursive resolver that is operated by their ISP or a third party. If left unencrypted, that traffic can be

[69] https://www.trustwave.com/Resources/SpiderLabs-Blog/DOH!-DNS-Over-HTTPS-Poses-Possible-Risks-to-Enterprises/

[70] See https://insights.sei.cmu.edu/cert/2015/03/the-risks-of-ssl-inspection.html and https://www.us-cert.gov/ncas/alerts/TA17-075A ("HTTPS Interception Weakens TLS Security")

eavesdropped upon and may end up revealing sensitive information about an end user's activities online. Even if DNS traffic is encrypted, however, a variety of side channels may still end up revealing sensitive information about the user's activities online – users must not be misled into believing that use of an encrypted recursive resolver will be a "magic pill" that will somehow manage to perfectly protect them from all network monitoring exposures.

Three encryption protocols have been created and are deployed that can help protect the user's DNS traffic from eavesdropping: DNSCrypt, DNS over TLS, and DNS over HTTPS. While there are advantages and disadvantages to each of those protocols, ultimately a user's choice of one over another will likely be a matter of what is preselected by default in an application, or what protocols are available or supported for the relevant devices and available service providers.

When a user is faced with making a choice from among multiple alternative DNS service providers, the choice of service provider may be framed in narrow technical terms:

- Which provider is the closest to me, has the lowest latency or is fastest?
- Which ones are unfiltered? Which ones implement DNSSEC? Which ones refrain from logging my queries? Which ones are accessible via IPv6?

Unfortunately, too little attention is paid to the motivations for offering encrypted recursive resolver service, including business models and the identity of the parties providing the service. Users, even highly privacy-focused users, may not be attuned to subtle technical issues such as use or non-use of Qname minimization practices or use of the EDNS0 Client Subnet Extension, even though these extensions may profoundly affect the trackability of their DNS query stream.

This technology review and tutorial has tackled some of these issues. Practical recipes for encrypting traffic are provided in a separate document, M^{3}AAWG Companion Document: Recipes for Encrypting DNS Stub Resolver-to-Recursive Resolver Traffic. That document covers Mac OS laptops, Microsoft windows laptops, iPhones, Android devices and even home broadband routers (this last via deployment of a sit-alongside Raspberry Pi recursor running Unbound).

The recommendations offered in this paper for M^{3}AAWG and M^{3}AAWG members, also include specific recommendations for software and hardware vendor members, ISPs, end users, and researchers.

Appendix 1: Understanding the Network Eavesdropping Risk in Concrete Terms

Important Note Related to the Following Discussion: Do **NOT** run dnstop, tcpdump, Wireshark or any other promiscuous-mode traffic-inspecting tools on M^{3}AAWG-provided connectivity (such as the M^{3}AAWG conference networks). Doing so is explicitly forbidden by the M^{3}AAWG terms of attendance and network acceptable use policies. These tools are **ONLY** mentioned here for your professional use in validating a resolver installed on a private home network or in conjunction with a resolver on an institutional network that you are authorized to operate and monitor.

App 1-1. Encryption of Web Traffic:

Most Web traffic is now routinely encrypted. For example, consider Google's encrypted traffic:

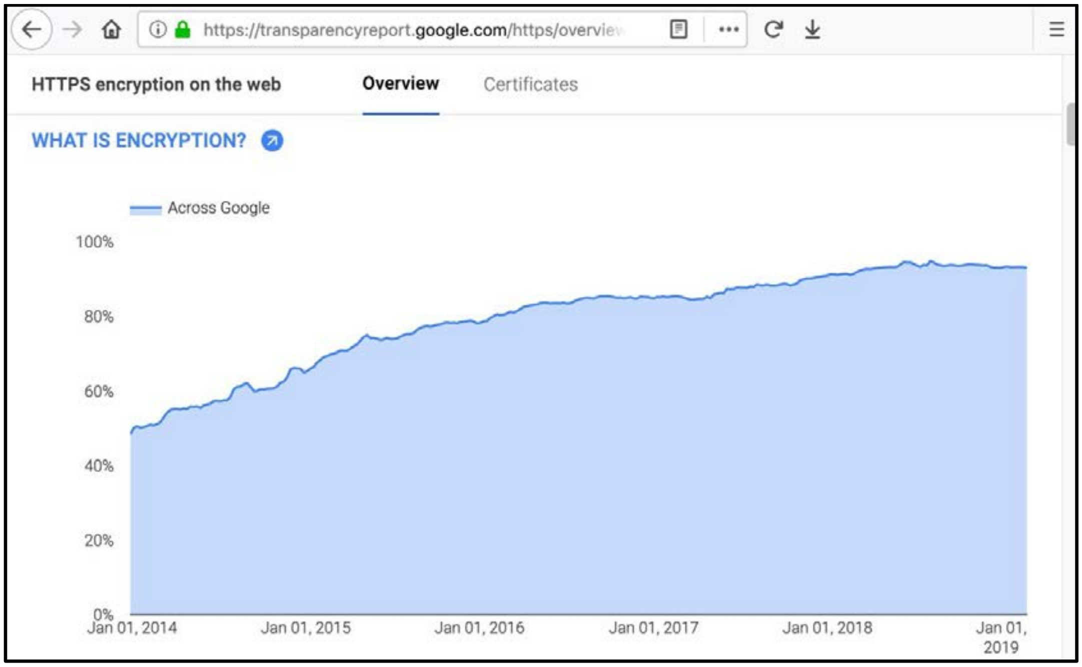
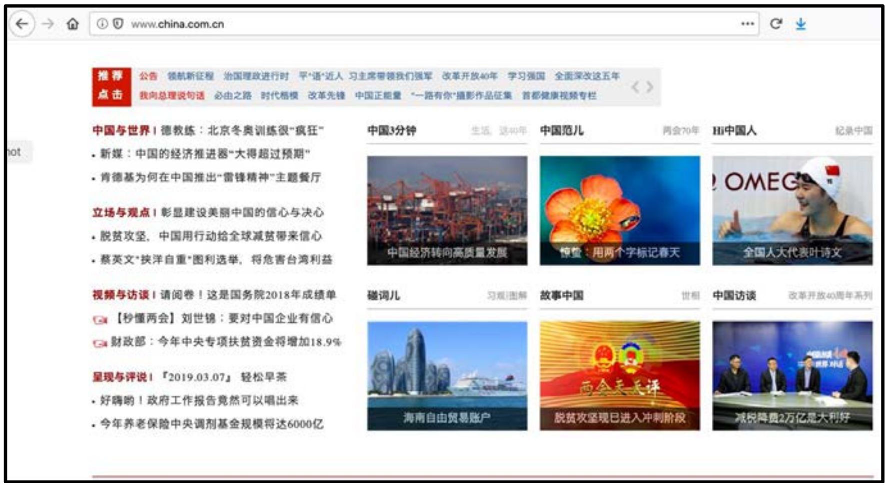


Figure 13. Google HTTPS Traffic Graph

Source: https://transparencyreport.google.com/https/overview?hl=en

App 1-2. Not All Web Traffic Is Encrypted:

However, while most Web traffic is encrypted, there are notable exceptions, particularly in Asia. For example, consider www.china.com.cn (#37 at https://www.alexa.com/topsites/countries/CN):



中国与世界 | 德教练：北京冬奥训练很"疯狂"
- 新媒：中国的经济推进器"大得超过预期"
- 肯德基为何在中国推出"雷锋精神"主题餐厅

立场与观点 | 彰显建设美丽中国的信心与决心
- 脱贫攻坚，中国用行动给全球减贫带来信心
- 蔡英文"挟洋自重"图利选举，将危害台湾利益

视频与访谈 | 请阅卷！这是国务院2018年成绩单
【秒懂两会】刘世锦：要对中国企业有信心
财政部：今年中央专项扶贫资金将增加18.9%

呈现与评说 | 『2019.03.07』 轻松早茶
- 好嗨哟！政府工作报告竟然可以唱出来
- 今年养老保险中央调剂基金规模将达6000亿

Figure 14. Sample Unencrypted Page from www.china.com.cn (#37 on the Alexa Top Sites for China)

App 1-3. Practical Example of What Can Be Seen if Web Traffic Is Not Encrypted:

The use of tcpdump to analyze network traffic is discussed in Appendix 2, but that treatment is rather tedious. Driftnet (https://github.com/deiv/driftnet) is an easy-to-demonstrate, higher-impact, Web traffic monitoring tool: "Driftnet watches network traffic, and picks out and displays JPEG and GIF images for display" (compare the images captured by Driftnet, as shown below, to the illustration above):

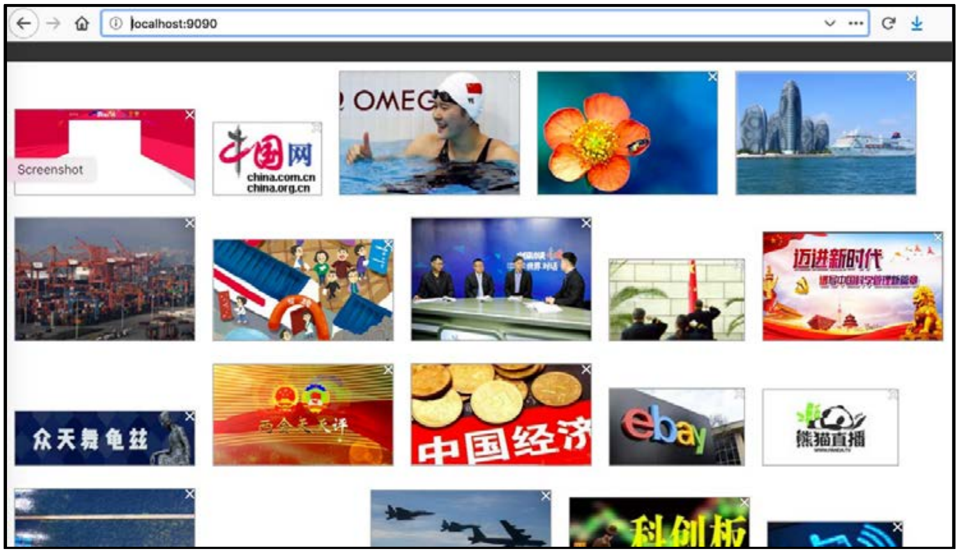


Figure 15. Images From www.china.com.cn Captured with Driftnet

This display should make it clear that unencrypted Web traffic can obviously be easily monitored.

App 1-4. Leakage of "Secure" Website Names:

Even when TLS is used, however, at least the **name of the sites** that users are accessing will typically be available due to current inherent weaknesses in SNI negotiation. Users are sometimes skeptical of the existence of this weakness for some reason – it is as if they cannot believe that anyone sniffing their network traffic could see the names of the encrypted sites they are visiting. Snidump is one tool that can easily be used to demonstrate the reality of this exposure. Install snidump from https://github.com/kontaxis/snidump

Sample run:

```
# snidump -p -i en0
[...]
Capturing ...
192.168.1.79:51892 -> 23.64.199.203:[443]
      20:www.dunkindonuts.com
192.168.1.79:51893 -> 104.92.114.54:[443]
      20:cloud.typography.com
192.168.1.79:51894 -> 104.112.169.57:[443]
     31:assets.secure.checkout.visa.com
[etc]
192.168.1.79:51921 -> 52.8.104.219:[443]
     15:krispykreme.com
[etc]
```

Another example of how you can see the names of the encrypted websites a user may be visiting is by using tshark. tshark is part of the popular network protocol analyzer Wireshark (see https://www.wireshark.org/).

For example:

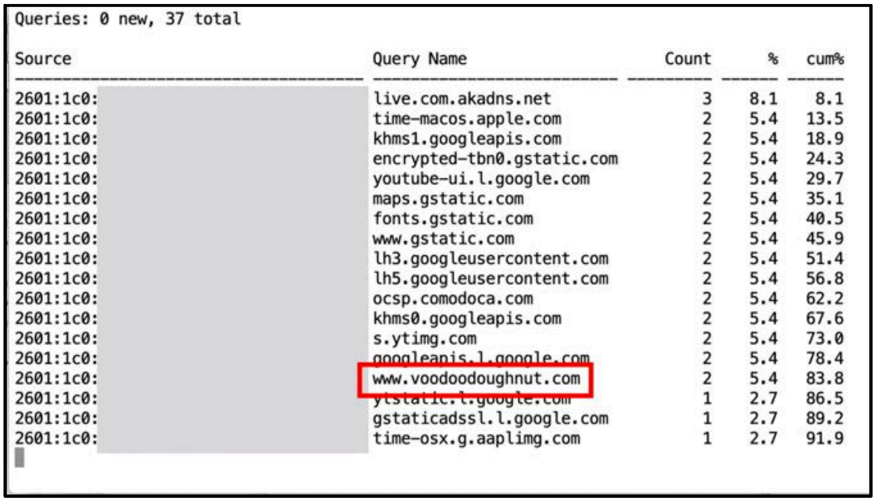
```
# tshark -i en0 -T fields -e tls.handshake.extensions_server_name -Y
tls.handshake.extensions_server_name -n
Capturing on 'Wi-Fi: en0'
www.dunkindonuts.com
assets.secure.checkout.visa.com
cloud.typography.com
[etc]
```

App 1-5. Encryption of DNS Traffic:

Just like unencrypted Web traffic, unencrypted DNS traffic can also be easily monitored.

dnstop is an easy way to watch live traffic on the local subnet for unencrypted DNS traffic.
($ **brew install dnstop** if you are using a Mac running the Homebrew package manager.) The display shown below is for # **dnstop -l 4 en0** (hit $ once the display is running to see Query Names).

Obviously, someone is contemplating a little snack in the following screen capture:



```
Queries: 0 new, 37 total

Source                                  Query Name                  Count      %   cum%
--------------------------------------- -------------------------- ---------- ------ ------
2601:1c0: [redacted]                    live.com.akadns.net                 3    8.1    8.1
2601:1c0: [redacted]                    time-macos.apple.com                2    5.4   13.5
2601:1c0: [redacted]                    khms1.googleapis.com                2    5.4   18.9
2601:1c0: [redacted]                    encrypted-tbn0.gstatic.com          2    5.4   24.3
2601:1c0: [redacted]                    youtube-ui.l.google.com             2    5.4   29.7
2601:1c0: [redacted]                    maps.gstatic.com                    2    5.4   35.1
2601:1c0: [redacted]                    fonts.gstatic.com                   2    5.4   40.5
2601:1c0: [redacted]                    www.gstatic.com                     2    5.4   45.9
2601:1c0: [redacted]                    lh3.googleusercontent.com           2    5.4   51.4
2601:1c0: [redacted]                    lh5.googleusercontent.com           2    5.4   56.8
2601:1c0: [redacted]                    ocsp.comodoca.com                   2    5.4   62.2
2601:1c0: [redacted]                    khms0.googleapis.com                2    5.4   67.6
2601:1c0: [redacted]                    s.ytimg.com                         2    5.4   73.0
2601:1c0: [redacted]                    googleapis.l.google.com             2    5.4   78.4
2601:1c0: [redacted]                    www.voodoodoughnut.com              2    5.4   83.8
2601:1c0: [redacted]                    ytstatic.l.google.com               1    2.7   86.5
2601:1c0: [redacted]                    gstaticadssl.l.google.com           1    2.7   89.2
2601:1c0: [redacted]                    time-osx.g.aaplimg.com              1    2.7   91.9
```

Figure 16. DNS query names captured with dnstop

The highlighted website looks like:

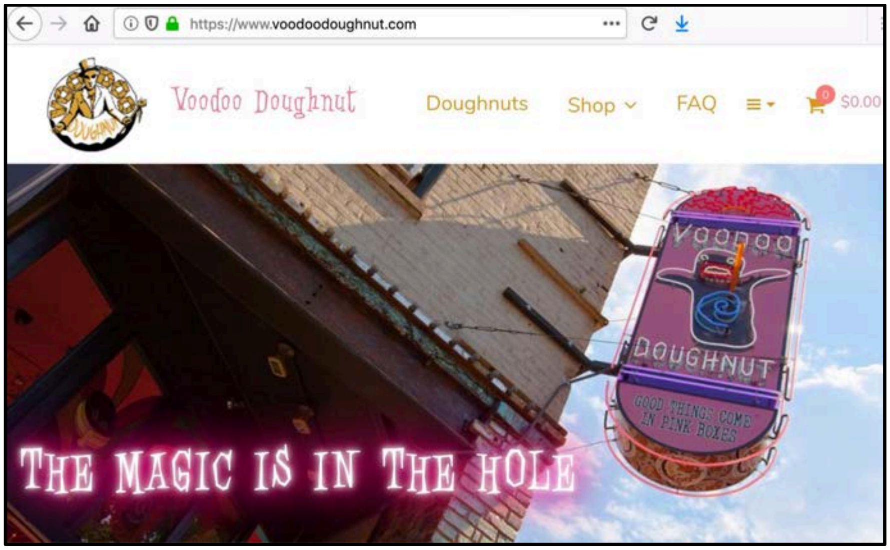


Figure 17. Bricks-and-Mortar Version of the Highlighted Web Site

The points we are making in this Appendix are:

- We have made great progress when it comes to encrypting Web traffic but not all sites use TLS encryption for their websites. When TLS is not implemented, network traffic can be easily eavesdropped on.
- Even when TLS encryption is used to protect Web traffic, that protection is not perfect due to issues like SNI leakage.
- Encryption of stub resolver-to-recursive resolver traffic is an equally important part of maintaining end-user network privacy and that is one reason why M^{3}AAWG has prepared this document.

Appendix 2: Diagnosing and Testing DNS Stub Resolver-to-Recursive Resolver Traffic

> **Important Note:** Do **NOT** run dnstop, tcpdump, Wireshark or any other promiscuous-mode traffic-inspecting tools on M^{3}AAWG-provided connectivity (such as the M^{3}AAWG conference networks). Doing so is explicitly forbidden by the M^{3}AAWG terms of attendance and network acceptable use policies. These tools are **ONLY** mentioned here for your professional use in validating a resolver installed on a private home network or in conjunction with a resolver on an institutional network that you are authorized to operate and monitor.

App 2-1. Check Top Domain Names That Are Being Resolved With dnstop[71] By Watching Live Network Traffic

Installation of dnstop is often possible via whatever package manager you are normally using on a given platform. For example:

```
# apt-get update && apt-get install dnstop   <-- Raspbian

$ brew install dnstop                        <-- Brew on Mac OS X
```

Once installed, try:

```
# dnstop -l 4 eth0
```

To see the source IP for the DNS query plus the domain being resolved (for up to four level names) hit a $

`Ctrl-C` interrupts the display. See `$ man dnstop` for more options.

App 2-2. Inspect DNS Traffic With tcpdump[72]

Ensure you have tcpdump installed. You should be able to install tcpdump using whatever package manager you normally use:

```
# apt-get update && apt-get install tcpdump           <-- Raspbian

$ brew install tcpdump
```

See if there is any DNS traffic on port 53 . . .

- `# tcpdump -nt -i eth0 port 53`

  Decoding those arguments (see `$ man tcpdump`):

`-n`	"Do not convert addresses (i.e., host addresses, port numbers, etc.) to names."
`-t`	"Do not print a timestamp on each dump line."
`-i`	"Listen on interface ..."
`port 53`	"Select just traffic using port 53"

[71] http://dns.measurement-factory.com/tools/dnstop/index.html

[72] http://www.tcpdump.org/

  - What if you are testing an installation that is using unencrypted local traffic from local hosts to a local resolver and see network traffic with FROM addresses in 192.168.1.0/24 TO addresses 192.168.1.0/24? This is normally acceptable (e.g., assuming the traffic is intra device, over hard Ethernet links, or over encrypted links).

- `# tcpdump -nt -i eth0 port 853`

  - Network traffic with FROM 192.168.1.0/24 TO the IP addresses of your upstream resolvers (e.g., 1.1.1.1 or 1.0.0.1) on port 853? Network traffic with addresses FROM your specified upstream resolvers (e.g., 1.1.1.1 or 1.0.0.1) TO 192.168.1.0/24 on port 853? That is also acceptable and as expected.

- Curious what else is on the network besides port 53 (normal DNS), port 853 (DNS over TLS), or port 22 (ssh)?

  ```
  # tcpdump -nt -i eth0 port not 53 and port not 853 and port not 22
  ```

  You will probably see ARP,[73] STP,[74] UPnP/SSDP traffic on port 1900,[75] ND traffic (IPv6 router advertisements)[76] (Now you know some reasons why the lights blink even when no one is doing anything.)

  Want to focus on what is left? Hide more of that traffic with . . .

  ```
  # tcpdump -nt -i eth0 port not 53 and port not 853 and port not 22
  and not arp and not stp and port not 1900
  ```

- Coming back to the DNS traffic, want to see still more detail?

  ```
  # tcpdump -vv -x -X -s 1500 -i eth0 port 53
  ```

  Decoding the new options:

`-vv`	"Even more verbose output."
`-x`	"When parsing and printing, in addition to printing the headers of each packet, print the data of each packet (minus its link level header) in hex. The smaller of the entire packet or snaplen bytes will be printed [...]"
`-X`	"When parsing and printing, in addition to printing the headers of each packet, print the data of each packet (minus its link level header) in hex and ASCII."
`-s1500`	"Snarf snaplen bytes of data from each packet [...]"

[73] https://en.wikipedia.org/wiki/Address_Resolution_Protocol

[74] https://en.wikipedia.org/wiki/Spanning_Tree_Protocol

[75] https://en.wikipedia.org/wiki/Simple_Service_Discovery_Protocol

[76] https://en.wikipedia.org/wiki/Neighbor_Discovery_Protocol

App 2-3. Verifying/Troubleshooting SSL/TLS Certificate Issues

Normally, the major alternative recursive resolver providers will have non-problematic SSL/TLS certificate installations that are readily accessible from most end-user networks or systems. However:

- If you are working from an environment that may be blocking, intercepting or hijacking DNS-related SSL/TLS traffic, you may need to figure out who is doing it and why.

- It is also possible that a smaller third party, alternative encrypted DNS service might have SSL/TLS certificate issues, such as expired certificates.

- You might be curious if your third party alternative encrypted DNS service provider's SSL/TLS installation is following best practices or what type of certificate they are using.

Nykolas Z has a Medium.com blog post[77] that does a nice job of introducing the use of the openssl client tool and the dns-over-tls-php-client for troubleshooting in a DNS over TLS context.

[77] https://medium.com/@nykolas.z/troubleshooting-dns-over-tls-e7ca570b6337

Appendix 3. The EDNS0 Client Subnet Extension

App 1-3. EDNS0 Client Subnet (ECS) Extension: Is It Supported or Stripped/Not Sent?

A small number of third party recursive resolvers[78] may provide hints (of varying specificity) about where you are geographically located via an extension known as the EDNS0 Client Subnet Extension,[79] or ECS. However, these are very busy resolvers that generate a substantial percentage (44.248%) of all the DNS traffic measured.[80]

EDNS0 Client Subnet Extension is a very subtle technical feature that is nonetheless potentially important for you to understand if you are privacy-minded. The problem it is designed to address typically arises when huge networks share recursive resolvers across hundreds of thousands or even millions of users, with those users spread out from coast to coast and even overseas. DNS traffic from all those users may be pooled and appear to "come from" just one or two places. Without the EDNS0 Client Subnet extension, all those users might appear to come from New York, for example, even if some of them are from San Diego or Italy or Peru.

The Good: EDNS0 Client Subnet Extension hints can help content distribution networks (CDN) and other internet services sort that out. For example, if EDNS0 Client Subnet Information is passed that shows users are working from New York, they can be serviced by an Atlantic CDN node On the other hand, if EDNS0 Client Subnet information shows that users are in fact working from California, they can be serviced by a Pacific CDN node, instead.

Similarly, EDNS0 Client Subnet can help ensure localization works as it should: users from France can be provided a French language experience, while users from Germany have a German language experience, and so on.

The Bad: At the same time, however, if ECS addresses are specified with too-fine granularity, upstream providers and others can see exactly (or nearly exactly) who is making each DNS query, and the normal privacy from having your DNS queries pooled with the queries of thousands of other users can be lost entirely or at least severely degraded.

App 3-2. Summary Results:

We have checked the EDNS0 Client Subnet Behavior of the eight third party recursive resolvers listed in Section II.9. To check them, we used the approach described in https://www.ietf.org/mail-archive/web/dnsop/current/msg16055.html

Third Party Recursive Resolver Services that Do Use the EDNS0 Client Subnet Extension:

Cisco/OpenDNS (we checked 208.67.222.222)
Google (we checked 8.8.8.8)
Oracle/Dyn (we checked 216.146.35.35)

[78] https://ithi.privateoctopus.com/graph-m3.htmlsays an average of 0.003% of all resolvers do the EDNS0 Client Subnet Extenson

[79] See https://tools.ietf.org/html/rfc7871and http://www.afasterinternet.com/

[80] https://ithi.privateoctopus.com/graph-m6.html

Third Party Recursive Resolver Services That Do Not Appear to Use the EDNS0 Client Subnet Extension:

- **Cleanbrowsing** (we checked 185.228.168.9)
- **Cloudflare** (we checked 1.1.1.1)
- **Comodo** (we checked 8.26.56.26)
- **IBM/PCH/GCA** (we checked 9.9.9.9)
- **Neustar** (we checked 156.154.70.5)

App 3-3. Which Should I Pick? Services that Do Use EDNS0 Client Subnet Extension or Services that Do Not Use It?

There is no single right or wrong answer on this one. If performance is your top consideration, you may prefer a service that does use it. If privacy is your overarching drive, you may want to select a service that does not use it.

App 3-4. You Did Not Test a Service that I am Interested In. Can I Test Other Services? How Did You Test?

See the examples below:

Sample Queries Showing EDNS0 Client Subnet Usage and Non-Usage:

A Provider That Does Use EDNS0 Client Subnet Extension -- Google:

```
$ dig @8.8.8.8 +short -t txt edns-client-sub.net | txt2jq[81]
{
  "ecs_payload": {
    "family": "1",
    "optcode": "0x08",
    "cc": "US",
    "ip": "[source IP elided for this report]",
    "mask": "24",
    "scope": "0"
  },
  "ecs": "True",
  "ts": "1541642160.86",
  "recursive": {
    "cc": "US",
    "srcip": "74.125.186.4",
    "sport": "50933"
  }
}
```

[81] See https://mailarchive.ietf.org/arch/msg/dnsop/jfVScq7O6WTD-Tn6IlMNSnoqWJo

A Provider That Does Not Use EDNS0 Client Subnet Extension -- Cloudflare

```
$ dig @1.1.1.1 +short -t txt edns-client-sub.net | txt2jq
{
  "ecs": "False",
  "ts": "1541645001.2",
  "recursive": {
    "cc": "US",
    "srcip": "[source IP elided for this report]",
    "sport": "63491"
  }s
}
```

A Provider That Does Not Respond to Test Queries -- Verisign:

```
$ dig @64.6.64.6 -t txt edns-client-sub.net

; <<>> DiG 9.10.6 <<>> @64.6.64.6 -t txt edns-client-sub.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16892
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;edns-client-sub.net.         IN   TXT

;; AUTHORITY SECTION:
edns-client-sub.net.     0    IN   SOA  ns1.edns-client-sub.net.
admin.edns-client-sub.net. 0 0 0 0 5

;; Query time: 148 msec
;; SERVER: 64.6.64.6#53(64.6.64.6)
;; WHEN: Mon Apr 22 09:43:41 PDT 2019
;; MSG SIZE  rcvd: 94
```

Appendix 4. Qname Minimization

App 4-1. Qname Minimization Use:

Qname minimization limits unnecessary domain information leakage to authoritative name servers. Currently a little over 18% of recursive resolvers use Qname minimization.[82] Focusing on our well-known third party resolvers:

Cloudflare:

```
$ dig qnamemintest.internet.nl txt @1.1.1.1 +short
a.b.qnamemin-test.internet.nl.
"HOORAY - QNAME minimisation is enabled on your resolver :)!"
```

Comodo:

```
$ dig qnamemintest.internet.nl txt @8.26.56.26 +short
a.b.qnamemin-test.internet.nl.
"HOORAY - QNAME minimisation is enabled on your resolver :)!"
```

Cisco's OpenDNS:

```
$ dig qnamemintest.internet.nl txt @208.67.222.222 +short
a.b.qnamemin-test.internet.nl.
"NO - QNAME minimisation is NOT enabled on your resolver :("
```

Cleanbrowsing:

```
$ dig qnamemintest.internet.nl txt @185.228.168.9 +short
a.b.qnamemin-test.internet.nl.
"NO - QNAME minimisation is NOT enabled on your resolver :("
```

Google:

```
$ dig qnamemintest.internet.nl txt @8.8.8.8 +short
a.b.qnamemin-test.internet.nl.
"NO - QNAME minimisation is NOT enabled on your resolver :("
```

IBM/PCH/GCA:

```
$ dig qnamemintest.internet.nl txt @9.9.9.9 +short
a.b.qnamemin-test.internet.nl.
"NO - QNAME minimisation is NOT enabled on your resolver :("
```

[82] https://ithi.privateoctopus.com/graph-m3.html

Neustar:

```
$ dig qnamemintest.internet.nl txt @156.154.70.5 +short
a.b.qnamemin-test.internet.nl.
"NO - QNAME minimisation is NOT enabled on your resolver :("
```

Oracle/Dyn:

```
$ dig qnamemintest.internet.nl txt @216.146.35.35 +short
a.b.qnamemin-test.internet.nl.
"NO - QNAME minimization is NOT enabled on your resolver :("
```

Verisign:

```
$ dig qnamemintest.internet.nl txt @64.6.64.6 +short
a.b.qnamemin-test.internet.nl.
"NO - QNAME minimisation is NOT enabled on your resolver :("
```

Appendix 5. DNS Padding

App 5-1. What is DNS Padding? Why Do We Need It?

RFC7830 ("The EDNS(0) Padding Option") introduces the need for DNS padding by saying:

> "The Domain Name System (DNS) [RFC1035] was specified to transport DNS messages in cleartext form. Since this can expose significant amounts of information about the Internet activities of an end user, the IETF has undertaken work to provide confidentiality to DNS transactions (see the DPRIVE working group at https://datatracker.ietf.org/doc/charter-ietf-dprive/). Encrypting the DNS transport is considered one of the options to improve the situation.
>
> However, even if both DNS query and response messages were encrypted, metadata could still be used to correlate such messages with well-known unencrypted messages, hence jeopardizing some of the confidentiality gained by encryption. One such property is the message size.
>
> This document specifies the Extensions Mechanisms for DNS (EDNS(0)) "Padding" option, which allows DNS clients and servers to artificially increase the size of a DNS message by a variable number of bytes, hampering size-based correlation of the encrypted message."

App 5-2. How Should We Actually Do DNS Padding?

RFC8467 ("Padding Policies for Extension Mechanisms for DNS (EDNS(0))"), published in October 2018, says:

> "[RFC7830] specifies the Extension Mechanisms for DNS (EDNS(0)) "Padding" option, which allows DNS clients and servers to artificially increase the size of a DNS message by a variable number of bytes, hampering size-based correlation of encrypted DNS messages.
>
> However, RFC 7830 deliberately does not specify the actual length of padding to be used. This memo discusses options regarding the actual size of padding, lists advantages and disadvantages of each of these "padding strategies", and provides a recommended (experimental) strategy.
>
> Padding DNS messages is useful only when transport is encrypted using protocols such as DNS over Transport Layer Security [RFC7858], DNS over Datagram Transport Layer Security [RFC8094], or other encrypted DNS transports specified in the future."

App 5-3. How Can I Use DNS Padding?

Users interested in DNS padding as an aspect of their DNS encrypted recursive resolver service should consult https://edns0-padding.org/implementations/ for an overview of encrypted recursive resolver products with padding support. (Support is still quite limited at the time this was written.)

As with all documents that we publish, please check the M^{3}AAWG website (www.m3aawg.org) for updates.