Measuring the Availability and Response Times of Public Encrypted DNS Resolvers

Ranya Sharma, Nick Feamster, Austin Hounsel

Abstract. Unencrypted DNS traffic between users and DNS resolvers can lead to privacy and security concerns. In response to these privacy risks, many browser vendors have deployed DNS-over-HTTPS (DoH) to encrypt queries between users and DNS resolvers. Today, many client-side deployments of DoH, particularly in browsers, select between only a few resolvers, despite the fact that many more encrypted DNS resolvers are deployed in practice. Unfortunately, if users only have a few choices of encrypted resolver, and only a few perform well from any particular vantage point, then the privacy problems that DoH was deployed to help address merely shift to a different set of third parties. It is thus important to assess the performance characteristics of more encrypted DNS resolvers, to determine how many options for encrypted DNS resolvers users tend to have in practice. In this paper, we explore the performance of a large group of encrypted DNS resolvers supporting DoH by measuring DNS query response times from global vantage points in North America, Europe, and Asia. Our results show that many non-mainstream resolvers have higher response times than mainstream resolvers, particularly for non-mainstream resolvers that are queried from more distant vantage points—suggesting that most encrypted DNS resolvers are not replicated or anycast. In some cases, however, certain non-mainstream resolvers perform at least as well as mainstream resolvers, suggesting that users may be able to use a broader set of encrypted DNS resolvers than those that are available in current browser configurations.

1 Introduction

The Domain Name System (DNS) is a critical component of the Internet's infrastructure that translates human-readable domain names (*e.g.*, `google.com`) into Internet Protocol (IP) addresses [23]. Most Internet communications begin with a client device sending DNS queries to a recursive resolver, which in turn queries one or more name servers, which ultimately refer the client to a server who can map the domain to an IP address. The *response times* of these queries—the time to contact a recursive resolver, query various name servers, and return the results—is important because the DNS underlies virtually all communication on the Internet. For example, loading a web page, a browser must first resolve the domain names for each object on the page before the objects themselves can be retrieved and rendered. Thus, the performance of DNS lookup is of utmost importance to application performance such as web performance, as slow DNS lookup times will lead to slow web page loads.

Browser	Cloudflare	Google	Quad9	NextDNS	CleanBrowsing	OpenDNS
Chrome	✓	✓		✓	✓	✓
Firefox	✓			✓		
Edge	✓	✓	✓	✓	✓	✓
Opera	✓	✓				
Brave	✓	✓	✓	✓	✓	✓

Table 1: *Modern browsers provide only a few choices for encrypted DNS resolver, which we define as* **mainstream** *resolvers.*

DNS did not originally take privacy and security into account: DNS queries have historically been unencrypted, leaving users susceptible to eavesdropping [29]; queries can also be intercepted and manipulated [19]. To address these types of privacy and security vulnerabilities, encrypted DNS protocols have been developed and deployed, including DNS-over-HTTPS (DoH) [13], which is now deployed—and even enabled by default—in many browsers. DoH enables clients to communicate with recursive resolvers over HTTPS, providing privacy and security guarantees that DNS previously lacked.

For better or worse, most contemporary deployments of DoH have occurred in browsers that provide limited options for resolvers [4, 7]. Although DoH protects against on-path eavesdropping, it does not prevent resolvers *themselves* from seeing the contents of DNS queries. Thus, some have argued that browser-based DoH deployments shift privacy concerns from eavesdroppers to potential misuse by major DNS providers [32].

Table 1 shows the DoH resolvers that have been deployed to users of major browsers as of October 20, 2021 [5, 11, 22, 25, 26]. We define the resolvers listed in Table 1 as *mainstream*. Yet, many other DoH resolvers have been deployed that are currently not in use by major browser deployments [8]—in other words, there are many non-mainstream DoH resolver deployments.

Previous studies have measured encrypted DNS performance, but they have mostly focused on mainstream DNS resolvers [12, 14, 15, 20]. In this paper, we expand on these previous studies, exploring the performance of all encrypted DNS resolvers—from a variety of global vantage points, as opposed to simply characterizing the mainstream DoH providers from well-connected vantage points. Towards this goal, we make the following contributions:

1. We measure DoH response times a large list of resolvers, including both mainstream DoH resolvers that are included in major browser vendors *and* a large collection of non-mainstream resolvers.
2. We study how the performance of various DoH resolvers differ based on vantage point.

To our knowledge, this paper presents the first study of DoH performance measurements for non-mainstream resolvers, as well as the first comparison of DoH performance across a variety of vantage points, for a large number of resolvers. To perform these experiments, we developed and released an open-source tool for measuring encrypted DNS performance to replicate and extend these results, and to support further research on DoH performance.

The rest of the paper is organized as follows. Section 2 provides background on DNS, including the origin of encrypted DNS and related standards, and discusses related work. Section 3 details our research questions, the experiments we conducted to study these questions, and the limitations of the study. Section 4 presents the results of these experiments. Section 5 concludes with a discussion of the implications of these results and possible directions for future work.

2 Background and Related Work

In this section, we provide background on encrypted DNS protocols, including the current deployment status of encrypted DNS, as well as various related work on measuring encrypted DNS.

2.1 Background: Encrypted DNS

The Domain Name System (DNS) translates human-readable domain names into Internet Protocol (IP) addresses, which are used to route traffic [23]. These queries have typically been unencrypted, which enables on-path eavesdroppers to intercept queries and manipulate responses.

Encrypted DNS. Protocols for encrypting DNS traffic have been proposed, standardized, and deployed in recent years, including DNS-over-HTTPS (DoH) and DNS-over-TLS (DoT). Zhu et al. proposed DoT in 2016 to address the eavesdropping and tampering of DNS queries [36]. It uses a dedicated port (853) to communicate with resolvers over a TLS connection. In contrast, DoH—proposed by Hoffman et al. in 2018—establishes HTTPS sessions with resolvers over port 443 [13]. This design decision enables DoH traffic to use HTTPS as a transport, facilitating deployment as well as making it difficult for network operators and eavesdroppers to intercept DNS queries and responses [6]. DoH can function in many environments where DoT is easily blocked.

Moving the privacy threat. Encrypting DNS queries and responses hides queries from eavesdroppers but the recipient of the queries—the DNS resolver—can see the queries [28]. By design, recursive resolvers receive queries from clients and typically need to perform additional queries to a series of authoritative name servers to resolve domain names. For these resolvers to determine the additional queries they need to perform (or determine if the query can be answered from cache), they must be able to see the queries that they receive from clients. Thus, although DoT and DoH make it difficult for eavesdroppers along an intermediate network path to see DNS traffic, recursive resolvers can still observe (and potentially, log) the queries that they receive from clients. The fact that many mainstream DoH providers (e.g., Google) already collect significant information about users potentially raises additional privacy concerns and makes it appealing for users to have a large number of encrypted DNS resolvers that are reliable and perform well. For this reason, users may wish to have more control over the recursive resolver that they use to resolve encrypted DNS queries. Having a reasonable set of choices that perform well in the first place is thus important, and determining whether such a set exists is the focus of this paper.

Status of browser DoH deployments. Most major browsers currently support DoH, including Brave, Chrome, Edge, Firefox, Opera, and Vivaldi. Operating systems have also announced plans to implement DoH, including iOS, MacOS, and Windows [17,18,31,34,35]. In this paper, we focus on DoH because it is more widely deployed than DoT. Each of these browsers and operating systems either currently support or have announced support for DoH (but, to our knowledge, not DoT).

2.2 Related Work

Previous measurement studies of encrypted DNS. Previous studies have typically measured DoT and DoH response times the protocols from the perspective of a few commonly used resolvers [20]; in contrast, in this paper, we study a much larger set of encrypted DNS resolvers, many of which are not available as default options in major browsers. Zhu et al. proposed DoT to encrypt DNS traffic between clients and recursive resolvers [36]. They modeled its performance and found that DoT's overhead can be largely eliminated with connection re-use. Böttger et al. measured the effect of DoT and DoH on query response times and page load times from a university network [6]. They find that DNS generally outperforms DoT in response times, and DoT outperforms DoH. They also find that much of the performance cost for DoT and DoH can be amortized by re-using TCP connections and TLS sessions. Hounsel et al. also measure response times and page load times for DNS, DoT, and DoH using Amazon EC2 instances [14]. They compare the recursive resolvers for Cloudflare, Google, and Quad9 to the local recursive resolvers provided by Amazon EC2 from five global vantage points in Ohio, California, Seoul, Sydney, and Frankfurt. They find that despite higher response times, page load times for DoT and DoH can be *faster* than DNS on lossy networks. Lu et al. utilized residential TCP SOCKS networks to measure response times from 166 countries and found that, in the median case with connection re-use, DoT and DoH were slower than conventional DNS over TCP by 9 ms and 6 ms, respectively [20]. In contrast to previous work, our focus in this paper is not to measure the DoH protocol itself or its relative performance to unencrypted DNS; instead, our goal is to compare the performance of encrypted DNS resolvers *to each other*, to understand the extent to which this larger set of DNS resolvers could be used by clients and applications in different regions.

Studies and remedies for the centralization of encrypted DNS. Other work has studied the centralization of the DNS and proposed various techniques to address it. Foremski et al. find that the top 10% of DNS recursive resolvers serve approximately 50% of DNS traffic [10]. Moura et al. [24] measured DNS requests to two country code top-level domains (ccTLD) and found that five large cloud providers being responsible for over 30% of all queries for the ccTLDs of the Netherlands and New Zealand. Hoang et al. [12] developed K-resolver, which distributes queries over multiple DoH recursive resolvers, so that no single resolver can build a complete profile of the user and each recursive resolver only learns a subset of domains the user resolved. Hounsel et al. also evaluate the performance of various query distribution strategies and study how these strategies affect the amount of queries seen by individual resolvers [16]. This line of research complements our work—these previous studies in many ways motivate an enable the use of multiple encrypted DNS resolvers, but designing a system to take advantage of multiple recursive resolvers must be informed about how the choice of resolver affects performance.

Other DNS performance studies. Researchers have also studied how DNS performance affects application performance. Sundaresan et al. used an early FCC Measuring Broadband America (MBA) deployment of 4,200 home gateways to identify performance bottlenecks for residential broadband networks [30]. This study found that page load times for users in home networks are significantly influenced by slow DNS response times. Allman studied conventional DNS performance from 100 residences in a neighborhood and found that only 3.6% of connections were blocked on DNS with lookup times greater than either 20 ms or 1% of the application's total transaction time [1]. Otto et al. found that the ability of a content delivery network to deliver fast page load times to a client could be significantly hindered when clients choosing recursive resolvers that are far away from CDN caches [27]; a subsequent proposal, namehelp, proxied DNS queries for CDN-hosted content and sent them directly to authoritative servers. Wang et al. developed WProf, a profiling system that analyzes various factors that contribute to page load times [33]; this study demonstrated that queries for uncached domain names at recursive resolvers can account for up to 13% of the critical path delay for page loads. We do not measure the performance of a large number of encrypted DNS resolvers from residential broadband access networks in this paper nor do we study the effect of the choice of a broad range of encrypted DNS resolvers on page load time, but doing so would be a natural direction for future work.

3 Method

In this section, we describe the metrics used, how these metrics are measured, and our experiment setup.

3.1 Metrics

Availability. We are interested in determining which DoH resolvers are still active and responding to queries. We define a resolver as unresponsive from a given vantage point if we fail to receive *any* response to the queries issued from a particular server.

Latency. We performed network latency measurements for each recursive resolver. Each time we issued a set of DoH queries to a resolver, we also issued four ICMP ping messages and computed the average round-trip time. This enabled us to explore whether there was a consistent relationship between high query response times and network latency.

DNS query response time. We define DNS query response time as the end-to-end time it takes for a client to initiate a query and receive a response. To measure query response times with various DoH resolvers, we extended the open-source DNS measurement tool developed by Hounsel et al. [14] The tool enables researchers to issue traditional DNS, DoT, and DoH queries. It utilizes the `getdns` library for traditional DNS and DoT, and `libcurl` for DoH.

For each DoH resolver, the tool establishes a TCP connection and an HTTPS session, encodes a DoH query, sends the query to the DoH resolver, and reports the response time to the client. Importantly, the tool includes the time it took to establish a TCP connection and an HTTPS session. We note that `libcurl` attempts to utilize TLS 1.3 when a recursive resolver supports it, and otherwise falls back to an older version (e.g., TLS 1.2). It also attempts to utilize HTTP/2, falling back to an older version when a recursive resolver does not support it.

We modified the tool to support continuous DoH response time measurements across multiple days. We also modified the tool to enable clients to provide a list of DoH resolvers they wish to perform measurements with, preventing clients from needing to re-run the executable for each resolver (link anonymized for review). After a set of measurements complete with a list of DoH resolvers and domain names, the tool writes the results to a JSON file.

3.2 Experiment Setup

To provide a comparative assessment of DNS performance across DoH resolvers, we perform measurements across 75 DoH resolvers, grouped by their geographical locations—17 in North America, 22 in Asia, and 36 in Europe [8]. We performed our measurements between October 15–25, 2021. We also took the four highest performing resolvers (`Google`, `Cloudflare`, `Quad9`, `Hurricane Electric`) located in North America and measured their performance in Europe and Asia to better understand how they compare in farther vantage points. We employed MaxMind's GeoLite2 databases to geolocate each DoH resolver [21].

Vantage Points. We performed our measurements from three global vantage points through Amazon EC2 [2]. We deployed one server in each of the Ohio, Frankfurt, and Seoul EC2 regions. We chose to perform measurements from multiple global vantage points to understand how DoH performance varies not only by which resolver is used, but also which geographic region the client is located in. Each server utilized 16 GB of RAM and 4 virtual CPU cores (the `t2.xlarge` instance type), and they each used Debian 10 [3].

Resolvers and Domain Names. Section A.2 on page 15 lists each of the DoH resolvers we measured. These resolvers were scraped from a list of public DoH resolvers provided by the `DNSCrypt` protocol developers [9]. Previous work has largely studied major DNS providers in use by web browsers; in contrast, we measure the performance of a larger set of encrypted DNS resolvers [12,14,15,20].

We issued queries for two domains to each resolver: `google.com` and `netflix.com`. We chose these domains based on their popularity, but other domain names would have likely sufficed. We do not expect our choice of domain names to unfairly skew our performance comparisons between resolvers.

Measurement Procedure. We performed the following steps to measure the performance of each of the encrypted DNS resolvers, from each of our three vantage points:

1. For each resolver that we aim to measure, establish an HTTPS session and send a DoH query, measuring the query response time for two domain names.
2. For each resolver, issue four ICMP ping probes and compute the average round-trip latency.

Limitations. Our work has several limitations. First, we do not measure how encrypted DNS affects application performance, such as web page load time. Ultimately, an assessment of the effects of encrypted DNS performance on application performance, including web page load time, across the full set of encrypted DNS resolvers, could provide a more comprehensive understanding of the effects of encrypted DNS on application performance. Another potential limitation of our work is that we perform measurements exclusively from Amazon EC2 instances, which are located in data centers. Future work could explore similar measurements from a wider variety of access networks, including cellular networks and broadband access networks. Furthermore, although we do not expect it to affect conclusions, it may be informative to perform measurements from a larger set domain names; our measurements perform DNS lookups to just two domain names. Finally, since DoH can re-use TCP connections and TLS sessions, future work should report connection setup times separately.

4 Results

In this section, we describe the results of our experiments. We explore which non-mainstream resolvers are available; how the performance of mainstream resolvers compares to that of non-mainstream resolvers; and whether (and to what extent) encrypted DNS response time correlates to high network latency. As described in Section 3, our results represent measurements from October 2021; future work could perform ongoing measurements based on the measurement framework we have developed to validate and extend these results.

4.1 Are Non-Mainstream Resolvers Available?

We first aimed to study the availability of encrypted DNS resolvers. We received responses from most resolvers that we queried. Table 2 shows the most common errors we received from attempting to communicate with the resolvers.[1] The most common errors were related to a failure to establish a connection. It is likely that in many of these cases, the resolver itself was

[1] Due to a bug, we did not record one rare error type.

Error	Count	% of All Responses
Couldn't Connect to Server	47,377	7%
HTTP Error Status	38,475	5.7%
Couldn't Decode Response	26,686	4%
SSL Connect Error	17,720	2.6%
Couldn't Resolve the Resolver's Domain Name	8,864	1.3%
SSL Certificate Error	4,465	0.7%
Other Error	234	$< 1\%$
SSL Timeout	27	$< 1\%$
Error in the HTTP/2 Framing Layer	2	$< 1\%$
Successful Responses	**531,528**	**78.7%**
All Errors	**143,848**	**21.3%**

Table 2: *Errors when trying to perform DoH queries from all vantage points.*

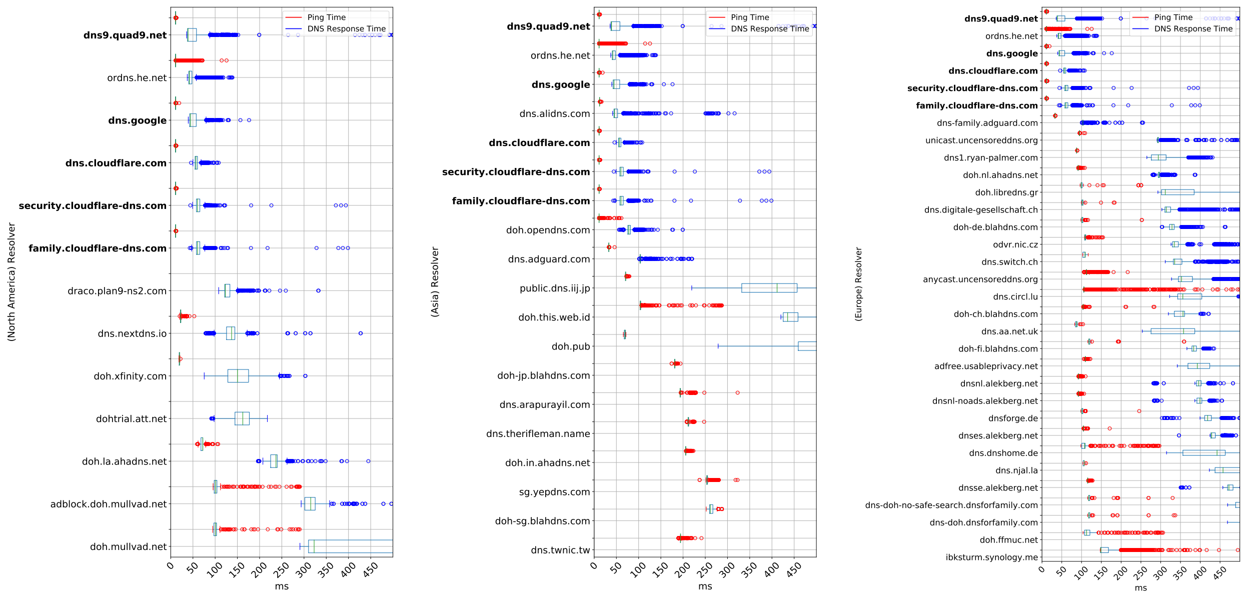
simply no longer operational; additional longitudinal measurements could confirm this hypothesis. We did not receive a response from eleven resolvers: `dns1.dnscrypt.ca`, `dns2.dnscrypt.ca`, `doh.cleanbrowsing.org`, `doh.post-factum.tk`, `doh.linuxsec.org`, `doh.tiar.app`, `jp.tiar.app`, `doh.appliedprivacy.net`, `doh.bortzmeyer.fr`, `doh.chewbacca.meganerd.nl`, `doh.powerdns.org`. However, we only performed measurements at a single point in time, and thus we lack enough measurements to draw general conclusions about the availability of these resolvers. Future work could extend this work to perform longitudinal measurements of availability of these resolvers.[2]

4.2 How Do Non-Mainstream Resolvers Perform?

Given the large number of non-mainstream resolvers that have not been previously studied, we aimed to study how the performance of these encrypted DNS resolvers compared to mainstream ones. As previously mentioned, one of our motivations in doing so is to better understand the global extent of encrypted DNS resolver deployment, as existing lists of public encrypted DNS resolvers [9] do not provide any overview of either reliability or performance. Additionally, given that most organizations who have deployed mainstream resolvers are based in the United States, we also wanted to explore how the performance of a broader set of encrypted DNS resolvers varied by geography.

Figures 1–3 show the distributions of DNS response times and ICMP ping times across encrypted DNS resolvers, as measured from vantage points in the United States, Asia, and Europe, respectively. The plots show distributions for both DNS response times and ICMP round-trip latency. Although some distributions extend beyond 500 ms, we have truncated the plots for ease of exposition, since responses beyond this range will not result in good application performance. Certain resolvers did not respond to our ICMP ping probes; for those resolvers, no latency data is shown.

[2] We will release our measurement framework and data upon publication of this work.

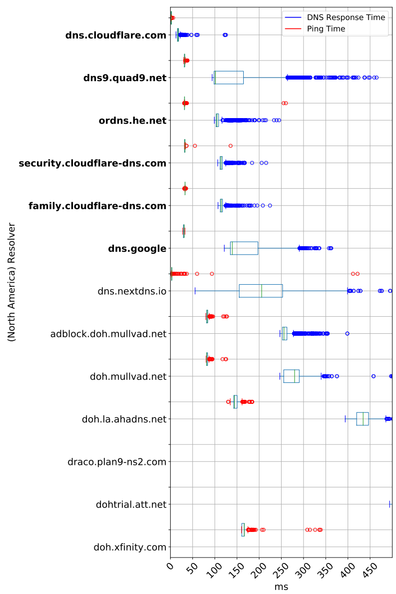


(a) North America (Local). (b) Asia. (c) Europe.

Fig. 1: *The DNS response time and ICMP ping time distributions for encrypted DNS resolvers measured from a vantage point in the United States (Ohio). Mainstream resolvers are shown in boldface across all three sub-figures.*

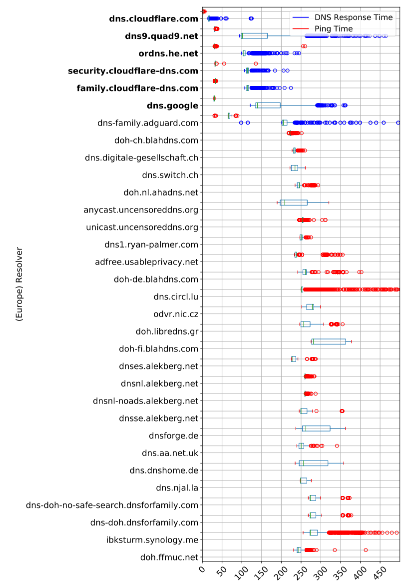
As expected, most mainstream resolvers outperformed non-mainstream resolvers from most vantage points. Non-mainstream resolvers also exhibited higher variability of median query response times. From North America, we observe that aside from the five resolvers with the lowest encrypted DNS response time, median query response times ranged from 60 ms to 323 ms, all considerably above typical DNS lookup response times. From Asia, median response times outside of the top five were extremely variable, ranging from 114 ms to 31.6 seconds. Although the slowest resolver in Asia as measured from Asia was an extreme outlier, we saw that several resolvers in Asia had slow median response times, even when queried from Asia. For example, the second-slowest resolver also exhibited slow performance, with a median response time of about one second from our vantage point in Asia. We observe more consistent performance for resolvers in Europe, but we still see median query response times outside the top five range from 19 ms to 156 ms.

In some cases, however, a particular non-mainstream resolver would outperform the mainstream DoH resolvers. As expected, `dns.quad9.net`, `dns.google`, and `dns.cloudflare.com` were among the top five highest performing DoH resolvers in North America, Europe, and Asia. Interestingly, however, `ordns.he.net`—a DoH resolver hosted by Hurricane Electric, a global Internet service provider (ISP)—managed to outperform `dns.google` and `dns.cloudflare.com` from all three vantage points. From Frankfurt, `dns-family.adguard.com` and `ordns.he.net` are the top two highest performing resolvers; from Seoul, `doh-jp.blahdns.com` and `ordns.he.net` outperforms `dns.google`.



(a) North America.

(b) Asia (Local).



(c) Europe.

Fig. 2: *The DNS response time and ICMP ping time distributions for encrypted DNS resolvers measured from a vantage point in Asia (Seoul, South Korea). Mainstream resolvers are shown in boldface across all three sub-figures.*

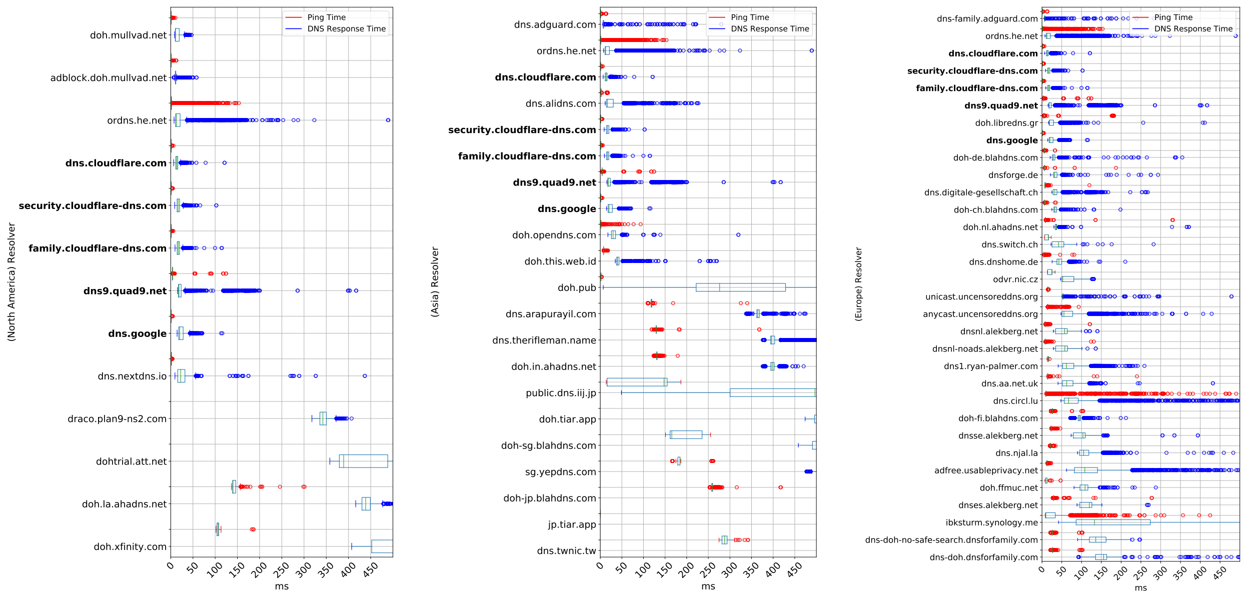
Resolver	**Vantage Point** Seoul (ms)	Frankfurt (ms)
dns.twnic.tw	31606.61	32319.90
doh-jp.blahdns.com	109.62	773.47
sg.yepdns.com	238.01	548.67
public.dns.iij.jp	200.82	496.74
doh-sg.blahdns	214.44	534.51

Table 3: *Median DNS response times for non-mainstream resolvers (Asia).*

Resolver	**Vantage Point** Frankfurt (ms)	Seoul (ms)
doh.ffmuc.net	108.92	1309.88
ibksturm.synology.me	132.66	1254.47
dns-doh-no-safe-search.dnsforfamily	135.88	1159.70
dnsforge.de	31.86	1043.03
dns-doh.dnsforfamily	155.81	1162.27

Table 4: *Median DNS response times for non-mainstream resolvers (Europe).*

To better understand the extent to which certain encrypted DNS resolvers perform well for clients in some regions but not others, we identified resolvers that exhibited low DNS response times in for clients in one region but not another. Tables 3 and 4 show the five encrypted DNS resolvers for Europe and Asia that exhibit the largest differences in median DNS response times when queried from a remote vantage point (queries of resolvers in Asia from Europe, and of resolvers of Europe from Asia, respectively). In both cases, Table 3 shows that non-mainstream resolvers located in Asia perform better from the vantage point in Seoul than the one in Frankfurt. Similarly, as expected, Table 4 shows that the median response times of non-mainstream resolvers in Europe are much lower when measured from Frankfurt than the response times of those same resolvers measured from Seoul.



(a) North America. (b) Asia. (c) Europe (Local).

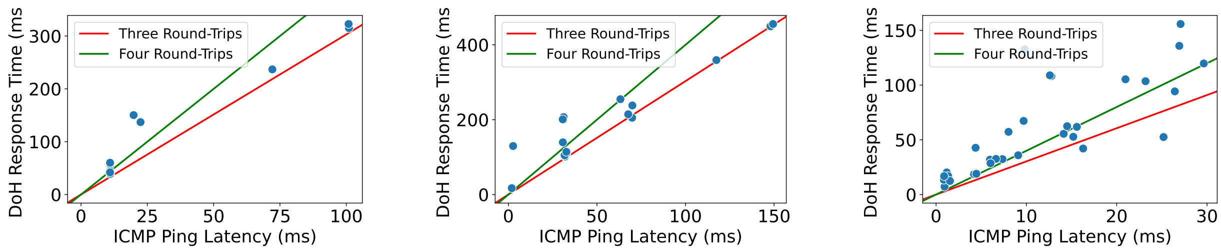
Fig. 3: *The DNS response time and ICMP ping time distributions for encrypted DNS resolvers measured from a vantage point in Europe (Germany). Mainstream resolvers are shown in boldface across all three sub-figures.*

4.3 Does Latency to Resolver Correlate with Performance?

Figure 4 compares median ICMP ping latencies to median query response times for each resolver. Higher network latency naturally translates to higher DNS response times (as encrypted DNS queries do require several network round trips): absent connection re-use, a DoH lookup will require at least three network round trips: one for the TCP three-way handshake, one for the TLS handshake (piggybacked on the third part of the three-way handshake), and one for the DNS query and response. `libcurl` uses TLS 1.3 when available on the server, and otherwise falls back to an older version (e.g., TLS 1.2), which requires an additional network round trip. It also attempts to use HTTP/2, falling back to an older version when necessary. Thus, we can expect that "normal" DoH lookup times would be about 3–4 times the network latency.

In some cases, certain resolvers performed worse than might be expected as a result of the latency from the vantage point to the resolvers. For example, from North America, we observed a median query response time of 872 ms to `doh.xfinity.com` despite a network round-trip latency of merely 166 ms. Many non-mainstream resolvers in Europe and Asia exhibit encrypted DNS response times that are more than 4x the round-trip network latency. These discrepancies between network latency and DNS response times may be due to a number of factors, including both caching and server load.

From Frankfurt, we observed two resolvers with median DoH query response times that are less than 3–4 times the median network latency to these resolvers:



(a) Ohio (Local). (b) Seoul (Local). (c) Frankfurt (Local).

Fig. 4: *Median DoH query response times vs. median round-trip network latency for each local DoH resolver, from each vantage point.*

`dns.switch.ch` and `odvr.nic.cz`. We hypothesize that this could be attributed to anomalous ICMP ping data and network optimizations that enable DoH queries to be completed in fewer round-trips. Two resolvers—`doh.this.web.id` and `dns.twnic.tw`—are not shown in Figure 4(b) because their median query response times are greater than 1,000 ms. For reference, the next slowest resolver from Seoul has a median query response time of 456 ms.

5 Conclusion

The increased deployment of encrypted DNS, including DNS-over-HTTPS (DoH) has been accompanied both with "mainstream" DoH deployments in major browser vendors, as well as a much broader deployment of encrypted DNS servers around the world that are not among the common choices for resolvers in major browsers. Understanding the viability of this larger set of encrypted DNS resolvers is important, particularly given that a lack of diversity of viable resolvers potentially could create new privacy concerns, if only a small number of organizations provided good performance. We find that many non-mainstream resolvers have higher median response times than mainstream ones, particularly if the resolvers are not local to the region; in contrast, most mainstream resolvers appear to be replicated and provide better response times across different geographic regions. Some non-mainstream resolvers exhibit particularly poor performance, exceeding four times the network round-trip latency between the client and resolver. In some cases, however, a local non-mainstream resolver can exhibit equivalent performance as compared mainstream resolvers (*e.g.*, `ordns.he.net` in North America, `dns.alldns.com` in Europe, and `doh.libredns.gr` in Europe). These results suggest both good news and room for improvement in the future: On the one hand, viable alternatives to mainstream encrypted DNS resolvers do exist. On the other hand, users need easy ways of finding and selecting these alternatives, whose availability and performance may be more variable over time than mainstream resolvers. It is also clear that there is an opportunity to invest in deploying and maintaining reliable, performant, global encrypted DNS infrastructure operated by a greater diversity of organizations.

References

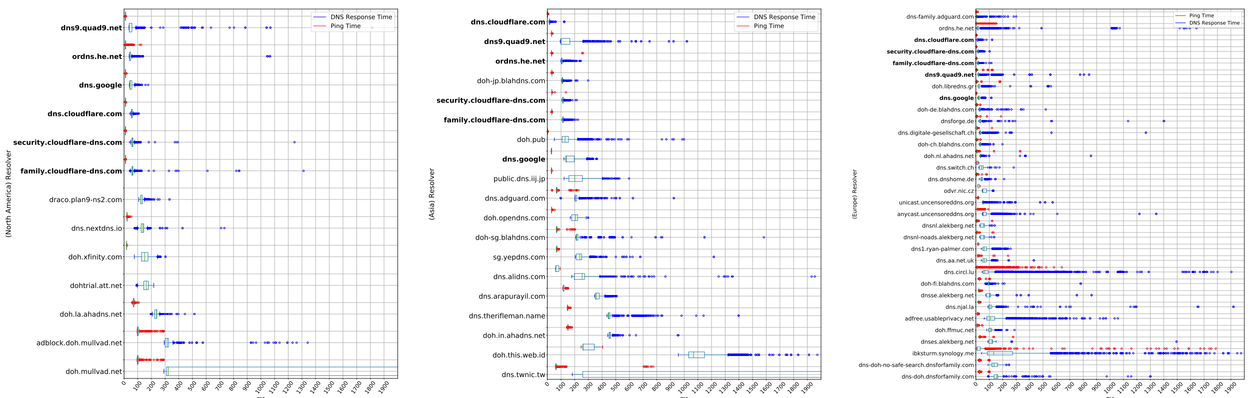
1. Allman, M.: Putting DNS in Context. In: Bustamante, F., Feamster, N. (eds.) Proceedings of the Internet Measurement Conference (IMC) 2020. Associatian for Computing Machinery (ACM) (2020), https://dl.acm.org/doi/10.1145/3419394.3423659
2. Amazon: Amazon EC2 (2021), https://aws.amazon.com/ec2
3. Amazon: Amazon EC2 Instance Types (2021), https://aws.amazon.com/ec2/instance-types/
4. Baheux, K.: A safer and more private browsing experience with Secure DNS (2020), https://blog.chromium.org/2020/05/a-safer-and-more-private-browsing-DoH.html
5. Brave: Brave (2021), https://www.brave.com
6. Böttger, T., Cuadrado, F., Antichi, G., Fernandes, E.L., Tyson, G., Castro, I., Uhlig, S.: An Empirical Study of the Cost of DNS-over-HTTPS. In: Proceedings of the 19th Internet Measurement Conference (IMC). Association for Computing Machinery (ACM) (2019), https://dl.acm.org/doi/pdf/10.1145/3355369.3355575
7. Deckelmann, S.: Firefox continues push to bring DNS over HTTPS by default for US users (2020), https://blog.mozilla.org/en/products/firefox/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users/
8. DNSCrypt: DNSCrypt and DoH Servers (2021), https://dnscrypt.info/public-servers/
9. DNSCrypt: DNSCrypt Public Resolvers (2021), https://github.com/dnscrypt/dnscrypt-resolvers
10. Foremski, P., Gasser, O., Moura, G.C.M.: DNS Observatory: The Big Picture of the DNS. In: Proceedings of the 19th Internet Measurement Conference (IMC). Association for Computing Machinery (ACM) (2019), https://dl.acm.org/doi/abs/10.1145/3355369.3355566
11. Google: Google Chrome (2021), https://www.google.com/chrome/index.html
12. Hoang, N.P., Lin, I., Ghavamnia, S., Polychronakis, M.: K-resolver: Towards decentralizing encrypted dns resolution. In: Proceedings of the Workshop on Measurements, Attacks, and Defenses for the Web (MADWeb) 2020. Internet Society (2020), https://www.ndss-symposium.org/wp-content/uploads/2020/02/23009-paper.pdf
13. Hoffman, P., McManus, P.: DNS Queries over HTTPS (DoH). Tech. Rep. 8484 (2018), https://www.ietf.org/rfc/rfc8484.txt, (Standards Track)
14. Hounsel, A., Borgolte, K., Schmitt, P., Holland, J., Feamster, N.: Comparing the Effects of DNS, DoT, and DoH on Web Performance. In: Proceedings of The Web Conference 2020. Association for Computing Machinery (2020), https://doi.org/10.1145/3366423.3380139
15. Hounsel, A., Schmitt, P., Borgolte, K., Feamster, N.: Can Encrypted DNS Be Fast? In: Passive and Active Network Measurement Conference (PAM). Springer (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3427563
16. Hounsel, A., Schmitt, P., Borgolte, K., Feamster, N.: Encryption without centralization: Distributing dns queries across recursive resolvers. In: Proceedings of the Applied Networking Research Workshop (ANRW) 2021 (2021), https://doi.org/10.1145/3472305.3472318
17. Jensen, T.: Windows Insiders can now test DNS over HTTPS (2020), https://techcommunity.microsoft.com/t5/networking-blog/windows-insiders-can-now-test-dns-over-https/ba-p/1381282

18. Johnson, R.: How to Enable Encrypted DNS on iPhone iOS 14 (2021), https://rodneylab.com/how-to-enable-encrypted-dns-on-iphone-ios-14/
19. Jones, B., Feamster, N., Paxson, V., Weaver, N., Allman, M.: Detecting DNS Root Manipulation. In: Passive and Active Measurement Conference (PAM) (2016), https://www.icir.org/mallman/pubs/JFP+16/JFP+16.pdf
20. Lu, C., Liu, B., Li, Z., Hao, S., Duan, H., Zhang, M., Leng, C., Liu, Y., Zhang, Z., Wu, J.: An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come? In: Proceedings of the 19th Internet Measurement Conference (IMC). Association for Computing Machinery (ACM) (2019)
21. MaxMind: GeoLite2 Free Geolocation Data (2021), https://dev.maxmind.com/geoip/geolite2-free-geolocation-data?lang=en
22. Microsoft: Microsoft Edge (2021), https://www.microsoft.com/en-us/edge
23. Mockapetris, P.: Domain names - implementation and specification. Tech. Rep. 1035 (1987), https://www.ietf.org/rfc/rfc1035.txt, (Standards Track)
24. Moura, G.C., Castro, S., Hardaker, W., Wullink, M., Hesselman, C.: Clouding up the Internet: how centralized is DNS traffic becoming? In: Proceedings of the Internet Measurement Conference (IMC) 2020. Association for Computing Machinery (ACM) (2020), https://dl.acm.org/doi/pdf/10.1145/3419394.3423625
25. Mozilla: Firefox (2021), https://www.mozilla.org/en-US/firefox/new/
26. Opera: Opera Web Browser (2021), https://www.opera.com
27. Otto, J.S., Sánchez, M.A., Rula, J.P., Bustamante, F.E.: Content Delivery and the Natural Evolution of DNS: Remote DNS Trends, Performance Issues and Alternative Solutions. In: Proceedings of the Internet Measurement Conference (IMC) 2012 (2012), https://www.aqualab.cs.northwestern.edu/wp-content/uploads/2019/02/OttoIMC2012.pdf
28. Rashid, F.: The Fight Over Encrypted DNS: Explained (2019), https://spectrum.ieee.org/the-fight-over-encrypted-dns-boils-over
29. Schmitt, P., Edmundson, A., Feamster, N.: Oblivious DNS: Practical Privacy for DNS Queries. In: Symposium on Privacy Enhancing Technologies (PETS) 2019. Stockholm, Sweden (2019), https://content.sciendo.com/view/journals/popets/2019/2/article-p228.xml
30. Sundaresan, S., Feamster, N., Teixeira, R., Magharei, N.: Measuring and Mitigating Web Performance Bottlenecks in Broadband Access Networks. In: Proceedings of the Internet Measurement Conference (IMC) 2013 (2013), https://hal.sorbonne-universite.fr/file/index/docid/937167/filename/paper.pdf
31. TechJourney: How to Enable DNS over HTTPS in Chrome / Edge / Opera / Chromium (2020), https://techjourney.net/how-to-enable-dns-over-https-in-chrome-edge-opera-chromium/
32. Vixie, P.: My Chromecast Ultra Would Not Start Until I Began Answering 8.8.8.8 (2019), https://mailarchive.ietf.org/arch/msg/dnsop/WCVv57IizUSjNb2RQNP84fBclI0/
33. Wang, X.S., Balasubramanian, A., Krishnamurthy, A., Wetherall, D.: Demystifying Page Load Performance with WProf. In: USENIX Symposium on Networked Systems Design and Implementation (NSDI) (2013), https://www.usenix.org/system/files/conference/nsdi13/nsdi13-final177.pdf
34. Wilton-Jones, T.: Vivaldi's powerful privacy settings (2019), https://vivaldi.com/blog/vivaldi-powerful-privacy-settings/
35. Wyman, A., Rodaro, M., Mozinet, Branton, W., Joni, Seburo, Gardenhire, L., Lazar, A., Fabi: Firefox DNS-over-HTTPS (2021), https://support.mozilla.org/en-US/kb/firefox-dns-over-https

36. Zhu, L., Hu, Z., Heidemann, J., Wessels, D., Mankin, A., Somaiya, N.: Connection-oriented DNS to Improve Privacy and Security. In: Proceedings of the IEEE Symposium on Security and Privacy. IEEE (2015), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7163025

A Appendix

A.1 Additional Figures



(a) North America (Local). (b) Asia (Local). (c) Europe (Local).

Fig. 5: *Resolvers measured from local vantage points (including mainstream resolvers). These plots do not truncate response times at 500 ms.*

A.2 Resolvers

– https://dns.google/dns-query
– https://dns.aa.net.uk/dns-query
– https://adfree.usableprivacy.net/dns-query
– https://dns.adguard.com/dns-query
– https://dns-family.adguard.com/dns-query
– https://doh.in.ahadns.net/dns-query
– https://doh.la.ahadns.net/dns-query
– https://doh.nl.ahadns.net/dns-query
– https://dns.alidns.com/dns-query
– https://dnsnl-noads.alekberg.net/dns-query
– https://dnsnl.alekberg.net/dns-query

– https://dns.arapurayil.com/dns-query
– https://dohtrial.att.net/dns-query
– https://dnses.alekberg.net/dns-query
– https://doh.bortzmeyer.fr/dns-query
– https://dns.circl.lu/dns-query
– https://doh.opendns.com/dns-query
– https://dns.cloudflare.com/dns-query
– https://family.cloudflare-dns.com/dns-query
– https://security.cloudflare-dns.com/dns-query
– https://odvr.nic.cz/dns-query
– https://dns.digitale-gesellschaft.ch/dns-query
– https://dns.digitale-gesellschaft.ch/dns-query
– https://dns1.ryan-palmer.com/dns-query
– https://doh.sb/dns-query
– https://dns.therifleman.name/dns-query
– https://dns1.dnscrypt.ca/dns-query
– https://dns2.dnscrypt.ca/dns-query
– https://dns-doh.dnsforfamily.com/dns-query
– https://dns-doh-no-safe-search.dnsforfamily.com/dns-query
– https://dnsforge.de/dns-query
– https://dns.dnshome.de/dns-query
– https://doh.pub/dns-query
– https://doh-ch.blahdns.com/dns-query
– https://doh.cleanbrowsing.org/dns-query
– https://doh.cleanbrowsing.org/dns-query
– https://doh.cleanbrowsing.org/dns-query
– https://doh.crypto.sx/dns-query
– https://doh-de.blahdns.com/dns-query
– https://doh-fi.blahdns.com/dns-query
– https://ibksturm.synology.me/dns-query
– https://doh-jp.blahdns.com/dns-query
– https://doh-sg.blahdns.com/dns-query
– https://doh.appliedprivacy.net/dns-query
– https://doh.ffmuc.net/dns-query
– https://doh.tiarap.org/dns-query
– https://ordns.he.net/dns-query
– https://doh.tiar.app/dns-query

- https://public.dns.iij.jp/dns-query
- https://doh.this.web.id/dns-query
- https://jp.tiar.app/dns-query
- https://jp.tiarap.org/dns-query
- https://doh.libredns.gr/dns-query
- https://doh.libredns.gr/dns-query
- https://doh.linuxsec.org/dns-query
- https://doh.linuxsec.org/dns-query
- https://adblock.doh.mullvad.net/dns-query
- https://doh.chewbacca.meganerd.nl/dns-query
- https://doh.mullvad.net/dns-query
- https://dns.nextdns.io/dns-query
- https://dns.njal.la/dns-query
- https://doh.post-factum.tk/dns-query
- https://draco.plan9-ns2.com/dns-query
- https://doh.powerdns.org/dns-query
- https://doh.seby.io/dns-query
- https://doh-2.seby.io/dns-query
- https://dns.twnic.tw/dns-query
- https://dns9.quad9.net/dns-query
- https://dns9.quad9.net/dns-query
- https://dnsse.alekberg.net/dns-query
- https://dns.switch.ch/dns-query
- https://dns.t53.de/dns-query
- https://unicast.uncensoreddns.org/dns-query
- https://anycast.uncensoreddns.org/dns-query
- https://sg.yepdns.com/dns-query
- https://doh.xfinity.com/dns-query