DNS Privacy with Speed? Evaluating DNS over QUIC and its Impact on Web Performance

Mike Kosek
Technical University of Munich
kosek@in.tum.de

Luca Schumann
Technical University of Munich
schumann@in.tum.de

Robin Marx
KU Leuven
robin.marx@uhasselt.be

Trinh Viet Doan
Technical University of Munich
doan@in.tum.de

Vaibhav Bajpai
CISPA Helmholtz Center for
Information Security
bajpai@cispa.de

ABSTRACT

Over the last decade, Web traffic has significantly shifted towards HTTPS due to an increased awareness for privacy. However, DNS traffic is still largely unencrypted, which allows user profiles to be derived from plaintext DNS queries. While DNS over TLS (DoT) and DNS over HTTPS (DoH) address this problem by leveraging transport encryption for DNS, both protocols are constrained by the underlying transport (TCP) and encryption (TLS) protocols, requiring multiple round-trips to establish a secure connection. In contrast, QUIC combines the transport and cryptographic handshake into a single round-trip, which allows the recently standardized DNS over QUIC (DoQ) to provide DNS privacy with minimal latency. In the first study of its kind, we perform distributed DoQ measurements across multiple vantage points to evaluate the impact of DoQ on Web performance. We find that DoQ excels over DoH, leading to significant improvements with up to 10% faster loads for simple webpages. With increasing complexity of webpages, DoQ even catches up to DNS over UDP (DoUDP) as the cost of encryption amortizes: With DoQ being only ~2% slower than DoUDP, encrypted DNS becomes much more appealing for the Web.

CCS CONCEPTS

• **Networks** → **Network measurement**; *Transport protocols*;

KEYWORDS

DNS Privacy, DNS over QUIC, Web Performance

ACM Reference Format:
Mike Kosek, Luca Schumann, Robin Marx, Trinh Viet Doan, and Vaibhav Bajpai. 2022. DNS Privacy with Speed? Evaluating DNS over QUIC and its Impact on Web Performance. In *Proceedings of the 22nd ACM Internet Measurement Conference (IMC '22), October 25–27, 2022, Nice, France.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3517745.3561445

1 INTRODUCTION

Led by the increased awareness for Internet security and privacy, HTTPS has replaced HTTP and became the default Web protocol over the last decade [6, 54]. However, despite the DNS being one of the most crucial parts of the Internet infrastructure, unencrypted DNS traffic using DNS over UDP (DoUDP) and DNS over TCP (DoTCP) is still the norm [11]. Hence, even with the encryption of the actual Web content, browsing behaviors and user profiles can still be derived and even tracked by observing unencrypted DNS queries [32, 33, 39, 56]. This problem was originally addressed by the encrypted protocols DNS over TLS (DoT) [24] and DNS over HTTPS (DoH) [21], which have been integrated by browsers and public DNS resolvers since 2016 [9, 12, 16, 17]. As these protocols have been extensively studied in terms of response times [5, 8, 23, 40, 40, 53] and impact on Web performance [4, 5, 22], it has become clear that both DoT and DoH are constrained by the round-trips required for the handshakes of the underlying transport (TCP) and encryption (TLS) protocols.

To overcome these limitations, the QUIC transport protocol [29], standardized in 2021, combines the transport and cryptographic handshake into a single round-trip. Consequently, DNS over QUIC (DoQ) [25] aims to provide DNS privacy with minimal latency. While it was only recently standardized in May 2022, DoQ is already deployed by privacy-focused DNS resolvers in production systems [1, 44]. However, as of September 2022, only one study focusing on DoQ exists: In our preliminary work, we compared DNS protocol performance measured from a single vantage point [37]. We showed that the adoption of DoQ by public DNS resolvers is slowly increasing and that although DoQ outperforms DoT and DoH in terms of DNS *single query response time*, around 40% of measurements still result in considerably slower response times than expected due to the enforcement of QUIC's traffic amplification limit [29].

To advance this state of the art, we (1) perform distributed measurements across 6 vantage points and (2) add support for TLS 1.3 `Session Resumption` and `0-RTT` for DoQ, DoT, and DoH. While we find that no public resolver supports `0-RTT`, our measurements are not constrained by QUIC's traffic amplification limit due to `Session Resumption`, which can therefore significantly improve the *single query response time*: DoQ outperforms DoT and DoH by ~33%, making encrypted DNS much faster. We further conduct *Web performance* measurements to analyze and compare the impact of DoQ on Web browsing. In our distributed measurements, we find

---

IMC '22, October 25–27, 2022, Nice, France

ACM ISBN 978-1-4503-9259-4/22/10…$15.00
https://doi.org/10.1145/3517745.3561445

that DoQ significantly improves over DoH by up to 10% faster loads for simple webpages. With increasing complexity of webpages, DoQ even catches up to DoUDP as the cost of encryption amortizes the more DNS queries are required for loading a webpage: with DoQ being only ~2% slower than DoUDP, encrypted DNS becomes much more appealing for the Web.

2 METHODOLOGY

To study the response times of DoQ in comparison to DoUDP, DoTCP, DoT, and DoH for single queries and assess their impact on Web performance, we issue distributed measurements using 6 vantage points while targeting 313 DNS resolvers worldwide.

Target Resolvers and Vantage Points. To identify DoQ resolvers, we issue a scan of the IPv4 address space in week 14 of 2022 from a single vantage point located in the research network of the Technical University of Munich, Germany, targeting all proposed DoQ ports (`UDP 784`, `853`, and `8853` [25, 26]). For this, we leverage the *ZMap* [57] network scanner, probing with a QUIC `INITIAL` packet with an invalid version number of 0: By receiving a `Version Negotiation` packet in response, we identify the IP addresses that support QUIC on the respective port, without creating state on the target [29] to avoid exhausting resources. We then establish a connection to the identified targets, offering the DoQ Application-Layer Protocol Negotiation (ALPN) identifiers [25, 26]; if the connection establishment is successful, the target is identified to support DoQ [20].

Using this methodology, we identify 1,216 DoQ resolvers. Comparing this finding with our preliminary work, which identified 1,217 DoQ resolvers in week 03 of 2022 [37], we observe that the adoption of DoQ is currently stagnating. To enable a comparison of DoQ to the established DNS protocols, we further check the identified DoQ resolvers for their support of DoUDP, DoTCP, DoT, and DoH. For this, we optimistically query the resolvers using *DNSPerf*, an open-source DNS measurement tool supporting all stated protocols [19]. Of the 1,216 identified DoQ resolvers, we find that 548 support DoUDP, 706 DoTCP, 1,149 DoT, and 732 DoH, while their full intersection (i.e, resolvers supporting every DNS protocol) results in 313 verified DoX resolvers (preliminary work: 264 [37]). While we acknowledge that public DNS resolvers often leverage IP anycast, we cross-reference anycast IP addresses used in related work [4, 8, 22, 36, 40, 53], although without finding an overlap. Fig. 1 (red dots) presents the geographical distribution of the verified DoX resolvers based on an IPv4 geolocation lookup service [27], for which we observe that the majority are located in Europe (EU) with 130 resolvers, followed by Asia (AS) with 128, North America (NA) with 49, and Africa (AF), Oceania (OC), and South America (SA) with 2 resolvers each. Moreover, we find that the resolvers are distributed over 107 Autonomous Systems, with the majority located in ORACLE (47, 15.0%), DIGITALOCEAN (20, 6.4%), MNGTNET (18, 5.8%), and OVHCLOUD (16, 5.1%). The remaining Autonomous Systems each host 12 or less resolvers. All measurements are performed using 6 distributed *Amazon EC2* instances (Fig. 1, blue dots), employing one vantage point per continent.

Single Query Response Time and Size. To study the single query response times and sizes of DoQ in comparison to DoUDP, DoTCP, DoT, and DoH, we leverage the open-source DNS measurement tool *DNSPerf* [19]. Targeting the 313 verified DoX resolvers, we issue *single query* measurements for all stated protocols on every vantage point, repeated every 2 hours, over the course of week 16 of 2022. For this, an `A` record for `google.com` is queried. We precede every measurement with an identical cache warming query to ensure that the following *actual* measurement is directly answered from a cached record at the resolver, which avoids inconsistencies in the measured response times caused by recursive lookups. This further allows us to reuse the TLS session parameters of the cache warming for the *actual* measurement of DoQ, DoT, and DoH: By adding support for TLS 1.3 `Session Resumption` and `0-RTT` to *DNSPerf*, we advance the state of the art of our preliminary work [37] (which does not consider either feature) and by default use both mechanisms if supported by the resolver. Additionally, we also store the negotiated `QUIC Version` as well as the `Address Validation` token received in a `New_Token` frame of the cache warming query. Reusing these in the QUIC `INITIAL` packet of the *actual* DoQ measurement ensures that the QUIC handshake is not influenced by its `Version Negotiation` or `Address Validation` mechanisms, which would otherwise add 1 RTT each [37]. Hence, our DoQ implementation follows the recommendations of the DoQ standard, stating that `Address Validation` tokens should only be used in union with `Session Resumption` [25]. Altogether, our methodology enables comparable response time measurements of a typical DNS usage scenario for all protocols for the first time, where a session between a client and a resolver is established to perform a single DNS query.

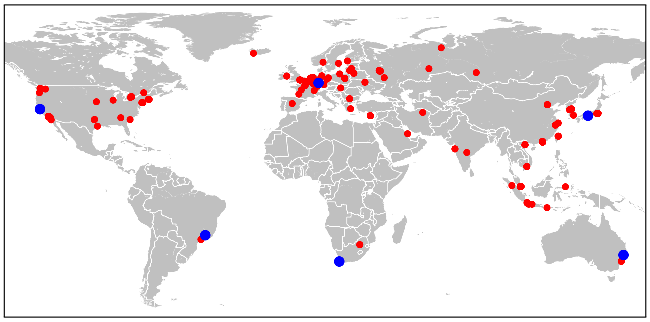


Figure 1: Geographical distribution of the 313 verified DoX resolvers (red dots) and vantage points (blue dots).

Web Performance. To assess the impact of DoQ on Web performance in comparison to DoUDP, DoTCP, DoT, and DoH, we develop an open-source framework using *Selenium* [51], *Chromium* [47], as well as *DNS Proxy* [14]. Using this framework, we issue Web performance measurements targeting the top 10 most popular webpages from the research-oriented *Tranco* top list [46] as of April 12, 2022. For this, we load every webpage using each DNS protocol via every one of the 313 verified DoX upstream resolvers from all vantage points, repeated every 48 hours, over the course of week 16 of 2022. For each measurement, *DNS Proxy* is newly setup as Chromium's local resolver on the *Amazon EC2* instances and configured to forward the queries to the upstream DoX resolver by using either DoQ, DoUDP, DoTCP, DoT, or DoH. The local DNS caches of both the operating system and *DNS Proxy* are disabled to ensure that queries are forwarded to the configured upstream resolver. In the next step, we leverage *Selenium* to launch *Chromium* and navigate to each webpage twice in succession: As with the DNS *single query*, the first navigation populates the upstream resolver's cache and ensures that the DNS queries of the second, *actual* measurement navigation are directly answered from that resolver's cache. As with *DNSPerf*, we extend *DNS Proxy* to support TLS 1.3 `Session Resumption` and `0-RTT`, and track the negotiated QUIC versions and tokens. As such, this approach is identical to the aforementioned *single query* measurements, following the recommendations of the DoQ standard [25]. After the cache warming navigation, all sessions of *DNS Proxy* are reset to ensure that a new session to the resolver is established for the *actual* Web performance measurement, where TLS `Session Resumption` and `0-RTT` are used if supported by the DoX resolver. Overall, this methodology allows us to compare DoQ with DoUDP, DoTCP, DoT, and DoH regarding their impact on Web performance for the first time, representing a typical usage scenario in which multiple DNS queries are sent when visiting a webpage.

Ethical Considerations. To adhere to ethical principles and minimize the impact of our measurements, we respectfully follow best practices of the Internet measurement community [13, 45]: We restrict our Internet-wide scans for the verification of DoX resolvers to one week and one vantage point in order to limit the traffic sent to the network operators' infrastructure. To allow targets to opt-out from our measurements, we display contact information and a description about the intent of our measurements on a webpage reachable via the IP address of each vantage point. Further, we only target publicly reachable IP addresses and exclude targets based on a blocklist which is maintained across research groups within our University, and, therefore, also covers targets excluded from previous measurement studies.

Reproducibility and Community Contributions. In order to enable the reproduction of our findings [2], we make the developed tools, the raw data of our measurements, and the analysis scripts publicly available [34]. Moreover, we upstream our changes to the tools used in our measurements as outlined in this chapter, aiming to facilitate future DNS protocol studies [15, 30, 31, 35].

3 EVALUATION

We begin the evaluation with an overview of the measurements, followed by the analysis of the *single query* measurements in § 3.1. In § 3.2, we detail our findings on the impact of DoQ on *Web performance* in comparison to DoUDP, DoTCP, DoT, and DoH.

Analyzing DoQ, we find that 89.1% of all measurements are performed using QUIC version `1`. The remaining measurements use the older QUIC `draft` versions `-34` (8.5%), `-32` (1.8%), and `-29` (0.6%). We find no differences between the QUIC versions, which confirms our expectations, as all observed versions are feature equivalent. While our tooling supports all available DoQ versions as of April 18, 2022 (*doq* for the standard [25], as well as *doq-i00* to *doq-i11* for the `draft` versions), we find that *doq-i02* is used in the majority of measurements with 87.4%, followed by *doq-i03* with 10.8%, and *doq-i00* with 1.8%. While the observed versions *doq-i00* and *doq-i02* are feature equivalent, *doq-i03* changed the QUIC stream mapping to include a 2 byte message length field in order to permit multiple responses for a single query. As with QUIC, however, we find no differences between DoQ versions. All DoQ measurements use TLS 1.3 as mandated by the QUIC standard [52]. As for DoT and DoH, around 99% of measurements are performed using TLS 1.3, whereas the remainder use TLS 1.2. Moreover, all DoH measurements use HTTP/2. For both the QUIC-based DoQ and the TCP-based DoH and DoT, we find that no resolver supports TLS 1.3 `0-RTT`. However, all resolvers support TLS 1.3 `Session Resumption` and respond with the maximum session ticket lifetime of 7 days as defined by the standard [48]; hence, `Session Resumption` is used in all TLS 1.3 measurements. Lastly, we find that no resolver supports `TCP Fast Open` (TFO) [7] or `edns-tcp-keepalive` [55].

Table 1: Median single query sizes in bytes, as well as sample sizes of single query response time and Web performance measurements.

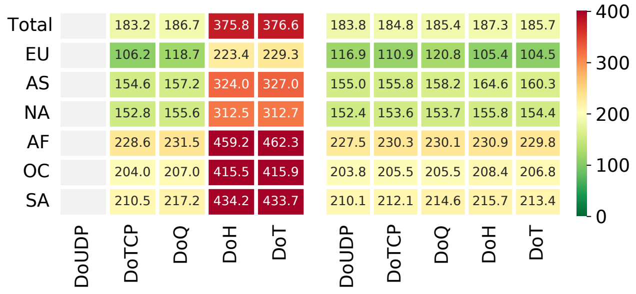
	DoUDP	DoTCP	DoQ	DoH	DoT
Single Query Sizes (median IP payload in bytes)					
— Total	122	382	4444	2163	1522
— Handshake C->R	—	72	2564	569	551
— Handshake R->C	—	40	1304	211	211
— DNS Query	59	149	190	579	261
— DNS Response	63	121	386	804	499
Single Query Response Time					
— Samples	154,092	154,503	159,676	157,637	158,959
Web Performance					
— Samples	57,032	56,428	57,393	56,840	56,440

3.1 Single Query Response Time and Size

The *single query* measurements reflect a typical DNS usage scenario, where a session between a client and a resolver is established in order to perform a single DNS query. Table 1 presents the sample sizes for the *single query* measurements, where we observe slight variations due to resolvers not responding to every DNS query. In our analysis, we differentiate between the *handshake time*, the *resolve time*, and the *sizes* to account for the different transport protocol mechanisms used by the measured protocols.

Handshake time. We define the *handshake time* as the time between the client sending the first packet of the transport protocol handshake until the (encrypted) session to the resolver is established. Thus, DoUDP is excluded from this analysis since UDP is connectionless. As no resolver supports TFO (see § 3), the DoTCP handshake is expected to complete within 1 round-trip due to the TCP 3-way handshake. For the encrypted protocols DoQ, DoH, and DoT, we find that no resolver supports `0-RTT`, but all resolvers support `Session Resumption` (see § 3). Hence, the DoQ handshake is also expected to complete within 1 round-trip due to QUIC's combination of the transport and encryption handshake. Because DoH and DoT leverage TCP and no resolver supports TFO, the transport and encryption handshake is expected to take 2 round-trips when TLS 1.3 is used (around 99% of measurements, see § 3), and 3 round-trips in case of TLS 1.2.

The median *handshake times* in ms per protocol and vantage point are presented in Fig. 2a. We find that both DoH and DoT show comparable *handshake times* as expected, with the median over all vantage points (*Total*, top row) being ~376ms for DoH



	DoUDP	DoTCP	DoQ	DoH	DoT
Total		183.2	186.7	375.8	376.6
EU		106.2	118.7	223.4	229.3
AS		154.6	157.2	324.0	327.0
NA		152.8	155.6	312.5	312.7
AF		228.6	231.5	459.2	462.3
OC		204.0	207.0	415.5	415.9
SA		210.5	217.2	434.2	433.7

	DoUDP	DoTCP	DoQ	DoH	DoT
Total	183.8	184.8	185.4	187.3	185.7
EU	116.9	110.9	120.8	105.4	104.5
AS	155.0	155.8	158.2	164.6	160.3
NA	152.4	153.6	153.7	155.8	154.4
AF	227.5	230.3	230.1	230.9	229.8
OC	203.8	205.5	205.5	208.4	206.8
SA	210.1	212.1	214.6	215.7	213.4

(a) ***Handshake time.*** **(b)** ***Resolve time.***

Figure 2: Median *Handshake time* (a, left) and *Resolve time* (b, right) in ms per protocol over all vantage points (top row) and per vantage point (bottom rows). Ordered by the number of verified DoX resolvers per continent.

and ~377ms for DoT. In comparison, both DoTCP and DoQ result in roughly half of that with ~183ms for DoTCP and ~187ms for DoQ, again confirming our expectations. While our preliminary work [37] found the *handshake times* of DoQ to be considerably slower in comparison to DoTCP, this was due to DoQ being limited by QUIC's traffic amplification limit: The handshake is prolonged by 1 round-trip if the X.509 certificate offered by the resolver does not fit into the traffic amplification limit of three times the amount of data the resolver received in the `INITIAL` from the client (at least 1,200 bytes, see *Sizes* in § 3.1). In contrast, the measurements presented are not constrained by this limit due to the usage of `Session Resumption` (see § 2), where the X.509 server certificate is not exchanged yet again.

Resolve time. We define the *resolve time* as the time between the client sending the first packet of the DNS query until a valid DNS response is received. As we ensure that the queried DNS record is cached on the target resolver (see § 2), the *resolve times* are expected to be similar for all measured protocols if the protocols are handled equally by the path.

The median *resolve times* in ms per protocol and vantage point are presented in Fig. 2b, where we find that all protocols indeed result in fairly similar *resolve times* on each vantage point (i.e., row-wise), and also over all vantage points (*Total*, top row). Moreover, we observe that the *resolve times* correlate with the locations of the vantage points and resolvers (see Fig. 1): While AF, OC, and SA host only 2 resolvers each (bottom rows), we observe the highest median *resolve times* on these vantage points due to larger geographical distances to the targeted resolvers. In turn, AS (128 resolvers) and NA (49 resolvers) show significantly faster median *resolve times*, only being outperformed by EU where we find the highest geographical density of DoQ resolvers (130 resolvers).

Sizes. There is a secondary general performance axis besides response times, namely size overhead. While DoUDP adds just a few 8-byte UDP packet headers, DoQ incurs a heavy cost due to its modern handshake. Table 1 shows the median incoming/outgoing IP payload bytes per protocol for a single `A` query for `google.com` to all DoX resolvers (using `Session Resumption` where possible), split over the handshake (Client->Resolver and vice versa) and actual DNS query/response.

We find that the encrypted protocols indeed transfer significantly more bytes than DoUDP and DoTCP. The bytes transferred for a single DoQ handshake then again more than doubles in comparison to DoH and DoT, as QUIC requires all its `INITIAL`-carrying datagrams to be padded to at least 1,200 bytes to ensure MTU allowance on the network [29]. However, DoQ's query and response sizes are relatively small in comparison to DoH due to the HTTP/2 overhead of DoH, e.g., message framing and header compression setup. Hence, our results indicate that re-using a QUIC connection for multiple queries will mitigate its up-front cost faster than DoH.

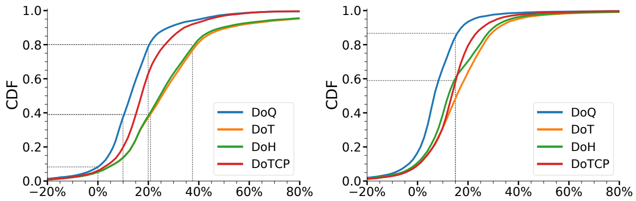
Takeaway: *Our findings on single query response time and size emphasize the importance of standards and their implementations:* `Session Resumption` *can significantly catalyze DoQ, outperforming DoT and DoH by ~33%. Hence, DoQ makes encrypted DNS much more appealing than DoH, where DoQ falls short of DoUDP by only ~50% (DoT and DoH: ~66%) for single queries. Consequently, DoQ's roughly double handshake size overhead over DoH seems a small price to pay.*

3.2 Web Performance

Applying our methodology of the *single query* measurements to *DNS Proxy* (see § 2), we issue *Web performance* measurements targeting the top 10 most popular webpages from the *Tranco* list [46]. To avoid initial redirects to the actual landing page (i.e., *google.com* will redirect to *www.google.com*), we replace the URLs by the actual landing page to ensure comparable results. Representing a typical usage scenario where multiple DNS queries are sent when visiting a webpage, we analyze two standard Web performance metrics: *First Contentful Paint* (FCP) and *Page Load Time* (PLT). FCP marks the moment when the very first visible image or text is shown on the screen [42]. For PLT, we calculate the time difference between the very start of the page load (corresponding to the start of the first DNS query/connection) and the `onLoad` event (corresponding to the moment when the webpage has finished loading), i.e., `LoadEventStart−NavigationStart` [43]. FCP occurs early in the page load and, thus, should be more impacted by the DNS response times than PLT, which occurs late and is influenced by many other Web performance aspects. Table 1 presents the sample sizes for the *Web performance* measurements, where we again observe slight variations due to resolvers not responding to every DNS query.

For each `[vantage point:resolver:DNS protocol]` combination, we perform four measurements using cold start page loads for every webpage. We determine the medians of these measurements, enabling the comparison of upstream resolvers with different response times (i.e., to account for different geographical distances of vantage point and resolver, see § 2). We then compare the per-protocol medians corresponding to a pair of `[vantage point:resolver]` to each other. The relative differences to DoUDP (baseline) are shown in Fig. 3.

FCP. In almost 40% of cases, using DoQ (Fig. 3a, blue line) delays the FCP by 10% or less when compared to DoUDP. On the other hand, DoT (orange line) and DoH (green line) delay it by more than 20% for the same fraction. Looking at the 80th percentile, in 20% of cases the FCP increases by more than 20% with DoQ, and almost



(a) ***First Contentful Paint*** **(b)** ***Page Load Time***

Figure 3: CDFs of the relative differences in FCP and PLT between DNS protocols with DoUDP as baseline.

twice as much with DoH. In summary, DoQ performs much better than DoH and DoT when comparing the FCP timings.

While both DoQ and DoTCP utilize a 1 round-trip connection setup (see § 3.1), we find that DoTCP is considerably slower than DoQ (Fig. 3a, red and blue lines). Given that no resolver supports `edns-tcp-keepalive` or TFO (see § 3), DoTCP initiates a new connection for every query. Hence, no resolver follows the recommendations for DoTCP [38] and each query takes 2 round-trips regardless of a previous connection establishment with the resolver.

In almost 10% of cases, we find that the FCP occurs faster when using DNS protocols other than DoUDP. Analyzing this observation, we find that DoUDP is skewed by outliers: While both TCP and QUIC offer transport layer retransmission with initial timeouts of 1 second [28, 49], DoUDP is dependent on *Chromium* retransmitting the DNS query on the application layer which uses a default initial timeout of 5 seconds [41].

PLT. The PLT presented in Fig. 3b confirms our expectations that the relative impact of the DNS protocol is lower for PLT than for the FCP. Overall, DoQ (blue line) shows the smallest degradation in comparison to DoUDP, where less than 15% of page loads increase the PLT by more than 15%. In contrast, for more than 40% of DoH page loads, the PLT also increases by more than 15% (green line). We find that the vast majority of the DoH worst cases result from *wikipedia.org*, *linkedin.com*, and *instagram.com*; since those pages load very fast (due to the landing page mainly consisting of a login or search form), the impact of the DNS protocol on PLT can still be relatively large.

Analyzing DoT (orange line), we find that it performs worse than DoH (green line). While both protocols are expected to re-use previously established connections for subsequent DNS queries independent of the support of `edns-tcp-keepalive` [21, 24], a root cause analysis revealed that the connection handling in *DNS Proxy* results in DoT repeating the full transport and encryption handshake in almost 60% of page loads: While a DoT query is currently in-flight and a new request is issued, *DNS Proxy* opens a new connection instead of re-using the existing one. Hence, we disregard DoT in the following discussion and address this issue as part of our community contributions (see § 2).

DoQ vs. DoH. We now take a closer look at DoQ and DoH to evaluate the performance differences of the encrypted DNS protocols in more detail. For this, we analyze the impact of the vantage point and webpage on PLT, where we present the relative differences between DoQ (horizontal baseline) and DoH (green line) in Fig. 4. Webpages are sorted from left to right by the average number of DNS queries required for loading each webpage (see columns); a lighter background color depicts a higher percentage of DoQ page loads being faster than DoH.

Overall, we find that DoQ mostly improves on DoH in all vantage point and webpage combinations, where the performance improvement diminishes the more DNS queries are required for loading a webpage (from left to right). Analyzing the more simple webpages *wikipedia.org* and *instagram.com*, we observe that DoQ improves the PLT over DoH by up to 10% in the median. Hence, the simple webpages profit the most from DoQ's 1 round-trip connection establishment (see § 3.1), as there is only one DNS query on average.

Analyzing the differences between vantage points, we find that EU shows the smallest differences between DoQ and DoH (top row). Since we also observed the lowest response times on that vantage point (see § 3.1), we suspect that lower response times result in a smaller influence of the DNS protocol on the PLT. We find that the other vantage points also align in that trend, where DoQ positively impacts the performance more often when the response times are larger. Nonetheless, we can already see an effect even with moderate response times, e.g., in around 50% of measurements, *linkedin.com* is more than 10% faster with DoQ than with DoH in AS. However, we cannot determine a linear correlation between DNS protocol and PLT.

DoQ vs. DoUDP. Because unencrypted DNS traffic is still the norm, we next analyze the performance difference between DoQ and DoUDP (Fig. 4, horizontal baseline and purple line). Expectedly, DoUDP shows a better performance than DoQ in almost every case. However, we also find DoUDP being slower than DoQ in some cases in the long tail, which is more pronounced in EU (top row) as well as for webpages with a higher number of DNS queries. As discussed for *FCP*, we attribute this observation to DoUDP being skewed by outliers due to application layer retransmissions.

For the more simple webpages *wikipedia.org* and *instagram.com*, we find that the performance cost of encryption is the largest with up to 10% slower PLT in the median due to the added overhead of DoQ's connection establishment. However, we find that the difference in PLT is reduced to only ~2% in the median between DoQ and DoUDP for the more complex webpages *microsoft.com* and *youtube.com*: DoQ even catches up to DoUDP as the encryption overhead amortizes the more DNS queries are required for loading a webpage.

Takeaway: *DoQ significantly improves over DoH. While we find that page loads using DoQ are up to 10% faster for simple webpages in comparison to DoH, the cost of encryption is the largest for the same webpages, where DoQ is up to 10% slower than DoUDP. With increasing complexity of webpages, however, DoQ catches up to DoUDP as the cost of encryption amortizes the more DNS queries are required for loading a webpage: DoQ is only ~2% slower than DoUDP, thus, making encrypted DNS much more appealing for the Web.*

4 LIMITATIONS AND FUTURE WORK

Limitations. Note that the Web performance measurements only consider a total number of 10 webpages, which might not be representative for the Web as a whole; with an increased number of requests per page and increased webpage complexity, the benefits of DoQ in comparison to DoH (e.g., fewer round-trips required for

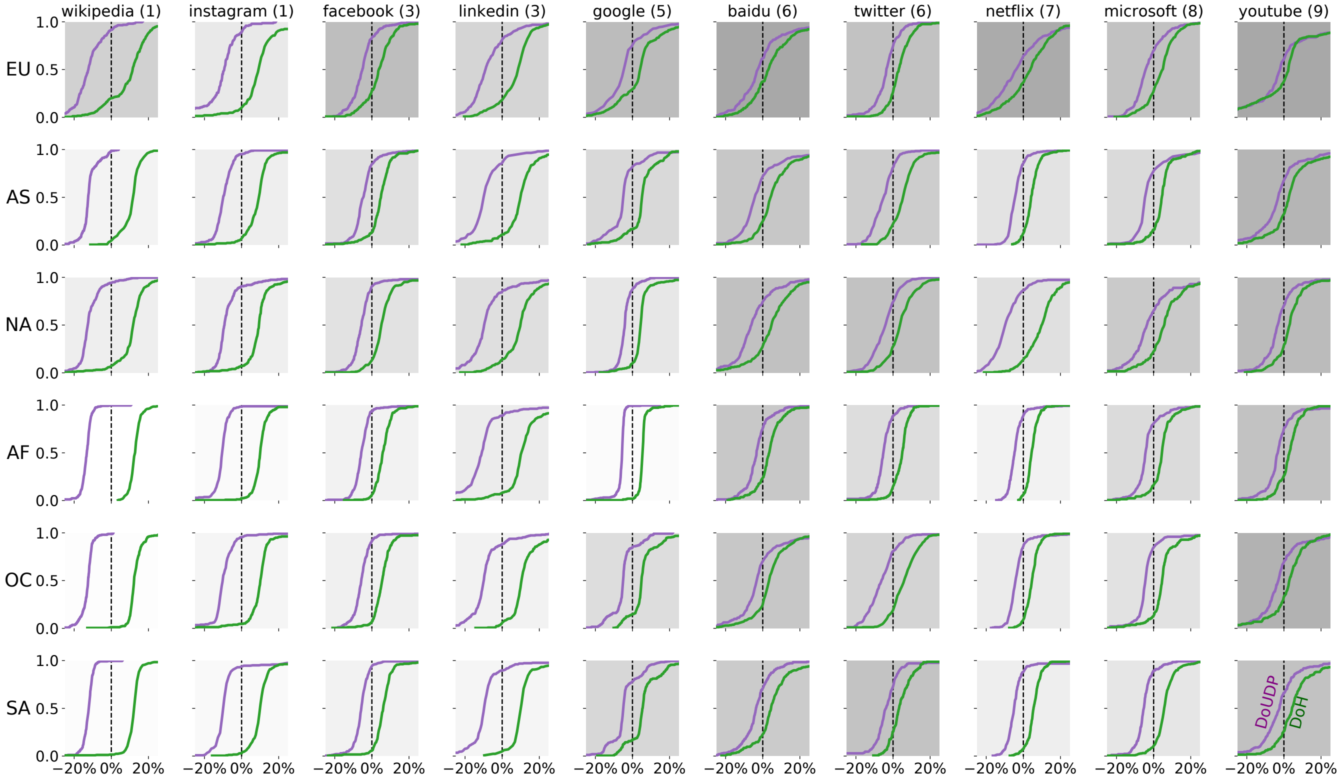


Figure 4: CDFs of the relative differences in PLT between DoQ (horizontal baseline), DoUDP (purple line), and DoH (green line), grouped by vantage point and webpage. A lighter background color depicts a higher percentage of DoQ page loads being faster than DoH. Sorted from left to right by the average number of DNS queries required for loading each webpage (in brackets) and from top to bottom by the number of verified DoX resolvers per continent.

the handshake) are diminished due to amortization and other confounding factors such as webpage rendering. Further, considering the limited number of 313 DoX resolvers which are heavily centered around Europe, some vantage points experience higher latency due to larger geographical distances to the targeted resolvers. While we briefly discuss resulting outliers in the previous sections, a detailed root cause analysis, esp. for the Web performance measurements, is left for future work.

Future Work. With the ongoing development and adoption of DoQ among resolvers, we expect resolvers to introduce support for 0-RTT in the future, which can shift the total response times of DoQ even closer to DoUDP. Thus, we plan to continue measuring and monitoring the rollout of DoQ. Moreover, while the DoH measurements in our study use HTTP/2 (see § 3), we will extend our work with an in-depth comparison to DNS over HTTP/3 (DoH3): The recently standardized HTTP/3 [3] also uses QUIC as its transport protocol. At the time of writing, DoH3 is not yet widely supported: While Cloudflare is one of the first to support DoH3 [10] by including HTTP/3 in the ALPN set of their `SVCB` records [50], we observe that state of the art browsers only connect to Cloudflare's resolvers via HTTP/2, which indicates that DoH3 support among browsers is still lacking. However, with its recent integration into Google Public DNS and Android [18], DoH3 is expected to gain momentum in the coming months.

5 CONCLUSION

Our study showed that encrypted DNS does not have to be a compromise between privacy and speed: Using DoQ, the single query response time is improved by ~33% in comparison to DoT and DoH. The Web performance measurements revealed that DoQ significantly improves over DoH with up to 10% faster loads for simple webpages. With increasing complexity of webpages, DoQ even catches up to DoUDP as the cost of encryption amortizes: With DoQ being only ~2% slower than DoUDP, encrypted DNS becomes much more appealing for the Web, especially once resolvers start supporting advanced features such as 0-RTT.

ACKNOWLEDGEMENTS

We thank Justus Fries, Sebastian Kappes, and Malte Granderath for their valuable support, as well as Jan Rüth, the anonymous reviewers, and our shepherd Stephen McQuistin for their insightful feedback. This work was partly supported by the Volkswagenstiftung Niedersächsisches Vorab (Funding No. ZN3695).

REFERENCES

[1] AdGuard. 2020. AdGuard DNS-over-QUIC. (2020). https://adguard.com/en/blog/dns-over-quic.html [Online; accessed 2022-Sep-18].

[2] Vaibhav Bajpai et al. 2019. The Dagstuhl Beginners Guide to Reproducibility for Experimental Networking Research. *SIGCOMM Comput. Commun. Rev.* 49, 1 (Feb. 2019). https://doi.org/10.1145/3314212.3314217

[3] Mike Bishop. 2022. HTTP/3. RFC 9114. (2022). https://doi.org/10.17487/RFC9114

[4] Kevin Borgolte et al. 2019. How DNS over HTTPS is Reshaping Privacy, Performance, and Policy in the Internet Ecosystem. In *TPRC47 2019*. https://doi.org/10.2139/ssrn.3427563

[5] Timm Böttger et al. 2019. An Empirical Study of the Cost of DNS-over-HTTPS. In *IMC 2019*. https://doi.org/10.1145/3355369.3355575

[6] Chia-ling Chan et al. 2018. Monitoring TLS adoption using backbone and edge traffic. In *IEEE INFOCOM 2018*. https://doi.org/10.1109/INFCOMW.2018.8406957

[7] Yuchung Cheng, Jerry Chu, Sivasankar Radhakrishnan, and Arvind Jain. 2014. TCP Fast Open. RFC 7413. (2014). https://doi.org/10.17487/RFC7413

[8] Rishabh Chhabra et al. 2021. Measuring DNS-over-HTTPS Performance around the World. In *IMC 2021*. https://doi.org/10.1145/3487552.3487849

[9] Cloudflare. 2018. Introducing DNS Resolver, 1.1.1.1. (2018). https://blog.cloudflare.com/dns-resolver-1-1-1-1/ [Online; accessed 2022-Sep-18].

[10] Cloudflare. 2022. Cloudflare Blog: Announcing experimental DDR in 1.1.1.1. (2022). https://blog.cloudflare.com/announcing-ddr-support/ [Online; accessed 2022-Sep-18].

[11] Casey Deccio and Jacob Davis. 2019. DNS Privacy in Practice and Preparation. In *CoNEXT 2019*. https://doi.org/10.1145/3359989.3365435

[12] DNS Privacy Project. 2022. Public Resolvers. (2022). https://dnsprivacy.org/public_resolvers/ [Online; accessed 2022-Sep-18].

[13] Zakir Durumeric et al. 2013. ZMap: Fast Internet-Wide Scanning and Its Security Applications. In *USENIX 2013*. https://dl.acm.org/doi/10.5555/2534766.2534818

[14] Justus Fries. 2022. DNS Proxy. (2022). https://github.com/justus237/dnsproxy [Online; accessed 2022-Sep-18].

[15] Justus Fries. 2022. DNS Proxy Pull Request Session Resumption and 0-RTT. (2022). https://github.com/AdguardTeam/dnsproxy/pull/268 [Online; accessed 2022-Sep-18].

[16] Google. 2016. Google Public DNS now offers DNS-over-HTTPS. (2016). https://groups.google.com/g/public-dns-announce/c/p2iYauFuzIg [Online; accessed 2022-Sep-18].

[17] Google. 2019. Google Public DNS now supports DNS-over-TLS. (2019). https://security.googleblog.com/2019/01/google-public-dns-now-supports-dns-over.html [Online; accessed 2022-Sep-18].

[18] Google. 2022. DNS-over-HTTP/3 in Android. (2022). https://security.googleblog.com/2022/07/dns-over-http3-in-android.html [Online; accessed 2022-Sep-18].

[19] Malte Granderath. 2022. DNSPerf. (2022). https://github.com/mgranderath/dnsperf [Online; accessed 2022-Sep-18].

[20] Malte Granderath. 2022. Verify DoQ. (2022). https://github.com/mgranderath/verify-doq [Online; accessed 2022-Sep-18].

[21] Paul E. Hoffman and Patrick McManus. 2018. DNS Queries over HTTPS (DoH). RFC 8484. (2018). https://doi.org/10.17487/RFC8484

[22] Austin Hounsel et al. 2020. Comparing the Effects of DNS, DoT, and DoH on Web Performance. In *WWW 2020*. https://doi.org/10.1145/3366423.3380139

[23] Austin Hounsel et al. 2021. Can Encrypted DNS Be Fast?. In *PAM 2021*. https://doi.org/10.1007/978-3-030-72582-2_26

[24] Zi Hu et al. 2016. Specification for DNS over Transport Layer Security (TLS). RFC 7858. (2016). https://doi.org/10.17487/RFC7858

[25] Christian Huitema et al. 2022. DNS over Dedicated QUIC Connections. RFC 9250. (2022). https://doi.org/10.17487/RFC9250

[26] Christian Huitema et al. 2022. *DNS over Dedicated QUIC Connections*. Internet-Draft. IETF. https://datatracker.ietf.org/doc/draft-ietf-dprive-dnsoquic/ Work in Progress.

[27] IP-API. 2022. IP Geolocation API. (2022). https://ip-api.com/ [Online; accessed 2022-Sep-18].

[28] Jana Iyengar and Ian Swett. 2021. QUIC Loss Detection and Congestion Control. RFC 9002. (2021). https://doi.org/10.17487/RFC9002

[29] Jana Iyengar and Martin Thomson. 2021. QUIC: A UDP-Based Multiplexed and Secure Transport. RFC 9000. (2021). https://doi.org/10.17487/RFC9000

[30] Sebastian Kappes. 2022. DNS Measurements Pull Request. (2022). https://github.com/mgranderath/dns-measurements/pull/2 [Online; accessed 2022-Sep-18].

[31] Sebastian Kappes. 2022. DNSPerf Pull Request. (2022). https://github.com/mgranderath/dnsperf/pull/3 [Online; accessed 2022-Sep-18].

[32] Dae Wook Kim and Junjie Zhang. 2015. You Are How You Query: Deriving Behavioral Fingerprints from DNS Traffic. In *SecureComm 2015*. https://doi.org/10.1007/978-3-319-28865-9_19

[33] Matthias Kirchler et al. 2016. Tracked Without a Trace: Linking Sessions of Users by Unsupervised Learning of Patterns in Their DNS Traffic. In *AISec 2016*. https://doi.org/10.1145/2996758.2996770

[34] Mike Kosek. 2022. DNS Privacy with Speed? Evaluating DNS over QUIC and its Impact on Web Performance. (2022). https://github.com/kosekmi/2022-imc-dns-over-quic-web-performance [Online; accessed 2022-Sep-18].

[35] Mike Kosek. 2022. DNS Proxy Pull Request DoT Connection Reuse. (2022). https://github.com/AdguardTeam/dnsproxy/pull/269 [Online; accessed 2022-Sep-18].

[36] Mike Kosek et al. 2022. Measuring DNS over TCP in the Era of Increasing DNS Response Sizes: A View from the Edge. *SIGCOMM CCR* 52, 2 (June 2022), 44–55. https://doi.org/10.1145/3544912.3544918

[37] Mike Kosek et al. 2022. One to Rule Them All? A First Look at DNS over QUIC. In *PAM 2022*. https://doi.org/10.1007/978-3-030-98785-5_24

[38] John Kristoff and Duane Wessels. 2022. DNS Transport over TCP - Operational Requirements. RFC 9210. (2022). https://doi.org/10.17487/RFC9210

[39] Jianfeng Li et al. 2018. Can We Learn what People are Doing from Raw DNS Queries?. In *INFOCOM 2018*. https://doi.org/10.1109/INFOCOM.2018.8486210

[40] Chaoyi Lu et al. 2019. An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?. In *IMC 2019*. https://doi.org/10.1145/3355369.3355580

[41] Linux manual page. 2022. resolv.conf(5). (2022). https://man7.org/linux/man-pages/man5/resolv.conf.5.html [Online; accessed 2022-Sep-18].

[42] MDN Web Docs. 2022. First contentful paint. (2022). https://developer.mozilla.org/en-US/docs/Glossary/First_contentful_paint [Online; accessed 2022-Sep-18].

[43] MDN Web Docs. 2022. Page load time. (2022). https://developer.mozilla.org/en-US/docs/Glossary/Page_load_time [Online; accessed 2022-Sep-18].

[44] NextDNS. 2021. Knowledge Base. (2021). https://help.nextdns.io/t/x2hmvas/what-is-dns-over-tls-dot-dns-over-quic-doq-and-dns-over-https-doh-doh3 [Online; accessed 2022-Sep-18].

[45] Craig Partridge and Mark Allman. 2016. Ethical Considerations in Network Measurement Papers. *Commun. ACM* 59, 10 (2016), 58–64. https://doi.org/10.1145/2896816

[46] Victor Le Pochat et al. 2019. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In *NDSS 2019*. https://doi.org/10.14722/ndss.2019.23386

[47] The Chromium Projects. 2022. Chromium open-source browser. (2022). https://www.chromium.org/Home [Online; accessed 2022-Sep-18].

[48] Eric Rescorla. 2018. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446. (2018). https://doi.org/10.17487/RFC8446

[49] Matt Sargent et al. 2011. Computing TCP’s Retransmission Timer. RFC 6298. (2011). https://doi.org/10.17487/RFC6298

[50] Benjamin M. Schwartz et al. 2022. *Service binding and parameter specification via the DNS (DNS SVCB and HTTPS RRs)*. Internet-Draft draft-ietf-dnsop-svcb-https. IETF. https://datatracker.ietf.org/doc/draft-ietf-dnsop-svcb-https/ Work in Progress.

[51] Selenium. 2022. Selenium web browser automation. (2022). https://github.com/seleniumhq/selenium [Online; accessed 2022-Sep-18].

[52] Martin Thomson and Sean Turner. 2021. Using TLS to Secure QUIC. RFC 9001. (2021). https://doi.org/10.17487/RFC9001

[53] Trinh Viet Doan et al. 2021. Measuring DNS over TLS from the Edge: Adoption, Reliability, and Response Times. In *PAM 2021*. https://doi.org/10.1007/978-3-030-72582-2_12

[54] W3Techs. 2022. HTTP usage statistics. (2022). https://w3techs.com/technologies/history_overview/site_element/all/y [Online; accessed 2022-Sep-18].

[55] Paul Wouters et al. 2016. The edns-tcp-keepalive EDNS0 Option. RFC 7828. (2016). https://doi.org/10.17487/RFC7828

[56] Liang Zhu et al. 2015. Connection-Oriented DNS to Improve Privacy and Security. In *IEEE Symposium on Security and Privacy 2015*. https://doi.org/10.1109/SP.2015.18

[57] ZMap. 2022. The ZMap project. (2022). https://zmap.io/ [Online; accessed 2022-Sep-18].