The Future of DNS Privacy: A Comparison of DNS over QUIC and DNS over HTTP/3

Philipp Bielefeld, Felix Hoffmann, Steffen Sasalla,
vasilis ververis, and Vaibhav Bajpai

Hasso Plattner Institute, University of Potsdam, Germany

Abstract. This study presents a large-scale empirical analysis of DNS-over-Encryption (DoE) protocols, focusing on the adoption, protocol feature support, and impact on webpage loading performance. We conducted measurements across over three thousand DoE resolvers, characterizing their support for features such as session resumption and 0-Round-trip Time (RTT) in DNS-over-QUIC (DoQ) and DNS-over-HTTP/3 (DoH/3). Despite broader feature adoption by DoQ, major browsers currently favor DoH/3. Our extensive latency measurements demonstrate that both protocols perform comparably, with DoQ slightly outperforming on average. Complementary experiments with the top one million websites show negligible overall page load time penalties when using DoQ or DoH/3 compared to traditional DNS-over-UDP (Do53), even under low-latency conditions.

Further, our analysis explores the relationship between webpage complexity, quantified via metrics including number of objects, queried servers, and `MIME` type diversity, and the performance impact of DoE. We find no statistically significant correlation, indicating that DoEs performance effects are consistent across a range of website architectures. The study also addresses limitations in current client support for key protocol enhancements and validates effective 0-RTT resumption using proxy resolvers. Our findings alleviate prevalent concerns about DoE-induced performance degradation, supporting broader adoption of encrypted Domain Name System (DNS) protocols without sacrificing user experience. We release our datasets, source code, and analysis scripts to facilitate reproducibility and foster further research into encrypted DNS ecosystems.

1 Introduction

Initially, Internet development prioritized data transport over encryption. However, as critical systems increasingly rely on Internet communication, security concerns necessitated encryption. Today, most Internet traffic is encrypted, though components like DNS [37] still depend on unencrypted communication. The DNS protocol is vital for domain resolution, traffic balancing, and Content Delivery Networks (CDNs) [33]. The rise of cloud providers has democratized access to these services, supporting diverse applications. While DNS traffic may seem less sensitive, it can disclose significant information, such as requested domains, requestor IP addresses, and query timestamps. Users typically remember domain names rather than numerical IP addresses, while machines operate on address-based systems. Although dynamic IP addresses complicate long-term tracking, behavioral patterns in DNS queries can still reveal user interests [35], highlighting the need for encrypted DNS traffic. To enhance privacy, DNS-over-TLS (DoT) was introduced in 2016 to encrypt DNS requests, but its adoption was limited due to performance concerns compared to Do53 [27]. For any encrypted DNS protocol to gain widespread use, it must balance privacy and performance. Recently standardized DoQ and DoH/3 offer reduced performance overhead, utilizing QUIC for improved speed and reliability. However, DoQ directly carries DNS queries, while DoH/3 encapsulates them within HTTP/3, complicating user decision-making. Given that domain resolution is crucial for web browsing, with numerous DNS requests per visit, any latency from encryption can hinder page load times. Users expect pages to load within two seconds [48], yet frequently visited sites generate at least 20 background DNS queries [6]. While existing research often compares RTT between DNS and newer protocols, there is limited evidence linking these metrics to real-world user experiences. Evaluations should prioritize user-perceived performance over network metrics. In light of these considerations, we address the following Research Questions (RQs):

RQ1: What percentage of resolvers support performance enhancement features such as session resumption and 0-RTT for DoQ and DoH/3?

RQ2: What is the performance penalty of DoE protocols such as DoQ and DoH/3 on website loading speed?

RQ3: Do certain website categories experience greater or lesser impacts from DoE resolvers, and what factors influence these variations?

To answer these RQs, we take a user-centric approach to evaluate encrypted DNS's impact on browsing, comparing features and performance costs across millions of websites. Our **research contributions** are:

1. Nearly all DoQ resolvers we measured support session resumption. Two thirds of DoQ resolvers also support 0-RTT. Only 65 % of DoH/3 resolvers support session resumption (see section 4).
2. While DoQ and DoH/3 offer comparable speeds, DoQ has a slight edge due to DoH/3's absence of 0-RTT support. Interestingly, major browsers prefer DoH/3. Resolvers supporting all DoE protocols show superior performance, and DoQ's response times in this subset even outperform the average Do53 speeds (see section 5).
3. There is no significant penalty for using DoQ or DoH/3 over Do53 in low-latency conditions. Average page load differences between DoQ, DoH/3, and Do53 are $\leq$1 %. There is no substantial correlation between the number of DNS requests made to load a website (i.e., web complexity) and its First Contentful Paint (FCP) performance (see subsection 5.1 and subsection 5.2).

We observe that nearly all DoQ resolvers support session resumption, with approximately two-thirds also enabling 0-RTT. In contrast, only 65 % of DoH/3 resolvers offer session resumption. Despite the more extensive feature adoption by DoQ, DoH/3 remains the preferred protocol in major web browsers. Performance comparisons indicate both protocols achieve similar speeds, with DoQ demonstrating a slight average advantage. Additionally, our assessment of DoE effects on page load times across the top one million websites reveals no significant performance penalty for using DoQ or DoH/3 compared to traditional Do53 under low-latency network conditions, with average webpage load time differences ranging between -2 ms to 16 ms.

Reproducibility In order to promote reproducibility and encourage further research, we have released our research artifacts, including the source code and analysis scripts, as well as the measurement study data [25]. Detailed documentation is provided to guide users on how to reproduce our results.

2 Background and Foundations

This section provides background on how unencrypted DNS enables user tracking—a privacy concern that modern encrypted protocols address. Although early encryption attempts were slow, newer protocols such as DoQ and DoH/3 leverage QUIC to improve both performance and privacy. Our study evaluates these claims by comparing DoQ and DoH/3.

2.1 DNS over Encryption Protocols

DoE protocols leverage existing connection protocols to securely transmit DNS queries and responses over encrypted channels, ensuring both the authenticity and integrity of the transmitted data. Although initially introduced to secure *stub-to-recursive* communication, technically they can also be used to secure *recursive-to-authoritative* communication [22]. Three such protocols have been standardized: DoT in May 2016 [28], DNS-over-HTTPS (DoH) in October 2018 [24], and DoQ in April 2024 [29]. To provide their security characteristics, they rely on Transport Layer Security (TLS) and its Public Key Infrastructure (PKI) based on X.509 certificates [11]. In the case of the QUIC protocol [31], the TLS 1.3 handshake is integrated directly into the protocol itself [66].

2.2 Transport Layer Security

TLS is designed to create a secure communication channel between two endpoints over an insecure network, ensuring confidentiality, integrity, and authenticity. Currently, TLS 1.2 [14] and TLS 1.3 [57] are the most widely deployed versions [53], with one of its primary applications being HTTPS [56] on the web. However, TLS is a versatile protocol used in various Internet applications. TLS consists of two main components: the record protocol and the handshake protocol. The record protocol is responsible for the integrity-protected and encrypted

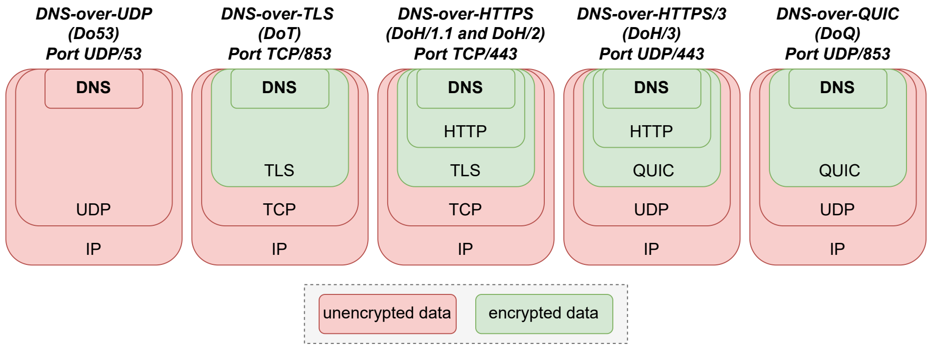


Fig. 1: The structure of the packet layers starting from the IP layer.

transmission of data using symmetric session keys. Meanwhile, the handshake protocol handles server (and client) authentication and establishes the session key for the record protocol.

To ensure authenticity of the server and optionally the client in the handshake phase, TLS relies on the X.509 PKI [11]. This PKI establishes authentication chains through a hierarchical structure (similar to DNS Security Extensions (DNSSEC)), where trust is anchored in a root Certificate Authority (CA) and cascades down through intermediate CAs, enabling secure verification of digital certificates across a network. This hierarchical model ensures that each entity's identity is authenticated by a trusted authority, creating a chain of trust from the root CA to the end user. Thus, a client can validate the identity and authenticity of a server's response, for example.

2.3 DNS over TLS

DoT is a DoE protocol designed to securely transmit DNS queries and responses over a TLS-encrypted channel, ensuring privacy and integrity of the exchanged data [28]. While initially defined for *stub-to-recursive* communication, DoT can also be extended to secure *recursive-to-authoritative* server connections. By default, DNS servers that run DoT should use port TCP/853 unless an alternative arrangement is negotiated between both parties [28]. Clients are responsible for maintaining knowledge of which DNS servers support TLS and must be capable of handling connections with both encrypted and unencrypted resolvers. When establishing a connection, clients are expected to follow the TLS protocol, including the proper verification of the server's certificate chain in accordance to best practices for secure communication [64].

Once the TLS handshake is completed, DNS queries and responses are exchanged over the TLS channel via the DNS wire format [46], a byte-level representation of DNS messages. This ensures that while the underlying data remains consistent with existing DNS standards, the communication is protected against eavesdropping and tampering.

2.4 DNS over HTTPS

DoH is a protocol designed to secure the transmission of DNS queries and responses by encapsulating them within HTTPS traffic, leveraging TLS to provide both authenticity and encryption [24]. In contrast to DoT, which operates DNS directly over TLS, DoH utilizes the intermediate layer HTTP between DNS and TLS (see Figure 1). This architectural difference allows DoH to take advantage of various HTTP features, such as redirection, proxying, client authentication, compression, and response format negotiation. Furthermore, DoH allows HTTP clients such as web applications to interact with the DNS ecosystem seamlessly via standard Application Programming Interfaces (APIs). However, a challenge with DoH lies in the potential ambiguity surrounding caching mechanisms and error codes, since both HTTP and DNS natively implement these features. DoH can operate on Transmission Control Protocol (TCP) and TLS with HTTP/1.1 (legacy) and HTTP/2. In addition, it also supports HTTP/3, which operates over User Datagram Protocol (UDP) and uses QUIC as its transport layer, similar to DoQ. By default, HTTPS traffic runs on port 443 [56].

Unlike DoT and DoQ, where clients only need to know the resolver and the port to exchange DNS information, DoH requires additional configuration. Specifically, DoH clients must be aware of the specific Uniform Resource Identifier (URI) path where the DNS queries are processed. For instance, Google's DoH resolver accepts queries at `https://dns.google/dns-query`. Additionally, DoH supports both HTTP GET and HTTP POST methods for transmitting DNS queries. When using HTTP POST, the DNS query is encoded in its wire format and embedded in the body of the HTTP request. For HTTP GET, the query is base64url [32] encoded and appended to the URI as a query parameter. For example, a GET request to Google's resolver would appear as `https://dns.google/dns-query?dns=<b64-dns-query>`. Although the DoH standardization specifies a URI path `dns-query` and parameter `dns`, it allows resolvers to use different configurations.

2.5 DNS over QUIC

QUIC is a secure transport protocol built on top of UDP, designed to minimize latency through features like 0-RTT resumption, advanced loss recovery, and multiplexing data streams to avoid head-of-line blocking [31,29]. Unlike TCP, QUIC implements reliability and ordering at the transport layer and integrates the TLS 1.3 handshake directly, ensuring encrypted and authenticated communication [66]. DoQ encapsulates DNS traffic within QUIC, providing equivalent security guarantees to DoT with performance benefits [29]. By default, DoQ servers listen on UDP port 853. Each DNS query is sent over a separate QUIC stream, enabling concurrent requests without TCP's head-of-line blocking, improving throughput and responsiveness. Queries and responses use the standard DNS wire format [45]. DoQ also defines new transport-specific error codes, such as `DOQ_EXCESSIVE_LOAD`, to signal server resource constraints and enhance error handling.

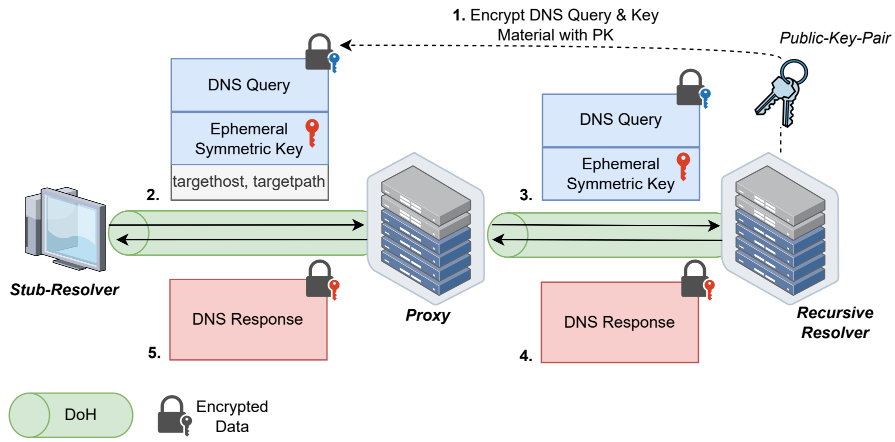


Fig. 2: Simplified illustration of the oDoH protocol. Green tunnels indicate DoH connections. Blue boxes show data encrypted with the resolver's public key; red boxes show data encrypted with the client's ephemeral symmetric key.

2.6 Oblivious DNS over HTTPS

While DoE protocols encrypt DNS queries between stub resolvers and Recursive Resolver (RR), the RR still learns the client's IP address, enabling user tracking similar to unencrypted Do53. To enhance privacy, Oblivious DNS-over-HTTPS (oDoH) was standardized in 2022 [34] as an extension of DoH that adds a proxy to prevent any single server from seeing both client identity and DNS query contents. As illustrated in Figure 2, the client encrypts its DNS query and an ephemeral symmetric key with the resolver's public key using Hybrid Public Key Encryption (HPKE), and sends this to a proxy over DoH (see subsection 2.4). The proxy forwards the encrypted query to the resolver but cannot decrypt it. Only the resolver, possessing the private key, can decrypt and answer the query, encrypting its response with the ephemeral symmetric key using an Authenticated Encryption with Associated Data (AEAD) scheme to ensure confidentiality and integrity. The proxy then relays the encrypted response back to the client, which decrypts it with the previously generated symmetric key.

This design ensures that the resolver cannot link client IPs to query contents, and the proxy cannot access query details. Even if routing information (`targethost`, `targetpath`) is tampered with, only the resolver can decrypt and respond correctly, preserving response integrity.

2.7 Security and Privacy Considerations

All DoE protocols inherit the security properties of the underlying TLS version, providing confidentiality, integrity, and authentication [63]. However, privacy risks arise during resolver discovery: clients typically probe the default DoE port (e.g., TCP/853 for DoT) to establish connections [13]. Such probing can be targeted by attackers performing downgrade or redirect attacks by blocking probes, forcing the client to fall back to unencrypted Do53.

RFC 8310 [13] defines two privacy usage profiles to mitigate this risk: *Opportunistic Privacy*, where clients prefer encryption but do not strictly authenticate resolvers, allowing use of potentially untrusted servers (e.g., discovered via DHCP). This profile protects against passive eavesdropping but remains vulnerable to active attacks. *Strict Privacy* requires pre-established trust, often implemented by pinning the resolver's public key fingerprint [18]. This prevents downgrades and ensures resolver authenticity but may lead to denial-of-service if connections fail or are blocked. These profiles, initially defined for DoT, apply conceptually to all DoE protocols, balancing privacy guarantees against availability and deployment complexity.

2.8 DNS Resolution Impact on Webpage Load Time

DNS resolution is a critical step in the webpage loading process, as the browser must resolve domain names to IP addresses before fetching any content. DNS lookups typically take between a few milliseconds and several hundred milliseconds, depending on factors such as server proximity, caching effectiveness, network congestion, and resolver performance. Since modern webpages often load resources from multiple distinct domains—including images, scripts, stylesheets, and third-party services—multiple DNS queries are triggered. Each additional lookup adds latency cumulatively, which can substantially prolong total page load time, especially on slower networks or mobile devices.

To mitigate this impact, techniques such as DNS prefetching allow browsers to proactively resolve domain names before they are actually needed, while preconnect can further reduce delays by initiating TCP and TLS handshakes early. CDN-based resolver distribution, anycast routing, and optimized TTL configurations also contribute to minimizing DNS-related latency. Effective DNS performance directly benefits user experience by reducing time to first byte and accelerating the loading sequence, thereby supporting improved search rankings, lower bounce rates, and higher user engagement. Our experiments incorporate DoE protocols to evaluate such latency effects within the broader webpage load timeline described in section 2.8.

Loading a Webpage Loading a webpage follows well-defined steps common to modern browsers like Chrome and Edge, both based on the Chromium engine [65]. Figure 3 illustrates the sequence of key events aligned with the *Navigation Timing* interface implemented in major browsers [69,68,61].

The process begins with a user-initiated request, minimizing redirects and disabling application caching to ensure consistent measurements. The browser first performs DNS resolution, influenced by the chosen DoE protocol. Next, it establishes the connection using TCP/TLS or QUIC, marked by `connectStart` and `connectEnd` during the TLS handshake. The HTTP `GET` request follows, with `responseStart` and `responseEnd` indicating receipt of the HTML document. As content streams in, the browser builds the Document Object Model

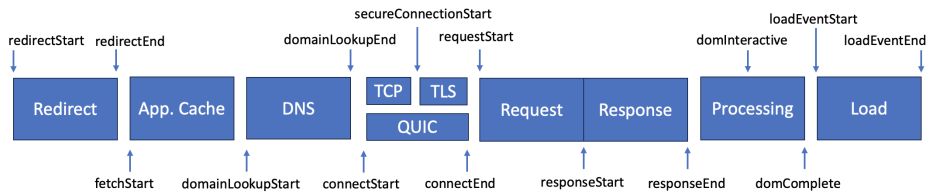


Fig. 3: Timeline of webpage loading highlighting key browser events captured in our experiments.

(DOM). The `domInteractive` event marks when the DOM is ready for interaction, allowing non-blocking scripts to execute. Subsequent resource loading and script execution conclude with `loadEventStart` and `loadEventEnd`, although asynchronous loading often continues beyond these points.

Page Performance and Relevancy Webpage performance critically impacts user satisfaction and business metrics [55,2]. In competitive domains like e-commerce, improved responsiveness can be a key differentiator [65,19]. Users typically expect answers within two seconds for simple queries [48], highlighting the importance of efficient DNS resolution. While search rankings are sensitive to page speed, the direct influence of DoE protocols on rankings remains unclear [61]. Variability in DNS performance across sites may partly explain ranking differences, motivating our analysis in section 5.

Page Complexity Modern webpages often have complex architectures, employing techniques like Single Page Applications (SPAs) that increase script usage and interactivity. This complexity affects the relative impact of DNS performance on overall load times. Key technical complexity factors include the `number of loaded objects` (total resources such as images, scripts, and stylesheets), the `total downloaded bytes` (larger payloads can reduce the proportional impact of DNS latency), the `distinct MIME types` (indicating content diversity and complexity), the `distinct queried servers` (reflecting microservices or third-party content distribution), the `non-origin queried servers` (often related to advertising and analytics domains), the `DNS request count` (higher request counts increase DNS protocol influence), and the `objects and bytes per MIME type` (providing deeper insight into how content types affect load times).

For example, `facebook.com` loads over 70 resources, including numerous JavaScript files, whereas `google.com` loads approximately 34 resources (see Figure 4). This illustrates the wide range of complexity that can impact load behavior [67,5].

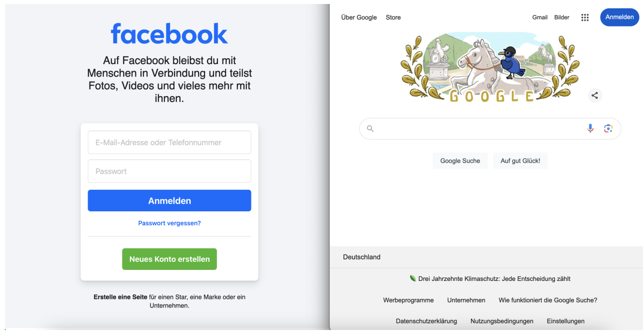


Fig. 4: Complexity comparison: Facebook (left) with 70+ objects versus Google (right) with fewer objects. Both display a simple interface but vary in underlying complexity.

2.9 Related Work

The effectiveness of any DNS protocol relies on resolver support. User adoption of DoQ has been limited by inadequate browser and DNS provider support. Early analyses [59] showed minimal QUIC adoption before standardization, with few hosts offering valid X.509 certificates. Despite this, QUIC's performance advantages over HTTP/2 [10] suggest potential benefits for DNS. Studies [43] found no DoQ resolvers prior to its 2019 standardization. However, DoE usage has increased in censorship-heavy regions, with DoH being less detectable than DoT. While DoE support has grown, actual usage remains low [20], with DoT dominating. Recent research [36] indicates a rise in DoQ resolvers, though many are experimental. A significant increase [40] in DoQ servers and improved certificate validity rates suggest growing productive use [42].

Existing DNS measurements [36] focus on latency, noting that misconfigured traffic amplification can inflate handshake times. Comparisons [6] show significant latency in DoT and DNS-over-HTTP/1.1 (DoH/1.1) compared to plain UDP, especially under TLS head-of-line blocking. Persistent connections are crucial for minimizing encryption overhead [43]. Performance comparisons indicate DoQ can outperform Do53 over short distances due to optimized hardware handling. Provider influence is significant, with response time disparities across DNS services [9]. When connection setups are minimized [26], median response times between Do53 and DoT become comparable.

Studies emphasize the impact of DNS resolvers on page load times. Research [37] suggests DoQ can delay time to first contentful paint, influenced by site-specific factors. QUIC's resilience in high-loss environments [10,37] correlates with improved performance. Studies [62] link DoQ and DNS-over-HTTP/2 (DoH/2) page load times to access technology, reporting significant latency increases, especially on mobile devices. This contrasts with earlier findings [67] that DNS lookups contribute modestly to critical path delays. Optimizing DNS loading times through persistent connection improvements remains essential. While

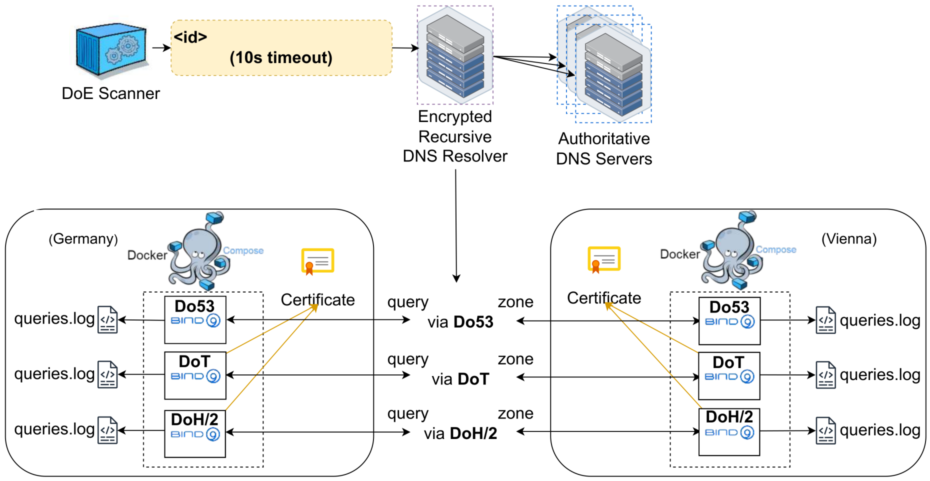


Fig. 5: Architecture of our authoritative DNS servers deployed in separate Docker containers to support multiple protocols and enable independent logging, with encrypted communication via DoT and DoH/2.

earlier DoE protocols have been investigated, a comparative evaluation of the latest DoQ and DoH/3 is still needed, highlighting a research gap that our study addresses.

3 Methodology

This section describes the experimental framework used to evaluate DNS resolver capabilities, web performance impacts, and the relationship between webpage complexity and DoE protocols. We designed and implemented three complementary measurement experiments focused on DNS performance, website loading behavior, and site complexity analysis. Figure 6 provides a visual overview of these experimental setups.

3.1 Authoritative DNS Server Setup

To analyze the adoption of encrypted *recursive-to-authoritative* DNS communication, standardized in RFC 9539 [22], we query all discovered DoE resolvers with uniquely crafted Query Names (QNAMEs) targeting `A` records in our controlled DNS zone. Each QNAME follows a unique pattern `<id>.measurement.example`, with a wildcard `*.measurement.example` pointing to an IPv4 address hosting our measurement infrastructure (see subsection 3.6). This approach ensures that every query is resolvable and identifiable, permitting detailed observation of DoE resolver recursive behaviors and revealing whether encrypted channels are used in recursive-to-authoritative communications.

Our authoritative name servers, located in Germany and Austria, run *bind9* [30], which natively supports DoT and DoH/2. Since *bind9* logs do not differentiate query transport protocols, we deploy separate Docker containers for each protocol, all sharing the same zone file (see Figure 5). These containers are based on Canonical's official *bind9* Ubuntu images [7]. Valid TLS certificates for DoT and DoH/2 are obtained via *certbot* using Let's Encrypt [16,17].

3.2 Discovery of IPv4 and IPv6 DNS Resolvers

We perform large-scale discovery of IPv4 DNS resolvers by executing frequent scans from a single vantage point using *ZMap* [15]. The scanner probes IPv4 addresses on UDP port 53 by requesting the `A` record for `www.google.com`[1], to maximize hits through cached responses due to the domain's high popularity [41] (see Figure 5). We filter the resulting IPv4 addresses against a comprehensive blocklist of private and reserved address spaces [54,12] and abuse-reported ranges supplied by the *MassDNS* project [4], to respect network operators' requests and avoid scanning inappropriate targets.

Due to the infeasibility of IPv6 exhaustive scans, we leverage the *IPv6 Hitlist Service* [21,60] which curates responsive IPv6 UDP/53 addresses, updated weekly. Though this introduces a minor time lag that may bias results due to address churn [51], it remains the most practical approach. To automate retrieval, the system daily fetches updates from the IPv6 Hitlist Service. Our scan producer coordinates the scanning workflow by consuming IP outputs from *ZMap* via named pipes.

To avoid backpressure and blocking caused by limited pipe buffers [50], we implemented a large internal buffer and concurrent go routines to continuously read and schedule scan tasks to *Apache Kafka*. This design ensures robust, scalable handling of scanning pipelines without data loss or process interruptions. The scan producer's parsing logic requires minimal knowledge of scanner output formats, supporting seamless integration of new scanning tool versions and immediate follow-up scanning to mitigate the effects of IP churn [38,58,44].

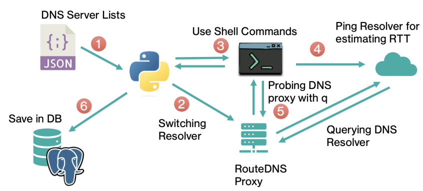
3.3 Evaluating DNS Performance

The DNS performance experiment (see Figure 6a) is managed by a Python script that merges resolver lists, removes duplicates, configures RouteDNS proxies for DoQ and DoH/3 (including fallbacks), and verifies resolver reachability with ping. It dispatches queries to test protocol support, warms resolver caches, measures round-trip times, session resumption, and 0-RTT. Results with resolver metadata and protocol support are stored in a database.

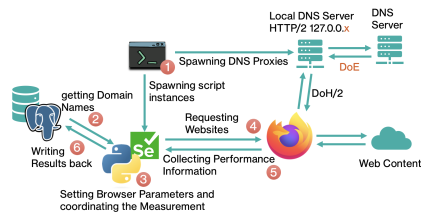
3.4 Assessing Website Performance

We evaluate web performance using the metrics established in [37]: FCP, Largest Contentful Paint (LCP), and Page Load Time (PLT). Testing the Tranco top

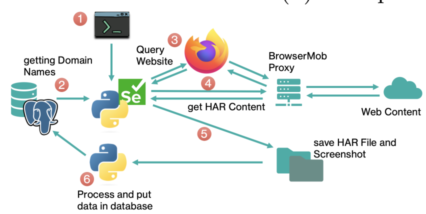
[1] A single query per IP is sufficient, given marginal gains from multiple probes.



(a) DNS performance measurement



(b) Web performance measurement



(c) Website complexity analysis

Fig. 6: Architectures of the three experimental setups: DNS performance testing, controlled web performance evaluation, and web complexity assessment.

1M sites [52] with Firefox (for TLS 1.3 0-RTT support [47,3]), we use a local DNS proxy resolving via UDP, QUIC, or HTTP/3. Unlike prior methods [37], we assign the proxy's IP directly to the Selenium WebDriver for scalability.

The procedure, shown in Figure 6b, comprises: 1. Starting DNS proxies and Python scripts with configuration parameters, 2. Obtaining domain sets from the database filtered by complexity, 3. Configuring WebDriver DNS to use the local proxy, 4. Performing warm-up requests to refresh upstream caches, 5. Executing measurement navigation upon successful warm-up; logging failures, 6. Recording all browser performance metrics in the database.

3.5 Measuring Web Complexity

The web complexity experiment (see Figure 6c) quantifies site structure effects on DNS protocol performance via parallel Python scripts collecting network traffic. Steps include: 1. Running multiple Python instances for parallel queries, 2. One query per website, with error detection, 3. Capturing HAR-format network traffic on page load via BrowserMob Proxy, 4. Storing HAR files and screenshots for verification, 5. Processing HARs to extract metrics (e.g., object counts, MIME types, queried servers) saved to a database. This structured approach enables thorough, scalable analysis of DNS and webpage performance interdependencies.

3.6 Ethical Considerations

We follow established best practices and ethical guidelines [39,8,49,23,1] to ensure responsible measurement. No user-related or personally identifiable data is collected; only publicly available information on DNS servers' and DoE configurations is analyzed. We do not exploit or probe insecure systems. To minimize network impact, DNS server discovery is limited to twice weekly, with caching to avoid redundant queries. Scans use *ZMap* [15] and the *IPv6 Hitlist Service* [21,60], which employ randomization to prevent network overload.

3.7 Global and AS-Level Distribution

We enriched our resolver discovery with geographical and Autonomous System (AS) location data, observing deployments in over 70 countries. The United States and several European countries accounted for a substantial proportion of advertised resolvers. Protocols like DoQ and DoH/2 showed the greatest diversity, with resolvers spanning hundreds of ASes, suggesting widespread but fragmented deployment, sometimes driven by smaller operators. In contrast, DoH/3 and DoT were hosted in a limited subset of ASes, often within large service providers such as AdGuard. This uneven distribution could have implications for the ecosystem's resilience and accessibility.

3.8 Performance

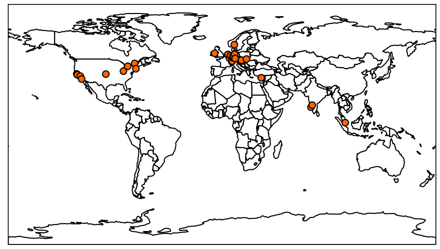
Latency measurements were collected for 28,792 successful DoE queries from a vantage point in Berlin, Germany. Figure 8a presents the Cumulative Distribution Function (CDF) of RTTs across all resolved queries, comparing performance of the five major DoE protocols. While DoQ and DoH/3 both use QUIC, latency results differed: DoH/3 showed the fastest median RTT, followed closely by DoH/2 and DoQ with comparable values. Interestingly, DoT exhibited the lowest average latency overall, with median RTT around 60 ms. These results suggest that although transport choice influences latency, factors including resolver location, network paths, and provider infrastructure significantly affect observed performance.

Figure 8b zooms in on resolvers operated by entities supporting multiple protocols (e.g., AdGuard and Control D). Here, the median RTTs for DoQ, DoH/2, and DoH/3 range narrowly between 115 ms to 123 ms, indicating that network locality and operational environment are major determinants of performance, potentially more so than specific protocol overheads.

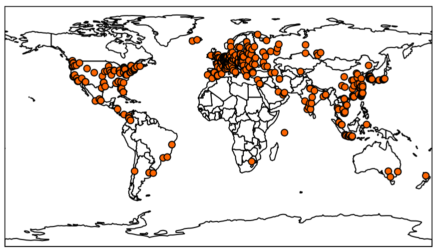
3.9 Errors and Reliability

Across more than 75,000 encrypted DNS requests, we identified and categorized connection failures, TLS errors, HTTP-layer problems (for DoH/2 and DoH/3), DNS errors, and responses with non-zero RCODEs. Connection problems such as unreachable endpoints and timeouts dominated, particularly among DoQ and DoH/2, while TLS certificate issues accounted for a significant share of failures, often due to expired certificates or unknown authorities. HTTP errors frequently resulted from invalid resource paths or non-compliant endpoints. Notably, a high

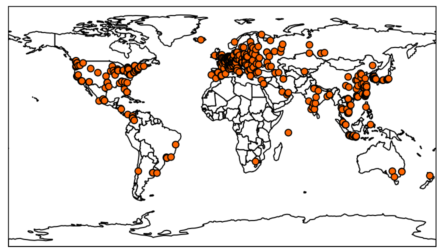
(a) DoH/1.1



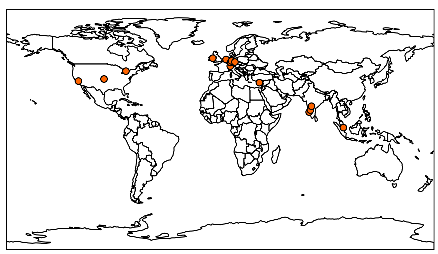
(b) DoT



(c) DoH/2



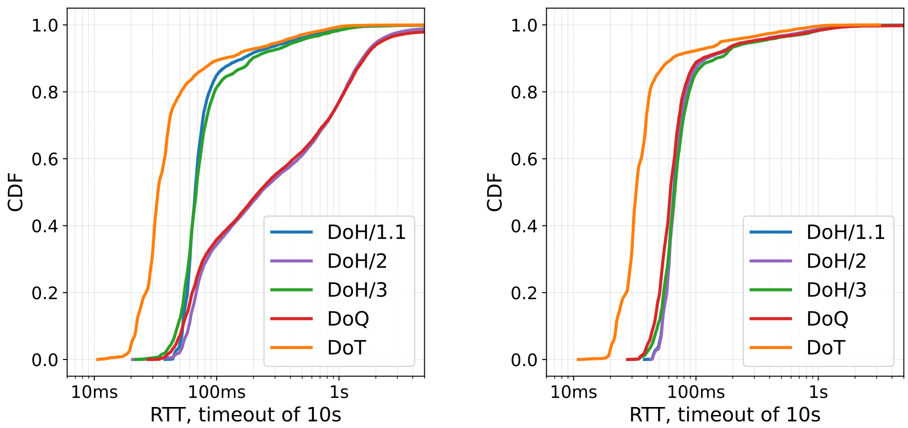
(d) DoQ



(e) DoH/3

Fig. 7: Global distribution of unique DNS over Encryption (DoE) resolvers per protocol. Each dot represents the approximate location of a distinct DoE resolver. As a single resolver may support multiple DoE protocols, dots can coincide across multiple protocol-specific maps. This visualizes the geographical spread and overlap of resolver deployments across different encrypted DNS protocols.

percentage of non-zero RCODEs consisted of REFUSED responses, indicative of mismatches between advertising and actual resolver capabilities. A comparative view across protocols showed that DoH/1.1, DoH/3, and DoT achieved the highest rates of successful DNS responses.



(a) Cumulative distribution function (CDF) of round-trip times (RTTs) for all successful DoE probes.

(b) CDF of RTTs for DoE probes specifically targeting resolvers within the *AdGuard* and *Control D* ASes.

Fig. 8: Latency distributions of discovered DoE resolvers during the probing phase. The left panel shows the overall RTT distribution for all probes that successfully returned a DNS response. The right panel focuses on RTTs measured solely from probes sent to resolvers operated by major providers supporting multiple DoE protocols. These CDFs provide insight into the variability and typical latency experienced across protocols and operators.

3.10 TLS Security Properties

All observed DoE resolvers negotiated either TLS 1.2 or TLS 1.3, with 99% preferring TLS 1.3, especially for QUIC-backed protocols. The dominant cipher suite was `TLS_AES_128_GCM_SHA256`, utilized in well over 90% of connections; secondary suites included `TLS_AES_256_GCM_SHA384` and `TLS_CHACHA20_POLY1305_SHA256`. Diffie-Hellman key exchange was universal, ensuring ephemeral session keys. No weak or deprecated configurations were identified, supporting a robust security posture among active resolvers.

3.11 Recursive Resolving Behavior

Using authoritative server-side logs, we observed repeated query behaviors: out of 75,299 tagged DNS queries sent to discovered DoE resolvers, roughly 22% were replayed, sometimes with delays of up to several weeks. Such replay patterns were concentrated in a handful of ASes, predominantly in China, aligning with prior descriptions of "traffic shadowing" or "DNS zombies" in literature. Additional anomalies included 142 instances where resolvers returned invalid IPv4 addresses, like `0.0.0.0`, mainly from U.S. and South Korean networks—signaling partial misconfiguration or deviation from standard DNS practices. Importantly,

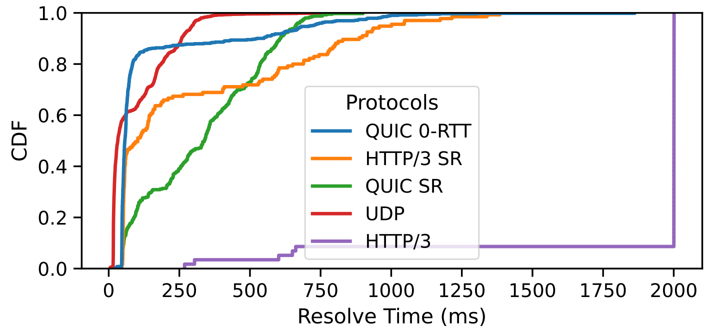


Fig. 9: CDF of DNS resolve times comparing resolvers with and without 0-RTT and session resumption.

Table 1: Performance comparison of DNS resolvers across HTTP/3, QUIC, and UDP, including session-resumption behavior, 0-RTT capabilities, request success rates, and response-time characteristics. The numbers in parentheses indicate results obtained during the third measurement run.

	HTTP/3	**QUIC**	**UDP**
Total Requests	554	1091	1529
Completed Requests	202	1112	1526
Failed Requests	391 (401)	3 (6)	3 (9)
Session Resumption	131	1039	–
0-RTT Support	0	733	–
0-RTT Error	554 (N/A)	6 (11)	–
Median Response Time (ms)	883 (2000)	88 (71)	33 (32)
Fastest Response (ms)	55 (46)	37 (23)	5 (4)
Slowest Response (ms)	2002 (2001)	1313 (1861)	1093 (800)

despite offering encrypted recursive-to-authoritative endpoints, no resolvers made use of these protocols, relying instead on traditional unencrypted recursion—likely a decision to minimize computational and operational overhead.

4 Session Resumption and 0-RTT

We performed two additional measurement campaigns to validate our findings and address a 0-RTT detection issue, which showed highly consistent results with only minor deviations. Table 1 displays the session resumption and 0-Round-Trip Time (RTT) support features, along with their corresponding response times.

Table 2: Fastest resolvers across all evaluated DNS protocols.

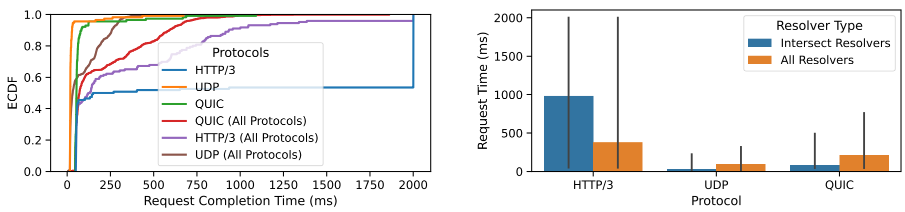
Rank	**Host**	**Avg. Time**	**DoH Time**	**Do53 Time**	**DoQ Time**
1.	2f07i9strpu.dns.controld.com.	46 ms	59 ms	20 ms	59 ms
52.	ams.core.access.zznet.fun.	66 ms	100 ms	21 ms	78 ms
53.	resolver64.dns4all.eu.	72 ms	93 ms	29 ms	92 ms
54.	nue2.moderateinfra.net.	76 ms	109 ms	20 ms	100 ms
55.	adguard.marcosbl.com.	96 ms	177 ms	29 ms	82 ms

Notably, nearly all DoQ resolvers (1039/1112) and 65 % of DoH/3 resolvers (131/202) supported session resumption, indicating improved DoE efficiency compared to previous findings [37]. However, DoH/3 showed no 0-RTT support. DoQ exhibited a significantly lower median response time (88 ms) than DoH/3 (883 ms), likely due to DoH/3's lack of 0-RTT. Performance outliers, such as consistently slow AdGuard DNS resolvers, further skewed DoH/3's median. Table 1 also highlights DoH/3's high unreliability, with 391 out of 401 resolvers failing measurements. This issue was not related to the implemented fallback mechanism. Despite these protocol differences, resolver selection is crucial to user experience. The fastest UDP resolver (5 ms) significantly outperformed the fastest DoQ (37 ms) and DoH/3 (55 ms) resolvers. This UDP advantage may be attributed to resolver proximity, reflecting the distance between our measurement point and the closest resolver. While DoH/3 optimization remains a challenge, DoQ resolvers are increasingly embracing 0-RTT support, as shown by these findings.

While Do53 requires only one round trip, DoH/3 and DoQ initially need three. However, session resumption and 0-RTT allow DoQ and DoH/3 to achieve Do53's round-trip efficiency. Figure 9 presents the CDF of resolve times, where DoH/3 shows a distinctive step pattern mainly due to the `adguard-dns.com` resolvers (covering approximately 85 % of the dataset). Their consistent response times suggest potential geographical or infrastructure limitations, which warrants further investigation. Resolvers supporting 0-RTT show lower average latency, but their fastest responses aren't quicker than non-0-RTT resolvers. This can be attributed to our fiber-optic vantage point, which reduces latency by minimizing propagation delays. After removing slow `adguard-dns.com` resolvers, nearly half of the DoH/3 resolvers with session resumption match DoQ's performance. Nonetheless, DoH/3 remains the least performant overall, possibly due to a larger proportion of experimental resolvers given its recent standardization.

5 DNS performance

Table 2 displays the fastest resolvers across all tested protocols. Unlike the previous analysis, this selection accounts for the resolver's proximity to our mea-



(a) CDF of DNS resolution times

(b) Mean and 95th percentile of resolution times

Fig. 10: Comparison of DNS resolve times between the subset of resolvers supporting all DoE protocols and the complete resolver set.

surement point, which is crucial for accurate web performance assessments. To minimize distance-related variations, we identified resolvers supporting all three protocols (Do53, DoQ, DoH/3). Although IP addresses may resolve to load balancers, potentially affecting routing, this approach ensured consistency. We selected resolvers that completed all protocol measurements and calculated their mean response time. Table 2 highlights the top performers. The highest-ranked resolver lacked 0-RTT support for DoQ, resulting in similar response times across all protocols. Since web performance measurements disabled 0-RTT, we prioritized resolvers with minimal DoH/3 and DoQ response time differences. Initial tests with the top resolver showed promise, but large-scale experiments revealed frequent timeouts. Therefore, the 53rd-ranked resolver, known for its stability, was ultimately chosen for the study.

Figure 10 compares response times for resolvers supporting all protocols against the full dataset. The subset generally exhibits lower response times, except for DoH/3, which is significantly influenced by `adguard-dns.com` outliers, as seen in the CDF. The bar plot presents average response times. While median Do53 resolvers outperform DoQ and DoH/3, subset DoQ resolvers surpass the overall Do53 average. The CDF reveals approximately 95 % of subset Do53 resolvers respond within 30 ms, with peak resolvers outperforming other protocols. Protocol-specific patterns emerge: Do53 shows a sharp initial response (approximately 60 % within 50 ms) before tapering off over 250 ms. DoQ and DoH/3 gradually increase response time distribution, with DoQ exhibiting a longer tail (approximately 1000 ms convergence). This indicates a minority of slow DoQ resolvers, while Do53 maintains a more uniform distribution. Overall, resolvers supporting all protocols perform better on average and occupy faster percentiles. The subset's 95th percentile response time is lower, driven by a consistently fast core group. The performance gap between DoH/3 and DoQ is due to DoH/3's lack of 0-RTT support. With approximately 65 % of DoQ resolvers supporting 0-RTT, their average RTT is significantly reduced. Both DoH/3 and DoQ suffer from longer tails due to a few slow resolvers, a trend absent in the Do53 CDF.

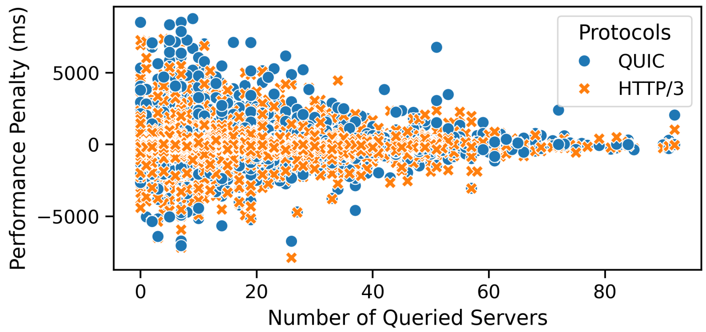


Fig. 11: Impact of the number of DNS queries on webpage FCP experience.

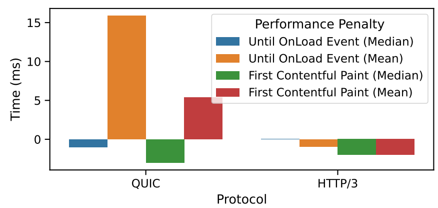
5.1 Impact of DNS on Website Performance

This section examines how various DNS protocols affect website loading times. Measurements were conducted from October 22 to 31, 2024, using three DNS stub resolver instances. To ensure consistent resolver distance, `resolver64.dns4all.eu` was used for all protocols. We probed 719,281 websites per DNS protocol, with each successful warm-up request followed by a measurement request. Ideally, this would yield 4,315,686 measurements. However, only 1,869,105 successful page loads were recorded, indicating significant website loading failures. Given that unsuccessful warm-up requests prevented measurements, and the complexity measurement only successfully loaded 572,367 websites, we obtained measurements for approximately half of the intended dataset.

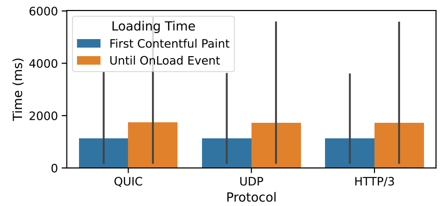
Our results indicate similar error counts across all DNS protocols for measurement queries. Despite these errors, the dataset, with nearly 700k completed measurements, remains robust for analysis. We applied the following filtering criteria to ensure data consistency and reliability: (a) Removed measurements with any recorded errors. (b) Excluded instances where the `loadEventEnd` was zero, but the FCP was not. (c) Focused solely on measurement requests, excluding warm-up requests. (d) Retained only websites with successful measurements across all protocols, reducing the dataset to 46,440 domains from the initial 455,677. This refined dataset guarantees that all per-protocol metrics and visualizations are based on the same set of websites, providing a fair and accurate assessment of how DNS protocols affect website performance.

We calculate the DNS loading times using $T_{\text{DNS}} = \texttt{domainLookupEnd} - \texttt{domainLookupStart}$ and website loading time using $T_{\text{Load}} = \texttt{loadEventEnd} - \texttt{fetchStart}$. We also measure FCP for user experience, especially on ad-supported websites.

Figure 11 reveals no substantial correlation between the number of queried servers and FCP performance. Performance penalties remain close to zero, suggesting that complex websites with numerous DNS requests effectively parallelize other tasks, thus minimizing impact. DoH/3 shows fewer outliers near zero



(a) Performance penalty in milliseconds per protocol



(b) Overall page loading times per protocol

Fig. 12: Website performance metrics for successfully measured cases across all protocols.

penalty, while DoQ exhibits more extreme values. Although most users experience negligible differences, certain websites encounter delays exceeding 2.5 s, which are noticeable and potentially disruptive. Therefore, given its lower incidence of extreme delays, DoH/3 may offer a better user experience.

Figure 12a compares performance differences and overall loading times (Figure 12b) for each protocol. Figure 12b shows minimal average loading time differences across DNS protocols, with similar 95th percentile intervals. The FCP to `onLoad` time gap remains consistent. The left bar chart confirms performance differences within $\pm 1\,\%$ of total load time, which is imperceptible to users. Since FCP contributes to `onLoad`, a shorter FCP implies reduced total loading time. While DoH/3 follows this trend, DoQ shows a larger `onLoad` average time spike, likely due to a few outlier websites with significantly longer load times (as shown in Figure 11). This delay occurs post-FCP, potentially due to inconsistent loading elements like advertisements. Surprisingly, websites using DoQ or DoH/3 load slightly faster than Do53, resulting in negative performance penalties. This contradicts earlier findings indicating that DoQ and DoH/3 have response times more than 200 % longer times than Do53. This suggests either enhanced packet loss recovery compensates for delays (unlikely in low-loss environments) or DNS response time doesn't strongly correlate with website load time within the observed range. The following section will examine website characteristics and their correlation with performance penalties to identify sensitivities to DNS protocol variations.

5.2 Impact of Website Complexity

Building on our prior analysis of DoQ and DoH/3 performance, this section examines why some websites experience greater performance impacts than others and why performance penalties tend to stabilize around zero as the number of DNS requests increases. Furthermore, we analyze potential correlations between webpage characteristics and performance variations across different DNS protocols.

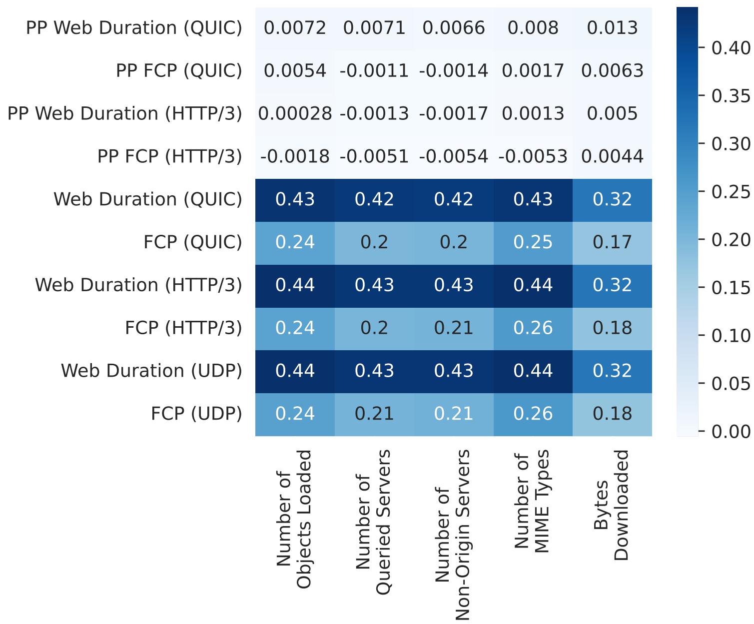


Fig. 13: Heatmap of the correlation between website complexity and performance across different DNS protocols.

The web complexity experiment, probed 1 million domains and identified 719,281 active websites. In a follow-up analysis, only 572,345 of these websites were accessible. This discrepancy suggests that many sites experienced temporary failures, maintenance issues, or permanent takedowns, especially among gambling, adult content, and streaming websites, which may face legal concerns. We found that a median webpage required downloading 1.2 MB across 42 resources, involving seven different servers. This results in seven DNS resolutions, with five typically being external to the domain owner. The median load time for all DNS protocols was approximately 0.9 s. To understand the relationship between website complexity and performance penalties, we calculated correlation coefficients and visualized them in heatmaps (Figure 13). We found weak correlations ($\leq$0.45) between complexity features and performance penalties. This suggests that complexity attributes do not significantly influence DoH/3 or DoQ performance penalties for either FCP or `onLoad`, likely due to efficient parallelization of DNS query durations (25 ms to 93 ms) within browser tasks. However, a positive correlation exists between complexity metrics and total load time (`fetchStart` to `onLoad`). This indicates increased loaded objects, queried servers, and resource types extend page load times. Interestingly, total website size has a minor impact. While FCP remains unaffected mainly, total load time increases as more resources are fetched before the `onLoad` event. Furthermore,

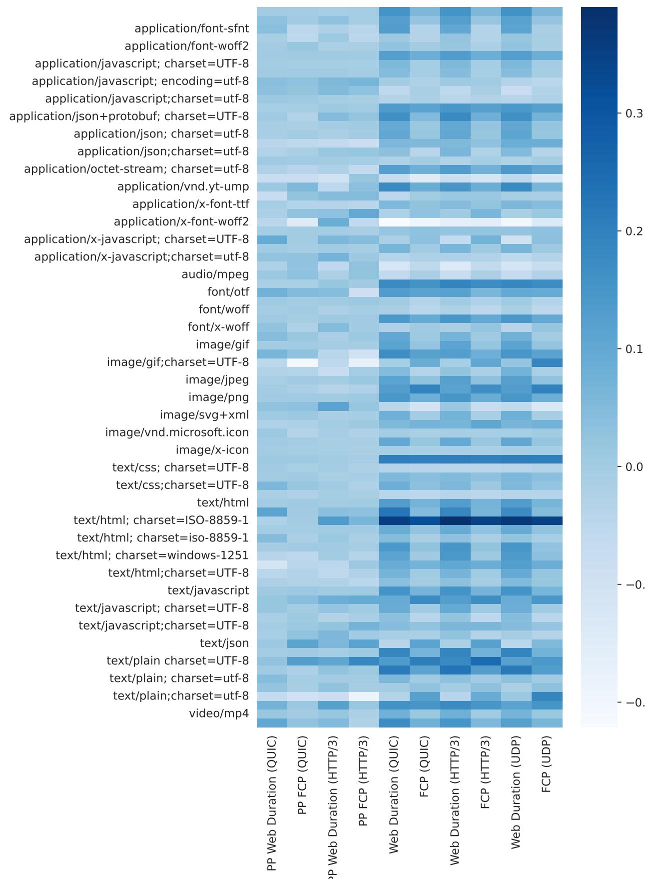


Fig. 14: Heatmap of the correlation between MIME types, DNS performance, and website loading times (*PP* stands for performance penalty).

the correlation remains consistent across different DNS protocols, suggesting minimal DNS impact in low-latency environments.

Impact of MIME Types Our findings show that performance penalties do not depend on the number of MIME types, we now examine the relationship between specific MIME types and their impact on performance penalties and loading times, as illustrated in Figure 14. We focused on MIME types appearing over 100 times, resulting in 82 valid types, and analyzed the correlation among the 40 most frequent ones. The correlation scale ranged from −0.2 to 0.4, indicating generally weak correlations. Specifically, the performance-related rows showed correlation coefficients between −0.2 and 0.3, lacking consistency across different performance metrics.

6 Conclusion

This study conducted three integral measurements to evaluate the adoption and performance implications of DNS protocols. First, we assessed the prevalence of resolvers supporting QUIC, which significantly enhances the performance of DoQ and DoH/3. Second, we examined how different DNS protocols influence query times and, consequently, webpage load speeds. Third, we analyzed the relationship between webpage characteristics and performance effects when applying DoE protocols. While DoE introduces a measurable "performance penalty" in terms of DNS response times, our results indicate that the overall impact on web performance is negligible on average. This suggests that initial concerns regarding DoE usage may be overstated when considering end-to-end webpage load metrics. We conclude by summarizing our research questions (see section 1):

RQ1: Nearly all DoQ resolvers (93 %) support session resumption, with two-thirds also endorsing 0-RTT. By comparison, only 65 % of DoH/3 resolvers support session resumption. Although we could not fully assess 0-RTT support for DoH/3 due to stub resolver limitations, the observed 66 % support in DoQ resolvers reflects a substantial adoption of QUIC features since 2022 [37].

RQ2: Despite DoE protocols significantly lengthening DNS query times, this increase typically does not translate into slower overall website loading. DoH/3 exhibits more consistent loading times than DoQ, performing better on both median and average metrics. These findings imply that DNS queries operate largely concurrently with other browser activities. However, the impact may differ in high-latency or packet-loss environments, and our evaluation did not incorporate 0-RTT, session resumption, or DNS caching, which could further affect results.

RQ3: Our analysis considering factors such as number of loaded objects, queried servers, website size, and MIME type distributions found no significant correlation between these webpage characteristics and the performance penalty induced by DoE. Our results demonstrate that while encrypted DNS protocols impose some overhead on DNS response times, they do not meaningfully degrade overall webpage load performance under typical conditions. This supports the broader adoption of privacy-enhancing DoE protocols without sacrificing user experience.

References

1. Allman, M., Paxson, V.: Issues and etiquette concerning use of shared measurement data. In: Dovrolis, C., Roughan, M. (eds.) Proceedings of the 7th ACM SIGCOMM Internet Measurement Conference, IMC 2007, San Diego, California, USA, October 24-26, 2007. pp. 135–140. ACM (2007). https://doi.org/10.1145/1298306.1298327, https://doi.org/10.1145/1298306.1298327
2. Basalla, M., Schneider, J., Luksik, M., Jaakonmäki, R., Vom Brocke, J.: On latency of e-commerce platforms. Journal of Organizational Computing and Electronic Commerce **31**(1), 1–17 (2021), publisher: Taylor & Francis

3. Benjamin, D.: TLS 1.3 0-RTT (Sep 2022), https://chromestatus.com/feature/5447945241493504
4. Blechschmidt, B.: GitHub — blechschmidt/massdns: A high-performance DNS stub resolver for bulk lookups and reconnaissance (subdomain enumeration) (2016), https://github.com/blechschmidt/massdns/
5. Butkiewicz, M., Madhyastha, H.V., Sekar, V.: Understanding website complexity: measurements, metrics, and implications. In: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference. pp. 313–328 (2011)
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 Internet Measurement Conference. pp. 15–21. ACM, Amsterdam Netherlands (Oct 2019). https://doi.org/10.1145/3355369.3355575, https://dl.acm.org/doi/10.1145/3355369.3355575
7. Canonical: dockerhub - ubuntu/bind9, https://hub.docker.com/r/ubuntu/bind9/
8. Cerf, V.G.: Guidelines for internet measurement activities. RFC **1262**, 1–3 (1991). https://doi.org/10.17487/RFC1262, https://doi.org/10.17487/RFC1262
9. Chhabra, R., Murley, P., Kumar, D., Bailey, M., Wang, G.: Measuring DNS-over-HTTPS performance around the world. In: Proceedings of the 21st ACM Internet Measurement Conference. pp. 351–365. ACM, Virtual Event (Nov 2021). https://doi.org/10.1145/3487552.3487849, https://dl.acm.org/doi/10.1145/3487552.3487849
10. Cook, S., Mathieu, B., Truong, P., Hamchaoui, I.: QUIC: Better for what and for whom? In: 2017 IEEE International Conference on Communications (ICC). pp. 1–6. IEEE, Paris, France (May 2017). https://doi.org/10.1109/ICC.2017.7997281, http://ieeexplore.ieee.org/document/7997281/
11. Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., Polk, W.T.: Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile. RFC **5280**, 1–151 (2008). https://doi.org/10.17487/RFC5280, https://doi.org/10.17487/RFC5280
12. Cotton, M., Vegoda, L.: Special use ipv4 addresses. RFC **5735**, 1–10 (2010). https://doi.org/10.17487/RFC5735, https://doi.org/10.17487/RFC5735
13. Dickinson, S., Gillmor, D.K., Reddy, T.: Usage profiles for DNS over TLS and DNS over DTLS. RFC **8310**, 1–27 (2018). https://doi.org/10.17487/RFC8310, https://doi.org/10.17487/RFC8310
14. Dierks, T., Rescorla, E.: The transport layer security (TLS) protocol version 1.2. RFC **5246**, 1–104 (2008). https://doi.org/10.17487/RFC5246, https://doi.org/10.17487/RFC5246
15. Durumeric, Z., Wustrow, E., Halderman, J.A.: Zmap: Fast internet-wide scanning and its security applications. In: King, S.T. (ed.) Proceedings of the 22th USENIX Security Symposium, Washington, DC, USA, August 14-16, 2013. pp. 605–620. USENIX Association (2013), https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/durumeric
16. Electronic Frontier Foundation: Certbot, https://certbot.eff.org/
17. Encrypt, L.: Free ssl/tls certificates, https://letsencrypt.org/de/
18. Evans, C., Palmer, C., Sleevi, R.: Public key pinning extension for HTTP. RFC **7469**, 1–28 (2015). https://doi.org/10.17487/RFC7469, https://doi.org/10.17487/RFC7469
19. Fariselli, P., Oughton, C., Picory, C., Sugden, R.: Electronic commerce and the future for SMEs in a global market-place: Networking and public policies. Small Business Economics **12**, 261–275 (1999), publisher: Springer

20. García, S., Hynek, K., Vekshin, D., Čejka, T., Wasicek, A.: Large Scale Measurement on the Adoption of Encrypted DNS (2021). https://doi.org/10.48550/ARXIV.2107.04436, https://arxiv.org/abs/2107.04436, version Number: 1
21. Gasser, O., Scheitle, Q., Gebhard, S., Carle, G.: Scanning the ipv6 internet: Towards a comprehensive hitlist. In: Botta, A., Sadre, R., Bustamante, F.E. (eds.) Traffic Monitoring and Analysis - 8th International Workshop, TMA 2016, Louvain la Neuve, Belgium, April 7-8, 2016. IFIP (2016), http://dl.ifip.org/db/conf/tma/tma2016/tma2016-final51.pdf
22. Gillmor, D.K., Salazar, J., Hoffman, P.: Unilateral opportunistic deployment of encrypted recursive-to-authoritative DNS. RFC **9539**, 1–24 (2024). https://doi.org/10.17487/RFC9539, https://doi.org/10.17487/RFC9539
23. van der Ham, J.: Ethics and internet measurements. In: 2017 IEEE Security and Privacy Workshops, SP Workshops 2017, San Jose, CA, USA, May 25, 2017. pp. 247–251. IEEE Computer Society (2017). https://doi.org/10.1109/SPW.2017.17, https://doi.org/10.1109/SPW.2017.17
24. Hoffman, P.E., McManus, P.: DNS queries over HTTPS (doh). RFC **8484**, 1–21 (2018). https://doi.org/10.17487/RFC8484, https://doi.org/10.17487/RFC8484
25. Hoffmann, F., Bajpai, V., ververis, v.: The future of dns privacy: A comparison of dns over quic and dns over http/3 (Dec 2025). https://doi.org/10.5281/zenodo.17860118, https://doi.org/10.5281/zenodo.17860118
26. Hounsel, A., Schmitt, P., Borgolte, K., Feamster, N.: Can Encrypted DNS Be Fast? In: Hohlfeld, O., Lutu, A., Levin, D. (eds.) Passive and Active Measurement, vol. 12671, pp. 444–459. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-72582-2_26, https://link.springer.com/10.1007/978-3-030-72582-2_26, series Title: Lecture Notes in Computer Science
27. Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., Hoffman, P.E.: Specification for DNS over Transport Layer Security (TLS). Request for Comments RFC 7858, Internet Engineering Task Force (May 2016). https://doi.org/10.17487/RFC7858, https://datatracker.ietf.org/doc/rfc7858, num Pages: 19
28. Hu, Z., Zhu, L., Heidemann, J.S., Mankin, A., Wessels, D., Hoffman, P.E.: Specification for DNS over transport layer security (TLS). RFC **7858**, 1–19 (2016). https://doi.org/10.17487/RFC7858, https://doi.org/10.17487/RFC7858
29. Huitema, C., Dickinson, S., Mankin, A.: DNS over dedicated QUIC connections. RFC **9250**, 1–27 (2022). https://doi.org/10.17487/RFC9250, https://doi.org/10.17487/RFC9250
30. Internet Systems Consortium Inc.: Bind 9 - isc.org, https://www.isc.org/bind/
31. Iyengar, J., Thomson, M.: QUIC: A udp-based multiplexed and secure transport. RFC **9000**, 1–151 (2021). https://doi.org/10.17487/RFC9000, https://doi.org/10.17487/RFC9000
32. Josefsson, S.: The base16, base32, and base64 data encodings. RFC **4648**, 1–18 (2006). https://doi.org/10.17487/RFC4648, https://doi.org/10.17487/RFC4648
33. Kim, D.W., Zhang, J.: You Are How You Query: Deriving Behavioral Fingerprints from DNS Traffic. In: Thuraisingham, B., Wang, X., Yegneswaran, V. (eds.) Security and Privacy in Communication Networks, vol. 164, pp. 348–366. Springer International Publishing, Cham (2015). https://doi.org/10.1007/978-3-319-28865-9_19, http://link.springer.com/10.1007/978-3-319-28865-9_19, series Title: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering

34. Kinnear, E., McManus, P., Pauly, T., Verma, T., Wood, C.A.: Oblivious DNS over HTTPS. RFC **9230**, 1–19 (2022). https://doi.org/10.17487/RFC9230, https://doi.org/10.17487/RFC9230
35. Kirchler, M., Herrmann, D., Lindemann, J., Kloft, M.: Tracked Without a Trace: Linking Sessions of Users by Unsupervised Learning of Patterns in Their DNS Traffic. In: Proceedings of the 2016 ACM Workshop on Artificial Intelligence and Security. pp. 23–34. ACM, Vienna Austria (Oct 2016). https://doi.org/10.1145/2996758.2996770, https://dl.acm.org/doi/10.1145/2996758.2996770
36. Kosek, M., Doan, T.V., Granderath, M., Bajpai, V.: One to Rule Them All? A First Look at DNS over QUIC. In: Hohlfeld, O., Moura, G., Pelsser, C. (eds.) Passive and Active Measurement, vol. 13210, pp. 537–551. Springer International Publishing, Cham (2022). https://doi.org/10.1007/978-3-030-98785-5_24, https://link.springer.com/10.1007/978-3-030-98785-5_24, series Title: Lecture Notes in Computer Science
37. Kosek, M., Schumann, L., Marx, R., Doan, T.V., Bajpai, V.: DNS privacy with speed?: evaluating DNS over QUIC and its impact on web performance. In: Proceedings of the 22nd ACM Internet Measurement Conference. pp. 44–50. ACM, Nice France (Oct 2022). https://doi.org/10.1145/3517745.3561445, https://dl.acm.org/doi/10.1145/3517745.3561445
38. Kührer, M., Hupperich, T., Bushart, J., Rossow, C., Holz, T.: Going wild: Large-scale classification of open DNS resolvers. In: Cho, K., Fukuda, K., Pai, V.S., Spring, N. (eds.) Proceedings of the 2015 ACM Internet Measurement Conference, IMC 2015, Tokyo, Japan, October 28-30, 2015. pp. 355–368. ACM (2015). https://doi.org/10.1145/2815675.2815683, https://doi.org/10.1145/2815675.2815683
39. Learmonth, I.R., Knodel, M., Grover, G.: Guidelines for Performing Safe Measurement on the Internet. Internet-Draft draft-irtf-pearg-safe-internet-measurement-10, Internet Engineering Task Force (Jul 2024), https://datatracker.ietf.org/doc/draft-irtf-pearg-safe-internet-measurement/10/, work in Progress
40. Li, R., Liu, B., Lu, C., Duan, H., Shao, J.: A Worldwide View on the Reachability of Encrypted DNS Services. In: Proceedings of the ACM Web Conference 2024. pp. 1193–1202. ACM, Singapore Singapore (May 2024). https://doi.org/10.1145/3589334.3645539, https://dl.acm.org/doi/10.1145/3589334.3645539
41. LTD, S.: Top websites ranking (12 2024), https://www.similarweb.com/top-websites/
42. Lu, C., Liu, B., Duan, H., Xing, Y., Li, R., Sun, J.: Open Encrypted DNS Servers (Apr 2024), https://port-53.info/data/open-encrypted-dns-servers/
43. 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 Internet Measurement Conference. pp. 22–35. ACM, Amsterdam Netherlands (Oct 2019). https://doi.org/10.1145/3355369.3355580, https://dl.acm.org/doi/10.1145/3355369.3355580
44. Mao, J., Rabinovich, M., Schomp, K.: Assessing support for dns-over-tcp in the wild. In: Hohlfeld, O., Moura, G.C.M., Pelsser, C. (eds.) Passive and Active Measurement - 23rd International Conference, PAM 2022, Virtual Event, March 28-30, 2022, Proceedings. Lecture Notes in Computer Science, vol. 13210, pp. 487–517. Springer (2022). https://doi.org/10.1007/978-3-030-98785-5_22, https://doi.org/10.1007/978-3-030-98785-5_22
45. Mockapetris, P.V.: Domain names - concepts and facilities. RFC **1034**, 1–55 (1987). https://doi.org/10.17487/RFC1034, https://doi.org/10.17487/RFC1034

46. Mockapetris, P.V.: Domain names - implementation and specification. RFC **1035**, 1–55 (1987). https://doi.org/10.17487/RFC1035, https://doi.org/10.17487/RFC1035
47. Mozilla: Early-Data - HTTP (Nov 2024), https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Early-Data
48. Nah, F.F.H.: A study on tolerable waiting time: how long are web users willing to wait? Behaviour & Information Technology **23**(3), 153–163 (2004), publisher: Taylor & Francis
49. Narayanan, A., Zevenbergen, B.: No encore for encore? ethical questions for web-based censorship measurement. SSRN Electronic Journal (2015). https://doi.org/10.2139/ssrn.2665148, http://dx.doi.org/10.2139/ssrn.2665148
50. Pages, L.M.: pipe(7) (5 2024), https://man7.org/linux/man-pages/man7/pipe.7.html
51. Plonka, D., Berger, A.W.: Temporal and spatial classification of active ipv6 addresses. In: Cho, K., Fukuda, K., Pai, V.S., Spring, N. (eds.) Proceedings of the 2015 ACM Internet Measurement Conference, IMC 2015, Tokyo, Japan, October 28-30, 2015. pp. 509–522. ACM (2015). https://doi.org/10.1145/2815675.2815678, https://doi.org/10.1145/2815675.2815678
52. Pochat, V.L., Goethem, T.v., Tajalizadehkhoob, S., Korczynski, M., Joosen, W.: Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In: 26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019. The Internet Society (2019), https://www.ndss-symposium.org/ndss-paper/tranco-a-research-oriented-top-sites-ranking-hardened-against-manipulation/
53. Qualys, Inc.: Qualys ssl labs - ssl pulse, https://www.ssllabs.com/ssl-pulse/
54. Rekhter, Y., Moskowitz, B.G., Karrenberg, D., de Groot, G.J., Lear, E.: Address allocation for private internets. RFC **1918**, 1–9 (1996). https://doi.org/10.17487/RFC1918, https://doi.org/10.17487/RFC1918
55. Rempel, G.: Defining standards for web page performance in business applications. In: Proceedings of the 6th ACM/SPEC International Conference on Performance Engineering. pp. 245–252 (2015)
56. Rescorla, E.: HTTP over TLS. RFC **2818**, 1–7 (2000). https://doi.org/10.17487/RFC2818, https://doi.org/10.17487/RFC2818
57. Rescorla, E.: The transport layer security (TLS) protocol version 1.3. RFC **8446**, 1–160 (2018). https://doi.org/10.17487/RFC8446, https://doi.org/10.17487/RFC8446
58. Richter, P., Smaragdakis, G., Plonka, D., Berger, A.W.: Beyond counting: New perspectives on the active ipv4 address space. In: Gill, P., Heidemann, J.S., Byers, J.W., Govindan, R. (eds.) Proceedings of the 2016 ACM on Internet Measurement Conference, IMC 2016, Santa Monica, CA, USA, November 14-16, 2016. pp. 135–149. ACM (2016), http://dl.acm.org/citation.cfm?id=2987473
59. Rüth, J., Poese, I., Dietzel, C., Hohlfeld, O.: A First Look at QUIC in the Wild. In: Beverly, R., Smaragdakis, G., Feldmann, A. (eds.) Passive and Active Measurement, vol. 10771, pp. 255–268. Springer International Publishing, Cham (2018). https://doi.org/10.1007/978-3-319-76481-8_19, http://link.springer.com/10.1007/978-3-319-76481-8_19, series Title: Lecture Notes in Computer Science
60. Scheitle, Q., Hohlfeld, O., Gamba, J., Jelten, J., Zimmermann, T., Strowes, S.D., Vallina-Rodriguez, N.: A long way to the top: Significance, structure, and stability of internet top lists. In: Proceedings of the Internet Measurement Conference 2018,

IMC 2018, Boston, MA, USA, October 31 - November 02, 2018. pp. 478–493. ACM (2018), https://dl.acm.org/citation.cfm?id=3278574
61. Schumann, L.: A Regional Analysis of DNS over QUIC and its Impact on Applications. Ma.S. thesis, Technical University of Munich (2022)
62. Sengupta, J., Kosek, M., Fries, J., Dikshit, P., Bajpai, V.: Web Privacy By Design: Evaluating Cross-layer Interactions of QUIC, DNS and H/3. In: 2023 IFIP Networking Conference (IFIP Networking). pp. 1–9. IEEE, Barcelona, Spain (Jun 2023). https://doi.org/10.23919/IFIPNetworking57963.2023.10186362, https://ieeexplore.ieee.org/document/10186362/
63. Sheffer, Y., Holz, R., Saint-Andre, P.: Summarizing known attacks on transport layer security (TLS) and datagram TLS (DTLS). RFC **7457**, 1–13 (2015). https://doi.org/10.17487/RFC7457, https://doi.org/10.17487/RFC7457
64. Sheffer, Y., Saint-Andre, P., Fossati, T.: Recommendations for secure use of transport layer security (TLS) and datagram transport layer security (DTLS). RFC **9325**, 1–34 (2022). https://doi.org/10.17487/RFC9325, https://doi.org/10.17487/RFC9325
65. StatCounter: Internet browser market share 2012-2024 (Sep 2024), https://www.statista.com/statistics/268254/market-share-of-internet-browsers-worldwide-since-2009/
66. Thomson, M., Turner, S.: Using TLS to secure QUIC. RFC **9001**, 1–52 (2021). https://doi.org/10.17487/RFC9001, https://doi.org/10.17487/RFC9001
67. Wang, X.S., Balasubramanian, A., Krishnamurthy, A., Wetherall, D.: Demystifying page load performance with WProf. In: Proceedings of the 10th USENIX Conference on Networked Systems Design and Implementation. pp. 473–486. nsdi'13, USENIX Association, USA (2013), event-place: Lombard, IL
68. Weiss, Y., Rosenthal, N., Grigorik, I., Reifsteck, T., Jain, A., Mann, J., Wang, Z., Quach, A.: Navigation and resource Timing (2024), https://developer.mozilla.org/en-US/docs/Web/Performance/Navigation_and_resource_timings
69. World Wide Web Consortium: Resource timing. https://www.w3.org/TR/resource-timing/ (2025), candidate Recommendation Draft