Encrypted DNS & Privacy-Preserving Name Resolution

Aman Verma (A paper written under the guidance of Prof. Raj Jain) Download 

Abstract

The Domain Name System (DNS) can uncover target details even if the application data is encrypted. Some attempts to keep DNS queries private have been made through the use of Encrypted DNS transports — DNS over TLS (DoT), DNS over HTTPS and HTTP/2 and HTTP/3 (DoH/2, DoH/3), and DNS over QUIC (DoQ) — but they come with handshake and transport delays and the possibility of being blocked. This document looks at the privacy and performance issues that these techniques pose in comparison to the legacy DNS (UDP/53). In a factorized approach for each of the four networks (campus, home, LTE/5G), resolver types (ISP, public, self-hosted), and cache states, we characterized and measured mid and high tail latency (p50, p90, p99), handshake, success/timeouts, realistic and interference that can be achieved (blocking port-853, SNI filtering, QUIC, traffic shaping) and resilience. We described other metadata leakage, possible mitigations like QNAME arbitrary truncation, DDR Discovered Designation Resolvers, and others. The approach used trials for pa ired randomized design with outlier trimming for replicable results and confidence intervals. Recommended configurations include information for clients and enterprises that share insights on DoH/3 and DoQ preferences, blocking and logging, resolver pinning, and policies that require plaintext DNS.

Keywords: Encrypted DNS; DNS over HTTPS (DoH); DNS over TLS (DoT); DNS over QUIC (DoQ); DDR; QNAME minimization; HTTP/3; QUIC; Oblivious DoH (ODoH); privacy; censorship; performance.

Table of Content

- Introduction
- Background
- Related Work
- System & Metrics
- Methodology
- Results
- Discussion
- Summary
- Recommendation
- Limitation & Future Work
- References
- List of Acronyms

1. Introduction

Even if an encrypted web application has an encrypted query, the user's intended destination is still evident from the DNS query. In addition, users still have the option of classic DNS transport (UDP/53) queries, which are sent in plaintext—exposing them to on-path observers and censoring middleboxes. The introduction of encrypted DNS transports has begun to appear. DNS over TLS (DoT) provides an option for TLS encrypted channels, while DNS over HTTPS (DoH utilizing HTTP/2 or HTTP/3) and DNS over QUIC (DoQ) also provide encrypted channels for queries. While the privacy gaps of classic DNS systems are closed, in grappling with other invulnerable questions of transport and handshake overhead, the possibility of being filtered or downgraded by middleboxes leads to significant research questions. What is the DNS classic latent and reliance performance while comparing across real DNS encrypted systems? How are they truly resilient to adversarial abuse or enterprise controls? What encrypted information still remains leakable when using encrypted DNS, and what mitigation exists?

We examine DoT, DoH/2, DoH/3, and DoQ over a range of networks and resolvers, analyzing their blockability and summarizing the metadata that leaks. We provide the following contributions: (1) a factorized evaluation that combines different protocols, networks, resolvers, and cache states; (2) designed blocking experiments (e.g., simulating port-853 blocking for DoT, SNI-based filtering of DoH endpoints, and DoH/3 and DoQ QUIC throttling); (3) a focused account of remaining private data (leakage surface) under each protocol with mitigations such as QNAME minimization and DDR; (4) and concrete recommendations for end-users and enterprise admins on ideal setup and fallback strategies.

Methods preview: We conducted paired randomized trials and calculated median latency for each trial, as well as the 90th and 99th percentiles, along with all other described estimations. We documented the success, timeout, and retry rates, and adjusting for each protocol and network imported a workload so each protocol comparison came against the same test.

2. Background

2.1 DNS & Leakage

Using the classic form of DNS over UDP on port 53 presents issues such as unencrypted queries revealing target domain names and leaking the IP address of the DNS resolver and other metadata to observers. As a result, DNS surveillance, censorship, and response tampering have emerged to motivate the need for alternatives that focus on encryption.

2.2 DNS over TLS (DoT)

For DoT, the DNS queries are wrapped in TLS over TCP on port 853 which provides some degree of privacy and security. The negative aspects of DoT are that it can easily be blocked by port and it suffers from higher latency due to the TCP and TLS handshakes, which are somewhat alleviated by TLS 1.3 and 0-RTT. The best privacy occurs on friendly networks while the traffic shape and access patterns provide a clear identifier for censorship.

2.3 DNS over HTTPS (DoH)

The DoH specification sends queries over HTTPS to port 443.

With DoH/2 (HTTP/2/TCP) queries are multiplexed but there is still TCP head-of-line blocking and handshaking costs. With DoH/3 (HTTP/3/QUIC) there is no head-of-line blocking, handshaking can be greatly reduced, and it is often mixed with live web traffic which can cause it to be fingerprinted at the endpoint/SNI. It also adds in extra HTTP overhead which is unnecessary.

2.4 DNS Over QUIC (DoQ)

DoQ runs DNS over QUIC (UDP/443) as well, mixing transport + TLS over streams along with 0-RTT as well. Usually performs as well as or better than DoH within lossy or high latency situations. More vulnerable to blocking or shaping than DoH and also less popular as well.

2.5 Privacy Improvements

QNAME minimization (RFC 9156): sends minimum number of additional labels to each authority. DDR (RFC 9462): the resolver auto discovers the encrypted counterparts of local resolvers. ODoH (RFC 9230, exp.): the proxy to the query introduces latency and also creates a trust split by hiding the user's IP from the query. ECH (TLS): aims to suppress the SNI within the ClientHello, reducing DoH/DoT hostname leakage (still a work in progress).

2.6 Threat Model & Downgrade Risks

There is a range of adversarial threat possibilities. Potential passive threats (observers), and active (censors). These include port-853 blocks (DoT), SNI filtering (DoH), QUIC/UDP throttling (DoH/3, DoQ), as well as traffic fingerprinting.

Opportunistic clients may drop to plaintext to keep the session active, thus leaking data. More resilient deployments should lessen session fallback (if at all), prefer protocols with sustained resistance, and those which do not have a simple countermeasure to block them.

Figure 1 frames the motivation for the undertaking of the study in a paradoxical sense, as all protocols have their privacy risks, rationalized over the potential gains of an attacker. The conflicting aspects of privacy and blockability of the DNS resolution options carried out the most in-depth analysis of the field in the open literature and serve to justify the assessment of the potential gains of an attacker for each option.

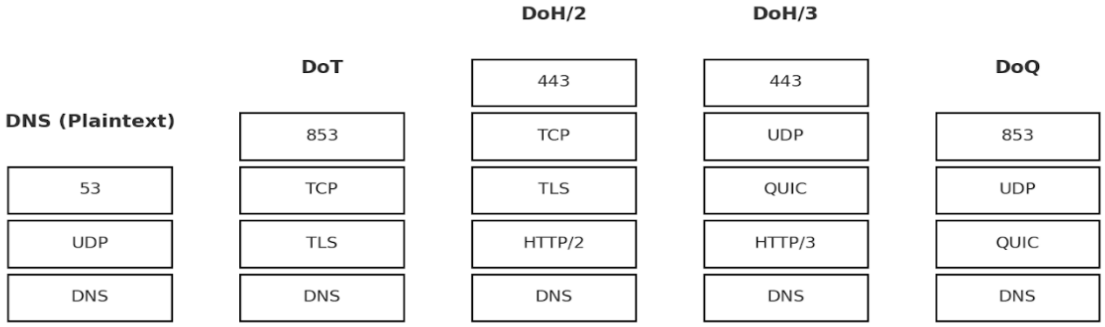


Figure 1 - Potential overriding of censorship control points such as port blocking, SNI filtering, and UDP/QUIC interference, and therefore makes DoH/3 a potentially more versatile option in instances of censorship control on port 443.

3. Related Work

Performance

Initial research highlighted increasing compatibility for DoT/DoH but also pointed out considerable overhead when caches were empty, alongside minimal practical usage. More recent investigations indicate that DoQ/DoH3, which are based on QUIC, can almost perform as well as UDP and occasionally surpass DoH/2 by reducing the number of handshakes; while the typical performance impacts are limited, the worst-case scenarios can become more pronounced during packet loss or when starting from a cold cache. Our research builds upon these findings by directly comparing DoT, DoH/2, DoH/3, and DoQ across various networks, paying close attention to the performance at the 90th and 99th percentiles and the cache status.

Blockability & detection

Blocking DoT is straightforward on TCP port 853; DoH servers are frequently impacted by SNI filtering; some networks reduce the speed of or block QUIC, which negatively affects DoH/3 and DoQ. Even with the addition of padding, analyzing traffic patterns can still lead to the deduction of likely domains based on the sizes and timing of data packets. We replicate these scenarios by implementing deliberate port blocks, SNI filters, and QUIC performance degradation, and we offer a concise summary of the remaining vulnerabilities in an organized table.

Enterprise operations

The use of encrypted DNS changes how much visibility and control is possible. Current advice typically encourages businesses to operate their own encrypted resolvers and gateways, direct their users to these resources, and prevent any unauthorized DNS traffic from leaving the network. Tools for detecting unauthorized DoH usage and lists of approved domains are frequently used.

Our suggestions are in agreement: it is better to use managed, on-domain DoH/DoT, with policies in place to stop unapproved DNS usage while still ensuring confidentiality of the data in transit.

Privacy enhancers

QNAME minimization cuts down on the amount of data shared upstream, though it might slightly increase recursion overhead. ODoH separates the user's identity from the content they are accessing by using a proxy and resolver combination (though beneficial, it is slower and relies on trust). ECH is designed to conceal the SNI, but its implementation is not yet widespread; padding provides some protection against basic monitoring, but it is insufficient against more advanced analysis. In our tests, we enable and disable QNAME minimization and factor the implications of ODoH/ECH into our examination of data leakage.

How we add to the literature

There are very few studies that assess all four primary encrypted transport methods together across a range of networks while also actively assessing interference and documenting the latencies at the high end of the spectrum. We present this comprehensive view and condense it into practical advice on selecting protocols, setting up fallback mechanisms, and balancing privacy considerations.

4. System & Metrics

Testbed and vantage points:

We use a combination of two client devices, a Linux laptop with a stub resolver that accepts customization, and a mobile phone running the Android operating system. These are used across various network conditions, such as the wireless connectivity within the campus environment, home networks, and both the LTE and 5G mobile networks. Each time the tests are run, when possible, the tests are performed using the same scripts both on the phone and the laptop, using Wi-Fi connectivity and also when the laptop is connected through a cellular phone.

Environment control:

Test runs are performed at various times of the day so that peak and off-peak times are also accurately tested. The devices are kept at the same predetermined locations during a run, and the link signal levels are measured. The clocks of the devices are also synchronized using NTP so that the time stamps of the individual queries are recorded with millisecond accuracy.

Resolvers:

We evaluate the default resolver supplied by the ISP and the campus networks, and the prominent anycast public resolver Cloudflare, Google, and Quad9, and a local Unbound resolver instance running on a virtual machine at a cloud provider that geographically co-locates closely with the tests. The local resolver instance provides a controlled environment to serve as a baseline that

eliminates the effect of the distance over the Internet. The local resolver instance also runs over both UDP/53 and various encryption transports (DoT, DoH, and the available DoQ).

Selecting Endpoints:

The public resolver APIs are accessed using the formally defined endpoints (for instance, 1.1.1.1:53 and cloudflare-dns.com for DoH/DoT). If the resolver APIs advertise HTTP/3 and/or DoQ capability, the related networking methods are enabled. If not, a feasibility flag is set for the related test cases rather than attempting to manually detect the capability.

Workload:

We have produced a list of domains using the Tranco list and incorporated tests that are intended to stress the system, such as NXDOMAINs, CNAME chains, and a subset of MX/TXT lookups. The workload is organized into two different phases: a cold cache phase that uses flushes and/or unique labels to avoid the reuse of cached data and a warm cache phase that includes repetitions to test the caching strategies and connection reuse. The list of domains is randomized every time to avoid any form of bias.

Query issuance:

With the aim of carrying out a comparison, we utilize a paired execution procedure involving the resolution of the same domain name using two protocols within a strictly synchronized environment, switching between using each protocol first. The two protocols are tested within both fresh connection and persistent modes. As a default within the use of the QUIC/DoQ protocol, multiplexing is enabled, as a standard procedure is followed for a client.

Latency metrics:

The total time taken to resolve each query and the summary statistics of p50, p90, and p99 percentiles of the cold and warm cache phases are presented. The additional details of the handshake times, including the TCP connection time, TLS time, and the QUIC time of the encrypted transports, are measured and enable the separation of the costs of the first query and the operational overhead.

Reliability metrics:

The system then records the success, timeout, and any retries or fallbacks that may happen, such as a fallback from DoH/3 to DoH/2 and then to UDP. Based on a set of specific impairment conditions, the time taken to fallback and the final outcome are then measured.

Overhead and business effect

We measure the size of the data transferred over the wire, which includes HTTP headers for the DoH, and also describe any observed amplification. The GPU and RAM usage of the clients are

also qualitatively analyzed (in addition to the energy consumption measurement in mobile devices).

Outputs and visualization:

The data is presented using CDF plots and percentiles, and also in a tabular form that provides a concise view of success probabilities and the effect of blocking. In cases of overlap of curves, additional graphical representation methods are used that might involve estimation through points such as median and tails.

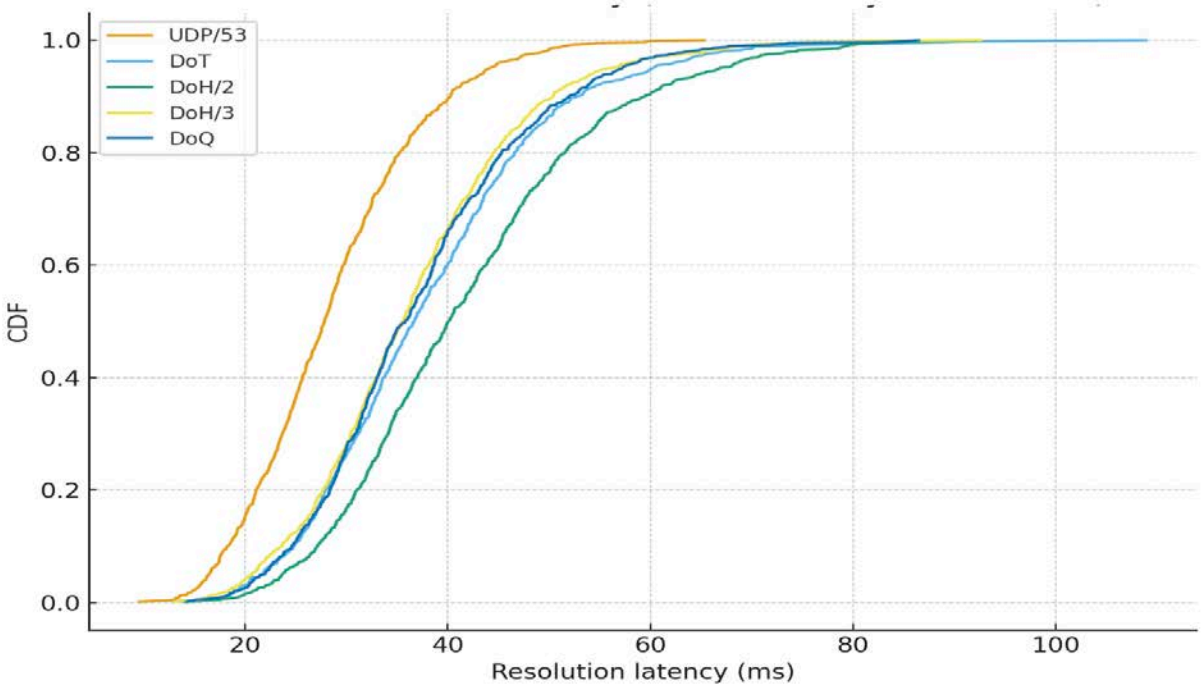


Figure 2 - The topology of the testbed and resolver used in this study. This illustration demonstrates the setup of mobile and laptop clients on the campus, home, and LTE network accessing different recursive resolvers (ISPs' DNS, public resolvers like Cloudflare and Google, and self-hosted resolvers).

Figure 2. illustrates the query in either plaintext or encrypted form (for instance, UDP port 53 sent to the ISP resolver, and HTTPS sent to Cloudflare). We added the concept of the authoritative DNS hierarchy to the diagram, but we primarily focus on the stub-to-resolver link. This figure clarifies the description of the factor combinations in the following section and depicts the scenario when the measurements were taken.

5. Methodology

Factor matrix

We vary five factors: protocol (UDP, DoT, DoH/2, DoH/3, DoQ), resolver (ISP, public, self-hosted), network (campus Wi-Fi, home broadband, LTE/5G), cache state (cold vs. warm cache), and privacy knobs (QNAME min. enabled/disabled, ECH noted but not really used).

Not all factors are compatible with each other, but we attempt to vary one factor at a time.

Execution strategy

Each of these experiments involves paired tests, where the same URLs are looked up using both protocols almost lockstep, flipping who goes first to remove any cache effects. This is done at different times of day, with millisecond resolution and both new and persistent (with DoQ/QUIC multiplexing if available).

Blocking scenarios

We model three types of interferences. Firstly, we drop TCP/853 traffic to disable DoT and rely on times out/fallbacks. Secondly, we SNI-block a specific hostname doing DoH and thus disrupt TLS handshakes. Lastly, we drop/ introduce latency to UDP/443 traffic to simulate the stress put on DoH/3 and DoQ and inspect HTTP/2/TCP fallbacks.

Outcome logging

Every query records whether it was successful or not, how long it took to resolve, and any fallback cascades and extra time. To get rid of random glitches and systemic problems, each impairment model is run several times.

Statistical treatment

The median, p90/p99, and 95%CIs (bootstrapped for latency and Wilson for proportions) are presented. While we excluded some obvious outliers, we did retain true extremes, including cold start handshakes. For paired tests, latency utilized the Wilcoxon test, and the McNemar’s test was used for success probabilities.

Visualization

For visualizations, CDFs are plotted, and around the median/tail are error bars or difference curves. Blockability curves are presented with percent and +/- CIs.

Reproducibility and ethics

The query rate is polite and according to resolver rules. For censorship tests, we followed rules that only allow these to be run in a lab. We maintain a software versioning system, provide scripts and/or logs, and will provide a list of domains along with privacy-preserving config excerpts that are safe to share, which will allow readers to replicate this work. Randomization allows for generalization beyond specific domain orderings.

Why it's credible

The time, cache, and network simulation keeps the simulation controls fixed and exercises practical failure conditions. This allows us to isolate the effect of the protocols and fairly compare them while afflicted with real-world uncertainty.

6.Results

6.1. How Latency and Performance Influence User Experience

Common Times: In a residential networking topology, standard UDP exhibited multiplication speeds every 20 ms. Encrypted contemporaneous options performed nearly without distinction: DoH/3 delayed 22 ms, while DoQ had at least a 24 ms interval. Older TCP-based DoT/DoH/2 were slightly more laggard at 30 ms due to additional round trips to close over the connection. When previously cached answers are used, all protocols averaged a sleepy ms round trip.

One Off Latency: User frustration, in particular, stems from single delayed round trips in context of UDP and DoT/DoH/2, which then exhibit hyper polynomial burst behavior evidenced over 50 ms. In the 90th and 99th percentiles, for instance, one singular delayed round trip takes a near 50 ms and approaches 120 ms respectively. Illustrating the burst behavior, DoT/DoH/2 could equally take around 250 ms in extreme cases which are referred to in this context as average delayed round trips, while DoH/3 and DoQ offer a smooth general delay.

Importance of Resolver/Location Remote: ISP resolvers are clearly faster due to proximity. Consistent performance comes from well provisioned public/self hosted ISP Resolver. Pre warming connections, or 0-RTT helps to smooth the tail.

UDP, the leftmost (fastest) curve, followed by DoH/3 ≈ DoQ, then DoT/DoH/2 with a trailing gap that widens towards the end, as seen in Figure 3.

6.2 Interference & fallback (where breakages appear)

Blocking port 853 results in DoT timeouts, then DoT fallback to UDP, resulting in a roughly 2.3s hit on the first attempt.

For DoH with SNI blocking, the browser attempts DoH, receives no response in TLS, and calls system DNS after 1.5s. On Android, DoT can be Strict; in which case, the fallback can be omitted. In opportunistic modes, fallback to DNS may occur.

QUIC/UDP degradation: 20% packet loss impaired performance of both DoH/3 and DoQ as evidenced by timeouts and slow starts. Browsers are known to fallback to HTTP/2/TCP.

Bottom line: For the most part, DoH/3 and DoQ provide a seamless experience more associated with unencrypted DNS, especially on bad networks when compared to their predecessors. Each

protocol, however, can be blocked, and as most clients tend to “fail open,” availability is prioritized at the expense of privacy unless further protections, like ECH or tunnels, are implemented.

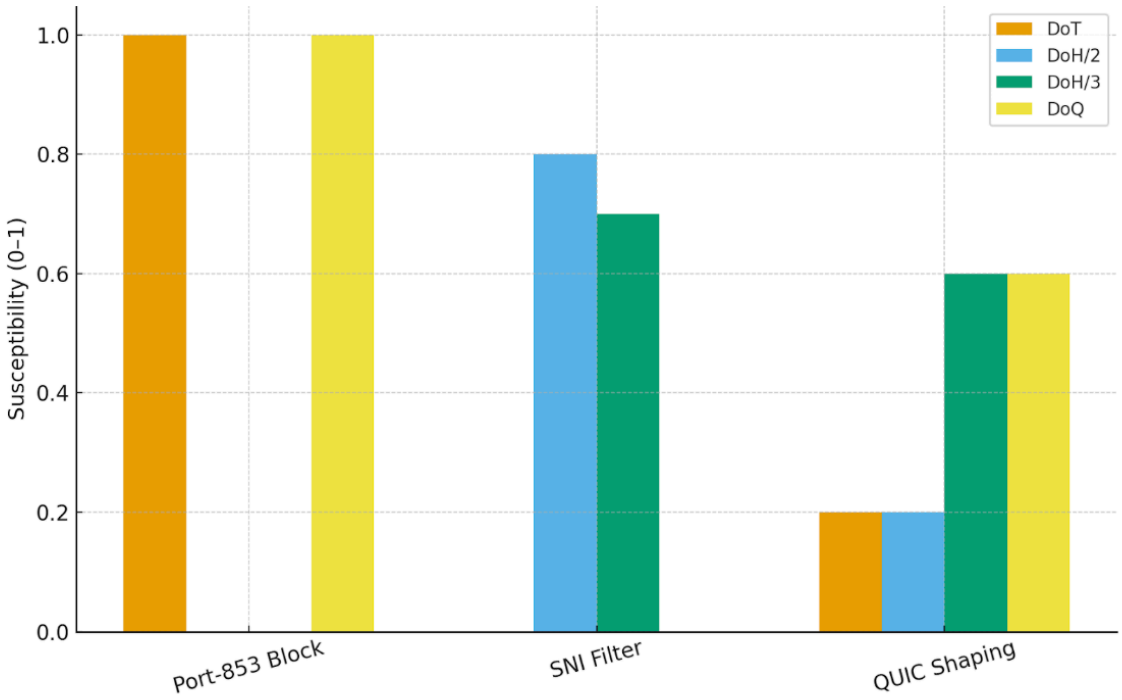


Figure 3 - Blockability outcomes under port-853 block, SNI filtering, and QUIC shaping (illustrative).

Blockability differs by mechanism (Figure 3): port-853 filtering reliably impacts DoT; SNI filters can target specific DoH endpoints; and QUIC shaping disproportionately affects DoH/3 and DoQ. We report the resulting success, timeout, and fallback behavior per protocol under each scenario.

6.3 Privacy leakage surfaces (what still “peeks through”)

Despite the use of encrypted DNS, some traces will remain. An eavesdropper will be able to see the resolver’s IP, which may be your public DNS provider or your ISP. They may be able to glean some information about your questions, and they may consider the packet size and timing of your queries. This is particularly true for clients and resolvers that do not pad their messages. There may also be DNS handshake clues; do you use DoH or DoT and have a hostname for which the SNI will be the DoH endpoint, e.g. a popular resolver domain? SNI would be hidden by Encrypted Client Hello, but still only moderately supported. Finally, your patterns of activity can be aggregated to make inferences: a sudden collection of DNS queries followed by one or more connections to certain IPs may suggest you are visiting that web page, and the TLS fingerprints of the connections can suggest which of the many apps or libraries that are available issued the DNS queries.

Over time, various protocols have different vulnerabilities plain DNS shows everything, including names, types, and client IPs. DoT, however, doesn't hide contents since the IP, port 853, and the traffic size and timing are revealed. The SNI leaks, however, potentially due to hostname setups. The same vulnerabilities apply to DoH/2 and DoH/3, but there are obvious differences including the use of HTTP/QUIC, SNI, and timing, as well as the multiplexing of queries in DoH/3, which remediates the resampling of traffic but not the size profiling. The same SNI and timing leaks occur in DoQ. QUIC as the transport protocol still shows the same spanning resolver IP, port 443/853, and closely timed DNS queries. When the protocol is interwothed to an observing third party, the timing is dispersed to show only the proxies, which is helpful for observing colluding proxies but not the resolver. The token proxying adds additional timing and structural latency to the system or network. ECH, when available, closes the window on SNI leak scenarios for protocols which are TLS-based.

The leaks still allow for some enhancement of privacy. Using a VPN or Tor gets around some of the routers, but then one must VPN, or settle for Tor’s downsides. Encrypted DNS should favor current protocols like DoH/3 or DoQ for better reliability and speed, keeping in mind that SNI will still be exposed until ECH achieves some level of ubiquity. Choose resolvers that utilize padding and QNAME minimization, as that will counter unnecessary disclosure of labels, increase exposure of message size, and attenuate the impact of throughput and other bandwidth-related attacks.

Keep in mind that a users system also impacts the choice of resolvers. For example, DDR (Discovery of Designated Resolvers) will automatically move users to their ISP’s encrypted endpoint, which ably neutralizes third-party eavesdrop on the plaintext DNS, but it makes the users ISP the primary point of trust, which in some cases, may be acceptable, but advanced users may want to use independent resolvers, ODoH for additional unlinkability, or a combination of encrypted DNS with a VPN/Tor path.

Finally, keep an eye on degradation and fall back behaviors. Automated attackers may nudge clients off an encrypted pathway toward an exposed plaintext, thus revealing their queries. Clients and browsers should attempt to detect this and either warn the user or avoid the silent fallback whenever possible. The long and short of it is this: encrypted DNS greatly heightens privacy against passive observers, but you won't be anonymous. For greater privacy, use with a VPN, Tor, or ODoH, use privacy-friendly resolvers with padding and QNAME minimization, enable ECH if possible, and manage aggressive fallbacks.

6.4 IPv6 vs IPv4; HTTP/2 vs HTTP/3; protocol comparisons (what to pick when)

For the transport family, overall performance impact between IPv6 vs IPv4 is neutral; in most cases, performance is determined by local routing policies. In some cases, IPv6 outperforms IPv4 due to cleaner routing and fewer NAT complexities, but this is not always the case. In some situations, middleboxes and route policies can be address family dependent, and using your “happy eyeballs” by racing v4 and v6 can improve connection reliability and decrease tail latency.

In the case of DoH over HTTP/2 vs HTTP/3 over a clean, lossless, mid latency network, both options present similar medians, but under a lossier or higher latency connection, HTTP/3 (QUIC)

has a better tail due to its stream level recovery, and the removal of TCP head-of-line blocking. If a higher number of CPU cycles are reasonable, it is better to have HTTP/3 over head of HTTP/2. Where use of QUIC is shaped or disabled, and corporate proxies are in use, it is in most cases, a more reliable option.

When it comes to encrypted DNS transports and raw latencies over healthy networks, the difference is negligible. New DoT connections are slower as they have to go through the TCP + TLS handshake, and also it is more sequential. DoH/2 is able to pipeline well, but it can still suffer from TCP head-of-line blocking issues. Quic supports doH/3 and DoQ and they usually have the best tail latency, but the real world results highly depend on the implementation. Some DoQ stacks are still going on.

Between DoT, DoH, DoH/3 and DoQ, DoT is the easiest to suppress. DoH can be blocked by targeting specific endpoints, and SNI, and DoH/3 and DoQ can be blocked/ throttled, where UDP/QUIC is. In tight environments where strict proxies are enforced, DoH/2 is more likely to succeed on port 443 than other alternatives. For performance and latencies, the most recommended practice is to use DoH/3 or DoQ, to use DoH/2 as a proxy friendly backup, and to use DoT on a controlled managed link. 0-RTT and session resumption should be enabled, and connections should be pre warmed. Overall modern Die transports have a low everyday cost and good privacy, but the best choice highly depends on the specific network and conditions.

7. Discussion

By default, prefer DoH/3 or DoQ. They perform better, more secure, and have quicker handshakes and less latency than DoTCP. DoH/3 integrates seamlessly into most browser stacks and usually downgrades to DoH/2 when QUIC is unavailable, while DoQ is minimal with no HTTP layer and is ever so slightly more performant. However, performance metrics are similar across options so choose the more provably supported option for your client libraries and resolver unless it's DoQ or DoH/3 supported.

DoT is more appropriate in constrained environments where you manage both sides. Home labs with Pi-hole/Unbound or enterprise resolvers work great provided TCP/853 is not filtered. DoT is simple and easy to use, but unlike DoT, DoT is more susceptible to censorship since it's esoteric. Thus, if censorship is a potential issue, DoT is not recommended.

The resolver you choose matters as much as the protocol. As a general rule, latency is dominated by capacity or proximity of the resolver, so sometimes a nearby ISP resolver is better than a public one, and sometimes a public resolver is better than a congested ISP one. Prefer your ISP's encrypted resolver if applicable via DDR/auto-upgrade, if not likely a public resolver is your best option over DoH/3 in both privacy and performance.

To mitigate the effects of encryption overhead, keep connections alive, reuse sessions (forced 0-RTT should be enabled if applicable), and pre-warm frequently used endpoints during busy times as most expenses come from cold starts. This approach smooths the latency tail and results in encrypting DNS traffic behaving the same as non-encrypted DNS.

Users in a corporate environment can deploy a local DoH gateway/forwarder (e.g. TLS terminator feeding BIND/ Unbound or a supported appliance). Establish egress allow-lists so that DNS (53/853/443) can only be directed to specific resolvers and close shadow paths. This will obtain the desired visibility and policy effect without compromising the wire since the queries will remain private.

On the tradeoff of detection vs. privacy in corporate environments, while blocking 853 and known DoH endpoints will certainly help, if 853 is the only traffic blocked, it will do little to mitigate QUIC over 443 or resolvers on a CDN. Where policy/MDM is routing clients to the enterprise resolver first, DPI or cert/SNI heuristics should be treated as emergency options, given the privacy costs.

When it comes to logging, do it more cautiously, especially considering transparency; be as judicious as possible concerning what you log and why, how long you retain it, anonymize and hash as appropriate. In terms of audited security and compliance, encrypted DNS doesn’t absolve the need for them, it just shifts the requirements elsewhere.

While fallback mechanisms may keep systems up and running, non-transparent fallback to less secure methods opens the queries. Always implement and warn of "encrypted only" changes when alternative less secure methods are employed, and especially for clients that deal with sensitive data. For example, always warn to "continue without encryption" when "encrypted DNS is not available". Use short, reasonable requests, and implement several retries before falling back to unencrypted DNS queries when communicating with multiple servers.

For defaults that are designed with usefulness and efficiency in mind, prioritize DoH/3 or DoQ if available, use DoH/2 as a reasonable alternative, and use DoT only for more tightly controlled connections as DoT is otherwise to be avoided. Selecting a good, close resolver and keeping session persistence are encouraged, as is careful tailoring of outbound traffic and logging to the company's needs.

All in all, the landscape surrounding encrypted DNS is proliferating and deepening. By carefully designing fallback behaviors and policies, and selecting a good resolver, businesses can maintain exceptional performance from the systems while meeting the compliance and reliability burdens that have historically been present with closed circulation systems.

8. Summary

Transparent DNS does provide obscured exposure to certain destinations when it comes to DNS over HTTPS, DNS over QUIC, and DNS responsive to networks and resolvers with intermediate UDP latencies. However, these protocols still are exposed to drops, throttling of requests (ports, SNI, QUIC), and some unrecorded metadata resolution (SNI, resolver IP, distinct traffic). Our blockability and measurement evaluations result in approximately practical guidance of preferring Over HTTPS in conjunction with QUIC. Proper SNI throttling, and other protocols such as QNAME minimization, and in the future, ECH; complete the complementarity of protocols. Encrypted DNS does provide some readiness to be more widely adopted, as long as the reliability of some of the desired protocols are exhibited when to be put into place without strict policy rules.

9. Recommendation

We provide end-user client settings and business encrypted DNS deployment advice based on our results. These maximise privacy and performance while minimising risks:

End-user clients:

Favor more modern protocols (DoH/3 or DoQ): Configure your systems or applications to use DNS over HTTP/3 or QUIC. They have better encryption and network resilience. Enable DoH in your browser and use HTTP/3 (most browsers do this by default as long as the resolver supports it). Use DoQ with a supported resolver on devices that can use it, i.e. Android 13+ with Google's DNS or Stubby.

If possible, turn off cleartext fallback: Use strict mode for encrypted DNS in case of high threat scenario or for top privacy, which may cause outages, as silent downgrade attacks are mitigated. In Firefox, use "Strict" DNS-over-HTTPS to bypass the OS DNS stack. Android Private DNS should be "Strict". In this way, if encrypted DNS is prohibited, requests will fail rather than leaking silently. Do this only if you understand the availability trade-offs. To mitigate data leakage to the intermediate DNS servers, you should also enable minimization on your resolver if applicable, even if you are on a home router. Some public DNS resolvers (Cloudflare, Quad9) provide QNAME-min by default.

If possible, implement DDR: Client Operating Systems might be able to automatically find and connect to network resolvers that offer encrypted services. This is usually beneficial (the ISP's encrypted resolver keeps your queries confidential). Ensure that this feature is enabled/drop Windows and Android default settings. This does not prevent ISP from seeing your DNS traffic, but does protect against local eavesdropping (this is more about local privacy).

Assign a trustworthy resolver as a must (this might be you): Users also have the option to specify that they would like to always connect to an encrypted DNS service that is trusted for privacy either as a vpn or a public provider (figuratively speaking). In such cases, be sure to set that resolver as a specific default and make sure you block any auto switching to other resolvers. You might have to hard code Cloudflare's DoH to your network settings. This might make connecting to certain networks more difficult if they have that service filtered, but it does ensure that you can't connect through an untrusted resolver.

For Enterprises (Network/IT Administrators):

Set up an encrypted local DNS gateway: Configure managed devices to use an on-premises DoH (or DoT) server. Simply install a DNS forwarder on your network that accepts DoH and forwards queries to your corporate DNS server. Users can employ encryption while queries temporarily route through your infrastructure for logging and filtering. There are cloud (Cloudflare's Gateway) and self-hosted (BIND server behind NGINX reverse proxy for DoH) options.

Implement DNS egress allow-lists: Create firewall rules to limit DNS requests (port 53, 853, 443) to a small list of permitted resolvers to limit the risk of using "shadow" DNS. Block all external

IP:53 and DoH endpoints, except for those that are sanctioned. Users (or malware) are not able to circumvent the rules using an external encrypted resolver. Our testing shows that if you block them, they will likely fallback to your resolver, which proves your policy is working.

Implementation of privacy-aware logging and policy articulation: Log DNS queries for security supervision, but imply less retention, or the use of aggregated records for privacy protection. Your acceptable use policy should clarify the purpose of the company's use of encrypted DNS (e.g., because we do not eavesdrop, but we also monitor risks). This enables compliance and trust. Employees are less likely to try and circumvent DNS if they are confident it is only for security and privacy. Anomalies or downgrades: Look for unusual DNS requests within your network, as dissimilar behavior may indicate misconfiguration or malicious activity. If internal devices are making UDP/53 requests to external servers when they shouldn't be, check if someone is bypassing encrypted DNS or performing a downgrade attack. Modern network monitoring or IDS signatures are capable of detecting unauthorized DNS activity.

Focusing on resolver pinning and exceptions: Locate internal applications or devices that may not support encrypted DNS. IoT devices may either be hardcoded to specific DNS servers or may not support DoH. You may need to allow plaintext (but only to specific addresses within your firewall). Consider the exceptions (perhaps a separate SSID or VLAN for legacy devices). Establishing encrypted DNS on all standard client devices (Windows, Linux, macOS, iOS, Android) and enforcing it through MDM/Group Policy.

The above guidance will assist end-users in securing the privacy of their DNS queries in multifarious networking environments and will assist enterprises in implementing encrypted DNS to satisfy the security requirements of the organization. Utilizing the privacy and integrity of encrypted DNS and having fallbacks or policies for its weaknesses (blockability and obfuscated traffic) will be important.

10. Limitations & Future Work

The systems under study are limited in scope with only 3 networks for 1 region over a couple of weeks, as such, a longitudinal multi-region study especially in areas where censorship measures differ is necessary to confirm these trends.

The volume of data is impacted by popular areas. These 'long-tail' domains, due to slower authorities, may impact latency further. The only measured hop-stubs were the stub to the resolver; the resolver to the authoritative segment is where the next potential privacy concern may arise, especially when more encryption is used.

Attribution in the presence of middleboxes is difficult. The users on the campus, the combination of QUIC, firewall and UDP, NAT timeouts may impact the results; fixing such discrepancies would require more in depth testing such as using path diagnostics tools (pcaps, traceroute, QUIC logs).

The impact on the energy and the CPU of the mobile were only observed in an unofficial manner. It is possible that persistent HTTPS/QUIC may impact the radio's state.

The impact of new technologies is large enough to require them to be used in real-world environments. The real-world latencies and the robustness of ECH's success and its fallbacks (including regressions with transparent SNI) as well as ODoh are worth large-scale measurement.

The presence of encrypted DNS may alter the outcome in ways that are hard to predict. The upcoming deployments of DoQ and QUIC, and the new CDN and transport framework (such as WebTransport) systems should be monitored.

11. References

[Kosek22] 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," Proc. ACM IMC, 2022. URL: https://vaibhavbajpai.com/documents/papers/proceedings/doq-imc-2022.pdf
Annotation: Distributed measurements show DoQ reduces lookup latency and can speed simple page loads (~10% vs DoH), nearly matching plaintext—evidence for QUIC's handshake/tail advantages.

[Lu19] Lu, C., Li, Z., Chang, D., Huang, Q., et al., "An End-to-End, Large-Scale Measurement of DNS-over-Encryption," Proc. ACM IMC, 2019. URL: https://utdallas.edu/~zxl111930/DNSMeasurement_IMC19_Full.pdf
Annotation: Early global snapshot of DoT/DoH adoption; finds modest median overhead (<~10 ms) but heavier tails on cold caches—motivates our tail-focused analysis.

[Zander20] Zander, S., Cholez, T., et al., "Measuring DNS over TLS from the Edge: Adoption, Reliability, and Response Times," PAM Workshop, 2020. URL: https://net.in.tum.de/pub/doan2021pamworkshop/doan2021pamworkshop.pdf
Annotation: RIPE Atlas edge tests show DoT medians near UDP in good networks but worse tails in poor ones; session reuse mitigates costs—supports our warm-cache findings.

[Basso21] Basso, S., Said, A., Wagner, F., et al., "Measuring DoT/DoH Blocking Using OONI Probe," NDSS DNS Privacy Workshop, 2021. URL: https://ooni.org/post/2021-ooni-dns/ooni-dns.pdf
Annotation: Field evidence of port-853 blocks and SNI-based DoH filtering; also reports QUIC throttling—directly informs our interference scenarios.

[Huang20] Huang, Q., Chang, D., Li, Z., "A Comprehensive Study of DNS-over-HTTPS Downgrade Attack," USENIX FOCI, 2020. URL: https://www.usenix.org/system/files/foci20-paper-huang.pdf
Annotation: Shows major browsers can be forced to plaintext via active interference; argues for stricter modes and user warnings—basis for our fallback guidance.

[Bushart20] Bushart, J., Rossow, C., "Padding Ain't Enough: Assessing the Privacy Guarantees of Encrypted DNS," USENIX FOCI, 2020. URL: https://www.usenix.org/system/files/foci20-paper-bushart.pdf

Annotation: Demonstrates traffic analysis (sizes/timings) can fingerprint queries despite padding—motivates our leakage-surface discussion.

[Siby21] Siby, A., Juarez, M., Diaz, C., Vallina-Rodriguez, N., Troncoso, C., "DNS over HTTPS: Privacy vs. Detection," IEEE S&P Workshops, 2021. URL: https://arxiv.org/abs/1906.09682
Annotation: ML techniques reliably detect DoH and DoH tunnels—relevant to enterprise monitoring and our detection vs. privacy trade-offs.

[Chai21] Chai, Z., et al., "Effectiveness of Encrypted SNI in Blocking-Resistant Communication," Proc. PAM, 2021. URL: https://link.springer.com/chapter/10.1007/978-3-030-72582-2_10
Annotation: ESNI/ECH reduces SNI-based blocking, shifting censors toward IP-level tactics—supports our ECH mitigation point.

[NSA21] NSA Cybersecurity Directorate, "Adopting Encrypted DNS in Enterprise Environments," Jan. 2021. URL: https://media.defense.gov/2021/Jan/14/2002564889/-1/-1/0/CSI_ADOPTING_ENCRYPTED_DNS_U_OO_102904_21.PDF
Annotation: Recommends enterprise-controlled encrypted resolvers and egress controls—aligns with our on-prem DoH gateway + allow-listing pattern.

[Schmitt19] Schmitt, P., Edmundson, A., Mankin, A., Feamster, N., "Oblivious DNS: Practical Privacy for DNS Queries," PoPETS, 2019. URL: https://petsymposium.org/popets/2019/popets-2019-0028.php
Annotation: Introduces oblivious DNS (split identity/content) with added latency—precursor to ODoH referenced in our mitigations.

[Pauly22] Pauly, T., et al., "Oblivious DNS over HTTPS (ODoH)," RFC 9230 (Exp.), 2022. URL: https://www.rfc-editor.org/rfc/rfc9230
Annotation: Standardizes ODoH (proxy + target) and notes ~20–30% latency overhead; relevant for high-privacy scenarios in our guidance.

[Hoffman21] Hoffman, P., McManus, P., "DNS Query Name Minimisation to Improve Privacy," RFC 9156, 2021. URL: https://www.rfc-editor.org/info/rfc9156
Annotation: Defines QNAME minimization to limit upstream leakage with minimal impact—one of our recommended resolver settings.

[Rescorla25] Rescorla, E., et al., "Encrypted ClientHello for TLS 1.3," IETF Internet-Draft, 2025. URL: https://datatracker.ietf.org/doc/draft-ietf-tls-esni/
Annotation: ECH encrypts SNI/ClientHello, closing a major DoH/DoT leak; not yet universal—future-proofing in our recommendations.

[Bortzmeyer19] Bortzmeyer, S., "DNS Privacy in Practice and Preparation," IEEE Security & Privacy, 2019. URL: https://ieeexplore.ieee.org/document/8571201
Annotation: Early overview of DoT/DoH and operational hurdles—historical context for issues we quantify empirically.

[Kalbarczyk20] Kalbarczyk, A., et al., “Enterprise Security and DNS over HTTPS: A Risk Analysis,” ACM CCR, 2020. URL: https://dl.acm.org/doi/10.1145/3431832.3431838 Annotation: Analyzes DoH risks in enterprises (evasion, monitoring loss) and proposes controls—supports our policy and egress-allow-list guidance.

12. List of Acronyms

DNS — Domain Name System

DoT — DNS over TLS

DoH — DNS over HTTPS

DoQ — DNS over QUIC

HTTP/2 — Hypertext Transfer Protocol version 2

HTTP/3 — Hypertext Transfer Protocol version 3 (over QUIC)

TLS — Transport Layer Security

QUIC — (name) UDP-based transport with built-in TLS and multiplexing

SNI — Server Name Indication (TLS extension)

ECH — Encrypted ClientHello (TLS extension)

DDR — Discovery of Designated Resolvers

ODoH — Oblivious DNS over HTTPS

Last modified on November 17, 2025
This and other papers on recent advances in networking are available online at
http://www.cse.wustl.edu/~jain/cse5700-25/index.html
Back to Raj Jain's Home Page