Securing the Missing Link: Encrypted Recursive-to-Authoritative DNS in the Wild

Yevheniya Nosyk
KOR Labs
Grenoble, France

Simon Fernandez
Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG
Grenoble, France

Andrzej Duda
KOR Labs
Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG
Grenoble, France

Maciej Korczyński
KOR Labs
Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG
Grenoble, France

ABSTRACT

DNS resolvers increasingly support various encryption protocols, ensuring their communication with end clients remains confidential. The recursive-to-authoritative link has long been overlooked though, despite multiple reports on traffic analysis and response injection by state censors. The experimental RFC 9539 addresses this confidentiality gap with a unilateral and opportunistic mechanism—recursive resolvers probe nameservers for DNS-over-TLS or DNS-over-QUIC support and, if successful, communicate over the encrypted channel. In this paper, we measure the deployment of RFC 9539 (ADoT/ADoQ, hereafter ADoX) in the wild, covering both recursive resolvers and authoritative nameservers. We identify fewer than 1% (3.1 M) of registered domains supporting ADoX, with one provider accounting for the vast majority of these deployments. Ultimately, our data-driven study informs DNS operators that increasingly consider the adoption of ADoT/ADoQ but lack concrete numbers on the current state of deployment.

CCS CONCEPTS

• **Security and privacy → Network security**.

KEYWORDS

DNS, Encryption, Privacy, DNS-over-TLS, DNS-over-QUIC

1 INTRODUCTION

The Domain Name System (DNS) is one of the oldest networking protocols to date [66, 67]. Yet, its original specification ensures neither message confidentiality, response integrity, nor data-origin authentication. Previously, the DNS Security Extensions (DNSSEC) [79–81] satisfied two of the above requirements. Yet, DNS traffic remained in cleartext—exposing query metadata that supports profiling, correlation, and censorship [1, 28, 35, 51, 72, 88].

Several mechanisms have emerged to address this confidentiality gap, including DNS-over-TLS (DoT) [46], DNS-over-HTTPS (DoH) [40], and DNS-over-QUIC (DoQ) [48]. The extensions are receiving increasing support but remain under-represented compared to traditional plaintext transport (Do53) [2]. Moreover, the proposed techniques have primarily been deployed between stubs and recursive resolvers [21]. The second part of the resolution chain, namely recursive-to-authoritative, remains in cleartext. Although generally considered less privacy-sensitive, such exchanges are still vulnerable to response injection by national censors [1, 28, 72, 88] or traffic analysis [35, 51]. Several countermeasures, including QNAME minimization [6, 7], local root [61], or aggressive DNSSEC caching [31] minimize privacy breaches, but do not eliminate them completely.

While no protection against active attackers exists yet, Gillmor et al. [33] proposed a unilateral, opportunistic approach to adding confidentiality on the recursive–to-authoritative path. The experimental RFC 9539 specifies how resolvers can probe nameservers over DoT or DoQ—termed ADoT/ADoQ or collectively ADoX—without prior coordination. Several early adopters emerged before the document was published, including the Meta (Facebook) / Cloudflare [9] pilot, Google [15], and B-root [36, 37]. More recently, substantial community outreach has aimed to drive ADoX deployment [22, 25, 29]. However, resolver operators note that investment in encryption is hard to justify if authoritative nameservers do not support it [25]—creating a "chicken-and-egg" problem that likewise discourages nameserver operators.

Prior work examined the encryption support among selected popular domains [21, 62, 63] as well as the presence of encrypted queries on authoritative nameservers [89]. However, no study has systematically quantified recursive-to-authoritative encryption at the Internet scale. The ADoX specification explicitly calls for empirical measurement to quantify early deployments and, more broadly, to assess the value of rolling out the protocol [33]. Accordingly, we provide data that supports operators in making informed ADoX deployment decisions. We perform Internet-scale in-the-wild measurements across the DNS resolution chain—root, TLDs, and registered domains—and both open and closed resolvers. In our methodology, we actively probe authoritative nameservers for ADoT/ADoQ support and, when successful, resolve the domains they are authoritative for. We additionally operate two custom domain names reachable only over these encrypted transports to test whether recursive resolvers can obtain answers for such zones.

In summary, our contributions are as follows:

- We identify 3.1 M registered domains (0.96% of 320 M analyzed) with support for ADoT/ADoQ. A single provider (One.com) accounts for the vast majority of deployments.
- We find that with ADoT support at one root server letter (B-root) and five top-level domains (`.cy`, `.arpa`, `.gr`, `.ελ`, `.kg`), only 818 registered domains achieve a fully encrypted recursive–to–authoritative path. No such path exists via ADoQ.

- We identify 100 ADoT-capable open resolvers, most of them forwarding requests to Quad9. We found no ADoQ open resolvers, nor any ADoT/ADoQ closed resolver.

2 BACKGROUND

This section reviews the three core DNS encryption protocols and explains how two of them—DoT and DoQ—can be applied on the recursive-to-authoritative link. We then survey ADoX support across major DNS software vendors.

2.1 DNS Encryption Protocols

The IETF *doh* and *dprive* working groups, both concluded as of August 2025, addressed DNS privacy. Below, we review the key standards they proposed and how they compare to Do53.

DNS-over-TLS [46] is the first protocol in the series, leveraging the Transport Layer Security (TLS) to hide DNS exchanges from passive observers. Clients connect to servers on a well-known port 853 either opportunistically, or via the out-of-band key-pinned authentication. At the time of writing, the protocol was primarily targeted at the stub-to-recursive link (as per the working group charter). Yet, it acknowledged that the scope could be broadened in future to cover the recursive-to-authoritative scenario. Conversely, DNS-over-HTTPS [40] reuses the established HTTPS protocol to embed DNS messages in HTTP exchanges. It requires clients to obtain the URI template (e.g., `/dns-query?dns`), leaving its discovery outside the scope of the protocol and not mandating any default value. More recently, DNS-over-QUIC [48] leveraged the newly standardized transport to provide similar privacy guarantees to DoT—both run on a dedicated port 853 and QUIC incorporates TLS 1.3 for authentication, key establishment, and encryption. DoQ is a general-purpose DNS protocol applicable to traffic between stubs, recursives, and authoritatives.

DNS encryption should not be confused with DNS Security Extensions (DNSSEC). The former ensures the channel privacy, while the latter adds data authentication and integrity. Therefore, these techniques are complementary.

2.2 Authoritative DoX

The RFC 9539 (Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS) details how the standards presented above apply to the communication between resolvers and nameservers [33]. Broadly, the proposal aims to protect against passive attackers while gaining initial operational experience on deploying ADoX. The mechanism is *unilateral* (does not require prior coordination) and *opportunistic* (encrypts what would otherwise be sent in cleartext). DoT and DoQ both satisfy these requirements, as clients can attempt to establish connections with nameservers on a well-known port 853. Consequently, DoH is explicitly left outside the scope of this proposal, as one cannot guess the URI template of the remote endpoint. While the Discovery of Designated Resolvers (DDR) solved this problem for recursives [76], there is no established signaling mechanism for nameservers. Some ongoing work [3, 84, 85] may help address this problem in the future.

Recursive resolvers probe nameservers on one or more encrypted transports along with Do53, tracking all the successful and failed connections. Authoritatives, in turn, commit to serve the same data regardless of the chosen transport. They may optionally add EDNS(0) padding to protect from trivial traffic analysis, but do not need to provide any particular means of authentication. A self-issued X.509 certificate is sufficient [33].

Note that RFC 9539 deliberately leaves server authentication out of its scope, meaning that resolvers may be downgraded to cleartext DNS either because of failed connection establishment or machine-in-the-middle attack. This opportunistic nature of ADoX allows for gradual deployment with protection from passive observers only.

2.3 Software Support

DNS software vendors have already released preliminary ADoX implementations on both sides—resolvers and nameservers [24]. While mostly presented as experimental, they enable early adoption and testing of recursive-to-authoritative encryption.

PowerDNS with its three products (PowerDNS Recursor, PowerDNS Authoritative, and dnsdist) collectively supports all the DNS encryption protocols [13]. They enabled opportunistic probing by Recursor in 2022, initiating a DoT connection to nameservers in parallel to Do53 [68]. PowerDNS Authoritative does not implement ADoX natively, but can be used in conjunction with the dnsdist proxy [78]. Knot Resolver supports both DoH and DoT transports [18], implementing a custom algorithm to auto-discover DoT nameservers with the SPKI fingerprints [19]. The authoritative Knot DNS, in turn, can provide DoQ [16] and DoT [17], the latter also supported by authoritatives BIND9 [53] and NSD [71]. The Unbound team reported on developing a non-public prototype of the unilateral probing mechanism in 2023 [86].

3 AUTHORITATIVE NAMESERVERS

We now measure the ADoX adoption on the authoritative side, analyzing root, top-level, and registered domains.

3.1 Methodology

We start by obtaining the list of top-level domains maintained by the Internet Assigned Numbers Authority (IANA) [49]. We then build the deduplicated dataset of registered domains from a passive DNS feed [83], Google's Certificate Transparency logs [12], and the ICANN Centralized Zone Data Service (CZDS) [50]. We use zdns [55] to map domains to **`NS`** records, followed by **`A`**/**`AAAA`** requests to obtain nameserver IPs. We then perform an operational check to find those nameservers supporting ADoT or ADoQ. We send non-recursive queries using dnspython [34], disabling certificate validation as allowed by RFC 9539. Having narrowed down the list to those nameservers implementing ADoT or ADoQ, we finally resolve each domain they are authoritative for directly. We keep domains and nameservers that respond with **`NOERROR`** to our **`SOA`** request when resolved over an encrypted transport.

3.2 Results

Table 1 summarizes the domain scan performed in November 2025. It achieved broad coverage, encompassing the root, 1.4 k TLDs and over 320 M registered domains. We analyzed all the 754 k IPv4 and 95 k IPv6 authoritative nameserver IPs.

Table 1: Summary of the ADoX scan performed in November 2025. We aggregate the results per root, top-level domains (TLDs), and registered domains (RDs).

	Domains			Nameservers		
	Root	TLDs	RDs	Root	TLDs	RDs
Total scanned	1	1,437	320,383,268	26	8,974	847,692
ADoT v4	1	5	3,047,567	1	7	1,385
ADoT v6	1	2	2,454,896	1	3	845
ADoQ v4	0	1	2,259,563	0	2	199
ADoQ v6	0	1	2,250,417	0	2	159
Total ADoX	1 (100%)	5 (0.35%)	3,075,168 (0.96%)	2 (7.69%)	10 (0.11%)	2,322 (0.27%)

3.2.1 Adoption Rates. Overall, the deployment remains low, with the great majority of nameservers timing out the probing encrypted requests we sent—only 2.3 k authoritative nameservers out of 848 k (or 0.27%) support ADoX. Having deliberately disabled the TLS validation as per the RFC, our methodology would not reject, e.g., expired or self-signed certificates. Therefore, the failed requests are due to timeouts or prematurely closed connections.

Next, we identify registered domains supporting ADoT or ADoQ. We recall that as per our methodology, we define a domain name reachable over an encrypted channel if its nameservers return the **`NOERROR`** response code for the **`SOA`** query we sent over ADoT or ADoQ. We successfully resolved 99.29% of domains served by ADoX nameservers. The remaining 21.9 k failures were due to timeouts (14.3 k domains) and DNS resolution failures (7.6 k domains). As a result, only 0.96% of registered domains support ADoX.

ADoT is the preferred transport, with slightly more than 3 M reachable domains (IPv4 and IPv6 combined) compared to 2.3 M in ADoQ. There is also an apparent dominance of IPv4 over IPv6, whether at the domain or nameserver levels (consistent with the general population of nameservers which is dominated by IPv4). While the vast majority of ADoT domains (79.13%) are reachable over both address families, IPv6 is rarely (0.79%) implemented alone. In ADoQ, the deployments are more uniform, with as many as 98.31% of domains supporting both IPv4 and IPv6. Interestingly, 2.2 M domains (72.01%) out of 3.1 M support all the protocol combinations—ADoT and ADoQ over IPv4 and IPv6. We will later show that these deployments are mainly driven by a single provider.

Moving up the DNS hierarchy, five top-level domains—**`.cy`**, **`.arpa`**, **`.gr`**, **`.ελ`**, **`.kg`**—support the recursive-to-authoritative encryption. The **`.kg`** is the only TLD doing ADoT/ ADoQ over IPv4/IPv6. At the root level, USC/ISI (B-root) runs the experimental ADoT service. It is also the operator providing IPv4/IPv6 ADoT for **`.arpa`**, the infrastructure TLD run by root server operators.

3.2.2 Operator Concentration. With only 2.3 k nameservers authoritatively serving millions of ADoX domains, adoption is likely driven by a small set of providers. We leverage the IPinfo Lite API [54] to map nameserver IPs to autonomous system names to reveal the organizations hosting the services.

Table 2 shows the top 10 organizations in terms of hosted nameservers and corresponding registered domains. Overall, we identify 490 unique organizations behind 2,322 nameserver IPs—480 host ADoT nameservers, while 79 are behind ADoQ machines.

Table 2: Organizations hosting ADoX nameservers, number of nameserver IPs, and number of domains they are authoritative for.

#	ADoT			ADoQ		
	Operator	IPs	Domains	Operator	IPs	Domains
1.	One.com A/S	24	2,008,043	One.com A/S	24	2,008,050
2.	JSC "TIMEWEB"	9	369,648	WEDOS [..]	17	243,591
3.	JSC "RetnNet"	1	358,043	NetActuate, Inc	3	11,323
4.	WEDOS [..]	17	258,906	Hetzner [..]	58	3,530
5.	Nazwa.pl Sp.z.o.o.	6	147,171	Naquadria S.R.L.	1	2,810
6.	OVH SAS	126	115,814	Microsoft [..]	1	2,807
7.	NAMESHIELD [..]	4	79,327	ip&more GmbH	4	2,669
8.	WIIT AG	7	79,204	dataforest GmbH	2	2,669
9.	Servergarden Kft.	6	39,549	CDLAN SpA	6	2,210
10.	Hetzner [..]	254	31,422	NS3 s.r.l.	4	2,127

Table 3: ADoX nameservers aggregated by registered domain names and the number of ADoX domains they are authoritative for.

#	Operator	ADoT Domains	Operator	ADoQ Domains
1.	*.one.com	1,472,781	*.one.com	1,472,787
2.	*.hostnet.nl	403,216	*.hostnet.nl	403,217
3.	*.timeweb.ru	372,676	*.wedos.cz	237,691
4.	*.timeweb.org	372,645	*.wedos.eu	237,509
5.	*.wedos.cz	253,048	*.wedos.com	237,295
6.	*.wedos.eu	252,852	*.g1-dns.com	87,519
7.	*.wedos.com	252,639	*.g1-dns.one	87,519
8.	*.nazwa.pl	147,097	*.antagonist.nl	44,527
9.	*.g1-dns.com	87,519	*.antagonist.net	44,527
10.	*.g1-dns.one	87,519	*.desec.io	11,262

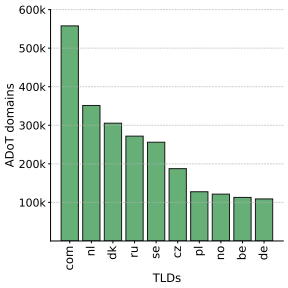

Figure 1: Top 10 TLDs by the number of ADoT domains.

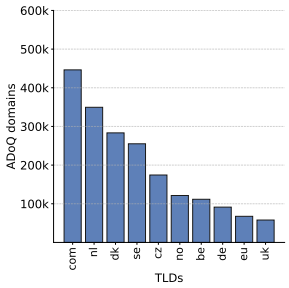

Figure 2: Top 10 TLDs by the number of ADoQ domains.

Our measurements indicate three deployment patterns: i) centralized, provider-wide enablement (e.g., One.com A/S), ii) ADoX-as-a-service for selected domains, and iii) infrastructure rental/colocation for custom authoritative stacks (e.g., Hetzner).

ADoX deployment is highly concentrated: One.com accounts for 2 M ADoX domains, dwarfing the next providers by an order of magnitude. In contrast, other operators (e.g., TIMEWEB, WEDOS, Nazwa.pl) each cover at most a few hundred thousand ADoT domains or far fewer under ADoQ. Timeweb ranks second in the number of ADoT domains but does not currently support ADoQ. Its deployment spans two autonomous systems: JSC TIMEWEB and JSC RetnNet. WEDOS, the EU-based DNS anycast provider, enables both ADoT and ADoQ for 259 k and 244 k domains, respectively, with fewer domains resolvable over ADoQ due to timeouts. Our

Table 4: Top 20 highest ranked ADoT domains appearing in the Tranco list.

Rank	Domain	Rank	Domain
4.	facebook.com	166.	cdn77.org
11.	instagram.com	169.	wildberries.ru
24.	fbcdn.net	251.	wikimedia.org
31.	wikipedia.org	278.	facebook.net
37.	whatsapp.net	398.	wb.ru
58.	whatsapp.com	521.	timeweb.ru
90.	root-servers.net	688.	fb.com
91.	wa.me	876.	threads.com
93.	cdninstagram.com	896.	fbsbx.com
127.	one.one	1178.	odoo.com

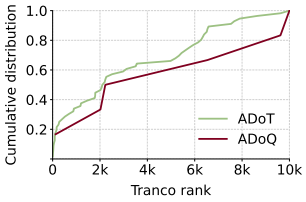

Figure 3: Tranco ranks of ADoX domains appearing in top 10 k list.

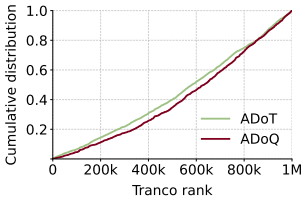

Figure 4: Tranco ranks of ADoX domains appearing in top 1 M list.

ongoing longitudinal measurements show that this is a consistent pattern rather than an individual scan artifact—WEDOS exhibits lower success rates when queried over ADoQ (similar sporadic failures may affect other providers). We finally observe tenant-driven deployments, such as 254 Hetzner machines serving 238 nameserver domains, and 126 OVH servers behind 116 k ADoT domains. Public claims of centralized ADoX remain sparse: among the top ten, only Nazwa.pl Sp.z.o.o. and WEDOS publicly acknowledge ADoT [70] or ADoQ [90] support.

Table 3 additionally aggregates ADoX nameservers by their registered domain name, for example, **`ns1.one.com`**, **`ns2.one.com`**, and **`ns3.one.com`** are represented as **`*.one.com`**. Overall, the ranking is dominated by the same provider seen in the IP-level analysis. One.com with its **`*.one.com`**, **`*.hostnet.nl`**, and **`*.antagonist.*`** (the two organisations it previously acquired [73, 74]) nameservers combined drives the ADoT and ADoQ deployment. We also see nameserver operators use different top-level domains for resiliency, such as **`wedos.eu`**, **`wedos.cz`**, and **`wedos.com`**. This example also highlights that no aggregation approach is perfect - while IP analysis may point to infrastructure reuse within cloud providers (e.g., OVH or Hetzner), same operator nameserver domains do not necessarily lay under the same suffix. Finally, we recall that counts reported in Table 2 and later Table 3 reflect both the supported protocols and transient reachability issues.

3.2.3 Distribution of ADoX Domains by TLD. We now analyze the distribution of registered ADoX domains by TLDs (e.g., **`.com`**, **`.pl`**). Despite the apparent diversity, ADoX domains in all but three TLDs are predominantly hosted by One.com—the major adopter of recursive–to-authoritative encryption. Notable exceptions include **`.cz`** and **`.ru`**, where over 99% of domains are served by WEDOS and TIMEWEB, respectively; for **`.pl`**, Nazwa.pl is authoritative for 85% of ADoT domains.

3.2.4 Domain Popularity. Raw domain counts quantify the ADoX deployment but do not indicate whether those domains or nameservers attract real client traffic. Ultimately, a single popular ADoX domain can affect more end users than millions of low-profile ones. Past incidents of on-path DNS manipulation affecting widely used services (e.g., the November 2021 **`whatsapp.net`** case [10]) highlight why prioritizing confidentiality on popular domains is disproportionately impactful [72].

We leverage the historical Tranco list to obtain popularity ranks for all 3.1 M domains at the time of our scan [77]. Overall, only 5.5 k entries appear in the top 1 M—5.4 k ADoT and much fewer

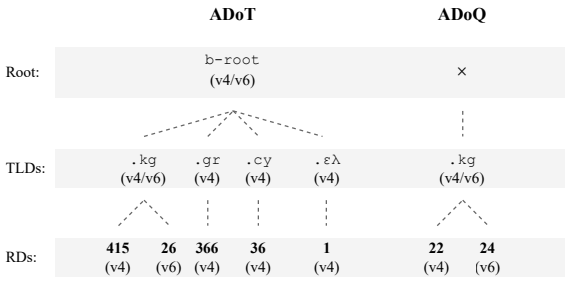

Figure 5: Fully encrypted ADoX resolution paths from the root down to registered domains (RDs). No such path exists for ADoQ.

(1.6 k) ADoQ domains. Figures 3 and 4 illustrate the cumulative distributions of top 10 k and 1 M ranks, respectively. ADoT domains skew more popular: one appears in the top-10, nine in the top-100, and 19 in the top-1,000. Table 4 lists the 20 most popular ADoT domains—dominated by eleven Meta (Facebook)-operated domains, such as **`facebook.com`** and **`whatsapp.com`**. Other prominent entries include **`wikipedia.org`** and **`wikimedia.org`** of the Wikimedia Foundation. By contrast, the most popular ADoQ domain appears at rank 127 (**`one.one`**), followed by **`eu.org`** at 2,019 and **`one.com`** at 2,225.

3.2.5 Resolver-side ADoT Evidence from Quad9. We now wonder whether end clients actually generate traffic to domains served by ADoX-enabled nameservers. Conventional passive DNS feeds have no visibility into encrypted recursive-to-authoritative exchanges. We therefore turn to Quad9—a major public resolver with millions of users worldwide who enabled experimental ADoT on parts of its infrastructure. They shared with us the list of 342 authoritative servers Quad9 successfully queried via ADoT in October 2025. These numbers, although an order of magnitude lower than those observed in the wild, can be attributed to the resolver operator's partial deployment of ADoT. While no per-query data was shared to protect user privacy, our measurements show the aforementioned ADoT 342 nameservers being authoritative for 447 k ADoT registered domains.

3.2.6 Fully Encrypted Resolution Paths. Assuming resolvers have empty caches and no local root zone, domain resolution starts at one of the 13 root servers and proceeds down the hierarchy until reaching the nameservers of registered domains. In this setting, a

fully encrypted path occurs when encryption is available at every step traversed. Below, we check how many registered domains, if any, have such a fully encrypted recursive-to-authoritative path. We recall that stub-to-resolver encryption is also necessary for full privacy, but is left outside the scope of this paper.

Figure 5 visualizes the available encrypted resolution paths. No root letter supports DNS-over-QUIC as of November 2025, making it impossible for any ADoQ domain to be resolved exclusively over an encrypted channel. Moreover, only one TLD **.kg** is currently ADoQ-reachable with as few as 24 unique ADoQ registered domains beneath. We therefore shift our focus to ADoT, which is supported by the B-root. Figure 5 shows the paths involving four ADoT top-level domains. Note that we exclude **.arpa** as it is an infrastructure TLD with no user-registered domains. We once again see **.kg** offering authoritative DoT in both address spaces for over 400 domains. Three other country-code TLDs contribute to the total of 818 ADoT registered domains with the fully encrypted resolution path (out of hundreds of billions of total resolution paths), making up 0.03% of all ADoX domains or 0.0003% of all the scanned domains. Note that resolvers must choose the B-root and send queries over IPv4 to all but **.kg** TLD.

3.2.7 Response Consistency. The RFC 9539 dictates that an "authoritative server implementing DoT or DoQ MUST populate the response from the same authoritative zone data as the unencrypted DNS transports [33]." We verify whether this requirement is met by the ADoX nameservers identified in the wild. We do so by following each ADoT/ADoQ **SOA** lookup as described in Section 3.1 with a regular Do53 request. We then compare non-empty **NOERROR** responses returned by the same nameserver over different transports.

We identify 3,920 domains with response discrepancies served by 118 nameservers. For the great majority of these domains (3,857), the difference comes from the Time-to-Live (TTL) field of the returned **SOA** record. Having manually verified these cases, we receive varying TTLs even when querying over the same transport. For example, the nameserver accounting for 1,477 domains serves TTL-deviating responses from different instances, as evidenced by the DNS Name Server Identifier (NSID) option [4]. The other type of response discrepancy, although much less common (155 domains), concerns the different **SERIAL** field. We recall that it is meant to be incremented every time a change in a zone file occurs [66]. While we do observe little changes (e.g., 61 and 62) or incremented numbers in each subsequent response returned (e.g., 1763561159 and 1763561172), our measurements mostly reveal persistent discrepancies in the zone file versions served over Do53 and ADoT/ADoQ.

Overall, we link the observed phenomena to complex DNS infrastructure deployments (e.g., the use of anycast or load balancing) rather than ADoX effects. As per RFC 9539, operators running a pool of nameservers are advised to keep it in a homogeneous state. This can be achieved by i) enabling the same encryption transport on all the nodes, ii) mapping clients based on their IPs, or iii) only forwarding encrypted client requests to encrypted nodes.

4 RECURSIVE RESOLVERS

We now set out to measure whether recursives can resolve domains with nameservers only reachable over ADoT or ADoQ.

4.1 Methodology

We first configure two domains—**adot.tld** and **adoq.tld**—each accessible over ADoT and ADoQ only. We use Knot DNS [20] as a backend nameserver and dnsdist as a load balancer. The latter provides extensive logging capabilities to let us observe decrypted incoming requests. Note that despite the two standards (ADoT/ADoQ) running on distinct transport-port combinations, we set up the two nameservers on separate servers to enforce a specific transport only. For the same reason, we also disable Do53 on both.

We then collect various datasets of recursive resolvers to test, including i) Open DNS API with open IPv4 resolvers [58, 69], ii) IPv6 Hitlist with open IPv6 DNS servers [32], and iii) RIPE Atlas with probes reaching local resolvers. We request open resolvers to query a unique subdomain of **[adot,adoq].tld** so that we associate domains seen on the nameservers to queried resolvers. For closed resolvers, we request all the connected RIPE Atlas probes to send such queries using their locally configured resolvers.

Using available lists of open resolvers alleviates the need to generate billions of probing DNS requests ourselves. Importantly, those services perform the Do53 discovery, potentially missing resolvers running on non-traditional ports or those only supporting encrypted transports. Yet, the work of Ververis et al. [89] has shown that encrypted resolvers did not manage to resolve the DoT/DoH domain, even if the original client query was sent via an encrypted channel. Nor there is any mechanism to instruct a resolver to perform ADoX. We therefore proceed with using our lists of Do53 resolvers to probe their support of ADoX.

4.2 Results

We performed the open resolver measurement in November 2025, collecting 1.4 M IPv4 resolvers and 366 k IPv6 hosts listening on port 53. None of those returned the response for the ADoQ domain, with only 88 IPv4 and 12 IPv6 open resolvers sending the response for the ADoT query. Focusing on these 100 resolvers, we determine whether they performed the resolution themselves or forwarded the request upstream (a common practice among open resolvers [58, 69]). Only three resolvers were not forwarders.

The absolute majority of the remaining 97 forwarders used Quad9 as an upstream provider—we subsequently saw it querying our nameservers from different backend IP addresses provided to us by Quad9. Two open resolvers forwarded to the Foundation for Applied Privacy that runs an experimental ADoT as part of its DNS privacy services [30]. The remaining forwarders triggered lookups coming from various cloud providers, including Amazon, I-Evolve, and Netcup. With no visibility into the path between open resolvers and their upstreams, we cannot conclude whether they used an encrypted channel to relay their request. Our measurements also did not identify experimental ADoT deployments of Cloudflare's 1.1.1.1 or Google's 8.8.8.8.

We then analyze two RIPE Atlas measurements covering 14 k probes. We obtained no answers for the ADoQ domain while only 44 probes successfully resolved the ADoT domain, all via forwarding to public resolvers - Quad9 (42 probes) and the Foundation for Applied Privacy (2 probes). Accordingly, we did not observe any closed resolvers supporting ADoX.

5 RELATED WORK

Prior work highlights privacy risks on the recursive–to-authoritative link. Queries can embed personally identifiable data [51], underscoring caution even with aggregated sharing [52]. Plaintext transport enables on-path manipulation with reports of interceptors/injectors affecting root-server traffic [28, 72]. Hardaker [35] advocated serving the root zone locally to reduce exposure, but censorship has also been observed on traffic to TLD nameservers [1].

A large body of work has examined DNS encryption on the stub-recursive hop: its adoption, performance, and privacy properties. The use of encrypted transports remains far less prevalent than plaintext Do53 [65] across DoT [26], DoH [56], and DoQ [59]. While encryption can add latency relative to plaintext [8, 14, 43, 60], several studies report cases when it improves page load times [41, 42]. By contrast, our work focuses on the recursive-to-authoritative link.

The evidence on the privacy gains from DNS encryption is mixed. It can help circumvent censorship in some cases [39, 57], yet remains vulnerable to traffic analysis even with padding [11, 45, 82, 87]. To avoid central points of observation or failure, Hounsel et al. advocated distributing queries across multiple resolvers [44] so that large public resolvers can be blocked or forced to downgrade to plaintext [5, 47, 64]. Moreover, Hoang et al. found a limited benefit when domains sit on unique servers, making them easily identifiable by destination [38].

Four previous studies concerned authoritative-side encryption. In 2019, Deccio et al. [21] found no TLD ADoT support and only 12 ADoT-capable nameserver IPs among the top-5 k Alexa domains. Li et al. [63] confirmed that no TLD nameservers supported DoT or DoH as of September 2022. Having further extended the measurements to 3 M registered domains, they found 295 DoT and 61 DoH nameservers. Next, Li et al. [62] took a different approach and performed an Internet-wide probing of the IPv4 address space, applying heuristics to identify authoritative nameservers reachable over DoT, DoH, and DoQ. They also enriched the domain seed with top 4 M popular domains. The measurements, performed in the second half of 2023, revealed several times more encrypted nameservers than the previous work. More recently, Ververis et al. [89] operated an ADoT/ADoH-reachable domain and observed no encrypted resolver traffic despite stub-recursive support.

Our paper extends the existing work in several ways. We greatly broaden the coverage, measuring 320 M registered domains compared to 4 M in existing studies. This paper covers the two RFC 9539 encryption protocols (ADoT/ADoQ) and performs measurements in both IPv4 and IPv6 address spaces.

6 DISCUSSION AND CONCLUSIONS

What our measurements show. Our work delivers an Internet-scale, operator-attributed view of confidentiality on the recursive-to-authoritative link. Rather than probing a handful of authorities, we i) map support across roots, TLDs, and registered domains, ii) attribute deployments to operators, and iii) provide the resolver-side evidence of actual encrypted use. The resulting picture is consistent: deployment exists but is sparse and highly concentrated. Fewer than 1% of registered domains support ADoX, with one operator (One.com) accounting for ∼2 M of them. ADoQ is effectively absent at the root and nearly absent at TLDs. Under conservative (cold-cache) assumptions, only 818 domains benefit from a fully encrypted resolver-to-authoritative path via experimental ADoT at B-root. The resolver-side evidence aligns with this observation: the ADoT successes provided by Quad9 following their partial deployment cover 342 authoritative servers (with 447 k registered domains behind as identified by our measurements) - a strict subset of what exists Internet-wide.

Where the results meet operators today. The measurements speak directly to operator sentiment captured at the IETF 123 ADoX side meeting [25]: today's encrypted authoritative traffic volumes are tiny, the ADoT performance worries operators at scale, and many prefer to land on ADoQ as implementations mature—yet the ecosystem remains stuck in a "chicken-and-egg" dynamic. Our data quantifies that impasse and indicates where movement matters the most. Because deployment is concentrated, a small number of large authorities and a few major resolvers can, if coordinated, deliver disproportionate privacy gains quickly.

Next steps. Authoritative-side DNS privacy is early but actionable. Our measurements establish a baseline, identify the operators with the greatest leverage, and illuminate protocol and deployment edges that currently limit impact the most. We hope this operator-grounded evidence helps align resolvers, authorities, and standards work on a pragmatic path, from opportunistic islands to material, user-visible privacy on the recursive-to-authoritative link, in step with the priorities and concerns voiced at IETF 123.

Community outreach is the most immediate next step for this work. Our data reveal clusters in which enabling ADoT at a single TLD could create fully encrypted resolution paths for hundreds of thousands of registered domains. At the same time, given operators' reluctance to deploy authoritative DNS encryption, evaluating the performance of ADoT/ADoQ would help quantify the latency and overhead introduced by these protocols. Such a follow-up study would equip implementers with the evidence needed to build a business case for adoption.

ACKNOWLEDGMENTS

This work has been partially funded by the European Union under Grant Agreement No. 101128042 (project ThreatChase) supported by the European Cybersecurity Competence Centre.

REFERENCES

[1] Anonymous. 2012. The Collateral Damage of Internet Censorship by DNS Injection. *SIGCOMM CCR* 42, 3 (jun 2012), 7 pages.
[2] APNIC Labs. 2025. Encrypted DNS World Map. https://stats.labs.apnic.net/edns.
[3] Tim April, Petr Špaček, Ralf Weber, and David C Lawrence. 2025. *Extensible Delegation for DNS.* Internet-Draft draft-ietf-deleg-02. Internet Engineering Task Force. Work in Progress.
[4] Rob Austein. 2007. DNS Name Server Identifier (NSID) Option. RFC 5001.
[5] Simone Basso. 2021. Measuring DoT/DoH Blocking Using OONI Probe: a Preliminary Study. In *NDSS Workshop on DNS Privacy*. The Internet Society, San Diego, USA, 1–10.
[6] Stéphane Bortzmeyer. 2016. DNS Query Name Minimisation to Improve Privacy. RFC 7816.
[7] Stéphane Bortzmeyer, Ralph Dolmans, and Paul E. Hoffman. 2021. DNS Query Name Minimisation to Improve Privacy. RFC 9156.
[8] Timm Böttger, Felix Cuadrado, Gianni Antichi, Eder Leão Fernandes, Gareth Tyson, Ignacio Castro, and Steve Uhlig. 2019. An Empirical Study of the Cost of DNS-over-HTTPS. In *IMC*. ACM, New York, USA, 15–21.
[9] Manu Bretelle. 2018. DNS over TLS: Encrypting DNS end-to-end. https://engineering.fb.com/2018/12/21/security/dns-over-tls.
[10] Manu Bretelle. 2021. [dns-operations] K-root in CN leaking outside of CN. https://lists.dns-oarc.net/pipermail/dns-operations/2021-November/021437.html.

[11] Jonas Bushart and Christian Rossow. 2020. Padding Ain't Enough: Assessing the Privacy Guarantees of Encrypted DNS. In *USENIX FOCI*. USENIX Association, USA, 1–8.

[12] Cali Dog Security. 2025. Certstream. https://calidog.io.

[13] Andrea Carpani. 2024. PowerDNS' progress in DNS encryption. https://blog.powerdns.com/powerdns-progress-in-dns-encryption.

[14] Rishabh Chhabra, Paul Murley, Deepak Kumar, Michael Bailey, and Gang Wang. 2021. Measuring DNS-over-HTTPS Performance Around the World. In *IMC*. ACM, New York, USA, 351–365.

[15] Tianhao Chi and Puneet Sood. 2023. Cache Poisoning Protection Deployment Experience. https://indico.dns-oarc.net/event/46/contributions/978/attachments/947/1754/Cache%20Poisoning%20Protection%20-%20Deployment%20Experience.pdf.

[16] CZ.NIC. 2025. DNS over QUIC. https://www.knot-dns.cz/docs/3.4/html/configuration.html#dns-over-quic.

[17] CZ.NIC. 2025. DNS over TLS. https://www.knot-dns.cz/docs/3.4/html/configuration.html#dns-over-tls.

[18] CZ.NIC. 2025. DoT and DoH (encrypted DNS). https://knot-resolver.readthedocs.io/en/stable/daemon-bindings-net_tlssrv.html.

[19] CZ.NIC. 2025. Experimental DNS-over-TLS Auto-discovery. https://www.knot-resolver.cz/documentation/latest/config-experimental-dot-auth.html.

[20] CZ.NIC. 2025. Knot DNS. https://www.knot-dns.cz.

[21] Casey Deccio and Jacob Davis. 2019. DNS Privacy in Practice and Preparation. In *CoNEXT*. ACM, New York, USA, 138–143.

[22] Sara Dickinson. 2025. The ADoT and ADoQ Deployment Initiative. https://419.consulting/encrypted-dns/f/the-adot-and-adoq-deployment-initiative.

[23] D Dittrich and E Kenneally. 2012. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research. https://catalog.caida.org/paper/2012_menlo_report_actual_formatted.

[24] DNS Privacy Project. 2025. ADoX Status and Deployment. https://dnsprivacy.org/adox_status_and_deployment/#implementation-status.

[25] DNS Privacy Project. 2025. IETF 123 ADoX Side meeting minutes. https://dnsprivacy.org/adox_status_and_deployment/ietf123sidemeetingminutes.

[26] Trinh Viet Doan, Irina Tsareva, and Vaibhav Bajpai. 2021. Measuring DNS over TLS from the Edge: Adoption, Reliability, and Response Times. In *PAM*. Springer-Verlag, Berlin, Heidelberg, 192–209.

[27] Zakir Durumeric, David Adrian, Phillip Stephens, Eric Wustrow, and J. Alex Halderman. 2024. Ten Years of ZMap. In *IMC*. ACM, New York, USA, 139–148.

[28] Xun Fan, John Heidemann, and Ramesh Govindan. 2013. Evaluating Anycast in the Domain Name System. In *IEEE INFOCOM*. IEEE, New York, USA, 1681–1689.

[29] Babak Farrokhi and Sara Dickinson. 2025. ADoT/ADoQ: Deployment Collaboration. https://ripe91.ripe.net/programme/meeting-plan/sessions/48/YTLL37.

[30] Foundation for Applied Privacy. 2025. DNS Privacy Services. https://applied-privacy.net/services/dns.

[31] Kazunori Fujiwara, Akira Kato, and Warren Kumari. 2017. Aggressive Use of DNSSEC-Validated Cache. RFC 8198.

[32] Oliver Gasser, Quirin Scheitle, Pawel Foremski, Qasim Lone, Maciej Korczyński, Stephen D. Strowes, Luuk Hendriks, and Georg Carle. 2018. Clusters in the Expanse: Understanding and Unbiasing IPv6 Hitlists. In *IMC*. ACM, New York, USA, 364–378.

[33] Daniel Kahn Gillmor, Joey Salazar, and Paul E. Hoffman. 2024. Unilateral Opportunistic Deployment of Encrypted Recursive-to-Authoritative DNS. RFC 9539.

[34] Robert Halley. 2025. dnspython. https://github.com/rthalley/dnspython.

[35] Wes Hardaker. 2018. Analyzing and Mitigating Privacy with the DNS Root Service. In *NDSS Workshop on DNS Privacy*. The Internet Society, San Diego, USA, 1–10.

[36] Wes Hardaker. 2022. TLS at a Root Experiment. https://indico.dns-oarc.net/event/43/contributions/937/attachments/900/1641/google-tls-abbrev.pdf.

[37] Wes Hardaker. 2023. USC/ISI's TLS at a Root Experiment Episode 2 – the Saga Continues. https://ant.isi.edu/events/dinr2023/S/s43.pdf.

[38] Nguyen Phong Hoang, Arian Akhavan Niaki, Nikita Borisov, Phillipa Gill, and Michalis Polychronakis. 2020. Assessing the Privacy Benefits of Domain Name Encryption. In *AsiaCCS*. ACM, New York, USA, 290–304.

[39] Nguyen Phong Hoang, Michalis Polychronakis, and Phillipa Gill. 2022. Measuring the Accessibility of Domain Name Encryption and Its Impact on Internet Filtering. In *PAM*. Springer-Verlag, Berlin, Heidelberg, 518–536.

[40] Paul E. Hoffman and Patrick McManus. 2018. DNS Queries over HTTPS (DoH). RFC 8484.

[41] Austin Hounsel, Kevin Borgolte, Paul Schmitt, Jordan Holland, and Nick Feamster. 2019. Analyzing the Costs (and Benefits) of DNS, DoT, and DoH for the Modern Web. In *ANRW*. ACM, New York, USA, 20–22.

[42] Austin Hounsel, Kevin Borgolte, Paul Schmitt, Jordan Holland, and Nick Feamster. 2020. Comparing the Effects of DNS, DoT, and DoH on Web Performance. In *WWW*. ACM, New York, USA, 562–572.

[43] Austin Hounsel, Paul Schmitt, Kevin Borgolte, and Nick Feamster. 2021. Can Encrypted DNS Be Fast?. In *PAM*. Springer-Verlag, Berlin, Heidelberg, 444–459.

[44] Austin Hounsel, Paul Schmitt, Kevin Borgolte, and Nick Feamster. 2021. Encryption Without Centralization: Distributing DNS Queries Across Recursive Resolvers. In *ANRW*. ACM, New York, USA, 62–68.

[45] Rebekah Houser, Zhou Li, Chase Cotton, and Haining Wang. 2019. An Investigation on Information Leakage of DNS over TLS. In *CoNEXT*. ACM, New York, USA, 123–137.

[46] Zi Hu, Liang Zhu, John Heidemann, Allison Mankin, Duane Wessels, and Paul E. Hoffman. 2016. Specification for DNS over Transport Layer Security (TLS). RFC 7858.

[47] Qing Huang, Deliang Chang, and Zhou Li. 2020. A Comprehensive Study of DNS-over-HTTPS Downgrade Attack. In *USENIX FOCI*. USENIX Association, USA, 1–8.

[48] Christian Huitema, Sara Dickinson, and Allison Mankin. 2022. DNS over Dedicated QUIC Connections. RFC 9250.

[49] IANA. 2025. Root Zone Database. https://www.iana.org/domains/root/db.

[50] ICANN. 2025. Centralized Zone Data Service. https://czds.icann.org.

[51] Basileal Imana, Aleksandra Korolova, and John Heidemann. 2018. Enumerating Privacy Leaks in DNS Data Collected Above the Recursive. In *NDSS Workshop on DNS Privacy*. The Internet Society, San Diego, USA, 1–7.

[52] Basileal Imana, Aleksandra Korolova, and John Heidemann. 2021. Institutional Privacy Risks in Sharing DNS Data. In *ANRW*. ACM, New York, USA, 69–75.

[53] Internet Systems Consortium. 2025. 8. Configuration Reference. https://bind9.readthedocs.io/en/v9.18.14/reference.html#namedconf-statement-listen-on-v6.

[54] IPinfo. 2025. IPinfo Lite. https://ipinfo.io/lite.

[55] Liz Izhikevich, Gautam Akiwate, Briana Berger, Spencer Drakontaidis, Anna Ascheman, Paul Pearce, David Adrian, and Zakir Durumeric. 2022. ZDNS: a Fast DNS Toolkit for Internet Measurement. In *IMC*. ACM, New York, USA, 33–43.

[56] Kamil Jerabek, Ondrej Rysavy, and Ivana Burgetova. 2023. Analysis of Well-Known DNS over HTTPS Resolvers. In *CCWC*. IEEE, New York, USA, 516–524.

[57] Lin Jin, Shuai Hao, Haining Wang, and Chase Cotton. 2021. Understanding the Impact of Encrypted DNS on Internet Censorship. In *WWW*. ACM, New York, USA, 484–495.

[58] Maynard Koch, Florian Dolzmann, Thomas C. Schmidt, and Matthias Wählisch. 2025. Forward to Hell? On the Potentials of Misusing Transparent DNS Forwarders in Reflective Amplification Attacks. In *CCS*. ACM, New York, USA, 1–15.

[59] Mike Kosek, Trinh Viet Doan, Malte Granderath, and Vaibhav Bajpai. 2022. One to Rule Them All? A First Look at DNS over QUIC. In *PAM*. Springer-Verlag, Berlin, Heidelberg, 537–551.

[60] Mike Kosek, Luca Schumann, Robin Marx, Trinh Viet Doan, and Vaibhav Bajpai. 2022. DNS Privacy With Speed? Evaluating DNS over QUIC and its Impact on Web Performance. In *IMC*. ACM, New York, USA, 44–50.

[61] Warren Kumari and Paul E. Hoffman. 2020. Running a Root Server Local to a Resolver. RFC 8806.

[62] Baiyang Li, Yujia Zhu, Yong Ding, Yong Sun, Yuedong Zhang, Qingyun Liu, and Li Guo. 2024. From Fingerprint to Footprint: Characterizing the Dependencies in Encrypted DNS Infrastructures. In *ESORICS*. Springer Nature Switzerland, Cham, 45–64.

[63] Ruixuan Li, Xiaofeng Jia, Zhenyong Zhang, Jun Shao, Rongxing Lu, Jingqiang Lin, Xiaoqi Jia, and Guiyi Wei. 2023. A Longitudinal and Comprehensive Measurement of DNS Strict Privacy. *IEEE/ACM Transactions on Networking* 31, 6 (2023), 2793–2808.

[64] Ruixuan Li, Baojun Liu, Chaoyi Lu, Haixin Duan, and Jun Shao. 2024. A Worldwide View on the Reachability of Encrypted DNS Services. In *WWW*. ACM, New York, USA, 1193–1202.

[65] Chaoyi Lu, Baojun Liu, Zhou Li, Shuang Hao, Haixin Duan, Mingming Zhang, Chunying Leng, Ying Liu, Zaifeng Zhang, and Jianping Wu. 2019. An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?. In *IMC*. ACM, New York, USA, 22–35.

[66] Paul Mockapetris. 1987. Domain names - concepts and facilities. RFC 1034.

[67] Paul Mockapetris. 1987. Domain names - implementation and specification. RFC 1035.

[68] Otto Moerbeek. 2022. Probing DoT Support of Authoritative Servers: Just Try It. https://blog.powerdns.com/2022/06/13/probing-dot-support-of-authoritative-servers-just-try-it.

[69] Marcin Nawrocki, Maynard Koch, Thomas C. Schmidt, and Matthias Wählisch. 2021. Transparent Forwarders: an Unnoticed Component of the Open DNS Infrastructure. In *CoNEXT*. ACM, New York, USA, 454–462.

[70] Nazwa.pl. 2025. Bezpieczna domena z DNSSEC i DNS over TLS w nazwa.pl. https://www.nazwa.pl/blog/bezpieczna-domena-z-dnssec-i-dns-over-tls-w-nazwa-pl.

[71] NLNet Labs. 2025. nsd.conf(5). https://nsd.docs.nlnetlabs.nl/en/latest/manpages/nsd.conf.html#tls~4.

[72] Yevheniya Nosyk, Qasim Lone, Yury Zhauniarovich, Carlos H. Gañán, Emile Aben, Giovane C. M. Moura, Samaneh Tajalizadehkhoob, Andrzej Duda, and Maciej Korczyński. 2023. Intercept and Inject: DNS Response Manipulation in the Wild. In *PAM*. Springer Nature Switzerland, Cham, 461–478.

[73] One.com. 2020. group.ONE to acquire Hostnet. https://www.group.one/en/news/group-one-to-acquire-hostnet.
[74] One.com. 2021. group.ONE acquires Dutch web hosting company Antagonist. https://www.group.one/en/news/group-one-acquires-dutch-web-hosting-company-antagonist.
[75] Craig Partridge and Mark Allman. 2016. Ethical Considerations in Network Measurement Papers. *Commun. ACM* 59, 10 (2016), 58–64.
[76] Tommy Pauly, Eric Kinnear, Christopher A. Wood, Patrick McManus, and Tommy Jensen. 2023. Discovery of Designated Resolvers. RFC 9462.
[77] Victor Le Pochat, Tom Van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczyński, and Wouter Joosen. 2019. Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation. In *NDSS*. The Internet Society, Reston, The USA, 1–15.
[78] PowerDNS. 2025. dnsdist Overview. https://www.dnsdist.org/index.html.
[79] Scott Rose, Matt Larson, Dan Massey, Rob Austein, and Roy Arends. 2005. DNS Security Introduction and Requirements. RFC 4033.
[80] Scott Rose, Matt Larson, Dan Massey, Rob Austein, and Roy Arends. 2005. Protocol Modifications for the DNS Security Extensions. RFC 4035.
[81] Scott Rose, Matt Larson, Dan Massey, Rob Austein, and Roy Arends. 2005. Resource Records for the DNS Security Extensions. RFC 4034.
[82] Sandra Siby, Marc Juarez, Claudia Díaz, Narseo Vallina-Rodriguez, and Carmela Troncoso. 2020. Encrypted DNS -> Privacy? A Traffic Analysis Perspective. In *NDSS*. The Internet Society, San Diego, USA, 1–18.
[83] SIE Europe. 2025. Passive DNS Data Sharing. https://www.sie-europe.net.
[84] Johan Stenstam, Leon Fernandez, and Erik Bergström. 2025. *Authoritative DNS Transport Signaling*. Internet-Draft draft-johani-dnsop-transport-signaling-01. Internet Engineering Task Force. Work in Progress.
[85] Satoru Sunahara, Yong Jin, and Katsuyoshi Iida. 2023. Authoritative DNS Server Discovery Method to Enhance DNS Privacy Preservation. In *CoNEXT Student Workshop*. ACM, New York, NY, USA, 31–32.
[86] Yorgos Thessalonikefs. 2023. Re: [dns-privacy] WGLC : draft-ietf-dprive-unilateral-probing. https://mailarchive.ietf.org/arch/msg/dns-privacy/U63a-sl9SfZDPp8aqcasNGNYDUI.
[87] Martino Trevisan, Francesca Soro, Marco Mellia, Idilio Drago, and Ricardo Morla. 2020. Does Domain Name Encryption Increase Users' Privacy? *SIGCOMM Comput. Commun. Rev.* 50, 3 (July 2020), 16–22.
[88] Mauricio Vergara Ereche. 2010. [dns-operations] Odd behaviour on one node in I root-server (facebook, youtube & twitter). https://lists.dns-oarc.net/pipermail/dns-operations/2010-March/005263.html.
[89] Vasilis Ververis, Steffen Sassala, Felix Roth, and Vaibhav Bajpai. 2025. Path to Encrypted DNS with DDR: Adoption, Configuration Patterns, and Privacy Implications. *Proc. Priv. Enhancing Technol.* 2025, 4 (2025), 465–484.
[90] WEDOS.zone. 2025. DNS over QUIC. https://wedos.zone/dns-over-quic.

A ETHICS

We designed our methodology to ensure it adheres to best current practices in the field of Internet measurements [23, 27, 75]. We send the minimum necessary number of DNS packets to meaningfully answer our research questions. We only target confirmed recursive resolvers and authoritative nameservers, therefore not overloading non-DNS systems with probing requests. Whenever possible, we use datasets provided by other researchers (e.g., the list of open IPv4 resolvers and IPv6 hosts open on port 53) to avoid duplicate scanning efforts.