On QoE Impact of DoH and DoT in Africa: Why a User's DNS Choice Matters

Enock S. Mbewe(✉) and Josiah Chavula

University of Cape Town, Cape Town 7701, WC, RSA
{embewe,jchavula}@cs.uct.ac.za

Abstract. Internet security and Quality of Experience (QoE) are two antagonistic concepts that the research community has been attempting to reconcile. Internet security has of late received attention due to users' online privacy and security concerns. One example is the introduction of encrypted Domain Name System (DNS) protocols. These protocols, combined with suboptimal routing paths and offshore hosting, have the potential to negatively impact the quality of web browsing experience for users in Africa. This is particularly the case in edge access networks that are far away from essential infrastructures such as DNS and content servers. In this paper, we analyse the QoE impact of using open public DoH and DoT resolvers when resolving websites that are hosted in Africa versus those hosted offshore. The study further compares the performance of DoT and DoH under different network conditions (mobile, community network, Eduroam and Campus wired network). Our results show that high latency and circuitous DNS resolution paths amplify the performance impact of secure DNS protocols on DNS resolution time and page load time. The study further shows that users' DNS resolver preferences hugely determine the level of QoE. This study proposes wider adoption of Transport Layer Security version 1.3 (TLSv1.3) to leverage its latency-reduction features such as *false start* and *Zero or One Round Trip Time* (0/1-RTT). The study further proposes the localisation of content and secure DNS infrastructure. This, coupled with peering and cache sharing recommended by other works, will further minimise the impact of secure DNS protocols on Quality of Experience.

Keywords: Networks · Network performance · Internet security · DNS privacy · QoE

1 Introduction

Domain Name System (DNS) [1] is one of the fundamental components of the Internet which maps the human-readable names to their respective IP addresses of Internet resources. For most of the Internet's history, these services have been delivered in plaintext providing a fertile ground for attackers to exploit this

R. Zitouni et al. (Eds.): AFRICOMM 2020, LNICST 361, pp. 289–304, 2021.
https://doi.org/10.1007/978-3-030-70572-5_18

vulnerability and compromise Internet users' security and privacy online. Some governments, Internet Service Providers and other players exploited this vulnerability by using DNS for pervasive monitoring, Internet censorship, content control and other attacks as reported in RFC 7258 [2]. As a result, various efforts have been developed to encrypt cryptographically sign the DNS queries. These efforts have resulted in the development of different protocols such as DNS over TLS (DoT) [3], DNS over DTLS, DNS over QUIC, DNS over HTTPS (DoH) [4] and DNSCrypt [5]. Although these protocols are relatively new, there has been increased adoption of some by service providers, OS vendors and software vendors. Lu *et al.* [6] collectively call these DNS encryption protocols *DNS over Encryption (DoE)* the term we use in this paper. Amongst these protocols, DoT and DoH are two standardised which are gaining grounds in the industry and research communities. Our study, therefore, focuses on these two protocols as measured from Internet user's networks and devices.

Much as these are desirable developments that provide essential security goals, Internet users should be willing to bear the extra QoE costs that come with security [7–9]. Generally, DNS-over-Encryption can incur performance overhead for DNS clients due to an extra delay TLS session setup and encryption [6]. Measuring the real impact of DoE would help the users make a rational decision and correctly estimate their QoE expectations. The Internet research community has tried to measure the impact of DoE on DNS resolution and page load time. However, none of the measurement studies has focused on edge access networks commonly found in developing regions such as Africa. Therefore, the findings from these studies cannot be generalised.

This paper presents the results of Internet security measurements study taken from different edge networks in Africa. We specifically aimed to find out the extent to which DoE coupled with latency and offshore content hosting would impact overall Quality of Experience. To ably achieve this aim, we carried out measurements from end-user networks in seven (7) African countries: Madagascar, Malawi, Nigeria, Kenya, Uganda, South Africa and Zambia. We measured the impact of DoE provided by the open DNS recursive resolvers on DNS resolution time (DRT) and page load time (PLT). To correctly estimate the impact of DoE, we measure the cost of resolving with regular plaintext DNS (hereafter referred to as Do53) from both the user network, which we call local Do53 and remote Do53 measured from each of the open public DNS recursors. The following is a summary of our major findings:

i. *We find that unencrypted DNS transport is by far faster than the encrypted DNS transport in high-delay, lossy edge networks.*
ii. *We find that network conditions, user's DNS resolver choice, webserver and DNS resolver geolocation hugely determine the QoE (DNS response times, page load times and success and failure rates of Secure DNS resolution).*
iii. *Comparably, we find that providers having their caches in Africa have a higher probability of successfully resolving names than distant recursors. Therefore, we motivate for the implementation of local DoE infrastructure by the Internet Service Providers (ISPs) to further reduce the DNS response time and page load time hence improving QoE for Internet users.*

2 Background

Unreliable, slow, insecure, expensive or non-existent Internet access remains a big problem for billions of people in the developing world where the physical infrastructure is still underdeveloped. Bandwidth is generally an expensive resource for developing regions with low user densities [10]. Despite the recent development of the internet infrastructure in these regions, Quality of Experience for users is often impacted by high latencies resulting from circuitous name resolution as observed by Formoso *et al.* [11]. Recent studies [12,13] report that African content is normally hosted in North America despite the availability of some Content Delivery Networks in the region. This may be attributed to the cost of hosting and unreliability of power in most of the underdeveloped countries. Apart from bandwidth, latency is caused by a number of factors including lossy links and lack of peering between the networks, preventing the sharing of CDN servers, as well as poorly configured DNS resolvers [14]. Besides these works, this study has especially been inspired by the study conducted by Calandro *et al.* [13]. The authors surveyed the type of content commonly produced and consumed in Africa. They further conducted active latency and traceroute measurements to locate webservers hosting the African content. They found that most of the content is hosted outside the countries owning such content and most often, offshore. In this study, we measure how these observations combined secure DNS resolution would impact DNS response time and page load time.

Given the recency of DoT and DoH, the research community is yet to establish the real performance cost of these protocols. At the writing of this paper, we know of very few measurement studies on the performance cost of DoT and DoH. An early preliminary study by Mozilla[1] found that DoH lookups are only marginally slower (6 ms) than conventional, unencrypted DNS over port 53 (Do53). Bottger *et al.* [15] studied the DoH ecosystem to understand the cost of the additional DNS security. Their findings indicate that the impact is marginal and does not heavily impact the page load times. In their works, Hounsel, et al. ([16] and [17]), compared the cost of DoT and DoH measured from campus network and Amazon ec2 instances. Their results show that although the resolution times of Do53 is better than that of DoT and DoH, both protocols can perform better than Do53 in terms of page load times. Lu *et al.* [6] conducted end-to-end DNS-over-Encryption measurements and found that that generally the service quality of DNS-over-Encryption is satisfying, in terms of accessibility and latency and that the added latency is worth it. DoH, in particular, is attracting the attention of the research community due to its current centralised implementation. Some fear to entrust valuable browsing information to a few providers. As such, some works are focusing on de-centralising DoH so that no single provider has all the browsing information. Hoang *et al.* [18] propose K-resolver to slice user information to different decentralised DoH resolvers. This,

[1] See https://blog.nightly.mozilla.org/2018/08/28/firefox-nightly-secure-dns-experimental-results.

however, suffers from increased latency when the servers are geographically separated. A similar study is conducted by Hounsel *et al.* [19] which proposes a distributed DoH server architecture called M-DNS.

In this paper, we measure and compare DNS response and page load times to websites hosted within Africa versus websites hosted in America and Europe respectively. We conduct measurements from edge network (3G/4G mobile networks, community wireless network and home broadband) vantage points in Africa. We perform these measurements against open public DNS recursive resolvers such as Google, Cloudflare, Quad9, CleanBrowsing and AdGuard. We also measure latency to each of the recursors and websites to provide a context for our findings.

3 Methodology

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

3.1 Metrics

This study aimed to understand how Do53, DoT and DoH impact browsing Quality of Experience (QoE). The study considered network-level and browser-level metrics. These metrics are latency, DNS response time (in this paper referred to as DRT), DNS success and failure rates and page load time (PLT).

Latency. Several studies have pointed out that African networks suffer higher latencies. Recent studies [11,13,14] have attributed these latencies to suboptimal routing, lack of peering and cache sharing. Other studies have attributed these latencies to offshore hosting and misconfiguration of DNS. However, none of these works has looked at the impact of latency on security protocols in the region. Latency determines the kind of applications that can run on affected networks. For example, VoIP and video conferencing may allow latency of not more than 400 ms and online gaming, not more than 200 ms. Therefore, it is important to understand the extent to which the secure DNS protocols add on to the already high latency in order to inform Internet users of what applications may run on a given network condition. Also, it is important to show which public DNS providers respond with reasonable latency as this would aid users in the choice of DNS recursive resolvers. We also perform latency measurements to resolvers and websites in order to explain the source of delays in our results. We conduct ping measurements to each of the recursors and domains using different DNS configurations. We then calculate the median RTT for each latency measurement.

DNS Resolution Time. DNS query response time is one of the major factors that affect the speed of page rendering in the browser. A web page normally contains several objects fetched from different servers. In this study, we measured DNS resolution time firstly for the main page, and thereafter, for each domain, we collected all the unique domains for components (i.e. images, JavaScript, CSS etc.) and measured their respective DNS Response time. We use *getdns* and *libcurl* C libraries to issue Do53, DoT, and DoH queries. *Getdns* provides an API that allows developers to perform DNS Do53 and DoT requests using different programming languages. Libcurl supports POST requests to be sent via HTTPS. This capability enables us to measure DoH DNS response time. We could have gotten the DNS response times from the collected HARs, however, we noted that some of the timings were not correct and decided to use the *getdns*. It is important to note that the DNS responses were not cached by the browser used in the measurements to make sure that the subsequent transaction is not affected by the cache.

DNS-Related Failure Rates. Failures within DNS can have a dramatic impact on the wider Internet, most notably preventing access to any services dependent on domain names (e.g. web, mobile apps) [20]. Recent studies on Do53, DoT and DoH have found that encrypted queries tend to fail more than the regular DNS. Hounsel et al. [16] found that in lossier conditions, such as 3G, DoH experiences higher failure rates compared to Do53. This work seeks to establish DNS failure rates from real 3G and 4G conditions. We argue that understanding the prevalence of errors resulting from a particular DNS protocol is essential in informing the users' choice of DNS protocols given their network conditions.

Page Load Time. Page load time is an important metric of browser-based QoE. It represents the amount of time a user has to wait before the page is loaded in a browser. In this study, Firefox was used in headless mode to visit a set of HTTPS-enabled websites. For each website, we collect HAR files in JSON format containing timing information, including blocking information, proxy negotiation, DNS lookup, TCP handshake, SSL, Requests, Waiting and Content download. From the HAR files, we record the *onLoad* timing - the time taken to completely load the page together with its components.

3.2 Experiment Setup

We begin by describing how we collected the dataset that we analyse in this study. The study uses Alexa top 50 global websites for African countries[2] and top 50 Alexa local websites[3] for each African country (hosted locally or operated by local entities). The local websites were particularly included to represent the

[2] https://www.alexa.com/topsites/countries.
[3] https://www.alexa.com/topsites/category/Top/Regional/Africa.

websites serving African content and observe how DoT and DoH impact the browsing QoE on the local websites. These websites are normally not heavily cached in different public DNS recursive resolvers. We managed to get 2294 unique websites altogether. We then used *pshtt* modules of domain-scanner[4] application to find the websites that were online and responsive on port 443. This process gave us 1583 websites.

We then used MaxMind to geolocate 1206 websites. Of the 1206 websites, we found that 55.7% of the websites are hosted in North America, 27.6% in Europe, 14.4% in Africa, 1.7% in Asia, 0, 5% in Oceania and 0.1% in South America. We then selected the first three continents which served the most websites in our dataset. We randomly selected an equal number (173) of websites from America and Europe datasets. The 173 value came from the lowest number of websites in the selected continents, which is Africa in our case. This gave us 519 websites which we use in this study. We did this to have a common denominator for on which to base our results and discussion. For each of these continents, we looked at the common TLS protocols negotiated. We found that America had the highest number of websites that negotiated TLS1.3 (84%) and the remaining 16% negotiated TLS1.2. Africa had 84% TLS1.2, 15% TLS1.3 and 1% TLS1.0 while Europe had 87% TLS1.2, 12% TLS1.3 and 1% TLS1.0.

To replicate web browser actions when a user visits a website, we follow a methodology used in a study by Hounsel *et al.* [16]. We use automated Firefox 67.0.1 to randomly visit the websites in our list in headless mode. This is a clean instance without any ad or pop-up blockers. We, however, install a plugin to export HTTP Archive objects (HARs) from each visited website. We store these HARs in a PostgreSQL database as JSON objects. The study also aimed at measuring how the selection of DNS recursive resolver and DNS transport affect browser performance which, in turn, affects user's QoE. As such, we use 5 DNS recursive resolvers each offering Do53, DoH and DoT. Additionally, we used default Do53 at each vantage point. It is important to note that the default resolvers only support Do53 and this serves as a baseline for the performance over Do53. Table 1 lists resolvers used in this study. Of the five resolvers, three (Google, Cloudflare and Quad9) negotiated TLS1.3 while CleanBrowsing and AdGuard negotiate TLS1.2.

Firefox web browser natively supports Do53 and DoH. On the other hand, DoT has to be configured on the user's machine outside of the browser. As such, we use Stubby for DoT resolution, a stub resolver based on the getdns library. Stubby listens on a loopback address and responds to Do53 queries. All DNS queries received by Stubby are then sent out to a configured recursor over DoT. We modify /etc/resolv.conf on our measurement systems to point to the loopback address served by Stubby. This forces all DNS queries initiated by Firefox to be sent over DoT.

Between the measurements, we were not able to control the caches of the recursive resolvers. We, therefore, randomised the order of arguments that were presented to the browser in the form of a tuple comprising websites, DNS

[4] https://github.com/18F/domain-scan.

Table 1. Compared DNS resolvers

Configuration	Do53/DoT address	DoH URI	Marker
Local	Default Do53	None	Local
Cloudflare	1.1.1.1	https://cloudflare-dns.com/dns-query	CF
Google	8.8.8.8	https://dns.google/dns-query	GG
Quad9	9.9.9.9	https://dns.quad9.net/dns-query	Q9
CleanBrowsing	185.228.168.168	https://doh.cleanbrowsing.org/doh/security-filter	CB
AdGuard	176.103.130.131	https://dns.adguard.com/dns-query	AG

recursive resolvers and DNS protocols. This was done to avoid biasing results due to network quiet and busy times, as well as the potential effect of a query warming the recursor's cache for subsequent queries from the other protocols tested.

This measurements study was done from February 2020 to 21 May 2020. The measurements were done from 14 vantage points located in 7 countries; Malawi, Madagascar, South Africa, Kenya, Zambia, Nigeria and Uganda. This study aimed at measuring the impact of DoT and DoH on user's Quality of Experience hence the measurements were conducted at network edges. As such we used our contacts from 5 of these seven countries. These countries are (with their respective networks we measured from enclosed in brackets after the country name): Madagascar (Widecom), Zambia (MTN, Liquid telecoms), Uganda (Airtel, Orange), Kenya (Airtel) and Nigeria (MTN). The researchers had access to two countries; Malawi (TNM, Airtel, wired Campus network) and South Africa (Vodacom, Eduroam, Campus wired network, Community network). The participants were compensated with extra Internet data bundles.

At each vantage point, we conducted two sessions of measurements; one under 4G and another under 3G. Measurements were also conducted on a wireless community network and two University campus networks (Wired and Eduroam) in South Africa. The community networks are becoming more prevalent in the region as a low-cost Internet access network managed and operated by communities to meet their communication needs [21]. The campus networks represent the well connected, higher resourced networks which we use to benchmark our results.

We ran the measurements on computers running Ubuntu 18.04 desktop version. We packaged the Firefox browser in a docker container for portability. The tools ran on i5 computes with 8 GB of RAM except for one PC which had 16 GB RAM.

4 Results

In this section, we present findings from the measurements conducted. We start with an overview of the data collected from all vantage points, and thereafter, we highlight vantage points and protocols that show peculiar results. We focus the discussion on comparing the performance of different DNS configuration from 4G

networks. The evaluation is also based on the continent in which the websites are hosted. We then benchmark these findings against measurements from university campus networks, representing the high-end networks. It is important to note that in the dataset we have timings longer than four seconds. However, using boxplots we can identify the distribution of the data and comfortably cut off outliers. As can be seen from the results in this section we place a cut-off point at 2000 ms for latency and DNS response time. We further use the median difference for page load time.

4.1 Transport Delay

Following our findings in terms of DNS response time and page load time, we deep-dived into other determinants of Internet performance, such as latency and DNS resolution paths. To do this, we conducted ICMP ping measurements and traceroute measurements.

Latency Measurements: Each time we performed a page load test, we performed ICMP five ping tests to each resolver. We observe that Quad9, Local, Cloudflare, Google, Cleanbrowsing, and Adguard have median round trip times (RTTs) of 229.4 ms, 328.8 ms, 333.8 ms, 381 ms, 443.4 ms and 1296 ms respectively. On the median case, we see that Quad9 has lower latency than the Local resolver. We note that AdGuard has the highest RTT. Zooming into the performance of providers in different countries, we observe varying results. Figure 1 shows the average latency from different countries to public DNS resolvers. From this figure, we observe that generally, Local resolver outperforms the remote DNS resolvers. This can be observed in Kenya, Madagascar, South Africa, Uganda and Zambia. This can be attributed to good peering enabled by Internet Exchange points available in the countries. On the other hand, Malawi's Local median RTT is almost equal to that of Google and Cloudflare. This suggests that the networks use either Cloudflare or Google as default resolver(s). However, Malawi's networks would have experienced lower latency (median 250 ms) if Quad9 is used as a default resolver. A similar pattern is observed from Nigeria, where the default resolver had minimum RTTs of >200 ms and hence outside our cleaned data. Nigeria's MTN network would have experienced lower latencies if it used Google (≈250 ms) as a default resolver. This is unsurprising since Google has a cache in Nigeria.

Network wise, we found that the RTTs vary from one network type to another. For example, in South Africa, we conducted measurements under 3G, 4G, community wireless network, Eduroam and Campus wired networks. Comparing the RTTs under these network types, we found that campus networks had lower RTTs. We found that ≈90% of latency to Cloudflare resolver from campus networks was under 20 ms. In the same range of 1 ms–20 ms, from 4G, 3G and community networks, no transaction was recorded. The RTTs to Cloudflare, under 3G, ranged from 140 ms to 210 ms with ≈90% of the transactions under 200 ms. On the other hand, under 4G, RTTs were in the range of 90 ms–110 ms

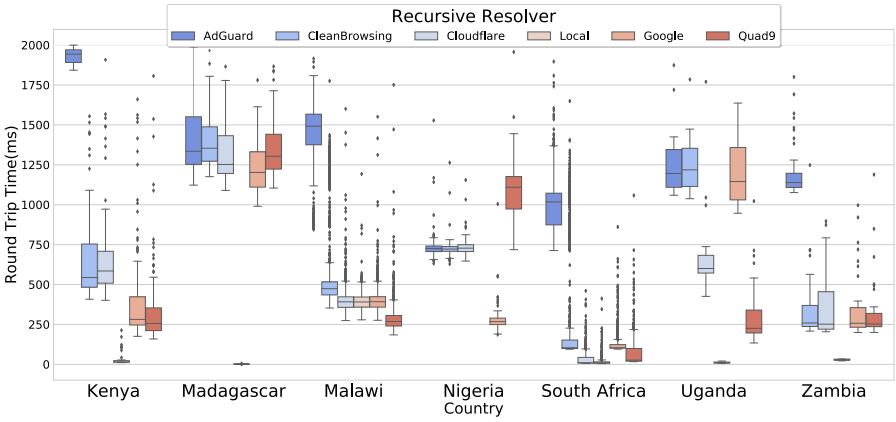


Fig. 1. Round Trip Time (RTT) to the public recursive resolvers from seven countries

with ≈96% of the transactions under 100 ms. We further categorised the RTTs based on DNS type. Interestingly, we observed that all the three protocols Do53, DoH and DoH had comparable RTTs suggesting that DNS resolvers (i.e. Do53, DoH and DoT) from the same provider are co-located.

We note in our dataset that a greater percentage of webservers in Africa (84%) and Europe (87%) negotiated TLSv1.2, a protocol that expends Two Round Trip Time (2-RTT) during TLS handshake. This implies that higher latency networks would experience even higher page load times (PLTs) and DNS response times when lower versions of TLS are used. We find that, in general, DoT performed better than DoH for websites hosted in Africa, with PLT average difference of 650 ms, even though 84% of such websites used TLSv1.2. We expect that QoE for websites hosted Africa and Europe would improve if webservers in these regions negotiated TLSv1.3, which uses 0/1-RTT when performing TLS handshake.

Traceroute Measurements: To understand the reason behind higher latencies to resolvers form some countries, we conducted traceroute measurements to geolocate the DNS recursors. We performed traceroute to each of the resolvers in our measurement tool. The findings show that the paths to some resolvers are longer than others. For example, looking at the previous host before the final destination, we notice that for DNS providers have their presence in South Africa. However, the paths taken from various countries to South Africa differ, even between two ISPs from the same country. For example, from a vantage point in Malawi, Airtel network had lower RTTs than Telkom Networks Malawi (TNM). To understand the reason behind these varying RTTs in these networks, we conducted traceroute measurements from our vantage points to the DNS resolvers. We notice that all the paths to the resolvers pass through South Africa; however, the traceroute measurements revealed that these networks use different network

paths to the same destination. For example, Cloudflare resolver (1.1.1.1) is one hop (ASN) away from Airtel subscribers compared to three hops (ASNs) under TNM.

4.2 Pageload Success and Failure Rates

Table 2 shows the success and failure rates for the page loads. It also presents error types we encountered during our measurements. Generally, Do53 has higher success rates compared to DoT and DoH under all the network conditions in all the three continents. DoH has the lowest success rate across networks when resolving websites hosted in all the three continents. A closer look to at the individual recursive resolver's performance, we observe that DoH is affected much with deteriorating network conditions and distance to the resolver. The worst DoH success rate is observed when resolving websites hosted in Europe on 3G with 24% success rate and 43% DNS error rate. This can be attributed to caching issues; users in Africa mostly consume content hosted in North America, which suggests that most of the American hosted content exist in African caches.

We noted that the *Other Errors* are quite high compared to *Selenium* and *Pageload timeout*. This prompted us to look into what might be these errors which included *refused*, *DoT stub errors* and *nss* errors.

We observe that the success or failure rates depend on the network conditions and DNS protocol. We note in our results that the rates are directly proportional to network conditions; the better the network conditions (bandwidth, delay), the higher the success rate and vice versa. For example, we note (Table 2) failure reduction as we move from 3G, 4G and Eduroam. These observations further indicate that the success of connection depends on the users' choice of DNS protocol.

4.3 DNS Resolution Delay

Overall, as expected, we find that Do53 has a lower DNS resolution time (DRT) compared to DoT and DoH across all the resolvers. It should be noted that we have two kinds of Do53; local and remote (provided by the open public resolvers). Figure 2 shows a category plot for DNS response times for different recursive resolvers grouped by continent and DNS protocol. This implies that users have to bear some substantial cost to benefit from DNS security. The difference between DoE and Do53 on the same DNS provider is substantially wide. We note from the latency results that DoE and Do53 from the same DNS provider were colocated except AdGuard which showed a median RTT difference of ≈200 ms. This RTT difference translates to a median response time difference of ≈750 ms between AdGuard's DoE and Do53 as shown in Fig. 2. We observe a marginal difference between DoE from the same DNS provider with DoH having lower response times than DoT except for Google which displays the opposite when resolving domains hosted in Europe and North America. However, Google's DoE seems to perform uniformly when resolving sites hosted in Africa. We further observe that Quad9's DoT has way higher than its DoH despite having comparable median.

Table 2. Success and Error rate for Do53, DoT and DoH to websites hosted in Africa, Europe and North America respectively under 3G, 4G and Eduroam networks.

Continent	Network	Protocol	Successful (%)	DNS error (%)	Pageload error (%)	Selenium error (%)	Other errors (%)
Africa	3G	dns	61.33	11	0	10.33	17.33
		doh	47.88	35.45	0	4.55	12.12
		dot	58.63	12.2	0	11.61	17.56
	4G	dns	79.37	2.73	1.02	1.26	15.63
		doh	61.14	23.63	0.7	1.17	13.37
		dot	79.52	2.64	1.14	1.39	15.31
	Eduroam	dns	85.98	2.49	1.85	2.12	7.56
		doh	65.06	24.9	1.08	2.16	6.8
		dot	77.3	11.93	1.41	2.32	7.04
Europe	3G	dns	54.7	4.27	0	14.53	26.5
		doh	24.62	43.85	0	18.46	13.08
		dot	55.3	5.3	0	15.15	24.24
	4G	dns	77.78	2.61	1.63	0.79	17.18
		doh	62.14	19.5	1.43	0.76	16.18
		dot	76.72	2.86	1.76	1.3	17.35
	Eduroam	dns	86.29	2.8	0.8	1	9.11
		doh	72.16	20.54	0.63	1.17	5.5
		dot	80.02	12.06	0.72	0.81	6.39
North America	3G	dns	64.22	7.33	0.43	17.67	10.34
		doh	49.22	31.01	0	12.4	7.36
		dot	60.38	8.46	1.15	17.69	12.31
	4G	dns	84.09	0.91	0.37	1.42	13.21
		doh	67.78	17.57	0.29	1.28	13.09
		dot	82.43	0.86	0.58	1.32	14.81
	Eduroam	dns	88.67	2.42	0.11	0.99	7.81
		doh	73.66	20.5	0.1	0.89	4.85
		dot	82.28	10.89	0	0.89	5.94

Much larger differences can be seen when we compare DNS providers against each other. From Fig. 2, we note that four of the five public resolvers (CleanBrowsing, Cloudflare, Google and Quad9) have ≈750 ms as their 3rd quartile. Surprisingly, CleanBrowsing shows even lower response times than Google and Quad9. We posit that the filtering performed by CleanBrowsing makes it skip some domains hence making it perform faster. As expected, AdGuard reports the highest DNS response times across the vantage points. This is as a result of the higher latencies to the resolvers. Cloudflare Do53 provides lower DNS response times than the ISP's (Local) resolvers in Fig. 2, cases. We mostly observe this from Zambia, Nigeria and Malawi (Fig. 3). It should be noted that Cloudflare does not support EDNS Client Subnet which scopes the cache per subnet which gives it the ability to aggressively cache DNS responses. Continent wise, we observe that cumulatively DoH reports lower response times for content hosted in Africa compared to content hosted offshore.

Figure 4 shows CDFs response times for Google, Cloudflare and Quad9 under 4G (Fig. 4a) and Campus wired network (Fig. 4b). We observe a noticeable difference between these networks. Of greater interest is the performance of Cloudflare's DoT on a wired network under 100 ms response time; it performs better than DoH and comparable to local Do53. For response times longer than 100 ms, DoH outperforms DoT. At response times longer than 400 ms, DoH seems to perform better than local Do53. This result concurs with the findings found by Hounsel *et al.* [16].

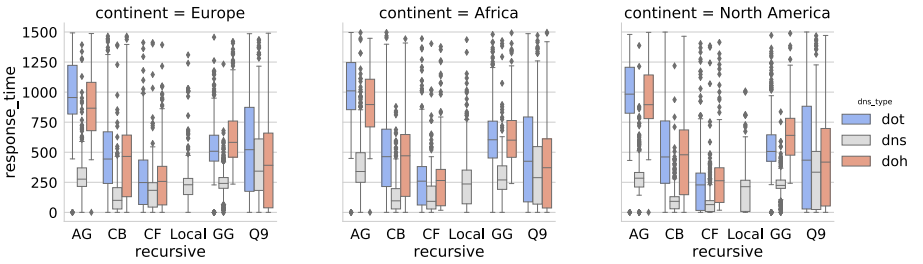


Fig. 2. DNS response time for different open public recursive resolvers when resolving websites hosted in Europe, Africa and North America from across the vantage points under 4G

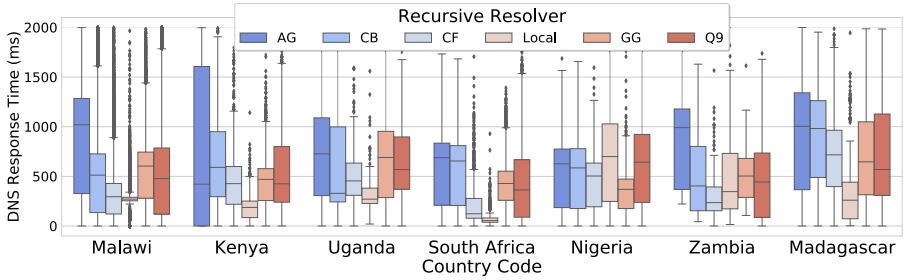
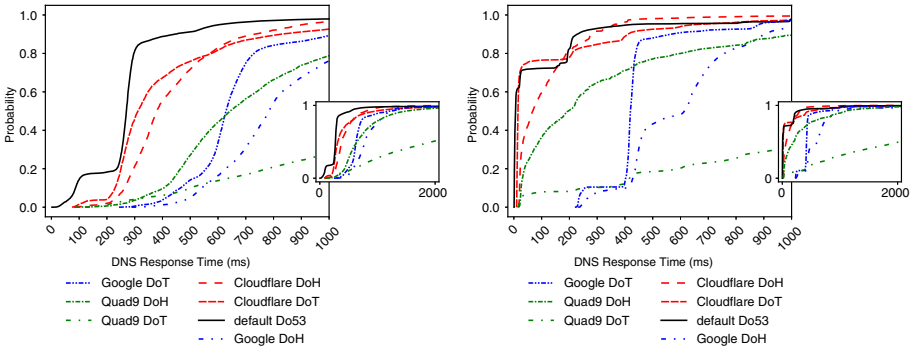


Fig. 3. DNS response time for each DNS recursive resolver across the vantage coutries under 4G

4.4 Page Load Times (PLT)

Pageload time is a more direct indication of how users experience web browsing. We have already seen the differences in query response times among the various DNS protocols under different network types across African vantage points. In this section, we show the relationship between the DNS response times and the page load times.



(a) DNS response time under 4G

(b) DNS response time under Campus Network

Fig. 4. DNS timings for local Do53 vs DoE from major DNS providers (Google, Cloudflare and Quad9) under 4G and Campus network

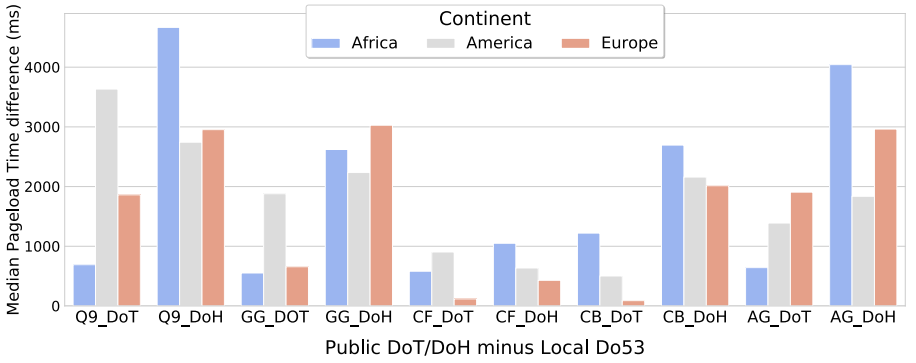


Fig. 5. Median pageload time differences between DoE and local Do53 when resolving websites hosted in Africa, North America and Europe measured from 4G networks

Figure 5 shows PLT differences between DoE resolvers (Google (GG), Cloudflare (CF), Quad9 (Q9), CleanBrowsing (CB) and AdGuard (AG)) and default Do53 when resolving websites hosted in Africa, America and Europe. The difference is calculated by taking the median page load time for a website/user using one secure resolver minus the median page load time of the same website/user using local resolver. The difference, therefore, is indicative of extra cost a user would bear when using secure DNS protocols provided by public DNS resolvers as compared to default Do53. From the graph, the lower PLT difference on the secure DNS resolvers implies that the performance is almost closer to that of default Do53.

Our first observation is that, unlike the pattern observed in DNS response times (Fig. 2) where DoT had relatively higher response times than DoH, Fig. 5 shows that generally, DoT has lower median response times than DoT. From Fig. 5, we note that DoT performs much better than DoH on websites hosted in

Africa, with a difference of less than 1000 ms. This behaviour can also be observed on the websites hosted in Europe except for CleanBrowsing's DoT which has a difference of ≈2000 ms. On the other hand, DoH has poorer performance in all DNS configurations for websites hosted in all continents, with a difference of more than 2000 ms. Quad9 DoH and AdGuard DoH, however, have the most impact, with PLT differences above 4000 ms. This implies that if 4G users configure DoH in place of default Do53, they should expect performance overhead of up to 4000 ms. We note that Cloudflare's DoT and DoH PLT differences are consistently lower across continents.

Zooming into Google's DoT and DoH PLT differences, we note an interesting result; Google's DoT PLT difference is ≈700 ms while DoH is ≈4700 ms. However, we expected Google to perform better in the region by the mere fact that Google has caches in several countries on the continent. This disparity could be due to protocol implementation issues, such as caching and ENDS Client Subnet support. Unlike Cloudflare, Google supports EDNS Client Subnet [22], which scopes the caches per subnet. This means that Google DoH would steer cache to ISPs' network, whereas Cloudflare cannot.

5 Limitations

This study has potential limitations which may affect the generalisation of our results. Firstly, we conducted the measurements from only 14 vantage points located in seven countries. Secondly, we conducted the measurements using automated Firefox on Ubuntu environment. Finally, we only used Maxmind as a geolocation database, which might affect the accuracy. Nonetheless, we argue that our findings provide an overview of DoT and DoH performance in Africa and their impact on the quality of browsing experience.

6 Conclusion

In this paper, we investigated the performance impact of public Do53, DoH, DoT on the websites hosted in Africa, North America and Europe. We also measured DNS resolution success rates and failure when local Do53, public Do53, DoT or DoH are used. While it is well understood that encrypted DNS protocols and systems are desirable for a safe and reliable Internet, these protocols have also been shown to negatively impact the quality of experience for web users. This is particularly true in higher-delay networks edge networks that are far away from critical infrastructures such as DNS resolvers and content servers. The negative impact is even more severe in developing regions such as Africa due to the prevalence of sub-optimal routing paths and offshore hosting. This paper has looked at the extent to which high latencies between users and resolvers, as well as offshore web hosting, impact the performance of secure DNS resolution and the overall web browsing performance.

Recent studies [11,13,14] have reported that networks in the region experience high latencies due to lack of local peering. Fanou *et al.* [14] further found that African countries hardly share caches leaving cacheless countries with no option but to fetch the content using longer paths. Our results show this pattern, where different countries show different results for the same recursive resolver. In addition to localisation of content and cache sharing proposed by these and other authors, this study recommends that ISPs should consider implementing local DNS over Encryption infrastructure to reduce DNS resolution path, which, in turn, will improve the Quality of Protection and Experience to their customers. We noted in the results that DoH was affected by network conditions and latency – implementing local DoH servers would improve its performance and success rate. We further recommend the wide adoption of newer security protocols such as TLS1.3, which is designed to reduce the latency impact of the older versions of TLS.

Acknowledgements. The authors are grateful for the financial support received from the Hasso Plattner Institute for Digital Engineering, through the HPI Research School at the University of Cape Town. The authors would like to thank Nick Feamster and Austin Hounsel for their help and inspiration in this study.

References

1. Mockapetris, P.: Domain names - concepts and facilities, RFC 1034, IETF, November 1987
2. Farrell, S., Tschofenig, H.: Pervasive monitoring is an attack, RFC 7258, IETF, May 2014
3. Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., Hoffman, P.: Specification for DNS over Transport Layer Security (DoTLS), RFC 7858, IETF, May 2016
4. McManus, P.H.P.: DNS queries over HTTPS (DoH), RFC 8484, IETF, October 2018
5. dnscrypt.info: DNSCrypt version 2 protocol specification. DNSCrypt, 14 July 2019. https://dnscrypt.info/protocol. Accessed 22 Aug 2019
6. Lu, C., et al.: An end-to-end, large-scale measurement of DNS-over-encryption: how far have we come?. In: Proceedings of the Internet Measurement Conference (2019)
7. Radmand, P., Talevski, A.: Impact of encryption on QoS in VoIP. In: 2010 IEEE Second International Conference on Social Computing, pp. 721–726, August 2010
8. Mohammed, H.A., Ali, A.H.: Effect of some security mechanisms on the QoS VoIP application using OPNET. Int. J. Current Eng. Technol. **3**, 1626–1630 (2013)
9. Spyropoulou, E., Levin, T., Irvine, C.: Calculating costs for quality of Security service. In: Proceedings 16th Annual Computer Security Applications Conference (ACSAC 2000), pp. 334–343, December 2000
10. Chen, J., Amershi, S., Dhananjay, A., Subramanian, L.: Comparing Web interaction models in developing regions. In: Proceedings of the First ACM Symposium on Computing for Development, ACM DEV 2010, pp. 6:1–6:9. ACM, New York (2010)
11. Formoso, A., Chavula, J., Phokeer, A., Sathiaseelan, A., Tyson, G.: Deep diving into Africa's inter-country latencies. In: IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, pp. 2231–2239, April 2018

12. Fanou, R., Tyson, G., Francois, P., Sathiaseelan, A.: Pushing the frontier: exploring the African Web ecosystem. In: Proceedings of the 25th International Conference on World Wide Web, WWW 2016, pp. 435–445. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva (2016)
13. Calandro, E., Chavula, J., Phokeer, A.: Internet development in Africa: a content use, hosting and distribution perspective. In: Mendy, G., Ouya, S., Dioum, I., Thiaré, O. (eds.) AFRICOMM 2018. LNICST, vol. 275, pp. 131–141. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-16042-5_13
14. Fanou, R., Tyson, G., Fernandes, E.L., Francois, P., Valera, F., Sathiaseelan, A.: Exploring and analysing the African Web ecosystem. ACM Trans. Web **12**, 22:1–22:26 (2018)
15. Böttger, T., et al.: An empirical study of the cost of DNS-over-HTTPs. In: Proceedings of the Internet Measurement Conference, IMC 2019, pp. 15–21, Association for Computing Machinery, New York (2019)
16. Hounsel, A., Borgolte, K., Schmitt, P., Holland, J., Feamster, N.: Analyzing the costs (and benefits) of DNS, DoT, and DoH for the modern web. In: Proceedings of the Applied Networking Research Workshop (2019)
17. Hounsel, A., Borgolte, K., Schmitt, P., Holland, J., Feamster, N.: Comparing the effects of DNS, DoT, and DoH on web performance. In: Proceedings of The Web Conference 2020, WWW 2020, pp. 562–572. Association for Computing Machinery, New York (2020)
18. Hoang, N.P., Lin, I., Ghavamnia, S., Polychronakis, M.: K-resolver: towards decentralizing encrypted DNS resolution. ArXiv, vol. abs/2001.08901 (2020)
19. Hounsel, A., Borgolte, K., Schmitt, P., Feamster, N.: D-DNS: towards redecentralizing the DNS, 02 2020
20. Yang, D., Li, Z., Tyson, G.: A deep dive into DNS query failures. In: 2020 USENIX Annual Technical Conference (USENIX ATC 20), pp. 507–514, USENIX Association, July 2020
21. Rey-Moreno, C.: Supporting the creation and scalability of affordable access solutions. Annual report, Internet Society, May 2017
22. Contavalli, C., van der Gaast, W., Lawrence, D., Kumari, W.: Client Subnet in DNS Queries, RFC 7871, IETF, May 2016