An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?

Chaoyi Lu[1,2], Baojun Liu[3], Zhou Li[4], Shuang Hao[5], Haixin Duan[1,2,6], Mingming Zhang[1], Chunying Leng[1], Ying Liu[1], Zaifeng Zhang[7] and Jianping Wu[1]
[1]Institute for Network Sciences and Cyberspace, Tsinghua University
[2]Beijing National Research Center for Information Science and Technology (BNRist), Tsinghua University
[3]Department of Computer Science and Technology, Tsinghua University [4]University of California, Irvine
[5]University of Texas at Dallas [6]Qi An Xin Technology Research Institute [7]360 Netlab

ABSTRACT

DNS packets are designed to travel in unencrypted form through the Internet based on its initial standard. Recent discoveries show that real-world adversaries are actively exploiting this design vulnerability to compromise Internet users' security and privacy. To mitigate such threats, several protocols have been proposed to encrypt DNS queries between DNS clients and servers, which we jointly term as DNS-over-Encryption. While some proposals have been standardized and are gaining strong support from the industry, little has been done to understand their status from the view of global users.

This paper performs by far the first end-to-end and large-scale analysis on DNS-over-Encryption. By collecting data from Internet scanning, user-end measurement and passive monitoring logs, we have gained several unique insights. In general, the service quality of DNS-over-Encryption is satisfying, in terms of accessibility and latency. For DNS clients, DNS-over-Encryption queries are less likely to be disrupted by in-path interception compared to traditional DNS, and the extra overhead is tolerable. However, we also discover several issues regarding how the services are operated. As an example, we find 25% DNS-over-TLS service providers use invalid SSL certificates. Compared to traditional DNS, DNS-over-Encryption is used by far fewer users but we have witnessed a growing trend. As such, we believe the community should push broader adoption of DNS-over-Encryption and we also suggest the service providers carefully review their implementations.

CCS CONCEPTS

• **Networks** → **Application layer protocols**; **Network measurement**; *Naming and addressing*.

Haixin Duan and Ying Liu are the corresponding authors.
This work is done during Chaoyi Lu's research internship at 360 Netlab.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
IMC '19, October 21–23, 2019, Amsterdam, Netherlands
© 2019 Copyright held by the owner/author(s). Publication rights licensed to ACM.
ACM ISBN 978-1-4503-6948-0/19/10…$15.00
https://doi.org/10.1145/3355369.3355580

KEYWORDS

Domane Name System, DNS Privacy, DNS-over-TLS, DNS-over-HTTPS, DNS Measurement

ACM Reference Format:
Chaoyi Lu[1,2], Baojun Liu[3], Zhou Li[4], Shuang Hao[5], Haixin Duan[1,2,6], Mingming Zhang[1], Chunying Leng[1], Ying Liu[1], Zaifeng Zhang[7] and Jianping Wu[1]. 2019. An End-to-End, Large-Scale Measurement of DNS-over-Encryption: How Far Have We Come?. In *Internet Measurement Conference (IMC '19), October 21–23, 2019, Amsterdam, Netherlands.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3355369.3355580

1 INTRODUCTION

Domain Name System (DNS) is one of the fundamental building blocks of the Internet, mapping a user-friendly domain name to numerical IP addresses. According to its initial IETF standard, DNS packets are transmitted over UDP protocol *in clear-text*. Therefore, communication integrity and confidentiality are absent. Unfortunately, this design makes DNS communications vulnerable to attacks like eavesdropping and tampering [29]. In fact, real-world adversaries have been exploiting DNS to harm Internet users. As an example, released secret documents show that NSA has been covertly monitoring and hijacking DNS traffic, under the MoreCowBell [44] and QuantumDNS [12] projects. A recent study also shows that network middleboxes are actively intercepting DNS packets and rerouting them to alternative resolvers [60].

One of the mainstream approaches to mitigating such threat is to *encrypt DNS communications*. To this end, various techniques are proposed, including DNS-over-TLS (DoT), DNS-over-HTTPS (DoH), DNS-over-QUIC and DNSCrypt. In this paper, we jointly term them as DNS-over-Encryption (DoE). Although most of the protocols have only been established for a few years, some have been gaining strong support from large DNS service providers [2, 4, 14], OS [24, 56] and software [6, 38, 63].

However, despite the "top-down" effort made by the industry, little has been done to understand the operational status of DNS-over-Encryption from the *"bottom-up" view*, or from the view of Internet users. In this paper, we aim to give a comprehensive and end-to-end review of DNS-over-Encryption, which we believe will provide good guidance in pushing the adoption and improving the ecosystem of DNS-over-Encryption in the future. The research questions we seek to answer include: 1) How many providers are offering DNS-over-Encryption services? Are their implementations secure? 2) What does their performance look like for users distributed globally? Is there any issue preventing access or causing

errors? 3) What does the real-world usage of DNS-over-Encryption look like?

Our Study. So far, DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH) are two *standardized and extensively supported protocols* to secure the traditional DNS, and our study focuses on measuring the two protocols. First, we perform a comparative study on the DNS-over-Encryption protocols to outline their strengths and weaknesses (Section 2). Second, we launch Internet-wide scanning to discover DNS-over-Encryption service providers and analyze their security issues (Section 3). Third, we assess the accessibility and performance of DNS-over-Encryption services by recruiting geographically distributed vantage points (Section 4). Getting access to real-world DNS-over-Encryption traffic from massive vantage points without violating participants' privacy is challenging. We address this challenge by running controlled experiments on a carefully designed Internet measurement platform. Finally, we compare the traffic volume between traditional DNS requests and DNS-over-Encryption requests using several large-scale datasets, including passive DNS datasets and 18-month NetFlow data from a large ISP (Section 5).

Findings. So far, we have obtained some unique discoveries about the deployment of DNS-over-Encryption. On one hand, the service quality of DNS-over-Encryption providers is satisfying in general, suggesting the industry is prepared for large-scale real-world usage. On the other hand, we also spot misconfigurations on some services, and more efforts should be made to push its correct adoption. Below, we highlight the key findings.

- We discover over 150 DoT and 17 DoH providers that offer DNS-over-Encryption services to client users with over 1.5K addresses. Interestingly, a lot of them do not show up in public resolver lists. However, 25% DoT providers, including large ones (Perfect Privacy), use invalid SSL certificates which could break the server authentication process. Particularly, TLS inspection devices are found to act as DoT proxies. In addition, we find that Quad9 DoH has a misconfiguration which causes DNS lookup errors. We have reported the issue to the provider.
- Compared to traditional DNS, the reachability to DNS-over-Encryption servers turns to be better, with only less than 1% global clients experiencing service disruption. But still, there are DNS-over-Encryption services disrupted by censorship (e.g., Google DoH blocked in China) and TLS interception, which diminishes the benefits brought by encrypting DNS queries.
- The extra overhead incurred by DNS-over-Encryption is tolerable to global users. On average, compared to traditional DNS, transmitting encrypted DNS queries brings several milliseconds of extra query latency.
- The traffic volume and active users of encrypted DNS are still at a small scale compared to traditional DNS. However, the usage of DNS-over-Encryption services has been growing in recent months. For example, Cloudflare DoT witnesses a 56% traffic increase from Jul 2018 to Dec 2018.

The "Early" View of Ecosystem. This paper presents the first systematic and large-scale study on the ecosystem of DNS-over-Encryption since its proposal. One may think the ecosystem is small, because major users still choose clear-text DNS, and the measurement study is yet too early. We agree the study is an early view in terms of user base, but on the other hand, the first DNS-over-Encryption protocol has been established for around 10 years, and many resolvers including Google and Cloudflare have started to run DNS-over-Encryption services. We believe it is necessary to understand the gap between the deployment and user adoption, and identify success and pitfalls of different protocols. Such effort can help the community to adjust the roadmap for the better future of DNS-over-Encryption. To this end, we also publish our collected data and results to help further studies, and will continue to monitor the ecosystem.

Contributions. The contributions of this paper are outlined as follows.

- *Comparative study.* Using 10 criteria under 5 categories, we present the first comparative study on five DNS-over-Encryption protocols, which sheds light on the development of the ecosystem.
- *Methodology.* Combining a suite of techniques, we design and deploy a large-scale measurement platform with 122,991 vantage points in 166 countries, to understand the client-side usability of DNS-over-Encryption services. Meanwhile, we launch Internet-wide scanning to discover new service providers.
- *Observations.* Leveraging several large-scale datasets, we investigate the current deployment and usage of DNS-over-Encryption. With multi-faceted insights, we provide concrete recommendations to the DNS community.
- *Dataset release.* We are continuously collecting data and measuring the development of DNS-over-Encryption. We release our datasets for public use at `https://dnsencryption.info`.

2 BACKGROUND

In this section, we first describe the privacy considerations regarding DNS. We then elaborate and perform a comparative study on current protocols to encrypt DNS communications.

2.1 DNS Privacy Considerations

DNS precedes almost all Internet activities: email senders look up recipients' server addresses; patients query hospital domain names; devices use DNS to discover each other. By design, DNS packets are sent in clear-text, which makes it vulnerable to both passive (e.g., on-path eavesdroppers) and active attackers (e.g., rogue DNS servers).

The unencrypted design of DNS exposes Internet users to privacy threats. It has been known that DNS traffic can be used to fingerprint client machines and analyze user behavior [32, 48, 54, 55]. Previous works have also shown that client machines can be tracked across the Internet, by simply analyzing passive DNS data [52]. What's worse, documents reveal that massive DNS surveillance does exist on the Internet, such as NSA's QuantumDNS and MoreCowBell projects [12, 44]. In short, unprotected DNS traffic can introduce significant privacy risks to Internet users.

2.2 DNS-over-Encryption Protocols

Driven by the concerns, the community has been devoting significant efforts to mitigating DNS privacy issues. Shown in Figure 1, the earliest proposal to protect DNS communications dates back to 2009. Since 2014, IETF have established two Working Groups, and various protocols have been proposed to secure traditional

Figure 1: Timeline of important DNS privacy events, including DNS-over-Encryption standards (blue), IETF WGs (orange), Informational RFC and Best Common Practice (purple).

DNS. Meanwhile, the techniques have gained support from large industrial providers including Mozilla [62] and Google [4]. In fact, it would be unsurprising that clear-text DNS will be replaced by the secured format in the near future, similar to HTTPS being mandated when visiting high-pro le websites (e.g., banking site).

Adding con dentiality and authentication properties to the DNS protocol is an e ective approach to addressing DNS privacy threats. In this work, we focus on techniques that are dedicated to securing the stub-to-recursive link of DNS resolutions, as it's the primary focus of the community and most proposals [45, 49, 50]. Below we give an overview and perform a comparative study on di erent DNS-over-Encryption protocols.

Evaluation Criteria. We consider 10 criteria under 5 categories to evaluate di erent DNS-over-Encryption protocols.

- Protocol Design: 1) whether the new protocol is based on traditional DNS or switches to a di erent application-layer protocol; 2) whether it provides a fallback option when certain cryptographic operations cannot be applied (i.e., back to non-authenticated or clear-text connections).
- Security: 1) whether the protocol is based on standard cryptographic protocols (e.g., TLS); 2) whether it can defend against on-path passive DNS tra c analysis (or at least o ers options against it).
- Usability: 1) changes that client users need to make before using the protocol: no extra software needed (low), extra software installation or con guration needed (medium), or no supporting software yet (high); 2) whether the protocol incurs query overhead over traditional DNS-over-UDP (e.g., by using TCP or requiring TLS handshake) or provides options to amortize it.
- Deployability: 1) whether the protocol is designed over standardized and well-supported protocols; 2) whether it is supported by mainstream DNS software (e.g., BIND [34], Knot Resolver [6] and Unbound [21], see Appendix A).
- Maturity. 1) whether the protocol is currently standardized by IETF; 2) whether it is extensively supported by DNS service providers (e.g., large public DNS resolvers, see Appendix A).

Currently, 5 major DNS-over-Encryption protocols are proposed to secure the stub-to-recursive link, including DNS-over-TLS (DoT), DNS-over-HTTPS (DoH), DNS-over-DTLS, DNS-over-QUIC and DNSCrypt. Using the criteria above, we present their evaluation in Table 1. Each protocol is categorized under satisfying (denoted as), partially satisfying (denoted as G), or not satisfying one criterion (denoted as #). Below we elaborate each protocol in detail.

DNS-over-TLS (DoT). DoT is standardized by RFC7858 [49] in 2016, and its concept is straightforward: clients and servers negotiate a Transport Layer Security (TLS) session before DNS lookups, and use it to wrap wire-format DNS queries transported through TCP. As a result, clients and recursive resolvers can exchange encrypted DNS messages (preventing passive monitoring), and resolvers can be authenticated by verifying SSL certi cates (preventing man-in-the-middle attackers). By default, DoT uses port 853 for communication. The use of a dedicated port could make DoT requests distinguishable from other tra c, but padding options (e.g., EDNS(0) padding [61]) can be leveraged to reduce adversaries' capability of tra c analysis.

To provide di erent levels of security and privacy protections, DoT is designed with two usage pro les (i.e., Strict Privacy pro le and Opportunistic Privacy pro le) for DNS clients [49], and provides fallback mechanisms. Under the Strict Privacy pro le, a DNS client is required to both authenticate the DoT server and encrypt transactions. If either requirement is not available, the DoT query will fail. By contrast, clients using an Opportunistic Privacy pro le only attempt for best protection, and may fallback to a non-authenticated connection or even clear-text connection.

Regarding implementation, as shown in Appendix A, DoT has been extensively supported by OS (e.g., Android 9 [56]), DNS software (e.g., Unbound [21] and Stubby [38]), and large public DNS resolvers (e.g., Cloud are [2], Google [4] and Quad9 [14]). For service providers, current implementations reduce the cost to operate a DoT resolver, and SSL certi cates are easy to install with automated CAs like Let's Encrypt [8]. However, before a client uses DoT, extra changes have to be made, including switching to new stub resolvers (e.g., by updating the OS or installing stub resolvers like Stubby) and manual con guration of DoT resolvers. With encryption and connection setup, DoT introduces extra query time overhead compared to DNS-over-UDP. However, it can be amortized by connection reuse [49] and we measure the overhead in Section 4.3.

DNS-over-DTLS. A variation of DoT is DNS-over-DTLS, which works over UDP for better performance. While DNS-over-DTLS and DoT share most properties, it is designed only as a backup proposal for DoT, and the RFC document expects DoT to be widely deployed [70]. To our best knowledge, DNS-over-DTLS has no real-world implementations yet, including stub and recursive resolvers,

Table 1: Comparison of di erent DNS-over-Encryption protocols

Category	Criterion	DNS-over-TLS	DNS-over-HTTPS	DNS-over-DTLS	DNS-over-QUIC	DNSCrypt
Protocol Design	Uses other application-layer protocols	#		#	#	
	Provides fallback mechanism		#			#
Security	Uses standard TLS					#
	Resists DNS tra c analysis	G		G	G	
Usability	Minor changes for client users	G		#	#	G
	Minor latency above DNS-over-UDP	G	G			G
Deployability	Runs over standard protocols				#	#
	Supported by mainstream DNS softwar		G	#	#	G
Maturity	Standardized by IETF				#	#
	Extensively supported by resolvers			#	#	G

Figure 2: Two types of DoH requests. They both contain a wire-format DNS A-type query of example.com

thus its usability for clients and deployability for DNS operators are ranked as low.

DNS-over-HTTPS (DoH). Described by RFC8484 [40], the core of DoH is to embed DNS queries into HTTPS messages, which are protected by TLS. Particularly, DoH uses URI templates (e.g., https://dns.example.com/dns-query{?dns}) to locate a service, and the hostname in the template should be resolved to bootstrap DoH lookups (e.g., via clear-text DNS). As shown in Figure 2, wire-format DNS packets are encoded in URI parameters (using GET) or HTTP message body (using POST). As such, two application-layer protocols (HTTP and DNS) are leveraged for DoH.

DoH shares port 443 with HTTPS visits to websites, which mixes DoH queries with other HTTPS tra c, and therefore e ectively resists tra c analysis that only targets DNS. By design, DoH requires both encryption and authentication of DNS servers (i.e., Strict-Privacy-pro le-only). Without fallback options, DoH lookups will fail if either operation is not available. Similar to DoT, query time overhead can be caused by connection establishment and encryption.

DoH runs on top of HTTPS, therefore is particularly suitable for user-space applications like web browsers. Typically, the applications already contain stub resolvers, so the changes for DNS clients to use DoH are minor (compared to updating OS or installing other software). As an example, Firefox supports DoH since Version 62 [63], and o ers a UI for DoH con guration. For DNS operators, however, as the combination of HTTP and DNS is less supported by mainstream DNS software (see Appendix A), they need to deploy other implementations in order to o er service. Currently, DoH is supported by large resolvers include Cloud are [2], Google [4] and Quad9 [14].

DNS-over-QUIC. On top of QUIC, DNS-over-QUIC o ers similar privacy properties as DoT, but has similar performance as DNS-over-UDP. According to its current draft, it is designed for minimum latency and solving issues like TCP's head-of-line blocking [50]. For better usability, it also provides a fallback mechanism, using DoT or plain-text DNS when the QUIC connection fails. DNS-over-QUIC is planning to use a dedicated port 784. Still, there are not yet real-world implementations for DNS clients or operators.

DNSCrypt. Proposed in 2011, DNSCrypt is not based on standard TLS, and uses the X25519-XSalsa20Poly1305 cryptographic construction [11]. DNSCrypt messages are transferred over port 443, which are also mixed with HTTPS tra c, and can be used over both UDP and TCP.

As one of the earliest protocols in the list, DNSCrypt has been supported by several large public resolvers for years, including OpenDNS (since 2011) [7], Yandex (since 2016) [25], and OpenNIC [9]. To use DNSCrypt, clients need to install extra software (e.g., DNSCrypt-proxy [3]), and servers need certi cates signed on dedicated hardware [11]. Since proposal, DNSCrypt has never been standardized by the IETF.

DNS-over-Encryption and DNSSEC. DNSSEC aims to protect the integrity of DNS records by signing them, but does not protect DNS privacy. DNS-over-Encryption and DNSSEC are dedicated to solving di erent problems, and they can be fully compatible and used together [49].

The above survey provides the rst comparative study of DNS-over-Encryption protocols as far as we know. We do acknowledge that there could be disagreement on the metrics we use and the grades we give to each protocol. However, we believe our survey shows new insights into the development of the DNS-over-Encryption ecosystem, and will enlighten the path for future development of this technology.

Scope of study. DNS-over-TLS (DoT) and DNS-over-HTTPS (DoH) are two leading and mature protocols to secure traditional DNS communications. On top of well-supported and standard protocols (i.e., TLS and HTTP), they are both standardized by IETF, and extensively implemented by various DNS software and public resolvers (see Table 8 of Appendix A). For the remaining of this paper, we focus on DoT and DoH and measure them from the view of Internet users.

3 SERVERS: TO OFFER DNS-OVER-ENCRYPTION

Servers, especially resolvers, play a vital role in the deployment of DNS-over-Encryption protocols. In this section, we describe our scanning methodology that can identify open DNS-over-Encryption resolvers operated in the wild, and their security analysis. Then, we report our ndings.

3.1 Methodology

Though, public resolver lists such as [39, 73] have already complied tens of providers o ering DNS-over-Encryption services, it is unclear to us whether they achieve good coverage of all such services, especially the ones less known but still in operation. As such, our rst step is to identify DoT and DoH servers through systematic service discovery.

Discovering open DoT resolvers. As DoT uses a dedicated port 853 for communication, it is required that by default, DNS servers that support DoT MUST listen for and accept TCP connections on this port [49]. Therefore, discovering open DoT resolvers is conceptually simple through Internet-wide scanning using port 853 as input. While a DoT resolver could choose other ports, such setting requires extra con guration changes on DoT clients, which is cumbersome for normal users. As such, those services are not considered in this study.

In practice, we rst use ZMap [42] to discover all IPv4 addresses with port 853 open (using the zmap -p 853 command), and then probe the addresses with DoT queries of a domain registered by us, using getdns API [17]. In the rst stage, our scan originates from 3 IP addresses in China and the US (on cloud platforms), and we con gure the tool to cover the entire IPv4 address space in a random order. For addresses with port 853 open, only those successfully responding to our DoT queries are regarded as open DoT resolvers. We repeat our scan process every 10 days from Feb 1, 2019 to May 1, 2019, and each scan takes 24 hours to nish.

For ethical considerations, we o er an opt-out option from our scanning activities, by setting a reverse DNS record for our scanning system and building a website that tells the scanning details and collects opt-out requests. During our scan period, we did not receive any opt-out requests.

Discovering open DoH resolvers. Compared to DoT resolvers, it is much more di cult to discover DoH servers, because they share port 443 with other HTTPS visits, and use URI templates to be located. While we have tried to look for DoH resolvers in public DNS zone les, the discovery turns out to be unsatisfying, as many resolvers are hosted on the subdomains of second-level domains (SLDs) of the providers (e.g., dns.example.com in Figure 2), while public zone les only contain SLDs. As an alternative approach, we attempt to discover DoH resolvers by inspecting a large-scale URL dataset provided by our industrial partner. The dataset consists of URLs from their web crawlers, malware sandbox and VirusTotal data feed. Over time, the dataset has recorded billions of URLs.

To discover DoH resolvers, we need to know their URI patterns. Fortunately, the DoH RFC and large resolvers have speci ed several common path templates (e.g., /dns-query and /resolve , see Figure 2) that can point to DoH resolvers, and most DoH resolvers in public lists [73] adopt the templates, including Cloud are [2] and Quad9 [14]. Therefore, we scan the whole URL dataset using the known templates. For ethics, the dataset does not contain user information or URL parameters, so the privacy risk should be minimized.

Limitations. Firstly, our Internet-wide scan only covers open resolvers, and misses those deployed by ISPs (i.e., local resolvers which are not open to public). To evaluate DoT deployment on local resolvers, we launch DoT queries of our own domain to local resolvers using RIPE Atlas [28]. In the end, only 24 of 6,655 probes (0.3%) succeed in the query, suggesting the current ISP DoT deployment is still scarce[1]. Therefore, we believe the impact of lacking local resolvers is small on the overall result. Secondly, while we do discover DoH resolvers (particularly, resolvers beyond known lists) using our methodology, resolvers with unknown URL patterns will be overlooked. Also, despite our URL dataset being large, it could be possible to nd more resolvers using other data traces. We do acknowledge that our method has limitations, but given the challenges discussed above, we regard our method as a best-e ort attempt.

Table 2: Top countries of open DoT resolvers

CC	# DoT Resolver		Growth	CC	# DoT Resolver		Growth
	Feb 1	May 1	%		Feb 1	May 1	%
IE	456	951	+108%	JP	34	27	-20%
CN	257	40	-84%	NL	30	36	+20%
US	100	531	+431%	GB	25	21	-16%
DE	71	86	+21%	BR	22	49	+122%
FR	59	56	-5%	RU	17	40	+135%

3.2 Open DNS-over-Encryption Resolvers

> Key observation 1: Except for large providers, there are many small providers which are less-known and missed by the public resolver lists. However, a quarter of DoT providers use invalid SSL certi cates on their resolvers, which exposes their users to security risks.

Finding 1.1: 1.5K open DoT resolvers are mostly owned by large providers, but there are also ones run by small providers which are absent from public resolver lists. By contrast, the number of open DoH resolvers is small. From each Internet-wide scan, we discover 2 to 3 million hosts with port 853 open (e.g., 356M on Feb 1 and 230M on May 1), yet a vast majority of them do not provide DoT (i.e., they cause getdns errors). As shown in Figure 3, over 1.5K open DoT resolvers are discovered in each scan, signi cantly more than the public resolver lists. Geographically, Table 2 shows the top 10 countries with most resolvers, and their uctuation during our scan period. DoT resolvers in Ireland, Brazil and Russia have doubled in three months, and those in the US increased by four times. By contrast, we also nd a signi cant drop of DoT resolvers (-84%) in China, and the shut resolvers mostly belong to a cloud hosting platform.

[1] Our ratio is lower than a previous report [47], because we exclude probes using well-known public resolvers (e.g., 8.8.8.8) as their local resolver. Example DoT-capable local resolvers we nd include 194.109.6.66 (AS3265, Xs4all Internet BV), 212.242.40.51 (AS9158, Telenor A/S) and 78.158.0.2 (AS43700, UAB Consilium Optimum)