Produce a technical plan for ”Irish” Trusted Recursive Resolvers

Tung-te Lin M.Sc.

A Dissertation

Presented to the University of Dublin, Trinity College

in partial fulfilment of the requirements for the degree of

Master of Science in Computer Science (Future Networked System)

Supervisor: Stephen Farrell

11 2020

Declaration

I, the undersigned, declare that this work has not previously been submitted as an exercise for a degree at this, or any other University, and that unless otherwise stated, is my own work.

Tung-te Lin

November 10, 2020

Permission to Lend and/or Copy

I, the undersigned, agree that Trinity College Library may lend or copy this thesis upon request.

Tung-te Lin

November 10, 2020

Acknowledgments

I am here to sincerely thank Dr Stephen Farrell. He is my supervisor who directed me and taught me the expertise.

Secondly, I am extremely grateful for my mother Lin Miao-Juan because she provided me with the funding to study at Trinity College Dublin.

Next, Martin John McAndrew, the person who helped me to win the appeal. And Cian Johnston, he is not only my Irish classmate but also the proofreader of this dissertation. I appreciate both your efforts for me.

I can not finish this dissertation without any of you.

Tung-te Lin

University of Dublin, Trinity College
11 2020

Produce a technical plan for "Irish" Trusted Recursive Resolvers

Tung-te Lin, Master of Science in Computer Science

University of Dublin, Trinity College, 2020

Supervisor: Stephen Farrell

The company Mozilla has started the problem Trusted Recursive Resolver(TRR) to protect the privacy of users. The TRR program requires the Domain Name System(DNS) server with DNS over HTTPS(DoH) service.

This study designed methods to analyze the possible DNS traffic in Ireland by using the data from some authoritative DNS servers. Then, installed a private DNS server with the DoH service to test the performance of DoH.

Finally, the study made a technical plan for building DNS servers in Ireland for TRR. The plan is including the required number and management of the DNS servers with the DoH service, and other conditions that the DNS provider needs to consider.

Summary

In summary, Trusted Recursive Resolver(TRR) program may provide a safer environment to protect the privacy of users base on using DNS over HTTPS(DoH) service to encrypt DNS queries. Moreover, TRR program also requires that DNS providers must allow civilians to supervise servers to avoid abusing data.

On the other hand, Ireland is not a big country and the population is not high. Thus the latency could be controlled in an acceptable range and the number of DNS queries is not tremendous if compare to other countries. Therefore it only needs 2 DoH DNS servers for the TRR program in Ireland, the locations could be Dublin and Cork respectively. Thus, it is worth constructing DoH DNS servers for the TRR program for Ireland.

In conclusion, The DNS provider could build 2 DNS servers with DoH service easily, but both DNS servers are compulsory to be supervised by the public if the DNS provider intends to join the TRR program.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

The browser company Mozilla plans to promote the program Trusted Recursive Resolver(TRR) to provide better privacy compare to using traditional Domain Name Servers(DNS) [8]. This paper is going to analyze how a TRR plan could be applied in the Republic of Ireland from a technical view.

Chapter 2 “the state of the art” describes how a DNS server works, and the problem of privacy would have in using DNS servers. Next, it describes the solutions for dealing with the problem of privacy so far, including Domain Name System Security Extensions(DNSSEC) [9], DNSCrypt [10], DNS over TLS(DoT) [11], and DNS over HTTPS(DoH) [12]. Moreover, TRR is introduced here. The chapter explains why Mozilla created TRR, what is the relation between TRR and DoH, and why this study intends to discuss about the TRR program.

Chapter 3 discusses the DNS traffic in Ireland. If people plan to deploy DNS servers to implement TRR in Ireland, they need to know how much DNS traffic would exist in Ireland. Thus, this chapter provides the method to estimate the DNS traffic in Ireland.

Chapter 4 discusses the required software. It discuss that if install a DoH DNS server, What kinds of software does a DNS provider needs? What applications exist in the market for each kind so far? Furthermore, this chapter makes a comparison among those applications, and provide some information from previous studies.

Chapter 5 designed an experiment to understand the performance of a DNS server can possess. The software used here are the applications mentioned in Chapter 4. This chapter describes the processes in the experiment, and explains the variables and results of the tests in the experiment.

Chapter 6 is "Other Concerns". Besides Irish DNS traffic, required software and performance, other considerations are analyzed in this chapter. Those considerations include DDOS attacks, Irish policy(censorship) and latency of DNS queries.

Chapter 7 "Overall Design" is the last chapter. The discussions from chapter 2 to chapter 6 are concluded here. This chapter also lists some conditions for resolving the possible issues that may occur if the TRR program is implemented in Ireland. Apart from that, some recommendations are also suggested here.

Chapter 2

The state of the art

2.1 The introduction of Domain Name Server

Domain Name System(DNS) [8] is the server which converts the domain name to Internet Protocol(IP) address. Machines need the IP address to find out the location of another machine [13] [14], not domain name [15]. When users type the domain name on the browser, for example, type 'www.dcard.tw" on a browser, then the browser will send the domain name "www.dcard.tw" to a DNS server. After that, the DNS server responses the IP address of the domain name "104.16.204.58" to the browser. Finally, the browser is enable to connect to the server of "www.dcard.tw" by using the its IP "104.16.204.58".

Moreover, there are 2 kinds of DNS servers: The recursive resolvers and the authoritative DNS server [16]. Recursive resolvers do not save all the IP addresses and domain names that users need. If users query the domain names that the recursive resolver does not know, then the recursive DNS resolver will inquire authoritative DNS servers about the IP address for the domain name. Next, the recursive resolver saves the domain name and its IP address in the cache, in case any users use this domain name in a short time, then the recursive resolver is able to reply its IP address immediately and not to inquire authoritative DNS servers again.

Authoritative DNS servers store IP addresses and domain names that users need, then users are able to utilize recursive resolvers to inquire authoritative DNS servers to get correspond IP addresses.

Furthermore, authoritative DNS servers are hierarchical [5]. The highest one is called a root server. A top-level authoritative DNS server can respond with an address of a low-level authoritative DNS server to users for their inquiry, and that lower level authoritative DNS server may have the IP address that users need. In that case, a authoritative DNS server does not need to save entire IP addresses and domain names, the workload can be divided. The levels of authoritative DNS servers are shown in Fig. 2.1.

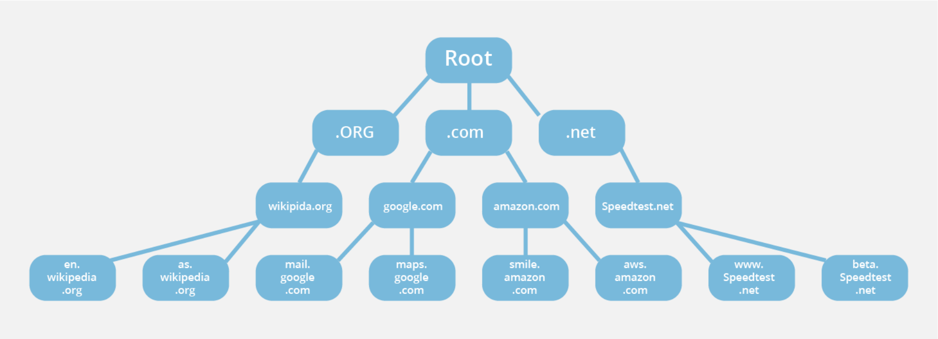


Figure 2.1: *The levels of authoritative DNS servers [5]*

2.2 The problem of privacy

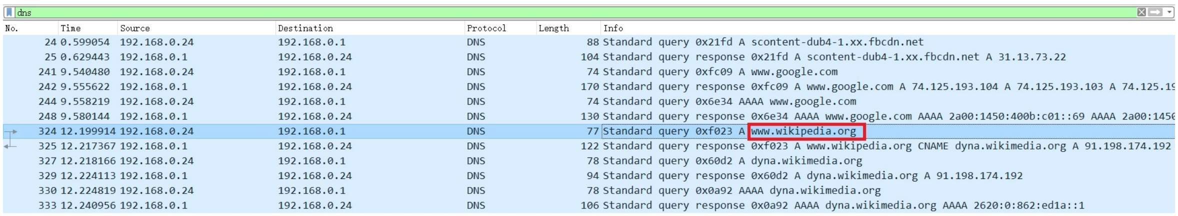
Request For Comments(RFC) [17] is the publication which is managed by Internet Engineering Task Force(IETF). IETF is the organization to design the standard of Internet [18].

RFC7626 [19] and its draft [20] discussed the problem of privacy in using a DNS server. The personal data could be discovered in the DNS servers, wire or DNS requests, including the IP of clients, the domain names which are researched by users, and even the applications that users use.

The root cause of this privacy problem is that the typical DNS traffic is not encrypted. On the other hand, DNS servers, especially recursive resolvers, they store the data of DNS queries in their log or cache. Thus the DNS providers are able to use the data to do some analysis or transfer the data to others. As for authoritative DNS servers, the privacy problem is lighter than recursive resolvers, because their cache is too limited to store the completed data [19].

If others get the packets from the typical DNS traffic, then they may understand what websites users browse or what applications users use.

In order to understand the situation clearly, this study did a test to get some traditional DNS packets from a user by using Wireshark. Wireshark is the software for catching packets. When the researcher typed a domain name of a website on a web browser, then that domain name was displayed on Wireshark. The screenshot is shown in Fig. 2.2.



```
dns
No.   Time      Source        Destination   Protocol  Length  Info
   24 0.599054  192.168.0.24  192.168.0.1   DNS           88 Standard query 0x21fd A scontent-dub4-1.xx.fbcdn.net
   25 0.629443  192.168.0.1   192.168.0.24  DNS          104 Standard query response 0x21fd A scontent-dub4-1.xx.fbcdn.net A 31.13.73.22
  241 9.540480  192.168.0.24  192.168.0.1   DNS           74 Standard query 0xfc09 A www.google.com
  242 9.555622  192.168.0.1   192.168.0.24  DNS          170 Standard query response 0xfc09 A www.google.com A 74.125.193.104 A 74.125.193.103 A 74.125.19
  244 9.558219  192.168.0.24  192.168.0.1   DNS           74 Standard query 0x6e34 AAAA www.google.com
  248 9.580144  192.168.0.1   192.168.0.24  DNS          130 Standard query response 0x6e34 AAAA www.google.com AAAA 2a00:1450:400b:c01::69 AAAA 2a00:1450
  324 12.199914 192.168.0.24  192.168.0.1   DNS           77 Standard query 0xf023 A www.wikipedia.org
  325 12.217367 192.168.0.1   192.168.0.24  DNS          122 Standard query response 0xf023 A www.wikipedia.org CNAME dyna.wikimedia.org A 91.198.174.192
  327 12.218166 192.168.0.24  192.168.0.1   DNS           78 Standard query 0x60d2 A dyna.wikimedia.org
  329 12.224113 192.168.0.1   192.168.0.24  DNS           94 Standard query response 0x60d2 A dyna.wikimedia.org A 91.198.174.192
  330 12.224819 192.168.0.24  192.168.0.1   DNS           78 Standard query 0x0a92 AAAA dyna.wikimedia.org
  333 12.240956 192.168.0.1   192.168.0.24  DNS          106 Standard query response 0x0a92 AAAA dyna.wikimedia.org AAAA 2620:0:862:ed1a::1
```

Figure 2.2: *The queried website is revealed in packets if using the typical method to query website*

2.3 The solutions for privacy

According to the description of RFC7626 [19], revealing the content of DNS queries can cause severe privacy problems. People may not be willing to let others to find what websites they browse. Thus, some solutions were created. There are 4 popular solutions to improve the privacy of DNS and they are widely used in different public DNS servers, which are Domain Name System Security Extensions(DNSSEC), DNS over TLS(DoT), DNS over HTTPS(DoH) and DNSCrypt [21].

The first solution is DNSSEC, it is not only the oldest but also the most popular solution among those 4 solutions [21]. It was created in 1997. The concept is making an extension of DNS to check the digital signature [9], thus it provides the basic protection for the privacy.

However, it has some disadvantages. For example, it uses digital signatures therefore the system needs higher performance to process digital signatures. Secondly, the complexity will be highly increased if DNS servers use DNSSEC, then high complexity can cause high possibility to make mistakes. Moreover, the typical DNSSEC does not encrypt the DNS query [22].

The second soluction is DNSCrypt. Unlike other 3 solutions, it does not follow any RFC, because it was a private standard. The creator is OpenDNS and it was announced in 2011. DNSCrypt does not use digital signatures, it uses cryptographic construction to encrypt queries [10].

The biggest problem is that it does not follow RFC, which means it is not proposed by IETF. Therefore it is just a private standard, not a public standard, then it is hard to be widely used by DNS providers and application developers. For example, the famous public DNS providers Cloudflare and Google do not support DNSCrypt [21].

The third solution is DoT, it was invented in 2016. The concept is using Transport Layer Security(TLS). TLS is an existing and popular security protocol [11]. Compare to DNSSEC and DNSCrypt, it has a lot of advantages. For example, it does not need a high performance to process encryption. The packet is encrypted, thus it can prevent a man-in-the-middle attack(MITM) [23]. Moreover, DoT follows RFC, therefore it uses a public standard which is proposed by IETF, hence it can be widely used by many DNS providers and developers.

The newest one among those 4 solutions is DoH. It was introduced in 2018, but it is in testing [12]. DoH is similiar to DoT, both DoH and DoT are utilizing TLS to be the tool to encrypt DNS queries. The different is that DoT uses TLS directly, in contrast, there is a protocol between DoH and TLS in the DoH model, which is HTTPS. HTTPS also uses TLS, thus DoH uses TLS indirectly and uses HTTPS directly [1]. The models of DoT and DoH are shown in Table 2.1 and Table 2.2.

As for the traditional DNS, it does not encrypt DNS queries and use port 53. It has an alias named Do53 [24].

DNS (The highest layer)
TLS
TCP
IP (The lowest layer)

Table 2.1: The model of DoT [1]

DNS (The highest layer)
HTTPS (The layer which is different from DoT)
TLS
TCP
IP (The lowest layer)

Table 2.2: The model of DoH [1]

Compare with DoT, DoH uses HTTPS, therefore it is easier to be used than DoT in a browser or other application. DoH server has a domain name of HTTPS, users just input the domain name in their browser then they can start to use DoH.

Even though DoH is still in testing, many public recursive name servers already use it, such as Cloudflare, Google, AdGuard, CleanBrowsing,OpenDNS and Quad9. Meanwhile, Google Chrome, Microsoft Edge, Mozilla Firefox and Opera, those 4 well-known browsers also already support DoH.

DoH has resolve many problems that previous solutions. It does not require high performance as DNSSEC requires, it follows RFC 8484, thus it is a public standard, unlike DNSCrypt is a private standard. However, the situation of DoH is still in testing, some issues map happen. Thus, this paper is going to use DoH server to collect some data to evaluate the functionality, performance and try to find out the problem may arise if using a DoH server.

The comparison of different solutions for encrypting DNS queries is shown in Table 2.3.

Solutions	DNSSEC	DNSCrypt	DoT	DoH
Introduced	1997	2011	2016	2018
RFC	4033,4034,4035	None	7858,8310	8484
Principle	Digital signature	Cryptography	TLS	HTTPS
Disadvantage	Too complex	Private protocol	Not popular	still in testing
Advantage	Popular	Encrypted packets	Encrypted packets	Encrypted packets and easy to use

Table 2.3: The solutions for encrypting DNS queries

2.4 The development of Trusted Recursive Resolver

As RFC7626 mentioned [19], the personal data could be revealed in the DNS traffic or DNS servers. About the DNS traffic, it can be encrypted by above 4 solutions in the last section. As for the DNS servers, it need another means to resolve the problem of privacy.

In this background, the concept of Trusted Recursive Resolver(TRR) [25] was designed by Mozilla for protecting privacy. On the one hand, TRR requires recursive resolvers use DoH to encrypt the content of DNS queries, on the other hand, recursive resolvers have to be supervised. Thus, the personal data both in DNS traffic and DNS servers can be protected from eavesdroppers or taken by others.

Cloudflare, NextDNS and Comcast are the 3 DNS providers who have joined the TRR program so far [26]. There are 3 regulations in the supervision to recursive resolvers in the TRR program [27].

The first one, the data should be limited. It may remain in the server only for 24 hours. Moreover, the data can not be sold or shared.

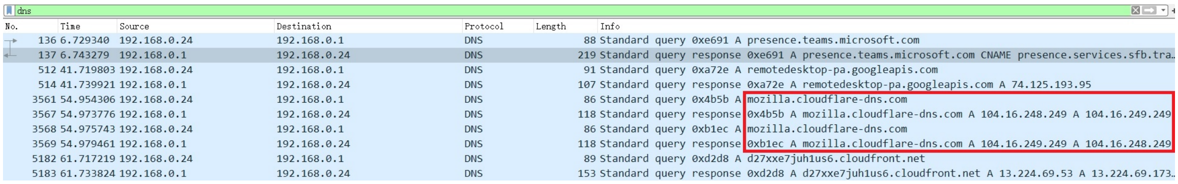
The second one, the data in recursive resolvers need to be transparent. People have the right to understand how the data are stored and used.

The third one, the data in recursive resolvers can not be blocked, filtered, modified, the exception is “required by law”.

In case a recursive resolver is able to satisfy those 3 conditions, then it will be “trusted” by Mozilla, then users may trust Mozilla. Hence, this recursive resolver is so-called “Trusted Recursive Resolver”.

Thus, not every recursive resolver is eligible to join the TRR program. The Mozilla Corporation selects it and provides a list of trusted recursive resolvers to users. So far, the Internet service provider Comcast and DNS providers Cloudflare and NextDNS have joined the TRR program.

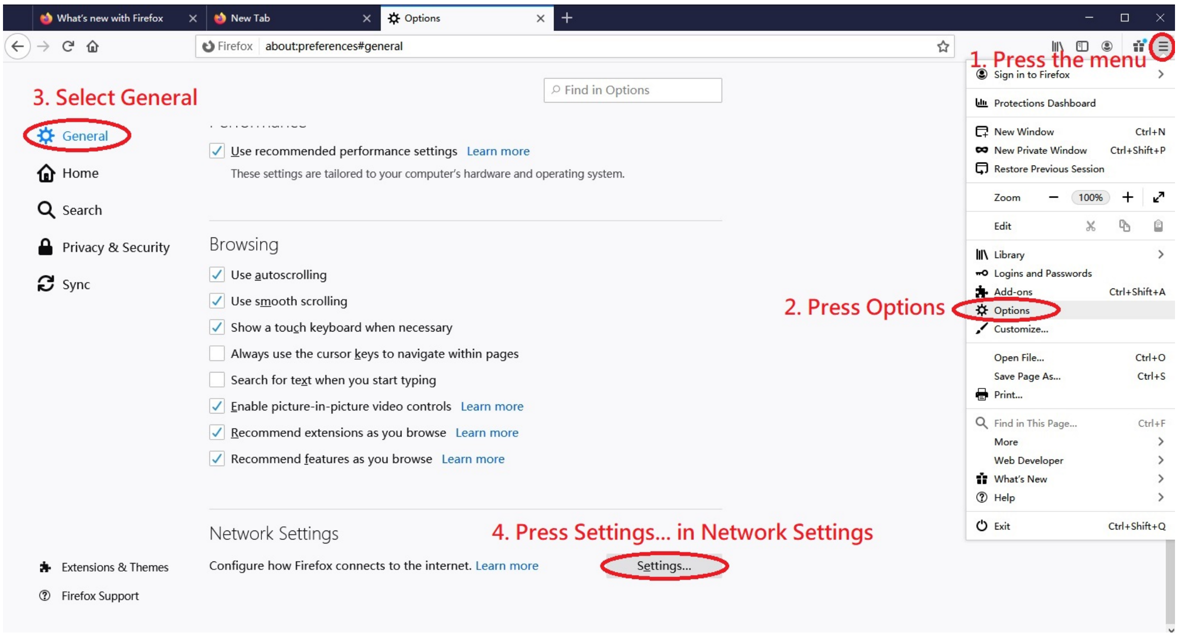
The TRR program has been implemented in Mozilla’s browser Firefox. If people enable the TRR function in Firefox instead of using the traditional DNS query, then we can not find any information about browsed websites in packets. The screenshot is shown in Fig. 2.3.



```
dns
No.   Time      Source        Destination   Protocol Length Info
  136 6.729340  192.168.0.24  192.168.0.1   DNS          88 Standard query 0xe691 A presence.teams.microsoft.com
  137 6.743279  192.168.0.1   192.168.0.24  DNS         219 Standard query response 0xe691 A presence.teams.microsoft.com CNAME presence.services.sfb.tra…
  512 41.719803 192.168.0.24  192.168.0.1   DNS          91 Standard query 0xa72e A remotedesktop-pa.googleapis.com
  514 41.739921 192.168.0.1   192.168.0.24  DNS         107 Standard query response 0xa72e A remotedesktop-pa.googleapis.com A 74.125.193.95
 3561 54.954306 192.168.0.24  192.168.0.1   DNS          86 Standard query 0x4b5b A mozilla.cloudflare-dns.com
 3567 54.973776 192.168.0.1   192.168.0.24  DNS         118 Standard query response 0x4b5b A mozilla.cloudflare-dns.com A 104.16.248.249 A 104.16.249.249
 3568 54.975743 192.168.0.24  192.168.0.1   DNS          86 Standard query 0xb1ec A mozilla.cloudflare-dns.com
 3569 54.979461 192.168.0.1   192.168.0.24  DNS         118 Standard query response 0xb1ec A mozilla.cloudflare-dns.com A 104.16.249.249 A 104.16.248.249
 5182 61.717219 192.168.0.24  192.168.0.1   DNS          89 Standard query 0xd2d8 A d27xxe7juh1us6.cloudfront.net
 5183 61.733824 192.168.0.1   192.168.0.24  DNS         153 Standard query response 0xd2d8 A d27xxe7juh1us6.cloudfront.net A 13.224.69.53 A 13.224.69.173…
```

Figure 2.3: *The queried website can not be revealed in packets while using TRR in Firefox*

Enabling the TRR function in Firefox is quite simple, only few steps to enable it. The steps are shown in Fig. 2.4 and Fig. 2.5. Compare to DoT, DoT can run on Android and IOS, but it needs some tools to run on Linux and Windows, thus it is more inconvenient [11].



1. Press the menu

2. Press Options

3. Select General

4. Press Settings... in Network Settings

Performance

☑ Use recommended performance settings Learn more

These settings are tailored to your computer's hardware and operating system.

Browsing

☑ Use autoscrolling

☑ Use smooth scrolling

☑ Show a touch keyboard when necessary

☐ Always use the cursor keys to navigate within pages

☐ Search for text when you start typing

☑ Enable picture-in-picture video controls Learn more

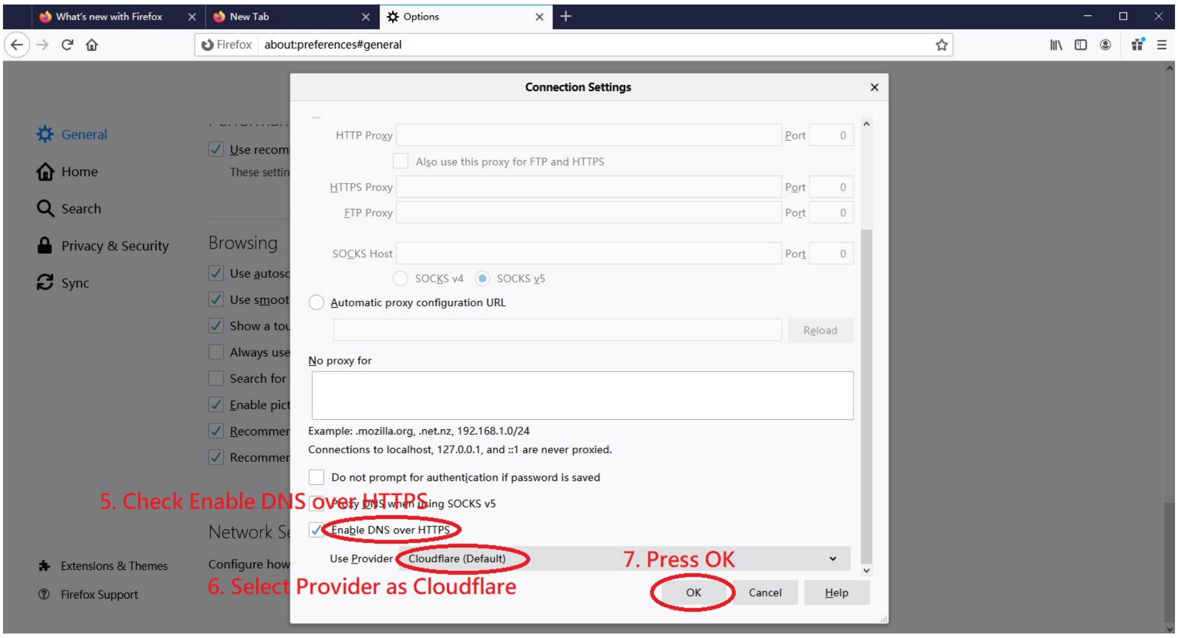
☑ Recommend extensions as you browse Learn more

☑ Recommend features as you browse Learn more

Network Settings

Configure how Firefox connects to the internet. Learn more

Figure 2.4: *The steps to enable TRR in Firefox - Part 1*



Connection Settings

HTTP Proxy Port 0

☐ Also use this proxy for FTP and HTTPS

HTTPS Proxy Port 0

FTP Proxy Port 0

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Connections to localhost, 127.0.0.1, and ::1 are never proxied.

☐ Do not prompt for authentication if password is saved

☐ Proxy DNS when using SOCKS v5

☑ Enable DNS over HTTPS

Use Provider Cloudflare (Default)

5. Check Enable DNS over HTTPS

6. Select Provider as Cloudflare

7. Press OK

Figure 2.5: *The steps to enable TRR in Firefox - Part 2*

Furthermore, Mozilla is also devoted in pushing TRR. In February 2020, Mozilla set TRR as the default setting of Firefox in USA, which means Firefox users used the DoH service if they do not do any change [28].

However, this policy caused a severe problem, after the TRR function was set as default setting in Firefox, the DNS provider NextDNS suffered a very high workload and struggled to handle the high traffic volume. It seems like a kind of DDOS attacking to those DNS providers, therefore Mozilla had to change the policy. In the later version Firefox 77.0.1 in June 2020, TRR has been removed the default setting, now users have to set the TRR function by themselves manually if they wish to enjoy DoH service [29].

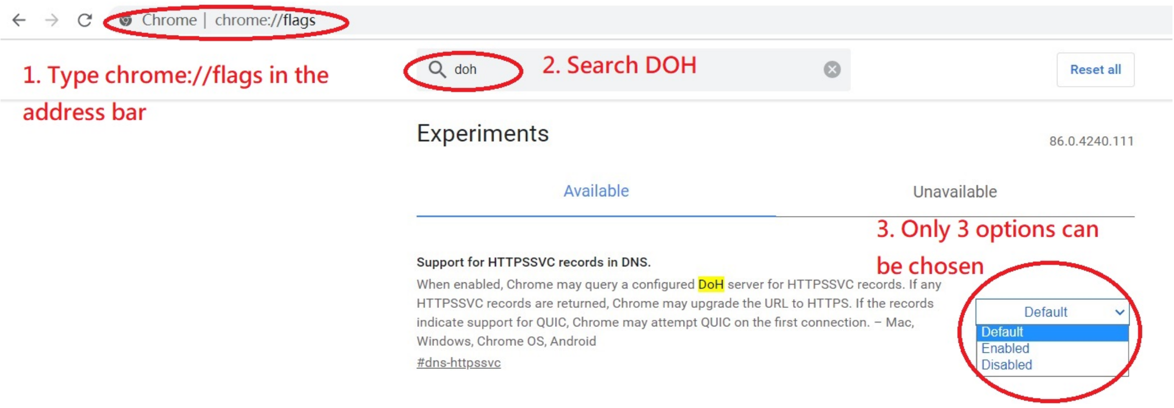
Hence, The time TRR been default setting was only lasted about 4 months(from February 2020 to June 2020). If Mozilla wants to make TRR being the default again, then the performance of DoH DNS servers must be capable to process the DNS queries of national scale.

As for Google Chrome, the main competitor to Mozilla Firefox, Chrome also supports DoH, and Google also intended to adjust DoH service to be the default setting for DNS queries as well [30].

The difference is that, the policy Google adopted is not TRR, because TRR is the unique program to Mozilla and its browser Firefox. The policy Google adopted is automatic upgrade. Which means, if the criteria that users have is met the requirement for using DoH service, then Chrome will change the setting to be DoH and users do not need to do anything. Google has already implemented this function in Chrome version 83 in May 2020 [31].

Another difference is that Chrome can not customize a DoH server in the browser, the options are only default, enabled and disabled in the DoH setting. Users have to set a DNS server which supports DoH in their operating systems. Contrarily, Firefox is more flexible, users are able to set a DoH DNS server which is different from the DNS server in their operating system. Therefore, it is easy to test or use a private DoH DNS server [32].

The interface of DoH setting is shown in Fig. 2.6.



1. Type chrome://flags in the address bar

2. Search DOH

3. Only 3 options can be chosen

Support for HTTPSSVC records in DNS.

When enabled, Chrome may query a configured DoH server for HTTPSSVC records. If any HTTPSSVC records are returned, Chrome may upgrade the URL to HTTPS. If the records indicate support for QUIC, Chrome may attempt QUIC on the first connection. – Mac, Windows, Chrome OS, Android

#dns-httpssvc

Figure 2.6: *DoH setting on Google Chrome*

Not only Firefox and Chrome support DoH, but also other browsers, such as Opera [33], Microsoft Edge and Vivaldi [34]. Every company or browser has their own plans to support DoH, those plans may be different and have their features, advantages and disadvantages.

However, this study just focuses on the TRR program which is executed by Mozilla Firefox. Thus, in a later chapter, this study is going to utilize the TRR function in Firefox to test a private DoH DNS server, which was built by the researcher, to perform benchmarks and determine the performance of the system.

Chapter 3

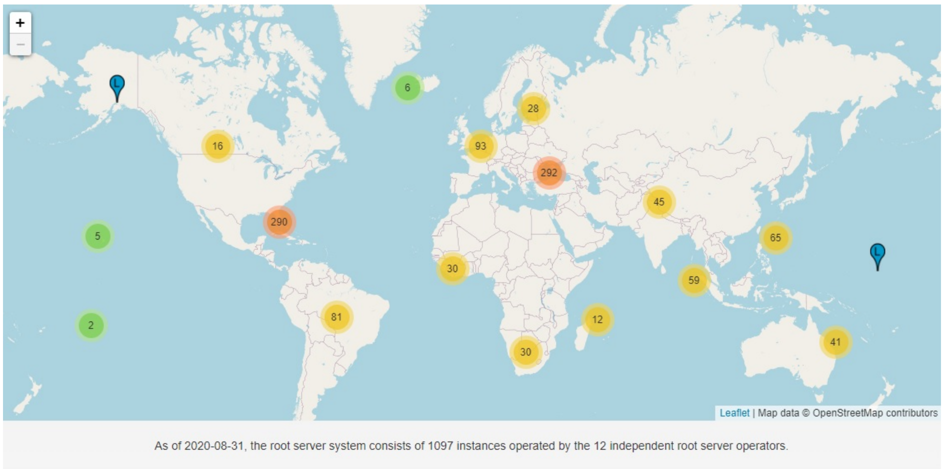
The DNS traffic in Ireland

3.1 The introduction of root servers

The DNS traffic is an important consideration for building a DNS server. Irish TRR servers have to be capable to deal with the DNS traffic of national scale traffic in Ireland.

Before understanding the DNS traffic in Ireland, it is necessary to understand the root servers first.

Root servers are the highest level DNS servers [5], there are 1097 instances in the root server system on 31 August 2020. They are divided into 13 root server zones, each zone has a representative letter, which are A, B, C, D, E, F, G, H, I, J, K, L and M [35]. Those root server zones are managed by 12 organizations [2], which are Verisign(It manages 2 root server zones), USC-ISI, Cogent Communications, University of Maryland, NASA Ames Research Center, Internet Systems Consortium, Defense Information Systems Agency, U.S. Army Research Lab, Netnod, RIPE NCC, ICANN and WIDE Project. Therefore, those 12 organizations have the information about DNS traffic.



As of 2020-08-31, the root server system consists of 1097 instances operated by the 12 independent root server operators.

Figure 3.1: *The root servers in the world [2]*

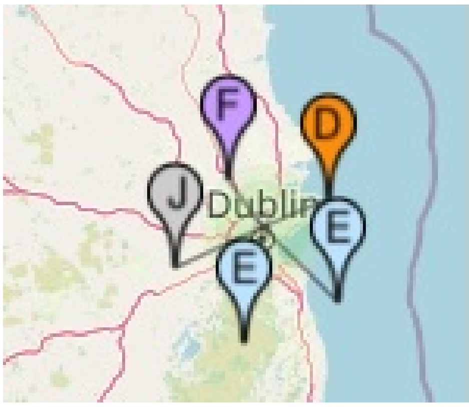


Figure 3.2: *The root servers in Dublin [2]*

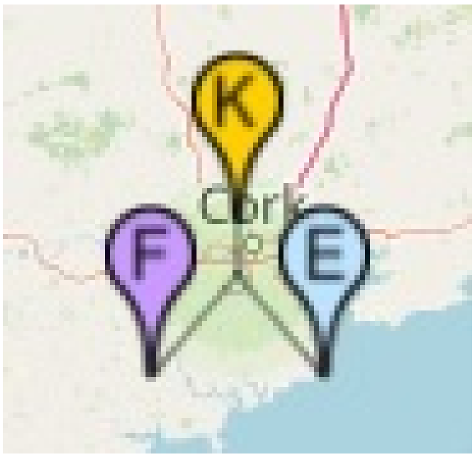


Figure 3.3: *The root servers in Cork [2]*

In the map from Root-servers.org, there are 8 root servers in Ireland, 5 servers are in Dublin and 3 servers are in Cork. As for organizations, 3 servers belong to E-root(E zone, it is managed by NASA Ames Research Center), 2 servers belong to F-root(F zone, it is managed by Internet Systems Consortium). K-root(RIPE NCC), D-root(University of Maryland), J-root(Verisign) have 1 server respectively [2]. The root servers are listed in Table. 3.1.

Zone	**Operator**	**Number in Ireland**
A	Verisign	0
B	USC-ISI	0
C	Cogent Communications	0
D	University of Maryland	1
E	NASA Ames Research Center	3
F	Internet Systems Consortium	2
G	Defense Information Systems Agency	0
H	U.S. Army Research Lab	0
I	Netnod	0
J	Verisign	1
K	RIPE NCC	1
L	ICANN	0
M	WIDE Project	0

Table 3.1: The list of root server zones [2]

The problem is the information those organizations provided is limited on the Internet. There is no statistic data of DNS queries in Ireland on their website.

It is very hard to collect the records about all DNS queries, because there are numerous recursive DNS servers and they are managed by many organizations [36], hence, the operators of root servers do not have their data.

3.2 Estimation using data from Akamai

It is hard to collect the number of entire DNS queries in Ireland, but the target of this study is to understand what the performance should a TRR server possess in Ireland. The number of DNS queries a root server received may help us to evaluate the required performance for a TTR server in Ireland.

In this paper, the researcher designs some methods to estimate the traffic a DNS server would have in Ireland by using the traffic in root servers.

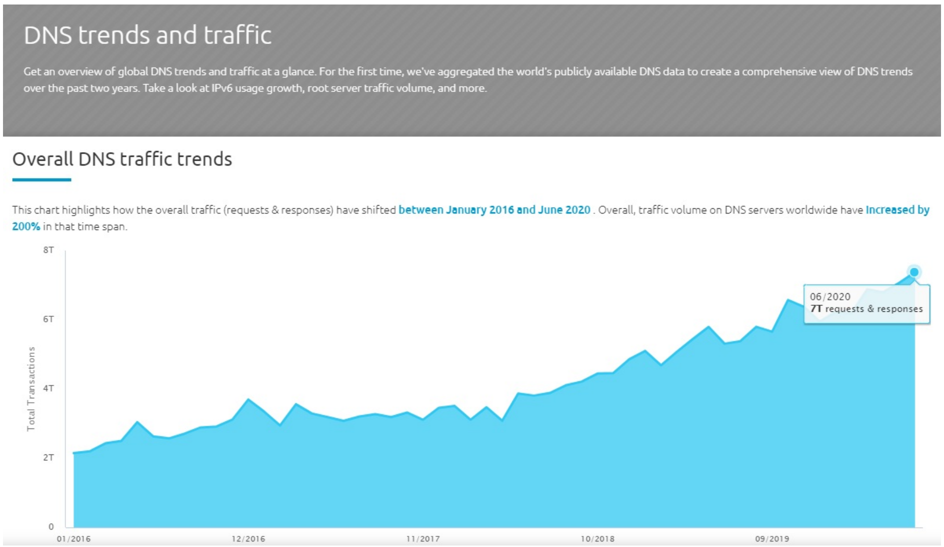
Method 1 is using the data on Akamai.com to estimate the DNS traffic [3].

In website Akamai.com, it collects the DNS traffic from 9 root server zones(B, C, D, E, F, I, K, L, M), but the DNS traffic is worldwide, it does not provide the data in national scale or city scale on the website.

Even though there is no national scale data on Akamai.com, but the worldwide data can be used to estimate the Irish DNS traffic.

In a report from Central Statistics Office of Ireland, it showed that there were 89% of Irish households have the internet at home in 2018 [37]. From the growth of households with the internet, the percentage is probably 90% in 2020. There were about 4.57 billion internet users in the world in July 2020 [38]. The population in Ireland was around 4.944 million in August 2020 [39]. Hence, the Irish Internet users may be about 4.113 million, it was approximately 0.09% of internet users in the whole world.

According to the data from Akamai.com [3], the overall DNS traffic in the world was about 7 Trillion transactions (Requests and responses) in June 2020. Then, 0.09% of DNS traffic in the world could be Irish DNS traffic, which is around 6.3 billion DNS transactions for one month in Ireland. On average, it could be 210 DNS million transactions in a day in Ireland.



DNS trends and traffic

Get an overview of global DNS trends and traffic at a glance. For the first time, we've aggregated the world's publicly available DNS data to create a comprehensive view of DNS trends over the past two years. Take a look at IPv6 usage growth, root server traffic volume, and more.

Overall DNS traffic trends

This chart highlights how the overall traffic (requests & responses) have shifted **between January 2016 and June 2020** . Overall, traffic volume on DNS servers worldwide have **Increased by 200%** in that time span.

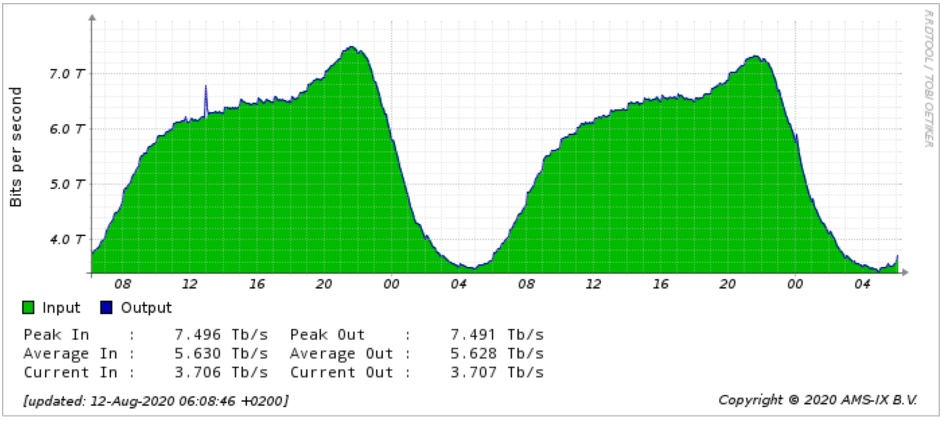
Figure 3.4: *The trend of DNS traffic in the world [3]*

Month	IPv4	IPv6	Total
06/2020	6T	1T	7T
01/2020	5T	969B	6T
07/2019	4T	919B	5T
01/2019	4T	848B	5T
07/2018	3T	564B	4T
01/2018	3T	426B	4T
07/2017	3T	371B	3T
01/2017	3T	363B	3T
07/2016	2T	248B	3T
01/2016	2T	171B	2T

Table 3.2: Overall DNS traffic trends(Unit:Transactions) [3]

However, internet traffic is changeable in different hours, it is necessary to understand when are the rush hours. For example, the internet rush hours are usually between 7 pm and 11 pm in UK [40]. In Sao Paulo, the internet rush hours are between 8 pm and 11 pm [41]. In USA, it is 8 pm to 10 pm [42]. In Berlin, the rush hours are

8 pm to 11 pm [43]. In Amsterdam, it is from 8 pm to 11 pm as well [4].

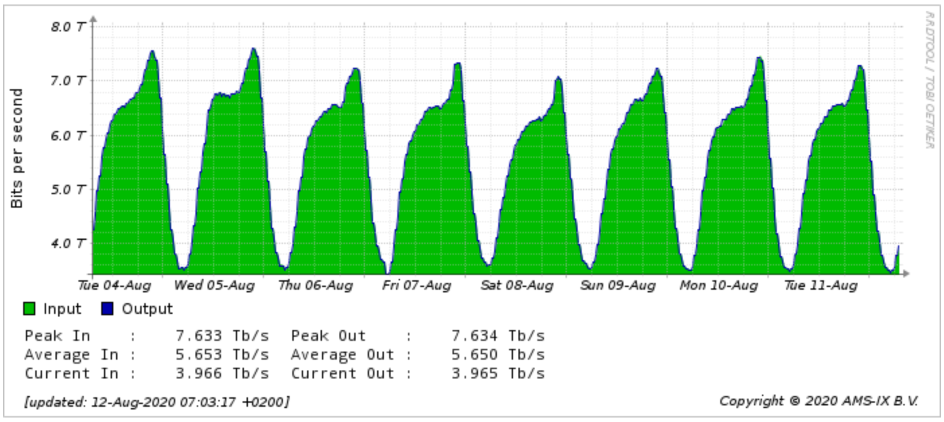


```
Peak In    :    7.496 Tb/s  Peak Out    :    7.491 Tb/s
Average In :    5.630 Tb/s  Average Out :    5.628 Tb/s
Current In :    3.706 Tb/s  Current Out :    3.707 Tb/s
```

[updated: 12-Aug-2020 06:08:46 +0200]

Copyright © 2020 AMS-IX B.V.

Figure 3.5: *The internet traffic in a day (Amsterdam) [4]*

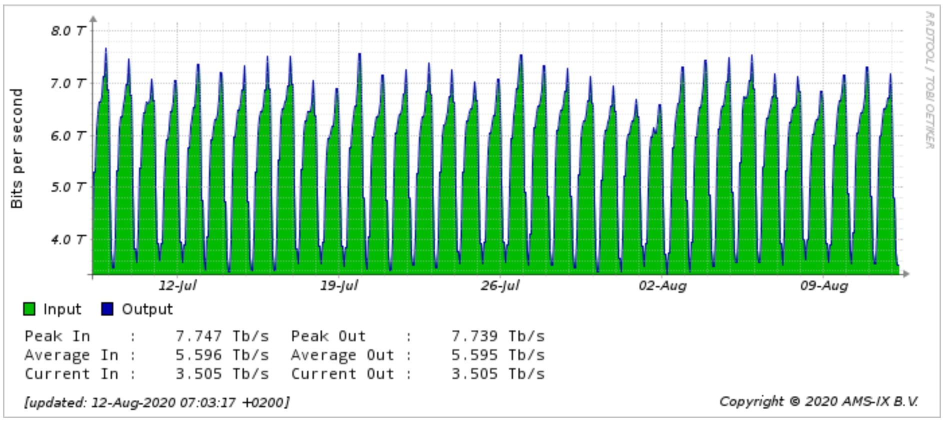


```
Peak In    :    7.633 Tb/s  Peak Out    :    7.634 Tb/s
Average In :    5.653 Tb/s  Average Out :    5.650 Tb/s
Current In :    3.966 Tb/s  Current Out :    3.965 Tb/s
```

[updated: 12-Aug-2020 07:03:17 +0200]

Copyright © 2020 AMS-IX B.V.

Figure 3.6: *The internet traffic in a week (Amsterdam) [4]*



```
Peak In    :   7.747 Tb/s  Peak Out    :   7.739 Tb/s
Average In :   5.596 Tb/s  Average Out :   5.595 Tb/s
Current In :   3.505 Tb/s  Current Out :   3.505 Tb/s
```

[updated: 12-Aug-2020 07:03:17 +0200]

Copyright © 2020 AMS-IX B.V.

Figure 3.7: *The internet traffic in a month (Amsterdam) [4]*

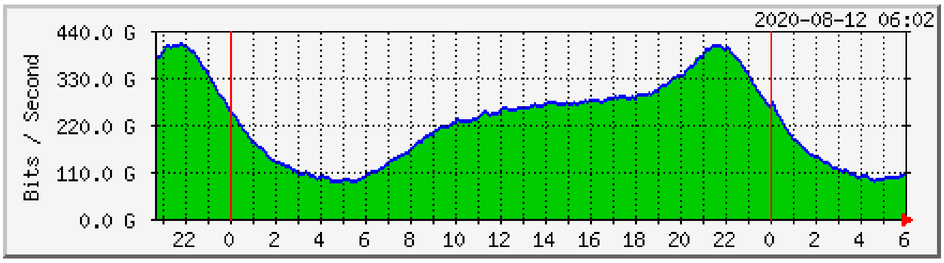


Figure 3.8: *The internet traffic in a day (Berlin) [4]*

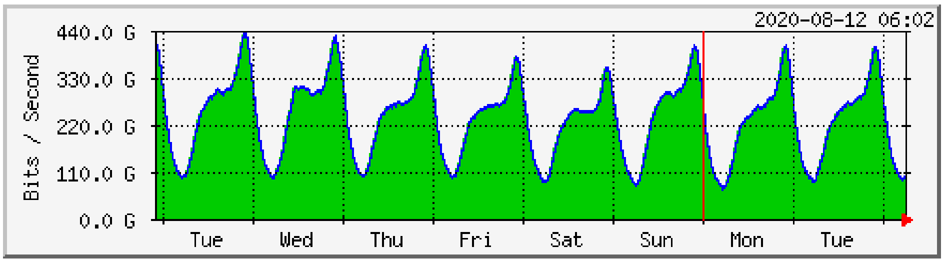


Figure 3.9: *The internet traffic in a week (Berlin) [4]*

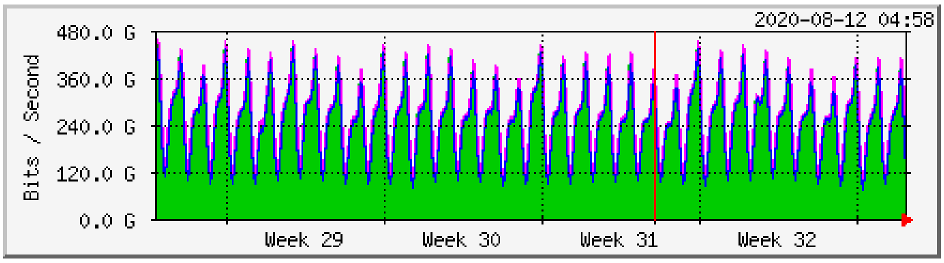


Figure 3.10: *The internet traffic in a month (Berlin) [4]*

All the reports in different countries or cities revealed that internet rush hours are from 8 pm to 11 pm in their local time zones, the distributions are pretty similar. Therefore, Irish internet rush hours could be assumed as from 8 pm to 11 pm as well.

As for the comparison in different days in a week, from Monday to Sunday, the change is not obvious. About the days in a month, from the beginning to the end of a month, there is no huge difference as well.

Taking the data in Amsterdam to estimate the percentage of usage in each hour, the result is shown in TABLE 3.3.

Hour(24)	**Trillion bit/s**	**Percentage**
0	5.8	4.3%
1	4.8	3.56%
2	4	2.96%
3	3.7	2.74%
4	3.6	2.67%
5	3.5	2.59%
6	3.6	2.67%
7	4	2.96%
8	4.8	3.56%
9	5.4	4%
10	5.8	4.3%
11	6	4.44%
12	6.2	4.59%
13	6.4	4.74%
14	6.4	4.74%
15	6.6	4.89%
16	6.6	4.89%
17	6.6	4.89%
18	6.5	4.81%
19	6.7	4.96%
20	6.9	5.11%
21	7.2	5.33%
22	7.2	5.33%
23	6.7	4.96%
Total	135	100%

Table 3.3: Internet traffic and its percentage in each hour in a day in Amsterdam [4]

After that, using the percentage to multiply the estimated number of daily DNS transactions in Ireland, which is 210 million, then the result is sown in TABLE 3.4. The 2 busiest hours are 9 PM and 10 PM, the number of DNS transactions could be

11.2 million in an hour.

Hour(24)	**Percentage**	**Million transactions**
0	4.3%	9.02
1	3.56%	7.47
2	2.96%	6.22
3	2.74%	5.76
4	2.67%	5.6
5	2.59%	5.44
6	2.67%	5.6
7	2.96%	6.22
8	3.56%	7.47
9	4%	8.4
10	4.3%	9.02
11	4.44%	9.33
12	4.59%	9.64
13	4.74%	9.96
14	4.74%	9.96
15	4.89%	10.27
16	4.89%	10.27
17	4.89%	10.27
18	4.81%	10.11
19	4.96%	10.42
20	5.11%	10.73
21	5.33%	11.2
22	5.33%	11.2
23	4.96%	10.42
Total	100%	210

Table 3.4: Using the daily distribution of Internet traffic of Amsterdam to estimate the DNS traffic in Ireland [4]

However, the data from Akamai.com does not include A, G, H and J root server zones. Thus, the number of transactions in rush hours should be higher than 11.2 million.

The numbers of transactions in every root server zone are very different, therefore it is hard to estimate the numbers in A, G, H and J root server zones. If we assume that the average number of A, G, H and J is close to the average number of the root servers for which we have data, then the estimated number of transactions in all root servers in rush hours could be 11.2÷9×13=16.18 million.

If convert it into a second, the number of DNS transactions could be 4,494 per second during the rush hour.

3.3 Estimation using real-time data from ICANN

Method 2 is using the data from ICANN to estimate DNS traffic.

ICANN (Internet Corporation for Assigned Names and Numbers) is the one of 12 organizations which are responsible for managing DNS root servers. The servers it manages are L-root servers. Unlike other 11 organizations, ICANN provides a website to display real-time DNS traffic, that is Stats.dns.icann.org [6].

The problems are ICANN does not have root servers in Ireland. Moreover, those data are only from ICANN, it does not include the data from other root server zones.

Thus, this study choose a city which has a similar population to Ireland to estimate the DNS traffic. Melbourne should be a ideal sample. The population in Melbourne is about 5 million in 2019 [44], which is close to the population in Ireland (4.9 million). Moreover, Melbourne is isolated, there is no big city near Melbourne,therefore the network connection may be similar to a country.

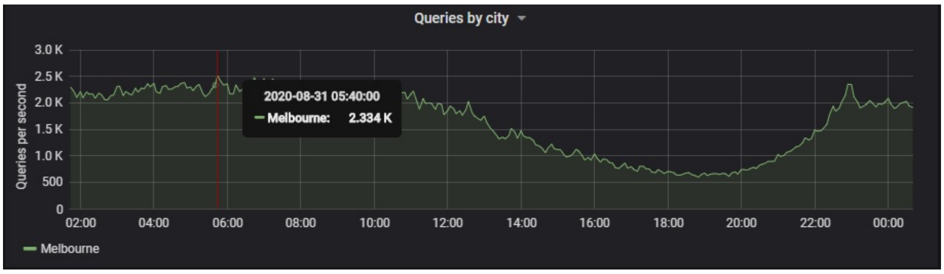


Figure 3.11: *The number of queries per second in a root server in Melbourne [6]*

From the data in Fig. 3.11, the highest value in a day is 2,334 per second, which was occurred at 05:40 UTC(19:40 in Melbourne).

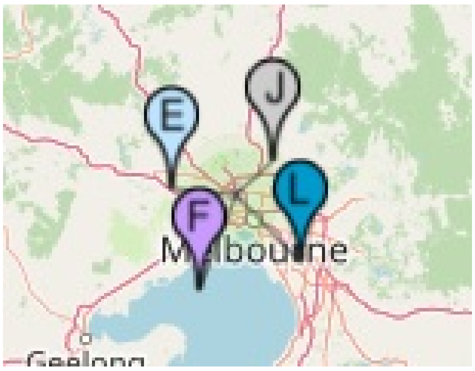


Figure 3.12: *The root servers in Melbourne [2]*

However, the data is only from a root server which is managed by ICANN, there are four root servers in Melbourne, the DNS traffic in other 3 root servers are not provided. Assuming the average traffic in other 3 root servers is close to the root server managed by ICANN, the whole DNS traffic in Melbourne could be 9,336 per second(2,334×4). Next, adjust the traffic to accord the population of Ireland, the DNS traffic could be 9,149 queries per second during the rush hour(9,336÷5×4.9).

The comparison between method 1 and method 2 is shown in TABLE 3.5.

	Method 1	**Method 2**
Source	Akamai.com	ICANN
Queries per second in rush hours	4,494	9,149
Drawback 1	No Irish data	No Irish data
Drawback 2	Only monthly data	The data is only from L-root

Table 3.5: The comparison between 2 methods for the estimation of the DNS traffic in Ireland

Chapter 4

The required software

4.1 The overview of required software

This study focuses on Trusted Recursive Resolver. Therefore, the DNS software we talk about here is the software to build a recursive resolver, not the authoritative DNS server. There are many existing recursive resolver implementations, such as BIND, Unbound, DNSMASQ, PowerDNS, Microsoft DNS and Cisco Network Registrar [45] [46].

In this study, Unbound, BIND and PowerDNS are recommended, because there are many discussions and tutorials about those 3 software on Internet [47]. These particular implementations are widely used and well-documented. Thus, users of this software will find it easy to build private or public recursive resolvers.

Unbound is a free open-source implementation of a recursive DNS server. It does not support the authoritative DNS server. The developer is NLnet Labs, the developer also designed another DNS software, which is NSD(Name Server Daemon). In contrast, NSD is only for building authoritative DNS servers [48]. Unbound supports some security functions, such as Domain Name System Security Extensions(DNSSEC) and DNS over TLS(DoT). Moreover, the operating systems for running Unbound can be

Linux, FreeBSD and Windows [49].

About BIND, its alias is Named. It is developed by Internet Systems Consortium(ISC). ISC is also the organization which is responsible for managing F root server zone. Unlike Unbound, BIND supports both modes of recursive resolver and authoritative DNS server. The stable version is BIND 9. It can run on Windows, Mac-OS and Linux [50].

PowerDNS supports both authoritative DNS server and recursive DNS server. Moreover, it provides a Graphic UI for management and uses relational databases to store data. The developer is PowerDNS.COM and operating systems are Linux and UNIX [51].

Apart from DNS software, building a DNS server for TRR also needs some other software, including operating systems, DoH tools and HTTP servers [52] [53].

The DoH DNS server need DoH tools to receive DoH queries and test the function. DoH-proxy is designed for this purpose, it is developed by Facebook. It can be installed on Linux but it requires Python 3.5 [54]. DoH-proxy inlcudes 4 tools, which are DoH-proxy, DoH-httpproxy, DoH-stub and DoH-client. DoH-httpproxy and DoH-client were used in this study, because DoH-httpproxy provides the DoH service, and DoH-client is the testing tool to connect a DoH DNS server to check the installation is successful or not.

After that, NGINX can provide the HTTP service. NGINX is a HTTP server with high performance, it can also provide different kinds of services. The operator can set the method for listening queries from users [55].

In choosing a operating system, there are many operating systems could be used to install DNS servers, such as Windows server, FreeBSD, Linux.

There are many members in the Linux family, such as Fedora,Red Hat Linux, CentOS, Ubuntu and Debian. CentOS was chosen for testing here, because it is free, and the structure is the offshoot of Red Hat enterprise, hence it is very stable.

The required software is shown in TABLE 4.1.

Category	**Software**
DNS	BIND
DNS	Unbound
DNS	PowerDNS
DoH Tool	DoH-proxy
HTTP Server	NGINX
Operating System	Linux

Table 4.1: The required software for building a DNS server for TRR

4.2 The comparison and installation among DNS software applications

In order to compare the ease of installation and configuration of BIND, Unbound and PowerDNS, the researcher tried to install those 3 DNS software on the local server and test them.

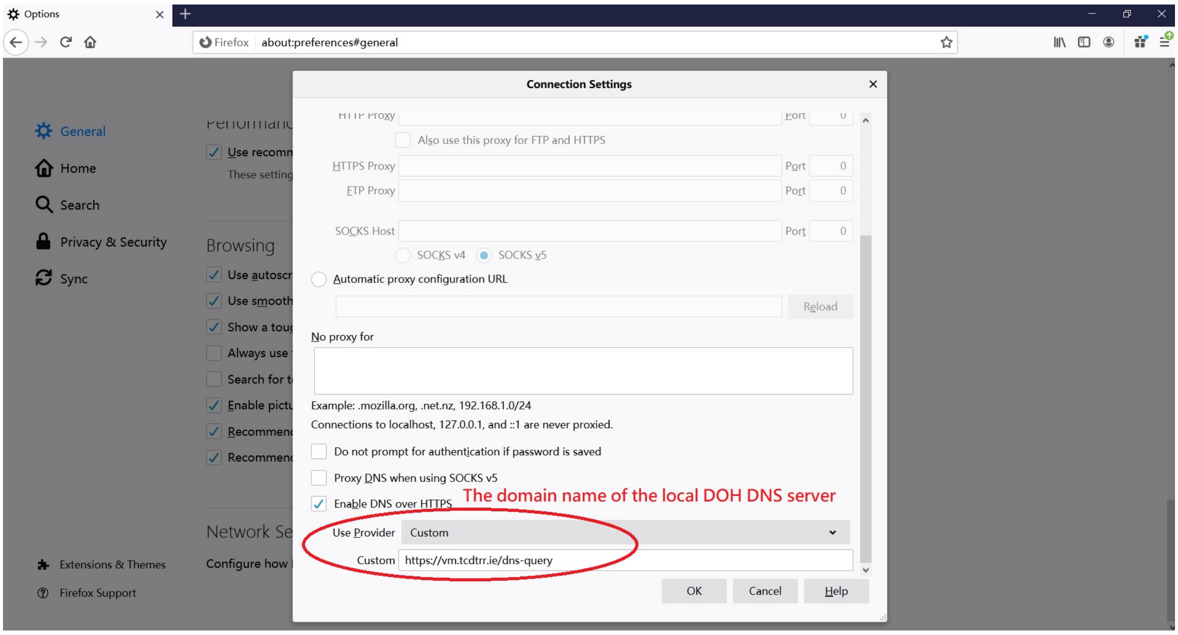
The equipment in this study was limited, only a personal computer can be utilized. Thus, the researcher had to use a virtual machine to install Linux on the personal computer. The software for running the virtual machine was VMware Workstation Player.

After installing the operating system, then the researcher installed BIND, Unbound and PowerDNS, and set the configuration files of those DNS servers, to make sure those DNS servers were in the same network zone with other testing devices.

Next, the researcher used Internet Information Services(IIS) to create a simple website on the personal computer, and gave fixed local IP addresses to all devices and the virtual machine. In the DNS server(BIND, Unbound and PowerDNS), a domain name was set to the simple website to match its IP address. This simple website was the website for testing.

Finally, used the testing devices(Android phone and IPad) to type the domain name of the testing website on browsers(Google Chrome and Safari). If the testing website could be displayed on testing devices, then the DNS server functioned well.

As for DoH service, the study also added it on the local DNS server and tested it. After the implementation of DoH service, the researcher enabled the TRR function in Firefox and input the domain name of the local DNS server in the TRR customized DoH provider to test it. The TRR function was working well on Firefox, therefore this local DoH server with its configuration can be the DNS server for TRR. The screenshots were displayed in Fig. 4.1 and Fig. 4.2. "vm.tcdtrr.ie" is the domain name of the local server which was built by the researcher.



Connection Settings

HTTP Proxy Port 0

☐ Also use this proxy for FTP and HTTPS

HTTPS Proxy Port 0

FTP Proxy Port 0

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

Reload

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Connections to localhost, 127.0.0.1, and ::1 are never proxied.

☐ Do not prompt for authentication if password is saved

☐ Proxy DNS when using SOCKS v5

☑ Enable DNS over HTTPS

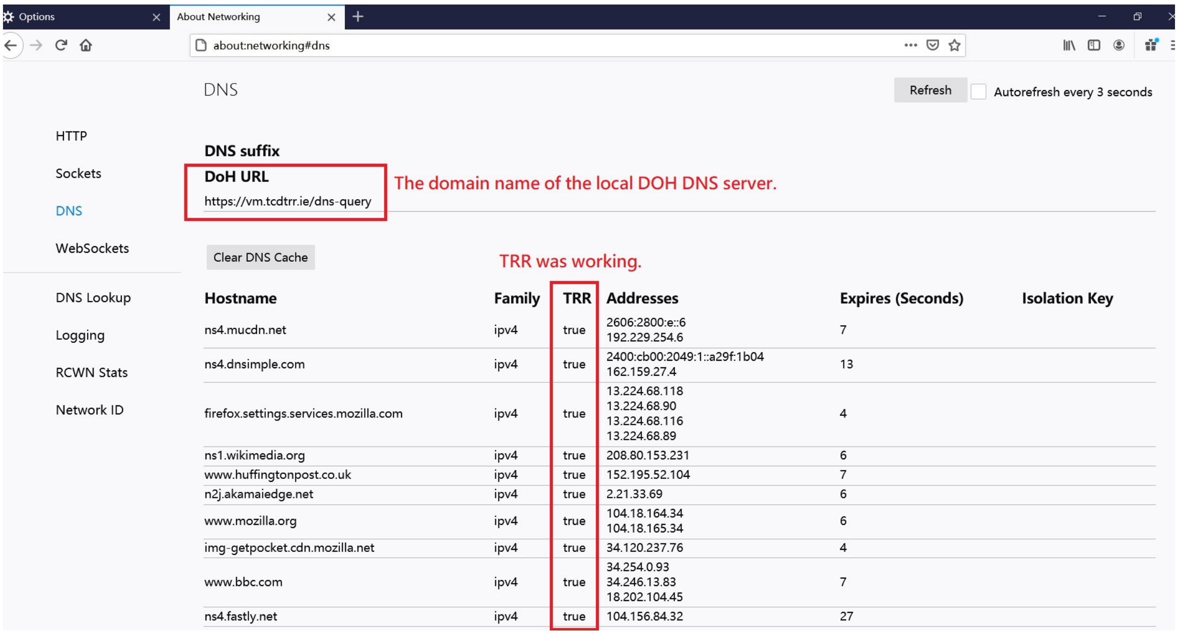
Use Provider Custom

Custom https://vm.tcdtrr.ie/dns-query

OK Cancel Help

The domain name of the local DOH DNS server

Figure 4.1: *Users can customize the DoH provider by its domain name.*



DNS

DNS suffix

DoH URL

https://vm.tcdtrr.ie/dns-query

The domain name of the local DOH DNS server.

TRR was working.

Hostname	Family	TRR	Addresses	Expires (Seconds)	Isolation Key
ns4.mucdn.net	ipv4	true	2606:2800:e::6 192.229.254.6	7	
ns4.dnsimple.com	ipv4	true	2400:cb00:2049:1::a29f:1b04 162.159.27.4	13	
firefox.settings.services.mozilla.com	ipv4	true	13.224.68.118 13.224.68.90 13.224.68.116 13.224.68.89	4	
ns1.wikimedia.org	ipv4	true	208.80.153.231	6	
www.huffingtonpost.co.uk	ipv4	true	152.195.52.104	7	
n2j.akamaiedge.net	ipv4	true	2.21.33.69	6	
www.mozilla.org	ipv4	true	104.18.164.34 104.18.165.34	6	
img-getpocket.cdn.mozilla.net	ipv4	true	34.120.237.76	4	
www.bbc.com	ipv4	true	34.254.0.93 34.246.13.83 18.202.104.45	7	
ns4.fastly.net	ipv4	true	104.156.84.32	27	

Figure 4.2: *The records of successful DNS queries of TRR.*

Above steps were the testing method for the study. The testing environment is shown in TABLE 4.2.

Platform	VMware Workstation 15.5.6 Player
Operating system(Server)	CentOS 8.2.2004
Internet connection	Bridge mode
Testing devices	Desktop, IPad, Android phone
Operating system(Client)	Windows, IOS, Android
Testing method	Browsing a local website

Table 4.2: The installation environment

The following discussion is about configuration. The configuration of BIND is using the style of C language to be the format of the configuration file. Therefore, in case the maintenance personnel does not have programming background, then it needs time to understand the syntax of C language.

Unbound's configuration file format is very simple, it does not belong to any kind of computer languages. The setting is just listed line by line.

PowerDNS stores information about domains and records in a relational database. The settings for DNS are stored in a configuration file.

The installation of PowerDNS is more complex than Unbound and BIND, because it uses the relational database. This requirement for a relational database causes more work at installation time. However, the trade-off is that PowerDNS provides a web interface to display the information of the DNS server or set the configuration. Hence the maintenance is easier than BIND and Unbound.

The comparison among BIND, Unbound, PowerDNS is shown in Table 4.3.

	BIND	**Unbound**	**PowerDNS**
Version	9.11.13	1.7.3	4.3.1
Configuration	C language	Line by line	RDBMS
Log style	Log file	Log file	MySQL
Installation difficulty	Easy	Easy	Difficult
Maintenance difficulty	Normal	Normal	Easy

Table 4.3: The comparison among BIND, Unbound, PowerDNS

4.3 Previous studies about the performance of DNS software

According to a report which was written by Hamza Boulakhrif in University of Amsterdam, the times for processing queries in BIND, Unbound and PowerDNS were similar [56]. The biggest difference was that when the time of processing exceeded 16 seconds, then PowerDNS did not respond. If the time exceeded 17 seconds, BIND did not respond, only Unbound can wait until the finish of processing then sent results to users .

According to the assumption of Hamza Boulakhrif, if processing time is under 1 milliseconds, then it is processed by the cache. The caches in DNS servers contain the matched IP addresses that users are looking for, thus DNS servers can respond to users in a very short time and do not need to forward users' requests to authoritative DNS servers.

As for running DNSSEC, there was no obvious difference if compare to the results without DNSSEC in his experiment.

The regulation in BIND and PowerDNS are similar, both of them have the time limit, thus in case the processing time reaches the time limit, then the query will be failed. In contrast, Unbound has a different working type, it allows the system to have a long time to wait for the answer after the process. Hamza Boulakhrif called those different working types as "Failed response over a late response" and "An answer is better than no answer". PowerDNS and BIND adopts "Failed response over a late response" and Unbound adopts "An answer is better than no answer" [56].

In conclusion, in choosing DNS resolver software, because BIND, Unbound, PowerDNS have similar performances, the point of the decision is allowing a long time to wait for the answer or not. If yes, the operator should choose Unbound. Otherwise, he should choose BIND or PowerDNS.

However, the report was written in 2015, which was 5 years ago, the performance may be different now.

Another paper wrote at Princeton University also researched the performance of DNS [57]. That paper did not compare DNS software. That paper compared the performance among the traditional DNS, DoT and DoH instead.

This study does not discuss DoT, thus we only took the comparison between traditional DNS and DoH from that paper. The comparison revealed that DoH service required the longer loading time if compare to the traditional DNS on websites in most cases.

In order to prove that, this study had an experiment to test the performance of DoH and the traditional DNS as well. The result and testing steps are described in chapter 5.

Chapter 5

The experiment

5.1 The implementation of the experiment

In order to understand the performance of a DoH server, the researcher designed an experiment. Unfortunately, the moment during this studying encountered Coronavirus disease(COVID-19) pandemic, it was mandatory to stay at home, hence the researcher has to use the personal computer and the home network to finish this study.

First of all, a DoH server was built in the local network. After that, used Python to design a testing program. The function of the testing program was sending massive DNS queries to the local DoH server in a very short time. Then, the testing program recorded results and latencies of the responses from the DoH server. The testing environment is described in Table 5.1.

The testing program utilized multi-thread to send queries, thus queries can be sent in a very short time. 50 to 500 queries can be sent between 0.01 and 0.07 seconds. The outputs of this testing program are CSV files, those CSV files contain the records and statistic of the tests in this experiment.

	Description
Server platform	VMware Workstation 15.5.6 Player
Server operating system	Linux CentOS 8.2.2004
Client operating system	Windows 10
Server CPU	Intel Core i7-7700(3.60GHz, 4 cores
Server memory	8 GB
Server hard-disk	20 GB
DNS resolver	BIND 9.11.13
DNS tools	DoH-proxy
HTTPS server	Nginx 1.14.1
Testing language	Python 3.9
DNS library	DNSPython, dnslib(paulc)
Other library	ssl, csv, json, base64, urllib, threading
Testing location	Dublin District 1 (a private accommodation)
The Internet	Virgin Media Ireland Broadband 250 Mb
Query name	The top 50 websites in Ireland
The DNS provider	Local(Built by the researcher)

Table 5.1: The testing environment of the experiment

This study adopted the top 50 websites in Ireland to be the query names for all tests. The meaning of the top 50 websites in Ireland is not the websites created by Irish nor located in Ireland. The meaning is the websites Irish browsed most, and the source is Alexa.com [58], the accessed date was 25 October 2020. Alexa.com is the company which makes the ranking to websites by popularity. Only the ranking of the top 50 websites is free. If the people need to know the ranking more than 50, then they have to pay for it.

Meanwhile, the testing program can set some parameters, therefore the researcher was able to gain the data from different parameters, those parameters were independent variables or controlled variables [59] in this experiment. The parameters are shown in Table 5.2. The independent variables were the changed parameters and the controlled variables were the unchanged ones.

Parameters	**Options**
Record type	A, AAAA, MX
DNS type	DoH(Wireformat), Traditional DNS
Query interval	No interval, 0.1 Sec., 0.02 Sec., 0.04 Sec., 0.06 Sec., 0.08 Sec.

Table 5.2: The parameters in the experiment

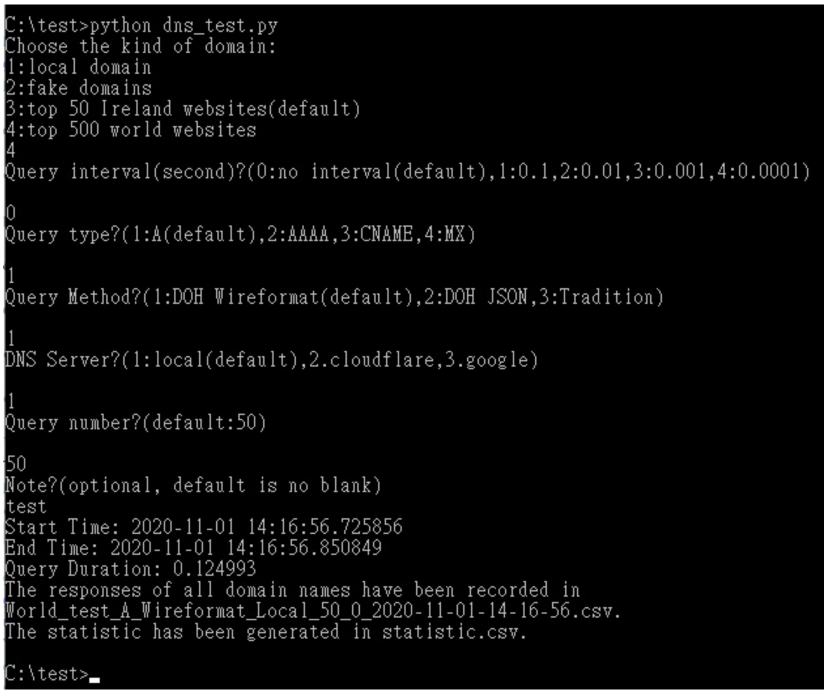
The outputs of the testing program were dependent variables, which were the results of the experiment. The researcher used those results from different parameters to analyze the performance of a DoH DNS server. The outputs are shown in Table 5.3.

There are 3 results of responses, which are Successful, Failed and No Answer. "Successful" is the query which is successful to get the IP address from the response from the DNS server. "Failed" means the DNS server can not find the matched IP address for the queried domain name, or the server is too busy to find the matched IP. The third result is "No Answer", if the DNS server respond any error message or no message, then the result is classified as "No Answer".

Outputs	**Results**
The results of responses	Successful, Failed, No Answer
The number of responses	A number of each result, from 0 to 500
The fastest response of a result	Seconds and the domain name
The latest response of a result	Seconds and the domain name
The average response of a result	Seconds
Responses in 0.1 Sec.	A number for each result, from 0 to 500
Responses between 0.1 and 1 Sec.	A number of each result, from 0 to 500
Responses between 1 and 5 Sec.	A number of each result, from 0 to 500
Responses more than 5 Sec.	A number of each result, from 0 to 500
Queries start time	Time
Queries end time	Time
Queries sending duration	Seconds

Table 5.3: The Outputs(Results) of testing

The screenshot of the testing program is displayed in Fig. 5.1. It runs as a Python application, and the researcher is able to input parameters by keyboard. The outputs are including the statistic and the results of all responses of DNS queries, they are saved into 2 CSV files.



```
C:\test>python dns_test.py
Choose the kind of domain:
1:local domain
2:fake domains
3:top 50 Ireland websites(default)
4:top 500 world websites
4
Query interval(second)?(0:no interval(default),1:0.1,2:0.01,3:0.001,4:0.0001)

0
Query type?(1:A(default),2:AAAA,3:CNAME,4:MX)

1
Query Method?(1:DOH Wireformat(default),2:DOH JSON,3:Tradition)

1
DNS Server?(1:local(default),2.cloudflare,3.google)

1
Query number?(default:50)

50
Note?(optional, default is no blank)
test
Start Time: 2020-11-01 14:16:56.725856
End Time: 2020-11-01 14:16:56.850849
Query Duration: 0.124993
The responses of all domain names have been recorded in
World_test_A_Wireformat_Local_50_0_2020-11-01-14-16-56.csv.
The statistic has been generated in statistic.csv.

C:\test>
```

Figure 5.1: *The screenshot of the testing program*

5.2 The test for DoH and the traditional DNS

This test was testing the difference of performance between the traditional DNS service and the DoH service. There are 2 kinds of DoH querying, which are Wireformat [60] and JavaScript Object Notation(JSON) [61] [62]. However, the local DoH server did not response the query with JSON format, therefore the study used Wireformat to do the test.

The test repeated 3 times, and the cache of the local DNS server was flushed before each test. The parameters were shown in Table 5.4. The results of 3 those repeated tests were displayed in Fig. 5.2 and Fig. 5.3.

Parameters	**Values**
Query name	The top 50 websites in Ireland
Record type	A
Query interval	No interval
Query time	From 21:37:53 to 21:40:13 7/11/2020

Table 5.4: The parameters for testing DoH and the traditional DNS

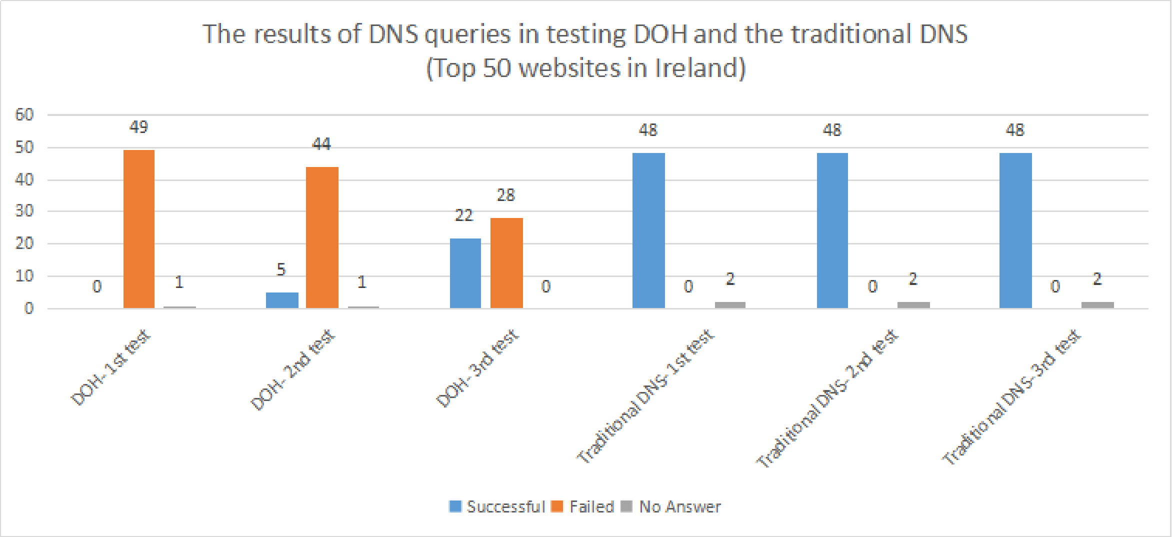


Figure 5.2: *The numbers of results of DNS queries in testing DoH and the traditional DNS, the parameters are shown in Table 5.4*

.

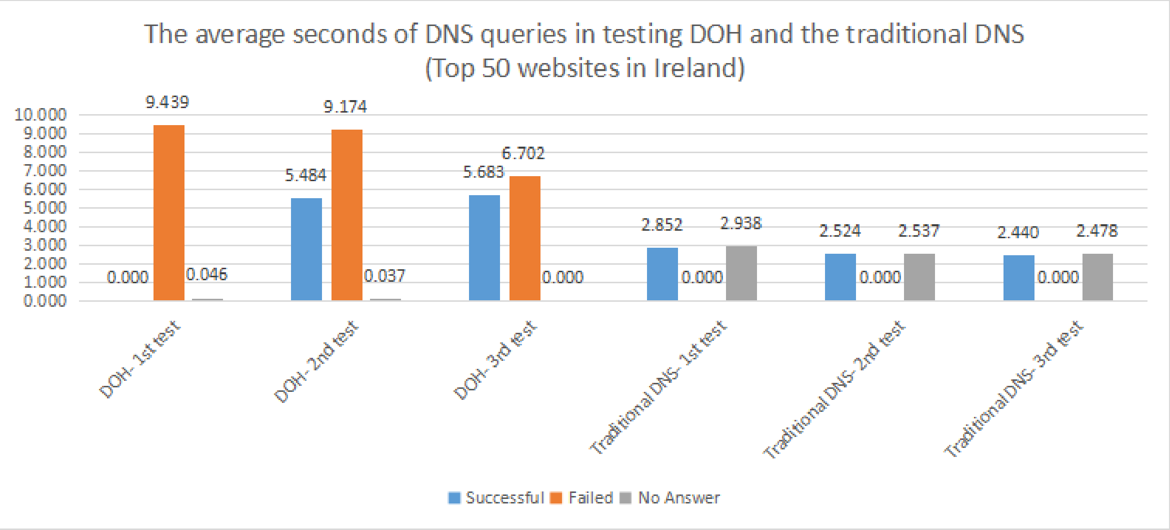


Figure 5.3: *The average seconds of DNS queries in testing DoH and the traditional DNS, the parameters are shown in Table 5.4*

.

The results illustrated that the performance of the traditional DNS service was better than the DoH service.

The traditional DNS has higher number of successful responses of DNS queries. Every DNS query is successful(48 domain name were valid, but 2 domain name were not accessible). On the other hand, the average time of responses is also obviously shorter than DoH. Contrarily, the failed number was higher in DoH, and it spent more time to process the DNS query.

The noticeable result is that the first time test of DoH did not have any successful response. This study assumes that the time executed the test was during the peak time, the Internet traffic might be very busy at that moment. Furthermore, the packet of DoH is bigger than the traditional DNS. Therefore, the authoritative DNS server could not deal with the massive DoH queries in extremely short time.

Nevertheless, this assumption can not explain why all DNS queries were successful in the traditional DNS(2 websites were not accessible). The gap was huge. However, the actual reason has not discovered yet. The further test of the performance of DoH was in the next section.

Overall, those results were also close to the results of the paper wrote at Princeton University [57].

5.3 The test for query intervals

The study assumes that the massive queries in a very short time could decline the performance of a DNS server. Hence, this test was designed to figure out how the performance is affected by the frequency of DNS query sending.

The testing program can set the query interval. For example, if the query interval is 0.1 second, then the next query will be sent after 0.1 second after the previous query. If the query interval is set as 0, then there is no query interval, the next query will be sent as fast as possible. In this case, the sending speed depends on the speed of processing in the testing program.

There were 6 intervals in this test, which were 0 second(no interval), 0.02 second, 0.04 second, 0.06 second, 0.08 second and 0.1 second. The parameters were shown in Table 5.5, and the cache was flushed before the testing as well.

The test also repeated 3 times. The results of those 3 repeated tests were shown in Fig. 5.4, Fig. 5.5, and Fig. 5.6.

Parameters	**Values**
Query name	Top 50 websites in Ireland
DNS type	DoH(Wireformat)
Record type	A
Query time	From 21:13:06 to 21:25:53 7/11/2020

Table 5.5: The parameters for testing query intervals

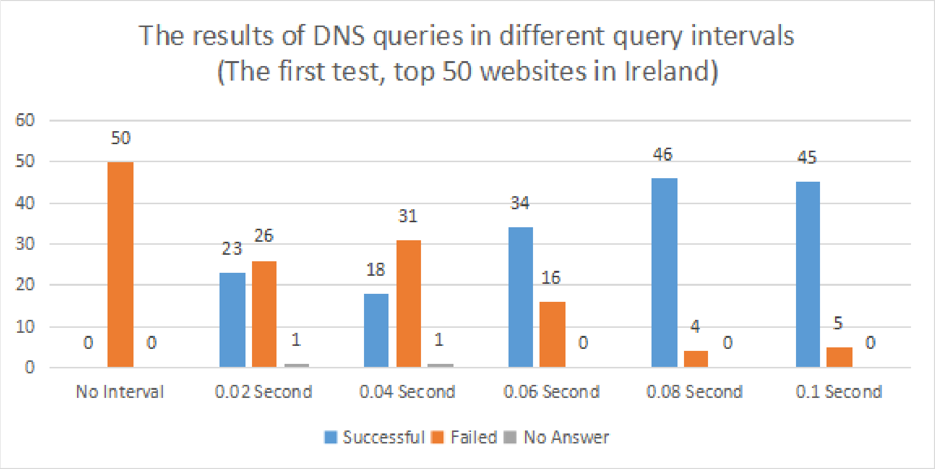


Figure 5.4: *The numbers of results of DNS queries in different query intervals for the first test, the parameters are shown in Table 5.5*

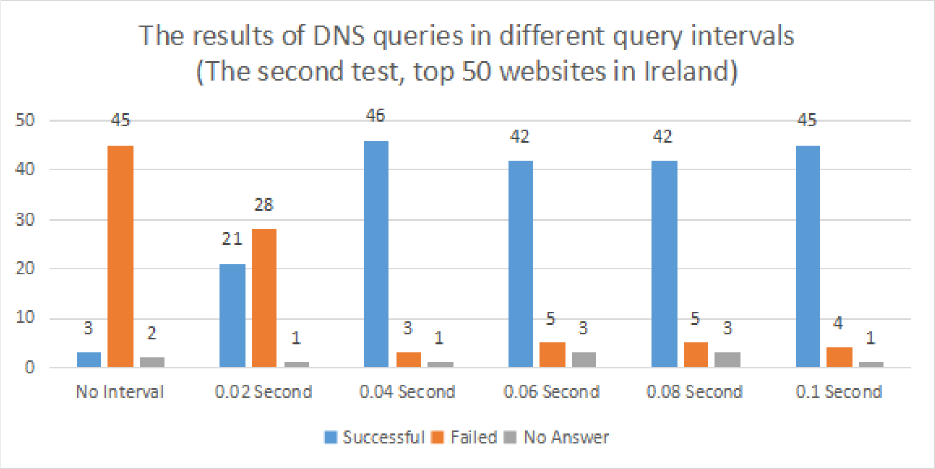


Figure 5.5: *The numbers of results of DNS queries in different query intervals for the second test, the parameters are shown in Table 5.5*

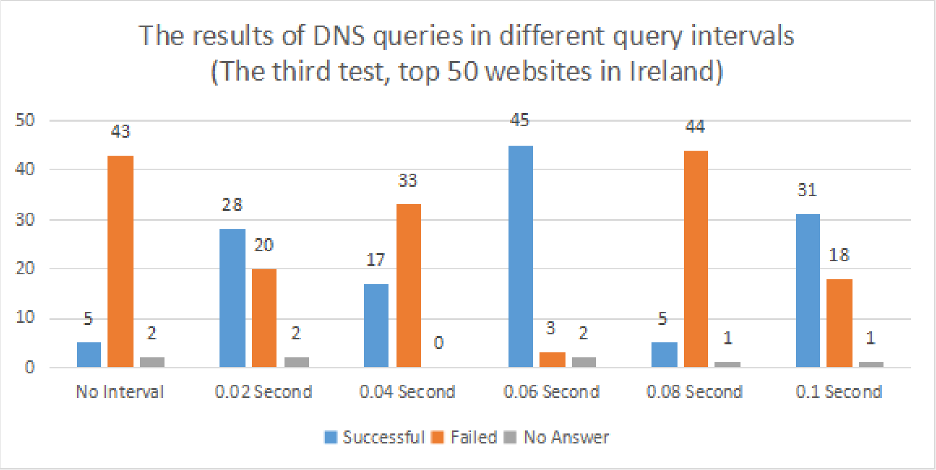


Figure 5.6: *The numbers of results of DNS queries in different query intervals for the third test, the parameters are shown in Table 5.5*

The figures showed that the interval of query sending affected the performance a lot. The longer interval usually had the better performance, but the relationship between the query interval and the performance was not absolute. The performances in some shorter intervals were better than the longer intervals. Thus, the results were not stable.

The numbers of successful responses were still very low in No Interval among those 3 repeated tests(they were 0, 3 and 5). Those results were also similar to the results in the previous section. If there was a little time between queries, even 0.02 second, the time interval could improve the performance of DoH a lot.

The study supposes that the longer interval was able to relieve the workload on a DNS server. However, the longer interval also made the query sending duration longer. Hence, the results of this test support the idea that massive or intensive queries can decrease the performance of a DNS server.

5.4 The test for DNS record types

The DNS record types [63] were also tested here. There are many DNS record types, but this study just used 3 types, which were A, AAAA, and MX. CNAME(Canonical Name) had been used to test, but all top 50 websites in Ireland do not have CNAME. Therefore the study removed CNAME from the results.

A is getting the IP address of IPv4 [13], it is the most popular DNS record type so far. AAAA is getting the IP address of IPv6 [14]. MX stands for Mail Exchange, it is used to getting the e-mail server.

However, not every domain name has A, AAAA or MX. there were 48 domain names has A, 19 domain names has AAAA, and 46 domain names has MX. Hence, this test does not compare the numbers of the successful DNS queries. Instead of the numbers, the comparison in this test used the average time of processing DNS queries.

This test repeated 3 times as well. The parameters were set as Table 5.6. The query interval was set as 0.1 second, because the performance of 0.1 second was the best in the test of the previous section. The cache was also flushed before testing. The results of those 3 repeated tests were illustrated in Fig. 5.7, Fig. 5.8 and Fig. 5.9.

Parameters	**Values**
Query name	The top 50 websites in Ireland
DNS type	DoH(Wireformat)
Query interval	0.1 Second
Query time	From 14:11:38 to 14:16:07 8/11/2020
Available number- A	48
Available number- AAAA	19
Available number- MX	46

Table 5.6: The parameters for testing different DNS record types

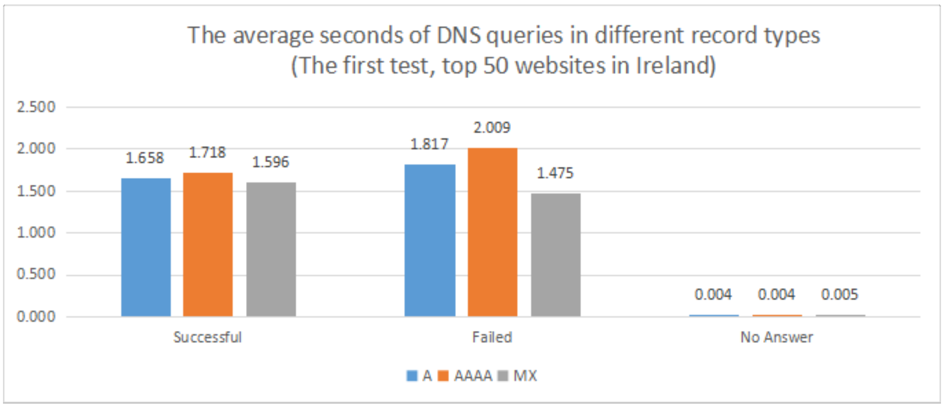


Figure 5.7: *The average seconds of DNS queries in different record types for the first test, the parameters are shown in Table 5.6*

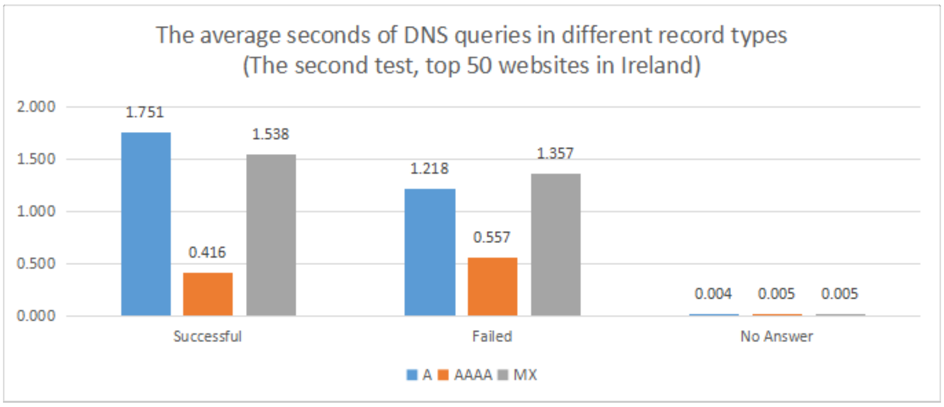


Figure 5.8: *The average seconds of DNS queries in different record types for the second test, the parameters are shown in Table 5.6*

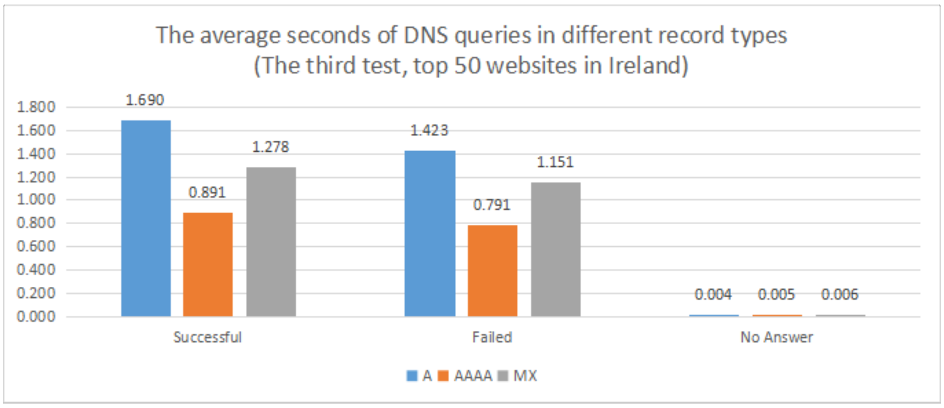


Figure 5.9: *The average seconds of DNS queries in different record types for the third test, the parameters are shown in Table 5.6*

The figures displayed that there was no significant difference among A, AAAA and MX in those 3 tests. AAAA had the lowest latency in the second and third tests, but it was highest in the first test. Thus, it was possible that the speed of computing or the network rose suddenly while testing AAAA in the second and third tests.

Another noticeable outcome was that the average times of “No Answer” were very short. They were about from 0.004 to 0.006 second. The reason may be the DNS queries with “No Answer” did not be processed by the DNS server. The DNS server just responded errors rapidly after receiving those DNS queries.

Overall, the DoH service was capable to carry out the DNS queries with different query record types. Furthermore, the gaps of their performances were not huge. The results also proved that the performance of DoH service was unstable.

Chapter 6

Other concerns

6.1 The concern about DDOS attacks

DDOS is also the important issue for building DNS server [64].

There are 2 sorts of DNS queries, recursive and iterative. At the beginning, users send queries to recursive servers, when recursive DNS servers receive requests, if they do not have the matched IP addresses, then recursive DNS servers can help users to ask authoritative DNS servers for getting IP addresses, then return results to users, that is the recursive query.

As for the iterative query, when authoritative DNS servers receive the queries from recursive DNS servers, if they do not have the matched IP addresses, they will give recursive servers the IP addresses of other authoritative DNS servers for querying, then recursive servers will ask other authoritative DNS servers, this type of querying is the iterative query [65].

However, the recursive queries may cause DDOS attacks. The content of packet could be faked, the IP address of a sender can be changed to be the IP address of the victim. In case thousands of computers send recursive queries to DNS servers, and all IPs of sources are changed to be the IP of a victim, then those DNS servers will send thousands of responses to that victim. After that, the traffic in the victim would be too high then cause some problems [7]. This type of DDOS attack is called DNS amplification attack [64].

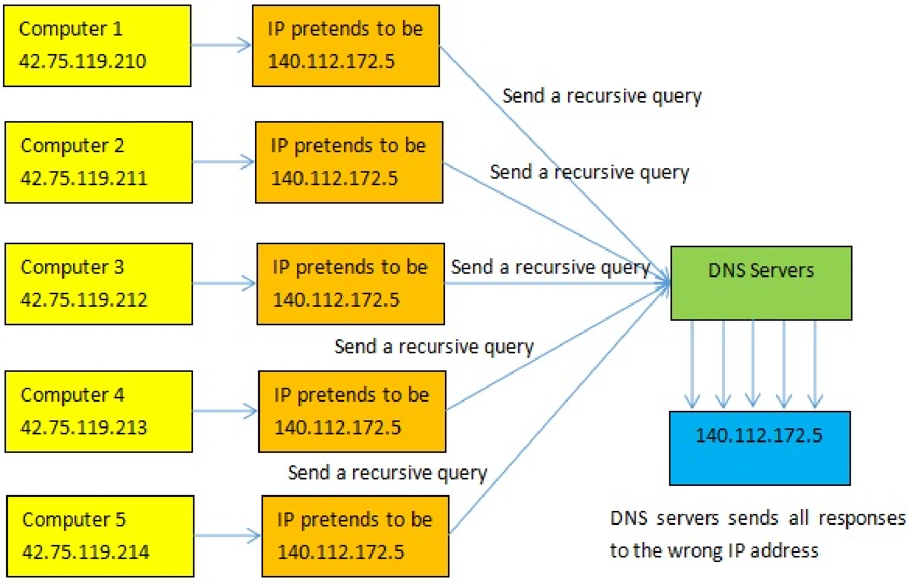


Figure 6.1: *The DDOS attack in recursive DNS queries [7]*

Thus, restricting DNS queries may be the ideal method to prevent DNS amplification attacks, the implementation is to disable the recursion for everyone, only local queries are allowed to be processed [66].

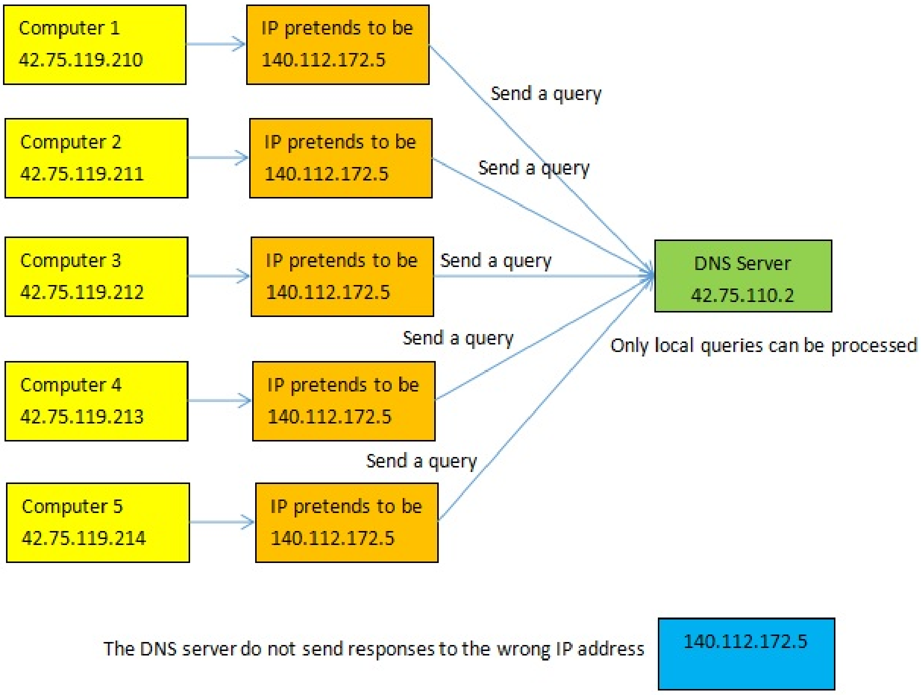
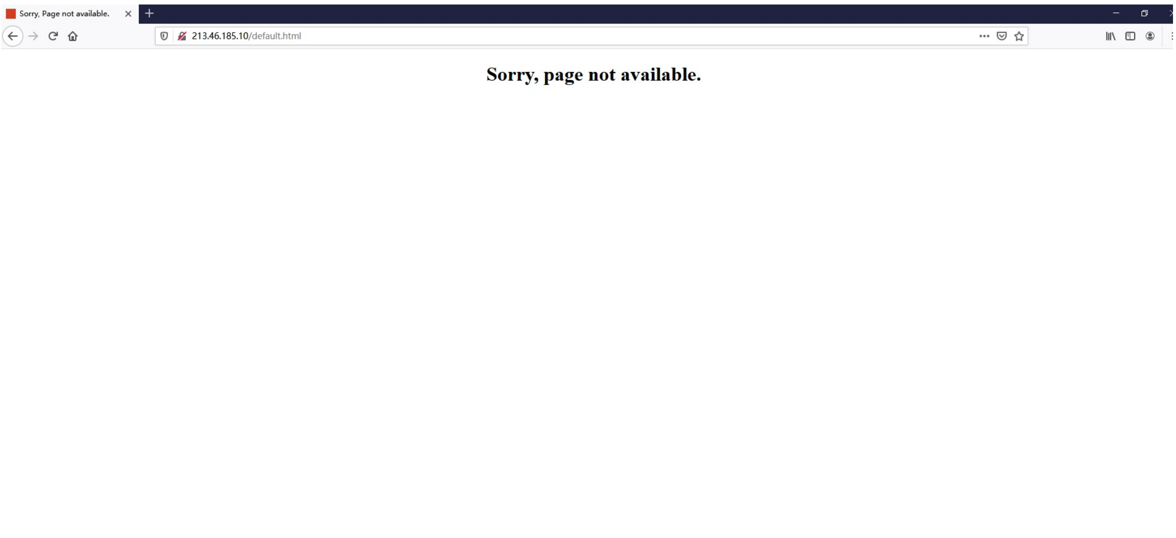


Figure 6.2: *Restricting DNS queries to prevent DNS amplification attacks [7]*

6.2 The concern about the policy

The Irish government has banned some websites for some reasons [67]. The problem is that users may utilize DoH to bypass the censorship from the government to browse the banned websites [68] [69], because the DNS queries are encrypted.

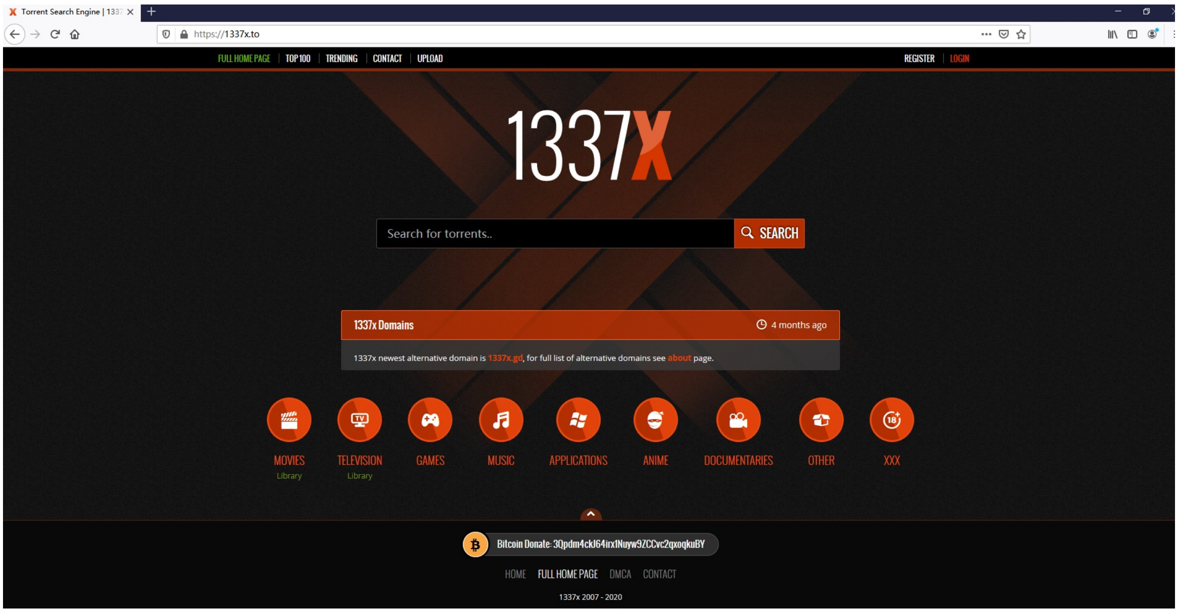
The study did a simple test. “1337x.to” [70] is one of the banned website in the Republic of Ireland. The reason is this website has the issue of copyright infringement. The researcher could not browse the website in Ireland at the beginning. The screenshot of the Firefox at that moment is displayed in Fig. 6.3.



Sorry, page not available.

Figure 6.3: *Firefox with default setting can not browse a banned website.*

After the researcher enabled the TRR function, the content of “1337x.to” was displayed in Fixfox, which means the censorship may not work for DoH users. The screenshot is shown in Fig. 6.4.



1337x Domains 4 months ago

1337x newest alternative domain is 1337x.gd, for full list of alternative domains see about page.

Bitcoin Donate: 3Qpdm4ckJ64irx1Nuyw9ZCCvc2qxoqkuBY

1337x 2007 - 2020

Figure 6.4: *Firefox can browse the banned website after enabling TRR.*

If users need to enable the DoH service manually, then this problem could be smaller. Nevertheless, both Mozilla and Google had plans to make DoH as default query, then people can just browse banned websites directly without any change. In this case, censorship is useless anymore if the Irish government does not adopt other technologies to block banned websites.

6.3 The concern about the latency

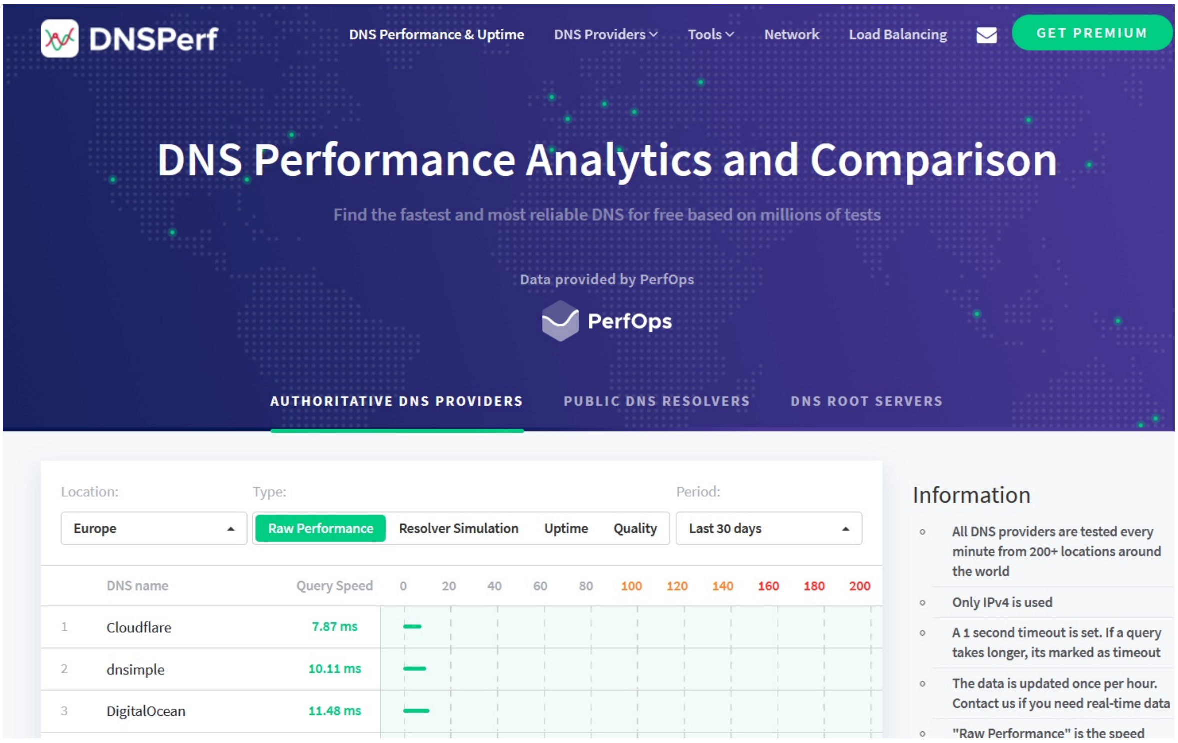
The computing of a data center can be increased, but the light speed is limited, therefore the quality of the DNS query would be worse if the DNS server is too far from the client [71].

The study assumes that the optical fiber is used to be the tool for transmitting signal, the latency will be about 5 microseconds per kilometers [72]. If the latency is including the time of the response, then the latency will be around 10 microseconds per kilometers.

Next discussion is talking about how much latency is acceptable? The acceptable range of everyone is different, but the current quality of DNS servers can be the reference to evaluate the acceptable latency.

According to the website DNSPerf, the DNS provider with the lowest latency is cloudflare in Europe, the latency is 7.97 ms [73]. The screenshot is displayed in Fig. 6.5. Thus, this study takes 8 ms to be the minimum requirement of the latency.

The distances of some far places from Dublin can reach about 394 kilometers. The distances are counted by Google Map in Fig. 6.6 and Fig. 6.7. The path bypasses the UK part in Northern Ireland.



DNS Performance Analytics and Comparison

Find the fastest and most reliable DNS for free based on millions of tests

Data provided by PerfOps

Location: Europe

Type: Raw Performance

Period: Last 30 days

	DNS name	Query Speed	0	20	40	60	80	100	120	140	160	180	200
1	Cloudflare	7.87 ms											
2	dnsimple	10.11 ms											
3	DigitalOcean	11.48 ms											

Information

- All DNS providers are tested every minute from 200+ locations around the world
- Only IPv4 is used
- A 1 second timeout is set. If a query takes longer, its marked as timeout
- The data is updated once per hour. Contact us if you need real-time data
- "Raw Performance" is the speed

Figure 6.5: *The ranking of DNS providers by latency in Europe.*

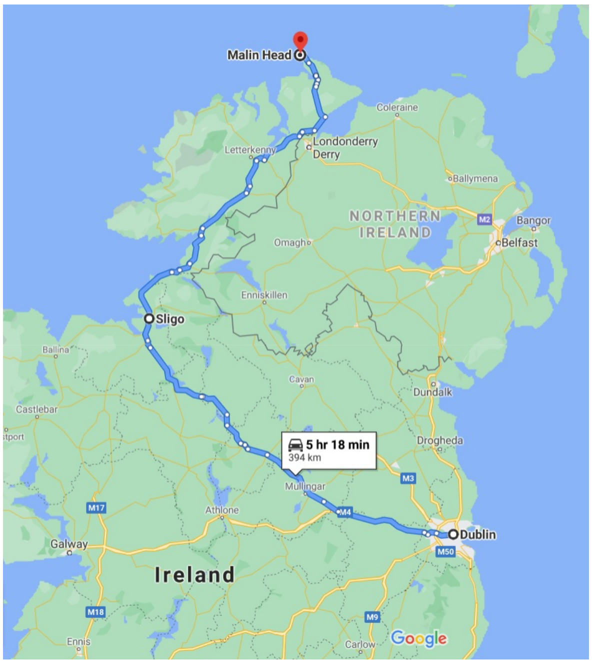


Figure 6.6: *The distance of a very far place in the north from Dublin.*

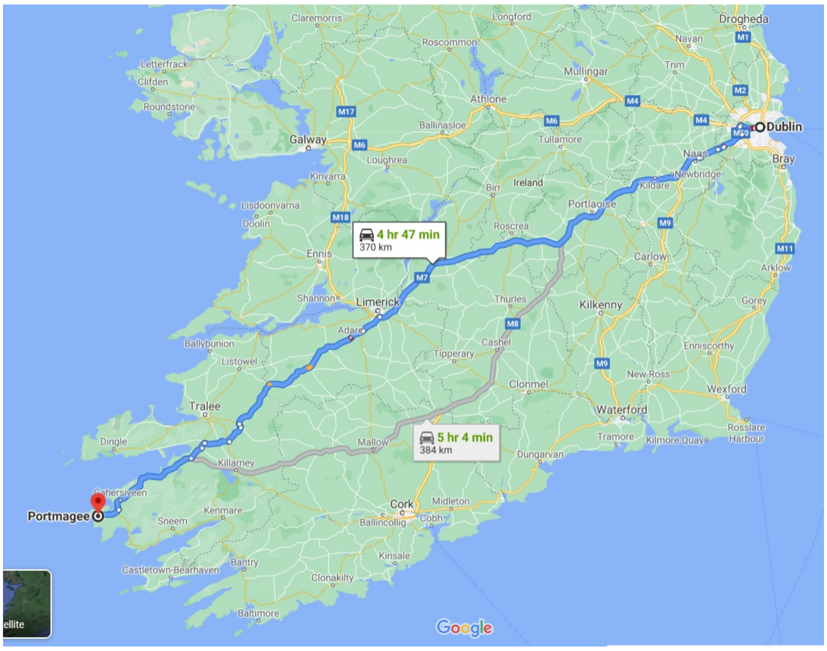


Figure 6.7: *The distance of a very far place in the south from Dublin.*

The distance 394 kilometers could cause approximately 4 ms for a DNS query [74], which means the latency of every place in Ireland is possible to be lower than 8 ms if the server is located in Dublin. Thus, the latency should not be a severe problem for building the DNS server in Ireland, because Ireland is not big enough to require many DNS servers to reduce the latency.

Even though the latency should be the problem, but the amplifiers and regenerators need to be deployed because the distance is longer than 100 kilometers if using optical fiber to transmit the data.

Chapter 7

Overall design

DoH service would raise privacy on the Internet. Meanwhile, the concept of the TRR program could further strengthen privacy on the basis of DoH. The idea of the TRR program is fine but the situation of the Republic of Ireland is necessary to be considered if the Irish DNS provider plan to join the TRR program. Hence, this chapter is going to make a technical conclusion for the implementation of the TRR program.

Previous chapters has discussed about the background of TRR, the Irish DNS traffic, the required software for building a recursive resolver, the performance of a recursive resolver, and the concern about DDOS attacks, the policy and the latency. After that, the study concludes the 6 conditions which need to be satisfied if building recursive resolvers for TRR in Ireland.

The first condition: Recursive resolvers have to be supervised. The data must be deleted after a certain time, it is visible and can not be changed. That is the policy of TRR, to make those recursive resolvers trusted.

The solution is that the software used for building the DNS server should be easy to construct a completed system to manage the data and provide the data to others for checking.

PowerDNS may be an ideal DNS software because PowerDNS uses MySQL to be the database, and it has its own graphic interface to control the recursive resolver. The recursive resolver provider may also utilize MySQL to design another system for supervision.

However, PowerDNS is just a choice, perhaps other DNS software may also provide the graphic interface and adopt the relational database as well, maybe some of them have more advanced functions. For some DNS software such as BIND or Unbound, they are also able to accomplish the requirement of the policy of TRR, but the provider may need to put more effort or time on designing the required system.

The second condition: Recursive resolvers must provide DoH service. TRR adopts DoH to encrypt the query, thus the DoH service is mandatory.

Many DNS software are able to provide DoH service, including BIND, Unbound, PowerDNS. The HTTP server is required by DoH service as well, the Linux users can just use Nginx or other software. However, providing DoH service should not be the big problem.

The third condition: Recursive resolvers should possess sufficient performance to deal with the DNS traffic in peak time.

Chapter 3 had a discussion about the Irish DNS traffic. The estimation of DNS queries per second in Ireland is possible to be 4,494 or 9,149. The number of queries in Ireland is not very high if compare to other countries.

However, the DNS provider also need to consider the DNS traffic in the future, because the DNS traffic should rise a lot in Ireland in next 5 years. The reason is the trend of population in Ireland in recently years is growing up [39], thus this study supposes that the Irish population will be higher than the current population in next 5 years, and the DNS queries will be more as well.

Furthermore, some events could cause a higher usage of the Internet. For example, the virus COVID-19 made the Internet traffic higher [75] [76]. Those factors and their effects are hard to be predicted and evaluated.

Thus, the DNS server should remain some extra computing performance to deal with the possible higher DNS traffic in the near future.

Accord to the experiment in chapter 5, a DNS server may process 10 queries per second without using cache. The DNS server should be installed in a data center. The data center could be tiny or giant. In some estimations, a data center would contain 15000 to 80000 servers servers [77] [78] [79] [80].

On the other hand, the server machine is more suitable than a personal computer for processing the task of a server, because a server machine contains more processor cores [81]. Thus the performance of a server should be better than the results in the experiment in this study. If the DNS provider takes a data center with 15000 servers, it should be able to compute at least 150000 DNS queries for one second. This number is pretty enough to deal with the DNS queries of the national scale in Ireland. The minimum number of server machines to handle the current DNS traffic of Irish nation scale is probably around 1000 if all servers focus on the computing of DNS queries(1 server can deal with at least 10 DNS queries per second, this study estimates that there are almost 10000 DNS queries per second in Ireland).

Even though the DNS queries is going to increase in the future, the computing of a data center is still capable to process that. Thus, the performance of the DNS server should not be a problem as well, if the DNS provider owns a data center.

Nevertheless, the DNS provider still needs to consider the highly intensive DNS queries in an extremely short time. The results of the experiment in chapter 5 revealed that the DoH recursive resolver may encounter some problems to process intensive DNS queries.

The forth condition: It is necessary to try to reduce DDOS attacks.

The setting of the DNS software can control the query, to decide which IP addresses can be accepted or not accepted. Some of DDOS attacks utilize DNS servers to attack others. If the DNS server only allows the local users to send queries to it, then the outside users can not use that DNS server to do DDOS attacks.

For example, if Irish DNS servers only allow the people who live in the Republic of

Ireland to query, then the clients from other countries can not use Irish DNS servers to execute DDOS attacks.

The fifth condition: The issue of bypassing censorship in using DoH needs to be discussed and resolved.

The study recommends the Irish government to use another method to ban websites because DoH can bypass the current censorship. On the other hand, DoH will be the default setting soon in some major browsers according to the plans of Google and Mozilla. Thus, it is necessary to change the method of banning websites if the government really want to ban them. The current method will be outdated. Otherwise, everyone is able to browse banned websites.

The six condition: The latency of the DNS query should be lower than 8 ms.

The section "The concern about the latency" mentioned that Ireland is not a big country, the farthest place from Dublin maybe just 400 kilometers. 400 kilometers merely causes around 4 ms to latency. Thus, the latency could be possible to be controlled under 8 ms in the whole of Ireland. The latency should not be a severe issue too.

Apart from those conditions, this study recommends that the number of the DoH DNS servers should be 2. The first one is located in the biggest Irish city Dublin, and the second one is in the second biggest city Cork. The location of Dublin is the east of Ireland, and the the location of Cork is in the south-west of Ireland, then they can cover the different areas.

Even if one DNS server is capable to deal with the whole DNS queries and the latency could be lower than 8 ms in Ireland, but 2 DNS servers are more reliable. In case one DNS server is failed, then the other one can be the spare DNS server to take over its job.

Another recommendation is enabling the JSON query, but that is not very important. The DNS server of Cloudflare supports the JSON query, this function is beneficial for some developers because many applications adopt JSON to be the data format, and it is easier to be understood by developers if compare to the Wireformat query. If the DNS server supports the JSON query, then it is more convenient for those developers.

However, this study just utilized the personal computer and the data from some authoritative DNS servers to emulate the possible results. It is necessary to take the data from some real recursive resolvers to analyze the DNS traffic and the performance of a recursive resolver if the DNS provider requires more precise analysis.

Bibliography

[1] pmtk.medium.com, “Compare dnssec, dnscrypt, dns over tls, dns over https.” [Online]. Available: https://pmtk.medium.com/%E5%AF%B9%E6%AF%944%E7%A7%8D%E5%BC%BA%E5%8C%96%E5%9F%9F%E5%90%8D%E5%AE%89%E5%85%A8%E7%9A%84%E5%8D%8F%E8%AE%AE-dnssec-dnscrypt-dns-over-tls-dns-over-https-2b6faca60892.

[2] root-servers.org, “root-servers.org.” [Online]. Available: https://root-servers.org/.

[3] Akamai.com, “Dns trends and traffic.” [Online]. Available: https://www.akamai.com/de/de/why-akamai/dns-trends-and-traffic.jsp.

[4] AMS-IX, “Total traffic statistics(amsterdam).” [Online]. Available: https://stats.ams-ix.net/index.html.

[5] Cloudflare, “What is a dns root server?.” [Online]. Available: https://www.cloudflare.com/learning/dns/glossary/dns-root-server/.

[6] stats.dns.icann.org, “stats.dns.icann.org.” [Online]. Available: https://stats.dns.icann.org/.

[7] Fashosts Internet, “What is recursive dns and why is it not recommended for most server owners?.” [Online]. Available: https://www.youtube.com/watch?v=W3wXkHAv3qo.

[8] J. Peters, “What is dns, how it works + vulnerabilities.” [Online]. Available: https://www.varonis.com/blog/what-is-dns/.

[9] Wikipedia, “Domain name system security extensions.” [Online]. Available: https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions.

[10] Wikipedia, “Dnscrypt.” [Online]. Available: https://en.wikipedia.org/wiki/DNSCrypt.

[11] Wikipedia, “Dns over tls.” [Online]. Available: https://en.wikipedia.org/wiki/DNS_over_TLS.

[12] Wikipedia, “Dns over https.” [Online]. Available: https://en.wikipedia.org/wiki/DNS_over_HTTPS.

[13] Wikipedia, “Ipv4.” [Online]. Available: https://en.wikipedia.org/wiki/IPv4.

[14] Wikipedia, “Ipv6.” [Online]. Available: https://en.wikipedia.org/wiki/IPv6.

[15] Wikipedia, “Domain name.” [Online]. Available: https://en.wikipedia.org/wiki/Domain_name.

[16] DNS Made Easy, “Authoritative vs. recursive dns servers: What’s the difference?.” [Online]. Available: https://medium.com/@DNSMadeEasyBlog/authoritative-vs-recursive-dns-servers-whats-the-difference-d0e5821c7617.

[17] Wikipedia, “Request for comments.” [Online]. Available: https://en.wikipedia.org/wiki/Request_for_Comments.

[18] Wikipedia, “Internet engineering task force.” [Online]. Available: https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force.

[19] S. Bortzmeyer, “Dns privacy considerations.” [Online]. Available: https://tools.ietf.org/html/rfc7626, August 2015.

[20] E. T. Wicinski, “Dns privacy considerations draft-ietf-dprive-rfc7626-bis-08.” [Online]. Available: https://tools.ietf.org/html/draft-ietf-dprive-rfc7626-bis-08, October 2020.

[21] Wikipedia, “Public recursive name server.” [Online]. Available: https://en.wikipedia.org/wiki/Public_recursive_name_server.

[22] The DNS Institute, “Disadvantages of dnssec.” [Online]. Available: `https://dnsinstitute.com/documentation/dnssec-guide/ch06s06.html`.

[23] IONOS, “Dns over tls: an improved security concept.” [Online]. Available: `https://www.ionos.com/digitalguide/server/security/dns-over-tls/`.

[24] IETF, “Dns resolver discovery protocol (drdp).” [Online]. Available: `https://tools.ietf.org/id/draft-mglt-add-rdp-02.html`, May 2020.

[25] Mozilla, “Trusted recursive resolver.” [Online]. Available: `https://wiki.mozilla.org/Trusted_Recursive_Resolver`.

[26] Mozilla, “Comcast’s xfinity internet service joins firefox’s trusted recursive resolver program.” [Online]. Available: `https://blog.mozilla.org/blog/2020/06/25/comcasts-xfinity-internet-service-joins-firefoxs-trusted-recursive-resolver-` June 2020.

[27] M. Brinkmann, “Comcast is the first isp that joins firefox’s trusted recursive resolver program.” [Online]. Available: `https://www.ghacks.net/2020/06/26/comcast-is-the-first-isp-that-joins-firefoxs-trusted-recursive-resolver-prog` June 2020.

[28] L. Abrams, “Mozilla enables dns-over-https by default for all usa users.” [Online]. Available: `https://www.bleepingcomputer.com/news/software/mozilla-enables-dns-over-https-by-default-for-all-usa-users/`.

[29] S. Gatlan, “Firefox 77.0.1 released to prevent ddosing doh dns providers.” [Online]. Available: `https://www.bleepingcomputer.com/news/security/firefox-7701-released-to-prevent-ddosing-doh-dns-providers/`.

[30] C. Cimpanu, “Google to run dns-over-https (doh) experiment in chrome.” [Online]. Available: `https://www.zdnet.com/article/google-to-run-dns-over-https-doh-experiment-in-chrome/`.

[31] M. Jackson, “Google chrome joins firefox – soft defaults to dns over https.” [Online]. Available: `https://www.ispreview.co.uk/index.php/2020/05/google-chrome-joins-firefox-soft-defaults-to-dns-over-https.html`.

[32] J. E. Dunn, “Chrome 83 adds dns-over-https support and privacy tweaks.” [Online]. Available: `https://nakedsecurity.sophos.com/2020/05/21/chrome-83-adds-dns-over-https-support-and-privacy-tweaks/`.

[33] Winaero, “Enable dns over https in opera (doh).” [Online]. Available: `https://winaero.com/enable-dns-over-https-in-opera-doh/`.

[34] C. Cimpanu, “Here’s how to enable doh in each browser, isps be damned.” [Online]. Available: `https://www.zdnet.com/article/dns-over-https-will-eventually-roll-out-in-all-major-browsers-despite-isp-op`

[35] Wikipedia, “Root name server.” [Online]. Available: https://en.wikipedia.org/wiki/Root name server.

[36] L. Bellon, “What is the difference between authoritative and recursive dns nameservers?.” [Online]. Available: `https://umbrella.cisco.com/blog/what-is-the-difference-between-authoritative-and-recursive-dns-nameservers`, June 2020.

[37] central statistics office (Ireland), “Information society statistics - households.” [Online]. Available: https://www.cso.ie/en/releasesandpublications/er/isshh/informationsocietystatistics-households2018/.

[38] J. Clement, “Global digital population as of july 2020.” [Online]. Available: https://www.statista.com/statistics/617136/digital-population-worldwide/.

[39] Worldometer, “Ireland population(live).” [Online]. Available: https://www.worldometers.info/world-population/ireland-population/.

[40] N. Cumins, “Avoiding the internet rush hour.” [Online]. Available: https://broadbanddeals.co.uk/avoiding-the-internet-rush-hour/.

[41] ix.br, “Selecione a localidade para ver as estatísticas de tráfego.” [Online]. Available: https://ix.br/trafego/agregado/sp.

[42] federal communications commission, “Measuring broadband america-july 2012.” [Online]. Available: https://www.fcc.gov/reports-research/reports/measuring-broadband-america/measuring-broadband-america-july-2012.

[43] DE-CIX, “Traffic statistics(berlin).” [Online]. Available: https://www.bcix.de/bcix/traffic/.

[44] Wikipedia, “Melbourne.” [Online]. Available: https://en.wikipedia.org/wiki/Melbourne.

[45] Wikipedia, “Comparison of dns server software.” [Online]. Available: https://en.wikipedia.org/wiki/Comparison of DNS server software.

[46] K. John, “Bind vs dnsmasq vs powerdns vs unbound.” [Online]. Available: `https://computingforgeeks.com/bind-vs-dnsmasq-vs-powerdns-vs-unbound/`.

[47] TINYDNS, “Compare the different dns servers: Which one is right for you?.” [Online]. Available: `https://tinydns.org/compare-different-dns-servers/`.

[48] Wikipedia, “Nsd.” [Online]. Available: https://en.wikipedia.org/wiki/NSD.

[49] NLNETLABS, “Unbound.” [Online]. Available: `https://nlnetlabs.nl/projects/unbound/about/`.

[50] NS1, “Bind dns: Pros, cons and alternatives.” [Online]. Available: `https://ns1.com/resources/bind-dns-pros-cons-and-alternatives`.

[51] PowerDNS, “About powerdns.” [Online]. Available: `https://www.powerdns.com/about.html`.

[52] Loull, “Dns resources.” [Online]. Available: https://www.cnblogs.com/549294286/p/5200255.

[53] ISHM, “Building dns over https server on centos 7.” [Online]. Available: https://ishm.idv.tw/?p=481.

[54] Facebookexperimental, “Dns over https proxy.” [Online]. Available: `https://github.com/facebookexperimental/doh-proxy`.

[55] NGINX, “Welcome to niginx wiki!.” [Online]. Available: https://www.nginx.com/resources/wiki/.

[56] W. T. Hamza Boulakhrif, Yuri Schaeffer, "Analysis of dns resolver performance measurements," tech. rep., University of Amsterdam, July 2015.

[57] P. S. Austin Hounsel, Kevin Borgolte, "Comparing the effects of dns, dot, and doh on web performance," tech. rep., Princeton University, University of Chicago, February 2020.

[58] Alexa, "Top sites in ireland." [Online]. Available: `https://www.alexa.com/topsites/countries/IE`.

[59] Sciencebuddies.org, "Variables in your science fair project." [Online]. Available: `https://www.sciencebuddies.org/science-fair-projects/science-fair/variables`.

[60] Cloudflare, "Using dns wireformat." [Online]. Available: `https://developers.cloudflare.com/1.1.1.1/dns-over-https/wireformat`.

[61] JSON.ORG, "Introducing json." [Online]. Available: `https://www.json.org/json-en.html`.

[62] Cloudflare, "Using json." [Online]. Available: `https://developers.cloudflare.com/1.1.1.1/dns-over-https/json-format`.

[63] JH Software, "Dns record types." [Online]. Available: `https://simpledns.plus/help/dns-record-types`.

[64] Imperva, "Dns amplification." [Online]. Available: `https://www.imperva.com/learn/ddos/dns-amplification/`.

[65] Cloudflare, "What is recursive dns?." [Online]. Available: `https://www.cloudflare.com/learning/dns/what-is-recursive-dns/`.

[66] Fashosts Internet, "What is recursive dns and why is it not recommended?." [Online]. Available: `https://help.fasthosts.co.uk/app/answers/detail/a_id/1276`.

[67] Wikipedia, "Internet censorship in the republic of ireland." [Online]. Available: `https://en.wikipedia.org/wiki/Internet_censorship_in_the_Republic_of_Ireland`.

[68] K. Leuven, "Does doh imply privacy?." [Online]. Available: https://www.esat.kuleuven.be/cosic/blog/does-doh-imply-privacy/.

[69] InCampass, "Understanding doh and dot." [Online]. Available: https://incompass.netstar-inc.com/blog/202.

[70] Wikipedia, "1337x." [Online]. Available: https://en.wikipedia.org/wiki/1337x.

[71] K. Miller, "Calculating optical fiber latency." [Online]. Available: https://www.m2optics.com/blog/bid/70587/calculating-optical-fiber-latency, January 2012.

[72] Rogerluethy, "What is latency?." [Online]. Available: https://rogerluethy.wordpress.com/2011/09/01/what-is-latency/, September 2011.

[73] DNSPerf, "Dns performance analytics and comparison." [Online]. Available: https://www.dnsperf.com/#!dns-providers,Europe.

[74] Timbercon, "Time delay of light in fiber calculator." [Online]. Available: https://www.timbercon.com/resources/calculators/time-delay-of-light-in-fiber-calculator/.

[75] N. P. Ella Koeze, "The virus changed the way we internet." [Online]. Available: https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html, April 2020.

[76] J. Quann, "Covid-19: Almost 80% of irish people reading or downloading online news." [Online]. Available: https://www.newstalk.com/news/covid-19-almost-80-irish-people-reading-downloading-online-news-1033425, June 2020.

[77] CERN, "Cern data centre." [Online]. Available: https://home.cern/science/computing/data-centre.

[78] P. Johnson, "With the public clouds of amazon, microsoft and google, big data is the proverbial big deal." [Online]. Available: https://www.forbes.com/sites/johnsonpierr/2017/06/15/

with-the-public-clouds-of-amazon-microsoft-and-google-big-data-is-the-prover June 2017.

[79] K. Pertsev, "How many servers does a typical data center house?." [Online]. Available: https://www.quora.com/How-many-servers-does-a-typical-data-center-house, April 2013.

[80] R. Solutions, "How many servers does a data center have?." [Online]. Available: https://www.racksolutions.com/news/blog/how-many-servers-does-a-data-center-have/, September 2020.

[81] Techquickie, "Servers vs desktop pcs as fast as possible." [Online]. Available: https://www.youtube.com/watch?v=ByI1PHMcPJQ, June 2014.

Appendices

Appendix 1: The testing program(Python code)

Appendix 2: The statistic generated by the testing program(CSV file)

Appendix 3: The records generated by the testing program(CSV files in a RAR file)

Appendix 4: The list of the top 50 websites in Ireland(CSV file)