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 16, 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 16, 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. He spent much time on that. The course director John Dingliana, he helped me in my appeal as well and allowed me to have more time to finish my dissertation. I appreciate all of your efforts for me.

I also thank other classmates and friends who have ever helped me during studying at Trinity College Dublin.

I can not accomplish this dissertation without any of you.

<div align="right">TUNG-TE LIN</div>

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 published the project Trusted Recursive Resolver(TRR) to enhance the privacy of users. Thus, this study researches the requirement and effect of deploying TRR servers in Ireland.

This study analyzes the possible Domain Name System(DNS) traffic in Ireland by using the data from some root servers. Then, the researcher installs a private DNS server with the DNS over HTTPS(DoH) service to test the performance because TRR requires DoH for implementation.

Moreover, the researcher discusses various considerations to implement TRR in Ireland, such as required software, Irish policy, latency, and the regulation of TRR.

Finally, the study introduces a technical plan for building TRR servers in Ireland. The plan includes the required number and management of TRR servers, and the conditions that the DNS provider needs to consider.

Summary

Trusted Recursive Resolver(TRR) is the project to enhance the protection of privacy for DNS queries. This study discusses the feasibility of implementation of TRR in Ireland from different aspects. Those aspects include the background of TRR, the required software, the policy in Ireland, the possible latency in Ireland, the possible Domain Name System(DNS) traffic in Ireland, the consideration of Distributed Denial-of-service(DDoS) attacks, and the performance of a DNS server with DNS over HTTPS(DoH).

The study explains the targets of TRR in the background of TRR. TRR has 2 targets, the first one is using DoH to encrypt DNS queries because The traditional DNS does not encrypt DNS queries. Moreover, DoH has higher protection of privacy in comparison to DNS over TLS(DoT), DNSEncrypt, and Name System Security Extensions(DNSSEC). The second target is supervising DNS servers, because DoH service does not include the supervision of DNS servers, therefore the data is possible to be abused by DNS providers.

The required software for building a DNS server include DNS software, DoH tools, and an HTTPS server. The ideal DNS software should adopt a fine database to make management and supervision easily, such as PowerDNS.

The study has designed an experiment to understand the performance of a DNS

server with the DoH service, but the results were not excellent, and other studies also mentioned that the performance of DoH is lower than the traditional DNS. Fortunately, Ireland is not a big nation and the population is not very high when compared to other countries. Therefore, the DNS traffic and latency of DNS queries could be very low. One DNS server in a data center is sufficient to satisfy the requirement of Irish national scale. However, two DNS servers are recommended because one DNS server could be the spare one to the other DNS server. The locations are suggested in Dublin and Cork, respectively.

On the other hand, the Irish government has banned some websites, but people are able to browse them while enabling DoH. Thus, the Irish government may need another method to ban websites, for example, using deep packet inspection. As for DDoS attacks, the administrator can reduce some DDoS attacks by setting the configuration.

Overall, building DNS servers with the DoH service for the TRR project is feasible in Ireland, and it would be beneficial for protecting the privacy of Irish citizens.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

The browser company Mozilla plans to promote the project Trusted Recursive Resolver(TRR) to provide better privacy compared to using traditional Domain Name Servers(DNS) [9]. This paper is going to analyze how the TRR project 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 potential privacy implications that may arise from using DNS servers. Next, it describes the solutions for dealing with the problem of privacy so far, including Domain Name System Security Extensions(DNSSEC) [10], DNSCrypt [11], DNS over TLS(DoT) [12], and DNS over HTTPS(DoH) [13]. 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 the TRR project.

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 a method to estimate the DNS traffic in Ireland.

Chapter 4 discusses the required software. It discusses the software requirements of a DNS provider when installing a DoH server, and what applications exist in the market for each kind so far. Furthermore, this chapter makes a comparison among those software.

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

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

Finally, chapter 7 "Overall Design" concludes the discussions from chapter 2 to chapter 6. This chapter also lists some conditions for resolving the possible issues that may occur if the TRR project 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) [9] is a system which converts domain names to Internet
Protocol(IP) addresses. Machines need the IP address to determine the location of
another machine [14] [15], not the domain name [16]. 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 responds with the IP address of the domain name "104.16.204.58" to the browser.
Finally, the browser is able to connect to the server of "www.dcard.tw" by using its IP
"104.16.204.58".

Moreover, there are 2 kinds of DNS servers: Recursive resolvers and authoritative
DNS servers [17]. 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 the corresponding 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 the recursive resolver for users' queries, and that the lower level authoritative DNS server may have the IP address that users need. In that case, a authoritative DNS server does not need to store the entire IP addresses and domain names of the Internet, the workload can be divided. The levels of authoritative DNS servers are shown in Fig. 2.1.
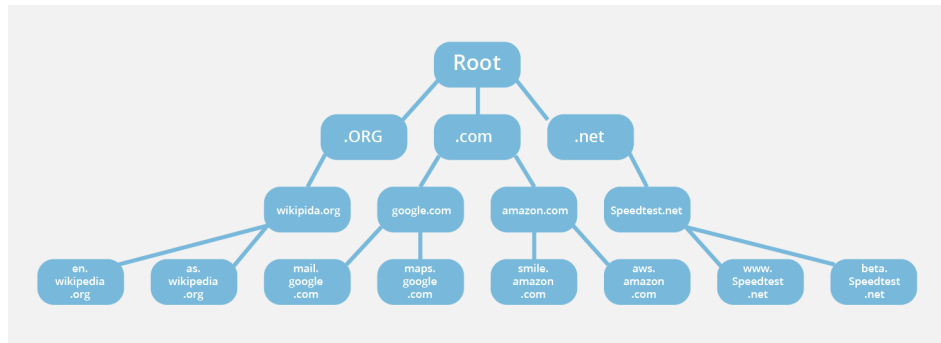
Figure 2.1: *Levels of authoritative DNS servers [5].*

The traditional DNS does not encrypt DNS queries. Moreover, it uses port 53. Thus, it has the alias named Do53 [18]. However, this paper still adopts "traditional DNS" to be its name in the following chapters and sections.

2.2 The problem of privacy

Request For Comments(RFC) [19] is the publication which is managed by Internet Engineering Task Force(IETF). IETF is the organization to design the standard of Internet [20].
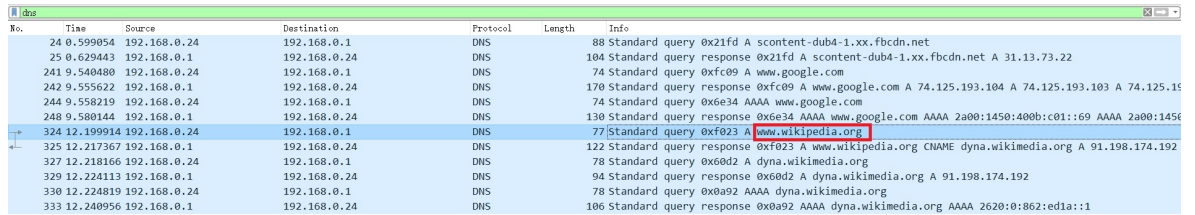
RFC7626 [21] and its draft [22] discussed the problem of privacy in using a DNS

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 searched 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, 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 [21].

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

To understand the situation clearly, this study did a test to get some traditional DNS packets 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.

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 websites.*

2.3 The solutions for privacy

According to the description of RFC7626 [21], revealing the content of DNS queries can cause severe privacy problems. People may not be willing to let others 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 [23].

The first solution is DNSSEC, it is not only the oldest but also the most popular solution among those 4 solutions [23]. It was created in 1997. The concept is making an extension of DNS to check the digital signature [10], 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 [24].

The second solution is DNSCrypt. Unlike other 3 solutions, it is a private standard and not managed by IETF. The owner is OpenDNS and it was announced in 2008. DNSCrypt does not use digital signatures, it uses cryptography to encrypt queries [25].

The biggest problem is that it is not proposed by IETF. Therefore it is just a private standard, not a public standard, then it is hard to be widely supported by application developers [26].

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 [12]. Compared to DNSSEC and DNSCrypt, it has a lot of advantages. For example, it does not need high performance to process the encryption. The packet is encrypted, thus it can prevent a man-in-the-middle attack(MITM) [27]. 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 [13]. DoH is similar to DoT, both DoH and DoT are utilizing TLS to be the tool to encrypt DNS queries. The difference 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 [1]. The models of DoT and DoH are shown in Table 2.1 and Table 2.2.

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].

In comparison to 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 just introduced recently, but many public recursive name servers already support it, such as Cloudflare, Google, AdGuard, NextDNS,OpenDNS and Quad9 [28]. On the other hand, it follows RFC 8484, thus it is a public standard, unlike DNSCrypt is a private standard.

Although DoH has resolved many problems that previous solutions may have, it still has some drawbacks. For example, the DNS queries hide in HTTPS traffic, therefore the visibility is low for monitoring, the administrator would be hard to control it [29]. Moreover, the DNS provider is still capable to see the contents of DNS queries [30].

Meanwhile, some reports mentioned that DoH may cause lower performance when compared to DoT or the traditional DNS [31] [32]. In addition, DoH may cause further deterioration to the performance of DoH in a network with poor conditions [31].

On the other hand, another paper indicated that the packets of DoH also have a larger size and higher number if compared to regular DNS packets [33]. It could be the cost of transmission. Nevertheless, that paper still suggested people use DoH instead of the traditional DNS because DoH can improve privacy a lot but the loss of performance is not significant, therefore it is worthy.

To figure out more detail about the performance of DoH, this paper designed its own experiment to use the DoH DNS server to collect some data to evaluate the functionality and performance. The steps and results are written in chapter 5.

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	Low visibility
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

Trusted Recursive Resolver(TRR) is a project to strengthen the protection for privacy, and it was introduced by Mozilla [34]. Mozilla called TRR as a program, but this study prefers to describe TRR as a project because some people may misunderstand TRR as a software program if we describe TRR as a program.

As RFC7626 mentioned [21], the personal data could be revealed in the DNS traffic

or DNS servers. About the DNS traffic, it can be encrypted by DoH or DoT. As for the DNS servers, it needs another means to resolve the problem of privacy.

In this background, the concept of TRR 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 project so far [35]. There are 3 regulations in the supervision to recursive resolvers in the TRR project [36].

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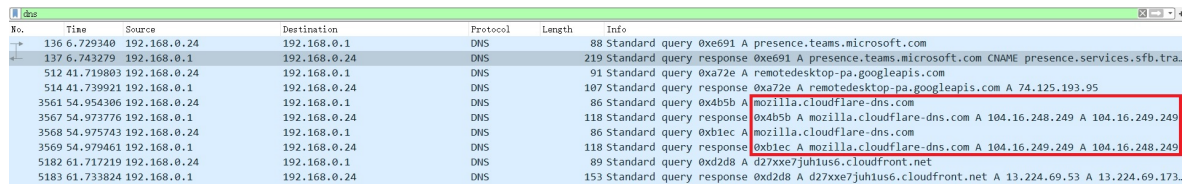
The second one, the data in recursive resolvers needs to be transparent. People have the right to understand how the data are stored and used.

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 project. 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 project.

The TRR project 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.

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 a few steps to enable it. The steps are shown in Fig. 2.4 and Fig. 2.5.
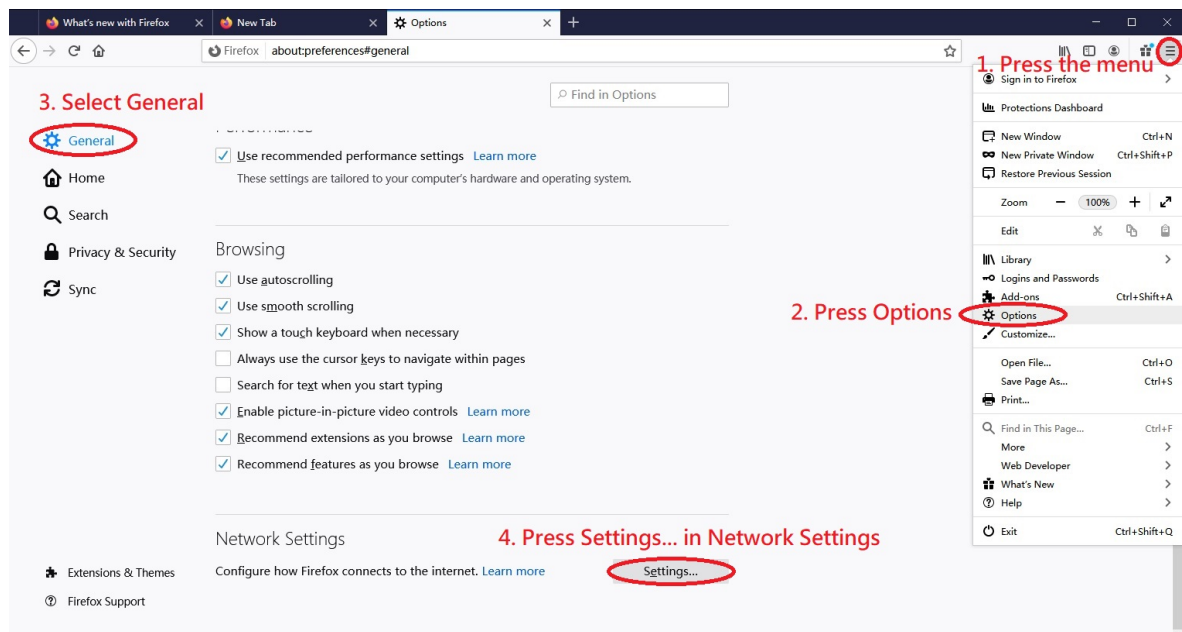
Figure 2.4: *The steps to enable TRR in Firefox - Part 1.*
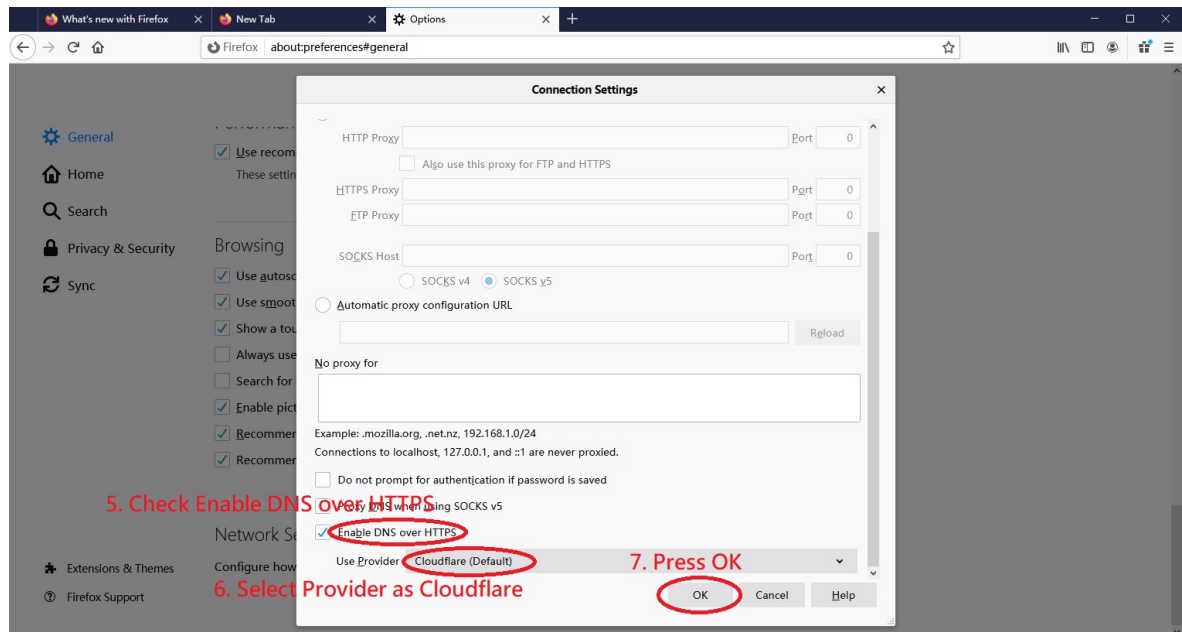
Figure 2.5: *The steps to enable TRR in Firefox - Part 2.*

Furthermore, Mozilla is also devoted to pushing TRR. In February 2020, Mozilla set TRR as the default setting of Firefox in the USA, which means Firefox users used the DoH service if they do not do any change [37].

However, this policy caused a severe problem, after the TRR function was set as the default setting in Firefox, the DNS provider NextDNS suffered a very high workload and struggled to handle the high traffic volume. It seemed 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 [38].

Hence, TRR only remained the default setting for 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, it is 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 too [39].

The difference is that the policy Google adopted is not TRR, because TRR is the unique project to Mozilla and its browser Firefox. The policy Google adopted is an 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 [40].

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. Contrarily, Firefox is more flexible, users are able to set their own DoH DNS servers in Firefox. Therefore, it is easy to test a private DoH DNS server [41].

The interface of the DoH setting in Chrome is shown in Fig. 2.6.
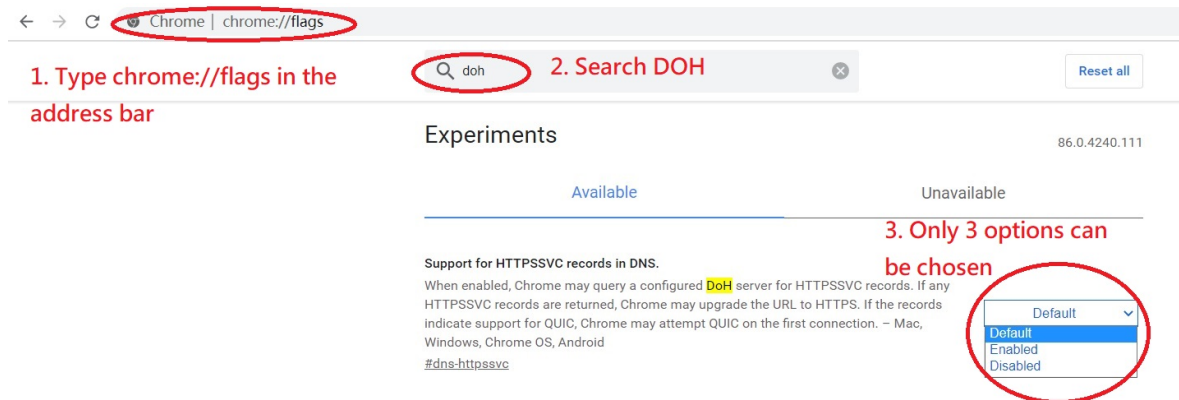
Figure 2.6: *DoH setting on Google Chrome.*

DoH is supported by not only Firefox and Chrome, but also other browsers, such as Opera [42], Microsoft Edge, and Vivaldi [43]. Every company or browser has its own plan to support DoH, those plans may be different and have their features, advantages, and disadvantages.

However, this study just focuses on the TRR project 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 of dealing 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 [2]. 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.
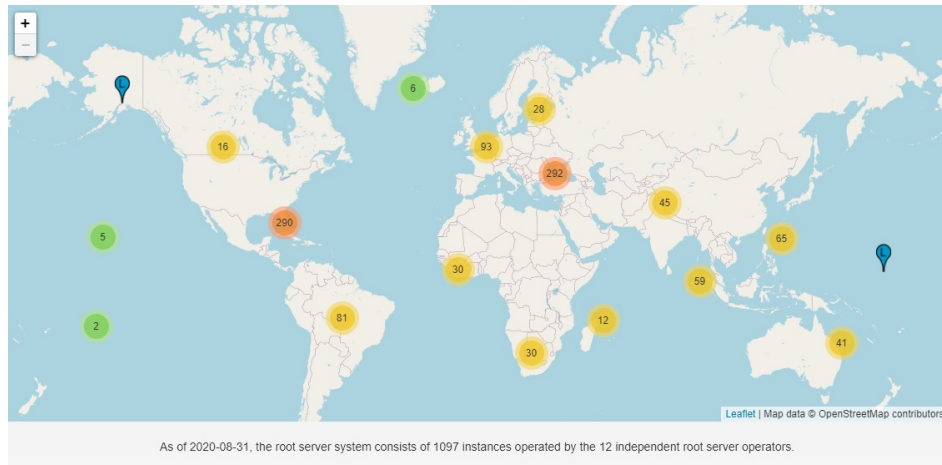
Figure 3.1: *The root servers in the world [2].*
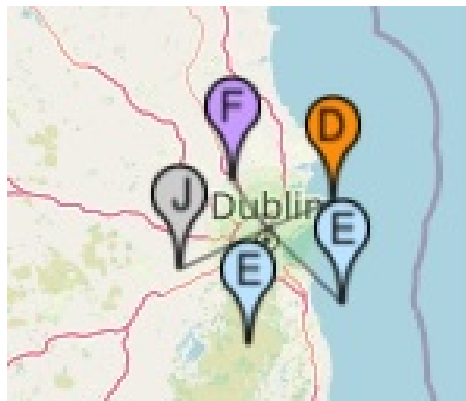
Figure 3.2: *The root servers in Dublin [2].*
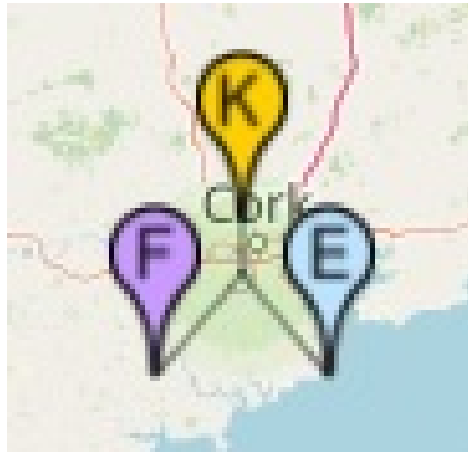
Figure 3.3: *The root servers in Cork [2].*

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

3.2   Estimation using data from Akamai

Although it is hard to collect the number of entire DNS queries in Ireland, the target of this study is to understand the performance requirements of a TRR server in Ireland. The number of DNS queries in a root server may help us to evaluate the required performance for a TRR server in Ireland. Those DNS queries are authoritative DNS queries because root servers are the highest level of authoritative DNS servers.

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 from Akamai.com to estimate the DNS traffic [3].

In the 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, the worldwide data of root server traffic can be used to estimate the Irish authoritative DNS traffic.

In a report from the Central Statistics Office of Ireland, it showed that there were 89% of Irish households having the internet at home in 2018 [44]. With the growth of households on the internet, the percentage is probably 90% in 2020. There were about 4.57 billion internet users in the world in July 2020 [45]. The population in Ireland was near 5 million in November 2020 [46]. Hence, the Irish Internet users may be about 4.5 million, it was approximately 0.1% of internet users in the whole world.

According to the data from "Akamai.com" [3], the overall DNS traffic of root servers in the world was about 7 Trillion transactions (Requests and responses) in June 2020. Then, about 0.1% of global authoritative DNS traffic could be Irish authoritative DNS traffic, which is around 7 billion authoritative DNS transactions for one month in Ireland. On average, it could be 233 million authoritative DNS transactions in a day in Ireland.
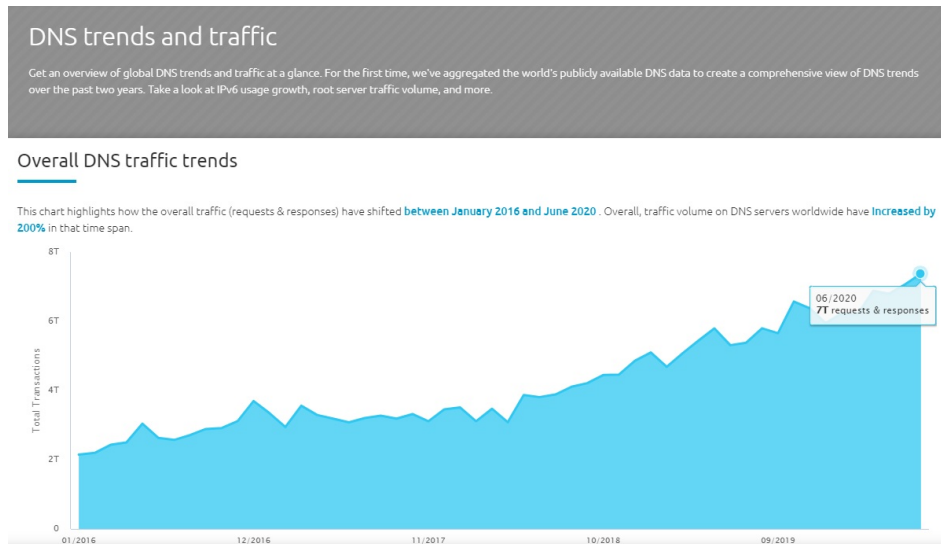
Figure 3.4: *The trend of DNS traffic in the world [3].*

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 root DNS traffic trends(Unit:Transactions) [3].

However, internet traffic is changeable in different hours, it is necessary to understand when are the rush hours(peak time). For example, the internet rush hours are usually between 7 pm and 11 pm in the United Kingdom [47]. In Sao Paulo, the internet rush hours are between 8 pm and 11 pm [48]. In USA, it is 8 pm to 10 pm [49]. In Berlin, the rush hours are 8 pm to 11 pm [50]. In Amsterdam, it is from 8 pm to 11 pm as well [4].
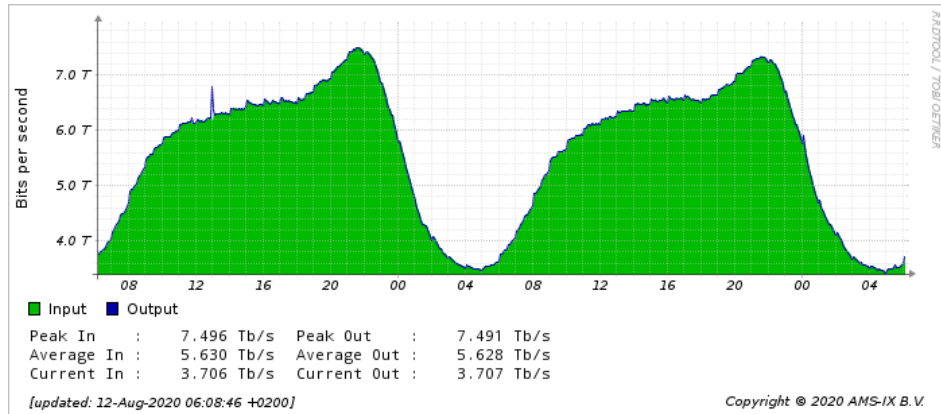
Figure 3.5: *The internet traffic in a day (Amsterdam) [4].*
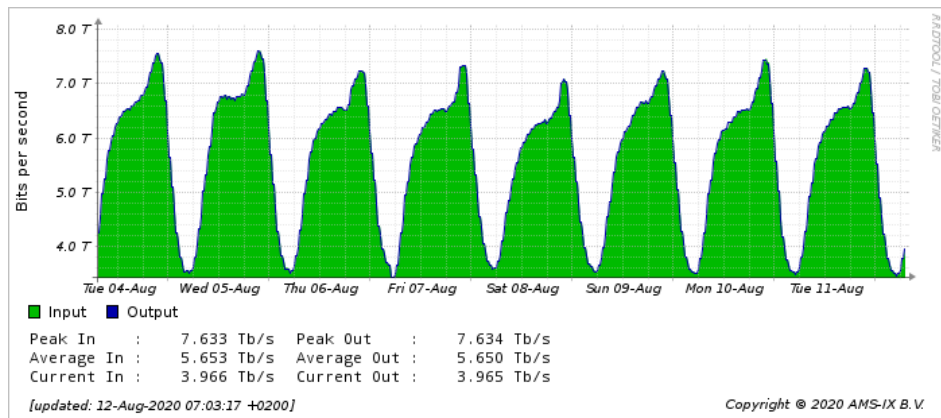
Figure 3.6: *The internet traffic in a week (Amsterdam) [4].*
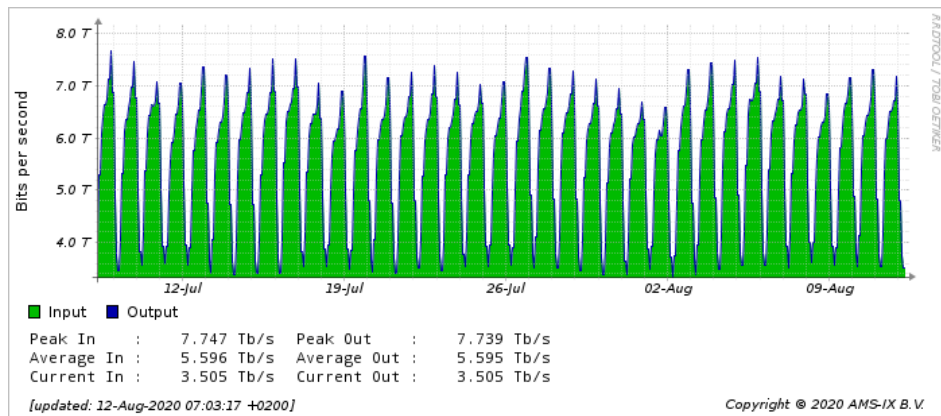
Figure 3.7: *The internet traffic in a month (Amsterdam) [4].*
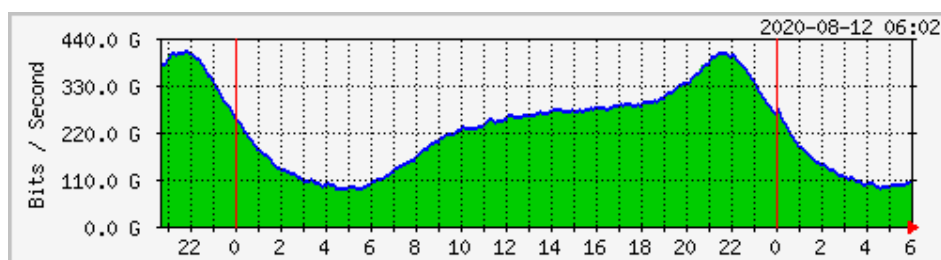
Figure 3.8: *The internet traffic in a day (Berlin) [4].*
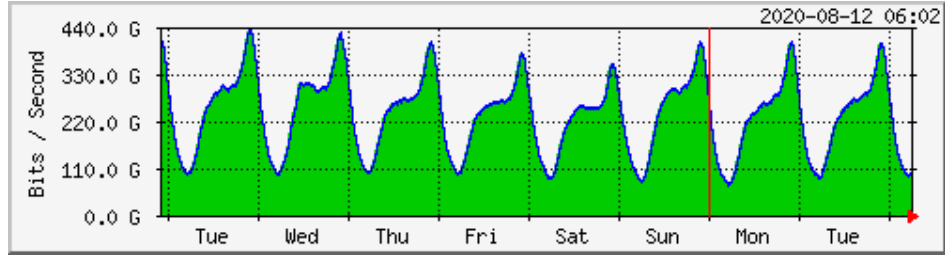
Figure 3.9: *The internet traffic in a week (Berlin) [4].*
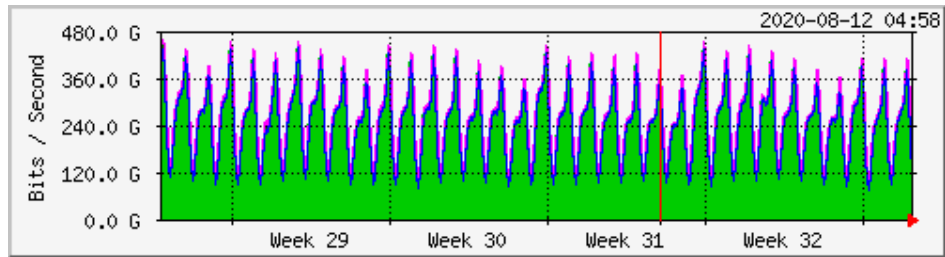
Figure 3.10: *The internet traffic in a month (Berlin) [4].*

All 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. Days in a month, from the beginning to the end of a month, there is no considerable 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 authoritative DNS transactions in Ireland, which is 233 million, then the result is shown in Table 3.4. The 2 busiest hours are 9 PM and 10 PM, the number of authoritative DNS

transactions could be 12.43 million in an hour.

Hour(24)	Percentage	Million transactions
0	4.3%	10.01
1	3.56%	8.28
2	2.96%	6.9
3	2.74%	6.39
4	2.67%	6.21
5	2.59%	6.04
6	2.67%	6.21
7	2.96%	6.9
8	3.56%	8.28
9	4%	9.32
10	4.3%	10.01
11	4.44%	10.36
12	4.59%	10.7
13	4.74%	11.05
14	4.74%	11.05
15	4.89%	11.39
16	4.89%	11.39
17	4.89%	11.39
18	4.81%	11.22
19	4.96%	11.56
20	5.11%	11.91
21	5.33%	12.43
22	5.33%	12.43
23	4.96%	11.56
Total	100%	233

Table 3.4: Using the daily distribution of Internet traffic of Amsterdam to estimate the authoritative 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 authoritative DNS transactions in a rush hour should be higher than 12.43 million.

The numbers of DNS 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 root servers for which we have data, then the estimated number of authoritative DNS transactions in all root servers in rush hours could be $12.43 \div 9 \times 13 = 17.95$ million. Then the average number of authoritative DNS transactions could be 4,987 per second during a 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 one of 12 organizations which are responsible for managing DNS root servers. The servers it manages are L-root servers. ICANN provides a website to display real-time DNS traffic, that is, "Stats.dns.icann.org" [6].

The problem is 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 chooses a city which has a similar population to Ireland to estimate the authoritative DNS traffic. Melbourne should be an ideal sample. The population in Melbourne is close to 5 million in 2019 [51], which is similar to the population in Ireland. Moreover, Melbourne is isolated, there is no big city near Melbourne, therefore the network connection may be similar to a country.
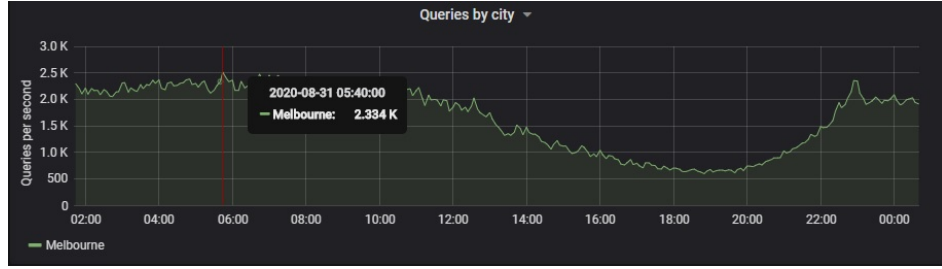
Figure 3.11: *The number of queries per second in a root server in Melbourne [6].*

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 the other 3 root servers are not provided. Assuming the average traffic in the other 3 root servers is close to the root server managed by ICANN, the whole authoritative DNS traffic in Melbourne could be 9,336 per second($2,334 \times 4 = 9,336$). Thus, the authoritative DNS traffic in Ireland could be approximately 9,000 to 10,000 per second during a rush hour.

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

	Method 1	**Method 2**
Source	Akamai	ICANN
Authoritative queries per second	about 5,000	about 9,000
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 during rush hours in Ireland.

Chapter 4

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 Erl-DNS [52] [53].

In this study, Unbound, BIND and PowerDNS are recommended, because there are many discussions and tutorials about those 3 software on Internet [52]. 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 [54]. 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 [55].

About BIND, its alias is Named. It is developed by Internet Systems Consortium(ISC). ISC is also the organization which is responsible for managing the F root server zone. Unlike Unbound, BIND supports both modes of the recursive resolver and authoritative DNS server. The stable version is BIND 9. It can run on Windows, Mac-OS, and Linux [56].

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 is Linux [57].

Apart from DNS software, building a DNS server for TRR also needs some other software, including operating systems, DoH tools, and HTTP servers [58] [59].

The DoH DNS server needs 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 [60]. DoH-proxy includes 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 HTTPS service. NGINX is an HTTP server with high performance, it can also provide different kinds of services. The operator can set the method for listening queries from users [61].

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 Arch Linux [62]. 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
HTTPS 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 3 DNS software

To compare the ease of installation and configuration of BIND, Unbound, and PowerDNS, the researcher tried to install those 3 DNS software on a 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 testing website on the personal computer and gave fixed local IP addresses to all devices and the virtual machine. The IP address and the domain name of this testing website were set in the local DNS server(BIND, Unbound, and PowerDNS).

Finally, the researcher 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.

The study also tested the DoH service. After the implementation of the 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 server 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.
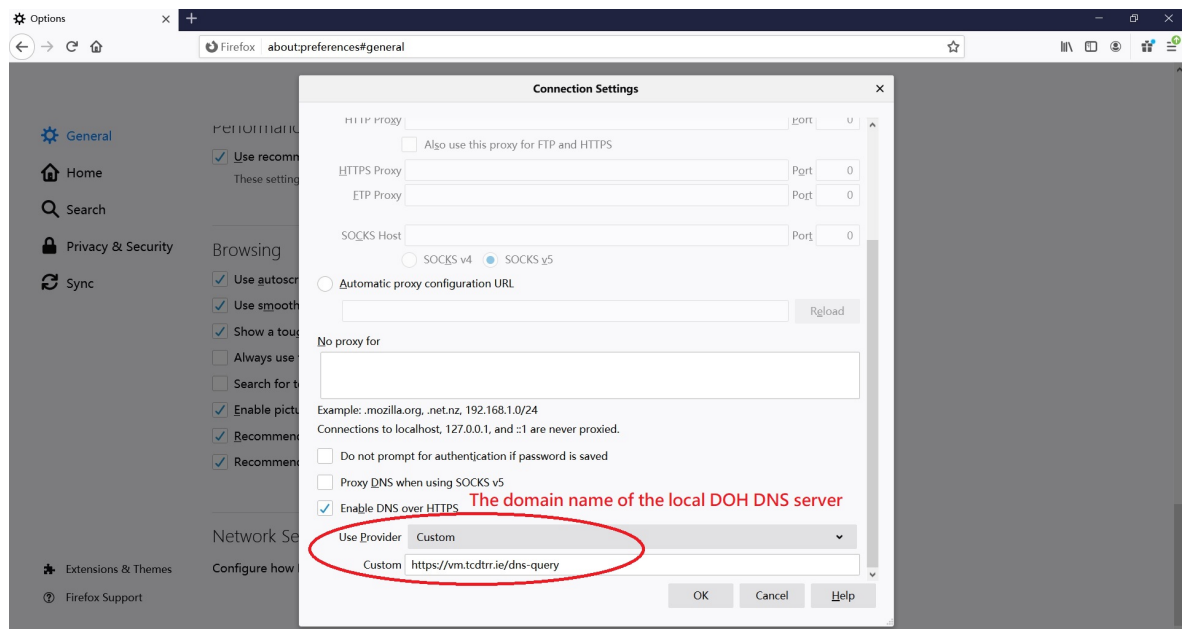
Figure 4.1: *Users can customize the DoH provider by its domain name.*
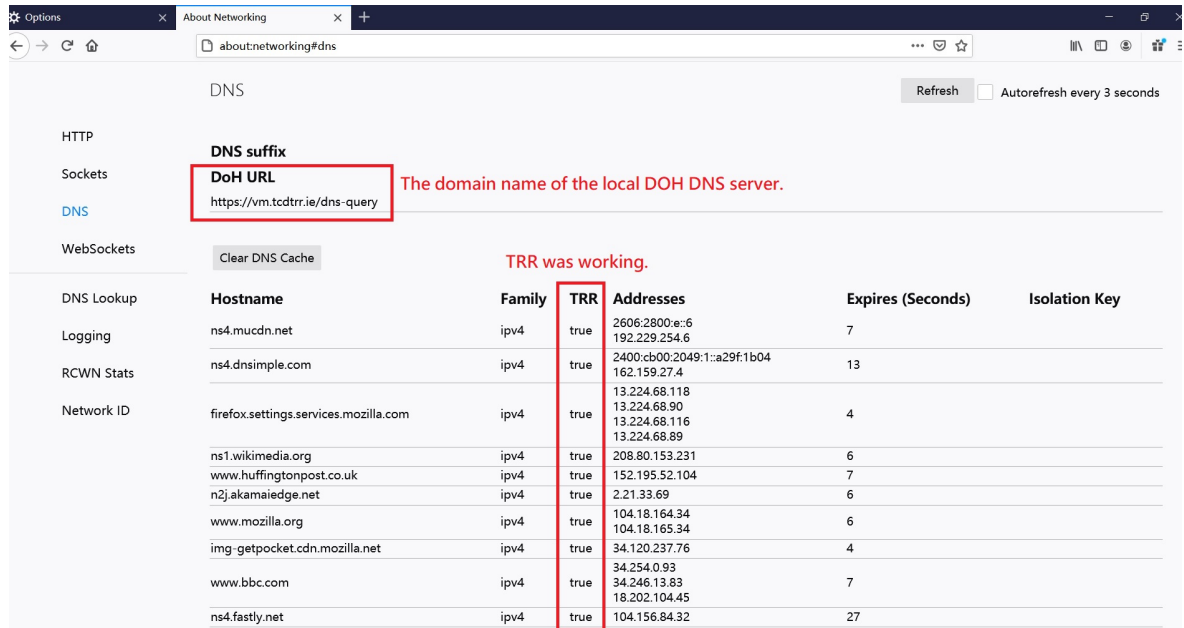
Figure 4.2: *The records of successful DNS queries of TRR.*

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 a programming background, then it needs time to understand the syntax of C language.

Unbound's configuration format is very simple; it is not like 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 style	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.

A report indicated that the times for processing queries in BIND, Unbound and PowerDNS were similar [63]. 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 that report, if processing time is under 1 millisecond, 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.

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. that report called those different working types as "Failed response over a late response" and "An answer is better than no answer". PowerDNS and BIND adopt "Failed response over a late response" and Unbound adopts "An answer is better than no answer" [63].

In conclusion, BIND, Unbound, PowerDNS had similar performances, therefore the point in selecting them is allowing a long time to wait for the answer or not. If yes, DNS providers should choose Unbound. Otherwise, they should choose BIND or PowerDNS.

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

Chapter 5

The experiment

5.1 The implementation of the experiment

In order to understand more about the performance, this study had an experiment to test the performance of DoH.

First of all, a DoH server was built in the local network. After that, the researcher used Python to design a testing program. The function of the testing program was to send 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 Python code of this testing program is attached as Appendix 1.

The testing program was able to send totally 50 DNS queries between 0.02 and 0.07 seconds. The outputs of this testing program were CSV files, those CSV files contained the records and statistics of the tests in this experiment. The records and statistics are attached as Appendix 2 and Appendix 3.

	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	10 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	Top 50 websites in Ireland(see Appendix 4)
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 [64], 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. The list of top 50 websites in Ireland is attached as Appendix 4.

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 [65] 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)
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.
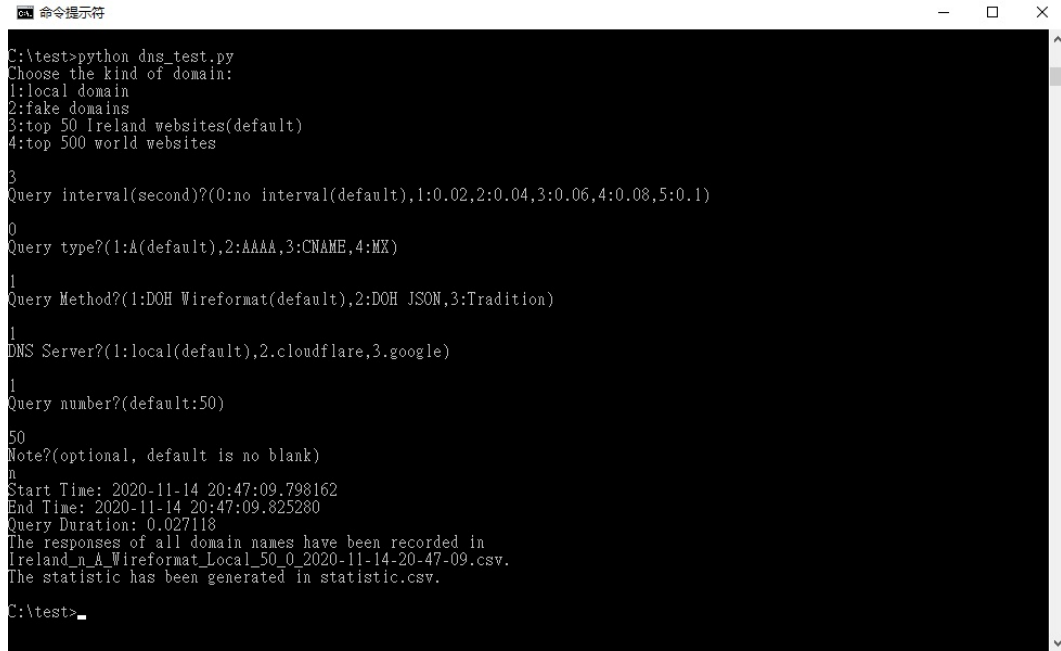
The outputs of the testing program were dependent variables, which were the results of the experiment. The researcher used those results from different parameters to analyze the performance of a DoH DNS server. The outputs are shown in Table 5.3.

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 responds 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 the keyboard. The outputs are including the statistic and the results of all responses of DNS queries, they are saved into 2 CSV files.

Figure 5.1: *The screenshot of the testing program.*

5.2 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 5.4, 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. 5.2, Fig. 5.3, and Fig. 5.4.

Parameters	Values
Query name	Top 50 websites in Ireland
DNS type	DoH(Wireformat)
Record type	A(48 are available)
Query time	From 21:13:06 to 21:25:53 7/11/2020

Table 5.4: The parameters for testing query intervals.
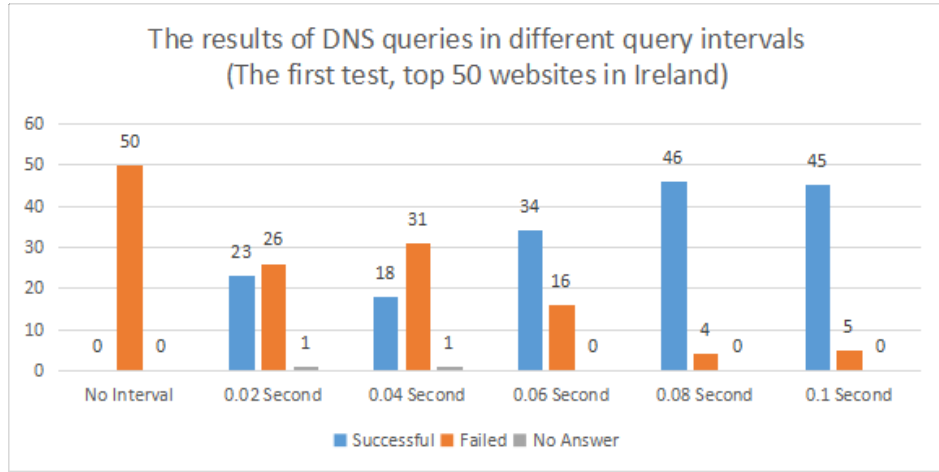
Figure 5.2: *The numbers of results of DNS queries in different query intervals for the first test, the parameters are shown in Table 5.4.*
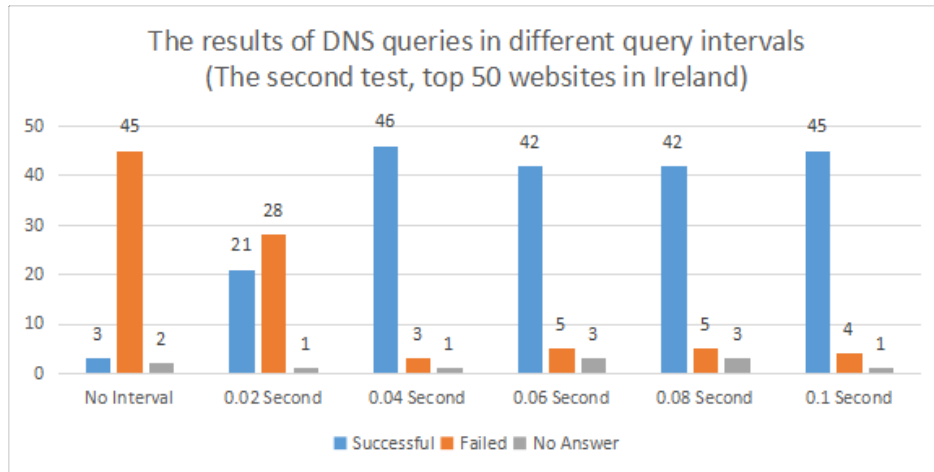
Figure 5.3: *The numbers of results of DNS queries in different query intervals for the second test, the parameters are shown in Table 5.4.*
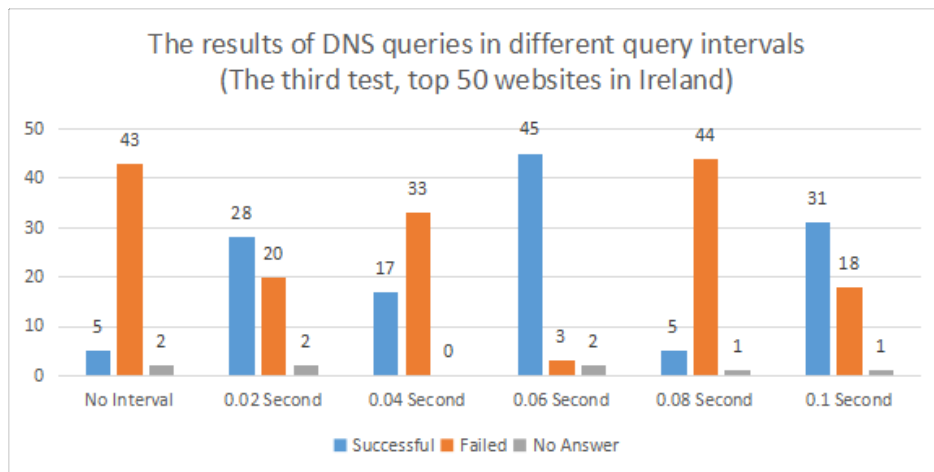
Figure 5.4: *The numbers of results of DNS queries in different query intervals for the third test, the parameters are shown in Table 5.4.*

The figures illustrate 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). 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 DoH DNS server.

5.3   The test for DNS record types

The DNS record types [66] 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.

Type A records are used for getting the IP address of IPv4 [14], it is the most popular DNS record type so far. Type AAAA records are used for getting the IP address of IPv6 [15]. MX stands for Mail Exchange, it is used for indicating the IP address of a server responsible for accepting e-mail.

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

This test was repeated 3 times as well. The parameters were set as shown in Table 5.5. 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. 5.5, Fig. 5.6 and Fig. 5.7.

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 5.5: The parameters for testing different DNS record types.
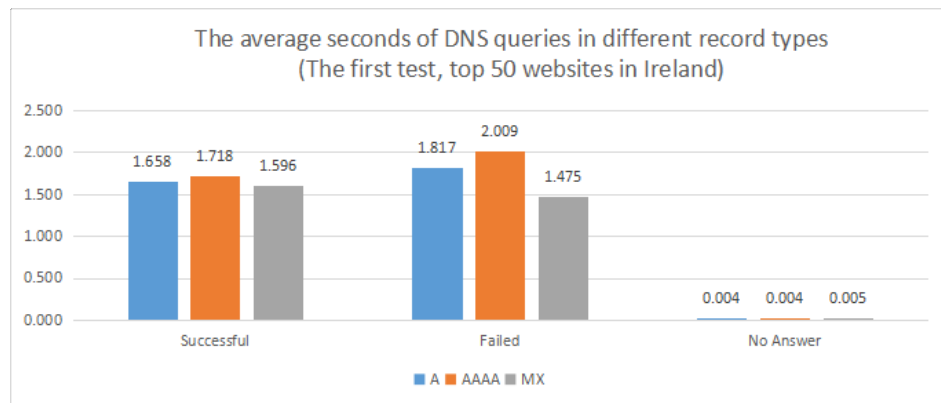
Figure 5.5: *The average seconds of DNS queries in different record types for the first test, the parameters are shown in Table 5.5.*
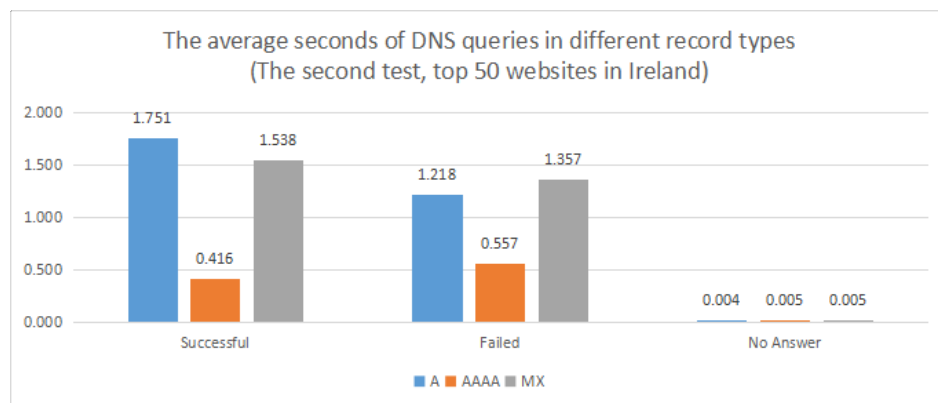
Figure 5.6: *The average seconds of DNS queries in different record types for the second test, the parameters are shown in Table 5.5.*
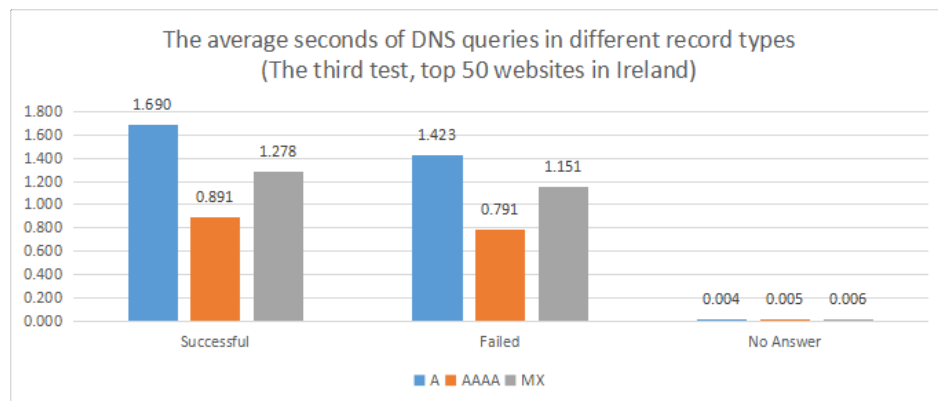
Figure 5.7: *The average seconds of DNS queries in different record types for the third test, the parameters are shown in Table 5.5.*

Those figures display that type 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 type AAAA in the second and third tests.

Another noticeable outcome is 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 in their performances were not huge. The results also indicate that the performance of the DoH service was unstable.

5.4   The test for using the cache

The last test was testing the performance of using the cache. A DNS server is capable to respond DNS queries rapidly by Using the cache [63]. Therefore this study tried to find out how is the gap between using the cache and not using the cache in responding DNS queries.

This test still used top 50 websites in Ireland as query names and it was repeated 3 times too. The server did not flush the cache, hence the cache contained all IP addresses for 48 top websites in Ireland(2 websites did not have matched IP). The parameters are listed in Table 5.6, and the results are illustrated in Fig. 5.8 and Fig. 5.9.

Parameters	Values
Query name	The top 50 websites in Ireland
DNS type	DoH(Wireformat)
Query interval	No interval
Record type	A(48 are available)
Query time	From 20:46:43 to 20:47:10 14/11/2020

Table 5.6: The parameters for testing the effect of the cache.
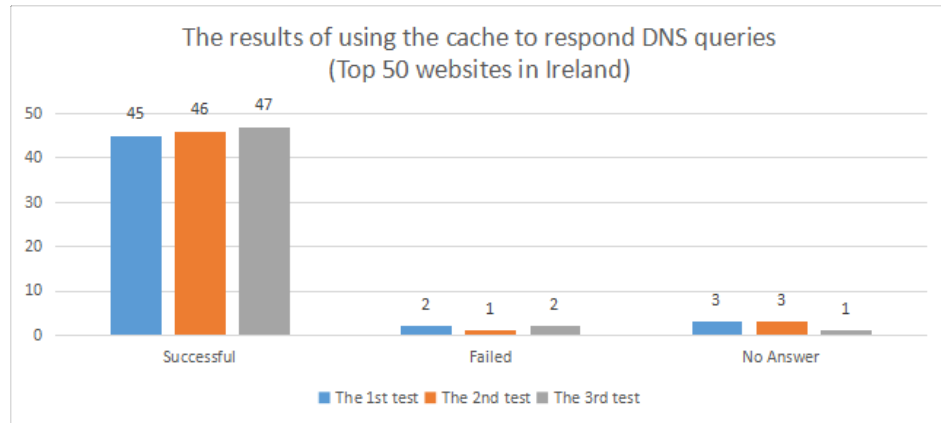
Figure 5.8: *The results of using the cache to respond DNS queries, the parameters are shown in Table 5.6.*
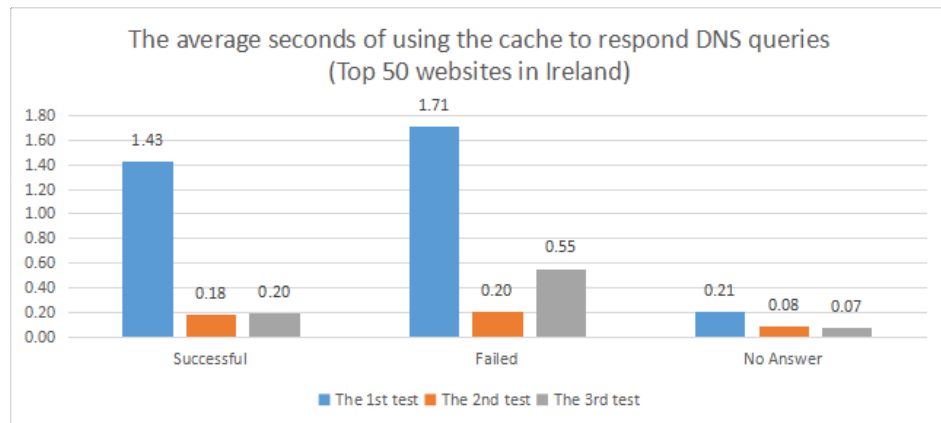
Figure 5.9: *The average seconds of using the cache to respond DNS queries, the parameters are shown in Table 5.6.*

The results of using the cache were far better than the results of previous tests for DoH. A noticeable result is that the latency of the first test was obviously higher than the second test and the third test. The possible reason may be the computer was busy at that moment because major processes should occur in the local computer base on using cache.

Although using the cache can improve the performance significantly, the researcher did not discover any percentage and number of responses by using the cache in real

recursive resolvers. Hence, the workload of using the cache in real recursive resolvers can not be assessed in this study.

Chapter 6

Other concerns

6.1 The concern about DDoS attacks

Distributed denial-of-service(DDoS) [67] is also an important issue to consider when building a DNS server [68].

There are 2 sorts of DNS queries: Recursive and iterative. Recursive queries occur when users send queries to recursive resolvers. When recursive resolvers receive requests, if they do not have IP addresses matching the user's queries, then recursive resolvers ask authoritative DNS servers for getting IP addresses. Next, recursive resolvers 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 [69].

However, recursive queries can be used in DDoS attacks. The content of the 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 [68].
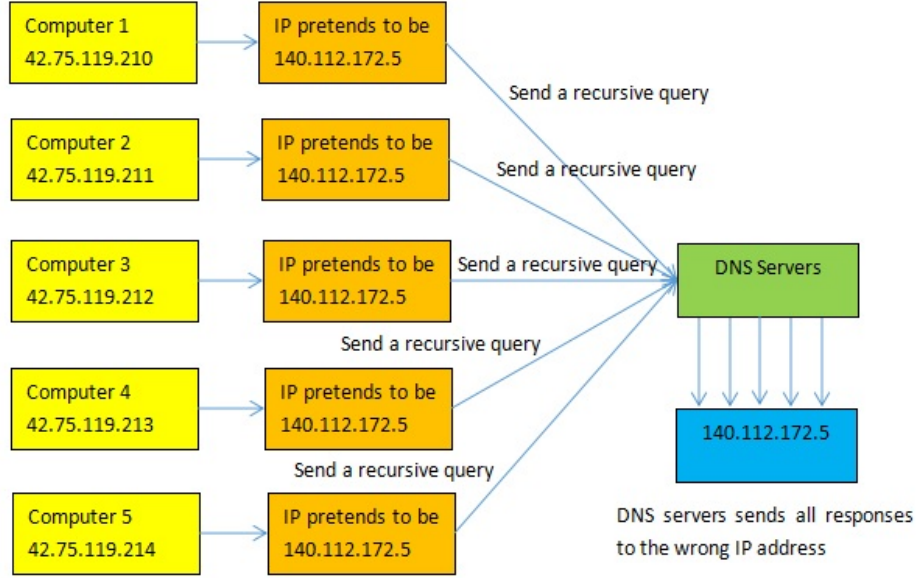
Figure 6.1: *The DDoS attack in recursive DNS queries [7].*

Thus, restricting DNS queries may be the ideal method to prevent DNS amplification attacks, which means only the DNS queries from the same region are allowed to be processed [70]. The users in other regions can not use that DNS server, but other regions should have their own DNS servers to process their users' DNS queries.
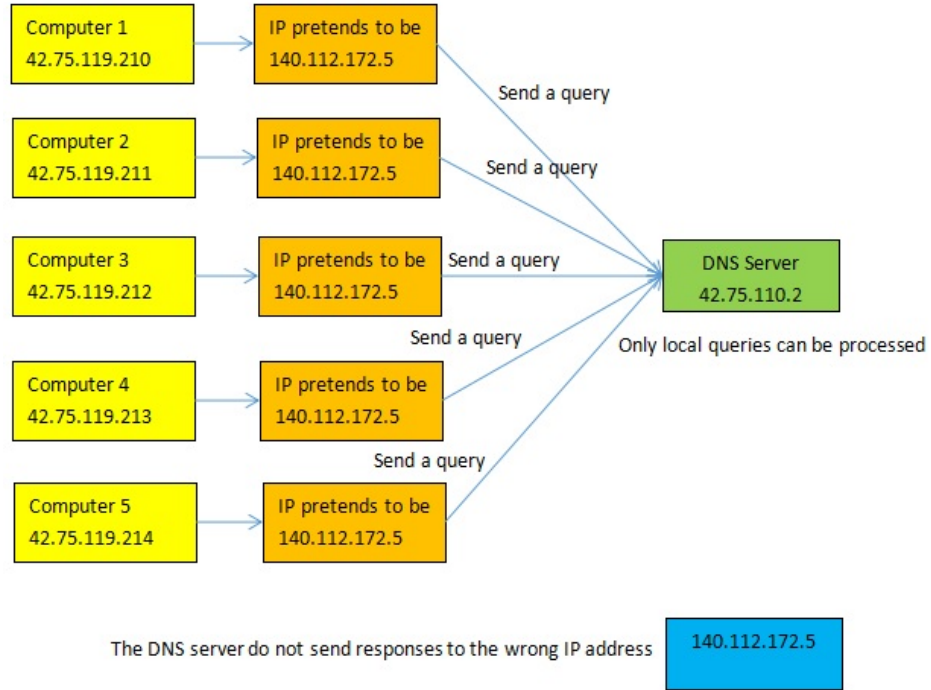
Figure 6.2: *Restricting DNS queries to prevent DNS amplification attacks [7].*

6.2 The concern about the policy

The Irish government has banned some websites for some reasons [71]. The problem is that users may utilize DoH to bypass the censorship from the government to browse banned websites [72] [73], because DNS queries are encrypted. It could be a severe issue for governments or Internet service providers(ISP) who intend to control the Internet [74].

The study did a simple test. "1337x.to" is one of the banned websites in the Republic of Ireland [71]. The reason is this website has the issue of copyright infringement. The researcher could not browse the website in Ireland without DoH. The screenshot of the Firefox at that moment is displayed in Fig. 6.3.

The method used to ban websites is probably DNS spoofing [75] because the IP address in Fig. 6.3 is fake. DoH could reduce the effect of DNS spoofing [76].

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 Firefox, which means the censorship may not work for DoH users. The screenshot is shown in Fig. 6.4.
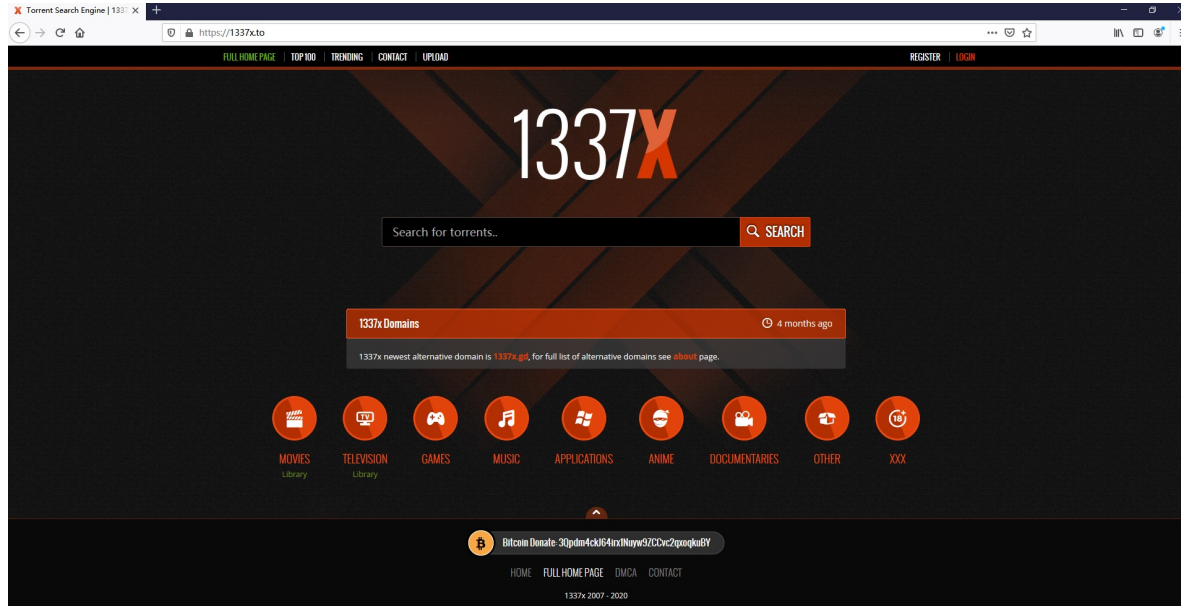
Figure 6.4: *Firefox can browse the banned website after enabling TRR.*

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 only adopt DNS spoofing to block banned websites.

6.3   The concern about the latency

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 [77].

The study assumes that the optical fiber is used to be the tool for transmitting signals, the latency will be about 5 microseconds per kilometers [78]. If the latency is including the time of the response, which is round-trip time(RTT) [79], 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 [80]. The screenshot is displayed in Fig. 6.5. Thus, this study takes 8 ms to be the minimum requirement of the latency.
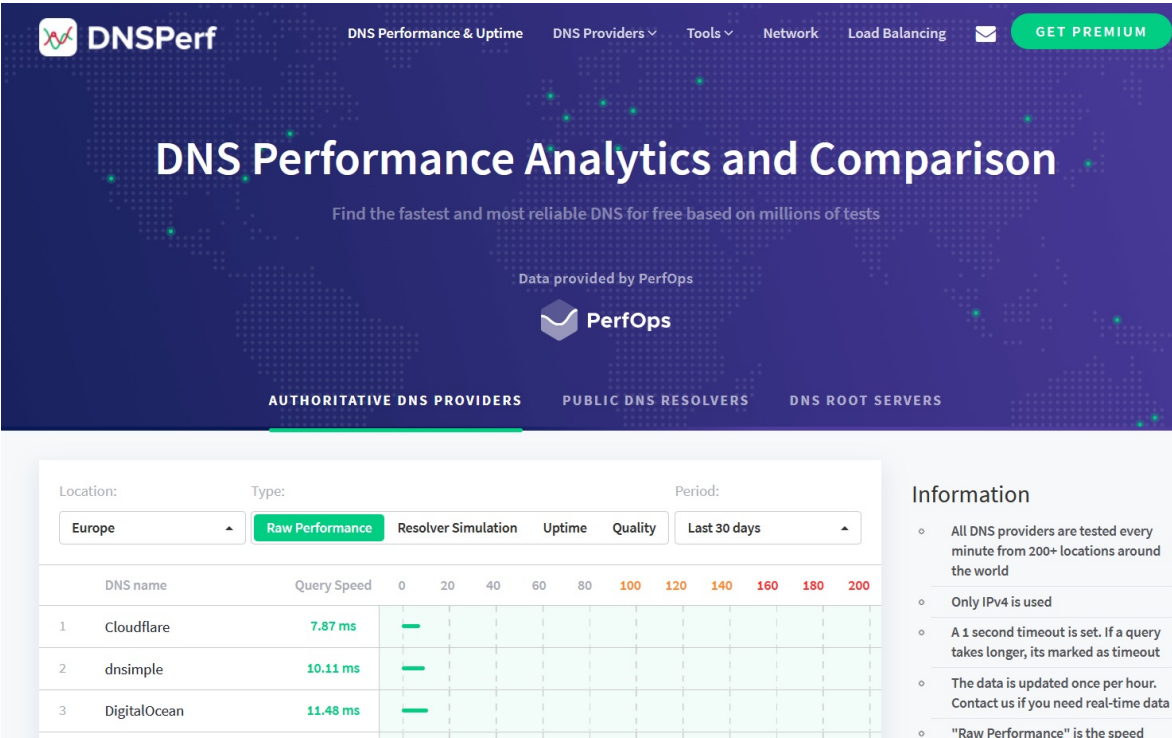
Figure 6.5: *The ranking of DNS providers by latency in Europe.*

The distance of networks needs to be known for calculating latency. The researcher has found a network map of Ireland [8]. The owner is Magnet but Magnet does not reveal the distance of its networks. The map is shown in Fig. 6.6. On the other hand, other companies have their own networks and their networks are different from Magnet [81].

Figure 6.6: *The map of Magnet networks in Ireland, the source is its website [8].*

This study has a lack of data about the distance of networks. Thus, the researcher utilized Google Map to estimate the distance of the possibly farthest network from Dublin. The distances of some far places from Dublin can reach about 394 kilometers. The distances are counted by Google Map in Fig. 6.7 and Fig. 6.8. The path bypasses the UK part in Northern Ireland.
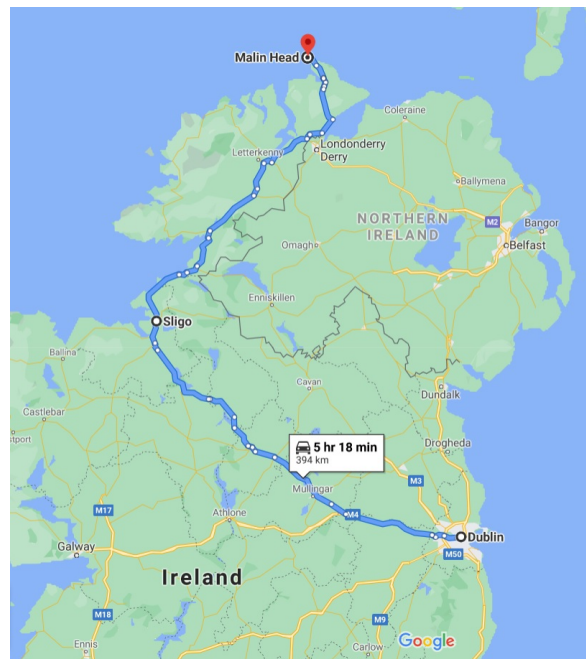
Figure 6.7: *The possible distance of a very far place in the north from Dublin.*
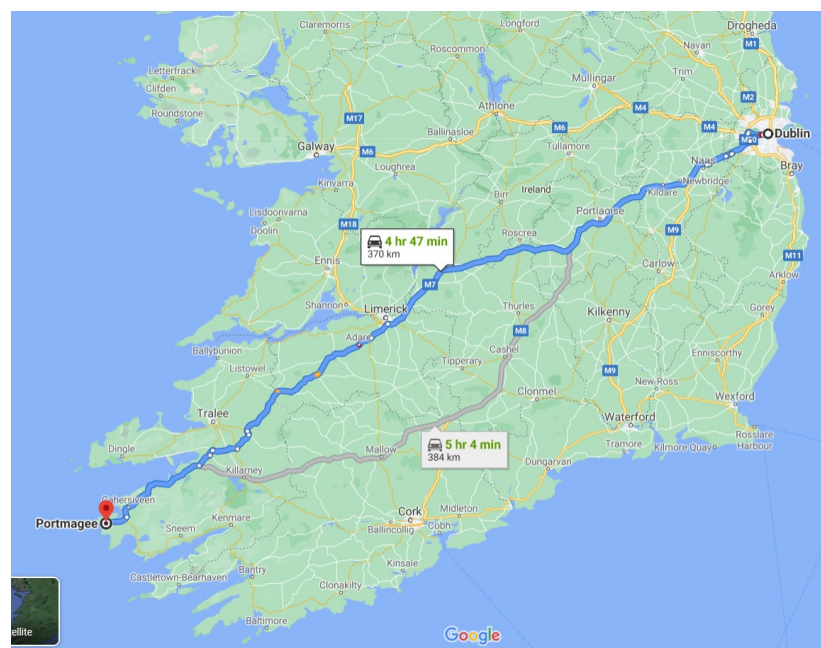
Figure 6.8: *The possible distance of a very far place in the south from Dublin.*

The distance 394 kilometers could cause approximately 4 ms for a DNS query [82], 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 not be the problem, but the amplifiers and regenerators need to be deployed if using optical fiber to transmit the data, because the distance is longer than 100 kilometers [78].

Chapter 7

Overall design

DoH service would raise privacy on the Internet. Meanwhile, the concept of the TRR project could further strengthen privacy on the basis of DoH. The idea of the TRR project 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 project. Hence, this chapter is going to make a technical plan for the implementation of the TRR project.

Previous chapters have discussed 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 make the management more transparent to the public.

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 the DoH service should not be a problem.

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

The performance could be very good by using cache for a recursive resolver in the experiment of chapter 5. Meanwhile, this study did not find the data about the situation of using the cache in real recursive resolvers. Thus this study only adopts authoritative DNS queries to assess the required performance for a recursive resolver. Authoritative DNS queries are the queries matched by authoritative DNS servers, not matched by the cache. The data of authoritative queries were from root servers.

Chapter 3 had a discussion about the Irish DNS traffic. The estimation of authoritative DNS queries per second in Ireland is possible around 5,000 or 9,000. The number of DNS queries in Ireland is not very high in comparison to other countries.

However, the DNS provider also needs to consider the increase of DNS traffic in the future, because the DNS traffic should rise a lot in Ireland in the next 5 years. The reason is the trend of the population in Ireland in recent years is growing up [46], thus

this study supposes that the Irish population will be higher than the current population in the next 5 years, and the DNS queries will ascend as well.

Furthermore, some events could cause a higher usage of the Internet. For example, the virus COVID-19 made the Internet traffic higher [83] [84]. Those factors and their effects are hard to be predicted and evaluated.

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

According to the experiment in chapter 5, a DNS server may process 10 DNS 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 server machines [85] [86] [87] [88].

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 [89]. Thus the performance of a server machine should be better than the results in the experiment in this study. If the DNS provider takes a data center with 15000 server machines, it should be able to compute at least 150000 authoritative 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 server machines focus on the computing of DNS queries(1 server machine can deal with at least 10 DNS queries without using the cache for 1 second, this study estimates that there are up to almost 10000 authoritative DNS queries per second in Ireland).

Even though the DNS queries are 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 DoH may encounter some problems in processing 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 not to adopt the DNS spoofing to ban websites because DNS spoofing may not work on DoH. 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 not to use DNS spoofing. Otherwise, everyone is able to browse banned websites.

If the Irish government really want to ban those websites, the ideal method may be Deep Packet Inspection [90], which is one of the methods adopted by the Chinese government to ban sensitive websites.

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

Chapter 6 mentioned that Ireland is not a big country, the farthest place from Dublin maybe only 400 kilometers. 400 kilometers merely causes around 4 ms to the latency of a DNS query. Thus, the latency could be possible to be controlled under 8 ms in the whole of Ireland.

Although the latency should not be a severe issue in Ireland, some remote areas would have worse quality of networks. Poor networks may reduce the performance of DoH a lot [31] [74]. In this case, the infrastructure of networks in remote areas should be improved.

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

Even if a DNS server in one data center is capable to deal with the whole DNS queries and the latency could be lower than 8 ms in Ireland, 2 DNS servers in two data centers are more reliable. In case one DNS server fails, 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 [33], 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.

Chapter 8

Conclusion and future work

Trusted Recursive Resolver(TRR) project may provide a safer environment to protect the privacy of users base on using DNS over HTTPS(DoH) service to encrypt DNS queries. Furthermore, the TRR project also requires that DNS providers must allow civilians to supervise their 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 when compared to other countries. Therefore only 2 DNS servers with DOH service are required in Ireland, the locations could be Dublin and Cork respectively. Thus, it is worth constructing DNS servers for the TRR project for Ireland.

In conclusion, The DNS provider could deploy 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 project.

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 a personal computer and a personal network to finish this study without any budget. If a server machine or a cloud server and a network with better quality could be given in the experiment, then the result could be more accurate.

Meanwhile, the researcher did not find the statistic data of real recursive resolvers. Therefore, this study just utilized the data from some root servers to emulate the possible results because only root servers announce their data on the Internet. It is necessary to take the data from real recursive resolvers to analyze the DNS traffic and the performance of a recursive resolver if a more precise analysis is required.

Thus, the researcher expects that some real recursive resolvers could offer the statistic data of DNS queries for further studies in the future. Especially the number of DNS queries with using the cache, that is one of the key points to evaluate the required performance of a recursive resolver with DoH service.

Bibliography

[1] program-think, "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`, Oct. 2018. Accessed on: Nov. 11, 2020.

[2] root-servers.org, "root-servers.org." [Online]. Available: https://root-servers.org/. Accessed on: Nov. 11, 2020.

[3] Akamai, "Dns trends and traffic." [Online]. Available: https://www.akamai.com/de/de/why-akamai/dns-trends-and-traffic.jsp. Accessed on: Jul. 29, 2020.

[4] AMS-IX, "Total traffic statistics(amsterdam)." [Online]. Available: https://stats.ams-ix.net/index.html, Aug. 2020. Accessed on: Aug. 12, 2020.

[5] Cloudflare, "What is a dns root server?." [Online]. Available: https://www.cloudflare.com/learning/dns/glossary/dns-root-server/. Accessed on: Nov. 11, 2020.

[6] stats.dns.icann.org, "stats.dns.icann.org." [Online]. Available: https://stats.dns.icann.org/, Aug. 2020. Accessed on: Aug. 31, 2020.

[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`, Jun. 2017. Accessed on: Nov. 12, 2020.

[8] Magnet, "Project leap." [Online]. Available: `https://www.magnet.ie/residential/project-leap/`. Accessed on: Nov. 13, 2020.

[9] J. Peters, "What is dns, how it works + vulnerabilities." [Online]. Available: `https://www.varonis.com/blog/what-is-dns/`, Mar. 2020. Accessed on: Nov. 10, 2020.

[10] DNSSEC.NET, "Dnssec: Dns security extensions." [Online]. Available: `https://www.dnssec.net/`, Sep. 2018. Accessed on: Nov. 10, 2020.

[11] OpenDNS, "Introducing dnscrypt." [Online]. Available: `https://www.opendns.com/about/innovations/dnscrypt/`. Accessed on: Nov. 10, 2020.

[12] L. Z. Z. Hu, J. Heidemann, A. Mankin, D. Wessels, and P. Hoffman, "Specification for dns over transport layer security (tls)." [Online]. Available: `https://tools.ietf.org/html/rfc7858`, May 2016. Accessed on: Nov. 10, 2020.

[13] P. Hoffman and P. McManus, "Dns queries over https (doh)." [Online]. Available: `https://tools.ietf.org/html/rfc8484`, Oct. 2018. Accessed on: Nov. 10, 2020.

[14] Information Sciences Institute, "Internet protocol." [Online]. Available: `https://tools.ietf.org/html/rfc791`, Sep. 1981. Accessed on: Nov. 10, 2020.

[15] S. Deering and R. Hinden, "Internet protocol, version 6 (ipv6)." [Online]. Available: `https://tools.ietf.org/html/rfc2460`, Dec. 1998. Accessed on: Nov. 10, 2020.

[16] P. Mockapetris, "Domain names - concepts and facilities." [Online]. Available: `https://tools.ietf.org/html/rfc882`, Nov. 1983. Accessed on: Nov. 10, 2020.

[17] 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`, Jul. 2013. Accessed on: Nov. 12, 2020.

[18] IETF, "Dns resolver discovery protocol (drdp)." [Online]. Available: `https://tools.ietf.org/id/draft-mglt-add-rdp-02.html`, May 2020. Accessed on: Nov. 11, 2020.

[19] J. Postel, "Request for comments on requests for comments." [Online]. Available: `https://tools.ietf.org/html/rfc825`, Nov. 1982. Accessed on: Nov. 10, 2020.

[20] IETF, "Who we are." [Online]. Available: `https://ietf.org/about/who/`. Accessed on: Nov. 10, 2020.

[21] S. Bortzmeyer, "Dns privacy considerations." [Online]. Available: `https://tools.ietf.org/html/rfc7626`, Aug. 2015. Accessed on: Nov. 10, 2020.

[22] T. Wicinski and Ed., "Dns privacy considerations draft-ietf-dprive-rfc7626-bis-08." [Online]. Available: `https://tools.ietf.org/html/draft-ietf-dprive-rfc7626-bis-08`, Oct. 2020. Accessed on: Nov. 10, 2020.

[23] J. Schaumann, "Dns security: Threat modeling dnssec, dot, and doh." [Online]. Available: `https://www.netmeister.org/blog/doh-dot-dnssec.html`, Oct. 2019. Accessed on: Nov. 11, 2020.

[24] The DNS Institute, "Disadvantages of dnssec." [Online]. Available: `https://dnsinstitute.com/documentation/dnssec-guide/ch06s06.html`. Accessed on: Nov. 10, 2020.

[25] S. Gallagher, "How to keep your isp's nose out of your browser history with encrypted dns." [Online]. Available: `https://arstechnica.com/information-technology/2018/04/how-to-keep-your-isps-nose-out-of-your-browser-history-with-encrypted-dns/`, Apr. 2018. Accessed on: Nov. 11, 2020.

[26] C. O'Connell, "Tenta dns over tls vs dnscrypt." [Online]. Available: `https://tenta.com/blog/post/2017/12/dns-over-tls-vs-dnscrypt`, Dec. 2017. Accessed on: Nov. 11, 2020.

[27] IONOS, "Dns over tls: an improved security concept." [Online]. Available: `https://www.ionos.com/digitalguide/server/security/dns-over-tls/`, Jul. 2020. Accessed on: Nov. 10, 2020.

[28] DNSCRYPT, "Dnscrypt and doh servers." [Online]. Available: `https://dnscrypt.info/public-servers/`. Accessed on: Nov. 11, 2020.

[29] Cloudflare, "Dns over tls vs. dns over https — secure dns." [Online]. Available: `https://www.cloudflare.com/learning/dns/dns-over-tls/`. Accessed on: Nov. 11, 2020.

[30] C. Crane, "Doh! firefox engages more secure dns over https protocol — here's what that means for you." [Online]. Available: `https://www.thesslstore.com/blog/DoH-firefox-engages-more-secure-dns-over-https-protocol-heres-what-that-mean` Mar. 2020. Accessed on: Nov. 11, 2020.

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

[32] J. Wijenbergh, "Performance comparison of dns over https to unencrypted dns," tech. rep., Radboud University, Oct. 2019.

[33] T. Böttger, F. Cuadrado, G. Antichi, E. L. Fernandes, G. Tyson, I. Castro, and S. Uhlig, "An empirical study of the cost of dns-over-https," tech. rep., Queen Mary University of London, Oct. 2019.

[34] Mozilla, "Trusted recursive resolver." [Online]. Available: `https://wiki.mozilla.org/Trusted_Recursive_Resolver`, Sep. 2020. Accessed on: Nov. 11, 2020.

[35] 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-` Jun. 2020. Accessed on: Nov. 11, 2020.

[36] 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` Jun. 2020. Accessed on: Nov. 11, 2020.

[37] 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/, Feb. 2020. Accessed on: Nov. 11, 2020.

[38] 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/`, Jun. 2020. Accessed on: Nov. 11, 2020.

[39] 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/`, Sep. 2019. Accessed on: Nov. 11, 2020.

[40] 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`, May 2020. Accessed on: Nov. 11, 2020.

[41] 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/`, May 2020. Accessed on: Nov. 11, 2020.

[42] S. Tkachenko, "Enable dns over https in opera (doh)." [Online]. Available: `https:` `//winaero.com/enable-dns-over-https-in-opera-DoH/`, Feb. 2020. Accessed on: Nov. 11, 2020.

[43] 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` Feb. 2020. Accessed on: Nov. 11, 2020.

[44] central statistics office (Ireland), "Information society statistics - households." [Online]. Available: https://www.cso.ie/en/releasesandpublications/er/isshh/informationsocietystatistics-households2018/, Aug. 2018. Accessed on: Nov. 11, 2020.

[45] J. Clement, "Global digital population as of july 2020." [Online]. Available: https://www.statista.com/statistics/617136/digital-population-worldwide/, Oct. 2020. Accessed on: Nov. 11, 2020.

[46] Worldometer, "Ireland population(live)." [Online]. Available: https://www.worldometers.info/world-population/ireland-population/. Accessed on: Nov. 12, 2020.

[47] N. Cumins, "Avoiding the internet rush hour." [Online]. Available: https://broadbanddeals.co.uk/avoiding-the-internet-rush-hour/, Jan. 2019. Accessed on: Aug. 12, 2020.

[48] ix.br, "Selecione a localidade para ver as estatísticas de tráfego." [Online]. Available: https://ix.br/trafego/agregado/sp, Aug. 2020. Accessed on: Aug. 12, 2020.

[49] 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, Jul. 2012. Accessed on: Aug. 12, 2020.

[50] DE-CIX, "Traffic statistics(berlin)." [Online]. Available: https://www.bcix.de/bcix/traffic/, Aug. 2020. Accessed on: Aug. 12, 2020.

[51] Macrotrends, "Melbourne, australia metro area population 1950-2020." [Online]. Available: https://www.macrotrends.net/cities/206168/melbourne/population. Accessed on: Nov. 11, 2020.

[52] TINYDNS, "Compare the different dns servers: Which one is right for you?." [Online]. Available: `https://tinydns.org/compare-different-dns-servers/`, Sep. 2017. Accessed on: Nov. 12, 2020.

[53] K. John, "Bind vs dnsmasq vs powerdns vs unbound." [Online]. Available: `https://computingforgeeks.com/bind-vs-dnsmasq-vs-powerdns-vs-unbound/`, Jun. 2019. Accessed on: Nov. 12, 2020.

[54] NLNETLABS, "Nsd." [Online]. Available: https://www.nlnetlabs.nl/projects/nsd/about/. Accessed on: Nov. 11, 2020.

[55] NLNETLABS, "Unbound." [Online]. Available: `https://nlnetlabs.nl/projects/unbound/about/`. Accessed on: Nov. 11, 2020.

[56] NS1, "Bind dns: Pros, cons and alternatives." [Online]. Available: `https://ns1.com/resources/bind-dns-pros-cons-and-alternatives`. Accessed on: Nov. 11, 2020.

[57] PowerDNS, "About powerdns." [Online]. Available: `https://www.powerdns.com/about.html`. Accessed on: Nov. 12, 2020.

[58] Loull, "Dns resources." [Online]. Available: https://www.cnblogs.com/549294286/p/5200255. Feb. 2016. Accessed on: Nov. 12, 2020.

[59] ISHM, "Building dns over https server on centos 7." [Online]. Available: https://ishm.idv.tw/?p=481, Oct. 2019. Accessed on: Nov. 12, 2020.

[60] Facebookexperimental, "Dns over https proxy." [Online]. Available: `https://github.com/facebookexperimental/DoH-proxy`, Oct. 2020. Accessed on: Nov. 12, 2020.

[61] NGINX, "Welcome to niginx wiki!." [Online]. Available: https://www.nginx.com/resources/wiki/. Accessed on: Nov. 12, 2020.

[62] J. Kiarie, "10 linux distributions and their targeted users." [Online]. Available: `https://www.tecmint.com/linux-distro-for-power-users/`, Sep. 2020. Accessed on: Nov. 11, 2020.

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

[64] Alexa, "Top sites in ireland." [Online]. Available: `https://www.alexa.com/topsites/countries/IE`, Oct. 2020. Accessed on: Oct. 25, 2020.

[65] Sciencebuddies.org, "Variables in your science fair project." [Online]. Available: `https://www.sciencebuddies.org/science-fair-projects/science-fair/variables`. Accessed on: Nov. 11, 2020.

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

[67] Cloudflare, "What is a ddos attack?." [Online]. Available: `https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/`. Accessed on: Nov. 14, 2020.

[68] Imperva, "Dns amplification." [Online]. Available: `https://www.imperva.com/learn/ddos/dns-amplification/`. Accessed on: Nov. 12, 2020.

[69] Cloudflare, "What is recursive dns?." [Online]. Available: `https://www.cloudflare.com/learning/dns/what-is-recursive-dns/`. Accessed on: Nov. 12, 2020.

[70] 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`, Apr. 2020. Accessed on: Nov. 12, 2020.

[71] N. Griffin, "Eight illegal streaming sites blocked as ireland steps up war against piracy." [Online]. Available: `http://www.iftn.ie/legal/LegalNews/?act1=record&only=1&aid=73&rid=4291428&tpl=archnews&force=1`, Jan. 2018. Accessed on: Nov. 11, 2020.

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

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

[74] K. Borgolte, T. Chattopadhyay, N. Feamster, M. Kshirsagar, J. Holland, A. Hounsel, and P. Schmitt, "How dns over https is reshaping privacy, performance, and policy in the internet ecosystem," tech. rep., Princeton University and The University of Chicago, Jul. 2019.

[75] U. Schrott, "Dns attacks: How they try to direct you to fake pages." [Online]. Available: `https://blog.eset.ie/2017/03/02/dns-attacks-how-they-try-to-direct-you-to-fake-pages/`, Mar. 2017. Accessed on: Nov. 13, 2020.

[76] Daniel, "Is dns-over-https (doh) the best choice for dns privacy?." [Online]. Available: `https://www.eurodns.com/blog/dns-over-https-dns-privacy`, Dec. 2018. Accessed on: Nov. 13, 2020.

[77] K. Miller, "Calculating optical fiber latency." [Online]. Available: `https://www.m2optics.com/blog/bid/70587/calculating-optical-fiber-latency`, Jan. 2012. Accessed on: Nov. 12, 2020.

[78] Rogerluethy, "What is latency?." [Online]. Available: `https://rogerluethy.wordpress.com/2011/09/01/what-is-latency/`, Sep. 2011. Accessed on: Nov. 12, 2020.

[79] Cloudflare, "What is round-trip time? — rtt definition." [Online]. Available: `https://www.cloudflare.com/learning/cdn/glossary/round-trip-time-rtt/`. Accessed on: Nov. 13, 2020.

[80] DNSPerf, "Dns performance analytics and comparison." [Online]. Available: `https://www.dnsperf.com/#!dns-providers,Europe`. Accessed on: Nov. 6, 2020.

[81] Aurora Telecom, "National network." [Online]. Available: `https://www.auroratelecom.ie/network-maps/national-network/`. Accessed on: Nov. 13, 2020.

[82] Timbercon, "Time delay of light in fiber calculator." [Online]. Available: `https://www.timbercon.com/resources/calculators/time-delay-of-light-in-fiber-calculator/`. Accessed on: Nov. 12, 2020.

[83] 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`, Apr. 2020. Accessed on: Nov. 12, 2020.

[84] 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`, Jun. 2020. Accessed on: Nov. 12, 2020.

[85] CERN, "Cern data centre." [Online]. Available: `https://home.cern/science/computing/data-centre`. Accessed on: Nov. 12, 2020.

[86] 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` Jun. 2017. Accessed on: Nov. 12, 2020.

[87] 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`, Apr. 2013. Accessed on: Nov. 12, 2020.

[88] 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/`, Sep. 2020. Accessed on: Nov. 12, 2020.

[89] Techquickie, "Servers vs desktop pcs as fast as possible." [Online]. Available: `https://www.youtube.com/watch?v=ByI1PHMcPJQ`, Jun. 2014. Accessed on: Nov. 12, 2020.

[90] Y. Xu, "Deconstructing the great firewall of china." [Online]. Available: `https://blog.thousandeyes.com/deconstructing-great-firewall-china/`, Mar. 2016. Accessed on: Nov. 14, 2020.

Appendices

Appendix 1: The testing program(Python code)

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

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

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

Appendix 5: The graphs in Chapter 5(Excel file)