

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 6, 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 6, 2020

Acknowledgments

...ACKNOWLEDGMENTS...

TUNG-TE LIN

University of Dublin, Trinity College
11 2020

Produce a technical plan for "Irish" Trusted Recursive Resolvers

Tung-te Lin, Master of Science in Computer Science

University of Dublin, Trinity College, 2020

Supervisor: Stephen Farrell

...ABSTRACT...

Summary

...SUMMARY...

Contents

Acknowledgments	iii
Abstract	iv
Summary	v
List of Tables	ix
List of Figures	xi
Chapter 1 Introduction	1
Chapter 2 The state of the art	3
2.1 The introduction of Domain Name Server	3
2.2 The problem of privacy	4
2.3 The solutions for privacy	5
2.4 The development of Trusted Recursive Resolver	8

Chapter 3	The required software	13
3.1	The overview of required software	13
3.2	The comparison and installation among DNS software applications . . .	15
3.3	Previous studies about the performance of DNS software	18
Chapter 4	The experiment	20
4.1	The implementation of the experiment	20
4.2	The test for the cache	24
4.3	The test for the 500 worldwide websites	26
4.4	The test for DNS types and DNS providers	30
4.5	The test for DNS record types	34
4.6	The test for query intervals	36
4.7	The test for different query times	38
Chapter 5	Overall design	41
5.1	The concern about DDOS attacks	41
5.2	The concern about the policy	43
5.3	The concern about the latency	45
5.4	The technical plan for constructing TRR in Ireland	48
Bibliography		52

List of Tables

2.1	The model of DOT [1]	7
2.2	The model of DOH [1]	7
2.3	The solutions for encrypting DNS queries	8
3.1	The required software for building a DNS server for TRR	15
3.2	The installation environment	17
3.3	The comparison among BIND, Unbound, PowerDNS	18
4.1	The testing environment of the experiment	21
4.2	The independent/controlled variables(parameters) in the experiment . .	22
4.3	The dependent variables(outputs) in the experiment	23
4.4	The controlled variable for testing the cache	25
4.5	The controlled variable for testing top 500 worldwide websites	27
4.6	The controlled variables for testing DNS types and providers	31
4.7	The controlled variables for testing DNS record types	34

4.8	The controlled variables for testing query intervals	36
4.9	The controlled variables for testing different query times	39

List of Figures

2.1	<i>The levels of authoritative DNS servers [2]</i>	4
2.2	<i>The queried website is revealed in packets if using the typical method to query website</i>	5
2.3	<i>The queried website can not be revealed in packets while using TRR in Firefox</i>	9
2.4	<i>The steps to enable TRR in Firefox - Part 1</i>	10
2.5	<i>The steps to enable TRR in Firefox - Part 2</i>	10
2.6	<i>DOH setting on Google Chrome</i>	12
3.1	<i>Users can customize the DOH provider by its domain name.</i>	16
3.2	<i>The records of successful DNS queries of TRR.</i>	17
4.1	<i>The screenshot of the testing program</i>	24
4.2	<i>The numbers of each result with flushed cache and non-flushed cache.</i>	25
4.3	<i>The average seconds of the responses with flushed cache and non-flushed cache.</i>	26
4.4	<i>The numbers of successful responses in testing top 500 worldwide websites.</i>	28

4.5	<i>The average seconds of successful responses in testing top 500 worldwide websites.</i>	28
4.6	<i>The numbers of results in each time the test in testing the top 50 world-wide websites</i>	29
4.7	<i>The average seconds of responses in each time the test in testing the top 50 worldwide websites</i>	30
4.8	<i>The numbers of all results in different DNS types(the local DNS server)</i>	31
4.9	<i>The average seconds of responses in different DNS types(the local DNS server)</i>	32
4.10	<i>The numbers of all results in different DNS types(the DNS server of Cloudflare)</i>	33
4.11	<i>The average seconds of responses in different DNS types(the DNS server of Cloudflare)</i>	33
4.12	<i>The numbers of all results in different DNS record types</i>	35
4.13	<i>The average seconds of responses in different DNS record types</i>	35
4.14	<i>The numbers of results in different DNS query intervals</i>	37
4.15	<i>The average seconds of responses in different DNS query intervals</i>	37
4.16	<i>The seconds of query sending durations in different DNS query intervals</i>	38
4.17	<i>The numbers of results in different query times</i>	39
4.18	<i>The average seconds of responses in different query times</i>	40
5.1	<i>The DDOS attack in recursive DNS queries [3]</i>	42
5.2	<i>Restricting DNS queries to prevent DNS amplification attacks [3]</i>	43

5.3	<i>Firefox with default setting can not browse a banned website.</i>	44
5.4	<i>Firefox can browse the banned website after enabling TRR.</i>	44
5.5	<i>The ranking of DNS providers by latency in Europe.</i>	46
5.6	<i>The distance of a very far place in the north from Dublin.</i>	47
5.7	<i>The distance of a very far place in the south from Dublin.</i>	47

Chapter 1

Introduction

The browser company Mozilla plans to promote the program Trusted Recursive Resolver(TRR) to provide better privacy compare to using traditional Domain Name Servers(DNS) [4]. This paper is going to analyze how a TRR plan could be applied in the Republic of Ireland from a technical view.

Chapter 2 “the state of the art” describes how a DNS server works, and the problem of privacy would have in using DNS servers. Next, it describes the solutions for dealing with the problem of privacy so far, including Domain Name System Security Extensions(DNSSEC) [5], DNSCrypt [6], DNS over TLS(DOT) [7], and DNS over HTTPS(DOH) [8]. Moreover, TRR is introduced here. The chapter explains why Mozilla created TRR, what is the relation between TRR and DOH, and why this study intends to discuss about the TRR program.

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

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

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

In Chapter 6, the overall design, which is the last chapter, is going to use the estimated DNS traffic in Chapter 3 and the evaluated performance of a DNS server in Chapter 5 to design a technical plan which can resolve the network traffic of the national scale in the Republic of Ireland.

Chapter 2

The state of the art

2.1 The introduction of Domain Name Server

Domain Name System(DNS) [4] is the server which converts the domain name to Internet Protocol(IP) address. Machines need the IP address to find out the location of another machine [9] [10], not domain name [11]. When users type the domain name on the browser, for example, type ‘www.dcard.tw’ on a browser, then the browser will send the domain name “www.dcard.tw” to a DNS server. After that, the DNS server responses the IP address of the domain name “104.16.204.58” to the browser. Finally, the browser is enable to connect to the server of “www.dcard.tw” by using the its IP “104.16.204.58”.

Moreover, there are 2 kinds of DNS servers: The recursive resolvers and the authoritative DNS server [12]. Recursive resolvers do not save all the IP addresses and domain names that users need. If users query the domain names that the recursive resolver does not know, then the recursive DNS resolver will inquire authoritative DNS servers about the IP address for the domain name. Next, the recursive resolver saves the domain name and its IP address in the cache, in case any users use this domain name in a short time, then the recursive resolver is able to reply its IP address immediately and not to inquire authoritative DNS servers again.

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

Furthermore, authoritative DNS servers are hierarchical [2]. The highest one is called a root server. A top-level authoritative DNS server can respond with an address of a low-level authoritative DNS server to users for their inquiry, and that lower level authoritative DNS server may have the IP address that users need. In that case, a authoritative DNS server does not need to save entire IP addresses and domain names, the workload can be divided. The levels of authoritative DNS servers are shown in Fig. 2.1.

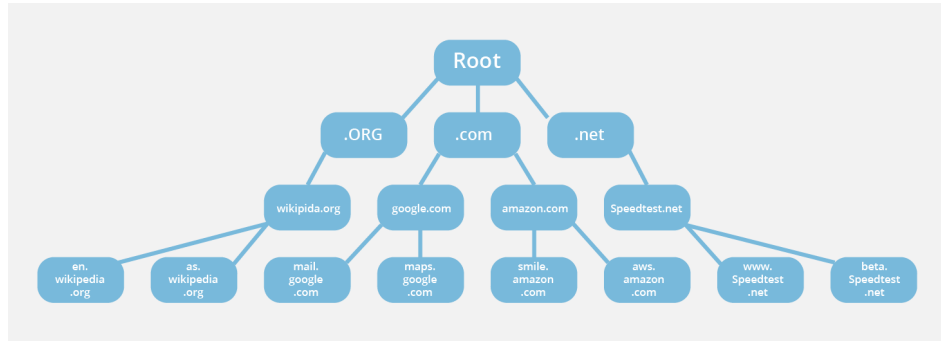


Figure 2.1: *The levels of authoritative DNS servers [2]*

2.2 The problem of privacy

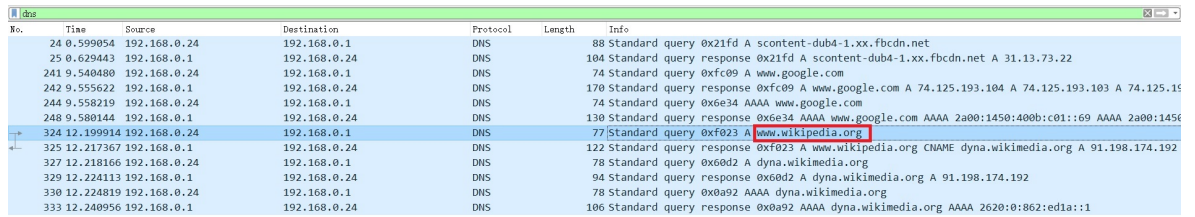
Request For Comments(RFC) [13] is the publication which is managed by Internet Engineering Task Force(IETF). IETF is the organization to design the standard of Internet [14].

RFC7626 [15] and its draft [16] discussed the problem of privacy in using a DNS server. The personal data could be discovered in the DNS servers, wire or DNS requests, including the IP of clients, the domain names which are researched by users, and even the applications that users use.

The root cause of this privacy problem is that the typical DNS traffic is not encrypted. On the other hand, DNS servers, especially recursive resolvers, they store the data of DNS queries in their log or cache. Thus the DNS providers are able to use the data to do some analysis or transfer the data to others. As for authoritative DNS servers, the privacy problem is lighter than recursive resolvers, because their cache is too limited to store the completed data [15].

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

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



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 74.125.193.102
244	9.558219	192.168.0.24	192.168.0.1	DNS	74	Standard query 0xe634 AAAA www.google.com
248	9.580144	192.168.0.1	192.168.0.24	DNS	130	Standard query response 0xe634 AAAA www.google.com AAAA 2a00:1450:400b:c01::69 AAAA 2a00:1450:400b:c01::68
324	12.199914	192.168.0.24	192.168.0.1	DNS	77	Standard query 0xf023 A www.wikipedia.org
325	12.217367	192.168.0.1	192.168.0.24	DNS	122	Standard query response 0xf023 A www.wikipedia.org CNAME dyna.wikimedia.org A 91.198.174.192
327	12.218166	192.168.0.24	192.168.0.1	DNS	78	Standard query 0x60d2 A dyna.wikimedia.org
329	12.224113	192.168.0.1	192.168.0.24	DNS	94	Standard query response 0x60d2 A dyna.wikimedia.org A 91.198.174.192
330	12.224819	192.168.0.24	192.168.0.1	DNS	78	Standard query 0x0a92 AAAA dyna.wikimedia.org
333	12.240956	192.168.0.1	192.168.0.24	DNS	106	Standard query response 0x0a92 AAAA dyna.wikimedia.org AAAA 2620:0:862:ed1a::1

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

2.3 The solutions for privacy

According to the description of RFC7626 [15], revealing the content of DNS queries can cause severe privacy problems. People may not be willing to let others to find what websites they browse. Thus, some solutions were created. There are 4 popular solutions to improve the privacy of DNS and they are widely used in different public DNS servers, which are Domain Name System Security Extensions(DNSSEC), DNS over TLS(DOT), DNS over HTTPS(DOH) and DNSCrypt [17].

The first solution is DNSSEC, it is not only the oldest but also the most popular solution among those 4 solutions [17]. It was created in 1997. The concept is making an extension of DNS to check the digital signature [5], 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 [18].

The second solution is DNSCrypt. Unlike other 3 solutions, it does not follow any RFC, because it was a private standard. The creator is OpenDNS and it was announced in 2011. DNSCrypt does not use digital signatures, it uses cryptographic construction to encrypt queries [6].

The biggest problem is that it does not follow RFC, which means it is not proposed by IETF. Therefore it is just a private standard, not a public standard, then it is hard to be widely used by DNS providers and application developers. For example, the famous public DNS providers Cloudflare and Google do not support DNSCrypt [17].

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 [7]. Compare to DNSSEC and DNSCrypt, it has a lot of advantages. For example, it does not need a high performance to process encryption. The packet is encrypted, thus it can prevent a man-in-the-middle attack(MITM) [19]. Moreover, DOT follows RFC, therefore it uses a public standard which is proposed by IETF, hence it can be widely used by many DNS providers and developers.

The newest one among those 4 solutions is DOH. It was introduced in 2018, but it is in testing [8]. DOH is similar to DOT, both DOH and DOT are utilizing TLS to be the tool to encrypt DNS queries. The different is that DOT uses TLS directly, in contrast, there is a protocol between DOH and TLS in the DOH model, which is HTTPS. HTTPS also uses TLS, thus DOH uses TLS indirectly and uses HTTPS

directly [1]. The models of DOT and DOH are shown in Table 2.1 and Table 2.2.

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

Table 2.1: The model of DOT [1]

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

Table 2.2: The model of DOH [1]

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

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

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

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

Solutions	DNSSEC	DNSCrypt	DOT	DOH
Introduced	1997	2011	2016	2018
RFC	4033,4034,4035	None	7858,8310	8484

Table 2.3: The solutions for encrypting DNS queries

2.4 The development of Trusted Recursive Resolver

As RFC7626 mentioned [15], the personal data could be revealed in the DNS traffic or DNS servers. About the DNS traffic, it can be encrypted by above 4 solutions in the last section. As for the DNS servers, it need another means to resolve the problem of privacy.

In this background, the concept of Trusted Recursive Resolver(TRR) [20] was designed by Mozilla for protecting privacy. On the one hand, TRR requires recursive resolvers use DOH to encrypt the content of DNS queries, on the other hand, recursive resolvers have to be supervised. Thus, the personal data both in DNS traffic and DNS servers can be protected from eavesdroppers or taken by others.

Cloudflare, NextDNS and Comcast are the 3 DNS providers who have joined the TRR program so far [21]. There are 3 regulations in the supervision to recursive resolvers in the TRR program [22].

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

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

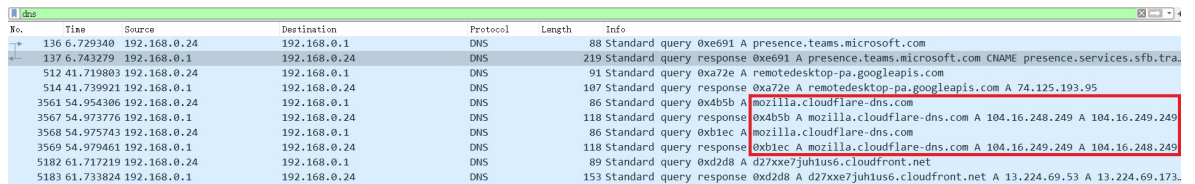
The third one, the data in recursive resolvers can not be blocked, filtered, modified, the exception is “required by law”.

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

so-called “Trusted Recursive Resolver”.

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

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



No.	Time	Source	Destination	Protocol	Length	Info
136	6.729340	192.168.0.24	192.168.0.1	DNS	88	Standard query 0xe691 A presence.teams.microsoft.com
137	6.743329	192.168.0.1	192.168.0.24	DNS	219	Standard query response 0xe691 A presence.teams.microsoft.com CNAME presence.services.sfb.tra.
512	41.719803	192.168.0.24	192.168.0.1	DNS	91	Standard query 0xa72e A remotedesktop-pa.googleapis.com
514	41.739921	192.168.0.1	192.168.0.24	DNS	107	Standard query response 0xa72e A remotedesktop-pa.googleapis.com A 74.125.193.95
3561	54.954386	192.168.0.24	192.168.0.1	DNS	86	Standard query 0x4b5b A mozilla.cloudflare-dns.com
3567	54.973776	192.168.0.1	192.168.0.24	DNS	118	Standard query response 0x4b5b A mozilla.cloudflare-dns.com A 104.16.248.249 A 104.16.249.249
3568	54.975743	192.168.0.24	192.168.0.1	DNS	86	Standard query 0xb1ec A mozilla.cloudflare-dns.com
3569	54.979461	192.168.0.1	192.168.0.24	DNS	118	Standard query response 0xb1ec A mozilla.cloudflare-dns.com A 104.16.249.249 A 104.16.248.249
5182	61.717219	192.168.0.24	192.168.0.1	DNS	89	Standard query 0xd2d8 A d27xxe7juh1us6.cloudfront.net
5183	61.733824	192.168.0.1	192.168.0.24	DNS	153	Standard query response 0xd2d8 A d27xxe7juh1us6.cloudfront.net A 13.224.69.53 A 13.224.69.173.

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

Enabling the TRR function in Firefox is quite simple, only few steps to enable it. The steps are shown in Fig. 2.4 and Fig. 2.5. Compare to DOT, DOT can run on Android and IOS, but it needs some tools to run on Linux and Windows, thus it is more inconvenient [7].

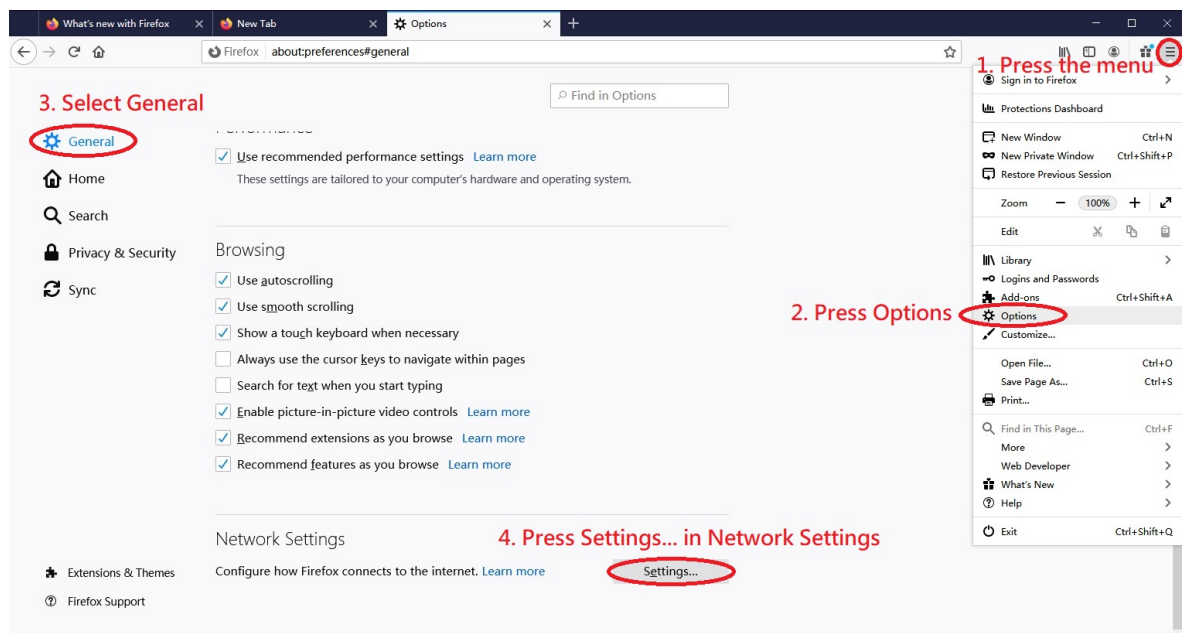


Figure 2.4: The steps to enable TRR in Firefox - Part 1

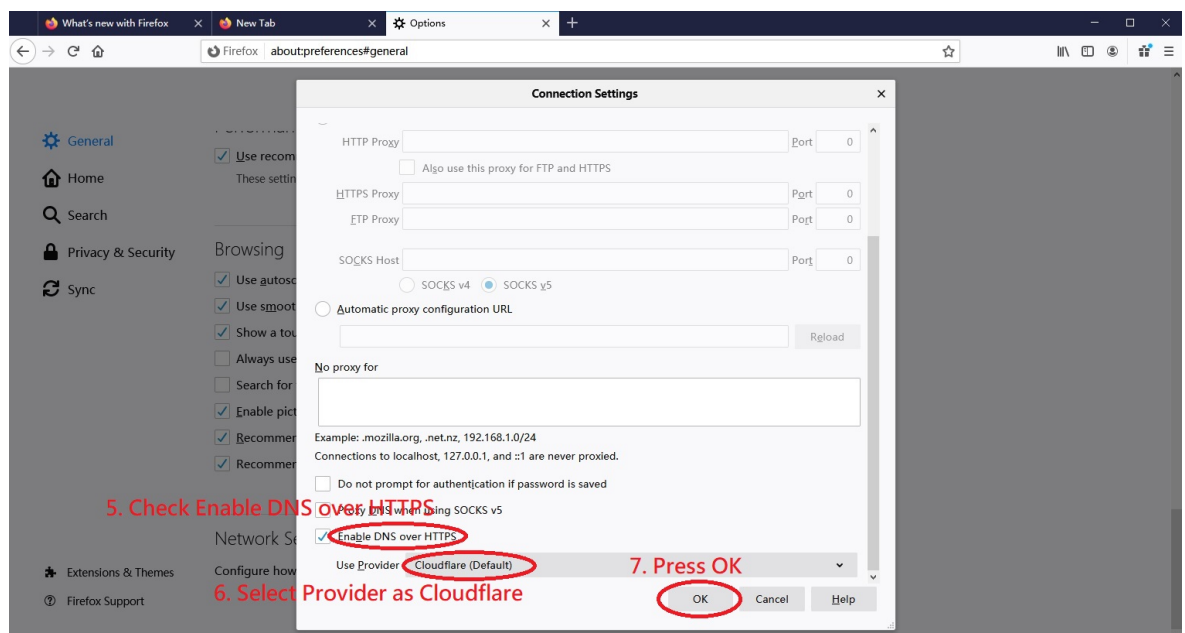


Figure 2.5: The steps to enable TRR in Firefox - Part 2

Furthermore, Mozilla is also devoted in pushing TRR. In February 2020, Mozilla set TRR as the default setting of Firefox in USA, which means Firefox users used the DOH service if they do not do any change [23].

However, this policy caused a severe problem, after the TRR function was set as default setting in Firefox, the DNS provider NextDNS suffered a very high workload and struggled to handle the high traffic volume. It seems like a kind of DDOS attacking to those DNS providers, therefore Mozilla had to change the policy. In the later version Firefox 77.0.1 in June 2020, TRR has been removed the default setting, now users have to set the TRR function by themselves manually if they wish to enjoy DOH service [24].

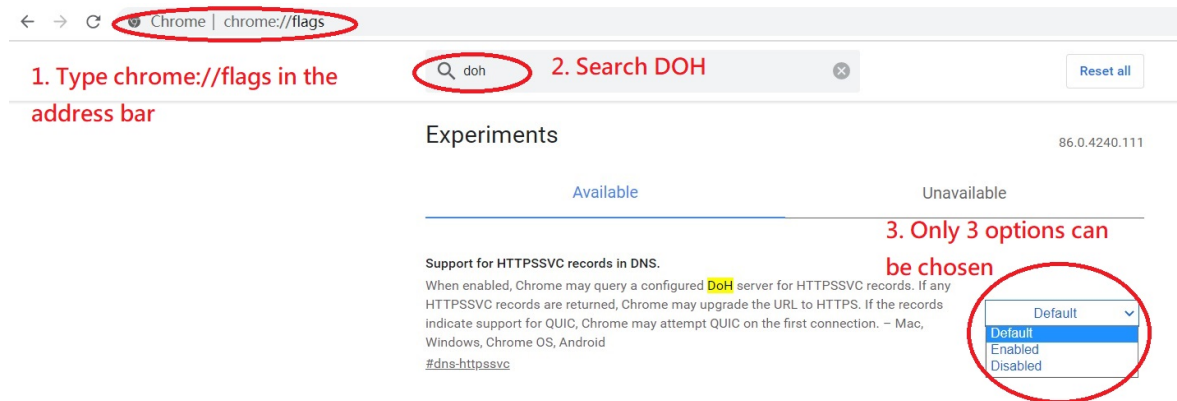
Hence, The time TRR been default setting was only lasted about 4 months(from February 2020 to June 2020). If Mozilla wants to make TRR being the default again, then the performance of DOH DNS servers must be capable to process the DNS queries of national scale.

As for Google Chrome, the main competitor to Mozilla Firefox, Chrome also supports DOH, and Google also intended to adjust DOH service to be the default setting for DNS queries as well [25].

The difference is that, the policy Google adopted is not TRR, because TRR is the unique program to Mozilla and its browser Firefox. The policy Google adopted is automatic upgrade. Which means, if the criteria that users have is met the requirement for using DOH service, then Chrome will change the setting to be DOH and users do not need to do anything. Google has already implemented this function in Chrome version 83 in May 2020 [26].

Another difference is that Chrome can not customize a DOH server in the browser, the options are only default, enabled and disabled in the DOH setting. Users have to set a DNS server which supports DOH in their operating systems. Contrarily, Firefox is more flexible, users are able to set a DOH DNS server which is different from the DNS server in their operating system. Therefore, it is easy to test or use a private DOH DNS server [27].

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

Figure 2.6: *DOH setting on Google Chrome*

Not only Firefox and Chrome support DOH, but also other browsers, such as Opera [28], Microsoft Edge and Vivaldi [29]. Every companies or browser has their own plans to support DOH, those plans may be different and have their features, advantages and disadvantages.

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

Chapter 3

The required software

3.1 The overview of required software

There are 2 kinds of DNS servers, authoritative DNS servers and recursive resolvers. The DNS software we talk about here is the software to build a recursive resolver. There are many choices to implement a DNS server, such as BIND, Unbound, DNSMASQ, PowerDNS, Microsoft DNS and Cisco Network Registrar [30] [31].

In this study, Unbound, BIND and PowerDNS are recommended, because there are many discussions and tutorials about those three software on Internet [32] [33] [34]. Thus, people may be easy to use them to build private or public recursive resolvers.

Unbound is the free open-source software which focuses on building a recursive DNS server, it does not support the authoritative DNS server. The developer is NL-net Labs, the developer also designed another DNS software, which is NSD(Name Server Daemon), in contrast, NSD is only for building authoritative DNS servers [35]. 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 [36].

About BIND, its alias is Named. Unlike Unbound, it supports both recursive and

authoritative DNS servers. It is developed by Internet Systems Consortium(ISC). ISC is also the organization which is responsible for managing F root server zone. The stable version is BIND 9. It can run on Windows, Mac-OS and Linux [37].

PowerDNS, it 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 Community and operating systems are Linux and FreeBSD [38].

Apart from DNS software, building a DNS server for TRR also needs other some software, including operating systems, DOH tools and HTTP servers [39] [32].

The DOH DNS server need DOH tools to receive DoH queries and test. doh-proxy is designed for this purpose, the developer is Facebook. It can be installed on Linux but it requires Python 3.5 [40]. 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 HTTP service. NGINX is a HTTP server with high performance, it can also provide different kinds of services. The operator can set the method for listening queries from users [41].

In choosing a operation 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, including Fedora, Red Hat Linux, CentOS, Ubuntu, Debian [42]. 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 3.1.

Category	Software	Note
DNS	BIND	
DNS	Unbound	Free and open-source software
DNS	PowerDNS	
DOH Tool	doh-proxy	
HTTP Server	NGINX	Free and open-source software
Operating System	Linux	Windows can be used as well

Table 3.1: The required software for building a DNS server for TRR

3.2 The comparison and installation among DNS software applications

In order to understand the situation of the setting and usability among BIND, Unbound and PowerDNS, the researcher tried to install those 3 DNS software on the local server and test them.

Due to the effect of Coronavirus(COVID-19) pandemic, students were not allowed to go inside the laboratory, hence this study has to be finished at home, therefore the equipment was limited, only 4 personal devices were available to the researcher, which were a personal desktop computer, 2 android phones and a iPad. The operating system on the personal desktop computer is Windows 10. Thus, there was no spare computer to install Linux, the researcher had to use a virtual machine to install Linux on the personal computer. The software for running virtual machine was VMware Workstation Player.

After installing the operation system, then 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, used Internet Information Services(IIS) to create a simple website on the personal computer, and gave fixed local IP addresses to all devices and the virtual

machine, then both the DNS server and website had the IP addresses. In the DNS server(BIND, Unbound and PowerDNS), set a domain name to the simple website to match its IP address. This simple website was the website for testing.

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

As for DOH service, the study also added it on the local DNS server and tested it. After the implementation of DOH service, the researcher enabled the TRR function in Firefox and input the domain name of the local DNS server in the TRR customized DOH provider to test it. The TRR function was working well on Firefox, therefore this local DOH server with its configuration can be the DNS server for TRR. The screenshots were displayed in Fig. 3.1 and Fig. 3.2. “vm.tcdtrr.ie” is the domain name of the local server which was built by the researcher.

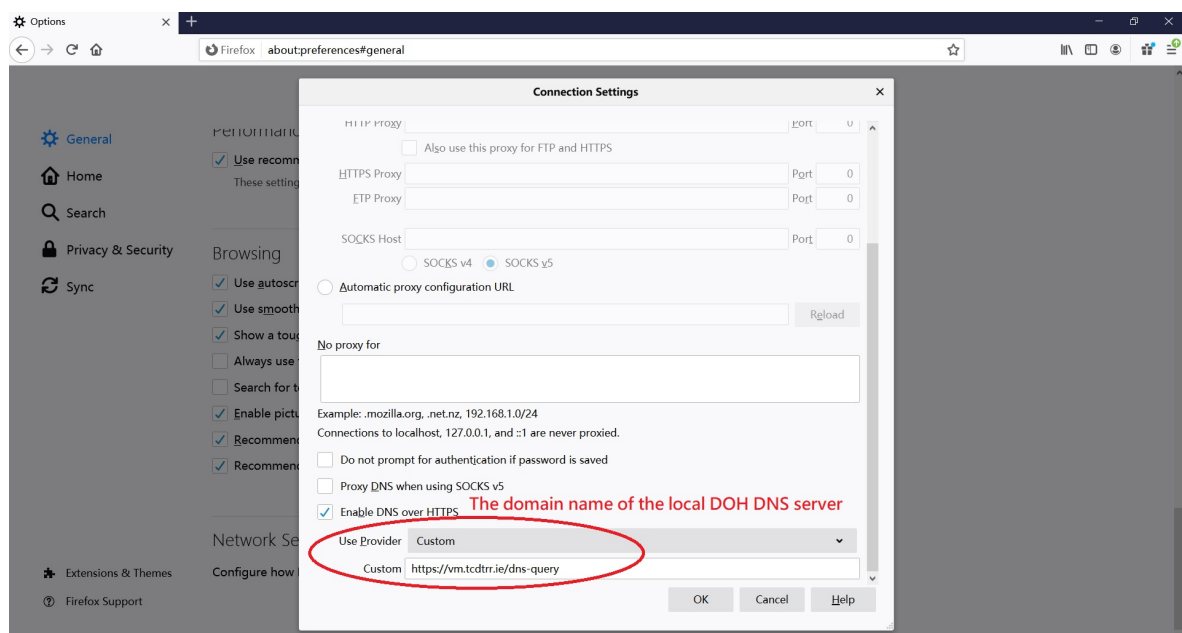


Figure 3.1: Users can customize the DOH provider by its domain name.

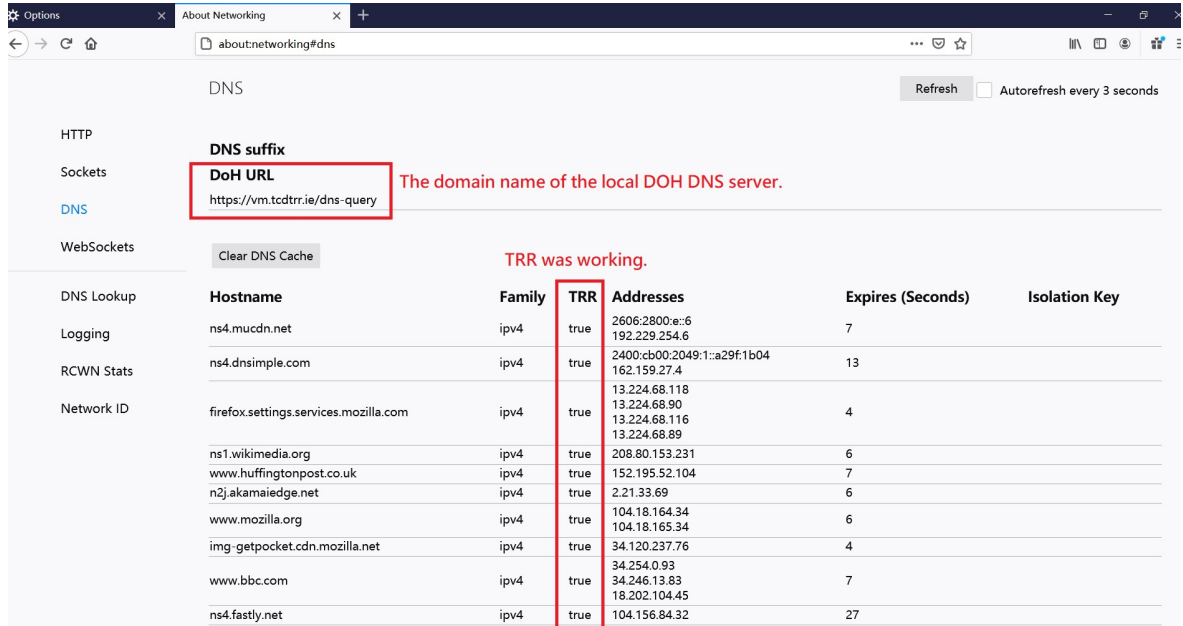


Figure 3.2: The records of successful DNS queries of TRR.

Above steps were the testing method for the study. The testing environment is shown in TABLE 3.2.

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 3.2: The installation environment

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

About Unbound, the format of configuration file is very simple, it does not belong

to any kind of computer languages. The setting is just listed line by line.

PowerDNS adopts relational database, thus the configuration of PowerDNS has 2 parts, the first part is the normal configuration file, it decides the setting for the database. The second part is in the database, the contain is including domains and records.

The installation of PowerDNS is more complex than Unbound and BIND, because it uses the rational database. However, it is a double-edged sword, it is not friendly for normal users during the installation, but after installation, PowerDNS provides the website interface to display the information of the DNS server, and the website is also the interface for the setting, hence the maintenance is easier than BIND and Unbound.

The comparison among BIND, Unbound, PowerDNS is shown in Table 3.3.

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

Table 3.3: The comparison among BIND, Unbound, PowerDNS

3.3 Previous studies about the performance of DNS software

According to a report which was written by Hamza Boulakhrif in University of Amsterdam, the times for processing queries in BIND, Unbound and PowerDNS were similar. The biggest difference was that when the time of processing exceeded 16 seconds, then PowerDNS did not response. If the time exceeded 17 seconds, BIND did not response, only Unbound can wait until the finish of processing then sent results to users [43].

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

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

The regulation in BIND and PowerDNS are similar, both of them have the time limit, thus in case the processing time reaches the time limit, then the query will be failed. In contrast, Unbound has a different working type, it allows the system to have a long time to wait for the answer after the process. Hamza Boulakhrif called those different working types as "Failed response over a late response" and "An answer is better than no answer". PowerDNS adopts "Failed response over a late response" and Unbound adopts "An answer is better than no answer", as for BIND, it is between PowerDNS and Unbound [43].

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

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

Chapter 4

The experiment

4.1 The implementation of the experiment

In order to understand the performance of a DOH server, the researcher designed an experiment. Unfortunately, the moment during this studying encountered Coronavirus disease(COVID-19) pandemic, it was mandatory to stay at home, hence the researcher has to use the personal computer and the home network to finish this study. The results may be worse than a DNS server in a formal data center.

First of all, a DOH server was built in the local network. After that, used Python to design a testing program. The function of the testing program was sending massive DNS queries to the 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 4.1.

The testing program utilized multi-thread to send queries, thus queries can be sent in a very short time. 50 to 500 queries can be sent between 0.1 and 0.4 seconds. The outputs of this testing program are CSV files, those CSV files contain the records and statistic of the tests in this experiment.

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

Table 4.1: The testing environment of the experiment

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 [44] in this experiment. The variables are shown in Table 4.2. The independent variables were the changed parameters and the controlled variables were the unchanged ones.

Independent variables	Options
Cache	Flushed cache, Non-flushed cache
Query name	The top 50 websites in Ireland, the top 500 websites in the world
Record type	A, AAAA, CNAME, MX
DNS type	DOH(Wireformat), DOH(JSON), Traditional DNS
DNS provider	Local(Built by the researcher), Cloudflare
Query interval	No interval, 0.1 Sec., 0.01 Sec. 0.001 Sec.
Query time	Peak time, Off-peak time

Table 4.2: The independent/controlled variables(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, those data can be used to conclude how many DOH DNS servers should have in Ireland. The dependent variables(output) are shown in Table 4.3.

There are 4 results of responses, which are success, NXDomain, no answer, and others. Success is that the query is successful to get the IP address from the response from the DNS server. NXDomain stands for Non-existent Internet domain name [45], which means the DNS server can not find the matched IP address for the queried domain name. The third result is no answer, if the DNS server respond any error message or no message, then the result is classified as no answer. The last one is others, if the query can not reach the DNS server, or the DNS server does not return the response, or any other situations happen, then those results are others.

The result "Others" was unusual, in the most tests, there was no others, only success, NXDomain, and no answer happened. The exception was testing the traditional DNS server, because timeout could happen, then it was categorized as others. Thus, in following sections, the graphs do not display the result "other" if the number of others was 0.

Dependent variables	Outputs
The results of responses	Success, NXDomain, No Answer, Others
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 4.3: The dependent variables(outputs) in the experiment

The screenshot of the testing program is displayed in Fig. 4.1. It runs as a Python application, and the researcher is able to input parameters by keyboard. All results, including the statistic and the results of all responses are saved into 2 CSV files.

```

C:\test>python dns_test.py
Choose the kind of domain:
1:local domain
2:fake domains
3:top 50 Ireland websites(default)
4:top 500 world websites
4
Query interval(second)?(0:no interval(default),1:0.1,2:0.01,3:0.001,4:0.0001)
0
Query type?(1:A(default),2:AAAA,3:CNAME,4:MX)
1
Query Method?(1:DOH Wireformat(default),2:DOH JSON,3:Tradition)
1
DNS Server?(1:local(default),2:cloudflare,3:google)
1
Query number?(default:50)
50
Note?(optional, default is no blank)
test
Start Time: 2020-11-01 14:16:56.725856
End Time: 2020-11-01 14:16:56.850849
Query Duration: 0.124993
The responses of all domain names have been recorded in
World_test_A_Wireformat_Local_50_0_2020-11-01-14-16-56.csv.
The statistic has been generated in statistic.csv.
C:\test>_

```

Figure 4.1: *The screenshot of the testing program*

4.2 The test for the cache

The experiment was separated into different small tests to test the effect from each variable.

The first test was cache. DNS servers use cache to save the IPs of used queries. If the user sends an used query again, the DNS server does not need to ask the authoritative DNS server again, just response the IP in the cache immediately, then it could save a lot of time. The controlled variables are shown in Table 4.4.

Controlled variables	Parameters
Query name	The top 50 websites in Ireland
Record type	A
DNS type	DOH(Wireformat)
DNS provider	Local(Built by the researcher)
Query interval	No interval
Query time	From 23:18:59 to 23:19:54 25/10/2020

Table 4.4: The controlled variable for testing the cache

The testing steps were that, firstly, typed "rndc flush" in Linux to flush the cache of BIND, then there was no IP record in the DNS server. Next, ran the testing program to gain the data with the flushed cache. After that, the IP records existed in the cache of DNS, then ran the testing program again to get the data without flushing cache (Non-flushed cache). The distribution of results is displayed in Fig. 4.2 and Fig. 4.3.

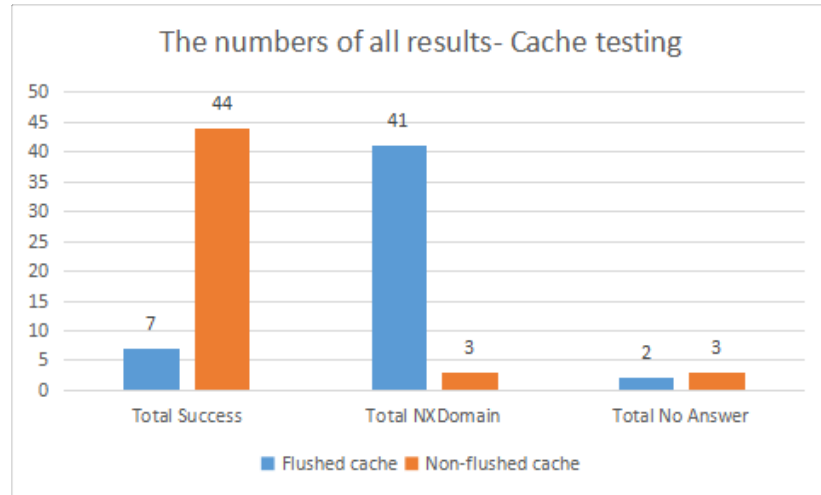


Figure 4.2: The numbers of each result with flushed cache and non-flushed cache.

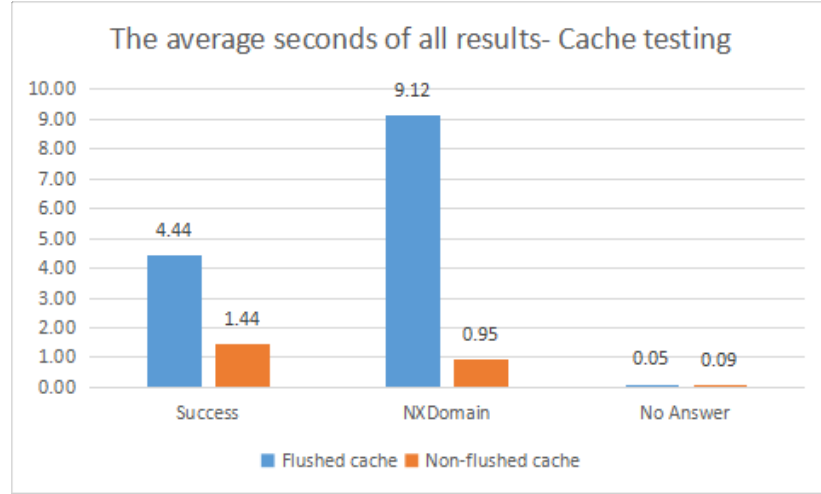


Figure 4.3: *The average seconds of the responses with flushed cache and non-flushed cache.*

The results showed that it was a huge difference, the almost responses with non-flushed cache were successful, contrarily, the almost responses with the flushed cache were failed. As for the average time of responses, the flushed cache also needed several times the time more than the non-flush cache to respond the client.

4.3 The test for the 500 worldwide websites

Next test was using the top 500 worldwide websites to test the DOH server. There were 2 kinds of websites in this experiment, the top 50 websites in Ireland, and the top 500 websites in the world. The ranking of the top 500 websites was decided by the score given from Moz.com [46], the accessed date was 13 October 2020. About the top 50 websites in Ireland, the meaning 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 [47], the accessed date was 25 October 2020.

Alexa.com is the company which makes the ranking to websites by popularity. The ideal samples should be the top 500 websites in Ireland, because this study planned to

use the huge number of websites to test, and the target is Ireland. Unfortunately, it needs to pay for the data, only the ranking of the top 50 websites is free. On the other hand, Moz.com provides their own ranking for the top 500 websites for free. Hence, in testing a huge number of websites, the study adopted the data from Moz.com, which is the top 500 websites in the world. As for other tests, the study just used the data from Alexa.com, which is top 50 websites in Ireland.

The testing steps were that, firstly, flushed the cache to remove all records in the DNS server. Secondly, queried top 500 worldwide websites 5 times in a row without flushing the cache. The controlled variables(fixed parameters) are shown in Table 4.5, and the distributions of results are displayed in Fig. 4.4 and Fig. 4.5.

Controlled variables	Parameters
Query name	The top 500 websites in the world
Record type	A
DNS type	DOH(Wireformat)
DNS provider	Local(Built by the researcher)
Query interval	No interval
Query time	From 7:34:15 to 7:39:48 29/10/2020

Table 4.5: The controlled variable for testing top 500 worldwide websites

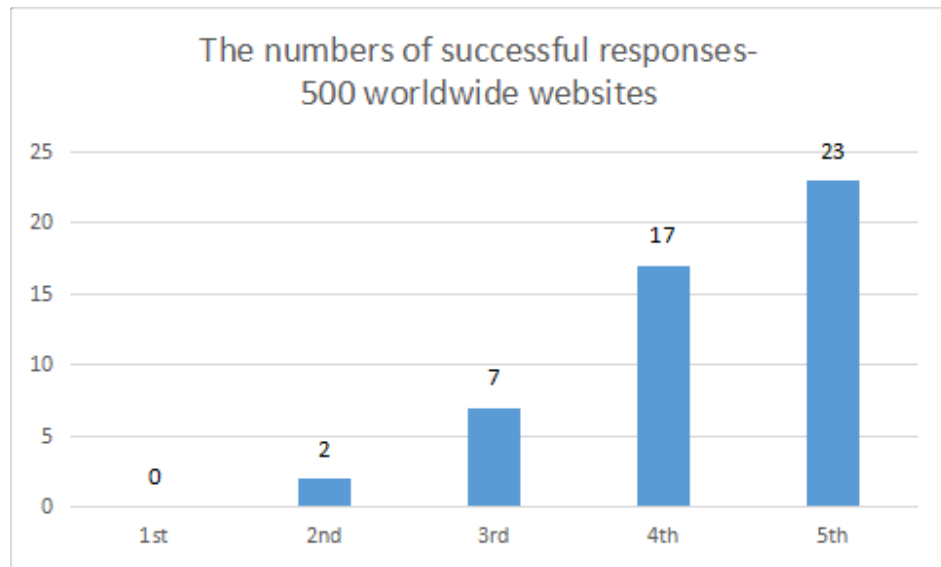


Figure 4.4: *The numbers of successful responses in testing top 500 worldwide websites.*

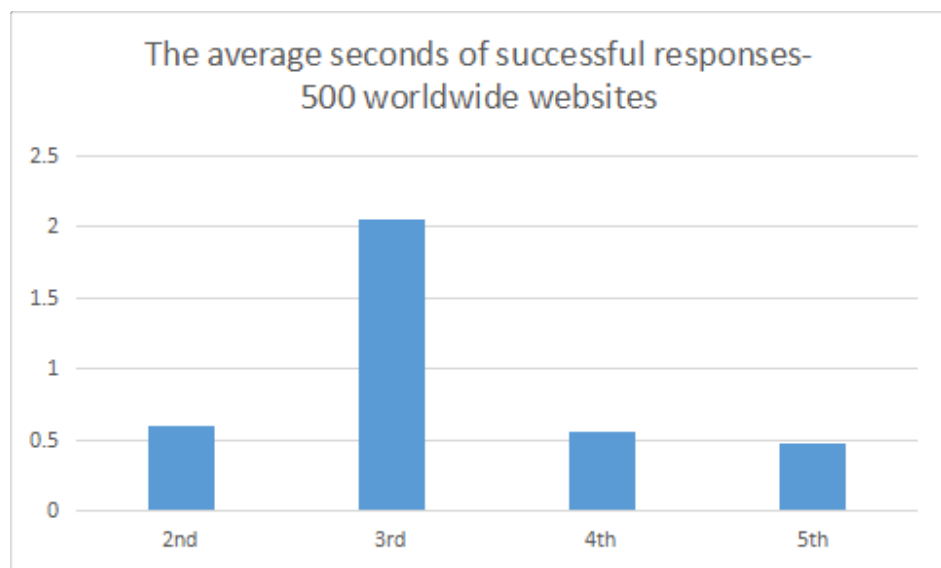


Figure 4.5: *The average seconds of successful responses in testing top 500 worldwide websites.*

The figures showed that the performance of querying 500 websites was far lower than the results in querying 50 websites. No response was successful in the first time of

the test. In the third time of the test, the average seconds was obviously longer than other times, because a response of a website spent 10.29 seconds.

Maybe the problem was from websites themselves, therefore, the study decided to make another test, just used the top 50 websites of the top 500 worldwide websites to query 5 times again. The results were shown in Fig.4.6 and Fig.4.7.

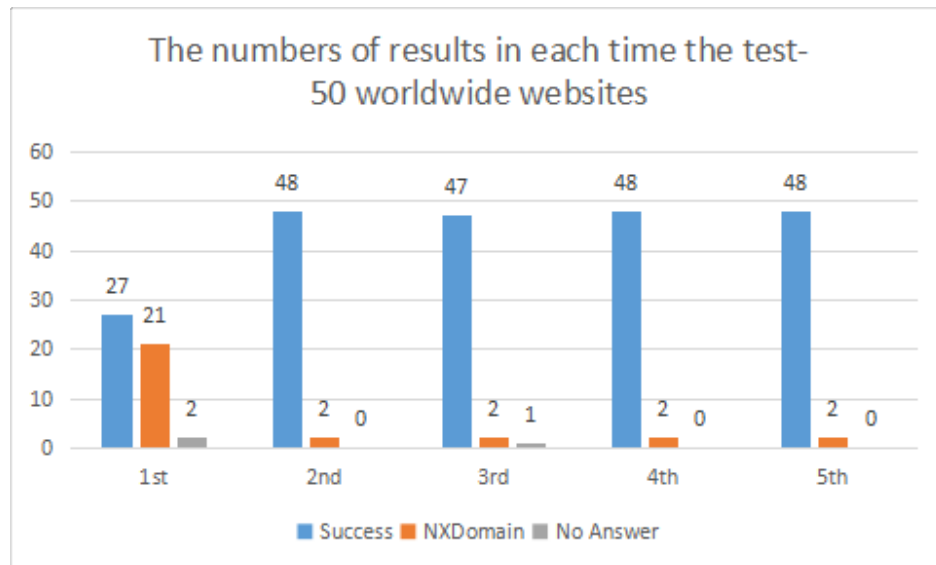


Figure 4.6: *The numbers of results in each time the test in testing the top 50 worldwide websites*

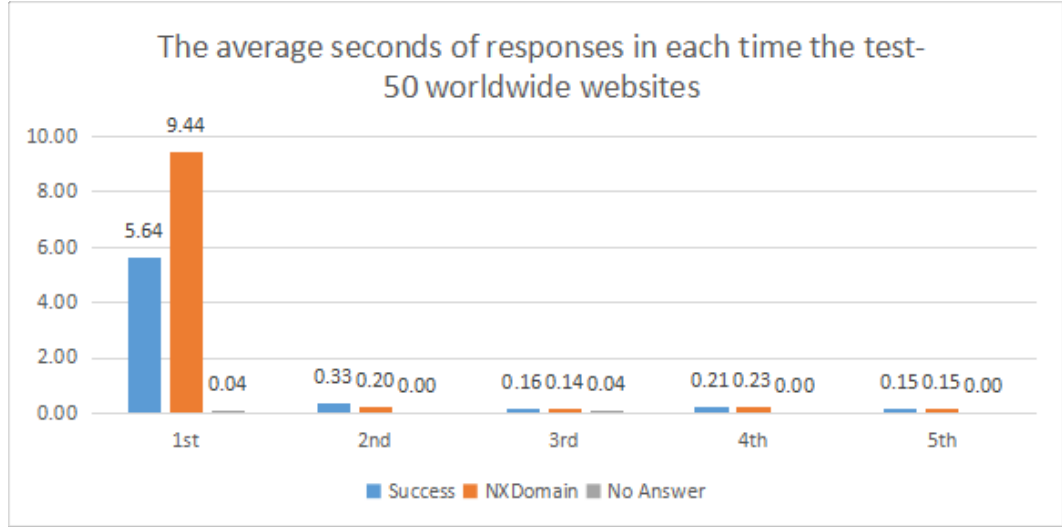


Figure 4.7: *The average seconds of responses in each time the test in testing the top 50 worldwide websites*

The results in testing the top 50 worldwide websites were similar to the results in testing the top 50 Irish websites, but number of successful responses was higher than the Irish one. Hence, the study assumes that the main reason to cause lower performance was too many queries in a short time.

4.4 The test for DNS types and DNS providers

This test was testing the difference of performance between the traditional DNS service and the DOH service. Moreover, there are 2 kinds of queries used in DOH querying, which are Wireformat [48] and JavaScript Object Notation(JSON) [49] [50]. However, the local DOH server did not response the query with JSON format, therefore the study used both the DNS server of Cloudflare and the local DOH server to test the DNS types. The cache was also flushed before testing in the local DOH server, but the cache of the DNS server of Cloudflare can not be flushed, because it is the public DNS server. The parameters were shown in Table 4.6. The results were displayed in Fig. 4.8, Fig. 4.9, Fig. 4.10, and Fig. 4.11.

Controlled variables	Parameters
Query name	The top 50 websites in Ireland
Record type	A
Query interval	No interval
Query time	From 4:51:51 to 4:56:57 2/11/2020

Table 4.6: The controlled variables for testing DNS types and providers

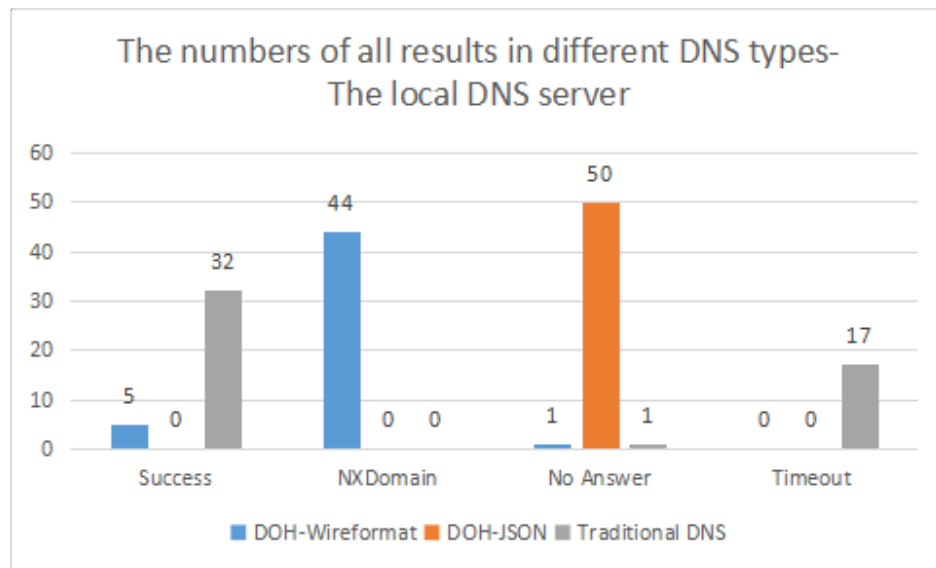


Figure 4.8: The numbers of all results in different DNS types(the local DNS server)

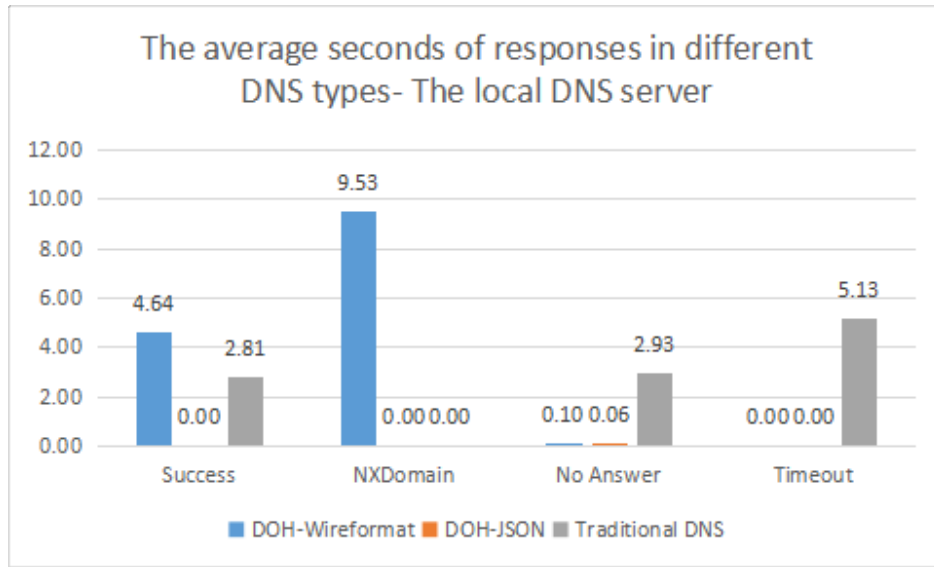


Figure 4.9: *The average seconds of responses in different DNS types(the local DNS server)*

In the test to the local DNS server, the timeout happened in the traditional DNS service. The default timeout is 5 seconds in BIND 9(the DNS software used here), the researcher did not change it. Contrarily, there was no timeout in the DOH service. Moreover, JSON format was not accepted in the local DOH service, thus it may need extra configuration to enable the function. Another noticeable difference was that the performance of DOH(Wireformat) was much lower than the traditional DNS. The successful responses were fewer and the average seconds of responses was longer in testing the DOH service.

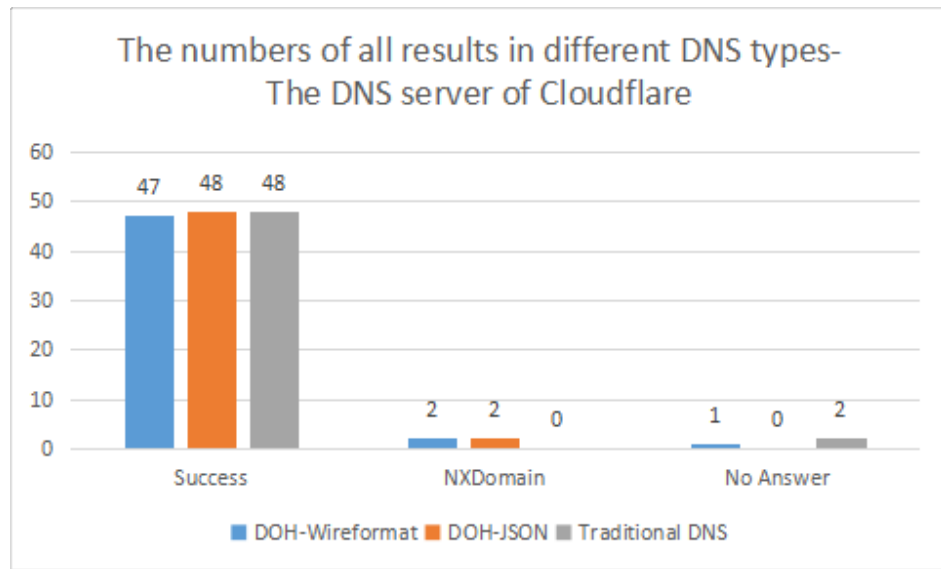


Figure 4.10: *The numbers of all results in different DNS types(the DNS server of Cloudflare)*

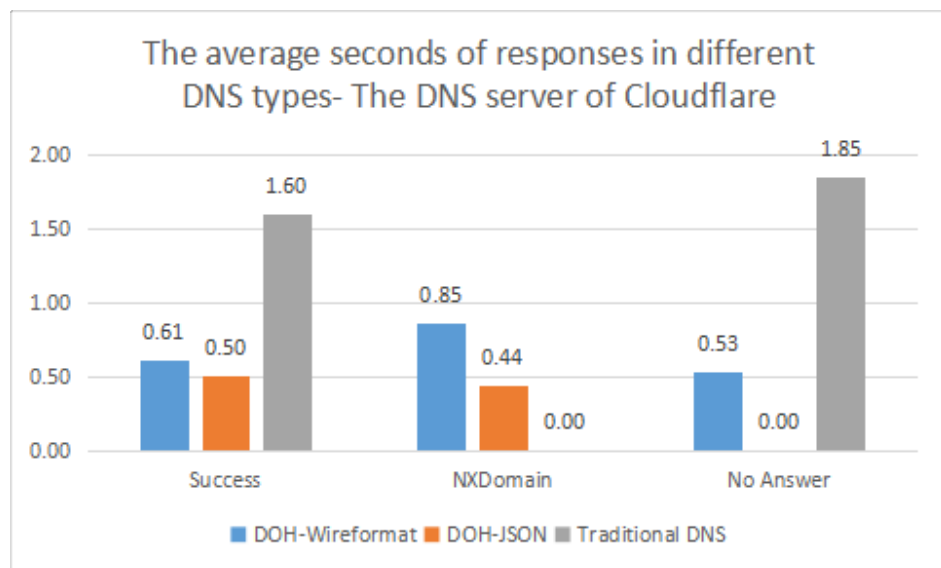


Figure 4.11: *The average seconds of responses in different DNS types(the DNS server of Cloudflare)*

As for testing the DNS server of Cloudflare, the JSON format worked, but the

cache can not be flushed, thus the performance could not be compared to the local DNS server. Overall, the results were good, the most responses were successful, the reason may be caused by using the data in the cache to respond.

However, there was a difference, the average seconds of responses in DOH service were shorter than the traditional DNS service, which means this result was different from the test in the local DNS server. Therefore, the study can not judge that which has better performance between DOH or the traditional DNS.

4.5 The test for DNS record types

The DNS record types [51] were also tested here. There are many DNS record types, but this study just used 4 types, which were A, AAAA, CNAME and MX.

A is getting the IP address of IPv4 [9], it is the most popular DNS record type so far. AAAA is getting the IP address of IPv6 [10]. CNAME stands for Canonical Name, it is used to getting the domain name alias. MX stands for Mail Exchange, it is used to getting the e-mail server.

The controlled variables(parameters) were set as Table 4.7. The cache was also flushed before testing. The results were shown in Fig. 4.12 and Fig. 4.13.

Controlled variables	Parameters
Cache	Flushed cache
Query name	The top 50 websites in Ireland
DNS type	DOH(Wireformat)
DNS provider	Local(Built by the researcher)
Query interval	No interval
Query time	From 9:56:49 to 9:58:39 2/11/2020

Table 4.7: The controlled variables for testing DNS record types

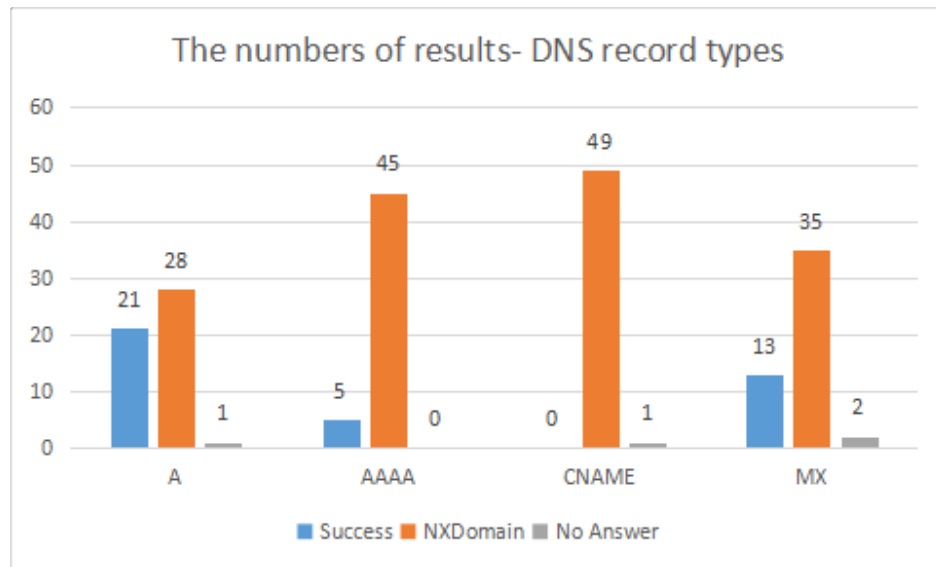


Figure 4.12: *The numbers of all results in different DNS record types*

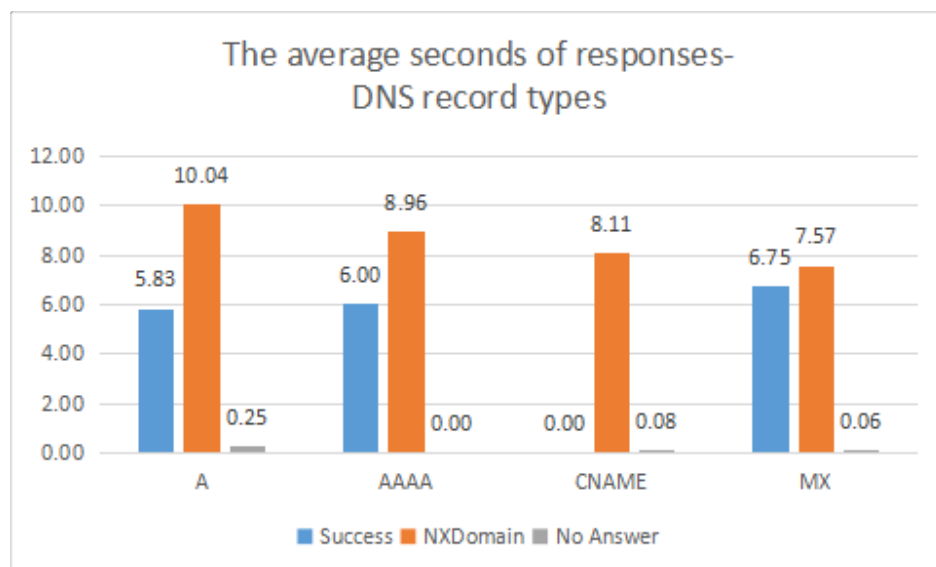


Figure 4.13: *The average seconds of responses in different DNS record types*

The results showed that only a few websites in the top 50 websites in Ireland have AAAA or MX and no CNAME was found in this test. Thus, the study just utilized the 5 successful samples of AAAA and the 13 successful samples of MX to analyze the

results.

In those successful responses of AAAA and MX, the average seconds were close to the average seconds of type A. Hence, the study supposes that different DNS record types can function well if the domain has the type apart from type A.

4.6 The test for query intervals

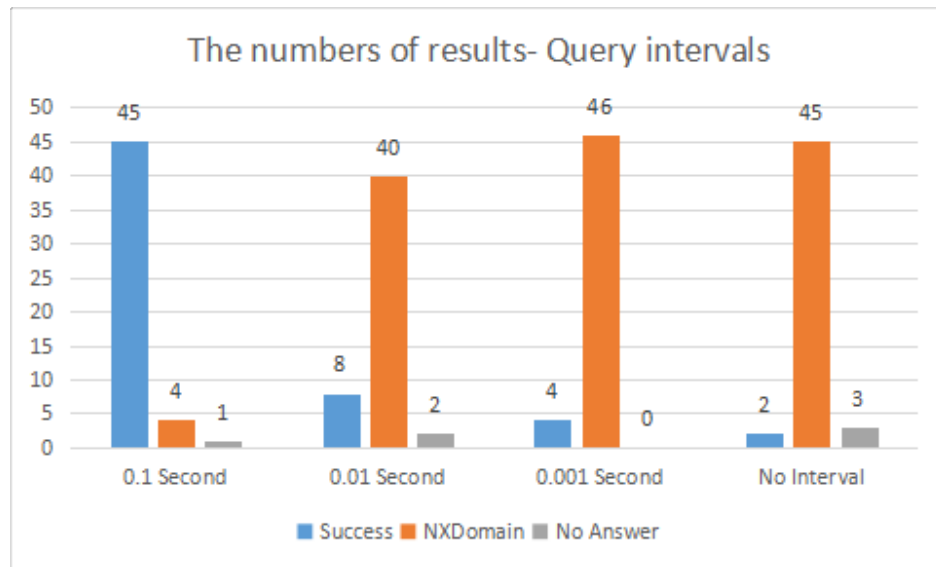
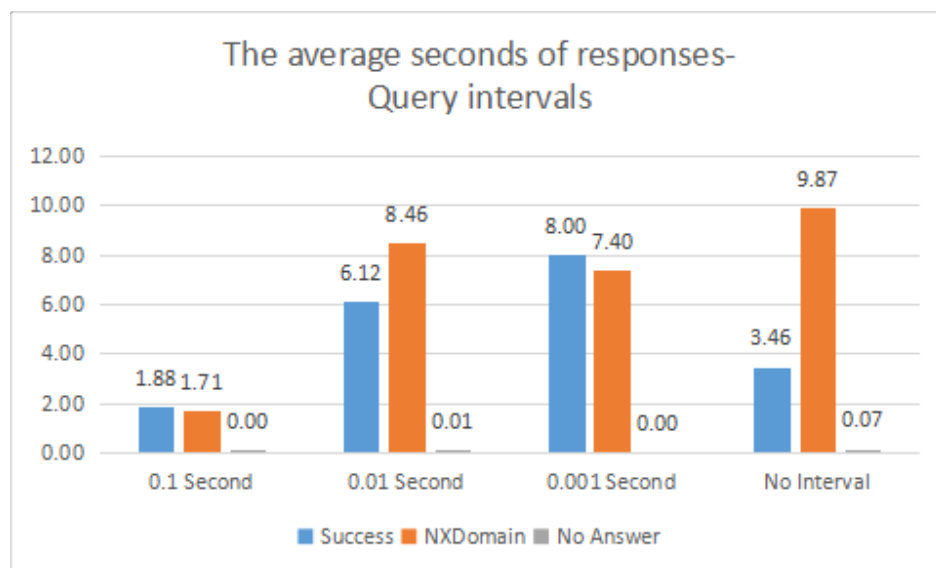
The study assumes that the massive queries in a very short time could decline the performance of a DNS server. Hence, an extra test was designed to figure out how the performance is affected by the frequency of DNS queries.

The testing program can set the query interval. For example, if the query interval is 0.01 second, then the next query will be sent after 0.01 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 4 intervals in this test, which were 0 second, 0.1 second, 0.01 second, 0.001 second. The controlled variables were shown in Table 4.8, and the cache was flushed before testing as well. The results were shown in Fig. 4.14, Fig. 4.15, and Fig. 4.16.

Controlled variables	Parameters
Cache	Flushed cache
Query name	The top 50 websites in Ireland
DNS type	DOH(Wireformat)
DNS provider	Local(Built by the researcher)
Record type	A
Query time	From 12:11:31 to 12:12:56 2/11/2020

Table 4.8: The controlled variables for testing query intervals

Figure 4.14: *The numbers of results in different DNS query intervals*Figure 4.15: *The average seconds of responses in different DNS query intervals*

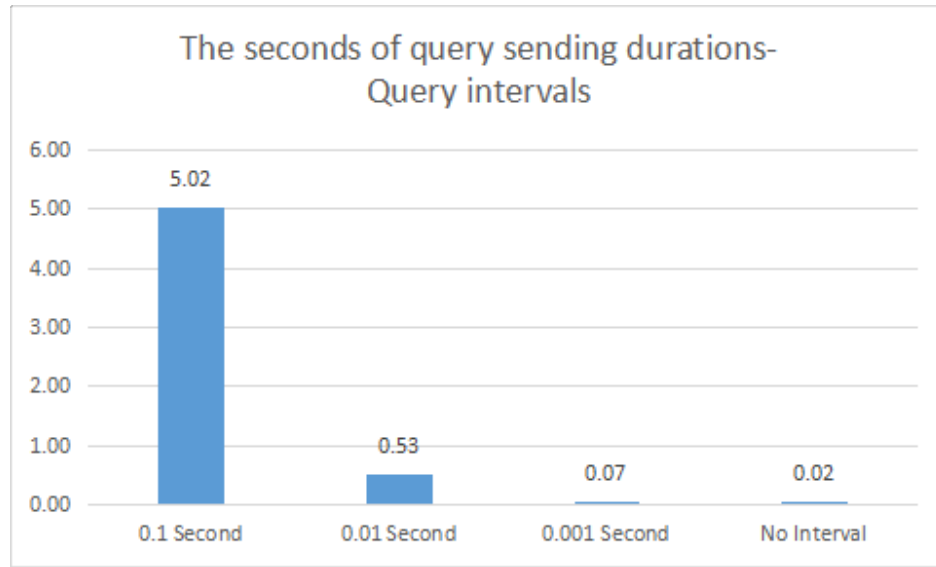


Figure 4.16: *The seconds of query sending durations in different DNS query intervals*

The figures showed that the interval of query sending affected the performance a lot. The results in the interval of 0.001 second were slightly better than no interval. 0.01 seconds was better than 0.001 seconds as well. The best one was the interval of 0.1 second, the performance was obvious better than other 3 query intervals.

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

4.7 The test for different query times

The last test was testing different query times. In the previous chapter, the study mentioned that the DNS traffic has peak time and off-peak time. Therefore, the performance of the DNS server may be different in peak time and off-peak time, because the queries in peak time should be much more than off-peak time.

This test used the data from different dates and different times to illustrate the change of the performance of the DNS server(some of the used data were from previous tests if their parameters were the same). The controlled variables(parameters) were listed in Table 4.9. The results were displayed in Fig. 4.17 and Fig. 4.18.

Those query times were 23:18:59 25/10/2020, 05:02:35 29/10/2020, 21:41:42 29/10/2020, 04:51:51 02/11/2020, 09:56:49 02/11/2020, and 12:11:31 02/11/2020. All the used data were gained from the tests with flushed cache.

Controlled variables	Parameters
Cache	Flushed cache
Query name	The top 50 websites in Ireland
DNS type	DOH(Wireformat)
DNS provider	Local(Built by the researcher)
Record type	A
Query interval	No interval

Table 4.9: The controlled variables for testing different query times

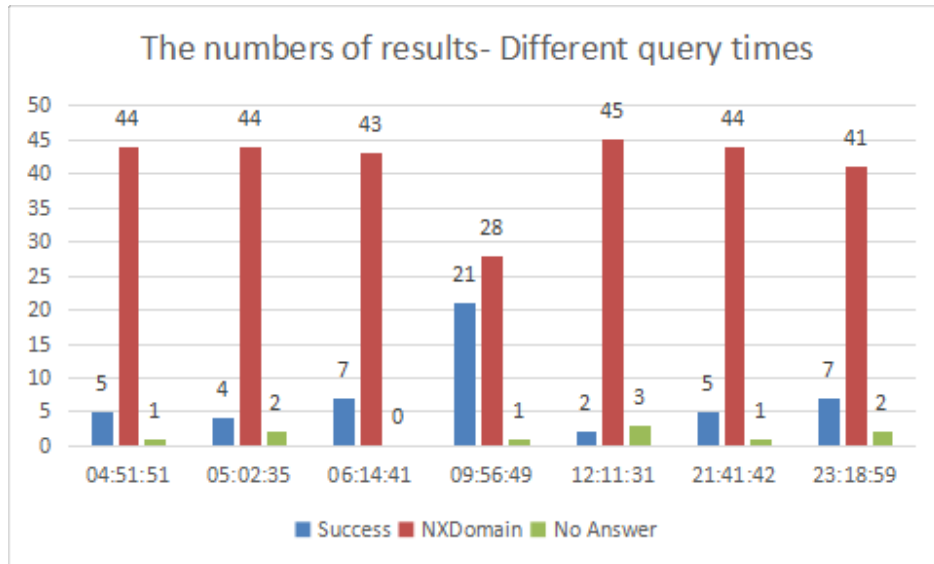


Figure 4.17: The numbers of results in different query times

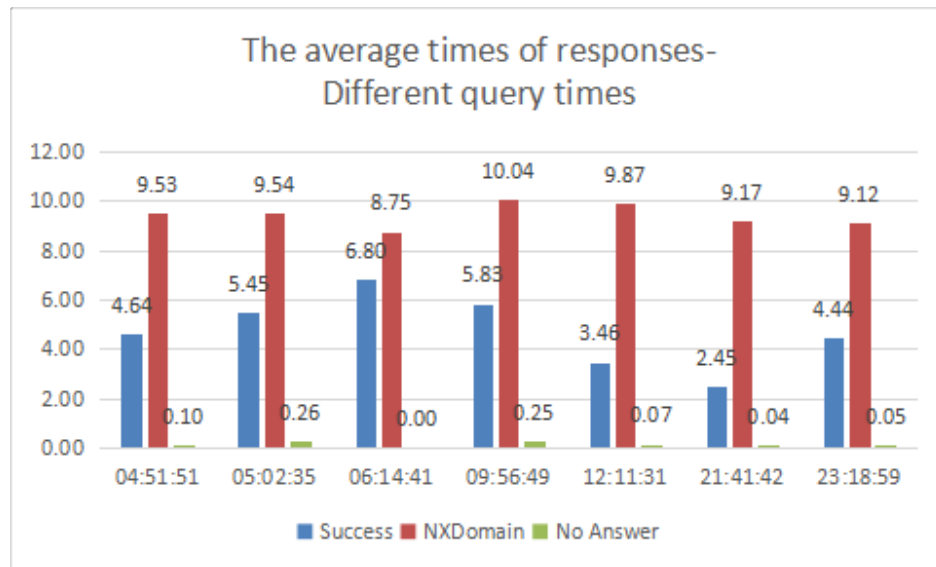


Figure 4.18: *The average seconds of responses in different query times*

The typical peak time is from 8 PM to 11 PM, but the performance did not have an obvious change in peak time. Therefore, there was no evidence to prove any relation between the performance of the DNS server and the query time in this study. The reason may be the authoritative DNS server is completely capable to process the queries in peak time, thus there was no obvious difference between peak time and off-peak time.

However, the results in 09:56:49 were apparently better than other times, but the typical DNS traffic at 9 AM to 11 AM is not on the lowest zone. The reason has not been found in this study, hence this study merely concludes that the performance of the DNS server can be very good sometimes.

Chapter 5

Overall design

5.1 The concern about DDOS attacks

DDOS is also the important issue for building DNS server [52].

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

As for the iterative query, when authoritative DNS servers receive the queries from recursive DNS servers, if they do not have the matched IP addresses, they will give recursive servers the IP addresses of other authoritative DNS servers for querying, then recursive servers will ask other authoritative DNS servers, this type of querying is the iterative query [53].

However, the recursive queries may cause DDOS attacks. The content of packet could be faked, the IP address of a sender can be changed to be the IP address of the victim. In case thousands of computers send recursive queries to DNS servers, and all IPs of sources are changed to be the IP of a victim, then those DNS servers will

send thousands of responses to that victim. After that, the traffic in the victim would be too high then cause some problems [3]. This type of DDOS attack is called DNS amplification attack [52].

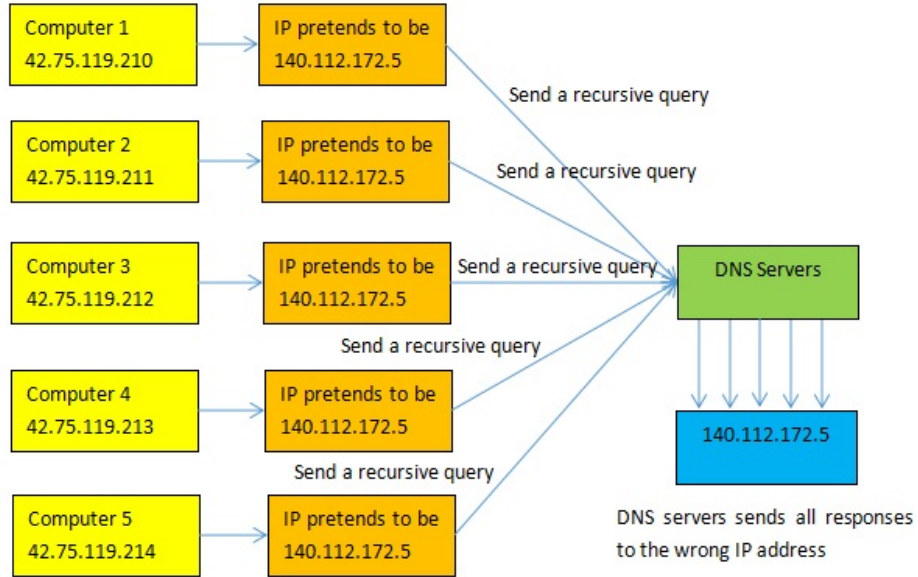


Figure 5.1: *The DDOS attack in recursive DNS queries [3]*

Thus, restricting DNS queries may be the ideal method to prevent DNS amplification attacks, the implementation is to disable the recursion for everyone, only local queries are allowed to be processed [54].

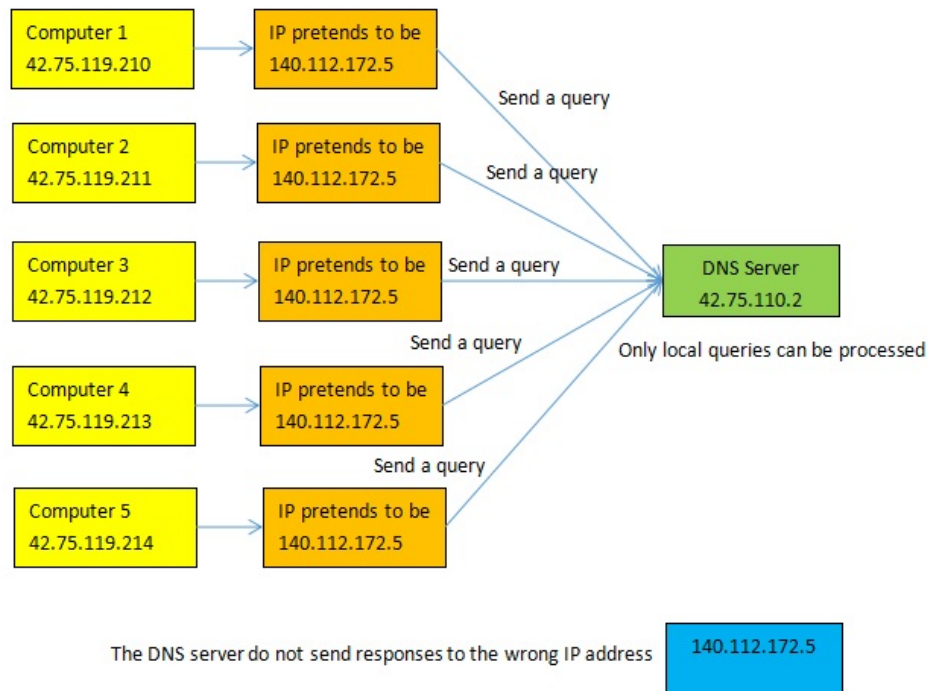


Figure 5.2: *Restricting DNS queries to prevent DNS amplification attacks [3]*

5.2 The concern about the policy

The Irish government has banned some websites for some reasons [55]. The problem is that users may utilize DOH to bypass the censorship from the government to browse the banned websites [56] [57], because the DNS queries are encrypted.

The study did a simple test. “1337x.to” [58] is one of the banned website in the Republic of Ireland. The reason is this website has the issue of copyright infringement. The researcher could not browse the website in Ireland at the beginning. The screenshot of the Firefox at that moment is displayed in Fig. 5.3.



Figure 5.3: *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. 5.4.

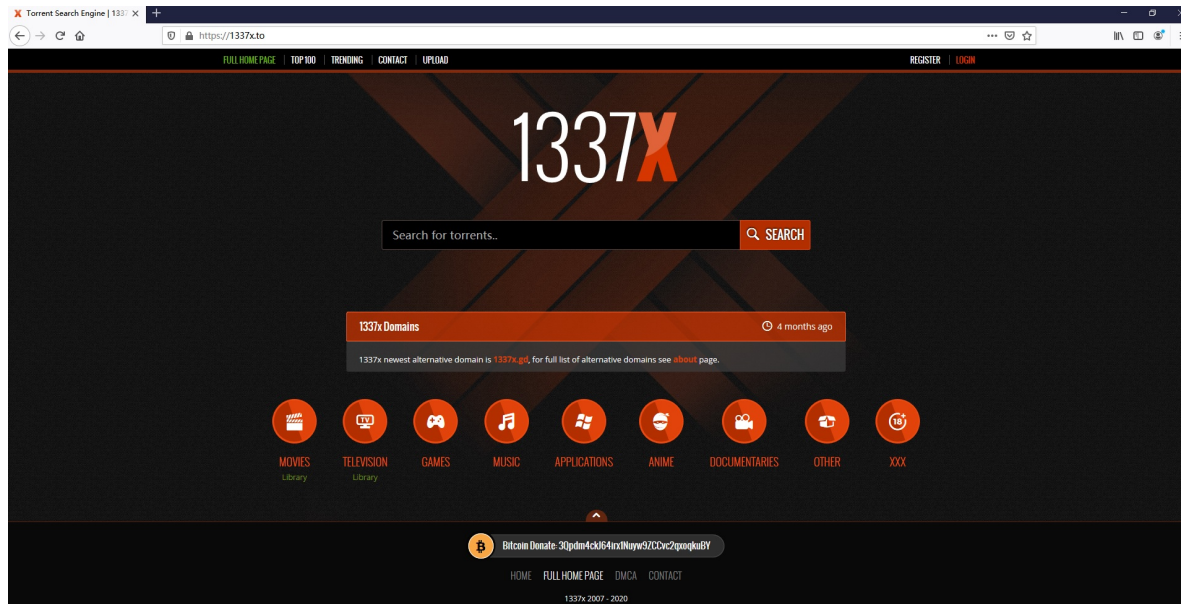


Figure 5.4: *Firefox can browse the banned website after enabling TRR.*

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

5.3 The concern about the latency

The computing of a data center can be increased, but the light speed is limited, therefore the quality of the DNS query would be worse if the DNS server is too far from the client [59].

The study assumes that the optical fiber is used to be the tool for transmitting signal, the latency will be about 5 microseconds per kilometers [60]. If the latency is including the time of the response, then the latency will be around 10 microseconds per kilometers.

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

According to the website DNSPerf, the DNS provider with the lowest latency is cloudflare in Europe, the latency is 7.97 ms. The screenshot is displayed in Fig. 5.5. This study takes 8 ms to be the minimum requirement of the latency.

The distances of some far places from Dublin can reach about 394 kilometers. The distances are counted by Google Map in Fig. 5.6 and Fig. 5.7. The path bypasses the UK part in Northern Ireland.

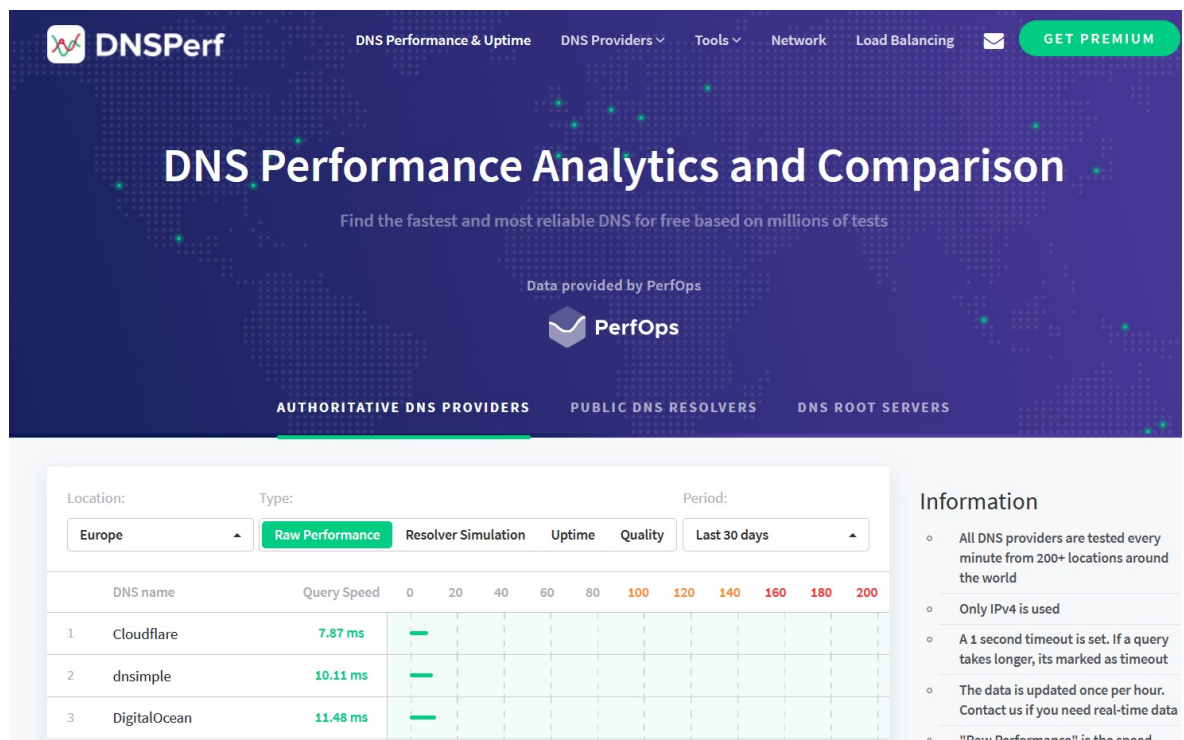


Figure 5.5: The ranking of DNS providers by latency in Europe.

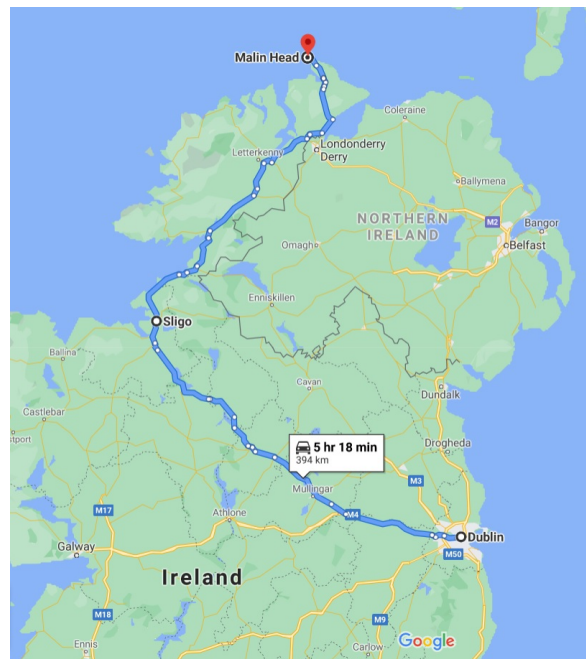


Figure 5.6: *The distance of a very far place in the north from Dublin.*

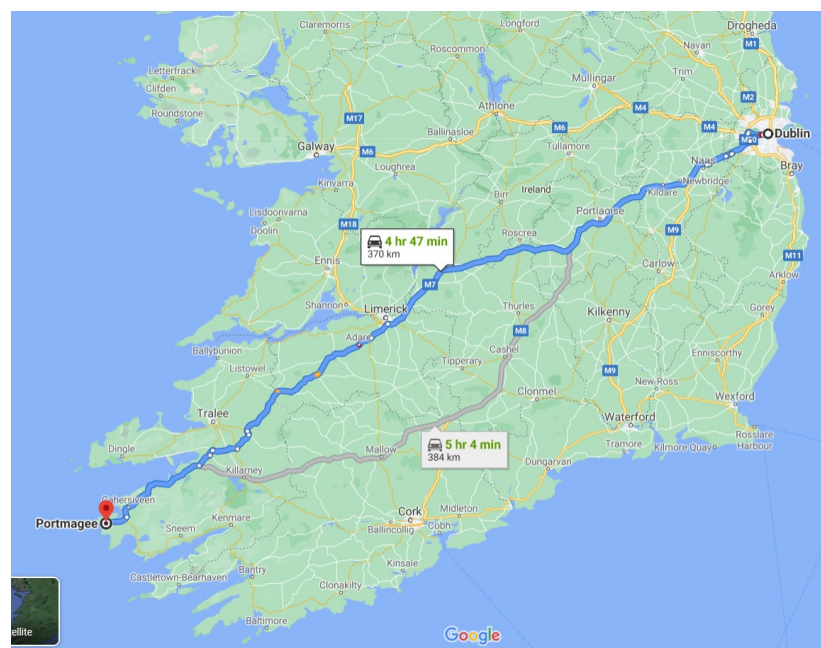


Figure 5.7: *The distance of a very far place in the south from Dublin.*

The distance 394 kilometers could cause approximately 4 ms for a DNS query [61], 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.

5.4 The technical plan for constructing TRR in Ireland

After the discussion about the background of TRR, the Irish DNS traffic, the required software for building a recursive resolver, the performance of a recursive resolver, and the concern about DDOS attacks, the policy and the latency, the study concludes the 5 conditions 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 second condition: Recursive resolvers must provide DOH service. TRR adopts DOH to encrypt the query, thus the DOH service is mandatory.

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

The fourth condition: It is necessary to deploy recursive resolvers in every area in Ireland. The purpose is to reduce DDOS attacks.

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

Apart from that, this study has 3 recommendations to satisfy those 5 conditions.

The first recommendation is that the software used for building the DNS server

not only should support the DOH service, but also should be easy to construct a completed system to manage the data and provide the data to others for checking. This recommendation is to satisfy the first condition and the second condition.

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 also may 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 recommendation is a list to estimate how many recursive resolvers should be deployed in each area in Ireland. This recommendation is to satisfy the third condition and the forth condition.

In the test for the cache in the previous chapter, the results revealed that the performance of the query of the first kind was much lower than the query of the second kind. The reason is that when the query of the first kind arrives the recursive resolver, the recursive resolver needs to ask the authoritative DNS server to get the matched IP address, but the recursive resolver is able to rapidly respond the matched IP for the query of the second kind because the cache has the matched IP.

Moreover, in a description in RFC7626 [15], the most queries belongs the second kind, only a few queries are the first kind but they affect the performance a lot. Therefore, the study just uses the query of the first kind to calculate the suitable number of queries.

In the test of the query interval in the previous chapter, all queries were the first kind, which was using the flushed cache. The interval with the best results was 0.1 second, and the number of successful responses was 45, which was close to the number of the responses with non-flushed cache(The query of the second kind). The number

of successful responses with non-flushed cache was 48.

Hence, this study assumes that 10 queries of the first kind for a second should be a suitable frequency.

Next step is counting the number of queries may have in each county in Ireland.

In the discussion about the DNS traffic in Ireland in the previous chapter, there were 2 estimated number of DNS queries per second in rush hours in Ireland, which were 4,494 and 9,149. This study adopts the higher number to be on the safe side. Those queries were collected from root servers, most of them should be sent from recursive resolvers, thus those queries are supposed to be the queries of the first kind.

After that, list the population of each county in Ireland, use the total population of Ireland to get the percentage of the population in every county in Ireland. Next, use the percentage of the population and estimated number of DNS queries per second to count the possible number of DNS queries per second in each county.

Finally, the suitable number of DNS queries is 10 per second, thus that possible number of DNS queries in each county can be used to count the reasonable number of required recursive resolvers in every county in Ireland. For example, if the possible number of DNS queries is 100 per second in a county, then the county requires 10 recursive resolvers.

The population of each county in Ireland in 2020 was not found on Internet, therefore the study used the data in 2016 to analyze. The source of the data of the population of Irish counties was from Wikipedia [62], even though it is different from the population of Ireland in 2020, which is 4,937,786 [63], but the gap is acceptable for this study, because the study just wanted to use the percentages to calculate, not population itself.

As for the word Recommended in the table, it was the number which is recommended by this study to deploy recursive resolvers in each county or area. The recommended number is 1.5 times the minimum number, because the trend of population in Ireland in recently years is growing up, thus the study supposes that the Irish population will be higher than the current population in next 5 years, and the DNS queries

will be higher as well.

Furthermore, some events could cause a higher usage of the Internet. For example, the virus COVID-19 made the Internet traffic higher [64] [65]. However, those factors and their effects are hard to be predicted and evaluated. For ensuring the high performance to deal with the possible coming DNS traffic, the suitable number of recursive resolvers should be higher than the minimum number. It is not necessary to make a far higher number than the minimum number, thus the recommended number 1.5 times the minimum number is reasonable. The number was also rounded up to be integer.

Those recommended numbers based on the computing of the personal computer and the network in the private accommodation. In case DNS providers have better computing and the better quality of the network in their data centers, than the required number of recursive resolvers can be reduced.

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

Bibliography

- [1] pmtk.medium.com, “Compare dnssec, dnscrypt, dns over tls, dns over https.” [Online]. Available: <https://pmtk.medium.com/%E5%AF%B9%E6%AF%944%E7%A7%8D%E5%BC%BA%E5%8C%96%E5%9F%9F%E5%90%8D%E5%AE%89%E5%85%A8%E7%9A%84%E5%8D%8F%E8%AE%AE-dnssec-dnscrypt-dns-over-tls-dns-over-https-2b6faca60892>.
- [2] Cloudflare, “What is a dns root server?.” [Online]. Available: <https://www.cloudflare.com/learning/dns/glossary/dns-root-server/>.
- [3] F. Internet, “What is recursive dns and why is it not recommended for most server owners?.” [Online]. Available: <https://www.youtube.com/watch?v=W3wXkHAv3qo>.
- [4] J. Peters, “What is dns, how it works + vulnerabilities.” [Online]. Available: <https://www.varonis.com/blog/what-is-dns/>.
- [5] Wikipedia, “Domain name system security extensions.” [Online]. Available: https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions.
- [6] Wikipedia, “Dnscrypt.” [Online]. Available: <https://en.wikipedia.org/wiki/DNSCrypt>.
- [7] Wikipedia, “Dns over tls.” [Online]. Available: https://en.wikipedia.org/wiki/DNS_over_TLS.

- [8] Wikipedia, “Dns over https.” [Online]. Available: https://en.wikipedia.org/wiki/DNS_over_HTTPS.
- [9] Wikipedia, “Ipv4.” [Online]. Available: <https://en.wikipedia.org/wiki/IPv4>.
- [10] Wikipedia, “Ipv6.” [Online]. Available: <https://en.wikipedia.org/wiki/IPv6>.
- [11] Wikipedia, “Domain name.” [Online]. Available: https://en.wikipedia.org/wiki/Domain_name.
- [12] D. M. 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>.
- [13] Wikipedia, “Request for comments.” [Online]. Available: https://en.wikipedia.org/wiki/Request_for_Comments.
- [14] Wikipedia, “Internet engineering task force.” [Online]. Available: https://en.wikipedia.org/wiki/Internet_Engineering_Task_Force.
- [15] S. Bortzmeyer, “Dns privacy considerations.” [Online]. Available: <https://tools.ietf.org/html/rfc7626>, August 2015.
- [16] E. T. Wicinski, “Dns privacy considerations draft-ietf-dprive-rfc7626-bis-08.” [Online]. Available: <https://tools.ietf.org/html/draft-ietf-dprive-rfc7626-bis-08>, October 2020.
- [17] Wikipedia, “Public recursive name server.” [Online]. Available: https://en.wikipedia.org/wiki/Public_recursive_name_server.
- [18] T. D. Institute, “Disadvantages of dnssec.” [Online]. Available: <https://dnsinstitute.com/documentation/dnssec-guide/ch06s06.html>.
- [19] IONOS, “Dns over tls: an improved security concept.” [Online]. Available: <https://www.ionos.com/digitalguide/server/security/dns-over-tls/>.
- [20] Mozilla, “Trusted recursive resolver.” [Online]. Available: https://wiki.mozilla.org/Trusted_Recursive_Resolver.

- [21] 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-program/> June 2020.
- [22] 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-program/> June 2020.
- [23] 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/>.
- [24] 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/>.
- [25] 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/>.
- [26] 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>.
- [27] 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/>.
- [28] Winaero, “Enable dns over https in opera (doh).” [Online]. Available: <https://winaero.com/enable-dns-over-https-in-opera-doh/>.
- [29] 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-opposition/>.

- [30] Wikipedia, “Comparison of dns server software.” [Online]. Available: [https://en.wikipedia.org/wiki/Comparison of DNS server software](https://en.wikipedia.org/wiki/Comparison_of_DNS_server_software).
- [31] K. John, “Bind vs dnsmasq vs powerdns vs unbound.” [Online]. Available: <https://computingforgeeks.com/bind-vs-dnsmasq-vs-powerdns-vs-unbound/>.
- [32] ISHM, “Building dns over https server on centos 7.” [Online]. Available: <https://ishm.idv.tw/?p=481>.
- [33] Archlinux, “Dns over https servers.” [Online]. Available: https://wiki.archlinux.org/index.php/DNS_over_HTTPS_servers.
- [34] TINYDNS, “Compare the different dns servers: Which one is right for you?.” [Online]. Available: <https://tinydns.org/compare-different-dns-servers/>.
- [35] Wikipedia, “Nsd.” [Online]. Available: <https://en.wikipedia.org/wiki/NSD>.
- [36] Wikipedia, “Unbound (dns server).” [Online]. Available: [https://en.wikipedia.org/wiki/Unbound\(DNS_server\)](https://en.wikipedia.org/wiki/Unbound(DNS_server)).
- [37] Wikipedia, “Bind.” [Online]. Available: <https://en.wikipedia.org/wiki/BIND>.
- [38] Wikipedia, “Powerdns.” [Online]. Available: <https://en.wikipedia.org/wiki/PowerDNS>.
- [39] Loull, “Dns resources.” [Online]. Available: <https://www.cnblogs.com/549294286/p/5200255>.
- [40] Facebookexperimental, “Dns over https proxy.” [Online]. Available: <https://github.com/facebookexperimental/doh-proxy>.
- [41] NGINX, “Welcome to nginx wiki!.” [Online]. Available: <https://www.nginx.com/resources/wiki/>.
- [42] Wikipedia, “List of linux distributions.” [Online]. Available: https://en.wikipedia.org/wiki/List_of_Linux_distributions.
- [43] W. T. Hamza Boulakhrif, Yuri Schaeffer, “Analysis of dns resolver performance measurements,” tech. rep., University of Amsterdam, July 2015.

- [44] Sciencebuddies.org, “Variables in your science fair project.” [Online]. Available: <https://www.sciencebuddies.org/science-fair-projects/science-fair/variables>.
- [45] D. Geek, “What is nxdomain?.” [Online]. Available: <https://www.dnsknowledge.com/whatis/nxdomain-non-existent-domain-2/>.
- [46] Moz.com, “The moz top 500 websites.” [Online]. Available: <https://moz.com/top500>.
- [47] Alexa, “Top sites in ireland.” [Online]. Available: <https://www.alexa.com/topsites/countries/IE>.
- [48] Cloudflare, “Using dns wireformat.” [Online]. Available: <https://developers.cloudflare.com/1.1.1.1/dns-over-https/wireformat>.
- [49] JSON.ORG, “Introducing json.” [Online]. Available: <https://www.json.org/json-en.html>.
- [50] Cloudflare, “Using json.” [Online]. Available: <https://developers.cloudflare.com/1.1.1.1/dns-over-https/json-format>.
- [51] J. Software, “Dns record types.” [Online]. Available: <https://simplifiedns.plus/help/dns-record-types>.
- [52] Imperva, “Dns amplification.” [Online]. Available: <https://www.imperva.com/learn/ddos/dns-amplification/>.
- [53] Cloudflare, “What is recursive dns?.” [Online]. Available: <https://www.cloudflare.com/learning/dns/what-is-recursive-dns/>.
- [54] F. Internet, “What is recursive dns and why is it not recommended?.” [Online]. Available: https://help.fasthosts.co.uk/app/answers/detail/a_id/1276.
- [55] Wikipedia, “Internet censorship in the republic of ireland.” [Online]. Available: https://en.wikipedia.org/wiki/Internet_censorship_in_the_Republic_of_Ireland.

- [56] K. Leuven, “Does doh imply privacy?.” [Online]. Available: <https://www.esat.kuleuven.be/cosic/blog/does-doh-imply-privacy/>.
- [57] InCompass, “Understanding doh and dot.” [Online]. Available: <https://incompass.netstar-inc.com/blog/202>.
- [58] Wikipedia, “1337x.” [Online]. Available: <https://en.wikipedia.org/wiki/1337x>.
- [59] K. Miller, “Calculating optical fiber latency.” [Online]. Available: <https://www.m2optics.com/blog/bid/70587/calculating-optical-fiber-latency>, January 2012.
- [60] Rogerluethy, “What is latency?.” [Online]. Available: <https://rogerluethy.wordpress.com/2011/09/01/what-is-latency/>, September 2011.
- [61] Timbercon, “Time delay of light in fiber calculator.” [Online]. Available: <https://www.timbercon.com/resources/calculators/time-delay-of-light-in-fiber-calculator/>.
- [62] Wikipedia, “List of irish counties by population.” [Online]. Available: https://en.wikipedia.org/wiki/List_of_Irish_counties_by_population.
- [63] Worldometer, “Ireland population(live).” [Online]. Available: <https://www.worldometers.info/world-population/ireland-population/>.
- [64] N. P. Ella Koeze, “The virus changed the way we internet.” [Online]. Available: <https://www.nytimes.com/interactive/2020/04/07/technology/coronavirus-internet-use.html>, April 2020.
- [65] J. Quann, “Covid-19: Almost 80% of irish people reading or downloading online news.” [Online]. Available: <https://www.newstalk.com/news/covid-19-almost-80-irish-people-reading-downloading-online-news-1033425>, June 2020.

Appendix

...