Produce a technical and business plan for an ”Irish” TRR

1st Stephen Farrell
School of Computer Science and Statistics
Trinity Dublin College
Dublin, Ireland
stephen.farrell@cs.tcd.ie

2nd Lin Tung-te
School of Computer Science and Statistics
Trinity Dublin College
Dublin, Ireland
tlin@tcd.ie

***Abstract*—abstract**
***Index Terms*—TRR**

I. Introduction

II. The policy in Ireland

III. The DNS traffic in Ireland

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

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

Root servers are the highest level DNS servers [1], 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 [3], which are Verisign(It manages 2 root server zones), USC-ISI, Cogent Communications, University of Maryland, NASA Ames Research Center, Internet Systems Consortium, Defense Information Systems Agency, U.S. Army Research Lab, Netnod, RIPE NCC, ICANN and WIDE Project. Therefore, those 12 organizations have the information about DNS traffic.

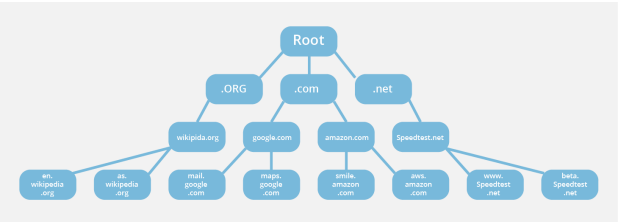

Fig. 1. *The levels of authoritative DNS servers [1]*

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 [3].

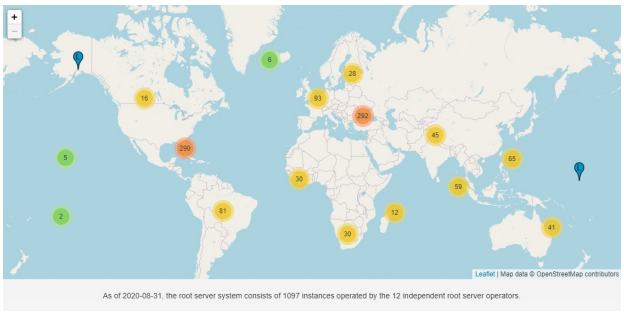

Fig. 2. *The root servers in the world [3]*

Fig. 3. *The root servers in Dublin [3]*

Fig. 4. *The root servers in Cork [3]*

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

Next, the recursive structure of DNS servers has to be figured out. There are two kinds of DNS servers, the first kind of DNS server is recursive DNS server, it could be private or public, but those recursive DNS servers are not controlled by

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 I
THE LIST OF ROOT SERVER ZONES [3]

the organizations mentioned above. When users send queries to DNS servers, the queries will arrive recursive DNS servers first, if recursive DNS servers have matched IP addresses in their caches, then they can respond IP addresses to users directly.

The second DNS server is authoritative DNS server, they store the IP addresses of websites. Moreover, they are hierarchical, the highest one is root server. The levels of authoritative DNS servers are shown in Fig. 1. If recursive DNS servers do not have matched IP addresses, they will ask authoritative DNS server for IP addresses and store it in their cache [4].

Thus, the recursive structure of DNS server causes another problem, it is very hard to collect the records about all DNS queries, because there are numerous recursive DNS servers and they are managed by many organizations [5], hence, the operators of root servers do not have their data.

However, it is not necessary to know the total number of DNS queries in Ireland, because the target in this research is to understand what the performance should a TTR server possess in Ireland. The number of DNS queries a root server may receive can help us to evaluate the required performance for a TTR server in Ireland.

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

Method 1 is using the data on Akamai.com to estimate the DNS traffic [6].

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

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

In a report from Central Statistics Office of Ireland, it showed that there were 89% of Irish households have the internet at home in 2018 [7]. From the growth of households with the internet, the percentage is probably 90% in 2020. There were about 4.57 billion internet users in the world in July 2020 [8]. The population in Ireland was around 4.944 million in August 2020 [9]. Hence, the Irish Internet users may be about 4.113 million, it was approximately 0.09% of internet users in the whole world.

According to the data from Akamai.com [6], the overall DNS traffic in the world was about 7 Trillion transactions (Requests and responses) in June 2020. Then, 0.09% of DNS traffic in the world could be Irish DNS traffic, which is around 6.3 billion DNS transactions for one month in Ireland. On average, it could be 210 DNS million transactions in a day in Ireland.

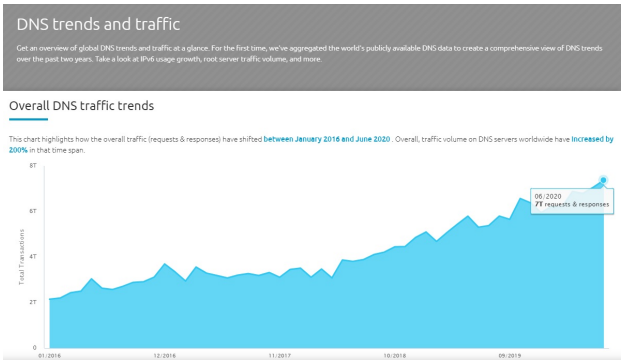

Fig. 5. *The trend of DNS traffic in the world [6]*

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 II
OVERALL DNS TRAFFIC TRENDS(UNIT:TRANSACTIONS) [6]

However, internet traffic is changeable in different hours, it is necessary to understand when are the rush hours. For example, the internet rush hours are usually between 7 pm and 11 pm in UK [10]. In Sao Paulo, the internet rush hours are between 8 pm and 11 pm [11]. In USA, it is 8 pm to 10 pm [12]. In Berlin, the rush hours are 8 pm to 11 pm [13]. In Amsterdam, it is from 8 pm to 11 pm as well [14].

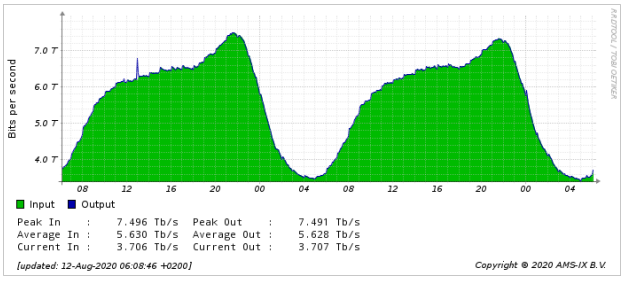

Fig. 6. *The internet traffic in a day (Amsterdam) [14]*

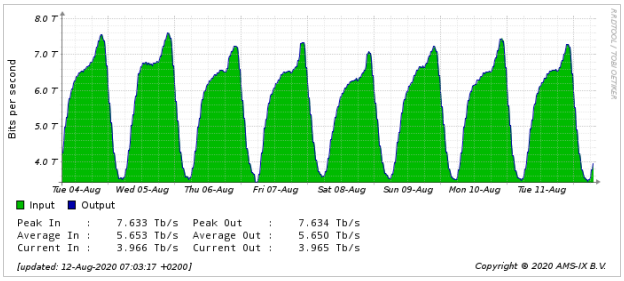

Fig. 7. *The internet traffic in a week (Amsterdam) [14]*

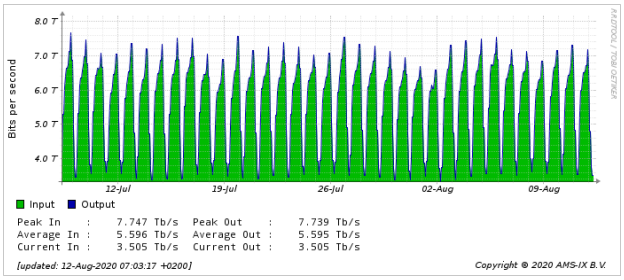

Fig. 8. *The internet traffic in a month (Amsterdam) [14]*

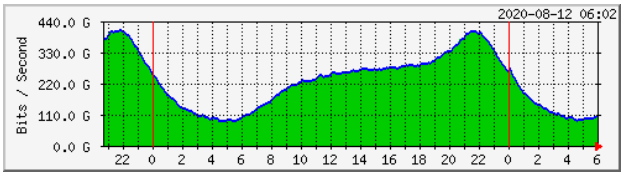

Fig. 9. *The internet traffic in a day (Berlin) [14]*

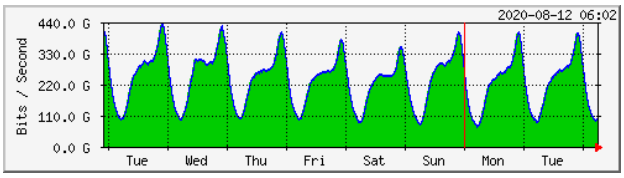

Fig. 10. *The internet traffic in a week (Berlin) [14]*

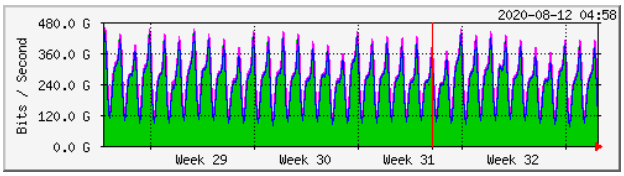

Fig. 11. *The internet traffic in a month (Berlin) [14]*

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

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

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

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 III
INTERNET TRAFFIC AND ITS PERCENTAGE IN EACH HOUR IN A DAY IN AMSTERDAM [14]

After that, using the percentage to multiply the estimated number of daily DNS transactions in Ireland, which is 210 million, then the result is sown in TABLE IV. The 2 busiest hours are 9 PM and 10 PM, the number of DNS transactions could be 11.2 million in an hour.

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

The numbers of transactions in every root server zone are very different, therefore it is hard to estimate the numbers in A, G, H and J root server zones. If assume that the average number of A, G, H and J is close to the average number of B, C, D, E, F, I, K, L, M, then the estimated number of transactions in all root servers in rush hours could be 11.2/9X13=16.18 million.

If convert it into a second, the number of DNS transactions could be 4,494 per second during the rush hour (16.18(million per hour)/60(minutes)/60(seconds)).

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

ICANN (Internet Corporation for Assigned Names and Numbers) is the one of 12 organizations which are responsible for managing DNS root servers, the servers it manages are L-root servers. Unlike other 11 organizations, ICANN provides a website to display real-time DNS traffic, that is Stats.dns.icann.org [15].

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

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

TABLE IV
USING THE DAILY DISTRIBUTION OF INTERNET TRAFFIC OF AMSTERDAM TO ESTIMATE THE DNS TRAFFIC IN IRELAND [14]

Thus, here chose a city which has a similar population to Ireland to estimate the DNS traffic. Melbourne should be a ideal sample. The population in Melbourne is about 5 million in 2019 [16], which is close to the population in Ireland (4.9 million). Moreover, Melbourne is isolated, there is no big city near Melbourne,therefore the network connection may be similar to a country.

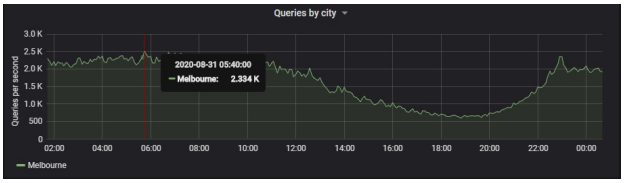

Fig. 12. *The number of queries per second in a root server in Melbourne [15]*

From the data in Fig. 12, the highest value in a day is 2,334 per second, which was occurred at 05:40 UTC(19:40 in Melbourne).

Fig. 13. *The root servers in Melbourne [3]*

However, the data is only from a root server which is managed by ICANN, there are four root servers in Melbourne, the DNS traffic in other 3 root servers are not provided. Assume the average traffic in other 3 root servers is close to the root server managed by ICANN, the whole DNS traffic in Melbourne could be 9,336 per second(2,334X4). Next, adjust the traffic to accord the population of Ireland, the DNS traffic could be 9,149 per second during the rush hour(9,336/5X4.9).

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

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

TABLE V
THE COMPARISON BETWEEN 2 METHODS FOR THE ESTIMATION OF THE DNS TRAFFIC IN IRELAND

IV. THE CONCERN OF DDOS ATTACKS

DDOS is the important issue for building DNS server.

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 [17].

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 [18]. This type of DDOS attack is called DNS amplification attack [19].

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 [20].

V. THE REQUIRED PERFORMANCE

A DNS transaction contains many packets.

VI. REQUIRED SOFTWARE

Building a DNS server for TRR needs some software, including the software for implementing DNS server, tools and server [21].

First, implement DNS server, there are many choices, such as BIND, Unbound, DNSMASQ, PowerDNS, Microsoft DNS

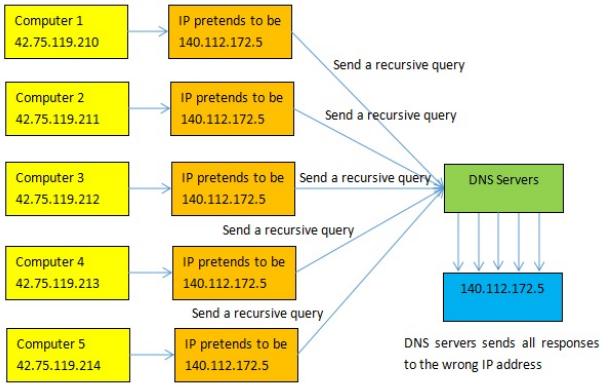

Fig. 14. *The DDOS attack in recursive DNS queries [18]*

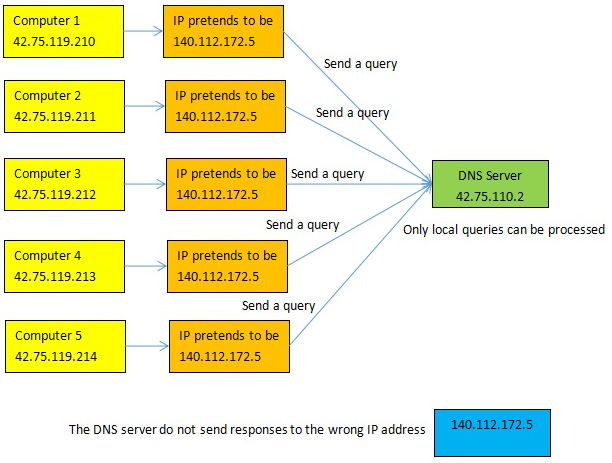

Fig. 15. *Restricting DNS queries to prevent DNS amplification attacks [18]*

and Cisco Network Registrar [22] [23]. In this research, Unbound and BIND are recommended, because those two software are popular to build a DNS server nowadays, both software support DNS over HTTPS (DoH), then users may use TRR to browse websites in Firefox [24] [25].

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 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 [26]. 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 [27].

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 [28].

Compare with Unbound and BIND, both software are good choices [29].

Next, the DNS server need tools to recieve 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 [30].

After that, NGINX can provide the web 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 in a port and the request from users [31].

About Operating System, Linux is recommended, because the much resource for building DNS servers is based on Linux [32].

The required software is shown in TABLE VI.

Category	Software	Note
DNS	BIND 9	
DNS	Unbound	Free and open-source software
Tool	DoH-proxy	
Server	NGINX	Free and open-source software

TABLE VI
THE REQUIRED SOFTWARE FOR BUILDING A DNS SERVER FOR TRR

VII. THE CONCERN OF OTHER ISSUES

COVID-19

VIII. CONCLUSION

REFERENCES

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

[2] Wikipedia, "Root name server." [Online]. Available: https://en.wikipedia.org/wiki/Root name server.

[3] root servers.org, "root-servers.org." [Online]. Available: https://root-servers.org/.

[4] 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.

[5] D. M. Easy, "What is the difference between authoritative and recursive dns nameservers?." [Online]. Available: https://umbrella.cisco.com/blog/what-is-the-difference-between-authoritative-and-recursive-dns-nameservers.

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

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

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

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

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

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

[12] 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.

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

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

[15] stats.dns.icann.org, "stats.dns.icann.org." [Online]. Available: https://stats.dns.icann.org/.

[16] Wikipedia, "Melbourne." [Online]. Available: https://en.wikipedia.org/wiki/Melbourne.
[17] Cloudflare, "What is recursive dns?." [Online]. Available: https://www.cloudflare.com/learning/dns/what-is-recursive-dns/.
[18] 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.
[19] Imperva, "Dns amplification." [Online]. Available: https://www.imperva.com/learn/ddos/dns-amplification/.
[20] 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.
[21] Loull, "Dns resources." [Online]. Available: https://www.cnblogs.com/549294286/p/5200255.html.
[22] Wikipedia, "Comparison of dns server software." [Online]. Available: https://en.wikipedia.org/wiki/Comparison of DNS server software.
[23] K. John, "Bind vs dnsmasq vs powerdns vs unbound." [Online]. Available: https://computingforgeeks.com/bind-vs-dnsmasq-vs-powerdns-vs-unbound/.
[24] ISHM, "Building dns over https server on centos 7." [Online]. Available: https://ishm.idv.tw/?p=481.
[25] Archlinux, "Dns over https servers." [Online]. Available: https://wiki.archlinux.org/index.php/DNS_over_HTTPS_servers.
[26] Wikipedia, "Nsd." [Online]. Available: https://en.wikipedia.org/wiki/NSD.
[27] Wikipedia, "Unbound (dns server)." [Online]. Available: https://en.wikipedia.org/wiki/Unbound(DNS_server).
[28] Wikipedia, "Bind." [Online]. Available: https://en.wikipedia.org/wiki/BIND.
[29] TINYDNS, "Compare the different dns servers: Which one is right for you?." [Online]. Available: https://tinydns.org/compare-different-dns-servers/.
[30] Facebookexperimental, "Dns over https proxy." [Online]. Available: https://github.com/facebookexperimental/doh-proxy.
[31] NGINX, "Welcome to niginx wiki!." [Online]. Available: https://www.nginx.com/resources/wiki/.
[32] M. Anicas, "How to configure bind as a private network dns server on ubuntu 14.04." [Online]. Available: https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-ubuntu-14-04.