Ex4 Assignment

First Part DOH

A. Beside the fact that the DOH is encrypted and secured there are many other advantages to this new method.
Another advantage that DOH have is this protocol uses TCP, this insure us that no information will be lost.
There people who can say that if this protocol uses TCP, it might be slower due to the secure and the encryption but in performance test which published in SamKnows, there a little influence but it so tiny and negligible that we can use it in our home network.

Country	ISP	ISP Do53	Cloudflare Do53	Cloudflare DoH	Google Do53	Google DoH
Germany	Deutsche Telekom	15.66	34.57	38.03	33.97	33.01
Germany	Kabel Deutschland	20.67	20.41	23.03	35.58	37.55
Germany	Telefonica	17.82	19.73	21.61	49.43	49.1
Greece	CYTA	59.07	47.78	25.82	79.0	76.14
Greece	Cosmote	18.41	19.97	22.57	75.03	73.02
Greece	Forthnet	26.45	65.48	75.22	81.97	88.49
Italy	Fastweb	21.28	14.54	16.77	46.1	48.73
Italy	Telecom Italia	40.53	39.19	37.55	60.06	61.46
Italy	Vodafone	57.87	22.1	26.62	57.04	62.85
Portugal	MEO	33.65	20.83	21.92	62.73	66.04
Portugal	Vodafone	26.12	18.29	8.52	48.1	50.31
Spain	Orange	15.24	15.2	19.84	48.79	48.97
Spain	Telefonica	20.2	12.83	15.93	45.15	45.08
Spain	Vodafone	12.27	5.11	9.82	47.65	51.73
UK	BT	29.63	21.61	28.42	41.91	43.44
UK	Plusnet	26.24	19.88	24.65	37.86	40.59
UK	Sky	13.83	13.95	27.23	13.82	41.43
UK	TalkTalk	9.86	16.32	21.88	35.38	36.97
UK	Virgin	14.57	17.6	21.4	39.2	38.73
UK	Vodafone	32.44	22.62	17.97	37.77	33.53

B. In our world there is no perfect, so also the DOH protocol have problem, we will present two of them.

1. If all of our network will be in the DOH protocol, it will weakens the cyber security. If all the DNS queries will be encrypted, companies which using DNS monitoring for cyber security will lose the visibility to catch people who use network for bad things such as cyber-attack.

2. The DOH might be slower than other methods that we use in today.

C. In aim to solve the problem that cyber security companies couldn't reach the "bad" people in the Internet, I suggest that every traffic in this protocol will have a unique serial number which only cyber companies and governments will have the permission to investigate this serial number which contain minor information such as the specific computer IP.
Of course, there will be rules which will be written, and using this rules companies and governments will be able to investigate the "bad" traffic.

D. There are four way to implement the DOH method, we will explain a little bit on each of them and provide the best (in our opinion) to use in.

1. <u>Implement DOH in the application level</u> (update our browser to this way) - with the DOH, my DNS traffic is sent over an encrypted tunnel using HTTPS, in that way, if we are using sniffing tool such as wireshark, the information will be encrypted to me (the user) and to outside world.
When I search a little bit, I have seen than not in all the browsers we can add the DOH option.

2. <u>Implement DOH in the Proxy layer in the network-</u>
A Proxy is a server that we trust on to make all the interaction with the outside world servers.
When we are using Proxy with DOH (most common provider of the DOH is cloudflare.com) at first we asking a query from the DOH provider , and then there are two option:
1. If our DOH provider has the wanted address we want to go to, we directly connect to it with no use in the Proxy server, which may not be routable from my internal network.

2. The DOH provider will give us the Proxy server's IP, and the Proxy will do all the other interaction with the outside world.
This method is a recursive one, and all the queries is sent from one server to another using DOH, due to that in the local network the query isn't encrypted.

3. <u>Implement DOH using local Proxy server -</u>
when we are using this method which might be a little bit similar to the previous one, al the queries are encrypted fully, unlike in the previous method, which in our local network it isn't encrypted.
In one have we might think this is a good solution but in the other hand it's very expensive to the client.

4. <u>Implement DOH using Plugin installation-</u>
Using a plugin mean to install a new plugin in our computer, with that plugin our computer will send encrypted message, for every browser we will use at.
Again it seems like a great way to use in, but it isn't flexible,
it means that when we add this plugin we cant choose if the information will be encrypted or not.

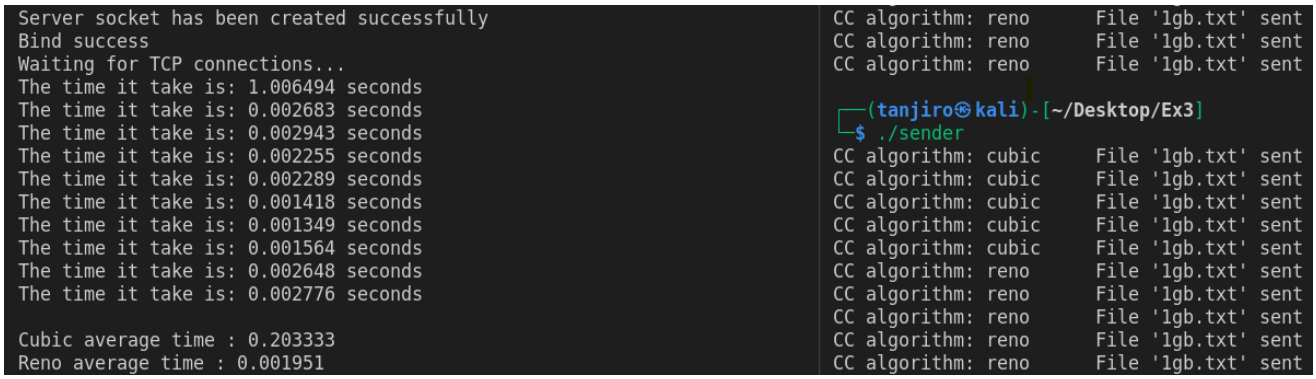
In my opinion, the best implementation is the first one, because when we use this way, we have the option if to encrypt our information or not, we can also choose that one browser will be encrypted and the other not.
For a costumer, when we are given the option to choose if to use something or not, and this is a dream in now days.

D. In this question we ask to give an advantage of the DOH in contrast to DO53.
Imagine that in our network there is packet loss, in unknown percent and we would like to load a website. In this case, if we will use the DOH method that uses the TCP protocol we can insure that most of the packet will arrive, that because the TCP protocol is insure that the packet will arrive to the destination (me) with the flow control mechanism which the TCP protocol provide.
However, DO53 uses the UDP protocol, which does not care about packet lost, it will send all the information and it does not insure everything, so the packet might be lost.
In conclusion, I think this is the main advantage that the DOH has in contrast to DO53.

Part 2- Client Socket & Measure

	Average time in seconds	
Packet Lost percent	**Cubic**	**Reno**
0 percent	**0.203333sec**	**0.001951 sec**
10 percent	**0.447072 sec**	**0.207694 sec**
15 percent	**9.330158 sec**	**7.668399 sec**
20 percent	**10.827781 sec**	**6.148545 sec**
25 percent	**12.039938 sec**	**10.196484 sec**
30 percent		

0% lost:



10% lost:

```
Server socket has been created successfully
Bind success
Waiting for TCP connections...
The time it take is: 1.152462 seconds
The time it take is: 0.424703 seconds
The time it take is: 0.222418 seconds
The time it take is: 0.207707 seconds
The time it take is: 0.228070 seconds
The time it take is: 0.031232 seconds
The time it take is: 0.208101 seconds
The time it take is: 0.507768 seconds
The time it take is: 0.064597 seconds
The time it take is: 0.226773 seconds

Cubic average time : 0.447072
Reno average time : 0.207694
```

```
CC algorithm: reno      File '1gb.txt' sent
CC algorithm: reno      File '1gb.txt' sent
CC algorithm: reno      File '1gb.txt' sent

┌──(tanjiro㉿kali)-[~/Desktop/Ex3]
└─$ ./sender
CC algorithm: cubic     File '1gb.txt' sent
CC algorithm: cubic     File '1gb.txt' sent
CC algorithm: cubic     File '1gb.txt' sent
CC algorithm: cubic     File '1gb.txt' sent
CC algorithm: cubic     File '1gb.txt' sent
CC algorithm: reno      File '1gb.txt' sent
CC algorithm: reno      File '1gb.txt' sent
CC algorithm: reno      File '1gb.txt' sent
CC algorithm: reno      File '1gb.txt' sent
CC algorithm: reno      File '1gb.txt' sent
```

15% lost:

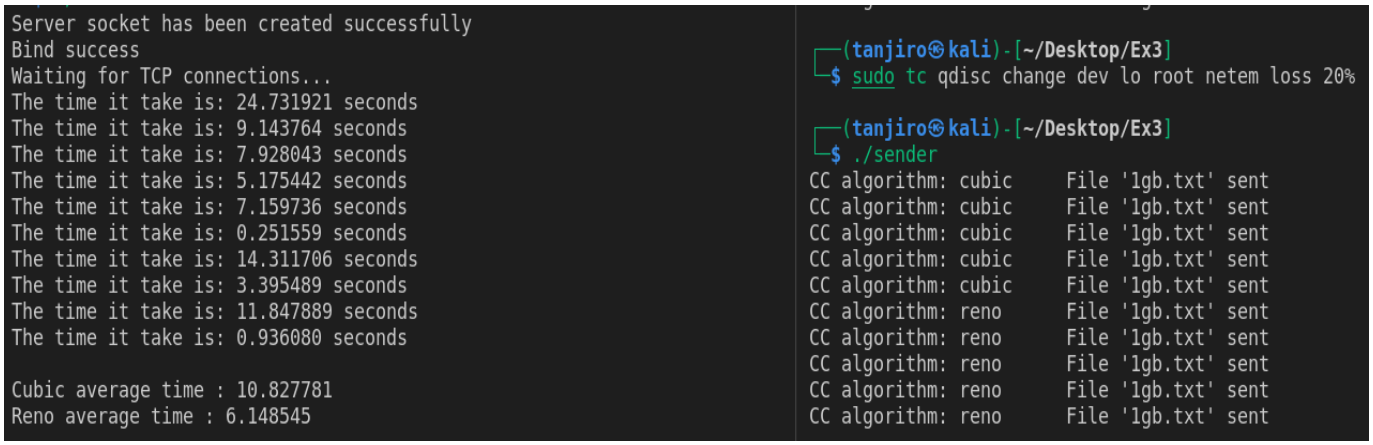
```
Server socket has been created successfully
Bind success
Waiting for TCP connections...
The time it take is: 1.107522 seconds
The time it take is: 0.000854 seconds
The time it take is: 4.151166 seconds
The time it take is: 0.016335 seconds
The time it take is: 41.374911 seconds
The time it take is: 0.443716 seconds
The time it take is: 33.234918 seconds
The time it take is: 3.512625 seconds
The time it take is: 0.258968 seconds
The time it take is: 0.891767 seconds

Cubic average time : 9.330158
Reno average time : 7.668399
```

```
CC algorithm: reno      File '1gb.txt' sent
CC algorithm: reno      File '1gb.txt' sent
CC algorithm: reno      File '1gb.txt' sent

┌──(tanjiro㉿kali)-[~/Desktop/Ex3]
└─$ ./sender
CC algorithm: cubic     File '1gb.txt' sent
CC algorithm: cubic     File '1gb.txt' sent
CC algorithm: cubic     File '1gb.txt' sent
CC algorithm: cubic     File '1gb.txt' sent
CC algorithm: cubic     File '1gb.txt' sent
CC algorithm: reno      File '1gb.txt' sent
CC algorithm: reno      File '1gb.txt' sent
CC algorithm: reno      File '1gb.txt' sent
CC algorithm: reno      File '1gb.txt' sent
CC algorithm: reno      File '1gb.txt' sent
```

20% lost:



25% lost:

30% lost:

This case was a little bit too hard for my computer, after a hour and a half I give up, hope you will forgive us.

Reno VS Cubic: