<u>Ex4 -Part A: Ohad Shirazi 318636693</u>

1 .In this question we will look about an advantage of the DoH:
DoH prevents "man in the middle" attack – since DNS queries are traditionally sent in plain text , DoH can reduce the risk of "man in the middle" attacks where someone can see what DNS queries you are running between you and your recursive server because it encrypts your queries.
In addition the encryption with DoH can protect sensitive information that DNS hijacking methodologies employ and obfuscate data that could be sniffed by third-party observer and ISPs
More than that because DoH centralizes DNS traffic to few DoH enable servers, load time performance is typically improved.

2. In this question we will look about some disadvantages of the DoH:
It overrides any sort of DNS filtering your network is doing to provide insight into security and your network info.
It provides a different experience from web browsing and to the rest of your computer and network. You might have some DNS packets going to one recursive server and then some going through your network settings, so you may have a different experience from browser to the rest of your network.
It weakens cyber-security. By encrypting DNS queries, companies using DNS monitoring for cybersecurity measures will lose visibility into data such as query type, response and originating IP that are used to determine bad actors.

3. One last disadvantage I want to discuss about is that it's almost impossible to have an end-to-end encrypted connection from your browser to "example.com" name server, without making it known to intermediate servers, due to the way DNS works.

It asks one of the internet root servers:
Question: "I want to visit www.example.com, do you know where it is?"
Answer: "No, but here are the nameservers for .com. Try your luck there!"
Then it asks the .com name servers:
Question: "So, can you tell me www.example.com's IP address?"
Answer: "You should ask the example.com name servers."
Finally it asks the example.com name servers:
Question: "What is the IP of www.example.com?"
Answer: "The ip is 123.123.123.123"
In each of these queries, the full hostname is sent to the DNS server. All of these servers now know that you want to visit www.example.com, even though this information is only of real interest to example.com's name server – obviously less than ideal in terms of privacy.

And now I want to discuss about a solution how to minimize this problem:
let's look about the same "conversation" from above in a different way:
It would ask the internet root servers:
Question: "Do you know the nameservers for .com?"
Answer: "Yes, here is their IP address"
Next, it would ask the .com nameservers:
Question: "Do you know the nameservers for example.com?"
Answer: "Yes, here is the IP address of the example.com nameserver"
Finally, it would ask the example.com nameservers:
Question: "Do you know the IP of www.example.com?"
Answer: "Yes, it is 123.123.123.123"

The only name server that knows the full hostname is the one for example.com, since it's also the only server that needs to know it. All the other servers only know a part of the query. This doesn't help you to stay completely anonymous, yet it does reduce the amount of data you give away.

4.

Type of implementation	**pros**	**cons**
DoH from the app layer	Some browsers have built-in DoH implementation and can thus perform queries by passing the operating system's DNS functionality.	The DoH transport method is HTTPS and most of the time this protocol is free to go over the organization's internal networks as well as over the internet. HTTPS is ubiquitous. It can freely go through any firewall and security solution. Its seldom analyzed and can go end to end without any control.
DoH proxy -network	We can use the proxy server as a regular web server at the same time that is acting as a proxy server.	The proxy serves a lot of people, so the path between the query to the proxy is visible to many more users and therefore, there are more chances to "man in the middle" attacks.
DoH proxy- local	Even if there is an attacker it the local network, he will not be able to read our DNS queries, since they are encrypted as soon as they leave our computer.	The proxy needs to be installed on each system wishing to use DoH, which might require a lot of effort in larger environments.
DoH from plugin	Available in most browsers, in addition there is flexibility about - the decision to use it or not	It may not inform the user if it skips DoH querying, either by misconfiguration or lack of support for DoH.

In my opinion, the preferred method out of the four is the 3rd- Implementing DoH at the local proxy server level. I think that the fact it can prevent attackers to be able to read our queries, overcomes the other's pros. His disadvantage is not so bad, I mean- it will cost us a lot of effort but it will be worth it. For me, as much protection and security as possible - more important than anything.

.5 A clear advantage that DOH has over Do53 is that the DoH send TCP queries (while the Do53 is working with UDP queries) – The TCP detects packet loss and performs retransmissions to ensure reliable messaging. Packet loss in a TCP connection is also used to avoid congestion and thus produces an intentionally reduced throughput for the connection.
The TCP requires an established connection before it can transmit traffic. It will also go back for any packets discarded during periods of high latency and resend the packets until the packets arrive at their destination.