Learn about DNS Over HTTPS

Mozilla's deployment of DNS over HTTPS has received a nomination for 'Internet Villain' of the Association of Internet Service Providers. Why so? What is DNS over HTTPS? Let's find out in the following article.

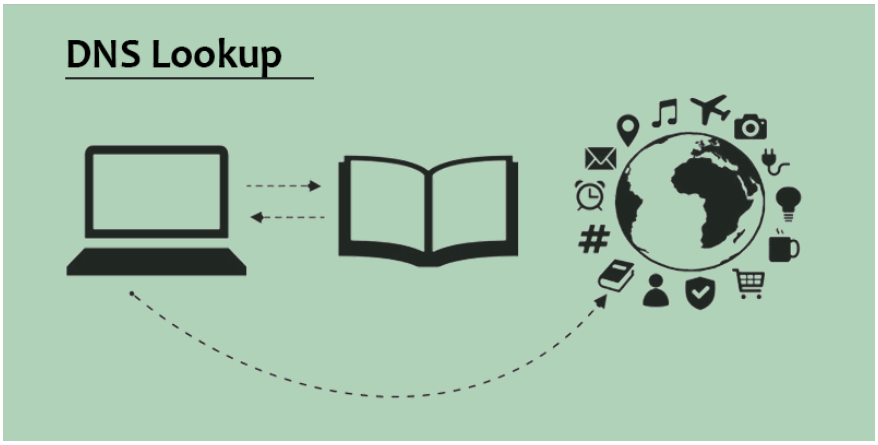
In general, when app developers add features that improve security, privacy and performance, they don't get much support. The deployment of Mozilla's DNS over HTTPS (an encryption way for computers to search for web addresses), has been nominated for 'Internet Villains' by the Association of Internet Service Providers (ISPA) of the UK and received many negative feedback from government agencies.

Why so? Because this feature encrypts the computer requests sent when it tries to find a site. UK service providers must comply with Internet monitoring and blocking rules, and many rules are implemented at the DNS level, so they do not agree that users have the right to bypass their filters.

Most Internet users disagree with the ISPA Association because DNS is encrypted that makes things better, keeps the browser more private, helps prevent network attacks and even works faster than regular DNS.

1. The best, fastest DNS list of Google, VNPT, FPT, Viettel, Singapore
2. The best top 10 Public DNS Server you should know now
3. 11 solutions to troubleshooting DNS Resolution

What is DNS? And what's the problem with it?

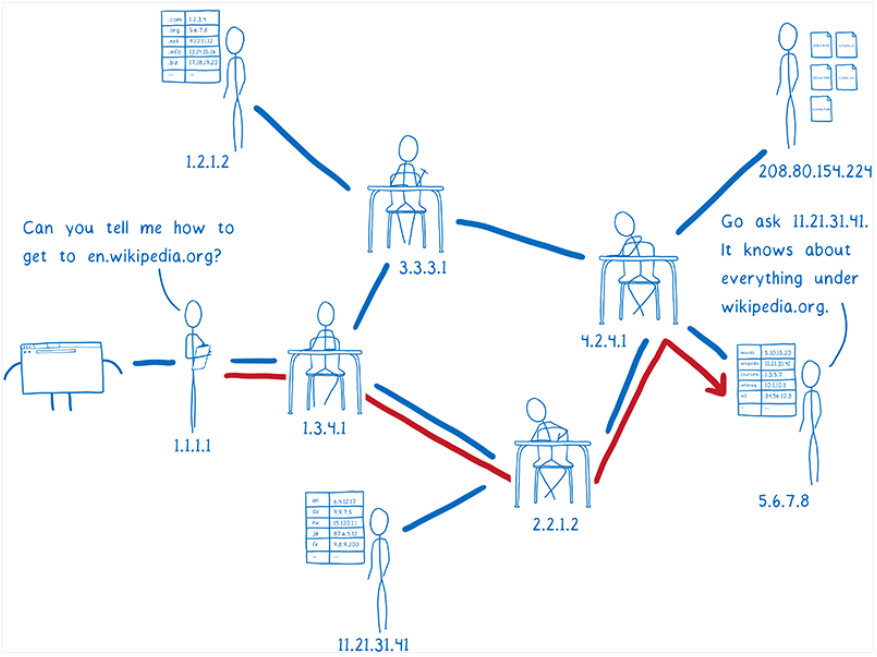


Without knowing how normal DNS works, this is a quick information about how it works:

1. All websites have IP addresses made up of numbers but are hard to remember so they often use names.
2. When we type the site name, ask for the appropriate number to be sent to the DNS server. This is where the IP address list is mapped to the name, requesting the phonebook server to indicate the actual number of

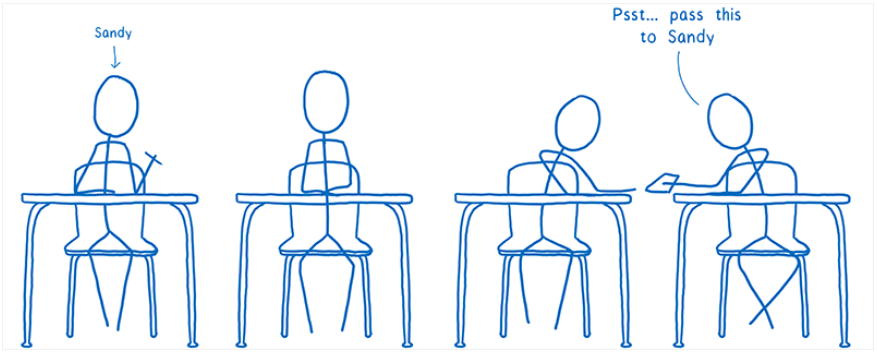
the website being accessed.

3. If it does not change, your default server will be the proposed server and / or server operated by your network provider. Your request will be there and the server will perform a series of tasks, transferring your request to several other places to put together.
4. After a few microseconds, the address you need will return to the device, allowing you to establish a connection to the web server you are visiting.



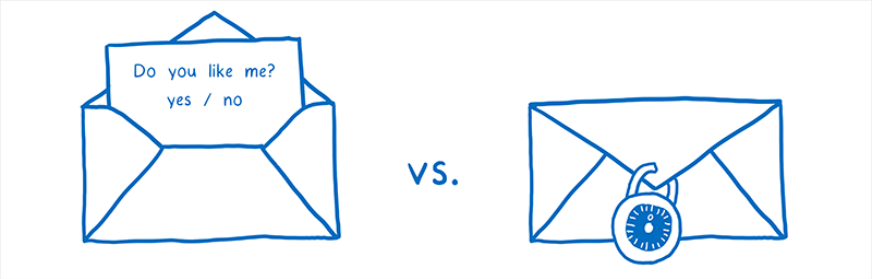
Basically, this is a complicated phonebook lookup process, and it only takes a few milliseconds. However, all this information is sent in plain text, so anyone who sees it (usually a service provider or maybe a hacker) can know where you visit and intervene. connect by blocking or sending the wrong address to access the malicious website.

1. How to enable redirection blocking to malicious websites on Google Chrome



The image above uses a metaphor for a student to pass a piece of paper to Sandy. This piece of paper can reach Sandy. But now everyone knows you need to switch to Sandy if you want them to read it or fake it. It would be better to have a way to write notes in secret code and send it to the recipient without anyone knowing. That's exactly what DNS over HTTPS does.

How is DNS over HTTPS different from regular DNS?



If sending data using HTTP (the basic protocol for data transfer over the web), the data will be in plain text, everyone can read it (similar to regular DNS). HTTPS is encrypted so no one can block readable data. With DNS over HTTPS, your DNS request is sent to the name server via the same secure channel of credit card data transfer when you are on the shopping site.

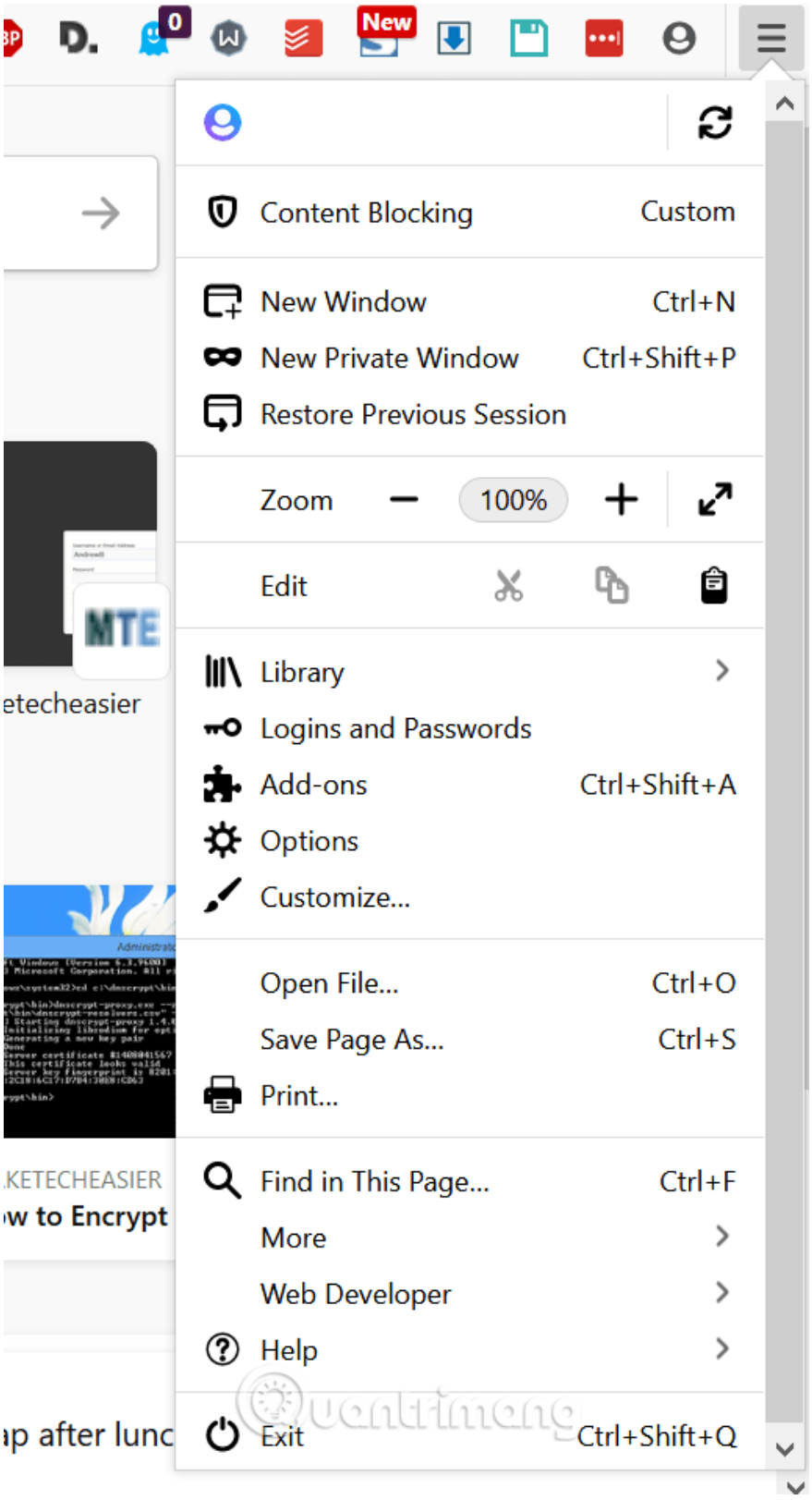
No one, including Internet service providers, can know the content inside. Requests cannot be blocked or logged in, so countries like Britain and China will have difficulty filtering and tracking traffic. This does not mean that you are not being followed completely because your service provider can still view the address you are connected to but does not know the details of your activity.

Firefox has also partnered with Cloudflare to 'break' your request into sections, so no server has the full address you are looking for.

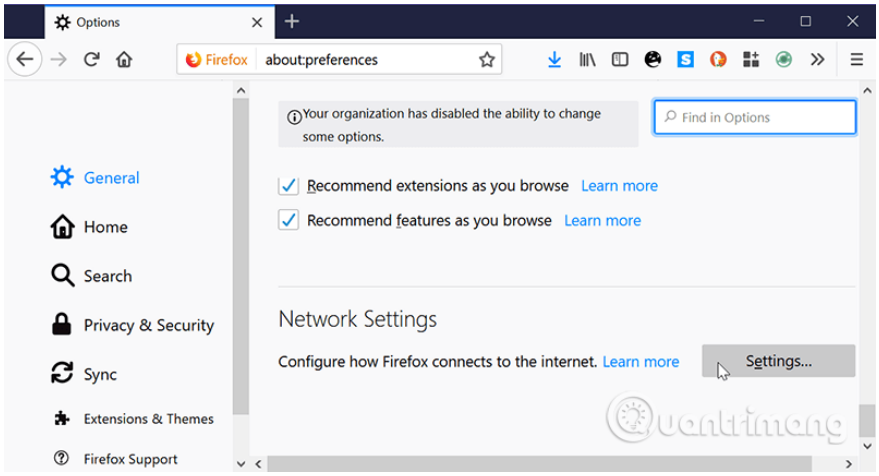
How to enable DNS over HTTPS

DNS over HTTPS is not currently enabled by default in Firefox, but enabling it is relatively simple.

Step 1 . Open the menu of three horizontal lines at the top.

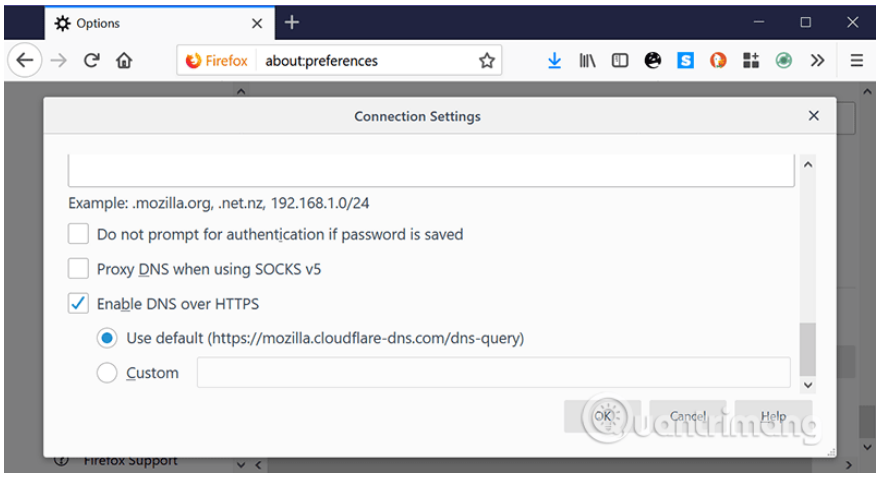


Step 2 . Go to **Options** and scroll down to the **General** section until you see the **Network Settings** option.



Step 3 . Select the option **Enable DNS over HTTPS** . You can use Cloudflare by default (recommended for use because it has many additional security features) or select **Custom** and enter your DNS service.

1. 4 major security risks that Cloudflare DNS can resolve



You can check its performance on Dnsleaktest.com. You will see the Cloudflare DNS server appear. So you've added some privacy, privacy and censorship settings when browsing online.

If you use Chrome, you'll have to wait until Google activates this feature.

1. How to change DNS to surf faster, speed up Internet

You finished reading the article "**Learn about DNS Over HTTPS**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.