# Lab - Using Anonsurf on Kali Linux to Stay Anonymous

## Overview

In this lab, you will learn how to hide your identity on the Internet using anonsurf. Anonsurf is a script made by the ParrotSec team that completely anonymizes you with just one click of a button using TOR proxies. Anonsurf automatically routes ALL your traffic through TOR, including your DNS requests to prevent DNS leaks.

## Requirements

- One updated virtual install of Kali Linux
- Internet access
- Logged on as root

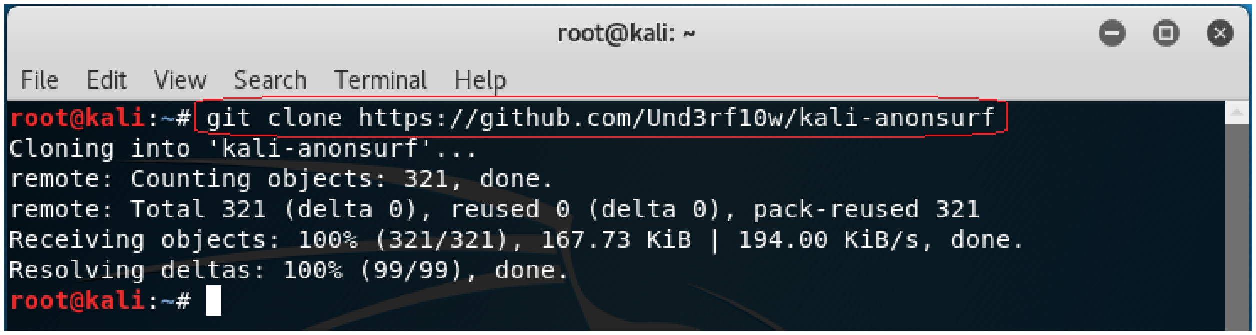
## Begin the lab!

To begin the lab, open a new terminal inside of Kali. We next need to download and install a repository called anonsurf.

Type or copy and paste the following command into your kali terminal.

```
git clone https://github.com/Und3rf10w/kali-anonsurf
```

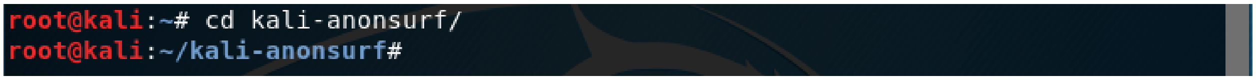
Hit enter.



```
root@kali:~# git clone https://github.com/Und3rf10w/kali-anonsurf
Cloning into 'kali-anonsurf'...
remote: Counting objects: 321, done.
remote: Total 321 (delta 0), reused 0 (delta 0), pack-reused 321
Receiving objects: 100% (321/321), 167.73 KiB | 194.00 KiB/s, done.
Resolving deltas: 100% (99/99), done.
root@kali:~#
```

We next to need to change directories over to the downloaded repository .

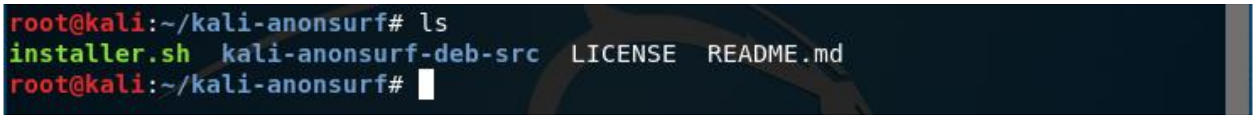
```
cd kali-anonsurf/
```



```
root@kali:~# cd kali-anonsurf/
root@kali:~/kali-anonsurf#
```

Notice your prompt changes to let you know you are inside the kali-anonsurf directory.

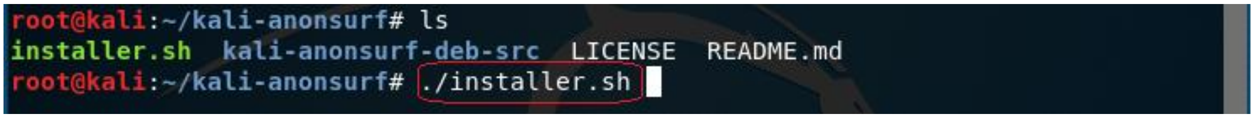
Type ls at the prompt to list the contents of the directory.



```
root@kali:~/kali-anonsurf# ls
installer.sh  kali-anonsurf-deb-src  LICENSE  README.md
root@kali:~/kali-anonsurf# 
```

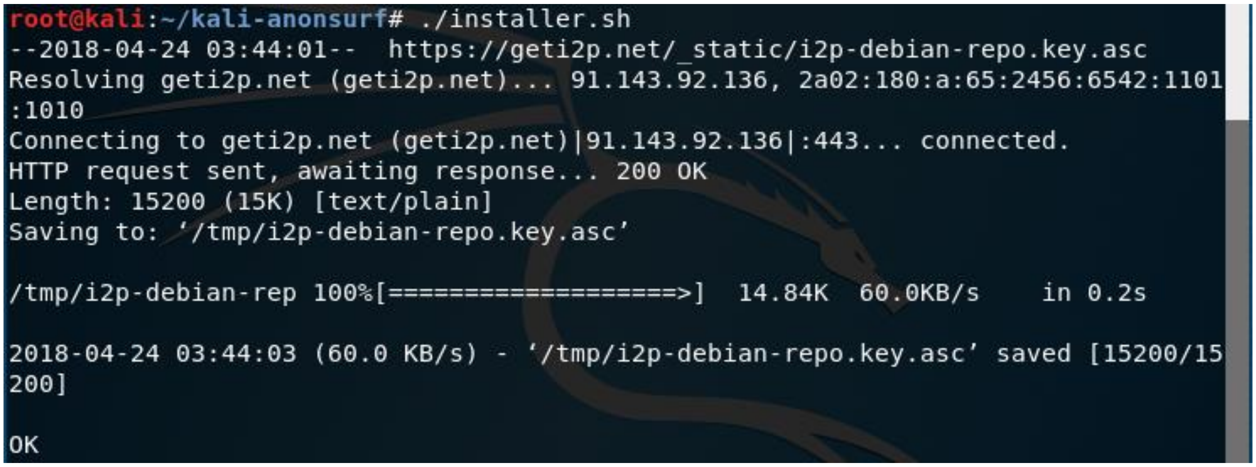
From the list of contents, we need to run the installer.sh.

At the prompt type: `./installer.sh`



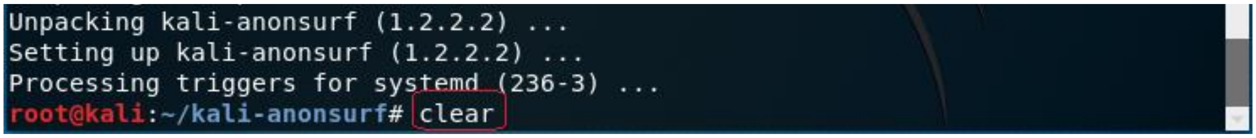
```
root@kali:~/kali-anonsurf# ls
installer.sh  kali-anonsurf-deb-src  LICENSE  README.md
root@kali:~/kali-anonsurf# ./installer.sh
```

Allow the install to complete. Be patient, it is a large repository and depending on how current your Kali install is; it may take a few minutes to update.



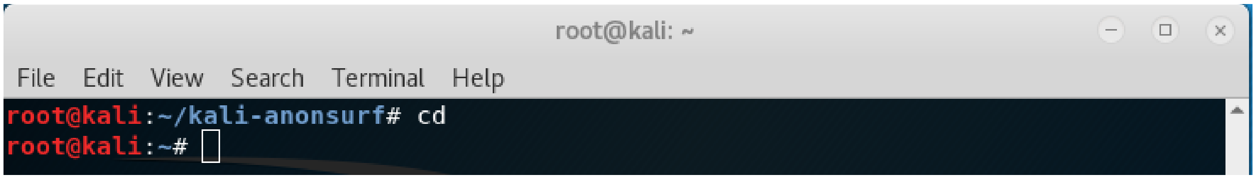
```
root@kali:~/kali-anonsurf# ./installer.sh
--2018-04-24 03:44:01--  https://geti2p.net/_static/i2p-debian-repo.key.asc
Resolving geti2p.net (geti2p.net)... 91.143.92.136, 2a02:180:a:65:2456:6542:1101
:1010
Connecting to geti2p.net (geti2p.net)|91.143.92.136|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15200 (15K) [text/plain]
Saving to: ‘/tmp/i2p-debian-repo.key.asc’

/tmp/i2p-debian-rep 100%[===================>]  14.84K  60.0KB/s    in 0.2s

2018-04-24 03:44:03 (60.0 KB/s) - ‘/tmp/i2p-debian-repo.key.asc’ saved [15200/15
200]

OK
```

Once the install completes, you can clear the terminal and return to your home directory.



```
Unpacking kali-anonsurf (1.2.2.2) ...
Setting up kali-anonsurf (1.2.2.2) ...
Processing triggers for systemd (236-3) ...
root@kali:~/kali-anonsurf# clear
```

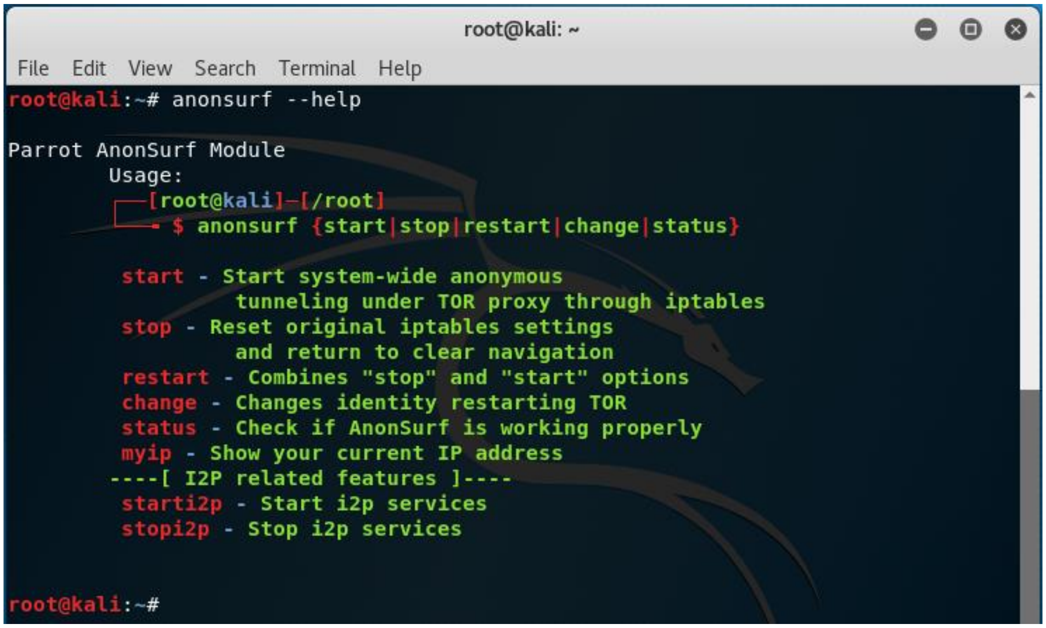
Return to your home directory.



```
root@kali:~/kali-anonsurf# cd
root@kali:~# 
```

Review the available switches by typing:

```
anonsurf –help
```



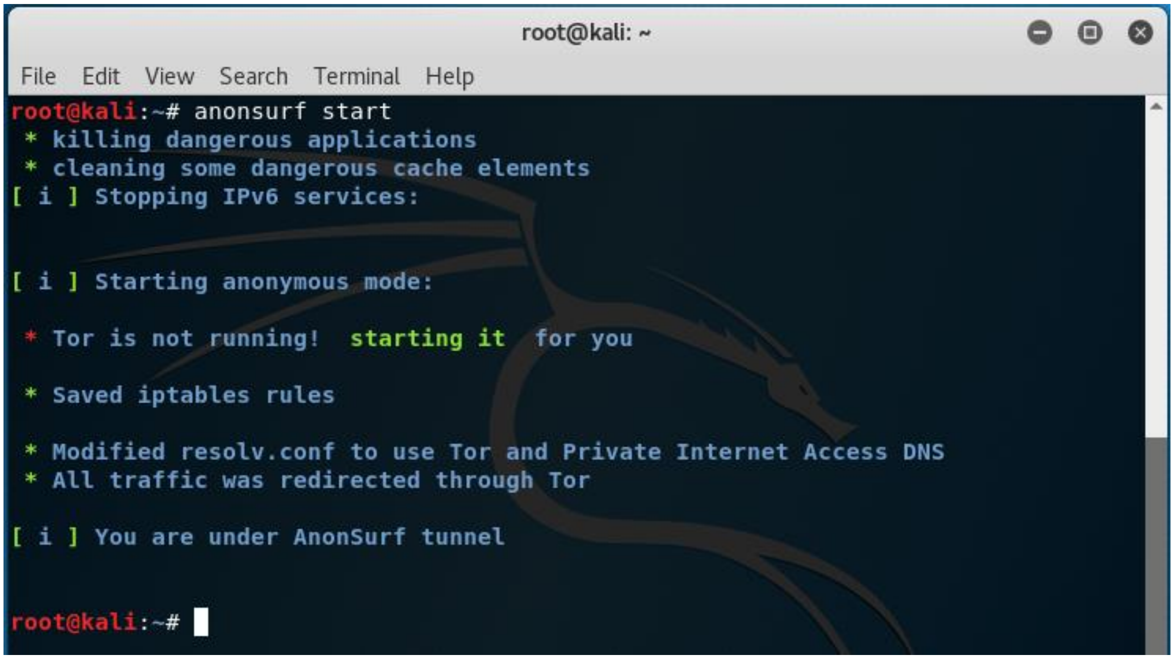
```
root@kali:~# anonsurf --help

Parrot AnonSurf Module
        Usage:
        ┌─[root@kali]─[/root]
        └──╼ $ anonsurf {start|stop|restart|change|status}

         start - Start system-wide anonymous
                  tunneling under TOR proxy through iptables
         stop - Reset original iptables settings
                  and return to clear navigation
         restart - Combines "stop" and "start" options
         change - Changes identity restarting TOR
         status - Check if AnonSurf is working properly
         myip - Show your current IP address
        ----[ I2P related features ]----
         starti2p - Start i2p services
         stopi2p - Stop i2p services

root@kali:~#
```

Here you are shown how easy it is to start, restart or stop anonsurf. Take the time to become familiar with the help menu as this will answer many f your question on how to start the program or change your geolocation.

**Using anonsurf**

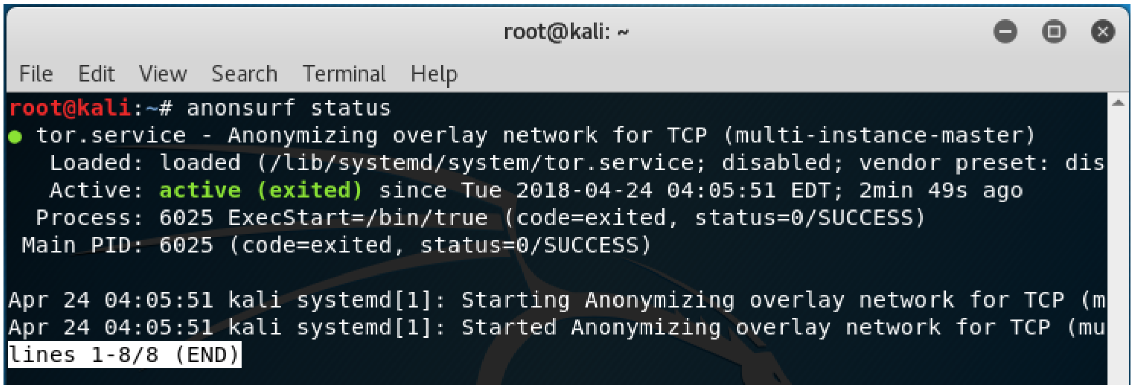
Anonsurf runs as a service so we can start anonsurf by typing **`anonsurf start`** at the terminal prompt.

Be sure to read everything on the terminal screen.



```
root@kali:~# anonsurf start
 * killing dangerous applications
 * cleaning some dangerous cache elements
[ i ] Stopping IPv6 services:


[ i ] Starting anonymous mode:

 * Tor is not running!  starting it  for you

 * Saved iptables rules

 * Modified resolv.conf to use Tor and Private Internet Access DNS
 * All traffic was redirected through Tor

[ i ] You are under AnonSurf tunnel


root@kali:~# █
```

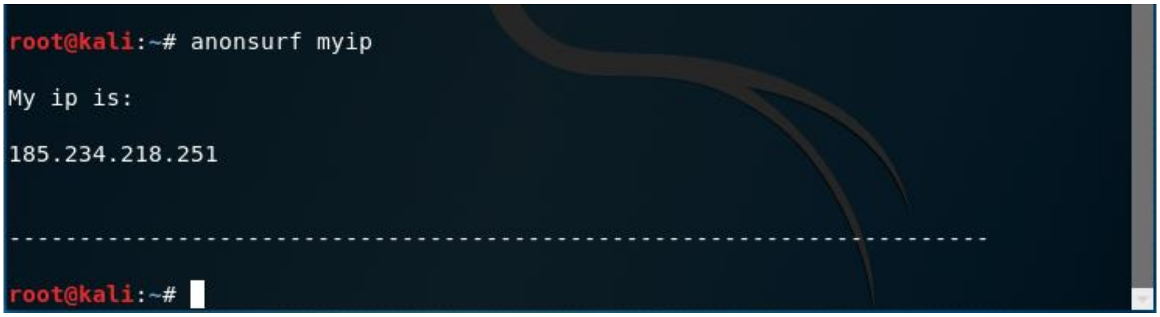
Check the status of anonsurf using the **`anonsurf status`** command. If the results show the service is running in green, anonsurf is running.



```
root@kali:~# anonsurf status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: dis
   Active: active (exited) since Tue 2018-04-24 04:05:51 EDT; 2min 49s ago
  Process: 6025 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 6025 (code=exited, status=0/SUCCESS)

Apr 24 04:05:51 kali systemd[1]: Starting Anonymizing overlay network for TCP (m
Apr 24 04:05:51 kali systemd[1]: Started Anonymizing overlay network for TCP (mu
lines 1-8/8 (END)
```

Close your terminal and open a fresh one.

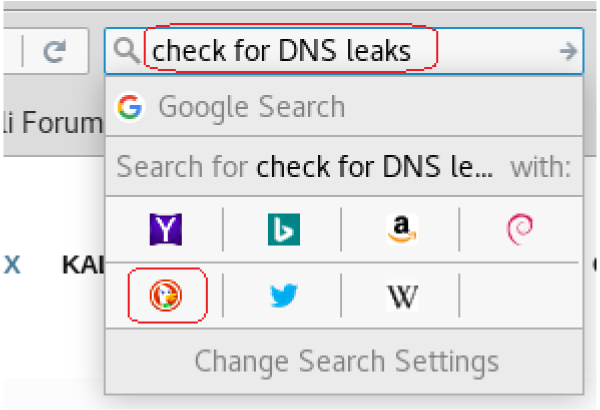
Use you up arrow and find the anonsurf –help command and hit enter. Find the switch that will show your current IP address. **`anonsurf myip`**



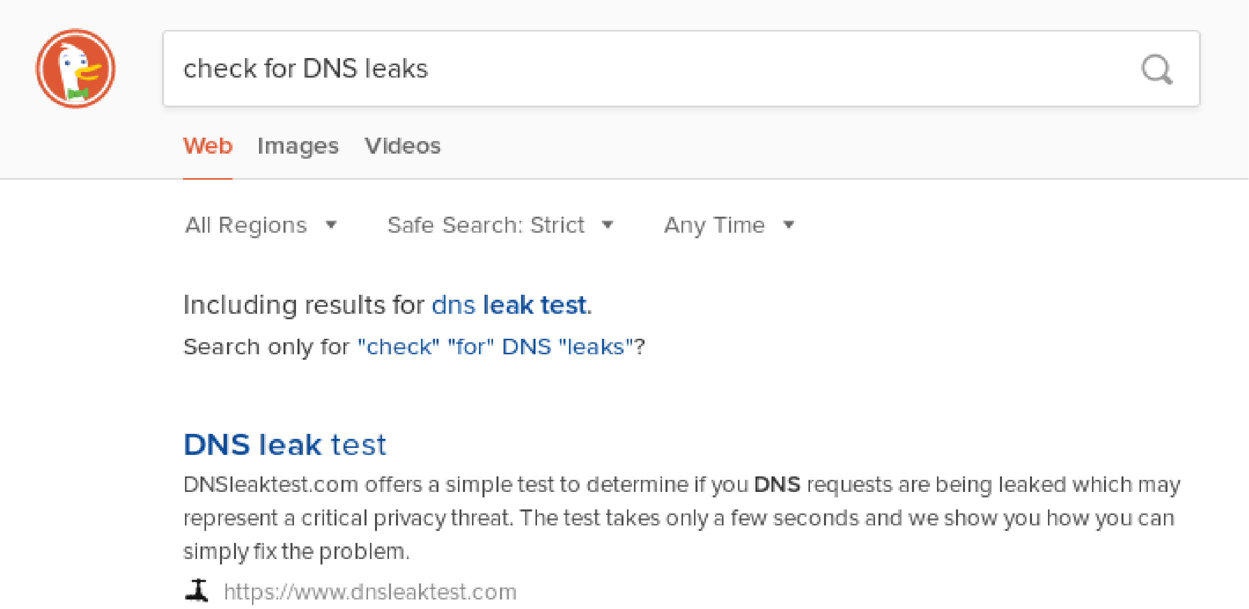
```
root@kali:~# anonsurf myip

My ip is:

185.234.218.251


-----------------------------------------------------------------------

root@kali:~# 
```

We can't really tell what country our IP is for, but as in our previous two labs, we can use our browsers search bar to search for search for DNS leaks.

From your Kali's quick launch bar, open your Firefox browser. In the search bar, type, "check for DNS leaks" without the quotes. Choose duckduckgo.com as your preferred search engine.



From the search results returned, select the first result from the list or find DNS leak test in the results.



Including results for dns **leak test**.

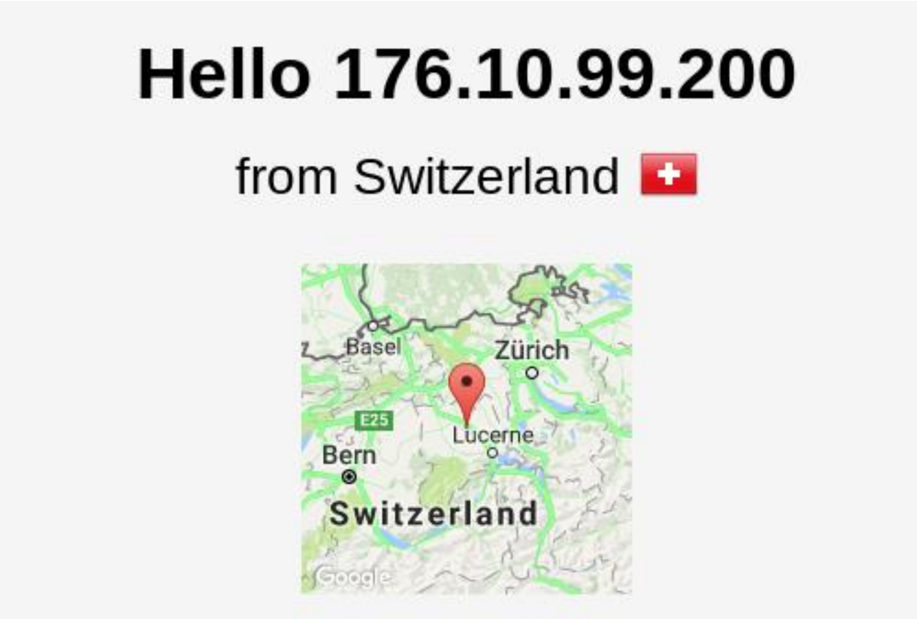
Search only for "check" "for" DNS "leaks"?

DNS leak test

DNSleaktest.com offers a simple test to determine if you **DNS** requests are being leaked which may represent a critical privacy threat. The test takes only a few seconds and we show you how you can simply fix the problem.

https://www.dnsleaktest.com

My result shows my current IP address is from Switzerland.

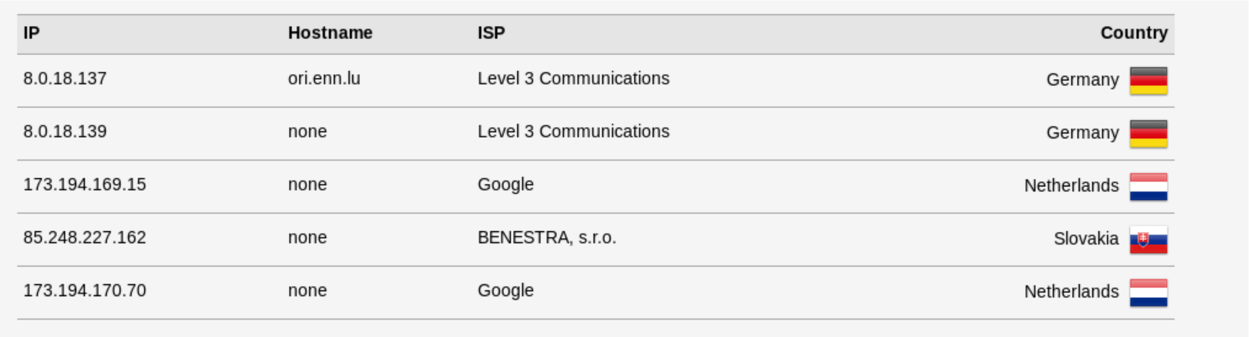


Hello 176.10.99.200

from Switzerland

If I scroll down the page and click on the button marked Standard Test, I have the option to conduct a DNS leak test.

Read everything on the results page.



| IP | Hostname | ISP | Country |
|---|---|---|---|
| 8.0.18.137 | ori.enn.lu | Level 3 Communications | Germany |
| 8.0.18.139 | none | Level 3 Communications | Germany |
| 173.194.169.15 | none | Google | Netherlands |
| 85.248.227.162 | none | BENESTRA, s.r.o. | Slovakia |
| 173.194.170.70 | none | Google | Netherlands |

I show several DNS providers but as stated in the results, each provider may or may not store your original IP address, and the privacy policy varies from one DNS provider to the next.

Use the **`anonsurf restart`** command to change your current identity and your DNS providers. You can do this as many times as you want.

**Summary**

Anonsurf is another tool we can use to help hide our real identity while surfing the Internet. Using a different surf engine such as duckduckgo.com can help reduce the tracks we leave on the Internet when conducting searches. Duckduckgo states it does not log search activity of anyone using their site.