

Redes de Computadores

Prof. Jean Carlos

Aluno

Rafael Augusto Campos Plinio

PROXY

Introdução

A internet está cheia de maravilhas, como por exemplo notícias em tempo real, vídeos, fotos, jogos, bate-papos, etc. Porém, durante o trajeto dos dados pela internet, os mesmos podem ser, de certa forma, obtidos e dependendo de quem o faz, podem nos trazer transtornos futuramente.

O servidor proxy serve como intermediário no fluxo do tráfego da internet, fazendo com que suas atividades virtuais pareçam estar vindo de outro lugar ao invés do seu local geográfico atual. Isto é bem útil para burlar restrições por região de algum serviço, como por exemplo Netflix. A Netflix oferece um catálogo diferente em sua biblioteca dependendo da região (país) que você está, então se você usar um Proxy para enganar a sua real localização, você pode ter acesso ao conteúdo de outro país.

Proxy

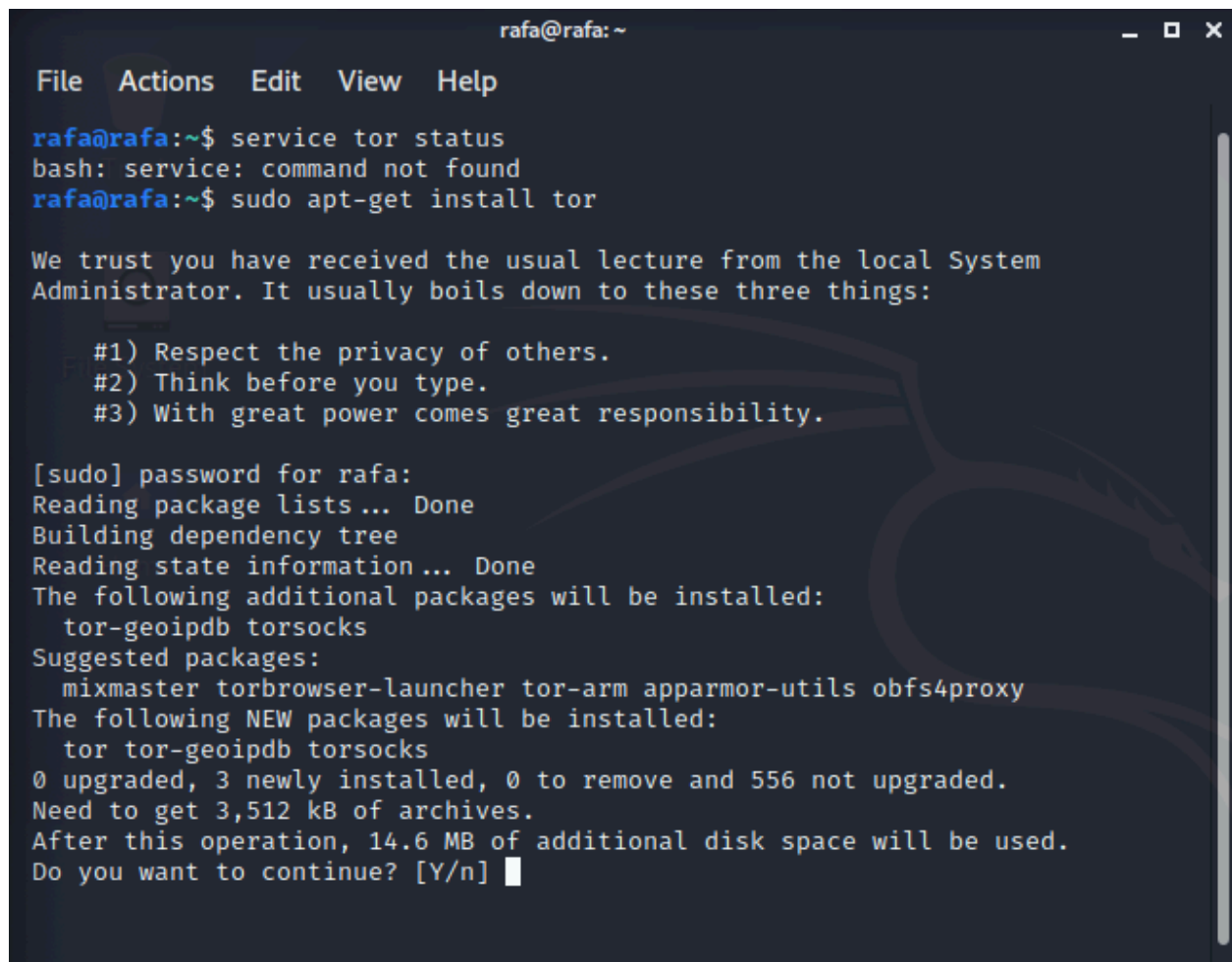
Os 2 tipos mais comuns de proxy são HTTP e SOCKS. A diferença entre eles é que o HTTP trabalha com tráfego de dados web, enquanto que o SOCKS é indiferente ao tipo de tráfego que passa por ele.

Nesta tarefa iremos utilizar:

- Sistema Operacional: Kali Linux (principal) e MacOS (para comparação)
- Software de Rede: TOR;
- Proxy: proxychains;

Vamos começar verificando se o sistema possui o serviço TOR: `service tor status`

Caso não tenha, instalar com: `sudo apt-get install tor`

A terminal window titled 'rafa@rafa: ~' with a menu bar (File, Actions, Edit, View, Help). The user runs 'service tor status', which returns 'bash: service: command not found'. Then, the user runs 'sudo apt-get install tor'. The terminal displays the standard Ubuntu-style warning about the System Administrator, followed by three numbered points: '#1) Respect the privacy of others.', '#2) Think before you type.', and '#3) With great power comes great responsibility.' The user is prompted for their password. The terminal then shows the package list being read, the dependency tree being built, and the state information being read. It lists additional packages to be installed (tor-geoipdb, torsocks) and suggested packages (mixmaster, torbrowser-launcher, tor-arm, apparmor-utils, obfs4proxy). It also lists the new packages to be installed (tor, tor-geoipdb, torsocks). Finally, it shows the disk space requirements: 0 upgraded, 3 newly installed, 0 to remove, and 556 not upgraded. It states that 3,512 kB of archives are needed and that 14.6 MB of additional disk space will be used. The prompt 'Do you want to continue? [Y/n]' is shown with a cursor. The background of the terminal has a faint dragon logo.

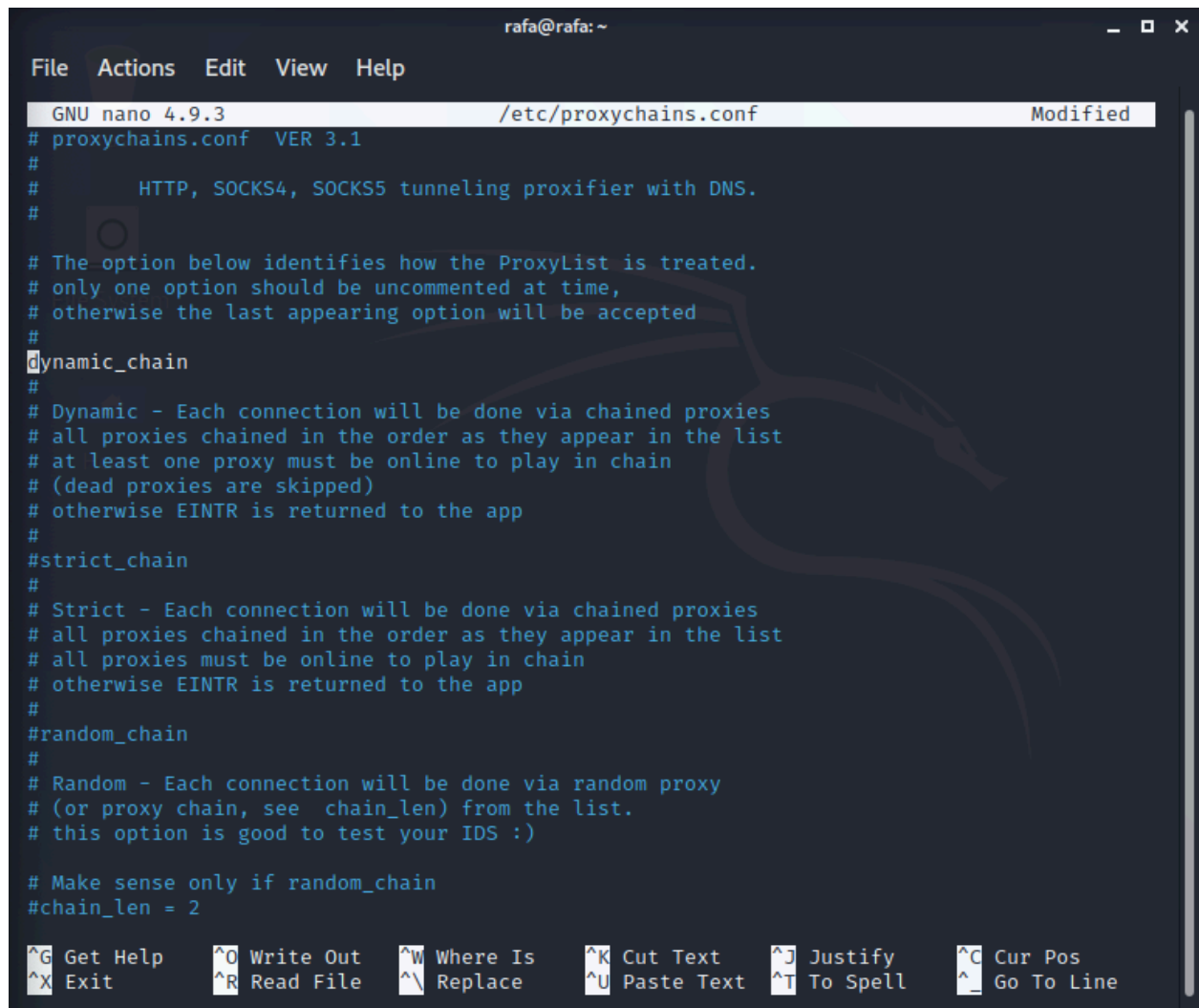
```
rafa@rafa: ~  
File Actions Edit View Help  
rafa@rafa:~$ service tor status  
bash: service: command not found  
rafa@rafa:~$ sudo apt-get install tor  
  
We trust you have received the usual lecture from the local System  
Administrator. It usually boils down to these three things:  
  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
  
[sudo] password for rafa:  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following additional packages will be installed:  
  tor-geoipdb torsocks  
Suggested packages:  
  mixmaster torbrowser-launcher tor-arm apparmor-utils obfs4proxy  
The following NEW packages will be installed:  
  tor tor-geoipdb torsocks  
0 upgraded, 3 newly installed, 0 to remove and 556 not upgraded.  
Need to get 3,512 kB of archives.  
After this operation, 14.6 MB of additional disk space will be used.  
Do you want to continue? [Y/n]
```

Só confirmar com "y" e dar ENTER

Agora configurar o serviço proxy (proxychains).

`nano /etc/proxychains.conf`

OBS: Use o editor de texto de sua escolha (prefiro o nano).

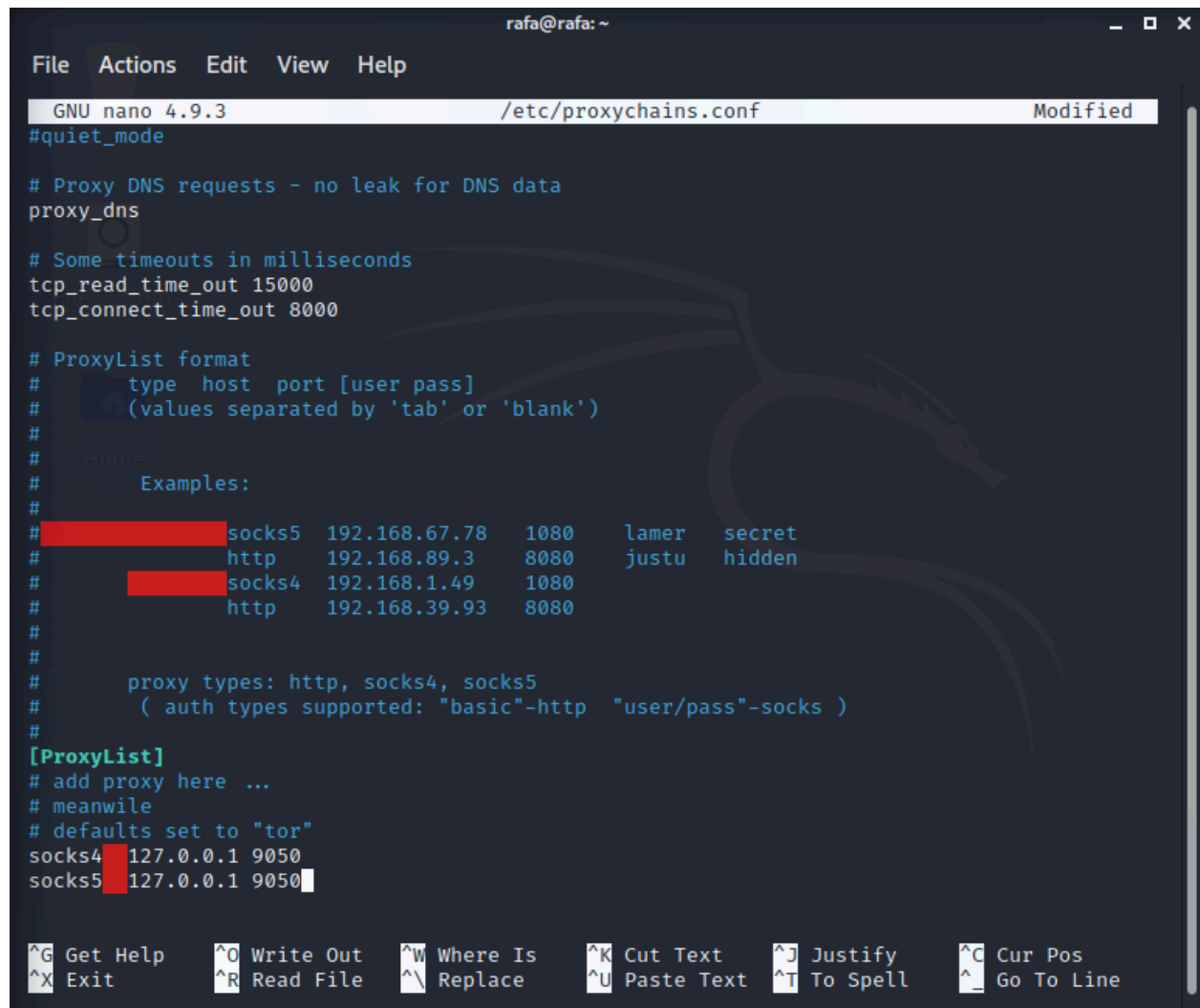


```
rafa@rafa: ~  
File Actions Edit View Help  
GNU nano 4.9.3 /etc/proxychains.conf Modified  
# proxychains.conf VER 3.1  
#  
# HTTP, SOCKS4, SOCKS5 tunneling proxifier with DNS.  
#  
# The option below identifies how the ProxyList is treated.  
# only one option should be uncommented at time,  
# otherwise the last appearing option will be accepted  
#  
dynamic_chain  
#  
# Dynamic - Each connection will be done via chained proxies  
# all proxies chained in the order as they appear in the list  
# at least one proxy must be online to play in chain  
# (dead proxies are skipped)  
# otherwise EINTR is returned to the app  
#  
#strict_chain  
#  
# Strict - Each connection will be done via chained proxies  
# all proxies chained in the order as they appear in the list  
# all proxies must be online to play in chain  
# otherwise EINTR is returned to the app  
#  
#random_chain  
#  
# Random - Each connection will be done via random proxy  
# (or proxy chain, see chain_len) from the list.  
# this option is good to test your IDS :)  
  
# Make sense only if random_chain  
#chain_len = 2  
  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos  
^X Exit ^R Read File ^\ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

Se apresentar um aviso vermelho dizendo que não pode ser alterado, refaça o comando utilizando sudo: `sudo nano /etc/proxychains.conf`

Remover o comentário (#) de “dynamic_chain” e adicionar # nas linhas “strict_chain” e “random_chain”

Mais embaixo no mesmo arquivo (proxychains.conf), deixar proxy_dns descomentado e adicionar socks5 127.0.0.1 9050 na ultima linha em proxy list.

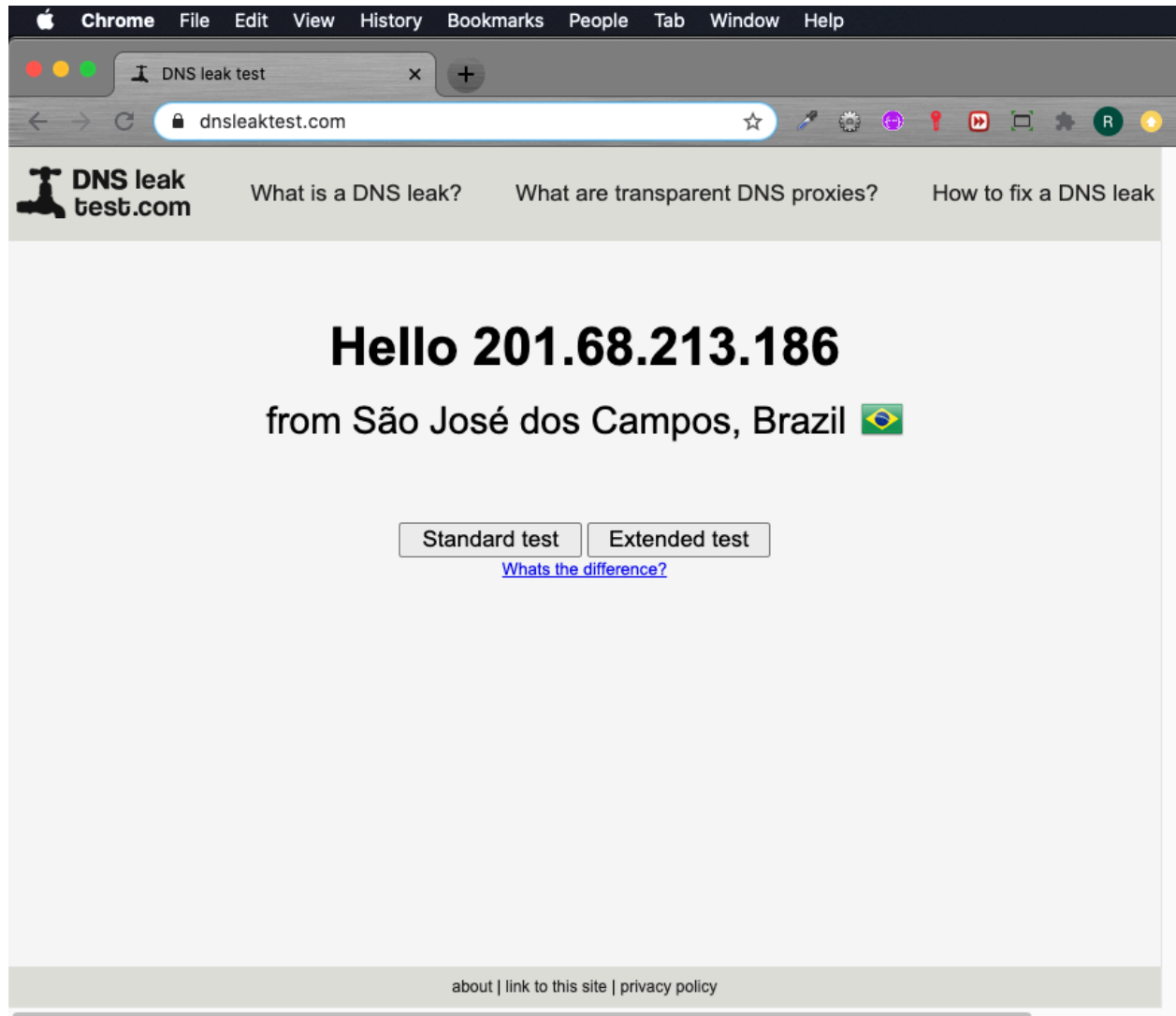


```
rafa@rafa: ~  
File Actions Edit View Help  
GNU nano 4.9.3 /etc/proxychains.conf Modified  
#quiet_mode  
  
# Proxy DNS requests - no leak for DNS data  
proxy_dns  
  
# Some timeouts in milliseconds  
tcp_read_time_out 15000  
tcp_connect_time_out 8000  
  
# ProxyList format  
# type host port [user pass]  
# (values separated by 'tab' or 'blank')  
#  
# Examples:  
# socks5 192.168.67.78 1080 lamer secret  
# http 192.168.89.3 8080 justu hidden  
# socks4 192.168.1.49 1080  
# http 192.168.39.93 8080  
#  
# proxy types: http, socks4, socks5  
# ( auth types supported: "basic"-http "user/pass"-socks )  
#  
[ProxyList]  
# add proxy here ...  
# meanwhile  
# defaults set to "tor"  
socks4 127.0.0.1 9050  
socks5 127.0.0.1 9050  
  
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos  
^X Exit ^R Read File ^_ Replace ^U Paste Text ^T To Spell ^_ Go To Line
```

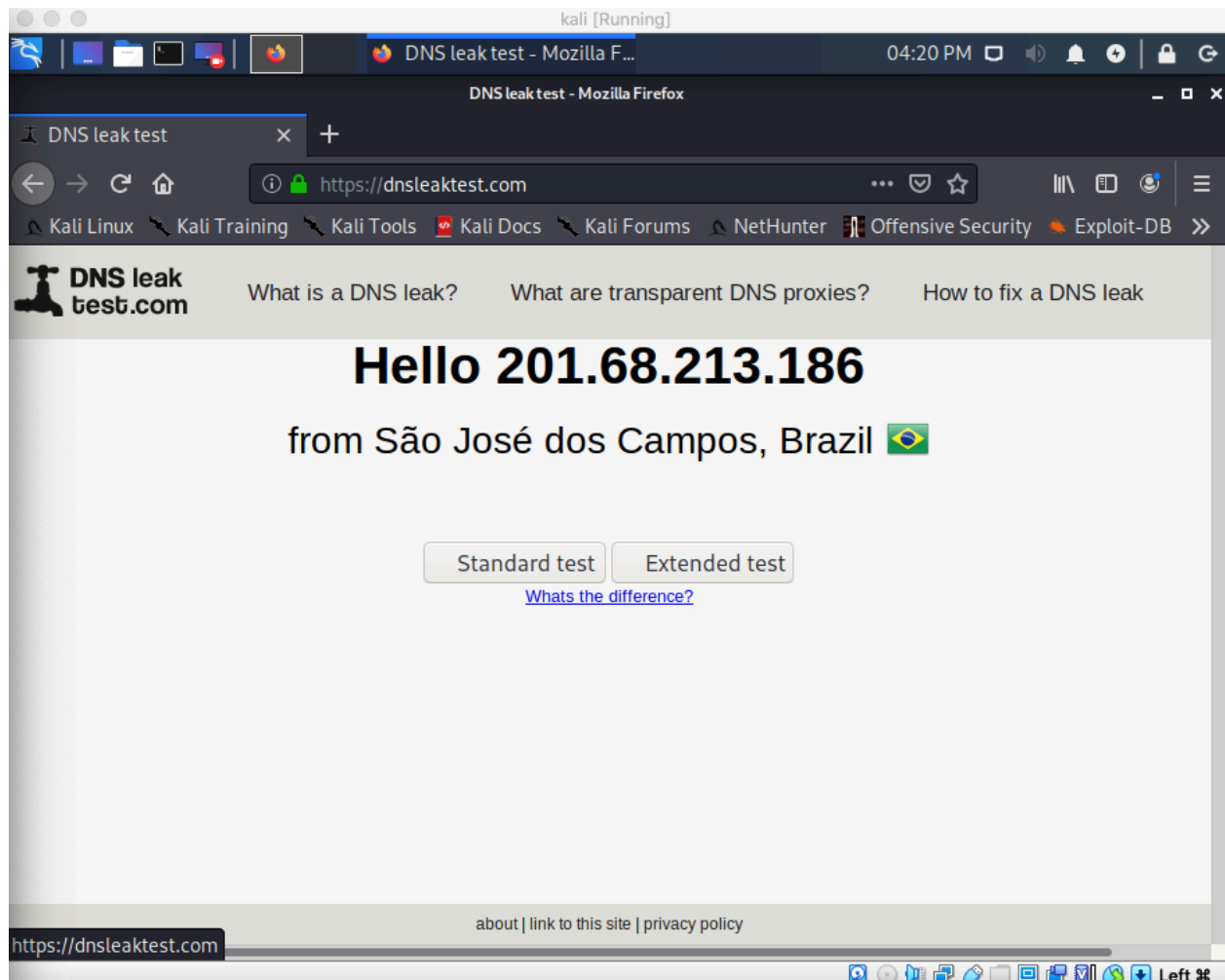
Salve o arquivo e feche o terminal.

Testando o proxy

Para testar o proxy iremos comparar o IP que o site <https://www.dnsleaktest.com/> nos retorna (é nosso endereço IP que devemos ver), vou abrir o navegador (chrome) em outro computador e sistema operacional usado será o macOS e ver qual endereço IP é exibido.



Agora vamos repetir o procedimento no computador (através da VirtualBox) em que instalamos e configuramos o nosso proxy (mas com o proxy ainda DESLIGADO), isto é para podermos confirmar que o IP realmente é o mesmo que obtivemos no computador anterior (macOS).

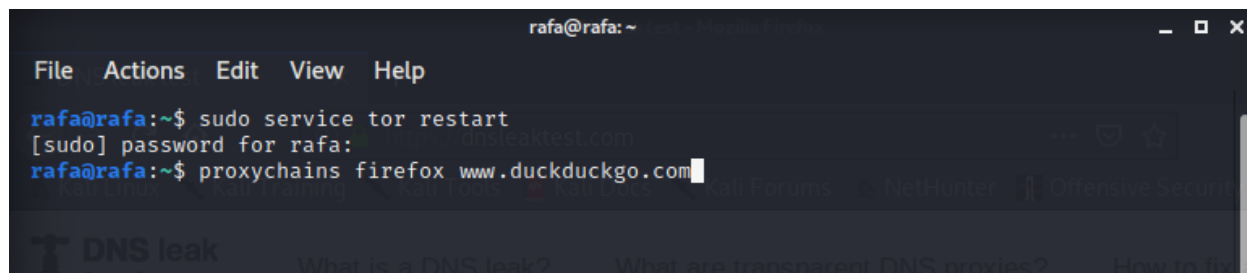


Podemos ver que o endereço IP é o mesmo.

Agora vamos repetir este procedimento com o nosso proxy LIGADO. Reinicie o TOR e inicie o proxychains no navegador (Firefox) com um link de algum site de busca (vou usar o duckduckgo).

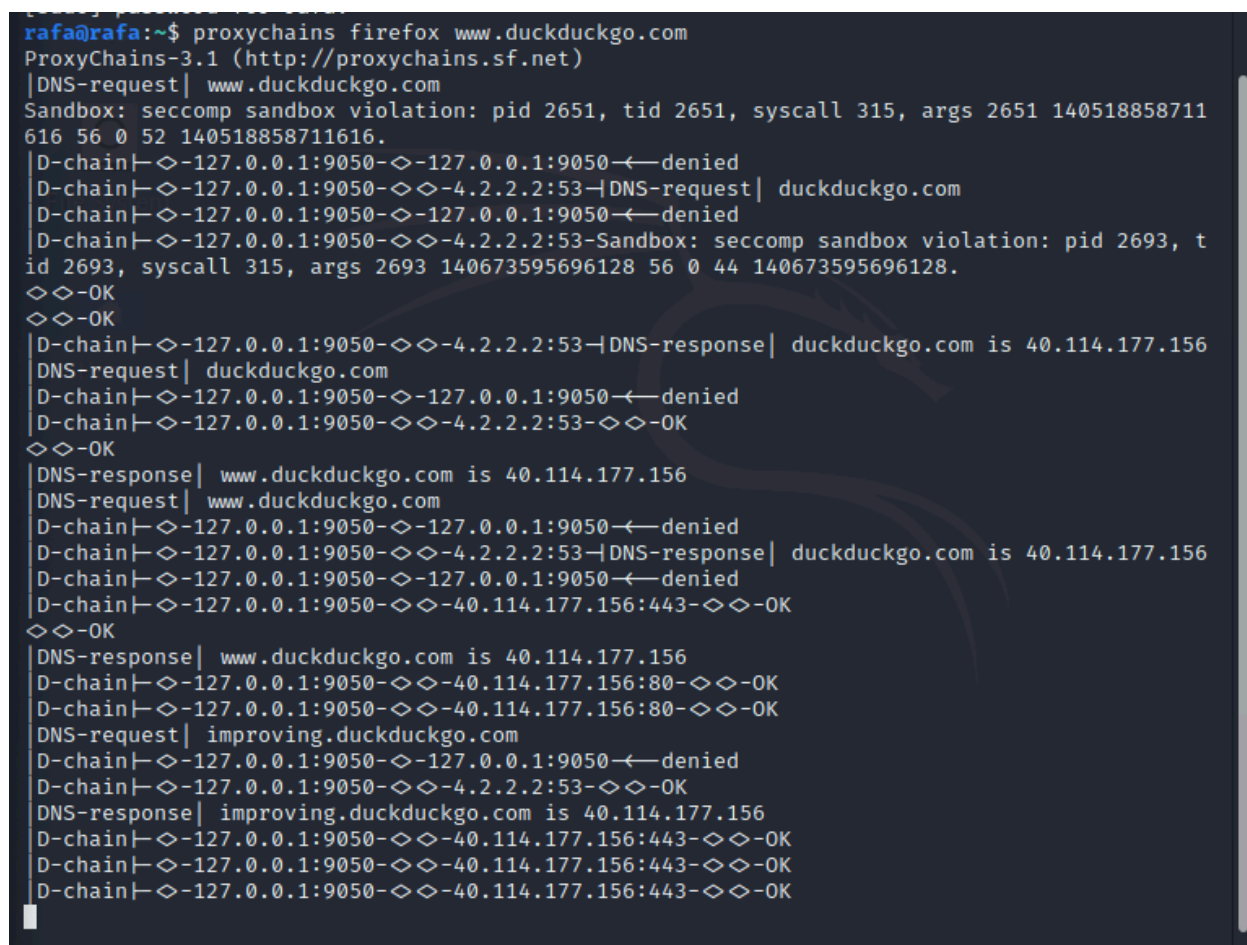
Reiniciando o TOR: `sudo service tor restart`

Iniciando o proxychains: `proxychains firefox www.duckduckgo.com`



```
rafa@rafa: ~  
File Actions Edit View Help  
rafa@rafa:~$ sudo service tor restart  
[sudo] password for rafa:  
rafa@rafa:~$ proxychains firefox www.duckduckgo.com
```

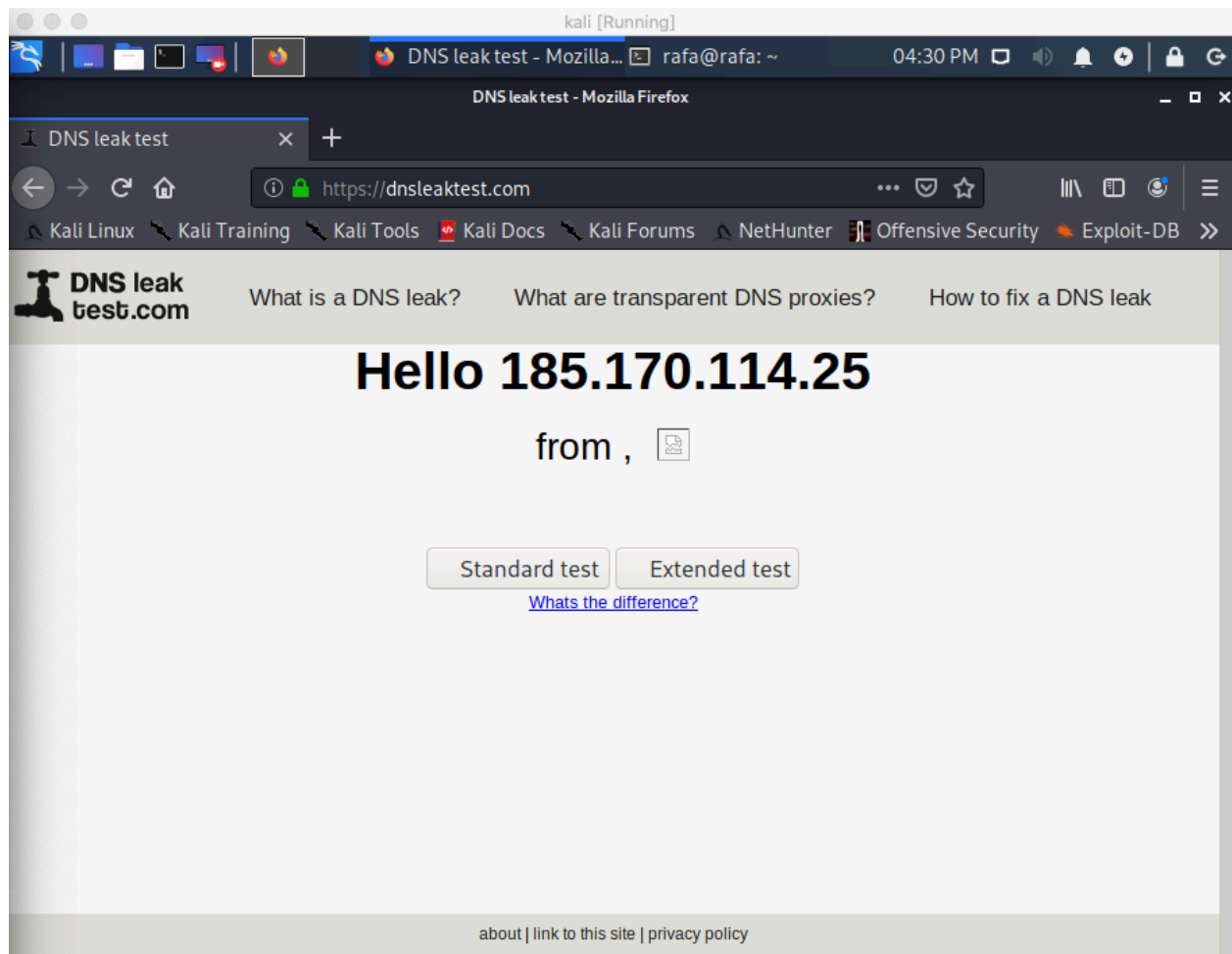
Ao iniciar o proxychains, o terminal ira exibir dados em tempo real da comunicação que ocorre, algo parecido com isso:



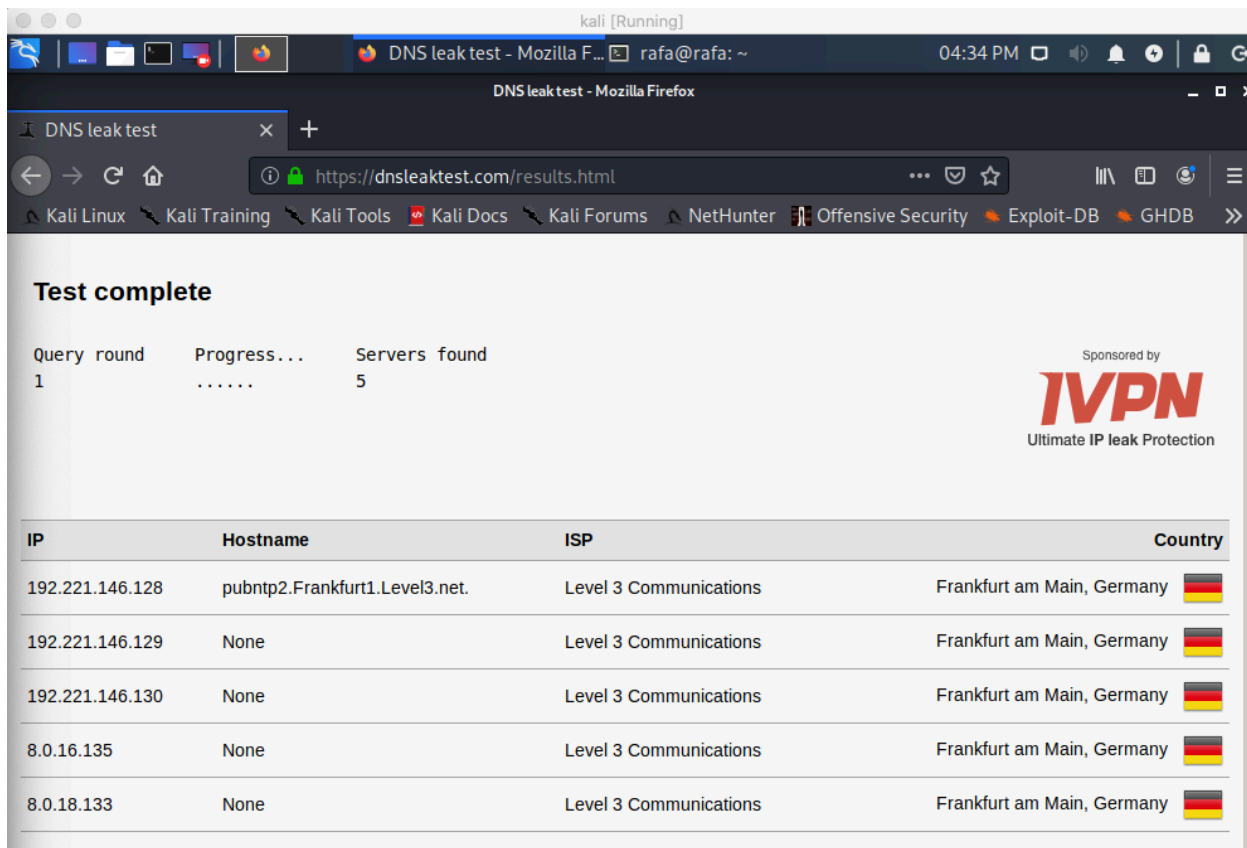
```
rafa@rafa:~$ proxychains firefox www.duckduckgo.com  
ProxyChains-3.1 (http://proxychains.sf.net)  
|DNS-request| www.duckduckgo.com  
Sandbox: seccomp sandbox violation: pid 2651, tid 2651, syscall 315, args 2651 140518858711616 56 0 52 140518858711616.  
|D-chain| -127.0.0.1:9050->-127.0.0.1:9050<-denied  
|D-chain| -127.0.0.1:9050->-4.2.2.2:53->DNS-request| duckduckgo.com  
|D-chain| -127.0.0.1:9050->-127.0.0.1:9050<-denied  
|D-chain| -127.0.0.1:9050->-4.2.2.2:53->Sandbox: seccomp sandbox violation: pid 2693, tid 2693, syscall 315, args 2693 140673595696128 56 0 44 140673595696128.  
<<-OK  
<<-OK  
|D-chain| -127.0.0.1:9050->-4.2.2.2:53->DNS-response| duckduckgo.com is 40.114.177.156  
|DNS-request| duckduckgo.com  
|D-chain| -127.0.0.1:9050->-127.0.0.1:9050<-denied  
|D-chain| -127.0.0.1:9050->-4.2.2.2:53-><<-OK  
<<-OK  
|DNS-response| www.duckduckgo.com is 40.114.177.156  
|DNS-request| www.duckduckgo.com  
|D-chain| -127.0.0.1:9050->-127.0.0.1:9050<-denied  
|D-chain| -127.0.0.1:9050->-4.2.2.2:53->DNS-response| duckduckgo.com is 40.114.177.156  
|D-chain| -127.0.0.1:9050->-127.0.0.1:9050<-denied  
|D-chain| -127.0.0.1:9050->-40.114.177.156:443-><<-OK  
<<-OK  
|DNS-response| www.duckduckgo.com is 40.114.177.156  
|D-chain| -127.0.0.1:9050->-40.114.177.156:80-><<-OK  
|D-chain| -127.0.0.1:9050->-40.114.177.156:80-><<-OK  
|DNS-request| improving.duckduckgo.com  
|D-chain| -127.0.0.1:9050->-127.0.0.1:9050<-denied  
|D-chain| -127.0.0.1:9050->-4.2.2.2:53-><<-OK  
|DNS-response| improving.duckduckgo.com is 40.114.177.156  
|D-chain| -127.0.0.1:9050->-40.114.177.156:443-><<-OK  
|D-chain| -127.0.0.1:9050->-40.114.177.156:443-><<-OK  
|D-chain| -127.0.0.1:9050->-40.114.177.156:443-><<-OK
```


Com o proxychains em execução, vamos ver qual endereço IP obtemos no site:

<https://www.dnsleaktest.com/>



Ao clicar no botão de Standart test também podemos ver que a localização do nosso proxy está baseado na Alemanha.



The screenshot shows a web browser window with the URL <https://dnsleaktest.com/results.html>. The page title is "DNS leak test - Mozilla Firefox". The test results are displayed as follows:

Test complete

Query round 1 Progress... Servers found 5

Sponsored by **IVPN**
Ultimate IP leak Protection

IP	Hostname	ISP	Country
192.221.146.128	pubntp2.Frankfurt1.Level3.net.	Level 3 Communications	Frankfurt am Main, Germany
192.221.146.129	None	Level 3 Communications	Frankfurt am Main, Germany
192.221.146.130	None	Level 3 Communications	Frankfurt am Main, Germany
8.0.16.135	None	Level 3 Communications	Frankfurt am Main, Germany
8.0.18.133	None	Level 3 Communications	Frankfurt am Main, Germany

Para obter resultados diferentes (localização), basta fechar o navegador, o terminal e reiniciar o TOR e ativar novamente o proxychains.

Conclusão

Os servidores proxies são, de certa forma, populares. Porém, podem ganhar ainda mais popularidade com a chegada da Neutralidade da Internet e Censura por aí, pois oferece uma solução alternativa para evitar estas supostas restrições. Mas é bom tomar cuidado pois os dados que trafegam através de um servidor proxy não são criptografados, sendo assim possíveis alvos fáceis de se interceptar. Talvez o mais recomendado seja usar uma VPN mesmo, pode ser um serviço mais caro mas é mais seguro.