

Mestrado em Engenharia Informática
Universidade do Minho

Engenharia de Segurança

Aula 04 TP - 06/03/2020

João Miranda - PG41845
Sandro Cruz - PG41906

16 de Março de 2020

Conteúdo

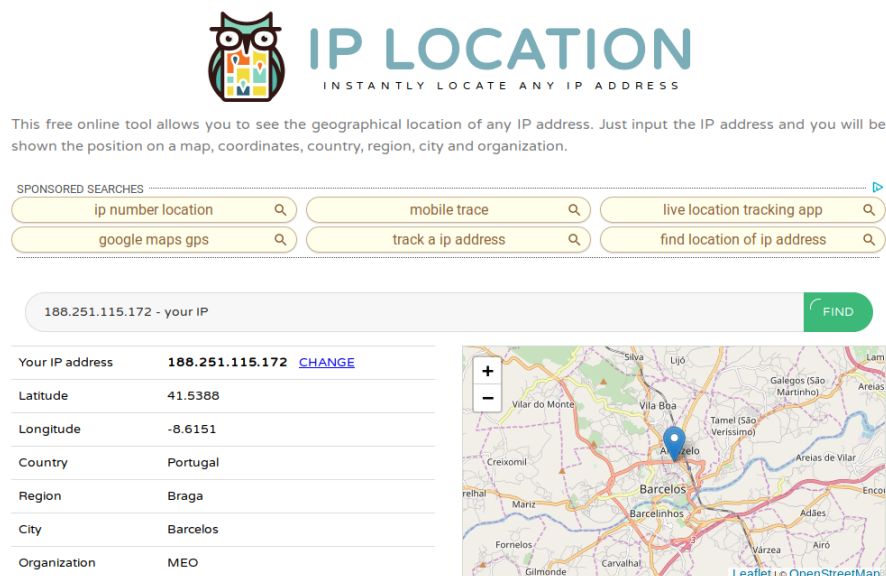
1	TOR (The Onion Router)	2
1.1	Experiência 1.1	2
1.1.1	Abra o browser e vá a https://iplocation.com/	2
1.1.2	Na linha de comando execute <code>sudo anonsurf start</code>	3
1.1.3	Faça reload (shift-reload) da página web onde se encontrava	3
1.1.4	Na linha de comando execute <code>sudo anonsurf change</code>	4
1.1.5	Faça reload (shift-reload) da página web onde se encontrava	4
1.1.6	Na linha de comando execute <code>sudo anonsurf stop</code>	4
1.1.7	Faça reload (shift-reload) da página web onde se encontrava	5
1.2	Pergunta P1.1	5
1.3	Experiência 1.2	6
1.3.1	No browser TOR acesse a página https://blog.torproject.org/italian-anti-corruption-authority-anac-adopts-onion-services . Clique no lado esquerdo da barra de URL ((i)) e verifique qual é o circuito para esse site.	6
1.3.2	Abra outro tab/pestaña no browser TOR e acesse a página https://www.expressvpn.com/blog/best-onion-sites-on-dark-web/ . Clique no lado esquerdo da barra de URL e verifique qual é o circuito para esse site.	7
1.4	Pergunta P1.2	8
1.4.1	Clique no lado esquerdo da barra de URL ((i)) e verifique qual é o circuito para esse site.	8
1.4.2	Porque existem 6 "saltos" até ao site Onion, sendo que 3 deles são "relay"? Utilize características do protocolo TOR para justificar.	8

Capítulo 1

TOR (The Onion Router)

1.1 Experiência 1.1

1.1.1 Abra o browser e vá a <https://iplocation.com/>



The screenshot shows the IP LOCATION website interface. At the top, there is a logo of an owl with glasses and the text "IP LOCATION" with the tagline "INSTANTLY LOCATE ANY IP ADDRESS". Below this, a description states: "This free online tool allows you to see the geographical location of any IP address. Just input the IP address and you will be shown the position on a map, coordinates, country, region, city and organization." There is a section for "SPONSORED SEARCHES" with several buttons: "ip number location", "mobile trace", "live location tracking app", "google maps gps", "track a ip address", and "find location of ip address". The main search bar contains the IP address "188.251.115.172 - your IP" and a "FIND" button. Below the search bar, there is a table with the following information:

Your IP address	188.251.115.172 CHANGE
Latitude	41.5388
Longitude	-8.6151
Country	Portugal
Region	Braga
City	Barcelos
Organization	MEO

To the right of the table is a map showing the location of Barcelos, Portugal, with a blue pin. The map includes labels for various locations like Vila Boa, Tamei (São Veríssimo), and Barcelos. The map is powered by Leaflet and OpenStreetMap.

Figura 1.1: Resultados do acesso a <https://iplocation.com/>

1.1.2 Na linha de comando execute `sudo anonsurf start`

```
user@CSI:~/Tools/kali-anonsurf$ sudo anonsurf start
* killing dangerous applications
* cleaning some dangerous cache elements
[ i ] Stopping IPv6 services:

[ i ] Starting anonymous mode:

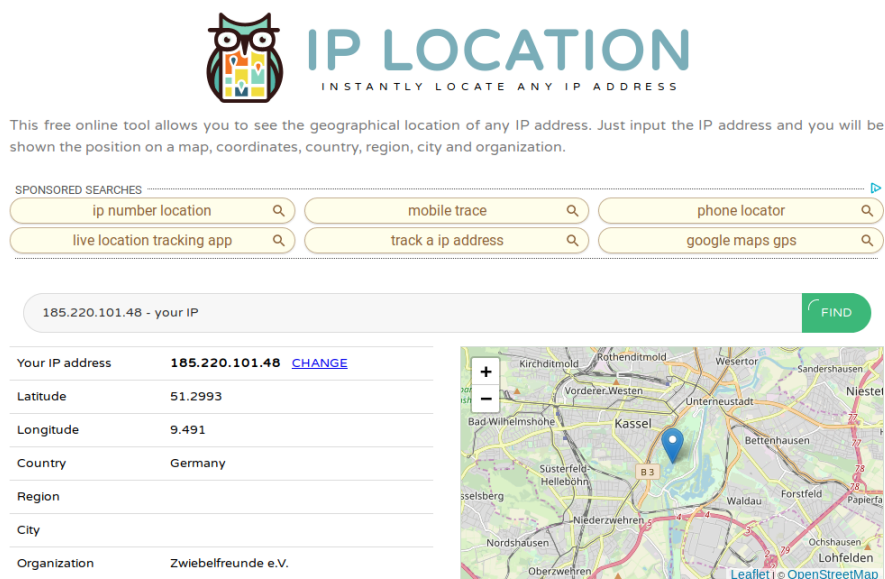
* Saved iptables rules

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

[ i ] You are under AnonSurf tunnel
```

Figura 1.2: Output da execução do comando `sudo anonsurf start`

1.1.3 Faça reload (shift-reload) da página web onde se encontrava



The screenshot shows the IP LOCATION website interface. At the top, there's a logo of an owl and the text "IP LOCATION INSTANTLY LOCATE ANY IP ADDRESS". Below this is a description: "This free online tool allows you to see the geographical location of any IP address. Just input the IP address and you will be shown the position on a map, coordinates, country, region, city and organization." There are several search buttons: "ip number location", "mobile trace", "phone locator", "live location tracking app", "track a ip address", and "google maps gps". The main search bar contains the IP address "185.220.101.48 - your IP" and a green "FIND" button. Below the search bar, there's a table with the following data:

Your IP address	185.220.101.48	CHANGE
Latitude	51.2993	
Longitude	9.491	
Country	Germany	
Region		
City		
Organization	Zwiebelfreunde e.V.	

To the right of the table is a map showing the location of the IP address in Kassel, Germany. The map includes labels for various districts and landmarks.

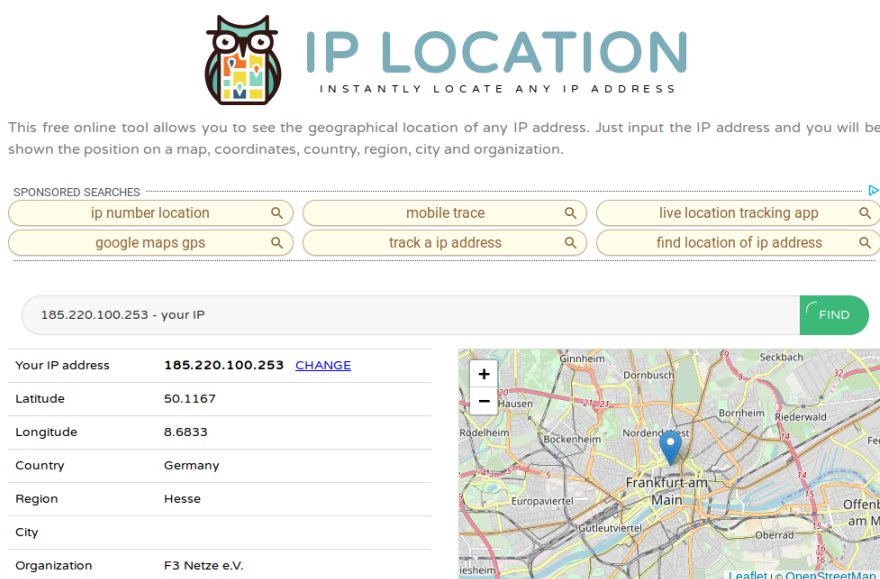
Figura 1.3: Resultados do reload de <https://iplocation.com/>

1.1.4 Na linha de comando execute `sudo anonsurf change`

```
user@CSI:~/Tools/kali-anonsurf$ sudo anonsurf change
* Tor daemon reloaded and forced to change nodes
```

Figura 1.4: Output da execução do comando `sudo anonsurf change`

1.1.5 Faça reload (shift-reload) da página web onde se encontrava



The screenshot shows the IP Location website interface. At the top, there's a logo of an owl and the text "IP LOCATION INSTANTLY LOCATE ANY IP ADDRESS". Below this, a description states: "This free online tool allows you to see the geographical location of any IP address. Just input the IP address and you will be shown the position on a map, coordinates, country, region, city and organization." There's a section for "SPONSORED SEARCHES" with buttons for "ip number location", "mobile trace", "live location tracking app", "google maps gps", "track a ip address", and "find location of ip address". The main input field contains "185.220.100.253 - your IP" and a "FIND" button. Below the input field, a table displays the following information:

Your IP address	185.220.100.253	CHANGE
Latitude	50.1167	
Longitude	8.6833	
Country	Germany	
Region	Hesse	
City		
Organization	F3 Netze e.V.	

To the right of the table is a map showing the location of Frankfurt am Main, Germany, with a blue pin indicating the specific location. The map is powered by Leaflet and OpenStreetMap.

Figura 1.5: Resultados do reload de <https://iplocation.com/>

1.1.6 Na linha de comando execute `sudo anonsurf stop`

```
user@CSI:~/Tools/kali-anonsurf$ sudo anonsurf stop
* killing dangerous applications
* cleaning some dangerous cache elements
[ i ] Stopping anonymous mode:

* Deleted all iptables rules

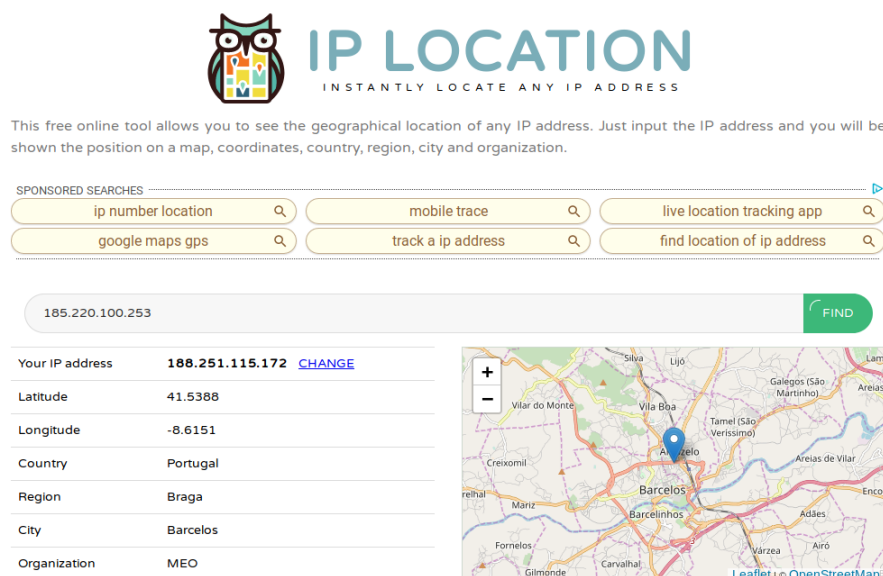
* Iptables rules restored

[ i ] Reenabling IPv6 services:

* Anonymous mode stopped
```

Figura 1.6: Output da execução do comando `sudo anonsurf stop`

1.1.7 Faça reload (shift-reload) da página web onde se encontrava



The screenshot shows the IP Location website interface. At the top, there is a logo of an owl with the text "IP LOCATION" and the tagline "INSTANTLY LOCATE ANY IP ADDRESS". Below this, a description states: "This free online tool allows you to see the geographical location of any IP address. Just input the IP address and you will be shown the position on a map, coordinates, country, region, city and organization."

Below the description, there is a section for "SPONSORED SEARCHES" with several search buttons: "ip number location", "mobile trace", "live location tracking app", "google maps gps", "track a ip address", and "find location of ip address".

The main search area shows the IP address "185.220.100.253" entered in a search bar, with a "FIND" button to the right. Below the search bar, there is a table of results:

Your IP address	185.220.100.253
Latitude	41.5388
Longitude	-8.6151
Country	Portugal
Region	Braga
City	Barcelos
Organization	MEO

To the right of the table, there is a map showing the location of Barcelos, Portugal, with a blue dot indicating the IP address location. The map includes labels for various locations like Vila Boa, Tamei (São Veríssimo), and Barcelos.

Figura 1.7: Resultados do reload de <https://iplocation.com/>

1.2 Pergunta P1.1

Não é impossível garantir que vai estar conectado nos EUA, porque quando o utilizador se conecta a uma *onion proxy* lhe "atribuído" o *ip* de um dos *onion routers* existentes na rede de forma a garantir a anonimato. Ou seja como a *onion proxy* escolhe um *onion router* a acaso não é possível garantir que o utilizador estará conectado nos EUA, mas quando o utilizador decidir aceder a um website localizado nos EUA irá ser procurada uma rota possível entre os *onion routers* de forma ao *onion router* final ser localizado nos EUA, assim fazendo com que o utilizador pareça estar "conectado" nos EUA, garantido assim que o utilizador pode aceder ao website.

1.3 Experiência 1.2

- 1.3.1 No browser TOR acesse a página <https://blog.torproject.org/italian-anti-corruption-authority-anac-adopts-onion-services>. Clique no lado esquerdo da barra de URL ((i)) e verifique qual é o circuito para esse site.

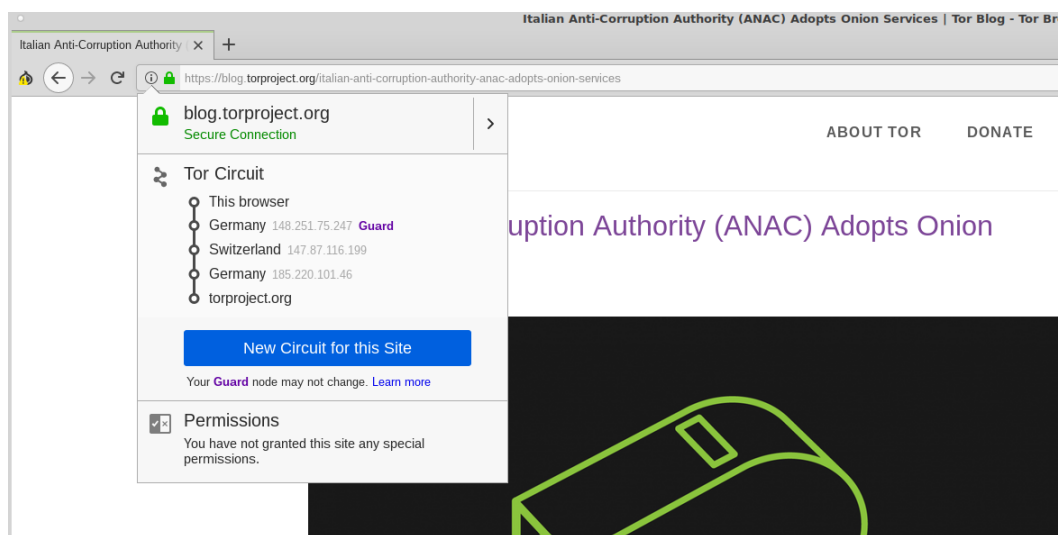


Figura 1.8: Circuito para o website <https://blog.torproject.org/italian-anti-corruption-authority-anac-adopts-onion-services>

1.3.2 Abra outro tab/pesta na no browser TOR e acheda à página <https://www.expressvpn.com/blog/best-onion-sites-on-dark-web/>. Clique no lado esquerdo da barra de URL e verifique qual é o circuito para esse site.

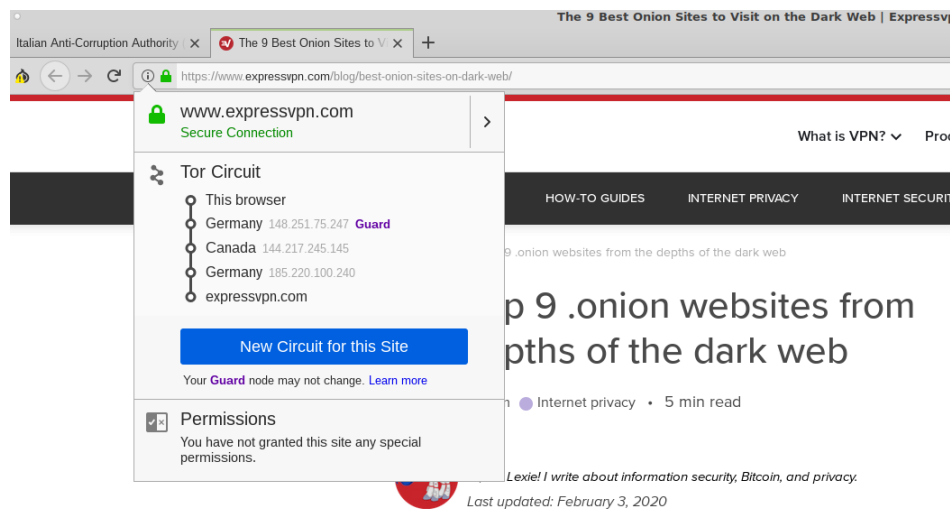


Figura 1.9: Circuito para o website <https://www.expressvpn.com/blog/best-onion-sites-on-dark-web/>

O primeiro OR (Onion Router) como podemos verificar é o mesmo, isto acontece dado que o primeiro OR atribuído será um "entry guard" que é um OR confiável e seguro. Esse primeiro OR será sempre o mesmo durante dois a três meses por motivos de segurança contra ataques, como por exemplo um OR que na verdade monitoriza que se acede a ele o que leva a quebra do anonimato. Os outros dois OR's são escolhidos de forma *random* dado que não existe a necessidade de ter mais um OR "guard" dado que em princípio o OR "guard" inicial não vai revelar a origem do tráfego.

1.4 Pergunta P1.2

1.4.1 Clique no lado esquerdo da barra de URL ((i)) e verifique qual é o circuito para esse site.

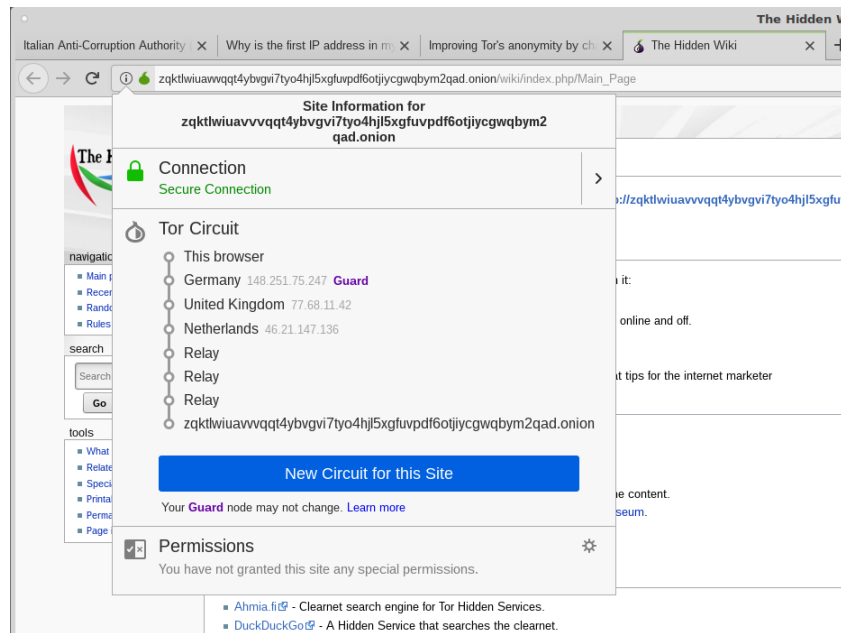


Figura 1.10: Circuito para o website `http://zqktlwiauavvqq4ybvvgvi7tyo4hj5xgfuvpdf6otjiycgwqby2qad.onion/`

1.4.2 Porque existem 6 "saltos" até ao site Onion, sendo que 3 deles são "relay"? Utilize características do protocolo TOR para justificar.

Isto acontece porque o website está anonimado por um "ponto de rendezvous", isto permite que um *service provider* consiga disponibilizar o seu serviço TCP sem revelar o seu IP. Quando um utilizador anonimizado tenta aceder um website também ele anonimizado, ele primeiro escolhe um OR como PR ("ponto de rendezvous") para se conectar ao website, assim o utilizador constrói um circuito até ao PR e fornece-lhe uma *rendezvous cookie* para depois reconhecer o website. A seguir é criado um *stream* anónimo até um dos pontos de introdução e o utilizador fornece uma mensagem encriptada com a chave pública do website, essa mensagem contém a *rendezvous cookie*, informação sobre o RP e o início da troca de chaves Diffie-Hellman. O ponto de introdução depois reencaminha essa mensagem para o website.

O website em questão para comunicar com o utilizador, cria um circuito até ao

RP e envia a *rendezvous cookie*, a segunda parte das chaves Diffie-Hellman e a chave da sessão do utilizador. O RP depois conecta o caminho do utilizador e o do website de forma a ambos poderem comunicar um com o outro, criando assim um caminho com 6 "saltos", 3 OR do lado do utilizador e outros 3 do lado do website. O RP não reconhece nem o utilizador nem o website, assim o website não conhece os OR's do utilizador e o utilizador não conhece os OR's do website.

Estabelecida a ligação entre eles o utilizador envia um *relay begin* através do circuito o OP do website a receber o *relay* fornece o serviço em questão.