Tor Rendezvous Specification

Configurando serviços ocultos com o TOR

Apresentado por:

Noilson Caio T. de Araújo

Objetivos

- *Entender* o roteamento cebola (Tor);
- *Exemplificar* a ocultação de serviços na rede Tor.

Privacidade em redes públicas

- Foram desenhadas para serem “claras”;
- Informações de roteamento são públicas;
- Encriptação não esconde identidades.

Anonimato

- Privacidade;
- Comunicações secretas em uma rede pública;
- Publicações resistentes a censura...

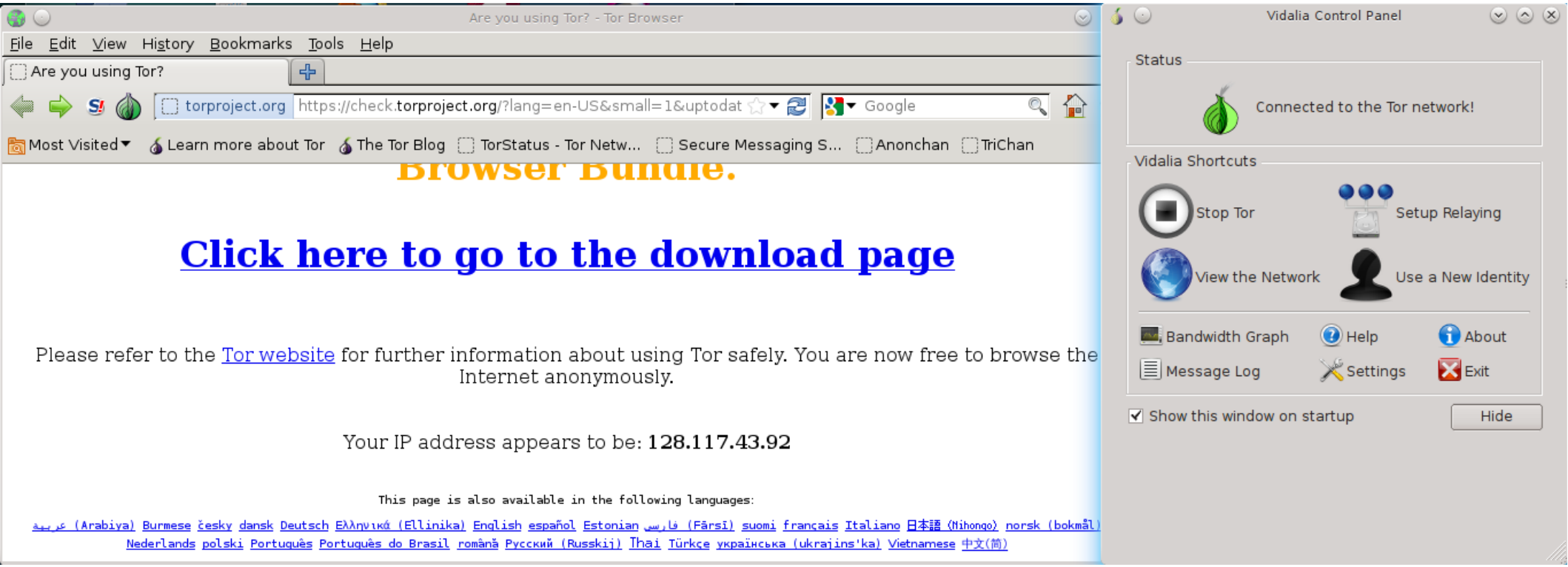
Redes anomimas

- Garlic Routing;
- Anonymizer;
- Java Anon Proxy [JAP ou JonDonym];
- FreeNet Project;
- Onion Routing.

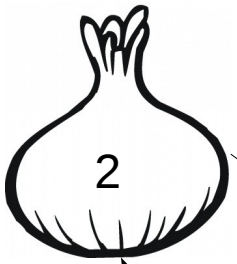
Onion Routing

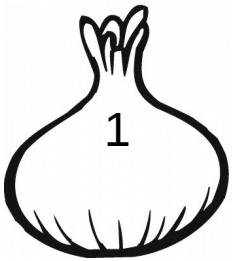
- Usa um proxy;
- Um roteador conhece apenas seu antecessor e sucessor.
- Roteia dados aleatoriamente
- Exclusivamente TCP
  - DDOS
    - 1 / 1 byte

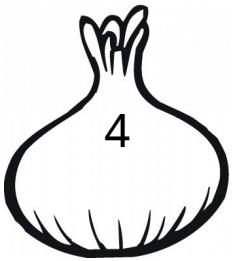
Cliente + Browser

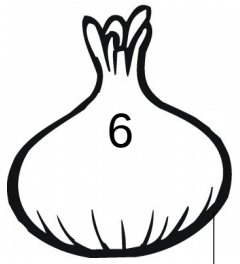


Descrição formal

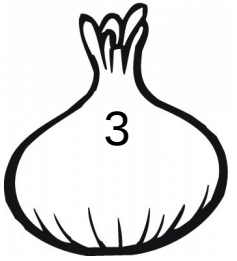


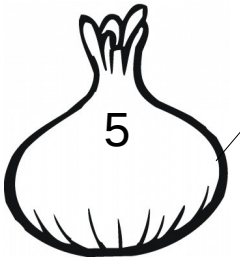




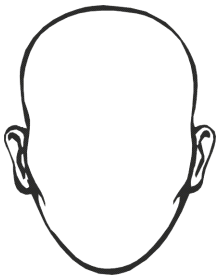


¿¿¿

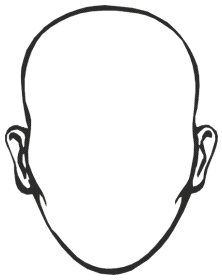




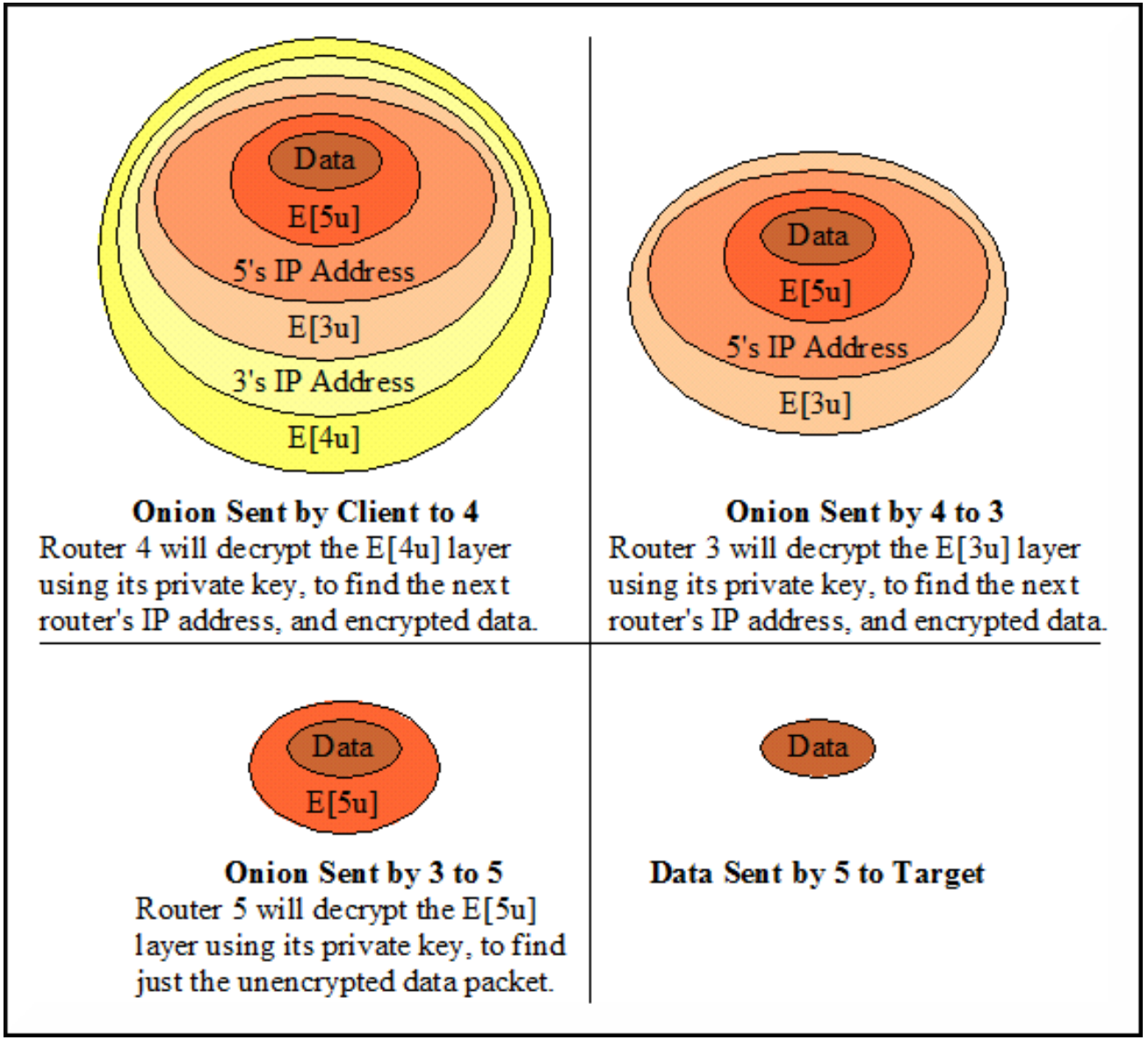
Zn*
Ex: 2,5,6

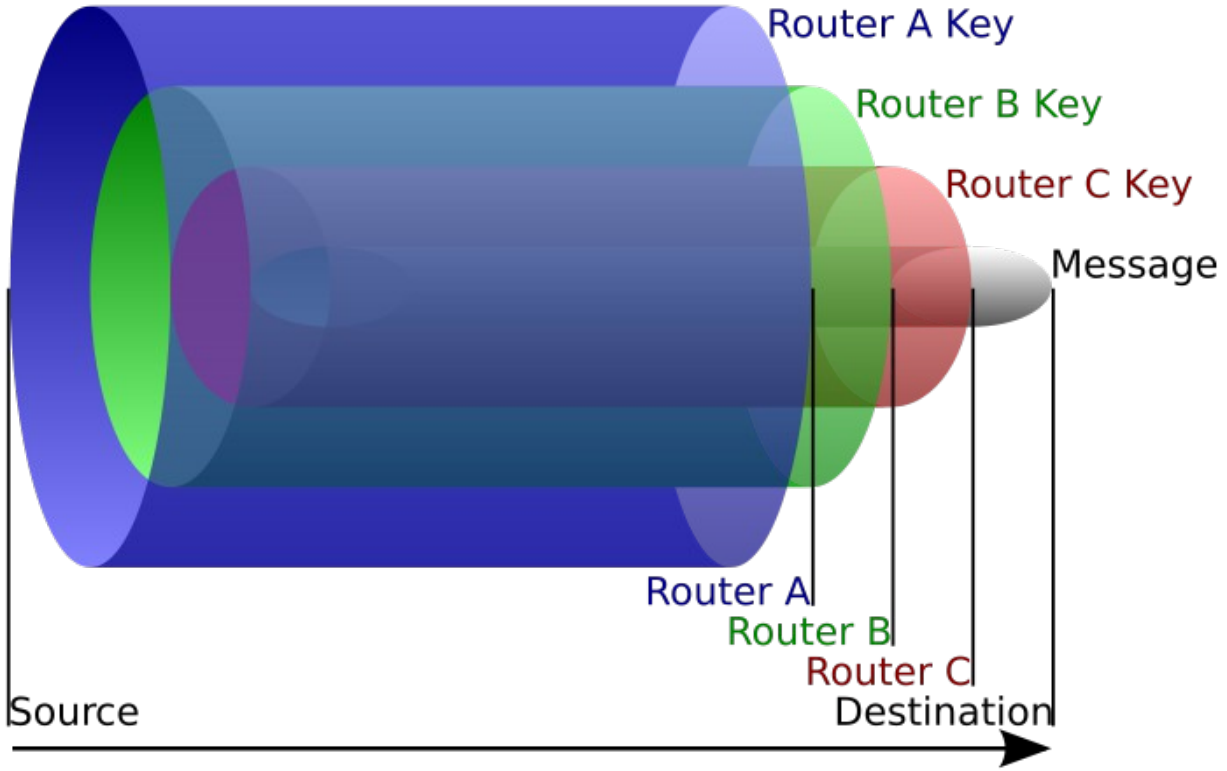


D[C.PU] (E[C.PR] (data))= dados
D[C.PR] (E[C.PU] (data))= dados



Descrição formal




Router A Key
Router B Key
Router C Key
Message
Router A
Router B
Router C
Source
Destination

Serviços ocultos com o TOR

Questionamento:

- Se o Tor é uma rede esclusivamente TCP, o que acontece quando eu preciso usar um serviço UDP (Exemplo: resolução de nomes DNS) ?

Nomes para redes Tor

Exemplo: zrrbldvzlvopglri.onion

Versão codificada: Base32 $\longrightarrow$ A-Z and 0-9

Quando você cria um serviço oculto, você gera um par de chaves.

Rendezvous points – Ponto de encontro

Provê serviço de localização oculta para a rede TOR. Possibilitando um determinado usuário oferecer um serviço através desta rede.

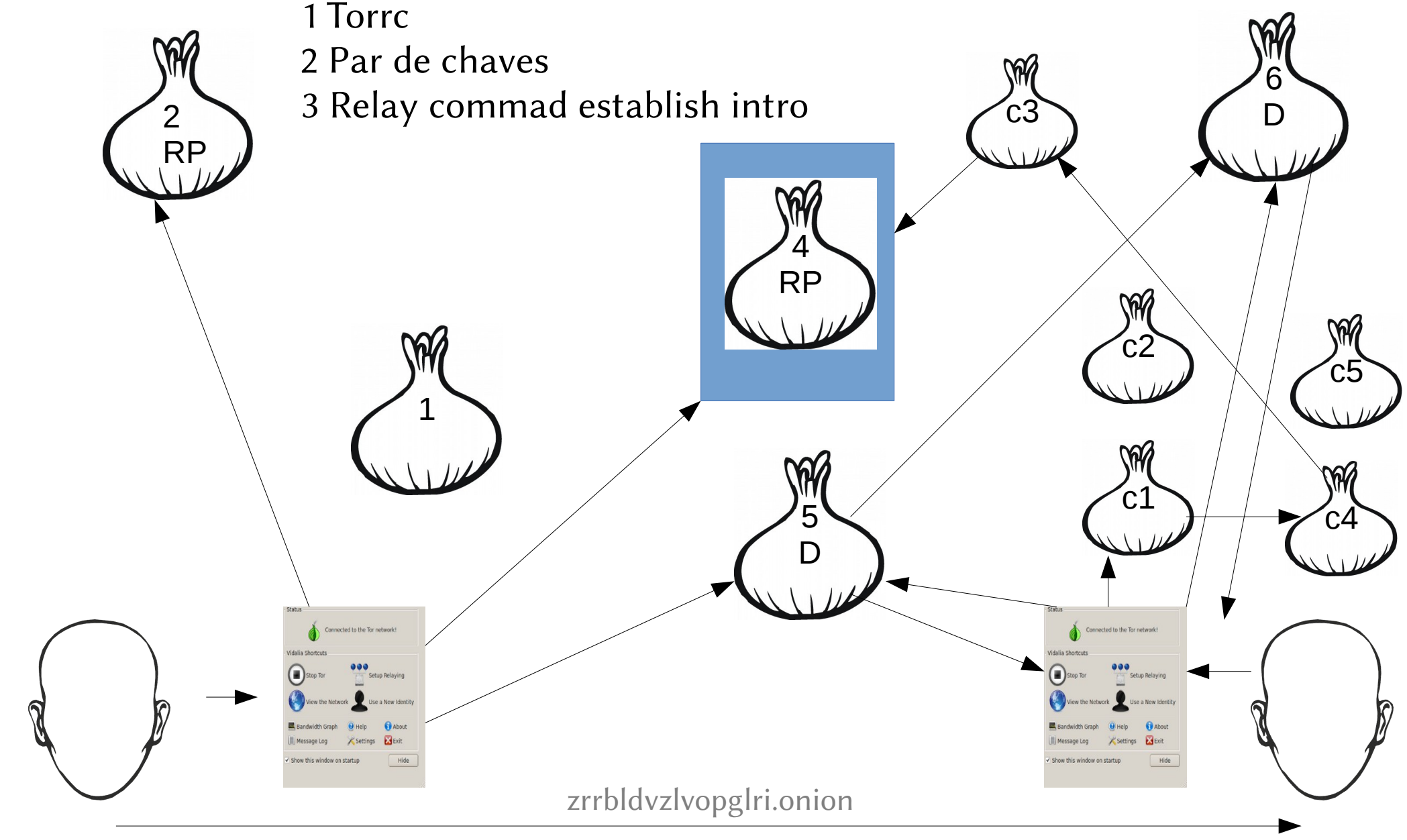
Cada roteador TOR que tem a porta do serviço de diretórios aberta, pode decidir se quer armazenar e servir descritores.

Flag → hidden-service-dir → Estou participando

Flag → HSDir → Autoridade → 24 horas → OK

Descrição Formal

1 Torrc
2 Par de chaves
3 Relay commad establish intro



Na prática ...

torrc

```
#
#
#
HiddenServiceDir ./tmp/www
HiddenServicePort 80 127.0.0.1:80
#
#
#
```

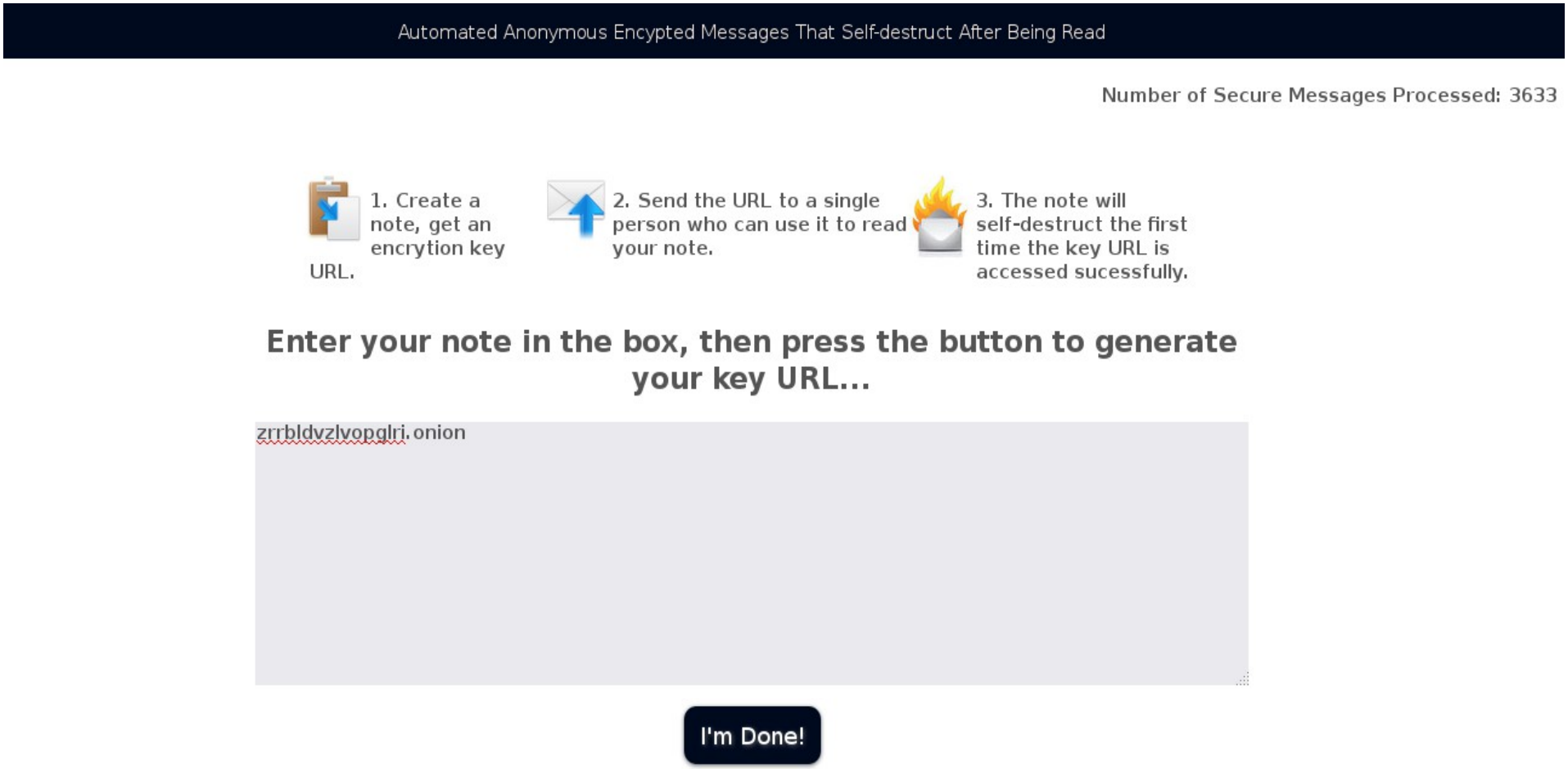
Hostname


bash-4.2# ls
hostname private_key
bash-4.2# cat hostname
zrrbldvzlvopglri.onion
bash-4.2#

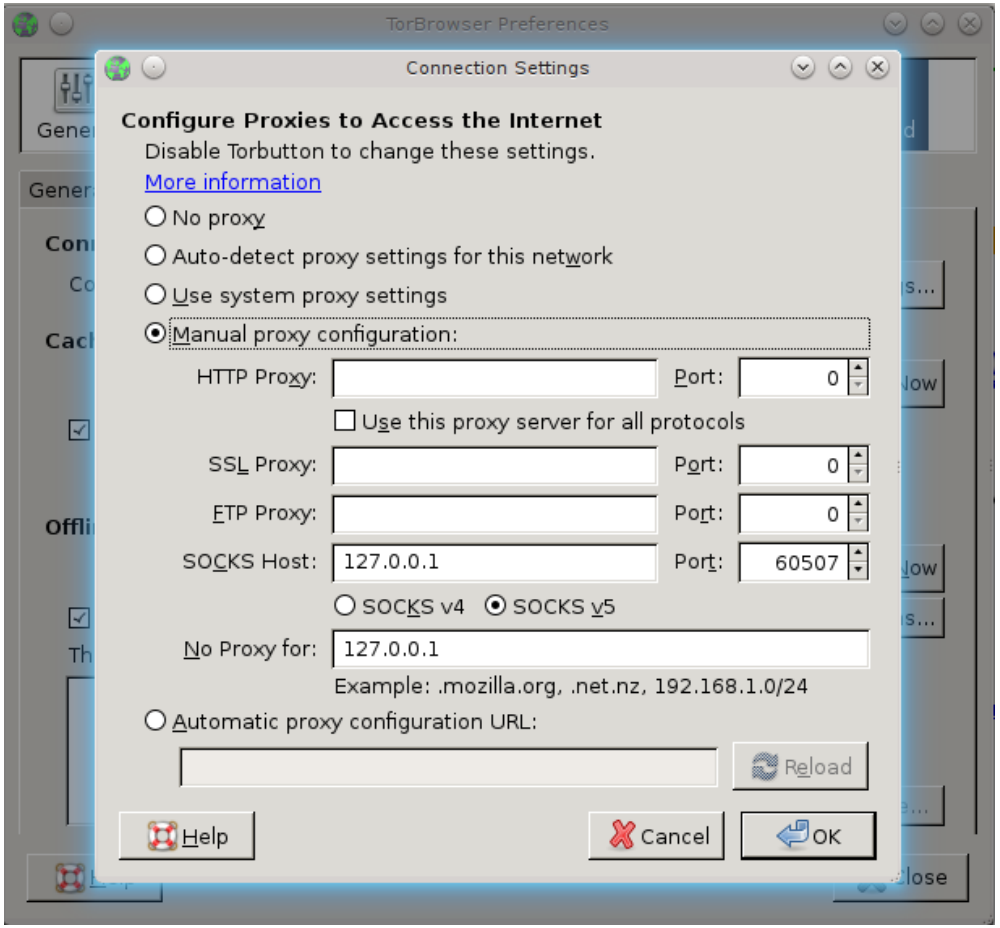
Virtual host

```
#
#  Virtual Host
#
<VirtualHost 127.0.0.1:80>
ServerName  zrrbldvzlvopglri.onion
DocumentRoot /var/www/htdocs
<Directory />
    AllowOverride none
    Require all granted
</Directory>
</VirtualHost>
#
#
#
```

Publicando endereço
Secure Messaging System for TOR



Acessando serviços ocultos



Ssh cliente

HiddenServiceDir ./tmp/ssh
HiddenServicePort 22 127.0.0.1:80

→ Connect.c ←

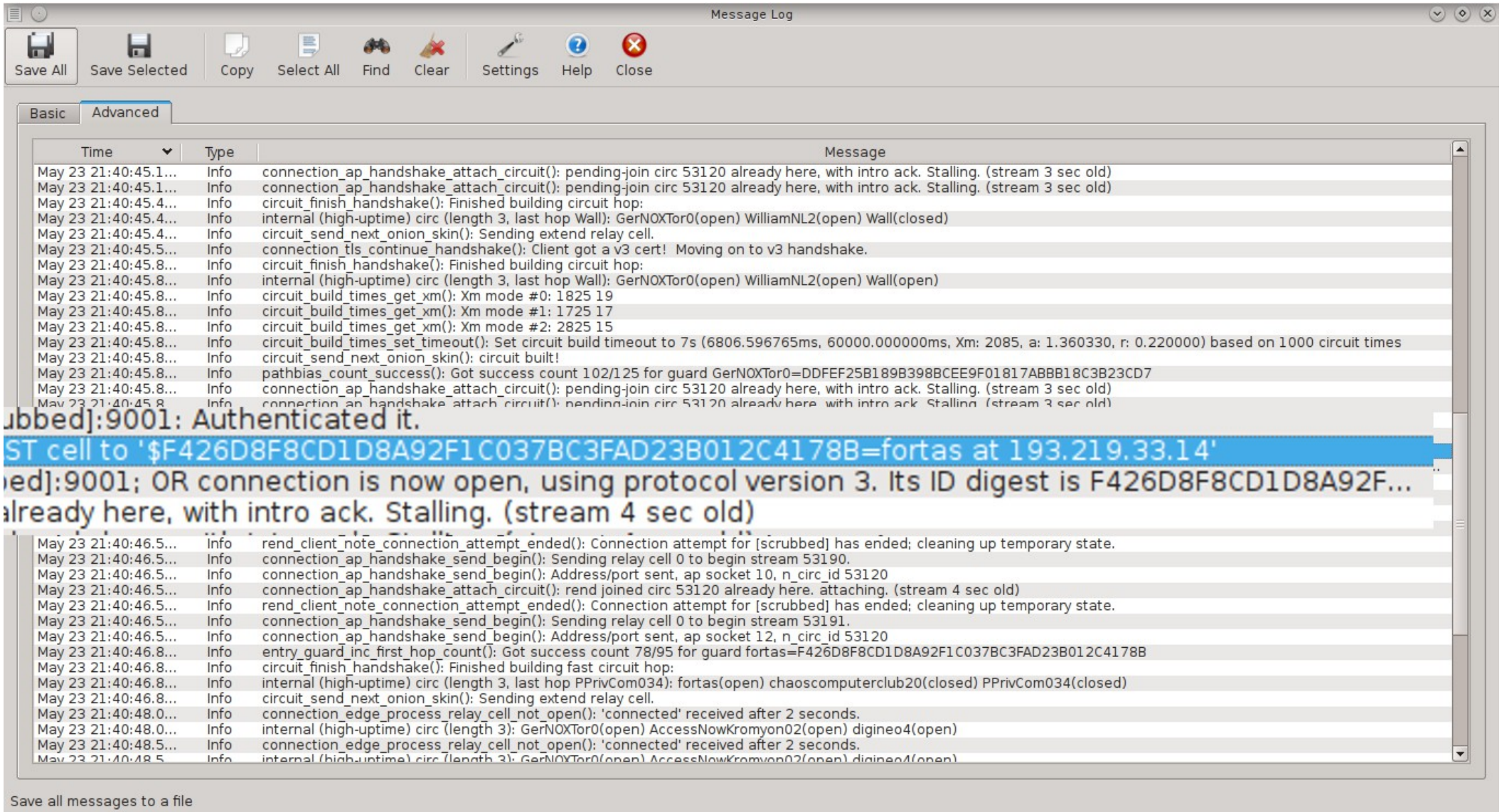
connect.c -- Make socket connection using SOCKS4/5 and HTTP tunne

~/.ssh/config

```
HOST      26qfpx2ahq7trree.onion
ProxyCommand  /tmp/connect -S localhost:49864 %h %p
```

ncaio@notebook:~$ ssh 26qfpx2ahq7trree.onion

O lado fraco


Message Log
Save All
Save Selected
Copy
Select All
Find
Clear
Settings
Help
Close
Basic
Advanced
Time
Type
Message
May 23 21:40:45.1... Info connection_ap_handshake_attach_circuit(): pending-join circ 53120 already here, with intro ack. Stalling. (stream 3 sec old)
May 23 21:40:45.1... Info connection_ap_handshake_attach_circuit(): pending-join circ 53120 already here, with intro ack. Stalling. (stream 3 sec old)
May 23 21:40:45.4... Info circuit_finish_handshake(): Finished building circuit hop:
May 23 21:40:45.4... Info internal (high-uptime) circ (length 3, last hop Wall): GerN0XTor0(open) WilliamNL2(open) Wall(closed)
May 23 21:40:45.4... Info circuit_send_next_onion_skin(): Sending extend relay cell.
May 23 21:40:45.5... Info connection_tls_continue_handshake(): Client got a v3 cert! Moving on to v3 handshake.
May 23 21:40:45.8... Info circuit_finish_handshake(): Finished building circuit hop:
May 23 21:40:45.8... Info internal (high-uptime) circ (length 3, last hop Wall): GerN0XTor0(open) WilliamNL2(open) Wall(open)
May 23 21:40:45.8... Info circuit_build_times_get_xm(): Xm mode #0: 1825 19
May 23 21:40:45.8... Info circuit_build_times_get_xm(): Xm mode #1: 1725 17
May 23 21:40:45.8... Info circuit_build_times_get_xm(): Xm mode #2: 2825 15
May 23 21:40:45.8... Info circuit_build_times_set_timeout(): Set circuit build timeout to 7s (6806.596765ms, 60000.000000ms, Xm: 2085, a: 1.360330, r: 0.220000) based on 1000 circuit times
May 23 21:40:45.8... Info circuit_send_next_onion_skin(): circuit built!
May 23 21:40:45.8... Info pathbias_count_success(): Got success count 102/125 for guard GerN0XTor0=DDFEF25B189B398BCEE9F01817ABBB18C3B23CD7
May 23 21:40:45.8... Info connection_ap_handshake_attach_circuit(): pending-join circ 53120 already here, with intro ack. Stalling. (stream 3 sec old)
ubbed]:9001: Authenticated it.
ST cell to '$F426D8F8CD1D8A92F1C037BC3FAD23B012C4178B=fortas at 193.219.33.14'
ed]:9001; OR connection is now open, using protocol version 3. Its ID digest is F426D8F8CD1D8A92F...
already here, with intro ack. Stalling. (stream 4 sec old)
May 23 21:40:46.5... Info rend_client_note_connection_attempt_ended(): Connection attempt for [scrubbed] has ended; cleaning up temporary state.
May 23 21:40:46.5... Info connection_ap_handshake_send_begin(): Sending relay cell 0 to begin stream 53190.
May 23 21:40:46.5... Info connection_ap_handshake_send_begin(): Address/port sent, ap socket 10, n_circ_id 53120
May 23 21:40:46.5... Info connection_ap_handshake_attach_circuit(): rend joined circ 53120 already here. attaching. (stream 4 sec old)
May 23 21:40:46.5... Info rend_client_note_connection_attempt_ended(): Connection attempt for [scrubbed] has ended; cleaning up temporary state.
May 23 21:40:46.5... Info connection_ap_handshake_send_begin(): Sending relay cell 0 to begin stream 53191.
May 23 21:40:46.5... Info connection_ap_handshake_send_begin(): Address/port sent, ap socket 12, n_circ_id 53120
May 23 21:40:46.8... Info entry_guard_inc_first_hop_count(): Got success count 78/95 for guard fortas=F426D8F8CD1D8A92F1C037BC3FAD23B012C4178B
May 23 21:40:46.8... Info circuit_finish_handshake(): Finished building fast circuit hop:
May 23 21:40:46.8... Info internal (high-uptime) circ (length 3, last hop PPrivCom034): fortas(open) chaoscomputerclub20(closed) PPrivCom034(closed)
May 23 21:40:46.8... Info circuit_send_next_onion_skin(): Sending extend relay cell.
May 23 21:40:48.0... Info connection_edge_process_relay_cell_not_open(): 'connected' received after 2 seconds.
May 23 21:40:48.0... Info internal (high-uptime) circ (length 3): GerN0XTor0(open) AccessNowKromyon02(open) digineo4(open)
May 23 21:40:48.5... Info connection_edge_process_relay_cell_not_open(): 'connected' received after 2 seconds.
Save all messages to a file

https://torstatus.info/

Router Information

Router Name:	fortas
Fingerprint:	F426 D8F8 CD1D 8A92 F1C0 37BC 3FAD 23B0 12C4 178B
Contact:	None Given
IP Address:	193.219.33.14
Hostname:	fortas.if.ktu.lt
Onion Router Port:	9001
Directory Server Port:	9030
Country Code:	LT
Platform / Version:	Tor 0.2.3.25 on Linux
Last Descriptor Published (GMT):	2013-05-23 14:53:19
Current Uptime:	84 Day(s), 9 Hour(s), 6 Minute(s), 8 Second(s)
Bandwidth (Max/Burst/Observed - In Bps):	6291456 / 10485760 / 67557 (In KBps: 6144 / 10240 / 65.97)
Family:	No Info Given

FIM

caiogore@gmail.com
http://ncaio.wordpress.com
http://br.linkedin.com/in/ncaio