una distro per dissidenti

Sonia Zorba

Tails

- Nata nel 2009
- Basata su Debian
- Modalità live USB
- (Idealmente) è un'implementazione di una specifica: *Privacy Enhancing Live Distribution (PELD)*
- Tutto il traffico transita attraverso Tor
- Hardening applicato a vari livelli (isolamento processi, flag del kernel, firewall, ...)

Sponsor famosi

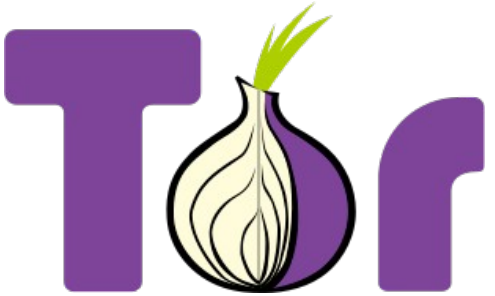
- 2015: DuckDuckGo: 25.000 $, Edward Snowden: 10.000 $
- 2017: Mozilla: 77.000 $
- 2018: DuckDuckGo: 38.000 $
- 2019: Mozilla: 146.000 $
- 2022: ProtonMail: 35.000 $
- 2023: ...

Sponsor famosi

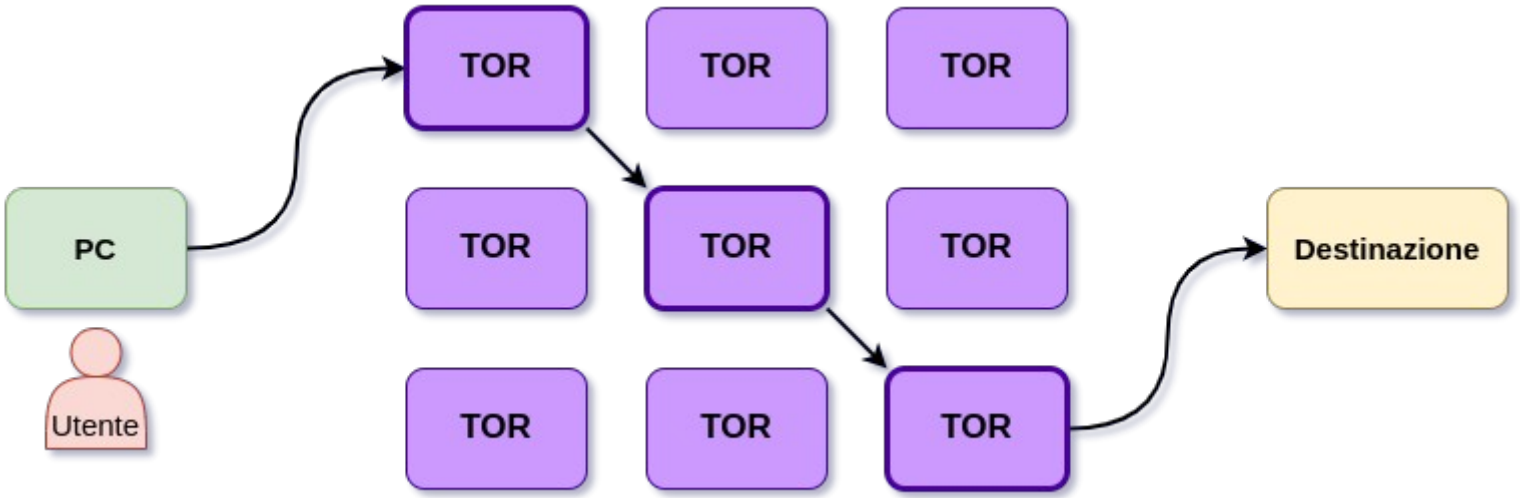
- 2015: DuckDuckGo: 25.000 $, Edward Snowden: 10.000 $
- 2017: Mozilla: 77.000 $
- 2018: DuckDuckGo: 38.000 $
- 2019: Mozilla: 146.000 $
- 2022: ProtonMail: 35.000 $
- 2023: Dipartimento di Stato USA: 215.000 $

Tor

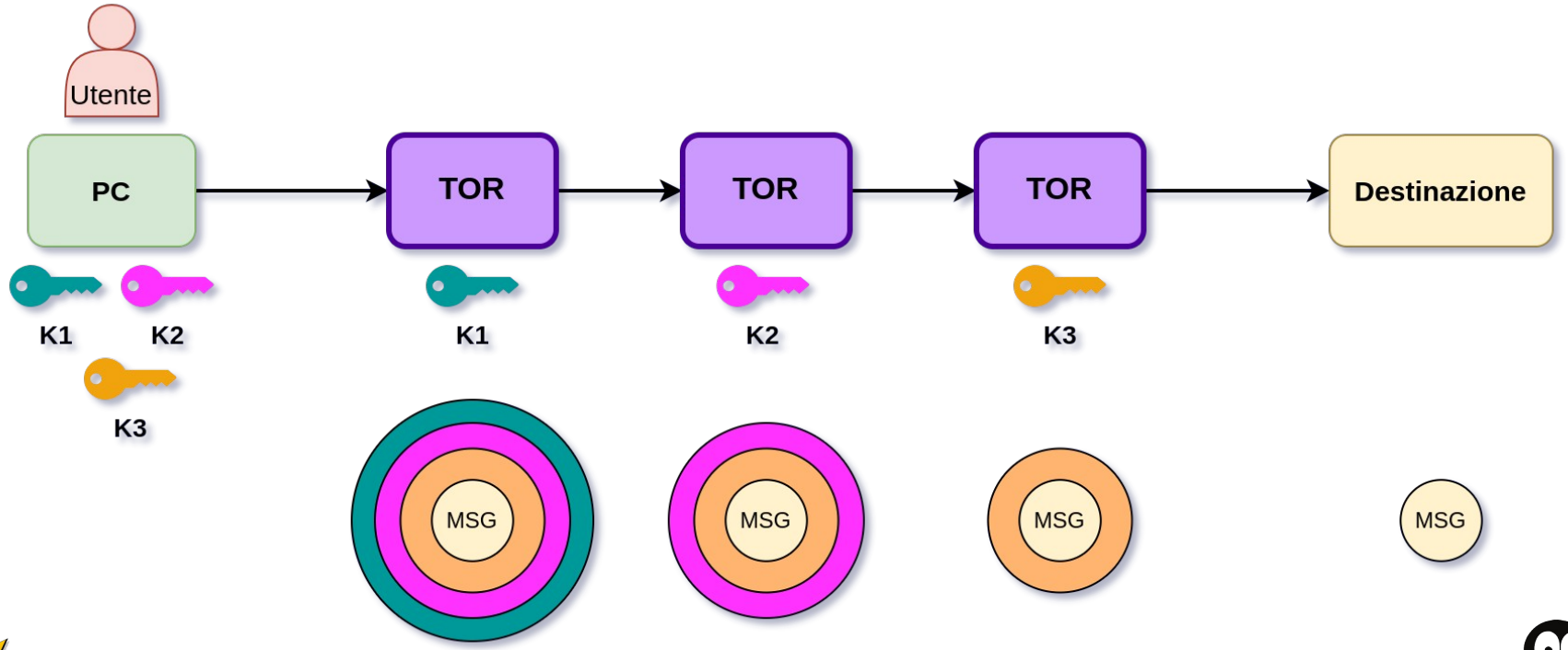
- Software open-source e overlay network
- Nato come progetto militare negli anni 90
- Oggi gestito da non-profit
- Circa 8000 relay, 4 milioni di utenti



Tor (The Onion Router)

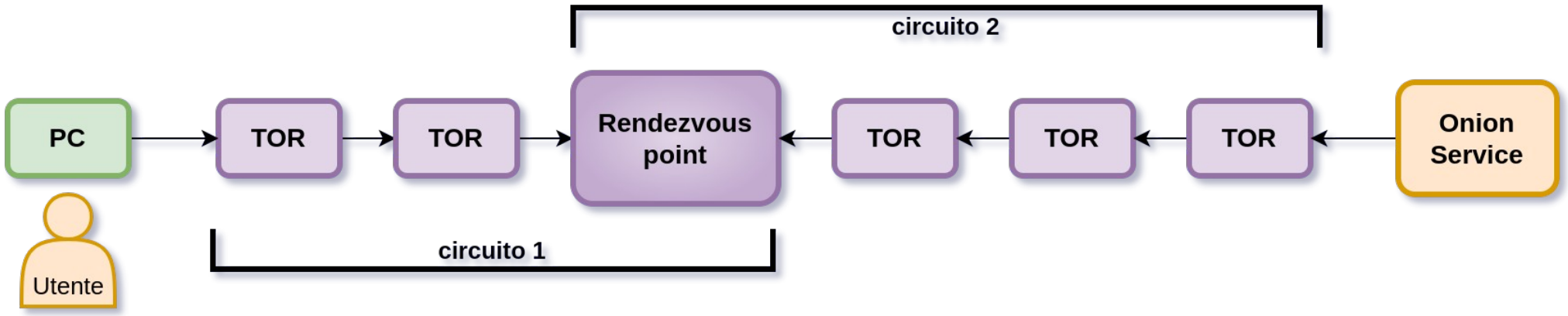


Tor (The Onion Router)



Lug Trieste

Onion Services (Hidden Services)




Oct 13 22:55
Arresto
Avvia Tails
Benvenuto in Tails!
Lingua & Regione
Lingua
Italiano - Italia (Italian - Italy)
Disposizione tastiera
Italian
Formati
Italia - Italiano (Italy - Italian)
Persistent Storage
You can save some of your files and configuration in an encrypted Persistent Storage on your Tails USB stick: your documents, browser bookmarks, Wi-Fi passwords, and so on.
Create Persistent Storage
Create and configure a Persistent Storage after starting Tails
Impostazioni aggiuntive
Le impostazioni predefinite vanno bene nella maggior parte dei casi. Per aggiungere un'impostazione personale, premi il pulsante "+" sotto.
+


Oct 13 22:56
Arresto
Avvia Tails
Benvenuto in Tails!
Lingua & R
Annulla
Impostazioni aggiuntive
Password di amministratore
Off (predefinito)
Anonimizzazione indirizzo MAC
On (predefinito)
Modalità offline
Attiva la rete (predefinito)
Browser non sicuro
Enabled (default)
Connessioni di rete
Obsoleto
Persistent
Impostazio
+

Trash

Segnala un errore

Documentazione di Tails

Connessione Tor

Qualsiasi cosa fai in internet usando Tails passa attraverso la rete Tor.

Tor cripta e anonimizza la tua connessione passandola attraverso 3 relay.
I relay di Tor sono server gestiti da diverse organizzazioni e volontari sparsi in tutto il mondo.

- ○ **Connetti a Tor automaticamente**

  Consigliamo di connettersi a Tor automaticamente se sei in una rete Wi-Fi pubblica o se molte persone nella tua nazione usano Tor per aggirare la censura.

- ◉ **Nascondi alla mia rete locale che mi sto connettendo a Tor**

  Potresti volere non farti notare se l'uso di Tor può sembrare sospetto da parte di qualcuno che monitora la tua connessione internet.

Maggiori informazioni su come Tails si connette a Tor

Connetti a Tor

Connessione Tor

Configura un bridge di Tor

I bridge sono relay di Tor segreti. Usa un bridge come primo relay di Tor se l'accesso ad esso viene bloccato da dove ti trovi.

Maggiori informazioni sui bridge di Tor

- ○ Use a default bridge
- ◉ Ask for a Tor bridge by email

  Send an empty email to `bridges@torproject.org` from a Gmail or Riseup email address with your phone and scan the QR code that is attached to the automatic reply.

  Scan QR code
- ○ Enter a bridge that you already know

  Bridge obfs4 ...

To save your bridge, create a Persistent Storage on your Tails USB stick.

Indietro Connetti a Tor

Trash

Segnala un errore

Documentazione di Tails

Tails - Sign in to the netwo ×

file:///usr/share/doc/tails/website/misc/captive_portal_warning.it.html

Tails

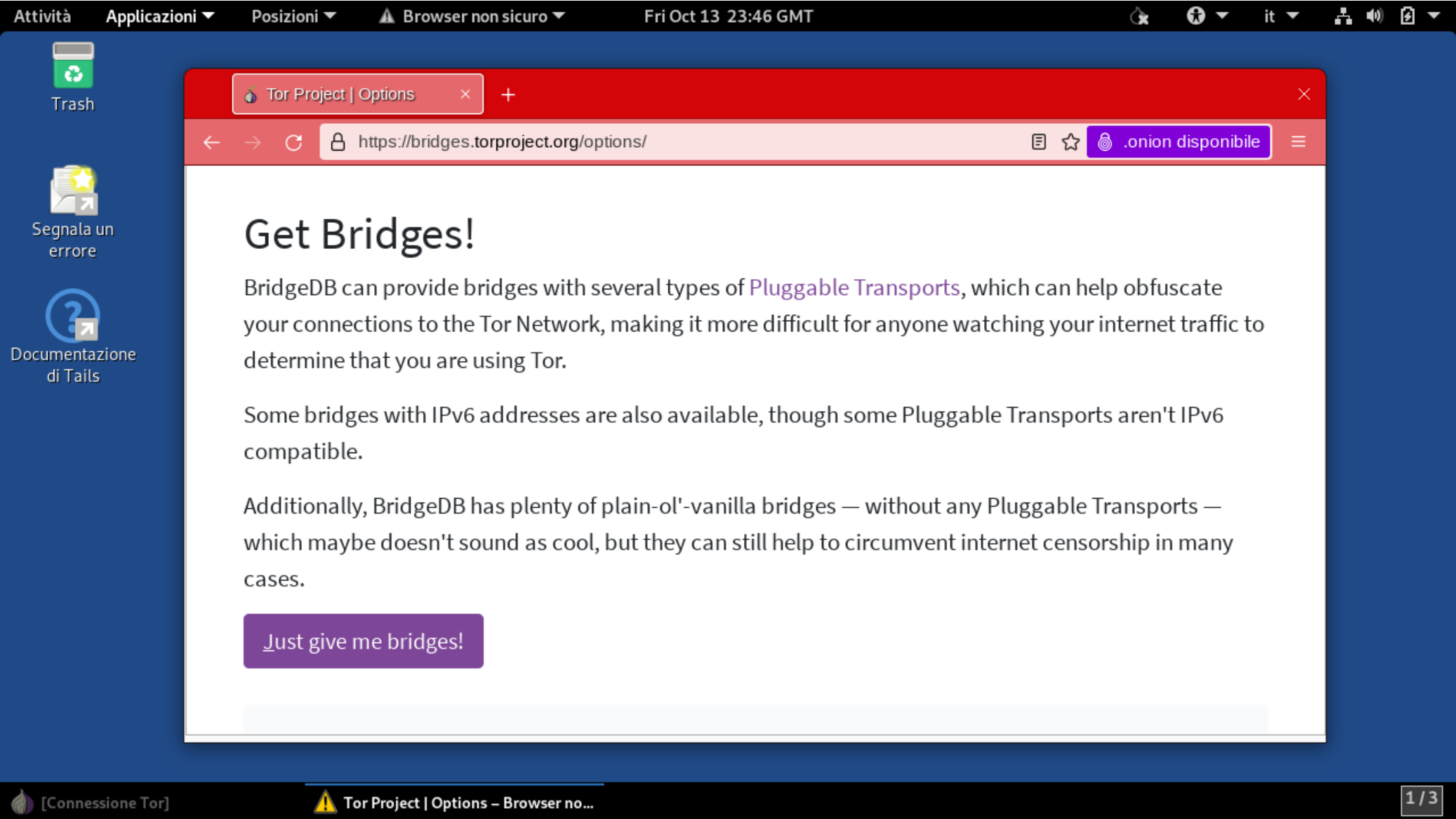
Sign in to the network

Italiano EN DE ES FR PT RU

You might have to sign in to this network before you can connect to the Tor network.

This browser is not anonymous.

Only use this browser to sign in to the network, then close it.


Attività
Applicazioni
Posizioni
Browser non sicuro
Fri Oct 13 23:46 GMT
it
Trash
Segnala un errore
Documentazione di Tails
Tor Project | Options
https://bridges.torproject.org/options/
.onion disponibile
Get Bridges!
BridgeDB can provide bridges with several types of Pluggable Transports, which can help obfuscate your connections to the Tor Network, making it more difficult for anyone watching your internet traffic to determine that you are using Tor.
Some bridges with IPv6 addresses are also available, though some Pluggable Transports aren't IPv6 compatible.
Additionally, BridgeDB has plenty of plain-ol'-vanilla bridges — without any Pluggable Transports — which maybe doesn't sound as cool, but they can still help to circumvent internet censorship in many cases.
Just give me bridges!
[Connessione Tor]
Tor Project | Options – Browser no...
1 / 3

Trash

Segnala un errore

Documentazione di Tails

Tor Project | Bridge Lines

https://bridges.torproject.org/bridges/?transport=obfs4

.onion disponibile

BridgeDB / Get Bridges!

Here are your bridge lines:

```
obfs4 107.210.123.168:10621 336BC480CB125457C0750840F3066AA3A547FCF1 ce
obfs4 172.105.78.187:7917 CB392D04834BC64C390C201BE7F8FC155B972654 cert
```

Copy All

Tras

Segnala error

Document di Tai

Connessione Tor

Configura un bridge di Tor

I bridge sono relay di Tor segreti. Usa un bridge come primo relay di Tor se l'accesso ad esso viene bloccato da dove ti trovi.

Maggiori informazioni sui bridge di Tor

- ○ Use a default bridge
- ○ Ask for a Tor bridge by email

  Send an empty email to `bridges@torproject.org` from a Gmail or Riseup email address with your phone and scan the QR code that is attached to the automatic reply.

  Scan QR code
- ◉ Enter a bridge that you already know

  Bridge obfs4 172.105.78.187:7

  To save your bridge, create a Persistent Storage on your Tails USB stick.

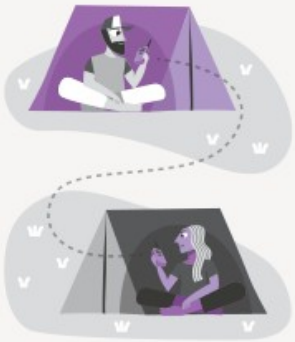
Indietro

Connetti a Tor

Connessione Tor

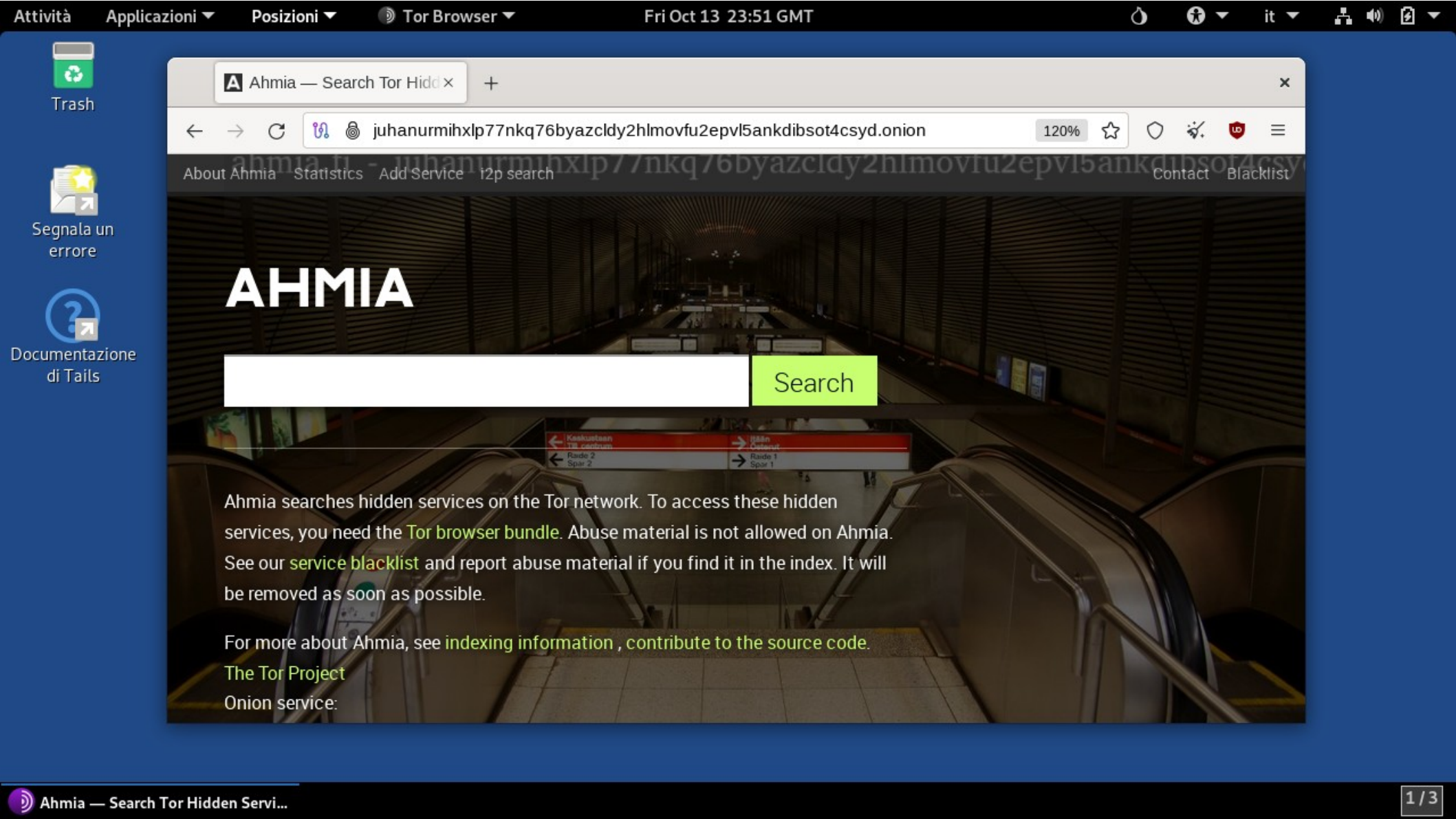
Connesso a Tor correttamente tramite bridge

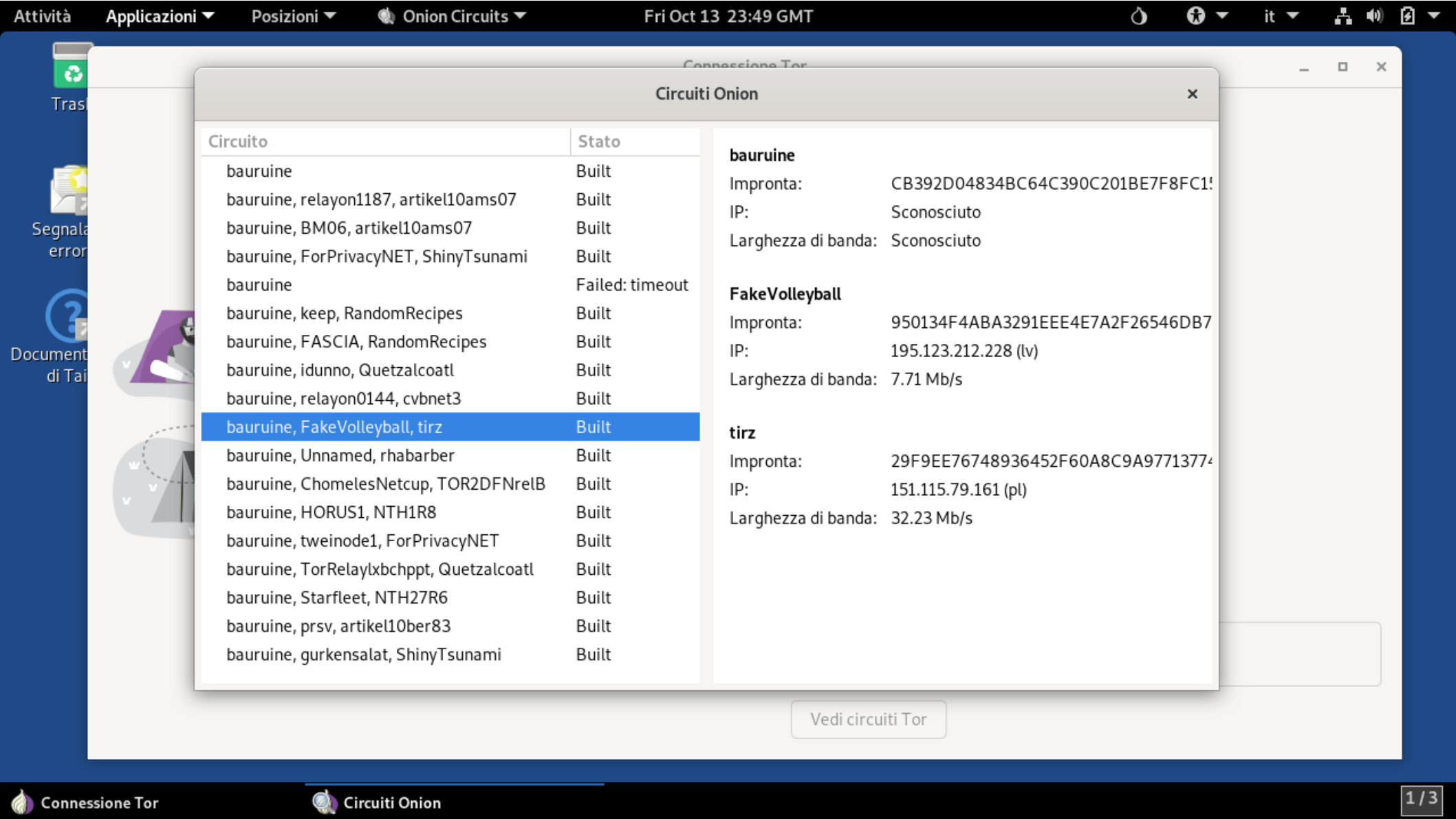
Ora puoi navigare in internet anonimamente e senza censure.

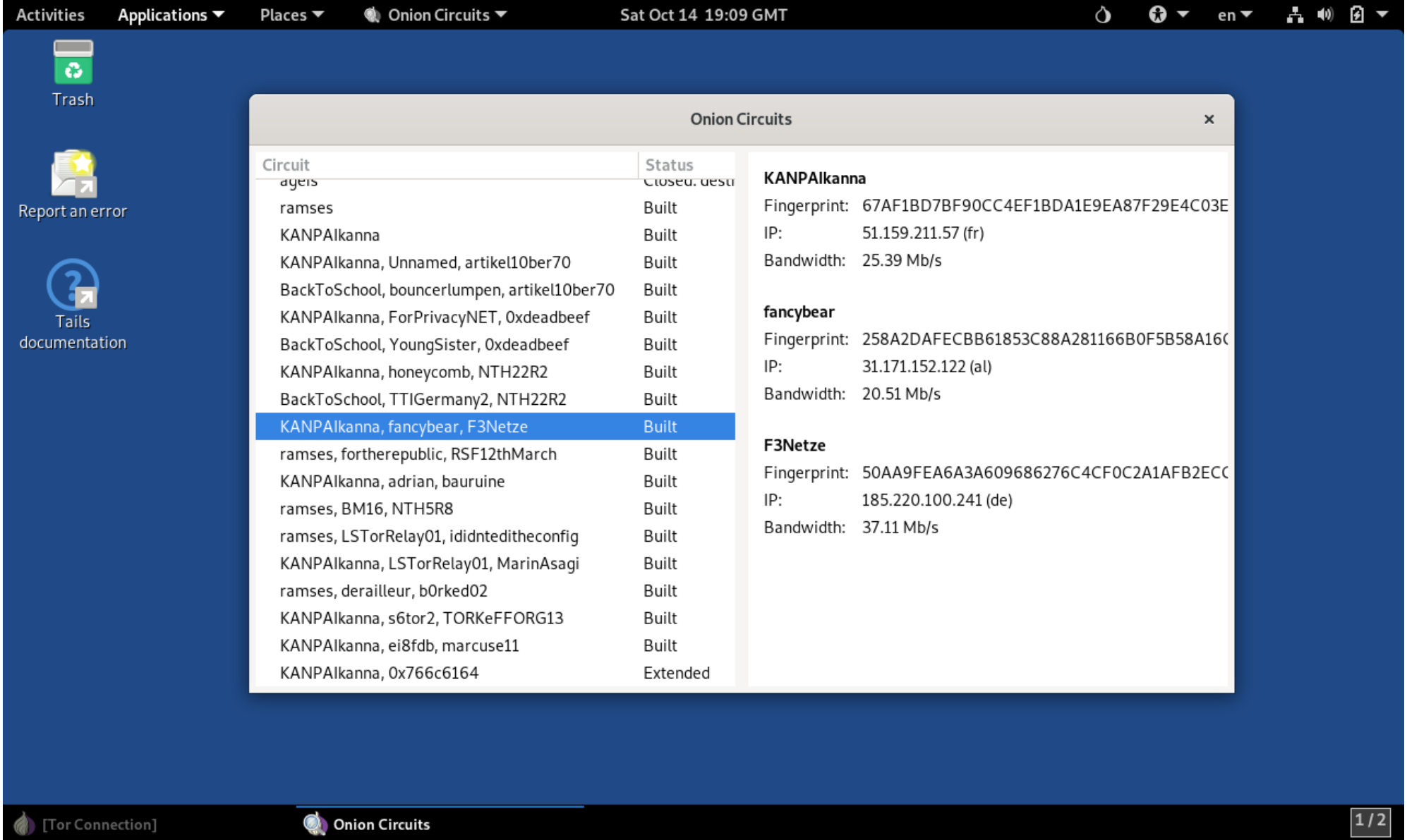


Avvia Tor Browser

Vedi circuiti Tor


Attività
Applicazioni
Posizioni
Tor Browser
Fri Oct 13 23:51 GMT
it
Trash
Segnala un errore
Documentazione di Tails
Ahmia — Search Tor Hidd
juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion
120%
About Ahmia
Statistics
Add Service
i2p search
Contact
Blacklist
AHMIA
Search
Ahmia searches hidden services on the Tor network. To access these hidden services, you need the Tor browser bundle. Abuse material is not allowed on Ahmia. See our service blacklist and report abuse material if you find it in the index. It will be removed as soon as possible.
For more about Ahmia, see indexing information , contribute to the source code.
The Tor Project
Onion service:
Ahmia — Search Tor Hidden Servi...
1 / 3


Attività
Applicazioni
Posizioni
Onion Circuits
Fri Oct 13 23:49 GMT
it
Connessione Tor
Circuiti Onion
Circuito
Stato
bauruine
Built
bauruine, relayon1187, artikel10ams07
Built
bauruine, BM06, artikel10ams07
Built
bauruine, ForPrivacyNET, ShinyTsunami
Built
bauruine
Failed: timeout
bauruine, keep, RandomRecipes
Built
bauruine, FASCIA, RandomRecipes
Built
bauruine, idunno, Quetzalcoatl
Built
bauruine, relayon0144, cvbnet3
Built
bauruine, FakeVolleyball, tirz
Built
bauruine, Unnamed, rhabarber
Built
bauruine, ChomelesNetcup, TOR2DFNrelB
Built
bauruine, HORUS1, NTH1R8
Built
bauruine, tweinode1, ForPrivacyNET
Built
bauruine, TorRelaylxbchppt, Quetzalcoatl
Built
bauruine, Starfleet, NTH27R6
Built
bauruine, prsv, artikel10ber83
Built
bauruine, gurkensalat, ShinyTsunami
Built
bauruine
Impronta: CB392D04834BC64C390C201BE7F8FC1
IP: Sconosciuto
Larghezza di banda: Sconosciuto
FakeVolleyball
Impronta: 950134F4ABA3291EEE4E7A2F26546DB7
IP: 195.123.212.228 (lv)
Larghezza di banda: 7.71 Mb/s
tirz
Impronta: 29F9EE76748936452F60A8C9A9771377
IP: 151.115.79.161 (pl)
Larghezza di banda: 32.23 Mb/s
Vedi circuiti Tor
Connessione Tor
Circuiti Onion
1 / 3


Activities
Applications
Places
Onion Circuits
Sat Oct 14 19:09 GMT
en
Trash
Report an error
Tails documentation
Onion Circuits
Circuit
Status
ramses Built
KANPAlkanna Built
KANPAlkanna, Unnamed, artikel10ber70 Built
BackToSchool, bouncerlumpen, artikel10ber70 Built
KANPAlkanna, ForPrivacyNET, 0xdeadbeef Built
BackToSchool, YoungSister, 0xdeadbeef Built
KANPAlkanna, honeycomb, NTH22R2 Built
BackToSchool, TTIGermany2, NTH22R2 Built
KANPAlkanna, fancybear, F3Netze Built
ramses, fortherepublic, RSF12thMarch Built
KANPAlkanna, adrian, bauruine Built
ramses, BM16, NTH5R8 Built
ramses, LSTorRelay01, ididntedittheconfig Built
KANPAlkanna, LSTorRelay01, MarinAsagi Built
ramses, derailleur, b0rked02 Built
KANPAlkanna, s6tor2, TORKeFFORG13 Built
KANPAlkanna, ei8fdb, marcuse11 Built
KANPAlkanna, 0x766c6164 Extended
KANPAlkanna
Fingerprint: 67AF1BD7BF90CC4EF1BDA1E9EA87F29E4C03E
IP: 51.159.211.57 (fr)
Bandwidth: 25.39 Mb/s
fancybear
Fingerprint: 258A2DAFECBB61853C88A281166B0F5B58A16
IP: 31.171.152.122 (al)
Bandwidth: 20.51 Mb/s
F3Netze
Fingerprint: 50AA9FEA6A3A609686276C4CF0C2A1AFB2EC
IP: 185.220.100.241 (de)
Bandwidth: 37.11 Mb/s
[Tor Connection]
Onion Circuits
1 / 2

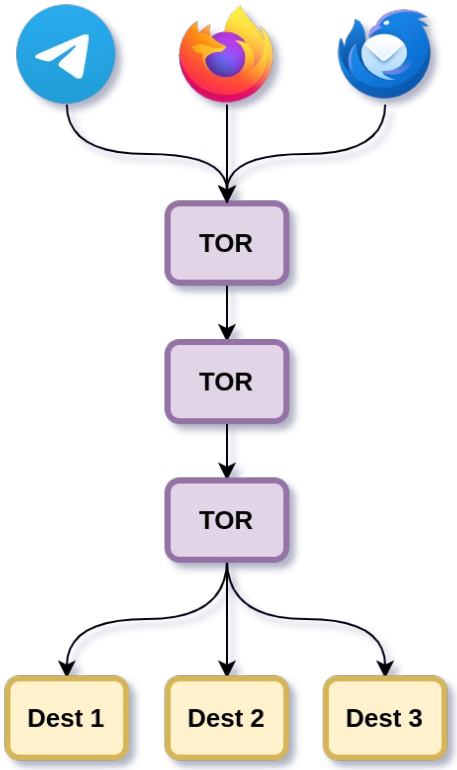
Le entry guards non cambiano!

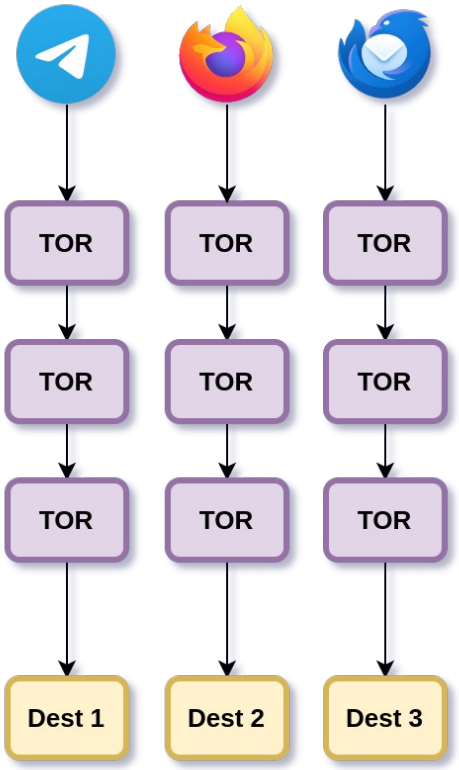
- Se controllo ingresso e uscita posso correlare il traffico
- Torproject sostiene che «The attacker noticing once is as bad as the attacker noticing more often»
- Se i nodi cambiano di continuo prima o poi capiterò nella combinazione sfigata, ma se becco una entry guard buona sono sicuro per sempre
- Quando il servizio tor si spegne salva le guard in /var/lib/tor/state
- Per un hidden service ha senso l'ingresso fisso: ci sono attacchi appositi

Mai incrociare i flussi!

Lug Trieste

Separazione dei circuiti





AppArmor

È gestito il confinamento di alcune applicazioni.

- Profili base presi da Debian
- Tor browser può leggere e scrivere solo in 2 cartelle: ~/Tor Browser e ~/Persistent/Tor Browser
- Evince (pdf reader) e Totem (video player) non possono leggere in ~/.ssh o ~/.gnupg

Protezione da attacchi cold boot

- I dati in RAM persistono per alcuni secondi dopo lo spegnimento
- Forzando lo spegnimento e alimentando di nuovo il PC è possibile recuperare dei dati tramite appositi tool
- Tails azzera la memoria allo spegnimento con il parametro del kernel **`init_on_free=1`**

Un’alternativa: Whonix

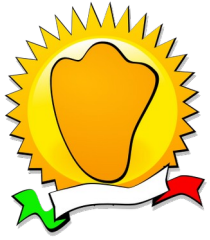
- Distribuzione basata su Kicksecure, che è una Debian hardened.
- Nata nel 2012 come TorBOX, rinominata poi in aos e infine in Whonix
- Kicksecure e Whonix sono mantenute da Patrick Schleizer
- Sponsors ignoti, supporto premium

Whonix

Funziona grazie a 2 virtual machine:

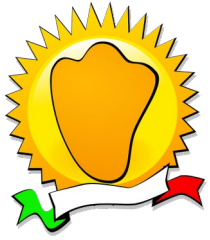
- **Whonix-Gateway**: si occupa del routing via Tor
- **Whonix-Workstation**: dove girano le applicazioni dell'utente

Tutte le connessioni di rete passano per il Gateway e la parte Workstation non ha modo di conoscere il vero indirizzo IP.

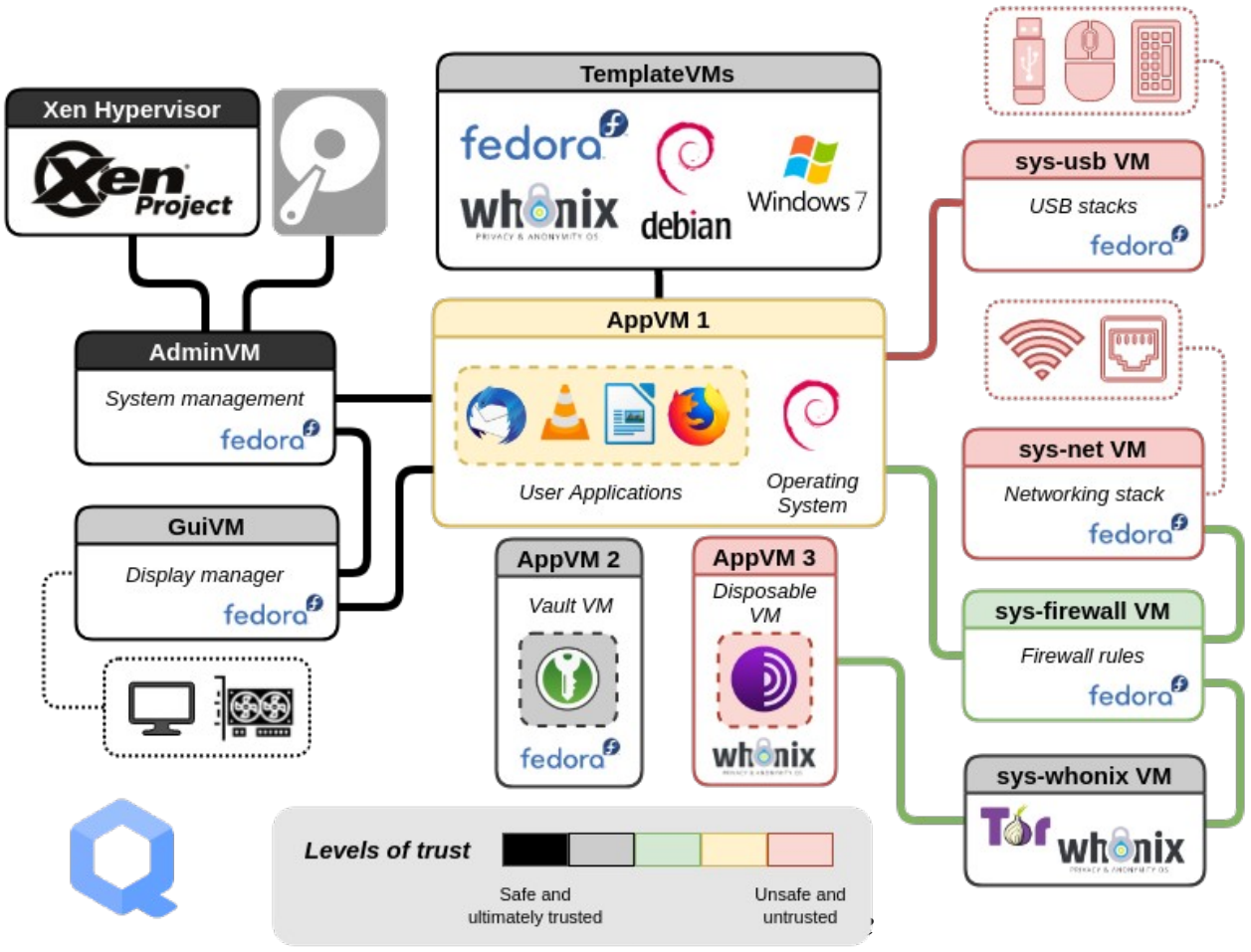


Whonix: chicche

- **Kloak**: keystroke anonymization
- **sdwdate**: Secure Distributed Web Date
- estesa documentazione su come hostare onion services



Qubes OS



Lug Trieste

Grazie per l’attenzione!

Domande?

(se so rispondere)