

Tor per comuni utenti

- Anonimato in rete nell'attività quotidiana:
 - Qual'è l'esperienza dell'utente?
 - Quali sono i problemi?
- Ingredienti:
 - Tor, Windows XP SP3, Anonymous Blogging Guide

Jan Reister

- Traduttore italiano del progetto Tor <https://torproject.org>
- Redattore Nazione Indiana <http://www.nazioneindiana.com>
- Contatti:
 - jan@seul.org
 - GPG: 0x8BC7F656

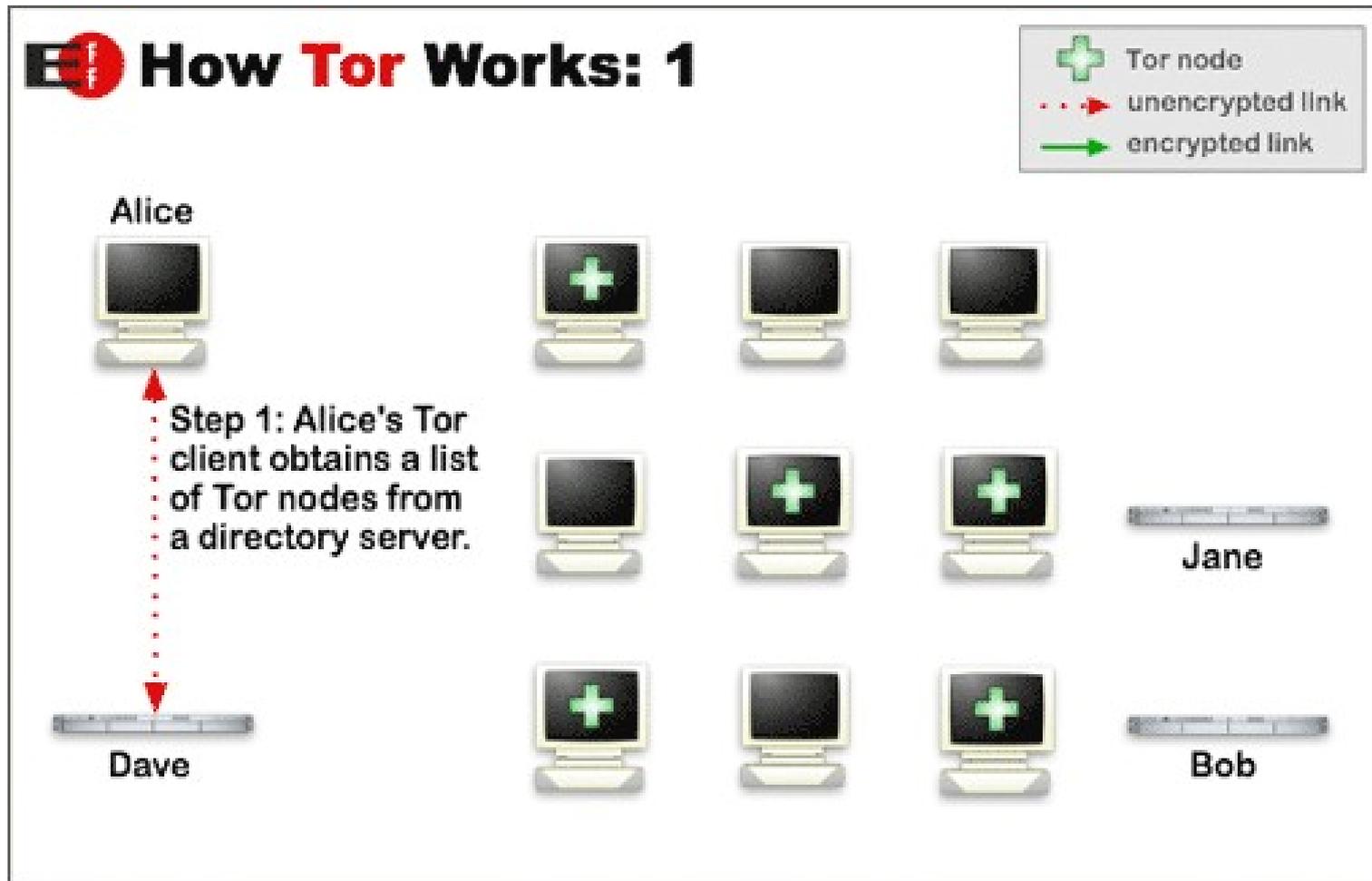
Lo stato del progetto Tor

- Dal 2004: 5 anni di vita
- Versioni: 0.2.0.34, 0.2.1.14-rc
 - Funzionanti, veloci
- 400.000+ utenti?
- 1000+ relay (500+ Exit)
- Disponibile per Windows, Macintosh, Linux

Usi di Tor

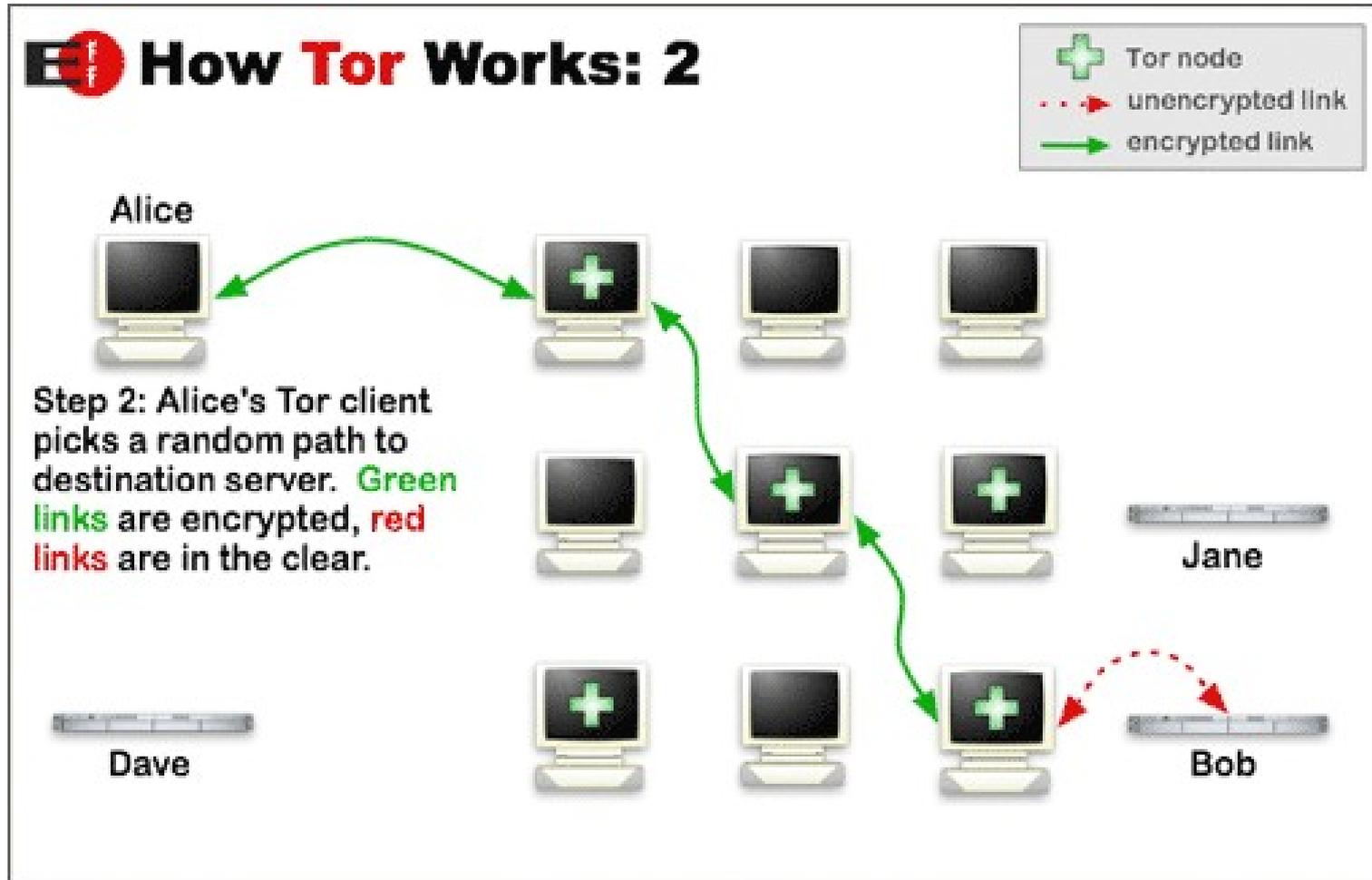
- Rete a bassa latenza che supporta TCP
- Adatto a trasportare il traffico di numerose applicazioni:
 - Web, ssh, IRC, email...
- Tor Browser Bundle (Windows):
 - presenta Tor principalmente come software per la navigazione web anonima

Come funziona Tor



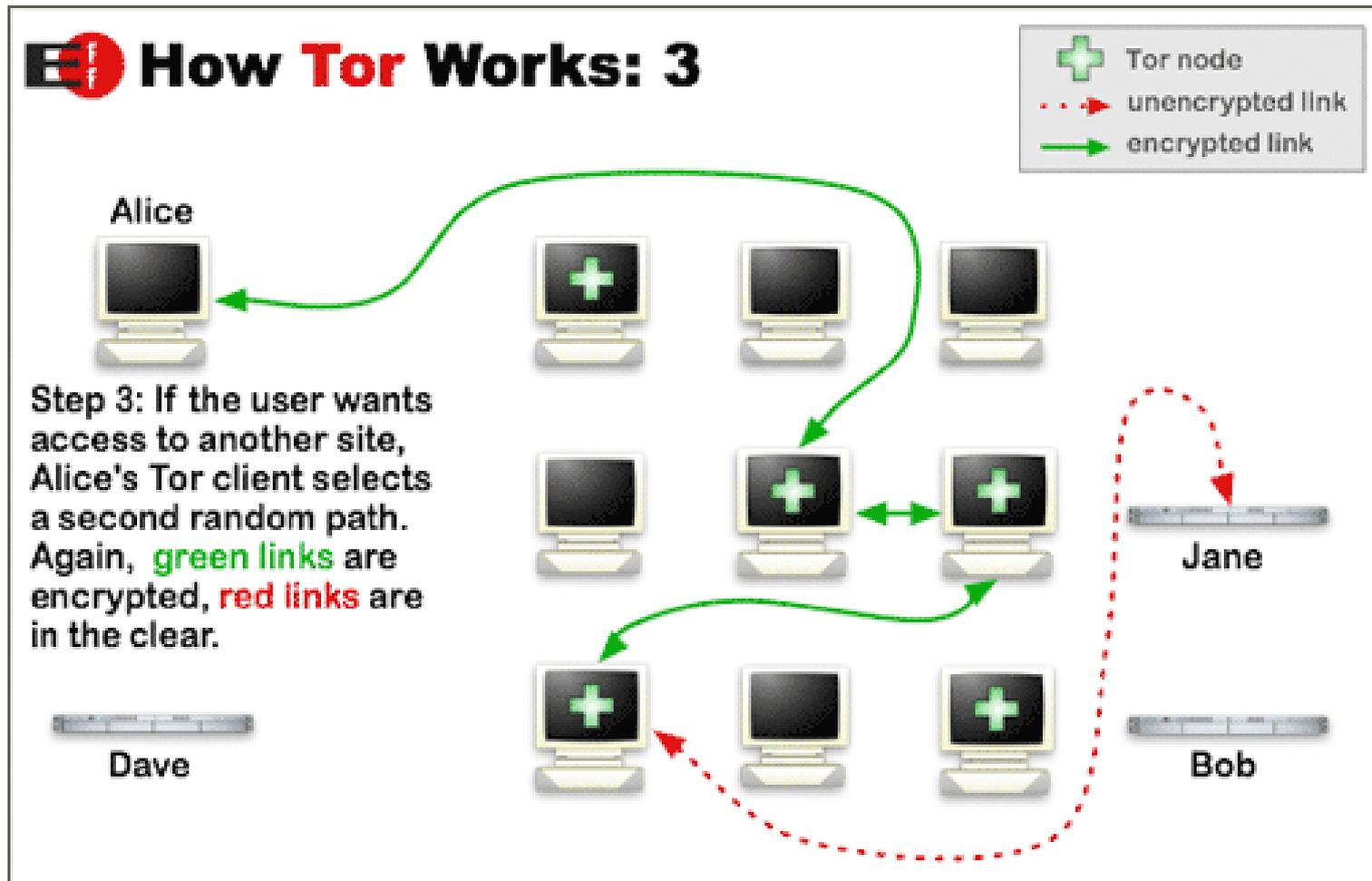
- Fonte: <http://www.torproject.org/overview.html.it>

Come funziona Tor 2



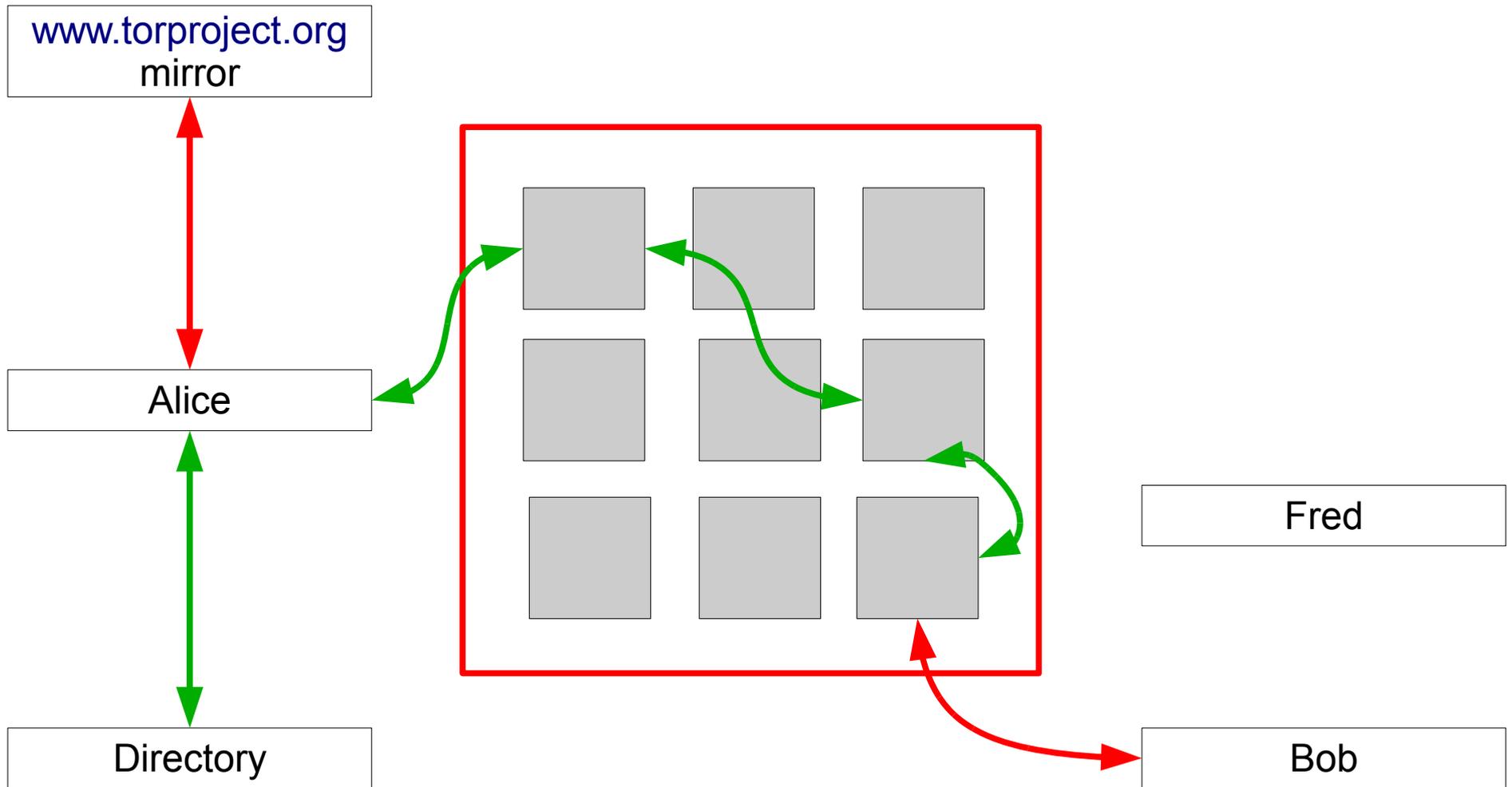
- Fonte: <http://www.torproject.org/overview.html.it>

Come funziona Tor 3



- Fonte: <http://www.torproject.org/overview.html.it>

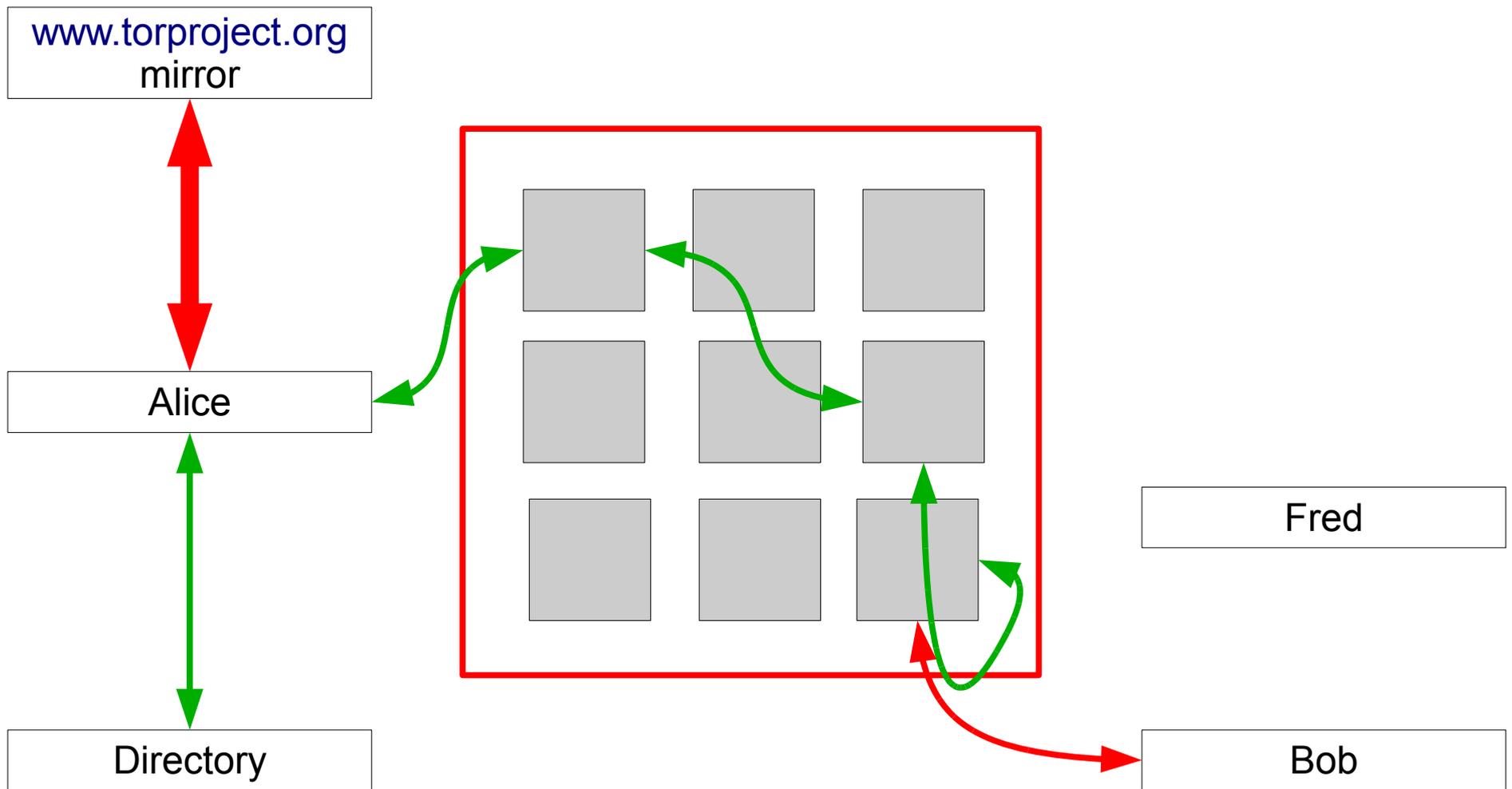
Punti critici ?



Punti critici:

- Ottenere Tor
 - Verifica dell'integrità del software
- Formazione e riuso del circuito
 - Lentezza? misuriamola!
- Exit relay
 - Ascolto e manipolazione da parte dell'exit node
- Sicurezza dell'applicazione usata
 - es. browser: DNS, java, javascript, DOM, CSS...

Ottenere e verificare Tor

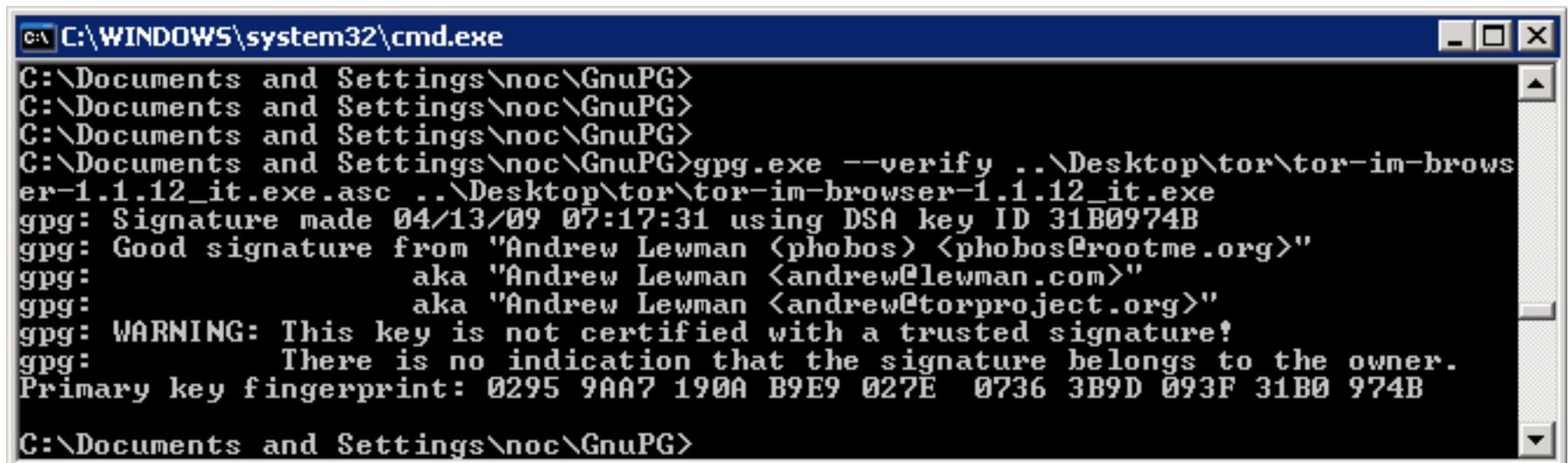


Ottenere Tor è facile

- Web download:
 - <http://www.torproject.org/easy-download.html.it>
 - Mirrors:
 - <http://www.torproject.org/mirrors.html.it>
 - Cache di una ricerca su Google
- Email: gettor@torproject.org
 - Il mittente deve usare DKIM (DomainKeys Identified Mail)
 - Per ora solo usando un account Google Mail (gmail)
<http://mail.google.com>
 - Altri provider DKIM?

Verificare Tor, anzi no.

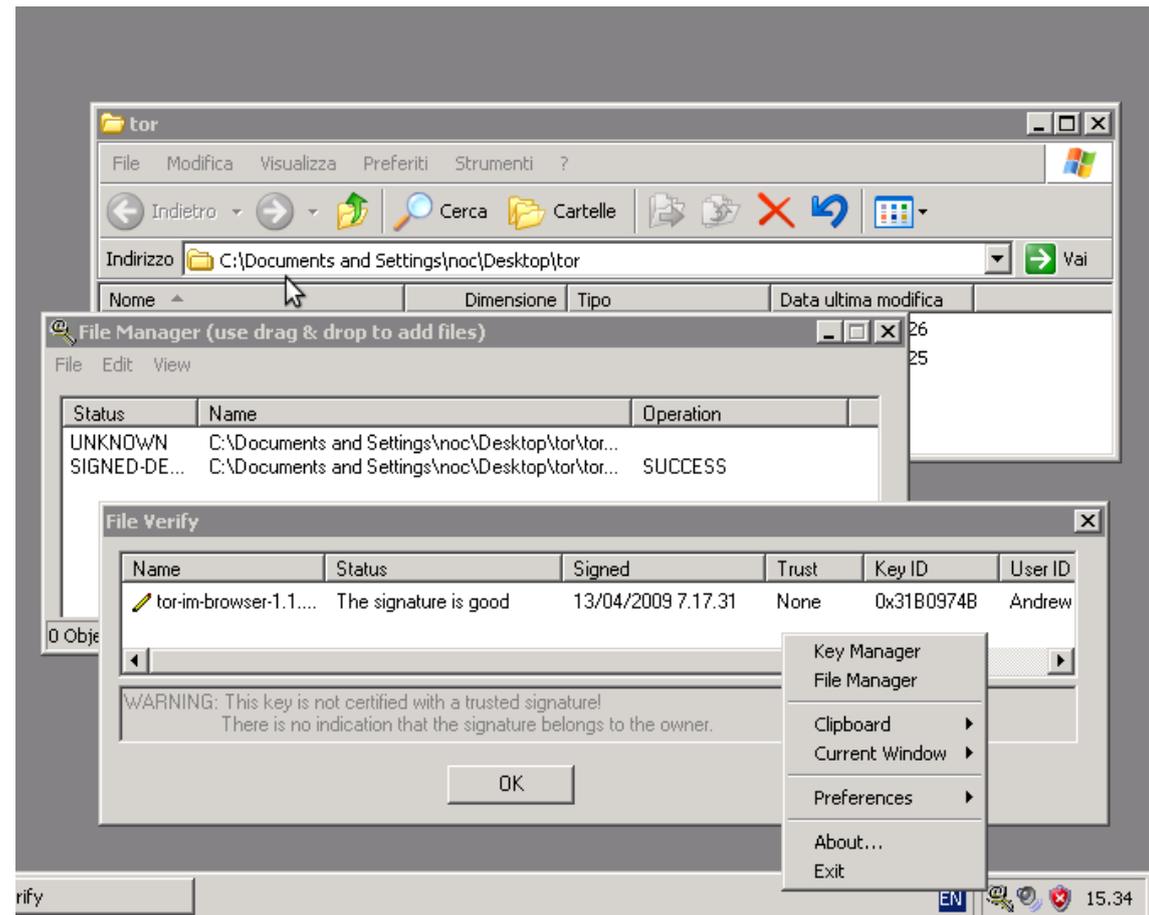
- Verifica delle firme crittografiche e dell'integrità del software
 - <http://www.torproject.org/verifying-signatures.html.it>
 - GnuPG a riga di comando:
 - `gpg -verify <nome>.asc <nome>`
 - <http://www.gnupg.org/download/index.it.html>



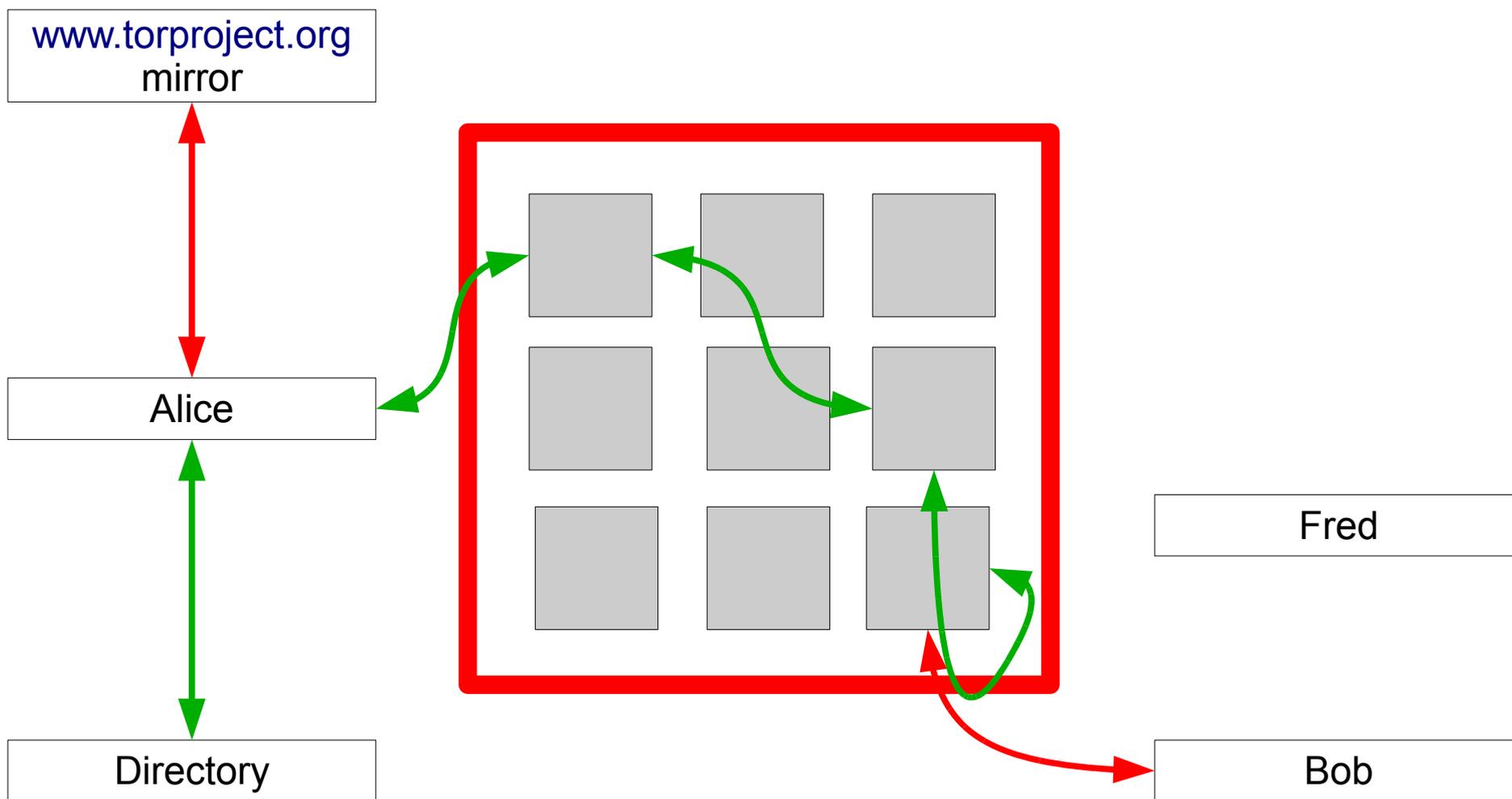
```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\noc\GnuPG>
C:\Documents and Settings\noc\GnuPG>
C:\Documents and Settings\noc\GnuPG>
C:\Documents and Settings\noc\GnuPG>gpg.exe --verify ..\Desktop\tor\tor-im-browser-1.1.12_it.exe.asc ..\Desktop\tor\tor-im-browser-1.1.12_it.exe
gpg: Signature made 04/13/09 07:17:31 using DSA key ID 31B0974B
gpg: Good signature from "Andrew Lewman (phobos) <phobos@rootme.org>"
gpg:          aka "Andrew Lewman <andrew@lewman.com>"
gpg:          aka "Andrew Lewman <andrew@torproject.org>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 0295 9AA7 190A B9E9 027E  0736 3B9D 093F 31B0 974B
C:\Documents and Settings\noc\GnuPG>
```

Verificare Tor, forse

- Applicazione GUI integrata in Windows?
- WinPT <http://winpt.gnupt.de/>
- GnuPT_Portable
 - Ancora laborioso!
 - Schermata:
- Alternative?



Prestazioni



Usare Tor Browser Bundle

- Contenuti:
 - Pannello di controllo Vidalia
 - Tor, Polipo
 - Firefox
 - Java è disabilitato di default
 - Torbutton
 - Pidgin (IM/chat client)

Tor Browser

File Modifica Visualizza Preferiti Strumenti ?

Indietro ◀ ▶ ↻ 🔍 Cerca 📁 Cartelle 📁 🗑️ ↺ 📅

Pannello di Controllo Vidalia

Stato

Loading relay information

Shortcut di Vidalia

- Stop Tor
- Mostra la rete
- Avviamento del relaying
- Usa una nuova identità
- Grafico dell'ampiezza di banda
- Log dei messaggi
- Aiuto
- Impostazioni
- Informazioni su
- Esci

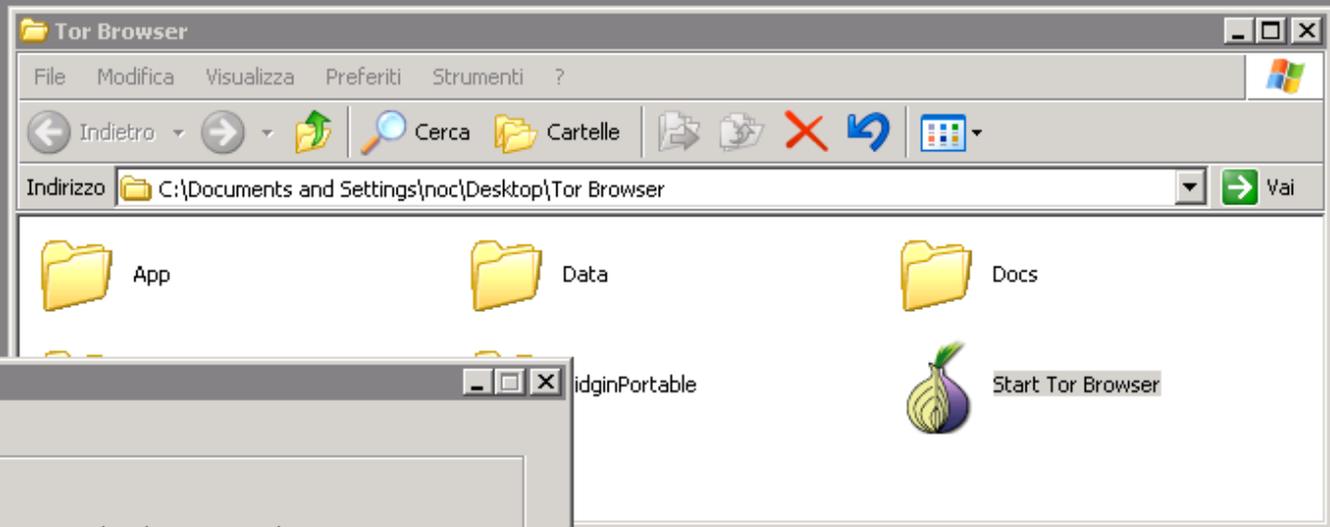
Mostra questa finestra all'avvio

Nascondi

Vai

Docs

Start Tor Browser



Pannello di Controllo Vidalia

Stato

 Connected to the Tor network!

Shortcut di Vidalia

-  Stop Tor
-  Mostra la rete
-  Grafico dell'ampiezza di banda
-  Log dei messaggi

Mostra questa finestra all'avvio

Are you using Tor? - Mozilla Firefox

File Modifica Visualizza Cronologia Segnalibri Strumenti ?

Indirizzo <https://check.torproject.org/?lang=it&small=1> Google

Più visitati About Tor TorCheck at Xenobite...

Congratulazioni. Stai usando Tor.

Per favore leggi [il sito web di Tor](#) per maggiori informazioni sull'uso sicuro di Tor.

Ulteriori informazioni:
Il tuo indirizzo IP sembra essere: 78.142.140.194
Questo piccolo script utilizza [tordnsel](#)
You may also be interested in the [Tor Bulk Exit List Exporter](#)

Questo server non raccoglie nei log nessuna informazione sui visitatori.

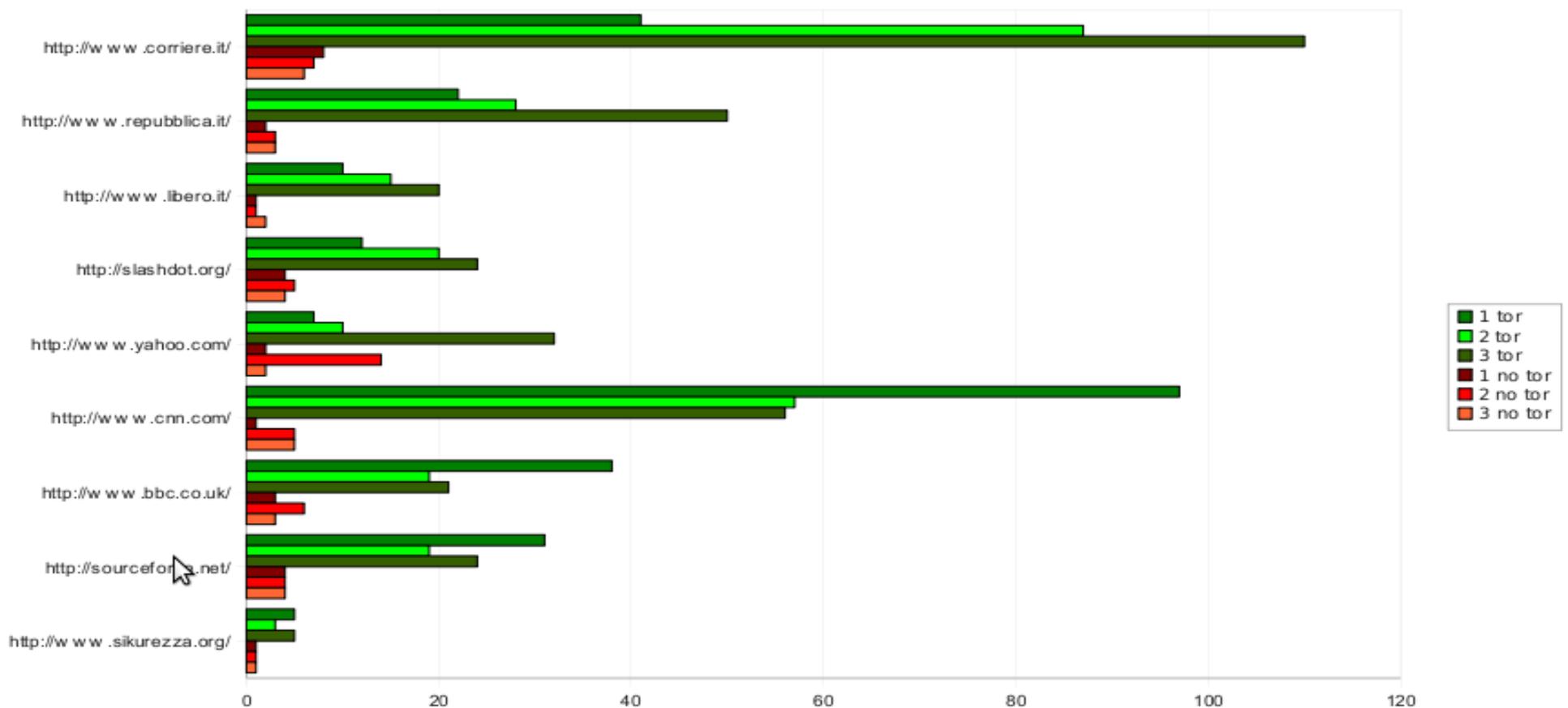


Completato check.torproject.org Tor attivato

Navigazione web

- Fonte: bbbluedefense
- Tempi in secondi

Statistiche accesso siti con e senza tor



Navigazione web

- Lentezza?
- Prestazioni adeguate al lavoro sul web
 - empiricamente: 5% di errori (siti irraggiungibili)
 - Buona salute della rete e degli exit node
- Ma tempi di caricamento più lunghi di 1 ordine di grandezza
- Contromisure:
 - Riutilizzo dei circuiti sulla stessa destinazione
 - Navigazione organizzata, a schede multiple

You Tube Broadcast Yourself™ Worldwide | English [Sign Up](#) | [QuickList \(0\)](#) | [Help](#) | [Sign In](#)

[Home](#) [Videos](#) [Channels](#) [Community](#) [Search](#) [Upload](#)

Meet the Media Guru: Cory Doctorow (BoingBoing) on Obama, privacy and copyright

Hello, you either have JavaScript turned off or an old version of Adobe's Flash Player. [Get the latest Flash player.](#)

Upgrade to Flash Player 10 for improved playback performance. [Upgrade Now](#) or [More Info](#).

★★★★★ 6 ratings 2,516 views

Favorite Share Playlists Flag

MySpace Facebook Twitter [\(more share options\)](#)

▶ **Statistics & Data**

▶ **Video Responses (0)** [Sign in to post a Video Response](#)

▼ **Text Comments (1)** [Options](#) [Sign in to post a Comment](#)

tookaysevon (1 month ago) [Reply](#) 0

I don't agree on the live performance example here, because it really depends on the music genre. If you go to a rock concert, of course you're expecting some sort of show. But go to a classical music concert and if there's a show it's just going to be ridiculous. Otherwise, very interesting answers.

Blogosfere

blogosfere [Subscribe](#)
March 06, 2009 [\(more info\)](#)

Cory Doctorow in Milan for "Meet the Media Guru" talks about the innovation Obama has brought in politics 2.0, copyright and creative commons, privacy on Facebook and State control. Interview and ...

URL

Embed

▼ **More From: blogosfere**

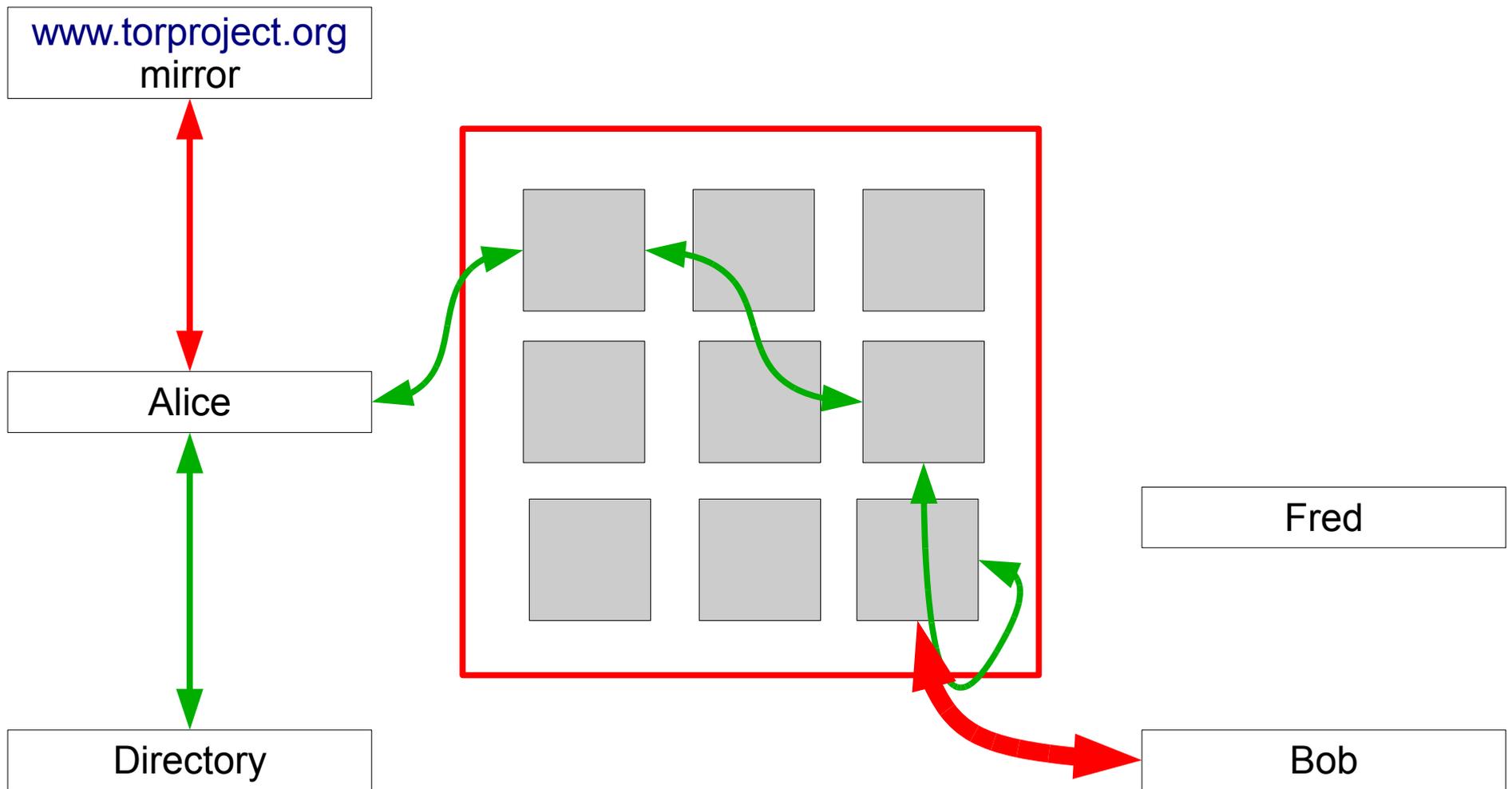
Women@Internet Show: parla Lorenzo Amadio di Pu...
32 views 3:00

Women@Internet Show: il parere degli spettatori
32 views 0:32

Esperienza utente: web 2.0

- I contenuti dinamici sono un rischio per l'anonimato:
 - Java, Flash, ActiveX, RealPlayer, Quicktime, Adobe PDF e altri possono essere usati per svelare il tuo indirizzo IP.
 - Il plugin Torbutton blocca o limita fortemente questi contenuti
- Difficoltà per chi lavora con multimedia (es. citizen journalism):
 - Usare Tor e non-Tor contemporaneamente

L'ultimo nodo d'uscita



Se l'autenticazione è in chiaro

- Un exit relay Tor (nodo d'uscita) può leggere le connessioni in chiaro:
 - Furto di credenziali
 - Manipolazione dei contenuti
 - Monitoraggio dell'uso
- Soluzioni?:
 - Usare sequenze di identità a perdere
 - Problema della perdita (assenza) di reputazione

Problema connessioni cifrate (https)

- Un exit relay Tor non può leggere le connessioni https, ma può impersonare il sito di destinazione (Man In The Middle):
 - Viene presentato comunque un certificato differente
- L'importanza della verifica dei certificati
 - Cattive abitudini personali (ignorare i numerosi messaggi del browser)
 - Difficoltà oggettive (chi annota su un taccuino il fingerprint dei siti visitati e li confronta?)
- L'estensione Perspectives
<http://www.cs.cmu.edu/~perspectives/firefox.html>
 - (Via Marco Bonetti)

Un ciclo di lavoro quotidiano

- Anonymous Blogging with Wordpress and Tor
 - di Ethan Zuckerman, pubblicato da Global Voices
 - <http://advocacy.globalvoicesonline.org/projects/guide/>
 - Traduzione italiana in corso
 - Una guida ad uso di attivisti civili, operatori umanitari e cittadini.
 - Come scrivere (e leggere) online senza rivelare propria identità.

1 Creare un indirizzo email

- Usare Google Mail per l'anonimato: un ossimoro?
- Gmail si usa per gettor e per ottenere i bridge
- Usare almeno un URL come:
 - <https://mail.google.com/mail/h/>
- I controlli antispam, captcha, password strength non interferiscono con l'uso di Tor

You are currently viewing Google Mail in basic HTML. [Switch to standard view](#) | [Set basic HTML as default view](#)

uqualsiasi@googlemail.com | [Settings](#) | [Help](#) | [Sign out](#)



Search Mail

Search the Web

[Show search options](#)

[Create a filter](#)

Compose Mail

Archive

Report Spam

Delete

More Actions... ▾

Go

[Refresh](#)

1 - 3 of 3

Inbox (3)

[Starred](#) ★

[Sent Mail](#)

[Drafts](#)

[All Mail](#)

[Spam](#)

[Trash](#)

- | | | | |
|--------------------------|-----------------------------|--|----------|
| <input type="checkbox"/> | The Google Mail Team | Customize Google Mail with colors and themes - To spice up your inbox | 11:35 am |
| <input type="checkbox"/> | The Google Mail Team | Access Google Mail on your mobile phone - The days of needing your | 11:35 am |
| <input type="checkbox"/> | The Google Mail Team | Import your contacts and old email - You can import your contacts and | 11:35 am |

Archive

Report Spam

Delete

More Actions... ▾

Go

[Refresh](#)

1 - 3 of 3

Contacts

Labels

[Edit labels](#)

Use the search box or **search options** to find messages quickly!

You are currently using 0 MB (0%) of your 7329 MB

Google Mail view: [standard](#) | **basic HTML** [Learn more](#)

2 registrare un nuovo blog

- <http://wordpress.com>
- L'attivazione dell'account wordpress.com è legata all'email fornita

Express yourself. Start a blog.

[See our free features →](#)

213,102 BLOGGERS, 176,382 NEW POSTS, 45,297,721 WORDS TODAY.

Preferred Language:

WordPress.com is also available in [Deutsch](#).

Already Hip?

Username:

Password:

Remember me

[Lost your password?](#)

Hawt Post [More →](#)



Announcing VideoPress.com

We've been busy lately here at WordPress.com — we've had an announcement of a new or updated feature for you every day this week. Today, you're getting a two-fer! Earlier this week, we announced VideoPress, the [...]

WordPress.com News



You are currently viewing Google Mail in basic HTML. [Switch to standard view](#) | [Set basic HTML as default view](#)

uqualsiasi@googlemail.com | [Settings](#) | [Help](#) | [Sign out](#)



Search Mail

Search the Web

[Show search options](#)

[Create a filter](#)

[Compose Mail](#)

[Refresh](#)
1 - 5 of 5

[Inbox \(3\)](#)

[Starred](#)

[Sent Mail](#)

[Drafts](#)

[All Mail](#)

[Spam](#)

[Trash](#)

<input type="checkbox"/>	WordPress.com	New Wordpress.com Blog: Qualsiasi's Blog - Your new Wordpress.com blog has	11:41 am
<input type="checkbox"/>	WordPress.com	Activate qualsiasi.wordpress.com - Howdy, Thank you for signing up with	11:40 am
<input type="checkbox"/>	The Google Mail Team	Customize Google Mail with colors and themes - To spice up your inbox with	11:35 am
<input type="checkbox"/>	The Google Mail Team	Access Google Mail on your mobile phone - The days of needing your	11:35 am
<input type="checkbox"/>	The Google Mail Team	Import your contacts and old email - You can import your contacts and mail	11:35 am

[Refresh](#)
1 - 5 of 5

[Contacts](#)

Labels

[Edit labels](#)

Search accurately with [operators](#) including **from:** **to:** **subject:**

You are currently using 0 MB (0%) of your 7329 MB

Google Mail view: [standard](#) | **basic HTML** | [Learn more](#)

- Dashboard
- Dashboard
- Blog Stats
- Blog Surfer
- My Comments
- Tag Surfer
- Subscriptions
- Readomatic
- My Blogs

- Posts
- Media
- Links
- Pages
- Comments
- Polls

- Appearance

Dashboard

WordPress tip: [Update your about page](#) so your readers can learn a bit about you.

Right Now

At a Glance

1 Post	1 Comment
1 Page	1 Approved
1 Category	0 Pending
0 Tags	0 Spam

Theme **Kubrick** with **0 Widgets** [Change Theme](#)

Akismet blocks spam from getting to your blog, but there's nothing in your [spam queue](#) at the moment.

Recent Comments

 From [Mr WordPress](#) on [Hello world!](#) #
Hi, this is a comment. To delete a comment, just log in, and view the posts!

QuickPress

Title

Upload/Insert     

Content

Tags

[Save Draft](#) [Reset](#) [Publish](#)

Recent Drafts

There are no drafts at the moment

Stats

Google
Talk

About Yourself

Biographical
Info

Share a little biographical information to fill out your profile. This may be shown publicly.

New
Password

If you would like to change the password type a new one. Otherwise leave this blank.

Type your new password again.

Strong

Hint: The password should be at least seven characters long. To make it stronger, use upper and lower case letters, numbers and

symbols like ! " ? \$ % ^ &).

Update Profile

3 Scrivere e pubblicare

- L'uso di AJAX crea talvolta errori per chi usa Tor+Torbutton
- L'operazione di pubblicazione soffre di frequenti errori imputabili a Tor + Torbutton,
- Ma è comunque possibile pubblicare normalmente.

Dashboard

Add New Post

- Posts
 - Edit
 - Add New**
 - Post Tags
 - Categories
- Media
- Links
- Pages
- Comments
- Polls

messaggio anonimo

Upload/Insert Visual HTML

B *I* ABC [List Icons] [Link Icon] [Image Icon] [Table Icon]

Un messaggio di esempio, senza indicazioni di sorta.

Path: p » span

Word count: 8

Excerpt

Publish

Save Draft Preview

Status: **Draft** [Edit](#)

Visibility: **Public** [Edit](#)

Schedule for: **May 22, 2009 @ 11:52** [Edit](#)

Schedule

Post Tags

Add new tag Add

Separate tags with commas.

[Choose from the most used tags in Post Tags](#)

Categories

All Categories Most Used

Qualsiasi's Blog

Just another WordPress.com weblog

messaggio anonimo

By qualsiasi

Un messaggio anonimo, senza indicazioni di sorta.
Un messaggio anonimo, senza indicazioni di sorta.

Possibly related posts: (automatically generated)

» [Un messaggio di pace a San Valentino](#)

This entry was posted on May 22, 2009 at 11:55 am and is filed under [Uncategorized](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can [leave a response](#), or [trackback](#) from your own site.

One Response to "messaggio anonimo"

qualsiasi Says:
[May 22, 2009 at 11:57 am](#) | [Reply](#)



un commento di qualsiasi

[response](#), or [trackback](#) from your own site.

One Response to "messaggio anonimo"

qualsiasi Says:

May 22, 2009 at 11:57 am | [Reply](#)



un commento di qualsiasi

un nome Says: *Your comment is awaiting moderation.*

May 22, 2009 at 12:04 pm | [Reply](#)



un altro commento qualunque

Leave a Reply

Name (required)

Mail (will not be published) (required)

Website

Notify me of follow-up comments via email.

Submit Comment

Conclusioni

- Tor è alla portata di un pubblico con competenze informatiche di base.
- Come tale è utile principalmente all'uso del web (IM a parte):
 - Nei suoi aspetti statici (testo, immagini)
 - Penalizzando i contenuti dinamici (flash, java)
- L'esperienza d'uso complessiva (lentezza, errori) richiede una adeguata motivazione degli utenti
 - Regimi oppressivi, dispute locali, antimafia...
 - No p2p, vandalismo, usi estemporanei.

Note

- "Tor" e l'"Onion Logo" sono marchi registrati di The Tor Project, Inc. <https://www.torproject.org/trademark-faq.html.it>
- wordpress.com è un marchio registrato di Automattic, Inc.
- Gmail, Google sono marchi registrati di Google, Inc.
- Questo lavoro è pubblicato sotto la Licenza Creative Commons Public License Attribuzione - Non commerciale - Condividi allo stesso modo 2.5 (Italia)
- <http://creativecommons.org/licenses/by-nc-sa/2.5/it/>