

# Introduzione a TOR



# Indice

- Come funziona Internet, cosa e' un indirizzo ip, cosa sono i proxy
- Cosa e' Tor e come funziona
- Punti deboli di Tor
- Uso “avanzato” di Tor
- Links
- Credits & Copyright

# Anonimato in rete

Delle persone che visitano un sito web è possibile conoscere molti dettagli:

1. da dove provengono (informazioni dall'*indirizzo IP, referral*)
2. con quale mezzo (il *browser*, il sistema operativo)
3. il dettaglio di cosa fanno in quel sito (*cookies*)
4. potenzialmente dove vanno quando lasciano il sito (*link, cookies* traccianti)

# Che cos'è l'anonimato in rete?

È la proprietà tecnologica di una connessione.

Garantisce al mittente che:

1. i dati trasportati siano leggibili solo dal destinatario
2. il destinatario non possa risalire all'*indirizzo IP* del mittente

# TOR



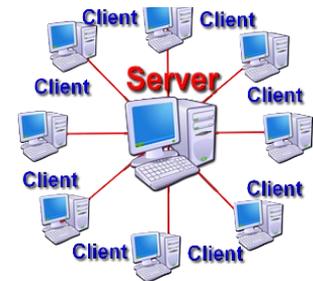
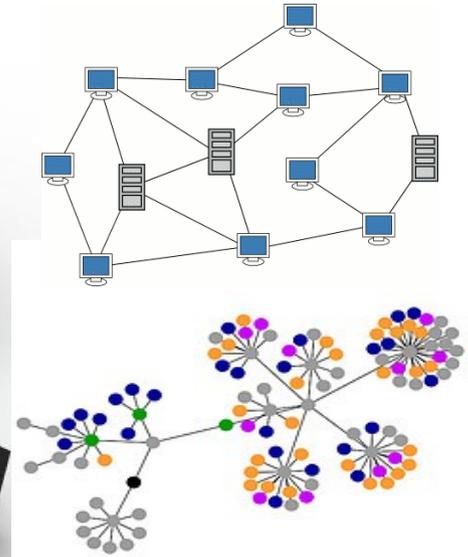
# L'indirizzo IP

L'indirizzo IP è un'etichetta numerica che **identifica** un dispositivo (più precisamente: la sua scheda di rete) collegato ad una rete informatica tramite il protocollo TCP/IP (per esempio, Internet) e quindi consente di individuare il percorso per **raggiungerlo** tramite un altro dispositivo di rete. (Es. 130.89.148.14)

Dimostrazione: *Wireshark*

# TOR

## COME FUNZIONA INTERNET?



# TOR

## COME FUNZIONA INTERNET?

- Demo <http://ip-check.info/?lang=en>

IP check - Tor Browser

Are you using Tor?

ip-check.info/index.php?jsID=12006764abc&auth=9728680308137236722525183=137236722525183c-757880182c-1303199526&referrer=unchanged

Private and Secure Web Surfing

JonDonym

By moving your mouse pointer over the underlined text fields, you get detailed information about the individual test results.

Your IP	77.171.200	Traceroute
Your location	Netherlands	Show on map
Your net provider	Routit BV	Whois IP
Reverse DNS	fi.██████████.net	Whois Domain

LEARN MORE about the individual tests performed by the IP Check... [Click here!](#)

Attribute	Value	Rating
Cookies	This web site may receive cookies from you	medium
Authentication	protected	good
HTTP session	10 minutes (until your Tor identity is changed)	medium
Referer	Original Websites may see from which other website you come from!	medium
Signature	8ab3a24c55ad99f4e3a6e5c03cad944f6 (Firefox)	good
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:17.0) Gecko/20100101 Firefox/17.0	good
SSL_session_id	687B16F61DFBD61FCD4006948B038794123FFB1F1DA864853FEA398567459426	neutral
Language	en-us;q=0.5	good
Content types	text/html,application/xhtml+xml,application/xml;q=0.9;*/.*;q=0.8	good
Encoding	gzip, deflate	good
Do-Not-Track		good

A plugin is needed to display this content.

Free Trial for Premium Services

Get your free test code for JonDonym Premium services!

JonDonym News

JonDoBrowser 0.7 - Status Report  
Tue, 04 June 2013  
Planned Maintenance  
Fri, 03 June 2013

Speaker's Corner

Terrorist Attacks  
Mon, 24 June 2013  
PRISM Brothers  
Wed, 12 June 2013

For your web site - free!

Your IP: Tor  
Browser: Firefox/Torbutton  
Location: Netherlands  
Net provider: Routit BV

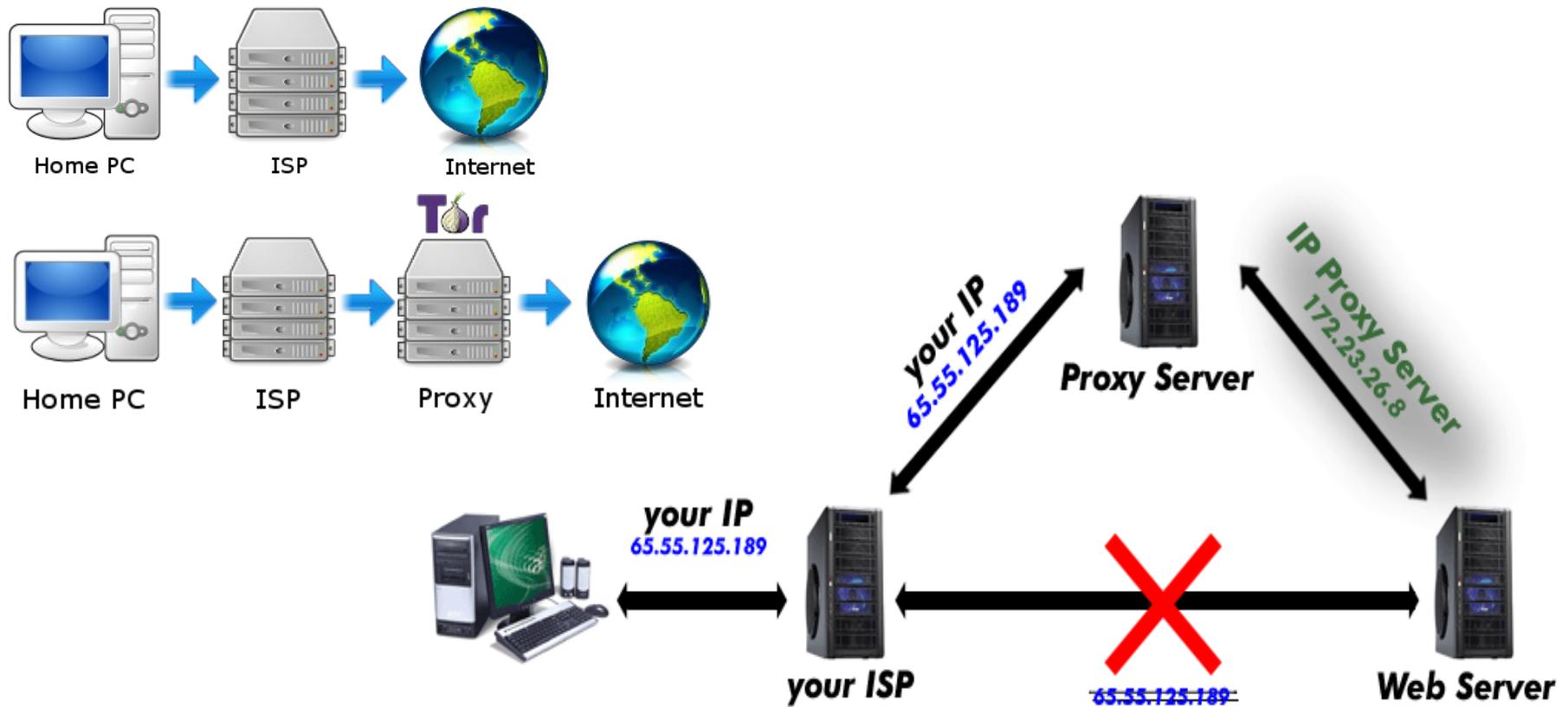
Use this image on your web site.  
**Get your own IP check here!**

More anonymity tests

BrowserLeak  
Whois.net  
MAXA Tools Privacy Test  
BrowserSPYak  
Master Reconnaissance Tool

# TOR

## COME FUNZIONA INTERNET?



# TOR

## COSA E' TOR?

Lo scopo di Tor è quello di rendere difficile l'analisi del traffico e proteggere così la privacy, la riservatezza delle comunicazioni, l'accessibilità dei servizi. Il funzionamento della rete Tor è concettualmente semplice: i dati che appartengono ad una qualsiasi comunicazione non transitano direttamente dal *client* al *server*, ma passano attraverso i server Tor che agiscono da *router* costruendo un circuito virtuale crittografato a strati.

*(wikipedia)*

# TOR

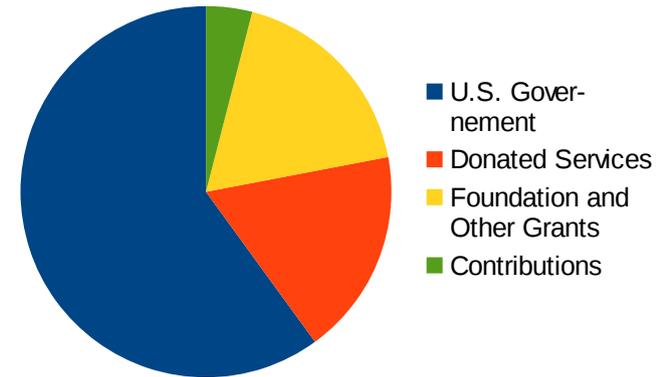
## COSA E' TOR?

- un software open-source e multiplatforma
- una rete di tunnel con il proprio protocollo
- consente di navigare in maniera anonima come se stessi usando un normale *proxy*, permette cioè di nascondere il nostro **Indirizzo IP**

# TOR

## CHI C'E' DIETRO TOR?

- Tor e' un software open-source rilasciato nel 2002 e portato avanti da “**The Tor Project, Inc.**” un'organizzazione no-profit dedita alla ricerca e sviluppo di strumenti per l'anonimato online e la privacy.



2012 - <http://www.torproject.org/about/financials>

- Finanziato dal Ministero della Difesa Americano, Electronic Frontier Foundation, Voice of America, Google, NLnet, Human Rights Watch, National Science Foundation, Dipartimento Esteri U.S., Swedish International Development Agency, the Knight Foundation, The Broadcasting Board of Governors, SRI International, e da molti *donatori* singoli sparsi per il mondo.

# TOR

## CHI C'E' DIETRO TOR?

La fondazione Tor fornisce diversi strumenti per la difesa della privacy:

- Tor Browser (T.B.B.),
- Vidalia,
- Tails,
- Orbot,
- Tor2web,
- Obfsproxy,
- ...

### Our Projects



#### Tails

Live CD/USB distribution preconfigured to use Tor safely.



#### Orbot

Tor for [Google Android](#) devices.



#### Tor Browser

Tor Browser contains everything you need to safely browse the Internet.



#### Arm

Terminal application for monitoring and configuring Tor.



#### Atlas

Site providing an overview of the Tor network.



#### Obfsproxy

Obfsproxy is a tool that attempts to circumvent censorship.



#### Stem

Library for writing scripts and applications that interact with Tor.



#### Tor cloud

A user-friendly way of deploying bridges to help users access an uncensored Internet.

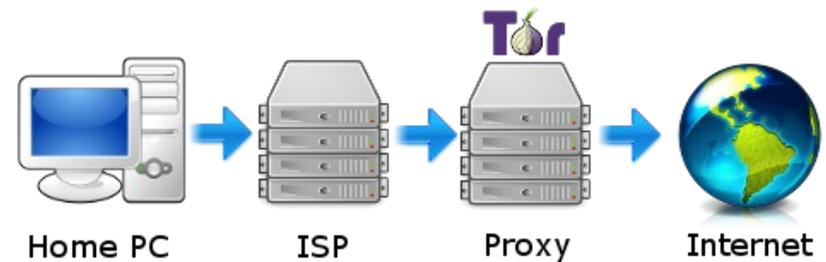
[Learn more about our projects »](#)

# TOR

## COME FUNZIONA TOR?

Le figure coinvolte sono:

- Mittente
- Rete Tor:
  - Entry node (o Guard node)
  - Nodo intermedio
  - Exit node
- Destinatario



# TOR

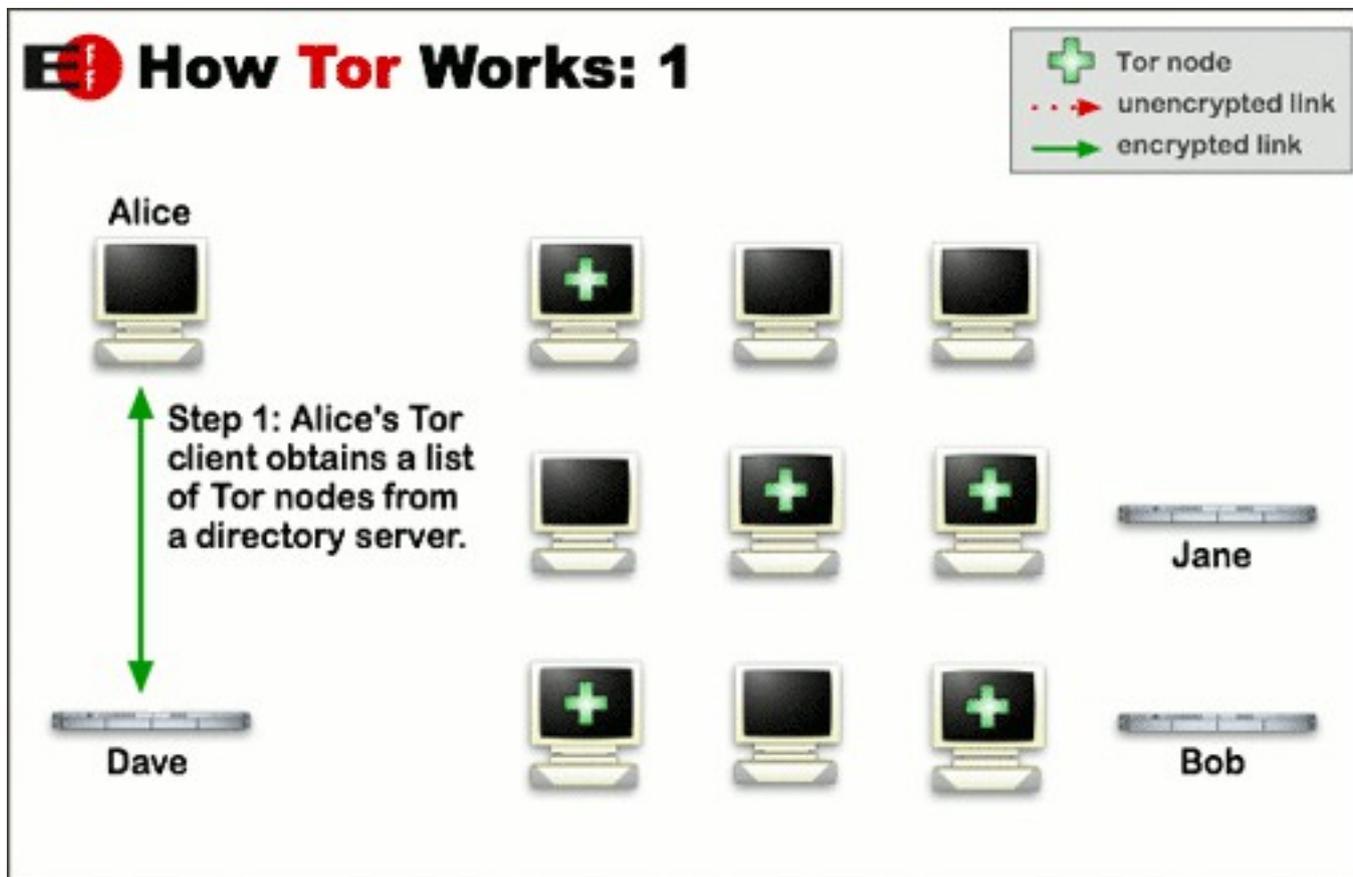
## DIFFERENZA TRA UN PROXY E TOR?

- Un normale proxy conosce:
  - il vostro indirizzo IP
  - il destinatario
  - il contenuto del messaggio
- Tor conosce:

	Entry node	Middle node	Exit node
...il tuo IP	X		
...il destinatario			X
...il contenuto			X

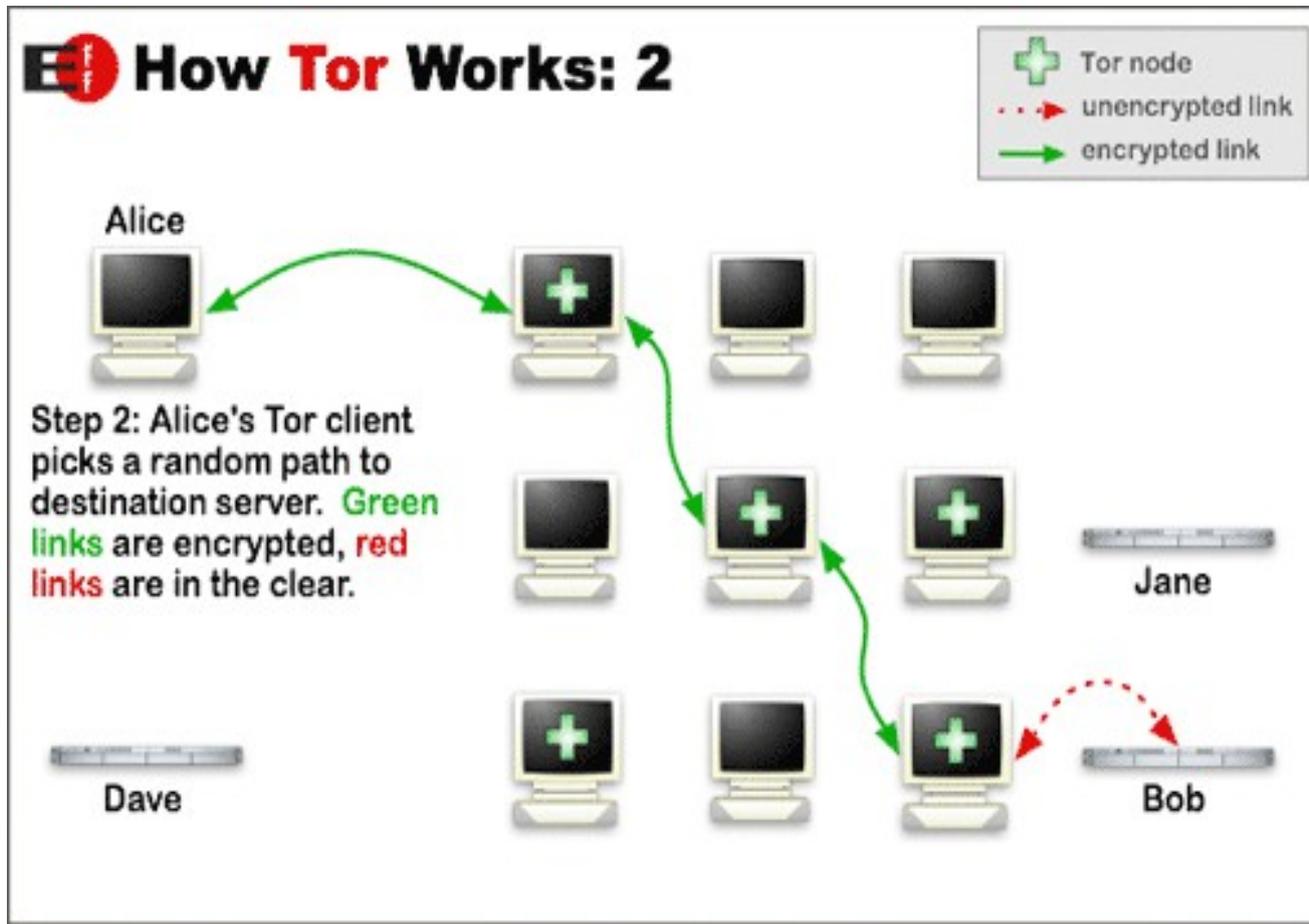
# TOR

## COME FUNZIONA TOR?



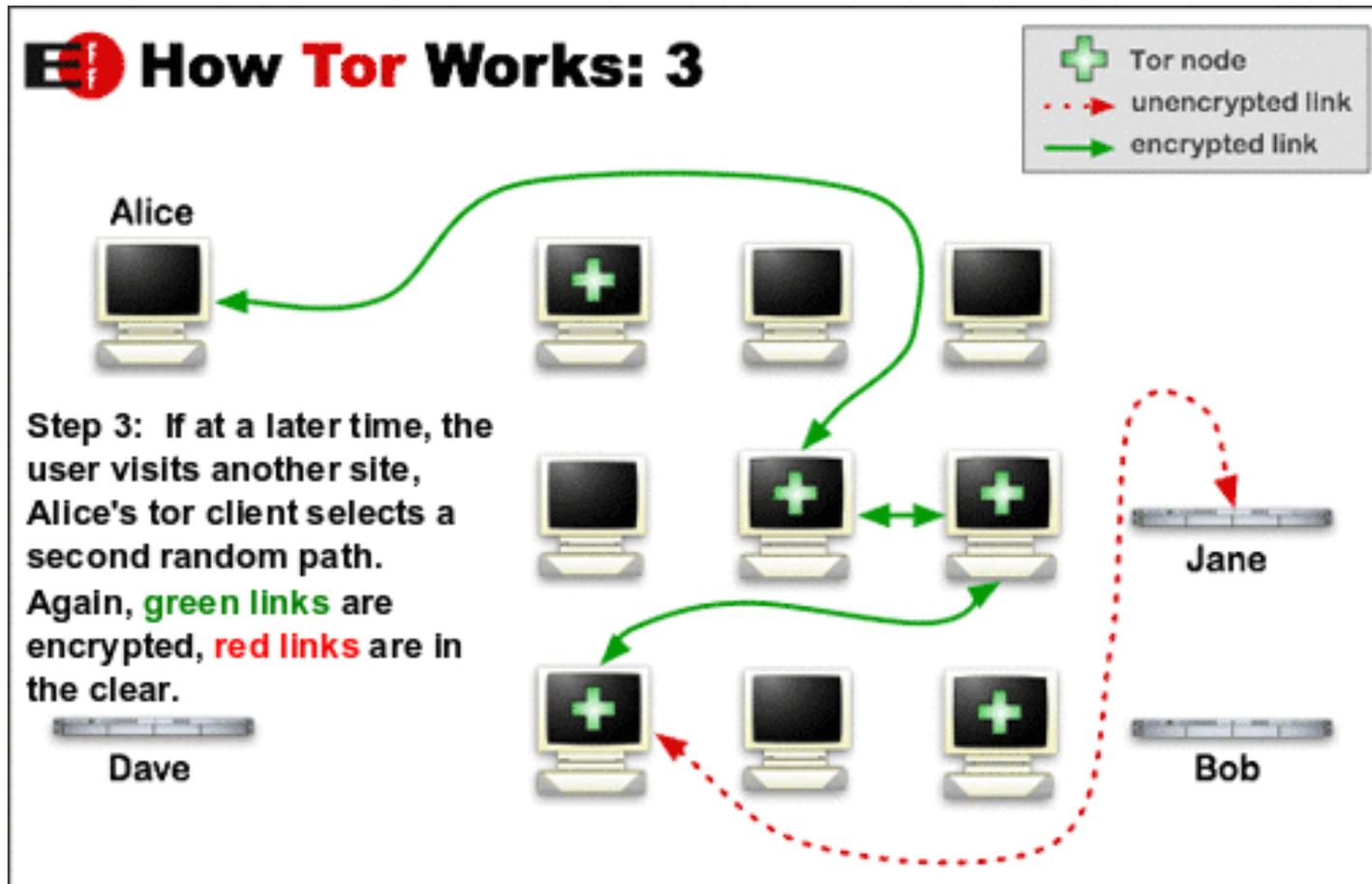
# TOR

## COME FUNZIONA TOR?

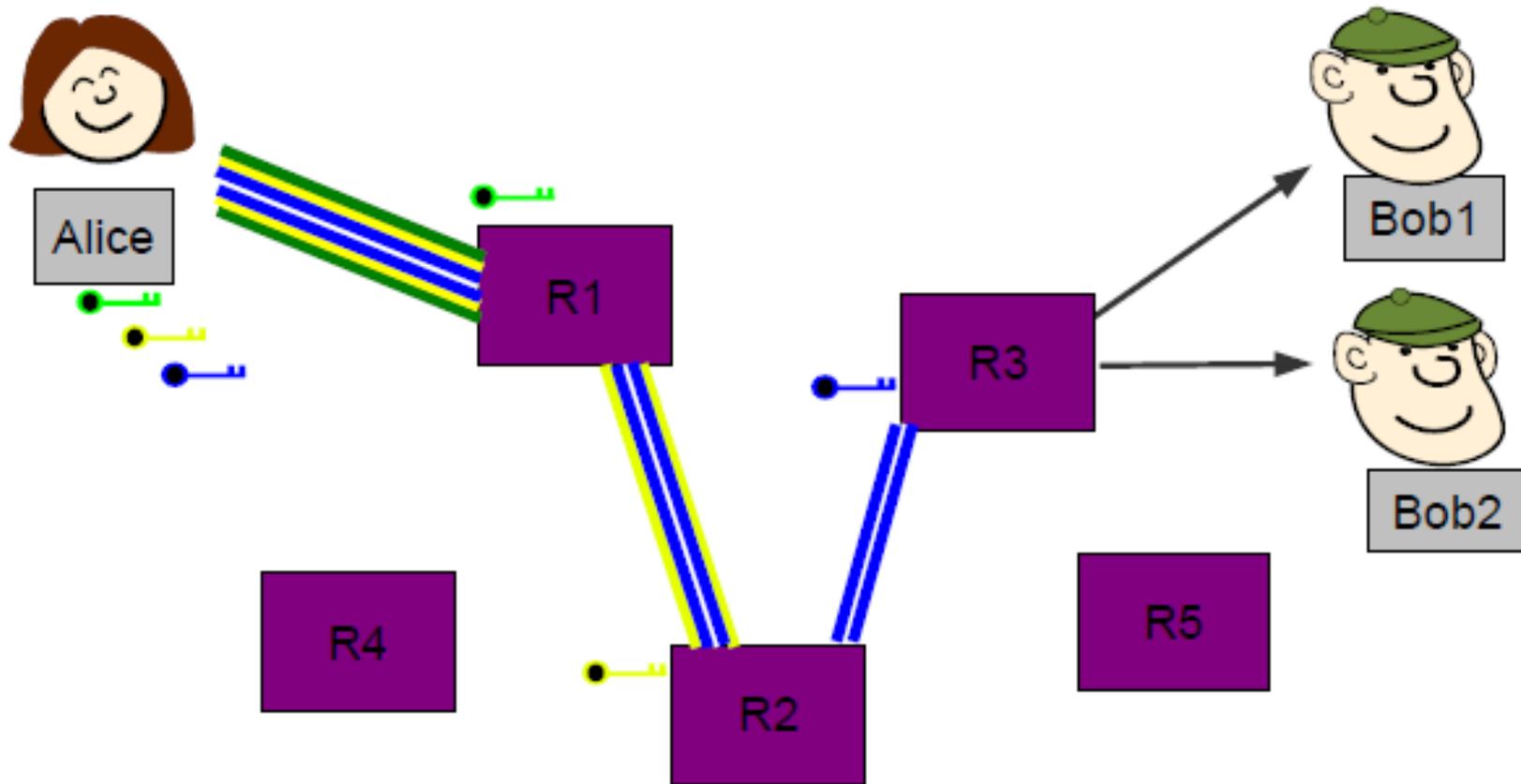


# TOR

## COME FUNZIONA TOR?

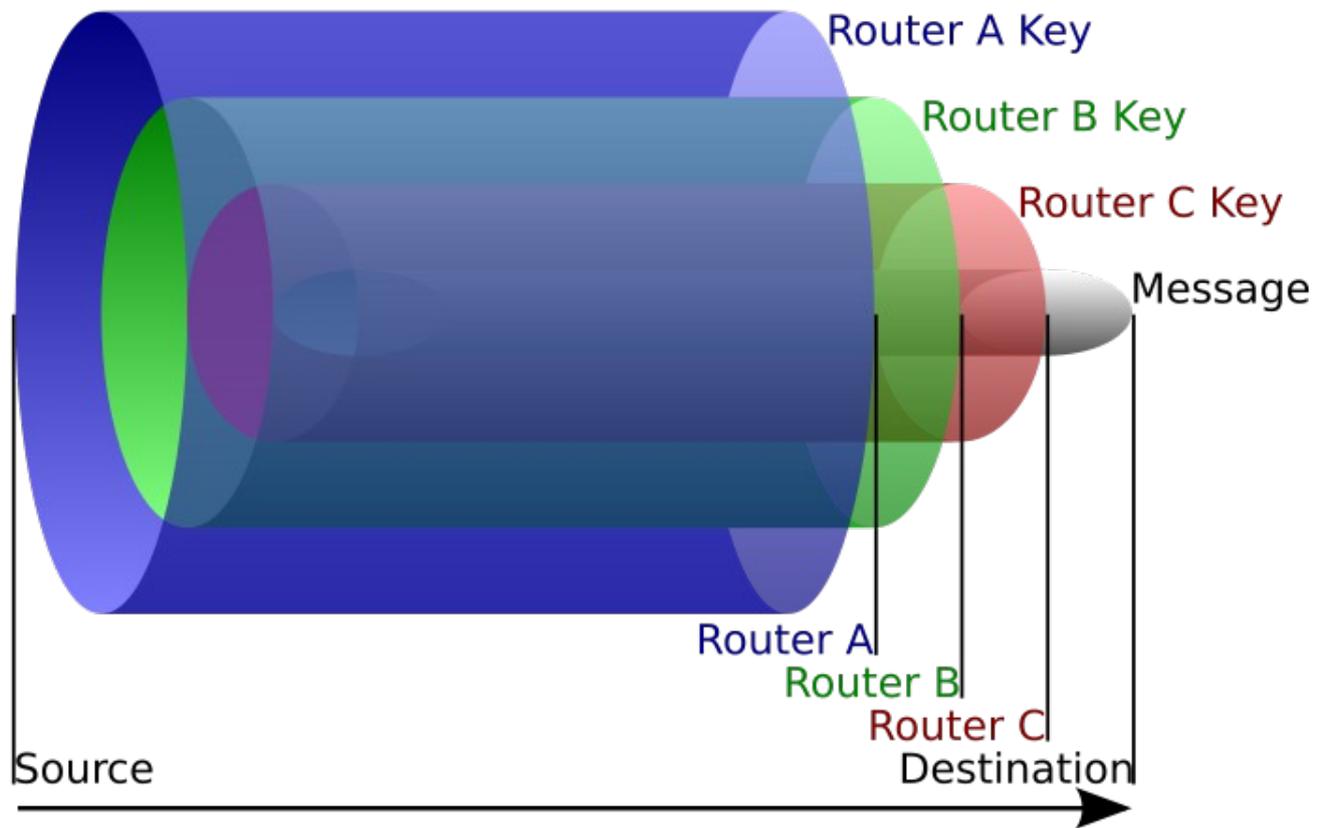


# TOR



# TOR

## COME FUNZIONA TOR?

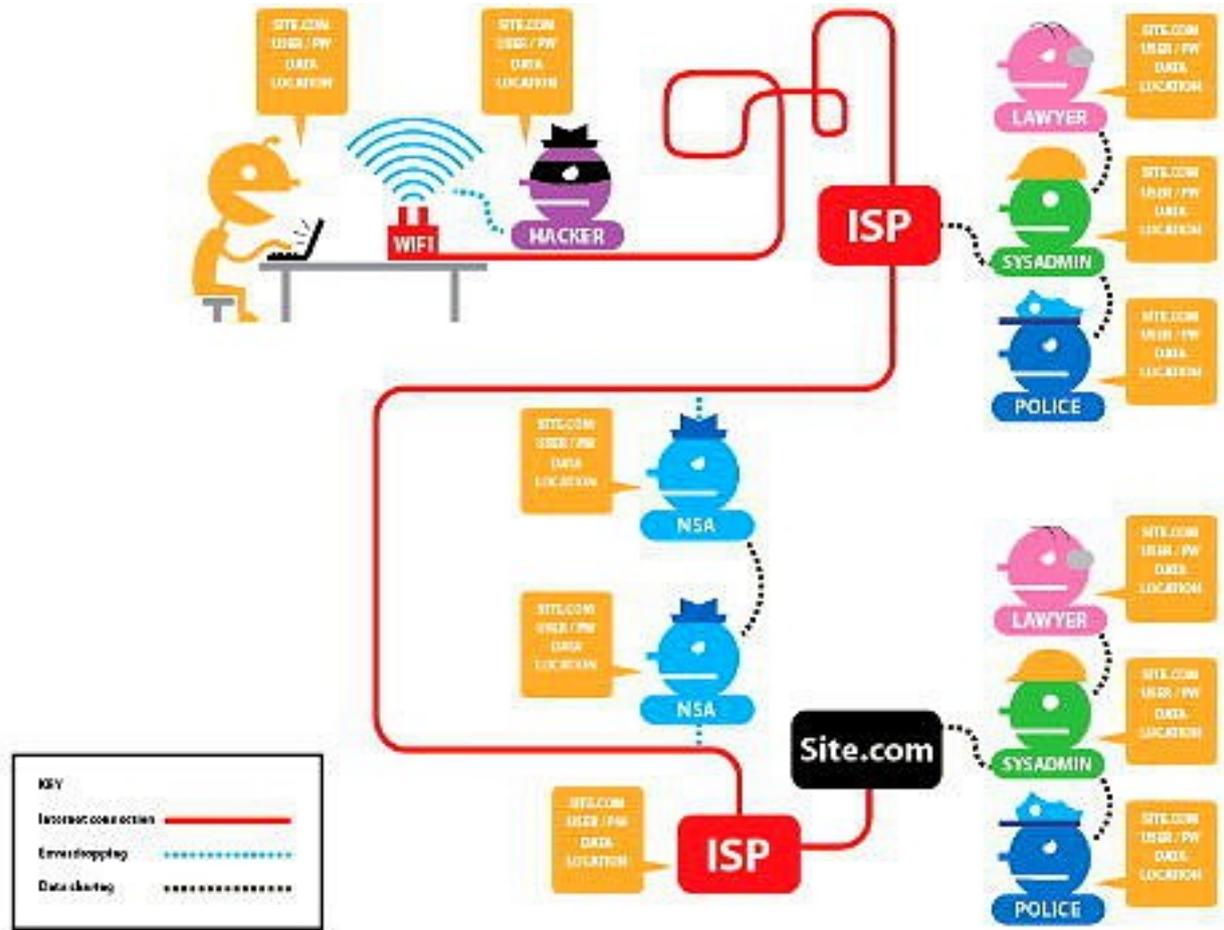


# TOR

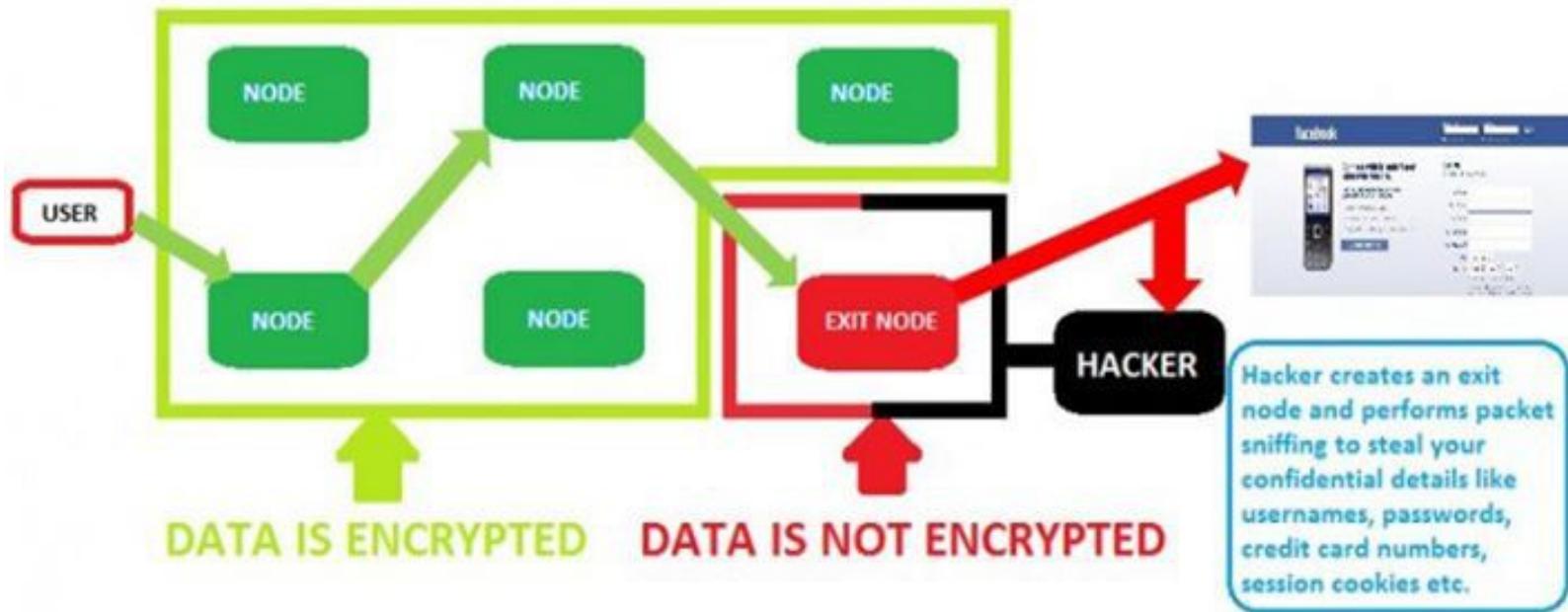
## PUNTI DEBOLI DI TOR?

- NON nasconde l'utilizzo della rete Tor
- NON protegge l'ultima parte della connessione dal router Tor di uscita (exit node) fino al server di destinazione
- NON protegge *il contenuto* delle informazioni trasmesse a meno che non si utilizzi esclusivamente il protocollo httpS
- NON impedisce alle applicazioni di far uscire informazioni rivelatrici attraverso la normale Rete (es. richieste DNS o DNS Leak)
- NON impedisce a contenuti passivi od attivi di rivelare l'identita' del mittente (cookies, javascript, flash, real player, quicktime, doc, pdf,...) su un canale esterno nascosto.

# TOR



# TOR



# TOR

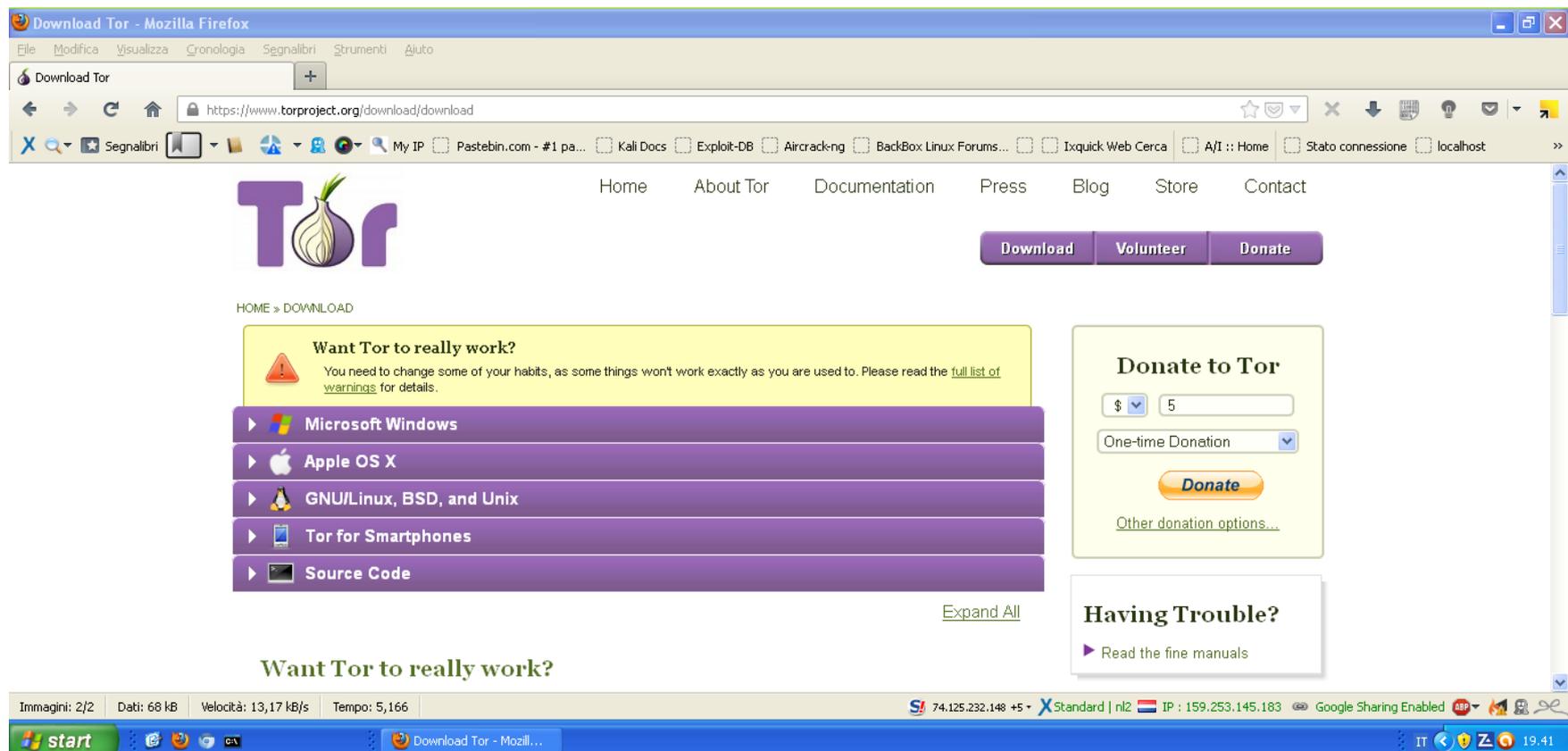
## COME SI USA TOR?

- Ci sono due metodi per navigare attraverso Tor:
  - Configurando il normale browser (Firefox > Preferenze > Avanzate > Rete > Impostazioni > Proxy Socks 127.0.0.1 porta 9050)
  - Servendosi del Tor Browser Bundle (TBB), il metodo raccomandato dal progetto Tor, basato su Firefox e già ottimizzato per il massimo dell'anonimato e per essere pronto all'uso

# Come installare TOR

- Prima di tutto navigare sulla pagina del download

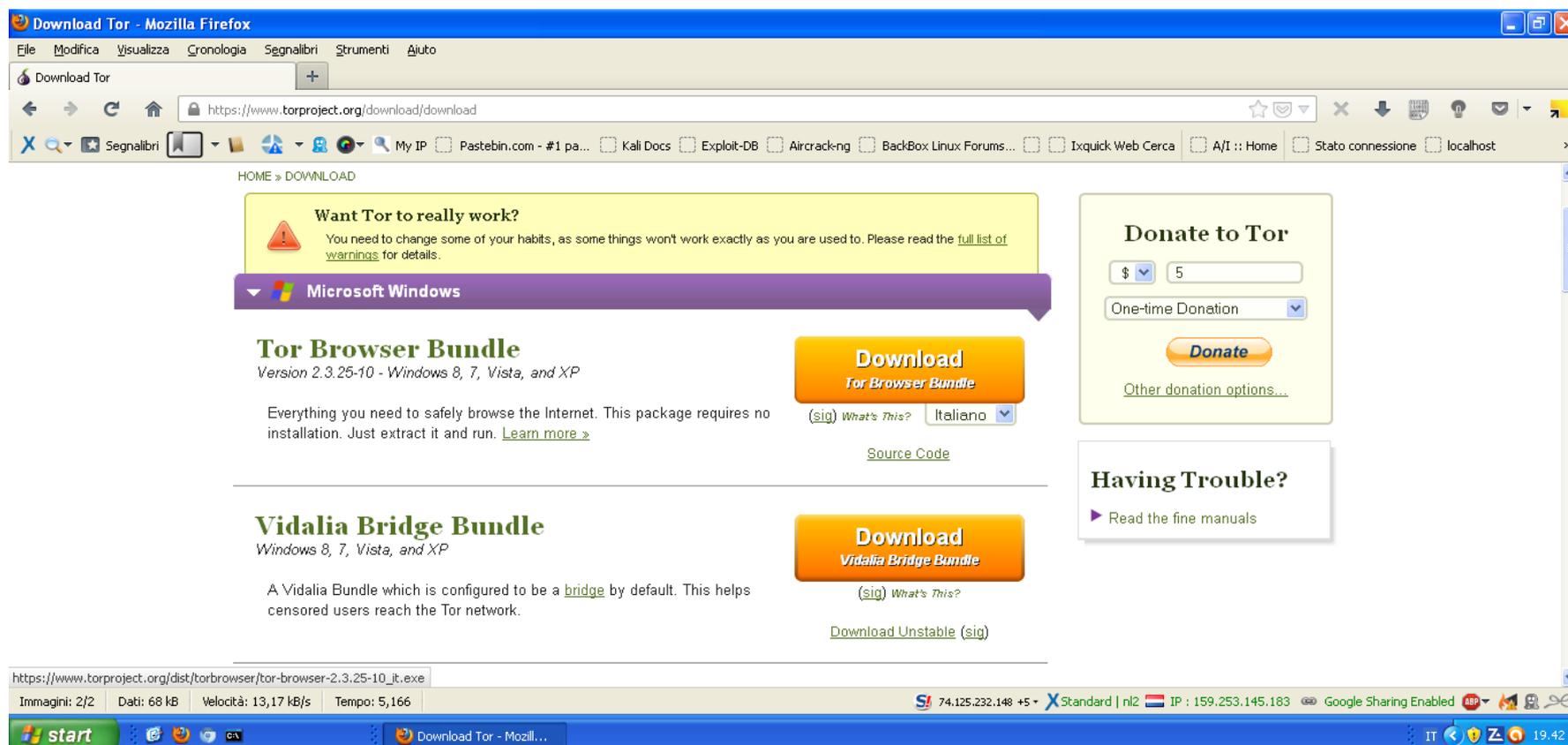
<https://www.torproject.org/download/download>



The screenshot shows a Mozilla Firefox browser window displaying the Tor Project's download page. The address bar shows the URL <https://www.torproject.org/download/download>. The page features the Tor logo (a purple onion) and navigation links: Home, About Tor, Documentation, Press, Blog, Store, and Contact. Below the logo are three buttons: Download, Volunteer, and Donate. A yellow warning box titled "Want Tor to really work?" contains a warning icon and text: "You need to change some of your habits, as some things won't work exactly as you are used to. Please read the [full list of warnings](#) for details." Below this is a list of operating systems with expandable sections: Microsoft Windows, Apple OS X, GNU/Linux, BSD, and Unix, Tor for Smartphones, and Source Code. To the right is a "Donate to Tor" section with a dropdown menu set to "\$ 5", a "One-time Donation" dropdown, and a "Donate" button. Below that is a "Having Trouble?" section with a link to "Read the fine manuals". The browser's status bar at the bottom shows system information like "Immagini: 2/2", "Dati: 68 kB", "Velocità: 13,17 kB/s", and "Tempo: 5,166". The Windows taskbar at the very bottom shows the Start button and several open applications.

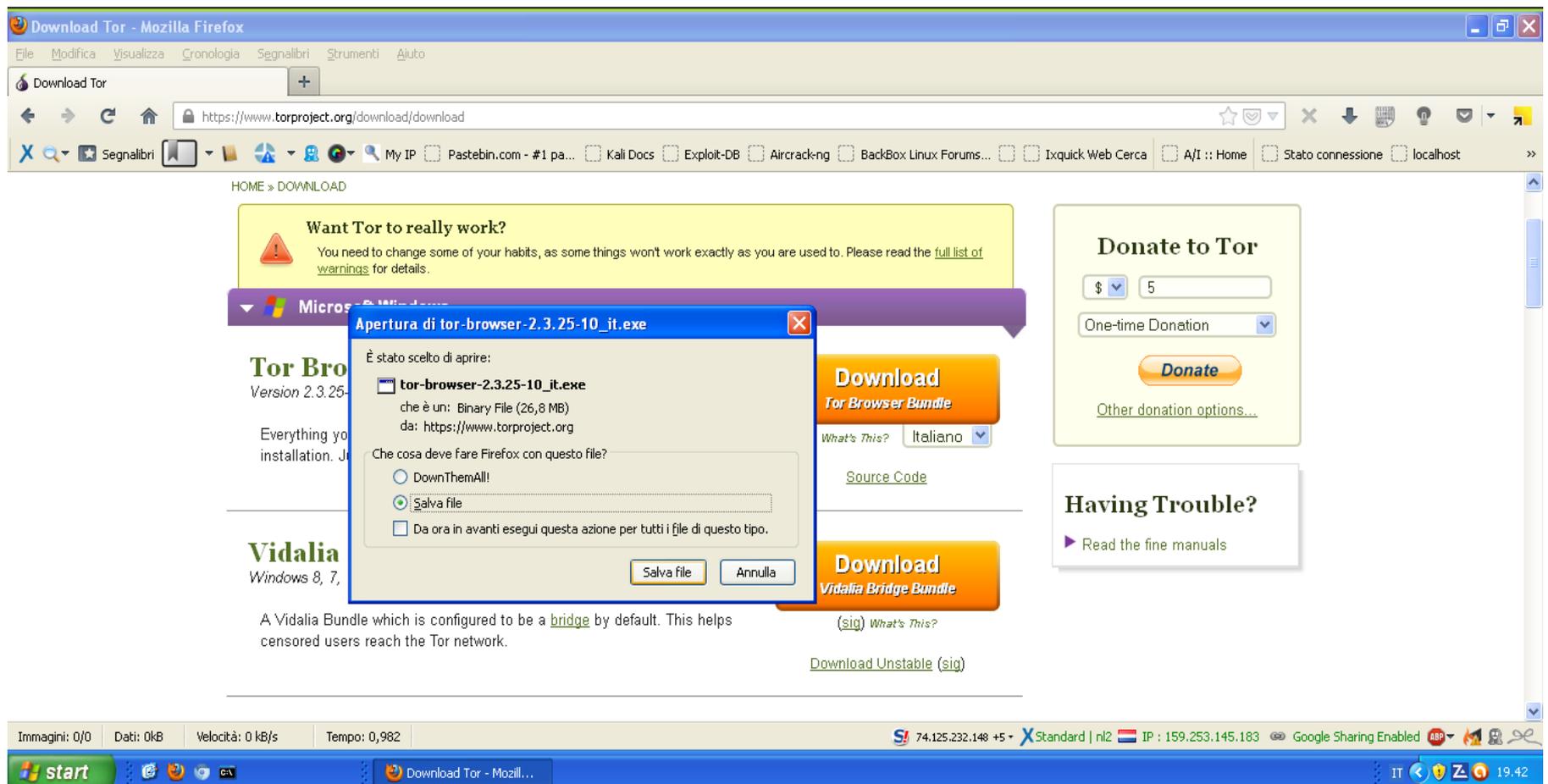
# Come installare TOR

- Scegliere quale versione scaricare in base al proprio sistema operativo e lingua preferita



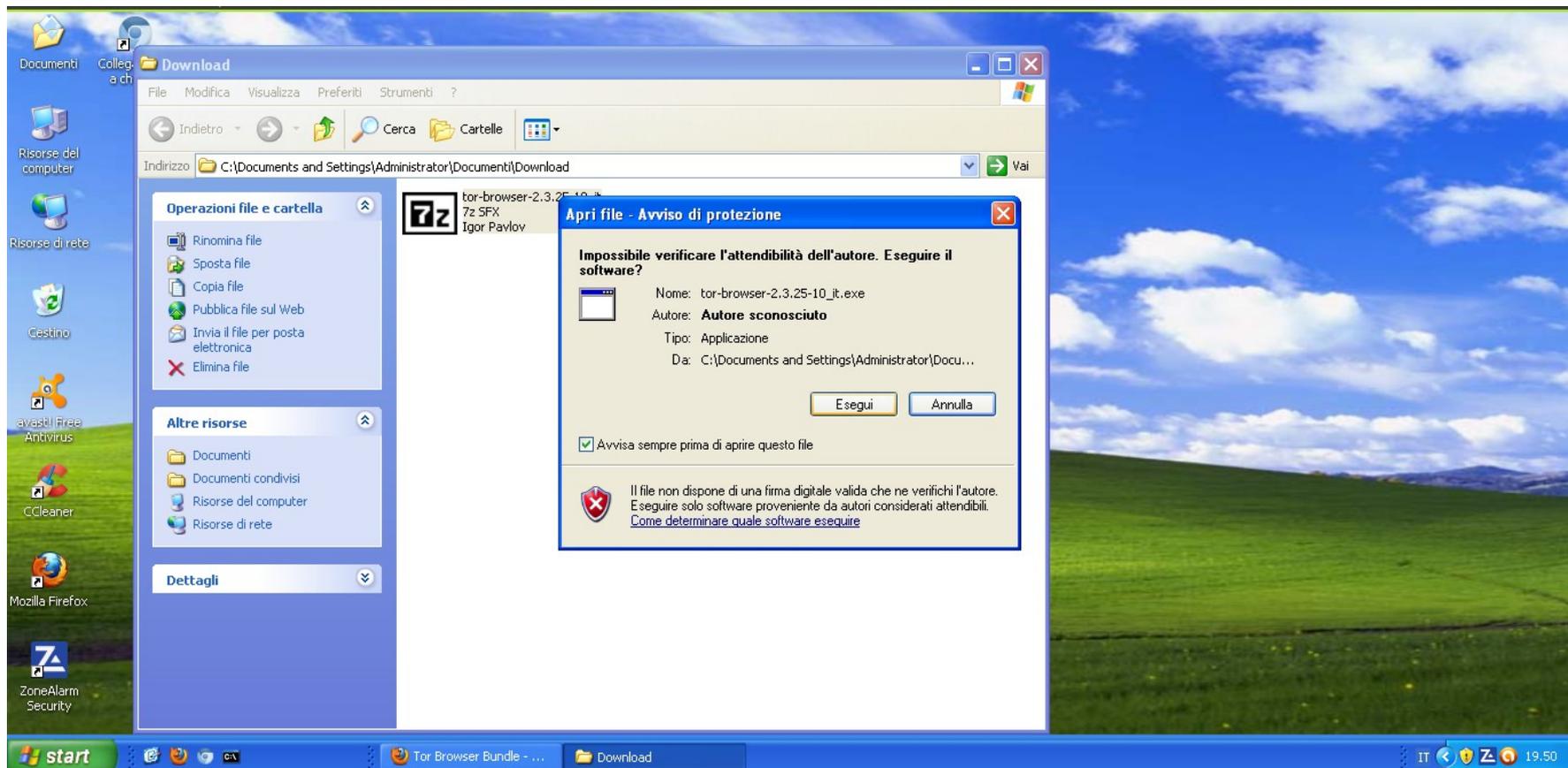
# Come installare TOR

- Salvare il file sul computer



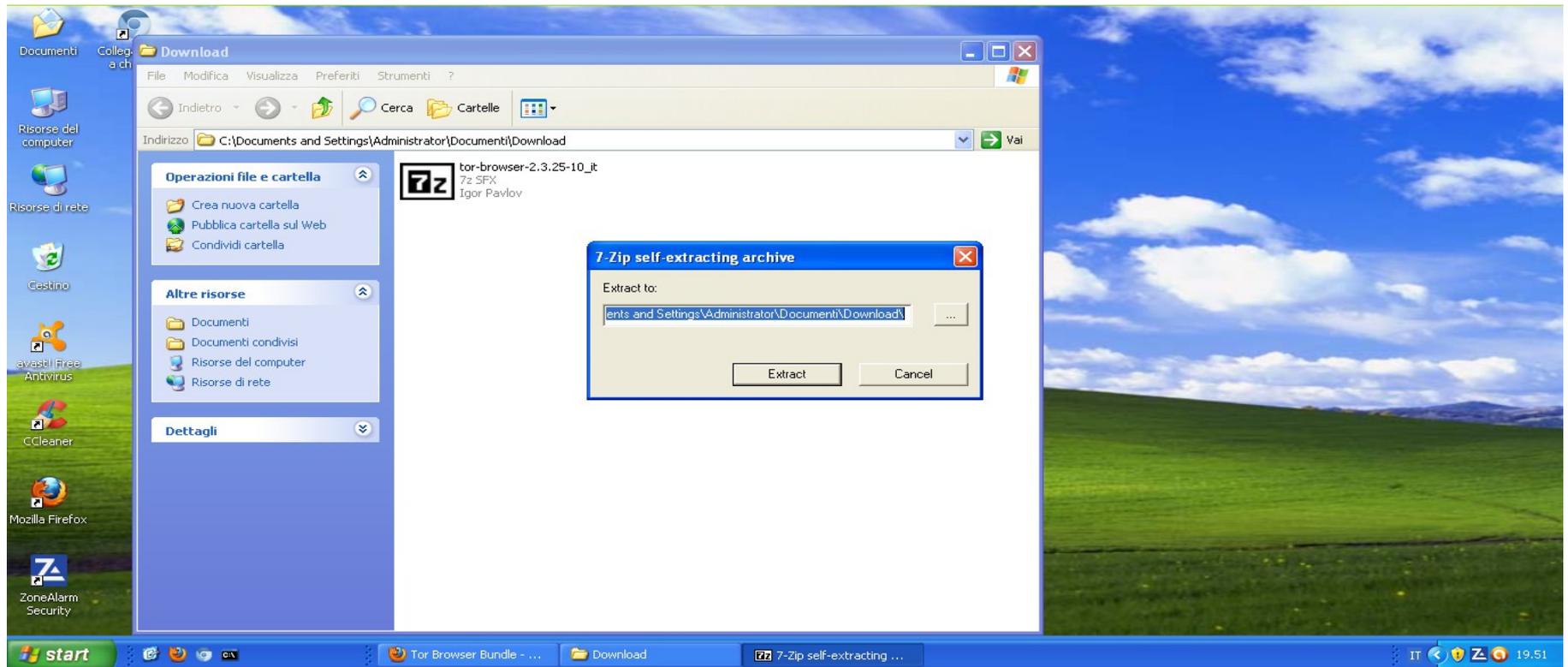
# Come installare TOR

- Una volta salvato, doppio click per eseguire



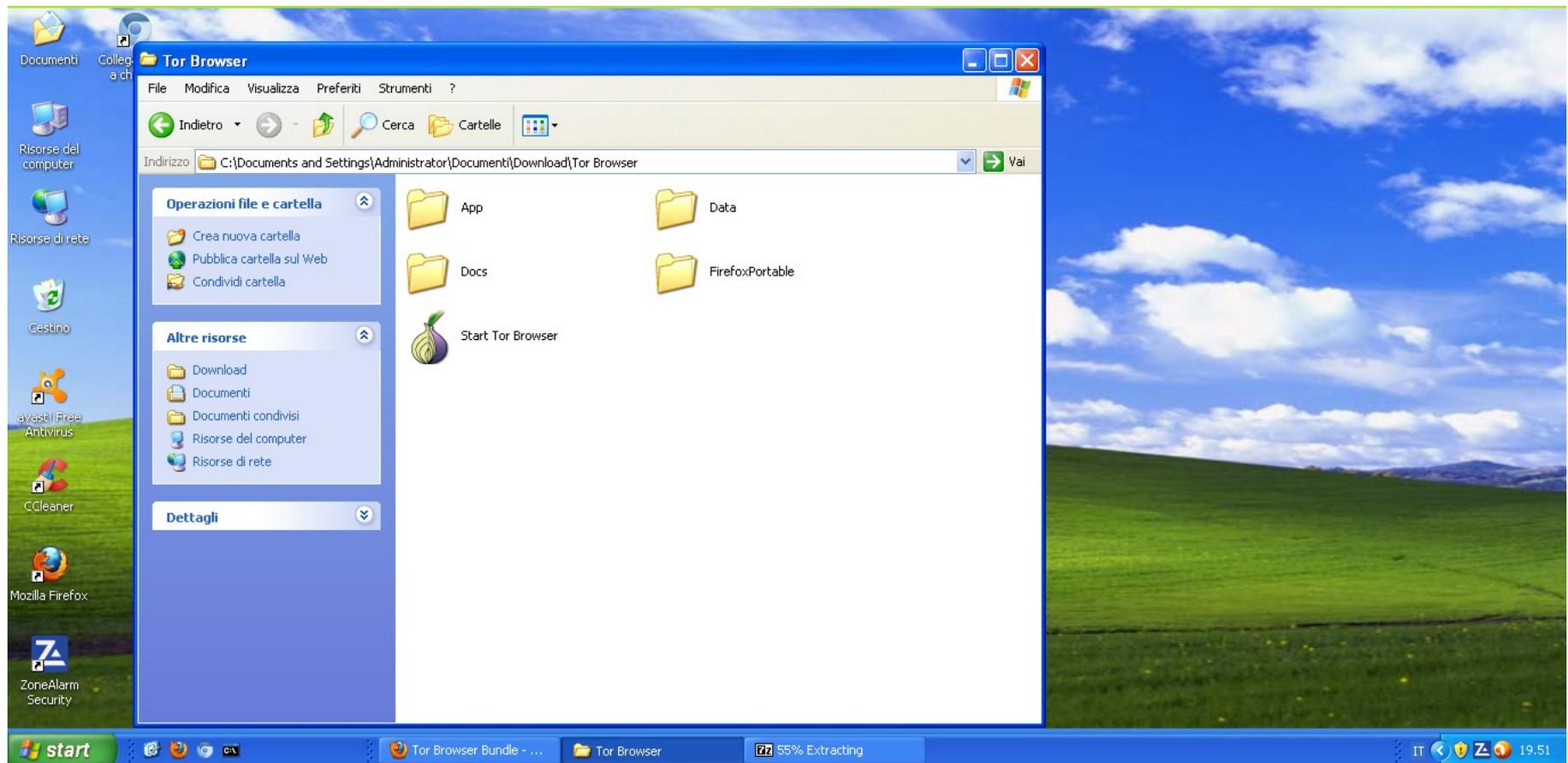
# Come installare TOR

- Verra' chiesto dove estrarre il contenuto, è possibile scegliere una destinazione a piacere, oppure lasciarlo dove lo si è scaricato



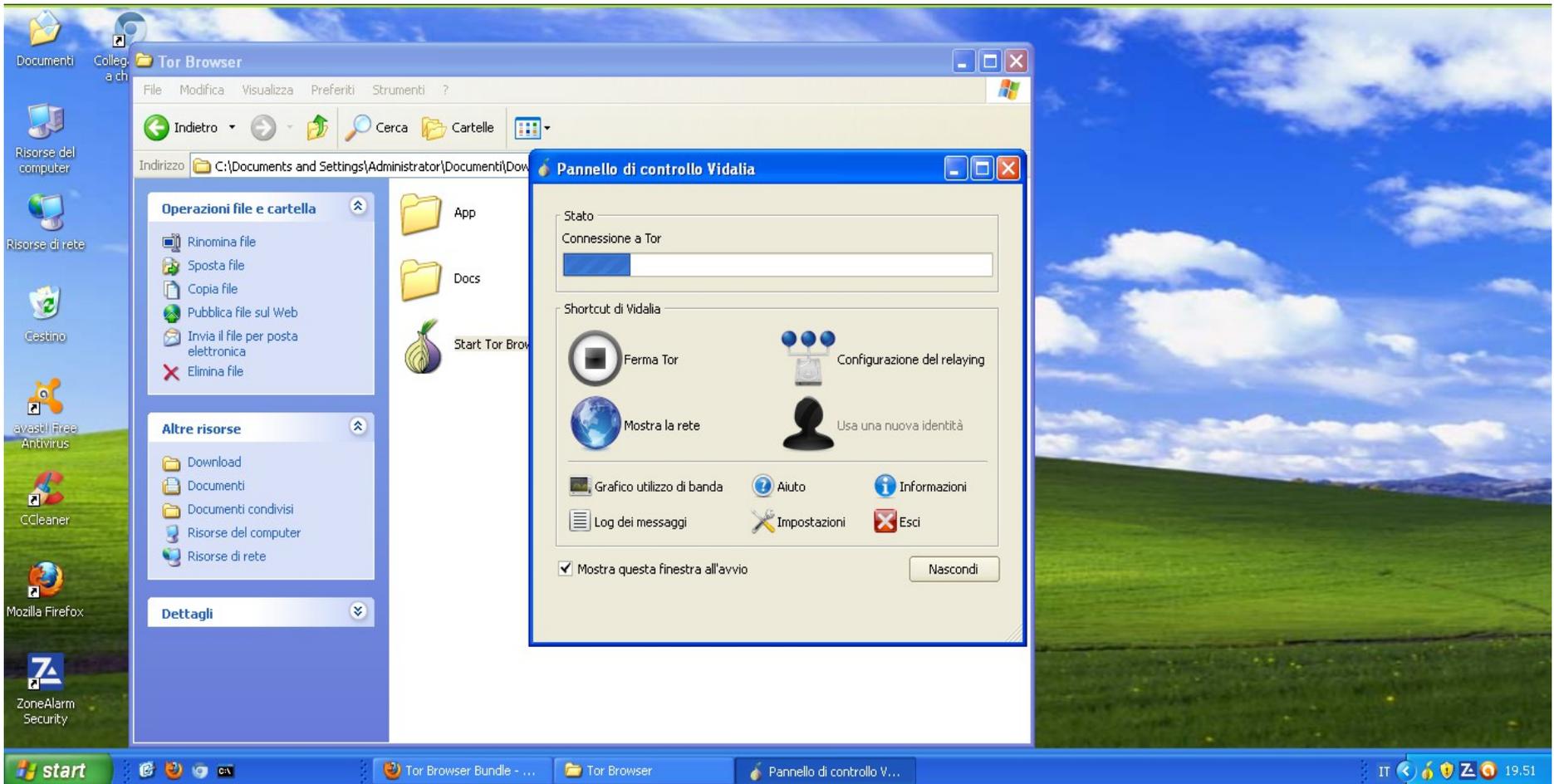
# Come installare TOR

- Questo è il contenuto della cartella appena estratta



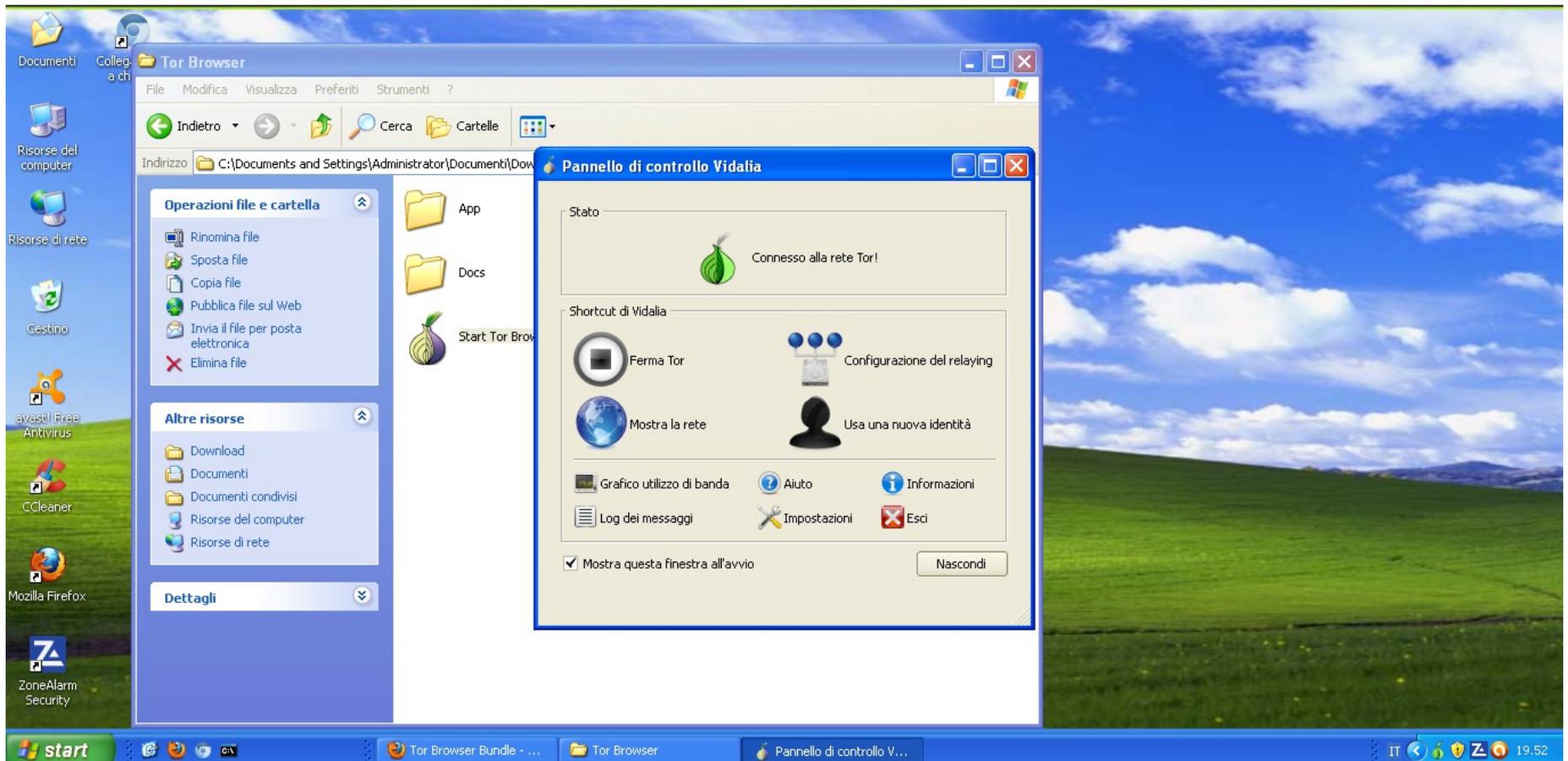
# Come installare TOR

- Non resta che eseguire Vidalia con un doppio click



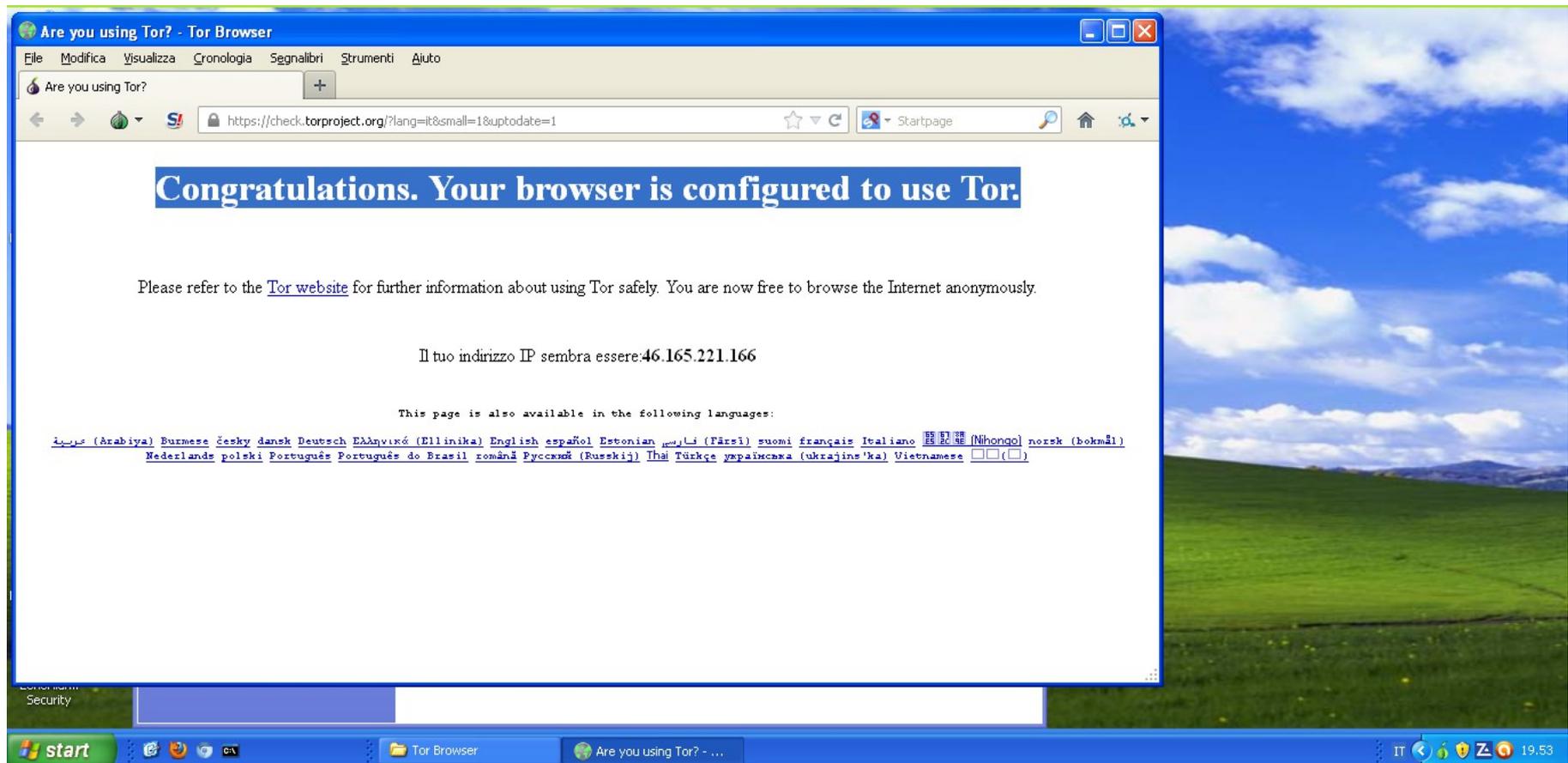
# Come installare TOR

- Attendiamo di essere connessi alla rete Tor



# Come installare TOR

- Automagicamente si avvia Firefox ed effettua un test di corretto funzionamento



# Come installare TOR

- In caso non sia possibile connettersi alla rete Tor, otterremo il seguente messaggio:



# USO AVANZATO DI TOR?

Ospitare un nodo:

- Permette di mantenere viva e neutrale la rete Tor condividendo un po della propria banda
- Il normale client Tor puo' essere configurato per diventare un nodo, senza bisogno di programmi aggiuntivi
- Entry node e nodi intermedi non corrono rischi legali, solo gli exit node

# USO AVANZATO DI TOR?

Bridge:

- Sono entry node “segreti”
- Evitano che la rete Tor venga bloccata dagli ISP tramite *blacklist*
- Vengono pubblicati un poco alla volta su:  
<https://bridges.torproject.org/>

# USO AVANZATO DI TOR?

## Hidden Service:

- Consente di offrire un servizio in modo anonimo, ovvero l'indirizzo IP del *server* rimane nascosto
- E' raggiungibile solamente tramite la rete Tor
- E' identificato da un dominio .onion

# USO AVANZATO DI TOR?

Tor non è la panacea di tutti i mali, certo ci fornisce un buon punto di partenza, ma è essenziale ricordare che da solo non basta se non si prendono in considerazione altri aspetti:

- L'uscita è in chiaro
- Viaggia su TCP, quindi il traffico UDP (es. DNS) “scavalca” la rete Tor
- La sicurezza è un processo che va “mantenuto” e non può essere demandato a terzi, dobbiamo svilupparlo in prima persona

# USO AVANZATO DI TOR?

Uscita in chiaro, come risolvo?

- L'utilizzo di plugin che “forzano” l'utilizzo di HTTPS. Per esempio [https-everywhere](#) è un ottimo plugin!
- Se siete più scafati un tunnel SSH è una buona soluzione
- Se siete scafati ma anche pigri, connettersi a Tor passando per una [VPN](#)

# USO AVANZATO DI TOR?

## Traffico UDP come risolvo?

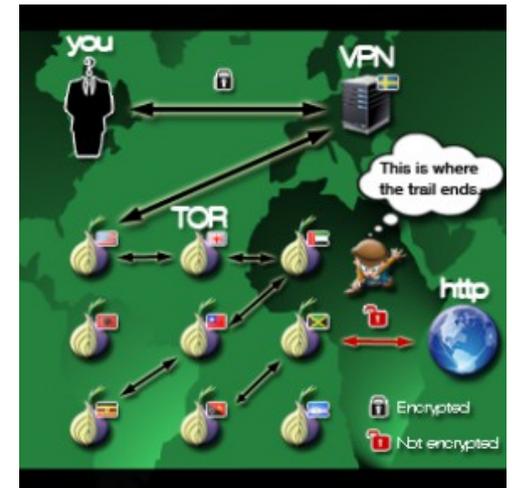
- Come detto prima Tor “torifica” solo il traffico TCP, questo significa che se tento di risolvere qualsiasi indirizzo (es. [www.google.it](http://www.google.it)) la mia richiesta utilizzerà la porta 53 UDP “scavalcando” di fatto il circuito Tor. E quindi? Quindi se non siamo attenti tutti i nostri sforzi per mantenere l'anonimato verranno vanificati; possiamo utilizzare “[Polipo](#)” o “[Privoxy](#)” o “[tor-resolve](#)”. Polipo in particolare è un “DNS proxy cache” ovvero tiene in memoria i siti visitati in modo che non si debba risolvere di nuovo l'indirizzo IP. Ancora una volta la miglior soluzione è l'utilizzo di una VPN.

# USO AVANZATO DI TOR?

## Piccola introduzione VPN

- L'utilizzo di una VPN prima di immettersi nel circuito Tor è forse il processo più “sicuro” da compiere per aumentare il livello di sicurezza e segretezza. Alcuni siti (es. RiseUp.net) mettono a disposizione questo servizio gratuitamente per i propri iscritti.

Nella fattispecie si tratta di OpenVPN, una particolare VPN definita “punto-a-punto” in questo modo viene creata una rete virtuale privata che ci connette direttamente al server VPN e avremo come “punto di uscita” (gateway) proprio uno dei server scelti. In questo modo un ipotetico osservatore vedrebbe arrivare richieste da un server VPN assieme a tutte quelle di altri utenti connessi, oltretutto questa VPN incanala TUTTI i servizi di TUTTE le porte TCP-UDP.



# USO AVANZATO DI TOR?

- La sicurezza come processo continuo, non delegabile a terzi o quarti. Qui non possiamo fare nulla, il vostro “comportamento” in rete dev'essere paragonabile alla vita reale. Possiamo mettervi a disposizione strumenti e risorse ma siete voi in prima persona che dovete mettervi nelle condizioni di non essere rintracciati. Utilizzando con sapienza e cognizione di causa gli strumenti adatti, alzando notevolmente il livello di paranoia, ed evitare di pensare “figurati se vengono da me!” oppure “non capiterà proprio a me!” perchè la risposta è proprio “Sì! Vengono da te!” e “Sì! Capita proprio a te!!”.

*La paranoia è una virtù... -Anon A/I-*

# TOR

## PROGETTI SIMILI A TOR?

- Freenet, i2P, GNUnet, JAP,.....altri?

# TOR



# TOR

## Links (1):

- Anon test:

<http://ip-check.info/?lang=en>

- Test corretto funzionamento Tor:

<https://check.torproject.org/>

- Manuale utente in italiano:

[https://www.torproject.org/dist/manual/short-user-manual\\_it.xhtml](https://www.torproject.org/dist/manual/short-user-manual_it.xhtml)

- Tor & Https – Grafica interattiva:

<https://www.eff.org/pages/tor-and-https>

# TOR

## Links (2):

- Test China firewall (Golden Shield Project):  
<https://en.greatfire.org/>
- Test China/Iran censorship:  
<http://viewdns.info/>
- List of government surveillance projects [en]:  
[https://en.wikipedia.org/wiki/List\\_of\\_government\\_surveillance\\_projects](https://en.wikipedia.org/wiki/List_of_government_surveillance_projects)
- Opt out of PRISM, the NSA's global data surveillance program:  
<http://prism-break.org/>
- Anonymity Bibliography:  
<http://freehaven.net/anonbib/full/date.html>

# TOR

## Links (3):

- Tor FAQ [en]:  
<https://www.torproject.org/docs/faq>
- EFF Self defence [en]:  
<https://ssd.eff.org/tech/tor>
- Archlinux Wiki [en]:  
<https://wiki.archlinux.org/index.php/Tor>
- RiseUp tutorial [en]:  
<https://www.riseup.net/en/tor>
- Tor Privoxy/Polipo Tutorial [en]:  
<http://bodhizazen.net/Tutorials/TOR>

# TOR

## Links (4):

- Tor e VPN/Proxy/SSH [en]:

<https://trac.torproject.org/projects/tor/wiki/doc/TorPlusVPN>

- Torify howto [en]:

<https://trac.torproject.org/projects/tor/wiki/doc/TorifyHOWTO>

- Tor scanner [en]:

<http://eng.xakep.ru/link/51074/>

- Achieving Anonymity with Tor – 5 parti [en]:

<http://resources.infosecinstitute.com/tor-part-2/>

# TOR

## Links (5):

- DNS Leak:

<http://www.dnsleaktest.com>

- DNS Leak Test [en]:

<http://sourceforge.net/p/whonix/wiki/LeakTests/#dns-leak-tests>

- DNS Nameserver Spoofability Test:

<https://www.grc.com/dns/dns.htm>

- Anon test Tools [en]:

<https://trac.torproject.org/projects/tor/wiki/doc/Testing/Tools#Sites>

# TOR

## Links (6):

- Freepto Distro:

<https://we.riseup.net/avana/freepto-docs>

- Tails Distro:

<https://tails.boum.org/>

- Whonix Distro:

<http://sourceforge.net/p/whonix/wiki/Home/#whonix-homepage>

# Credits

- PouL - Politecnico Open unix Labs  
<https://www.poul.org/>
- Progetto Winston Smith  
<https://www.winstonsmith.info>
- Guida pratica per dittatori  
<http://pwd.io/guide>

# Licenza – Some Right Reserved

- Questo documento viene rilasciato sotto licenza Creative Commons 3.0 “Attribuzione – Condividi allo stesso modo (CC-BY-SA)”
- Tu sei libero:
  - di riprodurre, distribuire, comunicare al pubblico, esporre in pubblico, rappresentare, eseguire e recitare quest'opera
  - di modificare quest'opera
  - di usare quest'opera per fini commerciali
- Alle seguenti condizioni:
  - Attribuzione - Devi attribuire la paternità dell'opera nei modi indicati dall'autore o da chi ti ha dato l'opera in licenza e in modo tale da non suggerire che essi avallino te o il modo in cui tu usi l'opera.
  - Condividi allo stesso modo - Se alteri o trasformi quest'opera, o se la usi per crearne un'altra, puoi distribuire l'opera risultante solo con una licenza identica o equivalente a questa.
- Testo integrale <http://creativecommons.org/licenses/by-sa/3.0/it/legalcode>

