

P2P: Anonimato

Matteo Dell'Amico

Master SIIT
4 luglio 2008

Scaletta

- 1 **Introduzione**
 - I motivi dell'anonimato
- 2 **Tor**
 - Onion routing
 - Hidden services
- 3 **Freenet**
 - Le chiavi di Freenet
 - Opennet
 - Darknet

Scaletta

- 1 Introduzione
 - I motivi dell'anonimato
- 2 Tor
 - Onion routing
 - Hidden services
- 3 Freenet
 - Le chiavi di Freenet
 - Opennet
 - Darknet

Anonimato: perché?

"Privacy is dead, get over it."

Scott McNealy, amministratore delegato SUN

"I worry about my child and the Internet all the time, even though she's too young to have logged on yet. Here's what I worry about. I worry that 10 or 15 years from now, she will come to me and say 'Daddy, where were you when they took freedom of the press away from the Internet?'"

Mike Godwin, Electronic Frontier Foundation

Anonimato: perché? (2)

- **Sicurezza e riservatezza** sono entrambe desiderabili, ma è necessario trovare un **compromesso**.
 - il fatto stesso di **indagare** incide sulla privacy.
- L'anonimato può essere necessario per la **libertà di espressione**.

Chi ha bisogno dell'anonimato? (1)

Compete CEO: ISPs Sell Clickstreams For \$5 A Month

posted on: **March 13, 2007**

Font Size: [T](#) [T](#) | [Print](#) | [Email](#)



Henry Blodget

At the Open Data 2007 conference in New York today, David Cancel, the CEO of Compete Inc. revealed that ISPs happily sell clickstream data -- and that it's a big business. They don't sell your name -- just your clicks -- but the clicks are tied to you as a specific user (User 1, User 2, etc.).

How much are your clicks worth? About 40 cents a month per user (per customer)... and the Compete CEO estimates that there are 10-12 big buyers of this data. In other words, your ISP is probably making about \$5 a month (\$60 a year) off your clickstreams.

Someone points out that this is just as bad as the AOL search thing. "It's much worse!" David says -- his excited eyes indicating that he's a happy customer. Someone else observes that "worse" is in the eye of the beholder: for the ISPs it's awesome.

David steps down. Thunderous applause.

Chi ha bisogno dell'anonimato? (2)

A Face Is Exposed for AOL Searcher No. 4417749

By **MICHAEL BARBARO** and **TOM ZELLER Jr.**

Published: August 9, 2008

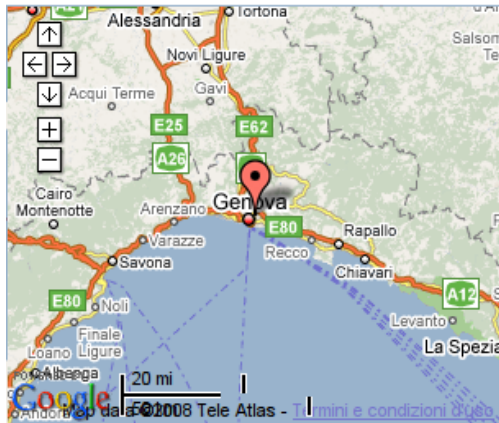
Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.




No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from “numb fingers” to “60 single men” to “dog that urinates on everything.”

And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for “landscapers in Lilburn, Ga,” several people with the last name Arnold and “homes sold in shadow lake subdivision gwinnett county georgia.”

Chi ha bisogno dell'anonimato? (3)

Your IP address is 130.251.61.251(Now detects many [proxy servers](#))

IP Address Location: Genova, 08 Italy 
Please see the [poll](#) for map accuracy.

Tools

[IP Lookup](#) **POPULAR**[Trace Email](#) **NEW!**[Visual Traceroute](#)[Traceroute](#)

Most Frequently Asked Questions

[How do I change my IP address?](#)[How do I hide my IP address?](#)[Is my IP address blacklisted?](#)[Can someone find out who I am?](#)[I've been banned, what do I do?](#)

130.251.61.251

IP Lookup now shows ISP, Org
Connection Type!

Chi ha bisogno dell'anonimato? (4)

```

External IP: 130.251.61.251
  Hostrame: firewall.dsi.unige.it
    Proxy: No Proxy or Invisible Proxy Used
Internal (LAN) IP:
  Outgoing Port: 25848
  Accept Content: text/html, application/xhtml+xml, application/xml;q=0.9, */*;q=0.8
  Accept Char Set: ISO-8859-15, utf-8;q=0.7, */*;q=0.7
  Accept Encoding: gzip, deflate
  Accept Language: it, en;q=0.7, es;q=0.3
  User Agent: Mozilla/5.0 (X11; U; Linux x86_64; it; rv:1.9) Gecko/2008061017 Firefox/3.0
Screen Resolution: 1280 x 800
  Referred From: http://www.torproject.org/torusers.html.it
  Cookies: Enabled
  Browser Plugins: iTunes Application Detector          Default Plugin
                   librhymbox-itms-detection-plugin.so  libnullplugin.so
                   Demo Print Plugin for unix/linux      GCJ Web Browser Plugin
                   libunixprintplugin.so                 gcjwebplugin.so
                   DivX Browser Plug-In                   QuickTime Plug-In 6.0 / 7
                   mplayerplugin-dvx.so                   mplayerplugin-qt.so
  
```

Chi ha bisogno dell'anonimato? (5)

China's Internet Censorship

Sites Focusing on Democracy, Tibet And Taiwan Are Blocked

NEW YORK, Dec. 3, 2002

 E-MAIL STORY

 PRINT STORY

 SPHERE

 SHARE

TEXT SIZE: A A A



(AP)

RELATED

AnswerTips™ enabled ([What's this?](#))

(AP) Internet sites on democracy, Tibet and Taiwan were among Web destinations most frequently blocked by the Chinese government, a study of Chinese online access shows.

Researchers at Harvard Law School's Berkman Center for Internet & Society said Tuesday that other sites blocked included those on health, education, news, entertainment, religion and pornography.

Ben Edelman, a Berkman researcher, and Jonathan Zittrain, the center's co-director, checked more than 204,000 Web sites, identified in part using search engines Google and Yahoo!, and found more than 19,000 inaccessible at least some of the time.

Chi ha bisogno dell'anonimato? (6)



ELECTRONIC FRONTIER FOUNDATION

...e i criminali?

FAQ sugli abusi

Tor può aiutare un criminale a violare la legge?

I criminali possono commettere reati già ora. Dato che sono disposti a infrangere la legge, hanno già a disposizione molti sistemi che forniscono una privacy *migliore* di quella offerta da Tor. Possono rubare telefoni cellulari, usarli e gettarli via; possono penetrare in un computer in Corea o in Brasile e usarlo per delle attività illegali; possono usare gli spyware, i virus e molte altre tecniche per prendere il controllo di milioni di computer Windows in tutto il mondo.

Lo scopo di Tor è dare protezione alle persone normali che rispettano la legge. Per adesso la privacy ce l'hanno soltanto i criminali, e non va bene.

Scaletta

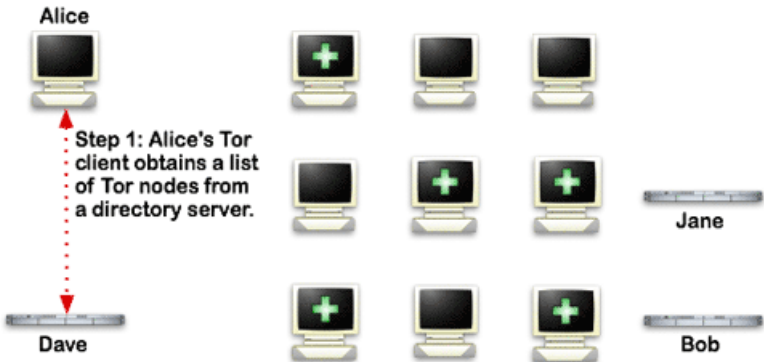
- 1 Introduzione
 - I motivi dell'anonimato
- 2 Tor
 - Onion routing
 - Hidden services
- 3 Freenet
 - Le chiavi di Freenet
 - Opennet
 - Darknet



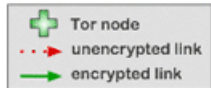
The Onion Router

- Usa il routing “a cipolla” per nascondere la provenienza dei messaggi.
- Nasconde l'indirizzo IP di chi usa il sistema: si limita a proteggere il **trasporto dei dati**.
- È necessario fare in modo che **anche l'applicazione non permetta l'identificazione**.
- Implementato tramite **proxy SOCKS**.
- Progetto finanziato dalla **Marina degli Stati Uniti**.

How Tor Works: 1



How Tor Works: 2



Alice



Step 2: Alice's Tor client picks a random path to destination server. **Green links** are encrypted, **red links** are in the clear.



Dave



Jane



Bob

How Tor Works: 3



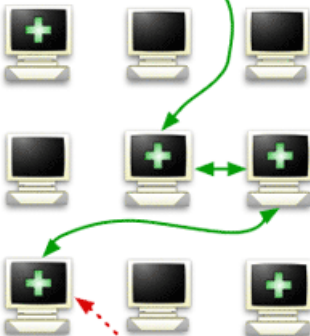
Alice



Step 3: If the user wants access to another site, Alice's Tor client selects a second random path. Again, **green links** are encrypted, **red links** are in the clear.



Dave



Jane



Bob

Come attaccare Tor

- Se si possono osservare i punti di entrata ed uscita del traffico, si può riconoscere che Alice sta comunicando con Bob.
- L'**analisi del traffico** può permettere di capire caratteristiche dei dati inviati **anche se sono cifrati**.

Possibile soluzione

- **Padding**. Invio di informazioni “spazzatura” per non fare capire quando passa il segnale.
 - Estremamente costoso.
 - Difficile da implementare (esempio: HTTP).
- **Non implementato** in TOR.

Come attaccare Tor

- Se si possono osservare i punti di entrata ed uscita del traffico, si può riconoscere che Alice sta comunicando con Bob.
- L'**analisi del traffico** può permettere di capire caratteristiche dei dati inviati **anche se sono cifrati**.

Possibile soluzione

- **Padding**. Invio di informazioni “spazzatura” per non fare capire quando passa il segnale.
 - Estremamente costoso.
 - Difficile da implementare (esempio: HTTP).
- **Non implementato** in TOR.

Entry Guard

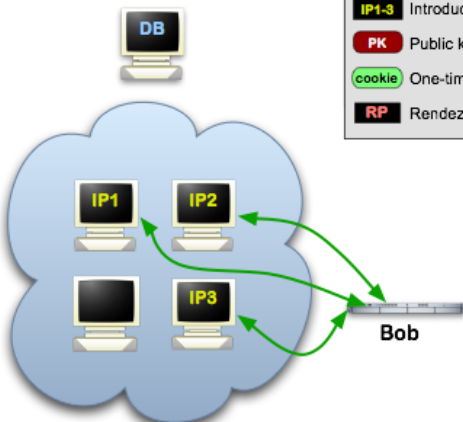
- Per sperare di osservare il punto di entrata, si può creare un nodo TOR e aspettare che Alice ci **chiami**.
- Contromisura: i punti di ingresso sono **un numero limitato**, scelto **all'ingresso nella rete**.







Diventare relay

- Tor è un'applicazione P2P: **chiunque può entrare** a fare parte dei relay.
- **Politiche di uscita** usate per selezionare su che porte inviare informazioni.
- **Migliore anonimato**: l'entry guard non può sapere se le informazioni che richiedi sono per te.

Tor Hidden Services: 1

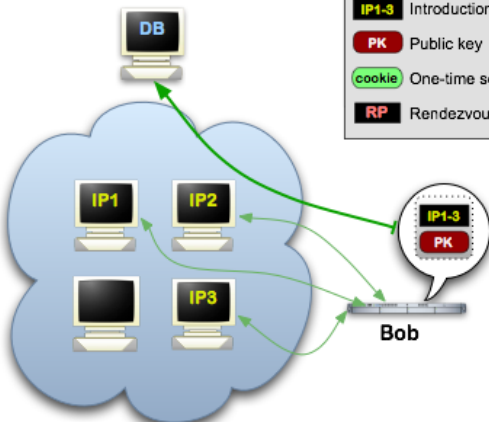
Step 1: Bob picks some introduction points and builds circuits to them.



-  Tor cloud
-  Tor circuit
-  Introduction points
-  Public key
-  One-time secret
-  Rendezvous point

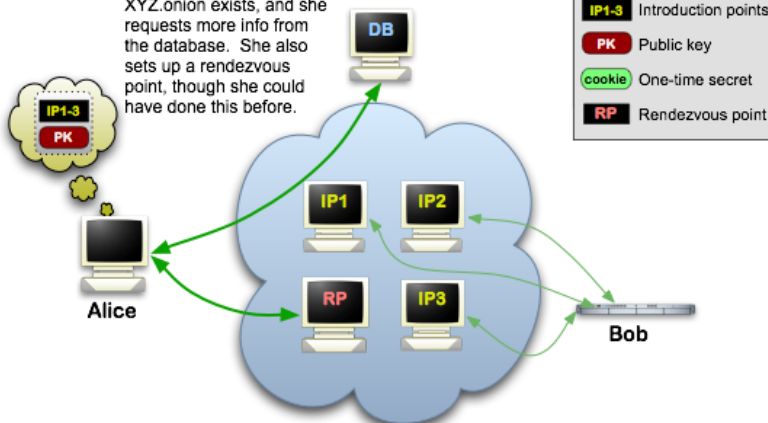
Tor Hidden Services: 2

Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.



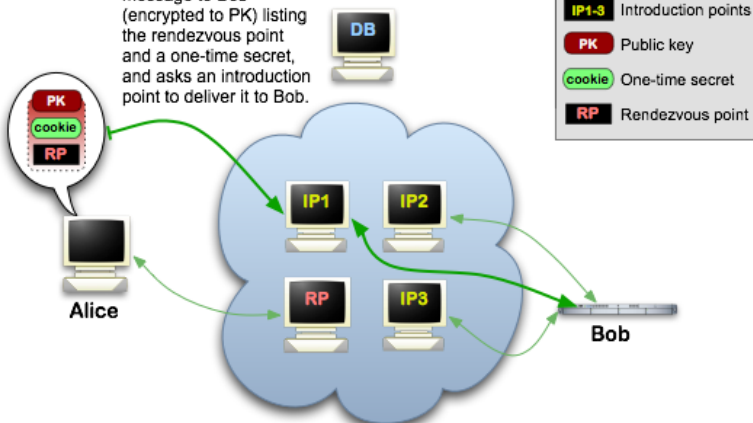
Tor Hidden Services: 3

Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.



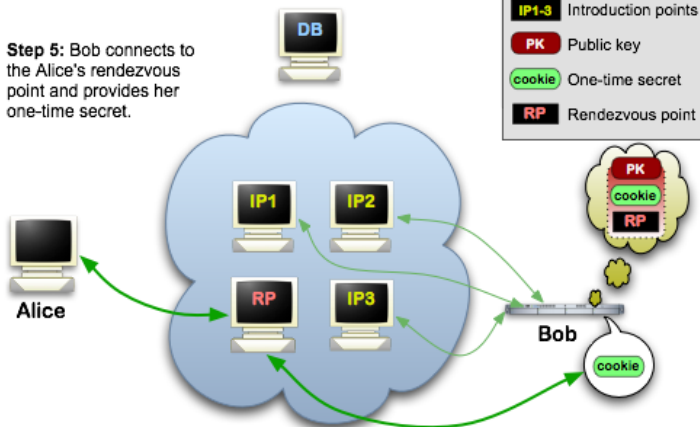
Tor Hidden Services: 4

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.



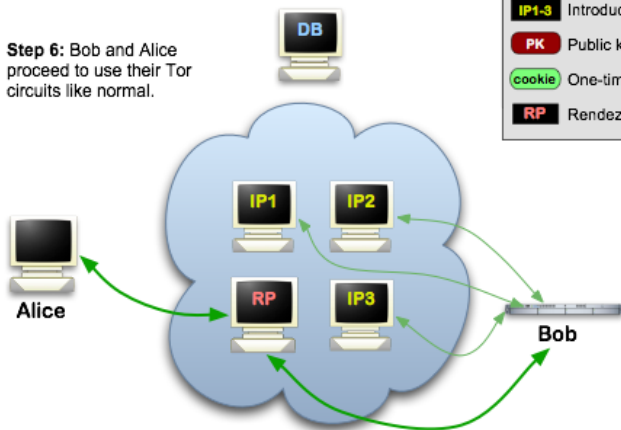
Tor Hidden Services: 5

Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.



Tor Hidden Services: 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.



	Tor cloud
	Tor circuit
	Introduction points
	Public key
	One-time secret
	Rendezvous point

Scaletta

- 1 Introduzione
 - I motivi dell'anonimato
- 2 Tor
 - Onion routing
 - Hidden services
- 3 Freenet
 - Le chiavi di Freenet
 - Opennet
 - Darknet

Freenet



- Rete che, oltre all'anonimato, vuole fornire **resistenza alla censura**.
- **Due overlay**: opennet (non strutturata, "á-la-Gnutella") e Darknet (rete sociale in stile web of trust).
- Principio fondante: quando un documento viene richiesto, viene **copiato sui peer che lo propagano**.
 - L'unico modo per fare scomparire un dato è **non chiederlo**.
- Dati cifrati: i peer possono **non conoscere i dati che possiedono** (*ripudiabilità*).

Immissione del contenuto

- Funziona analogamente ad una query: i nuovi dati vengono copiati su tutti i nodi raggiunti dalla richiesta.
- Il routing della query dipende dall'overlay usato: vedremo.

Content Hash Key

- Mantengono (pezzi di) file con contenuto statico.
- Riconosciute tramite un hash del contenuto.
- Formato: `CHK @ file hash , decryption key , crypto settings`.
- Identificatore per chi immagazzina il file: solo l'hash.

```
CHK @ SVbD9~HM5nzf3AX4yFCBc-A4dhNUF5DPJZLL5NX5Brs ,  
bA7qLNJR7IXRKn6uS5PAySjIM6azPFvK~18kSi6bbNQ , AAEA--8
```

- Si accede tramite il browser all'indirizzo
`http://localhost:8888/CHK@SVbD9~...`

Updateable Subspace Key

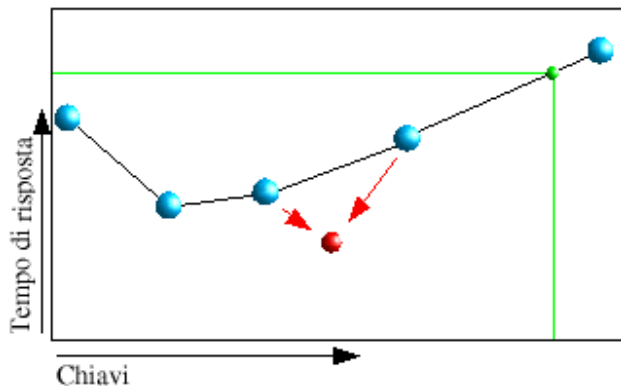
- Per contenuto aggiornabile.
- Formato: USK @ *public key hash* , *decryption key* , *crypto settings* / *user selected name* / *number* /.
- La chiave pubblica è (non cifrata) nel file.
- Identificatore per chi immagazzina il file: hash di chiave pubblica, nome e numero.
- Quando il documento viene richiesto, Freenet cerca automaticamente la versione *number*, o più recente.

Opennet

- Rete non strutturata, dove i nodi si collegano come in Gnutella.
- Le richieste seguono un “cammino casuale” all’inizio, poi i nodi cominciano a specializzarsi.
- Più un nodo “conosce bene” una parte dello spazio di hashing, più i vicini gli chiederanno di quella parte.
- Circolo virtuoso: questo porta a migliorare ancora la specializzazione.

Opennet: catalogare i vicini

Stima del tempo di risposta



La darknet

- Nella darknet di Freenet, i nodi scambiano dati **solo con persone fidate**: l'overlay può essere visto come una “web of trust”.
- Non è possibile sapere con certezza neppure che **sto usando Freenet**: i miei amici non divulgano il mio IP, e un osservatore vedrebbe solo traffico cifrato.

Routing sulla darknet

- Nodi disposti su un anello... come per Chord.
- Ogni nodo entra con un identificatore a caso.
- Nessun link a predecessore e successore: il routing non è garantito.
- I nodi, quando entrano in contatto, verificano le loro posizioni: se scambiarsi identificatore li porta più vicino ai loro amici, lo fanno.

Per saperne di più

- **Tor:** <https://www.torproject.org/>
- **Freenet:** <http://freenetproject.org/>