E-Privacy 2006
19,20 Maggio
Palazzo Vecchio, Firenze

Metro Olografix
http://www.olografix.org

Anonimato in rete con TOR

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org - Key ID: 0x08467AFC

Sommario

- Introduzione
  - Anonimato in rete, perché?
  - L'analisi del traffico
- TOR
  - Introduzione
  - Funzionamento
  - installazione

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

Anonimato in rete, perché?

Situazione: da un client vogliamo connetterci ad un sito internet remoto

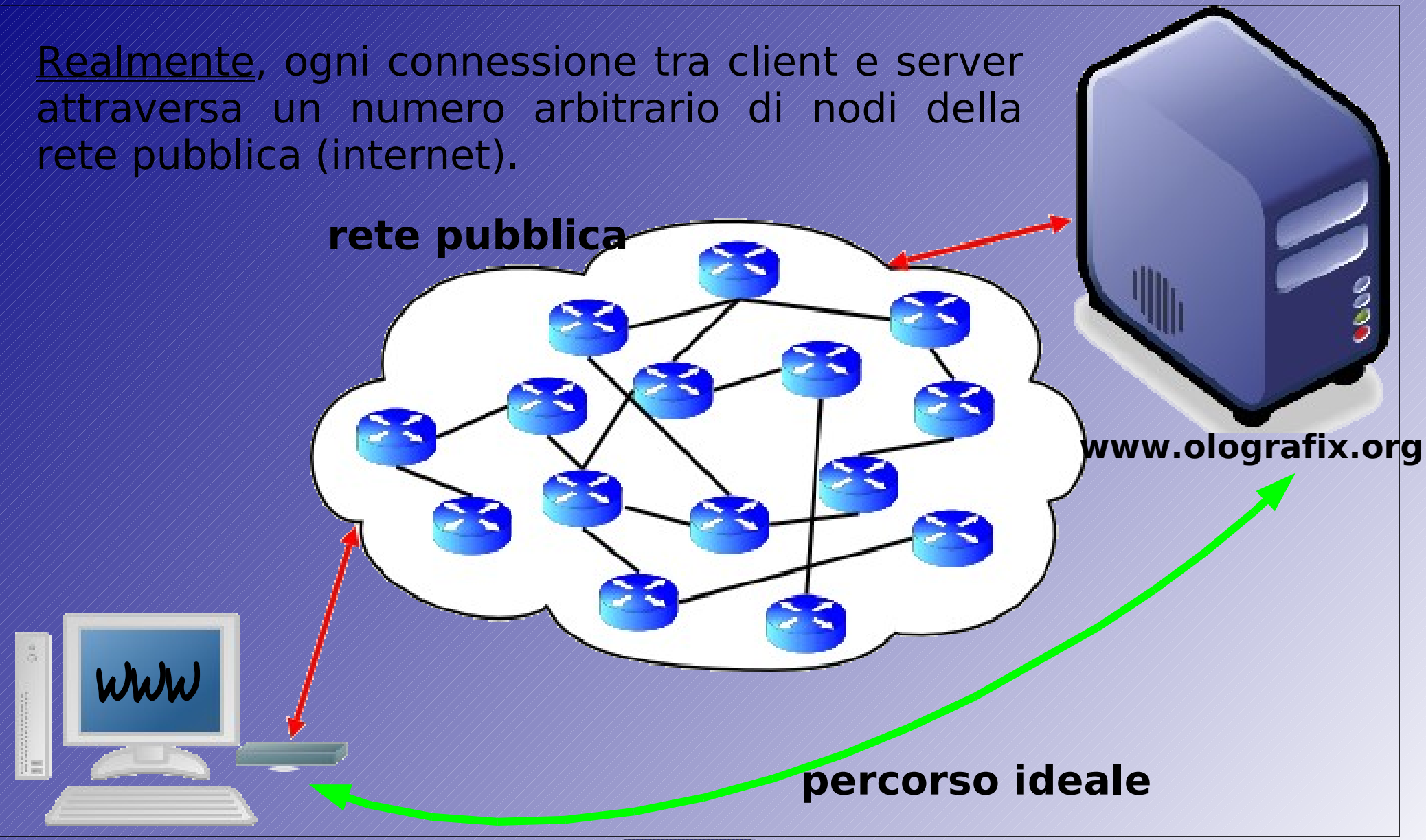
Idealmente la connesione dovrebbe avvenire direttamente tra il client e il server.

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

Anonimato in rete, perché?

Realmente, ogni connessione tra client e server attraversa un numero arbitrario di nodi della rete pubblica (internet).

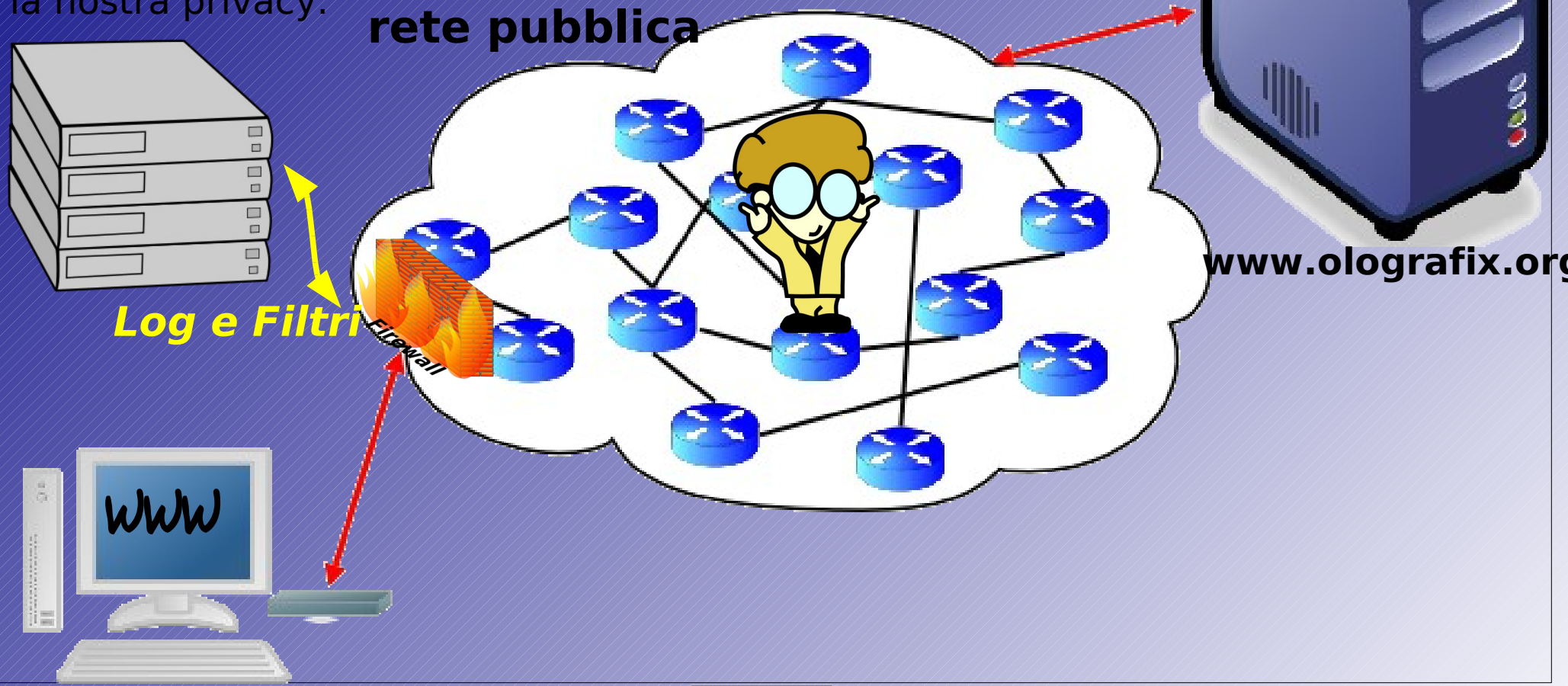


Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

Anonimato in rete, perché?

In uno qualsiasi di questi nodi l'uomo nel mezzo potrebbe intercettare la comunicazione.
Inoltre, la profilazione fatta dai siti web, le analisi del traffico effettuate dagli ISP (e autorizzate) o le intercettazioni locali che controllano il traffico dei dati sono una seria minaccia per la nostra privacy.



Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

Anonimato in rete con TOR
L'analisi del traffico

L'analisi del traffico può essere utilizzata per capire chi sta parlando con chi in una rete pubblica.
I pacchetti dati di internet sono divisi in due parti:

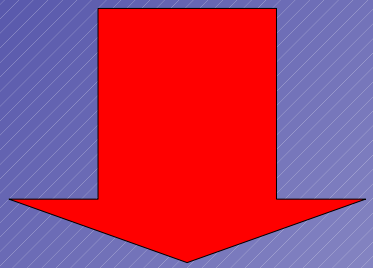
Il blocco dati contiene le informazioni che vogliamo trasmettere e può anche essere crittato, l'intestazione viene utilizzata per l'instradamento dei pacchetti e indica mittente e destinatario della comunicazione (oltre a dimensione e tempi).
L'analisi del traffico si concentra proprio sul blocco intestazione e permette di rilevare ciò che stiamo facendo. Ciò è molto importante perché permette di ricostruire le nostre abitudini e i nostri interessi personali, le nostre preferenze.

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

L'analisi del traffico

L'analisi del traffico permette, a chi la applica, di:
- conoscere le nostre abitudini
- applicare restrizioni sui siti a cui possiamo accedere



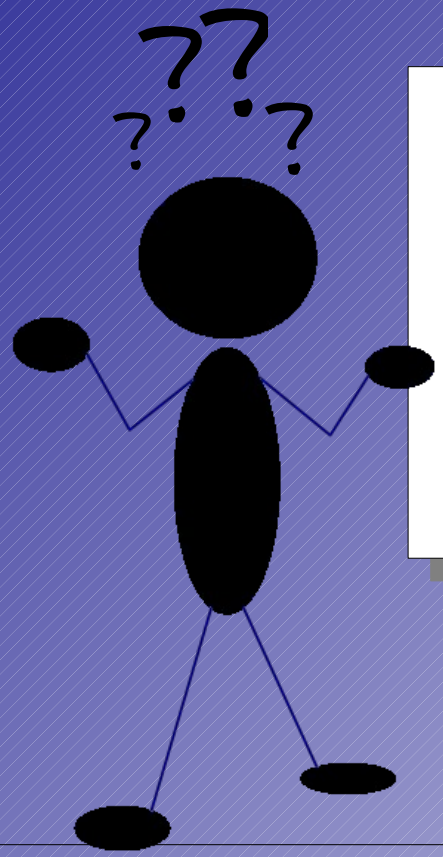
È IN DEFINITIVA UNA VIOLAZIONE DELLA NOSTRA PRIVACY E CONSENTE UNA LIMITAZIONE DELLE NOSTRE LIBERTÀ

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

Anonimato in rete con TOR
TOR: introduzione

Difendersi dall'analisi del traffico richiederebbe nascondere l'intestazione dei pacchetti riguardanti le nostre comunicazioni. Ma la cosa non è fattibile perché toglierebbe al pacchetto un'informazione essenziale: *"da dove vengo e dove sono diretto?"*.



MITTENTE

*#?**#*#

DESTINAZIONE

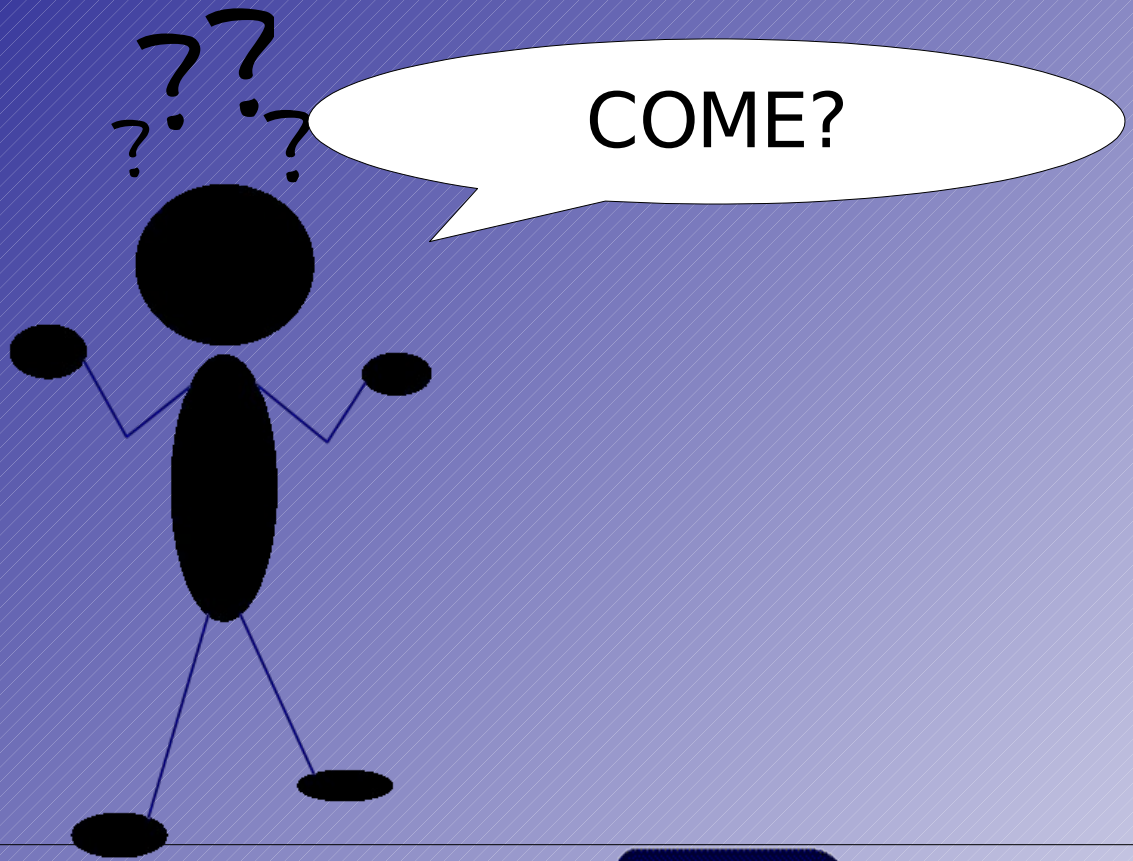
**?!##*#*?#

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

Anonimato in rete con TOR
TOR: introduzione

TOR consente di nascondere mittente e destinatario di ogni pacchetto, mantenendo possibile la connessione.



Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

TOR: funzionamento

Distribuire transazioni attraverso molti nodi della rete Internet, in modo che nessun singolo punto possa collegare una transazione alla sua destinazione.

- I pacchetti prendono un percorso casuale attraverso molti server che ne coprono le tracce
- Nessun server deve conoscere il percorso completo del pacchetto
- Il circuito di connessioni deve essere crittato
- Il circuito di connessioni va modificato periodicamente per evitare analisi statistiche

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

Anonimato in rete con TOR
TOR: funzionamento

CIFRATURA A CHIAVE PUBBLICA (o ASIMMETRICA)

Testo in chiaro (messaggio) → **CIFRARIO** → Testo cifrato (crittogramma) → **CIFRARIO** → Testo in chiaro (messaggio)

Chiave pubblica

Chiave privata

Pensato nel 1976 da Diffie ed Hellmann e poi applicato nel 1977 da Ron Rivest e con l'aiuto di altri due matematici del MIT l'israeliano Adi Shamir, e Leonard Adleman definendo l'RSA (acr. Rivest, Shamir, Adleman)

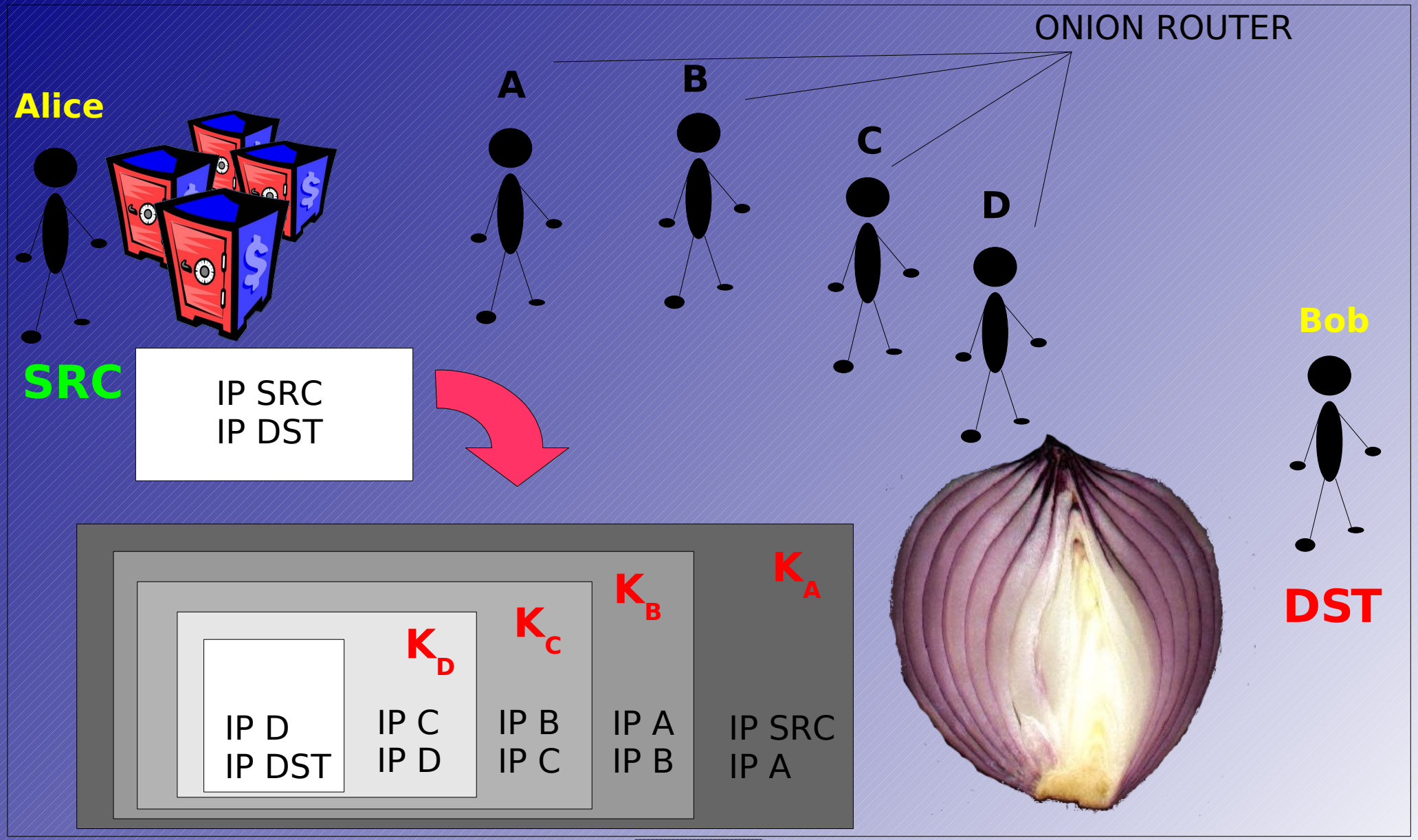
CHIAVE PUBBLICA

CHIAVE PRIVATA

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

Anonimato in rete con TOR
TOR: funzionamento

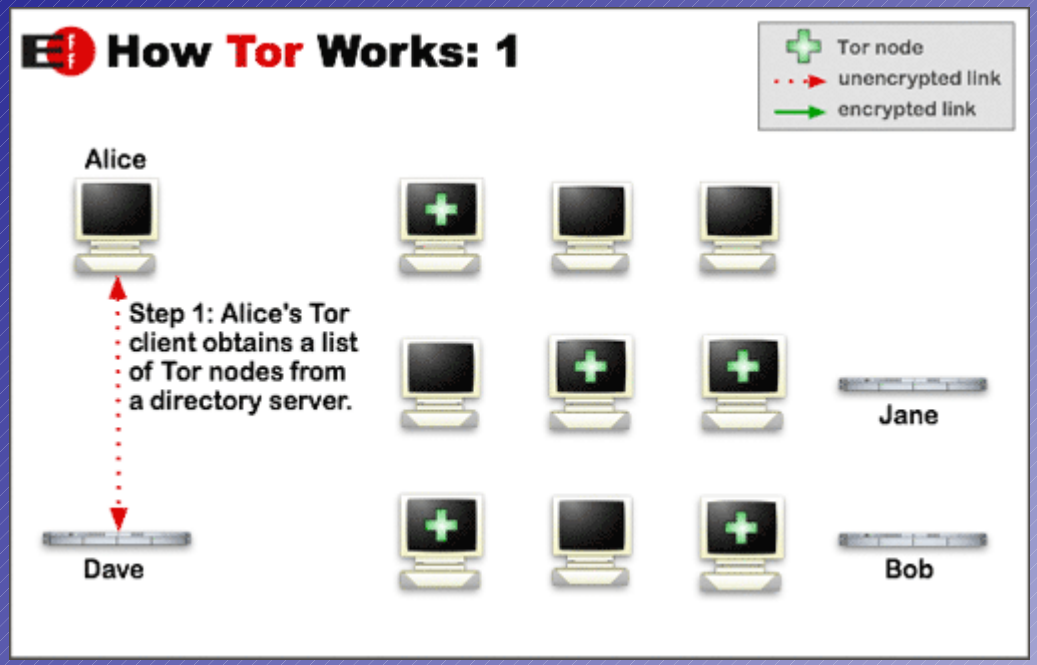


Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

Anonimato in rete con TOR
TOR: funzionamento passo-passo

I pacchetti dati nella rete Tor prendono un percorso casuale attraverso molti server che ne coprono le tracce, in modo che nessun osservatore situato in un singolo punto possa dire da dove venga o dove sia diretto un certo traffico.



Fonte http://tor.eff.org

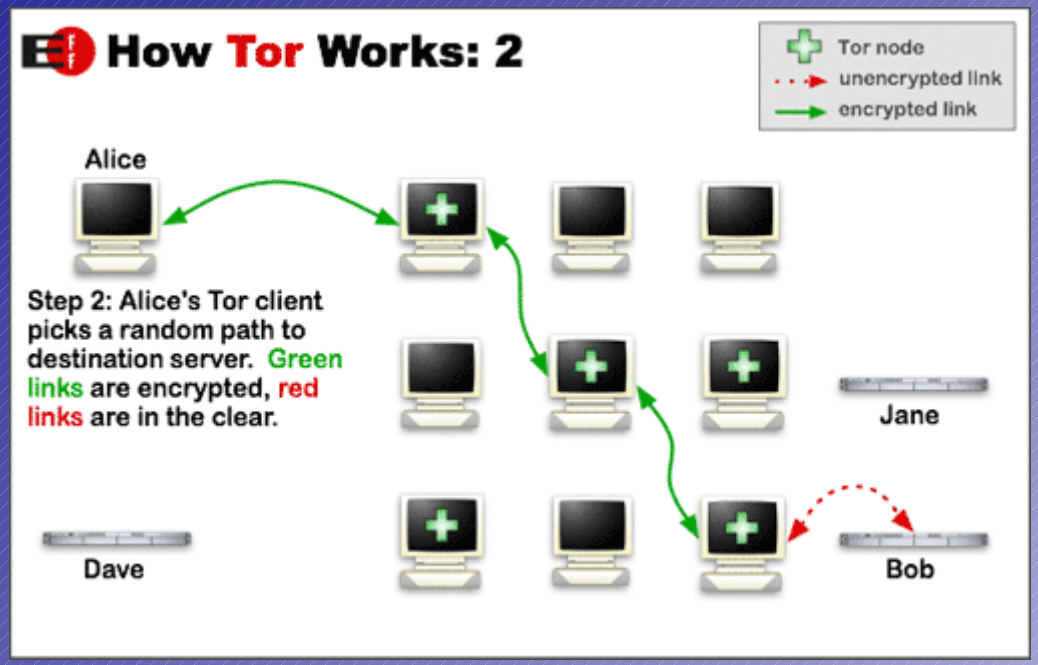
La fase uno richiede la conoscenza dei nodi TOR (gli onion router) disponibili.

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

Anonimato in rete con TOR
TOR: funzionamento passo-passo

Nella fase due il software genera una percorso di connessioni crittate attraverso gli *Onion Router*.



Fonte http://tor.eff.org

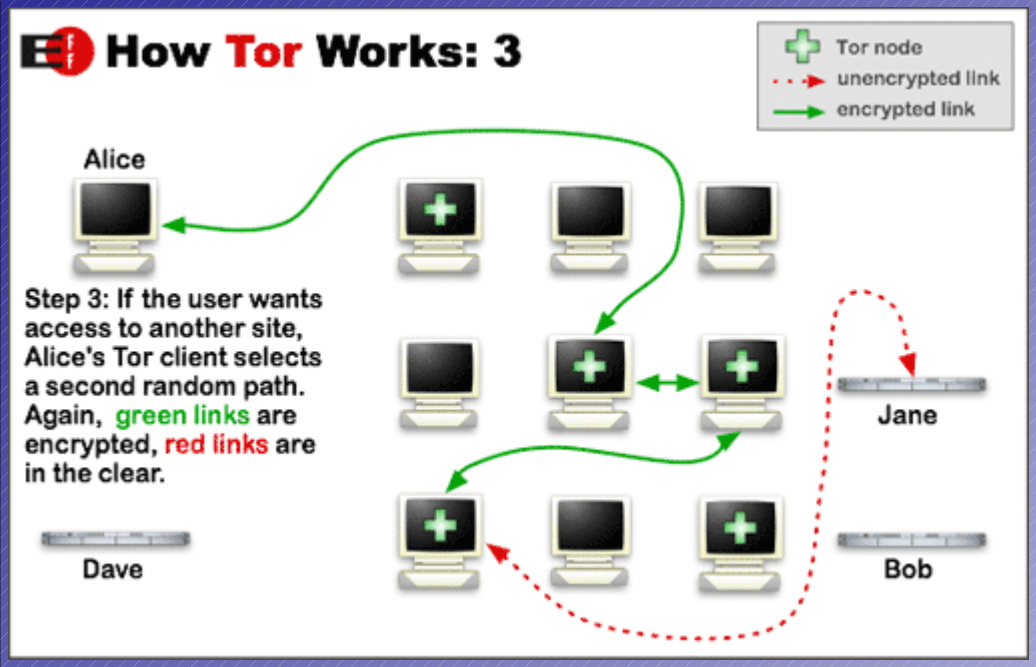
Ogni nodo è capace di vedere solo un singolo salto del circuito

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

Anonimato in rete con TOR
TOR: funzionamento passo-passo

Ogni minuto viene generato un nuovo percorso.



Fonte http://tor.eff.org

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

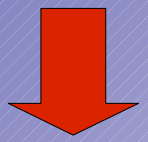
Anonimato in rete con TOR
TOR: restare anonimi

TOR funziona solo con i flussi TCP e richiede che l'applicazione abbia il supporto SOCKS.

TOR si concentra solo sulla protezione del trasporto dei dati.

Eventuali query ai nameserver passano in chiaro, i cookie non vengono bloccati, ...

La soluzione è utilizzare un *SOCKS4a Proxy* in modo che il browser non riveli le nostre richieste DNS.

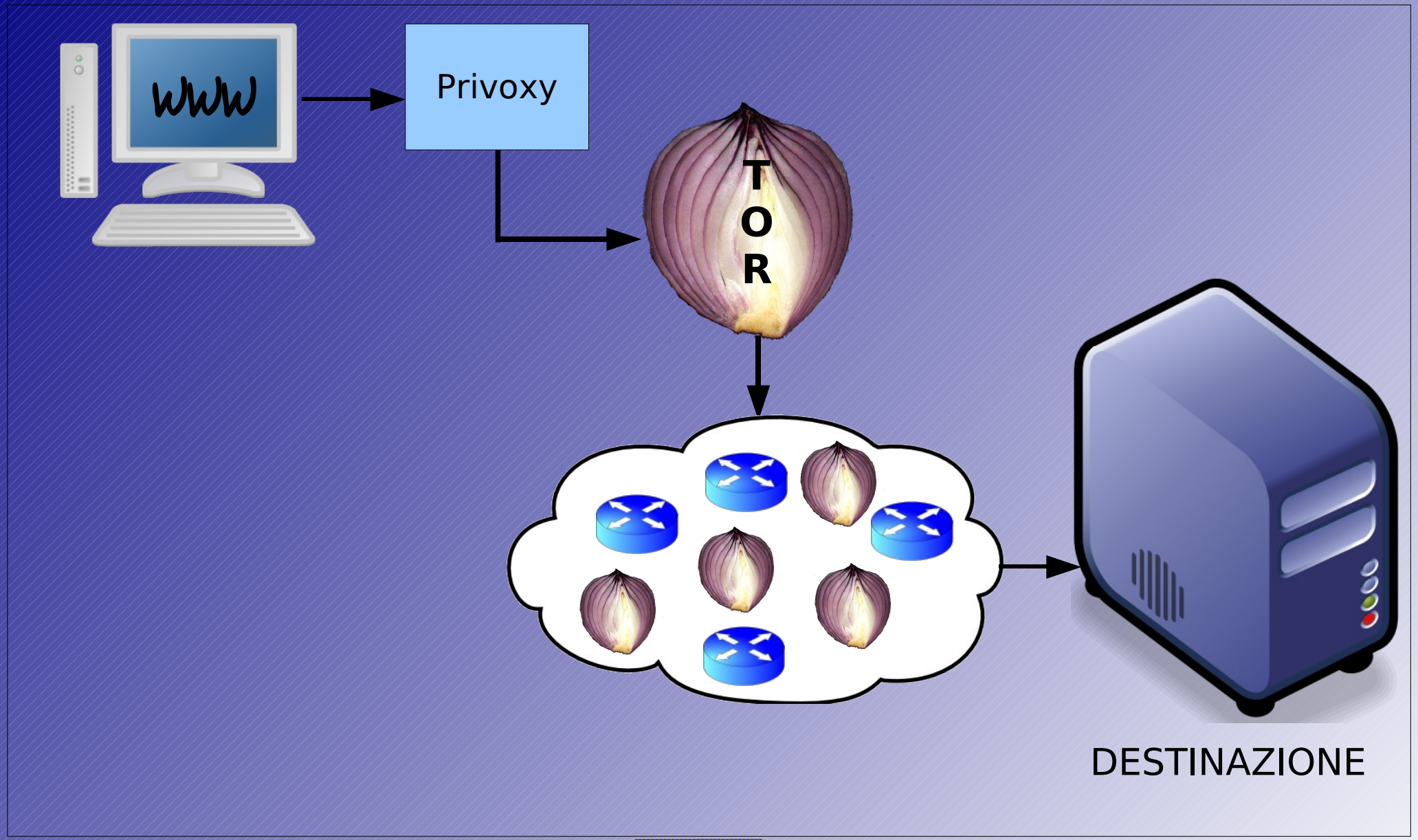


Privoxy

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

Anonimato in rete con TOR
TOR: restare anonimi



Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

TOR: installazione

L'installazione si suddivide nei seguenti passaggi:

- installazione TOR
- installazione Privoxy
- configurazione Privoxy
- configurazione browser
- test

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

TOR: installazione su GNU/Linux Debian

Scaricare e installare il software necessario:

```
~# apt-get install tor privoxy
```

Dopo l'installazione verranno creati due script di init che consentiranno l'avvio automatico di TOR e Privoxy:

```
~#/etc/init.d/tor
Usage:/etc/init.d/tor {start|stop|restart|reload|force-reload}

~#/etc/init.d/privoxy
Usage: /etc/init.d/privoxy {start|stop|restart|force-reload}
```

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

TOR: installazione su GNU/Linux Debian

E' necessario configurare Privoxy affinché usi TOR.

In un sistema Debian i file di configurazione di Privoxy si trovano in /etc/privoxy.

Il file da editare è /etc/privoxy/config aggiungendo la riga:

```
forward-socks4a / localhost:9050 .
```

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org

Metro Olografix
http://www.olografix.org

TOR: instalazione su GNU/Linux Debian

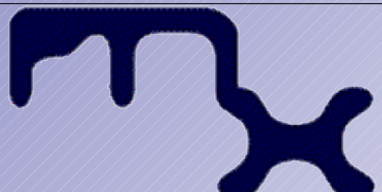
Riavviamo (o avviamo) TOR e Privoxy:

```
~#/etc/init.d/tor restart
~#/etc/init.d/privoxy restart
```

```
~# netstat -tulnp
Active Internet connections (only servers)
Proto  Local Address          Foreign Address        State       PID/Program name
tcp    127.0.0.1:8118         0.0.0.0:*              LISTEN      6947/privoxy
tcp    127.0.0.1:9050         0.0.0.0:*              LISTEN      6942/tor
```

Il sistema è pronto per funzionare. Ora resta solo da configurare le applicazioni affinché utilizzino privoxy, quindi TOR, per la navigazione e le connessioni attraverso la rete pubblica.

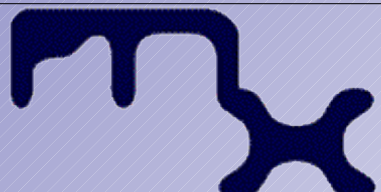
Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org



Metro Olografix
http://www.olografix.org

VEDIAMO IN PRATICA COME FUNZIONA

Mircha Emanuel `ryuujin` D'Angelo
ryuujin@olografix.org
http://www.ryuulab.org



Metro Olografix
http://www.olografix.org

creative commons

COMMONS DEED

Attribuzione 2.5

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.

Ogni volta che usi o distribuisci quest'opera, devi farlo secondo i termini di questa licenza, che va comunicata con chiarezza.

In ogni caso, puoi concordare col titolare dei diritti d'autore utilizzi di quest'opera non consentiti da questa licenza.

Le utilizzazioni consentite dalla legge sul diritto d'autore e gli altri diritti non sono in alcun modo limitati da quanto sopra.

Questo è un riassunto in linguaggio accessibile a tutti del
Codice Legale (la licenza integrale).

Limitazione di responsabilità