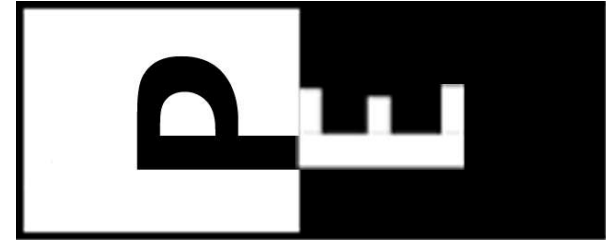


# E-privacy 2004

*data retention e diritto all'oblio*

Firenze, 14 - 15 maggio 2004



## I sistemi anonimi di condivisione delle informazioni

**Marco A. Calamari** - [marcoc@dada.it](mailto:marcoc@dada.it)

*The Freenet Project*

*Il Progetto Winston Smith*

**Copyright 2004, Marco A. Calamari**

È garantito il permesso di copiare,  
distribuire e/o modificare questo documento  
seguendo i termini della GNU General Public  
License, Versione 2 od ogni versione successiva  
pubblicata dalla Free Software Foundation.  
Una copia della licenza è acclusa come nota a  
questa slide, ed è anche reperibile all'URL

**<http://fly.cnuce.cnr.it/gnu/doc.it/gpl.it.html>**

*"Jimi, cerca di capire: io non voglio che quello che rimarra' di me dopo la morte resti chiuso nella banca dati di una multinazionale....."*

(Joystick a Jimi in "Nirvana", G. Salvatores, 1997)

# Di cosa parleremo

**Questo non e' un intervento su Freenet, anche se Freenet ne occuperà la parte principale.**

**Il tema dell'intervento e' la [pubblicazione anonima di informazioni sul web](#), od almeno su reti accessibili e con user experience simili a quelle usuali (web, chat, P2P), in modo che le informazioni possano essere navigate in maniera intuitiva anche da persone che non abbiano conoscenza diretta delle reti anonime.**

**In aggiunta, l'intervento coprirà l'uso di reti anonime per la condivisione di file in situazioni simili alle attuali reti di condivisione P2P.**

**E' forse il caso di accennare al motivo "filosofico" ma anche "contingente" che ci ha suggerito questo intervento.**

**Da una parte sta maturando in una parte consistente degli internauti un grado piu' o meno alto di consapevolezza che la vita in rete puo' e spesso e' costantemente tracciata od almeno tracciabile.**

**La **data retention** rende realizzabile anche in maniera differita questo tracciamento, personalizzabile ad hoc con tecniche di data mining; il tecnocontrollo acquisisce cosi' una marcia in piu'.**

Non sta invece maturando, se non tra i piu' virtuosi (e quindi paranoici) difensori della privacy, la percezione del disvalore presente e futuro di **tutte le piccole rinunce alla privacy** che sempre piu' spesso si compiono, soprattutto in rete.

Siamo quindi in una situazione in cui insegnare a pescare non porta (sicuramente non porta in tempi brevi) alla soluzione del problema fame, perche' evidentemente per una curiosa malattia o per l'abuso di medicinali, viviamo in un mondo dove la percezione della fame e' stata in gran parte rimossa.

E' quindi di valore creare intanto "nicchie di privacy nella Rete" in cui si possa far sopravvivere ed evolvere la pratica della privacy portata al suo limite estremo, il totale anonimato; sara' poi il singolo a decidere se di questo ha bisogno ed in cosa trasformare queste nicchie tecnologiche.

Bene, facciamo quindi tesoro e proseguiamo in questo intervento di tipo conoscitivo, antologico

Ci occupiamo del problema, storicamente piu' rilevante, della censura, trasportato sulla Rete

*"Come pubblicare informazioni (in rete) che non siano censurabili?"*

La risposta e'

*"Usando una rete anonima".*

Ma come ? Siamo qui proprio per parlare di questo.

Quali sono le reti anonime piu o meno "reali", cioe' implementate almeno in maniera prototipale, e che siano ancora in evoluzione e non morte (come Crowds) o gestite in maniera notoriamente inaffidabile (stendiamo un velo pietoso) ?

- **Freenet**

- **Entropy**

- **GnuNet**

- **Mute**

A nostro parere (ovviamente discutibile) non esistono, qui ed oggi, altre reti anonime dotate di una qualche funzionalita'.



Procediamo quindi con una veloce descrizione di:

- cosa queste reti sono,
- su quali principi si basano,
- che dimensione hanno, sia in termini di nodi che di contenuti già presenti ,
- quali strumenti reali, funzionanti e di (relativamente) semplice utilizzo mettono a disposizione degli autori di informazioni che necessitano di anonimato

Freenet e' una rete, anzi un protocollo di comunicazione anonimo, utilizzabile anche come layer in uno stack di protocolli di rete (se non vi e' chiaro non importa).

E' basato su protocolli di crittografia forte e su un datastore distribuito; tra le reti anonime e' quella piu' robusta in termini di algoritmi e protocolli.

Ha una dimensione attuale dell'ordine dei 1000 nodi (1-10 Terabyte); la dimensione non e' realmente importante.

Esistono, anche se in numero limitato, gateway web-Freenet

Ha contenuti in quantita' rilevante, stabili anche da anni

Ha un team di sviuppo piccolo ed agguerrito (anche con guerre interne, ma questa e' un'altra storia)

E' in sviluppo continuativo da oltre 4 anni

Ha un minimo di visibilita' mediatica (in passato ne ha avuta moltissima, ma col solito effetto "bolla"), che porta anche un minimo di raccolta di fondi (c'e' bisogno anche di voi, ma anche questa e' un'altra storia).

Ha alcune applicazioni ben sviluppate e ragionevolmente funzionali, che permettono di utilizzarla per scopi pratici senza richiederne una conoscenza tecnica.

Usa java, quindi dovete installarvi un JRE; non gira attualmente su Kaffe. Turatevi il naso, installate in locale la JRE di Sun versione 1.4.2 o superiori e giocate con le path. Sul Progetto Winston Smith trovate una documentazione nemmeno troppo vecchia.

# Freenet Insertion Wizard

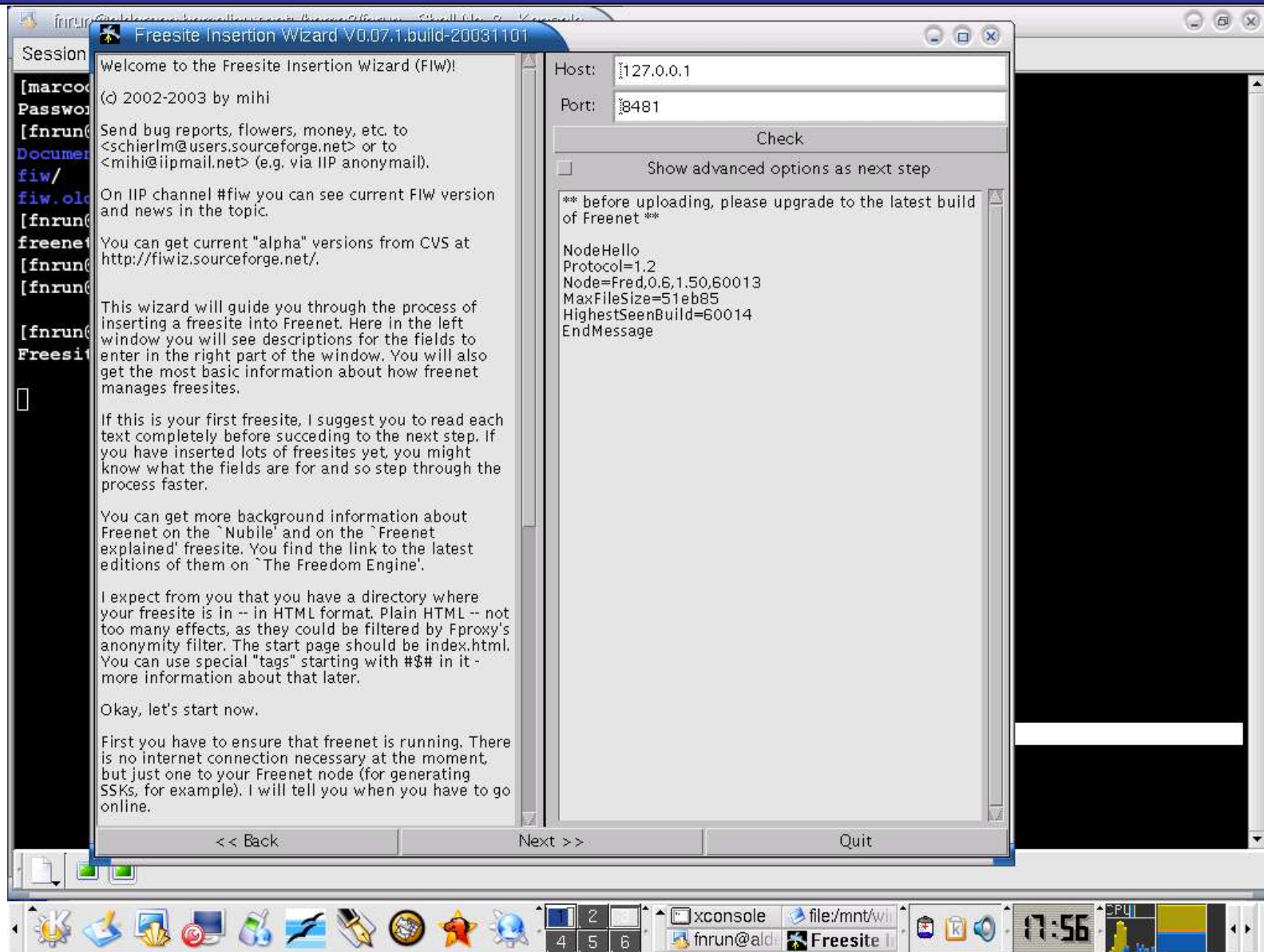
**FIW** (Freenet Insertion Wizard); scritto in java permette di inserire e mantenere freesite. E' autodocumentato, molto flessibile e dotato di strumenti di debugging e per aggiungere gadget ai freesite.

**Fortemente consigliato**, per inserire e gestire siti complessi ed aggiornabili.

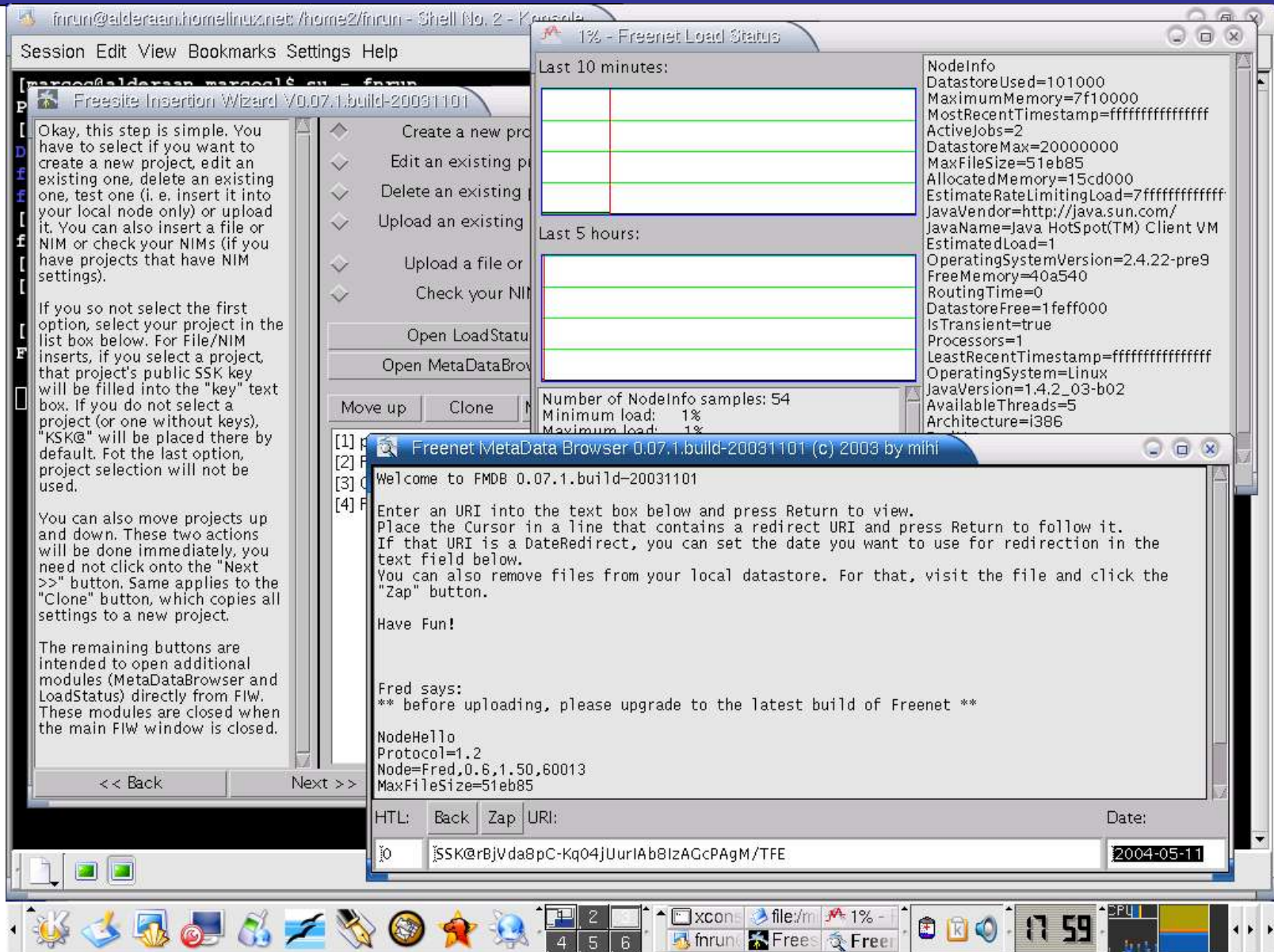
Funziona bene anche da windows (se proprio non ne potete fare a meno).

Funziona con varie JVM, quindi usate la stessa di Freenet.

# Freenet Insertion Wizard



# Freenet Insertion Wizard



Session Edit View Bookmarks Settings Help  
 [marco@alderaan.marcoal\$ su - frun  
 Freesite Insertion Wizard V0.07.1.build-20031101

Okay, this step is simple. You have to select if you want to create a new project, edit an existing one, delete an existing one, test one (i. e. insert it into your local node only) or upload it. You can also insert a file or NIM or check your NIMs (if you have projects that have NIM settings).

If you do not select the first option, select your project in the list box below. For File/NIM inserts, if you select a project that project's public SSK key will be filled into the "key" text box. If you do not select a project (or one without keys), "KSK@" will be placed there by default. For the last option, project selection will not be used.

You can also move projects up and down. These two actions will be done immediately, you need not click onto the "Next >>" button. Same applies to the "Clone" button, which copies all settings to a new project.

The remaining buttons are intended to open additional modules (MetaDataBrowser and LoadStatus) directly from FIW. These modules are closed when the main FIW window is closed.

Create a new project  
 Edit an existing project  
 Delete an existing project  
 Upload an existing project  
 Upload a file or NIM  
 Check your NIMs  
 Open LoadStatus  
 Open MetaDataBrowser  
 Move up Clone

**1% - Freenet Load Status**  
 Last 10 minutes:  


 Last 5 hours:  


 NodeInfo  
 DatastoreUsed=101000  
 MaximumMemory=7f10000  
 MostRecentTimestamp=ffffffffffffff  
 ActiveJobs=2  
 DatastoreMax=20000000  
 MaxFileSize=51eb85  
 AllocatedMemory=15cd000  
 EstimateRateLimitingLoad=7ffffffffffffff  
 JavaVendor=http://java.sun.com/  
 JavaName=Java HotSpot(TM) Client VM  
 EstimatedLoad=1  
 OperatingSystemVersion=2.4.22-pre9  
 FreeMemory=40a540  
 RoutingTime=0  
 DatastoreFree=1feff000  
 IsTransient=true  
 Processors=1  
 LeastRecentTimestamp=ffffffffffffff  
 OperatingSystem=Linux  
 JavaVersion=1.4.2\_03-b02  
 AvailableThreads=5  
 Architecture=i386  
 Number of NodeInfo samples: 54  
 Minimum load: 1%  
 Maximum load: 1%

**Freenet MetaData Browser 0.07.1.build-20031101 (c) 2003 by mihi**  
 Welcome to FMDB 0.07.1.build-20031101  
 Enter an URI into the text box below and press Return to view.  
 Place the Cursor in a line that contains a redirect URI and press Return to follow it.  
 If that URI is a DateRedirect, you can set the date you want to use for redirection in the text field below.  
 You can also remove files from your local datastore. For that, visit the file and click the "Zap" button.  
 Have Fun!  
 Fred says:  
 \*\* before uploading, please upgrade to the latest build of Freenet \*\*  
 NodeHello  
 Protocol=1.2  
 Node=Fred,0.6.1.50,60013  
 MaxFileSize=51eb85  
 HTL: Back Zap URI: Date:  
 [0] [SSK@rBjVda8pC-Kq04JUurlAb8IzAGcPAGM/TFE] [2004-05-11]

**Frost**; scritto in java e' una message board che permette anche la condivisione di file.

Ha una quantita' notevole di contenuti, anche se le sue condizioni di salute ovviamente sono legate a filo doppio a quelle di Freenet

# Frost

Frost 2002.11.03 16:48:49  
 File News Options Plugin Help

Frost Message System

- Frost
  - Frost
  - Boards
  - Test
- Freenet
  - Freenet
- Freesite boards
  - CofE
  - freesite\_announ
  - pws
  - italia
- Miscellaneous
  - linux
  - Bookz
  - cruft
  - news
  - mobile\_phone
  - Francophonie
  - pussygalore
  - jp\_anime
  - mp3
  - brazil
  - teens
- help\_!!
- gay
- snes\_romz
- jewish\_supremacy
- german

News Search Downloads Uploads

Index	From	Subject	Date
0	Troll Daddy	Re: argue on the troll board	2002.10.25 00:01:54GMT
1	Troll Daddy	Re: Feature request	2002.10.25 00:05:05GMT
2	Troll Daddy	theory on how many people actualy use frost	2002.10.25 00:06:42GMT
3	Troll Daddy	theory on how many people actualy use frost	2002.10.25 00:08:20GMT
4	Anonymous	Re: Feature request	2002.10.25 02:39:19GMT
5	Anonymous	Re: theory on how many people actualy use frost	2002.10.25 02:40:19GMT
6	Troll Daddy	how does frost upload files?	2002.10.25 03:15:03GMT
7	Anonymous	Re: Feature request	2002.10.25 04:24:01GMT
8	Anonymous	Re: how does frost upload files?	2002.10.25 04:25:00GMT

Filename Key

Up: 0 Down: 0 TOFUP: 0 TOFDO: 2 Results: 0 Selected board: frost



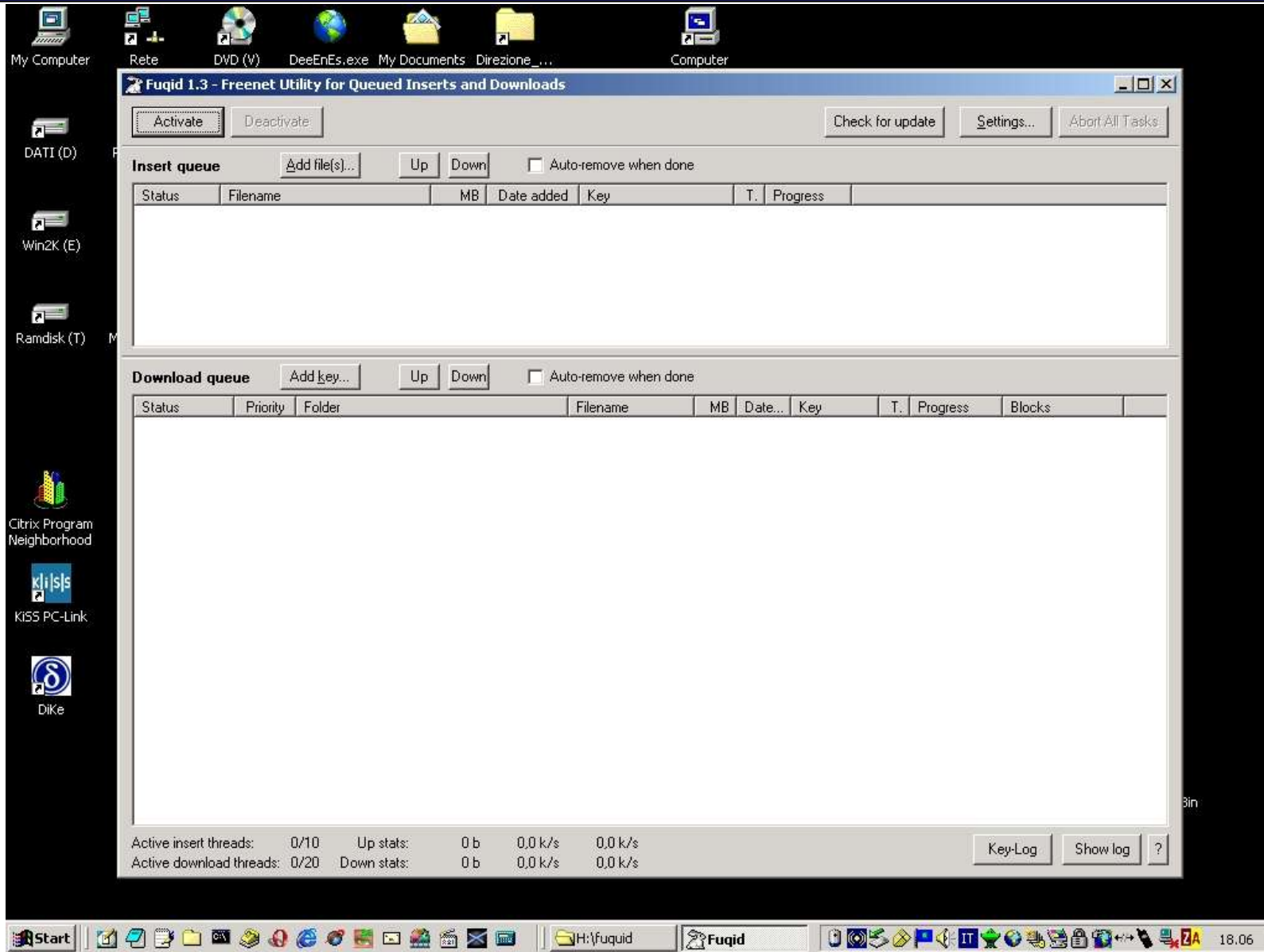
**FUQUID**; ahime' solo per windows, e' un tool per mass insertion/retrieval veramente potente e flessibile, nella sua semplicita' (fa una cosa sola e la fa bene)

Consigliato se non dovete inserire/recuperare siti ma file.

Ricordate pero' che Freenet non nasce come sistema P2P ma come sistema superanonimo.

Non vi aspettate quindi prestazioni esaltanti rispetto ai P2P classici, sia normali che anonimi.

# FUQUID



# Freenet Message Board

Ci sarebbe anche **Freenet Message Board**, con il suo sofisticato meccanismo di rating degli utenti ed i suoi splendidi scacchi anonimi, ma... volete che finiamo prima di domani, quindi stoppiamo l'esame di questo splendido software .....

..... anche perche' il suo sviluppo e' fermo da un paio d'anni (ci sono volontari ?)

# Freenet Message Board

freenet message board (alpha4a)
\_ □ ×

tree view table view archives chess lounge

n...	from	subject	date	reply to
	BadAssMofo (un...	Thanks	2002.10.18 17:38:23	?
	kiwi_uk (unverifi...	poo	2002.10.22 08:16:19	purist
	AcidFone	post it	2002.10.23 04:13:08	Pseudonym
	AcidFone (unveri...	IIP	2002.10.21 14:43:17	?
	Pseudonym (unv...	patch fails	2002.10.23 02:31:45	Purple
	Wookie (unverifi...	re: propagation	2002.10.22 03:42:31	?
	kiwi_uk (unverifi...	okaw here	2002.10.22 08:15:27	NonaimE

create new message

**from:** Wookie (De48eyKvA132GLzM3ilyon30JvoPAGM)

**source:** Green (4yWCicg2~QQosfqnsdI0-0TdMQcPAGM) verify

**date:** 2002.10.22 03:42:31

**newsgroup:**

**reply to:** (a message that has not yet been received)

**subject:** re: propagation

Since Yodel is a DBR site, you might not be able to fetch it because it hasn't been inserted today yet. You can try to see yesterday's version (append something like ?date=20021021 to the fproxy URL to see the main site, but not the images), or wait a little while until thoday's is inserted.

--

Wookie

reply to this message

**contact list**  
 sort contact list...

<b>Formerly know as Ano...</b>	288h
not listening on this channel	
<b>Dr. Papperlapapp</b>	388h
not listening on this channel	
<b>AcidFone</b>	276h
not listening on this channel	
<b>Wookie</b>	274h
not listening on this channel	
<b>Purple</b>	285h
not listening on this channel	
<b>kiwi_uk</b>	296h
not listening on this channel	
<b>Charizard</b>	391h
not listening on this channel	
<b>BadAssMofo</b>	383h
not listening on this channel	
<b>Green</b>	273h
not listening on this channel	
<b>Super_IMMY</b>	289h
not listening on this channel	
<b>plix</b>	301h
not listening on this channel	
<b>Pseudonym</b>	278h
not listening on this channel	
<b>emmv</b>	n/a

**announcement channel:**  
looking for slot 0 with 5 htl  
R

**Entropy** e' una rete di server paritetici basata su protocolli di crittografia forte

Ha una dimensione attuale dell'ordine dei 10 nodi

Ha contenuti stabili ma in piccola quantita'

E' basata in una certa misura su di una parte delle impostazioni e del codice di Freenet, pur essendo scritta in C

<http://entropy.stop1984.com/en/home.html>

Ha una utility per l'inserimento di freesite a linea comandi, e funzionalita' interne avanzate come una BBS


Ben funzionante, forse pero' solo a causa delle attuali piccole dimensioni. Non c'e' una documentazione che permetta di valutare con precisione il livello di anonimato raggiungibile.

# Entropy entry page

ENTROPY Gateway - Konqueror

Location Edit View Go Bookmarks Tools Settings Window Help


Location: http://127.0.0.1:9999/



... it flies like an Igel.

## Program version

# ENTROPY 0.4.2-261



... it flies like an Igel.

[ENTROPY Forum](#) | [The ENTROPY Project](#) | [ENTROPY Chat](#)

<p><b>Node load</b></p> <p>58%</p>	<p><b>Get a file from the ENTROPY network</b></p> <p>Key:<sup>2</sup> <input type="text"/> <input type="button" value="request"/></p>	<p><b>Latest build</b></p> <p>0.4.2-261</p>
<p><b>Links</b></p> <p><a href="#">KSK@qpl.txt</a> Click on this link to test your ENTROPY installation.</p> <p><a href="#">pullmoll's site</a> The very first ENTROPY site.</p> <p><a href="#">Entropy Engine</a> A site with links to more Entropy sites.</p> <p><a href="#">Entropy Engine</a> (Edition 1). The first edition of EE (w/o date based redirect)</p> <p>Read the <a href="#">Note</a> on links.</p>	<p><b>Put a file into the ENTROPY network</b></p> <p>Key:<sup>2</sup> <input type="text"/></p> <p>File:<sup>2</sup> <input type="text"/> <input type="button" value="Browse..."/></p> <p>Type:<sup>2</sup> <input type="button" value="auto (.ext)"/> <input type="button" value="insert"/></p>	<p><b>Thanks</b></p> <p>Many thanks to <a href="#">Parsimony</a> for the forum and chat facilities.</p> <p>Special thanks with kisses to <a href="#">Twister</a> for her patience, her love, the chocolate, the tobacco... etc.</p>
<p><b>ENTROPY Node Status</b></p> <p>Information about the state of this <a href="#">ENTROPY Node</a>:</p> <ul style="list-style-type: none"> <li>• Show the latest <a href="#">news</a> on your selected message boards</li> <li>• Configure your <a href="#">node</a> while it is running</li> <li>• List the ENTROPY <a href="#">processes</a> and running times</li> <li>• List the contacted <a href="#">peers</a> and their statistics</li> <li>• View the local <a href="#">data store's</a> current and maximum sizes</li> </ul>		
<p><b>Instructions and Links</b></p> <p>This is the HTTP gateway to the ENTROPY network. You will not be able to access <i>normal</i> Internet websites through this gateway, but you can access sites on the ENTROPY</p>		

Page loaded.

# Entropy BBS

ENTROPY 0.4.2-261 news (entropy) - Konqueror

Location Edit View Go Bookmarks Tools Settings Window Help

Location: http://127.0.0.1:9999/news/entropy

Gateway	News	Keypair	Config	Process	Peers	Store	
ENTROPY 0.4.2-261 news (entropy)							
Currently scanning board 'test' for date 2003-06-18							
No.	board	oldest	newest	total	today	new	create
1	<a href="#">test</a>	5 days 22,5 hours	7 hours 38 minutes	48	<u>12</u>	<u>36</u>	<a href="#">post</a>
2	<a href="#">discussions</a>	3 days 18,6 hours	12 hours 45 minutes	18	0	<u>18</u>	<a href="#">post</a>
3	<a href="#">entropy</a>	5 days 22,2 hours	7 hours 54 minutes	60	<u>10</u>	<u>50</u>	<a href="#">post</a>
4	<a href="#">mp3</a>	5 days 16,8 hours	5 days 16,8 hours	1	0	0	<a href="#">post</a>
5	<a href="#">stop1984</a>	5 days 19,5 hours	9 hours 4 minutes	8	<u>1</u>	0	<a href="#">post</a>
6	<a href="#">twisterstories</a>	3 days 23,2 hours	12 hours 36 minutes	9	0	0	<a href="#">post</a>
7	<a href="#">pr0n</a>	5 days 21,4 hours	5 days 1,4 hours	2	0	0	<a href="#">post</a>
8	<a href="#">porn</a>	-	-	-	-	-	<a href="#">post</a>
all	<a href="#">all boards</a>	5 days 22,5 hours	7 hours 38 minutes	146	<u>23</u>	<u>104</u>	<a href="#">rescan</a>

I found the following board announcements, besides the ones you subscribed:

none yet

msg	#9	from	Rescue	board	entropy	date	2003-06-19 04:31:31U
▲ ▼	<a href="#">reply</a>	subject	Website typo				

On the English Clients page:

"Freenet Tools  
The most important tools for thos, who"

Page loaded.

GnuNet e' una rete di proxy paritetici che realizzano, con l'ausilio di canali crittografati, una rete di proxy di servizi che applicano il concetto della rete Crowds, sviluppata in AT&T fino al 1998 (v 1.1.4) e ormai estinta. E' scritta in C, ottimamente documentata, sia come software che dal punto di vista accademico (<http://www.ovmj.org/GNUnet/>)

Realizza un anonimato ottenuto mediante l'offuscamento del traffico, in una maniera che ricorda quello del protocollo Mixmaster.

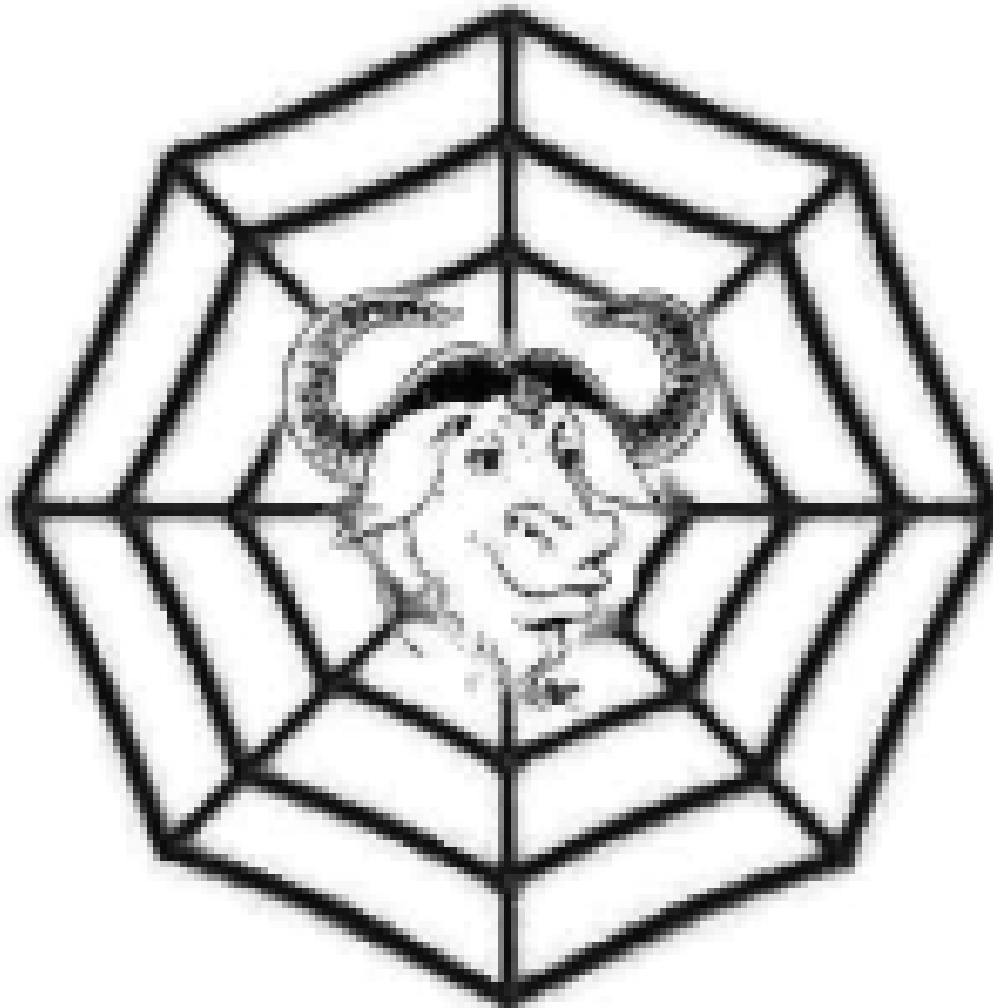
La dimensione della rete non e' stimabile, ma e' presente una certa quantita' di contenuti. E' sostanzialmente la cosa piu' vicina ad una Gnutella anonimizzata

L'anonimita' viene implementata a livello di filesystem (AFS – Anonymous File System). **E' un sistema P2P puro**, non un protocollo.

Non c'e' interfaccia grafica (anche se esiste un add-on di interfaccia gnunet-gtk) pero' c'e' comunque .....

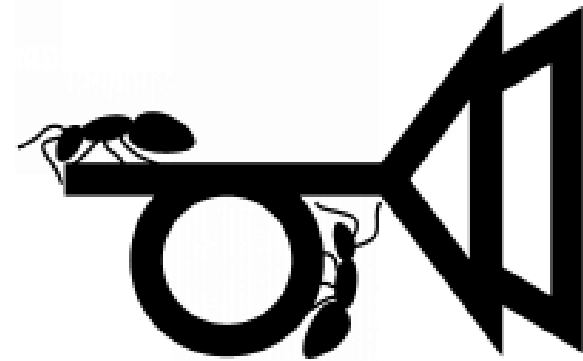


.... un bel logo!



Mute e' una rete di proxy anonimizzanti  
scritta in C

<http://mute-net.sourceforge.net/>



Utilizza connessioni criptate ed il concetto di IP virtuali per proteggersi dalle usuali tecniche di tracciamento tanto in voga; e' una reazione diretta agli attacchi al P2P di questi ultimi tempi, come il suo Manifest non manca di sottolineare.

Progetto ottimamente impostato dal punto di vista “commerciale” (nel senso della diffusione) e' un sistema P2P puro alla Gnutella; multiplatforma . Dategli qualche soldo !

# Mute

MUTE File Sharing

File

Search Downloads Uploads Connections Settings

mp3 Search

File Name	Size	Hash	Host Virtual Address
Clarence Carter-Strokin'(Unsen...	4.19 MiB	687D281B3576F10CEBF0057A...	B6266AE4C874E08C284A4B89
Pink Floyd - Another Brick in th...	3.69 MiB	D8C835723CA14D6CD114932...	B6266AE4C874E08C284A4B89
Guided By Voices- I Am a Scie...	2.19 MiB	26A3219AFD94315B6E87B788...	B6266AE4C874E08C284A4B89
Oingo Boingo - Dead Man's Pa...	5.83 MiB	FBAC6A95293631839E40663F...	B6266AE4C874E08C284A4B89
Oingo Boingo - Weird Science...	3.49 MiB	96834A30762A414A81A7BE0E...	B6266AE4C874E08C284A4B89
Peggy Lee - Is That All There I...	3.98 MiB	72D612FBBE6CE81D1EAF71D...	B6266AE4C874E08C284A4B89
03 - pavement - no life singed ...	2.47 MiB	2DF0200B1B2BC480CA01C113...	B6266AE4C874E08C284A4B89
Pavement - Summer Babe.mp3	3.00 MiB	73E923DC611902F739421E525...	B6266AE4C874E08C284A4B89
Pavement - In The Mouth A De...	3.54 MiB	163F3E1C30C6160AFA0FA480...	B6266AE4C874E08C284A4B89
dj shadow - 01 best foot forwar...	657.62 KiB	C8F410D893AC6933988D326C...	B6266AE4C874E08C284A4B89
DJ Shadow - Building Steam W...	6.13 MiB	7ADC5188159477B769FEED0B...	B6266AE4C874E08C284A4B89
Suzanne Vega & DNA - Toms ...	3.52 MiB	53731214E5A73E7B295459F64...	B6266AE4C874E08C284A4B89
Anti-Flag - Born To Die.mp3	1.88 MiB	156B109218AFF5681DE6D464...	B6266AE4C874E08C284A4B89
Bruce Springsteen - Born in the...	4.29 MiB	8FF2360B9E5E898F218AED50...	B6266AE4C874E08C284A4B89
Arlo Guthrie - Alice's Restoran...	17.00 MiB	255B71C3525F139B535B6D609...	B6266AE4C874E08C284A4B89
Square Pusher - Hard Normal ...	2.95 MiB	5762D49729659238DFA61B70...	B6266AE4C874E08C284A4B89
squarepusher - squarepusher world	4.72 MiB	709D03DB9C607ABD218BDEC...	B6266AE4C874E08C284A4B89

Download

**Ma allora....**

**cosa dobbiamo usare ?**

*Volete l'anonimato prima di tutto ?*

Allora usate Freenet ! FIW per i siti, Frost per comunicare e FUQUID per i file

*Volete fare P2P “abbastanza” anonimo (ma sempre infinitamente meglio dei classici programma P2P) ?*

Usate MUTE o GnuNet a seconda delle loro prossime evoluzioni e stati di salute

# Siamo tifosi, ma con un motivo

Sapete che nel Progetto Winston Smith facciamo della paranoia una virtu', infatti il nostro motto e' "*la paranoia e' una virtu'*"

Freenet, la piu' anonima tra le reti anonime e' quindi la nostra scelta di elezione; nel seguito dell'intervento tratteremo piu' a fondo proprio il funzionamento di .....

## Freenet !

“Freenet e' una rete adattativa di nodi peer-to-peer che si interrogano reciprocamente per immagazzinare e recuperare file di dati identificati da nomi (chiavi ) indipendenti dalla locazione.”

Freenet e' formata da server (nodi) paritetici; i nodi includono un proxy che permette di accedere al server Freenet con un form, utilizzando il protocollo HTTP.

“Freenet :

A Distributed Anonymous Information Storage and Retrieval System”

I.Clarke et al.

“Freenet e’ un sistema per scrivere e leggere file da Internet senza che si possa risalire a chi li ha scritti, chi li conserva sul disco e chi li recupera.”

Questo scopo viene raggiunto utilizzando il client (nodo) Freenet, che spezzetta, crittografa, duplica, disperde i contenuti del file, e riesce ad eseguire l’operazione inversa per recuperarli.

Freenet non permette di cancellare niente e non conserva informazioni su dove un file si trova.



# Cosa trovo su Freenet ?

Freenet non e' un applicazione ma un protocollo.

La cosa di gran lunga piu' utile che troviamo su Freenet sono i freesites.

Sono gruppi di chiavi Freenet che, accedute via browser, si comportano quasi esattamente come un normale sito web.

Esiste un "indice" non ufficiale od esaustivo ma di grande reputazione ed utilita', che elenca i freesite - "The Freedom Engine"

Esistono tre tipi di freesites:

**One shot** – sito inserito una sola volta, che sopravvive solo per un certo periodo

**DBR (Date Based Redirect)**, che visualizzano il contenuto riferito alla data odierna

**Edition-based**, che non cambiano ad intervalli fissi, ma visualizzano un avvertimento quando ne viene prodotta una edizione piu' recente

# Sono sicuri i Freesite ?

La navigazione su un freesite, normalmente anonima, puo' essere tracciata se un freesite "trappola" utilizza accorgimenti per tracciare il navigatore.

Freenet include filtri che rilevano gli accorgimenti noti ed avvertono il navigatore.

L'utilizzo di Freenet da parte di chi desidera anonimato non e' foolproof, ma deve essere fatto con attenzione.

“Per creare l'anonimato e' necessaria una complessa attivita' tecnica, per distruggerlo basta un click disattento.”

# Obiettivi da raggiungere

- **Anonimato** sia per il produttore che per il fruitore dell'informazione
- Il sistema non deve avere elementi di controllo centralizzati o di amministrazione
- Il sistema deve essere robusto rispetto ai problemi hardware/software
- Il sistema deve “adattarsi” e mutare nel tempo
- Le performance devono essere paragonabili ad altri sistemi (WWW)

- Modello centralizzato
  - Esempio : Napster
  - indice mantenuto da un autorità centrale - conoscenza globale dei dati (single point of failure)
  - contatto diretto tra richiedente e fornitore
- Modello decentralizzato
  - Esempio : Freenet, Gnutella
  - nessun indice globale – conoscenza locale dei dati (approximate answers)
  - contatti mantenuti da una “catena” di intermediari

- **Versione 0.5.2**
- **Realizzata in linguaggio java** - funzionante su differenti architetture
- Possiede una **interfaccia utente nativa** (inclusa in Fproxy) che permette di operare in maniera intuitiva, ma anche di controllare aspetti molto tecnici del nodo.
- **Datastore nativo crittografato** - non e' possibile cercare una categoria di contenuti, ma solo identificare un file dato

- **Routing adattativo** - il grafo delle connessioni logiche tra i nodi evolve nel tempo verso una stabilità ed efficienza maggiore, ed i nodi stessi si specializzano .
- **Comportamento non deterministico** - il funzionamento di Freenet non è completamente deterministico, e non consente di provare con certezza che un certo file presente nel datastore sia stato richiesto dal nodo locale e non da un altro nodo della rete

- **Resilienza della rete** - Freenet puo' perdere una rilevante percentuale di nodi senza un'apprezzabile riduzione di prestazioni, e la maggioranza dei suoi nodi senza cessare di funzionare
- **Comportamento "ecologico"** - l'informazione puo' essere inserita in Freenet ma non rimossa; puo' solo essere lasciata "morire" di morte naturale. L'informazione che viene richiesta si moltiplica su piu' nodi e si "avvicina" ai nodi che la richiedono; quella non richiesta scompare.



- **Anonimita'** sia di chi memorizza informazioni che di chi le recupera - nel caso si prevedano attacchi con memorizzazione del traffico sono necessarie cautele aggiuntive (Fproxy attraverso un tunnel SSL).
- **Autenticazione crittografica tra i nodi** - non e' possibile "impersonare" un nodo gia' noto alla rete sostituendosi ad esso

**Meccanismo di suddivisione ridondante dei file per l'inserimento ed il recupero di file di grosse dimensioni (FEC splitfile di Onion Networks).**

**L'inserimento di un grosso file in Freenet e' problematico; con la suddivisione di un file in parti piu' piccole si risolve il problema dell'inserimento, ma basta l'impossibilita' di recuperare un pezzo ed il file e' perso.**

**L'algoritmo FEC (Forward Error Correction) moltiplica di un certo fattore (tipicamente 1,5) il numero di parti, ma aumenta la possibilita' di recuperare integralmente il file perche' non e' necessario recuperarne tutte le parti.**

Supponiamo di avere un file di 10 Mb e di suddividerlo in 10 parti; supponiamo che la probabilita' di recuperare una chiave qualsiasi da freenet sia del 90%.

La probabilita di recuperare tutte e 10 le chiavi e'  $0.90^{10} = 0,3486$  cioe' meno del 35%.

Se inserisco invece 15 parti ridondate con l'algoritmo FEC, la probabilita' di recuperare l'intero file (cioe' almeno 10 blocchi su 15) e' del 99.8%.

Quest'ultimo calcolo statistico e' lasciato all'abilita' matematica del lettore, oppure e' disponibile dietro modico sovrapprezzo 8) .

# Cosa Freenet non puo' fare

- Non esiste attualmente la possibilita' di indicizzare le chiavi in modo da operare una ricerca intelligente.
- Il problema non e' risolto a livello di protocolli
- Esiste una proposta per la creazione e gestione di indici interni a Freenet (FASD, Kronfeld et al.) che pur descritta completamente a livello teorico, non e' stata ancora implementata

# Cosa Freenet non puo' fare

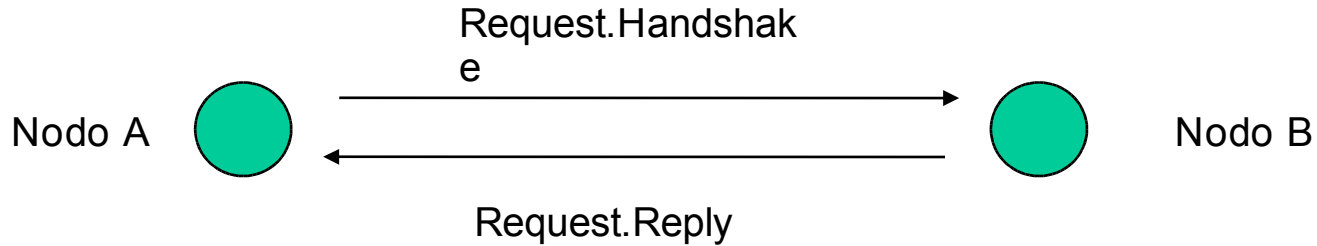
- Non esiste un meccanismo “sicuro” di boot di un nuovo nodo senza possedere un minimo di informazioni sulla rete.
- Attualmente, per bootstrappare un nuovo nodo, bisogna conoscere l’indirizzo di almeno un nodo “affidabile” di Freenet.
- Si utilizzano un server web del Progetto e/o un file aggiornato di nodi distribuito insieme ai file di supporto di Freenet

# Come funziona Freenet

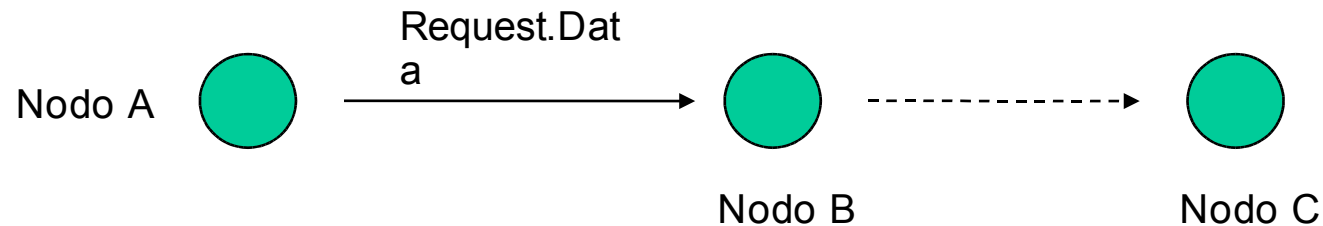
# Come funziona Freenet

- **I nodi comunicano tra loro con un semplice protocollo connection-oriented chiamato FNP (Freenet Network Protocol), normalmente realizzato sopra il tcp/ip**
- **I client applicativi (e.g. Frost) che vogliono utilizzare i servizi Freenet di un nodo locale utilizzano un altro protocollo chiamato FCP (Freenet Client Protocol)**

## Fase di Handshake



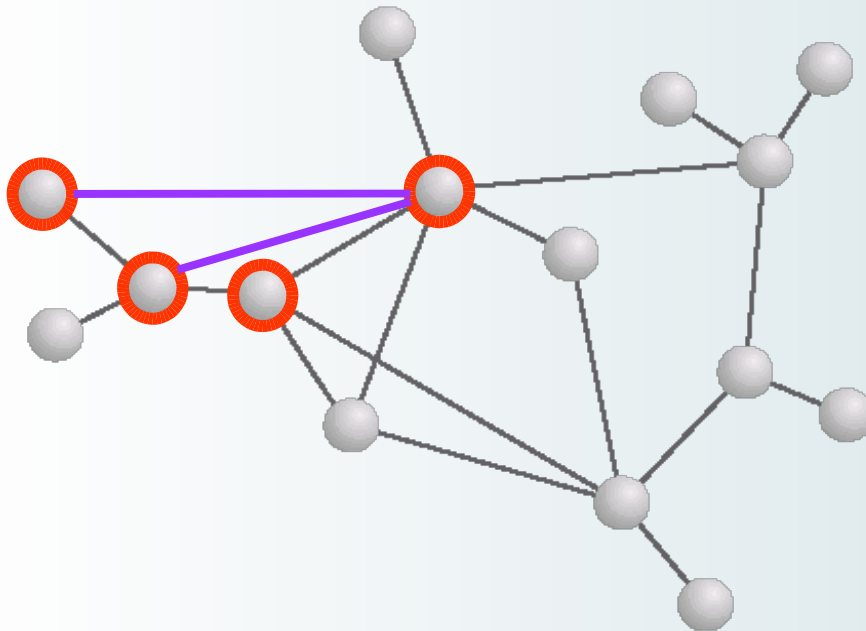
## Fase di richiesta dati





# Come funziona Freenet

- I nodi comunicano tra loro sulla base di una conoscenza locale dinamica dei nodi limitrofi
- Ogni nodo richiede una chiave, nell'ordine, ai nodi limitrofi

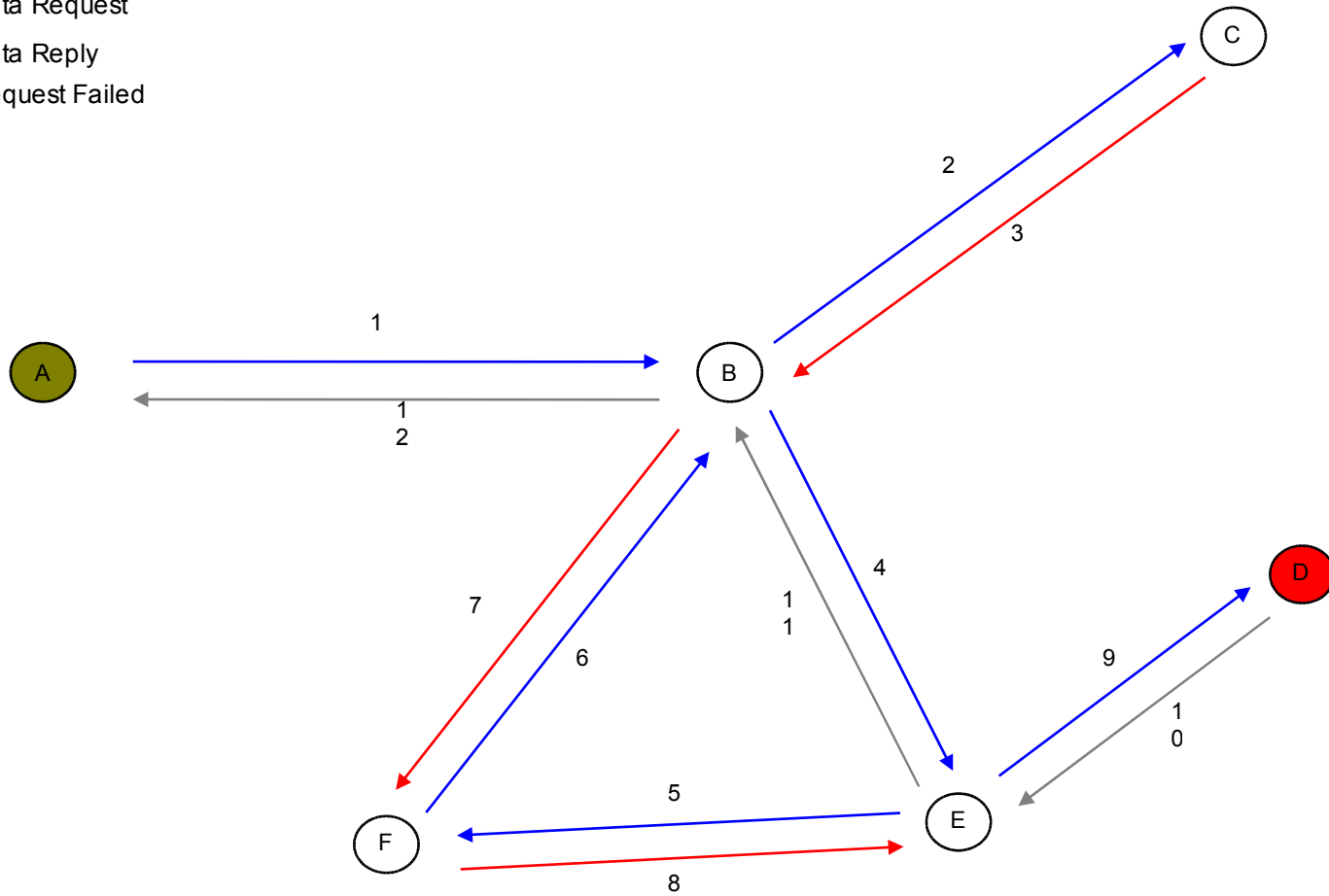


# Come funziona Freenet

- Un nodo che riceve da un confinante la richiesta di una chiave che ha precedentemente cercato e non trovato la rigetta immediatamente.
- Un nodo che deve inserire una chiave, prima la ricerca per evitare una collisione, e successivamente la inserisce
- La “profondita” della ricerca o dell’inserimento di una chiave e’ data dall’HTL (hops to live)
- Ogni nodo che deve passare una richiesta decrementa l’HTL di 1

# Come funziona Freenet

- Data Request
- Data Reply
- Request Failed



# Come funziona Freenet

- Ogni nodo memorizza le chiavi “alla rinfusa” in un database che viene denominato “datastore
- Una chiave esiste solitamente in piu’ copie su piu’ nodi, in dipendenza dalla profondita’ di inserimento della richiesta originale
- Ogni nodo che, dopo aver trasmesso una richiesta che ha avuto successo, riceve la chiave da ripassare al nodo richiedente, ne fa una copia nel datastore locale

# Come funziona Freenet

- Un “rumore di fondo probabilistico” viene inserito in tutte le decisioni di routing (variazione dell’HTL, possesso della chiave, etc.) per impedire che un eventuale registrazione del traffico possa far risalire al nodo che ha effettuato la richiesta o l’inserimento originali, e permettere all’operatore del nodo la ripudiabilità di un’eventuale attribuzione di responsabilità del contenuto del datastore.

# Come funziona Freenet

- I singoli datastore vengono gestiti con un watermark, sulla base della data e del numero degli accessi alle singole chiavi
- Le chiavi “popolari” si moltiplicano e si spostano “vicino” ai nodi che le richiedono
- Le chiavi “impopolari” scompaiono
- Si tratta di un comportamento “ecologico” che permette di realizzare un sistema in cui non esiste il comando “delete”

# Come funziona Freenet

- I singoli nodi si “specializzano” nel memorizzare alcune chiavi, basandosi su una “distanza lessicale” che viene calcolata utilizzando un hash del contenuto della chiave, e specializzandosi in un segmento di essa
- Le decisioni di routing delle richieste possono essere fatte in maniera intelligente, poiché’ i nodi pubblicizzano il segmento di spazio delle chiavi in cui sono “specializzati”

# Meccanismi crittografici



- I file in Freenet sono associati e memorizzati utilizzando oggetti detti “chiavi” :

**KSK** (keyword signed key)

**CHK** (content hash key)

**SSK** (signed subspace key)

- Nota : la funzione hash utilizzata è lo SHA-1 a 160 bit mentre l’algoritmo asimmetrico di cifratura è il DSA

- E' la chiave più semplice e user-friendly
  - Esempio -> freenet:KSK@mio\_file.txt
  - La stringa descrittiva (mio\_file) viene utilizzata per generare una coppia di chiavi pubblica/privata (algoritmo DSA)
  - La chiave pubblica viene utilizzata per produrre l'hash associato al file inserito (SHA-1)
  - La chiave privata viene utilizzata per “firmare” il file inserito.

# La chiave CHK

- E' derivata dall'hash del contenuto del file corrispondente. Tutti i file sono chiavi CHK
- Il file viene inoltre criptato utilizzando una chiave generata in modalità random
- Vengono pubblicati sia l'hash che la chiave di decrittazione
  - Esempio -> freenet:CHK@foto.gif
  - Una volta inserito, il dato potrà essere richiesto fornendo la seguente stringa :

CHK@zdfaGT.....,fpR12.....

- Costruzione di un “namespace” personale
  - Creiamo una coppia di chiavi pubblica/privata di tipo SSK
  - Utilizzeremo la chiave privata per inserire documenti “sotto” il nostro namespace
  - Pubblicheremo la nostra chiave pubblica per rendere accessibili i file pubblicati
  - Esempio -> SSK@public\_key/musica/song1.mp3  
SSK@public\_key/musica/song2.mp3

# Bibliografia

pagina

pagina

- **“Freenet : A Distributed Anonymous Information Storage and Retrieval System”** - I. Clarke et al.
- **“Performance in Decentralized Filesharing Networks”** - T. Hong
- **“Advanced Routing on Freenet”**: (Serapis) - Shu Yan Chan
- **“FASD: A Fault-tolerant, Adaptive, Scalable, Distributed Search Engine”** - Amr Z. Kronfol, Princeton University May 6, 2002

I documenti sono reperibili sul sito del progetto  
<http://freenetproject.org>

# Grazie a tutti per l'attenzione

contattatemi pure all'indirizzo [marcoc@dada.it](mailto:marcoc@dada.it)

**mail list su Freenet in italiano**

<http://lists.firenze.linux.it/mailman/listinfo/freenet-list>

**Sito ufficiale Freenet**

<http://www.freenetproject.org/>

**Il progetto Winston Smith**

[freenet:SSK@Dgg5IJQu-WO905TrIZ0LjQHxDdIPAgM/pws/14//](mailto:freenet:SSK@Dgg5IJQu-WO905TrIZ0LjQHxDdIPAgM/pws/14//)

mirror: <http://www.winstonsmith.it>