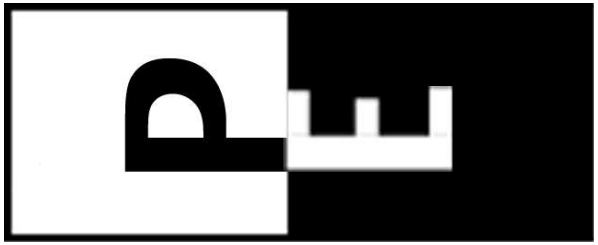
E-privacy 2004

data retention e diritto all'oblio

Firenze, 14 - 15 maggio 2004



I sistemi anonimi di condivisione delle informazioni

Marco A. Calamari - `marcoc@dada.it`

The Freenet Project

Il Progetto Winston Smith

"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 occupera' 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 coprira' 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.

Reti anonime

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.

Reti anonime

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'.

Reti anonime

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 gia' presenti ,
- quali strumenti reali, funzionanti e di (relativamente) semplice utilizzo mettono a disposizioni degli autori di informazioni che necessitino di anonimato

Freenet

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)

Freenet

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

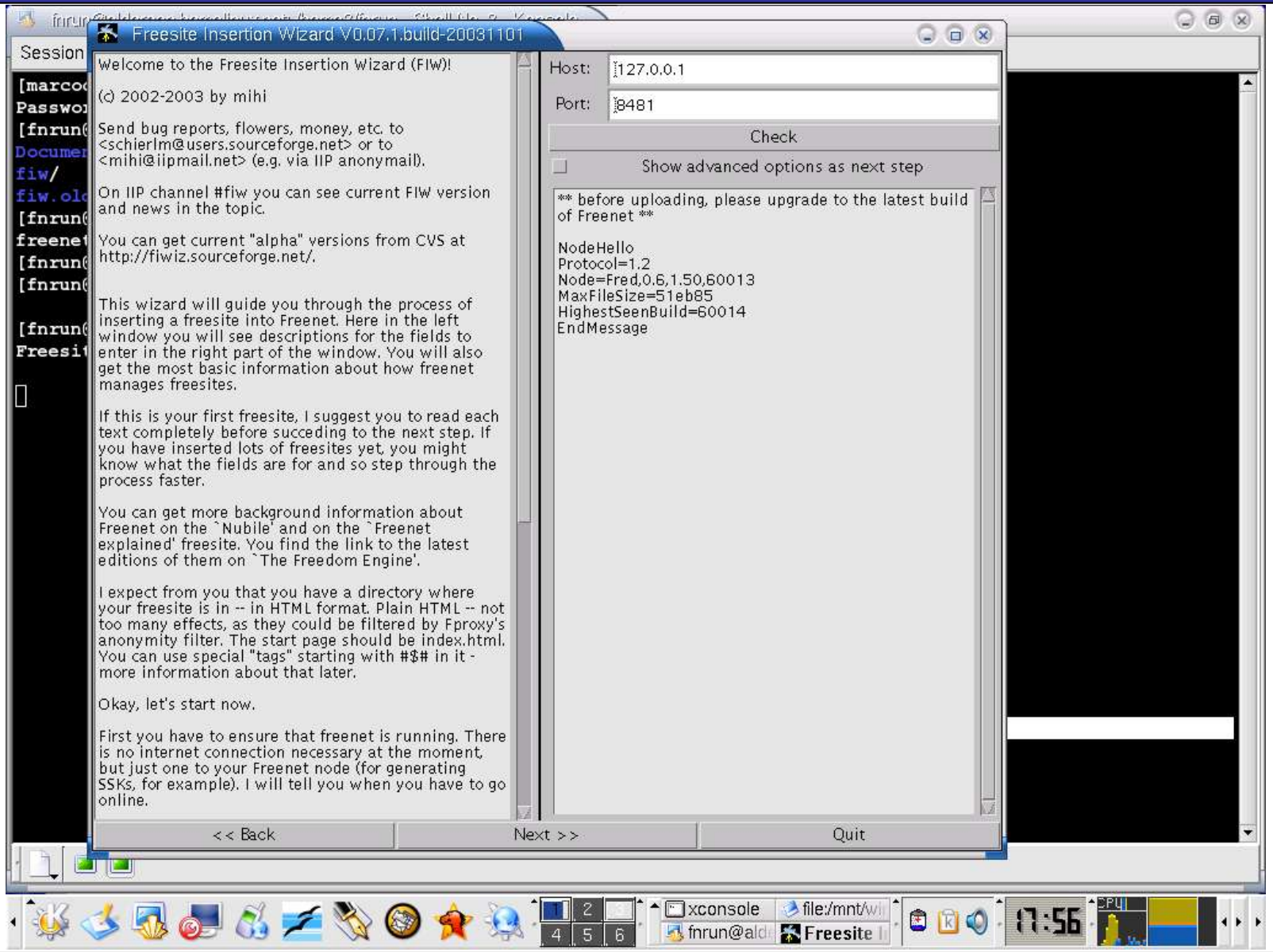
FIW (Freenet Insertion Wizard); scritto in java permette di inserire e mantenere freesite. E' autodocumentato, molto flessibile e dotato di strumenti di debugging e per aggiungere gadget ai freesite.

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

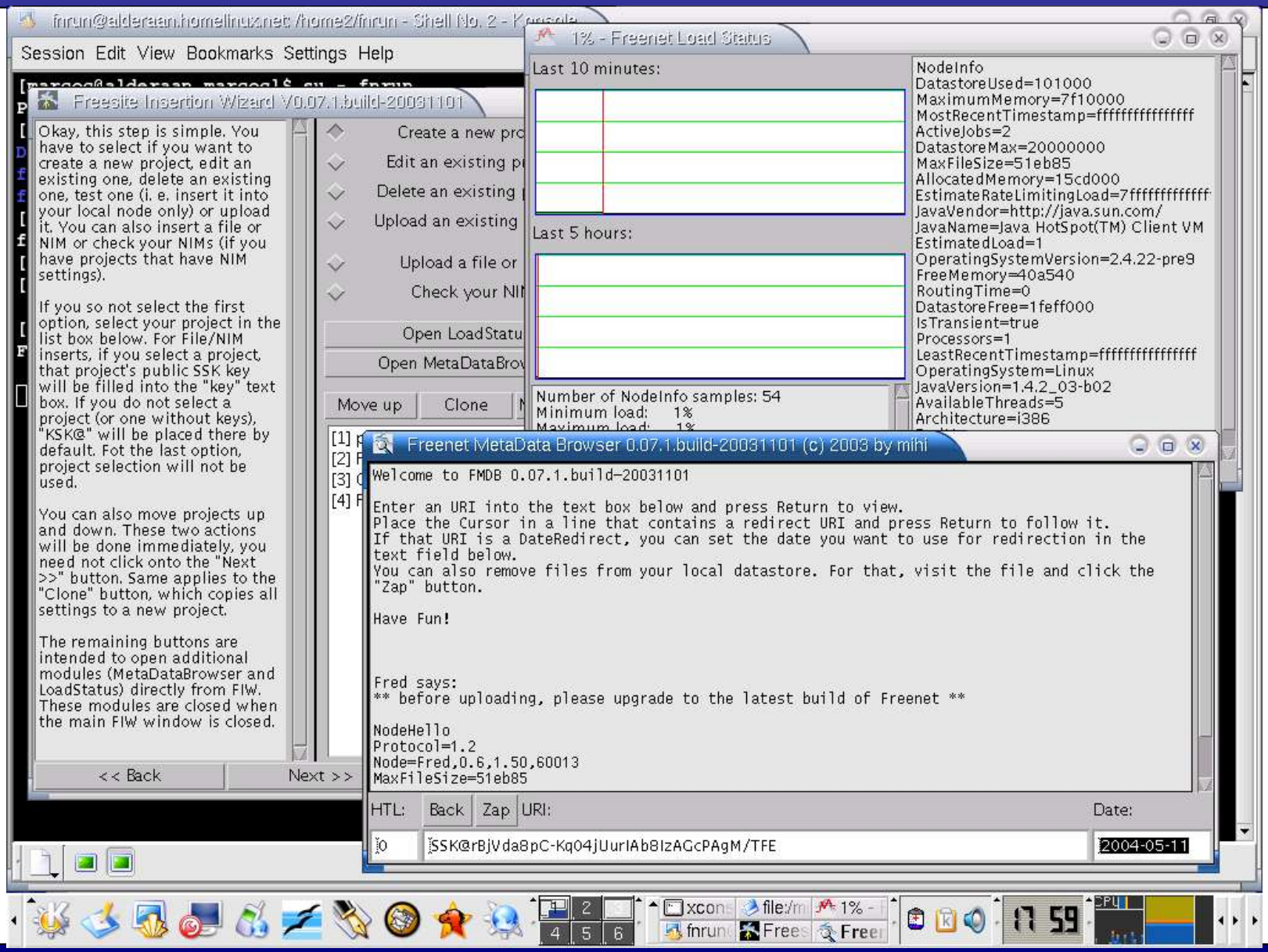
Funziona bene anche da windows (se proprio non ne potete fare a meno).

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

Freenet Insertion Wizard



Freenet Insertion Wizard

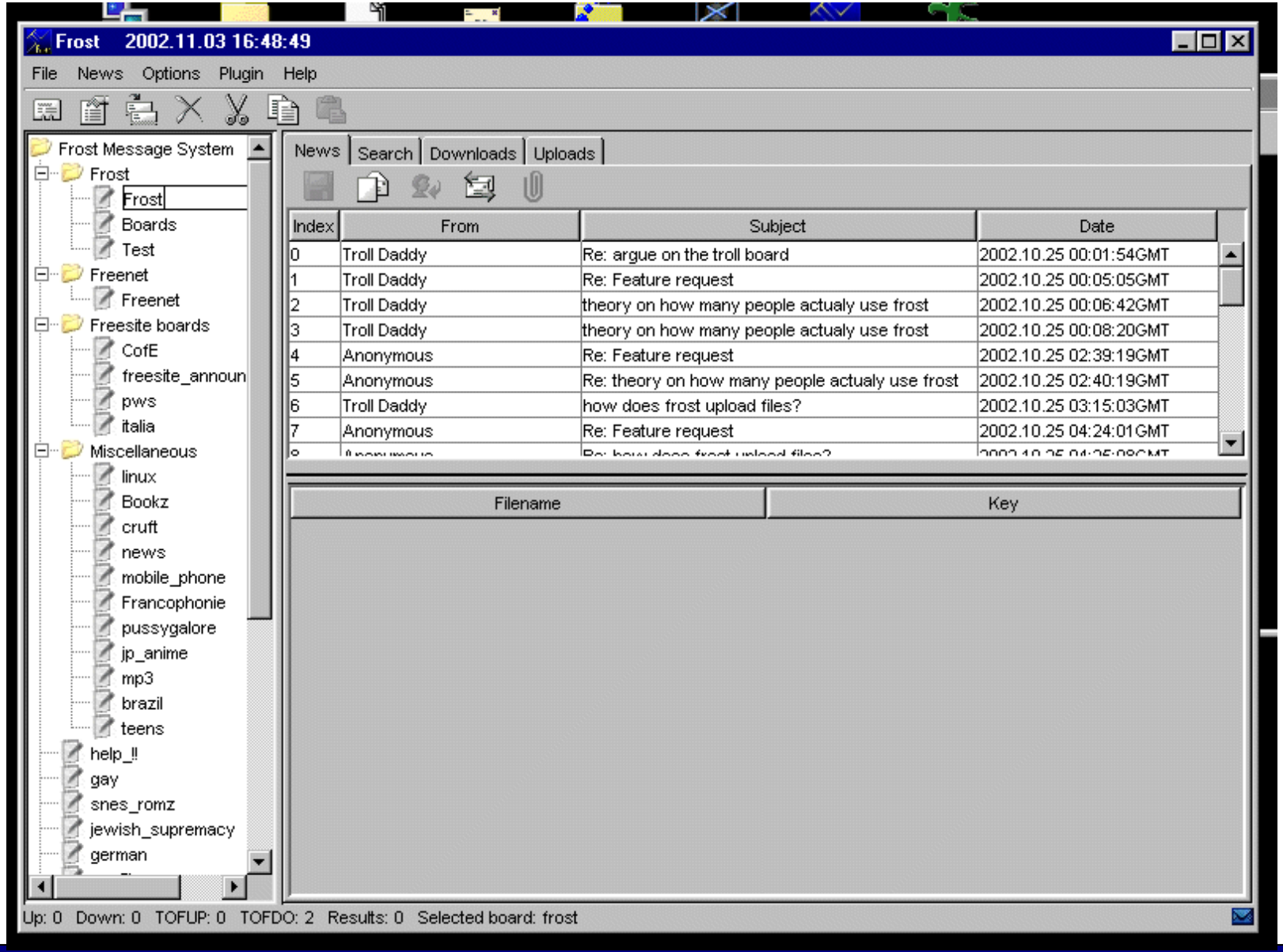


Frost

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



FUQUID

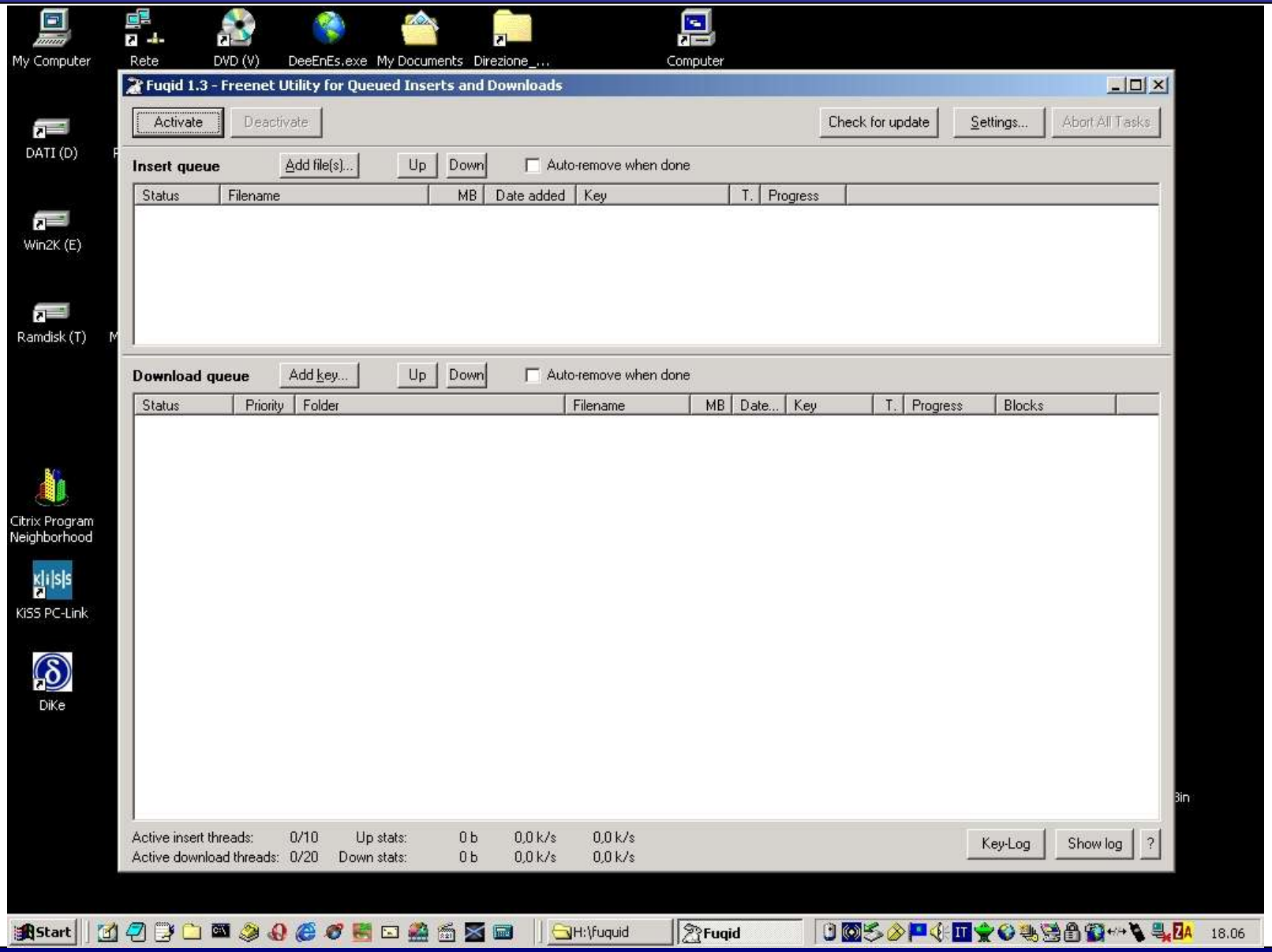
FUQUID; ahime' solo per windows, e' un tool per mass insertion/retrieval veramente potente e flessibile, nella sua semplicita' (fa una cosa sola e la fa bene)

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

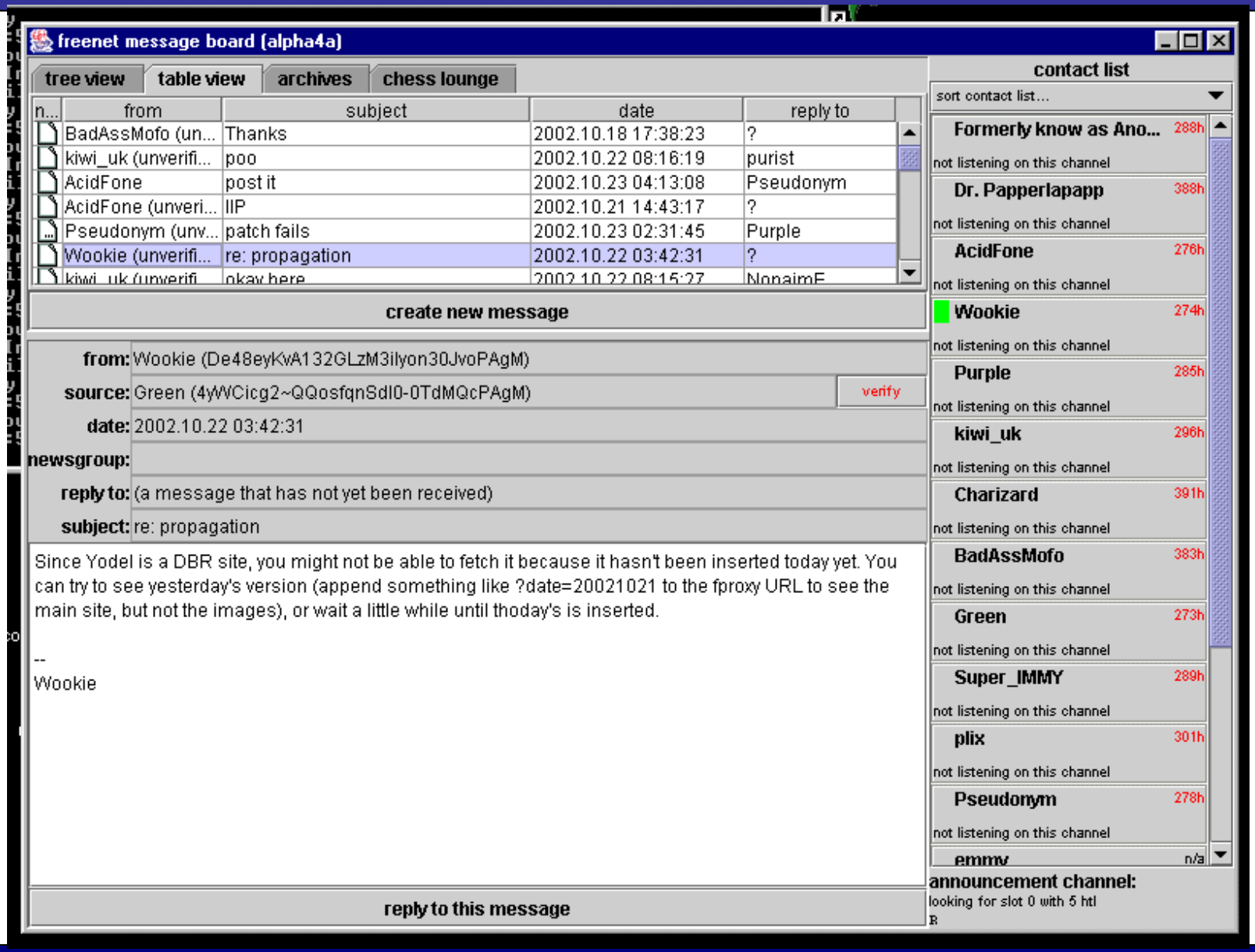


Freenet Message Board

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



Entropy

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

Ha una dimensione attuale dell'ordine dei 10 nodi

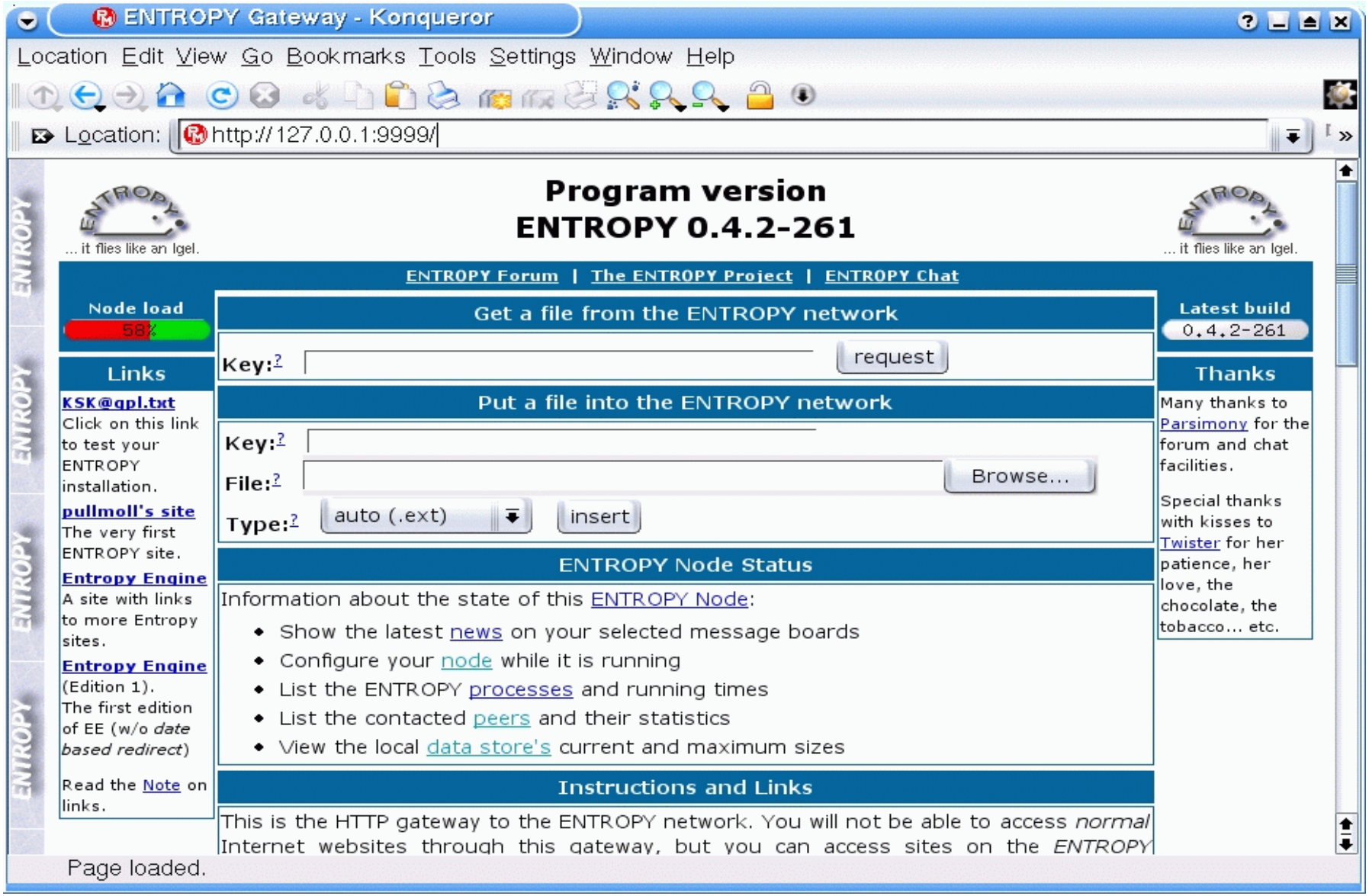
Ha contenuti stabili ma in piccola quantita'

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

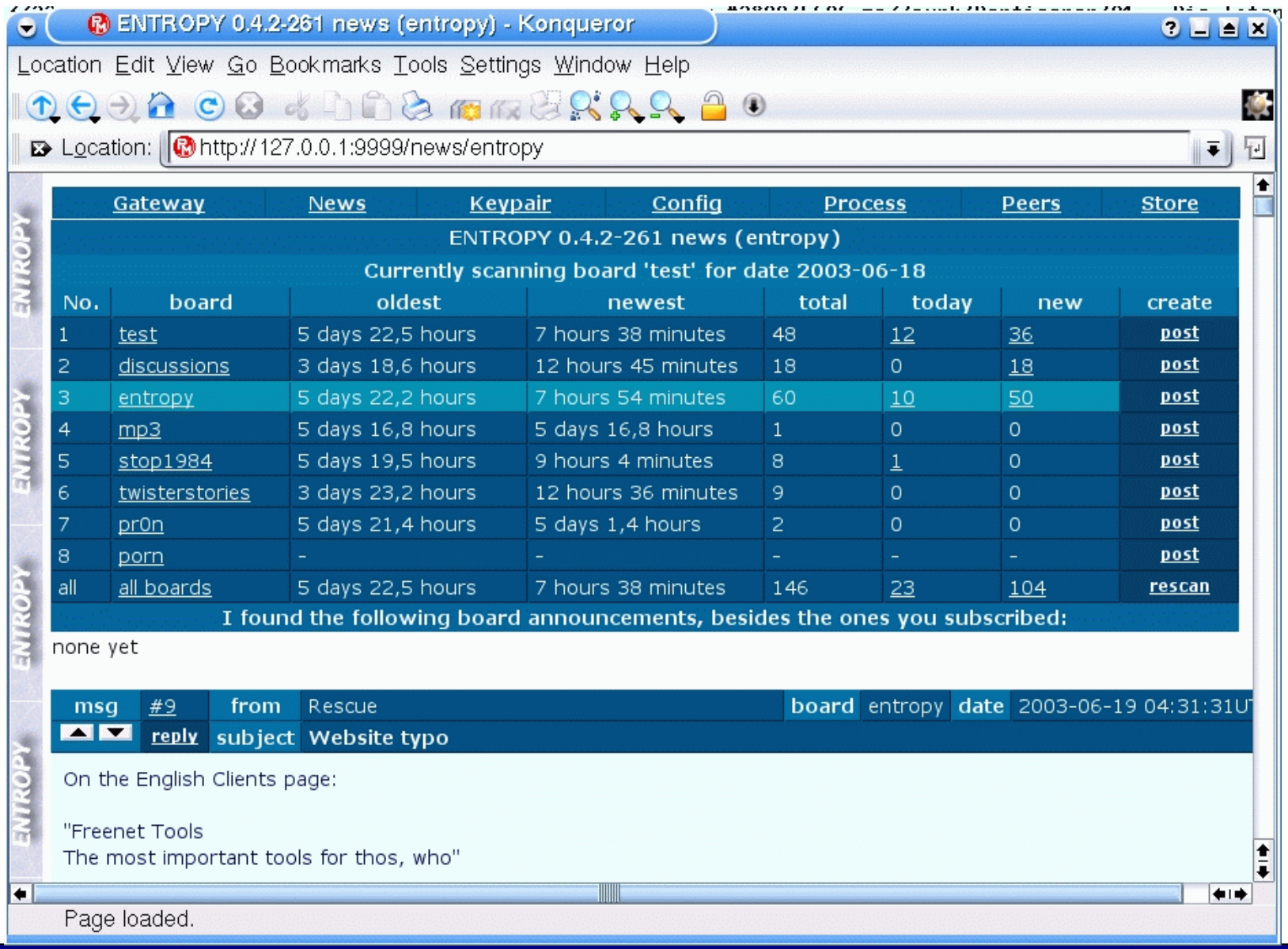
Ha una utility per l'inserimento di freesite a linea comandi, e funzionalita' interne avanzate come una BBS

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 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 test 5 days 22,5 hours 7 hours 38 minutes 48 12 36 post
2 discussions 3 days 18,6 hours 12 hours 45 minutes 18 0 18 post
3 entropy 5 days 22,2 hours 7 hours 54 minutes 60 10 50 post
4 mp3 5 days 16,8 hours 5 days 16,8 hours 1 0 0 post
5 stop1984 5 days 19,5 hours 9 hours 4 minutes 8 1 0 post
6 twisterstories 3 days 23,2 hours 12 hours 36 minutes 9 0 0 post
7 pr0n 5 days 21,4 hours 5 days 1,4 hours 2 0 0 post
8 porn - - - - - post
all all boards 5 days 22,5 hours 7 hours 38 minutes 146 23 104 rescan
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
reply subject Website typo
On the English Clients page:
"Freenet Tools
The most important tools for thos, who"
Page loaded.

GnuNet

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.

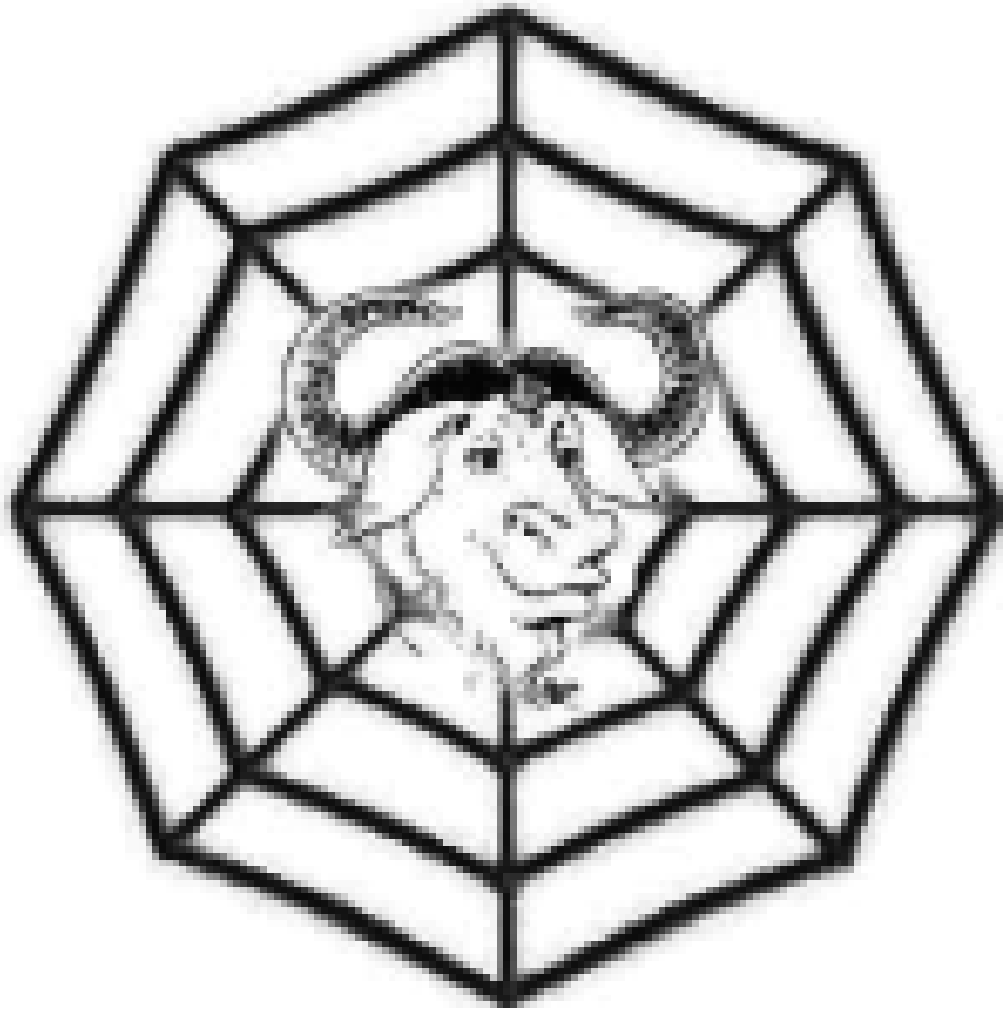
La dimensione della rete non e' stimabile, ma e' presente una certa quantita' di contenuti. E' sostanzialmente la cosa piu' vicina ad una Gnutella anonimizzata

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

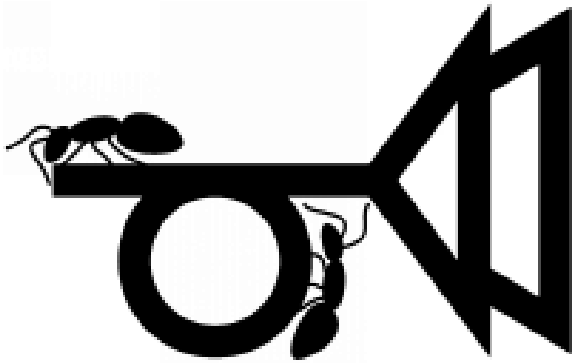
Non c'e' interfaccia grafica (anche se esiste un add-on di interfaccia gnunet-gtk) pero' c'e' comunque .....

GnuNet

.... un bel logo!



Mute



Mute e' una rete di proxy anonimizzanti

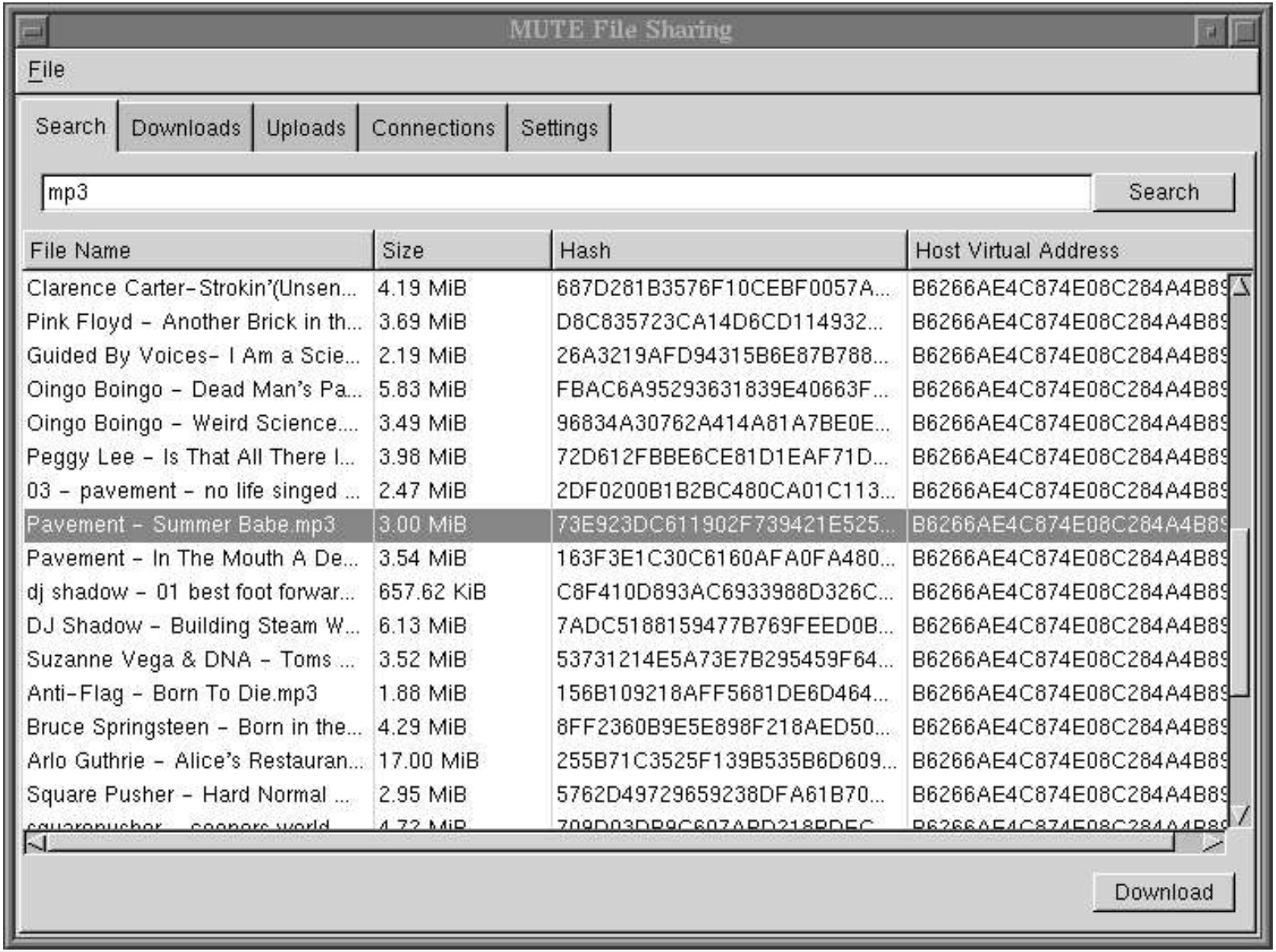
scritta in C

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; multipiattaforma . Dategli qualche soldo !

Mute



Ma allora....

cosa dobbiamo usare ?

Ricetta semplice

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 !

Cosa e' 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 Distribuited Anonymous Information Storage and Retrieval System"
I.Clarke et al.

… e tradotto in italiano ?

“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"

Cosa trovo su Freenet ?

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."

Obbiettivi 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)

Modelli Peer-to-peer

- 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

Caratteristiche

- **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

Caratteristiche

- **Routing adattativo** - il grafo delle connessioni logiche tra i nodi evolve nel tempo verso una stabilita' ed efficienza maggiore, ed i nodi stessi si specializzano .
- **Comportamento non deterministico** - il funzionamento di Freenet non e' 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

Caratteristiche

- **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.

Caratteristiche

- **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

FEC splitfile

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.

FEC splitfile - esempio

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

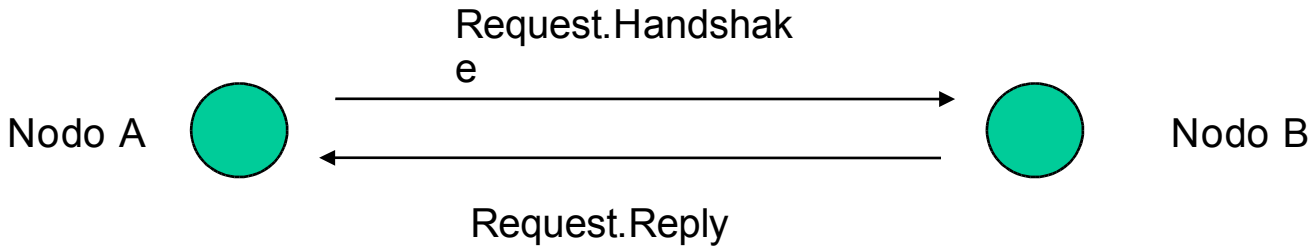
Come funziona Freenet

- I nodi comunicano tra loro con un semplice protocollo connection-oriented chiamato FNP (Freenet Network Protocol), normalmente realizzato sopra il tcp/ip

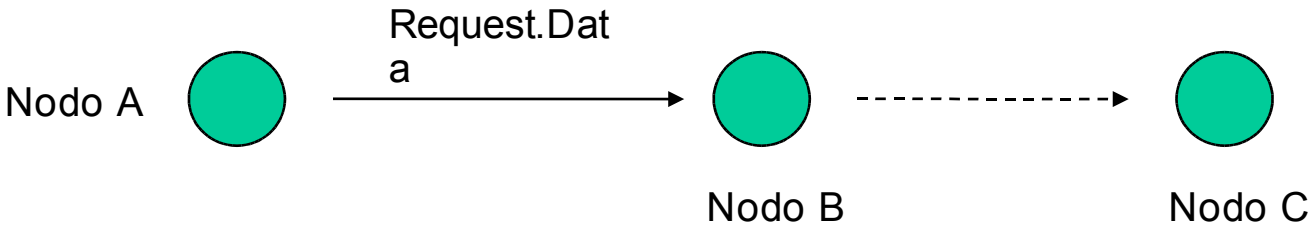
- I client applicativi (e.g. Frost) che vogliono utilizzare i servizi Freenet di un nodo locale utilizzano un altro protocollo chiamato FCP (Freenet Client Protocol)

Come funziona Freenet

Fase di Handshake

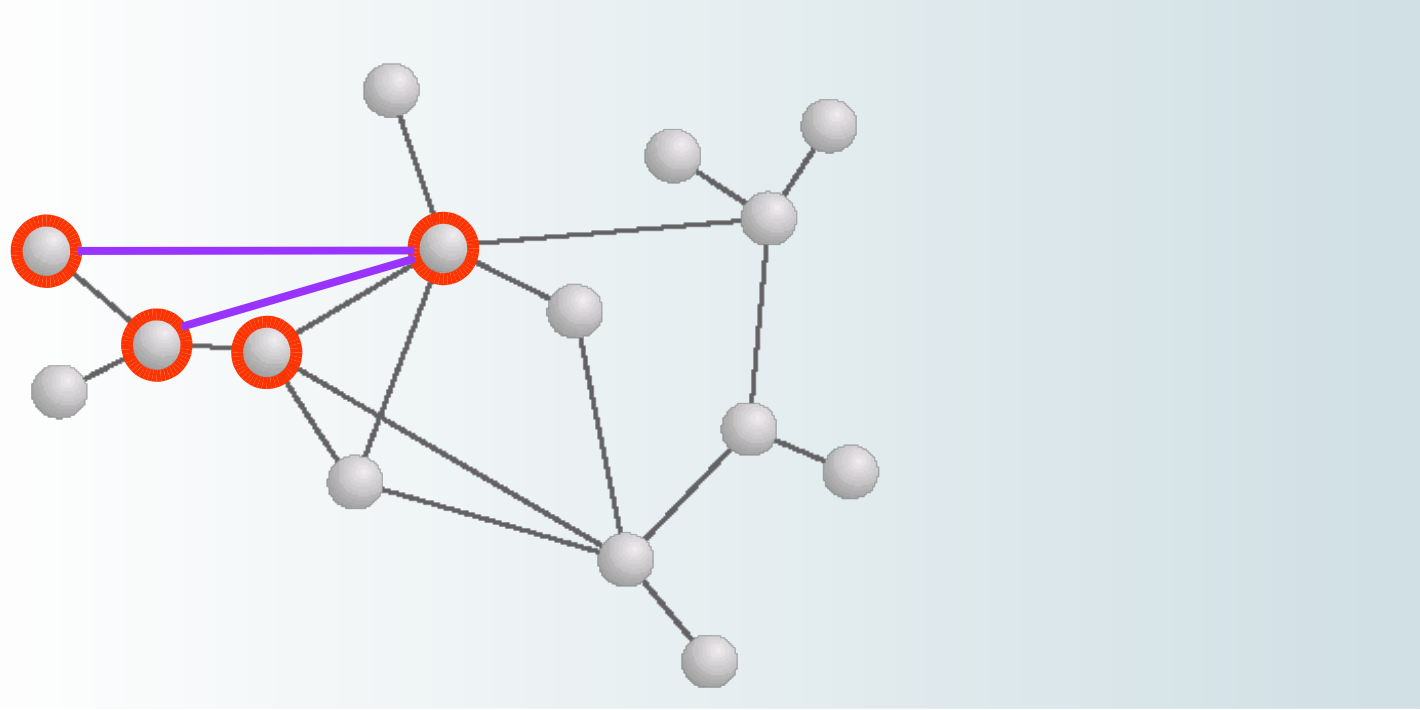


Fase di richiesta dati



Come funziona Freenet

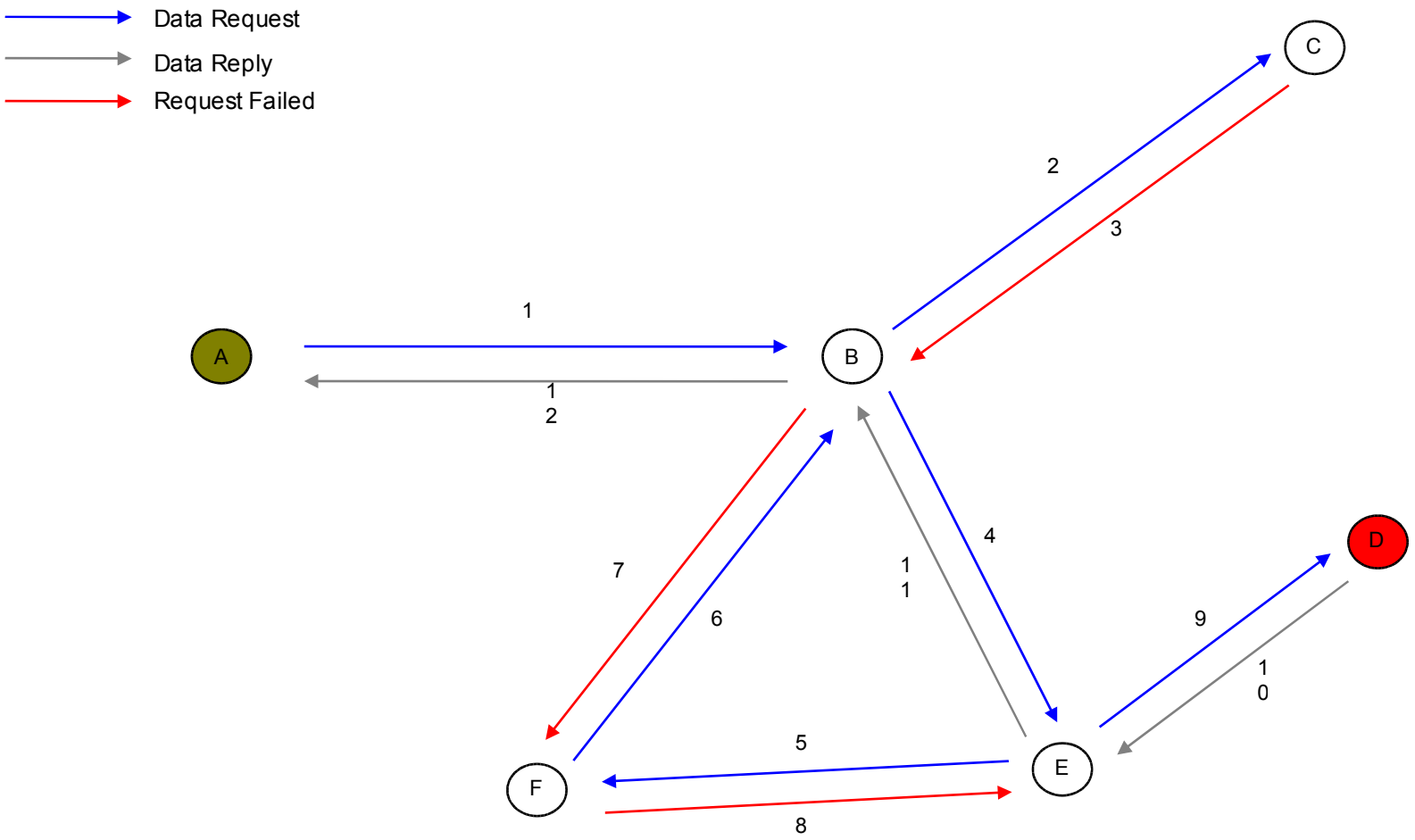
- I nodi comunicano tra loro sulla base di una conoscenza locale dinamica dei nodi limitrofi
- Ogni nodo richiede una chiave, nell'ordine, ai nodi limitrofi



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



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 ripudiabilita’ di un’eventuale attribuzione di responsabilita’ 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, poiche’ i nodi pubblicizzano il segmento di spazio delle chiavi in cui sono “specializzati”

Meccanismi crittografici

Le chiavi di Freenet

- 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

La chiave KSK

- 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…..

La chiave SSK

- 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

Bibliografia

- "**Freenet : A Distribuited 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**

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@Dgg5lJQu-WO905TrIZ0LjQHXDdIPAgM/pws/14//

mirror: **http://www.winstonsmith.it**