



Freenet / Hyphanet: the long game

Whenever a new type of data breach becomes known,
some remember the **Freenet project**,
but few really know it.
Let's change that.

Vision, fundamentals and innovations

dr Arne Babenhausserheide





Why Freenet?

Whenever new types of data breaches become known, some remember the Freenet project, but few really know it.

Therefore, this talk provides an introduction to Freenet 's capabilities today.¹ It explains why Freenet exists and what vision guides all of its advancements, provides a basic understanding of how it works and the tools it offers, and shows the advances it has made over the last 15 years.

A distributed network to protect free communication, a structure without centralized power, a place to coordinate the work for digital freedom if the battles for a free network should be temporarily lost, a plan B for an internet where communication works without itself to sell constantly.

A recording of this lecture is available at the [SUMA Congress 2022 Videos](#).



Why Freenet?

Why Freenet?

“There is now no shield from forced exposure. . . The foundation of Groklaw is over. . . the Internet is over” – Groklaw, [Forced](#)

[Exposure \(2013-08-20\)](#)



Why Freenet?

Why me?

- Developing peer-to-peer networks for 20 years
- Freenet release manager since 2017
- [Lecture on distributed systems at the DHBW](#)
- [Received the SUMA Award for Freenet in 2015](#)

Why Freenet?



functionality



tools



innovations



Summary



Why Freenet?

Questions

- Why is there Freenet?
- How does Freenet work?
- What does Freenet enable?
- What has changed?



What does Freenet offer?

Why Freenet? What's the point?

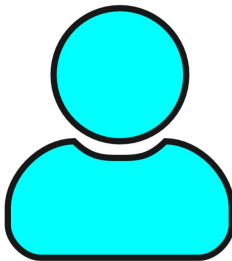
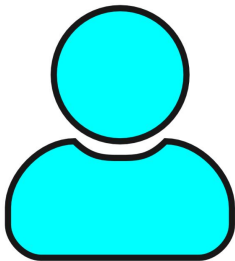
- Communicate confidentially or pseudonymously.
- Technical cornerstone for protection against censorship.
- In return: High level of data protection.

“Covers the needs for protection expected from a secure data broker for Multi-Party Data Exchange in IoT for Health” (?, Uni Bern) — [Article](#)



What does Freenet offer?

Talking to friends: Confidential



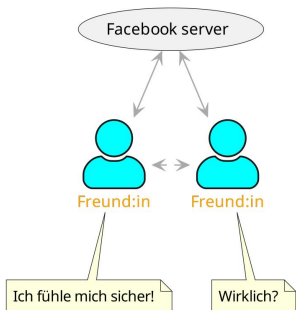
Freund:in

Freund:in



What does Freenet offer?

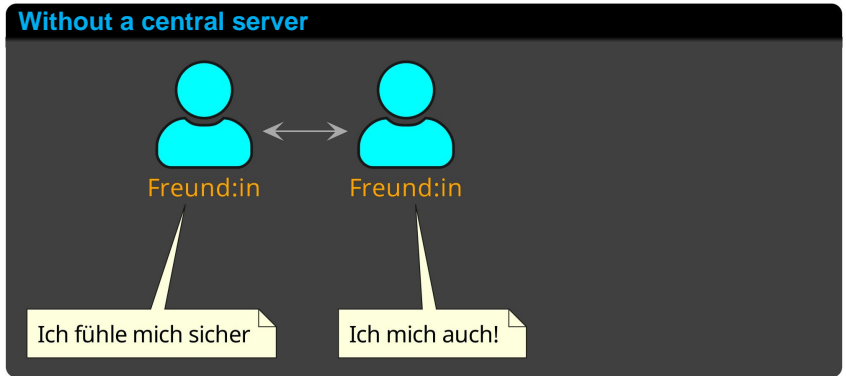
talk like with . . .





What does Freenet offer?

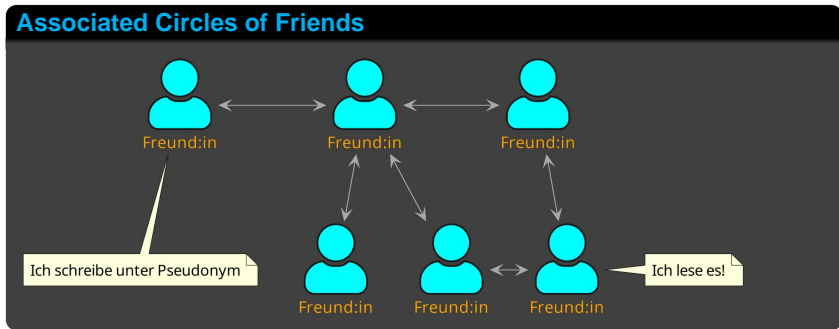
· · · but without the monitoring server





What does Freenet offer?

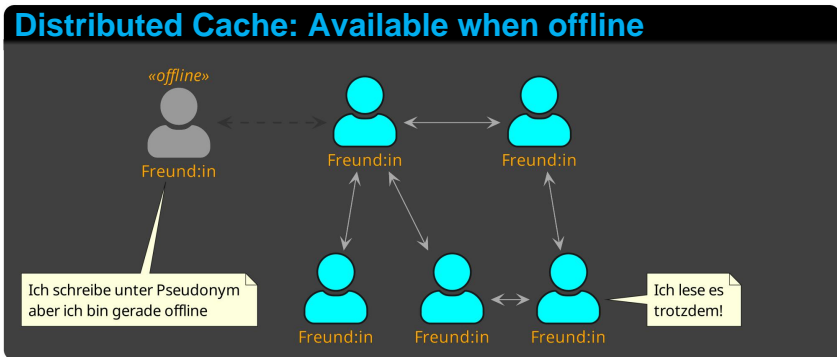
Talk to strangers





What does Freenet offer?

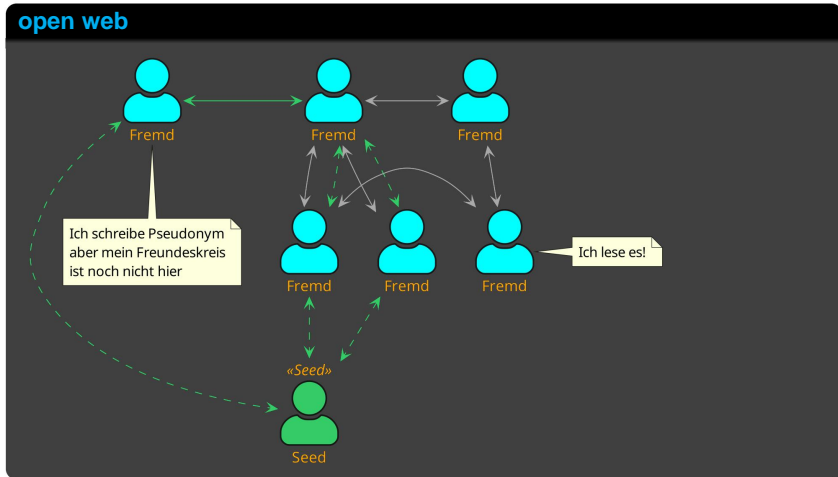
Without servers





What does Freenet offer?

Pioneer in the Circle of Friends?



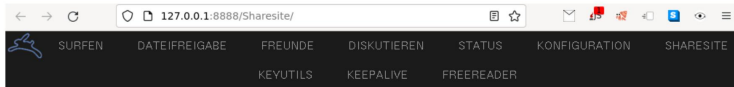
dr Arne Babenheuser



What does Freenet offer?

Throw in: We're launching a Sharesite page!

<http://127.0.0.1:8888/sharesite>



Your Sharesite freesites

Create a new freesite

You do not have any Sharesite freesites yet. Creating freesites with links to all your favorite files, images and other freesites is an easy and fun way to help spreading the content you love on Freenet. Sharesite freesites is also a practical way to collect everything you inserted yourself.

Backup and restore (advanced users)

[Get backup of all freesites](#)

The restored freesites will be added after the current ones. Nothing is overwritten. You will experience problem if you have multiple copies of the same freesite, delete all copies but the one you want to keep.

Browse... No file selected.

Restore backup

dr Arne Babenhauerheide

 Freenet / Hyphanet: the long game 



why do we need this

why do we need this

reflection of the world

Through the increasing blending of digital life with analogue analogue communication becomes a reflection of the limited life on the web.

— Arne Babenhauserheide, [Suma eV Congress 2015 :-\)](#)

The network is spreading

Without pseudonymous communication and without confidential communication on the Internet, we will also lose them in the analogue world.



why do we need this

analog communication

Confidential



On a small scale
Direct contact



why do we need this

analog communication

Confidential



On a small scale
Direct contact

Officially



self-censorship
foreign determined



why do we need this

analog communication

Confidential



On a small scale
Direct contact

Officially



self-censorship
foreign determined

pseudonym



Always on guard
Source protection!



why do we need this

analog communication

In the monitored network

Officially



self-censorship
foreign determined

Key word: panopticon



why do we need this

The Dystopia: Loss of Press Freedom

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, "[Fear of Freedom](#)" (1995)

The aim of the Freenet project is to ensure the free flow of information guarantee.

Even when criminals work as journalists and their threaten sources.



why do we need this

technology and politics

Tech alone is not enough

Total monitoring and control is possible.

tech and politics

Technology provides the basis on which politics can work: make surveillance and censorship so complex and expensive that we can win the political battle.

Politics alone is not enough

When surveillance and censorship are trivial, they are used.

The NSA surveillance doesn't scale.

– Constanze Kurz (EuroPython 2014)



why do we need this

freedom from censorship

- Core of everything in Freenet
- All possibilities and developments serve this goal
- Article 5 GG: there is no censorship



why do we need this

Conclusions: freedom of domination

Nobody should have power over the communication of others. Some of the Risks for communication:

Direct censorship removes posts by threat or deletion

Bullying or baiting shuts people out and drives them out

Flooding with irrelevant things makes important untraceable

Disruption of the culture of conversation prevents the evolution of ideas



Questions

Doesn't that need moderation?

Freenet enables moderation without a central authority

Choose who can block for you.

If your pseudonymous circle of friends blocks a pseudonym, it will be for automatically make you invisible as well, unless you explicitly have it unlocked.

The anti-spam system scales better than spam. Even without an army exploited content moderation teams from low-wage countries (further:

[Arte: "The Cleaners"](#)).

Today's distributed platforms [are slowly catching up](#).



And rush?

Pseudonyms help the victims more than the perpetrators

Anyone who has to fear violence cannot go public without a pseudonym communicate. Surveillance always helps the perpetrators.

People are more aggressive under real names

Results show that in the context of online firestorms, non anonymous individuals are more aggressive compared to an anonymous individuals

- Katja Rost et al.: [Digital Social Norm Enforcement: Online firestorms in social media](#)

Read more: [Mandatory real names harm online communication](#)



Questions

And propaganda?

Propaganda wants domination

Q: "Can I prevent someone from commenting in my thread?"

A: "You did understand the part about no power over others?"

Domination is centralized power

Tik Tok's algorithms are driving people into a maze of disinformation.

Deciding what influences we expose ourselves to is a question

Communicative self-determination.



And radicalization?

Social media does everything — and worse — that people ever do
Freenet feared. Except access to explosive information where
people really need them.

And besides being able to verbally stubbornly defy aggressive propagandists
offer without putting yourself in danger.



Questions

Summary

- freedom from censorship
- data protection
- Confidential Communication
- pseudonyms

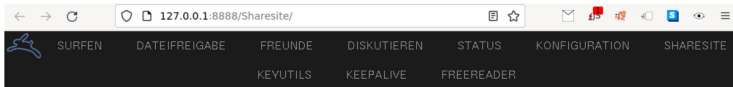
A technical pillar for informational self-determination.



Questions

Throw in: Our Sharesite!

<http://127.0.0.1:8888/sharesite>



Your Sharesite freesites

Create a new freesite

You do not have any Sharesite freesites yet. Creating freesites with links to all your favorite files, images and other freesites is an easy and fun way to help spreading the content you love on Freenet. Sharesite freesites is also a practical way to collect everything you inserted yourself.

Backup and restore (advanced users)

[Get backup of all freesites](#)

The restored freesites will be added after the current ones. Nothing is overwritten. You will experience problem if you have multiple copies of the same freesite, delete all copies but the one you want to keep.

Browse... No file selected.

Restore backup

dr Arne Babenhauerheide

 Freenet / Hyphanet: the long game 



Why do I want to know?

How Freenet works

- basic concepts
- interfaces
- protective measures



Why do I want to know?

Why look at how it works?

- Source of Freenet's strengths
- Understanding necessary for efficiency



Why do I want to know?

unique selling propositions

- Friend-to-friend Darknet (plus Opennet)
- Serverless Hosting (Upload and Disappear)
- Stable pseudonyms (private key)
- Cryptography via links (easy to use)
- Decentralized spam resistance (tested; helps communication culture)
- Use-based lifetime (anonymous)

Convenient: Used by thousands for 23 years.



Why do I want to know?

basic concepts

- Access to data: decentralized and scale-free (small world)
- Referencing data via content hash or public Key
- Private and public keys as links
- Updates via versioning

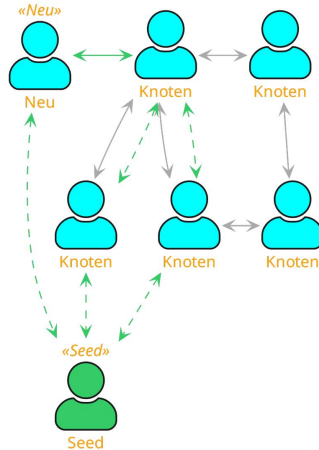


Started

Started

- Connect with friends1 (safer), or
- Connect to Seednode

1: High Security Mode: only with connect friends





Started

Small World / roughly scale-free network

- Connected to many nearby nodes and few distant ones
- 6 Degrees of Separation: Like letters about acquaintances
- Ring: Location is between 0.0 and 1.0
- Anyone who is at 0.3 knows people close to 0.3
- Realized at Opennet via the entrance
- With friend-to-friend about exchanging the location



data operations

Referencing Files: Key Types

- CHK: file by content
- SSK: Public/Private Key
 - USK: Upgradable
 - KSK: Shared password

CHKs are 32kiB, SSKs are 2kiB. Larger ones are trees of CHKs with SSK or CHK for the manifest.



data operations

Structure of key types

CHK@<routing>,<encryption>,<flags>/<name>/[optional-path]

SSK@<routing>,<encryption>,<flags>/<name>/[optional-path]

USK@<routing>,<encryption>,<flags>/<name>/<version>/[optional-path]

KSK@<password>

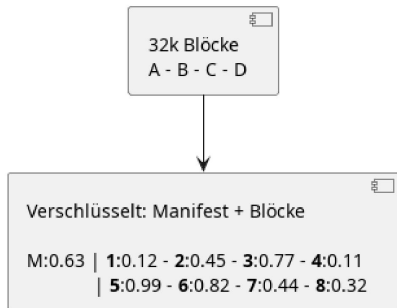
- CHK: [CHK@7ER. . . ,F2u. . . ,AAMC-8/fetchpull-lifetime realtime-success-count.png](#)
- SSK: [SSK@rQn. . . ,l1v. . . ,AQACAAE/gms-16/](#)
- USK: [USK@rQn. . . ,l1v. . . ,AQACAAE/gms/16/](#)
- KSK: [KSK@the-long-game](#)

Only <routing> is sent to the network. <encryption> remains local.

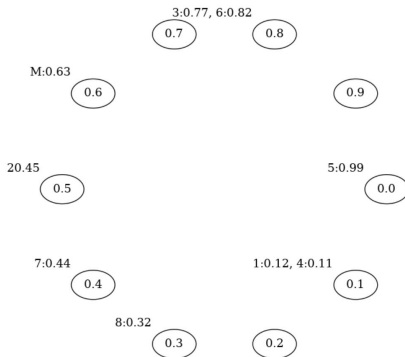


data operations

Split and upload files



Key is in the link (e.g. CHK).
Unlinked blocks not decryptable or
recognizable.

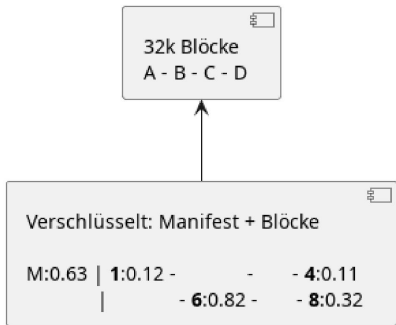


Overwrite blocks randomly.

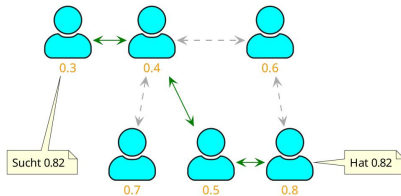


data operations

Find and merge blocks



Available while 50% of blocks
are discoverable.



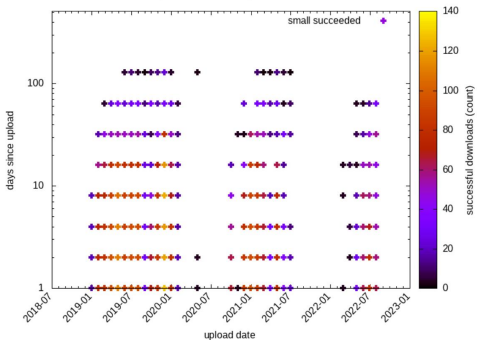
Routing in small-world network
about the positions of the friends of
friends (FOAF).



data operations

lifetime

fetchpull: lifetime: monthly success-count



Each access restarts the clock.

dr Arne Babenhausserheide

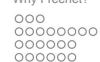


data operations

Right to be forgotten?

- lifetime in the public interest
- Right to be forgotten in technology
- Privacy friendly

Technical background: most important question in distributed storage networks:
how do we decide what to delete?



data operations

And update info? In Constant Time: Date Hints

- User: SSK@.../my-page-1/... ÿ
SSK@.../my-page-2/activelink.png
- Developer: USK@.../my/page/1
 - SSK@[key]/[sitename]-DATEHINT-[year]

HINT

46

2013-7-5

DATEHINT-[year], DATEHINT-[year]-WEEK-[week],
DATEHINT-[year]-[month], DATEHINT-[year]-[month]-[day]



Binder

Folder in Freenet: manifest data

Status Configuration KeyUtils Key Explorer Site Explorer Spittle Explorer Extra Calculator FBlob Viewer Key Converter About Chat Shoeshop jFniki FlogHelper IRC Chat Freereader KeepAlive Sharesite	Explore a freenet key Display the top level chunk as hexprint or list the content of a manifest Freenetkey to explore: <input type="text" value="SSK@LHeuG-SU5ZvYQXTu8Y9mhjCYyQxB-m-W~ryElufr-2M,Ij9lOU1Wa~FQu7GFBf~ciwUbCwJ"/> <input type="button" value="Explore!"/> <input type="checkbox"/> auto open as manifest if possible <input type="checkbox"/> parse manifest recursive (include multilevel metadata/subcontainers) Hex display columns: <input type="text" value="32"/>
	Key: SSK@LHeuG-SU5ZvYQXTu8Y9mhjCYyQxB-m-W~ryElufr-2M,Ij9lOU1Wa~FQu7GFBf~ciwUbCwpTFv6mWzks1YuoxQk,AQACAAE/arnebab-org-413 (MetaData) <pre> 000000: F853 B284 2D91 482B 0001 0303 0000 0000 0756 7A95 AS45 9275 489F 4A41 C2A5 052F .S...H+.....Vz...uK.JA.../ 000020: 065F B44A F525 2B17 DAE4 D78B 7F14 8388 DE50 18A1 A416 1B09 8BAF F0F8 D83A 8250 _..J%+.....P.....:.. 000040: 80ED C3D0 4C45 9390 81F6 E99D A59A 7FD6 E9D5 A03E AE00 0000 1880 0000 0000 ...LE.....>..... 000060: 0000 0000 0000 0000 1800 0000 0000 0007 0001 0184 0003 02FF FFCF 6FB9 0878 A078S.l{...0...T...g...o..x.{ 000080: 0000A0: 2204 AEE5 40CB BC80 74C6 CAEF 578B 84A9 AC6E 329C B104 5621 FD ...M...t...W...D...V.. </pre>
	Decomposed metadata Metadata version 1 Document type: ArchiveManifest MIME Type: application/x-tar Flags: HasTopData

- One archive (tarball), transparent access



Binder

Folder in Freenet: As manifest

Explore a site

List the content of a manifest

Freenetkey to explore:

parse manifest recursive (include multilevel metadata/subcontainers)

Key: SSK@LHeuG-SU5ZvYQXTu8Y9mhjCYyQxB-m-W~ryElufr-2M,lj9l0U1Wa~FQu7GFBf~ciwUbCwpTFv6mWZks1YuoxQk,AQACAAE/arnebab-org-413 (Manifest)

	Type	Name	Size	Mime	Target
0-R	[s] SMF		(34 Items)		
0-0	[c] SYS	/		<NoMime>	->index.html
0-0	[c] AMR	/software		<NoMime>	.metadata-0

[USK@LHe. . . ,lj9. . . ,AQACAAE/arnebab-org/413/](#)

dr Arne Babenhausserheide



interfaces

interfaces

- browsers
- Distributed database for programs
- plugins



interfaces

the browser

- Typically accessed at <http://localhost:8888>
- [freenetbrowser](#) (automatically generated Firefox profile) for better Security
- Optimizations for pre-fetching and media streaming

<http://localhost:8888/USK@rQn...I1v...AQACAAE/gms/16/>



interfaces

External programs

- Server for forums/NNTP (FMS) and IRC (FLIP)
- GUI programs (jSite)

○○○
 ○○○○○○○○
 ○○○○○○
 ○○○○○○

○○○○
 ○○
 ○○○○○○
 ○○
 ○○○●○○○
 ○○○○○○

○○
 ○○○○
 ○○○○○
 ○○○

○○○○○○
 ○○
 ○○
 ○○○
 ○○

○○○

interfaces

External programming interfaces

- FCP: Freenet client protocol
 - HTTP-like: Key: value line by line, optional data bytes at the end
 - <https://github.com/freenet/wiki/wiki/FCPv2>
- libraries
 - Maintained: Java, Python
 - [Unmaintained](#) or experimental: ruby, go, C+
 - +
<https://github.com/freenet/wiki/wiki/Projects#libraries> Plugins
- <https://github.com/freenet/wiki/wiki/Plugin-API> github.com/freenet/wiki/wiki/Projects#plugins



interfaces

Interface: FCP

Async for programs:

- Put/Putdir/Get
- Subscribe to key
- control plugins

ClientHello

Name=My Client

ExpectedVersion=2.0

EndMessage

NodeHello

...

EndMessage

client put

URI=CHK@

UploadFrom=disk

Filename=/tmp/debian-dvd1.iso

Identifier=sarge-disk-1

Global=true

EndMessage



latency in practice

- Up to 2kiB, raw, realtime mode: <30s
- Large files, in manifest: ~5 min

real time

PriorityClass . 2 ;; high
 MaxRetries . 0 ;; default: 10
 RealTimeFlag . true
 DontCompress . true
 ExtraInsertsSingleBlock . 0
 ExtraInsertsSplitfileHeaderBlock . 0

Bulk

PriorityClass . 3 ;; medium
 RealTimeFlag . false
 DontCompress . false



interfaces

Interface: plugins

- Integrated into the web interface
- Weak abstraction
- Access to the inner workings (risky)
- Easiest start: Adjust existing plugin

Examples: [sun](#) or [share site](#)



Basics of communication via Freenet

- Entry: seed keys + captcha queue: KSK prefix
- Search: User-specific pages with links, update information
- Distribution: Gossip keys, just upload files
- Disturbance resilience: Web of Trust with slowly increasing visibility

Interjection: Constructive Spammers: <https://xkcd.com/810/>



protective measures

protective measures

- Data protection despite browser
- deniability
- spam protection



protective measures

Content Sanitizing: Protect from the browser

Browser and media player: Different threat scenario

• Filter content to avoid access to clearnet resources

Example: Reload album art of a radio show via URL.



protective measures

Deniability: That was someone else

- Have requests Hops to Live (HTL)
- Decreased by 1 with each step
- HTL 18 is only reduced on 50% of connections — choice persists for the duration of the connection
- Requests with HTL 18 can always be from another node come



protective measures

spam protection

WoT (Web of Trust): One of two practically used possibilities.
The other is FMS (Freenet Message System).

- ID = USK
- Trust -100 to 100
- Rank: distance \ddot{y} capacity
- Score: Sum of all ratings: trust * rank
- Scaled at 22 messages per day² (Dunbar number)

²

<https://www.draketo.de/english/freenet/deterministic-load-decentralized-spam-filter>



○○○
 ○○○○○○○○
 ○○○○○○
 ○○○○○○

○○○○
 ○○
 ○○○○○○
 ○○
 ○○○○○○○
 ○○○●○

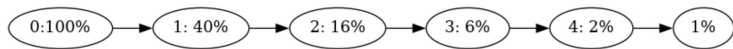
○○
 ○○○○
 ○○○○○
 ○○○

○○○○○○
 ○○
 ○○
 ○○
 ○○

○○○

protective measures

Capacity



- Rank 1 40%. rank 1: 100 trust, 40 points as a score.
- Rank 2 16%
- Rank 3 6%
- Rank 4 2%
- Rank 5 and below: 1%

Integer math: $2 * 6 / 100 = 0$.



protective measures

Summary

- circle of friends / Opennet,
- without server,
- key as a pseudonym,
- spam resistance,

- Small World
- Key types (CHK: content, USK: Upgradable, KSK: Password)
- Files are split redundancy
- lifetime after access frequency
- Binder
- interfaces
- protective measures

○○○
○○○○○○○○○
○○○○○○○
○○○○○○○

○○○○
○○
○○○○○○○
○○
○○○○○○○
○○○○○○○

●○
○○○○
○○○○○
○○○

○○○○○○○
○○
○○○
○○

○○○

tools

tools

Looks exciting, but what can I do practically with Freenet?



tools

the browser

- Browse
- Upload/Download
- plugins
- Friend-to-Friend Messages
- Bookmark with update info (5 min latency)
- Indexes with lists of pages (pseudonymous crawlers)



Concrete

Sharesite: Easiest pseudonymous publishing

<http://127.0.0.1:8888/sharesite>



Concrete

FMS and Flip: pseudonymous forums and IRC

- FMS: <http://127.0.0.1:8888/USK@0nnpnMrqZNKRCRoGojZV93UNHCMN-6UU3rRSAmP6jNLE,~BG-edFtdCC1cSH4O3BWdeIYa8Sw5DfyrSV-TKdO5ec,AQACAAE/fms/153/>
- FLIP: <http://127.0.0.1:8888/USK@pGQPA-9PcFiE3A2tCuCjacK165UaX07AQYw98iDQrNA,8gwQ67ytBNR03hNj7JU~ceeew22HVq6G50dcEeMcgks,AQACAAE/flip/17/>



Concrete

Sone: pseudonymous microblogging

Examples: [USK@nwa. . .](#), [DuQ. . .](#), [AQACAAE/sone/82/](#)



Concrete

Freemail: confidential email

[http://127.0.0.1:8888/USK@M0d8y6YoLpXOeQGxu0-IDg8sE5Yt~Ky6t~GPyyZe~zo, KlqljAj3~dA1Zf57VDljmp3vHUozndpxnH-P2RRugl,AQACAAE/freemail/8/](http://127.0.0.1:8888/USK@M0d8y6YoLpXOeQGxu0-IDg8sE5Yt~Ky6t~GPyyZe~zo,KlqljAj3~dA1Zf57VDljmp3vHUozndpxnH-P2RRugl,AQACAAE/freemail/8/)

○○○
○○○○○○○○○
○○○○○○○
○○○○○○○

○○○○
○○
○○○○○○○
○○
○○○○○○○
○○○○○

○○
○○○○
●○○○○
○○○

○○○○○○○
○○
○○○
○○

○○○

plugins

Shoeshop: Sneakernet with Freenet

[http://127.0.0.1:8888/USK@MYLAnId-ZEyXhDGGbYOa1gOtkZZrFNTXjFI1dibLj9E,Xpu27DoAKKc8b0718E-ZteFrGqCYROe7XBBI57pB4M,AQACAAE/shoe shop/3/](http://127.0.0.1:8888/USK@MYLAnId-ZEyXhDGGbYOa1gOtkZZrFNTXjFI1dibLj9E,Xpu27DoAKKc8b0718E-ZteFrGqCYROe7XBBI57pB4M,AQACAAE/shoe%20shop/3/)



plugins

jfniki: Wiki about Freenet

[http://127.0.0.1:
8888/USK@jZVIWXW-5nI4Bco~7IWbVazRzFQv78X9RnJsWWKdWm4,
Egn2limGcyEQ7mh~w~tRABGAYH6F4Zwoqfh8Cv7tVhY,AQACAAE/jFniki.
Index/12/Contributing.html](http://127.0.0.1:8888/USK@jZVIWXW-5nI4Bco~7IWbVazRzFQv78X9RnJsWWKdWm4,Egn2limGcyEQ7mh~w~tRABGAYH6F4Zwoqfh8Cv7tVhY,AQACAAE/jFniki.Index/12/Contributing.html)



plugins

KeyUtils: Technical details about uploads

<http://127.0.0.1:8888/KeyUtils/>



plugins

Keepalive: Keep some files available

<http://127.0.0.1:8888/KeepAlive/>



plugins

Freereader: Spread RSS via Freenet

<http://127.0.0.1:8888/freereader/feeds>



programs

pyFreenet: command line tools

<https://github.com/freenet/pyFreenet>

○○○
○○○○○○○○○
○○○○○○○
○○○○○○○

○○○○
○○
○○○○○○○
○○
○○○○○○○
○○○○○○○

○○
○○○○
○○○○○
●●○

○○○○○○○
○○
○○○
○○

○○○

programs

infocalypse: Version management via Freenet

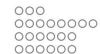
<https://hg.sr.ht/~arnebab/infocalypse/browse/Readme.txt>



programs

jSite: Upload websites with GUI

<http://127.0.0.1:8888/USK@1waTsw46L9-JEQ8yX1khjkfHcn--g0MIMsTIYHax9zQ,oYyxr5jyFnaTsVGDQWk9e3ddOWGKKnqEASxAk08MHT2Y,AQACAAE/jSite/15/>



innovations

innovations

What has happened in 15 years since the rewrite in 0.7.

One secret of success: relentless optimization.



innovations

Pitch black attack

In 2007, Christian Grothoff et al. found a vulnerability [and](#)
[proven](#).

Routing in the Dark: Pitch Black

Nathan S. Evans

Chris Gauthier Dickey

Christian Grothoff

Colorado Research Institute
for Security and Privacy

Department of Computer Science
University of Denver, USA
{natevans,chrisg.grothoff}@cs.du.edu



innovations

Pitch black solved

The mitigation

In 2021 we finally fixed them.



ÿ build 1490: “pitch black streaming” ÿ





innovations

WoT: Precisely updating and subscription-based



OPTIMIZING A DISTRIBUTED SPAM FILTER FOR FREENET

AKA

THE WEB OF TRUST DEVELOPER'S MANUAL

dr Arne Babenhauserheide



innovations

Better speed

- From 10kiB/s to 11MB/s (and more)
- Supports up to 15,000 subscriptions: updates within 5 minutes
see
- 30 second round trip time for chat



innovations

More HTML and CSS

- Support for parts of CSS3.
- Only where safety can be guaranteed.



multimedia

streaming audio

<http://127.0.0.1:8888/USK@~22K5. . . ,lwY. . . ,AQACAAE/stream radiocc-again/15/>

With live streaming:

<https://github.com/freenet/re-stream-into-freenet>

Example:

<http://127.0.0.1:8888/USK@j1V. . . , vs. . . ,AQACAAE/futo-ian interview-2022/3/>



multimedia

Video on demand

<http://localhost:8888/USK@rQn... ,1v... ,AQACAAE/gms/16/>

via <https://github.com/hyphanet/generate-media-site/>



mobile / cellphone

mobile-node: Freenet on Android

<https://freenet-mobile.github.io/app/>

dr Arne Babenhausser

 Freenet / Hyphanet: the long game 



mobile / cellphone

FreeChat: Chat on Android

<https://github.com/freenet/free-chat-2>

dr Arne Babenhausen

 Freenet / Hyphanet: the long game 



mobile / cellphone

icicles: connect messages from friends and nodes

<https://github.com/freenet/icicle>

dr Arne Babenhausen

 Freenet / Hyphanet: the long game 



open questions

open questions

- Better routing? (thanks to Pitch Black mitigation, new structures possible)
- Friend-to-friend connections via tor and i2p? (requires UDP!)
- Steganographic Transport Plugins (HTTP3?)
- Decentralized search in Freenet (Spider/Library needs optimization)



open questions

plans

No plan survives contact with reality, but a good plan provides set-pieces for the path you might actually walk.

- [High impact tasks](#)
- [High level roadmap](#) — structured by major version
- [Bug tracker roadmap](#) — very detailed but outdated



Summary

Summary 1

Why is there Freenet? Free communication

What does Freenet enable? Confidential and pseudonymous, without central Server, privacy-friendly database for distributed programs.

How does Freenet work? -

Entry: friend-to-friend (high security) or via Seed Node (Opennet)

Routing: Small world with FOAF routing

Files: split, encrypt, 100% redundancy, Available as long as used.



Summary

Summary 2

What has changed? Pitch Black solved, spam protection over
WoT/Sone and FMS, faster, IRC Chat,
Multimedia streaming, Android support, Sharesite
for the simplest websites, continuous optimization in
practical use.

○○○
 ○○○○○○○○
 ○○○○○○
 ○○○○○○

○○○○
 ○○
 ○○○○○○
 ○○
 ○○○○○○
 ○○○○○○

○○
 ○○○○
 ○○○○○○
 ○○○

○○○○○○
 ○○
 ○○○
 ○○

○○●

Summary

Use Freenet / Hyphanet!



- share site
- sun
- connection in circle of friends

freenetproject.org

other projects

- Tor with SecureDrop, e.g. at <https://taz.de/investigativ> (switches to the [Tor Browser](#), before you step aside!)

Sources

Images: Hare under GPL, all others cc by.

- <https://www.flickr.com/photos/anonymous-munich/3282278914> _
- <https://www.flickr.com/photos/gruenejugendffm/6272541036> _
- <https://www.flickr.com/photos/eppofficial/13564824463>
- <https://www.flickr.com/photos/maguide/6092244239>

sources 2

- <https://www.flickr.com/photos/okubax/15814107199>
- <https://www.flickr.com/photos/okubax/14248440483>
- <https://www.flickr.com/photos/okubax/15812839470>
- <https://www.flickr.com/photos/digitpedia/4709307610>

Sources 3

- <https://www.flickr.com/photos/focusc/4758319160>
- <https://www.flickr.com/photos/amitd/4693814169>
- commons.wikimedia.org/wiki/File:International_newspaper,_Rome_May_2
- commons.wikimedia.org/wiki/File:Edward_Snowden_2013-10-9_%281%29_%28cropped%29.jpg_

Sources 4

Licenses:

- <https://creativecommons.org/licenses/by/2.0/deed.en>
- <https://gnu.org/l/gpl>

(and newer versions)

References I

dr Arne Babenhausenheide



Freenet / Hyphanet: the long game

