

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
oooooo
ooo

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Freenet: the long game

Wann immer eine neue Art Datenschutzverletzung bekannt wird,
erinnern sich einige an das **Freenet Projekt**,
aber wenige kennen es wirklich.

Ändern wir das.

Vision, Grundlagen und Neuerungen

Dr. Arne Babenhauserheide





Warum 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)

Warum Freenet?

●●○
○○○○○○○
○○○○○○○
○○○○○

Funktionsweise

○○○○
○○
○○○○○○○
○○
○○○○○○○
○○○○○

Werkzeuge

○○
○○○○
○○○○○
○○○

Neuerungen

○○○○○○
○○
○○○
○○

Zusammenfassung

○○○

Warum Freenet?

Warum ich?

- Seit 20 Jahren in der Entwicklung von peer-to-peer Netzen
- Freenet Release-Manager seit 2017
- Vorlesung zu Verteilten Systemen an der DHBW
- 2015 den SUMA Award für Freenet entgegengenommen

Warum Freenet?

○○●
○○○○○○○
○○○○○○○
○○○○○

Funktionsweise

○○○○
○○
○○○○○○○
○○
○○○○○○○
○○○○○

Werkzeuge

○○
○○○○
○○○○○
○○○

Neuerungen

○○○○○○
○○
○○○
○○

Zusammenfassung

○○○

Warum Freenet?

Fragen

- Warum gibt es Freenet?
- Wie funktioniert Freenet?
- Was ermöglicht Freenet?
- Was hat sich geändert?



Warum Freenet? Was bringt es?

- Vertraulich oder pseudonym kommunizieren.
- Technischer Grundpfeiler für den Schutz gegen Zensur.
- Dafür: Hohes Datenschutzniveau.

“Covers the needs for protection expected from a secure data broker for Multi-Party Data Exchange in IoT for Health” (Benoist and Sliwa, 2020, Uni Bern) — [Artikel](#)

Warum Freenet?

ooo
o●ooooo
ooooooooo
ooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
ooooo
ooo

Neuerungen

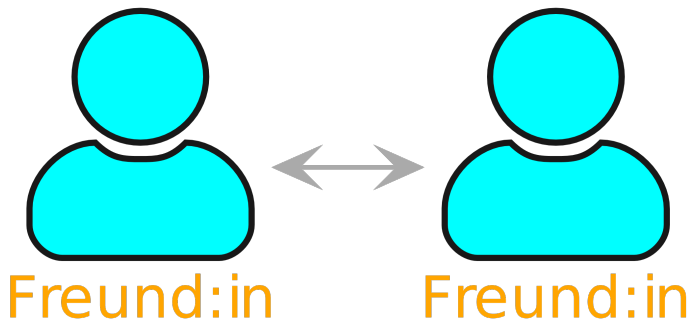
oooooo
oo
ooo
oo

Zusammenfassung

ooo

Was bietet Freenet?

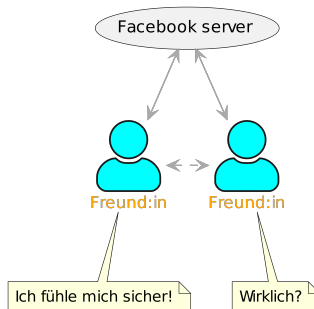
Im Freundeskreis sprechen: Vertraulich





Was bietet Freenet?

Sprechen wie mit ...



ooo
ooo●oooo
ooooooooo
ooooooooo

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

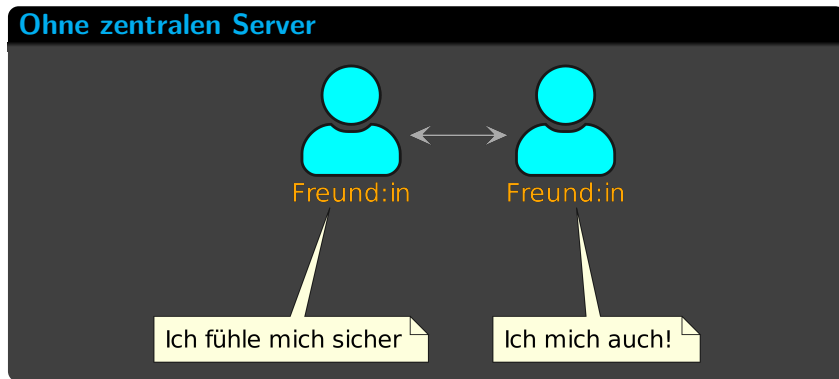
oo
oooo
oooooo
ooo

oooooo
oo
oo
oo

ooo

Was bietet Freenet?

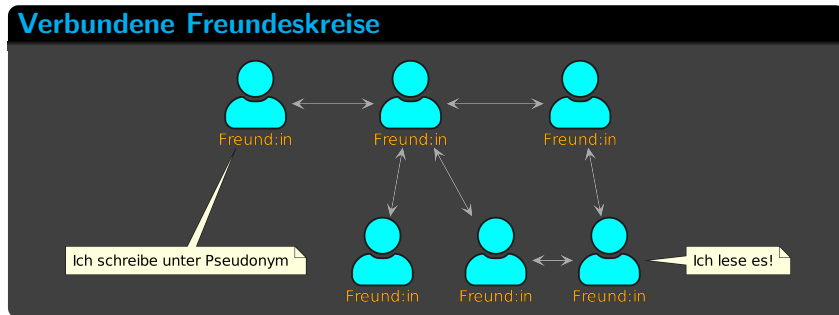
... aber ohne den Überwachungs-Server





Was bietet Freenet?

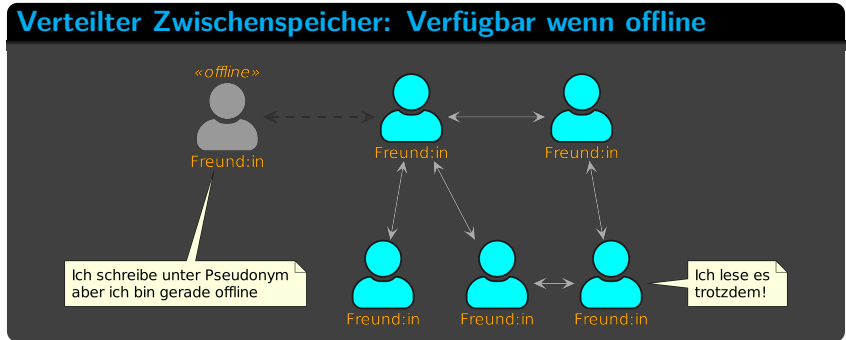
Mit Fremden sprechen





Was bietet Freenet?

Ohne Server



Warum Freenet?

ooo
oooooooo●o
ooooooooo
ooooooooo

Funktionsweise

ooooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
ooooo
oooooo
ooo

Neuerungen

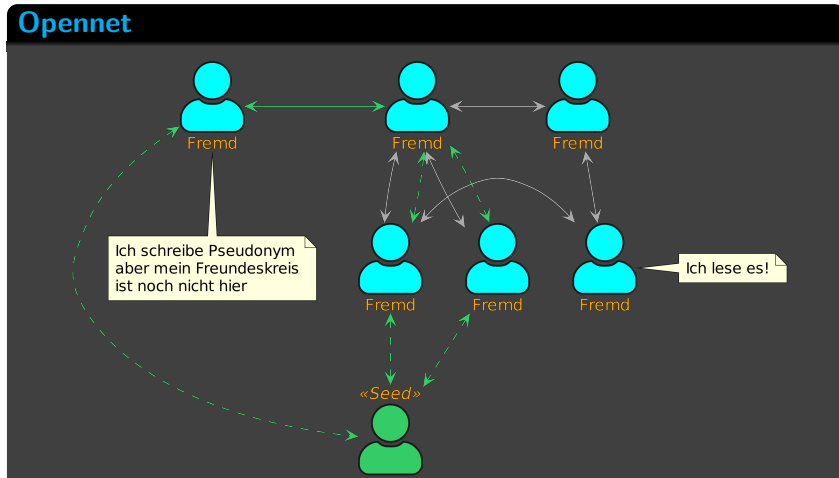
oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Was bietet Freenet?

Pionier im Freundeskreis?



Dr. Arne Babenhauserheide

 Freenet: the long game 

Warum Freenet?



Funktionsweise



Werkzeuge



Neuerungen



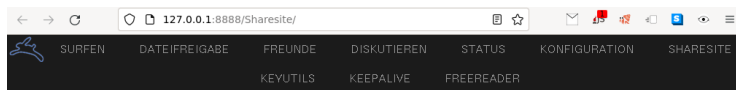
Zusammenfassung



Was bietet Freenet?

Einwurf: Wir starten eine Sharesite-Seite!

<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.

Dr. Arne Babenhauserheide

 Freenet: the long game 



Warum brauchen wir das?

Warum brauchen wir das?

Spiegelbild der Welt

Durch die steigende Vermengung des digitalen Lebens mit dem Analogen wird Analoge Kommunikation zu einem Spiegelbild des beschränkten Lebens im Netz.

— Arne Babenhauserheide, [Suma e.V. Kongress 2015 :-\)](#)

Das Netz verbreitet sich

Ohne pseudonyme Kommunikation und ohne vertrauliche Kommunikation im Internet, werden wir sie auch in der Analogen Welt verlieren.

Warum Freenet?

ooo
oooooooo
o●ooooo
oooooo

Funktionsweise

oooo
oo
oooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
ooooo
ooo

Neuerungen

oooooo
oo
ooo
oo

Zusammenfassung

ooo

Warum brauchen wir das?

Analoge Kommunikation

Vertraulich



Im kleinen Rahmen Direkter Kontakt

Dr. Arne Babenhauserheide

 Freenet: the long game 

Warum Freenet?

○○○
○○○○○○○
○●○○○○○
○○○○○

Funktionsweise

○○○○
○○
○○○○○○○
○○
○○○○○○○
○○○○○

Werkzeuge

○○
○○○○
○○○○○
○○○

Neuerungen

○○○○○○
○○
○○○
○○○
○○

Zusammenfassung

○○○

Warum brauchen wir das?

Analoge Kommunikation

Vertraulich



Offiziell



Im kleinen Rahmen
Direkter Kontakt

Selbstzensur
Fremdbestimmt

Dr. Arne Babenhauserheide

 Freenet: the long game 

Warum Freenet?

ooo
ooooooooo
o●ooooo
oooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
oooooo
ooo

Neuerungen

oooooo
oooo
ooo
ooo
oo

Zusammenfassung

ooo

Warum brauchen wir das?

Analoge Kommunikation

Vertraulich



Offiziell



Pseudonym



Im kleinen Rahmen
Direkter Kontakt

Selbstzensur
Fremdbestimmt

Stetig auf der Hut
Quellenschutz!



Warum brauchen wir das?

Analoge Kommunikation

Im Überwachten Netz

Offiziell



Selbstzensur
Fremdbestimmt



Warum brauchen wir das?

Die Dystopie: Verlust der Pressefreiheit

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)

Das Ziel des Freenet-Projektes ist es, den freien Informationsfluss zu gewährleisten.

Auch dann noch, wenn Kriminelle journalistisch Arbeitende und ihre Quellen bedrohen.



Warum brauchen wir das?

Technik und Politik

Tech alleine reicht nicht

Totale Überwachung und
Kontrolle sind möglich.

Politik alleine reicht nicht

Wenn Überwachung und
Zensur trivial sind, werden sie
genutzt.

Tech und Politik

Technologie liefert die Grundlage, auf der Politik arbeiten kann:
Überwachung und Zensur so aufwändig und teuer machen, dass
wir den politischen Kampf gewinnen können.

The NSA surveillance doesn't scale.
– Constanze Kurz (EuroPython 2014)



Warum brauchen wir das?

Die Vision: Ziele des Freenet Projekts

*The specific purpose of this corporation is to assist in developing and disseminating **technological solutions** to further the **open and democratic distribution of information** over the Internet or its successor electronic communication networks or organizations. It is also the purpose of this organization to guarantee consenting individuals the **free, unmediated, and unimpeded reception and impartation of** all intellectual, scientific, literary, social, artistic, creative, human rights, and cultural **expressions, opinions and ideas** without interference or limitation by or service to state, private, or special interests. It is also the purpose of this organization to educate the world community and be an advocate of these purposes. — The Freenet Project Inc, a 501(c)(3) non-profit (EIN 95-4864038) <https://freenetproject.org/pages/donate.html>*



Warum Freenet?

○○○
○○○○○○○○
○○○○○○●○
○○○○○○

Funktionsweise

○○○○
○○
○○○○○○○
○○
○○○○○○○○
○○○○○○

Werkzeuge

○○
○○○○
○○○○○
○○○

Neuerungen

○○○○○○
○○
○○○
○○

Zusammenfassung

○○○

Warum brauchen wir das?

Zensurfreiheit

- Kern von allem in Freenet
- Alle Möglichkeiten und Entwicklungen dienen diesem Ziel
- Artikel 5 GG: eine Zensur findet nicht statt



Warum brauchen wir das?

Folgerungen: Herrschaftsfreiheit

Niemand darf Macht über die Kommunikation anderer haben.

Einige der Risiken für Kommunikation:

Direkte Zensur entfernt Beiträge durch Drohung oder Löschung

Schikane oder Hetze schließt Leute aus und treibt sie raus

Fluten mit Irrelevantem macht Wichtiges unauffindbar

Zerrüttung der Gesprächskultur verhindert Evolution von Ideen



Braucht das nicht Moderation?

Freenet ermöglicht Moderation ohne zentrale Macht

Wähle selbst, wer für dich blocken kann.

Wenn dein pseudonymer Freundeskreis ein Pseudonym blockt, wird es für dich automatisch auch unsichtbar, es sei denn, du hast es explizit freigeschaltet.

Das Anti-Spam-System skaliert besser als Spam. Auch ohne ein Heer ausgebeuteter Content-Moderationsteams aus Billiglohnländern (weiter: [Arte: „The cleaners“](#)).

Heutige verteilte Plattformen [ziehen langsam nach](#).



Und Hetze?

Den Opfern helfen Pseudonyme mehr als den Tätern

Wer Gewalt fürchten muss, kann ohne Pseudonym nicht öffentlich kommunizieren. Überwachung hilft so immer den Tätern.

Unter Klarnamen sind Leute aggressiver

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

- Katja Rost et al.: *Digital Social Norm Enforcement: Online Firestorms in Social Media*

Weiterlesen: [Klarnamenspflicht schadet der Online-Kommunikation](#)



Und Propaganda?

Propaganda will Herrschaft

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

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

Herrschaft ist zentralisierte Macht

Tik Toks Algorithmen treiben Leute in ein Labyrinth aus
Desinformation.

Selbst zu entscheiden, welchen Einflüssen wir uns aussetzen, ist eine
Frage Kommunikativer Selbstbestimmung.



Und Radikalisierung?

Soziale Medien machen alles — und schlimmeres — was Leute jemals bei Freenet befürchtet haben. Außer Zugriff auf brisante Informationen wo Leute sie wirklich bräuchten.

Und außer der Möglichkeit, aggressiven Propagandisten verbal die Stirn zu bieten, ohne sich in Gefahr zu bringen.



Zusammenfassung

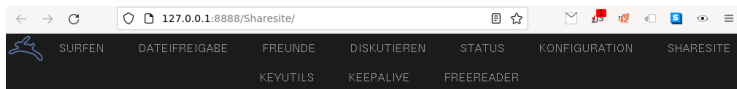
- Zensurfreiheit
- Datenschutz
- Vertrauliche Kommunikation
- Pseudonyme

Eine technische Säule für Informationelle Selbstbestimmung.



Einwurf: Unsere 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.

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

●ooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
ooooo
ooo

Neuerungen

oooooo
oo
ooo
oo

Zusammenfassung

ooo

Warum will ich das wissen?

Funktionsweise von Freenet

- Grundkonzepte
- Schnittstellen
- Schutzmaßnahmen

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

o●ooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
ooooo
ooo

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Warum will ich das wissen?

Warum Funktionsweise betrachten?

- Quelle der Stärken von Freenet
- Verständnis notwendig für Effizienz



Warum will ich das wissen?

Alleinstellungsmerkmale

- Freund-zu-Freund Darknet (plus Opennet)
- Hosting ohne Server (hochladen und verschwinden)
- Stabile Pseudonyme (privater Schlüssel)
- Kryptografie über Links (einfach nutzbar)
- Dezentrale Spamresistenz (erprobt; hilft Kommunikationskultur)
- Nutzungsabhängige Lebenszeit (anonym)

Praktisch: Seit 22 Jahren durch Tausende genutzt.

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

ooo●
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
ooooo
ooooo

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Warum will ich das wissen?

Grundkonzepte

- Zugriff auf Daten: dezentral und skalenfrei (small world)
- Referenzierung von Daten über Inhalts-Hash oder Öffentlichen Schlüssel
- Private und Öffentliche Schlüssel als Links
- Updates über Versionierung

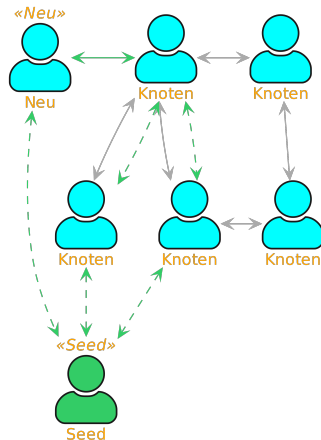


Einstieg

Einstieg

- Mit Freunden verbinden¹
(sicherer), oder
- Mit Seednode verbinden

¹: High Security Mode: nur mit
Freunden verbinden





Einstieg

Small World / grob Skalenfreies Netz

- Verbunden zu vielen Nahen Knoten und wenigen entfernten
- 6 Degrees of Separation: Wie Briefe über Bekannte
- Ring: Location liegt zwischen 0.0 und 1.0
- Wer bei 0.3 ist, kennt v.a. Leute nahe 0.3
- Bei Opennet über den Einstieg realisiert
- Bei Friend-to-Friend über Tausch der Location



Dateien referenzieren: Schlüsseltypen

- CHK: Datei nach Inhalt
- SSK: Public/Private Key
 - USK: Aktualisierbar
 - KSK: Gemeinsames Passwort

CHKs sind 32kiB groß, SSKs 2kiB. Größere sind Bäume von CHKs mit SSK oder CHK für das Manifest.



Struktur der Schlüsseltypen

```
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

Nur <routing> wird ins Netz geschickt. <encryption> bleibt lokal.

ooo
ooooooooo
ooooooooo
oooooo

oooo
oo
oo●oooo
oo
ooooooooo
oooooo

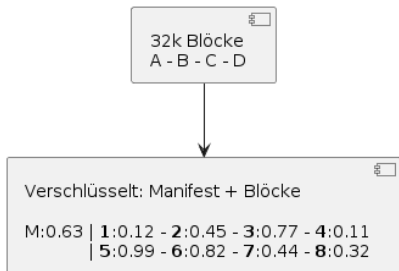
oo
oooo
ooooo
ooo

oooooo
oo
ooo
oo

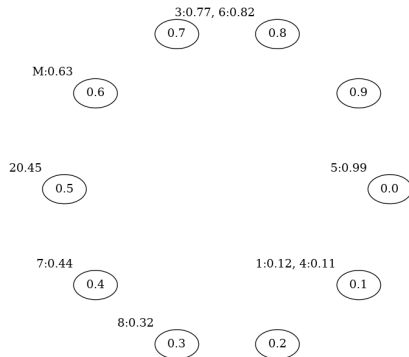
ooo

Datenoperationen

Dateien aufteilen und hochladen



Schlüssel ist im Link (z.B. CHK).
Blöcke ohne Link nicht
entschlüssel- oder erkennbar.



Blöcke zufällig überschreiben.

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooooo

ooooo
oo
ooo●ooo
oo
ooooooooo
oooooo

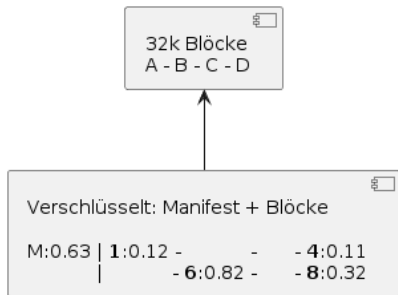
oo
ooooo
oooooo
ooo

ooooooooo
oo
ooo
oo

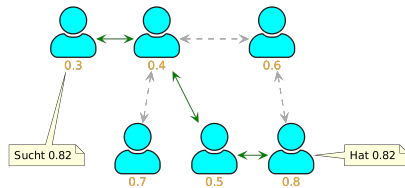
ooo

Datenoperationen

Blöcke finden und zusammenfügen



Verfügbar, solange 50% der Blöcke auffindbar sind.



Routing in Small-World Netzwerk über die Positionen der Freunde von Freunden (FOAF).

Warum Freenet?

○○○
○○○○○○○○
○○○○○○○○
○○○○○○○
○○○○○○

Funktionsweise

○○○○
○○
○○○○●○○
○○
○○○○○○○○
○○○○○○

Werkzeuge

○○
○○○○
○○○○○
○○○

Neuerungen

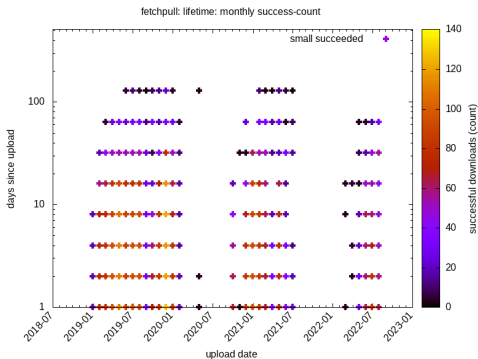
○○○○○○
○○
○○○
○○

Zusammenfassung

○○○

Datenoperationen

Lebenszeit



Jeder Zugriff startet die Uhr neu.

Dr. Arne Babenhauserheide

 Freenet: the long game 



Recht auf Vergessen?

- Lebenszeit aus öffentlichem Interesse
- Recht auf Vergessen in Technologie
- Datenschutzfreundlich

Technischer Hintergrund: wichtigste Frage bei verteilten Speichernetzen: wie entscheiden wir, was wir löschen?



Und Update-Infos? In konstanter Zeit: Date Hints

- Nutzer: SSK@.../meine-seite-1/... → SSK@.../meine-seite-2/activelink.png
- Entwickler: USK@.../meine/seite/1
 - SSK@[key]/[sitename]-DATEHINT-[year]

HINT

46

2013-7-5

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



Ordner in Freenet: Manifest-Daten

Status

Configuration

KeyUtils

Key Explorer

Site Explorer

Spittile 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:
☐ auto open as manifest if possible ☐ parse manifest recursive (include multilevel metadata/subcontainers) Hex display columns:

Key: SSK@LHeuG-SU5ZvYQXTu8Y9mhjCYyQxB-m-W-ryElufr-2M,Ij9l0U1Wa-FQu7GFBf-ciWUbCwPTFv6mWZkS1YuoxQk,AQACAAE/arnebab-org-413 (MetaData)

```

000000: F053 B284 2091 482B 0001 8303 0000 0000 0756 7A95 A5A5 9275 4B9F 4A41 C2A5 052F .S...H+.....Vz....uK.JA.../
000020: 065F B44A F525 2B17 DAE4 D788 7F14 B388 DE50 18A1 A416 1B09 8BAF F0F8 D83A 825D .J.%+.....P.....:]
000040: 88ED C3D8 4C45 9390 01F6 E990 A59A 7FD6 E9D5 A03E AE00 0000 0000 1880 0000 0000 .....LE.....>.....
000060: 0000 6CB7 CD00 0000 1800 0000 0000 0007 0001 6184 0003 02FF FFCF 6FB9 0078 A078 .....S.1(;...=U...'T...g.....{
000080: F617 F153 CE31 283B A90E 803D 55FD 9C27 1E54 9CFD 0067 17C1 AF10 EE09 BFFF F4B8 "...M...t...W....n2...V!..
0000A0: 2204 AEE5 4DCB CB00 74C6 CAEF 578B 84A9 AC6E 32BC B104 5621 FD

```

Decomposed metadata

Metadata version 1
Document type: ArchiveManifest
MIME Type: application/x-tar
Flags: HasTopData

■ Ein Archiv (Tarball), transparenter Zugriff



Ordner in Freenet: Als Manifest

Explore a site

List the content of a manifest

Freenetkey to explore: Explore!

☐ parse manifest recursive (include multilevel metadata/subcontainers)

Key: SSK@LHeuG-SU5ZvYQXTu8Y9mhjCYyQxB-m-W~ryElufr-2M,Ij9l0U1Wa~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. . . ,Ij9. . . ,AQACAAE/arnebab-org/413/

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooo

Funktionsweise

oooo
oo
oo
ooooooooo
oo
●oooooooo
oooooo

Werkzeuge

oo
ooo
ooooo
ooooo
ooo

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Schnittstellen

Schnittstellen

- Browser
- Verteilte Datenbank für Programme
- Plugins

ooo
 ooooooooo
 ooooooooo
 oooooo

oooo
 oo
 ooooooooo
 oo
 o●oooooooo
 oooooo

oo
 oooo
 oooooo
 ooo

oooooo
 oo
 ooo
 oo

ooo

Schnittstellen

Der Browser

- Zugriff üblicherweise auf <http://localhost:8888>
- [freenetbrowser](#) (automatisch generiertes Firefox-Profil) für bessere Sicherheit
- Optimierungen für Pre-Fetching und Media-Streaming

<http://localhost:8888/USK@rQn...,l1v...,AQACAAE/gms/16/>

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
oo●ooooo
oooooo

Werkzeuge

oo
oooo
ooooo
ooooo

Neuerungen

oooooo
oo
ooo
ooo

Zusammenfassung

ooo

Schnittstellen

Externe Programme

- Server für Foren/NNTP (FMS) und IRC (FLIP)
- GUI-Programme (jSite)

```

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooooo

```

```

ooooo
oo
ooooooooo
oo
ooo●oooo
oooooo

```

```

oo
ooooo
oooooo
ooo

```

```

ooooooo
oo
ooo
oo

```

```

ooo

```

Schnittstellen

Externe Programmier-Schnittstellen

- FCP: Freenet Client Protokoll
 - HTTP-Ähnlich: Key: value Zeilenweise, Optional Data-Bytes am Ende
 - <https://github.com/freenet/wiki/wiki/FCPv2>
- Bibliotheken
 - 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>
 - Beispiele: <https://github.com/freenet/wiki/wiki/Projects#plugins>

```

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooooo

```

```

oooo
oo
ooooooo
oo
oooo●ooo
oooooo

```

```

oo
oooo
ooooo
ooo

```

```

oooooo
oo
ooo
oo

```

```

ooo

```

Schnittstellen

Schnittstelle: FCP

Async für Programme:

- Put/Putdir/Get
- Subscribe to key
- Plugins kontrollieren

```
ClientHello
```

```
Name=My Client
```

```
ExpectedVersion=2.0
```

```
EndMessage
```

```
NodeHello
```

```
...
```

```
EndMessage
```

```
ClientPut
```

```
URI=CHK@
```

```
UploadFrom=disk
```

```
Filename=/tmp/debian-dvd1.iso
```

```
Identifier=sarge-disk-1
```

```
Global=true
```

ooo
 ooooooooo
 ooooooooo
 oooooo

oooo
 oo
 ooooooooo
 oo
 ooooo●oo
 oooooo

oo
 oooo
 ooooo
 ooo

oooooo
 oo
 ooo
 oo

ooo

Schnittstellen

Latenz in der Praxis

- Bis zu 2kiB, raw, realtime mode: <30s
- Große Dateien, im Manifest: ~5 min

Realtime

PriorityClass . 2 ;; high

MaxRetries . 0 ;; default: 10

RealTimeFlag . true

DontCompress . true

ExtraInsertsSingleBlock . 0

ExtraInsertsSplitfileHeaderBlock . 0

Bulk

PriorityClass . 3 ;; medium

RealTimeFlag . false

DontCompress . false



Schnittstellen

Schnittstelle: Plugins

- In die Web-Oberfläche integriert
- Schwache Abstraktion
- Zugriff auf das Innenleben (riskant)
- Leichtester Einstieg: Bestehendes Plugin anpassen

Beispiele: [Sone](#) oder [Sharesite](#)



Schnittstellen

Grundlagen der Kommunikation über Freenet

- Einstieg: Seed-keys + Captcha-Queue: KSK-Prefix
- Suche: Nutzerspezifische Seiten mit Links, Update-Infos
- Verteilung: Gossip keys, Dateien einfach hochladen
- Störungsresistenz: Web of Trust mit langsam steigender Sichtbarkeit

Einwurf: Konstruktive Spammer: <https://xkcd.com/810/>

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
●ooooo

Werkzeuge

oo
oooo
ooooo
ooo

Neuerungen

oooooo
oo
ooo
oo

Zusammenfassung

ooo

Schutzmaßnahmen

Schutzmaßnahmen

- Datenschutz trotz Browser
- Abstreitbarkeit
- Spam-Abwehr

Dr. Arne Babenhauserheide

 Freenet: the long game 



Content Sanitizing: Vor dem Browser schützen

Browser und Media-Player: Anderes Bedrohungs-Szenario

⇒ Inhalte filtern, um Zugriffe auf Clearnet-Ressourcen zu vermeiden

Beispiel: Album-Art einer Radiosendung über URL nachladen.



Abstreitbarkeit: Das war jemand anders

- Anfragen haben Hops to Live (HTL)
- Mit jedem Schritt um 1 verringert
- HTL 18 wird nur bei 50% der Verbindungen verringert — Wahl bleibt über die Dauer der Verbindung bestehen
 ⇒ Anfragen mit HTL 18 können immer von einem anderen Knoten kommen



Spam-Abwehr

WoT (Web of Trust): Eine von zwei praktisch genutzten Möglichkeiten. Die andere ist FMS (Freenet Message System).

- ID = USK
- Trust -100 bis 100
- Rank: Distanz → capacity
- Score: Summe über alle Wertungen: $\text{trust} * \text{rank}$
- Skaliert bei 22 Nachrichten pro Tag¹ (Dunbar-Zahl)

¹ <https://www.draketo.de/english/freenet/deterministic-load-decentralized-spam-filter>



Capacity



- Rank 1 40 %. rank 1: 100 trust, 40 Punkte als Score.
- Rank 2 16 %
- Rank 3 6 %
- Rank 4 2 %
- Rank 5 und niedriger: 1 %

*Integer-Mathematik: $2 * 6 / 100 = 0$.*



Zusammenfassung

- Freundeskreis / Opennet,
- Ohne Server,
- Schlüssel als Pseudonym,
- Spamresistenz,
- Small-World
- Schlüsseltypen (CHK: Inhalt, USK: Aktualisierbar, KSK: Passwort)
- Dateien werden aufgeteilt, Redundanz
- Lebenszeit nach Zugriffshäufigkeit
- Ordner
- Schnittstellen
- Schutzmaßnahmen

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

●o
oooo
ooooo
ooo

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Werkzeuge

Werkzeuge

Sieht spannend aus, aber was kann ich mit Freenet praktisch machen?

Dr. Arne Babenhauserheide

 Freenet: the long game 



Der Browser

- Browse
- Hoch-/Herunterladen
- Plugins
- Freund-zu-Freund-Nachrichten
- Lesezeichen mit Update-Info (5 min Latenz)
- Indexe mit Listen von Seiten (pseudonym betriebene Crawler)



Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
●ooo
ooooo
ooo

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Konkret

Sharesite: Einfachstes pseudonymes Veröffentlichen

<http://127.0.0.1:8888/Sharesite>

Dr. Arne Babenhauserheide

 Freenet: the long game 

ooo
 ooooooooo
 ooooooooo
 oooooo

oooo
 oo
 ooooooooo
 oo
 ooooooooo
 oooooo

oo
 o●oo
 ooooo
 ooo

oooooo
 oo
 oo
 ooo
 oo

ooo

Konkret

FMS and Flip: pseudonyme Foren and IRC

- FMS: <http://127.0.0.1:8888/USK@0nnpMrqZNKRCRoGojZV93UNHCMN-6UU3rRSAmP6jNLE,~BG-edFtdCC1cSH403BWdeIYa8Sw5DfyrSV-TKd05ec,AQACAAE/fms/153/>
- FLIP: <http://127.0.0.1:8888/USK@pGQPA-9PcFiE3A2tCuCjacK165UaX07AQYw98iDQrNA,8gwQ67ytBNR03hNj7JU~ceeew22HVq6G50dcEeMcgks,AQACAAE/flip/17/>

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oo●oo
ooooo
ooo

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Konkret

Sone: pseudonymes Microblogging

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

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
ooo●
ooooo
ooo

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Konkret

Freemail: vertrauliche E-Mail

[http://127.0.0.1:
8888/USK@M0d8y6YoLpX0eQGxu0-IDg8sE5Yt~Ky6t~GPyZe~zo,
K1qIjAj3~dA1Zf57VD1jkmp3vHUozndpxnH-P2RRugI,AQACAAE/
freemail/8/](http://127.0.0.1:8888/USK@M0d8y6YoLpX0eQGxu0-IDg8sE5Yt~Ky6t~GPyZe~zo,K1qIjAj3~dA1Zf57VD1jkmp3vHUozndpxnH-P2RRugI,AQACAAE/freemail/8/)

Dr. Arne Babenhauserheide

 Freenet: the long game 

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

oooo
oo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
●oooo
ooo

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Plugins

Shoeshop: Sneakernet mit Freenet

[http://127.0.0.1:
8888/USK@MYLAnId-ZEyXhDGGbY0a1g0tkZZrFNTXjF11dibLj9E,
Xpu27DoAKKc8b0718E-ZteFrGqCYR0e7XBBJI57pB4M,AQACAAE/
Shoeshop/3/](http://127.0.0.1:8888/USK@MYLAnId-ZEyXhDGGbY0a1g0tkZZrFNTXjF11dibLj9E,Xpu27DoAKKc8b0718E-ZteFrGqCYR0e7XBBJI57pB4M,AQACAAE/Shoeshop/3/)

Dr. Arne Babenhauserheide

 Freenet: the long game 

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

oooo
oo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
oooo
o●ooo
ooo

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Plugins

jfniki: Wiki über Freenet

[http://127.0.0.1:
8888/USK@jZVIWXW-5nl4Bco~7lWbVazRzFQv78X9RnJsWWKdWm4,
zBn2IimGcyEQ7mh~w~tRABGAYH6F4Zwoqfh8Cv7tVhY,AQACAAE/
jFniki.Index/12/Contributing.html](http://127.0.0.1:8888/USK@jZVIWXW-5nl4Bco~7lWbVazRzFQv78X9RnJsWWKdWm4,zBn2IimGcyEQ7mh~w~tRABGAYH6F4Zwoqfh8Cv7tVhY,AQACAAE/jFniki.Index/12/Contributing.html)

Dr. Arne Babenhauserheide

 Freenet: the long game 

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
ooo●oo
ooo

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Plugins

KeyUtils: Technische Details über Uploads

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

Dr. Arne Babenhauserheide

 Freenet: the long game 

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
oooo●o
ooo

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Plugins

Keepalive: Ein paar Dateien verfügbar halten

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

Dr. Arne Babenhauserheide

 Freenet: the long game 

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
oooo●
ooo

Neuerungen

oooooo
oo
oo
oo
oo

Zusammenfassung

ooo

Plugins

Freereader: RSS über Freenet verbreiten

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

Dr. Arne Babenhauserheide

 Freenet: the long game 

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
ooooo
ooooo
●ooo

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Programme

pyFreenet: Kommandozeilenwerkzeuge

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

Dr. Arne Babenhauserheide

 Freenet: the long game 

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
ooooo
ooo

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Programme

infocalypse: Versionsverwaltung über Freenet

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

Dr. Arne Babenhauserheide

 Freenet: the long game 

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
ooooo
ooooo
oo●

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

ooo

Programme

jSite: Webseiten hochladen mit GUI

[http://127.0.0.1:
8888/USK@1waTsw46L9-JEQ8yX1khjkhHcn--gOMlMsTlYHax9zQ,
oYyxr5jyFnaTsVGDQWk9e3ddOWGKnqEASxAk08MHT2Y,AQACAAE/
jSite/15/](http://127.0.0.1:8888/USK@1waTsw46L9-JEQ8yX1khjkhHcn--gOMlMsTlYHax9zQ,oYyxr5jyFnaTsVGDQWk9e3ddOWGKnqEASxAk08MHT2Y,AQACAAE/jSite/15/)

Dr. Arne Babenhauserheide

 Freenet: the long game 

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
ooooo
ooooo

Neuerungen

●ooooo
oo
ooo
oo

Zusammenfassung

ooo

Neuerungen

Neuerungen

Was sich in 15 Jahren seit dem Rewrite in 0.7 getan hat.

One secret of success: relentless optimization.



Pitch-Black Attack

2007 haben Christian Grothoff et al. eine Schwachstelle gefunden
und belegt.

Routing in the Dark: Pitch Black

Nathan S. Evans

Chris GauthierDickey

Christian Grothoff

Colorado Research Institute
for Security and Privacy

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

ooo
 ooooooooo
 ooooooooo
 ooooooo

oooo
 oo
 ooooooooo
 oo
 ooooooooo
 oooooo

oo
 oooo
 ooooo
 ooo

oo●ooo
 oo
 ooo
 oo

ooo

Neuerungen

Pitch black gelöst

The mitigation

2021 haben wir sie endlich gefixt.



→ build 1490: “pitch black streaming” ←

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
ooooo
ooo

Neuerungen

oooo●oo
oo
ooo
oo

Zusammenfassung

ooo

Neuerungen

WoT: Precisely updating and subscription-based



OPTIMIZING A DISTRIBUTED SPAM FILTER FOR FREENET

AKA

THE WEB OF TRUST DEVELOPER'S MANUAL

Dr. Arne Babenhauserheide

 Freenet: the long game 



Bessere Geschwindigkeit

- Von 10kiB/s bis 11MB/s (und mehr)
- Unterstützt bis zu 15.000 Subscriptions: Binnen 5 Minuten Updates sehen
- 30 Sekunden Round-Trip-Zeit für Chat



Mehr HTML and CSS

- Unterstützung für Teile von CSS3.
- Nur, bei was die Sicherheit garantiert werden kann.



Audio streaming

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

Mit Live-Streaming:

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

Beispiel:

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

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
ooooo
ooooo
ooo

Neuerungen

oooooo
o●
ooo
oo

Zusammenfassung

ooo

Multimedia

Video on demand

<http://localhost:8888/USK@rQn...,l1v...,AQACAAE/gms/16/>

Dr. Arne Babenhauserheide

 Freenet: the long game 

Warum Freenet?

○○○
○○○○○○○○
○○○○○○○
○○○○○○○
○○○○○○○

Funktionsweise

○○○○
○○
○○○○○○○
○○
○○○○○○○○
○○○○○○○

Werkzeuge

○○
○○○○
○○○○○
○○○○○
○○○

Neuerungen

○○○○○○
○○
●○○
○○

Zusammenfassung

○○○

Mobil / Handy

mobile-node: Freenet auf Android

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

Dr. Arne Babenhauserheide

 Freenet: the long game 

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
ooooo
ooooo
ooo

Neuerungen

oooooo
oo
oo
o●o
oo

Zusammenfassung

ooo

Mobil / Handy

FreeChat: Chat auf Android

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

Dr. Arne Babenhauserheide

 Freenet: the long game 

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
ooooo
ooo

Neuerungen

oooooo
oo
oo
oo●
oo

Zusammenfassung

ooo

Mobil / Handy

icicles: Nachrichten von Freunden und Knoten verbinden

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

Dr. Arne Babenhauserheide

 Freenet: the long game 



Offene Fragen

- Besseres Routing? (dank Pitch Black mitigation wurden auch neue Strukturen möglich)
- Freund-zu-Freund Verbindungen über tor und i2p? (braucht UDP!)
- Steganographic Transport Plugins
- Dezentrale Suche in Freenet (Spider/Library optimierungsbedürftig)



Pläne

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
- Bugtracker-Roadmap — very detailed but outdated



Zusammenfassung 1

Warum gibt es Freenet? Freie Kommunikation

Was ermöglicht Freenet? Vertraulich und Pseudonym, ohne zentrale Server, Datenschutzfreundliche Datenbank für verteilte Programme.

Wie funktioniert Freenet? -

Einstieg: Freund-zu-Freund (High Security) oder über Seednode (Opennet)

Routing: Small-World mit FOAF-Routing

Dateien: Aufteilen, Verschlüsseln, 100% Redundanz, Verfügbar solange genutzt.

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo
ooooooo

Funktionsweise

oooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
oooo
ooooo
ooo

Neuerungen

oooooo
oo
oo
ooo
oo

Zusammenfassung

o●o

Zusammenfassung

Zusammenfassung 2

Was hat sich geändert? Pitch Black gelöst, Spam-Schutz über WoT/Sone und FMS, schneller, IRC Chat, Multimedia-Streaming, Android-Unterstützung, Sharesite für einfachste Webseiten, Stetige Optimierung in praktischer Nutzung.

Warum Freenet?

ooo
ooooooooo
ooooooooo
ooooooooo

Funktionsweise

ooooo
oo
ooooooooo
oo
ooooooooo
oooooo

Werkzeuge

oo
ooooo
oooooo
ooo

Neuerungen

oooooo
ooooo
oo
ooo
oo

Zusammenfassung

oo●

Zusammenfassung

Nutzt Freenet!



- Sharesite
- Sone
- Verbindung im Freundeskreis

freenetproject.org

Dr. Arne Babenhauserheide

 Freenet: the long game 

Andere Projekte

- Tor mit SecureDrop

Quellen

Bilder: Hase unter GPL, alle weiteren 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>

Quellen 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>

Quellen 3

- <https://www.flickr.com/photos/focusc/4758319160>
- <https://www.flickr.com/photos/amitd/4693814169>
- http://commons.wikimedia.org/wiki/File:International_newspaper,_Rome_May_2005.jpg#metadata
- http://commons.wikimedia.org/wiki/File:Edward_Snowden_2013-10-9_%281%29_%28cropped%29.jpg

Quellen 4

Lizenzen:

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

(und neuere Versionen)

References I

Benoist, E. and Sliwa, J. (2020). *Applied Approach to Privacy and Security for the Internet of Things*, chapter Using Freenet as a Broker for Multi-Party Data Exchange in IoT for Health., pages 181–193. IGI Global.