

ANONYMITÄT:

Konzepte und Werkzeuge



ICH

- Name: Marc Seeger
- Studiengang: MIB¹
- Semester: 6/6
- Thesis: “The current state of anonymous file-sharing”

IHR

- Ethernet ?
- TCP/IP ?
- Kryptographie?

AGENDA

- Anonymität
- anonymer Dateitausch
 - Patterns
 - Implementationen

ANONYMITÄT

Verdachtsverteilung





ANONYMITÄT



ANONYMITÄT

SPUREN HINTERLASSEN

```
traceroute to mit.edu (18.7.22.69), 30 hops max, 40 byte packets
 1 192.168.1.250 (192.168.1.250) 0.767 ms 0.844 ms 0.944 ms
 2 192.168.100.1 (192.168.100.1) 1.054 ms 1.062 ms 1.049 ms
 3 ciscovlgw318.hdm-stuttgart.de (141.62.31.246) 1.048 ms 1.231 ms 1.688 ms
 4 firewall-h.hdm-stuttgart.de (141.62.1.1) 1.117 ms 1.155 ms 1.530 ms
 5 cisco.hdm-stuttgart.de (141.62.60.254) 1.834 ms 1.832 ms 2.044 ms
 6 Stuttgart1.belwue.de (129.143.101.201) 2.150 ms 1.062 ms 1.380 ms
 7 Stuttgart2.belwue.de (129.143.1.25) 2.194 ms 2.558 ms 2.809 ms
 8 xr-stu1-ge8-3.x-win.dfn.de (188.1.38.53) 2.818 ms 2.975 ms 2.964 ms
 9 xr-fzk1-te2-1.x-win.dfn.de (188.1.145.81) 4.459 ms 4.512 ms 4.564 ms
10 dfn-gw.rt1.fra.de.geant2.net (62.40.124.34) 8.838 ms 8.825 ms 8.825 ms
11 dfn.rt1.fra.de.geant2.net (62.40.124.33) 7.629 ms 7.717 ms 7.640 ms
12 abilene-wash-gw.rt1.fra.de.geant2.net (62.40.125.18) 331.319 ms 335.853 ms 334.037 ms
13 so-0-0-0.0.rtr.newy.net.internet2.edu (64.57.28.10) 114.697 ms 114.695 ms 114.673 ms
14 nox300gw1-VI-110-NoX-INTERNET2.nox.org (192.5.89.221) 105.856 ms 105.393 ms 105.355 ms
15 nox1sumgw1-VI-803-NoX.nox.org (192.5.89.237) 105.715 ms 105.452 ms 105.528 ms
16 nox1sumgw1-PEER-NoX-MIT-207-210-143-110.nox.org (207.210.143.110) 106.380 ms 105.793 ms 105.849 ms
17 W92-RTR-1-BACKBONE-2.MIT.EDU (18.168.1.25) 105.920 ms 105.788 ms 105.687 ms
18 WEB/MIT.EDU (18.7.22.69) 105.969 ms 105.947 ms 105.830 ms
```

Ich hab' nichts zu verbergen!

Blutgruppe B, Herzinfarktrisiko 14%, KV-Datensatz
(Genanalyse) liegt vor, Krankenversicherung: standard,
Zusatzversicherung angeboten (File 23A18)

Risikoklasse 4 - (Nachuntersuchung erforderlich
in Q8, Verdacht auf KV-Risiko Stufe 3)

Drogenkonsum: Nicht aktuell.

Alkoholkonsum mittel bis niedrig,

Einkommen €1434;-, RV, PV, KS, VWL

Kredit: DB, €40.000, Konto: €-729

Zahlungsmoral: nachlässig, Versand auf Rechnung
einstellen, Kundennr: 393848, Punkte: 2930,
Umsatzpotential nicht ausgeschöpft.

Interessensprofil Musik/Buch: liegt vor

Interessensprofil Reisen: liegt vor,

Bürgerklasse 3 (Normal, wiedervorlage, geplant 2009,

ID-Code C89A839A) Soziales Umfeld: Thomas B.,

Kerstin A., Verena L. (siehe Datensatz B33421)

Arbeitgeber K8273-23, Datenbankabgleich: OK

Verspätungen: 4, Abmahnung: Nein, Auto: Ford Fiesta,

TÜV, Teilkasko, Verkehrsdelikte: 2 (leicht) 0 (schwer)

Risikostufe: 3, Tendenz fallend, Maut-ID A38-92384

Fahrzeugbewegungsdaten: liegen vor ab 04/2006

Politische Ausrichtung: SPD (bis 2005), seit 2005

Nichtwähler, Teilnahme an AK-Demo 2005 (Video #0232-4)



... bis auf meine Privatsphäre.

WAS GIBT ES ZU WISSEN?

BEIM FILESHARING

- Wer du bist
- Was du hoch / runterlädst
- Mit wem du kommunizierst
- Dass du überhaupt im Netzwerk aktiv bist

WER WILL DAS WISSEN?

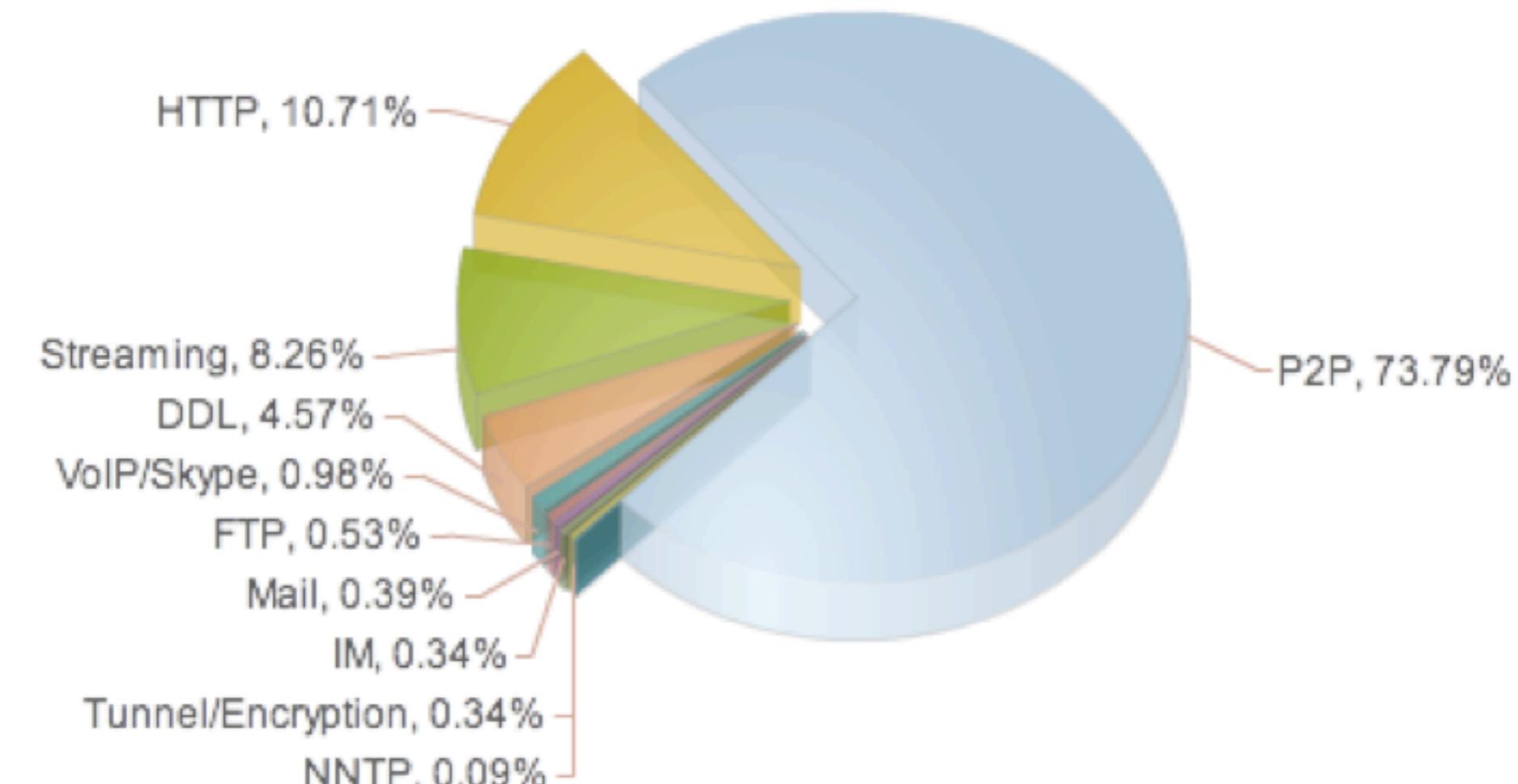
	Ebenbürtig	Allmächtig
Begrenzt durch Gesetze	<p><u>“Interessensvertreter”</u></p> <p>RIAA MPAA GVU ISP</p>	<p><u>“Gesetzesvertreter”</u></p> <p>Polizei</p>
Unbegrenzte Macht	<p><u>“Kriminelle”</u></p> <p>Wirtschaftsspionage Stalker Skriptkiddies</p>	<p><u>“Der große Unbekannte”</u></p> <p>Die “Great Firewall of China” BND NSA</p>

FILESHARING

Publikumsfrage:

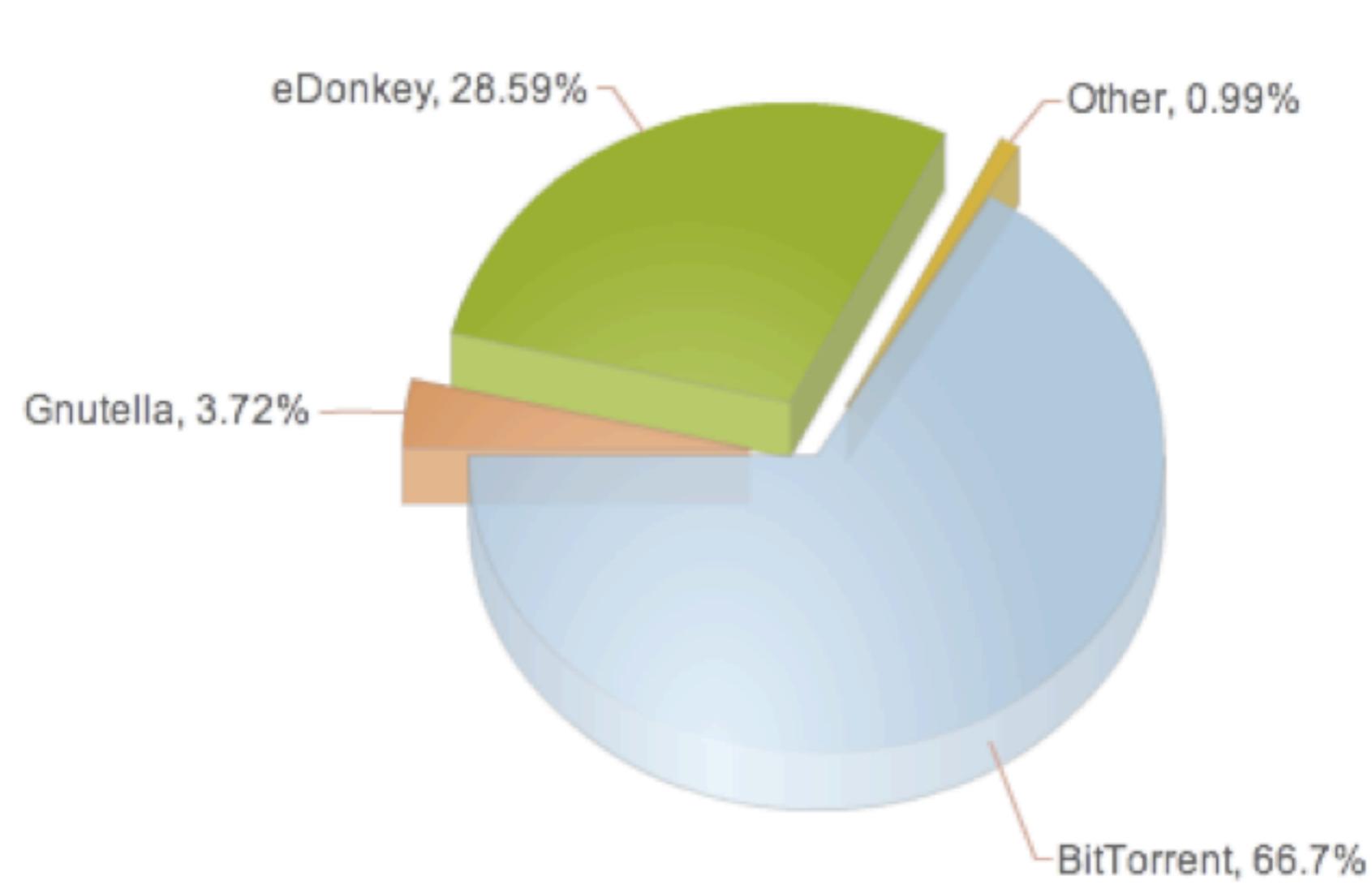
Wieviel Prozent des deutschen Internettraffics
werden durch Filesharing verursacht?

FILESHARING



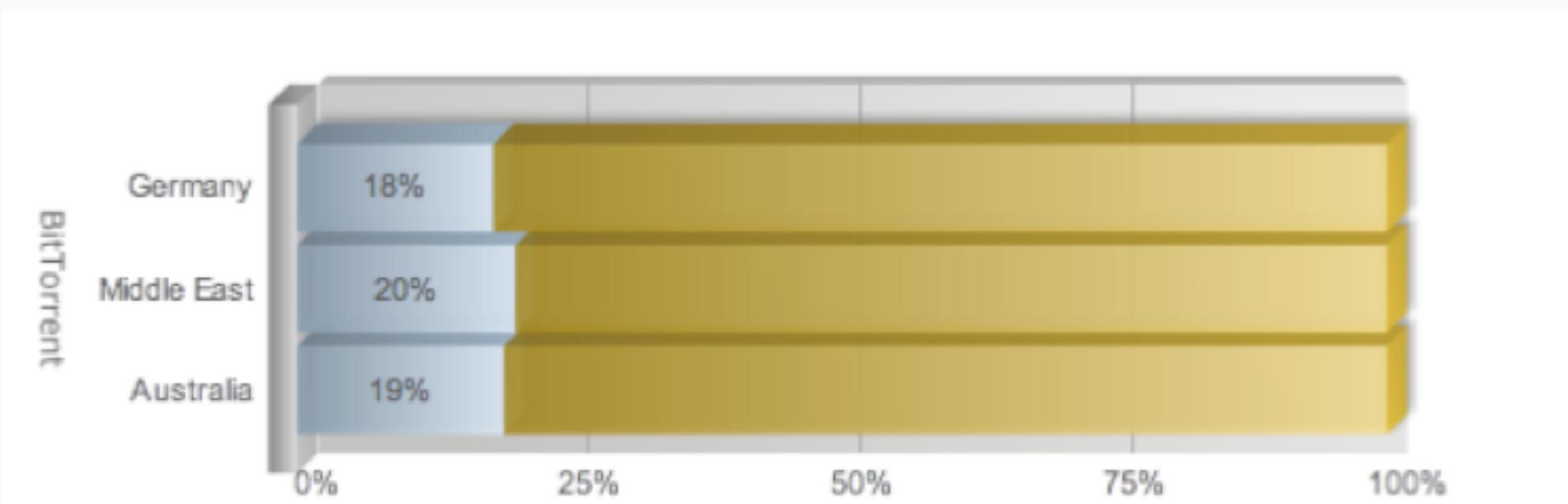
Quelle: iPoque Internet Study 2007

FILESHARING



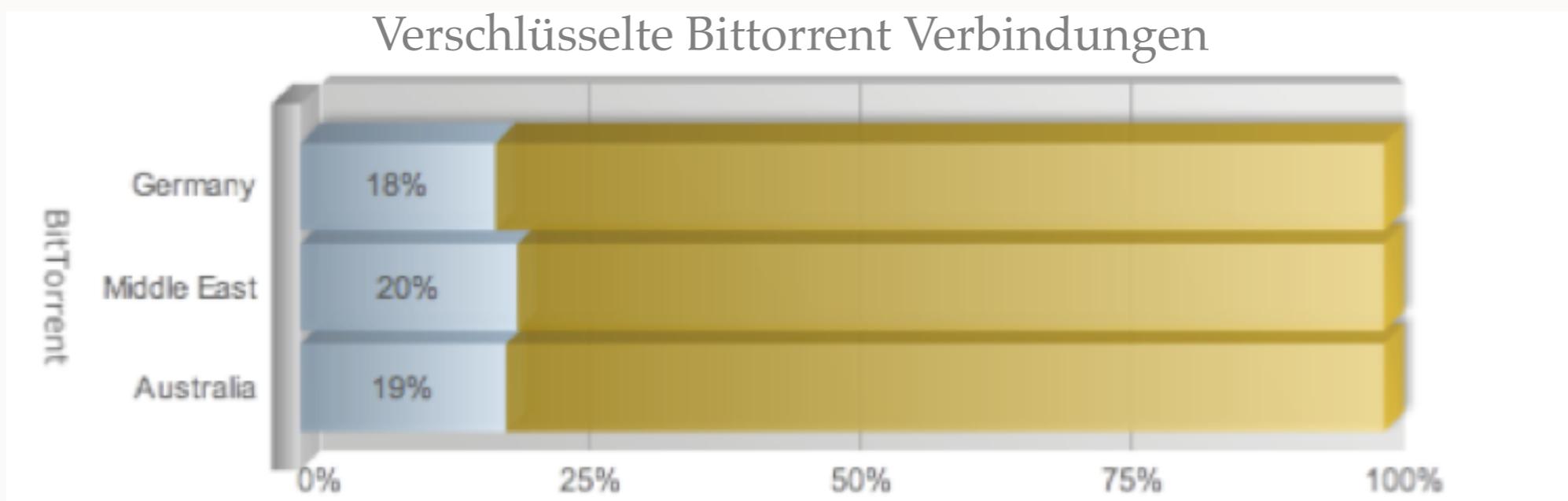
Quelle: iPoque Internet Study 2007

FILESHARING



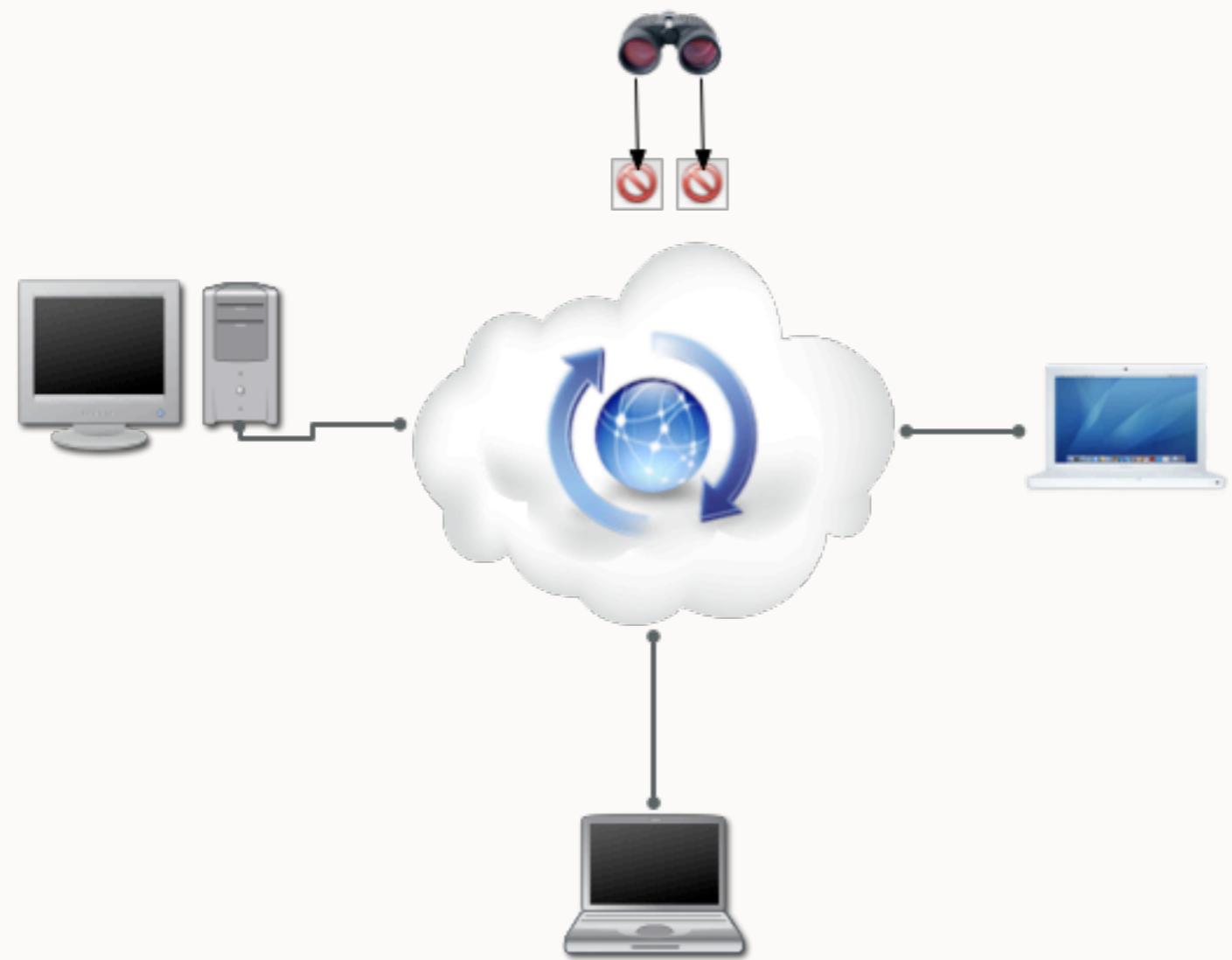
Quelle: iPoque Internet Study 2007

FILESHARING



Quelle: iPoque Internet Study 2007

ANONYMER DATEITAUSCH

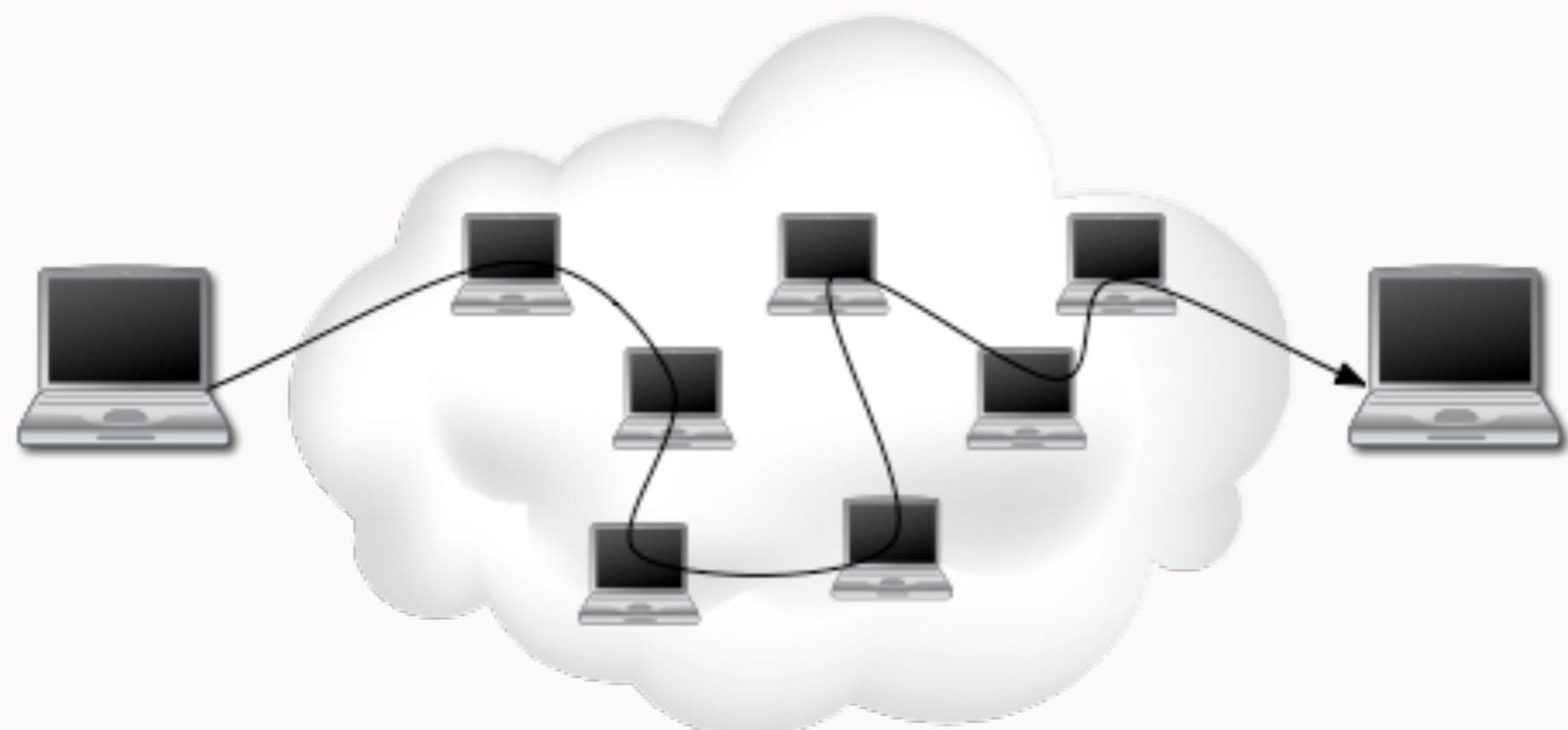


PATTERNS

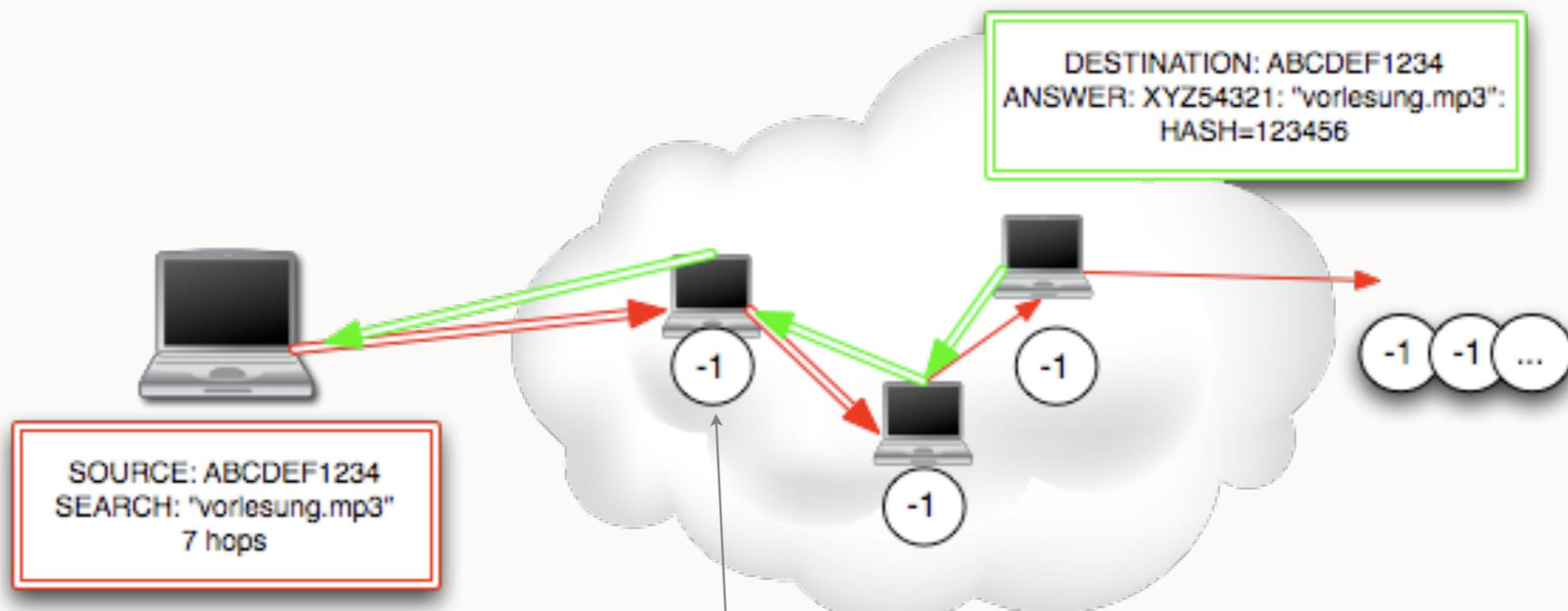
- Proxy Chaining
- End-to-End/Hop-to-Hop Encryption
- Darknet
- Brightnet

PROXY CHAINING

PROXY CHAINING



PROXY CHAINING



Von	An	Über
XXXXX		8.071.234
	YYYYY	12.121.542

PROXY CHAINING

§ 9 Teledienstegesetz (TDG) / § 8 Telemediengesetz (TMG) **Durchleitung von Informationen**

(1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie

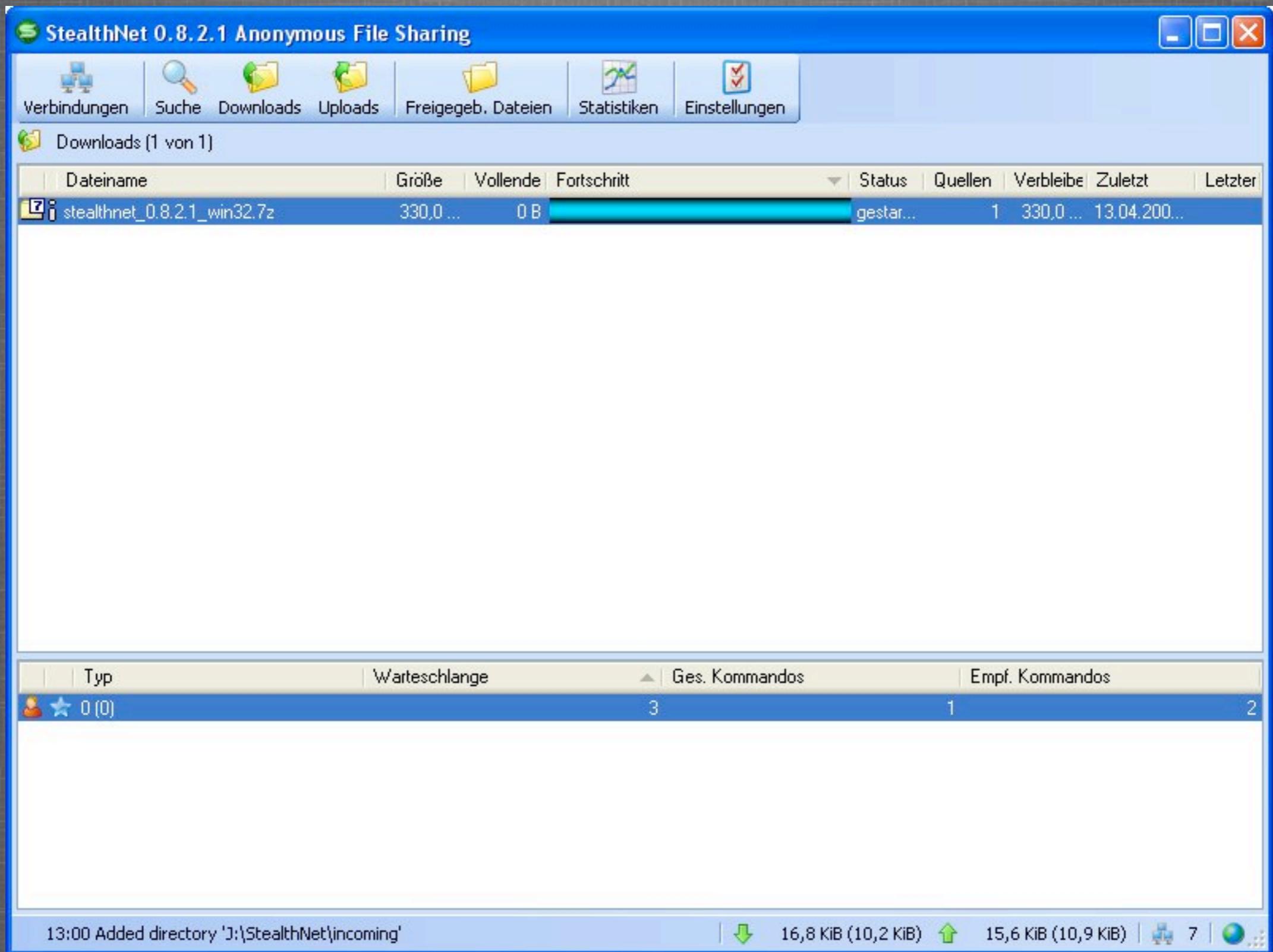
1. die Übermittlung nicht veranlasst,
2. den Adressaten der übermittelten Informationen nicht ausgewählt und
3. die übermittelten Informationen nicht ausgewählt oder verändert haben.

Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem der Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

<u>Von</u>	<u>An</u>	<u>Über</u>
XXXXX		8.071.234
	YYYYY	12.121.542

EVENTUALVORSATZ

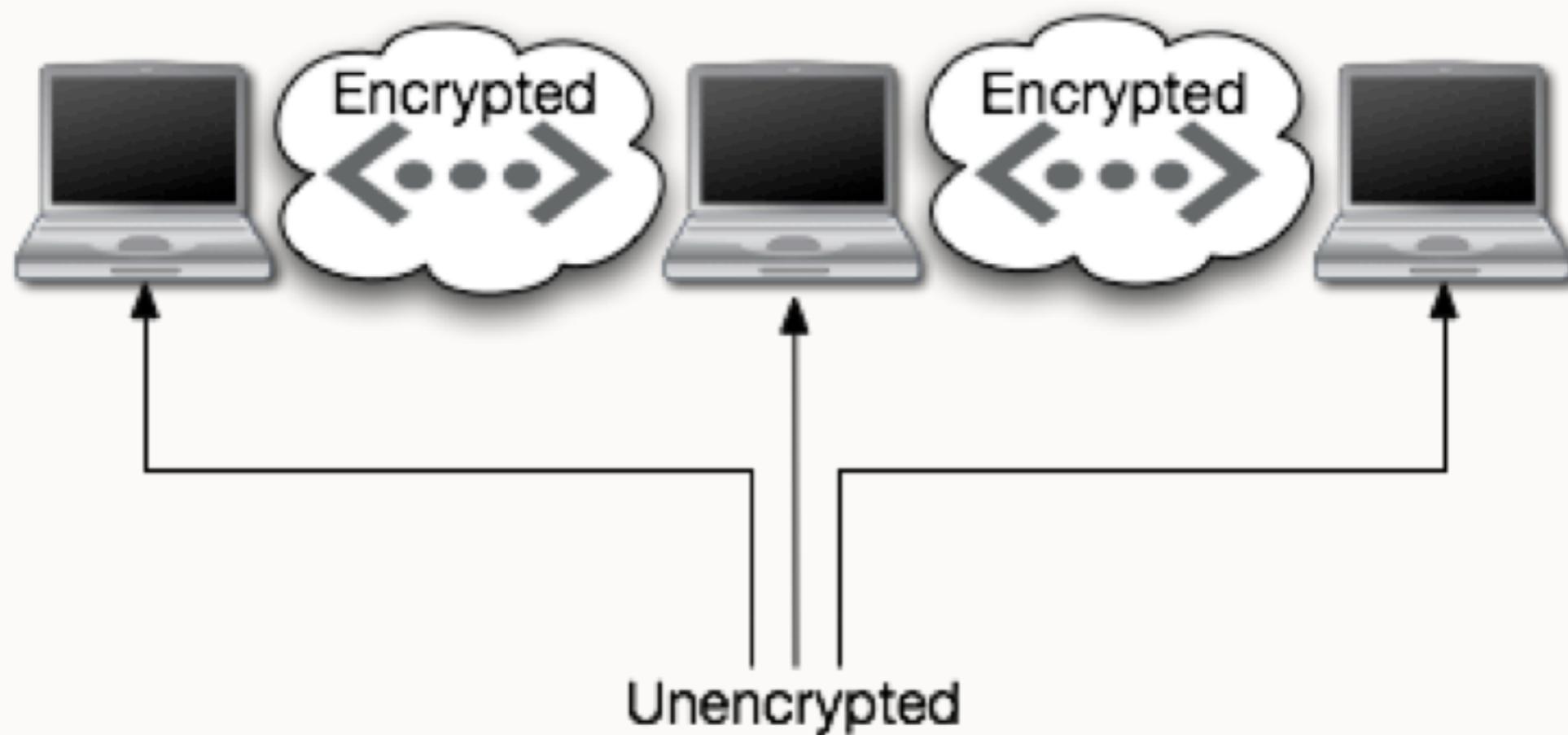
Fahrlässigkeit <--> Eventualvorsatz



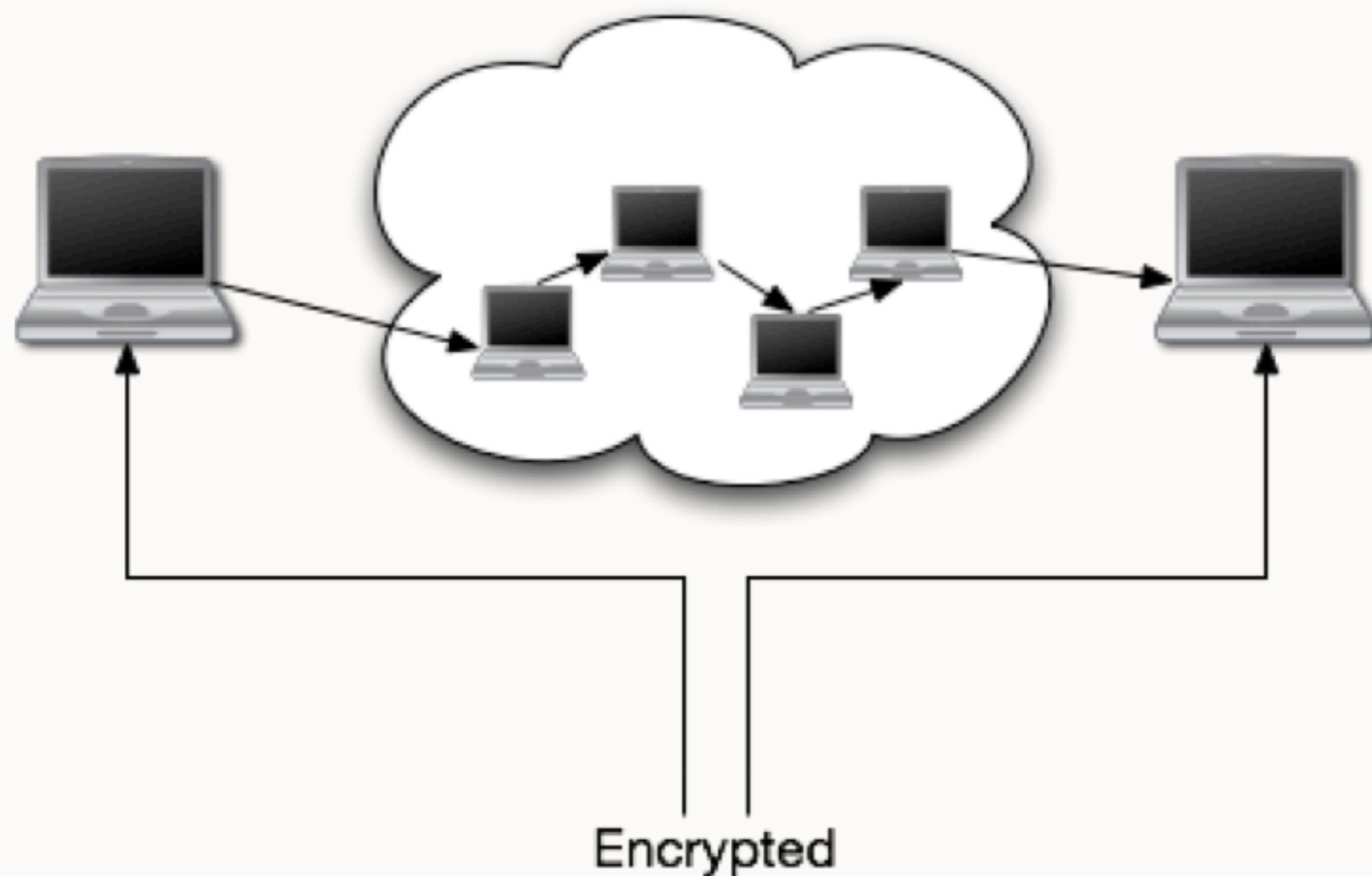
**PROXY CHAINING IMPLEMENTATION:
STEALTHNET:
C# (GUI IN WINDOWS, WEBINTERFACE AUF OSX/LINUX)**

HOP TO HOP / END TO END ENCRYPTION

HOP TO HOP/END TO END

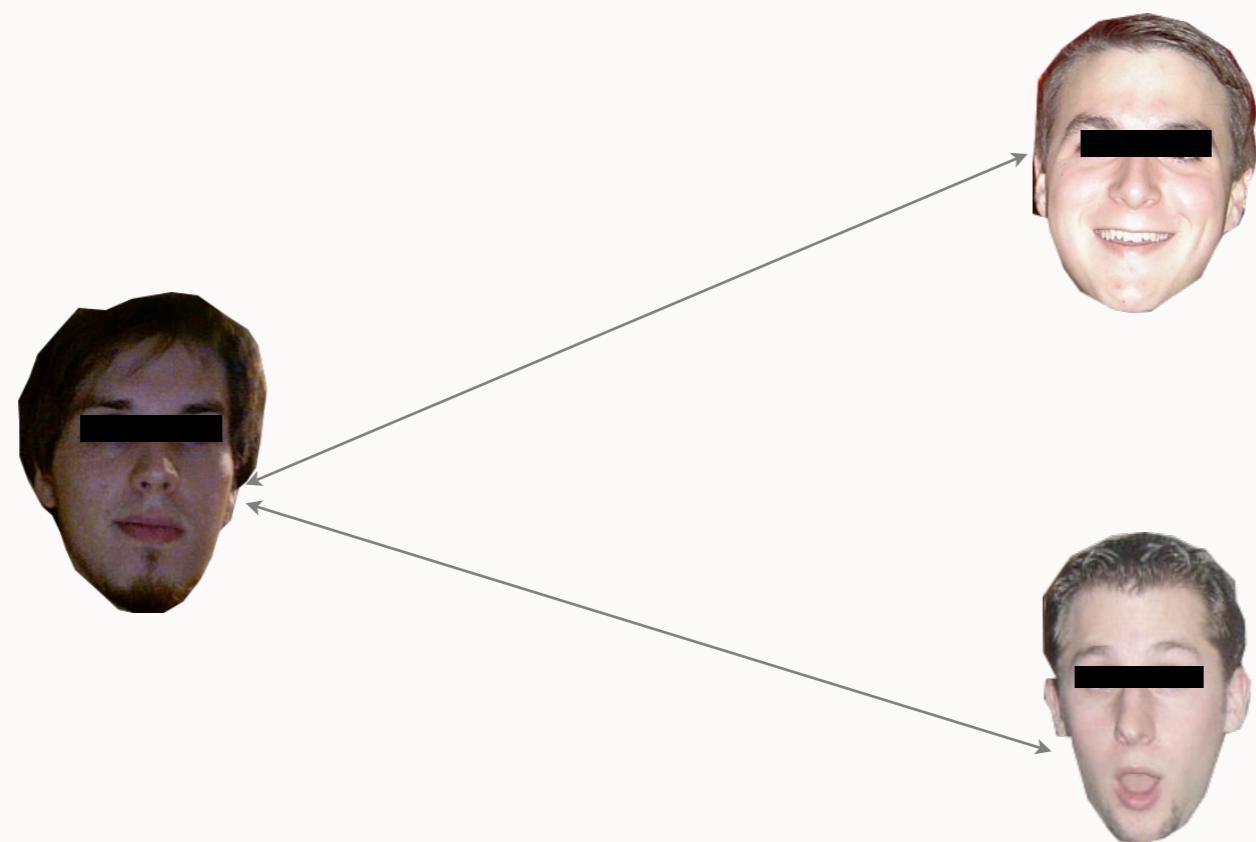


HOP TO HOP/END TO END

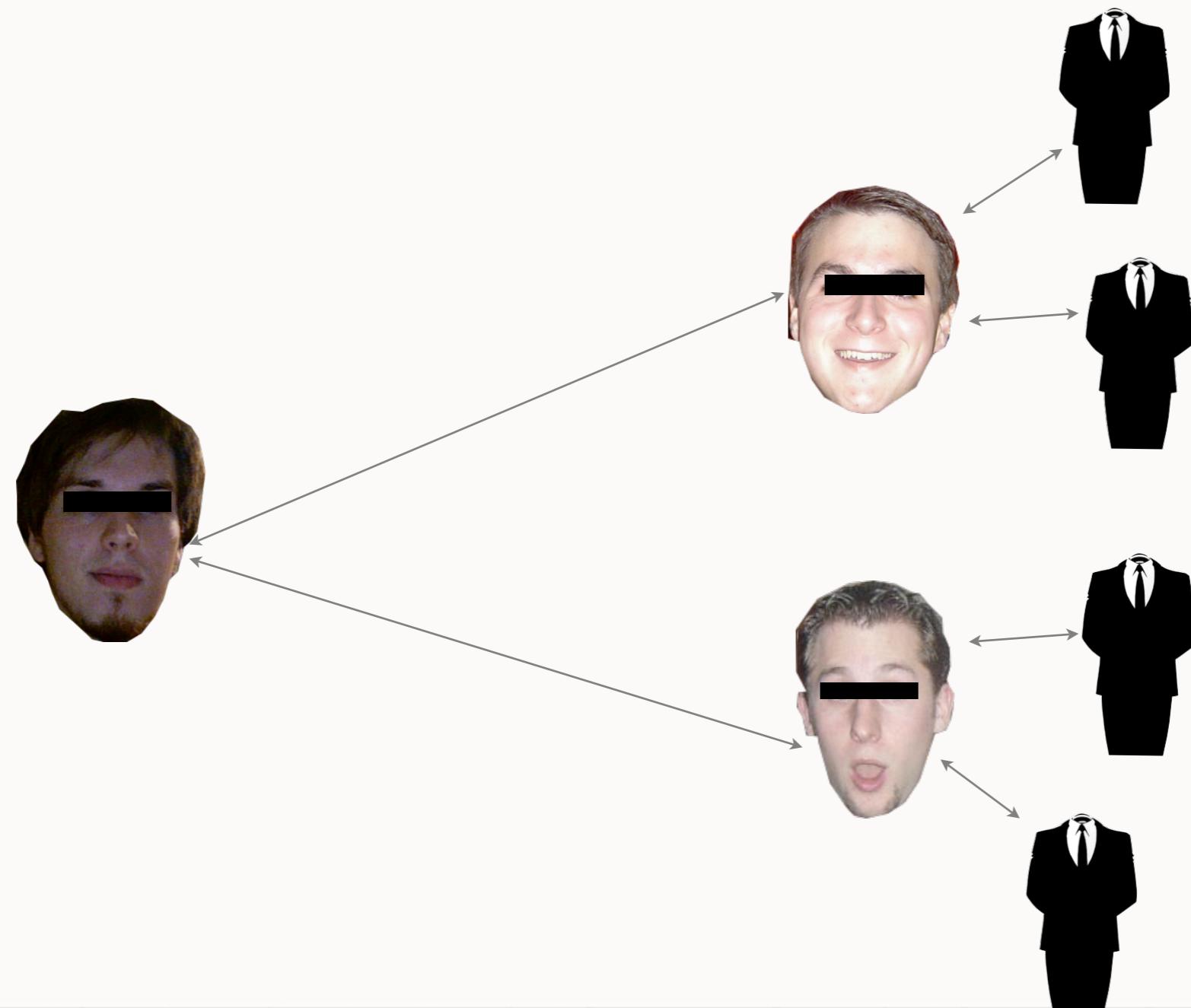


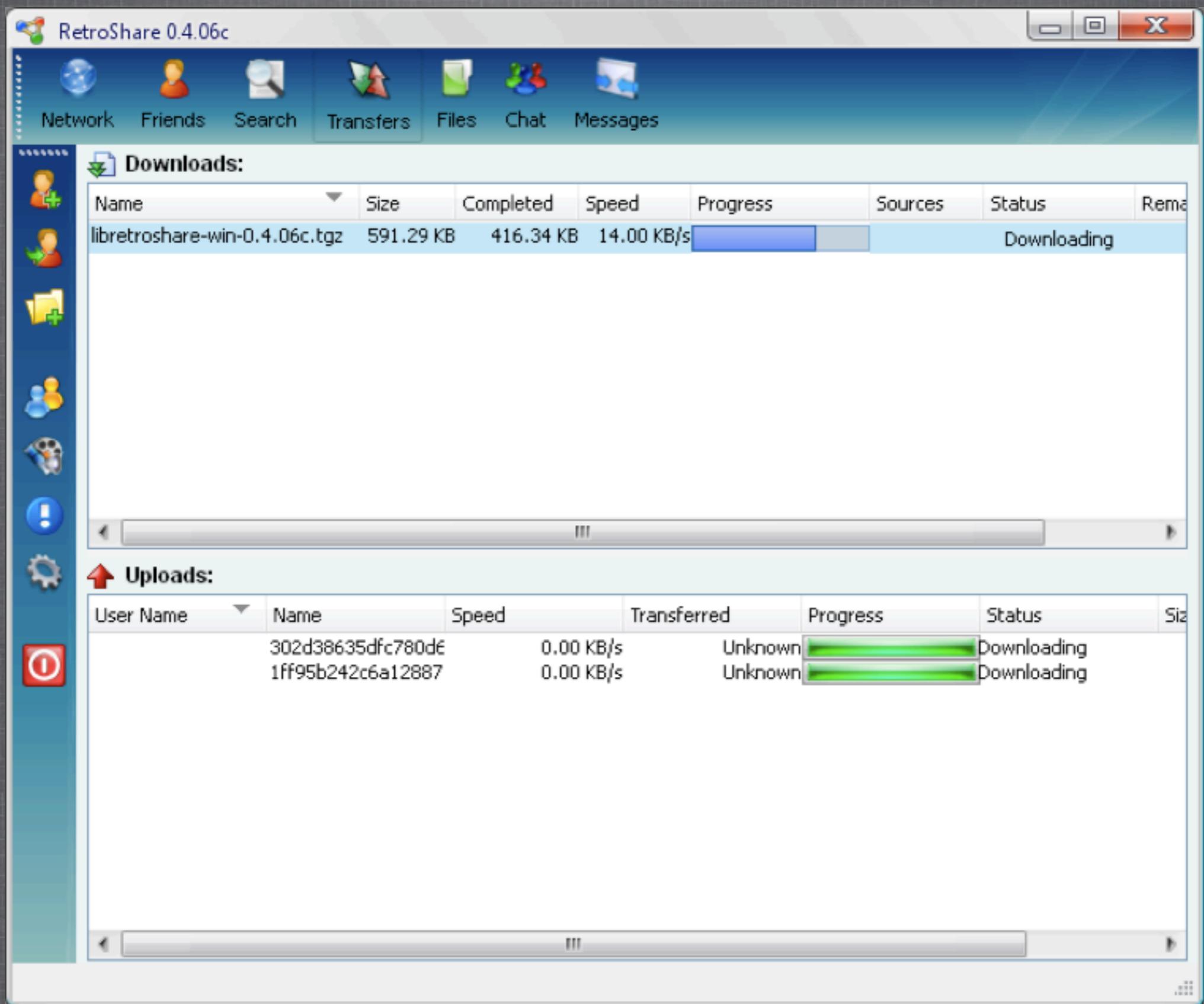
DARKNETS

DARKNET



DARKNET + Turtle hopping

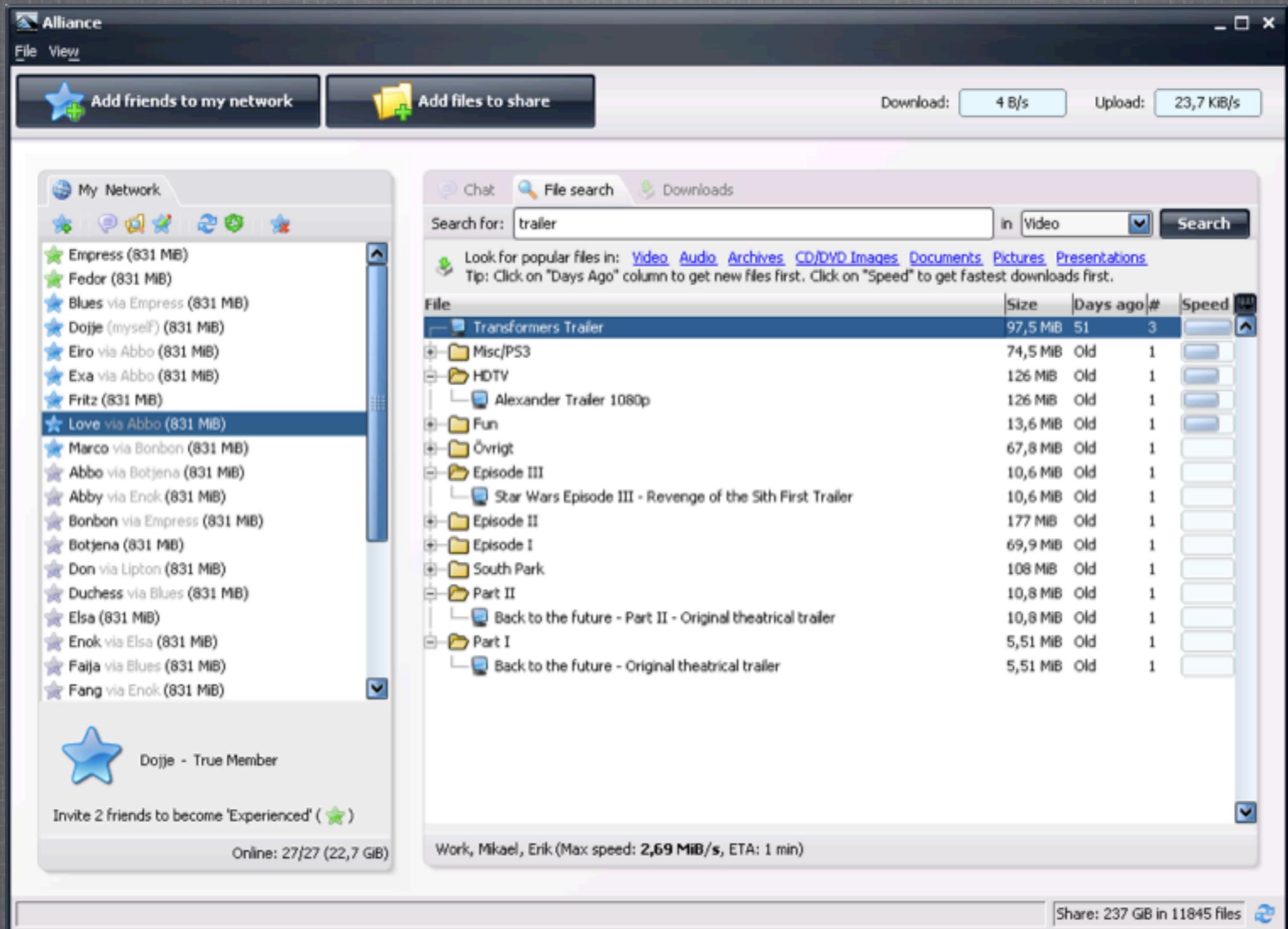




DARKNET IMPLEMENTATIONS

Retroshare: C++ / QT (Win/Lin/OS X)

AllianceP2P: Java (Win / Lin / OS X)



DARKNET IMPLEMENTATIONS

Retroshare: C++ / QT (Win/Lin/OS X)

AllianceP2P: Java (Win / Lin / OS X)

BRIGHTNETS

BRIGHTNETS

[...]

11. Anonymity in speech, communication and publishing is required for “Free Speech”
12. Reading, listening and watching are as much a part of the freedom of speech as writing, speaking, and performing.
13. Privacy in content discovery and access is required for “Free Speech” [Censorship]
14. Public access to published content is the fundamental reason for copyright’s existence.
 - a. "encouragement of learning"
 - b. Accessing legally made digital copies is unregulated by copyright and guaranteed by copyright law []
 - c. Libraries are good [same as above]

[...]

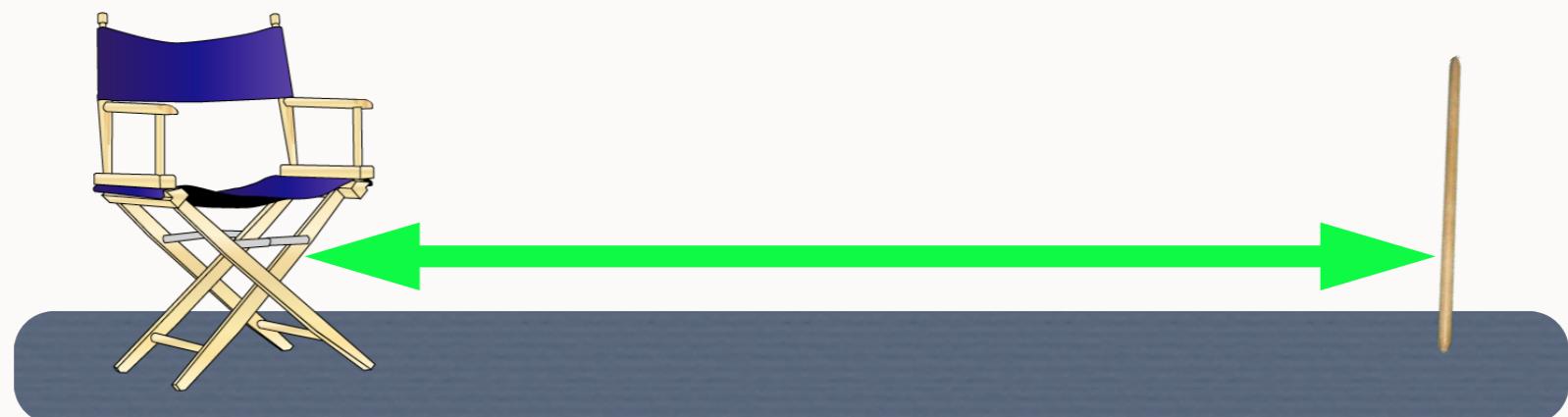
BRIGHTNETS

[...]

11. Anonymity in speech, communication and publishing is required for "Free Speech"
12. Reading, listening and watching are as much a part of the freedom of speech as writing, speaking, and performing
- "helping people NOT break the law and to not lose their existing rights"**
13. Privacy in content discovery and access is required for "Free Speech" [Censorship]
14. Public access to published content is the fundamental reason for copyright's existence.
 - a. "encouragement of learning"
 - b. Accessing legally made digital copies is unregulated by copyright and guaranteed by copyright law []
 - c. Libraries are good [same as above]

[...]

BRIGHTNETS



KURZE ZWISCHENFRAGE...

XOR?

Input A	Input B	XOR
1	1	0
1	0	1
0	1	1
0	0	0

BRIGHTNETS

Die Bibel.pdf



Goethe - Faust.pdf

CA1er7b/l?wwMp~T0dh

...

UKO4M2g-
SnxGxC.~IdyzECD 8y-
fu2uCL=p2AO=I03



VJ4lgK8e0~eC1
oO)7Q2D0arAueF~dFd
NIP9Bes[HCm

Verboten.mp3

DIE LUSTIGE COPYRIGHT SUCHE

Kai.Jaeger Ajax.in.der.Praxis.
2008.eBook.pdf

Britney.Spears.-.Random.Song.mp3

Marc Seeger – Current State of
anonymous filesharing.pdf



1010010110001001001001001010
1010010101010101010011110101
010101011010101001010000

DIE LUSTIGE COPYRIGHT SUCHE

Kai.Jaeger Ajax.in.der.Praxis.
2008.eBook.pdf

Britney.Spears.-.Random.Song.mp3

Marc Seeger – Current State of
anonymous filesharing.pdf



1010010110001001001001001010
10100101010101010011110101
010101011010101001010000

1. Neues Werk?

DIE LUSTIGE COPYRIGHT SUCHE

Kai.Jaeger Ajax.in.der.Praxis.
2008.eBook.pdf

Britney.Spears.–.Random.Song.mp3

Marc Seeger – Current State of
anonymous filesharing.pdf



1010010110001001001001001010
10100101010101010011110101
010101011010101001010000

1. Neues Werk?

Nein: Keine “geistige Schöpfung”
§2 II UrhG i.V.m §7

DIE LUSTIGE COPYRIGHT SUCHE

Kai.Jaeger Ajax.in.der.Praxis.
2008.eBook.pdf

Britney.Spears.-.Random.Song.mp3

Marc Seeger – Current State of
anonymous filesharing.pdf



1010010110001001001001001010
1010010101010101010011110101
010101011010101001010000

1. Neues Werk?

Nein: Keine “geistige Schöpfung”
§2 II UrhG i.V.m §7

2. Besteht altes Werk fort?

(Rückführbarkeit gewährleistet +
Jemand kann Urheberrecht behaupten)

DIE LUSTIGE COPYRIGHT SUCHE

Kai.Jaeger Ajax.in.der.Praxis.
2008.eBook.pdf

Britney.Spears.-.Random.Song.mp3

Marc Seeger – Current State of
anonymous filesharing.pdf



1. Neues Werk?

2. Besteht altes Werk fort?

(Rückführbarkeit gewährleistet +
Jemand kann Urheberrecht behaupten)

Nein: Keine “geistige Schöpfung”
§2 II UrhG i.V.m §7

Abhängig von Existenz anderer Blöcke?

DIE LUSTIGE COPYRIGHT SUCHE

Kai.Jaeger Ajax.in.der.Praxis.
2008.eBook.pdf

Britney.Spears.-.Random.Song.mp3

Marc Seeger – Current State of
anonymous filesharing.pdf



1010010110001001001001001010
1010010101010101010011110101
010101011010101001010000

1. Neues Werk?

2. Besteht altes Werk fort?

(Rückführbarkeit gewährleistet +
Jemand kann Urheberrecht behaupten)

Nein: Keine “geistige Schöpfung”
§2 II UrhG i.V.m §7

Abhängig von Existenz anderer Blöcke?

Problem: Jeder Block kann zu jedem anderen transformiert werden --> Jeder hätte Urheberrecht an allem?

DIE LUSTIGE COPYRIGHT SUCHE

Kai.Jaeger Ajax.in.der.Praxis.
2008.eBook.pdf

Britney.Spears.-.Random.Song.mp3

Marc Seeger – Current State of
anonymous filesharing.pdf



1010010110001001001001001010
10100101010101010011110101
010101011010101001010000

1. Neues Werk?

2. Besteht altes Werk fort?

(Rückführbarkeit gewährleistet +
Jemand kann Urheberrecht behaupten)

3. Gemeinsames Urheberrecht?

Nein: Keine “geistige Schöpfung”
§2 II UrhG i.V.m §7

Abhängig von Existenz anderer Blöcke?

Problem: Jeder Block kann zu jedem anderen transformiert
werden --> Jeder hätte Urheberrecht an allem?

DIE LUSTIGE COPYRIGHT SUCHE

Kai.Jaeger Ajax.in.der.Praxis.
2008.eBook.pdf

Britney.Spears.-.Random.Song.mp3

Marc Seeger – Current State of
anonymous filesharing.pdf



1010010110001001001001001010
1010010101010101010011110101
010101011010101001010000

1. Neues Werk?

2. Besteht altes Werk fort?

(Rückführbarkeit gewährleistet +
Jemand kann Urheberrecht behaupten)

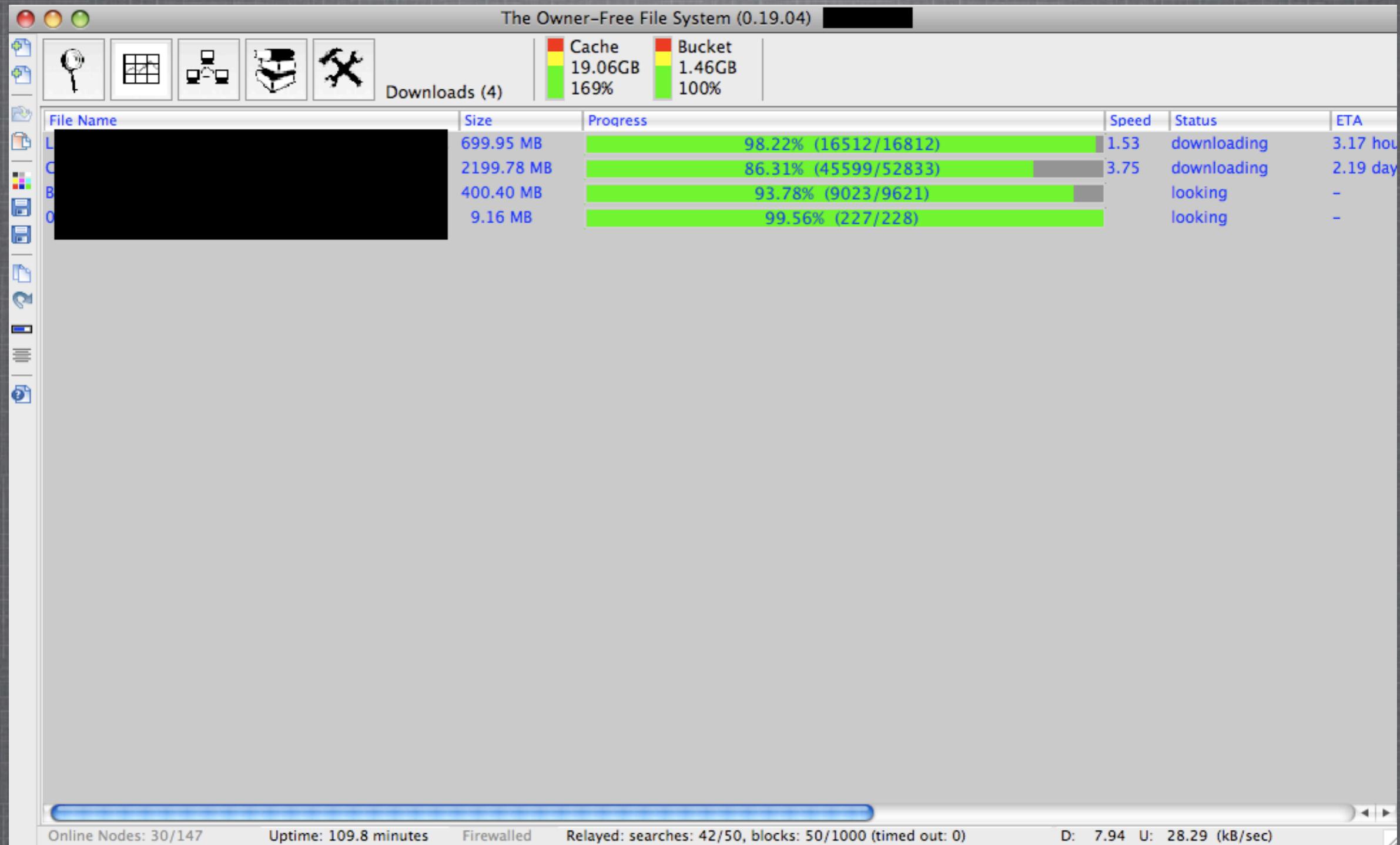
3. Gemeinsames Urheberrecht?

Nein: Keine “geistige Schöpfung”
§2 II UrhG i.V.m §7

Abhängig von Existenz anderer Blöcke?

Problem: Jeder Block kann zu jedem anderen transformiert werden --> Jeder hätte Urheberrecht an allem?

Miturheberschaft = “gemeinsame Schöpfung des Werkes”
§8 UrhG



OFF - OWNER FREE FILESYSTEM
C / WXWidgets (Win/Lin/OS X)

K



BYE