

(Keng) Panik am Netz!

Chaos Computer Club Lëtzebuerg A.S.B.L.

# Chaos Computer Club Lëtzebuerg (C3L)

- ✦ A.S.B.L.
- ✦ Gegrënnt 2008
- ✦ +/- 20 Memberen
- ✦ Tags:  
Informatiounssecherheet,  
Privatsphär, Datenschutz
- ✦ Politesch positionéiert,  
parteiolitesch neutral



# Initiativen

- ✦ entr0py
  - ✦ <http://entr0py.c3l.lu/>
- ✦ cypherpunks
  - ✦ <http://cypherpunk.lu>
- ✦ Freedom Not Fear (FNF)
  - ✦ <http://fnf.lu/>
- ✦ Repair Café
  - ✦ <http://repaircafe.lu/>

# Sam Grüneisen

- 23 Joër
- Erzéier bei der << Association Luxembourg Alzheimer >> (ALA) zu Ierpeldeng
- Finanzminister beim C3L & Präsident bei der << Frënn vun der Ënn >> (FVDE)
- Nick: virii
- Mail —> [virii@c3l.lu](mailto:virii@c3l.lu)
- Jabber (XMPP) —> [virii@adamas.ai](xmpp:virii@adamas.ai)
- Website: [adamas.ai](http://adamas.ai)
- (H)aktivist a politesch aktiv

# Dennis Fink

- ✦ 22 Joër
- ✦ Erzéier bei << Commune de Dudelange - Service Structures d'Accueil >> (Maison Relais)
- ✦ Aktiven Member vum C3L an Comité Member bei der FVDE
  - ✦ Haaptëntwéckler vun << ËnnStatus >>
- ✦ Nick: metalgamer
- ✦ Mail: [dennis.fink@c3l.lu](mailto:dennis.fink@c3l.lu)
- ✦ Jabber: [metalgamer@jabber.metalgamer.eu](jabber:metalgamer@jabber.metalgamer.eu)
- ✦ Website: <http://metalgamer.eu>
- ✦ Hacker/Musiker/Wëssenschaftler/Philosoph/Python Enthusiast/(H)aktivist/Evolutionären Humanist/Realist/Politker

# Jan Guth

- Chaos Computer Club Lëtzebuerg & Frënn vun der Ënn
- Erzéier an der Maison Relais << Haus vun de Kanner >> am Grond
- Student an der Informatik ob der OpenUniversity
- (H)aktivist
- KEEN Politiker
- Ireland

prometheus

Twitter: @JanGuth

w.: <http://avernak.is/>

e.: [prometheus@c3l.lu](mailto:prometheus@c3l.lu)

# Charel Lallemand

- ✦ Etudiant am Staadter Kolleisch
- ✦ Member fun C3L
- ✦ Member fun de Frenn van der Enn
- ✦ [charel.lallemand@gmail.com](mailto:charel.lallemand@gmail.com)

# CryptoWars

- ✦ Ugefangen huet et 1970
- ✦ Crypto = Waffen / Munitioun
- ✦ KEEN Export!
- ✦ 2005 eréicht gelockert ginn
- ✦ 2006 war de Cryptokriich eriwwer?



# Whistleblower

- Revelatiounen vu Whistleblower wéi dem Edward Snowden an dem Bradley / Chelsea Manning weisen den Géigendeel
- Systematesch probéiert' Crypto ze schwächen
- Geheimdängschter involvéiert
- Trotzdem Crypto bléift eis eenzeg Hoffnung
- Cypherpunk Movement gout gestäerkt!





Android

# TextSecure

(ab Android Version 2.3)

- OpenSource
- Verschlüsselt SMSen / MMSen
- Ersatz für den Standard SMS / MMS Programm
- Empfänger muss ebenfalls TextSecure installiert haben
- iOS Version auch an der Maach



# RedPhone

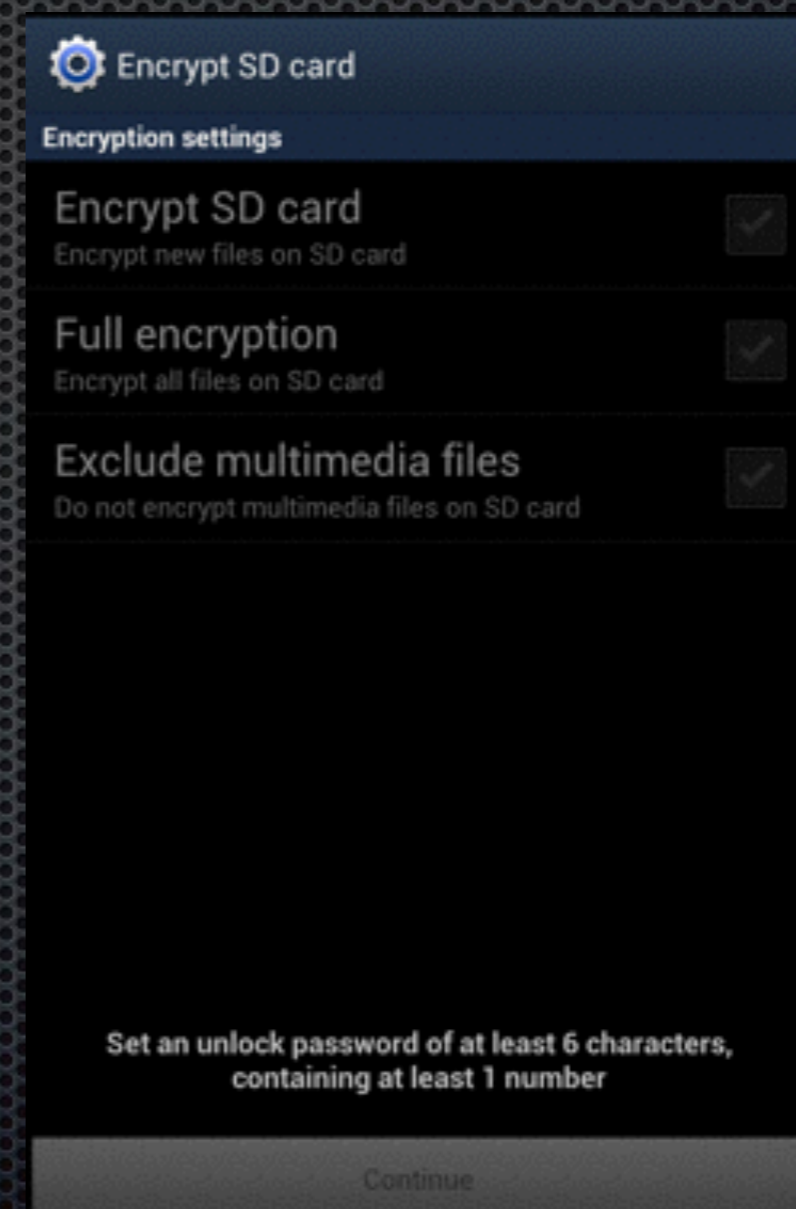
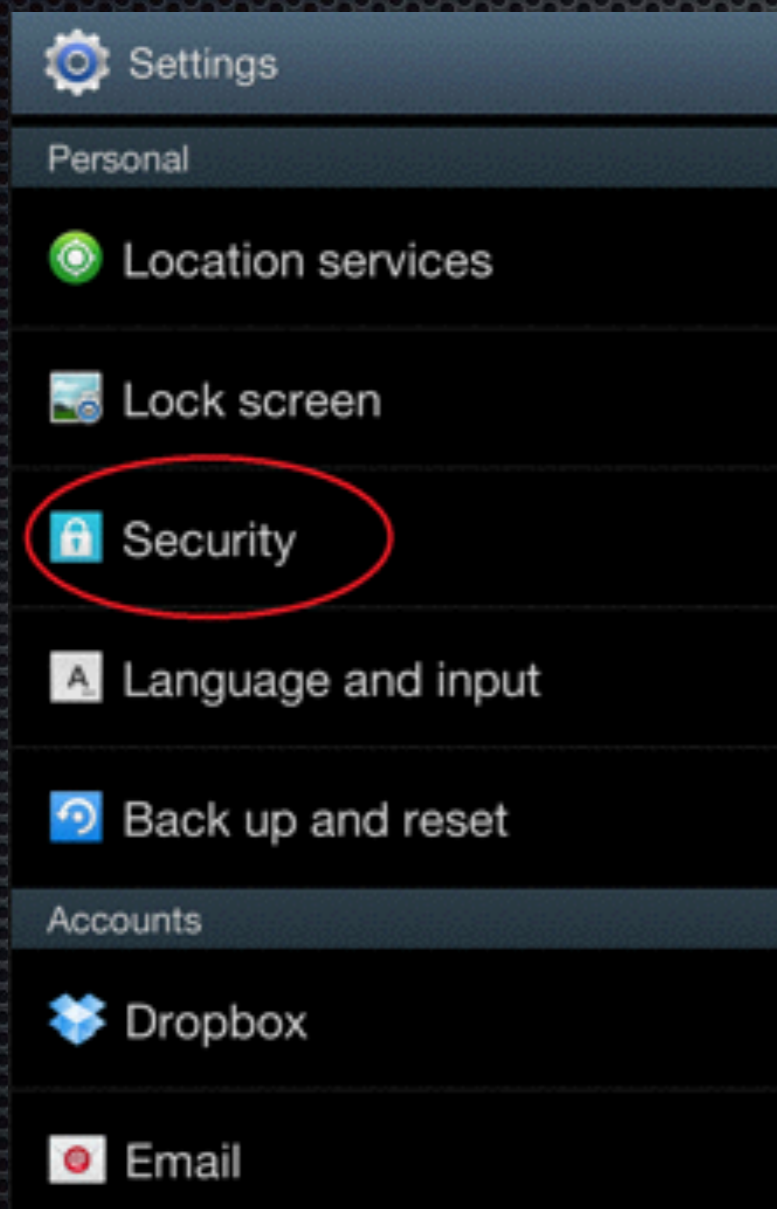
(ab Android Version 2.3)



- ✦ OpenSource
- ✦ Verschlüsselt Telefonater
- ✦ Ersatz fir den Standard Telefonsprogramm
- ✦ Empfänger muss ebenfalls RedPhone installéiert hunn

# SD Kaart verschlüsselen

(Ab Version 2.3.4)



iOS

Think different.



# iOS Security

## **System Architecture**

- ✦ App Sandboxing
- ✦ App Store Review Process
- ✦ ARM's Execute Never (XN)

## **Encryption and data protection**

- ✦ Hardware Encryption
- ✦ Third-Party App Data Protection
- ✦ Tangling

# iOS Security

## Network Security

- ✦ Built-In VPN / Per App VPN
- ✦ OCSP Support
- ✦ Bluetooth

## Device Access

- ✦ Restrictions
- ✦ OTA Passcode Enforcement
- ✦ Remote Wipe

## More information:

<http://www.apple.com/iphone/business/it/security.html>



# Apps

## Open Source

- ✦ Open Whisper Systems
  - ✦ RedPhone
  - ✦ TextSecure
- ✦ OpenVPN

## Partly Open Source

- ✦ SilentCircle

## Closed Source

- ✦ Seecrypt
- ✦ Wickr
- ✦ Encrypt SMS

# Wickr

*“[Wickr DOES NOT USE, COPY OR MODIFY USER DATA. IT’S IMPOSSIBLE FOR US TO DO THIS AS DATA IS ENCRYPTED AND WE CAN’T READ IT]”*



# (Smart)SpyPhones

- ✦ Keng sensibel Daten ob den SmartPhones! (z.B.: Passwierder, Keys, etc.)
- ✦ Keen SmartPhone benotzen fir sensibel Kommunikatioun!
- ✦ Sou mann wéi méiglech Apps!



# Football World Cup 2014



4 Mol sou vill Apps

## Spiele

## Gruppen

## Zweite Runde

## Gruppe A

	Land	SP	S	U	N	T	GT	TD	PKT
1	 Brasilien	2	1	1	0	3	1	2	4
2	 Mexiko	2	1	1	0	1	0	1	4
3	 Kamerun	1	0	0	1	0	1	-1	0
4	 Kroatien	1	0	0	1	1	3	-2	0

## Gruppe B

	Land	SP	S	U	N	T	GT	TD	PKT
1	 Niederlande	1	1	0	0	5	1	4	3
2	 Chile	1	1	0	0	3	1	2	3
3	 Australien	1	0	0	1	1	3	-2	0
4	 Spanien	1	0	0	1	1	5	-4	0

## Gruppe C

	Land	SP	S	U	N	T	GT	TD	PKT
1	 Kolumbien	1	1	0	0	3	0	3	3
2	 Elfenbeinküste	1	1	0	0	2	1	1	3
3	 Japan	1	0	0	1	1	2	-1	0
4	 Griechenland	1	0	0	1	0	3	-3	0

## Gruppe D

	Land	SP	S	U	N	T	GT	TD	PKT
1	 Costa Rica	1	1	0	0	3	1	2	3
2	 Italien	1	1	0	0	2	1	1	3
3	 England	1	0	0	1	1	2	-1	0
4	 Uruguay	1	0	0	1	1	3	-2	0

## Gruppe E

	Land	SP	S	U	N	T	GT	TD	PKT
1	 Frankreich	1	1	0	0	3	0	3	3
2	 Schweiz	1	1	0	0	2	1	1	3
3	 Ecuador	1	0	0	1	1	2	-1	0
4	 Honduras	1	0	0	1	0	3	-3	0

## Gruppe F

	Land	SP	S	U	N	T	GT	TD	PKT
1	 Argentinien	1	1	0	0	2	1	1	3
2	 Iran	1	0	1	0	0	0	0	1



Niederlande

1. in Gruppe B

[Spiele](#)

[Tabelle](#)

Heute, 18:00 - Gruppe B  
Estádio Beira-Rio, Porto Alegre



Australien

gegen

Niederlande



[Spielverlauf](#)

[Statistiken](#)

[Aufstellungen](#)

Das Spiel beginnt am Mi., 18. Juni um 18:00.

[🌐 Spielvorschau](#)

#### Weitere Spiele dieser Mannschaft (Niederlande)

Fr., 13. Juni, 21:00 gegen  Spanien **G 5 – 1** Beendet

Mo., 23. Juni, 18:00 gegen  Chile

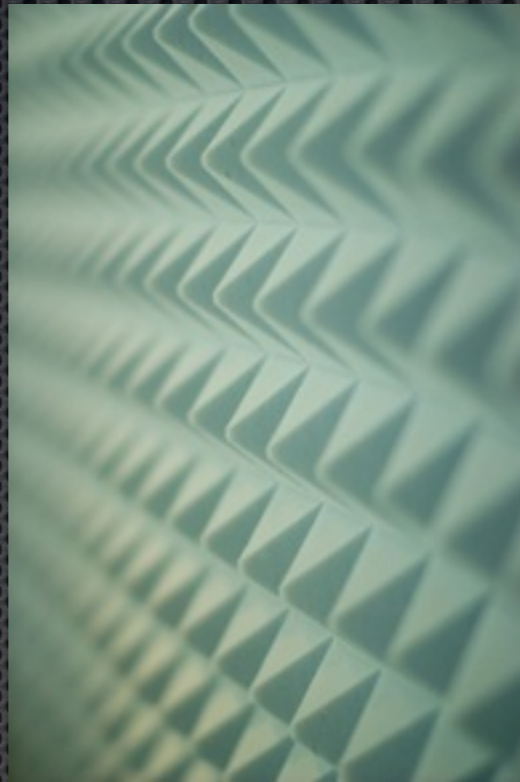
Alle Zeitangaben: Mitteleuropäische Zeit

Mehr auf [FIFA.com](http://FIFA.com)

# Secher Gespréicher



+



oder



- Keksdose, Konservendous, etc.
- Ausgekleed mat Schalldämmungsmaterial
- Oder an den Tiefkühler (awer net ze laang)!

# Secher Kommunikation am Schnellduerchloaf

1. Boar Geld
2. Aal, mee kompatibel  
GSMen koafen
3. SIM Koart mat Cash  
bezuelen
4. 1 Mol benotzten
5. An dem Bouttik nees lass  
ginn







XMPP

Och nach Jabber  
genannt

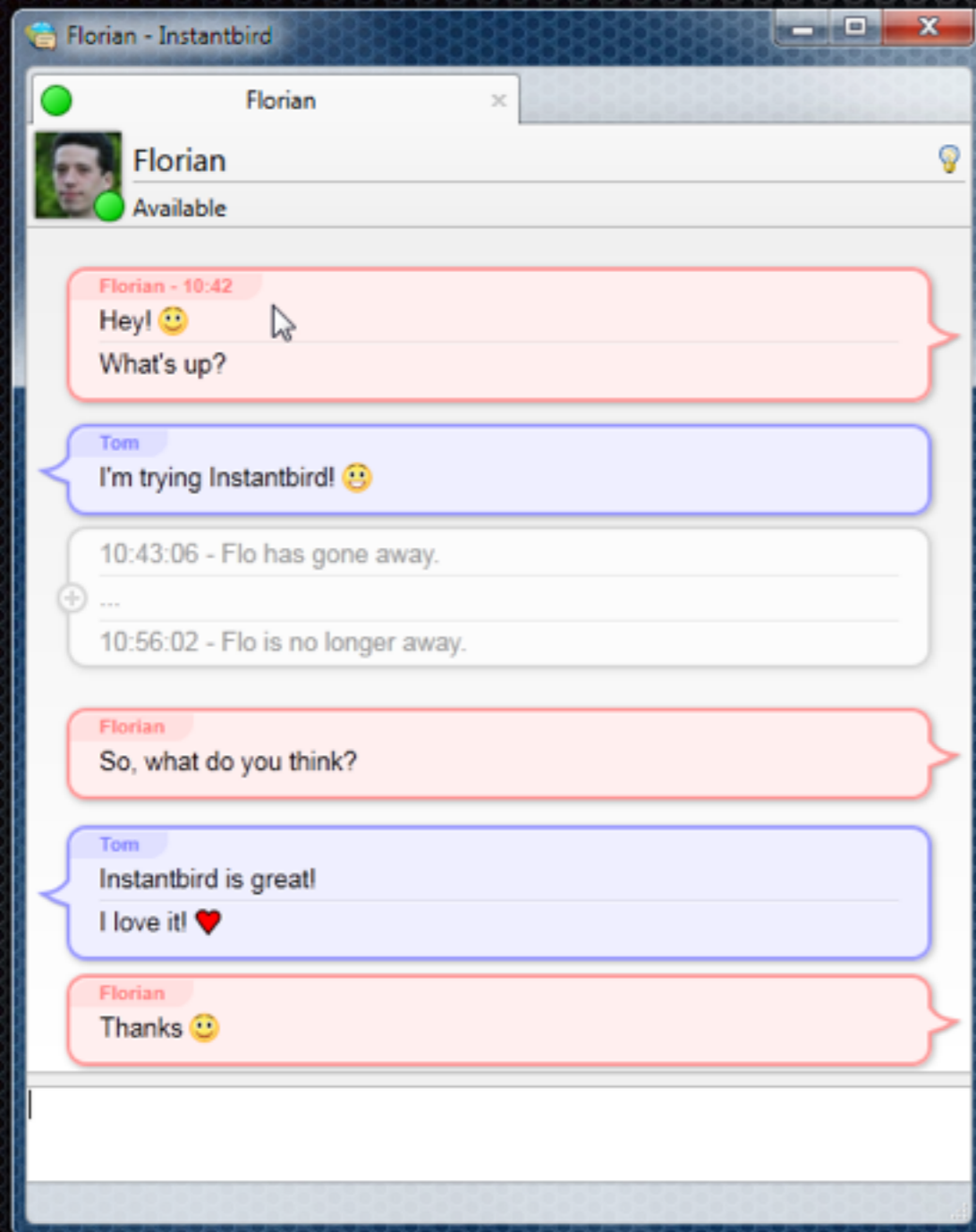
**XMPP**

# XMPP (Jabber)

- ✦ Dezentralisiert
- ✦ Open Standard
- ✦ Sicherheit
- ✦ Dynamik



# Alternativ zu...



- ✦ iMessage
- ✦ Facebook Chat
- ✦ What's App
- ✦ SnappChat
- ✦ etc.

# ChatSecure

- Free/Libre Open Source Software (F/LOSS)
- Verschlüsselten Chat iwwert XMPP (Jabber)
- Alternativ fir iMessage, Facebook Chat, WhatsApp, etc.
- Verfügbar fir Android & iOS
- Optional: mat Orbot och iwwert Tor



# Jitsi

- ✦ **Verschlüsselten** Video Chat  
iwwert XMPP (Jabber)
- ✦ Open Source
- ✦ **Alternativ zu Skype**
- ✦ **Features:** HD, Konferenzen, DesktopSharing



00:02:33 | Call

ptankov@jit.si (me)

chenzo@jit.si zrtp connected

d@jit.si zrtp connected

joro@jit.si zrtp connected

yana@jit.si zrtp connected

Hristo@jit.si connecting

00:01:01 | Call  
d@jit.si (d@jit.si/jitsi-39v9sil)

zrtp Connected

candy@jit.si

candy@jit.si x e@jit.si

yana@jit.si (Jabber) Mar 10, 2013 11:15:27  
I can also send it to you  
Let me check if I have donwload it

candy@jit.si Mar 10, 2013 11:15:43  
Ok that would be nice  
Looks very nice  
How long is it actually?

yana@jit.si (Jabber) Mar 10, 2013 11:16:59  
I'm not sure  
You can get more information here:  
<http://www.sintel.org/>  
And here it's the download:

Feb 21, 2013 15:27:03 Receiving file from yana@jit.si.  
sintel-2048-surround.mp4 (296.3 MB)

10.6 MB received

Cancel Speed:43.0 K/sec Estimated time:1 h 53 min 29 sec

00:03:52 | Call



demo3@demo.jit.si (me)



★ Demo2 User

connected



Demo11 User

connected



Demo4 User

connected



Demo6 User

connected



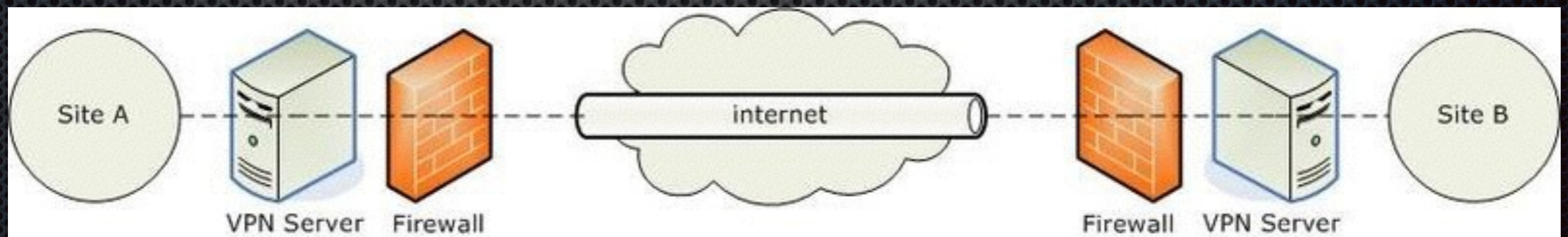
# VPN

- Virtual Private Network
- Kengem trauen!
- Selwechten Prinzip wéi bei den GSMen

- Hoster Lëscht:

[http://wiki.c3l.lu/  
doku.php?](http://wiki.c3l.lu/doku.php?)

[id=projects:providers#v  
pn](http://wiki.c3l.lu/doku.php?id=projects:providers#vpn)







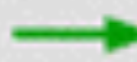
# Tor

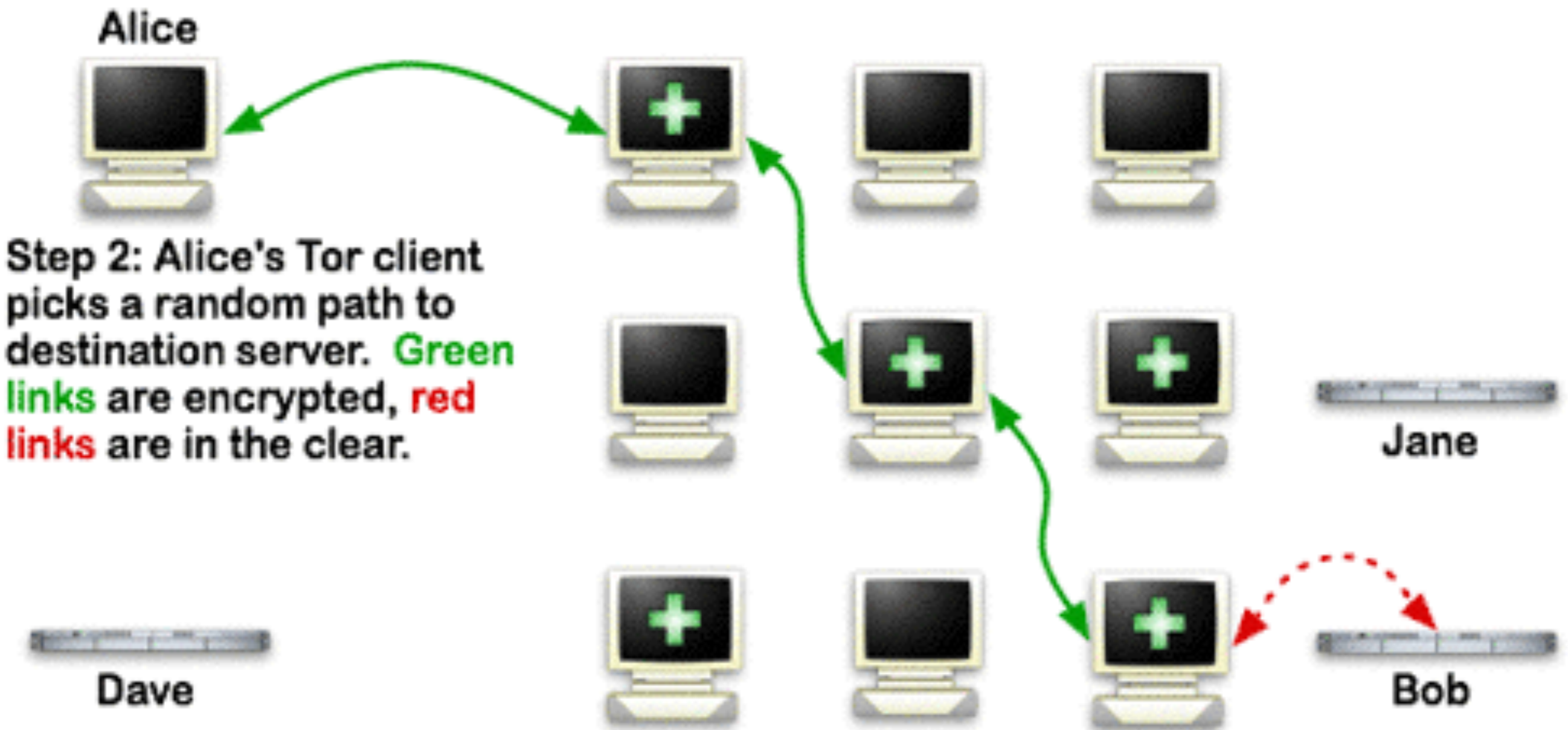
- ✦ Erlaabt ët “**anonym**” am Internet kënnen ze surfen
- ✦ Verschlësselt' Verbindungen
- ✦ Et kann een net erausfannen vun wou een sech konnektéiert



# How Tor Works: 2

Legend:

-  Tor node
-  unencrypted link
-  encrypted link



Step 2: Alice's Tor client picks a random path to destination server. **Green links** are encrypted, **red links** are in the clear.

Dave

Jane

Bob

# Ween benotzt Tor?

- ✦ Journalisten
- ✦ Whistleblower
- ✦ Leit an repressiven Staaten
- ✦ Leit déi zwengend anonym müsse sinn
- ✦ Och Lëtzebuurger! +/- 1600 Stéck (Stand: 15ten Juni 2014)

# Frënn vun der Ënn A.S.B.L.

- 2013 gegrënnt ginn (bei der éischer CryptoParty)
- Bedreiwen Tor Serveren (Bridges, Relays, Exits)
- Sinn eng Suborganisatioun vum C3L
- 26 Server um laafen (weltwäit)
- Kréien Réckendeckung vun engem Affekot
- Iwwerliewen duerch Spenden
- Eng vun 13 Partnerorganisatiounen

# Tails

- ✦ Live Betriebssystem (Operating System)
- ✦ **ALL** Verbindung geht iwwert Tor
- ✦ Einfach op den USB Stick oder ob eng CD gebrannt
- ✦ Starten a voila.
- ✦ Kann een als “normalen” Windows tarnen
- ✦ <https://tails.boum.org/>

- Computer
- amnesia's Home
- Trash
- Tails documentation
- Report a Bug

Are you using Tor? - Iceweasel

File Edit View History Bookmarks Tools Help

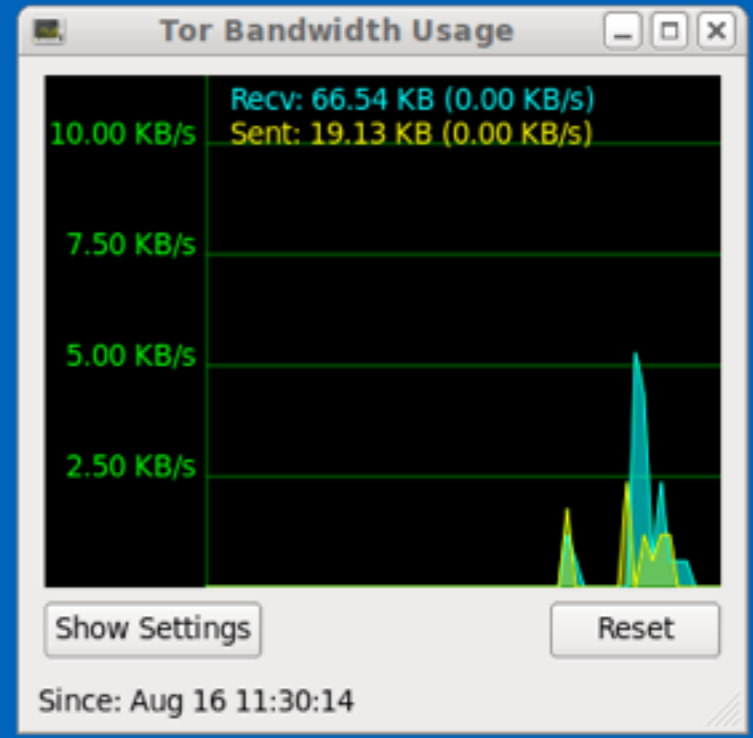
Are you using Tor?

https://check.torproject.org



**Congratulations. Your browser is configured to use Tor.**

Please refer to the [Tor website](https://www.torproject.org/) for further information about using Tor safely. You are now free to browse the Internet anonymously.



# OrBot

- Free/Libre Open Source Software (F/LOSS)
- Tor App fir Android
- OrWeb
  - Browser deen alles duerch Orbot tunnelt
- All App déi “Proxies” ënnerstetzt kann OrBot benotzen, z.B.: Offiziell Twitter App
- Fir d’Experten: bei gerootetem Android kann et wéi Tails benotzt ginn





# Alternatives

You do have a choice!



# Süchmaschinen



# ixquick & StartPage

- Surfboard Holding B.V.
- Sëtz zu New York an an den Niederlanden
- No eegener Ausso “the world’s most private search engine”
- Geéiert mam EU Datenschutzgütesiegel (14 Juli 2008)
- ixquick: Metasuchmaschinn
- startpage: beziit hier Resultater just vun Google (agéiert als Mëttelsmann)



# DuckDuckGo



- ✦ Programméierer: Gabriel Weinberg
- ✦ Hybrid (Meta + Crawler)
- ✦ No eegener Ausso *“The search engine that doesn’t track you.”*
- ✦ Réckfroen fir méi schnell dat gesichten Resultat ze fannen

# Réckfroën

The image shows a search engine results page for the query "Ireland". A green oval highlights the top row of results, which includes the main search result and several related terms. Below this row, there are several sponsored links and organic search results.

**Search Results:**

- Ireland**: An island in the Atlantic off the north-western coast of mainland Europe.
- Kathy Ireland**: An American model, actress, and entrepreneur.
- Jill Ireland**: An English actress, best known for her many films with her second husband, Charles.
- Éire**: The Irish name for the island of Ireland and the sovereign state of the same name.
- Ireland, Bedfordshire**: A hamlet in the civil parish of Southill, Bedfordshire, England.
- Ireland, Indiana**: An unincorporated community in Madison Townships, Dubois County, Indiana.
- Ireland, West Virginia**: An unincorporated community in Lewis County, West Virginia, United States.
- Ireland Island, Bermuda**: The northwesternmost island in the chain which comprises Bermuda.
- New Ireland Island**: A large island in Papua New Guinea, approximately 7,404 km<sup>2</sup> in area with ca. 120,000 people.
- Alexander Ireland**: A Scottish amateur and professional welter/middleweight boxer of the 1920s and '30s, who
- Andy Ireland**: A U.S. Representative from Florida.

**Sponsored Links:**

- Ireland jumpsuit**: Black and white Jungle Diamond print Silk-chiffon Self-tie skinny... [matchwefashion.com](#) Sponsored link

**Organic Search Results:**

- Ireland - Wikipedia, the free encyclopedia**: Ireland is an island in the North Atlantic to the west of Great Britain, from which it is separated by the North Channel, the Irish Sea and St Georges Channel, and after which it is the largest island of the British Isles archipelago. It is the third-largest island in Europe and the ... [en.wikipedia.org](#)
- Visit Ireland | Springtime in Ireland | Discover Ireland**: Browse Discover Ireland to plan an action-packed springtime in Ireland. See what's going on around the country and find information on where to stay and special offers. There's so much to do this spring for all the family, so make sure you have the perfect holiday. [discoverireland.ie](#)
- Ireland : Vacations in Ireland - Official Vacation Website ...**: Official Website of Tourism Ireland for visitors to Ireland. Information on accommodation in Ireland, activities in Ireland, events in Ireland and much more. [ireland.com](#)
- Ireland: Maps, History, Geography, Government, Culture, Facts ...**: Information on Ireland — geography, history, politics, government, economy, population statistics, culture, religion, languages, largest cities, as well as a map and the national flag. [infoplease.com](#)
- Ireland Tourism: 4,143 Things to Do in Ireland | TripAdvisor**: Ireland Tourism: TripAdvisor has 876,292 reviews of Ireland Hotels, Attractions, and Restaurants making it your best Ireland resource. [tripadvisor.com](#)
- Ireland: Information, News, Maps, History, Genealogy ...**: Ireland Information including News, Maps, History, Genealogy, Geography, Government, Culture, Facts, Tourist & Travel Guide and much more. [ireland-information.com](#)
- Ireland travel guide - Wikitravel - Wikitravel - The Free ...**: Open source travel guide to Ireland, featuring up-to-date information on attractions, hotels, restaurants, nightlife, travel tips and more. Free and reliable advice written by Wikitravellers from around the globe. [wikitravel.org](#)
- Country of Ireland - State**: Country portal offers a map and links to Background Notes, the US embassy and the current ambassador, press releases, fact sheets, annual Human Rights Reports and other major reports including Industry Market Reports.

# TrueCrypt

- ✦ Gëtt benotzt fir Festplatten ze verschlësselen oder “Container”
- ✦ Einfach ze benotzen
- ✦ OpenSource an GRATIS
- ✦ Gëtt et fir Windows, Mac OS & GNU/Linux
- ✦ <http://truecrypt.ch/>

# Image Sources

- ✦ [epSos.de](http://epSos.de)
- ✦ <https://www.flickr.com/photos/33256665@N00/111066379/>