

# - Tor Hidden Service (.onion) search -

AHMIA.FI

Juha Nurmi  
juha.nurmi@ahmia.fi



# Disclaimer

- These slides represent my personal assessment of the Ahmia software project.
- It is not an official presentation of any organizations mentioned in the slides.
- Do not quote this document as a work of these organizations.
- Contains humor!

# Summary

- What is Tor?
- How it works?
- How hidden services are working?
- Why anonymity is important?
- What are the adversaries of privacy?
- Some numbers about Tor
- Security issues with Tor
- Tor in popular news
- Statistics about the content
- My own project: Ahmia Search Engine

# Me



- Hacker/Researcher/Lecturer/Software engineer etc.
- I like to cook good and healthy food, read books and walk in the nature → I am doing this more than anything else everyday :-)
- My other hobbies are math, science, bicycling, networks, gym, Linux, programming, logic, fishing, cryptography, computer and network security, web services, distributed systems, biology, psychology, data mining, chemistry, physics... and listening good music with expensive sound systems
- Furthermore, I am making my own beers



# Peer-to-Peer Networks in general

- Many aspects of Peer-to-Peer networks are fascinating

*"Yes, [we will not find a solution to political problems in cryptography,] but we can win a major battle in the arms race and gain a new territory of freedom for several years. Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own."*

- Satoshi Nakamoto, the creator of Bitcoin



# P2P systems are changing the world

## New things like

- Ethereum
- WebRTC



## And systems that are already there

- BitTorrent
- Bitcoin
- **Tor** → Let's talk about it today :-)

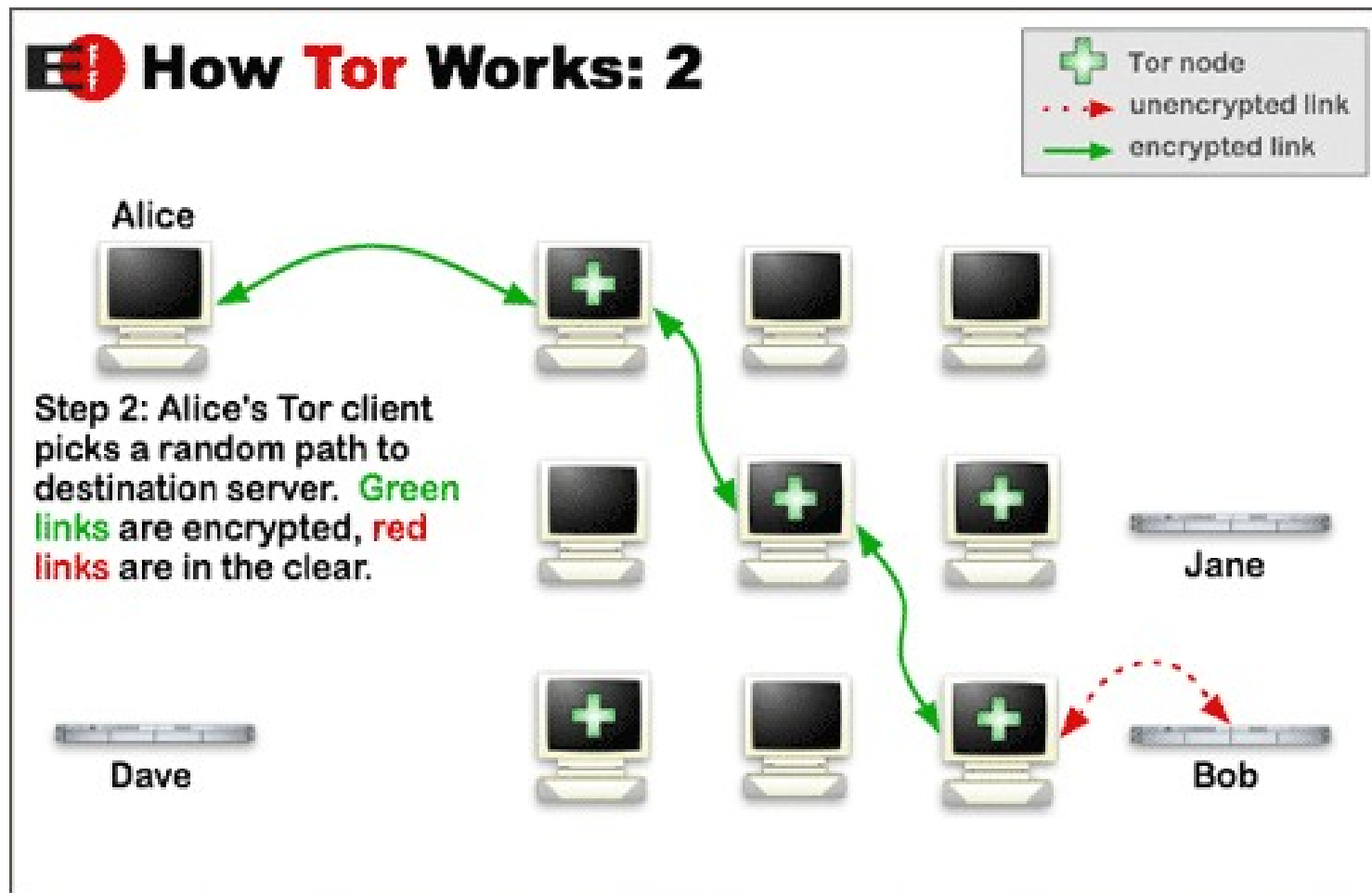




- Tor is an anonymity tool
- It helps people to circumvent censorship
- Share, publish and talk anonymously

According to top secret NSA documents disclosed by a whistleblower Edward Snowden, the Tor network has been too hard to spy by NSA and CIA. NSA even wrote in their top secret documents that **Tor is “the King of high secure, low latency Internet Anonymity”**.

# Anonymous TCP connections





# Why anonymity?

Anonymity is an important right in order to support freedom of speech and defend human rights.

*“Those who surrender freedom for security will not have, nor do they deserve, either one.”*

- Benjamin Franklin, one of the Founding Fathers of the United States

*"[Tor is a] part of an ecosystem of software that helps people regain and reclaim their autonomy. It helps to enable people to have agency of all kinds; it helps others to help each other and it helps you to help yourself. It runs, it is open and it is supported by a large community spread across all walks of life."*

*- Jacob Appelbaum*



# Tor has to defeat very powerful adversaries

- Orwellian surveillance system maintained by
  - China
  - Russia
  - United States
  - UK
  - Sweden
  - etc.



# ECHELON, year 2000

During 2000 ECHELON was investigated by a committee of the European Parliament. That was before 9/11. The international internet mass surveillance system did exist and yet it didn't prevent any terrorist attacks.

European Parliament resolution on the existence of a global system for the interception of private and commercial communications (Echelon interception system) (2001/2098(INI))

# Some quotes from the report

*“the existence of a global system for intercepting communications, operating by means of cooperation proportionate to their capabilities among the US, the UK, Canada, Australia and New Zealand under the UK USA Agreement, is no longer in doubt”*

# Some quotes from the report

*“no doubt that the purpose of the system is to intercept, at the very least, private and commercial communications, and not military communications”*

# Some quotes from the report

*“there is also ample evidence that Russia is likely to operate such a system”*



# Some quotes from the report

*“intelligence system which intercepted communications permanently and at random would be in violation of the principle of proportionality and would not be compatible with the ECHR”*



# Some quotes from the report

*“the Member States cannot circumvent the requirements imposed on them by the ECHR by allowing other countries’ intelligence services, which are subject to less stringent legal provisions, to work on their territory”*

# Some quotes from the report

*“private individuals should also be urged to encrypt e-mails; whereas an unencrypted e-mail message is like a letter without an envelope”*

# Finally it hits the mainstream media



*“Now, increasingly, we see that it’s happening domestically. And to do that, they - **the NSA specifically targets the communications of everyone.** It ingests them **by default.** It collects them in its system, and it filters them, and it analyzes them, and it measures them, **and it stores them** for periods of time, simply because that’s the easiest, most efficient and most valuable way to achieve these ends.”*

*- Edward Snowden*



facebook



Hotmail®

YAHOO!



YouTube



(TS//SI//NF)

## PRISM Collection Details



## Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection  
(Surveillance and Stored Comms)?

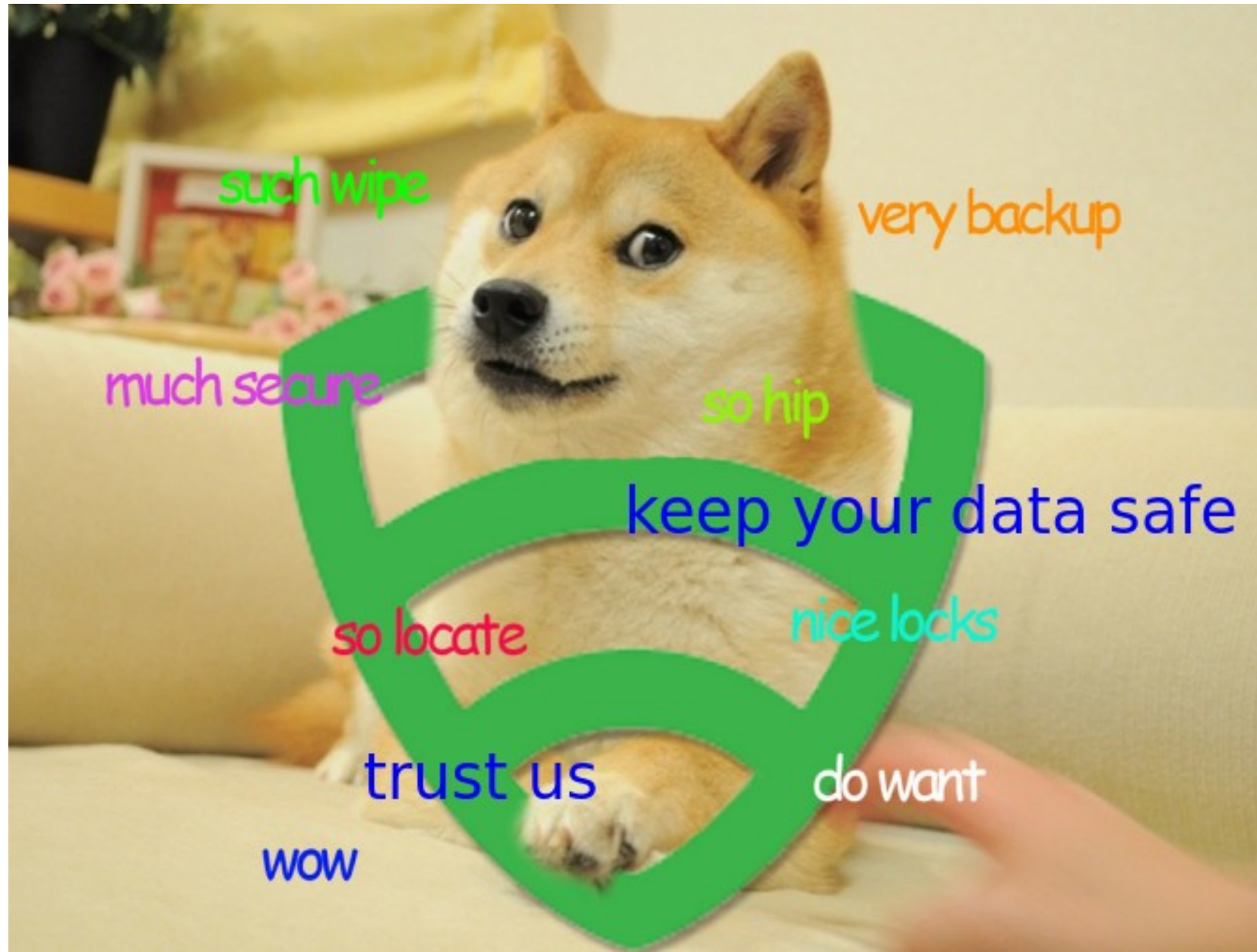
It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:  
Go PRISMFAA



# Hushmail, Gmail, Facebook, Skype: Privacy by trust









- **Privacy by design**
- Assumes that the network is under surveillance
- Assumes that some of the routers may be configured by the attackers
- Hybrid P2P network



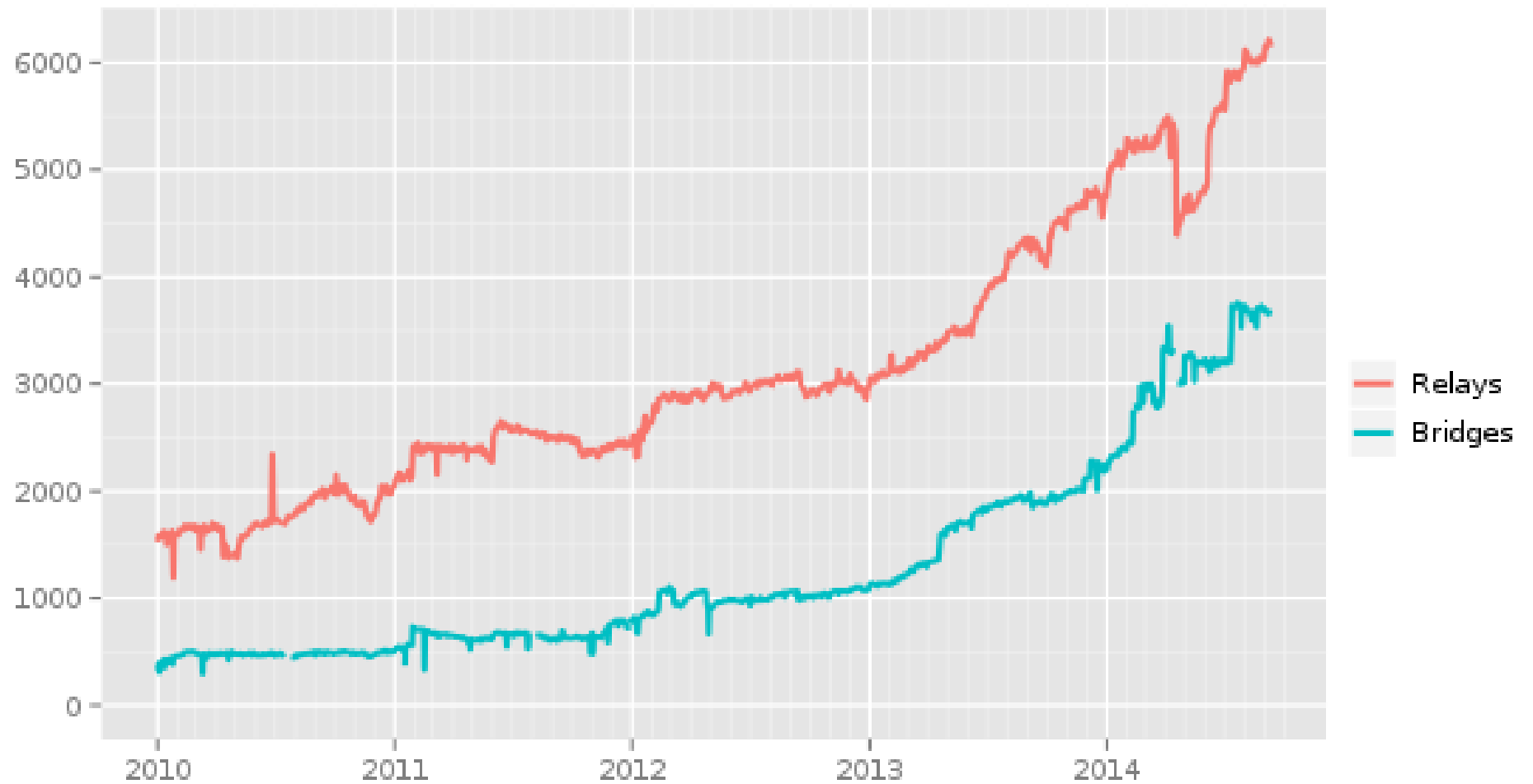
# Different types of relays

- **Guard**: This relay is suitable to be the first hop in a Tor circuit.
- **HSDir**: This relay is a v2 hidden service directory.
- **Exit**: This relay is configured to be the last hop in a Tor circuit.
- **Named**: This relay has a nickname.
- **Running**: This relay has been online within the past 45 minutes.
- **Stable**: This relay is considered stable.
- **V2Dir**: This relay supports the v2 directory protocol.
- **Valid**: This relay is running a working Tor version without any problems.
- **Unnamed**: This relay's configured nickname is used by another relay.
- **BadExit**: This relay breaks stuff, either maliciously or through misconf.
- **Fast**: This relay has lots of bandwidth available.

The Tor user is only a client by default.

There are also hidden relays, [bridges](#).

## Number of relays



The Tor Project - <https://metrics.torproject.org/>

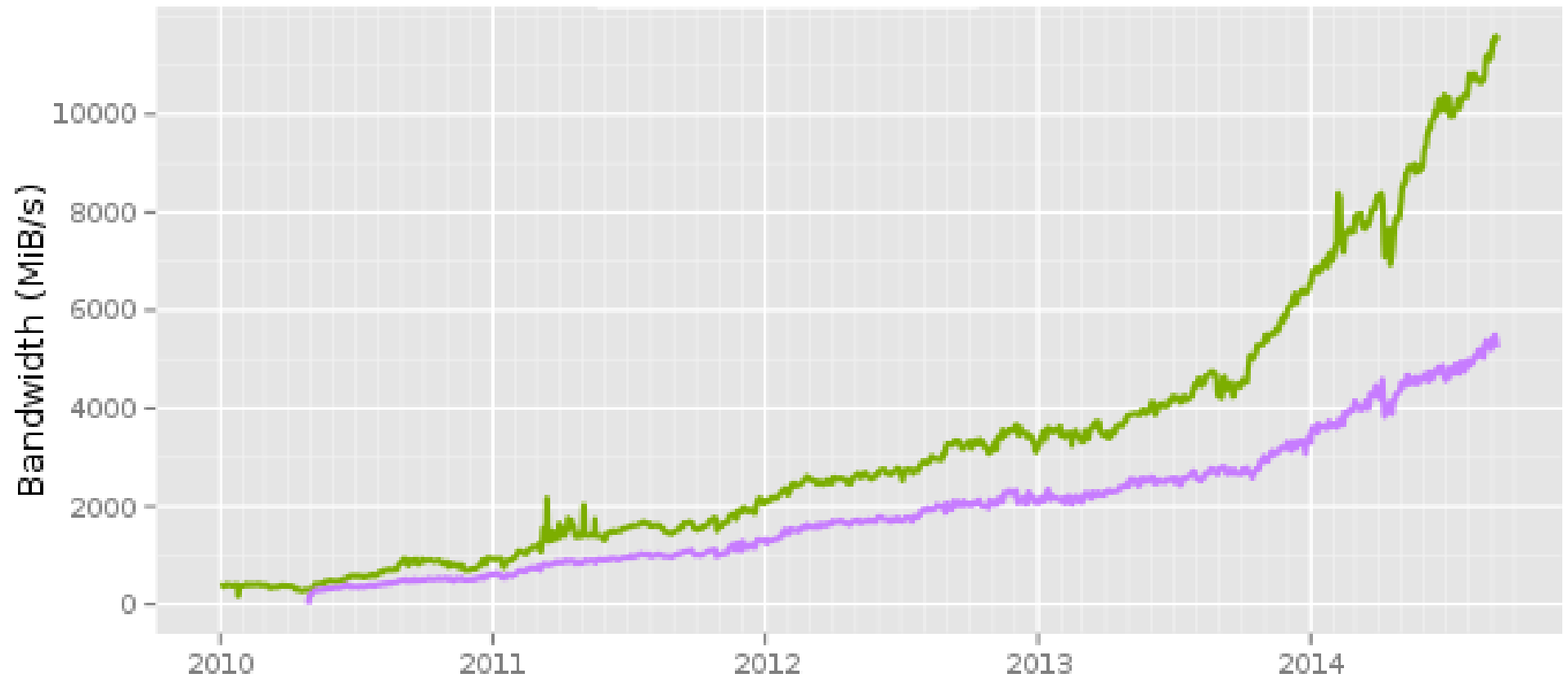
## Number of relays with relay flags assigned



The Tor Project - <https://metrics.torproject.org/>

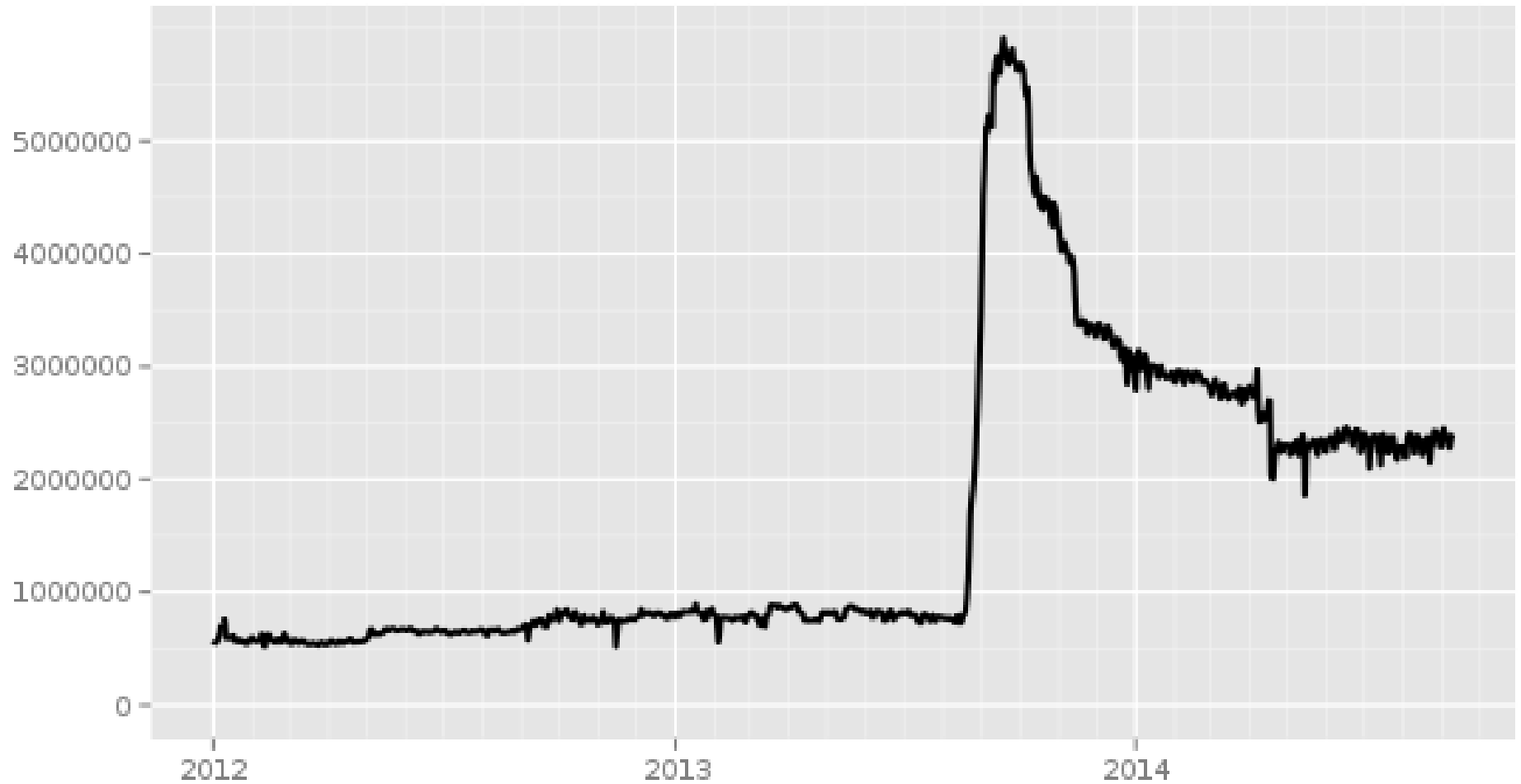
## Total relay bandwidth

- Advertised bandwidth
- Bandwidth history



The Tor Project - <https://metrics.torproject.org/>

## Directly connecting users



The Tor Project - <https://metrics.torproject.org/>

<b>Country</b>	<b>Mean daily users</b>
United States	333787 (14.30 %)
Germany	205966 (8.82 %)
Russia	160892 (6.89 %)
France	140281 (6.01 %)
Brazil	125736 (5.39 %)
Spain	93290 (4.00 %)
United Kingdom	90056 (3.86 %)
Italy	85867 (3.68 %)
Poland	65119 (2.79 %)
Argentina	55789 (2.39 %)

# Security issues

- Fortunately, there are no known cases where someone would be identified because of security issues in The Onion Routing
- However, there have been multiple security issues around Tor and the software people use around Tor



# Security issues

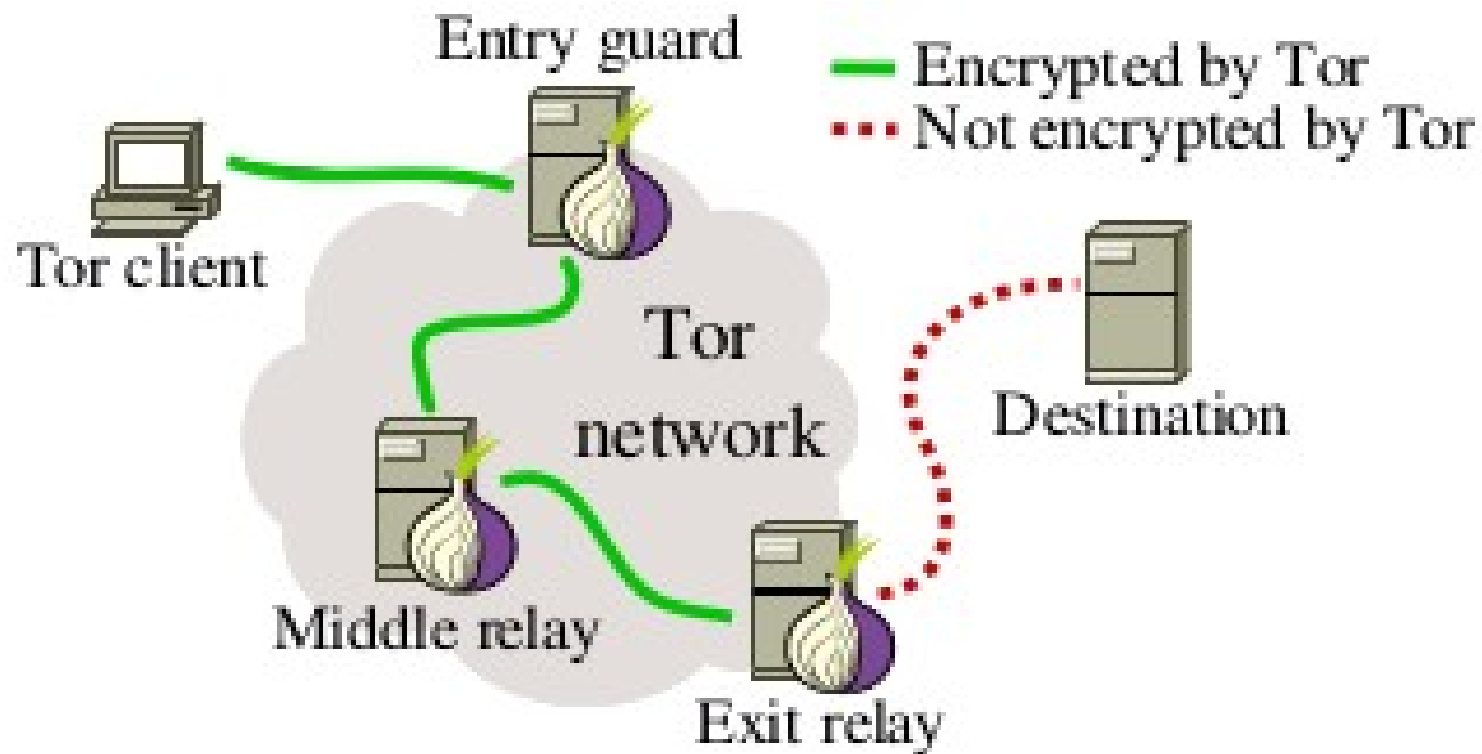
- 2014: "relay early" traffic confirmation attack
- 2013: JavaScript attack in the Tor-Browser
- Fingerprinting attacks against the Tor-Browsers
- Tor traffic correlation attacks by global adversaries





# Security issues

## Rotten exit nodes



# Security issues

- The code from the National Security Agency's XKeyscore software reveals the NSA's interest in anyone who uses Tor
- Targeted Sebastian Hahn's servers
- The NSA has been revealed to mark and consider potential "extremists" all users of Tor



# Hidden services

- Servers configured to receive inbound connections through Tor are called **hidden services**
- Rather than revealing a server's real IP address, a hidden service is accessed through the Tor network using **.onion** address



# Hidden services

- XYZ.onion where XYZ is a 16 character name derived from the service's public key
- <http://msydaqstlz2kzerdg.onion/>
- (or with proxy link <https://msydaqstlz2kzerdg.tor2web.fi/> which is not safe but works without Tor)

# Popular news

- Unfortunately, many times the popular news about Tor are telling about drugs, guns and child porn → bad for Tor's reputation
- In reality, there are only few these kind of sites
- Ahmia has the real statistics:
  - Less than 20 child porn sites
  - Less than 10 black markets
  - A few scamming sites

# A simple glance to what is published on the hidden websites





# Black Market







**ACT NOW!**

THESE GUNS ARE FOR SALE ONLINE







**Silk Road**  
anonymous market

messages 0 | orders 0 | account B0

Search

Go

Shop by Category

Drugs 4,086

Cannabis 983

Dissociatives 77

Ecstasy 318

Opioids 350

Other 157

Precursors 18

Prescription 901

Psychedelics 587

Stimulants 405

Apparel 82

Art 5

Books 778

Collectibles 15

Computer equipment 42

Custom Orders 27

Digital goods 369

Drug paraphernalia 152

Electronics 36

Erotica 296

Fireworks 5

Food 4



100 x Anadrol 50MG  
Oxymetholone (sealed )

\$12.41



1 gram MDMA

\$5.89



1/2g Cocaine

\$5.44



10 Pieces White Heart  
130-150mg MDMA Content

\$4.49



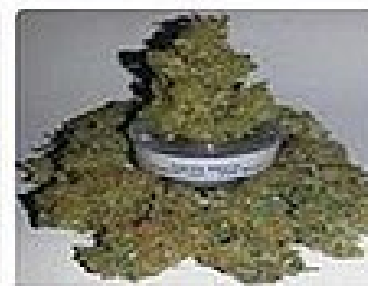
Red and White Filter (10  
packs x 20 cigarettes)

\$1.90



VEGA 100mg Sildenafil  
citrate 4 tablets

\$1.50



10 gram Santa Maria

\$11.58



1/4 oz G13

\$8.13



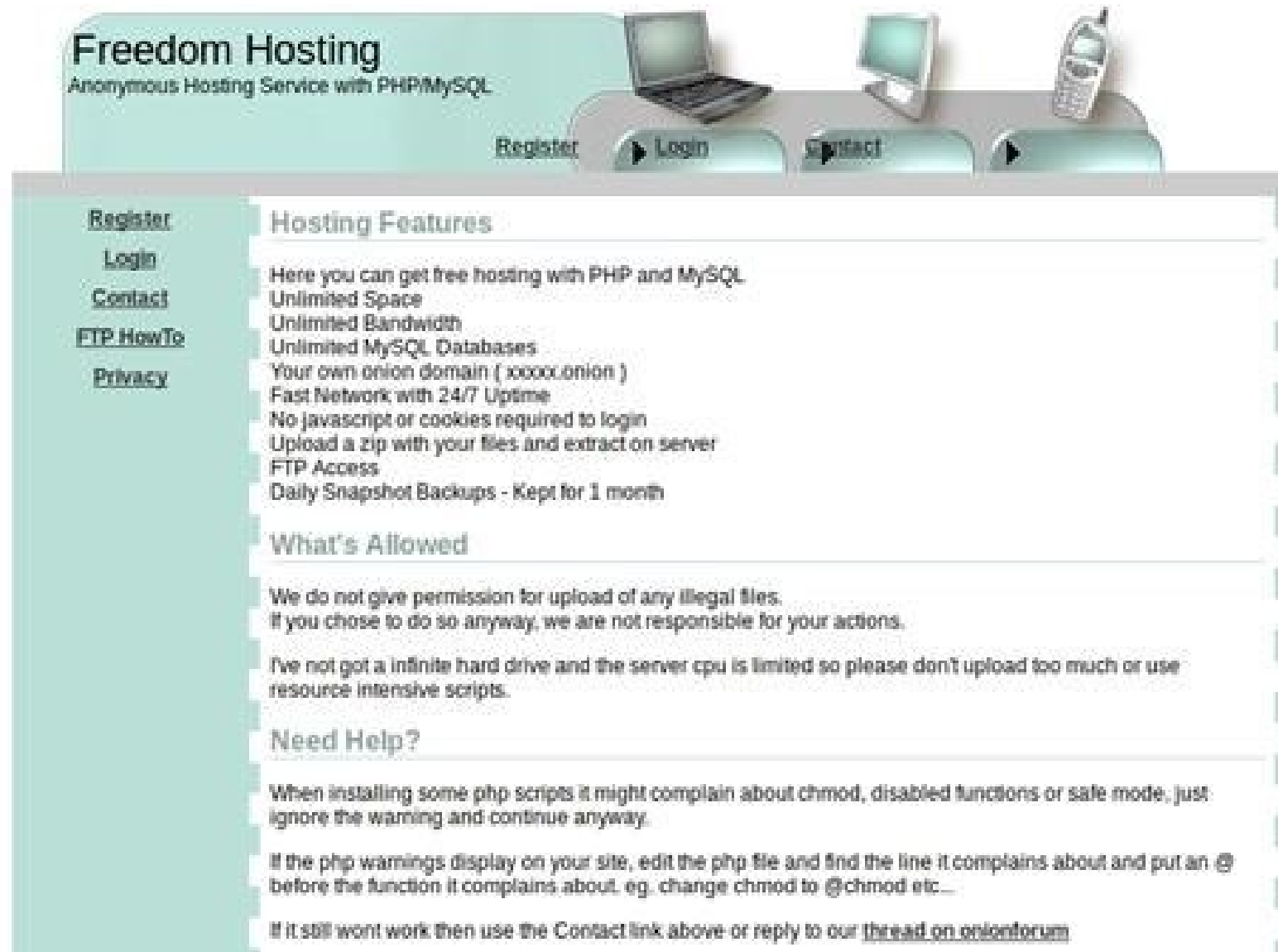
**THIS HIDDEN SITE HAS BEEN SEIZED**



# Ross William Ulbricht AKA Dread Pirate Roberts



# Freedom hosting



The screenshot shows the Freedom Hosting website. At the top, there's a header with the site name and a navigation bar with icons for a laptop, monitor, and phone. Below the header is a sidebar with links to Register, Login, Contact, FTP HowTo, and Privacy. The main content area is divided into sections: Hosting Features, What's Allowed, and Need Help?.

**Freedom Hosting**  
Anonymous Hosting Service with PHP/MySQL

Register Login Contact

[Register](#)  
[Login](#)  
[Contact](#)  
[FTP HowTo](#)  
[Privacy](#)

### Hosting Features

Here you can get free hosting with PHP and MySQL

- Unlimited Space
- Unlimited Bandwidth
- Unlimited MySQL Databases
- Your own onion domain ( xxxxx.onion )
- Fast Network with 24/7 Uptime
- No javascript or cookies required to login
- Upload a zip with your files and extract on server
- FTP Access
- Daily Snapshot Backups - Kept for 1 month

### What's Allowed

We do not give permission for upload of any illegal files.  
If you chose to do so anyway, we are not responsible for your actions.

I've not got a infinite hard drive and the server cpu is limited so please don't upload too much or use resource intensive scripts.

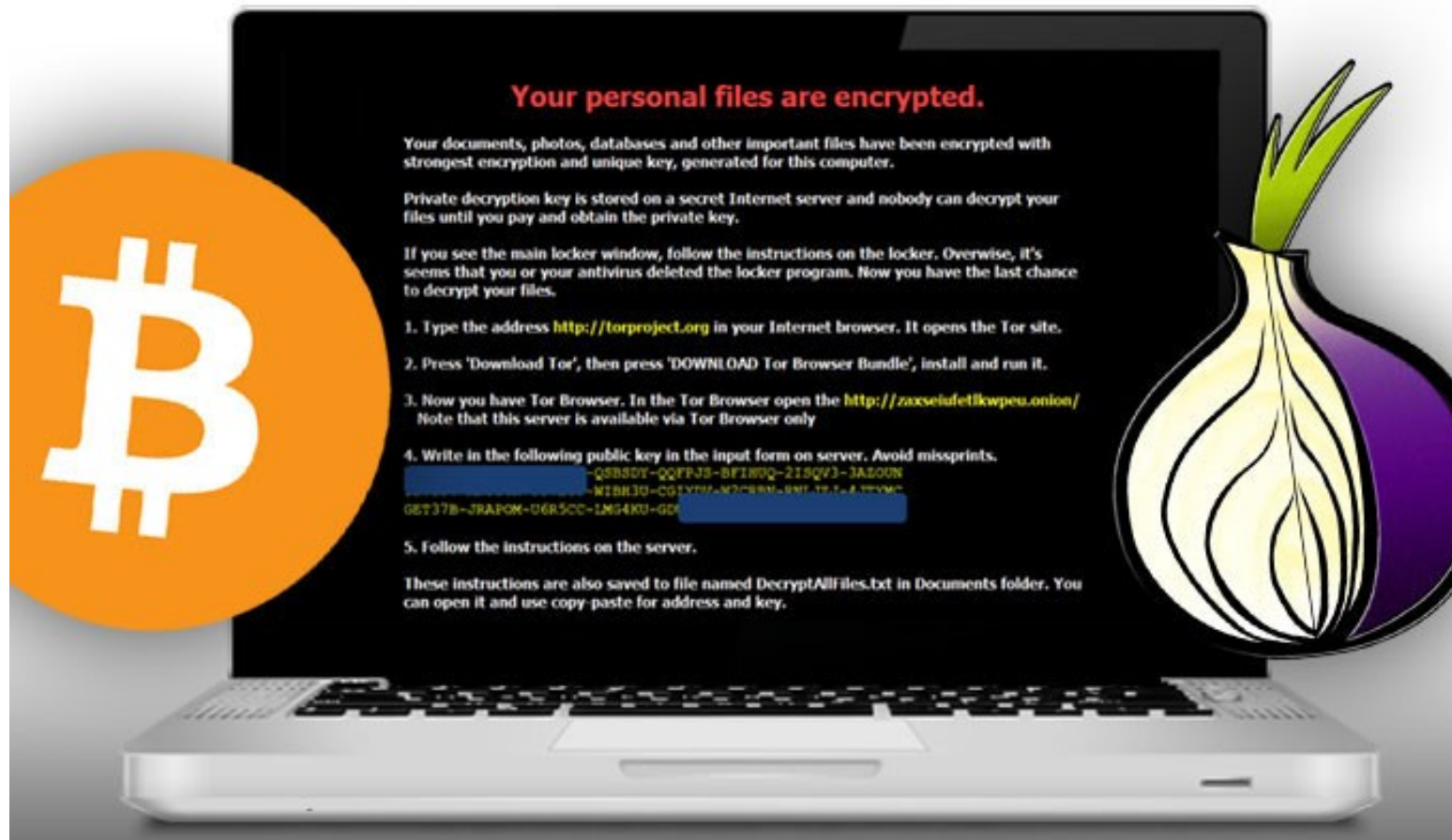
### Need Help?

When installing some php scripts it might complain about chmod, disabled functions or safe mode, just ignore the warning and continue anyway.

If the php warnings display on your site, edit the php file and find the line it complains about and put an @ before the function it complains about, eg. change chmod to @chmod etc...

If it still wont work then use the Contact link above or reply to our [thread on onionforum](#)

# Ransomware using Bitcoin, Tor and Tor2web :(



# Ahmia – search engine for Tor



**Tor Hidden Service (.onion) search**

AHMIA.FI

# Ahmia's history

2010

- I have been using Tor for years
- Didn't know much about hidden services
- Decided to crawl them and registered ahmia.fi
  - At first, a simple onion address directory
  - Basic PHP, HTML and JavaScript

# Ahmia's history

2012

- I started to operate exit nodes
- Got help from a few volunteers
- Site started to publish statistics



# Ahmia's history

2013

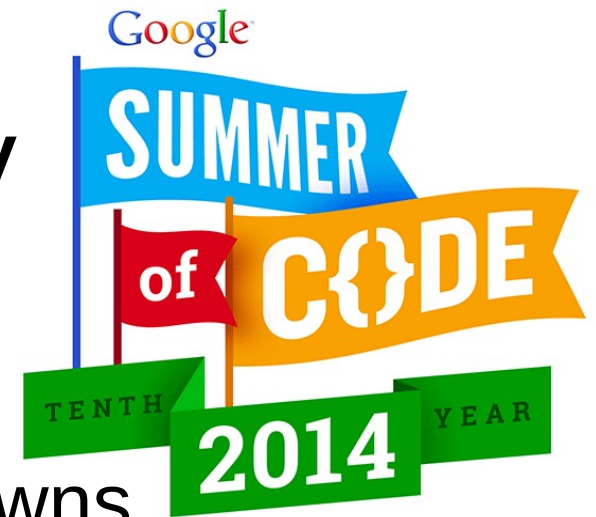
- I started to operate tor2web.fi
- Published full-text search engine based on YaCy P2P search engine software
- The back-end was real P2P software
- Exit nodes were shut down by the ISP
  - Fortunately, <http://tor.eff.org/>
  - Electronic Frontier Finland runs now exit nodes
  - I help Effi with this

# Ahmia's history

Attended to Observe. Hack. Make. 2013



# Ahmia's history



2014

- Tor2web.fi suffered multiple take downs
- Tor Project offered a place in the Google Summer of Code to develop Ahmia
- Ahmia got finally time, love and care
- <http://pinkmeth.com/> - caused troubles
- Tor Project's Summer 2014 Developers meeting that was hosted by Mozilla in Paris, France

# Ahmia

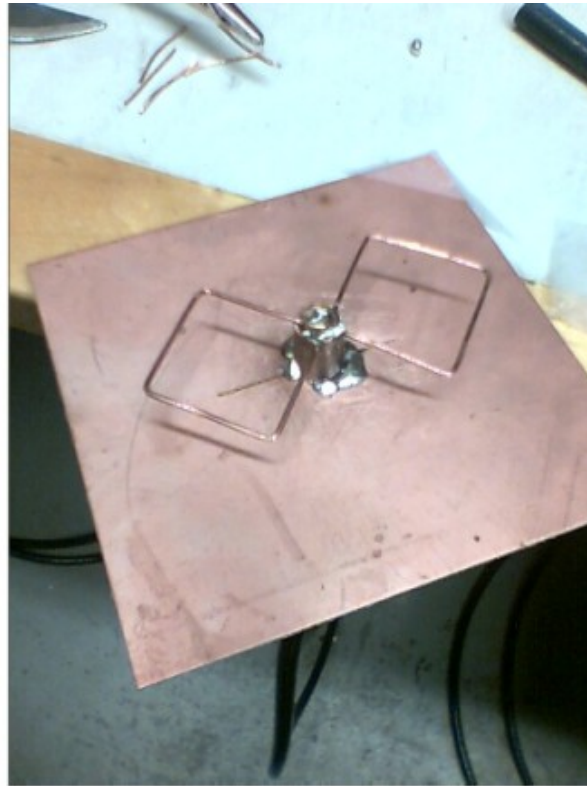
- <https://blog.torproject.org/blog/ahmia-search-after-gsoc-development>
- Full-text search
- YaCy software was replaced with own implementation called OnionBot
- Apache Solr database for crawler
- Django front-end
- OnionDir, filtering, statistics, integrations, APIs, visualizations...
- <https://github.com/juhanurmi/ahmia>

# Ahmia

- Search: <https://ahmia.fi/search/>
- OnionDir: <https://ahmia.fi/address/>
- Partners: <https://ahmia.fi/about/>
- Disclaimer: <https://ahmia.fi/disclaimer/>
- Indexing and crawling: <https://ahmia.fi/documentation/indexing/>
- Description.json: <https://ahmia.fi/documentation/descriptionProposal/>
- Popularity statistics: <https://ahmia.fi/stats/viewer>
- API and usage: <https://ahmia.fi/documentation/>

Feel free to hack with us! :-)





# Thank you all!

Please support [Tor](#)!

[juha.nurmi@ahmia.fi](mailto:juha.nurmi@ahmia.fi)