Anonymisierungsdienste

zum Schutz vor Tracking und Rückverfolgung

Dr. Dominik Herrmann

Universität Siegen

https://dhgo.to/slides-hasi

http://herdom.net

Rückverfolgung von Aktivitäten

Identitäten und Pseudonyme

Google hasi

All Videos Images News Maps More Search tools

About 17.000.000 results (0,83 seconds)

Hannon Armstrong Sustnbl Infrstr Cap Inc
NYSE: HASI - 16 Jun, 09:26 GMT-4

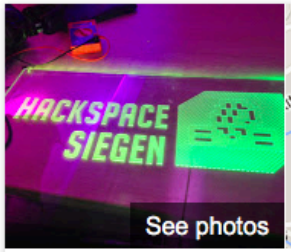
21,15 USD 0,00 (0,00 %)
Pre-market: 20,42 ▼0,73 (3,45 %)

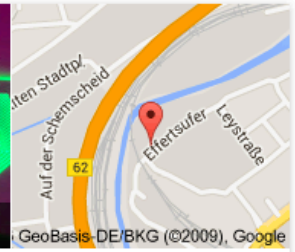
1 day 5 day 1 month 3 months 1 year 5 years max

After hours

21.5

Previous close





Hackspace Siegen

Website Directions

Google hasi Anmelden

Alle Bilder Videos News Maps Mehr Suchoptionen

Ungefähr 17.000.000 Ergebnisse (0,50 Sekunden)

Bilder zu hasi Unangemessene Bilder melden

Weitere Bilder zu hasi

HASI - Der Schmeckerbäcker
www.hasi-schmeckerbaecker.de/
So umschreibt Josef Reindl, Geschäftsführer des Familienunternehmens Hasi Schmeckerbäcker die Hasi-Philosophie, die wir seit Jahren mit unsererm ...
Filialen · Bewerbung · Aktuelles · Impressum

Source-IP-Adresse

```
80.187.103.981 - - [13/Jun/2016:22:20:05 +0200] "GET
/bytepix/data_1/images/logogross.jpg HTTP/1.1" 200 95485
"http://site.de/bytepix/start/fwl.php/user/login/start"
"Mozilla/5.0 (Linux; U; Android 4.4.2; de-de; GT-P5200
Build/KOT49H) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0
Safari/534.30"

80.187.103.981 - - [13/Jun/2016:22:20:18 +0200] "POST
/bytepix/start/fwl.php/user/login/post HTTP/1.1" 302 727
"http://site.de/bytepix/start/fwl.php/user/login/start"
"Mozilla/5.0 (Linux; U; Android 4.4.2; de-de; GT-P5200
Build/KOT49H) AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0
Safari/534.30"
```

Server-Side: IP Address Whois and IP Geocoding

Shows Your IP :

IP Address	141.99.199[redacted]
Host Name	
IP Address Loca	
Country	
State/Region	
City	
Organization	
ISP	
AS Number	
Timezone	
Local Time	
Latitude/Longit	
TCP/IP stack OS	
Passive, SYN	U: 1500 |

```
Abuse contact info: auftrag@nic.telekom.de

inetnum:          84.128.0.0 - 84.191.255.255
netname:          DE-TELEKOM-20040310
descr:            PROVIDER Local Registry
country:          DE
org:              ORG-DTA2-RIPE
admin-c:          DTAG-RIPE
tech-c:           DTAG-RIPE
status:           ALLOCATED PA
mnt-by:           RIPE-NCC-HM-MNT
mnt-by:           DTAG-NIC
mnt-lower:        DTAG-NIC
mnt-routes:       DTAG-RR
created:          2004-03-10T15:26:46Z
last-modified:    2016-06-01T06:46:56Z
source:           RIPE
```

WebRTC Leak Test :

Local IP Address	10.192.245.176	192.168.56.1	192.168.57.1
Public IP Address	141.99.199[redacted]	141.99.250[redacted]	

Tracking
im
Internet

THE WALL STREET JOURNAL.

WHAT THEY KNOW

Websites Vary Prices, Deals Based on Users' Information

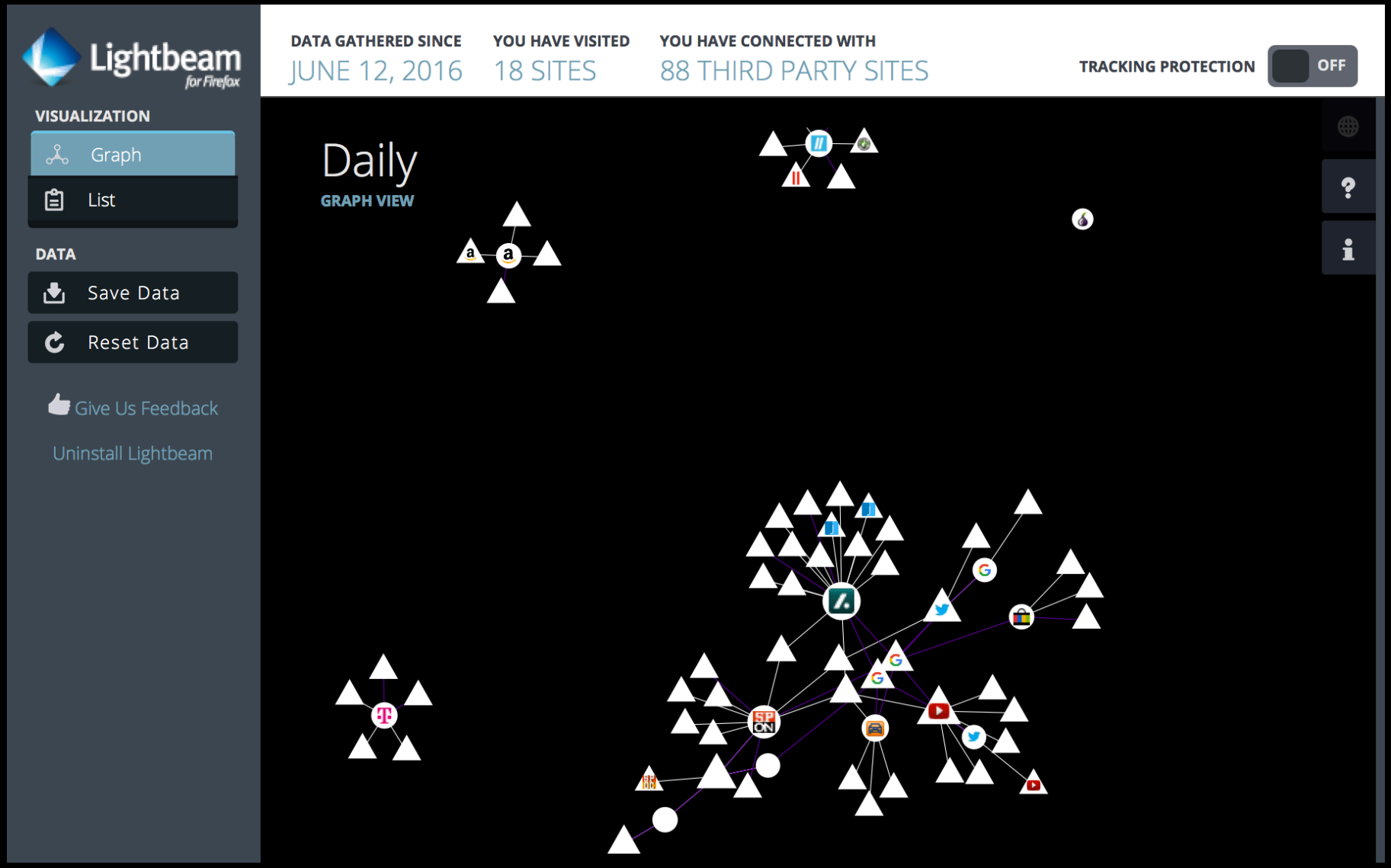
By JENNIFER VALENTINO-DEVRIES, JEREMY SINGER-VINE and ASHKAN SOLTANI

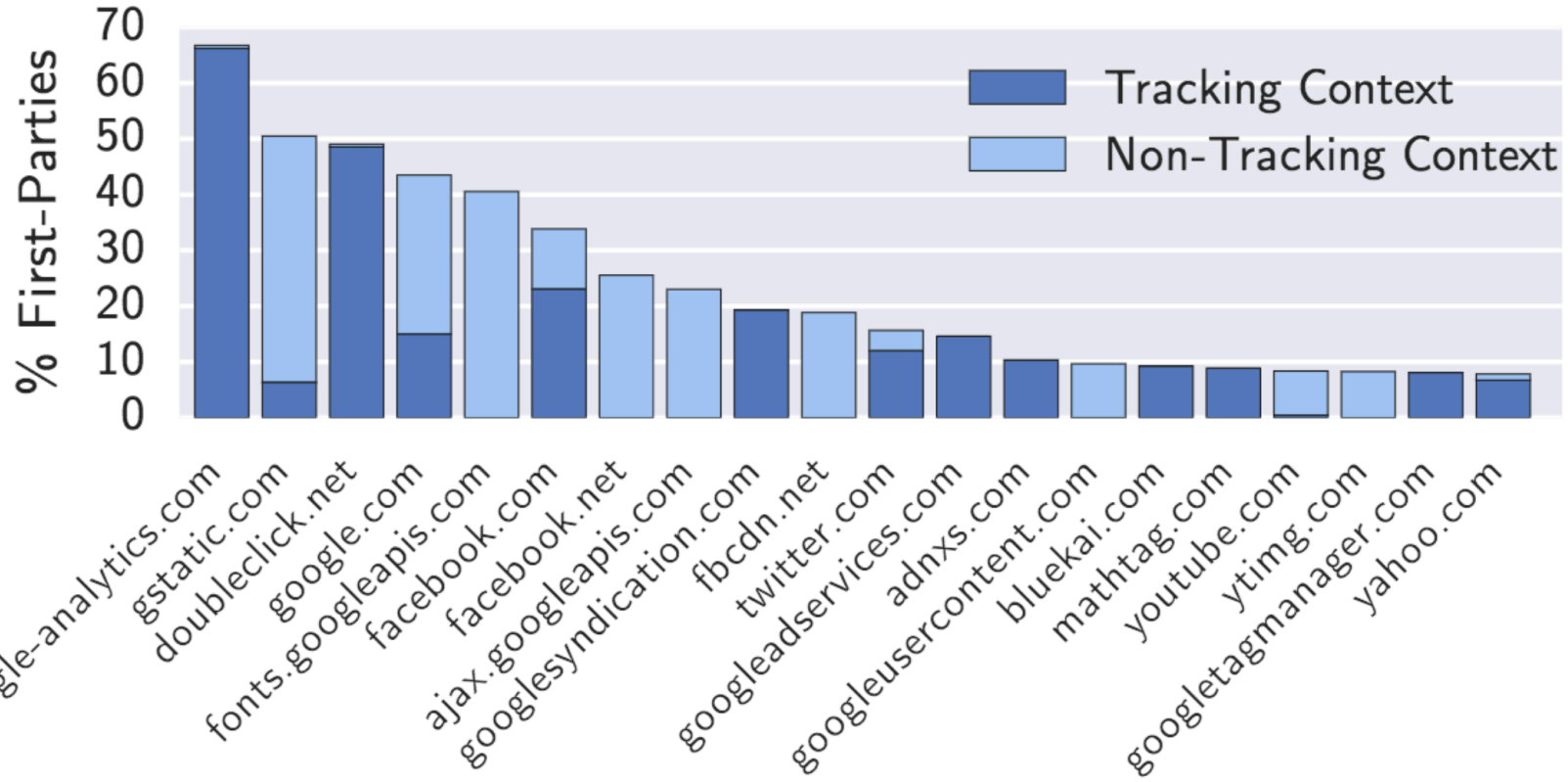
December 24, 2012

It was the same Swingline stapler, on the same Staples.com website. But for Kim Wamble, the price was $15.79, while the price on Trude Frizzell's screen, just a few miles away, was $14.29.

A key difference: where Staples seemed to think they were located.

Third-Party-Cookies


Lightbeam
for Firefox
VISUALIZATION
Graph
List
DATA
Save Data
Reset Data
Give Us Feedback
Uninstall Lightbeam
DATA GATHERED SINCE
JUNE 12, 2016
YOU HAVE VISITED
18 SITES
YOU HAVE CONNECTED WITH
88 THIRD PARTY SITES
TRACKING PROTECTION
OFF
Daily
GRAPH VIEW

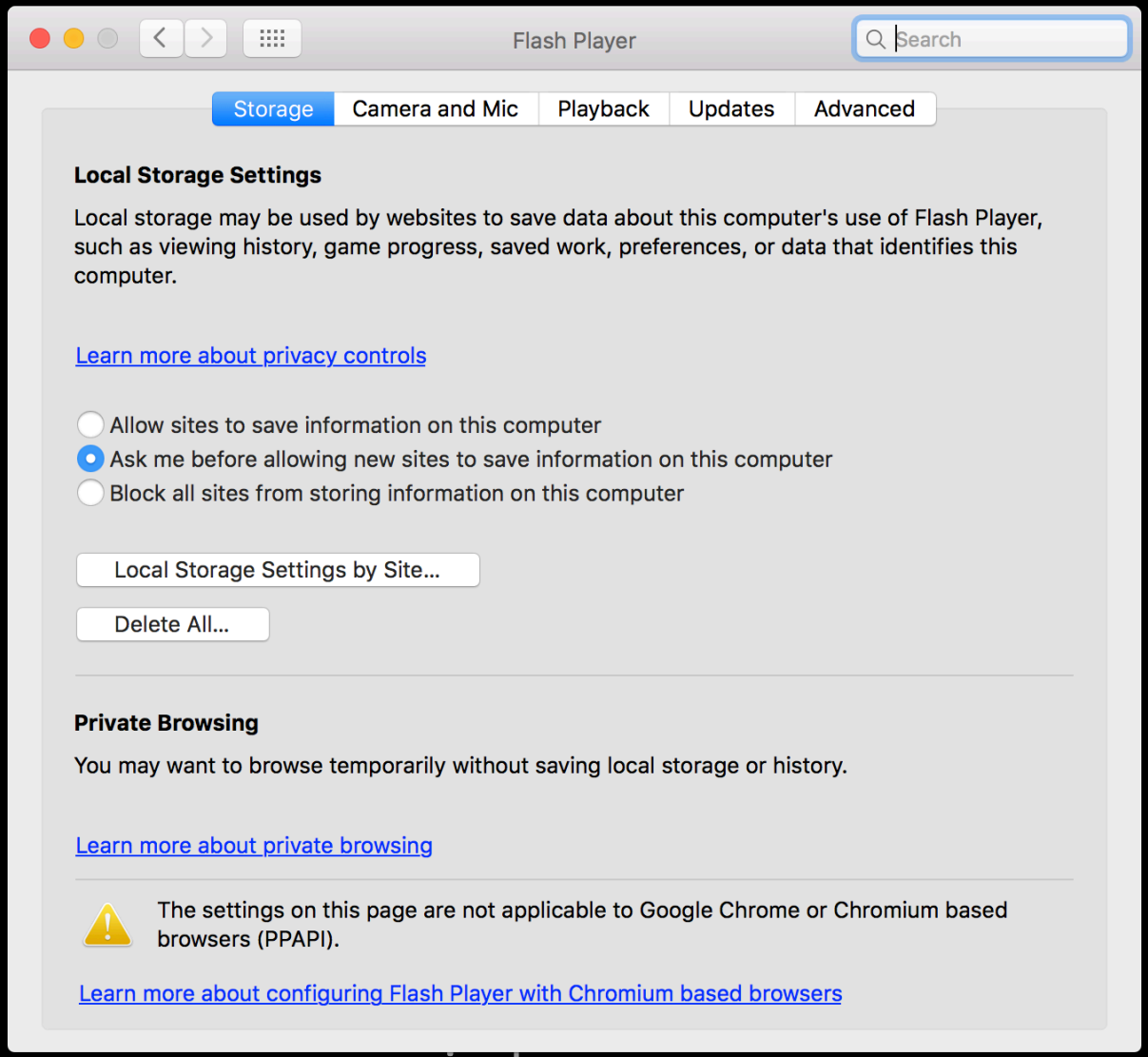


S. Englehardt & A. Narayanan (2016): Online tracking: A 1-million-site measurement and analysis, http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf

Super-Cookies

(Flash und Silverlight)
HTML 5 Storage

alte JavaScript-Features
window.name


Flash Player
Search
Storage
Camera and Mic
Playback
Updates
Advanced
Local Storage Settings
Local storage may be used by websites to save data about this computer's use of Flash Player, such as viewing history, game progress, saved work, preferences, or data that identifies this computer.
Learn more about privacy controls
Allow sites to save information on this computer
Ask me before allowing new sites to save information on this computer
Block all sites from storing information on this computer
Local Storage Settings by Site...
Delete All...
Private Browsing
You may want to browse temporarily without saving local storage or history.
Learn more about private browsing
The settings on this page are not applicable to Google Chrome or Chromium based browsers (PPAPI).
Learn more about configuring Flash Player with Chromium based browsers

window.name

evercookie accomplishes this by storing the cookie data in several types of storage mechanisms that are available on the local browser. Additionally, if evercookie has found the user has removed any of the types of cookies in question, it recreates them using each mechanism available.

Specifically, when creating a new cookie, it uses the following storage mechanisms when available:

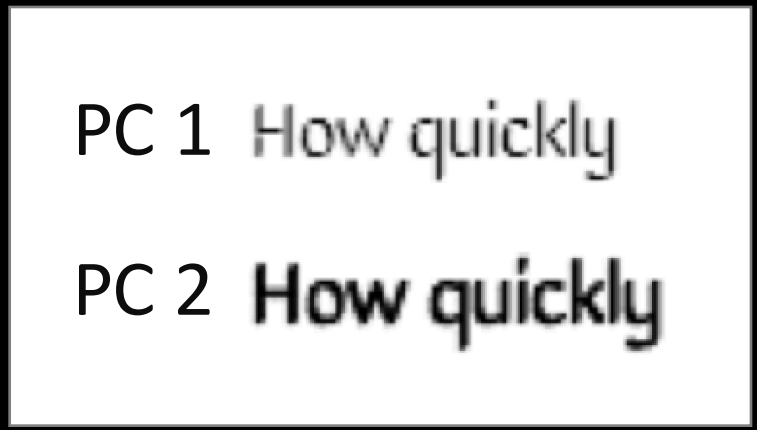
- **Standard HTTP Cookies**
- **HTTP Strict Transport Security (HSTS) Pinning**
- **Local Shared Objects (Flash Cookies)**
- **Silverlight Isolated Storage**
- **Storing cookies in RGB values of auto-generated, force-cached PNGs using HTML5 Canvas tag to read pixels (cookies) back out**
- **Storing cookies in Web History**
- **Storing cookies in HTTP ETags**
- **Storing cookies in Web cache**
- **window.name caching**
- **Internet Explorer userData storage**
- **HTML5 Session Storage**
- **HTML5 Local Storage**
- **HTML5 Global Storage**
- **HTML5 Database Storage via SQLite**
- **HTML5 IndexedDB**
- **Java JNLP PersistenceService**
- **Java CVE-2013-0422 exploit (applet sandbox escaping)**

Browser-Fingerprinting

Browser-Fingerprinting

HTML 5 Canvas

Fonts und Emojis



Fonts und Plugins

(a) Windows 7

(b) Windows 10

(c) Linux

(d) iOS

(e) Firefox OS

(f) Android 4.3 and before

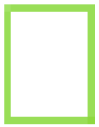
(g) Android 4.4

(h) Android 5.0

(i) Android on an LG device

(j) Android on a Samsung device

(k) Android on an HTC device



(l) Emoji not supported

Fig. 2. Comparison of the “Smiling face with open mouth" emoji on different devices and operating systems

Laperdrix et al. (2016): Beauty and the Beast: Diverting modern web browsers to build unique browser fingerprints, https://hal.inria.fr/hal-01285470/file/beauty-sp16.pdf

Browser-Fingerprinting

neue JavaScript-Features
Battery API
WebGL

The leaking battery

A privacy analysis of the HTML5 Battery Status API

Łukasz Olejnik[1], Gunes Acar[2], Claude Castelluccia[1], and Claudia Diaz[2]

[1] INRIA Privatics, Grenoble, France
{lukasz.olejnik,claude.castelluccia}@inria.fr
[2] KU Leuven, ESAT/COSIC and iMinds, Leuven, Belgium
{gunes.acar,claudia.diaz}@esat.kuleuven.be

neue JavaScript-Features
WebGL
Battery API

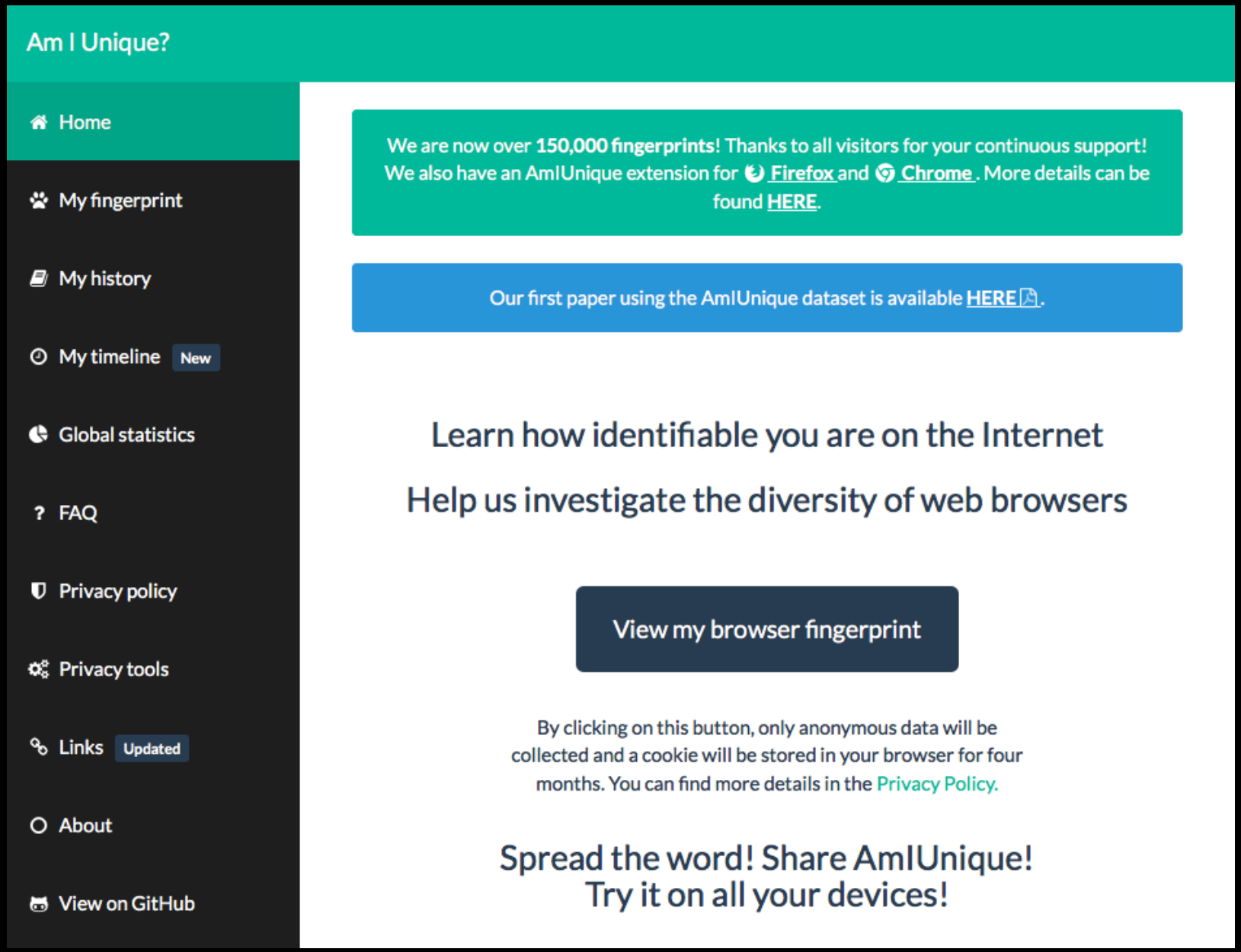
http://eprint.iacr.org/2015/616.pdf

VIRTUAL ART SESSIONS

https://www.chromeexperiments.com/webgl?page=0

Browser-Fingerprinting

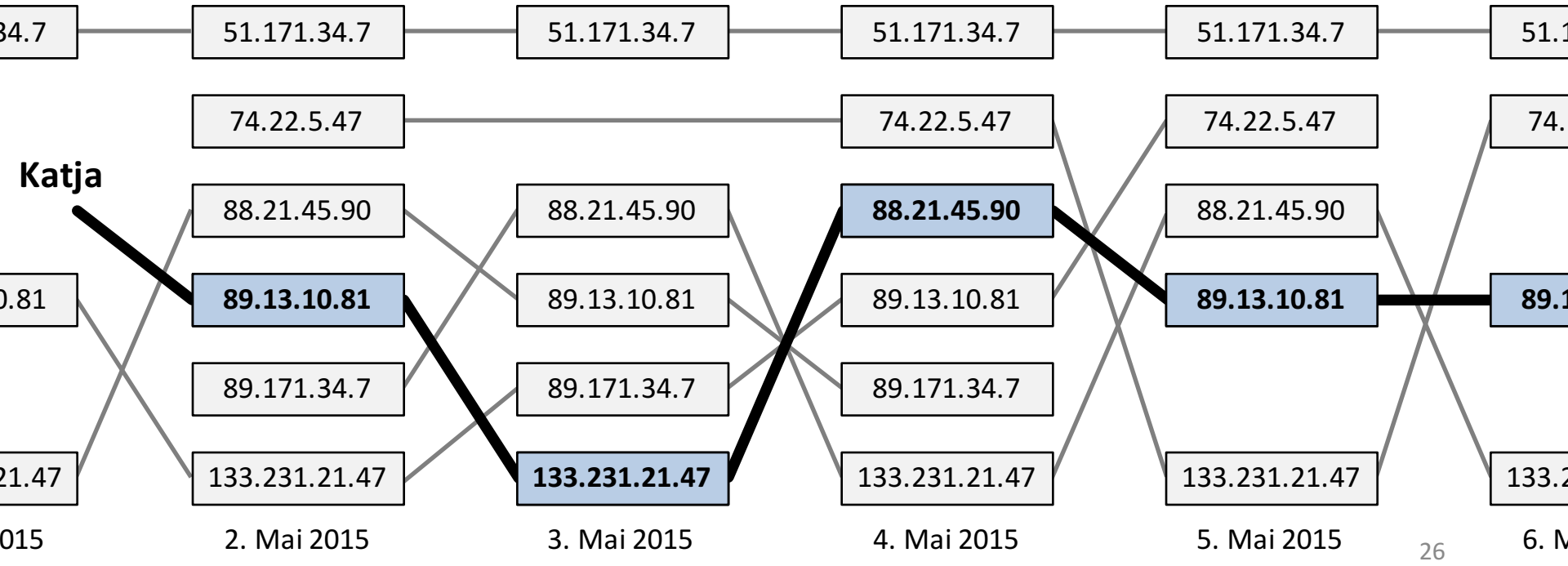

A RESEARCH PROJECT OF THE ELECTRONIC FRONTIER FOUNDATION
DONATE
PANOPTICLICK
Is your browser safe against tracking?
When you visit a website, online trackers and the site itself may be able to identify you – even if you've installed software to protect yourself. It's possible to configure your browser to thwart tracking, but many people don't know how.
Panopticlick will analyze how well your browser and add-ons protect you against online tracking techniques. We'll also see if your system is uniquely configured—and thus identifiable—even if you are using privacy-protective software.
TEST ME
Only anonymous data will be collected through this site.
Panopticlick is a research project of the Electronic Frontier Foundation. Learn more


Am I Unique?
Home
My fingerprint
My history
My timeline
New
Global statistics
FAQ
Privacy policy
Privacy tools
Links
Updated
About
View on GitHub
We are now over 150,000 fingerprints! Thanks to all visitors for your continuous support! We also have an AmIUnique extension for Firefox and Chrome. More details can be found HERE.
Our first paper using the AmIUnique dataset is available HERE.
Learn how identifiable you are on the Internet
Help us investigate the diversity of web browsers
View my browser fingerprint
By clicking on this button, only anonymous data will be collected and a cookie will be stored in your browser for four months. You can find more details in the Privacy Policy.
Spread the word! Share AmIUnique!
Try it on all your devices!

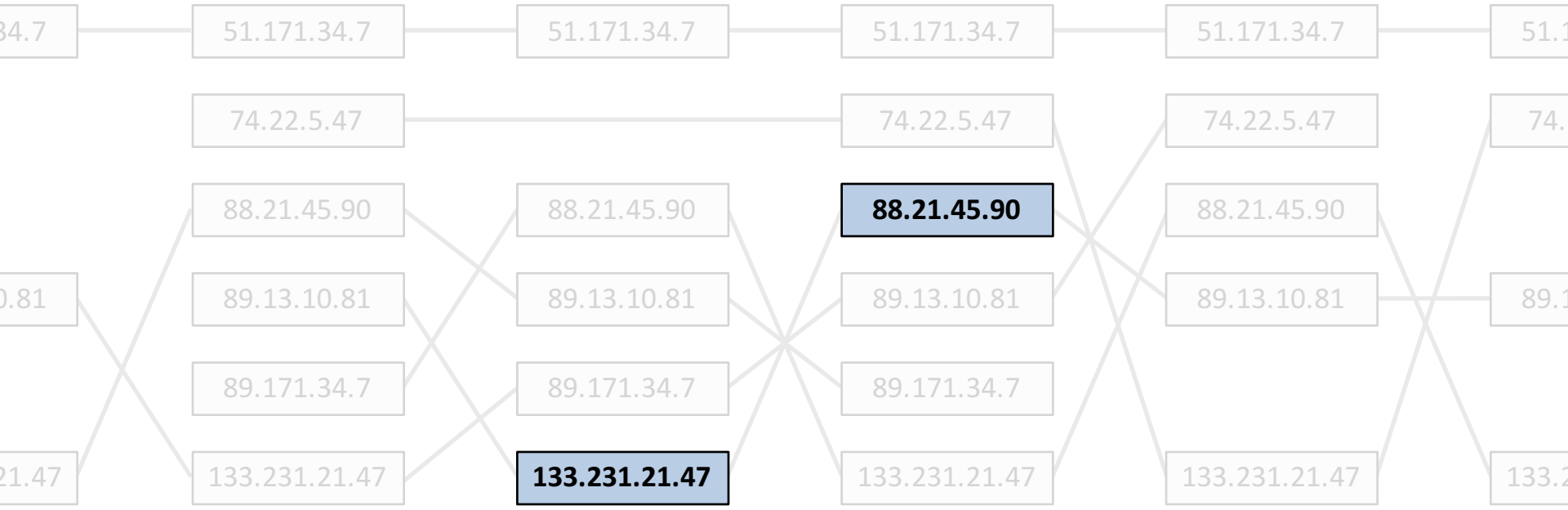

BrowserLeaks.com
Tweet
Web Browser Security — BrowserLeaks.com
Since the ancient times it is considered that the IP Address and the HTTP Cookies is the only reliable digital fingerprints which affects the online privacy and web browser identity. After a while, the privacy invaders began to looking for the ways to increase the user-tracking reliability to identify users from the general flow, they started to collect more and more additional user sensitive information.
Today the situation is more disappointing. Modern web browsers has not been architected to assure personal web privacy. Developers of major anonymity networks like TOR have no choice to edit the source code of a web browsers to somehow smooth over the situation, but this is sometimes not enough.
BrowserLeaks.com — It's all about Web Browser Fingerprinting. Here you will find the gallery of web browser security testing tools, that tell you what exactly personal identity data may be leaked without any permissions when you surf the Internet.
IP Address
Main tool that illustrates server-side abilities to expose the user identity. It contains a basic features, such as Showing Your IP Address and HTTP Request Headers. As well as Proxy Detection in all possible XFF headers. GeoIP Data Acquisition about the general IP Address and all of a Proxy IP's (Country, State, City, ISP/ASN, Local Time, Latitude/Longitude), and put all IP places to the Google Maps. In addition, here is a special features — Passive TCP/IP stack OS Fingerprinting, DNS and WebRTC Leak Tests.
JavaScript
A lot of user data can be obtained using common JavaScript functionality. DOM Window Object disclose much of sensitive information about the web browser: User-Agent, Architecture, OS Language, System Time, Screen Resolution. There is a listing of the NPAPI Plug-ins and Windows Explorer Components. Also there is already implemented: detection and obtaining data through a brand new HTML5 API's, such as the Battery Status API and Navigation Timing API.
Flash Player
Describes the Flash Player Runtime properties that can be provided through the use of AS3 System Capabilities: Flash Version, Plugin Type, Operating System, Manufacturer, System Language, Web Browser
Silverlight
Getting system information using Silverlight Plug-In, installed in your web browser. Shows your system environment details such as: OS Version, Processor Count, System Uptime, Time Zone, Installed Fonts, System and

Herausforderung für Werbenetze
Wiedererkennung von Nutzern trotz (meist täglich) wechselnder IP-Adressen

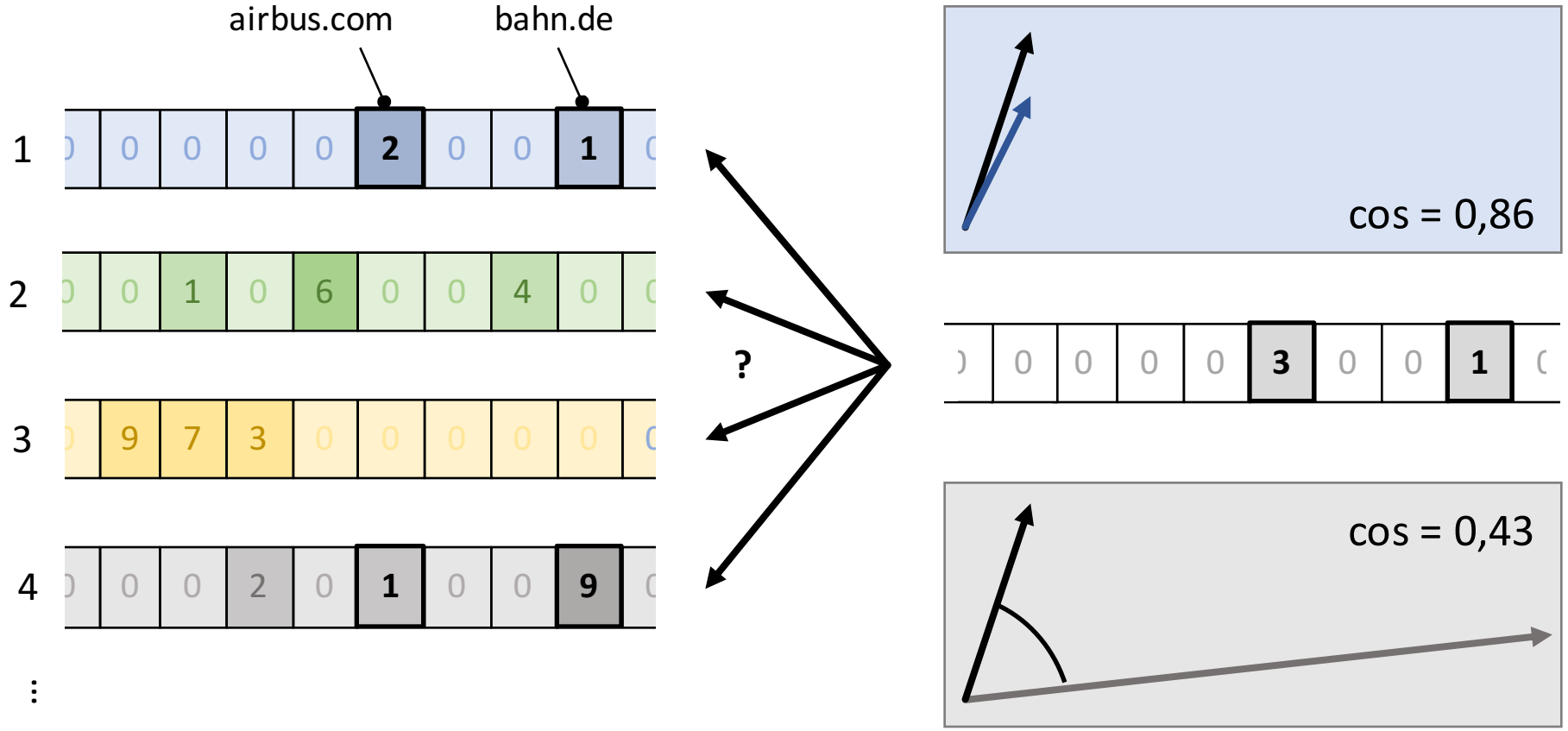
Bedrohung
verhaltensbasierte Wiedererkennung



3. Mai				4. Mai
spiegel.de	4 x	**Hypothese**	1 x	spiegel.de
google.de	15 x	Surfverhalten vieler Nutzer weist wiederkehrende und charakteristische Muster auf	9 x	google.de
apple.com	1 x		0 x	apple.com
siegen.de	**3 x**		**6 x**	**siegen.de**
airbus.com	**2 x**		**3 x**	**airbus.com**



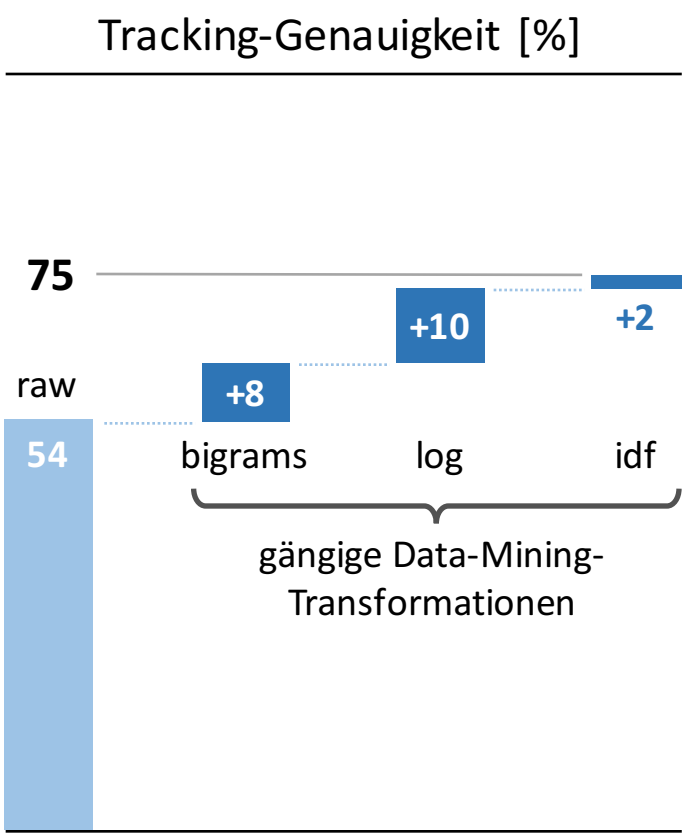
Tracking-Verfahren: Sessions werden als Vektoren modelliert und anhand ihrer Kosinus-Ähnlichkeit miteinander verglichen (1-Nächster-Nachbarn-Klassifikator).

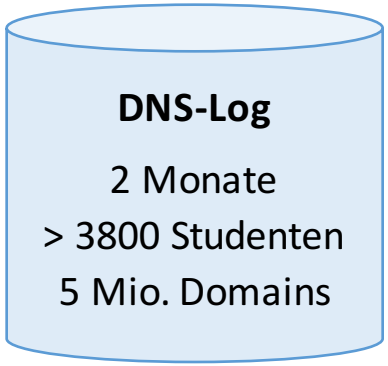


Genauigkeit des verhaltens-basierten Trackings?

Experimentelle Überprüfung

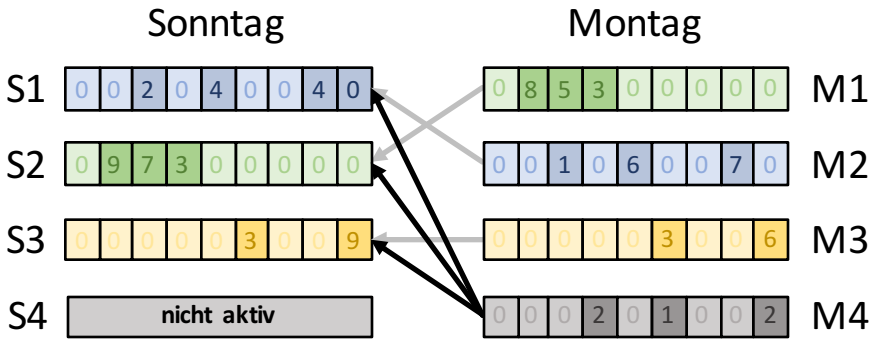
1. verdeckt DNS-Anfragen beobachten
2. Tracking simulieren (24h-Sitzungen)
3. Genauigkeit u. Robustheit bestimmen



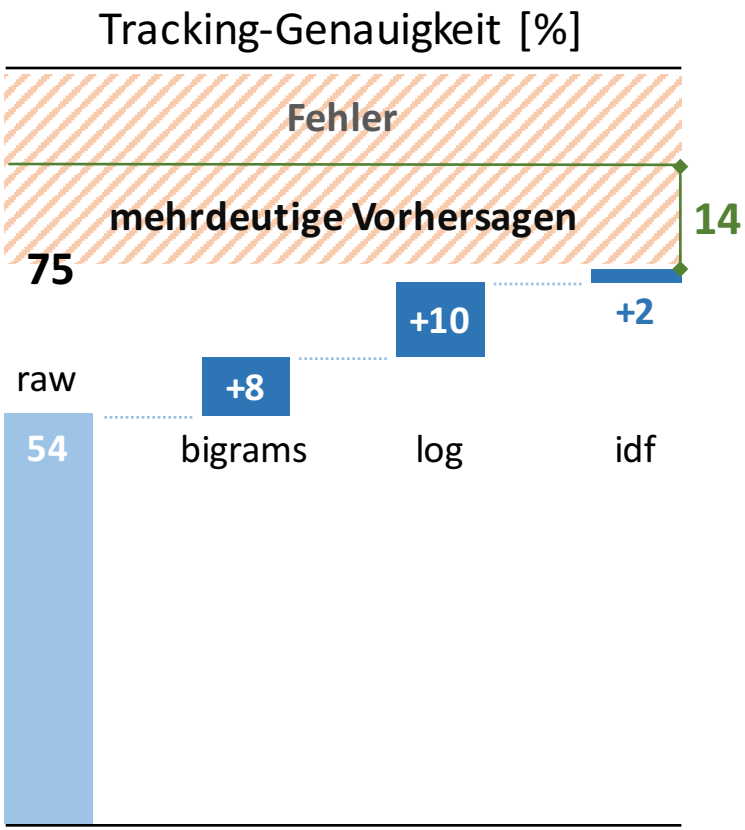


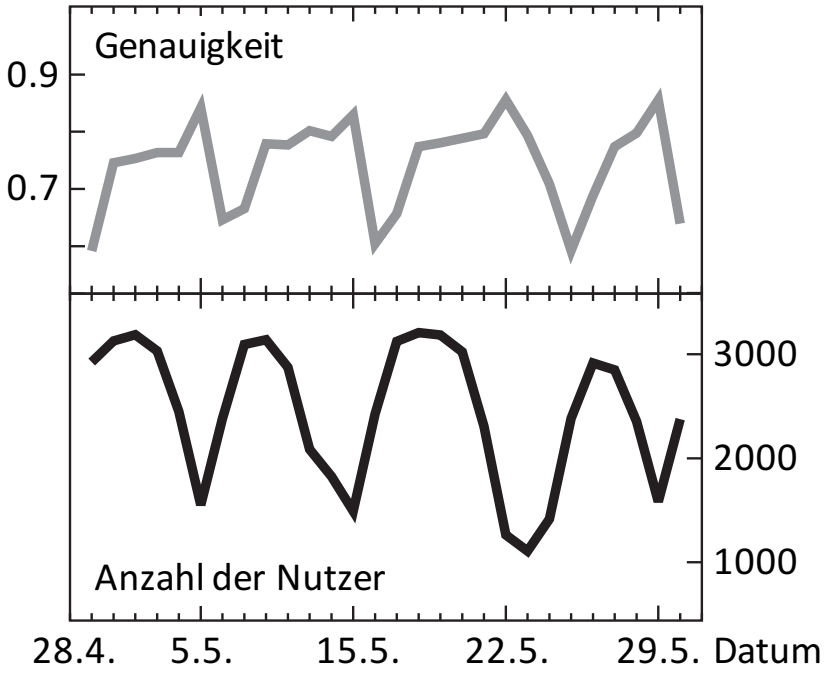
mit »ground truth«
(pseudonymisiert)

Genauigkeit des verhaltens-basierten Trackings?

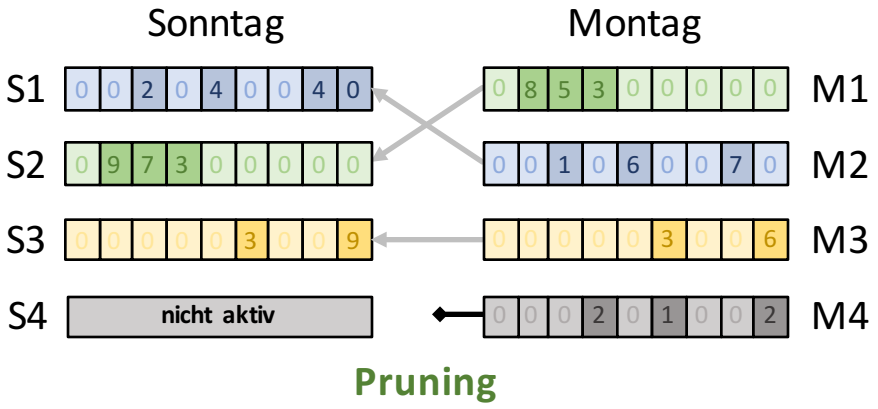


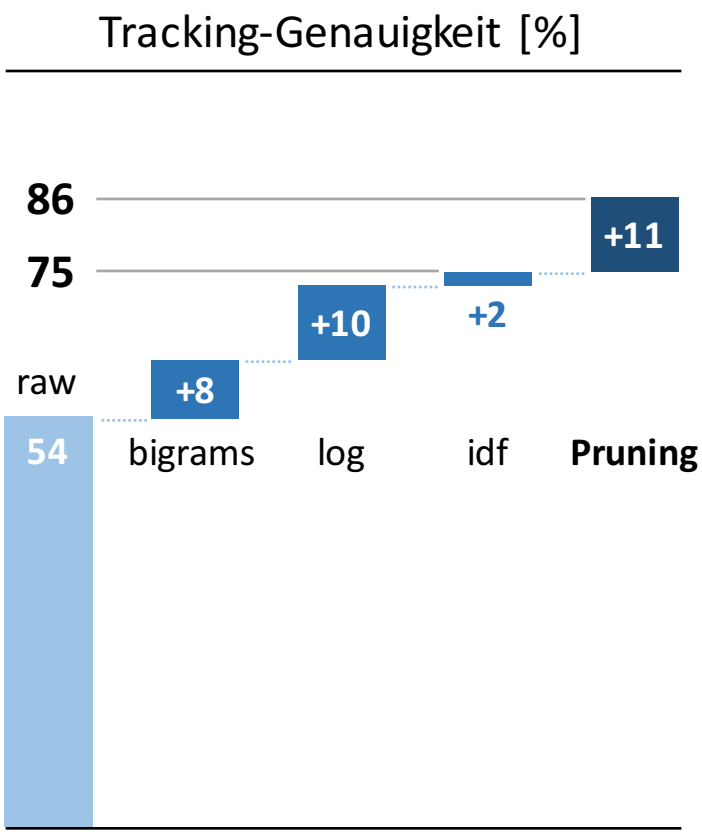
mehrdeutige Vorhersagen können aufgelöst werden

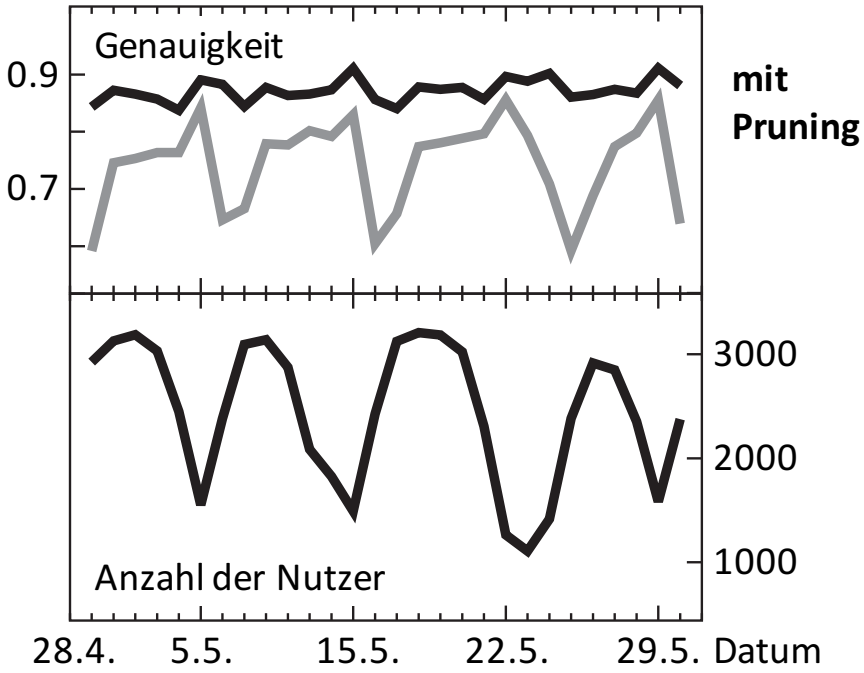




Genauigkeit des verhaltens-basierten Trackings?

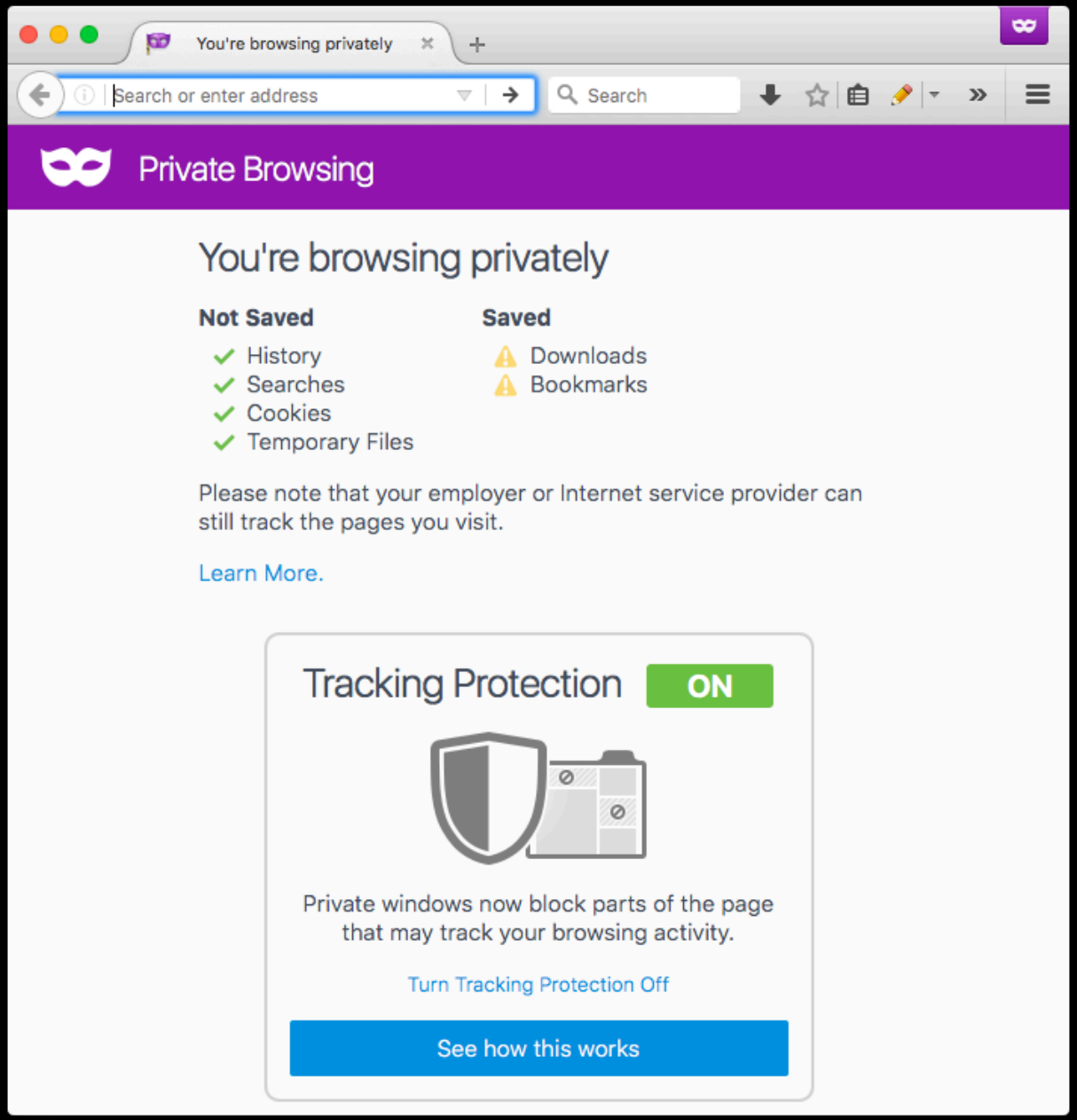






Möglichkeiten
zur
anonymen Internetnutzung

Private Browsing Mode


You're browsing privately
Search or enter address
Search
Private Browsing
You're browsing privately
Not Saved
History
Searches
Cookies
Temporary Files
Saved
Downloads
Bookmarks
Please note that your employer or Internet service provider can still track the pages you visit.
Learn More.
Tracking Protection
ON
Private windows now block parts of the page that may track your browsing activity.
Turn Tracking Protection Off
See how this works

Private Browsing Mode

Schutz vor Mitbenutzern
kein Schutz vor ISP
kein ausreichender Tracking-Schutz

Proxies & Virtual Private Networks


Verteilen
G+1
276
Port: Alle
Gateway: Alle
Anonymität: Alle
Reaktionszeit: Alle
Land: Alle
Verfügbarkeit: Alle
Listenstil:
Details
Copy&Paste
Anzahl: 50
Proxytyp:
HTTP
HTTPS
HTTP + HTTPS
Socks 4
Socks 5
Anzeigen
Zurücksetzen
letzte Seite
nächste Seite
Diese Suche als Favorit speichern
IP Port Gateway Level Zeit Land Online Check
203.88.170.183 8080 Nein 1 30.66 Sek. 78% 15:58
222.122.9.46 80 Nein 1 2.27 Sek. 99% 15:58
61.153.198.178 3128 Nein 3 10.39 Sek. 87% 15:58
103.15.62.69 8080 Nein 3 11.27 Sek. 54% 15:58


ZenMate
PRODUCTS
PREMIUM
ACADEMY
BUSINESS
LOG IN
SIGN UP
English (United States)
Enjoy Security Now
The easiest way to stay secure and private online while accessing the content you love
START FREE PREMIUM TRIAL
or
GET PREMIUM SECURITY NOW

IPREDATOR

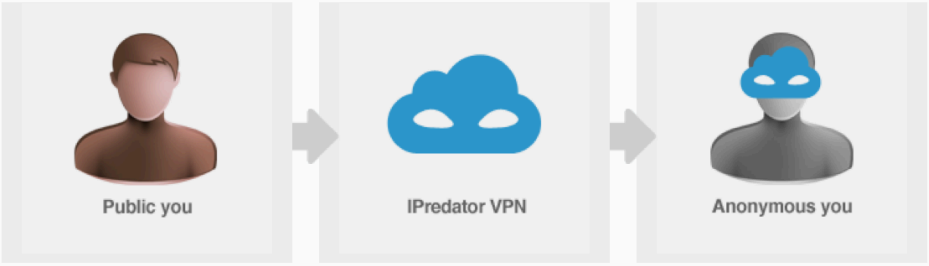
FAQ Guides Help me! Sign in

Big Brother is watching YOU ... we are not

Sign up, get a 3 day trial for free

You can choose a prepaid plan ranging from 1 to 12 months. A list of payment options and prices is available on the payment page.

„ I have been using it for couple of years now. Never had any problems. Rock Solid!"



How it works

IPredator provides you with an encrypted tunnel from your computer to the Internet. We are hiding your real IP address behind one of ours.

Proxies & Virtual Private Networks

Proxies: kein Schutz vor ISP & Proxy

VPN: kein Schutz vor VPN

kein akzeptabler Tracking-Schutz

Proxies & Virtual Private Networks

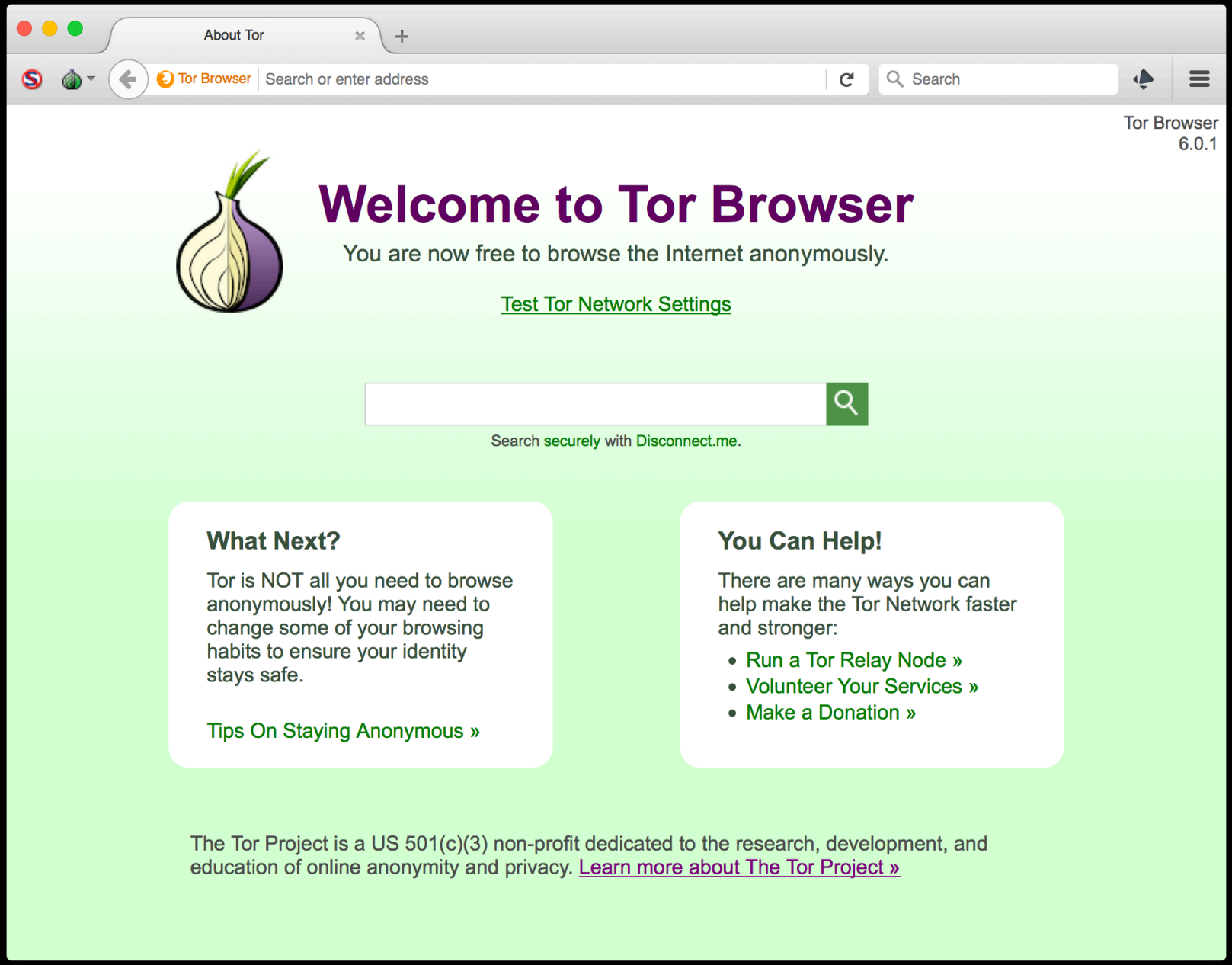
Proxies: kein Schutz vor ISP und Anbieter

VPN: kein Schutz vor Anbieter

Tor

Schutz vor ISP

Tracking-Protection


About Tor
Tor Browser
Search or enter address
Search
Tor Browser
6.0.1
Welcome to Tor Browser
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Search securely with Disconnect.me.
What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.
Tips On Staying Anonymous »
You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
Run a Tor Relay Node »
Volunteer Your Services »
Make a Donation »
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

To continue, please type the characters below:

calebr Submit

About this page

Our systems have detected unusual traffic from your computer network. This page checks to see if it's really you sending the requests, and not a robot. Why did this happen?

IP address: 163.172.136.101
Time: 2016-06-16T13:24:22Z
URL: https://www.google.de/search?sclient=psy-ab&site=&source=hp&btnG=Suche&q=hasi

At this security level, the following changes apply (mouseover for details):

HTML5 video and audio media become click-to-play via NoScript.

All JavaScript performance optimizations are disabled. Scripts on some sites may run slower.

Remote JAR files are blocked.

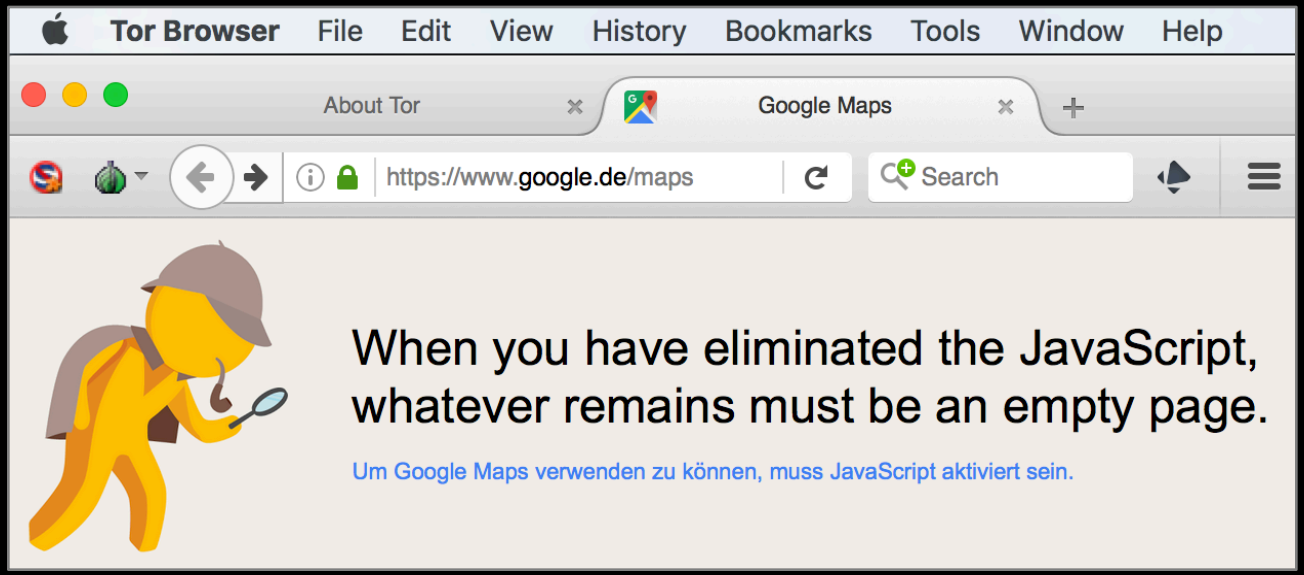
Some mechanisms of displaying math equations are disabled.

Some font rendering features are disabled.

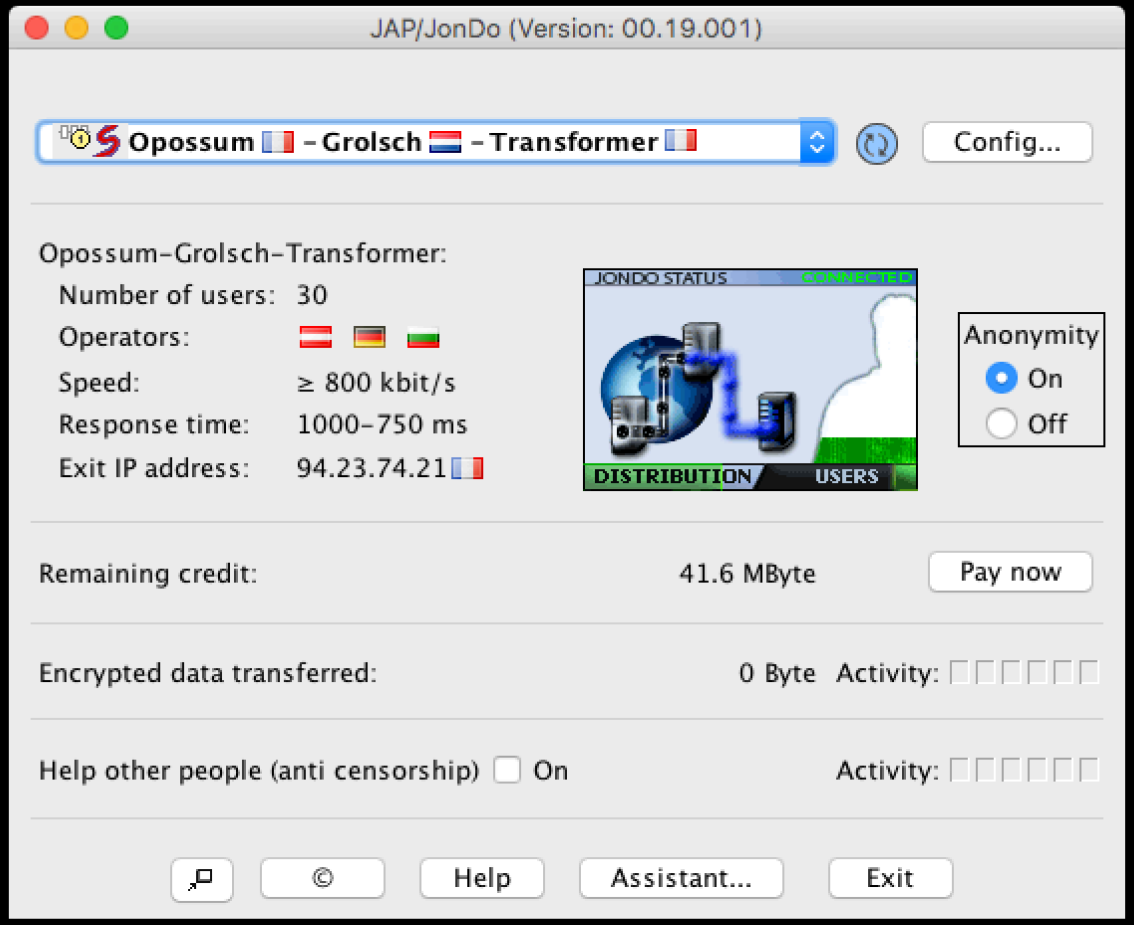
JavaScript is disabled by default on all sites.

Some types of images are disabled.

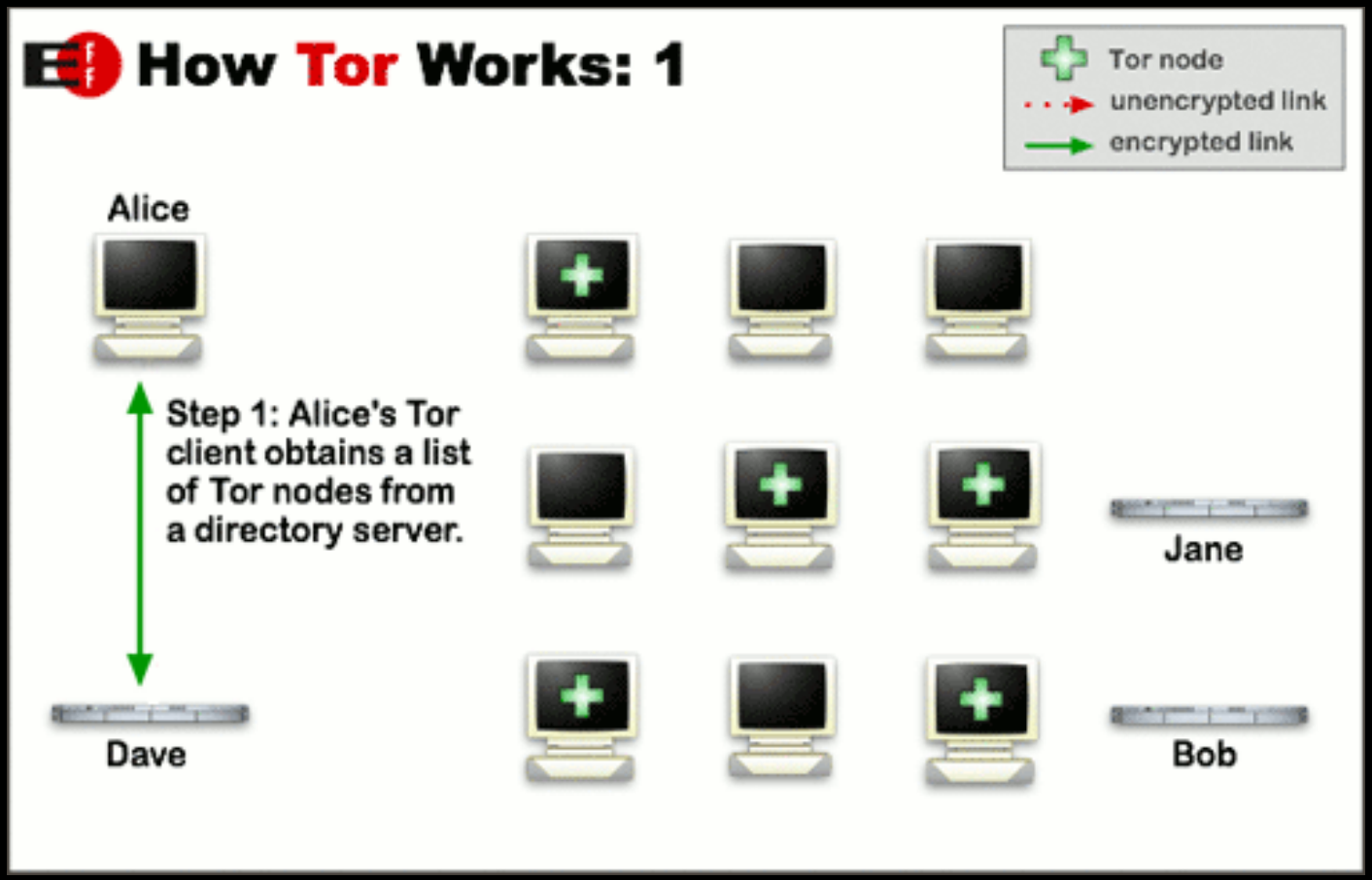
Some fonts and icons may display incorrectly.



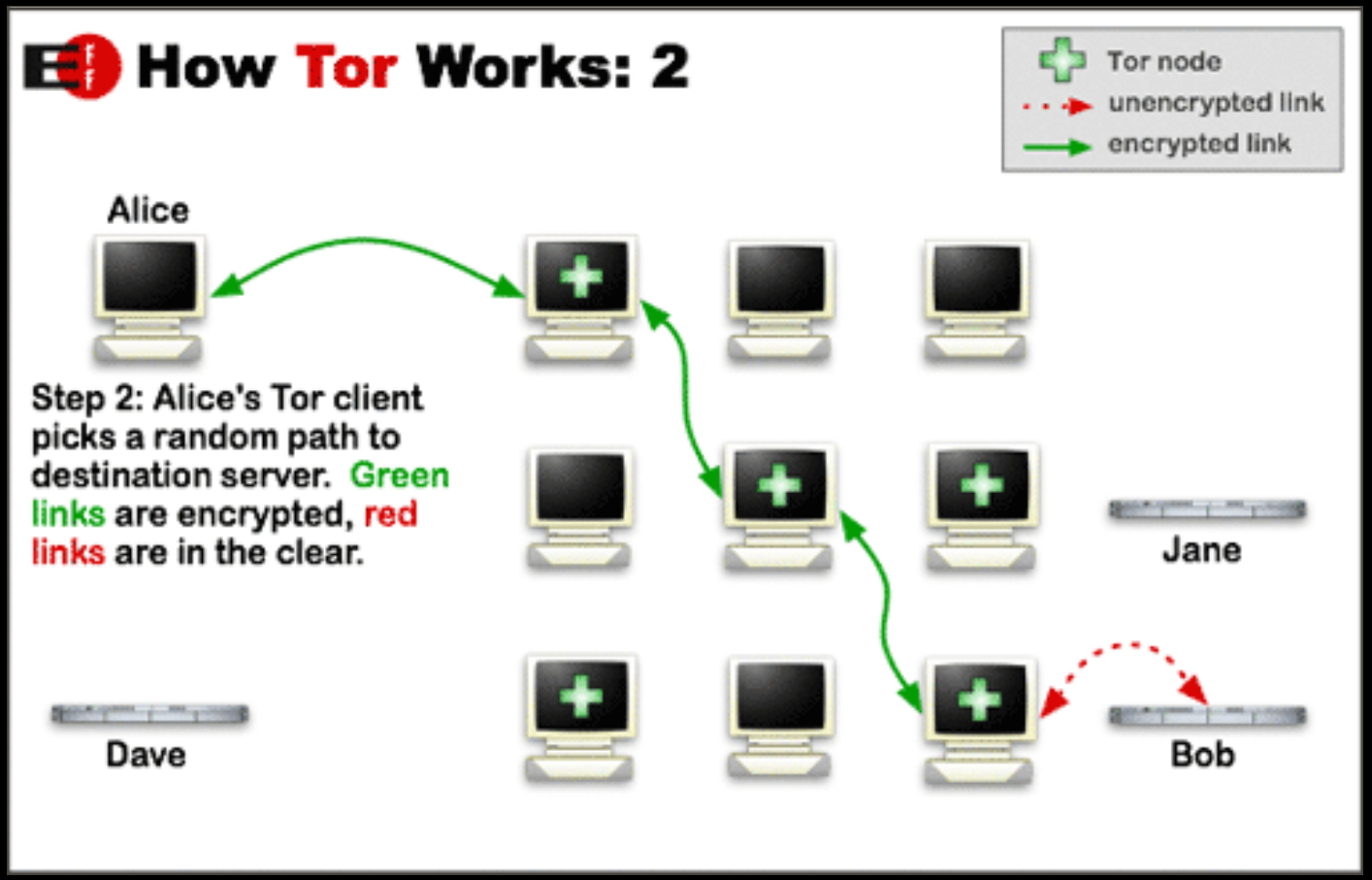
JonDonym


JAP/JonDo (Version: 00.19.001)
Opossum - Grolsch - Transformer
Config...
Opossum-Grolsch-Transformer:
Number of users: 30
Operators:
Speed: ≥ 800 kbit/s
Response time: 1000-750 ms
Exit IP address: 94.23.74.21
JONDO STATUS
CONNECTED
DISTRIBUTION
USERS
Anonymity
On
Off
Remaining credit:
41.6 MByte
Pay now
Encrypted data transferred:
0 Byte
Activity:
Help other people (anti censorship)
On
Activity:
©
Help
Assistant...
Exit

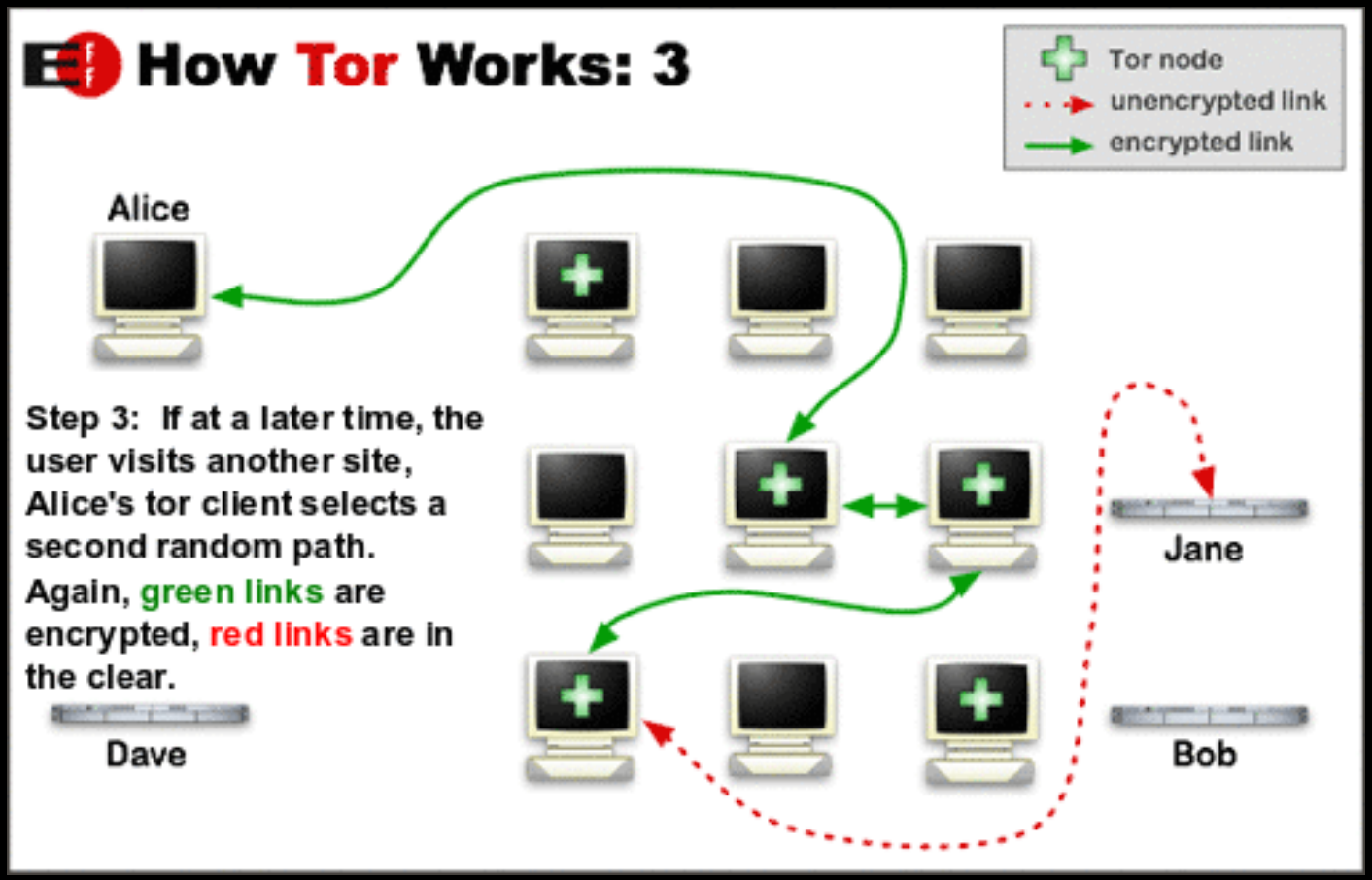
Funktionsweise von Tor



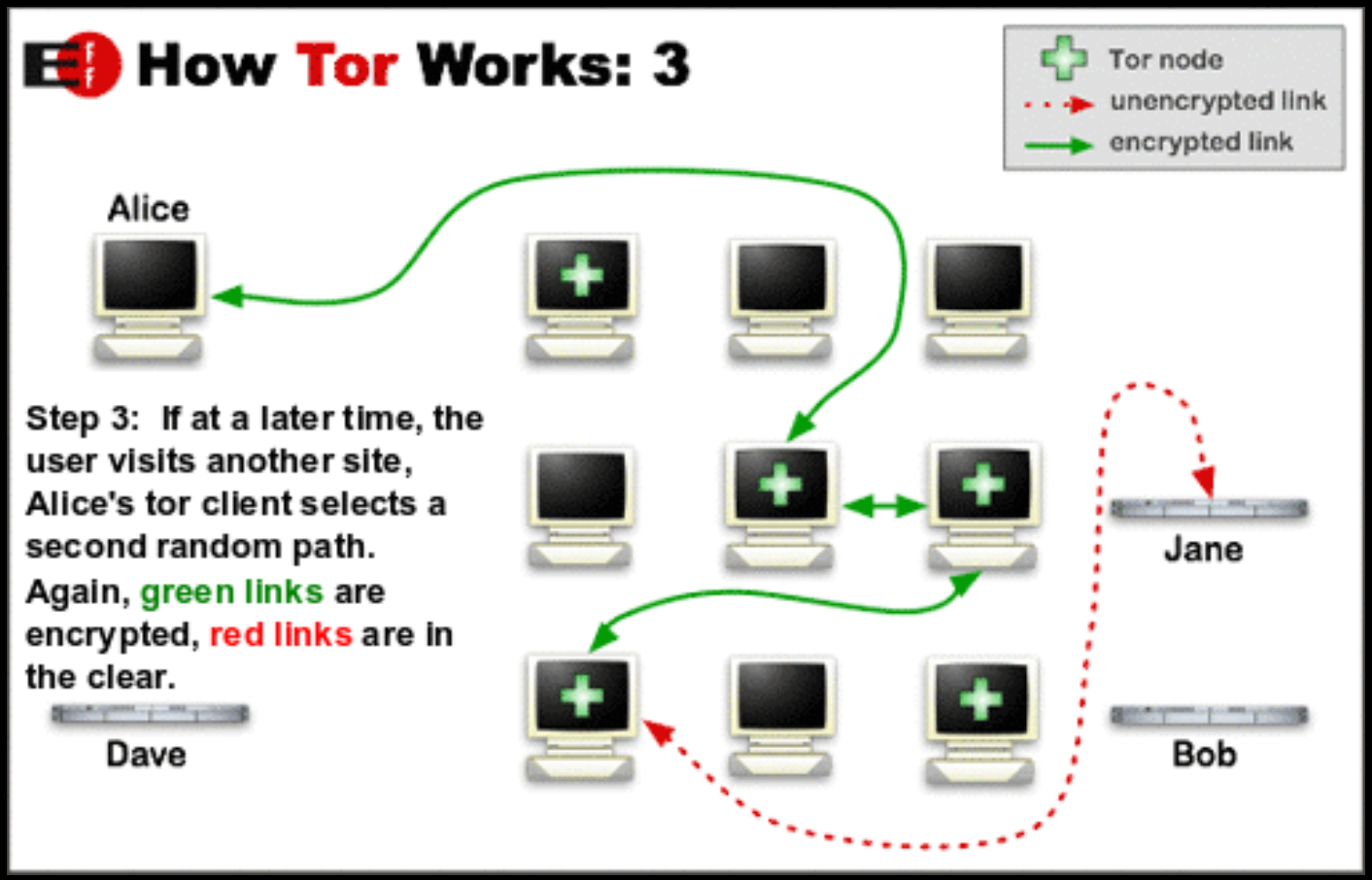
https://www.torproject.org/about/overview.html.en



https://www.torproject.org/about/overview.html.en



•https://www.torproject.org/about/overview.html.en



•https://www.torproject.org/about/overview.html.en

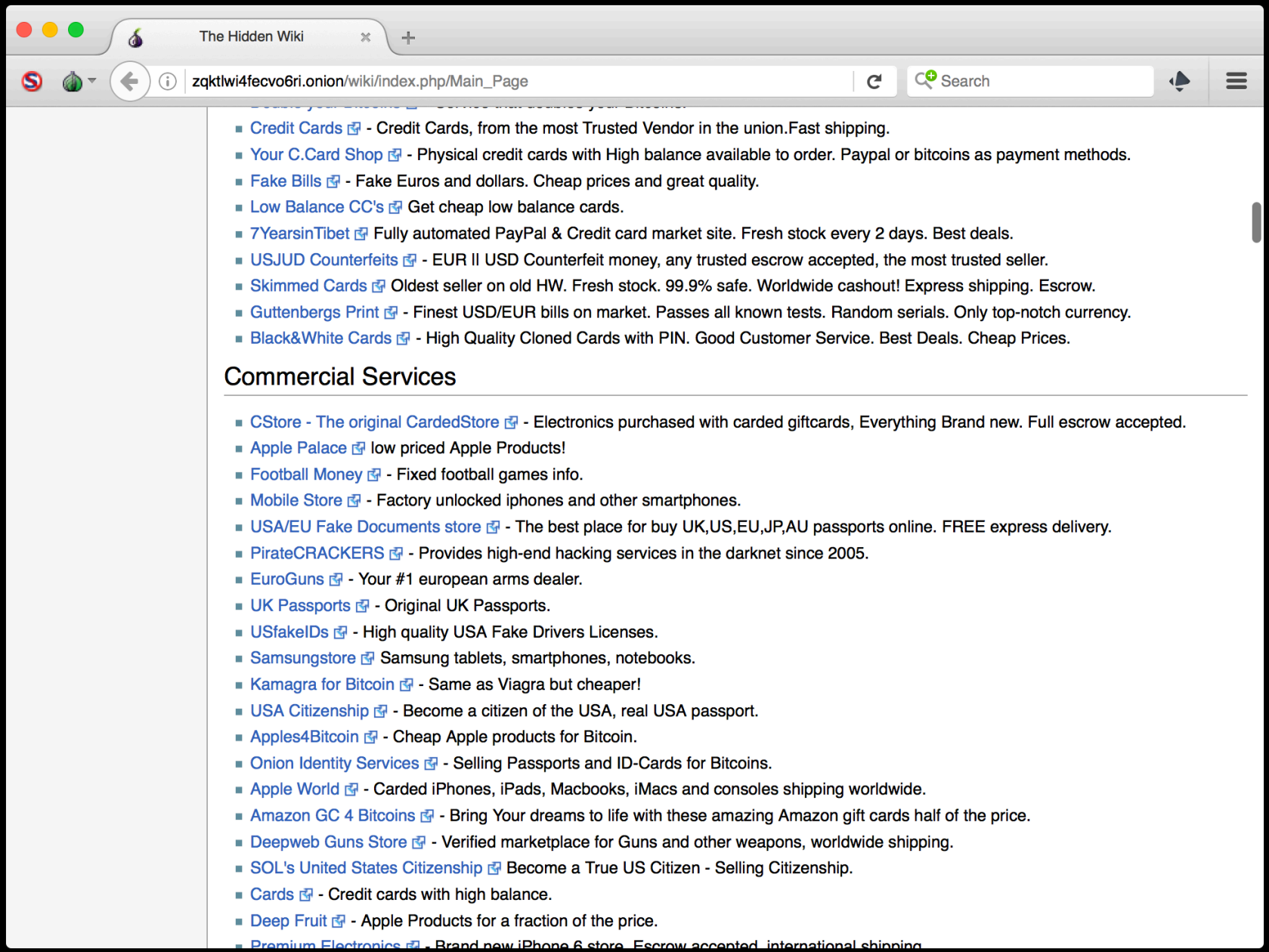
Tor

Usability (inzwischen) gut

Einschränkungen wegen JavaScript

Performance besser als gedacht

Tor Hidden Services


The Hidden Wiki
zqktlwi4fecvo6ri.onion/wiki/index.php/Main_Page
Search
Credit Cards - Credit Cards, from the most Trusted Vendor in the union.Fast shipping.
Your C.Card Shop - Physical credit cards with High balance available to order. Paypal or bitcoins as payment methods.
Fake Bills - Fake Euros and dollars. Cheap prices and great quality.
Low Balance CC's Get cheap low balance cards.
7YearsinTibet Fully automated PayPal & Credit card market site. Fresh stock every 2 days. Best deals.
USJUD Counterfeits - EUR II USD Counterfeit money, any trusted escrow accepted, the most trusted seller.
Skimmed Cards Oldest seller on old HW. Fresh stock. 99.9% safe. Worldwide cashout! Express shipping. Escrow.
Guttenbergs Print - Finest USD/EUR bills on market. Passes all known tests. Random serials. Only top-notch currency.
Black&White Cards - High Quality Cloned Cards with PIN. Good Customer Service. Best Deals. Cheap Prices.
Commercial Services
CStore - The original CardedStore - Electronics purchased with carded giftcards, Everything Brand new. Full escrow accepted.
Apple Palace low priced Apple Products!
Football Money - Fixed football games info.
Mobile Store - Factory unlocked iphones and other smartphones.
USA/EU Fake Documents store - The best place for buy UK,US,EU,JP,AU passports online. FREE express delivery.
PirateCRACKERS - Provides high-end hacking services in the darknet since 2005.
EuroGuns - Your #1 european arms dealer.
UK Passports - Original UK Passports.
USfakeIDs - High quality USA Fake Drivers Licenses.
Samsungstore Samsung tablets, smartphones, notebooks.
Kamagra for Bitcoin - Same as Viagra but cheaper!
USA Citizenship - Become a citizen of the USA, real USA passport.
Apples4Bitcoin - Cheap Apple products for Bitcoin.
Onion Identity Services - Selling Passports and ID-Cards for Bitcoins.
Apple World - Carded iPhones, iPads, Macbooks, iMacs and consoles shipping worldwide.
Amazon GC 4 Bitcoins - Bring Your dreams to life with these amazing Amazon gift cards half of the price.
Deepweb Guns Store - Verified marketplace for Guns and other weapons, worldwide shipping.
SOL's United States Citizenship Become a True US Citizen - Selling Citizenship.
Cards - Credit cards with high balance.
Deep Fruit - Apple Products for a fraction of the price.

Rückverfolgung anhand der IP leicht möglich

Tracking schwer zu verhindern

Tor und JonDonym inzwischen praxistauglich

Dr. Dominik Herrmann

Universität Siegen

https://dhgo.to/slides-hasi

http://herdom.net