

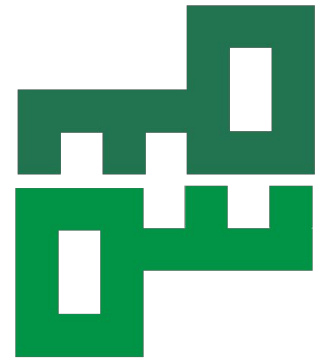
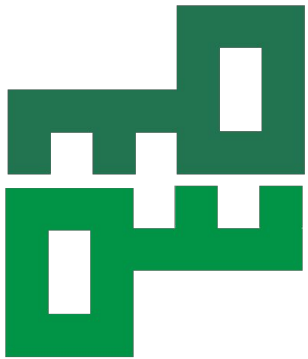
Webtracking and Countermeasures

Anton and Bernhard, [Cryptoparty Graz](#)

CC BY-NC-SA 4.0 (w/o product logos)

2015-04-25

[Linuxtage Graz](#), FH Joanneum



Anton

[PGP-key and Fingerprint](#)

2048R, 2014-02-27

A727 CC1E 08AD F9F3 9C43

E650 BFE1 E2F8 8AF5 A989

Bernhard Z.

[PGP-key and Fingerprint](#)

4096R, 2014-10-23

2015 C9D7 3FD4 355B 0D18

CFBD 3542 8539 ACDC 6F44

Structure

1. Commercial surveillance (= webtracking) and negative consequences
2. Available countermeasures
3. Measurement of effectiveness against surveillance
4. Rating of countermeasures for effectiveness and user comfort

Why commercial surveillance?

Euphemism of the decade: "Webtracking"

=> For Money!

- Get to know the users
- Create detailed profiles of persons (job, age, **buying power**, hobbies, politics, pregnancy ...)
- sell profiles to advertisement companies
- higher conversion rate with targeting
- higher prices for targeted ads

=> **Conversion tracking**

Problems:

- Profiling, Scoring
- Deanononymization
- Trade with profiles of persons (like stocks)
- insurances (tailored premiums)
- banks (tailored credit interests)
- employers (candidate screening)
- differential pricing
- political parties (election campaigns)

Further readings

Study (German): [Web-Tracking-Report](#)

Study (German): [Kommerzielle digitale Überwachung im Alltag](#)

Congressional Testimony: [What Information Do Data Brokers Have on Consumers?](#)

European Commission, Data Protection, [Article 29 Working Party](#)

2012-06-07, Opinion 04/2012 on Cookie Consent Exemption

2014-04-10, Opinion 05/2014 on Anonymisation Techniques

2014-11-25, Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting

Cane from JonDo [on browser tracking](#) (German)

Web Series [do not track](#) (in 4/2015 with 3rd party JS from google-analytics.com :-))

Articles

[How Microsoft and Yahoo Are Selling Politicians Access to You](#)

[Everything We Know About What Data Brokers Know About You](#)

So they don't sell information about my health?

[Insurers Test Data Profiles to Identify Risky Clients](#)

[Has Google Gone Too Far?](#)

[Parental Status Demographic Added to AdWords](#)

[Wie Facebook-Einträge einen Kredit verhindern können](#)

[EC-Datenfirma wollte zur neuen Schufa werden](#)

[Tricksen und täuschen mit System \(Differential Pricing\)](#)

[Auktion wie ein Wimpernschlag \(Real Time Bidding, find prices for targeted ads\)](#)

Actual state of commercial surveillance

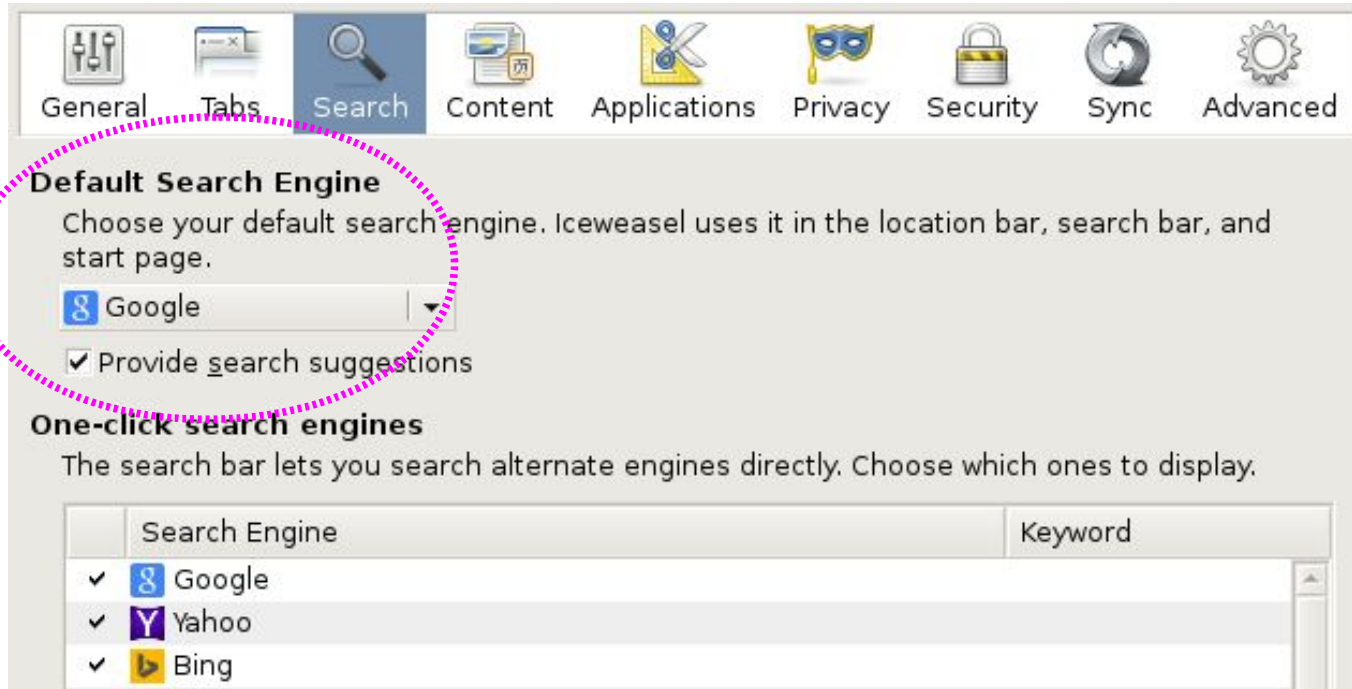
Alexa Top 20 Austria, Tue, 2015-04-21

Without tracking companies (no other trackers on their sites) and double sites: amazon.com, amazon.de, ebay.at, facebook.com, gmx.net, google.at, google.com, google.de, googleadservices.com, yahoo.com, youtube.com

- 1) orf.at, 2) de.wikipedia.org, 3) willhaben.at,
- 4) gmx.at, 5) derstandard.at, 6) ebay.de,
- 7) raiffeisen.at, 8) live.com, 9) sparkasse.at,
- 10) xhamster.com, 11) krone.at, 12) twitter.com,
- 13) streamcloud.eu, 14) geizhals.at, 15) xvideos.com
- 16) pornhub.com, 17) bankaustria.at, 18) a1.net,
- 19) herold.at, 20) spiegel.de

Standard Browser. Commercial surveillance!

The 300 M\$ setting. Unmodified Firefox:



2012 – 2014: Ca. 300 M\$ p.a. for being the default search.
Since 2015: US Yahoo, CN Baidu, RU Yandex, rest Google

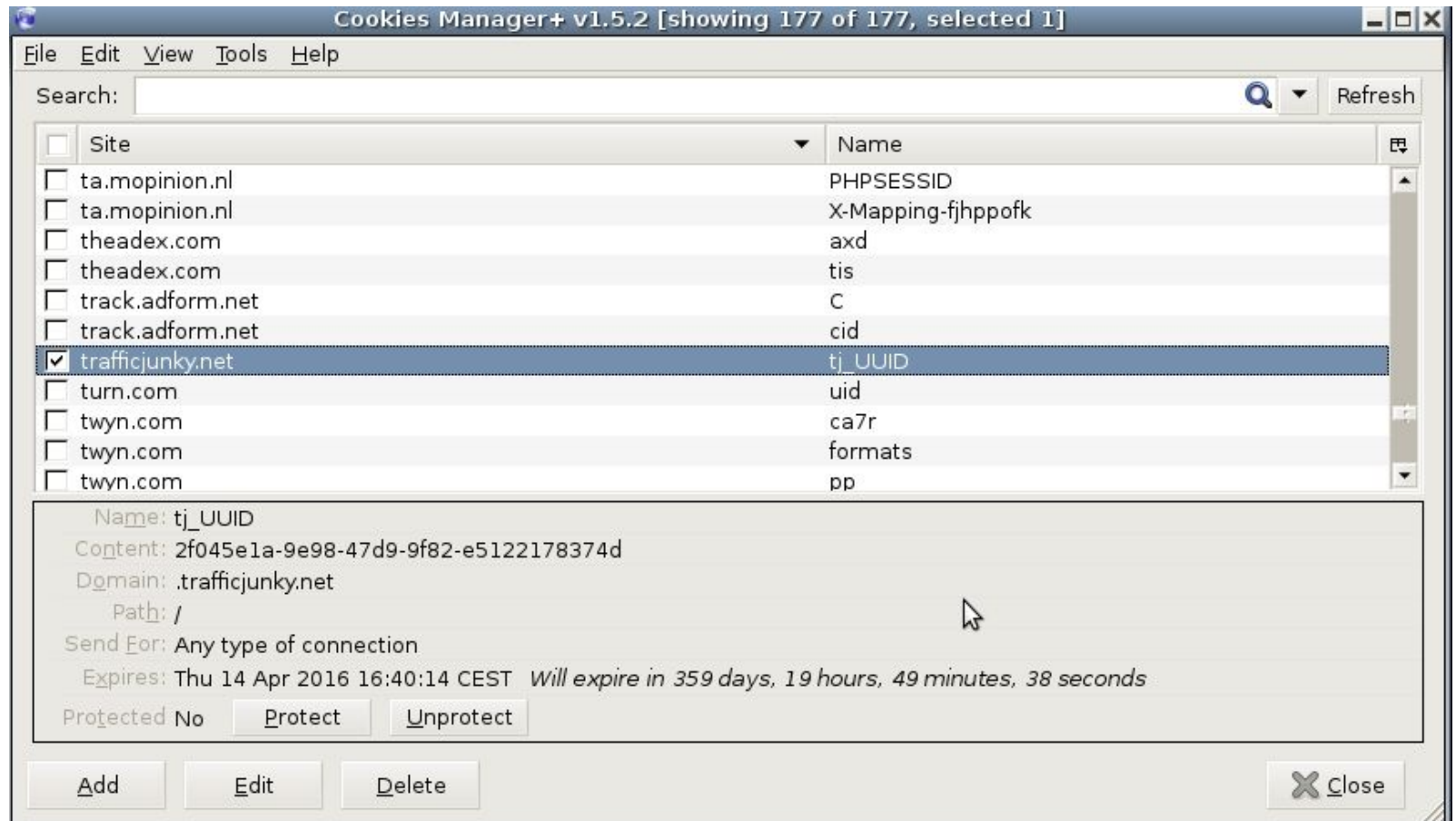
Note: In an earlier version of this presentation it was stated, that the 3rd party cookie from google.com, loaded directly after the start without further interaction, depended on this default search setting and is used for 3rd party tracking. This was wrong. The cookie is used for the [safebrowsing mode](#), and, [referencing to Google](#), sandboxed and not used for tracking purposes.

Mozilla is nevertheless your friend!

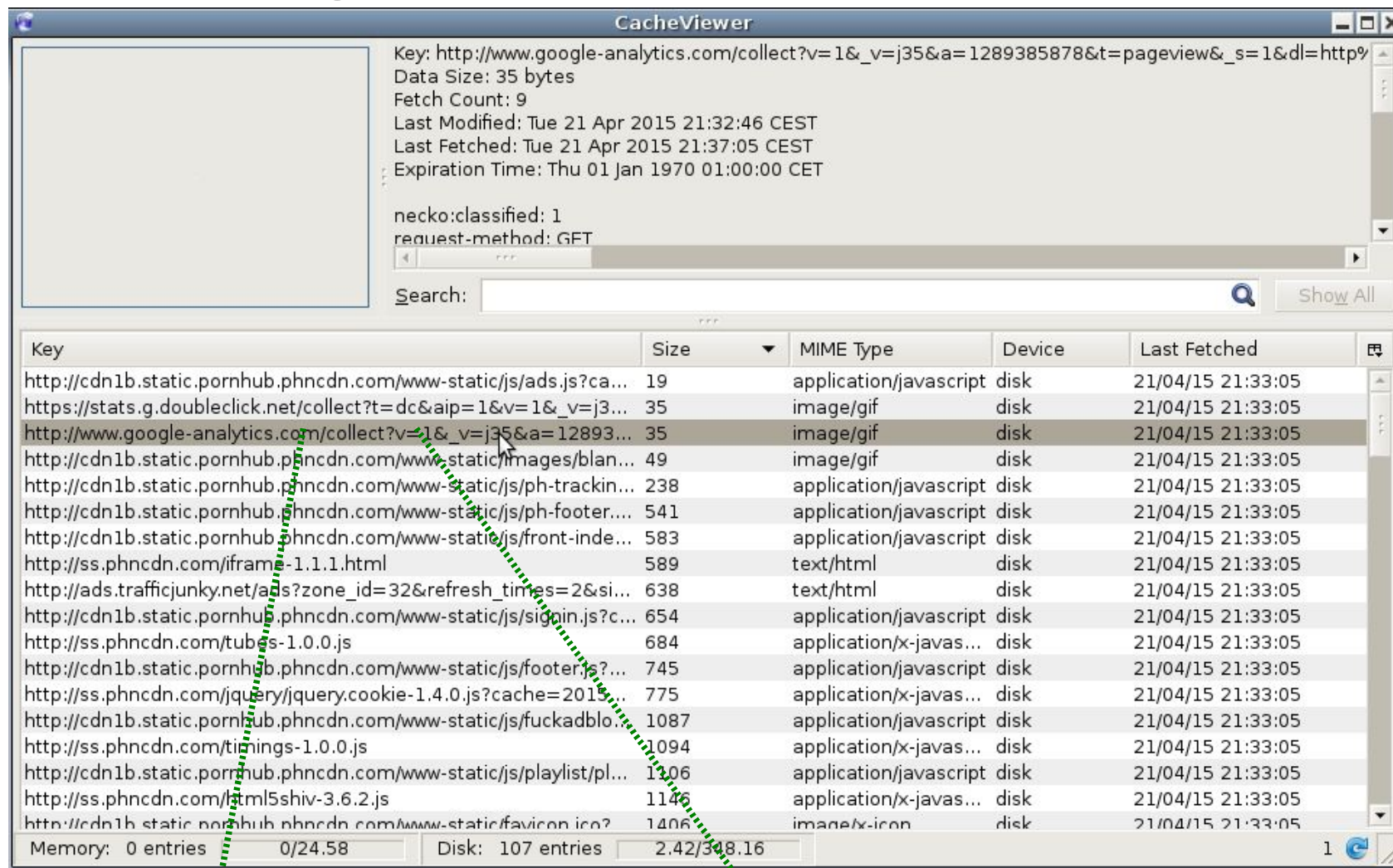
=> They just need money for the coders.

=> Buy merch articles, donate money!

Many cookies after normal surfing



Trackingpixels in Cache



CacheViewer

Key: http://www.google-analytics.com/collect?v=1&_v=j35&a=1289385878&t=pageview&_s=1&dl=http%3A%2Fwww.pornhub.com%2Fsd=24it&sr=1280x800&vp=1250x579&je=0&fl=11.2%20r202&_u=AGAAgAAB~&jid=984469428&cid=193702535.1429644766&tid=UA-2623535-1&z=1925177428

Data Size: 35 bytes
Fetch Count: 9
Last Modified: Tue 21 Apr 2015 21:32:46 CEST
Last Fetched: Tue 21 Apr 2015 21:37:05 CEST
Expiration Time: Thu 01 Jan 1970 01:00:00 CET

necko:classified: 1
request-method: GET

Search: Show All

Key	Size	MIME Type	Device	Last Fetched
http://cdn1b.static.pornhub.phncdn.com/www-static/js/ads.js?ca...	19	application/javascript	disk	21/04/15 21:33:05
https://stats.g.doubleclick.net/collect?t=dc&aip=1&v=1&_v=j3...	35	image/gif	disk	21/04/15 21:33:05
http://www.google-analytics.com/collect?v=1&_v=j35&a=12893...	35	image/gif	disk	21/04/15 21:33:05
http://cdn1b.static.pornhub.phncdn.com/www-static/images/blan...	49	image/gif	disk	21/04/15 21:33:05
http://cdn1b.static.pornhub.phncdn.com/www-static/js/ph-trackin...	238	application/javascript	disk	21/04/15 21:33:05
http://cdn1b.static.pornhub.phncdn.com/www-static/js/ph-footer....	541	application/javascript	disk	21/04/15 21:33:05
http://cdn1b.static.pornhub.phncdn.com/www-static/js/front-inde...	583	application/javascript	disk	21/04/15 21:33:05
http://ss.phncdn.com/iframe-1.1.1.html	589	text/html	disk	21/04/15 21:33:05
http://ads.trafficjunky.net/ads?zone_id=32&refresh_times=2&si...	638	text/html	disk	21/04/15 21:33:05
http://cdn1b.static.pornhub.phncdn.com/www-static/js/signin.js?c...	654	application/javascript	disk	21/04/15 21:33:05
http://ss.phncdn.com/tube/s-1.0.0.js	684	application/x-javas...	disk	21/04/15 21:33:05
http://cdn1b.static.pornhub.phncdn.com/www-static/js/footer.js?...	745	application/javascript	disk	21/04/15 21:33:05
http://ss.phncdn.com/jquery/jquery.cookie-1.4.0.js?cache=2015...	775	application/x-javas...	disk	21/04/15 21:33:05
http://cdn1b.static.pornhub.phncdn.com/www-static/js/fuckadblo...	1087	application/javascript	disk	21/04/15 21:33:05
http://ss.phncdn.com/timings-1.0.0.js	1094	application/x-javas...	disk	21/04/15 21:33:05
http://cdn1b.static.pornhub.phncdn.com/www-static/js/playlist/pl...	1106	application/javascript	disk	21/04/15 21:33:05
http://ss.phncdn.com/html5shiv-3.6.2.js	1116	application/x-javas...	disk	21/04/15 21:33:05
http://cdn1b.static.pornhub.phncdn.com/www-static/favicon.ico?	1406	image/x-icon	disk	21/04/15 21:33:05

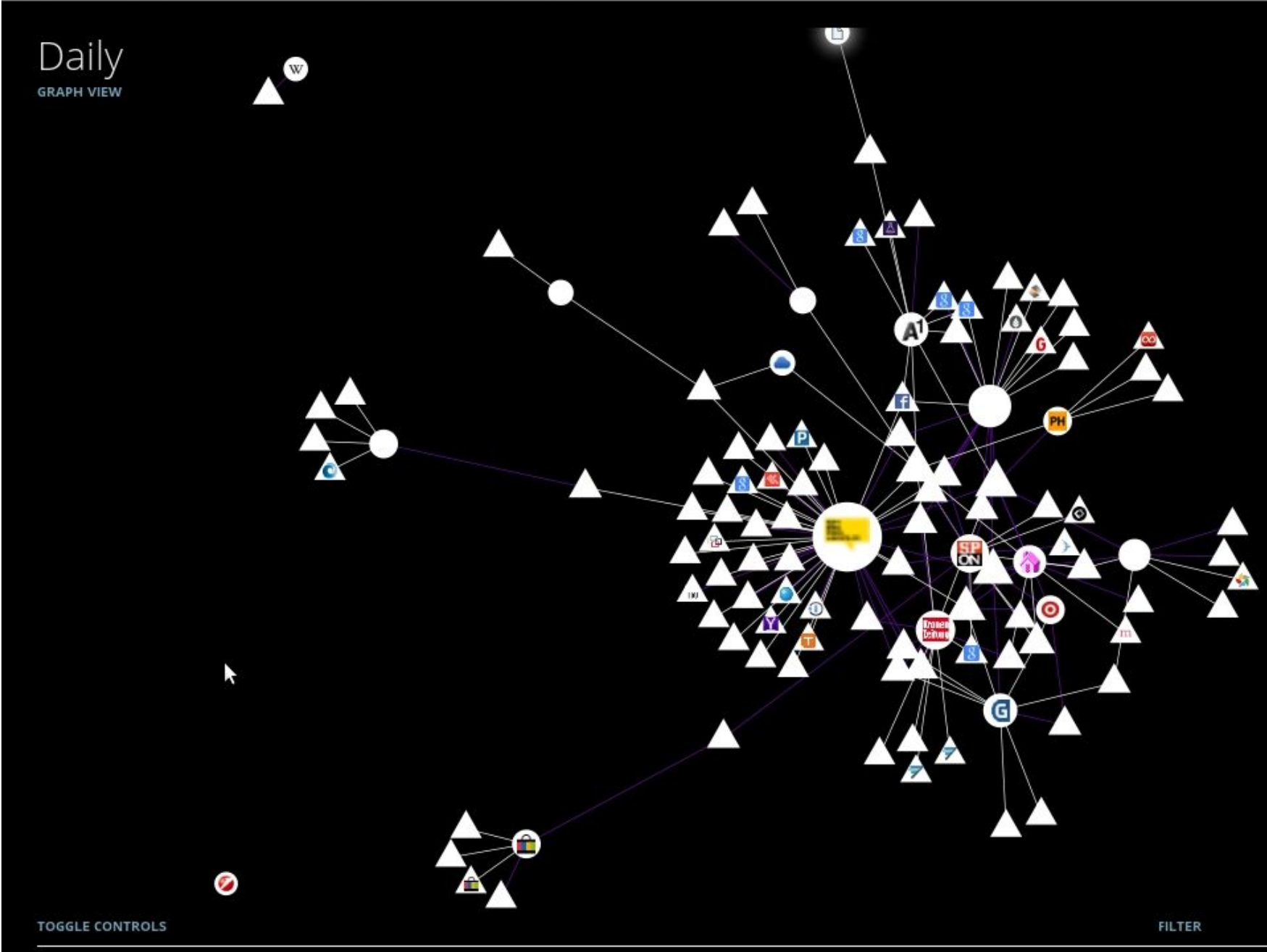
Memory: 0 entries 0/24.58 Disk: 107 entries 2.42/308.16

http://www.google-analytics.com/collect?v=1&_v=j35&a=1289385878&t=pageview&_s=1&dl=http%3A%2Fwww.pornhub.com%2Fsd=24it&sr=1280x800&vp=1250x579&je=0&fl=11.2%20r202&_u=AGAAgAAB~&jid=984469428&cid=193702535.1429644766&tid=UA-2623535-1&z=1925177428

Stalking parties

DATA GATHERED SINCE APR 20, 2015 YOU HAVE VISITED 19 SITES YOU HAVE CONNECTED WITH 115 THIRD PARTY SITES

TRACKING PR



Visualisation from Lightbeam

Browser Fingerprinting

- Sending of technical data from browser, programs, operating system and device to server.
- Passive via HTTP protocol and active via JavaScript (JS)
- Fingerprint = combination of many single data --> Very low probability for 2nd combination of browser - OS - machine with identical fingerprint
- Example Fingerprinters: **Panopticlick, Am I Unique**



Example adspirit fingerprinter:
IP, browser, OS, time, timezone, screen resolution, colour depth, CPU type, DNT header, language

Further tracking technologies

Browser based

Flash Cookies (LSO)

Canvas Fingerprinting via JS

Measurement of browser latency via JS

Potential misuse TLS (HSTS cookies)

Not browser based

TCP/IP Stack Fingerprinting

Clock Skew (see Heise, caida)

Deep packet injection by ISP

Countermeasures in Firefox

If possible: Use Firefox ESR (higher frequency!)

Only search engines: [Ixquick](#), [DuckDuckGo](#), [Qwant](#), [Startpage](#). Disable "Provide search suggestions"

Only 3 local standard fonts allowed

Language set to en-us, en

External applications: "Always ask"

Do not track header

Reject 3rd party cookies

Clear history when Firefox closes (delete everything)

Limit disk-cache to 0 MB of space

Disable automatically update of search engines

Set necessary plugins to "always ask" (e. g. Flash)

Deactivate/deinstall unnecessary plugins

NoScript:

Block 3rd party JS

Delete Whitelist

Block iFrames, WebGL

Firefox basis configuration, about:config

Broadcasted via HTTP and JS: Iceweasel user agent

```
general.userAgent.override =  
Mozilla/5.0 (X11; Linux i686; rv:37.0) Gecko/20100101 Firefox/37.0 instead of  
Mozilla/5.0 (X11; Linux i686; rv:37.0) Gecko/20100101 Firefox/37.0 Iceweasel/37.0.1
```

via http: From which site you come

ESR v31 for one variant

```
network.http.sendRefererHeader = 0
```

via JS: YYYYMMDDhhmmss compilation and location

```
general.buildID.override = empty  
geo.enabled = false
```

via JS: Public IP beside proxy via WebRTC

```
media.peerconnection.enabled = false
```

Stop pre-loading of linked sites (via HTTP)

```
network.dns.disablePrefetch = true  
network.prefetch-next = false
```

More standard user agents and proposals in the annex

AddOns against webtracking:

HTTPS everywhere v5.0.2

uBlock v0.9.1.0 (default filter lists)

NoScript v2.6.9.21

Privacy Badger v0.2.6

Request Policy Contd. v1.0b8.2

User Agent Overrider v0.2.5

Available Standard solutions:

Tor Browser Bundle v4.0.8

JonDonym v00.19.001, JonDoFox v2.11.0

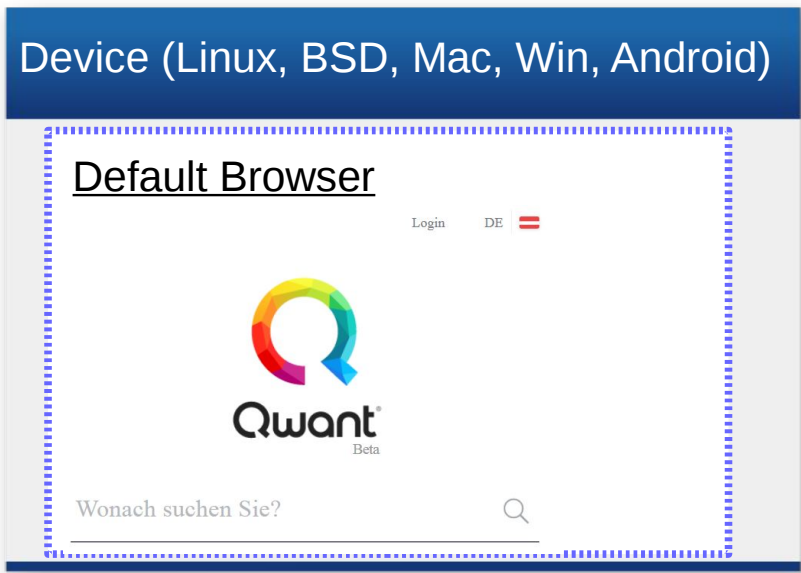
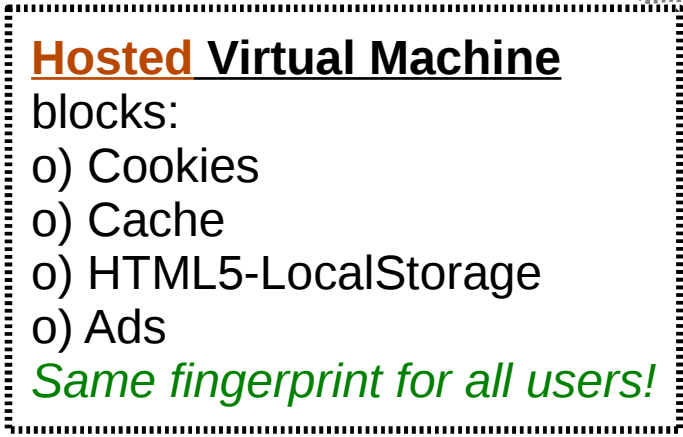
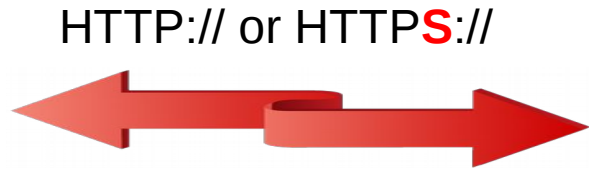
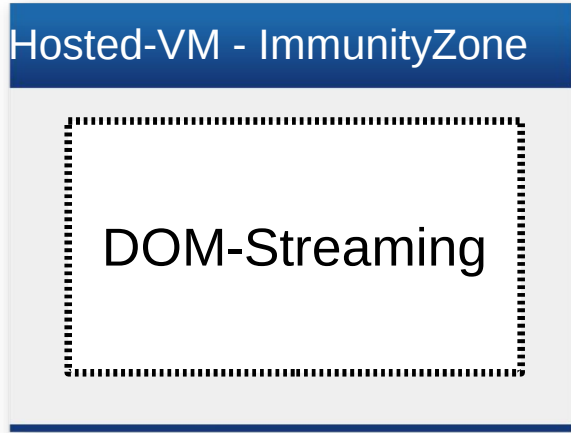
Immunity Zone with original Firefox



IMMUNITYZONE

Project page: immunityzone.com

Test at: amune.org



Status: Beta

good for Smartphones/Tablets
 good for PC's on work (no admin)
 bad for Netbanking

ImmunityZone.com
 Paid Version


Amune.org
 Ad-Based(tracking free)
 Shared VM/Only for Anti-Web-Blocking


facebook

Email or Phone Password
 Keep me logged in [Forgot your password?](#)

Connect with friends and the world around you on Facebook.

 **See photos and updates** from friends in News Feed.

 **Share what's new** in your life on your Timeline.

 **Find more** of what you're looking for with Graph Search.

Sign Up

It's free and always will be.

Birthday

[Why do I need to provide my birthday?](#) 



Privacy Machine

Internet (here *be dragons* ...)

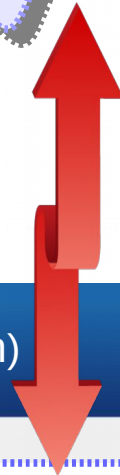


Smaug
(c) D. Melvin

My-IP
Login-Data



Anonym-IP
VPN or
mobile
broadband



PC (Linux, BSD, Mac, Win)

- Installed Fonts
- Screen resolution
- Hardware-ID's

Keepass

UseCase: Research (UI of VM)

Sites: e. g. Facebook, Twitter

User-Agent

(3rd-Party)-Cookies

Plugins



Local Virtual Machine (VirtualBox)

- o) (Flash-)Cookies/Cache/HTML5-LSO
-> Switchback VM-Snapshot: Delete all!
 - o) IP-Adress: changes via i.e. VPN
 - o) Browser-Fingerprint:
 - x) changing Browser (+User-Agent)
 - x) OS: install/deinstall fonts
 - x) change language/timezone
 - x) change screen resolution
- Browser-Fingerprint is unique, but changes in every Browsing-Session!

Status: Prototype

Join us!

C++ Devs needed, any OS

contact@privacymachine.eu

PrivacyMachine Update successful.

Select a new UseCase

- News
- OnlineBanking

Start

Details...

PrivacyMachine Update successful.

News/Investigation

Web Images Videos

About Advanced Settings

start page™

the world's most **private** search engine

PrivacyMachine

News/Investigation

Ubuntu Start Page - Mozilla Firefox

File Edit View History Bookmarks Tools Help

Ubuntu Start Page

Search or enter address

Google

Thu, 03 Apr 02:51 pm

Measurement of efficiency

Setup of experiment

- Debian Linux, i386, v7.8, fully patched
- Adobe Flash Player v11.2.202.451
- Firefox (Iceweasel) v37.0.1
- AddOns for measurement:
 - Cookies Manager+ v1.5.2
 - CacheViewer v0.8.6
 - NoScript v2.6.9.21
 - Lightbeam v1.2.1
 - User Agent Overrider v0.2.5

Variants to be measured

a) Original open. Firefox w/o modifications, as installed. Browser stays open

b) Original closed. Like a), close + re-open

c) DNT1. DO! NOT! TRACK! Base config, uBlock

d) DNT2. Base config, Privacy badger

e) DNT3. Base config, Request Policy

f) DNT4. Base config, no cookies, Request Policy block all, block all JS, all plugins off, *stepwise activation*.
User Agent v31 ESR → *bigger anonymity group!*

g) Original PW. Like b), but Priv. Window (Ctrl+Shift+P)

h) TBB. Tor Browser Bundle v4.0.8 (w. & w/o JS) *Free*

i) JDF. JonDonym v00.19.001, JonDoFox v2.11.0 *50-100 €/y*
6 €/GB

j) IZ. Raw F'fox, TLS to ext. VM ImmunityZone *0-240 €/y*

unmodified

home-grown

prefabricated

Results of measurement

Other working principle, connection from server ends at VM, see the slides

	2015-04-20, ISP: A1, dyn. IP in Graz/Austria					2015-04-21, ISP: A1, dyn. IP in Graz/Austria					
<i>?: not counted, estimation</i>	a) orig. open	b) orig. closed	c) DNT1	d) DNT2	e) DNT3	f) DNT4 "ESR"	g) orig. PW	h) TBB orig	h1) TBB no JS	i) JDF "ESR"	j) IZ
3rd party requests	?, many	-	?, many	?, many	?, many	10 (a)	?, many	?, many	?, many	?, many	0
Counted local markers before or after restart	before	after	before	before	before	before	after	before	before	before	before
Intended deletion of markers at closing OK?	not intend.	not intend.	yes	yes	yes	yes	in large part	yes	yes	yes	in large part
Cookies	267	180	83	86	86	73 (a)	4	0	0	?, 70 (a)	2
Cookies, 3rd party	?, many	95	0	0	0	0	4 (b)	0	0	0	1
Cache, elements disk	2030	2092	0	0	0	0	41	0	0	1114	1579
Cache, disk, in MB	45.7	45.5	0	0	0	0	1	0	0	20.8	27.8
Cache, elements RAM	168	0	9	28	22	31	0	1981	1225	1114	28
Cache, RAM, in MB	?	?	0.5	0.5	0.5	0.6	0	21.6	15.7	20.8	?, little
Cache, elements <= 76B	243	134	2	14	9	8	0	?, many	?, many	28	46
Cache, elements 3rd p.	?, many	?, many	0	10	5	7	41 (c)	?, many	?, many	?, few	2
Cache, "adult" pictures	?, many	?, many	0	0	0	0	0	?, many	?, many	?, some	?, some
Cache, "adult" videos	5	5	0	0	0	0	0	0	0	0	0
Cache, advert. videos	1	1	0	0	0	0	0	0	0	0	0
Flash cookies, LSO	1	1	0	0	0	0	1	0	0	0	0
Lightbeam, 3rd parties	89	89	11	24	17	8	0	8	0	10	1
Lightbeam, disconnected 1 st parties, no.	2, 8, 10, 17,	2, 8, 10, 17,	all	all	all	all	all	all	all	all	all
JS, 1st & 2nd party	20	-	20	20	20	8 (a)	20	20	8	8	1
JS, 3rd parties	63	-	5	5	5	5 (a)	?, 60	?	?, little	5	0
JS, 3rd p. on min. 2 pgs.	20	-	0	0	0	0	?, 20	?	0	0	0
JS, disconnected 1st parties, no.	2, 9, 17	2, 9, 17	all	all	all	all	?	all	all	all	all
Panopticlick, same Fp (d)	2	2	2	3	4	2430 (e)	3	1 (f)	10450	2430 (e)	6
share in %	0.00004	0.00004	0.00004	0.00006	0.00008	0.00015	0.00006	0.00002	0.20	0.00015	0.00011
Am I Unique, same Fp (g)	2	2	2	2	3	124 (e)	3	1 (f)	435	124 (e)	4
share in %	0.00282	0.00282	0.00282	0.00282	0.00423	0.00423	0.00423	0.00140	0.61	0.00423	0.00564
Broken sites		-	-	-	-	10, 13, 15, 16	-	10, 13, 15, 16	10, 13, 15, 16	10, 13, 15, 16	

(a) manual activation: 8 x cookie domains, 13 x JS domains, 10 x request (request only DNT4) (b) adnxs.com, google.com (c) wikipedia.org (d) basis 4/2015: 5.256 Mio Fingerpr. (e) JS off, user agent changed to Firefox v31 (ESR) on Linux i386 (preset in JDF). (f) browser windows size sent with activated JS, very individual, but only "fingerprintable" property (g) basis 4/2015: 0.071 Mio Fingerpr.

Mozilla/5.0 (X11; Linux i686; rv:28.0) Gecko/20100101 Firefox/28.0
version number increase to
 Mozilla/5.0 (X11; Linux i686; rv:37.0) Gecko/20100101 Firefox/37.0
same scheme for
 Mozilla/5.0 (X11; Linux x86_64; rv:28.0) Gecko/20100101 Firefox/28.0
 Mozilla/5.0 (Windows NT 6.1; rv:28.0) Gecko/20100101 Firefox/28.0
 Mozilla/5.0 (Windows NT 6.1; WOW64; rv:28.0) Gecko/20100101 Firefox/28.0

<https://amiunique.org>

basis (b) of measured fingerprints:
71,302

<https://panopticlick.eff.org>

basis (b) of measured fingerprints:
5,262,400

b increased during ca. 4 h from
 5,262,100 to 5,262,800
*one in x browsers have the same
 fingerprint as yours (x)*

Ffox version	release date yymmdd
28	140318
29	140429
30	140610
31	140722
32	140902
33	141014
34	141201
35	150113
36	150224
37	150331

Hier könnte ihre

Werbung stehen!

Linux		Windows	
i386	x64	i386	x64
75,174	21,391	59,126	12,126
86,265	17,197	44,220	6,907
142,220	13,704	38,132	8,771
2,166	16,092	5,051	6,410
99,286	50,598	58,475	9,265
154,770	40,478	38,983	5,822
122,376	37,320	58,475	8,557
187,934	33,095	54,821	7,122
219,257	39,865	49,649	10,807
478,379	51,089	89,200	14,340

Number (n) of tests with identical fingerprint

n is displayed on site

*n calculated: $n = 1 / x * b$*

Ffox version	release date yymmdd	Linux		Windows		Linux		Windows	
		i386	x64	i386	x64	i386	x64	i386	x64
28	140318	3	5	1	1	70	246	89	434
29	140429	2	5	1	27	61	306	119	762
30	140610	1	2	1	5	37	384	138	600
31	140722	124	9	440	13	2,430	327	1,042	821
32	140902	1	3	2	4	53	104	90	568
33	141014	1	5	4	61	34	130	135	904
34	141201	9	82	37	183	43	141	90	615
35	150113	5	29	8	105	28	159	96	739
36	150224	4	22	27	40	24	132	106	487
37	150331	5	9	7	19	11	103	59	367

Rating of countermeasures

Surveillance scenarios - commercial

C1) Commercial standard. 3rd party cookies, tracking pixels, 3rd party JS fingerprinting, IP

C2) Commercial advanced. Like C1), plus: 1st party JS fingerprinting, clock skew, deep packet injection by ISP, TCP/IP stack fingerprinting, canvas fingerprinting, latency measurement

C3) Commercial unknown. Like C2), plus: yet unknown commercial tracking measures. E. g. the Verizon X-UIDH header was detected only by accident after > 2 yrs in 10/2014.

!! INCREASE OF COST !!



Surveillance scenarios – intel. services

I1) Intel. services standard. Like C1), mainly passive wiretapping at net hubs. Automated analysis of **all metadata**.

I2) Intel. services advanced. Like C2), plus: Automated timing correlation at VPN servers (package flow in/out), automated attacks at browsers.

I3) Intel. services targeted. Like I2), plus: (Manual) deanon. of obfuscated traffic (Tor, JonDo, multihop VPN), search for user errors (email addresses for accounts, non-obfuscated IPs, MAC addresses, machine fingerprints, ...), **exploitation of programs, OS, firmware.**

!! INCREASE OF COST AND RISK !!

Rating of surveillance protection

Use at private internet connection, normal OS, browser closed once per day. Grades: 6 (insufficient) to 1 (very good)

	b) orig. closed	c) DNT1	c) DNT1, 1 VPN (I)	d) DNT2	e) DNT3	f) DNT4	f1) DNT4, 2 VPN (II)	g) orig. priv. Window	h) TBB orig.	h1) TBB no JS	i) JDF	j) IZ
C1	6	2	1	2 (III)	2 (III)	1	1	5	1	1	1	1
C2	6	5	3	5	5	2	1	6	1	1	1	1
C3	6	6	4	6	6	4	3 (IV)	6	2	1	2 (IV)	2 (VII)
I1	6	3	2	3	3	2	1	5	2	1	1	1
I2	6	5	4	5	5	3	3 (IV)	6	3 (V)	1	2 (IV)	4
I3	6	6	5	6	6	6	5	6	5	5+	5 (VI)	5
Comfort	1	3	3	3	3	6	6	2	4	5	5	3

(I): single hop VPN service (0-50 €/y), block TCP timestamp (Firewall)

(II): double hop VPN service (~ 100 €/y), block TCP timestamp

(III): filter algorithms / -lists should be improved, not further treated

(IV): JS on/off → 1st party fingerprintability

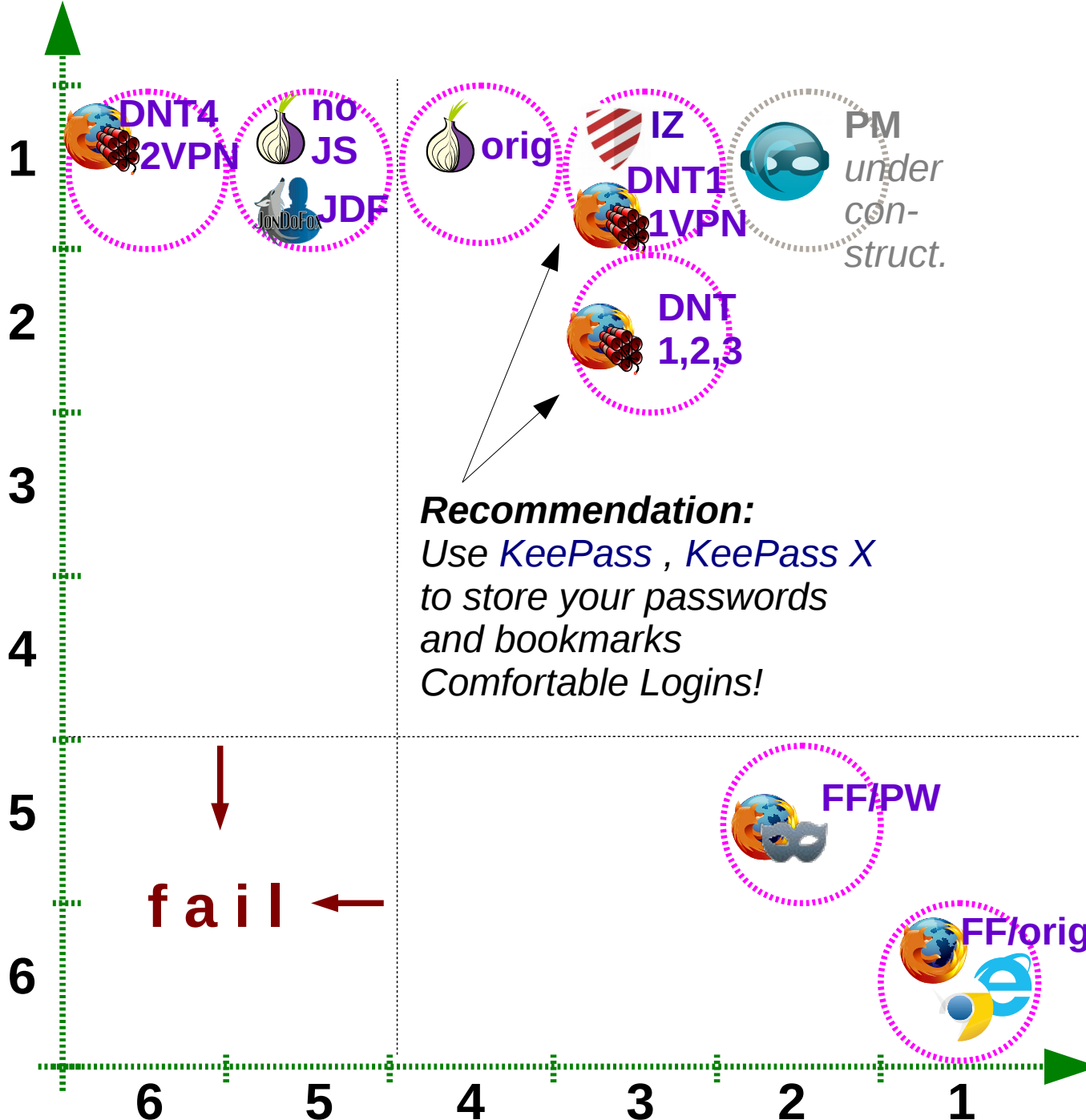
(V): activated JS increases attack surface










(VI): less JonDonym hubs than Tor hubs → deanonymization cheaper

(VII): depends on activity of operator

Choose commercial VPN services from EFF supporters!

Protection against Commercial Tracking - Level 1



-  **FF/orig** Firefox: w/o modifications
-  **FF/PW** Firefox w/o mod., Private Window
-  **DNT1 1VPN** basic config, uBlock block 3rd party JS single hop VPN
-  **DNT4 2VPN** basic config, no cookies, Request Pol. block all, block all JS, all plugins off stepwise activation double hop VPN
-  ImmunityZone: HTTPS to Hosted VM
-  **orig** TOR: orig
-  **noJS** TOR: JS off
-  **JDF** Jondonym JonDoFox
-  **PM** PrivacyMachine local VM (under construction)

Summary

- Unmodified browsers: Full surveillance from 1st click on. **Be aware of that!**

- Effective countermeasures are possible by own modifications.

- **DNT1 is a good and approved compromise.**

- **DNT4: block everything by default.**

Home-grown secure antitracking for masochists. ;-)

- Effective standard solutions are available (**Tor**, **JonDonym**, **ImmunityZone**. **Check TLS certificates! MITM!**)

- Future secure and comfortable countermeasures are under construction: **PrivacyMachine**. **Join us!**

- Find your own compromise between security and comfort, see the rating.

Annex

More tools to play with:

[Cookie Monster](#) . Administer your cookies.

[Profile Switcher](#) . Easy switching of F'fox profiles

[Policeman](#) . Similar to Request policy

[Secret Agent](#) . Creates obfuscation

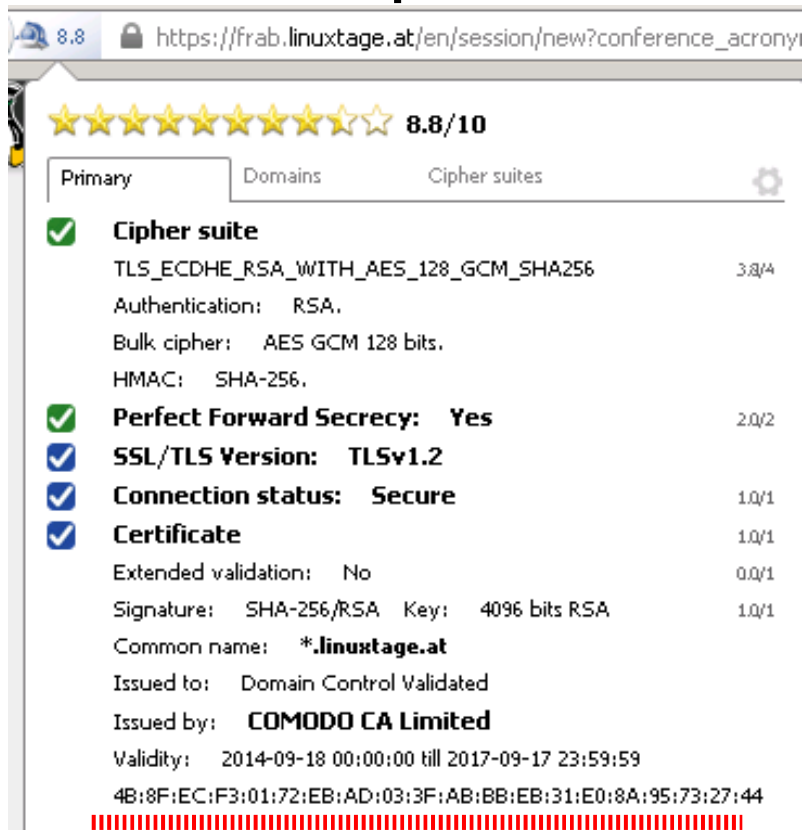
[Referrer Control](#) . Easy setting of referer options.

[Bleachbit](#) . Cleaner, read the descriptions!

[Fluxfonts](#) . Creates obfuscation for sent system fonts.

Proposal for manual check of TLS certificates

- Store the Fingerprint locally, e. g. in the appropriate entry of [KeePass](#) or [KeePassX](#).
- Use [SSLeuth](#) to easily show the TLS fingerprint of the connected server and compare the two hash values.
- Be sure to enter your password in the right server, counteract possible [MITM](#) attacks.



8.8 https://frab.linuxtage.at/en/session/new?conference_acronym

8.8/10

Primary Domains Cipher suites

- ✓ **Cipher suite** 3.8/4
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
Authentication: RSA.
Bulk cipher: AES GCM 128 bits.
HMAC: SHA-256.
- ✓ **Perfect Forward Secrecy: Yes** 2.0/2
- ✓ **SSL/TLS Version: TLSv1.2**
- ✓ **Connection status: Secure** 1.0/1
- ✓ **Certificate** 1.0/1
Extended validation: No 0.0/1
Signature: SHA-256/RSA Key: 4096 bits RSA 1.0/1
Common name: *.linuxtage.at
Issued to: Domain Control Validated
Issued by: COMODO CA Limited
Validity: 2014-09-18 00:00:00 till 2017-09-17 23:59:59
4B:8F:EC:F3:01:72:EB:AD:03:3F:AB:BB:EB:31:E0:8A:95:73:27:44

**AddOn for automatic check:
Certificate Patrol**

linuxtage.at frab			
Group:	Gruppen	Creation:	22/02/2014
Username:	****	Access:	05/03/2015
Password:	****	Modification:	05/03/2015
Attachment:		Expiration:	Never [-]
URL:	https://frab.linuxtage.at		
Comment:	SHA1 4B:8F:EC:F3:01:72:EB:AD:03:3F:AB:BB:EB:31:E0:8A:95:73:27:44 ##### #####@runbox.com		

More proposals for about:config

Filter for :// . Proposal: Delete, what does not aim at Mozilla URLs.

browser.contentHandlers.types.0.uri , browser.search.geoip.url ,
devtools.gcli.jquerySrc , devtools.gcli.lodashSrc , devtools.gcli.underscoreSrc ,
experiments.manifest.uri , gecko.handlerService.schemes.irc.0.uriTemplate ,
gecko.handlerService.schemes.ircs.0.uriTemplate ,
gecko.handlerService.schemes.mailto.0.uriTemplate ,
gecko.handlerService.schemes.mailto.1.uriTemplate ,
gecko.handlerService.schemes.webcal.0.uriTemplate , geo.wifi.uri ,
loop.oauth.google.scope , social.whitelist , toolkit.telemetry.server

!! Add Malware lists to uBlock from before changing safebrowsing !!
malwaredomainlist.com , malwaredomains.com

browser.safebrowsing.appRepURL , browser.safebrowsing.gethashURL ,
browser.safebrowsing.malware.reportURL , browser.safebrowsing.reportURL ,
browser.safebrowsing.updateURL

AddOns in about:config: Delete noscript-strings which contain "google"

More standard user agents:

Mozilla/5.0 (X11; Linux x86_64; rv:37.0) Gecko/20100101 Firefox/37.0

Mozilla/5.0 (Windows NT 6.1; rv:37.0) Gecko/20100101 Firefox/37.0

Mozilla/5.0 (Windows NT 6.1; WOW64; rv:37.0) Gecko/20100101 Firefox/37.0

3rd party JS, partly fingerprinters

1, **orf.at**, 2mdn.net, adworx.at, doubleclick.net, googlesyndication.com, meetrics.net, mxcdn.net, oewabox.at, 2, **de.wikipedia.org**, wikimedia.org, 3, **willhaben.at**, adition.com, adnxs.com, akamaihd.net, amazon-adsystem.com, apa.net, criteo.com, cxense.com, facebook.com, facebook.net, goldbach.com, google.at, googleadservices.com, oewabox.at, optimizely.com, revsci.net, styria-digital.com, twyn.com, 4, **gmx.at**, ad-balancer.net, adform.net, adnxs.com, criteo.com, doubleclick.net, googlesyndication.com, meetrics.net, mxcdn.net, plista.com, tifbs.net, ui-portal.de, uimserv.net, 5, **derstandard.at**, adserver.net, google-analytics.com, meetrics.net, mxcdn.net, oewabox.at, 6, **ebay.de**, ebayrtm.com, ebaystatic.com, ioam.de, 7, **raiffeisen.at**, elba.at, google-analytics.com, ttweb.net, 8, **live.com**, bkrtx.com, bluekai.com, demdex.net, gfx.ms, omtrdc.net, 9, **sparkasse.at**, 2mdn.net, adition.com, criteo.com, doubleclick.net, google-analytics.com, googlesyndication.com, googletagservices.com, insightexpressai.com, ioam.de, meetrics.net, moatads.com, mxcdn.net, theadex.com, yieldlab.net, 10, **xhamster.com**, trafficstars.com, 11, **krone.at**, adtech.de, chartbeat.com, google-analytics.com, googlesyndication.com, grm-pro.com, meetrics.net, mxcdn.net, oewabox.at, serving-sys.com, 12, **twitter.com**, google-analytics.com, twimg.com, 13, **streamcloud.eu**, ajax-googleapis.com, google-analytics.com, 14, **geizhals.at**, ad-balancer.net, adworx.at, gzhls.at, maxymiser.net, meetrics.net, mxcdn.net, oewabox.at, 15, **xvideos.com**, ajax.googleapis.com, trafficfactory.biz, 16, **pornhub.com**, contentabc.com, doublepimp.com, etahub.com, google-analytics.com, phncdn.com, trafficjunky.net, 17, **bankaustria.at**, - 18, **a1.net**, facebook.net, google-analytics.com, google.at, googleadservices.com, mopinion.nl, visualwebsiteoptimizer.com, 19, **herold.at**, adform.net, adition.com, ajax-googleapis.com, akamaihd.net, clicktale.net, facebook.com, google-analytics.com, googletagmanager.com, meetrics.net, mxcdn.net, oewabox.at, revsci.net, 20, **spiegel.de**, 2mdn.net, adition.com, criteo.com, doubleclick.net, google-analytics.com, googlesyndication.com, googletagservices.com, insightexpressai.com, ioam.de, meetrics.net, moatads.com, mxcdn.net, theadex.com, yieldlab.net

DNT4, manual activations

		3rd party requests				Javascript		Cookies
1	orf.at	-				-		-
2	de.wikipedia.org	-				-		-
3	willhaben.at	apa.net				-		-
4	gmx.at	ui-portal.de	gmx.net (to)	gmx.net (from)		gmx.at	gmx.net	gmx.net
5	derstandard.at	-				-		-
6	ebay.de	ebayimg.com	ebaystatic.com	ebay.com (to)	ebay.com (from)	ebay.de	ebaystatic.at	ebay.de
7	raiffeisen.at	-				raiffeisen.at	elba.at	raiffeisen.at
8	login.live.com	gfx.ms				live.com	gfx.ms	live.com
9	sparkasse.at	-				sparkasse.at		sparkasse.at
10	xhamster.com	<i>broken</i>				-		-
11	krone.at	-				-		-
12	twitter.com	twimg.com				twitter.com	twimg.com	twitter.com
13	streamcloud.eu	<i>broken</i>				-		-
14	geizhals.at	-				-		-
15	xvideos.com	<i>broken</i>				-		-
16	pornhub.com	<i>broken</i>				-		-
17	bankaustria.at	-				bankaustria.at		bankaustria.at
18	a1.net	-				a1.net		a1.net
19	herold.at	-				-		-
20	spiegel.de	-				-		-