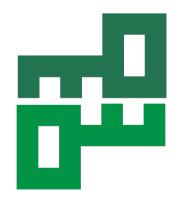
### DO! NOT! TRACK!

Workshop for Firefox

Anton, Cryptoparty Graz

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

#### 2015-04-25 Linuxtage Graz, FH Joanneum



**Anton** <u>PGP-key and Fingerprint</u> 2048R, 2014-02-27 A727 CC1E 08AD F9F3 9C43 E650 BFE1 E2F8 8AF5 A989

# Countermeasures against webtracking for Firefox (setting named "DNT1", see the study)

If possible: Use Firefox ESR (higher frequency!)

Only search engines:

Ixquick, DuckDuckGo, Qwant, Startpage



die diskreteste Suchmaschine der Welt



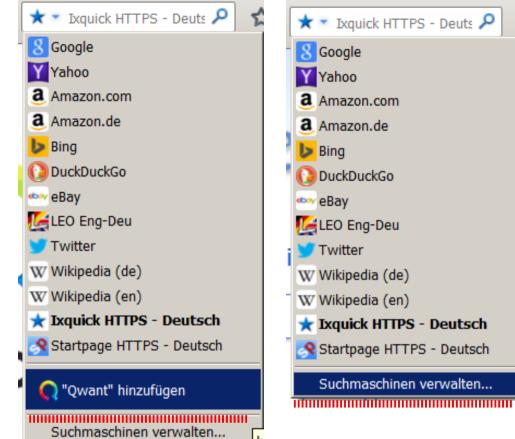
Zu Firefox hinzufügen | Als Startseite einrichten

=> promise of data
protection (one needs
to believe that ...)



die diskreteste Suchmaschine der Welt





# 🛨 Ixquick HTTPS - Deutsch Startpage HTTPS - Deutsch Suchmaschinen verwalten...

#### Liste der Suchmaschinen verwalten

Momentan sind folgende Suchmaschinen installiert: Schlüsselwort Name 8 Google DuckDuckGo 📩 Ixquick HTTPS ... Schlüsselwort bearbeiten... 옷 Startpage HTT... Nach oben 📿 Qwant.com Nach unten Entfernen Suchvorschläge anzeigen Weitere Suchmaschinen hinzufügen... Vorgaben wiederherstellen Abbrechen OK

X

# Only 3 local standard fonts (less data broadcastet, smaller fingerprint)

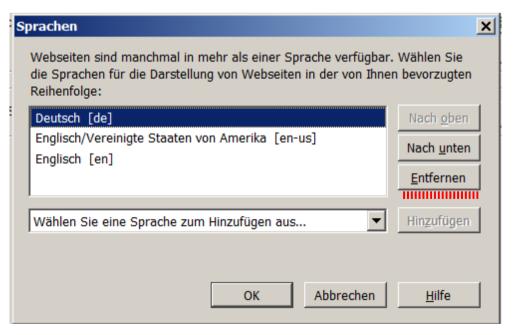
nstellungen							
		<b>页</b>		90		$\bigcirc$	١.
Allgemein	Tabs	Inhalt	Anwendungen	Datenschutz	Sicherheit	Sync	Erweitert
	Fenster bl	ockieren					<u>A</u> usnahmen
Schriftarten	& Farben-						
<u>S</u> tandard-Sc	hriftart:	Times Nev	v Roman		▼ <u>G</u> rö	ße: 16	▼ <u>E</u> rweitert
							<u>F</u> arben
Sprachen —							
Bevorzugte S	Sprachen f	für die Dars	stellung von <u>W</u> ebsi	tes wählen			<u>W</u> ählen
	Allgemein Allgemein C Pop-up-l Schriftarten Standard-Sc Sprachen	Allgemein Tabs	Allgemein Tabs Inhalt Pop-up-Fenster blockieren Schriftarten & Farben Standard-Schriftart: Times New Sprachen	Allgemein Tabs   Inhalt Anwendungen     Inhalt Anwendungen     Schriftarten & Farben   Standard-Schriftart: Times New Roman   Sprachen	Allgemein Tabs     Inhalt     Anwendungen        Datenschutz     Datenschutz     Schriftarten & Farben     Standard-Schriftart:   Times New Roman	Allgemein Tabs   Inhalt Anwendungen   Datenschutz   Sicherheit   Schriftarten & Farben Standard-Schriftart: Times New Roman    Image: Sprachen	Allgemein       Tabs       Inhalt       Anwendungen       Datenschutz       Sicherheit       Sync         Image: Schriftarten & Farben       Standard-Schriftart:       Times New Roman       Image: Sprachen       Größe:       16

### Here with Windows fonts, other for Mac, Linux, BSD

chriftarten	<u>×</u>
– <u>S</u> chriftarten fü	ir: Lateinisch
Proportional:	Serif Größe 16 💌
S <u>e</u> rif:	Times New Roman
S <u>a</u> ns Serif:	Arial
Feste Breite:	Courier New Größe 13 -
	Minimale Schriftgröße: Keine 💌
Seiten <u>d</u> as	Verwenden von eigenen statt der oben gewählten Schriftarten erlauben
Zeichenkodieru	ing für veralteten Inhalt
Diese Zeichenk angeben.	codierung wird für veraltete Inhalte verwendet, welche ihre Zeichenkodierung nicht
Zu verwenden	de Zeichenkodierung: Standard für derzeitige Sprache
	OK Abbrechen <u>H</u> ilfe

## Set language to en-us, en (most widespread, smaller fingerprint)

Einstellu	ngen								×
			<u>م</u>		90		O	ġ.	
Allger	nein	Tabs	Inhalt	Anwendungen	Datenschutz	Sicherheit	Sync	Erweitert	
		Fenster bl & Farben	ockieren					<u>A</u> usnahmen.	
<u>S</u> tand	lard-Sc	hriftart:	Times Nev	w Roman		▼ <u>G</u> rö	ße: 16	▼ Erweitert	·     -
								<u>F</u> arben	
Sprac	hen —								
Bevor	zugte S	prachen	für die Dars	stellung von <u>W</u> ebsi	ites wählen			<u>W</u> ählen	



### External applications: Always ask (less data broadcastet, smaller fingerprint, better security)

Einstellungen								×
Allgemein	Tabs	<b>国际</b> Inhalt	Anwendungen	Datenschutz	Sicherheit	Sync Sync	Erweitert	
				1				
Suchen								٩
Dateityp				Aktion				
📸 Adobe A	crobat For	ms-Dokume	ent (application/vr	n 👎 Jedes I	Mal nachfrage	n		
The Adobe A	crobat For	ms-Dokume	ent (application/vr	n 👎 Jedes I	Mal nachfrage	n		
📸 Adobe A	crobat XMI	-Datenpak	etdatei	🖓 Jedes I	Mal nachfrage	n		
🥾 irc				🖓 Jedes I	Mal nachfrage	n		
🧶 ircs				👎 Jedes I	Mal nachfrage	n		
🧶 mailto				Micros	oft Outlook vei	rwenden (:	Standard)	
Nodcast				🟸 Vorsch	au in Firefox			
🔧 Portable	Document	Format (P	DF)	👎 Jedes	Mal nachfrage	n		-
Video-Po	dcast			🖓 Vorsch	au in Firefox			
Web-Fee	ed				1al nachfrager			
al webcal				💷 Datei s	peichern			Jede
				🔀 Adobe	Acrobat verw	enden (Sta	andard)	Jeac
				_	Acrobat (in Fir	•	venden	
				Andere	Anwendung			
					ОК	Abbrech	en <u>H</u> i	lfe

#### Send Do-not-track header

#### Change settings for local storage

E	instellungen								×
	Allgemein	Tabs	<b>国际</b> Inhalt	Anwendungen	Datenschutz	Sicherheit	Sync	Erweitert	
-	ragement	1000	Innuic	I			Sync	Liwellert	
	Verfolgung	von Nutzera	ktivitäten -						
	Website	s mitteile <u>n</u> ,	meine Ak	tivitäten nicht zu v	refolgen				
	O Website	s mitteilen,	meine Ak	ti <u>v</u> itäten zu verfolg	jen				
	O Website	s keine Prä	iferenz übe	er die Verfolgung <u>i</u>	meiner Aktivitäte	en mitteilen			
	Weitere Info	ormationen							
	Chronik								
	Firefox wird	laina Chron	siles and a						
	Firefox wird	eine Chror		-			]		
			anle	gen nals anlegen					
				ı benutzerdefinier	tan Finstallunga	n anlegen			
				, Downloads, For			begriffe u	nd Cookies	
	speiche	ern.							
	Sie kör	inen auch d	lie kürzlich	angelegte Chroni	k oder einzelne	Cookies lösche	en.		
	Sie koi			angelegte en en		0001100 100011			
	 ⊢ Adressleiste								
	In der Adres	ssleiste F	inträge aus	s Chronik und Lese	ezeichen 🔻	vorschlagen			
	In <u>a</u> er nare.		intrage du	S Chronik and Eco		vorbenlagen			
						ОК	Abbrech	en <u>H</u> ilfe	e

#### Block 3rd party cookies Automatic deletion of locally stored markers

Einstellungen
Allgemein Tabs Inhalt Anwendungen Datenschutz Sicherheit Sync Erweitert
Allgemein       Tabs       Inhalt       Anwendungen       Datenschutz       Sicherheit       Sync       Erweitert         Verfolgung von Nutzeraktivitäten
<ul> <li>Immer den privaten Modus verwenden</li> <li>Besuchte Seiten und Download-Chronik speichern</li> </ul>
<ul> <li>Eingegebene Suchbegriffe und Formulardaten speichern</li> </ul>
✓     Cookies akzeptieren
Cookies von Drittanbietern akzeptieren:       Nie         Behalten, bis:       sie nicht mehr gültig sind       Cookies anzeigen         Die Chronik löschen, wenn Firefox geschlossen wird       Einstellungen         Adressleiste       Image: Cookies anzeigen
In <u>d</u> er Adressleiste Einträge aus Chronik und Lesezeichen 💌 vorschlagen
OK Abbrechen <u>H</u> ilfe

### Stop sending you entries in the address bar to search engines

							×
Tabs	」 Inhalt	Anwendungen	Datenschutz	Sicherheit	Sync	Erweitert	
Datenübern Ifen eren von To e bereits be en, wenn V natischen B en Bildlauf a warebeschle	nittlung N ext mit der im Eintippe Vebseiten v ildlauf aktiv aktivieren eunigung <u>v</u> e	etzwerk Update Tastatur zulasser n starten ersuchen umzulei ieren	Zertifikate				
					Abbrech	on 1	lilfe
	Tabs Tabs Datenüberr Ifen eren von Tr e bereits be en, wenn V natischen B en Bildlauf varebeschle	Tabs Inhalt Tabs Inhalt Datenübermittlung N Ifen eren von Text mit der e bereits beim Eintippe en, wenn Webseiten v natischen Bildlauf aktiv en Bildlauf aktivieren varebeschleunigung ve	Tabs       Inhalt       Anwendungen         Datenübermittlung       Netzwerk       Update         Ifen       Inhalt       Update         eren von Text mit der Tastatur zulasser       Image: Statum zulasser         e bereits beim Eintippen starten       Image: Statum zulasser         en, wenn Webseiten versuchen umzulei       Image: Statum zulasser         inatischen Bildlauf aktivieren       Image: Statum zulasser         en Bildlauf aktivieren       Image: Statum zulasser         warebeschleunigung verwenden, wenn versuchen       Image: Statum zulasser	Tabs       Inhalt       Anwendungen       Datenschutz         Datenübermittlung       Netzwerk       Update       Zertifikate         Ifen       eren von Text mit der Tastatur zulassen       e bereits beim Eintippen starten         en, wenn Webseiten versuchen umzuleiten oder neuzular	Tabs       Inhalt       Anwendungen       Datenschutz       Sicherheit         Datenübermittlung       Netzwerk       Update       Zertifikate       Sicherheit         Ifen       eren von Text mit der Tastatur zulassen       e       Sicherheit         e bereits beim Eintippen starten       en, wenn Webseiten versuchen umzuleiten oder neuzuladen       Sicherheit         natischen Bildlauf aktivieren       en Bildlauf aktivieren       Sicherheit         en Bildlauf aktivieren       Sicherheit       Sicherheit	Tabs       Inhalt       Anwendungen       Datenschutz       Sicherheit       Sync         Datenübermittlung       Netzwerk       Update       Zertifikate	Tabs       Inhalt       Anwendungen       Datenschutz       Sicherheit       Sync       Eweitert         Datenübermittlung       Netzwerk       Update       Zertifikate       Image: Sicherheit       Sync       Eweitert         Datenübermittlung       Netzwerk       Update       Zertifikate       Image: Sicherheit       Sync       Eweitert         Datenübermittlung       Netzwerk       Update       Zertifikate       Image: Sicherheit       Sync       Eweitert         Ifen       eren von Text mit der Tastatur zulassen       espreits beim Eintippen starten       Image: Sicherheit       Image: Sicher

#### Set cache disk to 0 MB (less tracking pixels)

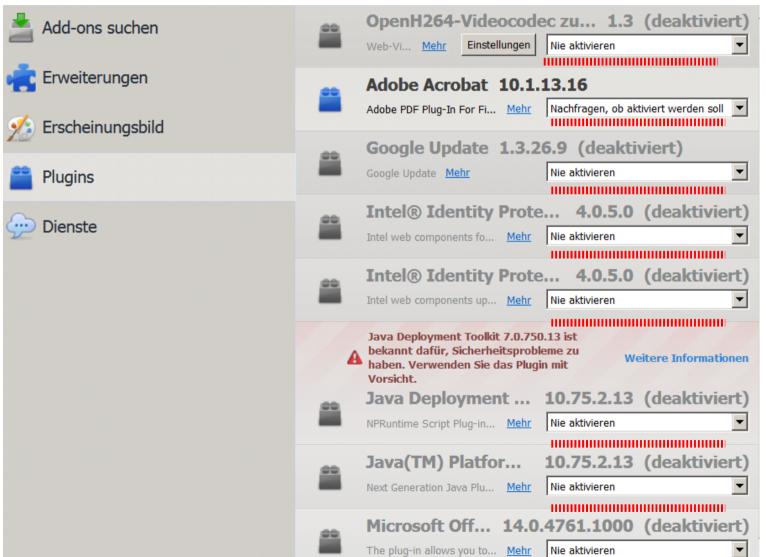
Einstellungen	×
	žÕj:
Allgemein Tabs Inhalt Anwendungen Datenschutz Sicherheit Sync	Erweitert
Allgemein Datenübermittlung Netzwerk Update Zertifikate	
	1
Verbindung	
Festlegen, wie sich Firefox mit dem Internet verbindet	Ei <u>n</u> stellungen
Zwischengespeicherte Webinhalte	
Ihr Webseiten-Cache belegt derzeit 17,0 KB Festplatten-Speicherplatz	<u>]</u> etzt leeren
Automatisches Cache- <u>M</u> anagement ausschalten	
Cache auf 0 MB Speicherplatz limitieren	
⊂ Offline-Webinhalte und -Benutzerdaten	
Ihr Anwendungs-Cache belegt derzeit 0 Bytes Festplatten-Speicherplatz	Jetzt leeren
Nachfragen, <u>w</u> enn Websites Daten für die Verwendung im Offline-Modus speichern	
möchten.	<u>A</u> usnahmen
Folgende Websites dürfen Daten für die Verwendung im Offline-Modus speichern:	_
	Entfernen
	1
OK Abbreck	nen <u>H</u> ilfe

### Disable automatic update of search engines (Google won't come back ...)

Einstellungen								X
Allgemein	Tabs	<b>国际</b> Inhalt	Anwendungen	Datenschutz	Sicherheit	Sync	Erweitert	
-			tzwerk Update					
Firefox-Up		J	minim	II <sup>1</sup>				
		icch inctalli	ron (omnfahlan	: erhöhte Sicherh	unit)			
			in Add-on deakt		ieit)			
			vor der Installatio					
				: Sicherheitsrisiko	-1			
			nicht empronien:	: Sichemeitsnsiko	1)			
Update- <u>C</u>	hronik anz	eigen						
Automatis	ch aktualisi	eren:						
Suchn	naschinen							
4000000								
					ОК	Abbrech	en <u>H</u> i	lfe

Set necessary plugins to always ask (e.g. Flash Player, PDF reader), disable the rest. Drastically reduces the amount of broadcastet data and the fingerprint. Improves the security, deactivates exploitable plugins.

n	Extras	<u>H</u> ilfe			-
		-	Strg+J		
	A <u>d</u> d-	ons	Strg+Umschalt+A		
	шүрү	ļ		0	
	Sync	einrich	ten	Ľ	
		-Entwic eninforr	kler •		1
	<u>E</u> inst	ellunge	n		



#### Measures in about:config

about:config ×	+
Firefox about:config	V C DuckGo P
	Hier endet möglicherweise die Gewährleistung! Änderungen der Standardwerte dieser erweiterten Einstellungen können gefährlich für Stabilität, Sicherheit und Geschwindigkeit dieser Anwendung sein. Sie sollten nur fortfahren, wenn Sie genau wissen, was Sie tun. Diese Meldung beim nächsten Mal anzeigen Ich werde vorsichtig sein, versprochen!

#### In case of Firefox/Iceweasel on Debian:

#### Set user agent to standard version of *actual release*

Mozilla/5.0 (X11; Linux i686; rv:37.0) Gecko/20100101 Firefox/37.0 or for x64 to Mozilla/5.0 (X11; Linux x86\_64; rv:37.0) Gecko/20100101 Firefox/37.0

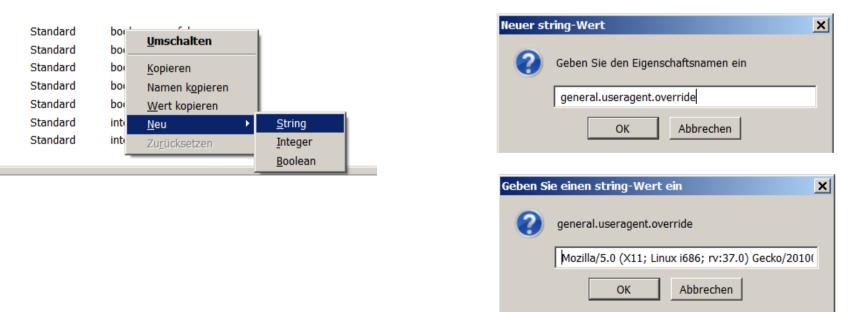
#### Much more widespread than

Mozilla/5.0 (X11; Linux i686; rv:37.0) Gecko/20100101 Firefox/37.0 Iceweasel/37.0.1

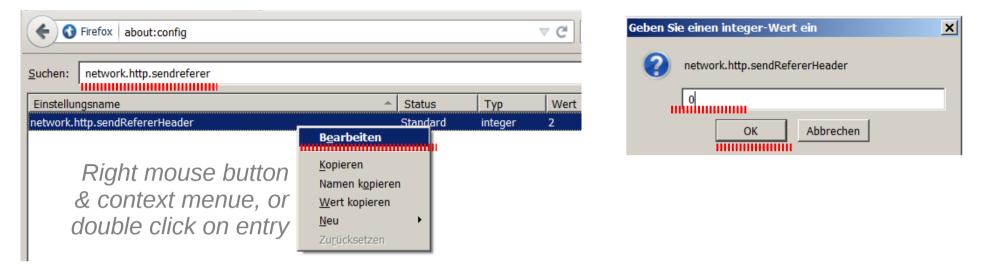
--> Leave small user group, enter bigger user group.

Right mouse click in about:config, new string

general.useragent.override



#### Stop telling, from which site you come



Stop telling public IP beside proxy via JS and WebRTC
media.peerconnection.enabled = false
Stop telling your location
geo.enabled = false
Stop pre-loading of linked sites (via http)
network.dns.disablePrefetch = true
network.prefetch-next = false

### AddOns

#### - Prefer encrypted version of sites

Surveillants at net hubs only see, **that** you connect to https://site1.eu, not **what** you do there

#### HTTPS everywhere

- Block 3rd party JS e. g. JS from tracker.com on site1.eu
   => mainly fingerprinters
   NoScript (setup next slide)
- Apply preconfigured filter lists for 3rd party tracking domains (blacklisting)

block at site1.eu connection to google.com, facebook.com, tracker1.de, tracker2.at, ...

uBlock (default filter lists, more available)

#### Setup NoScript

### Allow JS from 1st and 2nd party

8	≡			=		
S abo	out:newta	ab temporär erlä	auben			
Sab	out:new	tab erlauben				
🗐 Nic	ht vertra	uenswürdig				•
Sg Tel	mporär a	lle Beschränkun	gen für diese	Seite auf	heben	
SAlle	e Beschrä	inkungen für die	se Seite aufh	eben		
Skr	ipte allge	emein erlauben (	(nicht empfol	nlen)		
<u>E</u> in	stellunge	n				
Übe	er NoScri	pt 2.6.91				

#### (site1.eu, prefix/site1.eu, site1.eu/subsite1, ...)

🕙 NoScript - Einstellungen	_ 🗆 X
Allgemein Positivliste Eingebettete Objekte Aussehen Benachrichtigungen Erweitert	
<ul> <li>Jeweils aktuelle Top-Level-Site temporär erlauben</li> <li>Vollständige Adressen (http://www.noscript.net)</li> <li>Vollständige Domains (www.noscript.net)</li> </ul>	
Second-Level-Domains (noscript.net)	
Berechtigungen-Menü öffnen beim Überfahren des NoScript-Symbols mit dem Mauszeiger	
Berechtigungen für aktuelle Top-Level-Site mit Links-Klick auf die Symbolleisten-Schaltfläche umschalten     (ctrl+shift+BACK SLASH)	
C Vollständige Adressen (http://www.noscript.net)	
C Vollständige Domains (www.noscript.net)	
Second-Level-Domains (noscript.net)	
Petroffene Seiten beim Ändern der Berechtigungen automatisch neu laden	
Reload the current tab only	
Spenden Importieren Exportieren Zurücksetzen OK Abb	rechen

# Delete 3rd party JS fingerprinters, who bought their place on the NoScript whitelist

NoScript - Einstellungen	_ 🗆 🗙						
Allgemein Positivliste Eingebettete Objekte Aussehen Benachrichtigungen Erweitert							
Sie können festlegen, welchen Websites Sie das Ausführen von Skripten erlauben möchten. Geben Sie bitte die exakte Adresse oder die Domain der Website ein (z.B. "http://www.site.com" oder "site.com"), für die Sie dies zulassen möchten, und klicken Sie dann auf "Erlauben".							
Adresse der Website:							
	Erlauben						
google.com							
googleapis.com							
googlevideo.com gstatic.com							
hotmail.com							
informaction.com							
live.com							
live.net							
maone.net							
mootools.net							
mozilla.net							
Ausgewählte Websites entfernen       Imporäre Berechtigungen aufheben       Importieren         Skripte allgemein erlauben (nicht empfohlen)       Importieren	Exportieren						
<u>S</u> penden Importieren Exportieren <u>Z</u> urücksetzen OK	Abbrechen						

# Block iframes and WebGL, apply also to manually whitelisted sites.

🕘 NoScript	- Einstellun	gen					_ 🗆 X
Allgemein	Positivliste	Eingebettete Objekte	Aussehen	Benachrichtigungen	Erweitert		
Diese Ein	stellungen we	inkungen für nicht vo erden erst bei neuen oc		2	n wirksam		
Adob	<sup>™</sup> verbieten e® Flash® v osoft® Silverl re Plugins ve	erbieten I♥ ight™ verbieten □	<iframe> v <frame/> v</iframe>		fant face verbiet		
🗹 Dies	e Einschränl	kungen auch auf ver als nicht vertrauenswür	trauenswü	rdige Websites anw		en	
Platz	haltersymbol	hriften mittels WebGL v anzeigen anzeigen für Objekte vo		ortrauona wiirdia oinaa	uctuftan Sitas		
Bestä	itigungsmeldu	ung anzeigen, bevor eir en Elementen freigeber	i Objekt tem		stuiten sites		
					1	1	
<u>S</u> pender	1	Importieren	Exportiere	en <u>Z</u> urücksetzen	]	ОК	Abbrechen

#### Now we have got:

- Only search engines, who promise data protection
- No activation of plugins w/o confirmation
- Blocking of all 3rd party cookies
- Storage of cache markers only in RAM
- Deletion of locally stored markers at end of session
- Blocking of 3rd party cache elements (depending on <u>timeliness</u> of filter blacklists)
- Reduced data output to fingerprinters
- Blocking of 3rd party fingerprinters
- (+) Acceptable user comfort!
- (-) External password manager neededSometimes 3rd party JS is necessaryVery seldom: Necessity of 3rd party cookies

DO! NOT! TRACK! Hardcore (setting DNT4)

Masochist setting :-)

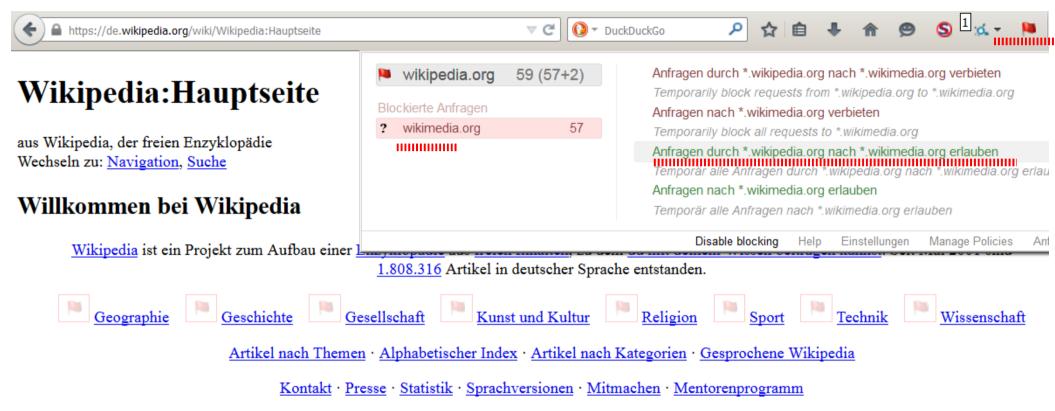
- Like before
- Block all cookies
- Block all Javascript
- Turn all plugins off
- Set user agent to v31, the actual ESR (bigger user group)
- Request Policy Contd. instead of uBlock
- Deactivate Request Policie's automatic whitelists
- Block all 3rd party requests by default.
- Stepwise activation of 3rd party requests, cookies and Javascript (manual whitelisting)

#### Setup Request policy

🚺 🕶 DuckDuckGo							
Fill	0 Disebbe blocking – Usia – Einstellungen – Manage Deliging – Auforgenehensile						
VT Homepage	Disable blocking Help <u>Einstellungen</u> Manage Policies Anfragenchronik						
Chrome://requestpolicy/content	s/settings/defaultpolicy.html 🗸 C DuckDuckGo 🔎 🛠 🖻 🖡 🎓 🥯 S						
RequestPolicy Default Policy							
Einstellungen	When you don't have any "allow" or "block" rules that match a request, this is what RequestPolicy will do. Learn more.						
Manage Policies	• Allow requests by default.						
Help	Block requests by default. (For advanced users. Breaks many websites.)						
About	Allow requests to the same domain (www.example.com -> static.example.com).						
	Changing your default rule means different subscriptions are available. Manage subscriptions.						
Your Policy							
Default Policy							
Subscriptions							

Chrome://requestpolicy/content	/settings/subscriptions.html		▼ C DuckDuckGo	م	☆	Ê	+	<b>^</b>	9	S
RequestPolicy	Subscriptio	n Policies								
Einstellungen Manage Policies			intained by us with help from t ng requests that impact your pri		y. Thes	e rules	are upd	lated a	utoma	tically a
Help About	Usability	Allow red	stinations that belong to the sam quests that are needed for websi quests for embedded content su	tes to work p	roperly	,	n webpa	age		
Your Policy Default Policy Subscriptions	Browser	11111	quests related to Mozilla and Fi quests that are needed for other			properly	Ÿ			

#### Manual activation of requests



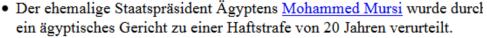
#### Artikel des Tages

#### In den Nachrichten

#### Der Völkermord an den Armeniern geschah während Oskar Gröning • Calbuco • Libor-Skandal

des Ersten Weltkrieges unter Verantwortung der jungtürkischen, von der Organisation Komitee für Einheit und Fortschritt gebildeten Regierung des Osmanischen Reichs. Einem der ersten systematischen Genozide des
20. Jahrhunderts fielen bei Massakern und Todesmärschen, die im Wesentlichen in den Jahren 1915 und

1916 stattfanden, je nach Schätzung zwischen 300.000 und mehr als 1,5 Millionen Menschen zum Opfer. Die Angaben zu den getöteten Armeniern während der Übergriffe in den beiden vorangegangenen Jahrzehnten variieren zwischen Zehntausenden und Hunderttausenden. Die Ereignisse, die von den Armeniern selbst mit dem Beoriff *Aghet* – "Katastrophe" – bezeichnet werden.  Im Zuge der <u>Operation Eikonal</u> hat der <u>BND</u> (Logo) bis zu 40.000 Ziele, darunter Politiker und Unternehmen in Deutschland und Westeuropa, ausgespäht und die Erkenntnisse an die <u>National</u> <u>Security Agency</u> weitergeleitet.



125

• Ein <u>Flüchtlingsboot im Mittelmeer</u> mit mehr als 700 Menschen an Bord kenterte in der Nacht auf den 19. April. Laut dem <u>UNHCR</u> ist dies

#### Now we have got:

- Standard setting like before
- Maximum protection from 3rd party tracking: only necessary 3rd party request are allowed
- Maximum protection from 1st party tracking: cookies and JS (evil fingerprinters!) only active, when allowed
- A big anonymity group: Firefox ESR users w/o JS and w/o cookies
- (+) highest privacy and security, home-grown!(-) a really, really bad user experience

=> Play around. Find you own compromise!