



# **CyberDragon Browser**

## **Quick Manual**

Second Fixed Draft.

# Tracker Blocker.

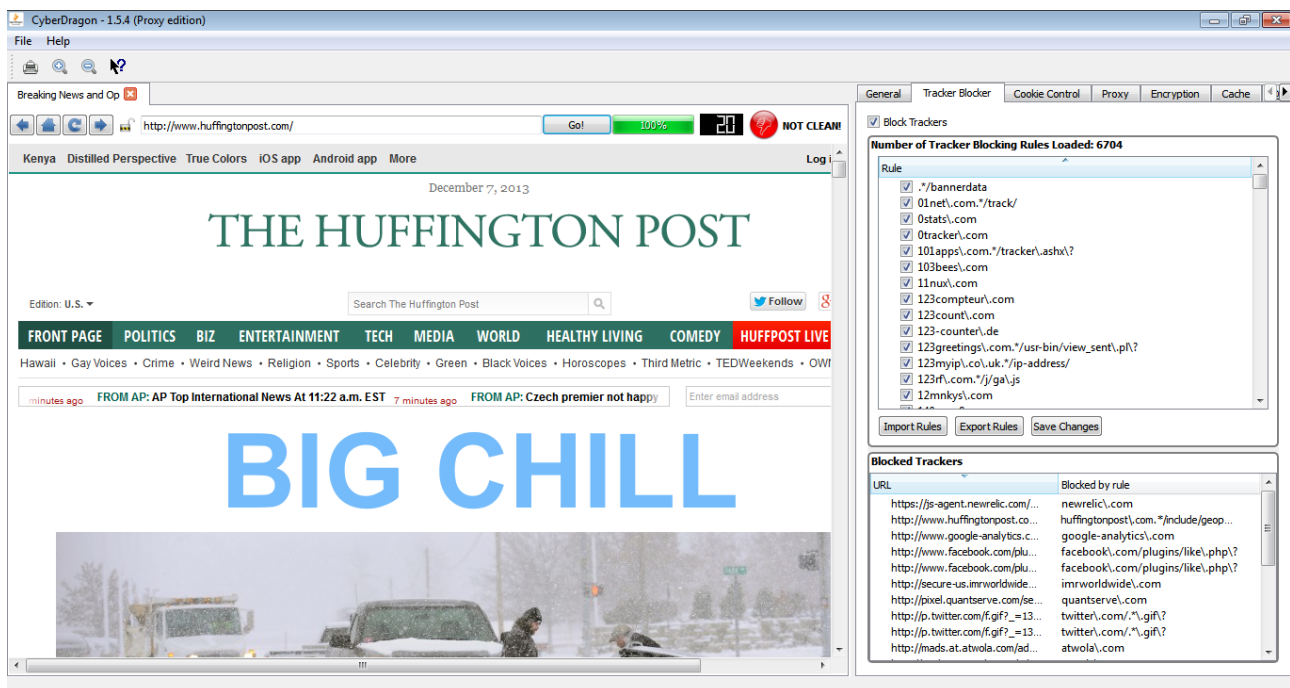
## Stop Tracking me Dammit!

Everytime you visit some site you will be silently and invisibly tracked by organisations, institutions, goverment agencies and most importantly companies. The reasons they track you varies from control to making just plain puck with your surfing habits. They invisibly and forcibly load your computer with unwanted and unneeded banners, scripts, widgets, advertising and other stuff, slowing your Internet connection, slowing your computer, invading your privacy, exposing you to security risks and most importantly making billions of dollars with your data.

Well, not anymore!

CyberDragon has built-in tracker blocker that let's you see who the trackers are and block them. It will let you to track the trackers!

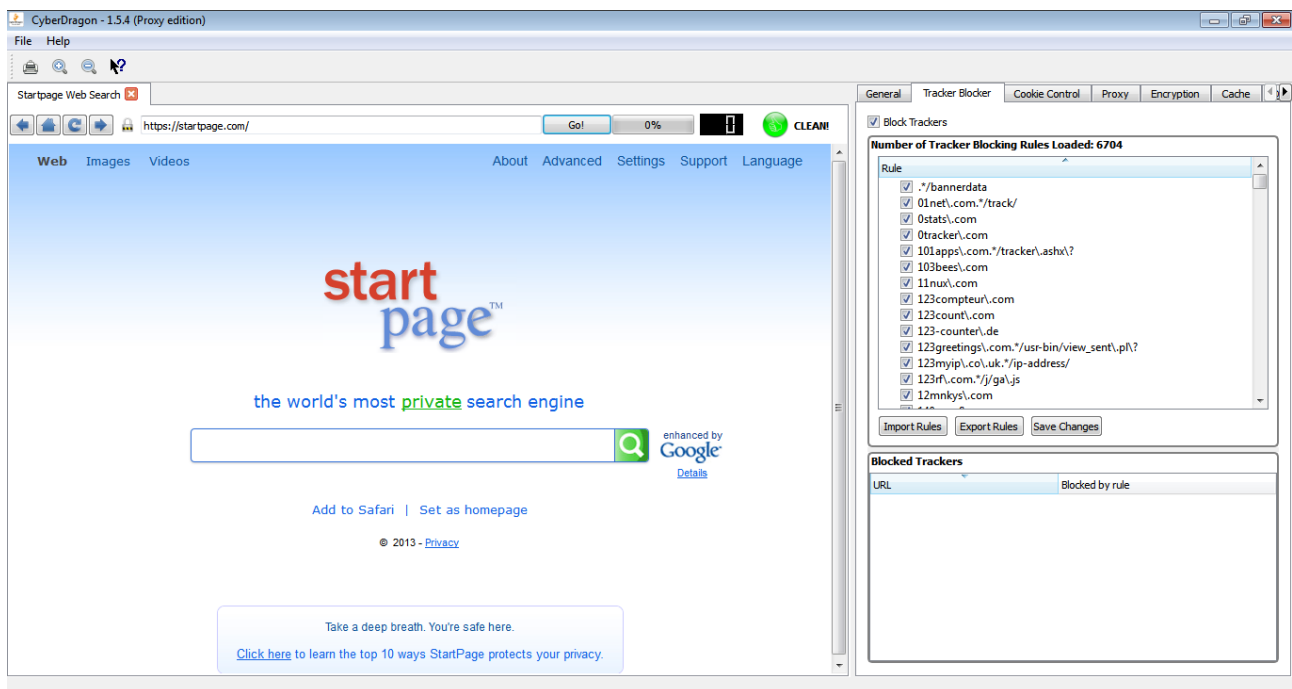
Heres where the magic happens.



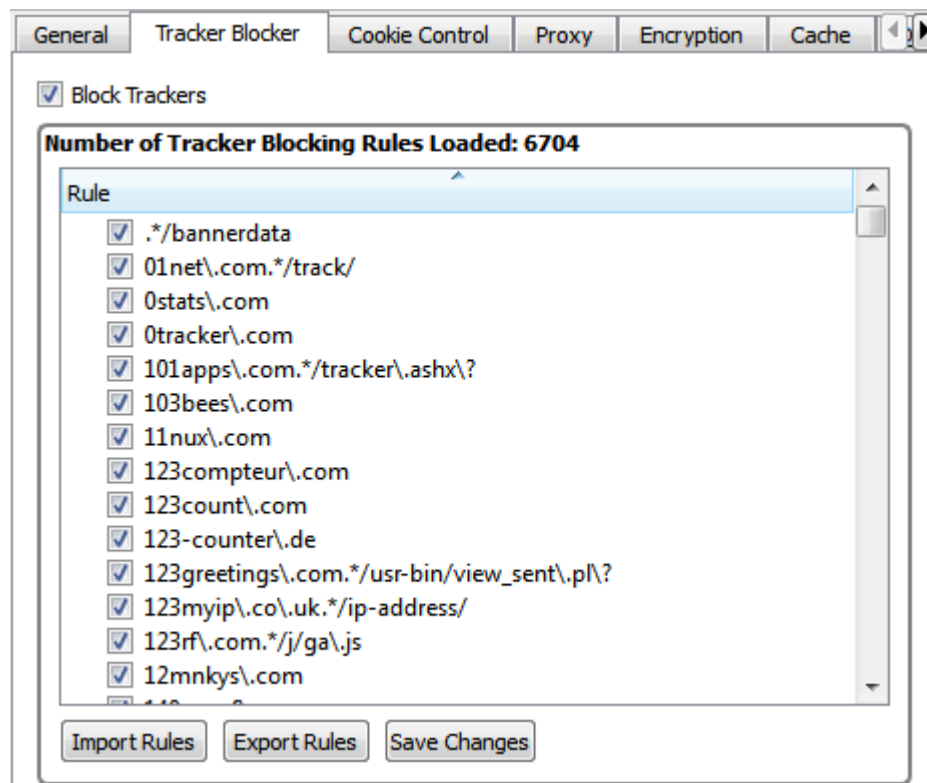


At the top right corner of the browser view you see how many trackers were found on this specific *page*. This number does not include any blocked cookies (more of that later), just the trackers that could be found. In addition to this numerical information it will also loudly tell you that this page was filthy by red orb with thumb down and message NOT CLEAN!

For sites that does not include any trackers (yes, there are those. For example: <https://startpage.com> ) it will show zero trackers and green orb with thumbs up and message CLEAN!



Then you have the master tracker blocker view that currently has over 6000 tracker blocker rules. And just below that you have the Blocked trackers view that will show you the bad guys URL and the rule that matched it. This is especially important to know because without knowing the correct tracker blocker rule you might not be able to disable it for temporarily.



Now why would you want to disable a tracker blocker rule? Even for temporarily? Well, you see, sometimes some sites use trackers as part of their functionality.

For example, YouTube comment feature uses tracker(s).

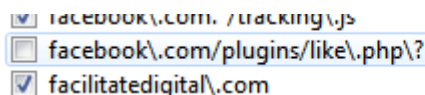
I don't currently remember the specific rule(s) but it might be the rules s\youtube\com and s2\youtube\com. In addition you might need to enable some cookies on Cookie Control tab and also check for blocked mixed content from Encryption tab. Lot's of trouble just for enabling YouTube video commenting .....

Or it might be that there is an actual legitame site that has ended up because of my mistake into that master tracker blocker rule list (Hey! Im a human being. And human beings make errors) and you need to disable it, or maybe even remove it.

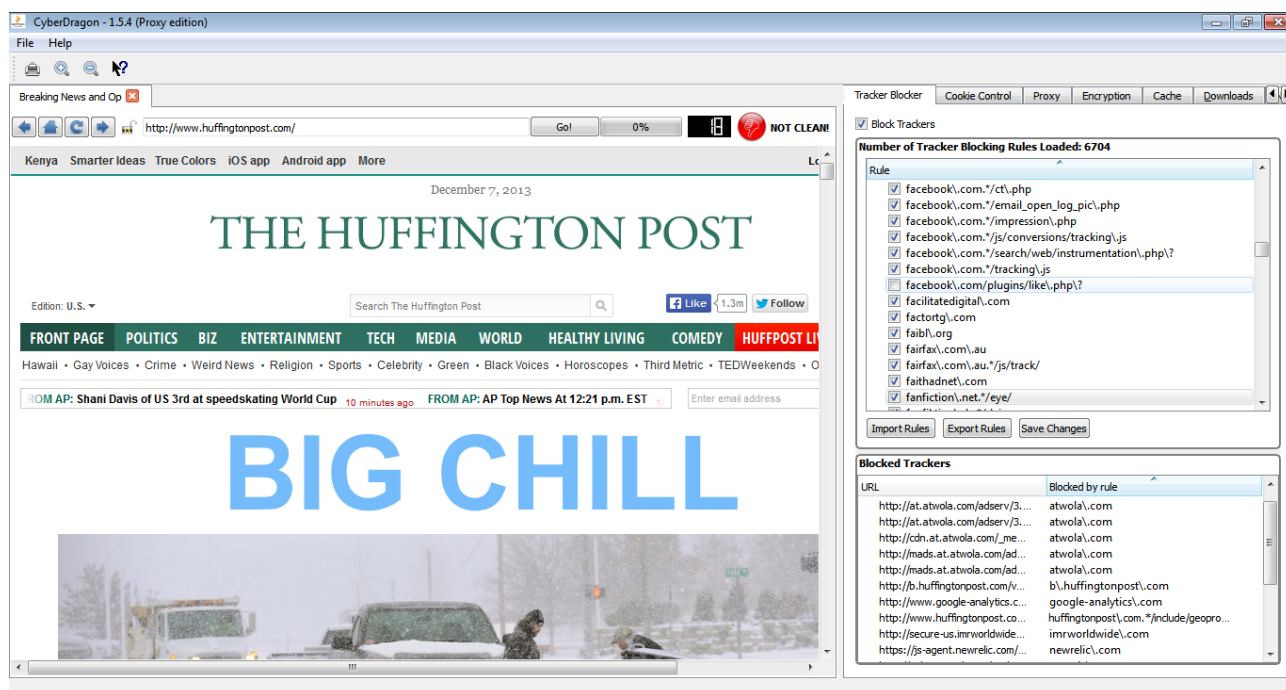
Let's go throught all the options you can do with this master blocker list.

## First: Disabling/Enabling Tracker Blocker Rule.

Like I told before you can temporarily disable/enable tracker blocker rule from the list by just clicking the checkbox in front of the rule. It might be that you want to just test if some rule is giving you trouble or not. Much easier than removing, testing, adding routine that you would have to do otherwise....

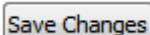


Let's temporarily disable facebook\.com/plugins/like\.php\? rule.



And then reload page. As you can see the tracker count is now 18 and you will also see facebook's like widget appearing this time. There is also no facebook\.com/plugins/like\.php\? appearing on Blocked Trackers view this time. Now that you have confirmed that tracker blocker works please enable facebook\.com/plugins/like\.php\? rule again.

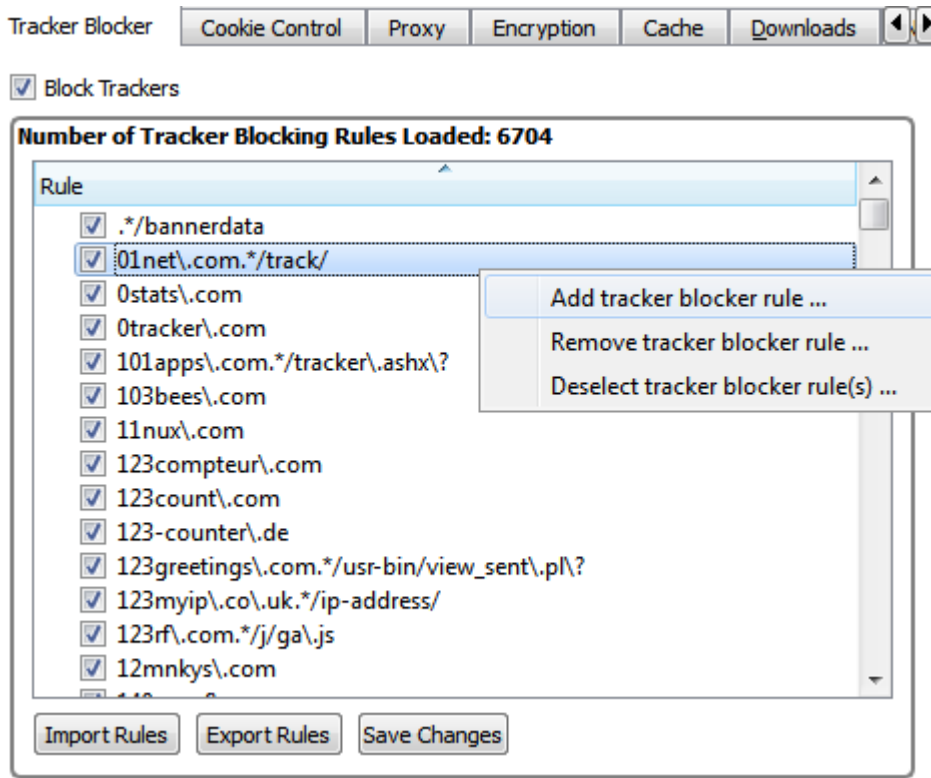
## Saving Changes



None of the operations, except disabling/enabling tracker rule and exporting rules to file, are saved without pressing this button. Because we are talking about master tracker blocker rule list here (the very thing that makes blocking those trackers possible) I have decided that you must confirm all the changes you make to it (importing, adding, changing and removing) permanent by pressing this button. Think it like as a last chance before there is no turning back in case you make a very serious mistake to the list (actually, there is hope even in that case: you can close the CyberDragon and manually edit file called **filters.txt** but you know how fun that is .... ). After you have pressed this button the CyberDragon will tell you what operation(s) you have made to master tracker blocker rule list.

## Adding completely new Tracker Blocker Rule.

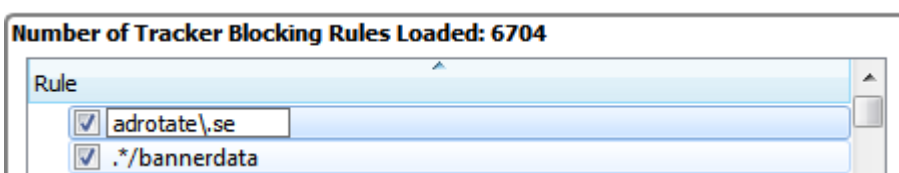
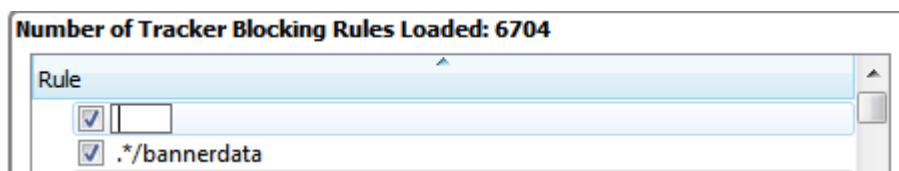
You can add completely new tracker blocker rule by right clicking with mouse over master tracker blocker list and selecting "Add Tracker Blocker Rule".



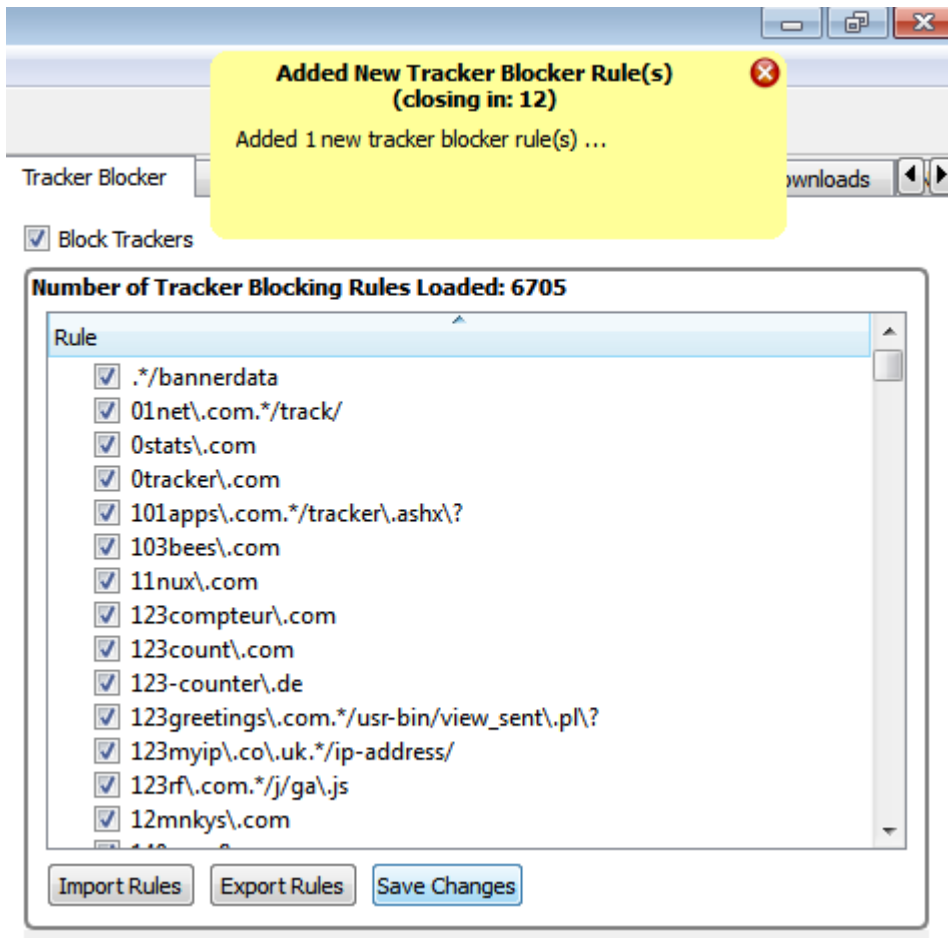
It will add a new empty field at the top of that 6000 list where you can type the name of the bad guys domain/subdomain or specific URL that points to some path or file. This list is automatically sorted so after you have pressed Enter it will put this new rule into its proper place, unless it is a duplicate rule.

Duplicates are silently discarded to keep this list as compact as possible. Empty fields, however, are currently not discarded. So be careful to not give any empty fields (they will end at the top of the list) and remove them!

Let's add a new rule that is missing from that list: adrotate.se



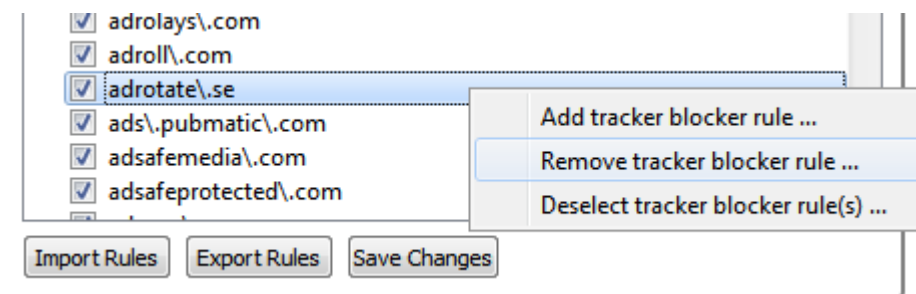
Press Enter and finally click "Save Changes"



As you can see CyberDragon will inform you that it has added new tracker blocker rule. If you had not pushed "Save Changes" button then all the changes you would have made so far with the master list would have disappeared at the exit of CyberDragon. Now remember, CyberDragon keeps this list sorted. So if you wonder where your brand new rule went just scroll down the list.

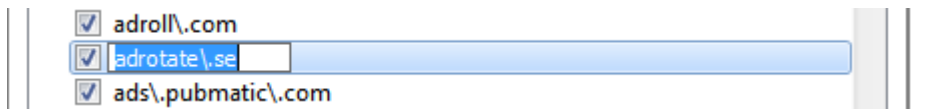
### Removing Tracker Blocker Rule.

Pretty simple. Just click the rule (or rules, you can press Shift + left mouse button or Ctrl + left mouse button to select multiple rules) that you want to remove and select "Remove tracker blocker rule" from context menu that pops up with right mouse click over master tracker blocker view.



## Changing Tracker Blocker Rule.

What? You found a mistake in master list? Okay. In that case just double-click on the rule that needs correction and press Enter-key.



## Importing Tracker Blocker Rule.

Import Rules

This is a much much much easier way of adding new tracker blocker rules (especially if you have lot's of them) than the method mentioned previously. Basically you make a normal text file which contains one rule at each line, click this button, select your file and press Ok. Your new rules will be merged to master rule list (duplicates and empty lines are skipped though...). When you are happy press "Save Changes" button. This is a great way to add and share rules with other CyberDragon users and keep the list up-to-date.

## Exporting rules.

Export Rules

And lastly, there is a way you can export rule(s) to an external text file (so that you can share them with your fellow CyberDragon users later). If you have not selected any specific rule(s) from the list then pressing this button will export the whole list (as does selecting one rule from the list, pressing Ctrl + A and then pushing Export button). If you want to export some specific rule(s) then press Shift + left mouse button (or Ctrl + left mouse button if you don't want continuous selection) and then press Export button.

Now you know all the functionality of the Tracker Blocker tab. However, one word about the format of those rules. Why they look so funny ? Why it reads s\youtube\com for example? Instead of just s.youtube.com ?

The reason is that they are regular expressions.

Regular expressions is too deep subject to handle here but I will give few quick examples.

Let's just say that they offer a way to make a very compact list of tracking rules if need to. For those interested please check the following links:

<http://perldoc.perl.org/perlretut.html>

<http://qt-project.org/doc/qt-5.0/qtcore/qregularexpression.html>

Characters dot (.), asterix (\*), question mark (?) and plus (+) have a special meaning in regular expressions. If you meant literal of those characters then you have to prefix them with '\' character.

- . = means any character.  
So example.com would be wrong. It would match exampleecom, example2com, exampleucom etc... Right domain match rule in this case would be example\com
- \* = means zero (0) or more occurrences of the character before it.  
So .\* means "zero or more occurrences of any character"



For example: `example.*\.com` would match `example.com`, `example12343.com`, `examplebaddomain.com` etc....

`example1*\.com` would match: `example.com`, `example1.com`, `example11.com`, `example111.com` etc...

`{m}` = Match exactly *m* characters before it. Rule `example\.{2}` would match `exmple.it`, `example.fr`, `example.jp`, etc..

Rule `exaple\.{3}` would match: `example.com`, `example.gov`, `example.edu` etc...

`{m,n}` = Match at least *m* but at most *n* characters before it.

Rule `example\.{2,3}` would match: `example.de`, `example.gov`, `example.fr`, `example.edu` etc...

`+` = means at least one (1) or more occurrences of the character before it.  
Rule `example+\.com` would match `example.com`, `examplee.com`, `exampleeeee.com` etc..

`[]` = Set of characters.

`|` = Alternative (OR operation)

And now the examples:

**Example 1:** There is a bad guy throwing targeted ads analyzing and profiling at fictitious domain `evilads.com`. We have rule `evilads\.com` in our list and it is blocking their crap nicely. Now, they suddenly registered three new domains: `evilads.fr`, `evilads.jp` and `evilads.de`.

Instead of adding three more rules for these rules we change the old rule to this:

`evilads\[com|fr|jp|de]+`

That `|` character means OR operation. So what this rule basically says is: "Match all domain names that include `evilads.` and that end with `com` OR `fr` OR `jp` OR `de`. All with just one line of rule! Without regular expressions we would have to write four rules (for `com`, `fr`, `jp` and `de`)!

**Example 2:** Bad guys at previous example went crazy and registered all the remaining tld domains for their name. Last time I checked, there were over 100+ tlds ... So instead of writing 100+ blocking rules we change our old rule to this: `evilads\.{2,3}`

Yes, just one rule that will block all their domains. That is basically: "Match all domain names that include `evilads.` and that has at least 2 character (like `de`, `fr`, `jp`, `gh` etc..) but at most 3 character (like `com`, `edu`, `mil` etc..) ending.

One rule. Over 100 matches.

By now I'm sure you have realized the power of regular expressions.

**Final note before we go to Cookie Control:** All Blocker Trackers views and the number of trackers blocked, are *tab specific*. That means, each tab handles its own tracking blocking, cookie blocking (next chapter) and mixed content blocking (last chapter).

Each tab is like a mini browser contained on its own private window (tab) with private network manager, private cookie control, private encryption control, 6 concurrent connections per tab (current Qtwebkit limitation) but shared disk cache (if enabled).

# Cookie Control.

## Crunshing Cookies



Network cookies are small text files that are stored on your computer hard drive by your browser each time you visit certain websites. The data they store about you in those cookie files is specific to server you have just connected and you have no control of it. Further, those sites could allow third parties to store even more cookies on your hard drive.

It's important to note that not *all* websites use cookies. There are cookie free sites and not all cookies are bad (although most of them are).

There are basically two uses and two types of cookies:

1. **Permanent cookies** (non-session cookies, tracking cookies)

These are cookies that are used to track you and have very rarely any other use. They are used by companies to track your surfing habits so that they can profile you and send you ads and make money. There are very very few cases where permanent cookies have valid usage.

Cookie usage: Tracking, selling ads and very rarely anything else.

2. **Session cookies**

These cookies have a lifetime only while you are logged into a certain service, like online bank, webmail or any other service that needs authentication. These type of cookies have valid usage. For example: without session cookies you would have to type your username and password each time over and over again when you browsed through your webmail. Session cookies will be destroyed after you have logged of the service.

Cookie usage: Making the many online services possible to use.

Traditionally, you would have very little control of what cookies to accept.

You could tell browser to either block all cookies (which is not really practical if you want to use Gmail, Yahoo, Facebook or even your online bank), allow all cookies (which would not be very smart, unless of course, you enjoy getting Viagra and diet ads into your mail) or something middle between.

We are interested of this middle ground.

With some browsers, you could further restrict cookies by blocking 3<sup>rd</sup> party cookies and maybe even allowing only session cookies. CyberDragon Browser goes even further with this protection. By default it will allow only cookies that are:

1. Secure.

Cookies that have **Secure** attribute set will be only sent through encrypted HTTPS connection. This will make hijacking your cookies with packet sniffers much much harder.

Sites that use authentication (like online banks) usually use Secure attribute with their cookies.

2. Safe.

Cookies that have **HttpOnly** attribute set will not be possible to access and manipulate with JavaScript scripting language. This restriction will mitigate (but not completely eliminate) XSS- (cross-site-scripting) attacks. Sadly few sites are setting their cookies with HttpOnly attribute.

Note that the name is a little bit of a misnomer: Cookies that have HttpOnly attribute set *can* be sent through HTTPS connections too, not just HTTP. Secure attribute and HttpOnly attribute do not exclude each other. HttpOnly attribute just means that don't allow any scripts to access cookies and Secure attribute means that only allow sending of cookies through HTTPS. Yeah, it's a bad name but I did not invent it.

Note: HttpOnly attribute makes sense only with session cookies (have to fix this on future CyberDragon version to only allow it when session cookies is checked ... )

3. Session cookies.

Obviously, because CyberDragon Browser is all about keeping your surfing habits out of advertisers and other groups, we don't want to allow non-session cookies that are permanently stored on your hard drive and then used to track you as long as you use that same computer.

4. Are not 3<sup>rd</sup> party cookies.

CyberDragon Browser will by default only allow cookies that come from the site you are visiting. Any other third party cookies are stopped.

These are good defaults and in a perfect world these would be all that is needed to surf without worrying advertisers and others while still using your favorite online service without a glitch.

Unfortunately, we don't live in a perfect world and not everyone sets their cookies correctly.

That's why we have to sometimes make an exception to this global cookie policy for specific cookies. Next: custom cookie rules!

Custom cookie rules will allow you to make an exception to global cookie policy you saw previously. This way you can make an online service that is ... ahem... broken less broken.

What you are basically telling CyberDragon is that: "Hey, if you see this cookie do this and just skip the global cookie settings, okay?". And CyberDragon will comply, either accepting or blocking cookie, depending what you set it to do.

These custom cookie rules are matched based on three criterias:

- First match the domain (or subdomain) of the cookie against the custom cookie rule.
- If the first test passed then match the path of the cookie against the custom cookie rule.
- Thirdly, if the second test passed too then match the cookie name-value pair against custom cookie rule.
- Lastly, if the third and final test was passed then proceed with the action user had set on this specific custom cookie rule, either by allowing it or blocking it.

And that's basically it. All the three fields: domain, path and name-value pair are regular expressions (take a look at previous chapter if you have already forgotted what they are) and with them you can make very powerfull cookie rules.

**Important Note:** The order of the rules is important!

For example: If you want to allow all cookies from yahoo.com *except* ads.yahoo.com then you *must* put the rule that blocks ads.yahoo.com first, before rule that allows yahoo.com.

The reason is that the custom cookie rule checking will stop checking immediately after it has met first rule that matches. Also note that there is no need to set any cookie attributes like Secure or HttpOnly on custom cookie rules. We are only interested of the domain (or subdomain), path and name-value pair of cookie and act accordingly.

Next: Cookie Control tab explained in detail.

This is where all the magic happens.



First you have global cookie settings. As you can see the settings are pretty self-explanatory.

**Global Cookie Settings**

- ☐ Allow 3rd party cookies (recommended value: off)
- ☒ Session cookies only (recommended value: on)
- ☒ Cookies with HttpOnly attribute set (recommended value: on)
- ☒ Cookies with Secure attribute set (recommended value: on)

After that you have custom cookie rules view where you can define your own cookie rules to either allow or block specific cookie(s).

Custom Cookie Rules				
Action	Domain	Path	Name-Value	
✓	\\.yahoo\\.com	/	__uvt=.*	
✓	accounts\\.goog...	.*	.*	
✓	mail\\.google\\.c...	.*	.*	
✓	.startpage.com	/	.*	
✗	mail\\.yahoo\\.c...	.*	.*	
✓	\\.yahoo\\.com	/	T=.*	
✓	ucs\\.query\\.yah...	/v1/console/	X-AC=.*	
✓	\\.yahoo\\.com	/	Y=.*	
✓	\\.yahoo\\.com	/	SSL=.*	

The buttons at the left side of custom cookie views are, from top to bottom: add custom cookie rule, remove custom cookie rule, move custom cookie rule up, move custom cookie rule down. These options are also available through context menu that you get when you right click on custom cookie rule view.

### Allowing/Blocking cookie

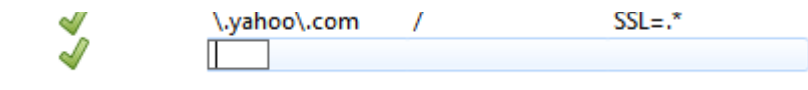
Pretty simple. Just click the icon on the left to either allow or block.



### Add custom cookie rule



When you select add custom cookie rule (by either pushing the button or selecting it from context menu) a new empty field will appear at the bottom of the custom cookie view. Double-clicking on the field will allow you to edit it.



There you must add the three required values: domain/subdomain, path (usually just '/' or maybe even '.\*' if you want to be very lax) and name-value pair. It is recommended that you fill this last part as *name=.\** at first, unless there is a specific need for exact match.

For example: If the name-value pair looks like some kind of user ID, like *SID=235353534*, then it should be written like this *SID=.\** because it is very unlikely that the value will be the same again the last time. Next time you try to log the same server it could send you a cookie with name-value pair as *SID=676868767* and it would not match the rule!

So look carefully what the server sends you from the Cookie List view and construct your rules accordingly. After you are happy with the rule click its Allow/Block icon and you are ready! However, if you have several rules for the same domain/subdomain where some rules block and some rules allow cookies then remember to check the order of the rules (like I told previously).

This was The Hard Manual Way™, of adding completely new cookie rule. There is a better, easier way but we don't get there just yet. Keep reading ...

### Remove custom cookie rule



This is really simple! Just click the rule (or rules, you can select several rules with pressing Shift or Ctrl down with one hand and clicking with left mouse button on other. Also, Ctrl + A will select all rules if that's what you want) and press remove custom cookie rules button (or select it from context menu that will pop up when you right mouse click custom cookie view)

## Move custom cookie rule up



Also simplicity in itself. Select rule (can only move one rule at the time currently) and push Move custom cookie rule up or select it from menu.


## Move custom cookie rule down



Same as above but obviously to another direction ...

## Cookie List

And lastly there is an live view of cookies that the server/site you are connected with tried to ram through your throat.

 ☒ Clear Cookie List on page load Clear Cookie List

Time	Action	Domain	Path	Name
la 7. joulu 2...	Blocked	.huffingtonpost...	/	snn_p
la 7. joulu 2...	Blocked	.huffingtonpost...	/	chec
la 7. joulu 2...	Blocked	.huffingtonpost...	/	sailth
la 7. joulu 2...	Blocked	.google.com	/	NID=
la 7. joulu 2...	Blocked	.twitter.com	/	guest
la 7. joulu 2...	Blocked	.twitter.com	/	guest
la 7. joulu 2...	Blocked	.google.com	/	NID=
la 7. joulu 2...	Blocked	.twitter.com	/	guest
la 7. ioulu 2...	Blocked	.aooale.com	/	NID=

What you see is the very live cookies that tried to sneak into your computer while you visited some site. For each cookie the following info is told: Time when it tried to invade your privacy, action CyberDragon took depending of either global cookie settings or custom cookie rules (custom cookie rules are always checked first, before global settings!), the domain/subdomain that the cookie belongs to, cookie path, cookie name-value pair, cookies expiration time (if it has time then it's permanent cookie, if it's empty then it's session cookie), if the cookie has Secure attribute set and if the cookie has HttpOnly attribute set.

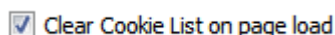
This view is automatically sorted based on time of cookie arrival but you can sort it anyway you like (just click the header for your sorting criteria). Also there are three controls: Move cookie rules up, Clear cookies on each page load and Clear cookie list.

## Move cookie rules up



This is the easy way how to add new custom cookie rules that I told you before. Just select the cookie (or cookies with Shift + left mouse or Ctrl + left mouse) that you want to add to custom cookie rule view and press Move up button (or select it from context menu with right click on Cookie List view). Your new cookie rules appear on custom cookie view where you can allow/block, edit, remove and move up/down them just like I previously told you. This way you don't have to do tiresome typing of all those rules and can only concentrate of allowing/blocking and possibly, editing/fine tuning the rules.

## Clear Cookie List on page load



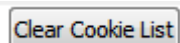
What this little checkbox basically does is that it tells CyberDragon to clear the Cookie List view everytime the URL changes (that is, each time there is an new page load). Without this option your Cookie List view would gather tons of cookies over time while you are surfing. So it is recommended that you keep this enabled always *except* in one case, logging the very first time to some online service that you have not visited before with CyberDragon.

The reason is simple: Most online services redirect user from login page to some other page where the actual authentication process is done. There that page quickly checks what cookies your browser send to it and then further send you to either to your proper place or rudely slams error page telling you that you have not enabled cookies. So if you have *Clear cookies on each page load* checked you have about few milliseconds time to see the cookies that were blocked by the actual authentication page !!! (remember, this option clears cookie list view with *each* page load, not just user typing www-address and pressing Go! button or clicking some hyperlink ...)

So for this reason, for very first time, you should *disable* *Clear cookies on each page load* option so that you can actually see what cookies were tried to send to you, in time order, and blocked. That's the only way you can see them and add them to custom cookie rules view (like previously told).

After you have added the right cookierules and set them to allow and confirmed that you can login successfully you can then check *Clear cookies on each page load* option back again.

## Clear cookie list



Over the time, *if* you have *Clear cookies on each page load* unchecked, your cookie list view will gather tons and tons of blocked (and maybe few allowed, depending of your settings) cookies. To clear this list you can push this button.

Also remember, this will only clear cookie *list* view for the *currently open tab*, not for any other open tabs. *It will also **not clear any cookies from memory** that have already been previously allowed and set.*

There is also not yet any "Clear all cookies" button but CyberDragon can manage just fine without it because no cookies, session or non-session, are ever stored permanently when CyberDragon exits. So it will always be cookie clean at next startup. This is a feature not a bug.

This ends the cookies chapter. Next stop: Encryption.



# Encryption.

## Keeping your data safe



Encryption is important. Without it all your data is like postcard, everyone can see it. Like all other browsers CyberDragon supports the standard HTTPS encryption. However, at this time, there is not much control of the browser settings of this HTTPS encryption. Currently the only option is to block mixed content (but I will add some more encryption specific features later).



### What is mixed content?

Normally, when you visit encrypted site (like your online bank or let's say <https://startpage.com>) you will see https:// in front of the page address and also that small padlock icon will close (and if you put mouse over it an tooltip will appear after few secs. and say Encrypted). This will tell you that you have just entered HTTPS encrypted site and you are safe and nobody can see what you are doing.

That's not the whole story though. You see, even though the *site itself is HTTPS encrypted*, there might be some third party content that is delivered to that page via unencrypted HTTP protocol (via http:// links). The content could be images, style sheets, scripts, whatever...

This poses a privacy (they can see from what IP-address you loaded they stuff and also send cookies. Or at least try sending cookies ... :-)) and possible security risk (if the target of http:// links is malicious JavaScript for example) for the user visiting such site.

For these reasons CyberDragon will by default block any http:// content that tries to sneak into an https:// protected site.

However, sometimes, for a proper working of the site, exceptions must be made.

In the case of encrypted search engines (like <https://startpage.com>) or with webmail (like gmail or yahoo) or with just badly coded webpages where links were absolute instead of relative.

In those cases a rule must be made that will tell CyberDragon: "Hey! Don't use mixed content blocking for this domain/subdomain or page). Without this list of you could not visit any http:// links for example if you would be searching through <https://startpage.com>

☒ Block mixed content



Allowed mixed content URLs



- ☒ startpage\.
- ☒ login\.
- ☒ encrypted\.
- ☒ duckduckgo\.
- ☒ accounts\.

Let's disable rule for startpage.com temporarily, go to <https://startpage.com>, search something and try accessing some of the http:// links and see what happens.

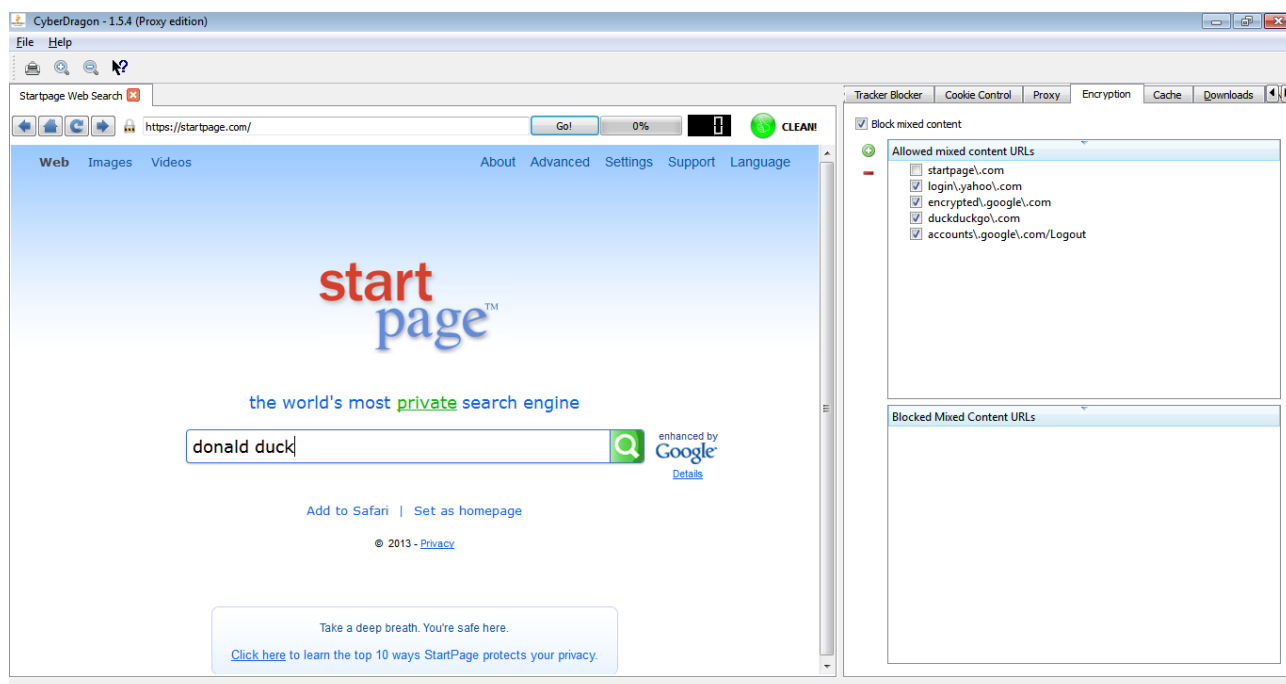
☒ Block mixed content

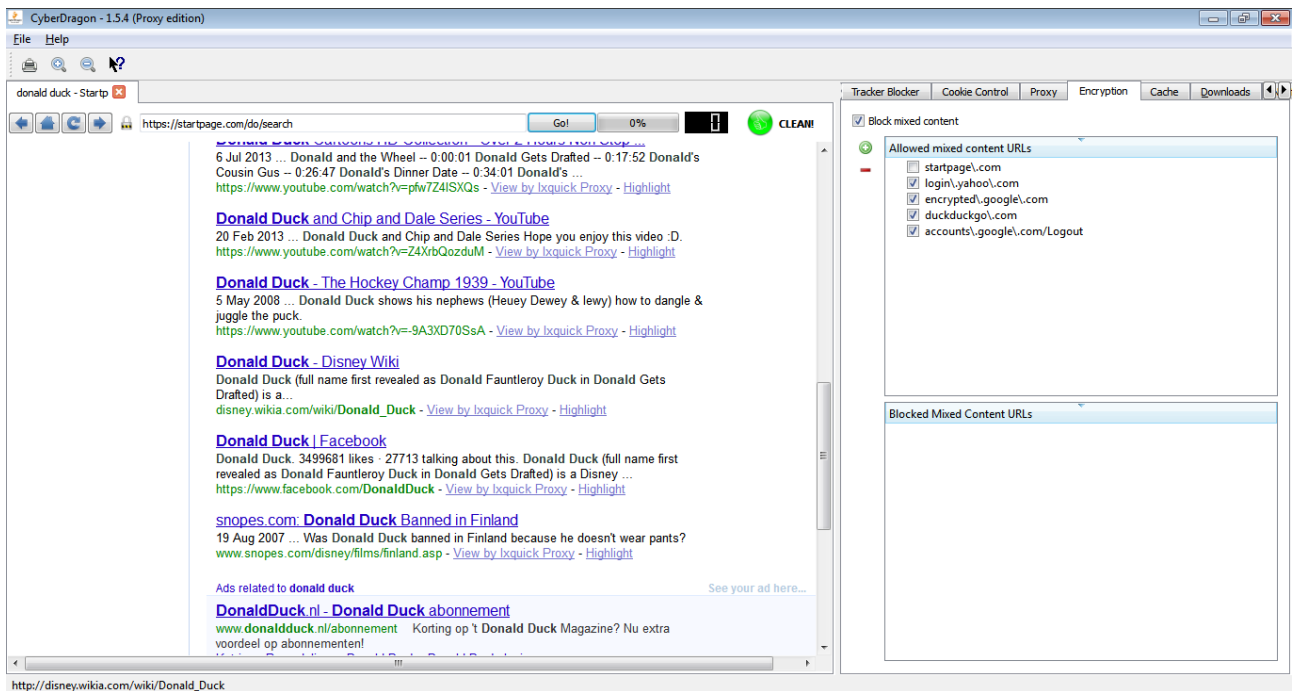


Allowed mixed content URLs

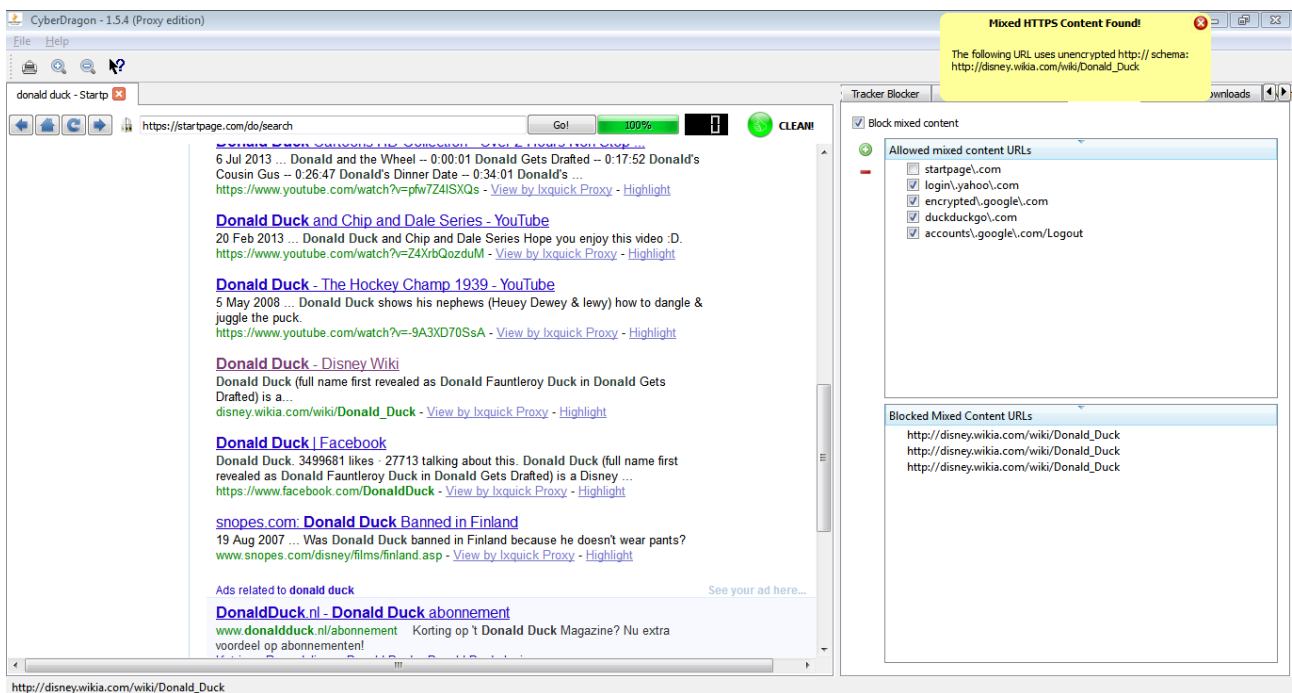


- ☐ startpage\.
- ☒ login\.



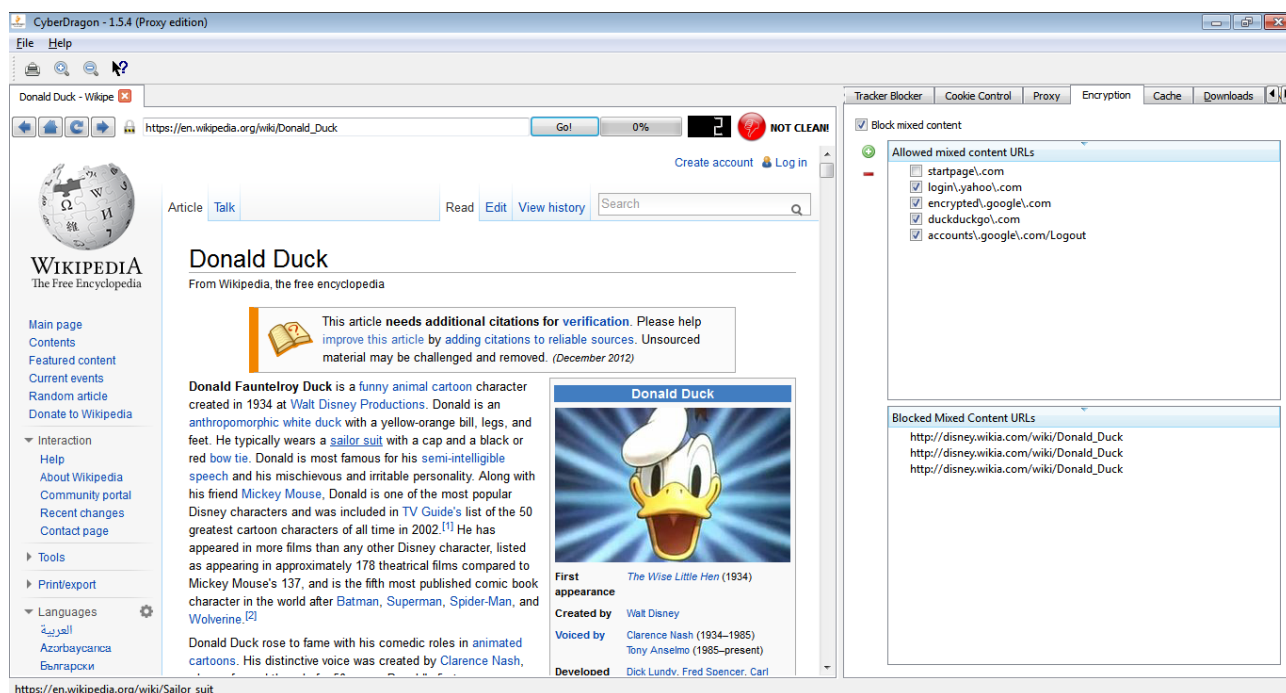


And CyberDragon would complain loudly and show the http:// link that tried to sneak through https:// protected site.



As you can see from the bottom of statusbar and from the Blocked Mixed Content URLs view, the blocked link was [http://disney.wikia.com/wiki/Donald\\_Duck](http://disney.wikia.com/wiki/Donald_Duck)

Any https:// links however would open just fine.



## Adding mixed content URLs



The adding and removing of these rules is very simple.

For adding an exception just click "Add mixed content URL" and start typing. Remember: This must be the https:// site or page that needs to allow unencrypted content. Not the blocked content address itself! Also, leave the https:// out of the rule name.

You can also temporarily disable/enabled the rule whenever you wish by clicking the checkbox in front of the rule.

## Removing mixed content URLs

For removing the rule, select it from the list and press "Remove mixed content URL".



As with Tracker Blocker, and Cookie Control, the Encryption Blocked Mixed Content URLs view is specific to that particular open tab.

This ends this very quick and crude manual. I try to make better at 1.5.5 version when I have better time.

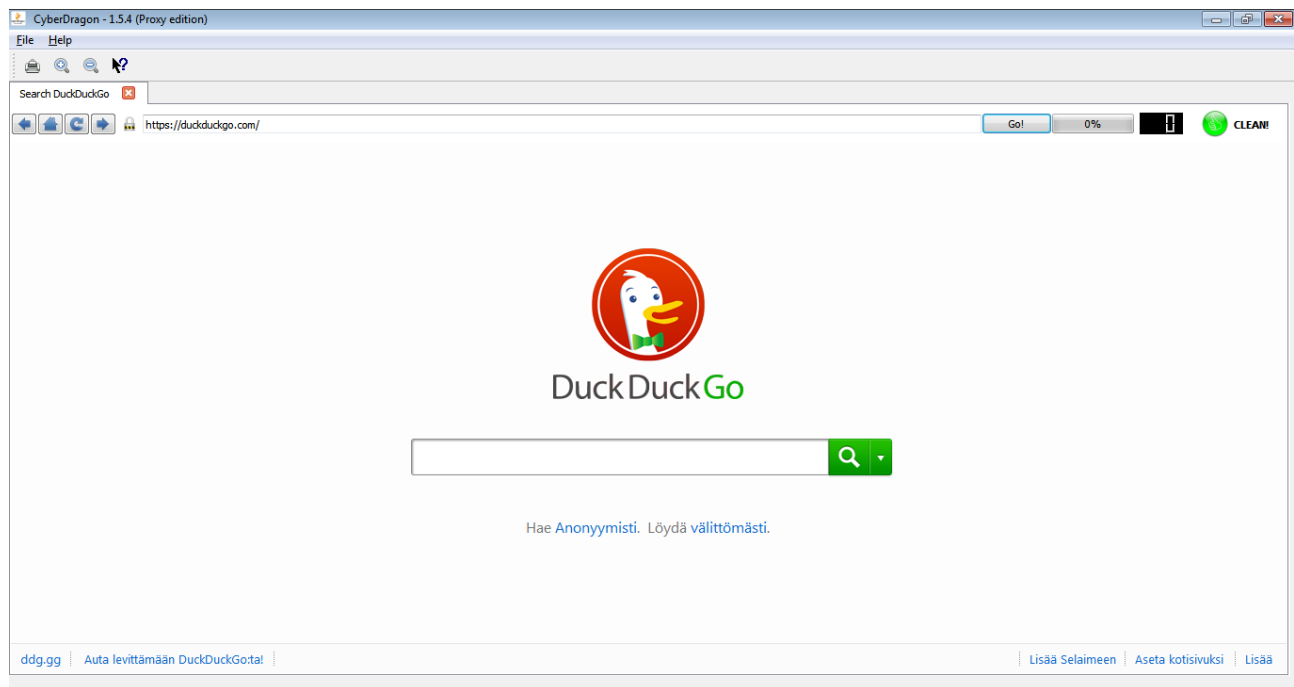
As this is one man show, my time is very limited but I try to fix all the bugs remaining as fast as I can find them and You can find them.

Any corrections, bugs or typos about this manual (I made this hastily within 4 hours, without native English skill) are wellcome to <http://www.binarytouch.com/contact.php>

And donations are wellcome to <http://www.binarytouch.com/windows.htm>

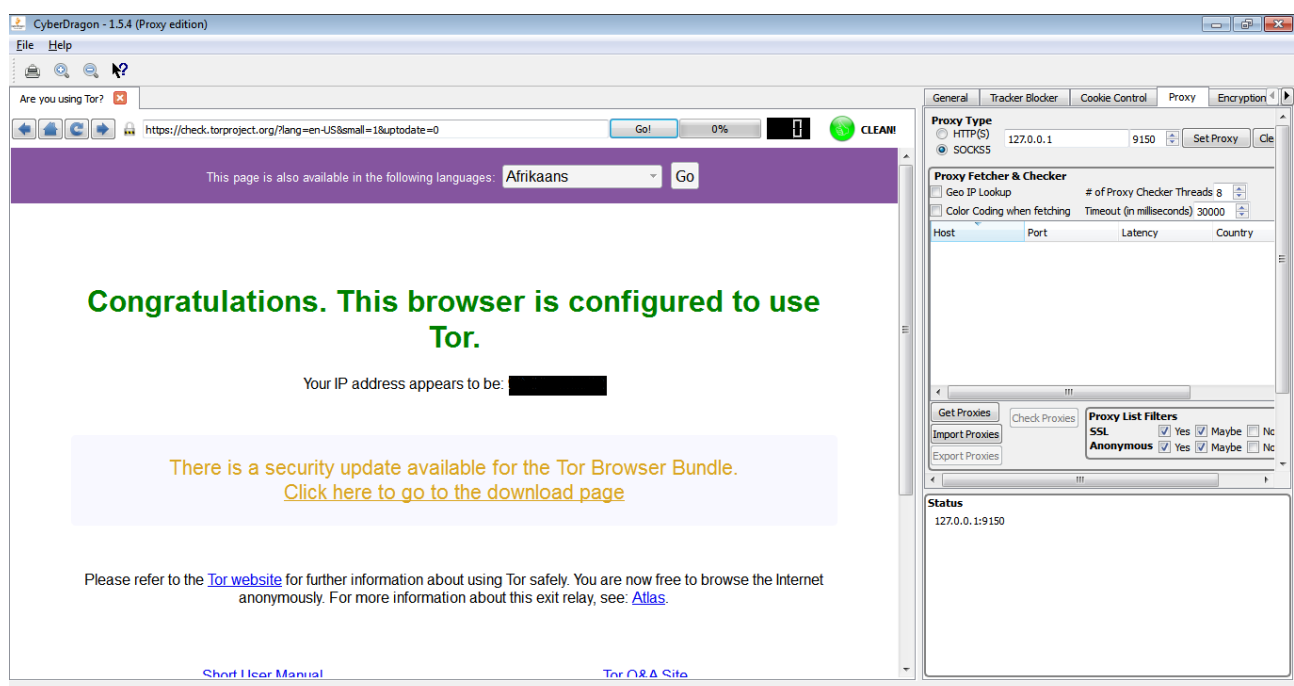
## What to expect in next manual ....

### Overview of the General Settings...



(You can surf in full mode view. Just drag the splitter to the right to hide settings)

## Proxy stuff ....



(You can use Tor with CyberDragon)

## Key shortcuts

Ctrl + P	Print current tab
Ctrl + T	Open new tab
Ctrl + W	Close current tab
Ctrl + +	Zoom in current page
Ctrl + -	Zoom out current page
F5	Reload current tab
F6	Switch between web page and URL bar
Backspace	Go forward in page history
Shift + Backspace	Go backward in page history
Alt + D	Go to Downloads tab