Comparison with other tools

The functionality of Haketilo partially overlaps with that of other programs. None of those, however, seemed to aim for exactly the goals of Haketilo when the decision to start its development was made.

LibreJS

Of existing tools LibreJS seems to be the only one with a software-freedom-oriented goal. It is a browser extension which inspects sites' scripts in search of license notices in a specified format. If it decides a given script is libre software or otherwise trivial, it allows it to run.

While LibreJS shares many of its social aims with Haketilo, its scope is different. At the time of this writing it facilitates script blocking (and not replacement or injection) on HTTP(s) pages in Mozilla-derived browsers.

More fundamentally, there is also a difference in the underlying assumptions about webmasters. Haketilo takes an adverserial view, refusing to trust or expect co-operation by default. LibreJS more charitably gives webmasters greater freedom to choose what scripts run in users' browsers. This happens at the cost of more burdensome requirement of maintaining license notice in scripts that are use on website. It should be noted that Haketilo's script blocking can be disabled, allowing for example LibreJS to be used for script blocking instead.

NoScript

NoScript is an extension often used as a content blocker. However, it actually does a bit more and is more properly described as a security suite. It can be used to block scripts on per-site basis and works with both Firefox- and Chromium-derived browsers. NoScript author, Giorgio Maone, has also worked on LibreJS as an FSF contractor.

NoScript, while sometimes useful for the task of blocking nonfree JavaScript, is not by itself fully freedom-oriented and for example has youtube.com in its default site whitelist.

uBlock Origin

Often abbreviated as "UBO", uBlock Origin is a selective content blocker. It gives quite fine-grained control over what kinds of elements are allowed to load, including the possibility of blocking third-party resources on a per-domain basis. Firefox and Chrome and at least 2 proprietary browsers are supported.

UBO is able to load and apply adware and spyware blacklists from several sources which makes it able to function as an ad-blocker. However, what's also relevant for people who want to hack on the software they use, is that UBO's codebase - although big - is rather clean and readable.

uMatrix

The uMatrix extension is UBO's twin. Developed by the same author, these 2 share part of their codebase. While UBO can be used rather easily, uMatrix was a content blocker aimed at more advanced users.

Greasemonkey

The tools discussed so far have all been content blockers. Greasemonkey, on the other hand, makes it possible to execute custom scripts on websites. These are usually referred to as "user scripts" and there are even sites (well, at least one) for sharing these between users. Greasemonkey only supports Firefox-derived browsers.

People often point at Greasemonkey as a possible solution when told about the need for a facility to replace sites' native JavaScript. Indeed, Greasemonkey could be used to achieve that. The fact that it doesn't block the original scripts is a small problem which gives the necessity of running some content blocker next to it. While generally suboptimal, this setup would be acceptable as a temporary solution to Haketilo's primary goal.

At the time of writing Greasemonkey doesn't execute user scripts in the context of a page but rather in the more privileged context of WebExtensions content scripts[1]. This might change with policy changes to extension stores[2]. The current approach brings in security issues, although largely mitigated by the use of sandbox. There might also be incompatibilities with scripts failing to execute the way they would in the usual context. These incompatibilities could possibly also be bypassed in some way.

Site's CSP rules cause yet another possible issue when customizing pages using Greasemonkey[3]. In some cases they may block custom injected elements like <script>s and <img>s.

ViolentMonkey

ViolentMonkey is similar to and largely compatible with Greasemonkey, with the benefit of supporting a wide range of browsers. All other potential issues listed for Greasemonkey still apply, however.

JShelter

JShelter improves browser security and privacy mainly by wrapping potentially dangerous browser APIs. It's not a content blocker nor a user script manager. Although it doesn't prevent proprietary JavaScript from running, it does greatly reduce its harm. It supports Firefox, Chrome, and Opera.

Hypothesis

Hypothesis project offers facility for community-driven annotating of web sites. This idea is similar to one of Haketilo's desired use-cases and it's even possible that Haketilo will, at some point, support Hypothesis annotations. However, the general goals of these project are different.

Woob

Woob tool implements graphical (QT) interfaces and programming APIs for various websites in Python programming language. It succeeds in achieving some of the goals we set in front of Haketilo. The main difference is that our project sticks to the usual technological stack of the Web (which has both good and bad sides) and also covers creations of a repository that can allow for greater scalability.

---

1. https://github.com/greasemonkey/greasemonkey/blob/efd22a93121225ada47f2fe9f021af0ab6100c21/src/bg/execute.js#L20 ↩
2. https://developer.chrome.com/docs/extensions/mv3/intro/mv3-overview/#remotely-hosted-code ↩
3. https://github.com/greasemonkey/greasemonkey/issues/2046 ↩