

The interactive HTTP proxy WebScarab – Installation and basic use

Author: Dr. Holger Peine, Fraunhofer IESE
Holger.Peine@iese.fraunhofer.de

To actively participate in the hands-on exercises of the tutorial, you need to install the software tool WebScarab on your computer. You can also follow the tutorial without this by watching the instructor demonstrate the solution to each exercise, but remember the (alleged?) Chinese proverb:

„I hear – and I forget; I see – and I remember; I do – and I understand!“

This text will explain in detail how to install and use WebScarab. While the explanation will use the Windows operating system as an example, WebScarab will also run under Linux, MacOS X or any other operating system supporting Java.

One more thing: Please don't let the number of pages of this instruction intimidate you: Everything is explained in all detail and nearly every step is illustrated by screen shots, which of course makes the number of pages grow considerably. Nevertheless, all steps are very common, and you should be able to complete the whole procedure in about 15-20 minutes. If you need any help, please email the author under his address above.

Java Installation

WebScarab needs Java to execute (JRE is sufficient, JDK not necessary) in any version not older than 1.4. Many computers will already have this installed; if this is the case with your computer can be checked in Control Panel / Add or Remove Programs.

If you don't have Java already installed, you can download the current JRE here:

<http://java.sun.com/javase/downloads/index.jsp> ; please choose „Java Runtime Environment (JRE) 6.0 Update *n*“ (click „Download“); click the radiobutton “Accept License Agreement“ and choose your operating system on the resulting page (e.g. „Windows Platform - J2SE(TM) Runtime Environment 6.0 Update *n*“) and choose „Windows Offline Installation, Multi-language“ (although the online installation should work as well).

Download WebScarab

You should find the WebScarab software for download somewhere on the ACSAC pages (probably close to description of this tutorial); if so, please download it from there, and proceed to the installation section. If for some reason you cannot download from the ACSAC pages, you can download WebScarab from its home page at http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project or you can also go to the download page directly: http://sourceforge.net/project/showfiles.php?group_id=64424&package_id=61823 . Please download WebScarab from this page by choosing the file webscarab-installer-20070504-1631.jar:

Package	Release (date)	Filename	Size (bytes)	Downloads	Architecture	Type
WebScarab						
Latest  20070504-1631  (2007-05-04 15:27)						
		webscarab-installer-20070504-1631.jar 	4949451	8679	Platform-Independent	.jar
		webscarab-selfcontained-20070504-1631.jar 	3024410	2914	Platform-Independent	.jar
		webscarab-src-20070504-1631.zip 	1834953	2470	Platform-Independent	Source .zip
<hr/>						
	 20060718-1904  (2006-07-18 10:19)					
	 20060621-0003  (2006-06-21 10:16)					
	 20051017-2127  (2005-10-17 12:50)					
	 20051012-0736  (2005-10-11 22:51)					
	 20050620-1046  (2005-06-20 07:09)					
<hr/>						
Totals:	6	18	48581066	91205		

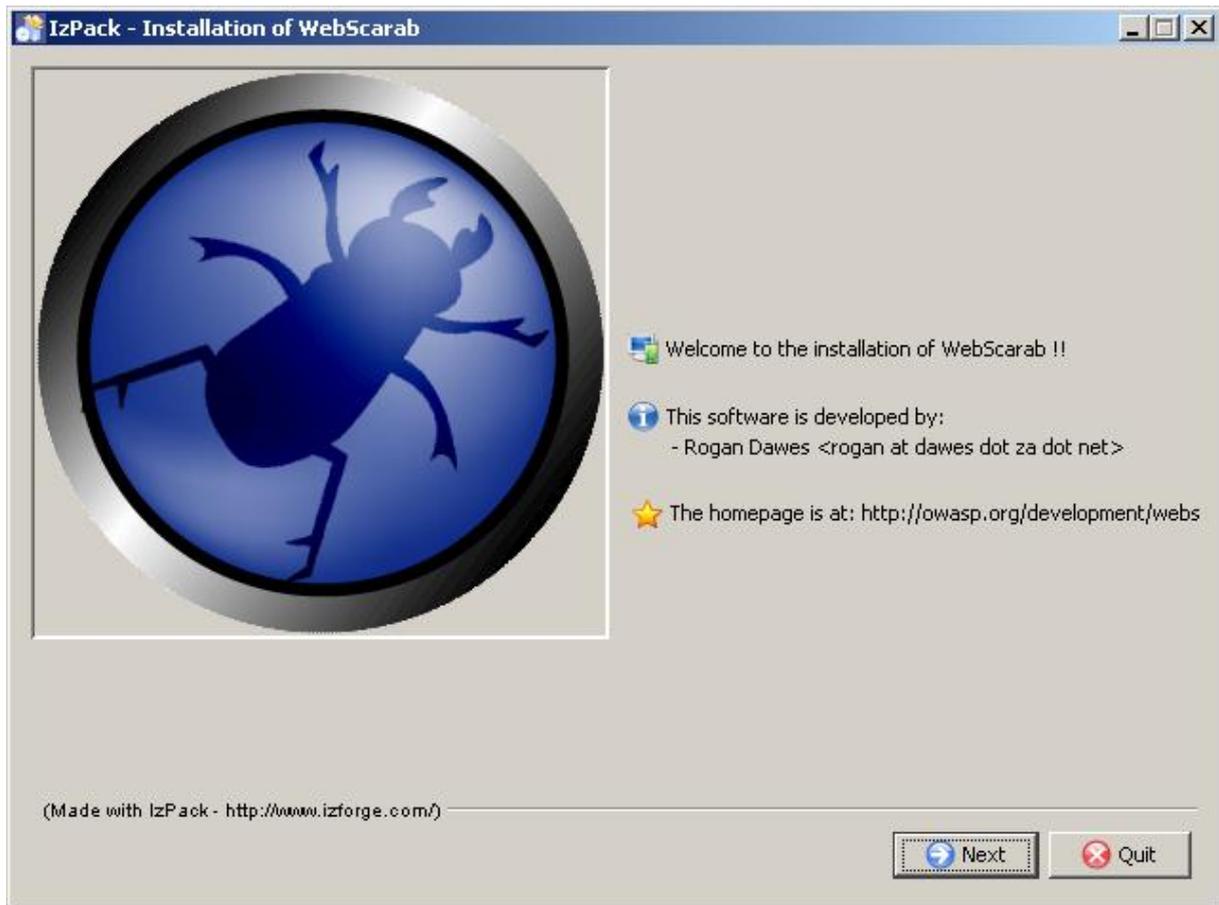
Clicking on that file name may or may not lead you to an intermediate page where you can choose one of a list of file server mirrors (or where one is chosen automatically for you).

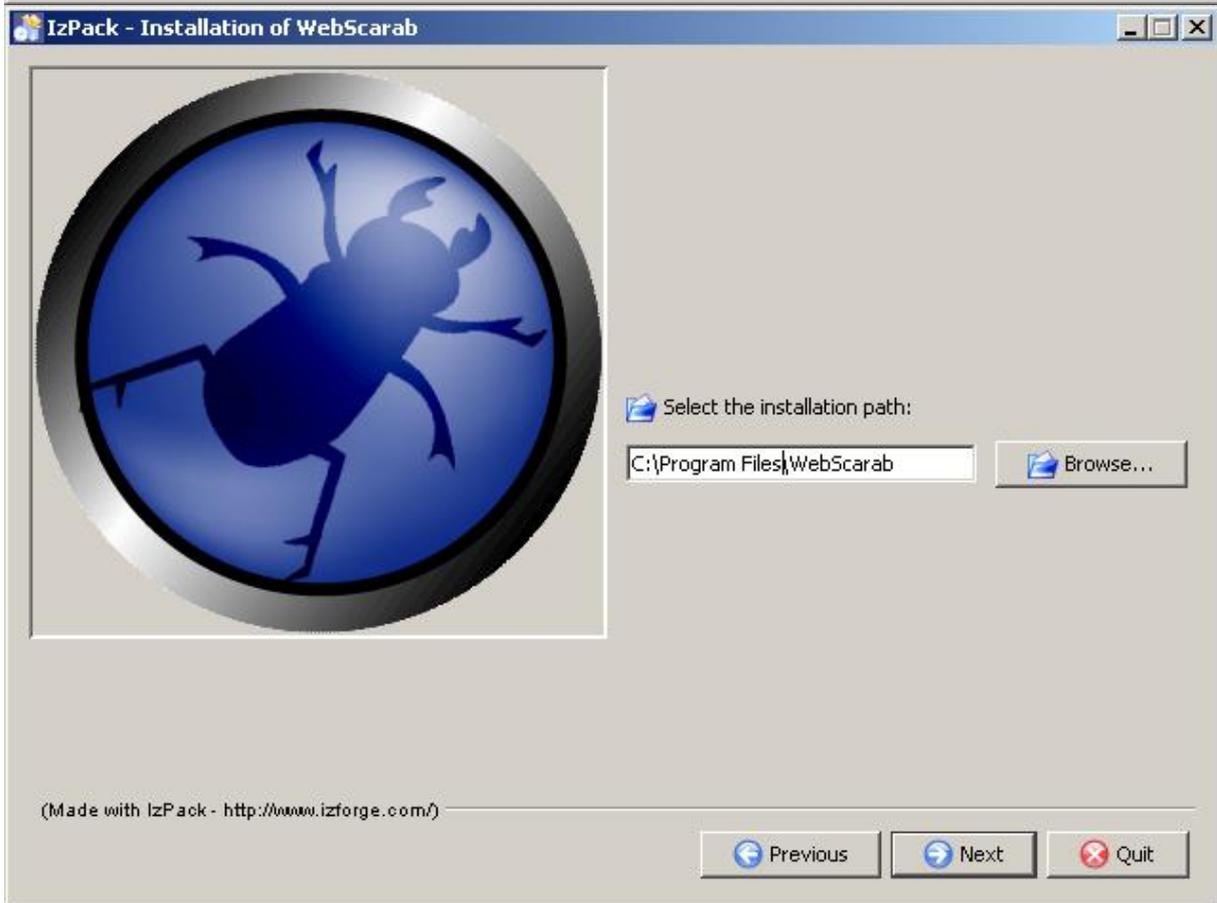
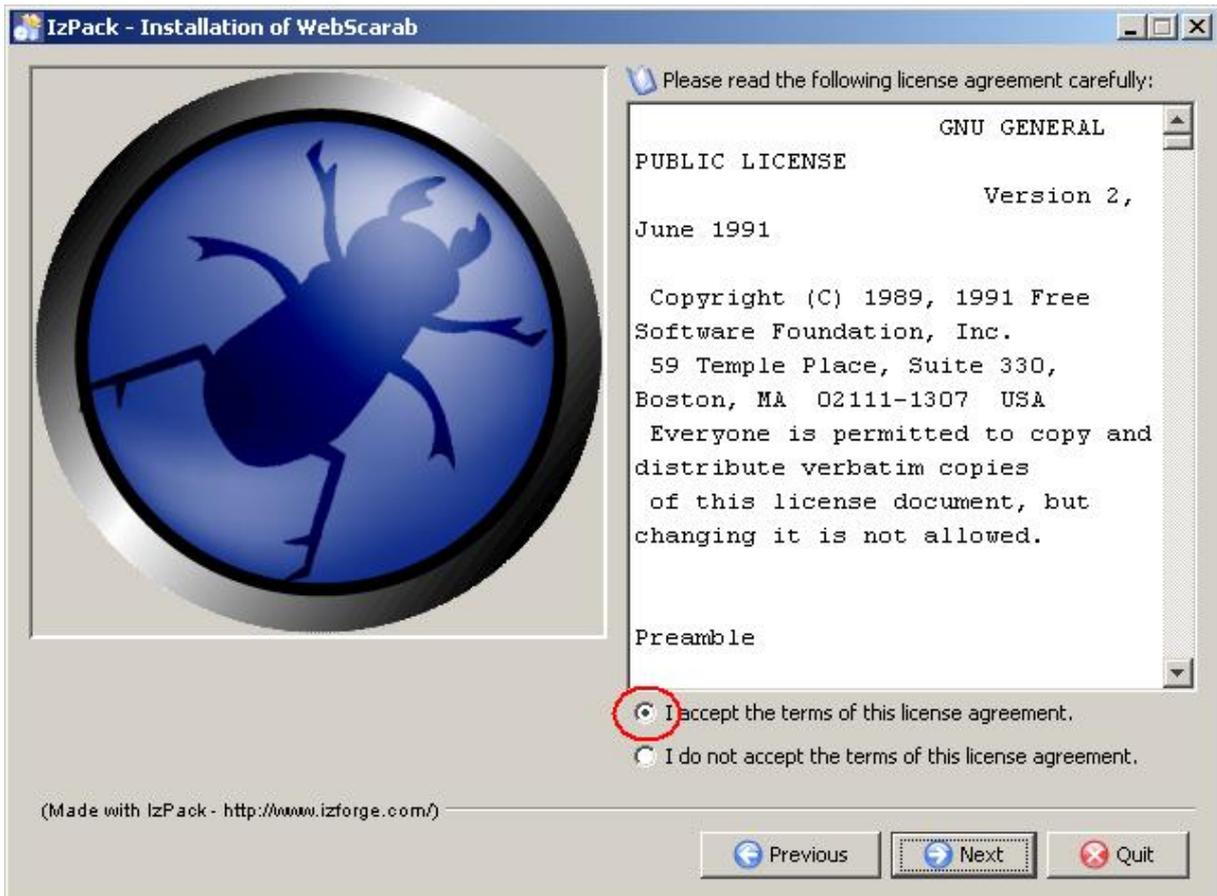
Please save the downloaded file in a suitable place (e.g. on your desktop) and install the software by double clicking on the file; installation should start automatically.

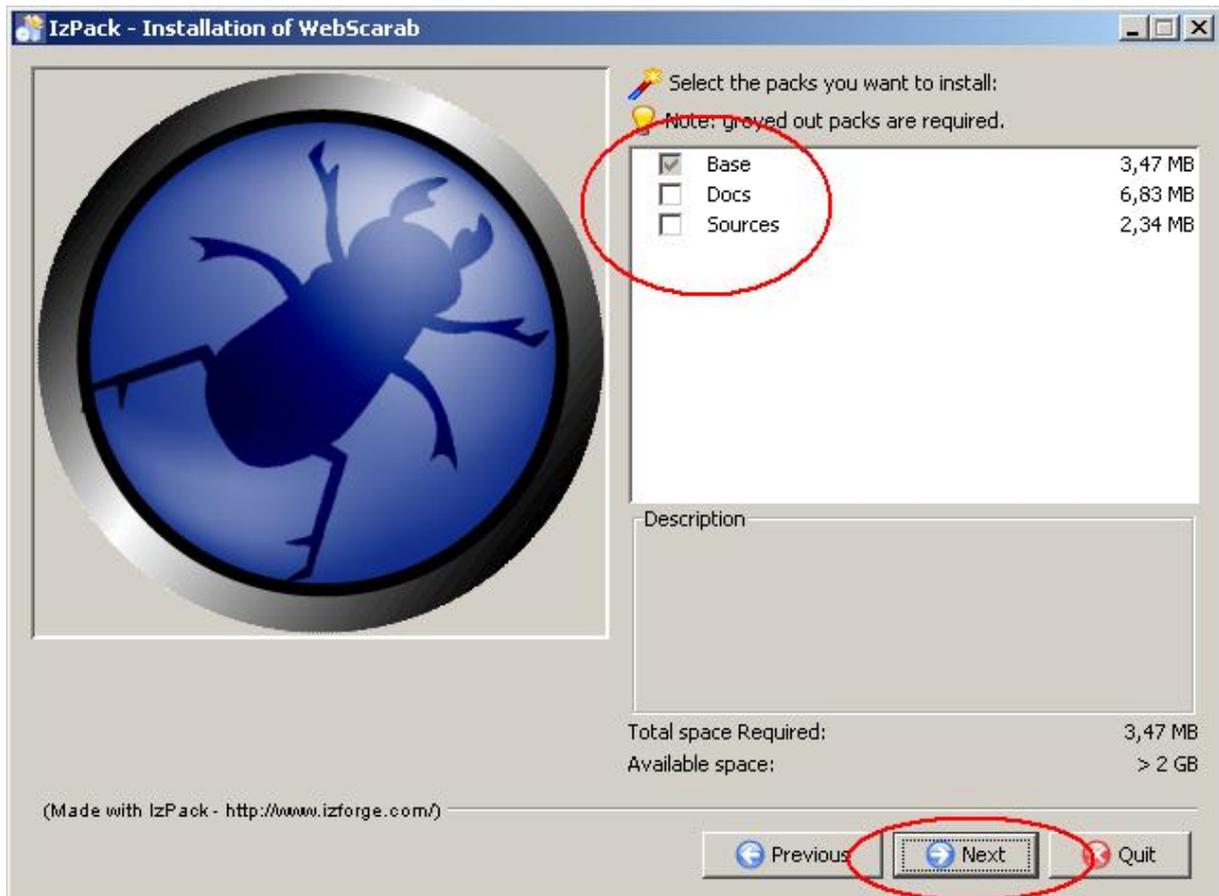
If installation does not start automatically, it may be because your Windows does not know yet how to execute a .jar file (namely, by handing that file to Java). If so, tell Windows how to do this: Right click on the .jar file, choose **Open With / Choose Program** and then choose the file `javaw.exe` in the Java installation directory on your computer (e.g. `C:\Program Files\Java\jre1.6.0_02\bin`), and check „Always use the selected program to open this kind of file“ or similar.

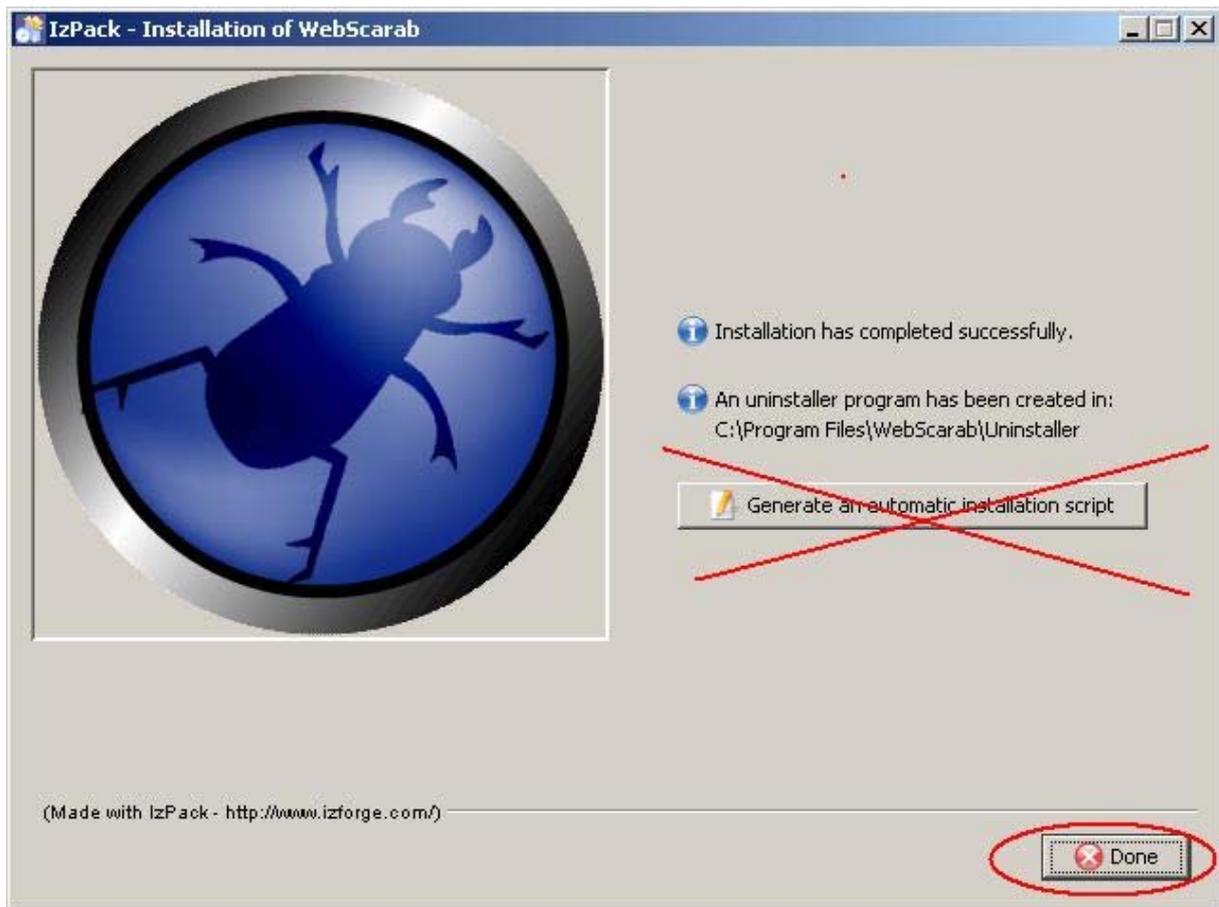
Installation

Install WebScarab like any other program (no administrative rights needed for this) by following the instructions of the installer; instead of `C:\Program Files` you can of course install it to any other place you want. Let the installation create a shortcut on the desktop for convenience during the tutorial.



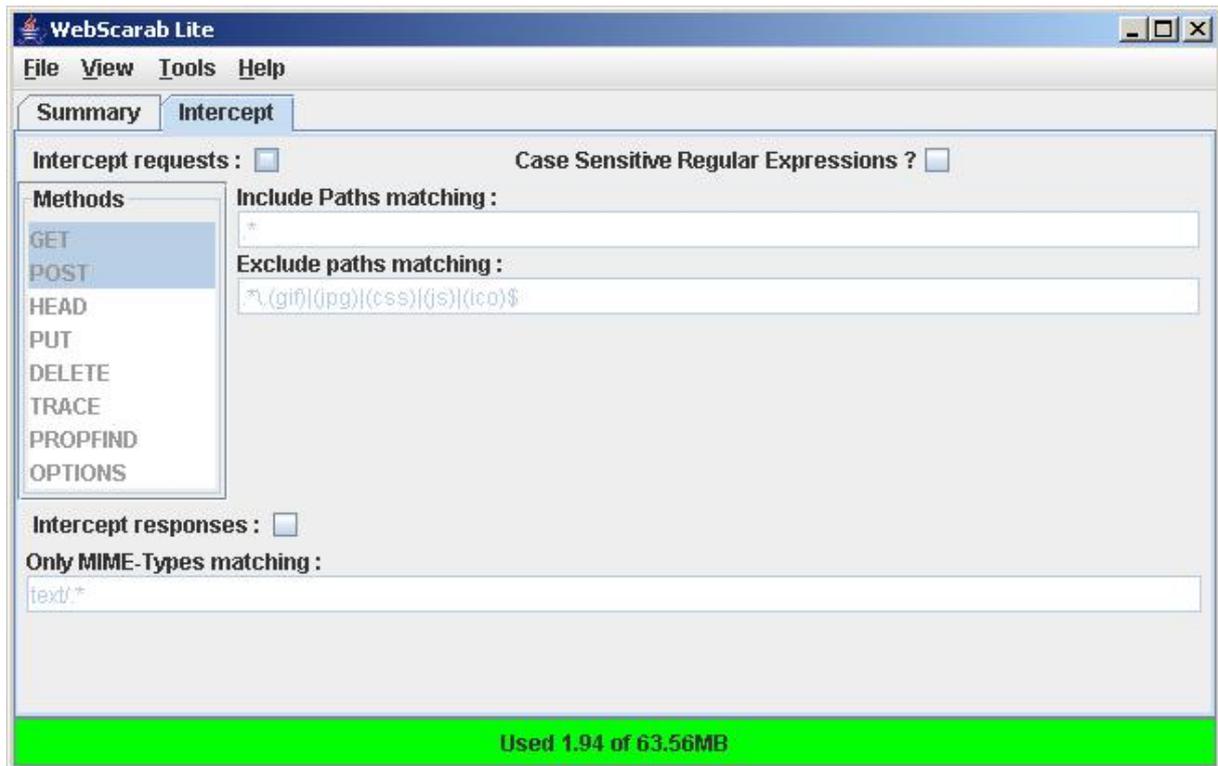






Starting WebScarab

After installation, you can start WebScarab by double clicking on the desktop shortcut just created (or by double clicking on the .jar in the directory where you installed WebScarab). If double clicking does not work, it may be because your Windows does not know yet how to execute a .jar file. The solution to that was described earlier in this text, at the end of the “Download” section. After a successful start, WebScarab should look like this:



Configuration

1) Set your external proxy in WebScarab

Start WebScarab, choose Tools / Proxies, and enter the name, port, and possibly exceptions of **your site's** HTTP proxy. Which one that is depends on your current network location: It may be the proxy of your company, or your home ISP, or none at all (in the latter case, you can just skip this step). If you don't know these settings, but can see web pages alright with Internet Explorer, you can copy Internet Explorer's settings using the "Get IE settings" button (only available on Windows). If that does not work, you copy the settings manually by reading them from IE's settings, to be found in the Tools menu of Internet Explorer: Tools / Internet Options / Connection / LAN Settings / Proxy Server.

During the actual tutorial at the conference, you will be in a dedicated wireless network where no such HTTP proxy is needed; accordingly, please delete the proxy settings in WebScarab at the start of the tutorial. However, to test WebScarab at your current location, you will need to enter the HTTP proxy settings that apply to you there (the instructor cannot help you to find out these settings; please ask a colleague or your help desk if you don't know these settings). Here is an example for the HTTP proxy settings (do not copy: these are valid only within the instructor's company network):

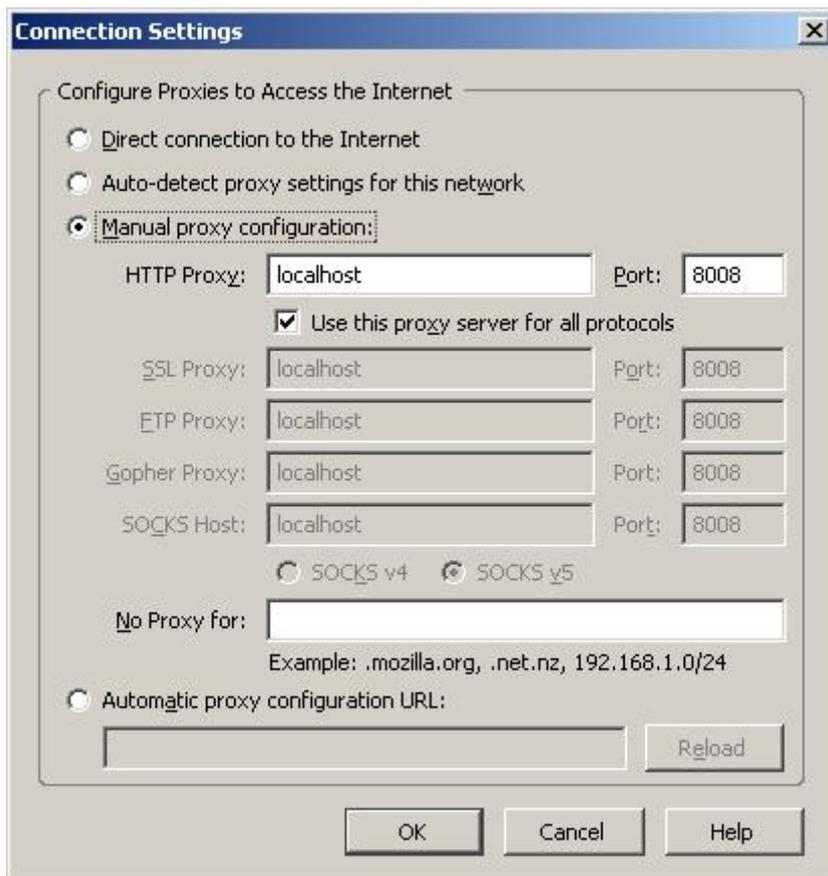


2) Set WebScarab as internal proxy in your browser

Now we need to tell the browser that, for the duration of using WebScarab, it should no longer use its usual external proxy, but instead use WebScarab as its proxy (“internal proxy”). We show how to do this for the Internet Explorer and Firefox browsers (for other browsers, such as Opera or Safari, you should easily find this out yourself):

Firefox

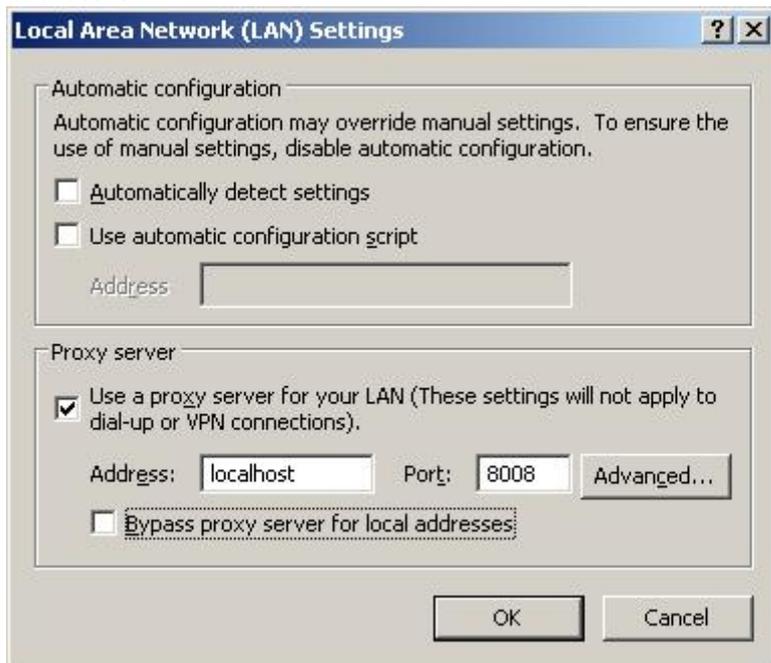
Please go to the following place: Tools / Options / Advanced / Network / Connection / Settings. Please enter localhost as the HTTP proxy, and 8008 as the port. Make sure that localhost does not(!) appear in the “No Proxy for” list:



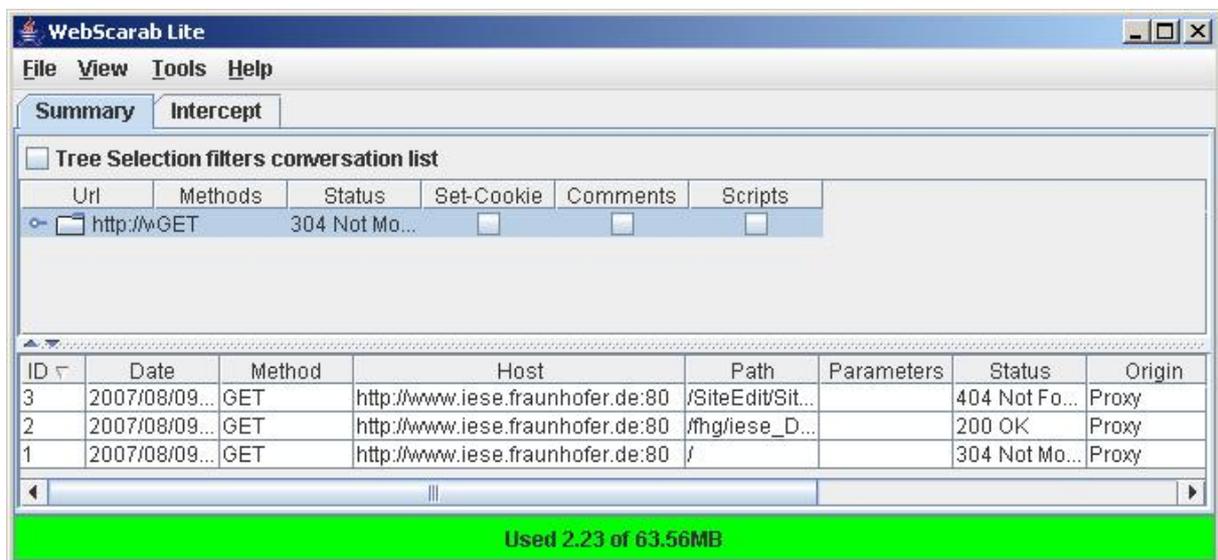
Internet Explorer

Please go to the following place:
Tools / Internet Options / Connections / LAN Settings

Check “Use a proxy server for your LAN“ and uncheck(!) „Bypass proxy server for local addresses“:



From now on, you need to have WebScarab running when you want to view a web page with your browser. It's best if you test this right now – you should be able to see a page in the browser, and the URL of that page should appear in the list of seen URLs in WebScarab's „Summary“-Tab (I've used the page www.iese.fraunhofer.de as an example in the picture below):



These steps are also described in the „WebScarab Tutorial“ http://www.owasp.org/index.php/WebScarab_Tutorial (but note that the screen shots there show the “full” user interface, not the “lite” one we use in this tutorial).

If you use WebScarab more than a few times, it becomes cumbersome to switch the browser's proxy repeatedly between WebScarab and the external proxy of your network. To ease this, if you use the Firefox browser, you can install an add-on named SwitchProxy from

<https://addons.mozilla.org/firefox/125/>; this lets you change the browser's proxy with a single click, once you have entered the proxies to choose from as a list.

Usage

WebScarab offers many flexible and automatable features to record, generate, edit, store and retrieve HTTP requests and responses, well as searching web sites, visualize session ids, and a few auxiliary functions for character encoding. However, most of these functions are not visible in the "lite" user interface (which is the default and which is sufficient for this tutorial); they can be accessed by choosing "Use full-featured interface" from the "Tools" menu).

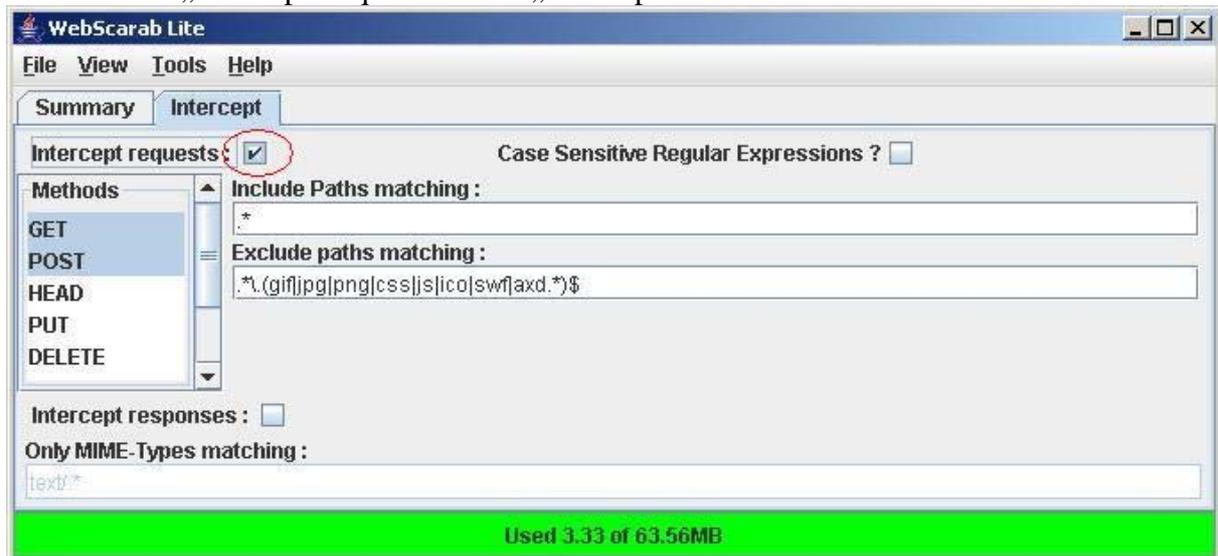
For the tutorial, we need only two functions of WebScarab:

- 1) Intercept, change and forward HTTP requests
- 2) Encode/decode character strings in Base64 and URL encoding

Both are shown in the following. If you want to know what else WebScarab can do (not needed for this tutorial), switch to the full-featured interface and consult the user manual at <http://dawes.za.net/rogan/webscarab/docs/> which is more detailed than what WebScarab shows under Help / Contents.

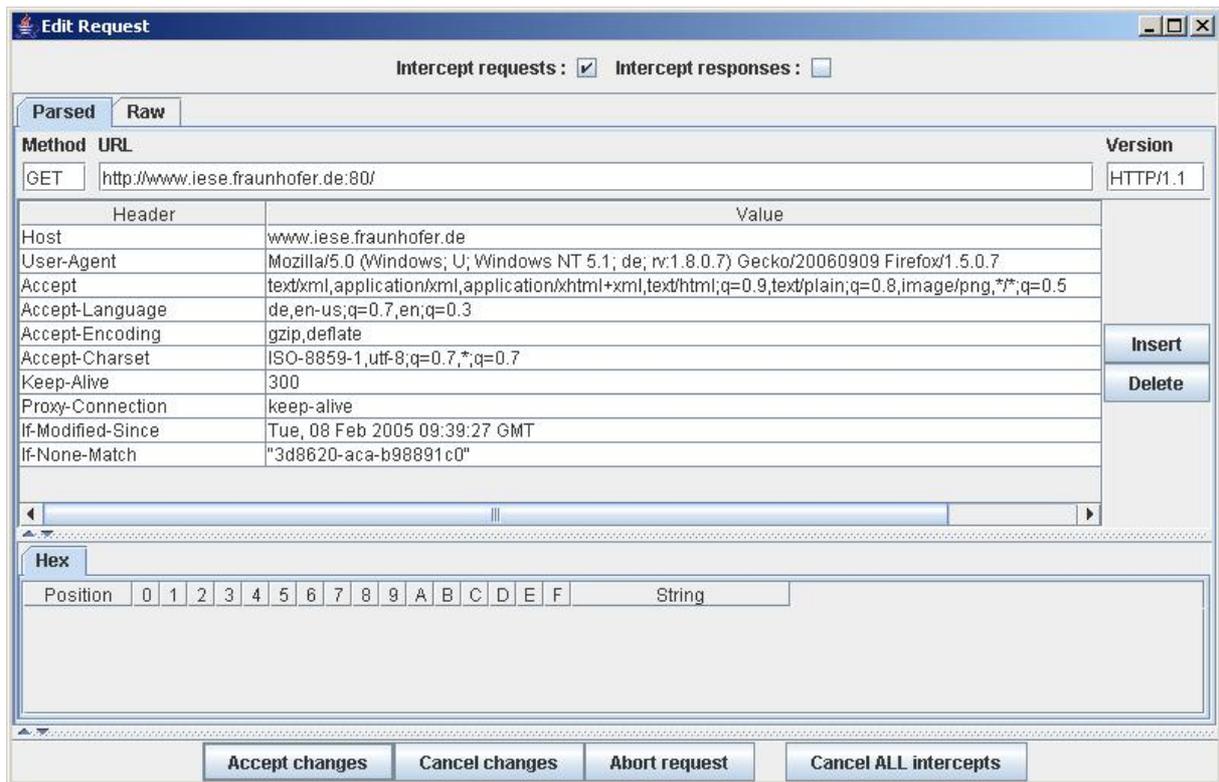
1) Intercept, change and forward HTTP requests

Please check „Intercept Request“ on the „Intercept“ tab:



Make sure that both GET and POST are active (i.e. with a blue background) – if not, activate them by control-leftclick.

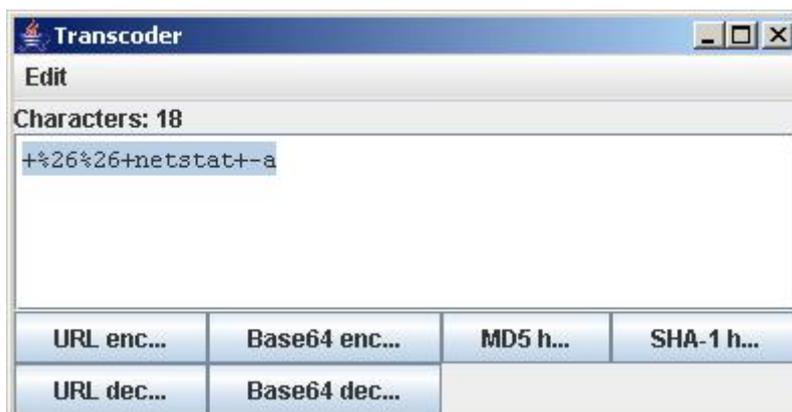
If you now want to view a web page with your browser, the HTTP request is intercepted by WebScarab and displayed for editing (the WebScarab icon in the desktop task bar is blinking):



Here you see an HTTP request for <http://www.iese.fraunhofer.de>. The request may be shown and edited in tabular form (“Parsed”, as in the picture above) or in linear textual form (“Raw”). After editing, you should uncheck „Intercept requests“ (on the top, in the middle of the window), before you forward the edited request with „Accept changes“ to its real destination (here: the web server at www.iese.fraunhofer.de). If you forget to uncheck, all subsequent requests will also be intercepted and offered for editing, and you have to click „Accept Changes“ quite a few times until the requested page finally appears in the browser.

2) (De-)Coding of strings in base64 or URL encoding

In HTTP, parameters in request URLs are URL-encoded (the “%” encoding; replaces blanks and special characters). HTTP authorization headers, for example, are base64-encoded. Under „Tools/Transcoder“ WebScarab offers a little tool to encode and decode such strings (also MD5 and SHA-1 hashes, but these are not needed for the tutorial). The strings can be pasted into and copied from the transcoder window by the usual ctrl-C / ctrl-V keys. The picture shows a string that was just URL-encoded:



Note that when editing parameter values in an intercepted request displayed in “Parsed” mode, you do not need to encode/decode manually: WebScarab does this automatically in that mode, i.e. you see the parameter value “as they should arrive”, and you can also write them in that way. (In “Raw” mode, you see parameter values URL-encoded and need to make sure that any of your changes are also URL-encoded.)