Valerio Colitta
Théo Foray

Testing:

The tests have been done at University.

Bad URL case:

To test if our proxy works correctly in this case, we tried it with the website URLs given in the assignment.

As it can be seen in the packet traces (Wireshark-Trace_UrlError), when the GET request is done, the proxy directly redirect because it has read SpongeBob in the URL, so the response received sends toward the appropriate error page https://www.ida.liu.se/~TDTS04/labs/2011/ass2/error1.html.

Bad content case:

To test, this case we tried the given website with a bad content, and the result is the redirection to https://www.ida.liu.se/~TDTS04/labs/2011/ass2/error2.html. As shown in the packet traces, (Wireshark-Trace_ContentError) there are two GET requests sniffed and two responses. This happened because, there is first, the GET request 'caught' by the proxy, and then because no problem have been detected in the URL, the new GET request our proxy generates (with the close connection). For the responses, the first sniffed, is from the website server to our proxy, but here our program detects forbidden content in the text data, so the proxy redirects.

Good website case:

Here, it is just to show, that the proxy doesn't alter the allowed content. Because the URL is correct, in the packet traces (Wireshark-Traces_GoodHTML) we see 2 GET Requests, the first that we catch, and then the second that leads to the same URL. Then, same for the responses, the first arrives to the proxy, it sees that everything is fine, and so forward it.

Discussing streaming, HTTPS, ...:

The goal of the proxy is to filter only HTTP request. This means all HTTPS requests do not pass by the proxy. In fact, we can browse Google, Youtube and any other website that uses HTTPS. The streaming works, so do Newspaper (lemonde.fr) websites (all using HTTPS).