Challenge 5

After some (pretty devastating) trial-and-error (~4 hrs), we managed to send a correct ipv6-packet with an empty tcp packet inside to the server. We had problems with tracking our files with wireshark, which weren‘t displayed for no apparent reason, until we moved location in the university (however that affects wireshark). Furthermore, the proxy does not seem to work properly as it does not says „packet sent“, although obviously the packets are received at the server.

We then created a working SYN-packet. Therefore, we manipulated the SYN-bit and edited the corresponding ports. We reveiced the SYN/ACK from the server and responded with a final ACK packet.

We then tried to build the HTTP-request inside the TCP-packet. We managed to figure out that we needed the „ISO-8859-1“ encoding and were able to get a response to our first HTTP request. It says „400- Bad Request“, and we did not had any clue why our request could be corrupted, since we basically copied it from the instructions. It was also displayed correctly within wireshark. After some extended research, we found the problem in the http specifications: We need to have a CLFR at the end of the request, so a normal ‚\n‘ does not suffice. We added the required ‚\r‘ and finally got our first hidden key.

We then proceeded to work with the next port/server, where a large http-respond was sent, which is divided into several segments. We therefore edited our receiving routine such that we send back appropiate ACK-packets upon receiving new data. The ACK-number is calculated with the sequence number of the incoming packet plus the data length of this packet. We had some problems with converting ints into byte arrays, but finally managed to receive the secret phrases from the second server.

These are the received phrases:

7710:

Daniel (416096):	The Gorilla Experiment
Jonas (428292):	The Zarnecki Incursion

7711:

Daniel (416096):	The Plimpton Stimulation
Jonas (428292):	The Rhinitis Revelation

Since we already invested ~7 hrs to get to the second server, and our exam weeks already start in about 10 days, we decided to stop here.

Jonas Becker (428292) & Daniel Beckmann (416096)